NetScaler Application Delivery Management 12.1

Machine translated content

Disclaimer

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

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Versionshinweise

February 5, 2024

In den Versionshinweisen für NetScaler Application Delivery Management (ADM) 12.1 werden die neuen Features, Erweiterungen vorhandener Features und die bekannten Probleme in einem Build beschrieben. Der Abschnitt mit den Versionshinweisen für die Version 12.1 umfasst 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
Release Rotes für Build 62.21 von NetScaler ADM 12.1 Release	Veröffentlichung: 13. Mai 2021	Version der Versionshinweise: 1.0
Release Rotes für Build 61.18 von NetScaler ADM 12.1 Release	Veröffentlicht: 04. Februar 2021	Version der Versionshinweise: 1.0
Versionshinweise für Build 60.16 von NetScaler ADM 12.1 Release	Veröffentlichung: 06. November 2020	Version der Versionshinweise: 1.0
Versionshinweise für Build 59.16 von NetScaler ADM 12.1 Release	Veröffentlichung: 28. September 2020	Version der Versionshinweise: 1.0
Versionshinweise für Build 58.14 von NetScaler ADM 12.1 Release	Veröffentlichung: 20. August 2020	Version der Versionshinweise: 1.0
Versionshinweise für Build 57.18 von NetScaler ADM 12.1 Release	Veröffentlichung: 11. Juni 2020	Version der Versionshinweise: 1.0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Versionshinweise	Datum der Veröffentlichung	Version
Versionshinweise für Build 56.22 von NetScaler ADM 12.1 Release	Veröffentlichung: 30. März 2020	Version der Versionshinweise: 1.0
Versionshinweise für Build 55.13 von NetScaler ADM 12.1 Release	Veröffentlichung: 07. November 2019	Version der Versionshinweise: 1.0
Versionshinweise für Build 54.13 von NetScaler ADM 12.1 Release	Veröffentlicht: 20. September 2019; aktualisiert am 26. September	Version der Release: 2.0
Versionshinweise für Build 53.12 von NetScaler ADM 12.1 Release	Veröffentlichung: 28. August 2019	Version der Release: 3.0
Versionshinweise für Build 52.15 von NetScaler ADM 12.1 Release	Veröffentlichung: 10. Juni 2019	Version der Versionshinweise: 1.0
Versionshinweise für Build 50.43 von NetScaler ADM 12.1 Release	Veröffentlichung: 17. Mai 2019	Version der Release: 2.0
Versionshinweise für Build 50.39 von NetScaler ADM 12.1 Release	Veröffentlichung: 17. Mai 2019	Version der Release: 2.0
Versionshinweise für Build 50.33 von NetScaler ADM 12.1 Release	Veröffentlichung: 16. April 2019	Version der Versionshinweise: 1.0
Versionshinweise für Build 50.30 von NetScaler ADM 12.1 Release	Veröffentlicht: 14. Januar 2019	Version der Versionshinweise: 1.0
Versionshinweise für Build 50.28 von NetScaler ADM 12.1 Release	Veröffentlichung: 1. Dezember 2018	Version der Versionshinweise: 1.0
Versionshinweise für Build 49.23 von NetScaler ADM 12.1 Release	Veröffentlichung: 29. August 2018	Version der Versionshinweise: 1.0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Versionshinweise	Datum der Veröffentlichung	Version
Versionshinweise für Build 48.18 von NetScaler ADM 12.1 Release	Veröffentlichung: 18. Juni 2018	Version der Release: 2.0

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

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, Systemanforderungen und Lizenzdetails lesen, bevor Sie Ihren Server auf die neueste Version von NetScaler ADM aktualisieren .

Schritt 1 - Überprüfen der Systemanforderungen

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

- **Informationen zur Lizenz**. Sie können beliebig viele Instanzen und Entitäten ohne Lizenz verwalten und überwachen. Sie können jedoch nur 30 erkannte Apps verwalten und Analyseinformationen für nur 30 virtuelle Server anzeigen, ohne eine Lizenz anzuwenden. Um mehr als 30 Apps zu verwalten oder Analysen für mehr als 30 virtuelle Server anzuzeigen, müssen Sie die entsprechenden Lizenzen erwerben. Erfahren Sie mehr.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Betriebssystem- und Empfängeranforderungen**. Überprüfen Sie diese Informationen, um sicherzustellen, dass Sie die richtige Empfängerversion für die unterstützten Betriebssysteme haben. Erfahren Sie mehr.
- **Anforderungen des Browsers**. 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 Datenverkehr. Sie können NetScaler ADM mit Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V und Linux KVM bereitstellen. Siehe:
  - NetScaler ADM mit Citrix Hypervisor
  - NetScaler ADM mit Microsoft Hyper-V
  - NetScaler ADM mit VMware ESXi
  - NetScaler ADM mit Linux KVM-Server
- **Bereitstellung mit hoher Verfügbarkeit.** Eine Hochverfügbarkeitsbereitstellung (HA) von zwei NetScaler ADM -Servern ermöglicht einen unterbrechungsfreien Betrieb. In einem

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Schritt 5: Konfigurieren des NTP-Servers auf NetScaler ADM

Konfigurieren Sie einen NTP-Server (Network Time Protocol) in NetScaler ADM, 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**. 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.
- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

So aktualisieren Sie NetScaler ADC SDX-Instanzen mithilfe von NetScaler ADM

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

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

Wie man ausgeführte Konfigurationsjobs wiederverwendet

Aktualisieren von NetScaler ADC-Instanzen mithilfe von NetScaler ADM

So verwenden Sie Variablen in Konfigurationsaufträgen auf NetScaler ADM

So verwenden Sie Konfigurationsvorlagen zum Erstellen von Überwachungsvorlagen auf NetScaler ADM

So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen in NetScaler ADM

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

Erstellen von Konfigurationsaufträgen für Citrix SD-WAN WO-Instanzen in Citrix ADM

So verwenden Sie Record and Play, um Konfigurationsaufträge zu erstellen

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

So verwenden Sie die Masterkonfigurationsvorlage in NetScaler ADM

So fragen Sie das Konfigurationsaudit von NetScaler ADC-Instanzen ab

So verwenden Sie Vorlagen für Konfigurationsprüfungen in Konfigurationsaufträgen wieder

So importieren und exportieren Sie Konfigurationsvorlagen

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zertifikatverwaltung

So konfigurieren Sie eine Unternehmensrichtlinie in NetScaler ADM

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

So aktualisieren Sie ein installiertes Zertifikat von NetScaler ADM

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

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

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

So verwenden Sie das SSL-Dashboard auf NetScaler ADM

Abfragen von SSL-Zertifikaten von NetScaler ADC Instanzen

Anwendungsverwaltung

Erstellen einer Anwendungsdefinition in Citrix ADM

StyleBooks

So zeigen Sie verschiedene Gruppen von StyleBooks an

So verwenden Sie StyleBooks, die mit Citrix ADM geliefert werden

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Analytics

Ereignisverwaltung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Authentifizierung

Kaskadieren externer Authentifizierungsserver

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

Diagnose und Problembehandlung von Citrix ADC Instanzen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Netzwerkfunktionen

So generieren Sie Berichte für Load-Balancing-Entitäten

So exportieren oder planen Sie den Export von Netzwerkfunktionsberichten

Übersicht

February 5, 2024

Citrix Application Delivery Management (ADM) ist eine zentralisierte Verwaltungslösung, die den Betrieb vereinfacht, indem Administratoren unternehmensweite Transparenz bieten und Verwaltungsaufträge automatisieren, 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 von Webseiten
- -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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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 außerdem angriffsbezogene Informationen wie Syn-Angriffe, Angriffe mit kleinem Fenster und DNS-Überschwemmungsattacken 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 wissen, was ein SSL-Zertifikat ist und wie Sie ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Konfigurationsverwaltung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-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.

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

Citrix 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

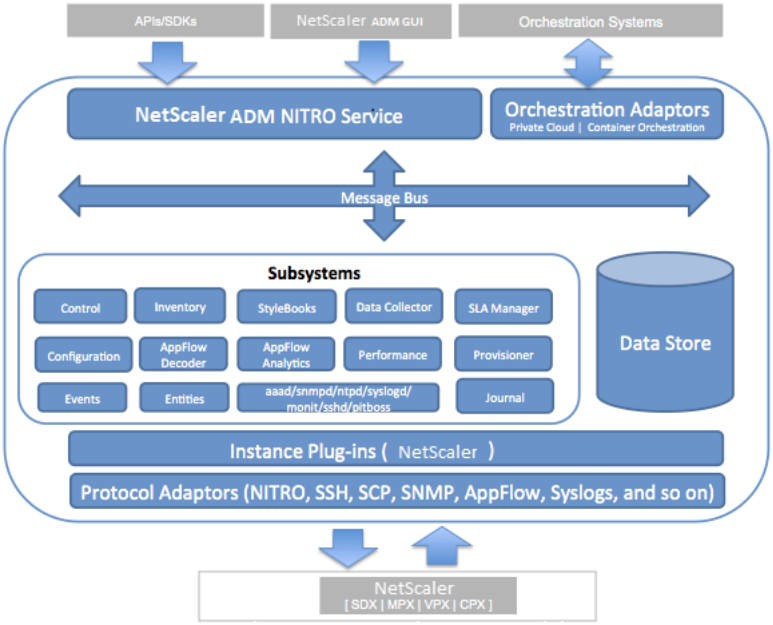
February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-Anforderungen und -Antworten verarbeitet, die über die GUI oder API an Subsytems innerhalb von ADM gesendet werden. Dabei werden die Ports 80 und 443 verwendet. 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 Teilsysteme —Inventory, StyleBooks, Datensammlung, Konfiguration, AppFlow Decoder, AppFlow Analytics, Leistung, Ereignisse, Entitäten, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

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

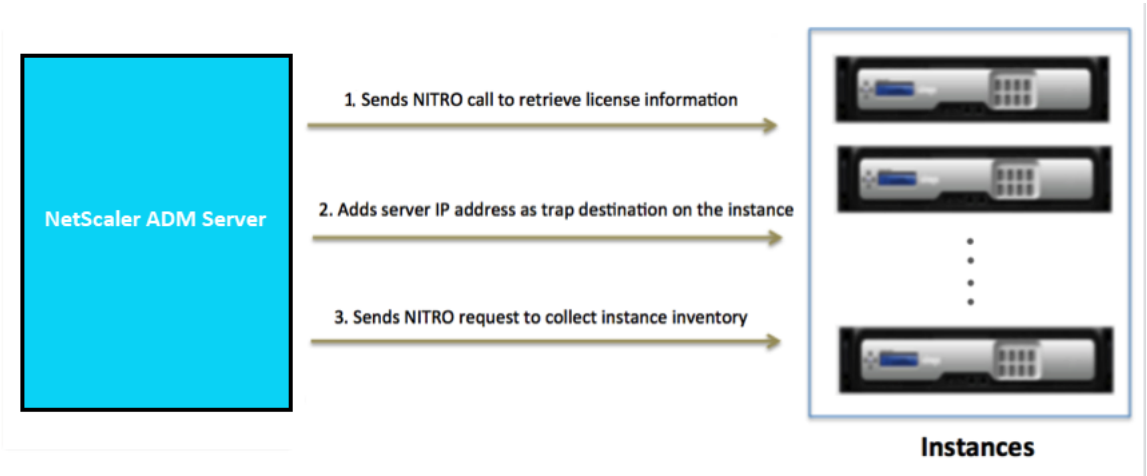
Sie können Instanzen hinzufügen, wenn Sie den NetScaler ADM-Server zum ersten Mal oder später einrichten.

> **Hinweis**
>
> NetScaler ADM verwendet die NetScaler IP (NSIP) -Adresse der NetScaler ADC Instanzen für die Kommunikation. ADM kann auch ADC-Instanzen mit Subnetz-IP (SNIP) -Adresse erkennen, für die der Verwaltungszugriff aktiviert ist. Informationen zu den Ports, die zwischen den ADC-Instanzen und ADM geöffnet sein müssen, finden Sie unter Ports.
>
> 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wie im Diagramm gezeigt, werden die folgenden Schritte implizit von Citrx ADM ausgeführt.

1. NetScaler ADM verwendet die Details des Instanzprofils, um sich bei der Instanz anzumelden. ADM ruft mithilfe eines ADC NITRO -Aufrufs die Lizenzinformationen der Instanz ab. Basierend auf den Lizenzinformationen wird bestimmt, ob es sich bei der Instanz um eine ADC-Instanz handelt, und um den Typ der ADC-Plattform (z. B. Citrix ADC MPX, ADC VPX, ADC SDX oder Citrix 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- und Citrix Gateway-Instanzen schlägt dieser Schritt möglicherweise auch fehl, 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, Zertifikatdetails, auf der Instanz konfigurierte Entitäten usw.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 30 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Abfrage-Typ	Abfrageintervall	Abgefragte Informationen	Verwendetes Protokoll	Konfiguration des Abrufin
Entitätsabfrage	Alle 30 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.	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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-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**.

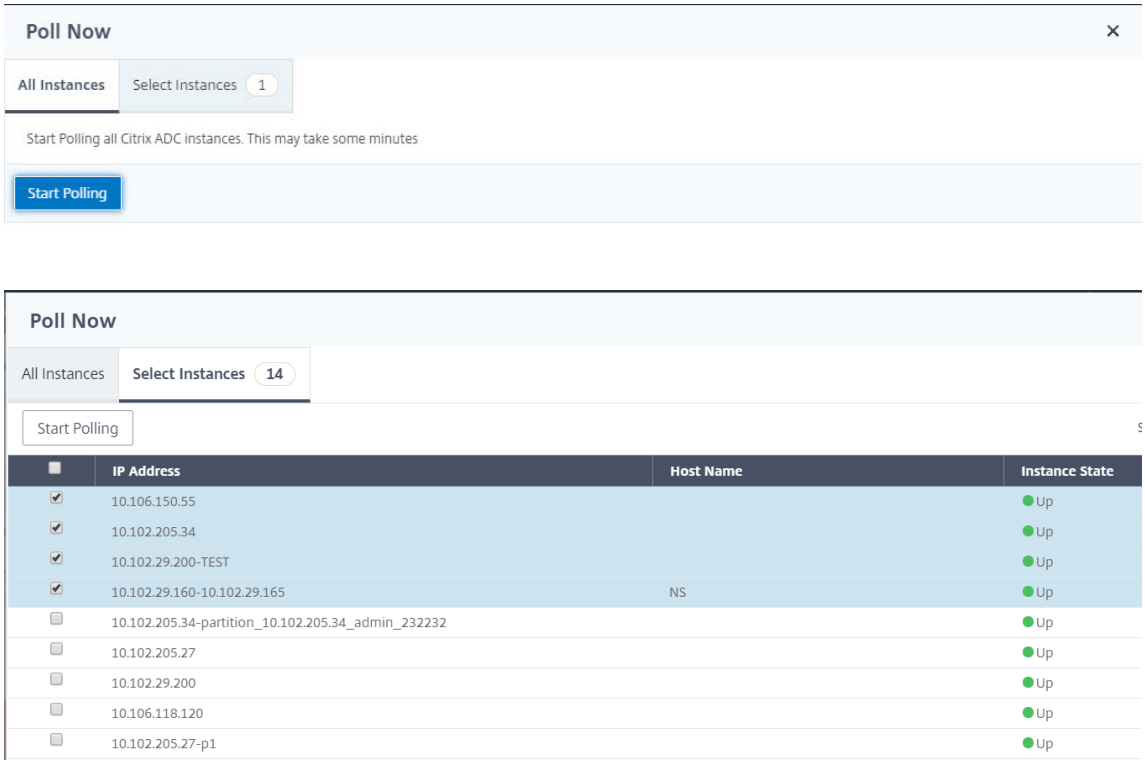
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix ADM nur diese Entität ab und aktualisiert den Status in der Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

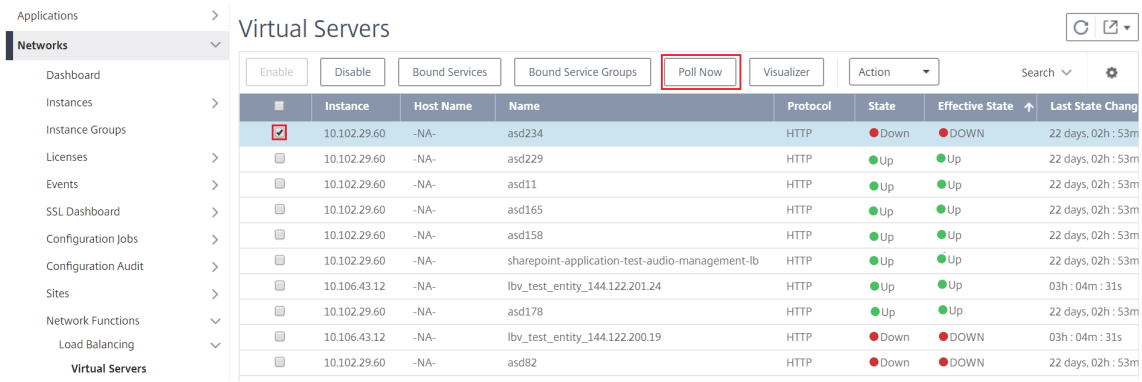
Sie können nun die folgenden Entitäten nach jedem Update in ihrem Status abfragen: Dienste, Dienstgruppen, virtuelle Server für den Lastausgleich, virtuelle Server zur Cachereduzierung, virtuelle Content Switching-Server, virtuelle Authentifizierungsserver, virtuelle VPN-Server, virtuelle GSLB-Server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

Die Kundenauthentifizierung ist für ein Unternehmen von entscheidender Bedeutung, da sie es dem Unternehmen ermöglicht, seine Netzwerkressourcen zu schützen, indem nur authentifizierte Kunden

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

oder Benutzer auf sein Netzwerk zugreifen können. Als Administrator ist es wichtig, dass Sie Ihre Benutzer identifizieren, bevor Sie sie eine Verbindung zu den Ressourcen im Citrix-Netzwerk herstellen lassen.

Ab Version 12.1 Release 50.x verlangt Citrix Application Delivery Management (ADM), dass Sie sich auf der ADM-GUI authentifizieren, bevor Sie auf die Informationen zugreifen können. Es ist erforderlich, dass Sie sich bei Citrix Cloud Services registrieren, bevor Sie sich bei ADM authentifizieren. Sie müssen die Citrix Cloud-Benutzeranmeldedaten auf der ADM-GUI angeben. Weitere Informationen finden Sie unter Registrieren für Citrix Cloud.

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, 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.
5. Die Seite Kundenidentität 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 auf Citrix Cloud, um sich zu registrieren.
6. Klicken Sie auf Authentifizieren und geben Sie Ihre E-Mail-Adresse ein, mit der Sie sich bei Citrix Cloud registriert haben.
7. Aktivieren Sie das Kontrollkästchen neben “Ich stimme zu, Daten für Telemetrie freizugeben” und klicken Sie auf Absenden.

Workflow, wenn Sie bereits ein Benutzer sind, der auf die neueste Version 12.1 aktualisiert

1. Geben Sie nach dem Upgrade von Citrix ADM auf die neueste Version in Version 12.1 in einem Webbrowser die IP-Adresse des Citrix ADM ein.
2. Geben Sie in den Feldern Benutzername und Kennwort die Administratoranmeldeinformationen ein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Die Seite Kundenidentität 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 auf Citrix Cloud, um sich zu registrieren.

4. Klicken Sie auf Authentifizieren und geben Sie Ihre E-Mail-Adresse ein, 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 zu einem späteren Zeitpunkt auf eine der folgenden beiden Arten in ADM konfigurieren:

- indem Sie zu **System** > Systemadministration navigieren und auf Authentifizierung klicken.
- indem Sie auf das Wolkensymbol oben rechts in der ADM-GUI klicken. Nach erfolgreicher Authentifizierung verwandelt sich das „X"in ein grünes 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 auf Citrix ADM und die Nutzung der Funktionen von Citrix ADM erklären Sie sich damit einverstanden, dass Citrix technische, Benutzer- oder verwandte Informationen zu Ihren Citrix-Produkten und -Diensten sammelt, speichert, überträgt, verwaltet, verarbeitet und verwendet.

Informationen, die Citrix erhält, werden jederzeit gemäß der Datenschutzrichtlinie von Citrix.com behandelt.

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 nur 30

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

virtuelle Server einsehen, ohne eine Lizenz beantragen zu müssen. Um mehr als 30 erkannte Anwendungen zu verwalten oder Analysen für mehr als 30 virtuelle Server anzuzeigen, müssen Sie Lizenzen erwerben und anwenden.

	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
	HDX Insight*	Nein	Ja	Enterprise (Berichterstattung < 1 Stunde) Premium (Berichterstattung = Unbegrenzt)
	Security Insight	Nein	Ja	Premium (oder) Enterprise mit App Firewall-Lizenz
	SSL Insight	Nein	Ja	Nicht zutreffend
	Gateway Insight	Nein	Ja	Enterprise (Berichterstattung < 1 Stunde) Premium (Berichterstattung = Unbegrenzt)
	TCP Insight	Nein	Ja	Nicht zutreffend
	Video Insight	Nein	Ja	Premium (Citrix-T 1000-Serie, VPX-T)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	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
	WAN-Einblick	Nein	Nicht zutreffend	Die Citrix SD-WAN-Instanz sollte Optimization Edition (WANOP) sein
Anwendungen				
	Anwendungsstatistiken (App-Dashboard, App-Sicherheitsdashboard)	Nein	Ja	Für Informationen zur Citrix ADC Web App Firewall zum App-Dashboard und zum App-Sicherheits-Dashboard ist eine Premium- (oder) Enterprise mit App Firewall-Lizenz erforderlich.
	StyleBooks	Ja	Nein	Nicht zutreffend
Netzwerke				
	Lizenzserver	Ja	Nein	Nicht zutreffend
	Inventarverwaltung—Infrastruktur-Dashboard, Instanzgruppen, Instanz-Dashboard und Sites	Ja	Nein	Nicht zutreffend

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	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
	Eventmanagement & Syslog	Ja	Nein	Nicht zutreffend
	Konfigurationsaufträge, Konfigurationsaudit und Konfigurationsberatung	Ja	Nein	Nicht zutreffend
	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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	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
System				
	RBAC & externe Authentifizierung (Instanzebene)	Ja	Nein	Nicht zutreffend
	RBAC & externe Authentifizierung	Ja	Nein	Nicht zutreffend
Orchestrierung				
	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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

*Für die Integration von Citrix Director mit der Citrix ADM-Unterstützung sollte 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.

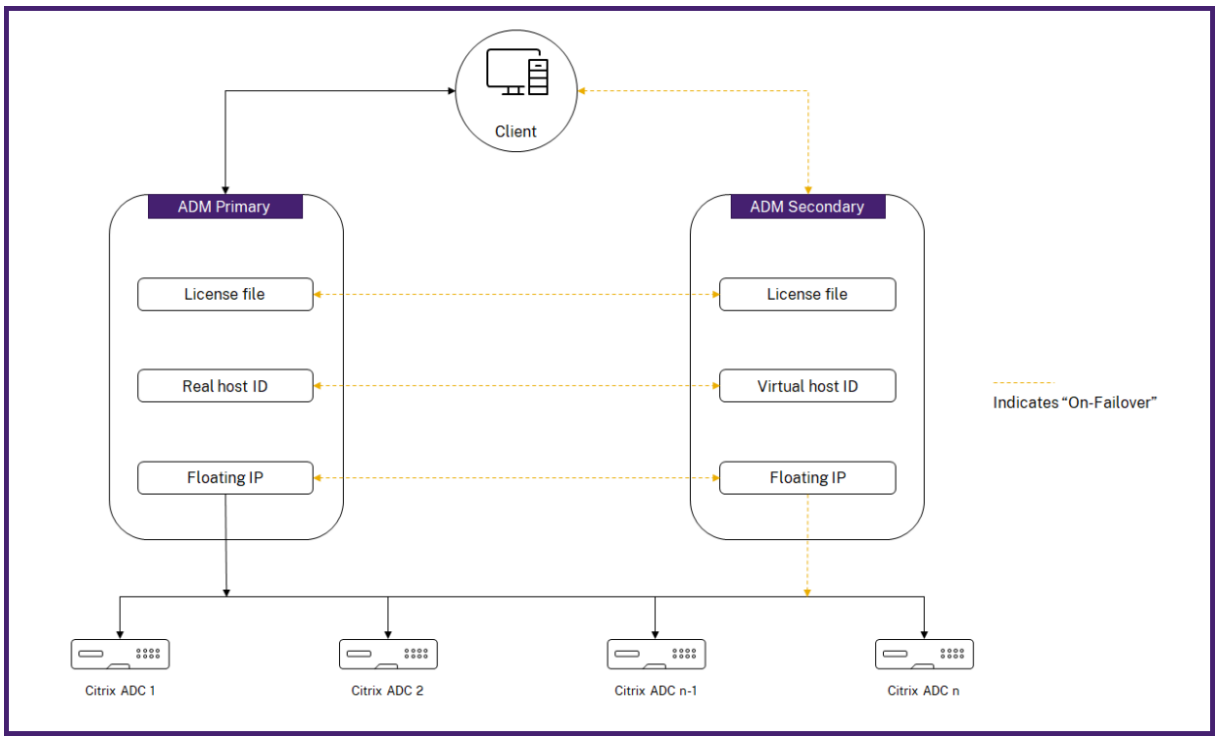
> **Hinweis**
>
> - Wenn Sie Citrix ADM 12.1.49.x oder frühere Versionen installiert haben, erhalten Sie eine Übergangsfrist von 30 Tagen, um die Lizenzierung auf dem sekundären Knoten aufrechtzuerhalten. Nach Ablauf der Übergangsfrist müssen Sie sich an Citrix wenden, um die ursprüngliche Lizenz erneut 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

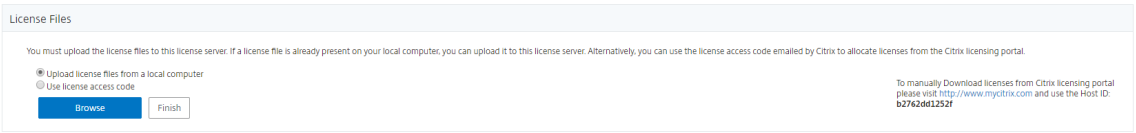
Aktualisieren Sie die virtuellen Serverlizenzen

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.

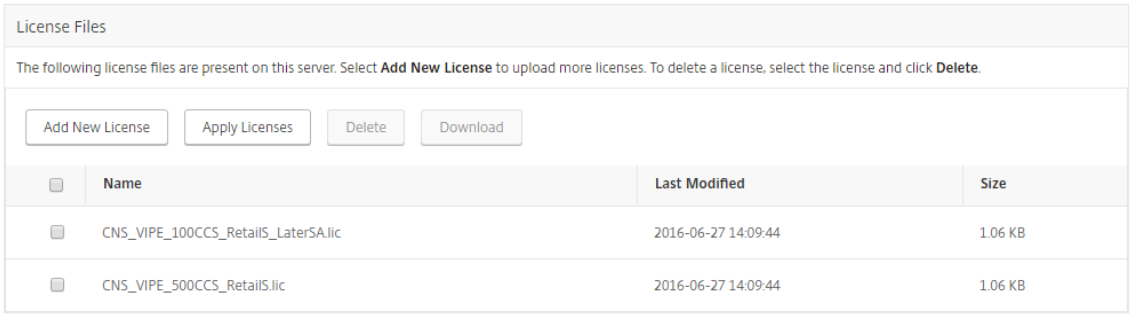
So aktualisieren Sie Ihre Appliance-Lizenzen:

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.



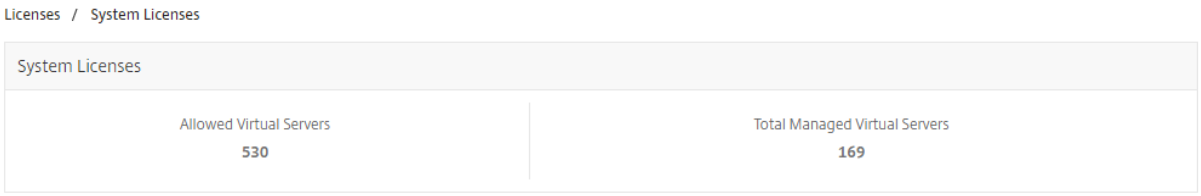
4. Auf der Seite Lizenzeinstellungen können Sie jederzeit weitere Lizenzen hinzufügen.



Verifizierung

Sie können die auf Ihrem Citrix ADM installierten Lizenzen überprüfen, indem Sie zu**Netzwerke** > **Lizenzen >**Systemlizenzen**navigieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Lizenzieren Sie die virtuellen Server

Sie können die virtuellen Server auswählen, die über Citrix ADM verwaltet und überwacht werden sollen. Wenn die Gesamtzahl der von den erkannten Citrix ADC-Instanzen gehosteten virtuellen Server niedriger ist als die Anzahl der installierten virtuellen Serverlizenzen, lizenziert Citrix ADM alle virtuellen Server.

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

Wichtige Hinweise:

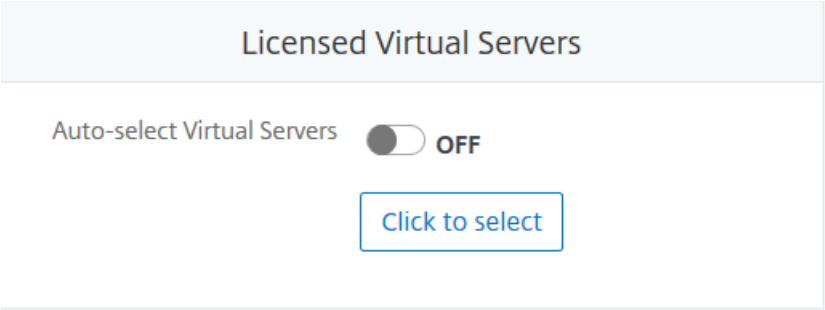
- Standardmäßig lizenziert Citrix ADM die virtuellen Server nach jedem virtuellen Serverabfragungszyklus automatisch nach dem Zufallsprinzip.
- Wenn die Gesamtzahl der in Ihrem Citrix ADM erkannten virtuellen Server niedriger ist als die Anzahl der installierten virtuellen Serverlizenzen, lizenziert 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.
- Citrix ADM lizenziert die nicht adressierbaren virtuellen Server nicht. Um sie zu verwalten, müssen Sie sie manuell lizenzieren.

Um die lizenzierten virtuellen Server zu verwalten:

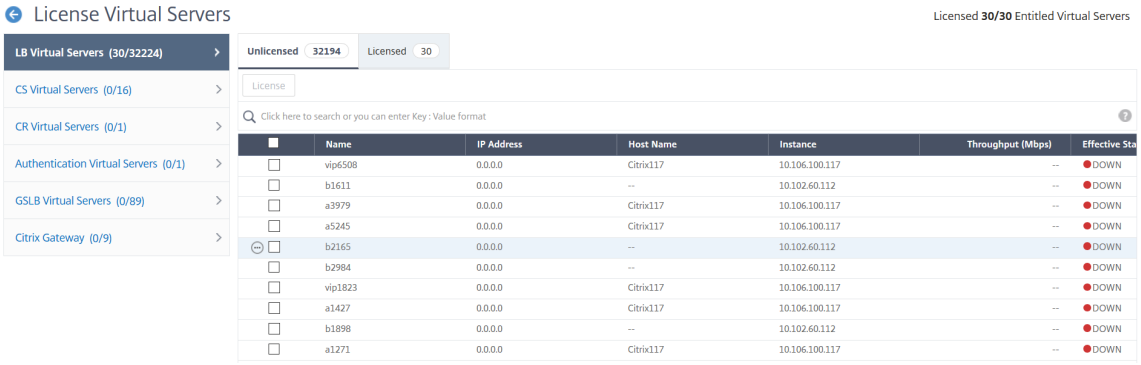
1. Melden Sie sich mit den Administratoranmeldeinformationen bei Citrix ADM an.
2. Navigieren Sie zu **Netzwerke > Lizenzen > Systemlizenzen**.

   Das Systemlizenz-Dashboard wird angezeigt.
3. Deaktivieren Sie unter **Lizenzierte virtuelle Server**die Option **Virtuelle Server automatisch auswählen** und klicken Sie auf die Option **Zum Auswählen klicken** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Wählen Sie im Fenster**Virtuellen Lizenzserver**den Typ der virtuellen Server aus, indem Sie auf die entsprechende Registerkarte klicken.



5. Wählen Sie auf der Registerkarte **Nicht lizenziert** die virtuellen Server aus, die Sie lizenzieren möchten, und klicken Sie auf **Lizenz**. Wählen Sie auf der Registerkarte **Lizenziert** die virtuellen Server aus, für die Sie die Lizenzierung aufheben möchten, und klicken Sie auf Lizenzierung **aufheben**.

6. Klicken Sie auf**Weiter**, um zur Registerkarte der anderen virtuellen Server zu wechseln, oder klicken Sie auf**Speichern und Beenden**, um die ausgewählten virtuellen Server zu lizenzieren.

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 neue Option unter **Netzwerke** > **Lizenzen** > **Systemlizenzen**. Das heißt, die neue Option **Automatische Auswahl nicht adressierbarer virtueller Server**. Wenn Sie diese Option aktivieren, können Sie jetzt explizit angeben, dass die Lizenzierung auch nicht adressierbare virtuelle Server enthalten muss.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Ablaufüberprüfungen 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-Profil:** SMS-Profil oder Verteilerliste für den Versand von Benachrichtigungen, wenn Lizenzen den Schwellenwert erreichen oder ablaufen.
    - **Warnschwellenwert:** 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.
    - **Tage bis zum Ablauf:**Anzahl der verbleibenden Tage bis zum Ablauf.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-Drive-Technologie (SSD) für Citrix ADM-Bereitstellungen.
Speicherplatz	Der Standardwert ist 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Verwenden Sie den Größenrechner, der im Abschnitt **Höchstgrenzen** (Seite 7) im Citrix 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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Komponente	Voraussetzung
	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	8 GB **Hinweis**: Der Standardwert ist 8 GB. Citrix empfiehlt, den Standardwert für eine bessere Leistung auf 32 GB zu erhöhen.
Virtuelle CPU	2 CPUs **Hinweis**: Die Standardeinstellung ist 2 CPUs. Citrix empfiehlt, den Standardwert für eine bessere Leistung auf 8 CPUs zu erhöhen.
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-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Platinum- und Enterprise-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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enterprise	Ja	Ja	Nein	Nein	Nein
Platinum	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 und 6.7
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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Unterstützte Ports

NetScaler ADM verwendet die NetScaler ADC-IP-Adresse (NSIP), um mit NetScaler ADC zu kommunizieren. Für die Kommunikation zwischen NetScaler ADC-Instanzen und NetScaler ADM oder Citrix SD-WAN-Instanzen und NetScaler ADM müssen die folgenden Ports in NetScaler ADM geöffnet sein:

> **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 Citrix ADM bleiben die folgenden Ports gleich.

Typ	Port	Details	Richtung der Kommunikation
———	——-	———	——
TCP	80/443	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 Hochverfügbarkeitsmodus.	NetScaler ADM an NetScaler ADC und NetScaler ADC an NetScaler ADM
TCP	22	Für die SSH-Kommunikation von NetScaler ADM zur NetScaler ADC - oder Citrix SD-WAN Instanz. Für die Synchronisierung zwischen NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus bereitgestellt werden. Und dieser Port ist für die SSH-Kommunikation zwischen dem ADM-Agent und NetScaler ADC erforderlich.	NetScaler ADM an NetScaler ADC und NetScaler ADM Agent an NetScaler ADC
UDP	4739	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
ICMP	Kein reservierter Port	Erkennen der Netzwerkerreichbarkeit zwischen NetScaler ADM- und NetScaler ADC-Instanzen, SD-WAN-Instanzen oder dem sekundären NetScaler ADM-Server, der im Hochverfügbarkeitsmodus bereitgestellt wird.
UDP	161, 162	So empfangen Sie SNMP-Ereignisse von der NetScaler ADC-Instanz an NetScaler ADM.	**Port 161**—Citrix ADM zu Citrix ADC
		Port 162 - NetScaler ADC zu NetScaler ADM
UDP	514	So empfangen Sie Syslog-Nachrichten von der NetScaler ADC - oder Citrix SD-WAN-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instanz an NetScaler ADM.|NetScaler ADC oder Citrix SD-WAN an NetScaler ADM |
TCP	25	So senden Sie SMTP-Benachrichtigungen von NetScaler ADM an Benutzer.
TCP	389/636	Standardport für Authentifizierungsprotokoll. Für die Kommunikation zwischen NetScaler ADM und dem externen LDAP-Authentifizierungsserver.|Externer Authentifizierungsserver von NetScaler ADM zu LDAP
UDP	123	Standard-NTP-Serverport für, Synchronisierung mit mehreren Zeitquellen.
RADIUS	1812	Standardport für Authentifizierungsprotokoll. Für die Kommunikation zwischen NetScaler ADM und dem externen RADIUS-Authentifizierungsserver. |NetScaler ADM zu RADIUS externer Authentifizierungsserver
TACACS	49	Standardport für Authentifizierungsprotokoll. Für die Kommunikation zwischen NetScaler ADM und dem externen TACACS Authentifizierungsserver. |Externer Authentifizierungsserver von NetScaler ADM zu TACACS
TCP	5563	Um ADC-Metriken (Leistungsindikatoren), Systemereignisse und Überwachungsprotokollmeldungen von der NetScaler ADC-Instanz an NetScaler ADM zu empfangen. |NetScaler ADC zu NetScaler ADM
TCP	5557/5558	Für die **Logstream**-Kommunikation (für Security Insight, Web Insight und HDX Insight) von Citrix ADC zu Citrix ADM. |NetScaler ADC zu NetScaler ADM
TCP	5454	Standardport für die Kommunikation und Datenbanksynchronisierung zwischen NetScaler ADM Knoten im Hochverfügbarkeitsmodus.|Primärer NetScaler ADM-Knoten zum sekundären NetScaler ADM-Knoten
TCP	27000	Lizenzport für die Kommunikation zwischen dem NetScaler ADM -Lizenzserver und der CPX-Instanz.|NetScaler ADC zu NetScaler ADM
TCP	7279	Port für Citrix Vendor Daemon.|NetScaler ADC zu NetScaler ADM
TCP| 443/8443/7443|Port für die Kommunikation zwischen NetScaler ADM Agent und NetScaler ADM. Der ADM-Agent initiiert die Kommunikation mit NetScaler ADM.	NetScaler ADM-Agent zu NetScaler ADM|

Einschränkungen

In 12.1 NetScaler ADM 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Bereitstellen

February 5, 2024

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

- **Bereitstellung auf einem Server**.In einer NetScaler ADM Einzelserverbereitstellung ist die Datenbank in den Server integriert, und ein einzelner Server verarbeitet den gesamten Datenverkehr. Sie können Citrix 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 (HA).** Eine HA-Bereitstellung von zwei Citrix ADM Servern sorgt für einen unterbrechungsfreien Betrieb. Bei einem Hochverfügbarkeit-Setup müssen beide NetScaler ADM Knoten im Aktiv-Passiv-Modus, im selben Subnetz mit derselben

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Softwareversion und demselben Build bereitgestellt werden und über dieselben Konfigurationen verfügen. Bei der HA-Bereitstellung macht die Möglichkeit, die Floating-IP auf dem primären Citrix ADM Knoten zu konfigurieren, einen separaten NetScaler Load Balancer überflüssig.Siehe:Konfiguration in Hochverfügbarkeitsbereitstellung.

- **Migrieren Sie von NetScaler Insight Center zu Citrix ADM**. Sie können Ihre NetScaler Insight Center-Bereitstellung zu Citrix ADM migrieren, ohne die vorhandene Konfiguration, Einstellungen oder Daten zu verlieren. Mit Citrix ADM können Sie nicht nur die verschiedenen Analysen anzeigen, die von den NetScaler- und NetScaler SD-WAN-Instanzen generiert wurden, sondern auch die gesamte globale Infrastruktur für die Anwendungsbereitstellung von einer einzigen, einheitlichen Konsole aus verwalten, überwachen und Fehler beheben. Siehe:Migration von NetScaler Insight Center zu NetScaler ADM
- **Integrieren Sie Citrix ADM mit Director**. Director lässt sich für Netzwerkanalyse und Leistungsmanagement in Citrix ADM integrieren. Siehe: Integrieren von NetScaler ADM mit Director

Voraussetzungen für die Installation von NetScaler ADM

February 5, 2024

Sie können Citrix 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 Version 12.1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	Citrix empfiehlt die Verwendung von Solid-State-Laufwerk-Technologie (SSD) für NetScaler ADM Bereitstellungen. Der Standardspeicherplatz beträgt 120 GB. Die tatsächliche Speicheranforderung hängt von der Schätzung der NetScaler ADM Größe ab. Verwenden Sie den Größenrechner, der im Abschnitt **Höchstgrenzen** (Seite 7) im Citrix 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 Speicheranforderung 120 GB überschreitet, müssen Sie einen zusätzlichen Datenträger bereitstellen. Citrix empfiehlt, zum Zeitpunkt der Erstbereitstellung den Speicher zu schätzen und zusätzlichen Datenträger anzuhängen. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler ADM mit 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.

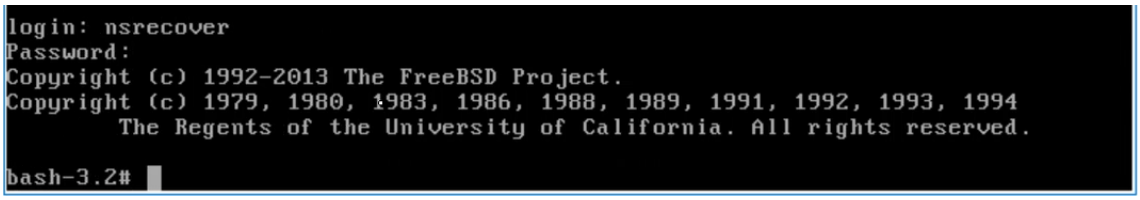
Komponente	Voraussetzung
Betriebssystem	Windows 7, Windows Server 2003 oder Windows 10
.NET-Framework	Version 2.0 oder höher
CPU	750 Megahertz (MHz), empfohlen: 1 Gigahertz (GHz) oder schneller
RAM	1 GB, Empfohlen: 2 GB
Netzwerkschnittstellenkarte	100 Megabit pro Sekunde (Mbit/s) oder schnellere NIC

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Installieren Sie Citrix Application Delivery Management

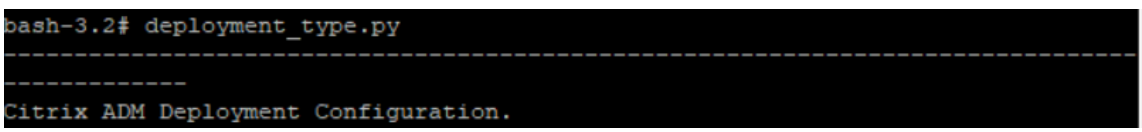
1. Importieren Sie die XVA-Image-Datei in Ihren Citrix Hypervisor und konfigurieren Sie auf der Registerkarte **Konsole** die anfänglichen Netzwerkkonfigurationsoptionen.

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.



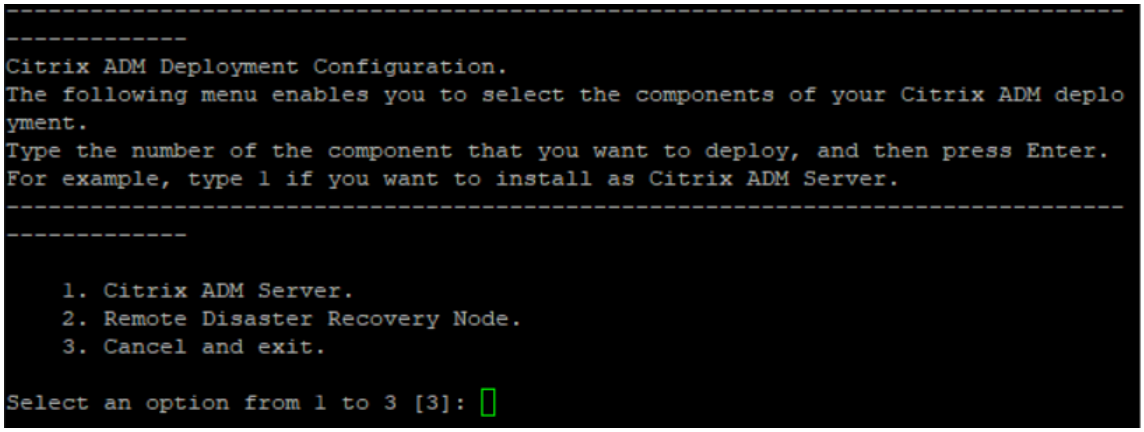
> **Hinweis**
>
> Wenn Sie nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie `networkconfig`ein, aktualisieren Sie die Konfiguration und speichern Sie sie.

4. Führen Sie das Deployment-Skript 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

Nachdem der Server installiert ist, können Sie auf die grafische Benutzeroberfläche (GUI) zugreifen, indem Sie die IP-Adresse des Citrix ADM Servers in den Webbrowser eingeben. Die standardmäßigen Administratoranmeldeinformationen für die Anmeldung am Server lauten nsroot/nsroot.

Der Browser zeigt das NetScaler ADM Konfigurationsprogramm an.

NetScaler ADM mit 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Megahertz (MHz), empfohlen: 1 Gigahertz (GHz) oder schneller
RAM	1 GB, Empfohlen: 2 GB
Netzwerkschnittstellenkarte	100 Megabit pro Sekunde (Mbit/s) oder schnellere NIC

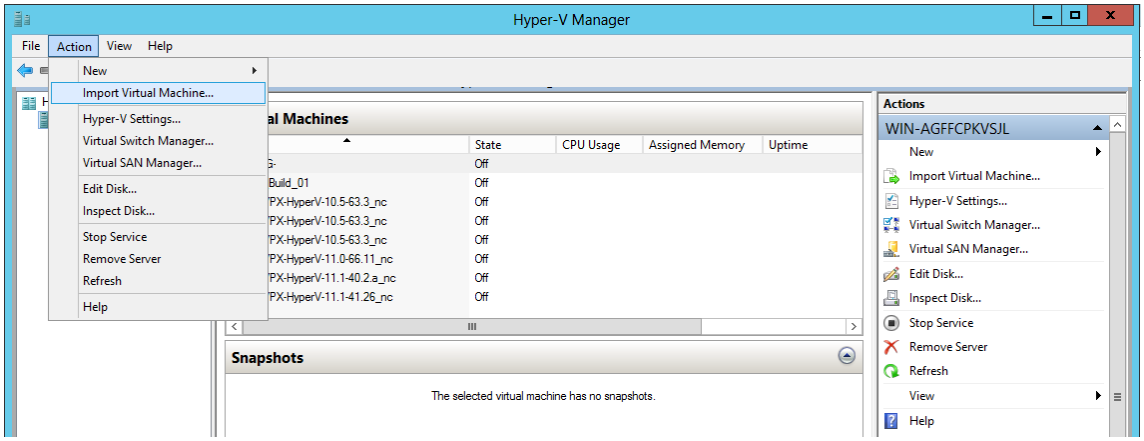
Installieren der NetScaler Application Delivery Management

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 Arbeitsstation.
2. Klicken Sie im Menü **Aktion** auf **Virtuelle Maschine importieren** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

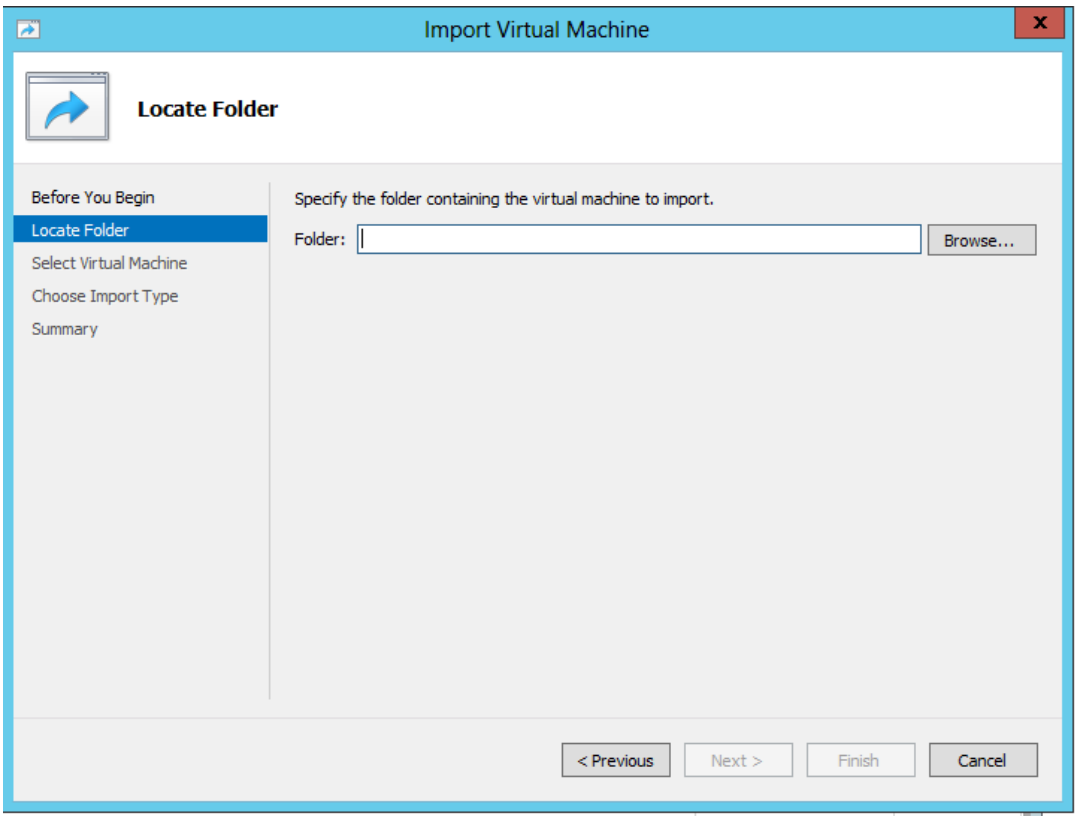
   b) Wählen Sie im Abschnitt Virtuelle Maschine auswählen den entsprechenden Namen der virtuellen Maschine aus.

   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.

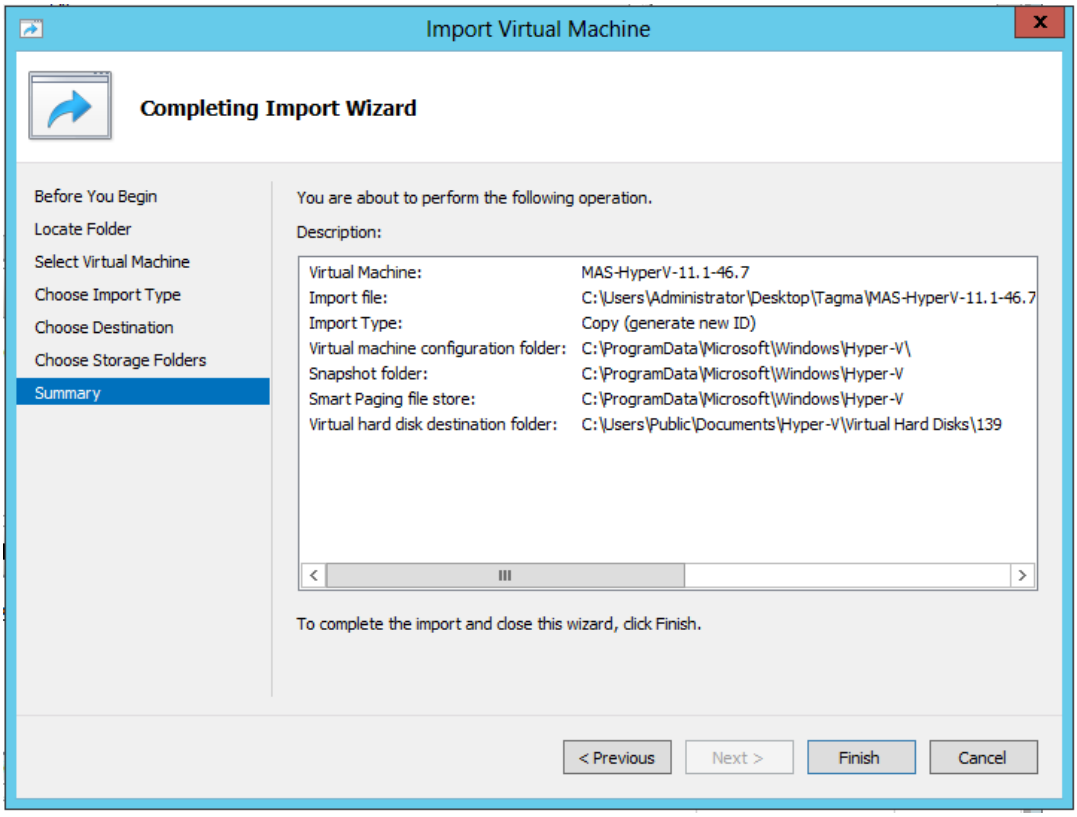
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

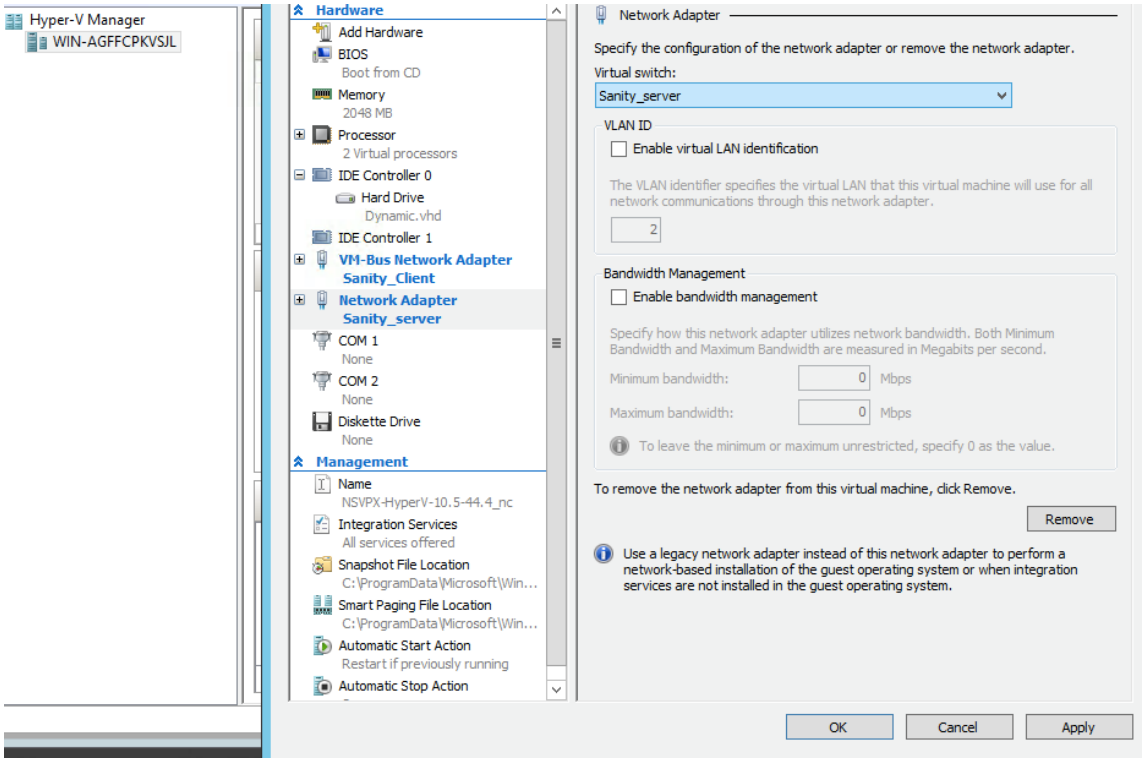
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



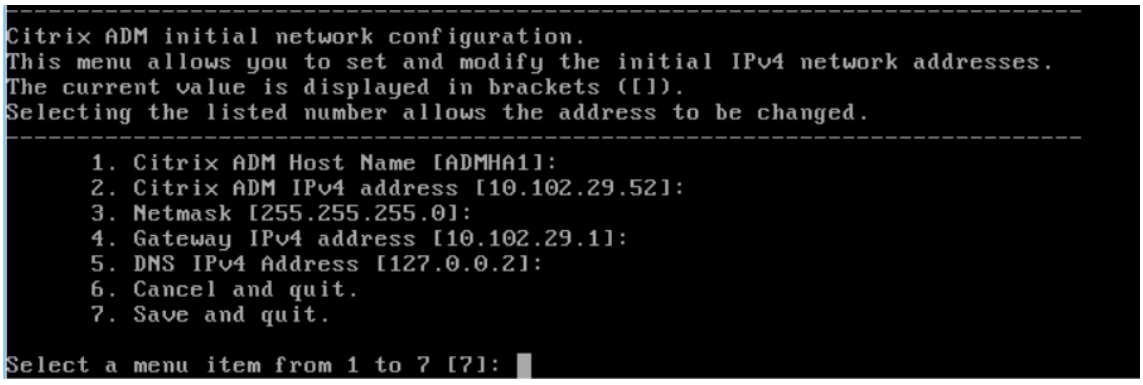
Das Citrix ADM Hyper-V-Image wird im rechten Fensterbereich angezeigt.

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 Dropdownliste Netzwerk das entsprechende Netzwerk aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

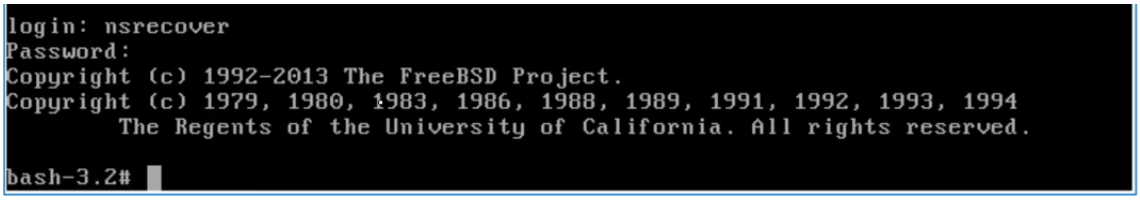


6. Klicken Sie auf **Übernehmen** und dann auf **OK**.
7. Klicken Sie mit der rechten Maustaste auf das Citrix ADM Hyper-V-Image, und klicken Sie auf **Verbinden**.
8. Klicken Sie im Konsolenfenster auf die Schaltfläche **Start** .
9. Konfigurieren Sie die anfänglichen Netzwerkkonfigurationsoptionen.



10. Speichern Sie die Konfigurationseinstellungen, nachdem Sie die erforderlichen IP-Adressen angegeben haben.
11. Wenn Sie dazu aufgefordert werden, melden Sie sich mit nsrecover/nsroot-Anmeldeinformationen an.

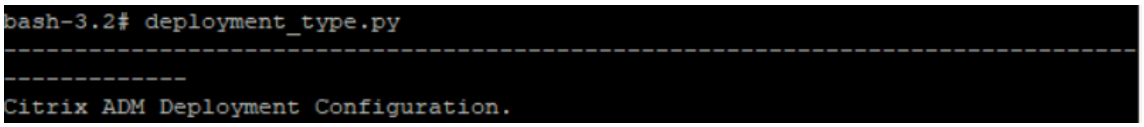
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

12. Führen Sie das Bereitstellungsskript 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**
>
> Nachdem Sie Citrix ADM installiert haben, können Sie die anfänglichen Konfigurationseinstellungen zu einem späteren Zeitpunkt aktualisieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verifizierung

Nach der Installation des Servers können Sie auf die grafische Benutzeroberfläche (GUI) zugreifen, indem Sie die IP-Adresse des Citrix 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 mit VMware ESXi

February 5, 2024

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

Voraussetzungen

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

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

> **Hinweis**
>
> vMotion wird auf Citrix ADM nicht unterstützt.

So installieren Sie NetScaler ADM

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Wählen **Sie im Dialogfeld OVF-Vorlagebereitstellen unter Aus einer Datei oder URL**bereitstellen die OVF-Datei aus, und klicken Sie auf**Weiter**.

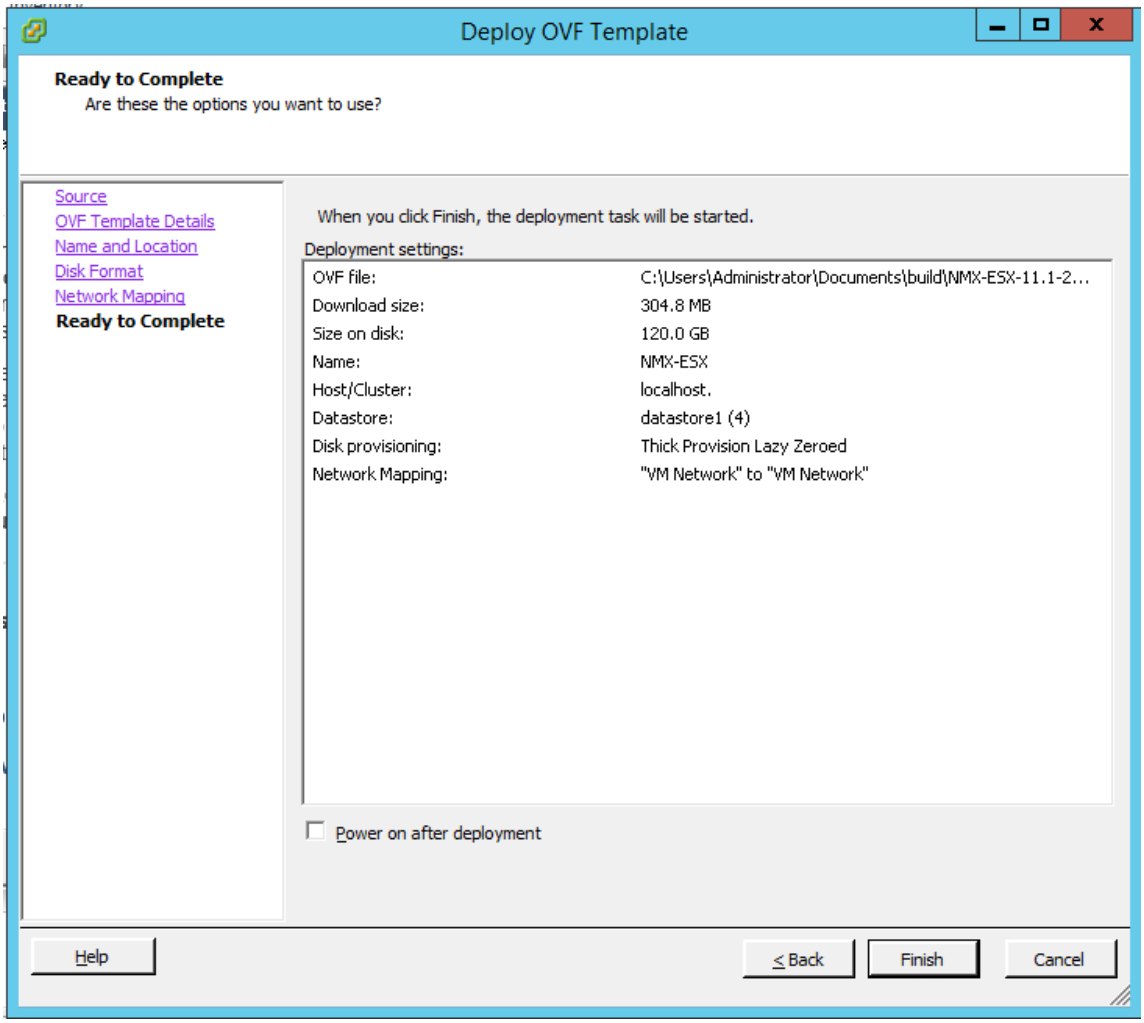
   > **Hinweis**
   >
   > Wenn eine Warnmeldung mit folgendem Text angezeigt wird: Die Betriebssystemkennung wird auf dem ausgewählten Host nicht unterstützt, prüfen Sie, ob der VMware Server das FreeBSD-Betriebssystem unterstützt. Klicken Sie auf **Ja**.

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.

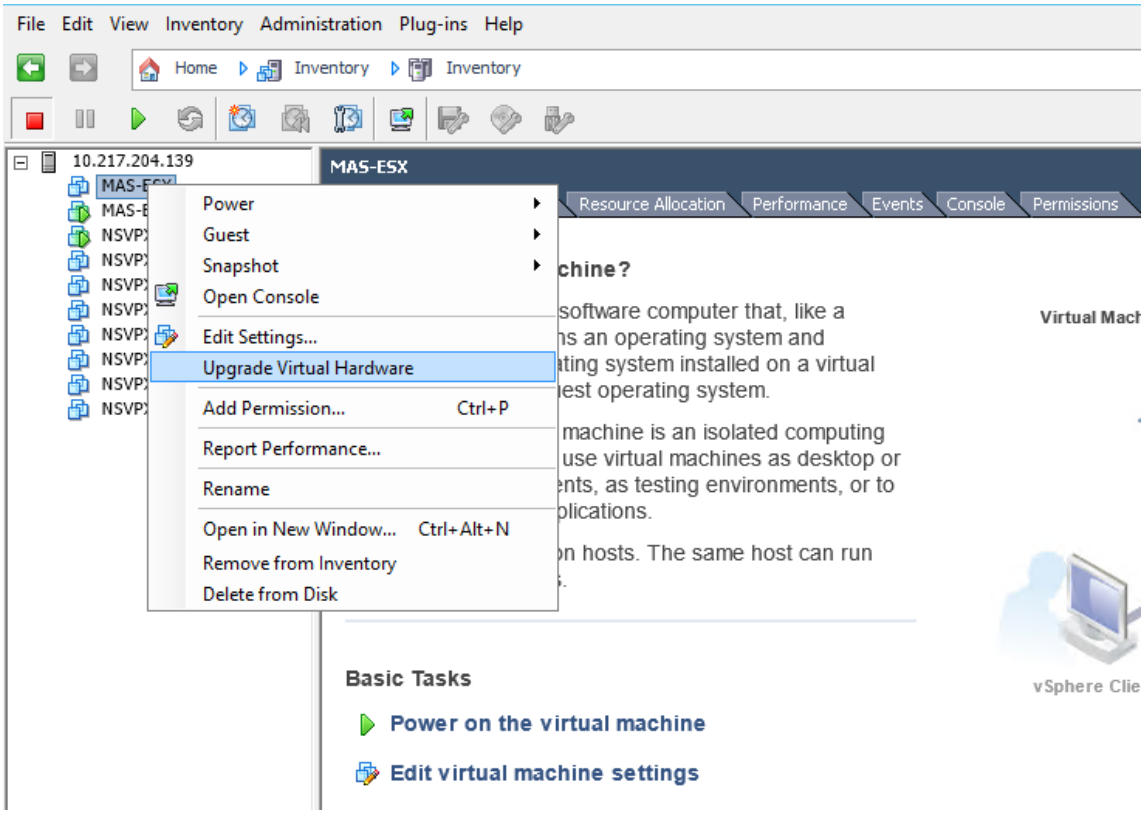
9. Klicken Sie auf **Fertig stellen**, um die Installation zu starten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



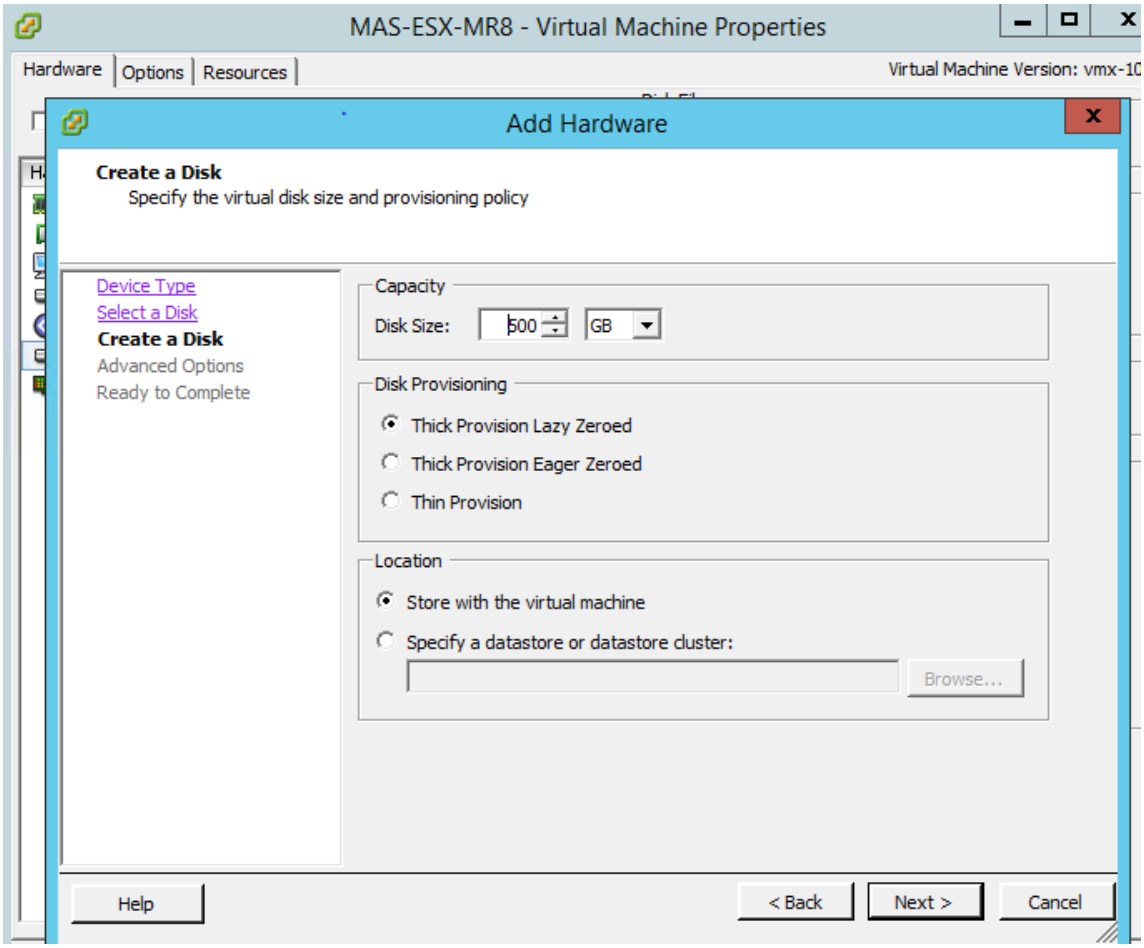
10. Sie können jetzt die virtuelle NetScaler ADM-Appliance starten.
11. Wählen Sie im Navigationsbereich die virtuelle Appliance aus, die Sie installiert haben. Klicken Sie im Menü **Inventar** mit der rechten Maustaste auf die **virtuelle Maschine**, und klicken Sie dann auf **Virtuelle Hardware aktualisieren**.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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



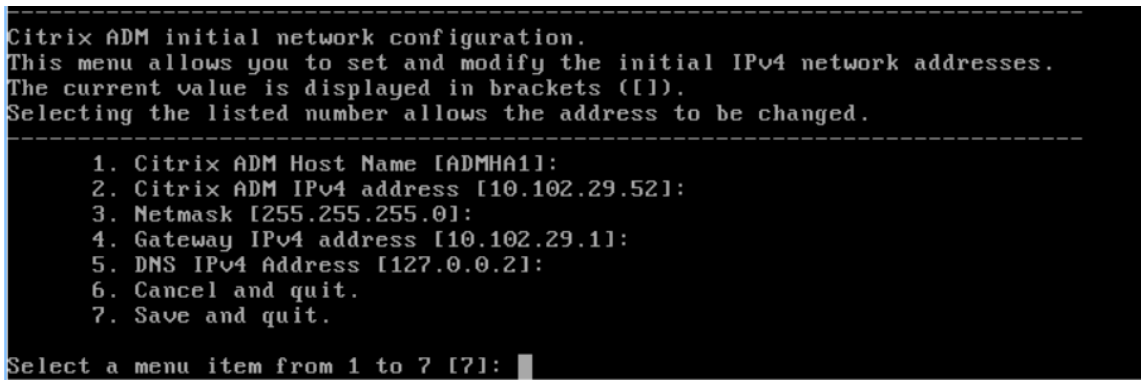
12. Klicken Sie im Menü **Inventar** auf **Virtuelle Maschine**und dann auf **Einstellungen bearbeiten**.
13. Klicken Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** auf der Registerkarte **Hardware** auf **Speicher**, und geben Sie dann im rechten Bereich als **Speichergröße** 32 GB an.
14. Klicken Sie auf **CPUs**, und geben Sie dann im rechten Bereich die CPUs als 8 an. Klicken Sie auf **OK**.
15. Fügen Sie eine zusätzliche Festplatte gemäß Ihren Anforderungen hinzu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

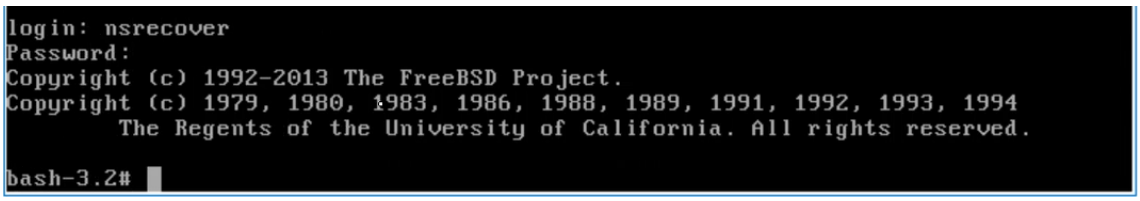
17. Klicken Sie auf die Registerkarte **Konsole**, um die Optionen für die anfängliche Netzwerkkonfiguration von NetScaler ADM anzuzeigen.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

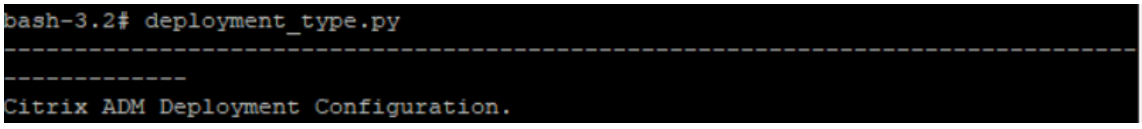
19. Melden Sie sich bei entsprechender Aufforderung mit den Anmeldeinformationen nsrecover/nsroot an.



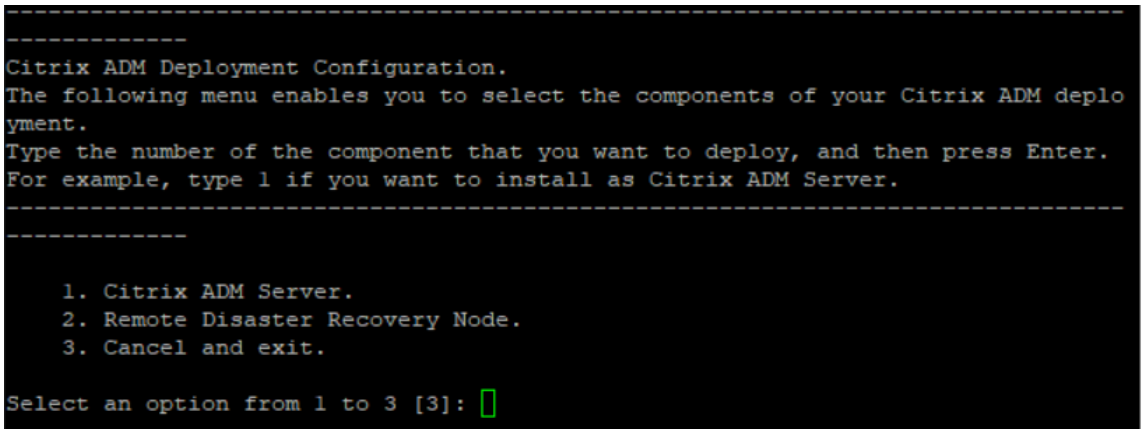
> **Hinweis**
>
> Wenn Sie nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie `networkconfig`ein, aktualisieren Sie die Konfiguration und speichern Sie sie.

20. Führen Sie das Bereitstellungsskript 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**
>
> Bei der Bereitstellung auf VMware ESXi kann es bis zu 30 Minuten oder länger dauern, bis Citrix ADM aktiviert wird.

NetScaler ADM mit 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 zum Verwalten 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, besser ist die Leistung von 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. Diese Schnittstelle sollte mit dem Verwaltungsnetzwerk des Linux-KVM-Hosts verbunden sein, damit Citrix ADM und Linux-KVM kommunizieren können.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Dropdownliste **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 12.1** aus.
6. Klicken Sie auf **Produktsoftware**, um sie zu erweitern, und klicken Sie auf den neuesten Build. Wählen Sie beispielsweise **Citrix ADM Release (Feature Phase) 12.1 Build 49.23/49.37** aus.

   Die ausgewählte Build-Seite wird angezeigt.
7. Wählen Sie in der Dropdownliste Zum **Download springen** das **Citrix ADM-Image für KVM, 12.1 Build xx.xx**
8. Klicken Sie auf **Datei herunterladen**, akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und laden Sie die komprimierte Imagedatei 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

```
root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build#
```

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. Quelldatei - Geben Sie den absoluten Quellpfad für das Datenträgerimage an. Der Dateipfad muss absolut sein.

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

   D. mode - Geben Sie den Modus an.

   E. modelltyp - Auf VirtIO setzen.

   F. source dev - Geben Sie die Schnittstelle 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. Define the VM attributes in the MAS1-KVM.xml file by using the following command: *virsh define <FileName>.xml*

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

Starten Sie das Citrix ADM, indem Sie den]*
folgenden Befehl eingeben: *virsh start [

vii.

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

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

root@ubuntu:/home/mas-build#
```

viii. Sie können mit dem folgenden Befehl eine Verbindung zur virtuellen Citrix ADM Maschine herstellen: *virsh console <DomainName>*

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

```
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]
```

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 Modul kvm_intel mit dem folgenden Befehl:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

rmmod kvm_intel

2. Deaktivieren Sie APICv und laden Sie das kvm_intel-Modul mit folgendem 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.

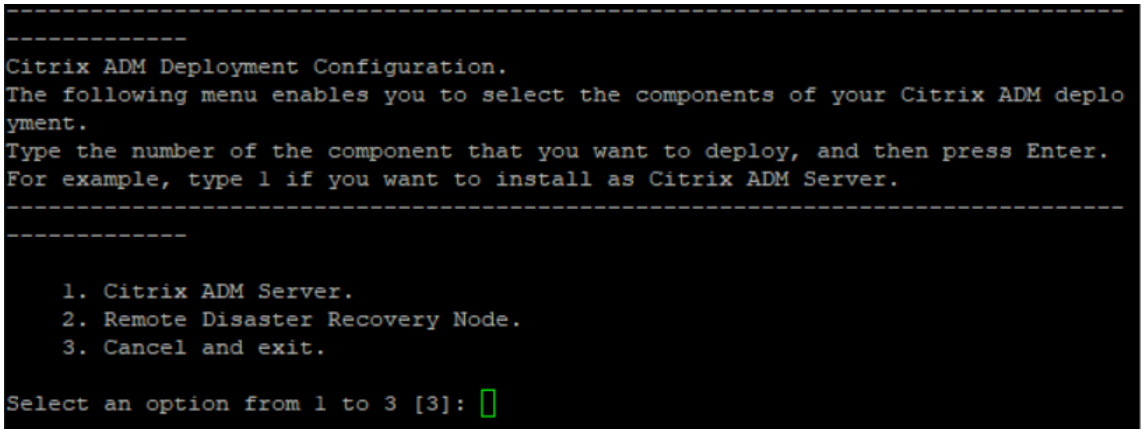
1. Verwenden Sie in der Befehlszeile die standardmäßigen Anmeldeinformationen des Systemadministrators, um sich am System anzumelden:
   - Benutzername: nsroot
   - Kennwort: nsroot

   Hinweis

   Nach der ersten Anmeldung müssen Sie das Administratorkennwort ändern. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Führen Sie das Bereitstellungsskript aus, indem Sie den folgenden 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*.

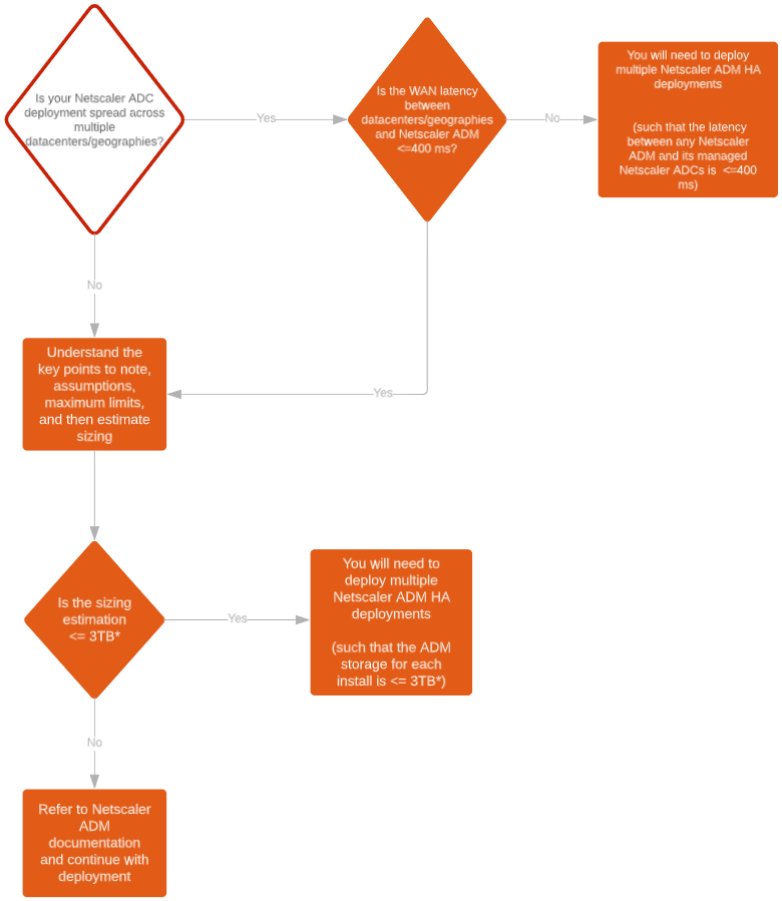
Bereitstellung mit hoher Verfügbarkeit konfigurieren

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

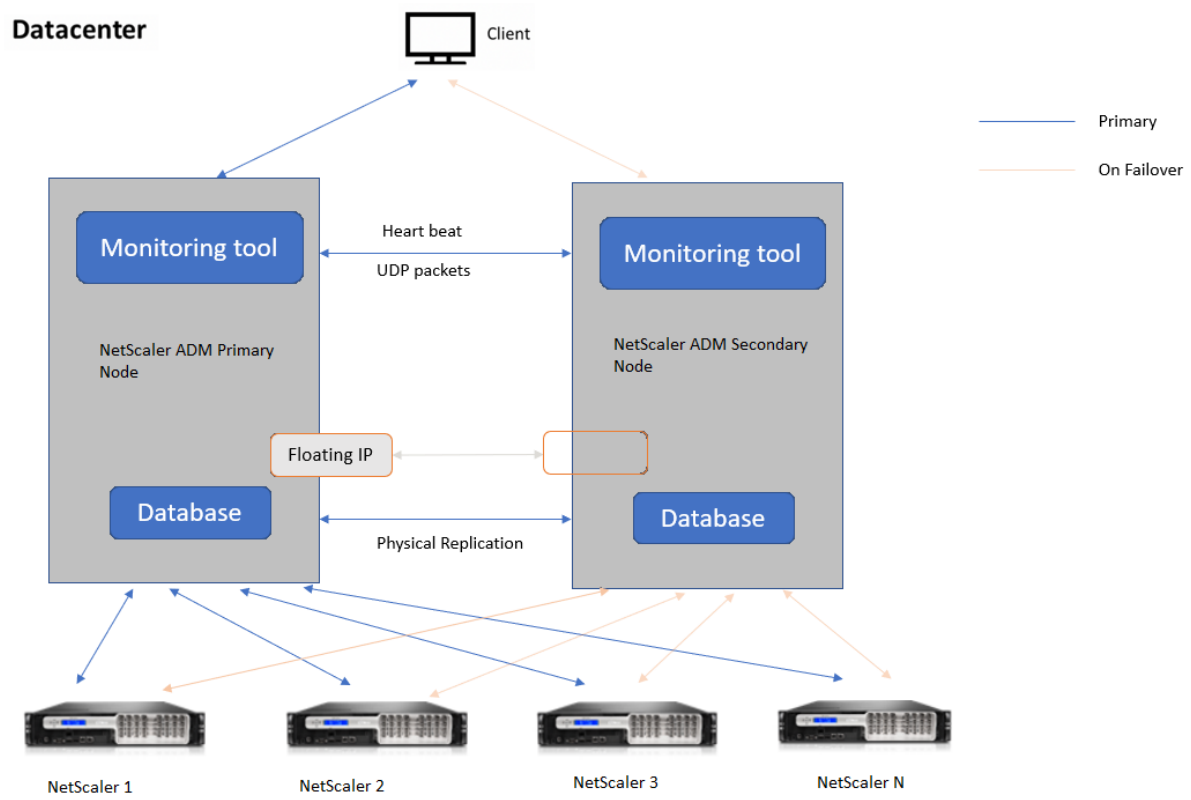
Begriff	Beschreibung
Floating-IP-Adresse	Eine Floating-IP ist eine IP-Adresse, die sofort von einem Knoten auf einen anderen im selben Subnetz verschoben werden kann. Intern ist es als Alias auf der Netzwerkschnittstelle des primären Knotens eingerichtet. Bei einem Failover wird die Floating-IP nahtlos 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

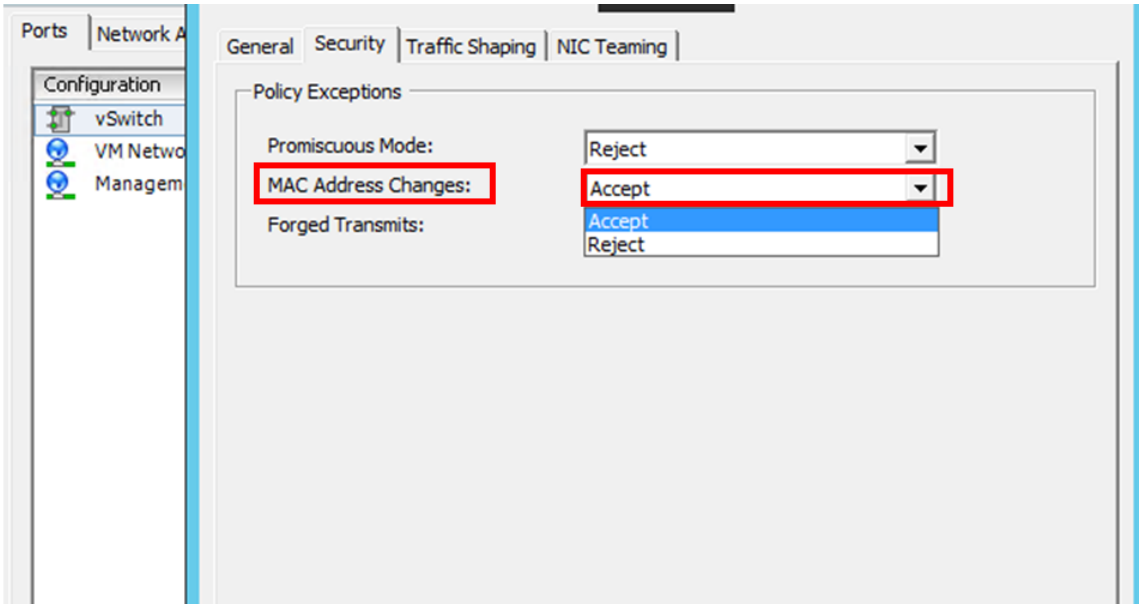
- Datenbank:
  - In einem Hochverfügbarkeits-Setup werden alle Konfigurationsdateien im Abstand von einer Minute automatisch vom primären Knoten zum sekundären Knoten synchronisiert.
  - Die Datenbanksynchronisierung erfolgt sofort durch physische Replikation der Datenbank.
  - Die Datenbank auf dem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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Komponente	Voraussetzung
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)

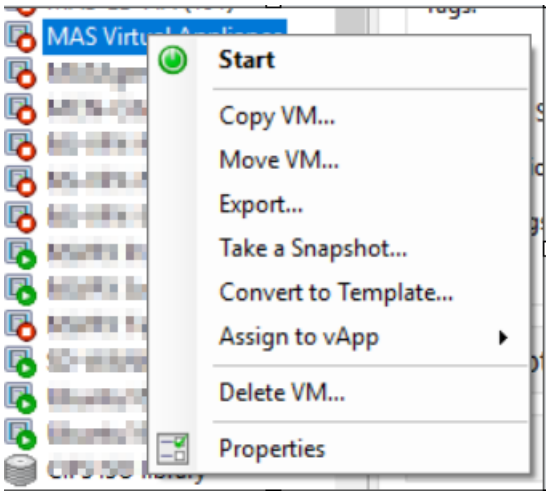
Um den ersten Knoten zu registrieren:

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

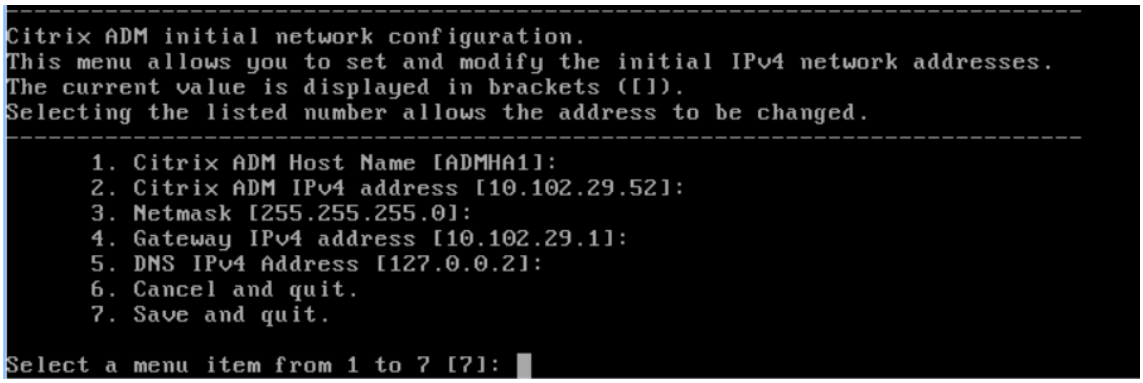
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.



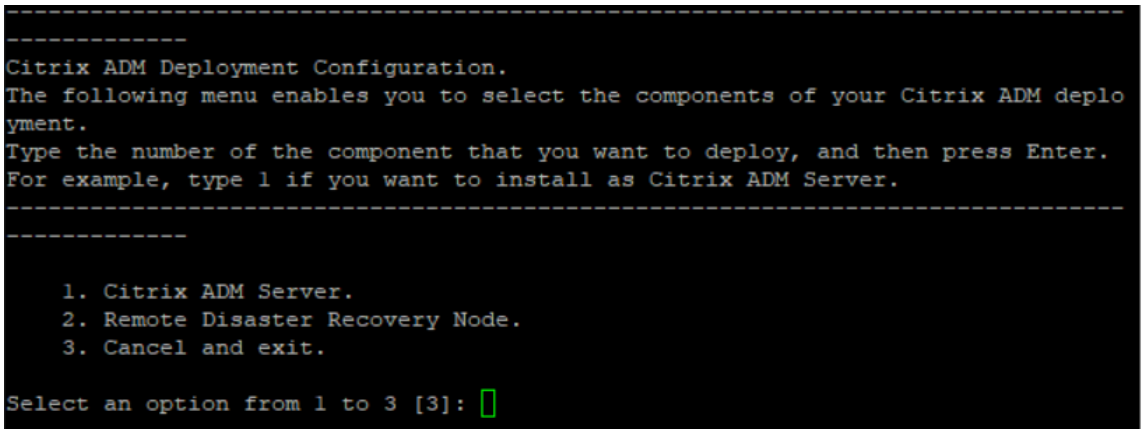
4. Nachdem die anfängliche Netzwerkkonfiguration abgeschlossen ist, fordert das System zur Anmeldung auf. Melden Sie sich mit den folgenden Anmeldeinformationen an: *nsrecover/nsroot*.

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

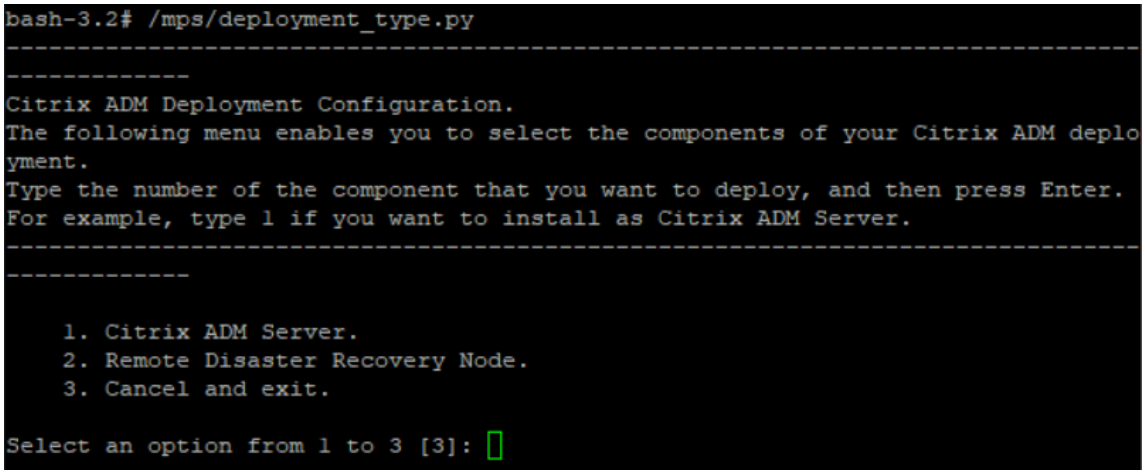
5. Geben Sie **/mps/deployment_type.py**ein, um den primären Knoten bereitzustellen. Das Kon-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

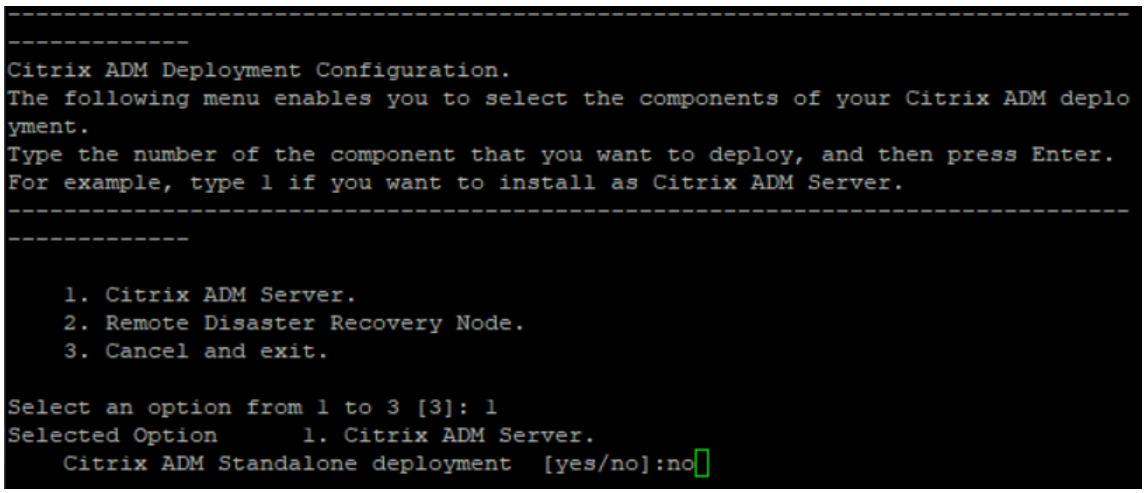
figurationsmenü für die Citrix ADM-Bereitstellung wird angezeigt.



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



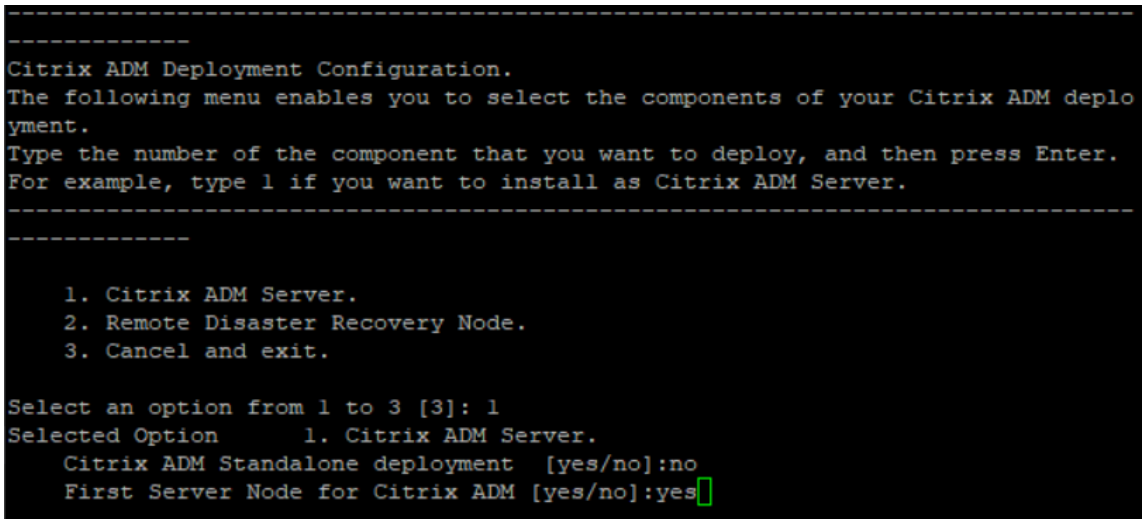
7. Die Konsole fordert Sie auf, die eigenständige NetScaler ADM Bereitstellung auszuwählen. Geben Sie**Nein** ein, um die Bereitstellung als Hochverfügbarkeit zu bestätigen.



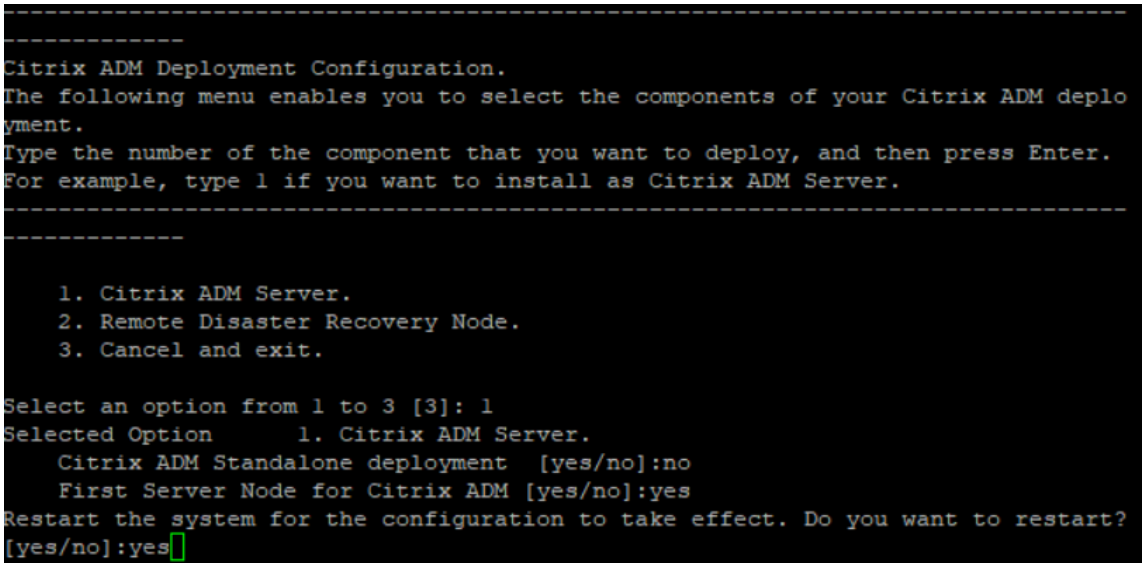
8. Die Konsole fordert Sie auf, den ersten Serverknoten auszuwählen. Geben Sie**Ja** ein, um den

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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)

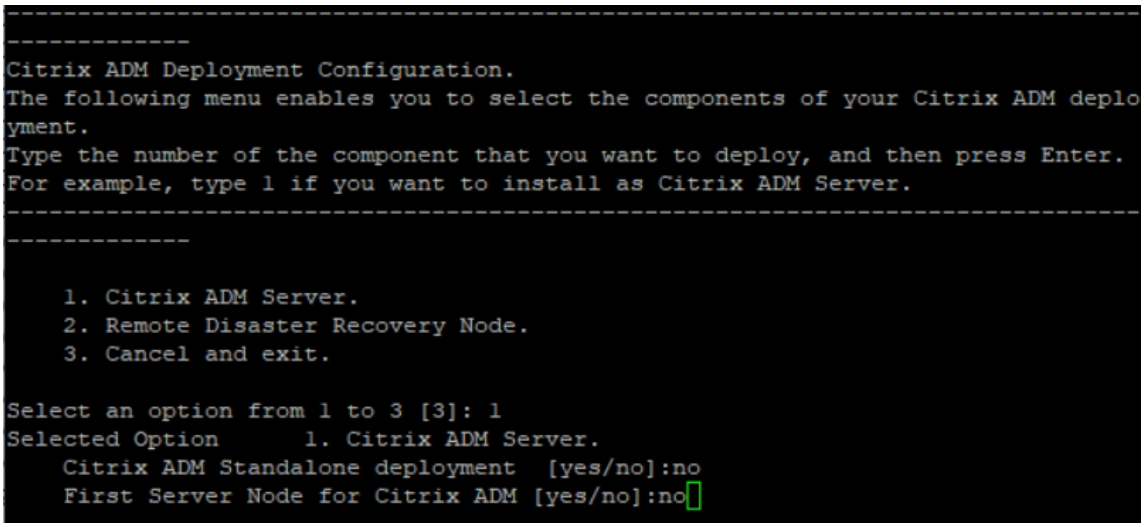
1. Verwenden Sie die **XVA-Imagedatei**, die von der Citrix Download-Site heruntergeladen wurde, und importieren Sie sie in Ihren Hypervisor.
2. Konfigurieren Sie Citrix ADM auf der Registerkarte **Konsole** mit den anfänglichen Netzwerkkonfigurationen, wie in der folgenden Abbildung dargestellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

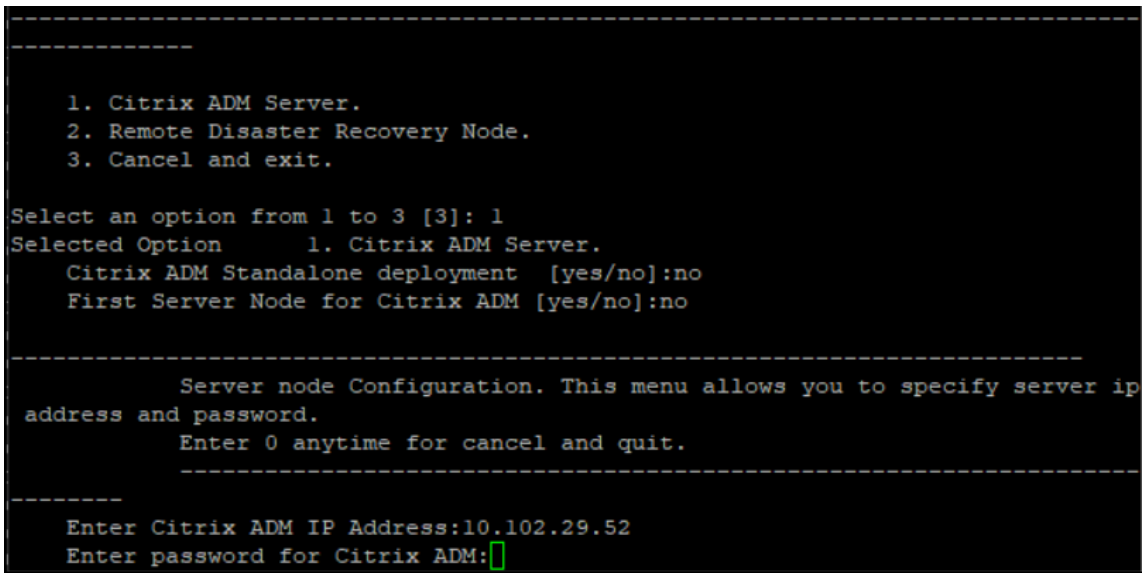
   > **Hinweis**
   >
   > Wenn Sie nach der Anmeldung die anfängliche Netzwerkkonfiguration aktualisieren möchten, geben Sie `networkconfig`ein, aktualisieren Sie die Konfiguration und speichern Sie sie.

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.

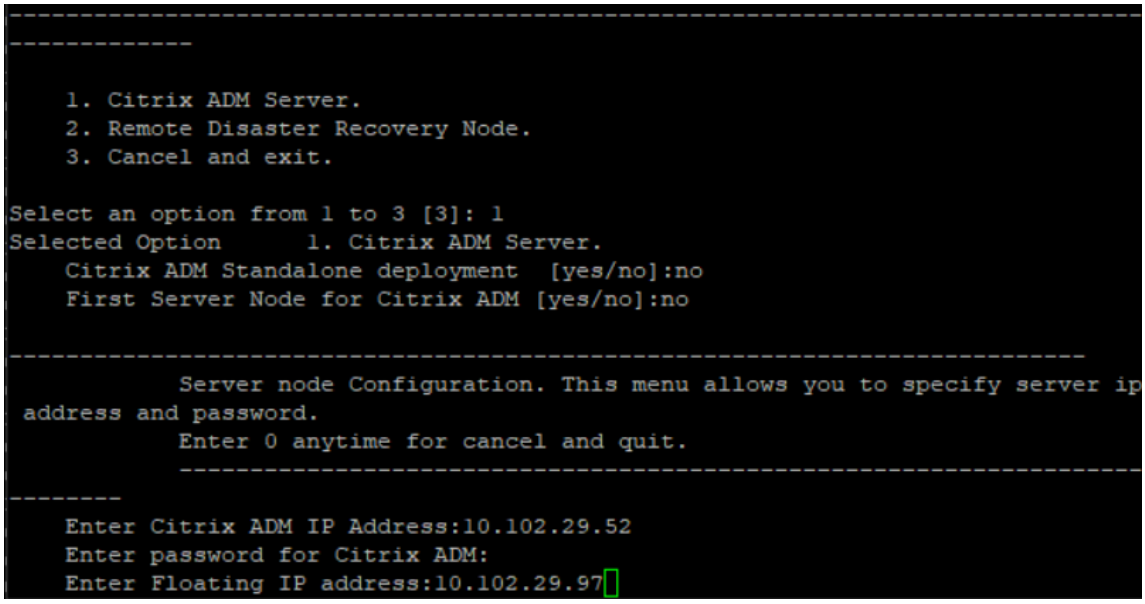


8. Die Konsole fordert Sie auf, die IP-Adresse und das Kennwort des primären Knotens einzugeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Mit Citrix ADM 12.1 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 12.1 Disaster Recovery (DR) -Funktion bietet vollständige Systemsicherungs- und Wiederherstellungsfunktionen für Citrix ADM, das im Hochverfügbarkeitsmodus bereitgestellt wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.
Knoten für die Notfallwiederherstellung	Der Wiederherstellungsknoten ist ein eigenständiger Knoten, der auf der Wiederherstellungs-Site bereitgestellt wird. Dieser Knoten wird betriebsbereit (für den neuen primären Knoten), falls ein Notfall den primären Standort trifft und nicht funktionsfähig ist.

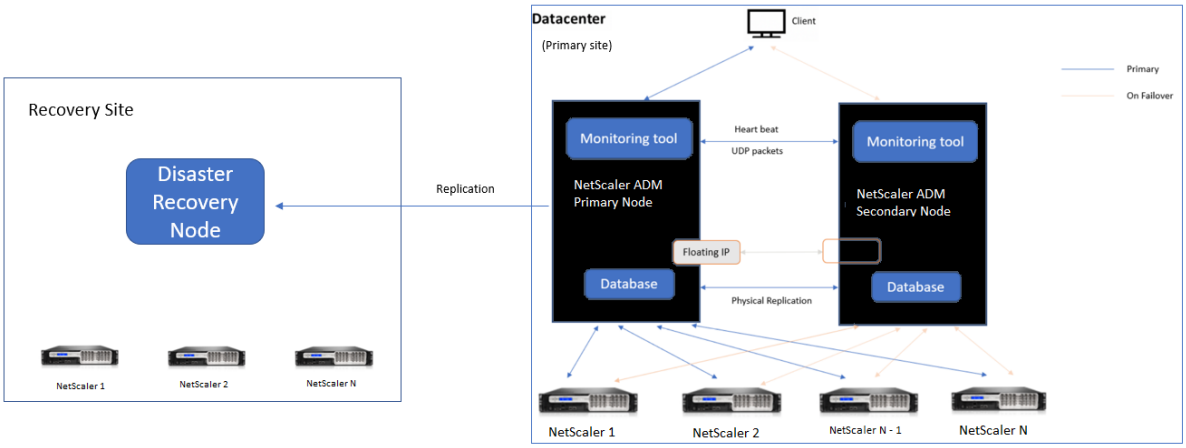
> Hinweis: Der primäre Standort und der DR-Standort kommunizieren über die Ports 5454 und 22 miteinander, und diese Ports sind standardmäßig aktiviert.
> Weitere Informationen zu Port- und Protokolldetails finden Sie unter Ports.

Disaster Recovery-Workflow

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 zusätzliche Festplatte 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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bereitstellen von NetScaler ADM im Hochverfügbarkeitsmodus

Stellen Sie sicher, dass Citrix ADM im Hochverfügbarkeitsmodus bereitgestellt wird, um Einstellungen für die Notfallwiederherstellung einzurichten. Informationen zur Bereitstellung von NetScaler ADM in Hochverfügbarkeit finden Sie unterHochverfügbarkeitsbereitstellung

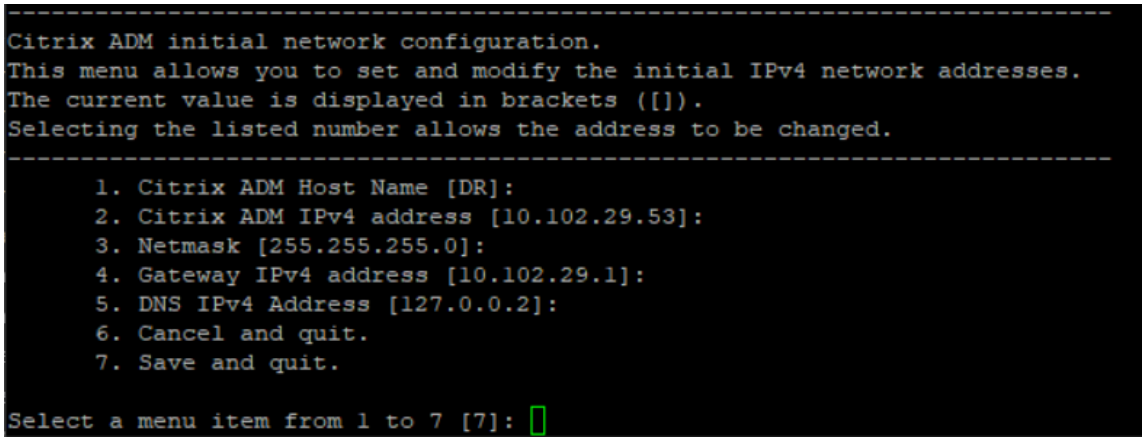
> **Hinweis**
>
> - Citrix ADM, das im Hochverfügbarkeitsmodus bereitgestellt wird, muss auf Citrix ADM Release Version 12.1 aktualisiert werden.
> - Eine**schwebende IP-Adresse ist obligatorisch**, um Disaster Recovery-Knoten beim primären Knoten zu registrieren.

Bereitstellen und Registrieren des NetScaler ADM Notfallwiederherstellungsknotens

So registrieren Sie den NetScaler ADM Notfallwiederherstellungsknoten:

1. Laden Sie die XVA-Imagedatei von der Citrix-Downloadsite 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*
   .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

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

Select an option from 1 to 3 [3]:
```

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

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

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

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. Die Konsole fordert zur Eingabe einer Floating-IP-Adresse des Hochverfügbarkeitsknotens und des Kennworts auf.
7. Geben Sie die schwebende IP-Adresse und das Kennwort ein, um den Disaster Recovery-Knoten beim primären Knoten zu registrieren.

```
------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    ------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

Der Notfallwiederherstellungsknoten ist jetzt erfolgreich registriert.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

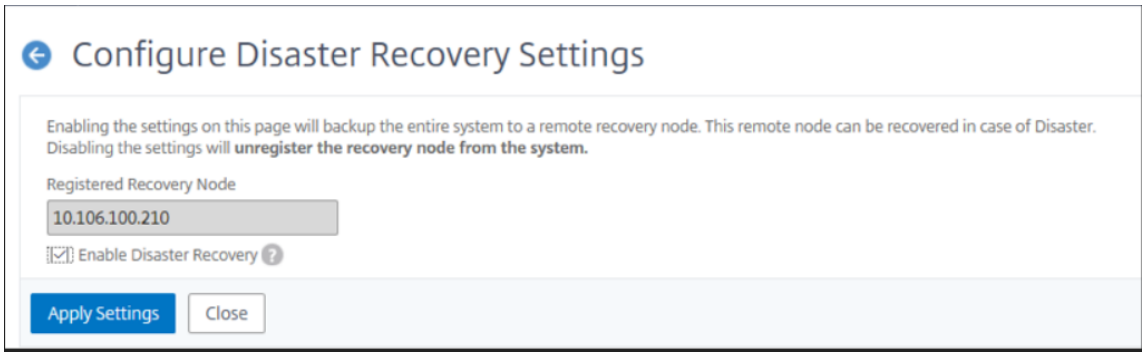
```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
    ------------------------------------------------------------------------
```

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

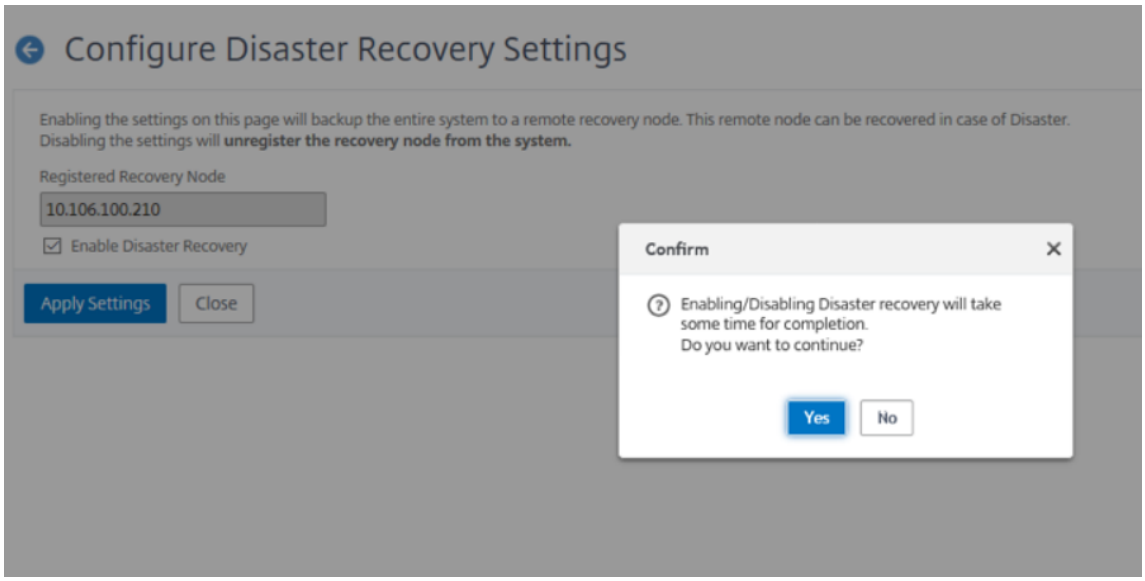
Aktivieren Sie die Disaster Recovery-Einstellungen über die Citrix ADM GUI

Nachdem der Disaster Recovery-Knoten erfolgreich registriert wurde, können Sie die Disaster Recovery-Einstellungen über die Citrix ADM primäre Site-Benutzeroberfläche aktivieren.

1. Navigieren Sie zu **System > Systemverwaltung > Notfallwiederherstellungseinstellungen.**
2. Aktivieren Sie auf der Seite **Disaster Recovery-Einstellungen** konfigurieren das Kontroll-kästchen Disaster Recovery aktivieren und klicken Sie auf **Einstellungen anwenden** .



3. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Ja**, um fortzufahren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Die Zeit, die für die Systemsicherung benötigt wird, hängt von der Datengröße und der WAN-Verbindungsgeschwindigkeit (Wide Area Network) ab.

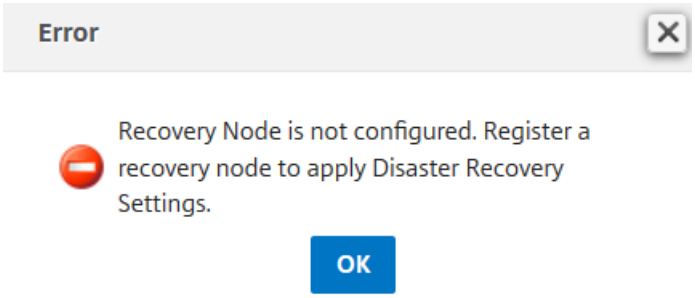
Um die Disaster Recovery-Einstellungen zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Disaster Recovery aktivieren** und klicken Sie auf **Einstellungen anwenden.**

Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf**Ja**, um fortzufahren.

> **Wichtig!**
>
> - Es liegt in der Verantwortung des Administrators, festzustellen, dass eine Katastrophe am primären Standort aufgetreten ist.
> - Der Disaster Recovery-Workflow ist nicht automatisiert und der Administrator muss ihn manuell initiieren, nachdem der primäre Standort ausgefallen ist.
> - Ein Administrator muss den Prozess manuell initiieren, indem er ein Wiederherstellungsskript auf dem Notfallwiederherstellungsknoten am Wiederherstellungs-Site ausführt.
> - Wenn Sie das HA-Paar am primären Standort aktualisieren, müssen Sie den eigenständigen Knoten am DR-Standort manuell aktualisieren.

Wenn Sie die Option **Disaster Recovery aktivieren** deaktivieren und auf **Einstellungen anwenden** klicken, erlaubt Ihnen Citrix ADM nicht, die Option **Disaster Recovery aktivieren** erneut auszuwählen.

Die folgende Fehlermeldung wird angezeigt, wenn Sie auf **Disaster Recovery-Einstellungen** klicken:



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

a) Melden Sie sich mit einem Hypervisor oder einer SSH-Konsole am DR-Knoten an.

b) Konfigurieren Sie den DR-Knoten, indem Sie das hier verfügbare Verfahren befolgen: Bereitstellen und Registrieren des NetScaler ADM Notfallwiederherstellungsknotens.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

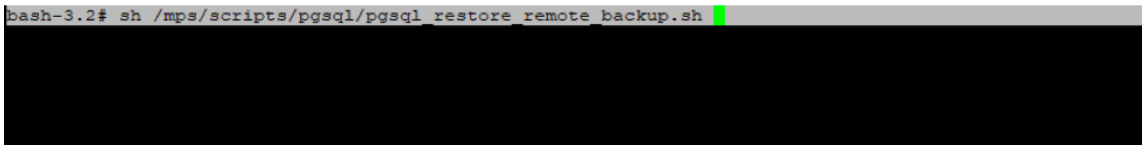
c) Aktivieren Sie die Disaster Recovery-Option.

Weitere Informationen finden Sie in den Häufig gestellten Fragen.

Workflow nach der Katastrophe

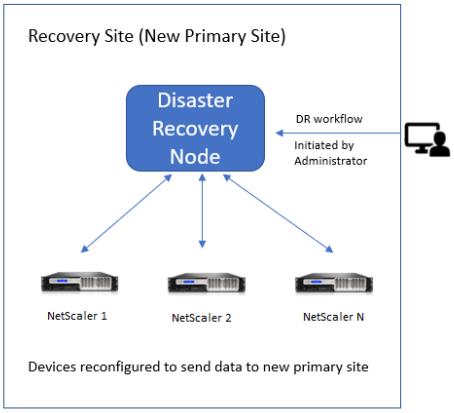
Wenn der primäre Standort nach einem Notfall ausfällt, muss der Disaster Recovery-Workflow wie folgt initiiert werden:

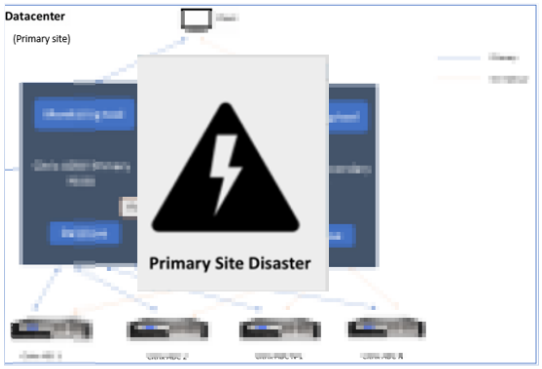
1. Der Administrator stellt fest, dass der primäre Standort von einer Katastrophe heimgesucht wurde und dieser nicht betriebsbereit ist.
2. Der Administrator leitet den Wiederherstellungsprozess ein.
3. Der Administrator muss das folgende Wiederherstellungsskript auf dem Notfallwiederherstellungsknoten (am Wiederherstellungsstandort) manuell ausführen: **/mps/scripts/pgsql/pgsql_restore_remote_backup.sh**



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nachträgliche Notfallwiederherstellung

Nachdem der Notfall eingetreten ist und der Administrator das Wiederherstellungsskript initiiert hat, wird der DR-Site nun zum neuen 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.

On-Prem-Agents für die Bereitstellung mehrerer Standorte konfigurieren

February 5, 2024

In früheren Versionen von Citrix ADM konnten Citrix ADC-Instanzen, die in Remote-Rechenzentren bereitgestellt wurden, von Citrix ADM aus verwaltet und überwacht werden, das in einem primären Rechenzentrum ausgeführt wird. NetScaler ADC Instanzen sendeten Daten direkt an das primäre NetScaler ADM, was zur Nutzung der WAN-Bandbreite (Wide Area Network) führte. Darüber hinaus nutzt die Verarbeitung von Analysedaten CPU- und Speicherressourcen des primären Citrix ADM.

Kunden haben ihre Rechenzentren auf der ganzen Welt. Agenten spielen eine wichtige Rolle in folgenden Szenarien, in denen die Kunden wählen können:

- um Agenten in entfernten Rechenzentren zu installieren, sodass der WAN-Bandbreitenverbrauch reduziert wird.
- um die Anzahl der Instanzen zu begrenzen, die Datenverkehr zur Datenverarbeitung direkt an das primäre Citrix ADM senden.

> **Hinweis**
>
> - Die Installation von Agenten für Instanzen im Remote-Rechenzentrum wird empfohlen, aber nicht zwingend erforderlich. Bei Bedarf können Benutzer Citrix ADC-Instanzen direkt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

zum primären Citrix ADM hinzufügen.

- Wenn Sie Agenten für die Remote-Rechenzentren installiert haben, erfolgt die Kommunikation zwischen den Agents und dem primären Standort über eine Floating-IP. Weitere Informationen finden Sie unter Port.
- Sie können Agenten installieren und gepoolte Lizenzen auf die Instanzen in dem/den Remote-Rechenzentrum (en) anwenden. In diesem Szenario erfolgt die Kommunikation zwischen dem primären Standort und dem/den Remote-Rechenzentrum (en) über die Floating-IP.

In Citrix ADM 12.1 können Instanzen mit Agenten konfiguriert werden, um mit dem primären Citrix ADM in einem anderen Rechenzentrum zu kommunizieren.

Hinweis

Lokale Agenten für die Bereitstellung an mehreren Standorten werden nur bei der Bereitstellung mit hoher Verfügbarkeit von Citrix ADM unterstützt.

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.

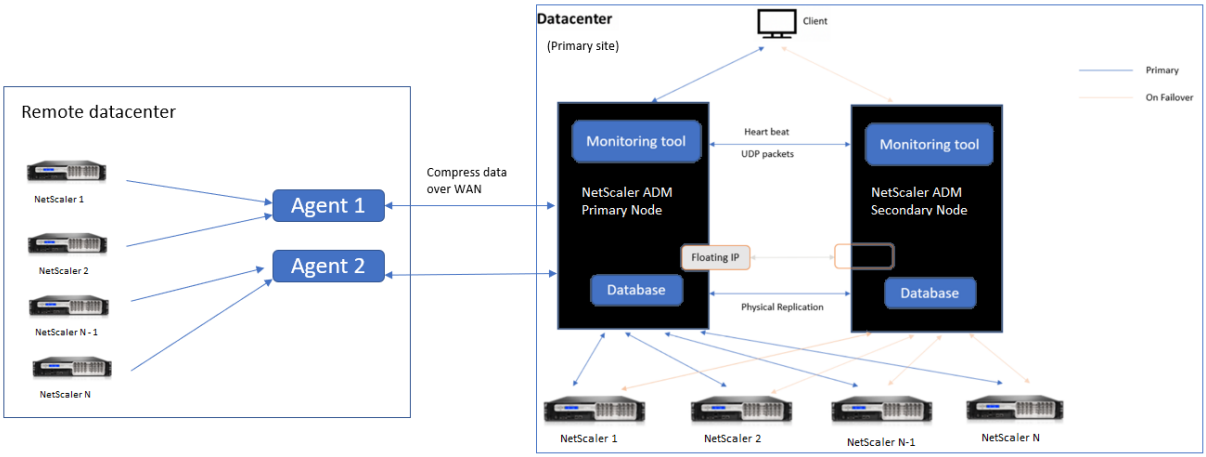
  Hinweis

  Die Anzahl der Agenten, die pro Standort installiert werden sollen, hängt vom verarbeiteten Datenverkehr ab. Derzeit hat Citrix zwei Agents pro Standort für das Agent-Failover-Szenario validiert. Citrix empfiehlt, mindestens zwei Agents pro Site zu installieren, damit der Datenverkehr im Falle eines Agent-Failovers an einen anderen Agenten fließt.

Architektur

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 hinzufügen
- 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 Rechen-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

zentrum 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**
>
> Lokale Agenten für die Bereitstellung an mehreren Standorten werden nur bei der Bereitstellung mit hoher Verfügbarkeit von Citrix ADM 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	8 GB **Hinweis**: Citrix empfiehlt , den Standardwert für eine bessere Leistung auf 32 GB zu erhöhen.
Virtuelle CPU	2 CPUs **Hinweis**: Citrix empfiehlt , den Standardwert für eine bessere Leistung auf 8 CPUs zu erhöhen.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

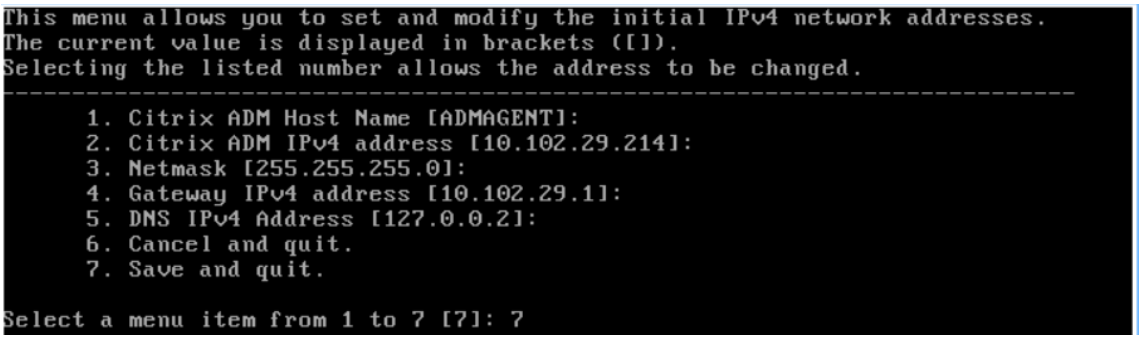
Typ	Port	Details
TCP	80	Für die NITRO -Kommunikation zwischen Agent und NetScaler ADC - oder Citrix SD-WAN Instanz.
TCP	22	Für die SSH-Kommunikation zwischen Agent und NetScaler ADC oder Citrix SD-WAN-Instanz. Für die Synchronisierung zwischen NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus bereitgestellt werden.
UDP	4739	Für die AppFlow Kommunikation zwischen Agent und NetScaler ADC - oder Citrix SD-WAN Instanz.
ICMP	Kein reservierter Port	Erkennen der Netzwerkerreichbarkeit zwischen NetScaler ADM- und NetScaler ADC-Instanzen, SD-WAN-Instanzen oder dem sekundären NetScaler ADM-Server, der im Hochverfügbarkeitsmodus bereitgestellt wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Typ	Port	Details
SNMP	161, 162	Zum Empfangen von SNMP-Ereignissen von der NetScaler ADC-Instanz an den Agenten.
Syslog	514	Zum Empfangen von Syslog-Nachrichten von der NetScaler ADC- oder Citrix SD-WAN-Instanz an den Agenten.
TCP	5557	Für die Logstream-Kommunikation zwischen Agent und Citrix ADC-Instanzen.

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-12.1-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.

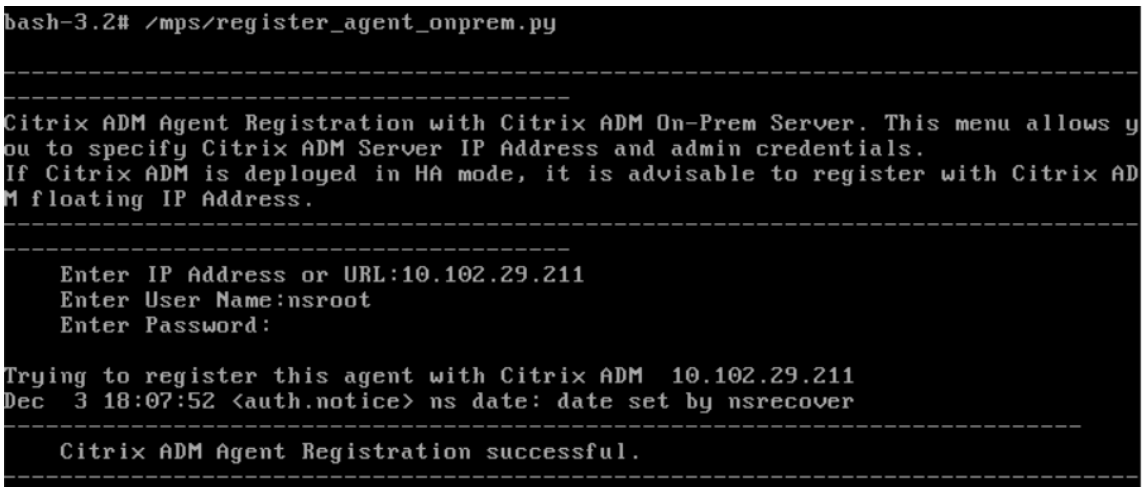


4. Nach erfolgreicher Registrierung wird die Konsole aufgefordert, sich anzumelden. Verwenden Sie *nsrecover/nsroot* als Anmeldeinformationen.
5. Um den Agenten zu registrieren, geben Sie**/mps/register_agent_onprem.py** ein. Die Anmelde-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

informationen 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 Agents auf die Citrix ADM GUI zu. Gehen Sie im Hauptmenü zur Seite **Netzwerke > Agents**, um den Status des Agents 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 zur Site hinzufügen

1. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen.**
2. Wählen Sie auf der Seite **Site anhängen** eine Site aus der Liste aus, oder erstellen Sie mithilfe der Schaltfläche mit dem Pluszeichen (+) eine neue Site.
3. Klicken Sie auf **Speichern**.

> **Hinweis**
>
> - Standardmäßig werden alle neu registrierten Agents zum Standard-Rechenzentrum hinzugefügt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - 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.

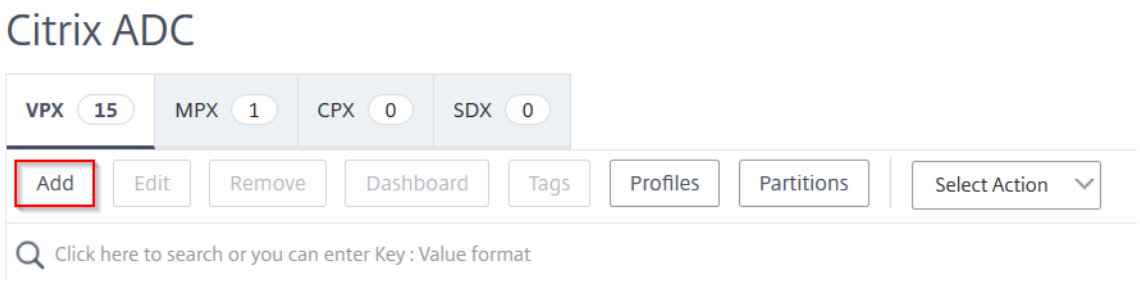
Hinzufügen NetScaler ADC-Instanzen

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 Secure Web Gateway
- Citrix SD-WAN WO

Neue Instanz hinzufügen

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



3. Markieren Sie die Option **Geräte-IP-Adresse eingeben** und geben Sie die IP-Adresse ein.
4. Wählen Sie unter **Profilname**das entsprechende Instanzprofil aus, oder erstellen Sie ein neues Profil, indem Sie auf das **Pluszeichen** klicken.

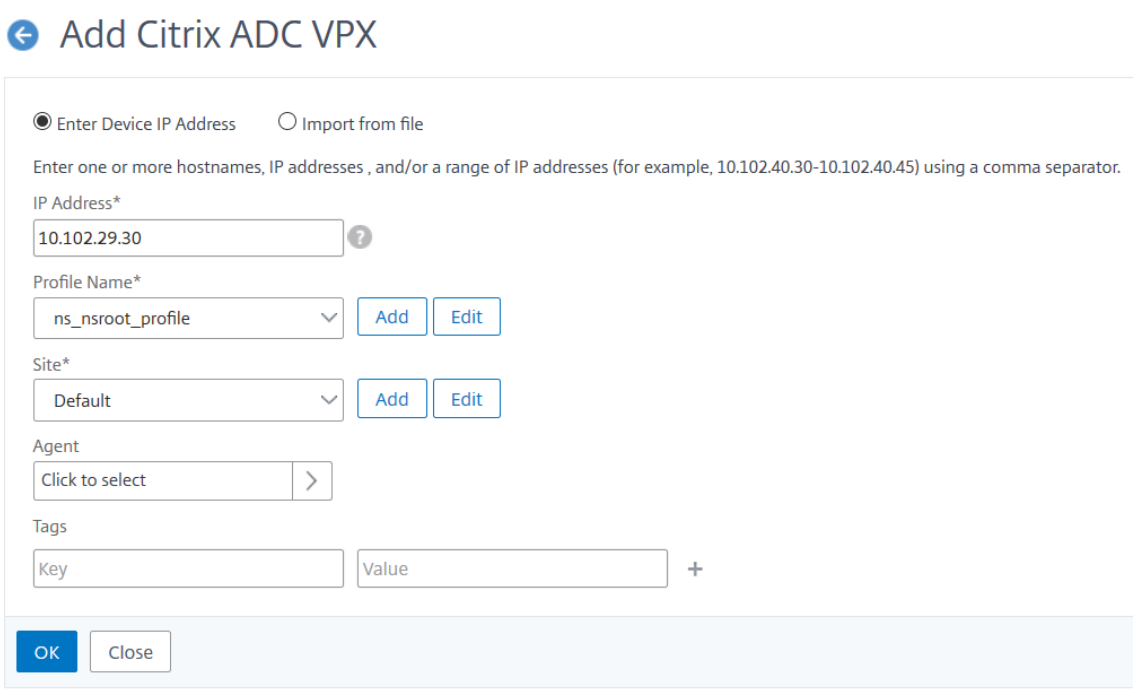
> **Hinweis**
>
> Für jeden Instanztyp ist ein Standardprofil verfügbar. Beispielsweise ist das ns-root-Profil

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

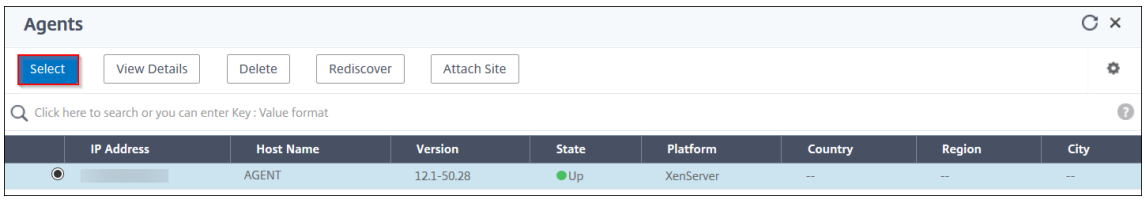
> das Standardprofil für NetScaler ADC-Instanzen.

5. Wählen Sie die **Site** aus, der Sie die Instanz zuordnen möchten.

> **Hinweis**
>
> Basierend auf der ausgewählten Site wird die Liste der Agents angezeigt, die dieser Site zugeordnet sind. Stellen Sie sicher, dass Sie die **Site** auswählen, mit der Sie die Instanz verknüpfen möchten.

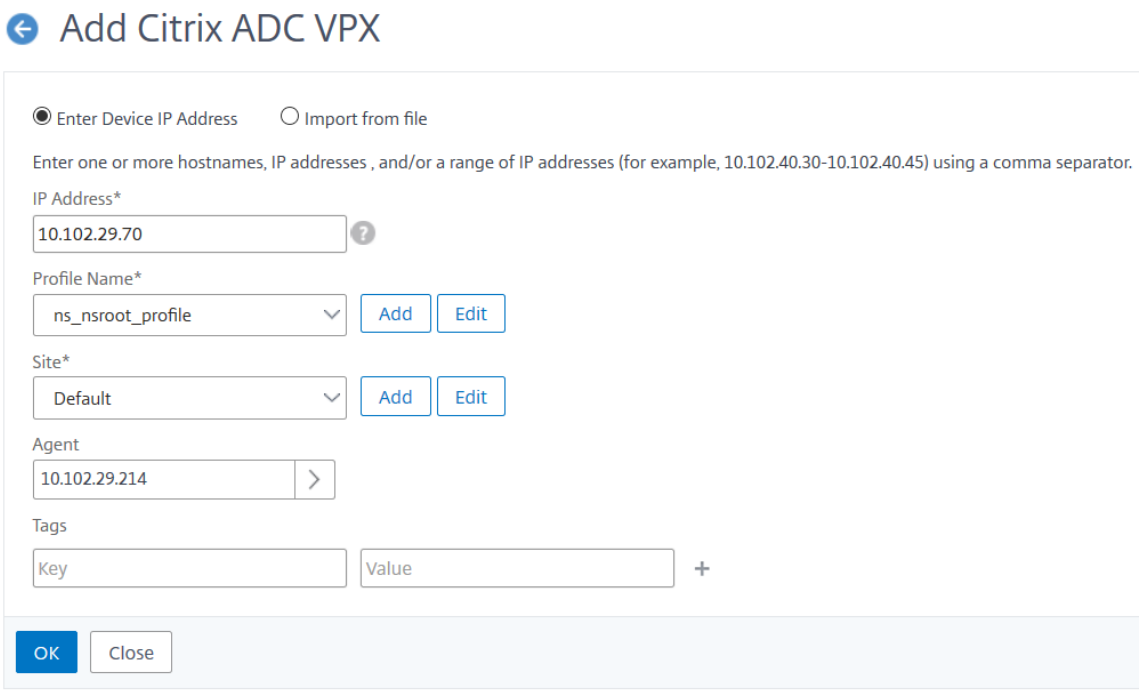


6. Klicken Sie, um den Agent auszuwählen. Wählen Sie auf der Seite **Agent** den Agent aus, dem Sie die Instanz zuordnen möchten, und klicken Sie dann auf **Auswählen**.



7. Klicken Sie auf der Seite Citrix VPX hinzufügen auf **OK.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vorhandene Instanz aktualisieren, um sie an einen Agent anzufügen

Wenn eine Instanz bereits zum primären Citrix ADM hinzugefügt wurde, können Sie sie an einen Agent anfügen, indem Sie den Workflow zum Hinzufügen von Instanzen bearbeiten und einen Agent auswählen.

1. Navigieren Sie zu **Netzwerke > Instanzen**, und wählen Sie den Instanztyp aus. Beispiel: NetScaler ADC.
2. Klicken Sie auf die Schaltfläche **Bearbeiten**, um eine vorhandene Instanz zu bearbeiten.
3. Klicken Sie, um den Agent auszuwählen.
4. Wählen Sie auf der Seite **Agent** den Agent 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 Trap-Ziel konfiguriert ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Agents für Citrix ADC-Instanzen in Remote-Rechenzentren wird empfohlen, ist aber nicht zwingend erforderlich.
>
> Wenn Sie die Instanz direkt zum primären MAS hinzufügen möchten, wählen Sie beim Hinzufügen von Instanzen keinen **Agent** aus.

Agent clustern

Der Begriff **Agentcluster** bezieht sich auf einen Mechanismus, bei dem Agents, die an eine Site angefügt sind, logisch gruppiert werden, sodass, wenn einer der Agents ausfällt, die Citrix ADC-Instanzen, die Datenverkehr an ihn senden, automatisch neu konfiguriert werden, um mit dem Senden von Datenverkehr an die anderen fehlerfreien Agents in dieser Gruppe oder Site zu beginnen.

Der Vorteil der Clusterung von Agents an einem Remote-Standort besteht darin, dass, wenn ein Agent ausfällt, dieser von Citrix ADM erkannt wird und implizit alle Instanzen an andere verfügbare Agents in diesem Cluster verteilt werden.

Zum Beispiel haben wir zwei Agents 10.106.1xx.2x und 10.106.1xx.7x, die am Standort Bangalore angeschlossen und einsatzbereit sind, wie unten gezeigt.

Wenn ein Agent ausfällt, erkennt Citrix ADM ihn und zeigt den Status als **down** an.

Die mit diesem Agent verbundenen Instanzen werden automatisch so konfiguriert, dass der andere Agent aus demselben Cluster für Trap-Ziel, Syslog-Server usw. verwendet wird.

> **Hinweis:**
>
> Bei der Neukonfiguration der Instanzen wird es zu einer gewissen Verzögerung kommen.

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

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

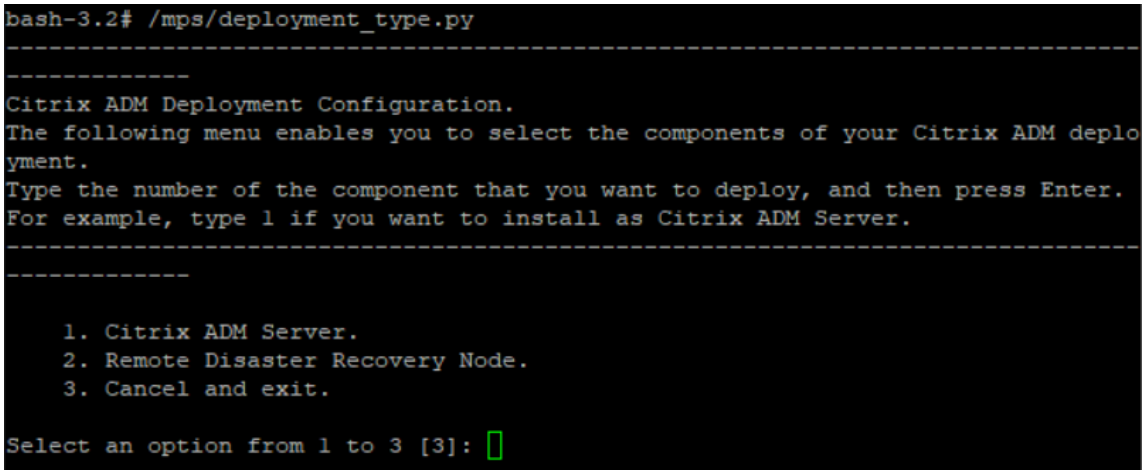
1. Änderung des vorhandenen Serverknotens
2. Provisioning des zweiten Serverknotens
3. Bereitstellung der beiden Knoten im HA-Modus
4. Konfiguration des Hochverfügbarkeitspaars

Ändern Sie den vorhandenen Citrix ADM Serverknoten

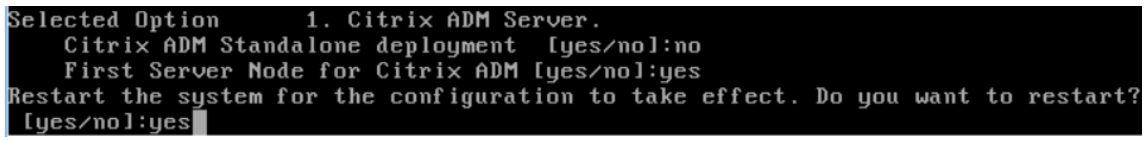
Um das Citrix ADM vom Einzelserver in den Hochverfügbarkeitsmodus zu migrieren, müssen Sie den anfänglichen Bereitstellungstyp des Serverknotens in den Hochverfügbarkeitsmodus ändern.

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 **/mps/deployment_type.py**ein, und drücken **Sie die EINGABETASTE**.
4. Wählen Sie den Bereitstellungstyp als Citrix ADM Serveraus. Wenn Sie keine Option auswählen, wird diese standardmäßig als Server bereitgestellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

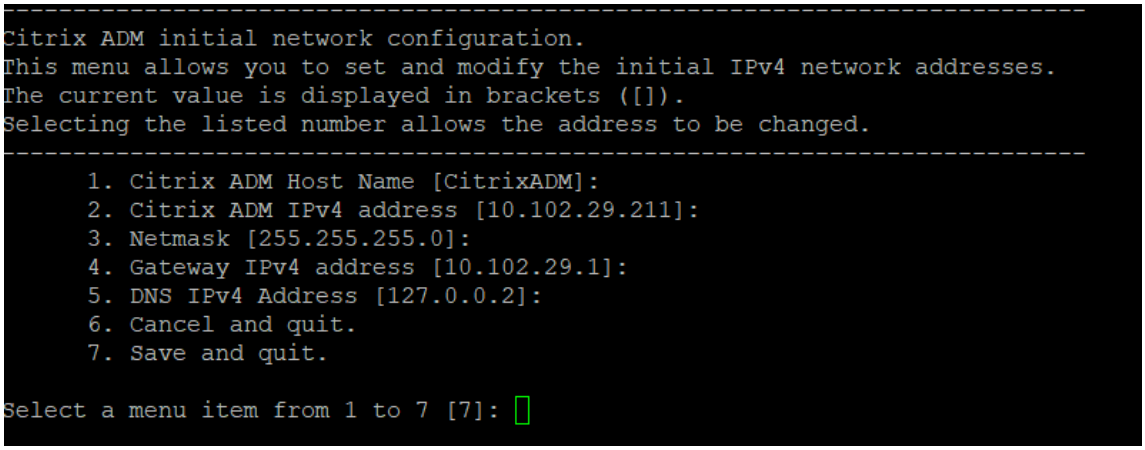


Bereitstellen des zweiten Serverknotens

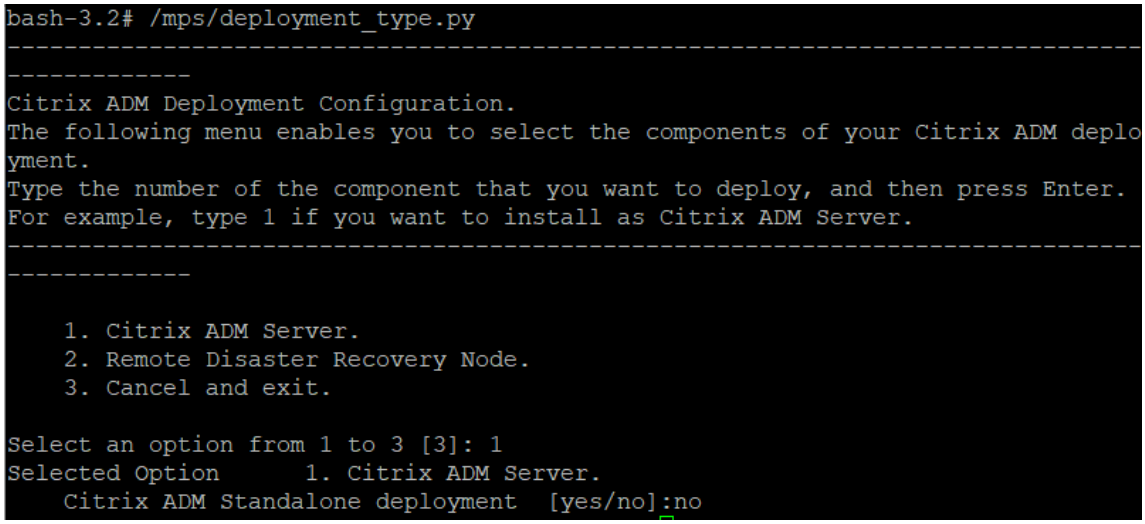
Sie müssen den zweiten Server auf Ihrem Hypervisor bereitstellen. Verwenden Sie dieselbe Imagedatei, mit der Sie den ersten Server installiert haben, oder beziehen Sie eine Imagedatei derselben Version von der Citrix Download-Site.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

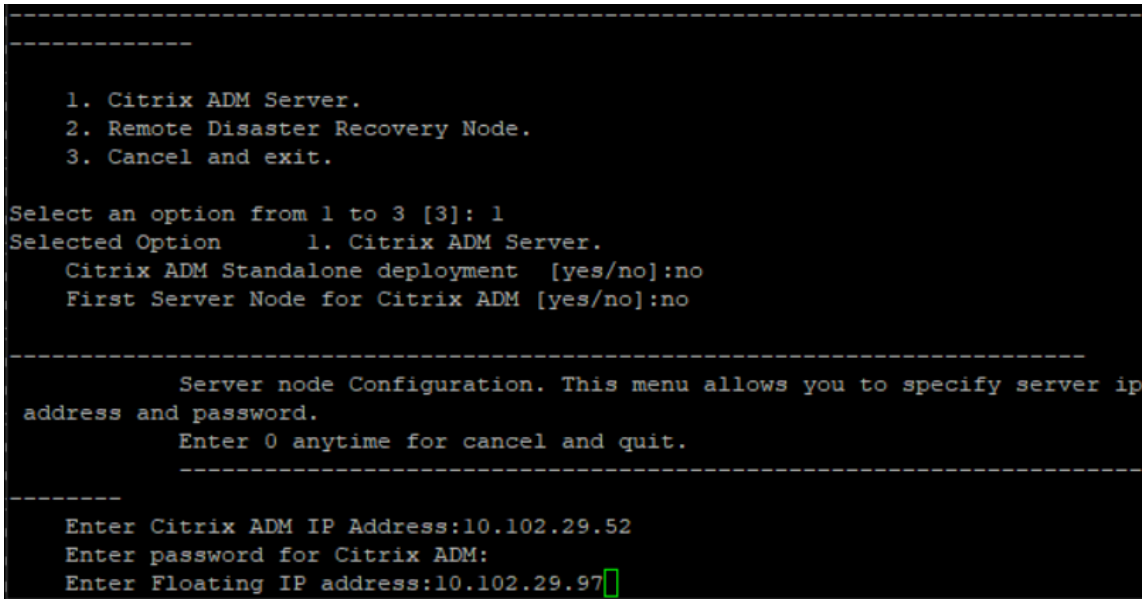
```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

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 mit der Floating-IP auf den primären Knoten 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 NetScaler-Instanzen generiert werden, die einer Anwendung zugeordnet sind, sondern auch die gesamte globale Infrastruktur für die Anwendungsbereitstellung von einer einzigen, einheitlichen Konsole aus verwalten, überwachen und Fehler beheben.

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

Voraussetzungen

Stellen Sie vor der Migration der virtuellen NetScaler Insight Center 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 Citrix ADM 12.0 Build 57.24 installieren und dann auf den neuesten Citrix ADM 12.1-Build aktualisieren. Weitere Informationen finden Sie unter Upgrade.

- Sie haben die neueste Version der NetScaler ADM 12.1 TGZ-Imagedatei heruntergeladen.

Hardwareanforderung

Komponente	Voraussetzung
RAM	32 GB
Virtuelle CPU	8 CPUs
Speicherplatz	120 GB

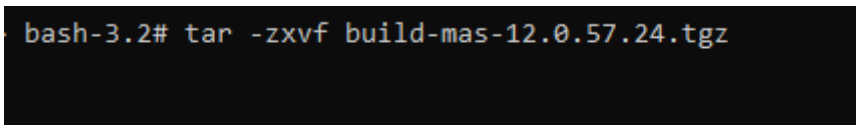
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Komponente	Voraussetzung
	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 an 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 Citrix ADM 12.0 Build 57.24 müssen Sie auf den neuesten Citrix ADM 12.1-Build aktualisieren, indem Sie die obigen Schritte ausführen.

Nach der Migration werden alle NetScaler-Instanzen, die im NetScaler Insight Center-Inventar entdeckt wurden, im Abschnitt Netzwerke > Instanzen von Citrix ADM angezeigt. Zum ersten Mal

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 30 virtuellen Servern an, die in den erkannten NetScaler-Instanzen erstellt wurden. Um mehr als 30 virtuelle Server zu überwachen und zu verwalten, installieren Sie die erforderlichen MAS-Lizenzen. Weitere Einzelheiten finden Sie unterNetScaler ADM-Lizenzierung.

Command Center-Konfigurationen zu NetScaler ADM migrieren

February 5, 2024

Sie können jetzt Ihre Command Center-Konfigurationen auf das NetScaler Application Delivery Management (ADM) migrieren, ohne die vorhandene Konfiguration, Einstellungen oder Daten Ihrer Command Center-Bereitstellung und NetScaler ADM-Bereitstellung zu verlieren. Sie können die migrierten Command Center-Konfigurationen in NetScaler ADM anzeigen, nachdem der Migrationsprozess abgeschlossen ist.

Punkte zu beachten

- Die Migration von Command Center-Konfigurationen zu NetScaler ADM wird in den folgenden Bereitstellungen unterstützt:
  - Command Center eigenständig bis NetScaler ADM Standalone-Bereitstellung oder NetScaler ADM-Hochverfügbarkeitsbereitstellung.
  - Command Center-Hochverfügbarkeit für die eigenständige NetScaler ADM-Bereitstellung oder die NetScaler ADM-Hochverfügbarkeitsbereitstellung.

  > **Hinweis:**
  >
  > Sie müssen nur die IP-Adresse des primären Knotens von Command Center und NetScaler ADM Hochverfügbarkeitsbereitstellung verwenden, während Sie die Command Center-Standalone-Bereitstellung oder Hochverfügbarkeitsbereitstellung auf NetScaler ADM Standalone-Bereitstellung oder Hochverfügbarkeitsbereitstellung migrieren.

- Sie können das Command Center -Tool mehrmals in gleichen oder anderen NetScaler ADM Bereitstellungen ausführen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Wenn Sie das Command Center-Tool über das erste Mal hinaus für dasselbe Citrix ADM ausführen, werden die Protokolle für die Konfigurationen, die bereits migriert wurden und in Citrix ADM vorhanden sind, als fehlgeschlagen angezeigt.
  - Wenn eine neue Konfiguration im Command Center von der früheren Ausführung des Tools bis jetzt für dasselbe NetScaler ADM hinzugefügt wurde, werden alle diese Konfigurationen mit Ausnahme der neuen benutzerdefinierten Aufgaben zu NetScaler ADM migriert.

- Das Migrieren von Command Center Konfigurationen zu Citrix ADM wird für Citrix ADC -, Citrix ADC SDX- und Citrix SD-WAN WO-Geräte unterstützt.
- Die gesamte Kommunikation zwischen Command Center und NetScaler ADM erfolgt über eine HTTPS-Verbindung.
- Es wird dringend empfohlen, die vorhandenen Daten von NetScaler ADM vor der Migration der Command Center-Konfigurationen zu sichern.
- Nach Abschluss der Command Center-Migration werden die Admin-Partitionen von NetScaler ADC im NetScaler ADM automatisch erkannt.

Einschränkungen

Die folgenden Command Center-Konfigurationen werden nicht von der Command Center-Appliance zur NetScaler ADM migriert:

- Konfigurationsdateien für Gerätebackups
- Timeout-Details in SD-WAN WO-Geräteprofilen
- Die folgenden Details unter Ereignis- und Alarmauslöser werden nicht migriert:
  - Details für die Befehlsaktion ausführen abbrechen
  - Aufgabendetails ausführen
  - Trigger mit ausschließlich leeren Parametern (Schweregrad/Kategorie/Instanzen/Fehlerobjekte) werden nicht migriert
  - Trigger mit Instanzen mit dem Status HA-Cluster, primär und sekundär werden nicht migriert, wenn alle drei Zustände der Instanzen ausgewählt sind
- Benutzerdefinierte Aufgaben ohne Beschreibung werden nicht migriert
- Einstellungen für den Schweregrad des Ereignisses
- Einzelheiten zum Zeitplan der Ereignisregeln
- Syslog unterdrückt Filter
- Einzelheiten der Konfigurationsaufgabe

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Audit-Vorlagen
- Prüfungsrichtlinien ohne Geräte
- Einzelheiten zum Zeitplan der Prüfungsrichtlinien
- Gruppen: Autorisierte Bereichseinstellungen für RBAC
- Datenbankmonitor- und Verwaltungseinstellungen
- Benutzerdefinierte Leistungsberichte
- Leistungsschwellen
- Benutzerdefinierte Ansichten von Fault/Syslog/Reports/Entity Monitoring
- AppFirewall- und NS-Gateway-Berichte und deren Zeitplandetails
- Automatische SD-WAN WO Konfigurationsdetails
- Einstellungen für hohe Verfügbarkeit
- Einstellungen für geplante Systemsicherungen
- Einstellungen für Datenbank-Wiederholungsversuche
- Zeitplan für die Syslog-Bereinigung
- Alle statistischen Daten wie Syslog, Ereignisse und Audit-Logs aller Module.

Voraussetzungen

Stellen Sie vor der Migration der Command Center-Konfigurationen zu NetScaler ADM sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie verwenden Command Center Version 5.2 Build 48.2 oder höher.
- Sie haben NetScaler ADM Version 12.0 Build 51.24 oder höher installiert und konfiguriert.
- Nur der Admin-Benutzer führt die Command Center-Konfigurationsmigration aus.
- Für eine erfolgreiche Migration von benutzerdefinierten Aufgaben ist das Beschreibungsfeld im Command Center obligatorisch.
- Die Kommunikation zwischen dem Command Center und NetScaler ADM basiert auf NITRO. Sie müssen die erforderlichen SSL- (Secure Socket Layer) und TLS (Transport Layer Security) -Protokolleinstellungen im Command Center und NetScaler ADM für die NITRO-Kommunikation konfigurieren und öffnen.

> **Hinweis**
>
> Wenn Sie eine Command Center Version vor 5.2 Build 48.2 verwenden, müssen Sie die Command

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

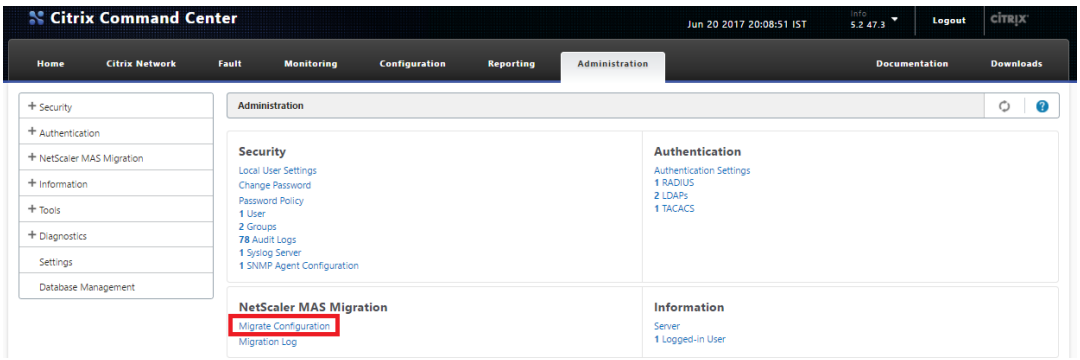
> Center-Version auf 5.2 Build 48.2 aktualisieren und dann die Command Center-Konfigurationen zu NetScaler ADM migrieren. Ausführliche Informationen zum Aktualisieren der Command Center-Appliance finden Sie unter Command Center aktualisieren.

Migrieren der Konfigurationen

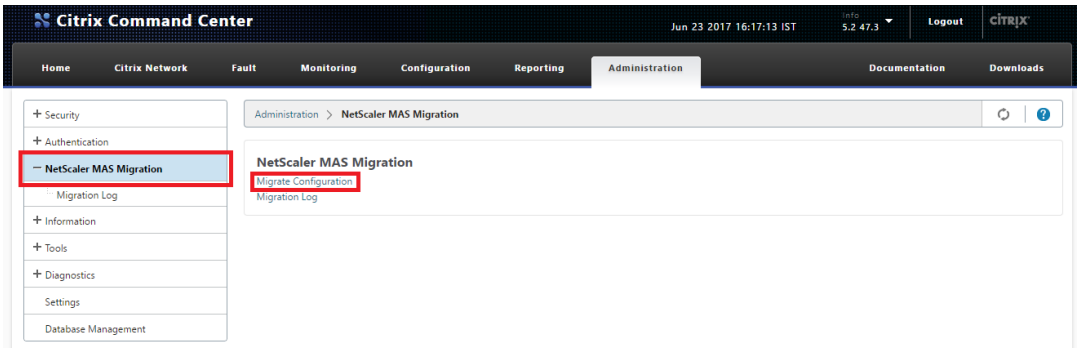
Um eine Command Center-Konfiguration zu NetScaler ADM zu migrieren, benötigen Sie die IP-Adresse der Command Center-Appliance und die Administratoranmeldeinformationen.

So migrieren Sie Command Center-Konfigurationen zu NetScaler ADM:

1. Geben Sie in einem Webbrowser die IP-Adresse der Command Center-Appliance ein.
2. Geben Sie in den Feldern**Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein und melden Sie sich an.
3. Wählen Sie nach erfolgreicher Anmeldung auf dem angezeigten Bildschirm die Registerkarte **Administration** aus, und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie im rechten Bereich unter **Citrix ADM Migration** die Option **Konfiguration migrieren** aus, wie in der folgenden Abbildung gezeigt.



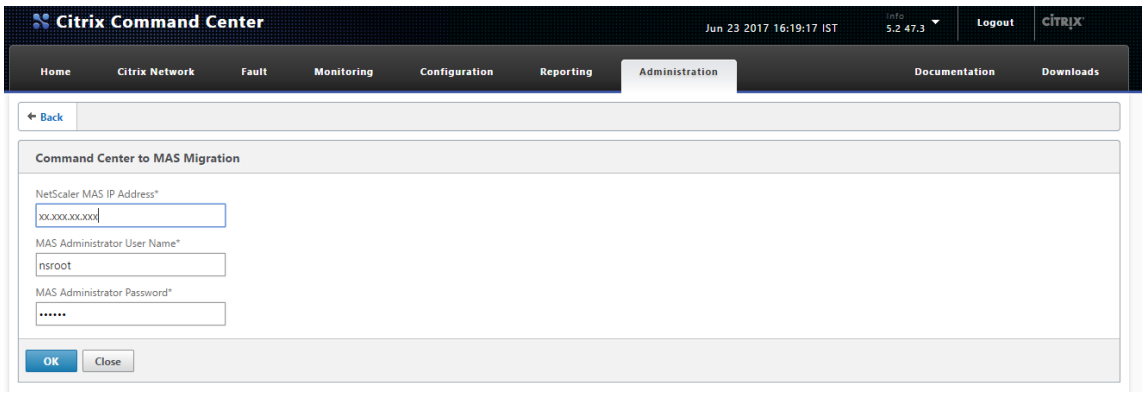
   - Wählen Sie im linken Bereich **Citrix ADM Migration** aus und klicken Sie dann auf **Konfiguration migrieren** , wie in der folgenden Abbildung gezeigt.



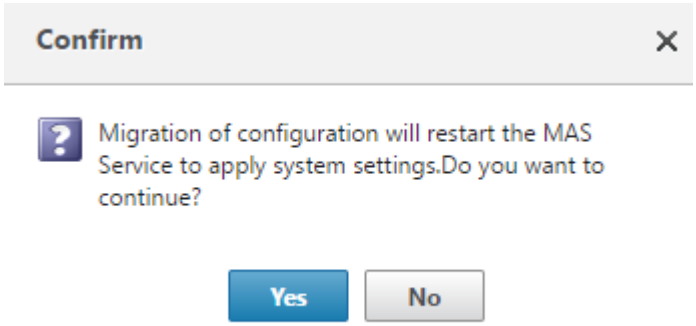
4. Geben Sie im Dialogfeld **Migration von Command Center zu MAS** die IP-Adresse des Citrix ADM Servers und die Administratoranmeldeinformationen ein und klicken Sie dann auf **OK** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

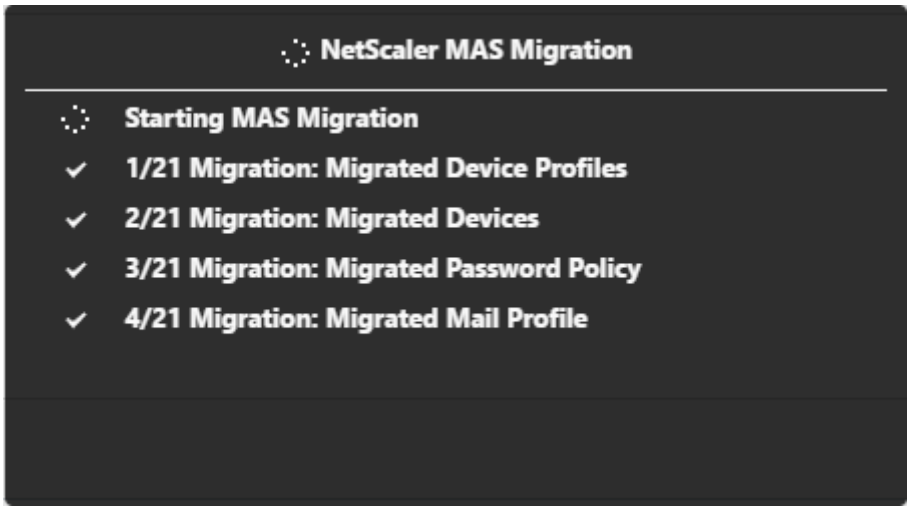
> **Hinweis: Geben Sie**
>
> bei der Bereitstellung mit NetScaler ADM Hochverfügbarkeit die IP-Adresse des primären Knotens ein.



5. Klicken Sie in der Bestätigungsaufforderung auf **Ja**.



Auf dem Bildschirm wird der Fortschritt der Migrationsaufgaben angezeigt.



Der Vorgang **"Konfiguration migrieren** "übernimmt die Details der NetScaler ADM Bereitstellung und

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

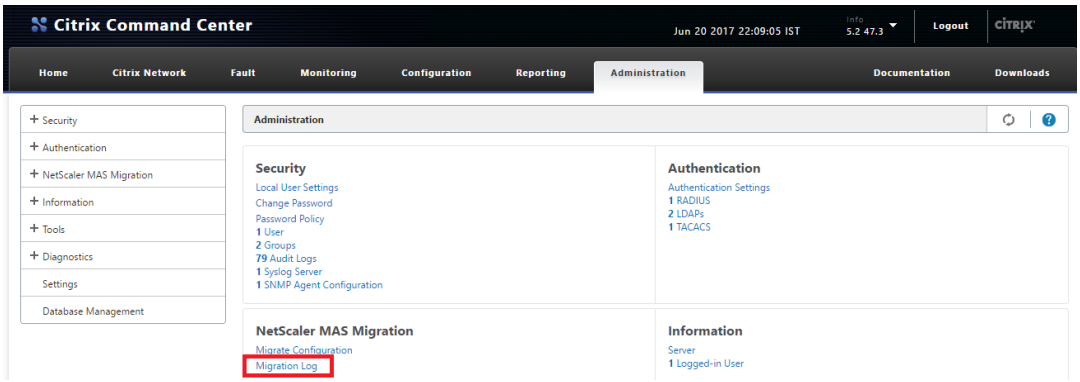
ihrer Administratoranmeldeinformationen als Eingabe. Der Vorgang **Konfiguration migrieren** migriert dann die Konfiguration der Command Center-Bereitstellung zur NetScaler ADM-Bereitstellung.

Wenn die Aufgaben abgeschlossen sind, können Sie die migrierte Command Center-Konfiguration anhand der Command Center-Migrationsprotokolle und NetScaler ADM-Daten überprüfen.

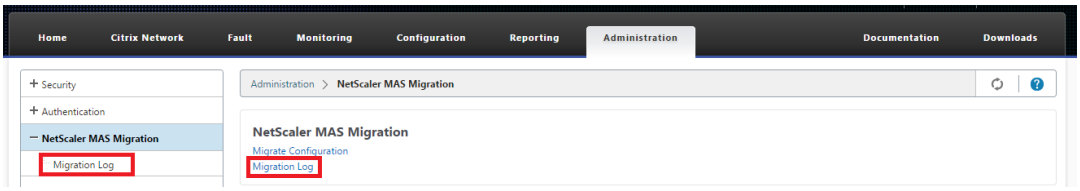
Um die Migration mithilfe der Command Center-Migrationsprotokolle zu überprüfen

1. Führen Sie in der Command Center Benutzeroberfläche auf der Registerkarte **Administration** einen der folgenden Schritte aus:

   - Klicken Sie im rechten Bereich unter **Citrix ADM**Migration** auf Migrationsprotokoll .

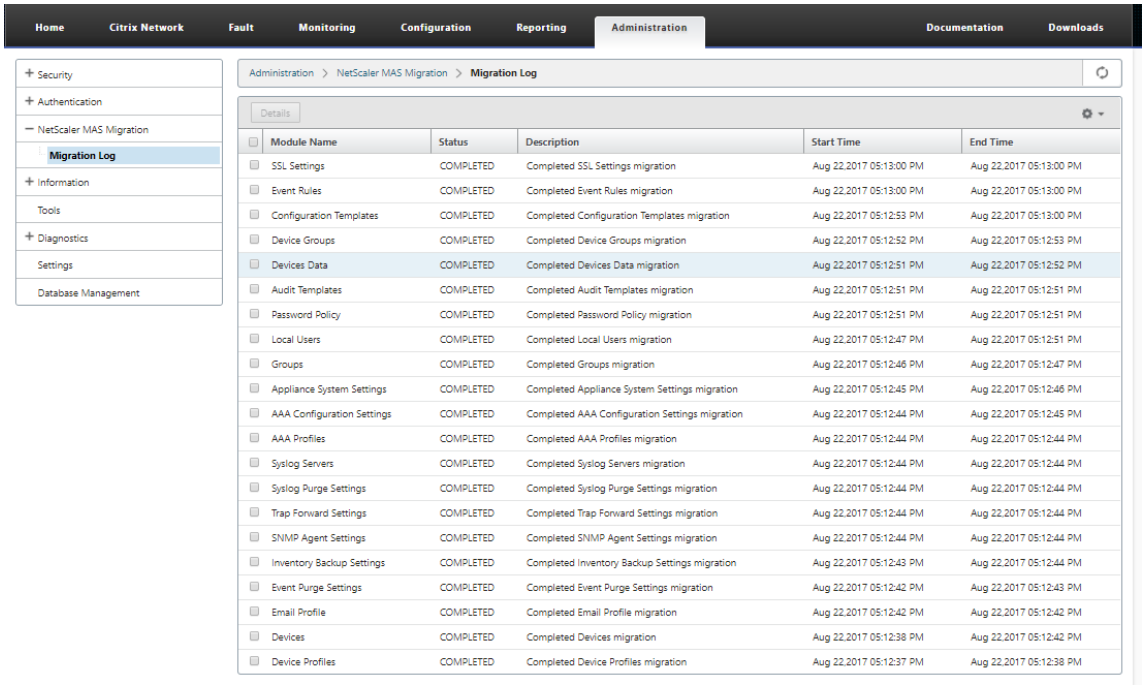
   

   - Wählen Sie im linken Bereich **Citrix ADM Migration** aus und klicken **Sie dann**auf Migrationsprotokoll .

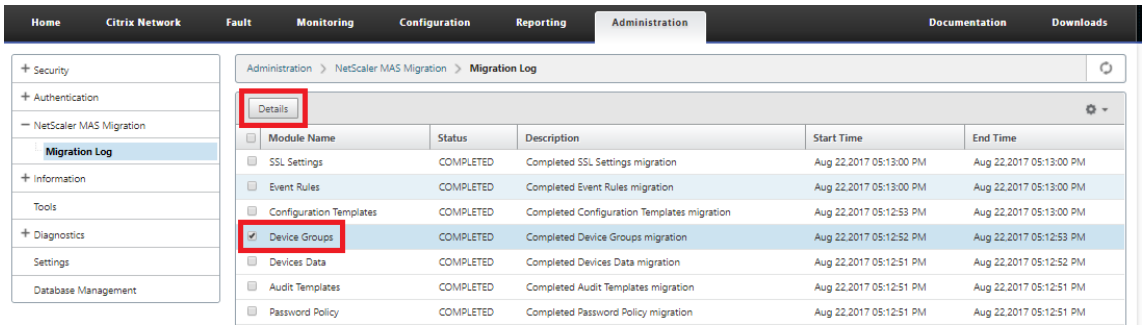
   

2. Überprüfen Sie die Liste der Migrationsprotokolle.

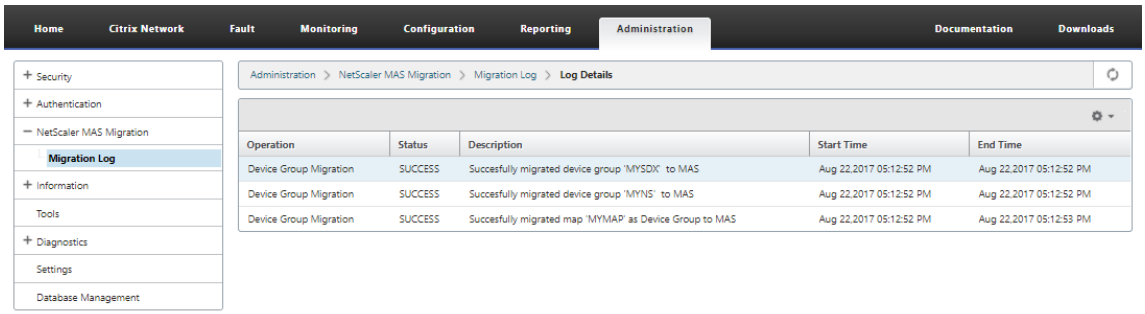
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Um weitere Details anzuzeigen, wählen Sie **Modulname**aus, oder um Details für ein bestimmtes Modul anzuzeigen, wählen Sie dieses Modul aus, und klicken Sie dann auf **Details**.



4. Das folgende Beispiel zeigt die Protokolldetails für ein ausgewähltes Modul.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

So überprüfen Sie die Migration mithilfe von NetScaler ADM

Während des Migrationsprozesses werden die Command Center-Konfigurationen zu NetScaler ADM migriert und in der NetScaler ADM-GUI als NetScaler ADM-Konfigurationen angezeigt.

Nach Abschluss des Migrationsprozesses wird der NetScaler ADM Server neu gestartet und es kann zu vorübergehenden Ausfallzeiten kommen. Wenn der NetScaler ADM Server läuft, greifen Sie auf die NetScaler ADM GUI zu, indem Sie die IP-Adresse des NetScaler ADM-Servers in die Adressleiste Ihres Browsers eingeben.

Die folgende Tabelle zeigt, wie die NetScaler ADM-Terminologie für die migrierten Konfigurationen der im Command Center verwendeten Terminologie entspricht.

Command Center-Terminologie	NetScaler ADM-Terminologie
Geräteprofile	Instanzprofile
Geräte und ihr Status (z. B. verwaltet/nicht verwaltet)	Instanzen und ihr Status (z. B. verwaltet/nicht verwaltet)
Anmerkungen zum Gerät	Instanzanmerkungen
Gerätegruppen	Instanzgruppen
Karten	Instanzgruppen
Ereignis- und Alarmauslöser	Ereignisregeln
Integrierte und benutzerdefinierte Taskbefehle	Konfigurationsvorlagen unter dem Editor zum Erstellen von Jobs
Richtlinien für geplante Audits	Audit-Vorlagen
Kennwort-Richtlinie	Kennwort-Richtlinie
Benutzer (nur lokale Benutzer)	Systembenutzer
Gruppen*	Systemgruppen
Authentifizierungsprofile und Authentifizierungseinstellungen	Authentifizierungsprofile und Authentifizierungskonfiguration
E-Mail-Einstellungen	E-Mail-Server/E-Mail-Verteilerliste
syslog-Server	syslog-Server
SSL-Einstellungen	SSL-Einstellungen
Konfiguration des SNMP-Agenten	SNMP-Manager
Trap-Forward-Einstellungen	Trap-Einstellungen
Einstellungen für das Löschen von Ereignissen	Einstellungen für Ereignisse einschränken
Bestandseinstellungen	Einstellungen für Instanz-Backups

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Command Center-Terminologie	NetScaler ADM-Terminologie
Einstellungen für das Syslog-Löschen	Syslog Prune-Einstellungen
Netzwerkeinstellungen der Appliance wie DNS, NTP und Zeitzone	NetScaler ADM-Netzwerkeinstellungen wie DNS, NTP und Zeitzone

*Gruppen mit allen Berechtigungen im Command Center werden als Gruppen mit einer "Admin"-Rolle in NetScaler ADM migriert. Alle anderen Command Center-Gruppen werden als Gruppen mit einer "schreibgeschützten"Rolle in NetScaler ADM migriert.

Integration von NetScaler ADM und Citrix Director

February 5, 2024

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

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

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

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

Voraussetzungen

Hardwareanforderungen für HDX Insight to Citrix ADM Migration

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Anforderungen an die Software

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 Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinweis

- Weitere Informationen zu Director und Schritte zur Integration von NetScaler ADM mit Director finden Sie unterhttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.html.
- Weitere Informationen zu HDX Insight finden Sie unterhttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Zusätzlichen Datenträger in NetScaler ADM bereitstellen

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 für die Speicherung Ihrer Daten benötigen, können Sie eine zusätzliche Festplatte anhängen.

Hinweis

- Schätzen Sie die Speicheranforderungen und fügen Sie zum Zeitpunkt der Erstbereitstellung von Citrix ADM eine zusätzliche Festplatte an den Server hinzu.
- Bei einer NetScaler ADM Bereitstellung mit einem Server können Sie zusätzlich zum Standarddatenträger nur einen Datenträger an den Server anhängen.
- Für eine Citrix ADM Bereitstellung mit hoher Verfügbarkeit müssen Sie jedem Knoten eine zusätzliche Festplatte hinzufügen. 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 eine zusätzliche Festplatte mit einer Kapazität von mehr als 2 Terabyte anhängen. 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 Anhängen eines neuen zusätzlichen Datenträgers, zum Erstellen von Partitionen und zur Größenänderung der zusätzlichen Datenträger erläutert:

1. Hinzufügen eines neuen zusätzlichen Datenträgers

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Starten Sie das Datenträgerpartitionierungstool
3. Erstellen von Partitionen auf dem neuen zusätzlichen Datenträger
4. Ändern der Größe des vorhandenen zusätzlichen Datenträgers
5. Entfernen von Partitionen auf dem zusätzlichen Datenträger

Hinzufügen eines zusätzlichen Datenträgers in einem eigenständigen Citrix 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. Fügen Sie im Hypervisor eine zusätzliche Festplatte mit der erforderlichen Datenträgergröße der virtuellen Citrix ADM Maschine hinzu.

   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. Mit diesem Tool können Sie auch die Größe vorhandener zusätzlicher Datenträger ändern. Die vorhandene externe Festplatte sollte 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-->
```

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
(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 wird, wird ein GUID-Partitionstabelle (GPT) -Partitionsschema 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 mit einem Master Boot Record (MBR) oder GPT-Schema ändern. Die Größe des Datenträgers sollte kleiner als 2 Terabyte und maximal 2 Terabyte sein.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
(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
```

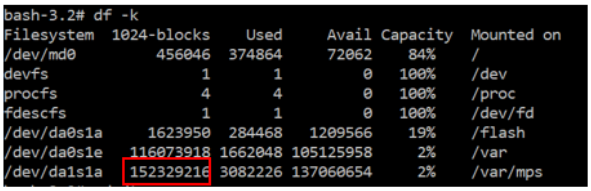
```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

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.

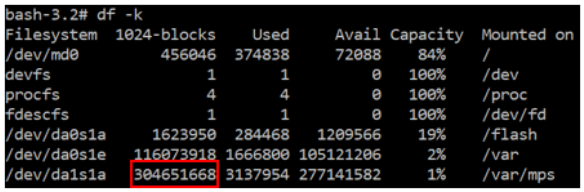
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
(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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Festplattenspeicher verfügbar ist (50% oder mehr), 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. Tarball erstellen.

```
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 mps_backup.tgz > mps_backup_checksum
<!--NeedCopy-->
```

6. Kopieren Sie deb Tarball und die Prüfsumme aus der Ferne.

```
scp
<!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

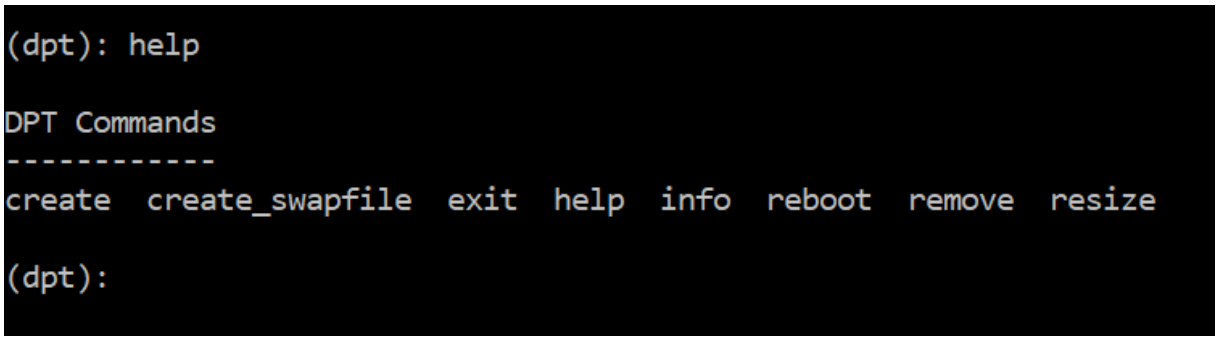
```
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
-------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
-------------
(dpt):
```

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 Citrix ADM Versionen erstellt wurden, die keine Swap-Partition haben. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
(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. Nehmen wir außerdem an, dass Sie zwei oder mehr Citrix 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Führen Sie die folgenden Schritte aus, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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 über die grafische Benutzeroberfläche (GUI) auf einen NetScaler ADM -Server zugreifen. Sie müssen auf die GUI zugreifen, um Instanzen hinzuzufügen, Ihre Instanzen und Apps zu verwalten und zu überwachen, Analysen anzuzeigen und den Citrix 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.

Web-Browser	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:

1. Geben Sie in einem Webbrowser die IP-Adresse von NetScaler ADM ein (z. B.http://192.168.100.1). Dies ist dieselbe IP-Adresse, die Sie bei der Installation des Servers angegeben haben.
2. ******** Geben Sie in den Feldern Benutzername und Kennwort die Administratoranmeldedaten ein. Die standardmäßigen Administratoranmeldedaten sind nsroot/nsroot.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Citrix ADM zur Verwaltung und Überwachung Ihrer Instanzen und Anwendungen verwenden, wird empfohlen, einige Systemeinstellungen zu konfigurieren, die eine optimale Leistung Ihres Citrix 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:

- Citrix ADC
  - NetScaler ADC MPX
  - NetScaler ADC VPX
  - NetScaler ADC SDX
  - NetScaler ADC CPX
- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

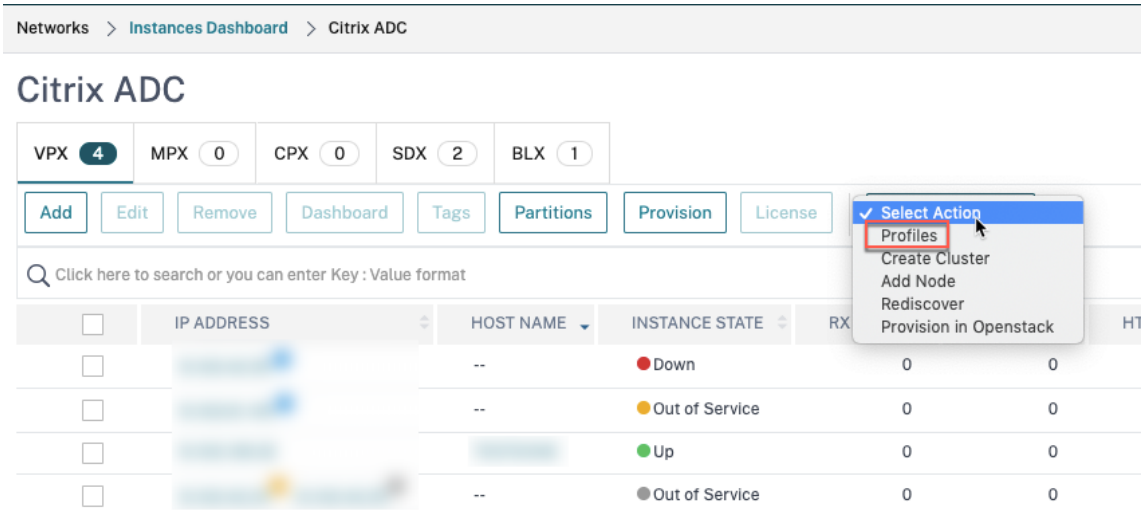
So erstellen Sie ein Citrix ADC-Profil

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. Beispielsweise ist nsroot das Standardprofil für Citrix 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.

So erstellen Sie ein NetScaler ADC Profil auf der Instanzseite:

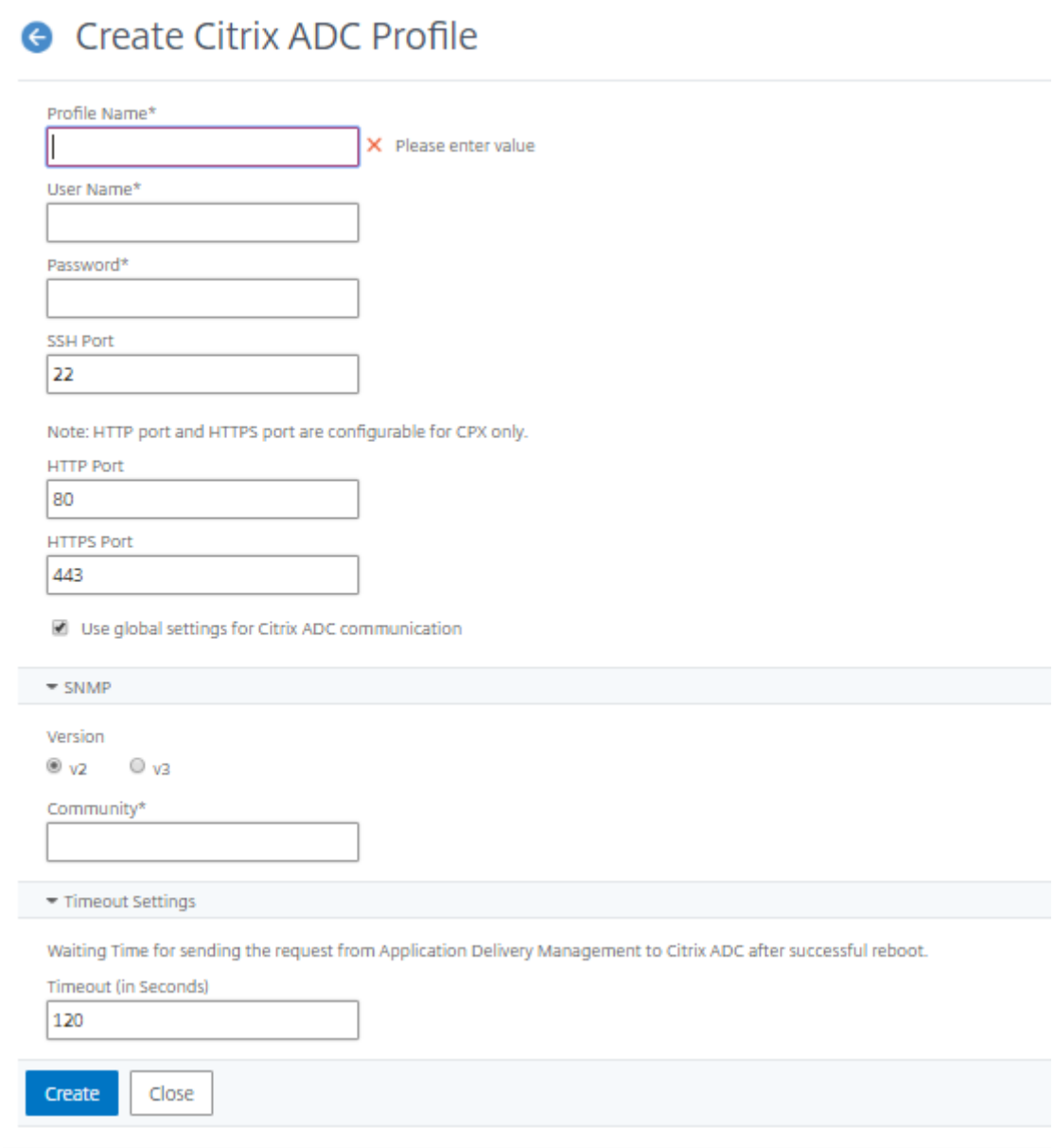
1. Navigieren Sie zu **Netzwerke > Instanzen**.
2. Wählen Sie eine Instanz aus. Beispiel: NetScaler ADC.
3. Wählen Sie auf der Seite NetScaler ADC die Option **Profile**aus.



4. Wählen Sie auf der Seite **Admin-Profile** die Option **Hinzufügen**aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

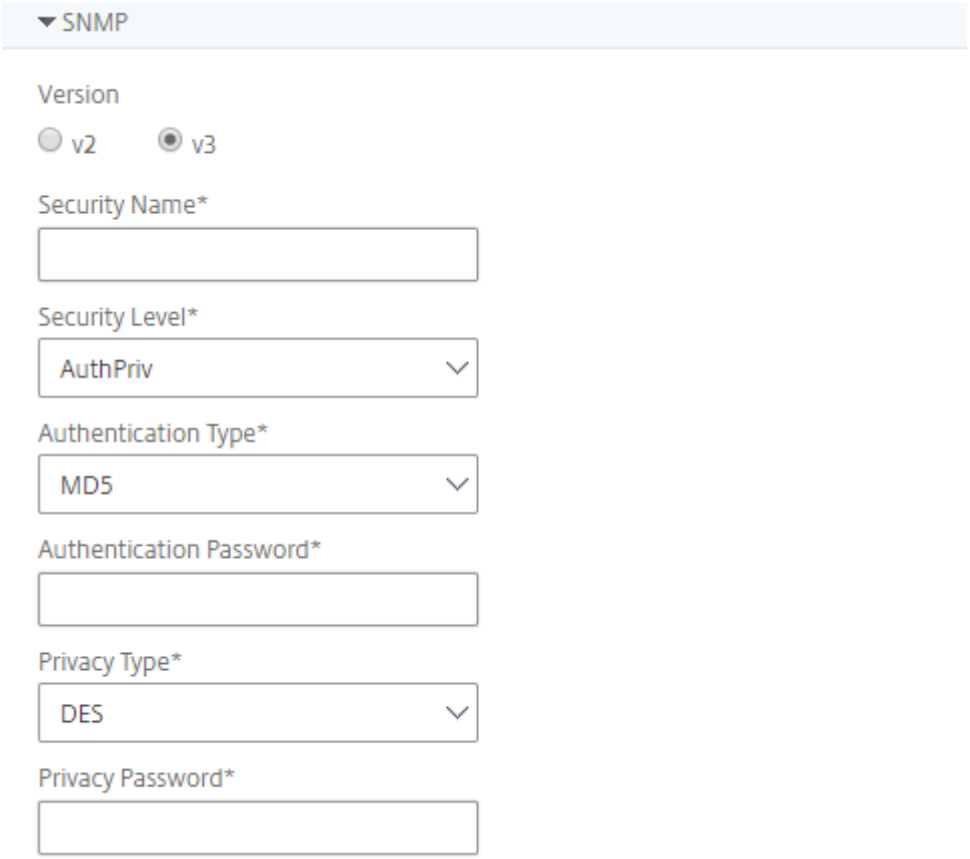
g) **Globale Einstellungen für die Citrix ADC-Kommunikation verwenden**: Wählen Sie diese Option, wenn Sie die Systemeinstellungen für die Kommunikation zwischen Citrix ADM und der Citrix ADC-Instanz verwenden möchten, andernfalls wählen Sie entweder http oder https.

h) **SNMP-Version**: Wählen Sie entweder **SNMPv2** oder **SNMPv3** aus, und führen Sie die folgenden Schritte aus:

   i. Wenn Sie SNMPv2 auswählen, geben Sie den **Community-Namen** für die Authentifizierung an.

   ii. Wenn Sie SNMPv3 auswählen, geben Sie den **Sicherheitsnamen** und die **Sicherheitsstufe an**. Wählen Sie basierend auf der Sicherheitsstufe den **Authentifizierungstyp** und den **Datenschutztyp**aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

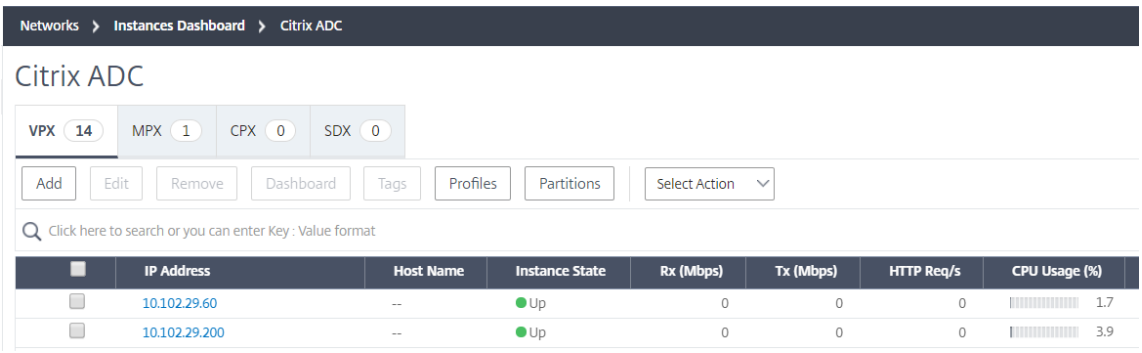
> **Hinweis**
>
> - Um NetScaler ADC-Instanzen hinzuzufügen, die in einem Cluster konfiguriert sind, müssen Sie entweder die Cluster-IP-Adresse oder einen der einzelnen Knoten im Cluster-Setup angeben. In NetScaler ADM wird der Cluster jedoch nur durch die Cluster-IP-Adresse dargestellt.
> - Bei NetScaler 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 den Administratoranmeldeinformationen bei Citrix ADM an.
2. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler 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. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die Instanz aus, die Sie erneut ermitteln möchten, und klicken Sie dann in der Liste **Aktion auswählen** auf **Erneut entdecken.**

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**.
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.

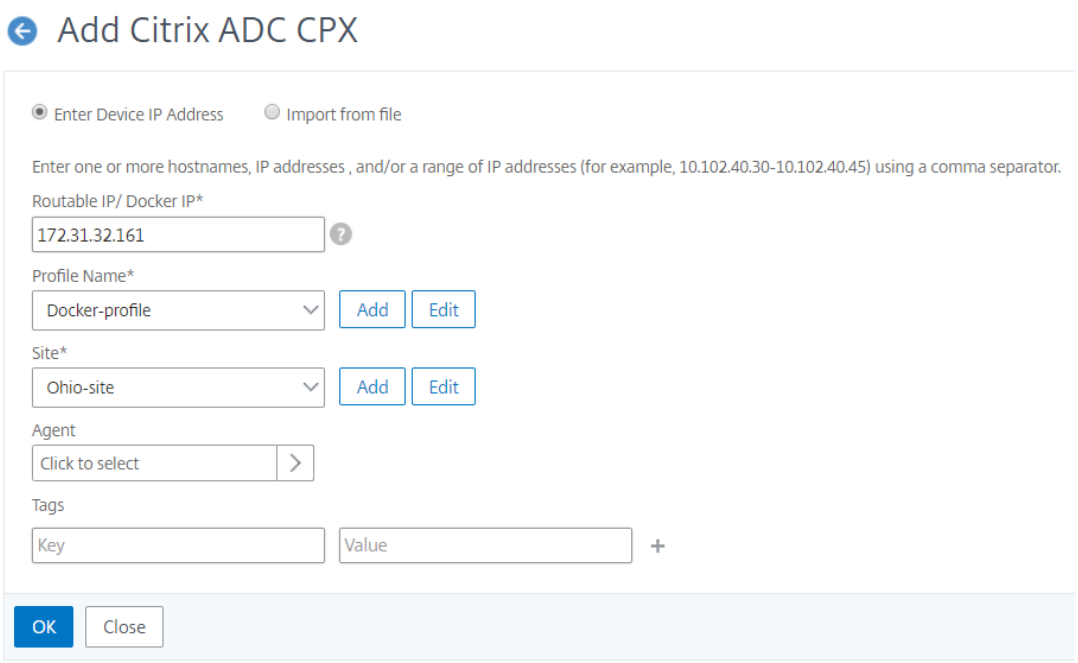
    b) Wählen Sie das Profil der CPX-Instanz aus.

    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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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**.

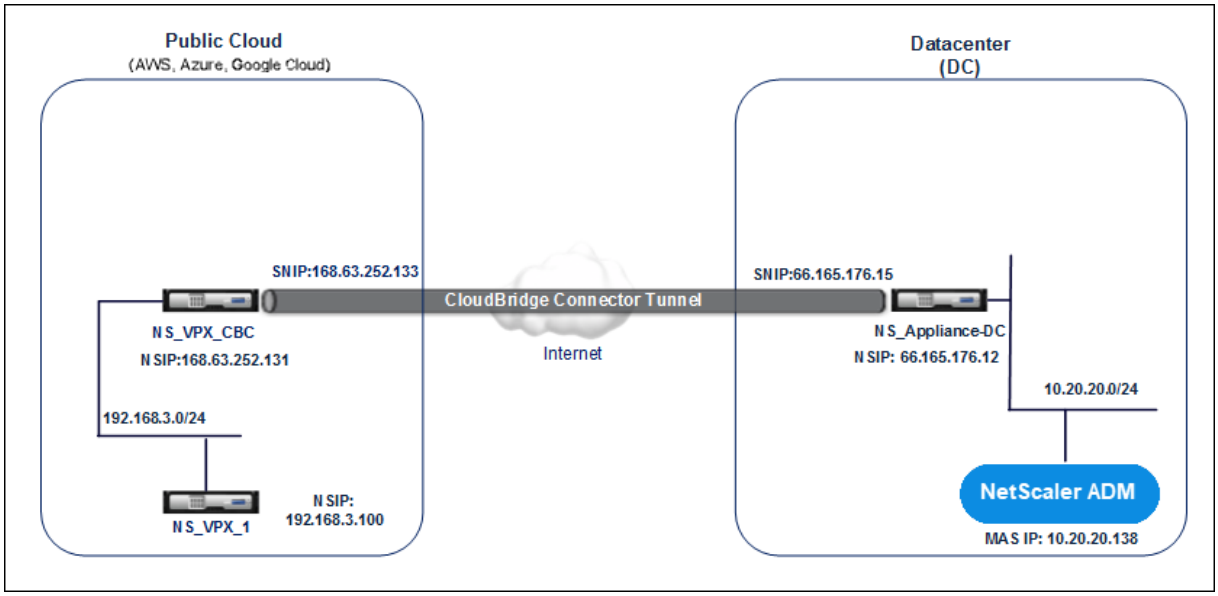
Hinzufügen von NetScaler ADC VPX Instanzen, die in der Cloud bereitgestellt werden, zu NetScaler ADM

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 NetScaler CloudBridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN in Azure oder Connectors von Drittanbietern wie Equinix usw. verwenden.

In der folgenden Beispieltopologie wird NetScaler CloudBridge Connector für Layer 3-Konnektivität zwischen Citrix ADM und den in der Cloud bereitgestellten Citrix ADC VPX Instanzen verwendet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ein CloudBridge Connector-Tunnel wird zwischen der Citrix ADC Appliance NS_Appliance-DC im Rechenzentrums-DC und der virtuellen Citrix 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.

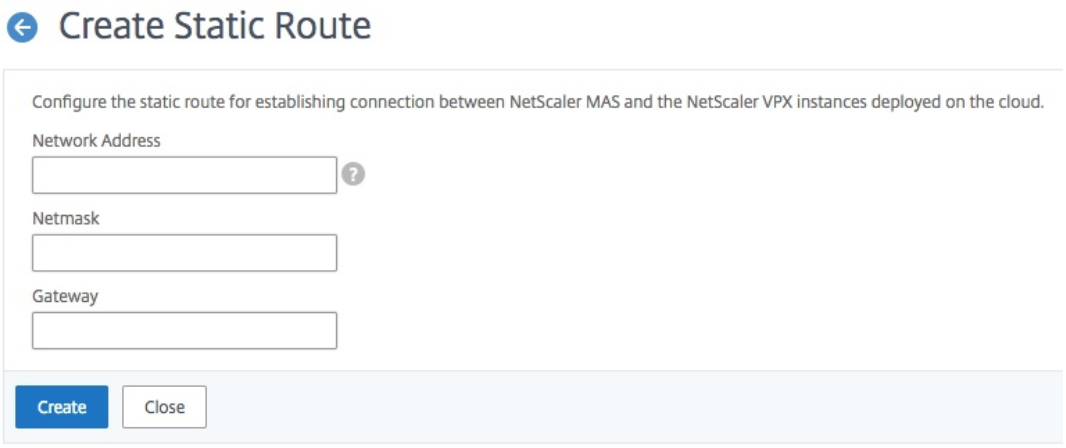
Gehen Sie wie folgt vor, um diese Topologie zu konfigurieren:

1. Installieren, konfigurieren und starten Sie eine NetScaler ADC VPX Instanz in der Public Cloud.
   - Anweisungen finden Sie unter Installation von Citrix ADC VPX auf AWS .
   - Anweisungen finden Sie unter Installieren von Citrix ADC VPX auf Microsoft Azure .
2. Stellen Sie eine physische NetScaler ADC Appliance bereit und konfigurieren Sie eine virtuelle NetScaler ADC-Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum.
   - Anweisungen finden Sie unter Installieren von Citrix ADC Virtual Appliances auf Citrix Hypervisor .
   - Anweisungen finden Sie unter Installation virtueller Citrix-Appliances auf VMware ESXi .
   - Anweisungen finden Sie unter Installieren virtueller Citrix ADC Appliances auf Microsoft Hyper-V .
3. Konfigurieren Sie den CloudBridge Connector zwischen dem Rechenzentrum und der Public Cloud. Anweisungen finden Sie unter CloudBridge Connector konfigurieren .
4. Konfigurieren Sie die statische Route für den Verbindungsaufbau zwischen Citrix ADM und den in der Cloud bereitgestellten Citrix ADC VPX-Instanzen wie folgt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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.

Analytics auf virtuellen Servern aktivieren

February 5, 2024

Sie können Analysen für einen bestimmten virtuellen Server auf der ausgewählten Instanz aktivieren, die einen Anwendungsserver darstellt, und den Datenverkehr dieses Anwendungsservers überwachen. Analytics liefert Statistiken für den virtuellen Server.

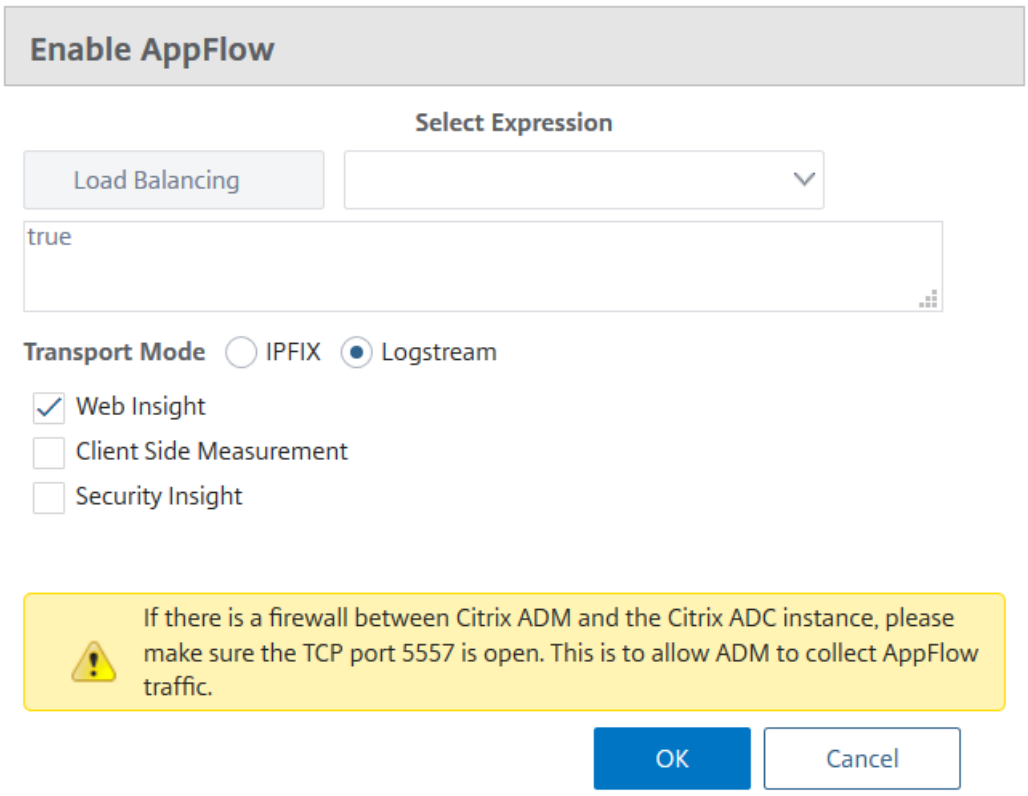
> **Hinweis**
>
> Für NetScaler ADC-Instanzen der Version 11.0, Version 65.30 und höher gibt es in NetScaler ADM keine Option, Security Insight explizit zu aktivieren. Stellen Sie sicher, dass Sie die AppFlow-Parameter auf den Citrix ADC-Instanzen konfigurieren. Nachdem die Konfiguration der AppFlow-Parameter abgeschlossen ist, empfängt Citrix ADM den Security Insight-Verkehr zusammen mit dem Web Insight-Verkehr. Weitere Informationen zum Festlegen der AppFlow-Parameter auf

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> NetScaler ADC-Instanzen finden Sie unterSo legen Sie die AppFlow-Parameter mithilfe des Konfigurationsdienstprogrammsfest.

So aktivieren Sie Analytics auf jeder Instanz auf Citrix ADM:

1. Navigieren Sie zu **Netzwerke** > **Instanzen** und wählen Sie die Citrix ADC-Instanz aus, für die Sie Analysen aktivieren möchten. Beispiel: NetScaler ADC.
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 in das Feld **Enable AppFlow** den Wert **true** ein und wählen Sie je nach den Analysen, die Sie aktivieren möchten, **Security Insight** oder **Web Insight** oder beides aus.

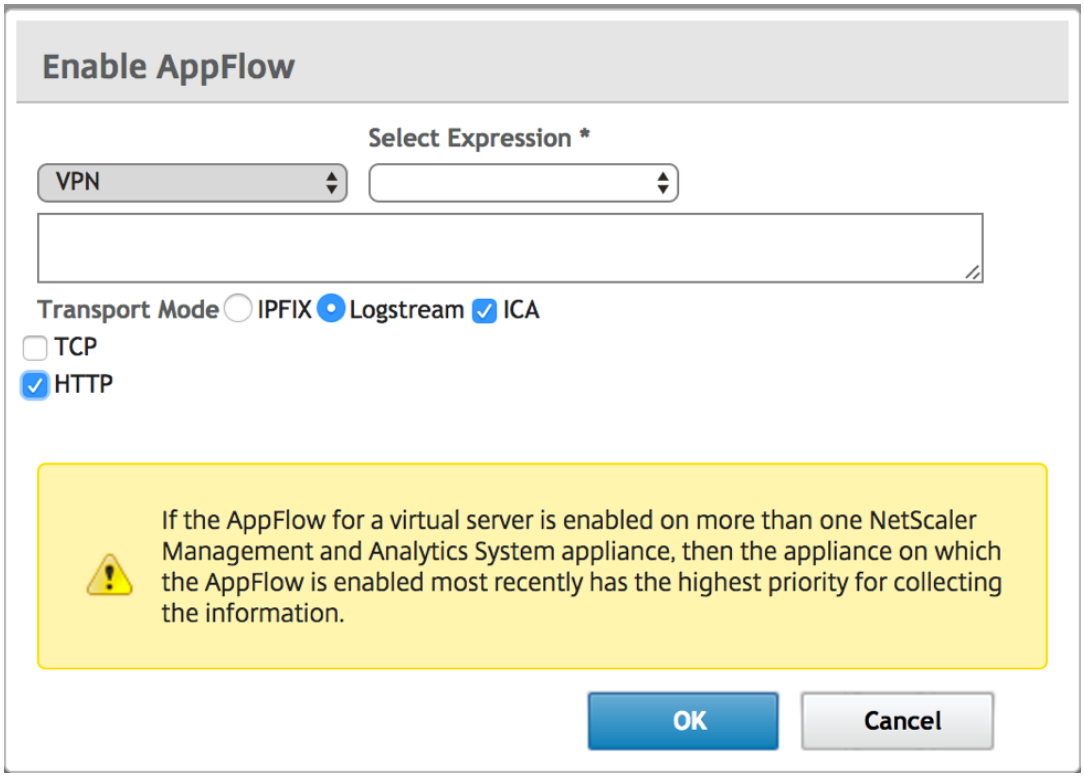


> **Hinweis**
>
> Citrix ADM verwendet Citrix ADC SNIP für Logstream und NSIP für IPFIX. Wenn zwischen der NetScaler ADM und der NetScaler ADC Instanz eine Firewall aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit NetScaler ADM AppFlow Datenverkehr erfassen kann:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Transport-Modus	Quell-IP	Typ	Port
IPFIX	NSIP	UDP	4739
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 Citrix ADC-Instanz konfiguriert ist, und die entsprechenden **ICA** - oder **HTTP**-Kontrollkästchen auswählen.



- Navigieren Sie für **TCP Insight** zu **System** > **Analytics-Einstellungen** > **Funktionen konfigurieren** und wählen Sie **TCP Insight aktivieren** aus.
- Für **Video Insight** müssen Sie die Konfigurationsänderungen auf der Citrix ADC Appliance vornehmen. Weitere Informationen zum Aktivieren von Analysen für Video Insight finden Sie unter Video Insight.
- Für **WAN Insight**
  a) Navigieren Sie zu **Infrastruktur** > **Instanzen** > **NetScaler SD-WAN WO** und wählen Sie die WAN-Optimierungs-Appliance für Rechenzentren aus.
  b) Klicken Sie in der Dropdown-Dropdown-Option **“Aktion”** auf **“Enable Insight”.**
  c) Wählen Sie die folgenden Parameter nach Bedarf aus:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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** für IPFIX oder Logstream auswählen und gleichzeitig AppFlow auf den erkannten Citrix ADC-Instanzen in Citrix 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 **Web Insight aktivieren** in Citrix ADM verwenden. Wenn Sie den Web Insight-Datenverkehr nicht überwachen möchten, können Sie die Option deaktivieren. Weitere Informationen finden Sie unter Verarbeitung des Web Insight-Datenverkehrs durch Citrix ADM.

NTP-Server konfigurieren

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 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 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Systemeinstellungen konfigurieren

February 5, 2024

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.

Konfigurieren von Systemalarmen

Sie sollten Systemalarme konfigurieren, um sicherzustellen, dass Sie kritische oder schwerwiegende 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 CPU-UsageHigh oder MemoryUsageHigh, können Sie Schwellenwerte festlegen und den Schweregrad (z. B. Critical oder Major) für jede Alarmkategorie definieren. Für einige Kategorien, wie inventoryFailed oder loginFailure, können Sie nur den Schweregrad definieren. Wenn der Schwellenwert für eine Alarmkategorie überschritten wird (z. B. MemoryUsageHigh) oder wenn ein Ereignis eintritt, das der Alarmkategorie entspricht (z. B. LoginFailure), wird eine Meldung im System aufgezeichnet, und Sie können die Nachricht als Syslog-Meldung anzeigen.

So konfigurieren Sie Systemalarme:

1. Navigieren Sie zu **System > Alarme** , wählen Sie den Alarm aus, den Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten** .
2. Wählen Sie auf der Seite **Alarm konfigurieren** den Schweregrad des Alarms aus, und legen Sie den Schwellenwert fest.
3. 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 eine Reihe von systembezogenen 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.

So konfigurieren Sie Systembenachrichtigungen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Navigieren Sie zu **System > Benachrichtigungen** . Klicken Sie unter **Einstellungen** auf Benachrichtigungseinstellungen **ändern** .
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 des Citrix ADM -Servers gespeichert werden, können Sie angeben, in welchem Intervall Citrix ADM Netzwerkberichtungsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle aufbewahrt werden 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 **Prune Settings** auf **System Prune Settings** .
2. Geben Sie auf der Seite **System-Prune-Einstellungen konfigurieren** die Anzahl der Tage an, für die Daten aufbewahrt werden sollen, und klicken Sie auf **OK**.

Einstellungen für das Systembackup konfigurieren

NetScaler ADM sichert das System täglich um 00:30 Uhr automatisch. 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 > Systemadministration**.
2. Klicken Sie unter **Backup-Einstellungen**auf **System-Backup-Einstellungen**.
3. 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 Sicherungsdateien verwenden, um die Stabilität wiederherzustellen, falls die Instanz instabil wird. Dies ist besonders

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 > Systemadministration**.
2. Wählen Sie unter **Backup-Einstellungen** die Option **Instanz-Backup-Einstellungen** aus und geben Sie die erforderlichen Werte an.

Einstellungen für das Ausschneiden von Instanzereignissen konfigurieren

Um die Anzahl der Ereignisnachrichtungsdaten zu begrenzen, die in der Datenbank des NetScaler ADM -Servers gespeichert werden, können Sie angeben, in welchem Intervall NetScaler ADM Netzwerkberichtungsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle beibehalten 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 > 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 Citrix ADM Server speichern möchten, und klicken Sie auf **OK** .

Konfiguration der Syslog-Löscheinstellungen für Instanzen

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 Citrix ADM gelöscht werden.

So konfigurieren Sie die Einstellungen zum Löschen von Instanzsyslog-Einstellungen:

1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter Prune Settings auf **Instance Syslog Purge Settings**.
2. Geben Sie auf der Seite Syslog-Löscheinstellungen für Instanzen konfigurieren die Anzahl der Tage zwischen 1 und 180 im Feld **Generische Syslog-Daten beibehalten** an.
3. Klicken Sie auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 finden Sie in den Versionshinweisen, die jeder Versionsankündigung beiliegen. Es ist auch wichtig, das Lizenzierungsframework und die Lizenztypen 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 Upgradepaket von der NetScaler ADM-Downloadsseite herunter und folgen Sie den Anweisungen in diesem Artikel, um Ihr System auf den neuesten 12.1-Build zu aktualisieren. Nach dem Start des Upgradevorgangs wird NetScaler ADM neu gestartet und die vorhandenen Verbindungen werden beendet und wieder verbunden, wenn das Upgrade erfolgreich 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 12.1 zu beachtensind:

- Wenn Sie von Version 11.1 oder von Version 12.0 Build vor 56.x auf die Version NetScaler ADM 12.1 Build 48.18 aktualisieren, führen Sie die folgenden Schritte aus.
  - Aktualisieren Sie von der vorhandenen Version auf 12.0 Build 57.24.
  - Führen Sie dann ein Upgrade auf den neuesten Build von Version 12.1 durch.

    Sie müssen diesem zweistufigen Prozess folgen, da für ein erfolgreiches Upgrade auf Version 12.1 bestimmte Bereinigungsverfahren erforderlich sind. Diese Prozeduren sind erst ab 12.0 Build 56.x verfügbar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Mit 12.1 bietet die Hochverfügbarkeitsbereitstellung die Möglichkeit, eine Floating-IP auf dem primären Knoten zu konfigurieren, sodass kein separater NetScaler ADC Load Balancer erforderlich ist. Aufgrund dieser Verbesserung muss sich die Hochverfügbarkeitsbereitstellung im selben Subnetz befinden. Wenn sich Ihre aktuelle Bereitstellung in verschiedenen Subnetzen befindet, müssen Sie diesen Artikel lesen, um mehr über den Upgrade-Prozess zu erfahren.
- Mit 12.1 wurde die erweiterte Backup-Unterstützung entfernt. Die erweiterte Backupfunktion ist nach dem Upgrade auf NetScaler ADM 12.1 nicht mehr verfügbar. Lesen Sie diesen Artikel für weitere Informationen.

> **Hinweis**
>
> Sie können NetScaler ADM nicht von einem 12.1-Build auf einen Build einer früheren Version herabstufen.

Empfohlene Vorsichtsmaßnahmen:

- 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. Es kann einige Minuten dauern, bis der Upgradevorgang abgeschlossen ist.

- 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:

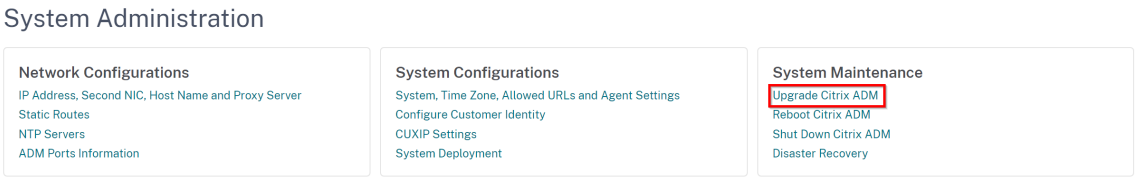
1. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler ADM-Servers ein.

   > **Hinweis: Geben Sie**
   >
   > für NetScaler ADM-Server in einem Hochverfügbarkeitsmodus die IP-Adresse eines der NetScaler ADM-Server im HA-Paar oder des virtuellen Lastausgleichsservers ein.

2. **** Geben Sie in den Feldern Benutzername und Kennwort die Administratoranmeldedaten ein.

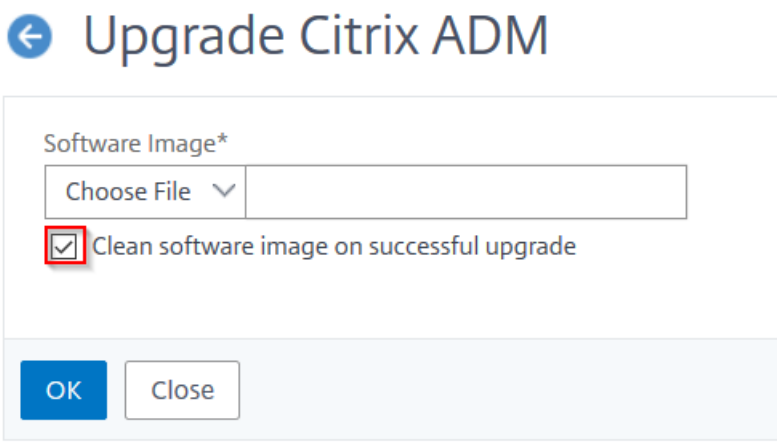
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. ****Navigieren Sie zu** System** > Systemadministrationen. Klicken Sie unter der Unterüberschrift **Systemadministration** auf **Upgrade NetScaler ADM**.



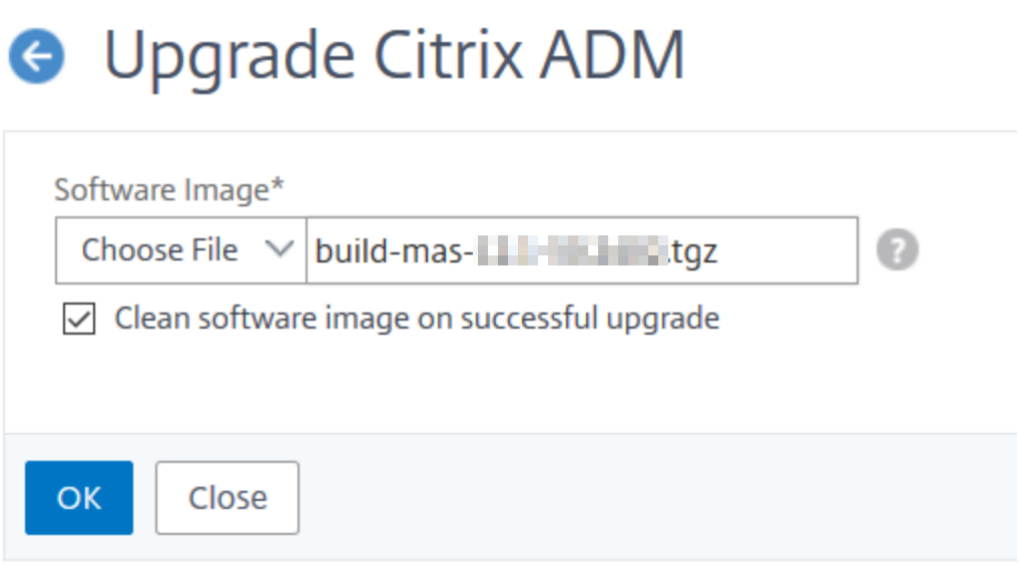
4. Aktivieren Sie auf der Seite**NetScaler ADM aktualisieren**das Kontrollkästchen**Software-Image bei erfolgreichem Upgrade säubern**, um Imagedateien nach dem Upgrade zu löschen. Wenn Sie diese Option auswählen, werden die NetScaler ADM Imagedateien beim Upgrade automatisch entfernt.

> **Hinweis**
>
> Diese Option ist standardmäßig ausgewählt. Wenn Sie dieses Kontrollkästchen vor dem Starten des Upgrade-Vorgangs nicht aktivieren, müssen Sie die Images manuell löschen.



5. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Das Dialogfeld “Bestätigen”wird angezeigt. Klicken Sie auf **OK**.

6. Klicken Sie auf **OK**.

   Der Upgrade-Prozess wird gestartet.

Aktualisieren Sie ein Hochverfügbarkeitspaar von früheren Versionen auf 12.1

Für NetScaler ADM-Server in einem Hochverfügbarkeitsmodus können Sie ein Upgrade durchführen, indem Sie entweder auf die IP-Adresse des aktiven Knotens oder auf die IP-Adresse des virtuellen Lastausgleichsservers zugreifen. Beide NetScaler ADM -Server werden automatisch auf den neuesten Build aktualisiert, sobald Sie den Upgradevorgang auf einem der Server initiieren.

> **Wichtig!**
>
> **Punkte, die beim Upgrade von NetScaler ADM im Hochverfügbarkeitsmodus zu beachten sind**
>
> Beim Upgrade von NetScaler ADM im Hochverfügbarkeitsmodus von einer früheren Version auf 12.1 wird die Hochverfügbarkeitsverbindung intern durch das “join HA”-Skript hergestellt, das auf dem sekundären Knoten ausgeführt wird. Die für den Upgrade-Vorgang benötigte Zeit hängt von der Netzwerkinfrastruktur, den in der Datenbank vorhandenen Daten und der Geschwindigkeit der Verbindung ab. Es kann einige Stunden dauern, bis die Verbindung zwischen den beiden Knoten wiederhergestellt ist. Während dieser Zeit empfängt der primäre Knoten keinen Herzschlag vom sekundären Knoten. Auf der primären Benutzeroberfläche wird eine Benachrichtigung über einen fehlenden Heartbeat angezeigt, bis der Upgrade-Vorgang abgeschlossen ist. Nach Abschluss des Upgrade-Vorgangs wird der sekundäre Knoten neu gestartet und die Hochverfügbarkeitsbereitstellung ist abgeschlossen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Um den Status des Upgrades zu erfahren, melden Sie sich mit SSH bei jedem Knoten an, führen Sie die folgenden Befehle aus und überprüfen Sie die Ausgabe:
>
> pgrep -lf installmas
>
> pgrep -lf maintenance
>
> pgrep -lf join_streaming_replication
>
> pgrep -lf pg_basebackup
>
> Wenn einer dieser Befehle einen laufenden Prozess auf einem der Knoten anzeigt, ist das Upgrade im Gange und sollte nicht unterbrochen werden. Starten Sie NetScaler ADM während dieser Zeit nicht neu oder versuchen Sie nicht, ein Failover auf dem sekundären Knoten zu erzwingen.
>
> Nach Abschluss des Upgrade-Vorgangs können Sie sich manchmal nicht mit nsroot/nsroot oder Ihren Benutzeranmeldeinformationen anmelden. Dies liegt daran, dass das NetScaler ADM-Subsystem nicht vollständig neu gestartet wurde oder die Migration möglicherweise noch läuft. Starten Sie NetScaler ADM nicht neu oder versuchen Sie nicht, das Kennwort wiederherzustellen. Dies könnte unerwünschte Auswirkungen haben und das System könnte sich inkonsistent verhalten. Falls erforderlich, können Sie versuchen, sich mit den Anmeldeinformationen für nsrecover/<your_password_for_the_nsroot_user> anzumelden.
>
> Stellen Sie nach dem Upgrade und vor dem Starten des Betriebs sicher, dass sowohl der primäre als auch der sekundäre Knoten aktualisiert wurden und der Neustart abgeschlossen ist.
>
> **Hinweis:**
>
> Sie können NetScaler ADM nicht im Hochverfügbarkeitsmodus mit der CLI aktualisieren.

Gebündelte Lizenzierung auf NetScaler ADM-Servern mit hoher Verfügbarkeit:

Wenn NetScaler ADM-Server in einem Hochverfügbarkeitsmodus bereitgestellt werden, wird die Lizenzdatei an den primären Knoten angehängt und mit der hostID oder der MAC-Adresse des Primärservers konfiguriert (knotengesperrt). Die Funktion für gepoolte Lizenzen wird jetzt von NetScaler ADM in Hochverfügbarkeit ab Version 12.1 unterstützt. Um die gepoolte Lizenzierungsfunktion auf beiden Knoten zu konfigurieren, müssen Sie auf beiden Knoten identische Lizenzdateien haben. Um eine identische Lizenz auf dem sekundären Knoten zu installieren, müssen Sie die Lizenz auf die hostID (MAC-Adresse) des sekundären Knotens rehosten.

Stellen Sie sich ein Szenario vor, in dem NetScaler ADM zwei Serverknoten S1 und S2 im Hochverfügbarkeitsmodus hat. Die ursprüngliche Lizenzdatei L1 ist auf dem Server S1 installiert. Die neu gehostete Lizenzdatei L2 sollte jetzt S2 zugewiesen werden.

Folgen Sie den Schritten, um NetScaler ADM im Hochverfügbarkeitsmodus von 12.0 auf 12.1 zu aktu-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

alisieren und die Funktion für gepoolte Lizenzen zu konfigurieren:

1. Melden Sie sich im Hochverfügbarkeitsmodus am primären Knoten der NetScaler ADM-Server an und führen Sie den Upgrade-Vorgang durch.
2. Installieren Sie die neu gehostete Lizenzdatei L2 auf dem sekundären Serverknoten S2.

   Zu diesem Zeitpunkt:

   - Wenn S2 der primäre Knoten ist, können Sie die L2-Lizenz installieren, indem Sie auf die GUI dieser Instanz zugreifen.
   - Wenn S2 der sekundäre Knoten ist, müssen Sie manuell einen Failover durchführen, sodass S2 jetzt zum primären Knoten wird. Installieren Sie die Lizenz L2 über die GUI auf dem neuen Primärknoten.
     Dies liegt daran, dass Sie über die GUI nur auf den Primärserver mit hoher Verfügbarkeit zugreifen können.
3. Konfigurieren Sie die Floating-IP auf dem neuen Primärknoten.
4. Löschen Sie die IP-Adressen der Lizenzserver auf den NetScaler ADC-Instanzen und konfigurieren Sie sie neu, um die Floating-IP zu verwenden. Führen Sie dies auf allen NetScaler ADC-Instanzen durch.

Citrix empfiehlt, dass Sie ein Upgrade der gepoolten NetScaler ADM-Hochverfügbarkeitslizenz durchführen, indem Sie ein Wartungsfenster für die NetScaler ADC-Instanzen erstellen. Dies liegt daran, dass das Entfernen des Lizenzservers und das Hinzufügen einer Floating-IP dazu führen, dass die NetScaler ADC-Instanzen vorübergehend zur Unterstützung der Mindestbandbreite zurückkehren.

Upgrade-Szenarien für hohe Verfügbarkeit

Es kann zwei Szenarien geben, in denen die NetScaler ADM-Server im Hochverfügbarkeitsmodus bereitgestellt werden.

- Die primären und sekundären Server werden im selben Subnetz bereitgestellt.
- Der Primär- und der Sekundärserver werden in verschiedenen Subnetzen bereitgestellt.

Dieses Upgrade-Dokument unterstützt Sie beim Upgrade von NetScaler ADM in diesen beiden Szenarien.

- Aktualisierung eines Hochverfügbarkeits-Setups im selben Subnetz
- Aktualisierung eines Hochverfügbarkeits-Setups in verschiedenen Subnetzen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

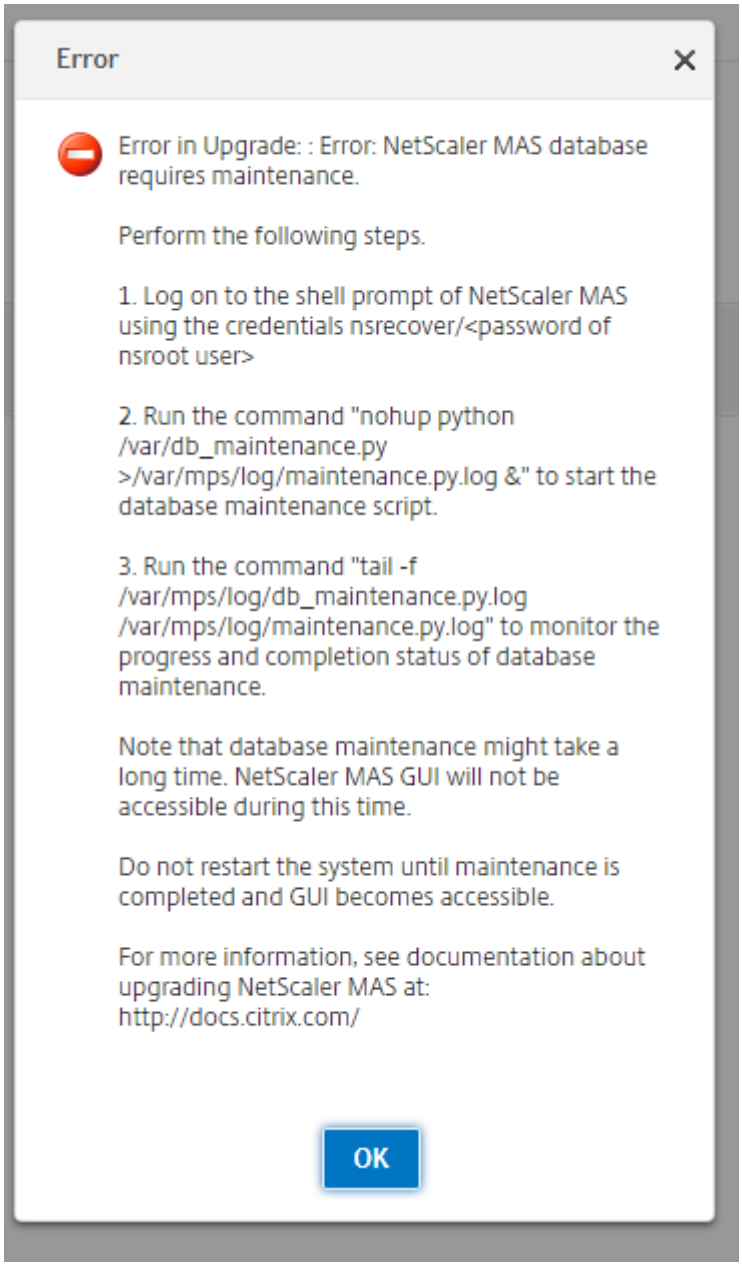
Aktualisieren Sie ein Hochverfügbarkeits-Setup im selben Subnetz

Das Upgrade von NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus im selben Subnetz bereitgestellt werden, wird automatisch von NetScaler ADM 12.1 abgewickelt.

So aktualisieren Sie NetScaler ADM, das im Hochverfügbarkeitsmodus im selben Subnetz bereitgestellt wird:

1. Melden Sie sich beim primären Knoten an und navigieren Sie zu **System** > **Systemadministrationen**.
2. Klicken Sie unter**Systemadministration** auf **Upgrade NetScaler ADM**.
3. Tritt während des Upgrades ein Fehler auf, wird die folgende Fehlermeldung angezeigt. Folgen Sie den Anweisungen in der Meldung auf dem Primärserver.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

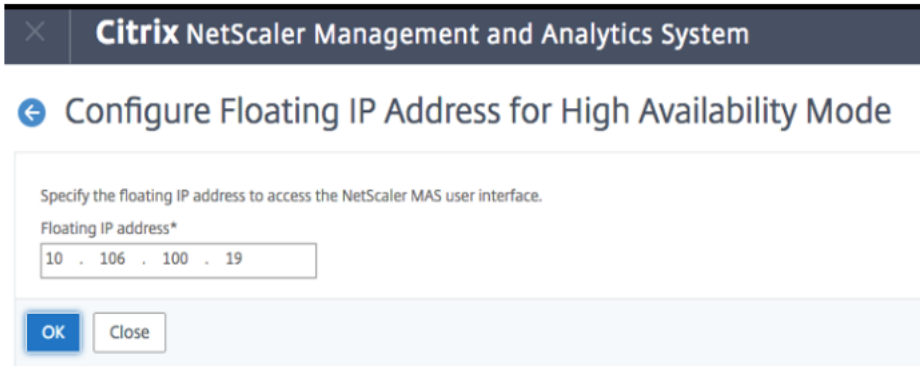


4. Im Rahmen des Upgrade-Vorgangs müssen Sie das Bereinigungsverfahren über die CLI durchführen. Während des Bereinigungsprozesses wird der sekundäre Knoten zum primären Knoten. Auf den alten Primärknoten kann nicht über seine GUI zugegriffen werden. Starten Sie den alten Primärknoten sowie den neuen Primärknoten nicht neu, während der Bereinigungsprozess läuft. Wenn der Bereinigungsprozess abgeschlossen ist, setzen Sie den Upgrade-Vorgang über den neuen primären Knoten fort.
5. Nach Abschluss des Upgrade-Vorgangs müssen die beiden Knoten ihre Datenbanken synchronisieren. Die Zeit, die für die vollständige Synchronisation und das Auftauchen des neuen sekundären Knotens benötigt wird, hängt von den in den Datenbanken vorhandenen Daten ab.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Nach erfolgreichem Upgrade müssen Sie die Floating-IP über die NetScaler ADM-Benutzeroberfläche konfigurieren.

6. Um eine Floating-IP zu konfigurieren, navigieren Sie zu**System > Bereitstellung > Floating-IP-Adresse für den Hochverfügbarkeitsmodus konfigurieren**.
7. Geben Sie die Floating-IP an, wie in der folgenden Abbildung gezeigt, und klicken Sie auf**OK**.



Aktualisieren Sie ein Hochverfügbarkeits-Setup in verschiedenen Subnetzen

Das Upgrade von NetScaler ADM-Servern, die im Hochverfügbarkeitsmodus in verschiedenen Subnetzen bereitgestellt werden, muss von einem Administrator durchgeführt werden.

In diesem Szenario befindet sich der NetScaler ADM HA-Knoten 1 (primär) in Subnetz 1 und der NetScaler ADM HA-Knoten 2 (sekundär) in Subnetz 2.

So aktualisieren Sie NetScaler ADM, das im Hochverfügbarkeitsmodus in verschiedenen Subnetzen bereitgestellt wird:

1. Brechen Sie das Hochverfügbarkeits-Setup manuell ab. Weitere Informationen finden Sie unter Hochverfügbarkeit deaktivieren.
2. Aktualisieren Sie den eigenständigen NetScaler ADM Knoten 1. Weitere Informationen zum Upgrade von NetScaler ADM finden Sie unter Aktualisieren eines einzelnen NetScaler ADM-Servers.
3. Richten Sie einen neuen NetScaler ADM Standalone-Knoten 3 in Subnetz 1 ein und registrieren Sie ihn.
4. Stellen Sie nach der Registrierung von Knoten 1 und Knoten 3 beide Knoten im Hochverfügbarkeitsmodus bereit. Einzelheiten finden Sie unter Bereitstellen des primären und sekundären Knotens als Hochverfügbarkeitspaar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Die Konfiguration der Floating-IP ist obligatorisch.

5. Löschen Sie den NetScaler ADM-Knoten 2.

Aktualisieren Sie ein Hochverfügbarkeitspaar von früheren 12.1-Versionen auf die neueste Version

Sie können NetScaler ADM-Server, die mit hoher Verfügbarkeit bereitgestellt werden, von einem früheren 12.1-Build auf einen späteren 12.1-Build aktualisieren.

So aktualisieren Sie NetScaler ADM, das im Hochverfügbarkeitsmodus bereitgestellt wurde:

1. Laden Sie die NetScaler ADM 12.1 Build 49.37-Image-Datei von der Downloadseite von Citrix.com herunter.
2. Melden Sie sich beim primären Knoten an und navigieren Sie zu **System** > **Systemadministrationen**.
3. Klicken Sie unter Systemadministration auf **Upgrade NetScaler ADM**.
4. Navigieren Sie zu dem Ordner, in dem das Image ist.

   Nehmen Sie während des Upgrades keine Konfigurationsänderungen an einem der Knoten vor.

   > **Warnung**
   >
   > - Aktualisieren Sie den Browser erst, wenn der Upgradevorgang erfolgreich abgeschlossen wurde. Es kann einige Minuten dauern, bis der Upgradevorgang abgeschlossen ist.

   Nach dem Upgrade kann sich der aktive Knoten in einem Hochverfügbarkeitspaar ändern.

Upgrade der Bereitstellung von NetScaler ADM Disaster Recovery

Das Upgrade der NetScaler ADM Disaster Recovery-Bereitstellung erfolgt in zwei Schritten:

Sie müssen zuerst die im Hochverfügbarkeitsmodus konfigurierten NetScaler ADM-Knoten am primären Standort aktualisieren. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie die NetScaler ADM-Server im Hochverfügbarkeitsmodus von älteren Versionen auf 12.1 aktualisieren, finden Sie in diesem Dokument unter Aktualisieren eines Hochverfügbarkeitspaars von früheren Versionen auf 12.1 .
- Wenn Sie mit dem Hochverfügbarkeitspaar ein Upgrade von einem früheren 12.1-Build auf einen späteren 12.1-Build durchführen, finden Sie in diesem Dokument unter Aktualisieren eines Hochverfügbarkeitspaars von früheren 12.1-Versionen auf die neueste Version .

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 den Anmeldeinformationen “nsrecover”auf den Disaster Recovery-Knoten hoch.
3. Melden Sie sich mit den Anmeldeinformationen “nsrecover”am Disaster Recover-Knoten an.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 31 05:41:16 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-mas-12.1-500.113.tgz
```

4. Navigieren Sie zu dem Ordner, in dem Sie die Imagedatei abgelegt haben, und entpacken Sie die Datei.
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.
   - Wenn Sie die NetScaler ADM-Server im Hochverfügbarkeitsmodus von älteren Versionen auf 12.1 aktualisieren, finden Sie in diesem Dokument unter Aktualisieren eines Hochverfügbarkeitspaars von früheren Versionen auf 12.1 .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Wenn Sie mit dem Hochverfügbarkeitspaar ein Upgrade von einem früheren 12.1-Build auf einen späteren 12.1-Build durchführen, finden Sie weitere Informationen unter Aktualisieren eines Hochverfügbarkeitspaars von früheren 12.1-Versionen auf die neueste Version

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 Anmeldeinformationen "nsrecover"auf den Agentknoten hoch.
3. Stellen Sie sicher, dass Sie das richtige Agent-Upgradeimage herunterladen. Der Name der Imagedatei hat das folgende Format:

   build-masagent-12.1-48.18.tgz
4. Melden Sie sich mit den "nsrecover"-Anmeldeinformationen beim On-Premises-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
```

Entfernen Sie die Unterstützung für die erweiterte Backup- und Wiederherstellungsfunktion von NetScaler ADM

Anstatt die erweiterte Backup-Funktion zu verwenden, um ein vollständiges Backup Ihres NetScaler ADM-Servers zu erstellen, können Sie jetzt die neue **Disaster Recovery-Funktion** verwenden, die in NetScaler ADM Version 12.1 verfügbar ist, um ein vollständiges Backup Ihres NetScaler ADM-Hochverfügbarkeits-Setups zu erstellen und bei Anwendungsfällen zur Geschäftskontinuität zu helfen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Wichtig!**
>
> 1. Die erweiterte Backupfunktion ist nach dem Upgrade auf NetScaler ADM 12.1 nicht mehr verfügbar. Informationen zum Entfernen der erweiterten Backup-Funktion und zur Fortsetzung der Backups mit der Notfallwiederherstellung finden Sie unter Backup von NetScaler ADM nach dem Upgrade auf NetScaler ADM 12.1. Disaster Recovery wird nur mit NetScaler ADM HA unterstützt.
> 2. Um weiterhin eine teilweise Backup des NetScaler ADM-Servers zu erstellen, die die Konfigurationsdateien, Instanzdetails, Systemdaten usw. enthält, und dann Ihren NetScaler ADM-Server in einer eigenständigen Bereitstellung (Teilsicherung) wiederherzustellen, finden Sie unter So sichern und wiederherstellen Sie Ihren NetScaler ADM-Server in einer Einzelserverbereitstellung.

Verwenden Sie im Falle eines Notfalls auf dem Primärserver die Disaster Recovery-Funktion, um NetScaler ADM auf demselben Primärserver zu starten und zu konfigurieren, ohne Daten zu verlieren.Die Funktion ist nur auf NetScaler ADM-Servern verfügbar, die in einem Hochverfügbarkeits-Setup ab NetScaler ADM Version 12.1 bereitgestellt wurden.

Sichern Sie Ihren NetScaler ADM-Server nach dem Upgrade auf NetScaler ADM 12.1

Um Ihren NetScaler ADM-Server weiter zu sichern, empfiehlt Citrix Folgendes:

1. Löschen Sie Ihre Remote-Backup-Einstellungen auf NetScaler ADM, indem Sie wie folgt vorgehen:
   a) Navigieren Sie zu **System** > **Systemadministration** > **Erweiterte System-Backup-Einstellungen**.
   b) Wählen Sie auf der Seite “Erweiterte Backup-Einstellungen konfigurieren”die Option **Nein** aus, um Remote-Backups zu deaktivieren.
   c) Klicken Sie auf **Einstellungen anwenden**. Bitte warten Sie, bis Ihr NetScaler ADM-Server neu gestartet wird, und wenden Sie die geänderten Einstellungen an.
   d) Löschen Sie Ihren Remote-Backup-Knoten.
2. Stellen Sie einen neuen NetScaler ADM-Server bereit und konfigurieren Sie ihn. Erstellen Sie ein Hochverfügbarkeits-Setup mit dem vorhandenen NetScaler ADM-Server, der im obigen Schritt neu gestartet wurde.
   - Weitere Informationen zur eigenständigen Bereitstellung von NetScaler ADM finden Sie unterBereitstellen von NetScaler ADM.
   - Weitere Informationen zur NetScaler ADM HA-Bereitstellung finden Sie unterHochverfügbarkeitsbereits

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Konfigurieren Sie Disaster Recovery, um weiterhin Daten zu Backup und wiederherzustellen.Weitere Informationen zur Notfallwiederherstellung findenSie unter Notfallwiederherstellung für hohe Verfügbarkeit konfigurieren.

Zusätzlichen Datenträger zum NetScaler ADM-Server hinzufügen

Wenn Ihre NetScaler ADM-Speicheranforderungen den Standardspeicherplatz (120 Gigabyte) überschreiten, können Sie einen zusätzlichen Datenträger bereitstellen. Sie können zusätzliche Datenträger sowohl in Einzelserver- als auch in Hochverfügbarkeitsbereitstellungen bereitstellen.

Wenn Sie NetScaler ADM von Version 12.0 auf 12.1 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 zusätzlicher Datenträger bleibt im aktualisierten Build dasselbe. 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 dem vorhandenen zusätzlichen Datenträger zu ändern. Weitere Informationen zum Bereitstellen zusätzlicher Datenträger und zum Verwenden des neuen Datenträgerpartitionierungstools finden Sie unter So stellen Sie einen zusätzlichen Datenträger für NetScaler ADM bereit.

NetScaler ADC-Instanzen in OpenStack mit StyleBooks bereitstellen

Ab NetScaler ADM 12.1 Build 49.23 wurde die Architektur des OpenStack-Orchestrierungsworkflows 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-->
```

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

24. Mai 2018

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzer können entweder intern von Citrix Application Delivery Management (ADM), extern von einem Authentifizierungsserver oder von beiden authentifiziert werden. Wenn die lokale Authentifizierung verwendet wird, muss sich der Benutzer in der NetScaler ADM -Sicherheitsdatenbank befinden. Wenn der Benutzer extern authentifiziert wird, sollte der „externe Name“des Benutzers je nach ausgewähltem Authentifizierungsprotokoll mit der externen Benutzeridentität übereinstimmen, die auf dem Authentifizierungsserver registriert ist.

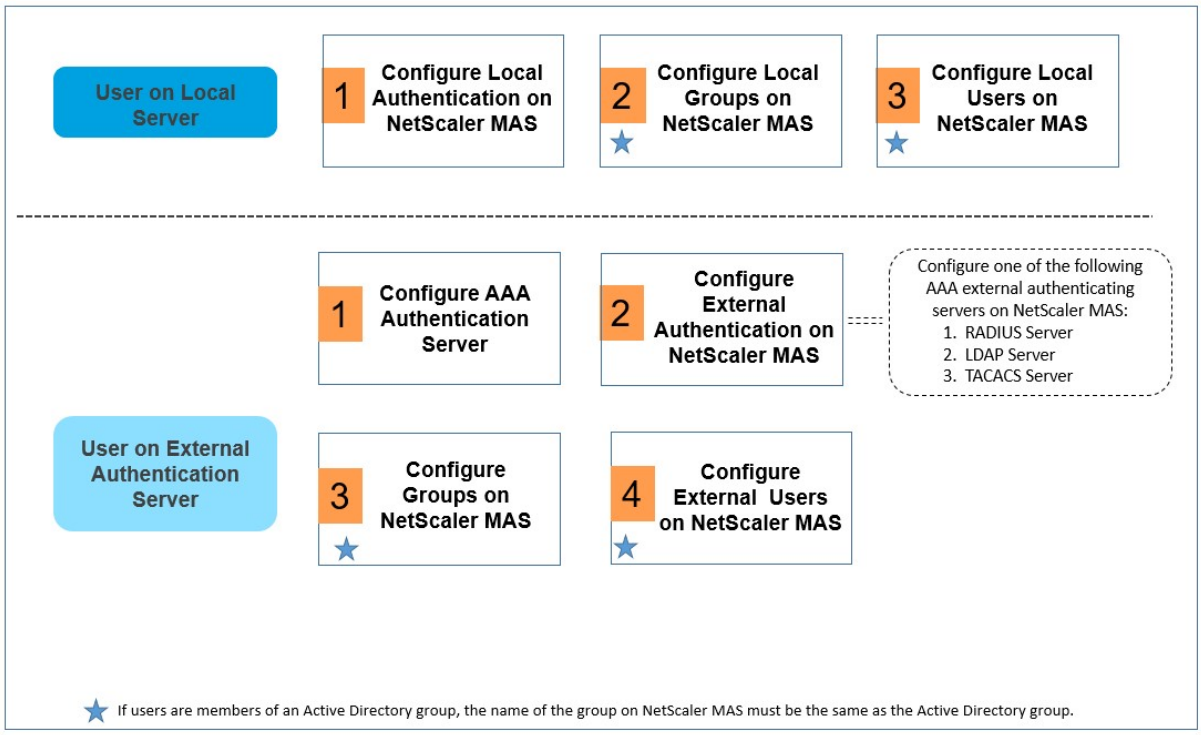
Citrix ADM unterstützt die externe Authentifizierung über RADIUS-, LDAP- und TACACS-Protokolle. Diese einheitliche Unterstützung bietet eine gemeinsame Schnittstelle zur Authentifizierung und Autorisierung aller lokalen und externen AAA-Serverbenutzer (Authentication, Authorization and Accounting), die 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, wird das entsprechende Protokoll verwendet, um den Benutzer in Citrix ADM zu identifizieren.

Sie können Ihre Benutzer in NetScaler ADM auf zwei Arten authentifizieren:

- Mithilfe von lokalen Citrix ADM Servern
- Durch die Verwendung externer Authentifizierungsserver

Das folgende Flussdiagramm zeigt den Arbeitsablauf, den Sie bei der Authentifizierung lokaler oder externer Benutzer befolgen müssen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Externe Authentifizierungsserver konfigurieren

Citrix ADM unterstützt verschiedene Protokolle, um externe Authentifizierungs-, Autorisierungs- und Buchhaltungsdienste (AAA) bereitzustellen.

Citrix ADM sendet alle Serviceanforderungen für Authentifizierung, Autorisierung und Abrechnung (AAA) an den Remote-RADIUS-, LDAP- oder TACACS+-Server. Der Remote-AAA-Server empfängt die Anfrage, validiert die Anfrage und sendet eine Antwort zurück an Citrix ADM. Wenn Citrix ADM für die Verwendung eines Remote-RADIUS-, TACACS+- oder LDAP-Servers für die Authentifizierung konfiguriert ist, wird Citrix ADM zu einem RADIUS-, TACACS+- oder LDAP-Client. In jeder dieser Konfigurationen werden Authentifizierungsdatensätze in der Remotehostserver-Datenbank gespeichert. Anmelde- und Abmeldekontoname, zugewiesene Berechtigungen und Zeitabrechnungsdatensätze werden ebenfalls für jeden Benutzer auf dem AAA-Server gespeichert.

Darüber hinaus 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 Servergruppen für bestimmte Arten der Authentifizierung erstellen. 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 verschiedener Typen in einer Gruppe konfigurieren und die interne Datenbank auch als Fallback-Authentifizierungs-Backup in die konfigurierte Liste der AAA-Server aufnehmen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren Sie einen RADIUS-Authentifizierungsserver

Sie können Citrix ADM so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren RADIUS-Servern authentifiziert wird. Ihre Konfiguration erfordert möglicherweise die Verwendung einer Netzwerkzugriffsserver-IP-Adresse (NAS-IP) oder einer Netzwerkzugriffsserver-ID (NAS-ID). Verwenden Sie bei der Konfiguration von Citrix ADM für die Verwendung eines RADIUS-Authentifizierungsservers die folgenden Richtlinien: Wenn Sie die Verwendung der NAS-IP-Adresse aktivieren, sendet die Appliance ihre konfigurierte IP-Adresse an den RADIUS-Server, anstatt die Quell-IP-Adresse zu senden, die beim Aufbau der RADIUS-Verbindung verwendet wurde.

- Wenn Sie die NAS-ID konfigurieren, sendet die Appliance den Bezeichner an den RADIUS-Server. Wenn Sie die NAS-ID nicht konfigurieren, sendet die Appliance ihren Hostnamen an den RADIUS-Server.
- Wenn Sie die NAS-IP-Adresse aktivieren, ignoriert die Appliance jede konfigurierte NAS-ID und verwendet die NAS-IP für die Kommunikation mit dem RADIUS-Server.

So konfigurieren Sie einen RADIUS-Authentifizierungsserver:

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** > **RADIUS**.
2. Klicken Sie auf der **RADIUS**-Seite auf **Hinzufügen**.
3. Stellen Sie auf der Seite **RADIUS-Server erstellen** die Parameter ein und klicken Sie auf **Erstellen**, um den Server zur Liste der RADIUS-Authentifizierungsserver hinzuzufügen. Die folgenden Parameter sind obligatorisch:

    a) **Name**. Name des RADIUS-Servers.

    b) **Servername/IP-Adresse**. Servername oder IP-Adresse des RADIUS-Servers.

    c) **Port**. Standardmäßig wird Port 1812 für die RADIUS-Authentifizierung verwendet. Sie können bei Bedarf eine andere Portnummer angeben.

    d) **Timeout (Sekunden)**. Zeit in Sekunden, in der das Citrix ADM System auf eine Antwort vom RADIUS-Server wartet.

    e) **Geheimer Schlüssel**. Jeder alphanumerische Ausdruck. Dies ist der Schlüssel, der von Citrix ADM und dem RADIUS-Server gemeinsam genutzt wird, um die Kommunikation zu ermöglichen.

4. Klicken Sie auf **Details**, um den Abschnitt zu erweitern und die zusätzlichen Parameter festzulegen, und klicken Sie dann auf **Erstellen**.

Weitere Informationen zum Hinzufügen von RADIUS-Servern finden Sie unter [Hinzufügen von RADIUS-Authentifizierungsservern].(/en-us/netscaler-application-delivery-management-software/12-1/authentication/authentication-how-to-articles/add-radius-authentication-server.html)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren Sie einen LDAP-Authentifizierungsserver

Sie können Citrix ADM so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren LDAP-Servern authentifiziert wird. Die LDAP-Autorisierung erfordert identische Gruppennamen in Active Directory, auf dem LDAP-Server und auf Citrix ADM. Die Zeichen und der Fall müssen ebenfalls übereinstimmen.

So konfigurieren Sie einen LDAP-Authentifizierungsserver:

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** > **LDAP** .
2. Klicken Sie auf der Seite **LDAP** auf **Hinzufügen**.
3. Stellen Sie auf der Seite **LDAP-Server erstellen** die Parameter ein und klicken Sie auf **Erstellen** , um den Server zur Liste der LDAP-Authentifizierungsserver hinzuzufügen. Die folgenden Parameter sind obligatorisch:

    a) **Name**. Name des LDAP-Servers.

    b) **Servername/IP-Adresse**. Servername oder IP-Adresse des LDAP-Servers.

    c) **Sicherheitstyp**. Art der erforderlichen Kommunikation zwischen dem System und dem LDAP-Server. Wählen Sie aus der Dropdownliste aus. Wenn die Klartextkommunikation nicht ausreicht, können Sie die verschlüsselte Kommunikation wählen, indem Sie entweder Transport Layer Security (TLS) oder SSL auswählen.

    d) **Port**. Standardmäßig wird Port 389 für die LDAP-Authentifizierung verwendet. Sie können bei Bedarf eine andere Portnummer angeben.

    e) **Servertyp**. Wählen Sie **Active Directory (AD)** oder **Novell Directory Service (NDS)** als LDAP-Servertyp aus.

    f) **Timeout (Sekunden).** Zeit in Sekunden, für die das Citrix ADM System auf eine Antwort vom LDAP-Server wartet.

Sie können zusätzliche Informationen angeben. Sie können das LDAP-Zertifikat auch validieren, indem Sie das Kontrollkästchen **LDAP-Zertifikat validieren** aktivieren und den Hostnamen angeben, der in das Zertifikat eingegeben werden soll. Einige der zusätzlichen Parameter, die Sie hinzufügen können, sind Domain Nameserver (DN) -Details für Abfragen an einen Verzeichnisdienst, Standardauthentifizierungsgruppe, Gruppenattribute und andere Attribute.

Der Basis-DN wird normalerweise vom Bind-DN abgeleitet, indem der Benutzername entfernt und die Gruppe angegeben wird, zu der die Benutzer gehören. Geben Sie im Textfeld Administrator Bind DN den Administrator-Bind-DN für Abfragen an das LDAP-Verzeichnis ein.

Beispiele für die Syntax für Basis-DN sind:

- ou=user, dc=ace, dc=com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- cn=Benutzer, dc=ace, dc=com

Beispiele für die Syntax für Bind DN sind:

- Domäne/Nutzername
- ou=administrator, dc=ace, dc=com
- user@domain.name (für Active Directory)
- cn=Administrator, cn=Benutzer, dc=ace, dc=com

Der Gruppenname und der Name der Benutzer, die Sie in Citrix ADM definieren, müssen denen ähneln, die auf dem LDAP-Server konfiguriert sind.

> **Hinweis**
>
> Bei der Konfiguration eines RADIUS- oder LDAP-Servers können Sie im Abschnitt **Details** den Namen einer **Standardauthentifizierungsgruppe eingeben**. Diese Standardgruppe wird ausgewählt, um den Benutzer zu autorisieren, wenn die Authentifizierung erfolgreich ist, unabhängig davon, ob der Benutzer an eine Gruppe gebunden ist oder nicht. Der Benutzer erhält dann eine Kombination von Berechtigungen, die für diese Standardgruppe und die anderen Gruppen konfiguriert sind, unabhängig davon, ob der Benutzer der Gruppe zugewiesen ist oder nicht.

Weitere Informationen zum Hinzufügen von LDAP-Servern finden Sie unter Hinzufügen von LDAP-Authentifizierungsservern .

Weitere Informationen zur Kaskadierung externer Authentifizierungsserver finden Sie unter So kaskadieren Sie externe Authentifizierungsserver.

Konfigurieren Sie einen TACACS-Authentifizierungsserver

TACACS verwaltet wie RADIUS und LDAP Fernauthentifizierungsdienste für den Netzwerkzugriff.

Konfigurieren Sie einen TACACS-Authentifizierungsserver:

1. Navigieren Sie in **Citrix ADM** zu **System** > **Authentifizierung** > **TACACS** .
2. Klicken Sie auf der **TACACS** -Seite auf **Hinzufügen** .
3. **Geben Sie auf der Seite „ TACACS-Server** erstellen “die folgenden Details ein:
    a) Name des TACACS-Servers
    b) IP-Adresse des TACACS-Servers
    c) Port und Timeout (in Sekunden)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

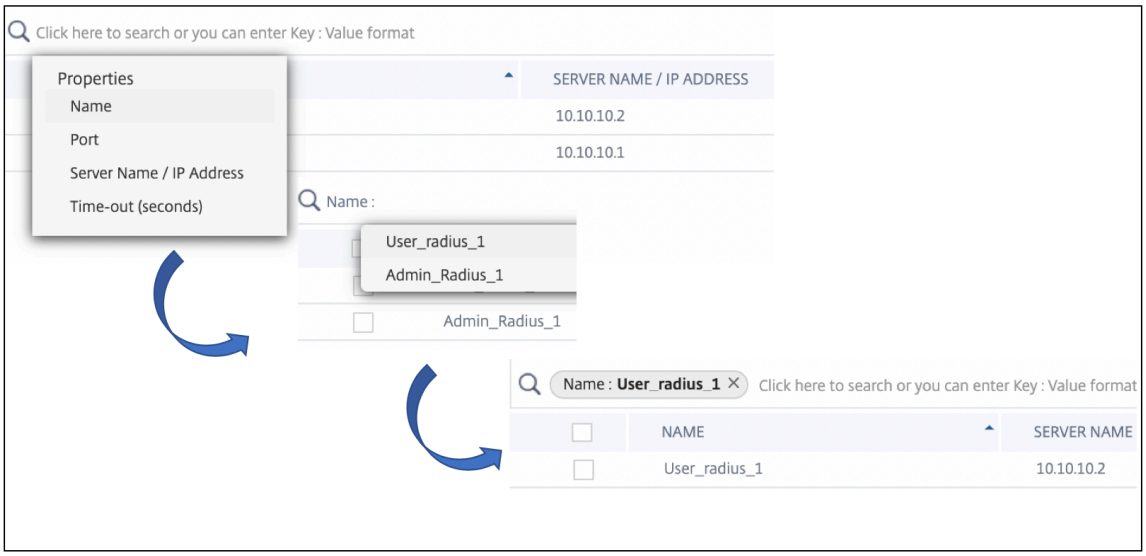
d) Der Schlüssel, der vom System und dem TACACS-Server für die Kommunikation gemeinsam genutzt wird.

e) Wählen Sie Accounting aus, wenn die Appliance Auditinformationen auf dem TACACS-Server protokollieren soll.

4. Klicken Sie auf **Erstellen**.

Weitere Informationen zum Hinzufügen von TACACS-Servern finden Sie unter Hinzufügen von TACACS-Authentifizierungsservern .

> **Hinweis**
>
> Um nach Authentifizierungsservern zu suchen, die in Citrix ADM hinzugefügt wurden, klicken Sie in die Suchleiste und wählen Sie die erforderlichen Suchkriterien aus.



Konfigurieren Sie eine lokale Authentifizierung von Benutzern in Citrix ADM

Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen Sie sie dann zu Gruppen hinzu, die Sie in Citrix ADM erstellen. Nach der Konfiguration von Benutzern und Gruppen können Sie Autorisierungs- und Sitzungsrichtlinien anwenden, Lesezeichen erstellen, Anwendungen angeben und die IP-Adresse von Dateifreigaben und Servern angeben, auf die Benutzer Zugriff haben.

So konfigurieren Sie eine lokale Authentifizierung in Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** und klicken **Sie auf**Authentifizierungskonfigurat
.

2. Wählen Sie auf der Seite **Authentifizierungskonfiguration** im Dropdownfeld **Servertyp** die Option **LOCAL** aus und klicken Sie auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurieren Sie eine externe Authentifizierung in Citrix ADM

Wenn Sie externe Authentifizierungsserver in Citrix ADM konfigurieren, werden die Benutzergruppen, die auf diesen externen Servern authentifiziert sind, in Citrix ADM importiert. Sie müssen keine Benutzer auf Citrix ADM erstellen. Die Benutzer werden auf den externen Servern von Citrix ADM verwaltet. Sie müssen jedoch sicherstellen, dass die Berechtigungsstufen der Benutzergruppen auf den externen Authentifizierungsservern in Citrix ADM beibehalten werden. Citrix ADM führt die Autorisierung von Benutzern durch, indem Gruppenberechtigungen für den Zugriff auf bestimmte virtuelle Lastausgleichsserver und auf bestimmte Anwendungen auf dem System zugewiesen werden. Wenn ein Authentifizierungsserver später aus dem System entfernt wird, werden die Gruppen und Benutzer automatisch aus dem System entfernt.

So konfigurieren Sie eine externe Authentifizierung in Citrix ADM:

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** und klicken Sie auf **Authentifizierungskonfiguration**.
2. Wählen Sie auf der Seite **Authentifizierungskonfiguration** in der Dropdownliste **Servertyp** die Option **EXTERNAL** aus.
3. Klicken Sie auf **Einfügen**.
4. Wählen Sie auf der Seite **Externe Server** einen Authentifizierungsserver aus. Optional können Sie mehrere Authentifizierungsserver für die Kaskadierung auswählen.

   > **Hinweis**
   >
   > Nur externe Server können kaskadiert werden.

5. Wählen Sie **Lokale Fallback-Authentifizierung** aktivieren , wenn die lokale Authentifizierung übernommen werden soll, wenn die externe Authentifizierung fehlschlägt.
6. Klicken Sie auf **OK**, um die Seite zu schließen.

   Die ausgewählten Server werden auf der **Seite Authentifizierungsserver**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.

Konfigurieren Sie Gruppen 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 „Admin“- oder „Nur lesen“-Rechte haben und alle Benutzer in dieser Gruppe erhalten die gleichen Berechtigungen.

In Citrix ADM ist eine Gruppe als eine Sammlung von Benutzern mit ähnlichen Berechtigungen definiert. Eine Gruppe kann eine oder mehrere Rollen haben. Ein Benutzer ist als eine Entität

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Nachdem Sie Gruppen konfiguriert haben, können Sie Autorisierungs- und Sitzungsrichtlinien anwenden, Lesezeichen erstellen, Anwendungen angeben und die IP-Adressen von Dateifreigaben und Servern angeben, auf die der Benutzer Zugriff hat.

Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen Sie sie zu Gruppen hinzu, die auf Citrix ADM konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppen.

> **Hinweis**
>
> Wenn die Benutzer Mitglieder einer Active Directory-Gruppe sind, müssen der Name der Gruppe und die Namen der Benutzer in Citrix ADM mit denen in der Active Directory-Gruppe übereinstimmen.

So konfigurieren Sie Benutzergruppen in Citrix ADM:

1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf der Seite **Gruppen** auf **Hinzufügen** , um eine Gruppe zu erstellen. Standardmäßig werden zwei Gruppen in Citrix ADM erstellt, wobei die Berechtigungen auf admin und schreibgeschützt festgelegt sind. Sie können Ihre Benutzer zu diesen Gruppen hinzufügen oder andere Gruppen für Ihre Benutzer erstellen.
3. Geben Sie auf der Seite **Systemgruppe erstellen** auf der Registerkarte **Gruppeneinstellungen** den Namen der Gruppe ein und legen Sie **Rollen** entweder auf admin oder schreibgeschützt fest. Sie können **Benutzersitzungstimeout konfigurieren** auswählen, um ein Timeoutlimit für die Benutzersitzungen festzulegen, die für diese Gruppe angemeldet sind.

   > **Hinweis**
   >
   > Stellen Sie sicher, dass der Name der auf Citrix ADM erstellten Benutzergruppe mit dem auf den externen Authentifizierungsservern identisch ist. Andernfalls erkennt das System die Gruppe nicht und die Gruppenmitglieder werden nicht in das System extrahiert.

4. Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die erforderlichen Gruppen aus. Klicken Sie auf **Gruppe erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Wählen Sie auf der Registerkarte **Benutzer zuweisen** die Benutzer aus, die Sie der Gruppe hinzufügen möchten. Die Benutzer werden dieser Tabelle hinzugefügt, wenn Sie Benutzer in Configure Users in Citrix ADM konfigurieren .
6. Klicken Sie auf **Fertig stellen**.

Wenn Sie mit der Erstellung einer Gruppe im System fertig sind, werden alle Benutzer auf dem externen Authentifizierungsserver in das System extrahiert. Wenn der Gruppenname mit dem Gruppennamen auf dem externen Authentifizierungsserver übereinstimmt, erbt der Benutzer alle Autorisierungsdefinitionen, wenn er am System angemeldet ist.

Benutzer in Citrix ADM konfigurieren

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. Wenn Sie Benutzer lokal authentifizieren, die auf externen Authentifizierungsservern vorhanden sind, stellen Sie sicher, dass dieselben Benutzer sowohl auf den Authentifizierungsservern als auch auf Citrix ADM vorhanden sind.

So konfigurieren Sie Benutzer in NetScaler ADM:

1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Benutzer**.
2. Klicken Sie auf der Seite **Benutzer** auf **Hinzufügen**, um Benutzer zu Citrix ADM hinzuzufügen.
3. Stellen Sie auf der Seite **Systembenutzer erstellen** die folgenden Parameter ein:
    a) **Nutzername**. Name des Benutzers
    b) **Kennwort**. Kennwort, mit dem sich der Benutzer bei Citrix ADM anmeldet
    c) **Aktivieren Sie die externe Authentifizierung**. Wenn dies nicht aktiviert ist, wird der Benutzer als lokaler Benutzer authentifiziert.
    d) **Konfigurieren Sie das Timeout**für Benutzersitzungen . Zeit, für die ein Benutzer aktiv bleiben kann. Dieser Zeitraum kann in Minuten oder Stunden festgelegt werden.
4. Wählen Sie in der Tabelle **Gruppen** die Gruppe aus, zu der Sie den Benutzer hinzufügen möchten. Die Gruppenmitglieder werden dieser Tabelle hinzugefügt, wenn Sie Gruppen unter Konfigurieren von Benutzergruppen in Citrix ADM konfigurieren.
5. Klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Wenn sich die Benutzer in Active Directory befinden, stellen Sie sicher, dass der Gruppenname

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> in Citrix ADM mit dem für die Active Directory-Gruppe auf dem externen Server übereinstimmt.

Extrahieren einer Authentifizierungsservergruppe

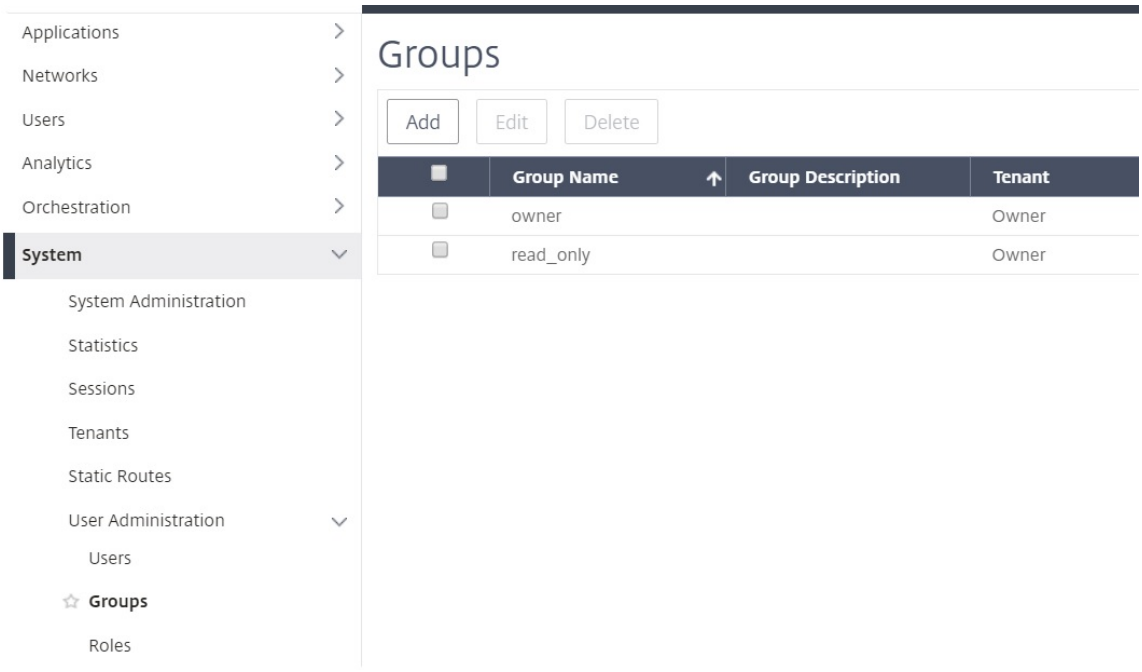
February 5, 2024

Mit Citrix Application Delivery Management (ADM) können Sie die Benutzergruppe extrahieren, die auf dem externen Authentifizierungsserver vorhanden ist, und ihnen je nach Rolle und gemäß den Citrix ADC-Definitionen Berechtigungen zuweisen. Das hat zwei Vorteile:

1. Sie müssen keine Benutzer auf Citrix ADM erstellen. Obwohl die Gruppen in den Citrix ADM-Server extrahiert werden, werden sie auf den externen Servern vom Citrix ADM verwaltet, anstatt sie dem System hinzuzufügen.
2. 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. Wenn der jeweilige Authentifizierungsserver in Zukunft aus dem System entfernt wird, werden die Gruppen und Benutzer automatisch aus dem System entfernt.

Gruppen konfigurieren und Gruppenberechtigungen zuweisen

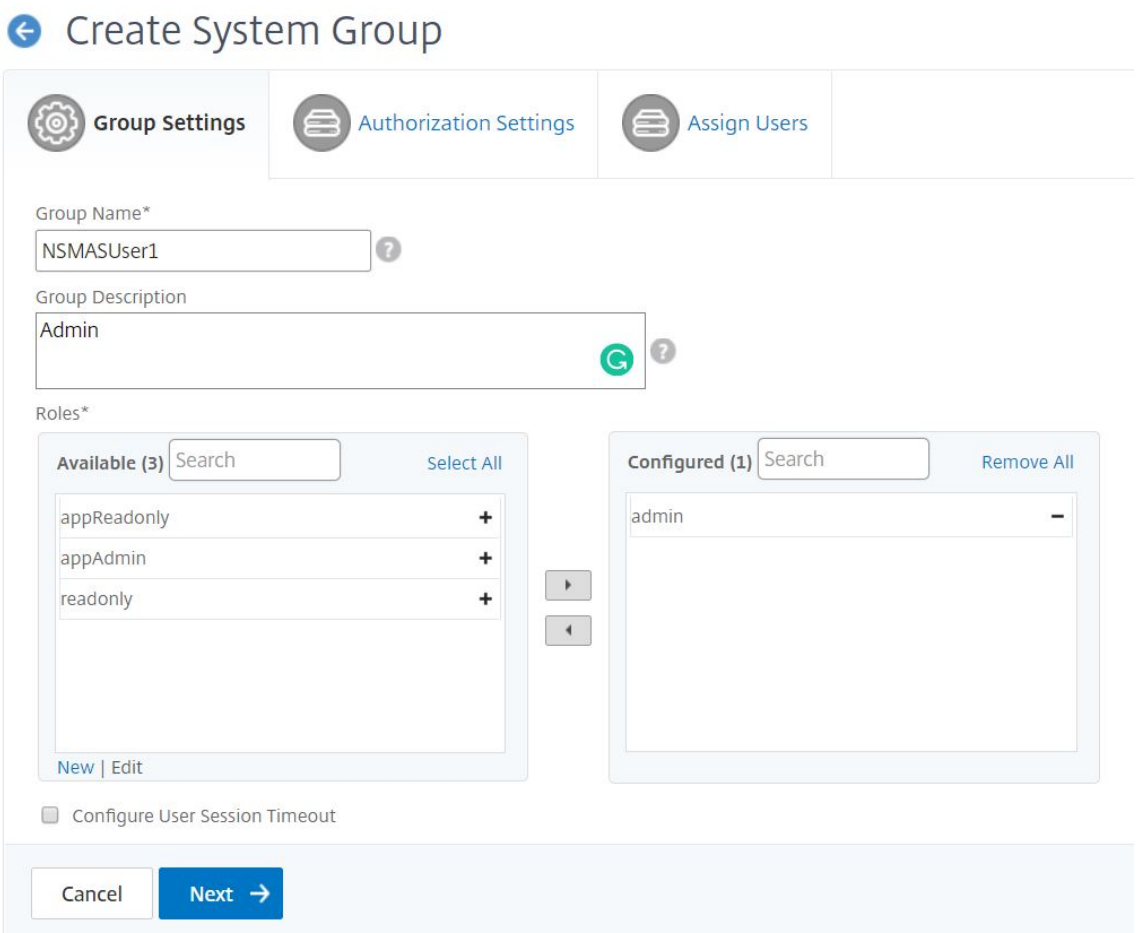
1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf **Hinzufügen**, um eine Gruppe zu erstellen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Geben Sie auf der Registerkarte **Gruppeneinstellungen** den Namen der Gruppe ein und legen Sie die Berechtigungen auf admin, readonly, appReadOnly oder appAdmin fest. Die anderen Optionen, die Sie konfigurieren können, sind das Sitzungs-Timeout, mit dem Sie ein Timeout-Limit für die angemeldeten Sitzungen der Benutzer dieser Gruppe festlegen können, und Sie können auch die VM-Instanzen festlegen, auf die die Gruppenmitglieder zugreifen können.

> **Hinweis**
>
> Stellen Sie sicher, dass der Name der auf Citrix ADM erstellten Benutzergruppe genau mit dem Namen übereinstimmt, der auf externen Authentifizierungsservern erstellt wurde. Andernfalls erkennt das System die Gruppe nicht und die Gruppenmitglieder werden nicht in das System extrahiert.



4. Auf der Registerkarte **Autorisierungseinstellungen** können Sie Autorisierungseinstellungen für die folgenden vier Gruppen angeben:

   - Instanzen
   - Anwendungen
   - Konfigurationsvorlagen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

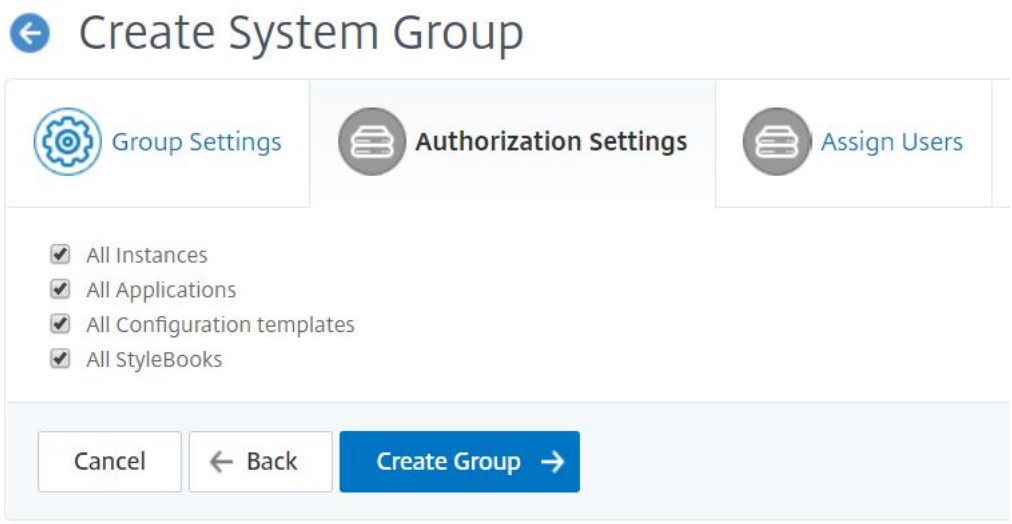
- StyleBooks

Standardmäßig kann Ihr Benutzer auf alle oben genannten Gruppen zugreifen. Sie können die Kontrollkästchen deaktivieren und für jede dieser Gruppen selektiven Zugriff gewähren.

Beispiel:

- Sie können das Kontrollkästchen**Instanzen** deaktivieren und nur die erforderlichen Instanzen auswählen, auf die Sie Ihren Benutzern Zugriff gewähren möchten.
- Deaktivieren Sie das Kontrollkästchen**Alle Anwendungen** und wählen Sie nur die erforderlichen Anwendungen und Vorlagen aus. Wenn Sie Anwendungen zu einer Gruppe in Citrix ADM hinzufügen, können Sie Regex verwenden, um die Anwendungen zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Die Benutzer, die an diese Gruppen gebunden sind, können nur auf diese spezifischen Anwendungen zugreifen. Der angegebene Regex-Ausdruck wird in NetScaler ADM beibehalten. Das heißt, Citrix ADM ermöglicht, dass die im Textfeld**Add Regular Expression** angegebene Regex im System gespeichert wird, und aktualisiert den Autorisierungsbereich dynamisch, wenn neue Anwendungen diesen Regex-Ausdruck erfüllen. Wenn dem System neue Anwendungen hinzugefügt werden, wendet Citrix ADM die Suchkriterien auf die neuen Anwendungen an, und die Anwendung, die die Kriterien erfüllt, wird der Gruppe dynamisch hinzugefügt. Sie müssen die neuen Anwendungen nicht manuell zur Gruppe hinzufügen. Die Anwendungen werden dynamisch im System aktualisiert, und die jeweiligen Gruppenbenutzer können die Anwendungen unter entsprechenden Modulen in NetScaler ADM sehen.
- Deaktivieren Sie das Kontrollkästchen**Alle Konfigurationsvorlagen** , um nur auf die erforderlichen Vorlagen zuzugreifen.
- Deaktivieren Sie das Kontrollkästchen**Alle StyleBooks** und wählen Sie die erforderlichen StyleBooks aus, auf die Ihr Benutzer zugreifen kann.
- 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. Die Konfigurationspakete dieses StyleBook sind auch in dem enthalten, worauf der Benutzer Zugriff hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wenn Sie die Erstellung einer Gruppe im System abgeschlossen haben, werden alle Benutzer auf dem externen Authentifizierungsserver in das System extrahiert. Sie können dies überprüfen, indem Sie die Gruppe auswählen und auf **Bearbeiten**klicken. In der Tabelle Benutzer unter Systemgruppe erstellen wird die Liste der Benutzer angezeigt, die mit der Gruppe verbunden sind. Sie können der Gruppe auch Benutzer auf der Registerkarte**Benutzer zuweisen zuweisen** .

Wenn der Gruppenname mit dem Gruppennamen auf dem externen Authentifizierungsserver übereinstimmt, erbt der Benutzer alle Autorisierungsdefinitionen, wenn er am System angemeldet ist.

LDAP-Authentifizierungsserver hinzufügen

February 5, 2024

Wenn Sie das LDAP-Protokoll in RADIUS- und TACAS-Authentifizierungsserver integrieren, können Sie Citrix 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

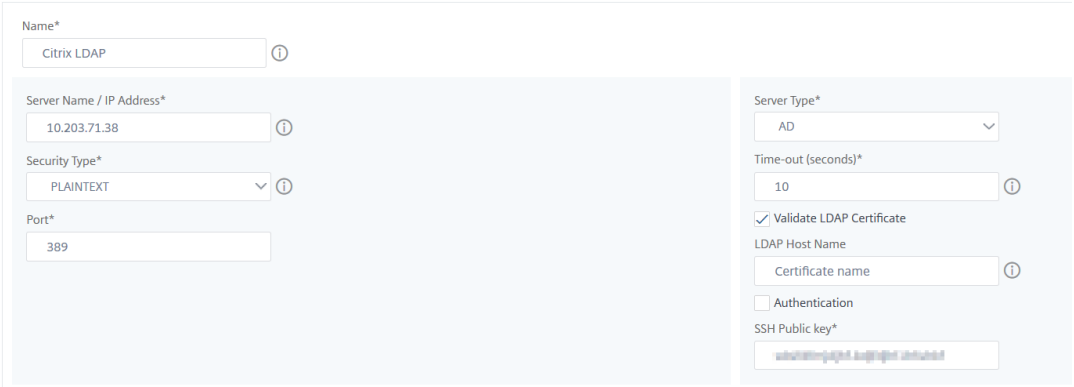
d) **Port** —Standardmäßig wird Port 389 für PLAINTEXT verwendet. Sie können auch Port 636 für SSL/TSL angeben

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 die Liste der öffentlichen Schlüssel abrufen, die auf dem Benutzerobjekt gespeichert sind. Diese öffentlichen Schlüssel werden über SSH auf dem LDAP-Server gespeichert.



Geben Sie unter Verbindungseinstellungen die folgenden Parameter an:

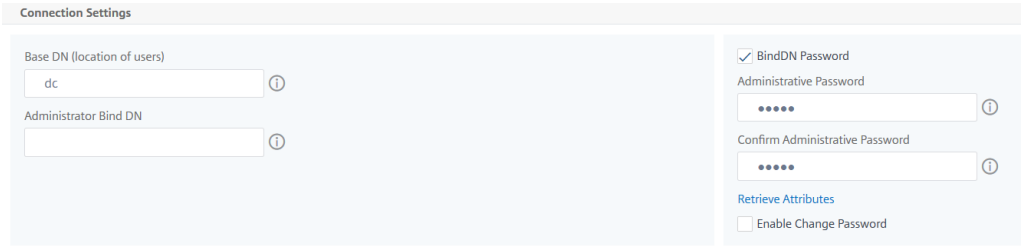
i. **Basis-DN** —Der Basisknoten für den LDAP-Server, um die Suche zu starten

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Geben Sie unter **Andere Einstellungen**die folgenden Parameter an

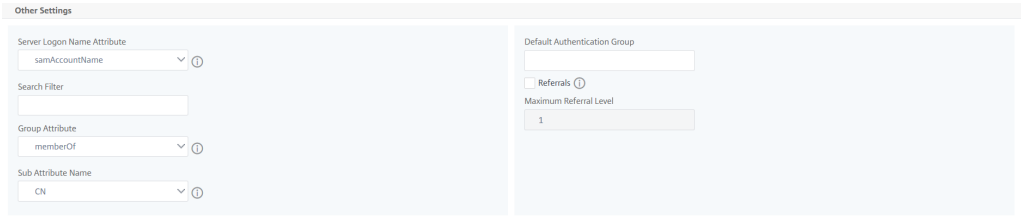
i. **Server-Anmeldenamensattribut** —Namensattribut, das vom System verwendet wird, um den externen LDAP-Server oder ein Active Directory abzufragen. Wählen Sie **samAccountname** aus der Liste aus.

ii. **Suchfilter** —Konfigurieren Sie externe Benutzer für die Zwei-Faktor-Authentifizierung gemäß dem im LDAP-Server konfigurierten Suchfilter. Zum Beispiel würde vpnallowed=true mit dem ldaploginamen samaccount und dem vom Benutzer angegebenen Benutzernamen bob eine LDAP-Suchzeichenfolge von: ergeben. `&(vpnallowed=true)(samaccount=bob)`

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aktivieren der lokalen Fallback-Authentifizierung

February 5, 2024

Die lokale Fallback-Authentifizierung ermöglicht es, die lokale Authentifizierung zu übernehmen, wenn die externe Authentifizierung fehlschlägt. Ein Benutzer, der sowohl in Citrix Application Delivery Management (ADM) als auch auf einem externen Authentifizierungsserver konfiguriert ist, kann sich bei Citrix ADM anmelden, obwohl der konfigurierte externe Authentifizierungsserver ausgefallen oder nicht erreichbar ist. Damit die lokale Fallback-Authentifizierung funktioniert, stellen Sie sicher, dass die folgenden drei Faktoren erfüllt sind:

- Sie sollten auch nach einem Ausfall des externen Authentifizierungsservers auf Citrix ADM zugreifen können.
- Sie sollten sowohl auf Citrix ADM als auch auf dem externen Authentifizierungsserver konfiguriert sein.
- Sie sollten mindestens einen externen Server hinzufügen.

Gehen Sie wie folgt vor, um die lokale Fallback-Authentifizierung zu aktivieren:

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** und klicken **Sie auf**Authentifizierungskonfigurat
   .
2. Wählen Sie in der Liste Servertyp die Option **EXTERN** aus.

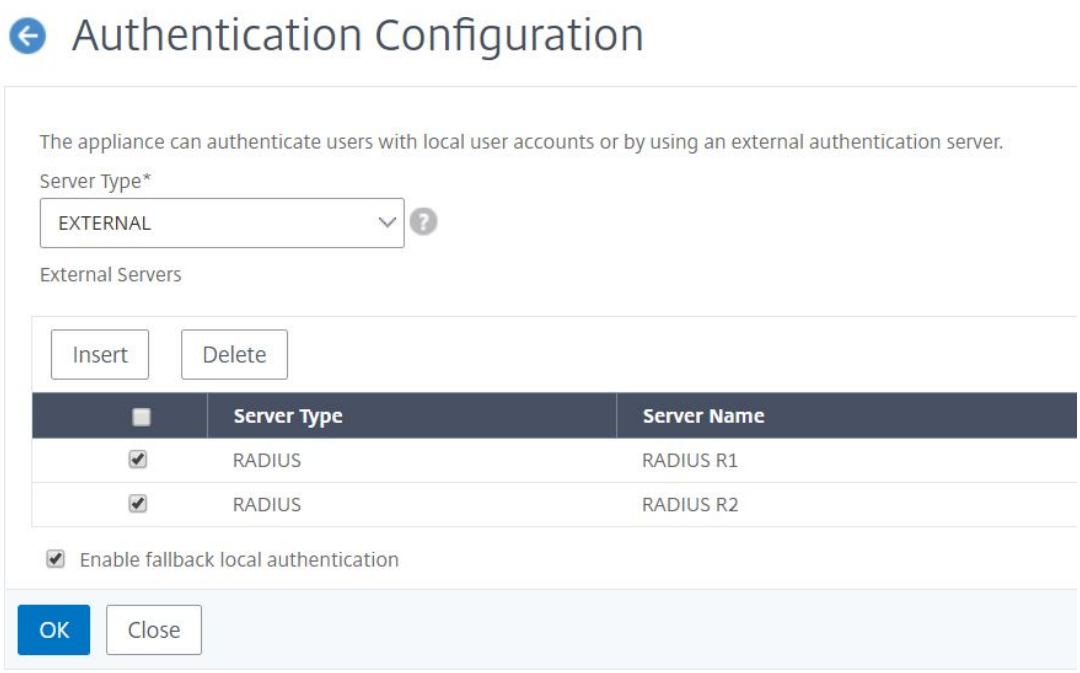
   > **Hinweis**: Wenn Sie **LOCAL** aus der Liste auswählen, erfolgt die Authentifizierung der Benutzer auf dem lokalen Standardauthentifizierungsserver.

3. Klicken Sie auf **Einfügen,** wählen Sie einen externen Server aus der angezeigten Liste der externen Server aus und klicken Sie auf **OK**, um den externen Server hinzuzufügen.

   > **Hinweis** Sie sollten die externen Server bereits vor diesem Schritt hinzugefügt haben, damit sie in der Liste angezeigt werden. Weitere Informationen zum Hinzufügen externer Server finden Sie in den folgenden Artikeln:
   >
   > - So fügen Sie Radius-Server hinzu
   > - So fügen Sie LDAP-Server hinzu
   > - So fügen Sie TACACS-Server hinzu

4. Wählen Sie die Option **Lokale Fallback-Authentifizierung aktivieren** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hinzufügen von RADIUS-Authentifizierungsservern

February 5, 2024

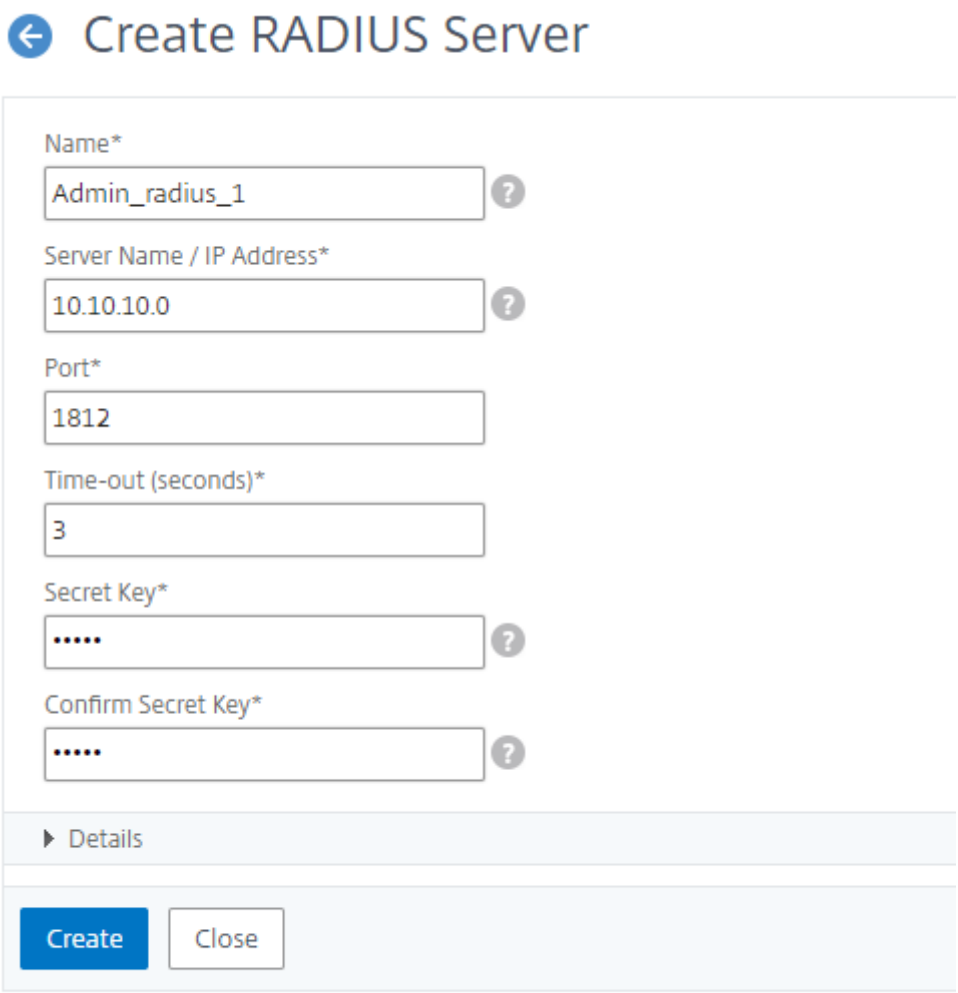
Ein RADIUS-Authentifizierungsserver arbeitet mit dem User Datagram Protocol (UDP). Der RADIUS-Server empfängt die Verbindungsanforderung eines Benutzers und authentifiziert den Benutzer. Der Server gibt dann die Konfigurationsinformationen an das System zurück, das Dienste für den Benutzer bereitstellt. Der RADIUS-Server ist mit einem Netzwerkzugriffsserver (NAS) verbunden. Wenn das NAS eine Zugriffsanforderung sendet, durchsucht der RADIUS-Server seine Datenbank nach dem Benutzernamen und anderen Details. Wenn der Benutzername nicht in der Datenbank vorhanden ist, sendet der RADIUS-Server sofort eine Access-Reject-Nachricht, oder er kann ein Standardprofil auf Citrix ADM laden. In RADIUS sind Authentifizierung und Autorisierung miteinander gekoppelt. Wenn die Benutzerdetails authentifiziert sind, gibt der RADIUS-Server eine Access-Accept-Antwort zurück. Es sendet auch eine Liste von Attribut-Wert-Paaren, die die Parameter beschreiben, die für diese bestimmte Sitzung verwendet werden sollen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfiguration eines RADIUS-Authentifizierungsservers

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** > **RADIUS**.
2. Klicken Sie auf der **RADIUS**-Seite auf **Hinzufügen**.
3. Legen Sie auf der Seite „ **RADIUS-Server erstellen** “die Parameter fest und klicken Sie auf **Erstellen** , um den Server zur Liste der RADIUS-Authentifizierungsserver hinzuzufügen.
4. Die folgenden Parameter sind für die Erstellung des RADIUS-Servers erforderlich:
   - **Name**—geben Sie den Namen des RADIUS-Servers ein
   - **Servername/IP-Adresse**—geben Sie den Servernamen oder die IP-Adresse des RADIUS-Servers ein
   - **Port**—Standardmäßig wird Port 1812 für RADIUS-Authentifizierungsnachrichten verwendet. Sie können bei Bedarf eine andere Portnummer angeben.
   - **Timeout (Sekunden)**—geben Sie die Anzahl der Sekunden ein. Die Zeit, zu der das Citrix ADM System auf eine Antwort vom RADIUS-Server wartet.
   - **Geheimer Schlüssel**—geben Sie einen beliebigen alphanumerischen Ausdruck ein. Der Schlüssel, der zwischen dem Citrix ADM und dem RADIUS-Server für die Kommunikation gemeinsam genutzt wird.
5. Klicken Sie auf **Details**, um den Abschnitt zu erweitern und die zusätzlichen Parameter festzulegen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



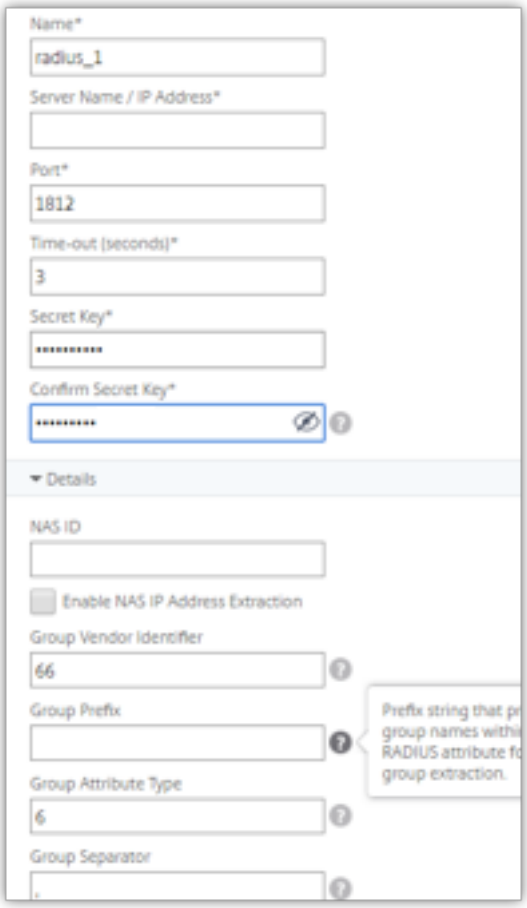
Sie können beim Hinzufügen eines RADIUS-Servers weitere optionale Details angeben. Einige der zusätzlichen Parameter, die Sie eingeben können, sind NAS-Details, Herstellerinformationen, Attributinformationen und die Art der Kennwortauthentifizierung.

> **Hinweis**
>
> Damit die RADIUS-Authentifizierung funktioniert, stellen Sie sicher, dass die auf Citrix ADM konfigurierte Gruppe und die über den RADIUS-Benutzer extrahierte Gruppe identisch sind. Der Benutzer wird auf der Grundlage der der Gruppe zugewiesenen Berechtigungen autorisiert.
>
> Stellen Sie sich zum Beispiel ein Szenario auf dem FreeRADIUS-Server vor, in dem
>
> - Klartext-Kennwort = „1.citrix“
> - Group-Names = „radiusgroup1, group1”

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In diesem Fall gehört der Benutzer zu zwei Gruppen - radiusgroup1 und group1. Das Gruppentrennzeichen lautet in diesem Fall „,“

Wenn Sie sich bei Citrix ADM als RADIUS-Benutzer „RadiusUser1”anmelden, der zur Gruppe „radiusgroup1”gehört, stellen Sie sicher, dass derselbe Gruppenname „radiusgroup1”auch auf Citrix ADM konfiguriert ist.



Geben Sie die Details zur Anbieter-ID, zum Attributtyp und zum Gruppentrennzeichen (falls zutreffend) an, damit die Gruppenextraktion wie in der folgenden Abbildung gezeigt erfolgt.

```
#
# Created for Citrix Use

# currently only using attribute 6 in this setup.

VENDOR Citrix 66


BEGIN-VENDOR Citrix
ATTRIBUTE Group-Names 6 string
END-VENDOR Citrix
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinzufügen von TACACS-Authentifizierungsservern

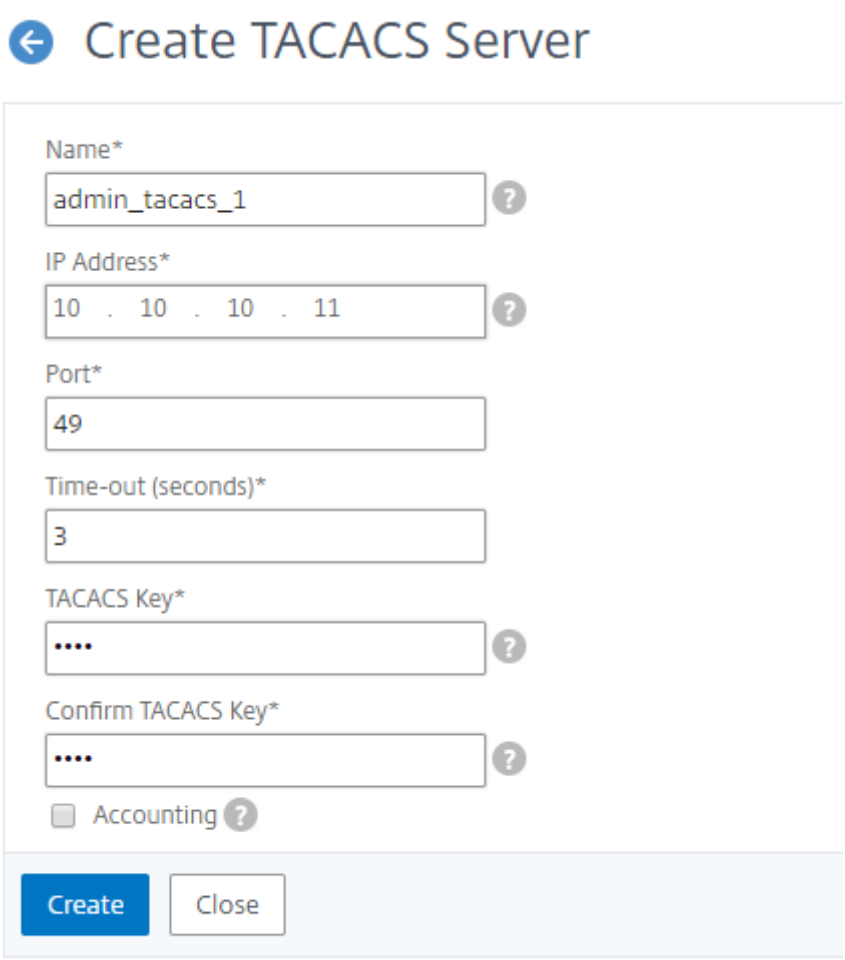
February 5, 2024

TACACS verwaltet zusammen mit RADIUS und LDAP Fernauthentifizierungsdienste für den Netzwerkzugriff.

Konfiguration eines TACACS-Authentifizierungsservers

1. Navigieren Sie in **Citrix ADM** zu **System** > **Authentifizierung** > **TACACS** .
2. Klicken Sie auf der **TACACS**-Seite auf **Hinzufügen** .
3. **Geben Sie auf der Seite „ TACACS-Server** erstellen ‘‘die folgenden Details ein:
    a) Name des TACACS-Servers
    b) IP-Adresse des TACACS-Servers
    c) Port und Timeout in Sekunden
    d) Geben Sie den Schlüssel ein, der vom System und dem TACACS-Server für die Kommunikation gemeinsam genutzt wird.
4. Wählen Sie **Accounting** , wenn die Appliance Auditinformationen mit dem TACACS-Server protokollieren soll.
5. Klicken Sie auf **Erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Kaskadieren externer Authentifizierungsserver

February 5, 2024

Ein Citrix Application Delivery Management (ADM) unterstützt ein einheitliches System von Authentifizierungs-, Autorisierungs- und Abrechnungsprotokollen (AAA), einschließlich RADIUS, LDAP und TACACS, und unterstützt zusätzlich lokale Server für die Authentifizierung lokaler Benutzer und Gruppen. Die einheitliche Unterstützung bietet eine gemeinsame Schnittstelle zur Authentifizierung und Autorisierung aller lokalen 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

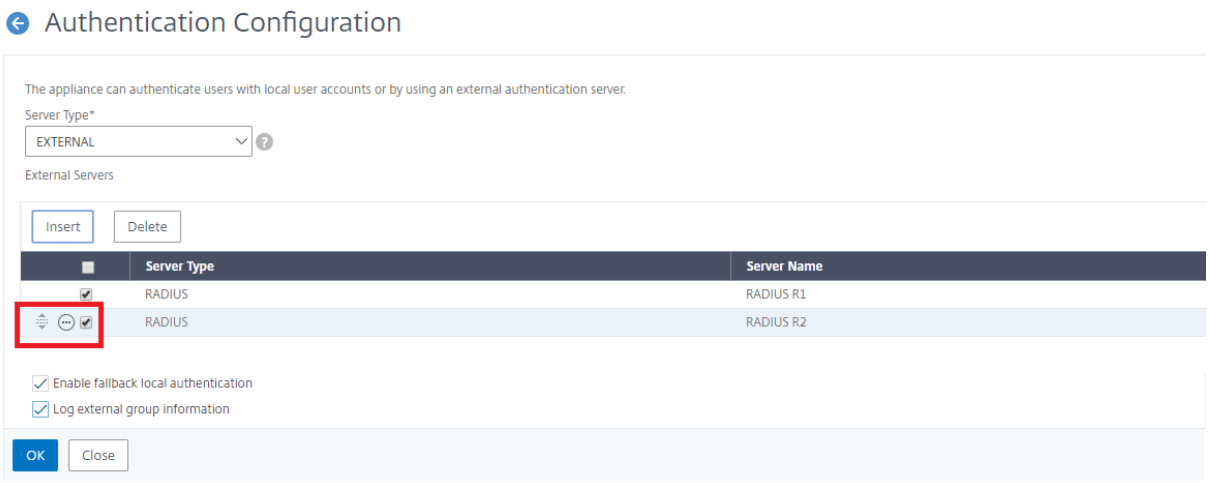
zur Authentifizierung und Autorisierung externer Benutzer. Wenn die Authentifizierung auf dem ersten Authentifizierungsserver fehlschlägt, versucht NetScaler ADM, den Benutzer mithilfe des zweiten externen Authentifizierungsservers zu authentifizieren usw. Um die kaskadierende Authentifizierung zu aktivieren, müssen Sie die externen Authentifizierungsserver zu Citrix ADM hinzufügen. Sie können jeden Typ der unterstützten externen Authentifizierungsserver (RADIUS, LDAP und TACACS) hinzufügen. Wenn Sie beispielsweise vier externe Authentifizierungsserver für die kaskadierende Authentifizierung hinzufügen möchten, können Sie zwei RADIUS-Server, einen LDAP-Server und einen TACACS-Server hinzufügen, oder alle Server können vom Typ RADIUS sein. Sie können bis zu 32 externe Authentifizierungsserver in NetScaler ADM konfigurieren.

Konfiguration von kaskadierenden externen Authentifizierungsservern

1. Navigieren Sie in Citrix ADM zu **System** > **Authentifizierung** .
2. Klicken Sie auf **der**Seite **Authentifizierung** auf Authentifizierungskonfiguration .
3. Wählen Sie auf der Seite **Authentifizierungskonfiguration** in der Dropdownliste **Servertyp** die Option **EXTERN** 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 Sie kaskadieren möchten.
5. Wählen Sie **Lokale Fallback-Authentifizierung** aktivieren , wenn die lokale Authentifizierung übernommen werden soll, wenn die externe Authentifizierung fehlschlägt.
6. Klicken Sie auf **OK**, um die Seite zu schließen.

Die ausgewählten Server werden unter Externe Server angezeigt, wie in der Abbildung unten dargestellt.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 als Teil des Prozesses der allerersten 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 mithilfe der RADIUS-, LDAP- und TACACS-Protokolle. 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 des Benutzers ausgeführt werden, tun dürfen. Auf diese Weise versucht die Zugriffskontrolle, Aktivitäten zu verhindern, die zu einer Sicherheitsverletzung führen könnten. 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 Application Delivery Management (ADM) bietet eine detaillierte, rollenbasierte Zugriffskontrolle (RBAC), mit der Sie Zugriffsberechtigungen auf der Grundlage der Rollen einzelner Benutzer in Ihrem Unternehmen gewähren können. In diesem Zusammenhang ist der Zugriff die Möglichkeit, eine bestimmte Aufgabe auszuführen, z. B. eine Datei anzuzeigen, zu erstellen, zu ändern oder zu löschen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Rollen werden entsprechend der Autorität und Verantwortlichkeit der Benutzer innerhalb des Unternehmens definiert. Ein Benutzer kann beispielsweise alle Netzwerkvorgänge ausführen, während ein anderer Benutzer den Datenverkehr in Anwendungen beobachten und bei der Erstellung von Konfigurationsvorlagen unterstützen 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 Citrix ADM ist das Erstellen von Rollen und Richtlinien spezifisch für die RBAC-Funktion in Citrix ADC. Rollen und Richtlinien können einfach erstellt, geändert oder eingestellt werden, wenn sich die Anforderungen des Unternehmens entwickeln, ohne dass die Berechtigungen für jeden Benutzer individuell aktualisiert werden müssen.

Rollen können feature- oder ressourcenbasiert sein. Stellen Sie sich beispielsweise einen SSL-/Sicherheitsadministrator und einen Anwendungsadministrator vor. Ein SSL/Sicherheitsadministrator muss vollständigen Zugriff auf die Verwaltungs- und Überwachungsfunktionen von SSL-Zertifikaten haben, sollte jedoch schreibgeschützten Zugriff für Systemverwaltungsvorgänge haben. Ein Anwendungsadministrator sollte nur auf die Ressourcen zugreifen können, die in seinem Zuständigkeitsbereich liegen.

Beispiel:

Chris, der Leiter der ADC-Gruppe, ist der Superadministrator von NetScaler ADM in seiner Organisation. Er erstellt drei Administratorrollen: Sicherheitsadministrator, Anwendungsadministrator und Netzwerkadministrator.

David, der Sicherheitsadministrator, muss vollständigen Zugriff auf die Verwaltung und Überwachung von SSL-Zertifikaten haben, sollte aber schreibgeschützten Zugriff für Systemverwaltungsvorgänge haben.

Steve, ein Anwendungsadministrator, benötigt nur Zugriff auf bestimmte Anwendungen und nur bestimmte Konfigurationsvorlagen.

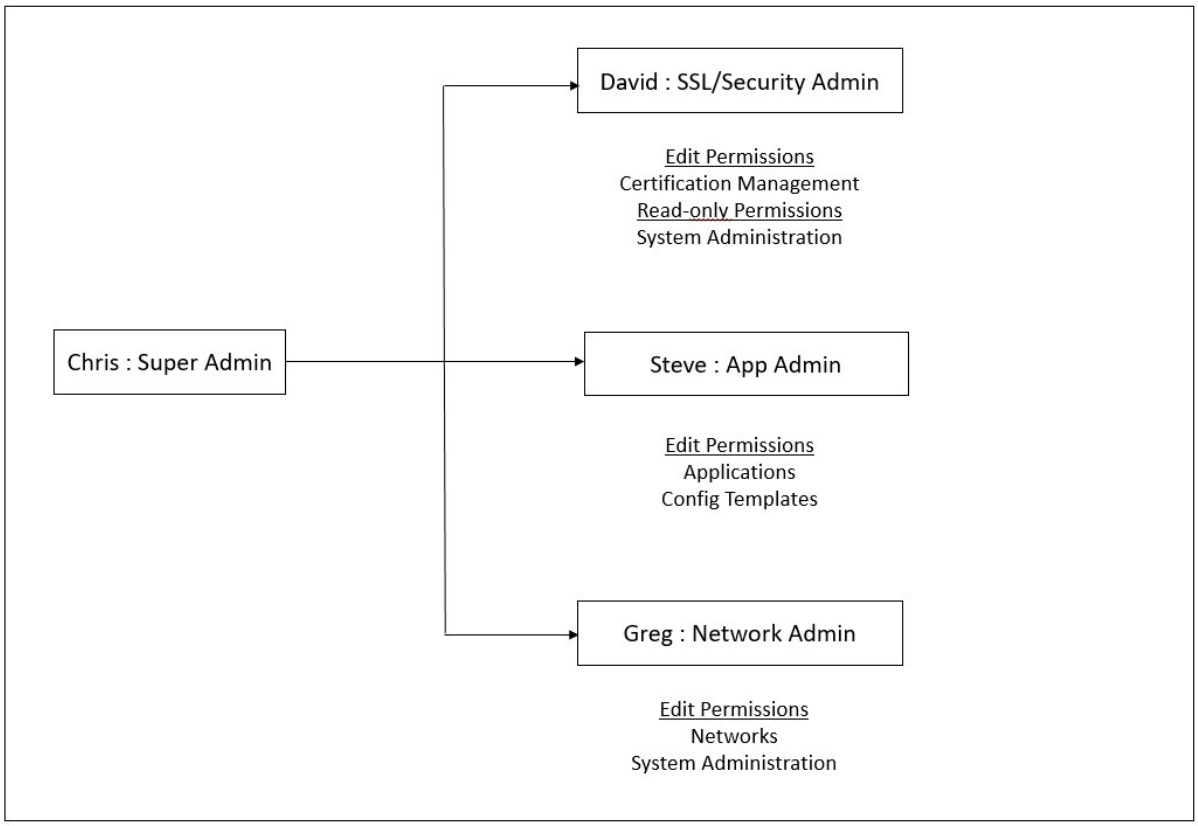
Greg, ein Netzwerkadministrator, benötigt Zugriff auf System- und Netzwerkadministration.

Chris muss außerdem RBAC für alle Benutzer bereitstellen, unabhängig davon, ob es sich um lokale, externe oder mandantenfähige Benutzer handelt.

NetScaler ADM Benutzer 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **StyleBooks** —RBAC wird für StyleBooks nicht vollständig unterstützt.
  - In Citrix ADM werden StyleBooks und Konfigurationspakete als separate Ressourcen betrachtet. Zugriffsberechtigungen (Anzeigen, Bearbeiten oder beides) können für StyleBook und Konfigurationspakete separat oder gleichzeitig bereitgestellt werden. Eine Berechtigung zum Anzeigen oder Bearbeiten von Konfigurationspaketen erlaubt dem Benutzer implizit, die StyleBooks anzuzeigen, was für das Abrufen der configpack-Details und das Erstellen neuer Konfigurationspakete unerlässlich ist.
  - Die Zugriffsberechtigung für bestimmte StyleBooks oder Konfigurationspakete wird nicht unterstützt.
    Beispiel: Wenn die Instanz bereits ein configpack enthält, können Benutzer die Konfiguration auf einer Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis** Die vordefinierten Richtlinien können nicht bearbeitet werden.

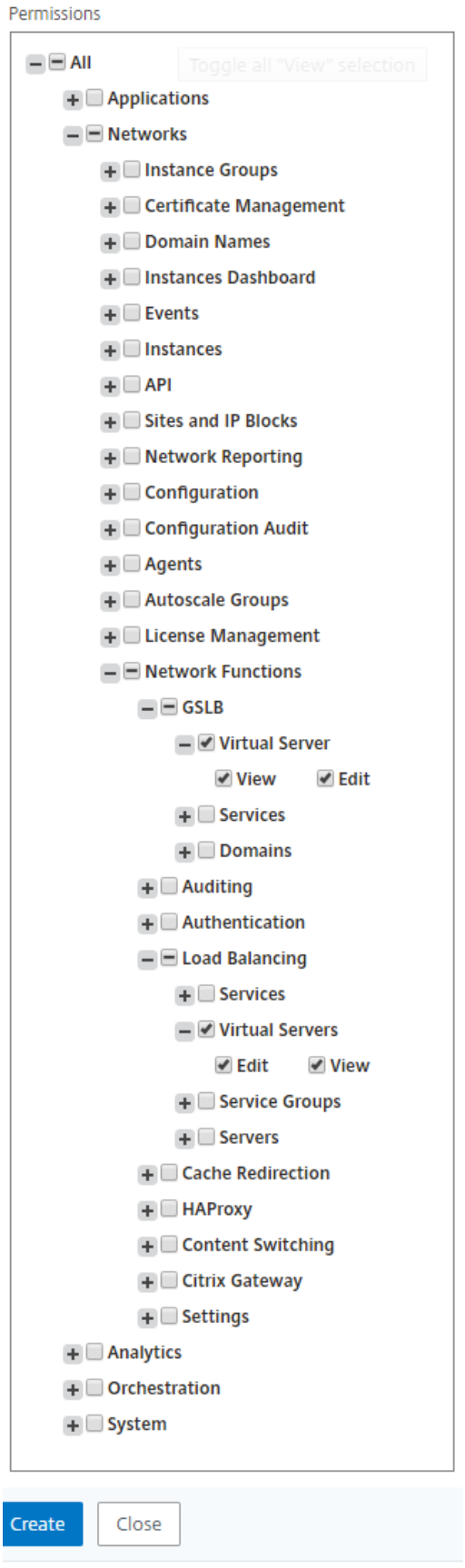
Sie können auch Ihre eigenen (benutzerdefinierten) Richtlinien erstellen.

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.
4. Im Abschnitt **Berechtigungen** werden alle Citrix ADM-Funktionen mit Optionen zum Angeben von Schreibschutz- oder Bearbeitungszugriff aufgeführt. Klicken Sie auf das Symbol (+), um jede Feature-Gruppe in mehrere Features zu erweitern. Sie müssen das Kontrollkästchen neben dem Funktionsnamen aktivieren, um den Benutzern entweder die Berechtigungen zum Anzeigen oder Bearbeiten zu erteilen. Die Option Bearbeiten beinhaltet die Berechtigung zum Anzeigen. Wählen Sie **Anzeigen** für schreibgeschützten Zugriff oder **Bearbeiten** für vollen Zugriff.

   > **Hinweis** Erweitern Sie Load Balancing und GSLB, um weitere Konfigurationsoptionen anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



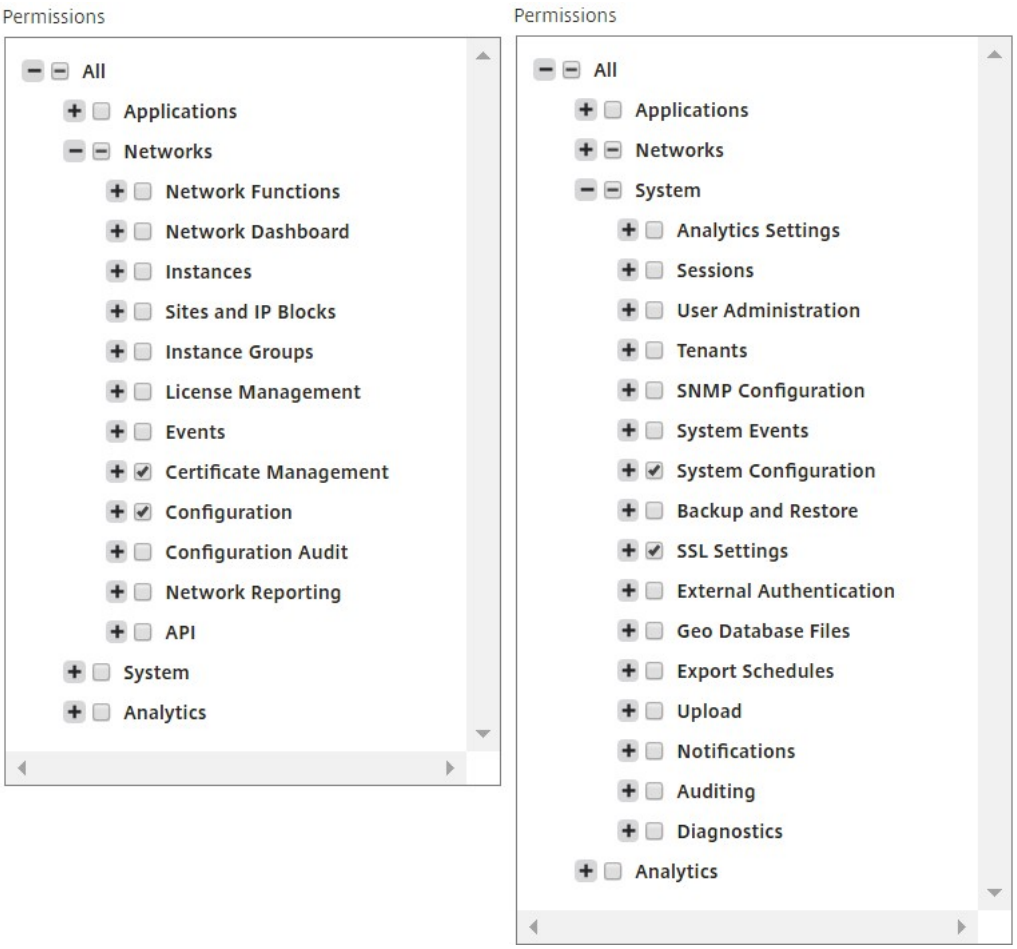
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**: Wenn Sie **Bearbeiten** auswählen, werden möglicherweise intern abhängige Berechtigungen zugewiesen, die im Abschnitt **Berechtigungen** nicht als aktiviert angezeigt werden. Wenn Sie beispielsweise Bearbeitungsberechtigungen für die Fehlerverwaltung aktivieren, stellt NetScaler ADM intern die Berechtigung zum Konfigurieren eines E-Mail-Profils oder zum Erstellen von SMTP-Serverkonfigurationen bereit, damit der Benutzer den Bericht als E-Mail senden kann.

Beispiel:

David ist der Administrator für SSL-Zertifikatsverwaltung/Sicherheit in Citrix ADM. In der David zugewiesenen Richtlinie aktiviert der Administrator die folgenden Kontrollkästchen im Abschnitt **Berechtigungen**:

- **Networks** > **Configuration** > **Edit**
- **Networks** > **Certificate Management** > **Edit**
- **System** > **SSL Settings** > **Edit**
- **System** > **System Configuration** > **Edit**



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Klicken Sie auf **Erstellen**.

Gruppen konfigurieren

February 5, 2024

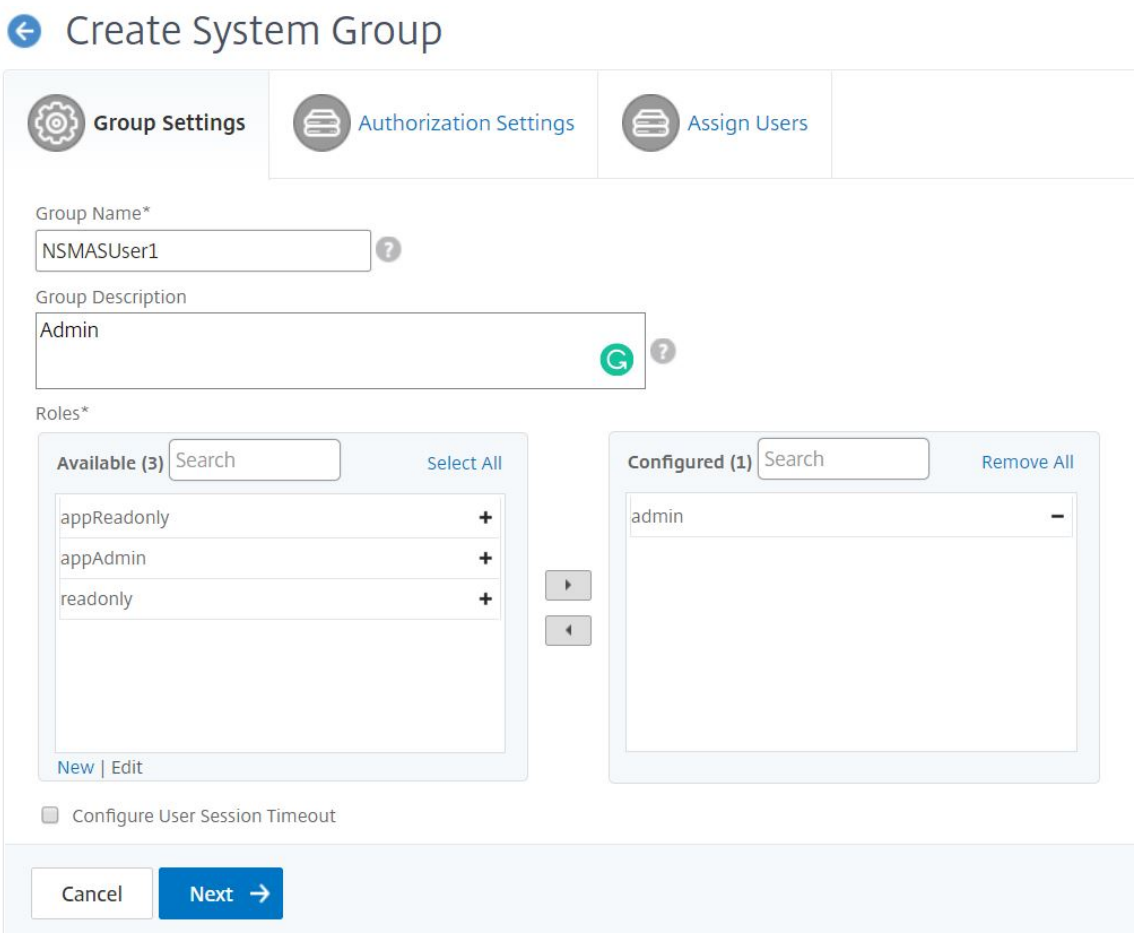
In Citrix Application Delivery Management (ADM) kann eine Gruppe sowohl auf Feature- als auch auf Ressourcenebene zugreifen. Beispielsweise hat eine Benutzergruppe möglicherweise nur Zugriff auf ausgewählte Citrix ADC-Instanzen, eine andere Gruppe nur auf einige ausgewählte Anwendungen usw. Wenn Sie 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.

Um Benutzergruppen zu erstellen und Benutzergruppen Rollen zuzuweisen:

1. Navigieren Sie in NetScaler ADM zu **System** > **Benutzerverwaltung** > **Gruppen**.
2. Klicken Sie auf **Hinzufügen**.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Sie können eine neue Rolle erstellen, indem Sie auf**Neu**klicken , oder Sie können zu**System** >**Benutzerverwaltung**>**Benutzer** navigieren und von diesem Bildschirm aus neue Benutzer erstellen.

6. Klicken Sie auf **Weiter**. Auf der Registerkarte **Autorisierungseinstellungen** können Sie Autorisierungseinstellungen für die folgenden vier Gruppen angeben:

   - Instanzen
   - Anwendungen
   - Konfigurationsvorlagen
   - StyleBooks

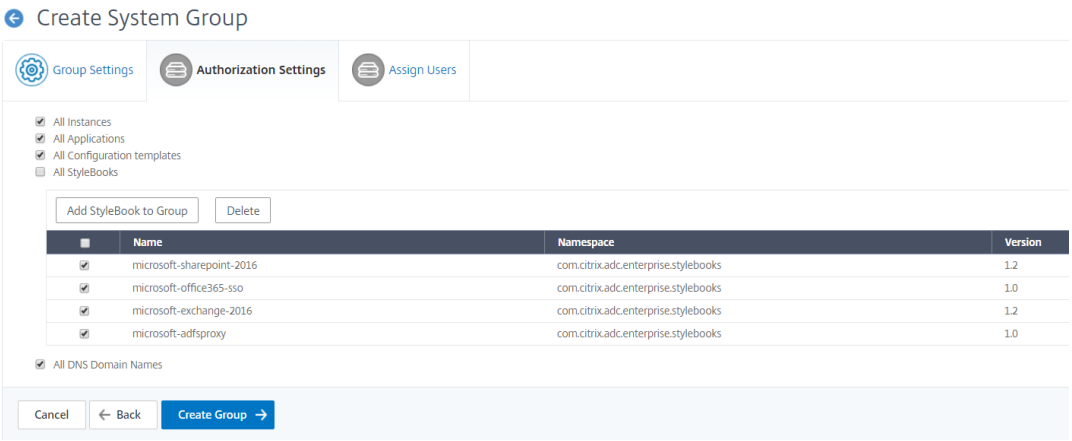
   Standardmäßig kann Ihr Benutzer auf alle oben genannten Gruppen zugreifen. Sie können die Kontrollkästchen deaktivieren und für jede dieser Gruppen selektiven Zugriff gewähren.

   Beispiel:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Sie können das Kontrollkästchen**Instanzen** deaktivieren und nur die erforderlichen Instanzen auswählen, auf die Sie Ihren Benutzern Zugriff gewähren möchten.
- Deaktivieren Sie das Kontrollkästchen**Alle Anwendungen** und wählen Sie nur die erforderlichen Anwendungen und Vorlagen aus. Wenn Sie Anwendungen zu einer Gruppe in Citrix ADM hinzufügen, können Sie Regex verwenden, um die Anwendungen zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Die Benutzer, die an diese Gruppen gebunden sind, können nur auf diese spezifischen Anwendungen zugreifen. Der angegebene Regex-Ausdruck wird in NetScaler ADM beibehalten. Das heißt, Citrix ADM ermöglicht, dass die im Textfeld**Add Regular Expression** angegebene Regex im System gespeichert wird, und aktualisiert den Autorisierungsbereich dynamisch, wenn neue Anwendungen diesen Regex-Ausdruck erfüllen. Wenn dem System neue Anwendungen hinzugefügt werden, wendet Citrix ADM die Suchkriterien auf die neuen Anwendungen an, und die Anwendung, die die Kriterien erfüllt, wird der Gruppe dynamisch hinzugefügt. Sie müssen die neuen Anwendungen nicht manuell zur Gruppe hinzufügen. Die Anwendungen werden dynamisch im System aktualisiert, und die jeweiligen Gruppenbenutzer können die Anwendungen unter entsprechenden Modulen in NetScaler ADM sehen.
- Deaktivieren Sie das Kontrollkästchen**Alle Konfigurationsvorlagen** , um nur auf die erforderlichen Vorlagen zuzugreifen.
- Deaktivieren Sie das Kontrollkästchen**Alle StyleBooks** und wählen Sie die erforderlichen StyleBooks aus, auf die Ihr Benutzer zugreifen kann.

  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. Die Konfigurationspakete dieses StyleBook sind auch in dem enthalten, worauf der Benutzer Zugriff hat.

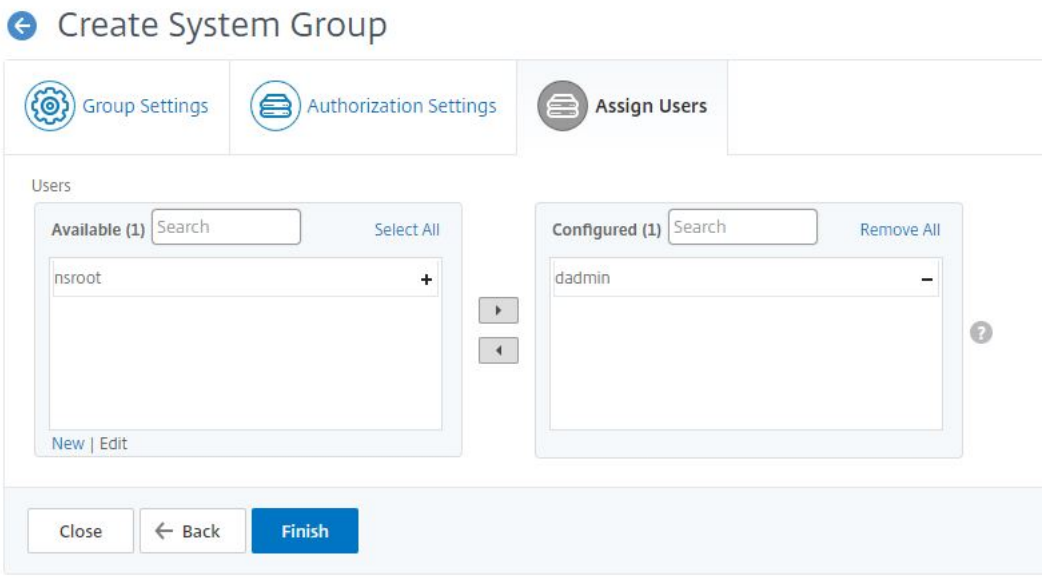


- Deaktivieren Sie das Kontrollkästchen **Alle DNS-Domainnamen** und fügen Sie die Domainnamen aus der Liste hinzu, auf die Ihre Benutzer zugreifen sollen.

7. Klicken Sie auf **Gruppe erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Wählen Sie auf der Registerkarte „ **Benutzer zuweisen** “den Benutzer aus der Liste „ **Verfügbar** “aus und fügen Sie ihn der Liste „ **Konfiguriert** “hinzu. Zum Beispiel „dadmin“.



> **Hinweis:** Sie können auch neue Benutzer hinzufügen, indem Sie auf **Neu**klicken.

9. Klicken Sie auf **Fertig stellen**.

> **Hinweis**
>
> Als Citrix ADM-Administrator können Sie Ihren Benutzern entweder „Nur Lesen“oder „Anzeigen und Bearbeiten“für einzelne ADM-Modul-Benutzeroberflächen basierend auf den Zugriffsrichtlinieneinstellungen in RBAC gewähren. Wenn der Benutzer zwei oder mehr Gruppen zugewiesen ist, d. h. wenn der Benutzer intern mehr als einem Autorisierungsbereich und mehr als einer Zugriffsrichtlinie zugeordnet ist, führt ADM die Berechtigungen all dieser Gruppen zusammen und autorisiert den Benutzer entsprechend.
>
> Stellen Sie sich beispielsweise vor, dass Benutzer1 einer Gruppe zugewiesen ist, die zwei Zugriffsrichtlinien hat, P1 und P2. Jede Richtlinie hat eine andere Art von Genehmigung. P1 hat die Berechtigung „Nur Lesen“, während P2 über die Berechtigung „Anzeigen und Bearbeiten“verfügt. Sie möchten, dass Ihr Benutzer eine Reihe von Anwendungen als Teil der P1-Richtlinie anzeigt und eine andere Gruppe von Anwendungen als Teil der P2-Richtlinie bearbeitet. Als Standardverhalten kombiniert Citrix ADM die beiden Berechtigungstypen und weist dem Benutzer die Berechtigung „Anzeigen und Bearbeiten“zu. So kann Ihr Benutzer jetzt alle Anwendungen anzeigen und bearbeiten.
>
> ADM unterstützt solche Anwendungsfälle nicht, in denen Sie demselben Benutzer verschiedene

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Arten von Berechtigungen zuweisen können. Sie können Ihren Benutzern nur einen Berechtigungstyp zuweisen. ADM kann entweder Benutzer1 erlauben, alle Apps oder eine ausgewählte Gruppe von Apps anzuzeigen, oder Benutzer1 erlauben, alle Apps oder eine ausgewählte Gruppe von Apps anzuzeigen und zu bearbeiten.

Zuordnung von RBAC beim Upgrade von Citrix ADM von 12.0 auf 12.1

Wenn Sie Citrix ADM von 12.0 auf 12.1 aktualisieren, werden Ihnen beim Erstellen von Gruppen keine Optionen zum Erteilen 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 12.1 zugeordnet sind:

12.0	Nur Anwendungen zulassen	12.1
Admin Lese-/Schreibzugriff	False	Admin
Admin Lese-/Schreibzugriff	True	App-Admin
Admin schreibgeschützt	False	nur lesen
Admin schreibgeschützt	True	App Nur lesbar

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.)

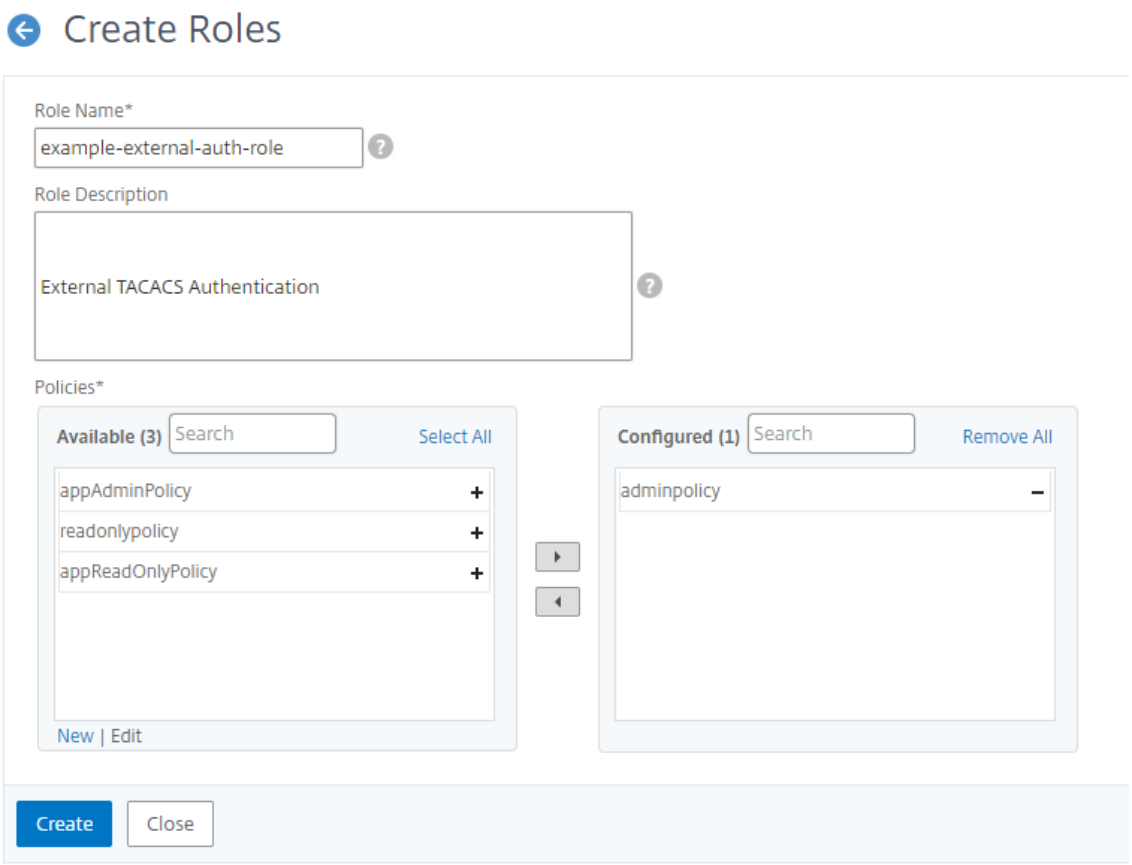
> **Hinweis** Die vordefinierten Rollen können nicht bearbeitet werden.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

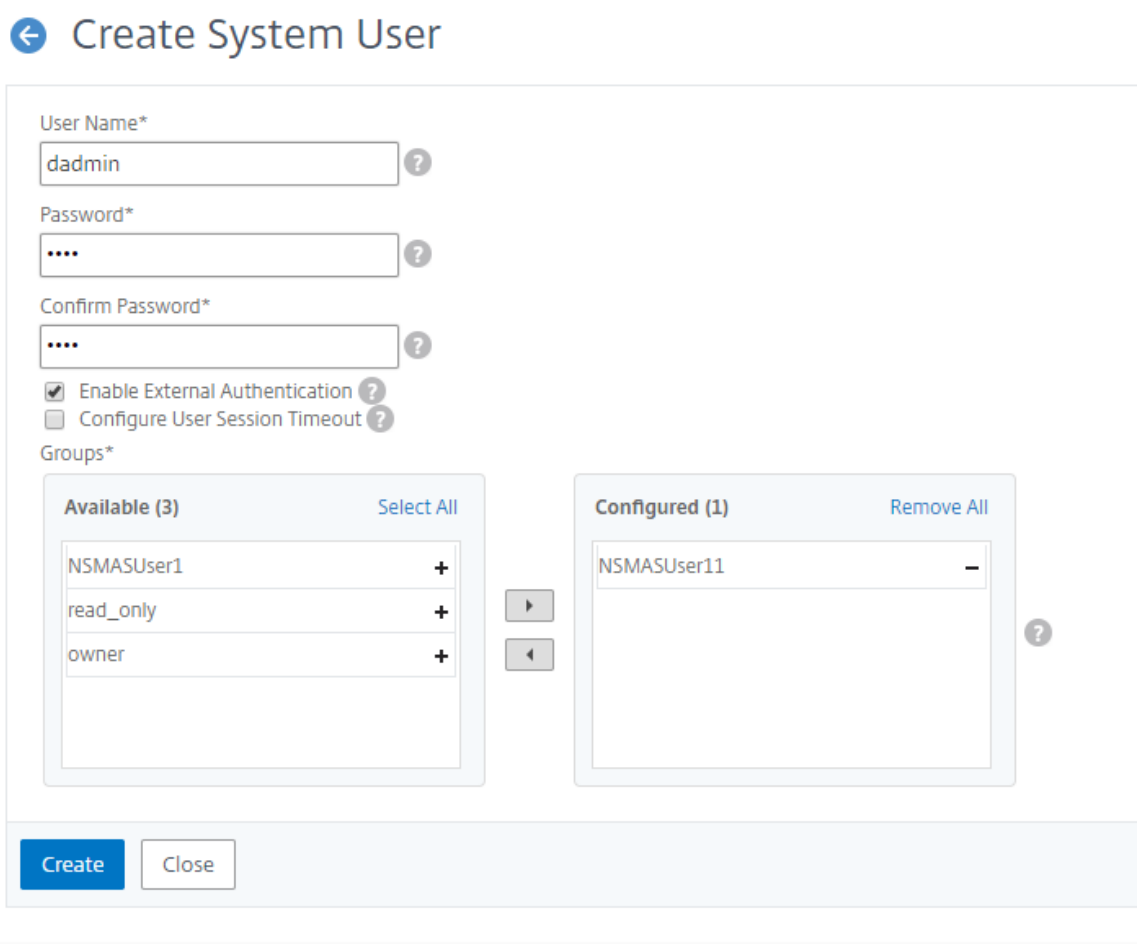
Sie können zusätzliche Benutzer erstellen, indem Sie Konten für sie konfigurieren. Wenn Sie neue Benutzer zu Citrix ADM hinzufügen, können Sie deren Berechtigungen definieren, indem Sie die entsprechenden Gruppen, Rollen und Richtlinien zuweisen.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Mehrmandantenfähigkeit: Bieten Sie Ihren Mandanten eine exklusive Verwaltungsumgebung

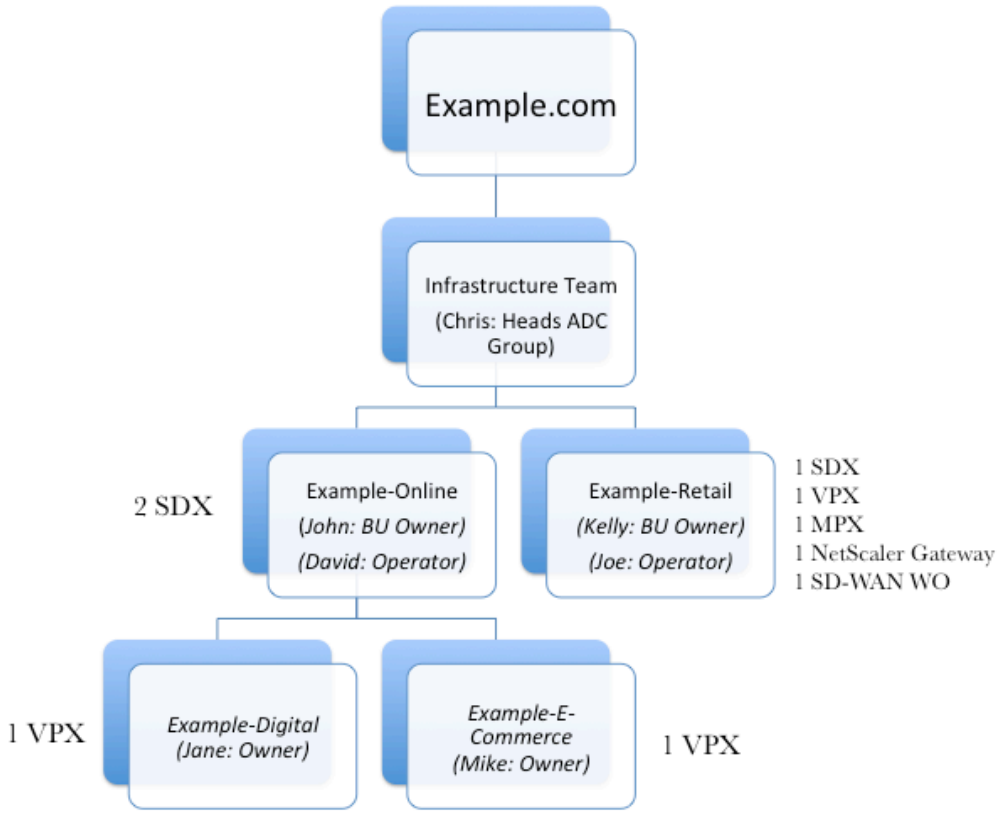
February 5, 2024

Citrix Application Delivery Management (ADM) bietet Mehrmandantenfunktionen, mit denen Sie das System für mehrere Mandanten konfigurieren können. Jeder Mandant kann seine Netzwerkinstanzen hinzufügen, diese Instanzen und Anwendungen verwalten und überwachen sowie eigene Benutzer und Gruppen erstellen. Kein Mandant hat Einblick in die Instanzen und Anwendungen der anderen Mandanten. Nur der Systemadministrator hat Einblick in alle Instanzen, Anwendungen und Berichte aller Mandanten. Der Systemadministrator kann jedoch keine Benutzer für die Mandanten erstellen. Alle Aufgaben auf Systemebene können nur vom Systemadministrator ausgeführt werden.

Stellen Sie sich ein Szenario vor, in dem eine Organisation wie example.com über eine Infrastrukturgruppe und mehrere Geschäftsbereiche verfügt. Sie möchten alle Instanzen in ihrem Netzwerk zentral verwalten. Sie möchten jedoch jeder Geschäftseinheit ein exklusives Umfeld bieten.

Die folgende Abbildung zeigt, wie die Organisationsinfrastrukturgruppe example.com strukturiert ist. Sie möchten, dass jede der vier Geschäftsbereiche über exklusive Managementumgebungen verfügt. Dieses Bild zeigt auch die Anzahl der Instanzen, die jede Geschäftseinheit verwalten möchte.

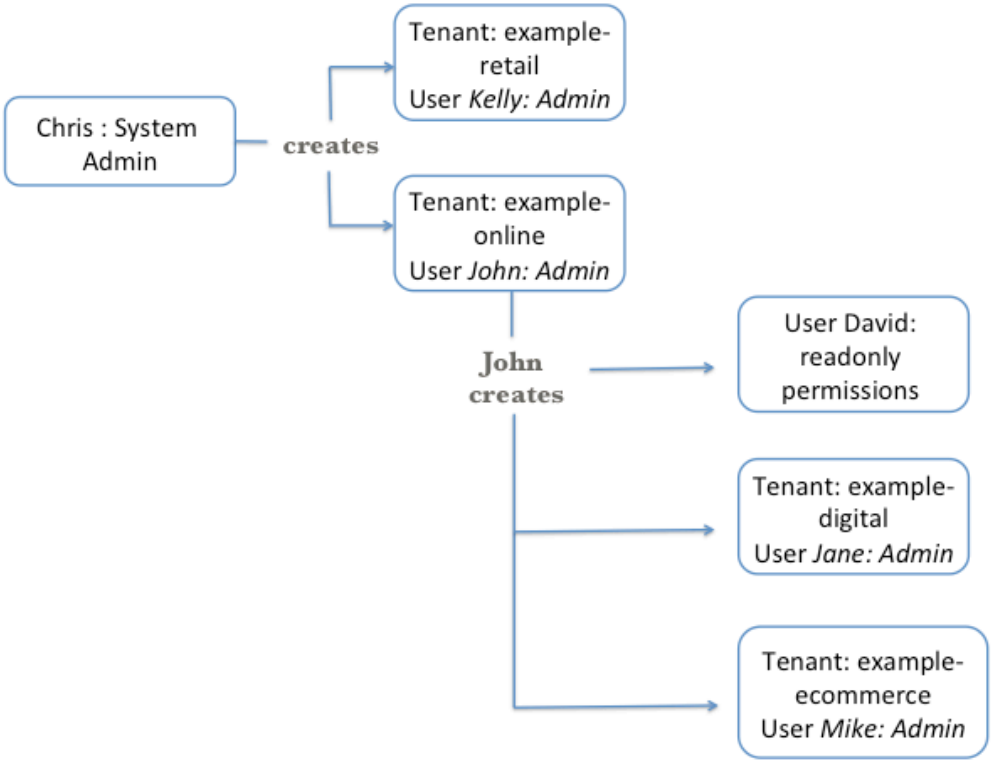
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Chris, der ADC-Gruppenleiter, ist der Systemadministrator von NetScaler ADM. Chris erstellt zwei Mandanten für die beiden Geschäftsbereiche, Example-online und Example-Retail, und weist zwei Benutzer als Administratoren dieser Mandanten zu. Jeder Mandantenadministrator kann jetzt weitere Benutzer hinzufügen, Instanzen hinzufügen, die er verwalten möchte, und Untermandanten in seiner Mandantenumgebung erstellen.

Die folgende Abbildung zeigt die Mandanten und Benutzer, die in NetScaler ADM für dieses Beispiel erstellt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



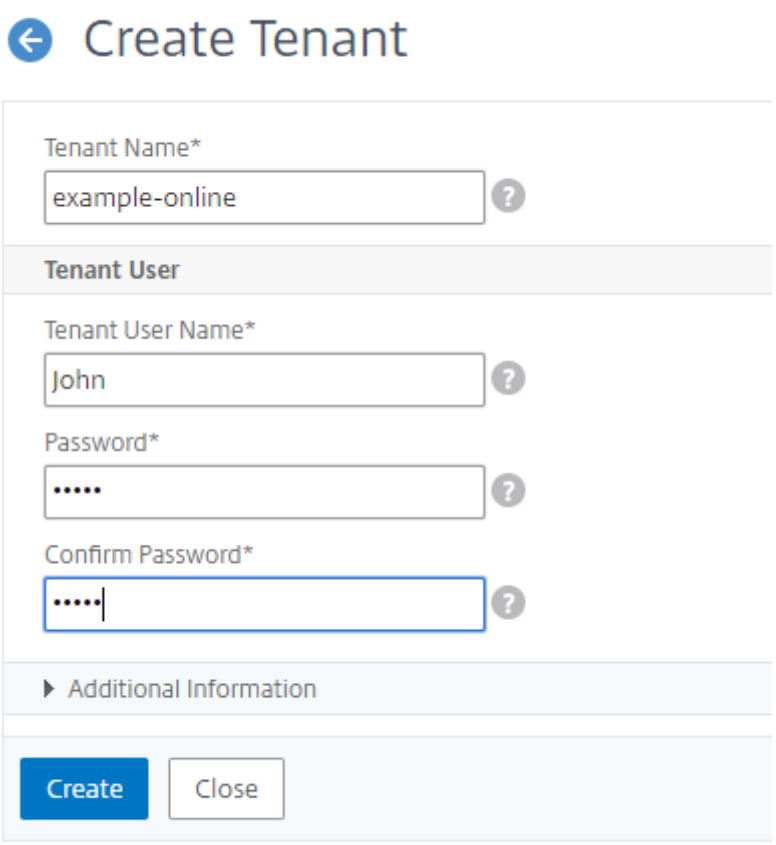
Mandanten hinzufügen

In diesem Beispiel Chris erstellt der Systemadministrator zwei Mandanten: example-online und example-retail. Während der Erstellung der Mandanten erstellt Chris auch einen Standard-Admin-Benutzer für jeden Mandanten.

Mandanten hinzuzufügen

1. Navigieren Sie zu **System** > **Mandanten**und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite „ **Mandant erstellen** “den Mandantennamen und den Mandantenbenutzernamen an, den Sie als Administrator für diesen Mandanten zuweisen möchten. Geben Sie außerdem das Kennwort ein.
3. Klicken Sie auf **Erstellen**.

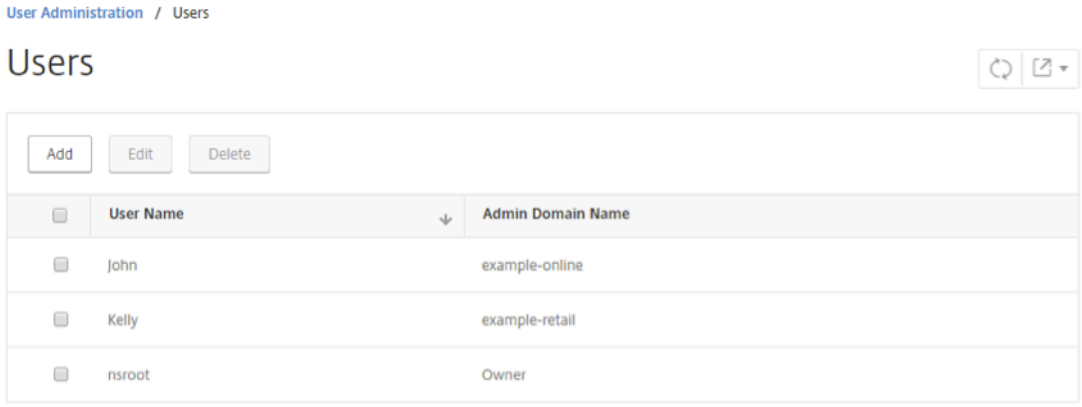
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Auf der Seite **Mandanten** können Sie die Liste der Mandanten anzeigen, die erstellt werden.

Sie können die Liste der Admin-Benutzer für jeden Mandanten auch auf der Seite **System** > **Benutzerverwaltung** > **Benutzer** anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

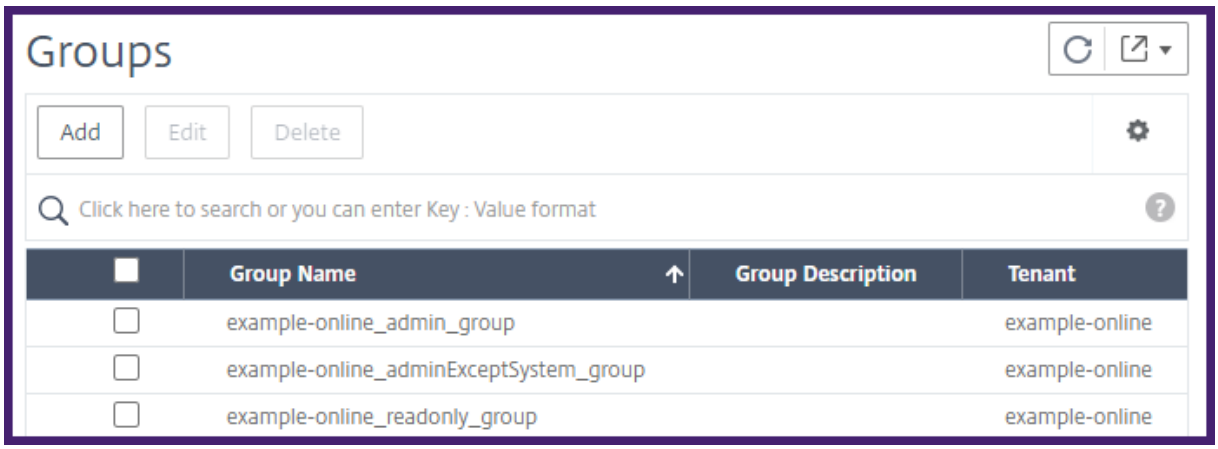


Wenn Sie einen Mandanten erstellen, werden drei Standardsystemgruppen erstellt, admin, adminExceptSystem_group, and read-only.

Beispiel:

Der Tenant example-online hat die folgenden Standardgruppen:

- `example-online_admin_group`
- `example-online_adminExceptSystem_group`
- `example-online_readonly_group`



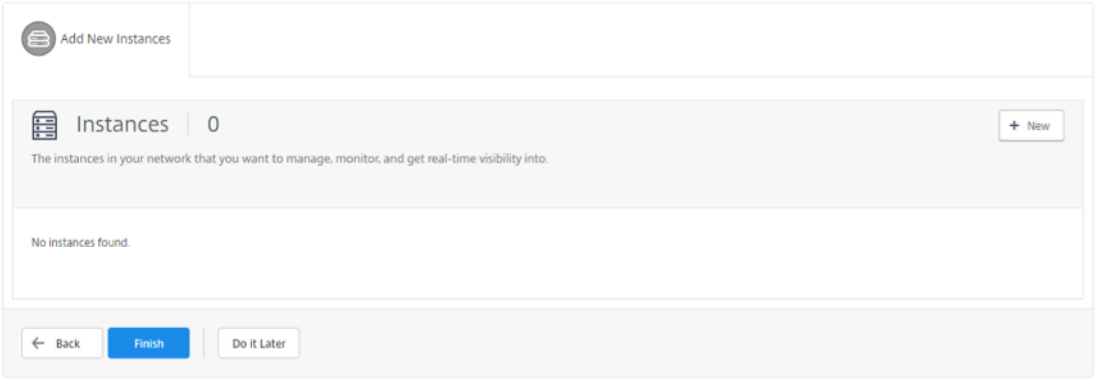
Anmelden bei NetScaler ADM als Mandantenbenutzer

Nachdem die Mandanten erstellt wurden, kann sich ein Mandantenbenutzer mit den Anmeldeinformationen des Mandantenbenutzers bei Citrix ADM anmelden. Dazu muss ein Mandant sowohl den Domainnamen als auch den Benutzernamen angeben, zum Beispiel example-online\John.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinzufügen von Instanzen als Mandantenbenutzer

Nachdem sich ein Mandant angemeldet hat, fordert Citrix ADM den Mandanten auf, Instanzen hinzuzufügen. Klicken Sie auf **+ Neu**, um die Instanzen hinzuzufügen, die Sie verwalten möchten. Alternativ können Sie auf Später erledigen klicken und die Instanzen zu einem späteren Zeitpunkt auf der Registerkarte Infrastruktur hinzufügen. Weitere Informationen finden Sie unter *Hinzufügen einer Instanz zu NetScaler ADM*.



In diesem Beispiel fügt John zwei NetScaler ADC SDX-Instanzen hinzu.

Geben Sie den Instanztyp, die IP-Adressen (durch Komma getrennt) und den Profilnamen an, den Citrix ADM für den Zugriff auf die Instanzen verwenden kann, und klicken Sie dann auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

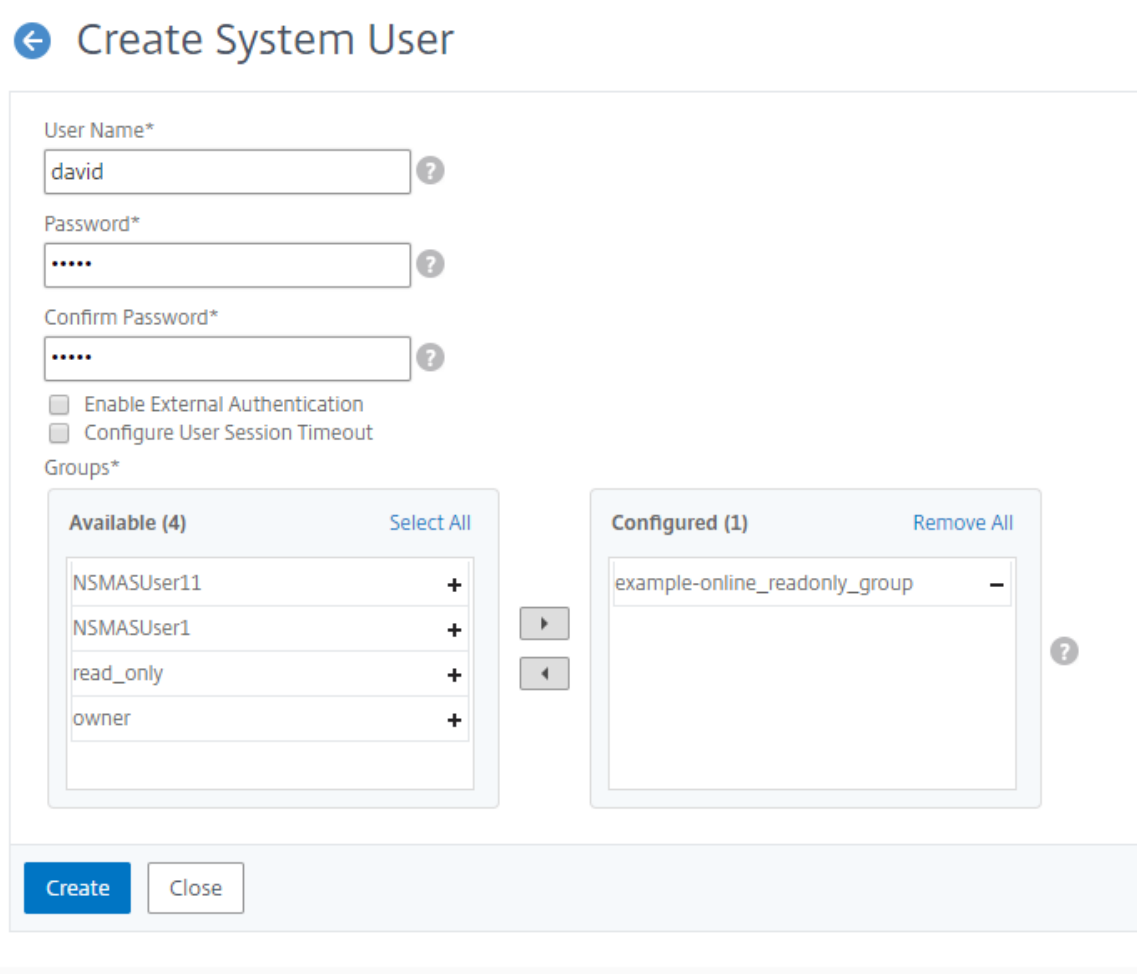
Erstellen Sie einen Benutzer

John, der Mandantenadministrator, möchte nun einen Benutzer für David erstellen, damit David alle Instanzen und Anwendungen dieses Mandanten überwachen kann. Chris möchte jedoch nicht, dass David eine Konfigurationsaufgabe für die Instanzen durchführt oder Systemeinstellungen für den Mandanten ändert. Chris erstellt also einen Benutzer david mit Readonly Berechtigungen.

So erstellen Sie einen Benutzer:

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Benutzer** und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite "**Systembenutzer erstellen** "den Benutzernamen und das Kennwort für den Benutzer an, den Sie erstellen möchten.
3. Wählen Sie unter **Gruppen**die Gruppe aus, die Sie diesem Benutzer zuweisen möchten. In diesem Beispiel wird dem Benutzer david die example-online_readonly_group zugewiesen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



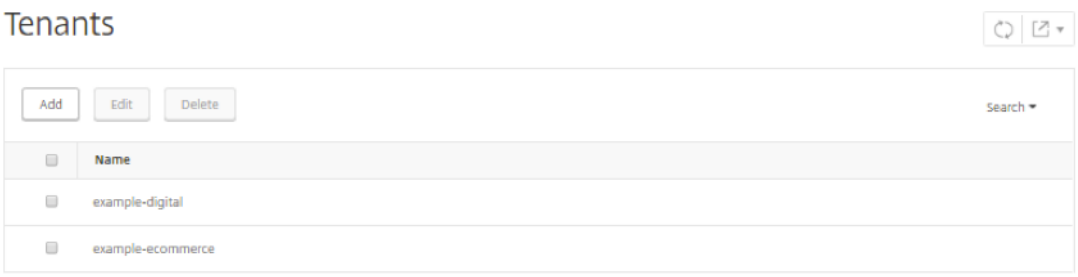
Mandanten innerhalb von Mandanten erstellen

Ein Mandantenadministrator kann Untermandanten erstellen, wenn er seinen Mandanten weiter partitionieren möchte. Er kann jedoch nur eine Ebene von Untermandanten erstellen. In diesem Beispiel erstellt John zwei Untermandanten, example-digital und example-ecommerce. Während der Erstellung dieser beiden Untermandanten weist Chris Jane und Mike jeweils als Admin-Benutzer zu.

Um einen Mandanten innerhalb eines Mandanten zu erstellen, folgen Sie den unter Mandanten hinzufügenbeschriebenen Schritten.

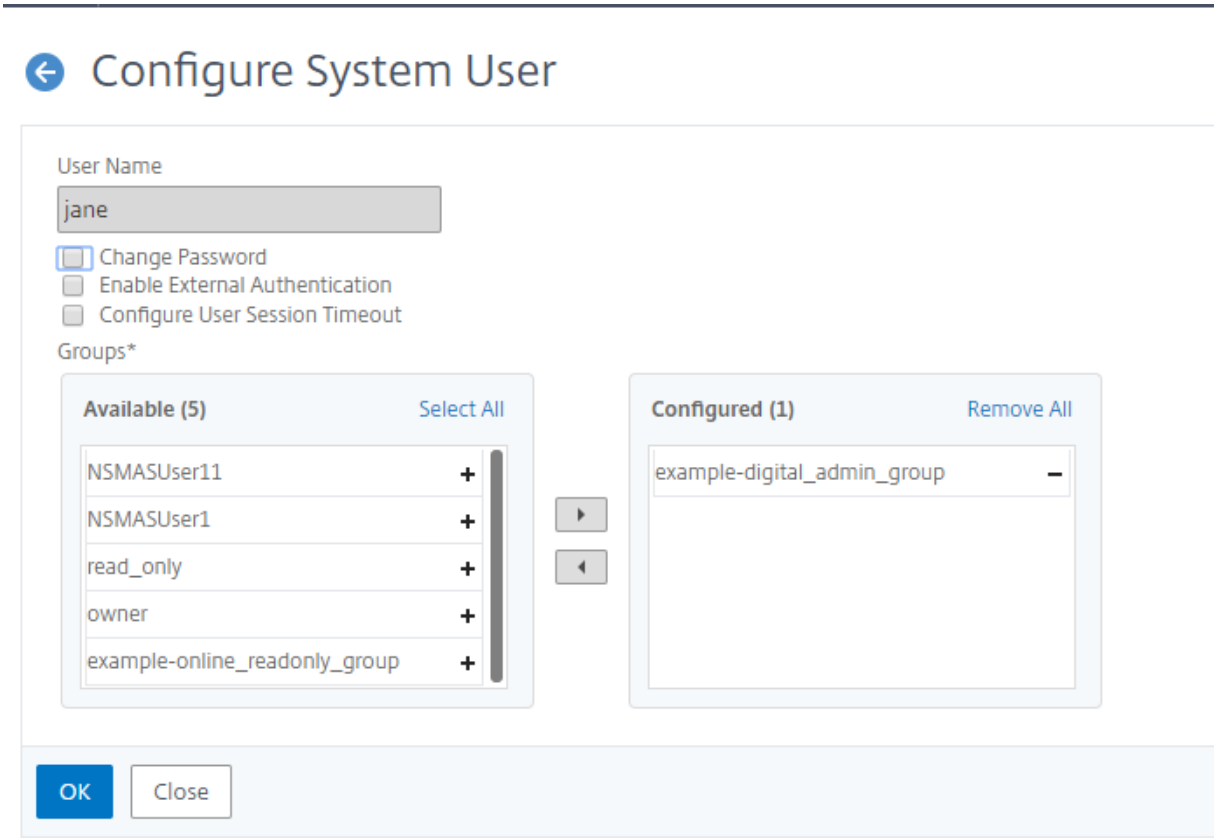
Sie können die Mandanten anzeigen, die auf der Seite **Mandanten** erstellt wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Sie können auch die Berechtigungen anzeigen, die den Benutzern zugewiesen wurden. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Benutzer**, wählen Sie einen Benutzer aus, und klicken Sie auf **Bearbeiten**.

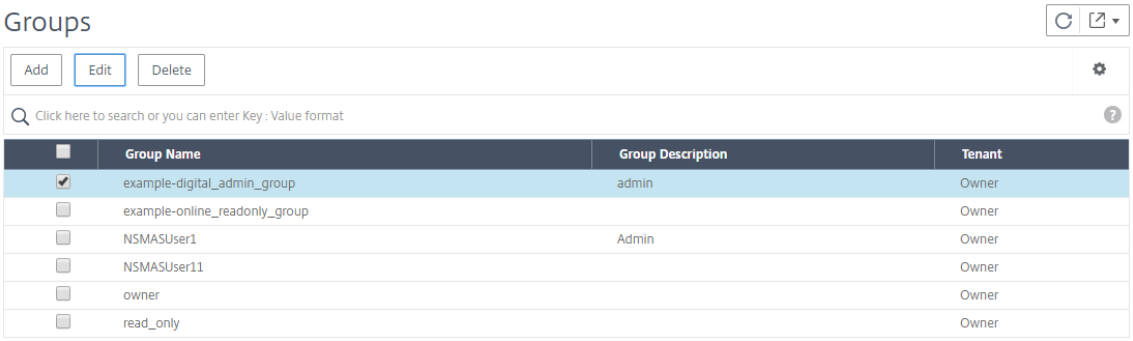
Auf der Seite **Systembenutzer konfigurieren** unter Gruppen können Sie die Gruppen anzeigen, die diesem Benutzer zugewiesen sind. In diesem Beispiel sehen Sie, dass example-digital_admin_group Jane zugewiesen ist.



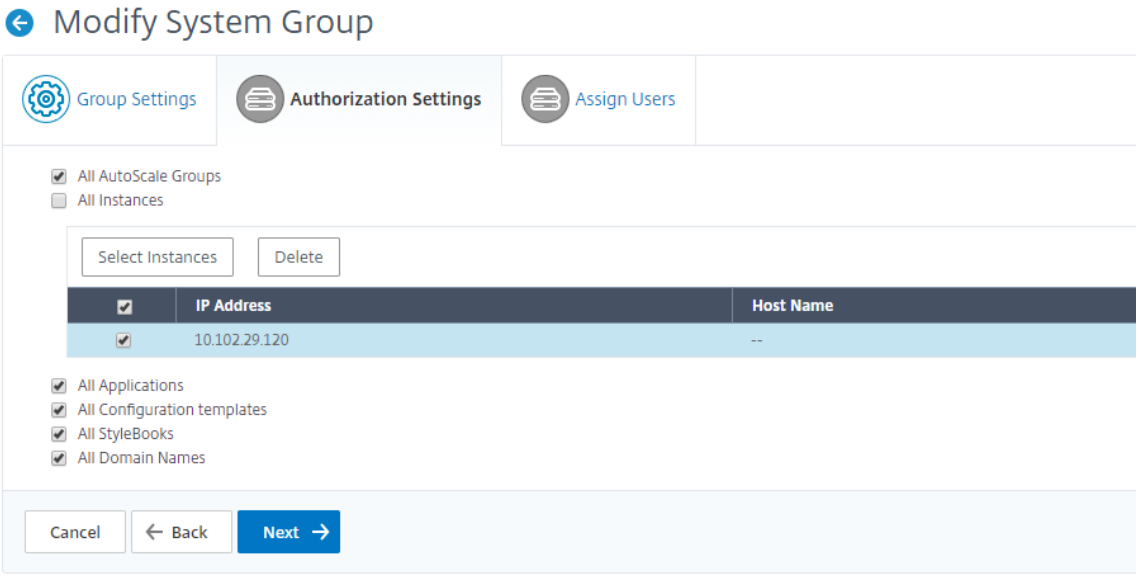
Wenn Sie als Mandantenadministrator bereits Instanzen zu Citrix ADM hinzugefügt haben, können Sie die Instanzen Benutzern in Ihrem Mandanten oder Untermandanten zur Verwaltung und Überwachung zuweisen. Beispielsweise kann John Jane eine VPX-Instanz zu Verwaltungszwecken zuweisen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Gruppe**.
2. Wählen Sie die Gruppe aus, der der Benutzer zugewiesen ist, und klicken Sie auf **Bearbeiten**.



3. Deaktivieren Sie auf der Seite **Systemgruppe ändern** auf der Registerkarte **Autorisierungseinstellungen** das Kontrollkästchen **Alle Instanzen**.



4. Wählen Sie die Instanzen aus, die der Benutzer verwalten soll, und klicken Sie dann auf **Instanzen auswählen**.
5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Anwendungen

February 5, 2024

Die Anwendungsanalyse- und Verwaltungsfunktion von NetScaler ADM stärkt den anwendungsorientierten Ansatz, um Ihnen bei der Bewältigung verschiedener Herausforderungen bei der Anwendungs-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

bereitstellung zu helfen. Dieser Ansatz gibt Ihnen Einblick in die Integritätsbewertung von Anwendungen, hilft Ihnen bei der Bestimmung der Sicherheitsrisiken und hilft Ihnen, Anomalien im Anwendungsdatenverkehr zu erkennen und Abhilfemaßnahmen zu ergreifen.

Die folgende Abbildung bietet einen Überblick über die verschiedenen Aufgaben, die Sie für Application Management and Analytics ausführen können:

Anwendungen können entweder erkannte Anwendungen, HAProxy-Anwendungen oder benutzerdefinierte Anwendungen sein.

Entdeckte Anwendungen

Anwendungen, die automatisch für jeden verwalteten virtuellen Server erstellt werden. Entdeckte Anwendungen haben immer einen virtuellen Server, und diese Anwendungen können nicht direkt bearbeitet oder gelöscht werden.

Benutzerdefinierte Anwendungen

Anwendungen, die von Benutzern aus erkannten Anwendungen erstellt wurden. Mit Citrix ADM können Sie diese Anwendungen hinzufügen, bearbeiten und löschen. Benutzerdefinierte Anwendungen werden erstellt von:

- Ein oder mehrere virtuelle Server
- Ein oder mehrere HAProxy-Frontends.

Wenn Sie eine benutzerdefinierte Anwendung erstellen, werden alle erkannten Anwendungen, die der benutzerdefinierten Anwendung hinzugefügt wurden, aus dem App-Dashboard entfernt.

Wichtige Hinweise

- Sie können eine erkannte Anwendung nicht mehreren benutzerdefinierten Anwendungen hinzufügen.
- Sie können keine benutzerdefinierte Anwendung erstellen, wenn alle erkannten Anwendungen bereits einer anderen benutzerdefinierten Anwendung zugewiesen sind. Sie müssen eine vorhandene benutzerdefinierte Anwendung löschen, um die erkannten Anwendungen für die weitere Zusammenstellung neuer benutzerdefinierter Anwendungen freizugeben.
- Sie können keine benutzerdefinierte Anwendung erstellen, die virtuelle Server und HAProxy-Frontends enthält.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HAProxy-Anwendungen

HAProxy diskrete Anwendungen werden automatisch für jedes verwaltete HAProxy-Frontend erstellt. Sie können diese Anwendungen auch gruppieren, um benutzerdefinierte Anwendungen zu erstellen, die NetScaler ADC Anwendungen ähnlich sind. Weitere Informationen finden Sie unter Verwaltung und Überwachung von HAProxy-Instanzen mit Citrix ADM.

Wichtige Hinweise

Die folgenden App-Dashboard-Funktionen oder -Metriken werden für HAProxy-Anwendungen nicht unterstützt:

- App-Aktivitäts-Ermittler
- AppScore
- Bedrohungsindex
- Trend zur Spitzenauslastung
- Durchsatz
- Serververbindungen
- Transaktionen

Eine benutzerdefinierte Anwendung erstellen

Sie können benutzerdefinierte Anwendungen erstellen, indem Sie beim Definieren einer Anwendung eine oder mehrere erkannte Anwendungen hinzufügen.

So erstellen Sie eine benutzerdefinierte Anwendung:

1. Navigieren Sie zu **Anwendungen** > **Dashboard**, und klicken Sie auf **Benutzerdefinierte App definieren**.
2. Stellen Sie auf dem Bildschirm „Anwendung definieren“die folgenden Parameter ein:

Feld	Beschreibung
Name	Name der benutzerdefinierten Anwendung
Kategorie	Name der Kategorie, für die alle zu dieser Kategorie gehörenden Anwendungen im Anwendungs-Dashboard zusammengefasst werden.

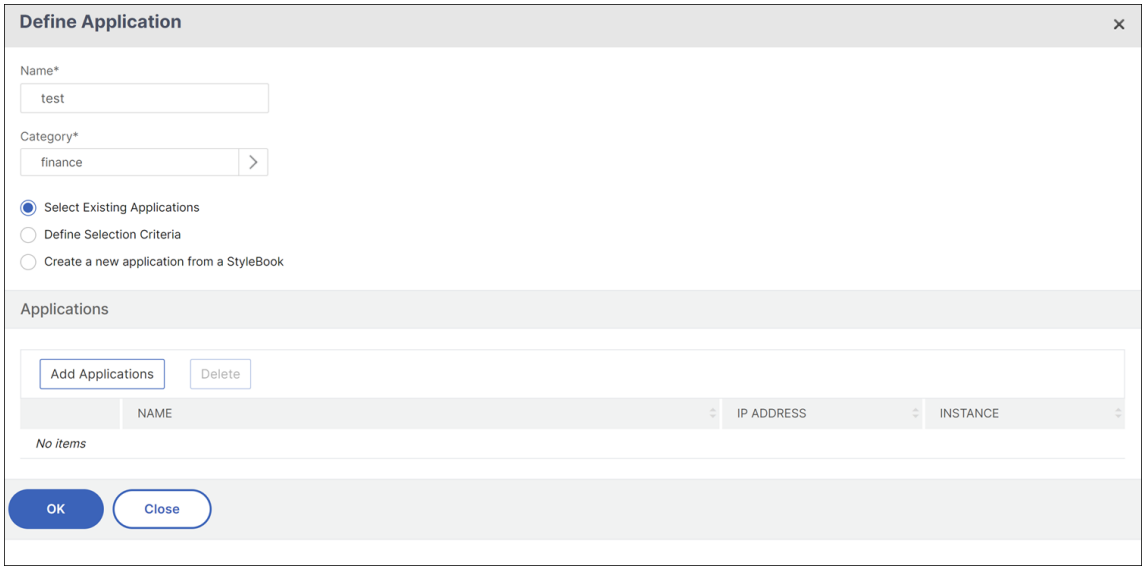
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Feld	Beschreibung
Vorhandene Anwendungen auswählen	Option zum Hinzufügen virtueller Server, wenn die Definitionskriterien auf den lizenzierten virtuellen Servern basieren, die von Citrix ADM überwacht werden.
Auswahlkriterien definieren	Option zum Definieren der Anwendung nach virtuellem Serverbereich oder nach IP-Adressbereich des Ursprungsservers/-dienstes. • **Server.** Sie geben die Server- oder Dienst-IP-Adresse, 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. • **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.

3. Klicken Sie auf OK.

> **Hinweis**
>
> Derzeit unterstützt Application Dashboard nur virtuelle Server für Lastausgleich und Content Switching.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

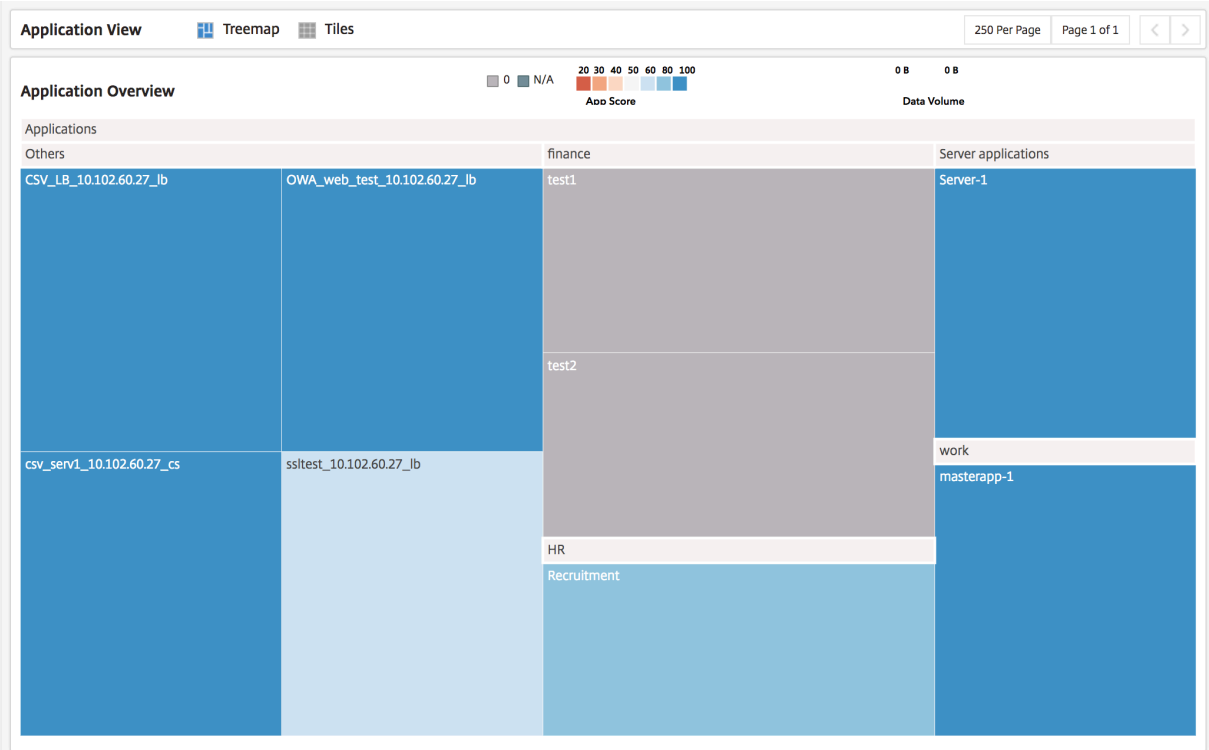


Gruppieren Sie Ihre Bewerbungen

Durch die Gruppierung Ihrer Anwendungen können Sie sie mühelos verwalten und überwachen. Sie können Ihre Anwendungen gruppieren, indem Sie bei der Definition einer Anwendung eine Kategorie auswählen oder erstellen. Um die Kategorie zu erstellen oder auszuwählen, während Sie die Anwendung definieren, klicken Sie auf die Schaltfläche **>** neben dem Feld Kategorie.

Anwendungen, die keiner Kategorie hinzugefügt wurden, werden unter der Kategorie **Andere** angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Anwendungsdashboard

Das Anwendungs-Dashboard bietet eine ganzheitliche Ansicht aller von Citrix ADM überwachten Anwendungen und enthält wichtige Informationen zu allen Anwendungen. Das Dashboard zeigt beispielsweise Leistungs- und Sicherheitsmetriken, Zähler und den Integritätsstatus der Anwendungen an. Um Informationen zu einer bestimmten Anwendung anzuzeigen, wählen Sie die Anwendung aus. Und im Übersichtsbereich zeigen Balkendiagramme Kennzahlen wie App-Score und Bedrohungsindizes für alle überwachten Anwendungen an.

Sehen Sie sich Ihre Bewerbungen an

Das Anwendungs-Dashboard zeigt Anwendungen als Knoten auf einer Baumkarte an, deren Größe dem Datenvolumen der Anwendung entspricht. Die Farbe einer Kachel gibt den App-Score der Anwendung an, wobei Rot für minimale Gesundheit und Blau für gute Gesundheit steht.

Sie können Ihre Anwendungs-Dashboard-Ansicht auf Treemap oder Kacheln umstellen, indem Sie eine der Optionen auf dem Anwendungs-Dashboard-Bildschirm auswählen, auf dem Sie die Details der Anwendungen in Form von Karten sehen können. Standardmäßig werden 250 Anwendungen im Anwendungs-Dashboard angezeigt. Um weitere Anwendungen anzuzeigen, klicken Sie auf die Option „Nächste Seite“.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anwendungen werden nach den Kategorien gruppiert, die bei der Definition der Anwendungen ausgewählt wurden. Anwendungen können sortiert oder sichtbar gemacht werden, indem Anwendungsmetriken aus dem Bereich mit der Anwendungsübersicht ausgewählt werden. Wenn Sie beispielsweise die Anwendungen anzeigen möchten, deren App-Score im Bereich 20-40 liegt, wählen Sie das entsprechende Balkendiagramm im Bereich App Score des App-Übersichtsfensters aus. Ebenso können Sie im App-Übersichtsbereich andere Metriken auswählen.

Bereich „App-Zusammenfassung“

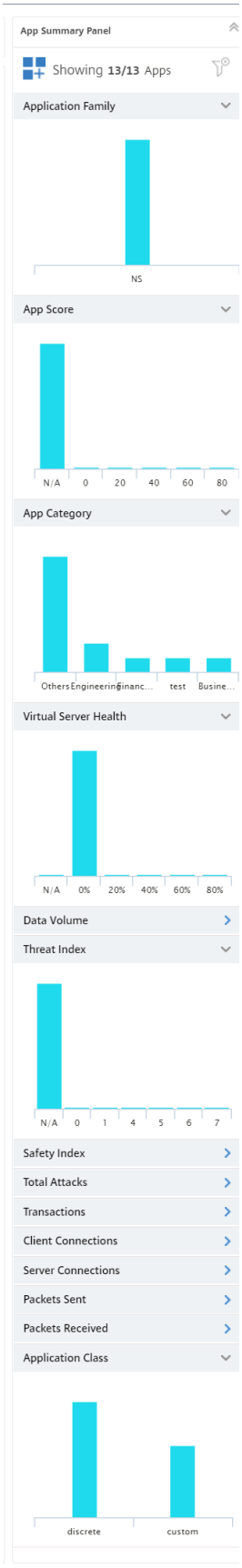
Das App-Übersichtsfeld zeigt alle Metriken der Anwendungen an, die im Anwendungs-Dashboard sichtbar sind. In diesem Bereich können Sie die Anwendungen im Dashboard sortieren und anzeigen, indem Sie Anwendungsmetriken auswählen oder abwählen. Das App-Übersichtsfeld zeigt die folgenden Metriken an:

Metriken	Beschreibungen
Anwendungsfamilie	Ein Balkendiagramm, das die Anzahl der Anwendungen je nach Typ der Citrix ADC-Instanzen gruppiert, auf denen sie konfiguriert sind.
AppScore	Ein Bewertungssystem, das die Leistung einer Anwendung definiert
App-Kategorie	Ein Balkendiagramm, das ein Histogramm für alle in Citrix ADM definierten Kategorien anzeigt. Alle diskreten Anwendungen werden jetzt in der Kategorie „Andere“angezeigt, und benutzerdefinierte Anwendungen werden unter ihren jeweiligen Kategorienamen angezeigt.
Virtual Server Integrität	Ein Balkendiagramm, das die Anzahl der Anwendungen in jeder Kategorie anzeigt. Die Anwendungen sind so kategorisiert, dass sie einen Gesundheitswert von 0%, 20%, 40%, 60%, 80% und 100% haben.
Datenvolume	Ein Bewertungssystem, das die Anzahl der Anwendungen nach dem Datenvolumen der Anwendung gruppiert. Das Datenvolumen wird anhand der Gesamtzahl der von den Anwendungen angeforderten Byte und der Anzahl der Byte berechnet, die als Antworten von den Anwendungen empfangen wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibungen
Bedrohungsindex	Ein einstelliges Bewertungssystem, das die Kritikalität von Angriffen auf die Anwendung angibt, unabhängig davon, ob die Anwendung durch eine Citrix ADC Appliance geschützt ist oder nicht.
Sicherheitsindex	Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler ADC-Instanzen zum Schutz von Anwendungen vor externen Bedrohungen und Sicherheitslücken konfiguriert haben.
Angriffe insgesamt	Die Gesamtzahl der Angriffe auf die Anwendungen
Transaktionen	Die Bandbreite der von den Anwendungen ausgeführten Transaktionen.
Clientverbindungen	Die Anzahl der von den Anwendungen hergestellten Client-Verbindungen.
Serververbindungen	Die Anzahl der Serververbindungen, die von den Anwendungen hergestellt wurden.
Gesendete Pakete	Die Anzahl der von den Anwendungen gesendeten Pakete.
Empfangene Pakete	Die Anzahl der Pakete, die von den Anwendungen empfangen werden.
Anwendungsklasse	Ein Balkendiagramm, das die Anzahl der Anwendungen gruppiert, je nachdem, ob es sich um diskrete oder benutzerdefinierte Anwendungen handelt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



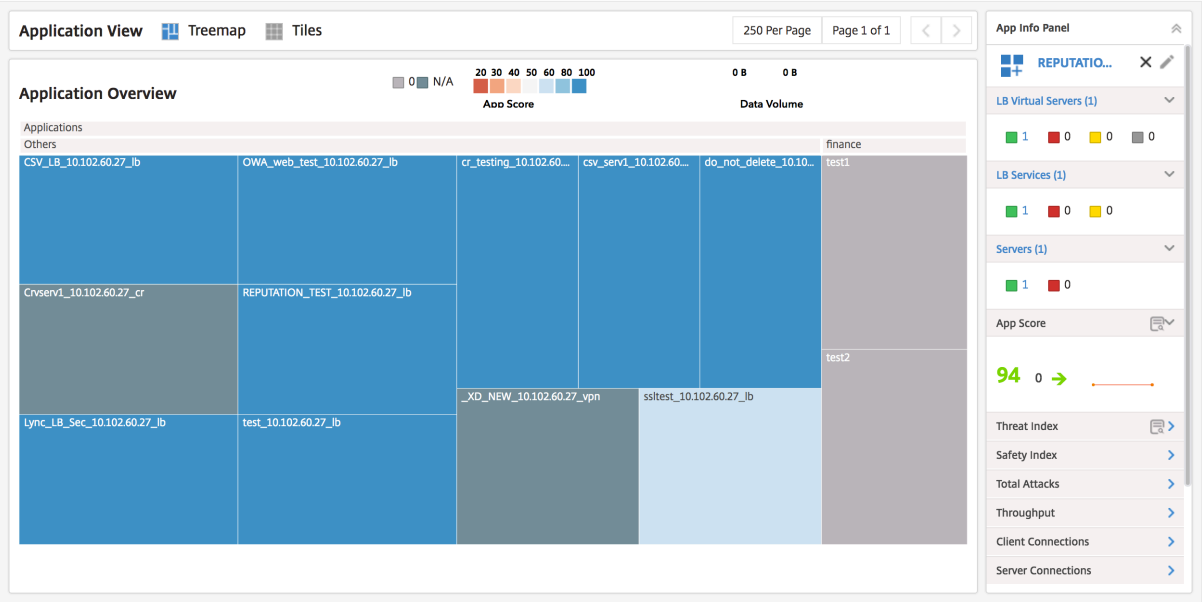
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Scrollen Sie beispielsweise im Übersichtsbereich der App nach unten, um das Balkendiagramm „Virtual Server Health“zu finden. Im Integritätsbalkendiagramm des virtuellen Servers klassifiziert NetScaler ADM Anwendungen basierend auf dem Prozentsatz der Integrität des virtuellen Servers. Das Balkendiagramm zeigt die Anzahl der Anwendungen an, deren Integritätswert der virtuellen Server zwischen 0% und 100% liegt.

Der Zustand virtueller Server stellt den Zustand virtueller Server dar, die unter diskreten Anwendungen gruppiert sind. Wenn es jedoch benutzerdefinierte Anwendungen gibt, die zwei oder mehr virtuelle Server umfassen, wird die geringste Virtual Server Integrität in der Gruppe berücksichtigt.

Sie können nun einen Filter anwenden und nur die Anwendungen im Anwendungs-Dashboard anzeigen, die den Auswahlkriterien entsprechen. Klicken Sie auf den Balken mit der Aufschrift 0%. In dieser Leiste wird die Anzahl der Anwendungen angezeigt, deren virtueller Serverzustand zwischen 0% und 20% liegt. Sie können jetzt Anwendungen mit einem niedrigen Zustand des virtuellen Servers trennen und Abhilfemaßnahmen ergreifen.

App-Informationsfeld Der Bereich „App-Informationen“befindet sich auf der ersten Ebene, wenn Sie eine Anwendung genauer untersuchen. Es zeigt die wichtigsten Metriken und Komponenten der Anwendung zusammen mit ihrem Status an. Beispielsweise zeigt das App-Informationsfeld für jede ausgewählte Anwendung die Gesamtzahl der virtuellen Server, die Gesamtzahl der Dienste, den App-Score und andere Informationen an. Um das App-Informationsfeld anzuzeigen, klicken Sie im Anwendungs-Dashboard auf eine beliebige Anwendungskachel. Das App-Info-Bedienfeld ersetzt dann das Bedienfeld “App-Zusammenfassung”.



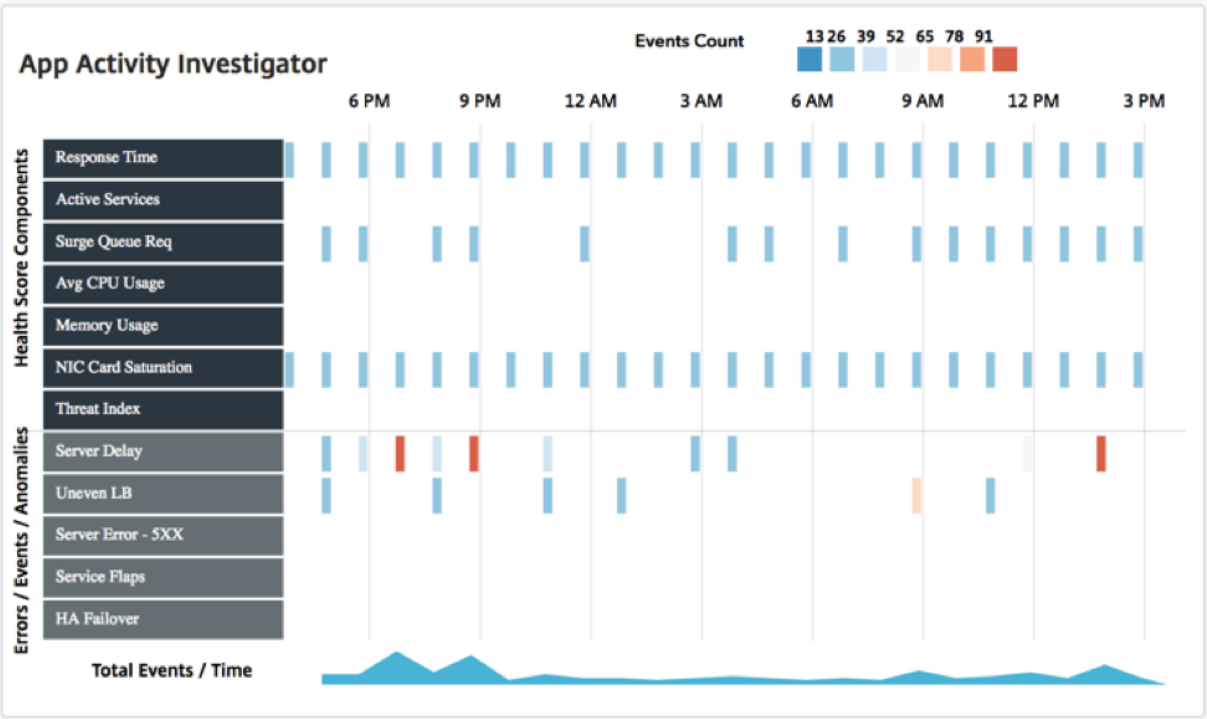
Ermittler für App-Aktivitäten Der App Activity Investigator ist eine der zweiten Ebenen, wenn Sie von einer Anwendung aus einen Drilldown durchführen. Sie erreichen den App Activity Investigator,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

indem Sie das Suchsymbol im Bereich App-Informationen auswählen oder im Anwendungs-Dashboard auf die Anwendungskachel doppelklicken.

Der App Activity Investigator zeigt wichtige Informationen wie App Score-Komponenten, Fehler, Ereignisse und Anomalien an.

Jede der Legenden wird in Intervallen von einer Minute aggregiert, wenn die gewählte Dauer eine Stunde beträgt, und in einem Intervall von einer Stunde, wenn die gewählte Dauer einen Tag beträgt.



Diese Abweichungen werden als rechteckige Legenden im Diagramm angezeigt. Diese Legenden werden aggregiert und werden entsprechend der Anzahl der aufgetretenen Ereignisse farbcodiert. Blau steht für die niedrigste Anzahl von Ereignissen und Rot für die maximale Anzahl. Sie können den Mauszeiger auf eine Legende bewegen, um Details wie Fehlertyp, Uhrzeit und die Anzahl der für die ausgewählte Legende aggregierten Ereignisse anzuzeigen. Sie können den Zeitraum des Diagramms anpassen, indem Sie die Zeit aus dem Drop-down-Menü Zeitraum auswählen.

Trend zur App-Nutzung In den meisten Fällen treffen Sie als Geschäftsinhaber Entscheidungen über die Effektivität Ihrer Anwendung und Nutzungstrends auf der Grundlage von Statistiken und Daten. Um den Trend zur Anwendungsnutzung zu verstehen, müssen Sie Informationen von mehreren Entitäten in Ihrer Bereitstellung zusammenstellen, z. B. von der Backend-Infrastruktur, Proxys, CDN-Netzwerken usw. Korrelieren Sie dann die gesammelten Informationen, um die richtigen Analysen zu erhalten. Dies nimmt viel Zeit in Anspruch.

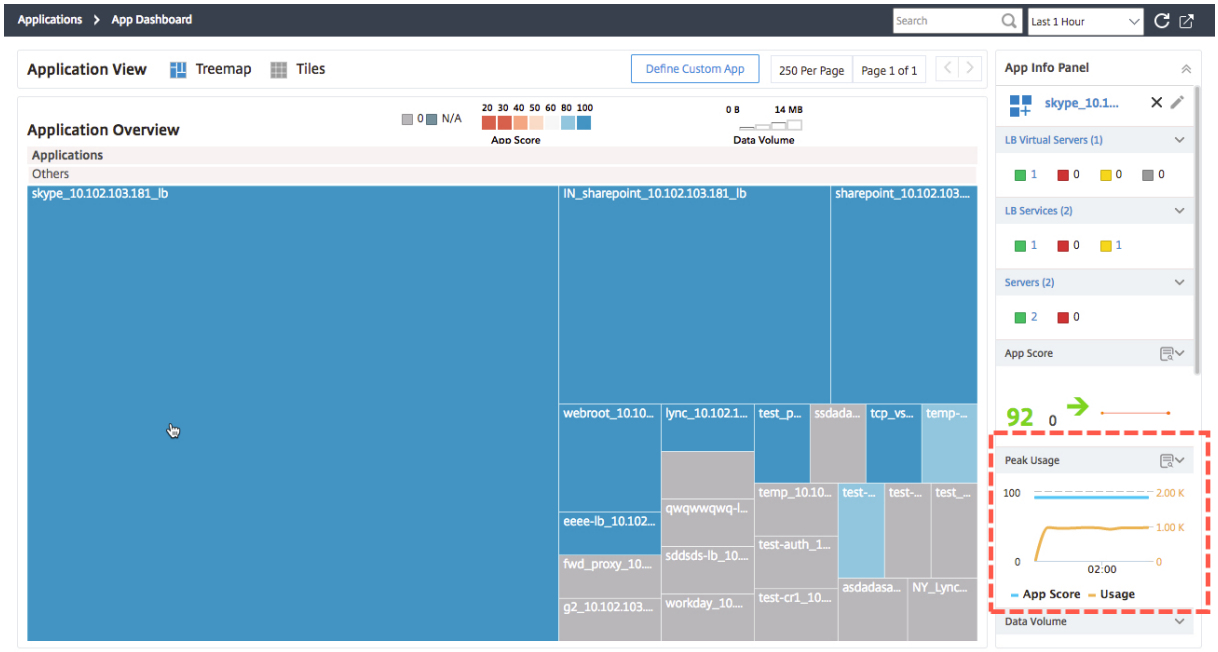
Stattdessen enthält die Citrix ADC Appliance, die als ADC in Ihrer Bereitstellung bereitgestellt wird, alle

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Informationen zur Anwendung und die Nutzungsstatistiken der Anwendung. Sie können diese Informationen an Citrix ADM weiterleiten. Citrix ADM sammelt diese Informationen und bietet detaillierte Einblicke in die Nutzung und Leistung der Anwendung. Sie können diese Erkenntnisse nutzen, um effektive Entscheidungen auf der Grundlage der Anwendungsnutzung und -leistung zu treffen.

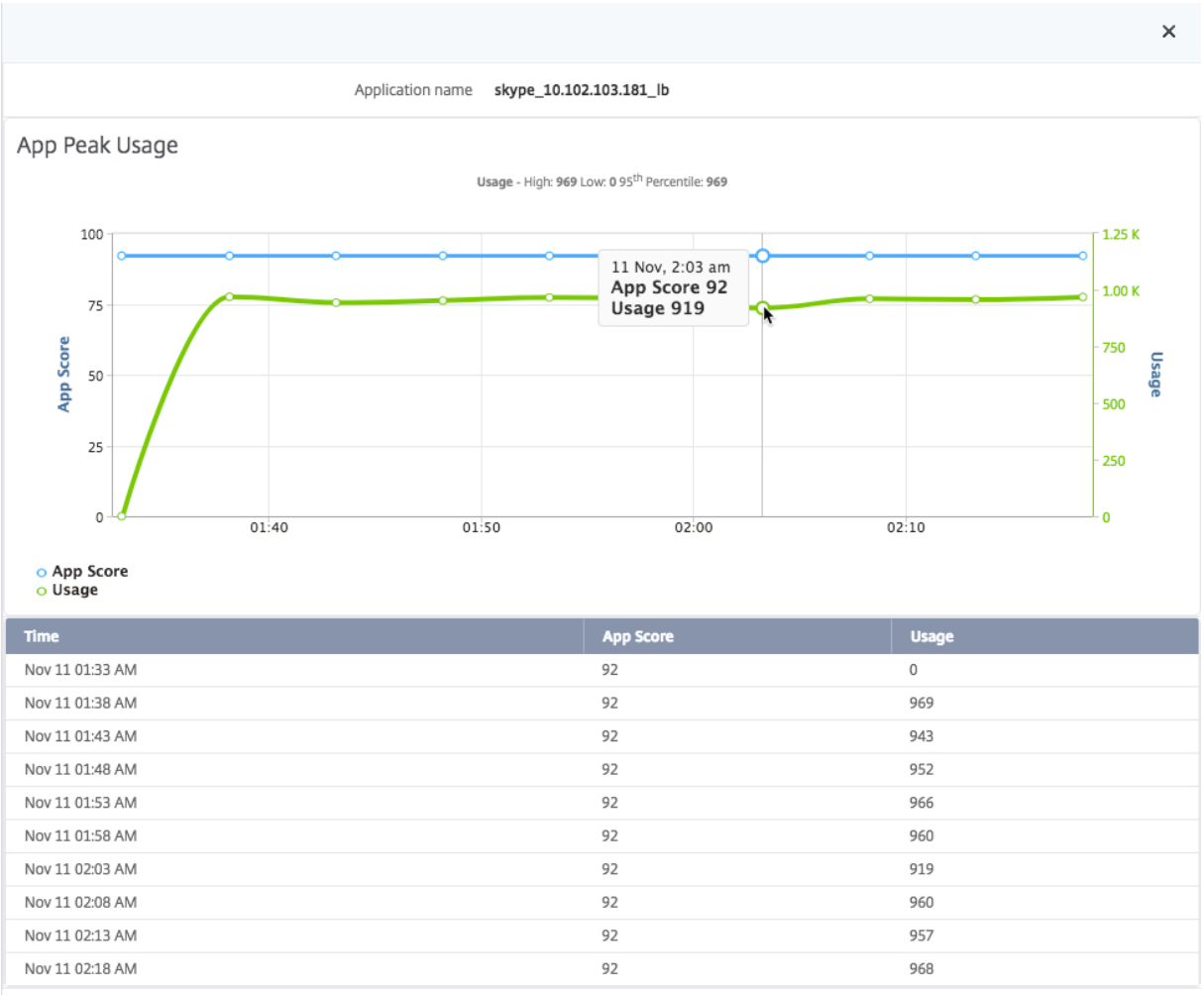
Das App-Info-Panel im Anwendungs-Dashboard zeigt den Spitzennutzungstrend einer Anwendung an. Sie können den Trend zur Spitzenauslastung verwenden, um die Leistung der Anwendung zu bewerten und geeignete Maßnahmen zu ergreifen, um die Leistung der Anwendung zu verbessern.

Um den Trend zur Spitzennutzung einer Anwendung anzuzeigen, navigieren Sie zu **Anwendungen > App-Dashboard** . Wählen Sie die Anwendung aus. Der Trend zur Spitzenauslastung der Anwendung wird im Bereich **Spitzenauslastung** im App-Infobereich angezeigt.



Sie können weiter auf den Abschnitt **Peak Usage** klicken, um den App Score und die Anwendungsnutzung einzusehen. Anhand dieser Informationen können Sie die Spitzenauslastung der Anwendung ermitteln und sie mit dem entsprechenden App-Score verknüpfen, um die Performance-Auswirkungen auf die Anwendung während der Spitzenauslastung zu bewerten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Time	App Score	Usage
Nov 11 01:33 AM	92	0
Nov 11 01:38 AM	92	969
Nov 11 01:43 AM	92	943
Nov 11 01:48 AM	92	952
Nov 11 01:53 AM	92	966
Nov 11 01:58 AM	92	960
Nov 11 02:03 AM	92	919
Nov 11 02:08 AM	92	960
Nov 11 02:13 AM	92	957
Nov 11 02:18 AM	92	968

Exportieren von Berichten über App-Dashboard und Sicherheits-Dashboard

Mit Citrix ADM können Sie eine Momentaufnahme der aktuellen Seite des App Dashboards und des App Security 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- oder PDF-Berichte extrahieren.

> **Hinweis** Im Gegensatz zu anderen Berichtsexportoptionen in Citrix ADM können Sie die App Dashboard- und Security Dashboard-Berichte nur als PDF- oder PNG-Dateien exportieren. Andere Optionen wie JPG und.csv werden derzeit nicht unterstützt.

1. Klicken Sie auf der Seite **ApplicationDashboard oder App Security** Dashboard auf das Exportsymbol oben rechts auf der Seite.
2. Wählen Sie die Exportoption entweder als PDF- oder PNG-Datei.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Klicken Sie auf **OK**.

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.

Analyse der Anwendungsleistung

February 5, 2024

App Score ist das Produkt eines Bewertungssystems, das definiert, wie gut eine Anwendung funktioniert. Es zeigt, ob die Anwendung in Bezug auf die Reaktionsfähigkeit gut funktioniert, und alle Systeme sind betriebsbereit. App-Score wird auf Anwendungsebene angezeigt. Die Berechnung der Punktzahl basiert auf den folgenden drei Schlüsselkomponenten:

- **App Performance Score (APDEX Score der Anwendung)**. Abgeleitet von der Server-Antwortzeitvariation der Anwendung.
- **Citrix ADC -Systemressource**. Basierend auf drei weiteren Komponenten abgeleitet:
  - CPU-Nutzung
  - Speichernutzung
  - NIC-Karten-Sät
- **App-Server-Ressource**. Abgeleitet von zwei weiteren Komponenten:
  - Prozentsatz der aktiven Dienste
  - Warteschlangen-Überspannungsanforderungen

Die App-Bewertung wird aus diesen Werten berechnet, bei denen die NetScaler ADC -Systemressourcenbewertung und die App Server-Ressourcenbewertung von der App-Leistungsbewertung abgezogen werden. App Score ist für alle Anwendungen verfügbar, die mit Load Balancing und Content Switching virtueller Server definiert sind, die erkannt werden, sowie für die benutzerdefinierten Anwendungen, die Sie im Anwendungs-Dashboard definieren.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) **Unterer Schwellenwert für Überspannungswarteschlange**. Der niedrigere Schwellenwert des Verhältnisses der Gesamtzahl der Verbindungen, die für den virtuellen Server und die etablierten Verbindungen ausstehen.

b) **Höherer Schwellenwert für Überspannungswarteschlange**. Der höhere Schwellenwert des Verhältnisses der Gesamtzahl der Verbindungen, die für den virtuellen Server und die etablierten Verbindungen ausstehen.

c) **Niedriger CPU-Schwellenwert (%)**. Der niedrigere Schwellenwert der gesamten CPU-Auslastung in der NetScaler ADC-Instanz.

d) **Hoher CPU-Schwellenwert (%)**. Der höhere Schwellenwert der gesamten CPU-Auslastung in der NetScaler ADC-Instanz.

e) **Niedriger Speicherschwellenwert (%)**. Der niedrigere Schwellenwert der Gesamtspeicherauslastung in der NetScaler ADC-Instanz.

f) **Hoher Speicherschwellenwert (%)**. Der höhere Schwellenwert der Gesamtspeicherauslastung in der NetScaler ADC-Instanz.

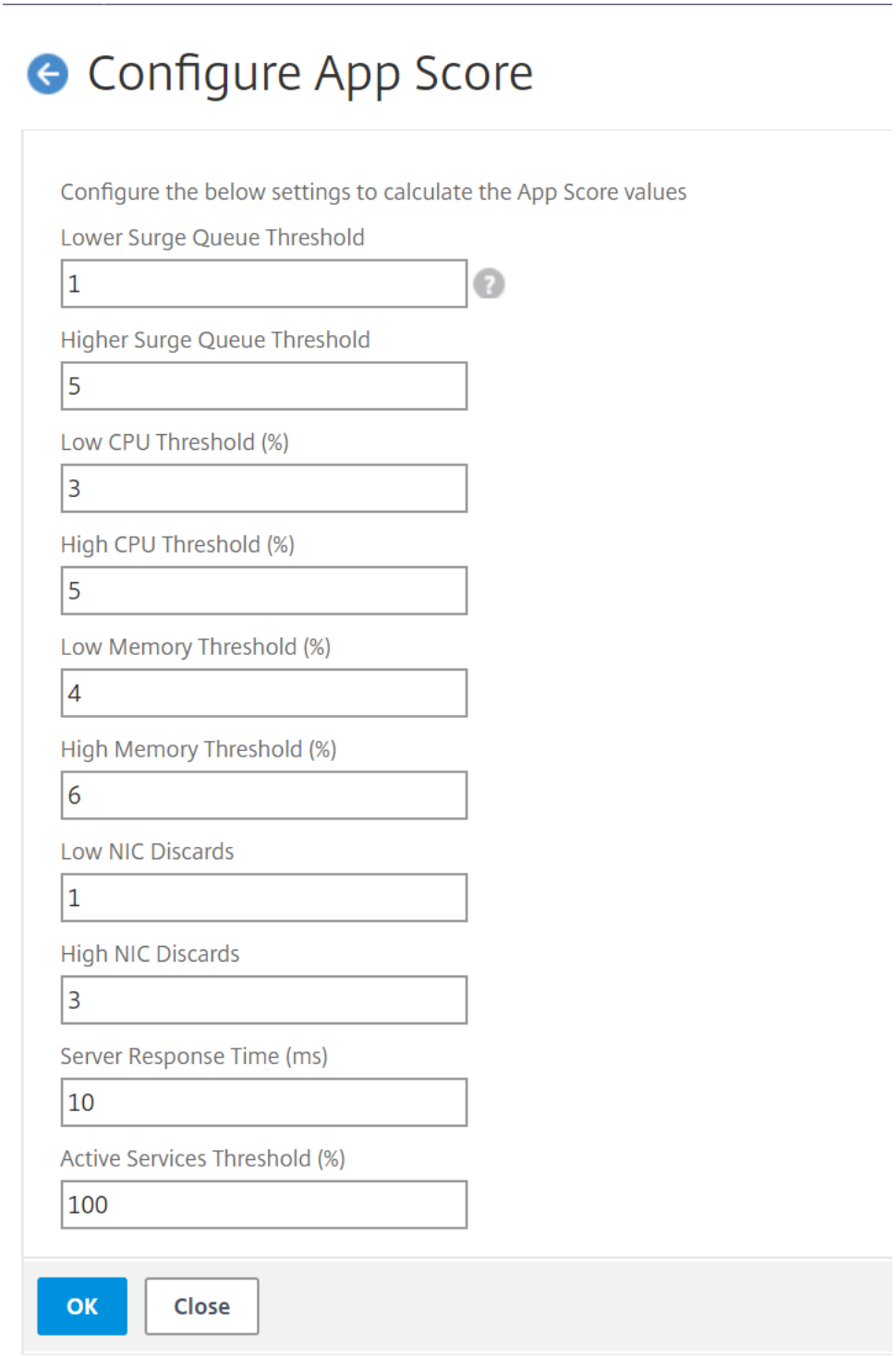
g) **Low NIC Discards**. Der untere Schwellenwert der Pakete, die von den Schnittstellen verworfen werden.

h) **High NIC Discards**. Der höhere Schwellenwert der Pakete, die von den Schnittstellen verworfen werden.

i) **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.

j) **Schwellenwert für aktive Dienste**. Der Schwellenwert des Prozentsatzes der Dienste, die aktiv sein müssen, die an den virtuellen Server gebunden sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Klicken Sie auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Analysen zur Anwendungssicherheit

February 5, 2024

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-Attacken, Small Window-Angriffe und DNS-Flood-Angriffe für die erkannten Citrix ADC-Instanzen an.

> **Hinweis**
>
> Um die Metriken des App Security Dashboards anzuzeigen, sollte AppFlow for Security Insight auf den Citrix ADC Instanzen aktiviert sein, die Sie überwachen möchten.

So zeigen Sie die Sicherheitsmetriken einer Citrix ADC Instanzen auf dem App-Sicherheits-Dashboard an:

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Application Delivery Management ein (z. B. http://192.168.100.1).
2. Geben Sie unter **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Anwendungen** > **App Security Dashboard** und wählen Sie die Instanz-IP-Adresse aus der Dropdownliste **Geräte** aus.

Sie können die im App Security Investigator gemeldeten Diskrepanzen weiter aufgliedern, indem Sie auf die im Diagramm gezeichneten Blasen klicken.

Erstellen einer Anwendungsdefinition

February 5, 2024

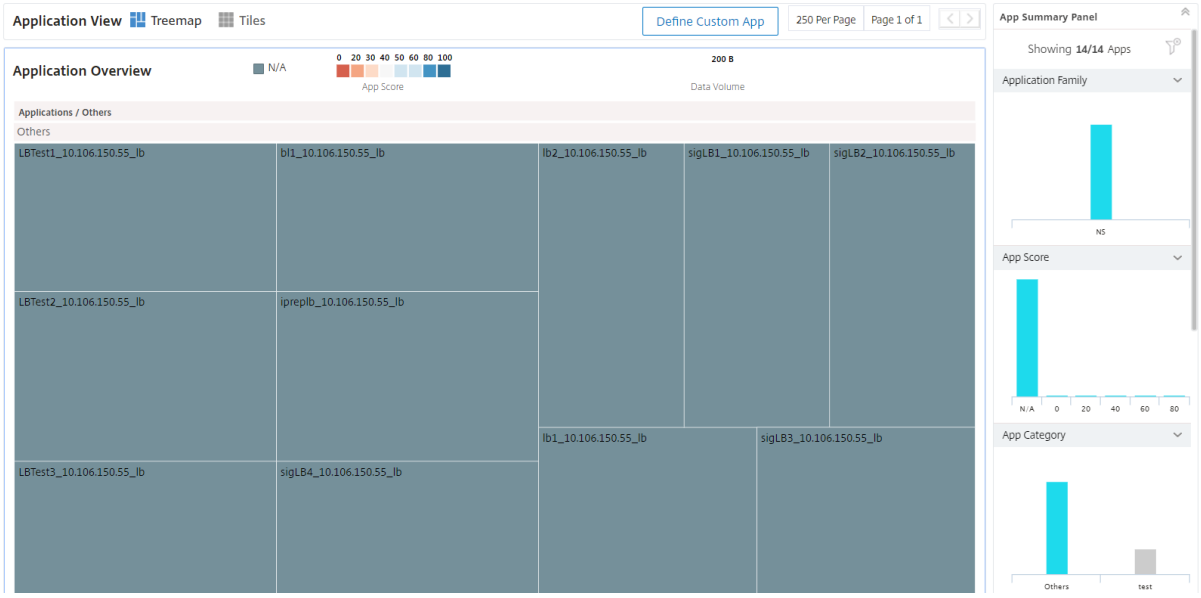
Sie können eine benutzerdefinierte Anwendung basierend auf einer Sammlung erkannter Anwendungen in Citrix ADM definieren.

Wenn Sie in Citrix ADM zum **Anwendungs-Dashboard**navigieren, werden auf der Seite **Anwendungsübersicht** Standardanwendungen angezeigt. Diese Standardanwendungen oder diskrete Anwendungen sind die 30 Anwendungen, für die Sie die Standardlizenzen haben. Sie erkennen diese Anwendungen, wenn Sie Citrix ADM in Ihrer Unternehmensumgebung installieren.

Wenn Sie benutzerdefinierte Anwendungen erstellen, ersetzen die benutzerdefinierten Anwendungen die diskreten Anwendungen. Die benutzerdefinierten Anwendungen werden auf dem Dashboard entsprechend der Kategorie angeordnet, die Sie beim Erstellen ausgewählt haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können diese Anwendungen, sowohl entdeckt als auch benutzerdefinierte, auf zwei Arten anzeigen - Treemap und Kacheln.



Sie können eine benutzerdefinierte Anwendung entweder über eine statische oder dynamische Konfiguration erstellen.

1. **Statische Definition von Anwendungen** - In einer statischen Definition können Sie eine Anwendung definieren. Diese Definition wird nicht aktualisiert, wenn neue virtuelle Server auf der Citrix ADC Instanz konfiguriert sind. Sie müssen diese Liste manuell aktualisieren, um weitere virtuelle Server einzuschließen.
2. **Dynamische Definition von Anwendungen** - In einer dynamischen Definition können Sie eines der drei unten aufgeführten Kriterien verwenden, um eine Anwendung zu definieren:

    a) **Server**: Geben Sie die Server- oder Dienst-IP-Adresse, 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.

    b) **Virtuelle Server**. Sie können eine der folgenden Optionen angeben:

        i. IP-Adresse des virtuellen Servers

        ii. Name des virtuellen Servers oder

        iii. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. **StyleBooks**. Sie können benutzerdefinierte Anwendungen erstellen, indem Sie entweder ein Standard- oder ein benutzerdefiniertes StyleBook verwenden, das bereits im Citrix ADM vorhanden ist. StyleBooks vereinfachen die Verwaltung komplexer NetScaler ADC Konfigurationen für Ihre Anwendungen. Wählen Sie ein StyleBook aus, das in Citrix ADM vorhanden ist, und geben Sie die StyleBook-Parameterwerte ein. Citrix ADM erstellt die Konfiguration (configpack) auf den Citrix ADC Zielinstanzen basierend auf dem ausgewählten StyleBook. Citrix ADM erstellt außerdem eine benutzerdefinierte Anwendung, die alle im Configpack definierten virtuellen Server enthält.

> **Hinweis**
>
> Eine benutzerdefinierte Anwendung und ein Konfigurationspaket werden erstellt, wenn ausreichende Citrix ADC Lizenzen verfügbar sind.

Wenn Sie eine Anwendung erstellen, die diese oben definierten Bedingungen in einem der drei Kriterien erfüllt, wird die Anwendung automatisch im Application Dashboard aktualisiert, wenn Citrix ADM die Entitäten abfragt. Um eine Umfrage manuell zu starten, klicken Sie auf der Registerkarte **Anwendungen** auf **Jetzt abfragen**.

So erstellen Sie eine Anwendung

1. Navigieren Sie in NetScaler ADM zu **Anwendungen** > **Dashboard** und klicken Sie auf **Benutzerdefinierte App definieren**, um eine benutzerdefinierte Anwendung zu erstellen.
2. Geben **Sie im Fenster 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. Sie können eine benutzerdefinierte Anwendung mit einer der folgenden drei Methoden erstellen:

    a) **Wählen Sie Vorhandene Anwendungen**aus. Um vorhandene Anwendungen auszuwählen, stellen Sie sicher, dass die **Option Vorhandene Anwendungen auswählen** aktiviert ist. Wählen Sie die Anwendung aus der Liste im Abschnitt **Anwendungen** aus. Klicken Sie auf **Anwendungen hinzufügen**, um der Liste neue Anwendungen hinzuzufügen.

    b) **Definieren Sie Auswahlkriterien**. Sie können auch ein Auswahlkriterium definieren, um Anwendungen in Citrix ADM hinzuzufügen. Sie können Apps mit einer der folgenden drei Methoden hinzufügen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

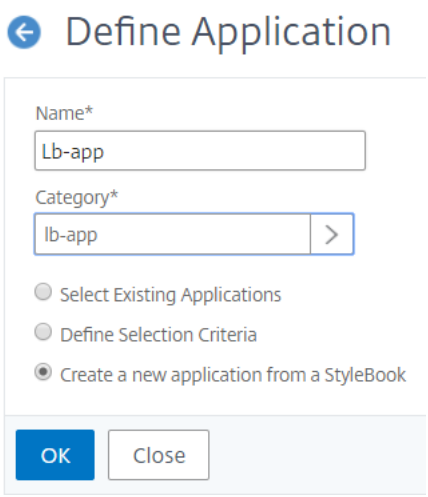
i. Geben Sie die IP-Adresse des virtuellen Servers an. Sie können eine IP-Adresse oder einen Bereich von IP-Adressen oder eine Kombination von beiden durch Kommas getrennt eingeben.

ii. Geben Sie den Namen des Servers an, auf dem die Anwendungen oder Dienste ausgeführt werden.

> **Hinweis**
>
> Sie können auch nach Servernamen suchen, indem Sie Platzhalterweiterungen verwenden. Beispielsweise fügt ssl* alle virtuellen SSL-Server zur Anwendung hinzu.

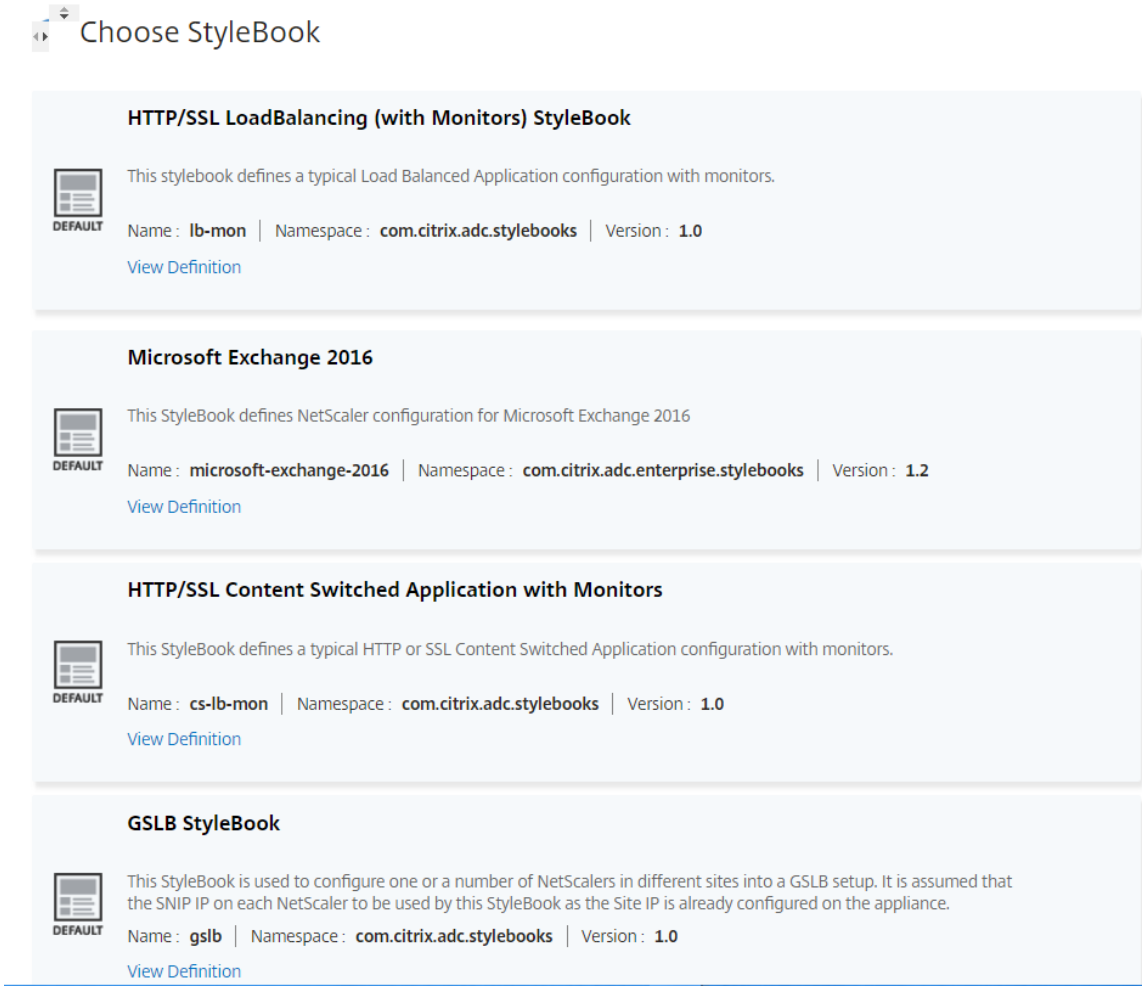
iii. Angeben der Portnummer, an der die Anwendung auf dem ausgewählten Server abhört.

c) **Erstellen Sie eine neue Anwendung aus StyleBook**. Wählen Sie das erforderliche StyleBook in Citrix ADM aus, um Config Packs auf den Citrix ADC Instanzen zu erstellen und die virtuellen Server einer benutzerdefinierten Anwendung zuzuordnen.



5. Klicken Sie auf **OK**. Wenn Sie sich für das Erstellen von Anwendungen aus StyleBooks entschieden haben, wird die Seite **StyleBook auswählen** geöffnet. Diese Seite enthält eine Liste aller StyleBooks, die in NetScaler ADM vorhanden sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



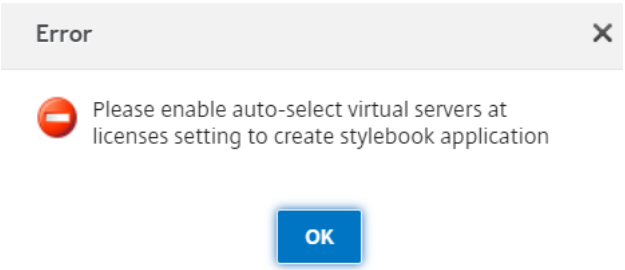
6. Wählen Sie das StyleBook aus. Das StyleBook wird als Benutzeroberflächenformular geöffnet. Geben Sie die Werte für alle Parameter im StyleBook ein. Sie können auch auf **View Definition** klicken, um das Konstrukt des StyleBook anzuzeigen, bevor Sie es verwenden. Weitere Informationen zur Verwendung von benutzerdefinierten oder standardmäßigen StyleBooks finden Sie unter Verwenden von Standard-StyleBooks.
7. Eine benutzerdefinierte Anwendung und das Konfigurationspaket werden nun auf den Citrix ADC Instanzen erstellt, die Sie im Zielabschnitt im StyleBook ausgewählt haben.

> **Hinweis:**
>
> Eine benutzerdefinierte Anwendung und ein Konfigurationspaket werden erstellt, wenn ausreichende Citrix ADM -Lizenzen verfügbar sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

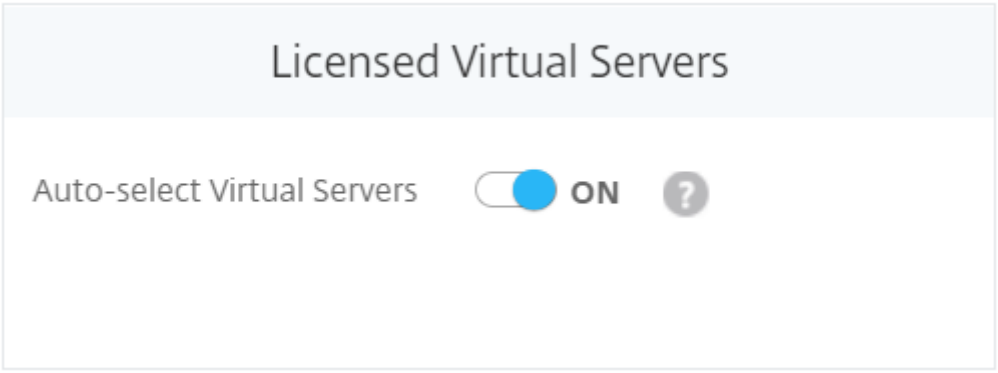
So wählen Sie virtuelle Server für die Lizenzierung automatisch aus

Sie müssen zulassen, dass NetScaler ADM die virtuellen Server für die Lizenzierung automatisch auswählen kann, wenn Sie die StyleBook-Option zum Erstellen von Konfigurationen verwenden. Wenn Sie die automatische Auswahl nicht aktiviert haben, erhalten Sie möglicherweise eine Fehlermeldung, wie im folgenden Bild gezeigt:



So aktivieren Sie die automatische Auswahl virtueller Server:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Lizenzen** > **Systemlizenzen**.
2. Klicken Sie auf **Virtuelle Server automatisch auswählen**, um die Option im Abschnitt **Lizenzierte virtuelle Server** zu aktivieren.



Wenn diese Option aktiviert ist, wählt NetScaler ADM automatisch die virtuellen Server aus, die lizenziert werden sollen. Und wenn es nicht aktiviert ist, müssen Sie die virtuellen Server explizit auswählen.

So zeigen Sie Anwendungsdetails in Citrix ADM an

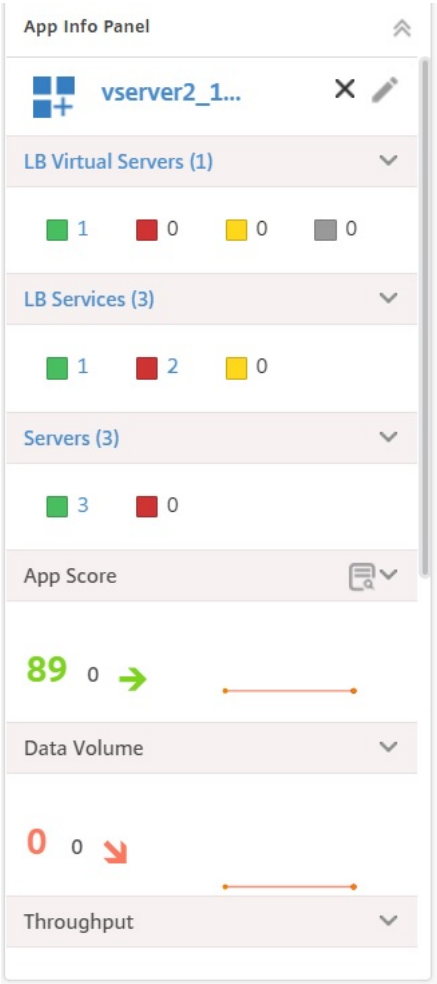
Citrix ADM zeigt alle Details einer Anwendung in einem separaten Bereich auf der rechten Seite an, der als **App-Info-Panel**bezeichnet wird.

So zeigen Sie das App-Info-Panel an:

1. Navigieren Sie in Citrix ADM zu **Anwendung** > **Dashboard**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Klicken Sie im Abschnitt **Anwendungsübersicht** auf die Anwendung, für die Sie die Details anzeigen möchten.



Die Entitäten, die an die ausgewählte Anwendung gebunden sind, werden im **Bereich App-Info** vertikal angeordnet. Vertikal angeordnete Felder im Bereich zeigen Folgendes an:

- Name jeder Entität
- die Anzahl der aktiven Entitäten
- inaktive Entitäten
- Entitäten, die außer Betrieb sind

Die Entitäten, die hier angezeigt werden, sind die virtuellen Server, Dienste, Dienstgruppen und die Anwendungsserver. Im Bereich werden auch andere Daten wie App-Score, Datenvolumen, Durchsatz, Server- und Clientverbindungen sowie die Transaktionen angezeigt, die in jeder Anwendung stattfinden.

Sie können die Anzahl der virtuellen Server, Dienste und Dienstgruppen anzeigen, die sich in unterschiedlichen Zuständen für jede Anwendung befinden. Sie können auf den Namen der Entität oder

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

die angezeigte Anzahl klicken, um die Entitäten direkt zu aktivieren oder zu deaktivieren. Sie können auch andere gebundene Entitäten wie virtuelle Server, Dienste und Dienstgruppen aktivieren oder deaktivieren.

Weitere Informationen zum Konfigurieren von Lastausgleichsservern finden Sie unter Erstellen von Lastausgleichsunterstützung über das Anwendungs-Dashboard.

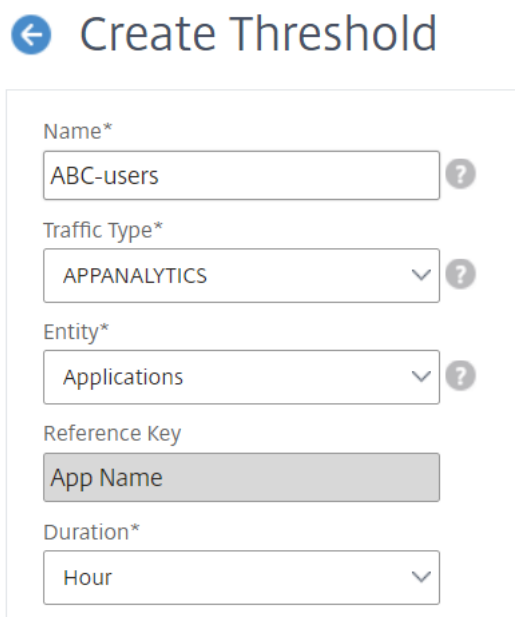
Schwellenwert und Warnung für Anwendungsanalysen erstellen

February 5, 2024

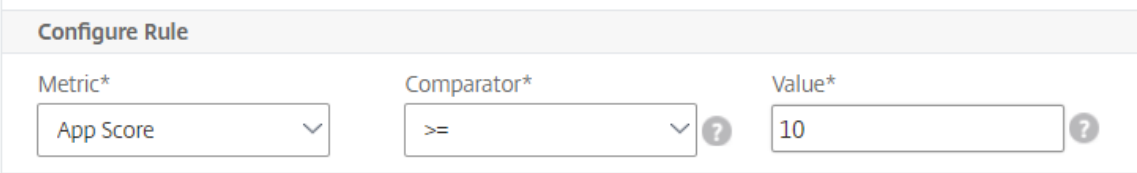
Mit der Anwendungsanalyse auf Citrix ADM können Sie die verschiedenen Arten von Datenverkehr überwachen, der durch Citrix-Instanzen geleitet wird. Mit NetScaler ADM können Sie Schwellenwerte für verschiedene Leistungsindikatoren festlegen, die zur Überwachung des Datenverkehrs verwendet werden. Sie können auch Regeln konfigurieren und Warnungen in Citrix ADM erstellen.

1. Navigieren Sie in NetScaler ADM zu **Analytics** > **Einstellungen** > **Schwellenwerte**. Klicken Sie auf der Seite **Schwellenwerte** auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwert erstellen** die folgenden Details an:
    a) **Name**. Geben Sie einen Namen zum Erstellen eines Ereignisses ein, für das Citrix ADM eine Warnung generiert.
    b) **Traffic Type**. Wählen Sie im Listenfeld APPANALYTICS aus.
    c) **Entität**. Wählen Sie im Listenfeld die Kategorie oder den Ressourcentyp aus. Standardmäßig wird Anwendungen als Entität ausgewählt.
    d) **Reference Key**. 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.

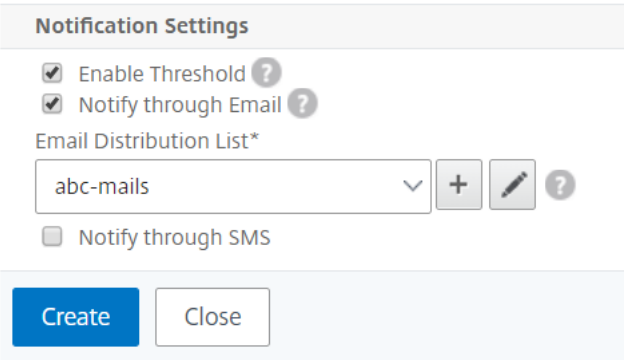
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Erstellen Sie im Abschnitt **Regel konfigurieren** eine Regel, indem Sie die **App-Score**-Metrik, einen erforderlichen Komparator, auswählen und einen Schwellenwert angeben.



4. Klicken Sie auf **Schwellenwert aktivieren**, damit Citrix ADM mit der Überwachung der Entitäten beginnen kann.
5. Konfigurieren Sie optional Aktionen wie E-Mail-Benachrichtigungen und SMS-Benachrichtigungen. Klicken Sie auf **Erstellen**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 auf einem Citrix ADC und dem gewünschten Zustand, den Sie angegeben haben, und nimmt die erforderlichen Änderungen an der Infrastruktur vor. Da StyleBooks eine deklarative Syntax verwenden, die in YAML geschrieben wird, können Komponenten eines StyleBook in beliebiger Reihenfolge angegeben werden, und NetScaler ADM bestimmt die richtige Reihenfolge basierend auf den berechneten Abhängigkeiten.
- **Atomic**: Wenn Sie StyleBooks zum Bereitstellen von Konfigurationen verwenden, wird die vollständige Konfiguration bereitgestellt oder keine davon bereitgestellt. Dadurch wird sichergestellt, dass die Infrastruktur immer in einem konsistenten Zustand bleibt.
- **Versioniert**: Ein StyleBook hat einen Namen, einen Namespace und eine Versionsnummer, die es eindeutig von jedem anderen StyleBook im System unterscheidet. Jede Änderung an einem StyleBook erfordert eine Aktualisierung seiner Versionsnummer (oder seines Namens oder Namespace), um dieses eindeutige Zeichen zu erhalten. Mit dem Versionsupdate können Sie auch mehrere Versionen desselben StyleBook verwalten.
- **Composable**: Nachdem ein StyleBook definiert wurde, kann das StyleBook als Einheit zum Erstellen anderer StyleBooks verwendet werden. Sie können vermeiden, gängige 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StyleBook-Gruppen

February 5, 2024

StyleBooks in Citrix Application Delivery Management (ADM) können auf zwei Arten gruppiert werden. Sie können entweder als Standard-StyleBooks oder als benutzerdefinierte StyleBooks gruppiert werden. Sie können auch als öffentliche oder private StyleBooks gruppiert werden. In Citrix ADM können Sie alle StyleBooks anzeigen, die im System vorhanden sind. Mit Citrix ADM können Sie die StyleBooks auch sortieren und anzeigen. Sie können auch eine grafische Darstellung anzeigen, wie StyleBooks miteinander verbunden sind.

In diesem Dokument erfahren Sie auch, wie Sie benutzerdefinierte StyleBooks herunterladen und löschen. Sie können ein benutzerdefiniertes StyleBook herunterladen, um Änderungen vorzunehmen oder ein neues StyleBook zu erstellen, das auf dem früheren basiert. Sie können auch ein benutzerdefiniertes StyleBook löschen.

Standard- und benutzerdefinierte StyleBooks

- Standard-StyleBooks sind die StyleBooks, die im Citrix ADM-Dateisystem vorhanden sind und mit denen Sie Konfigurationen erstellen können, die Sie auf Ihren Citrix ADC-Instanzen bereitstellen können.
- Benutzerdefinierte StyleBooks sind Ihre eigenen StyleBooks, die Sie schreiben und in Citrix ADM importieren und Konfigurationsobjekte erstellen können.

Sowohl Standard- als auch benutzerdefinierte StyleBooks können entweder öffentlich oder privat sein.

Öffentliche und private StyleBooks

StyleBooks, aus denen Sie Konfigurationspakete für die Bereitstellung auf den Citrix ADC-Instanzen erstellen können, können als "öffentliche"StyleBooks kategorisiert werden. Das heißt, sie sind alle für Ihre direkte Verwendung zum Erstellen von Konfigurationen verfügbar.

Einige StyleBooks werden jedoch als Bausteine für andere StyleBooks verwendet. Diese Bausteine sind die integrierten StyleBooks, aus denen die Standard-StyleBooks bestehen. Solche StyleBooks werden "private"StyleBooks genannt. Obwohl sie nicht direkt zum Erstellen von Konfigurationspaketen auf den Instanzen verwendet werden, möchten Sie diese StyleBooks möglicherweise auf dem Citrix ADM anzeigen. Um ein StyleBook als privat zu markieren, können Sie das private Attribut verwenden, um zu verhindern, dass ein StyleBook im Citrix ADM aufgeführt wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

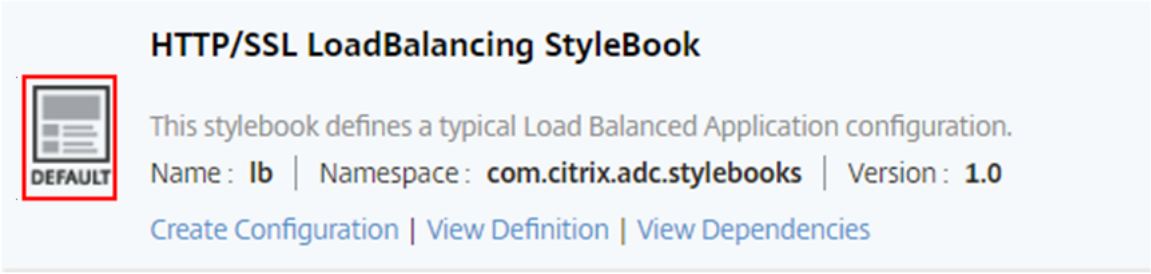
```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
    configuration and is a building block to build other load balancing
    configurations.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

StyleBooks anzeigen

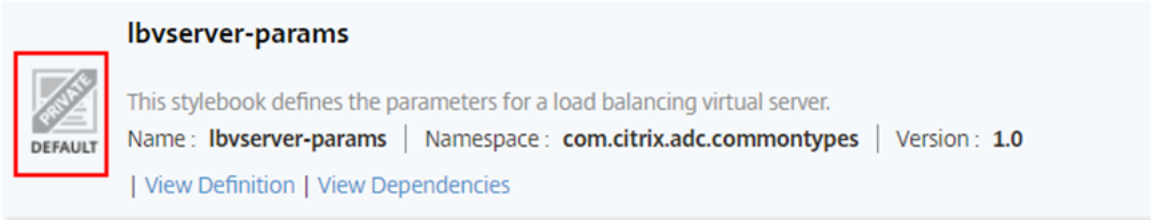
Die Anzahl der StyleBooks - sowohl Standard als auch privat - nimmt in Citrix ADM zu. Vielleicht möchten Sie nach dem bestimmten StyleBook suchen, auf das Sie zugreifen möchten. Möglicherweise möchten Sie auch beide Arten von StyleBooks separat anzeigen.

Wenn Sie in Citrix ADM zu **Anwendungen** > **StyleBooks** navigieren, können Sie eine Liste der StyleBooks anzeigen, die im System vorhanden sind.

Ein standardmäßiges öffentliches StyleBook hat das folgende Symbol im Bedienfeld:



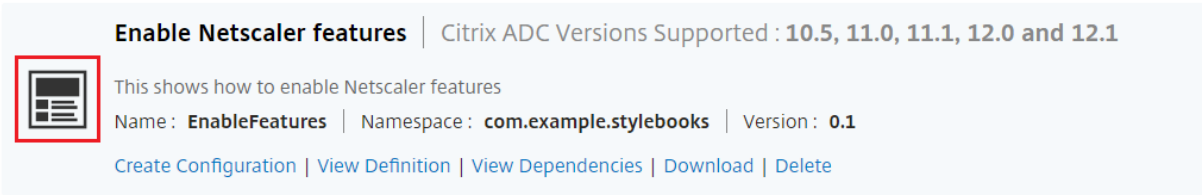
Wohingegen ein standardmäßiges privates StyleBook ein Symbol hat, das es als privates StyleBook deklariert:



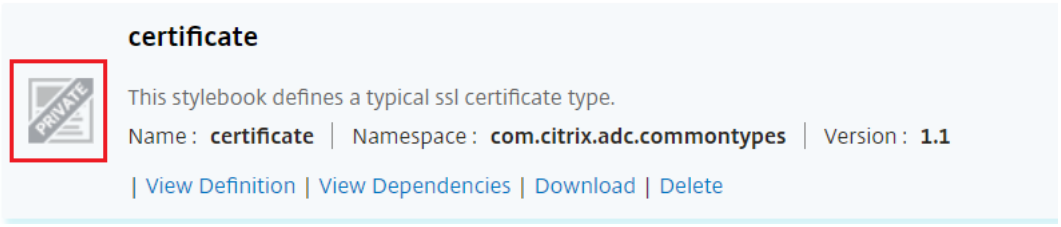
Sie können zwar die Definition und Abhängigkeiten eines privaten StyleBook anzeigen, aber Sie können kein Konfigurationspaket aus einem privaten StyleBook erstellen. Sie können weiterhin ein privates StyleBook in Ihrem eigenen StyleBook verwenden.

Ein benutzerdefiniertes öffentliches StyleBook hat ein anderes Symbol, wie in der folgenden Abbildung gezeigt:

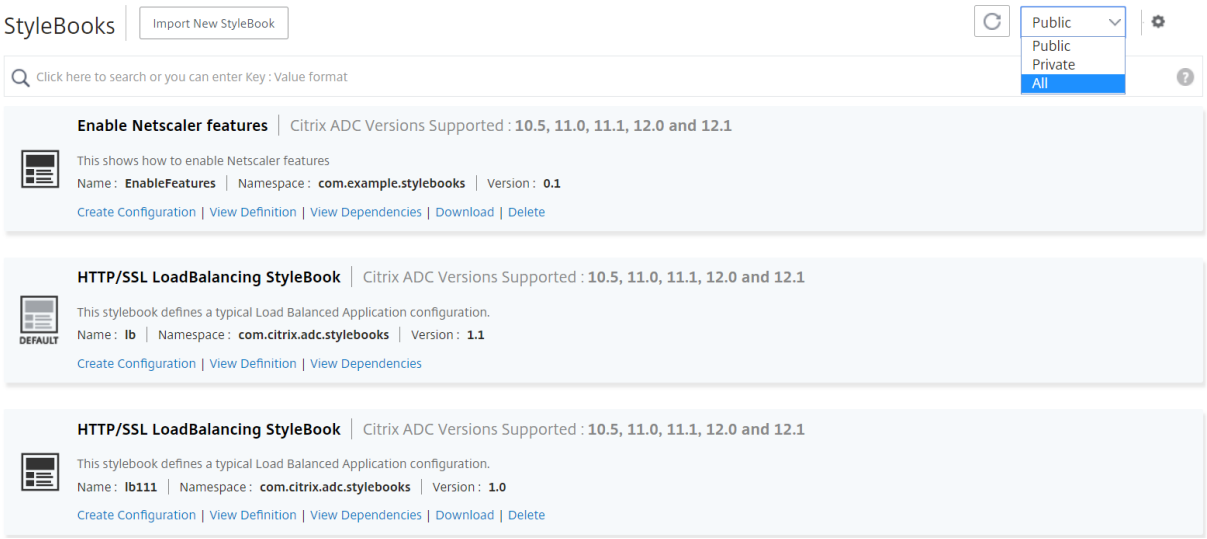
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Während wird ein benutzerdefiniertes privates StyleBook mit folgendem Symbol angezeigt:

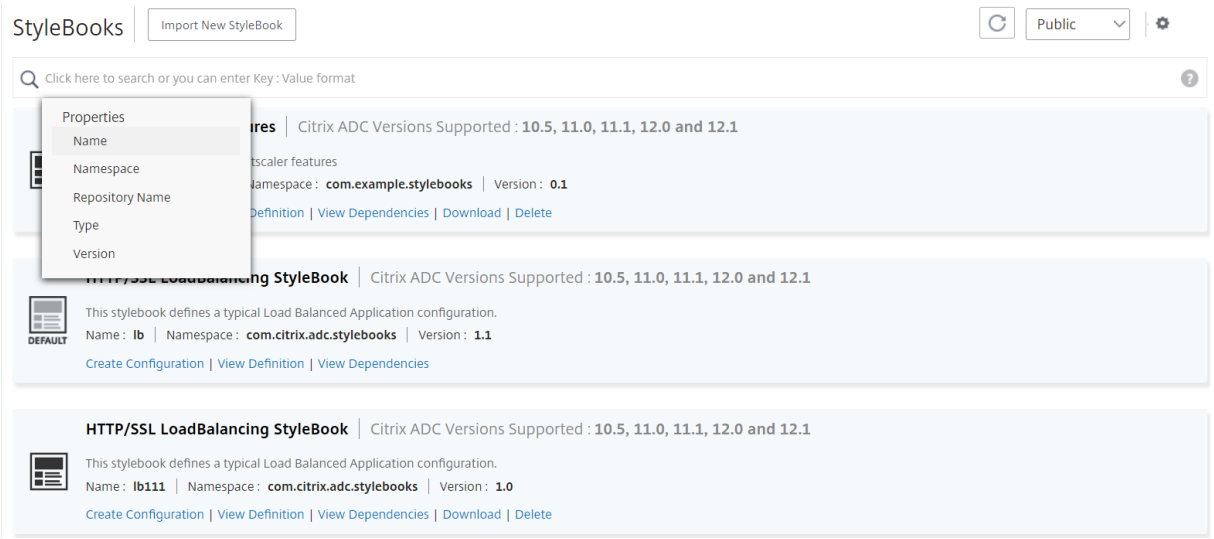


Oben rechts auf der Seite sehen Sie eine Option zum Sortieren der StyleBooks. Es gibt drei Optionen - alle, öffentliche oder private StyleBooks. Klicken Sie auf eine der Optionen.



Sie können auch nach einem bestimmten StyleBook suchen, indem Sie auf das Suchsymbol klicken. Die drei verfügbaren Suchoptionen sind Name, Namespace und Version. Bei der Suche wird die Groß- und Kleinschreibung nicht berücksichtigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Anzeigen von StyleBook-Abhängigkeiten

Mit NetScaler ADM können Sie eine grafische Darstellung der Verbindung von StyleBooks anzeigen.

In Citrix ADM können Sie entweder die Standard-StyleBooks verwenden, um Konfigurationen für Ihre Bereitstellung zu erstellen. Sie können auch Ihre eigenen StyleBooks entwerfen und sie in Citrix ADM importieren.

Eine wichtige und leistungsstarke Funktion von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können. Sie können ein StyleBook in ein anderes StyleBook importieren. Ein importiertes Stylebook wird als Typ deklariert und von Komponenten oder Parametern des zweiten StyleBook verwendet.

Ein StyleBook, das von anderen StyleBooks verwendet wird, kann nicht aus dem System entfernt werden. Durch eine grafische Anzeige von StyleBooks können Sie jedoch feststellen, welche StyleBooks das Entfernen eines StyleBook verhindern. Wenn Sie sich das Diagramm ansehen, können Sie die Beziehungen zwischen mehreren StyleBooks erkennen.

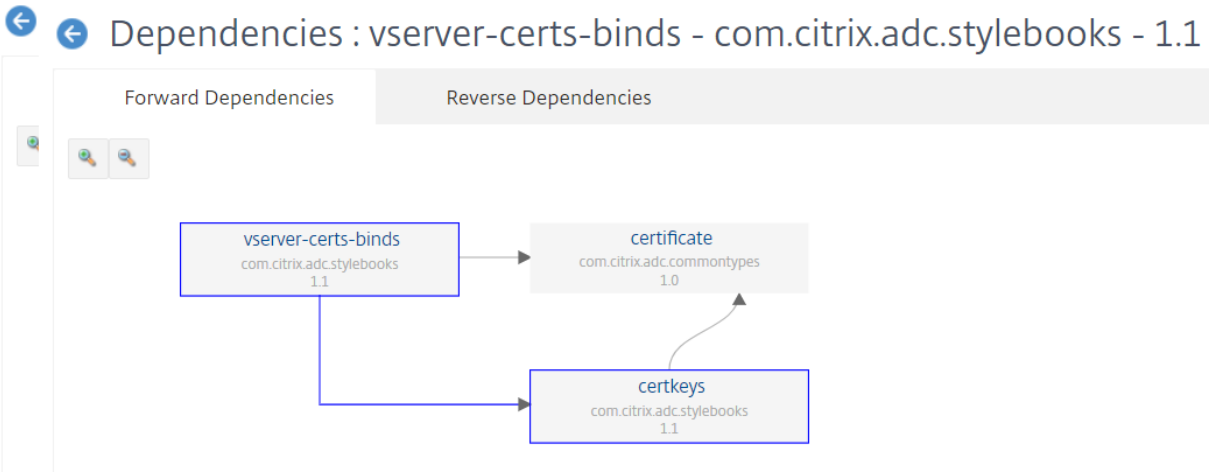
StyleBook-Abhängigkeiten anzeigen

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. Das StyleBook-Bedienfeld zeigt Links zum Erstellen einer Konfiguration, zum Anzeigen der StyleBook-Definition und zum Anzeigen der StyleBook-Abhängigkeiten an. Klicken Sie **auf Abhängigkeiten anzeigen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

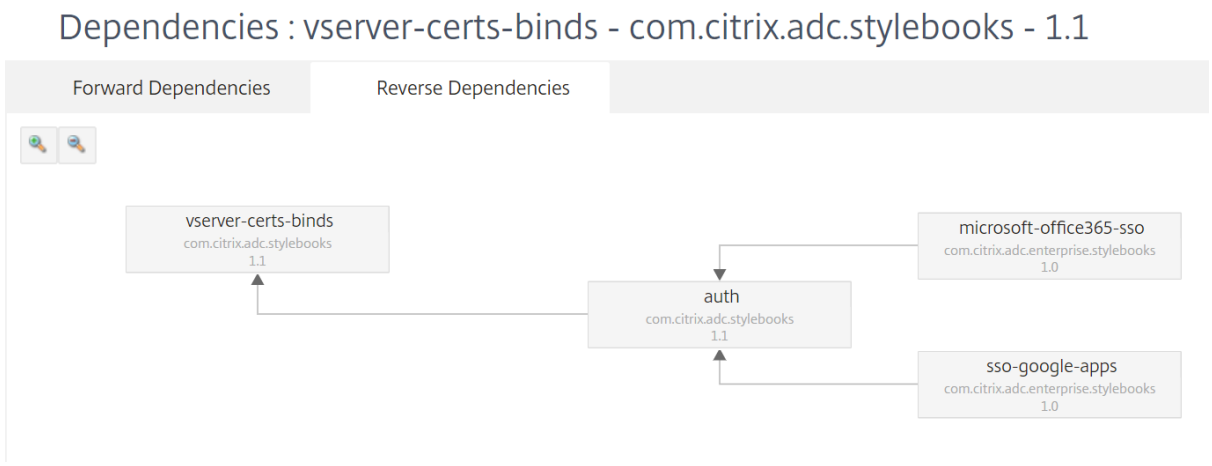
Vorwärtsabhängigkeiten

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 im Display auf Ihr StyleBook zeigen. Einige StyleBooks verwenden möglicherweise direkt das StyleBook und einige StyleBooks verwenden das StyleBook möglicherweise über ein anderes StyleBook.

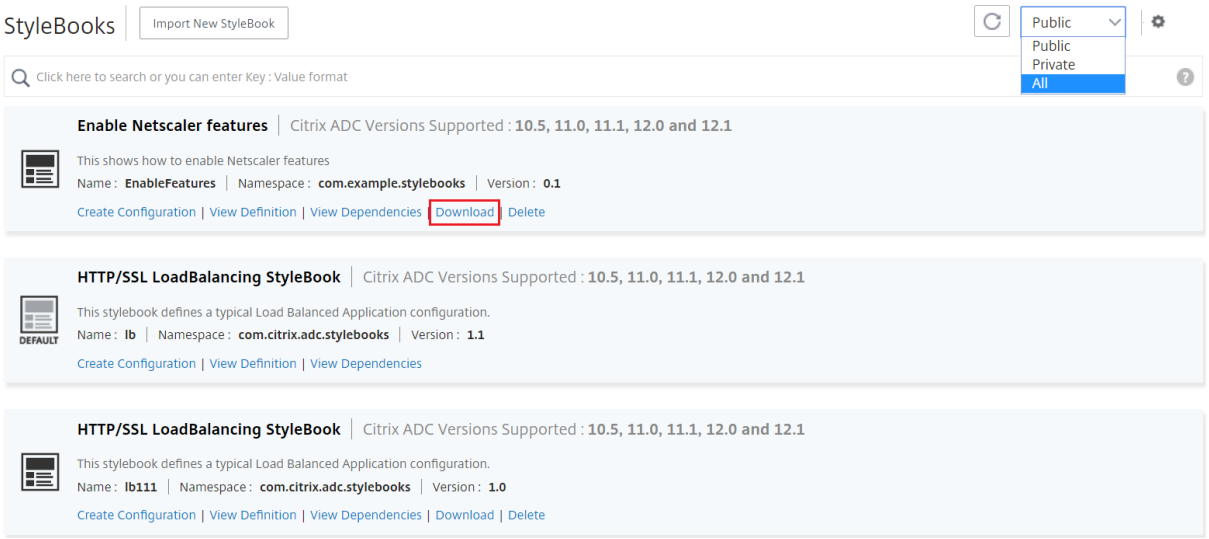


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Herunterladen benutzerdefinierter StyleBooks

Um benutzerdefinierte Stylebooks von Citrix ADM herunterzuladen, navigieren Sie zu **Anwendungen** > **StyleBooks** > **Konfigurationen**. In der Liste der StyleBooks, die auf der rechten Seite angezeigt werden, haben die benutzerdefinierten StyleBooks die Möglichkeit, sie herunterzuladen. Klicken Sie auf **Download**. Wenn das StyleBook abhängige benutzerdefinierte StyleBooks hat, werden auch diese StyleBooks auf Ihr System heruntergeladen.

> **Hinweis:**
>
> Sie können keine standardmäßigen oder benutzerdefinierten StyleBooks herunterladen, die als öffentlich oder privat markiert sind.

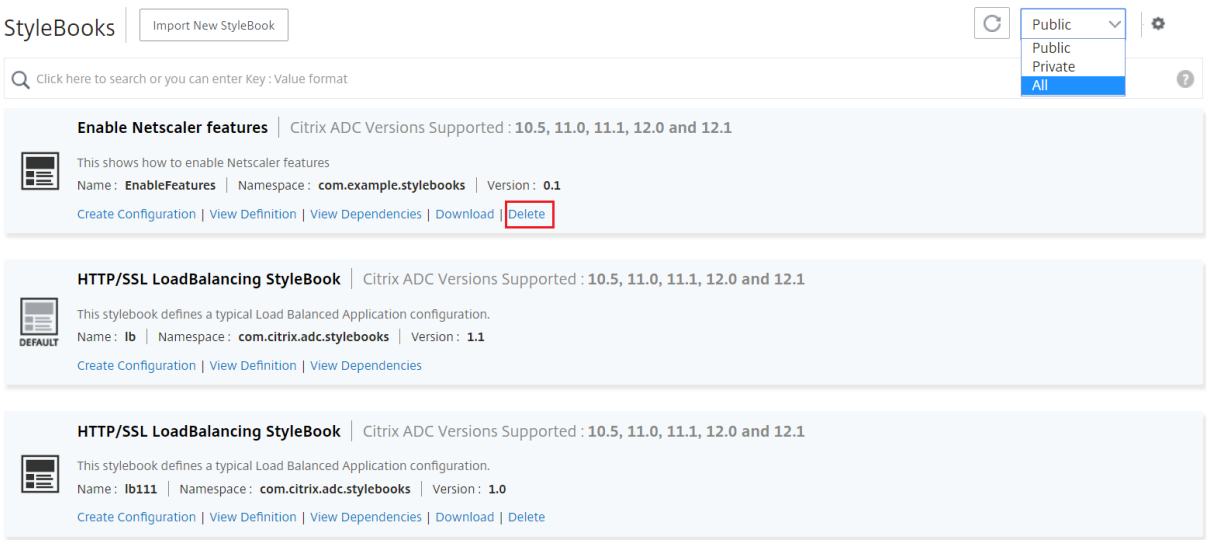


> **Hinweis**
>
> NetScaler ADM Standard-StyleBooks können nicht heruntergeladen werden. Sie können jedoch ihre Definitionen und Abhängigkeiten anzeigen, indem Sie im StyleBook-Bedienfeld auf die Links **Definition anzeigen** und **Abhängigkeiten anzeigen** klicken.

Benutzerdefinierte StyleBooks löschen

Sie können benutzerdefinierte StyleBooks auch löschen, indem Sie auf das Symbol „X“auf der rechten Seite des StyleBook-Bedienfelds 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 (die nicht von anderen StyleBooks verwendet werden), können Sie diese auch entfernen, indem Sie das Kontrollkästchen aktivieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Sie können kein benutzerdefiniertes StyleBook löschen, das andere StyleBooks in NetScaler ADM enthält, die davon abhängen.

StyleBooks aus dem GitHub-Repository importieren und synchronizieren

February 5, 2024

Bedenken Sie, dass Sie CI/CD-Prozesse für Ihre Entwicklung verwenden oder dass Sie alle Bereitstellungsobjekte in GitHub verwalten. Möglicherweise haben Sie mehrere StyleBooks für die Bereitstellung Ihrer Citrix ADC-Konfigurationen erstellt und verwalten die StyleBooks in GitHub-Repositorys. Jetzt können Sie diese StyleBooks direkt in Citrix Applications and Delivery Management (ADM) importieren. Sie müssen sie nicht manuell aus GitHub kopieren und in Citrix ADM hochladen.

Sie können jetzt ein Repository in Citrix ADM definieren, das ein GitHub-Repository darstellt, indem Sie die GitHub-Repository-URL angeben. Sie müssen Ihren in GitHub erstellten Benutzernamen und Ihr Kennwort (oder API-Token) angeben. Das bedeutet, dass nur autorisierte Benutzer, die über ein gültiges Konto bei GitHub verfügen, StyleBooks importieren und synchronisieren können.

Nachdem Sie das Repository erstellt haben, können Sie NetScaler ADM mit Ihrem GitHub-Repository synchronisieren. Citrix ADM importiert StyleBooks, die in diesem Repository gefunden wurden, validiert sie dann und fügt sie der Liste der StyleBooks in Citrix ADM hinzu. StyleBooks werden NetScaler ADM nicht hinzugefügt, wenn die Validierung fehlschlägt. Du musst die Fehler korrigieren und aktualisierte Versionen in dein GitHub-Repository übertragen. Später können Sie versuchen, sie zu importieren oder erneut mit NetScaler ADM zu synchronisieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> - Derzeit können Sie nur StyleBooks importieren und synchronisieren, denen keine abhängigen StyleBooks zugeordnet sind. Das heißt, das StyleBook muss alle Konfigurationen haben, die es benötigt, um in einer Datei definiert zu werden.
> - Die Synchronisierung aus einem GitHub-Repository muss manuell über die Citrix ADM GUI oder API initiiert werden. Das heißt, der Import von StyleBooks erfolgt derzeit nicht automatisch basierend auf der GitHub-Commit-Aktivität.
>
> Derzeit können Sie StyleBooks-Dateien nur aus dem Master-Zweig importieren.

Voraussetzungen

- Sie müssen ein gültiges Konto in GitHub haben.
- StyleBook-Dateien müssen im Stammordner des Master-Branches im GitHub-Repository vorhanden sein.

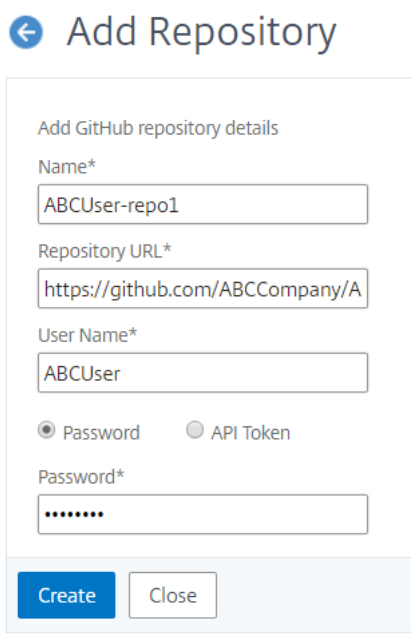
Hinzufügen eines Repositorys und Importieren von StyleBooks aus GitHub

1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfigurationen** > **Repositorys** .
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. Sie können sie auch verwenden, um sich über die Standardauthentifizierung bei der API zu authentifizieren.

3. Klicken Sie auf **Erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

- **Zurücksetzen**. Sie können alle StyleBooks in Citrix ADM synchronisiert aus diesem Repository entfernen, ohne den Repository-Eintrag tatsächlich aus Citrix ADM zu löschen.
- **Dateien auflisten**. Sie können eine Liste aller in Citrix ADM vorhandenen StyleBooks sehen, die aus dem GitHub-Repository stammen.

Standard-StyleBooks verwenden

February 5, 2024

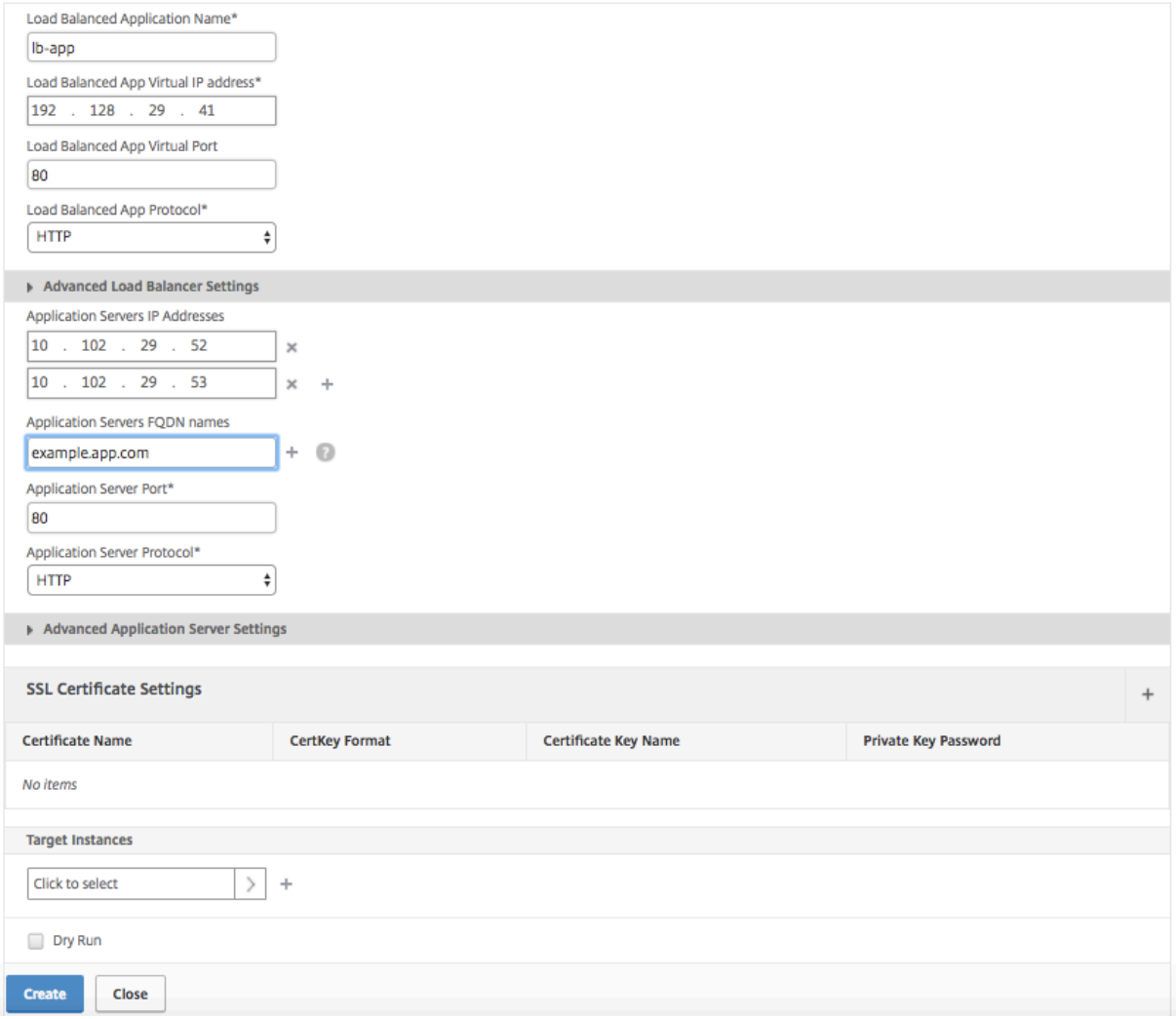
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die Liste nach unten scrollen, um das StyleBook zu finden.

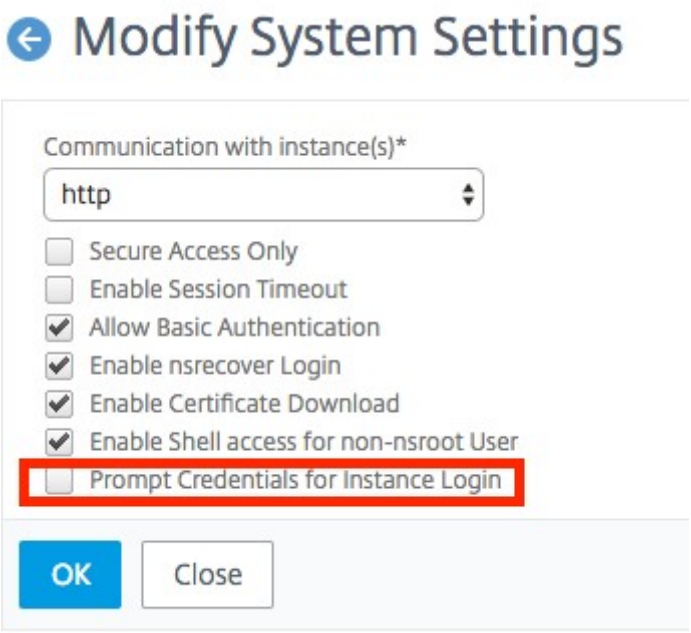
2.Klicken Sie auf **Konfiguration erstellen**. Geben Sie die erforderlichen Werte für die Parameter an.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

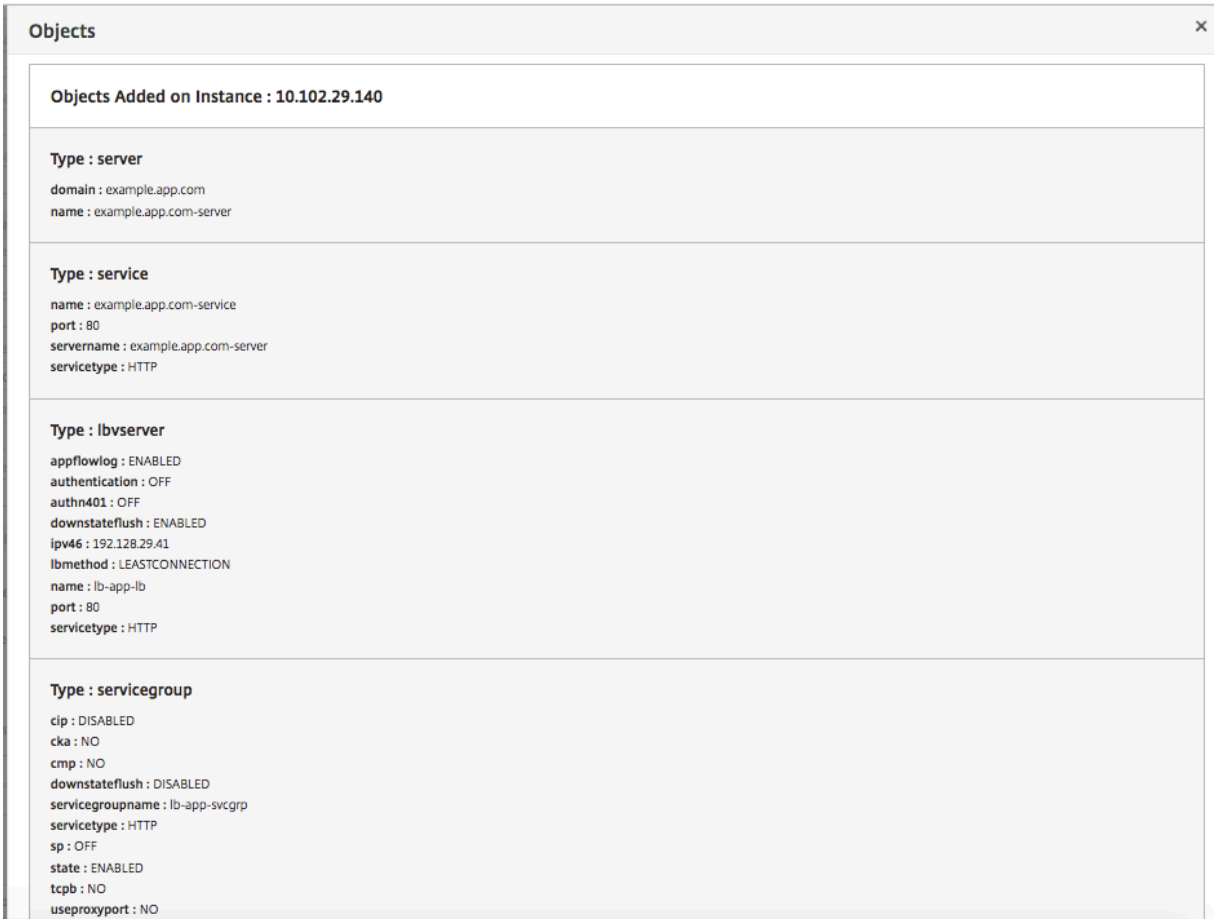
3.Wählen Sie unter **Target Instances** die IP-Adresse der NetScaler ADC-Instanz aus, in der Sie die Konfiguration ausführen möchten. Wenn Sie diese Konfiguration auf mehreren Instanzen ausführen möchten, klicken Sie auf "+", um weitere Instanzen hinzuzufügen.

Wenn die Option**Anmeldeinformationen für Instanzanmeldung auffordernunter Citrix ADM**>**System > Systemeinstellungenändern > Systemeinstellungenändern**aktiviert 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

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

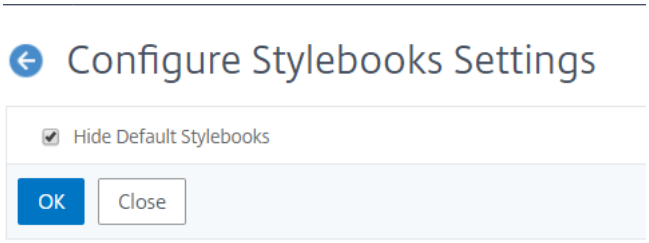
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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. 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

Konfigurationsdetails:

In der folgenden Tabelle sind die erforderlichen Mindestsoftwareversionen aufgeführt, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess sollte auch mit höheren Versionen derselben funktionieren.

Produkt	Erforderliche Mindestversion
Citrix ADC	Version 11.0, Enterprise/Platinum-Lizenz

In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und/oder internen DNS-Einträge erstellt haben, um Authentifizierungsanforderungen an eine von NetScaler ADC überwachte IP-Adresse weiterzuleiten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 AAA-Server verwendet wird, an den die Google Apps SAML-IdP-Richtlinie gebunden ist.
    c) **SAML-Regelausdruck**. Standardmäßig wird der folgende Ausdruck der Citrix ADC Richtlinie (PI) verwendet: HTTP.REQ.HEADER (Referer).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 Referer-Header von einer Google-Domain stammt.
4. Im Abschnitt SAML Idp Settings können Sie Ihre NetScaler 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.
    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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, die Standardeinstellungen beizubehalten, da diese Einstellungen für die Verwendung 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. Zum Beispiel cn=Manager, dc=netscaler, dc=com

c) **LDAP (Active Directory) Bindet DN Kennwort**. Geben Sie das Kennwort des Domänenkontos für die Authentifizierung ein.

d) Einige andere Felder, die Sie in diesem Abschnitt eingeben müssen, sind wie folgt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, das zum Extrahieren von Anmeldenamen verwendet wird, 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 die Dateierweiterungen.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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Ebenfalls

> **Tipp**
> > >
> Citrix empfiehlt, dass Sie vor der Ausführung der eigentlichen Konfiguration **Dry Run** auswählen , um die Konfigurationsobjekte, die auf den Citrix ADC-Zielinstanzen 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, Enterprise/Platinum-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.

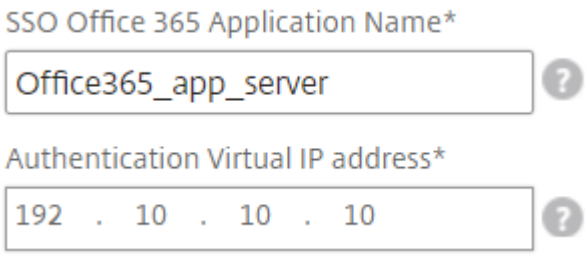
So stellen Sie SSO Microsoft Office 365 StyleBook bereit

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.

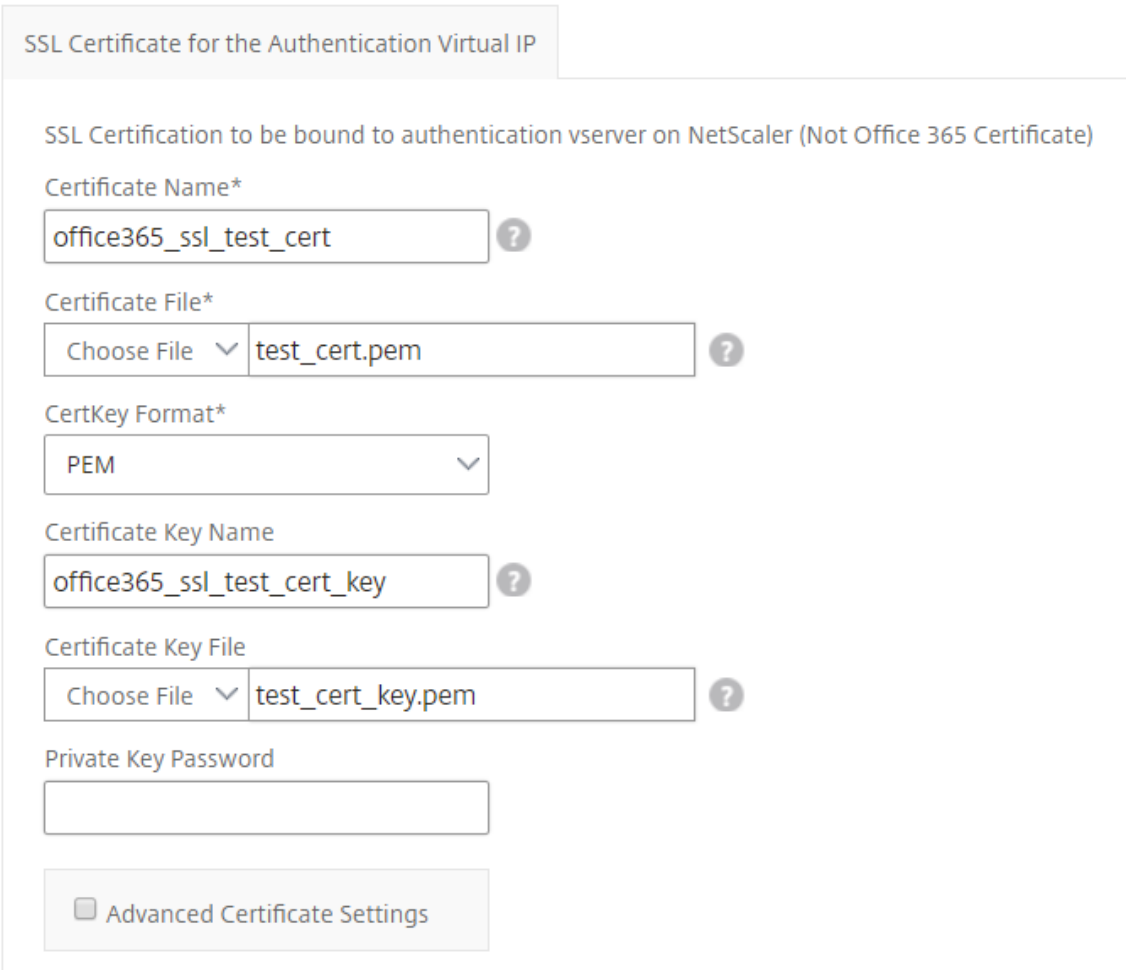
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

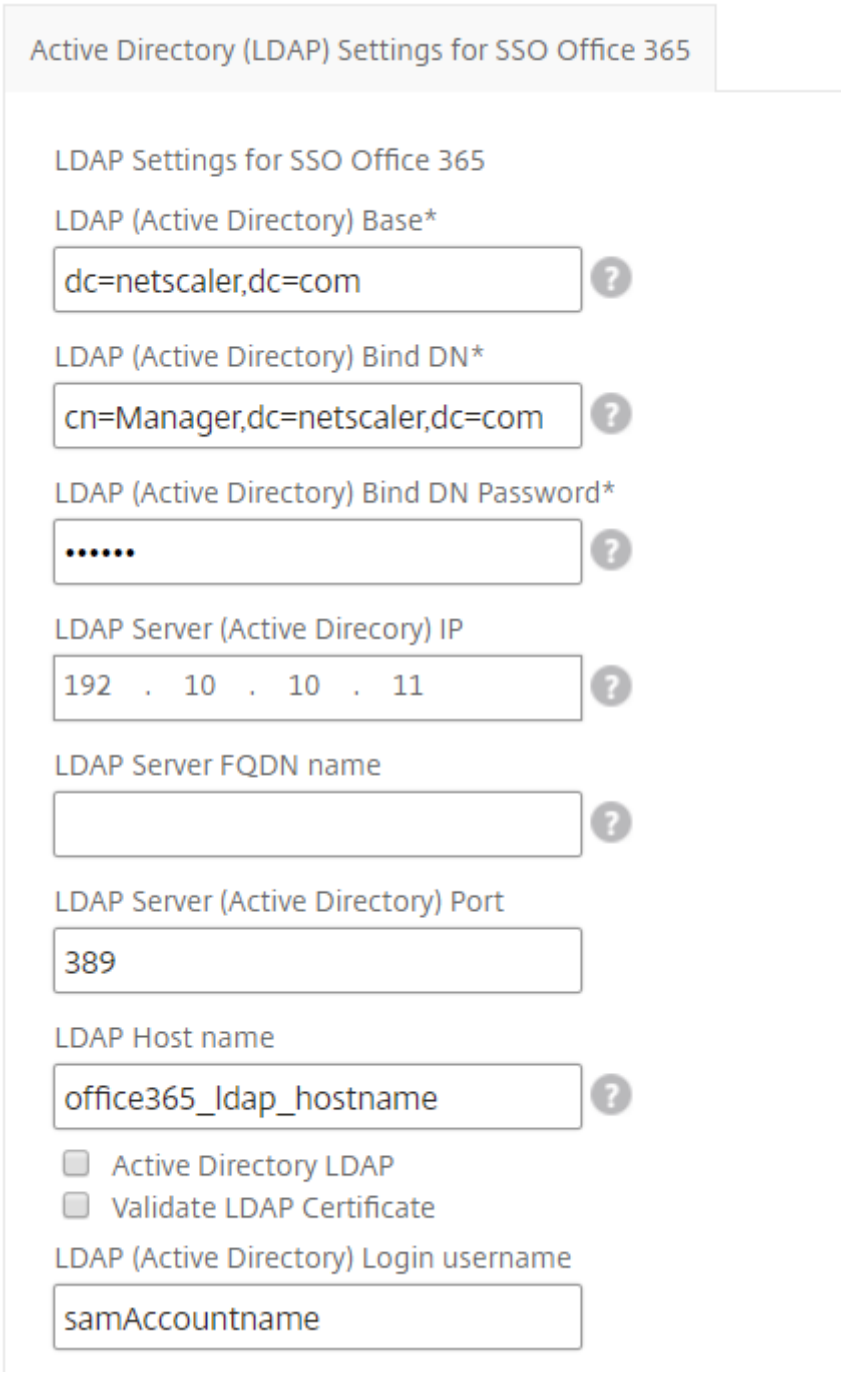
6. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.
7. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat 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 Verwendung einer E-Mail-Adresse zur Vereinfachung der Konfiguration), das über die Rechte zum Durchsuchen der AD-Struktur verfügt. Zum Beispiel cn=Manager, dc=netscaler, dc=com
   - **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



9. Im Abschnitt **SAML-IdP-Zertifikat** können Sie die Details der SSL-Zertifikate angeben, die für die SAML-Assertion verwendet werden.

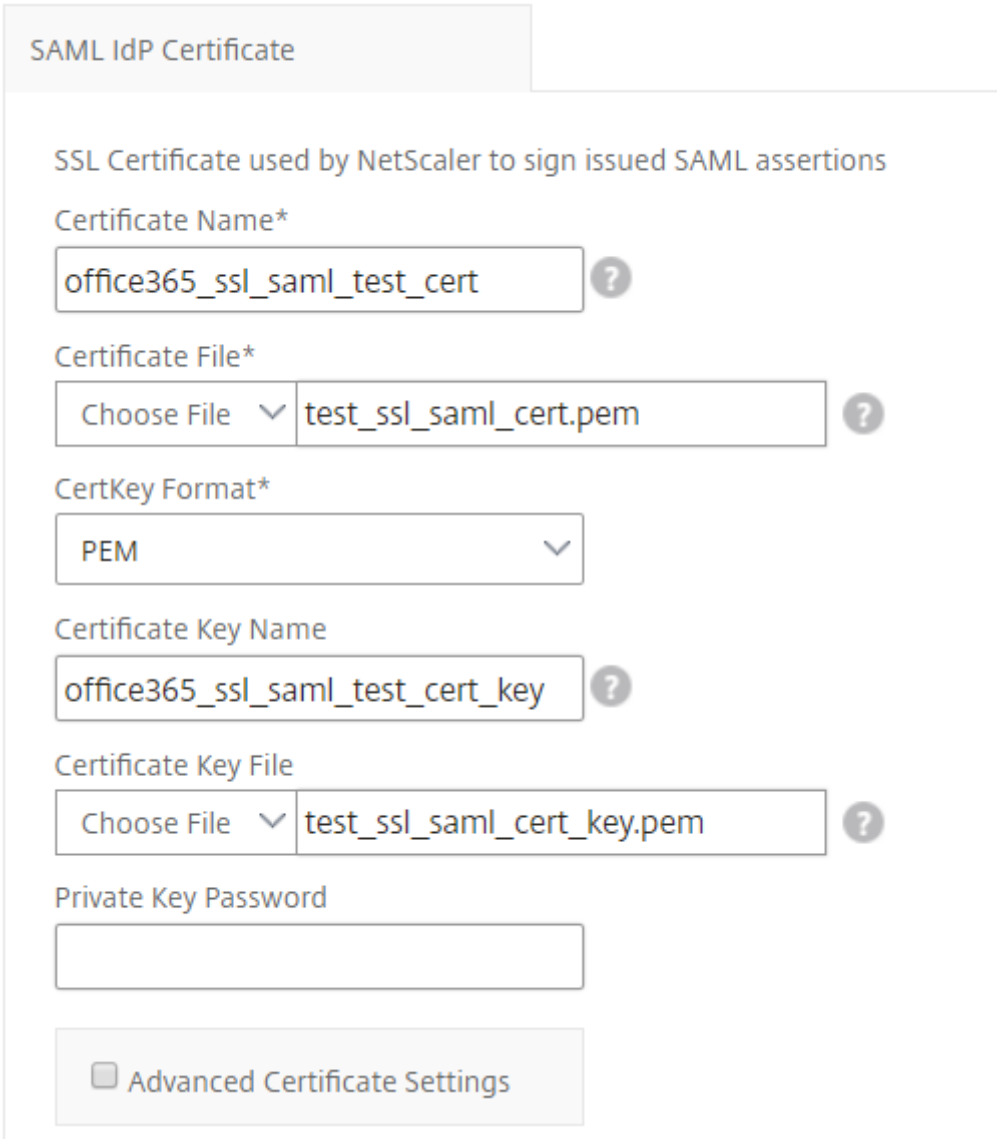
   - **Name des Zertifikats**. Geben Sie den Namen des SSL-Zertifikats ein.
   - **Zertifikatdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System.
   - **CertKey-Format**. Wählen Sie das Format des Zertifikats und der Dateien mit privatem

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

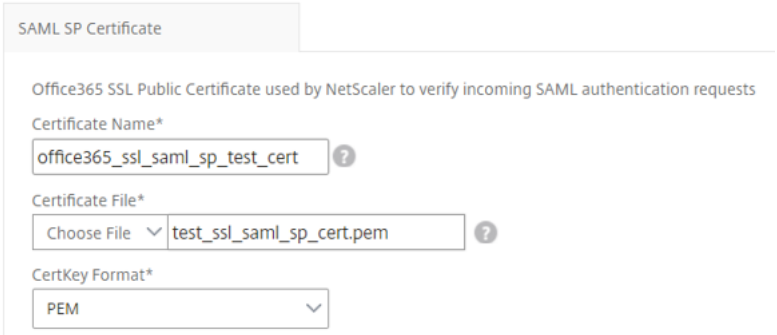
Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Ablauf der Benachrichtigung des Zertifikats eingeben, den Ablaufmonitor des Zertifikats aktivieren oder deaktivieren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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“).

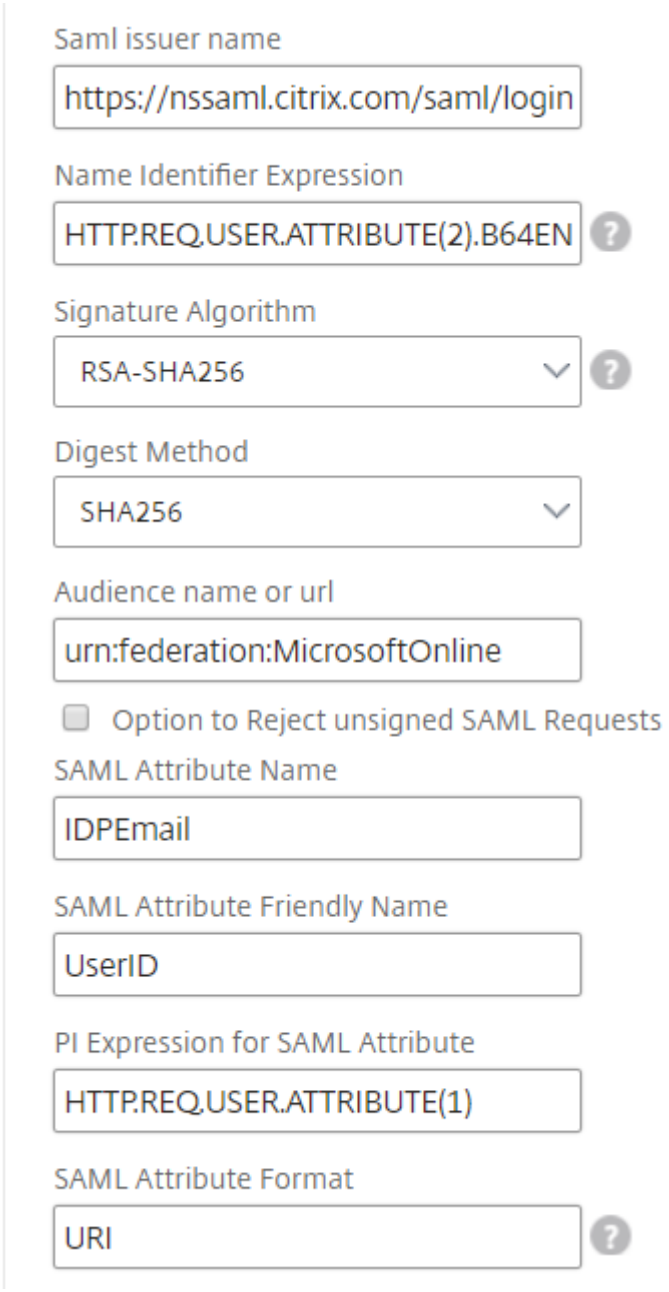
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

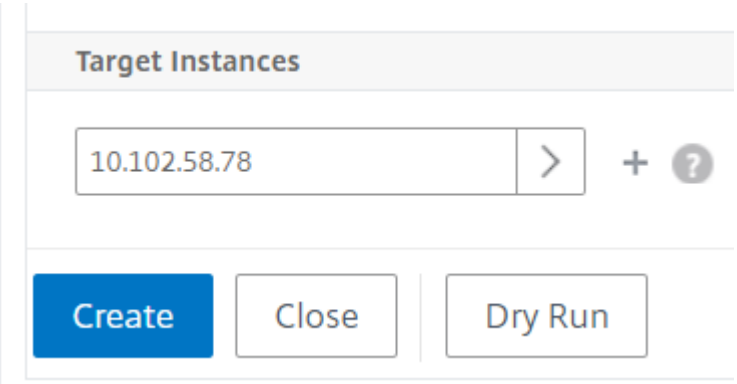
  > **Tipp**
  >
  > Citrix empfiehlt, die Standardeinstellungen beizubehalten, da diese Einstellungen für die Verwendung mit Microsoft Office 365-Apps getestet wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

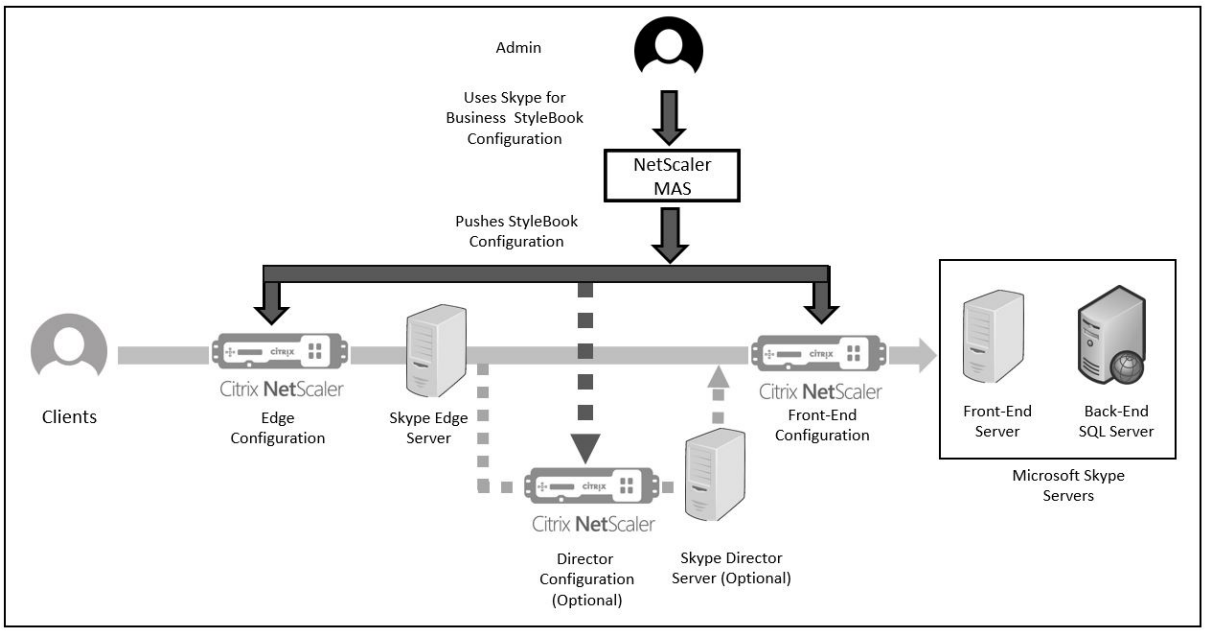
Director-Server

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

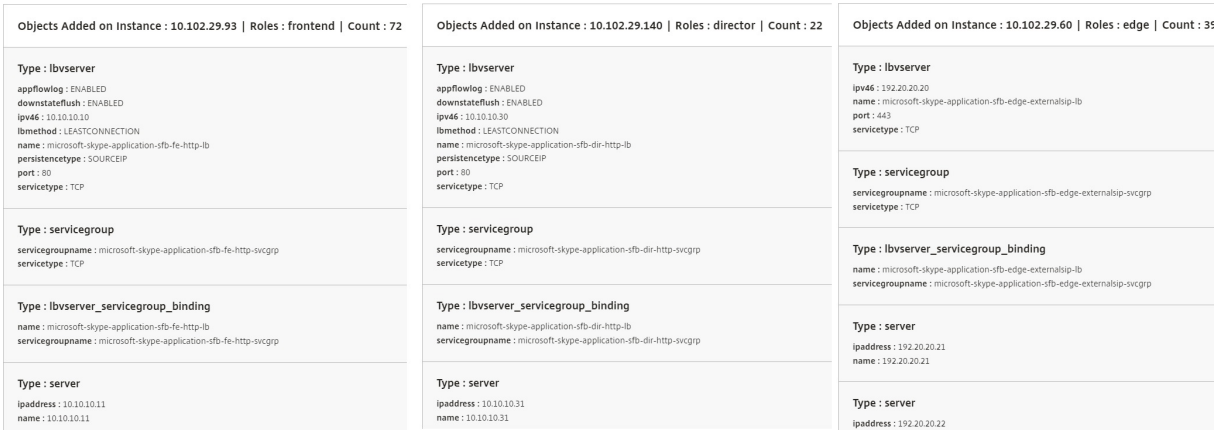
> **Hinweis**
>
> Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich erkannte Citrix ADC Instanzen in Citrix ADM zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

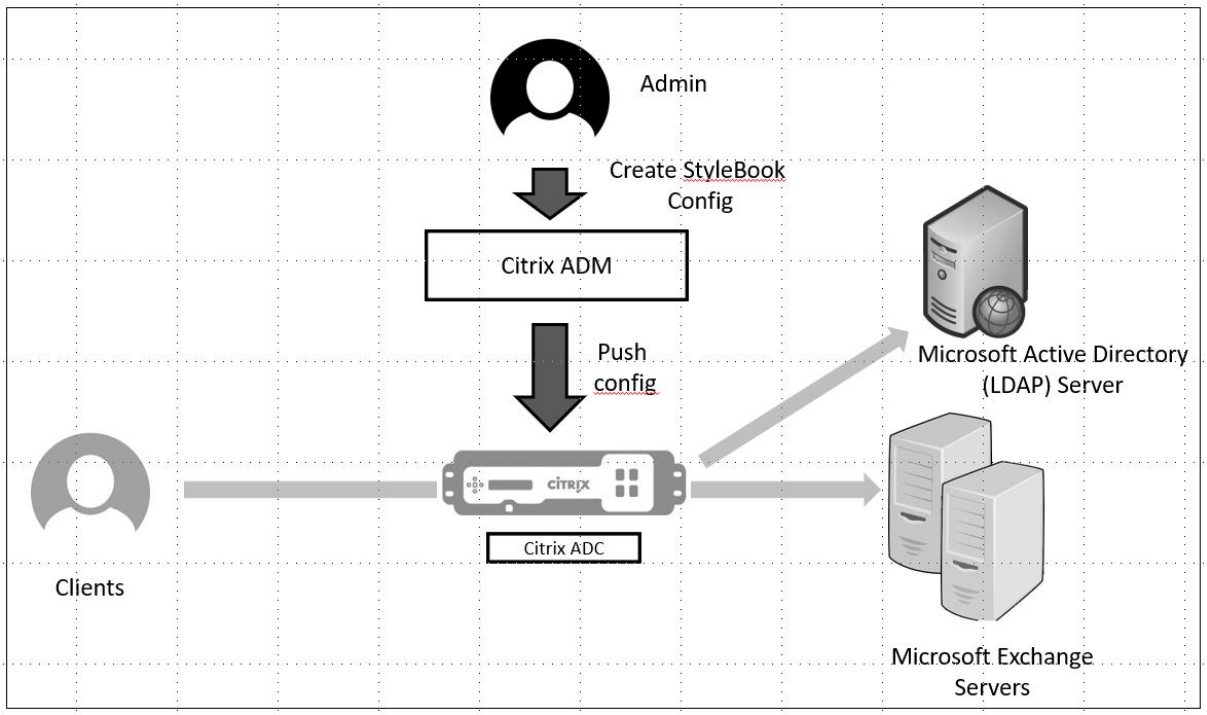
NetScaler ADC-Funktionen, die mithilfe von Microsoft Exchange StyleBook konfiguriert wurden

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

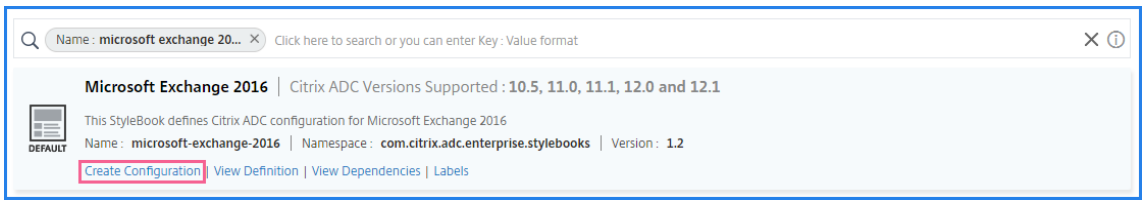
Konfigurieren Sie das Microsoft Exchange StyleBook in Ihrem Unternehmen für die Bereitstellung der NetScaler ADC-Konfiguration.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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"

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

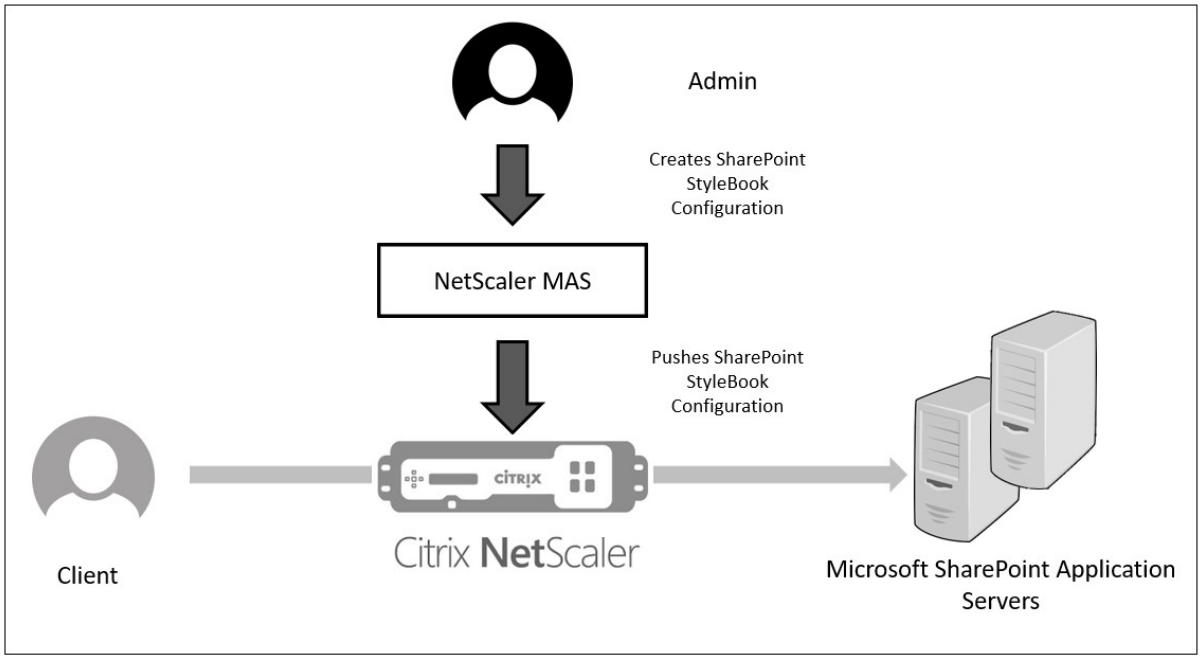
Client-Browsers, die Daten zu dekomprimieren, hängt davon ab, welchen Algorithmus oder welche Algorithmen er unterstützt: GZIP, DEFLATE oder beides.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

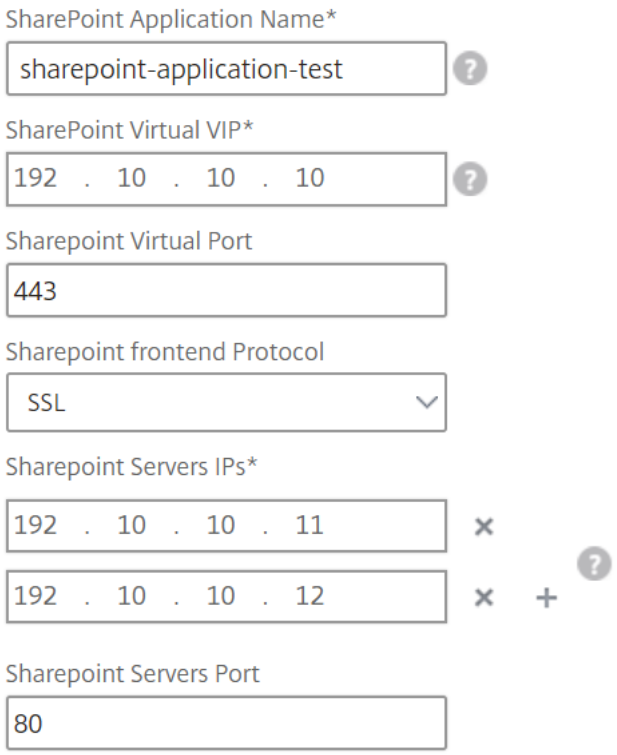
   d) **SharePoint-Frontend-Protokoll**. Wählen Sie das SharePoint-Frontend-Protokoll aus der Dropdownliste aus. Die verfügbaren Optionen sind HTTP oder SSL.

      > **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.

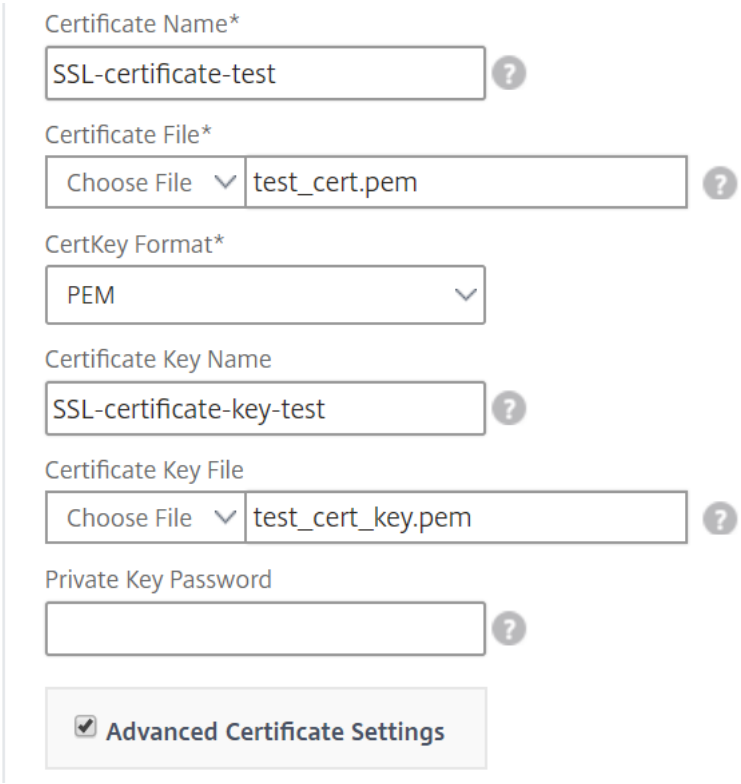
   f) **Anschluss für SharePoint-Server** Von den SharePoint-Servern verwendete TCP-Portnummer In der Standardeinstellung ist dies 80. Sie können diesen Wert bei Bedarf bearbeiten, stellen Sie jedoch sicher, dass auf diesen Port auf Microsoft SharePoint 2016-Servern zugegriffen werden kann.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

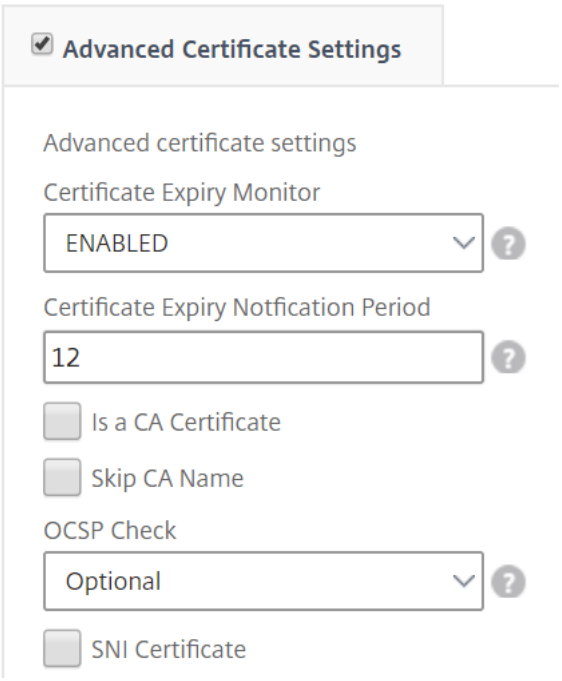


3. Klicken Sie im Abschnitt **Einstellungen für SSL-Zertifikate** auf +, um den Namen des SSL-Zertifikats und den Zertifikatschlüssel einzugeben und die entsprechenden Dateien aus Ihrem lokalen Speicherordner auszuwählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



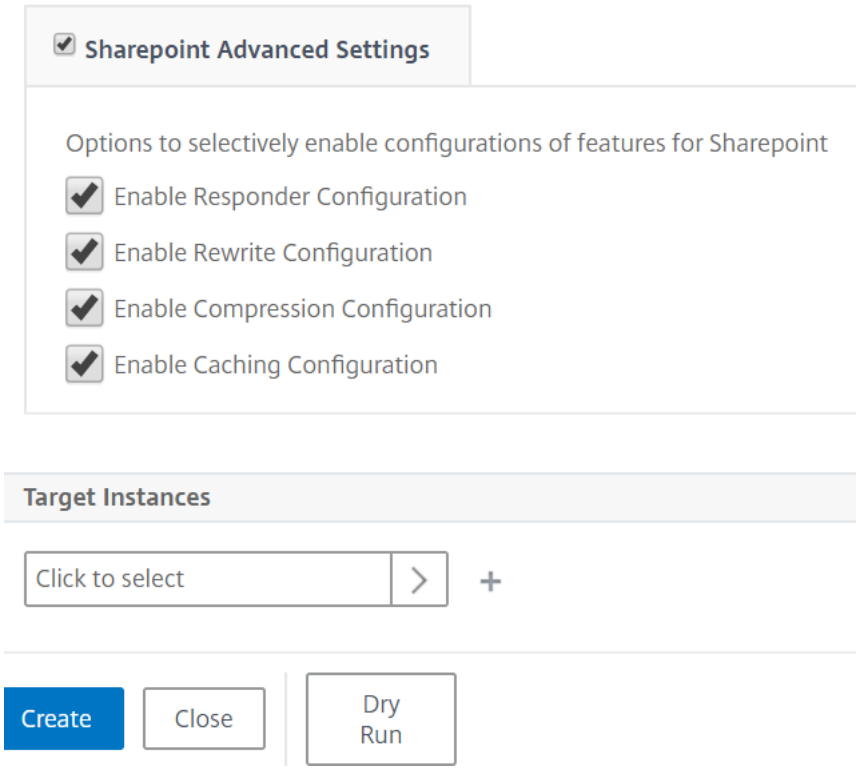
4. Klicken Sie optional auf **Erweiterte Zertifikateinstellungen**, um die Ablaufüberwachung von SSL-Zertifikaten zu aktivieren oder zu deaktivieren. Wenn Sie die Überwachung des Zertifikatablaufs aktivieren, legen Sie die Anzahl der Tage fest, damit NetScaler ADM nach diesen vielen Tagen, wenn das Zertifikat abläuft, einen Alarm ausgibt. Sie haben auch die Möglichkeit, die OCSP-Prüfung als optionales Feature oder als obligatorisches Feature durchzuführen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft ADFS-Proxy-StyleBook

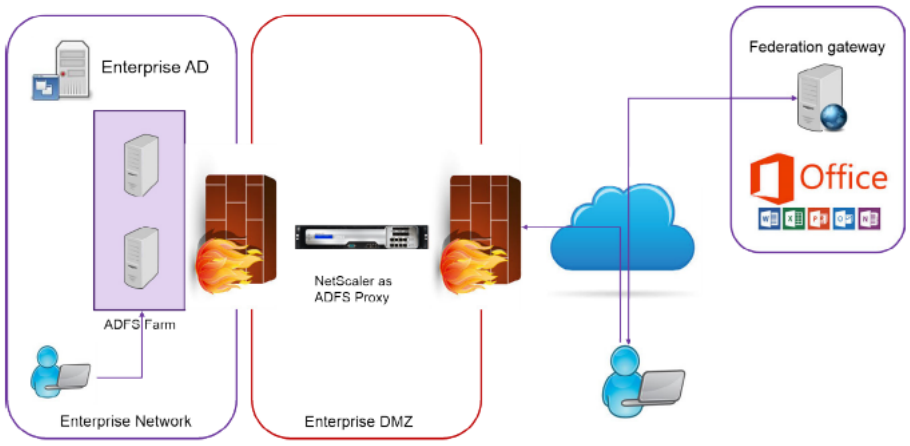
February 5, 2024

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

   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, Enterprise/Platinum-Lizenz

In den folgenden Anweisungen wird davon ausgegangen, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben.

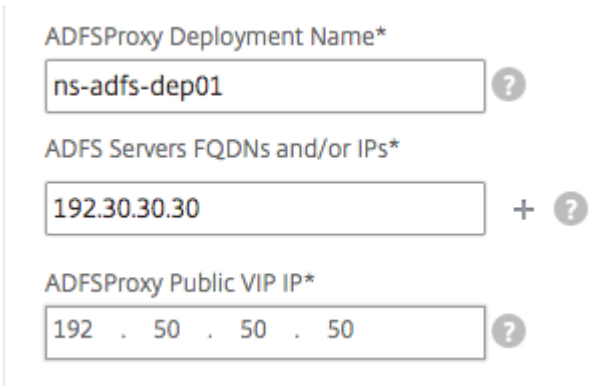
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

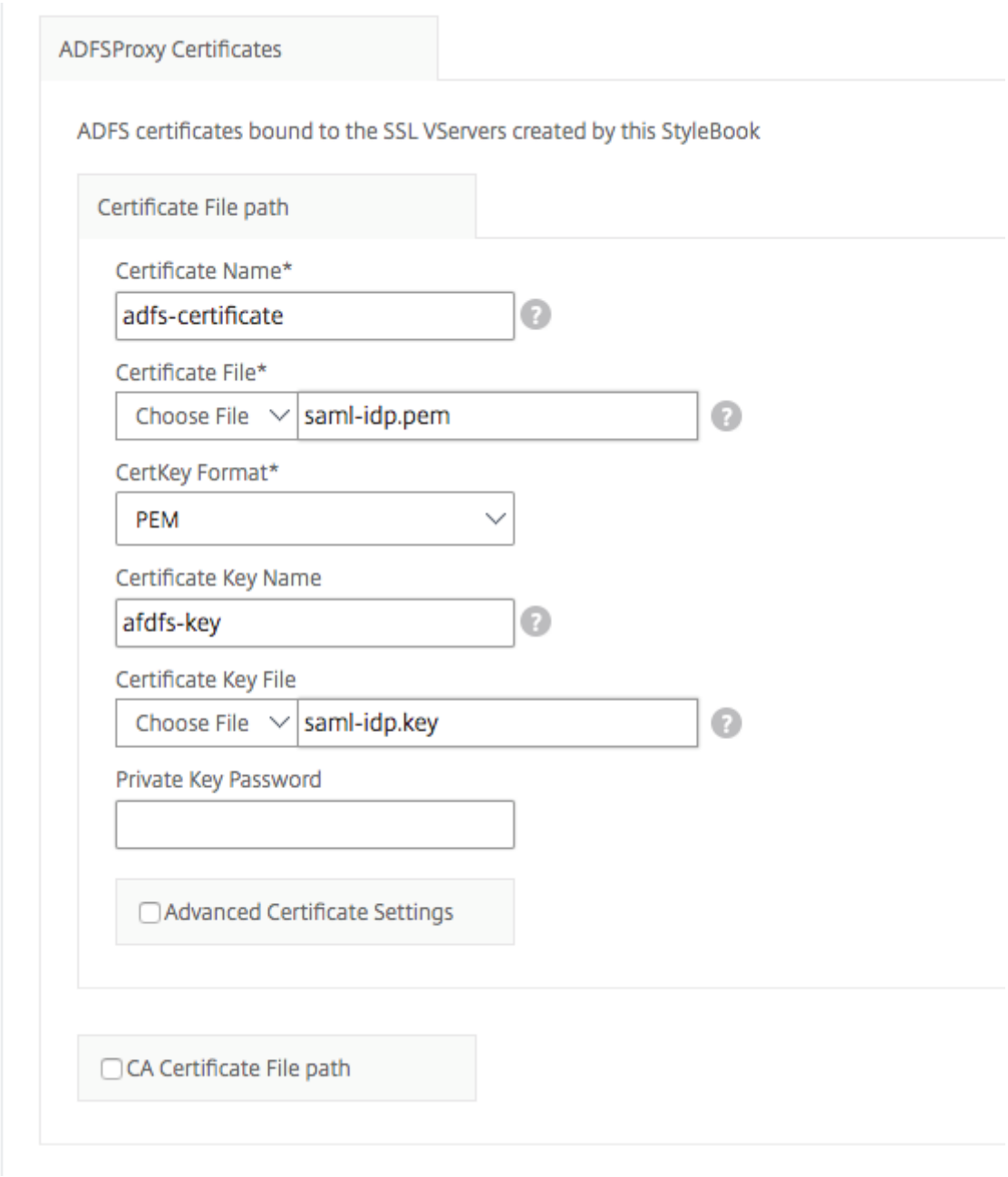


4. Geben Sie im Abschnitt **ADFS-Proxyzertifikate** die Details des SSL-Zertifikats und des Zertifikatsschlüssels ein.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

rectory für die Benutzerauthentifizierung verwendeten DNS-Domänennamen ein. Sie können dann die Authentifizierung entweder für aktive oder passive Clients oder für beide konfigurieren.

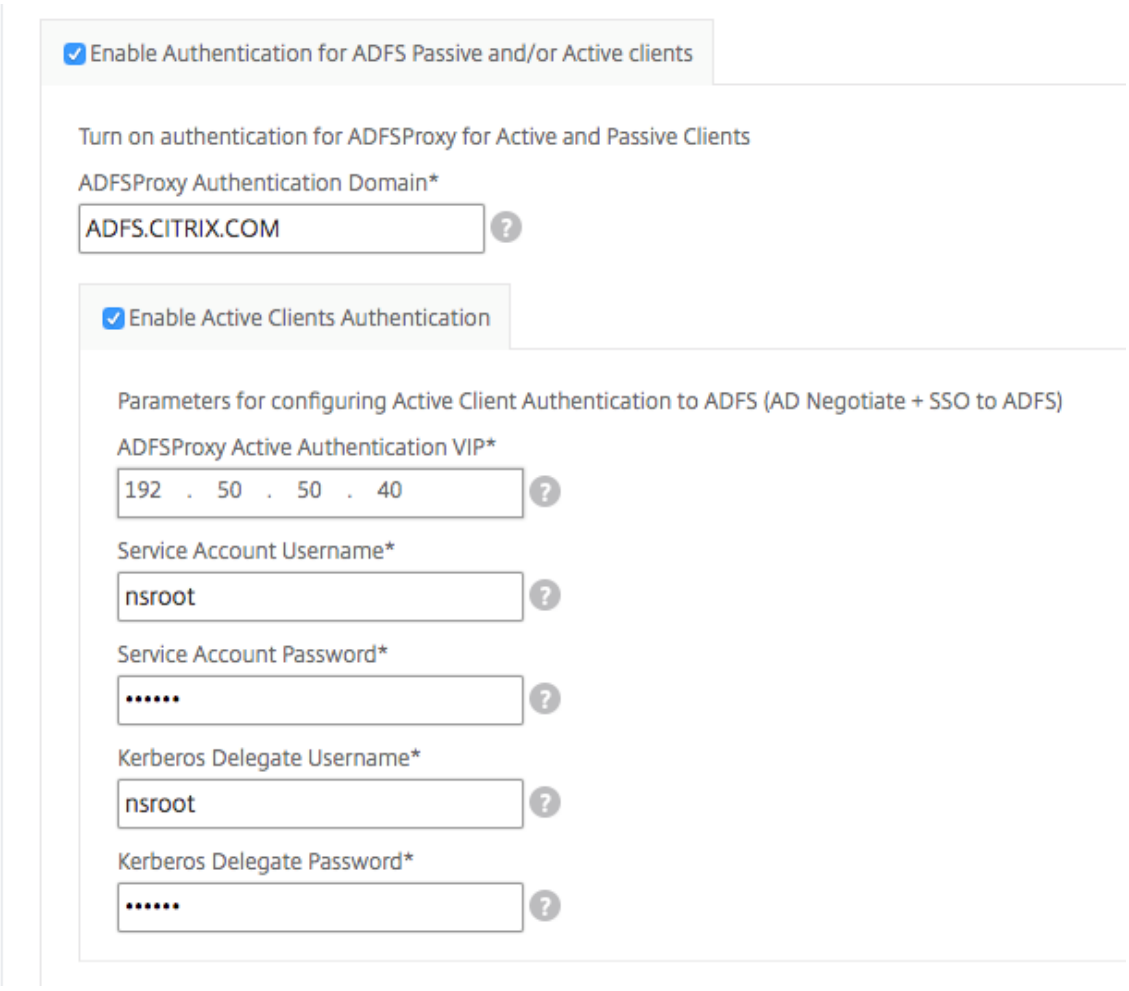
7. Geben Sie die folgenden Details ein, um die Authentifizierung für aktive Clients zu aktivieren:

> **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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

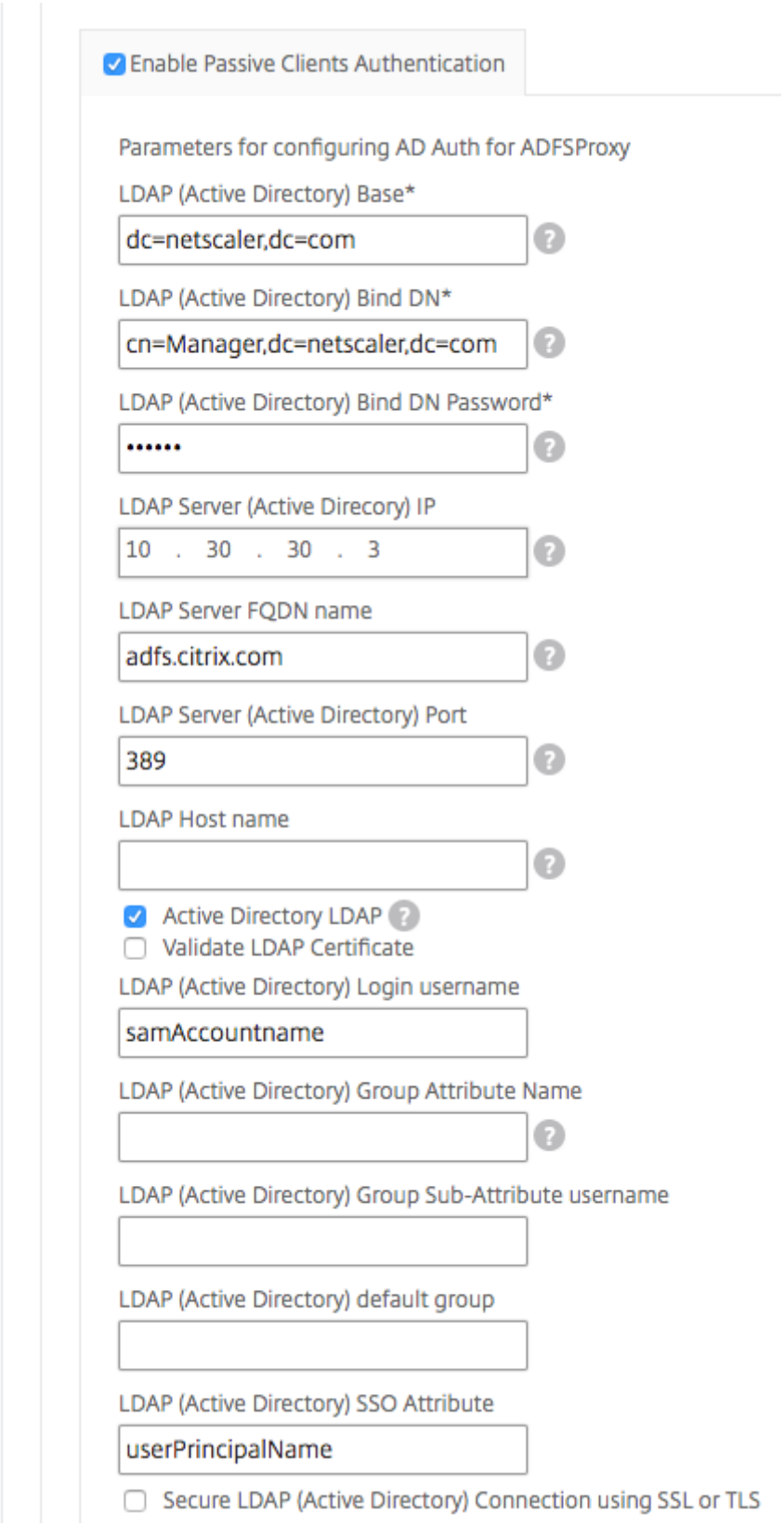
   f) **Active Directory-Port für LDAP-Server**. Standardmäßig sind die TCP- und UDP-Ports für das LDAP-Protokoll 389, wohingegen der TCP-Port für Secure LDAP 636 ist.

   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.

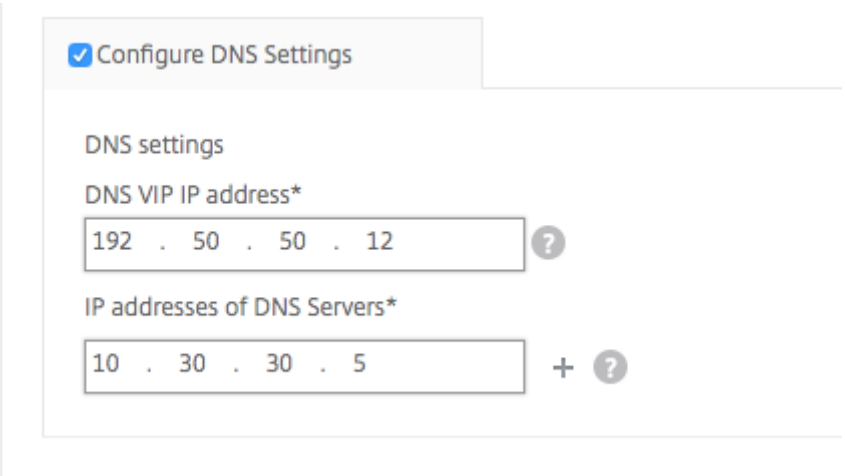
      > **Hinweis:**
      >
      > Die mit * gekennzeichneten Felder sind Pflichtfelder.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

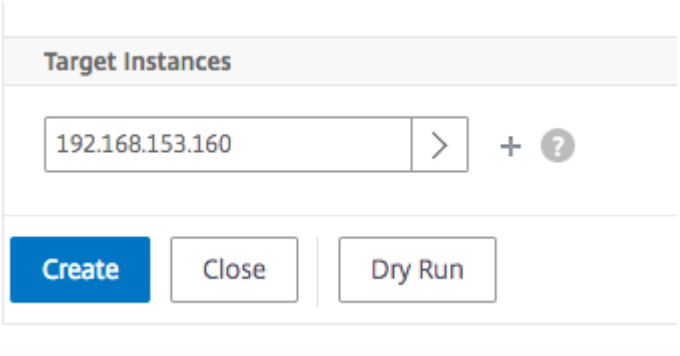


9. Optional können Sie auch eine DNS-VIP für Ihre DNS-Server konfigurieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

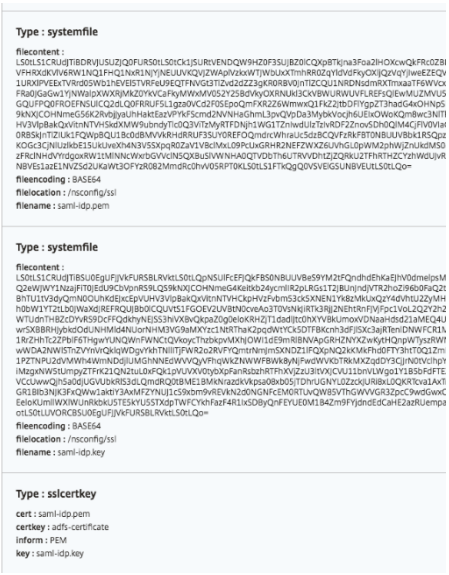


> **Hinweis**
>
> Citrix empfiehlt, dass Sie vor der Ausführung der eigentlichen Konfiguration die Option **Testlauf auswählen.** Sie können zunächst die Konfigurationsobjekte anzeigen, die vom StyleBook auf den NetScaler ADC Zielinstanzen erstellt werden. Sie können dann auf **Erstellen** klicken, um 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

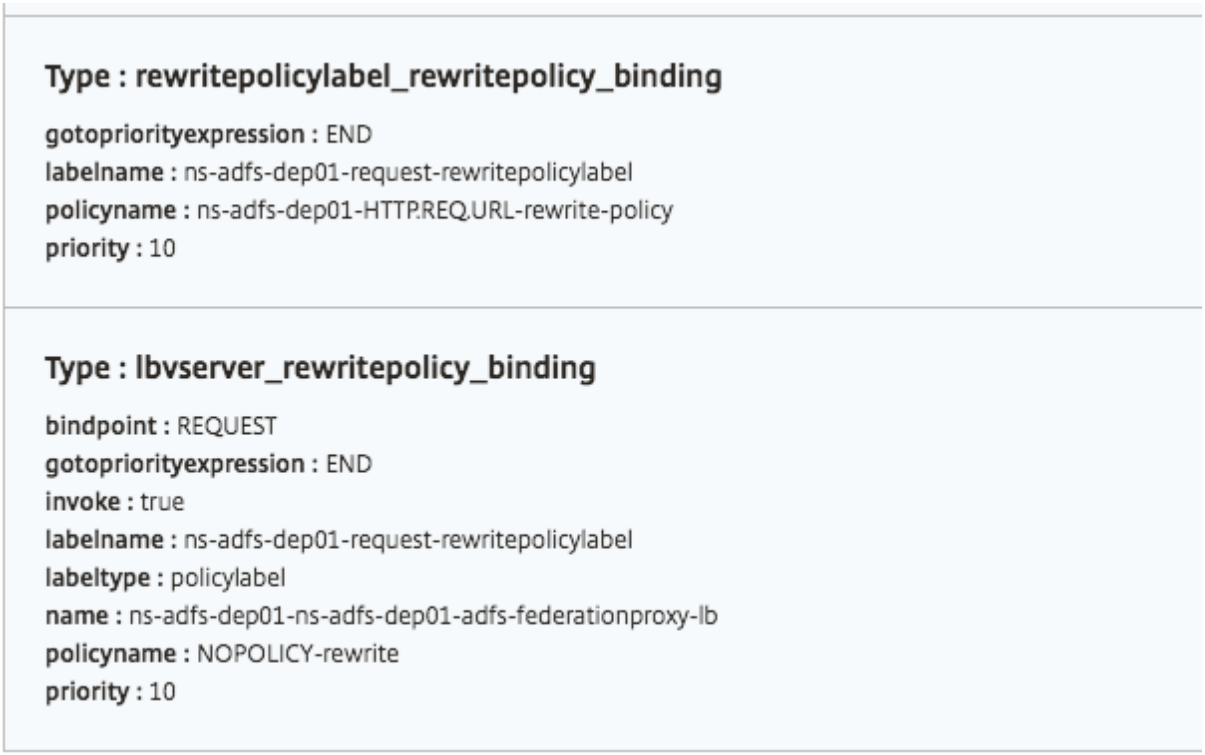
Type : rewriteaction

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"))

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

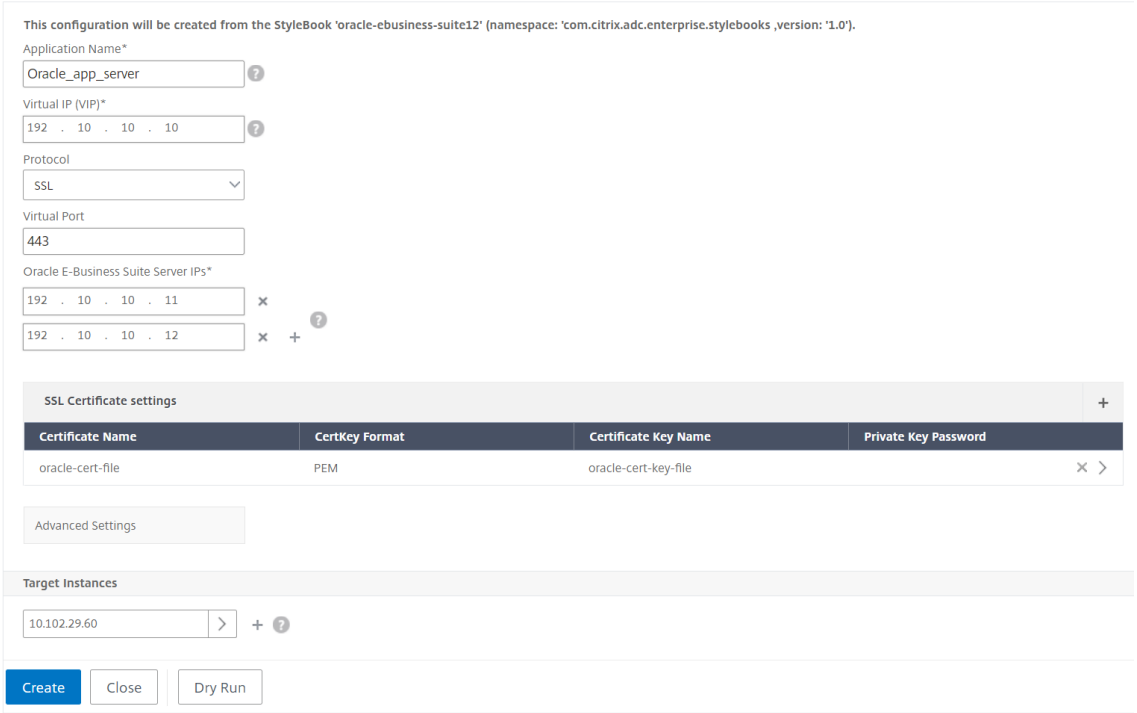
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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:

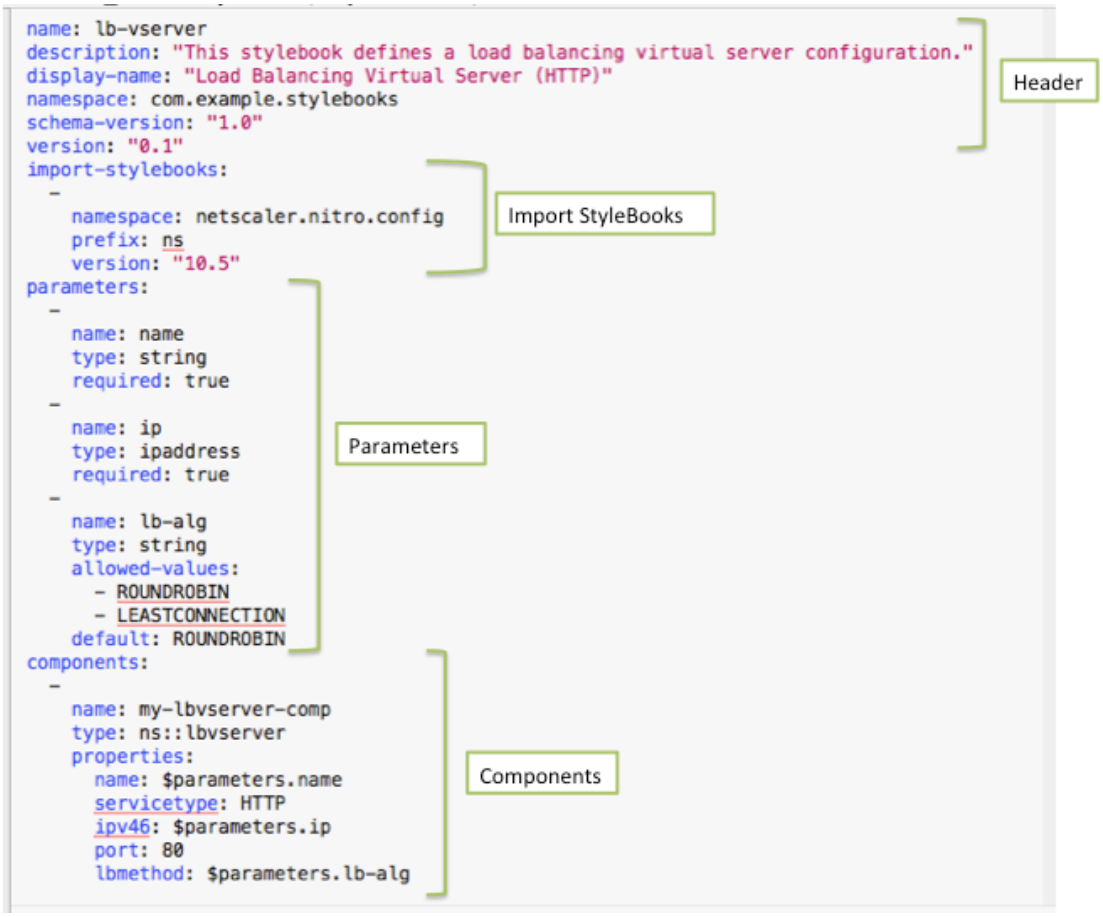
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Header

Die ersten sechs Zeilen eines StyleBook bilden den Header-Bereich. In diesem Beispiel ist der Header-Abschnitt wie folgt geschrieben:

```
name: lb-vserver
description: This StyleBook defines a load balancing virtual server
   configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 integrierte 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
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 (method) used for
     load balancing client request between the application servers.
  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 Pa-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> rameter 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Standardstyle Book, das mit NetScaler ADM ausgeliefert wird. Weitere Informationen zu Composite StyleBooks finden Sie unter Erstellen eines Composite StyleBook.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--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:
 -
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 verwenden, 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

basic-lb-config.yamlgespeichert. 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:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
47      name: $parameters.name + "-lb"
48      servicetype: HTTP
49      ipv46: $parameters.ip
50      port: 80
51      lbmethod: $parameters.lb-alg
52    -
53     name: svcg-comp
54     type: ns::servicegroup
55     properties:
56       servicegroupname: $parameters.name + "-svcgrp"
57       servicetype: HTTP
58
59    -
60     name: lbvserver-svg-binding-comp
61     type: ns::lbvserver_servicegroup_binding
62     properties:
63      name: $components.lbvserver-comp.properties.name
64      servicegroupname: $components.svcg-comp.properties.servicegroupname
65    -
66     name: members-svcg-comp
67     type: ns::servicegroup_servicegroupmember_binding
68     repeat: $parameters.svc-servers
69     repeat-item: srv
70     properties:
71      ip: $srv
72      port: 80
73      servicegroupname: $components.svcg-comp.properties.servicegroupname
74  outputs:
75  -
76    name: lbvserver-comp
77    value: $components.lbvserver-comp
78    description: The component that builds the Nitro lbvserver
         configuration object
79  -
80    name: servicegroup-comp
81    value: $components.svcg-comp
82    description: The component that builds the Nitro servicegroup
         configuration object
83  <!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
  -
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--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. Sie können auch eine zusammenfassende Ansicht eines Parameters vom Typ object [] (Objektliste) als Tabelle anzeigen, wobei die inneren Parameter die Spalten darstellen. Um einen inneren Parameter in die Zusammenfassungsansicht einzubeziehen oder aus ihr auszuschließen, können Sie das summary_display-Attribut im GUI-Abschnitt wie folgt verwenden:

```
name: settings
label: Settings
type: object[]
parameters:
  -
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

Beispiel. Einige StyleBooks 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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerdefinierte StyleBooks verwenden

February 5, 2024

Nachdem Sie Ihr StyleBook erstellt haben, müssen Sie es in NetScaler ADM importieren, um es verwenden zu können. 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 nun zum Erstellen von Konfigurationen verwendet werden.

NetScaler ADM verfügt auch über einen integrierten YAML-Editor, mit dem Sie die StyleBook YAML-Inhalte erstellen können. Mit dem YAML-Editor können Sie Ihre YAML-Konstrukte von Citrix ADM GUI selbst überprüfen. 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.

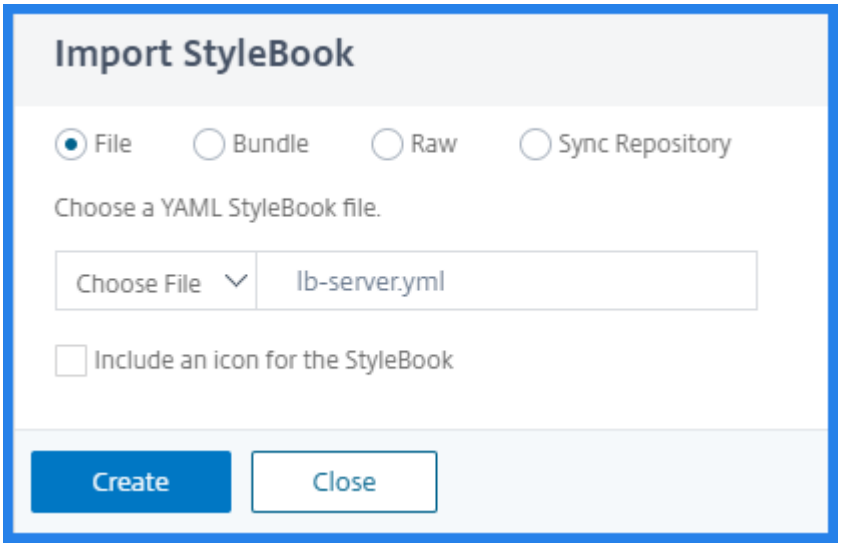
- **Farbcodiert**. Der Editor zeigt den StyleBook-Inhalt gemäß YAML-Richtlinien analysiert, und die Farbcodierung hilft Ihnen, leicht zwischen den Tasten und den Werten zu unterscheiden, die im YAML-Inhalt definiert sind.
- **YAML-Validierung**. Der Inhalt wird bei der Eingabe auf YAML-Fehler überprüft und jede Abweichung wird sofort hervorgehoben. Auf diese Weise können Sie Text schreiben, der den YAML-Richtlinien entspricht, noch bevor Sie das StyleBook in NetScaler ADM importieren. Derzeit validiert der Editor den Inhalt gemäß den YAML-Richtlinien. Es validiert nicht auf Code Korrektheit und typografische Fehler.

Importieren Sie Ihr StyleBook

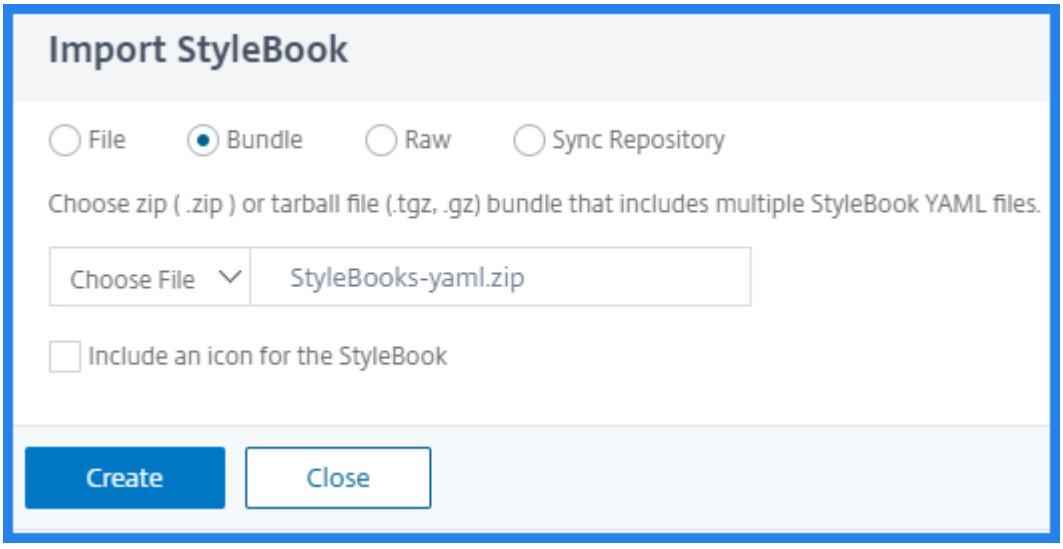
1. Navigieren Sie in Citrix ADM zu **Anwendungen** > **Konfiguration** > **StyleBooks** und klicken Sie dann auf **Neues StyleBook importieren** .
2. Klicken Sie auf eine der drei verfügbaren Optionen, um das StyleBook zu importieren.
   a) **Datei**. Wählen Sie die erforderliche Datei oder das Dateipaket aus Ihrem lokalen Speicher aus.

   > **Hinweis** Importieren Sie in diesem Beispiel das StyleBook „lb-vserver.yaml“, das Sie in StyleBook erstellt haben, um einen virtuellen Load Balancing-Server zu erstellen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) **Bündel**. Mit NetScaler ADM können Sie mehrere StyleBooks im YAML-Format importieren. Sie können mehrere YAML StyleBook-Dateien importieren, die im ZIP-Format (.zip) oder im Tarballformat (.tgz,.gz) komprimiert sind.

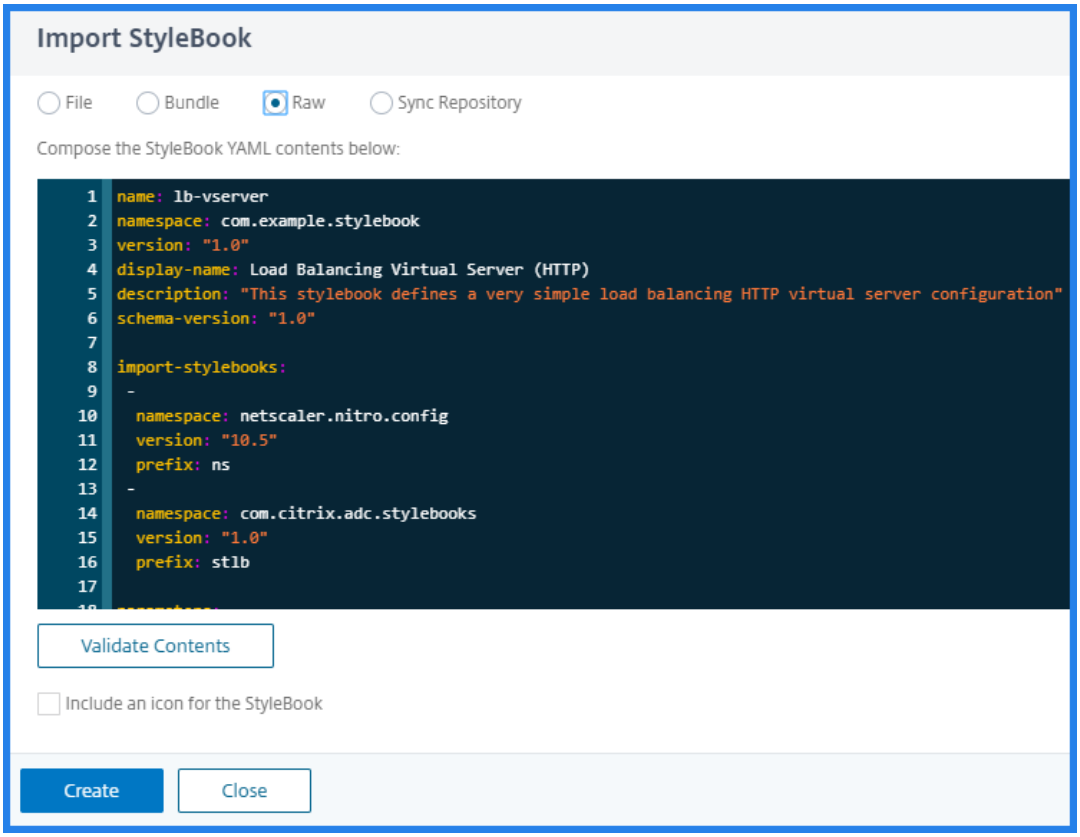


c) **Roh**. Verfassen Sie den Inhalt Ihres StyleBook im YAML-Editor.

> **Hinweis**
>
> Stellen Sie beim Verfassen von StyleBook sicher, dass Sie über folgende Kenntnisse verfügen:
>
> - NITRO API
> - YAML

Weitere Informationen zum Schreiben eigener StyleBooks finden Sie unter How To Create Your Own StyleBooks.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Sie können den Inhalt auch aus einer StyleBook YAML-Datei kopieren und einfügen, um den Inhalt zu validieren.

3. 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 es keine Fehler gibt, wird das StyleBook erfolgreich importiert und nun auf der Seite StyleBooks 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-Grammatik .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Um Konfigurationen aus diesem StyleBook zu erstellen, klicken Sie auf den Link **Konfiguration erstellen** . Das StyleBook öffnet sich als Benutzeroberflächenseite, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
5. Geben Sie die erforderlichen Werte für die Parameter an. ****Im folgenden Beispiel können Sie sehen, dass der Anwendungsname und die **IP-Adressfelder des Load Balancers** als Pflichtfelder angezeigt werden und Benutzerwerte akzeptieren können. Der **LB-Algorithmus** hat nur zwei Werte, aus denen Sie wählen können, und standardmäßig ist ROUNDROBIN ausgewählt.
6. **Klicken Sie unter Zielinstanzen auf die IP-Adresse der Citrix ADC-Instanz, auf der Sie die Konfiguration ausführen möchten, und wählen Sie sie aus. Sie können die Konfiguration auch auf mehreren NetScaler ADC bereitstellen, indem Sie beliebig viele Zielinstanzen angeben.

Wenn Sie sich die Citrix ADC (Nitro) -Konfigurationsobjekte ansehen möchten, die auf Ihrem Citrix ADC erstellt werden, bevor Sie die Konfiguration tatsächlich erstellen, klicken Sie auf **Dry Run**. Wenn Ihre Konfiguration gültig ist, werden die Konfigurationsobjekte angezeigt, die auf der Grundlage der von Ihnen angegebenen Werte erstellt würden. In diesem Beispiel wird nur ein Objekt vom Typ lbvserver durch dieses Beispiel StyleBook erstellt. Dieser lbvserver war die einzige Komponente, die in diesem grundlegenden Beispiel StyleBook definiert wurde. Sie können später auf **Erstellen** klicken , um die Konfiguration auf den ausgewählten Citrix ADC-Instanzen tatsächlich zu erstellen.

Sobald die Erstellung abgeschlossen ist, wird das neue ConfigPack auf der Seite Konfigurationen aufgeführt.

> **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 Ihre benutzerdefinierten StyleBooks inmitten einer großen Anzahl von Standard-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 angezeigten Suchleiste in der ersten Liste die Option **Typ** aus, und wählen Sie **Benutzerdefiniert** aus der nächsten Optionsliste aus.
4. Citrix ADM zeigt nur die benutzerdefinierten StyleBooks an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 handeln. 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
25    type: string
26    required: true
27
28  components:
29   -
30    name: upload-file-comp
31    type: ns::systemfile
32    properties:
33     filename: $parameters.filename
34     filelocation: "/var/Citrix ADC/inbuilt_db/"
35     filecontent: base64.encode($parameters.filecontents)
36  <!--NeedCopy-->
```

Erstellen von Konfigurationen zum Hochladen von Dateien

Im folgenden Verfahren wird eine Konfiguration für eine ausgewählte 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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 configpacks erfolgreich ist, wird die Datei im Citrix ADC Instanzdateisystem unter dem Pfad /var/netscaler/inbuilt_db/ gespeichert.

> **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 Citrix ADM API zum Erstellen eines Configpacks

Sie können die Citrix ADM API auch verwenden, um ein Configpack zu erstellen, das Dateien in die ausgewählte Citrix 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 sind - der Name des virtuellen lb-Servers und die Namen der SSL-Zertifikate, die Sie beim Erstellen des configpacks 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
1 name: lb-vserver-ssl
2 description: "This stylebook defines a load balancing virtual server
     configuration."
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  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

components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 443
    lbmethod: $parameters.lb-alg
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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-->
```

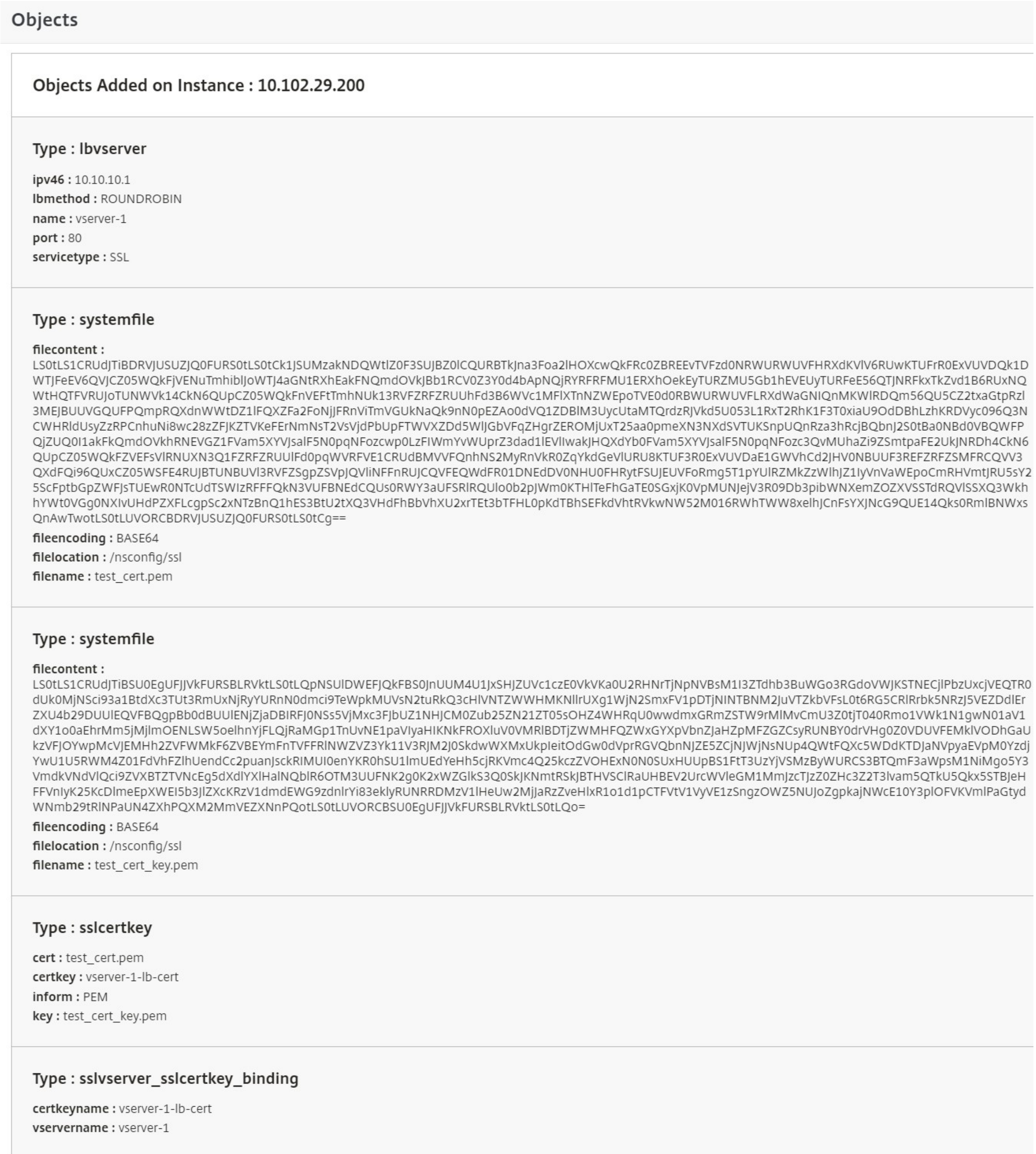
Verwenden der NetScaler ADM -API zum Erstellen eines Konfigurationspakets

Sie können die Citrix ADM API auch verwenden, um ein Configpack zu erstellen, das Cert und Key-Dateien in die ausgewählte Citrix 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 (configpack) auf Citrix ADM erstellt wurde, klicken Sie auf **Objekte anzeigen**, um alle Citrix ADC Objekte anzuzeigen, die auf der Citrix ADC-Zielinstanz erstellt wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Analytics aktivieren und Alarme auf einem virtuellen Server konfigurieren, der in einem StyleBook definiert ist

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 aus diesem StyleBook ein Configpack erstellt wird, wird die Citrix ADM Analysefunktion so konfiguriert, dass Appflow-Datensätze auf den virtuellen Servern gesammelt werden, die beim Erstellen eines Configpacks 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-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Configpacks erstellt wurden, finden Sie in der Citrix 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 Configpack zu erstellen und dieselbe Konfiguration auf mehrere Citrix ADC-Instanzen anzuwenden. Ein solches Szenario, in dem die Konfiguration auf allen ADC-Instanzen identisch ist, kann als symmetrische Konfiguration bezeichnet werden.

Mit der Funktion “Instanzrollen”von StyleBooks können Sie jetzt eine asymmetrische Konfiguration erstellen, d. h. ein Configpack, das auf mehrere ADC-Instanzen angewendet werden kann, jedoch mit unterschiedlichen Konfigurationen auf verschiedenen ADC-Instanzen.

Wenn ein StyleBook mit Instanzrollen verwendet wird, um ein Configpack zu erstellen, kann jeder ADC-Instanz in einem Configpack eine andere Rolle zugewiesen werden. Diese Rolle bestimmt die Konfigurationsobjekte des Configpacks, die die ADC-Instanz erhält.

Zu beachtenswerte Punkte:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Die Gruppe der Instanzrollen in einem StyleBook werden beim Erstellen des StyleBook definiert.
- Die Rollen werden einer bestimmten ADC-Instanz zugewiesen, wenn das Configpack erstellt oder aktualisiert wird.

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-Targets die obligatorische Mindestanzahl von ADC-Instanzen an, denen diese Rolle zugewiesen werden sollte, wenn ein Configpack aus diesem StyleBook erstellt wird, und max-targets geben die maximale Anzahl von ADC-Instanzen an, denen diese Rolle zugewiesen werden kann, wenn ein Configpack aus diesem StyleBook erstellt wird.

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 einer ADC-Instanz beim Erstellen eines Configpacks keine bestimmte Rolle zugewiesen ist, wird die Instanz implizit der “Standard”-Rolle zugewiesen. Die Instanz erhält nun alle Konfigurationsobjekte, die von Komponenten mit der Rolle “Standard”generiert werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Configpacks 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:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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-->
```

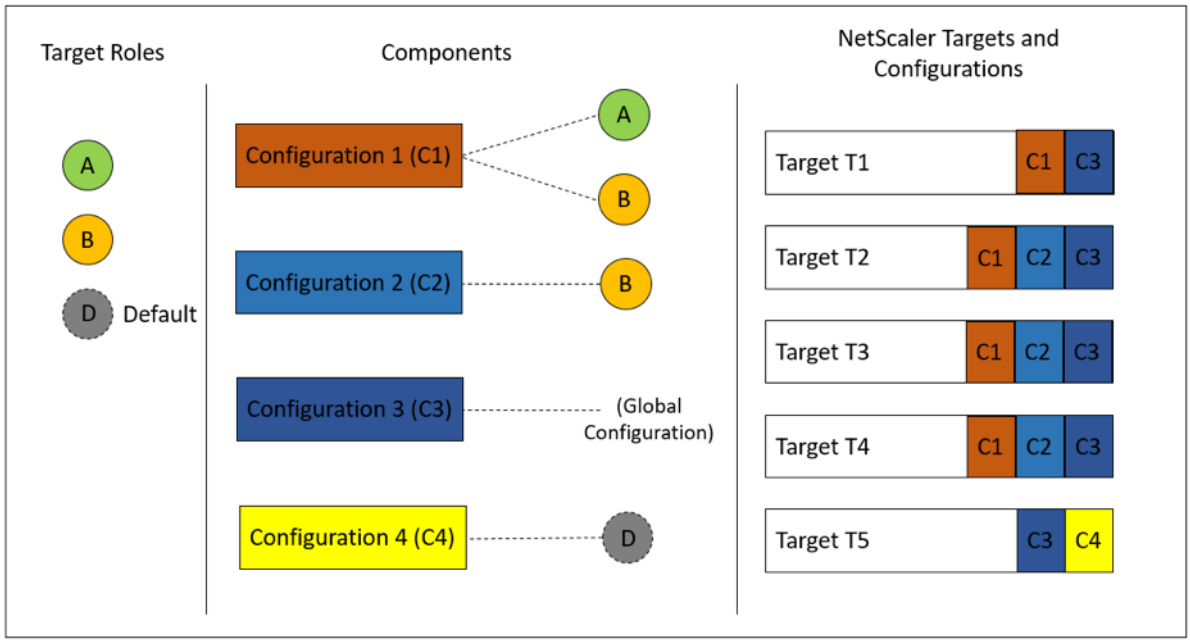
Beachten Sie, dass für die Komponente C3 keine Rolle definiert ist, was bedeutet, dass die Komponente unabhängig von ihrer Rolle auf allen Instanzen bereitgestellt wird. Auf der anderen Seite hat die Komponente C4 die Rolle "default", was bedeutet, dass sie auf jede Instanz angewendet wird, der keine explizite Rolle zugewiesen ist.

Stellen Sie sich nun vor, dass Sie mit diesem StyleBook ein Configpack 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Beachten Sie, dass die Komponente C3 unabhängig von der Rolle auf allen Instanzen bereitgestellt wird, da diese Komponente kein Rollenattribut hatte.

Sie können beim Erstellen eines Configpacks auch die Funktion „Dry Run“verwenden, um die korrekte Rollenzuweisung und die Konfigurationsobjekte, die auf jeder ADC-Instanz erstellt werden, anzuzeigen und zu überprüfen.

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt des StyleBooks “demo-target-roles”finden Sie unten:

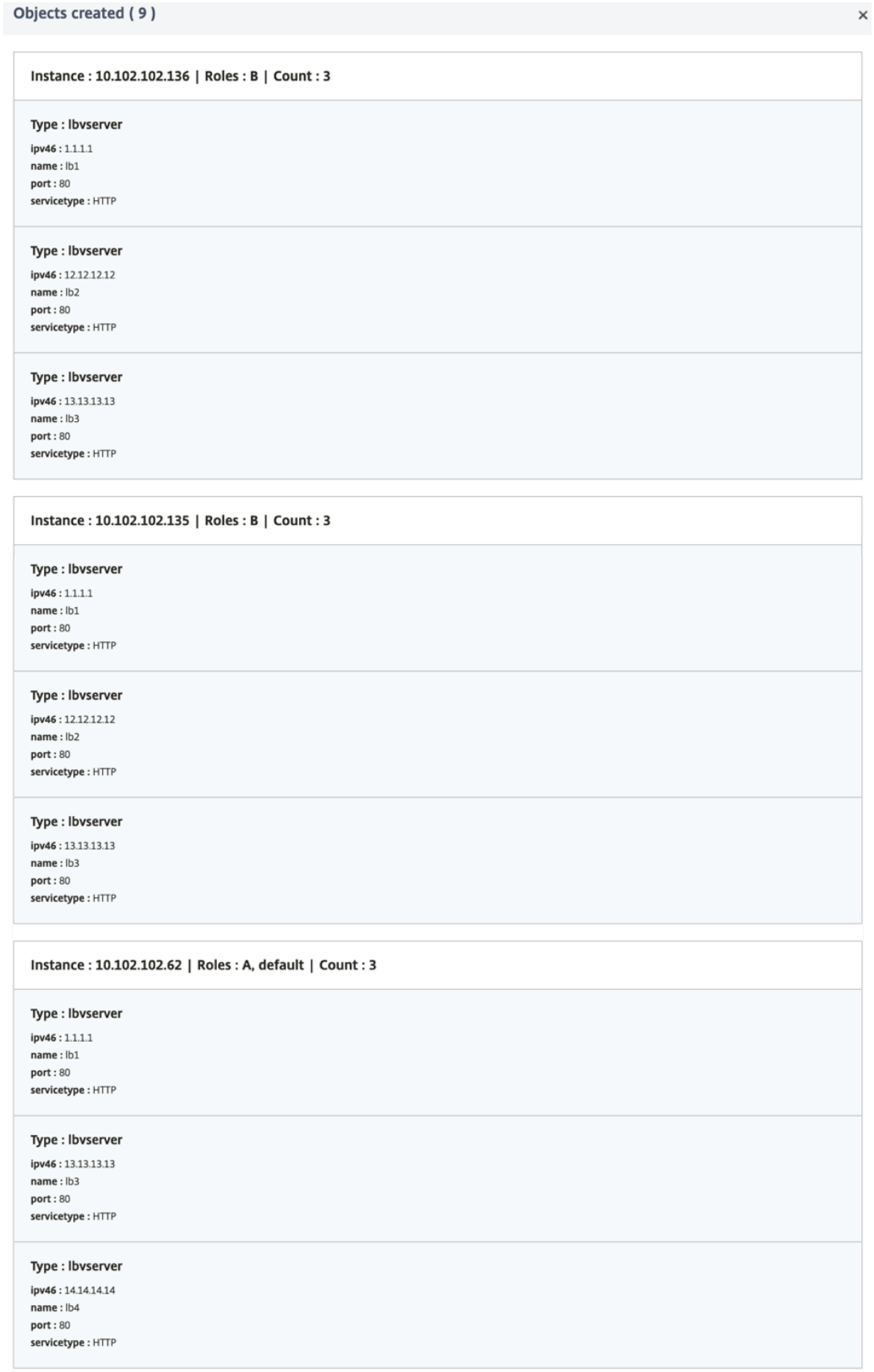
```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

Das folgende Bild zeigt die Objekte, die für ein Beispiel-Configpack erstellt wurden:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwenden von APIs

Wenn Sie die REST-API verwenden, können Sie Rollen für jede ADC-Instanz angeben, wenn Sie das Configpack wie folgt erstellen oder aktualisieren. 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",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
32            "roles": ["A", "B"]
33           }
34  ,
35          {
36
37            "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
38            "roles": ["default"]
39           }
40
41        ]
42       }
43
44  }
45
46  <!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Configpack 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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",
    ...
    }

 ]
 }

<!--NeedCopy-->
```

Wenn die Konfiguration (configpack) erfolgreich erstellt wurde, erhalten Sie die folgende HTTP-Antwort:

```
200 OK
Content-Type: application/json
{

  "configpack":
  {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    "config_id": "1460806080"
   }

 }

<!--NeedCopy-->
```

Sie haben Ihre erste Konfiguration (configpack) erstellt, die mit der ID 1460806080 eindeutig identifiziert wird. Mit dieser ID können Sie die Konfiguration abfragen, aktualisieren oder löschen.

Beispiel 2

Sie können dasselbe StyleBook verwenden, um eine andere Konfiguration oder ein Configpack zu erstellen und es auf denselben oder anderen Citrix ADC Instanzen auszuführen. Erstellen Sie in diesem Beispiel eine weitere Konfiguration, geben Sie einen anderen Namen und eine andere IP-Adresse für den virtuellen Server an und geben Sie LEASTCONNECTION als Lastausgleichsmethode an. Stellen Sie diese Konfiguration auf zwei NetScaler ADC-Instanzen bereit.

Die HTTP-Anfrage lautet wie folgt:

```
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": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
     }
 ,
    "target_devices"
    [
     {
 "id": "deecee30-f478-4446-9741-a85041903410" }
 ,
     {
 "id": "debecc60-d589-4557-8632-a74032802412" }

    ]
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    }

 }

<!--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 configpacks wird die folgende HTTP-Antwort empfangen:

```
200 OK
Content-Type: application/json
{

   "configpack":
  {

     "config_id": "1657696292"
   }

 }

<!--NeedCopy-->
```

Dieses neue configpack 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 Configpack aus diesem StyleBook wie folgt zu erstellen:

```
POST

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":
    {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
10
11        "name": "myapp",
12        "ip": "10.70.122.25",
13        "svc-servers":
14        ["192.168.100.11","192.168.100.12"],
15         "svc-port": 8080
16       }
17  ,
18     "target_devices":
19     [
20      {
21
22       "id": "deecee30-f478-4446-9741-a85041903410"
23       }
24  ,
25      {
26
27       "id": "debecc60-d589-4557-8632-a74032802412"
28       }
29
30     ]
31    }
32
33  }
34
35  <!--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 Configpack aus diesem StyleBook wie folgt zu erstellen:

```
1  POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
      example.stylebooks/0.1/composite-example/configpacks
2  <!--NeedCopy-->
```

```
1  Content-Type: application/json
2  Accept: application/json
3  {
4
5    "configpack":
6    {
7
8      "parameters": {
9
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        "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 configpacks wird die folgende HTTP-Antwort empfangen:

```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Aktualisieren einer Konfiguration

Um diese Konfiguration zu aktualisieren, indem Sie zum Beispiel einen neuen Backend-Server mit der IP-Adresse 10.102.29.54 zum Lastenausgleichsserver myapp hinzufügen, verwenden Sie die API, um ein configpack wie folgt zu aktualisieren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 configpacks wird die folgende HTTP-Antwort empfangen:

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Löschen einer Konfiguration

Um diese Konfiguration (aus allen Citrix ADC Instanzen) zu löschen, können Sie die API zum Löschen eines Configpacks wie folgt 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-->
```

Beim erfolgreichen Löschen des Configpacks wird die folgende HTTP-Antwort empfangen:

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Sie können sich bei der Citrix ADC Instanz anmelden und überprüfen, ob alle Konfigurationsobjekte, die Teil dieses Configpacks sind, entfernt wurden.

Wenn Sie die Konfiguration von bestimmten Citrix ADC Instanzen anstelle von allen entfernen möchten, verwenden Sie den oben beschriebenen Konfigurationsvorgang “configpack”, und ändern Sie das Attribut “target_devices”in der JSON-Payload, um die spezifischen Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Configpack 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": {

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                    "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 Configpack wird durch die ID 8c158e7a-0087-423f-91b0-0ccf16de552a eindeutig identifiziert. Mit dieser ID können Sie die Konfiguration abfragen, aktualisieren oder löschen. Bei erfolgreicher Aktualisierung des Configpacks 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 Citrix Application Delivery Management (ADM) -API verwenden, um ein Config-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

pack zu erstellen, das Dateien in die ausgewählte Citrix 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. Wie im Beispiel im obigen Thema, erstellen Sie ein configpack und geben Sie den Wert des Parameters locationfile als Dateipfad der Standortdatei in Citrix ADM an.
Verwenden Sie die REST-API, um ein configpack 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 Configpack aus diesem StyleBook zu erstellen, wie folgt in einem beliebigen Werkzeug wie dem curl-Befehlszeilentool oder

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

der Postman Chrome-Browsererweiterung. 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",

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    "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:

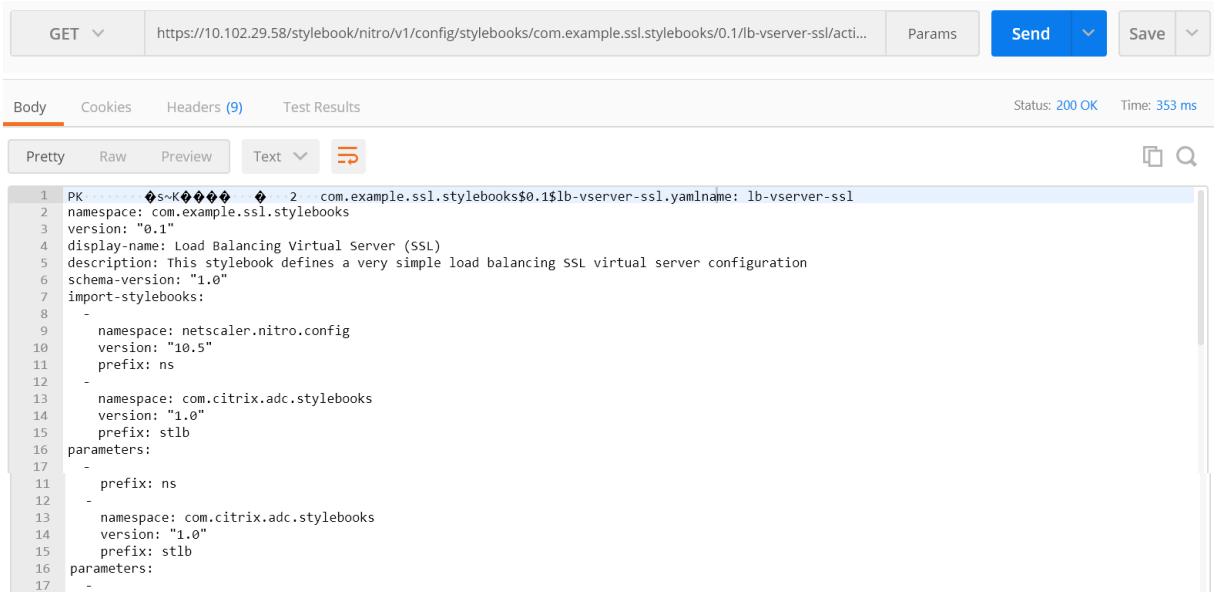
```
GET

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-->
```

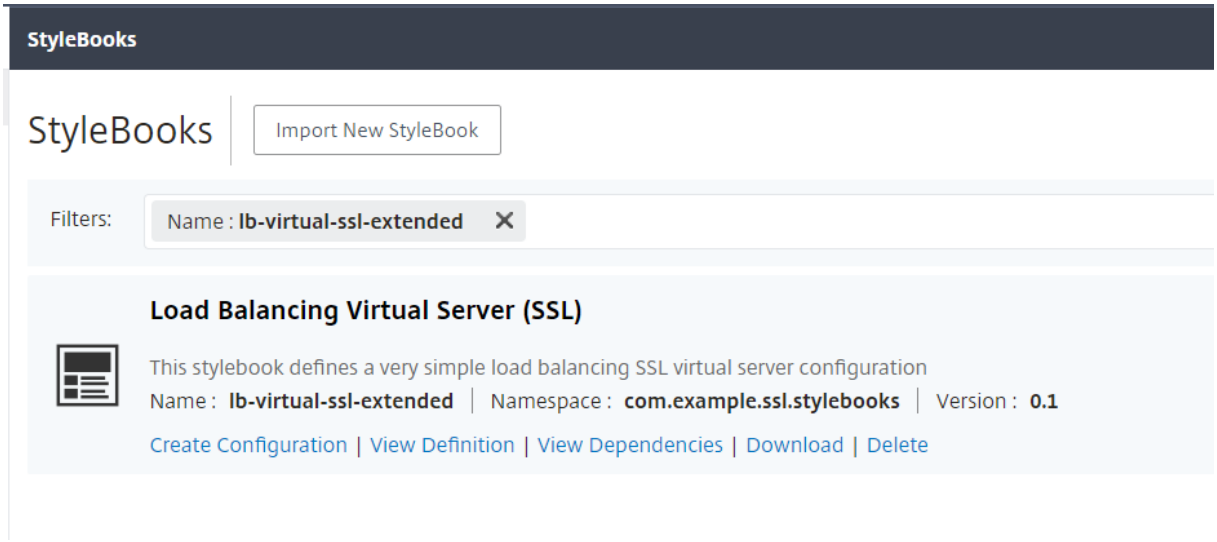
Wenn der Abfrageparameter für Abhängigkeiten in der URL nicht bereitgestellt wird oder sein Wert auf false gesetzt ist, werden die StyleBook-Abhängigkeiten nicht gelöscht (nur das StyleBook selbst wird gelöscht).

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.

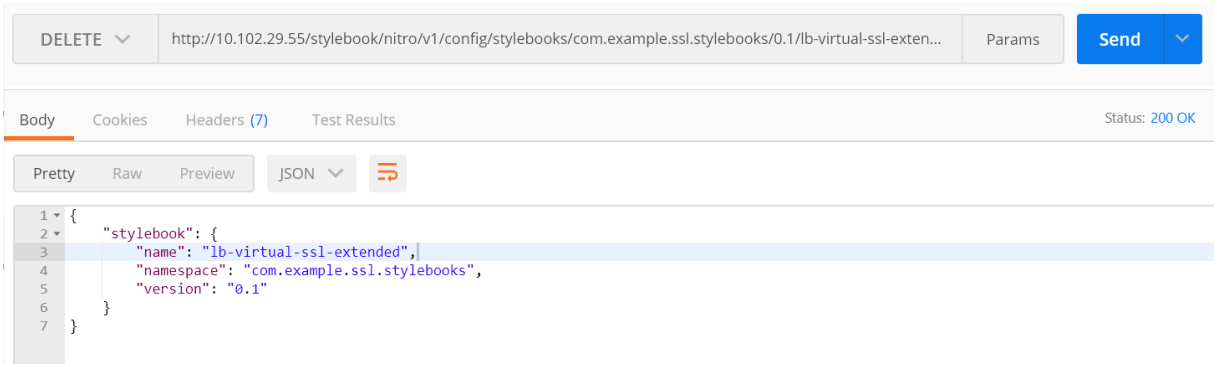
Angenommen, Sie haben ein StyleBook mit dem Namen lb-virtual-ssl-extended in Citrix ADM erstellt. Sie haben sich später entschieden, dieses StyleBook zu löschen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

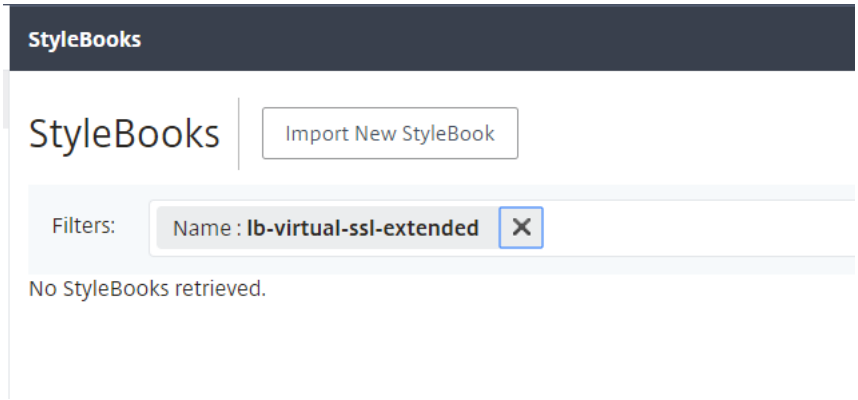


Sie können die API in jedem Tool wie dem curl-Befehlszeilentool oder der Postman Chrome-Browsererweiterung ausführen, nachdem Sie Änderungen an den Feldern IP-Adresse, Name, Version und Namespace vorgenommen haben.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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/12-1/stylebooks/stylebooks-grammar/header-section.html)	[StyleBooks importieren](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/import-stylebooks-section.html)
[Parameters](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-section.html)	[Parameters-Default-Sources-Konstrukt](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html)
[Substitutions](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions.html)	[Components](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components.html)
[Optionale Eigenschaften](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/optional-properties.html)	[Hilfskomponenten](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/helper-components.html)
[Eigenschaften, Standardquellen](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/properties-default-sources.html)	[Verschachtelte Komponenten](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-components.html)
[Konditionskonstrukt](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/condition-construct.html)	[Konstrukt wiederholen](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-construct.html)
[Konstrukt für Wiederholungsbedingung](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	[Outputs](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/outputs.html)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

|
| [Verschachtelte Wiederholungen](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-repeats.html) | [Übergeordnete Referenz](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parent-reference.html)
|
[Parameterreferenz](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameter-reference.html)	[Substitutionsreferenz](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions-reference.html)
[Komponentenreferenz](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components-reference.html)	[Operations](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/operations.html)
[Variablenreferenz](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/variable-reference.html)	[Alarms](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/alarms.html)
[Analytics](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/analytics.html)	[Integrierte Funktionen](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/built-in-functions.html)
[Expressions](/de-de/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/expressions.html)	[Abhängigkeitserkennung](/de-de/netscaler-application-delivery-management-software/12-1/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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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| Desription|
—	—
name	Ein Name zur Identifizierung des StyleBook. Dieses Attribut ist obligatorisch.
Beschreibung	Eine Beschreibung, die definiert, was ein StyleBook tut. Diese Beschreibung wird auf der NetScaler ADM GUI angezeigt. Dies ist ein optionales Attribut.
Anzeigename	Ein beschreibender Name für das StyleBook. Dieser Name wird auf der NetScaler ADM GUI angezeigt. Dies ist ein optionales Attribut.
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)
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    namespace: com.example.stylebooks
    schema-version: "1.0"
    version: "0.1"
<!--NeedCopy-->
```

Die Kombination aus Name, Namespace und Version identifiziert ein StyleBook im System eindeutig. Sie können nicht zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version in 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
6       -
7        namespace: com.acme.stylebooks
8         version: "0.1"
9         prefix: stlb
10  <!--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 dies ein optionaler Abschnitt ist, benötigen die meisten StyleBooks möglicherweise einen. Im Parameterabschnitt können Sie die Fragen definieren, die Benutzer beantworten sollen, wenn sie das StyleBook verwenden, um eine Konfiguration auf einer Citrix ADC Instanz zu erstellen.

Wenn Sie Ihr StyleBook in Citrix ADM importieren und es zum Erstellen einer Konfiguration verwenden, verwendet die GUI diesen Abschnitt des StyleBook, um ein Formular anzuzeigen, das Eingaben für Werte der von Ihnen definierten Parameter übernimmt.

Im folgenden Abschnitt werden die Attribute beschrieben, die Sie für jeden Parameter in diesem Abschnitt angeben müssen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

name

Der Name des Parameters, den Sie definieren möchten. Sie können einen alphanumerischen Namen angeben.

Der Name muss mit einem Alphabet beginnen und kann zusätzliche Alphabete, Zahlen, Bindestriche (-) oder Unterstriche (_) enthalten.

Beachten Sie, dass Sie beim Schreiben eines StyleBook dieses Attribut name verwenden können, um auf den Parameter in anderen Abschnitten zu verweisen, indem Sie die Notation $parameters verwenden. <name>.

Obligatorisch? Ja

Bezeichnung

Eine Zeichenfolge, die in der ADM-GUI als Name dieses Parameters angezeigt wird.

Obligatorisch? Nein

Beschreibung

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

typ

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.
- Zahl: 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.
- boolean: Kann entweder true oder false sein. Beachten Sie auch, dass alle Literale von YAML als boolesche Werte betrachtet werden (z. B. Ja oder Nein).
- ipaddress: Ein String, der eine gültige IPv4- oder IPv6-Adresse darstellt.
- tcp-Port: Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port darstellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- password: Stellt einen undurchsichtigen/geheimen Zeichenfolgenwert dar. Wenn Citrix ADM GUI einen Wert für diesen Parameter anzeigt, wird er als Sternchen (*****) angezeigt.
- certfile: Stellt eine Zertifikatdatei dar. Auf diese Weise 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/ gespeichert/ns_ssl_certs in ADM.

  Die Zertifikatsdatei wird der Liste der Zertifikate hinzugefügt, die von ADM verwaltet werden.
- keyfile: Stellt eine Zertifikatsschlüsseldatei dar. Auf diese Weise können Sie die Datei direkt von Ihrem lokalen System hochladen, wenn Sie eine StyleBook-Konfiguration mit der Citrix ADM GUI erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis /var/mps/tenants/ gespeichert/ns_ssl_keys in Citrix ADM.

  Die Zertifikatschlüsseldatei wird der Liste der Zertifikatschlüssel hinzugefügt, die von Citrix ADM verwaltet werden.
- file: Stellt eine Datei dar.
- Objekt: Dieser Typ wird verwendet, wenn Sie mehrere verwandte Parameter unter einem übergeordneten Element gruppieren möchten. Sie müssen den übergeordneten Parameter den Typ als Objekt angeben. Ein Parameter vom Typ “object”kann einen verschachtelten Abschnitt “parameter”haben, um die darin enthaltenen Parameter zu beschreiben.
- ein anderes StyleBook: Wenn Sie diesen Parametertyp verwenden, erwartet dieser Parameter, dass sein Wert in Form der Parameter ist, die im StyleBook definiert sind, der seinen Typ angibt.

Ein Parameter kann auch einen Typ haben, der eine Liste aller oben aufgeführten Typen ist,
indem [] am Ende des Typs hinzugefügt wird. Wenn das type-Attribut beispielsweise string [] ist, nimmt dieser
Parameter eine Liste von Zeichenfolgen als Eingabe an. Sie können eine, zwei oder mehrere Zeichenfolgen für
diesen Parameter angeben, wenn Sie eine Konfiguration aus diesem StyleBook erstellen.

Obligatorisch? Ja

Schlüssel

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 aus demselben StyleBook (auf derselben oder anderen Citrix ADC Instanzen) unterschiedliche Konfigurationen erstellen, weist jede Konfiguration einen anderen/eindeutigen Wert für

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

diesen
Parameter auf.

Der Standardwert ist falsch.

Obligatorisch? Nein

erforderlich

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 NetScaler ADM GUI zwingt den Benutzer, einen gültigen Wert für diesen Parameter anzugeben.

Der Standardwert ist falsch.

Obligatorisch? Nein

> **Hinweis**
>
> Wenn ein Parameter `type: object`und hat `required: false`, werden die Unterparameter dieses Parameters nicht ausgewertet.

Wenn Sie möchten, dass der Standardwert der Unterparameter wirksam wird, setzen Sie `required : true`für den Hauptparameter wie folgt ein:

```
    type: object
    required: true
    gui:
      collapse_pane: true
<!--NeedCopy-->
```

Das Attribut collapse_pane zeigt das Objekt und seine Unterparameter in der Benutzeroberfläche reduziert an, es sei denn, der Benutzer erweitert den Bereich.

zulässige Werte

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 NetScaler ADM GUI wird der Benutzer aufgefordert, einen Parameterwert aus dieser Liste auszuwählen.

Beispiel 1:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name: IP-Adresse

type: string

zulässige Werte:

- SOURCEIP
- DEST IP
- NONE

Beispiel 2:

name: TCP-Port

type: tcp-port

zulässige Werte:

- 80
- 81
- 8080

Beispiel 3:

(Liste der tcp-ports, wobei jedes Element der Liste nur Werte in
zulässigen Werten haben kann)

name: tcpports

Typ: tcp-port []

zulässige Werte:

- 80
- 81
- 8080
- 8081

Obligatorisch? Nein

Standard

Verwenden Sie dieses Attribut, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer beim Erstellen einer
Konfiguration keinen Wert angibt, wird der Standardwert verwendet.

Wenn ein Benutzer beim Erstellen der Konfiguration über die Citrix ADM GUI
keinen Wert für einen Parameter angibt, der keinen Standardwert hat, wird
für diesen Parameter kein Wert festgelegt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Beispiel 1:

name: timeout

type: number

Def ault: 20

Beispiel 2:

(wobei der Standardwert des Parameters eine Liste von Werten ist):

name: Protokolle

type: string []

Standard:

- TCP
- UDP
- IP

Beispiel 3:

name: timeout

type: number

default: 20

Beispiel 4:

name: tcpport

type: tcp-port

default: 20

Obligatorisch? Nein

Muster

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

Muster: „[a-z] +“

Obligatorisch? Nein

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

min-value

Verwenden Sie dieses Attribut, um den Minimalwert für Parameter vom Typ number oder tcp-port zu definieren.

Beispiel:

name: audio-port

type: tcp-port

min-value: 5000

Der Min-Wert von Zahlen kann negativ sein, aber der Min-Wert für tcp-port sollte nicht negativ sein.

Obligatorisch? Nein

max-value

Mit diesem Attribut definieren Sie den Maximalwert für Parameter vom Typ number oder tcp-port.

Der Maximalwert sollte größer als der Minimalwert sein, falls definiert.

Beispiel:

name: audio-port

type: tcp-port

min-value: 5000

max-value: 15000

Obligatorisch? Nein

min-length

Verwenden Sie dieses Attribut, um die Mindestlänge der Werte zu definieren, die für einen Parameter vom
Typ “string”akzeptiert werden.

Die Mindestlänge der Zeichen, die als Werte definiert sind, sollte größer oder gleich Null sein.

Beispiel:

name: appname

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

type: string

min-Länge: 3

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.

Die maximale Länge der Werte sollte größer oder gleich der Länge
der in min-length definierten Zeichen sein.

Beispiel:

name: appname

type: string

max-length: 64

Obligatorisch? Nein

min-items

Verwenden Sie dieses Attribut, um die minimale Anzahl von Elementen in einem Parameter zu definieren,
der eine Liste ist.

Die Mindestanzahl von Elementen sollte größer oder gleich Null sein.

Beispiel:

name: server-ips

type: ipaddress[]

min-items: 2

Obligatorisch? Nein

max-items

Verwenden Sie dieses Attribut, um die maximale Anzahl von Elementen in einem Parameter zu definieren,
der eine Liste ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die maximale Anzahl von Elementen sollte größer sein als die minimale Anzahl von Elementen, wenn sie definiert sind.

Beispiel:

name: server-ips

type: ipaddress[]

min-items: 2

max-items: 250

Obligatorisch? Nein

GUI

Verwenden Sie dieses Attribut, um das Layout des Parameters vom Typ "object"in der Citrix ADM GUI anzupassen.

Obligatorisch? Nein

Spalten

Dies ist ein Unterattribut des GUI-Attributs. Verwenden Sie dies, um die Anzahl der Spalten zu definieren, die in der Citrix ADM GUI angezeigt werden sollen.

Obligatorisch? Nein

updatable

Dies ist ein Unterattribut des GUI-Attributs. Mit dieser Option
können Sie angeben, ob der Parameter nach der Erstellung der Konfiguration aktualisiert werden kann.

Wenn der Wert auf false gesetzt ist, wird das Parameterfeld ausgegraut, wenn Sie die Konfiguration aktualisieren.

Obligatorisch? Nein

collapse_pane

Dies ist ein Unterattribut des GUI-Attributs. Geben Sie hier an, ob der Bereich, der das Layout dieses Objektparameters
definiert, zusammenklappbar ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

     updatable: false
<!--NeedCopy-->
```

Beispiel für einen vollständigen Parameterabschnitt:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

       -

         name: ip

         label: IP Address

         description: The virtual IP address used for this application

         type: ipaddress

         required: true

      -

         name: svc-servers

         label: Servers

         type: object[]

         required: true

         parameters:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
57                    description: The TCP port of the server
58
59                    type: tcp-port
60
61                    default: 80
62
63        -
64
65            name: lb-alg
66
67            label: LoadBalancing Algorithm
68
69            type: string
70
71            allowed-values:
72
73              - ROUNDROBIN
74
75              - LEASTCONNECTION
76
77            default: ROUNDROBIN
78
79        -
80
81            name: enable-healthcheck
82
83            label: Enable HealthCheck?
84
85            type: boolean
86
87            default: true
88  <!--NeedCopy-->
```

Im Folgenden finden Sie ein Beispiel, das alle Attribute einer Liste und die in früheren Abschnitten

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

erläuterten Werte definiert:

“‘YAML
-Name: Features-Liste

Typ: string []**

min-length: 1

max-length: 3

min-items: 1

max-items: 3

pattern: “[A-Z]+”

allowed-values:

- SP

- LB

- CS

default:

- LB

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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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]\*\*
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    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.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
24      condition: $parameters.server-pools
25      repeat: $parameters.server-pools
26      repeat-item: pool
27      repeat-condition: $pool.rule
28      repeat-index: ndx
29      properties:
30        appname: $parameters.appname + "-cs"
31        cs-virtual-ip: $parameters.vip
32        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
       HTTP")
33        cs-service-type: $parameters.protocol
34        pools:
35          -
36            lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
       , "0.0.0.0", 0, $pool.servers)
37            rule: $pool.rule
38            priority: $ndx + 1
39  <!--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.

```
1  substitutions:
2       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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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/12-1/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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
        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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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: $srv
33                        port: str($parameters.svc-port)
34                        servicegroupname: $parent.properties.name
35  <!--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 verwendet, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--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:
           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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                            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: $parameters.svc-port
                                   servicegroupname: $parent.properties.
    name
<!--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:

```
           -
           name: members-svcg-comp
           type: ns::servicegroup_servicegroupmember_binding
           repeat:
             repeat-list: $parameters.svc-servers
           properties:
                  ip: $repeat-item
                  port: $parameters.svc-port
                  servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Neben der Möglichkeit, auf das aktuelle Element während der Iteration über eine Liste zu verweisen, ist es auch möglich, auf den aktuellen Index des Elements in der Liste mit **repeat-index**zu verweisen. Im folgenden Beispiel wird 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
6               properties:
7                   ip: $parameters.app-ip
8                   port: $parameters.base-port + repeat-index
9                   servicegroupname: $parent.properties.name
10 <!--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:

```
1       -
2               name: services
3               type: ns::service
4               repeat:
5                  repeat-list: $parameters.app-services
6                  repeat-item: srv
7                  repeat-index: idx
8               properties:
9                   ip: $parameters.app-ip
10                  port: $parameters.base-port + $idx
11                  servicegroupname: $parent.properties.name
12 <!--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:

```
1  components
2     -
3        name: der-key-files-comp
4        type: ns::systemfile
5        repeat:
6        repeat-list: $parameters.certificates
7        repeat-item: certificate
8          repeat-condition: $certificate.ssl-inform == DER
9          properties:
10          filecontent: base64($certificate.keyfile.contents)
11          fileencoding: BASE64
12          filelocation: /nsconfig/ssl
13          filename: $certificate.keyfile.file
14 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:
  -
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
         repeat-list: $parameters.vips
         repeat-item: ip
         repeat:
              repeat-list: $parameters.vip-ports
              repeat-item: port
      properties:
         name: str("lb-") + str($ip) + '-' + str($port)
         servicetype: HTTP
         ipv46: $ip
         port: $port
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
components:
-
     name: lbvservers-comp
     type: ns::lbvserver
     repeat:
         repeat-list: $parameters.vips
         repeat:
            repeat-list: $parameters.vip-ports
     properties:
        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
    -1)
         servicetype: HTTP
         ipv46: $repeat-item
         port: $repeat-item-1
<!--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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
    repeat: $parameters.svc-server-domain-names
    repeat-item: server-name
    properties:
      name: $server-name + "-server"
      domain: $server-name
    components:
      -
         name: service-members-comp
         type: ns::service
         properties:
           name: $server-name + "-service"
           servername: $parent.properties.name
           servicetype: $parameters.svc-service-type
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            port: $parameters.svc-server-port
<!--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.

Alle Citrix ADM Insight, die auf Citrix ADC-Instanzen über StyleBooks aktiviert sind, verwenden IPFIX-Protokoll (AppFlow), um die Daten von den Instanzen an Citrix ADC zu senden.

Wenn Sie Web Insight aktivieren, sind clientseitige Messungen auf dem Lastausgleichs- und den virtuellen Content Switching-Server aktiviert.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Attribut	Beschreibung	Erforderlich
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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Attribut	Beschreibung	Erforderlich
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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Attribut	Beschreibung	Erforderlich
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 nach-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dem, 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

Eines der mächtigsten Funktionen von StyleBook ist die Verwendung von Ausdrücken. Sie können StyleBooks-Ausdrücke in verschiedenen Szenarien verwenden, um dynamische Werte zu berechnen. Das folgende Beispiel zeigt einen Ausdruck, um einen Parameterwert mit einer Literalzeichenfolge zu verketten.

Beispiel:

$parameters.appname + “-mon”

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Dieser Ausdruck ruft den Parameter appname ab und verkettet ihn mit der Zeichenfolge -mon.

Die folgenden Ausdruckstypen werden unterstützt:

Arithmetische Ausdrücke

- Zusatz (+)
- Substraction (-)
- 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

Zeichenfolgenausdrücke

- 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 ist [81, 82], dann ergibt $parameters.ports-1 + $parameters.ports-2 eine Liste [80, 81, 81, 82]

Relationale Ausdrücke

- ==: Testet, ob zwei Operanden gleich sind und gibt true zurück, wenn sie gleich sind, andernfalls wird false zurückgegeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ! =: 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 Gleichheitsoperators: $parameters.name = abcd
- Verwendung von Ungleichheitsoperator: $parameters.name! = Standard
- Beispiele für andere relationale Operatoren
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

Logische (boolesche) Ausdrücke

- 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.
- Hinweis: Der unäre Operator. Wenn der Operand wahr ist, ist das Ergebnis falsch und umgekehrt.
- in: Prüft, ob das erste Argument ein Teilstring des zweiten Arguments ist
- in: Prüft, ob ein Element Teil einer Liste ist

> **Hinweis**
>
> Sie können Umwandlungen eingeben, in denen Zeichenfolgen in Zahlen umgewandelt werden können und Zahlen in Zeichenfolgen konvertiert werden können. Ebenso kann ein tcp-port in

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> eine Zahl umgewandelt werden, und eine IP-Adresse kann in eine Zeichenfolge umgewandelt werden.

Sie müssen ein Trennzeichen vor und nach einem Operator verwenden. Sie können die folgenden Trennzeichen verwenden:

> - Vor einem Operator: Leerzeichen, Tabulator, Komma, (,), [,]
> - Nach einem Operator: space, tab, (, [
> - Beispiel:
> - abc + def
> - 100 % 10
> - 10 > 9

Ausdruckstypvalidierung

StyleBook-Engine ermöglicht jetzt eine stärkere Typprüfung während der Kompilierzeit, dh die beim Schreiben des StyleBook verwendeten Ausdrücke werden während des Imports von StyleBook selbst validiert und nicht beim Erstellen des Konfigurationspakets.

Alle Verweise auf Parameter, Substitutionen, Komponenten, Eigenschaften von Komponenten, Komponentenausgaben, benutzerdefinierte Variablen (repeat-item, repeat-index, Argumente für Substitutionsfunktionen usw.) werden alle auf ihre Existenz und Typen überprüft.

Beispiel für Typprüfungen:

Im folgenden Beispiel lautet der erwartete Typ der Port-Eigenschaft von lbvserver StyleBook tcp-port. In früheren Versionen von Citrix Application Delivery Management (ADM) berechnete der StyleBook-Compiler den Wert als Zeichenfolge, und das StyleBook wurde importiert und ausgeführt. Nun passieren Typvalidierungen zur Kompilierungszeit (Importzeit). Der Compiler stellt fest, dass string und tcp-port nicht kompatible Typen sind und daher der StyleBook-Compiler einen Fehler auslöst und den Import oder die Migration des StyleBook fehlschlägt.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP

You should now declare this as a number for the compiler to
   successfully compile this StyleBook.
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
12
13    port: 80
14  <!--NeedCopy-->
```

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 wird das StyleBook nicht in Citrix ADM importiert.

In diesem Beispiel lautet der Ausdruck, der der Eigenschaft name in der Komponente lb-sg-binding-comp zugewiesen ist: $components.lbvserver-comp.properties.lbvservername. Es gibt jedoch keine Eigenschaft namens lbvservername in der Komponente 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. Sie müssen solche Fehler manuell korrigieren und die StyleBooks importieren.

```
1  components:
2    -
3      name: lbvserver-comp
4      type: ns::lbvserver
5      properties:
6        name: mylb
7        ipv46: 10.102.190.15
8        port: 80
9        servicetype: HTTP
10   -
11     name: sg-comp
12     type: ns::servicegroup
13     properties:
14       servicegroupname: mysg
15       servicetype: HTTP
16   -
17     name: lb-sg-binding-comp
18     type: ns::lbvserver_servicegroup_binding
19     condition: $parameters.create-binding
20     properties:
21       name: $components.lbvserver-comp.properties.lbvservername
22       servicegroupname: $components.sg-comp.properties.servicegroupname
23 <!--NeedCopy-->
```

Indizierung von Listen

Auf Elemente einer Liste kann jetzt zugegriffen werden, indem Sie sie direkt indizieren:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, bei der es sich um eine Ausgabe des ersten Elements der lbcomps-Komponente handelt.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 5, 2024

Ausdrücke in StyleBooks können integrierte Funktionen nutzen.

Zum Beispiel können Sie die eingebaute Funktion str () verwenden, um eine Zahl in einen String zu transformieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

str($parameters.order)

Oder Sie können die integrierte Funktion int () verwenden, um eine Zeichenfolge in eine ganze Zahl zu transformieren.

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 Funktion str() wandelt das Eingabeargument in einen Zeichenfolgenwert um.

Zulässige Argumenttypen:

- string
- number
- TCP-port
- boolean
- IP-Adresse

Beispiele:

- “set-“+ str(10) returns “set-10”
- str(10) returns “10”
- str(1.1.1.1) returns “1.1.1.1”
- str(T rue) returns “T rue”
- str(mas) returns “mas”

int()

Die int() Funktion nimmt einen String, eine Zahl oder tcpport als Argument und gibt eine ganze Zahl zurück.

Beispiele:

- int(“10”) returns 10
- int(10) returns 10

bool()

Die bool() Funktion nimmt einen beliebigen Typ als Argument. Wenn der Argumentwert falsch, leer oder nicht vorhanden ist, gibt diese Funktion false zurück.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Andernfalls wird true zurückgegeben.

Beispiele:

- bool(true) returns “true”
- bool(false) returns “false”
- bool($parameters.a) returns false if the
- $parameters.a is false, empty, or not present.

len()

Die Funktion len() nimmt 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:

Elemente: [“123”, „abc“, „xyz”]

len($substitutions.items) returns 3

Beispiel 2:

len(“netscaler mas”) returns 13

Beispiel 3:

len ($parameters.vips) gibt 3 zurück, wenn $parameters.vip ein
Wert zugewiesen wird [‘1.1.1.1’, ‘1.1.1.2’, ‘1.1.1.3’]

min()

Die min() Funktion nimmt 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:

- min(80, 100, 1000) returns 80
- min(-20, 100, 400) returns -20
- min(-80, -20, -10) returns -80
- min(0, 100, -400) returns -400

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Support $parameters.ports ist eine Liste von TCP-Ports und hat den Wert: [80, 81, 8080].

  min($parameters.ports) returns 80.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

max()

Die Funktion max() nimmt 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:

- max(80, 100, 1000) returns 1000
- max(-20, 100, 400) returns 400
- max(-80, -20, -10) returns -10
- max(0, 100, -400) returns 100

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Support $parameters.ports ist eine Liste von TCP-Ports und hat den Wert: [80, 81, 8080].

  max($parameters.ports) returns 8080.

bin()

Die Funktion bin() nimmt eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Binärformat darstellt.

Beispiele für Ausdrücke:

bin(100) returns “0b1100100”

oct()

Die Funktion oct() nimmt eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Oktalformat darstellt.

Beispiele für Ausdrücke:

oct(100) returns “0144”

hex()

Die hex() -Funktion nimmt eine Zahl als Argument und gibt eine Kleinbuchstabe zurück, die die Zahl im hexadezimalen Format darstellt.

Beispiele für Ausdrücke:

hex(100) returns “0x64”

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

lower()

Die lower() Funktion nimmt eine Zeichenfolge als Argument und gibt die gleiche Zeichenfolge in Kleinbuchstaben zurück.

Beispiel:

lower(“MAS”) returns “mas”

upper()

Die Funktion upper() nimmt eine Zeichenfolge als Argument und gibt die gleiche Zeichenfolge in Großbuchstaben zurück.

Beispiel:

upper(“netscaler_mas”) returns “NET SCALER_MAS”

sum()

Die Funktion sum() 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

  sum($substitutions.list-of-numbers) returns 88

Beispiel 2:

Wenn $parameters.ports [80, 81, 82] ist, gibt sum ($parameters.ports) 243 zurück

pow()

Die Funktion pow() nimmt zwei Zahlen als Argumente und gibt eine Zahl zurück, die das erste Argument auf die
Potenzstärke des zweiten darstellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Beispiel:

pow(3,2) returns 9

ip()

Die IP-Funktion nimmt eine Zeichenfolge oder eine IP-Adresse als Argument gibt die IP-Adresse basierend auf dem Eingabewert zurück.

Beispiele:

- ip(“2.1.1.1”) returns “2.1.1.1”
- ip(3.1.1.1) returns “3.1.1.1”

base64.encode()

Die base64.encode() Funktion nimmt ein String-Argument und gibt die base64-codierte Zeichenfolge zurück.

Beispiel:

base64.encode(“abcd”) returns “YWJjZA==”

base64.decode()

Die base64.decode-Funktion nimmt base64-codierte Zeichenfolge als Argument und gibt die decodierte Zeichenfolge zurück.

Beispiel:

base64.decode(“YWJjZA==”) returns “abcd”

exists()

Die Funktion exists nimmt ein Argument eines beliebigen Typs und gibt einen Booleschen Wert zurück. Der Rückgabewert ist True, wenn die Eingabe einen beliebigen Wert hat. Der Rückgabewert ist False Wenn das Eingabeargument keinen Wert hat (d. h. keinen Wert).

Beachten Sie, dass $parameters.monitor ein optionaler Parameter ist. Wenn Sie diesen Parameter beim Erstellen eines configpacks einen Wert angeben, gibt exists ($parameters.monitor) True zurück.

Andernfalls wird False zurückgegeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

filter()

Die Funktion filter() nimmt zwei Argumente an.

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, in der jedes Element auf True ausgewertet wird, wenn es an die Substitutionsfunktion im ersten
Argument übergeben wird.

Beispiel:

Angenommen, wir haben eine Substitutionsfunktion wie folgt definiert.

Substitutionen:

```
1  x(a): $a != 81
```

Diese Funktion gibt True zurück, wenn der Eingabewert nicht gleich 81 ist. Andernfalls wird False zurückgegeben.

Angenommen,...

$parameters.ports ist [81, 80, 81, 89]

filter ($substitutions.x, $parameters.ports) gibt [80, 89] zurück, indem alle Vorkommen von 81 aus der Liste entfernt werden.

if-then-else()

Die Funktion if-then-else() nimmt drei Argumente.

Argument 1: Boolescher Ausdruck

Argument 2: Beliebiger Ausdruck

Argument 3: Beliebiger Ausdruck (optional)

Wenn der Ausdruck in Argument 1 den Wert True ergibt, gibt die Funktion den Wert des als Argument 2 angegebenen 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, gibt die Funktion keinen Wert zurück.

Beispiel 1:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

if-then-else($parameters.servicetype == HTTP, 80, 443) returns “80”if $parameters.servicetype has value “HTTP.”Andernfalls gibt die Funktion
“443”zurück.

Beispiel 2:

if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport) returns the value of “$parameters.hport”if $parameters.servicetype has value “HTTP.”

Andernfalls gibt die Funktion den Wert von $parameters.sport.

Beispiel 3:

if-then-else($parameters.servicetype == HTTP, 80) returns “80”if $parameters.servicetype has value “HTTP.”

Andernfalls gibt die Funktion keinen Wert zurück.

join()

Die Funktion join() nimmt zwei Argumente:

Argument 1: Liste von Zahlen, tcp-ports, Strings oder ipaddresses

Argument 2: Trennzeichenfolge (optional)

Die Funktion verbindet die Elemente der Liste, die als Argument 1 zur Verfügung gestellt wird, in einer Zeichenfolge, wobei jedes Element durch die Trennzeichenfolge getrennt wird, die als Argument zwei bereitgestellt wird. Wenn Argument zwei nicht angegeben wird, werden Elemente in der Liste als eine Zeichenfolge miteinander verbunden.

Beispiel:

- $parameters.ports ist [81, 82, 83].
  - Mit Trennzeichen Argument:

    join($parameters.ports, ‘-‘) returns “81-82-83”
  - Ohne Trennzeichen Argument:

    join($parameters.ports) returns “818283”

map()

Die Kartenfunktion nimmt zwei Argumente an;

Argument 1: Jede Funktion

Argument 2: Eine Liste von Elementen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Die Funktion gibt eine Liste zurück, in der jedes Element in der Liste das Ergebnis der Anwendung der mapfunction (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

  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:

    map($substitutions.add-10,

    $parameters.nums) gibt eine Liste von Zahlen zurück:
    [91, 92, 93]

Das Ergebnis dieser Kartenfunktion ist eine Liste von Zahlen, jedes Element wird berechnet, indem die Substitutionsfunktion $substitutions.add-10 auf das entsprechende Element in der Eingabeliste ($parameters.nums) angewendet wird.

quotewrap()

Die quotewrap Funktion nimmt eine Zeichenfolge als Argument und gibt eine Zeichenfolge zurück, nachdem doppelte Anführungszeichen vor und nach dem Eingabewert hinzugefügt wurde.

Beispiel:

quotewrap(“mas”) returns ““mas””

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

replace()

Die Funktion replace verwendet drei Argumente:

Argument 1: Zeichenfolge

Argument 2: Zeichenfolge

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 Argument 1 entfernt (mit anderen Worten, durch leere Zeichenfolge ersetzt).

Ersetzen Sie eine Teilzeichenfolge durch eine andere Teilzeichenfolge:

- replace(‘abcdef’, ‘def’, ‘xyz’) returns ‘‘abcxyz’’.
  - Alle Vorkommen von def werden durch xyz ersetzt.
- replace(‘abcdefabc’, ‘def’) returns ‘‘abcabc’’.
  - Da es kein drittes Argument gibt, wird def aus der resultierenden Zeichenfolge entfernt.

trim()

Die Trim-Funktion gibt einen String zurück, in dem die führenden und nachfolgenden Leerzeichen aus der Eingabezeichenfolge entfernt werden.

Beispiel:

trim(‘abc ‘) returns ‘‘abc’’

truncate()

Die Funktion truncate nimmt zwei Argumente an:

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:

truncate(‘netscaler mas’, 9) returns ‘‘netscaler’’

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

url.encode

Die Funktion url.encode gibt einen String zurück, in dem Zeichen mit ASCII-Zeichensatz gemäß RFC 3986 transformiert werden.

Beispiel:

url.encode(“a/b/c”) returns “a%2Fb%2Fc”

url.decode

Die Funktion url.decode gibt eine Zeichenfolge zurück, in der das URL-codierte Argument in eine reguläre Zeichenfolge gemäß RFC 3986 decodiert wird.

Beispiel:

url.decode(“a%2Fb%2Fc”) returns “a/b/c”

ist-ipv4 ()

Die Funktion is-ipv4 () verwendet eine IP-Adresse als Argument und gibt „true“zurück, wenn die IP-Adresse das IPv4-Format hat.

is-ipv4 (10.10.10.10) gibt „Wahr“zurück

ist-ipv6 ()

Die Funktion is-ipv6 () verwendet eine IP-Adresse als Argument und gibt „true“zurück, wenn die IP-Adresse das IPv6-Format hat.

is-ipv6 (2001:DB8::) gibt „Wahr“zurück

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
<!--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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
     name: mylb
      servicegroupname: $components.sg-comp.properties.servicegroupname
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: $components.lbvserver-comp.properties.servicetype
<!--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 zu einem späteren Zeitpunkt einrichten. Nachdem Sie NetScaler ADM In-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

stanzen 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 entweder beim ersten Einrichten des NetScaler ADM -Servers oder zu einem späteren Zeitpunkt hinzufügen. 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

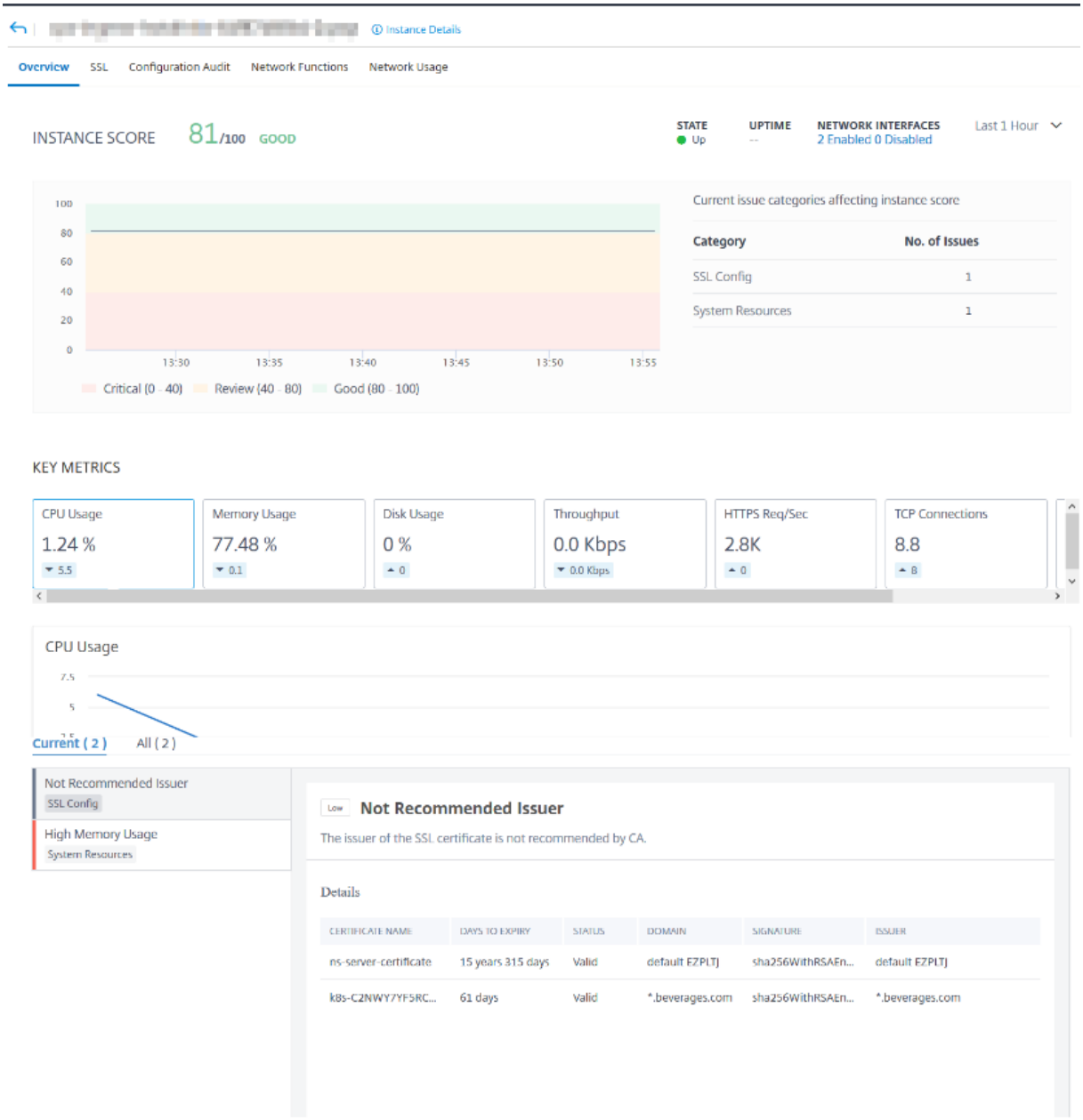
Das Instanzen-Dashboard in NetScaler ADM zeigt Daten in einem tabellarischen und grafischen Format für die ausgewählte Instanz an. Daten, die während des Abfragevorgangs von Ihrer Instanz gesammelt wurden, werden im Dashboard angezeigt.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **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.
- **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, die Daten wie Clientverbindungen, Durchsatz und Serververbindungen anzeigen.
- **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 zusätzlichen 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.

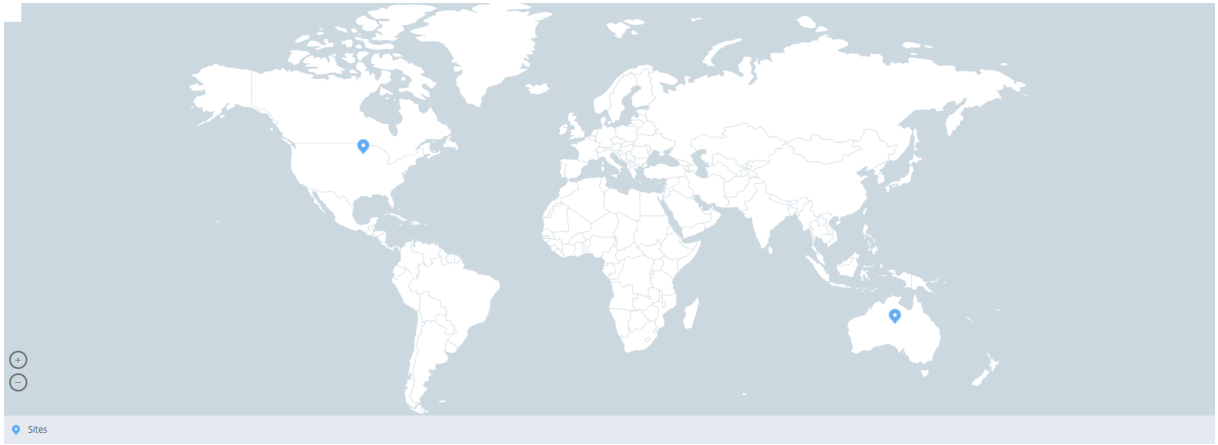
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

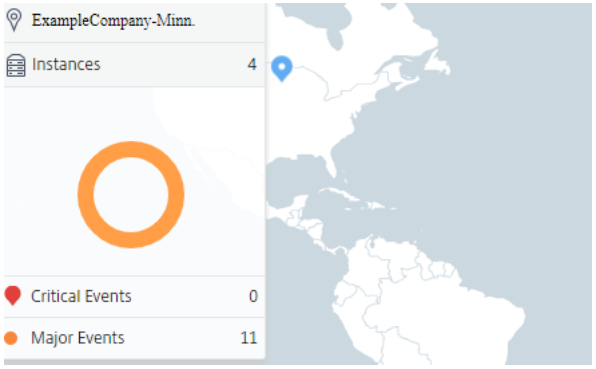
Geomaps in NetScaler ADM bieten Ihnen eine grafische Darstellung Ihrer Websites. Geomaps schlüsselt auch Ihre Netzwerküberwachungserfahrung nach Geografie auf. Mit Geomaps können Sie Ihre Netzwerkinstanzverteilung nach Standort visualisieren und alle Netzwerkprobleme überwachen. Sie können zur Seite "**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.



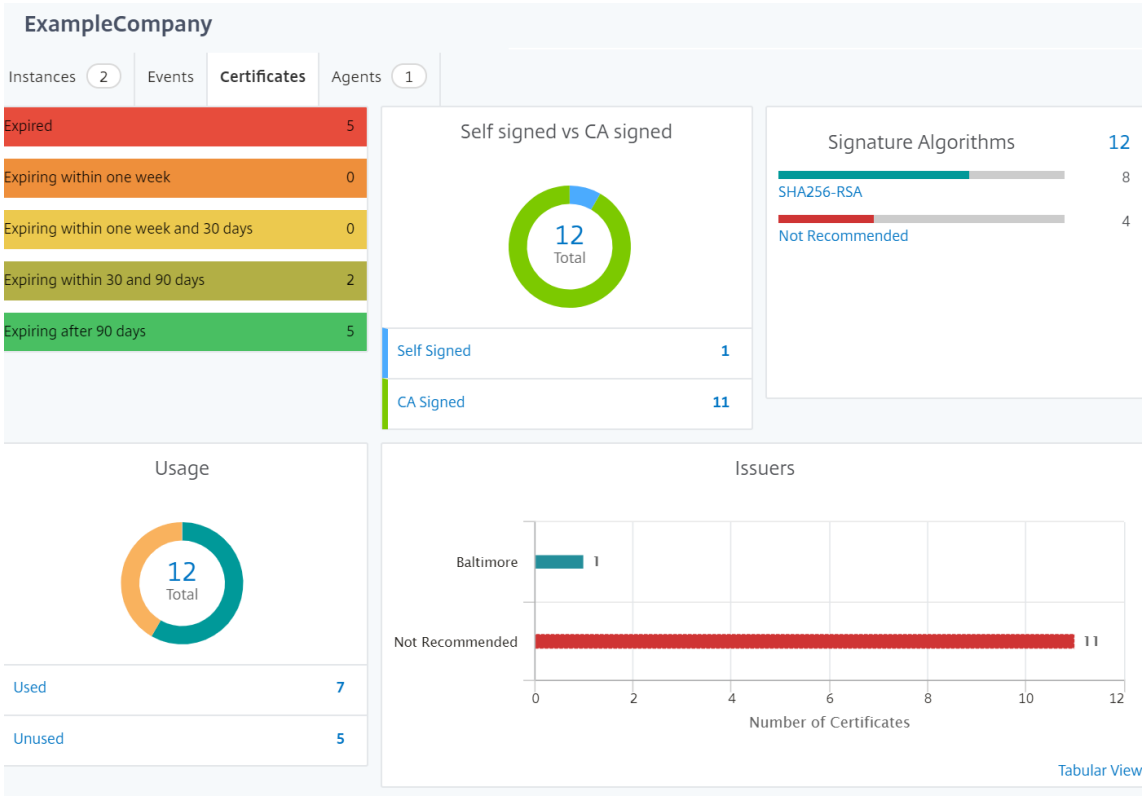
Die Marker zeigen auch eine Zahl an, die die Anzahl der Anwendungen an jedem Standort anzeigt. Sie können auf diese Marker klicken, um weitere Informationen zu den einzelnen Websites zu erhalten.



Klicken Sie auf die Registerkarten, um weitere Informationen anzuzeigen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

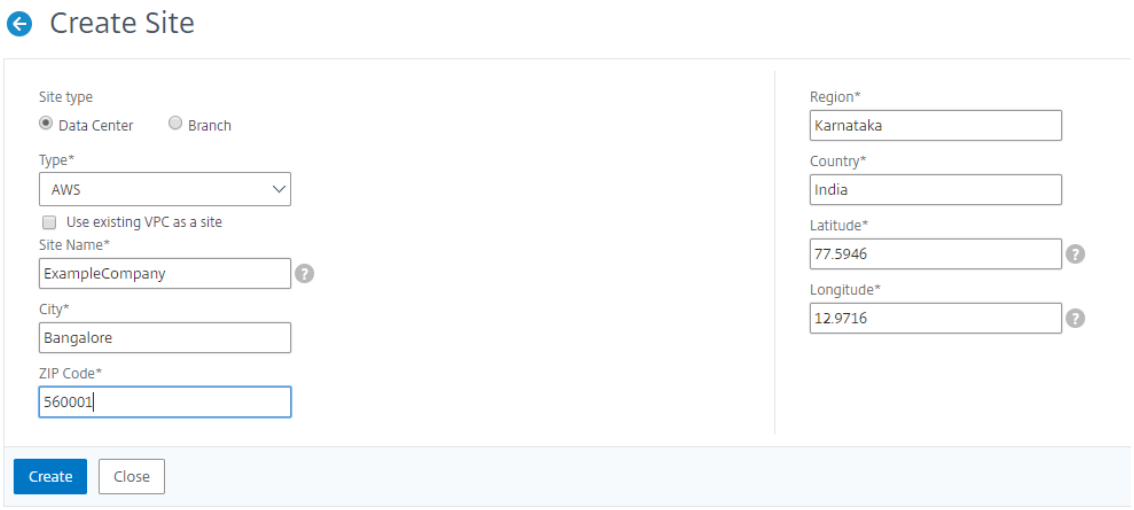
   Geben Sie für den südlichen Breitengrad negative Werte an. Beispiel: `-77.5946`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

i) **Längengrad**: Geben Sie den Längengrad der Position ein.

Geben Sie für den westlichen Längengrad negative Werte an. Beispiel: `-12.9716`.

2. Klicken Sie auf **Erstellen**.



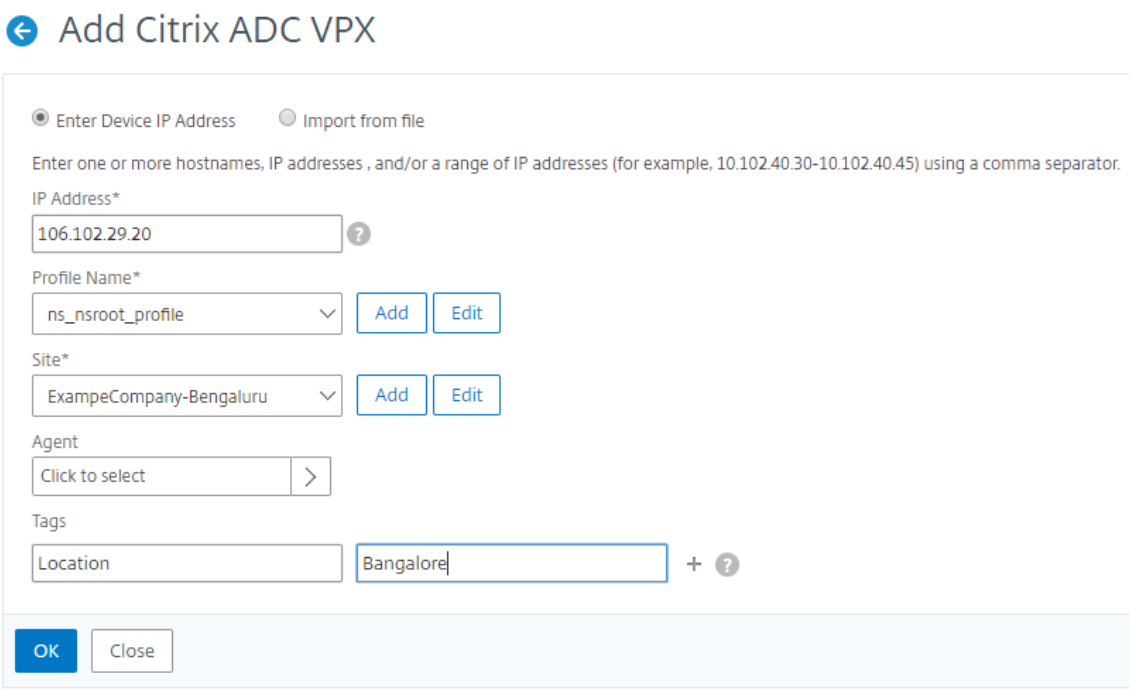
So fügen Sie Instanzen hinzu und wählen Sie Sites aus:

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.

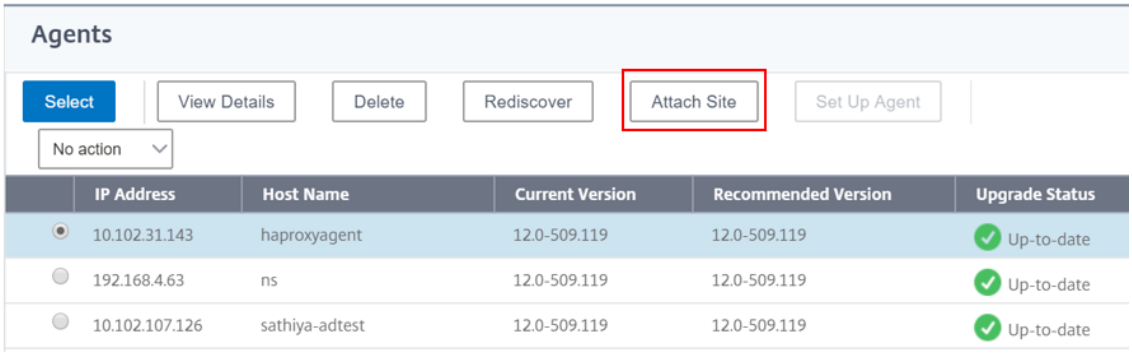
Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler ADM hinzufügen. Sie können die zuvor erstellte Site auswählen, oder Sie können auch eine Site erstellen und die Instanz zuordnen.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

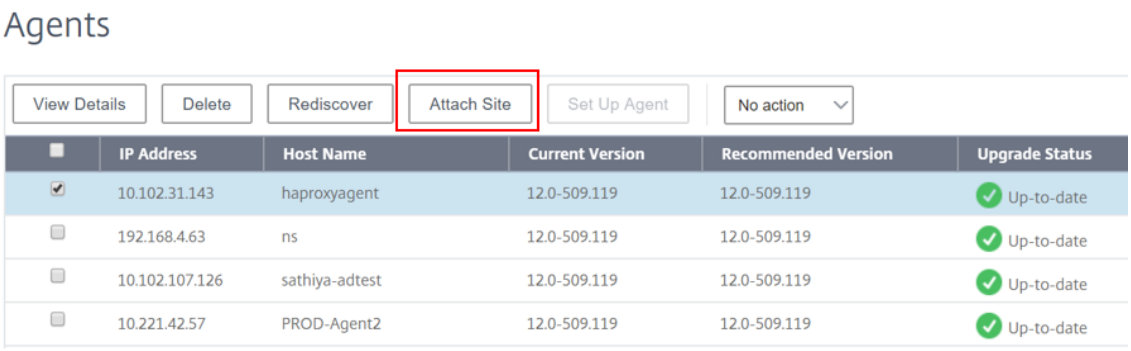
1. Klicken Sie auf **OK**.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Markieren von Instanzen Ihnen hilft, diese besser zu überwachen.

- **Anwendungsfall 1**: Sie können ein Tag erstellen, um alle Instanzen zu identifizieren, die sich im Vereinigten Königreich befinden. Hier können Sie ein Tag mit dem Schlüssel Land und dem Wert UK erstellen. Mit diesem Tag können Sie alle Instanzen suchen und überwachen, die sich in Großbritannien befinden.
- **Anwendungsfall 2**: Sie möchten nach Instanzen suchen, die sich in der Stagingumgebung befinden. Hier können Sie ein Tag mit dem Schlüssel als Zweck und 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**: Stellen Sie sich eine Situation vor, in der Sie die Liste der Citrix ADC Instanzen ermitteln möchten, die sich in Swindon im Vereinigten Königreich befinden und im Besitz von Ihnen sind, David T. Sie können Tags für all diese Anforderungen erstellen und diese allen Instanzen zuweisen, die diese Bedingungen erfüllen.

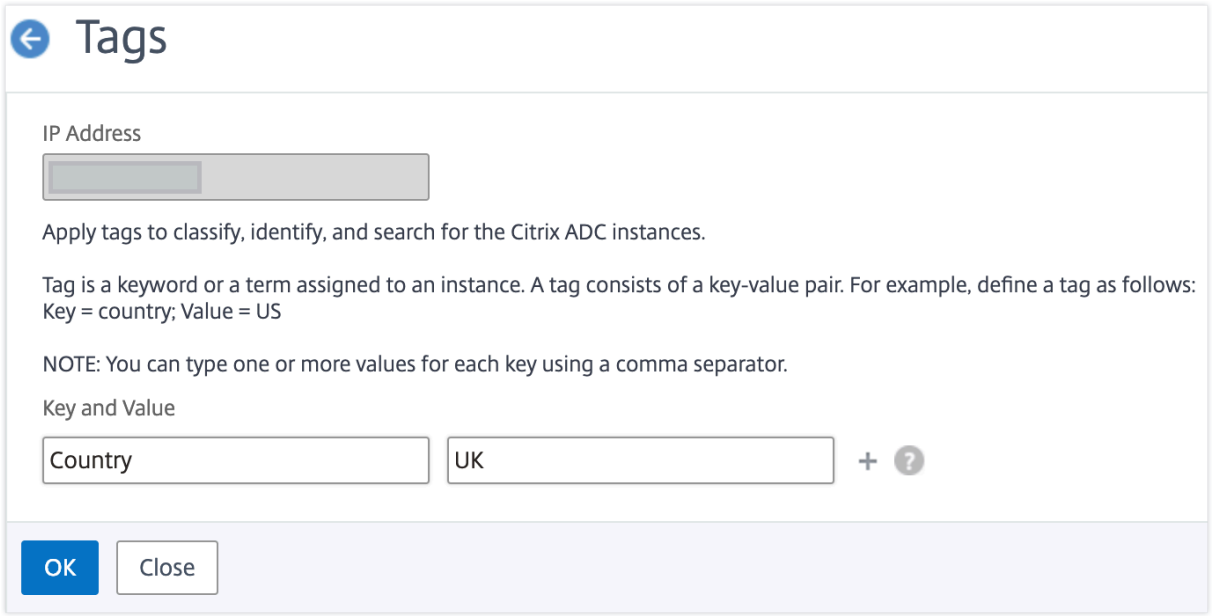
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

So weisen Sie der NetScaler ADC VPX Instanz Tags zu:

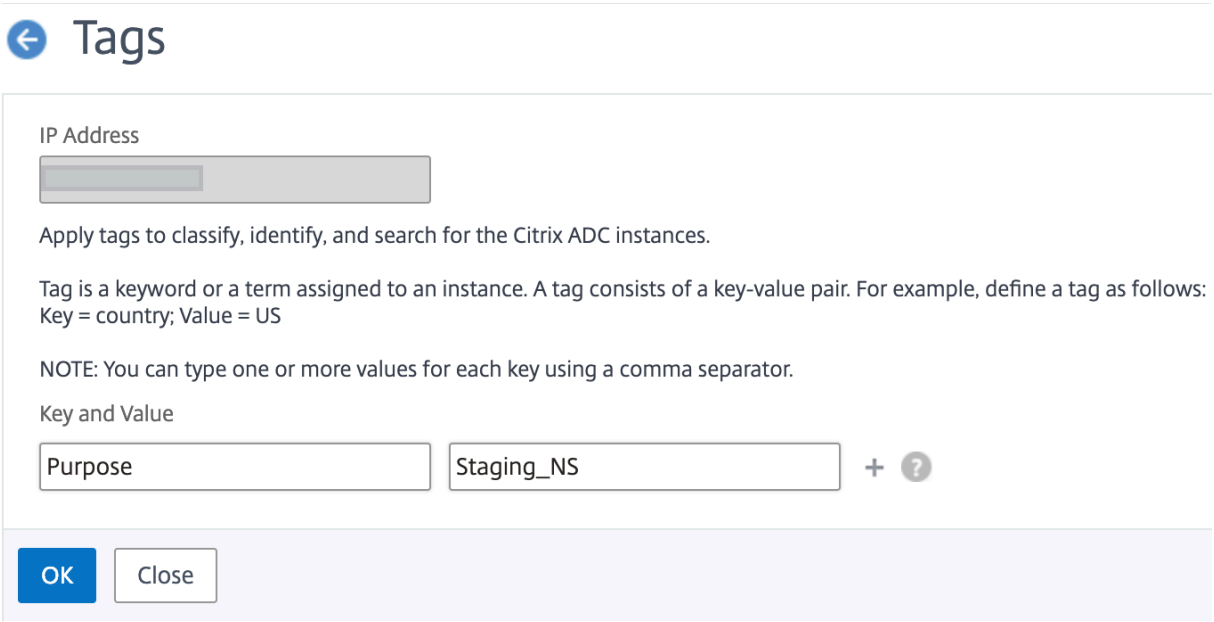
1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **Instanzen** > **Citrix ADC**.
2. Wählen Sie die Registerkarte **NetScaler ADC VPX** aus.
3. Wählen Sie das erforderliche Citrix VPX aus.
4. Klicken Sie **auf Tags**.
5. Erstellen Sie Tags und klicken Sie auf **OK**.

Im angezeigten **Tags-Fenster** können Sie Ihre eigenen "Schlüssel-Wert"-Paare erstellen, indem Sie jedem von Ihnen erstellten Schlüsselwort Werte zuweisen.

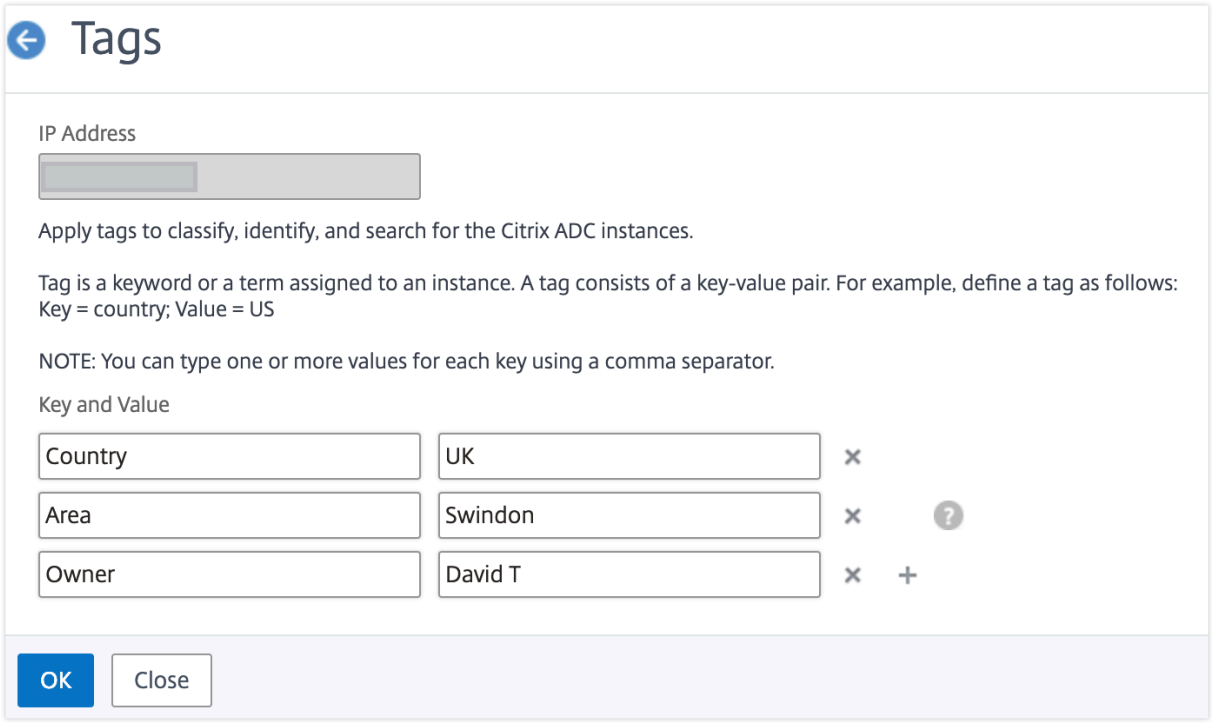
Die folgenden Bilder zeigen beispielsweise einige erstellte Keywords und deren Werte. Sie können eigene Schlüsselwörter hinzufügen und für jedes Schlüsselwort einen Wert eingeben.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



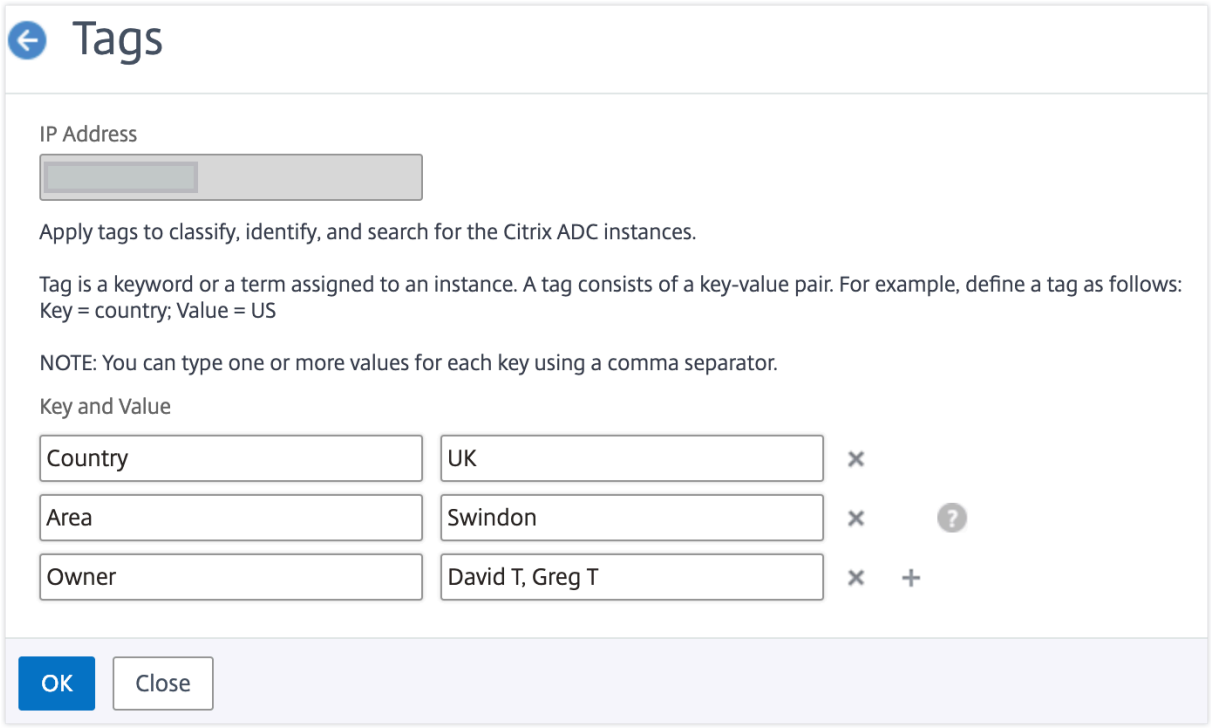
Sie können auch mehrere Tags hinzufügen, indem Sie auf "+"klicken. Durch das Hinzufügen mehrerer und aussagekräftiger Tags können Sie sehr effizient nach den Instanzen suchen.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen darüber, wie Sie anhand von Tags nach Instances suchen, finden Sie unter So suchen Sie Instances mithilfe von Werten von Tags und Eigenschaften .

> **Hinweis**
>
> Sie können später neue Tags hinzufügen oder vorhandene Tags löschen. Es gibt keine Einschränkung für die Anzahl der Tags, die Sie erstellen.

Instanzen über Werte von Tags und Eigenschaften suchen

February 5, 2024

Es kann eine Situation geben, in der Citrix Application Delivery Management (ADM) eine große Anzahl von Citrix 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 von Ihnen einer NetScaler ADC-Instanz zugewiesen werden können, um zusätzliche Beschreibung zur NetScaler ADC-Instanz hinzuzufügen. Sie können Ihre NetScaler ADC-Instanzen nun Tags zuordnen. Diese Tags

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Beispielsweise hat jede Instanz ihren eigenen Hostnamen, IP-Adresse, Version, Host-ID, Hardware-Modell-ID usw. 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 So erstellen Sie Tags und Zuweisen zu Instanzen.

Sie können eine Kombination aus Tags und Eigenschaften verwenden, um eigene Suchkriterien zu erstellen.

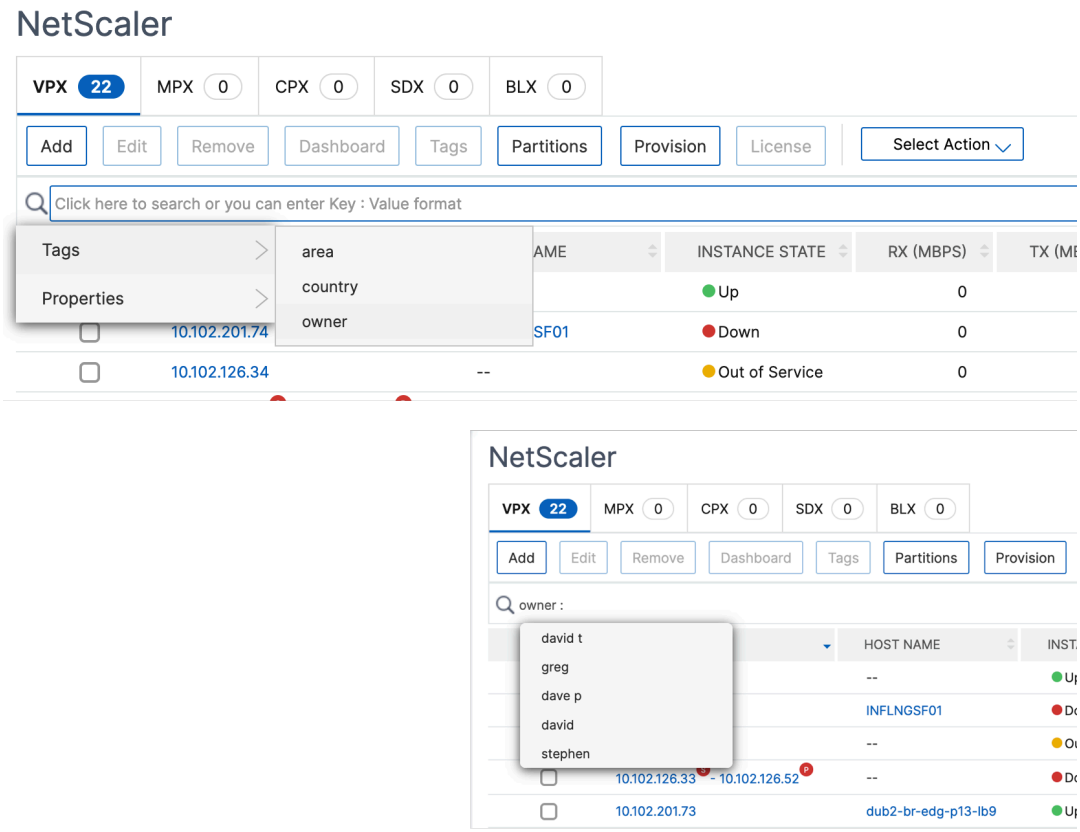
So suchen Sie nach NetScaler ADC VPX Instanzen

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.

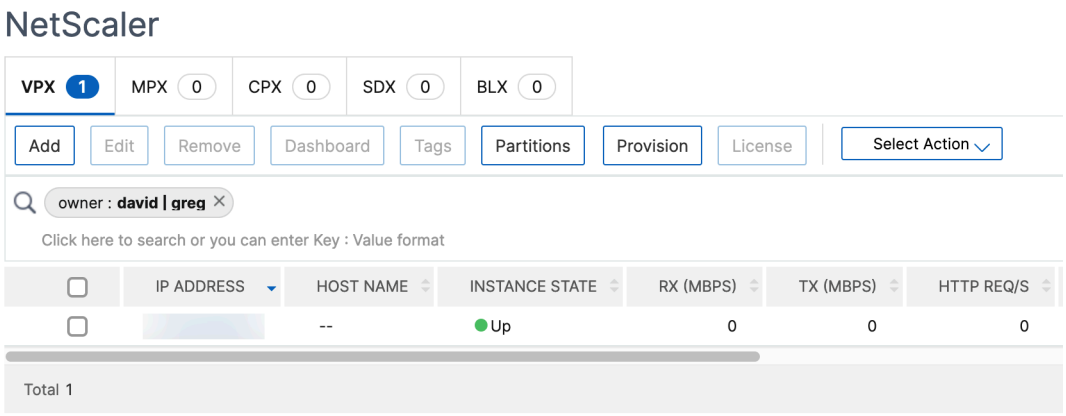
   a) Wählen Sie die Option **Tags** und dann **Besitzer**aus. Wählen Sie “David T.”

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



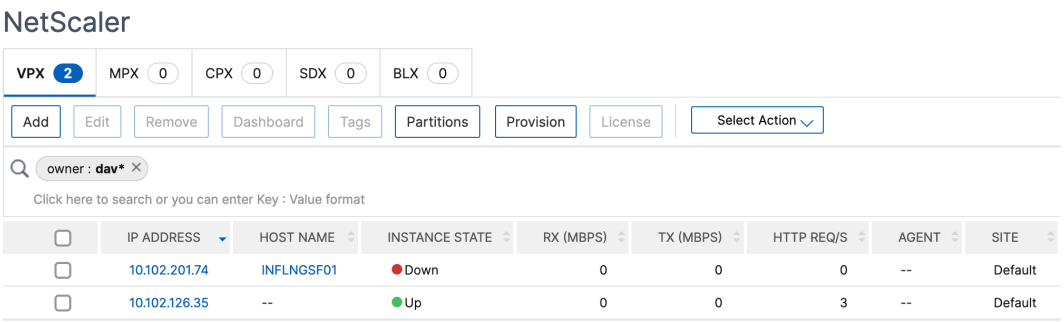
NetScaler ADM unterstützt reguläre Ausdrücke und Platzhalterzeichen in den Suchausdrücken.

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*”eingeben, um nach allen Instanzen zu suchen, die David T und Dave P gehören.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

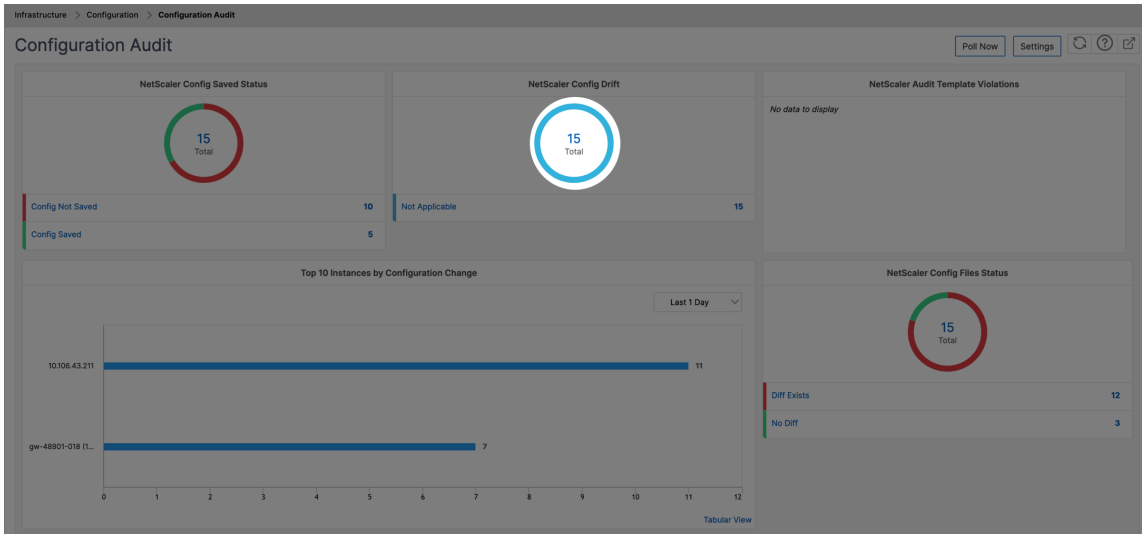
Nachdem Sie die Admin-Partition erstellt haben, können Sie zu Prüfungszwecken auch die Funktion zum Unterschied des Versionsverlaufs und die Funktion Auditvorlage für die Admin-Partition verwenden.

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.

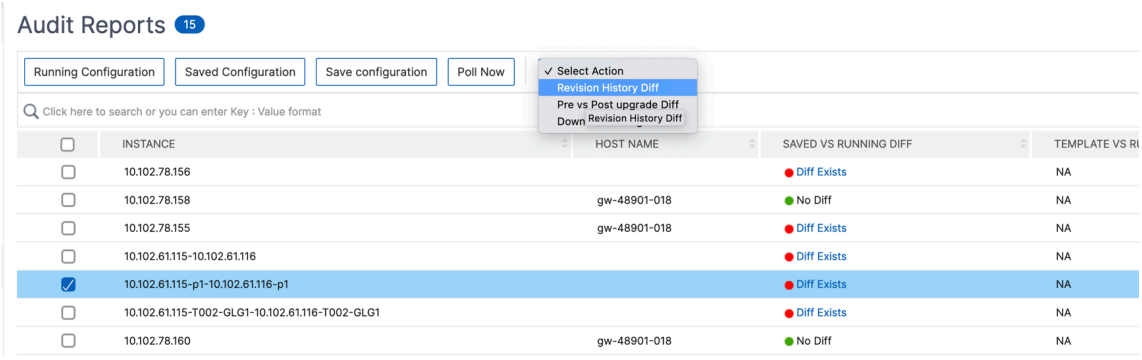
So zeigen Sie die Differenz der Versionshistorie an:

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.

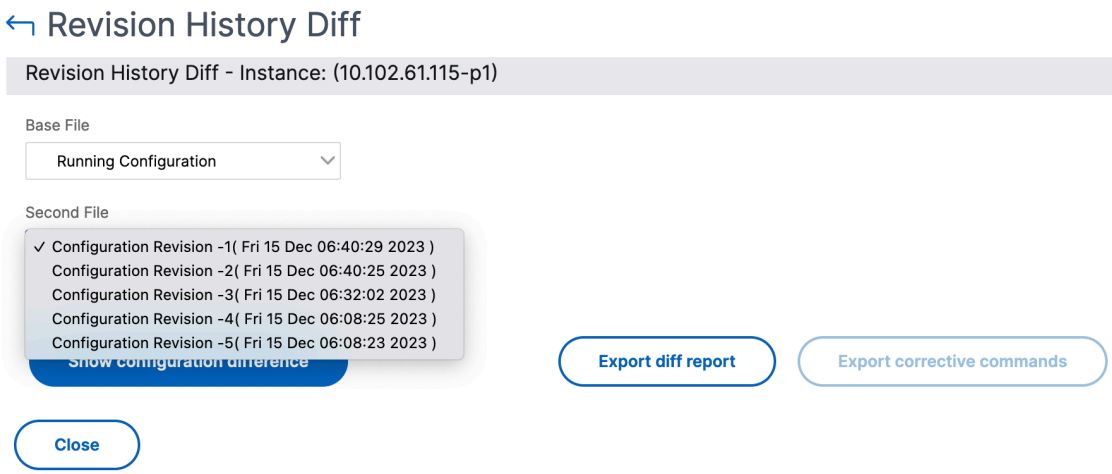
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Klicken Sie im Menü **Aktion** auf **Versionsverlauf Diff.**

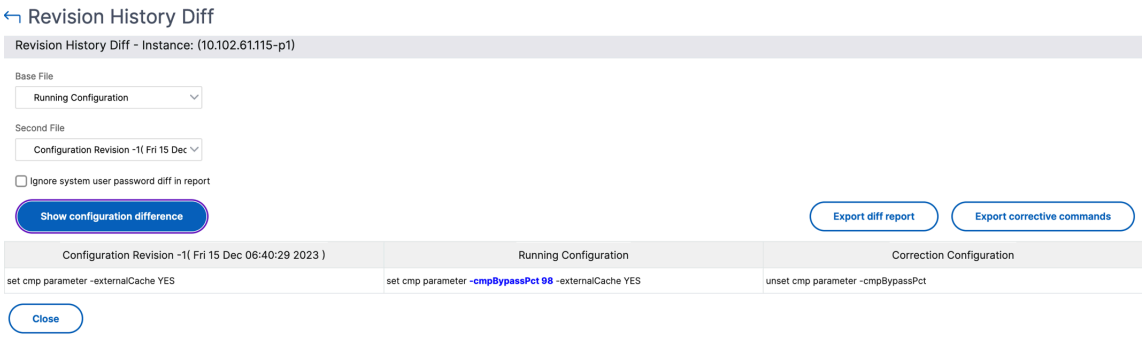


3. Wählen Sie auf der Seite **Versionsverlauf-Diff** die Dateien aus, die Sie vergleichen möchten. Vergleichen Sie beispielsweise die gespeicherte Konfiguration mit der Konfigurationsversion -1, und klicken Sie dann auf **Konfigurationsdifferenz anzeigen**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

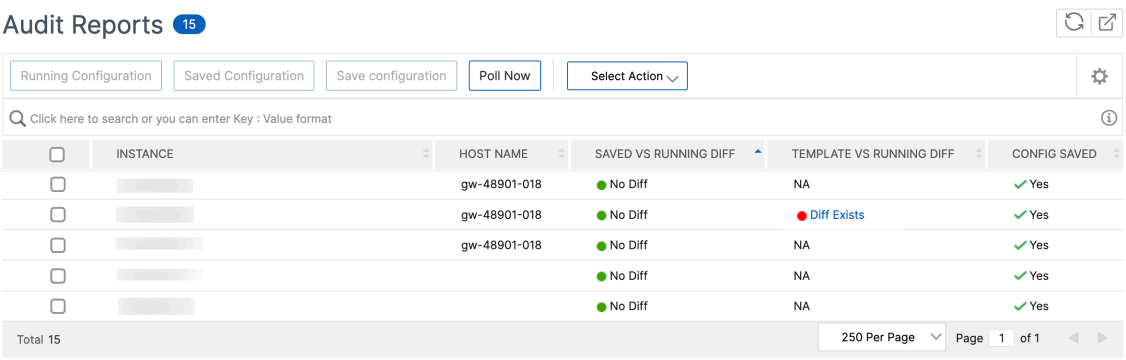
4. Sie können dann den Unterschied zwischen den fünf neuesten Konfigurationsdateien für die ausgewählte partitionierte NetScaler ADC Instanz anzeigen, wie unten gezeigt. Sie können auch die Korrekturkonfigurationsbefehle anzeigen und diese Korrekturbefehle in Ihren lokalen Ordner exportieren. Diese Korrekturbefehle sind die Befehle, die in der 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.

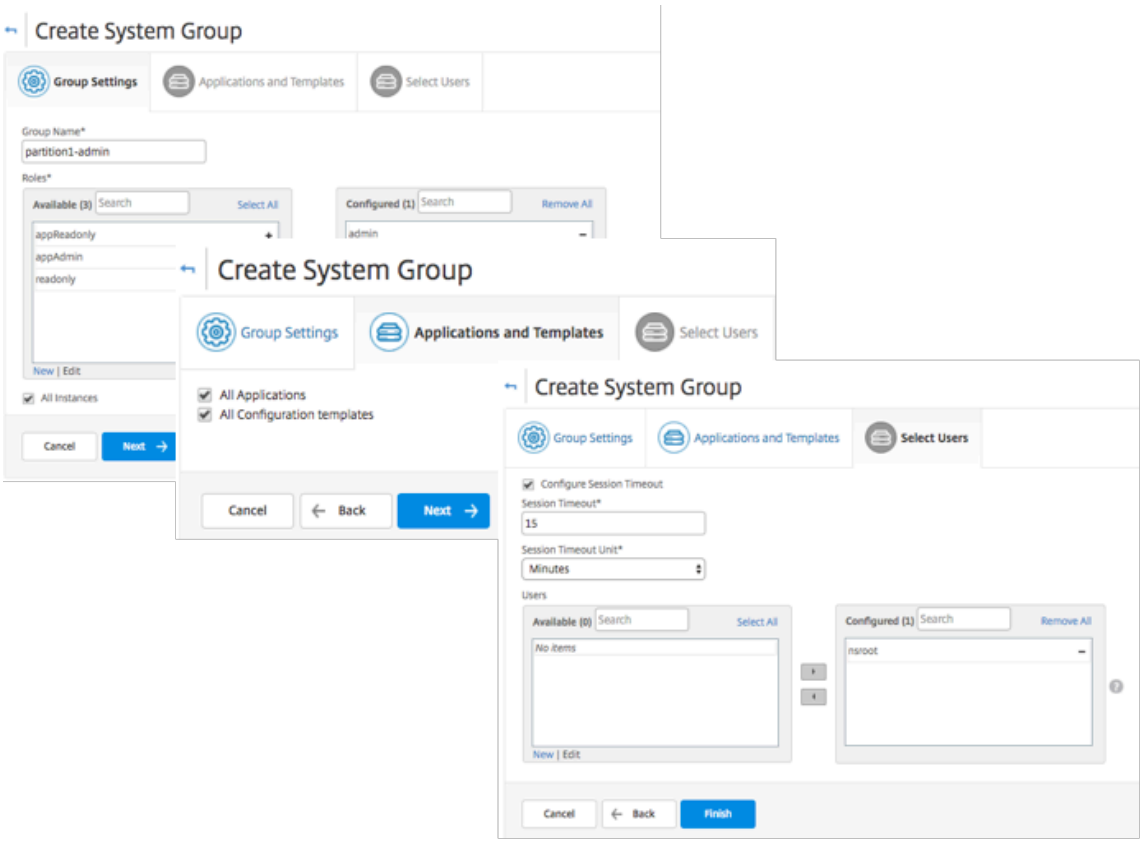


2. Wenn zwischen der Überwachungsvorlage und der laufenden Konfiguration ein Unterschied besteht, wird der Unterschied als Hyperlink angezeigt. Klicken Sie auf den Hyperlink, um die Unterschiede anzuzeigen, falls vorhanden. Neben den Unterschieden in der Konfiguration werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So erstellen Sie Gruppen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Gruppen**, und klicken Sie dann auf **Hinzufügen**.
2. Geben **Sie auf der Seite "Systembenutzer erstellen** "Folgendes an:
   - Registerkarte „**Gruppeneinstellungen** ": Geben Sie den Gruppennamen und die Rollenberechtigungen ein. Um den Zugriff auf bestimmte Instances zu ermöglichen, deaktivieren Sie das Kontrollkästchen**All Instances**und wählen Sie dann Ihre Instances auf der Seite **Select Instances aus** .
   - Registerkarte „**Anwendungen und Vorlagen** ": Sie können wählen, ob Sie diese Gruppe für alle Anwendungen und Konfigurationsvorlagen verwenden möchten.
   - Registerkarte**Benutzer auswählen** : Wählen Sie Benutzer aus, die Sie dieser Gruppe hinzufügen möchten. Sie können auf den Link **Neu** in der Tabelle **Verfügbar** klicken, um neue Benutzer zu erstellen. Konfigurieren Sie optional das Sitzungstimeout, in dem Sie den Zeitraum konfigurieren können, wie lange ein Benutzer aktiv bleiben kann.
3. Klicken Sie auf **Fertig stellen**.



So erstellen Sie Benutzer:

1. Navigieren Sie zu**System**>**Benutzerverwaltung**>**Benutzer**, und klicken Sie dann auf **Hinzufügen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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. Sie müssen eine Instanz immer sichern, bevor Sie sie aktualisieren oder aus vorsorglichen Gründen. Backup eines stabilen Systems ermöglicht es Ihnen, es wieder zu einem stabilen Punkt wiederherzustellen, wenn es instabil wird.

Es gibt mehrere Möglichkeiten, Backups und Wiederherstellungen auf einer NetScaler 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

Weitere Informationen finden Sie unter [Sichern und Wiederherstellen einer ADC-Instanz].(https://docs.citrix.com/en-us/citrix-adc/12-1/system/basic-operations/backup-restore-citrix-adc-appliance.html)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> - 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 maximal 50 Backupdateien in diesem Verzeichnis 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:

Navigieren Sie in NetScaler ADM zu **System** > **Systemadministration**. **Wählen Sie im rechten Bereich unter Instanzeinstellungen die Option Instanz-Backup-Einstellungen** aus und geben Sie Folgendes an:

1. **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.
2. **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.

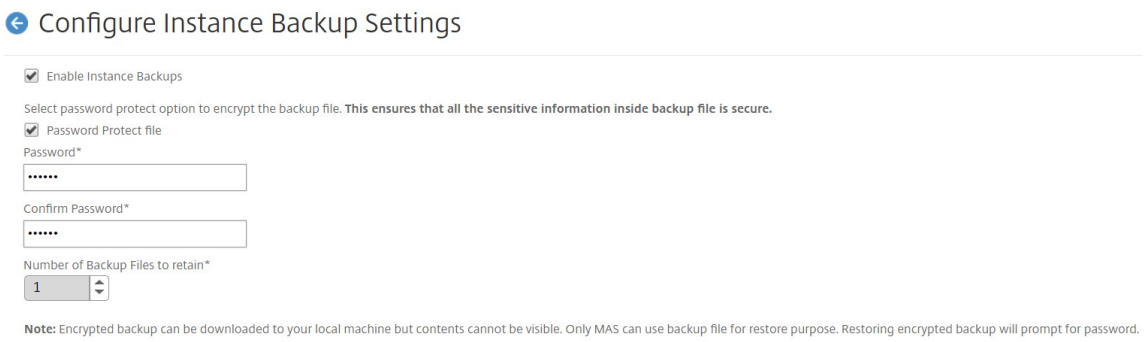
   > **Hinweis**
   >
   > Sie können die verschlüsselte Backupdatei auf Ihren lokalen Computer herunterladen, Sie können die Datei jedoch weder mit NetScaler ADM GUI noch mit einem Texteditor öffnen. Die Datei kann allein von Citrix ADM abgerufen und verwendet werden. Beim Wiederherstellen der verschlüsselten Backupdatei werden Sie aufgefordert, das Kennwort

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> anzugeben. Sie können jedoch eine unverschlüsselte Sicherungsdatei auf Ihrem System öffnen.

3. **Anzahl der beizubehaltenden Backupdateien**: Geben Sie die Anzahl der Backupdateien an, die in NetScaler ADM aufbewahrt werden sollen. Sie können bis zu 50 Sicherungsdateien des aktuellen Status einer Citrix ADC-Instanz 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.

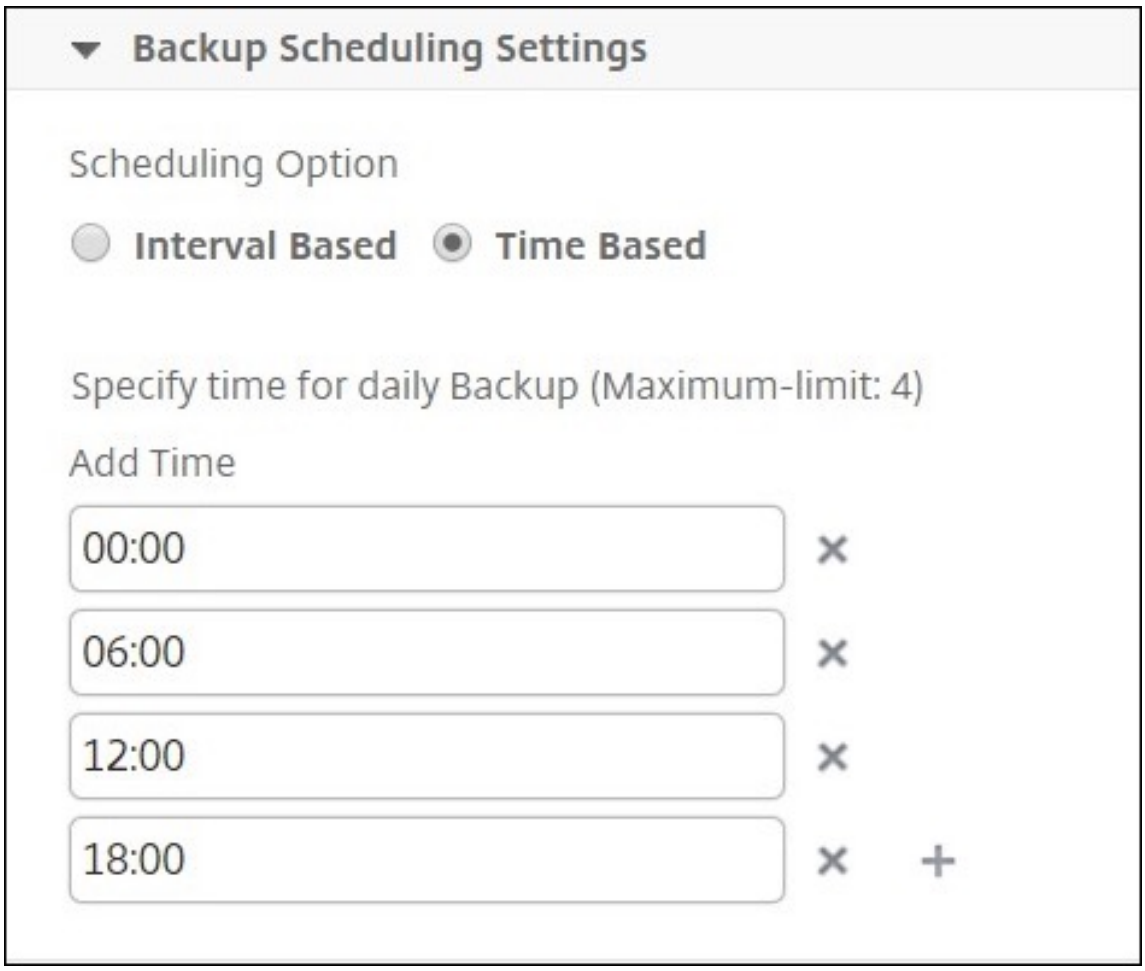


4. **Einstellungen für die Backupplanung**: (optional) Zum Erstellen von Backupdateien stehen zwei Optionen zur Verfügung, obwohl Sie jeweils nur eine Option verwenden können:

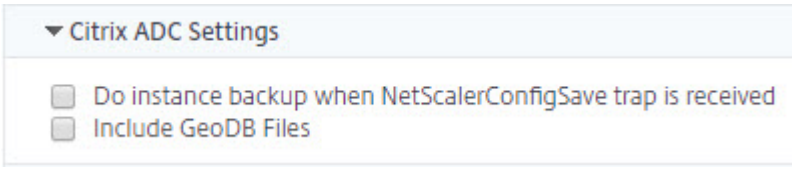
   a) Die Standardoption für die Backupplanung ist “intervalbasiert”. Nach Ablauf des angegebenen Intervalls wird in Citrix ADM eine Backupdatei erstellt. Das Standardintervall für Backups ist 12 Stunden.

   b) Sie können auch den Typ der geplanten Backups in “zeitbasiert”ändern. In dieser Option geben Sie die Uhrzeit im Format „Stunden:Minuten“an, zu der das Backup erfolgen soll. Mit NetScaler ADM können maximal vier tägliche Backups auf den Instanzen durchgeführt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. **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.
6. **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.



7. **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.

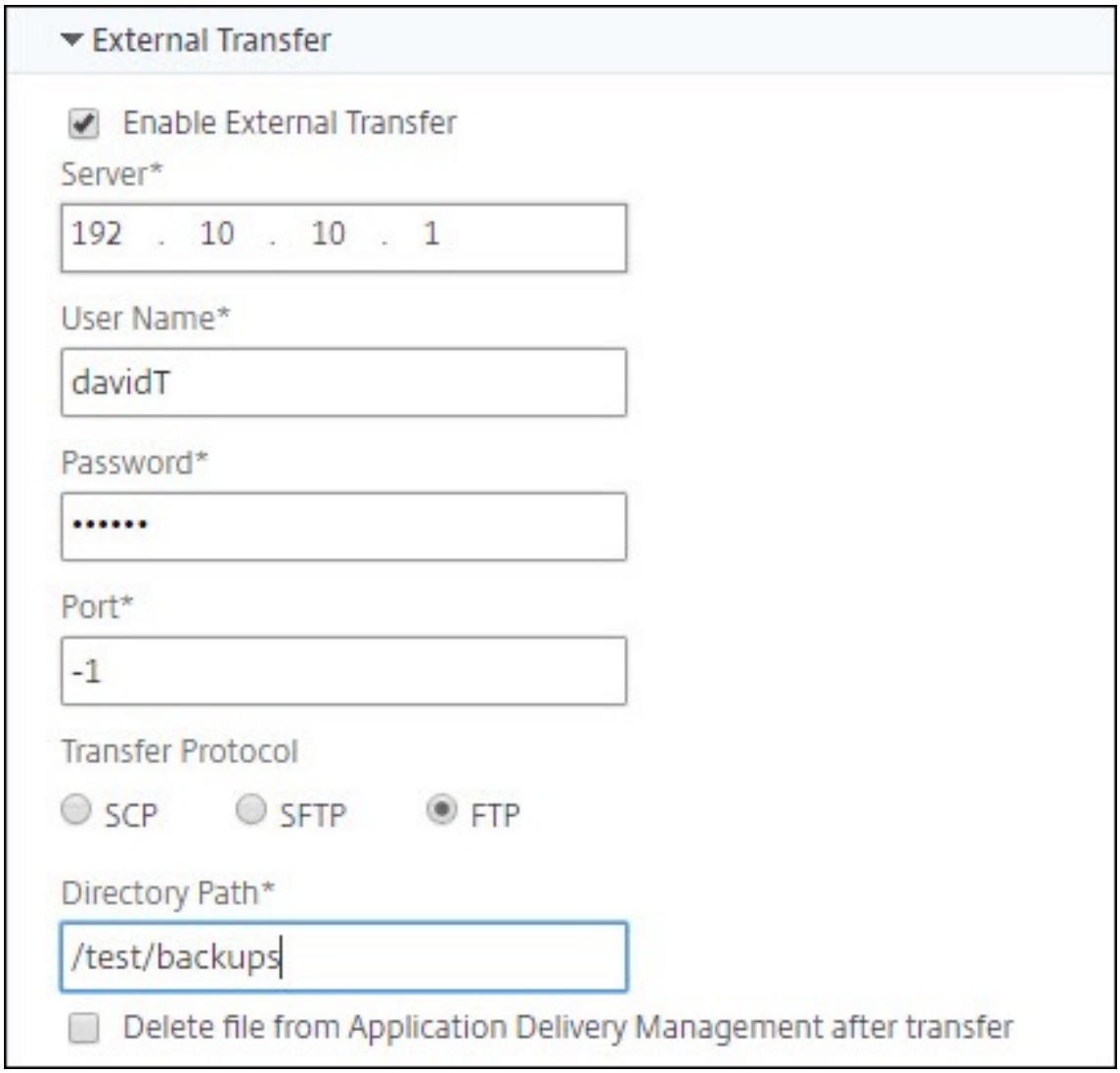
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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) Sie haben auch die Möglichkeit, die Sicherungsdatei aus Citrix ADM zu 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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- und VPX-Instanzen **Backup/Restore** aus der Liste **Select Action** aus.
   - Klicken Sie für eine SDX-Instanz auf **Backup/Restore**.
3. Klicken Sie auf der Seite **Backupdateien** auf **Backup**.
4. Sie können angeben, ob Ihre Sicherungsdatei für zusätzliche Sicherheit verschlüsselt werden soll. 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

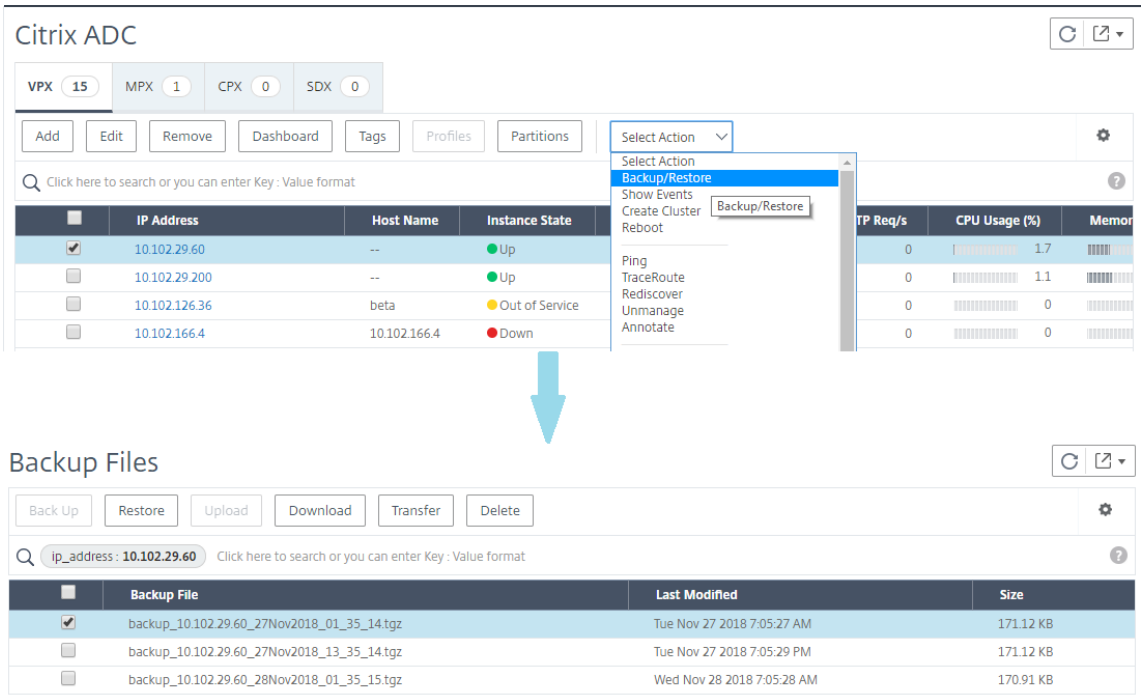
> Hinweis:
>
> Wenn Sie NetScaler ADC-Instanzen in einem HA-Paar haben, müssen Sie Folgendes beachten:
>
> - Stellen Sie dieselbe Instanz wieder her, aus der die Backupdatei erstellt wurde. Betrachten wir beispielsweise ein Szenario, dass ein Backup von der primären Instanz des HA-Paares genommen wurde. 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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)

Sie müssen Ihre NetScaler ADC SDX-Appliance auf die in der Backupdatei verfügbare Konfiguration wiederherstellen. Während der Wiederherstellung der Appliance wird die gesamte aktuelle Konfiguration gelöscht.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie die NetScaler ADC SDX-Appliance mithilfe einer Sicherung einer anderen NetScaler ADC SDX-Appliance wiederherstellen, stellen Sie sicher, dass Sie die Lizenzen hinzufügen und die Verwaltungsdienst-Netzwerkeinstellungen der Appliance so konfigurieren, dass sie mit denen in der Sicherungsdatei übereinstimmen, bevor Sie den Wiederherstellungsvorgang starten.

Stellen Sie sicher, dass die gesicherte Citrix ADC SDX-Plattformvariante mit der Version identisch ist, auf der Sie wiederherstellen möchten. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

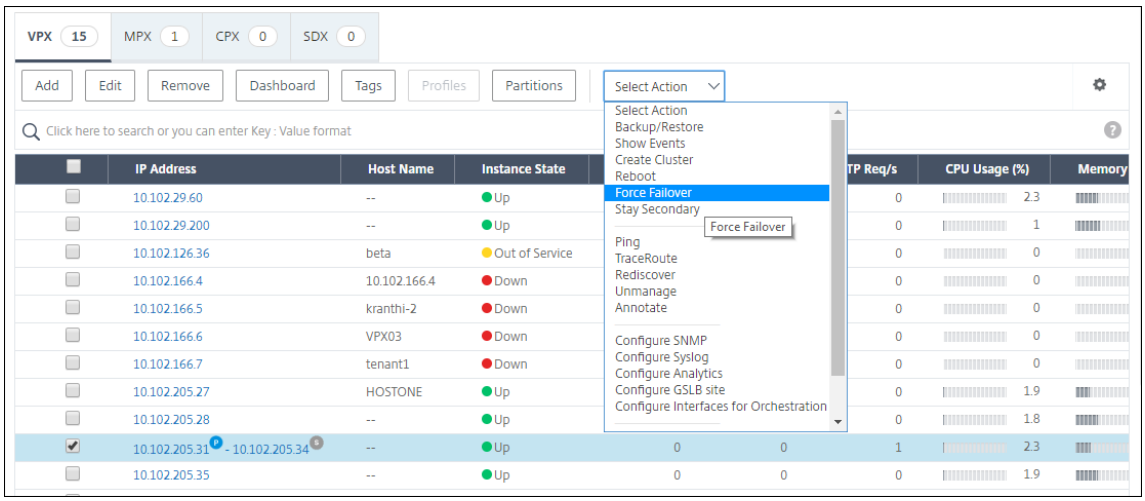
- Sie erzwingen ein Failover auf einem eigenständigen System.
- Die sekundäre Instanz ist deaktiviert oder inaktiv. Wenn sich die sekundäre Instanz in einem inaktiven Zustand befindet, müssen Sie warten, bis ihr Status AKTIV ist, um ein Failover zu erzwingen.
- Die sekundäre Instanz ist konfiguriert, 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 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 **Force Failover**aus.
4. Klicken Sie auf **Ja**, um die Aktion “Failover erzwingen”zu bestätigen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 wird der primäre Knoten möglicherweise einige Sekunden lang heruntergefahren, aber Sie möchten nicht, dass der sekundäre Knoten übernommen wird. Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

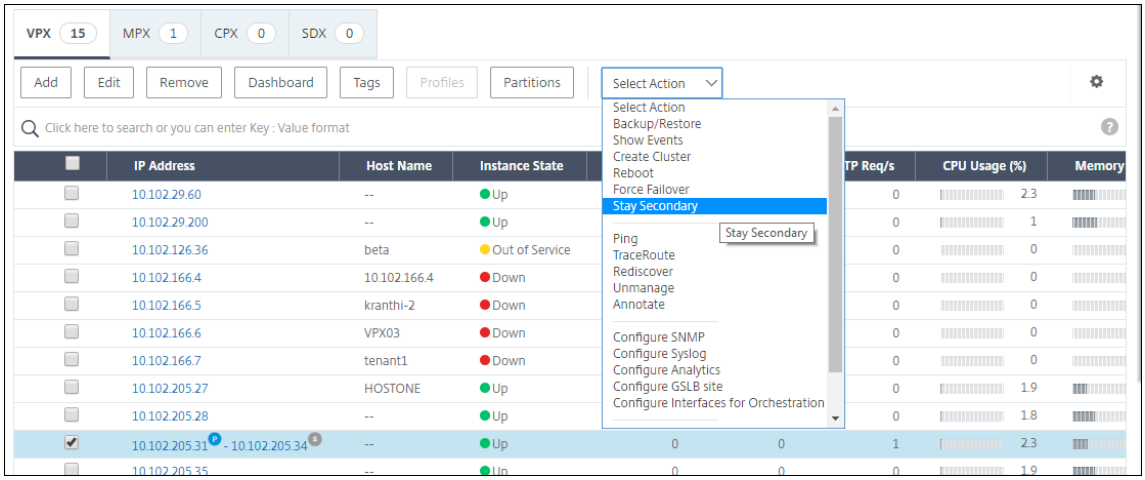
Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er auch dann sekundär, wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Instanzgruppen erstellen

February 5, 2024

Um eine Instanzgruppe zu erstellen, müssen Sie zuerst alle Ihre Citrix Application Delivery Controller (ADC) -Instanzen zu Citrix Application Delivery Management (ADM) hinzufügen. Nachdem Sie die Instanzen erfolgreich hinzugefügt haben, erstellen Sie Instanzgruppen auf der Grundlage ihrer Gerätefamilie. Indem Sie eine Gruppe von Instanzen erstellen, können Sie Aktionen wie Upgrade, Backup und Wiederherstellung gleichzeitig für alle Instanzen ausführen, die gruppiert wurden, anstatt sie für jede Instanz separat durchzuführen.

So erstellen Sie eine Instanzgruppe mit Citrix ADM:

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Instanzgruppen**, und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie Ihrer Instanzgruppe einen Namen und wählen Sie die Instance-Familie aus der Liste aus.
3. **Wählen Sie im Menü Instanzfamilie den Instanztyp aus.
4. Klicken Sie auf **Instanzen** auswählen und wählen Sie die Instanzen aus dem Fenster aus, das eingeblendet wird.
5. Klicken Sie auf **Erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wiedererkennen mehrerer Citrix VPX-Instanzen

February 5, 2024

Sie können jetzt mehrere Citrix VPX-Instanzen in Ihrem Citrix Application Delivery Management (ADM) -Setup wiedererkennen. Zuvor konnten Sie nur einzelne Citrix VPX-Instanzen wiederfinden. Sie können mehrere Citrix VPX-Instanzen neu erkennen, wenn Sie die neuesten Status 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 standardmäßigen Administratoranmeldeinformationen sind nsroot und nsroot.
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

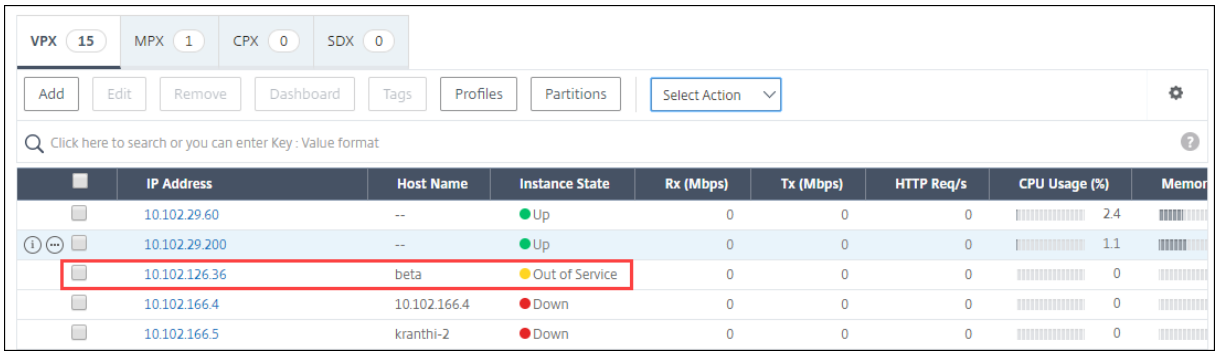
Wenn Sie den Informationsaustausch zwischen Citrix Application Delivery Management (ADM) und den Instanzen im Netzwerk beenden möchten, können Sie die Verwaltung der Instanzen aufheben.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Der Status der ausgewählten Instanz ändert sich in “**Abgemeldet**”, wie in der folgenden Abbildung dargestellt.



Die Instanz wird nicht mehr von Citrix ADM verwaltet und tauscht keine Daten mehr mit Citrix ADM aus.

Tracing einer Route zu einer Instanz

February 5, 2024

Wenn Sie die Route eines Pakets von Citrix Application Delivery Management (ADM) zu einer Instanz verfolgen, finden Sie Informationen wie die Anzahl der Hops, die erforderlich sind, um die Instanz zu erreichen. Traceroute verfolgt den Pfad des Pakets von Quelle zu Ziel. Es zeigt die Liste der Netzwerk-Hops zusammen mit dem Hostnamen und der IP-Adresse der einzelnen Entitäten in der Route an.

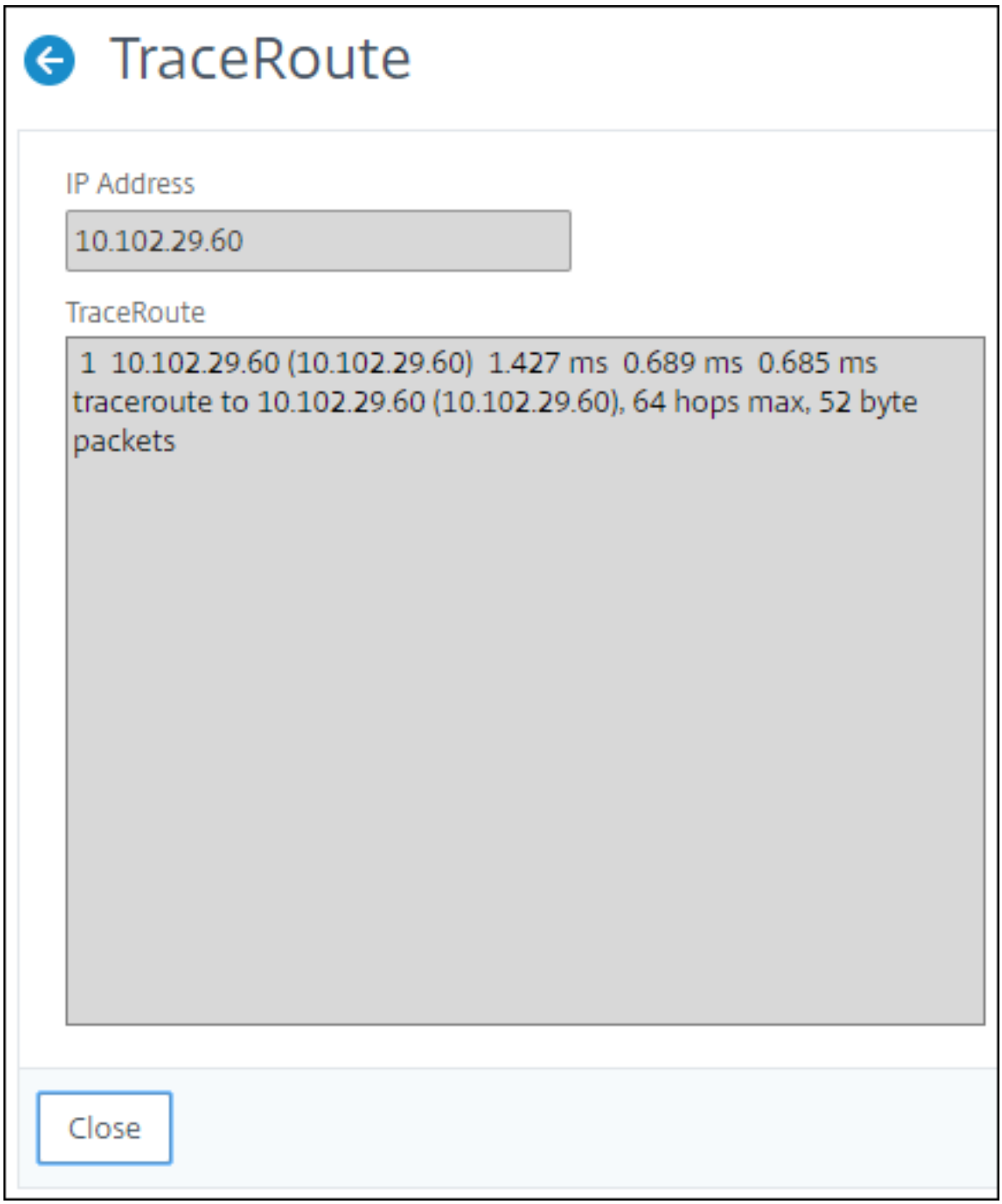
Traceroute erfasst auch die Zeit, die ein Paket für die Reise von einem Hop zum anderen nimmt. Wenn die Übertragung von Paketen unterbrochen wird, zeigt Traceroute, wo das Problem besteht.

So verfolgen Sie die Route einer Instanz:

1. Navigieren Sie in NetScaler ADM 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 Instanz und die von jedem Hop verbrauchte Zeit in Millisekunden an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ereignisse

February 5, 2024

Wenn die IP-Adresse einer Citrix Application Delivery Controller Instanz (ADC) zu NetScaler Application

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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.

Citrix ADM prüft auch die Ereignisse, die auf Instanzen generiert werden, um Alarme unterschiedlicher Schweregrade zu bilden, und zeigt sie als Meldungen an, von denen einige möglicherweise sofortige Aufmerksamkeit erfordern. Beispielsweise könnte ein Systemausfall als Schweregrad "kritisch" eingestuft werden und müsste sofort behoben werden.

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung einer großen Anzahl von Ereignissen, die in der Citrix ADC Infrastruktur generiert wurden.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, NetScaler ADC-Instanzen, Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können auch sicherstellen, dass für ein bestimmtes Zeitintervall für ein Ereignis mehrere Benachrichtigungen ausgelöst werden, bis das Ereignis gelöscht wird. Als zusätzliche Maßnahme können Sie Ihre E-Mail mit einer bestimmten Betreffzeile, einer Benutzernachricht anpassen und einen Anhang hochladen.

Ereignisdashboard verwenden

February 5, 2024

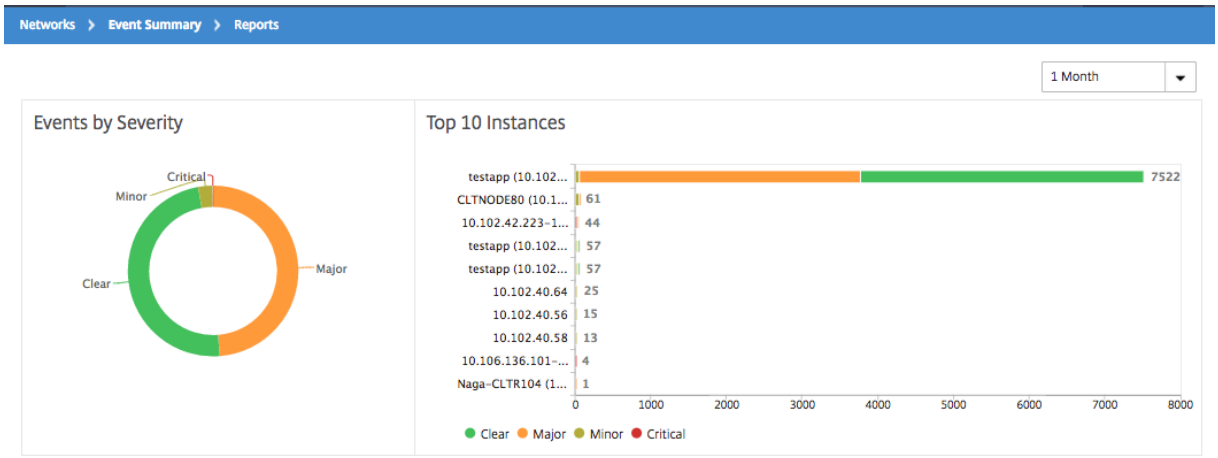
Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenwertverletzungen und Änderungen des Entitätsstatus auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen sowie Ereignisse und deren Schweregrad für bestimmte Instanzen einsehen. 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**.

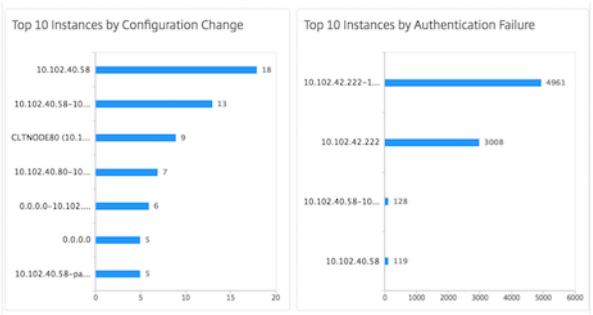
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Das Diagramm Top 10 Geräte auf dem Dashboard zeigt einen Bericht der Top 10 Instanzen anhand der Anzahl der auf ihnen erzeugten Ereignisse an. Sie können auf eine Instanz im Diagramm klicken, um weitere Details zum Schweregrad des Ereignisses anzuzeigen.



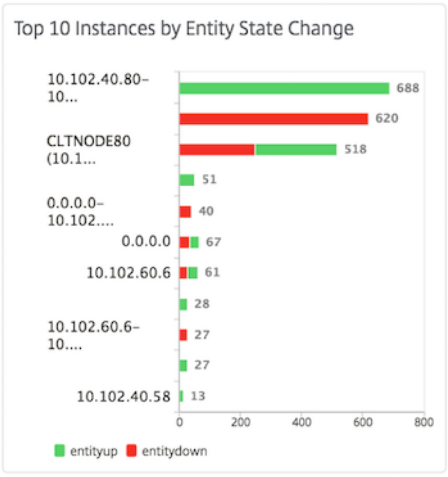
****Sie können weitere Details anzeigen, indem Sie zum Citrix ADC-Instanztyp (Netzwerke > **Ereignisse** > **Berichte** > **NetScaler/NetScaler SDX/NetScaler SD-WAN WO**) navigieren, um Folgendes anzuzeigen:

- Top 10 Geräte nach Hardwarefehler
- Top 10 Geräte nach Konfigurationsänderung
- Top 10 Geräte durch Authentifizierungsfehler

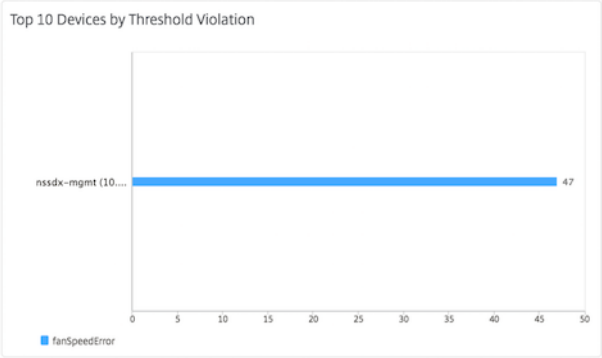


- Top 10 Geräte nach Entitätsstatusänderungen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 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.

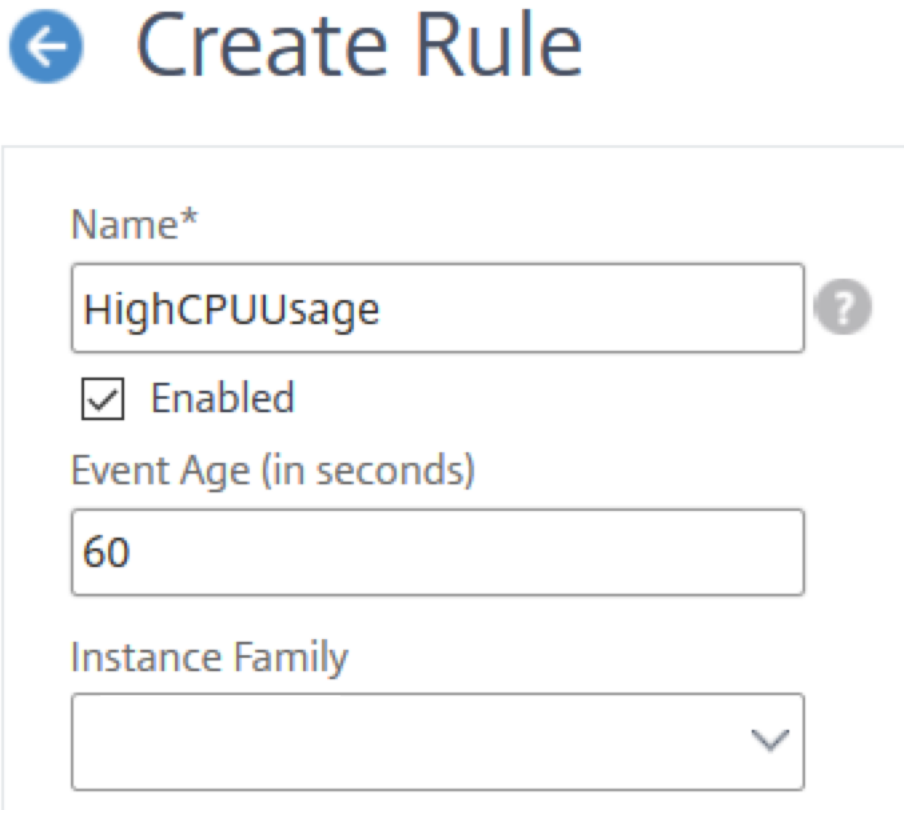
Stellen Sie sich beispielsweise vor, dass Sie verschiedene ADC-Appliances verwalten und per E-Mail benachrichtigt werden möchten, wenn einer Ihrer virtuellen Server für 60 Sekunden oder länger ausfällt. Sie können eine Ereignisregel mit den erforderlichen Filtern erstellen und das Ereignisalter der

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Regel auf 60 Sekunden festlegen. Wenn dann ein virtueller Server 60 oder mehr Sekunden lang heruntergefahren bleibt, erhalten Sie eine E-Mail-Benachrichtigung mit Details wie Entitätsname, Statusänderung und Zeit.

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 obigen Beispiel die Traps entityup, entitydown und entityofs aus.

Ereignisfilter planen

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

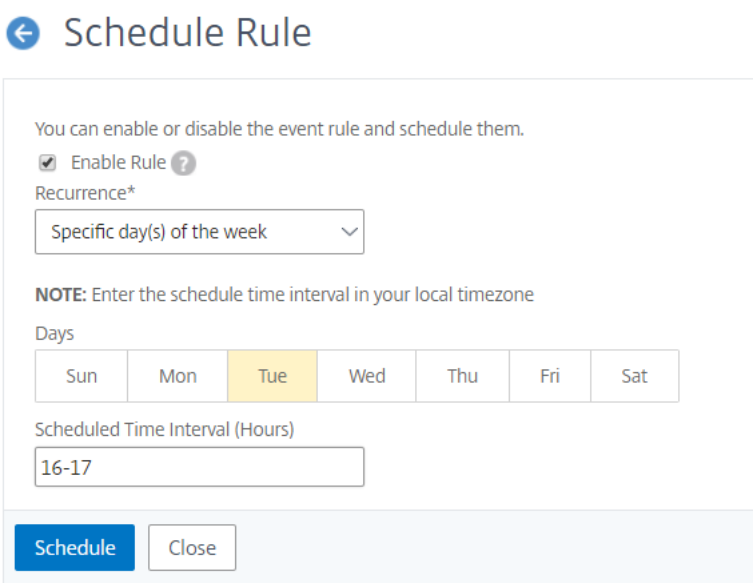
Wenn Sie einen Filter für diese Alarme konfiguriert und E-Mail-Benachrichtigungen für diese Filter aktiviert haben, sendet der Server eine große Anzahl von E-Mail-Benachrichtigungen, wenn Citrix ADM diese Traps empfängt. Wenn Sie möchten, dass der Server diese E-Mail-Benachrichtigungen nur während eines 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 das geplante Ereignis 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)** —Stunde (n), zu der die Regel geplant werden soll (verwenden Sie das 24-Stunden-Format).
4. Klicken Sie auf **Zeitplan**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

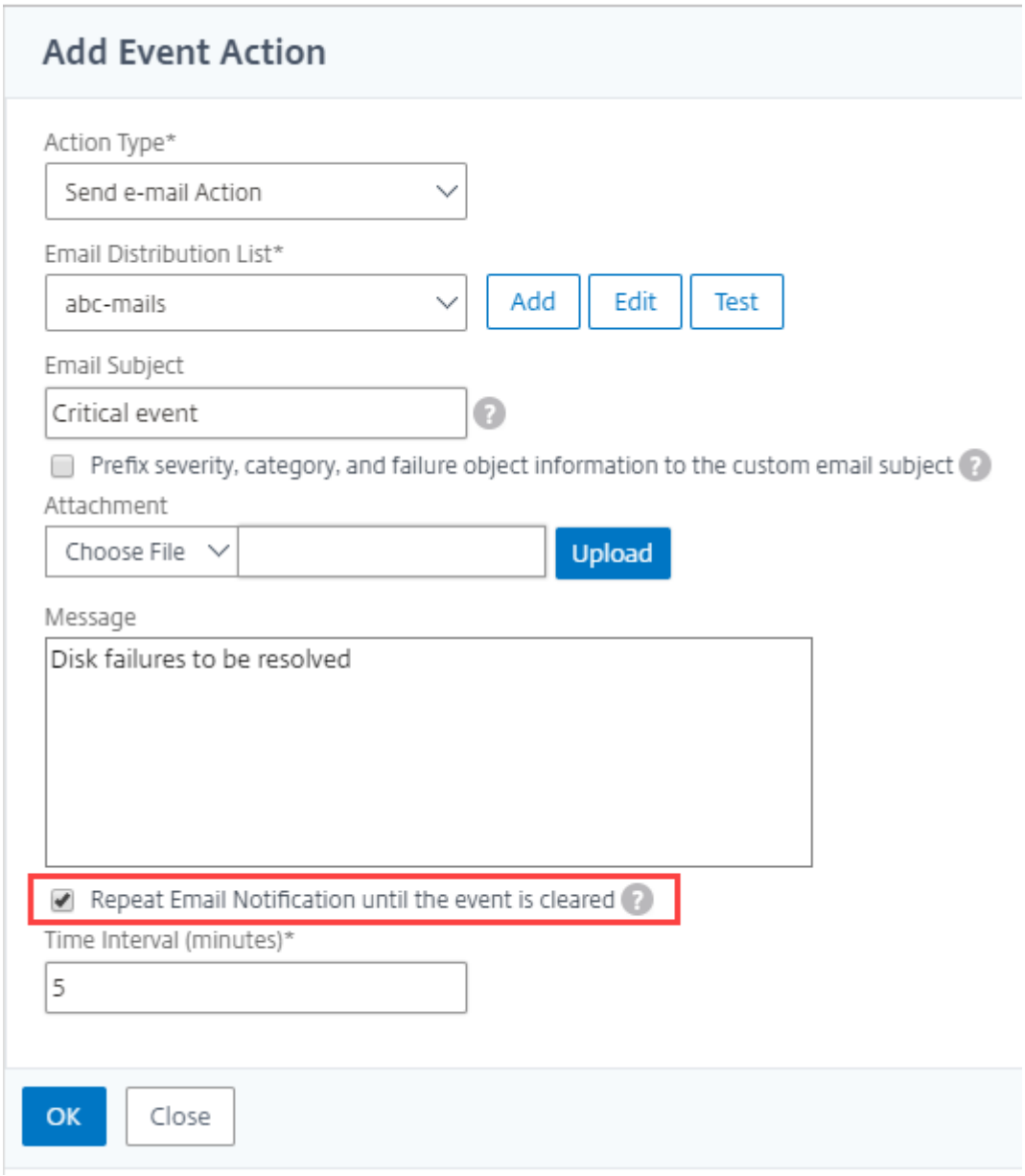
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ereignisse unterdrücken

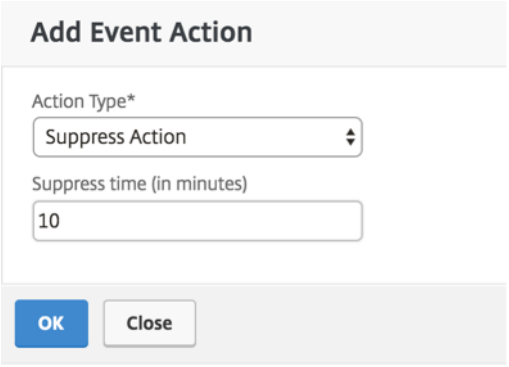
February 5, 2024

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.

So unterdrücken Sie Ereignisse mithilfe von NetScaler ADM:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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** aus der Dropdownliste **Aktionstyp die Option Aktionunterdrücken**, 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

24. Mai 2018

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung einer großen Anzahl von Ereignissen, die in Ihrer Citrix Application Delivery Controller (ADC) -Infrastruktur generiert wurden.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen für die Erstellung von Filtern sind: Schweregrad, NetScaler ADC-Instanzen, Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

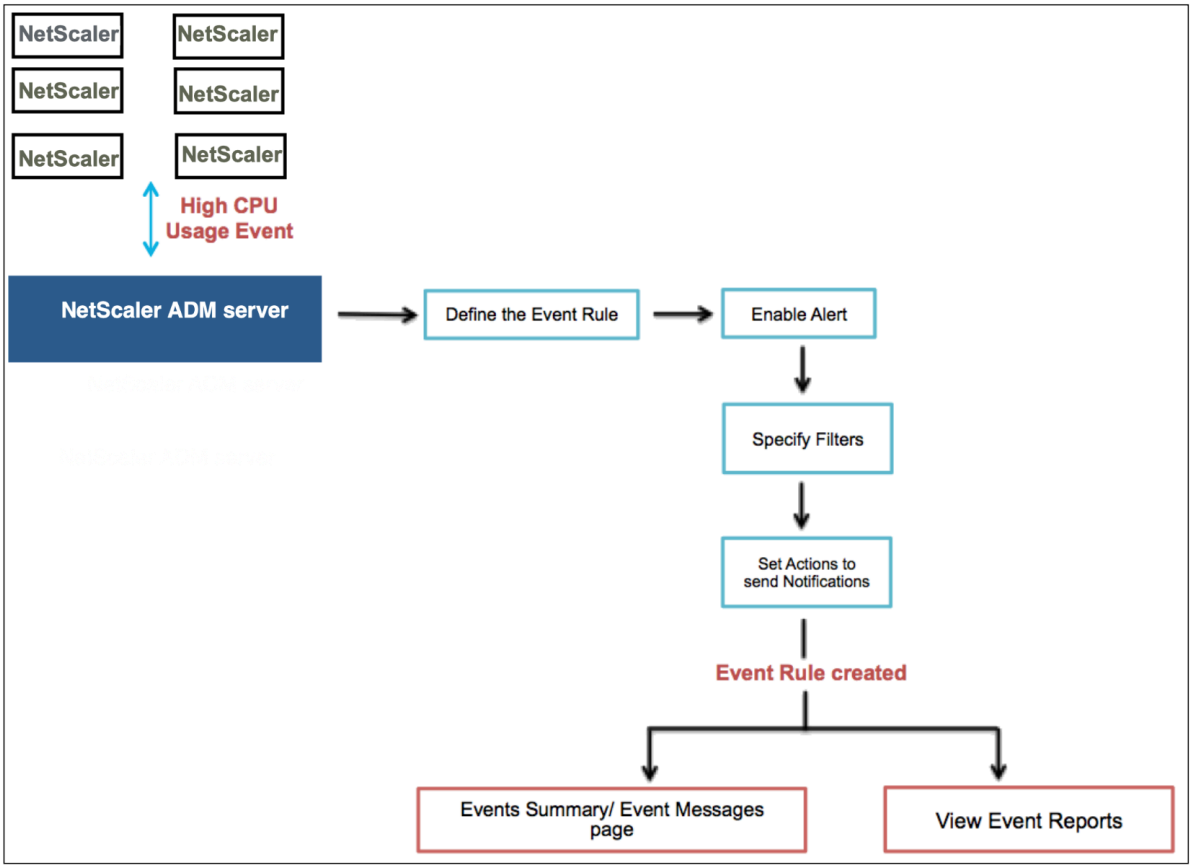
Sie können den Ereignissen die folgenden Aktionen zuweisen:

- **E-Mail-Aktion senden**: Senden Sie eine E-Mail für die Ereignisse, die den Filterkriterien entsprechen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Trap-Aktion senden**: SNMP-Traps an ein externes Trap-Ziel senden oder weiterleiten
- **SMS-Aktion**senden : Senden Sie eine SMS-Nachricht (Short Message Service) für jedes Ereignis, das den Filterkriterien entspricht.
- **Befehlsaktion ausführen**: Führen Sie einen Befehl aus, wenn ein eingehendes Ereignis die konfigurierte Regel erfüllt.
- **Job-Aktion**ausführen: Ausführen eines Jobs ist für Ereignisse vorgesehen, die den von Ihnen angegebenen Filterkriterien entsprechen.
- **Aktion unterdrücken**: Unterdrückt das Löschen eines Ereignisses für einen bestimmten Zeitraum.

Sie können Benachrichtigungen auch in einem bestimmten Intervall erneut senden lassen, bis ein Ereignis gelöscht wird. Und Sie können die E-Mail mit einer bestimmten Betreffzeile, einer Benutzernachricht und/oder 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 der NetScaler ADC-Instanzen führen können. Sie könnten eine Regel zur Überwachung der Instanzen erstellen und eine Aktion angeben, die Ihnen eine E-Mail-Benachrichtigung sendet, wenn ein Ereignis in der Kategorie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

„hohe CPU-Auslastung“eintritt. Sie können die Regel so planen, dass sie zu einer bestimmten Zeit ausgeführt wird, z. B. zwischen 11 und 23 Uhr, sodass 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 angeben
6. Zusätzliche Filter angeben
7. Aktionen angeben, die ausgeführt werden sollen, wenn die Regel ein Ereignis erkennt

Schritt 1 - Definieren einer Ereignisregel

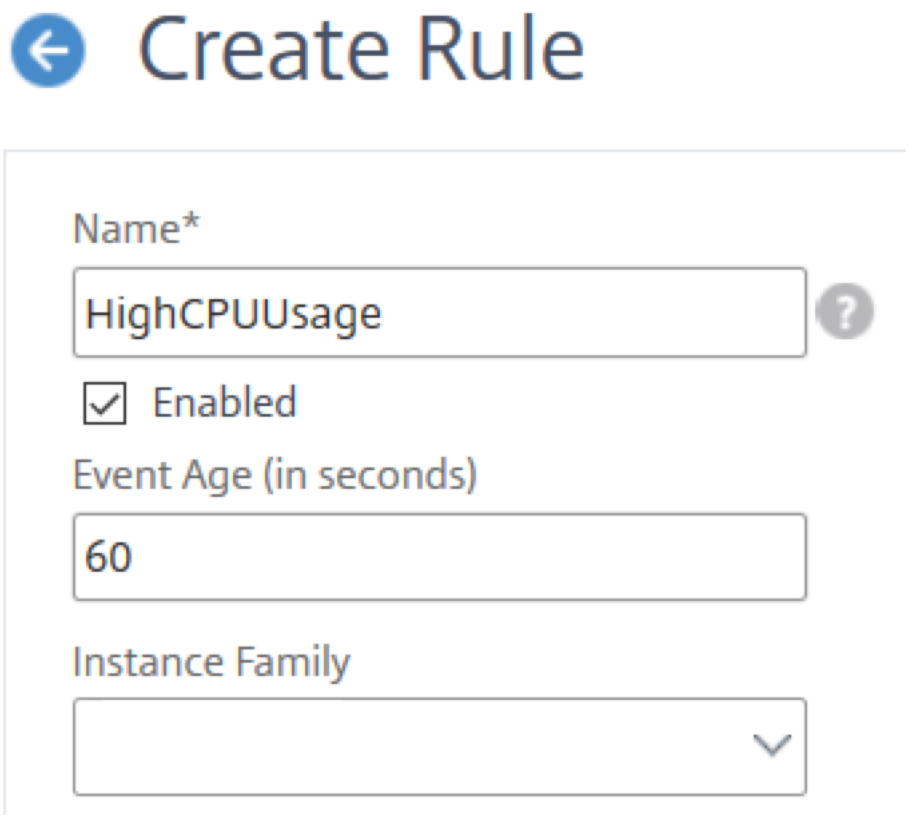
Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Regeln**, und klicken Sie auf **Hinzufügen**. Wenn Sie Ihre Regel aktivieren möchten, **aktivieren Sie das Kontrollkästchen Regel aktivieren**.

Sie können die Option **Event Age** festlegen, um das Zeitintervall (in Sekunden) anzugeben, nach dem Citrix Application Delivery Management (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 Citrix ADC-Instanz für einen Zeitraum von 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 Citrix ADC-Instanz 60 Sekunden oder länger ein Ereignis mit „hoher CPU-Auslastung“aufweist, eine E-Mail-Benachrichtigung mit Details zum Ereignis erhalten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

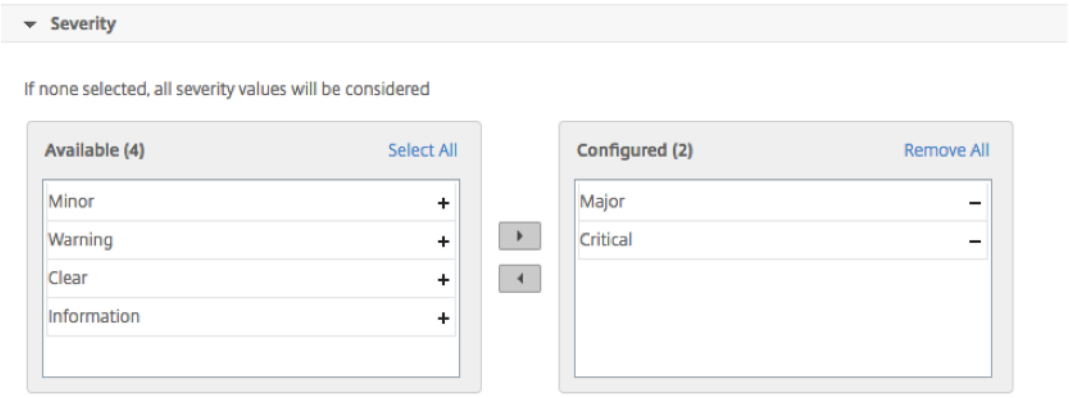


Sie können Ereignisregeln auch nach **Gerätefamilie** filtern, um die Citrix ADC Instanz zu verfolgen, von der Citrix ADM ein Ereignis empfängt.

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.



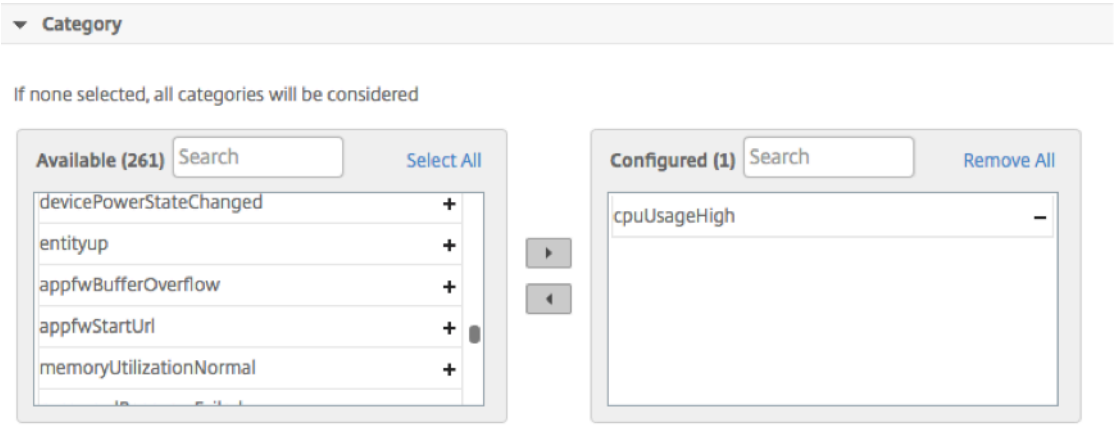
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Sie können den Schweregrad für allgemeine und unternehmensspezifische 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 —Angabe der Event-Kategorie

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**.

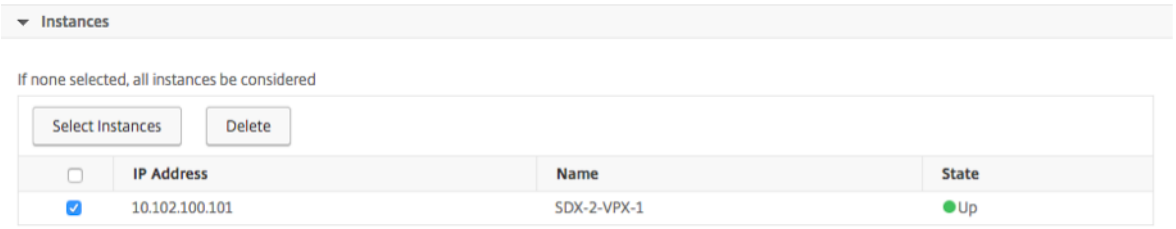
Im obigen Beispiel müssen Sie “cpuUsageHigh”als Ereigniskategorie aus der angezeigten Tabelle auswählen.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

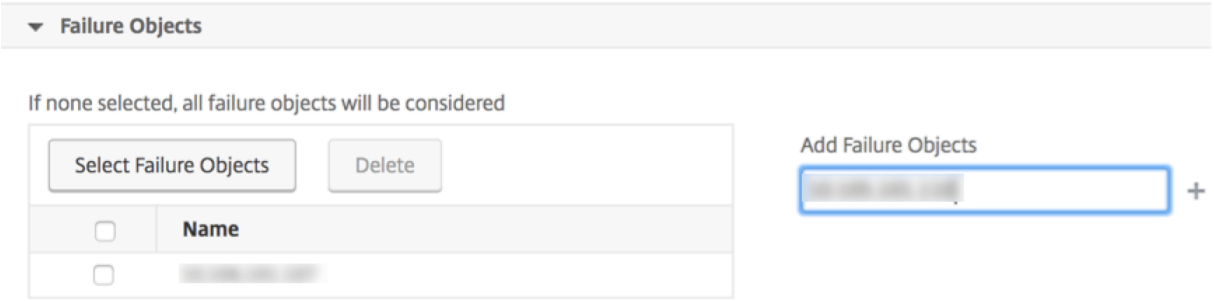


Schritt 5 - Auswählen von Fehlerobjekten

Sie können entweder ein Fehlerobjekt aus der Dropdownliste auswählen oder ein Fehlerobjekt hinzufügen, für das ein Ereignis generiert wurde. Fehlerobjekte sind Entitätsinstanzen oder Leistungsindikatoren, für die ein Ereignis generiert wurde.

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. Wenn ein Benutzer beispielsweise Probleme mit der Anmeldung hat, ist das Fehlerobjekt hier der Benutzername oder das Kennwort, z. B. „nsroot“.

Diese Liste kann Leistungsindikatornamen für alle mit Schwellenwert verbundenen Ereignisse, Entitätsnamen für alle Entity-bezogenen Ereignisse, Zertifikatnamen für zertifikatbezogene Ereignisse usw. enthalten.

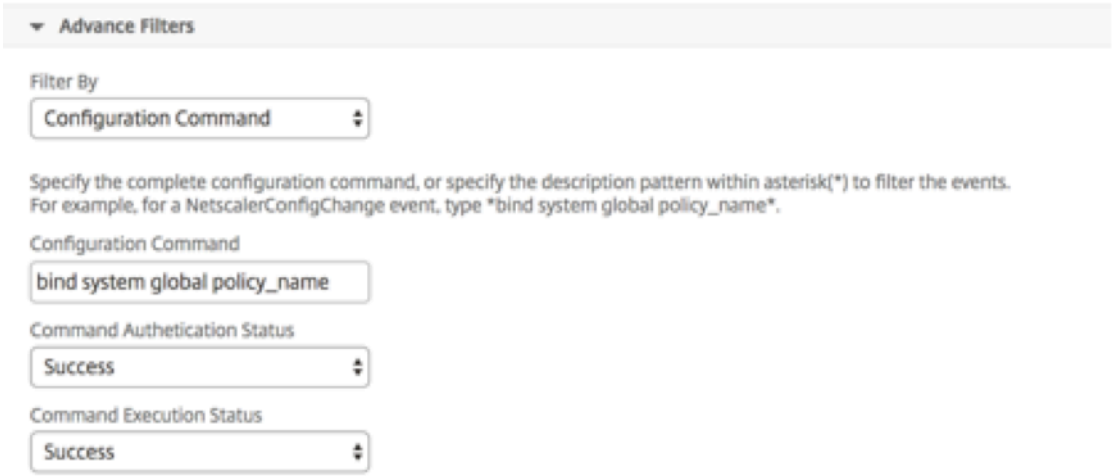


Schritt 6 - Zusätzliche Filter angeben

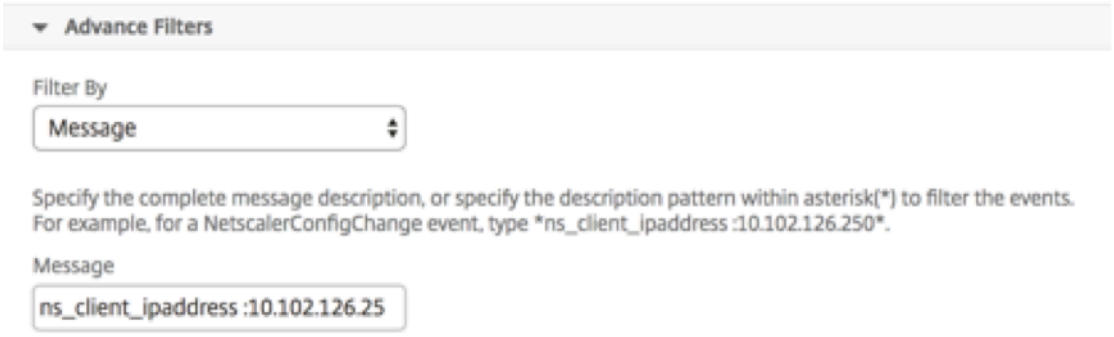
Sie können eine Ereignisregel weiter filtern nach:

- **Konfigurationsbefehle** - Sie können den vollständigen Konfigurationsbefehl angeben oder das Beschreibungsmuster innerhalb eines Sternchens (*) angeben, um die Ereignisse zu filtern. Zusätzlich zum Befehl können Sie die Ereignisregel weiter nach dem Authentifizierungsstatus und/oder dem Ausführungsstatus des Befehls filtern. Geben Sie beispielsweisefür ein NetScalerConfigChange-Ereignis *bind system global policy_name* ein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Nachrichten** - Sie können die vollständige Nachrichtenbeschreibung angeben oder das Beschreibungsmuster innerhalb von Sternchen (*) angeben, um die Ereignisse zu filtern.Geben Sie beispielsweise
  für ein NetScalerConfigChange-Ereignis *ns_client_ipaddress:10.102.126.250* 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 Aktion
- Trap-Aktion senden
- Aktion „SMS senden“
- Befehls-Aktion ausführen
- Auftragsaktion ausführen
- Aktion unterdrücken

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

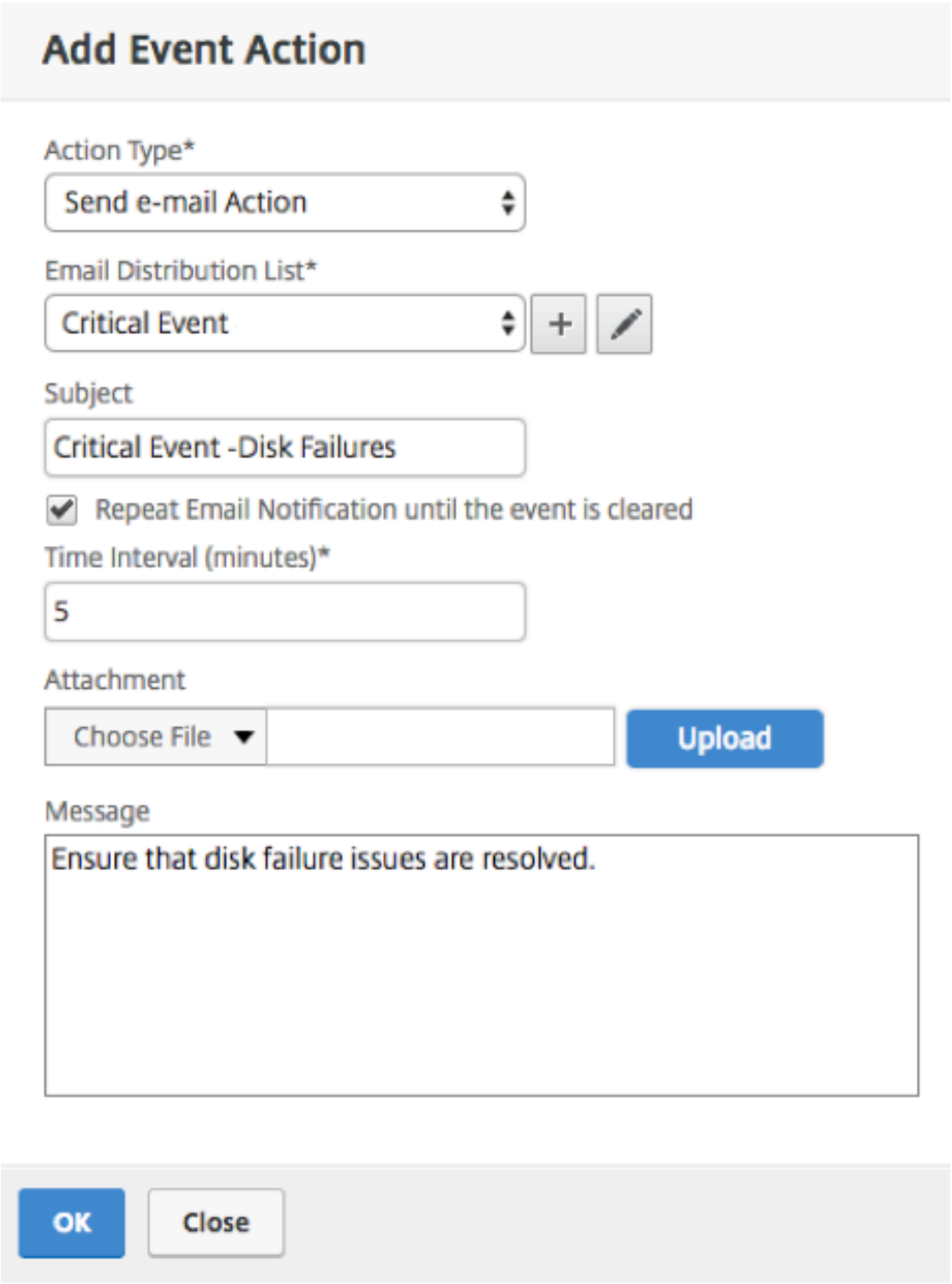
So legen Sie die E-Mail-Ereignisregelaktion fest:

Wenn Sie den Aktionstyp E-Mail-Aktion 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.

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.

Mit dieser Option können Sie 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 gelöscht ist** , aktivieren, um wiederholte E-Mail-Benachrichtigungen für Ereignisregeln zu senden, die den von Ihnen ausgewählten Kriterien entsprechen. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



So legen Sie die Trap-Event-Regelaktion fest:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-Ziel- und Trap-Profildetails) werden Trap-Nachrichten an bestimmte Trap-Listener gesendet, wenn Ereignisse die definierten Filterkriterien erfüllen.

So legen Sie die Aktion für SMS-Ereignisregeln fest:

Wenn Sie den Ereignistyp **SMS-Aktion senden** wählen, wird für jedes Ereignis, das den Filterkriterien entspricht, eine SMS-Nachricht (**Short Message Service**) angezeigt. Sie müssen entweder eine SMS-Verteilerliste erstellen, indem Sie den SMS-Server oder die SMS-Profildetails angeben, oder Sie können eine SMS-Verteilerliste auswählen, die Sie zuvor erstellt haben.

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. Wenn beispielsweise bei einer Konfigurationsänderung auf einer verwalteten Instanz ein Ereignis mit dem Schweregrad „Kritisch“ausgelöst wird, können Sie ein Befehlsskript ausführen.

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.

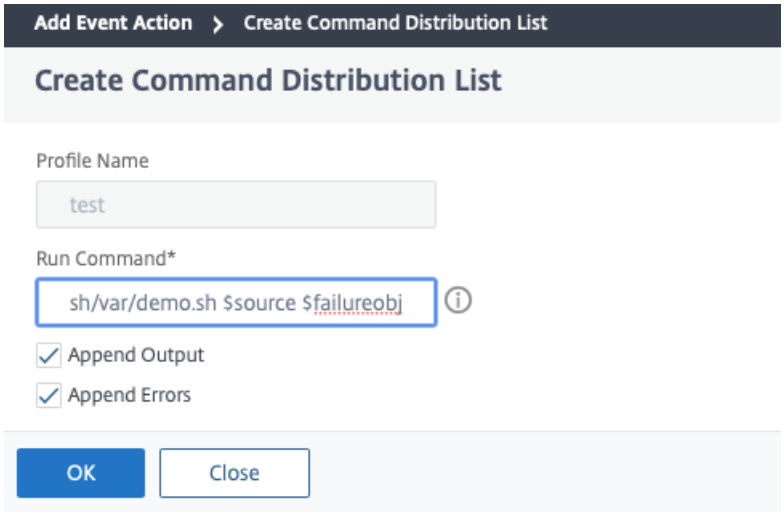
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

$ 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.

So konfigurieren Sie die Ereignisaktion „Befehlsaktion ausführen“auf Citrix ADM:

1. ****Klicken Sie unter Ereignisregelaktionen auf **Aktion hinzufügen** und wählen Sie im Dropdownmenü Aktionstyp die Option Befehlsaktion ausführen** aus.
2. **Geben** Sie auf der Seite „Befehlsverteilerliste erstellen “einen Profilnamen und den auszuführenden Befehl an. Dieser Befehl wird ausgeführt, wenn die Ereignisse die definierten Filterkriterien erfüllen.



> **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

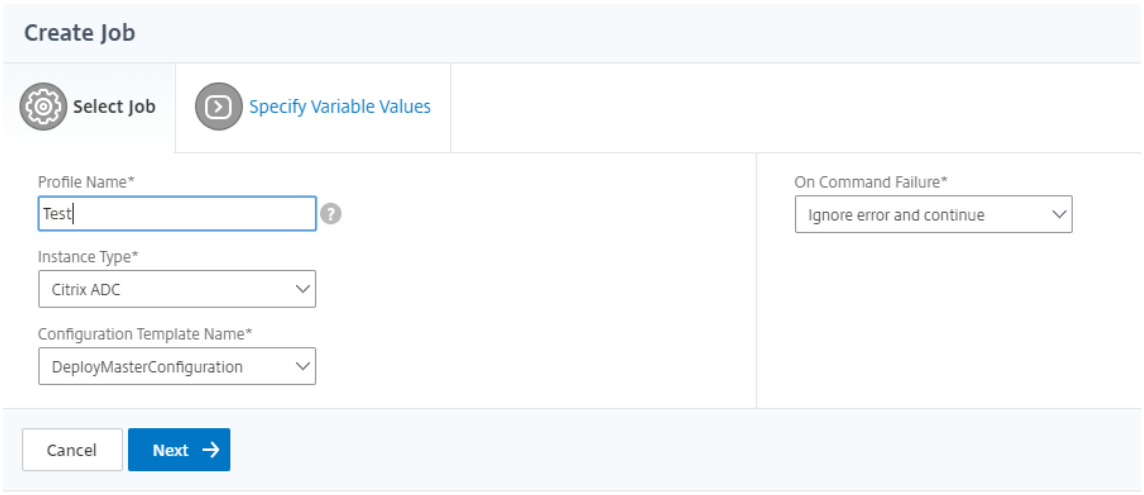
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> während der Ausführung des Befehlsskripts generiert wurden.

So legen Sie die Aktion „Job ausführen“fest:

Durch das Erstellen eines Profils mit Konfigurationsaufträgen wird ein Job als integrierter Job oder als benutzerdefinierter Job für Citrix ADC-, Citrix SDX- und Citrix SD-WAN WO-Instanzen für Ereignisse und Alarme ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen.

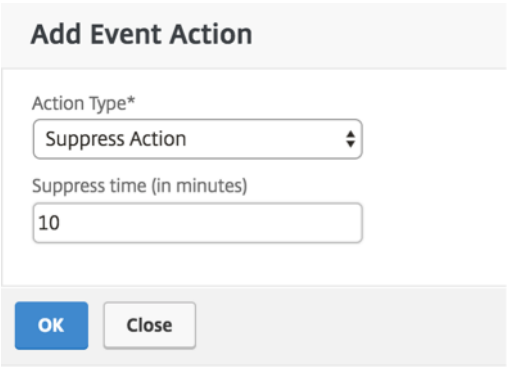
1. ****Klicken Sie unter Ereignisregelaktionen auf **Aktion hinzufügen** und wählen Sie im Menü Aktionstyp die Option Jobaktion ausführen** aus.
2. Erstellen Sie ein Profil mit einem Job, den Sie ausführen möchten, wenn die Ereignisse die definierten Filterkriterien erfüllen.
3. Geben Sie beim Erstellen eines Auftrags einen Profilnamen, den Instanztyp, die Konfigurationsvorlage und die Aktion an, die Sie ausführen möchten, wenn die Befehle für den Auftrag fehlschlagen.
4. Geben Sie anhand des ausgewählten Instanztyps und der gewählten Konfigurationsvorlage die Variablenwerte an, und klicken Sie auf **Fertig stellen**, um den Job zu erstellen.



So legen Sie die Aktion „Unterdrücken“fest:

Wenn Sie die Ereignisaktion **Aktion unterdrücken** auswählen, können Sie einen Zeitraum in Minuten konfigurieren, für den ein Ereignis unterdrückt oder gelöscht wird. Sie können das Ereignis mindestens 1 Minute unterdrücken.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ihre Ereignisregel wird jetzt mit geeigneten Filtern und gut definierten Ereignisregelaktionen erstellt.

Gemeldeten Schweregrad von Ereignissen auf NetScaler ADC-Instanzen ändern

February 5, 2024

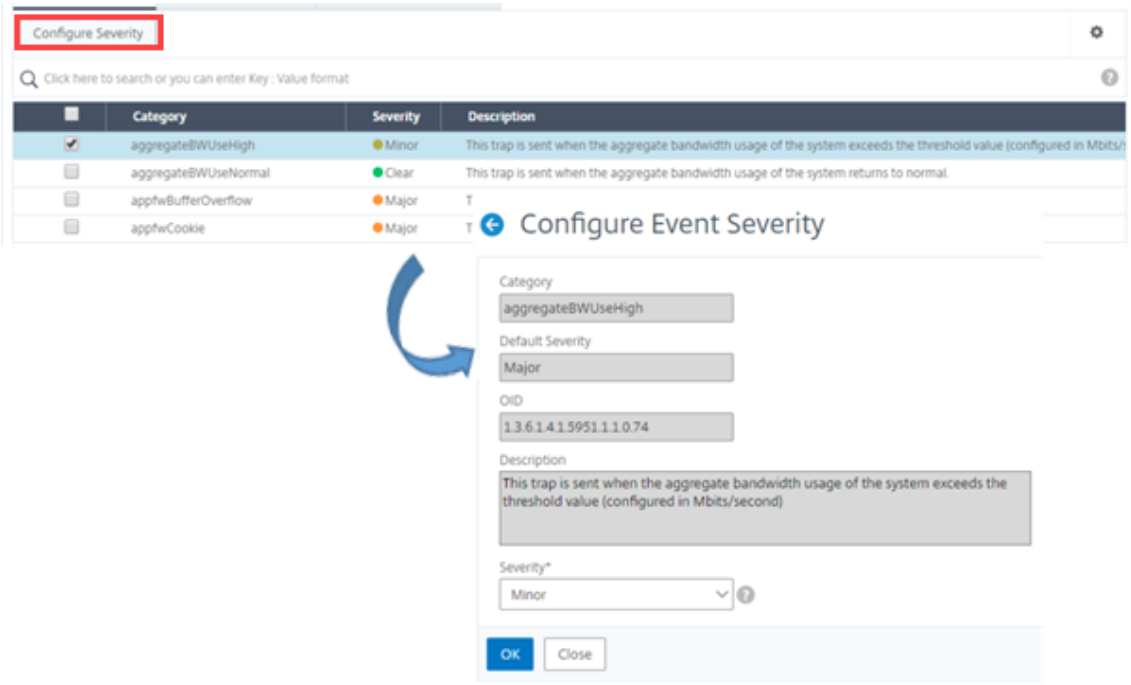
Sie können die Berichterstattung über Ereignisse verwalten, die auf all Ihren Geräten generiert wurden, sodass Sie Ereignisdetails zu einem bestimmten Ereignis in einer bestimmten Instanz einsehen und Berichte auf der Grundlage des Schweregrads des Ereignisses einsehen können. Sie können Ereignisregeln 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** > **Ereigniseinstellungen**.
2. Klicken Sie auf die Registerkarte für den Instanztyp von Citrix Application Delivery Controller (ADC), den Sie ändern möchten. Wählen Sie dann die Kategorie aus der Liste aus und klicken Sie auf **Schweregrad konfigurieren**.
3. Wählen **Sie unter Konfigurieren des Ereignisschweregrads**den Schweregrad aus der Drop-downliste aus.
4. Klicken Sie auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



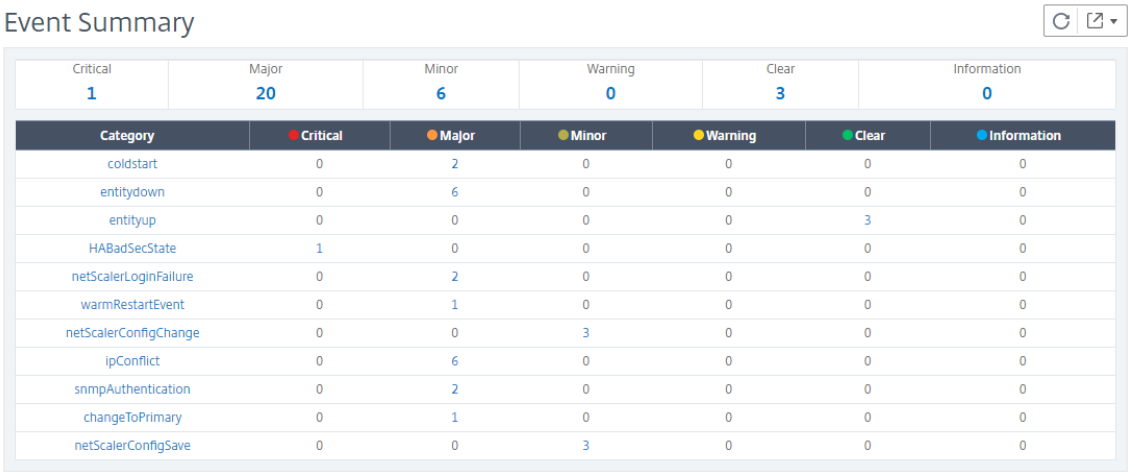
Zusammenfassung der Ereignisse anzeigen

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:

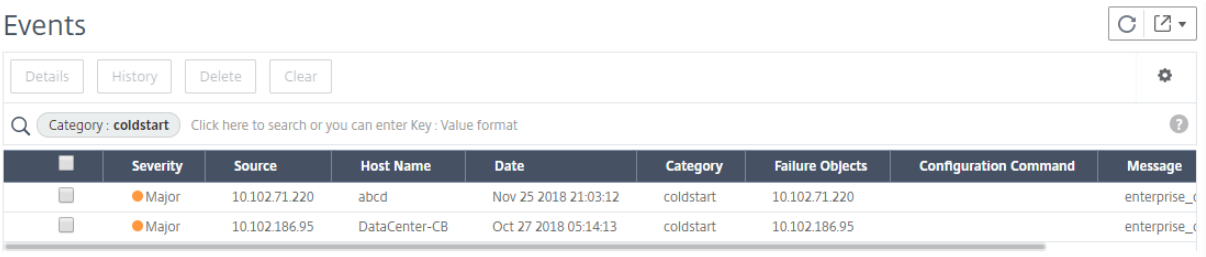
- **Zusammenfassung aller Ereignisse, die NetScaler ADM erhalten hat**. Die Ereignisse sind nach Kategorien sortiert, und die verschiedenen Schweregrade werden in verschiedenen Spalten angezeigt: Kritisch, schwerwiegend, geringfügig, Warnung, Klar und Information. Ein kritisches Ereignis tritt beispielsweise 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 erklärt wird, warum die Instanz ausgefallen ist, die Zeit, für die sie ausgefallen war usw. Das Ereignis wird dann auf der Seite “Ereignisübersicht”aufgezeichnet, auf der Sie eine Zusammenfassung anzeigen und auf die Details des Ereignisses zugreifen können.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **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 eine 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Durch Klicken auf das Diagramm gelangen Sie zur Seite "**Schweregrad basierte Ereignisse** ", auf der Sie alle Details darüber sehen können, wann ein kritisches Ereignis für die ausgewählte Dauer aufgetreten ist: Instanzquelle, Datum, Kategorie und Nachrichtenbenachrichtigung, die gesendet wurde, wenn das kritische Ereignis aufgetreten ist.

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 die Instanz auch auswählen und das Dashboard der jeweiligen Citrix Instanz für weitere Details anzeigen.

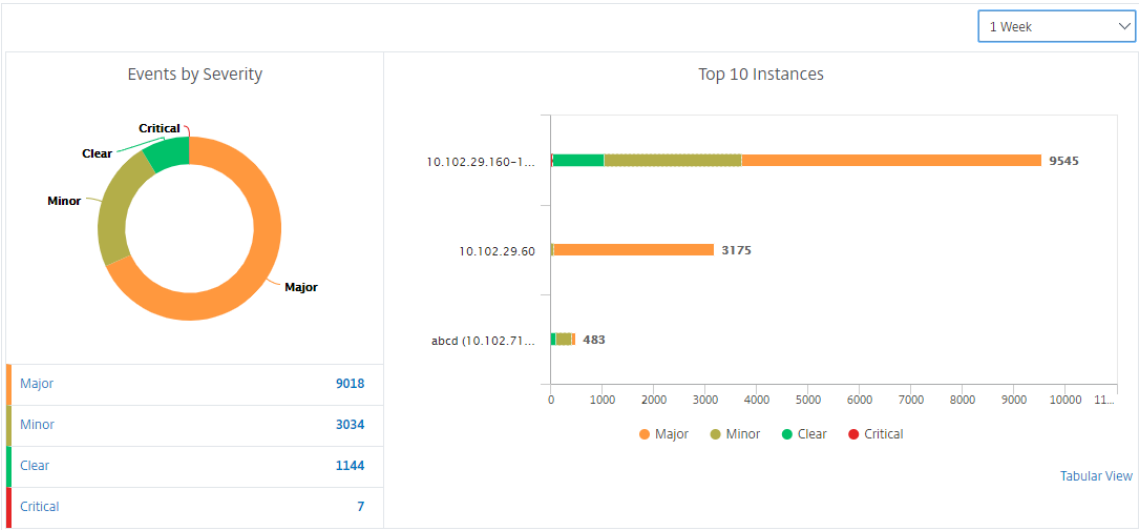
So wählen Sie bestimmte Ereignisse nach Schweregrad in NetScaler ADM aus:

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

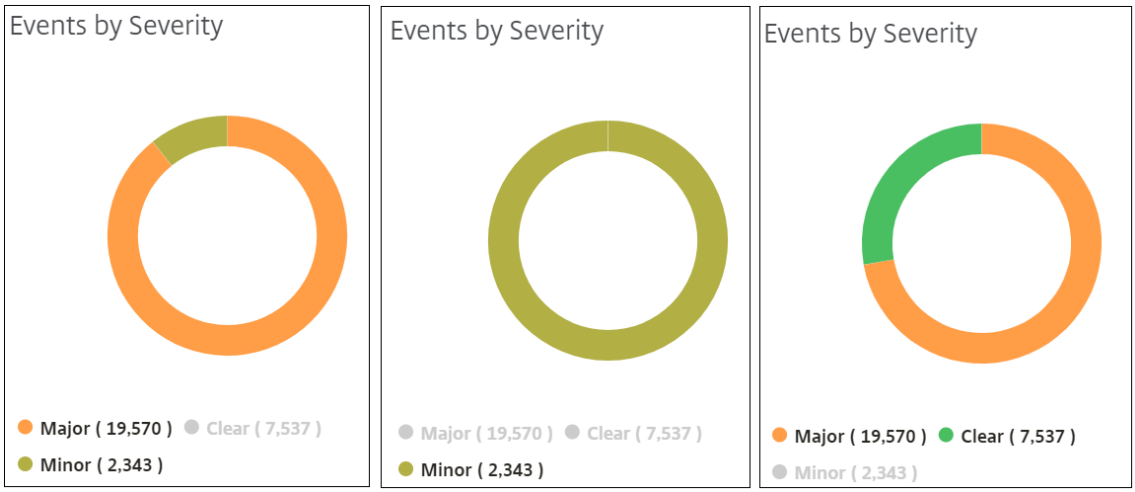


4. Das Donutdiagramm **Ereignisse nach Schweregrad**zeigt eine visuelle Darstellung aller Ereignisse nach ihrem Schweregrad an. Verschiedene Arten von Ereignissen werden als unterschiedliche farbige Abschnitte dargestellt, und die Länge jedes Abschnitts entspricht der Gesamtzahl der Ereignisse dieser Art von Schweregrad.
5. Sie können auf jeden Abschnitt des Ringdiagramms klicken, um die entsprechende Seite mit schweregradbasierten **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 einfacher anzuzeigen und zu überwachen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.”

Syslog-Nachrichten exportieren

February 5, 2024

Sie können nun Syslog-Nachrichten anzeigen, ohne sich bei NetScaler Application Delivery Management (ADM) anzumelden, indem Sie einen Export aller auf dem Server empfangenen Syslog-Nachrichten planen. Sie können Syslog-Nachrichten, die auf Ihren Citrix Application Delivery Controller (ADC) -Instanzen generiert werden, in PDF-, CSV-, PNG- und JPEG-Formaten exportieren. Sie können den Export dieser Berichte an bestimmte E-Mail-Adressen in verschiedenen Intervallen planen.

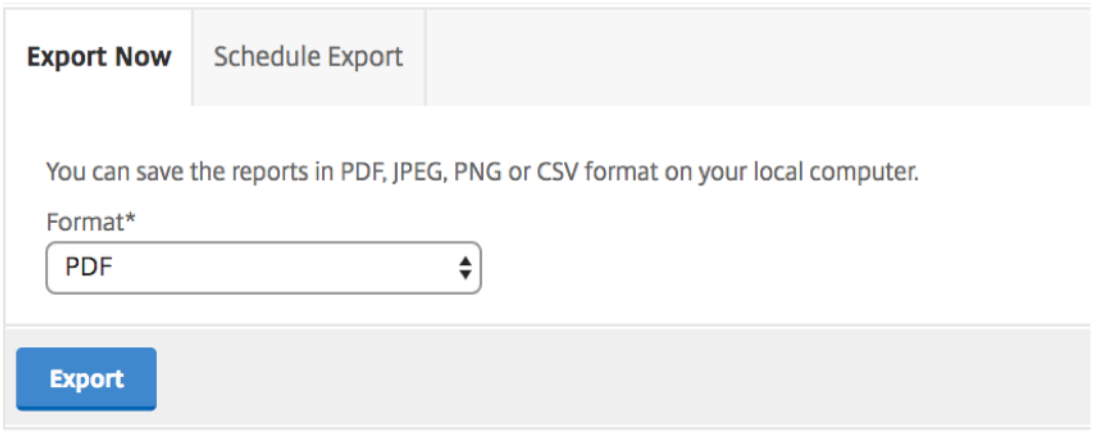
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Weitere Informationen zur Konfiguration eines Syslog-Servers, zum Syslog-Daten- und Zeitformat sowie zum Anzeigen von Syslog-Meldungen auf Citrix ADM finden Sie unter Auditinformationenanzeigen.

Um Syslog-Nachrichten anzuzeigen, navigieren Sie zu**Netzwerke**>**Ereignisse**>**Syslog-Nachrichten**. Im rechten Bereich unter Syslog **Viewer** können Sie die Syslog-Meldungen, die Sie anzeigen möchten, nach Modul, Ereignistyp, Schweregrad und Quell-IP-Adresse filtern. Klicken Sie auf**Übernehmen**, um die Syslog-Nachrichten zu generieren.

So exportieren Sie einen Syslog-Meldungsbericht mithilfe von NetScaler ADM:

1. Navigieren Sie zu**Netzwerke**> **Ereignisse** > **Syslog-Nachrichten**.
2. Klicken Sie im rechten Bereich auf die Schaltfläche Exportieren in der oberen rechten Ecke der Seite Syslog-Nachrichten.
3. Wählen Sie auf der Registerkarte **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

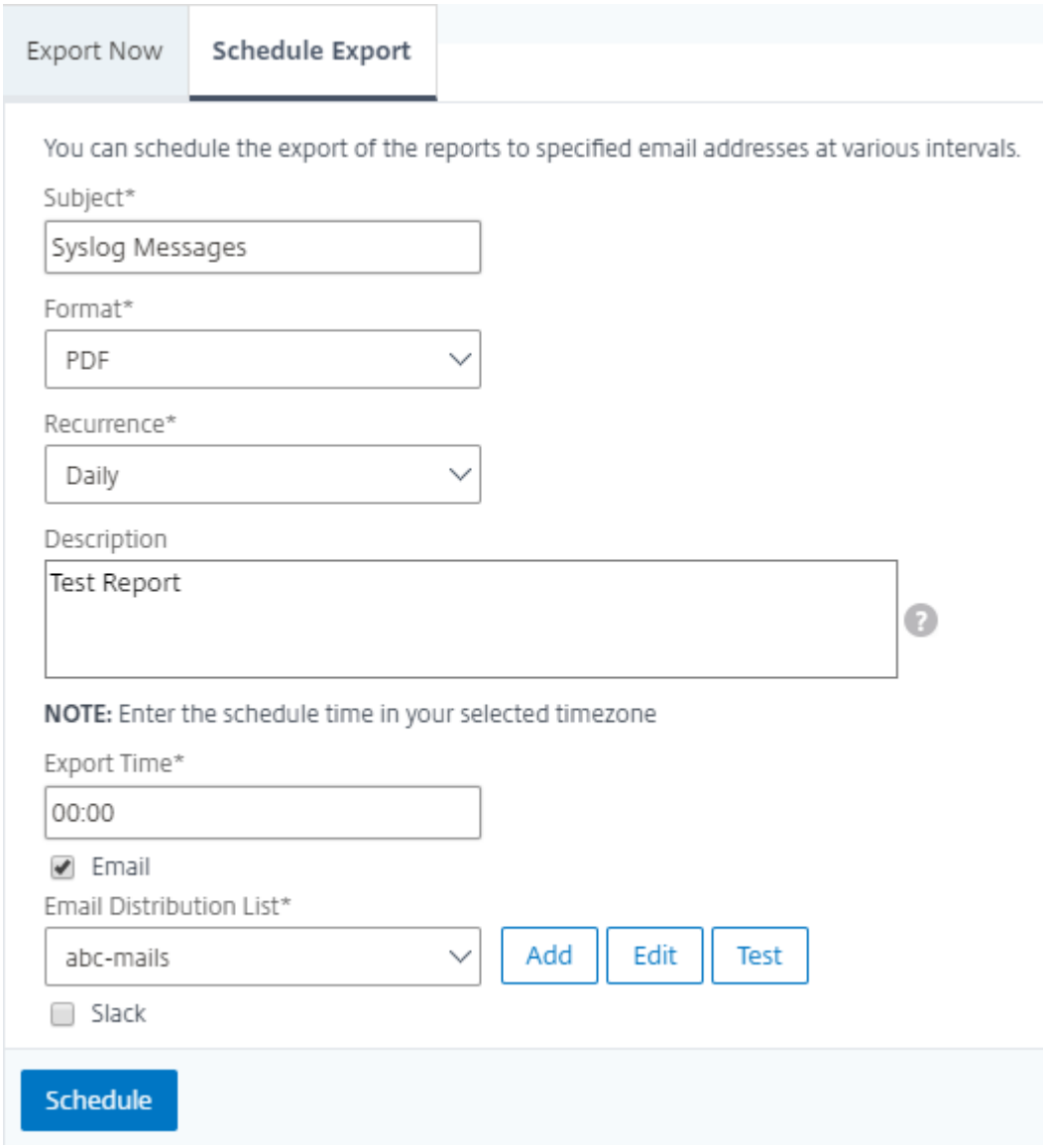


So planen Sie den Export von Syslog-Meldungsberichten mithilfe von NetScaler ADM:

1. Navigieren Sie zu **Netzwerke** > **Ereignisse** > **Syslog-Nachrichten**.
2. Klicken Sie auf der Seite **Syslog-Nachrichten** im rechten Bereich auf **Exportieren**.
3. Legen Sie auf der Registerkarte **Bericht planen** die folgenden Parameter fest:
    - **Beschreibung**: Meldung, die den Grund für den Export des Berichts beschreibt.
    - **Format**: Format, in dem der Bericht exportiert werden soll.
    - **Wiederholung**: Intervall, in dem der Bericht exportiert werden soll.
    - **Exportzeit**: Der Zeitpunkt, zu dem die Auswertung exportiert werden soll. Geben Sie die Uhrzeit im 24-Stunden-Format für Ihre lokale Zeitzone ein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **E-Mail-Verteilerliste**: Liste der Empfänger, die den Bericht per E-Mail erhalten sollen. Wählen Sie eine E-Mail-Verteilerliste aus der bereitgestellten Dropdownliste aus. Eine E-Mail wird ausgelöst, wenn der Bericht generiert wird und die geplanten Zeitkriterien erfüllt. Wenn Sie eine neue E-Mail-Verteilerliste erstellen möchten, klicken Sie auf **+** und geben Sie die Mailserver- und E-Mail-Profildetails an.



Konfigurieren der Einstellungen zum Ausschneiden von Ereignissen mithilfe von NetScaler ADM

Um die Anzahl der Ereignisnachrichtungsdaten zu begrenzen, die in der Datenbank des NetScaler ADM -Servers gespeichert werden, können Sie angeben, in welchem Intervall NetScaler ADM Netzwerkberichtungsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle beibehalten soll.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Standardmäßig werden diese Daten alle 24 Stunden (um 00.00 Uhr) bereinigt.

Navigieren Sie zu **System** > **Systemadministration**. ****Klicken Sie unter Instanzeinstellungen auf ****Events Prune Settings** . Geben Sie das Zeitintervall in Tagen ein, für das Sie Daten auf dem Citrix ADM Server speichern möchten, und klicken Sie auf **OK** .

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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

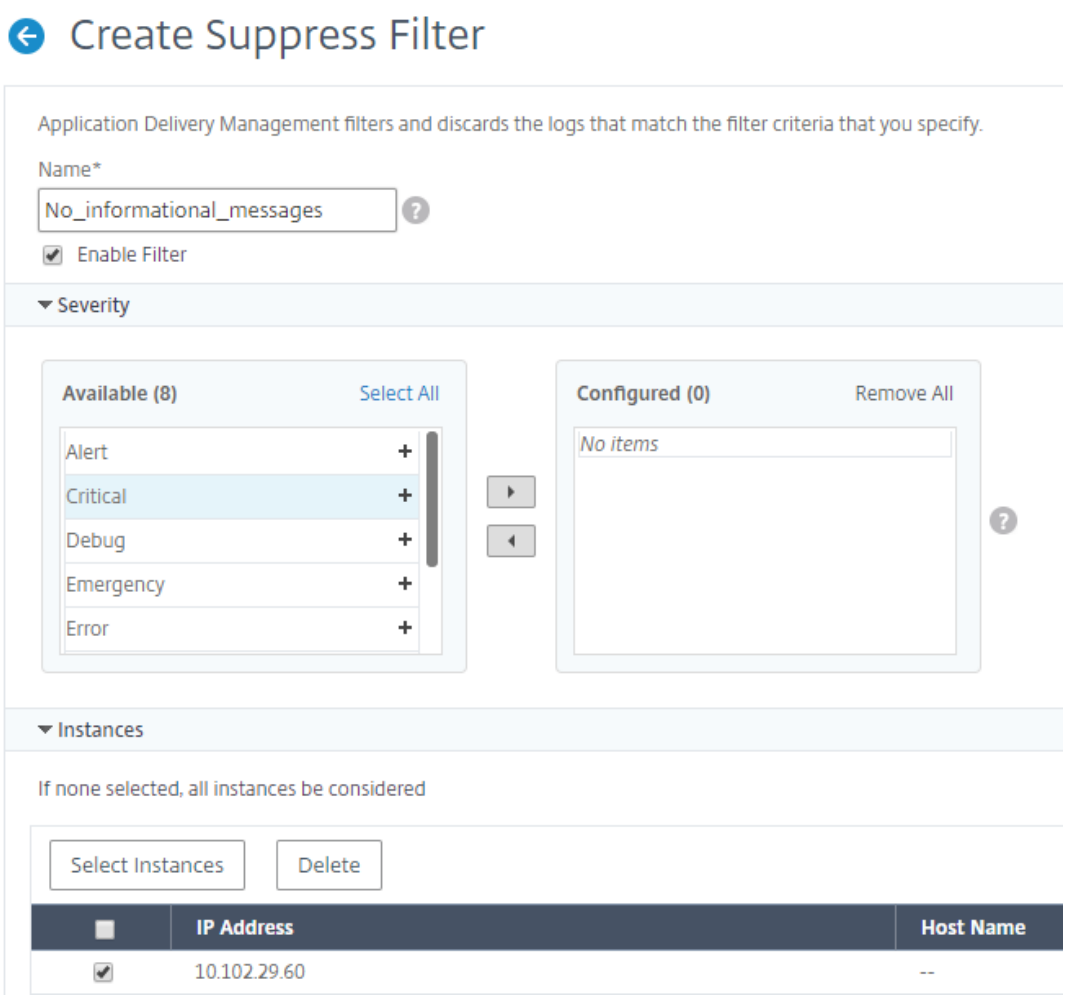
   a) **Name** - geben Sie einen Namen für den Filter ein.

   > **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.

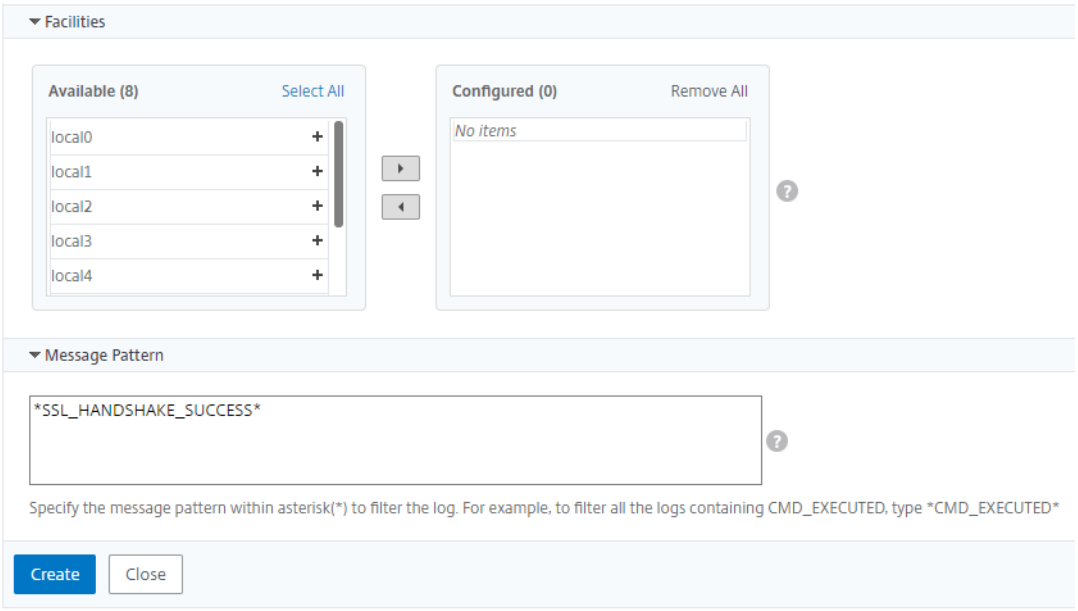
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

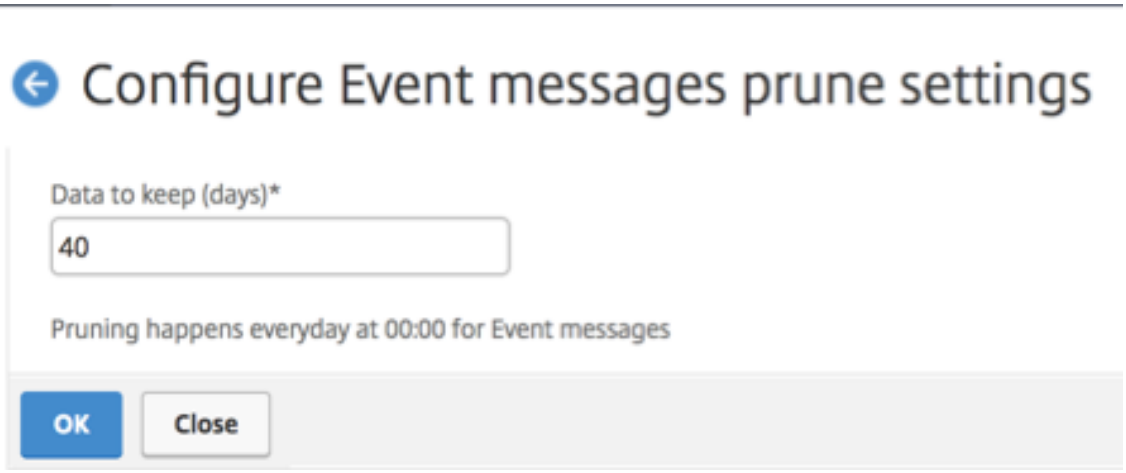
> **Hinweis**
>
> Der Wert, den Sie angeben können, darf 40 Tage nicht überschreiten oder weniger als 1 Tag be-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> tragen.

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-Dashboard

February 5, 2024

NetScaler Application Delivery Management (ADM) optimiert jetzt jeden Aspekt der Zertifikatsverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht verwendete oder bald ablaufende Zertifikate im Auge behalten. Um mit der Nutzung des SSL-Dashboards von Citrix ADM und seiner Funktionen zu beginnen, müssen Sie verstehen, was ein SSL-Zertifikat ist und wie Sie Citrix ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Ein SSL-Zertifikat (Secure Socket Layer), das Teil einer SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der Citrix Application Delivery Controller (ADC) -Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung des asymmetrischen Schlüssels (oder des öffentlichen Schlüssels) abzuschließen.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Von einer autorisierten Zertifizierungsstelle (CA)
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der Citrix ADC-Appliance

NetScaler ADM bietet eine zentrale Ansicht der in allen verwalteten NetScaler ADC-Instanzen installierten SSL-Zertifikate. Im SSL-Dashboard können Sie Diagramme anzeigen, mit denen Sie Zertifikatsaussteller, wichtige Stärken, Signaturalgorithmen, abgelaufene oder nicht verwendete Zertifikate usw. nachverfolgen können. Sie können auch die Verteilung der SSL-Protokolle sehen, die auf Ihren virtuellen Servern ausgeführt werden, und die Schlüssel, die auf ihnen aktiviert sind.

Sie können auch Benachrichtigungen einrichten, um Sie darüber zu informieren, wann Zertifikate ablaufen werden, und Informationen darüber enthalten, welche NetScaler ADC-Instanzen diese Zertifikate verwenden.

Sie können die Zertifikate einer NetScaler ADC Instanz mit einem Zertifizierungsstellenzertifikat verknüpfen. Stellen Sie jedoch sicher, dass die Zertifikate, die Sie mit demselben CA-Zertifikat verknüpfen, dieselbe Quelle und denselben Aussteller haben. Nachdem Sie die Zertifikate mit einem Zertifizierungsstellenzertifikat verknüpft haben, können Sie die Verknüpfung aufheben.

Verwenden des SSL-Dashboards

February 5, 2024

Sie können das SSL-Zertifikats-Dashboard in Citrix Application Delivery Management (ADM) verwenden, um Grafiken anzuzeigen, die Ihnen helfen, den Überblick über Zertifikatsaussteller, wichtige Stärken und Signaturalgorithmen zu behalten. Das SSL-Zertifikat-Dashboard zeigt außerdem Diagramme an, die Folgendes angeben:

- Anzahl der Tage, nach denen Zertifikate ablaufen
- Anzahl verwendeter und nicht verwendeter Zertifikate
- Anzahl selbstsignierter und von einer Zertifizierungsstelle signierter Zertifikate
- Anzahl der Emittenten
- Signatur-Algorithmen
- SSL-Protokolle
- Top 10 Instanzen nach Anzahl der verwendeten Zertifikate

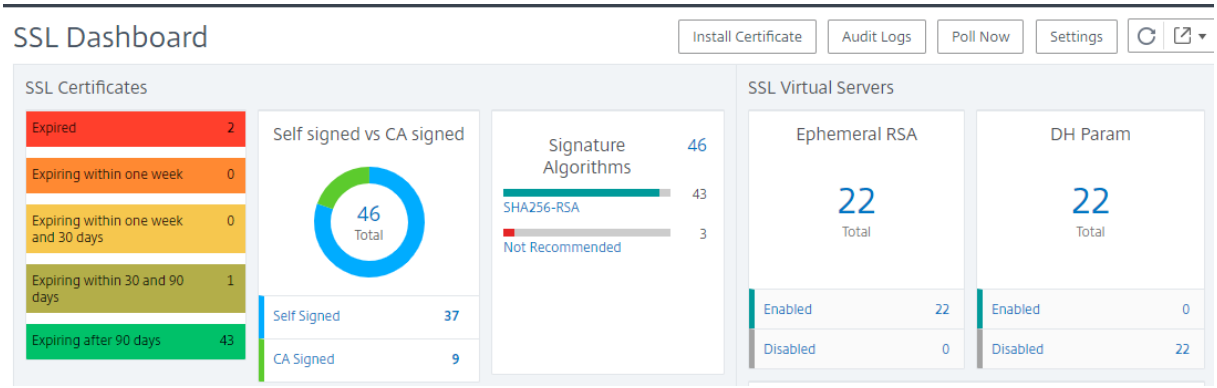
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

So überwachen Sie SSL-Zertifikate

Sie können das SSL-Dashboard in NetScaler ADM verwenden, um Ihre Zertifikate zu überwachen, wenn Ihr Unternehmen über eine SSL-Richtlinie verfügt, in der Sie bestimmte SSL-Zertifikatanforderungen definiert haben, z. B. alle Zertifikate müssen Mindestschlüsselstärken von 2048 Bit aufweisen und eine vertrauenswürdige Zertifizierungsstelle autorisieren muss.

In einem anderen Beispiel haben Sie möglicherweise ein neues Zertifikat hochgeladen, aber vergessen, es an einen virtuellen Server zu binden. Das SSL-Dashboard hebt die verwendeten oder nicht verwendeten SSL-Zertifikate hervor. Im Abschnitt Verwendung sehen Sie die Anzahl der installierten Zertifikate und die Anzahl der verwendeten Zertifikate. Sie können weiter auf das Diagramm klicken, um den Namen des Zertifikats, die Instanz, auf der es verwendet wird, seine Gültigkeit, seinen Signaturalgorithmus usw. zu sehen.

Um SSL-Zertifikate in Citrix ADM zu überwachen, navigieren Sie zu**Netzwerke**> **SSL-Dashboard**.

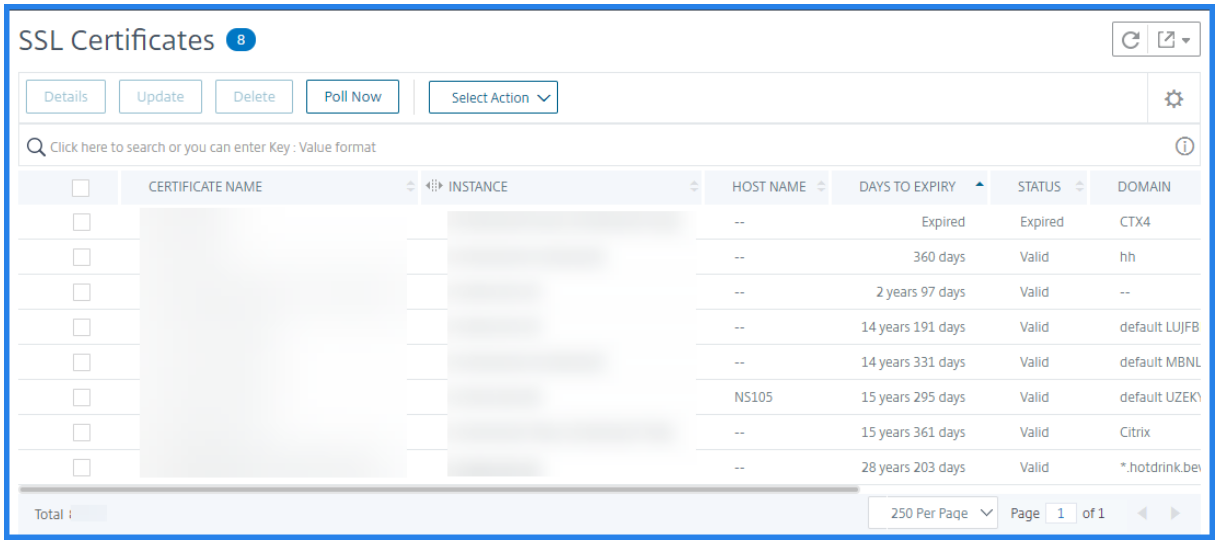


Mit Citrix ADM können Sie SSL-Zertifikate abfragen und alle SSL-Zertifikate der Instanzen sofort Citrix ADM hinzufügen. ****Navigieren Sie dazu zu Netzwerke >** SSL-Dashboard** und klicken Sie auf **Jetzt** abfragen . Die Seite **Jetzt** abfragen wird geöffnet und bietet die Option, alle Citrix Application Delivery Controller (ADC) -Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

Sie können das Citrix ADM SSL-Dashboard verwenden, um die Details von Citrix ADC SSL-Zertifikaten, virtuellen SSL-Servern und SSL-Protokollen anzuzeigen oder zu überwachen. Gesamtzahl sind Hyperlinks, auf die Sie klicken können, um Details zu SSL-Zertifikaten, virtuellen SSL-Servern oder SSL-Protokollen anzuzeigen.

Zum Beispiel, wenn ein Benutzer auf die Zahl 52 unter Selbstsigniert vs. Zertifizierungsstelle signiert" in der obigen Abbildung wird ein neues Fenster mit Details zu den 52 SSL-Zertifikaten auf den NetScaler ADC-Instanzen angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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. Die unterstützten Protokolle sind SSLv2, SSLv3, TLS1.0, TLS1.1 und TLS1.2. Die auf virtuellen Servern verwendeten SSL-Protokolle werden in einem Balkendiagrammformat angezeigt. Wenn Sie auf ein bestimmtes Protokoll klicken, wird eine Liste der virtuellen Server angezeigt, die dieses Protokoll verwenden.

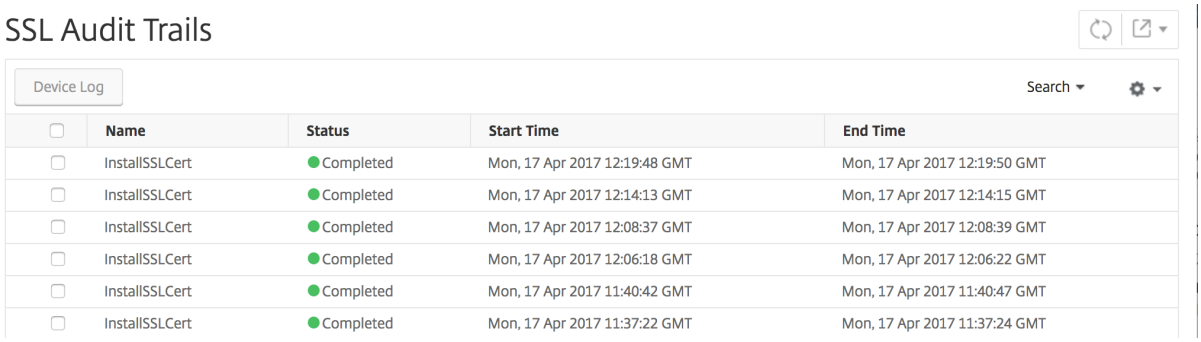
Ein Donutdiagramm wird angezeigt, nachdem Diffie-Hellman (DH) oder Ephermeral RSA-Schlüssel auf dem SSL-Dashboard aktiviert oder deaktiviert sind. Diese Schlüssel ermöglichen eine sichere Kommunikation mit Exportclients, auch wenn das Serverzertifikat keine Exportclients unterstützt, wie im Fall eines 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

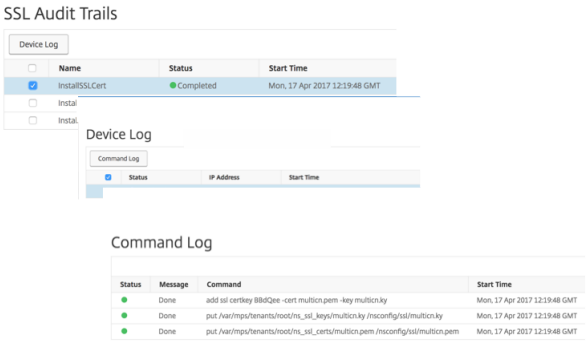
Sie können jetzt Protokolldetails von SSL-Zertifikaten auf Citrix ADM anzeigen. In den Protokolldetails werden Vorgänge angezeigt, die mit SSL-Zertifikaten auf Citrix ADM ausgeführt wurden, z. B.: Installieren von SSL-Zertifikaten, Verknüpfen und Aufheben der Verknüpfung von SSL-Zertifikaten, Aktualisieren von SSL-Zertifikaten und Löschen von SSL- Audit-Pfadinformationen sind nützlich, während SSL-Zertifikatänderungen in einer Anwendung mit mehreren Eigentümern überwacht werden.

****Um ein Auditprotokoll für einen bestimmten Vorgang anzuzeigen, der auf Citrix ADM mithilfe von SSL-Zertifikaten ausgeführt wurde, navigieren Sie zu Netzwerke > **SSL-Dashboard** > **SSL Audit Trails** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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, auf der der Vorgang ausgeführt wurde, und die Befehle, die auf dieser Instanz ausgeführt wurden, anzeigen.



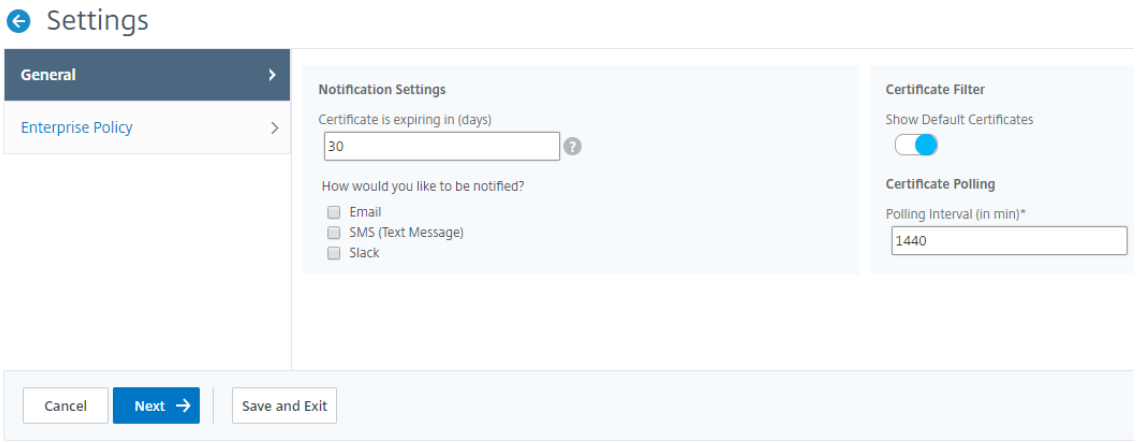
So schließen Sie standardmäßige Citrix ADC Zertifikate im SSL-Dashboard aus

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

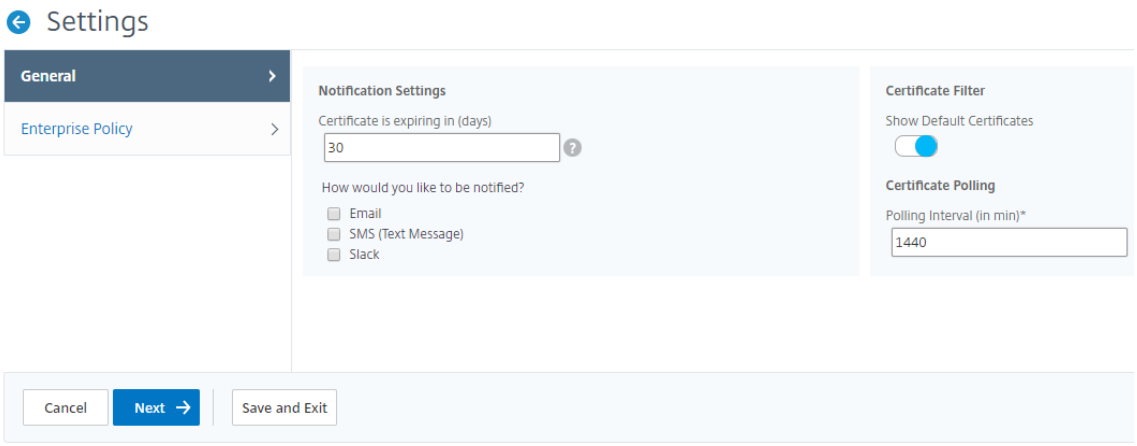
1. Navigieren Sie in NetScaler Application Delivery Management (ADM) zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Klicken Sie auf der Seite **SSL-Einstellungen** auf das Symbol **Bearbeiten**.
4. Geben Sie im Abschnitt **Benachrichtigungseinstellungen** 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 NetScaler-Instances installieren**“die folgenden Parameter an:

    a) Zertifikatquelle
    Wählen Sie die Option aus der **Instanz importieren aus**.

    - Wählen Sie die **Instanz** aus, aus der Sie das Zertifikat importieren möchten.
    - Wählen Sie das **Zertifikat** aus der Liste aller SSL-Zertifikatsdateien auf der Instanz aus.

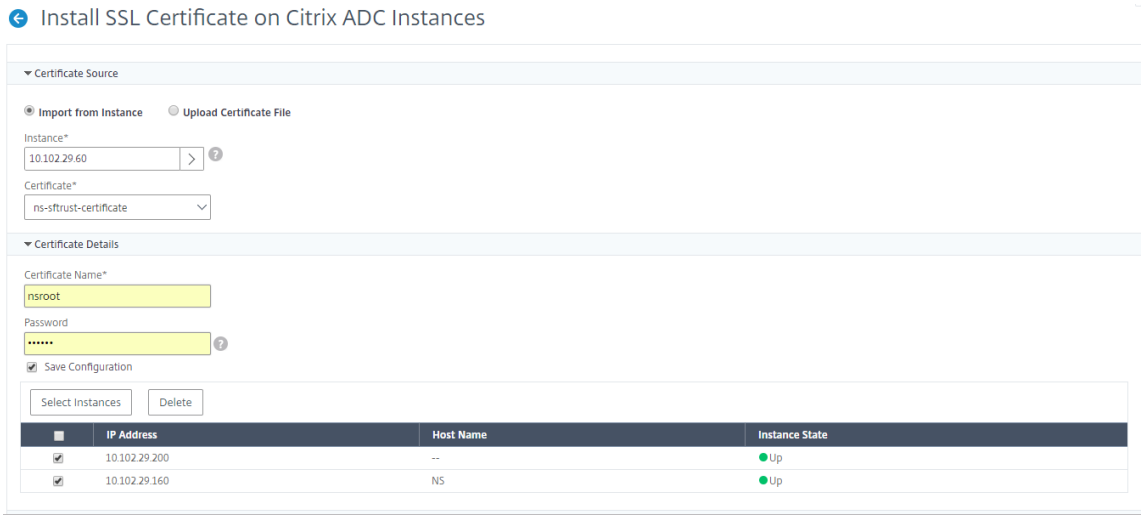
    b) Zertifikatdetails

    - **Name des Zertifikats**. Geben Sie einen Namen für den Zertifikatsschlüssel an.
    - **Kennwort**. Kennwort zum Verschlüsseln des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.

4. Klicken Sie auf **Instanzen auswählen**, um die NetScaler ADC-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

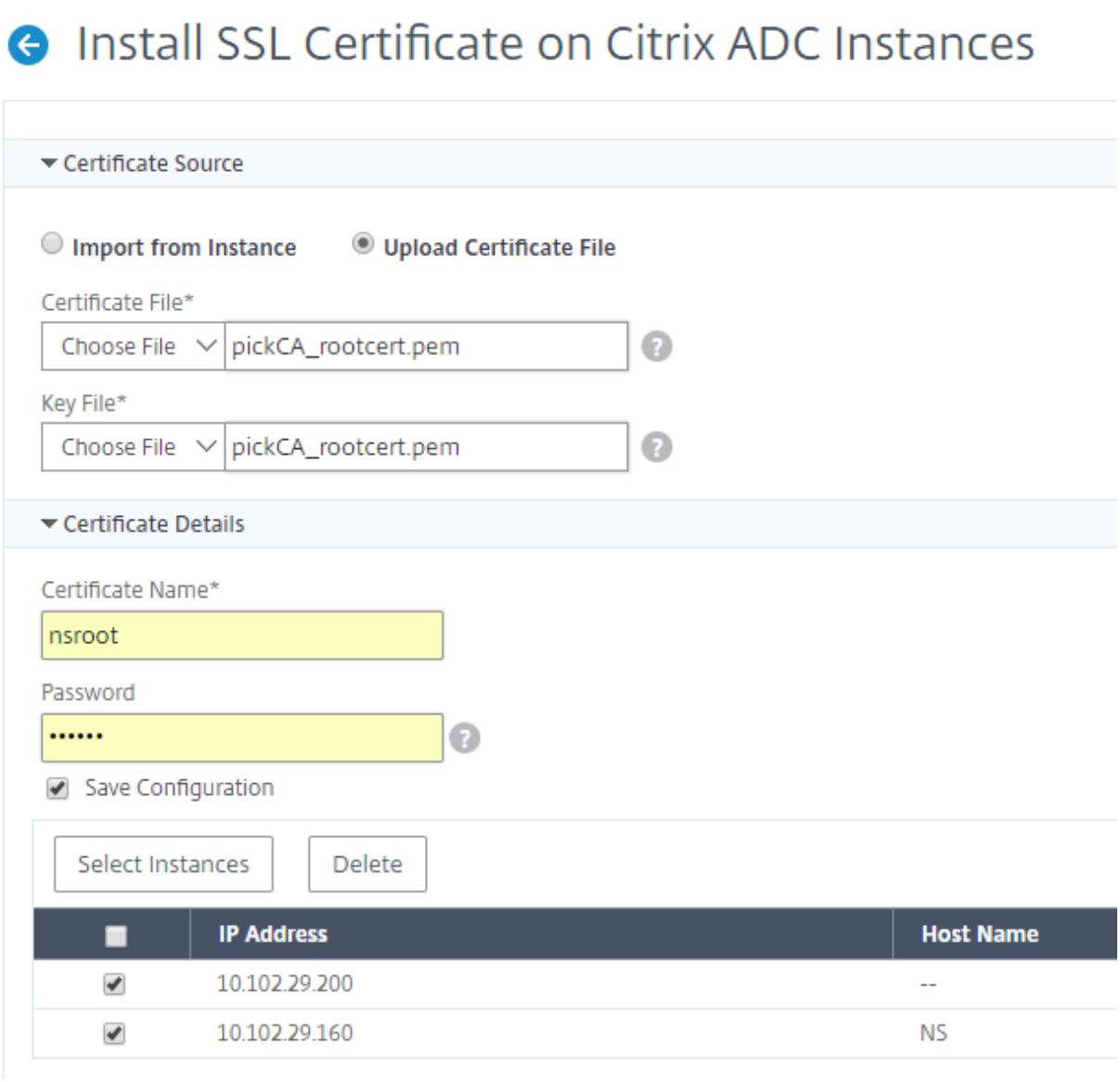
5. Klicken Sie auf **OK**.



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 Instanz installieren** die Option **Zertifikatdatei hochladen** aus, und geben Sie die folgenden Parameter an:
   - **Zertifikatdatei** —Laden Sie eine SSL-Zertifikatsdatei hoch, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** auswählen (die Zertifikatdatei muss auf der 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der folgenden Seite zusätzliche Details an. Wenn Sie die CSR erstellen möchten, ohne die Standardeinstellungen zu ändern, klicken Sie auf **Weiter**.

> **Hinweis**
>
> Die meisten Felder haben Standardwerte, die aus dem Betreff des ausgewählten Zertifikats extrahiert wurden. Der Betreff enthält Details wie den allgemeinen Namen, den Namen der Organisation, den Bundesstaat und das Land.
>
> Die meisten Zertifizierungsstellen akzeptieren Zertifikatsübermittlungen per E-Mail. 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die Zertifikate, die auf der Citrix Application Delivery Controller (ADC) -Instanz installiert sind, nicht der Unternehmensrichtlinie hinzugefügt wurden, zeigt das SSL-Zertifikat-Dashboard den Aussteller dieser Zertifikate als Nicht empfohlen an.

Wenn die Schlüsselstärke des Zertifikats nicht der in der Unternehmensrichtlinie empfohlenen Schlüsselstärke entspricht, zeigt das SSL-Zertifikat-Dashboard die Stärken dieser Schlüssel außerdem als Nicht empfohlenan.

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

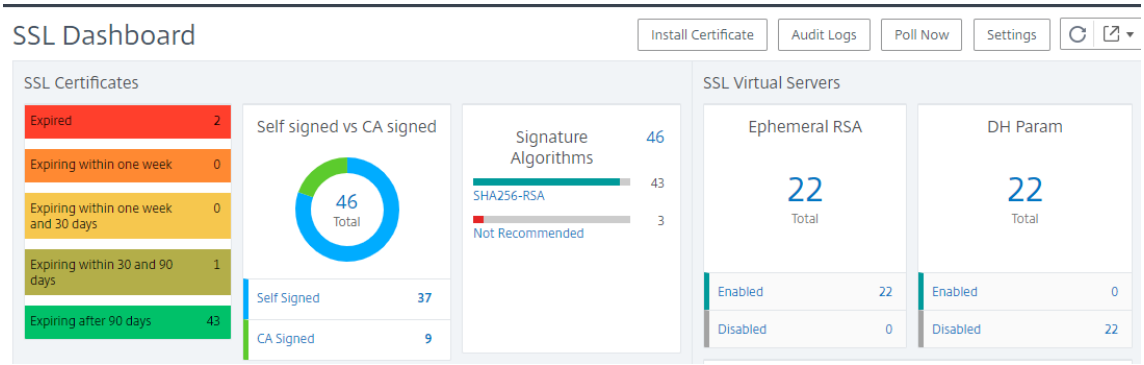
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

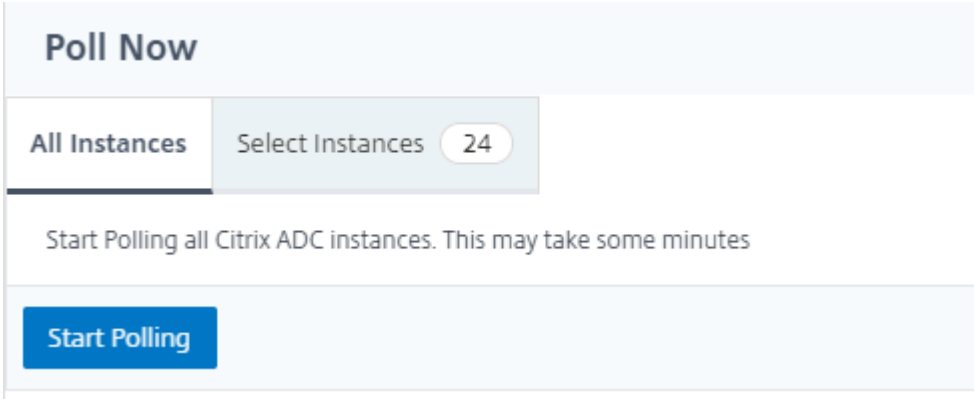
So fragen Sie SSL-Zertifikate auf Citrix ADC-Instanzen ab:

1. Navigieren Sie in Citrix ADM zu **Netzwerke** > **SSL-Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** oben rechts auf **Jetzt abfragen**.



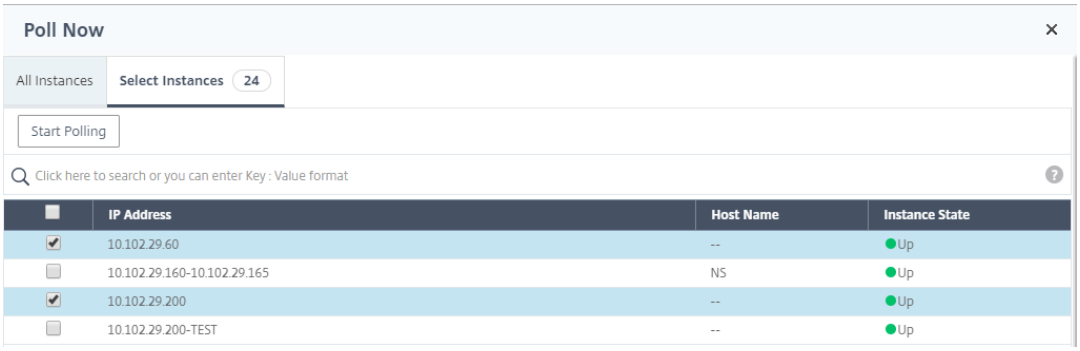
3. Die **Seite „Jetzt abfragen** “wird geöffnet und bietet Ihnen die Möglichkeit, alle Citrix ADC-Instanzen im Netzwerk oder die ausgewählten Instanzen abzufragen.

   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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

Mit Citrix ADM können Sie Konfigurationsaufträge erstellen, die Ihnen helfen, all diese Aktivitäten mit Leichtigkeit 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 dieser Optionen, um eine wiederverwendbare Quelle von Befehlen und Anweisungen für das System zum Ausführen eines Konfigurationsauftrags zu erstellen.

1. Konfigurationsvorlage
2. Instanz
3. Datei
4. Aufnehmen und Abspielen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurationsvorlage

Sie können Konfigurationsvorlagen erstellen, während Sie einen neuen Job 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. 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 auch wählen, ob der Job sofort ausgeführt werden soll oder den Job 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 auch eine Citrix ADC Instanz aktualisieren, indem Sie die ausgeführte Konfiguration oder eine gespeicherte Konfiguration extrahieren und die Befehle auf einer anderen Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aufnehmen und Abspielen

Mit Job erstellen können Sie entweder eigene CLI-Befehle eingeben oder die Schaltfläche Aufzeichnen und Wiedergeben verwenden, um Befehle aus einer Citrix ADC -Sitzung abrufen zu können. 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 Jobnamen an und wählen Sie den Instanztyp aus der Dropdownliste aus.
4. **Wählen Sie in der Dropdownliste 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfigurationsvorlagen importieren. Sie können auch mehrere Vorlagen verschiedener Typen im Konfigurationseditor hinzufügen, während Sie einen Job in den Konfigurationsaufträgen erstellen. Wählen Sie in der Dropdownliste Konfigurationsquelle die verschiedenen Vorlagen aus und ziehen Sie die Vorlagen dann per Drag & Drop in den Konfigurationseditor. Die Vorlagentypen können Konfigurationsvorlage, Integrierte Vorlage, Masterkonfiguration, Aufnahme und Wiedergabe, Instanz und Datei sein.

> **Hinweis**
>
> Wenn Sie die Jobvorlage „Hauptkonfiguration bereitstellen“zum ersten Mal hinzufügen und dann eine Vorlage eines anderen Typs hinzufügen, entspricht die gesamte Auftragsvorlage dem Typ „Masterkonfiguration“.

5. 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 zu einem späteren Zeitpunkt neu anordnen und anordnen, während Sie den Konfigurationsjob bearbeiten.
6. Sie können Variablen definieren, mit denen Sie unterschiedliche Werte für diese Parameter zuweisen oder einen Job über mehrere Instanzen hinweg 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.
7. **Wählen Sie auf der Registerkarte „Instanzen** auswählen“die Instanzen aus, für die Sie das Konfigurationsaudit ausführen möchten, und klicken Sie auf Weiter**.**
8. 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
9. Klicken Sie auf **Weiter**.
10. ****Sie können die Befehle, die auf jeder Instanz ausgeführt werden sollen, auf der Registerkarte Jobvorschau auswerten und überprüfen. Um Rollback-Befehle auszuwerten, aktivieren Sie das Kontrollkästchen **Vorschau der Rollback-Befehle**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11. Wählen Sie auf der Registerkarte „ Ausführen “, ob Sie Ihren Job entweder jetzt ausführen oder die Ausführung des Jobs zu einem späteren Zeitpunkt planen möchten.** Außerdem müssen Sie auswählen, welche Aktion Citrix ADM ergreifen soll, wenn der Befehl fehlschlägt.

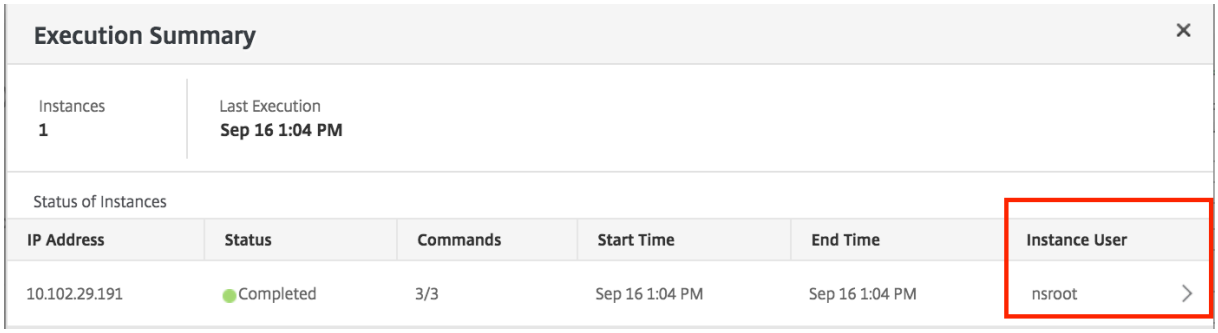
Um eine E-Mail-Benachrichtigung für einen Job zu senden:

Eine E-Mail-Benachrichtigung wird jetzt jedes Mal gesendet, wenn ein Job ausgeführt oder geplant wird. Die Benachrichtigung enthält Einzelheiten wie den Erfolg oder Misserfolg des Auftrags sowie die entsprechenden Details.

Nachdem Sie einen Job erstellt haben, aktivieren Sie auf der Registerkarte Ausführen das Kontrollkästchen E-**Mail** im Abschnitt Ausführungsbericht empfangen über. Wählen Sie eine E-Mail-Verteilerliste aus der Dropdownliste aus. Sie können auch eine E-Mail-Verteilerliste erstellen, indem Sie auf das Symbol **+** klicken und Details des E-Mail-Servers angeben.

So zeigen Sie Details zur Ausführungszusammenfassung an:

Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**. Wählen Sie einen Job aus und klicken Sie auf **Details** . **Klicken Sie auf Ausführungsübersicht , um den Status der Instanz, auf der der Job ausgeführt wurde, die für den Job ausgeführten Befehle, die Start- und Endzeit des Jobs und den Namen des Instanzbenutzers anzuzeigen.



Aufzeichnung und Wiedergabe zum Erstellen von Konfigurationsaufträgen verwenden

February 5, 2024

Wenn Sie es gewohnt sind, die NetScaler GUI zum Konfigurieren einer NetScaler-Instanz zu verwenden, kann es manchmal schwierig sein, die genauen CLI-Befehle abzurufen, um eine Konfigurationsaufgabe zu erstellen und sie auf mehreren NetScaler-Instanzen auszuführen.

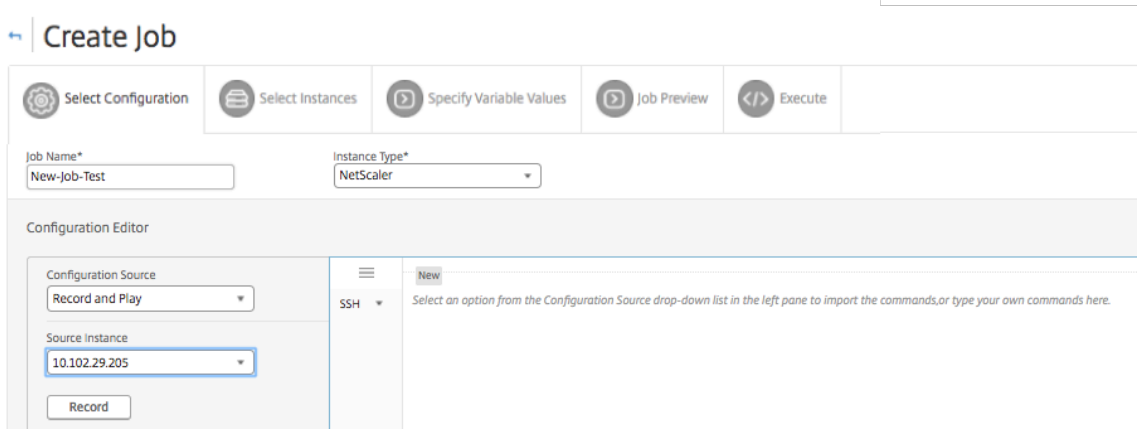
Mit NetScaler ADM können Sie die Konfigurationsaufgaben aufzeichnen, die mit der GUI einer NetScaler-Instanz ausgeführt wurden, und sie in CLI-Befehle konvertieren. Sie können dann aus

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

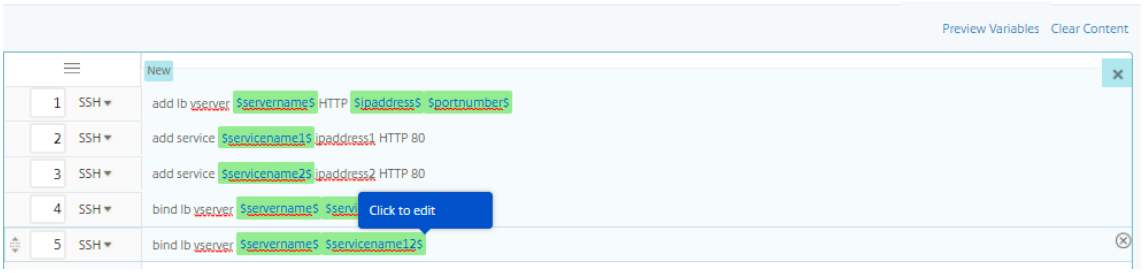
diesen CLI-Befehlen eine Konfigurationsaufgabe erstellen und diesen Task auf mehreren Instanzen ausführen.

So zeichnen Sie die GUI-Konfiguration auf und konvertieren sie in eine Konfigurationsaufgabe

1. Navigieren Sie zu **Networks > Configuration Jobs** und klicken Sie dann auf **Create Job**.
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**.



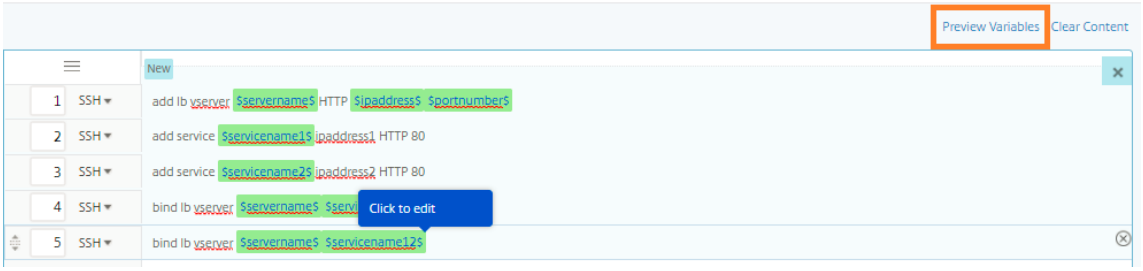
4. Die **NetScaler GUI** wird geöffnet. Konfigurieren Sie die Features und Einstellungen, die die Konfigurationsaufgabe enthalten soll. Schließen Sie dann das NetScaler GUI-Fenster und klicken Sie im **Konfigurationseditor** auf **Stopp**. Die Befehle werden im linken Fensterbereich als Link angezeigt. Ziehen Sie die Befehle per Drag & Drop 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.

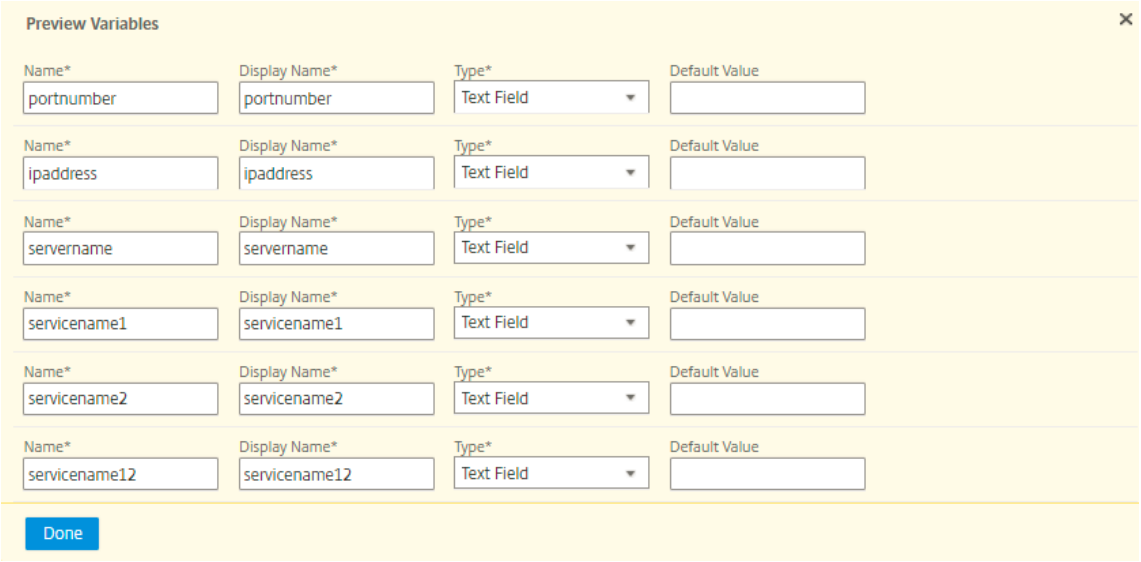
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 **Variablen in der Vorschau anzeigen**, um eine Vorschau der Variablen in einer einzigen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.

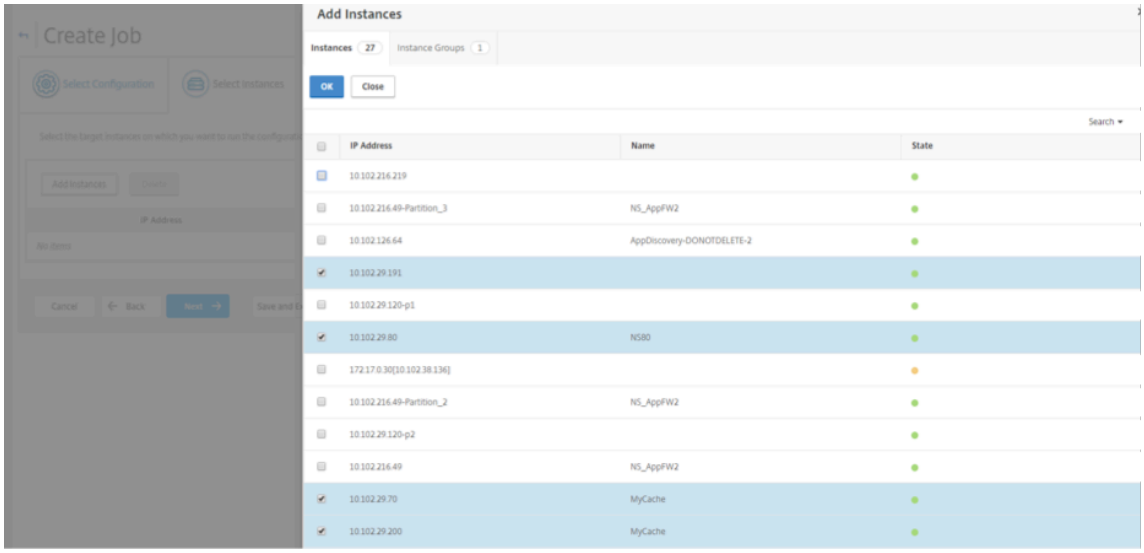


8. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

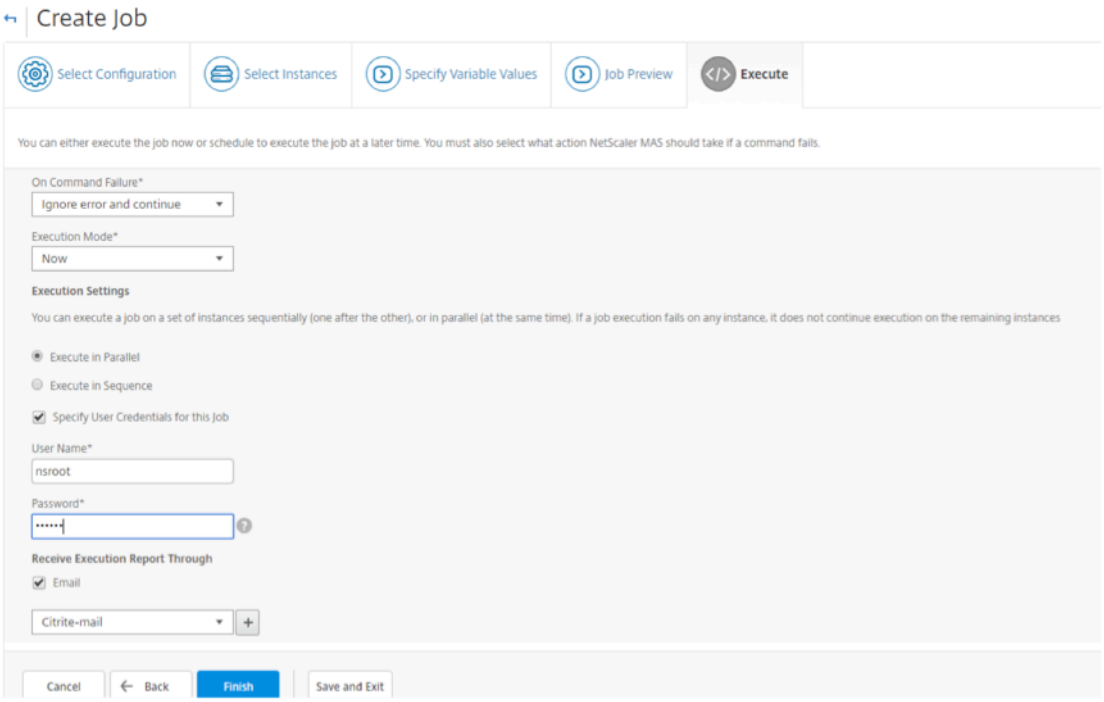
Um die ausgeführten Konfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk > Konfigurationsaufträge** und klicken Sie auf **Job erstellen**. Auf der Seite **Job erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame 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 Konfigurationsjobs anzuzeigen, während Sie einen Konfigurationsjob bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Jobnamen 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.

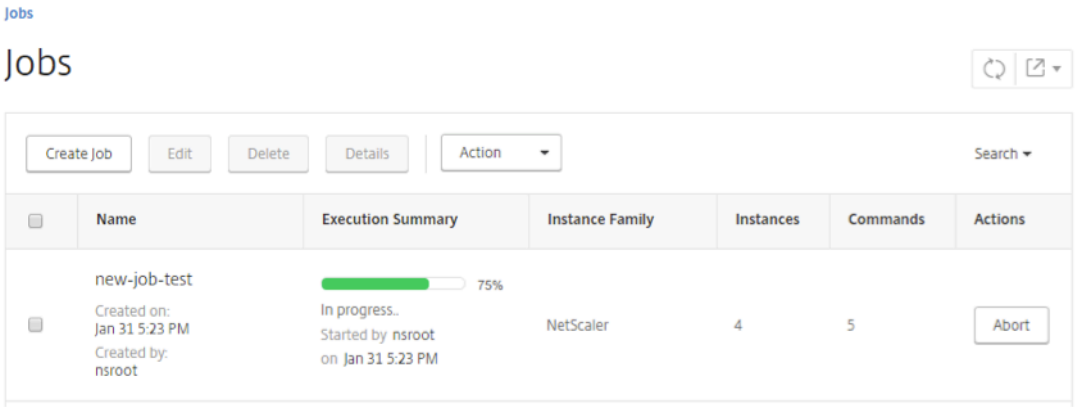
11. Auf der Registerkarte**Auftragsvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen.
12. Auf der Registerkarte**Ausführen**können Sie Ihren Job jetzt ausführen oder planen, dass er zu einem späteren Zeitpunkt ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen soll, wenn der Befehl fehlschlägt.

    Sie können auch festlegen, dass autorisierte Benutzer Jobs auf Ihren verwalteten Instances ausführen dürfen, und Sie können wählen, ob eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details gesendet werden soll.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 NetScaler-Instanz zu extrahieren und auf mehreren Instanzen zu replizieren.

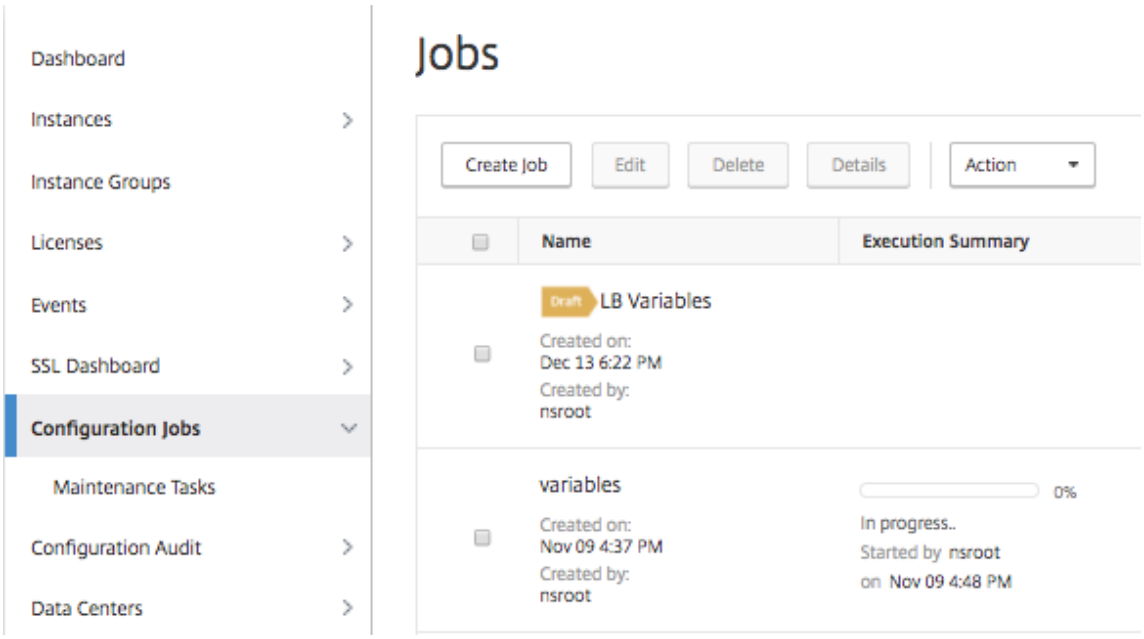
Beispielsweise haben Sie möglicherweise sowohl Load Balancing als auch Front-End-Optimierung

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(FEO) auf einer NetScaler-Instance für Ihre Bereitstellung konfiguriert. Jetzt möchten Sie jedoch nur die FEO-Konfiguration auf andere NetScaler-Instanzen replizieren.

So rufen Sie die Konfiguration von einer Instanz auf andere NetScaler-Instanzen ab und replizieren sie:

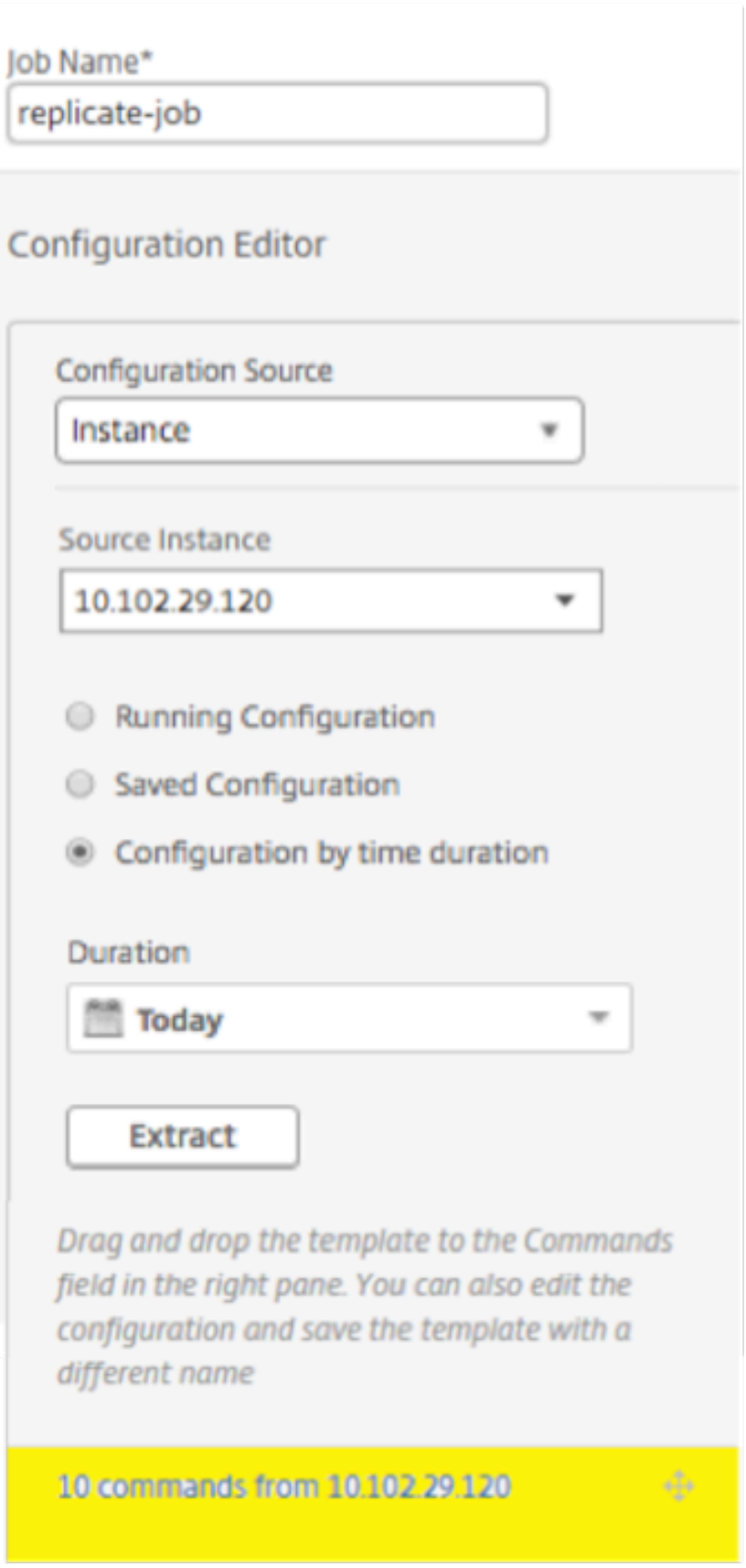
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge**, und klicken Sie dann auf **Job erstellen**.



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 in dem von Ihnen ausgewählten Zeitraum auf dieser Instanz ausgeführt wurden, wird auf dem Bildschirm angezeigt, wie in der Abbildung unten hervorgehoben.

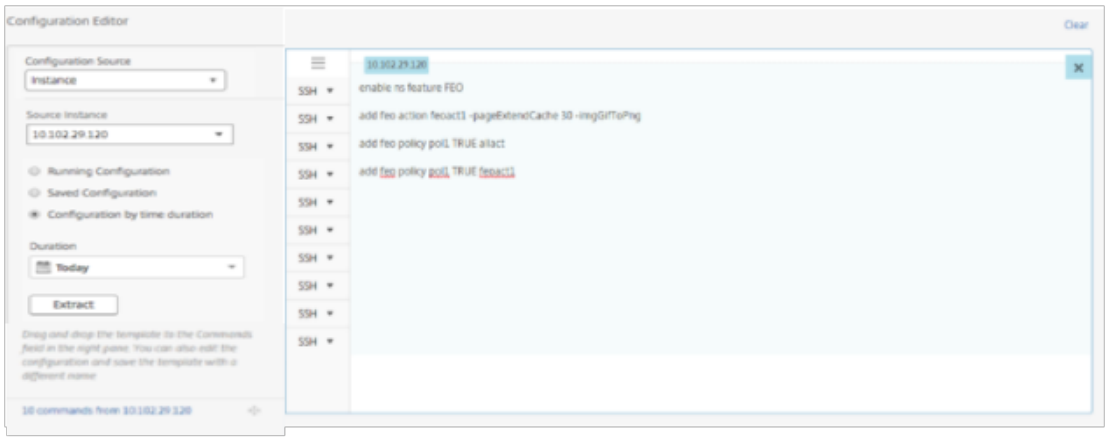
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Ziehen Sie die Befehle per Drag & Drop in das Feld **Befehle** im rechten Bereich.

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 **Ausführen** auf **Fertig stellen**, um den Job auf den ausgewählten NetScaler-Instanzen auszuführen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Variablen in Konfigurationsaufträgen verwenden

February 5, 2024

Ein Konfigurationsjob 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 unterschiedliche Werte für die in Ihrer Konfiguration verwendeten Parameter verwenden. Sie können Variablen definieren, mit denen Sie unterschiedliche Werte für diese Parameter zuweisen oder einen Job über mehrere Instanzen hinweg 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:

füge lb vserver **Servername** HTTP IP-**Adresse Portnummer** hinzu

Dienstname **1 IP**-**Adresse1** HTTP 80 hinzufügen

Service Servicename**2** IP-**Adresse2** HTTP 80 hinzufügen

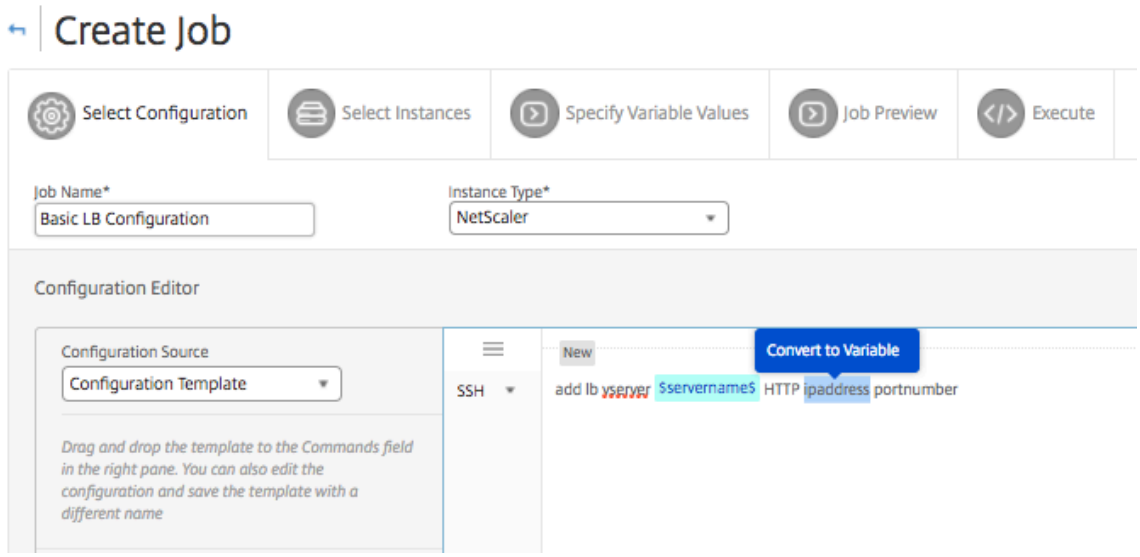
bind lb vserver **servername servicename1**

bind lb vserver **servername servicename2**

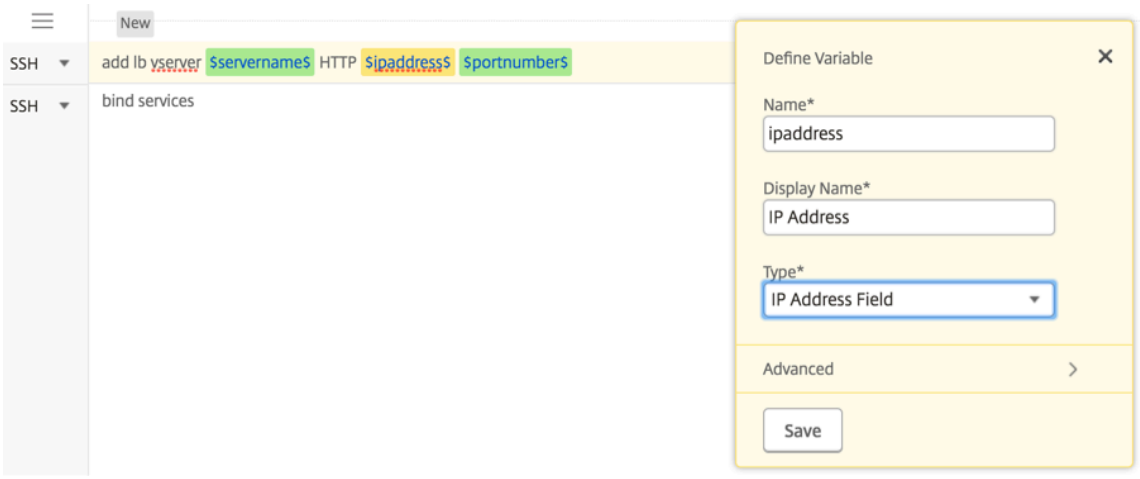
So erstellen Sie einen Konfigurationsauftrag durch Definieren von Variablen in NetScaler ADM:

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 konvertieren**. Wählen Sie beispielsweise die IP-Adresse *ipaddress* des Load Balancing-Servers aus und klicken Sie auf **In Variable konvertieren**, wie in der Abbildung unten gezeigt.

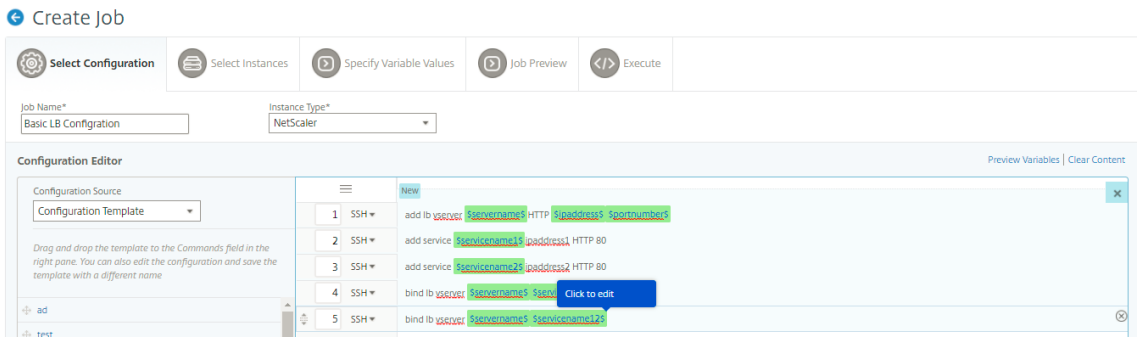
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Sobald Sie sehen, dass der Wert der Variablen von Dollarzeichen umgeben ist, klicken Sie auf die Variable, um die Details der Variablen wie Name, Anzeigename und Typ weiter 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-

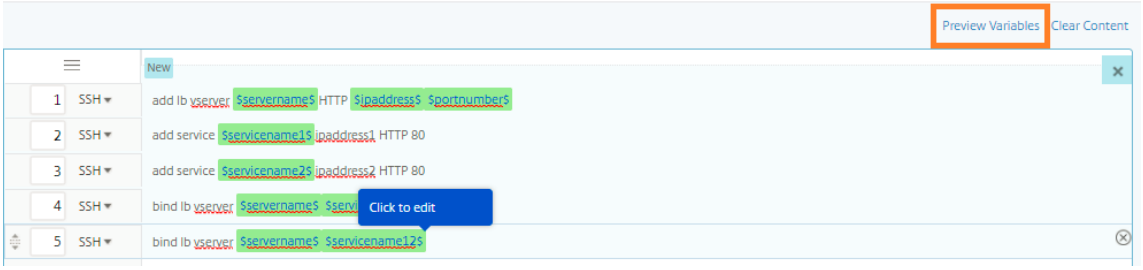
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

tionsauftrags in einer einzigen konsolidierten Ansicht definiert haben.

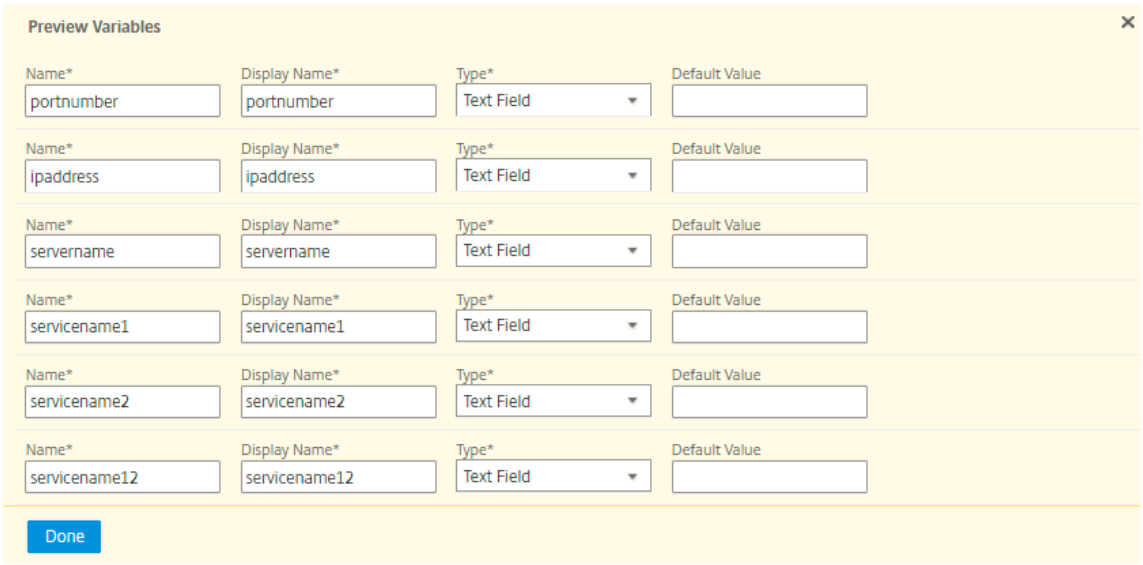
7. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

   - 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 **Variablen in der Vorschau anzeigen**, um eine Vorschau der Variablen in einer einzigen 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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

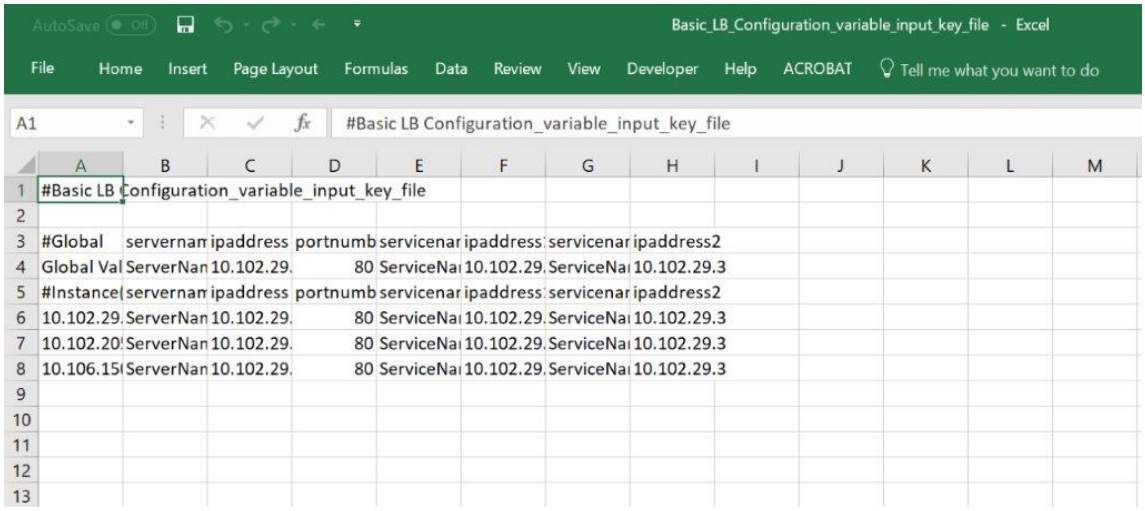
10. Anschließend können Sie die Befehle im Konfigurationseditor neu anordnen und neu anordnen. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und dort ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben 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 NetScaler-Instanz angeben, die Sie zuvor ausgewählt haben, 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-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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Wichtig!**
>
> Wenn Sie eine CSV-Datei von einem Mac hochladen, speichert Mac die CSV-Datei mit Semikolons statt Kommas. Dies führt dazu, dass die Konfiguration fehlschlägt, wenn Sie die Eingabedatei hochladen und den Auftrag ausführen. Wenn Sie einen Mac verwenden, verwenden Sie einen Texteditor, um die erforderlichen Änderungen vorzunehmen und dann die Datei hochzuladen.

15. Sie können auch gemeinsame Variablenwerte für alle Instanzen angeben und auf **Hochladen** klicken, um die Eingabeschlüsseldatei auf Citrix ADM hochzuladen.

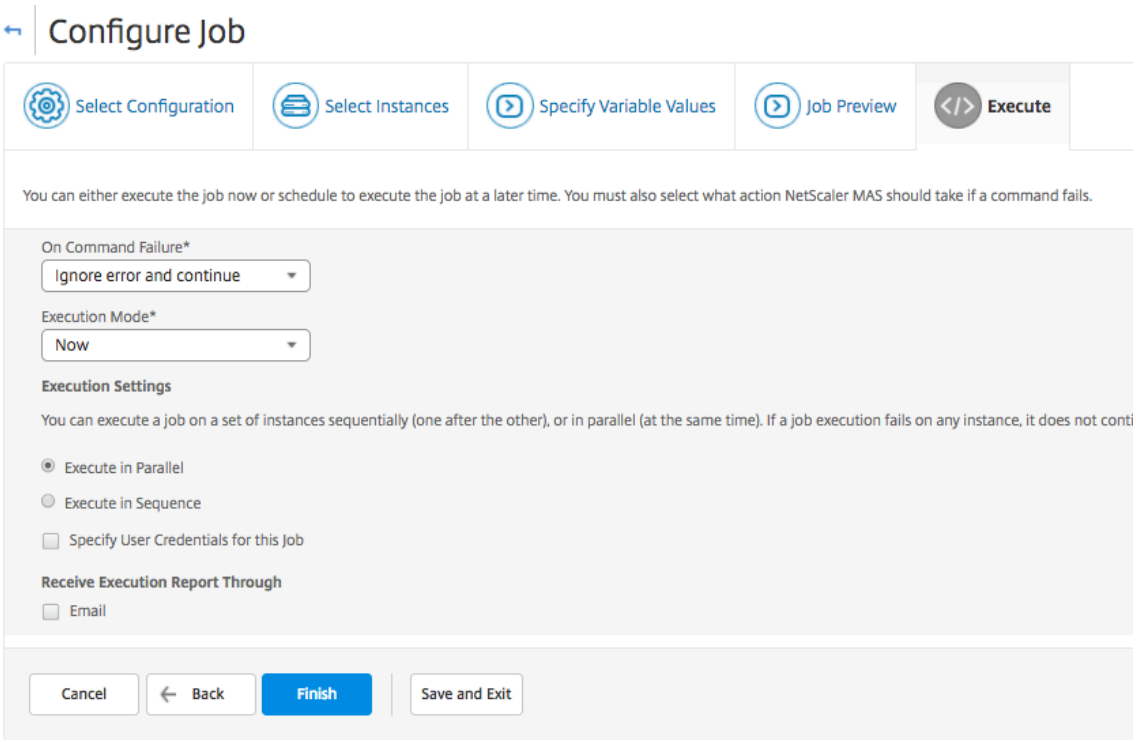
    Die wichtigsten Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsjobs beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

    Um die ausgeführten Konfigurationsaufträge 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 Konfigurationsjobs anzuzeigen, während Sie einen Konfigurationsjob bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Jobnamen 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).

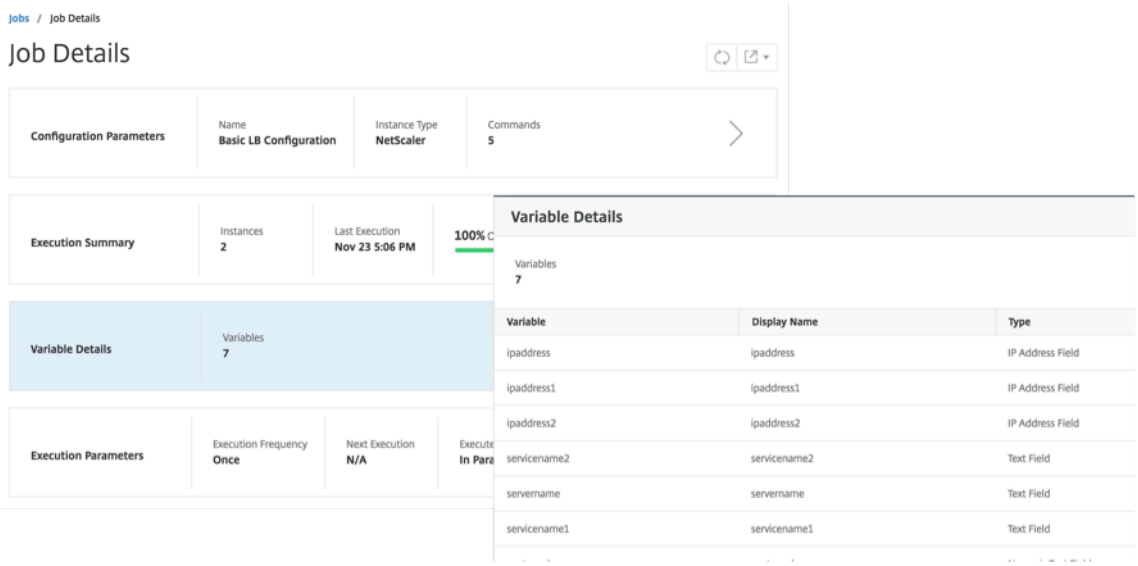
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 wählen, ob Sie Ihren Job jetzt ausführen möchten oder ob er zu einem späteren Zeitpunkt ausgeführt werden soll. Sie können auch auswählen, welche Aktion Citrix ADM ergreifen soll, wenn der Befehl fehlschlägt und ob 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 Jobdetails sehen, indem Sie zu **Netzwerke** > **Konfigurationsjobs** navigieren und den Job auswählen, den Sie gerade konfiguriert haben. Klicken Sie auf **Details** und dann auf **Variablendetails**, um die Liste der Variablen zu sehen, die zu Ihrem Job hinzugefügt wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

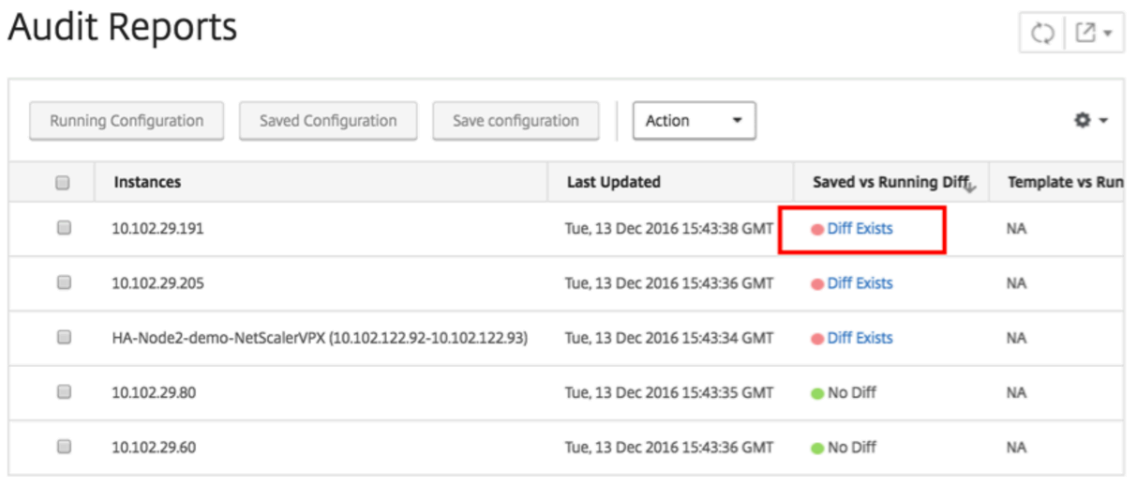
Wenn Sie feststellen, dass sich die Konfiguration einiger Instanzen ändert, können Sie die NetScaler ADM-Korrekturbefehle verwenden, um einen Konfigurationsauftrag mit den geänderten und korrigierten Konfigurationsbefehlen für bestimmte NetScaler ADC-Instanzen zu erstellen.

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 Korrekturbefehle auch verwenden, um einen Konfigurationsjob zu erstellen und diesen auf den spezifischen Citrix ADC-Instanzen auszuführen, um sie wieder in die gewünschte Konfiguration zu bringen.

So erstellen Sie einen Konfigurationsauftrag 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-Instanz auf eine andere replizieren

February 5, 2024

24. Mai 2018

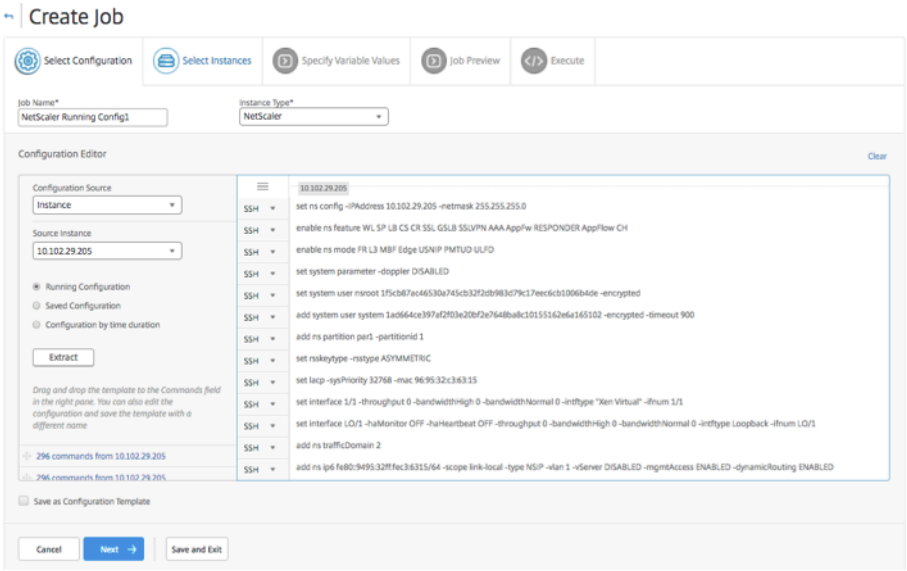
Sie können jetzt die Konfiguration einer NetScaler-Instanz auf anderen Instanzen replizieren. Wenn Sie einen Auftrag in NetScaler ADM konfigurieren, wählen Sie eine Instanz als Konfigurationsquelle aus, und wählen Sie die ausgeführte oder gespeicherte Konfiguration der ausgewählten Instanz aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie beispielsweise **Laufende Konfiguration** auswählen und auf **Extrahieren** klicken, sendet NetScaler ADM eine Anforderung an die ausgewählte NetScaler-Instanz, um die ausgeführte Konfiguration zu finden, und zeigt sie als Vorlage an. Sie können die Vorlage per Drag & Drop in das Feld **Befehle** im rechten Fensterbereich ziehen. Sie können Befehle, Parameter und die 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 *NetScaler Running Config1* als Namen Ihres Jobs und den Instanztyp *NetScaler* an.
3. Wählen Sie **Instanz** als **Konfigurationsquelle**, und wählen Sie die Quellinstanz aus, deren Konfiguration Sie auf anderen Instanzen replizieren möchten.
4. Sie werden die folgenden drei Optionen sehen:
   - Laufende Konfiguration
   - Konfiguration gespeichert
   - Konfiguration nach Zeitdauer
5. Wählen Sie **Konfiguration ausführen**und klicken Sie auf **Extrahieren**. Die Anzahl der laufenden Konfigurationsbefehle, die auf dieser Instanz ausgeführt wurden, wird angezeigt.



6. Ziehen Sie die Befehle per Drag & Drop in das Feld **Befehle** im rechten Bereich.
7. Sie können die Befehle im Feld Befehle bearbeiten. Wenn die extrahierten Befehle beispielsweise eine NetScaler-Instanz einrichten sollen. Dazu gehören das Hinzufügen von Partitionen, das Einrichten des Lastausgleichs, das Binden des Lastausgleichsservers an Dienste usw.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können Ihre Befehle bearbeiten, um Ihre neuen NetScaler-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 wählen, ob Sie Ihren Job jetzt ausführen möchten oder ob er zu einem späteren Zeitpunkt ausgeführt werden soll. Sie können auch auswählen, welche Aktion Citrix ADM ergreifen soll, wenn der Befehl fehlschlägt, und ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details senden möchten.

Wiederverwenden ausgeführter Konfigurationsaufträge

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 stößt und die weitere Ausführung stoppt.

Citrix Application Delivery Management (ADM) bietet eine Funktion, um die abgeschlossenen Jobs erneut auszuführen. Mit dieser Funktion können Jobs, die vollständig ausgeführt wurden, erneut ausgeführt werden, ohne den Jobnamen zu ändern.

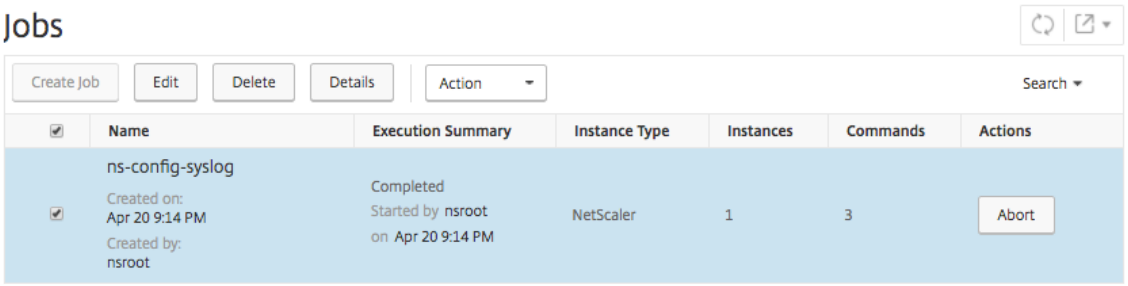
> **Hinweis:** Sie können nur die Jobs erneut ausführen, die ausgeführt werden, wenn der Ausführungsmodus „Jetzt“ist.

So bearbeiten Sie abgeschlossene Aufträge:

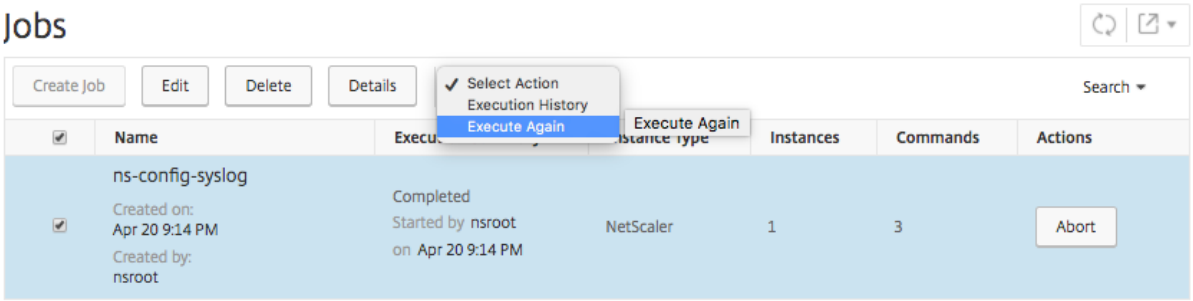
1. Navigieren Sie auf der Citrix ADM-Startseite zu **Netzwerke > Konfigurationsjobs**.
2. Wählen Sie auf der Seite **Jobs** einen Job aus, der die Ausführungsübersicht als abgeschlossen anzeigt, und klicken Sie auf **Bearbeiten**. Sie können einen geplanten Konfigurationsauftrag auch bearbeiten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 denselben Befehlssatz auf denselben 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

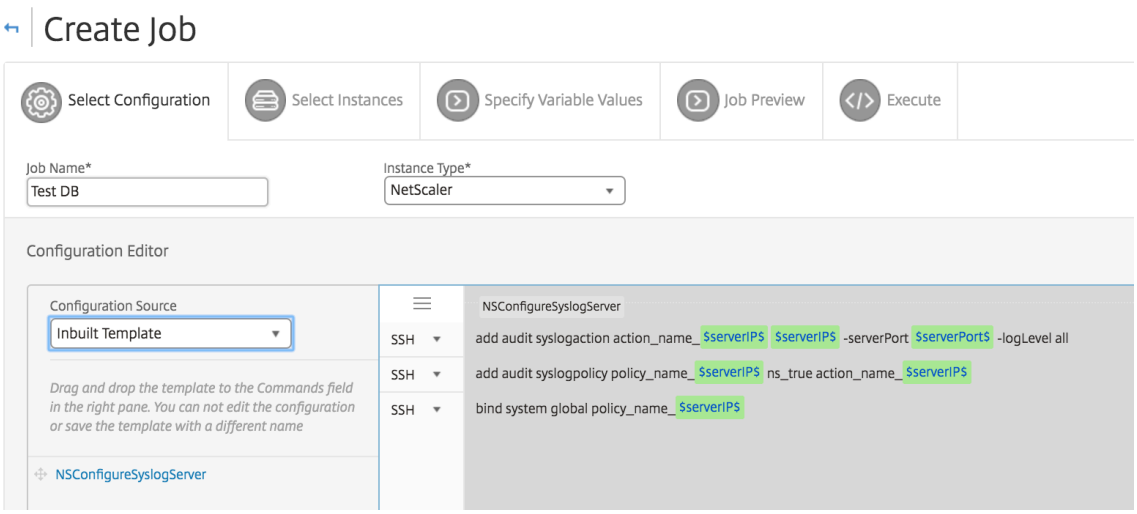
February 5, 2024

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 planen, dass er zu einem späteren Zeitpunkt ausgeführt wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

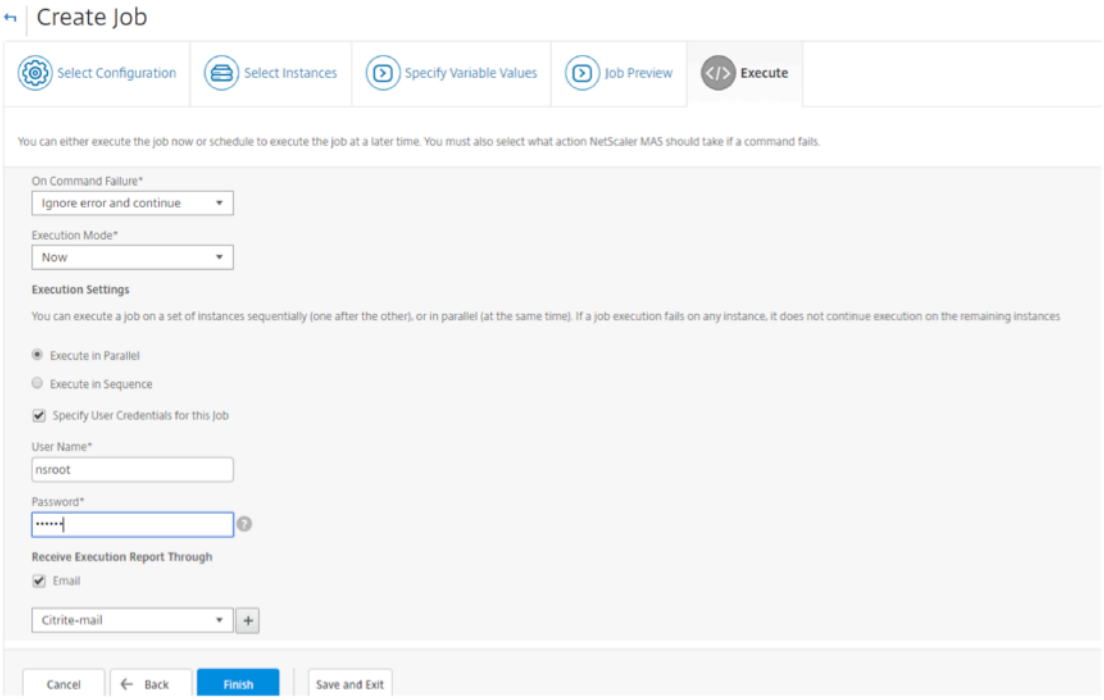
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Bei fehlgeschlagener** Anweisung —Wenn ein Befehl fehlschlägt, können Sie entweder die Fehler ignorieren und mit der Ausführung des Jobs fortfahren oder die weitere Ausführung des Jobs beenden. Wählen Sie die Aktion, die Sie ausführen möchten, aus der Dropdownliste aus.
- **Ausführungsmodus** —Sie können den Job entweder jetzt ausführen oder die Ausführung des Jobs zu einem späteren Zeitpunkt 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 Job auch sequentiell oder parallel auf einer Gruppe von Instanzen 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 festlegen, dass autorisierte Benutzer Jobs auf Ihren verwalteten Instances ausführen dürfen. 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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwenden von Wartungsaufträgen zum Aktualisieren von NetScaler SDX-Instanzen

February 5, 2024

Sie können ein Einzelbündel-Upgrade Ihrer NetScaler SDX-Instanzen mit NetScaler Version 11.0 und höher durchführen. Um ein Einzelbündel-Upgrade durchzuführen, verwenden Sie einen integrierten Task in NetScaler ADM. Mit dieser integrierten Aufgabe können Sie den NetScaler SDX Management Service, Citrix Hypervisor und die zusätzlichen Pakete und Hotfixes für Citrix Hypervisor aktualisieren.

So aktualisieren Sie NetScaler SDX-Instanzen mithilfe von NetScaler ADM:

1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge.**
2. Klicken Sie auf **Job erstellen**. Wählen Sie auf der Seite „Job erstellen“die integrierte Aufgabe „ **NetScaler SDX** aktualisieren “aus, um Ihre NetScaler SDX-Instanzen zu aktualisieren. Klicken Sie auf **Weiter**.
3. ****Geben Sie auf einer oder mehreren Seiten „NetScaler Appliances aktualisieren“auf der Registerkarte Instanzauswahl den Jobnamen an und klicken Sie auf **Instanzen hinzufügen .**
4. Wählen Sie die Zielinstanzen oder Instanzgruppen aus, die Sie aktualisieren möchten.
5. Nachdem Sie die NetScaler-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-Instanzen angezeigt.
6. Wählen Sie auf der Seite**Upgrade ändern NetScaler Appliance (s)** die Registerkarte**Upgrade**aus. Wählen Sie im **Software-Image**-Menü entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Build-Datei muss auf Citrix ADM vorhanden sein).
7. Sie können auch sehen, ob Instanzen Fehler beim Upgrade vor der Validierung aufweisen. Diese Fehler werden in Form einer Nachricht angezeigt. Die Meldungen zeigen die Fehler im Zusammenhang mit Speicherplatz, Festplattenlaufwerk und Benutzeranpassungen an. Wenn Sie nicht mit Instanzen fortfahren möchten, die die Überprüfung vor der Validierung fehlgeschlagen haben, können Sie die Instanzen entfernen. Um die Instanzen zu entfernen, wählen Sie die Instanzen aus, und klicken Sie auf**Löschen.**
8. Auf der Registerkarte**Task planen**können Sie auch Ausführungsdetails festlegen, in denen Sie den Upgradevorgang jetzt durchführen oder für einen späteren Zeitpunkt planen können. Sie können auch wählen, ob Sie Ihre NetScaler SDX-Instanz Backup, einen Ausführungsbericht per E-Mail erhalten oder ein zweistufiges Upgrade für Knoten in HA durchführen möchten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 wählen, ob Sie den Job sofort ausführen oder den Job später ausführen möchten. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Eingebaute Vorlage	Beschreibung
AddLink	Durch das Erstellen oder Definieren von Verknüpfungen kann die SD-WANOP-Appliance Überlastung und Verlust der Verbindungen verhindern und Traffic Shaping durchführen. Sie können die maximale Bandbreite festlegen, die über die Verbindung gesendet oder empfangen wird, und auch angeben, dass es sich um LAN-seitigen oder WAN-seitigen Datenverkehr handelt.
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, ermöglicht es Ihnen, Berechtigungen zuzuweisen, die in der AddUser-Vorlage nicht verfügbar sind.
AddService-class	Erstellt eine Serviceklasse für die Citrix SD-WANOP-Appliance mit einem oder mehreren Service-Class-Filtern und aktiviert diese.
SetApplication	Setzt die Definition des Anwendungsklassifizierers
AddorRemoveVideoCachingPorts	Fügt die Portnummer hinzu, an der die Videoquelle Daten senden oder empfangen kann. Der Standardport ist 80.
RemoveVideoCachingSource	Entfernt eine oder mehrere Videozwischenspeicherquellen. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Eingebaute Vorlage	Beschreibung
SetVideoCaching	Legt die maximale Größe für zwischengespeicherte Objekte fest. Ein Objekt, das größer als dieser Grenzwert ist, wird nicht zwischengespeichert. Standardmäßig beträgt die maximale Größe des Caching-Objekts 100 MB.
AddVideoCachingSource	Fügt die IP-Adresse oder den Domainnamen der Videoquelle hinzu. Enthält Optionen zum Aktivieren oder Deaktivieren des Video-Caching für diese Quelle.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

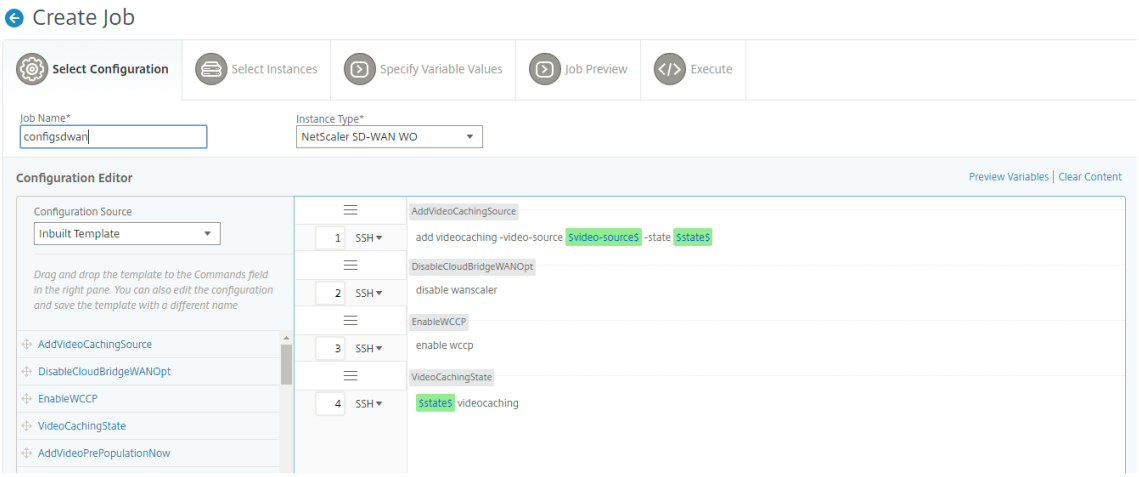
Eingebaute Vorlage	Beschreibung
AddVideoPrePopulation	Erstellt einen Videoeintrag zur Vorbevölkerung, mit dem Sie ein Video im Voraus herunterladen und zwischenspeichern können. Sie können auch angeben, wann ein Video zwischengespeichert werden soll.
UpdateVideoPrePopulation	Ändert einen Videovorbelegungseintrag, 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.
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.

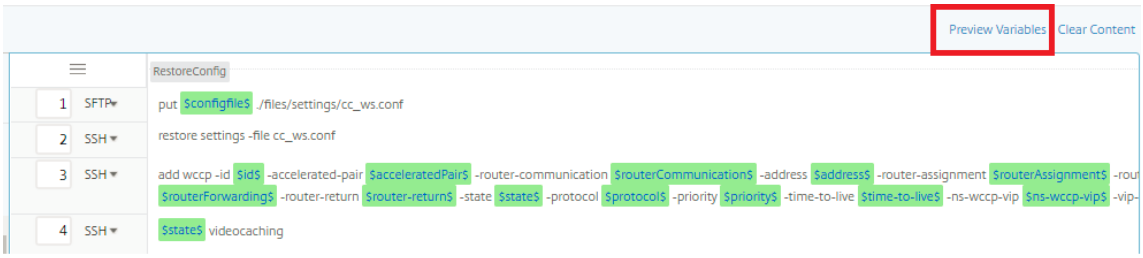
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

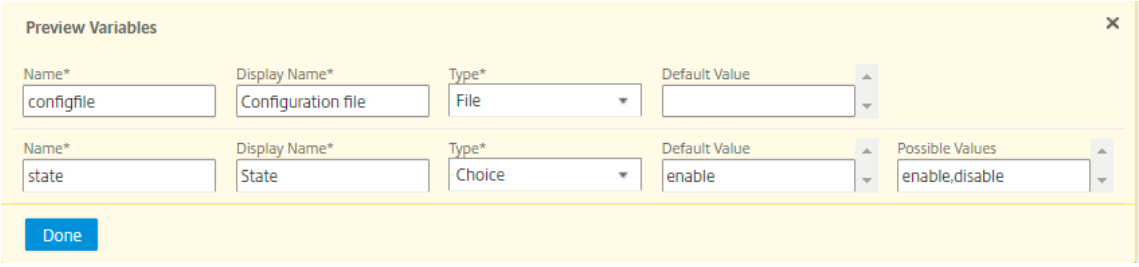
   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Netzwerke > Konfigurationsaufträge** und wählen Sie **Job erstellen** aus. Auf der Seite **Job erstellen** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Während Sie einen 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 **Variablen in der Vorschau anzeigen**, um eine Vorschau der Variablen in einer einzigen konsolidierten Ansicht anzuzeigen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben.



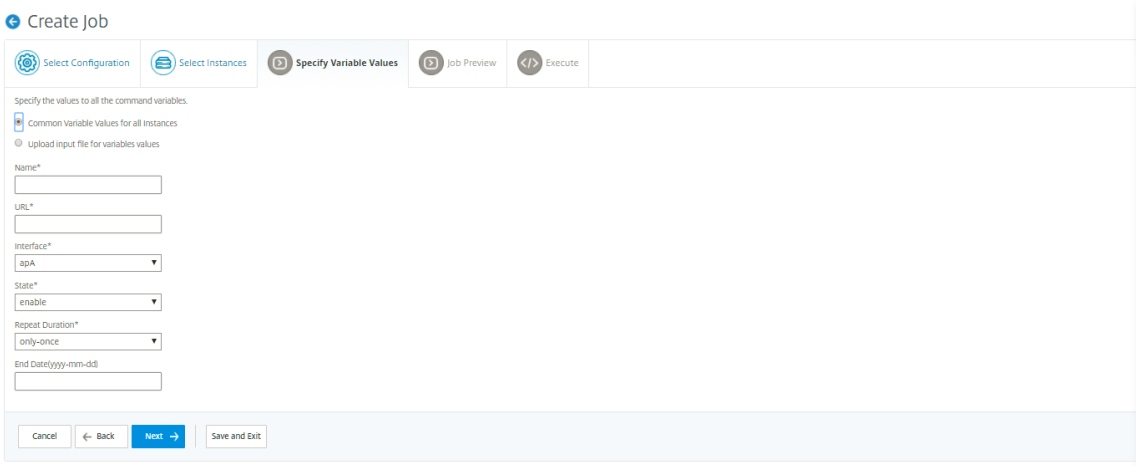
8. Ein neues Popup-Fenster wird angezeigt, in dem alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem tabellarischen Format angezeigt werden. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 ausgeführten Konfigurationsaufträge 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 hochgelade-

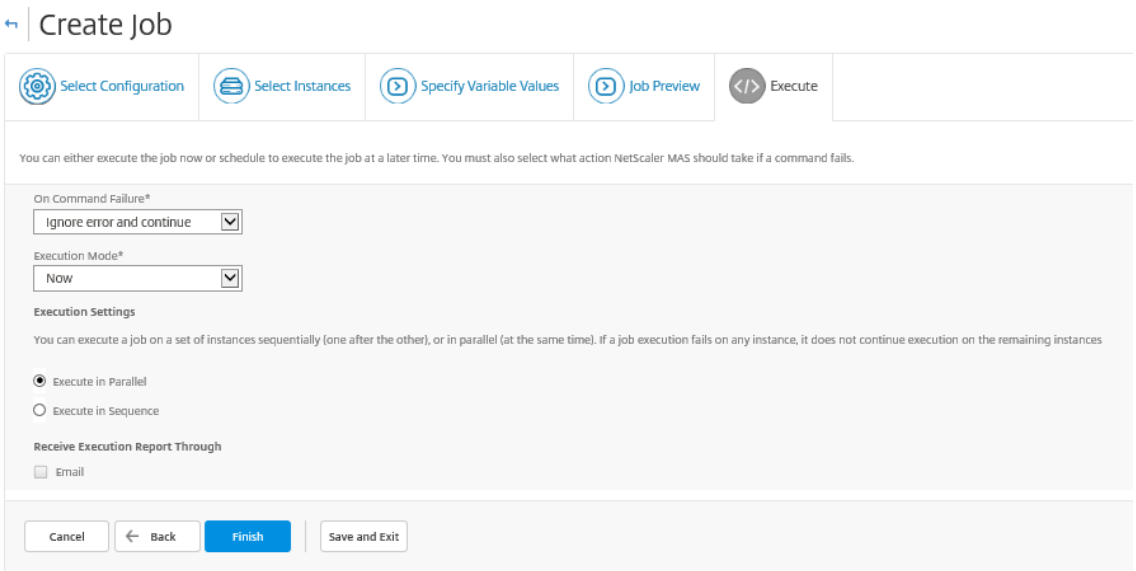
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nen 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 während der Bearbeitung 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).

11. Klicken Sie auf **Weiter**, auf der Registerkarte **Auftragsvorschau**können Sie die Befehle auswerten und überprüfen, die als Job ausgeführt werden sollen.
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 Job sofort aus oder planen Sie die Ausführung für einen späteren Zeitpunkt. 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**die Option aus, um den Job sequentiell (nacheinander) oder parallel (gleichzeitig) auszuführen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

14. Wenn Sie einen Bericht zur Auftragsausführung per E-Mail an eine Liste von Empfängern senden möchten, aktivieren Sie das Kontrollkästchen **E-Mail** im Abschnitt **Ausführungsbericht empfangen 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 Masterkonfigurationsvorlage ist eine flexible Option zum Erstellen und Bereitstellen einer Masterkonfiguration 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 Masterkonfigurationsvorlage aus 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 Masterkonfigurationsvorlage mithilfe der Konfigurationsvorlage ‘DeployMasterConfiguration’bereitstellen, während Sie einen neuen Job erstellen, können Sie sie für jede spezifische ADC-Instanz weiter anpassen, indem Sie zusätzliche 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 keinen Konfigurationsauftrag mit der DeployMasterConfiguration-Vorlage auf Citrix ADC CPX-Instanzen, in einem Cluster konfigurierten Instanzen oder auf partitionierten

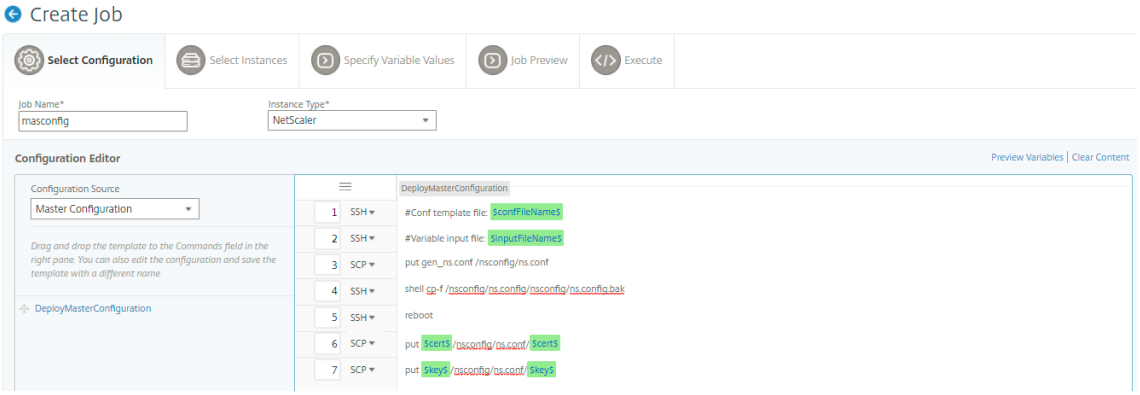
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 per Drag & Drop 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 zusätzlich zur Konfigurationsvorlagendatei und den variablen Eingabedateien Zertifikat- und Schlüsseldateien hochladen.



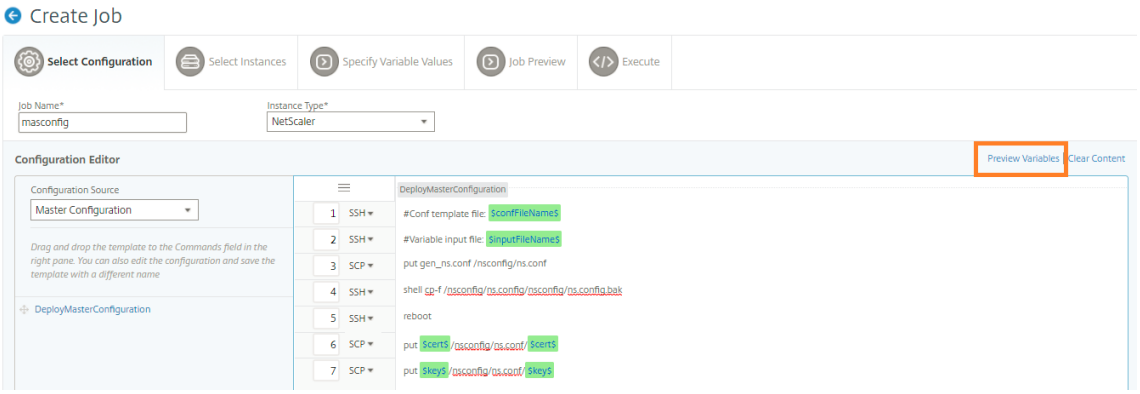
4. Sie können alle Variablen überprüfen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags in einer einzigen konsolidierten Ansicht definiert haben.
5. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

   - 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

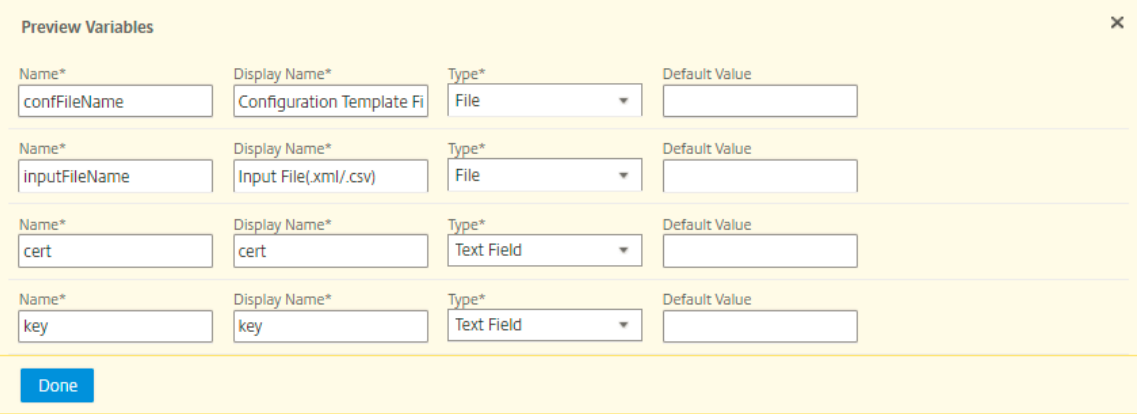
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Seite **Job konfigurieren** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

6. Sie können dann auf die Registerkarte **Variablen in der Vorschau anzeigen**, um eine Vorschau der Variablen in einer einzigen 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

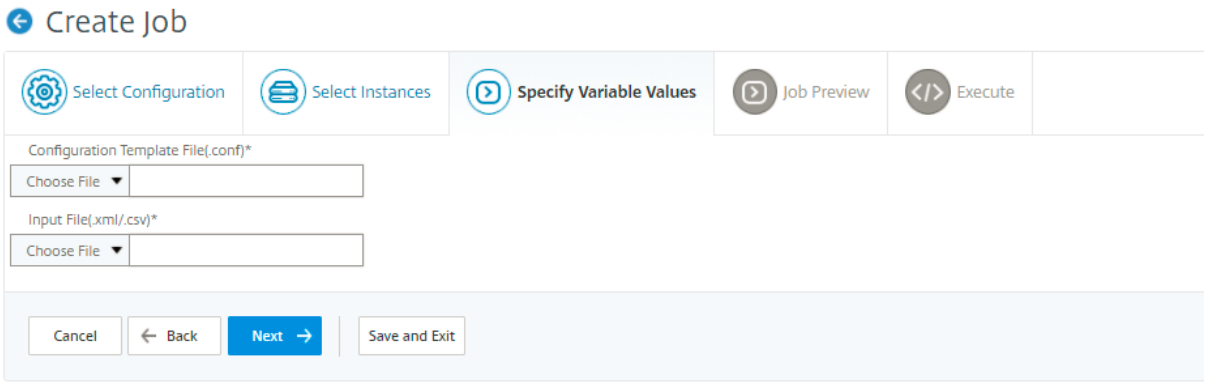
Eine Beispiel-XML-Datei wird hier für Ihre Verwendung bereitgestellt. Stellen Sie sicher, dass die xml-Dateien die Details enthalten, die den von Ihnen verwendeten ADC-Instanzen entsprechen.

```
<?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.

-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters
   and value.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence in
   the execution.

-  name. This attribute represents the IP Address of the instance.
    Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>.
   Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within
   the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
   names are case sensitive.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>

<!-- HA PAIR-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```

10. Klicken Sie auf **Weiter**.



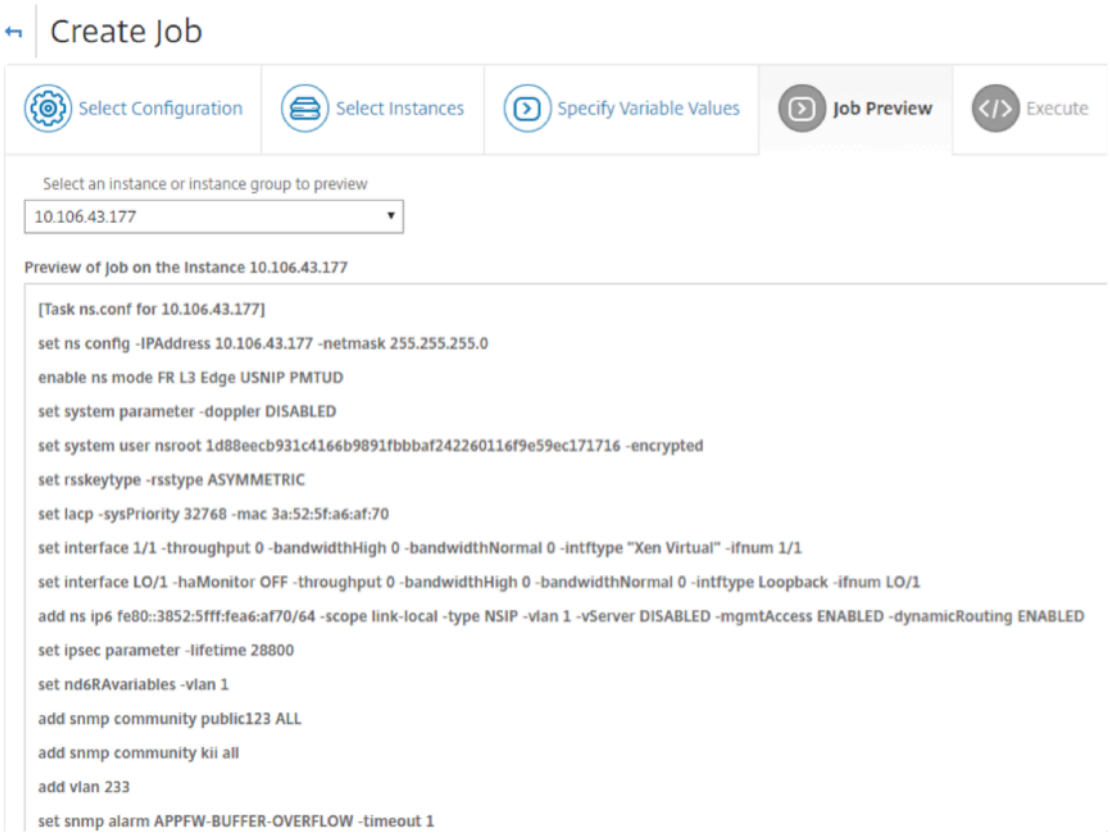
Die Eingabedateien, die die Variablenwerte enthalten, werden in den Konfigurationsaufträgen beibehalten (mit demselben Dateinamen). Sie können diese Eingabedateien anzeigen und bearbeiten, die Sie früher beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben.

Um die ausgeführten Konfigurationsaufträge 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 Konfigurationsjobs anzuzeigen, während Sie einen Konfigurationsjob bearbeiten, navigieren Sie zu **Netzwerk > Konfigurationsjobs**, wählen Sie den Jobnamen 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**.

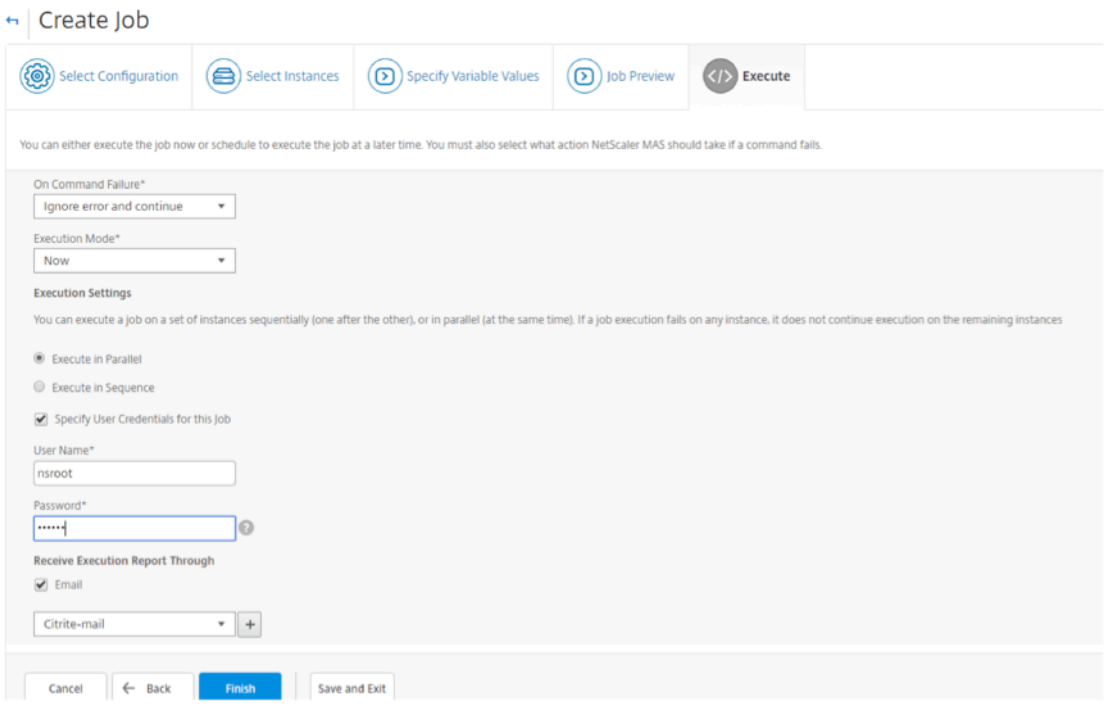
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



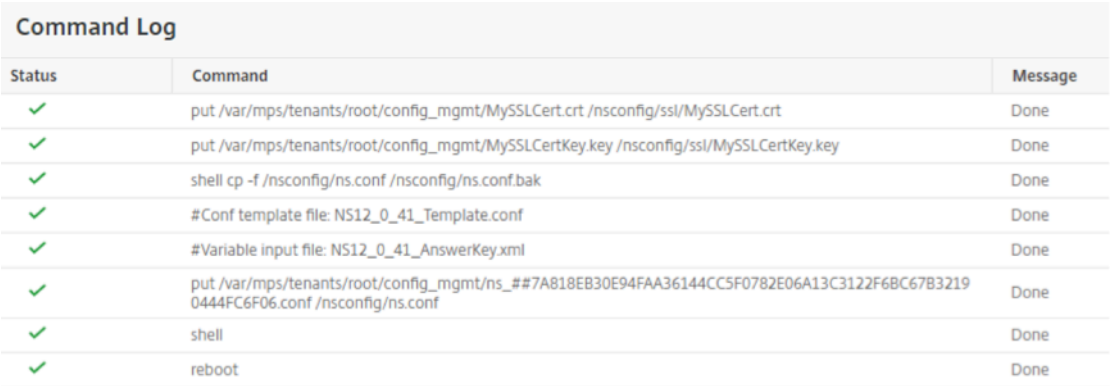
2. Auf der Registerkarte **Ausführen** können Sie wählen, ob Sie Ihren Job jetzt ausführen möchten oder ob er zu einem späteren Zeitpunkt ausgeführt werden soll. Sie können auch auswählen, welche Aktion Citrixx ADM ergreifen soll, wenn der Befehl fehlschlägt.

   Sie können auch festlegen, dass autorisierte Benutzer Jobs auf Ihren verwalteten Instances ausführen dürfen, und Sie können wählen, ob eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details gesendet werden soll.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nachdem Sie Ihren Job ausgeführt haben, können Sie die Jobdetails sehen, indem Sie zu**Networks** >**Configuration Jobs** navigieren und den Job auswählen, den Sie gerade konfiguriert haben. Klicken Sie auf**Details** und dann auf**Ausführungsübersicht**, um die Details Ihres Jobs zu sehen. Klicken Sie auf die Instanz, um die **Befehlsprotokolle** anzuzeigen und die Befehle zu sehen, die für den Job ausgeführt wurden.



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. Stellen Sie vor dem Upgrade einer Instanz sicher, dass Sie

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

die richtigen Build- und Dokumentationsdateien in die NetScaler ADC-Instanzen hochgeladen haben. Sie müssen das Lizenzierungsframework und die Lizenztypen kennen, bevor Sie eine Instanz aktualisieren.

Wenn Sie die Citrix ADC Instanz durch Erstellen einer Wartungsaufgabe aktualisieren, können Sie Folgendes tun:

- Führen Sie eine Überprüfung vor der Validierung der Instanzen durch, die aktualisiert werden. Die Vorvalidierungsprüfung besteht aus folgenden Prüfungen:
    1. Überprüfen Sie, ob vorhandene Anpassungen für Citrix ADC Instanzen vorhanden sind, und löschen Sie die Anpassungen. Sie können alle Anpassungen nach Abschluss des Upgradevorgangs erneut anwenden.
    2. Überprüfen Sie die Datenträgerverwendung von Citrix ADC Instanzen. Wenn die Datenträgerauslastung mehr als 80% beträgt, bereinigen Sie den Speicherplatz.
    3. Suchen Sie nach Hardwareproblemen von NetScaler ADC Instanzen.
- Führen Sie das NetScaler ADC HA-Paar-Upgrade in zwei Stufen durch.
    1. Führen Sie den Upgrade-Task sofort auf einem Knoten aus, oder Sie können dies sogar für einen späteren Zeitpunkt planen.
    2. Planen Sie das Upgrade für den anderen Knoten später. Sie muss geplant werden, nachdem der anfängliche Knoten aktualisiert wurde.

Beachten Sie beim Upgrade eines Citrix ADC HA-Paares Folgendes:

- Derzeit wird der zweite Knoten des HA-Paares zuerst aktualisiert, und dann wird das Upgrade für den ersten Knoten geplant, später durchgeführt werden.
- Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
- Nach dem Upgrade beider Knoten wird eine Fehlermeldung im Ausführungsverlauf angezeigt (die angibt, dass HA-Synchronisierung nicht aktiviert ist), wenn sich die Knoten im HA-Paar auf verschiedenen Builds oder Versionen befinden.

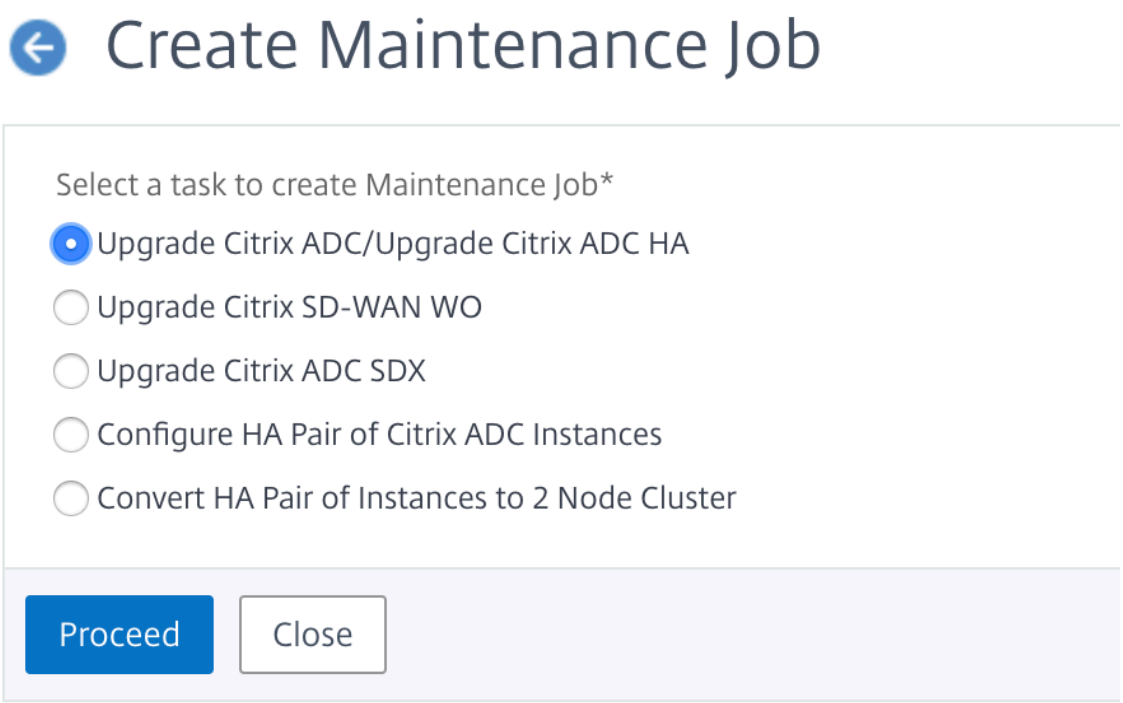
So erstellen Sie eine Wartungsaufgabe zum Aktualisieren Ihrer NetScaler ADC-Instanz:

> **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 zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**.

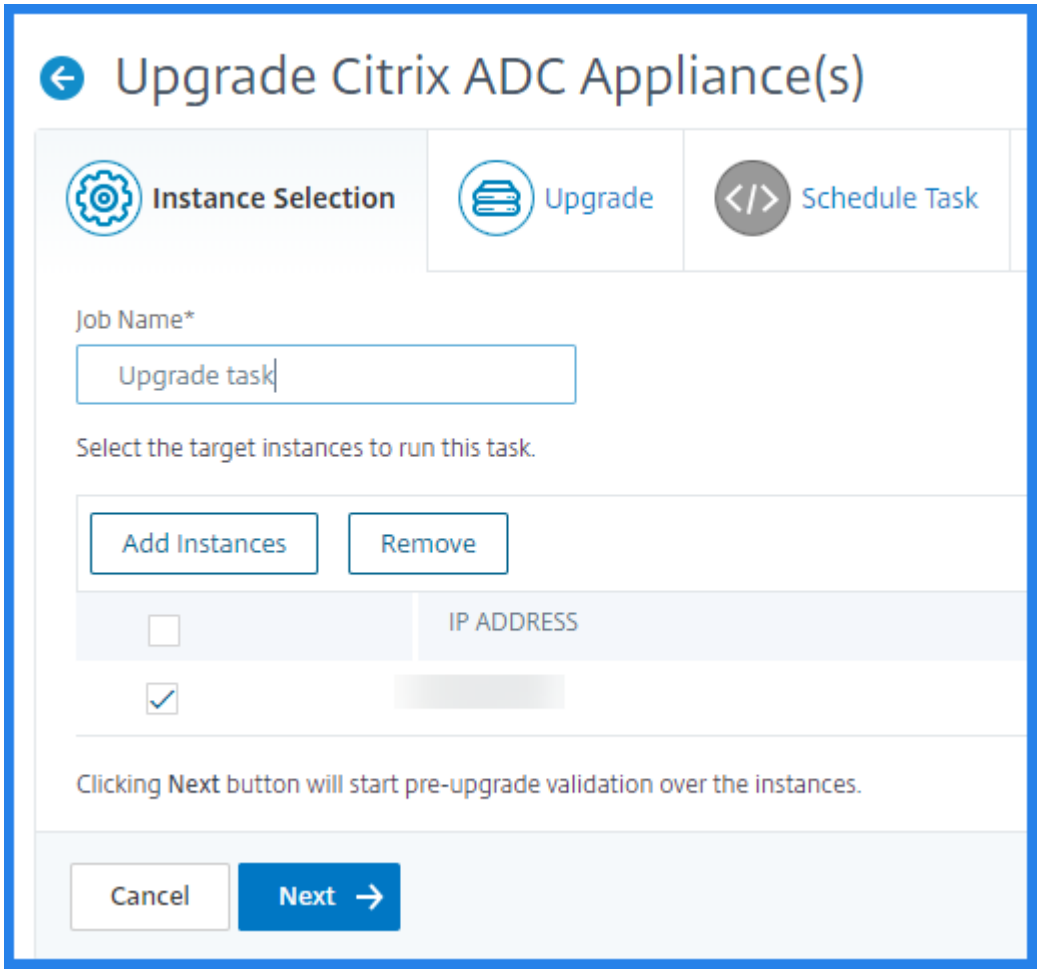
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Klicken Sie auf der Seite Wartungsaufträge auf **Job erstellen**.
3. Wählen Sie auf der Seite Wartungsauftrag erstellen **NetScaler ADC aktualisieren/NetScaler ADC HA aktualisieren** und klicken Sie auf **Fortfahren**.



4. Geben Sie auf einer oder mehreren NetScaler ADC Appliance (en) aktualisieren auf der Registerkarte **Instanzauswahl** den **Auftragsnamen** an und klicken Sie auf **Instanzen hinzufügen.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Wählen Sie die Zielinstanzen oder Instanzgruppen aus, die Sie aktualisieren möchten.

   Hinweis

   - Um NetScaler ADC Instanzen im Hochverfügbarkeitsmodus zu aktualisieren, müssen Sie IP-Adressen der primären oder sekundären Instanzen auswählen. Es wird jedoch empfohlen, immer den primären Knoten für das Upgrade zu verwenden.
   - Um NetScaler ADC Instanzen im Clustermodus zu aktualisieren, wählen Sie die Cluster-IP-Adresse aus.

6. 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.

7. Wählen **Sie auf der Seite NetScaler ADC Appliance (en)aktualisieren die Registerkarte Upgrade**aus. Wählen Sie im Menü**Software-Image**entweder**Lokal**(Ihr lokaler Computer) oder**Appliance** (die Build-Datei muss in NetScaler ADM vorhanden sein).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. 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.

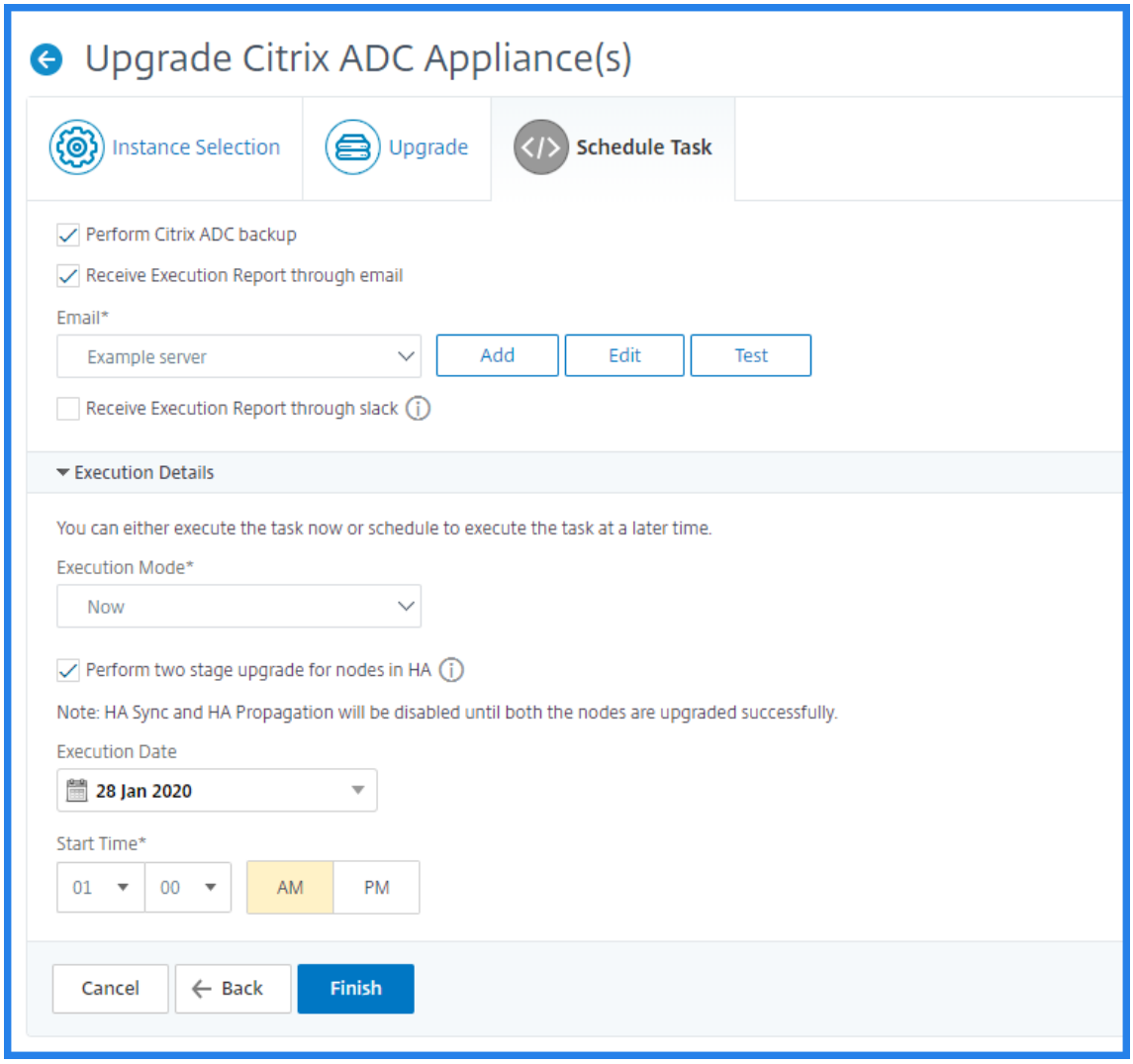
Wenn Sie nicht mit Instanzen fortfahren möchten, die die Überprüfung vor der Validierung fehlgeschlagen haben, können Sie die Instanzen entfernen. Um die Instanzen zu entfernen, wählen Sie die Instanzen aus, und klicken Sie auf **Löschen**.

1. Klicken Sie auf **Weiter**.

   > **Hinweis**
   >
   > Es wird dringend empfohlen, den Upgrade-Prozess fortzusetzen, nur wenn die Überprüfung vor dem Upgrade für die NetScaler ADC Instanzen bestanden ist.

2. Auf der Registerkarte **Task planen** können Sie auch Ausführungsdetails festlegen, in denen Sie den Aktualisierungsprozess jetzt durchführen oder ihn für ein späteres Datum planen können.
3. Sie können E-Mail-Benachrichtigungen aktivieren, um den Ausführungsbericht zum Aktualisieren von NetScaler ADC-Instanzen zu erhalten. Klicken Sie auf das Kontrollkästchen **Ausführungsbericht per E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren. So erstellen Sie eine E-Mail-Verteilerliste:
   - Wählen Sie das Pluszeichen (**+**), um die E-Mail-Verteilerliste zu erstellen.
   - 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 werden soll. Fügen Sie im Feld **Von** die E-Mail-Adresse hinzu, von der Nachrichten gesendet werden sollen. Fügen Sie im Feld **An** 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.
4. Auf der Registerkarte **Task planen** können Sie auch das zweistufige Upgrade für Knoten in HA durchführen. Sie können das Upgrade entweder sofort durchführen oder einen Zeitpunkt festlegen, zu dem die Knoten nacheinander aktualisiert werden. Synchronisation und Weitergabe der Knoten werden deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-Instanzen angewendet werden können. Beim Erstellen einer Überwachungsvorlage können Sie zuvor gespeicherte Konfigurationsvorlagen per Drag & Drop in das Feld Befehle ziehen und die Vorlage entsprechend Ihren Anforderungen bearbeiten. Anschließend können Sie die Überwachungsvorlage auf bestimmte NetScaler-Instanzen anwenden. NetScaler ADM vergleicht diese Instanzen mit der Überwachungsvorlage und meldet etwaige Abweichung. Dieser Prozess hilft Ihnen, Fehler zu erkennen und rechtzeitig

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

zu beheben.

Sie können Konfigurationsvorlagen erstellen, während Sie einen neuen Job 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

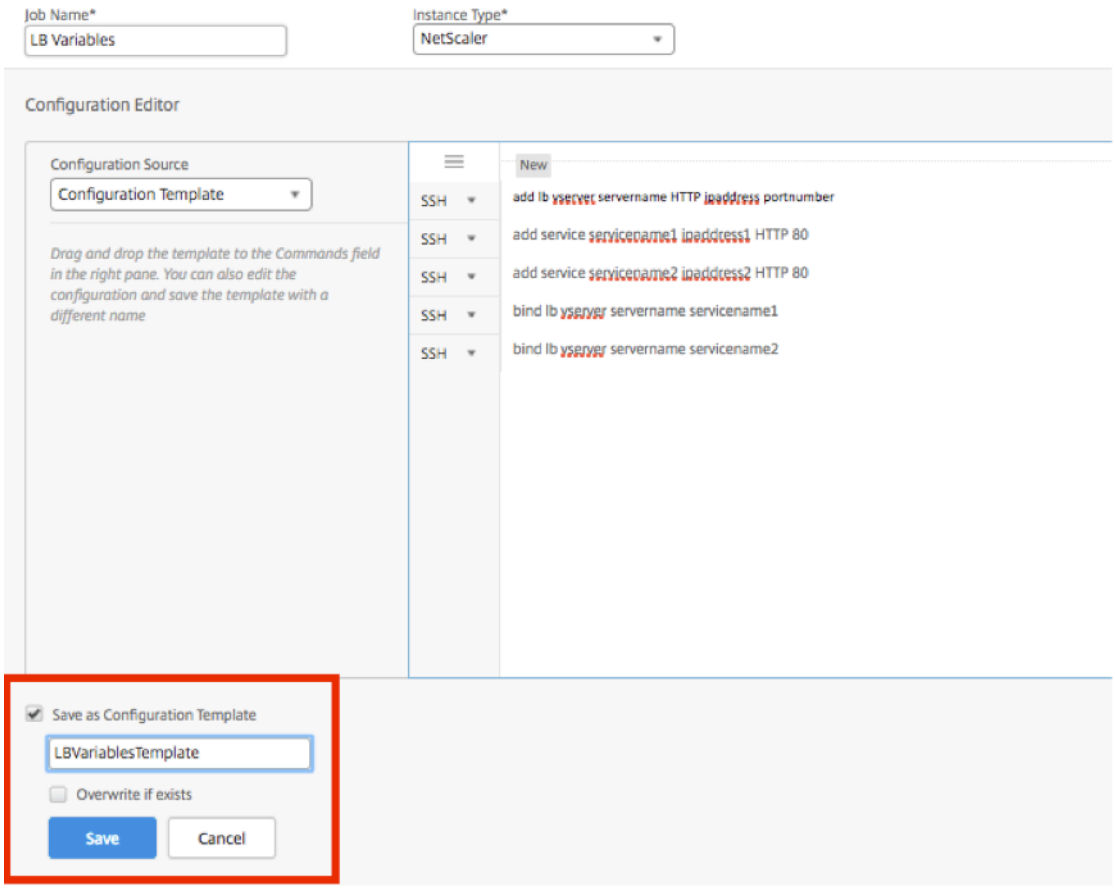
bind lb vserver **servername servicename1**

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 ein. Sie können andere Vorlagen mit demselben Namen überschreiben.
5. Klicken Sie auf **Speichern**.

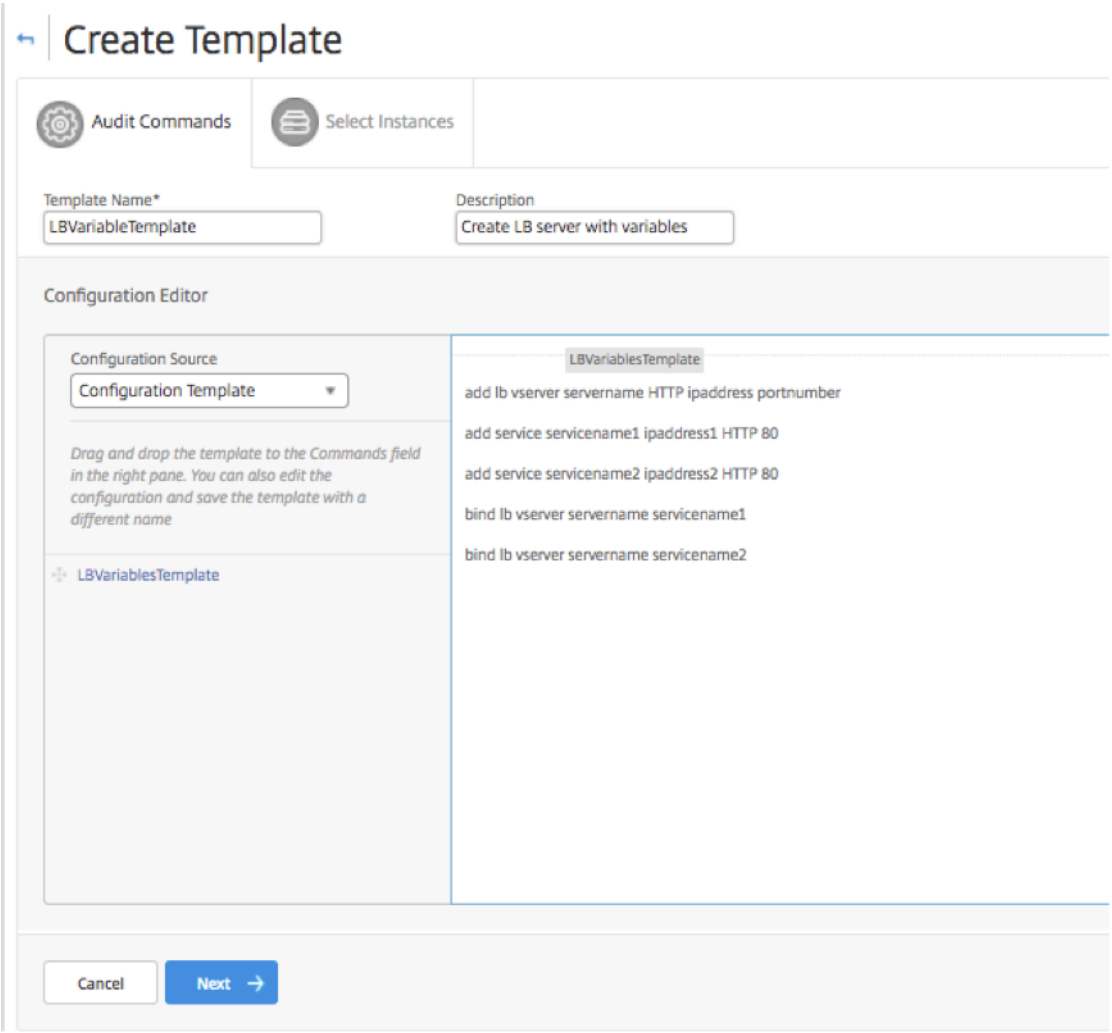
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 aus der Liste der **Konfigurationsquellen** die Option **Konfigurationsvorlage**aus, und ziehen Sie die Vorlage dann per Drag & Drop in das Feld Befehle im rechten Bereich. 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-Instanz oder -Instanzen hochzuladen oder zu übertragen.

> **Hinweis** Die Datei wird auf Citrix ADM hochgeladen und später in die ausgewählten NetScaler-Instanzen kopiert (abgelegt). Die hochgeladene Datei wird in NetScaler ADM gespeichert und nur gelöscht, wenn der Auftrag gelöscht wird. Dies ist für Jobs erforderlich, die für die Ausführung zu einem späteren Zeitpunkt geplant sind.

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 Jobs unterschiedliche Dateien für denselben Satz von NetScaler-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 Konfigurationsjob erstellen möchten, der eine auf Ihrem lokalen System gespeicherte SSL-Zertifikatsdatei auf mehrere NetScaler-Instanzen kopiert, können Sie einen „put“-Befehl hinzufügen, der eine Variable anstelle des Namens einer bestimmten Datei verwendet, und den Variablentyp als „Datei“definieren.

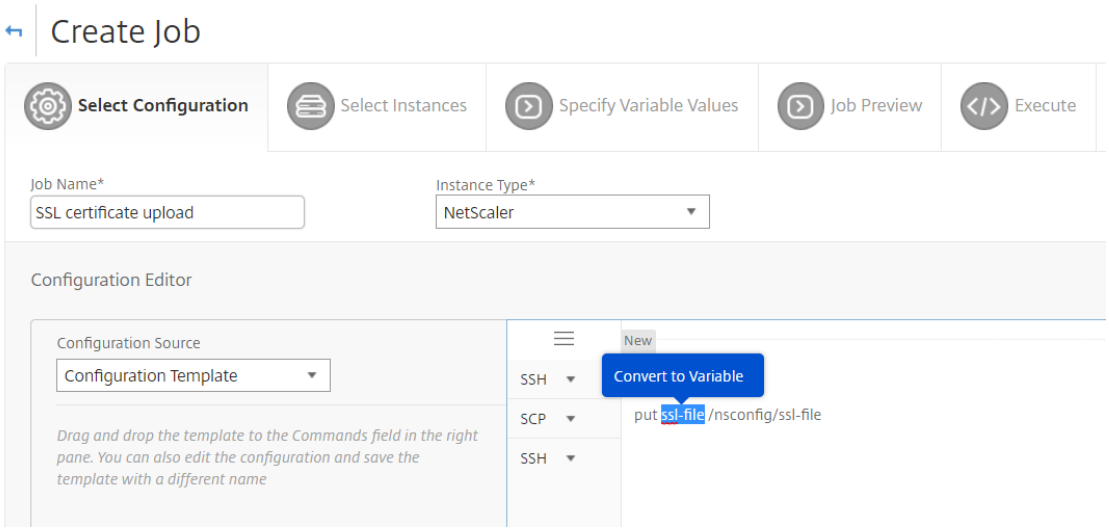
   ```
   1 put ssl-file /nsconfig/ssl-file
   2 <!--NeedCopy-->
   ```

   In diesem Beispiel wird

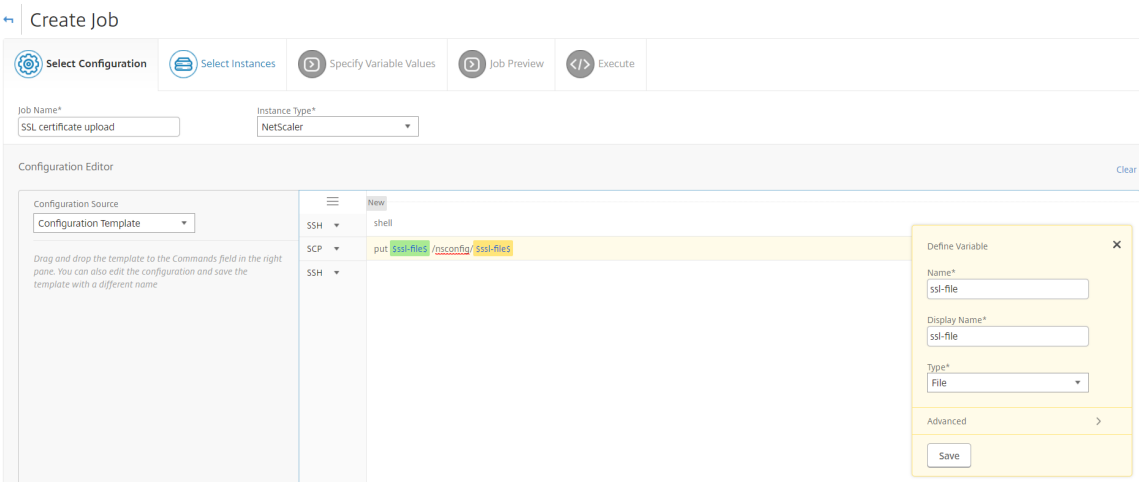
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ssl-file —Dies ist der Name der Datei, die in die NetScaler-Instanz hochgeladen werden muss.
- /nsconfig/ssl-file - Dies ist der Zielordner auf der Instanz, in der die ssl-Datei nach der Ausführung der Aufgabe abgelegt wird.

4. Wählen Sie in dem Befehl, den Sie gerade eingegeben haben, den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann auf In**Variable konvertieren**, wie in der folgenden Abbildung dargestellt.

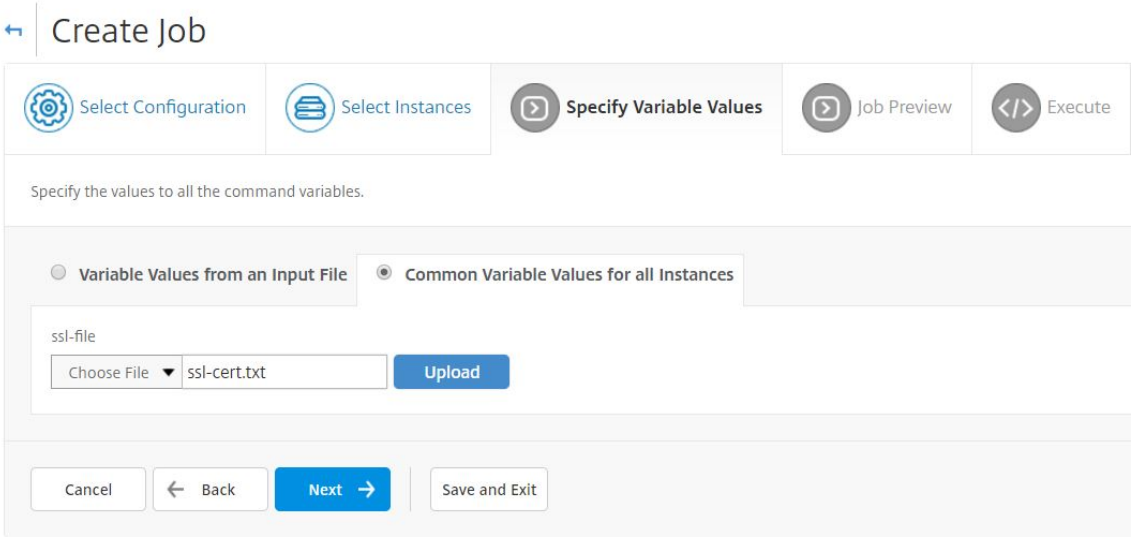


5. Stellen Sie sicher, dass der Dateiname von Dollarzeichen eingeschlossen wurde (was darauf hinweist, dass es sich jetzt um eine Variable handelt), und klicken Sie dann auf die Variable.
6. Geben Sie die Details der Variablen an, wie Name, Anzeigename und Typ.
7. Wählen **Sie in der Dropdownliste Typ** die Option **Datei**aus. Klicken Sie auf **Speichern**. Wenn Sie die Variable als Dateityp deklarieren, können Sie Dateien in NetScaler ADM hochladen.



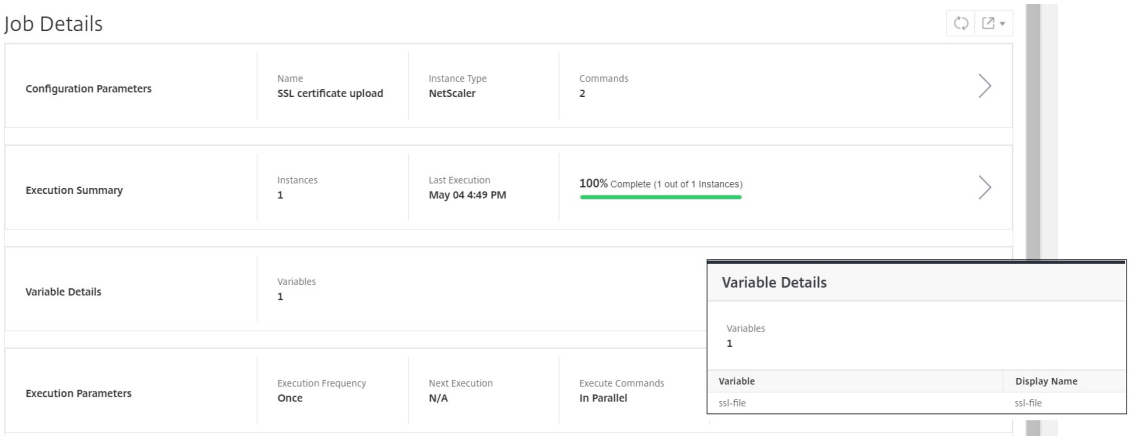
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Klicken Sie **auf** Weiter und wählen Sie die NetScaler-Instanzen aus, auf 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 zu einem späteren Zeitpunkt ausgeführt wird. Sie können auch auswählen, welche Aktion NetScaler ADM ausführen soll, 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 einsehen, indem Sie zu **Netzwerke** > **Konfigurationsaufträge** navigieren und den Job auswählen, den Sie gerade konfiguriert haben. Klicken Sie auf **Details**, und klicken Sie dann auf **Variablendetails**, um die Variablen aufzulisten, die Ihrem Auftrag hinzugefügt wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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. Dies ist nützlich, wenn Sie denselben Befehlssatz auf denselben Instanzen ausführen müssen. Manchmal kann der Auftrag einen vorübergehenden Fehler von der Serverseite auftreten, und Sie müssen den Auftrag möglicherweise erneut ausführen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

```
1  add lb vserver servername HTTP ipaddress portnumber
2
3  add service servicename1 ipaddress1 HTTP 80
4
5  add service servicename2 ipaddress2 HTTP 80
6
7  bind lb vserver servername servicename1
8
9  bind lb vserver servername servicename2
10 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

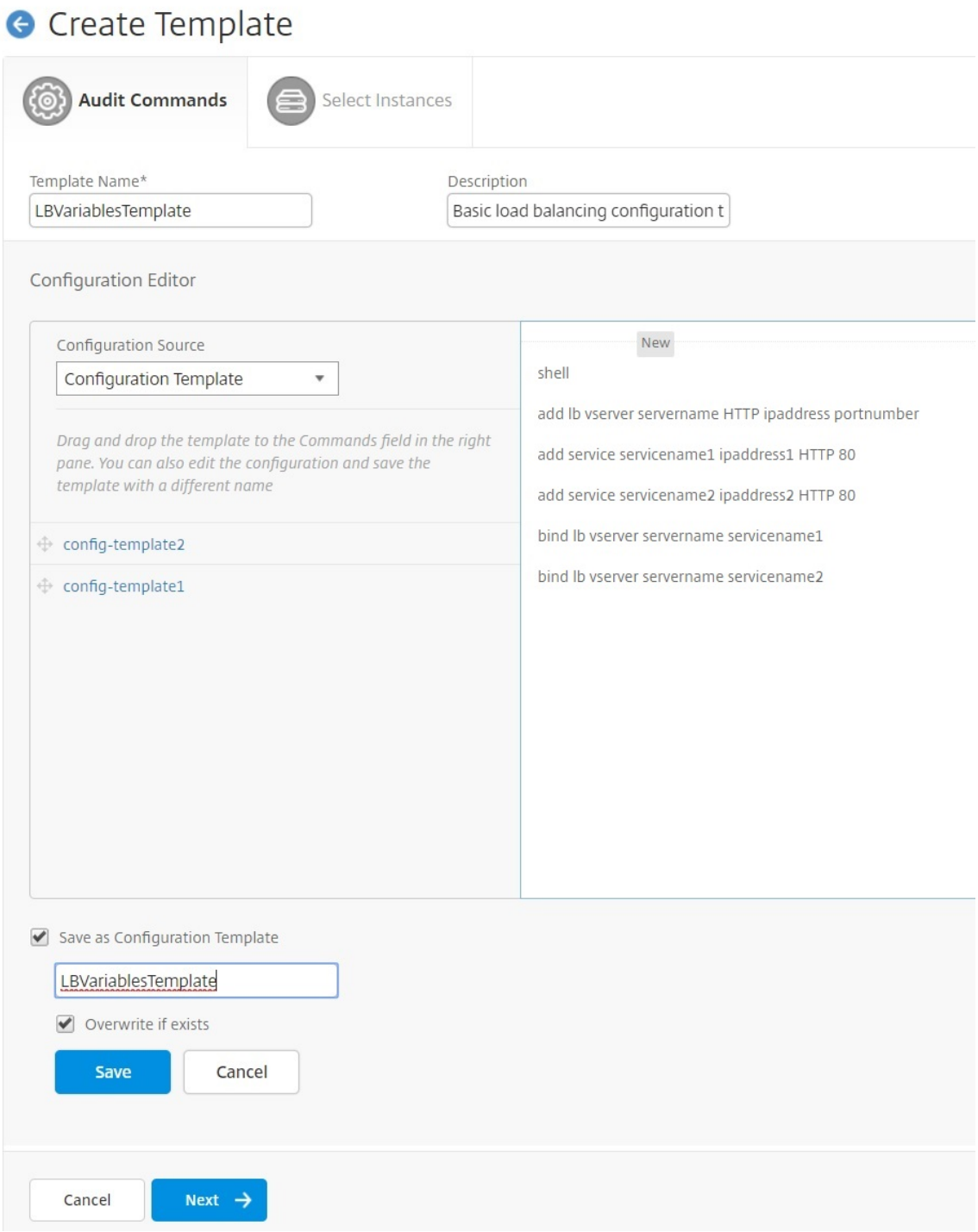
So erstellen Sie eine Überwachungsvorlage:

1. Navigieren Sie in Citrix ADM zu **Netzwerke > Configuration Audit > Audit-Vorlage**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. Sie können diese Vorlage beispielsweise als “LBVariablesTemplate” benennen. Sie können andere Vorlagen mit demselben Namen überschreiben.

   > **Hinweis:** Der Name der Prüfvorlage kann mit dem Namen der Konfigurationsvorlage identisch sein.

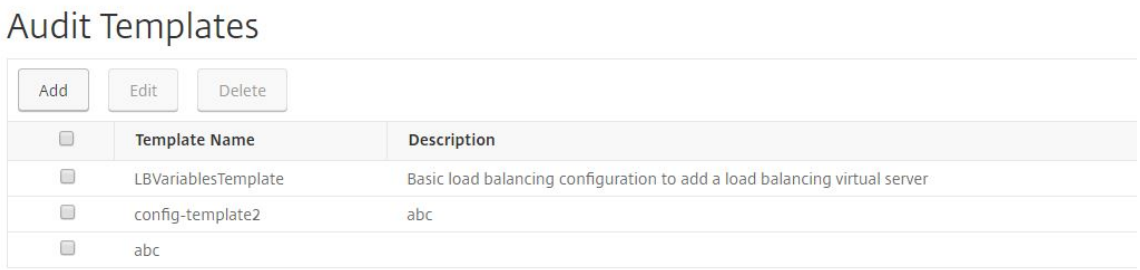
5. Klicken Sie auf **Speichern** und dann auf **Weiter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Job ein, wählen Sie den Instanztyp aus und ziehen Sie die Vorlage per Drag & Drop in den Befehlsbereich.

   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 Jobs unterschiedliche Dateien für denselben Satz von Citrix ADC-Instanzen zuweisen.

2. Wählen Sie in dem eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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“per Drag & Drop in den Befehlsbereich. 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

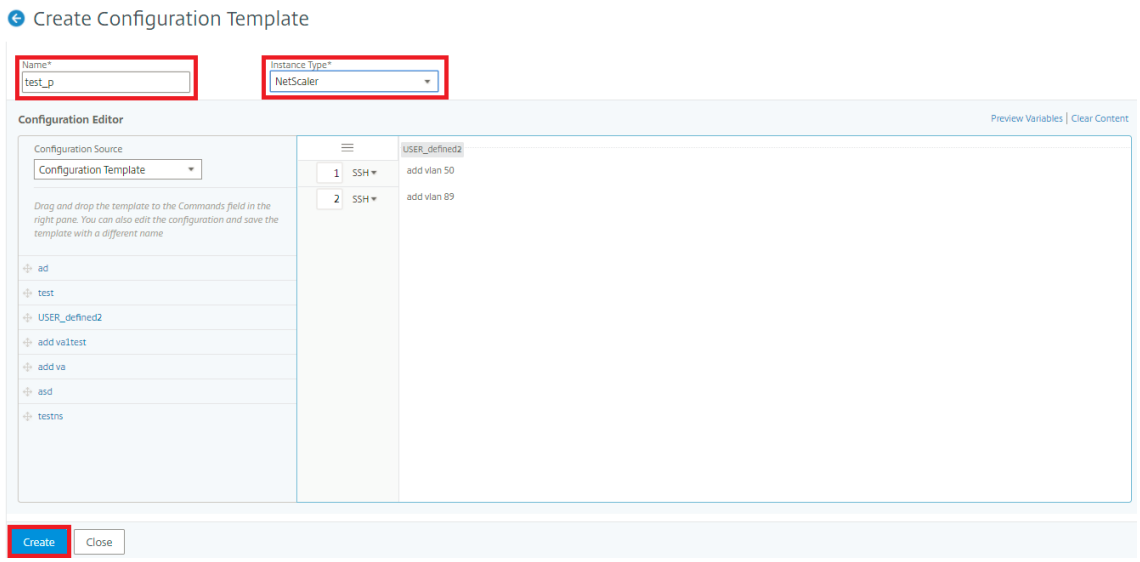
Sie können die Konfigurationsvorlagen aus jedem Citrix Application Delivery Management (ADM) exportieren. Sie können die Datei auch jederzeit in dasselbe oder ein anderes Citrix ADM importieren. Die Daten der Konfigurationsvorlagen (wie Konfigurationsbefehle, Variablendefinitionen und Parameter) gehen 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.

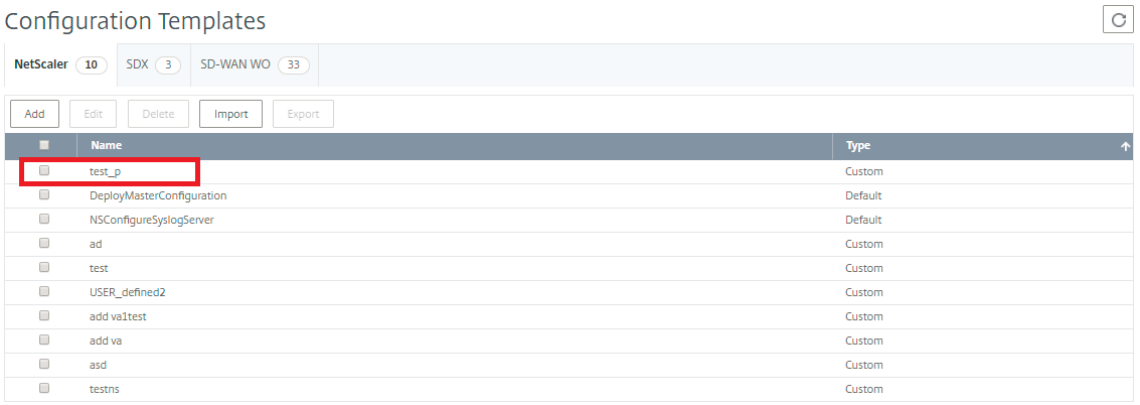
So exportieren Sie die Konfigurationsvorlagen:

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 per Drag & Drop in den Konfigurationseditor ziehen. Klicken Sie auf **Erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

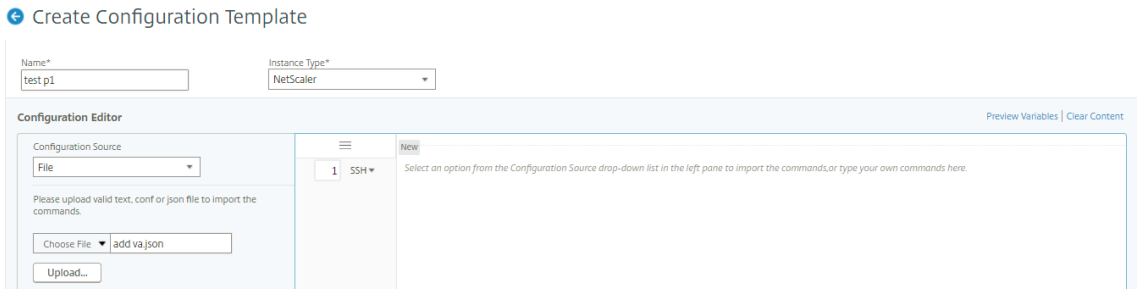
Die entsprechende Konfigurationsvorlage wird im **JSON-Format** auf Ihrem lokalen System heruntergeladen.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

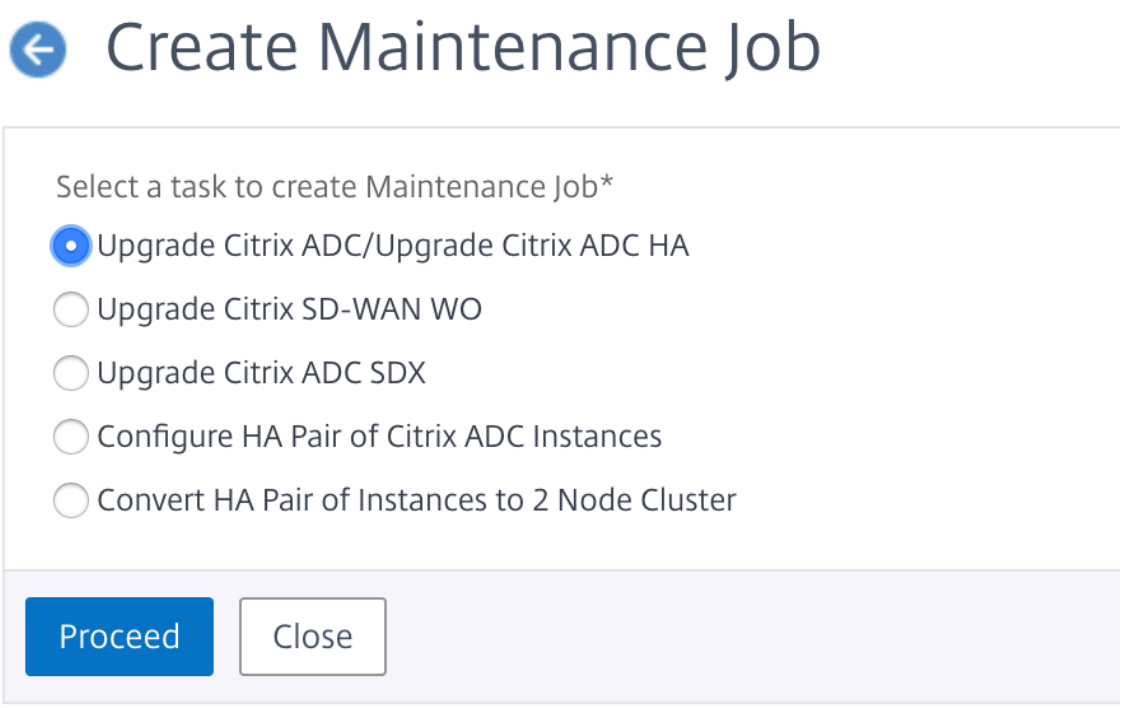
Sie können die folgenden Wartungsjobs mit Citrix ADM erstellen. Anschließend können Sie die Wartungsarbeiten an einem bestimmten Datum und zu einer bestimmten Uhrzeit planen.

- Upgrade von NetScaler ADC-Instanzen
- Citrix SD WAN-WO-Instanzen aktualisieren
- Upgrade von NetScaler ADC SDX-Instanzen
- HA-Paar der NetScaler ADC-Instanzen konfigurieren
- HA-Instanzen in Cluster mit 2 Knoten konvertieren

Upgrades der NetScaler ADC-Instanzen planen

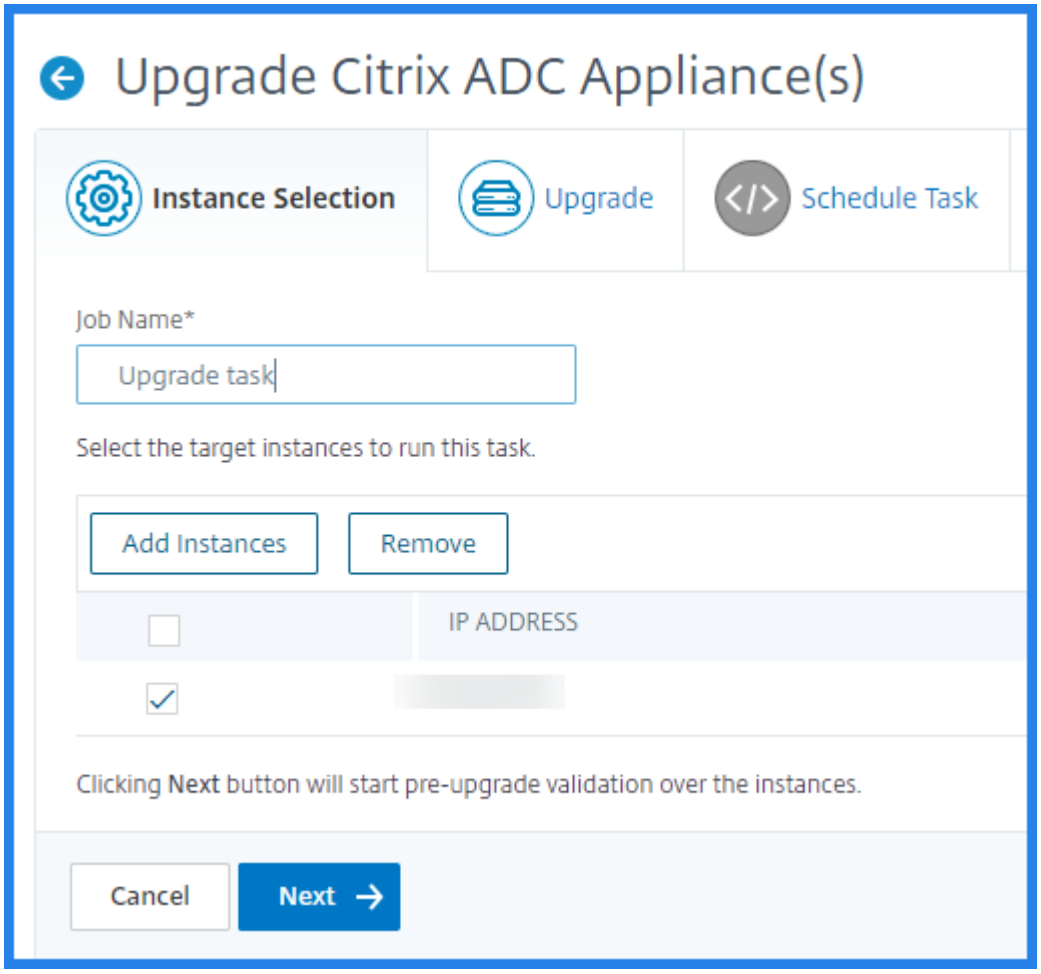
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Auftrag erstellen**.
2. Wählen Sie auf der Seite “Wartungsaufgabe erstellen”die Option **Citrix ADC/Upgrade Citrix ADC HA** aus und klicken Sie auf **Fortfahren**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



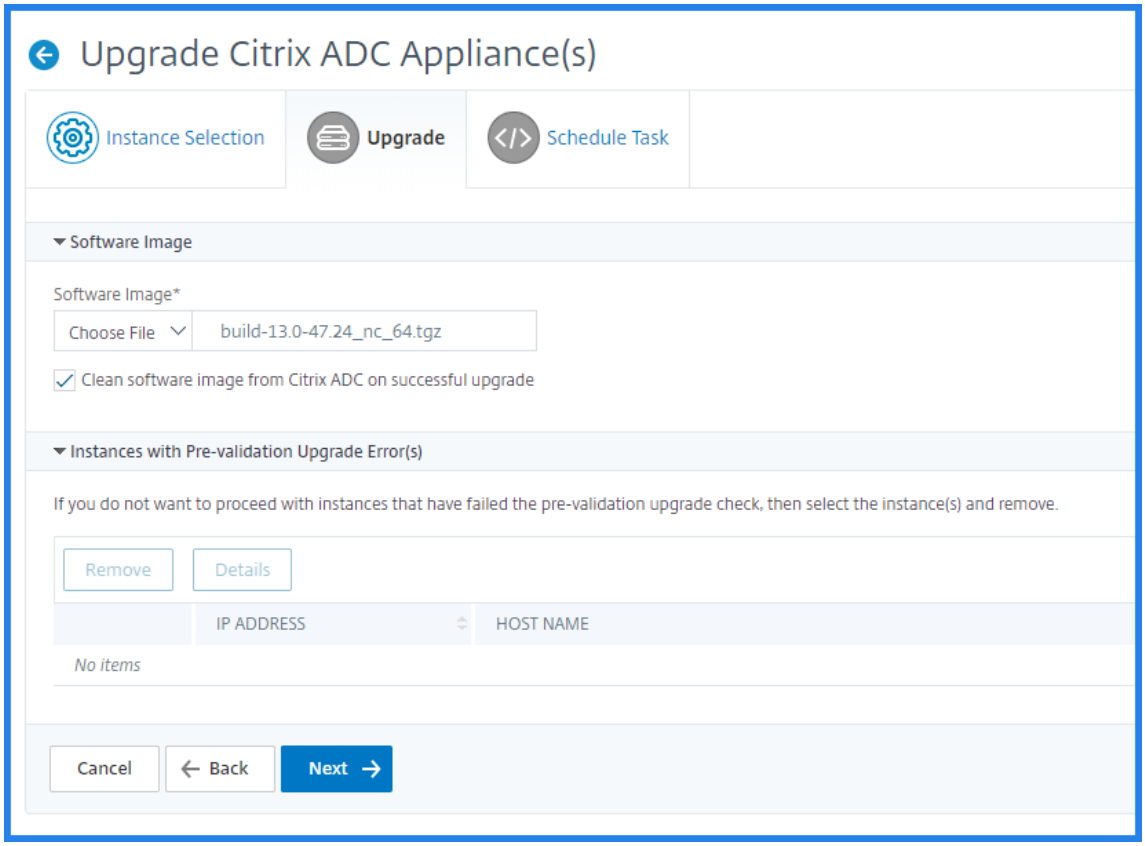
3. Fügen Sie auf der Seite "Upgrade Citrix ADC Appliance(s)"auf der Registerkarte **Instanzauswahl** die Citrix ADC-Instanzen hinzu, auf denen Sie den Upgrade-Vorgang ausführen möchten. Klicken Sie auf **Weiter**, um die Validierung vor dem Upgrade für die ausgewählten Instanzen zu starten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



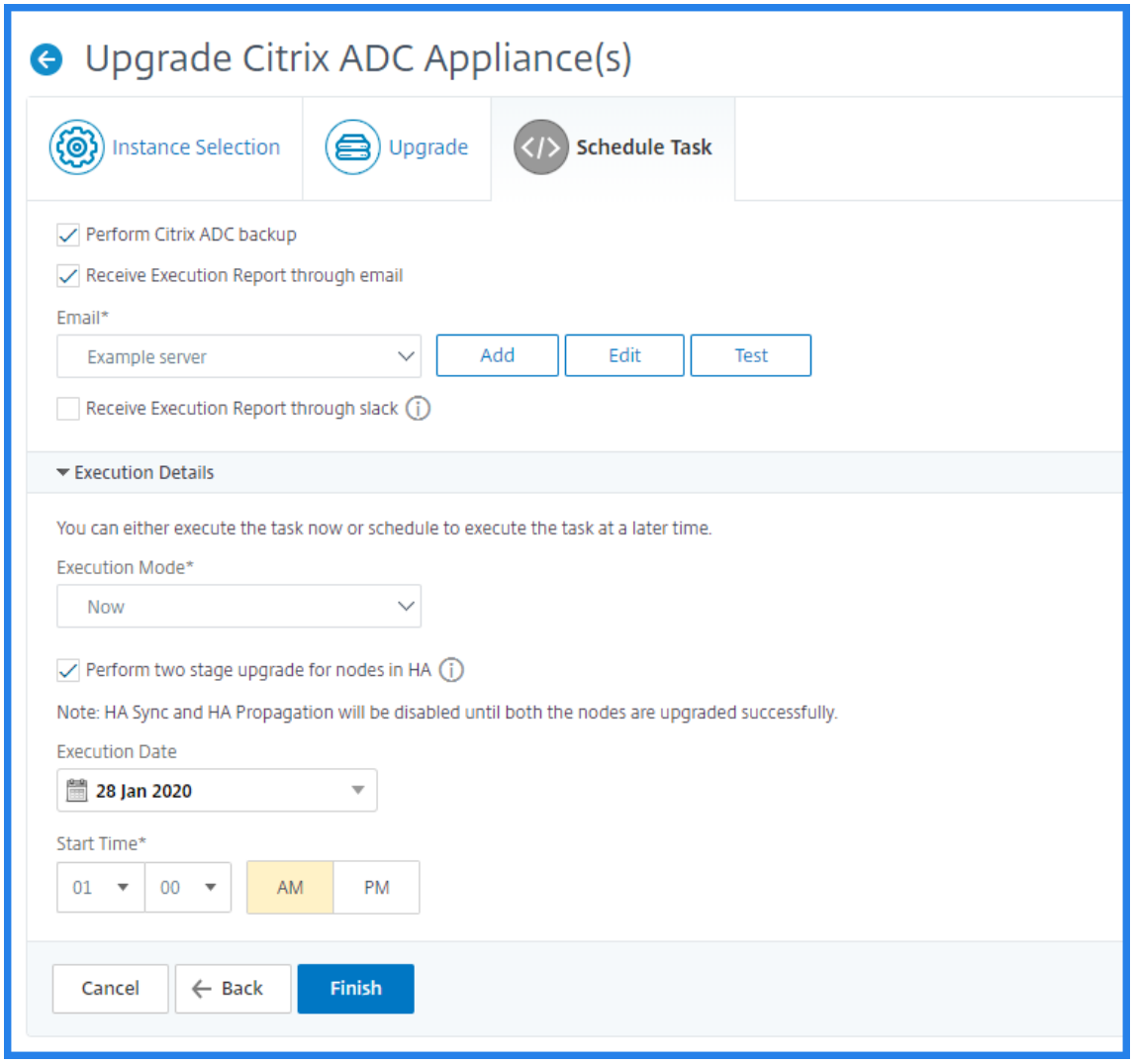
4. Wählen Sie auf der Registerkarte **Upgrade** in der Liste Software-Image entweder Lokal (Ihr lokaler Computer) oder Appliance aus (die Build-Datei muss auf der virtuellen Citrix ADM Appliance vorhanden sein).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



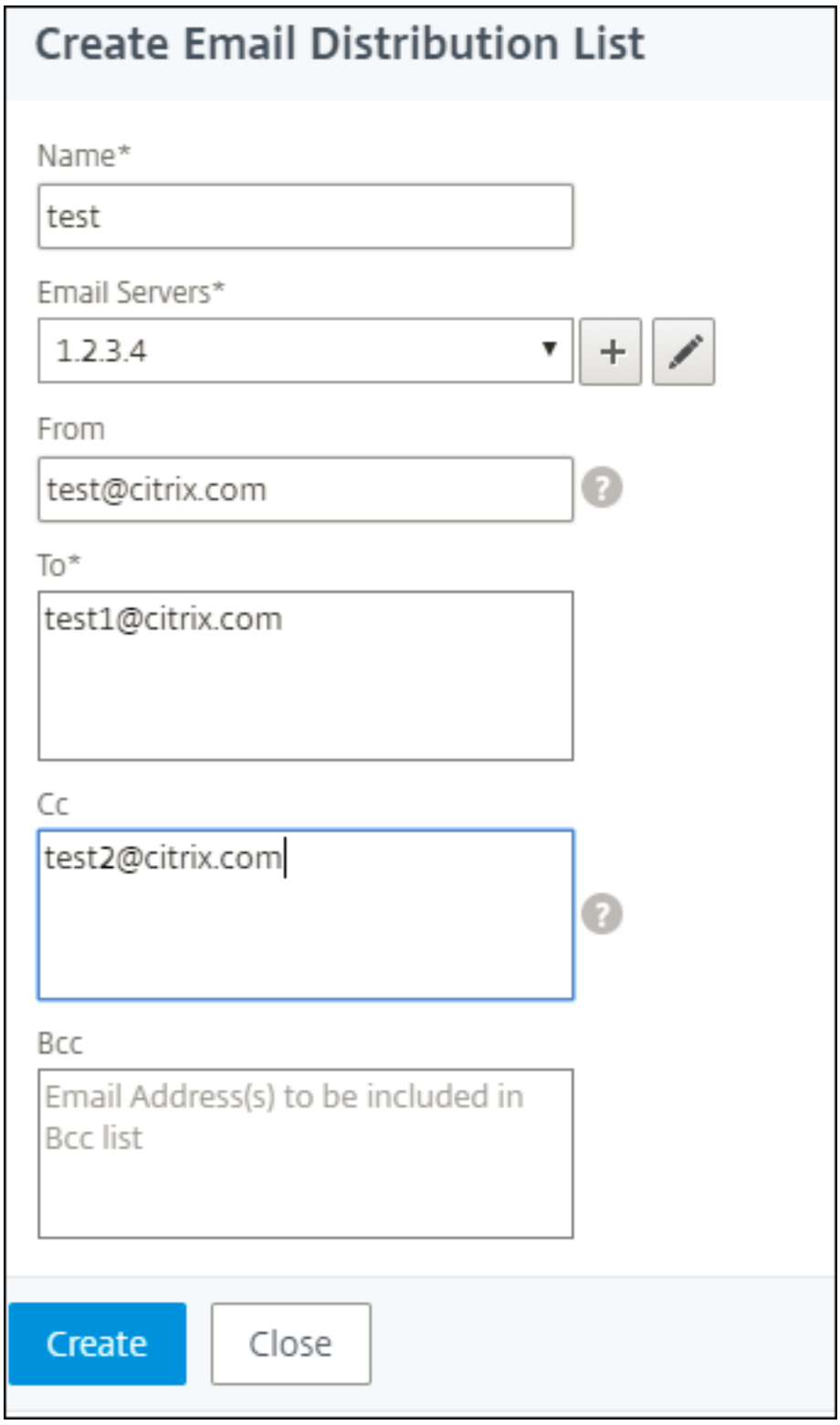
5. Sie können E-Mail-Benachrichtigungen aktivieren, um den Ausführungsbericht zum Aktualisieren von NetScaler ADC-Instanzen zu erhalten. Klicken Sie auf das Kontrollkästchen **Ausführungsbericht per E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.
6. Wählen Sie das Symbol +, um die E-Mail-Verteilerliste zu erstellen.
7. Um die Citrix ADC-Instanz jetzt zu aktualisieren, wählen Sie **Jetzt** aus der Liste Ausführungsmodus aus.
8. Um die Citrix ADC-Instanz zu einem späteren Zeitpunkt zu aktualisieren, wählen Sie **Später** aus der Liste Ausführungsmodus aus. Anschließend können Sie das Ausführungsdatum und die Startzeit für das Upgrade der Citrix ADC-Instanzen auswählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



9. 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 werden soll. Fügen Sie im Feld **Von** die E-Mail-Adresse hinzu, von der Nachrichten gesendet werden sollen. Fügen Sie im Feld **An** 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.

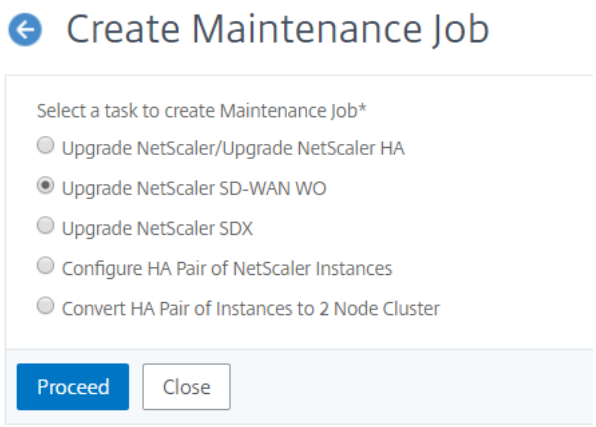
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



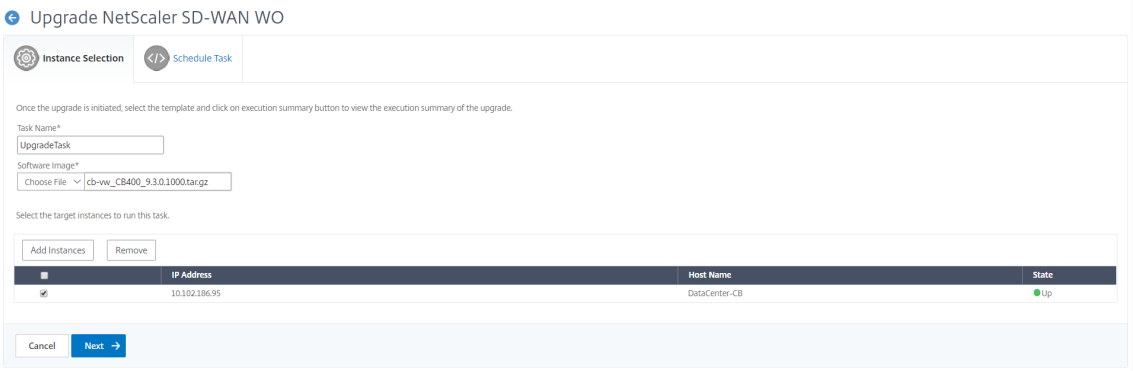
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Planen der Aktualisierung von Citrix SD-WAN WO-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 Citrix SD-WAN WO** aus, und klicken Sie auf **Weiter**.



3. Fügen Sie auf der Seite **Upgrade Citrix SD-WAN WO** auf der Registerkarte **Instanzauswahl** einen **Tasknamen** hinzu. Wählen Sie in der Liste Software-Image entweder Lokal (Ihr lokaler Computer) oder Appliance aus (die Build-Datei muss auf der virtuellen Citrix MAS-Appliance vorhanden sein). Fügen Sie die Citrix SD-WAN WO-Instanzen hinzu, auf denen Sie den Upgrade-Prozess ausführen möchten. Klicken Sie auf **Weiter**.

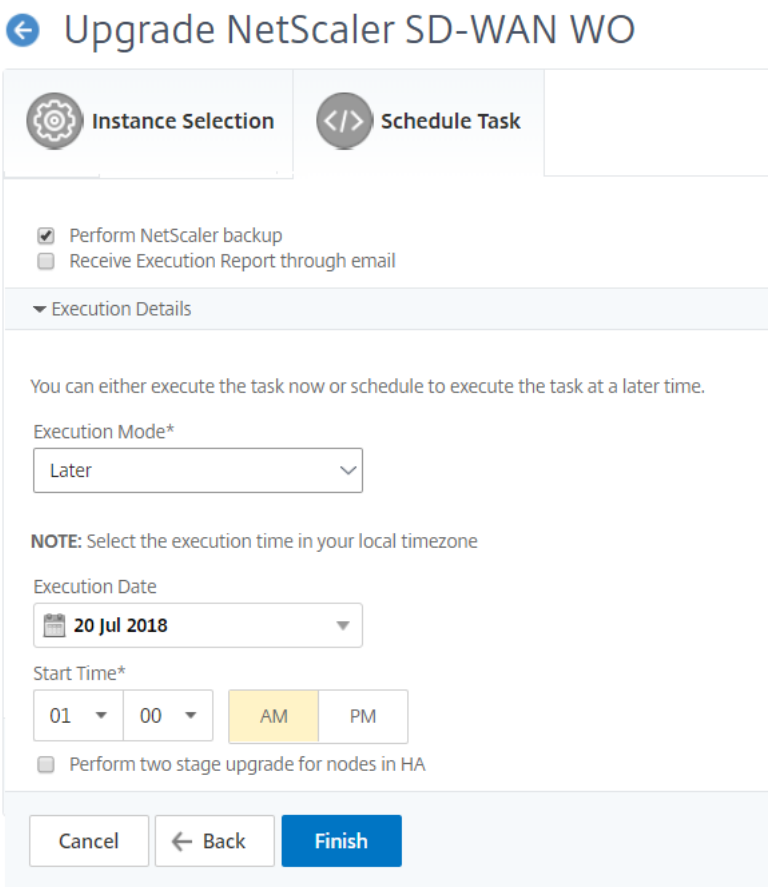


4. Um die Citrix SD-WAN WO-Instanz jetzt zu aktualisieren, wählen Sie **Jetzt** aus der Liste **Ausführungsmodus** aus. Klicken Sie auf **Fertig stellen**.
5. Um die Citrix SD-WAN WO-Instanz zu einem späteren Zeitpunkt zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Anschließend können Sie das Ausführungsdatum und die Startzeit für das Upgrade der Citrix SD-WAN WO-Instanz auswählen.
6. Sie können die E-Mail-Benachrichtigung aktivieren, um den Ausführungsbericht für das Upgrade der Citrix SD-WAN WO-Instanz zu erhalten. Klicken Sie auf das Kontrollkästchen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ausführungsbericht per E-Mail empfangen, um die E-Mail-Benachrichtigung zu aktivieren.

7. Wählen Sie das **Plus-Symbol** aus, um die E-Mail-Verteilerliste zu erstellen.



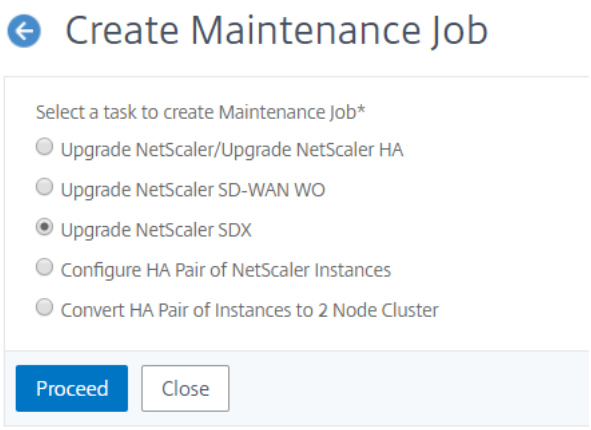
8. Geben Sie auf der Seite **E-Mail-Verteilerliste erstellen** einen Namen für die E-Mail-Verteilerliste an. Fügen Sie den SMTP-Mailserver hinzu, der zum Senden von E-Mail-Benachrichtigungen an den E-Mail-Server verwendet wird. Fügen Sie im Feld **Von** die E-Mail-Adresse hinzu, von der Nachrichten gesendet 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Wählen Sie auf der Seite **Wartungsauftrag erstellen** die Option **Upgrade NetScaler ADC SDX** aus, und klicken Sie auf **Weiter**.

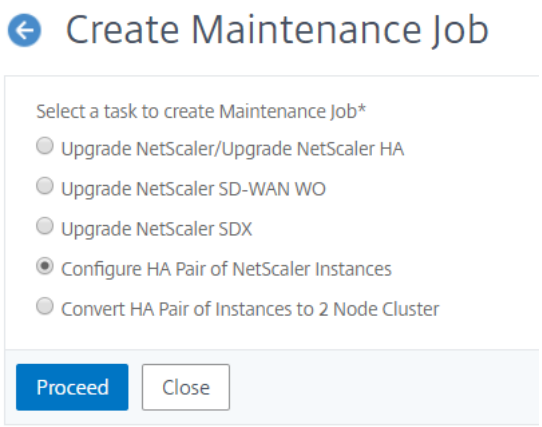


3. Fügen Sie auf der Seite **NetScaler ADC SDX-Appliance (s) aktualisieren** auf der Registerkarte **Instanzauswahl** einen **Task-Namen**hinzu. Wählen Sie in der Liste Software-Image entweder Lokal (Ihre lokale Maschine) oder Appliance (die Builddatei muss auf der virtuellen Citrix ADM Appliance vorhanden 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. Klicken Sie auf das Kontrollkästchen **Ausführungsbericht per 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** aus. 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.

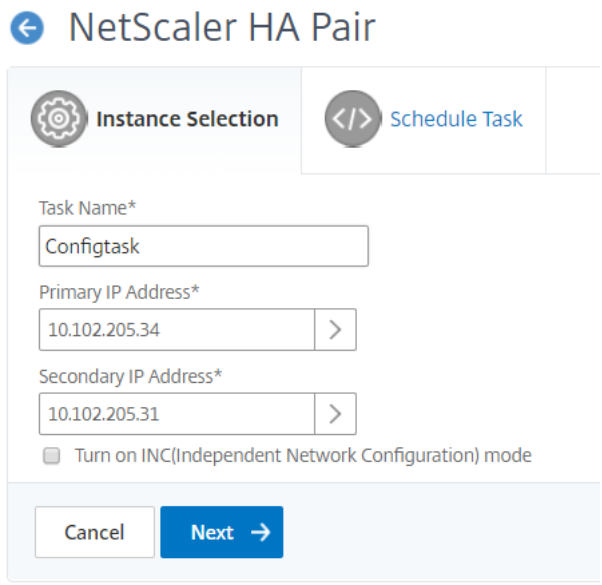
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Planen der Konfiguration von HA-Paar von NetScaler ADC 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 **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 Aus-

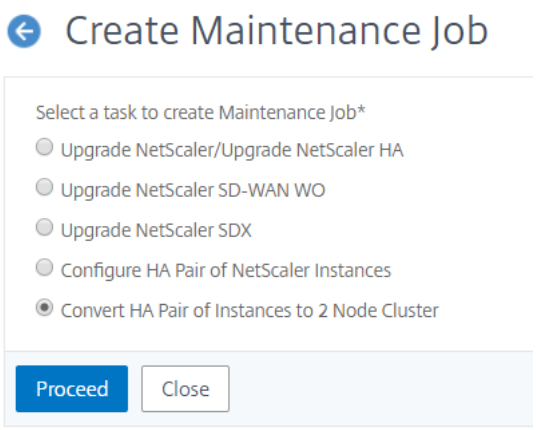
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

führungsbericht des NetScaler ADC HA-Paares zu erhalten. Klicken Sie auf das Kontrollkästchen **Ausführungsbericht per E-Mail empfangen**, um die E-Mail-Benachrichtigung zu aktivieren.

6. Um das Citrix ADC HA-Paar zu einem späteren Zeitpunkt zu konfigurieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. 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. Klicken Sie auf das Kontrollkästchen **Ausführungsbericht per 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

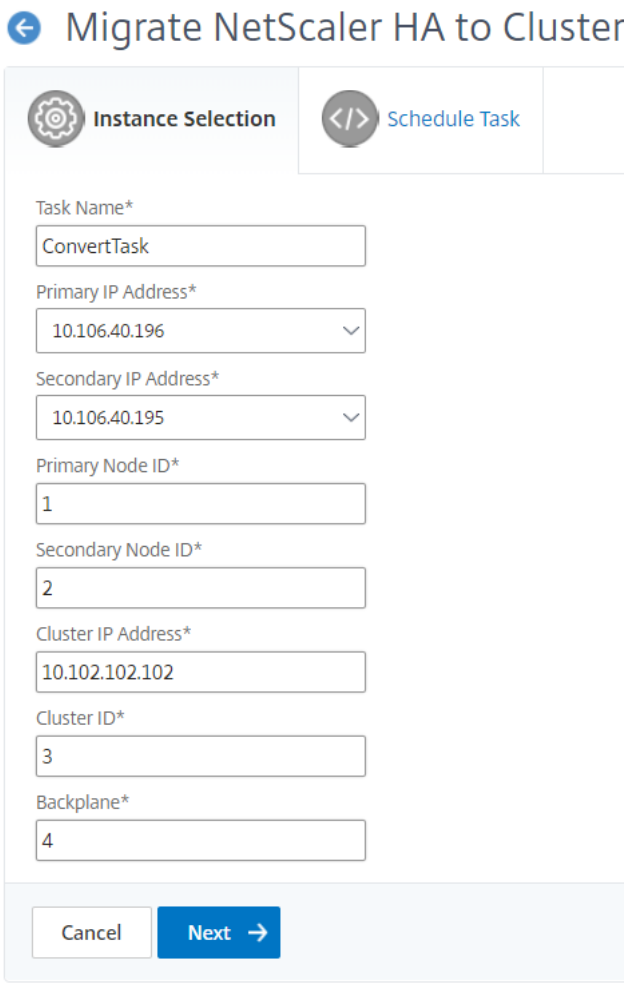
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsaufträge** > **Wartungsaufträge**. Klicken Sie auf die Schaltfläche **Auftrag erstellen**.
2. Wählen Sie auf der Seite **Wartungsauftrag erstellen** die Option **HA-Instanzen in Cluster mit 2 Knoten konvertieren** aus, und klicken Sie auf **Weiter**.



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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix ADC HA-Paar zu einem späteren Zeitpunkt zu konfigurieren, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. 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. Klicken Sie auf das Kontrollkästchen **Ausführungsbericht per 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
- So führen Sie eine Umfrage zur Konfigurationsüberprüfung von NetScaler-Instances durch

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 soll

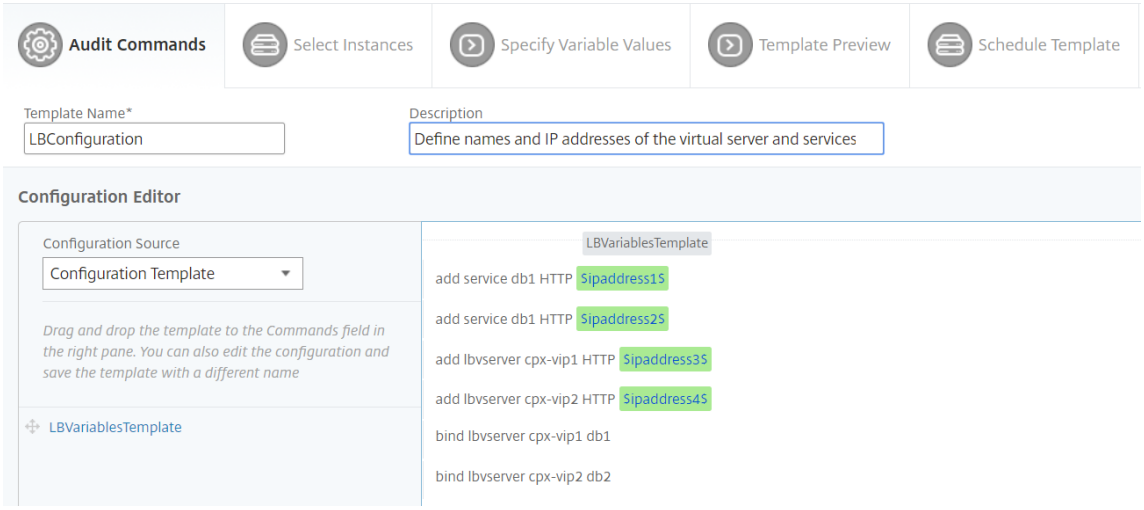
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Festlegen der Häufigkeit, mit der Citrix ADM die Vorlage ausführen soll. 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.

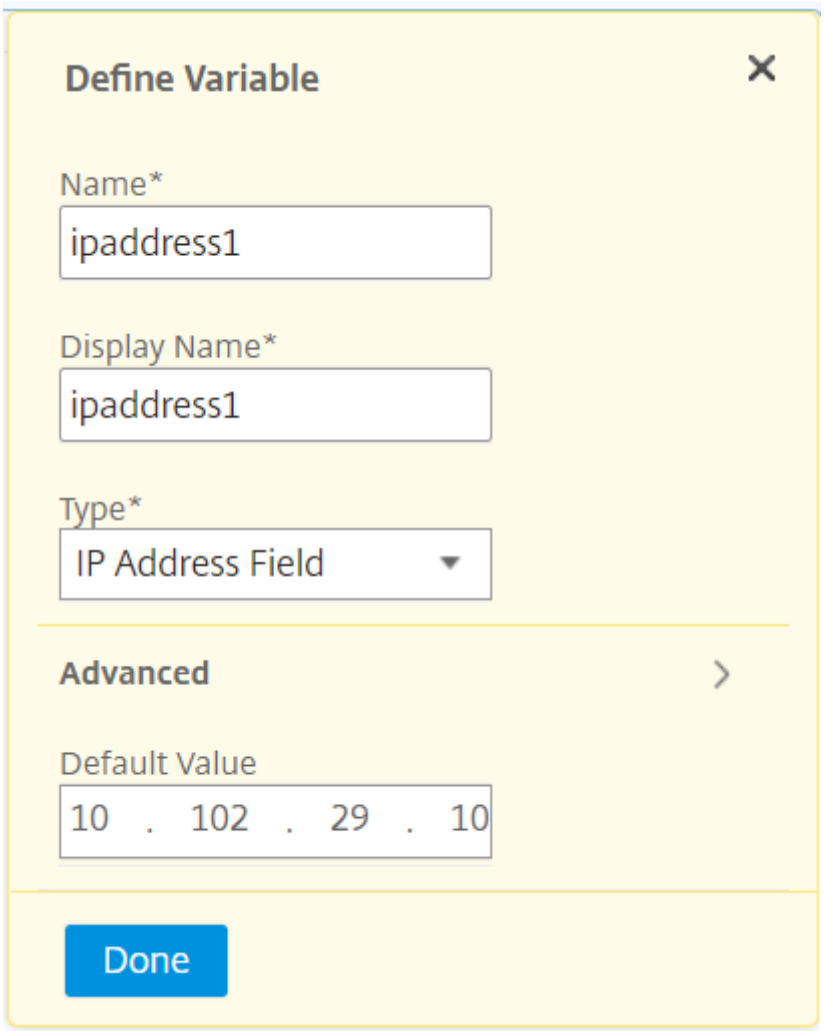
So erstellen Sie Überwachungsvorlagen:

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.

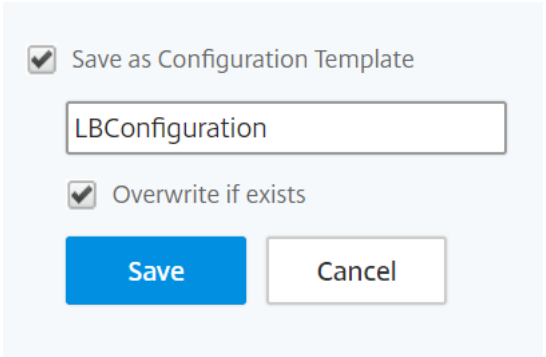


Legen Sie im Fenster **Variable definieren** die Eigenschaften für diese Variable fest: Name, Anzeigename und Typ der Variablen. Klicken Sie auf die Option**Erweitert**, wenn Sie einen Standardwert für die Variable angeben möchten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

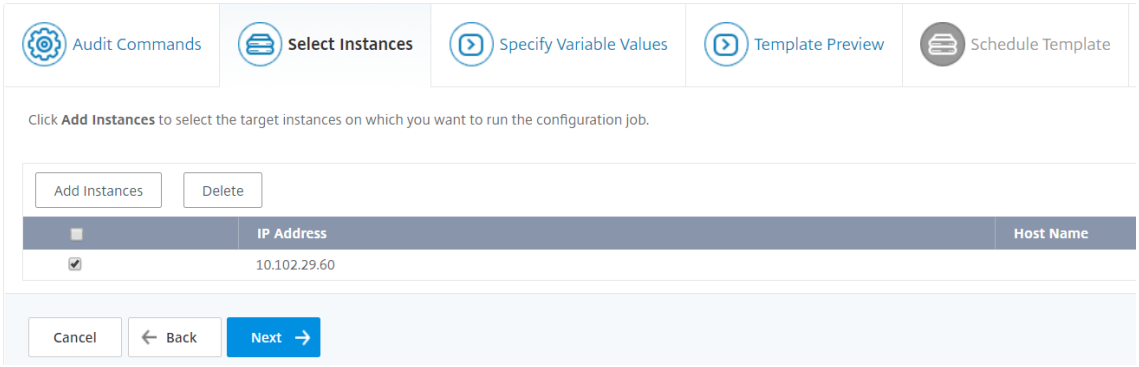


Sie können die Befehle auch als Konfigurationsvorlage speichern.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

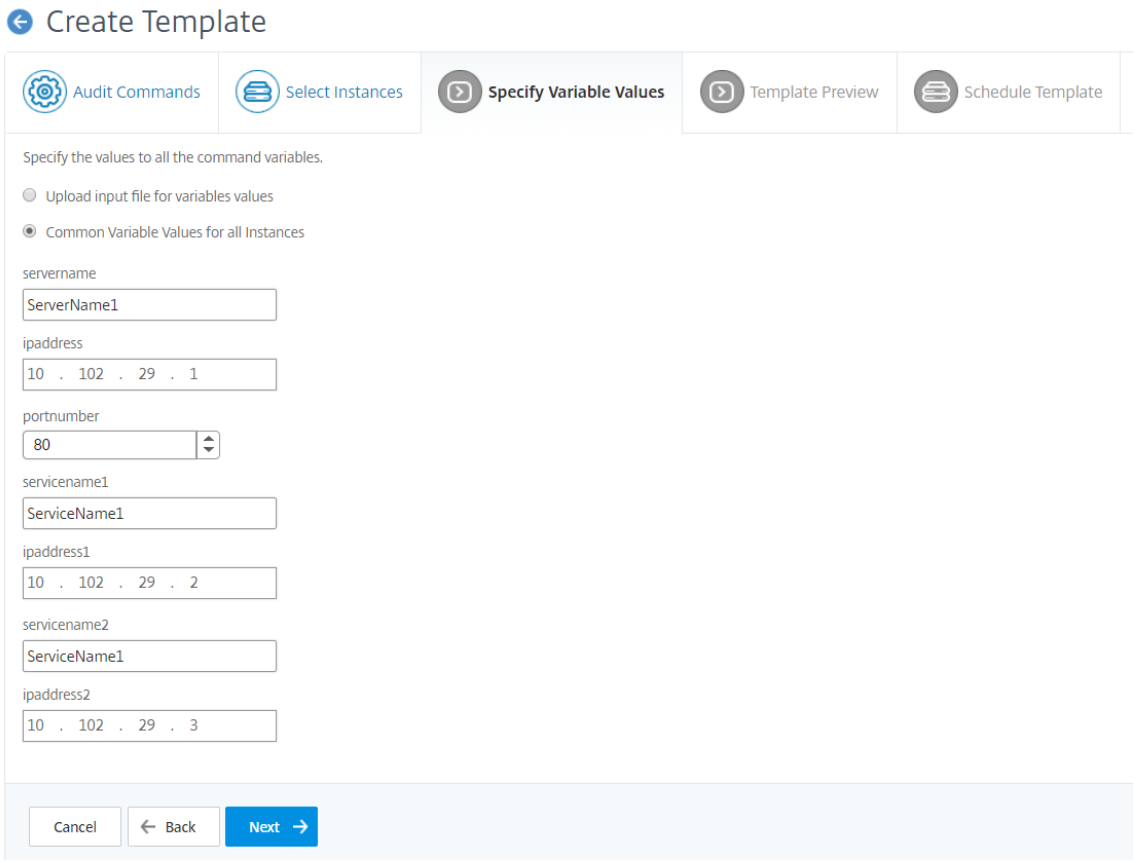


7. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:

   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.

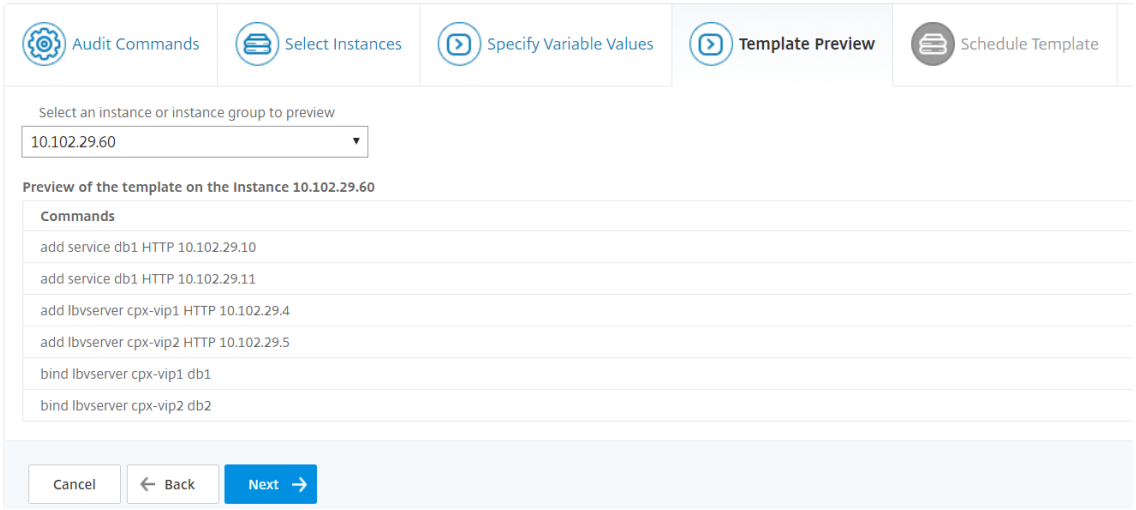
   b) Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

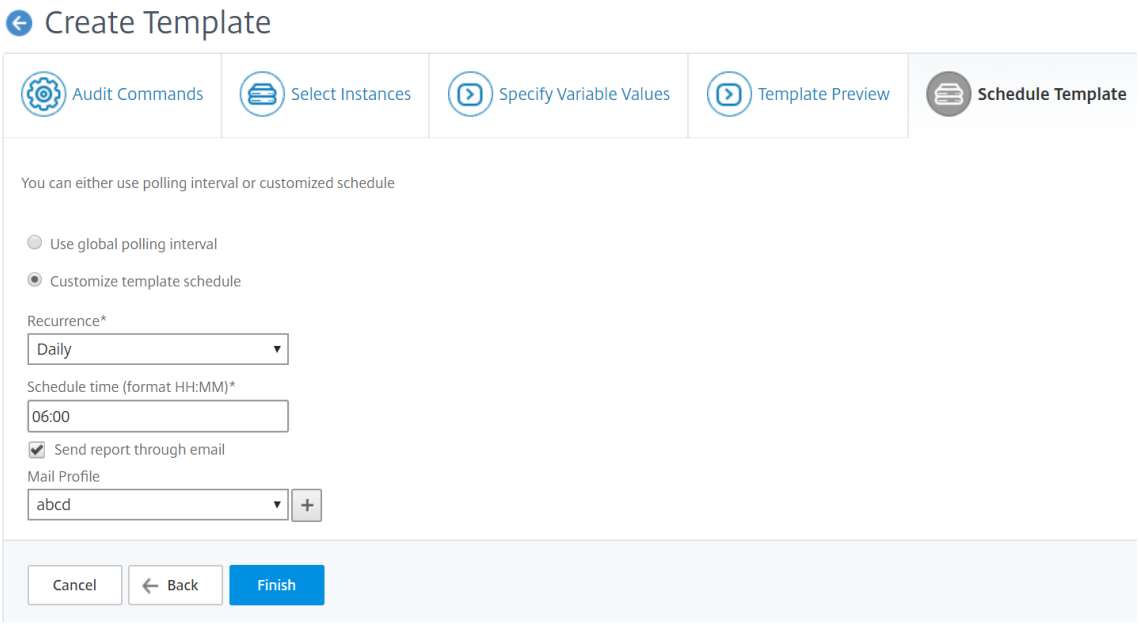
    - **Verwenden Sie das globale Polling-Intervall** Wählen Sie diese Option aus, um die Vorlage auf den Instanzen zu einem Zeitpunkt auszuführen, der global auf NetScaler ADM konfiguriert ist.

      > **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 Citrix ADM die Instanzen global abfragen soll.

    - **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 soll.

11. Klicken Sie auf **Fertig stellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

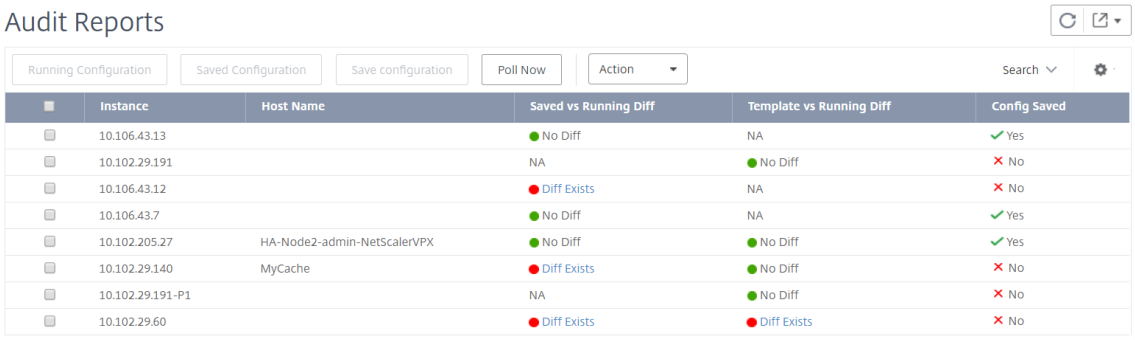
Die Überwachungsvorlagen, die in der Liste Überwachungsvorlagen angezeigt werden, werden zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt. Das Diagramm **NetScaler Config Drift** im **Konfigurationsüberprüfungs-Dashboard** zeigt allgemeine Details zu Konfigurationsänderungen 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

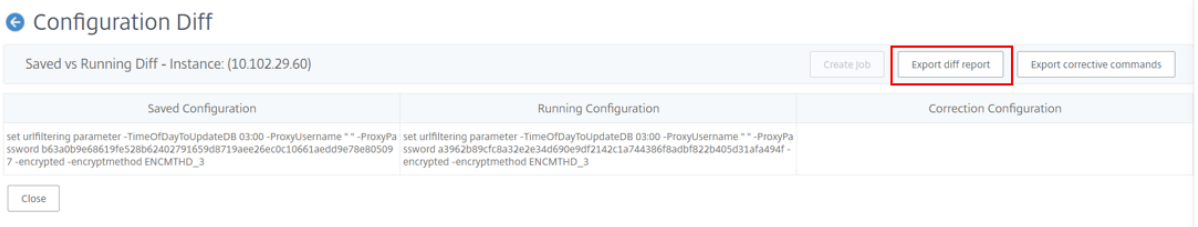


Im Bild sehen Sie, dass für einige Instanzen ein Diff nur in **Saved Vs Running Diff** vorhanden ist und für einige Instanzen ein Diff nur in **Template vs Running Diff** vorhanden ist. In einigen Fällen gibt es Unterschiede sowohl zwischen **Saved Vs Running Diff** als auch **Template vs Running Diff.**

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.

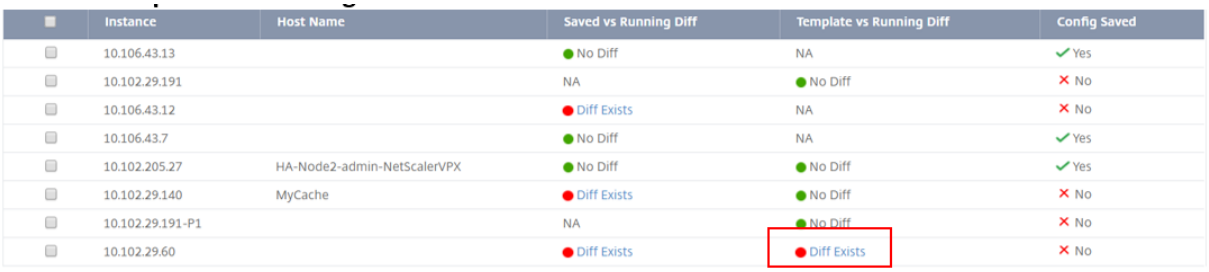


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

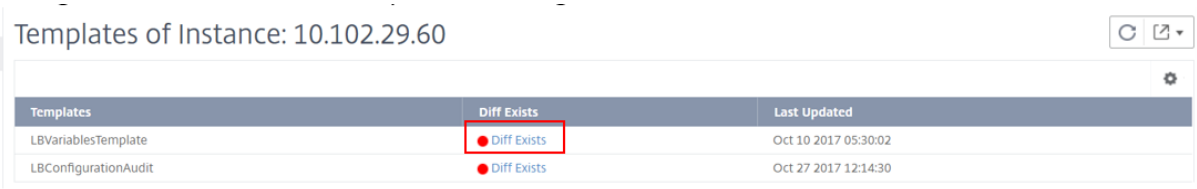
Klicken Sie auf **Diff-Bericht exportieren**, um eine CSV-Datei des Diff-Berichts herunterzuladen. Sie können auch auf Korrekturbefehle exportieren klicken, um die Befehle in eine TXT-Datei zu exportieren. Anschließend können Sie die Befehle für die zugeordnete Citrix ADM Instanz über Konfigurationsaufträge ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

Template gegen Running Diff

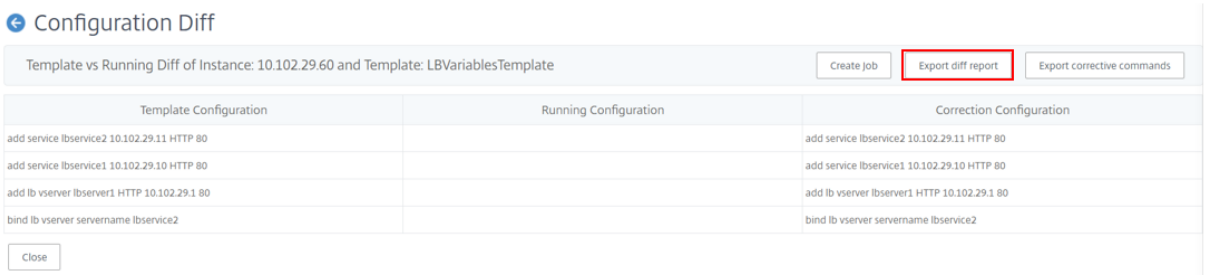
Das **Template vs Running Diff** enthält alle Vorlagen außer **Saved Vs Running Diff**, der Standardvorlage. Sie können den Unterschied anzeigen, der zwischen der Vorlage und der laufenden Konfiguration besteht.Klicken Sie beispielsweise für eine der Instanzen unter **Vorlage vs Laufende**Diff auf Diff 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.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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 auf bestimmten Instanzen ausgeführt werden sollen. 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.

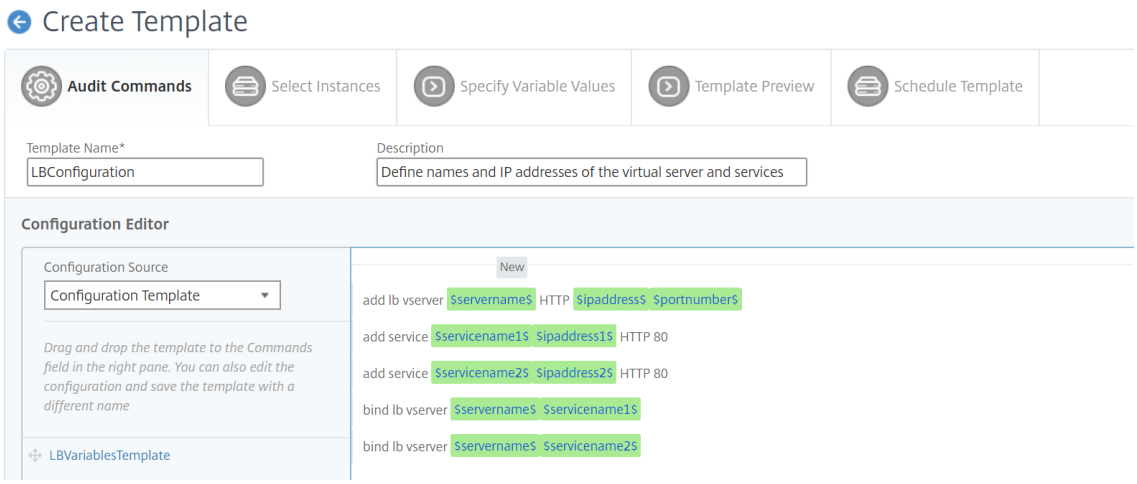
Sie können die Ausführung der Überwachungsvorlage automatisieren, indem Sie den Zeitpunkt planen, zu dem die Vorlage ausgeführt werden soll. Sie können auch festlegen, mit welcher Häufigkeit Citrix ADM die Vorlage ausführen soll. Sie können die Vorlage täglich, an einem bestimmten Tag in einer Woche 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 > Configuration Audit >** Auditvorlagen 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 und ablegen.

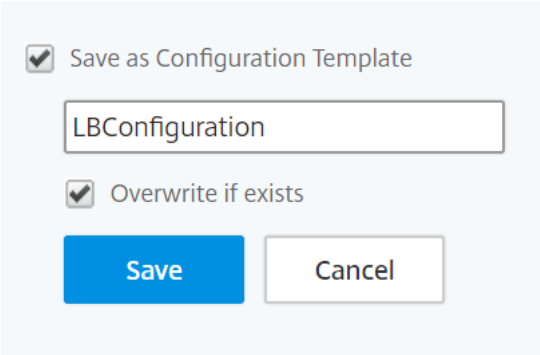
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Lastausgleichsservers “ipaddress”aus, und klicken Sie auf **In Variable konvertieren**, 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.



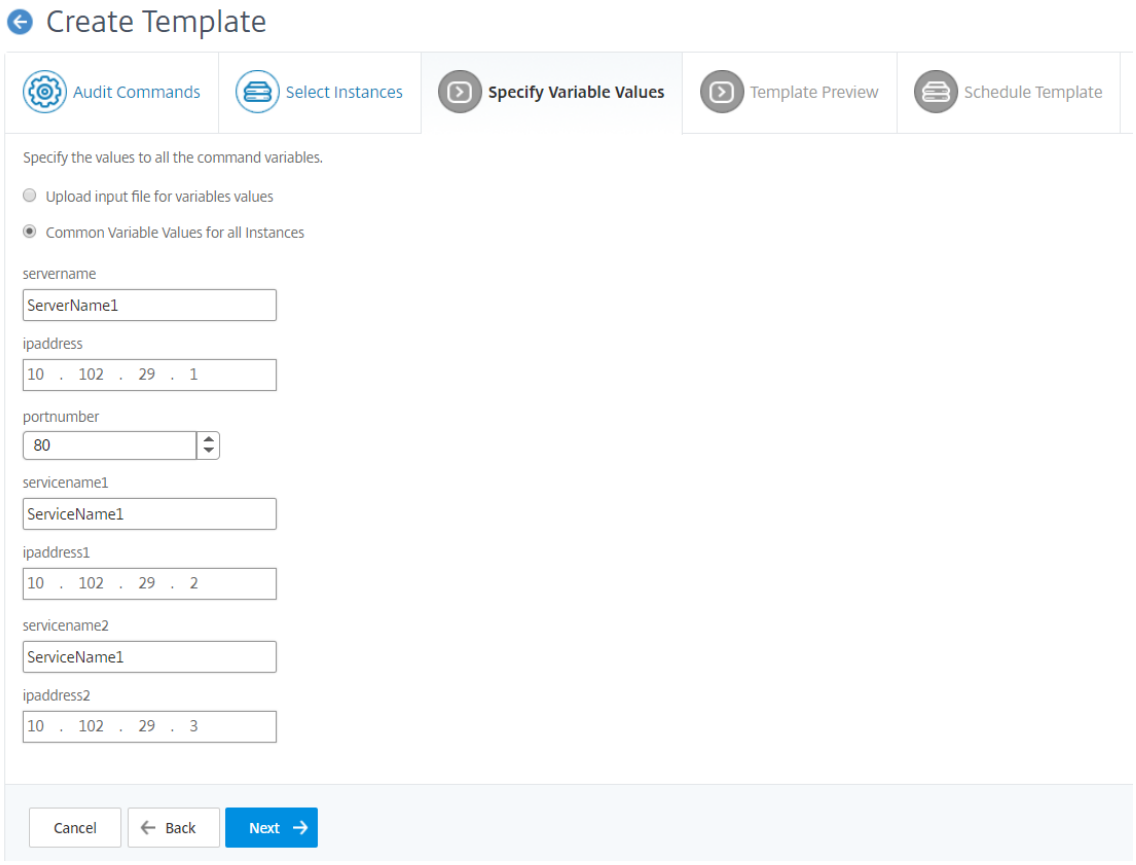
5. Klicken Sie auf**Speichern** und dann auf **Weiter**.
6. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen Sie die Konfigurationsüberprüfung ausführen möchten.
7. Auf der Registerkarte**Variablenwerte angeben** stehen Ihnen zwei Optionen zur Verfügung:

    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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. Klicken Sie auf **Weiter**.

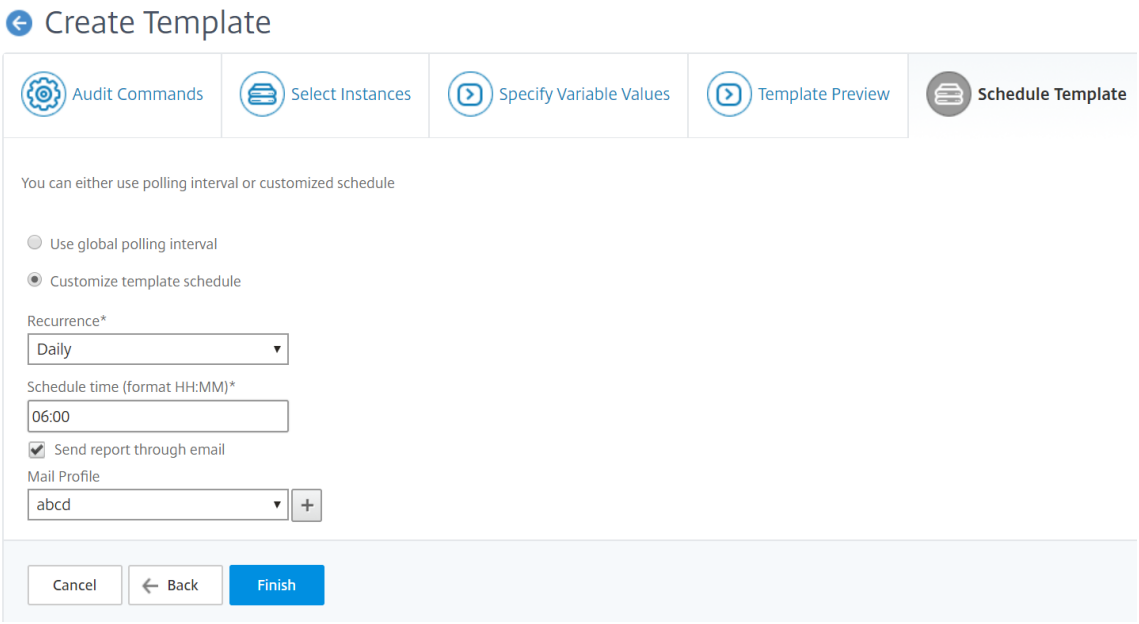


9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle auswerten und überprüfen, die für jede Instanz oder Instanzgruppe ausgeführt werden sollen. Klicken Sie auf **Weiter**.
10. Auf der Registerkarte **Zeitplanvorlage** haben Sie drei Optionen, um die Ausführung der Vorlage zu automatisieren, 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 soll.

11. Klicken Sie auf **Fertig stellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

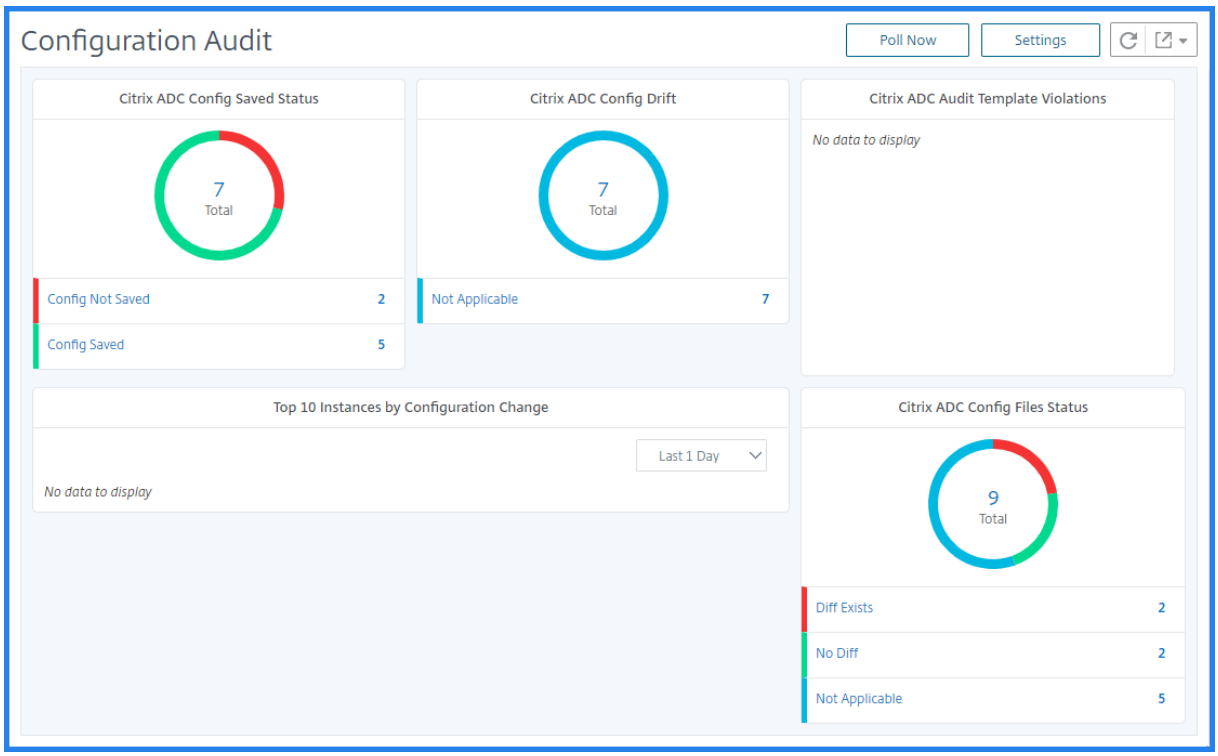


Die Überwachungsvorlage wird in der Liste Überwachungsvorlagen angezeigt und zum geplanten Zeitpunkt für die Konfigurationen in den angegebenen Instanzen ausgeführt.

Details zu Konfigurationsänderungen anzeigen

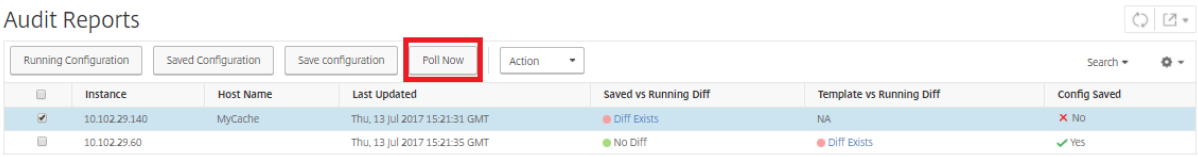
Sie können das Configuration Audit-Dashboard auch verwenden, um allgemeine Details zu Konfigurationsänderungen anzuzeigen, z. B. die zehn wichtigsten Instanzen nach Konfigurationsänderung oder die Anzahl der gespeicherten und nicht gespeicherten Konfigurationen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Mit NetScaler ADM können Sie Konfigurationsaudits manuell abfragen und alle Konfigurationsaudits der Instanzen sofort dem NetScaler ADM hinzufügen. **Navigieren Sie dazu zu Netzwerke**> **Configuration Audit,** klicken Sie auf **Jetzt** abfragen . Auf der Popup-Seite **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 das Diagramm **NetScaler Config Saved Status** oder das **NetScaler Config Drift**-Diagramm. Wählen Sie auf **der Seite**Auditberichte die Instanz aus und wählen Sie in der Liste **Aktion** die Option **Jetzt abfragen**aus.



So richten Sie Benachrichtigungen zur Konfigurationsprüfung ein:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Es kann jedoch vorkommen, dass einige Konfigurationen keine Standardkonfigurationen sind und dies die Leistung Ihrer Anwendungen beeinträchtigen kann.

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:

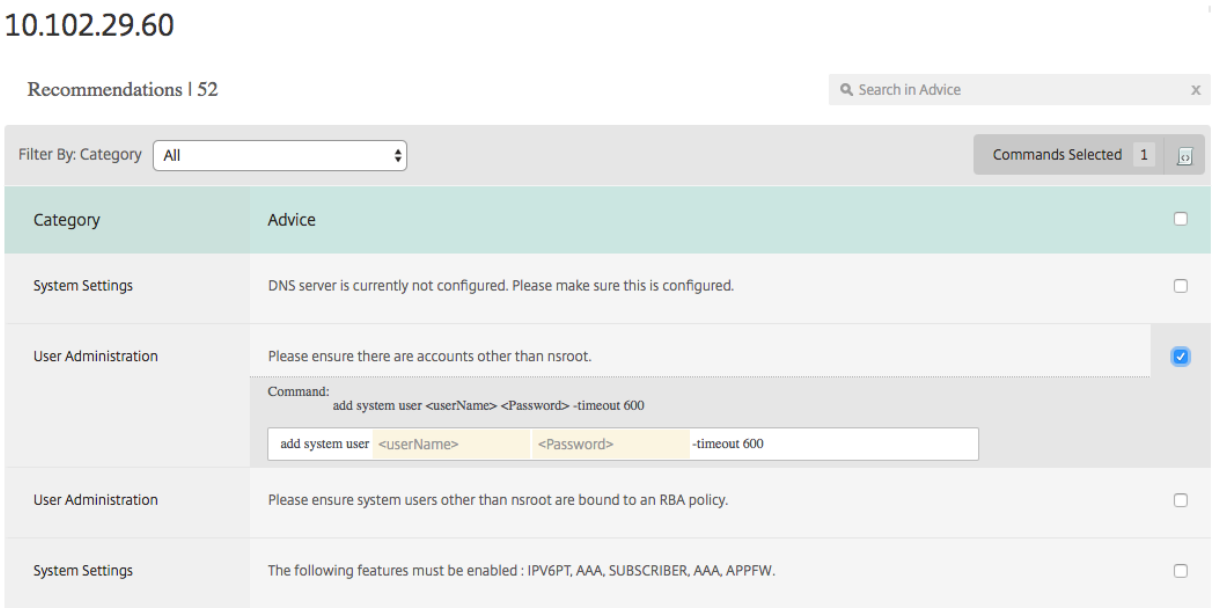
1. Navigieren Sie zu **Netzwerke** > **Konfigurationsüberwachung** > **Konfigurationshinweise**.
2. Führen Sie einen der folgenden Schritte aus:

   - 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.

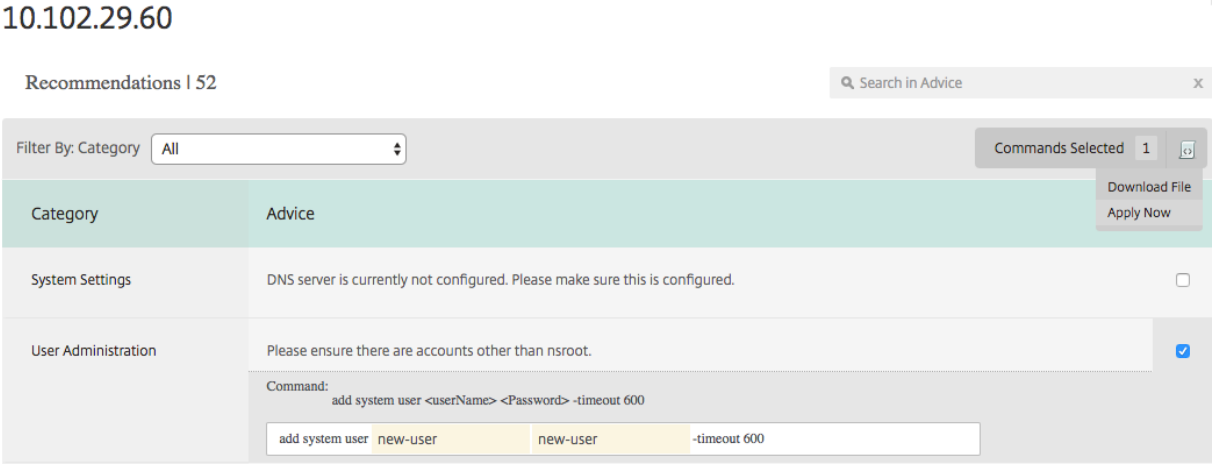
Citrix ADM analysiert die Konfiguration in Ihrer Instanz und bietet eine Liste mit Konfigurationsempfehlungen, wie in der Abbildung unten dargestellt. Aktivieren Sie das Kontrollkästchen neben einer Konfigurationsempfehlung, um die Korrekturbefehle anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

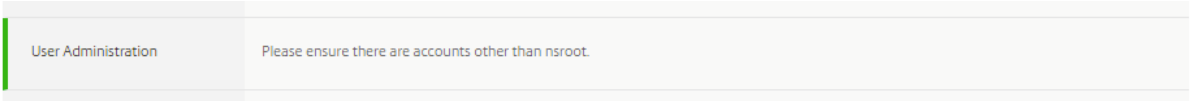


Wenn Sie Ihre Konfiguration aktualisieren möchten, geben Sie die Werte für die Variablen in den Korrekturbefehlen an und klicken Sie auf **Jetzt anwenden**, wie in der Abbildung unten gezeigt.

> **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, die Ihrer Meinung nach nicht bearbeiten sollten, einen eingeschränkten privilegierten Zugriff gewähren.

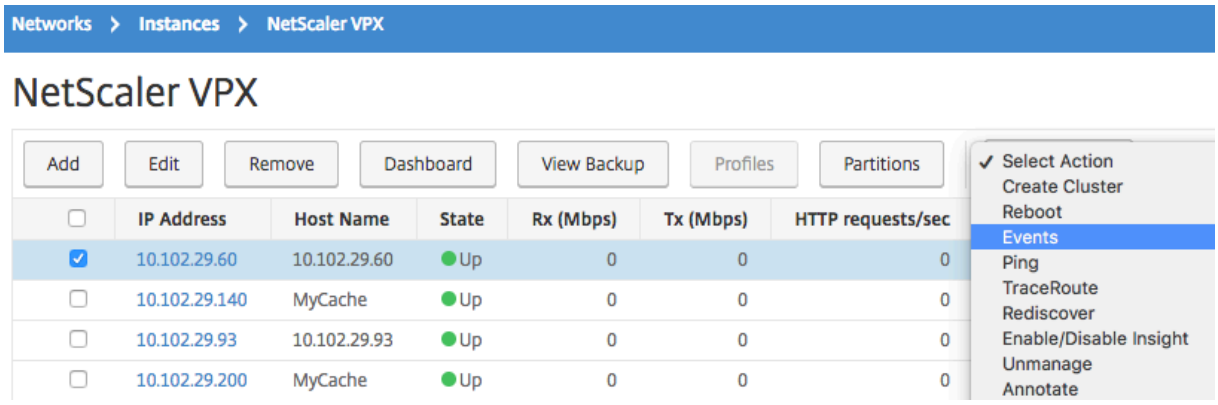


Wenn der Befehl auf der Netzwerkinstanz erfolgreich ausgeführt wird, wird das Kontrollkästchen neben dem Hinweis ausgeblendet.

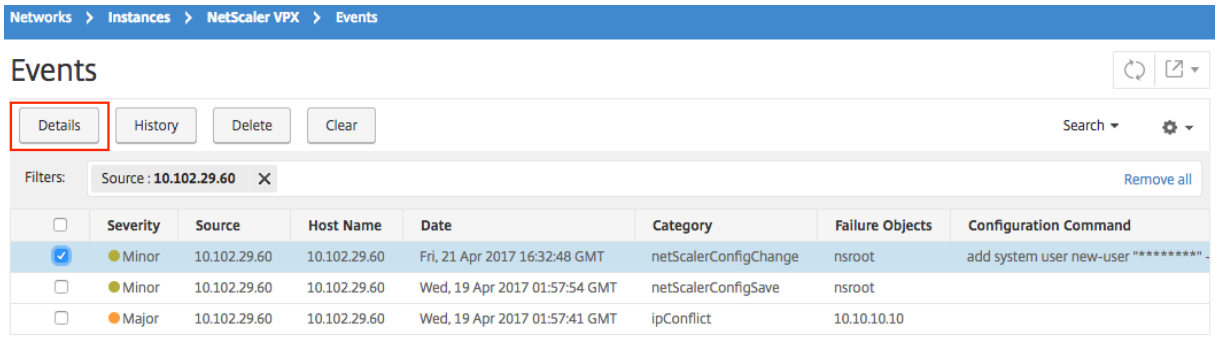


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn Sie die Details der Befehle anzeigen möchten, die auf Ihrer Netzwerkinstanz ausgeführt werden, navigieren Sie zu **Networks** > **Instances** > **, <Instance_Type>**wählen Sie die IP-Adresse der Instance aus und klicken Sie dann in der Dropdownliste **Aktionen** auf **Events** .



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.

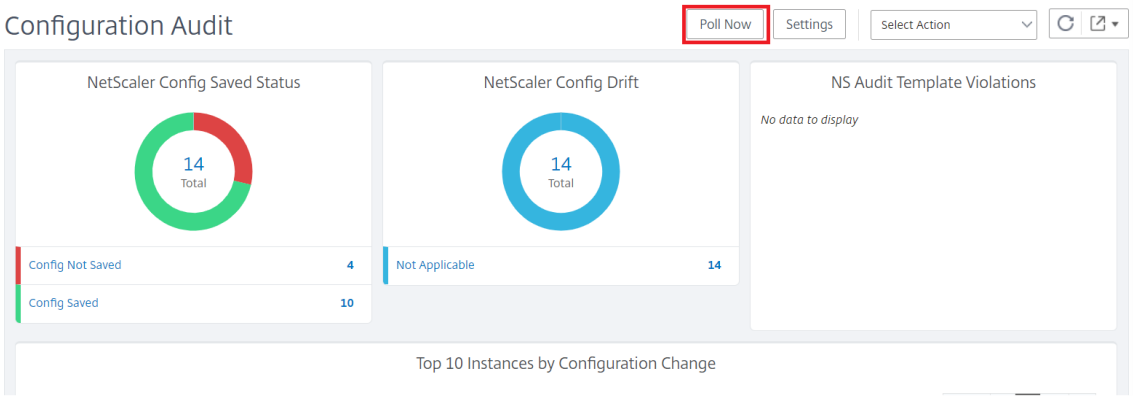
Anstatt die gesamte Konfigurationsüberwachung der NetScaler ADC-Instanzen abzufragen, können Sie nur die Konfigurationsaudits einer ausgewählten Instanz oder Instanzen manuell abfragen.

So fragen Sie Konfigurationsaudits von NetScaler ADC-Instanzen ab:

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Konfigurationsüberwachung**.

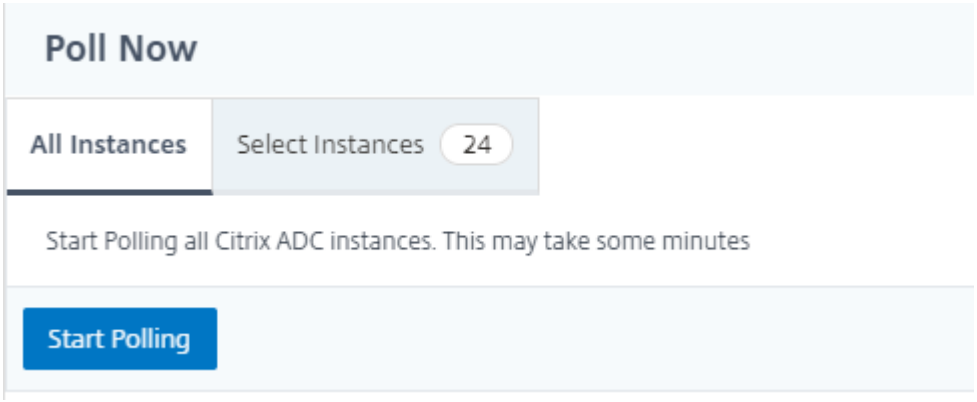
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Klicken Sie auf der Seite **Konfigurationsüberwachung** oben rechts auf **Jetzt abfragen**.

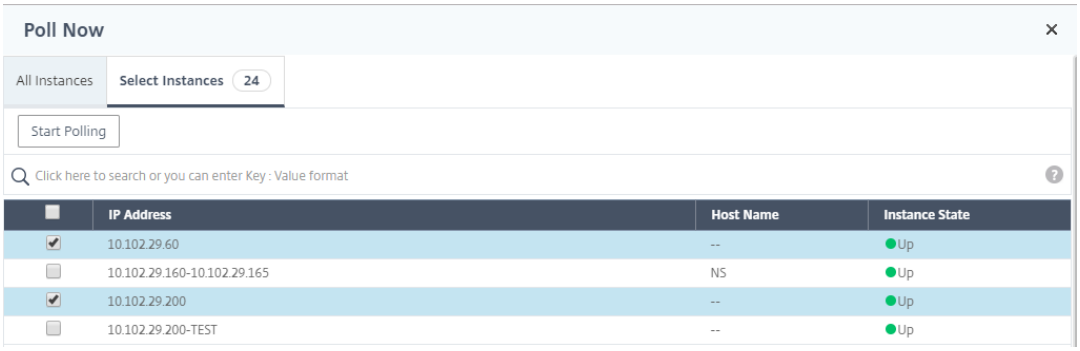


3. Die Seite **Jetzt abfragen** wird geöffnet und bietet Ihnen die Möglichkeit, alle NetScaler ADC-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

   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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Korrekturbefehle verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen Citrix ADC Instanzen auszuführen. Wenn Sie den Konfigurationsauftrag ausführen, werden die Instanzen zur gewünschten Konfiguration zurückgesetzt. Weitere Informationen zum Erstellen 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

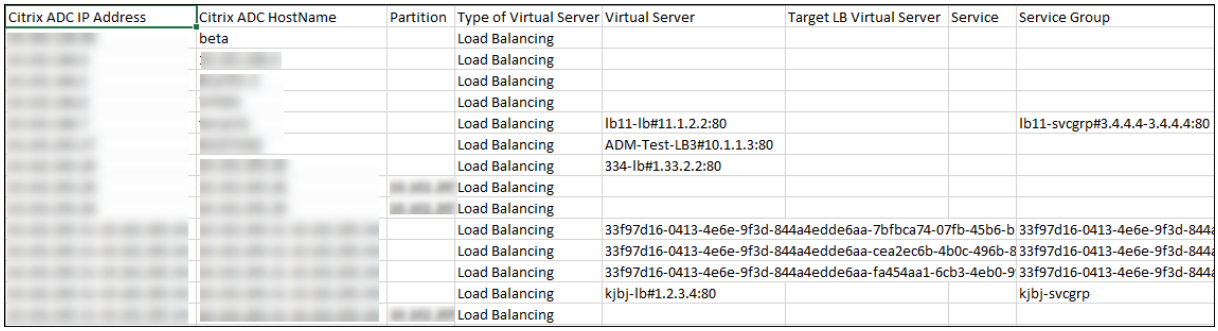
Mit Citrix Application Delivery Management (ADM) können Sie die Berichte der Citrix Application Delivery Controller (ADC) -Instanzentitäten auf allen Ebenen anzeigen. Es gibt zwei Arten von Berichten, die Sie in NetScaler ADM > Netzwerkfunktionen herunterladen können: konsolidierte Berichte und einzelne 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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** auf  .
3. Auf der sich öffnenden Seite **Exportieren** haben Sie zwei Optionen, um den Bericht anzuzeigen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

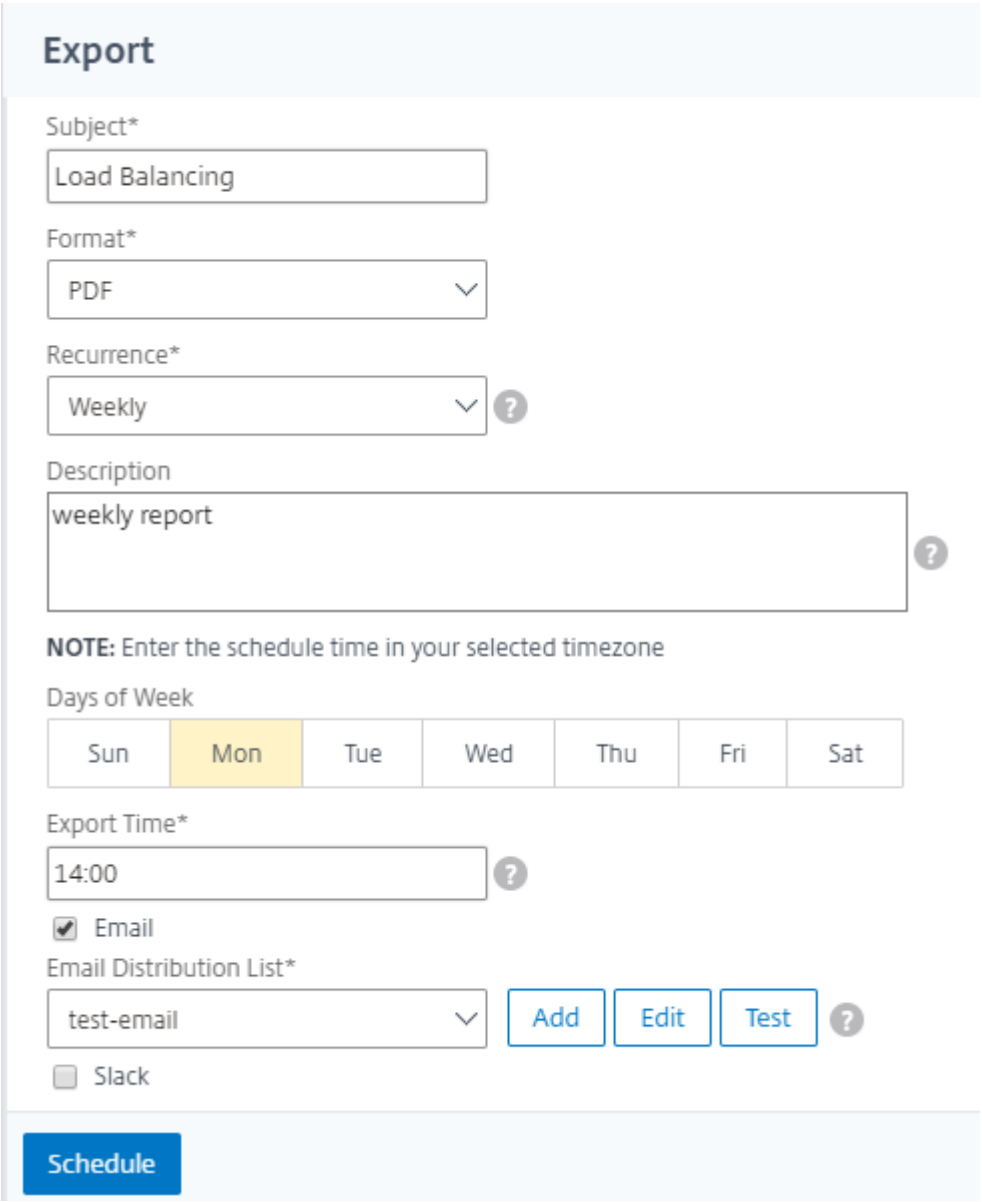
   i. **Wiederholung** —wählen Sie im Drop-down-Listenfeld die Option **Täglich**, **Wöchentlich**oder **Monatlich** aus.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

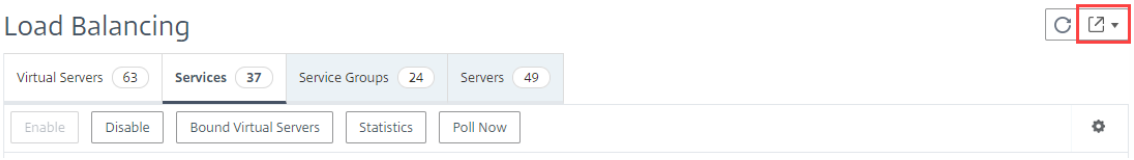
Sie können einen individuellen Bericht für einen bestimmten Entitätstyp generieren und exportieren, der den Instanzen zugeordnet ist. Betrachten Sie beispielsweise ein Szenario, in dem Sie eine Liste aller Lastausgleichsdienste im Netzwerk anzeigen möchten.

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen** > **Load Balancing >**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix ADC-Instanzen, Partitionen und den entsprechenden gebundenen Entitäten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind. Sie können diese Berichte im CSV-Dateiformat exportieren.

Der Bericht zeigt die folgenden virtuellen Serverdaten an:

- NetScaler IP-Adresse
- Hostname
- Daten partitionieren
- Name des virtuellen Servers
- Typ des virtuellen Servers
- Virtueller Server
- Virtueller LB-Zielserver

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

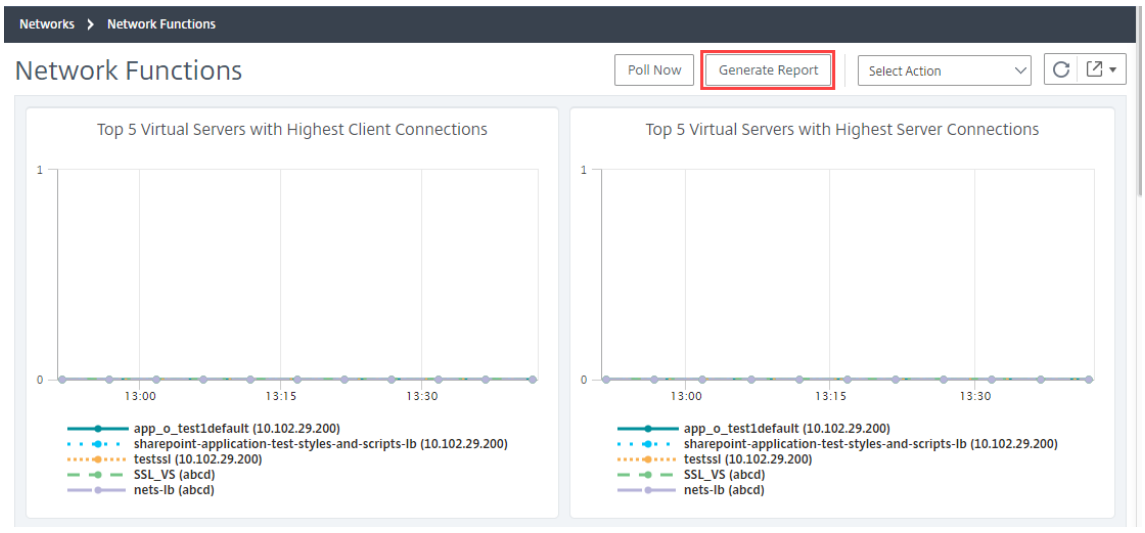
> **Hinweis**
>
> Für virtuelle Server mit Content Switching und Cache-Umleitung werden in der Spalte Virtueller Ziel-LB-Server alle LB-Server aufgeführt, d. h. sowohl Standardserver als auch richtlinienbasierte Server.
>
> - Name des Dienstes
> - Name der Dienstgruppe

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:

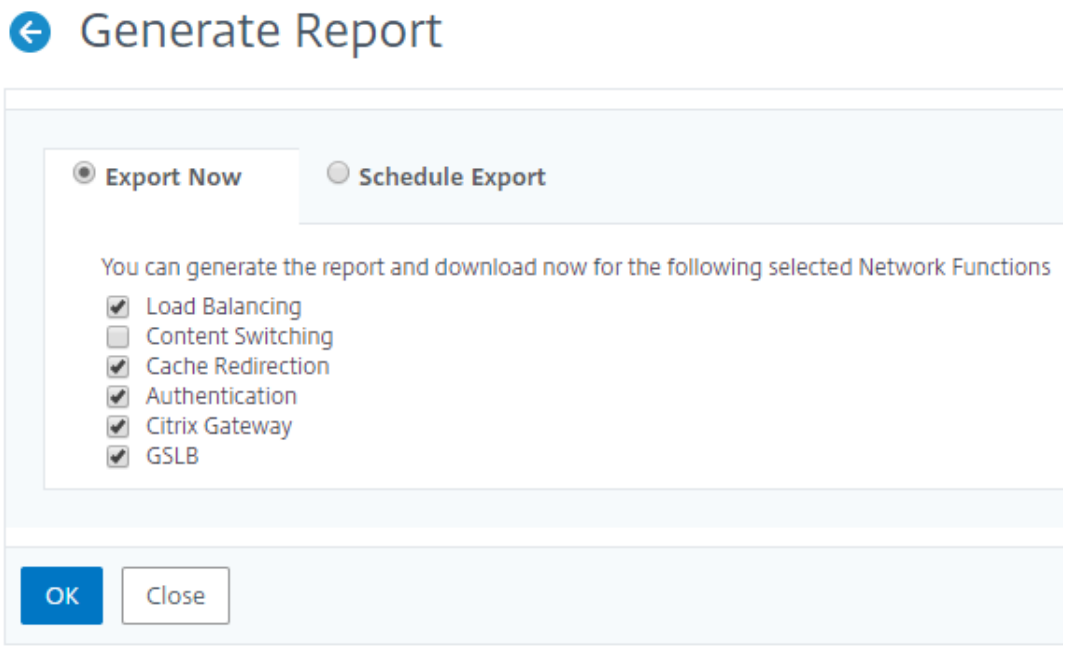
1. Navigieren Sie zu**Netzwerke > Netzwerkfunktionen**.
2. Klicken Sie auf der Seite**Netzwerkfunktionen** im rechten Bereich oben rechts auf der Seite auf**Bericht generieren**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

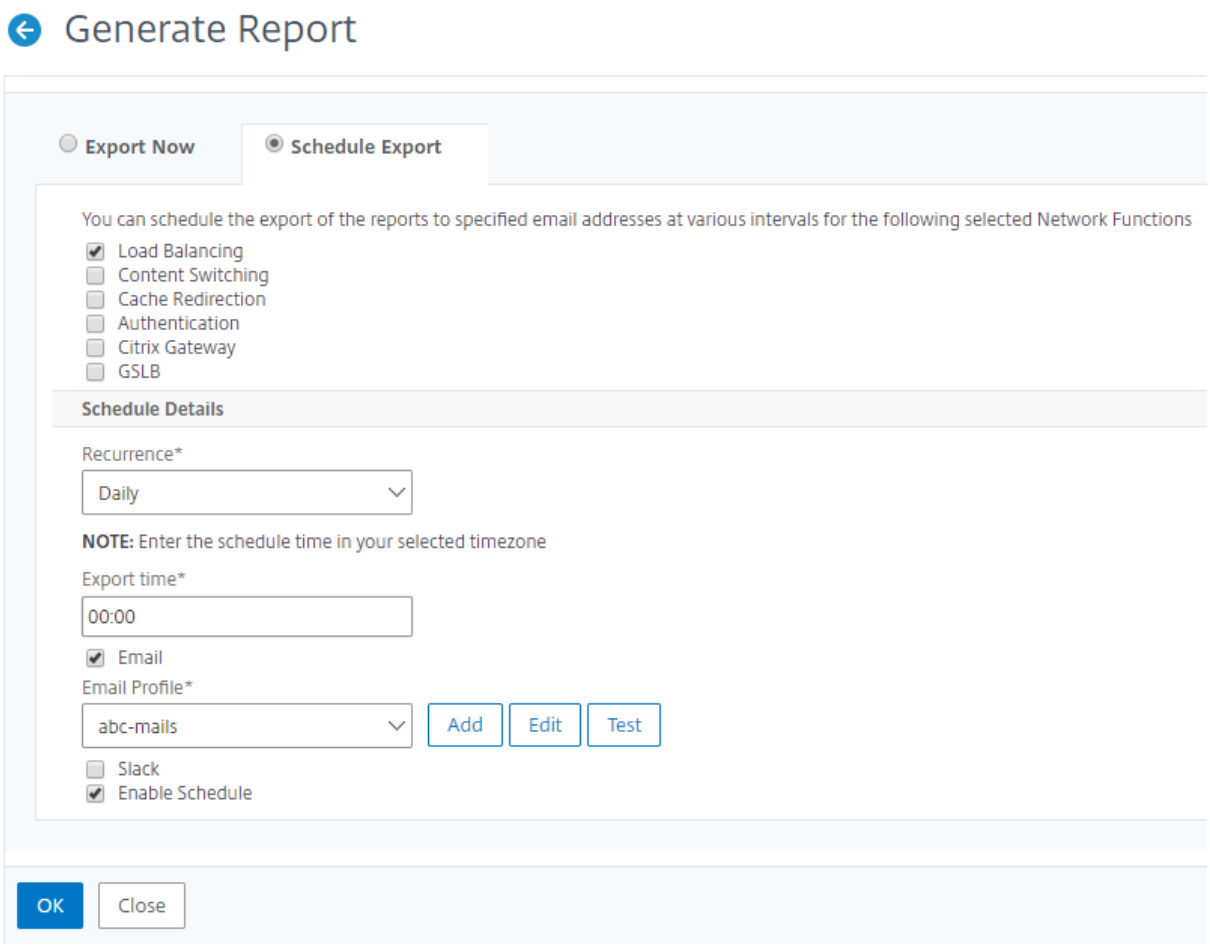
      i. **Wiederholung**- Wählen Sie im Dropdownlistenfeld**Täglich**,**Wöchentlich**oder**Monatlich**aus.

      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 generieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Netzwerkberichterstellung

February 5, 2024

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichte in Citrix Application Delivery Management (ADM) überwachen. Möglicherweise verfügen Sie über eine verteilte Bereitstellung mit vielen Anwendungen, die an mehreren Standorten bereitgestellt werden. Um eine optimale Leistung Ihrer Anwendungen sicherzustellen, haben Sie auch mehrere Citrix Application Delivery Controller (ADC) -Instanzen bereitgestellt, um den Lastausgleich, den Inhaltswechsel oder die Komprimierung des Datenverkehrs durchzuführen. Die Netzwerkleistung kann sich auf die Anwendungsleistung auswirken. Um die Leistung Ihrer Anwendungen weiterhin aufrechtzuerhalten, müssen Sie regelmäßig die Netzwerkleistung 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

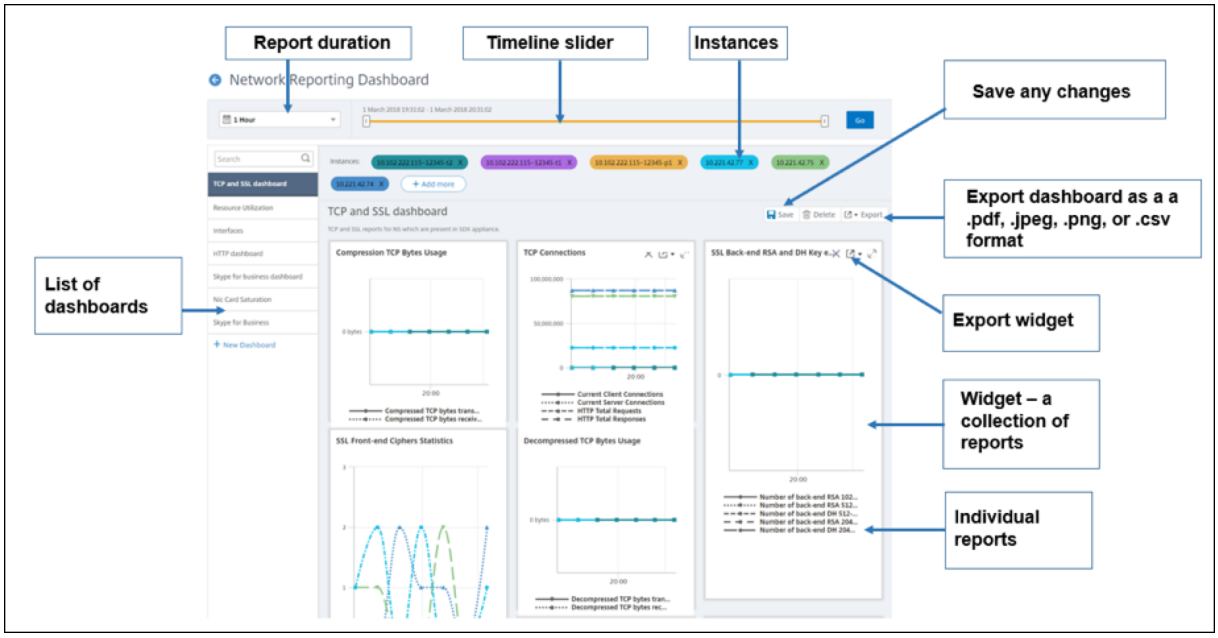
sowohl NetScaler ADC - als auch SD-WAN-Instanzen. Die virtuellen Server, für die Sie Berichte erstellen können, sind wie folgt:

- Server mit Lastenausgleich
- Content Switching-Server
- Cache-Umleitung
- 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 dieser Berichte 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 eine Vielzahl von Berichten anzuzeigen. Ein Widget stellt einen Bericht auf dem Dashboard dar, d. h. eine Sammlung von

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

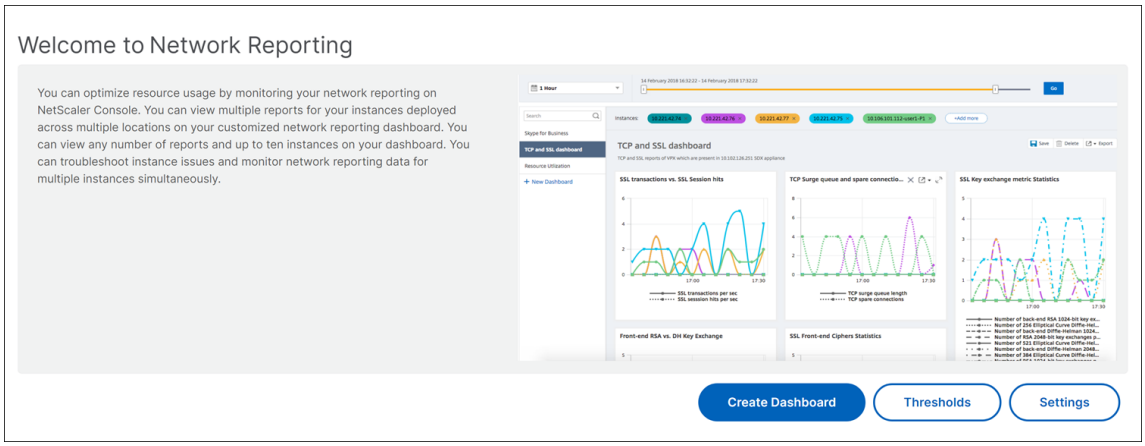
verwandten Berichten. Beispielsweise enthält ein komprimierter TCP-Byte-Nutzungsbericht Berichte für komprimierte TCP-Bytes, die pro Sekunde übertragen und empfangen wurden.

- 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 planen, wann der Bericht erstellt werden soll. Sie können auch eine E-Mail-Verteilerliste konfigurieren, an die die Berichte gesendet werden sollen.
- Im Abschnitt Instanzen oben im Dashboard werden die IP-Adressen aller Instanzen aufgeführt, für die der Bericht generiert wird.
- Sie können Instanzen entweder entfernen, indem Sie auf X klicken oder weitere Instanzen zu den Berichten hinzufügen. Derzeit können Sie jedoch Berichte für zehn Instanzen von Citrix ADM anzeigen.
- Sie können das gesamte Dashboard auch als PDF-, JPEG-, PNG- oder CSV-Format in Ihr System exportieren. Alle am Dashboard vorgenommenen Änderungen müssen gespeichert werden. Klicken Sie auf Speichern, um die Änderungen zu speichern.

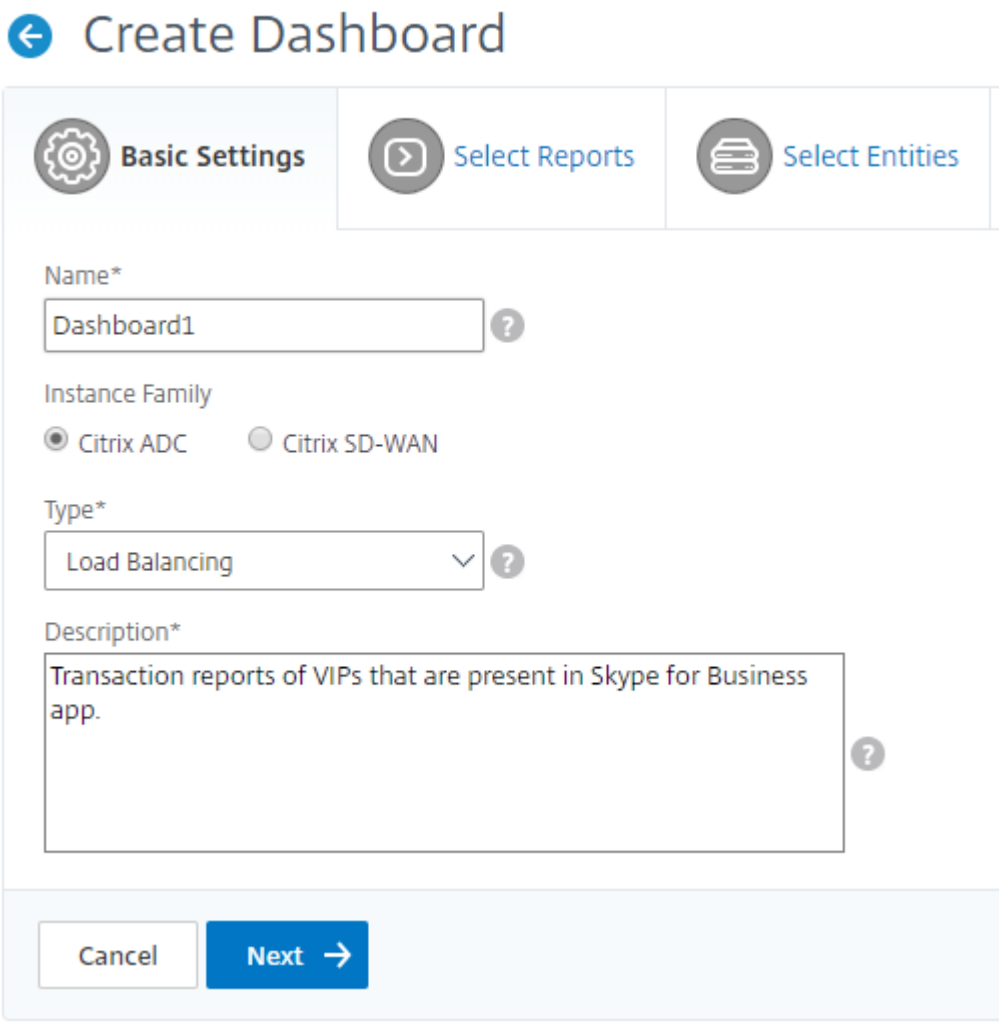
Im folgenden Abschnitt werden ausführlich die Aufgaben zum Erstellen eines Dashboards, zum Generieren von Berichten und zum Exportieren von Berichten erläutert.

So zeigen Sie ein Dashboard an oder erstellen es

1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkberichterstattung**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



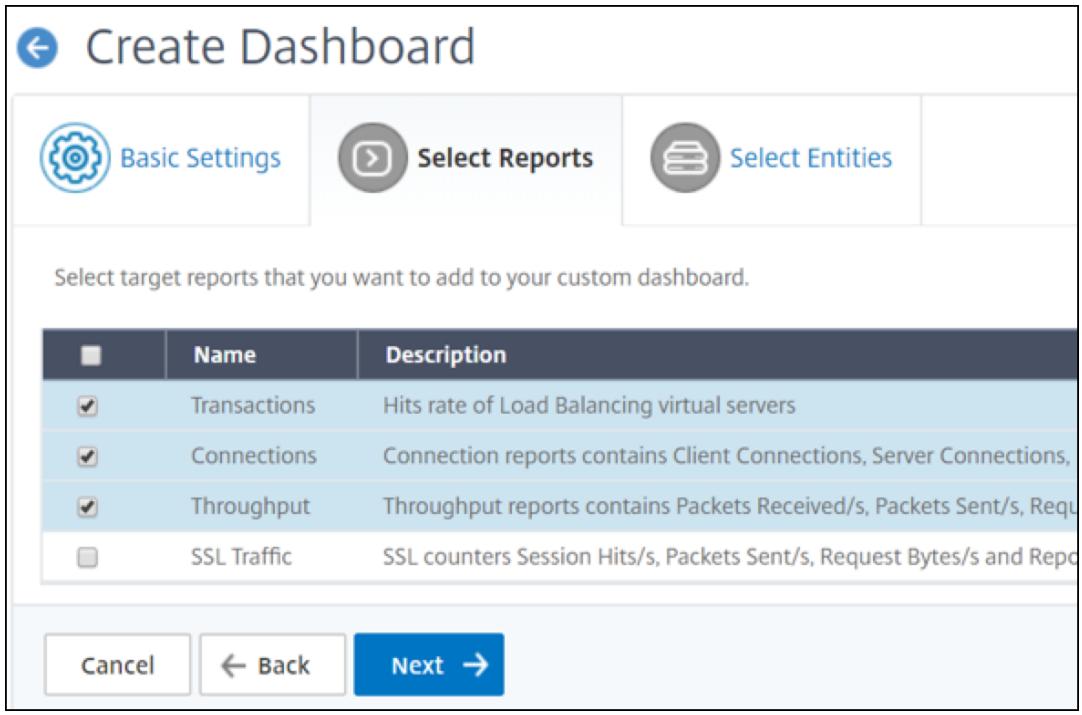
2. **Wählen Sie auf der Registerkarte Berichte** auswählen die erforderlichen Berichte aus. In diesem Beispiel können Sie Transaktionen, Verbindungen und Durchsatz auswählen. Klicken Sie auf **Weiter**.
3. Klicken Sie auf Dashboard anzeigen, um die vorhandenen **Dashboards anzuzeigen**. Die Seite **Network Reporting Dashboard** wird geöffnet, auf der Sie alle Dashboards und Berichtwidgets anzeigen können.
4. Zum Erstellen eines Dashboards klicken Sie auf **Dashboard erstellen**.
5. Die Seite **Dashboard erstellen** wird geöffnet.
6. Geben Sie auf der Registerkarte **Grundeinstellungen** die folgenden Details ein:
    a) **Name**. Geben Sie den Namen des Dashboards ein.
    b) **Instanzfamilie**. Wählen Sie den Instanztyp aus - Citrix ADC oder Citrix SD-WAN

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

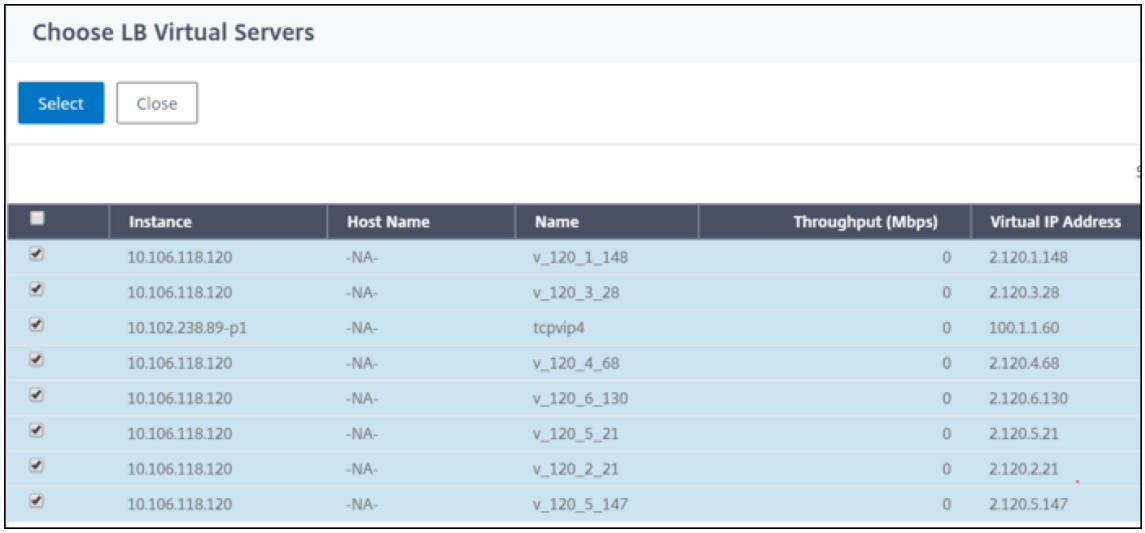
c) **Typ**. Wählen Sie den Entitätstyp aus, für den Sie Berichte erstellen möchten. Wählen Sie in diesem Beispiel virtuelle Server für den Lastenausgleich aus.

d) **Beschreibung**. Geben Sie eine aussagekräftige Beschreibung für das Dashboard ein.

e) Klicken Sie auf **Weiter**.



7. Klicken **Sie auf der Registerkarte Entitäten auswählen** auf **Hinzufügen**.
8. **Wählen Sie im Fenster Virtuelle LB-Server** auswählen, das eingeblendet wird, eine beliebige Anzahl von virtuellen Servern aus, die Sie überwachen möchten.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Je nach dem Entitätstyp, den Sie auf der Registerkarte Grundeinstellungen ausgewählt haben, wird die Registerkarte Entitäten mit entsprechenden Entitäten gefüllt. Wenn Sie beispielsweise global auswählen, können Sie Instanzen hinzufügen.

9. Klicken Sie auf **Erstellen.**

Das **TCP- und SSL**-Dashboard wird erstellt und zeigt alle Berichte an, die Sie ausgewählt haben.

> **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**.

Beim Planen von Netzwerkberichten können Sie die Überschrift des Berichts anpassen, indem Sie eine Textzeichenfolge in das Feld Betreff eingeben. Der Bericht, der zum geplanten Zeitpunkt erstellt wurde, hat diese Zeichenfolge als Name.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Derzeit ist diese Option nur verfügbar, wenn Sie den Export von Berichten planen. Sie können dem Bericht keine Überschrift hinzufügen, wenn Sie sie sofort exportieren.

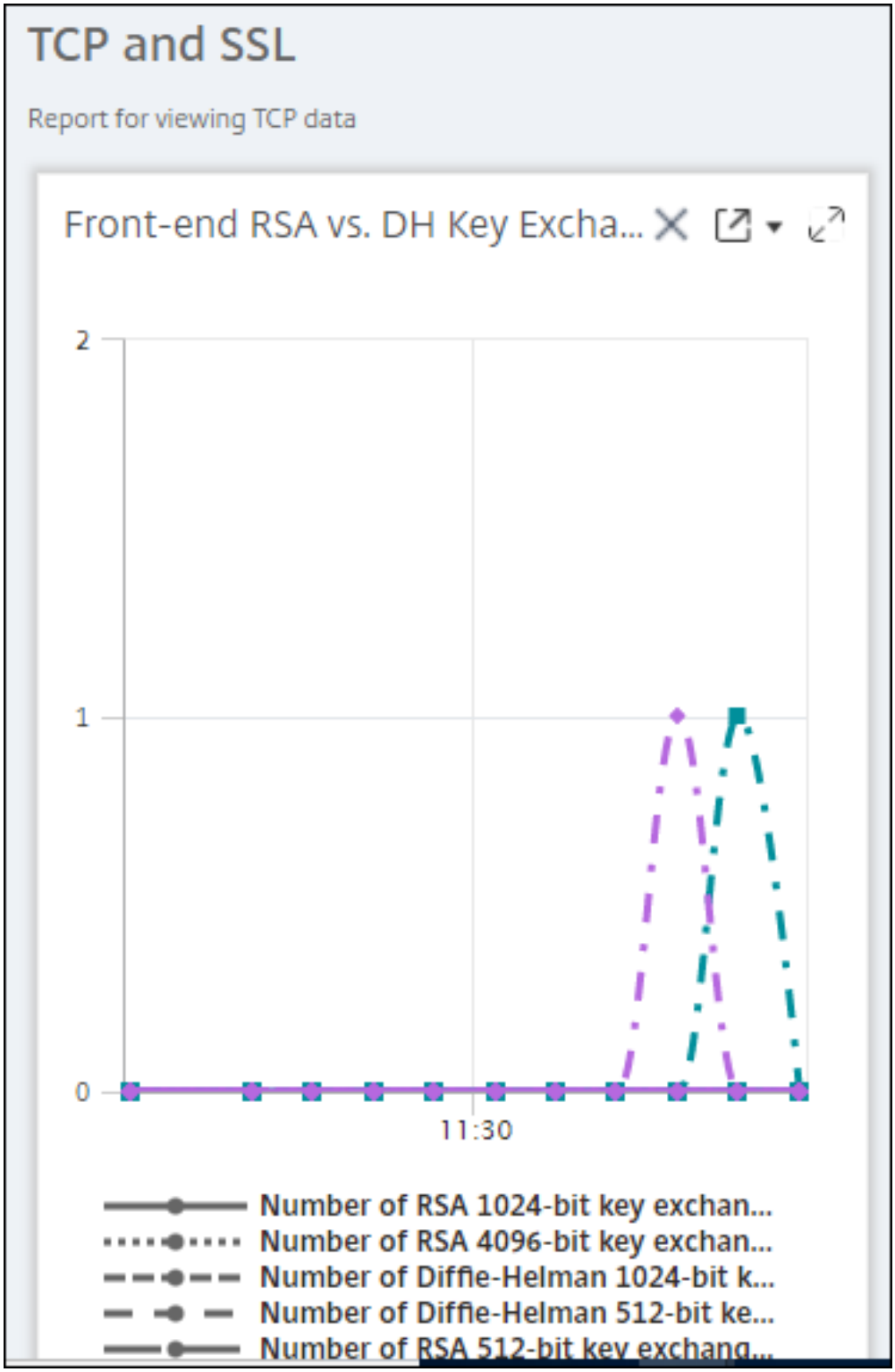
So exportieren Sie Dashboard-Berichte:

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**.**

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 **TCP und SSL** .
4. Wählen Sie ein Widget aus. Wählen **Sie beispielsweise Front-end RSA vs. DH-Schlüsselaustausch**.
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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 überschreitet oder unterschreitet (wie in der Regel angegeben), wird ein Ereignis mit dem angegebenen Schweregrad generiert, das auf ein leistungsbezogenes Problem hinweist. Wenn der Zählerwert zu einem Wert zurückkehrt, den Sie als normal betrachten, wird das Ereignis gelöscht. Diese Ereignisse können angezeigt werden, indem Sie zu **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.

Um einen Schwellenwert zu erstellen

1. ******** Navigieren Sie in Citrix ADM zu Netzwerke > Netzwerkberichterstattung > Schwellenwerte . Klicken Sie unter**Schwellenwerte**auf**Hinzufügen**.

1. Geben Sie auf der Seite Schwellenwert **erstellen die**folgenden Details an:

    - **Name**des Schwellenwerts . 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.

2. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

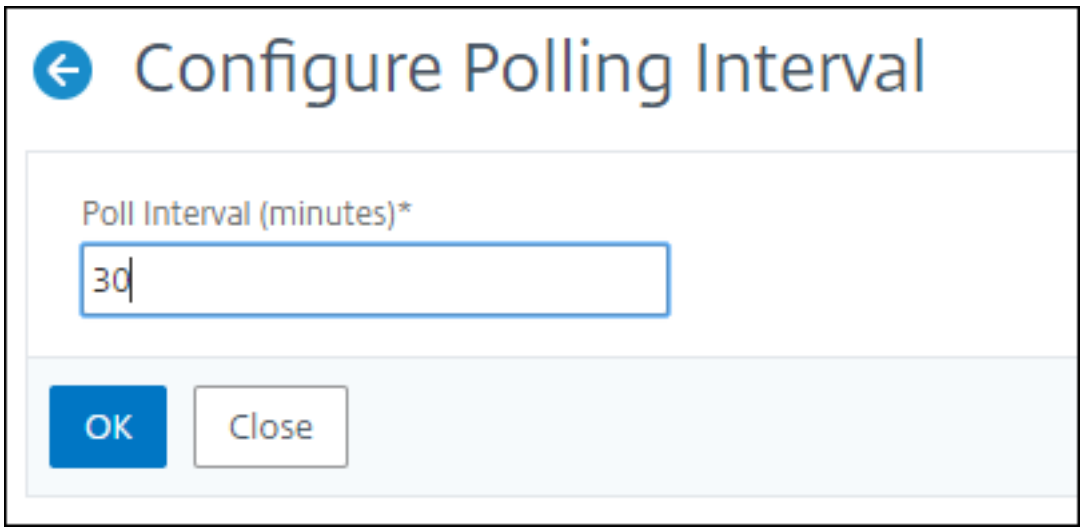
3. Wählen Sie die IP-Adresse der Instanz oder der Instanzen, für die Sie den Schwellenwert festlegen möchten.
4. Sie können zusätzlich eine **Ereignismeldung**hinzufügen. Geben Sie eine Nachricht ein, die angezeigt werden soll, wenn der Schwellenwert erreicht ist. NetScaler ADM hängt den überwachten Wert und den Schwellenwert an diese Nachricht an.
5. Wählen Sie**Aktivieren**, um den Schwellenwert für die Generierung von Alarmen zu aktivieren.
6. Optional können Sie **Aktionen** wie E-Mail- und/oder SMS-Benachrichtigungen konfigurieren.
7. Klicken Sie auf **Erstellen**.

Festlegen des Intervalls für Leistungsabfragen

Standardmäßig erfassen NITRO -Aufrufe alle 5 Minuten Leistungsdaten für das Netzwerk-Reporting. Dadurch werden Instanzstatistiken wie Zählerinformationen abgerufen und auf der Basis von pro Minute, pro Stunde, pro Tag oder pro Woche aggregiert. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Konfigurieren von Netzwerkberichterstattungseinstellungen

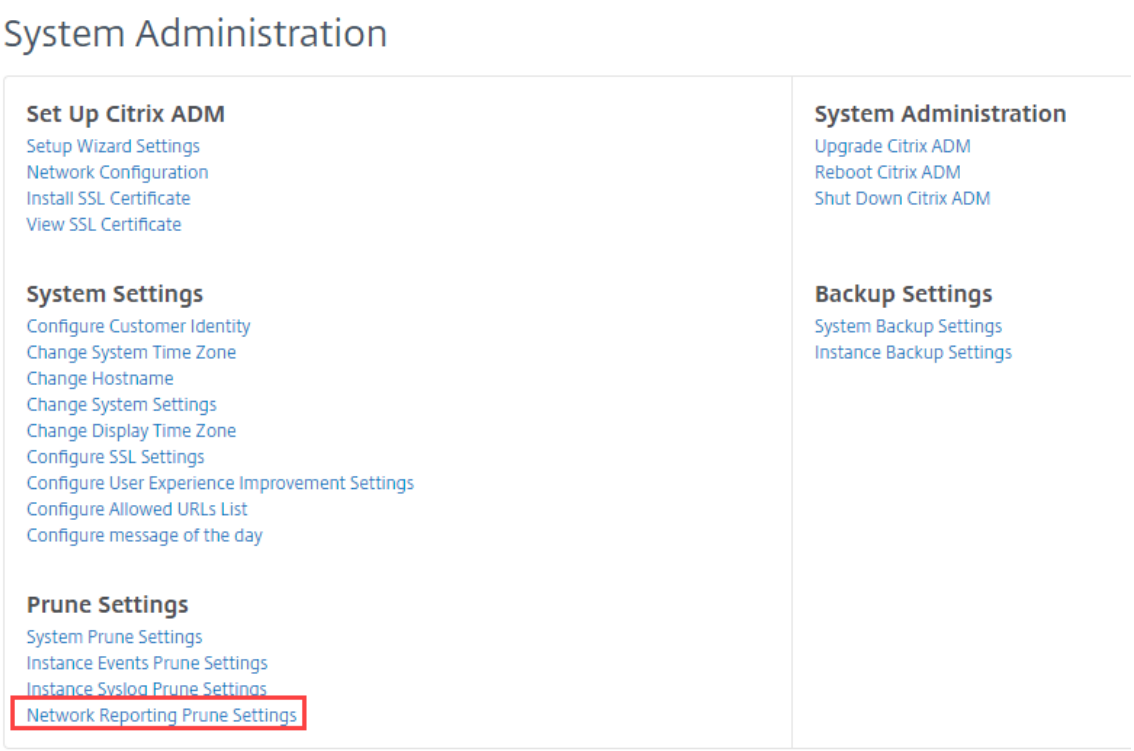
Sie können das Löschintervall von Netzwerkberichtsdaten in NetScaler ADM konfigurieren. Dadurch wird die Menge der Netzwerkberichtungsdaten begrenzt, die in der Datenbank des Citrix ADM -Servers gespeichert werden. Standardmäßig erfolgt die Beschneidung alle 24 Stunden (um 01.00 Uhr) für das Netzwerk, das historische Daten meldet.

> **Hinweis** Der Wert, den Sie angeben können, darf 90 Tage nicht überschreiten und nicht weniger als 1 Tag betragen.

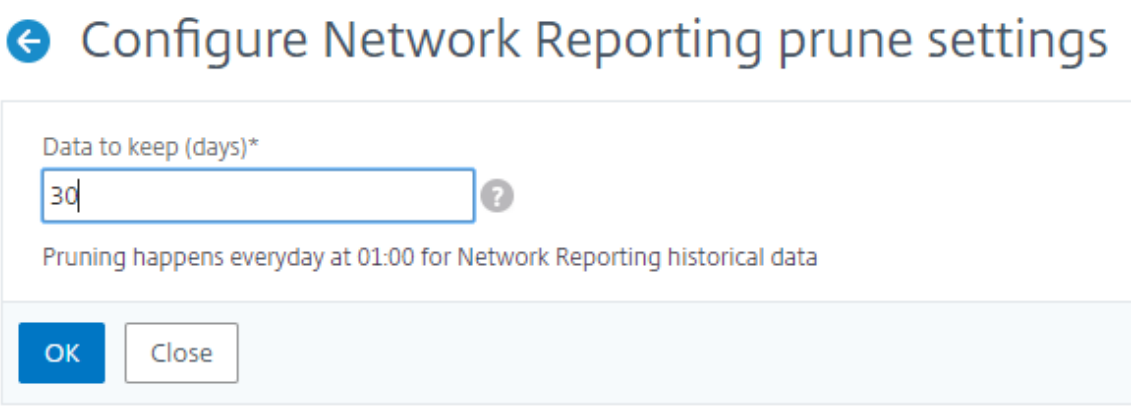
So konfigurieren Sie die Prune-Einstellungen für Netzwerkberichte:

1. Navigieren Sie zu **System > Systemadministration**. Klicken Sie unter **Prune-Einstellungen** auf **Network Reporting Prune-Einstellungen** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Geben Sie auf der Seite „**Network Reporting Prune-Einstellungen konfigurieren** “die Anzahl der Tage an, für die Daten aufbewahrt werden sollen, und klicken Sie auf **OK** .



Alle Leistungsdaten der Netzwerkberichterstattung werden für die ausgewählte Anzahl von Tagen in der Citrix ADM-Datenbank gespeichert.

Analytics

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Analytics-Funktion	Beschreibung
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.
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 Citrix ADM wird in allen Citrix ADC-Lizenzeditionen (Standard/Enterprise/Platinum) unterstützt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Funktionen von NetScaler ADM Analytics	NetScaler ADC-Lizenzanforderung
HDX Insight	Der HDX Insight-Bericht auf Citrix ADM wird auf jeder der folgenden Citrix ADC-Lizenzen unterstützt: Enterprise Edition (für Berichte unter 1 Stunde) oder Platinum Edition (für unbegrenzte Berichterstattung). **Hinweis:** Die Standard-Lizenzausgabe wird nicht unterstützt.
Security Insight	Der Security Insight-Bericht zu Citrix ADM wird in der Platinum Edition oder Enterprise 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 Citrix ADM wird in allen Citrix ADC-Lizenzeditionen (Standard/Enterprise/Platinum) unterstützt.
Gateway Insight	Der Gateway Insight-Bericht auf Citrix ADM wird auf jeder der folgenden Citrix ADC-Lizenzen unterstützt: Enterprise Edition (für Berichte unter 1 Stunde) oder Platinum Edition (für unbegrenzte Berichterstattung). **Hinweis:** Die Standard-Lizenzausgabe wird nicht unterstützt.
TCP Insight	TCP Insight-Bericht wird auf allen Citrix ADC-Lizenzeditionen (Standard/Enterprise/Platinum) 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

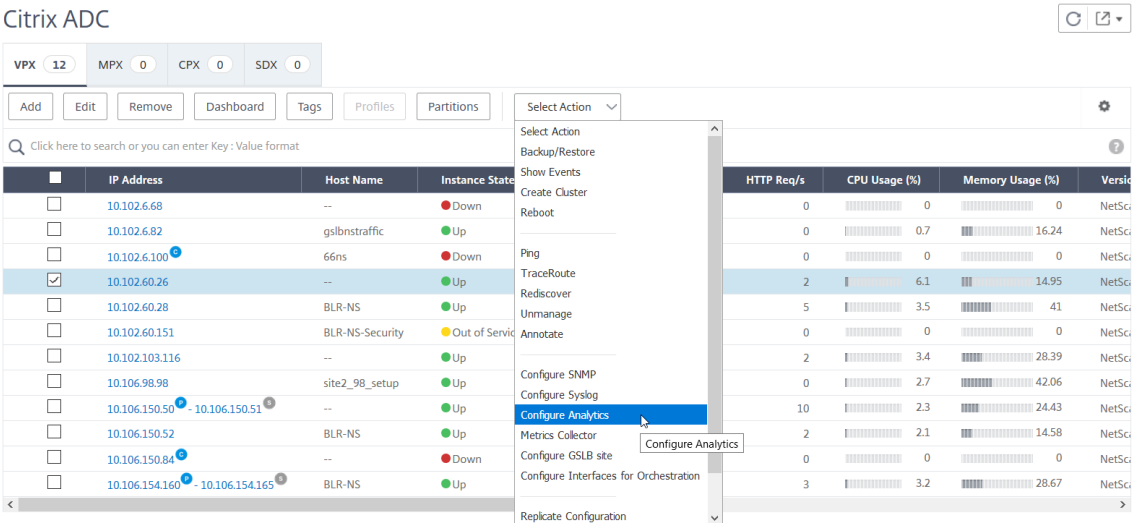
- IPFIX ist ein offener IETF-Standard (Internet Engineering Task Force), der in RFC 5101 definiert ist. IPFIX verwendet UDP-Protokoll, das ein unzuverlässiges Transportprotokoll für den Datenfluss in eine Richtung ist. Da IPFIX das UDP-Protokoll verwendet, führt die Einhaltung des IPFIX-Standards dazu, 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 andere Erkenntnisse. Für die Citrix ADC-Version ab **12.0 bis zur neuesten Version** können Sie entweder Logstream oder IPFIX als Transportmodus auswählen.

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

So verwenden Sie Logstream als Kommunikationsmodus beim Aktivieren von Analysen auf Citrix ADM:

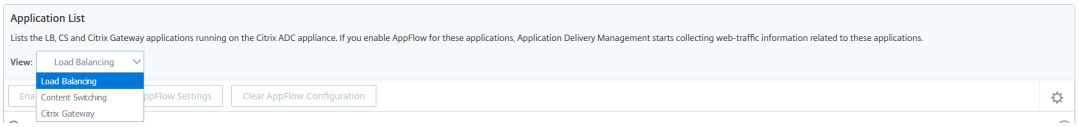
1. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie die NetScaler ADC-Instanz aus, für die Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.



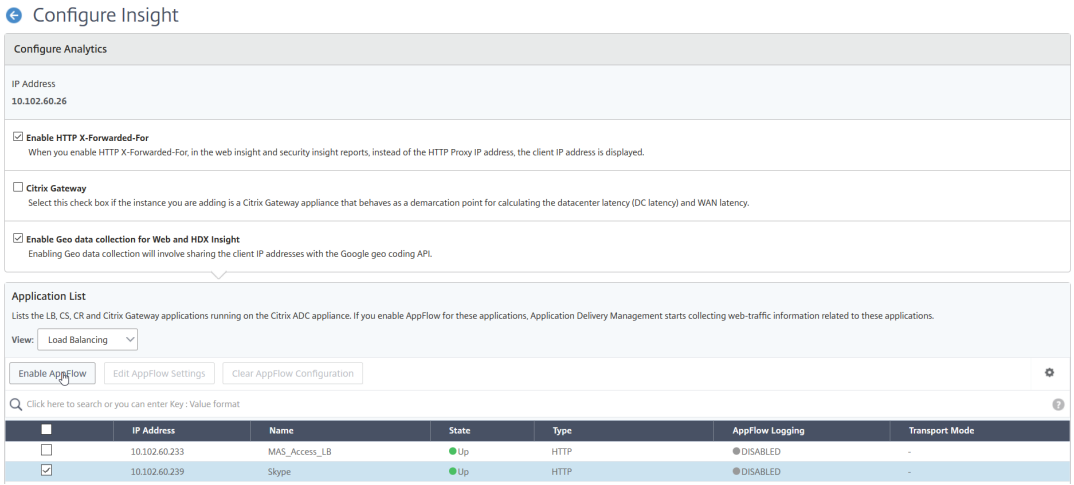
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.



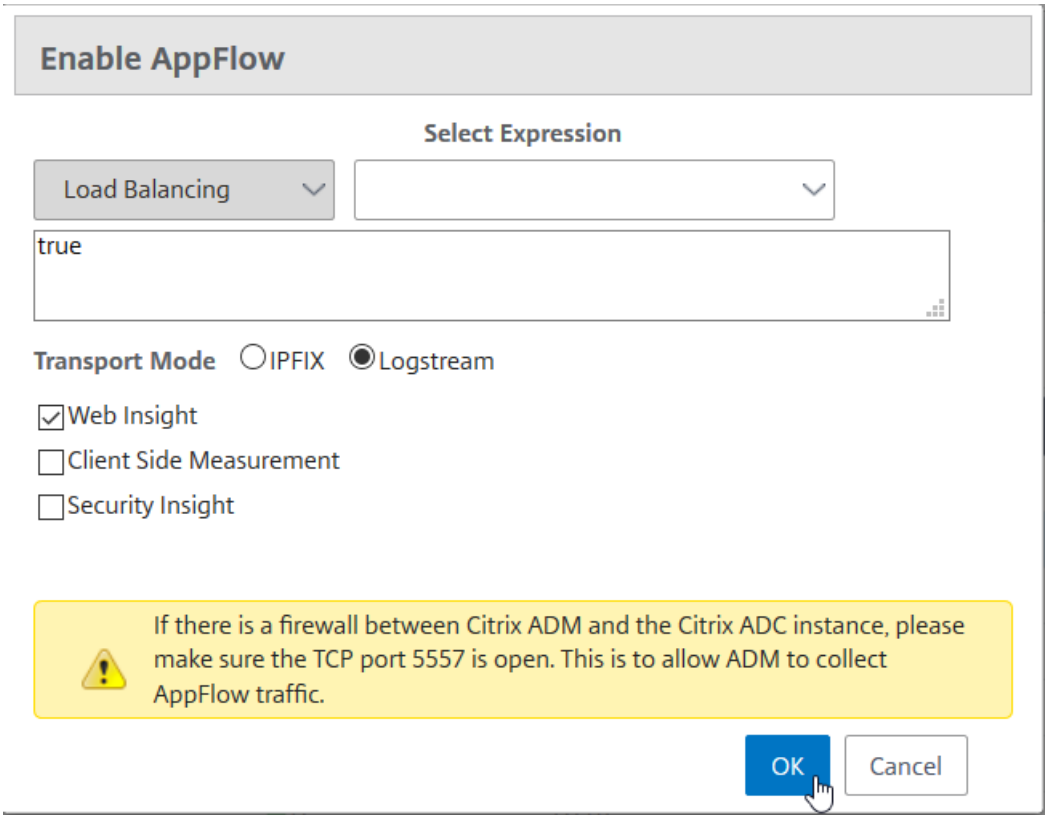
4. Gehen Sie im Dialogfeld “AppFlow aktivieren”wie folgt vor:

   - Geben Sie **true** in das Textfeld ein
   - Wählen Sie **Logstream** als Transportmodus

     > **Hinweis**
     >
     > Citrix empfiehlt, Logstream als Transportmodus auszuwählen.

   - Wählen Sie den Insight-Typ aus und klicken Sie auf **OK** .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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	•	•

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

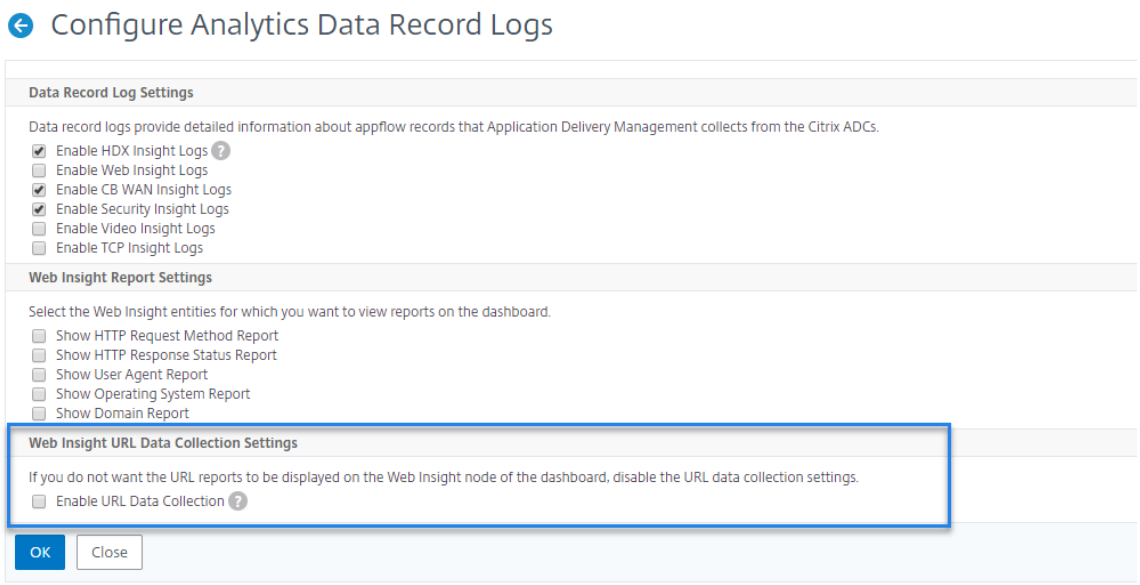
URL-Datenerfassung deaktivieren

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 empfangen Sie Benachrichtigungen über verschiedene Kanäle wie E-Mail, Pufferzeit oder SMS, wenn der Schwellenwert überschreitet.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

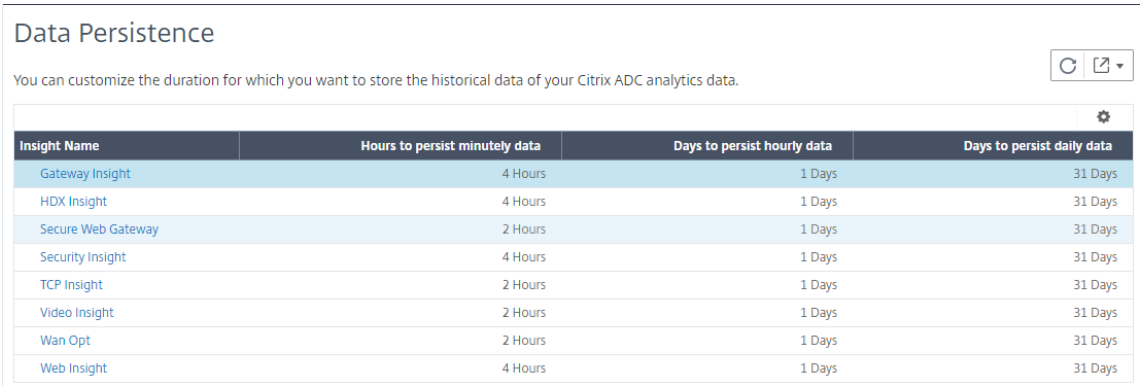
Wenn Sie Datenbankpersistenz in Citrix Application Delivery Management (ADM) konfigurieren, können Sie die Dauer anpassen, in der Sie die historischen Daten der Citrix ADC Analysedaten speichern möchten. Sie können die folgenden Datenbankpersistenztypen für die historischen Daten Ihrer Analysen wählen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

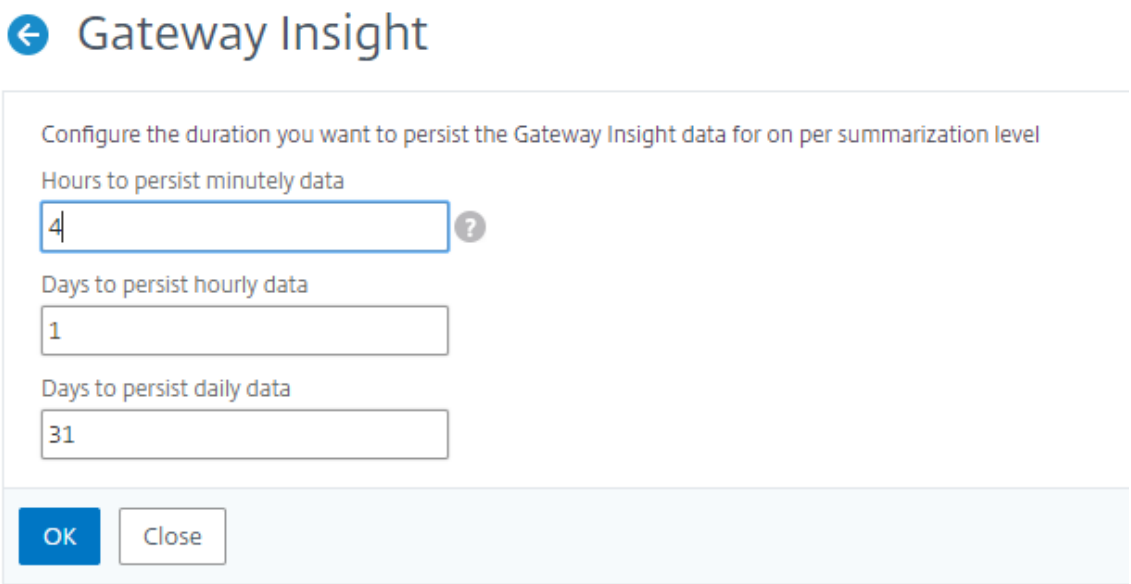
- Stunden, um kleinste Daten zu speichern
- Tage, um die Stundendaten beizubehalten
- Tage, die täglich erfasste Daten erhalten bleiben

So konfigurieren Sie die Datenbankpersistenz

1. Navigieren Sie zu > **Analytics** > **Einstellungen** > **Datenbankpersistenz**.
2. Klicken Sie auf den Insight-Typ, für 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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
- Secure Web Gateway Analytics

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.

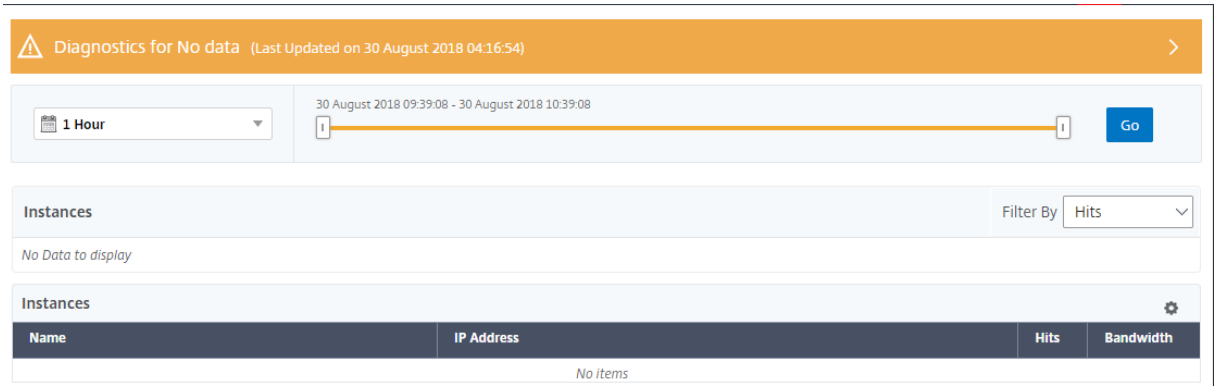
Wenn beispielsweise die AppFlow-Richtlinie nicht an einen virtuellen Server gebunden ist oder ein virtueller Server nicht lizenziert ist, erhält NetScaler ADM nicht die gewünschten Daten für die Web Insight-Überwachung. Die Self-Service-Diagnose identifiziert die Probleme und generiert einen Diagnosebericht. Sie können den Diagnosebericht anzeigen, um die Probleme zu überprüfen und Korrekturmaßnahmen durchzuführen.

Diagnosebericht anzeigen

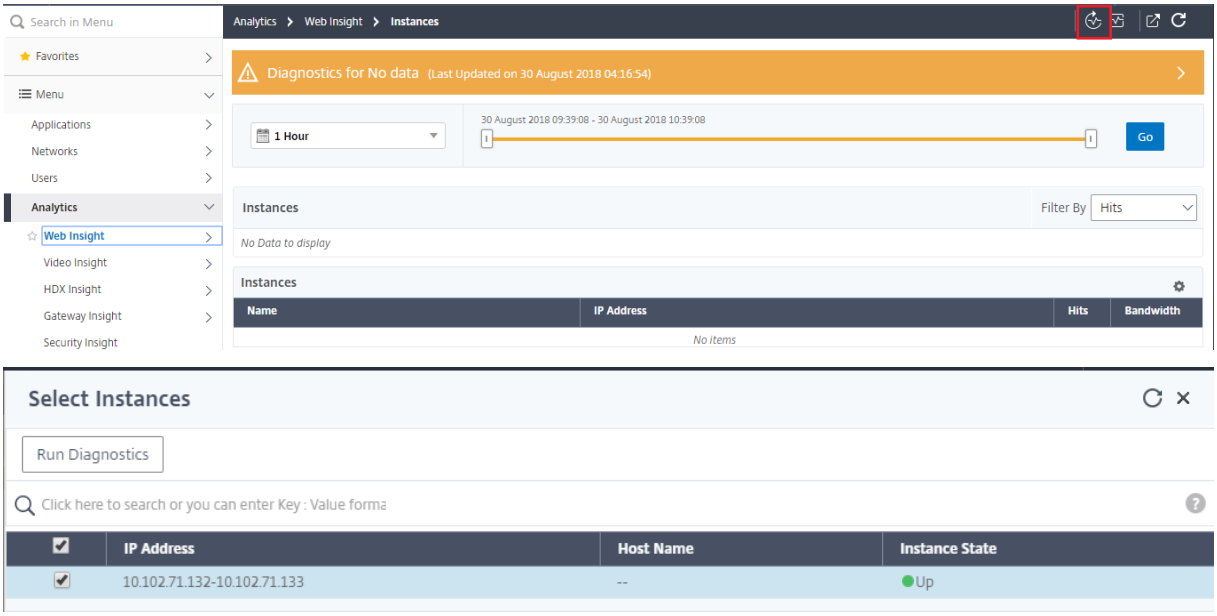
Um die Diagnoseberichte für die angegebenen Analytics-Features anzuzeigen, müssen Sie im Dashboard von NetScaler ADM zum entsprechenden Analytics-Knoten wechseln.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

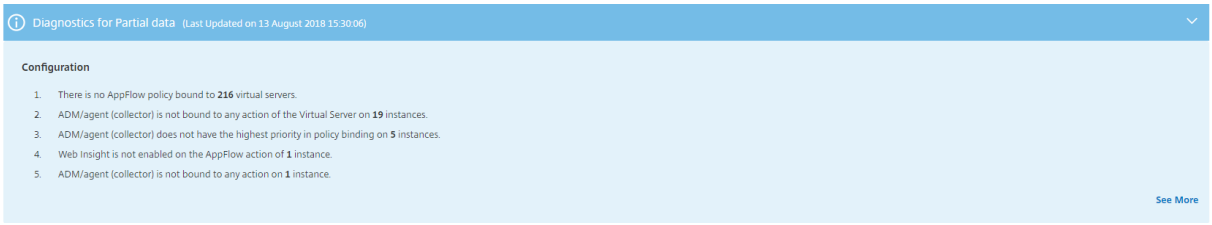
Die Self-Service-Diagnose zeigt den Diagnosebericht je nach Kritikalität der Probleme entweder in orangefarbenem oder blauem Hintergrund an.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

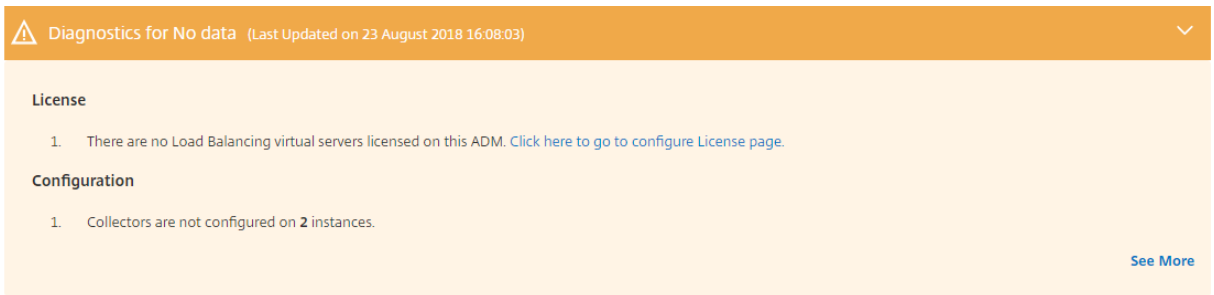


> **WICHTIG**: Die Self-Service-Diagnose überprüft nicht den Verkehrsfluss. Es prüft nur auf Lizenz- oder Konfigurationsprobleme, die mit den angegebenen Analysefunktionen auf den verwalteten Instanzen verbunden sind. Manchmal werden keine Analysedaten angezeigt, da kein aktiver Datenverkehr durch virtuelle 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.

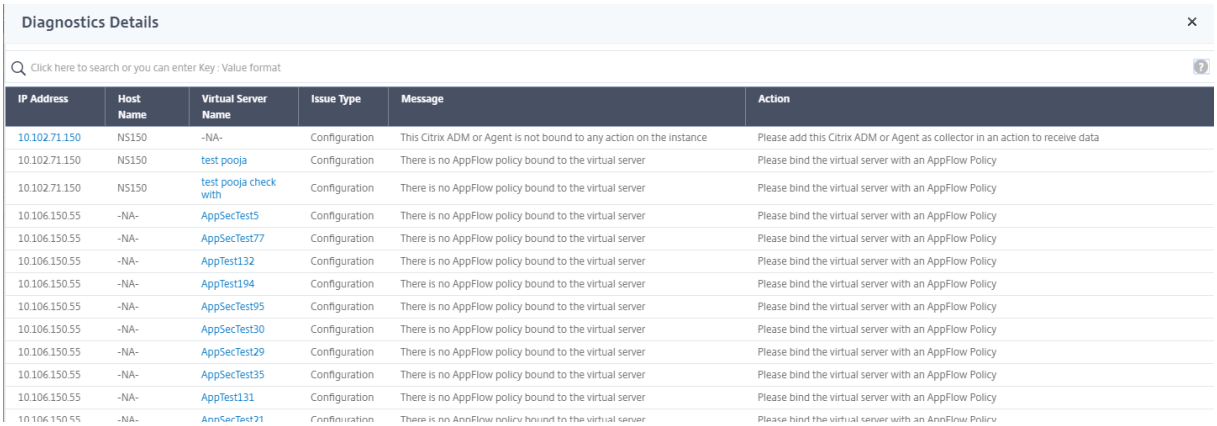
Wenn beispielsweise keine virtuellen Lastenausgleichsserver auf Ihrem NetScaler ADM lizenziert sind, enthält die Übersichtsseite einen Hyperlink, der Sie zur Seite "**Systemlizenzen** "weiterleitet.



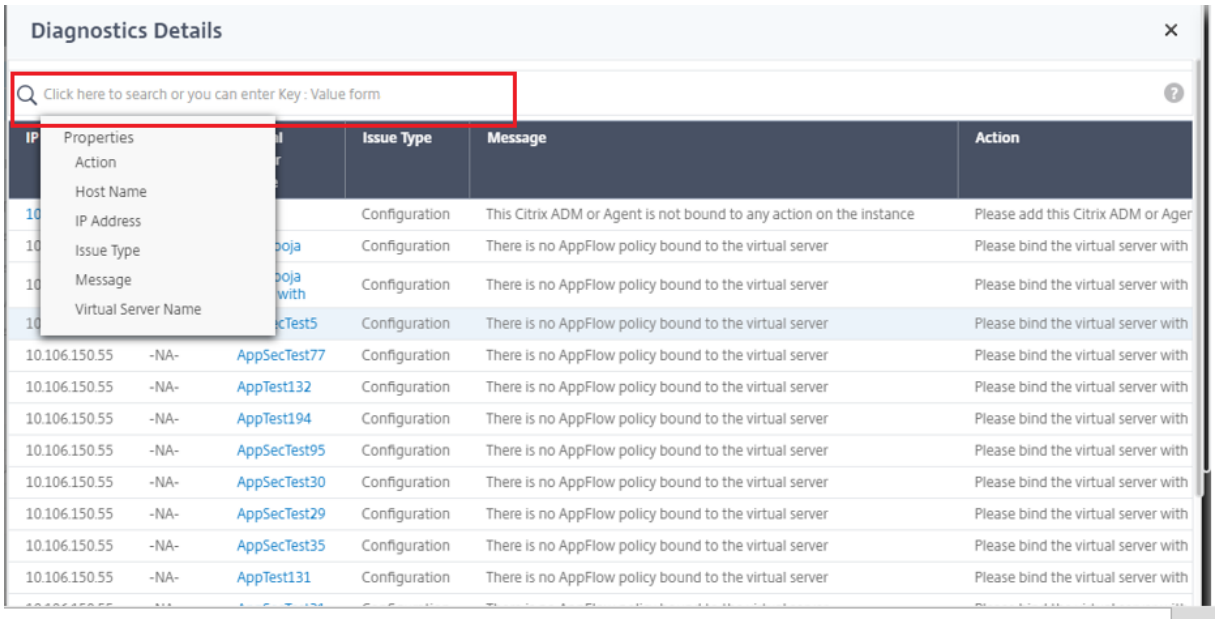
Um detaillierte Informationen zu den Problemen anzuzeigen, klicken Sie auf der Übersichtsseite auf **Mehr** anzeigen.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

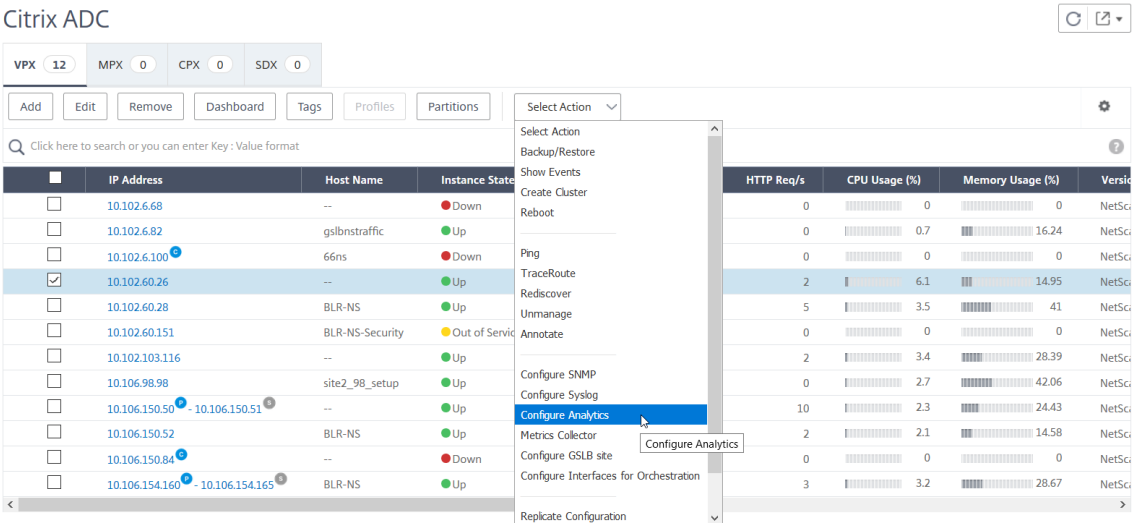
Im Folgenden finden Sie einige der Anwendungsfälle, die Sie mit Web Insight anzeigen können:

- 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
- Wenige Seiten einer Anwendung sind langsam von einem bestimmten Client und vom Backend-Server
- Anwendung ist langsam, wenn von einem bestimmten Client und vom Backend-Server aus zugegriffen wird

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:

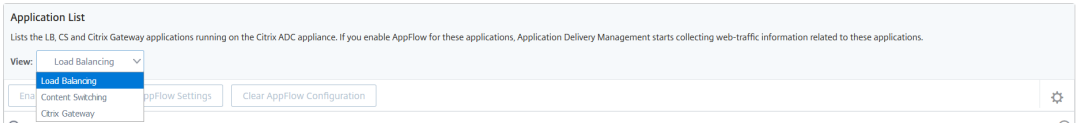
1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler ADC**, und wählen Sie die NetScaler ADC-Instanz aus, für die Sie die Analyse aktivieren möchten.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

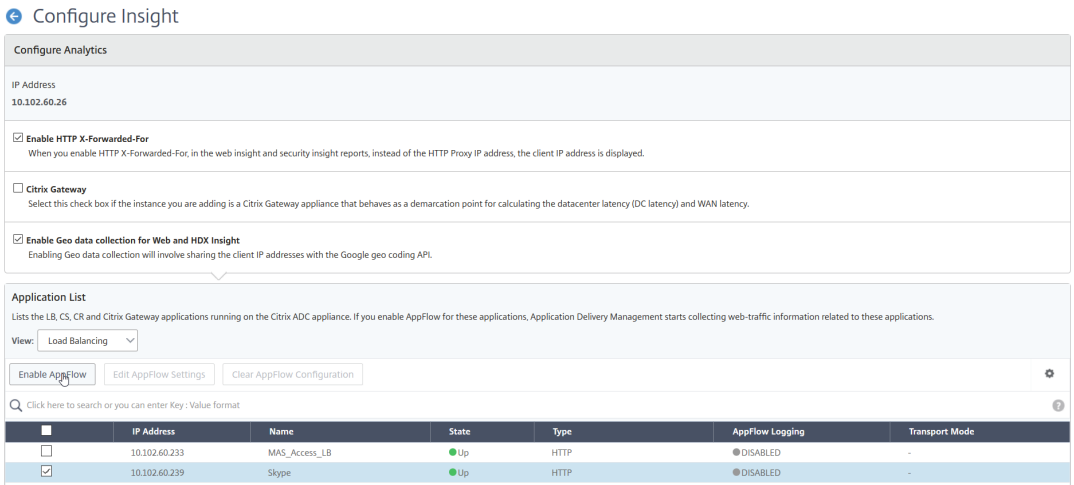


4. Gehen Sie auf der Seite **“Insight konfigurieren** “wie folgt vor:

   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**.



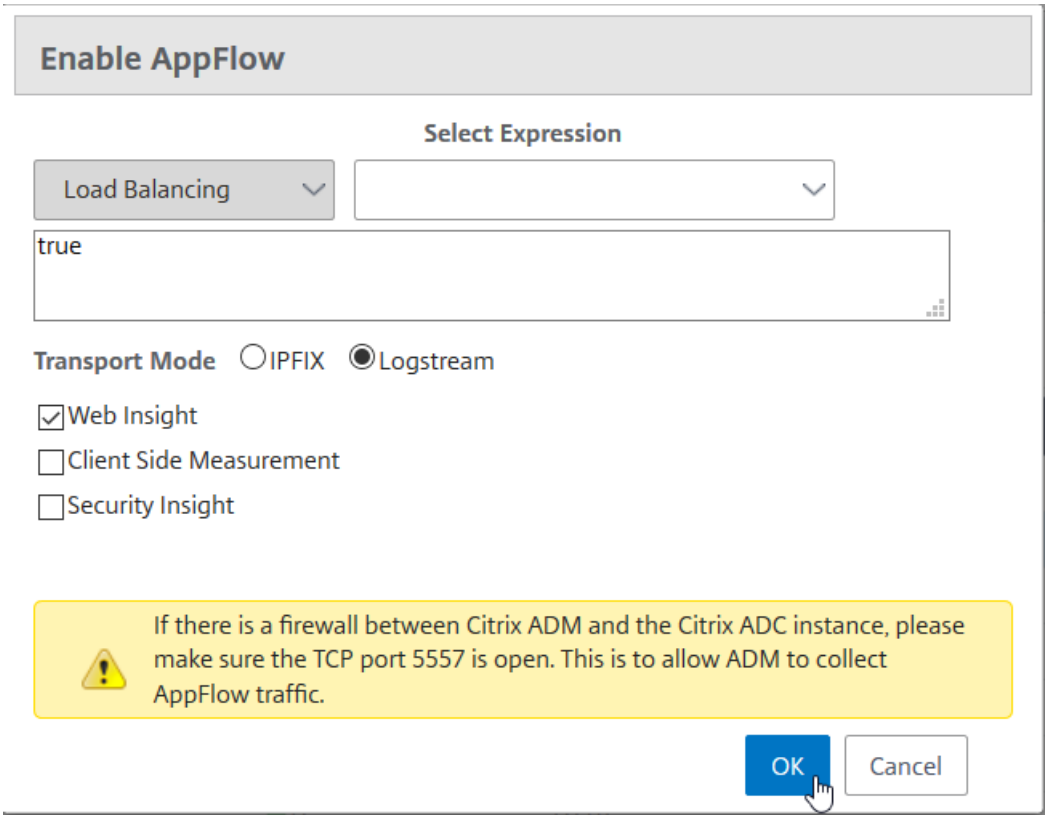
5. Gehen Sie im Dialogfeld “AppFlow aktivieren”wie folgt vor:

   - 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

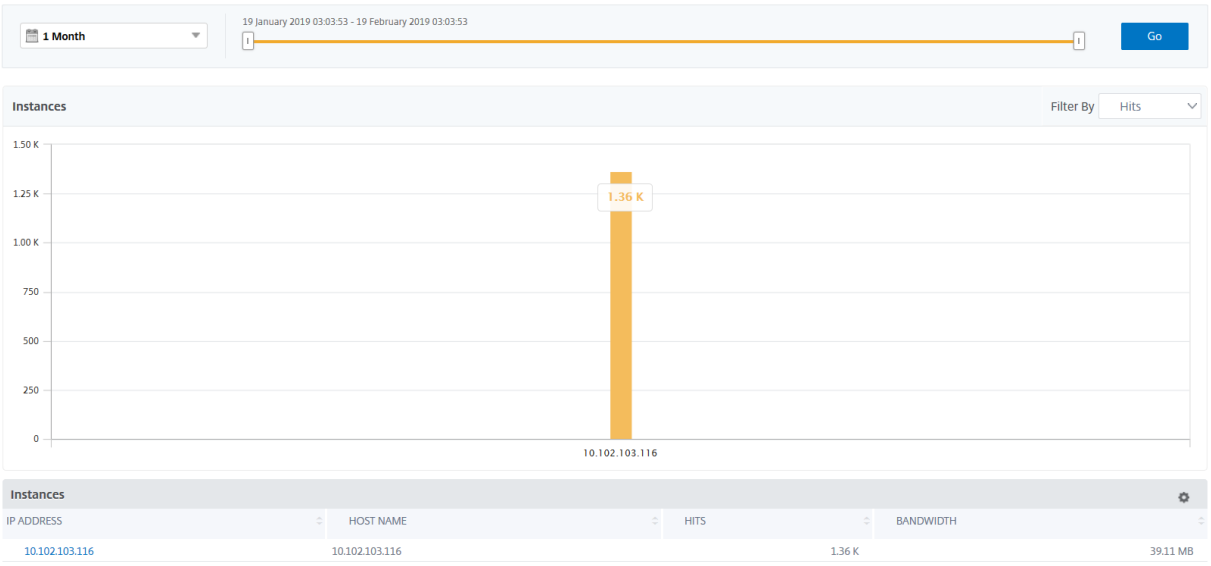


Analysieren von Problemen mit Webanwendungen

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.

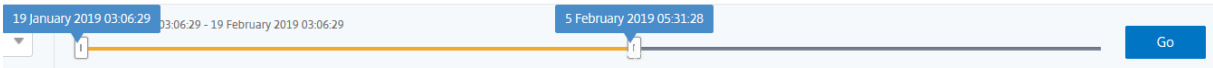
Wenn Sie zu **Analytics** > **Web Insight** navigieren, werden die NetScaler ADC-Instanzen angezeigt, die mit Web Insight aktiviert sind. Sie können detaillierte Informationen zu den Instanzen wie IP-Adresse, Hostname, Gesamtzahl der Treffer und Bandbreite anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



In der Liste können Sie die Zeitdauer auswählen, um die Einblicke für die Instanzen anzuzeigen.

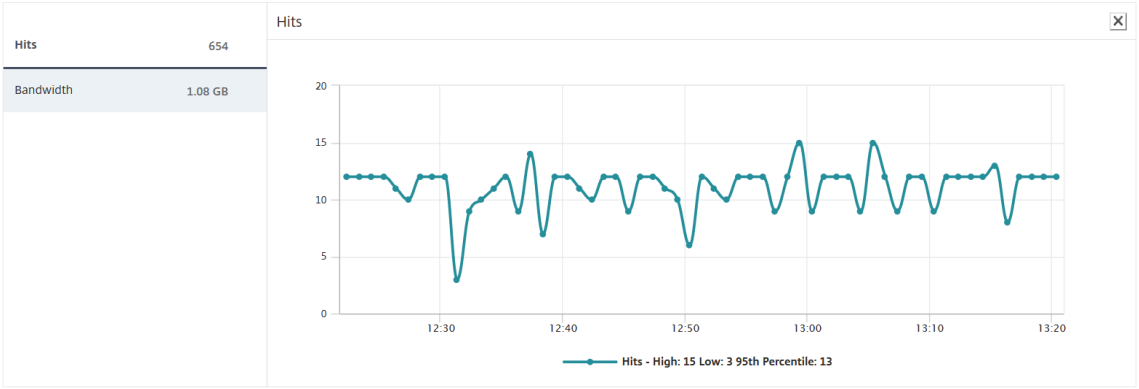
Sie können den Schieberegler auch verwenden, um die Zeitdauer anzupassen, und klicken Sie auf **Los**, um die Ergebnisse anzuzeigen.



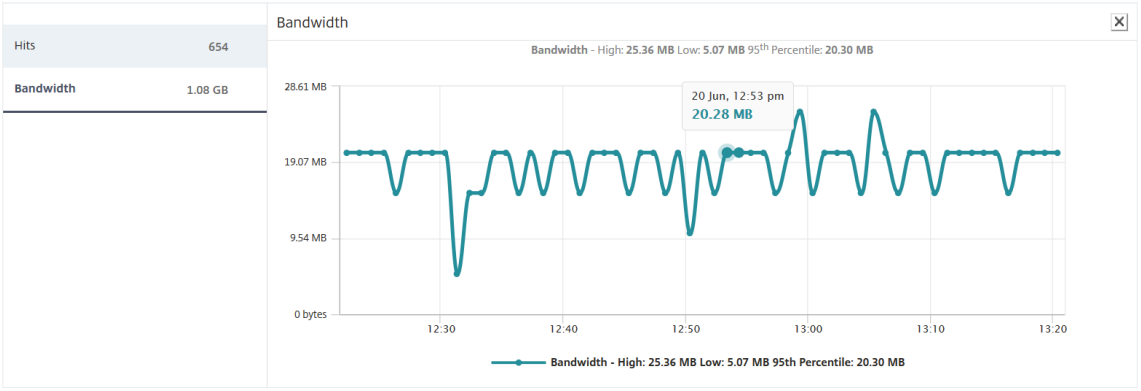
Wenn Sie auf das Diagramm oder die IP-Adresse der Instanz klicken, werden die detaillierten Informationen zur Instanz angezeigt. Sie können Einblicke für Folgendes anzeigen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

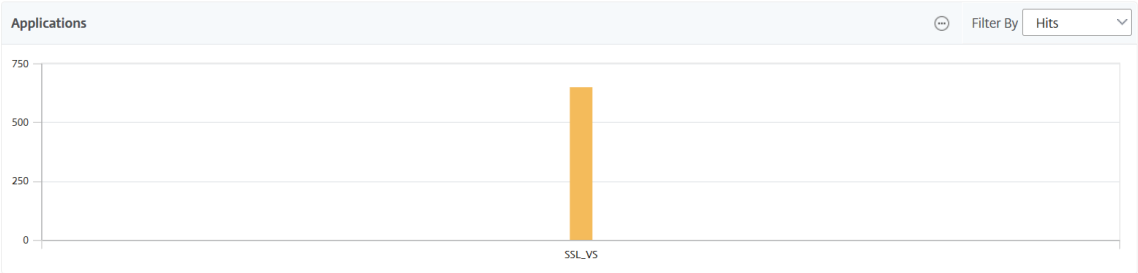
- **Gesamtzahl der Treffer**



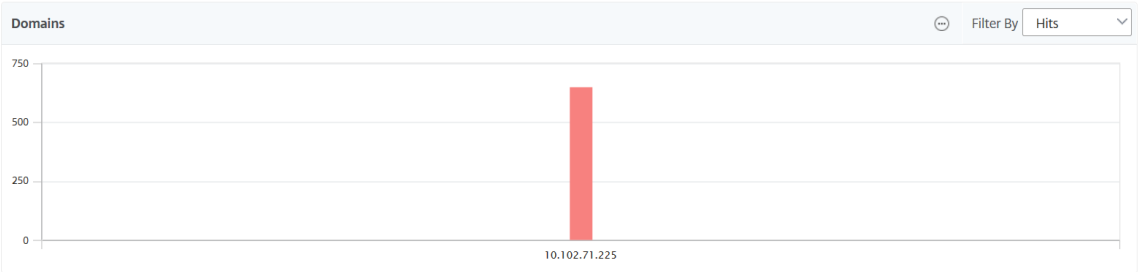
- **Bandbreite**



- **Anwendungen**

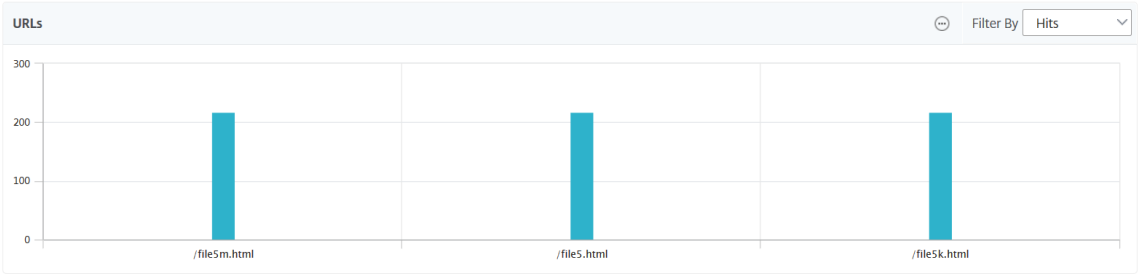


- **Domänen**

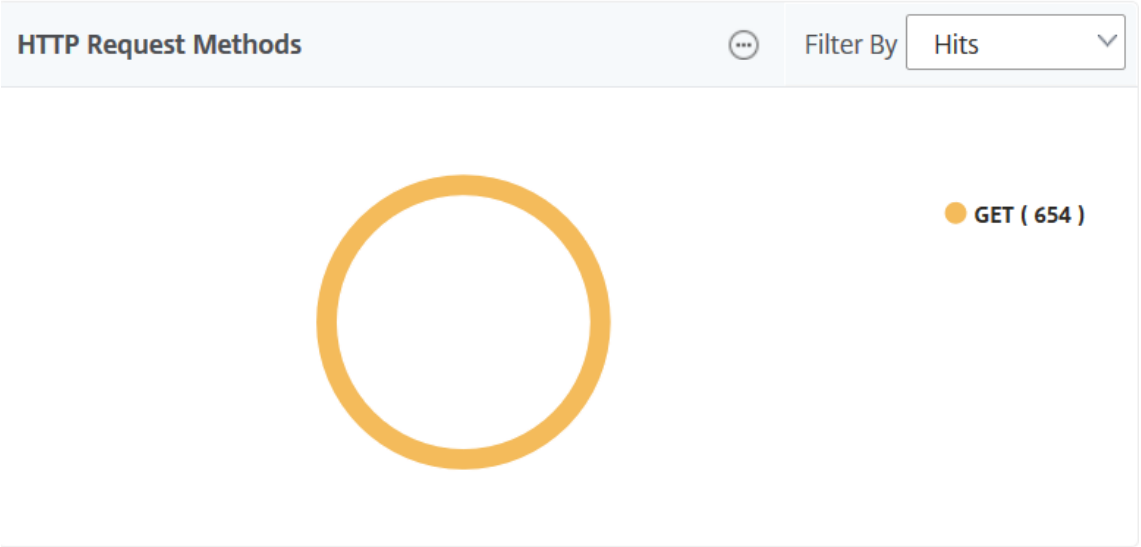


- **URLs**

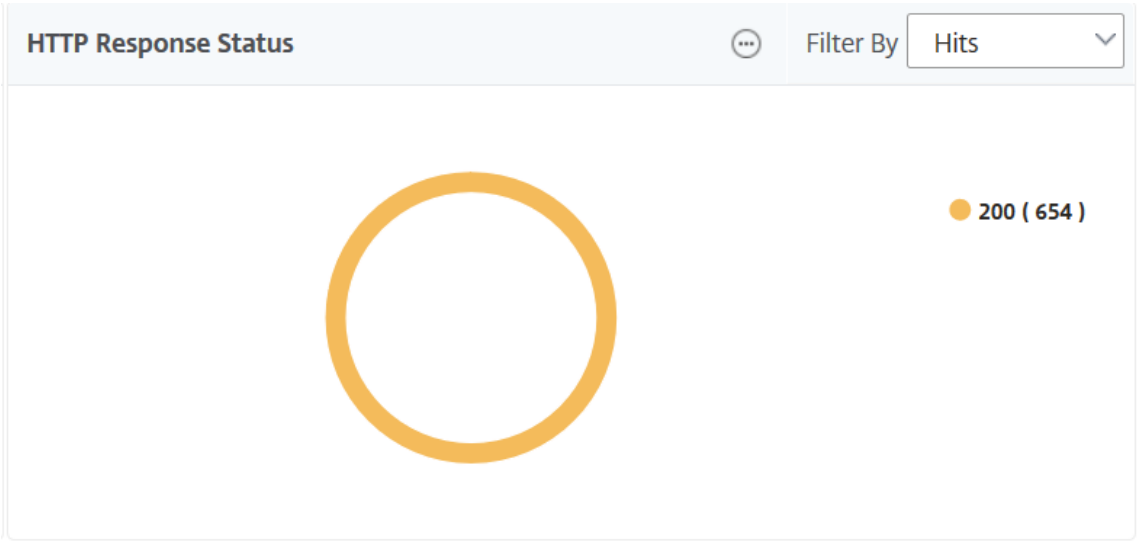
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **HTTP-Anforderungsmethoden**

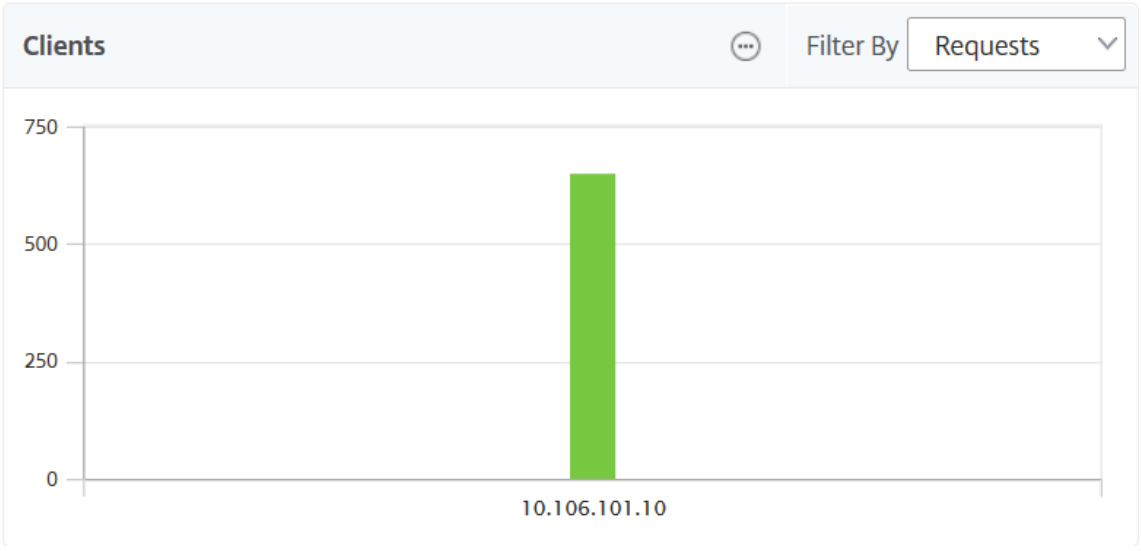


- **HTTP-Antwortstatus**

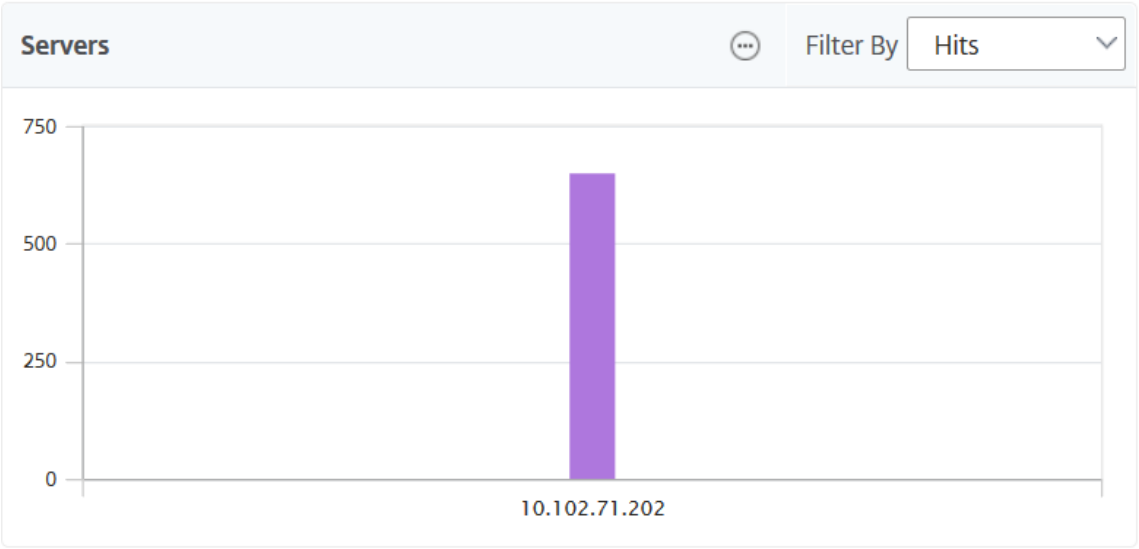


- **Clients**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

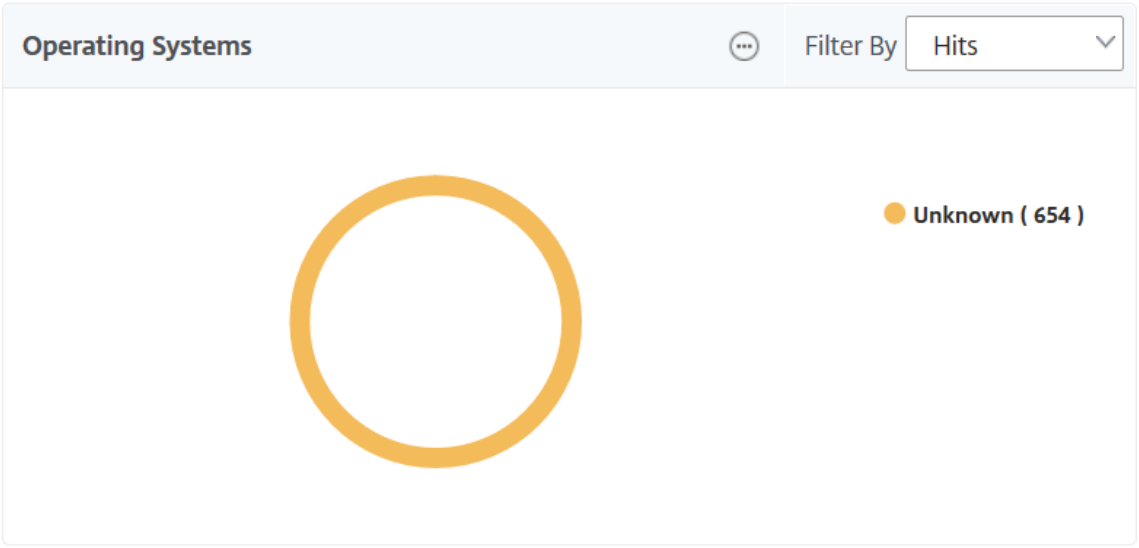


- **Server**

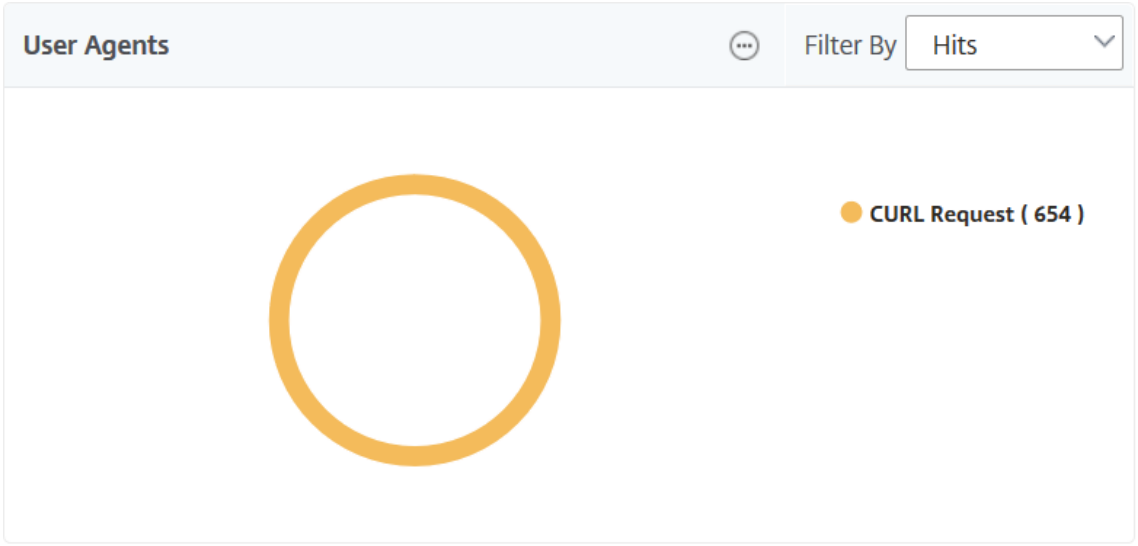


- **Betriebssysteme**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



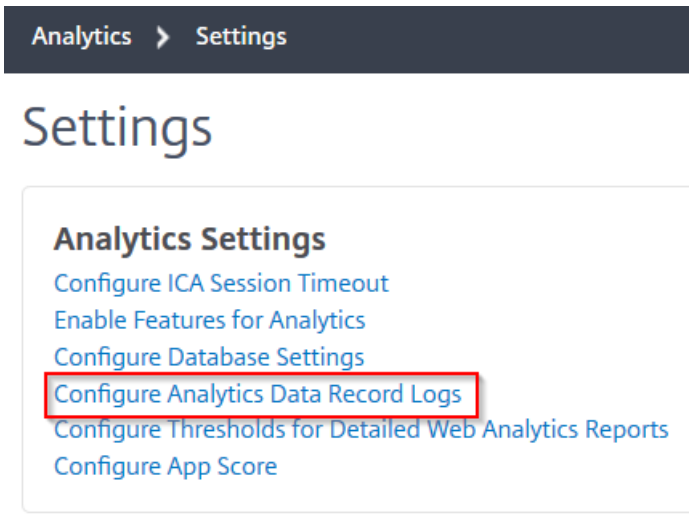
- **Benutzeragents**



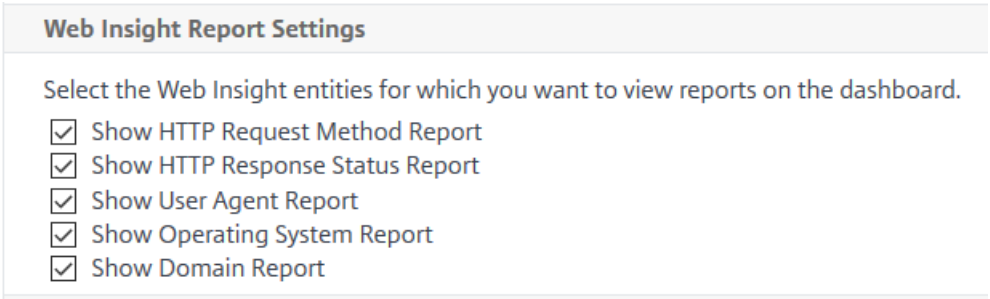
Sie können auch **Web Insight-Entitäten** auswählen, für die Sie Berichte auf der GUI anzeigen möchten.

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Einstellungen**.
2. Klicken Sie auf **Analytics-Datensatzprotokolle konfigurieren**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Wählen Sie unter **Web Insight-Berichtseinstellungen**die Entitäten aus, die Sie Berichte auf der GUI anzeigen möchten.



4. Klicken Sie auf **OK**.

Um einen Drilldown für weitere Analysen durchzuführen, können Sie in der GUI unter Web Insight auf jede Einsichtskategorie 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

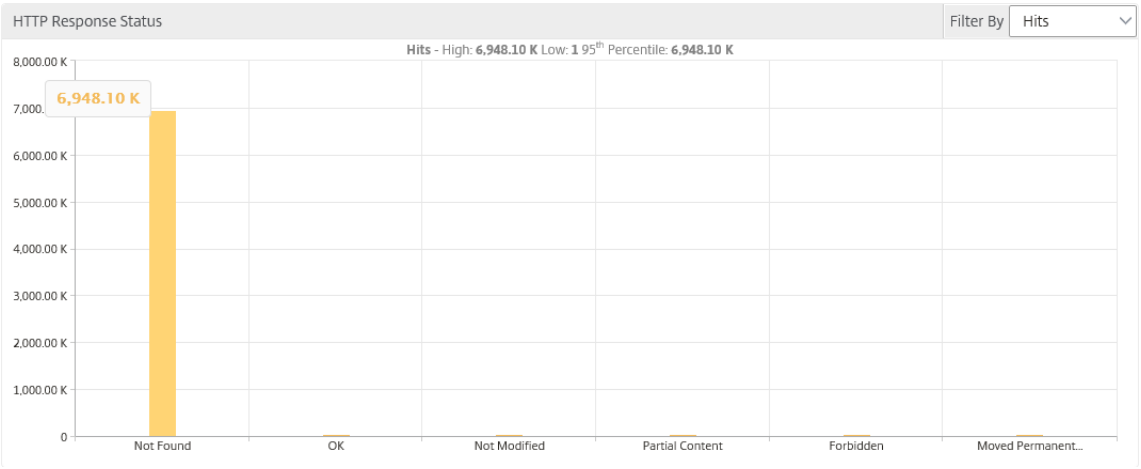
Betrachten Sie ein Szenario, dass Ihre Benutzer Unzugänglichkeit Fehler 500 für Ihre Webanwendung haben. Der Fehler 500 (Not Found) ist HTTP-Antwortstatusfehler, der auf ein Problem auf dem Webserver hinweist, aber der Server gibt das Problem nicht explizit an. So identifizieren und aufgliedern Sie das eigentliche Problem:

1. Navigieren Sie zu **Analytics** > **Web Insight** > **Antwortstatus**.

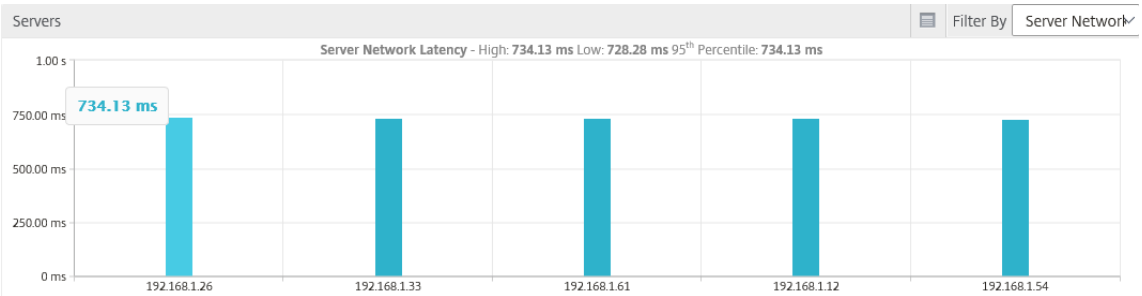
   Die Dashboard-Seite wird angezeigt. Das Dashboard stellt Ihnen die Metriken zur Verfügung, mit denen Sie den Erfolg und Fehler der verarbeiteten HTTP-Transaktionen analysieren können.

2. Klicken Sie im Diagramm auf **Nicht gefunden**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

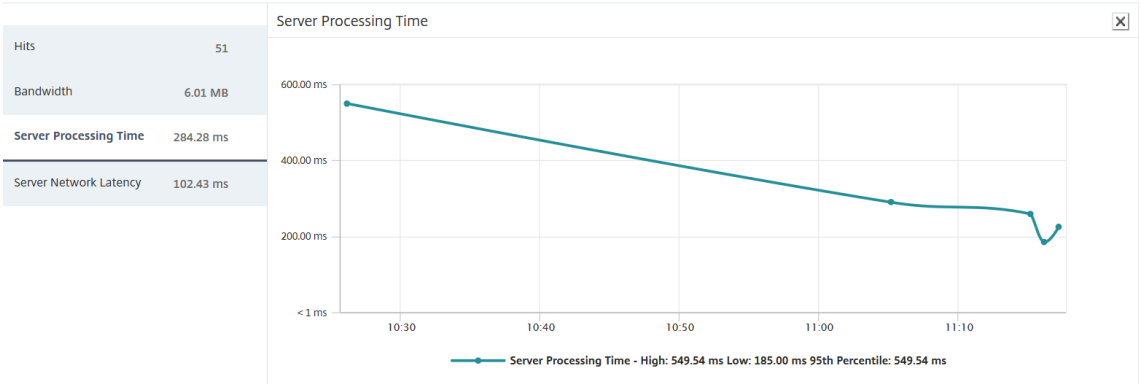
- Anzahl der Anforderungen in der Warteschlange.
- Die Bandbreite, die von jeder Anforderung zur Verarbeitung der HTTP-Transaktion belegt wird.

  Das Serverdiagramm kann Ihnen helfen, die Verarbeitungszeit jedes Servers für die von den

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Servern verarbeitete Anforderung zu verstehen. Ebenso zeigt das Anwendungsdiagramm die Treffer, die Antwortzeit und die Bandbreite an, die von jeder HTTP-Transaktion belegt wird.

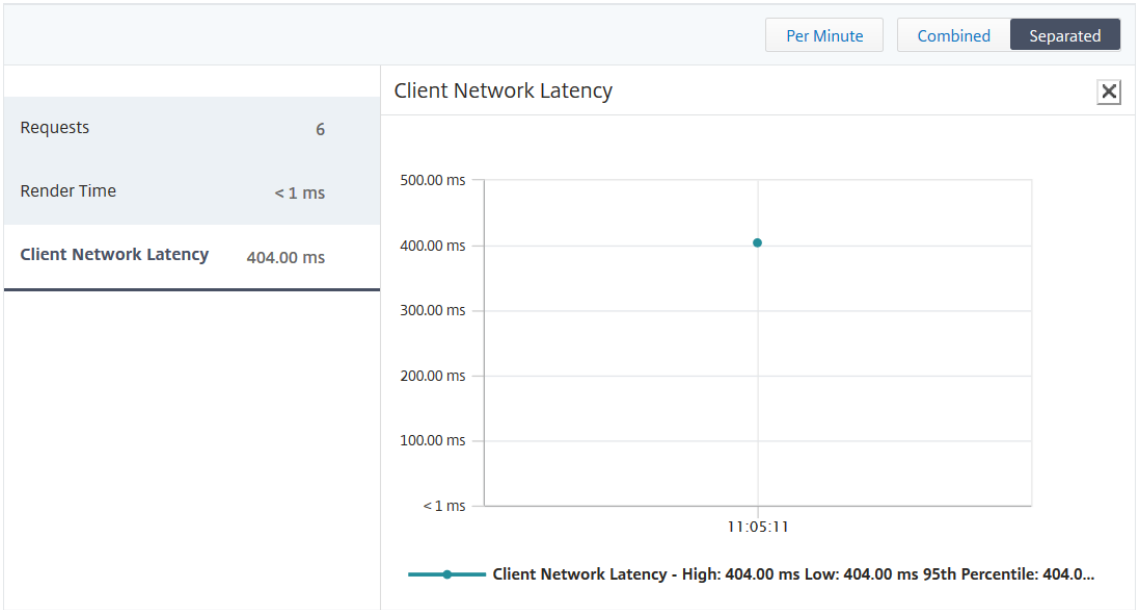
1. Navigieren Sie zu **Analytics** > **Web Insight** > **Server**.
2. Wählen Sie den Server aus dem Diagramm aus.
3. Klicken Sie auf **Serververarbeitungszeit**, um die Verarbeitungszeit des Servers zu analysieren.



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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In diesem Beispiel können Sie als Administrator sehen, dass die Ursache des Problems aus dem Clientnetzwerk stammt, da die Clientnetzwerklatenz eine hohe Latenz anzeigt.

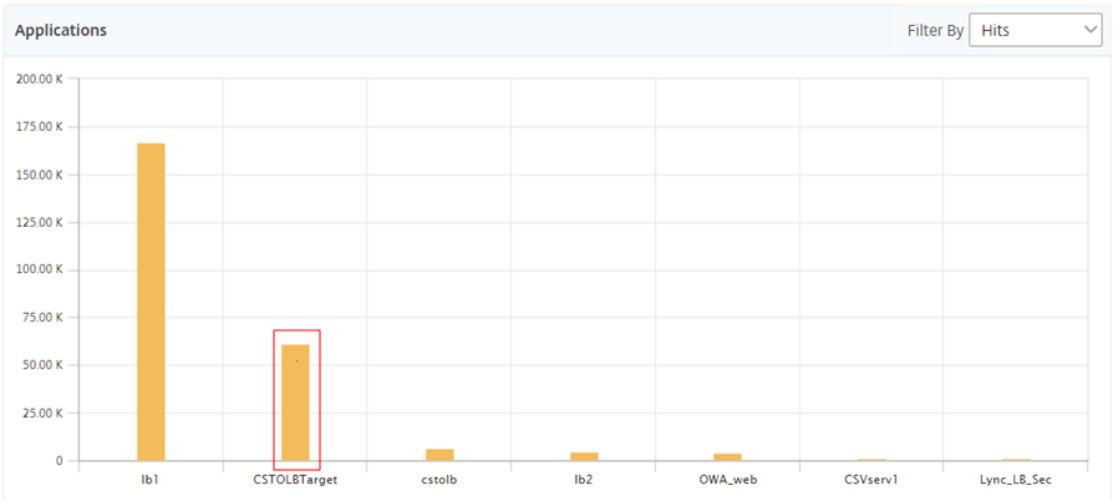
Anwendungsfall 3 - Langsamkeit beim Zugriff auf die Webanwendung

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

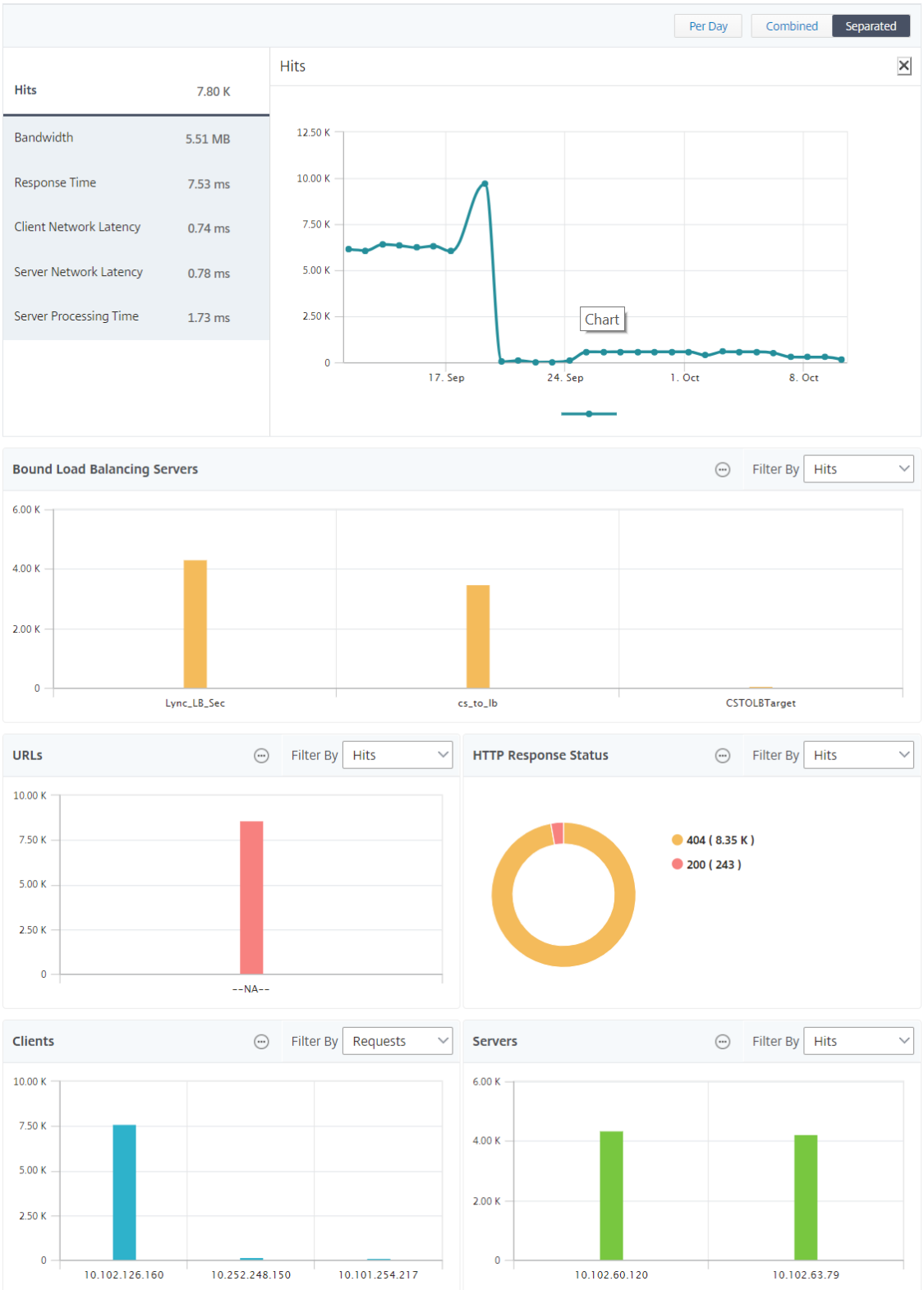


Applications

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

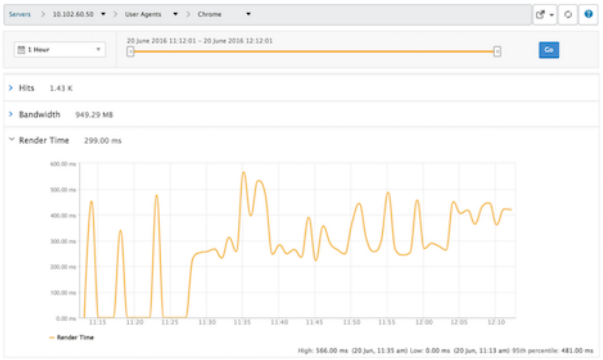
Sie können weiter auf die gebundenen Lastausgleichsserver klicken, um die Web Insight-Details dieser Anwendungen anzuzeigen.

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 vornehmen, um festzustellen, welche Anwendungsseiten mit der höchsten Rendering-Zeit für diesen Browser verknüpft sind.

Sie können beispielsweise Google Chrome auswählen und die entsprechenden Rendering-Zeiten für die verschiedenen URL-Seiten für eine bestimmte Anwendung anzeigen.



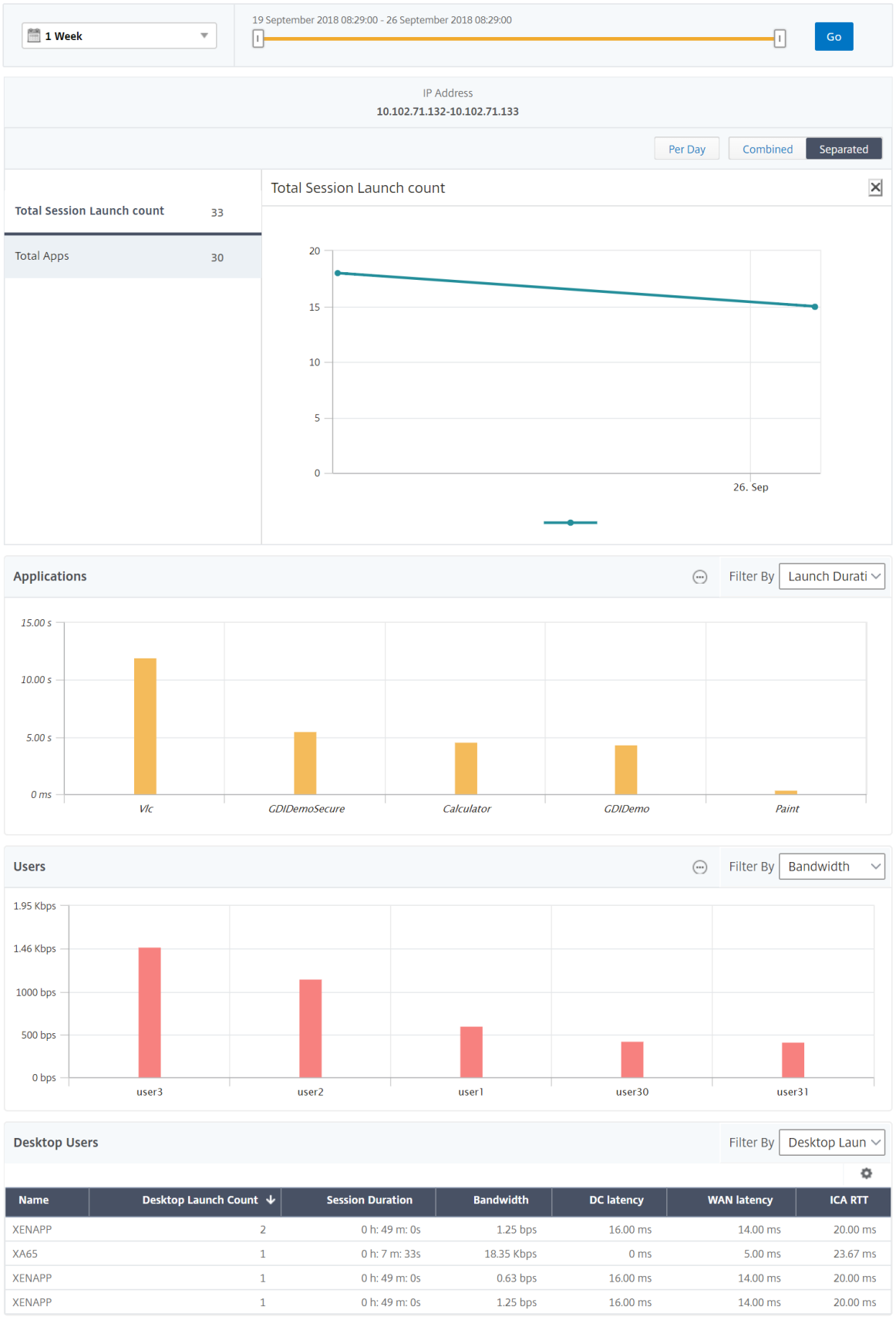
NetScaler ADC-Instanzen, die im Hochverfügbarkeitsmodus bereitgestellt werden

Citrix ADM stellt Berichte für ADC-Instanzen bereit, die im Hochverfügbarkeitsmodus bereitgestellt werden. Aggregierte Berichte für Instanzen im Hochverfügbarkeitsmodus werden in allen Analysen unterstützt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können auf den Namen der Instanzen klicken, die sich in hoher Verfügbarkeit befinden, um weitere Details anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

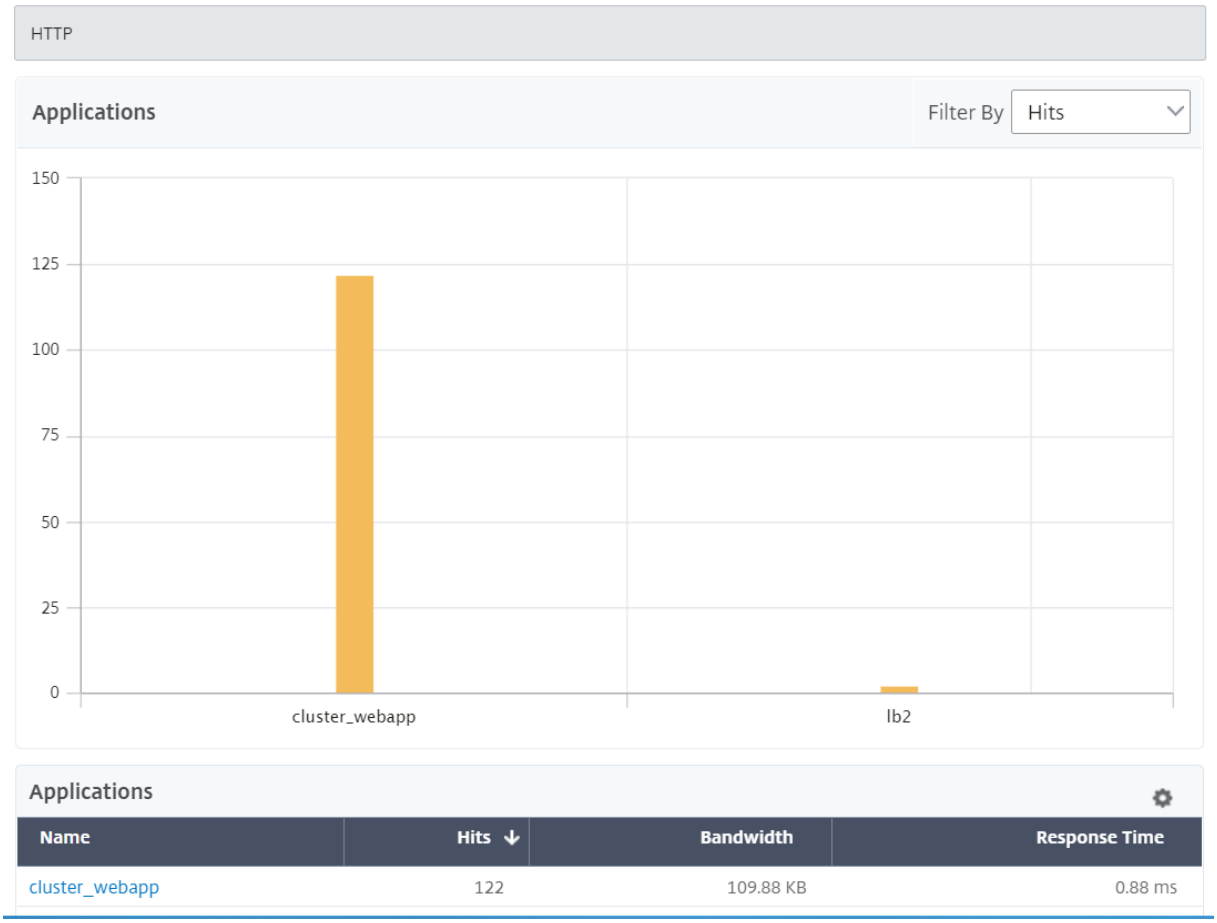


Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

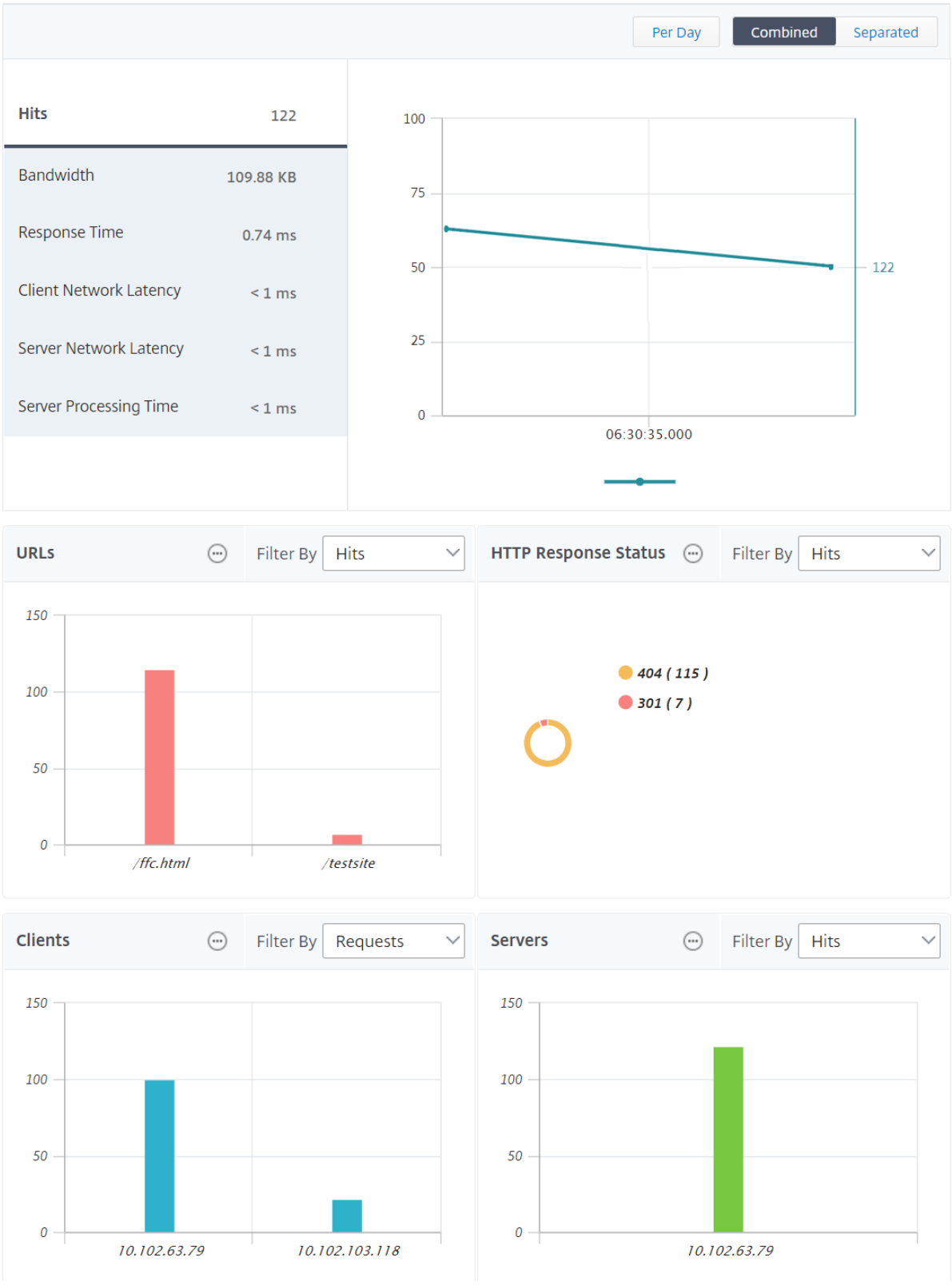
NetScaler ADC-Instanzen, die im Clustermodus bereitgestellt werden

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hinweis

- Alle Daten, die zuvor vor dem Upgrade auf Citrix ADM 12.1 Build 503.x gesammelt wurden, werden weiterhin als unabhängige Berichte für den Zeitraum angezeigt, bis die Daten weiterhin bestehen.
- Bei ADC-Instanzen, die im Clustermodus bereitgestellt werden, werden Observation Domain ID/Observation Domain Names durch CLIP Hostname und CLIP ersetzt. Alle zuvor gesammelten Daten melden weiterhin Observation Domain ID/Observation Domain Name.

Web Insight-Geomap-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.

Geomap bietet Informationen zu den folgenden Kennzahlen, die für ein Land, ein Bundesland 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.

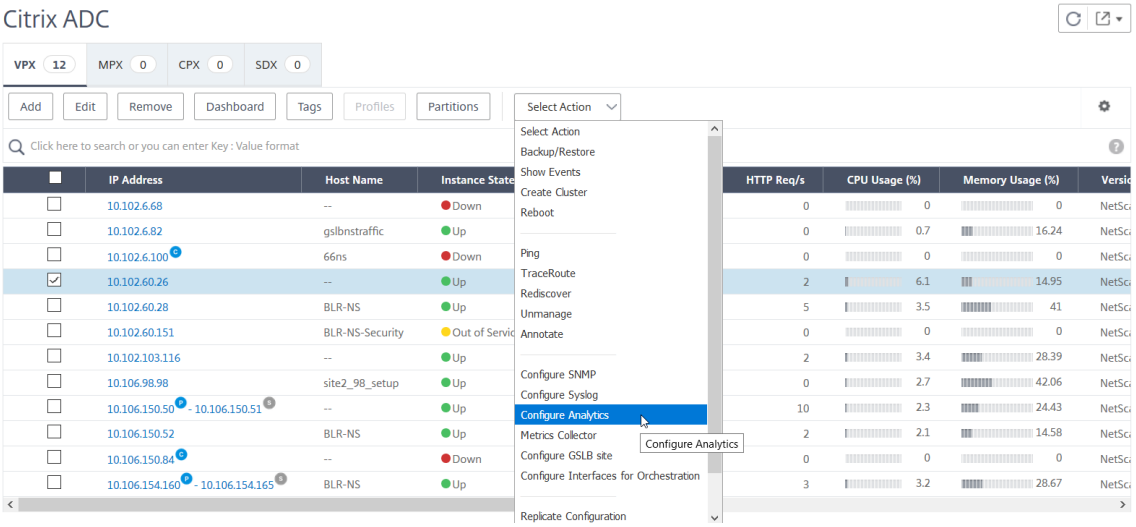
Konfigurieren von Geomaps für private IP-Adressen

Um den Webanwendungsdatenverkehr anzuzeigen, der von privaten IP-Adressen auf der Geomap stammt, müssen Sie zuerst private IP-Adressblöcke erstellen und dann die Geodatenerfassung aktivieren.

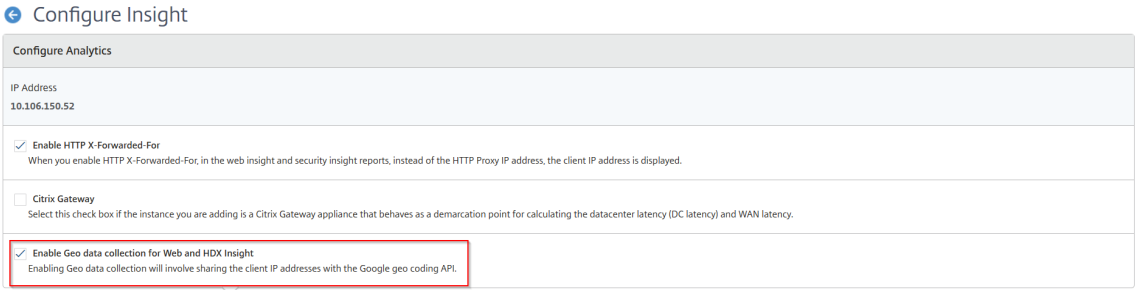
So aktivieren Sie die Geo-Datenerfassung:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

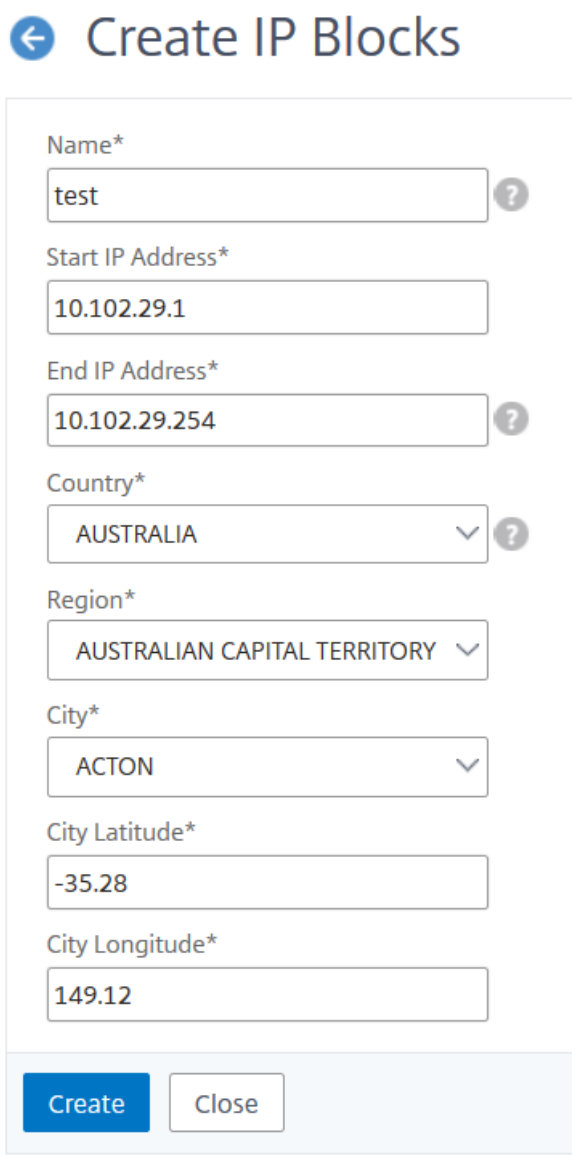
So erstellen Sie einen IP-Block:

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

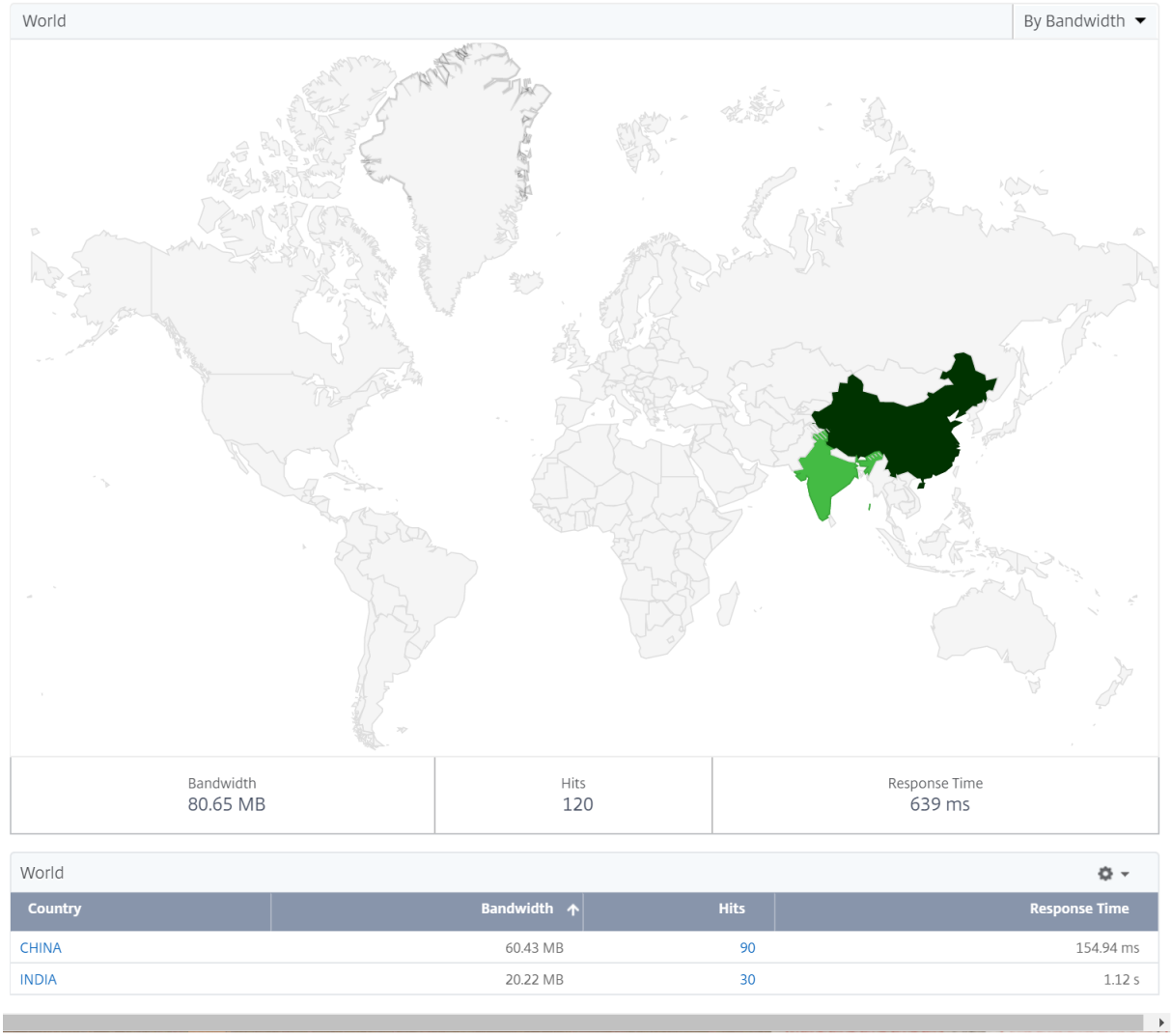
3. Klicken Sie zum Abschluss auf **Erstellen**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Für die Verwendung des öffentlichen IP-Blocks ist die einzige Voraussetzung, dass Sie die Geodatenerfassung aktivieren auf der Seite Insight konfigurieren aktivieren müssen.

> 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

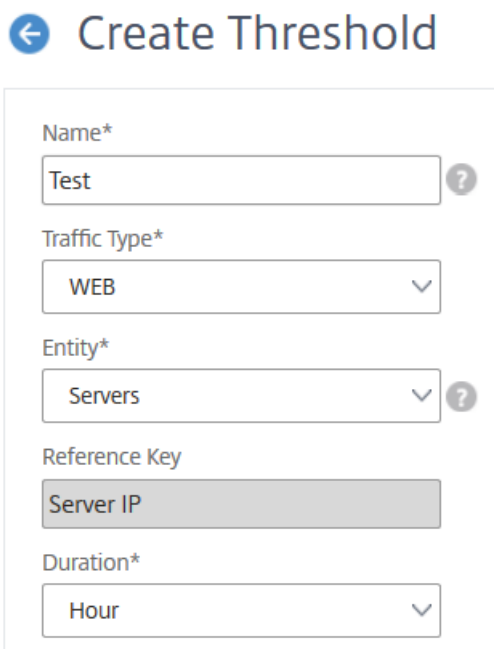
   b) **Traffic Type** - Wählen Sie in der Liste WEB aus.

   c) **Entity** - Wählen Sie in der Liste die Kategorie oder den Ressourcentyp aus. Standardmäßig wird “Anwendungen”als Entität ausgewählt.

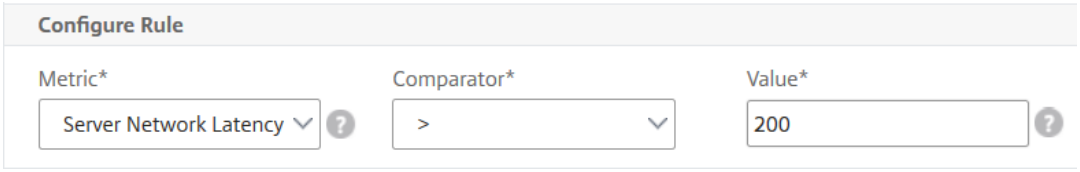
   d) **Referenzschlüssel** - Ein Referenzschlüssel wird automatisch basierend auf dem ausgewählten Datenverkehrstyp und der ausgewählten Entität generiert.

   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.

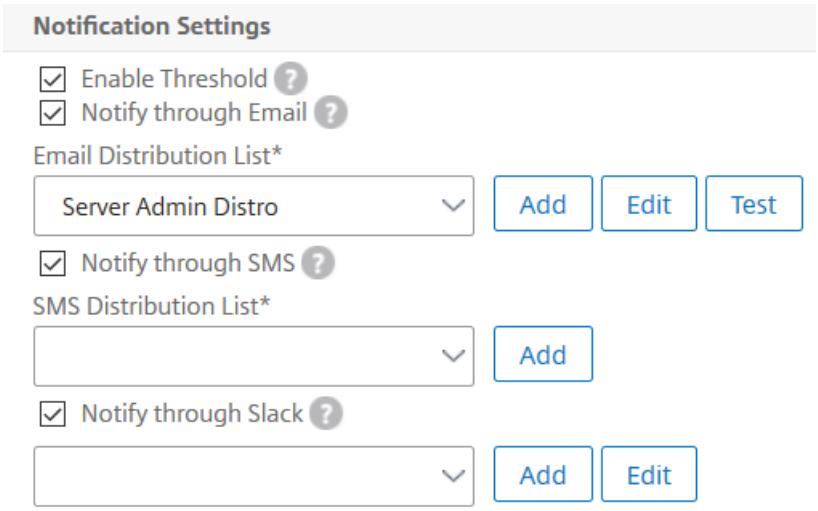
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX Insight

February 5, 2024

HDX Insight bietet End-to-End-Sichtbarkeit für HDX-Datenverkehr zu Citrix Virtual Apps and Desktops, der über NetScaler ADC geleitet wird. Darüber hinaus können Administratoren Echtzeitmetriken für Client- und Netzwerklatenz, historische Berichte, End-to-End-Performance-Daten anzeigen und Leistungsprobleme beheben. Die Verfügbarkeit von Echtzeit- und historischen Sichtbarkeitsdaten ermöglicht es 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-Roundtrip-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 durchgeführt hat. Weitere Informationen umfassen mehrere Latenzstatistiken und während der Sitzung verbrauchte Bandbreite. Sie können auch Bandbreiteninformationen von einzelnen virtuellen Kanälen wie Audio, Druckerzuordnung und Clientlaufwerkzuordnung abrufen.

Sie können auch 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

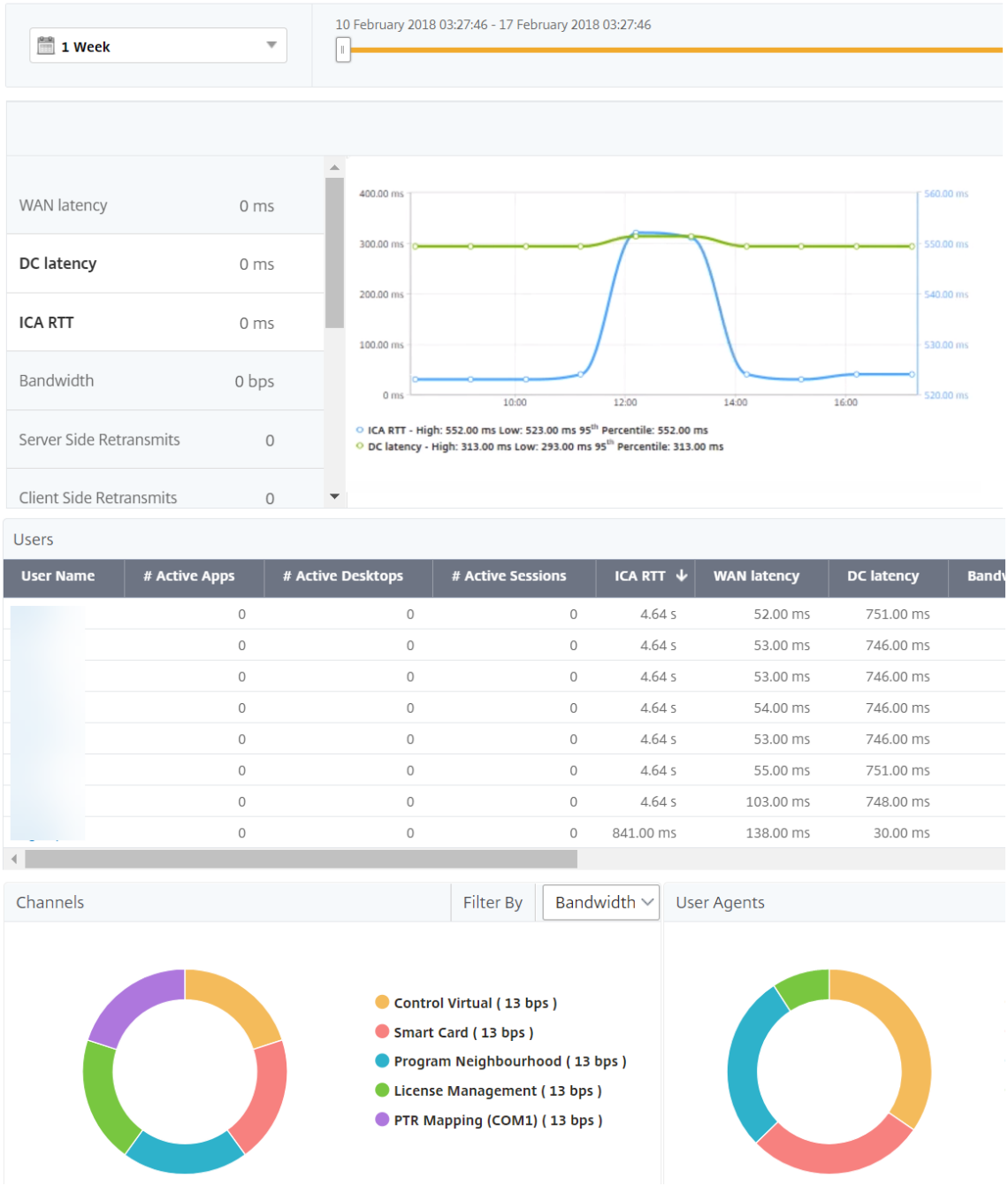
Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

- WAN-Latenz
- DC-Latenz
- Hostverzögerung

So zeigen Sie die Client-Metriken an:

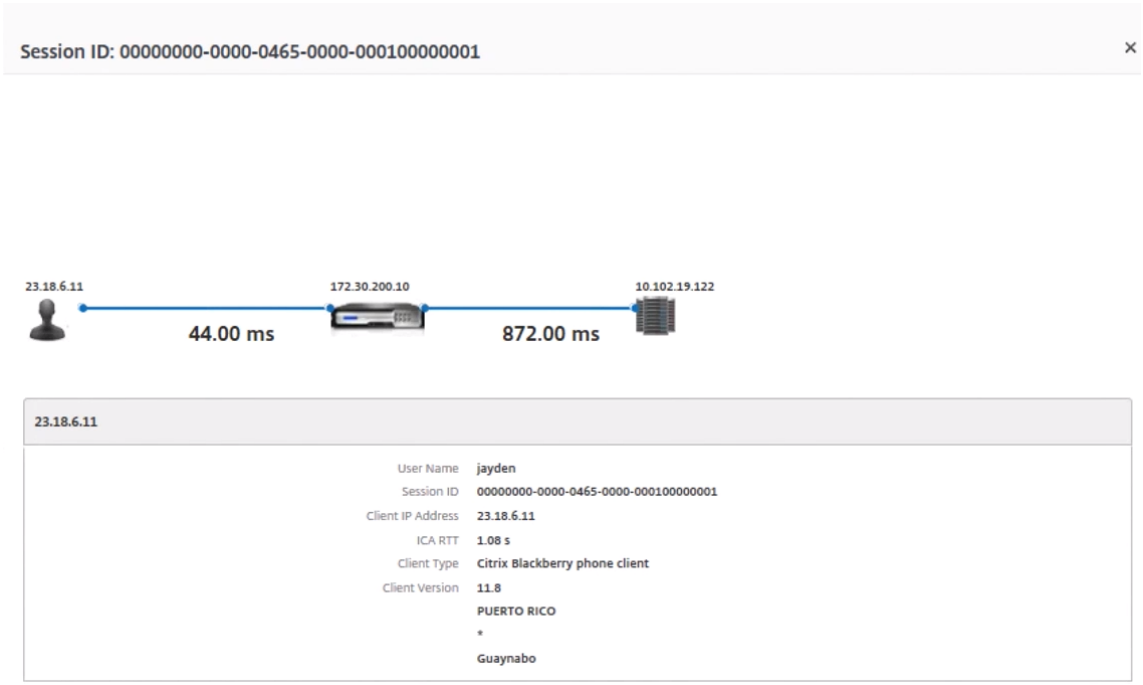
1. Navigieren Sie auf der Registerkarte “**Analytics**”zu “**HDX Insight** “> “**Benutzer**”.
2. Scrollen Sie nach unten, wählen Sie den Benutzernamen und wählen Sie den Zeitraum aus der Liste aus. Der Zeitraum kann ein Tag, eine Woche, ein Monat sein, oder Sie können sogar den Zeitraum anpassen, für 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Zusammenfassung In diesem Beispiel beträgt die **DC-Latenz** 751 Millisekunden, die **WAN-Latenz** 52 Millisekunden und **Hostverzögerungen** 6 Sekunden. Dies weist darauf hin, dass es beim Benutzer aufgrund der vom Servernetzwerk verursachten durchschnittlichen Latenz zu Verzögerungen kommt.

Szenario 2

Es kommt zu Verzögerungen beim Starten einer Anwendung auf Citrix Virtual Apps oder Desktops

Die Verzögerung kann auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen, Latenz im Client-Netzwerk oder auf die zum Starten einer Anwendung benötigte Zeit zurückzuführen sein.

Analysieren Sie die folgenden Metriken, um die Grundursache des Problems zu ermitteln:

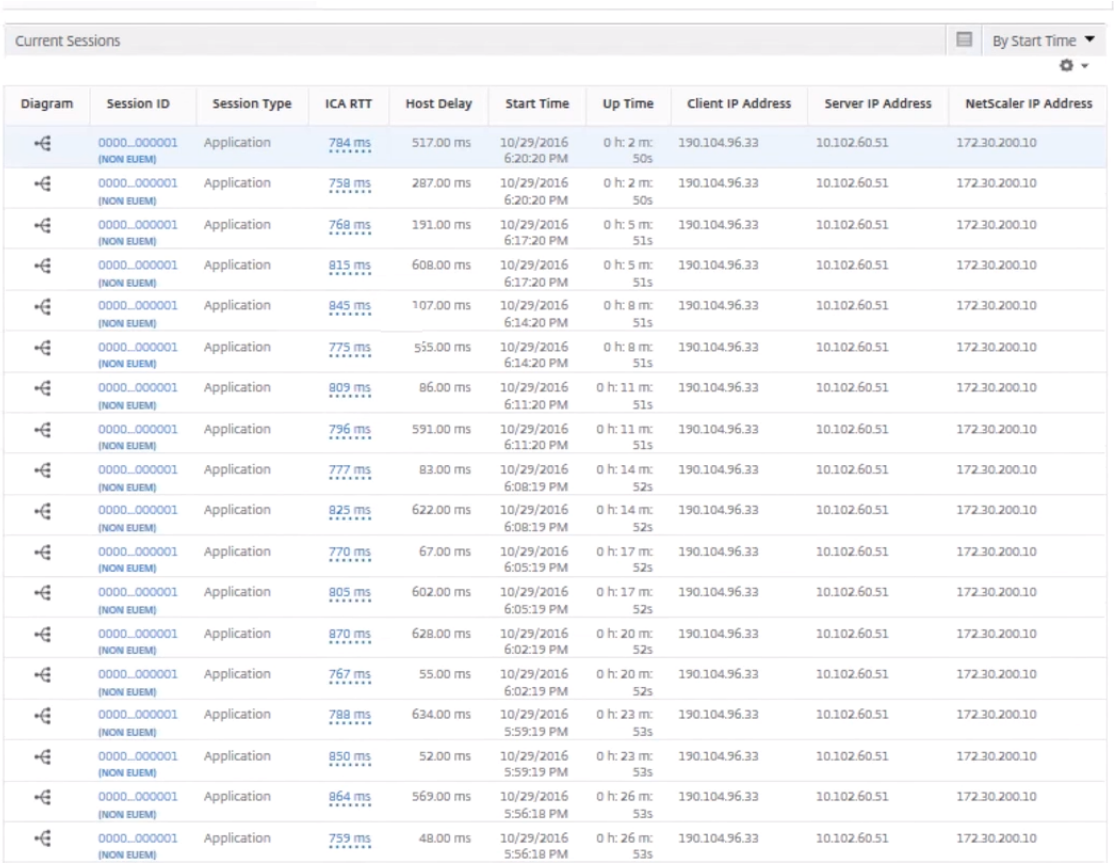
- WAN-Latenz
- DC-Latenz
- Host-Verzögerung

So zeigen Sie die Benutzermetriken an:

1. Navigieren Sie auf der Registerkarte **Analytics** zu **HDX Insight** > **Benutzer .**
2. Scrollen Sie nach unten und klicken Sie auf den Benutzernamen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Notieren Sie sich 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	535.00 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 zusätzliche Benutzermetriken an, z. B. WAN-Jitter und serverseitige Retransmeldungen, wenn Sie Citrix ADM verwenden, auf dem Software 11.1 Build 51.21 oder höher ausgeführt wird. Um diese Metriken anzuzeigen, navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**, und wählen Sie einen Benutzernamen aus. Die Benutzermetriken werden in der Tabelle neben dem Diagramm angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 auf der Karte im Abschnitt Welt 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

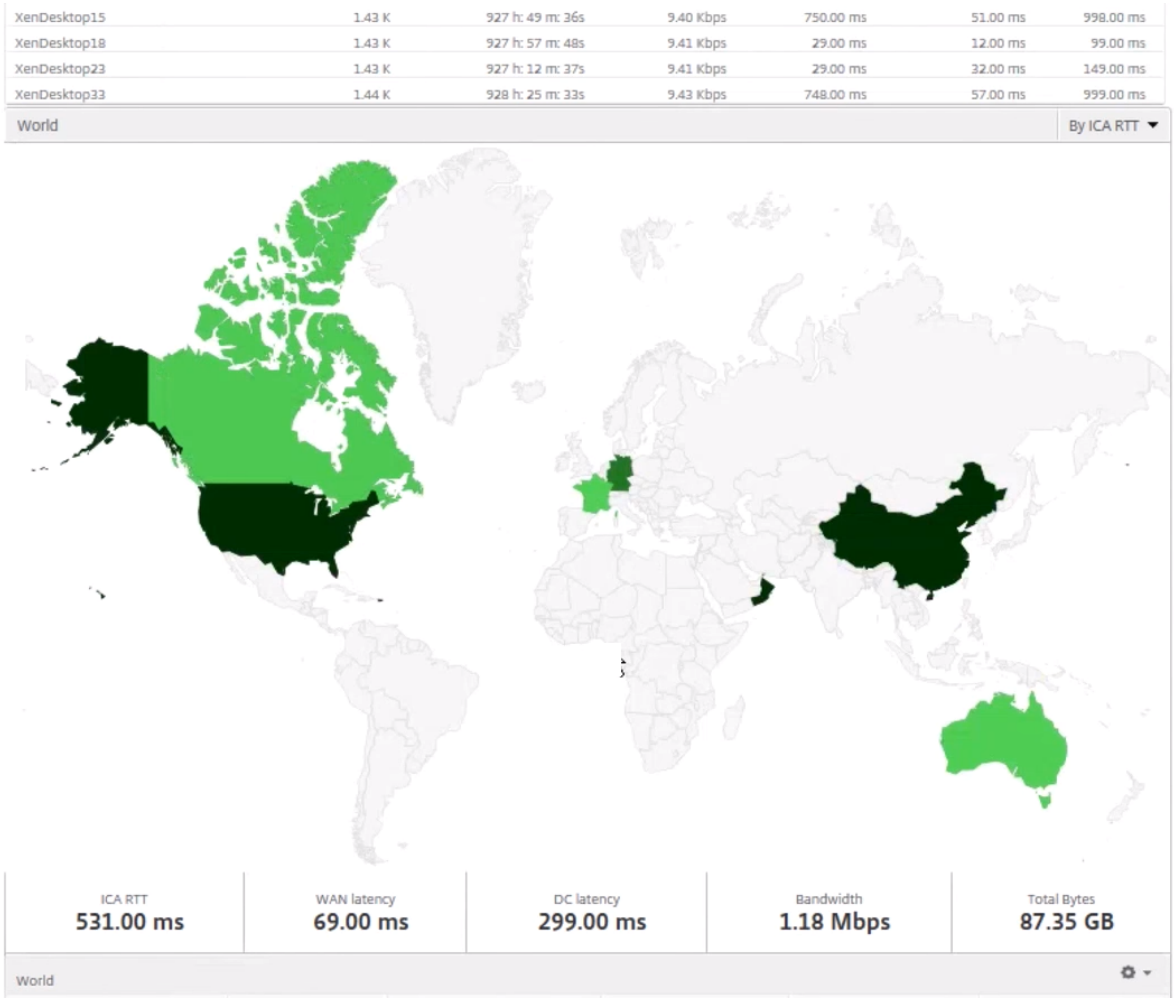
Betrachten Sie ein Szenario, in dem Organisation ABC 2 Niederlassungen hat, eine in Santa Clara und die andere in Indien.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Geomap-Funktionalität verwenden, um den Datenverkehr im Büro von Santa Clara anzuzeigen. Die Karte zeigt, dass die Reaktionszeit im Büro in Santa Clara sehr hoch ist, da das Büro in Santa Clara nur über eine Citrix Gateway-Appliance verfügt, über die Benutzer auf den VPN-Verkehr 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 Enterprise-Lizenz verfügen, werden in Citrix ADM für HDX Insight festgelegte Schwellenwerte nicht ausgelöst, da analytische Daten nur 1 Stunde lang erfasst werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Anwendungsstruktur. HDX Insight kann Benutzerprobleme sofort erfassen, Daten über virtuelle Desktopverbindungen sammeln, AppFlow Datensätze generieren und als visuelle Berichte präsentieren.

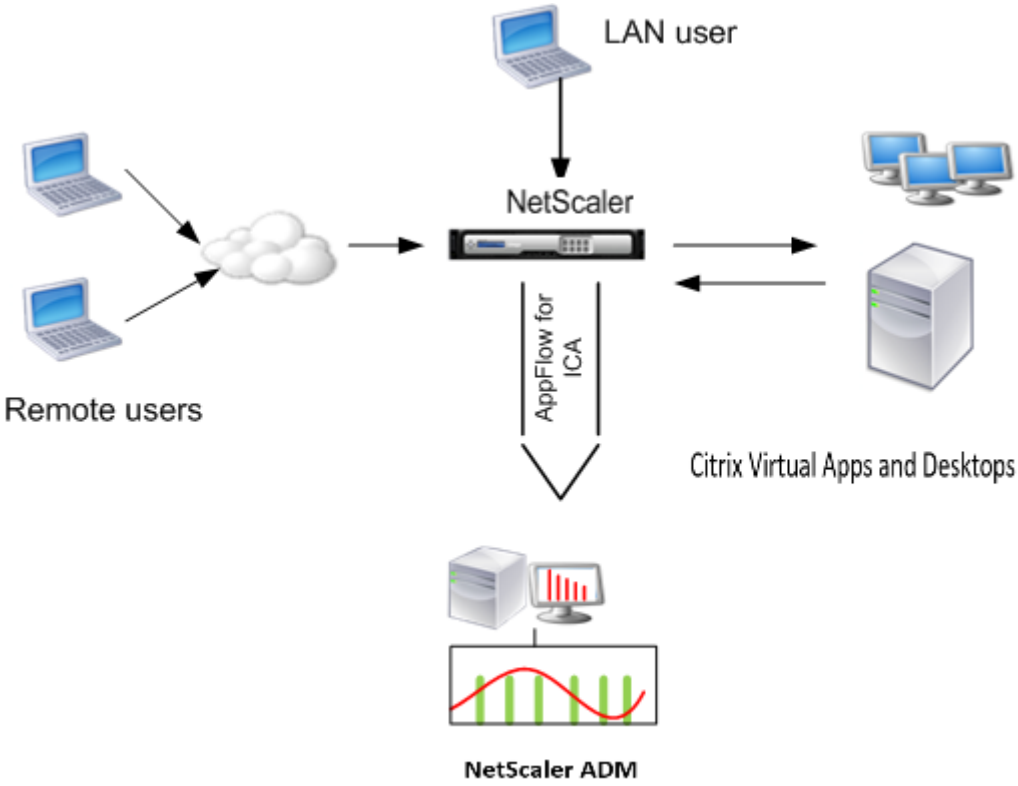
Die Konfiguration zur Aktivierung der Datenerfassung im NetScaler ADC unterscheidet sich von der Position der Appliance in der Bereitstellungstopologie.

Aktivieren der Datenerfassung für die Überwachung der im LAN-Benutzermodus bereitgestellten Citrix ADCs

Externe Benutzer, die auf Citrix Virtual Apps and Desktops-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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis:** NetScaler ADM und NetScaler Gateway Gerät befinden sich im selben Subnetz.

Um die in diesem Modus bereitgestellten Citrix ADC-Appliances zu überwachen, fügen Sie zuerst die Citrix ADC-Appliance zum NetScaler Insight-Inventar hinzu, aktivieren Sie AppFlow und zeigen Sie dann die Berichte auf dem Dashboard an.

Nachdem Sie die NetScaler ADC Appliance zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

> **Hinweis**
>
> - Auf einer ADC-Instanz können Sie zu **System** > **AppFlow** > **Collectors**navigieren, um zu überprüfen, ob der Collector (d. h. Citrix ADM) aktiv 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 .

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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>]

   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 or OFF)]

   add vpn trafficPolicy <name> <rule> <action>

   Beispiel

   ```
   add vpn trafficAction act1 tcp -HDX ON

   add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
   <!--NeedCopy-->
   ```

3. Fügen Sie NetScaler ADM als Appflow-Sammler auf der NetScaler ADC Appliance hinzu.

   add appflow collector <name> **-IPAddress** <ip_addr>

   Beispiel:

   ```
   add appflow collector MyInsight -IPAddress 192.168.1.101
   <!--NeedCopy-->
   ```

4. Erstellen Sie eine Appflow-Aktion, und ordnen Sie den Collector der Aktion zu.

   add appflow action <name> **-collectors** <string> …

   Beispiel:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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>

   Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die Appflow-Richtlinie an einen globalen Bindungspunkt.

   bind appflow global <policyname> <priority> **-type** <type>

   Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

   > **Hinweis** Der Wert von type sollte ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er für den ICA-Verkehr gilt.

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
<!--NeedCopy-->
```

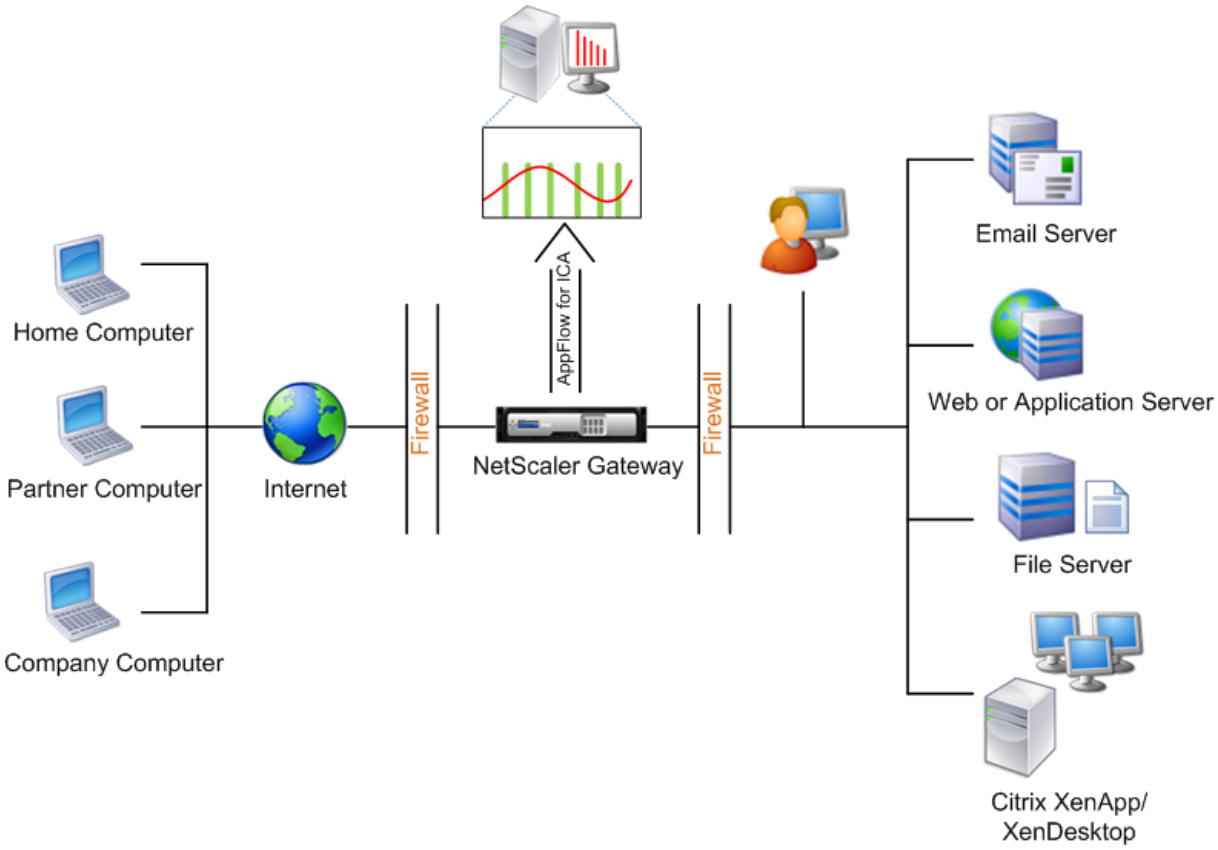
8. Speichern Sie die Konfiguration. Typ: `save ns config`

Aktivieren der Datenerfassung für Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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 Dropdownliste Aktion** auswählen die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen VPN-Server aus und klicken Sie auf **AppFlow aktivieren**.
6. Geben Sie in das Feld **Enable AppFlow** den Wert **true**ein und wählen Sie **ICA**aus.
7. Klicken Sie auf **OK**.

> Hinweis: Die folgenden Befehle werden im Hintergrund ausgeführt, wenn Sie AppFlow im Single-Hop-Modus aktivieren. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

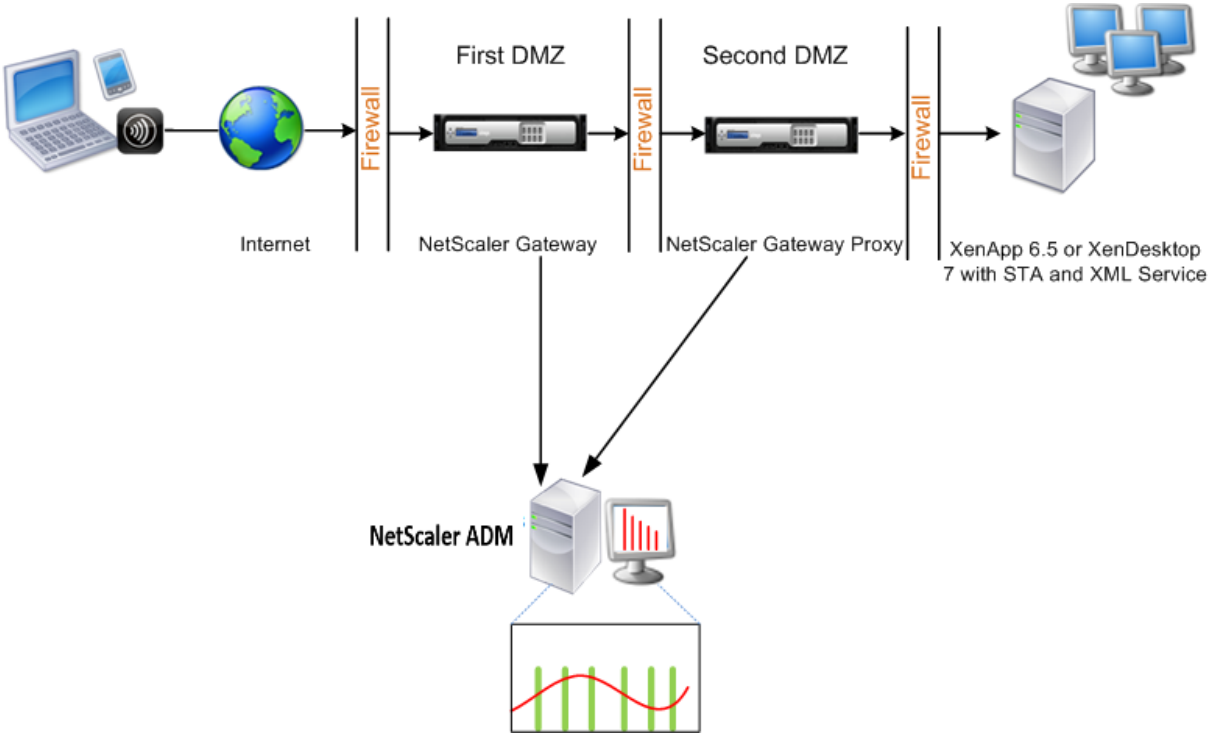
- add appflow collector <name> -IPAddress <ip_addr>
- add appflow action <name> -collectors <string>
- set appflow param -flowRecordInterval <secs>
- disable ns feature AppFlow
- enable ns feature AppFlow
- add appflow policy <name> <rule> <expression>
- set appflow policy <name> -rule <expression>
- bind vpn vserver <vsname> -policy <string> -type <type> -priority <positive_integer>
- set vpn vserver <name> -appflowLog ENABLED
- save ns config

Virtuelle EUEM-Kanaldaten sind Teil von HDX Insight Daten, die NetScaler ADM von Gateway-Instanzen erhält. Der virtuelle EUEM-Kanal stellt die Daten über ICA-RTT bereit. Wenn der virtuelle EUEM-Kanal nicht aktiviert ist, werden die verbleibenden HDX Insight Daten weiterhin in NetScaler ADM angezeigt.

Aktivieren der Datenerfassung für Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Citrix Gateway-Appliances zum Citrix ADM-Inventar hinzugefügt und die Datenerfassung aktiviert haben, exportiert jedes der Appliances die Berichte, indem es 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die in diesem Modus bereitgestellten Citrix Gateway-Appliances zu überwachen, müssen Sie zuerst das Citrix Gateway zum Citrix ADM-Inventar hinzufügen, AppFlow auf Citrix ADM aktivieren und dann die Berichte auf dem Citrix 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 überwinden, müssen Sie AppFlow für ICA auf einer der ersten Citrix Gateway-Appliances und dann AppFlow für TCP auf der zweiten Appliance aktivieren. Dadurch 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 Dropdownliste Aktion** auswählen die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen VPN-Server aus und klicken Sie auf **AppFlow aktivieren**.
6. Geben Sie im Feld **AppFlow aktivieren** den Wert **true** ein, und wählen Sie **ICA/TCP** für ICA-Datenverkehr bzw. TCP-Datenverkehr aus.

   > **Hinweis** Wenn die AppFlow-Protokollierung für die entsprechenden Dienste oder Dienstgruppen auf der Citrix ADC Appliance nicht aktiviert ist, zeigt das Citrix ADM-Dashboard die Datensätze nicht an, auch wenn in der Spalte Insight 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

Konfiguration von Citrix Gateway über die 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 <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>

   VPN vserver vs1 binden -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 oder 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Geräten:

   set appFlow param [**-connectionChaining** (ENABLED or DISABLED)]

   setze den Appflow-Parameter -ConnectionChaining ENABLED

Konfigurieren von NetScaler Gateway mit dem Konfigurationsprogramm:

1. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ für die Kommunikation mit dem NetScaler Gateway in der zweiten DMZ, und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

   a) Erweitern Sie auf der Registerkarte**KonfigurationNetScaler Gateway**, und klicken Sie auf**Virtuelle Server**.

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option**Veröffentlichte Anwendungen**.

   c) Klicken Sie auf**Next Hop Server**, und binden Sie einen nächsten Hop-Server an das zweite NetScaler Gateway Gerät.

2. Aktivieren Sie den Double-Hop auf dem NetScaler Gateway in der zweiten DMZ.

   a) Erweitern Sie auf der Registerkarte**KonfigurationNetScaler Gateway**, und klicken Sie auf**Virtuelle Server**.

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server und klicken Sie in der Gruppe**Grundeinstellungen** auf das Bearbeitungssymbol.

   c) Erweitern Sie **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 Bearbeitungssymbol.

   c) Erweitern Sie**Mehr**, und deaktivieren Sie die Option**Authentifizierung aktivieren**.

4. Aktivieren Sie eines der Citrix Gateway-Appliances, um TCP-Datensätze zu exportieren.

   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 GruppeErweitertdie OptionRichtlinien.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) Klicken Sie auf das Pluszeichen und wählen Sie in der Dropdownliste **Richtlinie auswählen** die Option **AppFlow** aus und wählen Sie in der Dropdownliste **Typ auswählen** die Option **Andere TCP-Anfrage** 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 Pluszeichen und wählen Sie in der Dropdownliste**Richtlinie auswählen**die Option**AppFlow** aus und wählen Sie in der Dropdownliste Typ auswählen die Option**Andere TCP-Anfrage**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**.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe **Grundeinstellungen**auf das Symbol "Bearbeiten".

c) Erweitern Sie Mehr , wählen Sie **Double Hop** und klicken Sie auf **OK** .

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 Bearbeitungssymbol.

c) Erweitern Sie**Mehr**, und deaktivieren Sie die Option**Authentifizierung aktivieren**.

10. Aktivieren Sie eines der Citrix Gateway-Appliances, um TCP-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 Dropdownliste Choose Policy die Option **AppFlow** aus und wählen Sie in der Dropdownliste **Choose Type** die Option **Andere TCP-Anfrage** 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**Pluszeichen**und**wählen Sie in der Dropdownliste Richtlinie** auswählen**AppFlow** a und wählen Sie in der Dropdownliste **Typ auswählen**die Option**Andere TCP-Anfrage**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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Aktivieren der Datenerfassung zur Überwachung von Citrix ADCs, die im transparenten Modus bereitgestellt werden

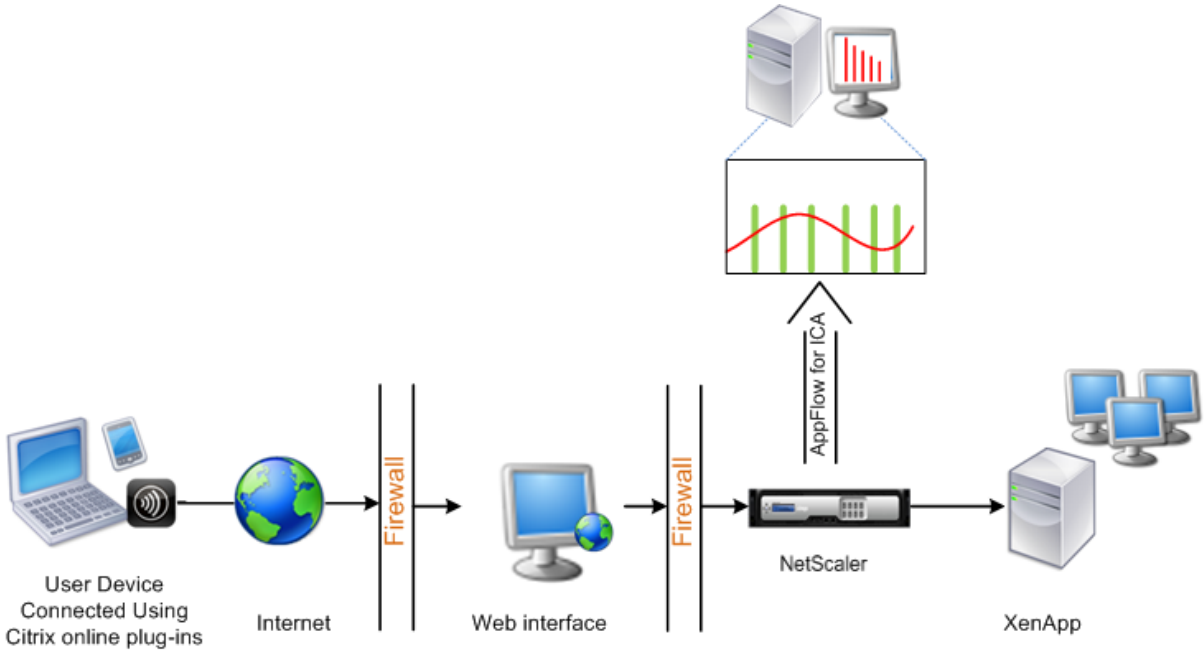
Wenn ein NetScaler ADC im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne dass ein virtueller Server vorhanden ist. Wenn eine NetScaler ADC Appliance im transparenten Modus in einer Citrix Virtual Apps and Desktop-Umgebung bereitgestellt wird, wird der 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 Citrix ADM als AppFlow Collector auf jeder Citrix ADC Appliance 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Citrix ADC Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Beispiel:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Hinweis** Verwenden Sie den Befehl show appflow collector, um die auf der Citrix ADC Appliance konfigurierten**Appflow-Collectors anzuzeigen** .

4. Erstellen Sie eine Appflow-Aktion, und ordnen Sie den Collector der Aktion zu.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Beispiel:

Appflow Action Act hinzufügen —Collectors MyInsight

5. Erstellen Sie eine Appflow-Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die Appflow-Richtlinie an einen globalen Bindungspunkt.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Hinweis** Der Wert von**type** sollte ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er für den ICA-Verkehr gilt.

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. Typ: `save ns config`

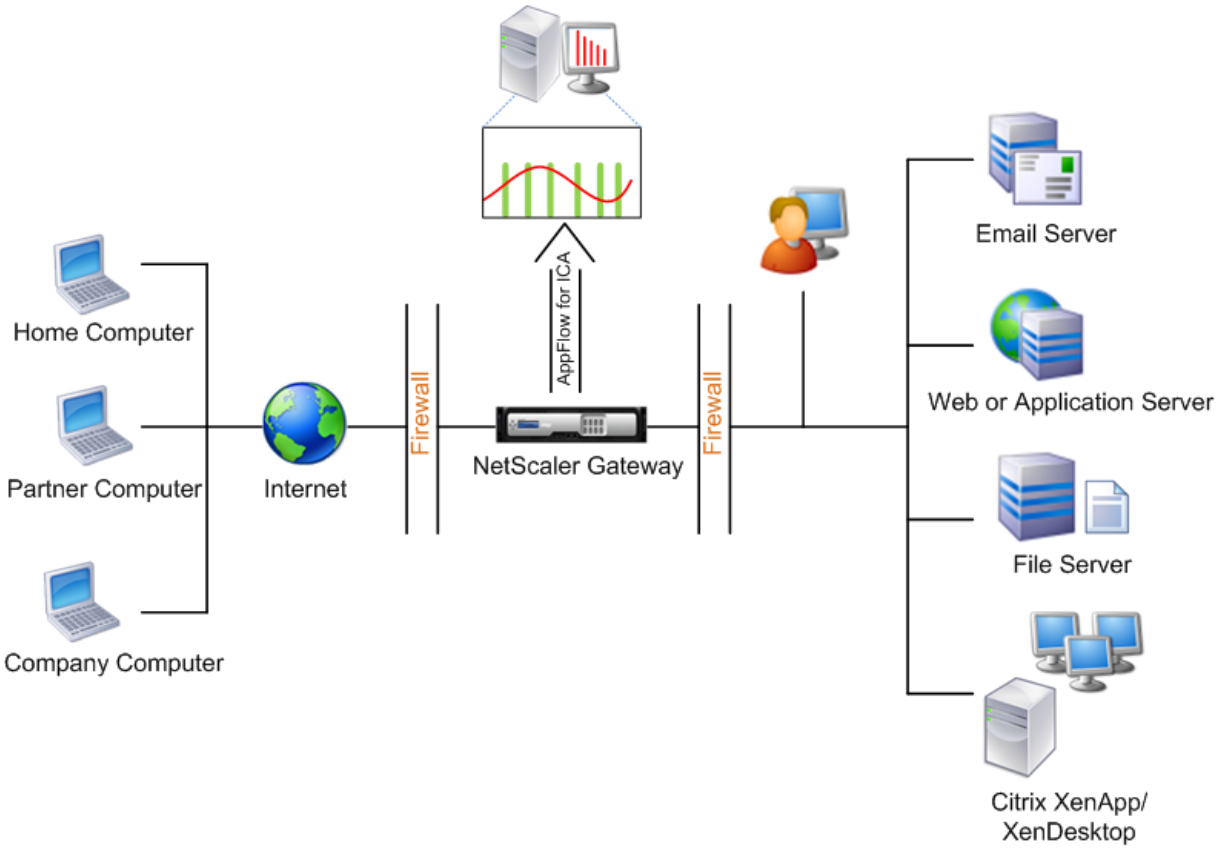
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Navigieren Sie zu **Infrastruktur** > **Instanzen** und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
4. Wählen Sie im Drop-down-Menü **Aktion** die Option **Insight aktivieren/deaktivieren** aus.
5. Wählen Sie die **virtuellen VPN-Server** aus und klicken Sie auf **AppFlow aktivieren** .
6. Geben Sie in das Feld **Enable AppFlow** den Wert **true**ein und wählen Sie **ICA**aus.
7. Klicken Sie auf **OK**.

> **Hinweis** Die folgenden Befehle werden im Hintergrund ausgeführt, wenn Sie AppFlow im Single-Hop-Modus aktivieren. Diese Befehle werden hier explizit zur Fehlerbehebung angegeben.
>
> - add appflow collector <name> -IPAddress <ip_addr>
> - add appflow action <name> -collectors <string>
> - set appflow param -flowRecordInterval <secs>
> - disable ns feature AppFlow
> - enable ns feature AppFlow
> - add appflow policy <name> <rule> <expression>
> - set appflow policy <name> -rule <expression>
> - bind vpn vserver <vsname> -policy <string> -type <type> >-priority <positive_integer>
> - set vpn vserver <name> -appflowLog ENABLED
> - save ns config

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 zum Überwachen von im transparenten Modus bereitgestellten s 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 dazwischengeschaltet wird. Wenn eine NetScaler Appliance im transparenten Modus in einer Citrix Virtual Apps and Desktops-Umgebung bereitgestellt wird, wird der ICA-Datenverkehr nicht über ein VPN übertragen.

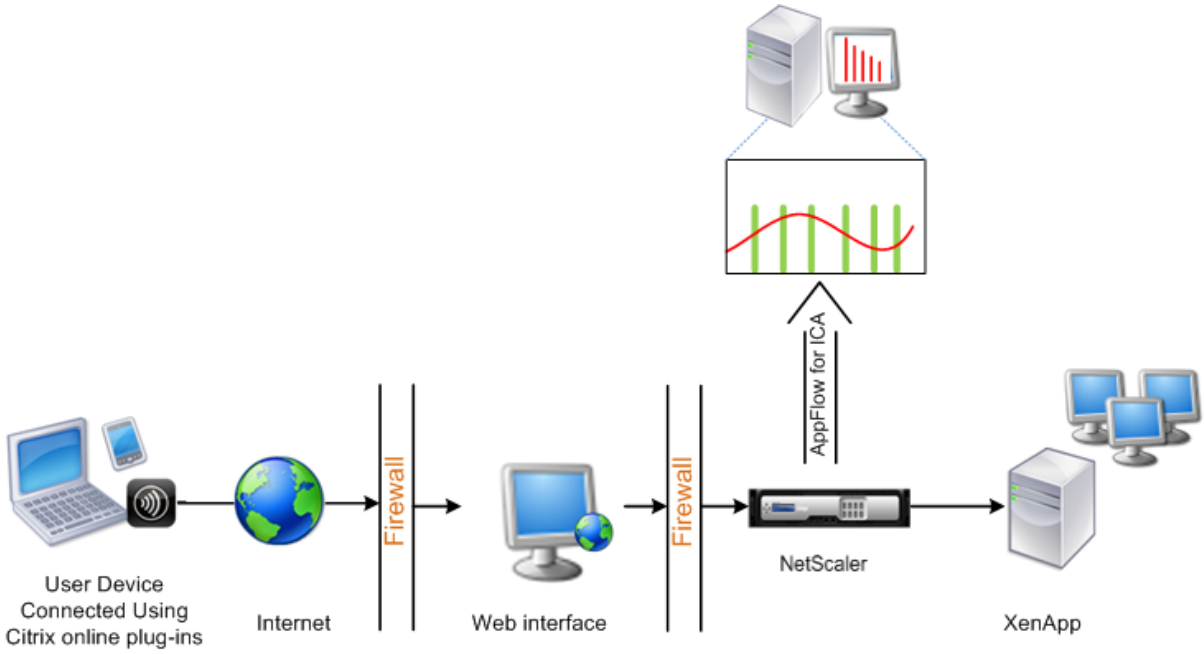
Nachdem Sie NetScaler ADC zur NetScaler ADM Bestandsliste hinzugefügt haben, müssen Sie AppFlow für die Datensammlung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und vom

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Modus ab. In diesem Fall müssen Sie Citrix ADM als AppFlow-Collector auf jeder NetScaler-Appliance 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 mit dem Citrix ADM-Konfigurationsprogramm 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 Citrix ADM, wenn ein NetScaler ADC in einem transparenten Modus bereitgestellt wird:



So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die NetScaler Appliance auf Datenverkehr wartet.

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Hinweis** Verwenden Sie den Befehl show appflow collector, um die auf der NetScaler Appliance konfigurierten**Appflow-Collectors anzuzeigen** .

4. Erstellen Sie eine Appflow-Aktion, und ordnen Sie den Collector der Aktion zu.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Beispiel:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Erstellen Sie eine Appflow-Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die Appflow-Richtlinie an einen globalen Bindungspunkt.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Beispiel:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

Hinweis Der Wert von**type** sollte ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er für den ICA-Verkehr gilt.

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-->
```

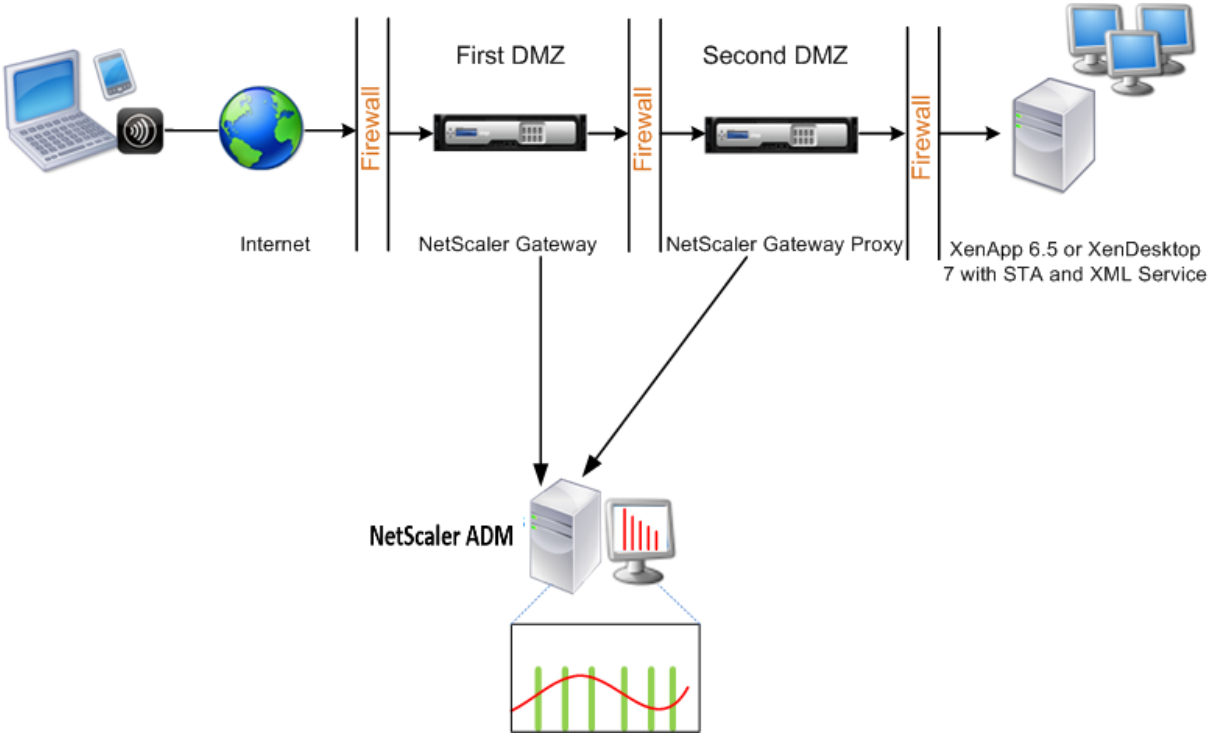
Datensammlung für NetScaler Gateway-Geräte im Double-Hop-Modus aktivieren

February 5, 2024

Der 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.

Abbildung 3. NetScaler ADM im Double-Hop-Modus bereitgestellt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Citrix Gateway-Appliances zum Citrix ADM-Inventar hinzugefügt und die Datenerfassung aktiviert haben, exportiert jedes der Appliances die Berichte, indem es 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die in diesem Modus bereitgestellten Citrix Gateway-Appliances zu überwachen, müssen Sie zuerst das Citrix Gateway zum Citrix ADM-Inventar hinzufügen, AppFlow auf Citrix ADM aktivieren und dann die Berichte auf dem Citrix 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-Geräte und dann AppFlow für ICA auf dem zweiten Gerät aktivieren. Dadurch exportiert eine der Appliances ICA AppFlow Datensätze, und die andere Appliance exportiert TCP-AppFlow-Datensätze. Dies spart auch die Verarbeitungszeit beim Analysieren des ICA-Datenverkehrs.

So aktivieren Sie die AppFlow Funktion von NetScaler ADM:

1. Navigieren Sie zu **Infrastruktur** > **Instanzen** und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie im Drop-down-Menü **Aktion** die Option **Insight aktivieren/deaktivieren** aus.
3. Wählen Sie die virtuellen VPN-Server aus und klicken Sie auf **AppFlow aktivieren**.
4. Geben Sie im Feld **AppFlow aktivieren** den Wert **true** ein, und wählen Sie **ICA/TCP** für ICA-Datenverkehr bzw. TCP-Datenverkehr aus.

   > **Hinweis** Wenn die AppFlow-Protokollierung für die jeweiligen Dienste oder Dienstgruppen auf der NetScaler Appliance nicht aktiviert ist, zeigt das NetScaler ADM-Dashboard die Datensätze nicht an, auch wenn in der Spalte Insight Aktiviert angezeigt wird.

5. Klicken Sie auf **OK**.

Konfigurieren von NetScaler Gateway Geräten zum Exportieren von Daten

Nach der Installation der NetScaler Gateway Geräte müssen Sie die folgenden Einstellungen auf den NetScaler Gateway-Geräten konfigurieren, um die Berichte in NetScaler ADM zu exportieren:

- Konfigurieren Sie virtuelle Server der NetScaler Gateway-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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

Konfiguration von Citrix Gateway über die 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**] ...

```
add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
<!--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** (DISABLED)] [**- appflowLog** (DISABLED)] [**-** ENABLED ENABLED

```
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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 DISABLED)]
param [**-connectionChaining** (ENABLED

```
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**Konfiguration** die Option **NetScaler Gateway** und klicken Sie auf **Virtuelle Server**.

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe Erweitert die Option**Veröffentlichte Anwendungen**.

   c) Klicken Sie auf**Next Hop Server** und binden Sie einen 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**KonfigurationNetScaler Gateway**, und klicken Sie auf**Virtuelle Server**.

   b) Doppelklicken Sie im rechten Bereich auf den virtuellen Server und klicken Sie in der Gruppe**Grundeinstellungen** auf das Bearbeitungssymbol.

   c) Erweitern Sie **More**, wählen Sie **Double Hop**, und klicken Sie auf**OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die Option**Authentifizierung aktivieren**.
4. Aktivieren Sie eines der Citrix Gateway-Appliances, um TCP-Datensätze zu exportieren.
    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 GruppeErweitertdie OptionRichtlinien.
    c) Klicken Sie auf das Symbol + und wählen Sie in der Liste **Richtlinie wählen** die Option **AppFlow** aus, und wählen Sie in der Liste **Typ auswählen** die Option **Andere TCP-Anforderung** aus.
    d) Klicken Sie auf **Weiter**.
    e) Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Schließen**.
5. Aktivieren Sie 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 wählen** 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) Klicken Sie im rechten Bereich in der Gruppe**Einstellungen** auf **Appflow-Einstellungen ändern**.
    c) Wählen Sie **Verbindungsverkettung** aus, und klicken Sie auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

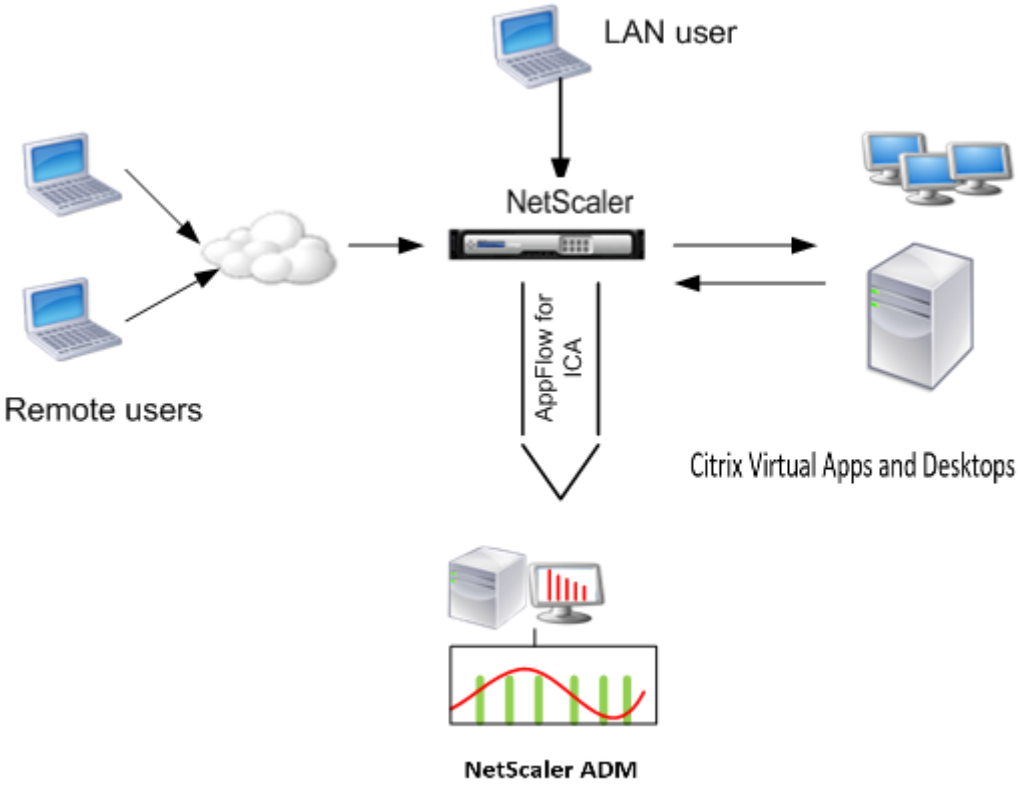
Datenerfassung zur Überwachung von s im LAN-Benutzermodus aktivieren

February 5, 2024

Externe Benutzer, die auf Citrix Virtual Apps and Desktops-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 Appliance umgeleitet werden.

Um diese Herausforderungen zu bewältigen und LAN-Benutzer direkt mit Citrix Virtual Apps and Desktops-Anwendungen zu verbinden, können Sie die NetScaler Appliance in einem LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cache-Umleitungsserver konfigurieren, der als SOCKS-Proxy auf der Citrix Gateway-Appliance fungiert.

Figure 4. NetScaler ADM im LAN-Benutzermodus bereitgestellt



> **Hinweis**
>
> Citrix ADM und die Citrix Gateway-Appliance befinden sich im selben Subnetz.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Um die in diesem Modus bereitgestellten Citrix Appliances zu überwachen, fügen Sie zuerst die Citrix Appliance zum NetScaler Insight-Inventar hinzu, aktivieren Sie AppFlow und zeigen Sie dann die Berichte im Dashboard an.

Nachdem Sie die Citrix Appliance zum Citrix ADM-Inventar 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 mit dem Citrix ADM-Konfigurationsprogramm aktivieren.
> - Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie in der Befehlsreferenz .
> - Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke .

So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance mithilfe der Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei einer Appliance an.
2. Fügen Sie einen virtuellen Forward-Proxy-Cache-Umleitungsserver mit Proxy-IP und Port hinzu, und geben Sie den Diensttyp als HDX an.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Beispiel:

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Hinweis:** Wenn Sie mit einem NetScaler Gateway -Gerät auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, die von einer Richtlinie angewendet wird, die dem VPN-Datenverkehr entspricht.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

Beispiel:

```
add vpn trafficAction act1 tcp -HDX ON

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Fügen Sie NetScaler ADM als Appflow-Sammler 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 Collector der Aktion zu.

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

Beispiel:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Erstellen Sie eine Appflow-Richtlinie, um die Regel zum Generieren des Datenverkehrs anzugeben.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

Beispiel:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Binden Sie die Appflow-Richtlinie an einen globalen Bindungspunkt.

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
    type\>
<!--NeedCopy-->
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Hinweis** Der Wert von type sollte ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, damit er für den ICA-Verkehr gilt.

7. Legen Sie den Wert des Parameters flowRecordInterval für Appflow auf 60 Sekunden fest.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 Anwendungsentität mit einer Anzahl von Treffern, der von der Anwendung verbrauchten Bandbreite und der Antwortzeit 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weise können Sie realistischere Schwellenwerte für eine Entität festlegen.

Einige Beispiele sind wie folgt aufgeführt:

- Schwellenwertregel1: ICA RTT (Metrik) für Benutzer (Entität) sollte <= 100 ms sein
- Schwellenwertregel2: WAN-Latenz (Metrik) für Benutzer (Entität) sollte <= 100 ms betragen

Ein Beispiel für eine Schwellenwertgruppe kann sein: {Schwellenwertregel 1 + Schwellenwertregel 2}

Um eine Regel zu erstellen, sollten 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.

Beispiel-Anwendungsfälle

ABC Inc. ist ein globales Unternehmen und hat Niederlassungen in über 50 Ländern. Das Unternehmen verfügt über zwei Rechenzentren, eines in Singapur und eines in Kalifornien, in denen Citrix Virtual Apps and Desktops gehostet werden. Mitarbeiter des Unternehmens greifen 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 Administrator für ABC Inc. möchte die Benutzererfahrung für alle ihre Büros verfolgen, um die Apps und die Desktopbereitstellung für jederzeit und überall zu optimieren. Eric möchte auch die User-Experience-Metriken wie ICA-RTTs und Latenzen überprüfen und etwaige Abweichungen proaktiv erhöhen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

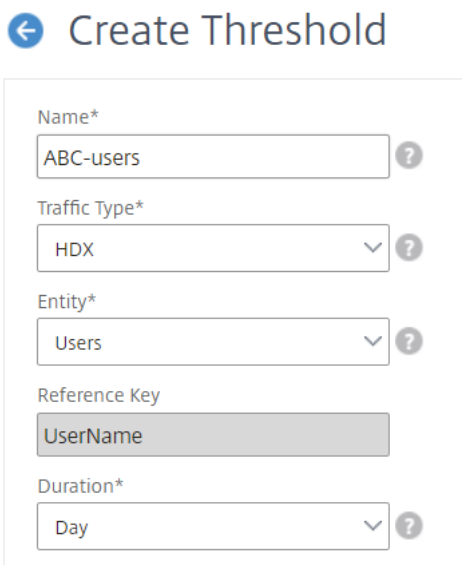
Die Anwender von ABC Inc. haben eine verteilte Präsenz. Einige Benutzer befinden sich in der Nähe des Rechenzentrums, während sich einige weiter vom Rechenzentrum entfernt befinden. Da die Benutzerbasis breit verteilt ist, variieren auch die Metriken und die entsprechenden Schwellenwerte zwischen diesen Standorten. Beispielsweise kann die ICA-RTT für einen Standort in der Nähe des Rechenzentrums 5-10 ms betragen, während die gleiche für einen Remote-Standort etwa 100 ms betragen kann.

Mit der Schwellenwertregelgruppenverwaltung für HDX Insight kann Eric geospezifische Schwellenwertregelgruppen für jeden Standort festlegen und sich per E-Mail oder SMS bei Verstößen pro Bereich benachrichtigen lassen. 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:

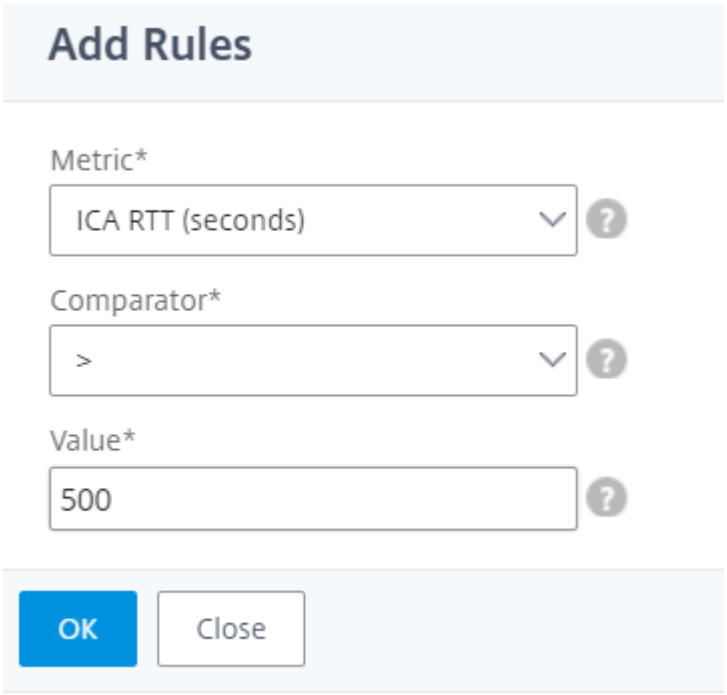
1. Navigieren Sie in Citrix ADM zu**Analytics** > **Einstellungen** > **Schwellenwerte**. Klicken Sie auf der Seite **Schwellenwerte**, die geöffnet wird, auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwerte und Warnungen erstellen** die folgenden Details an:
    a) **Name**. Geben Sie einen Namen zum Erstellen eines Ereignisses ein, für das Citrix ADM eine Warnung generiert.
    b) **Art des Datenverkehrs**. Wählen Sie im Dropdown-Listenfeld HDX aus.
    c) **Entität**. Wählen Sie im Dropdown-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 aus dem Dropdown-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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



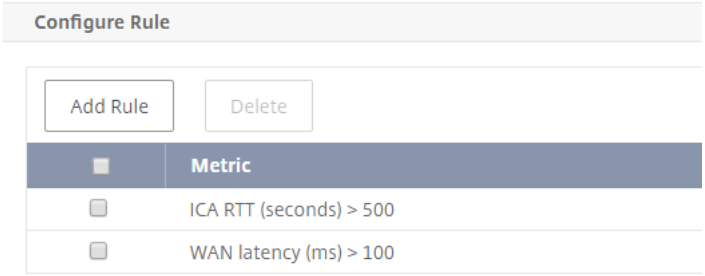
3. Erstellen von Schwellenwertregelgruppen für alle Entitäten:

   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.



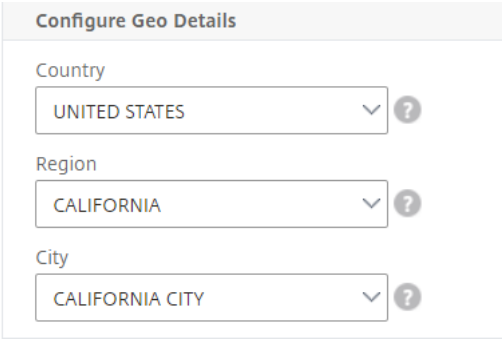
   Sie können mehrere Regeln erstellen, um jede Entität zu überwachen. Wenn Sie mehrere Regeln in einer einzigen Gruppe erstellen, können Sie die Entitäten als Gruppe von Schwellenwertregeln anstelle einzelner Regeln überwachen. Klicken Sie auf **OK**, um das Fenster zu schließen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Apps and Desktops zugreifen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

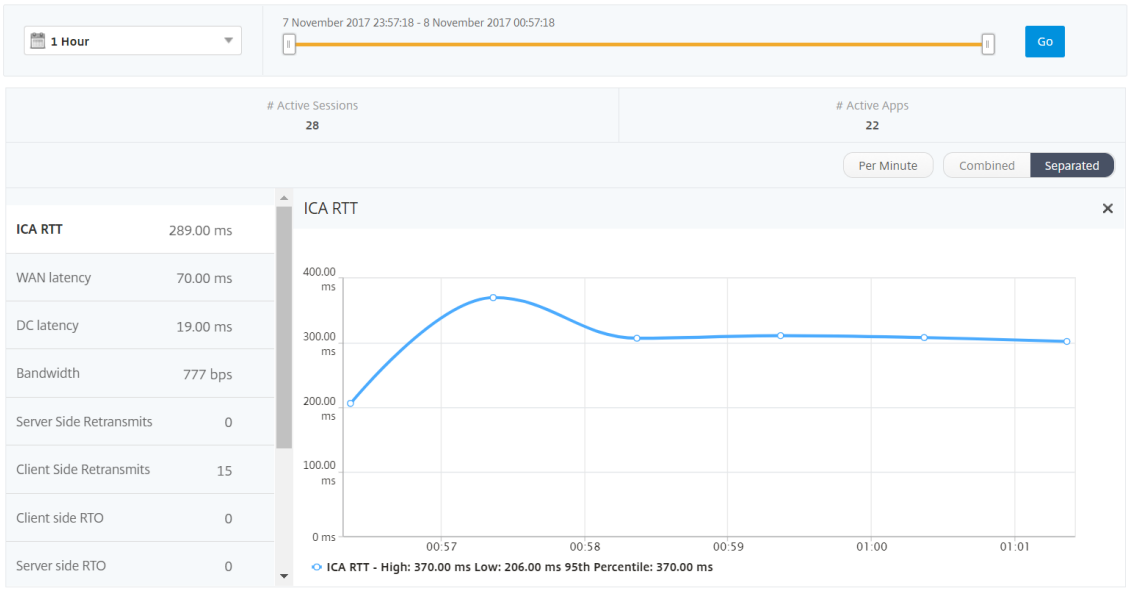
Benutzer: Berichte und Metriken anzeigen

06. Nov 2017

Die Berichte und Metriken in dieser Ansicht werden pro Benutzer von Citrix Virtual Apps and Desktops angezeigt.

So navigieren Sie zur Ansicht Benutzer:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**



Berichte und Metriken zur Benutzeransicht bestehen aus den folgenden Abschnitten:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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**.

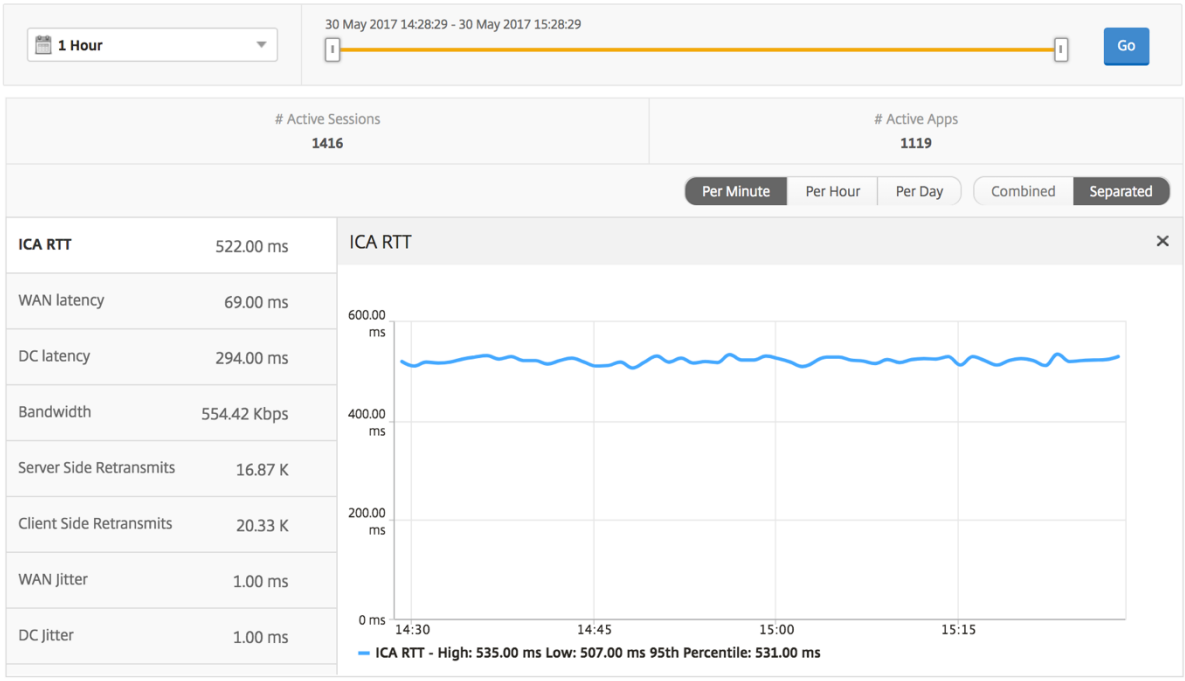
Liniendiagramm

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 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 wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Zusammenfassungsbericht für Benutzer Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
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.
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.

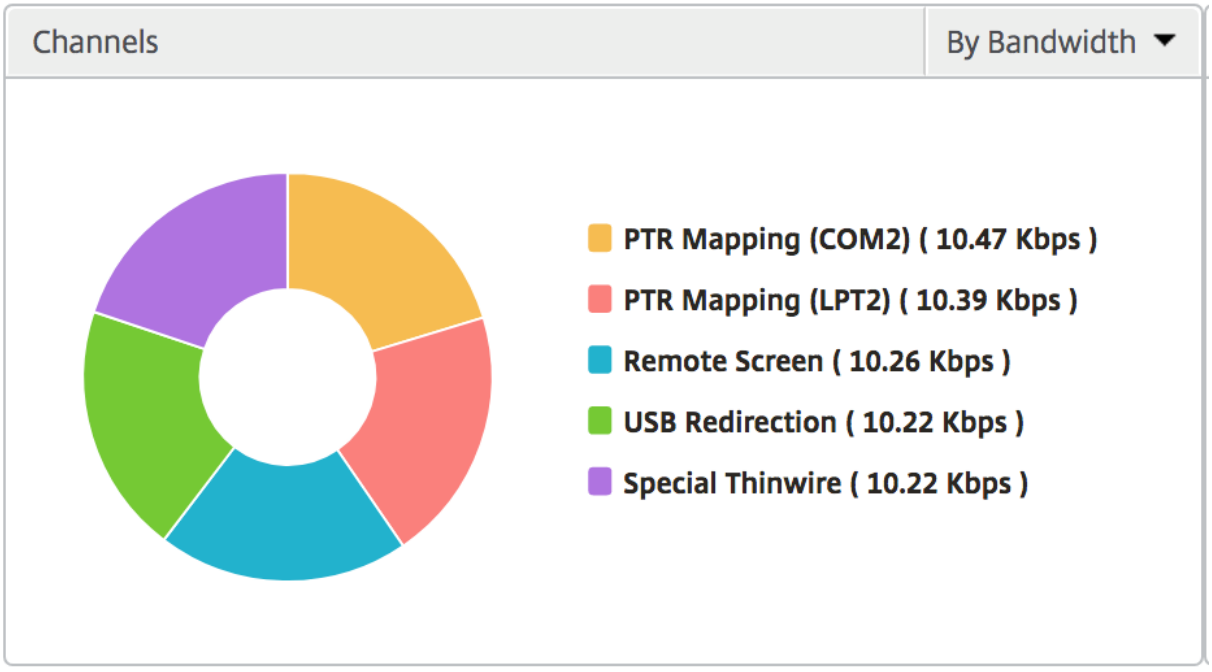
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Users

Search

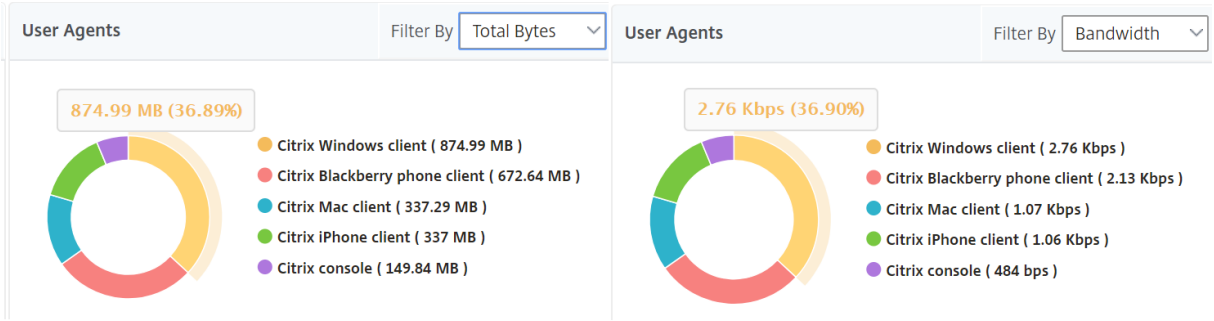
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	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.

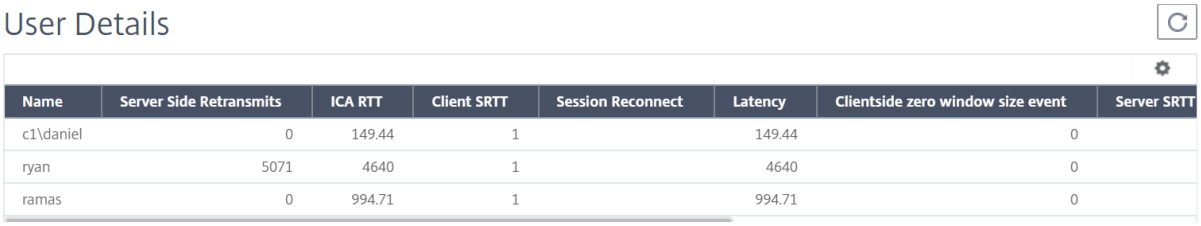


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzeragents 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 Verstöße bei Schwellenwerten Die Metriken für die Anzahl der Schwellenwertverstöße stellen die Anzahl der Schwellenwerte dar, die im ausgewählten Zeitraum überschritten wurden.

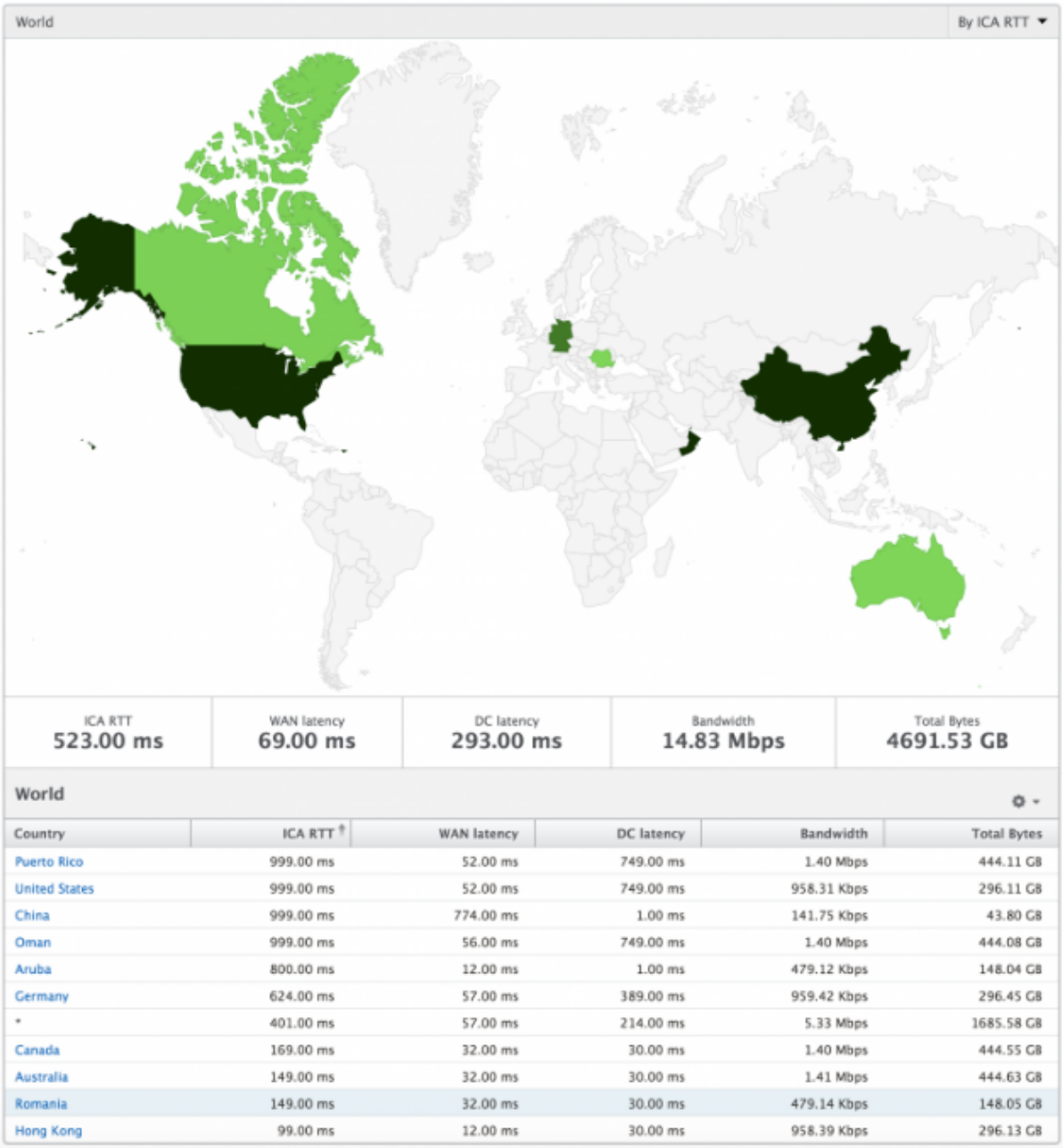
Weltkarte Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. Die Administratoren können eine Weltanschauung des Systems, Drilldown zu einem bestimmten Land und weiter in die Städte als auch durch Klicken auf die Region. Die Administratoren können weitere Informationen nach Stadt und Bundesstaat anzeigen. Ab NetScaler 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, Wiederverbindungen von Sitzungen und ACR-Anzahl 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	Empfängertyp: Citrix Windows Client
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

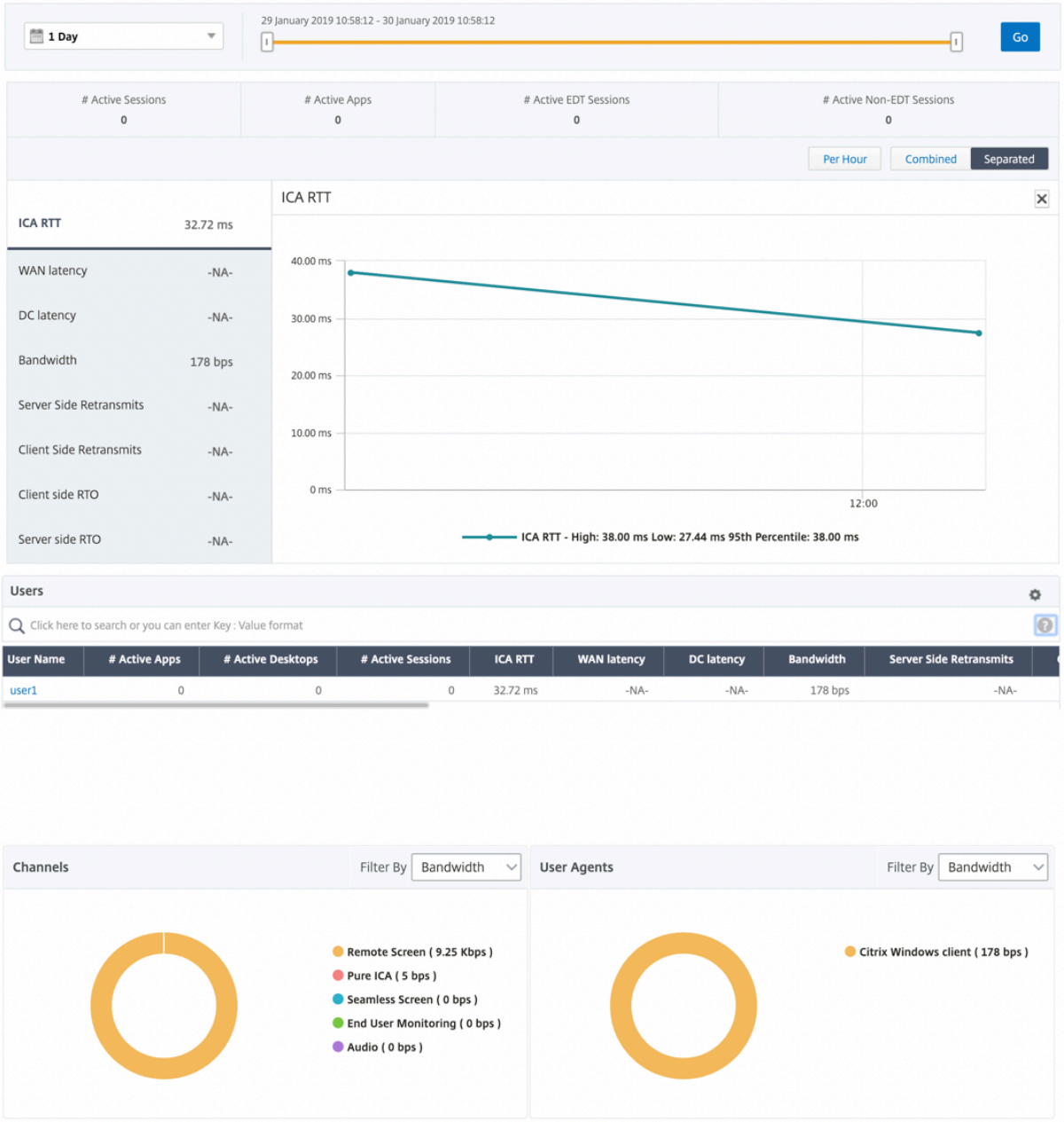
Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die 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.

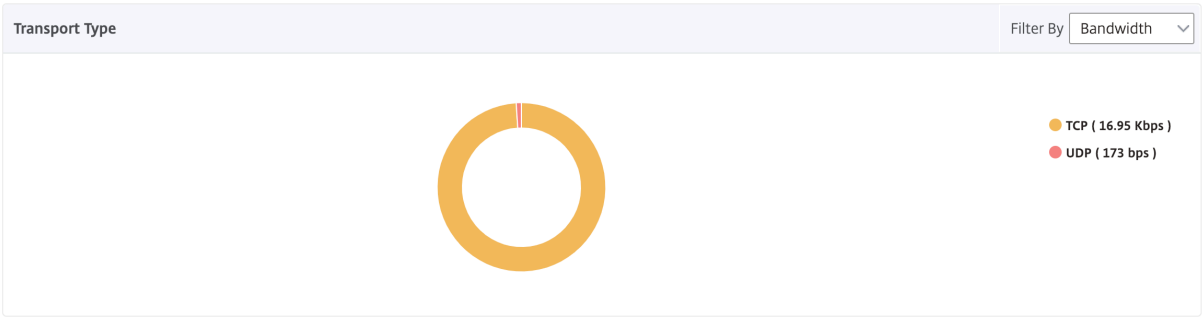
HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über aktive Sitzungen an. In der Tabelle Benutzer wird ein detaillierter Bericht aller Benutzer im System angezeigt. Die Tabelle zeigt Metriken wie WAN-Latenz, DC-Latenz, erneute Übertragungen, RTOs. Einige dieser Metriken sind für Benutzer mit EDT-Sitzungen nicht verfügbar, da sie derzeit aus dem TCP-Stack berechnet werden. Daher werden sie als “NA”angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

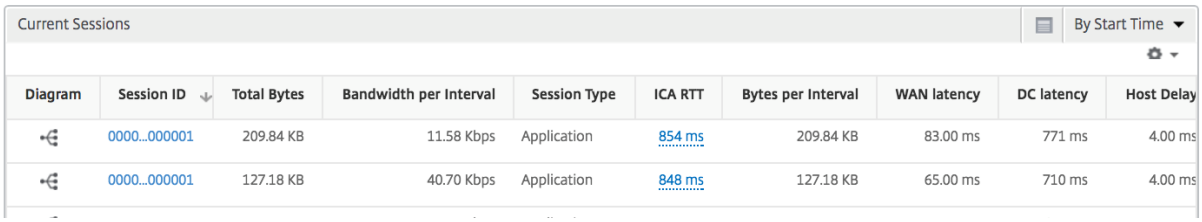
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



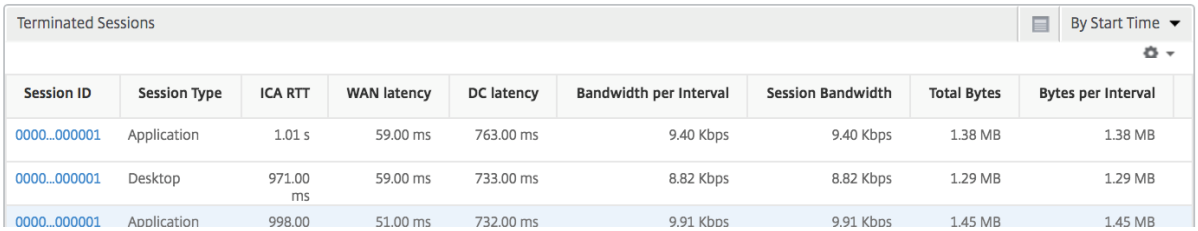
> **Hinweis:**
>
> EDT in HDX Insight wird von NetScaler ADM ab Version 12.1 Build 50.28 unterstützt und ist für ADC-Instanzen ab Version 12.1 Build 49.23 verfügbar.

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.

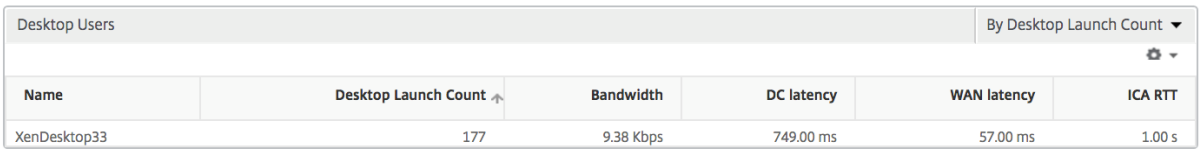


© 1999–2024 Cloud Software Group, Inc. All rights reserved.



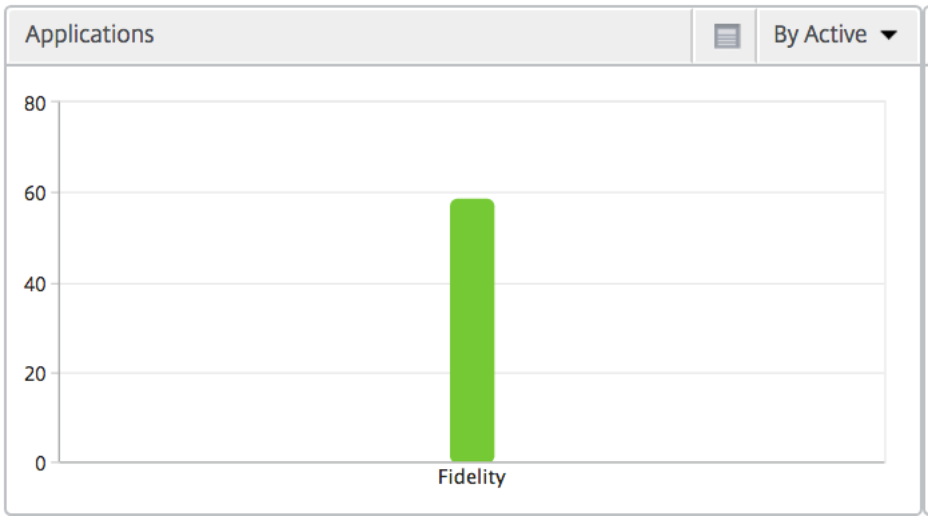
Desktop-Benutzer Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
DC-Latenz	Latenz, die 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.

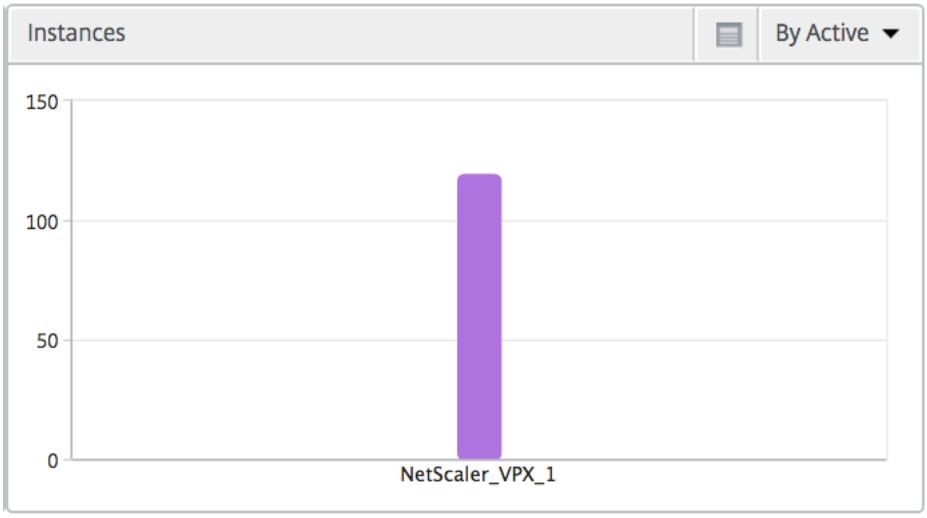


Anwendungen Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Starts und Startdauer darstellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

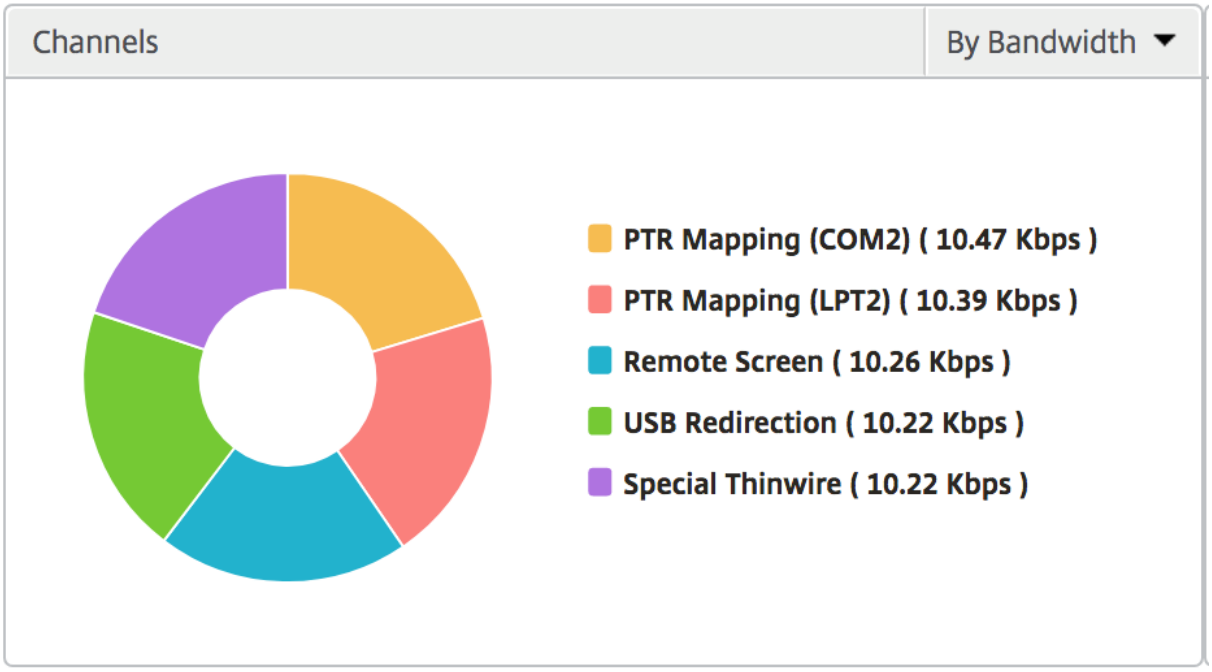


Instanzen Ein Balkendiagramm, das NetScaler ADC Instanzen darstellt, sortiert nach Active und Apps insgesamt

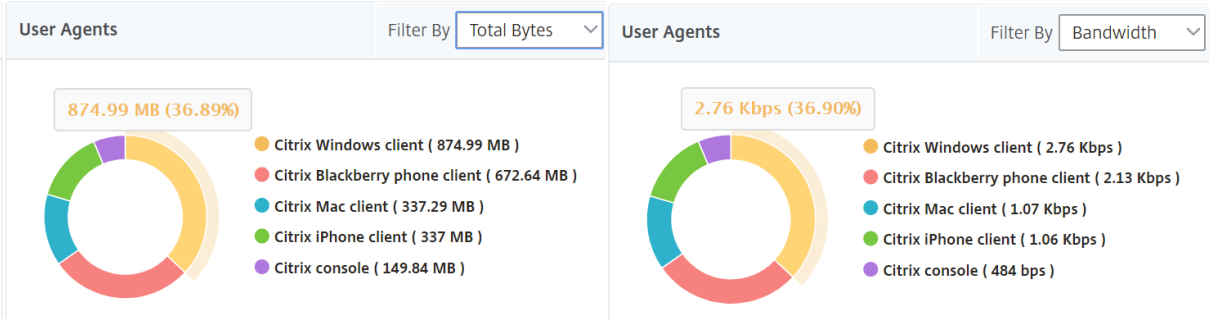


Kanäle Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Benutzeragents 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. 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.

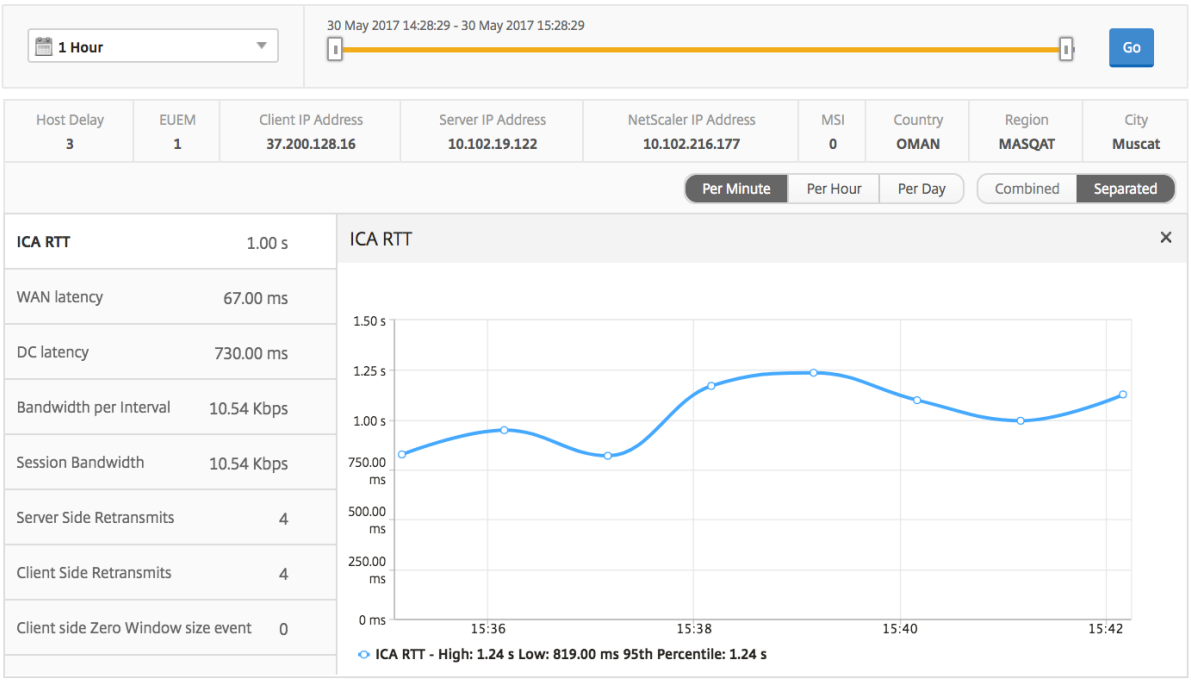
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Apps-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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

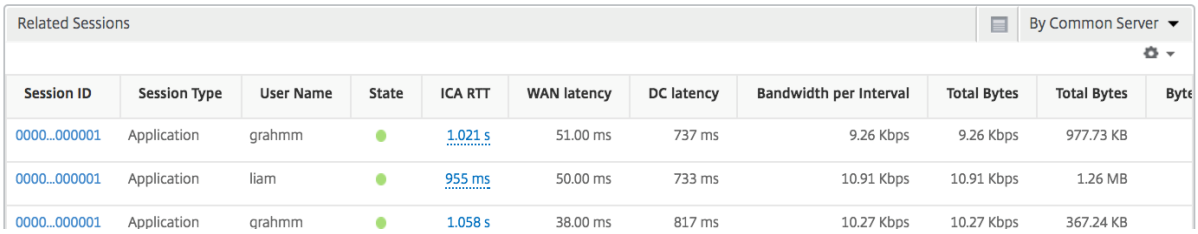
Metriken	Beschreibung
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis 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.

Verbundene 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Anwendung: Berichte und Metriken anzeigen

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Apps.

So navigieren Sie zur Anwendungsansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.

Übersichtsansicht

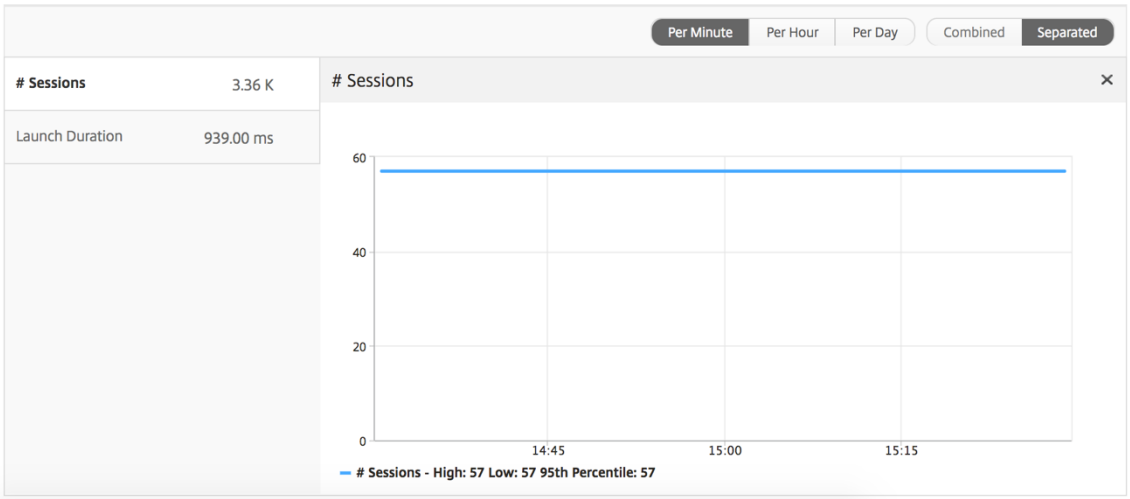
In der Zusammenfassungsansicht werden die Berichte für alle Anwendungen angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

Alle unten aufgeführten Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die entsprechenden Werte für den ausgewählten Zeitraum.

Liniendiagramm

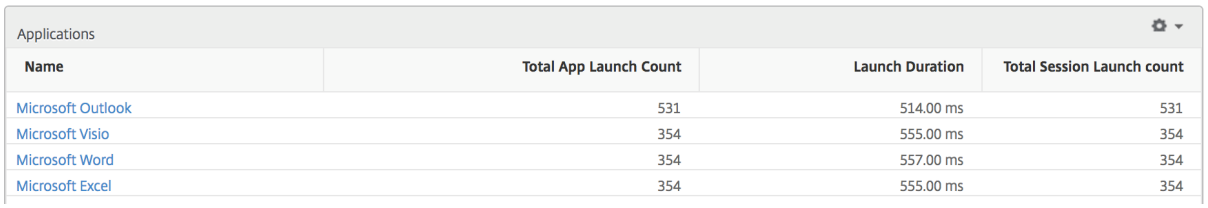
Metriken	Beschreibung
Anzahl Sitzungen	Gesamtzahl der Sitzungen während eines bestimmten Zeitintervalls.
Dauer des Starts	Durchschnittliche Zeit zum Starten einer Anwendung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Zusammengefasster Bericht

Metriken	Beschreibung
Name	Name der Citrix Virtual Apps.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual Apps-Sitzungen während des angegebenen Zeitintervalls.
App-Starts insgesamt	Gesamtzahl der Citrix Virtual Apps, die während des angegebenen Zeitintervalls gestartet wurden.
Startdauer	Durchschnittliche Zeit für den Start der Citrix Virtual App.

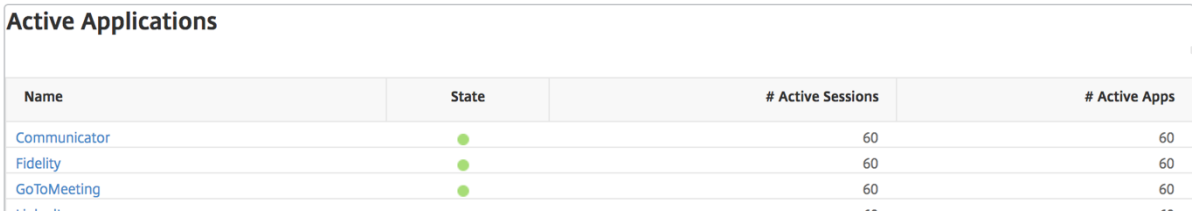


Bericht über aktive Anwendungen

Metriken	Beschreibung
Name	Name der Citrix Virtual App.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

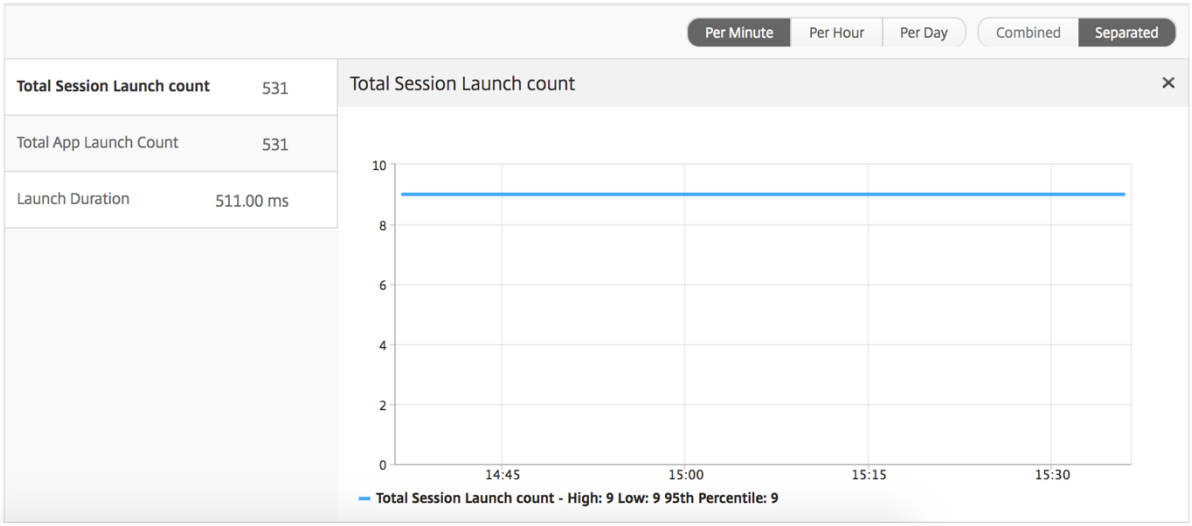


Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* im ausgewählten Zeitraum als *Anwendung* ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Bericht über aktuelle Sessions

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 Apps-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

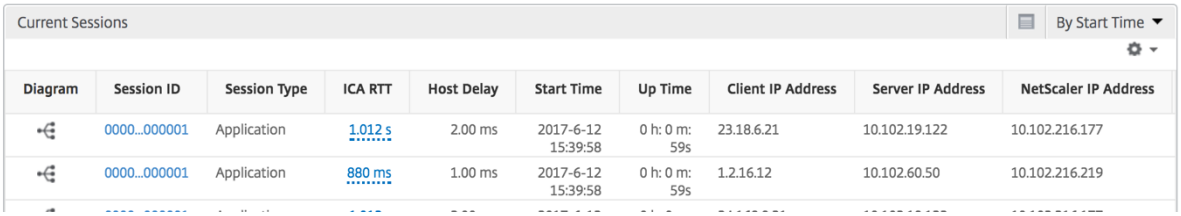
Metriken	Beschreibung
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch 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, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Serverseitige Neuübertragungen	Die Anzahl der 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.
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmte Citrix Virtual App zugreift.
Sitzungs-ID	Eindeutige ID für die Citrix Virtual Apps-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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler 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 den Citrix Virtual Apps beobachtet wurde. Diese Metrik ist nützlich, wenn Nicht-Citrix Geräte im Bereitstellungspfad vorhanden sind.



Ansicht “Sitzung 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.

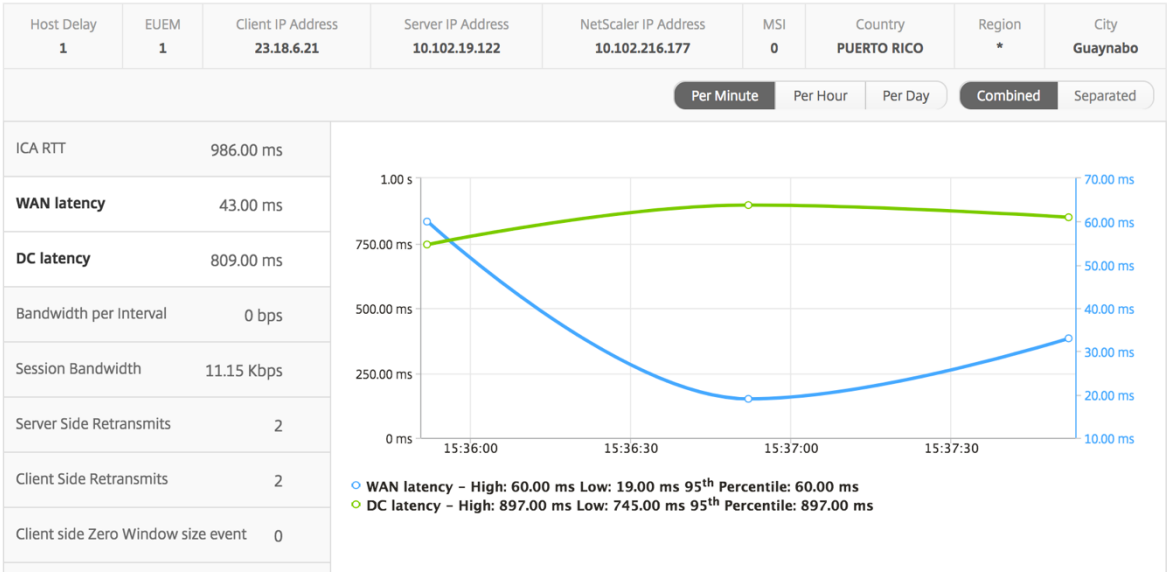
Liniendiagramm

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

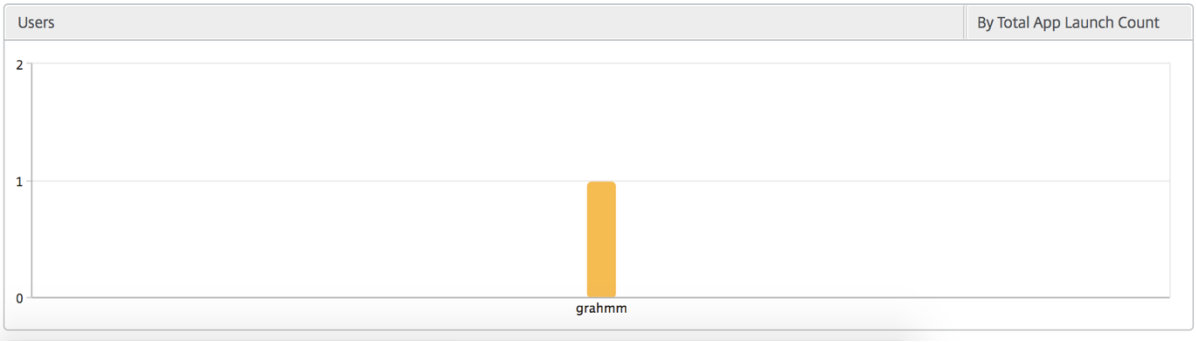
Metriken	Beschreibung
Wiederverbindung der Sitzung	Häufigkeit, mit der die Sitzung wieder verbunden wurde.
ACR-Anzahl	Gesamtzahl der Male, mit denen ein Client Benutzer automatisch wieder mit getrennten Sitzungen verbindet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion 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 zu Backend-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.
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.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



Benutzerbalkendiagramm Das Balkendiagramm des Benutzers stellt die Benutzer dar, die in dieser speziellen App angemeldet sind.



Desktop-Ansicht von Berichten und Metriken

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf Citrix Virtual Desktops.

So navigieren Sie zur Desktopansicht:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 unten aufgeführten Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die entsprechenden Werte für den ausgewählten Zeitraum.

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 Apps-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 wurden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler ADC und Backend-Server erneut übertragen werden.

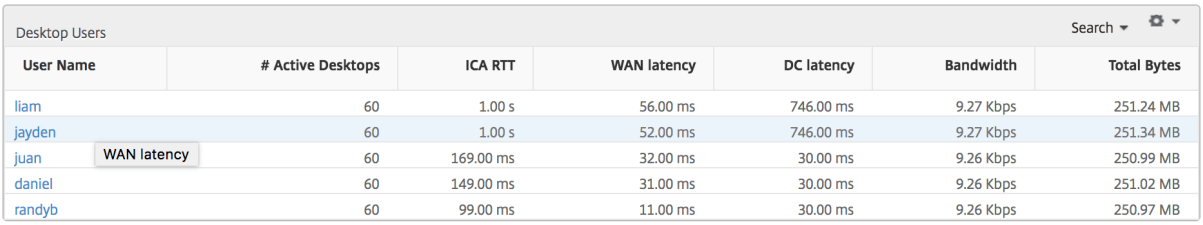
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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	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.

Desktop-Zusammenfassungsbericht

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktops-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 wurden.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Bericht "Schwellenwert" Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde. Weitere Informationen finden Sie unter Erstellen von Schwellenwerten.

Pro Desktop-Ansicht

Die Ansicht pro Desktop bietet detaillierte Berichte zur Endbenutzererfahrung für einen ausgewählten Citrix Virtual Desktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

So navigieren Sie zur jeweiligen Desktop-Ansicht:

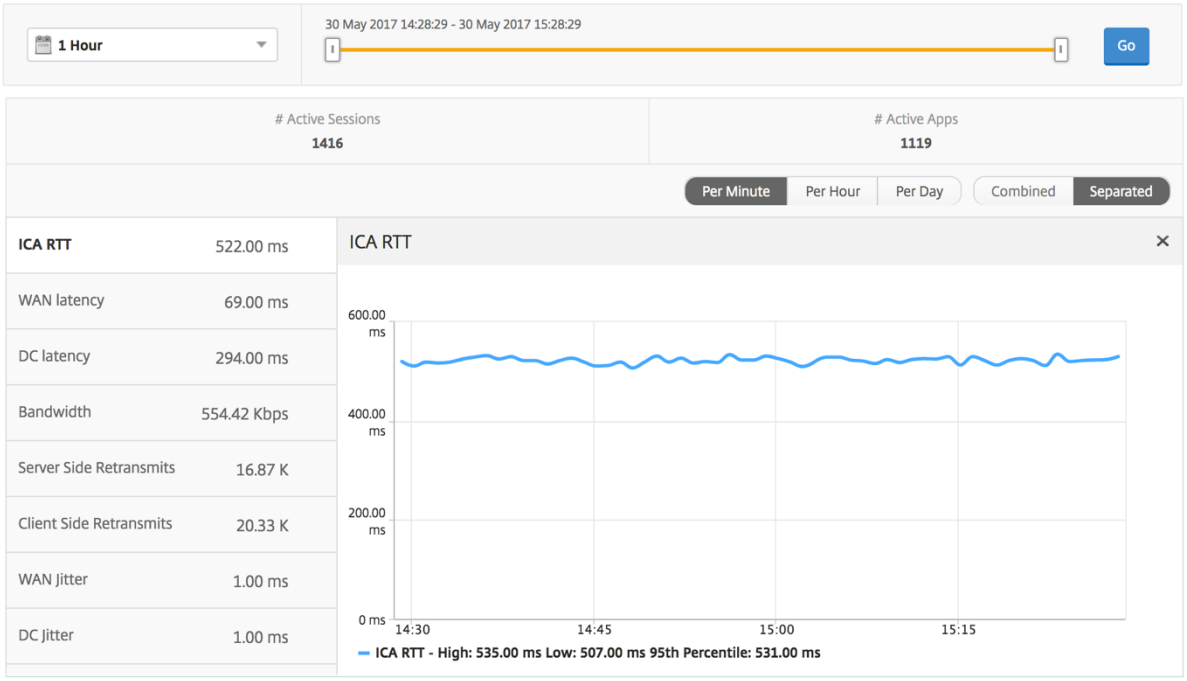
1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem Citrix ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Desktop**.
3. Wählen Sie im **Desktop-Zusammenfassungsberichteinen bestimmten Desktop**aus.

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 Apps-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 wurden.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.
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.

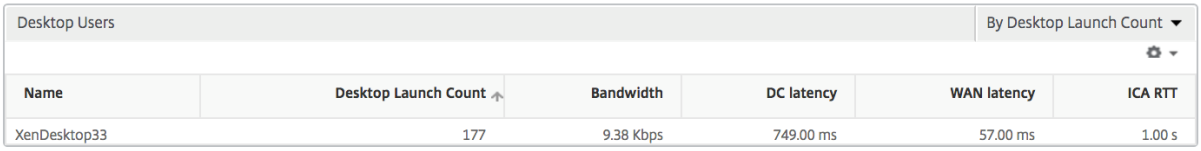


Bericht "Desktop-Benutzer" Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. Das heißt, zwischen NetScaler Gateway und VDI- oder CVAD- oder StoreFront-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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 Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

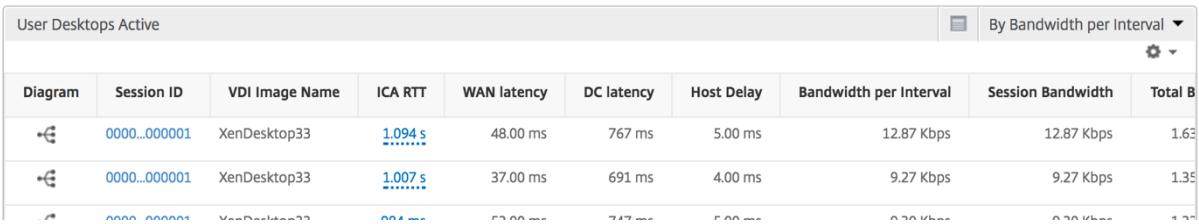
Metriken	Beschreibung
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual Apps-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und Backend-Server.
VDI-Imagename	Name des Citrix Virtual Desktop, mit dem der Benutzer verbunden ist
Diagramm	



Sitzungsansicht pro Desktop

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:

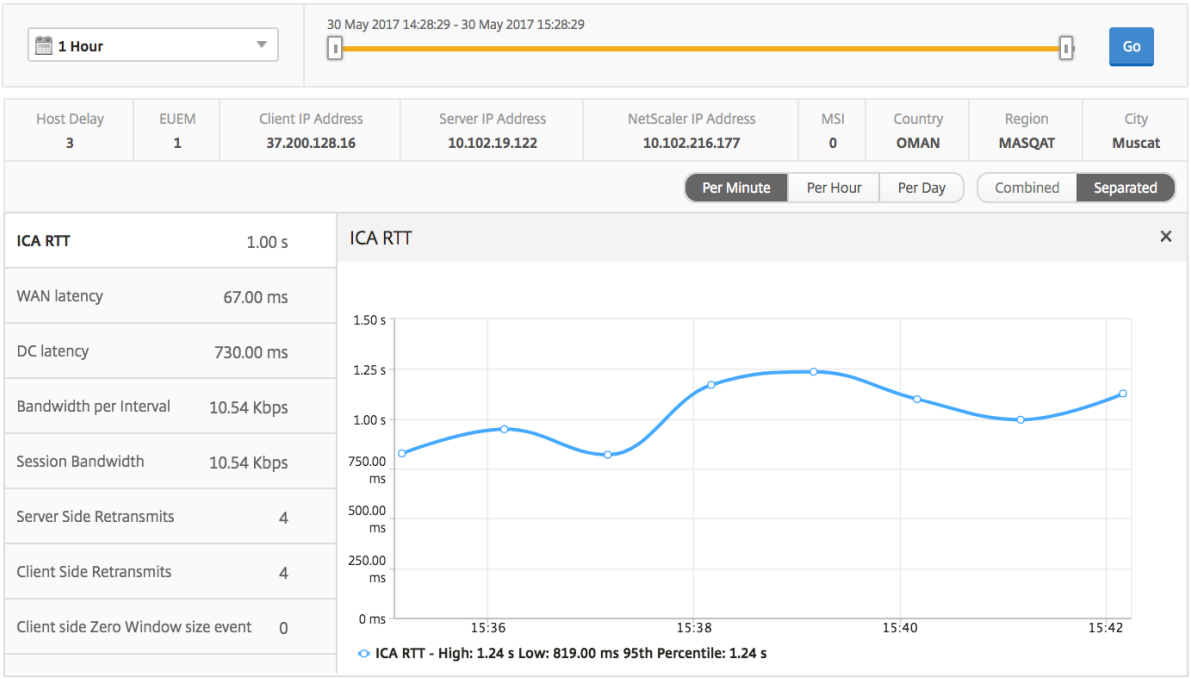
1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**.
3. Wählen Sie im Abschnitt **Benutzerübersichtsbericht** einen bestimmten Benutzer aus.
4. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Apps-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 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.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



Bericht zu verwandten Desktop-Sitzungen Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die Citrix ADCs fließt, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

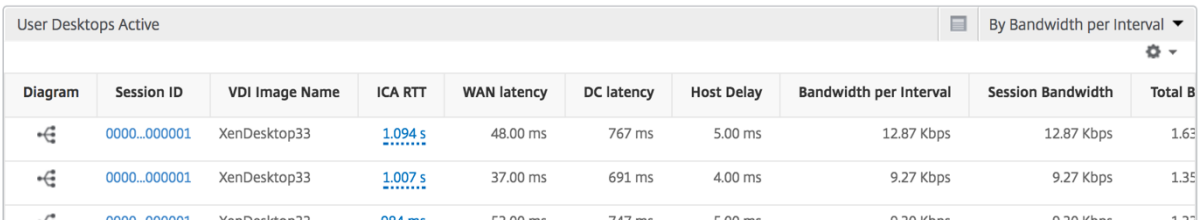
Metriken	Beschreibung
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Byte pro Intervall	Anzahl der Bytes, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wurden.
Startzeit	Startzeit der Sitzung.
Betriebszeit	Dauer der Sitzung.
Client-IP-Adresse	Endbenutzer-IP.
Server-IP-Adresse	Backend/Citrix Virtual Apps-Server-IP.
NetScaler IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Empfängertyp: Citrix Windows Client
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Anzahl der HA-Failover	Häufigkeit, mit der ein HA-Failover aufgetreten ist.
Grund für die Kündigung	Zeigt den Grund für einen Sitzungsabbruch an. Beispiel: ICA-Sitzungstimeout, Sitzung wurde vom Benutzer beendet.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler 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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler ADC und Backend-Server.



Instanz: Berichte und Metriken anzeigen

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf die NetScaler ADC Instanz (n).

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

Ansicht "Instanzübersicht"

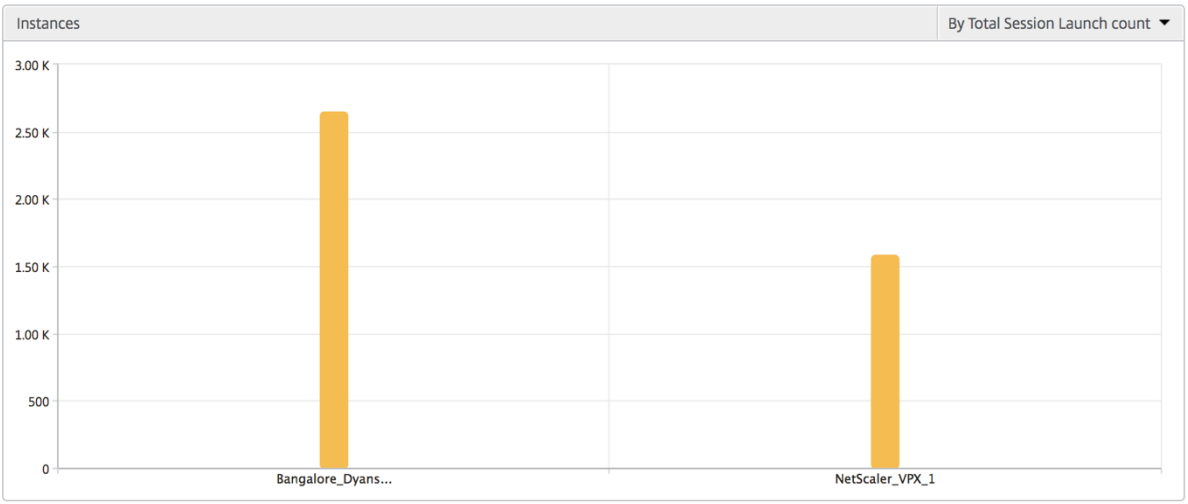
Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler ADC Instanzen anzeigt, die NetScaler ADM hinzugefügt werden.

Alle unten aufgeführten Metriken/Berichte, sofern nicht explizit erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Instanzbalkendiagramm

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

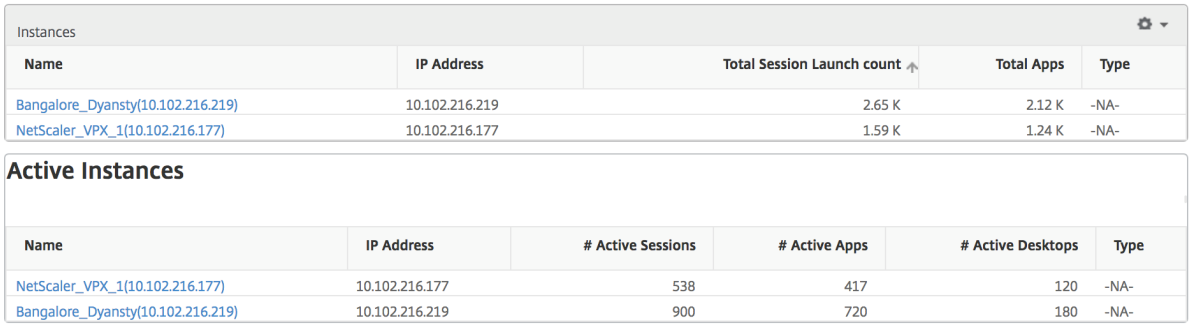
In diesem Diagramm wird die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts angezeigt.	Gesamtzahl der Apps, die aus dem Drop-down-Menü oben rechts auf der Diagramm-Arbeitsfläche ausgewählt werden können.



Zusammenfassungsbericht zu Instanzen/aktiven Instances

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	–

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Instances

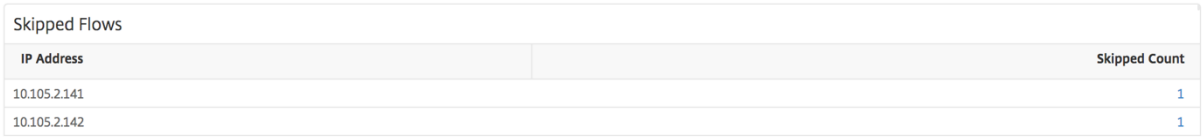
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

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 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 Receiver sind möglicherweise nicht Teil der Receiver auf der Positivliste; daher werden diese Sitzungen von der Überwachung übersprungen.



Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

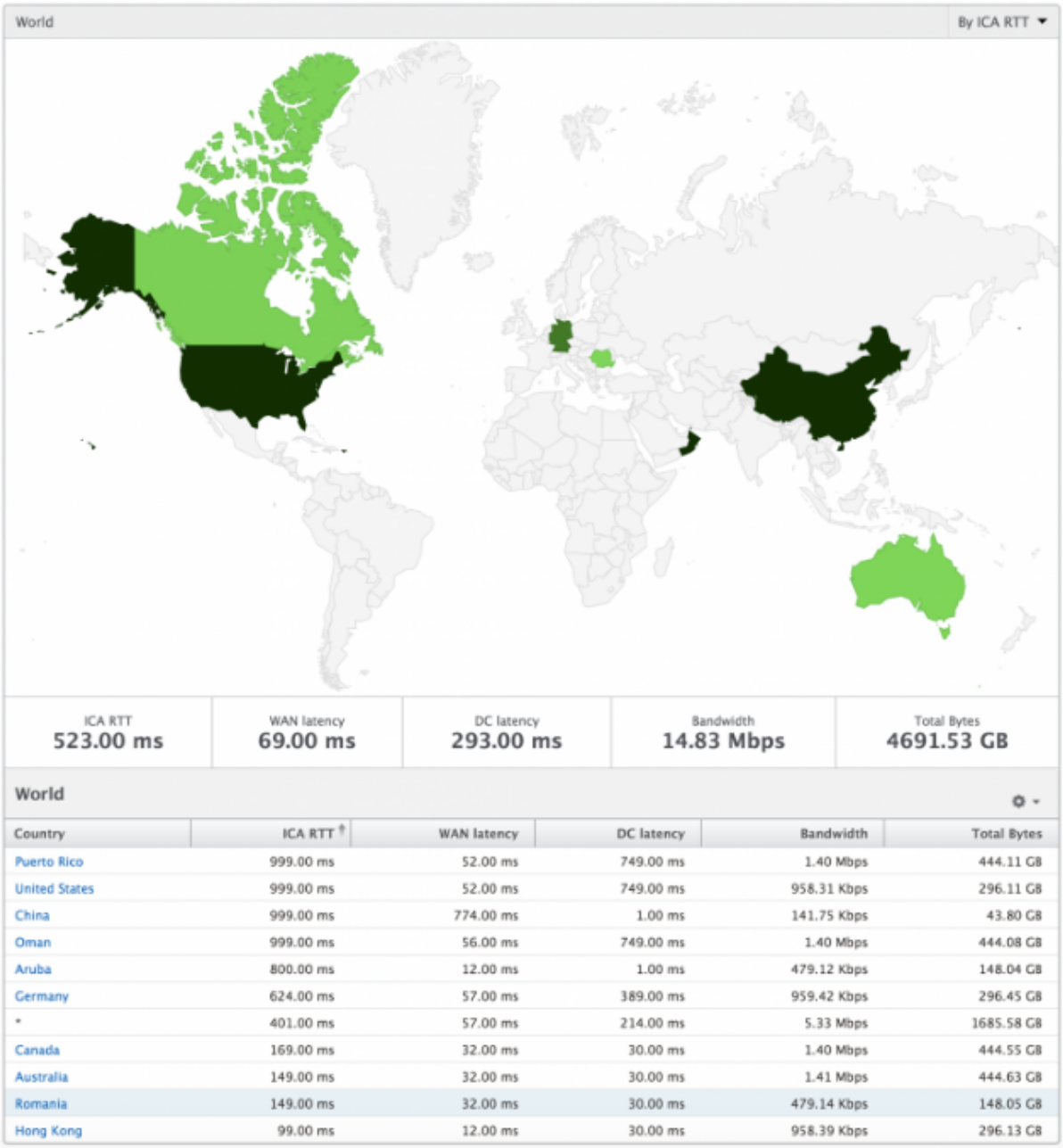
Weltansicht Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, einen Drilldown zu einem bestimmten Land und weiter in Städte durchführen, indem sie einfach auf die Region klicken. 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 der einzelnen Metriken wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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:

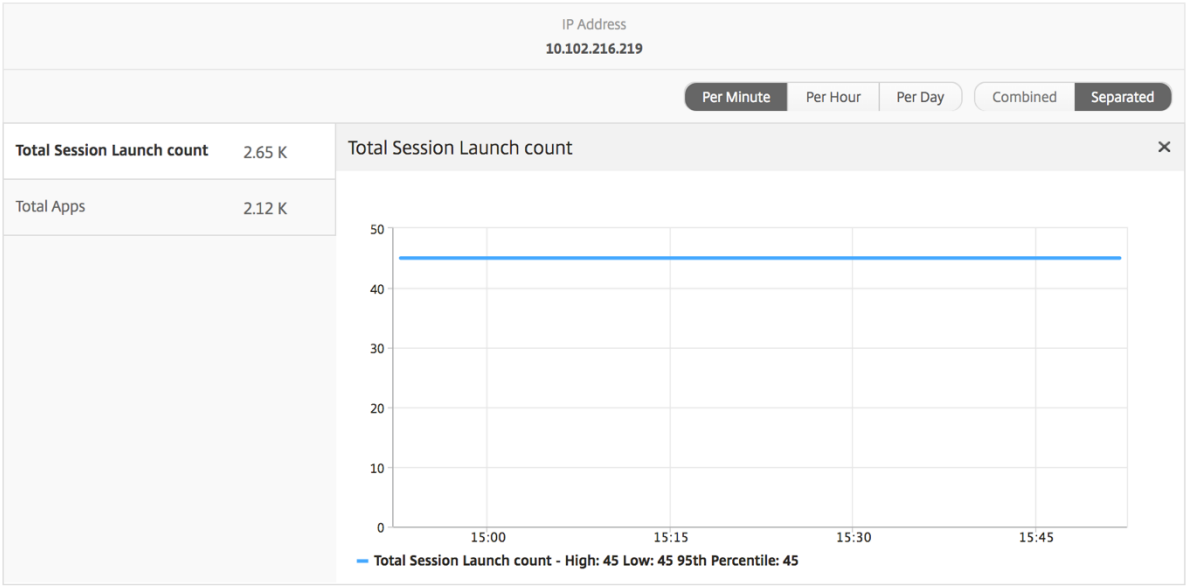
1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Navigieren Sie zu **Analytics > HDX Insight > Instances**.
3. Wählen Sie im **Bericht Instanzzusammenfassung eine bestimmte Instanz** aus.

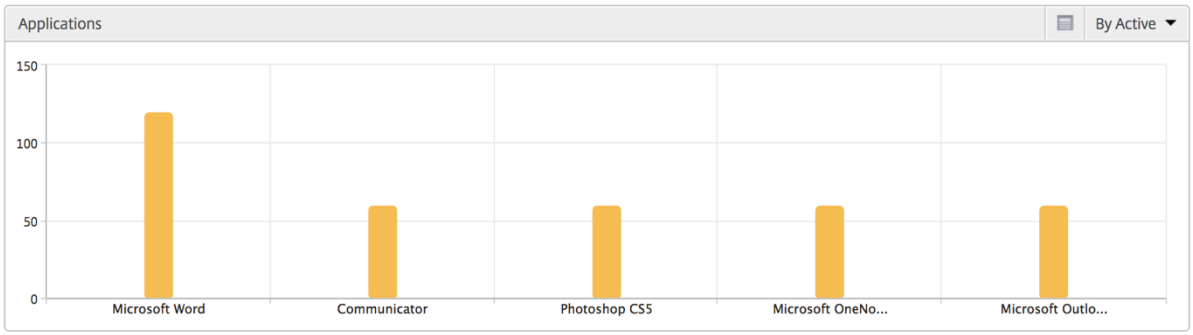
Liniendiagramm

Metriken	Beschreibung
IP-Adresse	Dies stellt die NetScaler-IP-Adresse der ausgewählten Instanz dar.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual Apps-Sitzungen während des angegebenen Zeitintervalls.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.



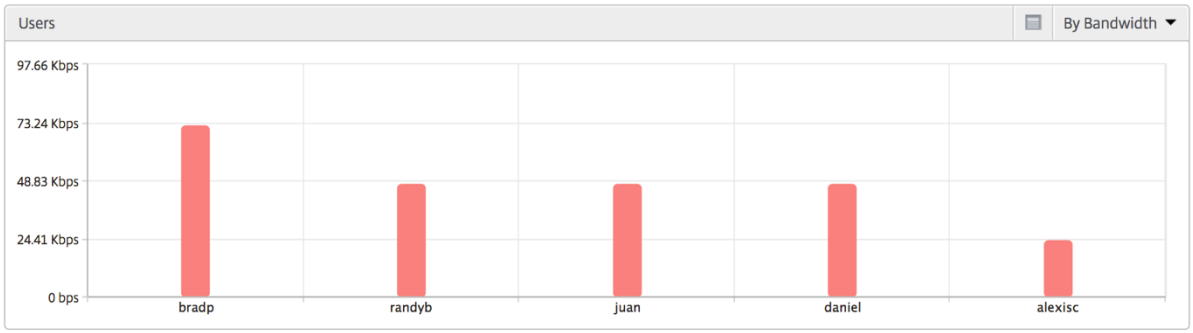
Balkendiagramm für Anwendungen Zeigt die 5 besten Anwendungen basierend auf den folgenden Kriterien an: nach aktiven Apps, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Start-Anzahl oder Startdauer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Balkendiagramm "Benutzer" Das Balkendiagramm "Benutzer"zeigt die fünf wichtigsten Benutzer anhand der folgenden Kriterien an:

- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT

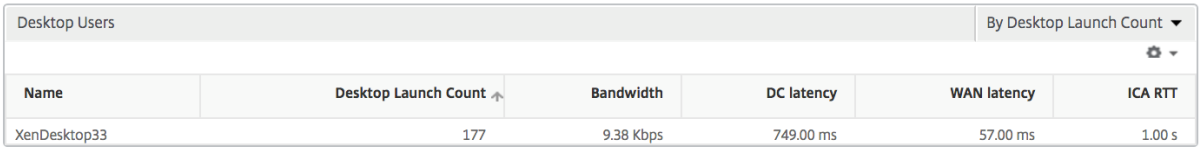


Bericht "Desktop-Benutzer" Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Anzahl der Desktop-Starts und Bandbreite sortiert werden.

Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

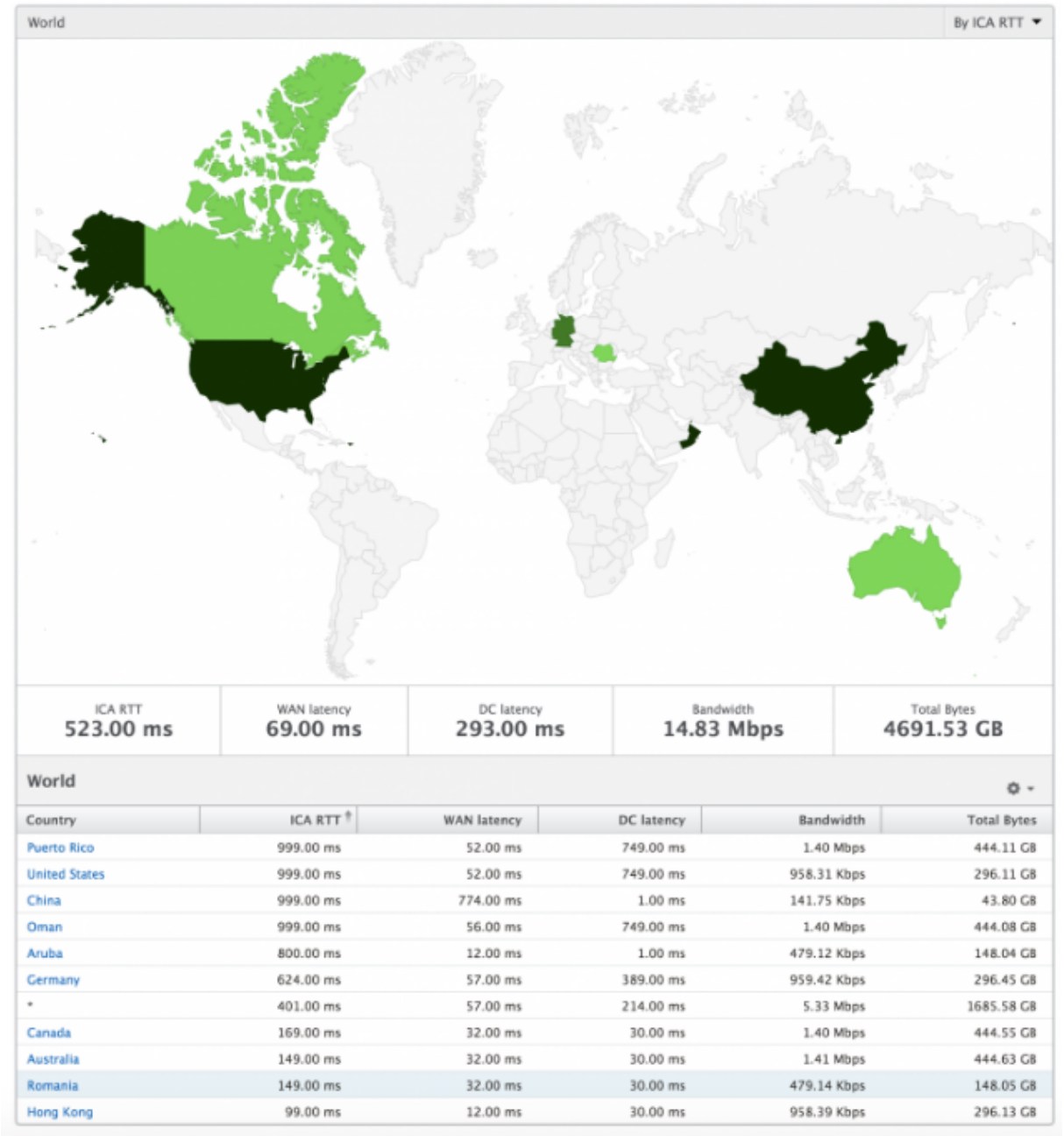


Weltansicht Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, einen Drilldown zu einem bestimmten Land und weiter in Städte durchführen, indem sie einfach auf die Region klicken. 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 der einzelnen Metriken wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

Lizenz Berichte und Metriken anzeigen

Die Lizenzansicht enthält Details zu den NetScaler Gateway -Lizenzinformationen.

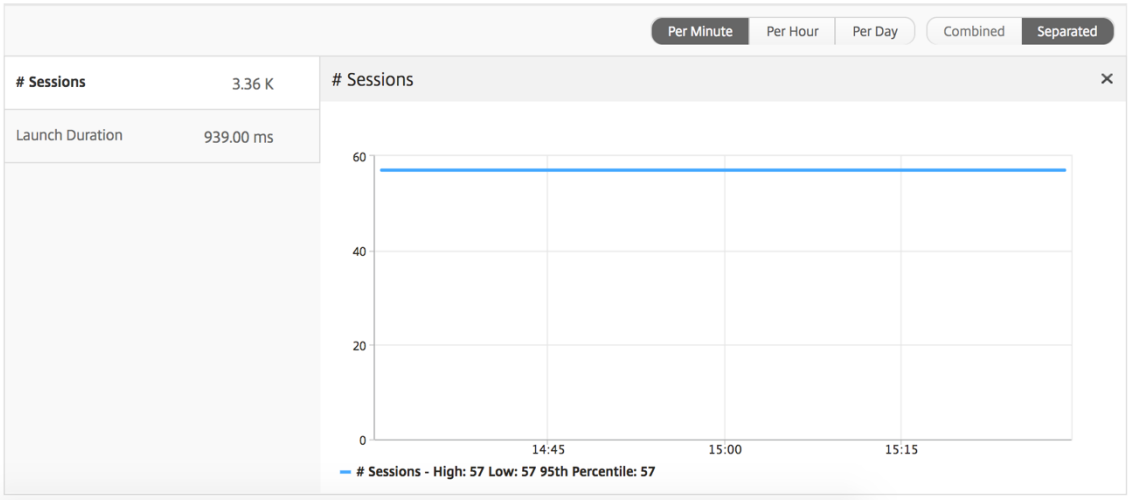
So navigieren Sie zur Lizenzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics > HDX Insight > Lizenzen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 die Citrix Virtual Apps.

So navigieren Sie zur Anwendungsansicht:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.

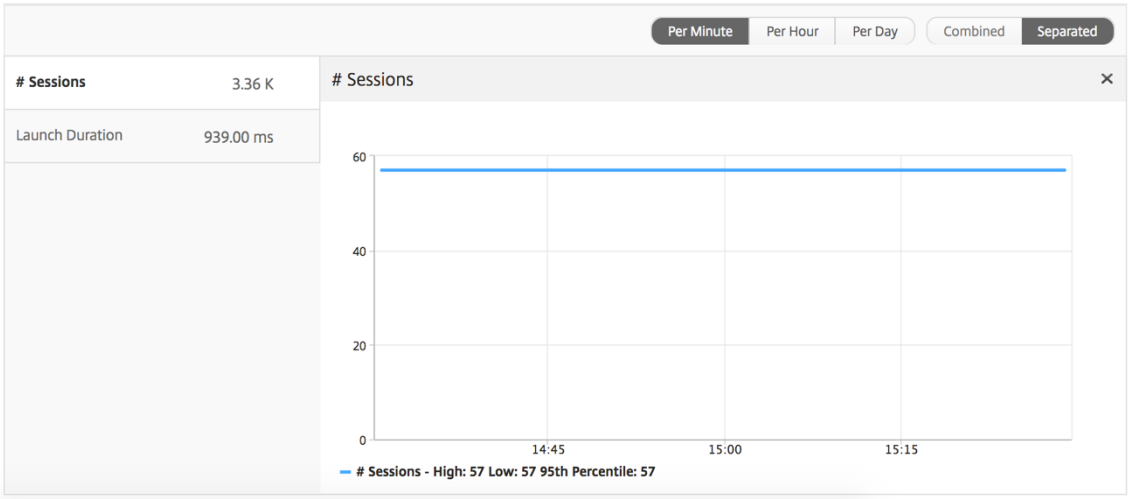
Zusammenfassende Ansicht

In der Zusammenfassungsansicht werden die Berichte für alle Anwendungen angezeigt, die während der ausgewählten Zeitachse angemeldet sind.

Alle 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.

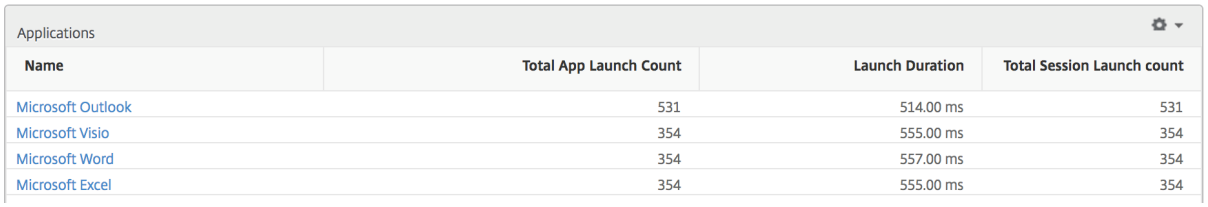


Anwendungsübersichtsbericht

Metriken	Beschreibung
Name	Name der Citrix Virtual App.

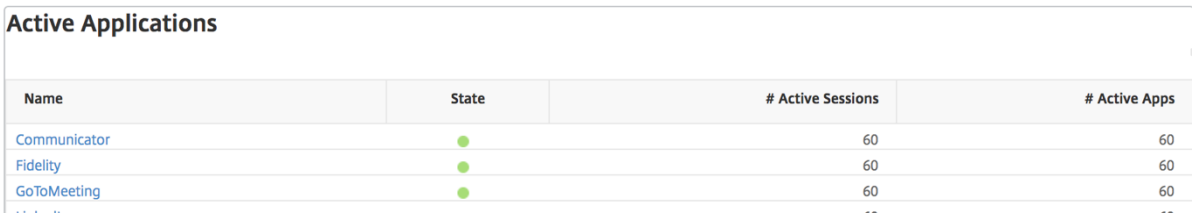
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen während des angegebenen Zeitintervalls.
App-Starts insgesamt	Gesamtzahl der Citrix Virtual Apps, die während des angegebenen Zeitintervalls gestartet wurden.
Startdauer	Durchschnittliche Zeit, die zum Starten der Citrix Virtual Apps benötigt wird.



Bericht Aktive Anwendung

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.



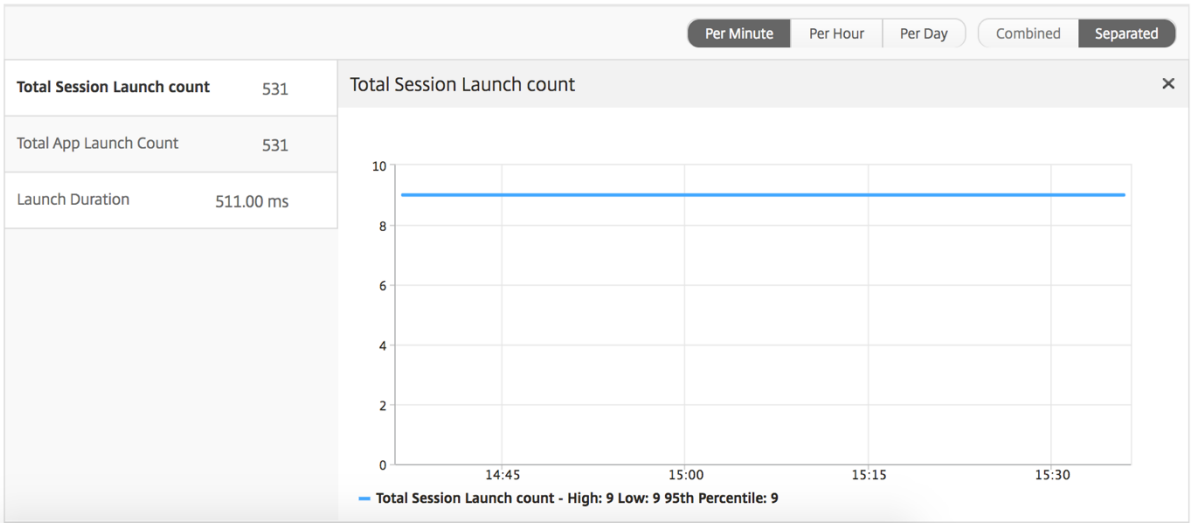
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode 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 Aktuelle Sitzungen

Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
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	Empfängertyp - Citrix Windows Client usw.
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.

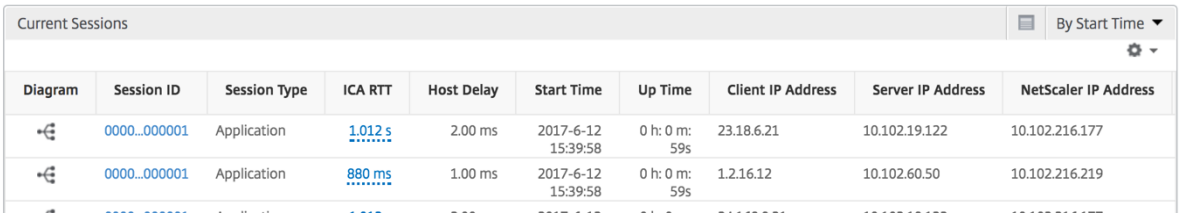
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
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 und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
Benutzername	Der Benutzername des Benutzers, der auf diese bestimmten Citrix Virtual Apps zugreift.
Sitzungs-ID	Eindeutige Kennung für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird “Anwendung”sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für Inaktiv.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn ein definierter Schwellenwert für ein festgelegtes Zeitintervall überschritten wird.
Durchschnittliche Latenz bei Sicherheitsverletzungen	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand “L7-Latenz verletzt”befindet.
Anzahl von L7-Schwellenwertverletzungen	Gibt an, wie oft eine L7-Schwellenverletzung aufgetreten ist.
L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-Instanz beobachtet wurde. Diese Metriken sind nützlich, wenn Nicht-Citrix-Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler Gerät und den Citrix Virtual Apps beobachtet wurde. Diese Metriken sind nützlich, wenn Nicht-Citrix-Geräte im Bereitstellungspfad vorhanden sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Session-Ansicht pro Anwendung

Die Session-Ansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

So zeigen Sie die Sitzungsberichte an:

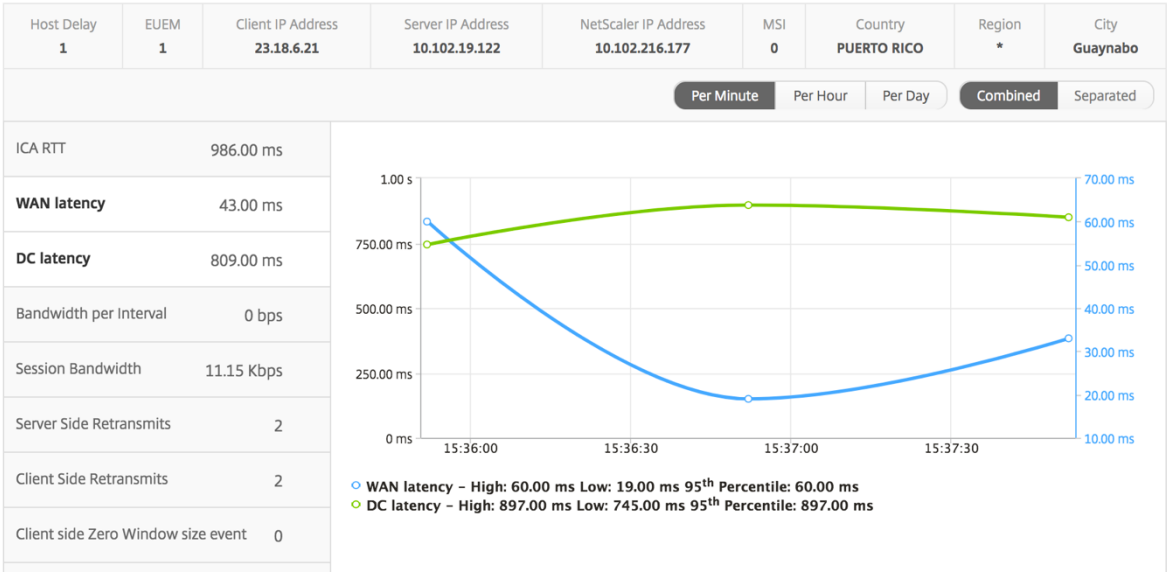
1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Anwendungen**.
2. Wählen Sie im Anwendungsübersichtsbericht einen bestimmten Benutzer aus.
3. Eine Sitzung aus dem Bericht über aktuelle Sitzungen ausgewählt.

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 vom NetScaler zum Endbenutzer.
Serverseitiges Ereignis mit Zero Window-Größe	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung während dieses bestimmten Zeitintervalls verbraucht wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

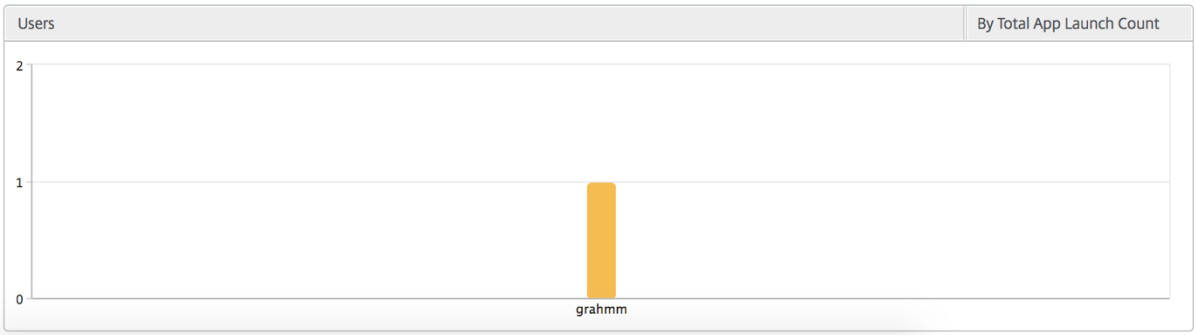
Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Benutzerleistendiagramm

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 die 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**.

Zusammenfassende Ansicht

In der Zusammenfassungsansicht werden die Berichte für alle Citrix Virtual Desktops angezeigt, die während der ausgewählten Zeitleiste angemeldet sind.

Alle unten aufgeführten Metriken/Berichte haben, sofern nicht ausdrücklich erwähnt, die entsprechenden Werte für den ausgewählten Zeitraum.

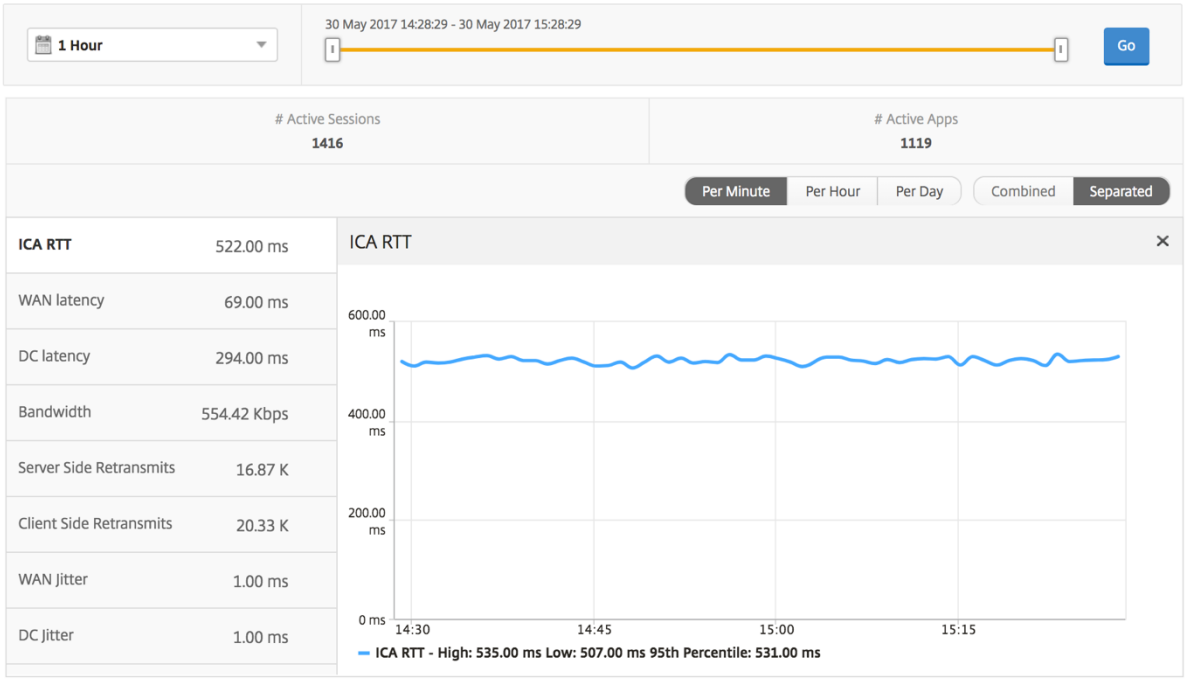
Liniendiagramm

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

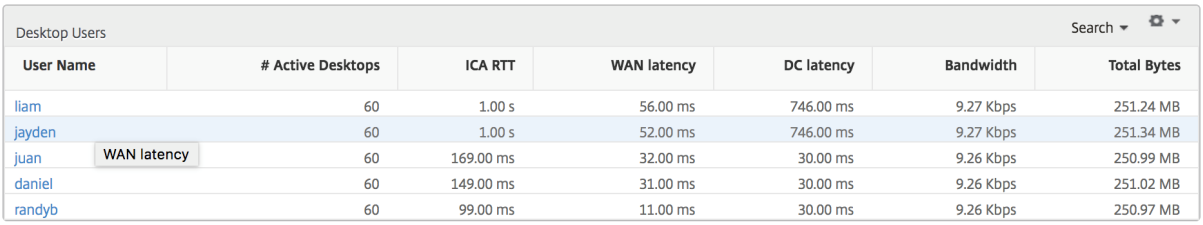


Desktopübersichtsbericht

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 vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.



Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Desktop ausgewählt wurde. 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.

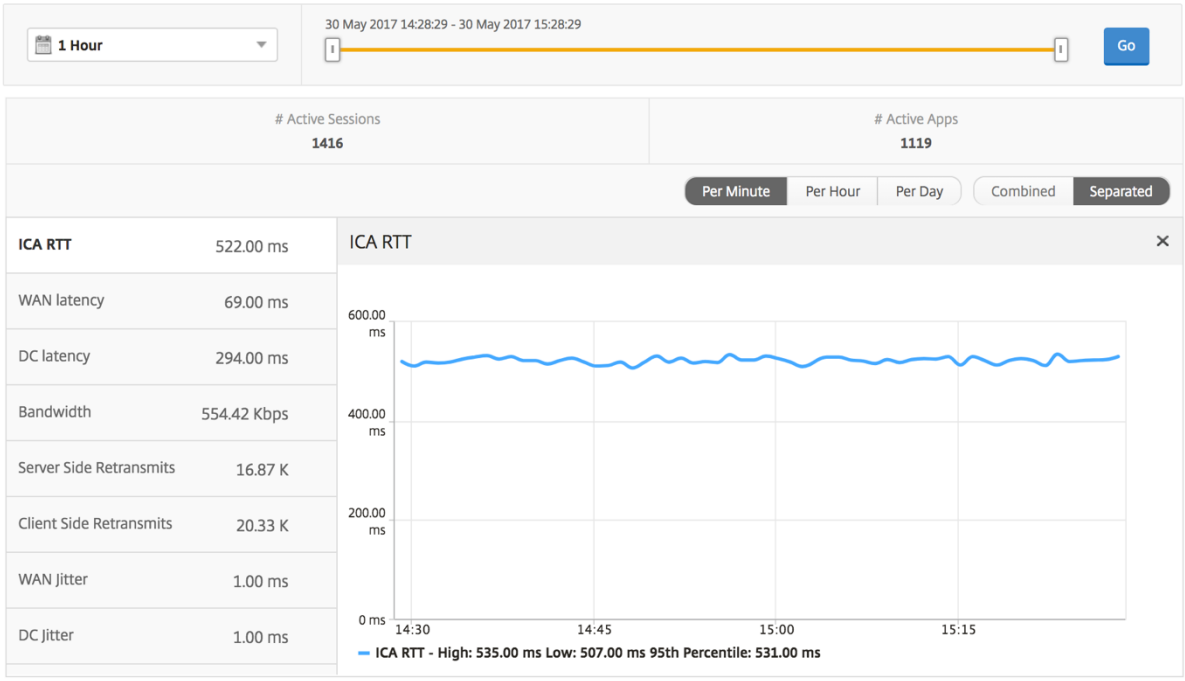
Liniendiagramm

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 Apps-Sitzungen an.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

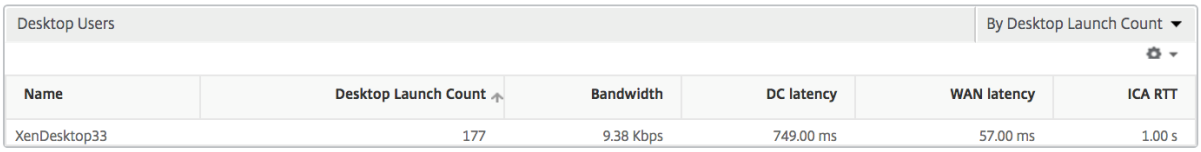


Desktopbenutzer-Bericht

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. D.h. von NetScaler zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Benutzerdesktops Aktiv/Inaktiv Bericht

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

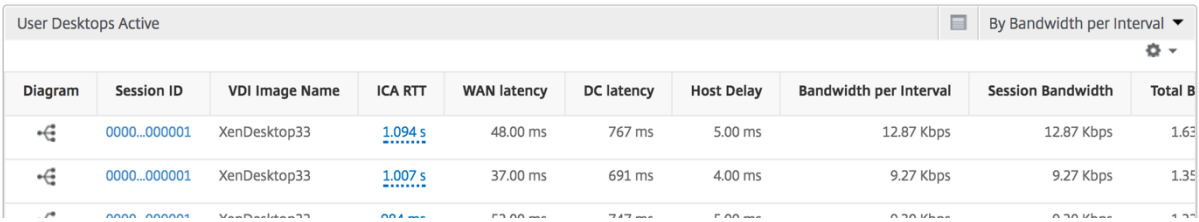
Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die NetScaler ADCs geleitet wird, verursacht durch das Servernetzwerk.
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	Empfängertyp - Citrix Windows Client usw.
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

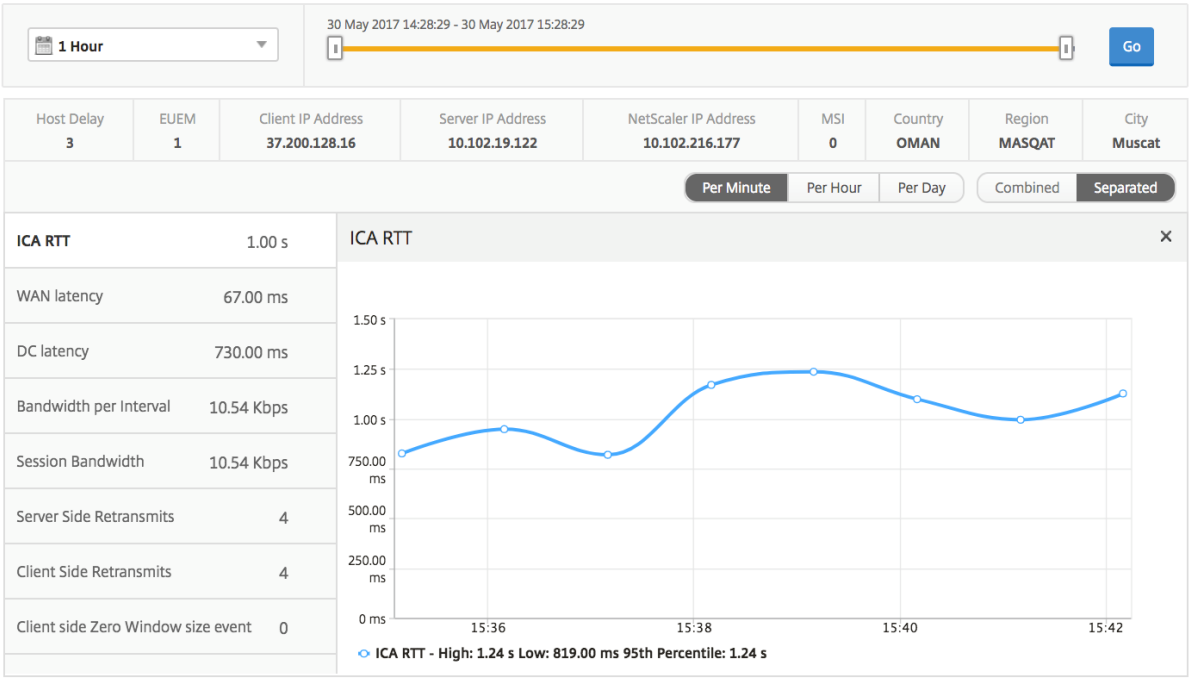
So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

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 Apps and Desktops-Sitzungen an.
ACR-Anzahl	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps-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 vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bericht zu verwandten Desktop-Sitzungen

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählung sortiert werden.

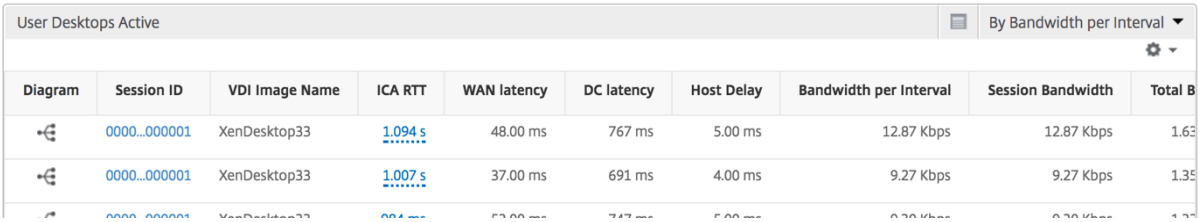
Metriken	Beschreibung
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Hostverzögerung	Durchschnittliche Verzögerung des ICA-Datenverkehrs, der durch die NetScaler ADCs geleitet wird, verursacht durch das Servernetzwerk.
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	Empfängertyp - Citrix Windows Client usw.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
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 Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
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 und Backend-Server erneut übertragen werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
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 Benutzer von Citrix Virtual Apps and Desktops angezeigt.

So navigieren Sie zur Ansicht Benutzer:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler ADM an.
2. Navigieren Sie zu **Analytics** > **HDX Insight** > **Benutzer**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

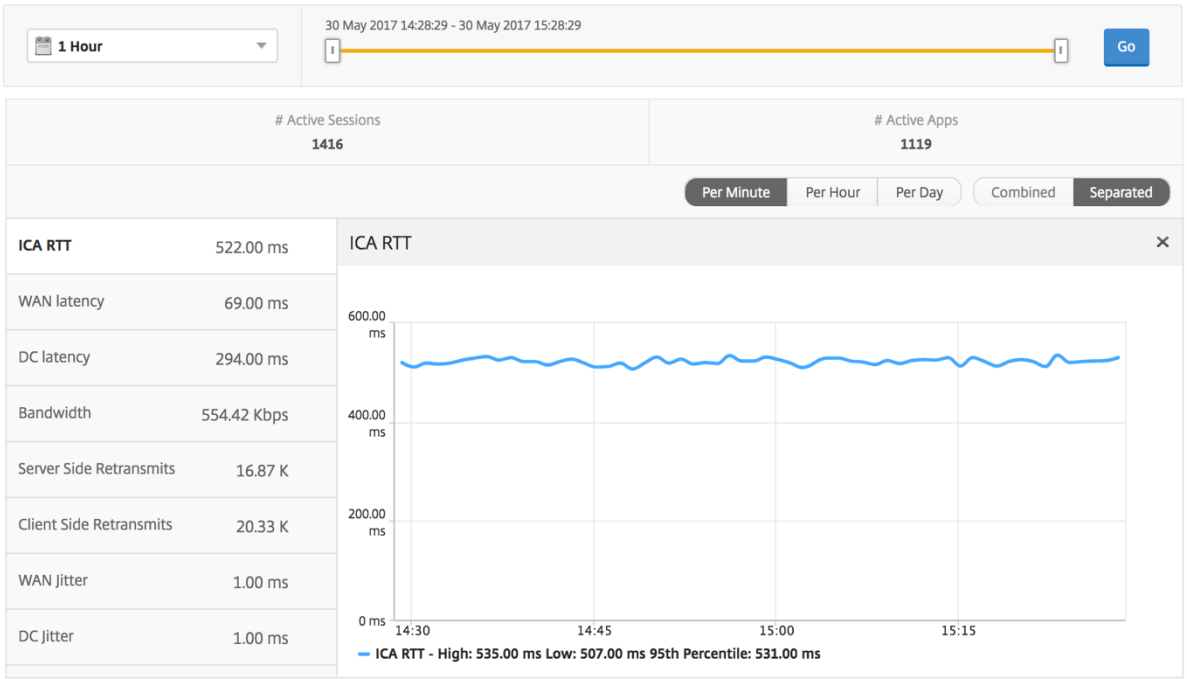
1. Verwenden Sie das Dropdownmenü für den Zeitraum oder den Zeitschieberegler, um das gewünschte Zeitintervall festzulegen.
2. Klicken Sie auf **Go**.

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 Apps-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 vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

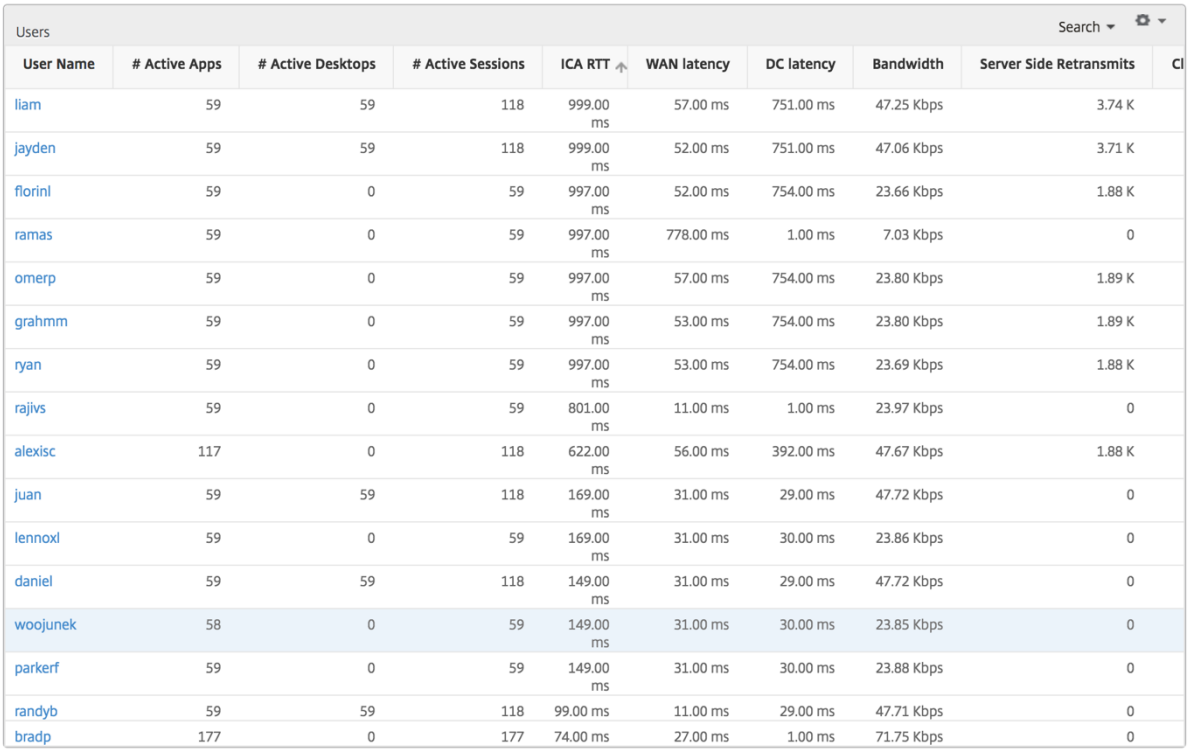
Benutzerübersichtsbericht

Im Folgenden finden Sie die Metriken, die für diesen Bericht spezifisch sind.

Metriken	Beschreibung
Anzahl aktiver Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
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 and Desktops gehostet werden.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.
App-Starts insgesamt	Gesamtzahl der Apps, die vom Benutzer während des ausgewählten Zeitraums gestartet wurden.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops in einem bestimmten Zeitintervall.



Users

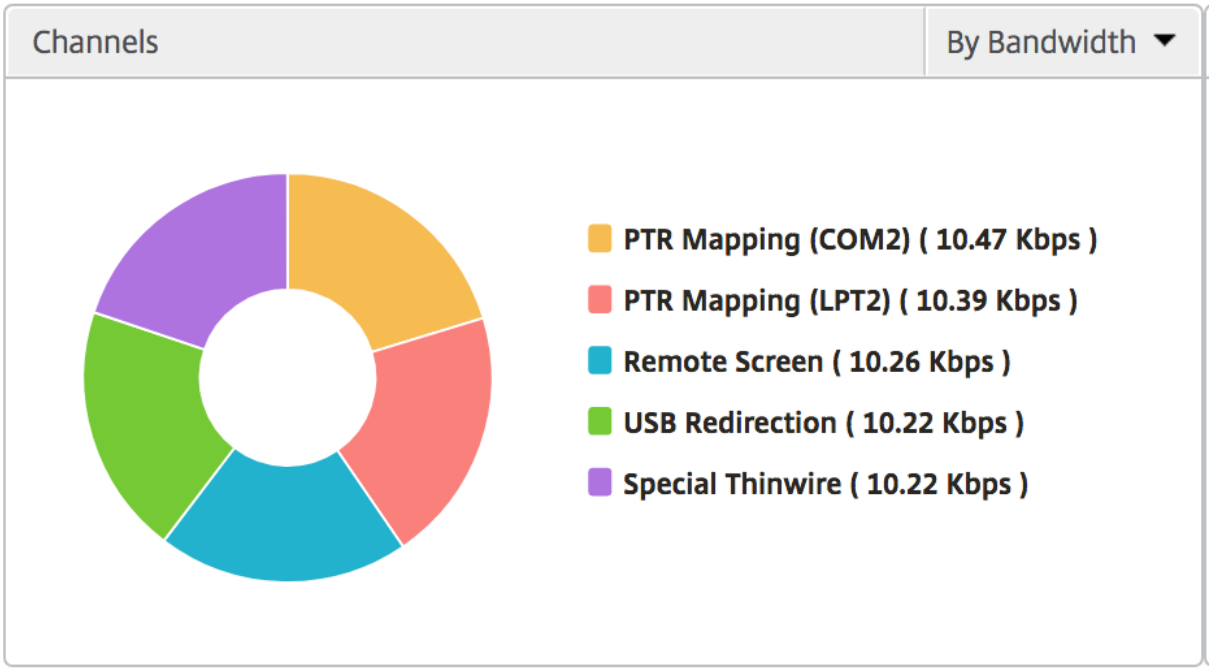
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

Kanäle

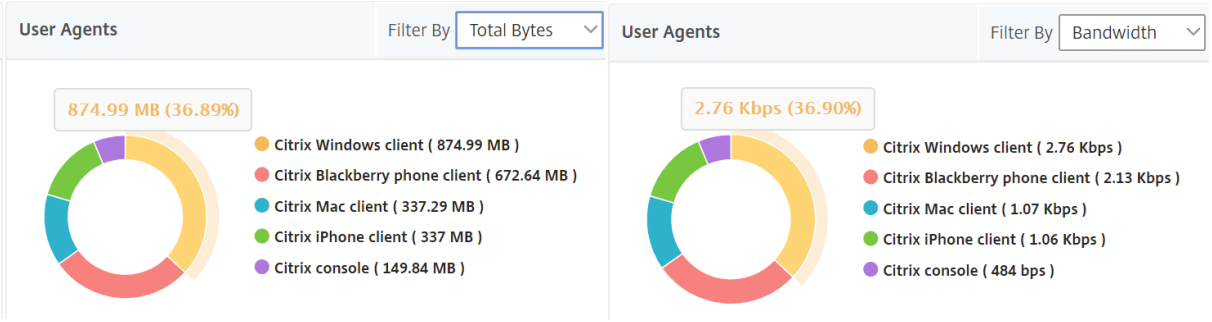
Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Benutzeragents

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 Schwellenwerte für Verstöße

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

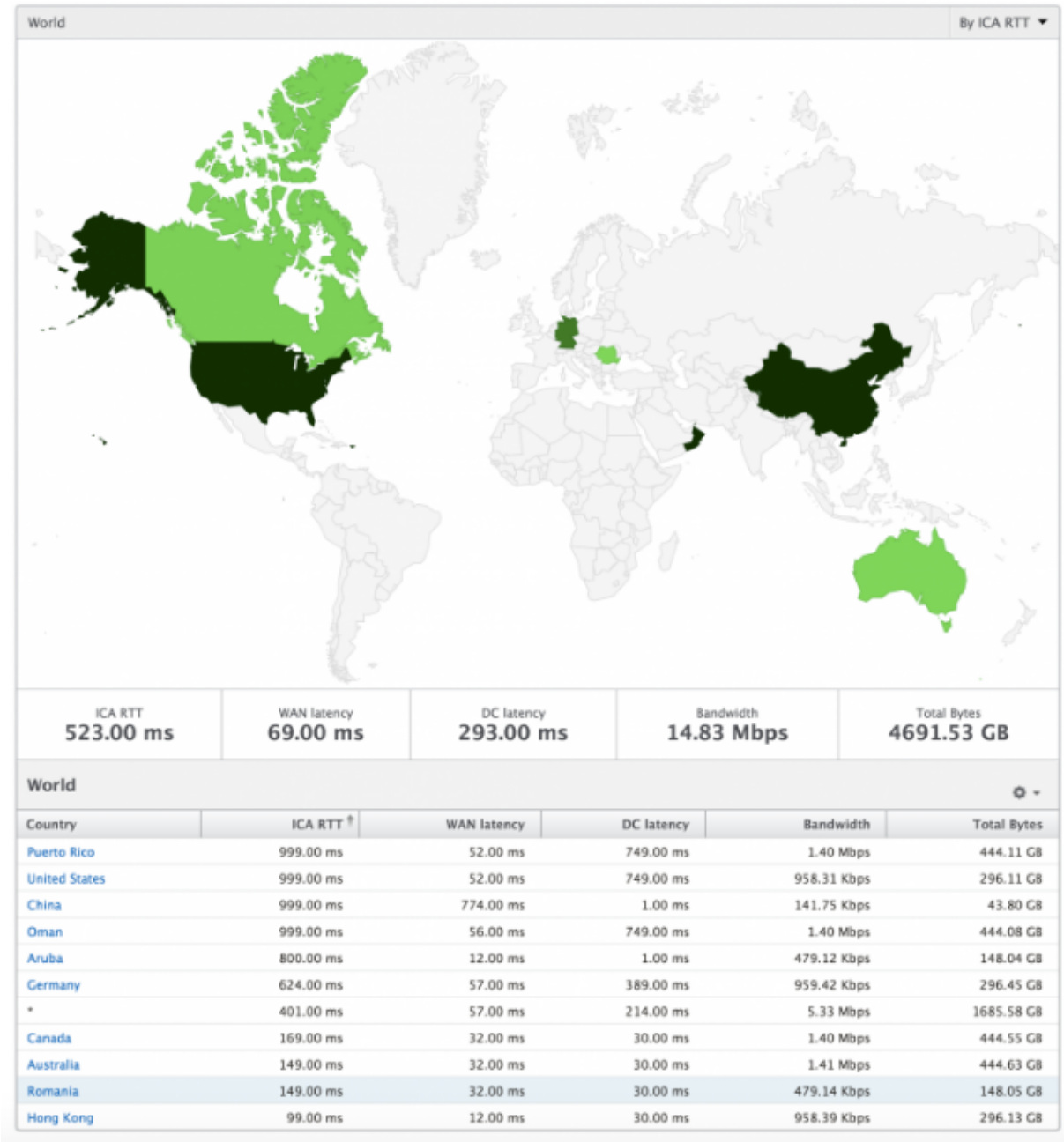
Weltkarte

Mit der Weltkartenansicht in HDX Insight können Administratoren die historischen und aktiven Benutzerdetails aus geografischer Sicht anzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, einen Drilldown zu einem bestimmten Land und weiter in Städte durchführen, indem sie einfach auf die Region klicken. 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 der einzelnen Metriken wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Liniendiagramm

Das Liniendiagramm zeigt eine Zusammenfassung aller Metriken für den ausgewählten Benutzer während des ausgewählten Zeitraums an.

Bericht über aktuelle/beendete 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	Empfängertyp - Citrix Windows Client usw.
Clientversion	Receiver-Version.
MSI	Boolescher Wert (Ja/Nein). Gibt an, ob es sich bei der Sitzung Multistream-ICA ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Bytes insgesamt	Gesamtzahl der Bytes, die der Benutzer während des ausgewählten Zeitraums belegt hat.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

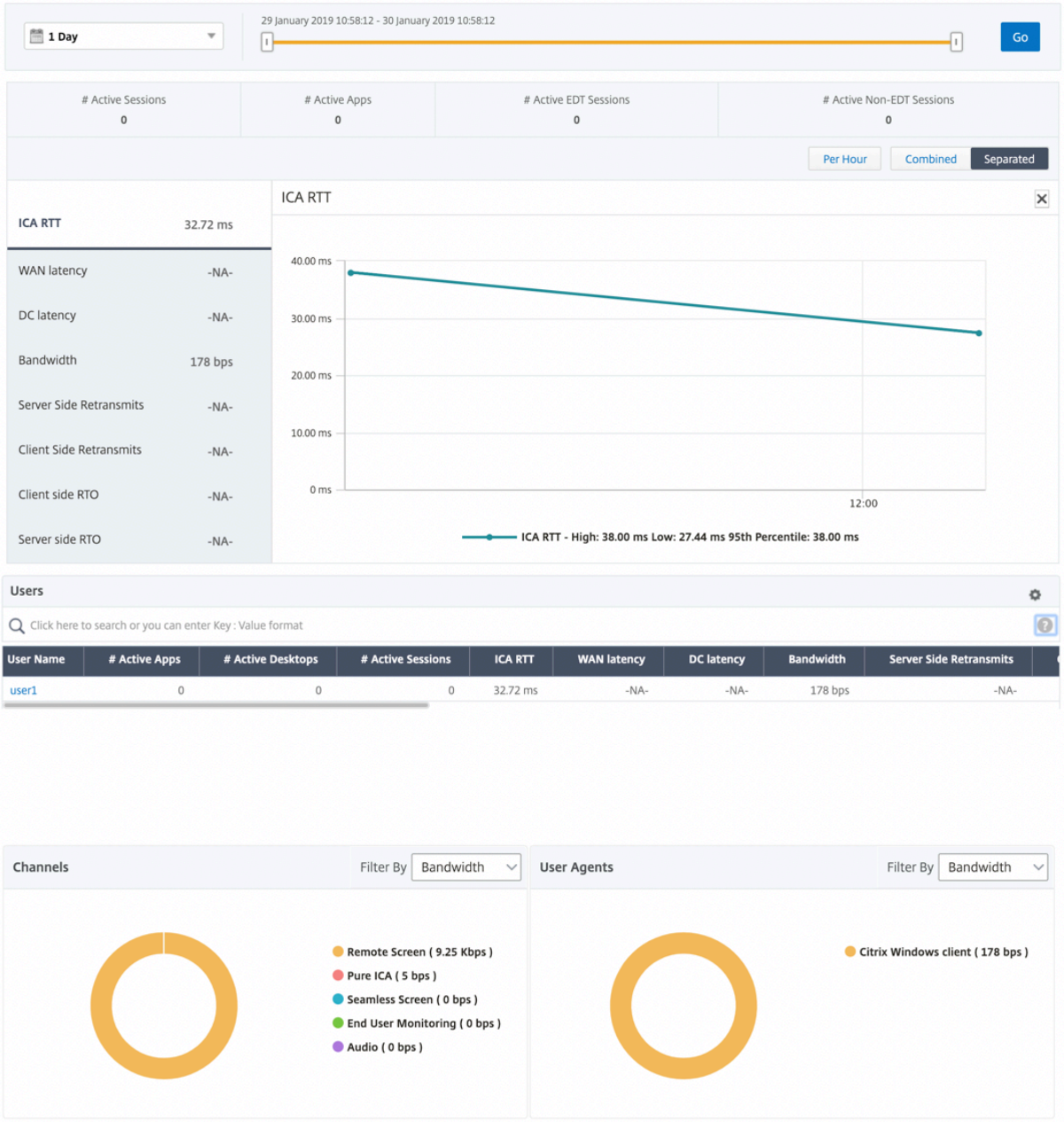
Metriken	Beschreibung
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Clientseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Client ein TCP-Fenster mit Null angekündigt hat.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Ereignis mit Zero Window-Größe	Dieser Leistungsindikator gibt an, wie oft der Server ein TCP-Fenster mit Null angekündigt hat.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.

Unterstützung für EDT in HDX Insight

NetScaler Application Delivery Management (ADM) unterstützt jetzt Enlightened Data Transport (EDT) zur Anzeige von Analysen für HDX Insight. Das heißt, ADM unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für NetScaler Gateway gewährleistet eine hochauflösende Benutzererfahrung virtueller Desktops während der Sitzung für Benutzer, die Citrix Receiver ausführen.

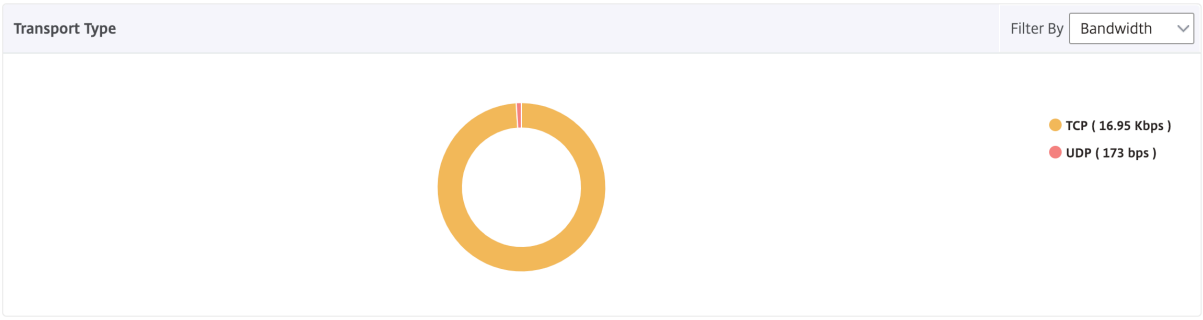
HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über aktive Sitzungen an. In der Tabelle Benutzer wird ein detaillierter Bericht aller Benutzer im System angezeigt. Die Tabelle zeigt Metriken wie WAN-Latenz, DC-Latenz, erneute Übertragungen, RTOs. Einige dieser Metriken sind für Benutzer mit EDT-Sitzungen nicht verfügbar, da sie derzeit aus dem TCP-Stack berechnet werden. Daher werden sie als “NA”angezeigt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



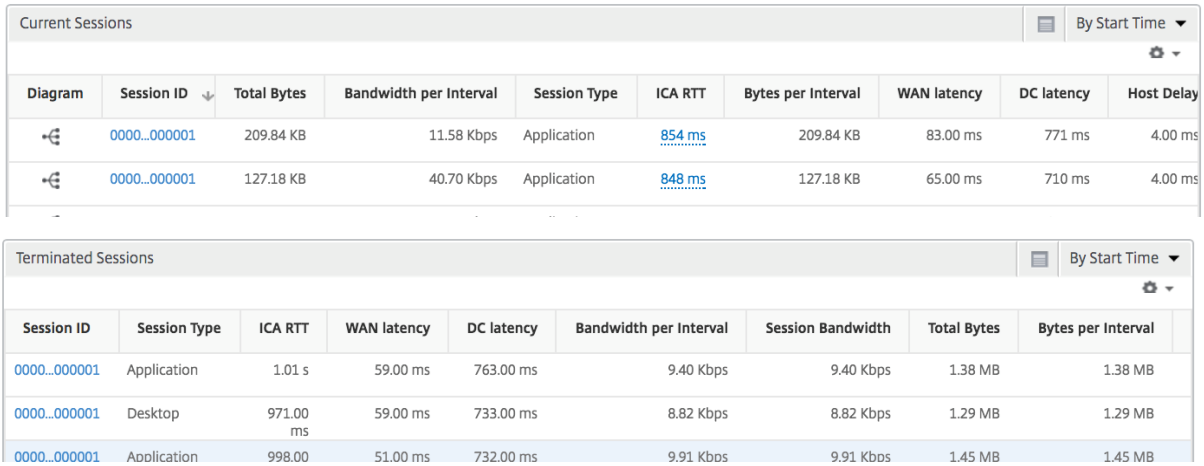
Es wurde ein neues Donutdiagramm eingeführt, mit dem Sie die vom Benutzer verbrauchte Bandbreite und die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



HDX Insight Metriken, die ab NetScaler ADM 12.0 und höher verfügbar sind:

L7 Clientseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-Instanz beobachtet wurde. Diese Metriken sind nützlich, wenn Nicht-Citrix-Geräte im Bereitstellungspfad vorhanden sind.
L7 Serverseitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler Gerät und der Citrix Virtual App beobachtet wurde. Diese Metriken sind 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.

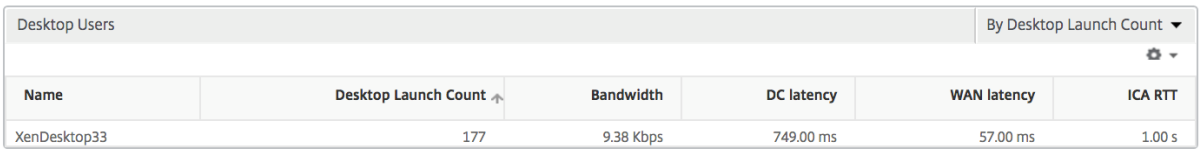


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

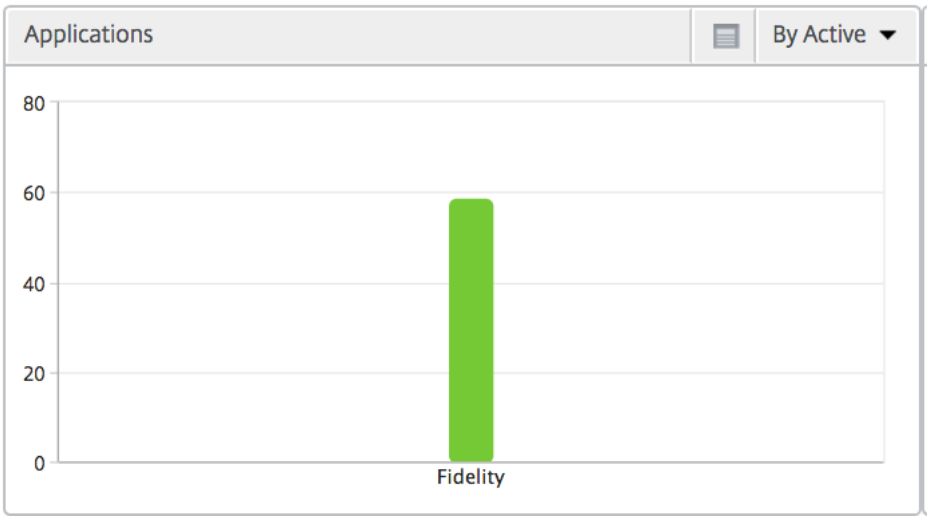
Metriken	Beschreibung
Name	Name des Citrix Virtual Desktop.
Anzahl der Desktop-Starts	Häufigkeit, mit der der Desktop gestartet wurde.
Bandbreite	Gesamtzahl der Byte pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler 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.



Anwendungen

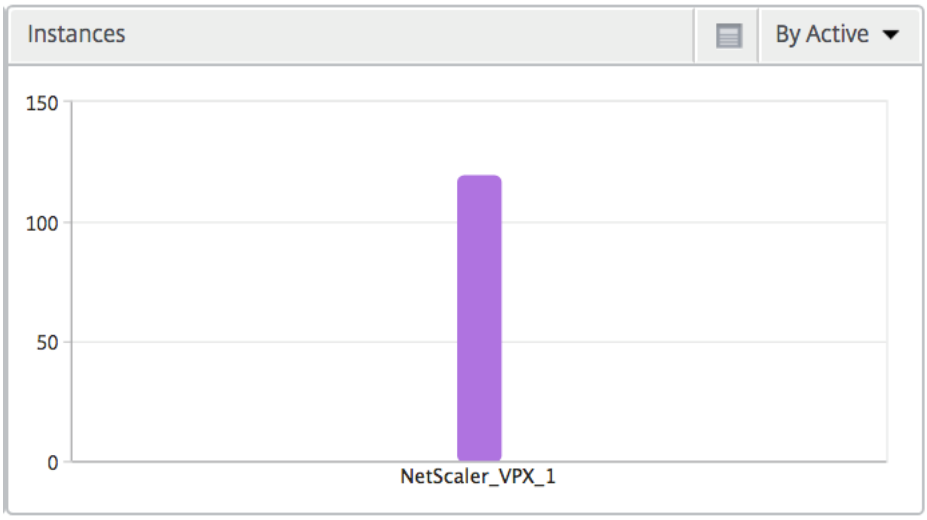
Ein Balkendiagramm, das Apps sortiert nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Starts und Startdauer darstellt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Instanzen

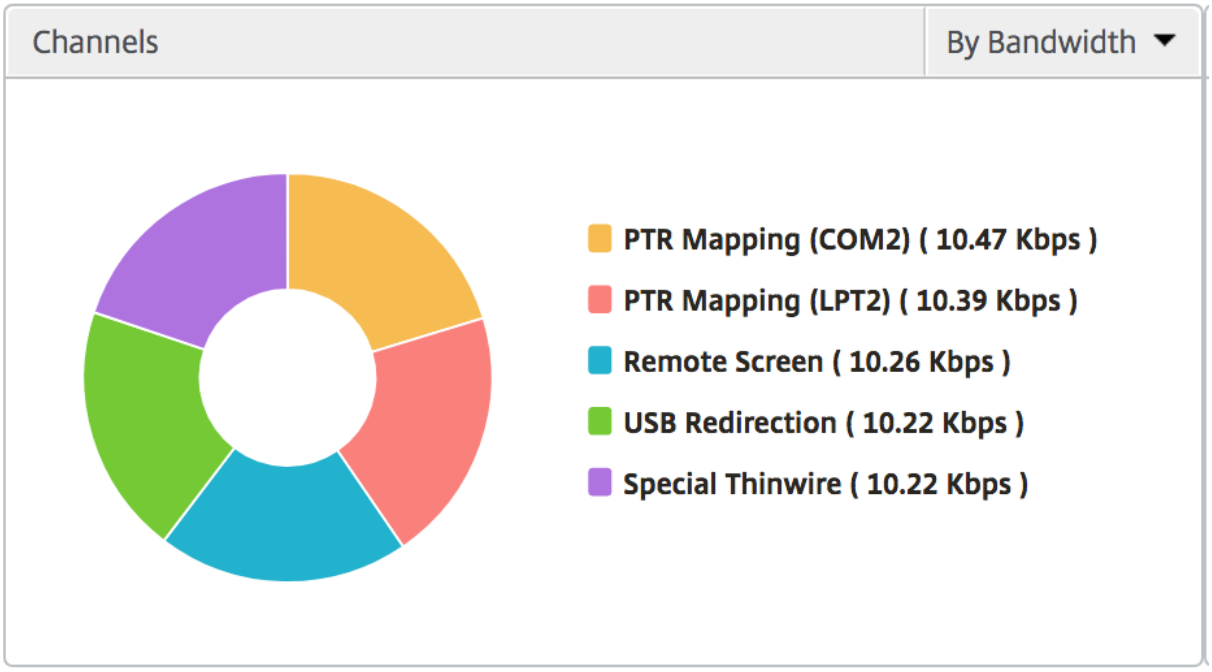
Ein Balkendiagramm, das NetScaler Instanzen darstellt, sortiert nach Active und insgesamt Apps



Kanäle

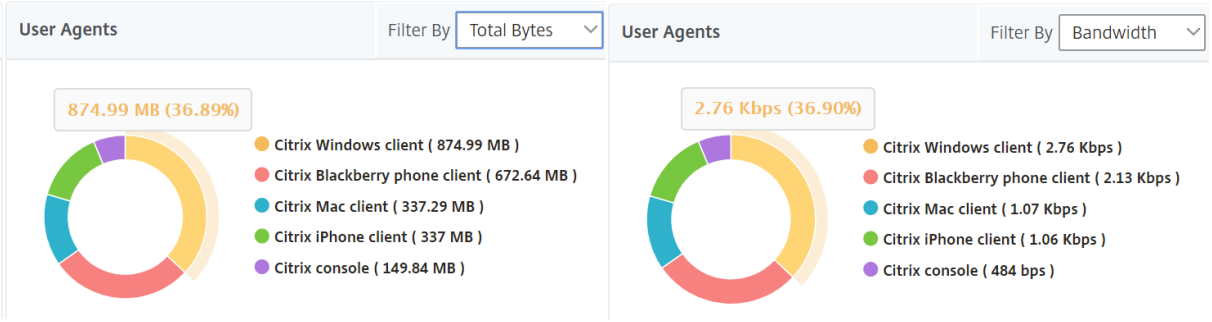
Kanäle stellen die Gesamtbandbreite oder die Gesamtzahl der von jedem virtuellen ICA-Kanal verbrauchten Bytes in Form eines Ringdiagramms dar. Sie können die Metriken auch nach Bandbreite oder Total Bytes sortieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Benutzeragents

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.



Session-Ansicht 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

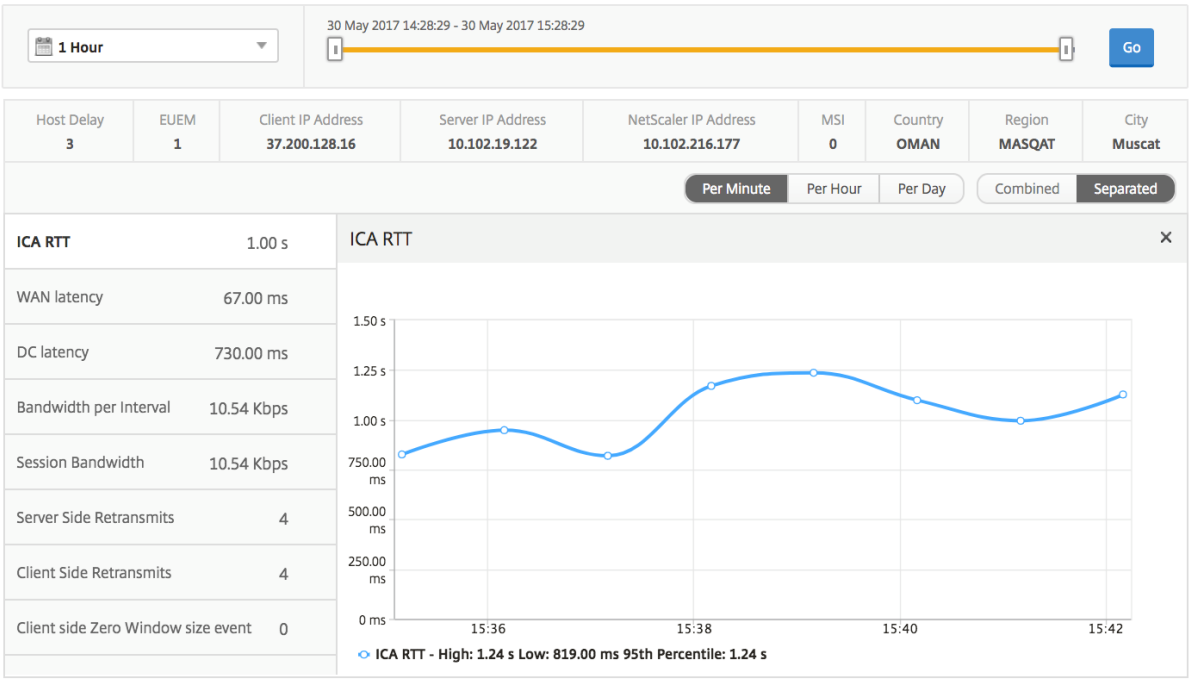
3. Wählen Sie in der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** eine Sitzung aus.

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, die auf Citrix Virtual Apps and Desktops gehostet wird.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und Backend-Server erneut übertragen werden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen werden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern eine hohe Bandbreitennutzung aufgrund von Neuübertragungen anzeigt.
Schnelle RTO auf der Clientseite	Häufigkeit, mit der das Zeitlimit für die erneute Übertragung bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitige schnelle RTO	Anzahl der Zeitüberschreitungen für die erneute Übertragung bei der Verbindung zwischen NetScaler und Backend-Server.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



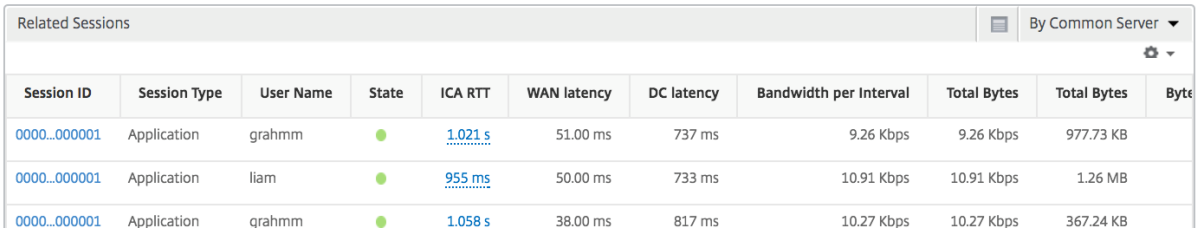
Aktive Anwendung

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verbundene Sitzungen

Im Abschnitt “Sessions”werden die zugehörigen Sitzungen der Sitzungen des ausgewählten Benutzers angezeigt. Die Beziehung kann als gemeinsame Server oder gemeinsames NetScaler ausgewählt werden.



Instanzansichtsberichte und -metriken

February 5, 2024

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf die NetScaler Instance (en).

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** > **Instanzen**.

Instanzzusammenfassungsansicht

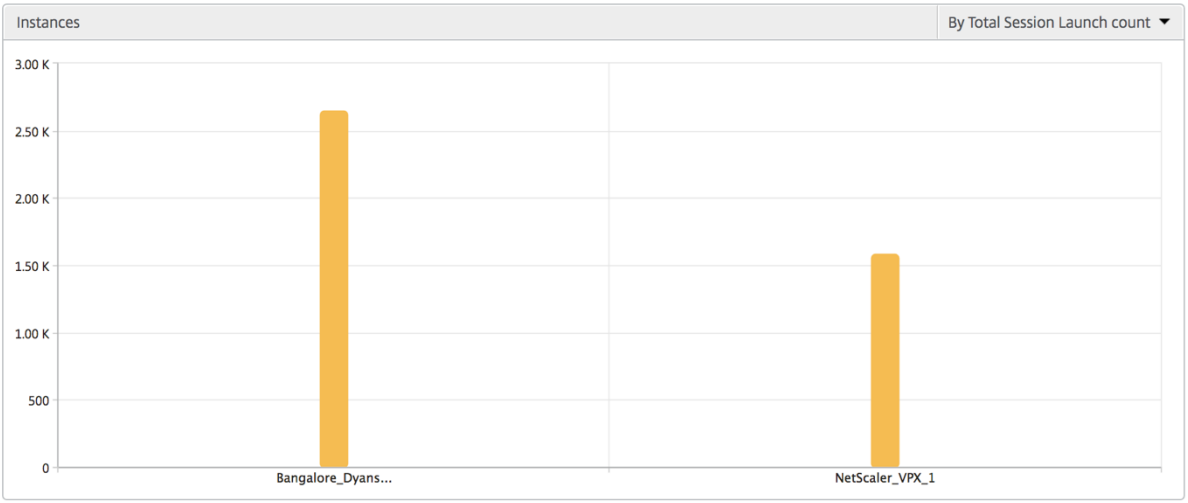
Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler Instanzen anzeigt, die NetScaler ADM hinzugefügt werden.

Alle unten aufgeführten Metriken/Berichte, sofern nicht explizit erwähnt, haben die Werte, die ihnen für den ausgewählten Zeitraum entsprechen.

Instanz-Bargraph

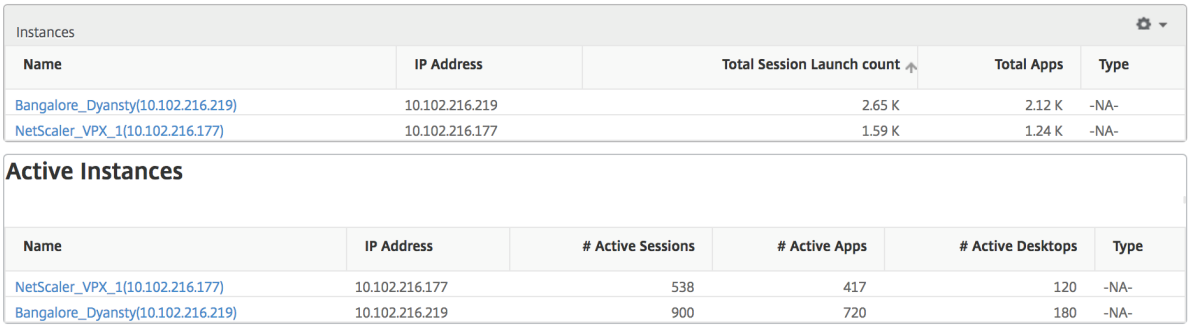
Dieses Diagramm zeigt die Instanz im Vergleich zur Gesamtzahl der Session Startanzahl und Gesamtzahl der Apps an, die im Dropdownmenü oben rechts auf der Graph-Zeichenfläche ausgewählt werden können.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Zusammenfassungsbericht zu Instanzen/aktiven Instanzen

Metriken	Beschreibung
Name	Hostname der NetScaler-Instanz.
IP-Adresse	NetScaler-IP-Adresse.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der eindeutigen Benutzersitzungen, die während eines bestimmten Zeitintervalls erstellt wurden.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.
Typ	–


Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

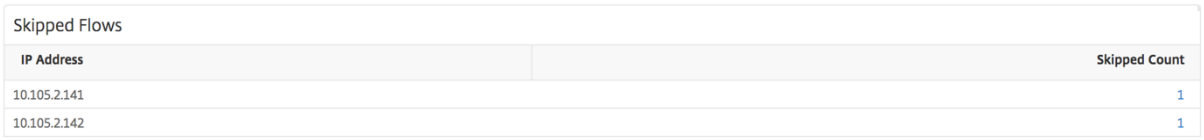
Schwellenwertbericht

Der Schwellenwertbericht stellt die Anzahl der Schwellenwerte dar, die überschritten wurden, wenn die *Entität* in der ausgewählten Periode als Instanz ausgewählt wurde. Weitere Informationen finden Sie unter So erstellen Sie Schwellenwerte und Warnungen .

Übersprungene Flows

Ein übersprungener Flow ist ein Datensatz, der die Parsing ICA-Verbindung übersprungen hat. Dies kann mehrere Gründe haben, z. B. die Verwendung nicht unterstützter Versionen von Citrix Virtual Apps and Desktops, nicht unterstützter Versionen des Receivers oder des Empfängertyps usw. Diese Tabelle zeigt die IP-Adresse und die Anzahl der übersprungenen Flows. Diese Receiver sind möglicherweise nicht Teil der Receiver auf der Positivliste; daher werden diese Sitzungen von der Überwachung übersprungen.

Bitte besuchen Sie**Fehler! Hyperlink-Referenz ungültig.** finden Sie weitere Informationen zu Problemen im Zusammenhang mit der ICA-Analyse.


Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

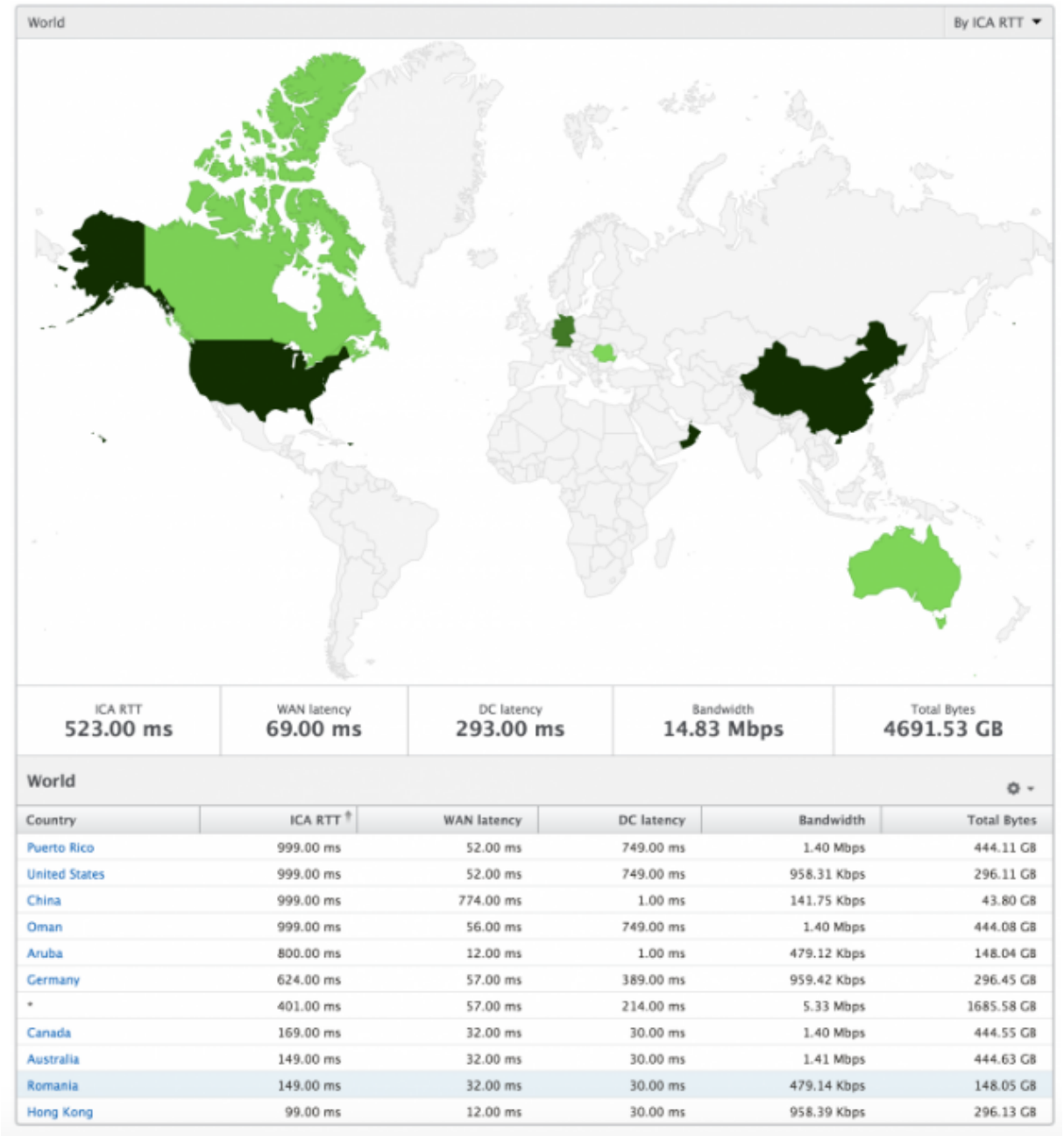
Weltanschauung

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, einen Drilldown zu einem bestimmten Land und weiter in Städte durchführen, indem sie einfach auf die Region klicken. 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 der einzelnen Metriken wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Ansicht pro Instanz

Die Ansicht pro Instanz bietet detaillierte Berichte über die Benutzererfahrung für eine bestimmte ausgewählte NetScaler Instanz.

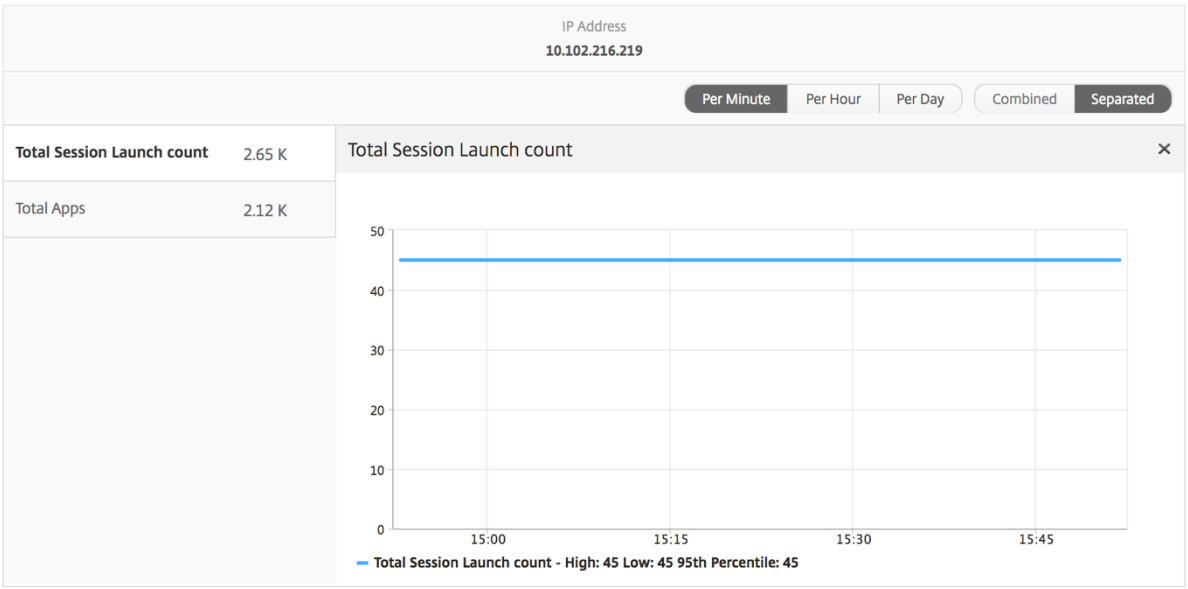
So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Analytics** > **HDX Insight** > **Instanzen**.
2. Wählen Sie im **Bericht Instanzzusammenfassung eine bestimmte Instanz** aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Liniendiagramm

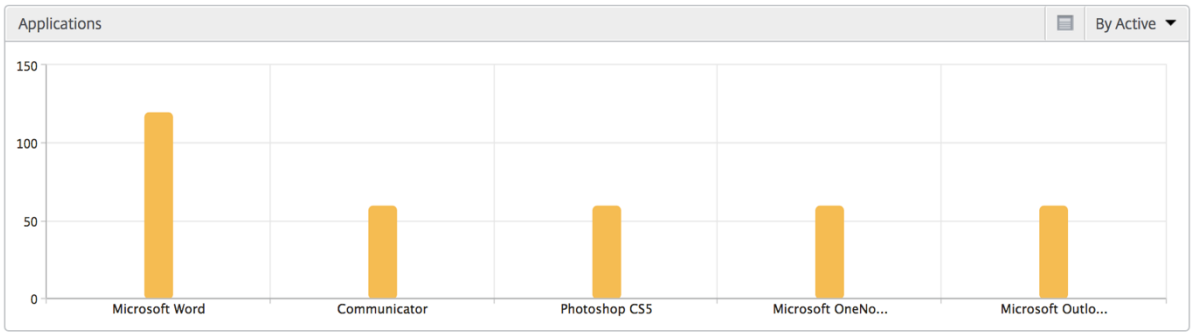
Metriken	Beschreibung
IP-Adresse	Dies stellt die NetScaler-IP-Adresse der ausgewählten Instanz dar.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual Apps-Sitzungen während des angegebenen Zeitintervalls.
Apps insgesamt	Gesamtzahl der eindeutigen Anwendungen, die während eines bestimmten Zeitintervalls gestartet wurden.



Balkendiagramm für Anwendungen

Zeigt die 5 besten Anwendungen basierend auf den folgenden Kriterien an: nach aktiven Apps, Gesamtzahl der Sitzungsstarts, Gesamtzahl der App-Start-Anzahl oder Startdauer.

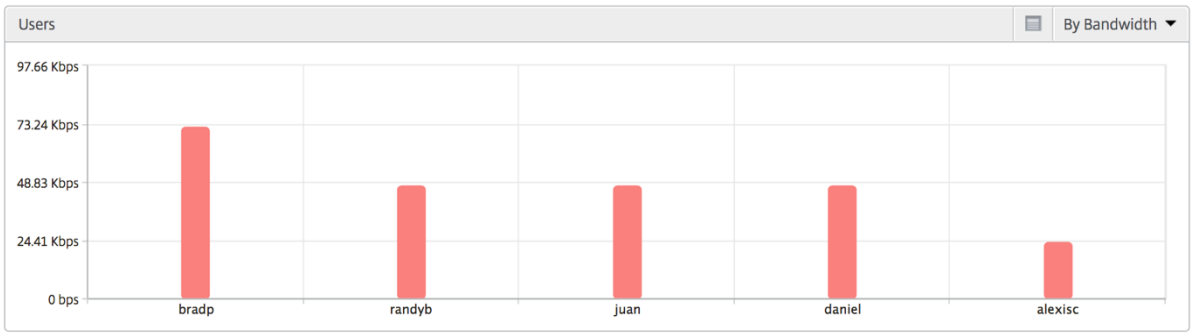
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Balkendiagramm für Benutzer

Das Balkendiagramm “Benutzer”zeigt die fünf wichtigsten Benutzer anhand der folgenden Kriterien an:

- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA RTT



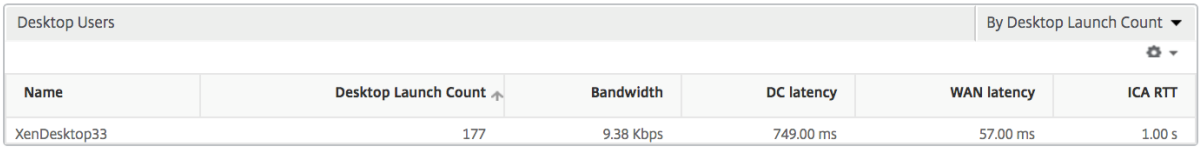
Desktopbenutzer-Bericht

Diese Tabelle gibt einen Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
DC-Latenz	Latenz, die von der Serverseite des Netzwerks verursacht wird. D.h. von NetScaler zu Backend-Servern.
WAN-Latenz	Latenz, die von der Client-Seite des Netzwerks verursacht wird. Das heißt vom NetScaler 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.



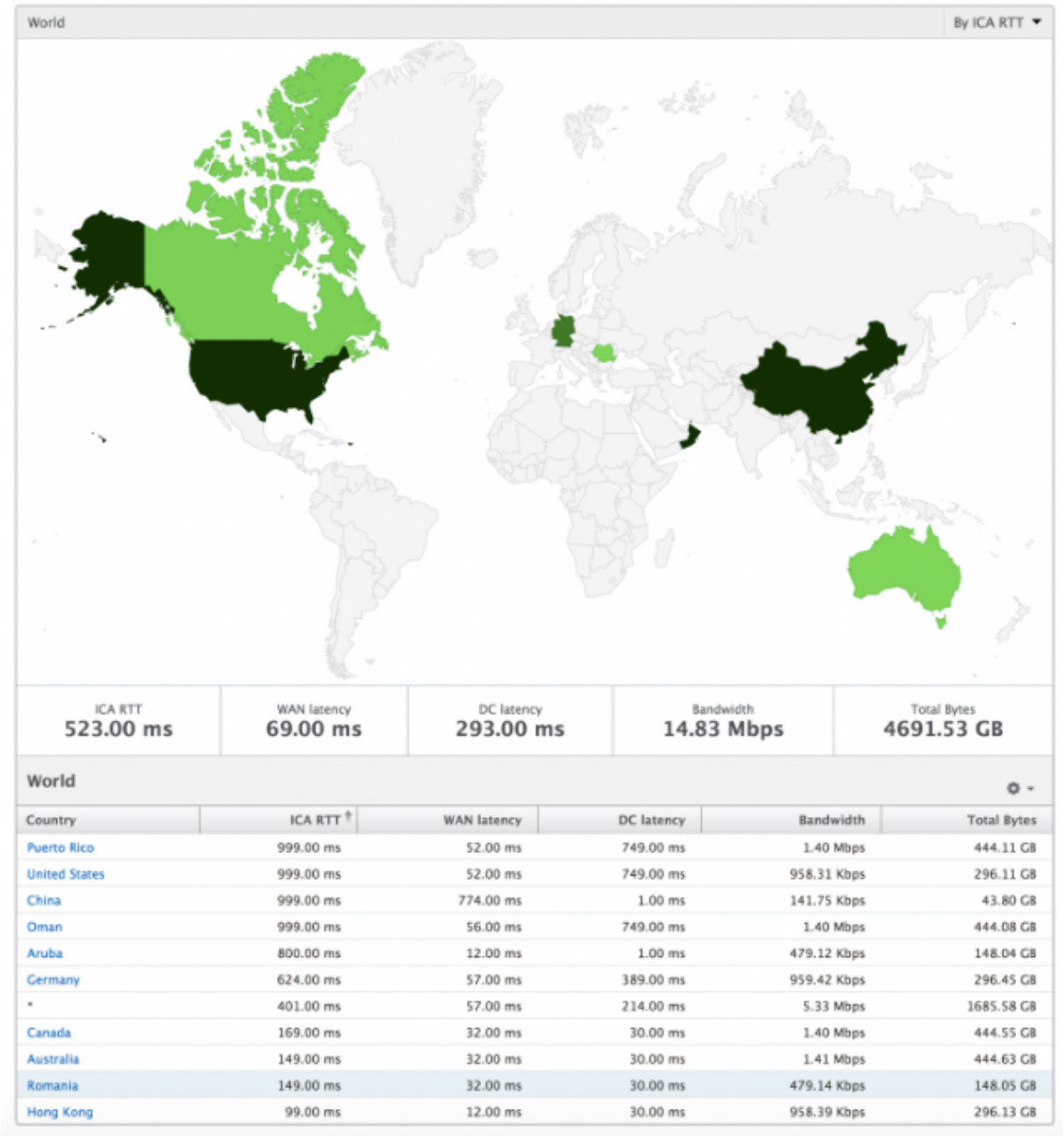
Weltanschauung

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die historischen und aktiven Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, einen Drilldown zu einem bestimmten Land und weiter in Städte durchführen, indem sie einfach auf die Region klicken. 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 der einzelnen Metriken wird in Form einer Heatmap angezeigt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Bytes insgesamt

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Lizenzansichtsberichte und -metriken

February 5, 2024

Die Lizenzansicht enthält Details zu den NetScaler Gateway -Lizenzinformationen.

So navigieren Sie zur Lizenzansicht:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrem NetScaler MA Service 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.

! [lokalisiertes Bild] (/en-us/netscaler-application-delivery-management-software/media hdx-line-chart.png)

Schwellenwertbericht

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 `show running | grep -i <appflow_policy>`Befehl 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.
- Aktivieren Sie den Parameter "appflowlog"in Citrix Gateway oder VPN-Server ist für Access Gateway oder Double-Hop-Bereitstellung aktiviert. 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 AppFlow Richtlinientreffer 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 "`für die Protokollvalidierung 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 App

  Lösung: Aktualisieren Sie die Citrix Workspace App auf eine unterstützte Version. Einzelheiten finden Sie unter Citrix Workspace-App.

- Log: **Fehler von Expand Packet - Überspringen der gesamten hdx-Verarbeitung für diesen Flow**

  Ursache: Problem beim Dekomprimieren von ICA-Verkehr

  Lösung: Für diese ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Log: **Ungültiger Übergang: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT**

  Ursache: Problem beim Analysieren des ICA-Handshakes

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

- Protokoll: **EUEM ICA RTT fehlt**

  Ursache: Kanaldaten der Endbenutzer-Erlebnisüberwachung können nicht analysiert werden

  Lösung: Stellen Sie sicher, dass der Dienst zur Überwachung der Benutzererfahrung auf den Citrix Virtual Apps and Desktops-Servern gestartet wurde. Stellen Sie sicher, dass Sie die unterstützten Versionen der Citrix Workspace App verwenden.

- Protokoll: **Ungültiger Channel-Header**

  Ursache: Channel-Header konnte nicht identifiziert werden

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wurde.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Code überspringen	Fehlermeldung	Ursache des Fehlers
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
124	NS_ICA_ERR_INVALID_PURE_CMD	Ungültiger Befehl bei der Verarbeitung reiner ICA-Kanaldaten
125	NS_ICA_ERR_INVALID_PURE_LEN0	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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Code überspringen	Fehlermeldung	Ursache des Fehlers
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
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 er sich nicht in der White-Liste befindet

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Code überspringen	Fehlermeldung	Ursache des Fehlers
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 Reconnect 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
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Code überspringen	Fehlermeldung	Ursache des Fehlers
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	CDR unterstützt Reducer Version 3 nicht
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Client unterstützt Reducer Version 3 nicht
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unerwartete Anzahl von Byte im ICA-Handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Höhere CGP-Wiederaufnahme-Sequenznummer von Peer-post-Wiederverbindung
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Code überspringen	Fehlermeldung	Ursache des Fehlers
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 von Service Reconnect Ticket im Service-Knoten
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 HDXInsight 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 Zählerdetails aus.

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_tot_ica_conn	Gibt die Gesamtzahl der von NS erkannten reinen ICA-Verbindungen an. Wird immer dann erhöht, wenn eine ICA-Verbindung erkannt wird, die auf der ICA-Signatur auf einer Client-Leiterplatte basiert.	Statistiken
hdx_tot_cgp_conn	Zeigt die Gesamtzahl der von NS erkannten CGP-Verbindungen an (Sitzungszuverlässigkeit EIN). Wird immer dann erhöht, wenn eine CGP-Verbindung basierend auf der CGP-Signatur auf einer Client-PCB erkannt wird.	Statistiken
hdx_dbg_tot_udt_conn	Zeigt die Gesamtzahl der von NS erkannten UDP-ICA-Verbindungen an	Statistiken
hdx_dbg_tot_nsap_conn	Gibt die Gesamtzahl der von NS erkannten NSAP-unterstützten Verbindungen an	Statistiken

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_tot_skip_conn	Gibt an, wie viele ICA-Verbindungen vom Parser aufgrund einer ungültigen ICA- oder CGP-Signatur übersprungen	Statistiken
hdx_dbg_active_conn	Gesamtzahl der aktiven EDT/CGP/ICA-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_active_nsap_conn	Gesamtzahl der aktiven EDT/CGP/ICA-NSAP-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_skip_appflow_disabled	Gesamtzahl der Instanzen, in denen AppFlow aufgrund der Deaktivierung von AppFlow von einer Sitzung getrennt wurde	Stats/Diagnostik
hdx_dbg_transparent_user	Gesamtzahl der transparenten Benutzerzugriffe	Stats/Diagnostik
hdx_dbg_ag_user	Gesamtzahl der Access Gateway-Benutzerzugriffe	Stats/Diagnostik
hdx_dbg_lan_user	Gesamtzahl der Zugriffe auf den LAN-Benutzermodus	Stats/Diagnostik
hdx_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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_dbg_reconnected_session	Gesamtzahl der Wiederverbindungsanforderungen vom Client ohne NetScaler ADC-Fehler	Stats/Diagnostik
hdx_dbg_host_rejected_ns_reconnect	Gesamtzahl der vom Client abgelehnten Wiederverbindungsanforderungen von Hosts	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-Regler deaktiviert.Die Sitzung funktioniert für diese Sitzung nicht.	Fehler
hdx_err_skip_no_msi	Auf dem XA/XD-Server fehlt die MSI-Fähigkeit. Dies weist auf eine ältere Serverversion hin. HDX Insight überspringt diese Verbindung.	Fehler
hdx_err_skip_old_server	Alte, nicht unterstützte Serverversion	Fehler
hdx_err_clnt_not_whitelist	Clientempfänger nicht in der Whitelist, HDX Insight überspringt diese Verbindung	Fehler
hdx_sm_ica_cam_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CAM_CHANNEL	Diagnose

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
hdx_sm_ica_usb_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_USB_CHANNEL	Diagnose
hdx_sm_ica_clip_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CLIP_CHANNEL	Diagnose
hdx_sm_ica_ccm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CCM_CHANNEL	Diagnose
hdx_sm_ica_cdm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CDM_CHANNEL	Diagnose
hdx_sm_ica_com1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM1_CHANNEL	Diagnose
hdx_sm_ica_com2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM2_CHANNEL	Diagnose
hdx_sm_ica_cpm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CPM_CHANNEL	Diagnose
hdx_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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Name des HDX-Zählers	Zweck	Kategorie (Statistiken/Fehler/Diagnose)
dx_dbg_sm_ica_msi_disabled	Gesamtzahl der Fälle, in denen MSI über die SmartAccess-Richtlinie deaktiviert ist	Diagnose
hdx_sm_ica_file_channel_disabled	Die Gesamtzahl von NS_ICA_FILE_CHANNEL ist über die SmartAccess-Richtlinie deaktiviert	Diagnose
hdx_dbg_usb_accept_device	Gesamtzahl der akzeptierten USB-Geräte	Diagnose
hdx_dbg_usb_reject_device	Gesamtzahl der abgelehnten USB-Geräte	Diagnose
hdx_dbg_usb_reset_endpoint	Gesamtzahl der zurückgesetzten USB-Endpunkte	Diagnose
hdx_dbg_usb_reset_device	Gesamtzahl der zurückgesetzten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device	Gesamtzahl der gestoppten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device_response	Gesamtzahl der Antworten von gestoppten USB-Geräten	Diagnose
hdx_dbg_usb_device_gone	Gesamtzahl der ausgelaufenen USB-Geräte	Diagnose
hdx_dbg_usb_device_stopped	Gesamtzahl der gestoppten USB-Geräte	Diagnose

nstrace-Validierung

Suchen Sie nach dem CFLOW-Protokoll, um zu sehen, dass alle AppFlow-Datensätze aus NetScaler 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 Citrix ADM AppFlow Datensätze empfängt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.
- Technisches Support-Paket, das durch Ausführen des `show techsupport`Befehls an der Citrix ADC Eingabeaufforderung erfasst wurde.
- 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 `show arp`Sie den Befehl ausführen.

Bekannte Probleme

Bekannte Probleme in HDX Insight finden Sie in den NetScaler ADC Versionshinweisen.

Gateway Insight

February 5, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 ein Benutzer nicht in der Lage ist, sich bei Citrix Gateway anzumelden, und Sie möchten die Benutzeraktivität und die Gründe für den Anmeldefehler kennen, diese Informationen sind jedoch in der Regel nur verfügbar, wenn der Benutzer eine Anforderung zur Lösung sendet.

Gateway Insight bietet Einblick in die Fehler, die bei der Anmeldung bei Citrix Gateway auftreten, unabhängig vom Zugriffsmodus. Sie können eine Liste aller verfügbaren Benutzer, die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen sowie die 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Eine Stunde Gateway Insight-Berichte können für Citrix ADC-Instanzen mit Unternehmenslizenz angezeigt werden. Eine Platinum-Lizenz ist erforderlich, um Gateway Insight-Berichte über eine Stunde hinaus anzuzeigen.

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

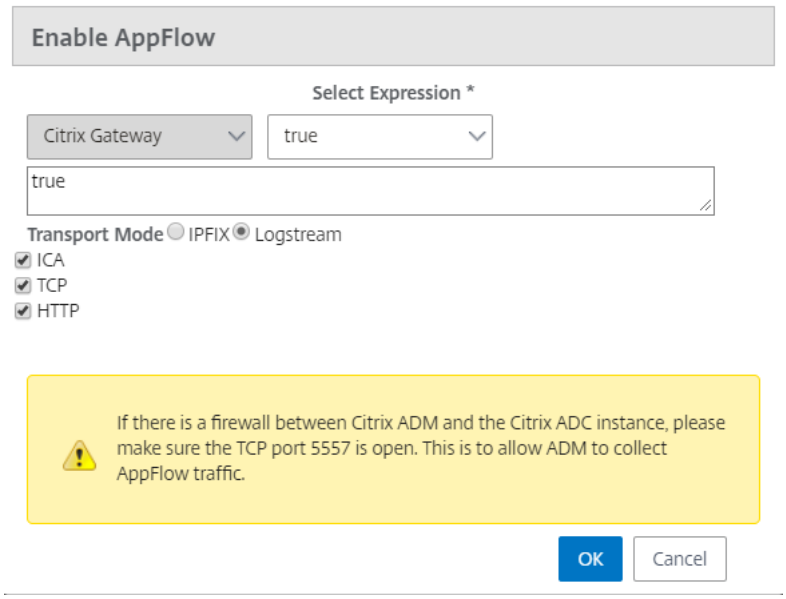
Um Gateway Insight für Ihr Citrix Gateway Gerät zu aktivieren, müssen Sie das Citrix Gateway-Gerät zunächst Citrix ADM hinzufügen. Anschließend müssen Sie AppFlow für den virtuellen Server aktivieren, der die VPN-Anwendung darstellt. Informationen zum Hinzufügen von Geräten zu Citrix ADM finden Sie unter Geräte hinzufügen.

> **Hinweis**
>
> Um EPA-Fehler (Endpoint Analysis) in Citrix ADM anzuzeigen, müssen Sie die AppFlow Authentifizierung, Autorisierung und Überwachung von Benutzernamen auf dem Citrix Gateway Gerät aktivieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

So aktivieren Sie AppFlow für einen virtuellen Server in Citrix ADM

1. Melden Sie sich bei Citrix ADM an.
2. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die Instanz aus, für die Sie AppFlow aktivieren möchten.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
4. Wählen **Sie auf der Seite Configure Insight** unter **Configure Analytics** die Option **Citrix Gateway** aus.
5. Wählen Sie den virtuellen Server aus, für den Sie AppFlow aktivieren möchten, und klicken Sie auf **AppFlow aktivieren**.
6. Klicken Sie auf dem Bildschirm **AppFlow aktivieren** in der Liste **Ausdruck auswählen** auf true.
7. Aktivieren Sie neben **Transportmodus** das Kontrollkästchen **Logstream**.



> **Hinweis**
>
> Sie können entweder IPFIX oder `Logstream` als Transportmodus wählen.

8. Klicken Sie auf **OK**.

So aktivieren Sie die AppFlow-Authentifizierung, Autorisierung und Überwachung der Benutzernamenprotokollierung auf einem Citrix Gateway-Gerät mithilfe der GUI

1. Navigieren Sie zu **Konfiguration > System > AppFlow > Einstellungen**, und klicken Sie dann auf **AppFlow Einstellungen ändern**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

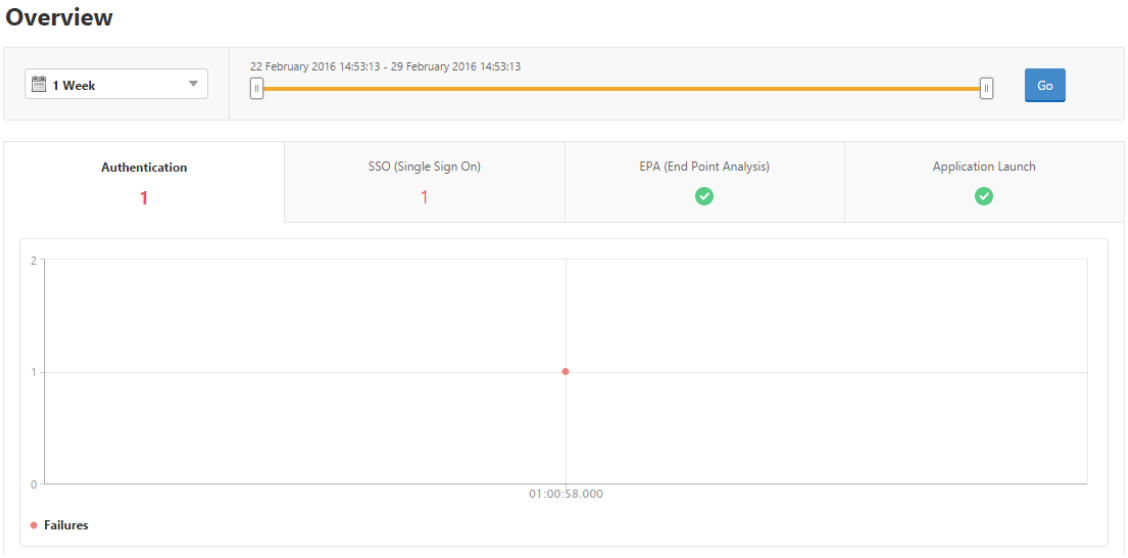
2. Wählen **Sie im Bildschirm AppFlow-Einstellungen konfigurieren** die Option **AAA-Benutzername**aus, und klicken Sie dann auf **OK**.

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.

So zeigen Sie EPA-, SSO-, Authentifizierungs-, Autorisierungs- und Anwendungsstartfehler an

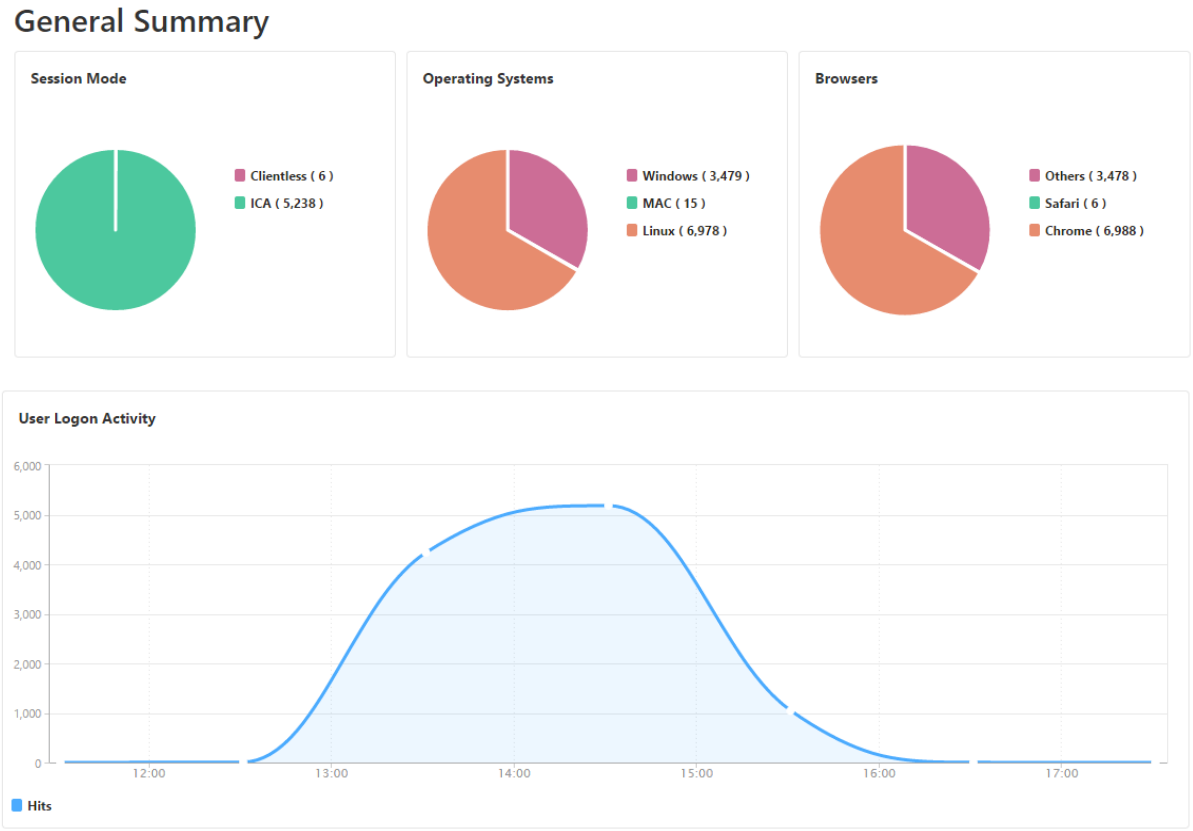
1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarten EPA (Endpunktanalyse), Authentifizierung, Autorisierung, SSO (Single Sign On) oder Anwendungsstart, um die Fehlerdetails anzuzeigen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

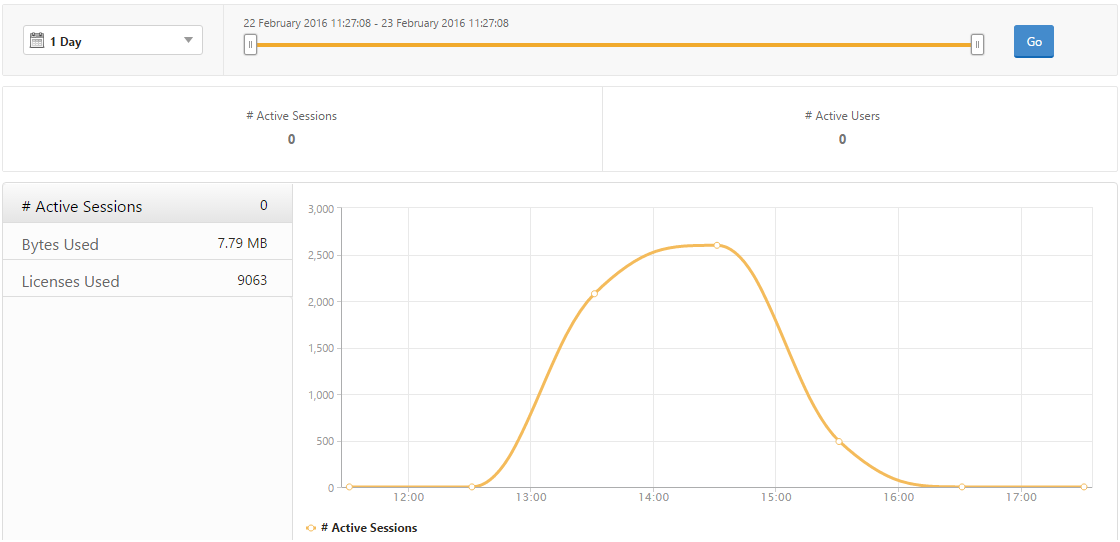
Sie können Berichte für alle Benutzer anzeigen, die den Citrix Gateway-Appliances zugeordnet sind. Sie können die EPA-, Authentifizierungs-, SSO- und Anwendungsstartfehler für einen Benutzer anzeigen. Sie können auch die Details zu aktiven und beendeten Sitzungen für einen Benutzer anzeigen.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Sie können nun 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

Auf der Registerkarte **Benutzer** oder **Aktive Benutzer** können Sie in der Spalte **Benutzername** auf einen Benutzer klicken, um die Fehler beim Starten von EPA, Authentifizierung, SSO und Anwendung sowie andere Details für diesen Benutzer anzuzeigen.

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.

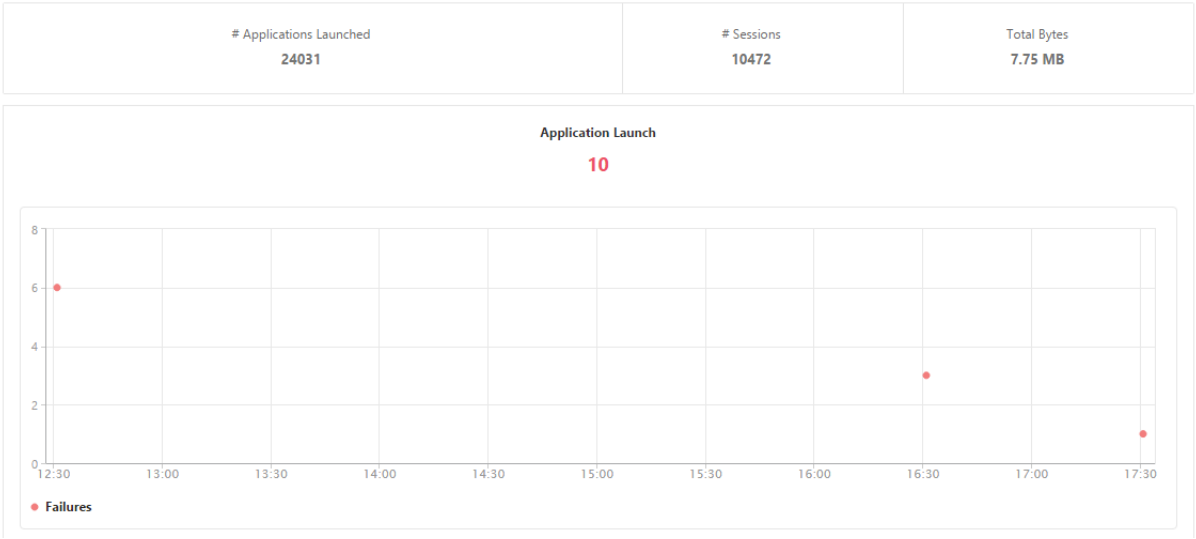
So zeigen Sie Anwendungsdetails an

1. Navigieren Sie in NetScaler ADM zu **Analytics > Gateway Insight > Anwendungen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Gesamtzahl der Byte und die Bandbreite anzeigen, die von allen Gateways verwendet werden, die einem Citrix Gateway-Gerät zugeordnet sind, zu einem bestimmten Zeitpunkt. Sie können EPA, Authentifizierung, Single Sign-On

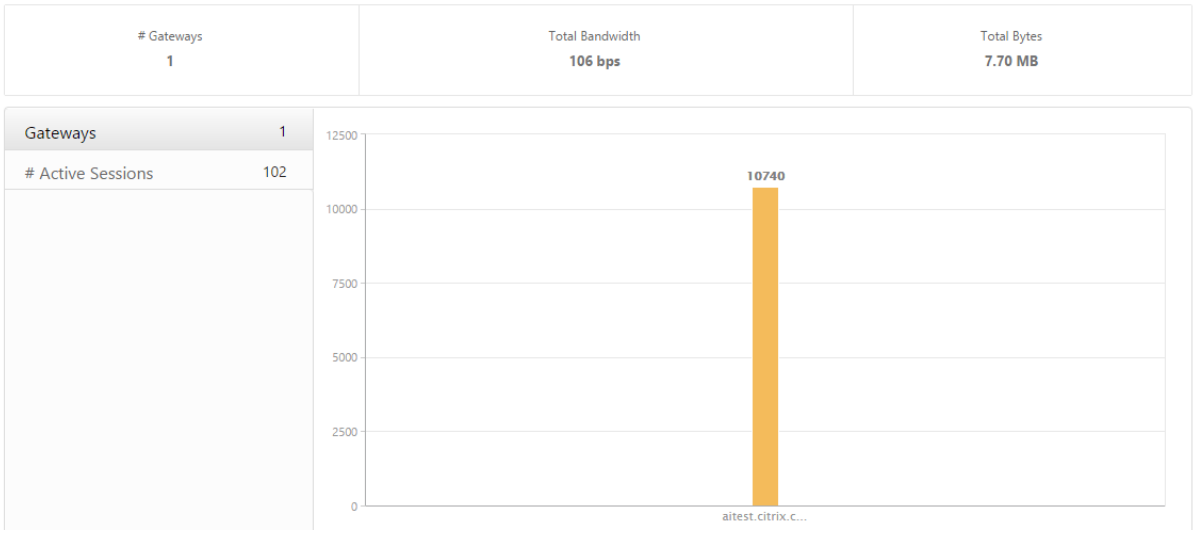
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivitäten anzeigen.

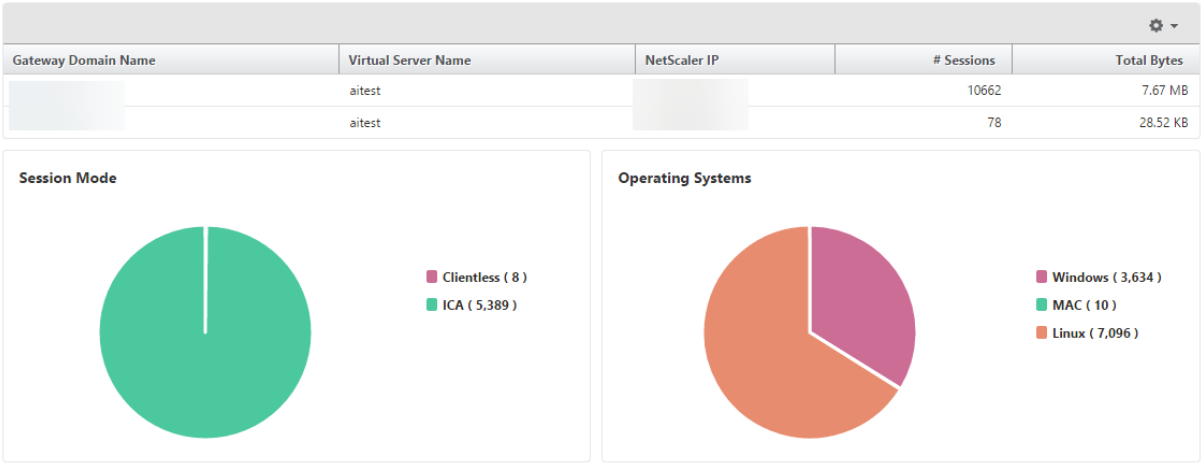
So zeigen Sie Gateway Details an

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

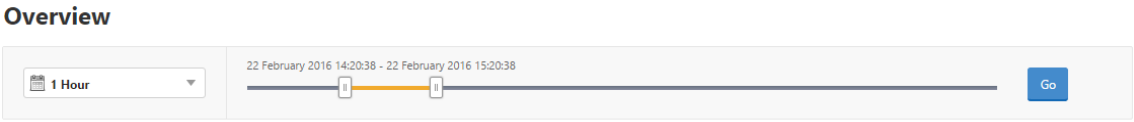
Authentifizierungsfehler

Sie können Authentifizierungsfehler wie falsche Anmeldeinformationen oder keine Antwort vom Authentifizierungsserver anzeigen. Wenn Sie die zweistufige Authentifizierung eingerichtet haben, können Sie sehen, ob die primäre, sekundäre oder beide Phasen der Authentifizierung fehlgeschlagen sind.

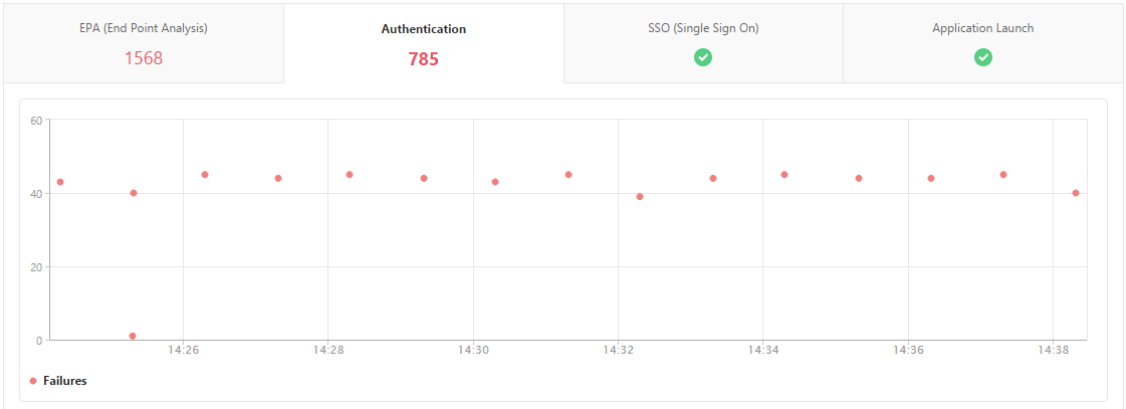
So zeigen Sie die Details zum Authentifizierungsfehler an:

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Klicken Sie auf die Registerkarte **Authentifizierung**. Sie können die Anzahl der Authentifizierungsfehler zu einem bestimmten Zeitpunkt im Diagramm "**Fehler** "anzeigen.



Führen Sie einen Bildlauf nach unten durch, um Details zu jedem Authentifizierungsfehler wie **Benutzername, Client-IP-Adresse, Fehlerzeit, Authentifizierungstyp, IP-Adresse des Authentifizierungsservers**und mehr aus der Tabelle auf derselben Registerkarte anzuzeigen. In der Spalte **Fehlerbeschreibung** in der Tabelle wird der Grund für den Anmeldefehler angezeigt, und in der Spalte **Status** wird angezeigt, in welchem Stadium einer zweistufigen Authentifizierung der Fehler aufgetreten ist.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Authentifizierungsfehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie den Abwärtspfeil verwenden, wie im folgenden Screenshot angegeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

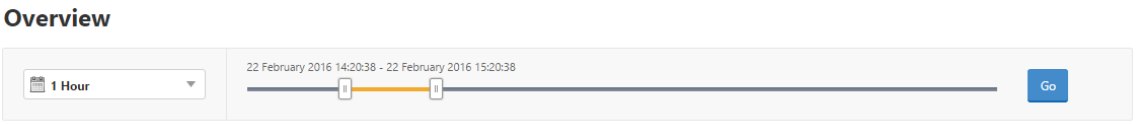
EPA-Fehler

Sie können EPA-Fehler in der Vor- oder Nachauthentifizierung 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.

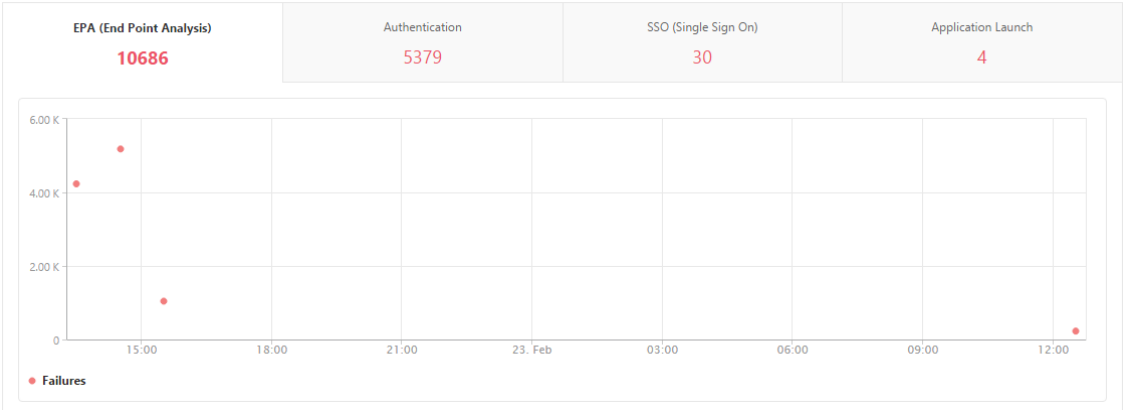
So zeigen Sie EPA-Fehlerdetails an:

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

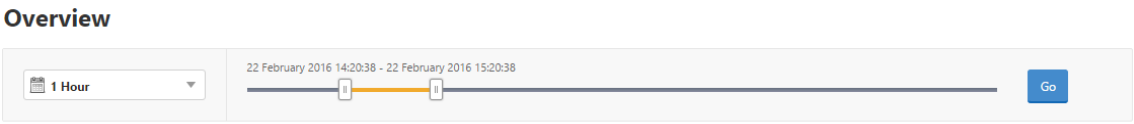
SSO-Fehler

Sie können zu jedem Zeitpunkt alle SSO-Fehler eines Benutzers anzeigen, der über das Citrix Gateway-Gerät auf Anwendungen zugreift.

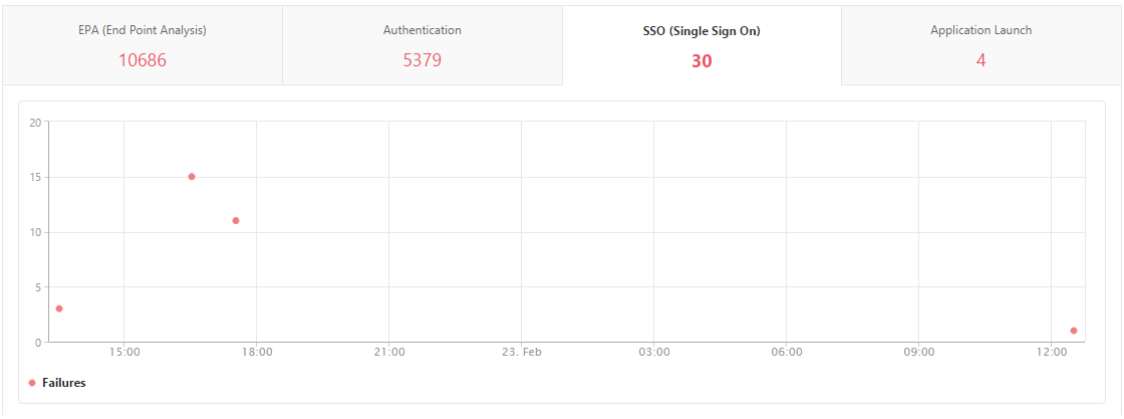
So zeigen Sie die Details zum SSO-Fehler an:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

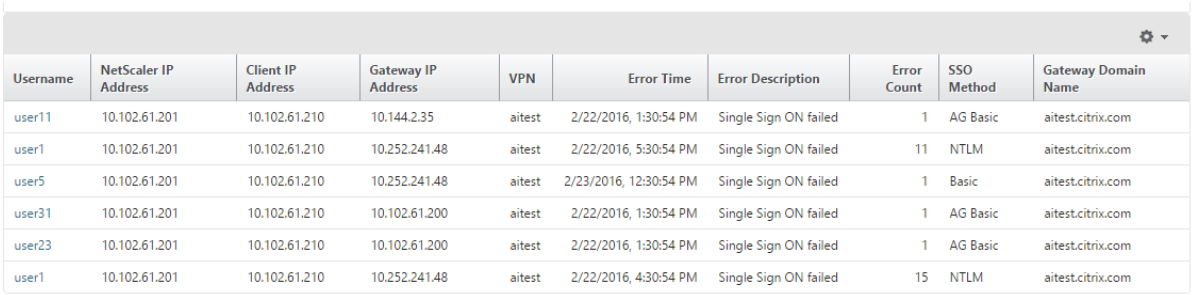
1. Navigieren Sie in Citrix ADM zu **Analytics > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.



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.

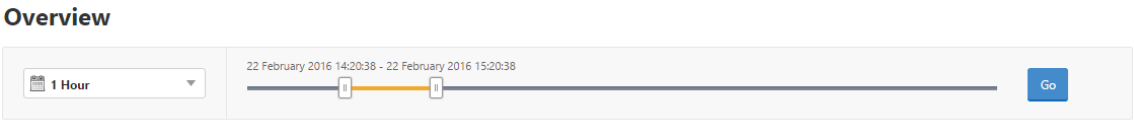
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Nach erfolgreicher Anmeldung bei Citrix Gateway kann ein Benutzer keine virtuelle Anwendung starten

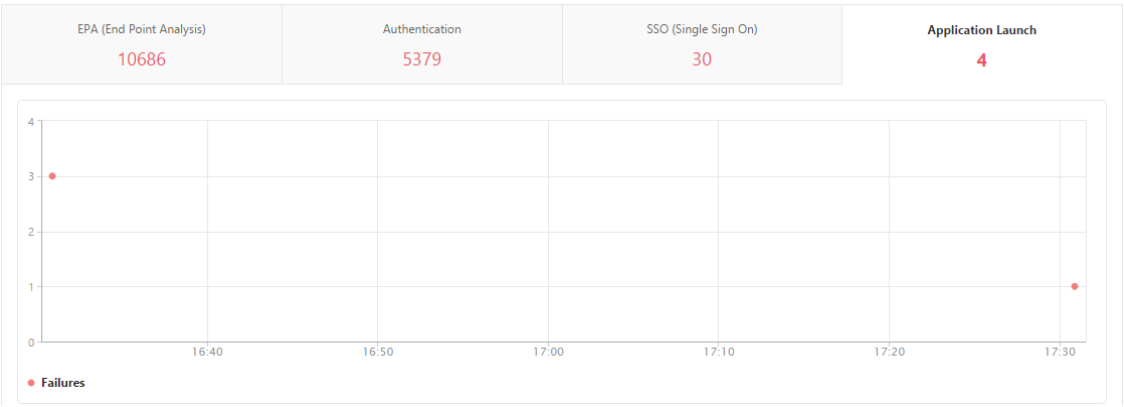
Bei einem fehlgeschlagenen Anwendungsstart können Sie einen Einblick in die Gründe erhalten, z. B. unzugängliche Secure Ticket Authority (STA) oder Citrix Virtual Apps-Server oder ein ungültiges STA-Ticket. Sie können den Zeitpunkt des Auftretens des Fehlers, Details des Fehlers und die Ressource anzeigen, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

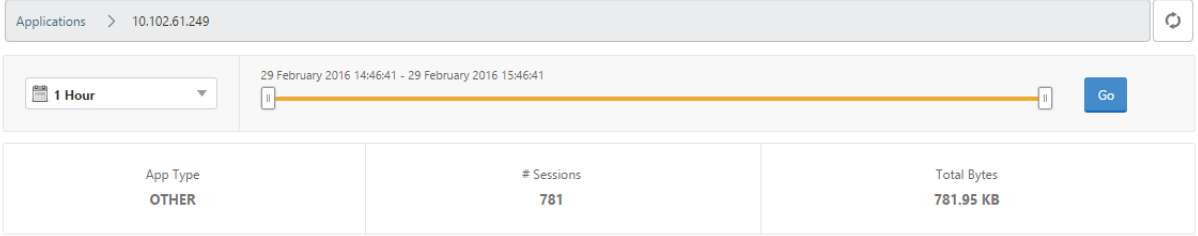
So zeigen Sie die Gesamtanzahl von Bytes und Bandbreite an, die von einer Anwendung verbraucht wird:

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.

ICA Applications | Other Applications

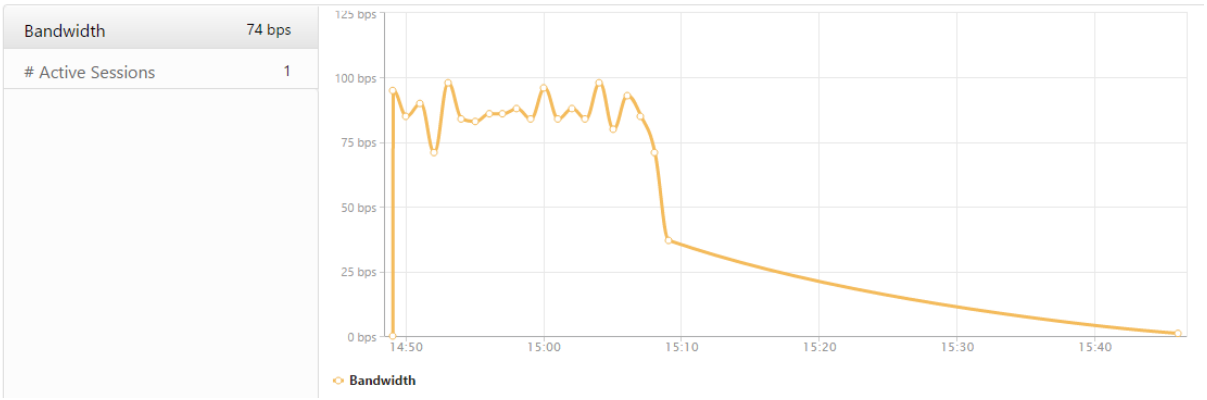
Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

Sie können die Anzahl der Sitzungen und die Gesamtanzahl der Bytes anzeigen, die von dieser Anwendung belegt werden.



Sie können auch die von dieser Anwendung verbrauchte Bandbreite anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

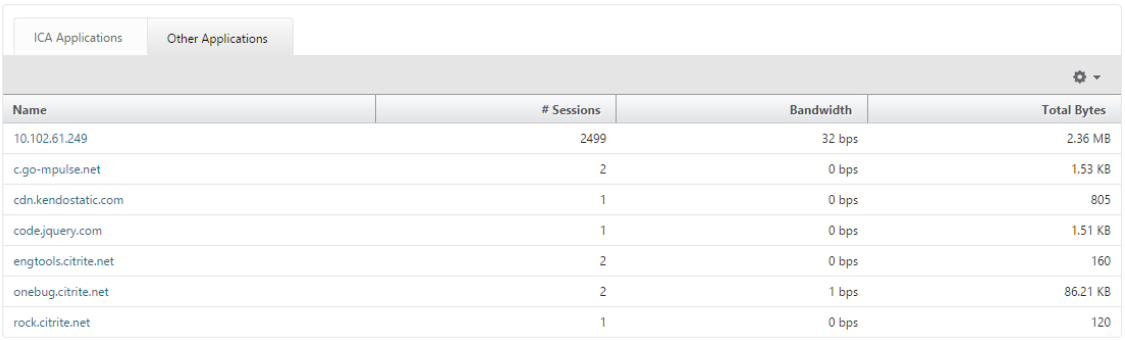


Ein Benutzer hat sich erfolgreich bei Citrix Gateway angemeldet, kann jedoch nicht auf bestimmte Netzwerkressourcen im internen Netzwerk zugreifen

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

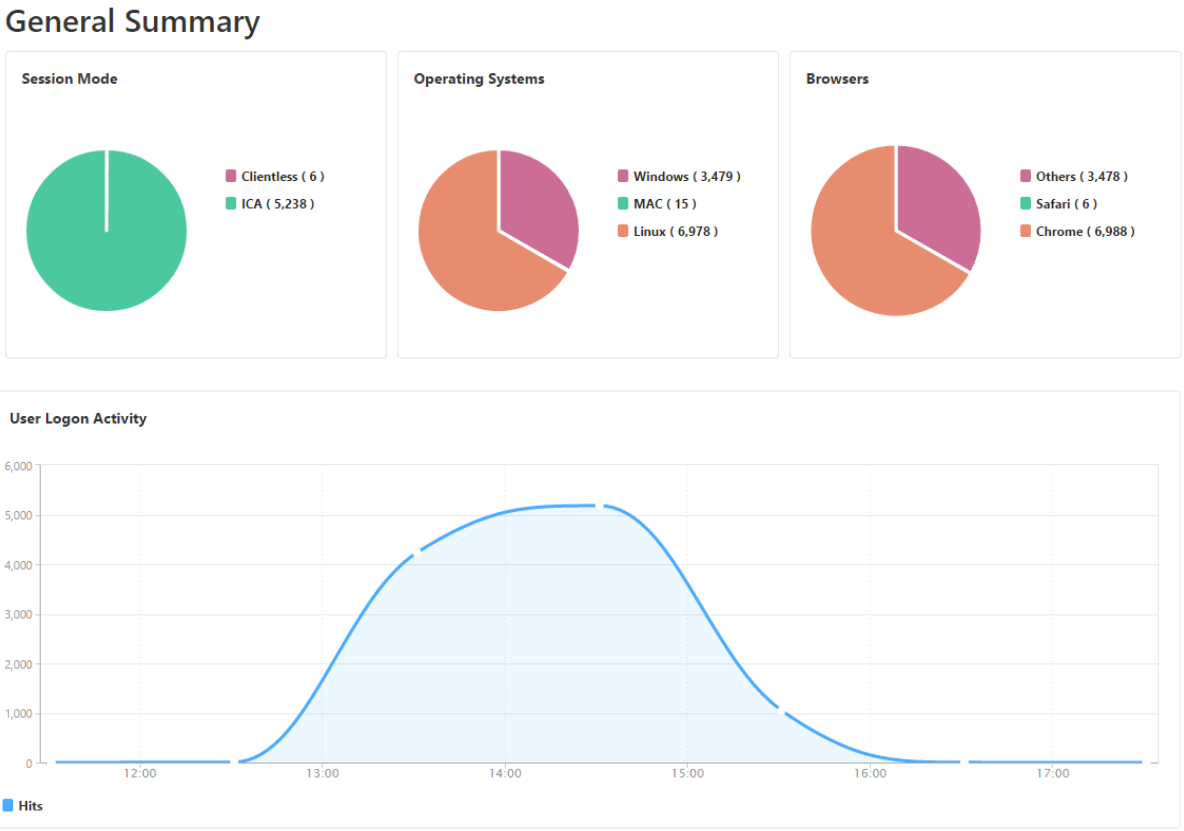
Mit Gateway Insight können Sie eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern für die Anmeldung verwendet werden, die Clienttypen und die Anzahl der stündlich

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 eine 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 NetScaler ADC aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die Gateway Insight-Konfiguration in der NetScaler ADC Konfiguration.

  Führen Sie den `show running | grep -i <appflow_policy>`Befehl aus, um die Gateway Insight-Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp REQUEST ist. Zum Beispiel;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- Stellen Sie bei der Bereitstellung von Single-Hop-, Access Gateway- oder Unified Gateway-Bereitstellung sicher, dass die Gateway Insight AppFlow Richtlinie an den virtuellen VPN-Server gebunden ist, auf dem der VPN-Datenverkehr fließt. Einzelheiten finden Sie unter HDX Insight-Datenerfassung aktivieren.
- Aktivieren Sie den Parameter “appflowlog”im virtuellen Citrix 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 AppFlow Richtlinientreffer 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Datensatzgenerierung in NetScaler ADC Checkliste

- Führen Sie den `nsconmsg -d stats -g ai_tot`Befehl aus, und prüfen Sie, ob die Statistikschritte in Citrix ADC vorhanden sind.
- Erfassen Sie nstrace-Protokolle und suchen Sie nach CFLOW-Paketen, um zu bestätigen, dass Citrix ADC AppFlow Datensätze exportiert.

Validierungen in NetScaler ADM

- Führen Sie den `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"`Befehl aus, um die Protokolle zu überprüfen, um zu bestätigen, dass Citrix ADM AppFlow Datensätze empfängt.
- Stellen Sie sicher, dass die NetScaler ADC-Instanz zu NetScaler ADM hinzugefügt wird.
- Stellen Sie sicher, dass der virtuelle NetScaler Gateway/VPN-Server in NetScaler ADM lizenziert ist.

Gateway Insight-Statistiken

Die folgenden Gateway Insight-Statistiken sind verfügbar.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled

Wenden Sie sich an den technischen Support von Citrix

Stellen Sie für eine schnelle Lösung sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie sich an den technischen Support von Citrix wenden:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Einzelheiten zur Bereitstellung und Netzwerktopologie.
- NetScaler ADC- und NetScaler ADM-Versionen.
- Technisches Support-Paket für NetScaler ADC und NetScaler ADM.
- nstrace Capture während des Problems.

Bekannte Probleme

Informationen zu bekannten Problemen in Gateway Insight finden Sie in den NetScaler ADC Versionshinweisen

Security Insight

February 5, 2024

Web- und Webdienstanwendungen, die dem Internet ausgesetzt sind, sind zunehmend anfällig für Angriffe geworden. Um Anwendungen vor Angriffen zu schützen, benötigen Sie einen Überblick über Bedrohungen, verwertbare Echtzeitdaten zu Angriffen und Empfehlungen für 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Überprüfungen der Anwendungsfirewall durchgeführt wurden, aber die Sicherheitsmaßnahmen des Citrix ADC -Systems, z. B. ein sicheres Kennwort für den nsroot-Benutzer, nicht übernommen wurden, wird den Anwendungen ein niedriger Sicherheitsindex zugewiesen.

- **Umsetzbare Informationen.** Informationen, die Sie benötigen, um den Bedrohungsindex zu senken und den Sicherheitsindex zu erhöhen, wodurch die Anwendungssicherheit erheblich verbessert wird. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 [**-SecurityInsightRecordInterval**] [**-SecurityInsightTraffic** (ENABLED DISABLED)]

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>

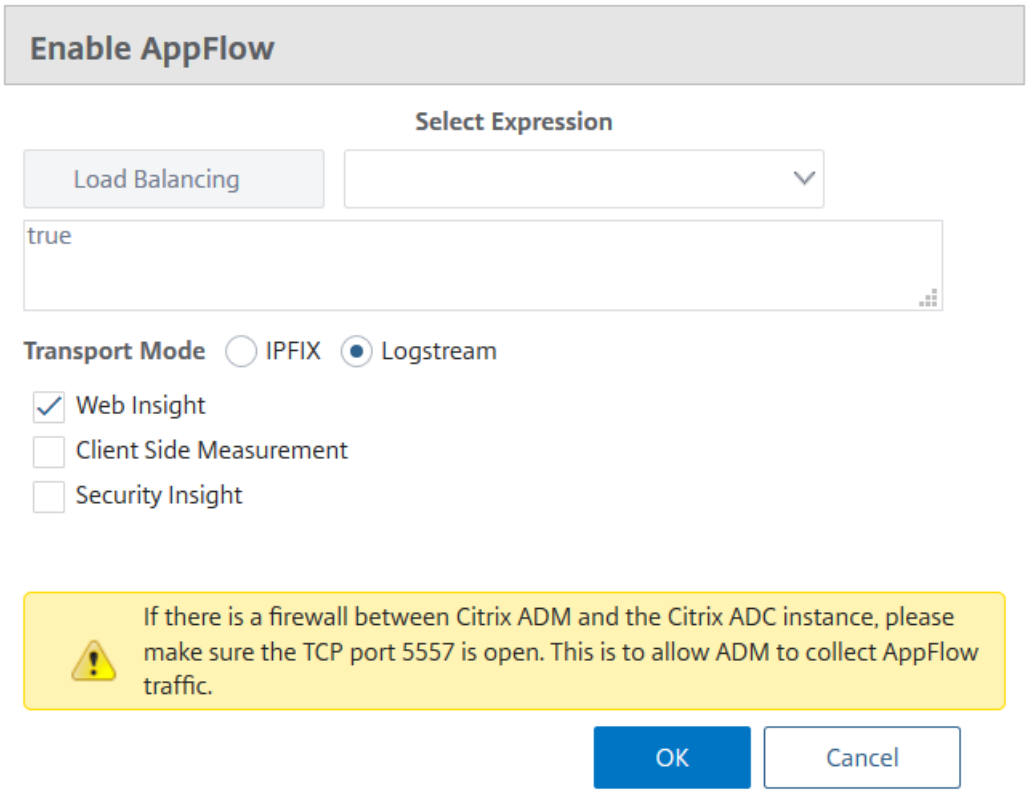
```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
   SecurityInsightTraffic ENABLED
add appflow action act1 -collectors col
add appflow action af_action_Sap_10.102.63.85 -collectors col
add appflow policy pol1 true act1
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
6  add appflow policy af_policy_Sap_10.102.63.85 true
      af_action_Sap_10.102.63.85
7  bind appflow global pol1 1 END -type REQ_DEFAULT
8  or,
9  bind lb vserver Sap  – policyName af_action_Sap_10.102.63.85  –
      priority  “ 20 ”
10 <!--NeedCopy-->
```

So aktivieren Sie AppFlow von Citrix ADM aus:

1. Geben Sie in einem Webbrowser die IP-Adresse des **Citrix 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 AppFlow aktiviert werden soll.
4. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
5. Wählen Sie die virtuellen Server aus, und klicken Sie auf **AppFlow aktivieren**.
6. Geben Sie im Feld **AppFlow aktivieren** den **Wert true**ein, und wählen Sie **Security Insight**aus.
7. Klicken Sie auf **OK**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 einen Namen für Stadt, Bundesland und Land sowie 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

IP-Reputation überwachen

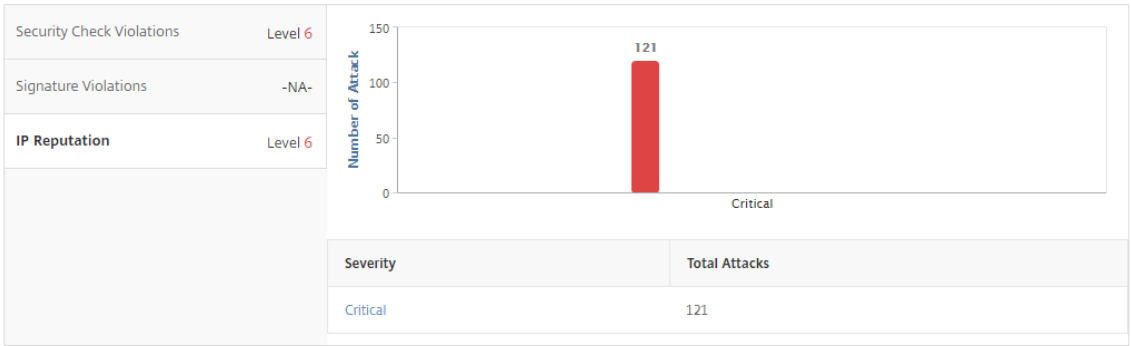
Die IP-Reputation-Funktion bietet angriffsbezogene Informationen über bösartige IP-Adressen. Beispielsweise werden IP-Reputationsbewertung, IP-Reputationskategorie, IP-Reputation-Angriffszeit, Geräte-IP und Details zur Client-IP-Adresse gemeldet.

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
81–100	Vertrauensvoll

So überwachen Sie die IP-Reputation:

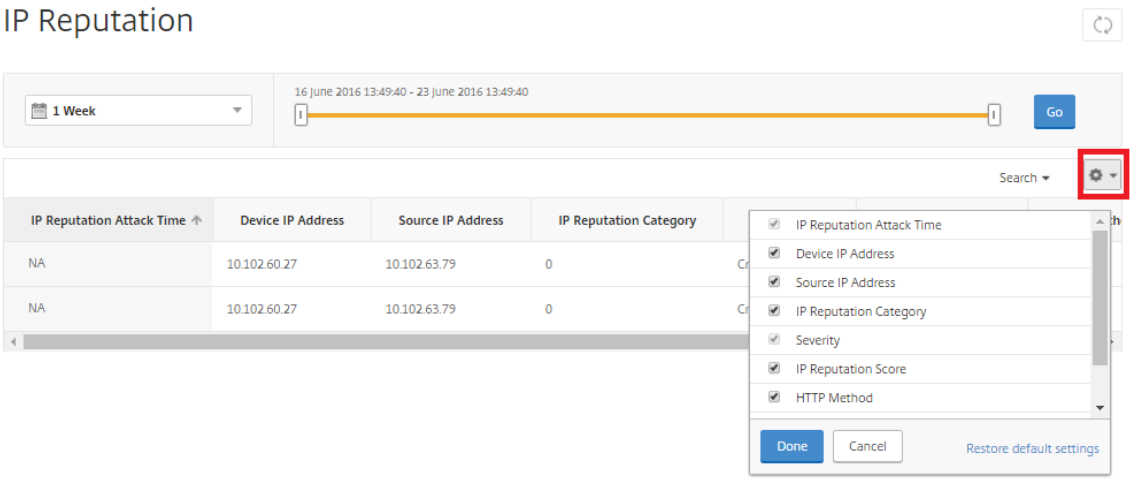
1. Navigieren Sie zu **Analytics**> **Security Insight**, und wählen Sie die Anwendung aus, die Sie überwachen möchten.
2. Wählen Sie auf der Registerkarte **Bedrohungsindex** die Option **IP-Reputation** aus.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

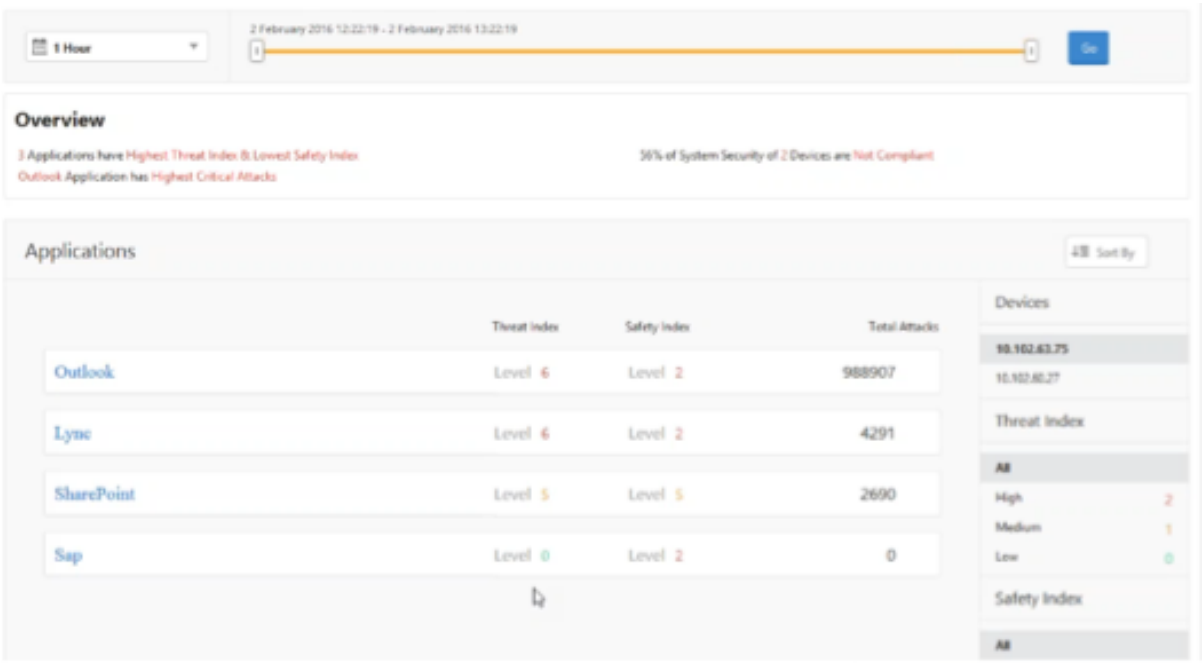
In diesem Anwendungsfall verfügen Sie über eine Reihe von Anwendungen, die Angriffen ausgesetzt sind, und Sie haben NetScaler ADM für die Überwachung der Bedrohungsumgebung konfiguriert. Sie müssen den Bedrohungsindex, den Sicherheitsindex sowie die Art und Schwere der Angriffe, denen die Anwendungen ausgesetzt sein könnten, regelmäßig überprüfen. Diese Überprüfung ermöglicht es Ihnen, sich zunächst auf die Anwendungen zu konzentrieren, die die meiste 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.

Beispielsweise können Sie Microsoft Outlook, Microsoft Lync, SharePoint und eine SAP-Anwendung überwachen und eine Zusammenfassung der Bedrohungsumgebung für diese Anwendungen überprüfen.

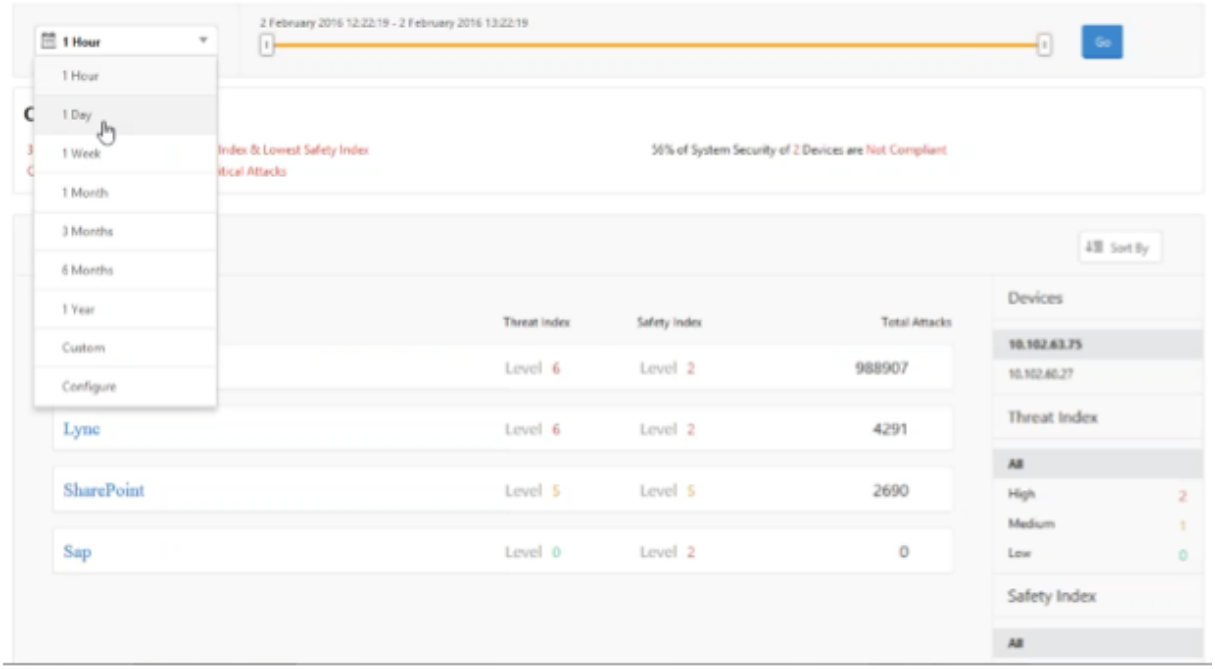
Um eine Zusammenfassung der Bedrohungsumgebung zu erhalten, melden Sie sich bei **NetScaler ADM**an und navigieren Sie dann zu **Analytics > Security Insight**.

Für jede Anwendung werden Schlüsselinformationen angezeigt. Der Standardzeitraum ist 1 Stunde.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

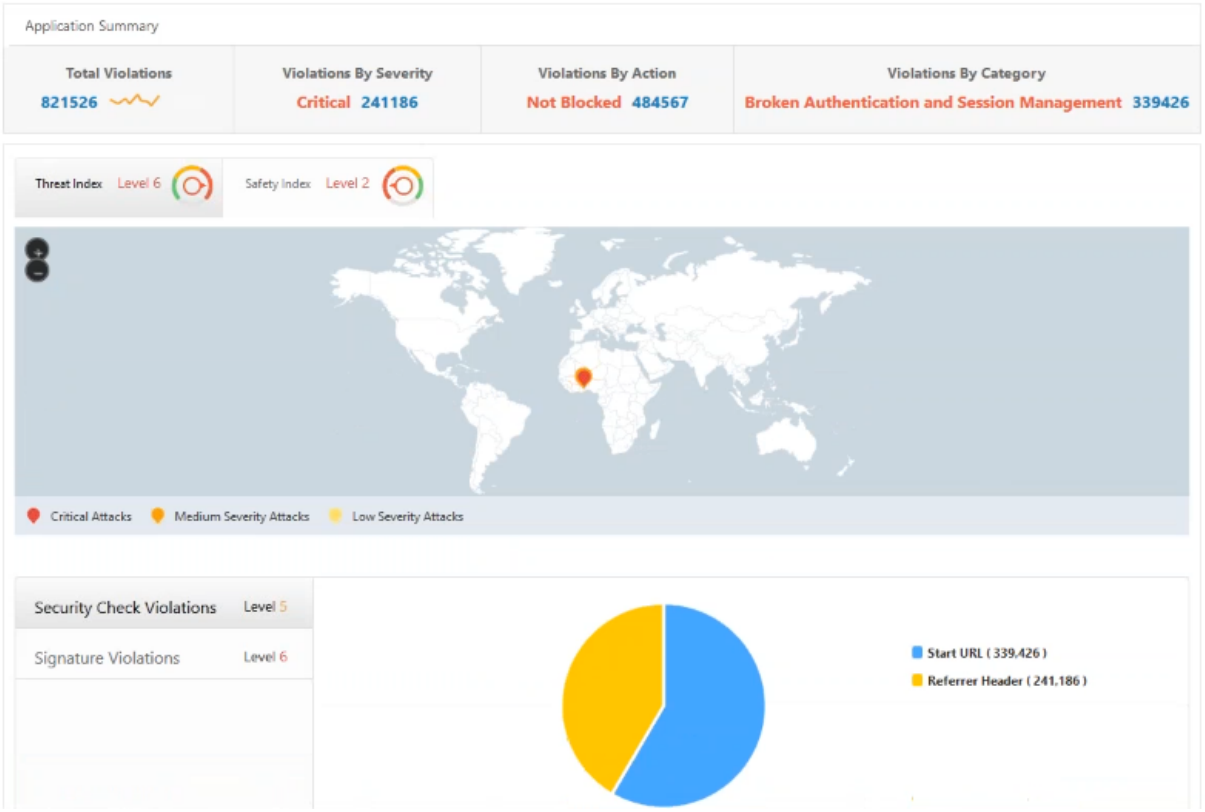
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

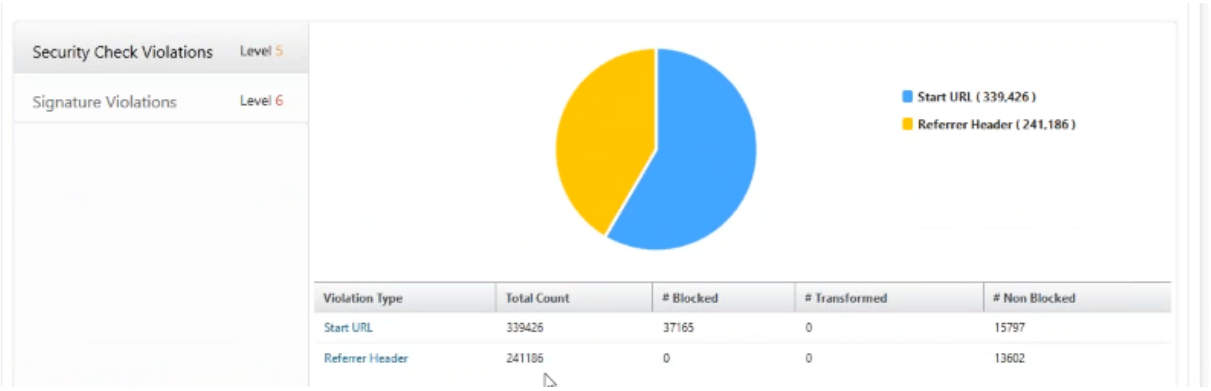
In diesem Beispiel hat Microsoft Outlook den Bedrohungsindexwert 6, und Sie möchten wissen, welche Faktoren zu diesem hohen Bedrohungsindex beitragen.

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.

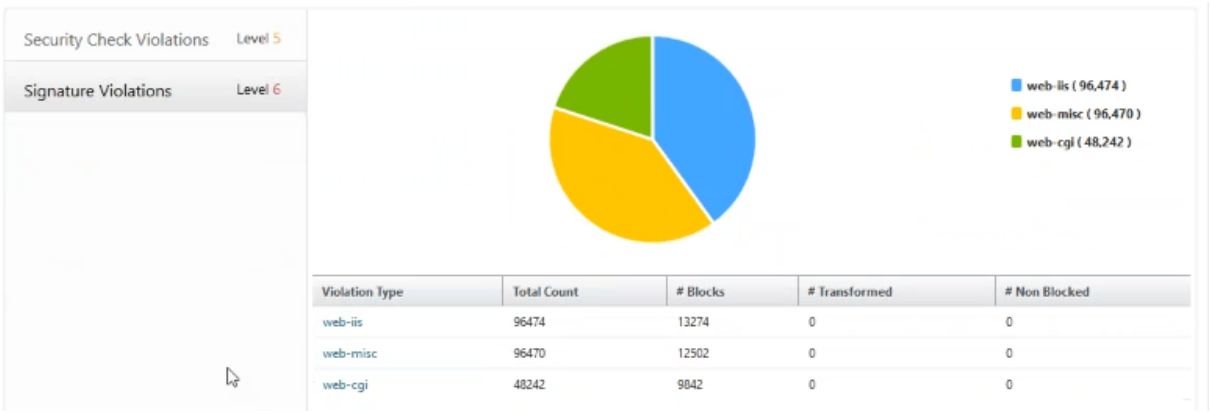


Klicken Sie auf **Bedrohungsindex > Sicherheitsüberprüfungsverstöße**, und überprüfen Sie die angezeigten Informationen zur Verletzung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Klicken Sie auf **Signaturverletzungen**, und überprüfen Sie die angezeigten Verstoßinformationen.



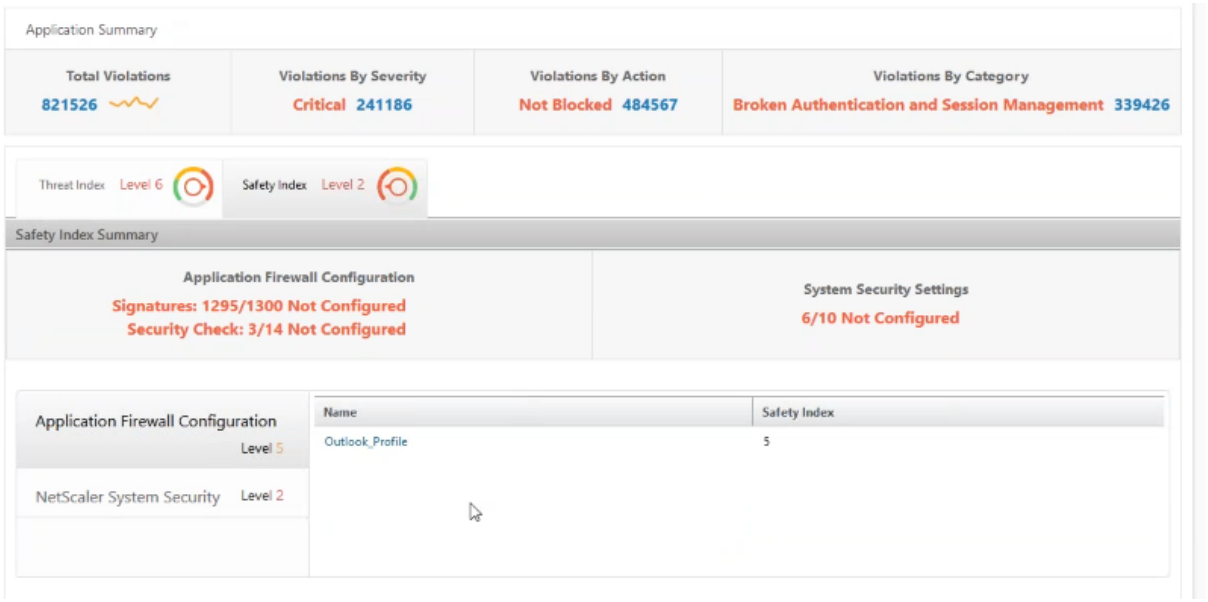
Bestimmen der vorhandenen und fehlenden Sicherheitskonfiguration für eine Anwendung

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.

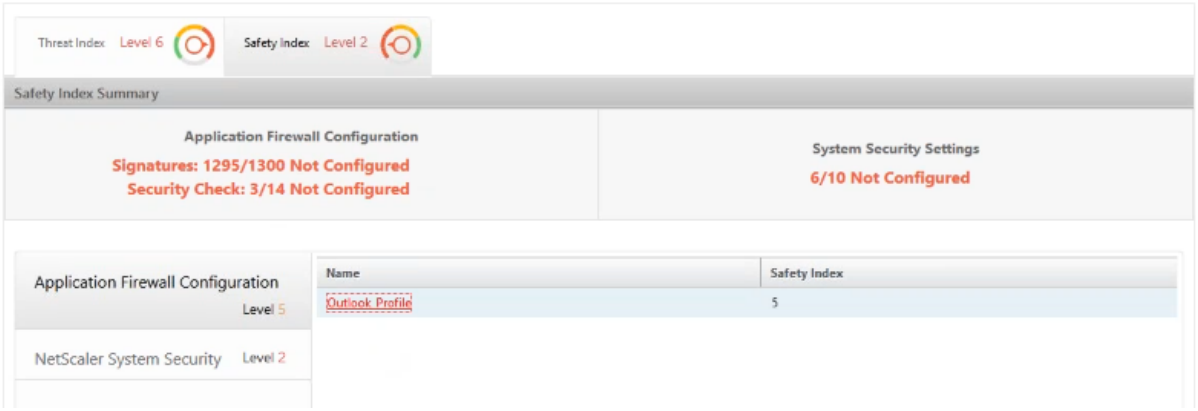
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

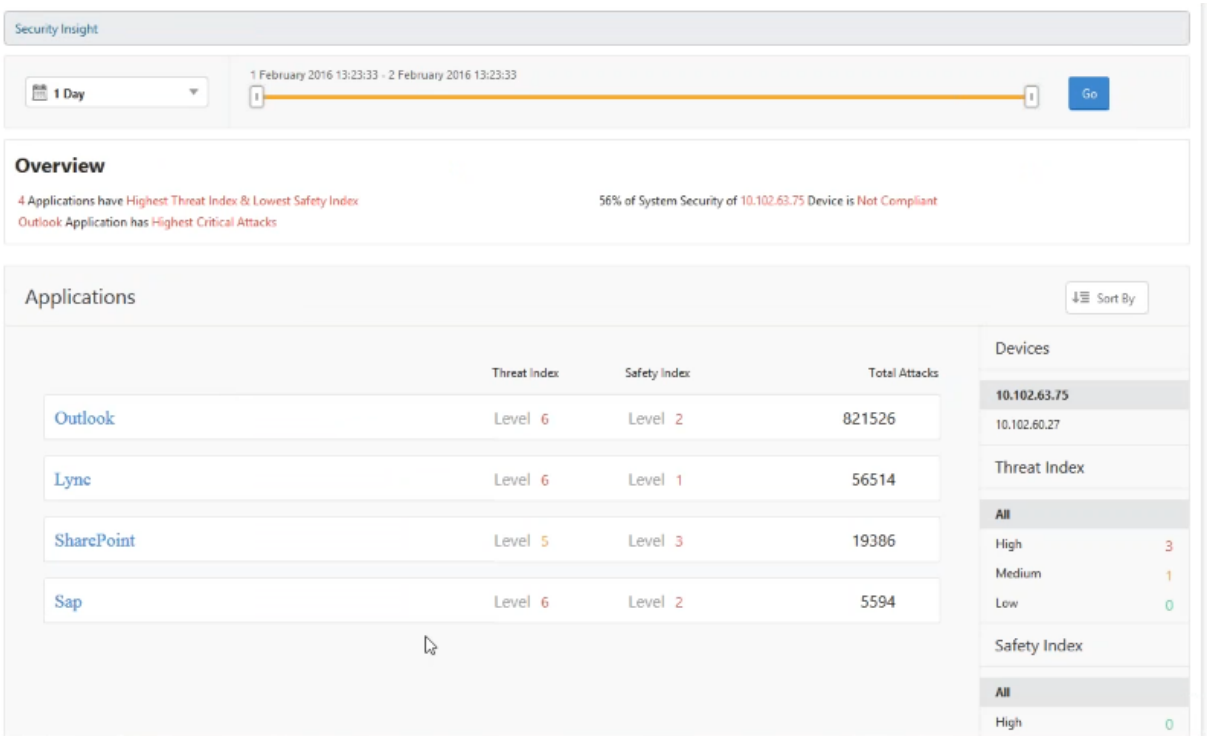
Klicken Sie auf den Knoten **NetScaler System Security**, und überprüfen Sie die Systemsicherheitseinstellungen und Empfehlungen von Citrix, um den Anwendungssicherheitsindex zu verbessern.

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.

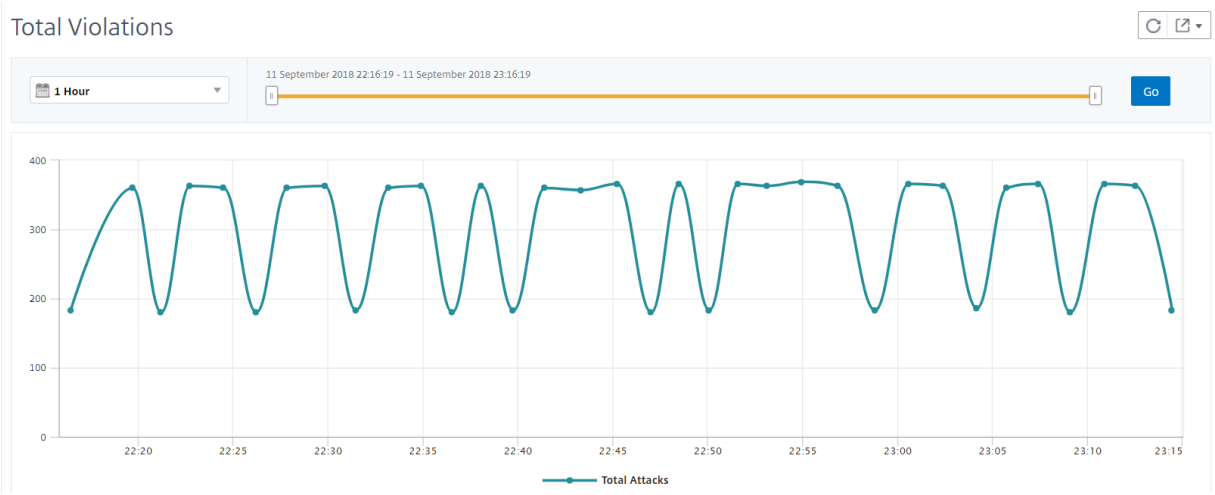
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Ermitteln Sie die Anzahl der Angriffe in einem bestimmten Zeitraum

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.

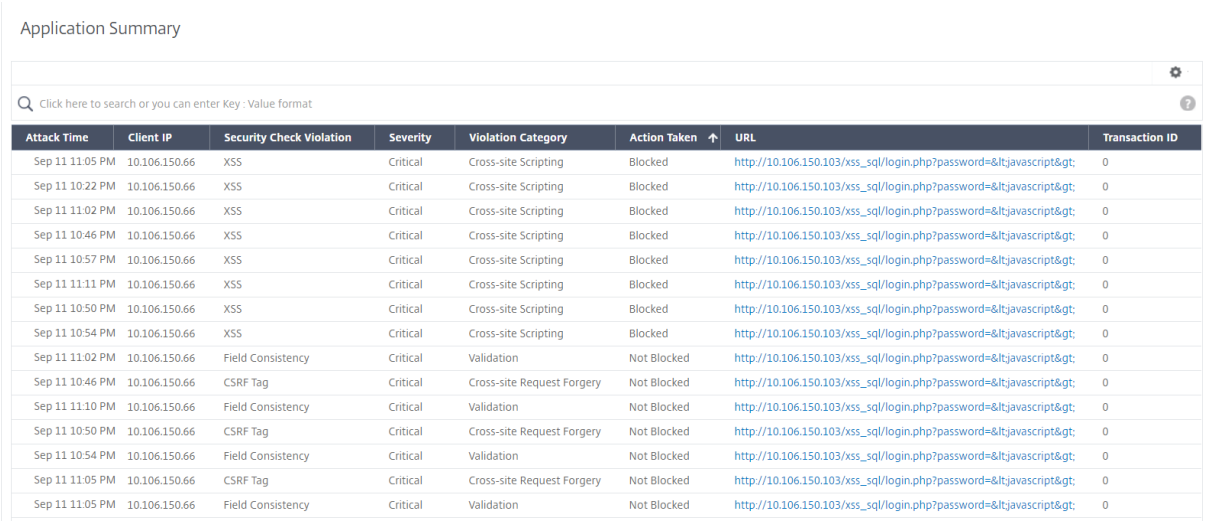
Klicken Sie auf der Seite Security Insight auf eine Anwendung und klicken Sie in der **Anwendungsübersicht** auf die Anzahl der Verstöße. Auf der Seite Total Violations werden die Angriffe grafisch für eine Stunde, einen Tag, eine Woche und einen Monat angezeigt.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

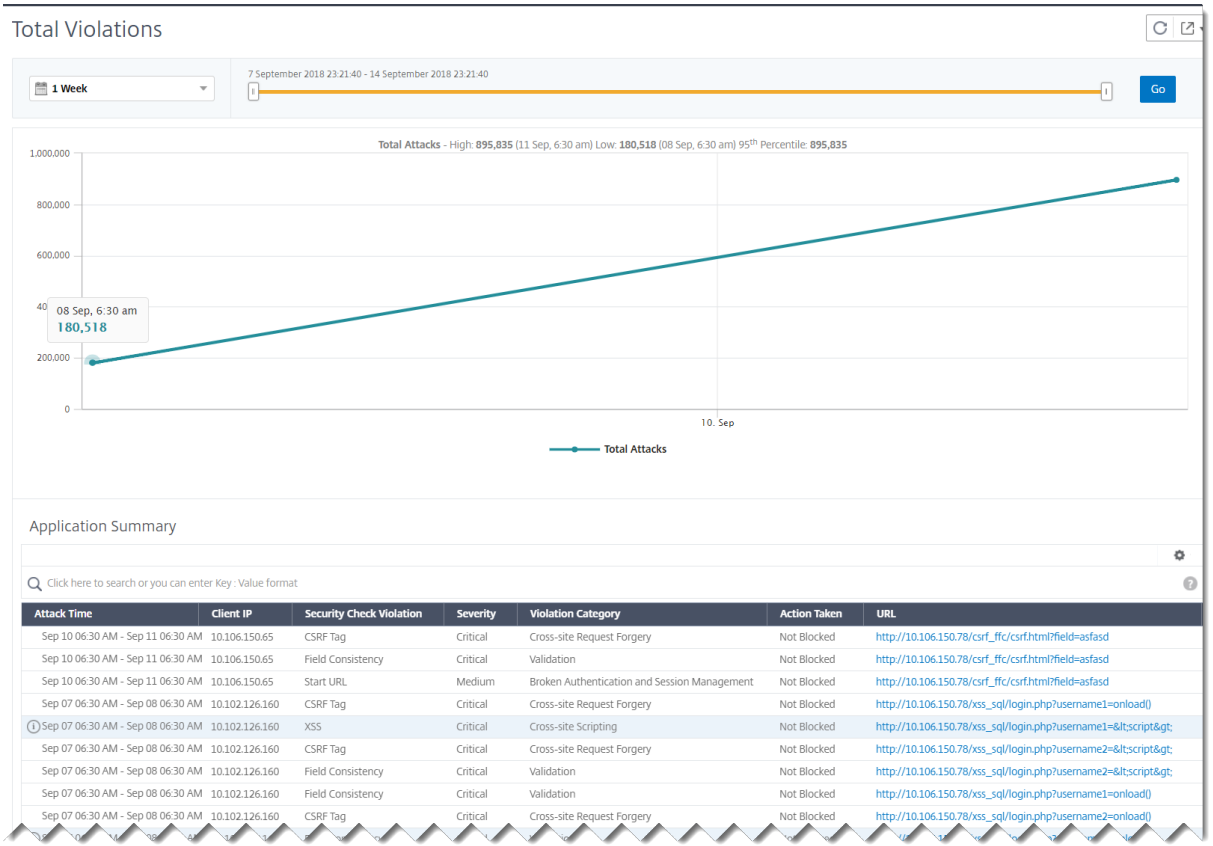

Application Summary

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



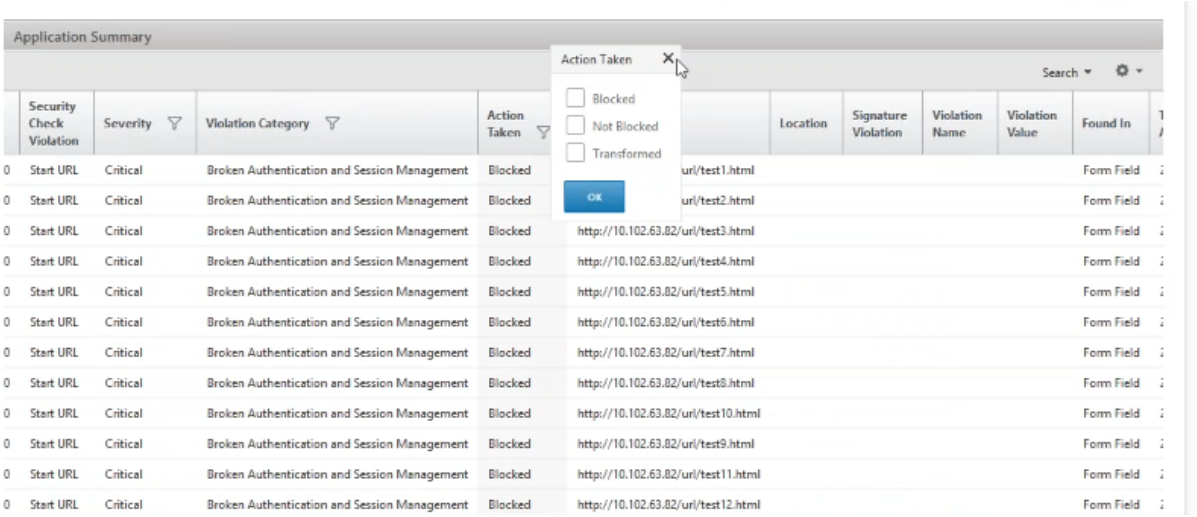
Erhalten Sie detaillierte Informationen über Sicherheitsverletzungen

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

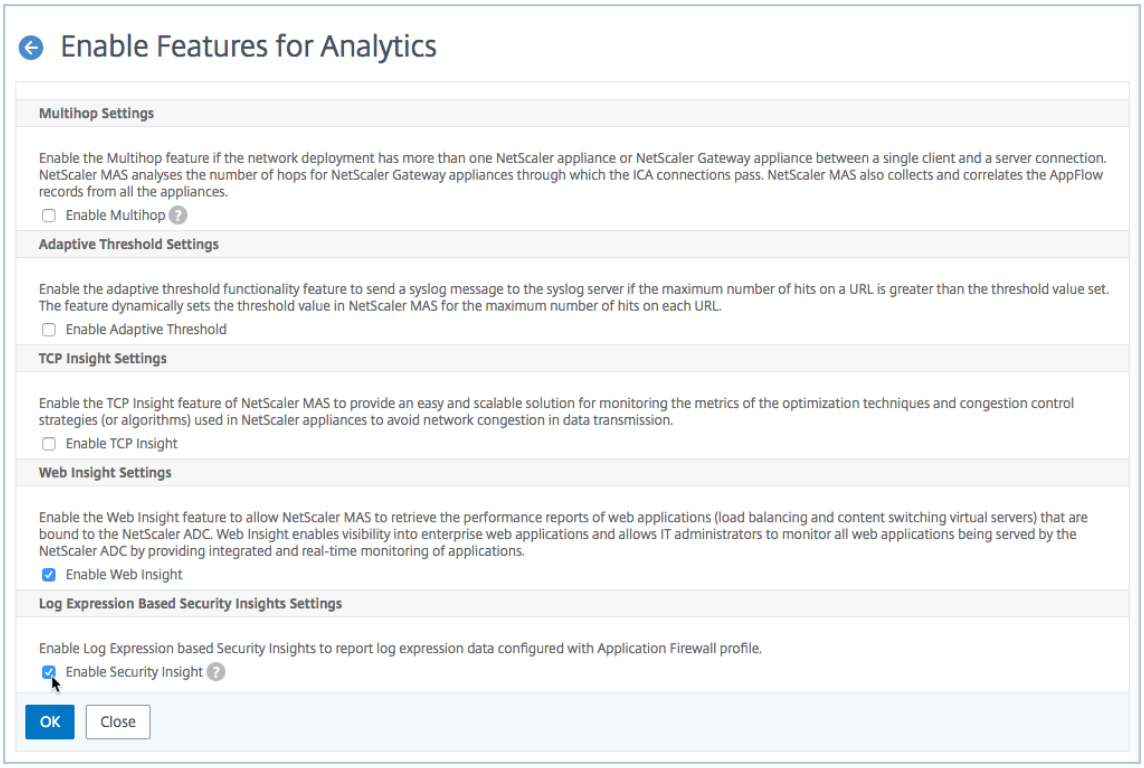
Citrix ADC Instanzen verwenden Protokollausdrücke, die mit dem Application Firewall-Profil konfiguriert sind, um Maßnahmen für Angriffe auf eine Anwendung in Ihrem Unternehmen zu ergreifen. In Security Insight können Sie die Werte anzeigen, die für die Protokollausdrücke zurückgegeben werden, die von 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**.

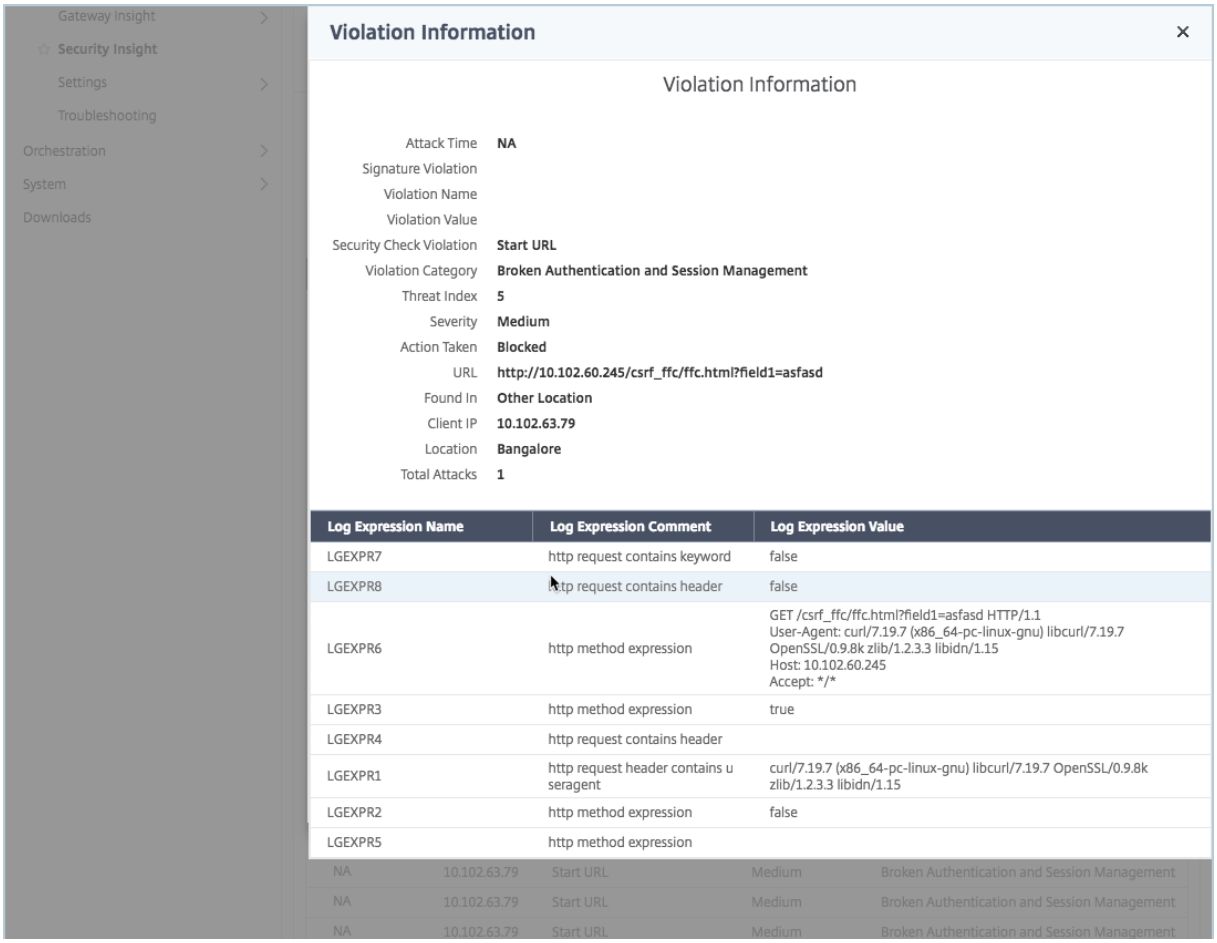
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



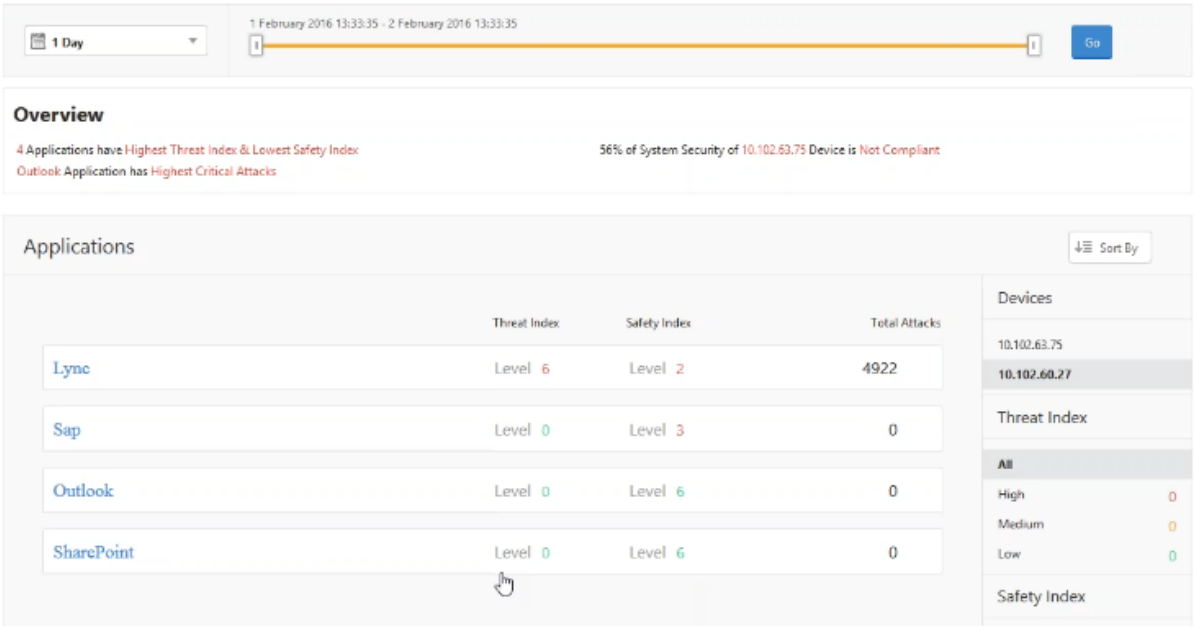
Ermitteln Sie den Sicherheitsindex, bevor Sie die Konfiguration bereitstellen

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.

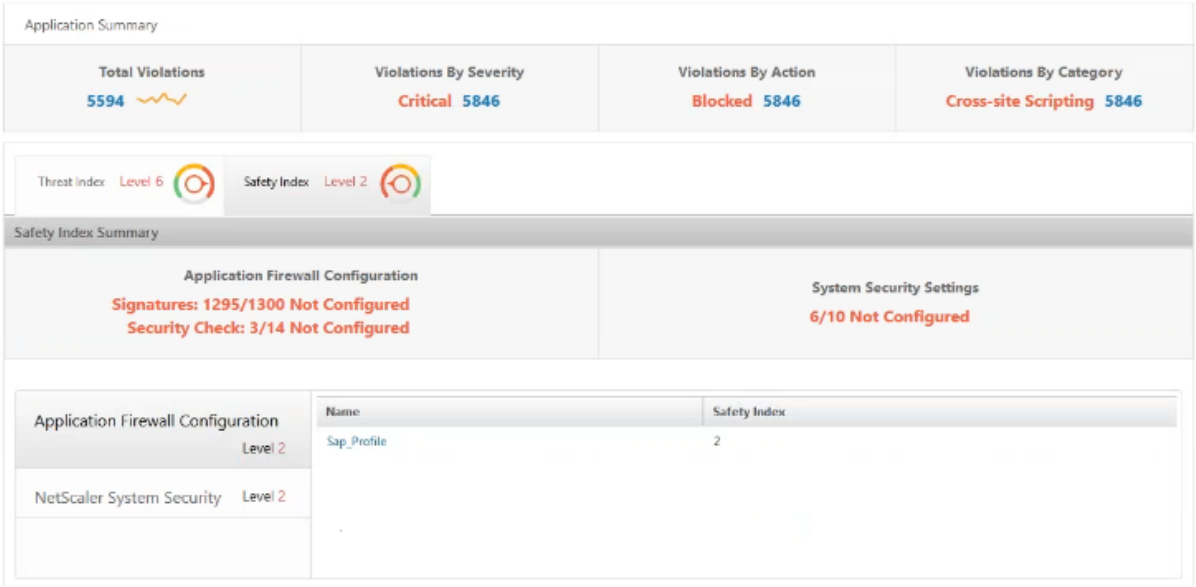
Sie können beispielsweise den Sicherheitsindex der Konfiguration für die SAP-Anwendung auf der Citrix ADC Instanz mit der IP-Adresse 10.102.60.27 bewerten.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

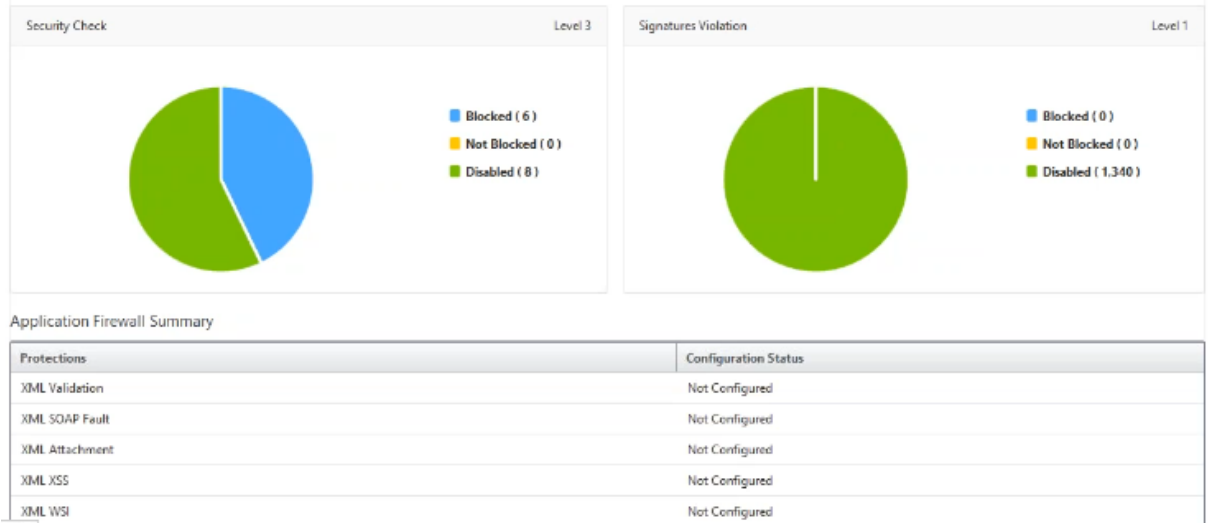


Klicken Sie auf **SAP > Sicherheitsindex > SAP_profile** und bewerten Sie die angezeigten Sicherheitsindexinformationen.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

- **Auswirkungen von Konfigurationsänderungen auf die Nutzung**durch den Kunden ermitteln : Der Administrator kann nachvollziehen, welche Auswirkungen eine Konfigurationsänderung wie das Ausschalten von SSLv3 oder das Entfernen einer Chiffre wie RC4-MD5 auf 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, Chiffren 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Konfigurieren von SSL Insight

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.

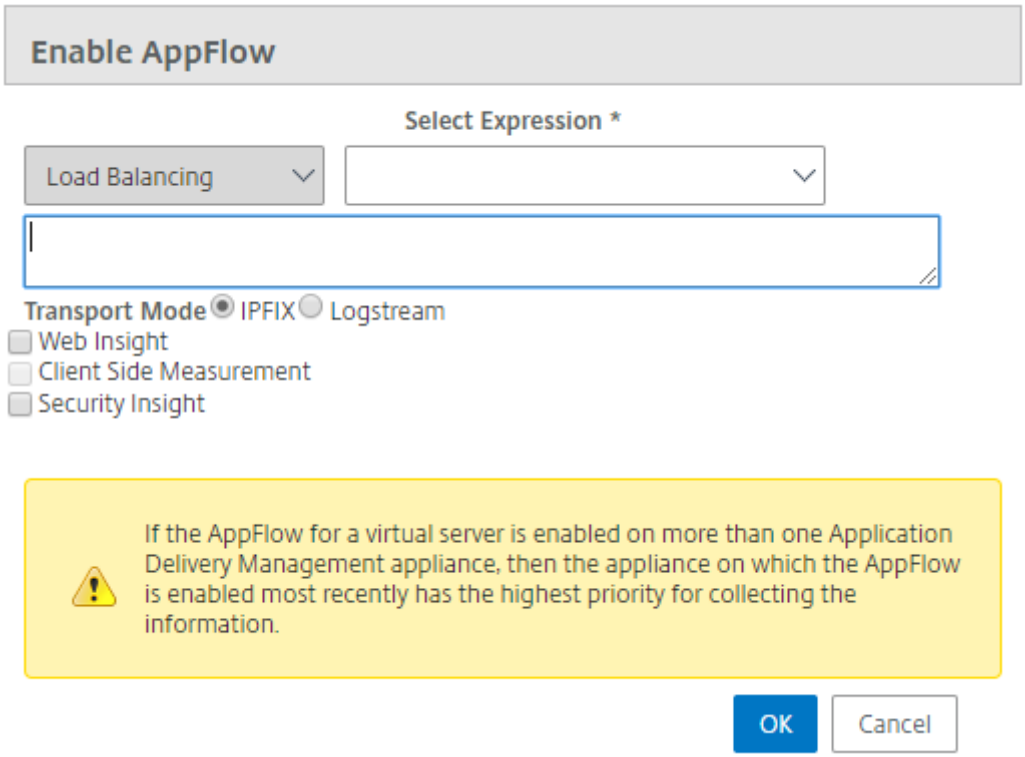
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

1. Navigieren Sie zu **Netzwerke** > **Instanzen**, und wählen Sie die Citrix ADC Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren** aus.
3. Wählen Sie die virtuellen Server aus, und klicken Sie auf **AppFlow aktivieren**.
4. Geben Sie im Feld AppFlow aktivieren **true**ein, und wählen Sie **Web Insight**aus.
5. Wiederholen Sie die Schritte 3 bis 6 auf jeder Citrix ADC Instanz.
6. Klicken Sie auf **OK**.



> **Hinweis**
>
> Sie können die Datenerfassung auf einem virtuellen Server nicht aktivieren, wenn der Betriebszustand des virtuellen Servers nicht UP ist.

So aktivieren Sie das AppFlow Feature mithilfe der NetScaler ADC GUI:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

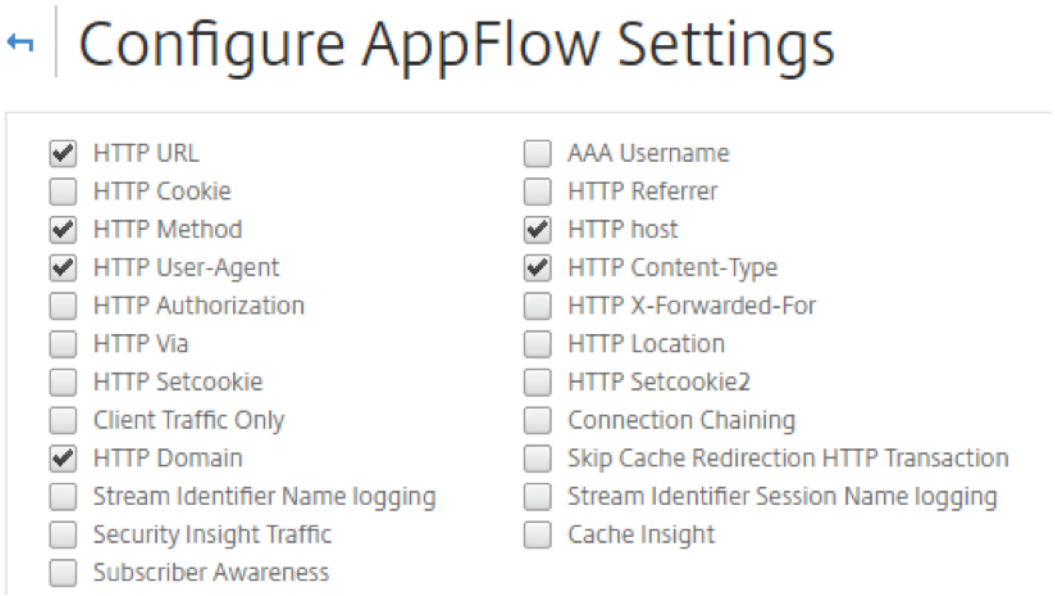
Navigieren Sie in der Benutzeroberfläche einer NetScaler ADC Instanz zu **Konfiguration** > **System** > **Einstellungen**, klicken Sie auf **Erweiterte Funktionen konfigurieren**und wählen Sie **AppFlow**aus.

Aktivieren von SSL Insight-Parametern

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

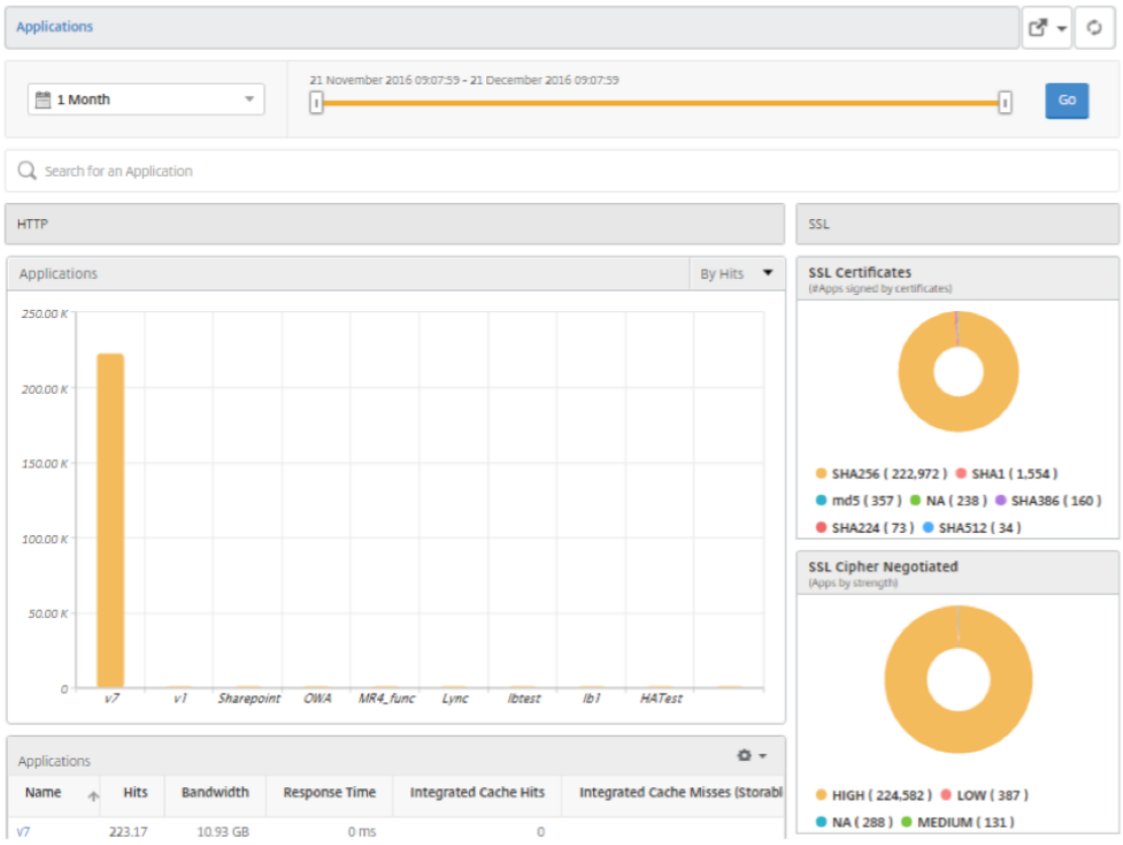
SSL Insight-Metriken in NetScaler ADM bieten einen detaillierten Überblick über die Leistung der SSL-Transaktionen, die von den NetScaler ADC Instanzen bereitgestellt werden. Sie können die SSL Insight-Metriken auf Client-, Server- oder Anwendungsebene sowie die Metriken für SSL-Erfolgs- und Fehlschlagstransaktionen einsehen. Mit Hilfe dieser Metriken können Sie die Citrix ADC HTTPS-Einstellungen und SSL-Zertifikateinstellungen analysieren und optimieren und Leistungsprobleme nachverfolgen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

So überwachen Sie SSL-Insight-Metriken in NetScaler ADM:

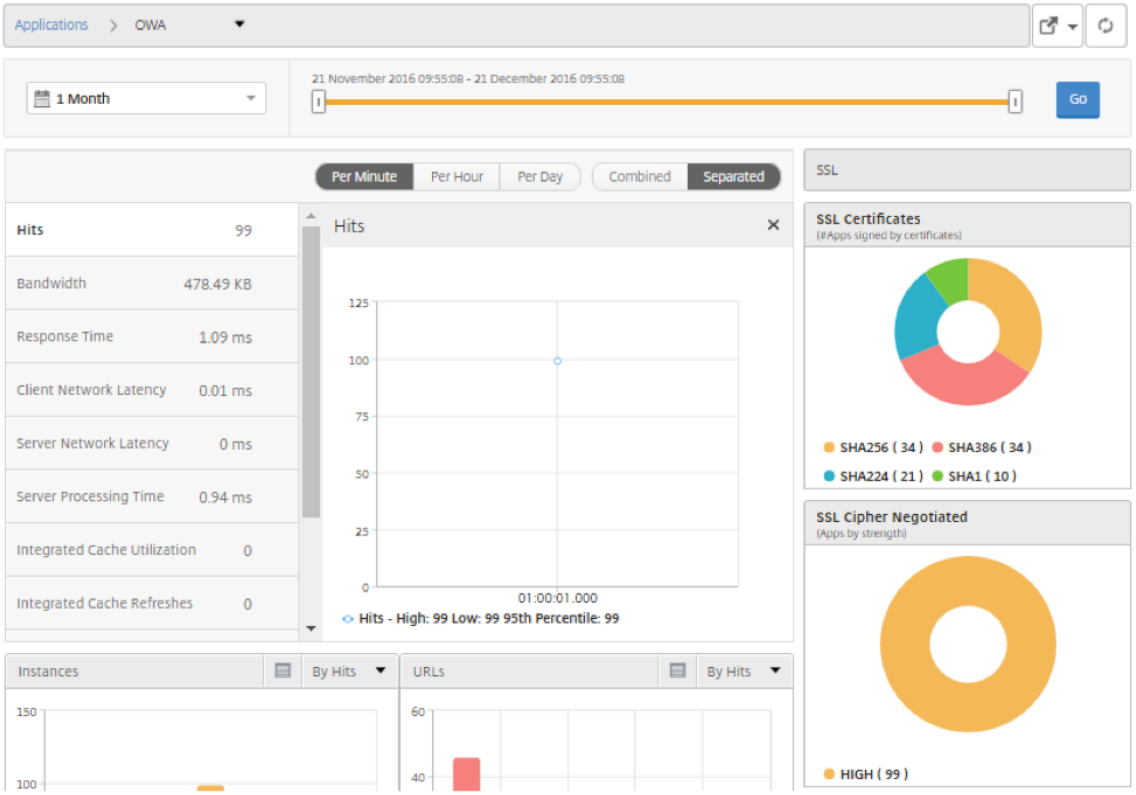
1. Navigieren Sie auf der Registerkarte **Analytics** zu Web Insight und klicken Sie auf den Knoten **Client, Server**oder **Application**, um die Metriken über Clients, den Server oder die Anwendungen anzuzeigen.
2. Wählen Sie im oberen linken Bereich in der Periodenliste den Zeitrahmen aus, dessen Metriken angezeigt werden sollen. Sie können den Zeitrahmen mithilfe des Zeitrahmen-Schiebereglers anpassen. Klicken Sie auf **Go**.
3. Die SSL Insight-Metriken werden als Kreisdiagramme angezeigt, auf die Sie klicken können, um weitere Details zu erhalten.

   > **Hinweis**
   >
   > Die Kreisdiagramme zeigen die Metriken aller Anwendungen, Clients oder Server an.



4. Um Details für eine bestimmte Anwendung, einen bestimmten Client oder einen bestimmten Server anzuzeigen, klicken Sie auf den entsprechenden Wert im Balkendiagramm.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Um die fehlgeschlagenen SSL-Transaktionen anzuzeigen, wählen Sie im Abschnitt SSL das Optionsfeld im Abschnitt SSL aus.

Anwendungsfall: Erhalten Sie einen Überblick über die SSL-Transaktionen von Anwendungen, Clients oder Servern

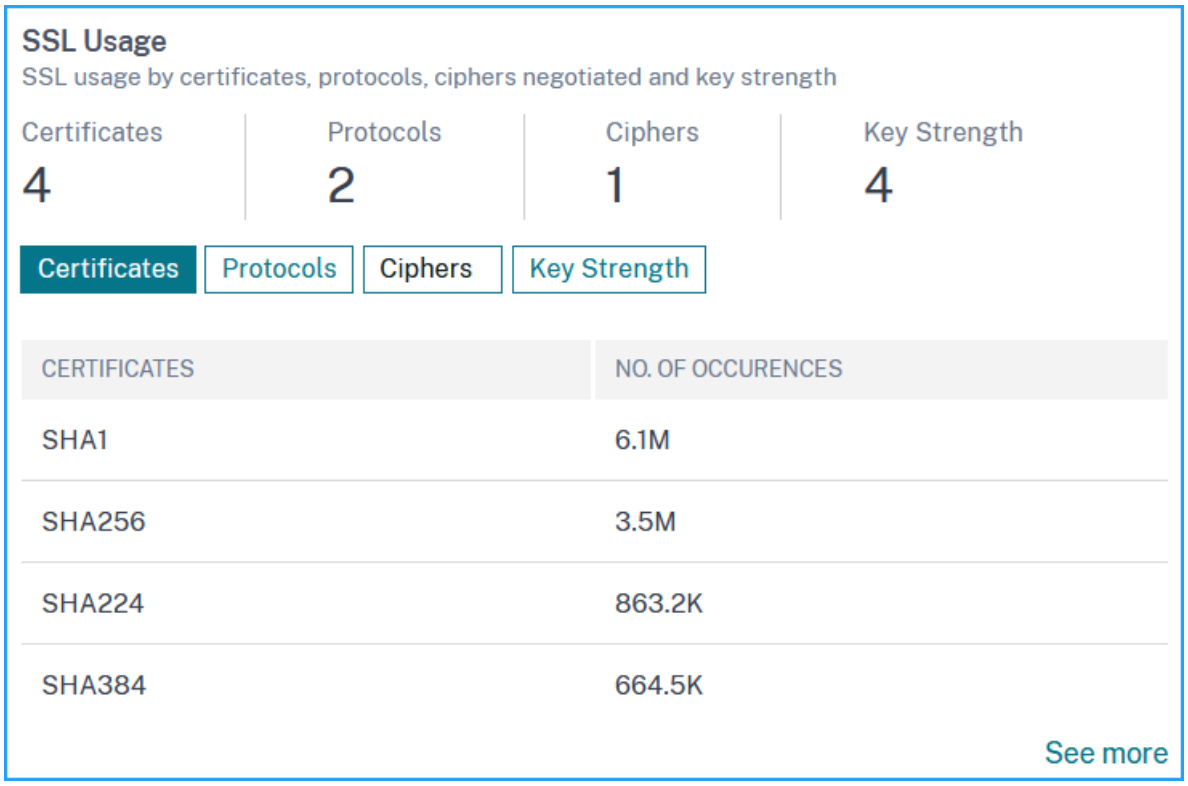
Im folgenden Anwendungsfall wird beschrieben, wie Sie SSL Insight verwenden können, um die Verwendung verschiedener SSL-Parameter in Anwendungen, Clients und Servern zu bewerten und Sicherheitsmaßnahmen zu verbessern.

Beachten Sie, dass Sie über eine Reihe von Anwendungen verfügen, die SSL-Transaktionen (HTTPS) für die Kommunikation verwenden, und Sie 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 SSL-Insight-Dashboard bietet eine Zusammenfassung der verschiedenen SSL-Parameter, die von Ihren Anwendungen über einen von Ihnen gewählten Zeitraum und für ein ausgewähltes Citrix ADC Gerät verwendet werden. Sie sind:

- SSL-Zertifikate
- SSL-Protokolle
- SSL-Verschlüsselung ausgehandelt

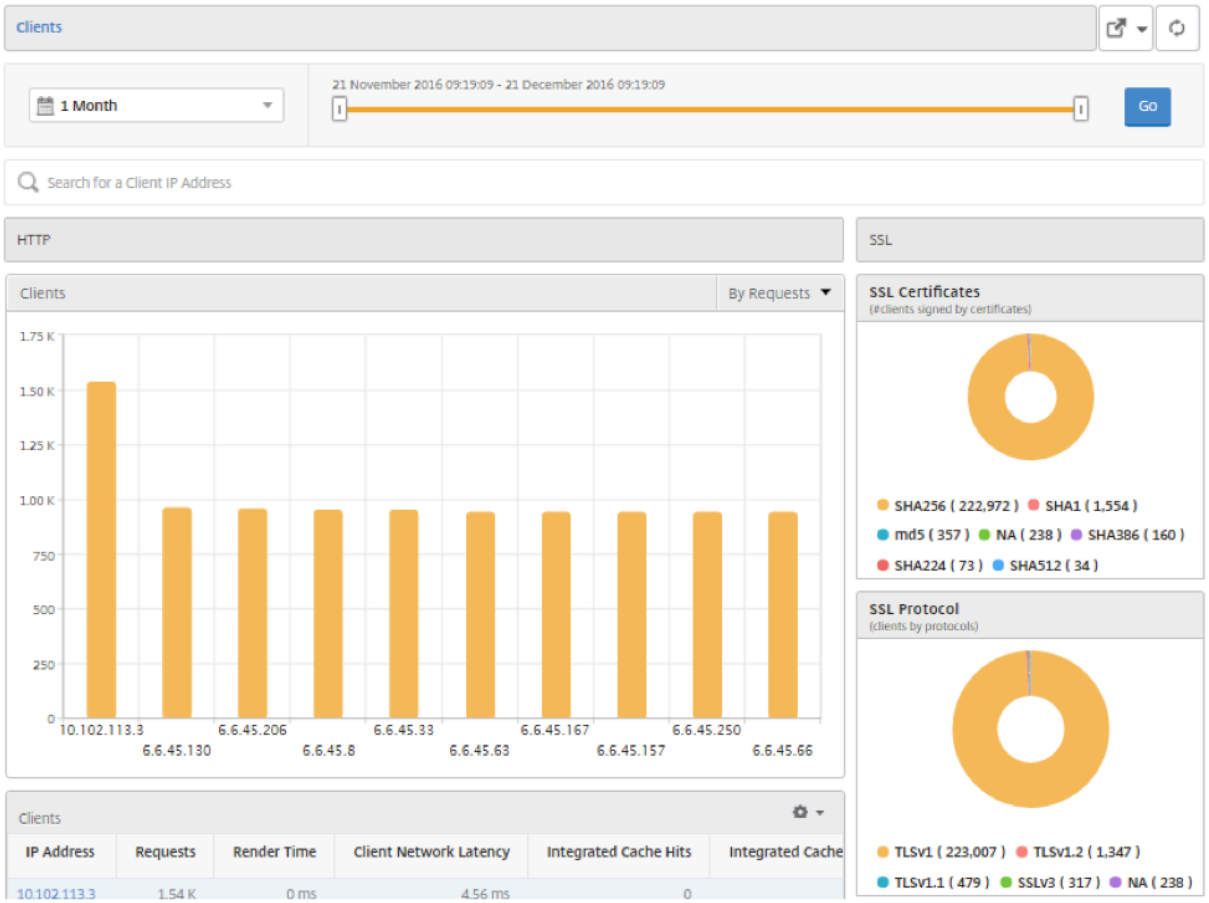
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SSL-Schlüsselstärke
- SSL-Fehler —Frontend
- SSL-Fehler —Backend



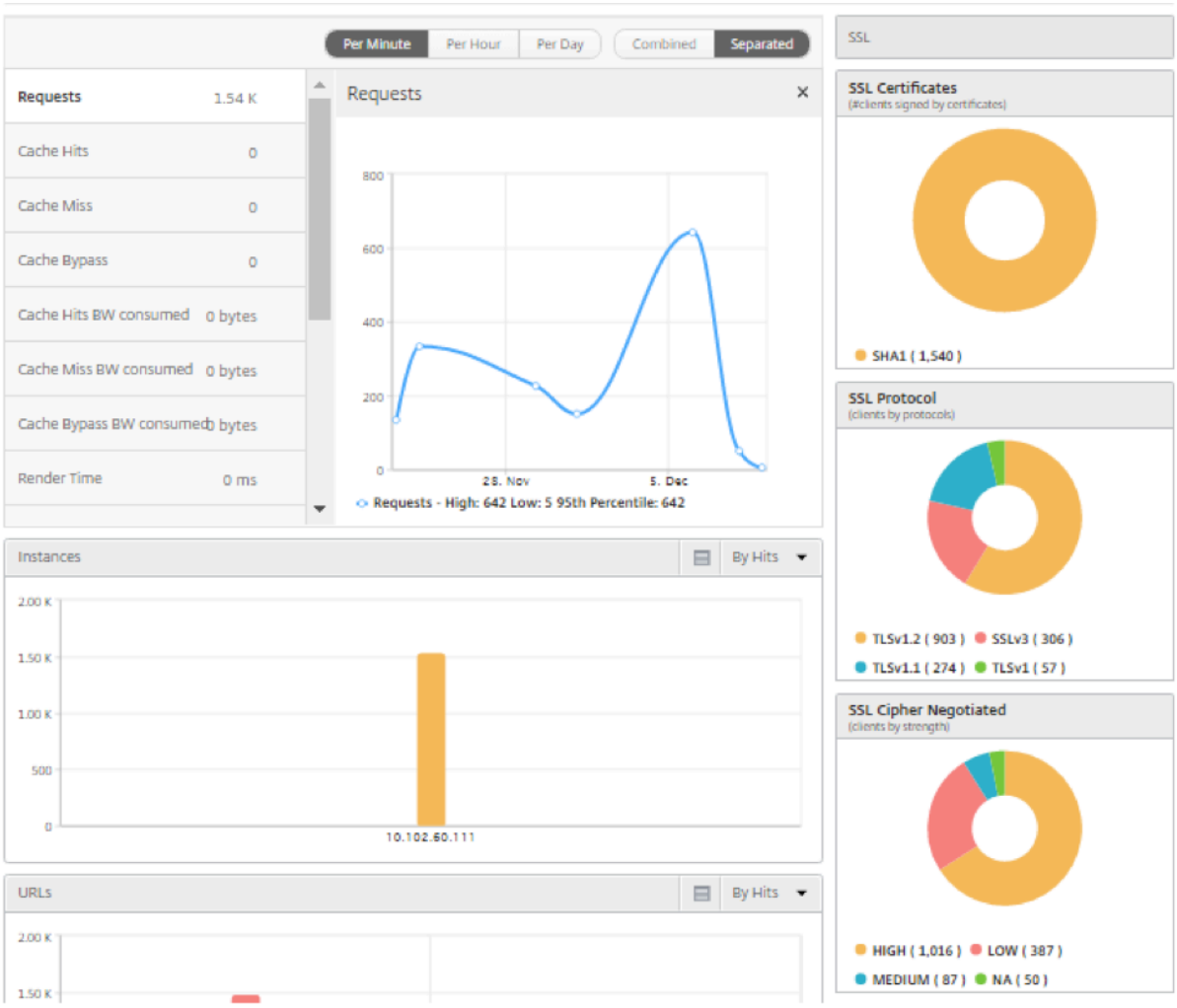
Im folgenden Beispiel sehen Sie eine Liste der Clients (identifiziert durch ihre IP-Adressen) und die SSL-Zugriffe pro Client. Rechts können Sie auch die SSL-Parameter für alle Clients anzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



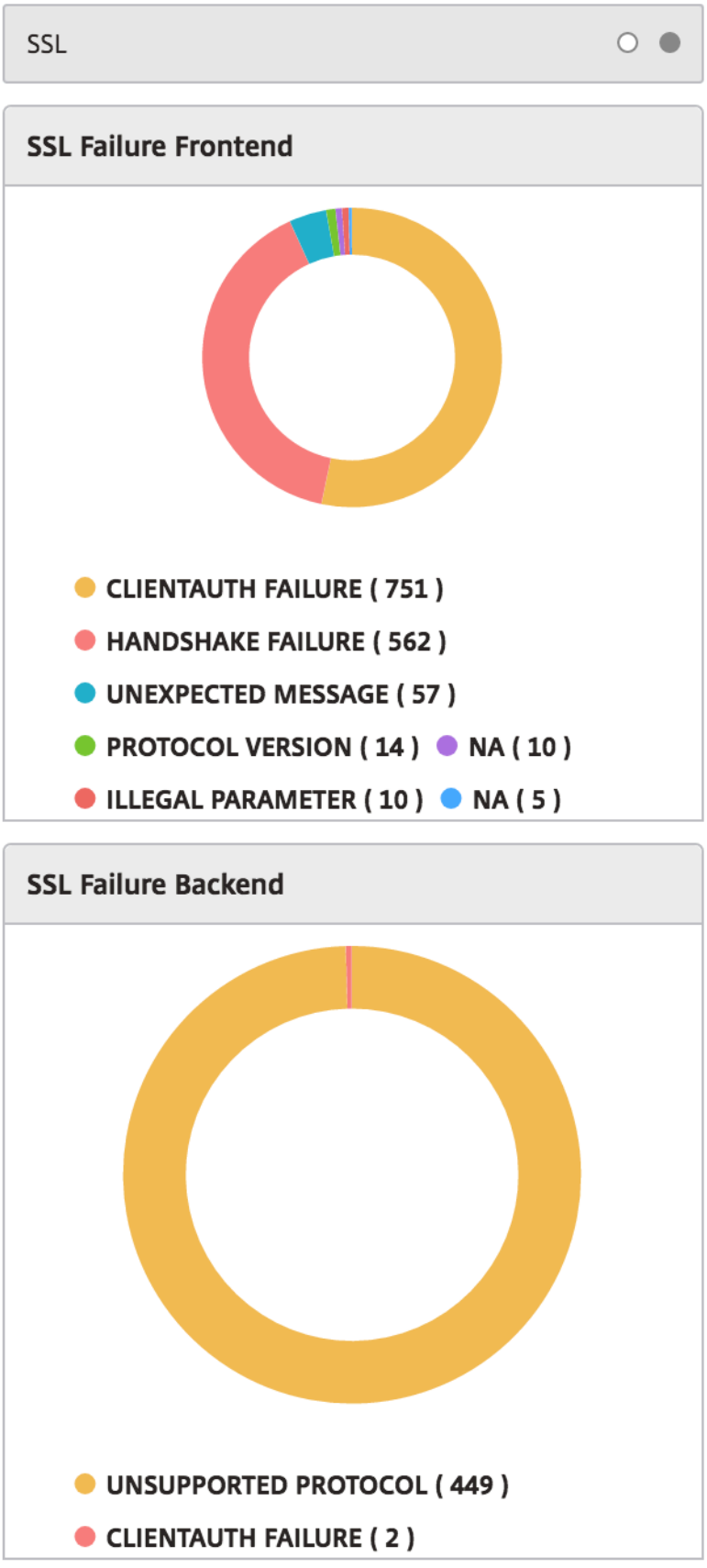
Um SSL-Details für einen Client anzuzeigen, wählen Sie den Client im Balkendiagramm oder in der Tabelle unterhalb des Diagramms aus. Im folgenden Beispiel verwenden die Transaktionen des ausgewählten Clients ein SHA1-SSL-Zertifikat und vier Hauptprotokolle: TSLv1.2, TSLv1.1, TSLv1 und SSLv3. Sie können auch sehen, dass Chiffre verschiedener Stärken ausgehandelt wurden. Der Farbcode gibt die Stärke des SSL-Protokolls an, das Ihnen Informationen über schwache Chiffre und starke Chiffre gibt.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Um die Informationen über die fehlgeschlagenen SSL-Transaktionen anzuzeigen, wählen Sie das Optionsfeld im Abschnitt **SSL**. SSL-Frontend- und Back-End-Fehler werden getrennt in zwei Kreisdiagrammen angezeigt. Im folgenden Beispiel können Sie anzeigen, dass die wichtigsten Back-End-SSL-Fehler Handshake-Fehler sind und die wichtigsten Front-End-SSL-Fehler Unzulässige Parameter sind.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 anzeigen, wie Datenvolumen, Durchsatz und Geschwindigkeit, und diese Informationen verwenden, um das von den Citrix ADC Instanzen bereitete Verkehrsvolumen zu messen und die Vorteile der TCP-Optimierung zu überprüfen. Für die Metriken werden Aufschlüsselungen nach Stream-Richtung (vom Client zu Citrix ADC und Citrix ADC zum Ursprungsserver), TCP-Port und virtuellem LAN 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.

Hardwareanforderungen für Citrix ADM:

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	4 **Hinweis** Citrix empfiehlt, für eine bessere Leistung 8 CPUs zu verwenden.
Stauraum	120 GB

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Komponente	Voraussetzung
	Hinweis Citrix empfiehlt, 500 GB für eine bessere Leistung zu verwenden.

TCP Insight aktivieren

Bevor Sie die TCP Insight-Metriken anzeigen können, müssen Sie die Funktion in NetScaler ADM aktivieren.

So aktivieren Sie TCP Insight:

1. Melden Sie sich mit den Administratoranmeldeinformationen bei Citrix ADM an.
2. Navigieren Sie zu **Analytics** > **Einstellungen**, und klicken Sie auf **Features für Analytics aktivieren**.
3. Wählen Sie auf der Seite **Features für Analysen aktivieren** die Option **TCP Insight aktivieren** aus.
4. Klicken Sie im Bestätigungsfenster auf **OK**.

Anzeigen der TCP Insight-Metriken in Citrix 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 mithilfe des Einstellungssymbols in der Tabelle anpassen. Sie können auch den Zeitraum auswählen, auf den sich die Metriken beziehen, und den Zeitschieberegler verwenden, um den Zeitraum anzupassen.

Sie können auch Metriken für beispielsweise Schnittstellen, Ports und Bitraten anzeigen, indem Sie aus der TCP Insight-Liste auswählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anwendungsfälle

Die folgenden Anwendungsfälle veranschaulichen einige Möglichkeiten zur Verwendung von TCP Insight auf NetScaler ADC Appliances:

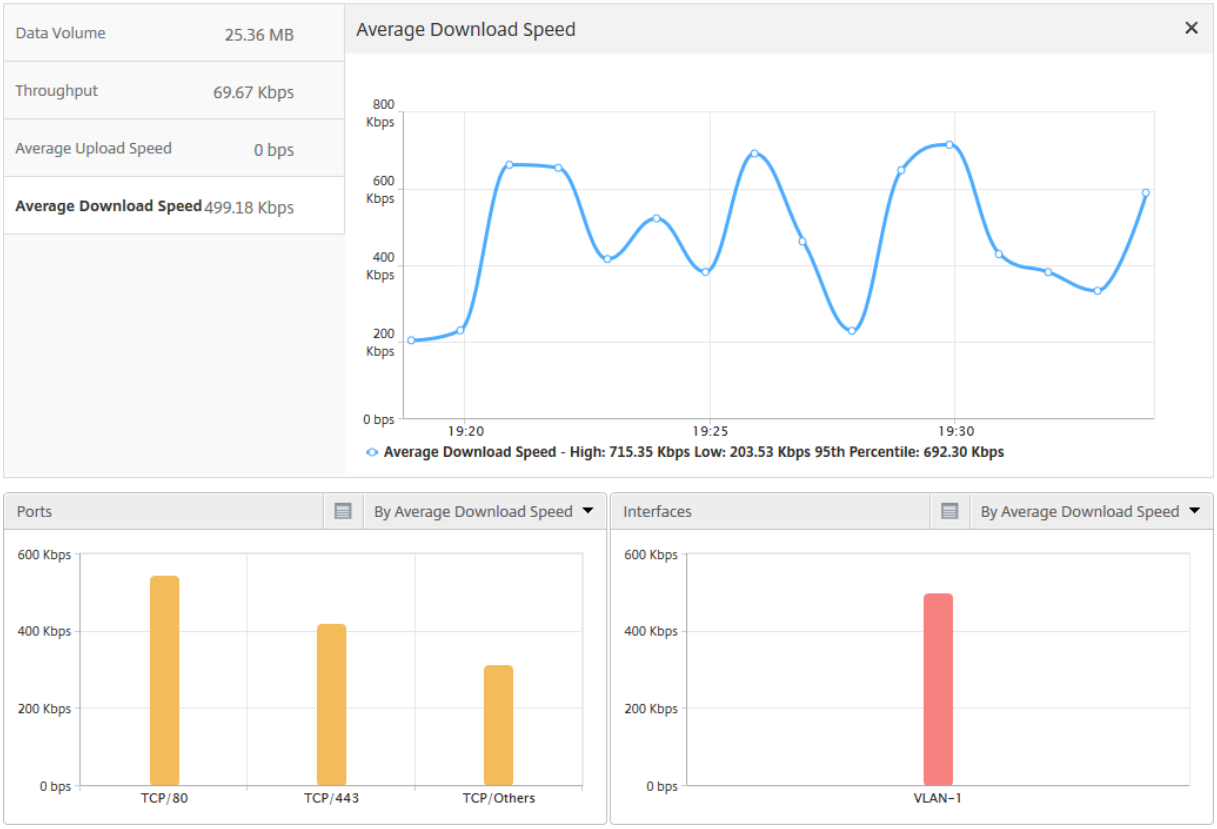
- Bewertung der Vorteile der TCP-Optimierung
- TCP-Parameter optimieren
- Messung der Auswirkungen der TCP-Optimierung auf das Verkehrsaufkommen

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.
Indem Sie die TCP-Insight-Metriken untersuchen, können Sie die Geschwindigkeitsverbesserung quantifizieren, die durch die Optimierung von TCP-Flows erzielt wurde.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

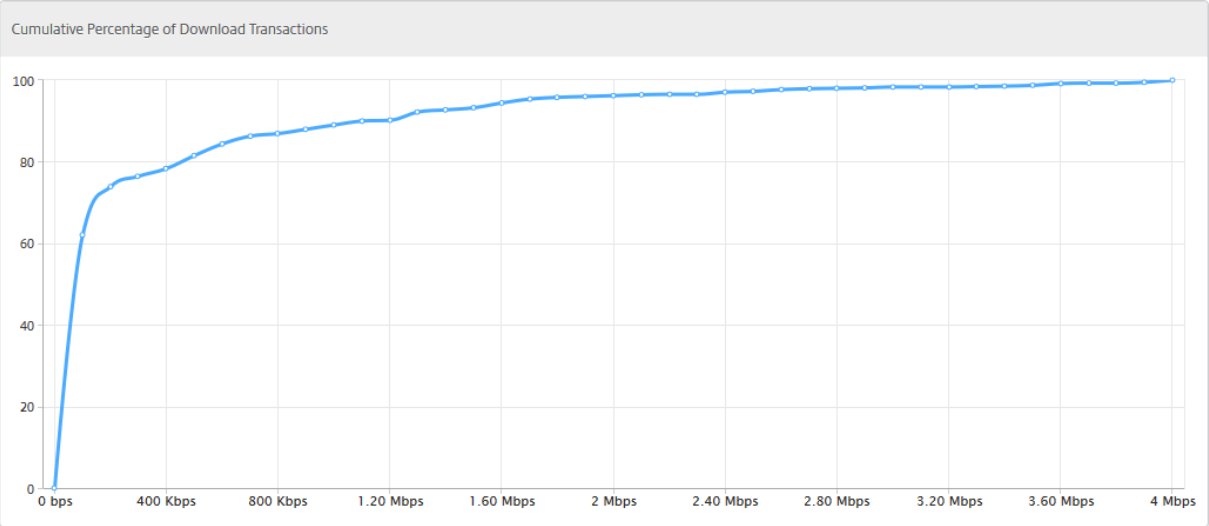


TCP-Parameter optimieren

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



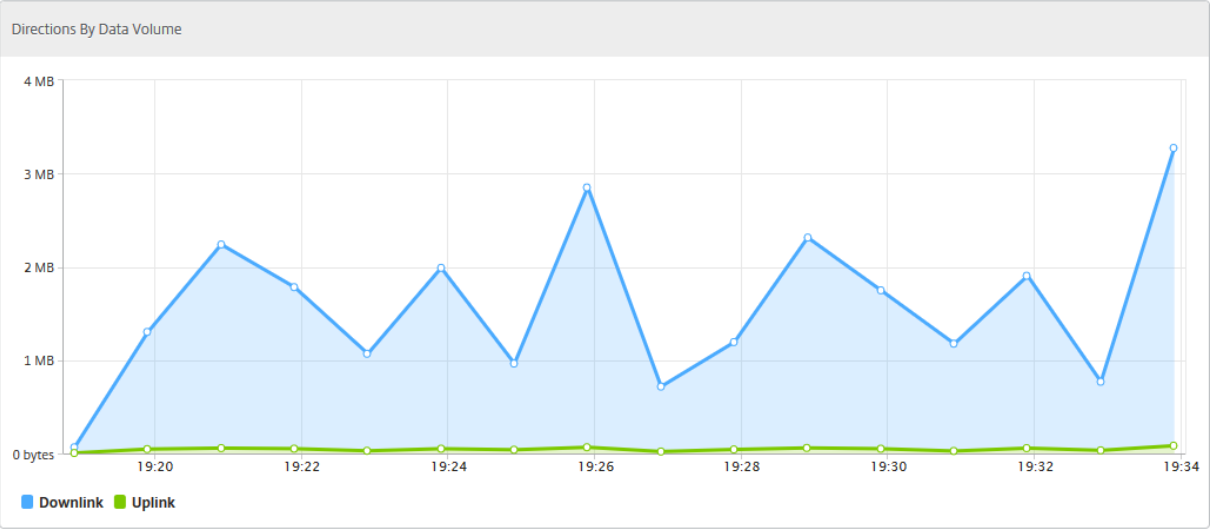
Messung der Auswirkungen der TCP-Optimierung auf das Verkehrsaufkommen

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



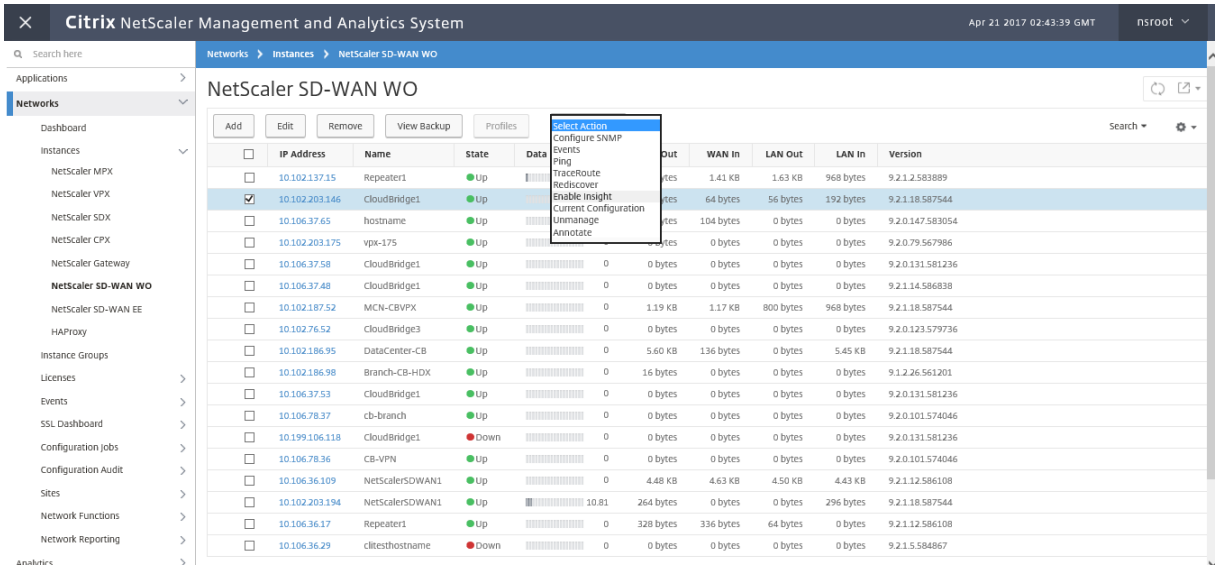
WAN-Einblick

February 5, 2024

Die Citrix SD-WAN -Optimierungs-Appliances (WO) optimieren die Bereitstellung einer großen Anzahl von Anwendungen über das WAN, indem die Effizienz des Datenflusses über das Netzwerk zwischen dem Rechenzentrum und den Zweigstandorten verbessert wird. 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 Einblick in Clients, Anwendungen und Zweigstellen im Netzwerk, um Netzwerkprobleme effektiv zu beheben. Live- und Verlaufsberichte ermöglichen es Ihnen, Probleme proaktiv zu lösen, falls vorhanden

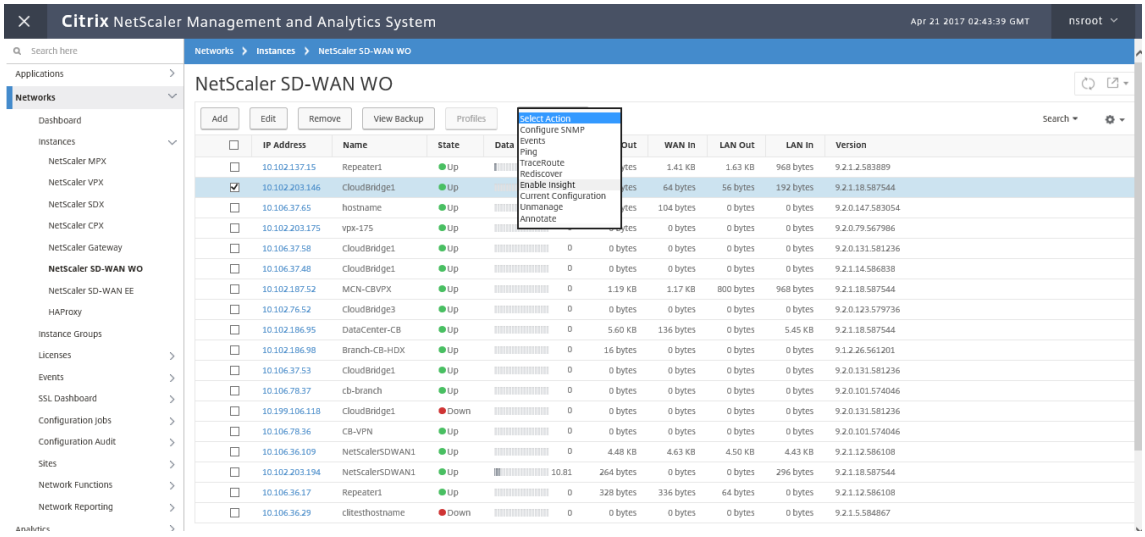
Durch die Aktivierung von Analysen auf der WAN-Optimierungs-Appliance des Rechenzentrums kann NetScaler Application Delivery Management (ADM) Daten sammeln und Berichte und Statistiken für das Rechenzentrum und die WAN-Optimierungs-Appliances für Zweigstellen bereitstellen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



So aktivieren Sie Analysen auf der WAN-Optimierungs-Appliance:

1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADM ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Netzwerke**> **Instanzen** > **Citrix SD-WAN**, und wählen Sie die SD-WAN WO-Instanz aus.



4. Wählen Sie im Drop-down-Menü **Aktion auswählen** die Option **Analytics konfigurieren** aus.
5. Wählen Sie die folgenden Parameter nach Bedarf aus:

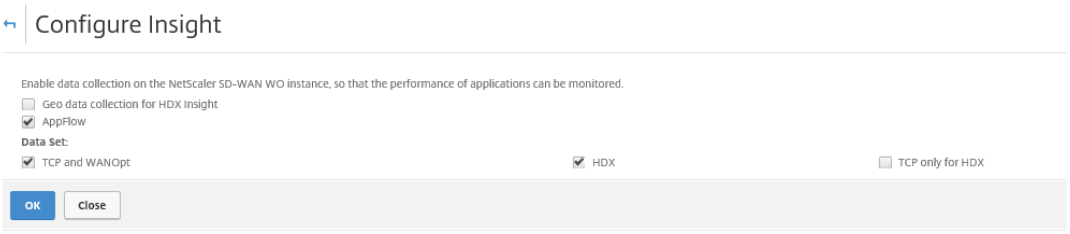
   - **Geodatenerfassung für HDX Insight**: Freigabe der Client-IP-Adresse mit der Google Geo API.

   - **AppFlow**: Beginnt das Sammeln von Daten aus WAN-Optimierungsinstanzen.

     - **TCP und WANOpt**: Bietet TCP- und WANOpt Insight-Berichte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **HDX**: Stellt HDX Insight-Berichte bereit.
- **TCP nur für HDX**: Bietet TCP nur für HDX Insight Berichte.



6. Klicken Sie auf **OK**.

So zeigen Sie WAN Insight-Berichtean:

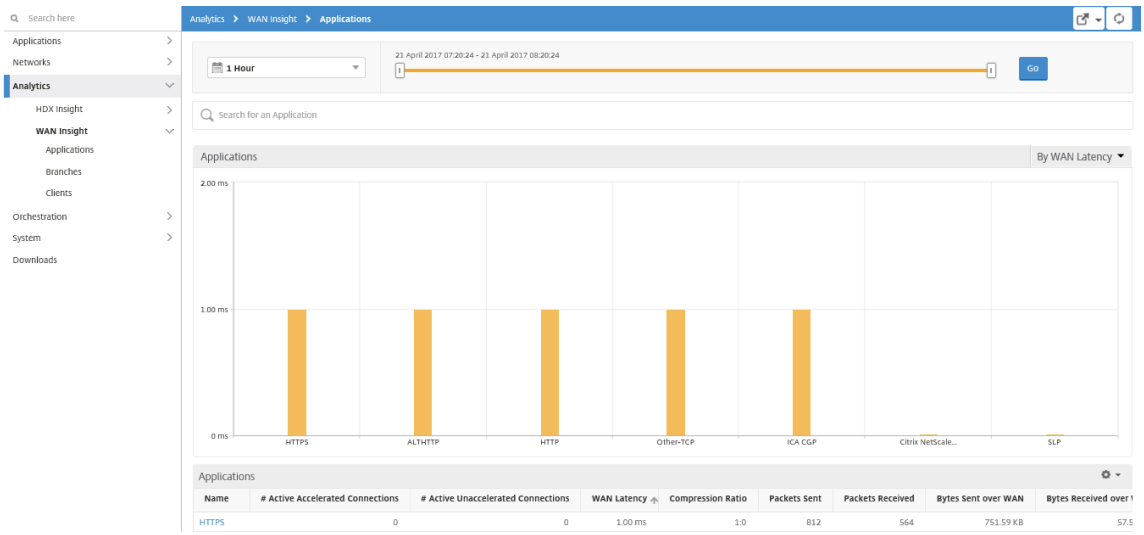
1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADM ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Analytics** > **WAN Insight**.

> **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Zweigstelle und Rechenzentrum-Appliances 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metrik	Beschreibung
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.
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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>

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-->
```

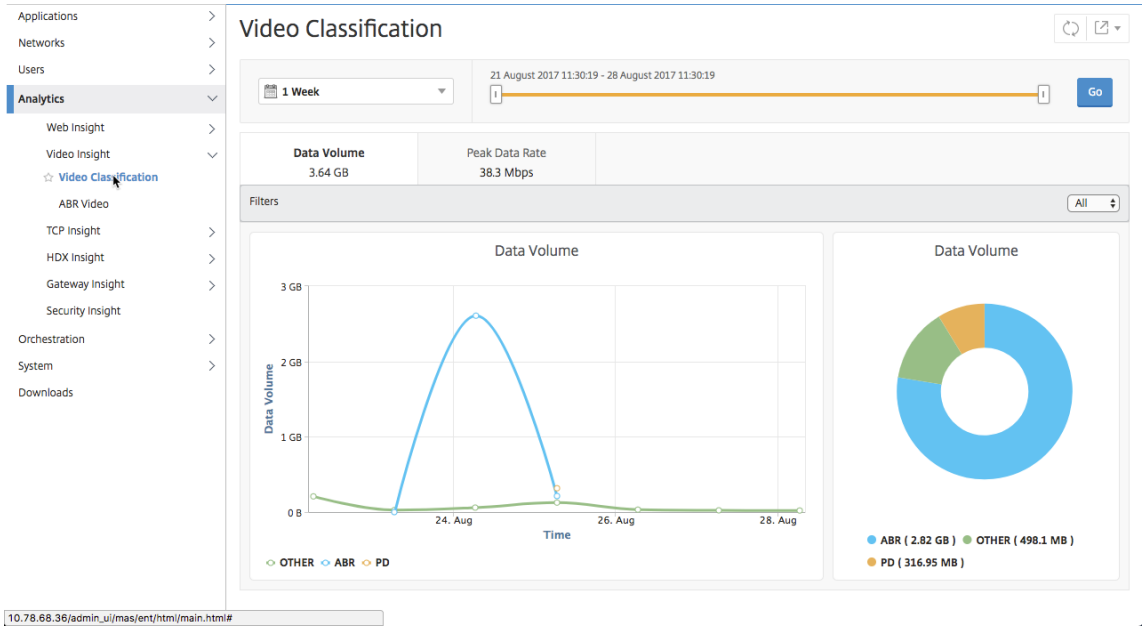
Anzeigen der Video Insight-Metriken in NetScaler ADM

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Hinweis**
>
> Die von der Legende **OTHER** in den Diagrammen bereitgestellten Werte stellen die Nicht-ABR- und Nicht-PD-Daten im Videoverkehr dar, je nachdem, welchen Filter Sie ausgewählt haben:
>
> - **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

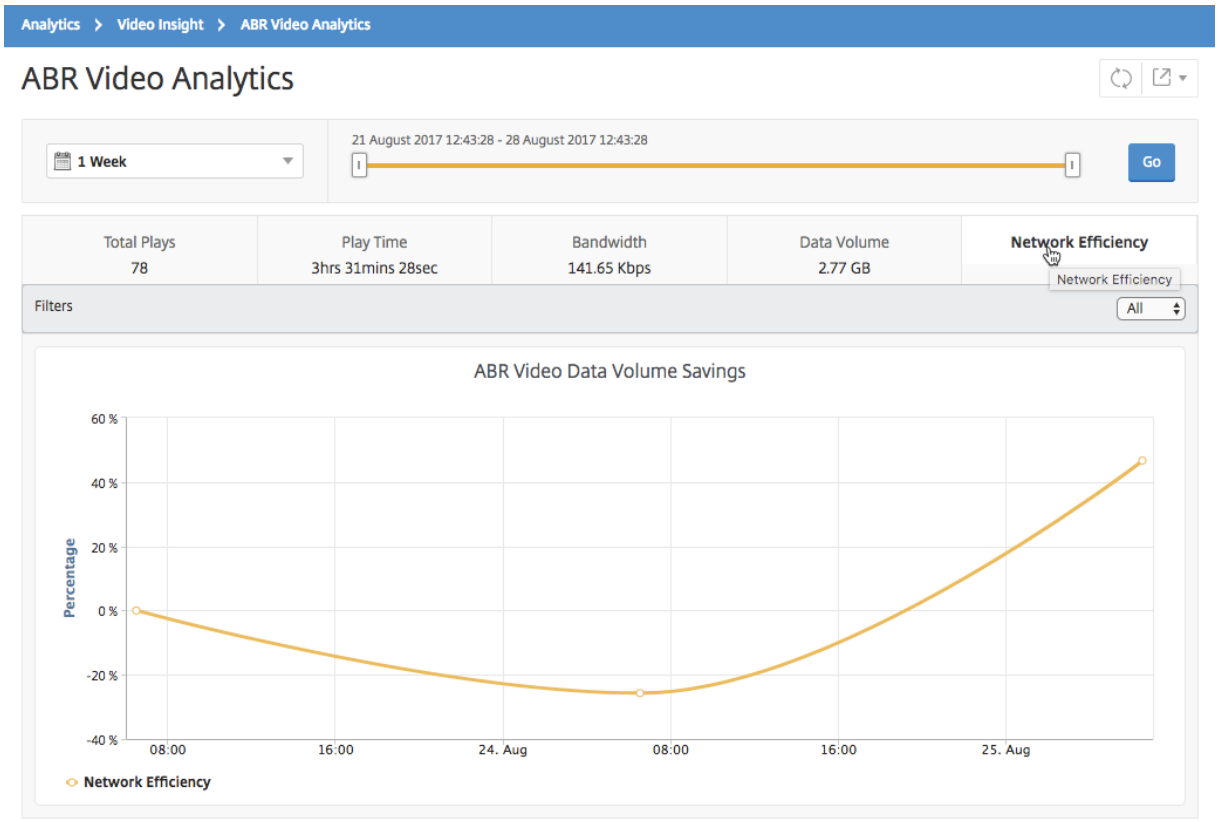
Für einen bestimmten Zeitraum stellt Citrix Application Delivery Management (ADM) ein Diagramm bereit, das das Verhältnis von optimierten zu nicht optimierten Videositzungen im Zeitrahmen anzeigt. Es zeigt auch den Prozentsatz der durch die Optimierung eingesparten Bandbreite an. Der Prozentsatz der eingesparten Bandbreite wird mit der folgenden Formel berechnet:

Prozentsatz der gesparten Bandbreite = **Durchschnittliches optimiertes ABR-Videodatenvolumen/Durchschn des nicht optimierten ABR-Videodatenvolumens**.

Um den Prozentsatz der durch die Optimierung eingesparten Bandbreite anzuzeigen, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video**. Wählen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Netzwerkeffizienz**.



Datenvolumen von optimierten und nicht optimierten ABR-Videos vergleichen

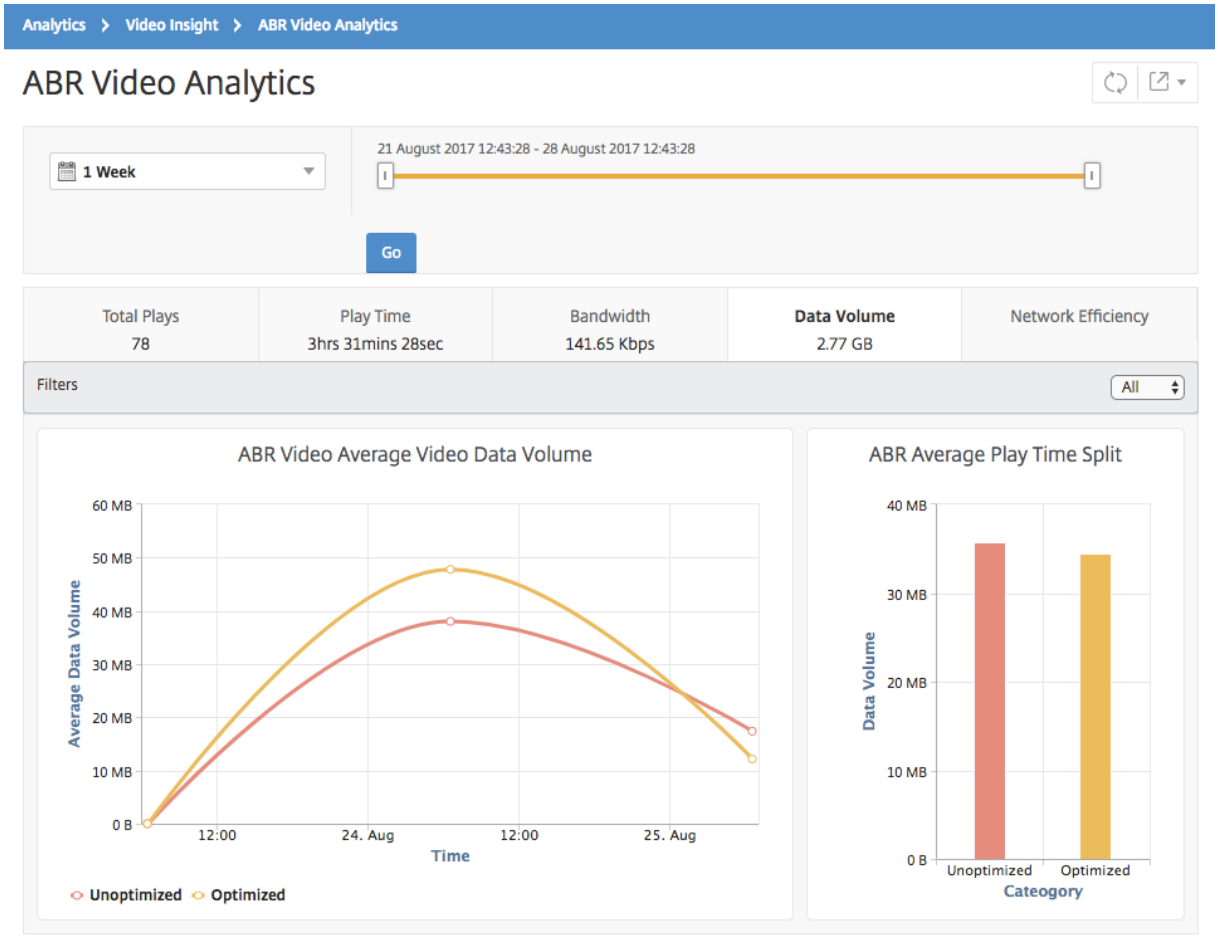
February 5, 2024

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, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video** . Wählen Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Datenvolumen** aus.

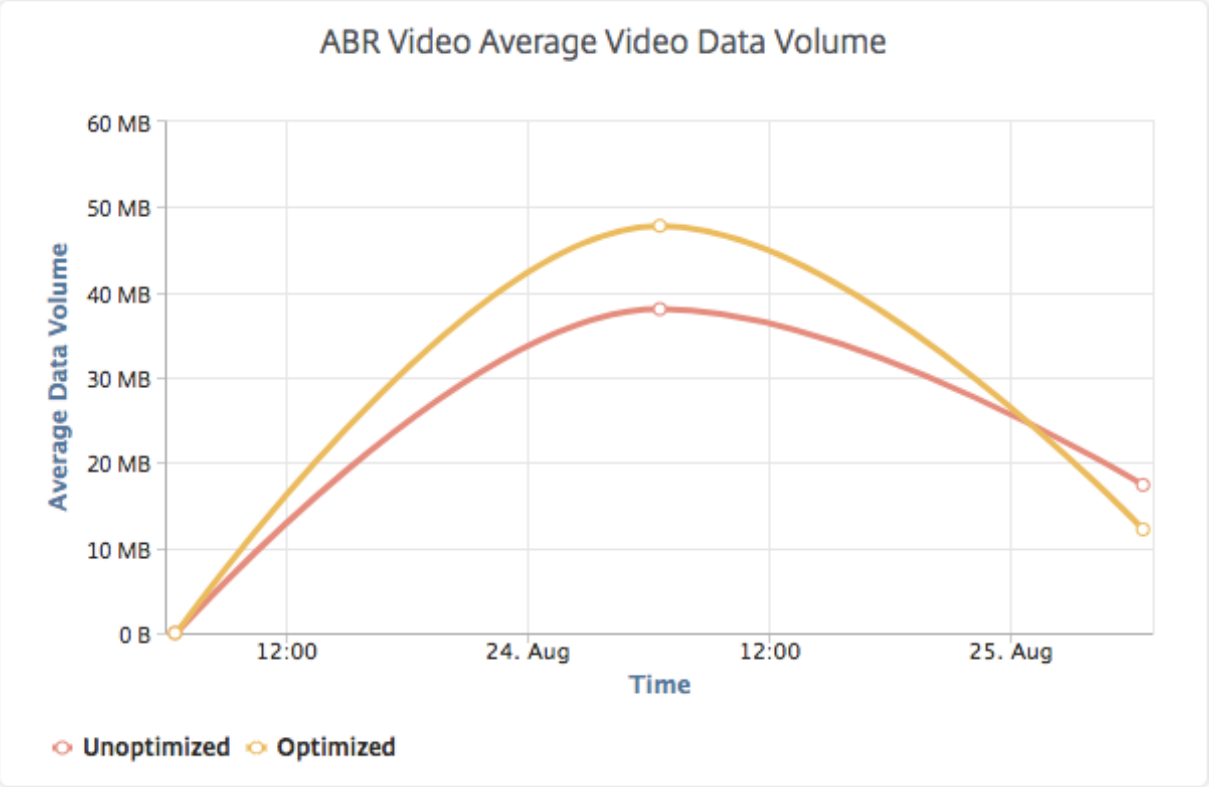
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können die Dropdownliste **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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Typs der gestreamten Videos und des vom Netzwerk verbrauchten Datenvolumens anzegien

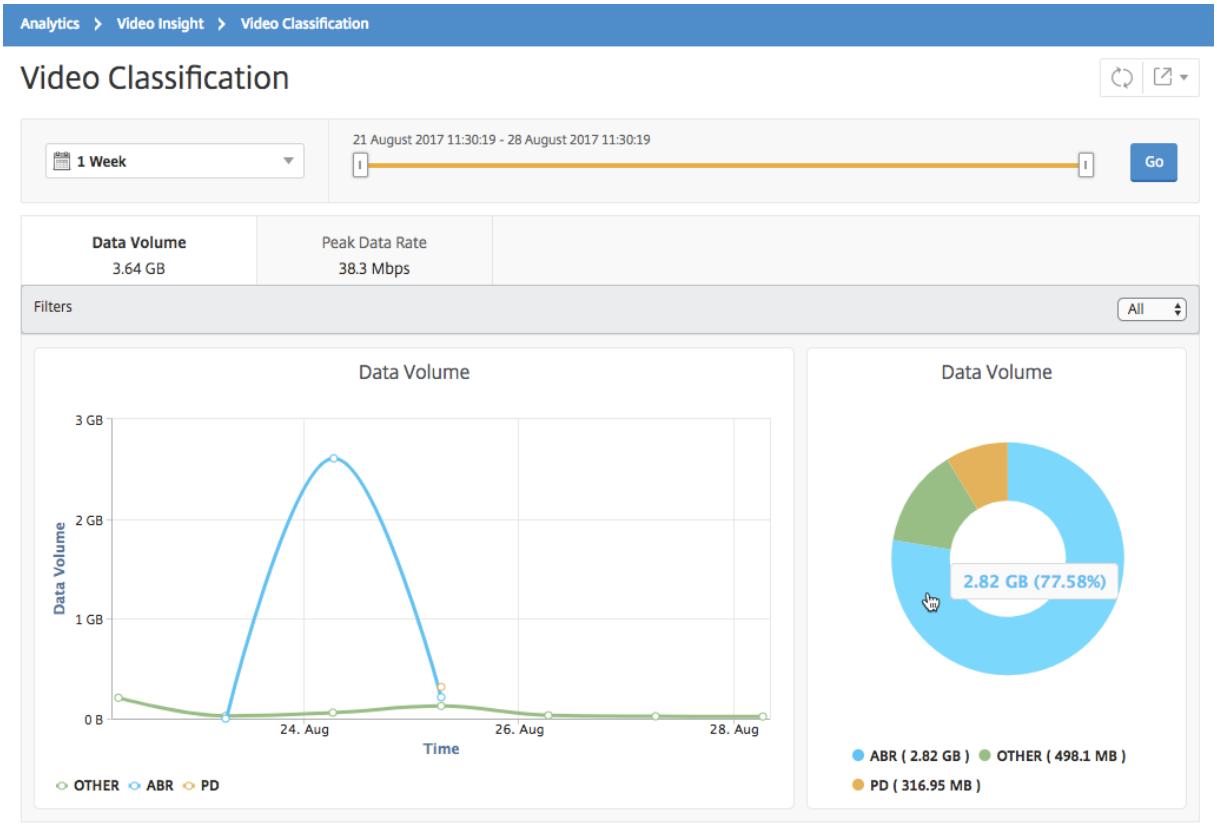
February 5, 2024

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.

Um die Videotypen und das verbrauchte Datenvolumen zu sehen, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **Video Classification** . Wählen Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Go**.

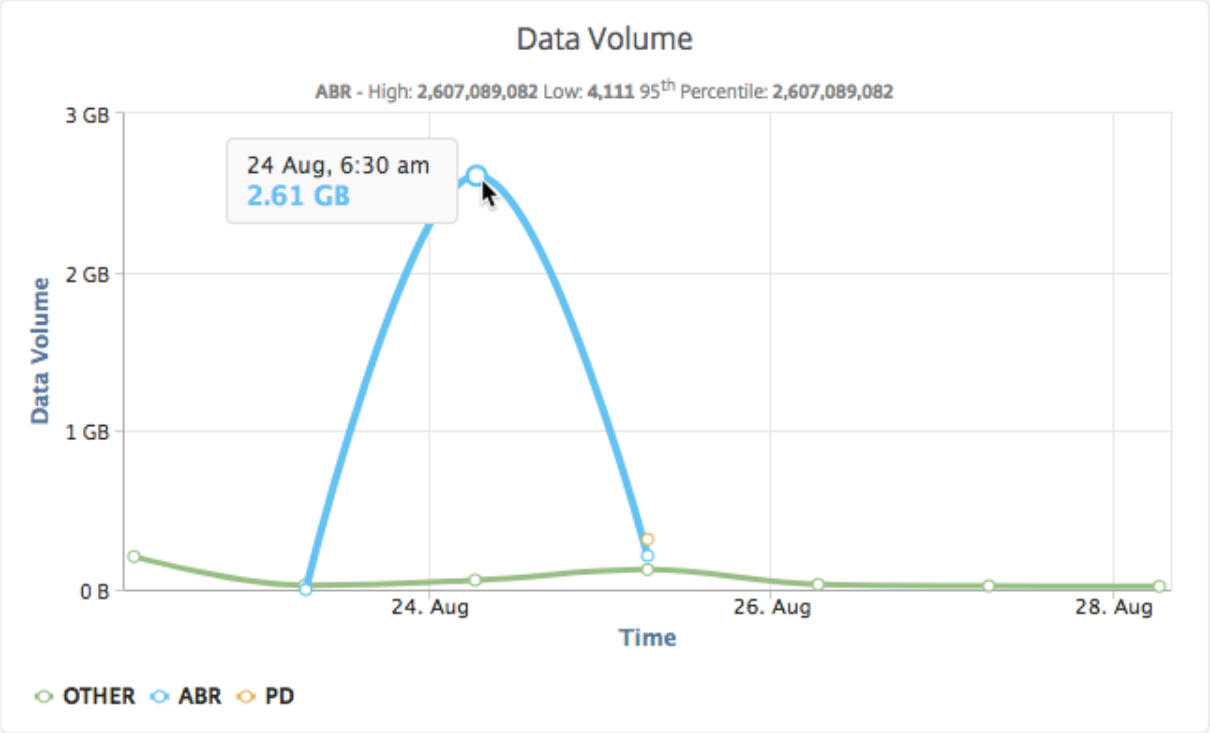
Sie können die Dropdownliste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Verkehr auszuwählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



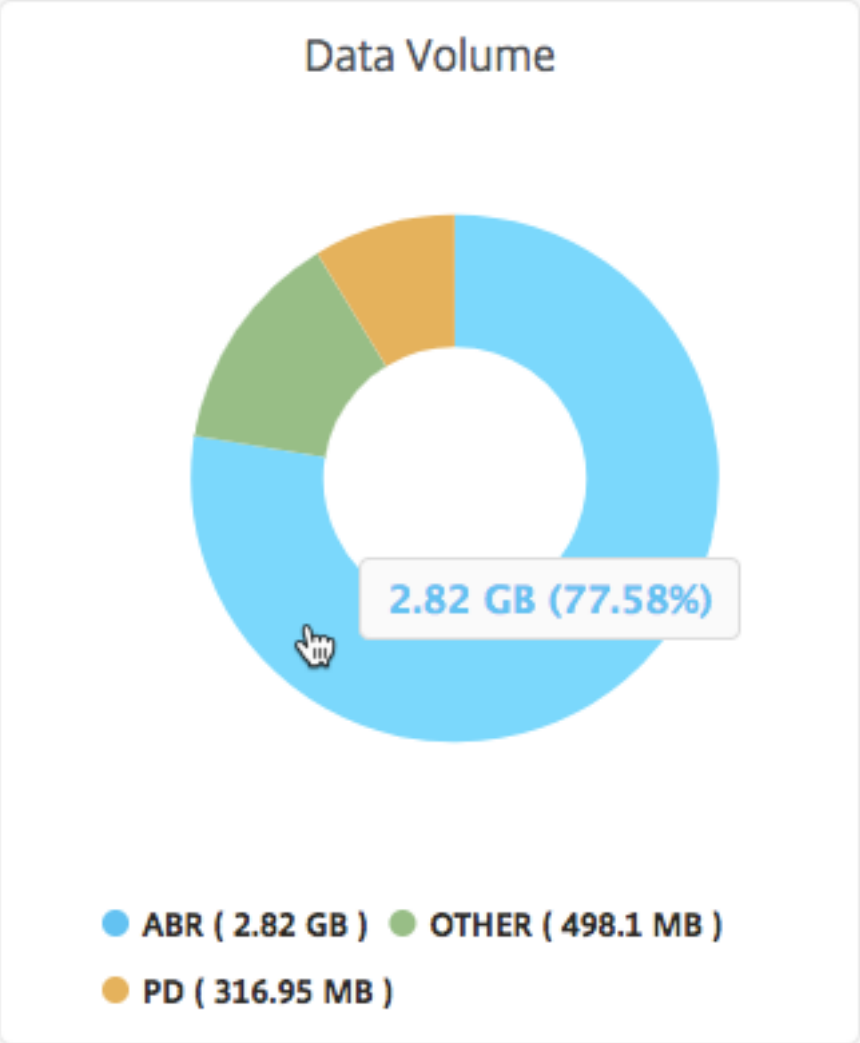
Die Registerkarte **Datenvolumen** enthält ein Liniendiagramm und ein Kreisdiagramm, in dem die Arten des Streamings von Videoverkehr aus Ihrem Netzwerk und das Datenvolumen angezeigt werden, das von Ihrem Netzwerk verbraucht wird. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die während eines bestimmten Zeitrahmens verbrauchten Daten anzuzeigen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Außerdem können Sie den Mauszeiger auf das Kreisdiagramm bewegen, um den Prozentsatz des Datenvolumens anzuzeigen, der von einem bestimmten Typ von Videoverkehr verbraucht wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Optimierte und nicht optimierte Wiedergabezeit von ABR-Videos vergleichen

February 5, 2024

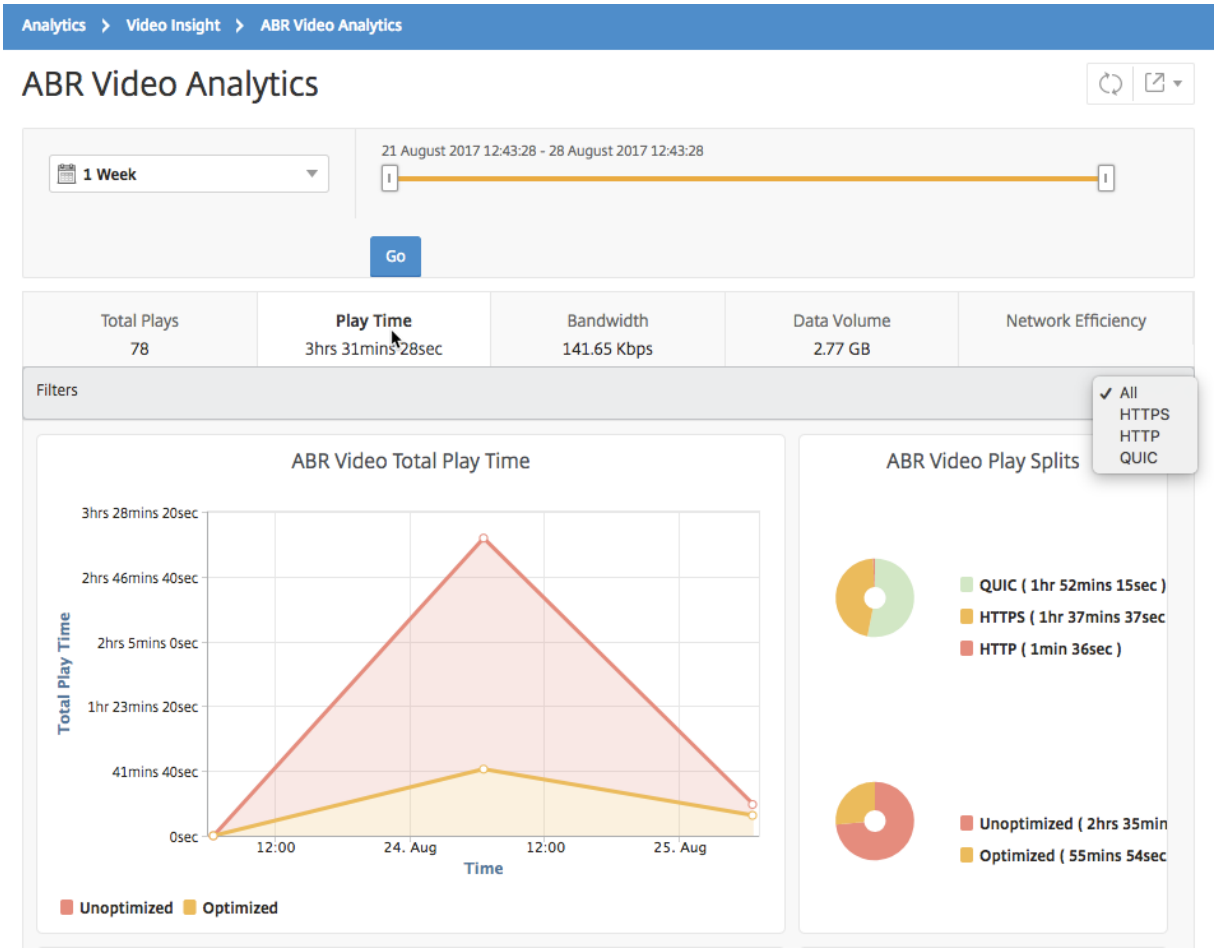
Für einen bestimmten Zeitraum liefert Citrix Application Delivery Management (ADM) die Wiedergabezeit von ABR-Videos und ermöglicht es Ihnen auch, die Wiedergabezeit optimierter und nicht optimierter ABR-Videos in Ihrem Netzwerk zu vergleichen.

Um die Spielzeit anzuzeigen, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video**. Wählen Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Wiedergabezeit**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

aus.

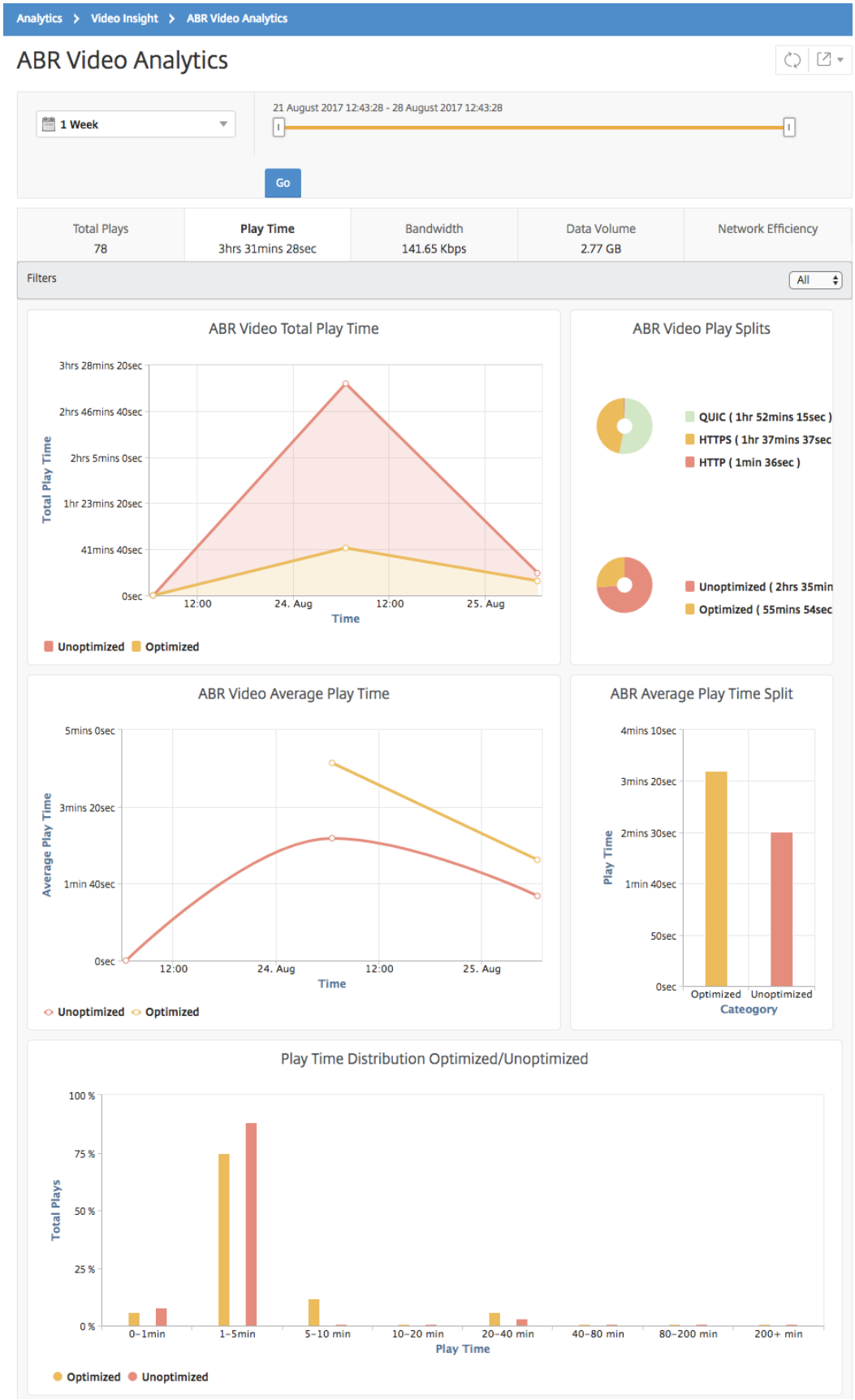
Sie können die Dropdownliste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



Für den ausgewählten Zeitraum enthält die Registerkarte **Wiedergabezeit** ein Liniendiagramm und ein Kreisdiagramm, in dem Folgendes beschrieben wird:

- Gesamte Wiedergabezeit von ABR-Videos aus Ihrem Netzwerk
- Gesamtspielzeit der optimierten und nicht optimierten Wiedergaben von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum.
- Gesamtspielzeit verschlüsselter und unverschlüsselter ABR-Videos.
- Durchschnittliche Wiedergabezeit von ABR-Videos
- Durchschnittliche Wiedergabezeit optimierter und nicht optimierter Wiedergaben von ABR-Videos
- Durchschnittliche Wiedergabezeit von verschlüsselten und unverschlüsselten ABR-Videos
- Wiedergabe der Zeitverteilung zwischen optimierten und nicht optimierten ABR-Videos

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Bandbreitenverbrauch optimierter und nicht optimierter ABR-Videos vergleichen

February 5, 2024

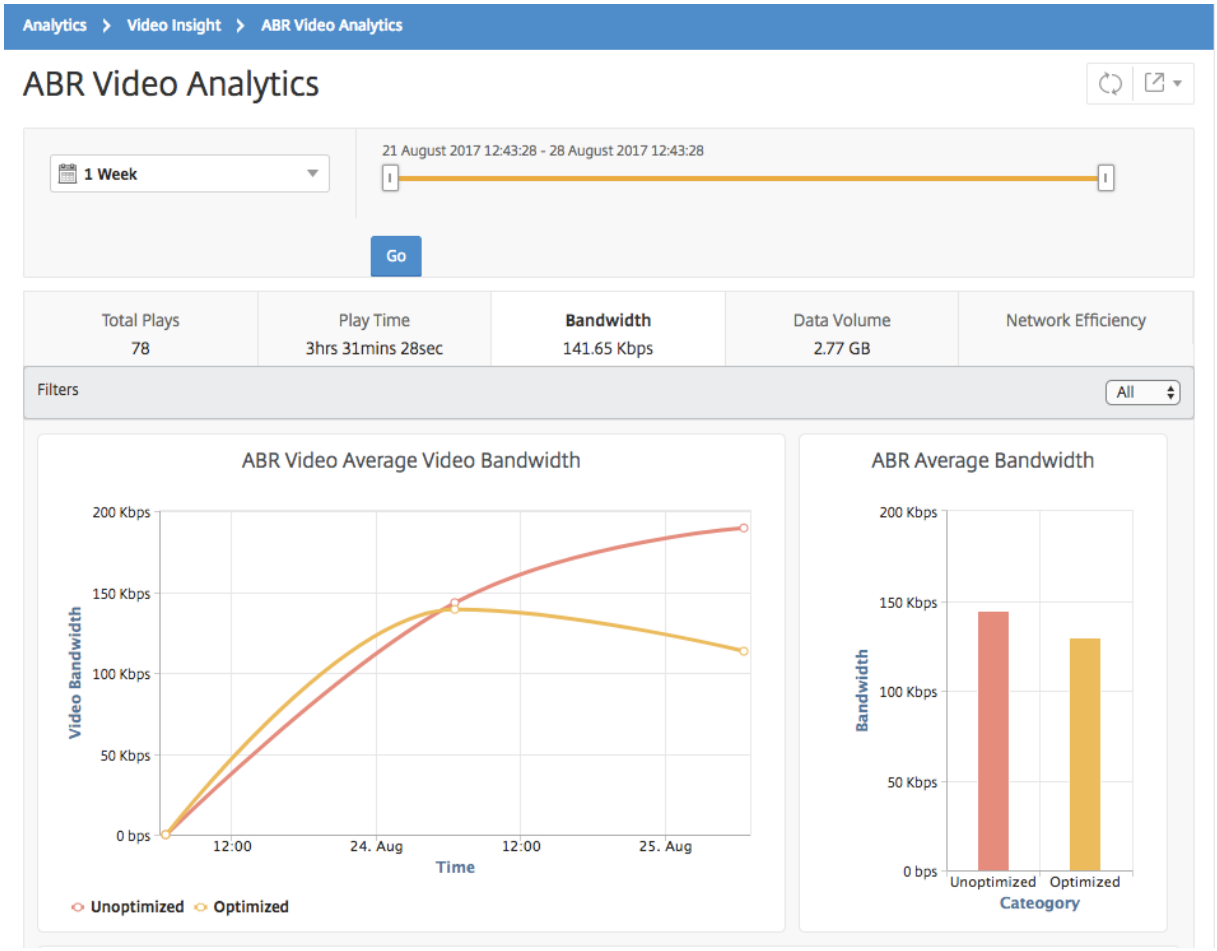
Für einen bestimmten Zeitraum bietet Citrix Application Delivery Management (ADM) die Bandbreite, die von optimierten und nicht optimierten ABR-Videos belegt wird. Außerdem können Sie die Bandbreite vergleichen, die von optimierten und nicht optimierten ABR-Videos in Ihrem Netzwerk belegt wird, basierend auf:

- Spielzeit
- Datenvolume

Um den Bandbreitenverbrauch anzuzeigen, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video Analytics**. Wählen Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Bandbreite** aus.

Sie können die Dropdownliste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC -ABR-Videos auszuwählen.

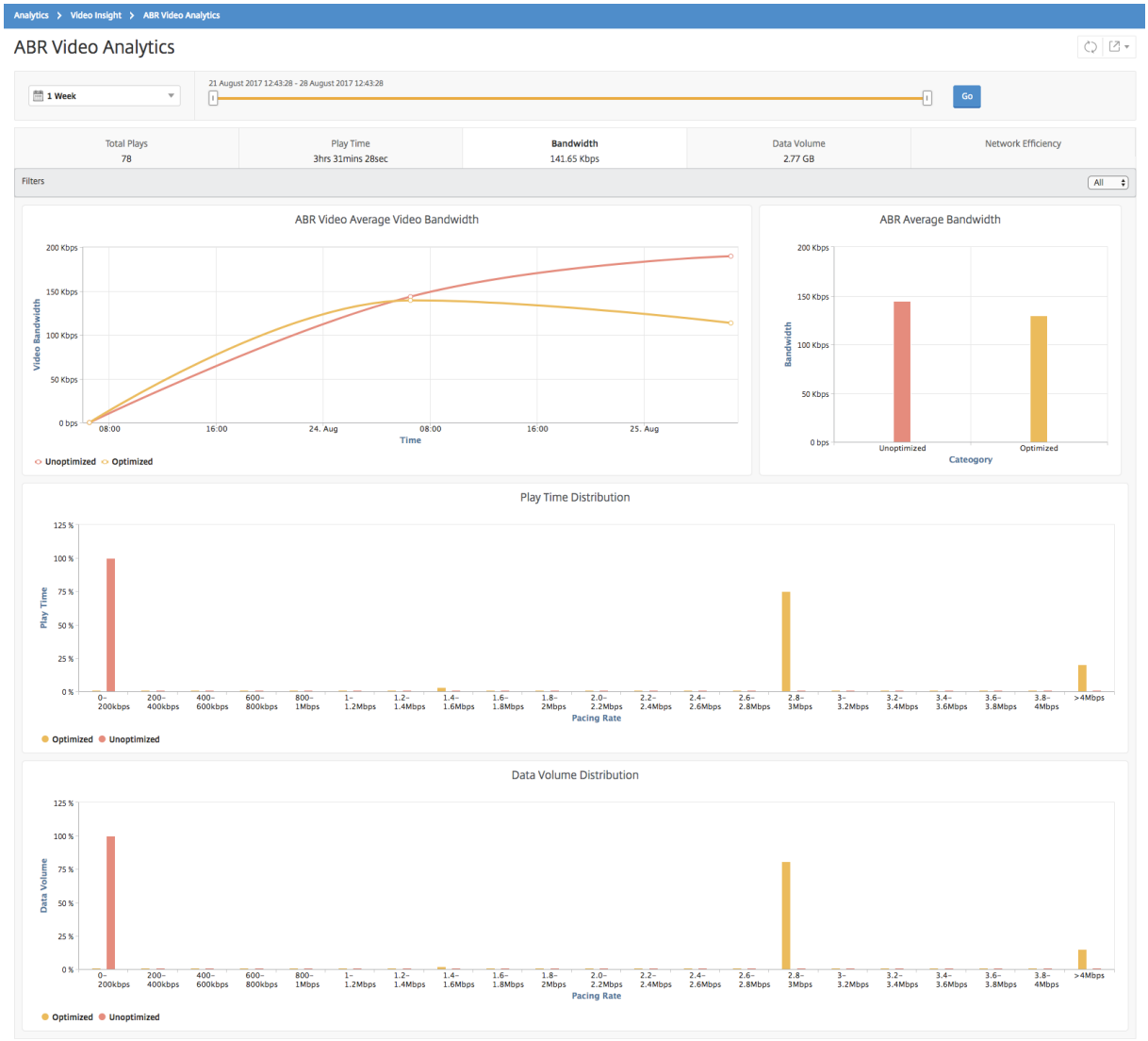
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Optimierte und nicht optimierte Wiedergabezahlen von ABR-Videos vergleichen

February 5, 2024

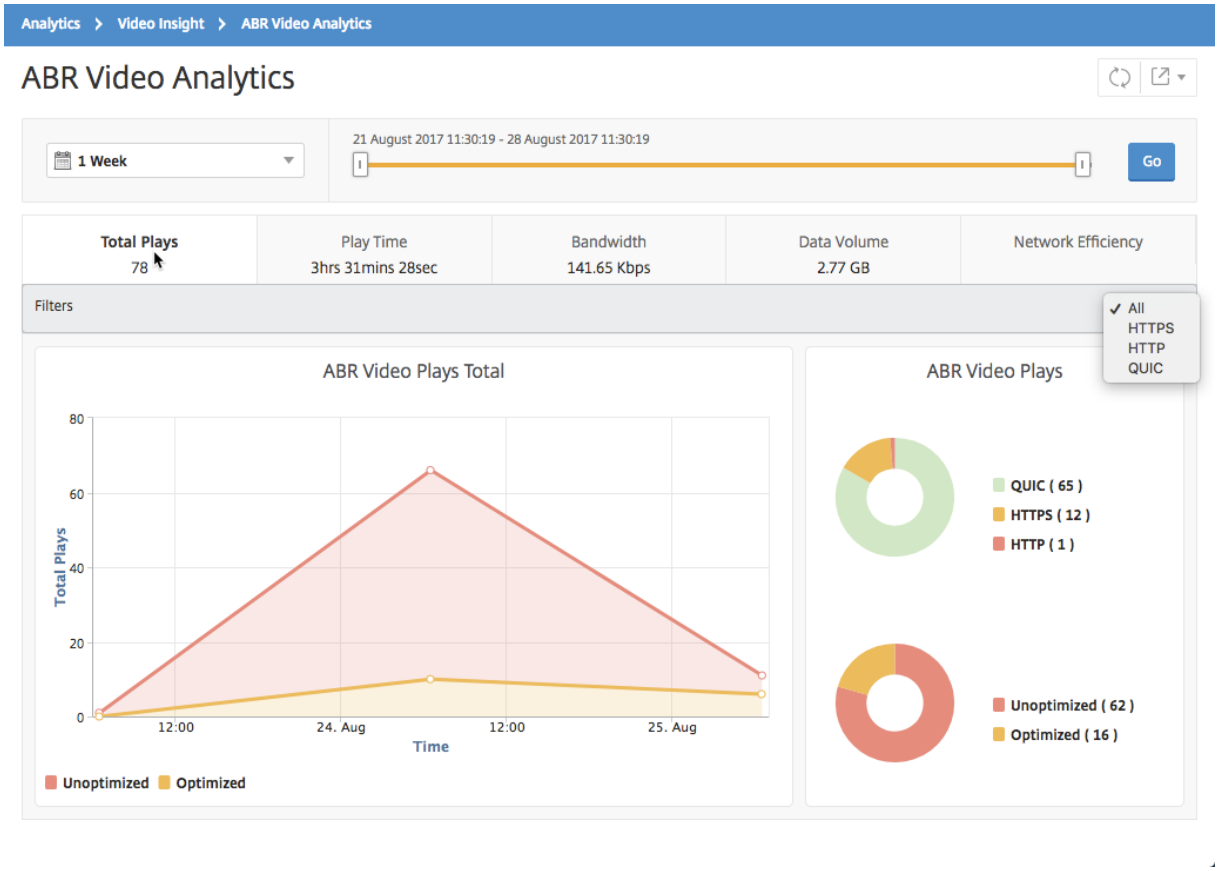
Für einen bestimmten Zeitraum zeigt NetScaler Application Delivery Management (ADM) die Anzahl der Abspielungen von ABR-Videos an und ermöglicht es Ihnen, die Anzahl der optimierten und nicht optimierten Wiedergaben in Ihrem Netzwerk zu vergleichen.

Um die Anzahl der Wiedergaben zu sehen, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **ABR Video Analytics**. Wählen Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

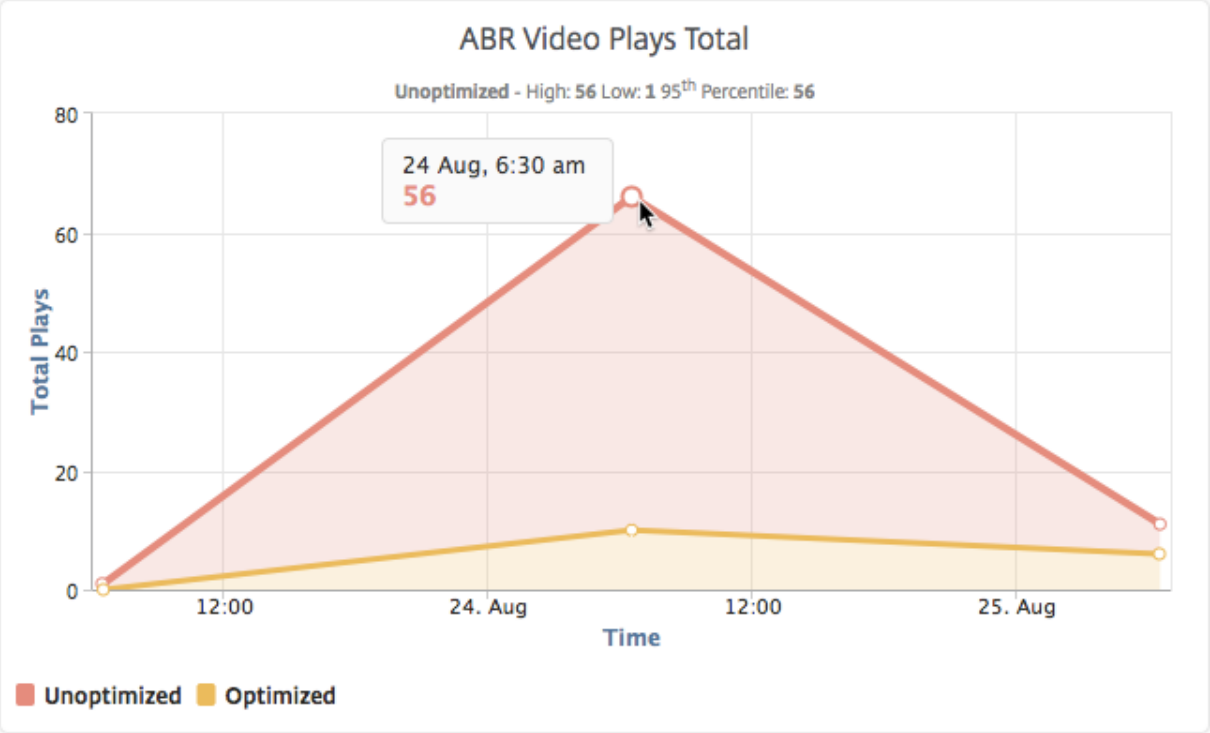
Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Los** und wählen Sie die Registerkarte **Anzahl der Wiedergaben**.

Sie können die Dropdownliste **Filter** verwenden, um die HTTP-, HTTPS- oder QUIC-ABR-Videos auszuwählen.



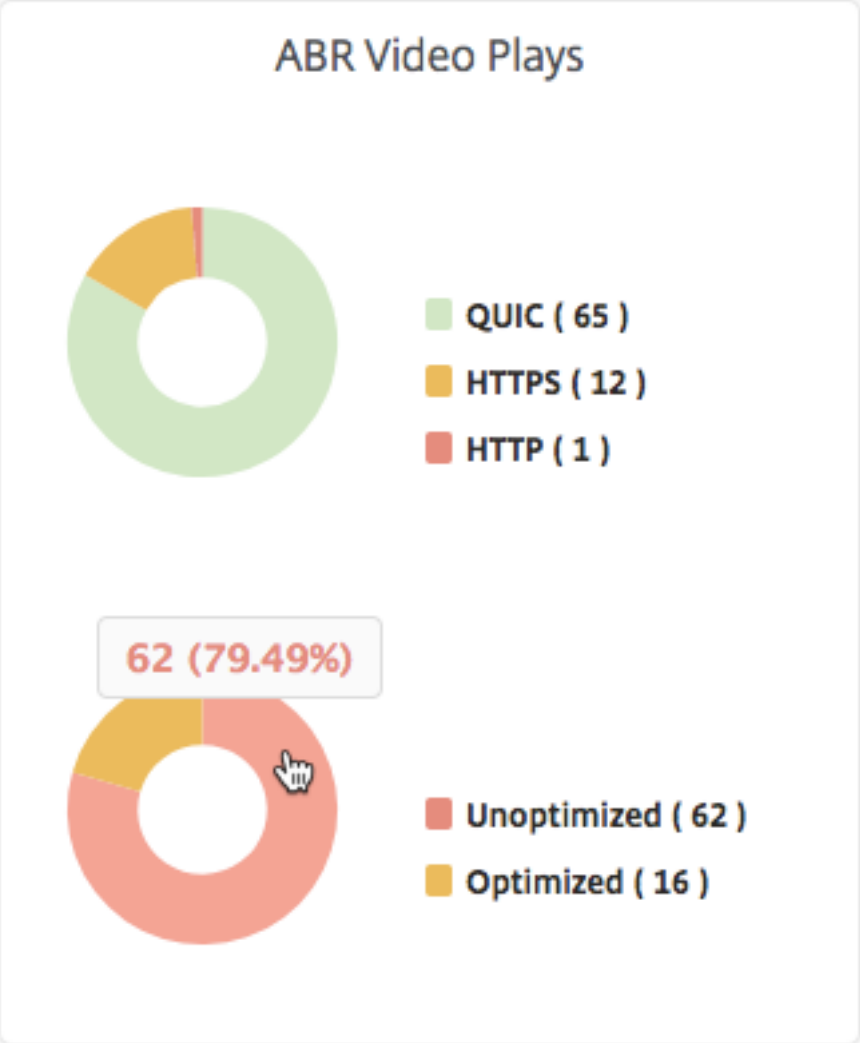
Die Registerkarte **Anzahl der Wiedergaben** enthält ein Liniendiagramm und ein Kreisdiagramm, das die Anzahl der Wiedergaben von ABR-Videos aus Ihrem Netzwerk sowie die Anzahl der optimierten und nicht optimierten Wiedergaben von ABR-Videos aus Ihrem Netzwerk für den ausgewählten Zeitraum beschreibt. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die Anzahl der Wiedergaben während eines bestimmten Zeitrahmens anzuzeigen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Spitzendatenrate für einen bestimmten Zeitraum anzeigen

February 5, 2024

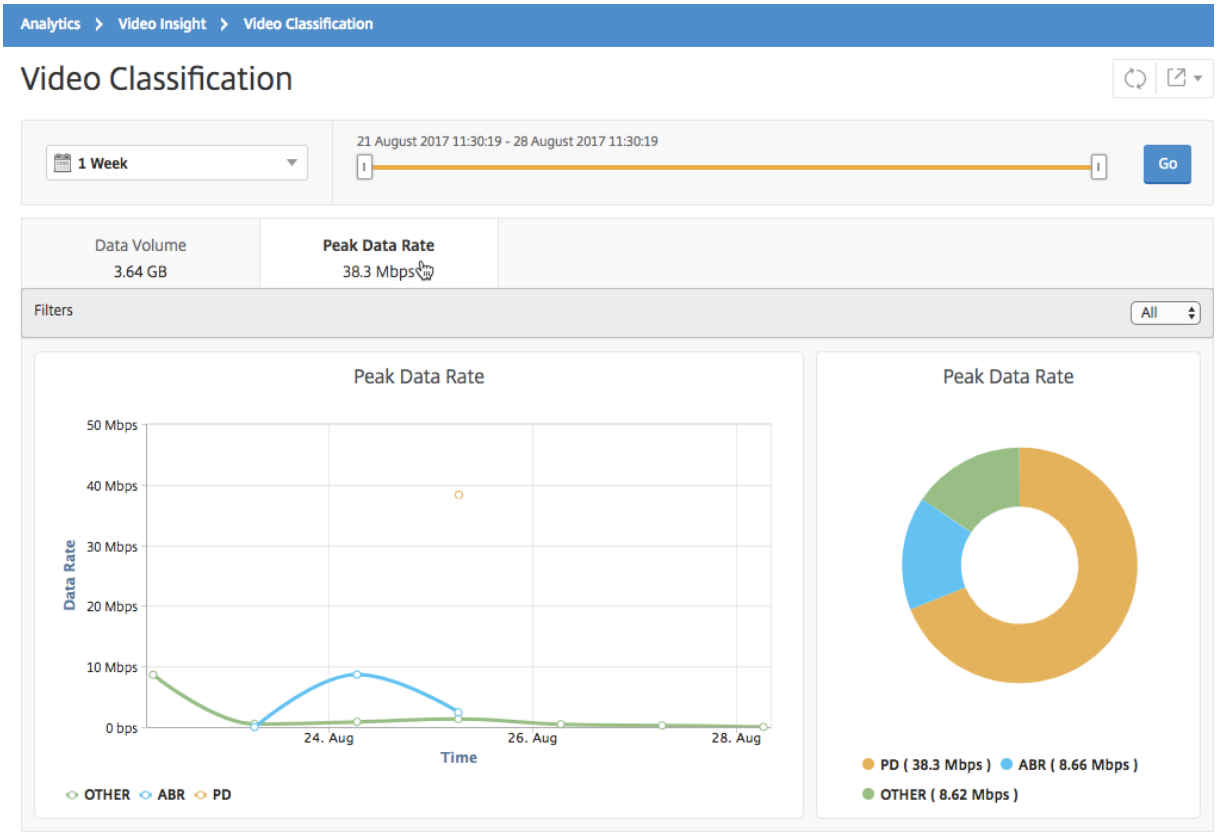
NetScaler Application Delivery Management (ADM) zeigt den Spitzendurchsatz oder die Datenrate des Videodatenverkehrs in Ihrem Netzwerk an.

Um die Spitzendatenrate des Videoverkehrs zu sehen, melden Sie sich bei Citrix ADM an, navigieren Sie zu **Analytics > Video Insight** und klicken Sie auf **Video Classification** . Wählen Sie dann im rechten Bereich einen Zeitrahmen aus der Dropdownliste aus. Sie können den Zeitrahmen weiter anpassen, indem Sie den Zeitrahmen-Schieberegler verwenden. Klicken Sie auf **Los**, und wählen Sie die Registerkarte **Spitzendatenrate** aus.

Sie können die Dropdownliste **Filter** verwenden, um den HTTP-, HTTPS- oder QUIC-Verkehr

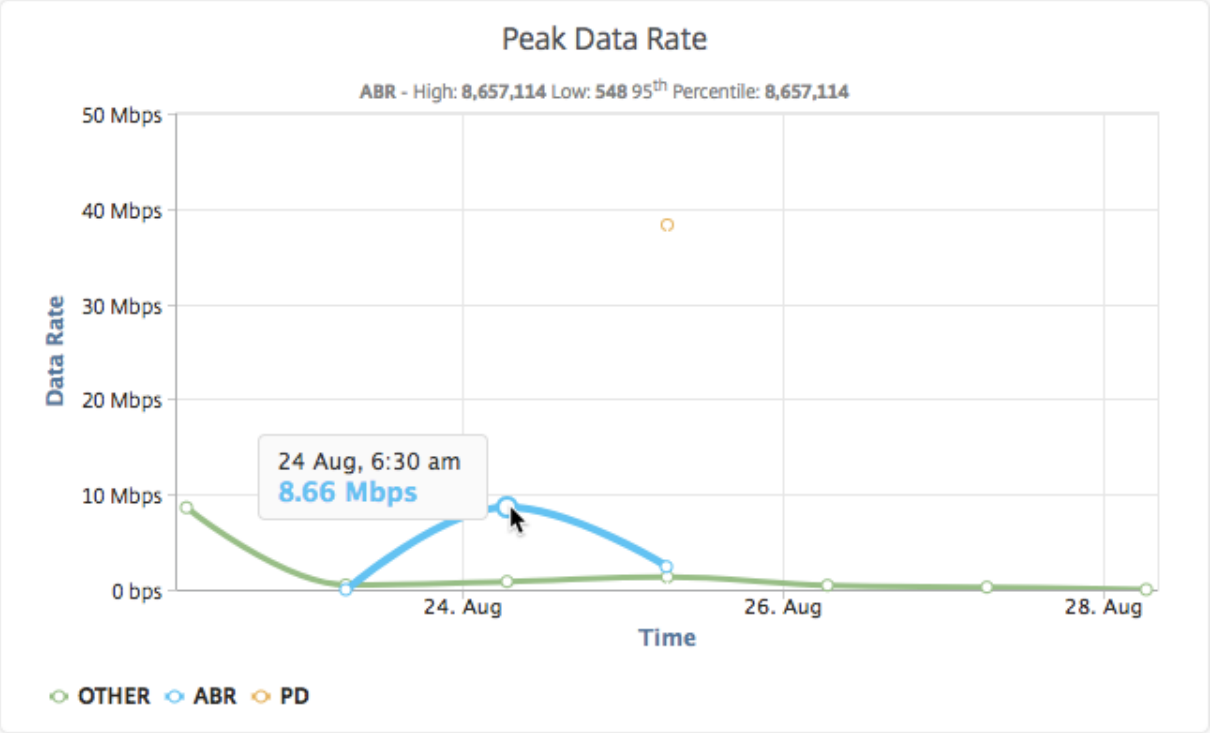
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

auszuwählen.



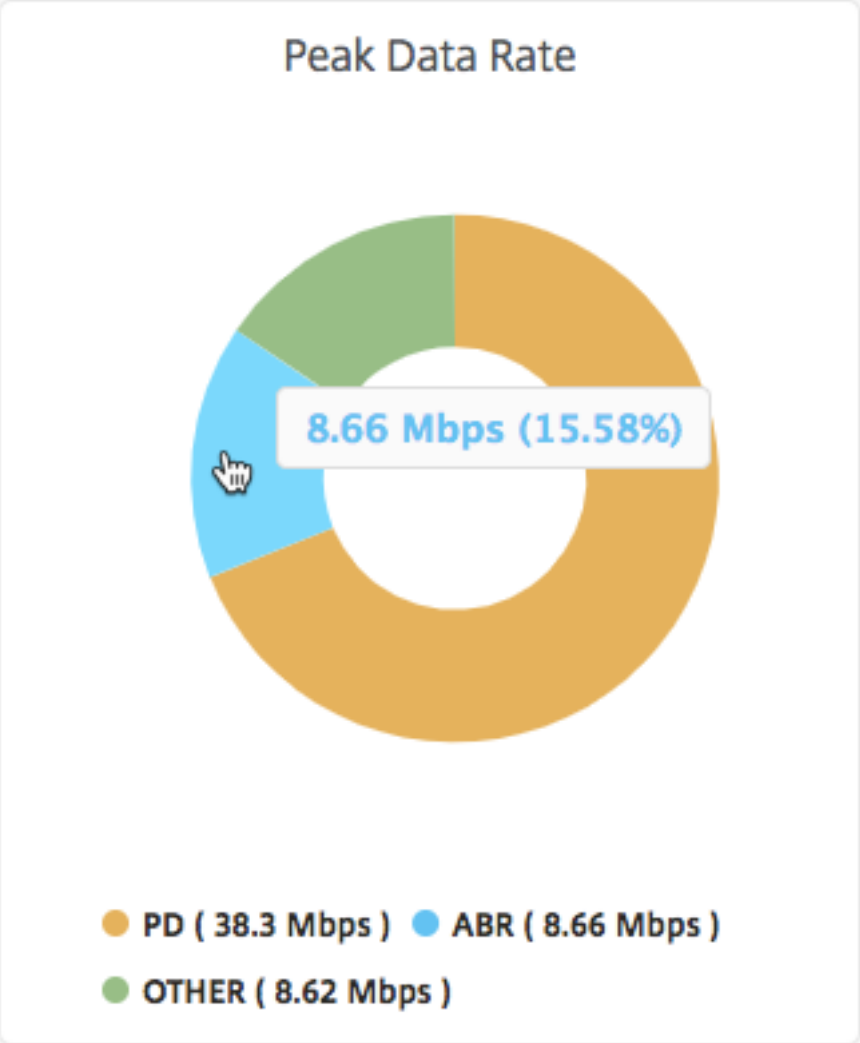
Die Registerkarte **Spitzendatenrate** enthält ein Liniendiagramm und ein Kreisdiagramm, das die Spitzendatenrate des vom Netzwerk ausgehenden Videodatenverkehrs und die Spitzendatenrate des Videodatenverkehrs im Netzwerk während des ausgewählten Zeitrahmens beschreibt. Sie können den Mauszeiger auf das Liniendiagramm bewegen, um die Spitzendatenrate während eines bestimmten Zeitrahmens anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Secure Web Gateway Analytics

February 5, 2024

Eine Citrix Secure Web Gateway (SWG) -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 Secure Web Gateway .

Wenn Sie das Citrix Application Delivery Management (ADM) in eine Citrix SWG-Appliance integrieren,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

werden die protokollierte Benutzeraktivität und die nachfolgenden Datensätze auf der Appliance mithilfe von Logstream in Citrix 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. Mit diesen Schlüsselmetriken können Sie Ihr Netzwerk überwachen und Korrekturmaßnahmen mit der Citrix SWG-Appliance durchführen.

So integrieren Sie eine Citrix SWG-Appliance in Citrix ADM:

1. Aktivieren Sie auf der Citrix SWG Appliance bei der Konfiguration des Secure Web Gateway **Analytics** und geben Sie die Details der Citrix ADM-Instanz an, die Sie für Analysen verwenden möchten.
2. Fügen Sie in NetScaler ADM die Citrix SWG-Appliance als Instanz zu NetScaler ADM hinzu. Weitere Informationen finden Sie unter Instanzen zu NetScaler ADM hinzufügen.

Dashboards

February 5, 2024

24. Mai 2018

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 Verkehr

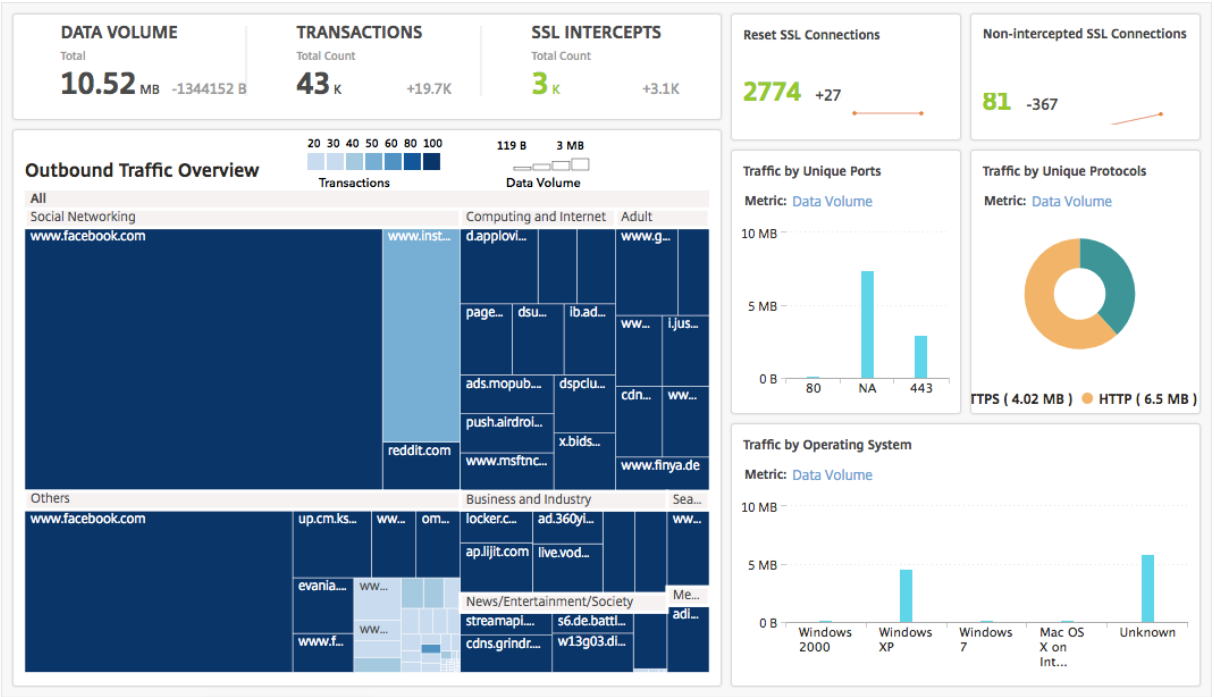
Das **Dashboard für ausgehenden Datenverkehr** enthält eine Zusammenfassung der URLs oder Domänen, auf die von Ihrem Netzwerk zugegriffen wird. Es bietet eine ganzheitliche Ansicht aller URLs oder Domänen nach Anzahl der Transaktionen oder Datenvolumen, die von den URLs oder Domains verbraucht werden.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Anzahl der SSL-Verbindungen, die von der Citrix SWG-Appliance während der Transaktionen abgefangen wurden.
4. Anzahl der SSL-Verbindungen, die während der Transaktionen nicht von der Citrix SWG-Appliance abgefangen wurden.
5. Anzahl der SSL-Verbindungen, die von der Citrix SWG-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**.

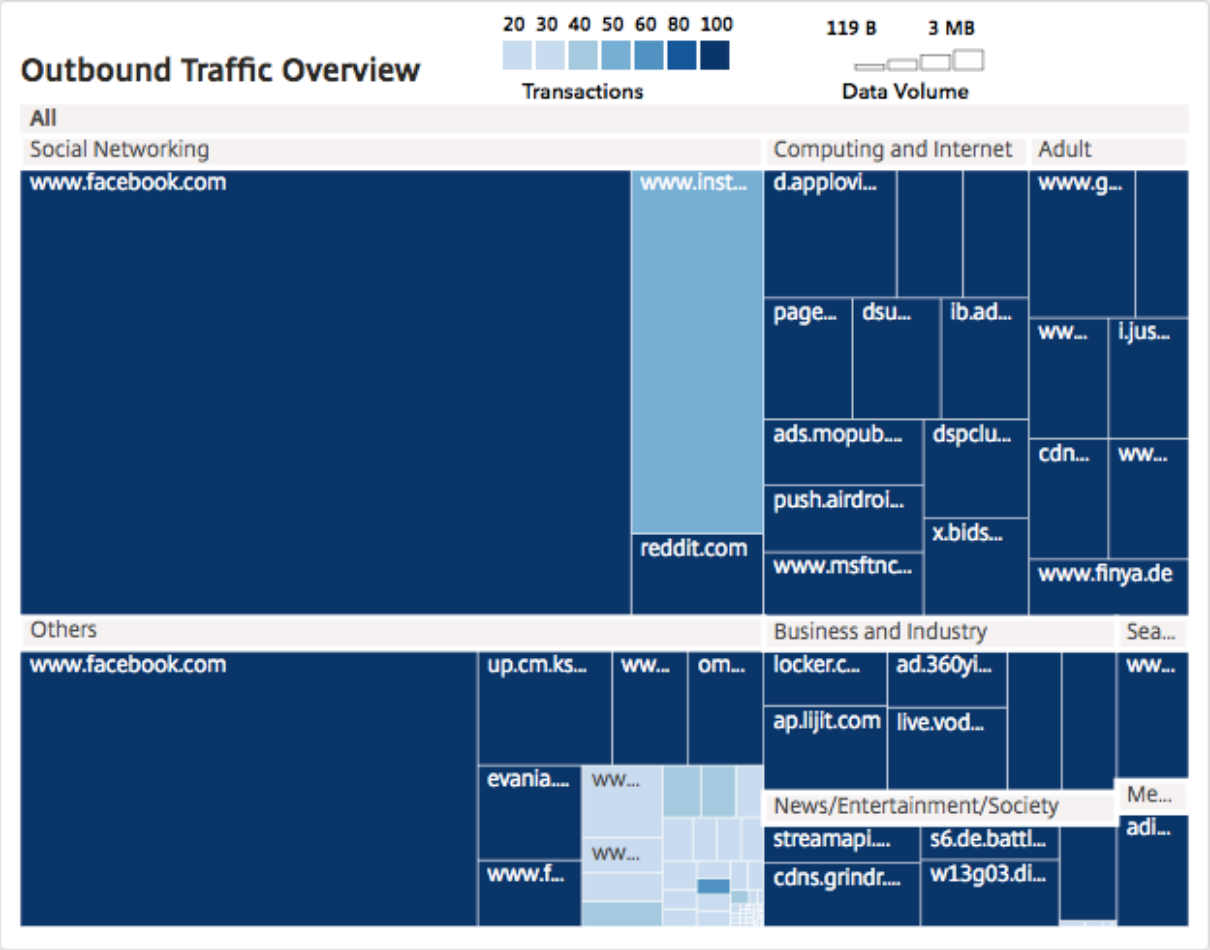


Den ausgehenden Verkehr aus dem Netzwerk anzeigen

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 und Details zur Kategorie für den angegebenen Zeitraum anzuzeigen.

Benutzer-Dashboard

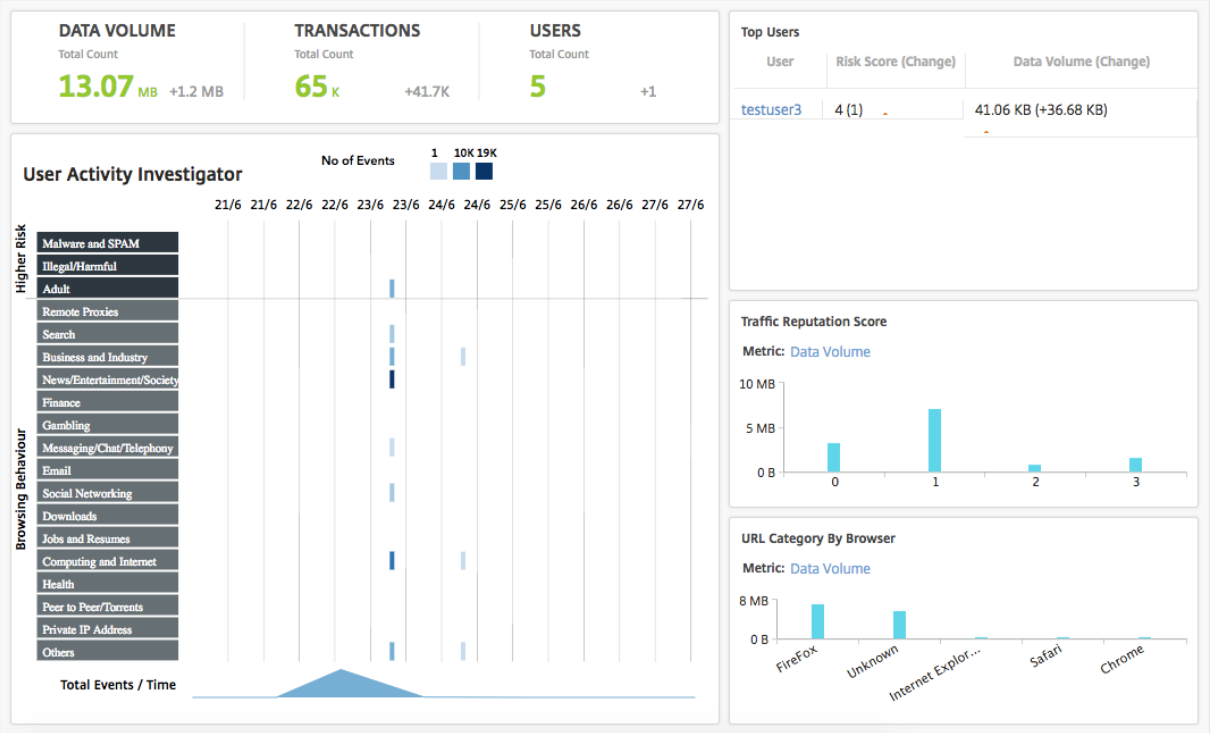
Das **Benutzerdashboard** zeigt eine Zusammenfassung der Aktivitäten an, die von den Benutzern in Ihrem Unternehmen ausgeführt werden. Es enthält wichtige Metriken, anhand derer Sie Folgendes ermitteln können:

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.



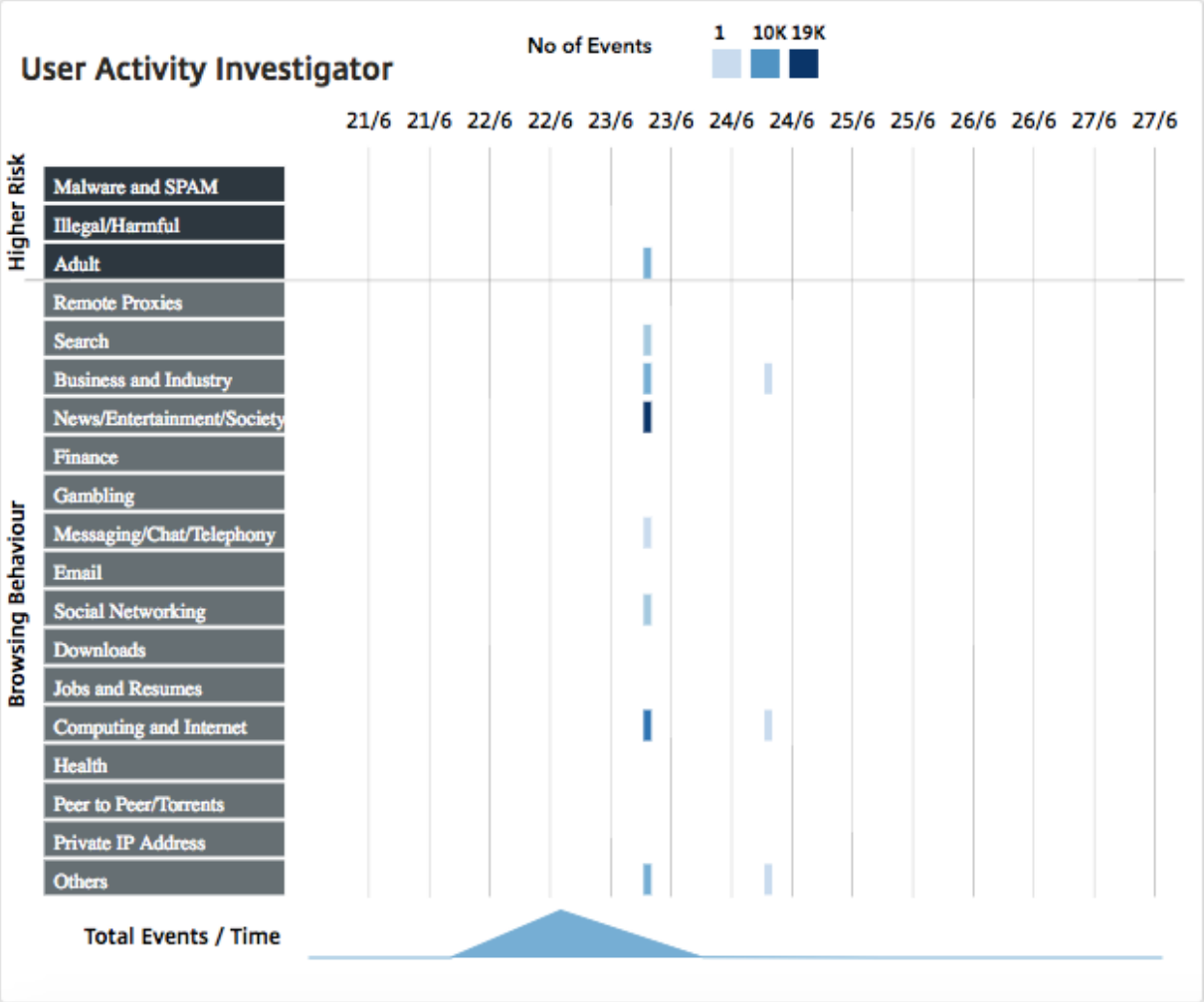
Sie können im Bereich **Top-Benutzer auf einen Benutzer** klicken, um die Diagramme so zu filtern, dass Details der Webaktivitäten angezeigt werden, die der Benutzer im angegebenen Zeitraum ausgeführt hat.

Ermittler für Benutzeraktivitäten

Das **Benutzer-Dashboard** enthält einen Bereich **Ermittlungsprogramm**, in dem verschiedene Webaktivitäten angezeigt werden, die von den Benutzern ausgeführt werden. Es zeigt die URL-Kategorien, auf die die Benutzer während des ausgewählten Zeitrahmens zugreifen, und verschiedene Ereignisse, die pro URL-Kategorie ausgelöst werden. Sie können auf die Ereignisse klicken, um die Details auf Transaktionsebene abzurufen.

Der **User Activity Investigator** zeigt wichtige Informationen wie das Browserverhalten des Benutzers, die Aktivität mit hohem Risiko des Benutzers und die ausgelösten Ereignisse pro URL-Kategorie an. Die Ereignisse werden 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 im Dropdownmenü Zeitraum eine Zeit auswählen.

Sie können auf die Ereignisse klicken, um weitere Informationen zu den Transaktionen zu erhalten.

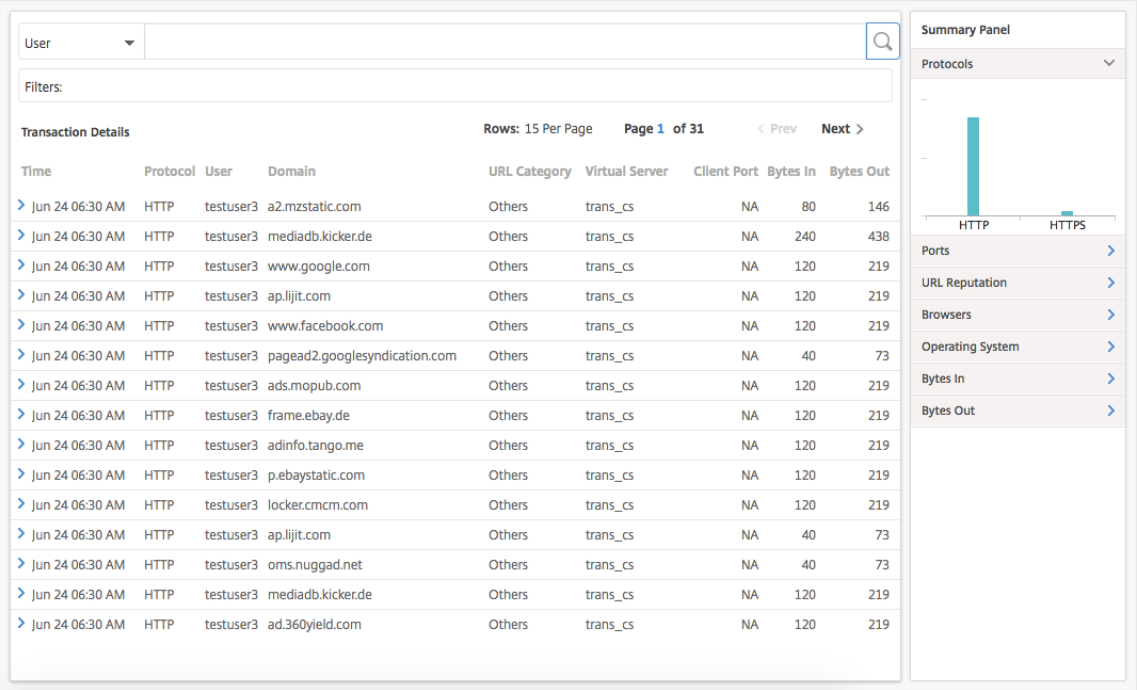
Benutzertransaktionen

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Domain, auf die der Benutzer zugegriffen hat
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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metriken	Beschreibung
Betriebssystem	Für die Transaktionen verwendetes Betriebssystem
Bytes In	Datenmenge, die über die Citrix SWG-Appliance empfangen wurde.
Bytes aus	Datenmenge, die über die Citrix SWG-Appliance gesendet wurde.

Risikobewertung

Risk Score ist ein Bewertungssystem, das in NetScaler ADM verwendet wird, um die Risiken zu ermitteln, die mit Benutzern in Ihrem Unternehmen verbunden sind. Citrix ADM weist eine Risikobewertung zu, die auf der URL-Reputationsbewertung basiert, die von der Citrix SWG-Appliance für die URLs zugewiesen wurde, auf die die Benutzer in Ihrem 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Anwendungsfälle

February 5, 2024

Überwachung der SSL-Interceptions

Mit einer Citrix SWG-Appliance können Sie Ihren verschlüsselten ausgehenden Verkehr überprüfen. Sie können alle HTTPS-Anfragen auf der Grundlage der 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:

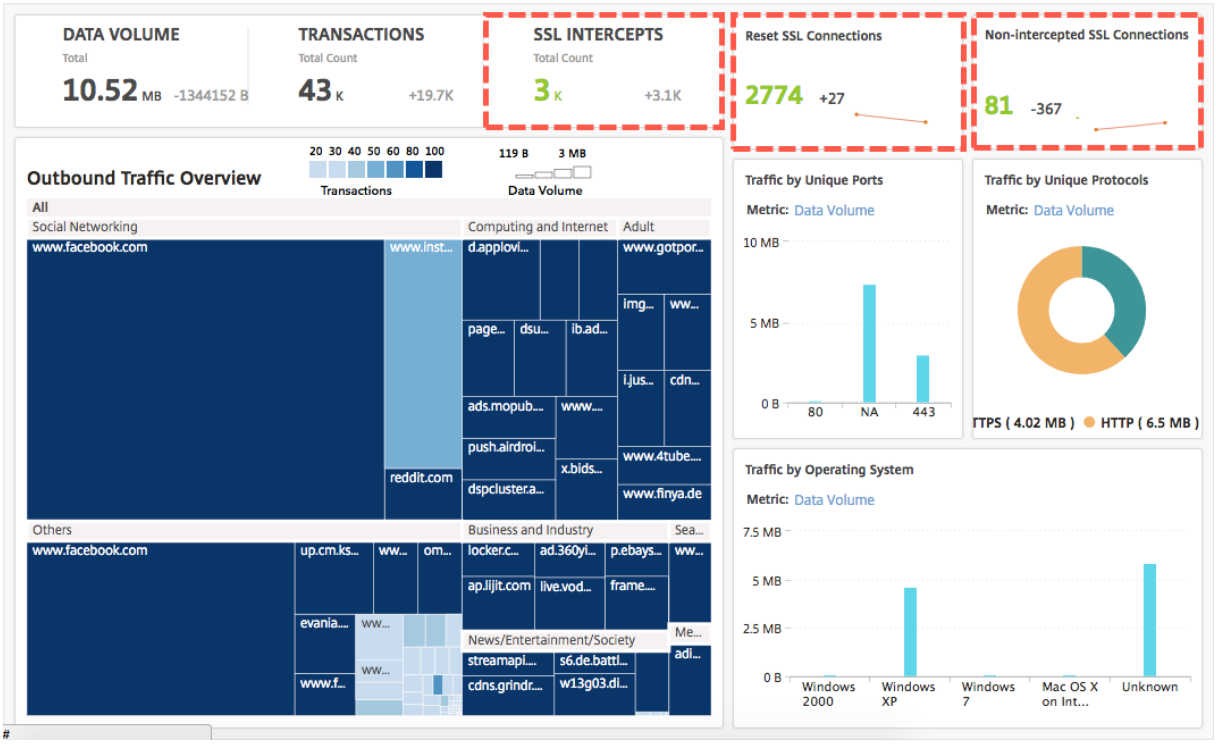
- Anzahl der SSL-Verbindungen, die von der Citrix SWG-Appliance abgefangen, nicht abgefangen und zurückgesetzt werden
- Transaktionsdetails der SSL-Verbindungen

Mithilfe dieser Details können Sie die Richtlinien auf Ihrer Citrix SWG-Appliance weiter optimieren, um den verschlüsselten ausgehenden Verkehr effizient zu überprüfen. Weitere Informationen finden Sie unter Citrix Secure Web Gateway .

So zeigen Sie die Anzahl der SSL-Verbindungen an, die abgefangen, nicht abgefangen und zurückgesetzt wurden:

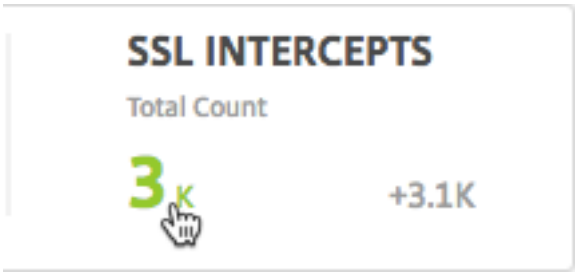
Navigieren Sie zu **Anwendungen > Dashboard für ausgehenden Datenverkehr**.Das Outboard Traffic Dashboard zeigt die Anzahl der SSL-Verbindungen an, die abgefangen, nicht abgefangen und zurückgesetzt werden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



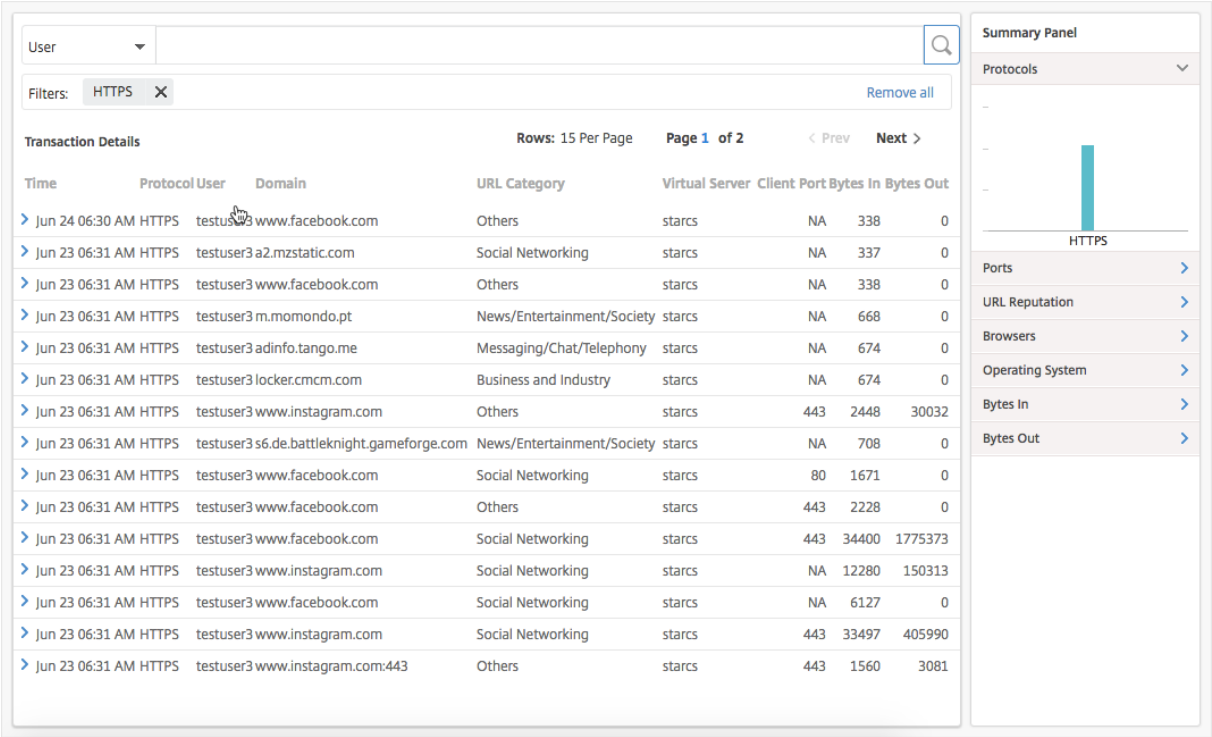
So zeigen Sie die Transaktionsdetails der abgefangenen SSL-Verbindungen an:

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



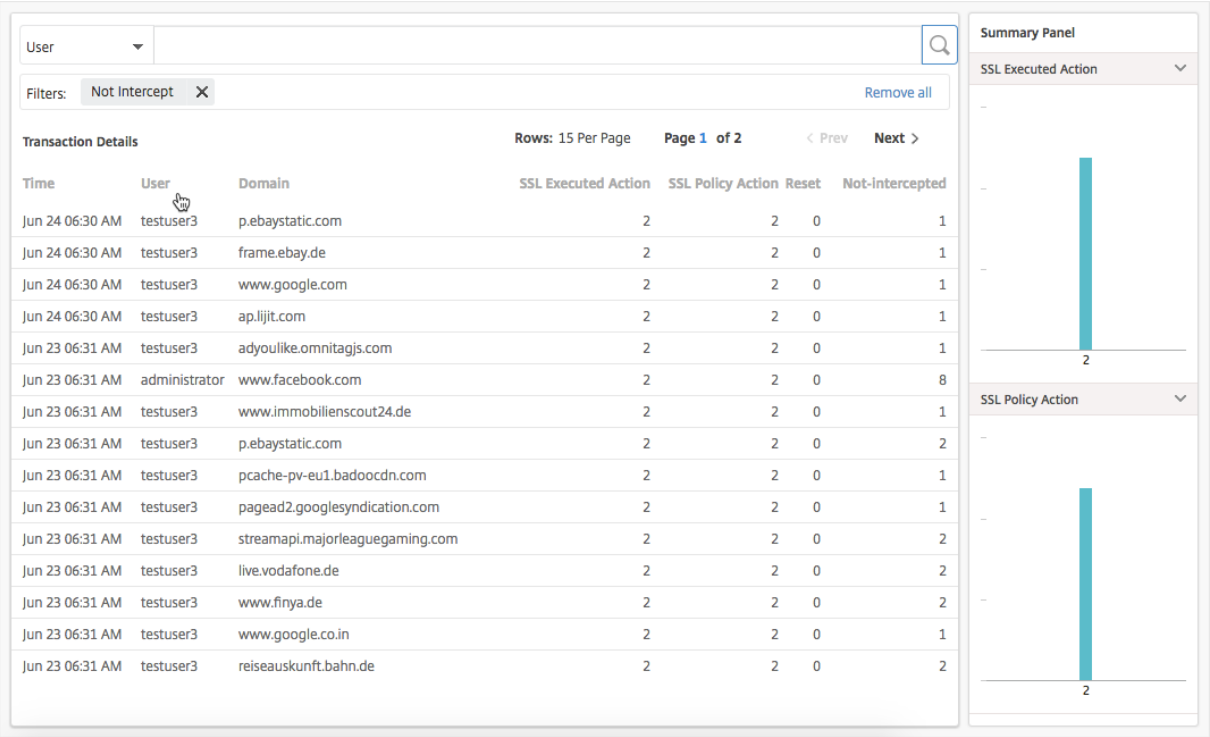
Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



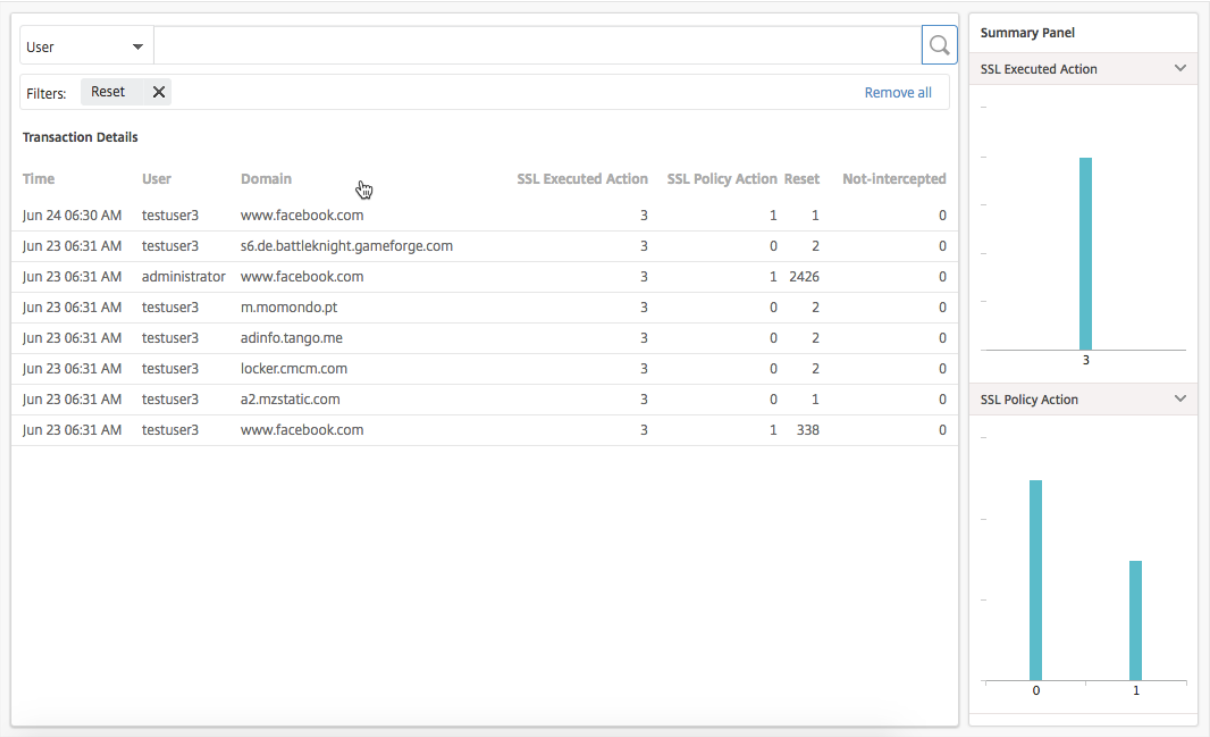
Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Sie können die Transaktionsdetails weiter nach Benutzer und URL-Kategorie filtern.

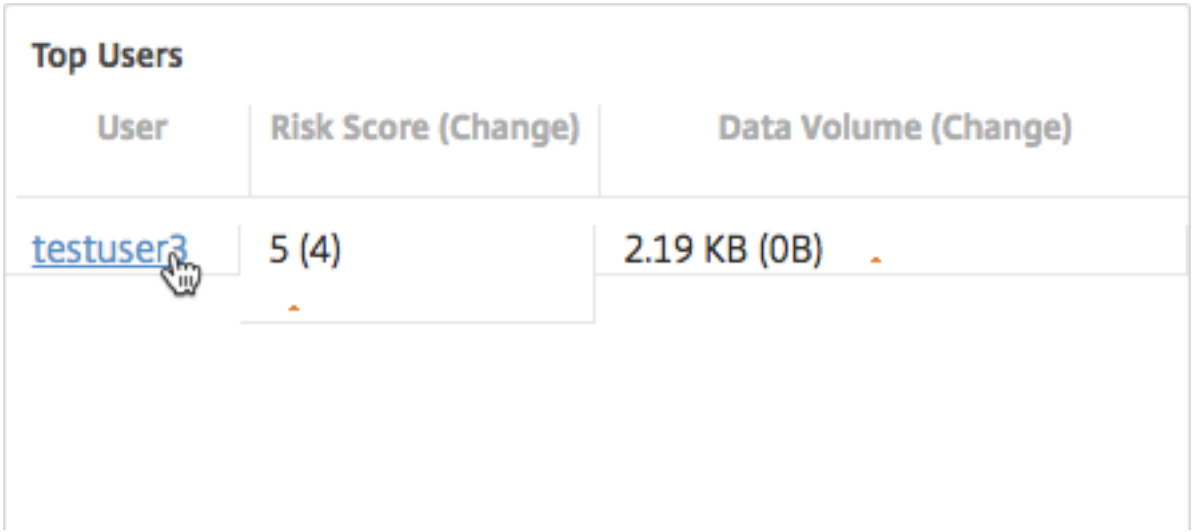
Endpunkte überprüfen

Die Richtlinien, die Sie auf einer Citrix SWG-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:

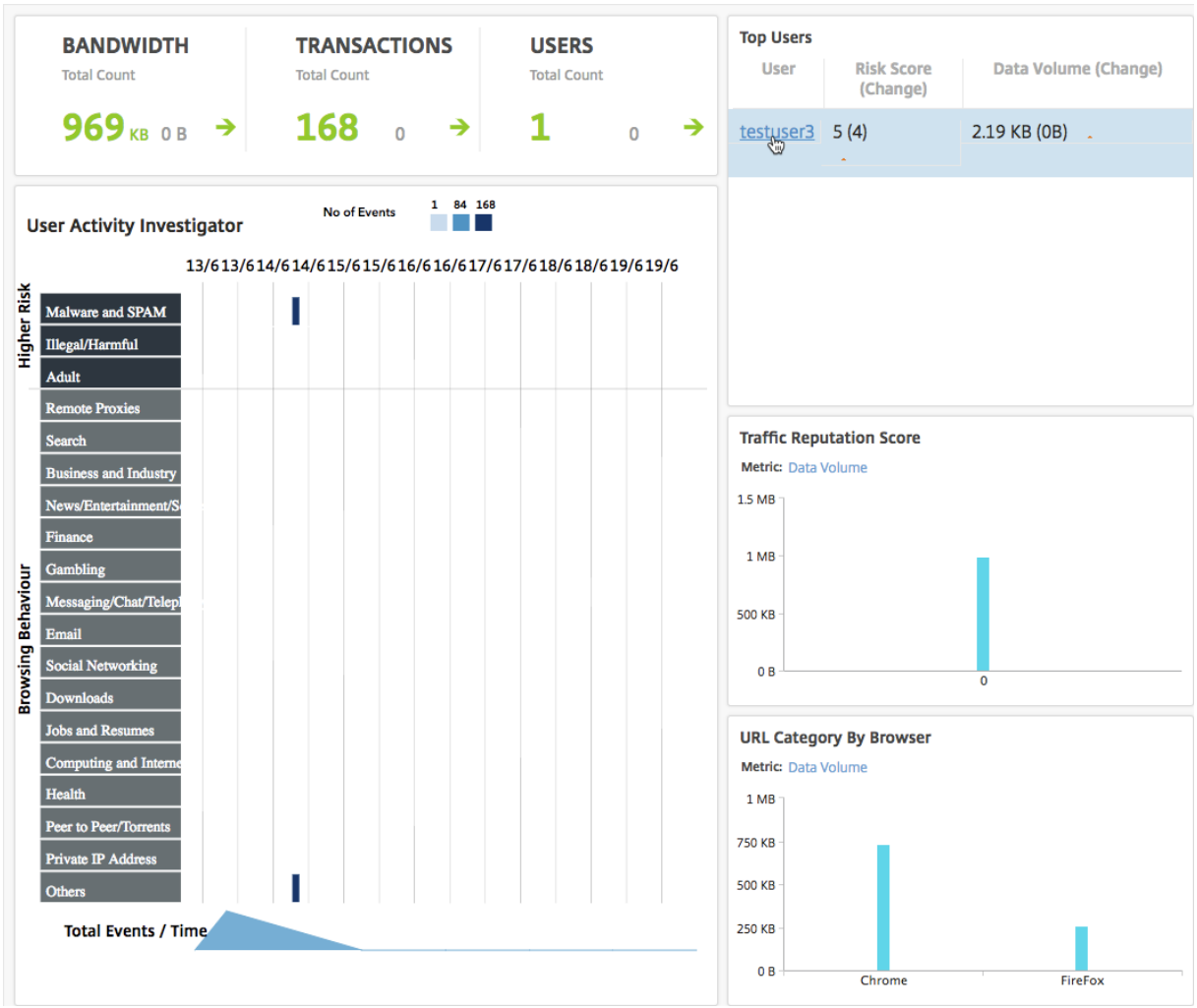
1. Das Surfverhalten der Benutzer in Ihrem Unternehmen.
2. URL-Kategorien, auf die die Benutzer in Ihrem Unternehmen zugreifen.
3. Die fünf besten Benutzer, basierend auf ihren Risikobewertungen und der Bandbreite, die sie verbrauchen. Weitere Informationen zu Risikobewertungen finden Sie unter Risikobewertung.
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 der Benutzer-ID testuser3 ständig auf Websites im Zusammenhang mit Malware 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

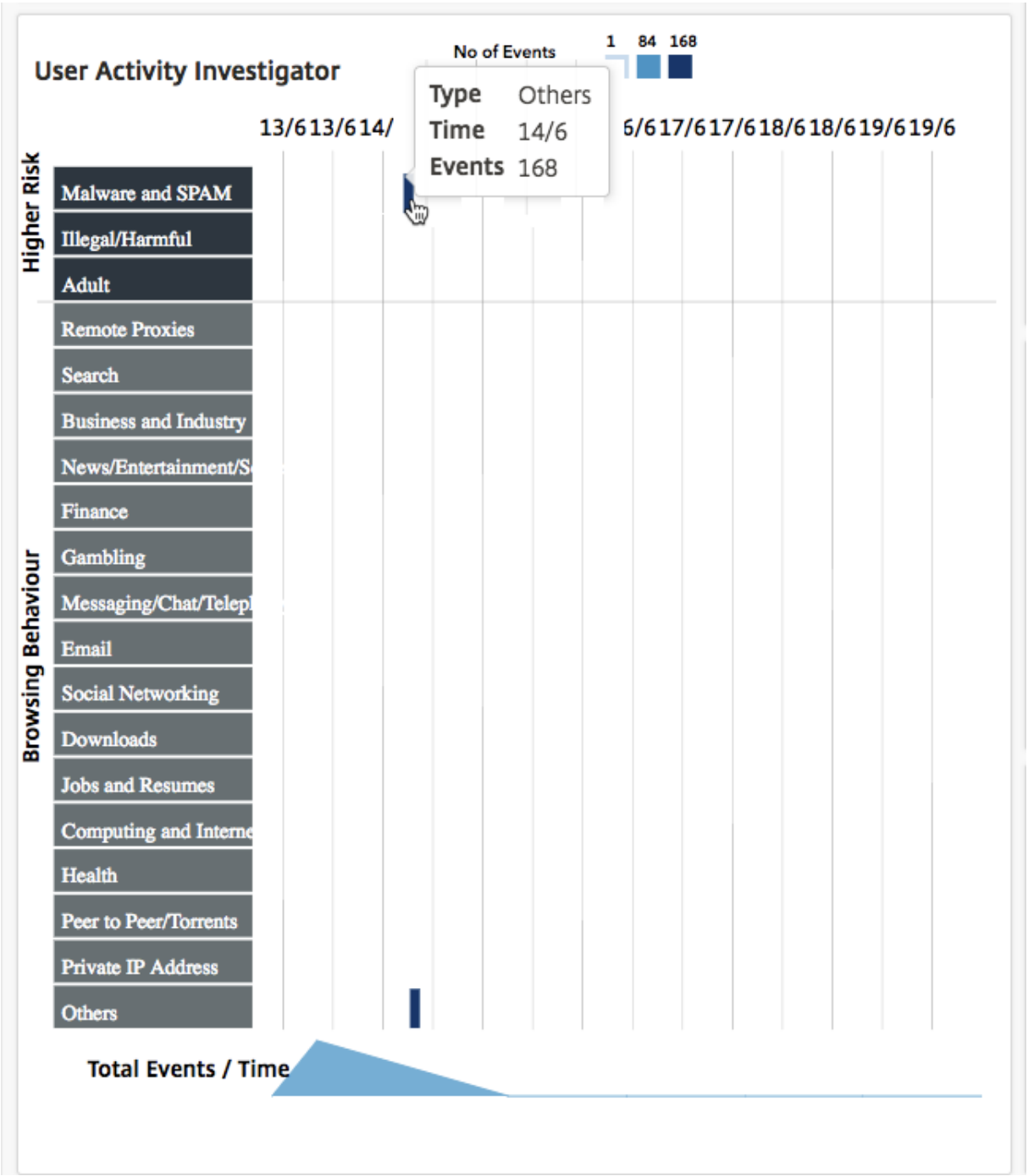


Sie können auf testuser3 klicken, um das **Benutzer-Dashboard** so zu filtern, dass alle wichtigen Metriken zu testuser3 angezeigt werden.



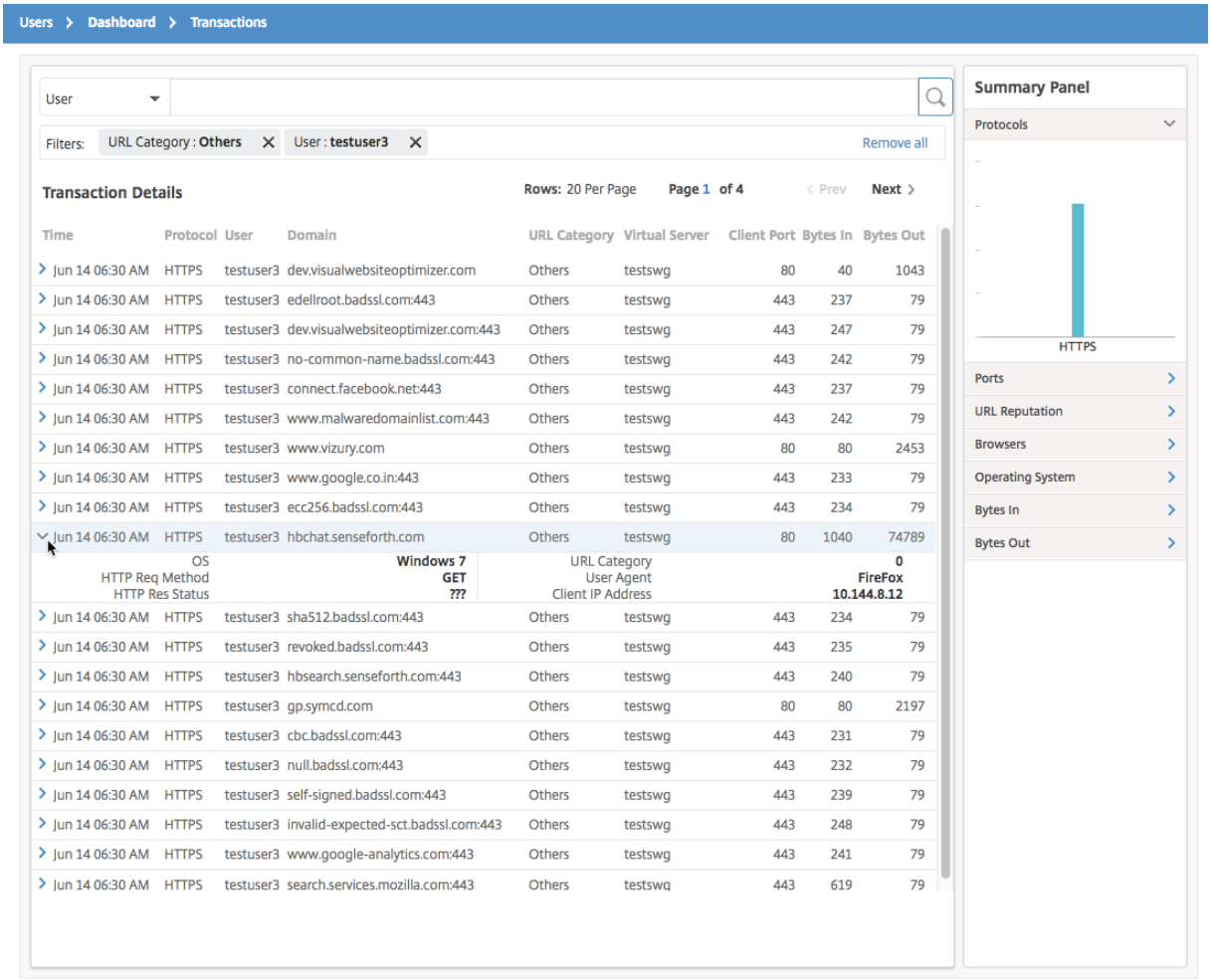
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 stattgefunden haben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



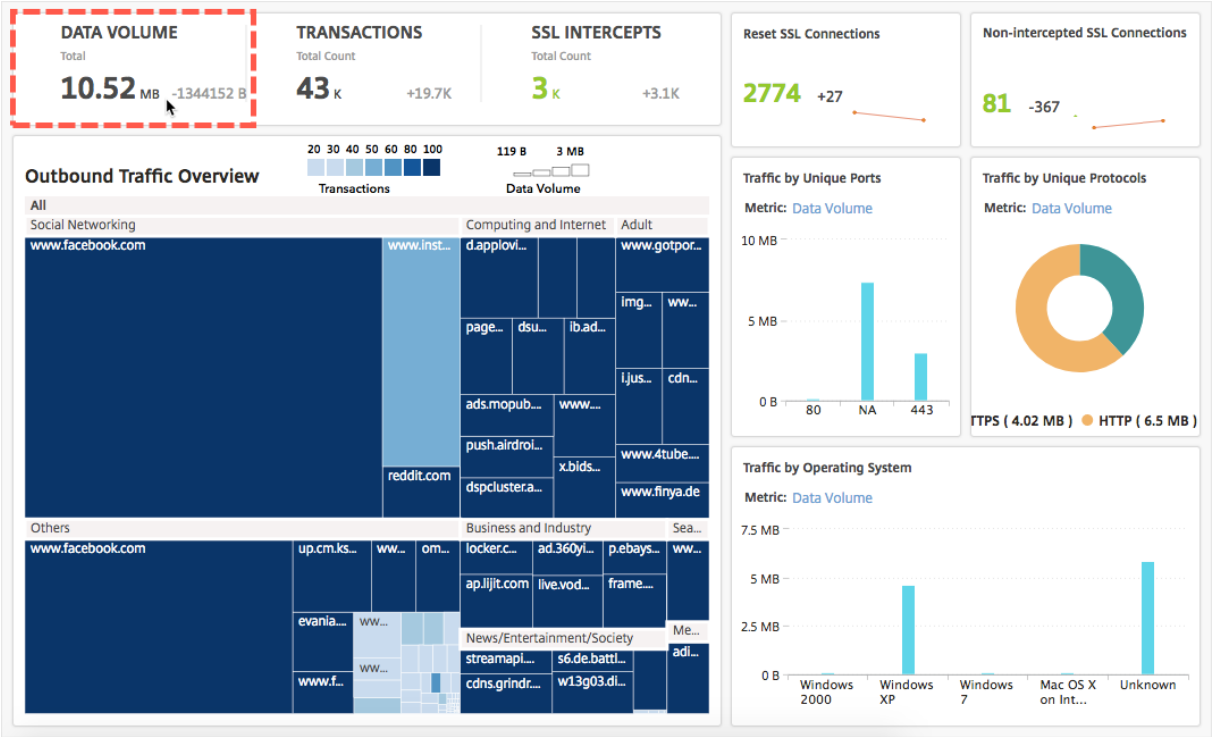
Anhand dieser Informationen können Sie feststellen, ob das System des Benutzers mit Malware infiziert ist, oder Sie können das Bandbreitenverbrauchsmuster des Benutzers verstehen und Ihre Citrix SWG-Richtlinien optimieren. Weitere Informationen finden Sie in der Citrix Secure Web Gateway-Dokumentation .

Berichterstattung über den Bandbreitenverbrauch

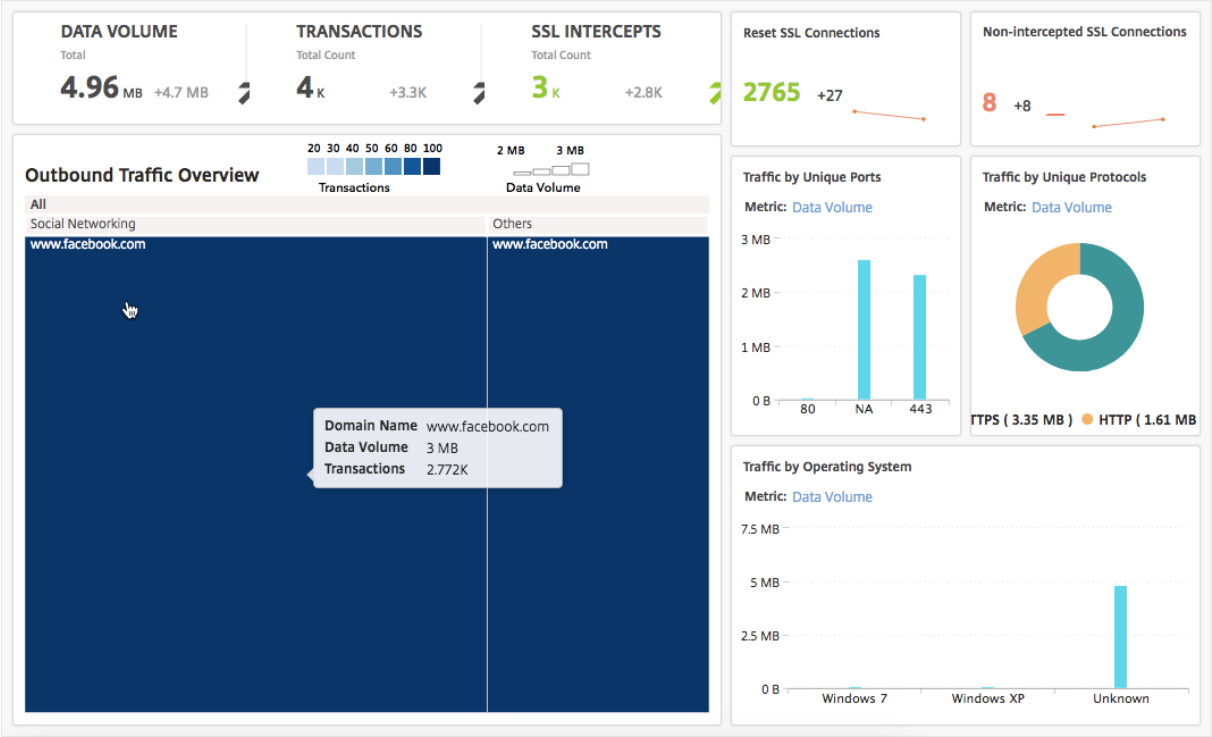
Das **Dashboard für ausgehenden Datenverkehr** und das **Benutzerdashboard** stellen mehrere Diagramme bereit, in denen die Websites oder Anwendungen zusammengefasst werden, auf die vom Unternehmensnetzwerk zugegriffen wird, sowie die Aktivitäten, die von den Benutzern im Netzwerk ausgeführt werden.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



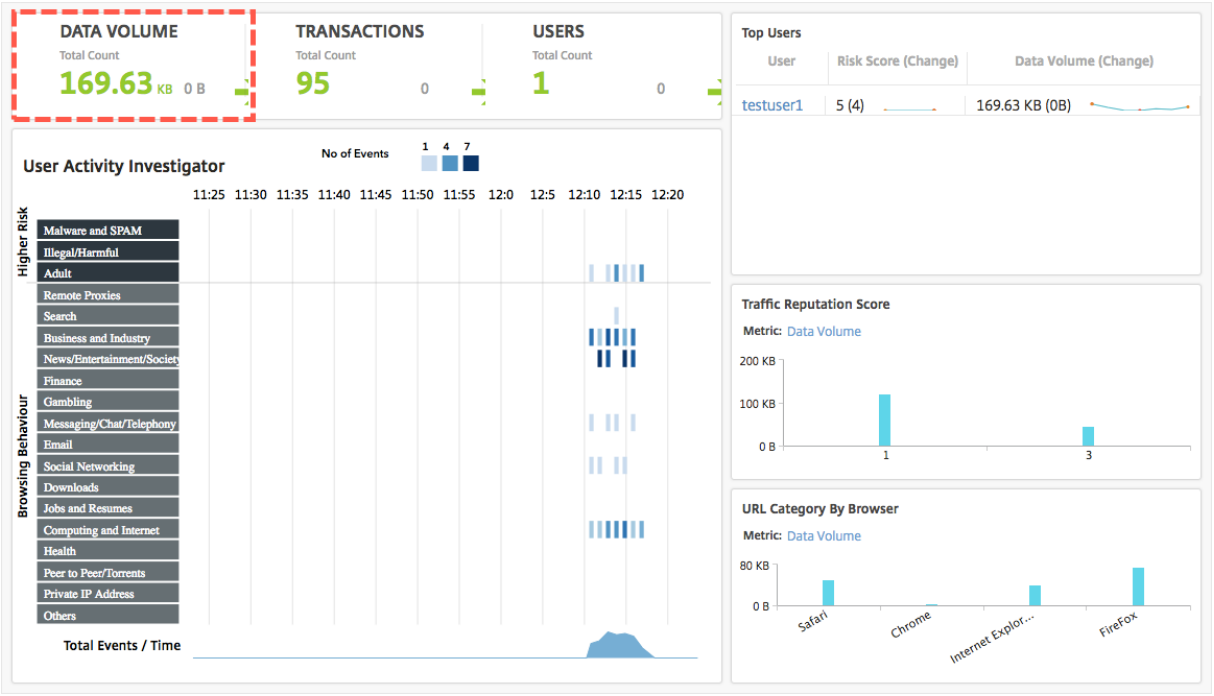
Im Bereich Übersicht über den ausgehenden **Traffic** können Sie auf eine Domain oder URL klicken, um die Details des von der Domain oder URL verbrauchten Datenvolumens anzuzeigen.



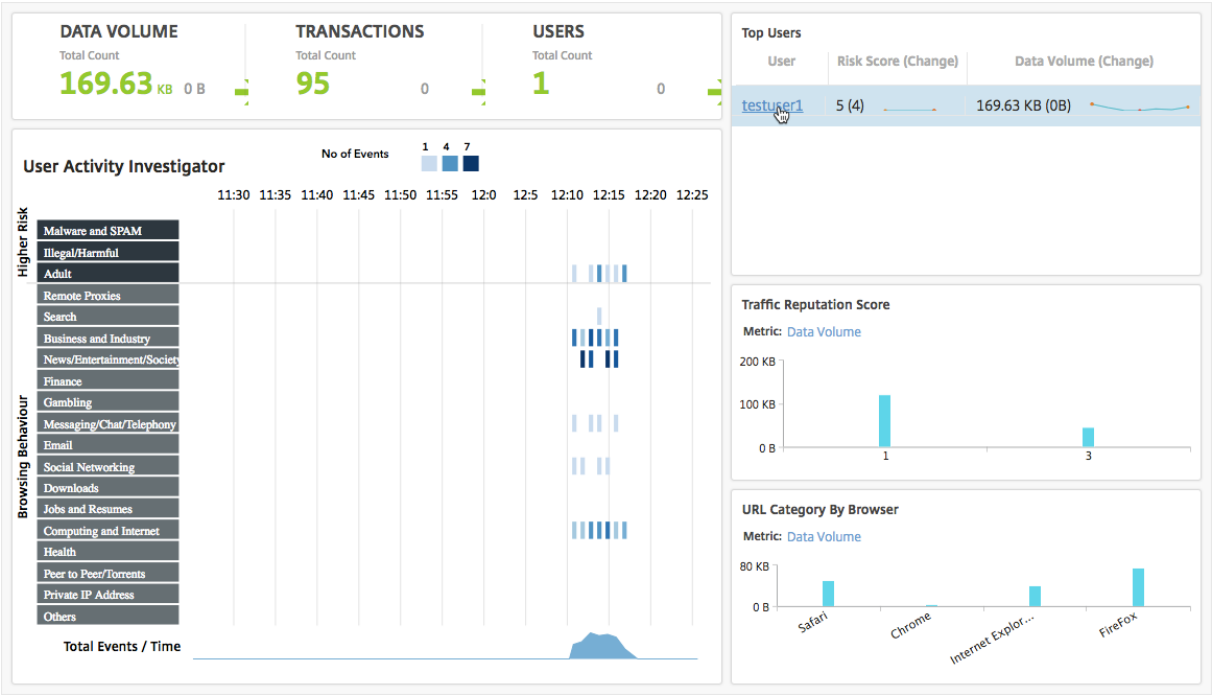
Das **Benutzerdashboard** enthält Details zur Bandbreite, die von den Benutzern in Ihrem Netzwerk belegt wird. Navigieren Sie zu **Benutzer > Dashboard**, um die Details der von Benutzern verbrauchten

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 verstehen. Wenn ein Benutzer beispielsweise auf Websites sozialer Netzwerke zugreift und dies zu einem

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

hohen Bandbreitenverbrauch geführt hat, kann der Administrator auf die Citrix SWG-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 Citrix SWG-Appliance bietet URL-Kategorisierungs- und Filterfunktionen, mit denen Sie die URLs kategorisieren können, auf die von Ihrem Netzwerk aus 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:

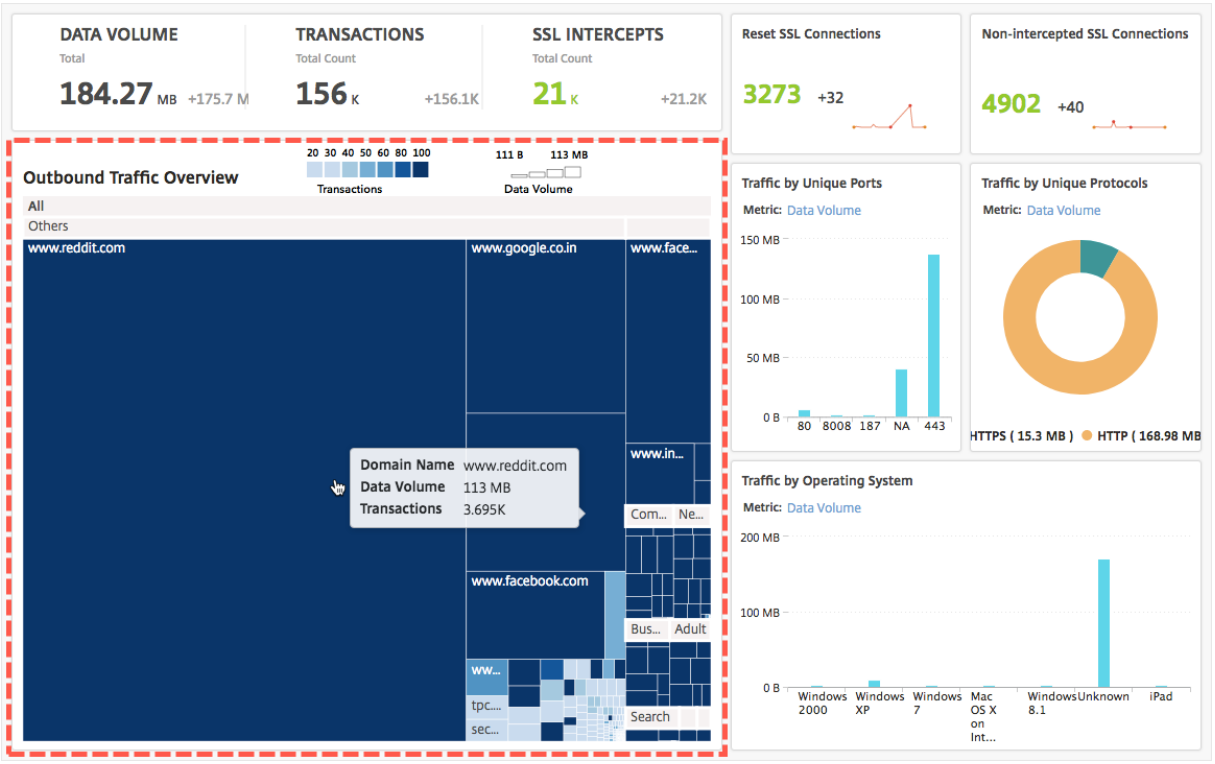
1. Beim Zugriff auf die URL verbrauchte Bandbreite
2. Transaktionen, die beim Zugriff auf die URL aufgetreten sind
3. Anzahl der SSL-Verbindungen, die beim Zugriff auf die URL abgefangen, nicht abgefangen und zurückgesetzt wurden

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Ihren Netzwerkverkehr mithilfe eines auf Ihrer SWG-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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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, die Zuweisung eines VPX von einem bestimmten Edge-Gateway im Rahmen des Dienstlöschens aufzuheben und dasselbe VPX für ein anderes Edge-Gateway erneut 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Automatisierte, bedarfsgerechte Zuweisung neuer ADC-Dienste als Teil eines Workflows zur Anwendungsbereitstellung
- Vereinfachte Konfiguration anwendungsspezifischer, erweiterter ADC-Funktionalität durch Anwendungsvorlagen
- Aufgabenteilung für mehrere Mandanten und ein Self-Service-Nutzungsmodell, das Cloud-Administratoren gleichzeitig einen zentralen Kontrollpunkt bietet
- 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 Sie Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler ADC -Treiber für OpenStack Neutron LBaaS

OpenStack Neutron LBaaS-Plugin enthält einen Citrix ADC -Treiber, der OpenStack die Kommunikation mit dem Citrix 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 Sie Citrix ADM und OpenStack miteinander

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Auf 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 Key Manager 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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

Anwendungsfall-Szenario

Im folgenden Anwendungsfall wird der Workflow für die Einbettung von NetScaler ADM mit der OpenStack-Plattform erläutert:

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 Citrix ADM installieren und konfigurieren und sie für die Zusammenarbeit 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

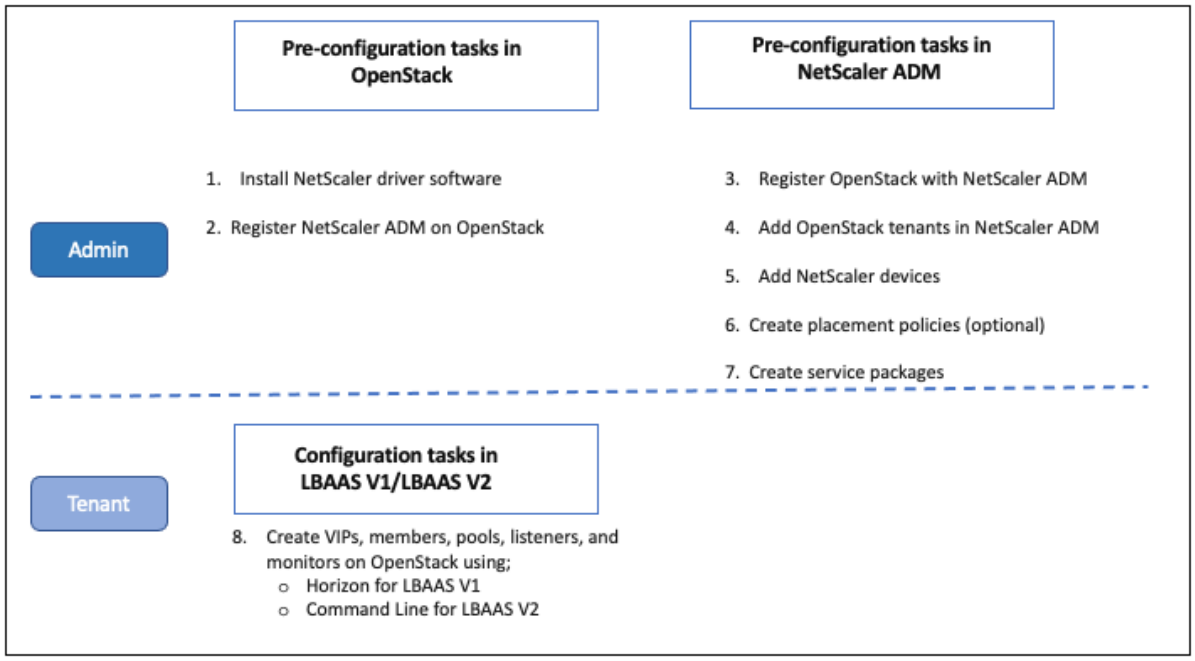
zu stellen. Das heißt, Steve wählt im Servicepaket eine Instanz aus, die nicht gemeinsam genutzt wird, für Tom. Anschließend weist er dem Servicepaket viele Citrix ADC VPX Instanzen zu und ordnet Example-Sportonline zusammen mit anderen Mandanten zu, die ein dediziertes Citrix ADC mit dem Servicepaket 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.

Citrix ADM-Integration mit dem OpenStack-Workflow

Das folgende Flussdiagramm zeigt den Workflow, dem Sie folgen müssen, wenn Sie LBaaS V1 und LBaaS V2 konfigurieren.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 12.1 wird auf einer unterstützten Hypervisor Arbeitsstation installiert, die die Mindestanforderungen an die Hardware erfüllt.
- OpenStack-Komponenten werden installiert und ausgeführt.
- Citrix ADM 12.1 unterstützt die folgenden OpenStack-Versionen: Newton, Ocata und Pike.

NetScaler ADM Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die Sie auf Ihrem OpenStack-Server zur Installation virtueller Citrix ADC Instanzen haben sollten.

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	8
Stauraum	500 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s oder 100 Mbit/s

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

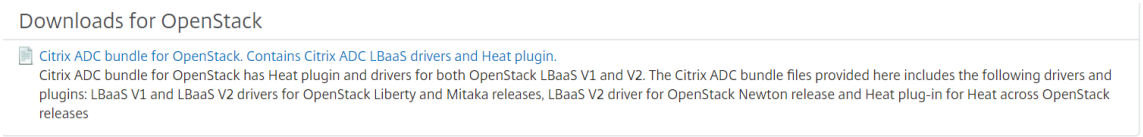
Installieren Sie NetScaler ADM auf einem unterstützten Hypervisor. Weitere Informationen zum Herunterladen und Installieren von NetScaler ADM finden Sie unter Bereitstellen von NetScaler ADM.

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 **Download-Seite** in Citrix ADM finden Sie Links zum Herunterladen des **Citrix ADC -Bundles 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`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

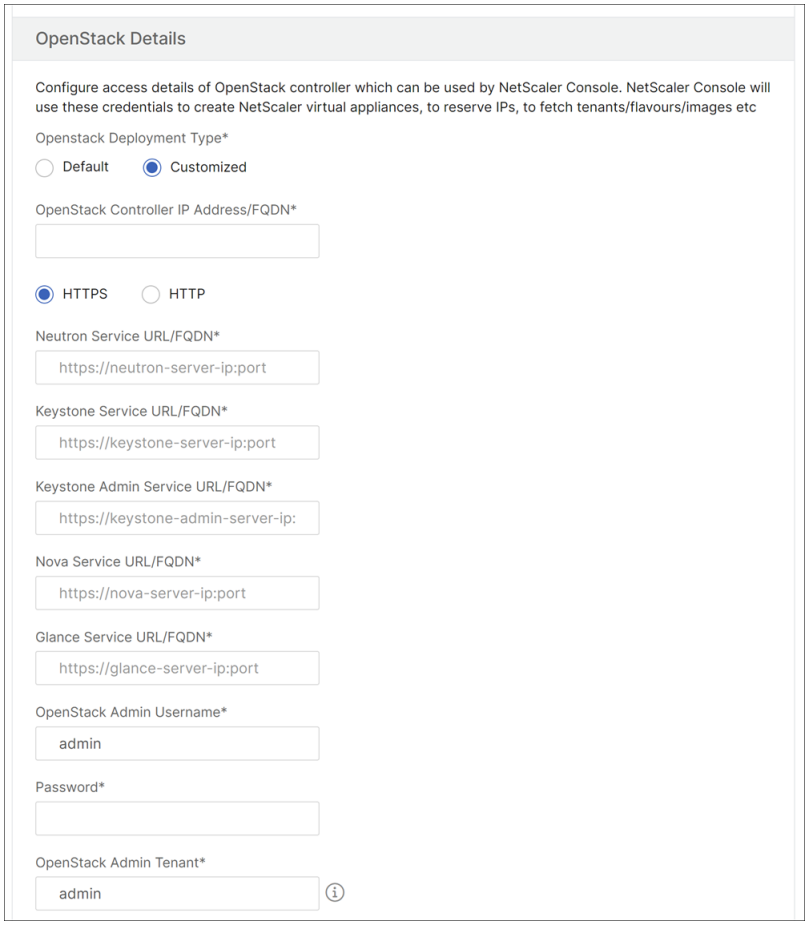
   Für Newton- und Ocata Versionen von OpenStack können Sie entweder den standardmäßigen oder den angepassten Bereitstellungstyp verwenden. Für die Pike-Version müssen Sie jedoch den benutzerdefinierten Bereitstellungstyp verwenden, um OpenStack bei Citrix ADM zu registrieren.

- **Standard-Bereitstellungstyp**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Address - 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-Controller. 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.



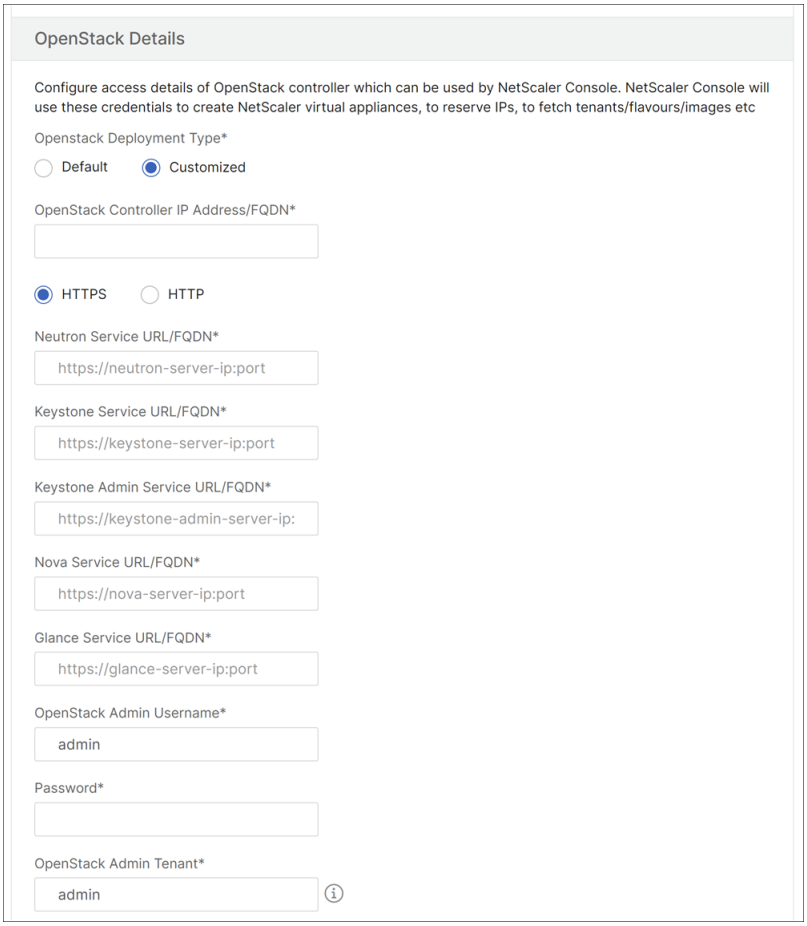
- **Angepasster Bereitstellungstyp**

  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. Das Registrieren von OpenStack Newton- und Ocata Releases bei Citrix ADM unterscheidet sich von der Registrierung von OpenStack Pike Release.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Newton und Ocata veröffentlichen OpenStack:

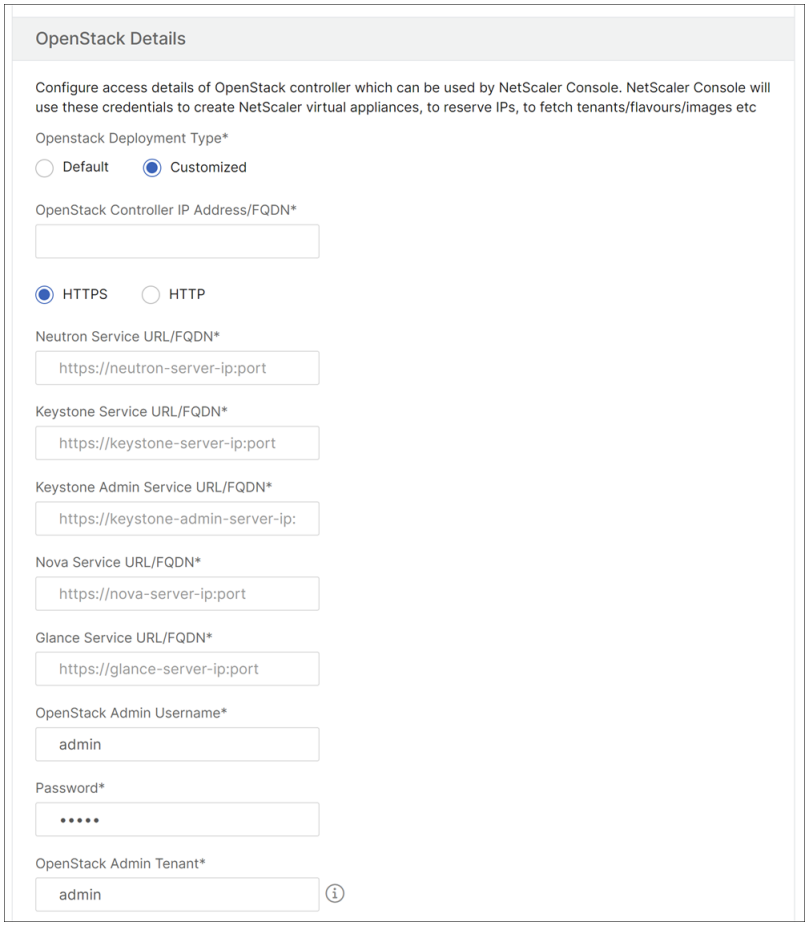
1. Geben Sie die Portnummern für die verschiedenen OpenStack-Dienste an, wenn Sie Newton Release von OpenStack registrieren.
2. Geben Sie den OpenStack Admin-Benutzernamen, das Kennwort und den OpenStack Admin-Mandanten-Benutzernamen an, wie Sie zuvor in den **Standardeinstellungen** angegeben hatten.



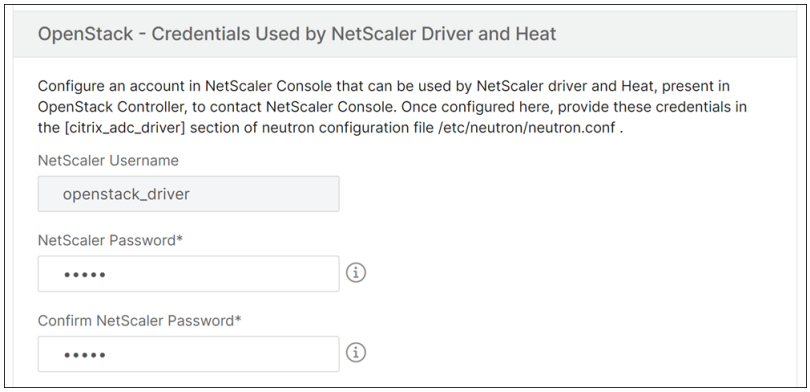
Pike Release von OpenStack:

Wenn Sie die Pike Release von OpenStack registrieren, geben Sie die Details der OpenStack-Dienste ein, wie in der folgenden Abbildung dargestellt. Sie müssen außerdem den OpenStack Admin-Benutzernamen, das Kennwort und den OpenStack Admin Mandanten-Benutzernamen wie in den Standardeinstellungen angeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Citrix ADC -Treiberinstallationsskript im OpenStack-Controller ausführen.



2. Klicken Sie auf **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 stellt der Identitätsdienst in OpenStack Authentifizierungsdienste für jeden OpenStack-Dienst bereit. 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
- Automatisches Provisioning der NetScaler 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
- Automatisches Provisioning der NetScaler VPX-Geräte auf OpenStack

Vorbereitstellung von NetScaler ADC Geräten

Installieren Sie das Citrix ADC-Gerät auf einer der Hypervisor-Plattformen 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

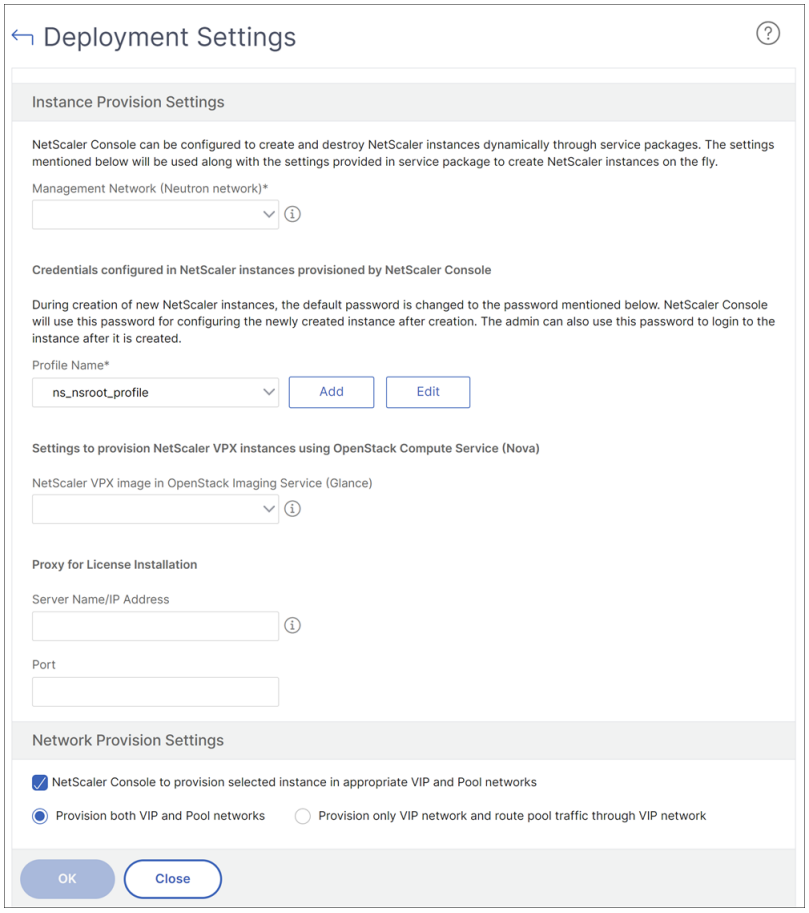
Autoprovisioning von Citrix ADC Geräten

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: Geben Sie die Citrix ADM -Lizenzaktivierungscodes (LAC) an, die für die Lizenzierung neuer automatisch bereitgestellter Citrix ADC Instanzen verwendet 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 Citrix ADC Instanz lädt dann die Lizenzdateien von der Citrix Website mit dem hier angegebenen LAC 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

Aktivieren des Datenverkehrs von Citrix ADC Instanzen zu Backend-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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 NetScaler ADC VPX-Images aus, das auf der NetScaler ADC SDX-Plattformvorhanden ist.LBaaS V2 über die Befehlszeile konfigurieren

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. Stellen Sie eine Verbindung zu einem beliebigen Neutron-Client her und führen Sie die Konfigurationsaufgaben aus. Weitere Informationen zum Ausführen von Konfigurationsbefehlen finden Sie unter Konfiguration von LBaaS V2 mithilfe der Befehlszeile.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Barbicanverwalteten Zertifikaten, Zertifikatspaketen (einschließlich zwischengeschalteter Zertifizierungsstellen), SNI-Unterstützung sowie den regulären Load Balancing-Funktionen. LBaaS V2 unterstützt nur 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 SSL-Abladefunktion

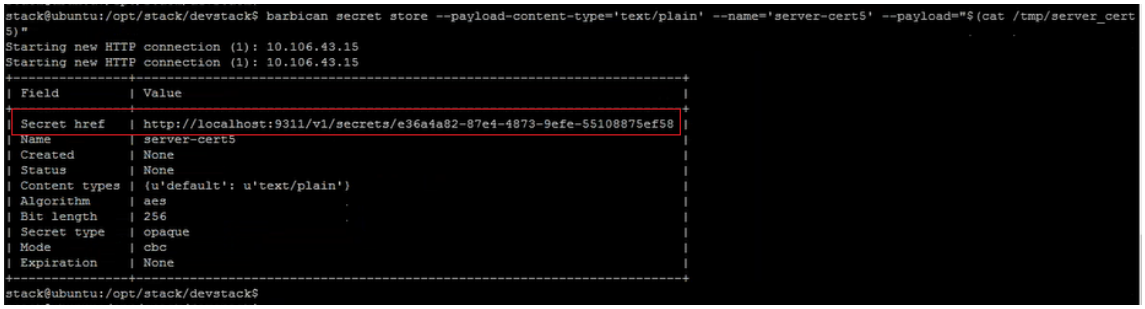
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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>

   Beispiel: barbican Secret Store —payload-content-type='text/plain'—name='hp_server_certificate' —payload="hp_server/tmp/server_certificate"



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>

   Beispiel: barbican Secret Store —payload-content-type='text/plain'—name='shp_server_key' —payload="hp-server/tmp/server_key"

   Hinweis

   Wenn Sie diese beiden Barbican-Befehle ausführen, um das Zertifikat und den Schlüssel zu laden, geben die geheimen href-Felder 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 stellen Sie diese Links als Parameter bereit, wenn Sie den Container im Barbican-Dienst in Schritt 3 erstellen.

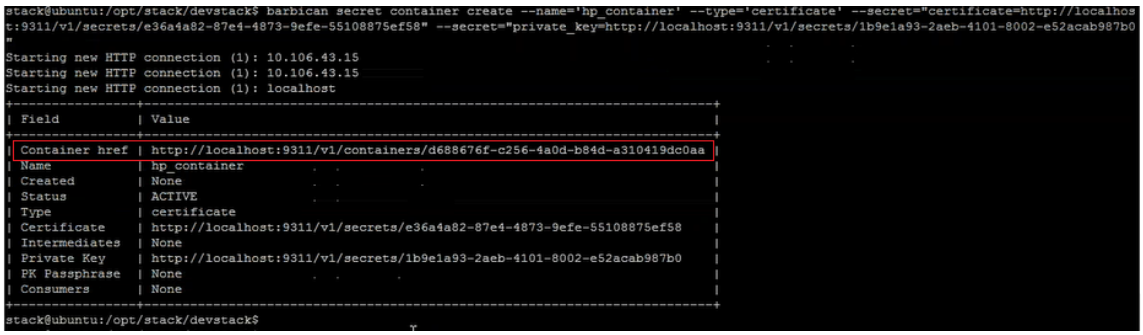
3. Erstellen Sie einen Container im Barbican-Dienst, um das Zertifikat und den Schlüssel mit dem folgenden Befehl zu speichern:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ersetzen Sie im Befehl durch <certificate_url> die URL, die Sie beim Hochladen des Zertifikats aus dem Feld “Geheime href”erhalten haben. Ersetzen Sie in ähnlicher Weise durch <key_url> die URL, die Sie aus dem Feld “Geheime href”erhalten haben, wenn Sie den Schlüssel hochgeladen haben.

barbican secret container create –name<container_name> –type<container_type> –secret<certificate_url> –secret<key_url>

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”



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

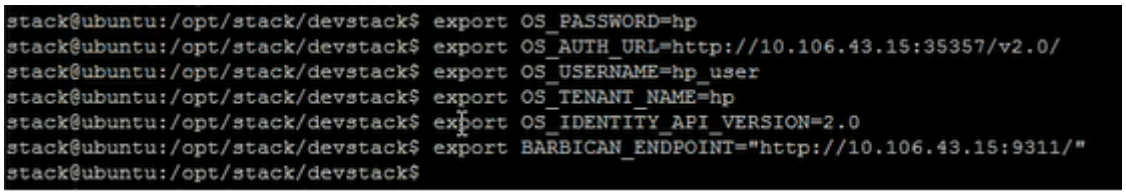
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   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/”



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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>

   Beispiel: neutron lbaas-loadbalancer-create –name hp-lb-test hp-sub1 –provider netscaler

```
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:

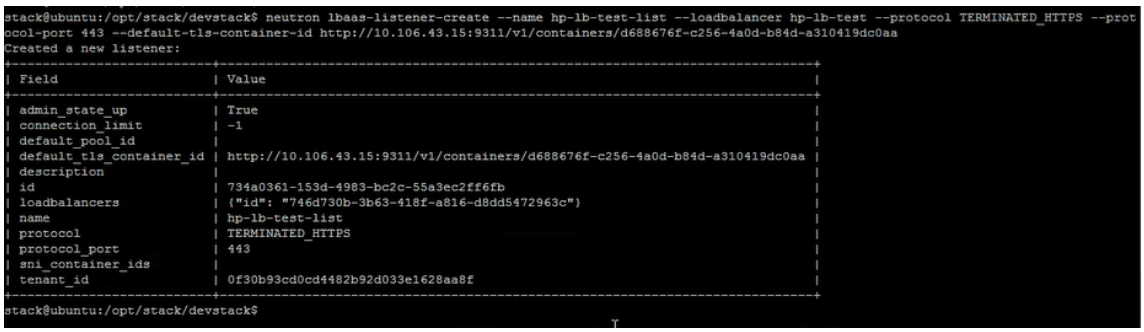
   neutron lbaas-listener-create –loadbalancer <loadbalancer-name> –name <listener-name> –protocol <protocol_type> –protocol-port <port_number> –default-tls-container-id<container_url>

   Beispiel: Neutron lbaas-listener-create —name hp-lb-testliste —loadbalancer hp-lb-test —protokoll TERMINATED_HTTPS —protokoll-port 443 —default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa

> **Hinweis**
>
> Wenn Sie einen Listener ohne SSL-Offload-Unterstützung erstellen, führen Sie den folgen-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

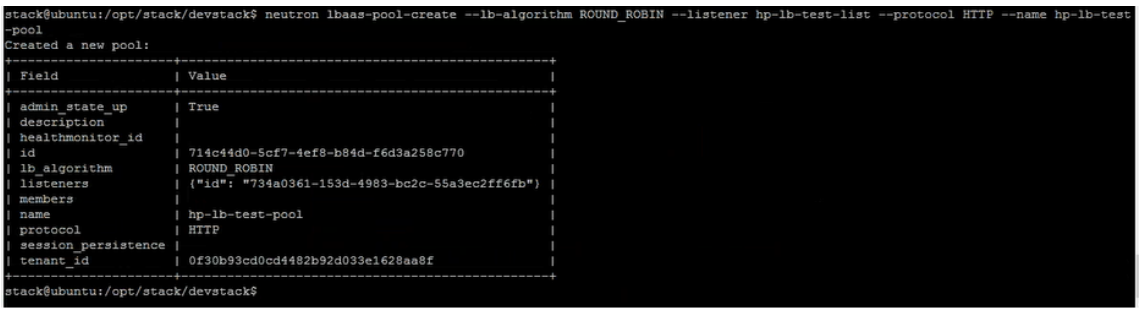
> den Befehl aus, ohne Speicherorte für den Container bereitzustellen:
>
> neutron lbaas-listener-create –loadbalancer <loadbalancer-name> –name <listener-name> –protocol <protocol_type> –protocol-port <port_number>



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>

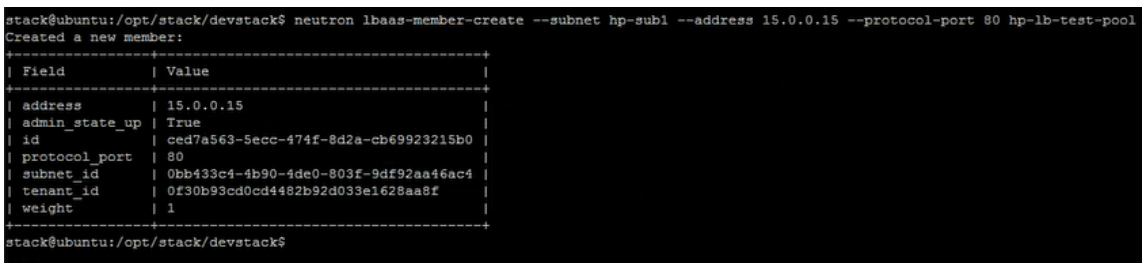
   Beispiel: neutron lbaas-pool-create –lb-algorithm LEAST_CONNECTIONS –listener demolistener –protocol http –name demopool



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>

   Beispiel: neutron lbaas-member-create –subnet hp-sub1 –address 15.0.0.15 –protocol-port 80 hp-lb-test-pool



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 sollte folgendes Format haben:

http://\<mas_ip\>/\<admin_ui\>/mas/ent/html/cc_tenant_main.html

Hierbei <mas-ip-address> handelt es sich um die Citrix ADM IP-Adresse, die bei OpenStack registriert ist.

> **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. Dadurch wird die Leistung des Load Balancers verbessert, 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`sollte ein Endbenutzer, der nach sucht, von einem Serverpool bedient werden, der Inhalte über das Unternehmen und die Dienste hostet, während ein Benutzer, der nach sucht, von einem anderen Serverpool bedient werden `http://example-sports.com/shopping-cart-football`sollte, der ermöglicht es den Benutzern, Online-Einkäufe zu tätigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 sollten im Wesentlichen bestimmte Inhaltstypen bereitstellen. Beispielsweise könnte ein Server nur Bilder bereitstellen, ein anderer Server kann serverseitige Skriptsprachen wie PHP und ASP ausführen, und ein anderer könnte 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 value Parameter 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-.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**
>
> Die Hostname-, Pfad-, Header- und Cookie-Attribute unterstützen alle Vergleichstypen, aber das file_type-Attribut 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Nicht autorisierte Antwort zurückgeben, um den Benutzern den Zugriff für 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Anforderung 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 ist immer eine Standardrichtlinie mit einem csvserver mit der Priorität 1 zugeordnet. Diese Standardrichtlinie gibt die Anzahl der TCP-Verbindungen an, die ein lbvserver zu einem bestimmten Zeitpunkt verarbeiten soll. 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 werden zuerst die Richtlinien “reject”und/oder “redirect_to_url”ausgewertet und dann die Richtlinie “redirect_to_pool”ausgewertet. In einer NetScaler ADC Instanz werden die Responder-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

richtlinien 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 sollten keine identischen Ausdrücke haben. Die abgeleiteten Ausdrücke sollten in den Responder- und Inhaltswechselrichtlinien hinzugefügt werden, 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 ist immer eine Standardrichtlinie mit einem csvserver mit der Priorität 1 zugeordnet. Diese Standardrichtlinie gibt die Anzahl der TCP-Verbindungen an, die ein lbvserver zu einem bestimmten Zeitpunkt verarbeiten soll. 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 werden zuerst die Richtlinien "reject"und/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 sollten ähnliche Ausdrücke haben. Ähnliche abgeleitete Ausdrücke sollten in den Responder- und Inhaltswechselrichtlinien hinzugefügt werden, 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
    >
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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 License Activation Code (LAC), den Sie von Citrix erhalten haben, die entsprechende Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

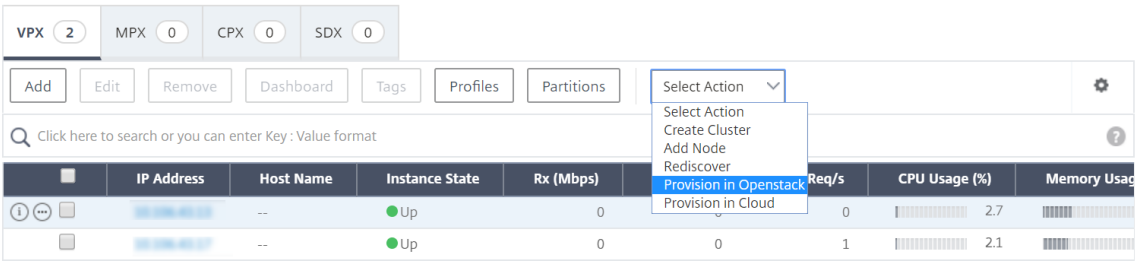
   c) **Citrix ADC Instanz Provisioning** : Wählen Sie **Instanz OnDemand** erstellen, um Citrix ADC Instanzen während der Konfiguration selbst zu erstellen.

   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.



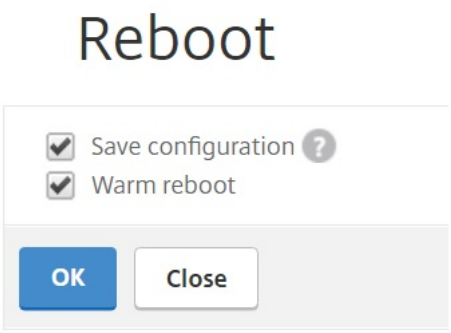
   a) Geben Sie auf der Seite **Device Provisioning** den Namen des Geräts ein, und wählen Sie das Servicepaket aus, das Sie im vorherigen Schritt erstellt haben.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Melden Sie sich bei der Instanz an, wenn der Citrix ADC VPX Instnace in Ihrem Browserfenster geöffnet wird. 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. Stellen Sie eine Verbindung zu einem beliebigen Neutron-Client her und führen Sie die Konfigurationsaufgaben aus. Weitere Informationen zum Ausführen von Konfigurationsbefehlen finden Sie unter Konfiguration von LBaaS V2 mithilfe der Befehlszeile.

Provisioning der NetScaler ADC VPX Instanz auf OpenStack mit StyleBook

February 5, 2024

Im OpenStack-Orchestrierungsworkflow verwendet Citrix Application Delivery Management (ADM) jetzt das StyleBook “os-cs-lb-mon”, um LBAAS-Konfigurationen auf Citrix 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 im OpenStack-Workflow bietet folgende Vorteile:

- Bessere Visualisierung durch Anzeigen aller Konfigurationsobjekte.
- Zuverlässigkeit durch Rollback.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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:

- Führen Sie einen Bildlauf durch, um das Konfigurationspaket "os-cs-lb-mon"anzuzeigen, das für den Load Balancer bereitgestellt wurde.
- Klicken Sie im StyleBook-Bedienfeld "os-cs-lb-mon"auf **View Definition**, um die Konfiguration zu überprüfen, die auf den Instanzen 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 des OpenStack-Orchestrierungsworkflows 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-->
```

- Beim Ausführen des Migrationsskripts werden Konfigurationspakete des StyleBook "os-cs-lb-mon"erstellt, 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 auf den Instanzen mit dem StyleBook "os-cs-lb-mon"erst bereitstellen, nachdem Sie das Migrationsskript von Version 12.1 Build 49.23 ausgeführt haben.
- Alle Konfigurationen, die von OpenStack versucht werden, schlagen fehl, 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> neueste Version aktualisiert haben. Verwenden Sie die Citrix ADC-Bundledateien, die zusammen mit dem neuesten Citrix ADM 12.1 Build 49.23 bereitgestellt werden.

LBaaS V2 API-Implementierungen werden über Neutron LBaaS-Befehle durchgeführt. Stellen Sie eine Verbindung zu einem beliebigen Neutron-Client her und führen Sie die Konfigurationsaufgaben aus. Weitere Informationen zum Ausführen von Konfigurationsbefehlen finden Sie unter Konfiguration von LBaaS V2 mithilfe der Befehlszeile.

VPX-Ein- und Auscheck-Lizenz und gepoolte Lizenzunterstützung für OpenStack-Umgebung

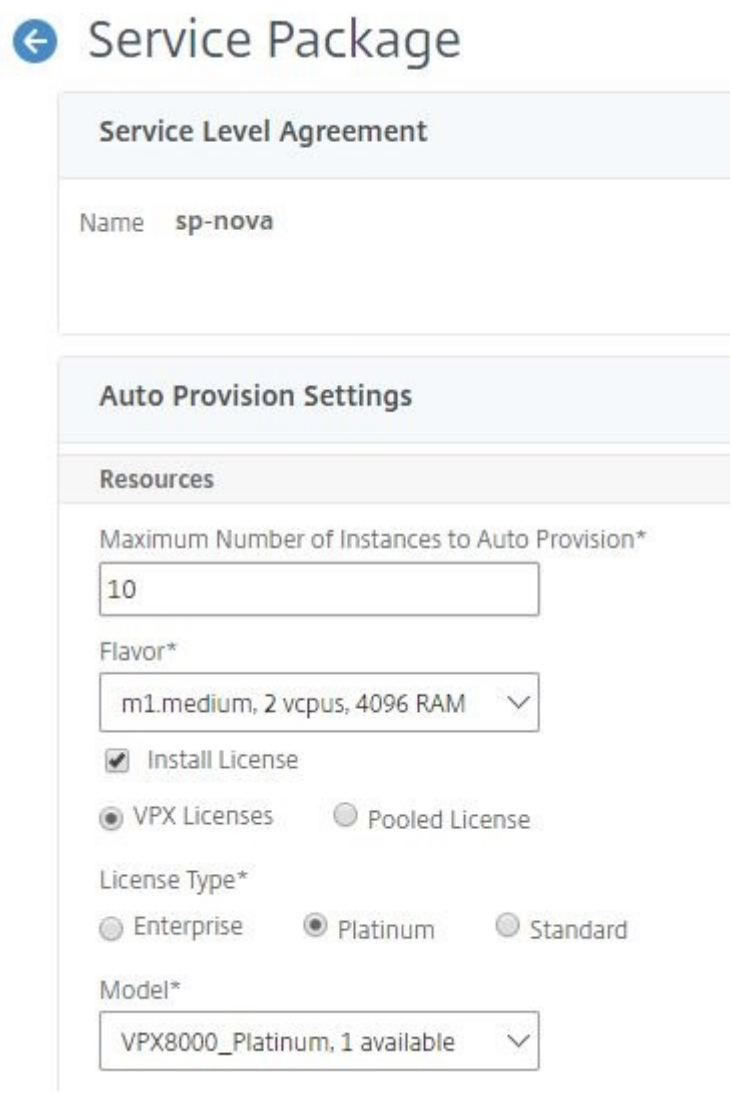
February 5, 2024

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.

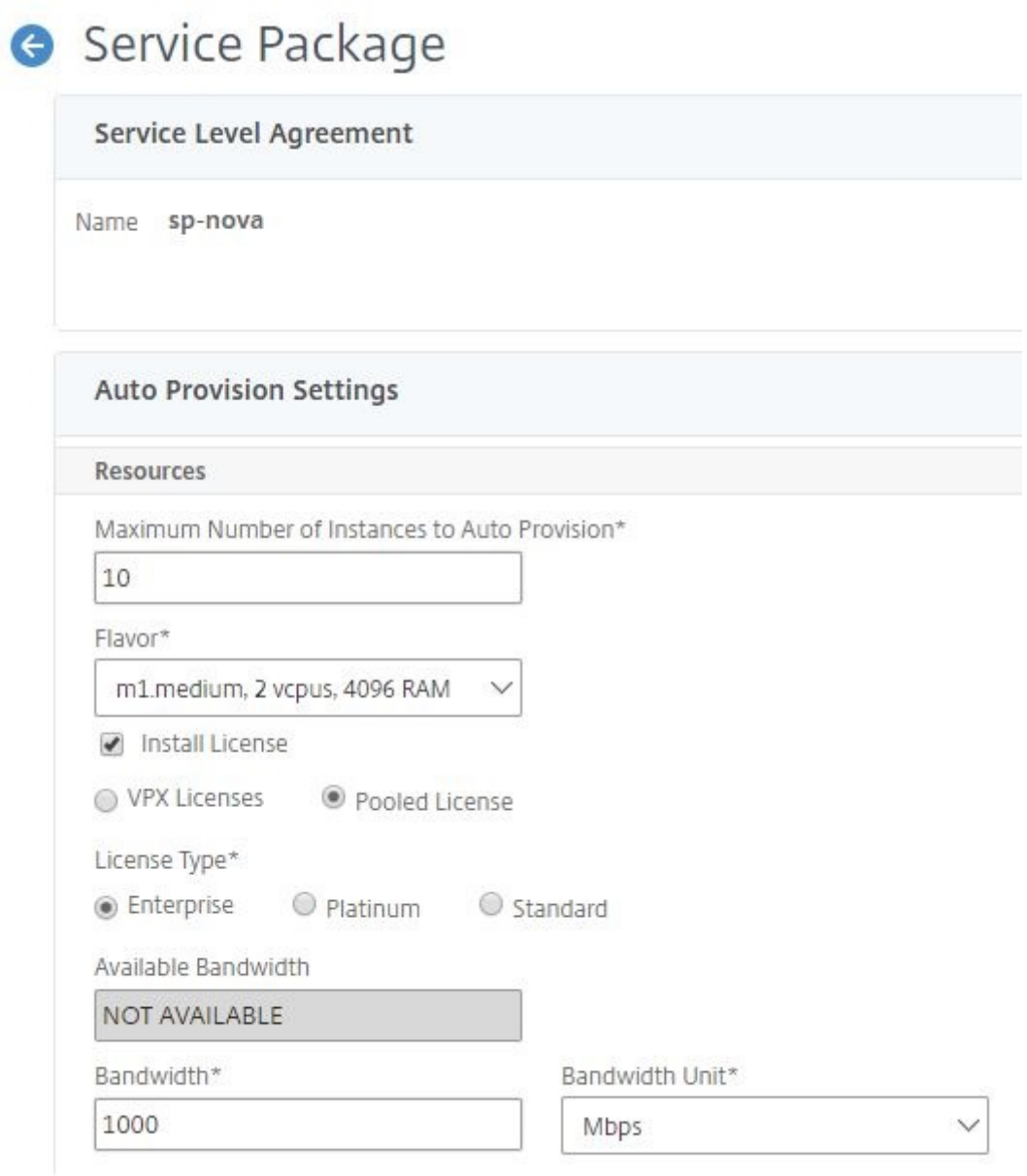
- Wenn es sich um eine Ein- und Auscheck-Lizenz handelt, können Sie die zu installierende Lizenz aus den verschiedenen verfügbaren Lizenzen auswählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- Wenn es sich um eine Poollizenz handelt, können Sie sowohl die Bandbreite als auch den Typ der zu installierenden Lizenzedition auswählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

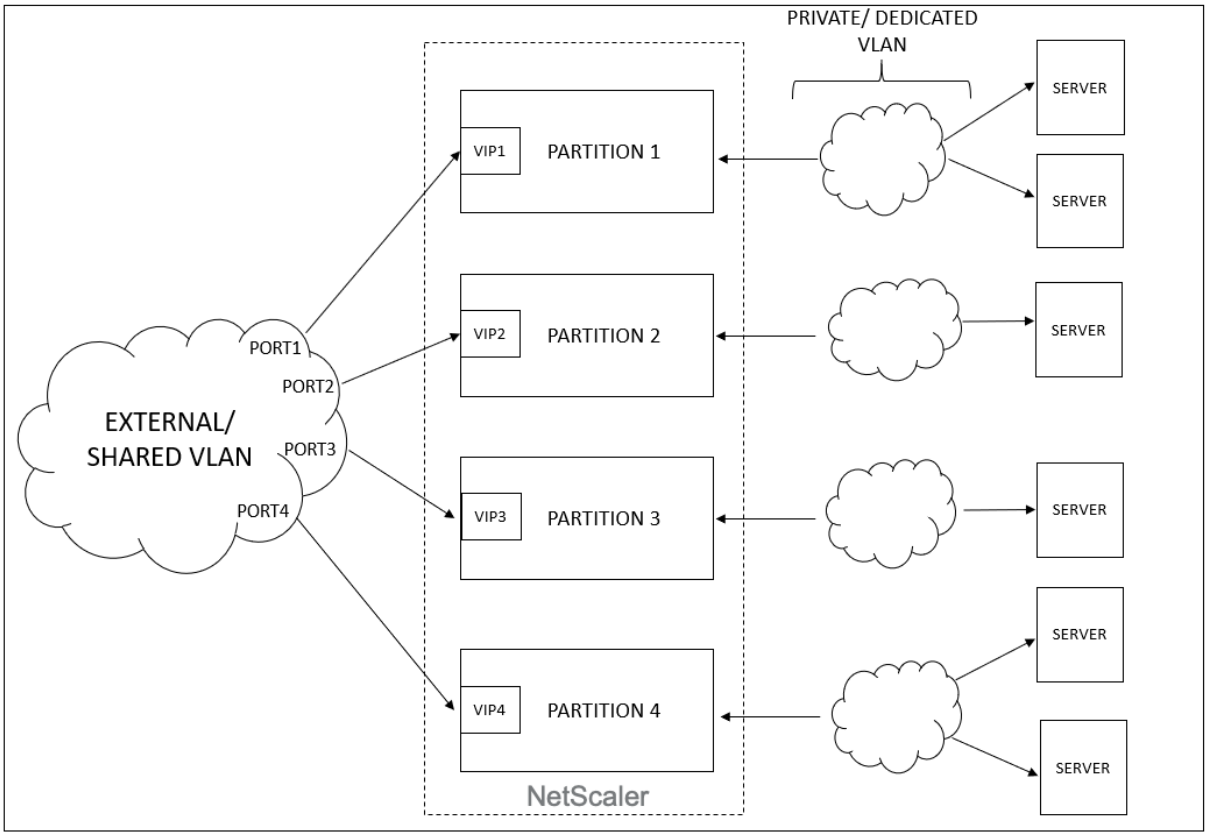
> dass die Lizenzen auf das aktuelle aktive oder primäre Citrix ADM MAS-HA-1 hochgeladen werden. Wenn Sie die erste Anforderung bereitstellen und Citrix ADM die Citrix ADC VPX Instanzen erstellt, checkt die Instanz die erforderlichen Lizenzen von MAS-HA-1 aus. Zu einem späteren Zeitpunkt wird davon ausgegangen, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

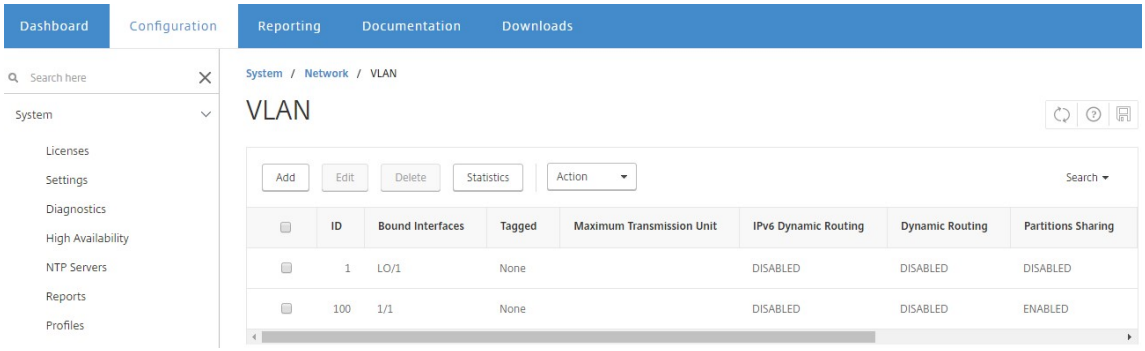
Konfigurieren von freigegebenem VLAN von der Citrix ADC Instanz

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

festzulegen.

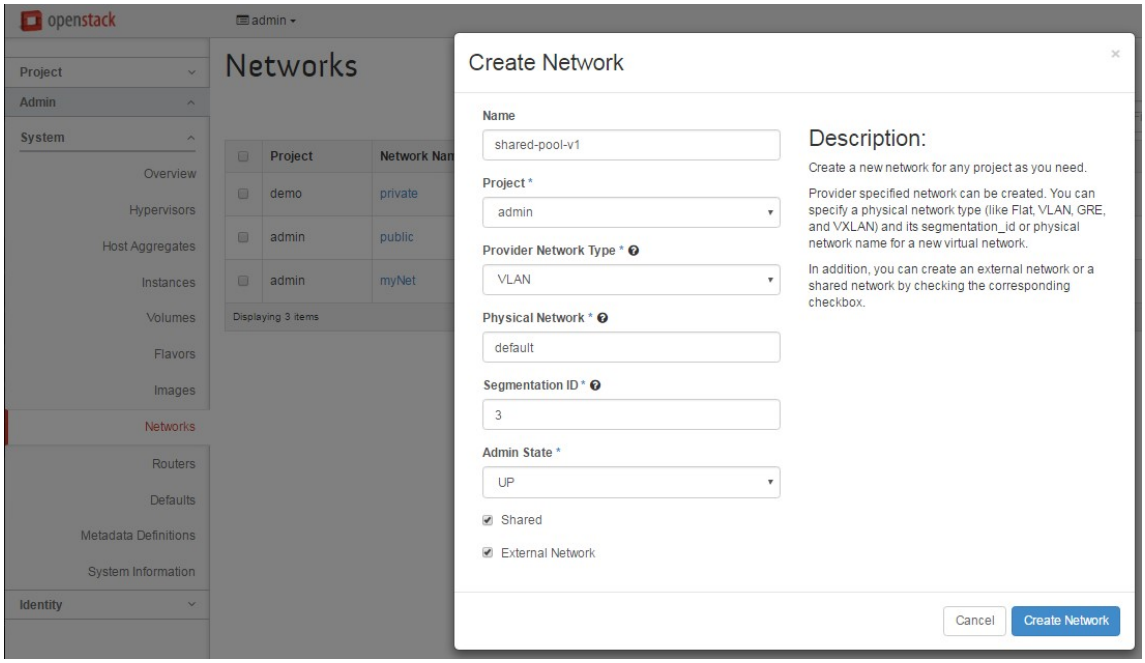
2. Aktivieren Sie auf der Seite **VLAN konfigurieren** das Kontrollkästchen **Partitions Sharing**.
3. Klicken Sie auf **OK**.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 Citrix ADC VPX Instanz kontaktiert das Citrix Lizenzierungsportal während der Einrichtung und verwendet den License Activation Code (LAC), um die Lizenzdateien automatisch herunterzuladen und zu installieren.

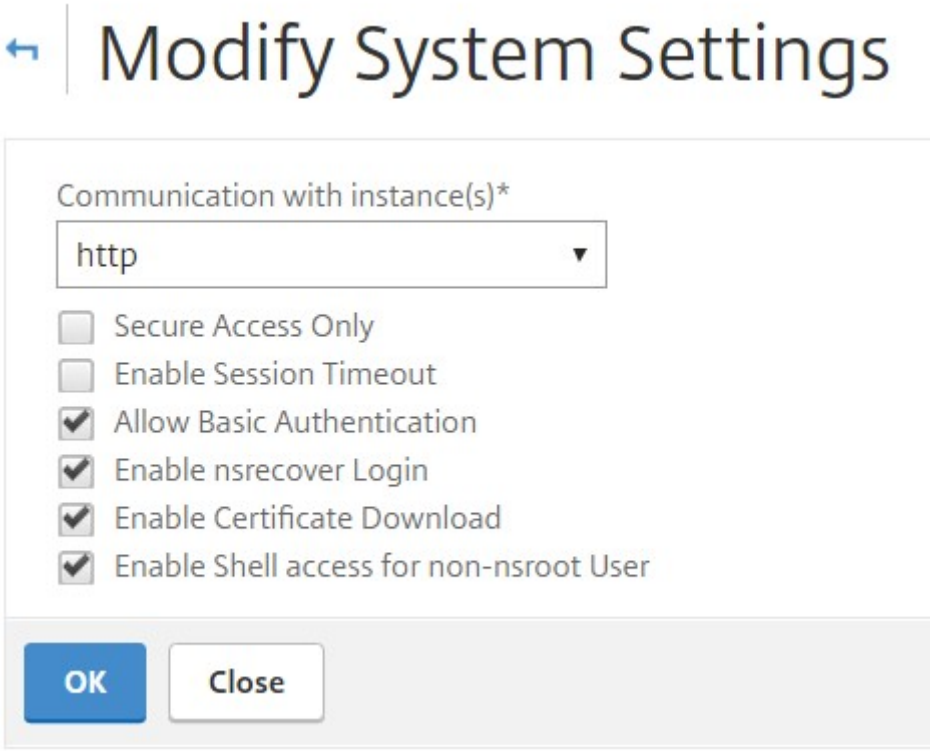
Test-Lizenzen

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 RESTful-API verwaltet, und die API ermöglicht es Mandanten, REST-Aufrufe zum Erstellen, Aktualisieren und Löschen von LBaaS-Objekten durchzuführen. 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

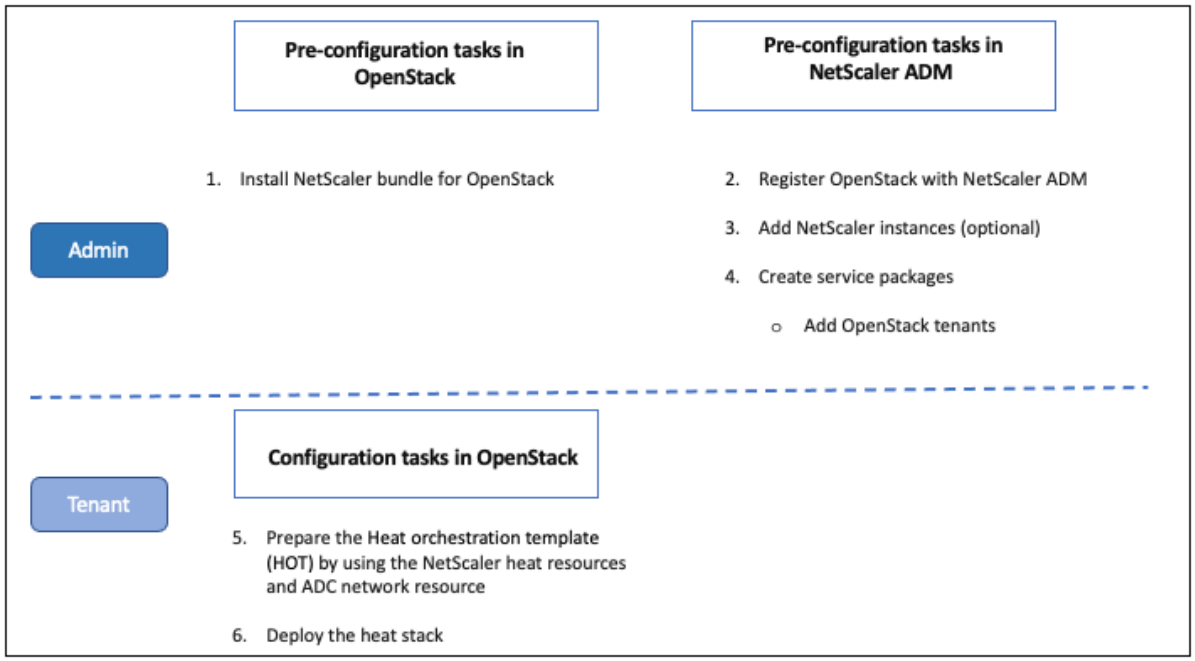
Citrix Application Delivery Management (ADM) StyleBooks können zum Erstellen und Konfigurieren von Citrix ADC Funktionen verwendet werden. Genau wie Heat-Vorlagen sind auch die StyleBooks in YAML geschrieben. Für jede Funktionalität können separate StyleBooks erstellt werden, und ein einzelnes StyleBooks 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**
>
> Citrix ADM im Hochverfügbarkeitsmodus bereitstellen, 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. Benutzername des Administrators

      iii. Kennwort

      iv. OpenStack Admin-Mandant

      v. NetScaler ADC-Treiber und Heatkennwort

      > **Hinweis:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 Citrix 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-

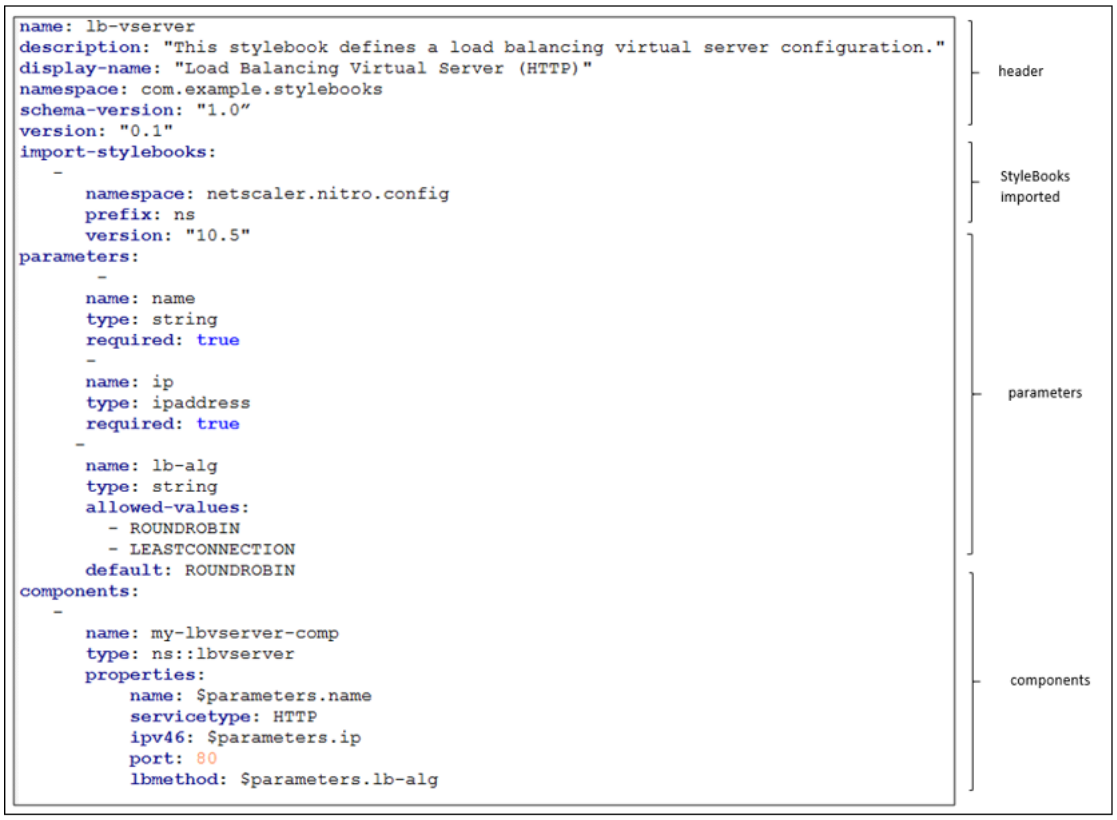
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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 Citrix ADM, um zu beobachten, dass die Citrix ADC Instanzen erfolgreich in Form von StyleBooks Configpacks konfiguriert wurden.

Ein Beispiel für ein NetScaler ADM StyleBooks:

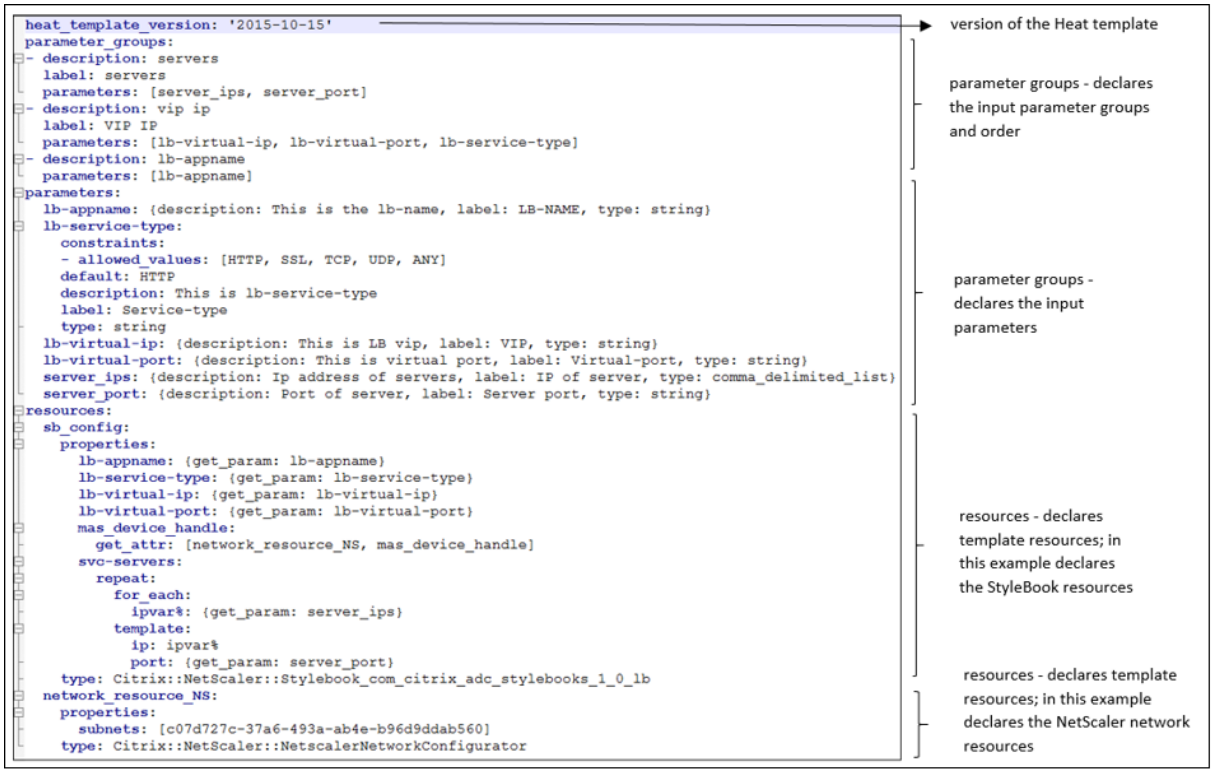
Die folgende Abbildung zeigt ein Beispiel für die Konstruktion eines NetScaler ADM StyleBooks und erläutert kurz die Komponenten. Weitere Informationen zu NetScaler ADM StyleBooks und zur Verwendung der mitgelieferten StyleBooks finden Sie unter StyleBooks.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Weitere Informationen zu Heat-Diensten und zum Erstellen von Vorlagen finden Sie in derOpenStack Heat-Dokumentation.

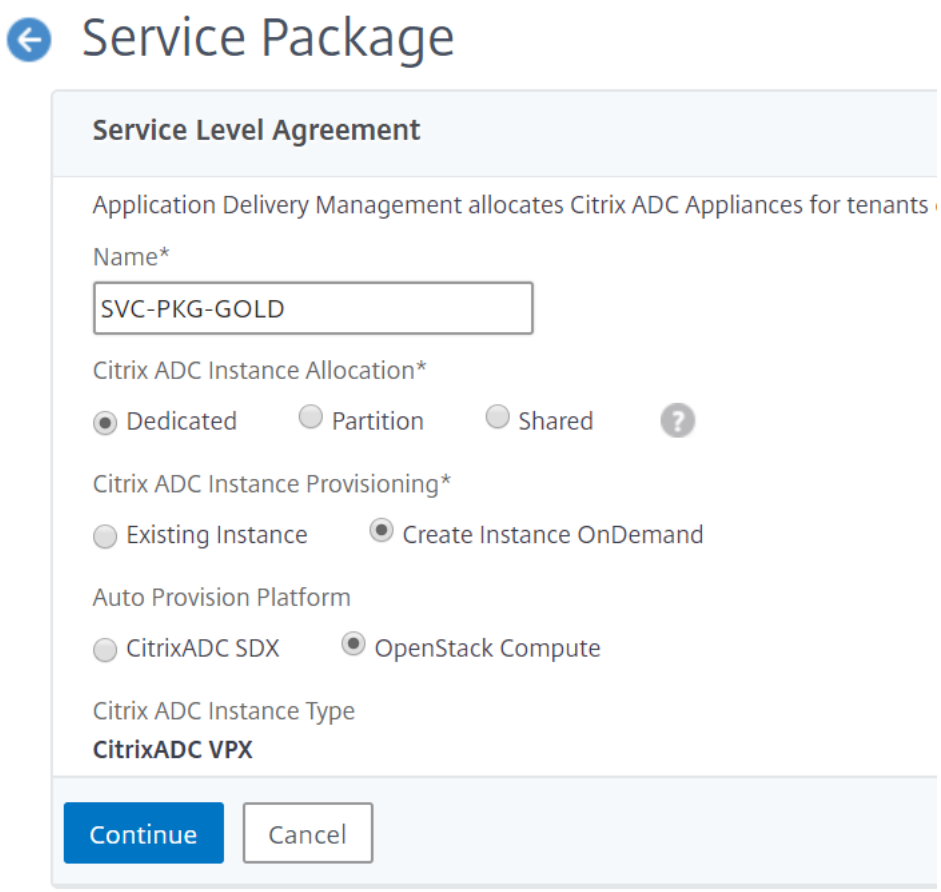
Servicepaket-Isolationsrichtlinien

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.

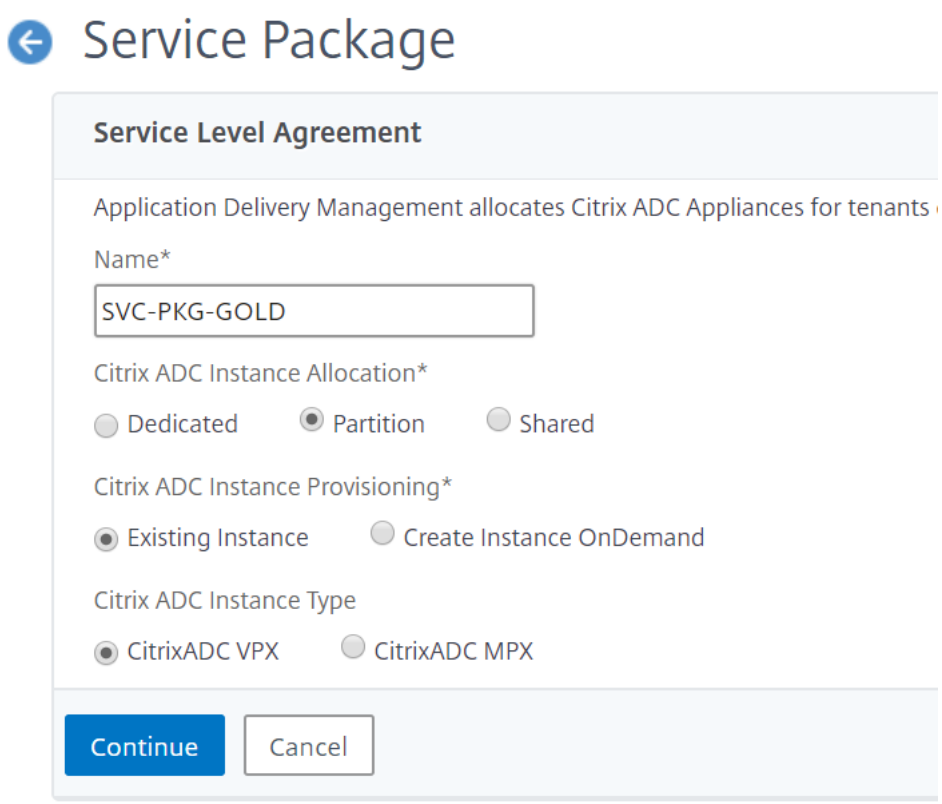
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

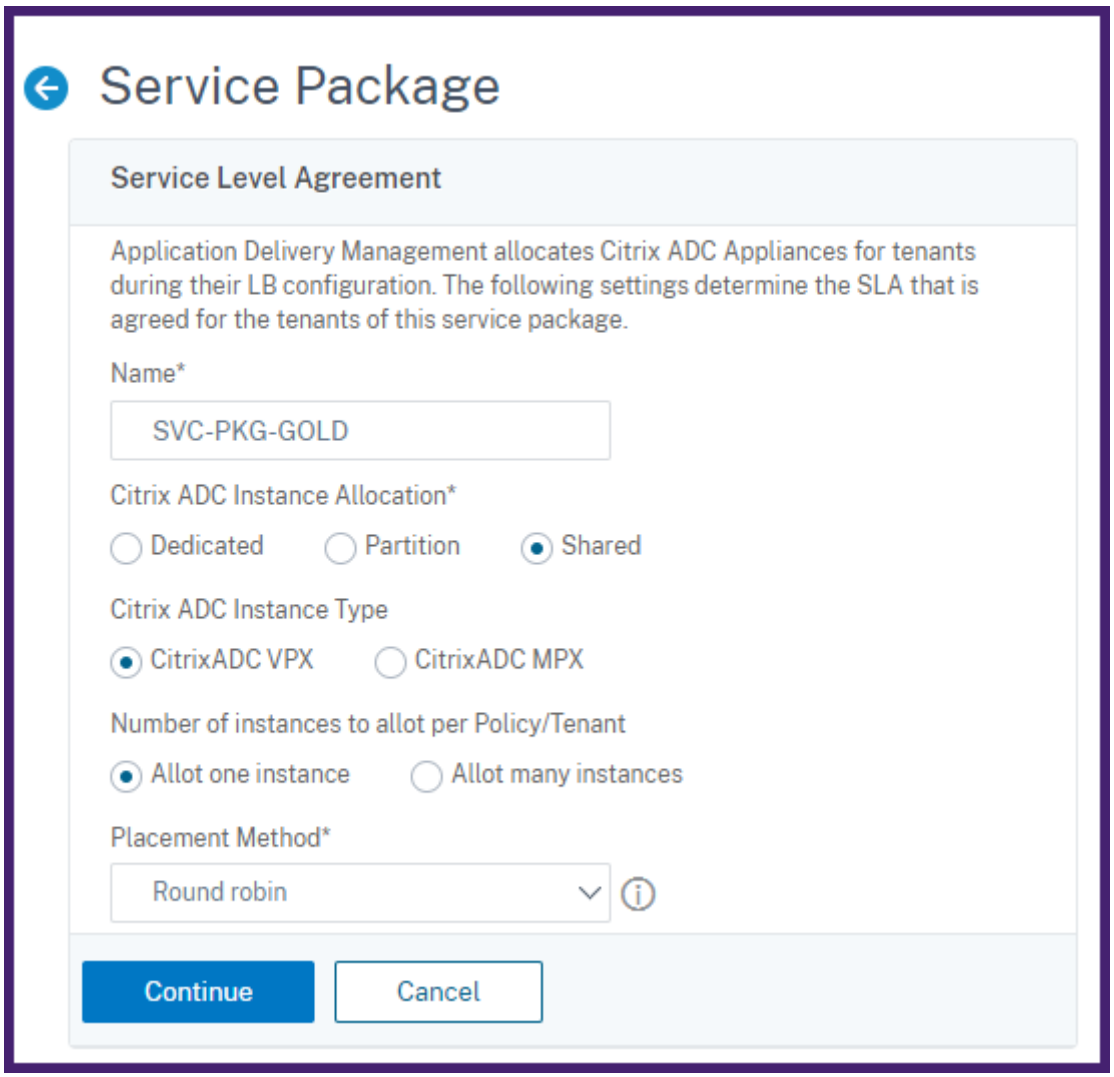


Freigegebene Isolationsrichtlinie

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Hinweis

Sie können auch flexible Platzierungsrichtlinien erstellen, bei denen die Poilicies nicht nur auf dem Mandantennamen oder der ID basieren, sondern auch auf anderen benutzerdefinierten Attributen. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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”

2. Pool-Subnetzname basierter Richtlinienausdruck

   config [“pools”] [“subnet_name”] == “us-west-payment-subnet1”

3. Load Balancer-Subnetname basierter Richtlinienausdruck

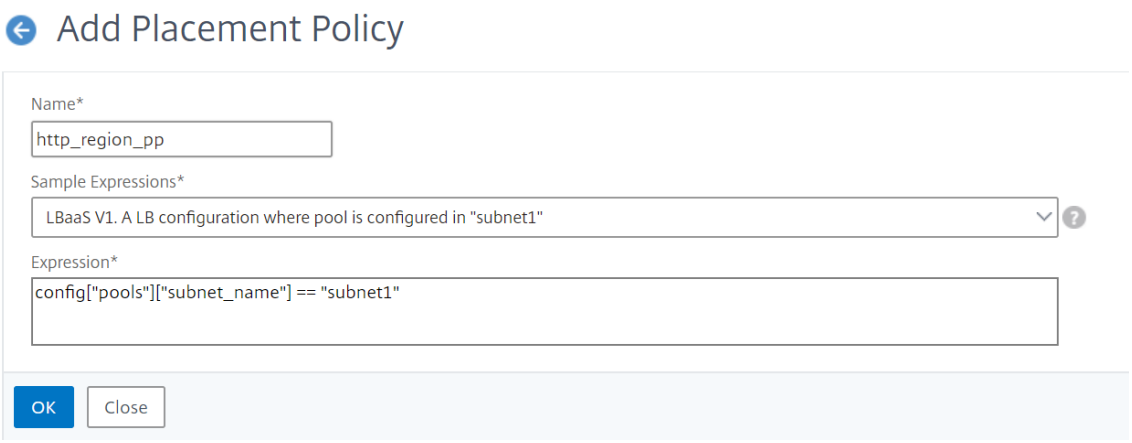
   config [“loadbalancers”] [“subnet_name”] == “mas-Subnetz”

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

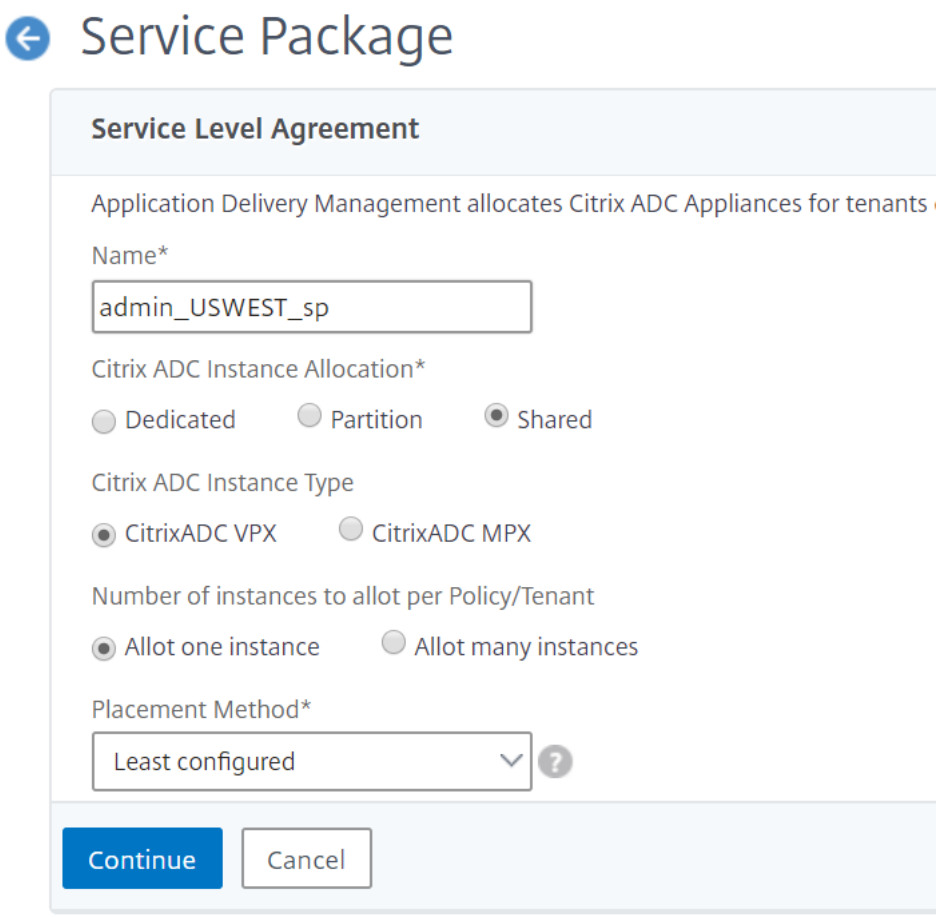
   Wählen Sie **Ein Gerät zuweisen** aus, wenn alle Load Balancer-Konfigurationen eines Mandanten an ein Gerät gebunden werden sollen. Wählen Sie **Viele Geräte zuweisen**, wenn jede Load Balancer-Konfiguration eines Mandanten auf der Grundlage von Platzierungsrichtlinien auf mehrere Geräte verteilt werden 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.

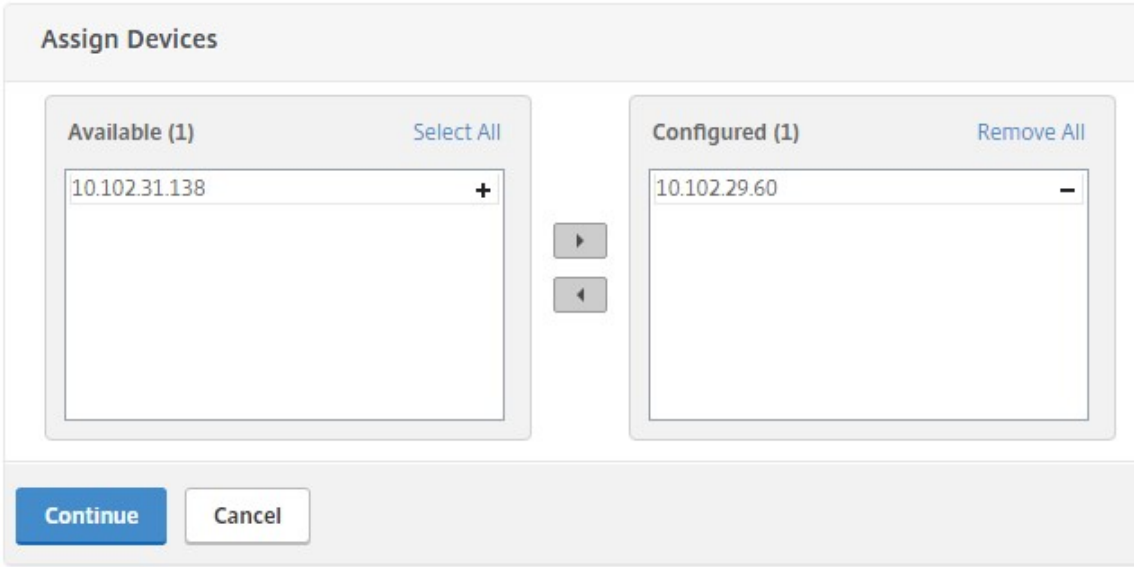
   d) Platzierungsmethode —Wählen Sie **Am wenigsten konfiguriert**

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

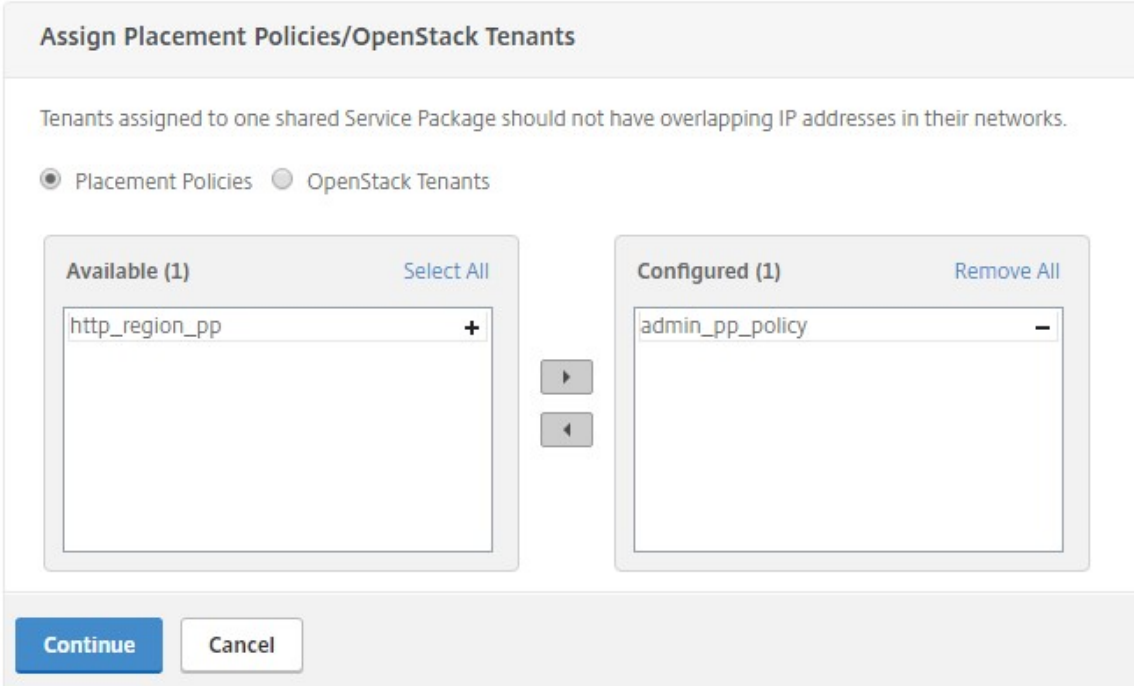


6. Klicken Sie auf **Weiter**.
7. Fügen **Sie im Abschnitt Geräte zuweisen** die verfügbaren NetScaler ADC Geräte zur Liste der konfigurierten Geräte hinzu.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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: "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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 12.1 auf einem der unterstützten Hypervisoren finden Sie unter Bereitstellen von NetScaler ADM.

VMware ESXi Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die Sie auf Ihrem VMware ESXi -Server benötigen, um eine virtuelle Citrix ADM Appliance zu installieren.

Komponente	Voraussetzung
RAM	8 GB
Virtuelle CPU	8
Speicherplatz	500 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

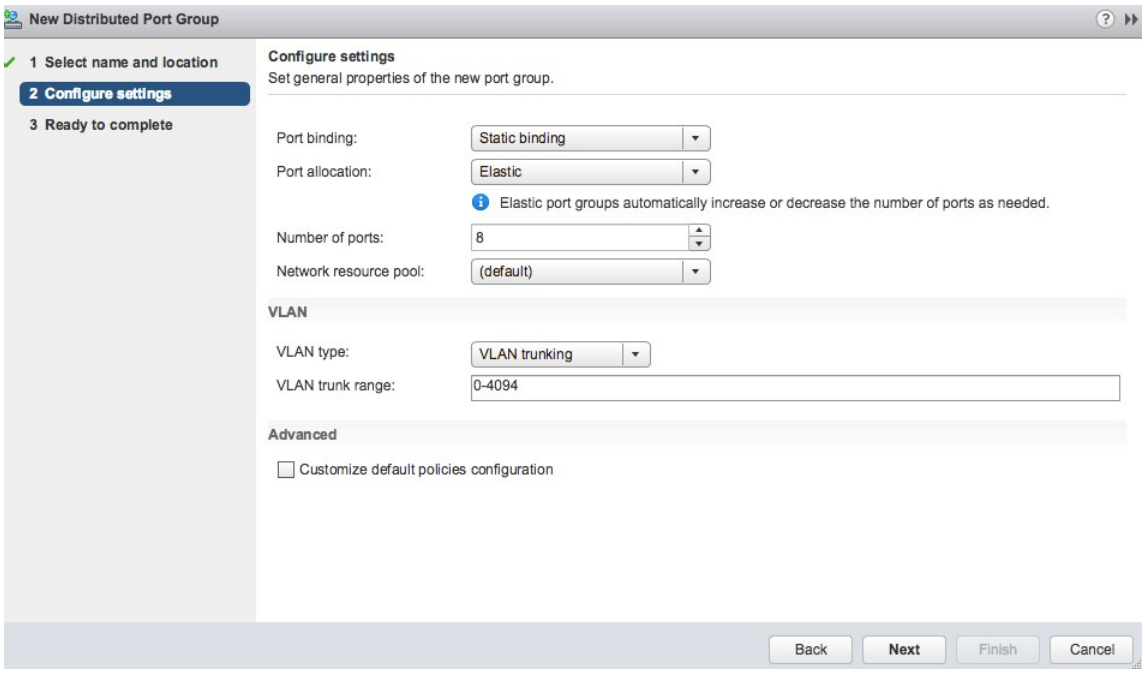
Konfiguration von VMware NSX

- Erstellen Sie einen Pool von Citrix ADC VPX Instanzen mit unterschiedlichen Kapazitäten, die den verschiedenen Servicepaketen hinzugefügt werden.

Beispiel:

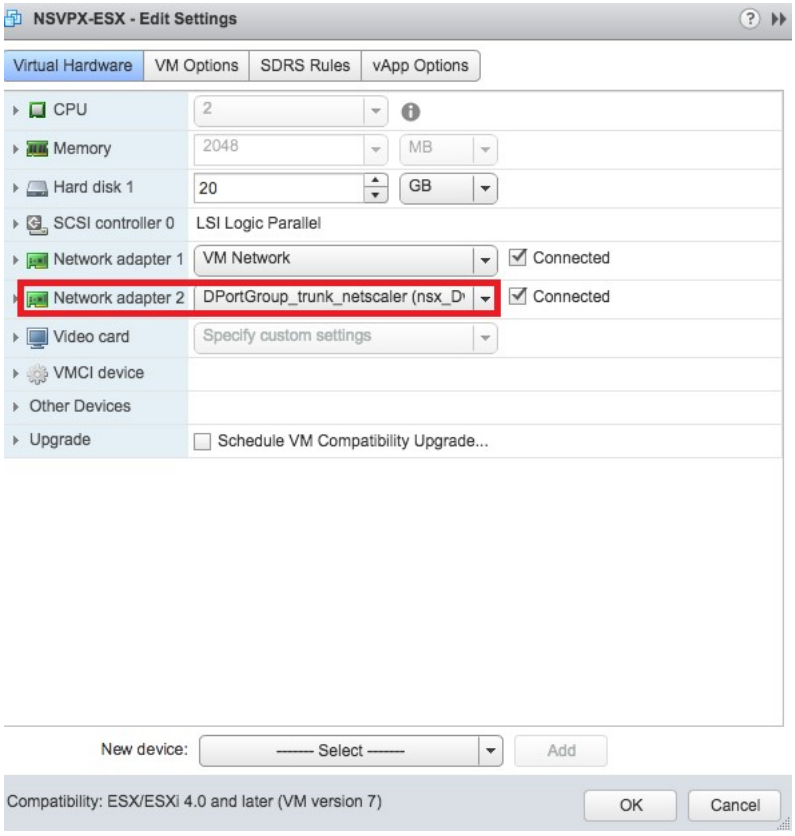
- Erstellen Sie fünf Citrix ADC VPX Instanzen von VPX1000 (1 Gbit/s). Diese Instanzen werden dem Gold-Servicepaket hinzugefügt.
- Erstellen Sie fünf Citrix ADC VPX Instanzen von VPX10 (10 Mbit/s). Diese Instanzen werden dem Bronze-Servicepaket hinzugefügt.

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.

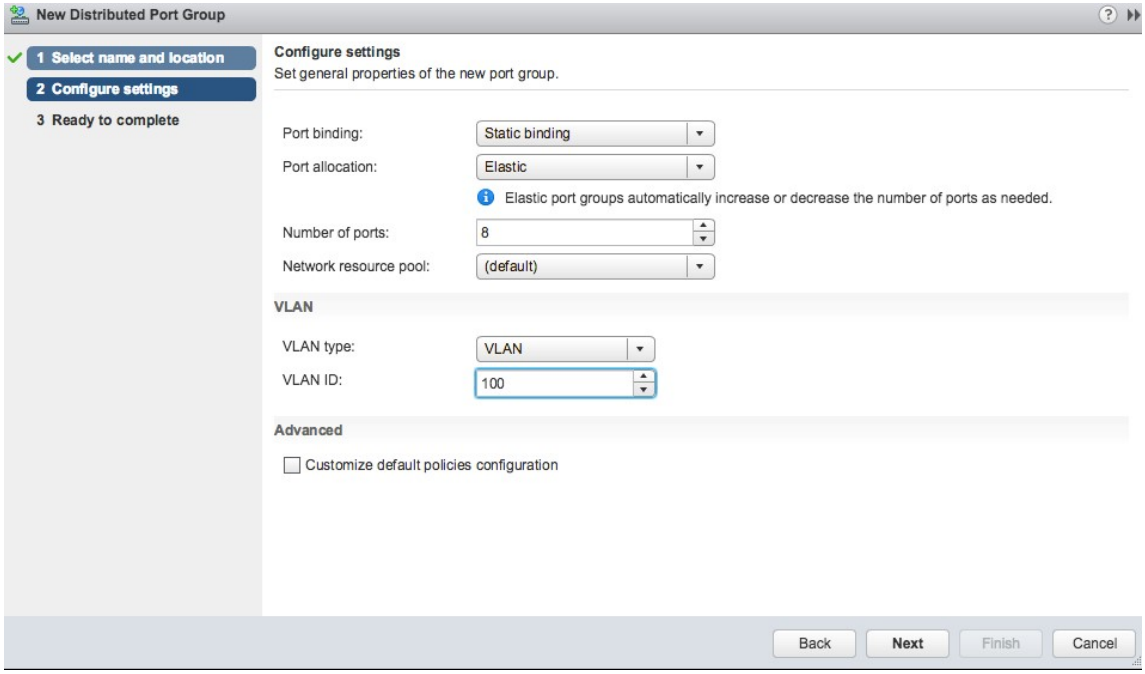
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

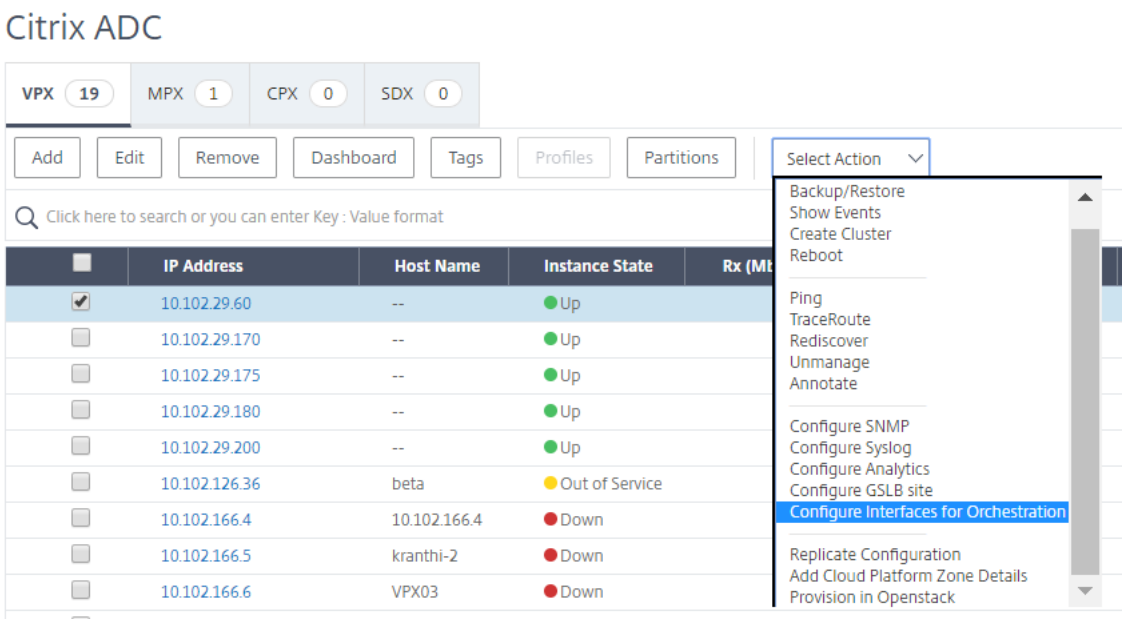


Hinzufügen der NetScaler ADC VPX Instanz in NetScaler ADM

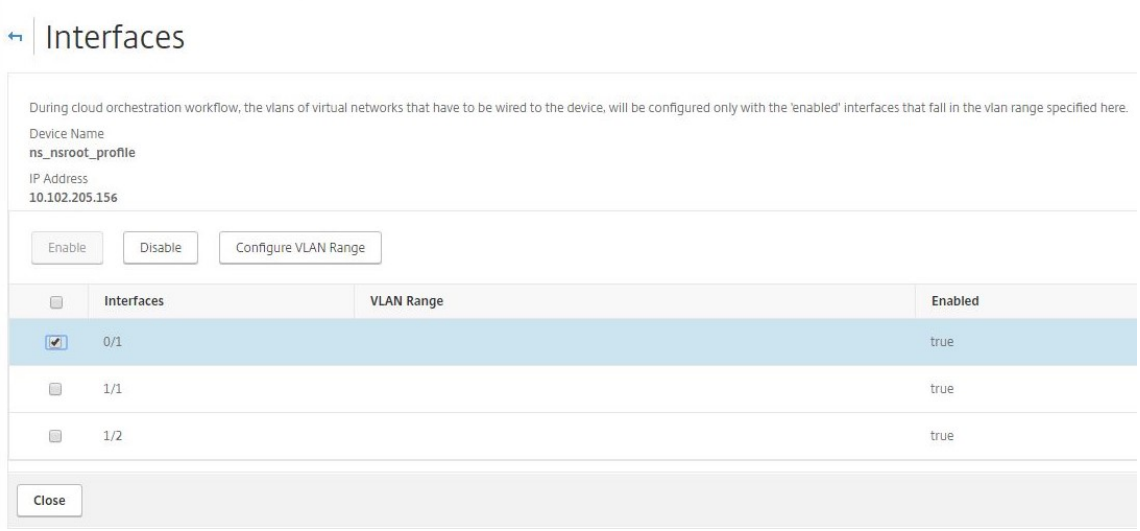
Fügen Sie Citrix ADC VPX Instanzen in Citrix ADM hinzu, und geben Sie den VLAN-Bereich der Trunked Group für jedes Gerät an.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

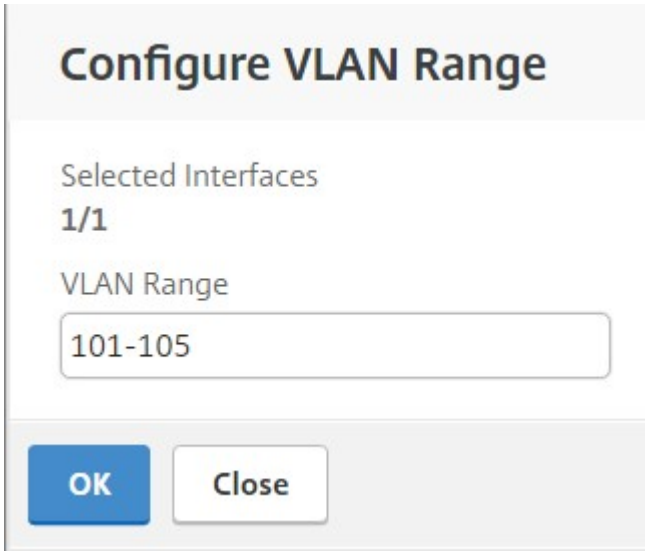


5. Wählen Sie auf der Seite **Schnittstellen** die Verwaltungsschnittstelle aus, und klicken Sie auf **Deaktivieren**, um die Bindung von VLAN an die Verwaltungsschnittstelle zu deaktivieren.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

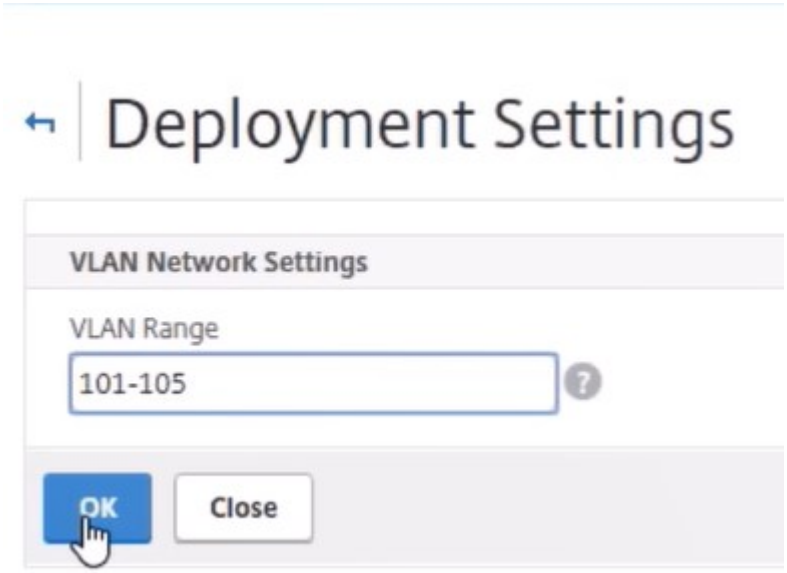


Registrieren von VMware NSX Manager bei NetScaler ADM

Registrieren Sie VMware NSX Manager bei Citrix ADM, um einen Kommunikationskanal zwischen ihnen zu erstellen.

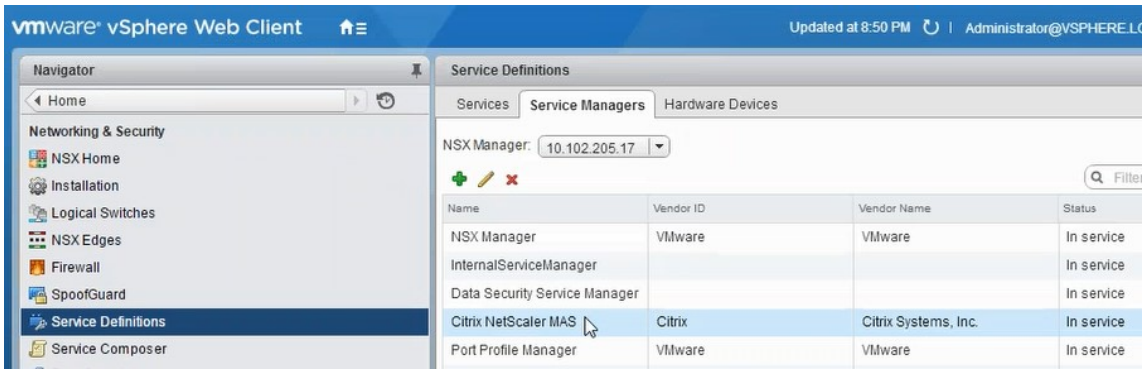
1. Navigieren Sie in NetScaler ADM in der Dropdownliste zu**Orchestration> SDN Orchestration**>**VMware NSX Manager**und klicken Sie auf**NSX Manager-Einstellungen konfigurieren**.
2. **Legen Sie auf der Seite NSX Manager-Einstellungen konfigurieren** die folgenden Parameter fest:
   a) NSX Manager-IP-Adresse: IP-Adresse von NSX Manager.
   b) NSX Manager-Benutzername - Administrativer Benutzername von NSX Manager.
   c) Kennwort - Kennwort des administrativen Benutzers von NSX Manager.
3. Legen **Sie im Abschnitt Citrix ADM-Konto, das von NSX Manager verwendet wird**, den Citrix ADC -Treiber-Benutzernamen und das Kennwort für 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.



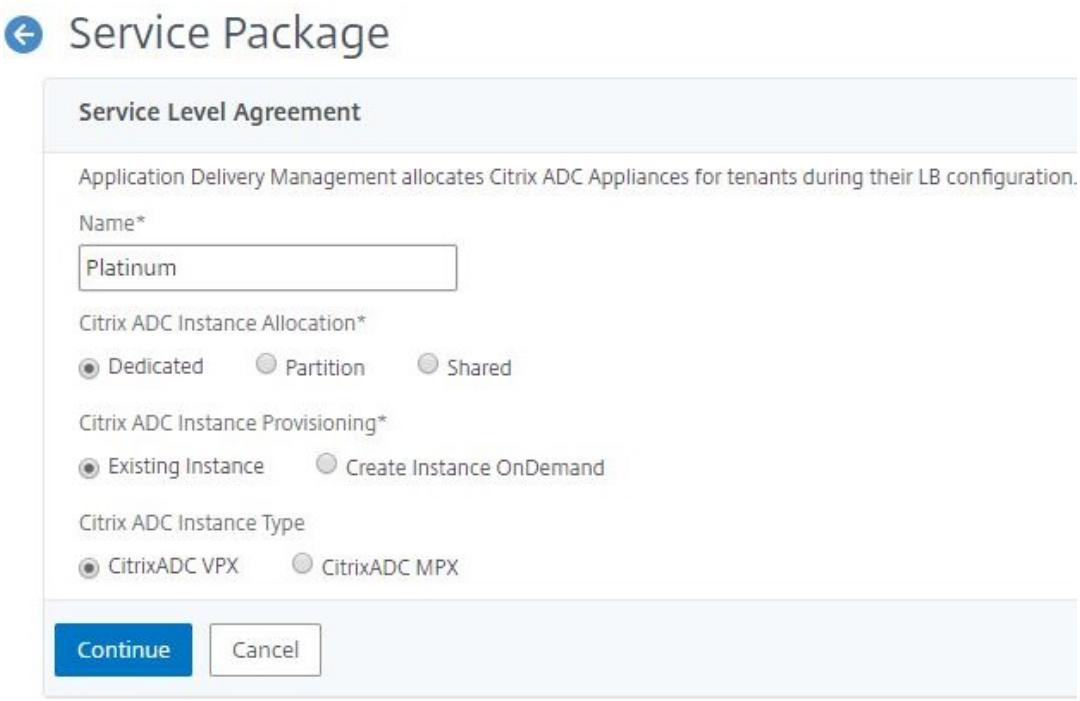
Erstellen eines Servicepakets in NetScaler ADM

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

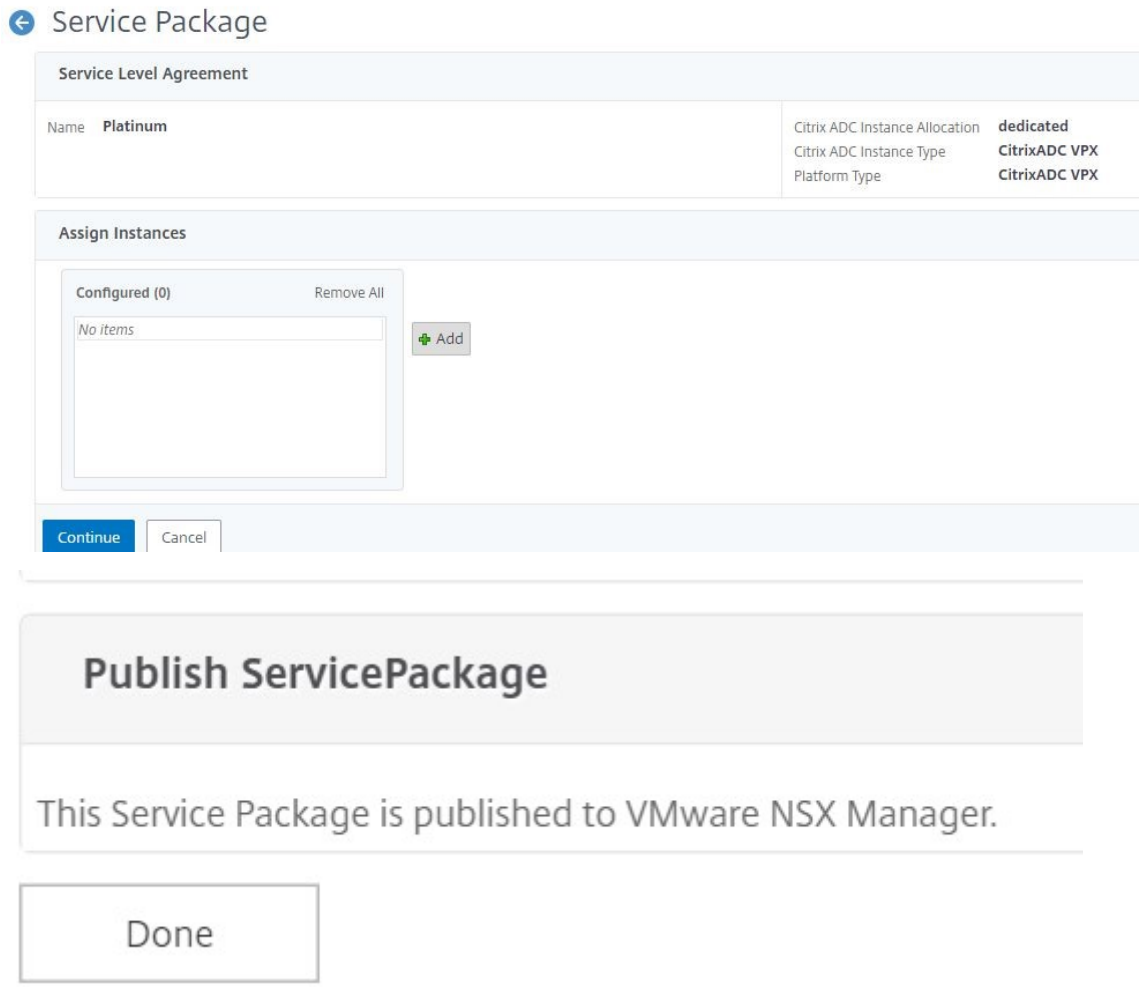
> **Hinweis**
>
> Diese Werte sind in dieser Version standardmäßig festgelegt und können nicht geändert werden.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.**

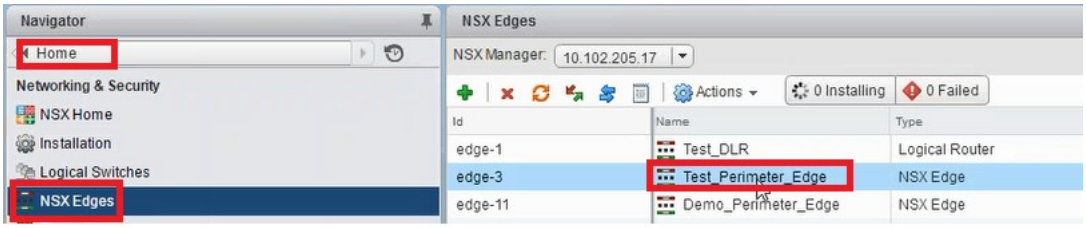
   Sie können sehen, dass das NetScaler ADM Dienstpaket registriert ist.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

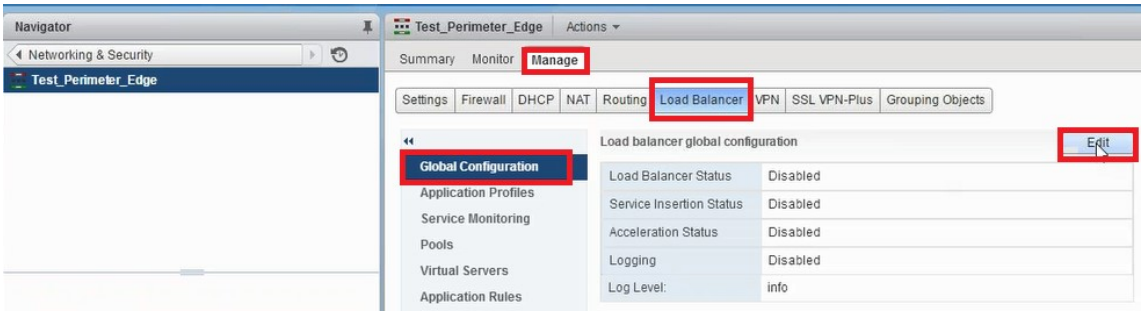
Ausführen des Lastausgleichsdiensteinfügens für Edge

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.

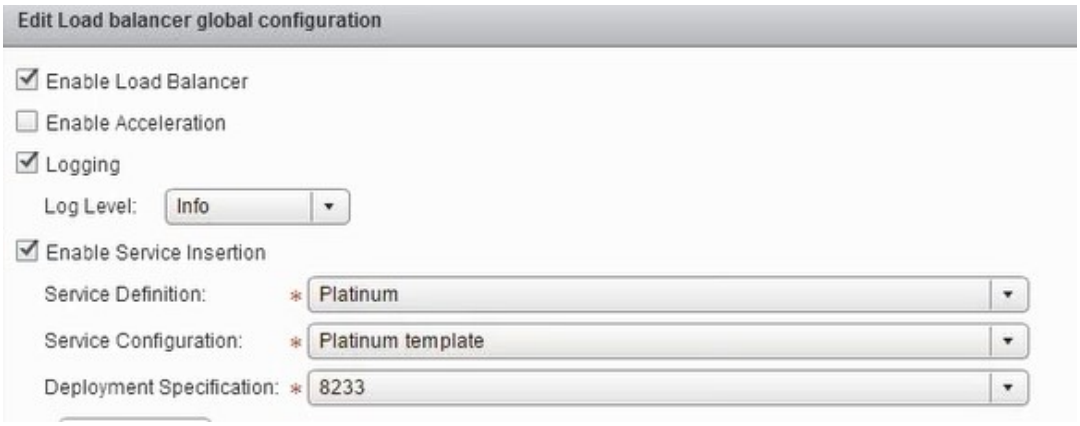


2. Klicken Sie auf **Verwalten**, wählen Sie auf der Registerkarte **Load Balancer** die Option **Globale Konfiguration** aus, und klicken Sie auf **Bearbeiten**.



3. Wählen Sie **Load Balancer aktivieren**, **Protokollierung**, **Diensteinfügung aktivieren** aus, um sie zu aktivieren.

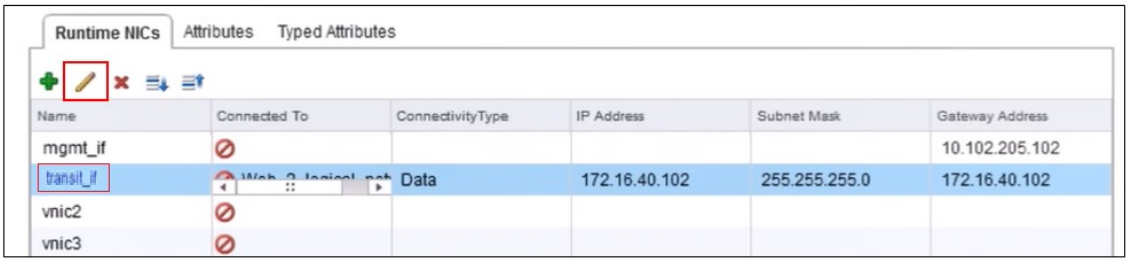
   a) Wählen Sie unter **Dienstdefinition** das Dienstpaket aus, das in NetScaler ADM erstellt und in NSX Manager veröffentlicht wurde.



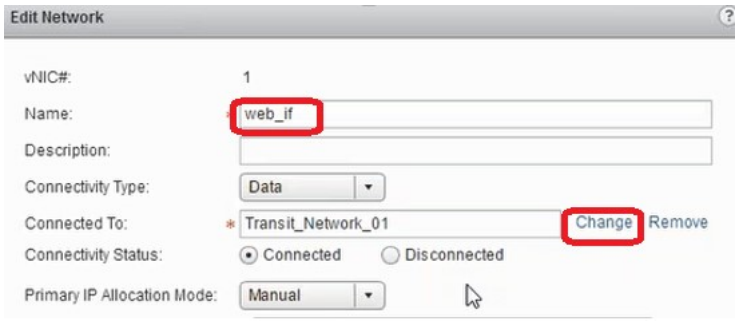
4. Wählen Sie die vorhandenen Laufzeit-NICs aus, und klicken Sie auf das Symbol Bearbeiten, um Laufzeit-NICs zu bearbeiten, die bei der Zuweisung von NetScaler ADC VPX verbunden werden

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

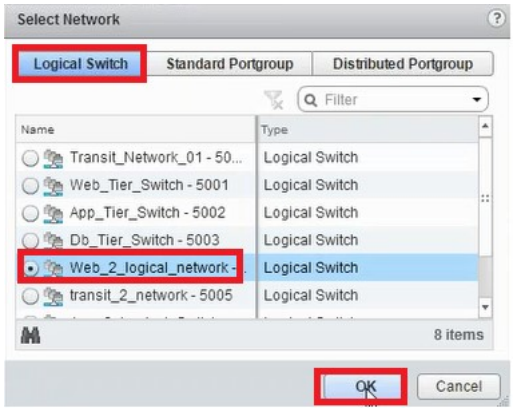
müssen.



5. Bearbeiten Sie den Namen der Netzwerkkarte, geben Sie Konnektivitätstyp als **Daten**an, und klicken Sie auf **Ändern**.



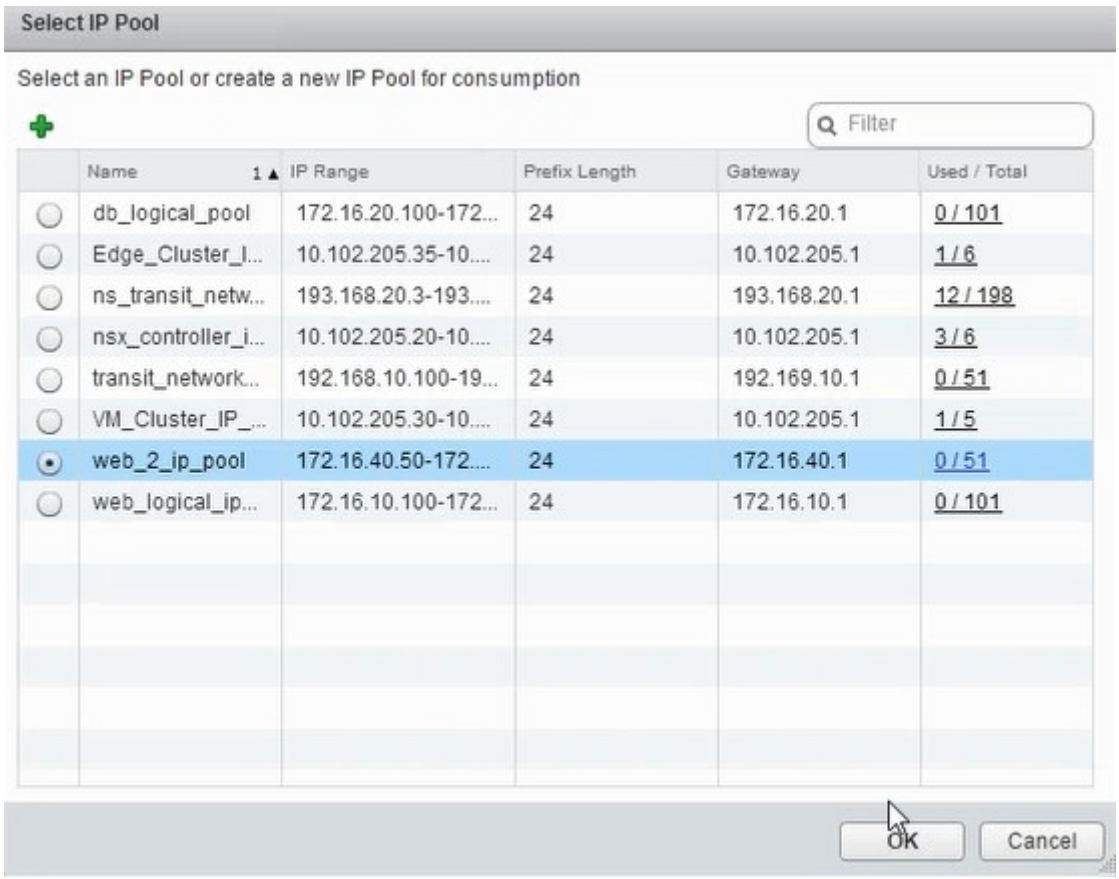
6. Wählen Sie den entsprechenden logischen Web-Switch aus.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. **Wählen Sie im Fenster IP-Pool** auswählen den entsprechenden IP-Pool aus, und klicken Sie auf **OK**.

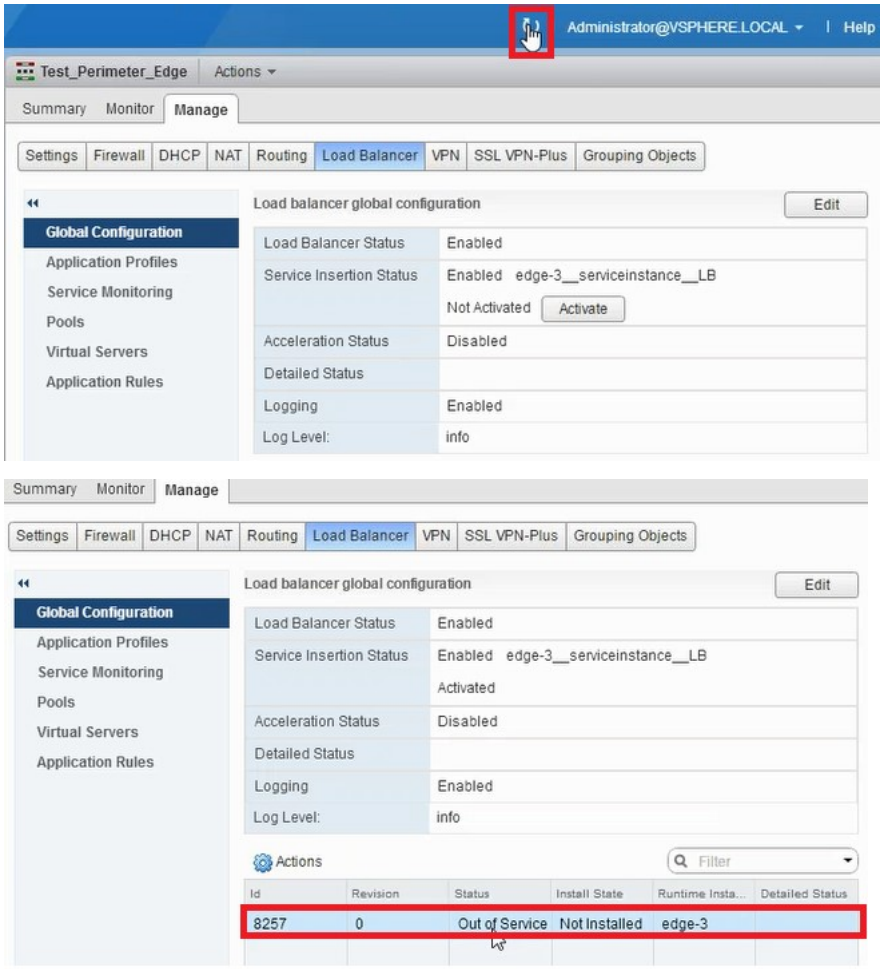


Die IP-Adresse wird erfasst und als Quellnetz-IP-Adresse in der NetScaler ADC VPX Appliance festgelegt. Im NSX Manager wird ein L2-Gateway erstellt, um das VXLAN dem VLAN zuzuordnen.

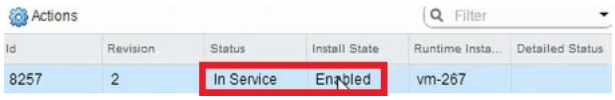
> **Hinweis:**
>
> Alle Datenschnittstellen sind als Laufzeit-NICs verbunden und sollten Teil der Schnittstellen für DLR sein.

9. Aktualisieren Sie die Ansicht, um die Erstellung der Laufzeit anzuzeigen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



10. Nachdem die VM gestartet wurde, ändert sich der Wert von Status **in In Dienst** und der Wert des Installationsstatus in **Aktiviert**.

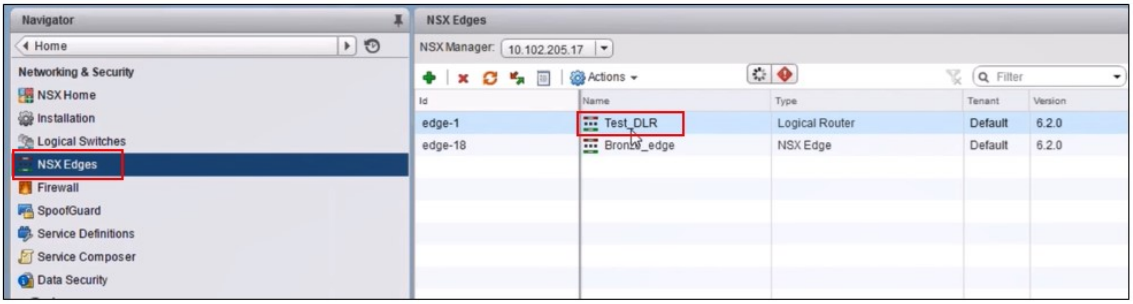


> **Hinweis:**Navigieren Sie
>
> in NetScaler ADM zu **Orchestration** > **Requests**, um Fortschrittsdetails zum Abschluss der LB-Diensteinfügung anzuzeigen.

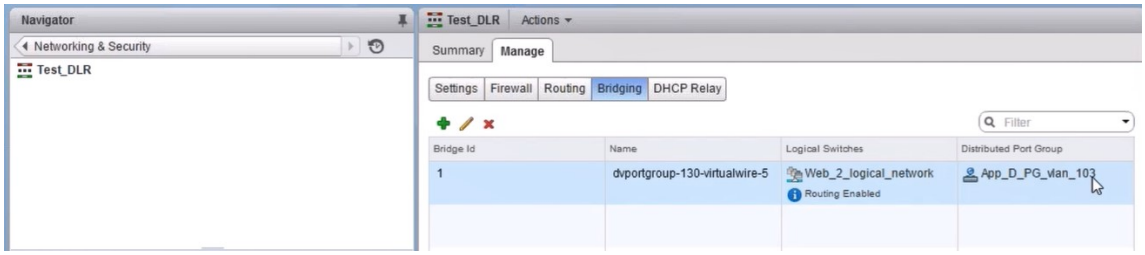
L2-Gateway auf NSX Manager anzeigen

1. Melden Sie sich beim NSX Manager auf vSphere Web Client an, navigieren Sie zu **NSX Edges**, und wählen Sie das erstellte DLR aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



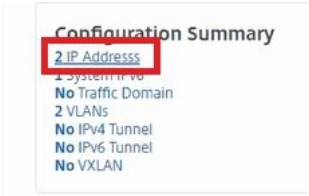
2. Navigieren Sie auf der DLR-Seite zu **Verwalten** > **Bridging**. Das L2-Gateway wird in der Liste angezeigt.



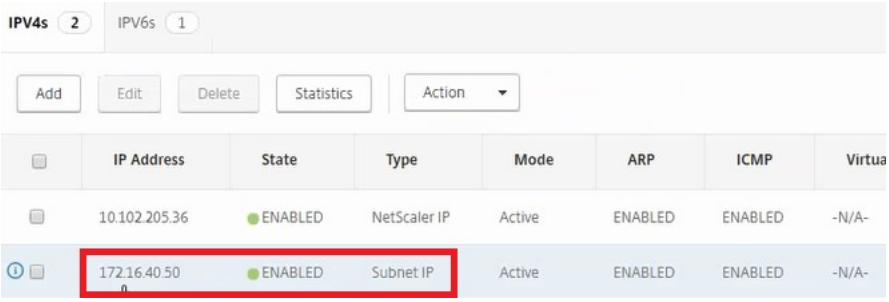
> **Hinweis**
>
> Ein L2-Gateway wird für jede Datenschnittstelle erstellt.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Navigieren Sie zu **Konfiguration** > **System** > **Lizenzen**, um die Lizenzen anzuzeigen, die auf diese Instanz angewendet werden.

Konfigurieren der Citrix ADC VPX Instanz mit StyleBook

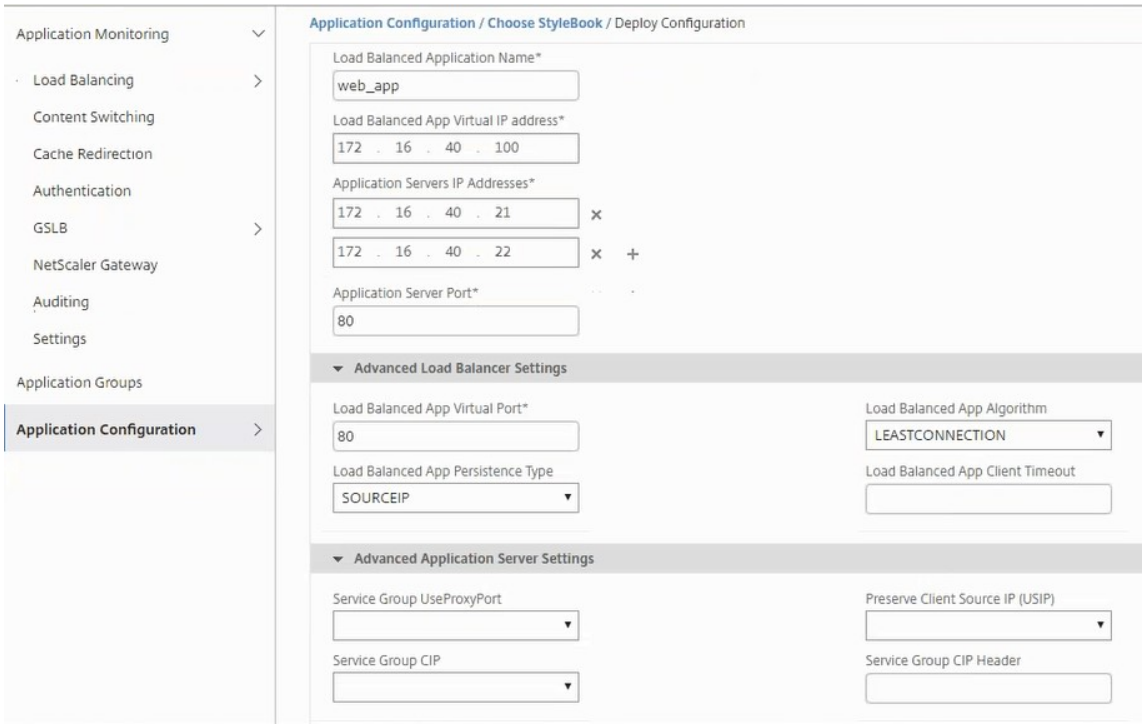
1. Navigieren Sie in NetScaler ADM zu **Orchestration** > **SDN Orchestration** > **NSX Manager konfigurieren** > **Edge-Gateways**.

   Notieren Sie sich die Citrix ADC Instanz-IP, die dem jeweiligen Edge-Gateway zugewiesen ist, auf dem die Load Balancing-Konfiguration über StyleBooks angewendet werden muss.

2. Erstellen Sie ein neues Stylesheft. Navigieren Sie zu **Anwendungen** > **Konfiguration** , importieren Sie das StyleBook und wählen Sie das Stylebook aus der Liste aus.

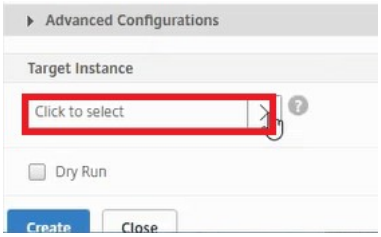
   Informationen zum Erstellen eines neuen Stylebooks finden Sie unter Erstellen Sie Ihr eigenes Stylebook .

3. Geben Sie Werte für alle erforderlichen Parameter an.

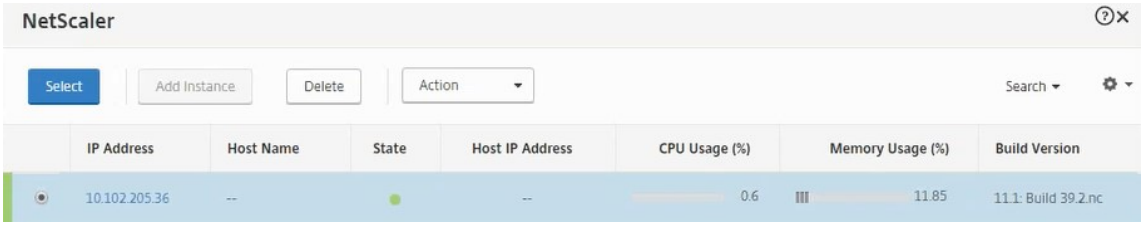


4. Geben Sie die NetScaler ADC VPX Instanz an, auf der diese Konfigurationseinstellungen ausgeführt werden sollen.

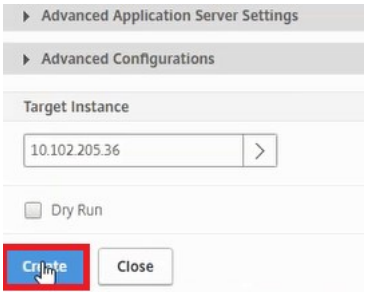
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. Wählen Sie die zuvor notierte IP-Instanz aus, und klicken Sie auf **Auswählen**.

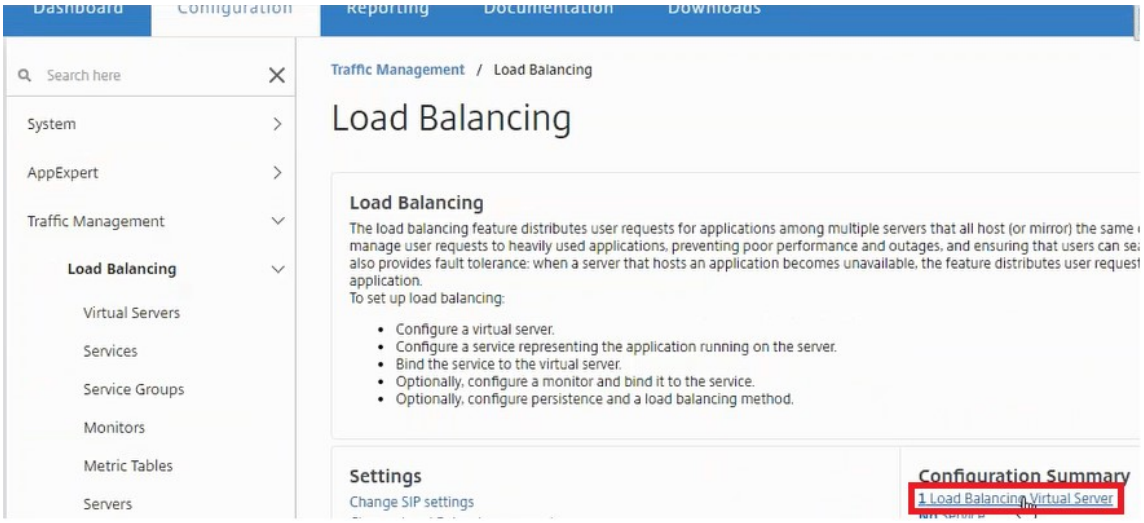


6. Klicken Sie auf **Erstellen**, um die Konfiguration auf das ausgewählte Gerät anzuwenden.



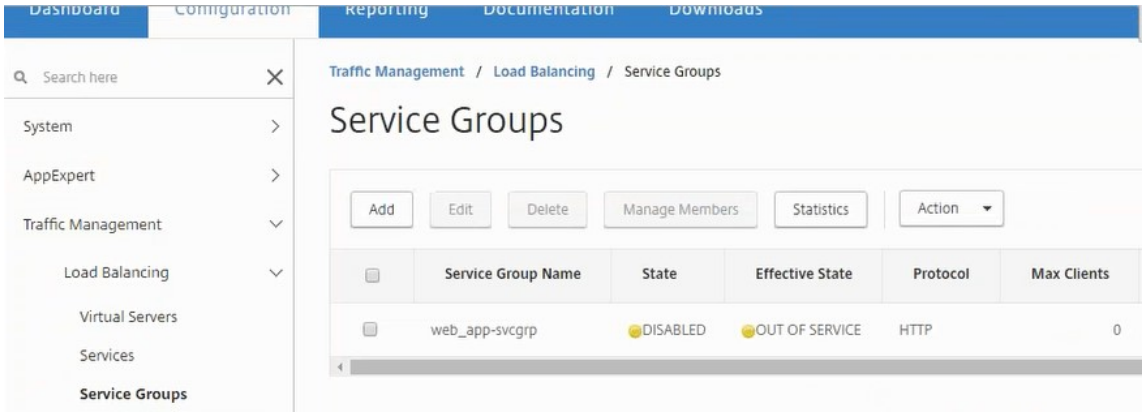
Load Balancer-Konfiguration anzeigen

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.

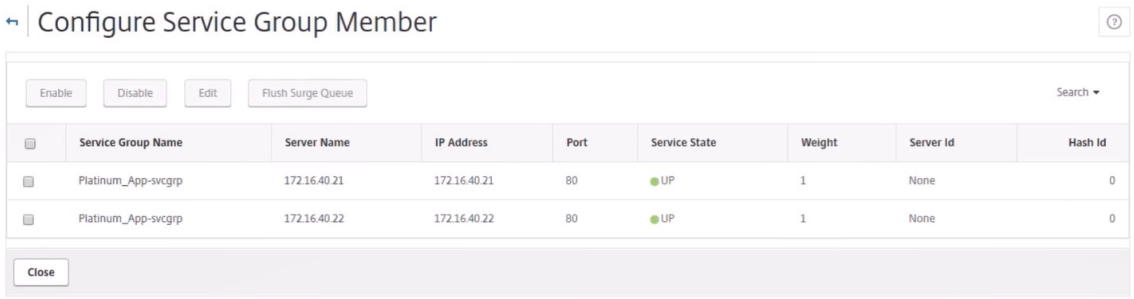


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

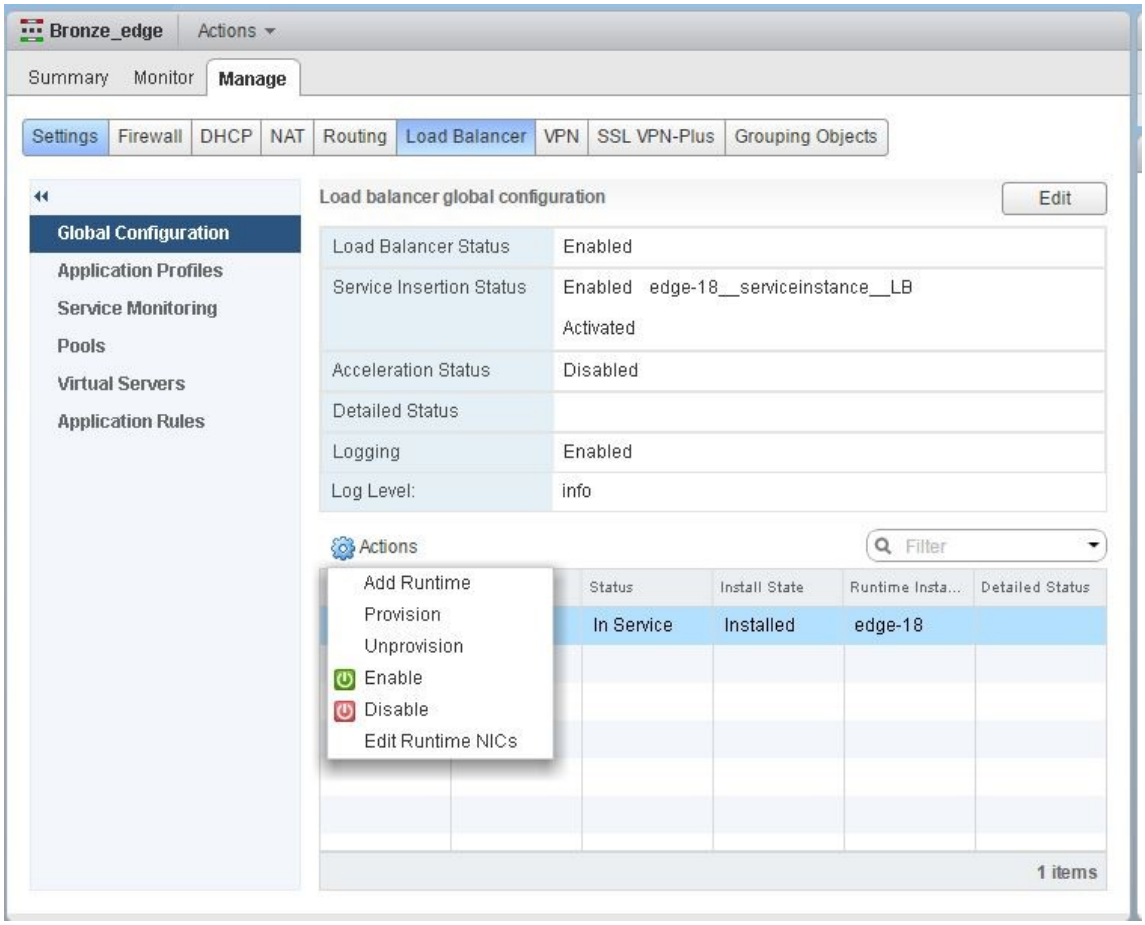


Löschen des Load Balancer-Dienstes

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 NetScler MAS entspricht Laufzeiteinträgen in NSX Manager.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 12.1 Setup in hoher Verfügbarkeit und auf ESX installiert.
- Citrix ADC VPX, Version 12.1
- Citrix ADC VPX -Lizenzen für Citrix ADC VPX Instanzen, Version 12.1
- 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.

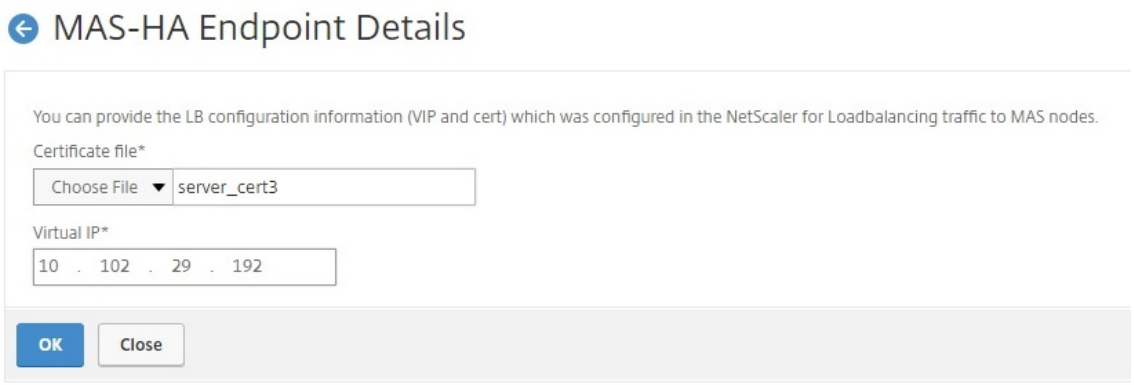
So stellen Sie Konfigurationsinformationen für den Lastausgleich in Citrix ADM bereit:

1. Navigieren Sie im Citrix ADM HA-Knoten zu **System** > **Bereitstellung**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) NSX Manager-Benutzername - Administrativer Benutzername 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**.

Laden Sie Lizenzen in Citrix ADM hoch

Laden Sie die NetScaler ADC VPX -Lizenzen in NetScaler ADM hoch, damit NetScaler ADM den Instanzen während der Orchestrierung mit NSX automatisch Lizenzen zuweisen kann.

So installieren Sie Lizenzdateien auf NetScaler ADM:

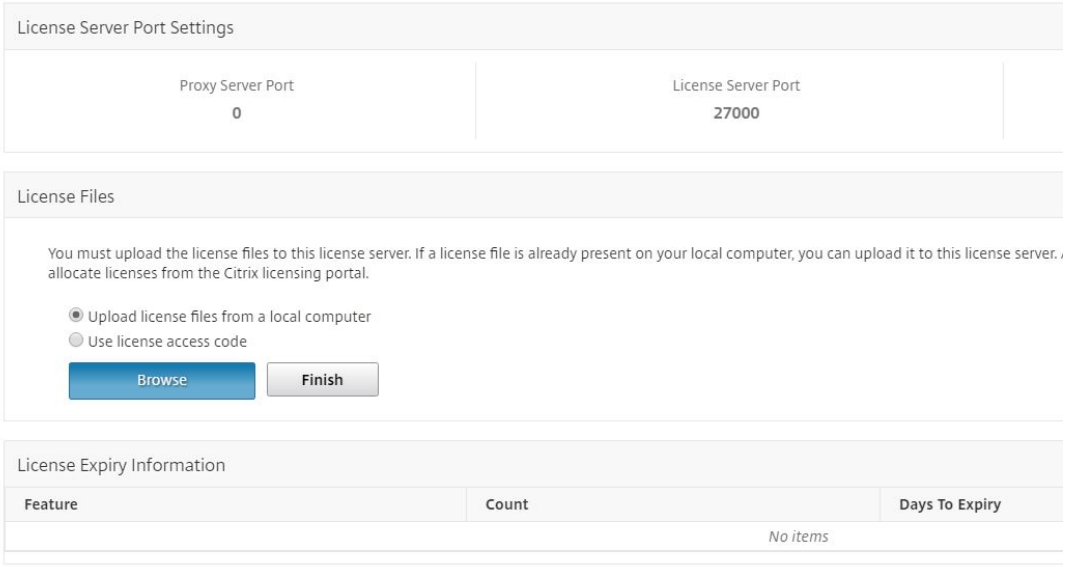
1. Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Lizenzen.**
2. Wählen Sie im Abschnitt **Lizenzdateien** eine der folgenden Optionen aus:

   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) **Lizenzzugriffscode verwenden** : Citrix sendet den License Access Code (LAC) für die erworbenen Lizenzen per E-Mail. Um Lizenzdateien hinzuzufügen, geben Sie den LAC in das Textfeld ein und klicken Sie dann auf **Lizenzen** abrufen.

   > **Hinweis:**Sie können dem NetScaler ADM
   >
   > jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Laden Sie Citrix ADC VPX-Bilder in Citrix ADM hoch

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-Bilder 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 Sie Servicepakete 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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

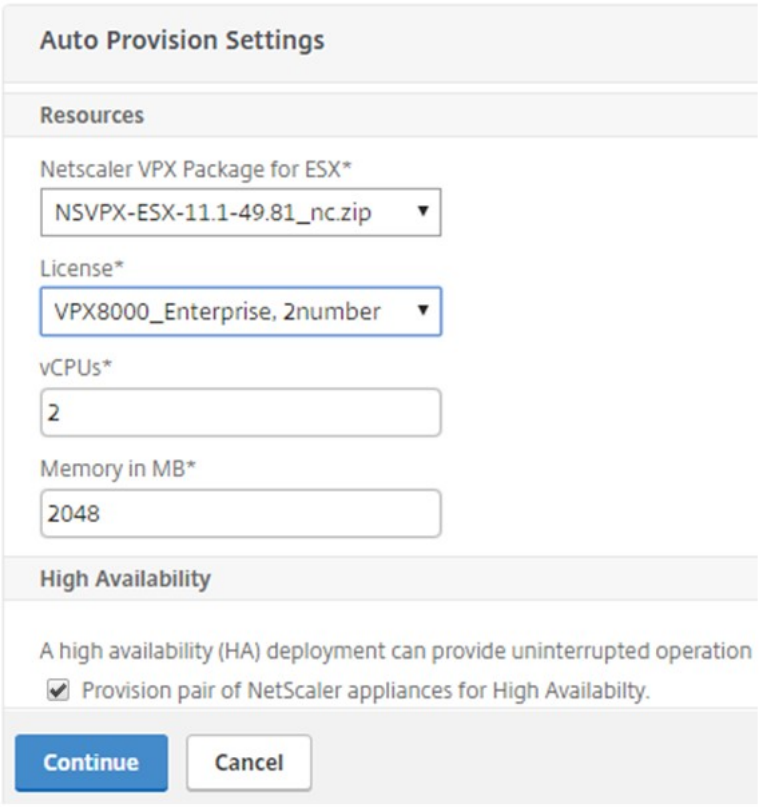
c) Citrix ADC Instanz Provisioning: Wählen Sie **Instanz bei Bedarf erstellen**.

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 im Listenfeld in der obigen Abbildung angezeigt wird, VPX8000_Enterprise, 2number, ist ein Beispiel und wird wie folgt erklärt:
>
> - VPX: Die Lizenz besteht darin, NetScaler ADC VPX Instanzen bereitzustellen.
> - 8000 —Die verbrauchbare Bandbreite beträgt 8 GB
> - Enterprise —Citrix bietet drei Lizenztypen an: Standard, Enterprise und Platinum

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - 2number: Mit dieser Lizenz können zwei NetScaler ADC VPX Instanzen 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.

Führen Sie das Einfügen des Load Balancer-Dienstes für Edge durch

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.

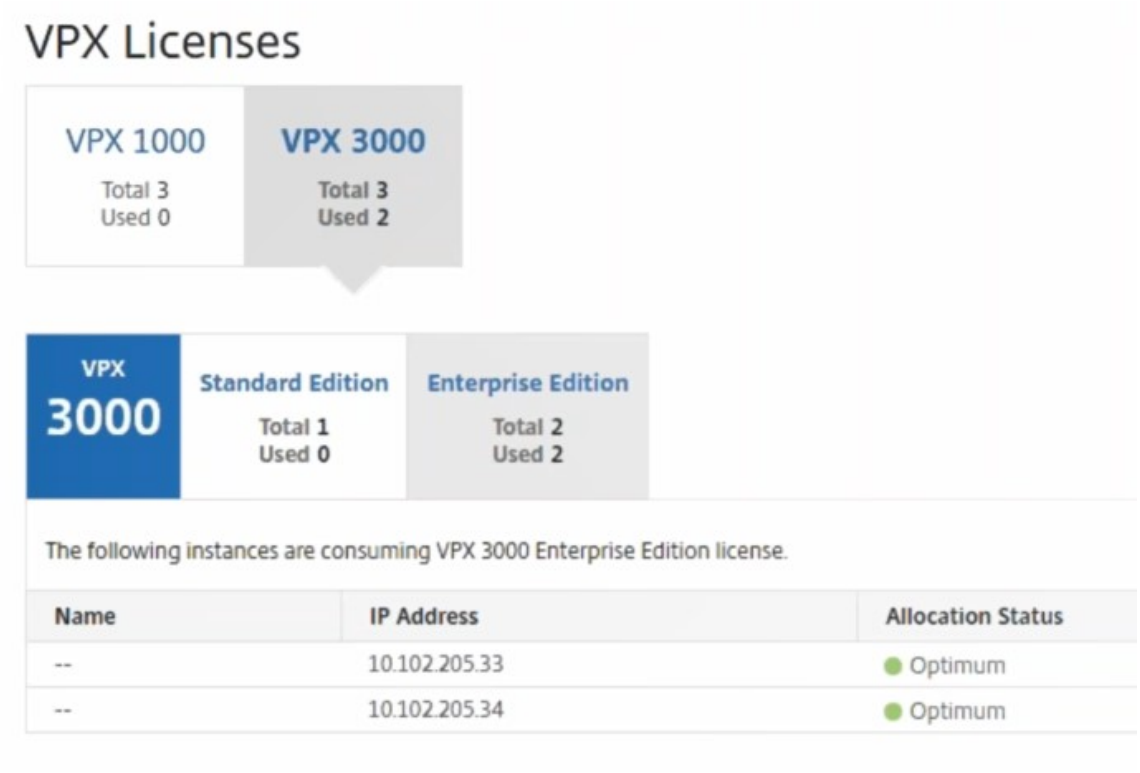
10. Navigieren Sie in Citrix ADM zu **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge-Gateways**. Im rechten Seitenbereich können Sie anzeigen, dass Citrix ADC VPX dem NSX Edge Gateway hinzugefügt wurde.

    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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wenn die Diensteinfügung abgeschlossen ist, können Sie StyleBooks verwenden, um die NetScaler ADC Instanzen mit einer der folgenden beiden Methoden zu konfigurieren:

- Konfigurieren Sie die Load Balancing-Dienste auf Citrix ADC VPX in der VMware NSX Manager-GUI
- Konfigurieren Sie die Load Balancing Services auf Citrix ADC VPX in der Citrix ADM GUI

Konfigurieren Sie die Load Balancing-Dienste auf Citrix ADC VPX in der 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

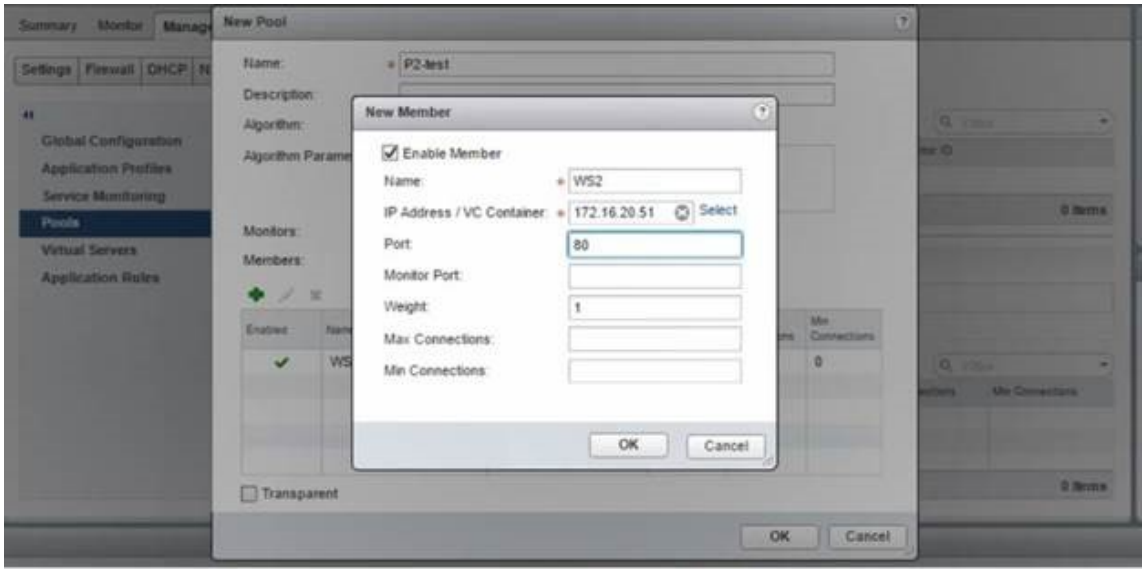
d) Mitglieder —Klicken Sie auf „+“, um Mitglieder zum Pool hinzuzufügen, und geben Sie die erforderlichen Parameter in das Fenster Neues Mitglied ein.

   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.



Virtuelle Server erstellen

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.

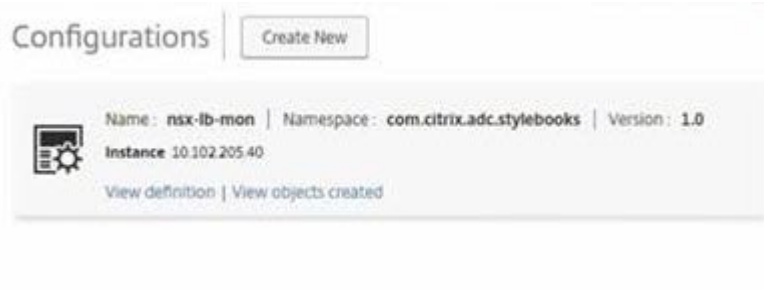
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix ADM zu **Anwendungen** > **Konfiguration**, und überprüfen Sie, ob das Konfigurationspaket "nsx-lb-mon"erstellt wurde.



Konfigurieren Sie die Load Balancing Services auf Citrix ADC VPX in der Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Überprüfen Sie die Erstellung virtueller Server und Dienstgruppen in Citrix ADC VPX-Instanzen

Sie können sehen, 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-Dienste 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 die entsprechende Zuordnung des Edge-Gateway zu gelöschter Instanz nicht vorhanden sein sollte.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

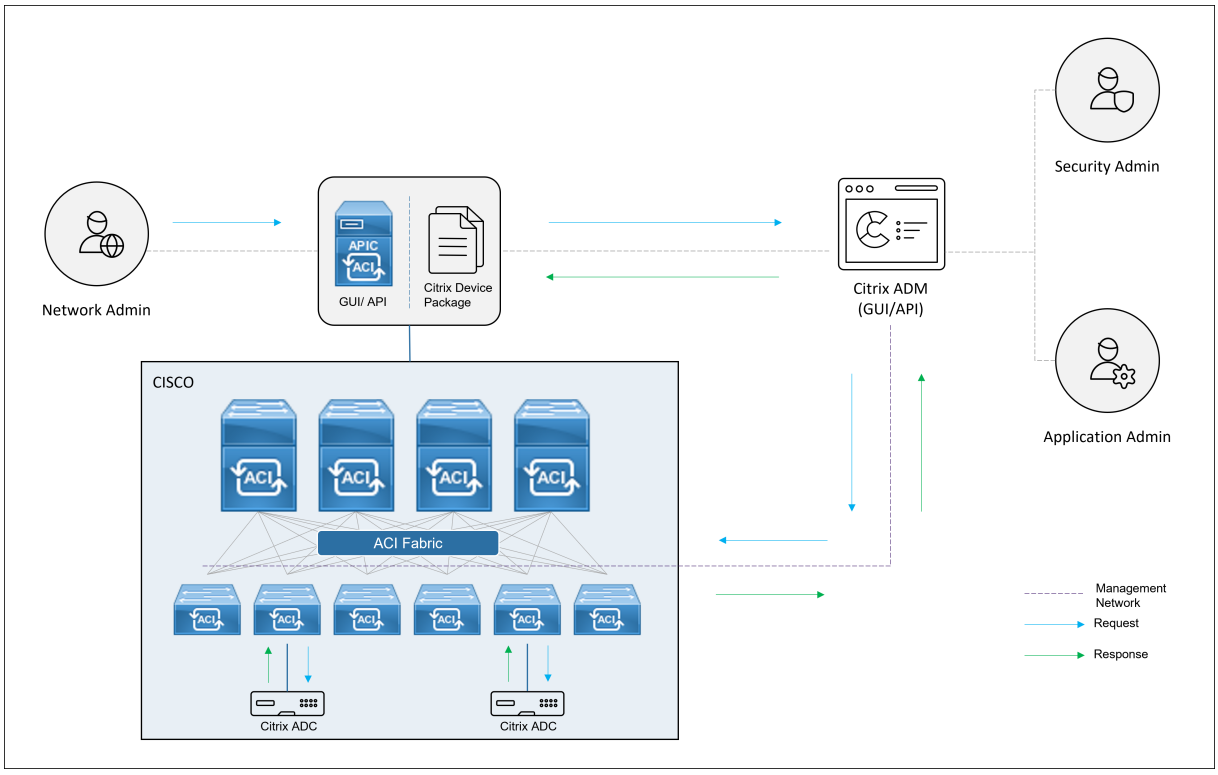
NetScaler ADC Automatisierung mit NetScaler ADM im Cisco ACI-Hybridmodus

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:

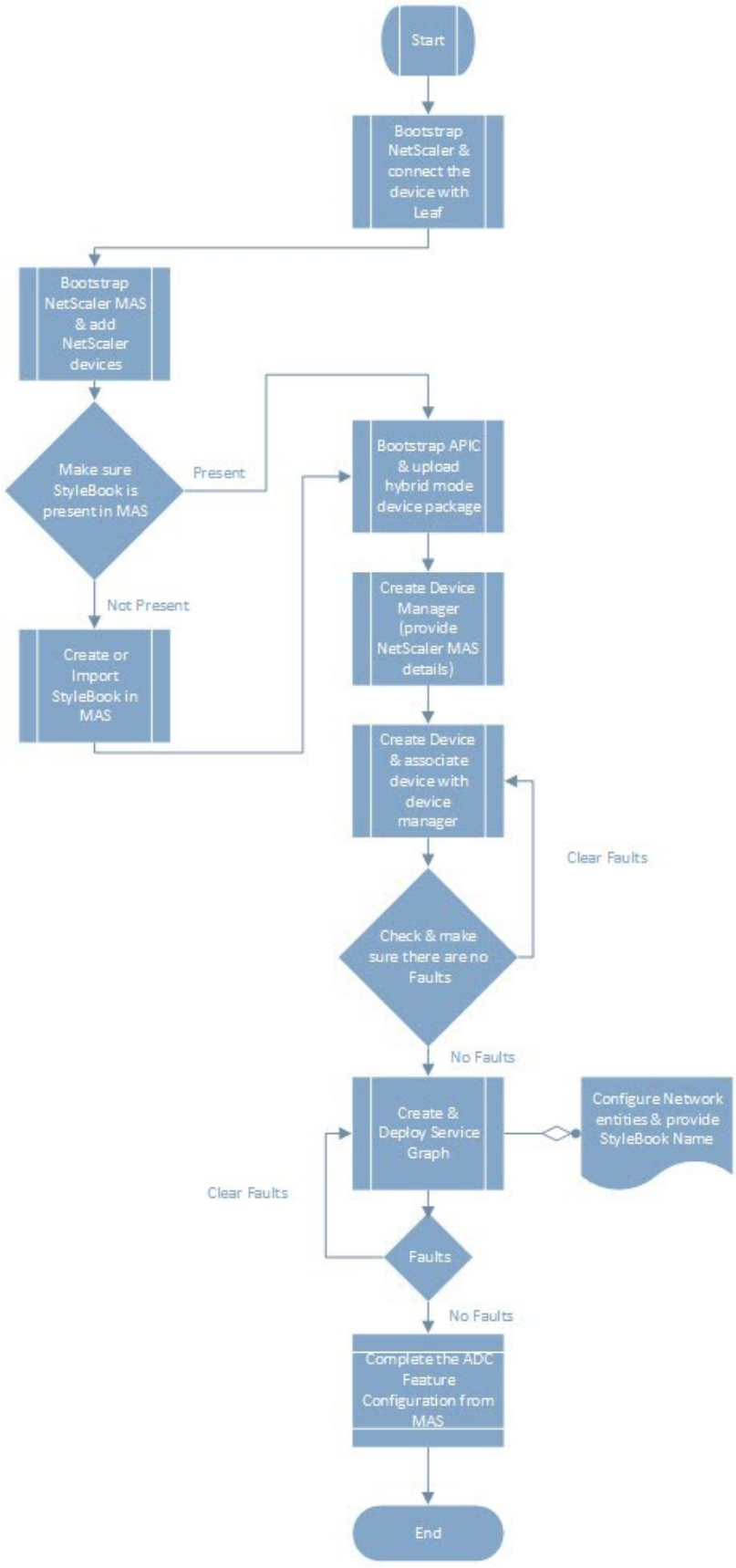
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen

February 5, 2024

Stellen Sie sicher, dass:

- 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 Citrix ADM 12.1 .
- 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

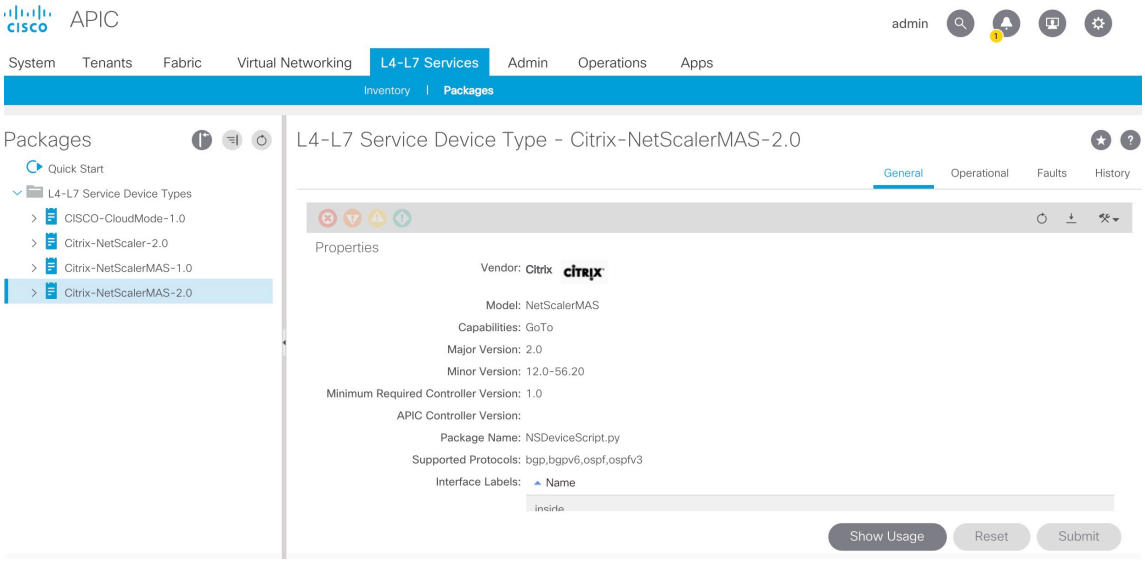
> **Hinweis**
>
> Das Gerätepaket im Hybridmodus kann mit einem Gerätepaket im vollständig verwalteten Modus koexistieren.

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.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

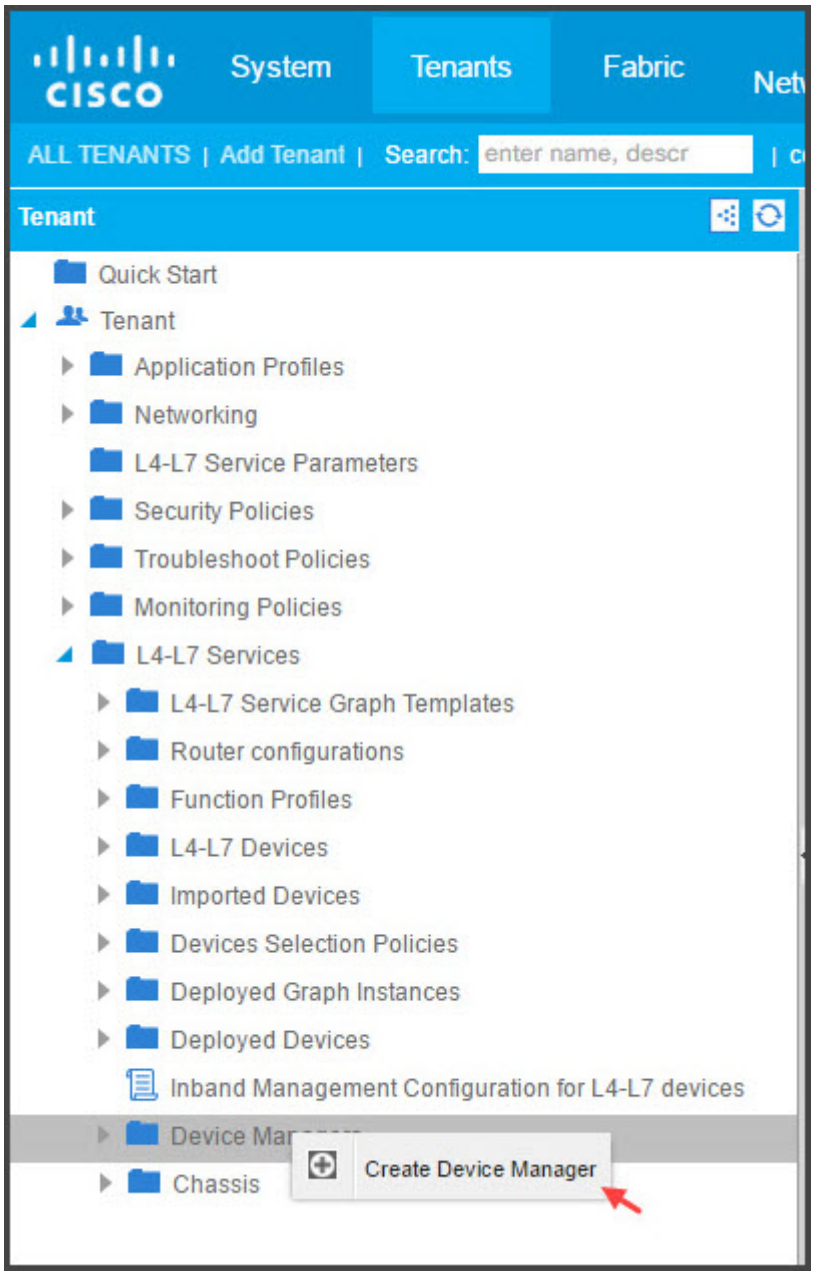
Citrix Application Delivery Management (ADM) fungiert als zentralisierter Geräte-Manager für Citrix ADC, der auf Cisco ACI bereitgestellt wird. Sie müssen Citrix ADM als Geräte-Manager im Cisco APIC hinzufügen.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

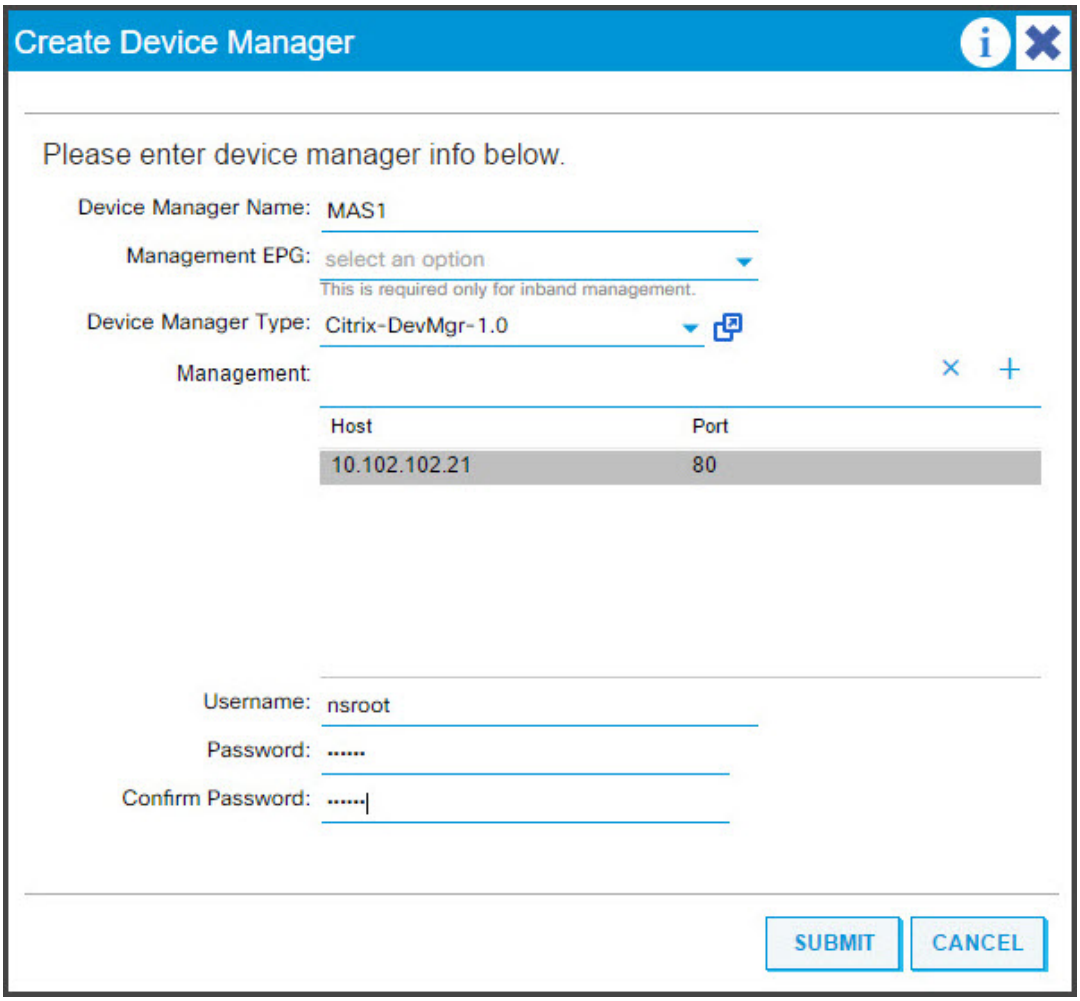
c) Wählen Sie in der Dropdownliste **Geräte-Manager-TypCitrix-Devmgr-1.0**aus.

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.

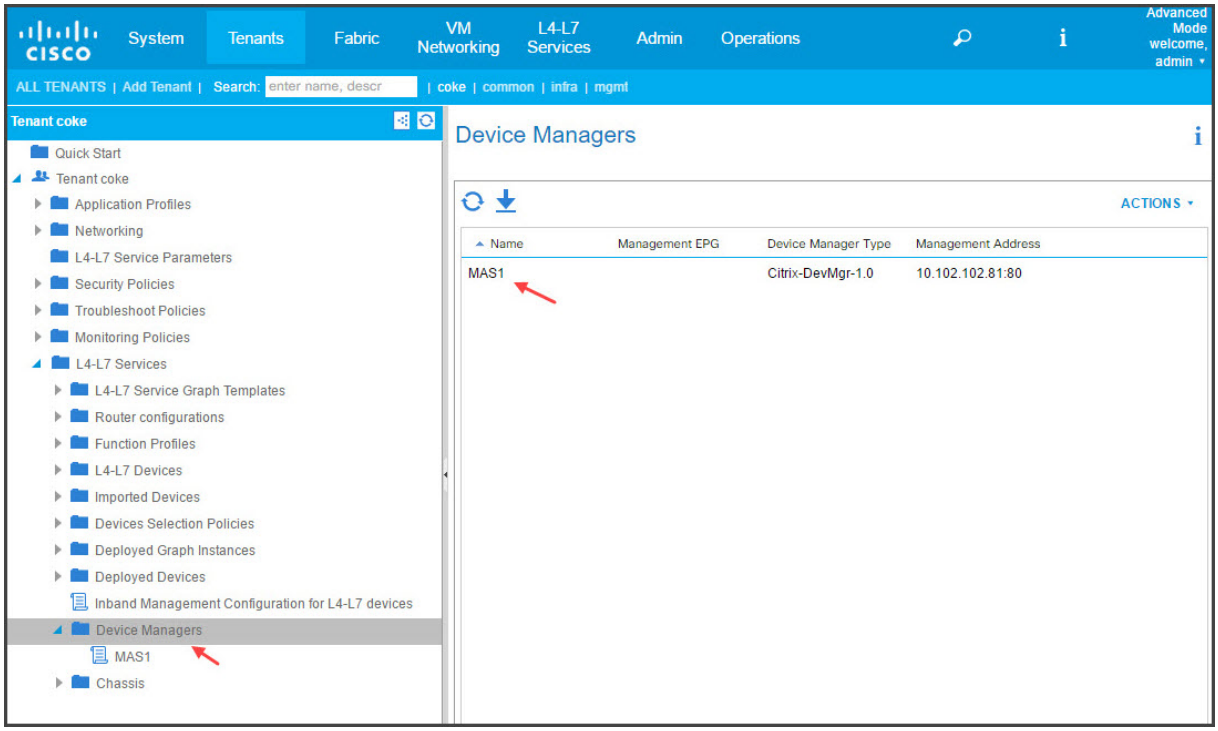
f) Geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** das Kennwort für den Zugriff auf Citrix ADM ein.

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.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

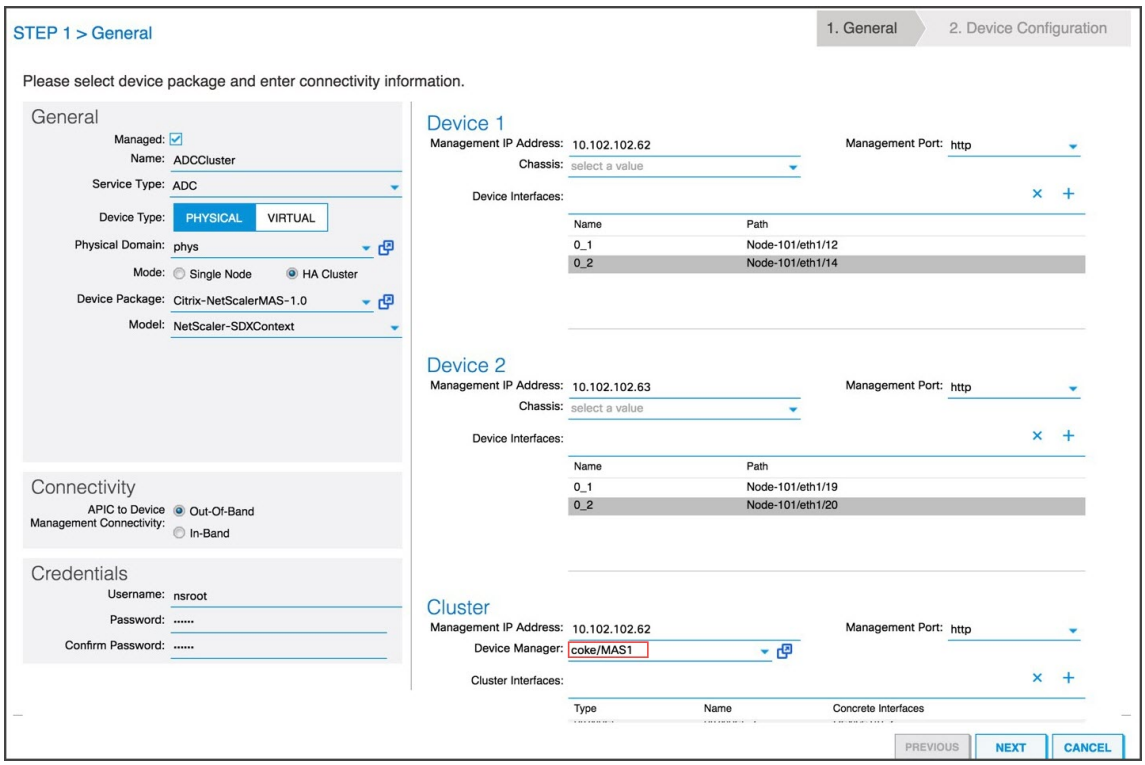
1. Wechseln Sie in der Menüleiste zu **Mandanten > Alle Mandanten**.
2. Doppelklicken Sie im **Arbeitsbereich** auf den Namen des Mandanten.
3. Wählen Sie im **Navigationsbereich*tenant_name* > L4-L7-Dienste > L4-L7-Geräte aus.**
4. Wählen Sie im Arbeitsbereich **Aktionen > L4-L7-Geräte erstellen**aus.
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

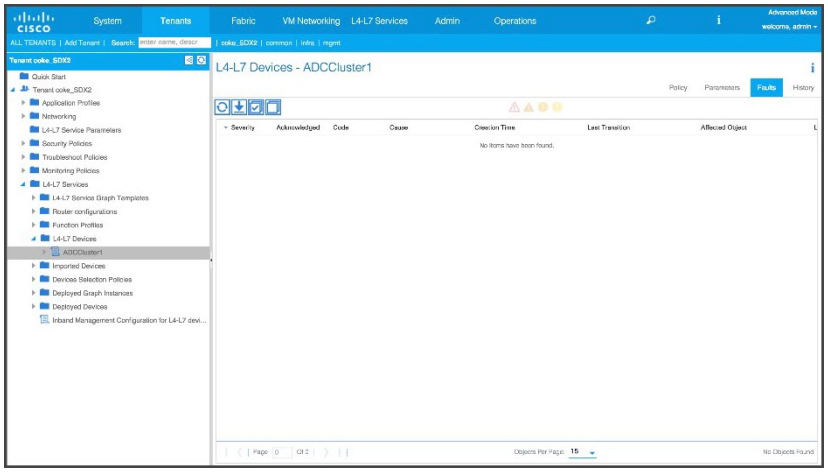
8. Füllen Sie im Abschnitt **Gerät 1bzw. Gerät 2** die verwaltungsbezogene Konfiguration aus.
9. Führen Sie im Abschnitt **Cluster** die verwaltungbezogene Konfiguration für den Cluster aus. Stellen Sie sicher, dass Sie in der Dropdownliste **Geräte-Manager** den Geräte-Manager auswählen, den Sie unter 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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"/>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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/
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            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:

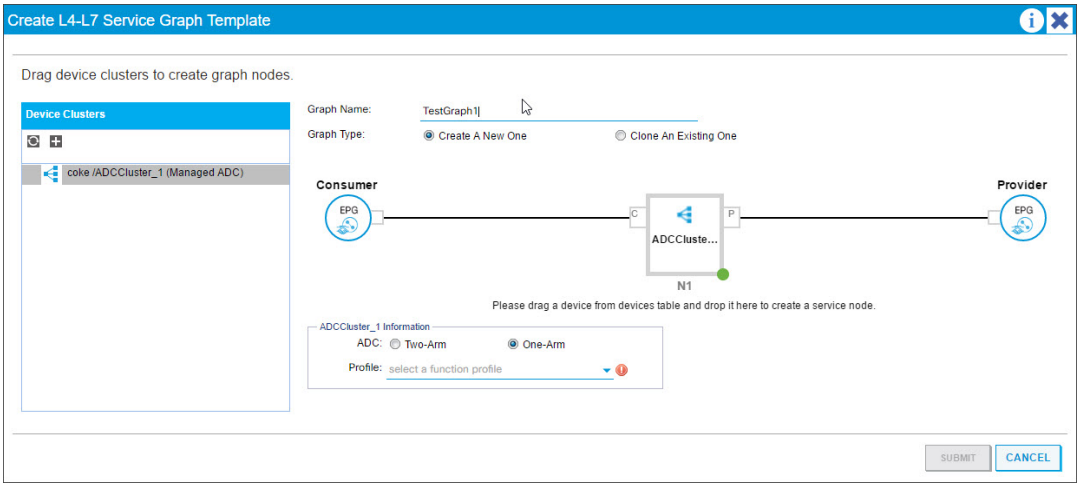
1. Wechseln Sie in der Menüleiste zu **Mandanten > Alle Mandanten**.
2. Doppelklicken Sie im **Arbeitsbereich** auf den Namen des Mandanten.
3. Wählen Sie im **Navigationsbereich*tenant_name* > L4-L7 Services > L4-L7 Service Graph Templates aus.**
4. Wählen Sie im **ArbeitsbereichAktionen > Eine L4-L7-Service 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

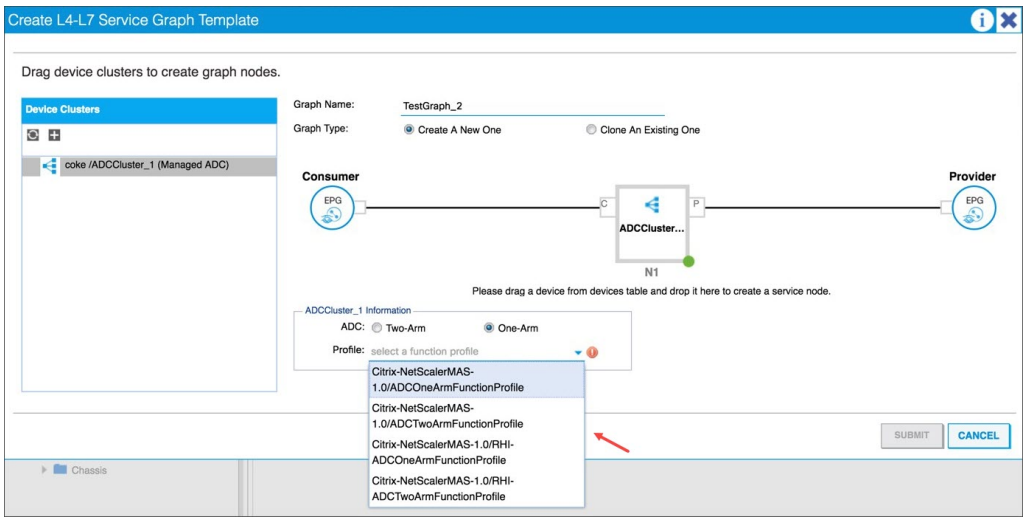
c) Ziehen Sie das **Gerät aus dem Abschnitt Gerätecluster** per Drag-and-Drop zwischen die Endpunktgruppe für Verbraucher und die Endpunktgruppe des Anbieters, um einen Dienstknoten zu erstellen.



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.

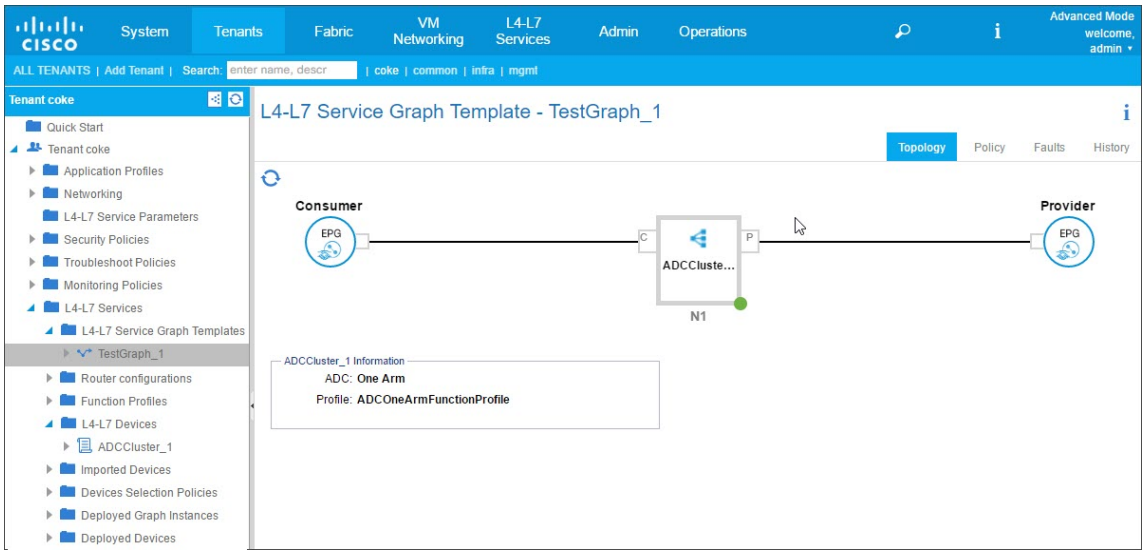


iii. Klicken Sie auf **SENDEN**.

6. Klicken Sie im **Navigationsbereich** auf die Service-Graph-Vorlage. Der Bildschirm zeigt eine grafische Topologie der Service-Graph-Vorlage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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.



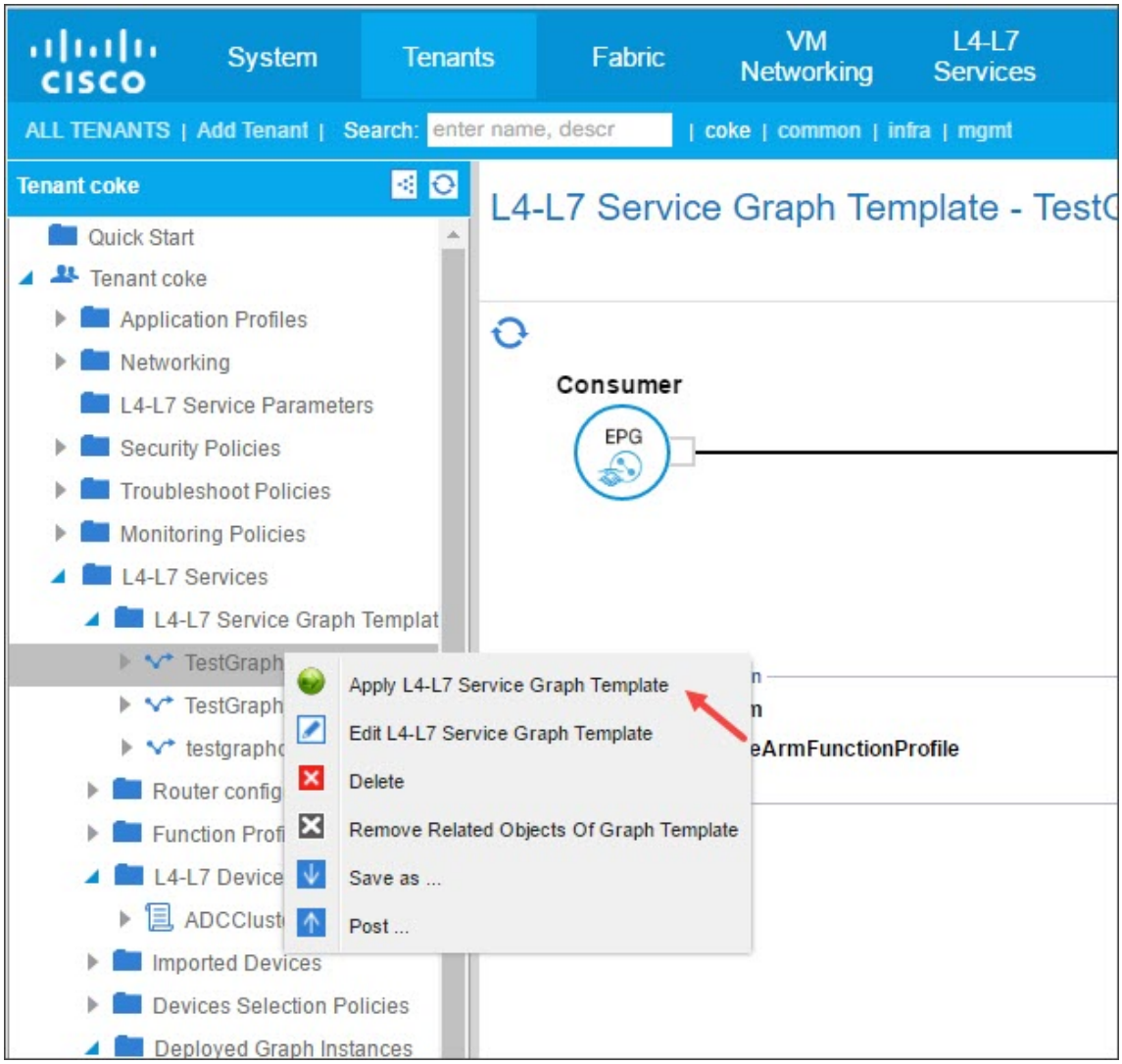
Anwendung der Service Graph-Vorlage auf Endpunktgruppen

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



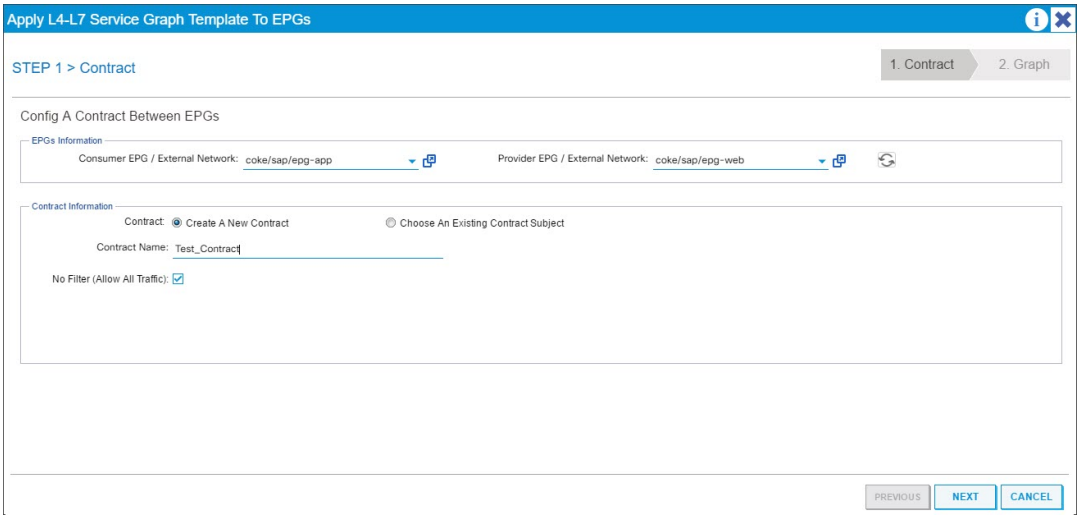
5. Füllen **Sie im Dialogfeld „L4-L7-Service Graph-Vorlage auf EPGs anwenden** “im Abschnitt „ **EPG-Informationen** “die folgenden Felder aus:

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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:

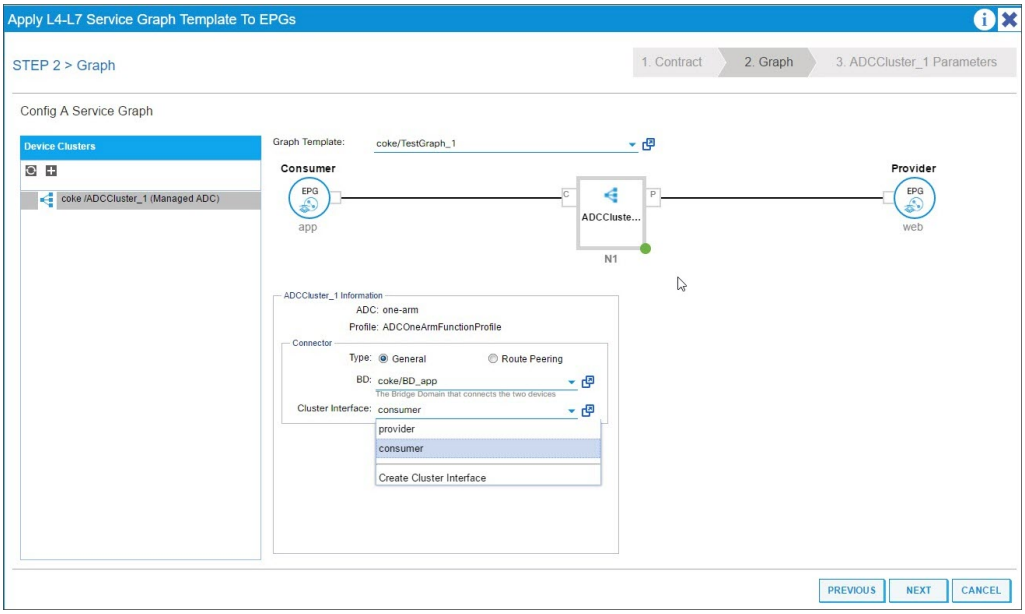
   i. Wählen Sie im Feld **Typ** die Option Allgemein aus.

   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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

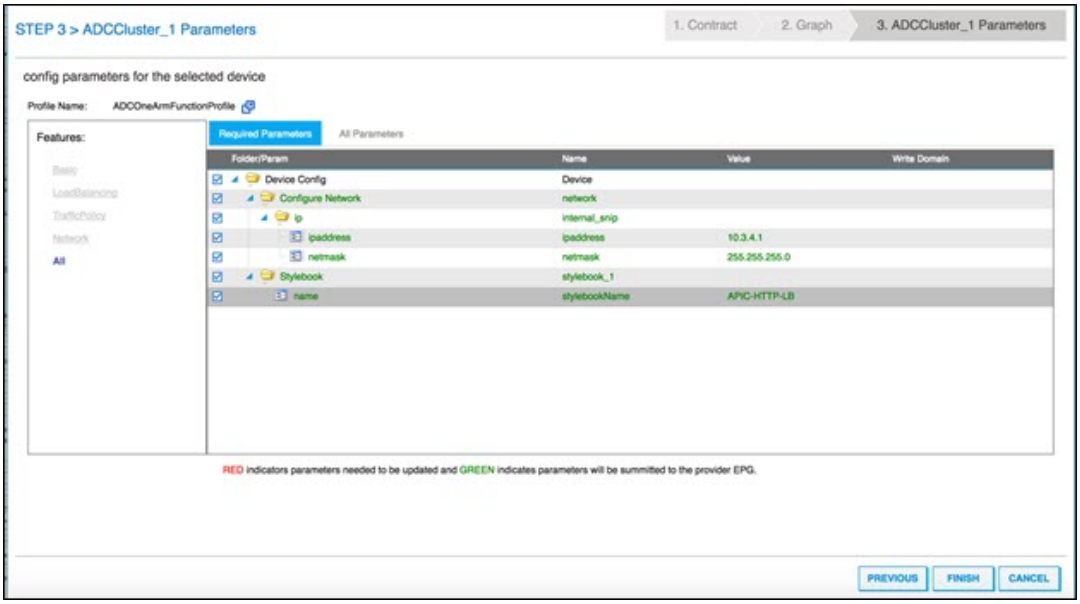


iv. Klicken Sie auf **Weiter**.

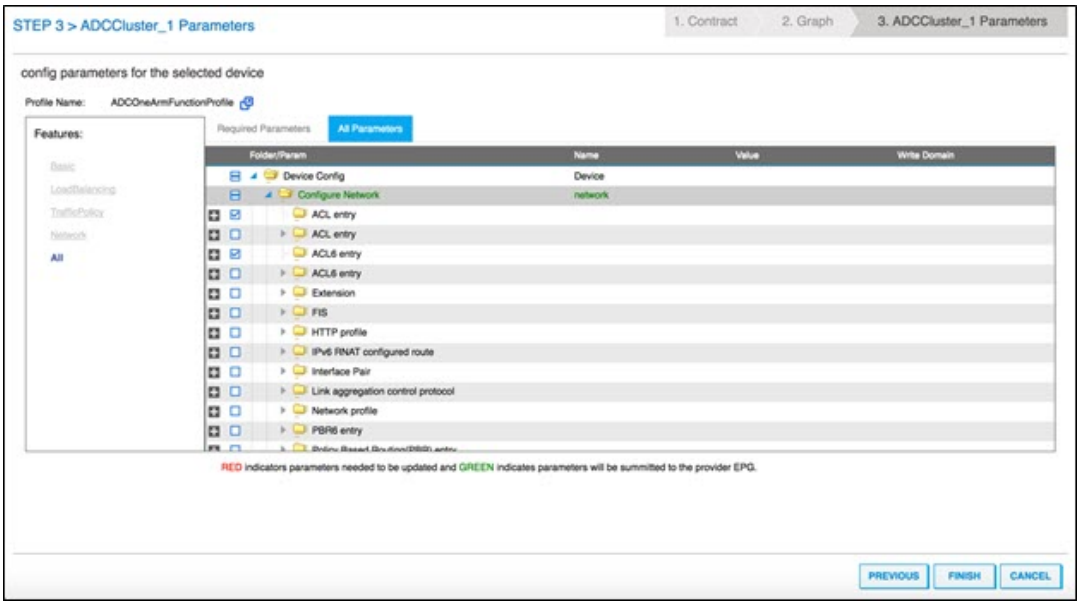
Geben Sie auf dem Bildschirm **Parameter** auf der Registerkarte **Erforderliche Parameter** die L2-L3-spezifischen Details ein, z. B. die IP-Adresse, die für das Profil vorgeschrieben ist. Der andere Schlüsselparameter ist der StyleBook-Name. Dies kann das integrierte StyleBook **APIC-HTTP-LB** sein, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.



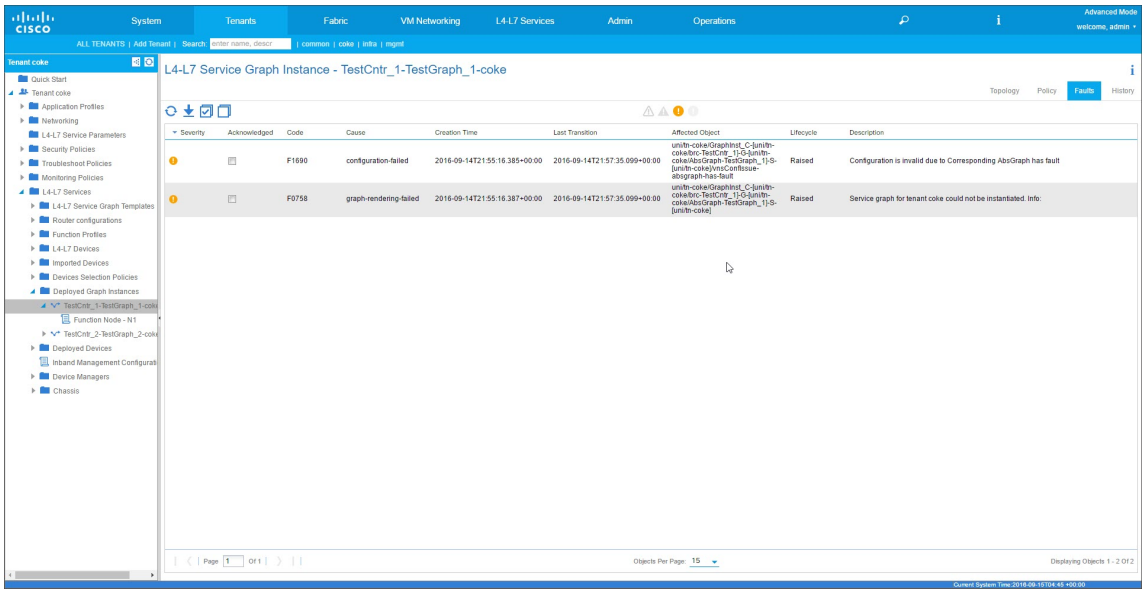
> **Hinweis**
>
> Standardmäßig müssen Sie für ein integriertes einarmiges Profil SNIP-Details wie IP-Adresse und Netzmaske angeben. Sie können andere Netzwerkparameter anzeigen, indem Sie auf **Alle Parameter** klicken und den **Configure Network** Tree in der Cisco

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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"/>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
                        <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>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    <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"/>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

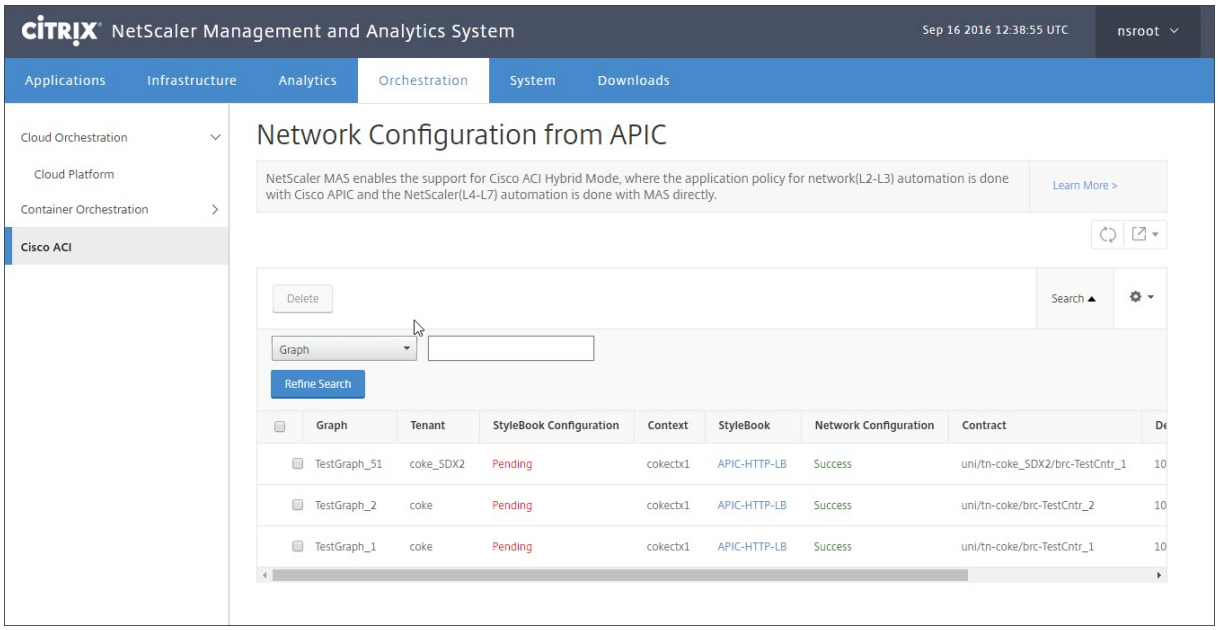
```
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

L4-L7-Parameter von NetScaler ADM mit StyleBook konfigurieren

February 5, 2024

24. Mai 2018

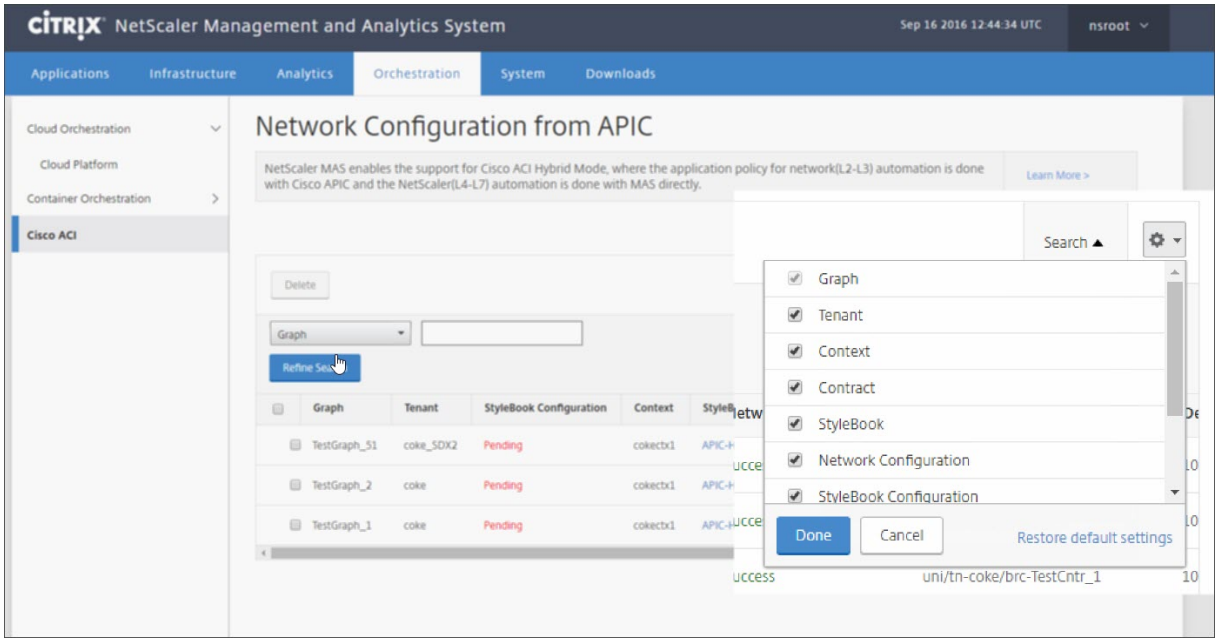
In Citrix Application Delivery Management (ADM) können Sie die Details des bereitgestellten Dienstdiagramms auf der Registerkarte **Orchestration** unter **Cisco ACI**anzeigen. In der tabellarischen Ansicht werden die Servicediagrammdetails wie Diagrammname, Mandantenname, Kontext, StyleBook-Name und Netzwerkkonfigurationsstatus angezeigt.



> **Hinweis**
>
> Wenn das Diagramm aus dem Cisco APIC gelöscht wird, wird die entsprechende Konfiguration vom Gerät entfernt, einschließlich der L4-L7-Konfiguration.

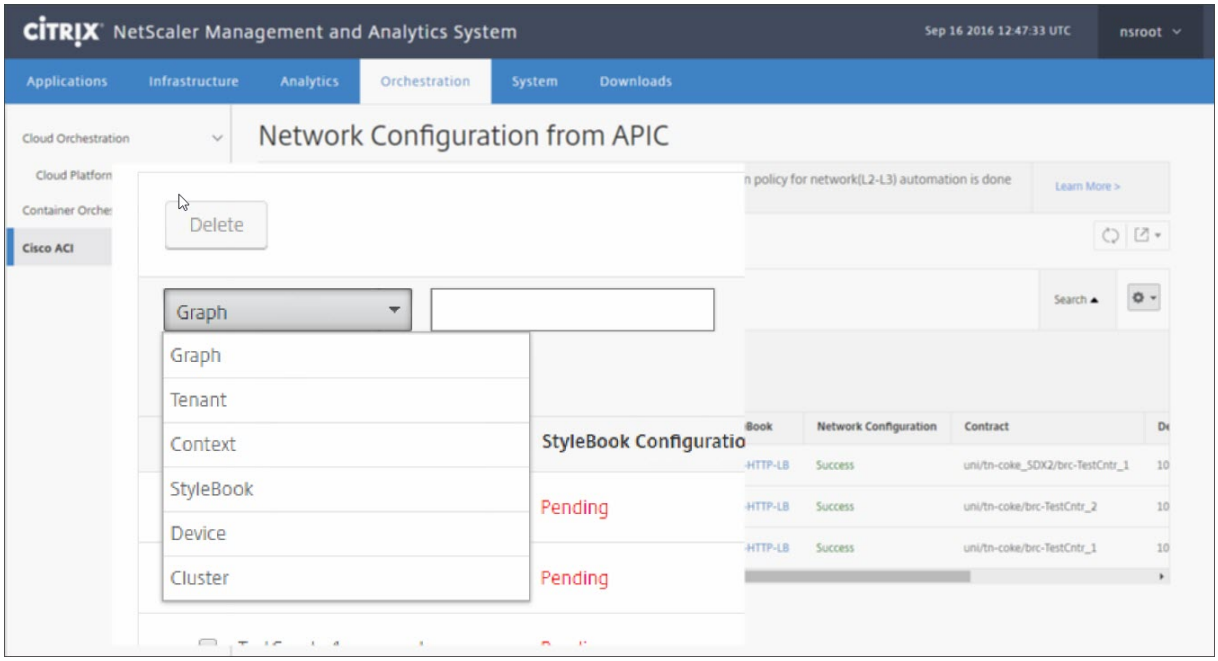
Darüber hinaus können Sie in der tabellarischen Ansicht nach jeder in der Tabelle angezeigten Spalte sortieren und die Daten mithilfe der Suchoption filtern. Sie können die Spaltendetails auch anpassen, indem Sie die Spaltennamen aus der Drop-down-Spaltenliste auswählen oder abwählen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

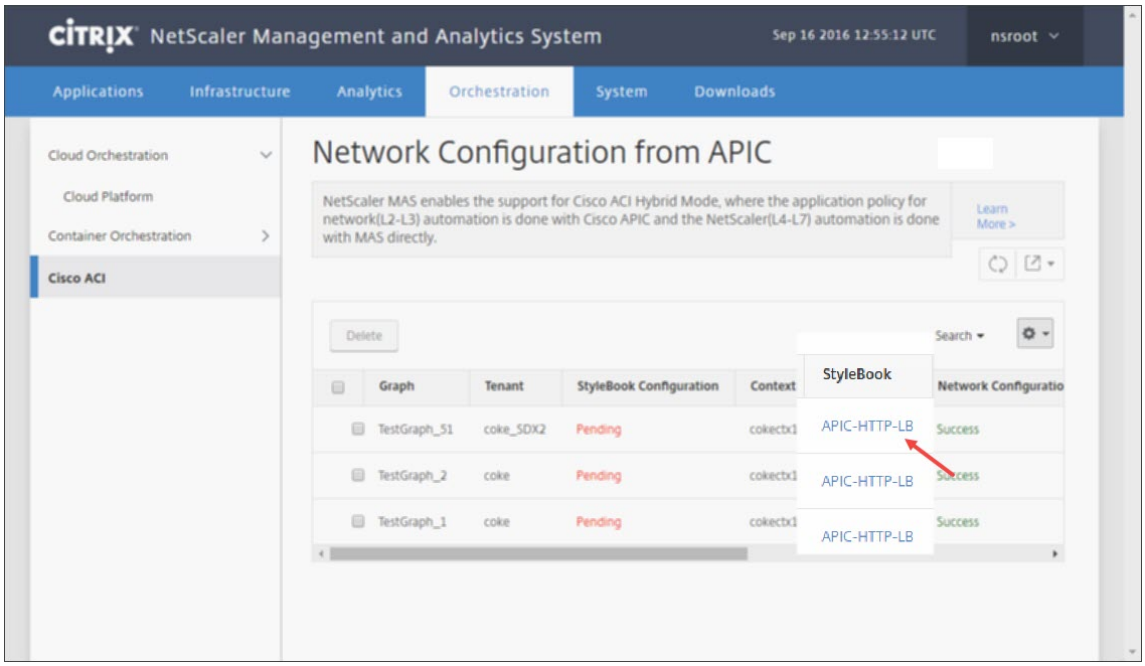
> **Hinweis**
>
> Bei der Suchfunktion wird zwischen Groß- und Kleinschreibung unterschieden, und Sie müssen die genauen Suchkriterien angeben.



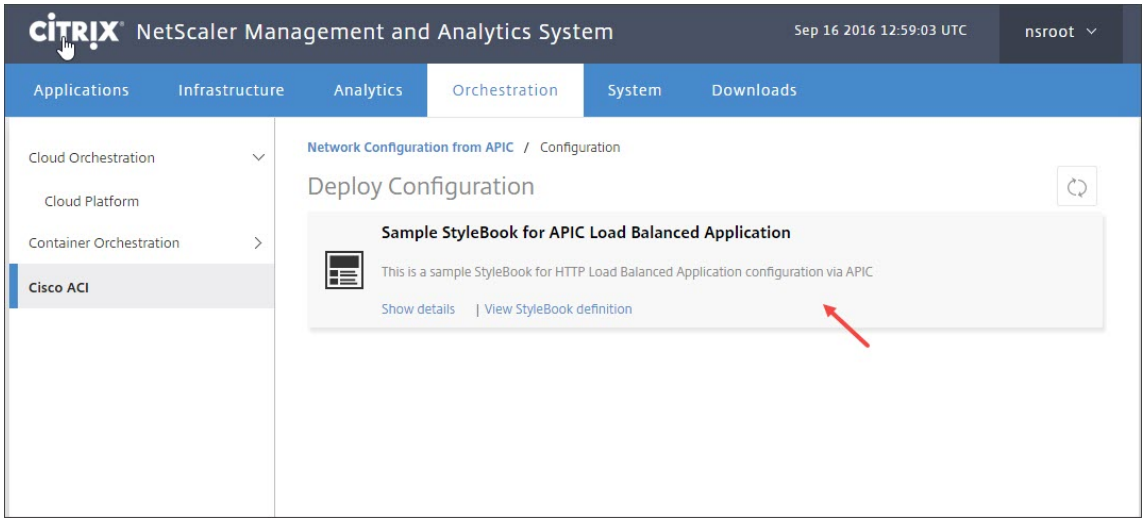
So stellen Sie die L4-L7-Konfiguration mithilfe von StyleBook in Citrix ADM bereit:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Klicken Sie auf den StyleBook-Namen, der in der tabellarischen Ansicht als URL angezeigt wird.



2. Doppelklicken Sie im Konfigurationsfenster auf **StyleBook**.

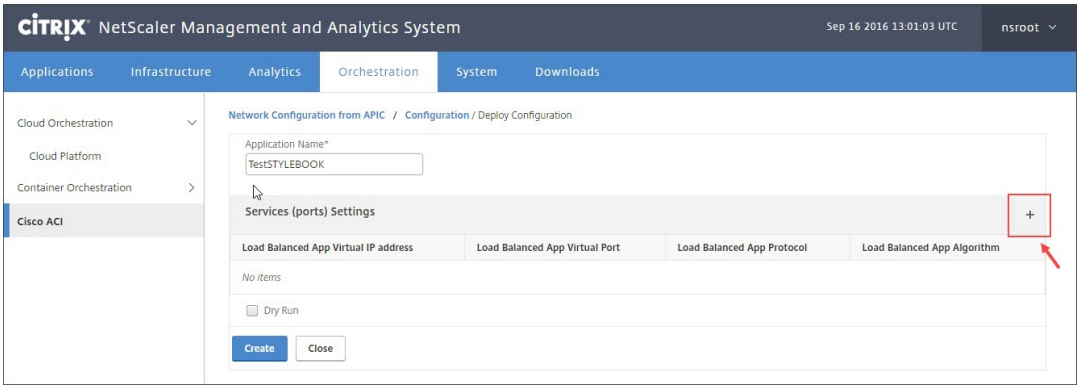


3. Gehen Sie im Fenster Konfiguration bereitstellen wie folgt vor:

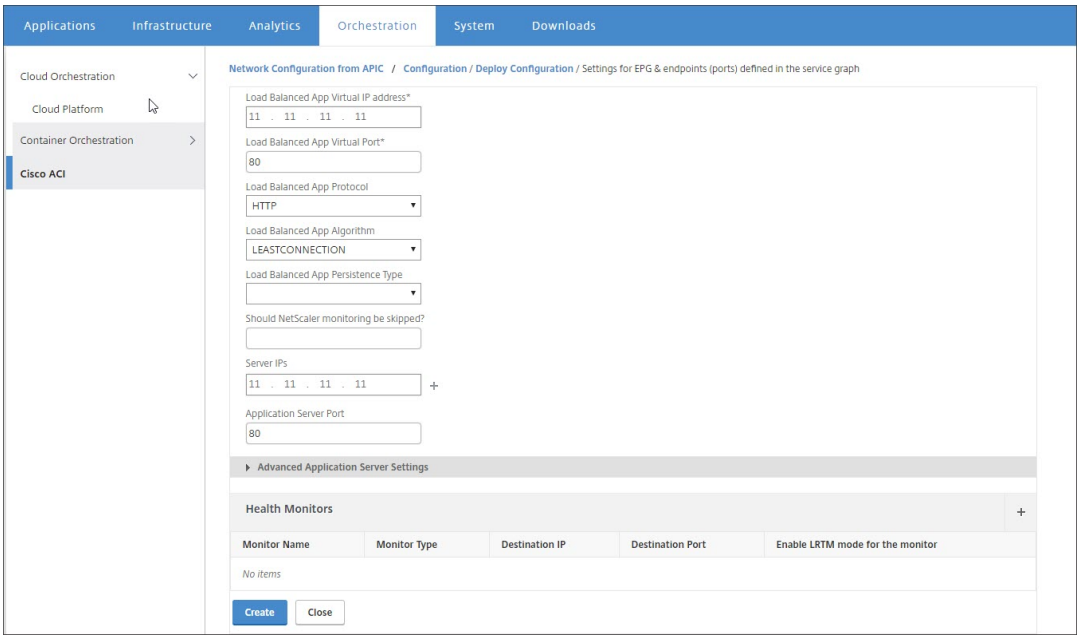
   a) Geben Sie im Feld **Anwendungsname** den Namen für die ADC-Funktionskonfiguration ein, der dem Servicediagramm der Anwendung im APIC entspricht.

   b) Klicken Sie im Abschnitt Service (Ports) Settings auf **+**.

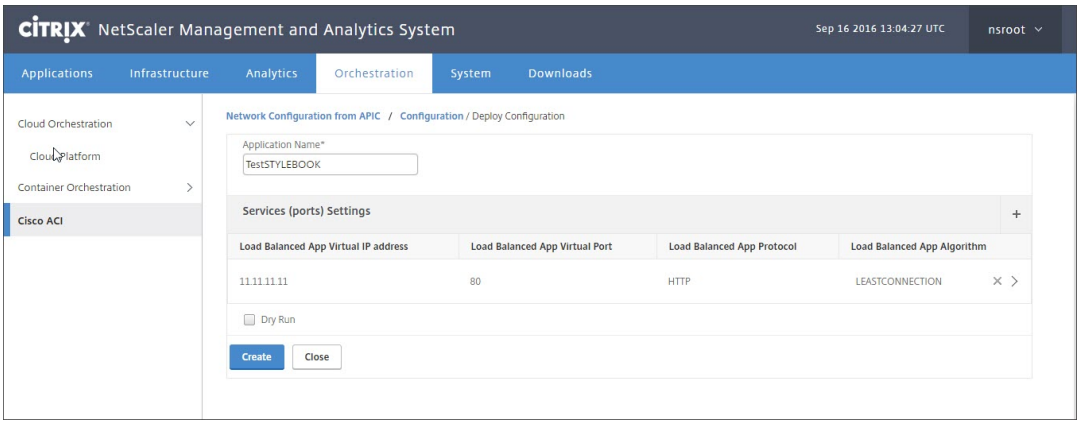
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.**

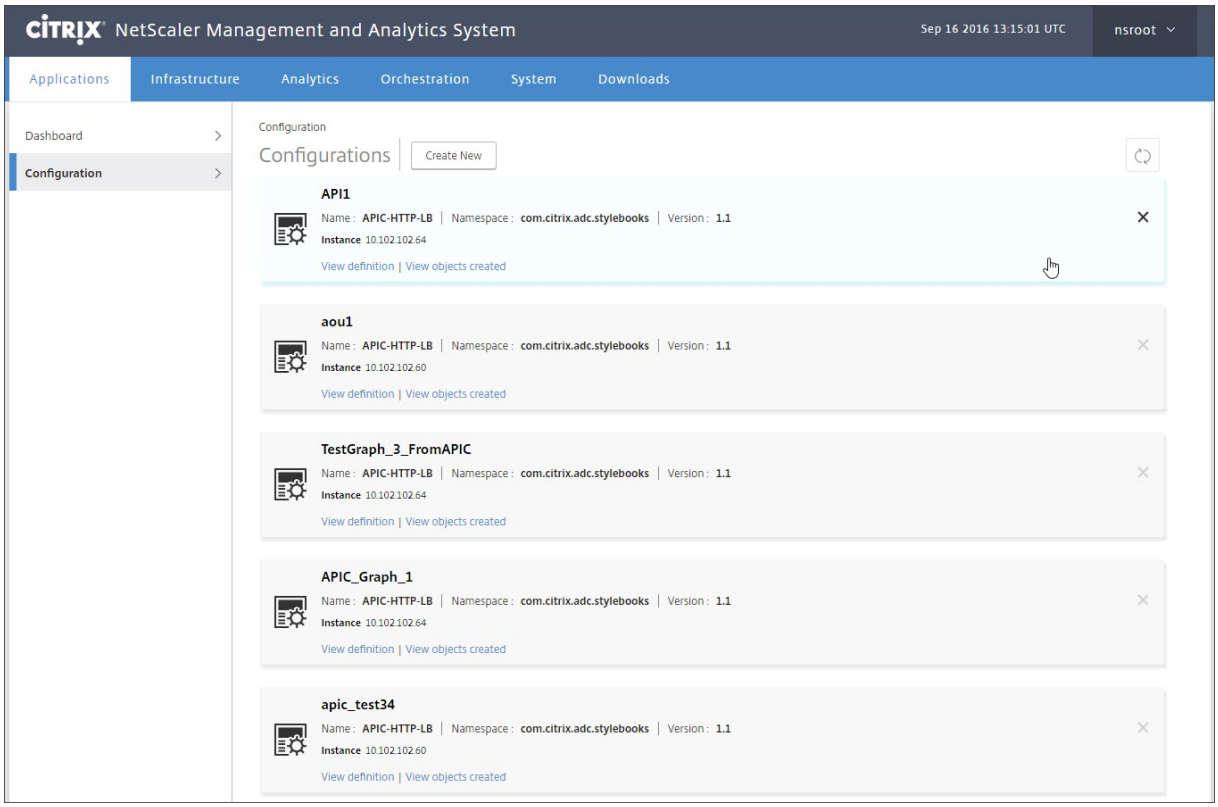


d) Klicken Sie auf **Erstellen**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

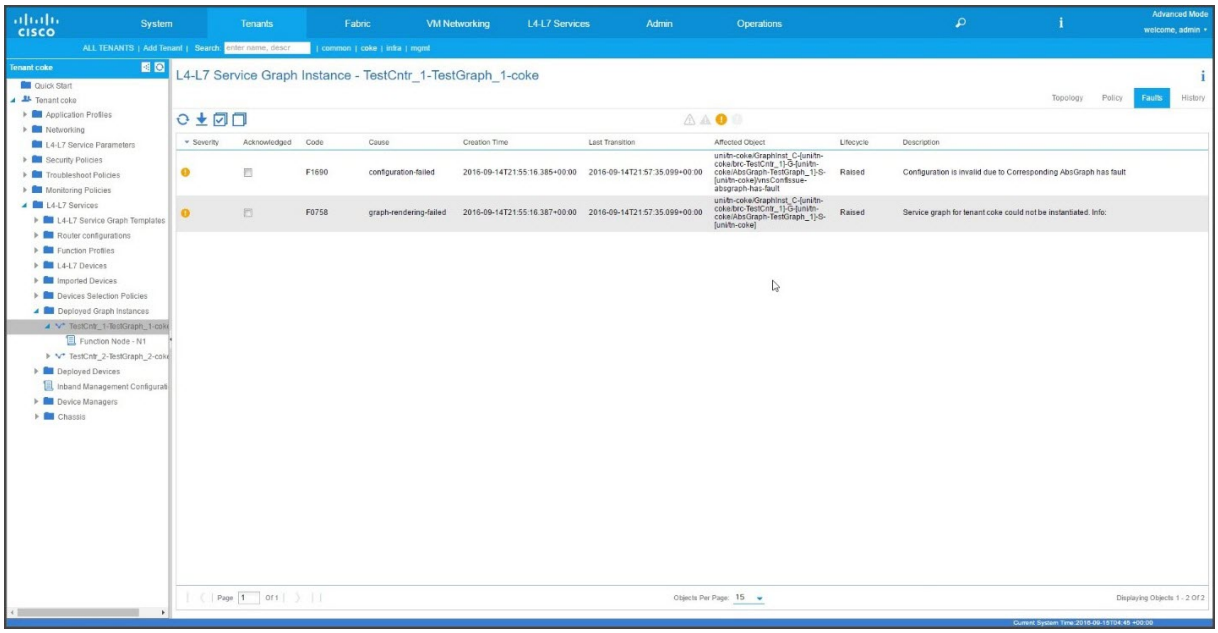
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
    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 }
 }
 }
 }
 }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 }
, '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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
            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   }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 = {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
161   0: [], 1: [], 3: [] }
162
163      2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList
             = []
164      2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
            attachIpList = [] dettachIpList = []
165      2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
166   '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 }
167
168   <!--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= {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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' }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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   }
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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,
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
           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.

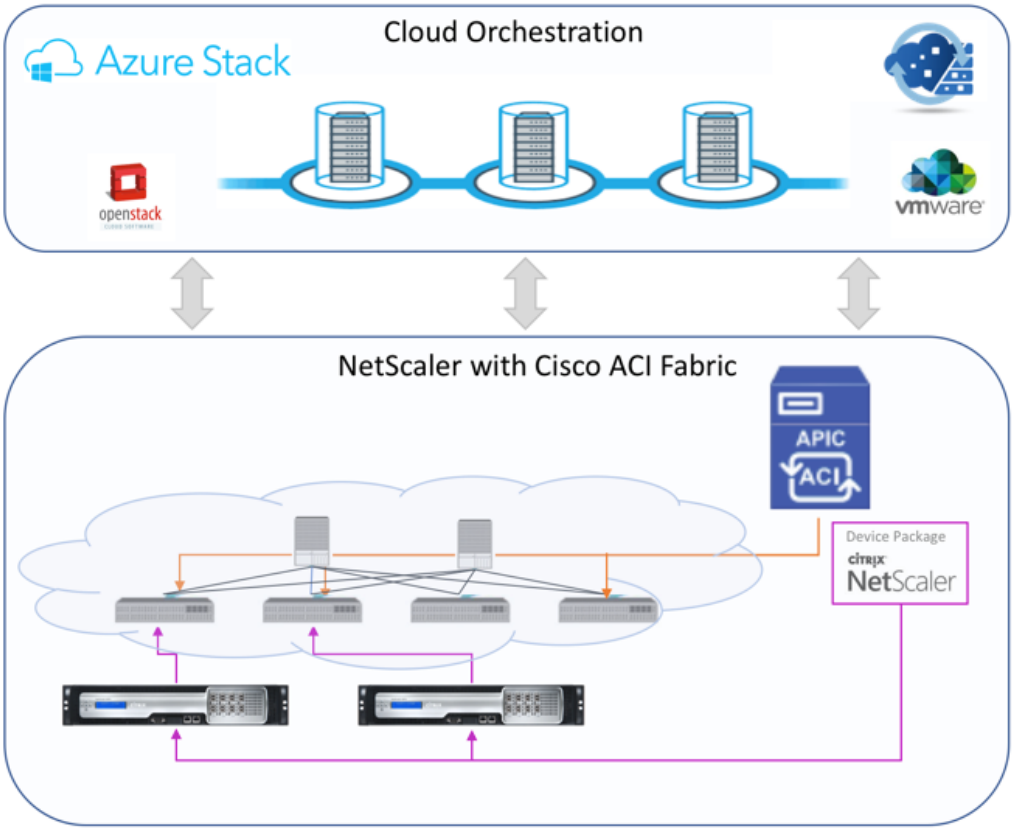
Der Cisco ACI Cloud Orchestrator-Modus mithilfe der NetScaler ADC-Lösung bietet folgende Vorteile:

- 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



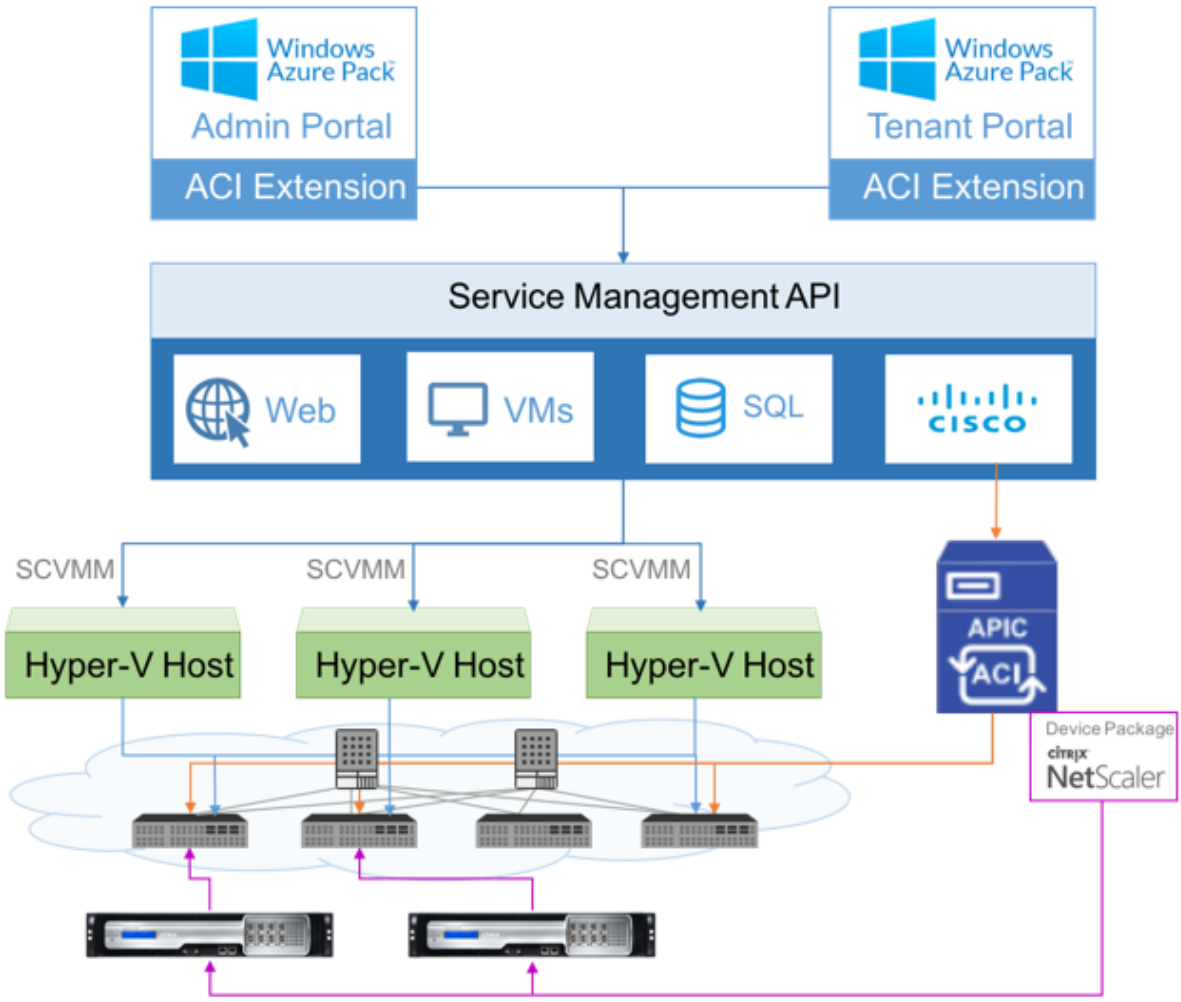
Die Lösung für den Cloud-Orchestrator-Modus mit Microsoft Azure Pack umfasst viele Integrationspunkte, wie Azure Pack zu Cisco APIC, Cisco APIC zu System Central Virtual Machine Manager (SCVMM) und Cisco APIC zu NetScaler ADC. Als Mandant in der Private Cloud können Sie NAT aktivieren, Netzwerkdienste 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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
- Bandbreitenpool
- Instanzpool
- Citrix 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

aus der Bandbreite und den Instanz-Pools 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. Sie können jedoch keine NetScaler ADC gepoolte Kapazität für eine andere NetScaler ADC-Hardwareinstanz verwenden.

Plattformlizenzen verwalten und installieren. 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

Citrix ADC VPX-Instanzen, auf denen die Citrix ADC-Softwareversion 12.0 Build 51.24 und höher ausgeführt wird, unterstützen die folgenden Hypervisoren und Cloud-Plattformen gepoolte Kapazität

- Microsoft Hyper-V
- AWS
- Microsoft Azure

> **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 Citrix ADC VPX-Instanzen zu Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Um den Datenverkehr zu verarbeiten, muss eine Instanzlizenz aus dem Pool ausgecheckt werden.

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, Enterprise und Platinum). 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 Instanz-Pool definiert die Anzahl der VPX-Instanzen oder CPX-Instanzen, die über NetScaler ADC gepoolte Kapazität verwaltet werden können, oder die Anzahl der VPX-Instanzen in einer SDX-Z-Instanz.

Beim Auschecken aus dem Pool entsperrt eine Lizenz die Ressourcen der MPX-Z-, SDX-Z-, VPX- und CPX-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 Citrix ADC verwendet die Citrix ADM Software, die als Lizenzserver konfiguriert ist, um gepoolte Kapazitätslizenzen zu verwalten: Bandbreitenpoollizenzen und Instanzpoollizenzen. Sie können Citrix ADM 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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 Mindestbandbreiteneinheit unterscheidet sich von der Mindestbandbreitenanforderung. 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.

Die Tabellen 1, 2 und 3 fassen die maximale Bandbreite/Instanzen, die minimale Bandbreite/Instanzen und die minimale Bandbreiteneinheit für alle unterstützten NetScaler-Instanzen zusammen. Tabelle 4 fasst die Lizenzanforderungen für verschiedene Formfaktoren zusammen. Für alle unterstützten Citrix ADC-Instanzen:

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	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX 8900Z	33	5	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX-14000Z-Serie	100	20	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX-15000Z-Serie	100	20	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX-25000Z-40G	200	100	Nicht verfügbar	Nicht verfügbar	1 Gbit/s
MPX-24000Z-Serie	150	100	40	80	1 Gbit/s
SDX 8015Z	15	2	1	5	1 Gbit/s
SDX 89XX Serie	33	10	2	7	1 Gbit/s

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Produkt-Linie	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
SDX-115XX-Serie	42	7	2	20	1 Gbit/s
SDX-14000Z-Serie	100	10	2	25	1 Gbit/s
SDX 15000Z-50G	100	10 (Hinweis: 20 Gbit/s für Versionen unter 12.1 54.x)	2 (Hinweis: 5 Instanzen für Versionen unter 12.1 54.x)	55	1 Gbit/s
SDX- 15000Z	100	10 (Hinweis: 20 Gbit/s für Versionen unter 12.1 54.x)	2 (Hinweis: 5 Instanzen für Versionen unter 12.1 54.x)	55	1 Gbit/s
SDX-22XXX-Serie	120	20	10	80	1 Gbit/s
SDX-25000Z-40G	200	50	10	115	1 Gbit/s
SDX 26000Z-100G	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 8005Z	15	2	1	2	1 Gbit/s
SDX-24000Z-Serie	150	50	10	80	1 Gbit/s

> Hinweis
>
> Die Mindestbandbreite und die Mindestinstanzen gelten für SDX-Instanzen, auf denen die folgenden Versionen und höher ausgeführt werden: 11.1 64.x, 12.0 63.x und 12.1 54.x.
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestanforderung des Systems.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tabelle 2. Unterstützte gepoolte Kapazität für CPX-Instanzen

	Maximale Bandbreite (Gbit/s)	Minimale Bandbreite (Gbit/s)	Minimale Instanzen	Maximale Anzahl Instanzen	Einheit für minimale Bandbreite
CPX	10	1	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	5 Gbit/s	10 MBit/s	1	1	10 MBit/s
Azure	3 Gbit/s	10 Mbit/s	1	1	10 MBit/s

> Hinweis:
>
> Die Mindestabnahmemenge unterscheidet sich von der Mindestsystemanforderung.

Tabelle 4. 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

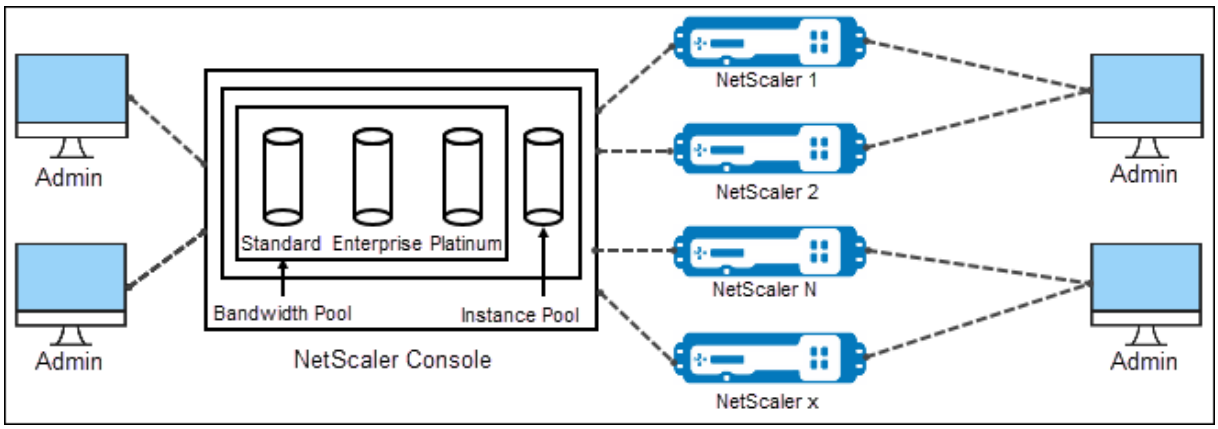
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Produkt-Linie	Kauf von Hardware ohne Kapazität	Bandbreite & Edition-Abonnement	Instanz-Abonnement
CPX	-	-	Lizenz erforderlich

Gepoolte NetScaler ADC-Kapazität konfigurieren

February 5, 2024

Citrix Application Delivery Management (ADM) ist der Lizenzserver für alle Citrix ADC-Instanzen, die zu ADM hinzugefügt wurden. Sie können die Lizenzdateien mit gepoolter Kapazität (Bandbreitenpool oder Instanzpool) auf den Lizenzserver hochladen. Sie können Citrix ADC-Instanzen bei Bedarf Lizenzen im Lizenzpool zuweisen. Sie können die Lizenzen von Citrix ADM zuweisen oder die Lizenzen von Citrix ADC-Instanzen (MPX-Z /SDX-Z/VPX/CPX) entsprechend der minimalen und maximalen Kapazität der Instanz auschecken.



Unterstützte Hardware- und Softwareversionen

NetScaler ADC-Softwareversion	Citrix ADC MPX Hardware mit Nullkapazität	Citrix ADC SDX Hardware mit Nullkapazität	Unterstützte Hypervisoren für Citrix ADC VPX
11.1 Build 54.14 und höher	MPX-14000Z, MPX-14000Z-40G, MPX-25000Z-40G	SDX-14000Z, SDX-14000Z-40G, SDX-25000Z-40G	VMware ESX 6.0, Citrix Hypervisor, Linux KVM

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

NetScaler ADC-Softwareversion	Citrix ADC MPX Hardware mit Nullkapazität	Citrix ADC SDX Hardware mit Nullkapazität	Unterstützte Hypervisoren für Citrix ADC VPX
12.0 Build 51.24 und höher			Microsoft Hyper-V, Amazon AWS, Microsoft Azure

Konfiguration von Citrix ADM als Lizenzserver

Sie können Citrix ADM als Lizenzserver für die gepoolte Kapazität von Citrix ADC konfigurieren. Es gibt zwei Möglichkeiten für eine Citrix ADC-Instanz, Bandbreite oder Instanzlizenz oder beides zu erhalten:

- Eine Citrix ADC-Instanz kann die Check-Out-Anfrage an Citrix ADM initiieren, um ihre Bandbreiten- und/oder Instanzlizenzen zu erhalten.
- Die Lizenzen können einer Citrix ADC-Instanz über Citrix ADM zugewiesen werden.

> **Hinweis**
>
> Die gepoolte Kapazität wird auf Citrix ADM nur angezeigt, wenn dem Citrix ADM gepoolte Lizenzen hinzugefügt werden.

Im Folgenden sind die Betriebsmodi der Citrix ADC-Instanzen aufgeführt, die die Citrix ADC Pooled Capacity verwenden:

- **Optimal**—Die Instanz läuft mit der richtigen Lizenzkapazität.
- **Kapazitätskonflikt** —Die Instanz wird mit einer Kapazität ausgeführt, die unter der vom Benutzer konfigurierten Kapazität liegt.
- **Grace** —Die Instanz läuft mit der Grace-Lizenz.
- **Grace & Mismatch** —Die Instanz läuft auf Grace, hat aber eine Kapazität, die unter der vom Benutzer konfigurierten Kapazität liegt.
- **Nicht verfügbar** —Die Instanz ist nicht bei Citrix ADM für die Verwaltung registriert oder die Nitro-Kommunikation von Citrix ADM zur Instanz funktioniert nicht.
- **Nicht zugewiesen** —Die Lizenz wird der Instanz nicht zugewiesen.

So installieren Sie Lizenzdateien auf NetScaler ADM:

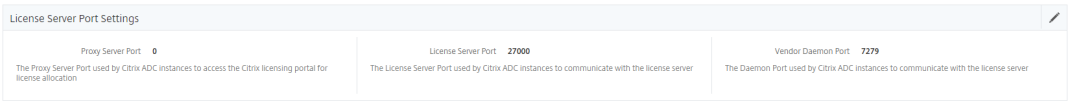
1. Geben Sie in einem Webbrowser die IP-Adresse des **Citrix ADM** ein (z. B. http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **Netzwerke > Lizenzen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

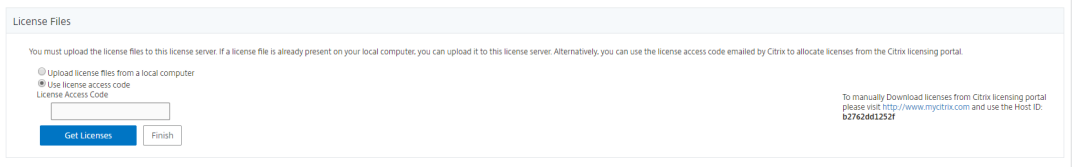
4. Wählen Sie im Abschnitt **Lizenzdateien** eine der folgenden Optionen aus:

   - **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**.

     > **Hinweis**
     >
     > Wenn die hochgeladenen Lizenzdateien die Lizenzen in der Citrix ADC Pooled-Kapazität nicht hinzufügen, können Sie die Lizenzdateien auswählen und auf **Lizenzen anwenden** klicken, um die Lizenzen dem Pool hinzuzufügen.

   - **Lizenzzugriffscode verwenden** : Citrix sendet den License Access Code (LAC) für die erworbenen Lizenzen per E-Mail. Um Lizenzdateien hinzuzufügen, geben Sie den LAC in das Textfeld ein und klicken Sie dann auf **Lizenzen** abrufen.

     > **Hinweis**
     >
     > Sie können Citrix ADM jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.

So weisen Sie Citrix ADC Pooled Capacity-Lizenzen von Citrix ADM zu:

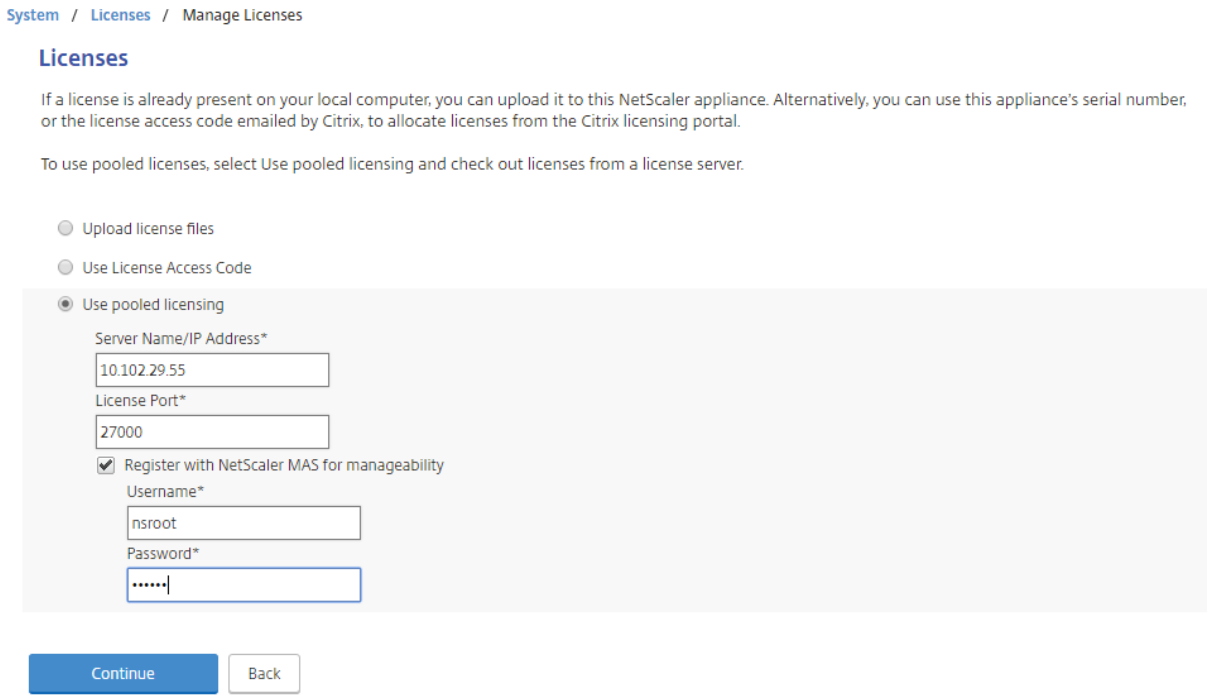
> **Hinweis**
>
> Wenn Sie die Citrix ADC-Instanz nicht bei Citrix ADM registriert haben, können Sie Lizenzen von Citrix ADM auschecken, aber nicht von Citrix ADM der gepoolten Instanz mit aktivierter Kapazität von Citrix ADC zuweisen.

Stellen Sie sicher, dass die folgende Voraussetzung erfüllt ist, bevor Sie den ADC-Instances gepoolte Kapazitätslizenzen zuweisen.

> **Voraussetzung**
>
> Bevor Sie die Poollizenzen Ihrer Instanz über Citrix ADM verwalten können, müssen Sie die Citrix ADC-Instanz bei Citrix ADM registrieren. Navigieren Sie in der Citrix ADC GUI zu **System** > **Lizenzen** > **Lizenzen verwalten** und aktivieren Sie das Kontrollkästchen **Bei Citrix ADM für Verwalt-**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **barkeit registrieren**, wenn Sie die Citrix ADM IP hinzufügen.

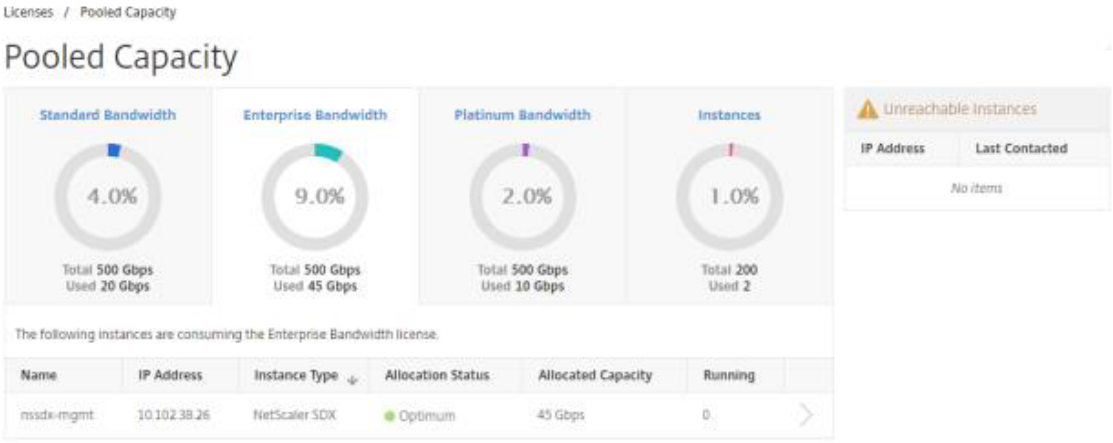


> **Hinweis**
>
> Geben Sie in den Feldern **Benutzername** und **Kennwort** auf dem obigen Bildschirm die Citrix ADM-Anmeldeinformationen ein.

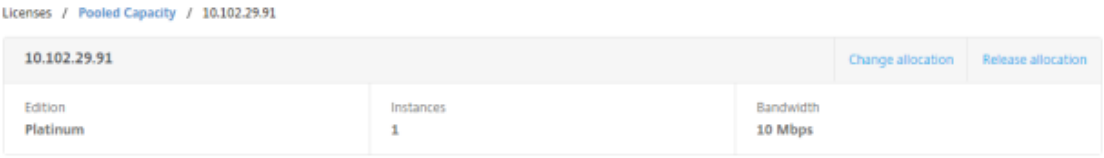
Nachdem die Instanz beim Lizenzserver registriert wurde, weisen Sie die Lizenzen wie folgt zu:

1. Geben Sie in einem Webbrowser die IP-Adresse von **Citrix 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 > Pooled Capacity**.
4. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten.
5. Wählen Sie eine Citrix ADC-Instanz aus der Liste der verfügbaren Instanzen aus, indem Sie auf die Schaltfläche **>** klicken.

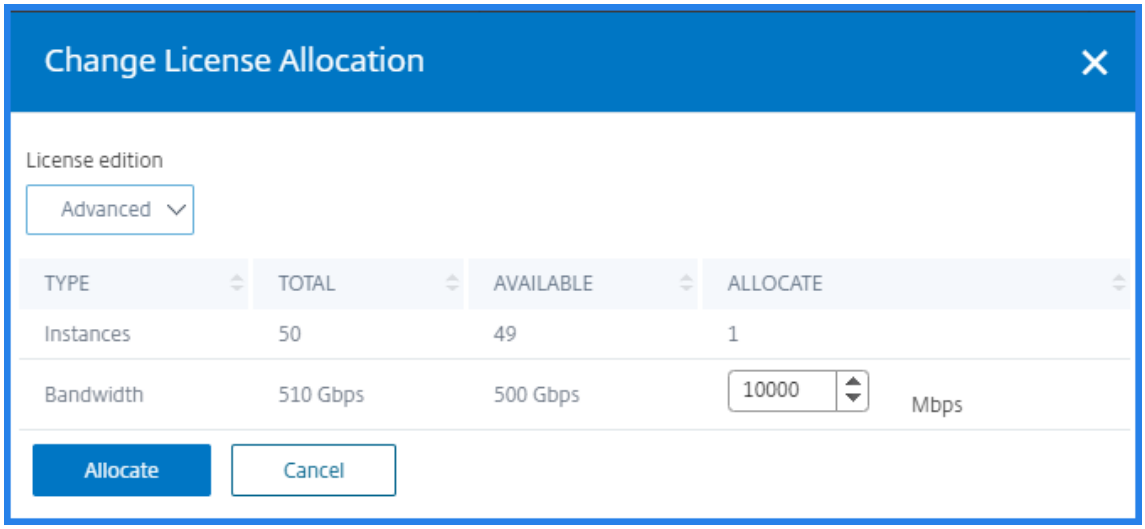
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Wenn Sie eine Lizenzzuweisung ändern oder freigeben möchten, klicken Sie auf **Zuweisung ändern oder Zuweisungfreigeben**.



7. Wenn Sie auf **Zuordnung ändern** klicken, wird ein Popup-Fenster mit den verfügbaren Lizenzen auf dem Lizenzserver angezeigt.



8. Sie können die Bandbreite oder Instanzzuweisung für die Citrix ADC-Instanz auswählen, indem Sie die Dropdownoptionen **Zuweisen** festlegen. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf **Zuweisen**.
9. Sie können die zugewiesene Lizenzedition auch über die Dropdownoptionen im Fenster Lizenzzuweisung ändern ändern.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfiguration der gepoolten Kapazität von Citrix ADC auf MPX-Z

MPX-Z ist die Citrix ADC MPX-Appliance mit gepoolter Kapazität. MPX-Z unterstützt Bandbreitenpooling für Platinum-, Enterprise- oder Standard Edition-Lizenzen.

MPX-Z benötigt seine Plattformlizenzen, bevor es eine Verbindung zum Lizenzserver herstellen kann. Sie können die MPX-Z-Plattformlizenz installieren, indem Sie entweder die Lizenzdatei von einem lokalen Computer hochladen oder die Hardware-Seriennummer der Instanz oder den Lizenzzugriffscode im Abschnitt **System** > **Lizenzen** der GUI der Citrix ADC-Instanz verwenden. Wenn Sie die MPX-Z-Plattformlizenz entfernen, wird die Funktion für gepoolte Kapazität deaktiviert und alle ausgecheckten Lizenzen werden auf dem Lizenzserver eingecheckt.

Sie können die Bandbreite einer MPX-Z-Instanz ohne Neustart dynamisch ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis**
>
> Wenn Sie die Instance neu starten, checkt sie automatisch die gepoolten Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

Konfiguration der gepoolten Kapazität von Citrix ADC auf einer Citrix ADC VPX-Instanz

Eine Citrix ADC VPX-Instanz mit aktivierter Poolkapazität kann Lizenzen aus einem Bandbreitenpool (Platinum/Enterprise/Standard Editions) auschecken. Sie können die Citrix ADC GUI verwenden, um Lizenzen vom Lizenzserver auszuchecken.

Sie können die Bandbreite einer VPX-Instanz ohne Neustart dynamisch ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzversion ändern möchten.

> **Hinweis**
>
> Wenn Sie die Instance neu starten, checkt sie automatisch die gepoolten Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

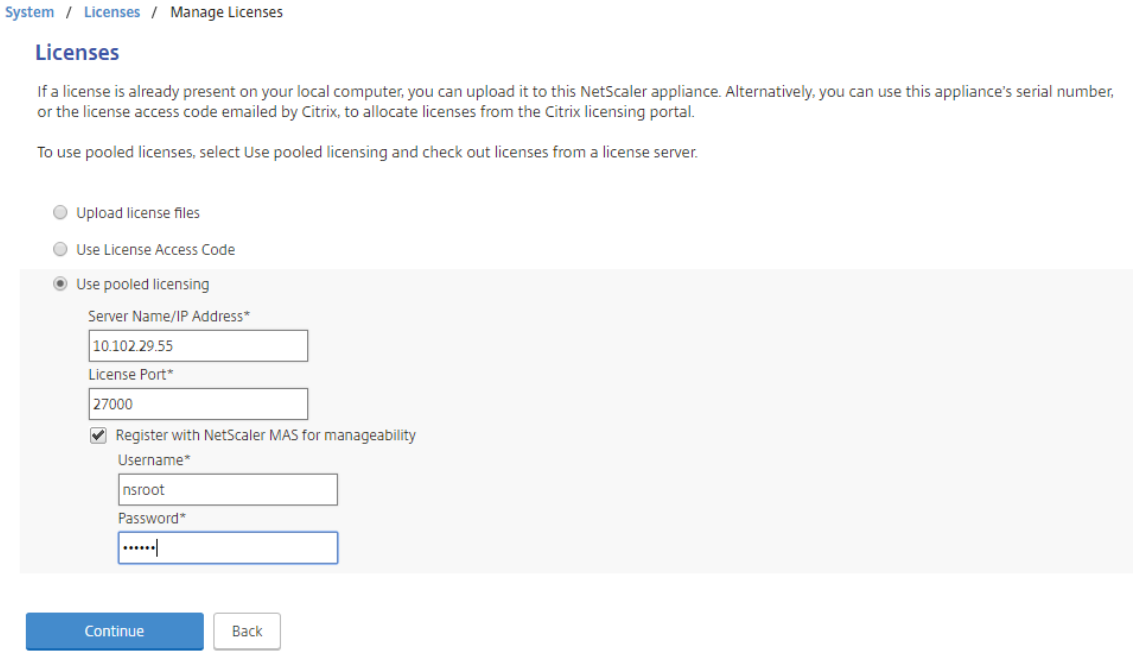
Zuweisen von Poollizenzen zu einer Citrix ADC MPX-Z- oder Citrix ADC VPX-Instanz

So weisen Sie Ihre Lizenzen zu:

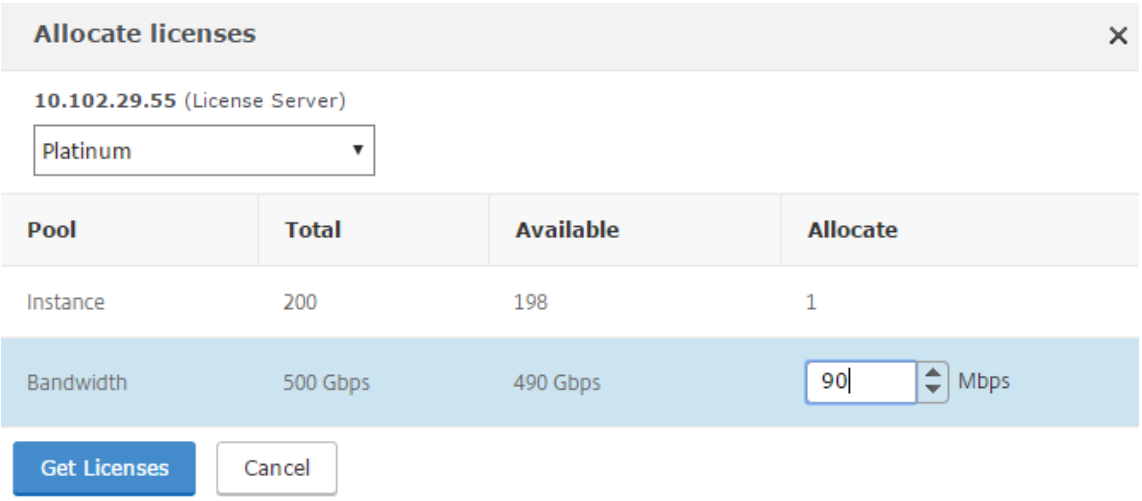
1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Instanz ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen > Lizenzen verwalten** , klicken Sie auf **Neue Lizenz hinzufügen** und wählen Sie **Pool-Lizenzierung verwenden** aus.

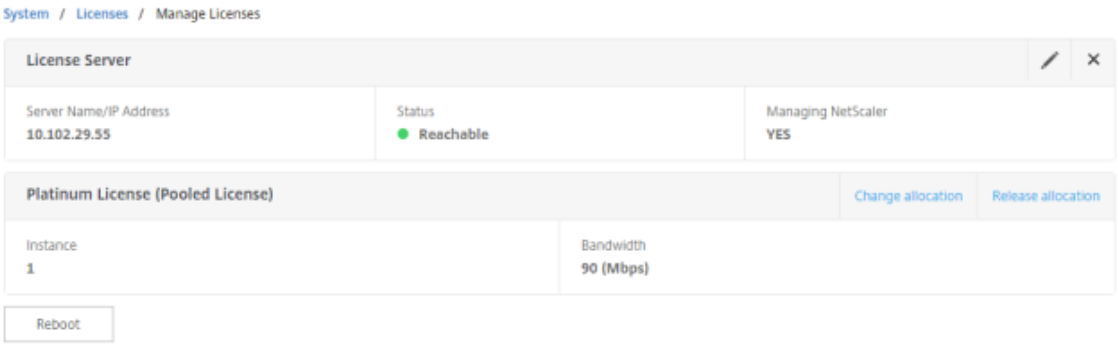


4. Geben Sie die Details des Lizenzservers in das Feld **Servername/IP-Adresse** ein.
5. Wenn Sie die Poollizenzen Ihrer Instanz über Citrix ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Zur Verwaltbarkeit bei Citrix ADM registrieren** und geben Sie ADM-Anmeldeinformationen ein.
6. Wählen Sie die Lizenzversion und die erforderliche Bandbreite aus, klicken Sie auf **Lizenzen abrufen**.



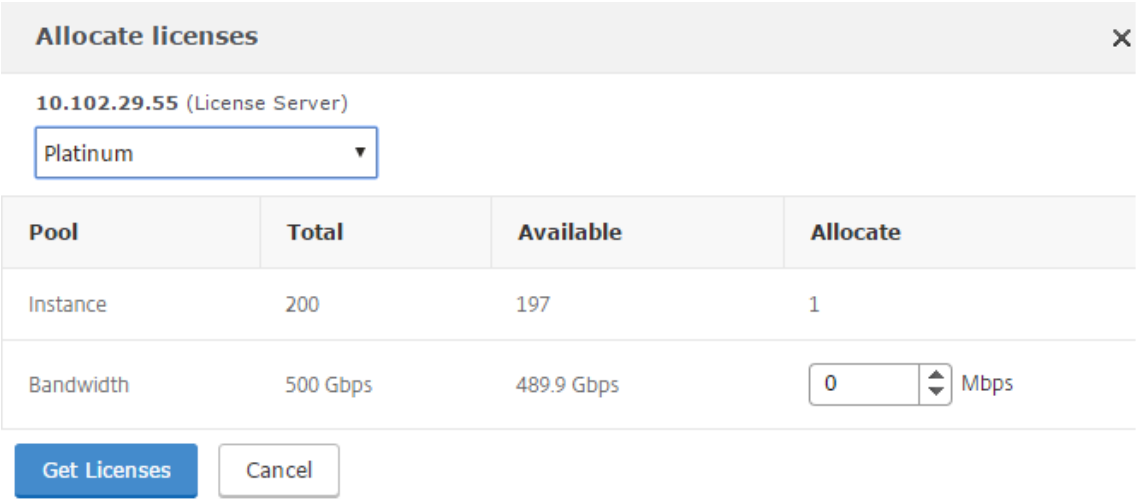
7. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie **Zuordnung ändern oder Zuordnungfreigeben**wählen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. Wenn Sie auf **Zuweisung ändern**klicken, werden in einem Popup-Fenster die auf dem Lizenzserver verfügbaren Lizenzen angezeigt.

> **Hinweis**
>
> Ein Neustart ist nicht erforderlich, wenn Sie die Bandbreitenzuweisung ändern, aber ein warmer Neustart ist erforderlich, wenn Sie die Lizenzversion ändern.



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**
>
> Die Bandbreitenzuweisung sollte ein Vielfaches der Mindestbandbreiteneinheit betragen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfiguration der gepoolten Kapazität von Citrix ADC auf SDX-Z

Eine SDX-Z-Instanz ist eine Instanz mit gepoolter Kapazität von Citrix ADC SDX. SDX-Z unterstützt Bandbreitenpooling für Platinum-, Enterprise- und Standard-Editionen sowie Instance-Pooling. Nachdem Sie die SDX-Z-Plattformlizenz angewendet haben, bietet der Management Service Optionen zum Ein- und Auschecken
von Lizenzen vom Lizenzserver und zum Zuweisen von Bandbreitenkapazität zu den Citrix ADC-Instanzen, die auf der SDX-Z-Plattform ausgeführt werden.

> **Hinweis**
>
> NetScaler ADC VPX-Instanzen, die auf SDX-Z ausgeführt werden, können Lizenzen nicht direkt vom Lizenzserver aus oder in diesen einchecken. Dies kann durch den Management Service in SDX erfolgen.

Sie können die SDX-Z-Plattformlizenz installieren, indem Sie entweder die Lizenzdatei vom lokalen Computer hochladen oder die Hardware-Seriennummer der Instanz oder den Lizenzzugangscode verwenden.

Wenn Sie die SDX-Z-Plattformlizenz entfernen, wird die Funktion für gepoolte Kapazität deaktiviert und alle Lizenzen werden wieder in den Lizenzserver eingecheckt.

> **Hinweis**
>
> Wenn Sie die Instance neu starten, checkt sie die gepoolten Lizenzen aus, die für die konfigurierte Kapazität erforderlich sind.

Poolkapazität auf Citrix ADC SDX

Instanzpool:

Eine SDX-Appliance kann dieselbe Anzahl von Instanzen bereitstellen, die im Instanzpool der SDX-Appliance verfügbar sind.

Bandbreitenpool:

Während der NetScaler ADC-Instanzbereitstellung wird der Instanz Bandbreite zugewiesen. Sie können die Edition und die erforderliche Bandbreite auswählen, um eine Virtual Citrix ADC-Instanz bereitzustellen. Der Management Service ermöglicht die Fortsetzung der Bereitstellung nur, wenn die Instanz über ausreichende Bandbreite für die angeforderte Edition verfügt. Sie werden benachrichtigt, wenn die Bandbreite nicht ausreicht.

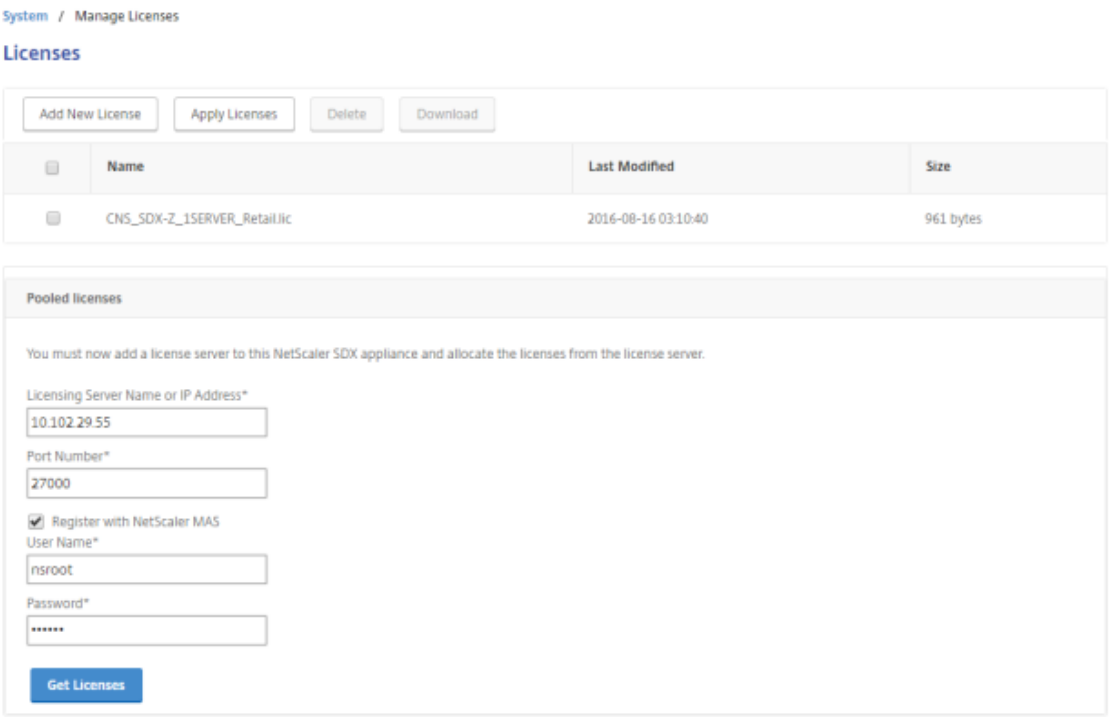
> **Hinweis**
>
> Für die Änderung der Bandbreite ist kein Neustart der Instanz erforderlich.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Zuweisen von Poollizenzen zu einer Citrix ADC SDX-Z-Instanz

So weisen Sie Ihre Lizenzen zu:

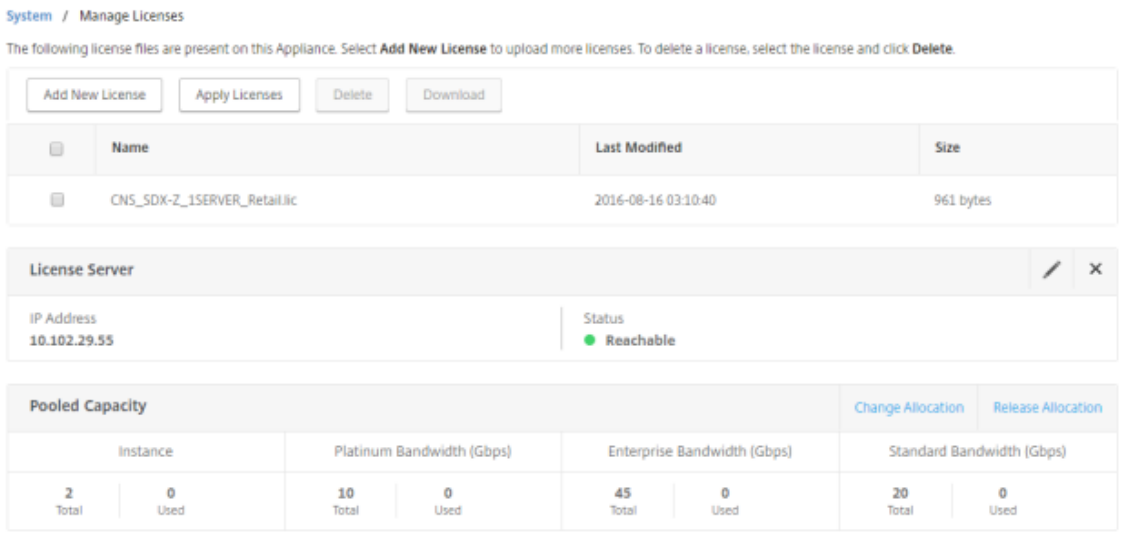
1. Geben Sie in einem Webbrowser die IP-Adresse Ihrer Citrix ADC SDX-Z-Instanz ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte Konfiguration zu **System > Lizenzen** und wechseln Sie zu **Pooled Capacity.**



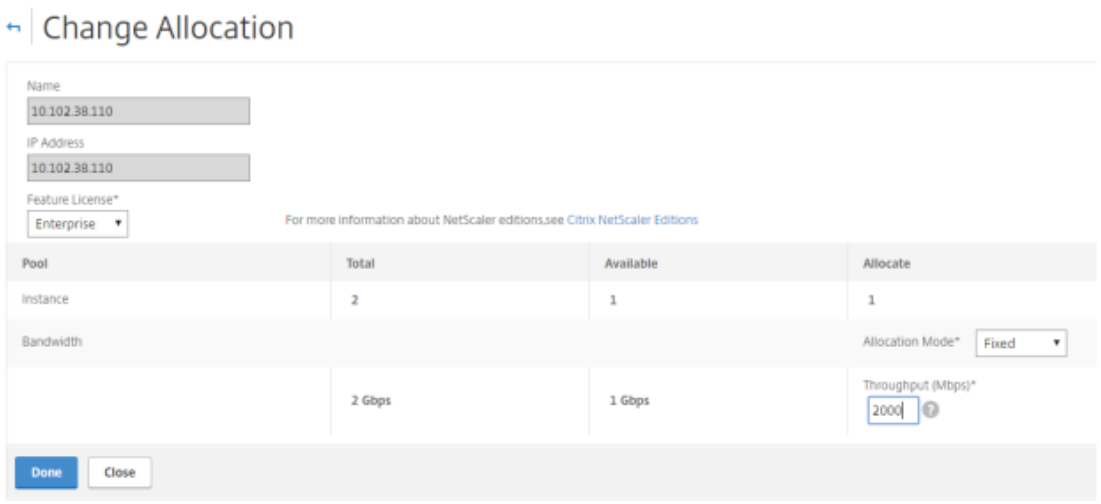
4. Geben Sie die Details des Lizenzservers in das Feld **Servername/IP-Adresse** ein.
5. Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Bei NetScaler ADM registrieren**, und geben Sie die ADM-Anmeldeinformationen ein.
6. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie **Zuordnung ändern oder Zuordnungfreigeben**wählen.

> **Hinweis**
>
> Die ausgecheckten Lizenzen werden vom ADM in einem separaten Pool gespeichert.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. Um die Lizenzzuweisung für eine bestimmte VPX-Instanz in der SDX-Z-Instanz zu ändern, wählen Sie die Instanz im Abschnitt **Instanzen** aus und klicken Sie auf **Zuordnung ändern.** In einem neuen Fenster werden die verfügbaren Lizenzen angezeigt.



8. Sie können die Bandbreitenversion der Instance in der Dropdownliste **Feature-Lizenz** und die erforderliche Bandbreite im Feld Durchsatz **(Mbit/s)** ändern. Klicken Sie dann auf **Done**.

> **Hinweis**
>
> Die Bandbreitenzuweisung sollte ein ganzzahliges Vielfaches der minimalen Bandbreiteneinheit des entsprechenden Formfaktors sein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Konfiguration der gepoolten Kapazität von Citrix ADC auf einer Citrix ADC CPX-Instanz

Während der Bereitstellung der Citrix ADC CPX-Instanz können Sie die Citrix ADC CPX-Instanz so konfigurieren, dass sie Citrix ADC Pooled Capacity verwendet. Im Befehl ***docker run*** müssen Sie die Details des Citrix ADC Lizenzservers angeben. Die Citrix ADC CPX-Instanz checkt Lizenzen aus dem Instanzpool aus.

> **Hinweis**
>
> Standardmäßig checkt die Citrix ADC CPX-Instanz eine Instanzlizenz aus dem Instanzpool aus und der Durchsatz wird automatisch auf 1000 Mbit/s festgelegt. Sie können die der Instance zugewiesene Bandbreite von 1000 Mbit/s nicht ändern.

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>

<!--NeedCopy-->
```

So konfigurieren Sie die gepoolte Kapazität von Citrix ADC bei der Bereitstellung der Citrix ADC CPX-Instanz:

Definieren Sie bei der Bereitstellung einer Citrix ADC CPX-Instanz den Citrix Licensing Server als Umgebungsvariable im Befehl ***docker run*** , wie unten gezeigt:

```
docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name
    <container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --
    cap-add=NET_ADMIN <REPOSITORY>:<TAG>

<!--NeedCopy-->
```

Ort:

- <LS_IPADDRESS>ist die IP-Adresse des Citrix Lizenzservers.
- <LS_PORT>ist der Port des Citrix Lizenzservers. Standardmäßig ist der Port 27000.

Aktualisieren Sie eine unbefristete Lizenz in Citrix ADC MPX auf Citrix ADC Pooled Capacity

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,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 zur Konfiguration der Citrix ADC Pooled Capacity-Lizenz für Citrix ADC MPX-Instanzen im Hochverfügbarkeitsmodus finden Sie unter Aktualisieren der unbefristeten Lizenz im Citrix ADC MPX High Availability Pair auf Citrix ADC Pooled Capacity.

> **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 Citrix ADC Pooled Capacity :

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.

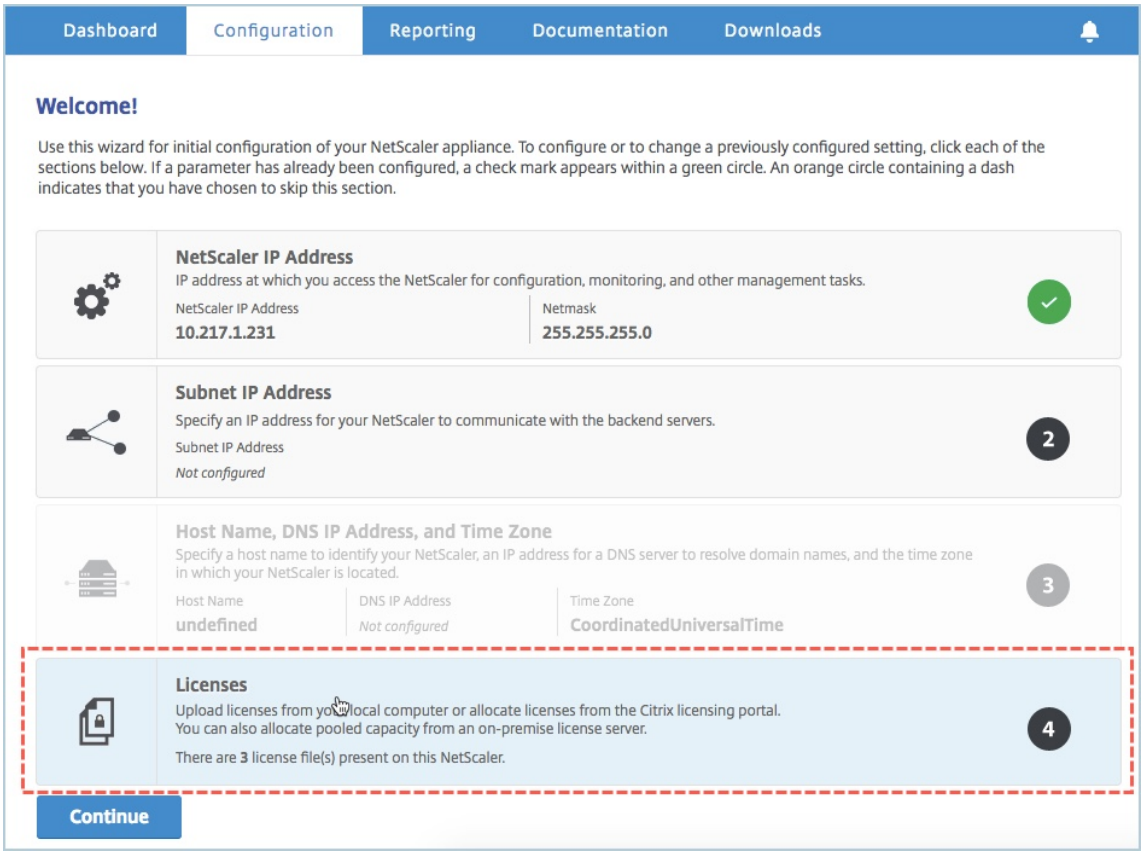
   Stellen Sie sicher, dass keine Konfigurationen gespeichert sind, bevor Sie die Appliance neu starten.

   > **Warnung**
   >
   > Nach der Anwendung der MPX-Z-Lizenz werden die Funktionen, einschließlich SSL-Offloading auf der Appliance, nicht lizenziert. Die Appliance beendet die Verarbeitung von HTTPS-Anforderungen.
   >
   > Wenn die Option **Nur sicherer Zugriff** auf der Appliance vor dem Upgrade aktiviert ist, können Sie keine Verbindung mit der Appliance über die NetScaler ADM GUI über HTTPS herstellen.

8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.
9. Melden Sie sich nach dem Neustart der Appliance an.

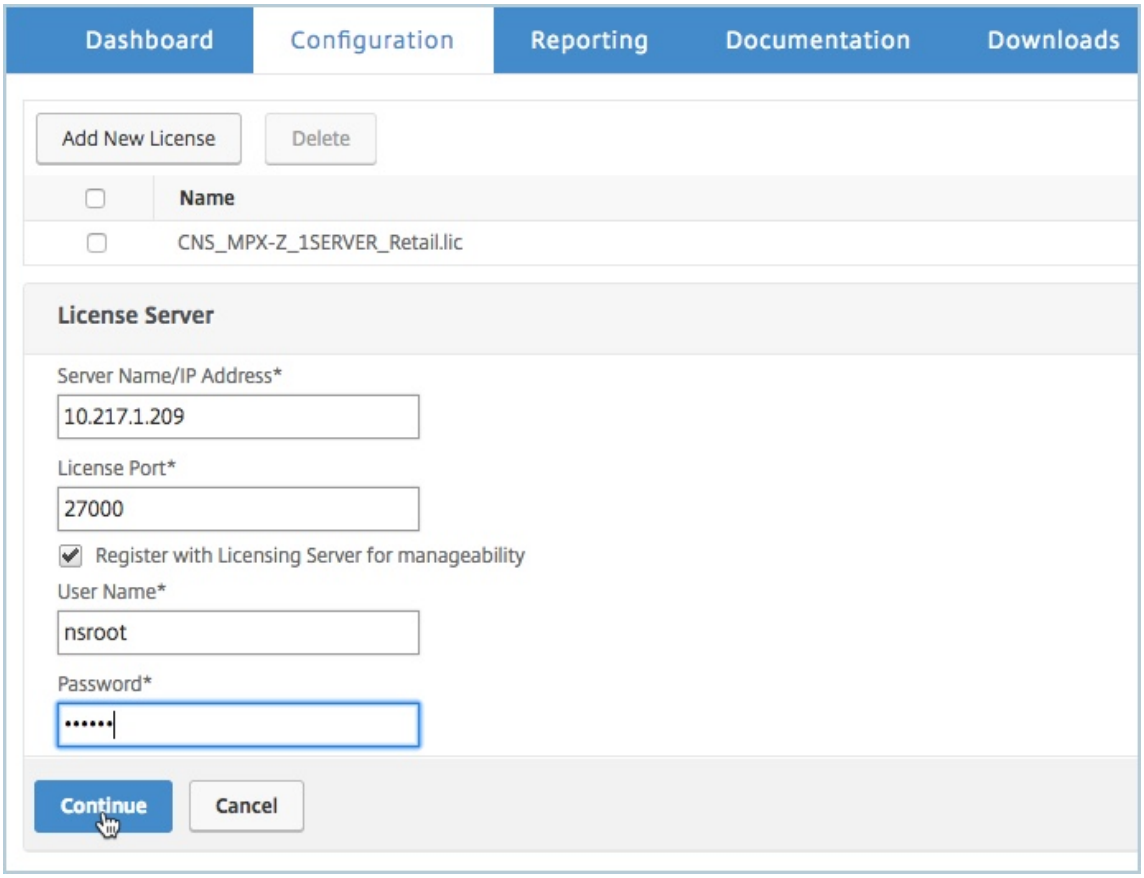
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. Klicken Sie auf der Willkommensseite auf den Abschnitt **Lizenzen** .



11. Führen Sie im Abschnitt **Lizenzserver** die folgenden Schritte aus:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

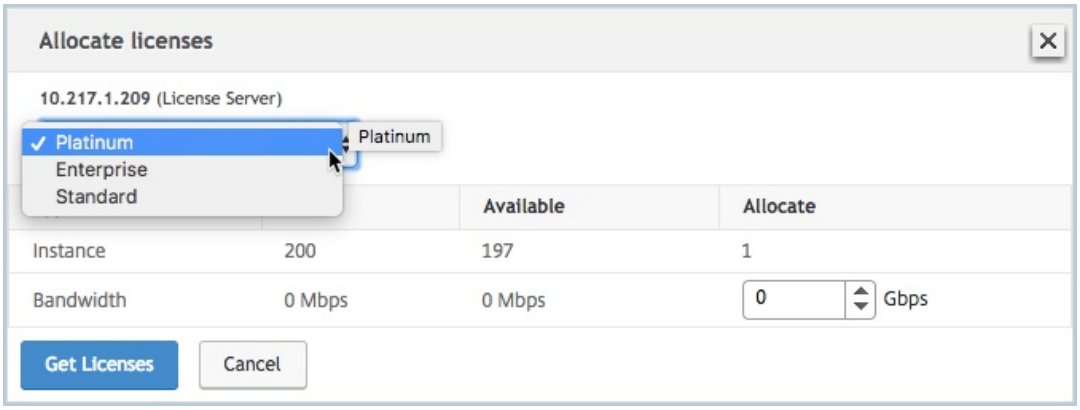
c) Wenn Sie die Poollizenzen Ihrer Instanz über Citrix ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Registrieren bei Lizenzierungsserver für Verwaltbarkeit**, und geben Sie ADM-Anmeldeinformationen ein.

d) Klicken Sie auf **Weiter**.

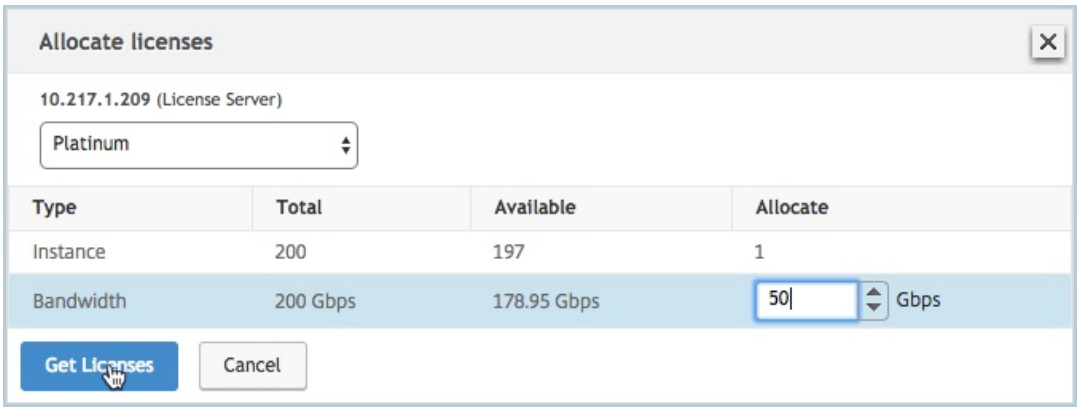
12. Gehen Sie im Fenster Lizenzen zuweisen wie folgt vor:

a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

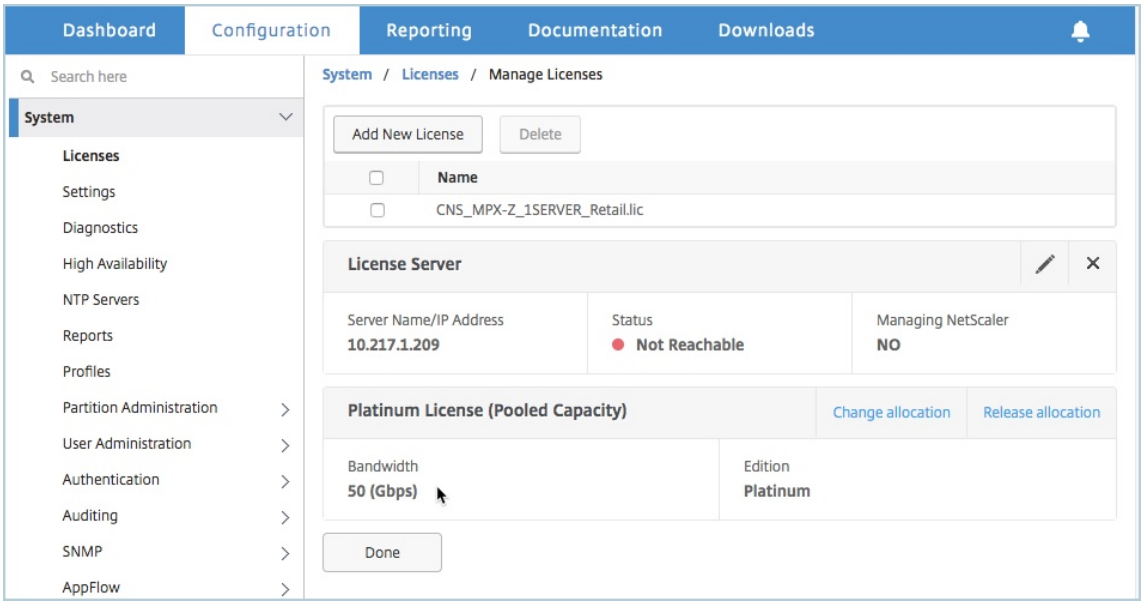
13. Melden Sie sich nach dem Neustart der NetScaler ADC MPX-Appliance bei der NetScaler ADC MPX-Appliance an. Klicken Sie auf der **Willkommensseite** auf **Weiter**.

    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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Aktualisieren Sie die unbefristete Lizenz im Citrix ADC MPX High Availability Pair auf Citrix ADC Pooled Capacity

Für NetScaler ADC MPX Appliances, die im Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie NetScaler ADC Pooled Capacity sowohl auf der primären als auch auf der sekundären NetScaler ADC-Instanz im HA-Paar konfigurieren. Sie müssen Lizenzen mit derselben Kapazität sowohl den primären als auch den sekundären NetScaler ADC Instanzen im HA-Paar zuweisen. Wenn Sie beispielsweise eine Kapazität von 1 Gbit/s von jeder Instanz im HA-Paar benötigen, müssen Sie 2 Gbit/s Kapazität aus dem gemeinsamen Pool zuweisen, damit Sie je 1 Gbit/s den primären und sekundären NetScaler ADC Instanzen im HA-Paar zuweisen können.

> **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.

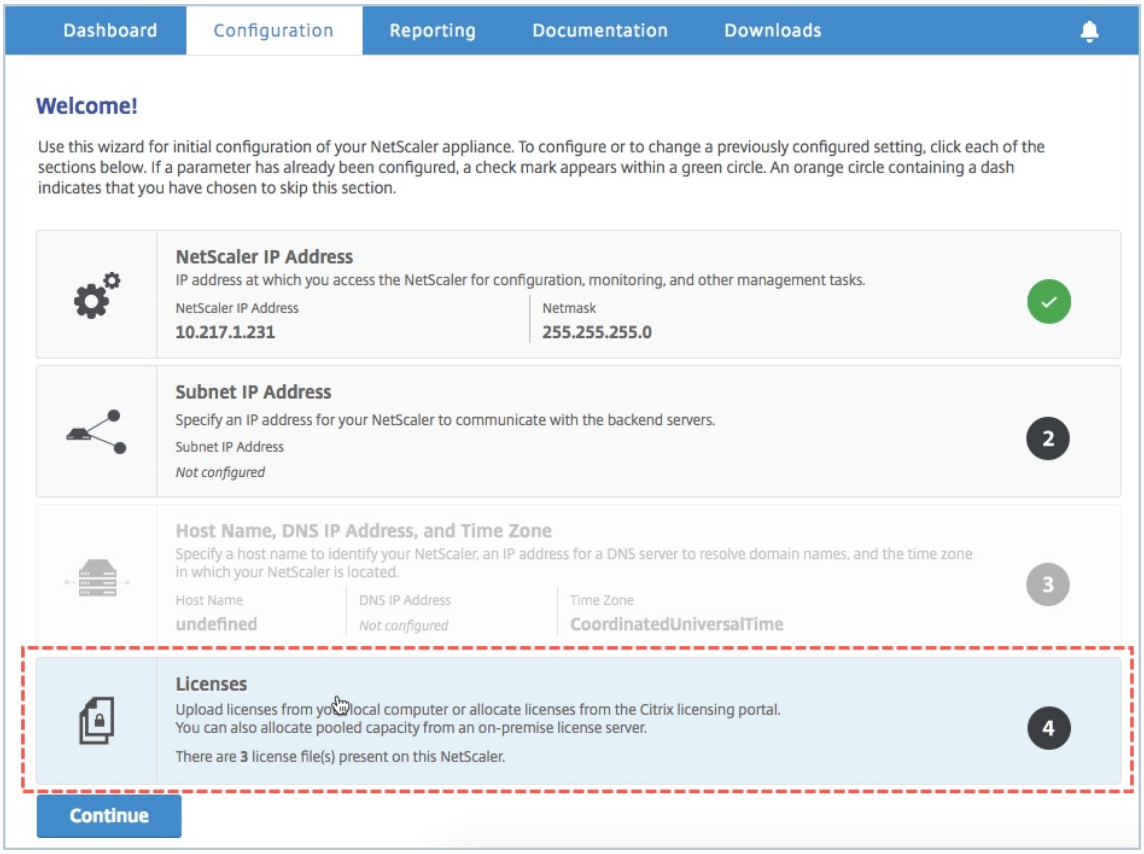
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

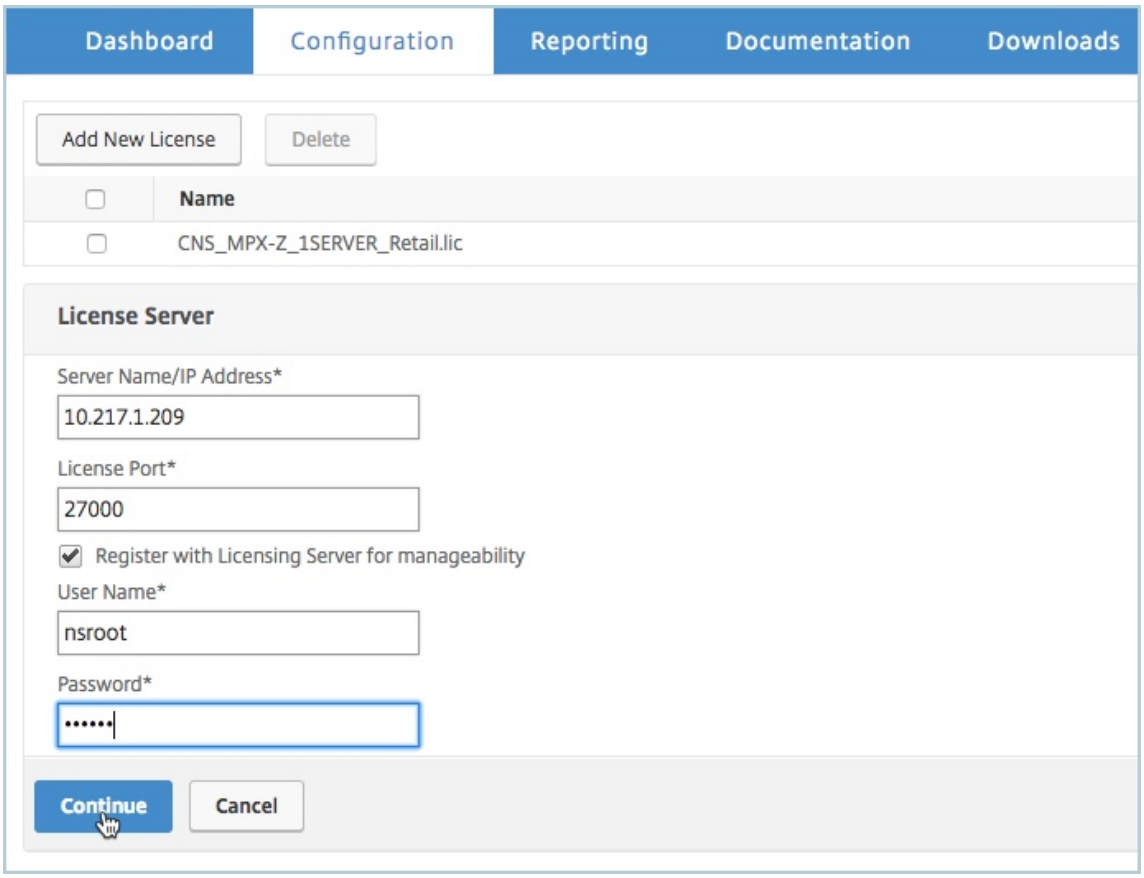
So aktualisieren Sie ein vorhandenes HA-Setup auf NetScaler ADC Pooled Capacity:

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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

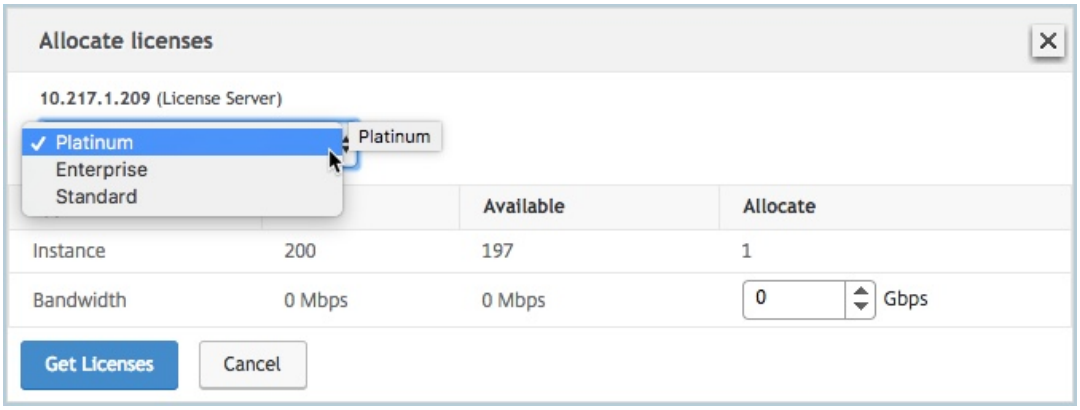
   c) Wenn Sie die Poollizenzen Ihrer Instanz über Citrix ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Registrieren bei Lizenzierungsserver für Verwaltbarkeit**, und geben Sie ADM-Anmeldeinformationen ein.

   d) Klicken Sie auf **Weiter**.

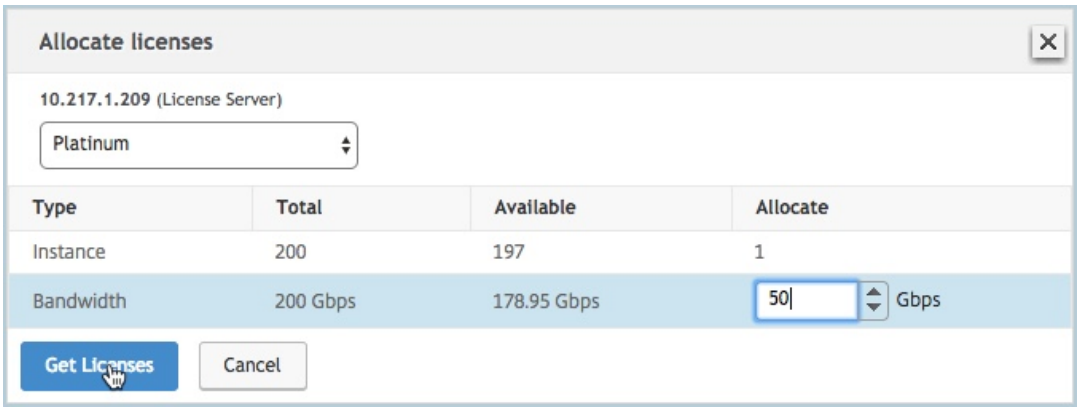
5. Gehen Sie im Fenster **Lizenzen zuweisen** wie folgt vor:

   a) Wählen Sie die Lizenzversion aus der Dropdownliste aus.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

Nachdem die sekundäre NetScaler ADC MPX-Appliance neu gestartet wurde, wird sie zur primären NetScaler ADC MPX-Appliance im HA-Paar.

6. Melden Sie sich bei der vorhandenen primären Citrix 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.

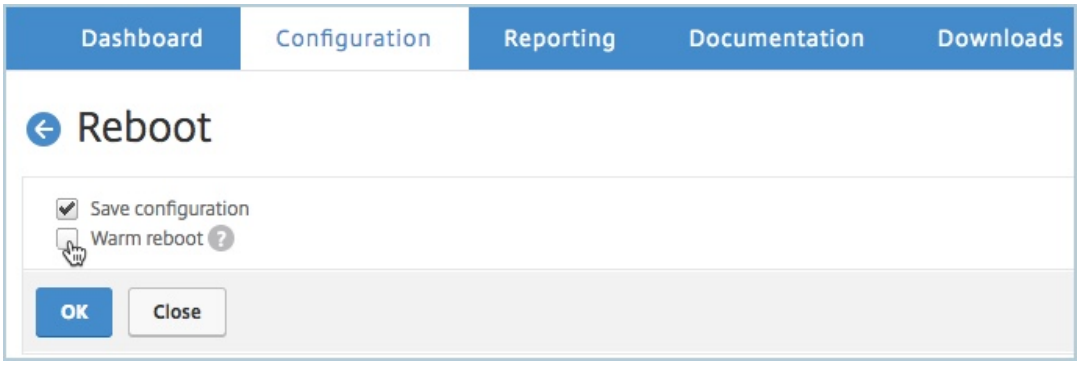
c) Klicken Sie auf der **Willkommensseite** auf **Weiter**.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nachdem die primäre NetScaler ADC MPX-Appliance neu gestartet wurde, wird sie zur sekundären NetScaler ADC MPX-Appliance im HA-Paar. Bei Bedarf können Sie die primäre und sekundäre Instanz im HA-Paar in Ihre ursprüngliche HA-Paar-Konfiguration ändern, indem Sie den folgenden Befehl für jede Instanz im HA-Paar verwenden:

```
> 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. Durch ein Upgrade auf die Citrix ADC Pooled Capacity-Lizenz können Sie Citrix ADC Appliances bei Bedarf Lizenzen aus dem Lizenzpool zuweisen. Sie können die NetScaler ADC Pooled-Capacity-Lizenz auch für NetScaler ADC-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind.

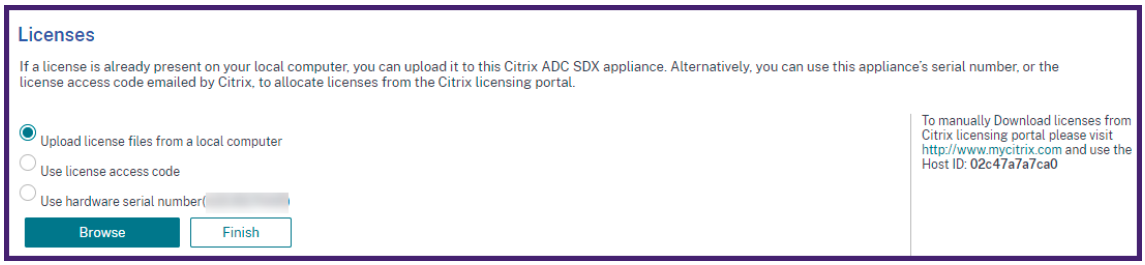
> **Wichtig!**
>
> Um die SDX-Appliance auf die Citrix ADC Pooled Capacity-Lizenz zu aktualisieren, müssen Sie die SDX-Z-Lizenz auf die Appliance hochladen.

So aktualisieren Sie auf NetScaler ADC gepoolte Kapazität:

1. Geben Sie in einem Webbrowser die IP-Adresse der SDX ADC-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**.

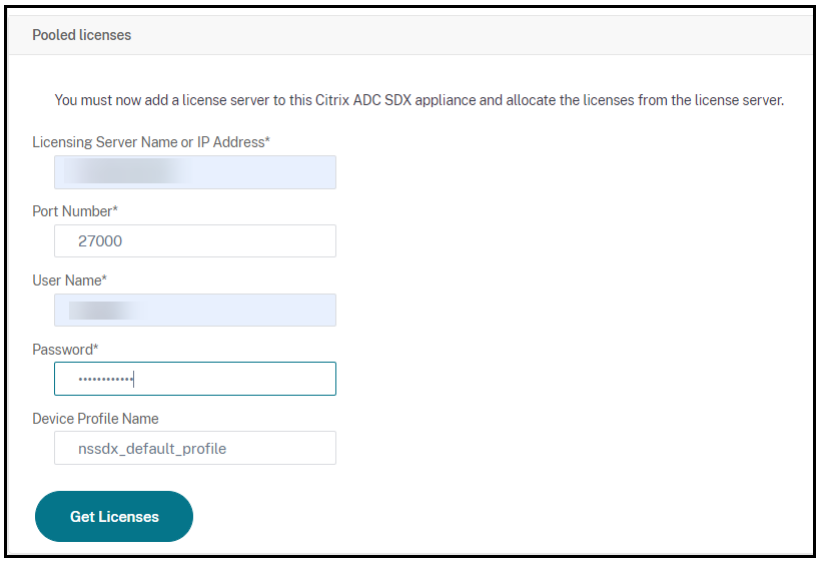
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Laden Sie die Lizenz ohne Kapazität hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen** .
5. Navigieren Sie zu **System** > **Lizenzen** .
6. Klicken Sie auf der Seite **Lizenzen** auf **Lizenzen verwalten** und dann auf **Neue Lizenz hinzufügen**.
7. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien hochladen** aus und klicken Sie auf **Durchsuchen**, um die Nullkapazitätslizenz von 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.

8. Führen Sie im Abschnitt **Pooled Lizenzen** die folgenden Schritte aus:



a) Geben Sie im Feld **Lizenzservername oder IP-Adresse** die Details des Lizenzservers ein.

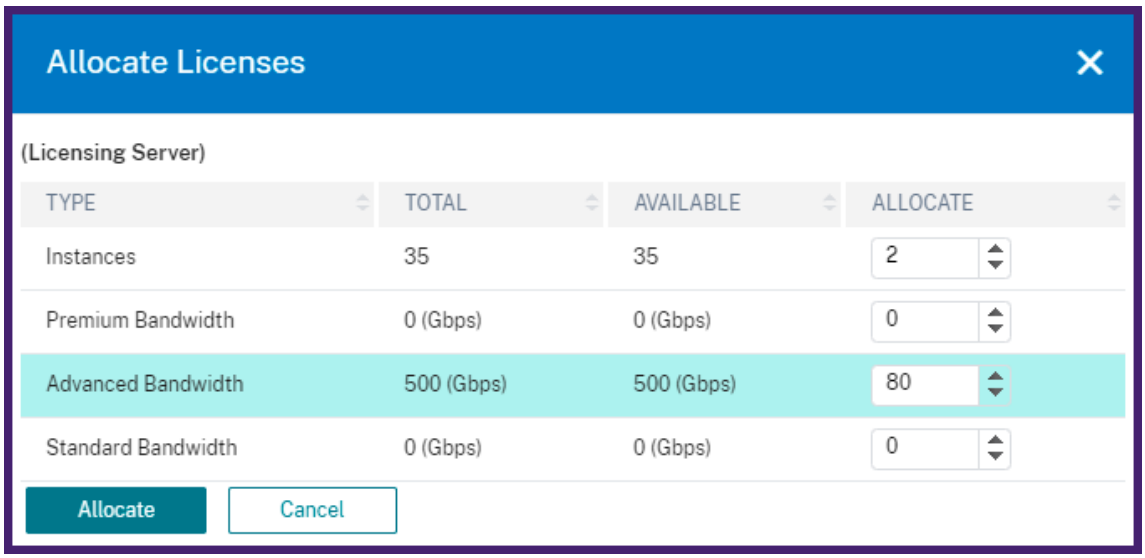
b) Geben Sie im Feld **Portnummer** den Lizenzserverport ein. Standardwert: 27000.

c) Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler ADM verwalten möchten, aktivieren Sie das Kontrollkästchen **Bei NetScaler ADM registrieren**, und geben Sie die ADM-Anmeldeinformationen ein.

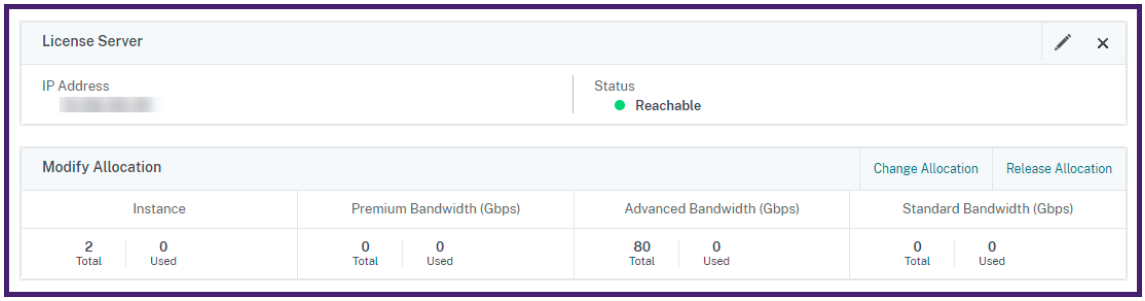
d) Klicken Sie auf **Get Licenses**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. 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 Lizenzedition sowie der zugewiesenen Instanzen und Bandbreite aus dem Pool anzeigen.



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. Im Folgenden sind die Voraussetzungen für die Konfiguration der gepoolten Kapazität auf Citrix ADC-Instanzen im Clustermodus aufgeführt:

- Instanzen sollten einzeln in einem Lizenzmodus mit gepoolter Kapazität ausgeführt werden, um den Cluster zu bilden.
- Alle Instanzen sollten mit derselben Bandbreite ausgeführt werden.
- Alle Instanzen sollten die gepoolte Kapazität aus demselben Citrix Application Delivery Management (ADM) auschecken.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.

Bei jedem Kapazitäts-Check-out aus dem Citrix ADC-Cluster wird allen Clusterknoten dieselbe Kapazität zugewiesen und die Checkout-Bandbreite = bereitgestellte Bandbreite * Anzahl der Knoten.

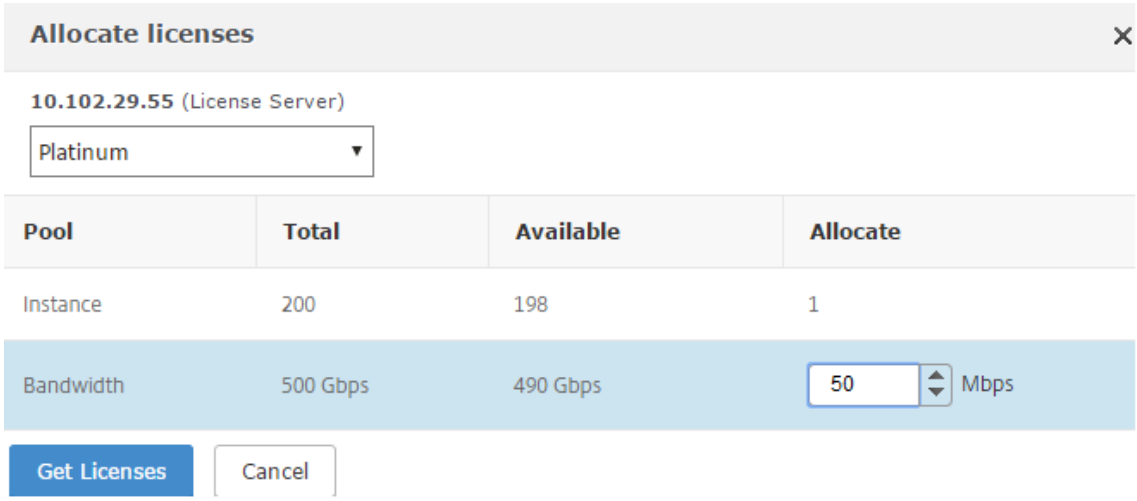
Wenn Sie beispielsweise 50 Mbit/s Bandbreite aus dem Citrix ADC-Cluster auschecken und der Cluster 12 Instanzen umfasst, erhält jede Instanz automatisch 50 Mbit/s; und 600 Mbit/s werden aus dem Pool ausgecheckt.

> **Hinweis**
>
> Wenn eine oder mehrere Instances im Cluster nicht mehr reagieren, arbeitet der Cluster weiterhin mit der Kapazität der verbleibenden Instances.

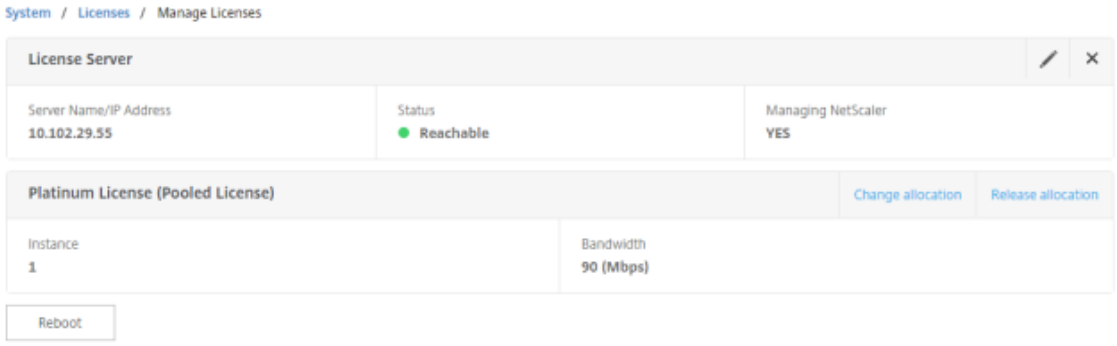
So weisen Sie Citrix ADC Pooled Capacity auf Citrix ADC-Instanzen im Clustermodus zu:

1. Geben Sie in einem Webbrowser die IP-Adresse der **Cluster-IP**-Adresse (CLIP) 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 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



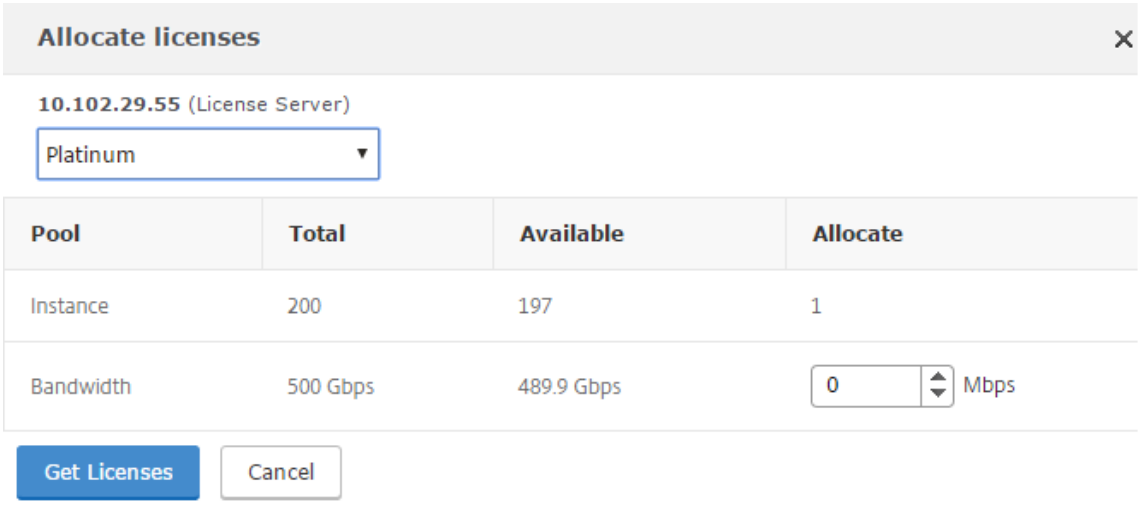
7. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie **Zuordnung ändern oder Zuordnungfreigeben**wählen.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

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.

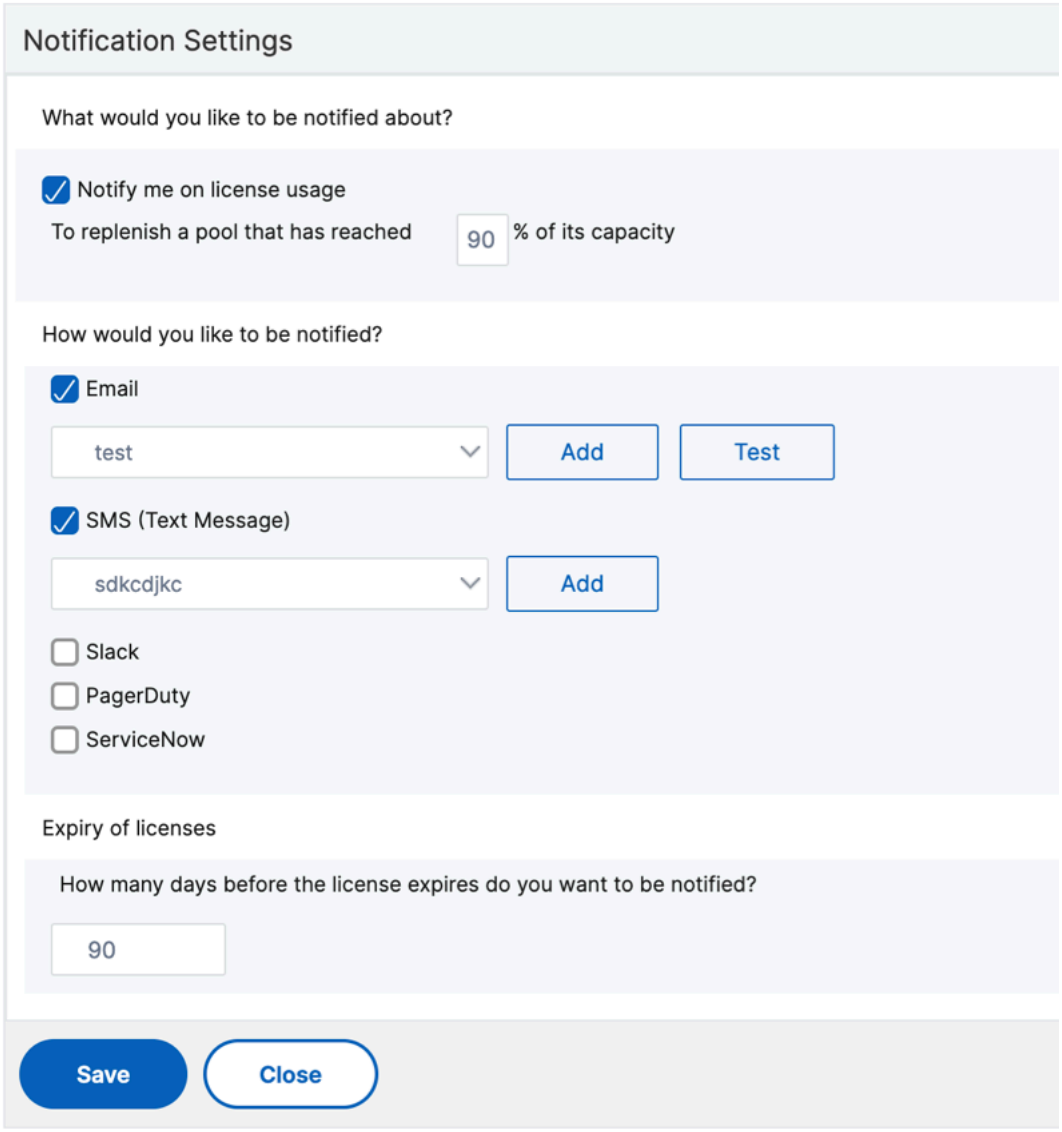
Gnadenfrist

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Citrix ADC wird weiterhin mit der aktuellen Kapazität für 30 Tage arbeiten. Wenn die Verbindung zum Lizenzserver nach 30 Tagen nicht wiederhergestellt wird, verliert Citrix 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 Anforderung zum Auschecken aller Lizenzen vom Lizenzserver.

Sowohl der Lizenzserver als auch die NetScaler ADC Instanz mit aktivierter Kapazität reagieren nicht mehr

Wenn sowohl der Lizenzserver als auch die Citrix ADC Instanz mit aktivierter Kapazität neu gestartet und die Verbindung wiederhergestellt wird, checkt der Lizenzserver alle Lizenzen nach 10 Minuten ein, und die Citrix ADC-Instanzen mit aktivierter Kapazität 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 die Lizenzen einchecken, wird die Citrix ADC Instanz mit aktivierter Kapazität nach dem Neustart

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nicht lizenziert. Wenn Sie die Lizenzen beibehalten möchten, werden sie beim Herunterfahren der Instanz beim Lizenzierungsserver eingecheckt. Nach dem Neustart der Instanz stellt sie die Verbindung mit dem Lizenzserver wieder her und checkt die Lizenzen wie in der gespeicherten Konfiguration angegeben aus.

Wenn das System neu gestartet wird und das Auschecken fehlschlägt, weil keine Kapazität im Pool verfügbar ist, überprüft Citrix ADC die Bestandsaufnahme der Citrix Application Delivery Management (ADM) Poollizenzen und überprüft die verfügbare Kapazität. Ein SNMP-Alarm wird ausgelöst, um diesen Zustand an den Benutzer zu benachrichtigen, wenn Citrix ADC nicht mit voller Kapazität gemäß Konfiguration ausgeführt wird. Wenn im Bandbreitenpool keine Kapazität verfügbar ist, wird die Poolkapazitätsaktivierte Instanz 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

NetScaler ADC VPX Ein- und Auschecken Lizenzierung

February 5, 2024

Sie können Citrix ADC VPX-Instanzen bei Bedarf über Citrix Application Delivery Management (ADM) VPX-Lizenzen zuweisen. Die Lizenzen werden von NetScaler ADM gespeichert und verwaltet, das über ein Lizenzierungsframework verfügt, das skalierbare und automatisierte Lizenzbereitstellung ermöglicht. Eine NetScaler ADC VPX Instanz kann die Lizenz vom NetScaler ADM auschecken, wenn eine NetScaler ADC VPX Instanz bereitgestellt wird, oder ihre Lizenz an NetScaler ADM zurückchecken, wenn eine Instanz entfernt oder zerstört wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.
   - **Lizenzzugriffscode verwenden** : Citrix sendet den License Access Code (LAC) für die erworbenen Lizenzen per E-Mail.
     Um Lizenzdateien hinzuzufügen, geben Sie den LAC 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 LAC-Code für die Installation der Lizenzen verwenden.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

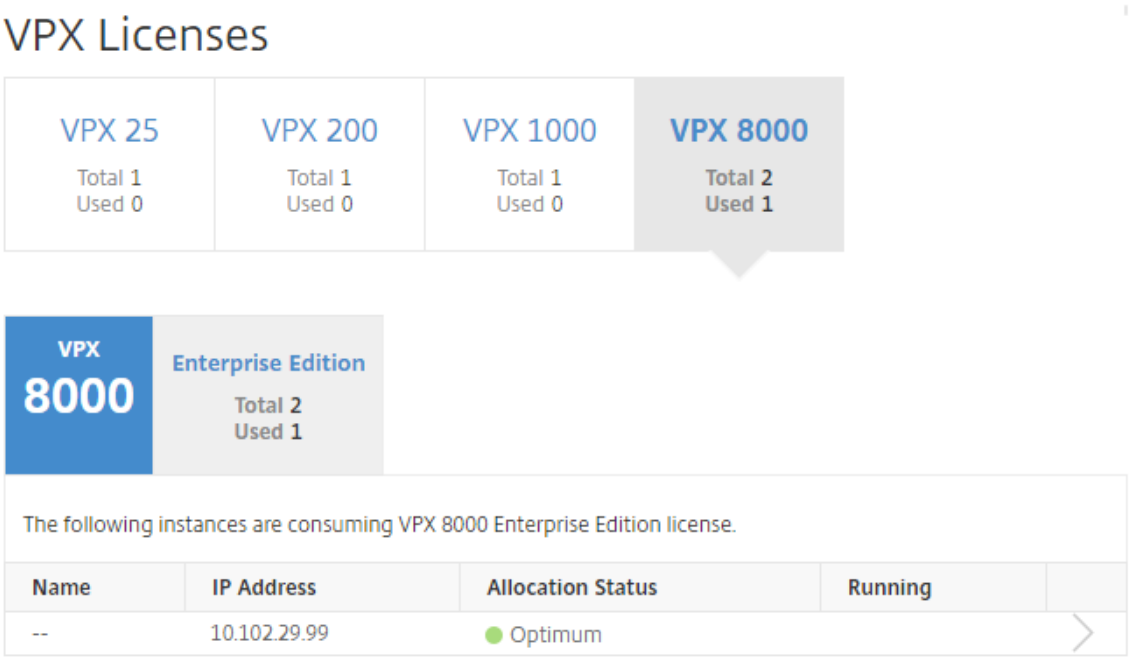
Sie können dem NetScaler ADM jederzeit über die Lizenzeinstellungen weitere Lizenzen hinzufügen.

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.**



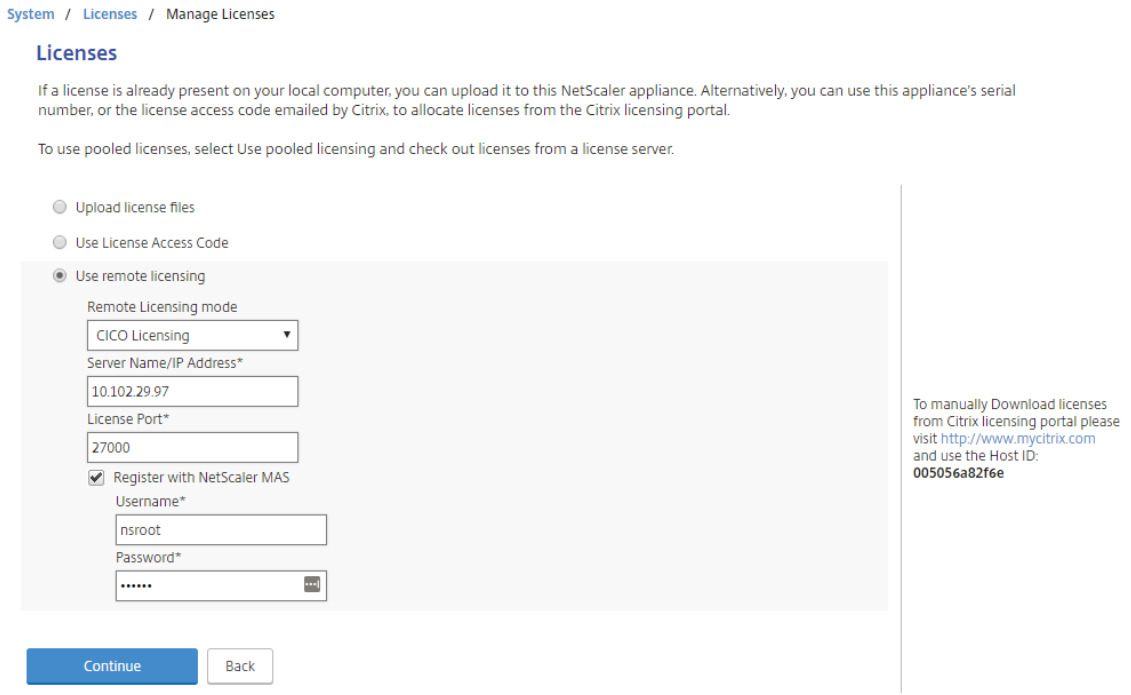
4. Sie können die zugewiesenen Lizenzen in der Tabelle im Abschnitt Verfügbare Lizenzen anzeigen.

Zuweisen von VPX-Lizenzen zu einer NetScaler ADC VPX Instanz mithilfe der NetScaler ADC-GUI

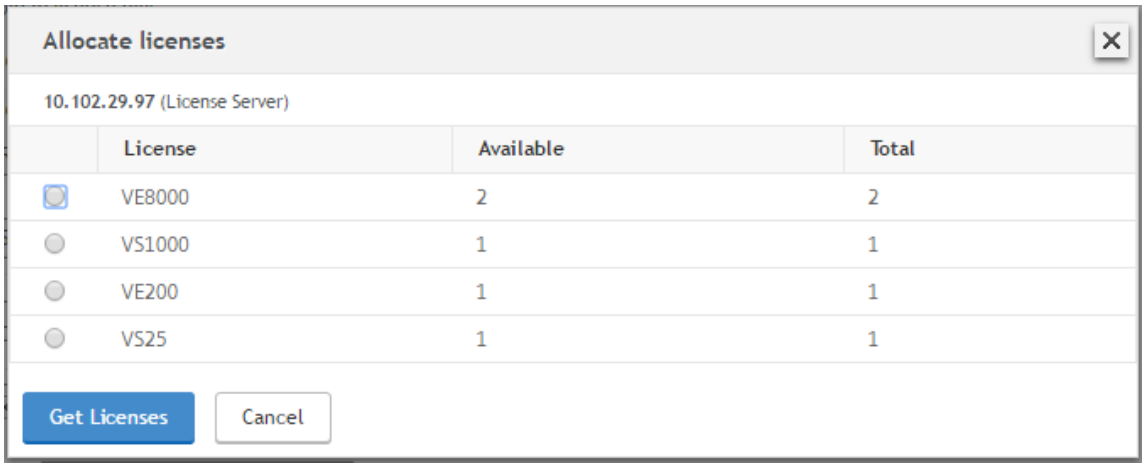
1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler ADC Instanz ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > Lizenzen > **Lizenzenverwalten**, klicken Sie auf**Neue Lizenz hinzufügen**und wählen Sie**Remote-Lizenzierung verwenden** aus.
4. Geben Sie die Details des Lizenzservers in das **Feld**Servername**/IP-Adresse** ein .
5. Wenn Sie die VPX-Lizenzen Ihrer Instanz über Citrix ADM () verwalten möchten, aktivieren Sie das Kontrollkästchen Bei **Citrix ADM registrieren** und geben Sie die Citrix ADM-Anmeldeinformationen ein.

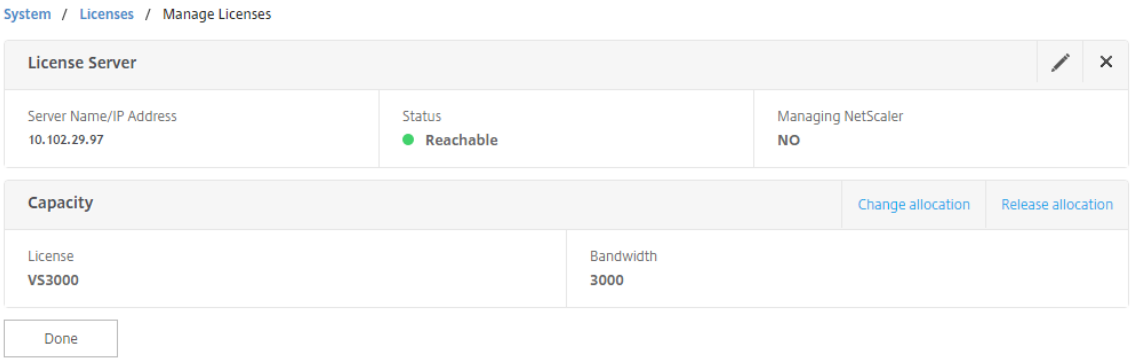


6. Wählen Sie die Lizenzedition mit der erforderlichen Bandbreite aus, und klicken Sie auf **Lizenzen abrufen**.



7. Klicken Sie auf **Reboot** , Ihre Citrix ADC VPX-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.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-Lizenzen zu einer NetScaler ADC VPX Instanz mithilfe der NetScaler ADC-CLI

1. Geben Sie in einem SSH-Client die IP-Adresse der Citrix ADC-Instanz ein und melden Sie sich mit Administratoranmeldeinformationen an.
2. Geben Sie den folgenden Befehl ein, um einen Lizenzserver hinzuzufügen:

```
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:

```
1 sh licenseserverpool
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<!--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
```

Zuweisen von VPX-Lizenzen zu einer NetScaler ADC VPX Instanz mithilfe der API

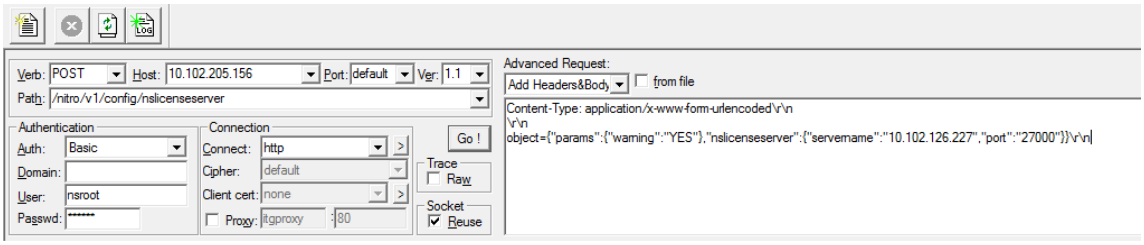
Melden Sie sich in einem Webbrowser oder einem API-Client an der Citrix ADC VPX Instanz mit den Administratoranmeldeinformationen an.

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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

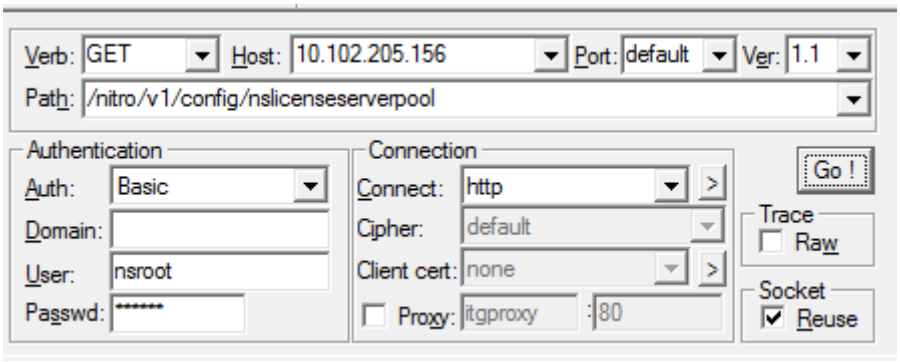


NetScaler ADM antwortet auf die Anforderung. Die folgende Beispielantwort zeigt Erfolg.

```
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.

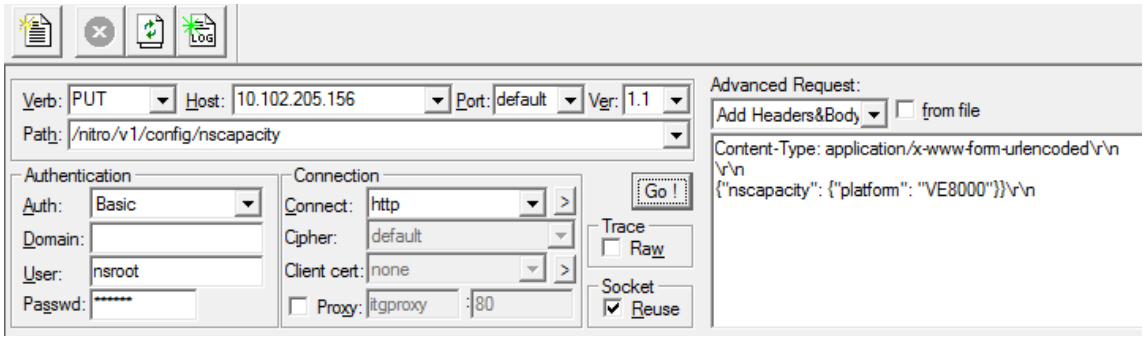
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 VPX Appliance eine Lizenz zu:

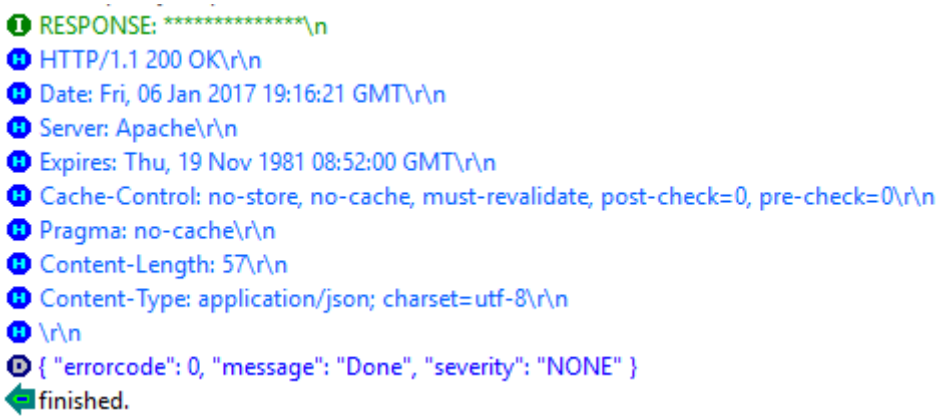
1. Legen Sie den Anforderungstyp auf **Post**fest.
2. Stellen Sie den Pfad zu /nitro/v1/config/nscapacity.
3. Legen Sie die Nutzlast wie folgt fest:

```
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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Konfigurieren von Ablaufprüfungen für NetScaler ADC VPX Ein-/Auscheck-Lizenzen

Sie können jetzt den Grenzwert für den Lizenzablauf für NetScaler ADC VPX-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 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Eine solche Bewegung erfordert auch, dass die Softwareanforderungen dynamisch, flexibel und agil sind, um die sich ständig ändernden Geschäftsanforderungen zu erfüllen. Es wird erwartet, dass Lizenzen von einem zentralen Management-Tool verwaltet werden, das volle Einblick in die Nutzung bietet.

Virtuelle CPU-Lizenzierung für NetScaler 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

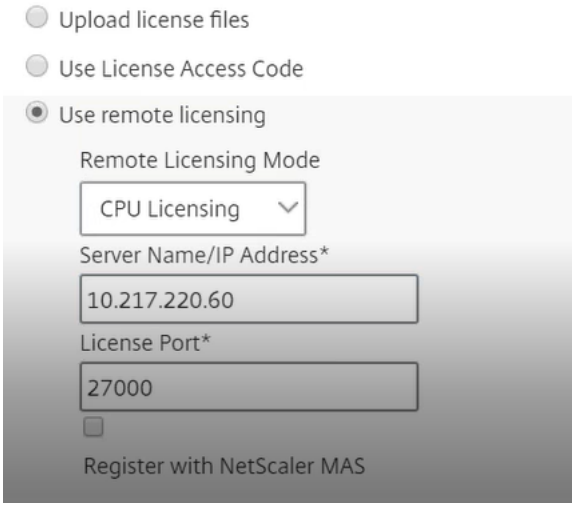
In der virtuellen CPU-Usage-basierten Lizenzierungsfunktion gibt die Lizenz die Anzahl der CPUs an, auf die ein bestimmtes NetScaler ADC VPX berechtigt ist. Daher kann Citrix ADC VPX Lizenzen nur für die Anzahl der auf ihm ausgeführten virtuellen CPUs vom Lizenzserver aus auschecken. NetScaler ADC VPX 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 handelt es sich bei den drei Editionen, die für virtuelle CPU-Lizenzen verwaltet werden, um Standard, Enterprise und Platinum. 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. Sie müssen den NetScaler ADC VPX neu starten, nachdem Sie die Lizenzen ausgecheckt haben.

So konfigurieren Sie den Lizenzierungsserver in NetScaler ADC VPX mit der GUI:

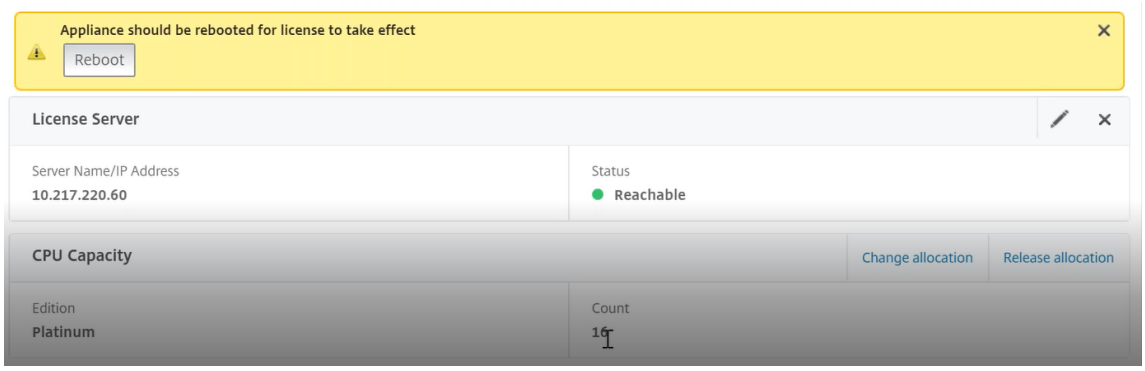
1. Navigieren Sie in NetScaler ADC VPX zu **System** > **Lizenzen** und klicken Sie auf **Lizenzen verwalten**.
2. Klicken Sie auf der Seite **Lizenz** auf **Neue Lizenz hinzufügen**.
3. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden** .
4. Wählen Sie **CPU-Lizenzierung** aus der Liste **Remote-Lizenzierungsmodus** aus.
5. Geben Sie die IP-Adresse des Lizenzservers und die Portnummer ein.
6. Klicken Sie auf **Weiter**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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 Enterprise 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 platinum
<!--NeedCopy-->
```

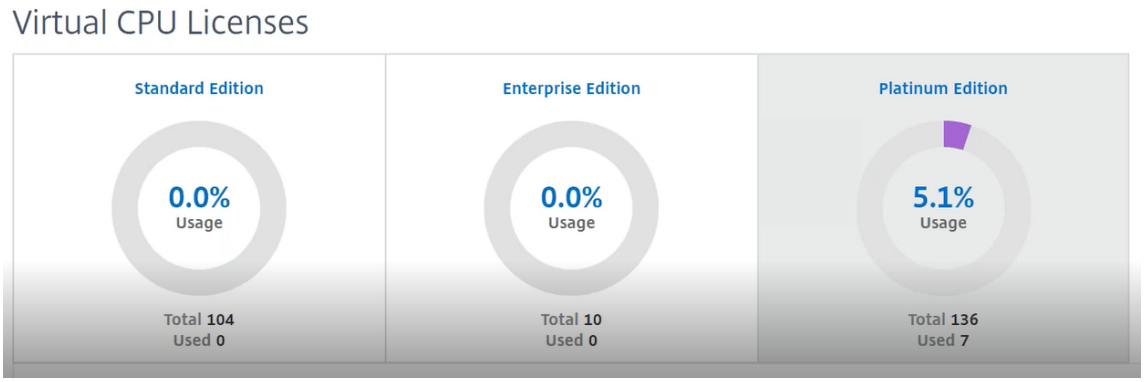
   Wenn Sie dazu aufgefordert werden, starten Sie die Instanz neu, indem Sie den folgenden Befehl eingeben:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
reboot -w
<!--NeedCopy-->
```

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 Citrix 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>
<!--NeedCopy-->
```

Für die CPX-Lizenzierung stehen drei Lizenztypen zur Verfügung:

1. Unterstützte virtuelle CPU-Abonnementlizenzen für CPX und VPX
2. Lizenzen für gepoolte Kapazität

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

Sie müssen die Anzahl der vCPU-Lizenzen angeben, die die Citrix ADC CPX-Instanz verwendet.

- Dieser Wert wird als Umgebungsvariable über Docker, Kubernetes oder Mesos/Marathon eingegeben.
- Die Zielvariable lautet "CPX_CORES". Die CPX kann 1 bis 7 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-Instanz checkt die Anzahl der Lizenzen "n"aus, wenn die Instanz mit "n"CPUs ausgeführt wird.

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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Multicore-CPX-Anwendungsfälle checken „n"vCPUs aus (wobei „n"zwischen 1 und 7 steht).

```
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 BANDWIDTH=2000 cpx:11.1
2 <!--NeedCopy-->
```

Kapazität gepoolt. Mit diesem Befehl wird eine Lizenz aus dem Instanzpool ausgecheckt und 1000 Mbit/s Bandbreite aus dem Platin-Bandbreitenpool verbraucht, aber CPX kann bis zu 2000 Mbit/s laufen.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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Stellen Sie Citrix ADM mit VMware ESXi bereit

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

So ändern Sie den gemeldeten Schweregrad von Ereignissen, die auf NetScaler-Instances 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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-Appliances werden als verwaltete Instanzen in Citrix ADM registriert und ihre AppFlow Datensätze werden erfasst. Bei einer Citrix

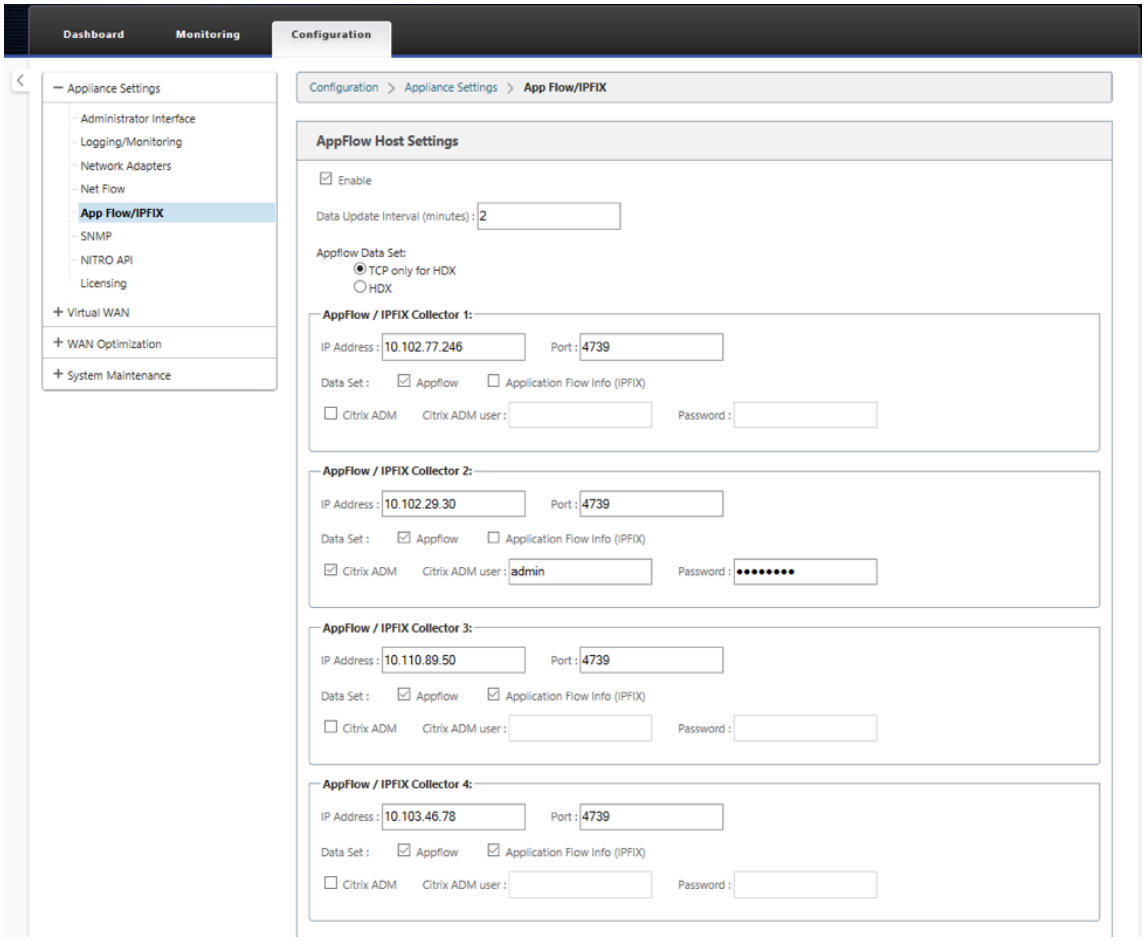
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

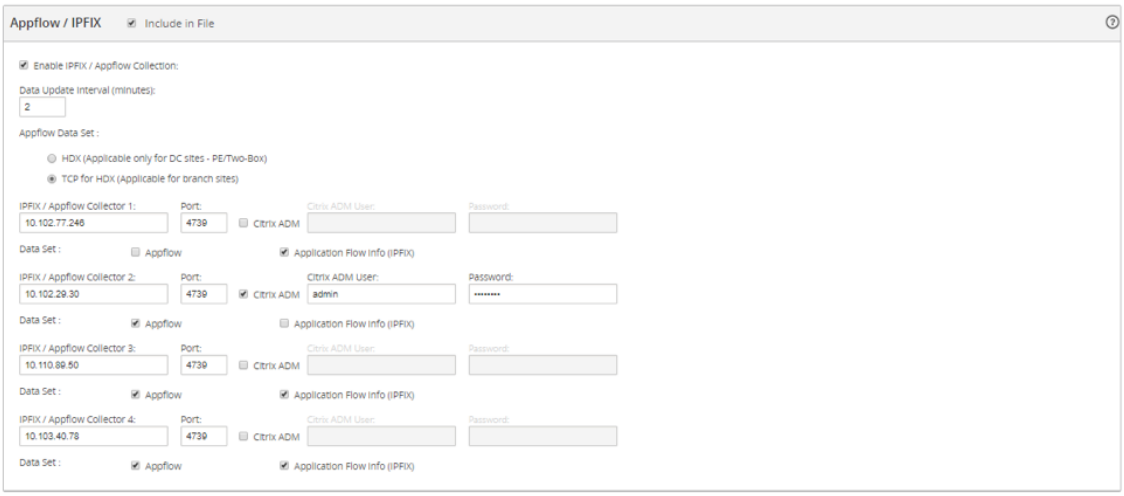
8. Geben Sie die Anmeldeinformationen für den Citrix ADM -Server ein
9. Klicken Sie auf **Einstellungen anwenden**.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

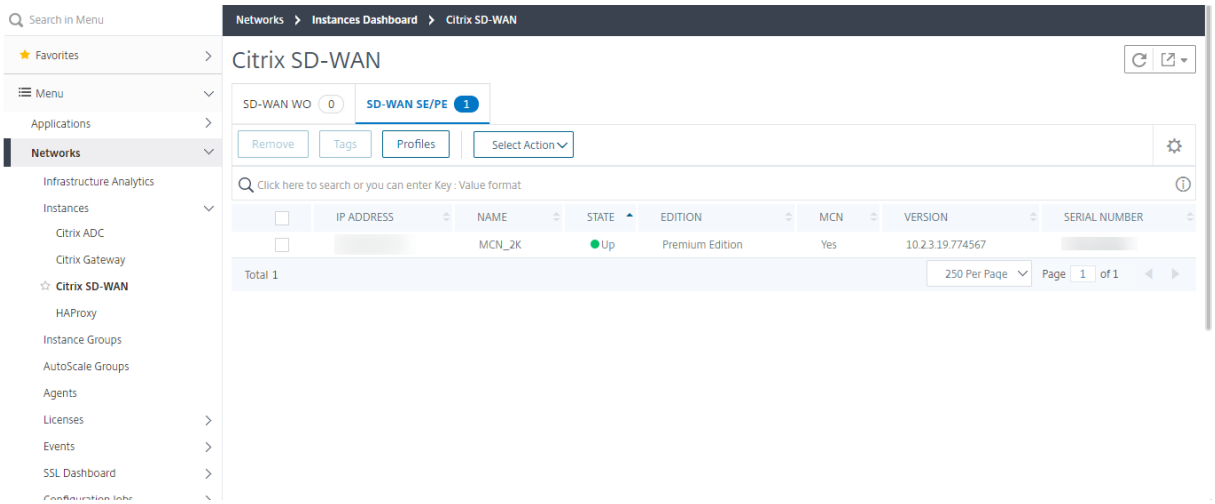
> Sie können bis zu vier AppFlow-Kollektoren hinzufügen. NetScaler ADM oder ein AppFlow Collector, der das IPFIX-Protokoll unterstützt.

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.

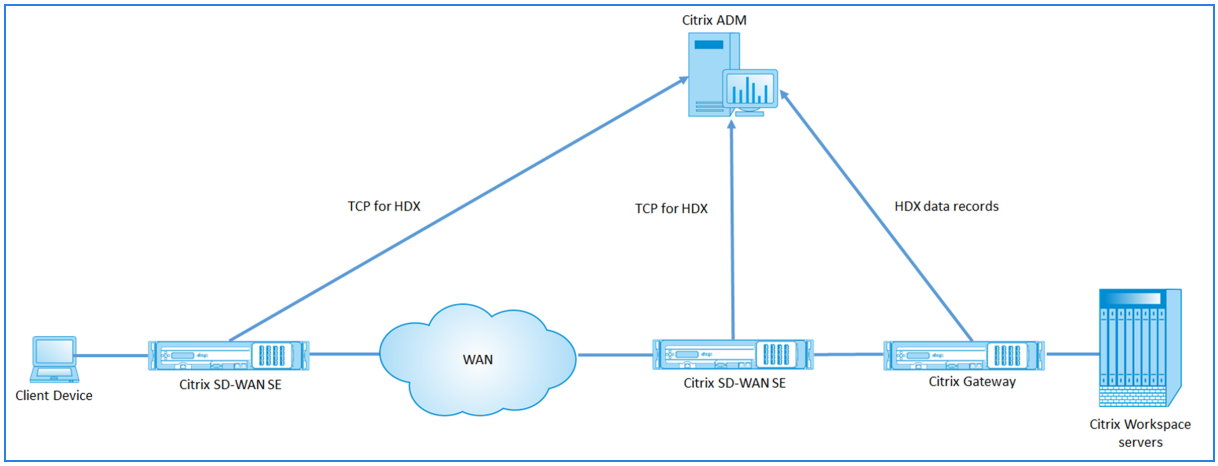
Bei einer Citrix SD-WAN PE-Appliance können Sie je nach AppFlow Konfiguration HDX-Datensätze oder Multi-Hop-Daten anzeigen. Eine Citrix SD-WAN SE-Appliance stellt nur Multi-Hop-Daten bereit. Weitere Informationen finden Sie unter Anzeigen von HDX Insight-Berichten und -Metriken und Anzeigen von Citrix SD-WAN Analytics-Daten für die Multi-Hop-Bereitstellung.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

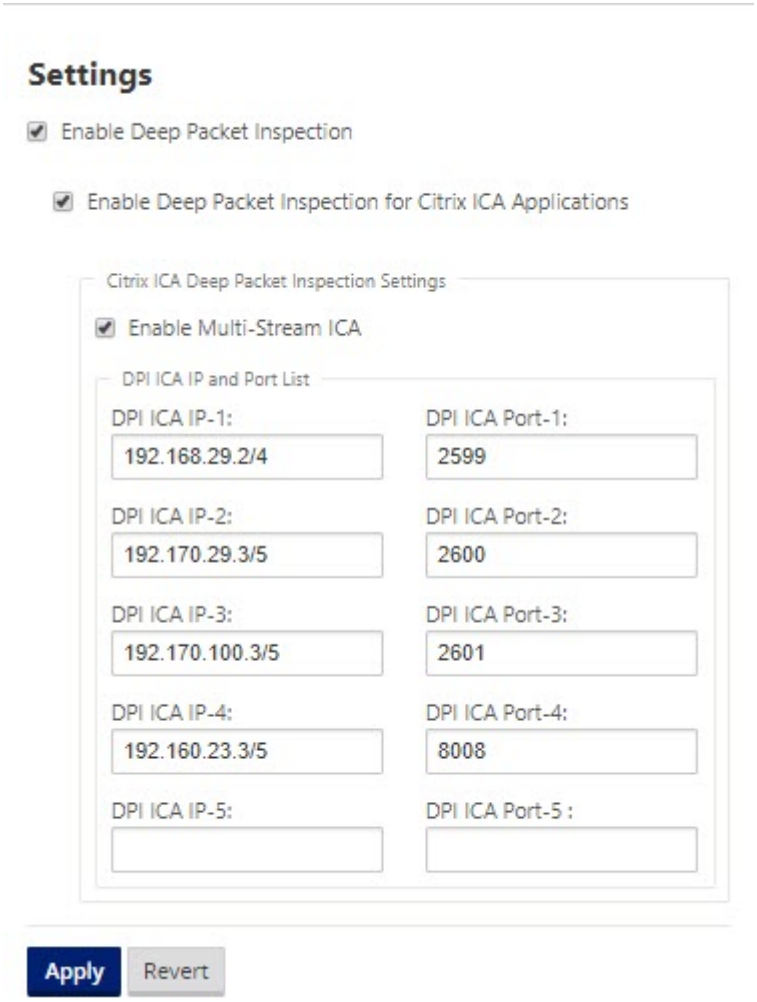
Citrix ADM verwendet die Hop-Anzahl und die Verbindungsketten-ID, um die Daten von den Appliances zu korrelieren, und generiert die Berichte.

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**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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-

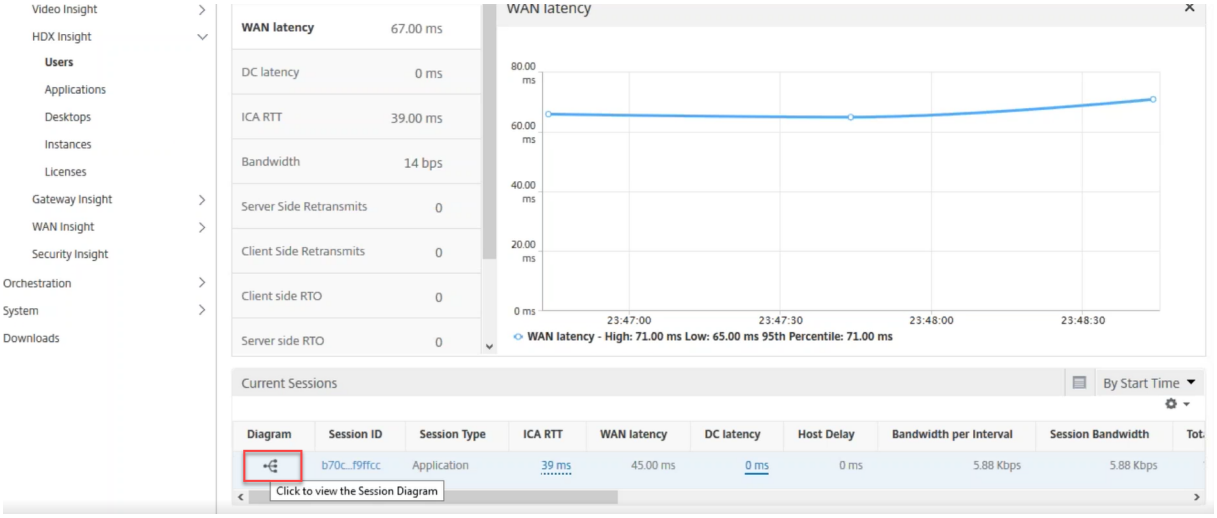
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Appliance aktiviert sein.

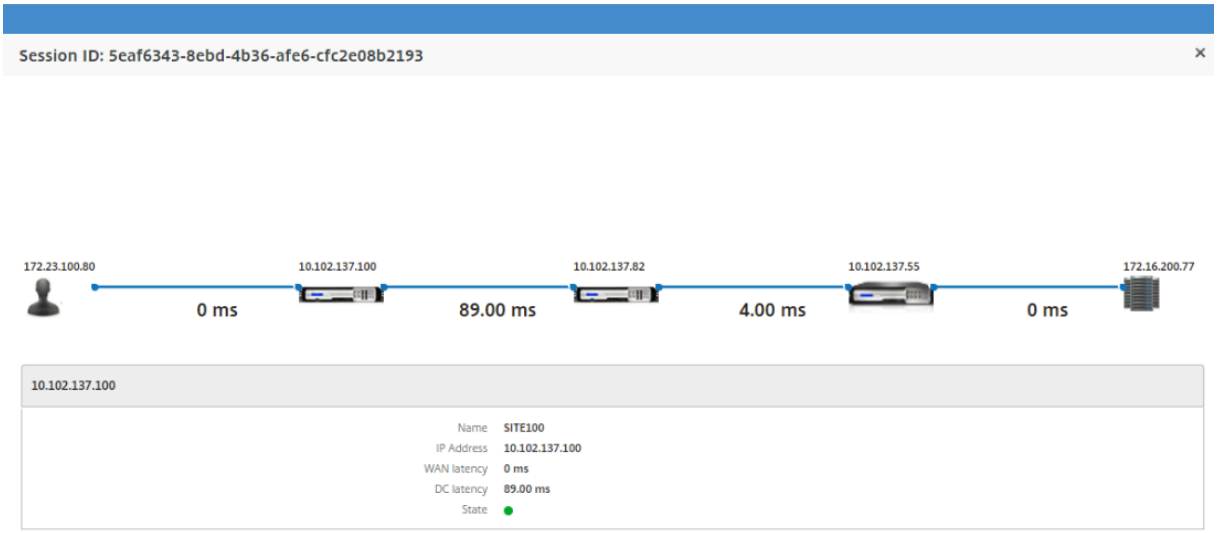
> **Hinweis**
>
> Stellen Sie in einer Multi-Hop-Bereitstellung sicher, dass nur eines der Netzwerkgeräte HDX Insight-Daten sendet. Die übrigen Netzwerkgeräte können TCP für HDX-Daten senden.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Hinweis**
>
> Die angezeigten Informationen hängen vom ausgewählten Netzwerkelement ab.

Die folgenden Parameter werden für Citrix Appliances angezeigt:

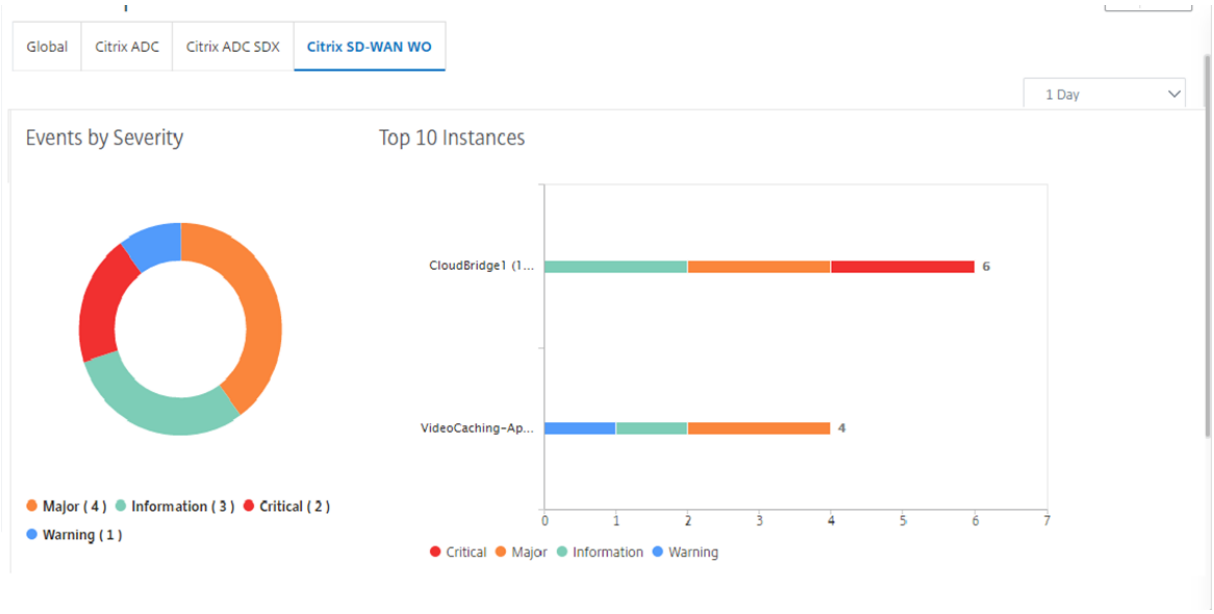
- **Name**: Name der Citrix-Appliance.
- **IP-Adresse**: IP-Adresse der Appliance.
- **WAN-Latenz**: Latenz, die durch die Client-Seite des Netzwerks verursacht wird. Das heißt, von der Citrix-Appliance bis zum Endbenutzer.
- **DC-Latenz**: Latenz, die durch die Serverseite des Netzwerks verursacht wird. 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.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

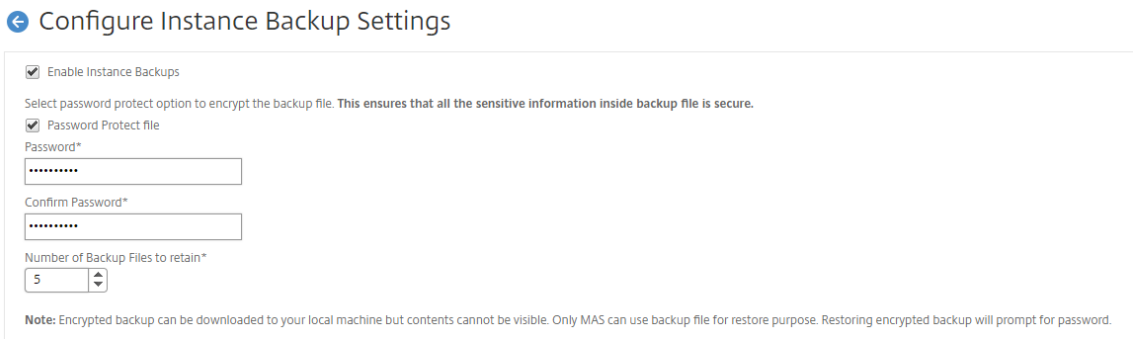
Bevor Sie ein Backup der Citrix SD-WANOP-Instanz in Citrix ADM erstellen, müssen Sie die Einstellungen für das Instanzbackup in Citrix ADM konfigurieren.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

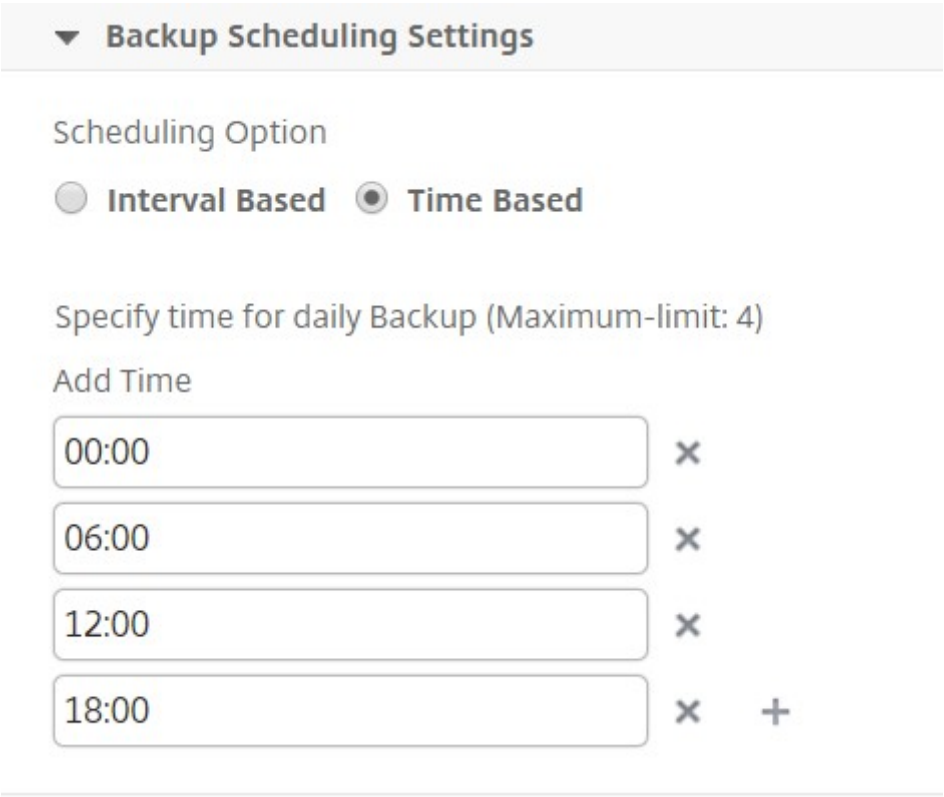
> **Hinweis**
>
> Jede Backupdatei erfordert einige Speicheranforderungen. Citrix empfiehlt, dass Sie gemäß Ihren Anforderungen eine optimale Anzahl von Backupdateien auf Citrix ADM speichern.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



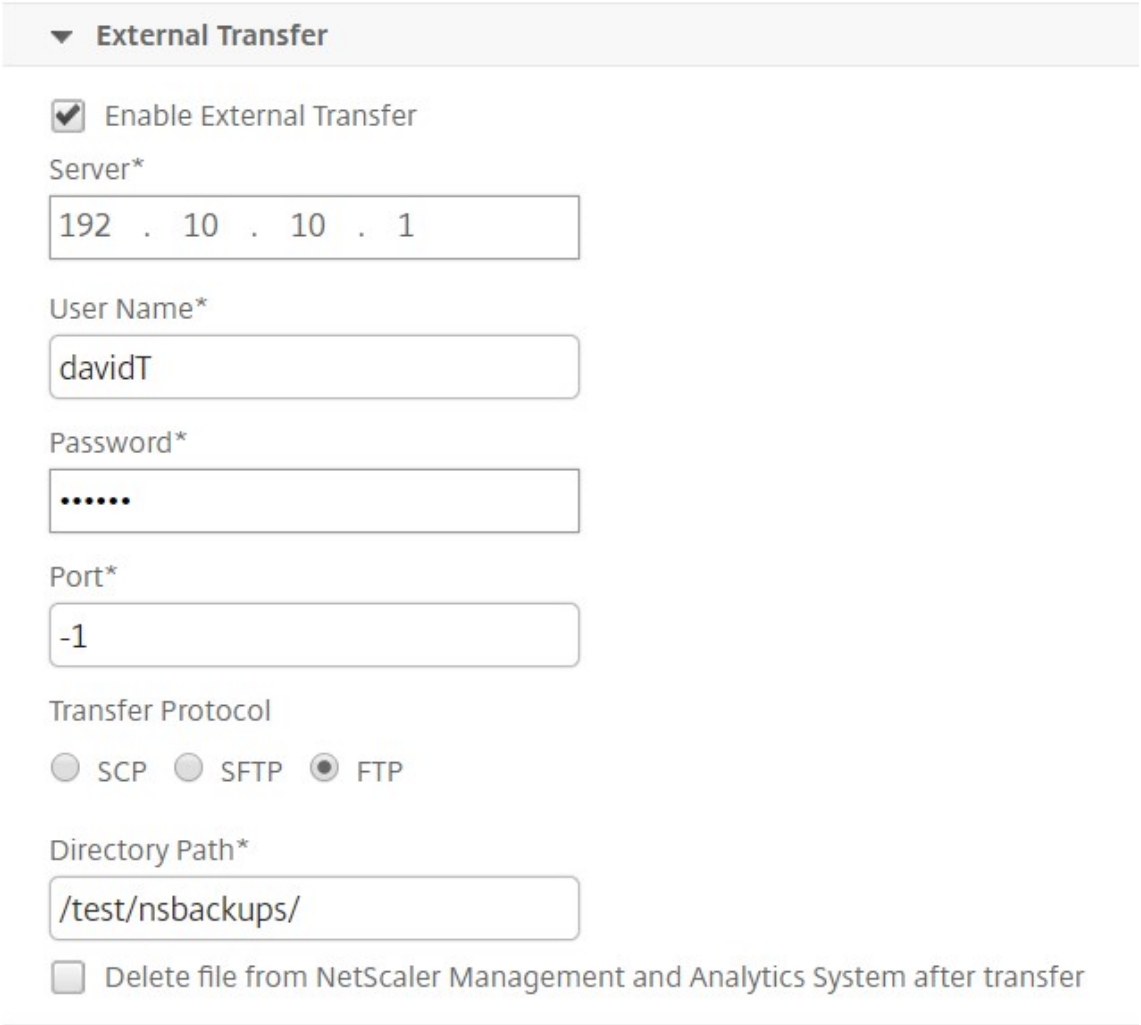
> **Hinweis**
>
> Ignorieren **Sie den Abschnitt Citrix ADC-Einstellungen**. Diese Einstellungen gelten nicht für Citrix SD-WANOP-Instanzen.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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.

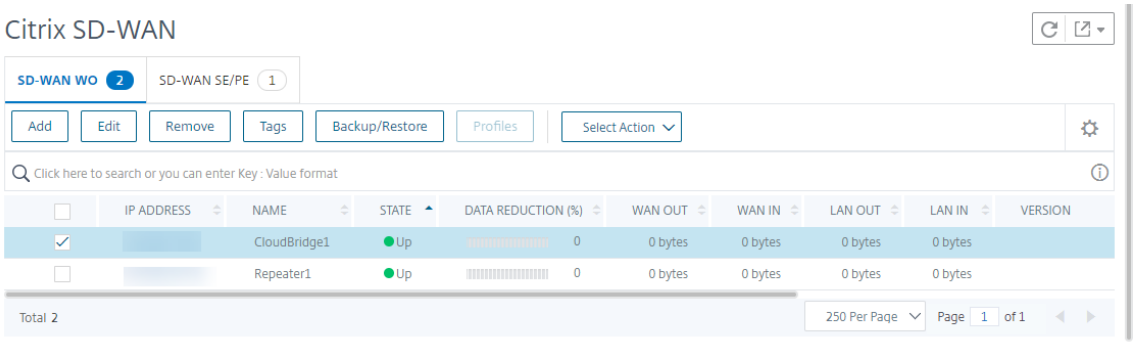
Weitere Informationen dazu, wie ein benutzerdefinierter Benutzer ein Backp einer Citrix SD-WANOP-Instanz erstellen kann, finden Sie unter Erstellen eines Backups der Citrix SD-WANOP-Instanz für benutzerdefinierte Benutzer in diesem Thema.

Stellen Sie sicher, dass eine Citrix SD-WANOP-Instanz zu NetScaler ADM hinzugefügt wird. Weitere Informationen finden Sie unter Instanz zu NetScaler ADM hinzufügen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

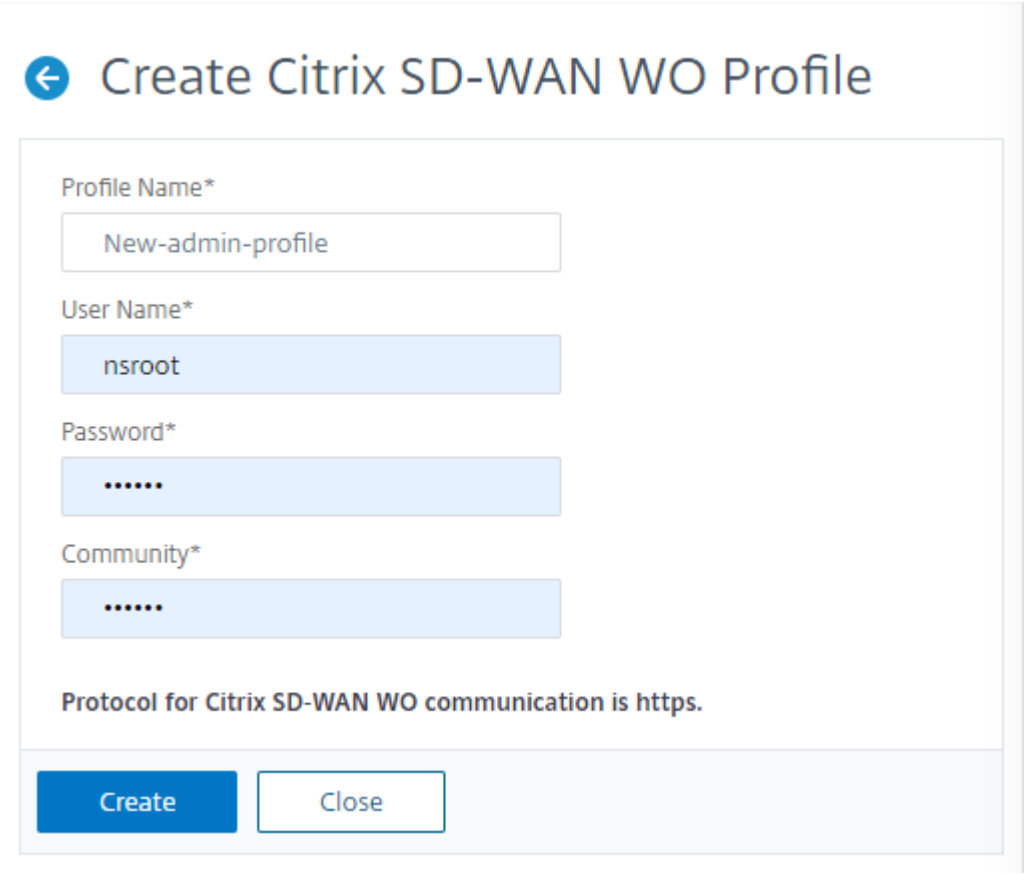
Backup-Vorgang durch benutzerdefinierte Benutzer wird auf 400/800/1000WS/2000/2000WS/3000/4000/5000/410 SD-WANOP-Plattformen nicht unterstützt.

> **Hinweis**
>
> Citrix empfiehlt, das standardmäßige nsroot-Profil zu verwenden, während Sie ein Backup der erweiterten Citrix SD-WAN Plattformen in Citrix ADM erstellen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

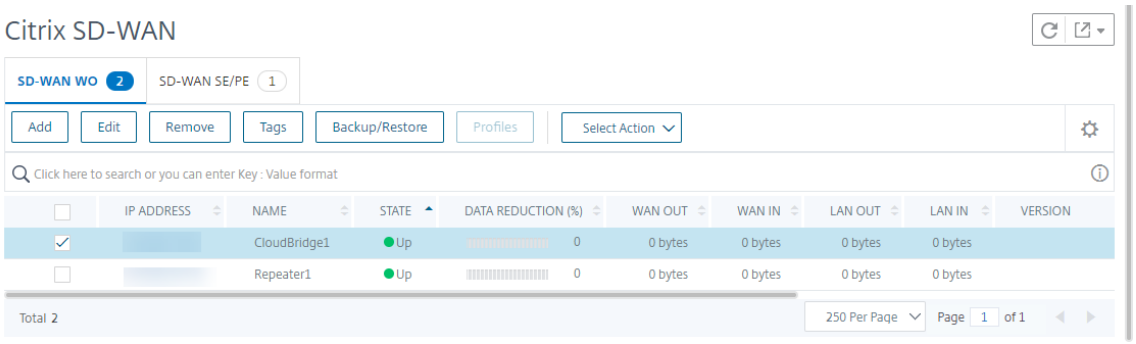


5. Geben Sie im **Feld Profilname**einen Namen für das Profil ein.
6. **Geben Sie im Feld Benutzername den Benutzernamen des benutzerdefinierten Benutzers ein, den Sie in der SD-WANOP-Instanz erstellen.**
7. Geben Sie im **Feld Kennwort**das Kennwort ein, das Sie für den benutzerdefinierten Benutzer 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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/*

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

/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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Voraussetzungen

Stellen Sie sicher, dass Sie:

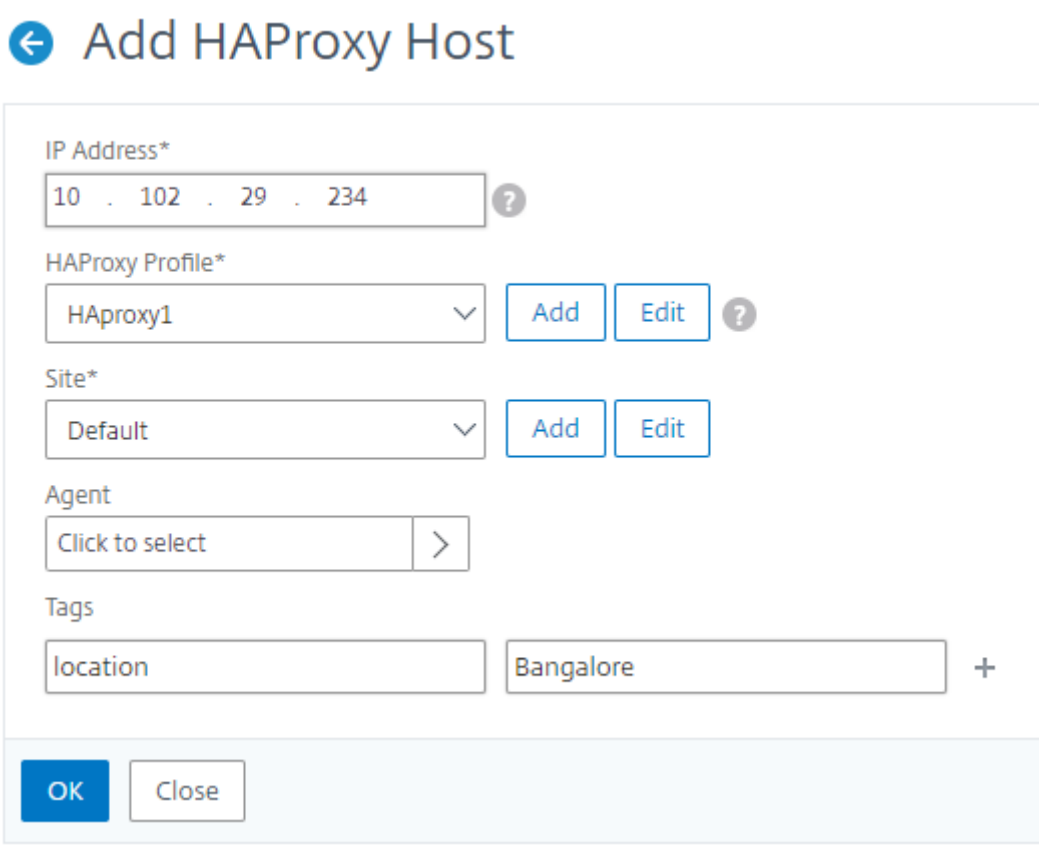
- Eine HAProxy-Instanz auf einem Host in Ihrer Bereitstellung bereitgestellt. Weitere Informationen finden Sie unter http://www.haproxy.org/#docs.
- Identifiziert und entschieden für die Anzahl der Frontends, für die Sie die Anwendungsstatistiken im HAProxy App Dashboard anzeigen möchten. Standardmäßig 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!**
>
> Citrix ADM benötigt Zugriff auf den Host, um die darin vorhandenen HAProxy-Instanzen zu ermitteln. 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. Geben Sie in einem Webbrowser die IP-Adresse von **Citrix Application Delivery Management** ein (z. B. http://192.168.100.1).
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldedaten ein. Die standardmäßigen Administratoranmeldeinformationen sind “nsroot”und “nsroot”.
3. Navigieren Sie zu **Netzwerke** > **Instanzen**. Wählen Sie unter **InstanzenHAProxy**aus und klicken Sie auf**Hinzufügen** .
4. Führen **Sie im Dialogfeld HAProxy-Host hinzufügen** die folgenden Schritte aus:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

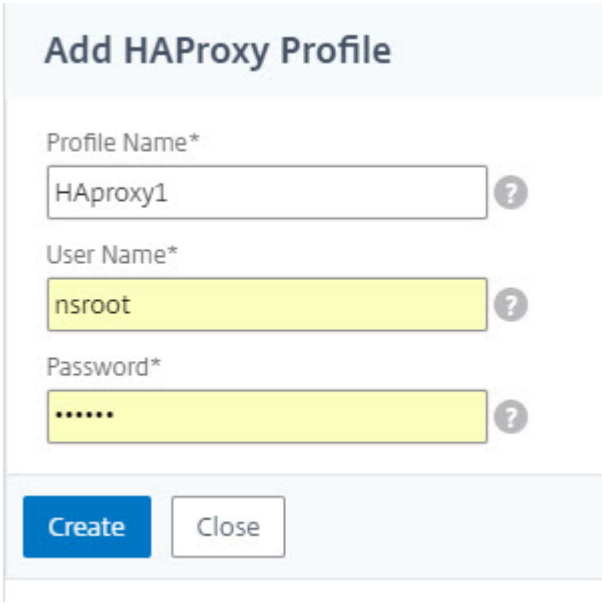


1. Geben Sie im Feld **IP-Adresse** die IP-Adresse des Hosts ein, auf dem Sie die HAProxy-Instanzen bereitgestellt haben.

    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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



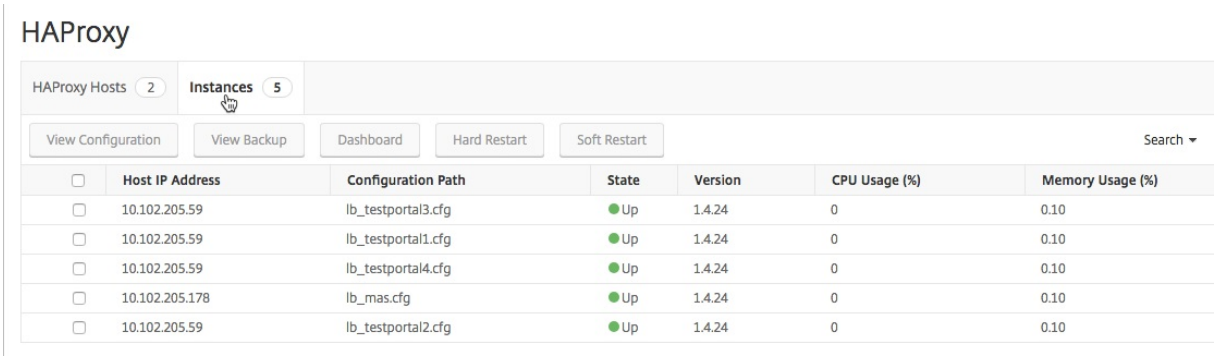
i. Geben Sie im Feld **Profilname** den Profilnamen ein.

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**.

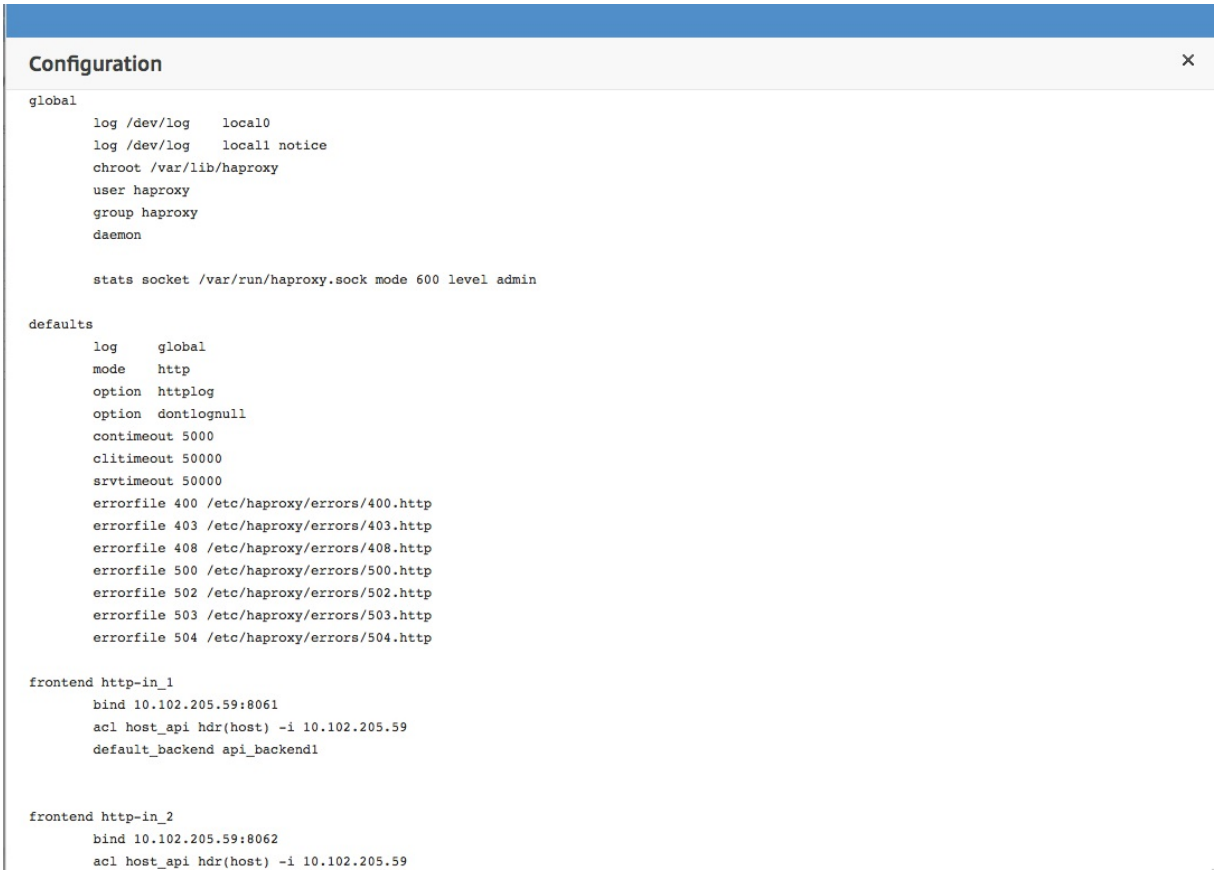
NetScaler ADM erkennt die auf dem Host bereitgestellten HAProxy-Instanzen und Sie können alle HAProxy-Instanzen auf der Registerkarte **Instanzen** anzeigen.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 aller HAProxy-Frontends, die von Citrix Application Delivery Management (Citrix ADM) überwacht werden. Es listet die Frontends als diskrete Anwendungen auf und stellt Informationen zu Transaktionen, Durchsatz und Sitzungen zu den Anwendungen bereit.

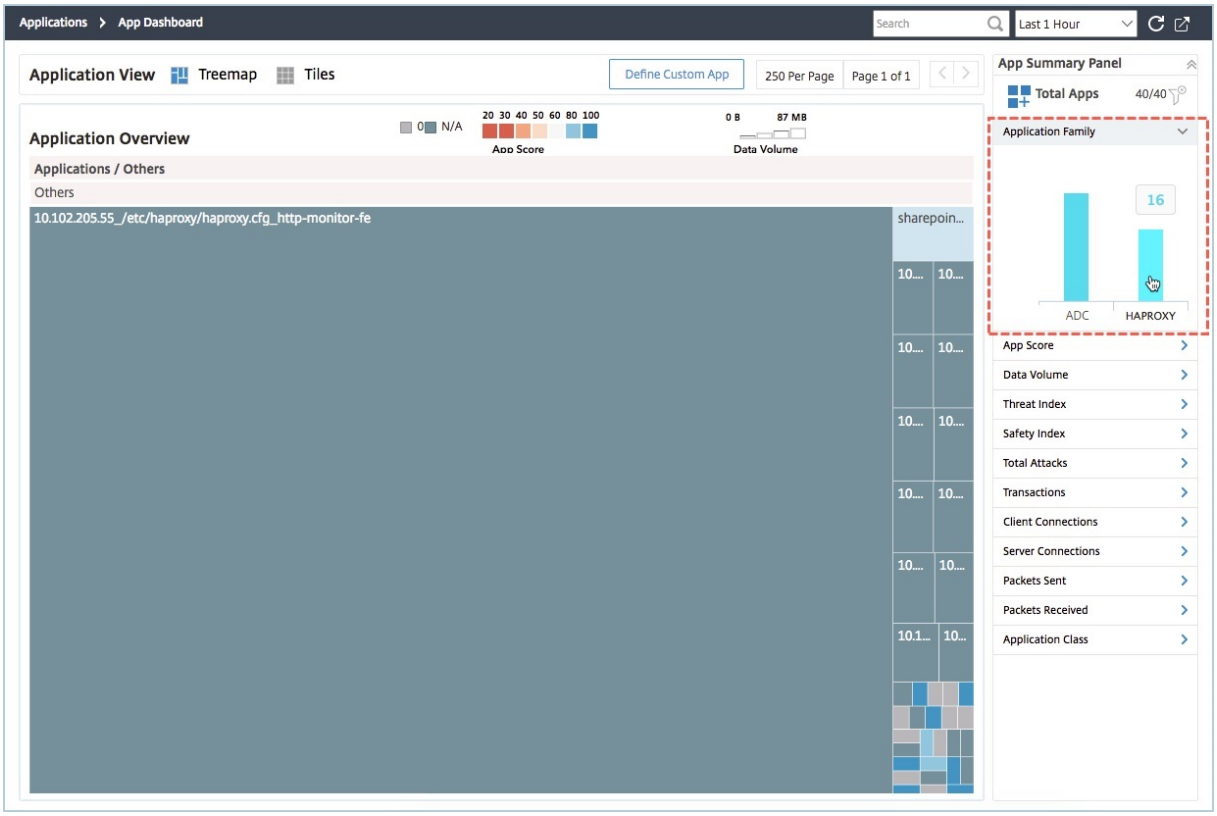
> **Wichtig!**
>
> Stellen Sie sicher, dass Sie **Statistiken** in der HAProxy-Instanzkonfigurationsdatei aktivieren. Um **Statistiken**zu aktivieren, bearbeiten Sie Ihre HAProxy-Konfigurationsdatei und fügen Sie nach

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

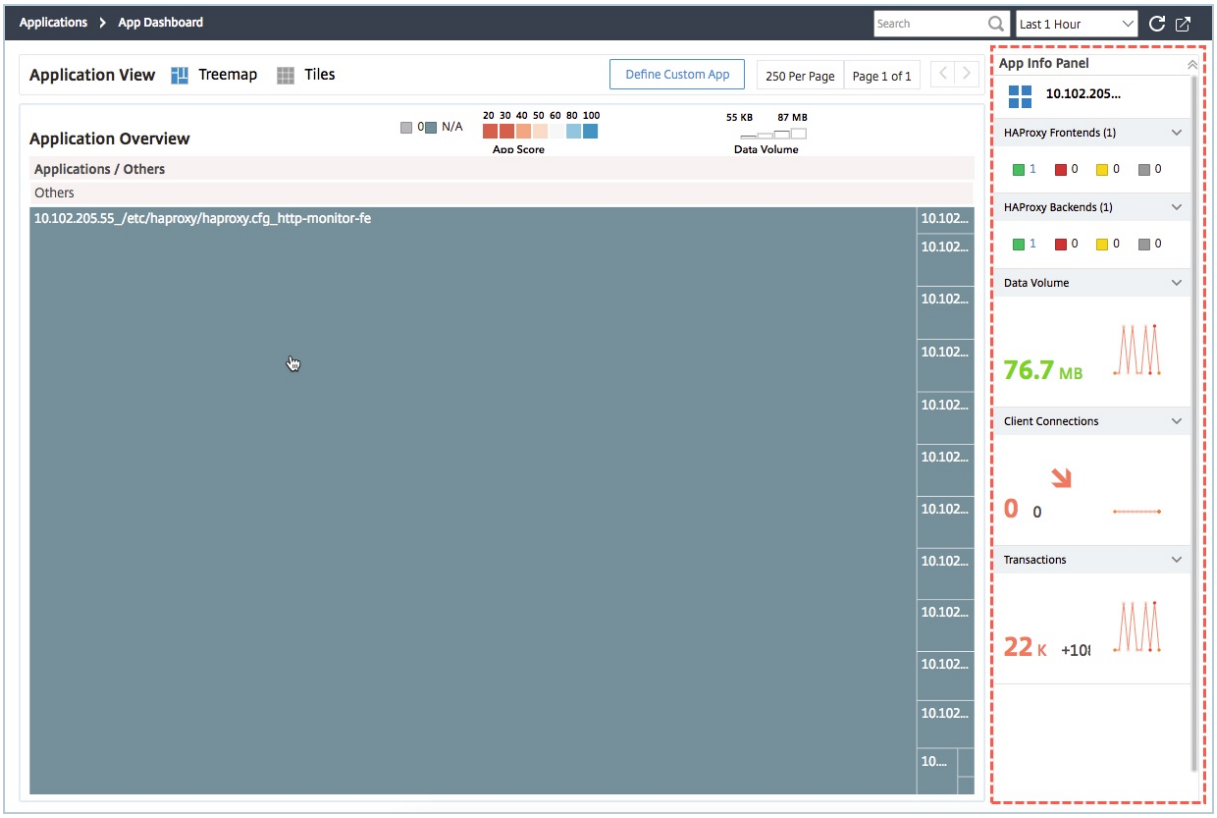


Wichtige Metriken der HAProxy-Anwendung anzeigen

Das App-Info-Panel befindet sich auf der ersten Ebene, wenn Sie einen Drilldown für eine HAProxy-Anwendung durchführen. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HAProxy-Backends, das Datenvolumen, den Trend der Clientverbindungen und die Transaktionen an. Um die wichtigsten Metriken der HAProxy-Anwendung anzuzeigen, klicken Sie auf die HAProxy-Anwendungskachel im Anwendungs-Dashboard. Das App-Info-Bedienfeld ersetzt dann das Bedienfeld "App-Zusammenfassung".



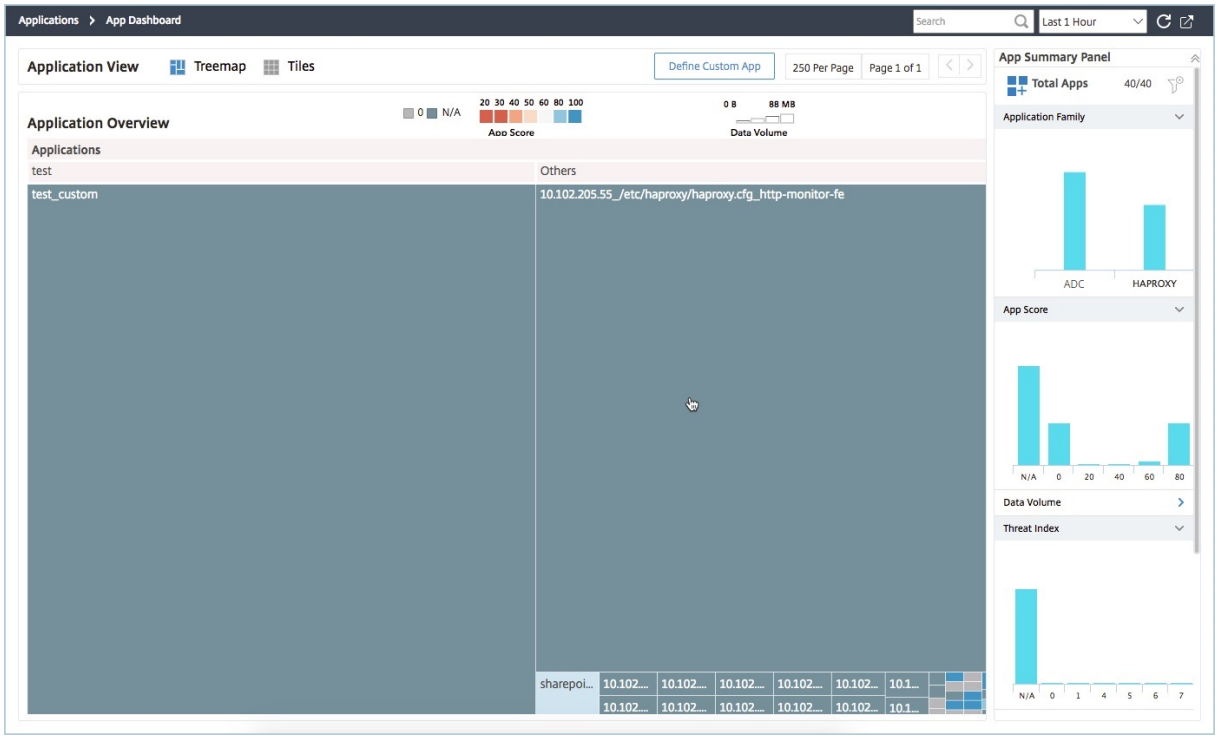
Anzeigen der Echtzeit-Performance der HAProxy-Anwendung

Mit Citrix ADM können Sie die Echtzeit-Performance Ihrer HAProxy-Anwendungen anzeigen. Es liefert die folgenden Echtzeit-Details der ausgewählten HAProxy-Anwendung:

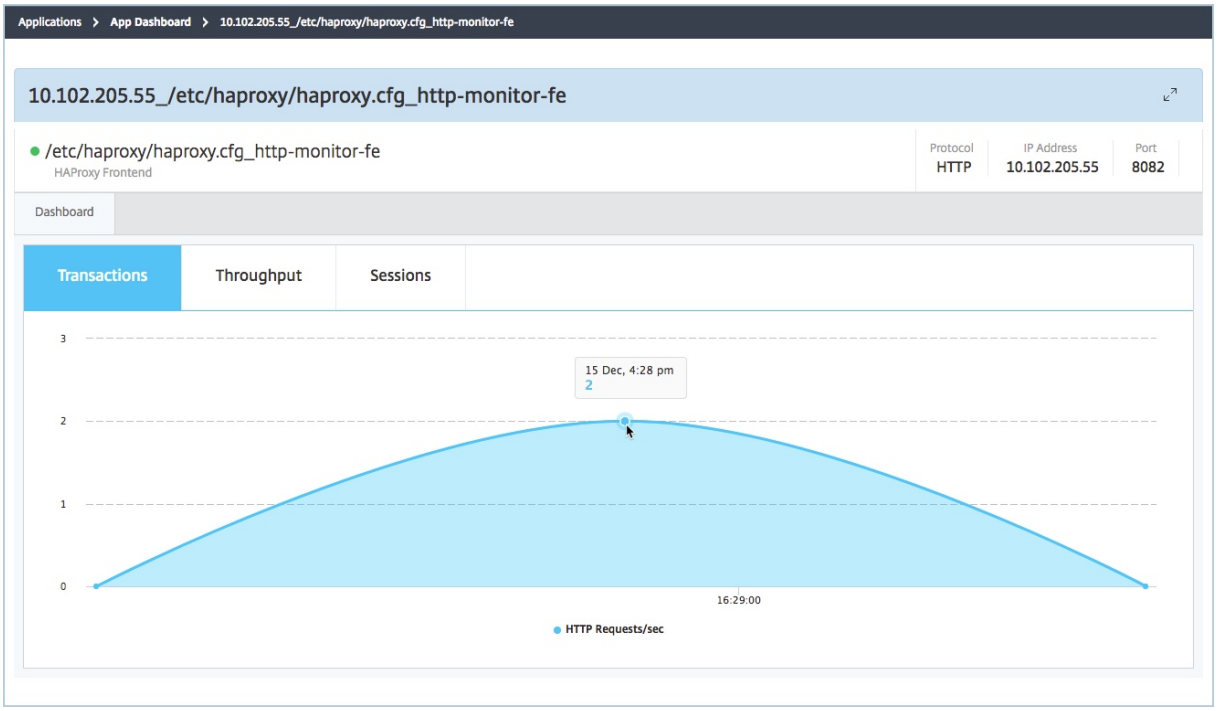
- **Transaktionen.** Transaktionen, die von der Anwendung durchgeführt werden.
- **Durchsatz.** Durchsatz der Anwendung.
- **Sitzungen.** Anzahl der Sitzungen, die von der Anwendung erstellt wurden.

Um die Echtzeit-Performance Ihrer HAProxy-Anwendung anzuzeigen, doppelklicken Sie im **Application Dashboard**auf die HAProxy-Anwendungskachel.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

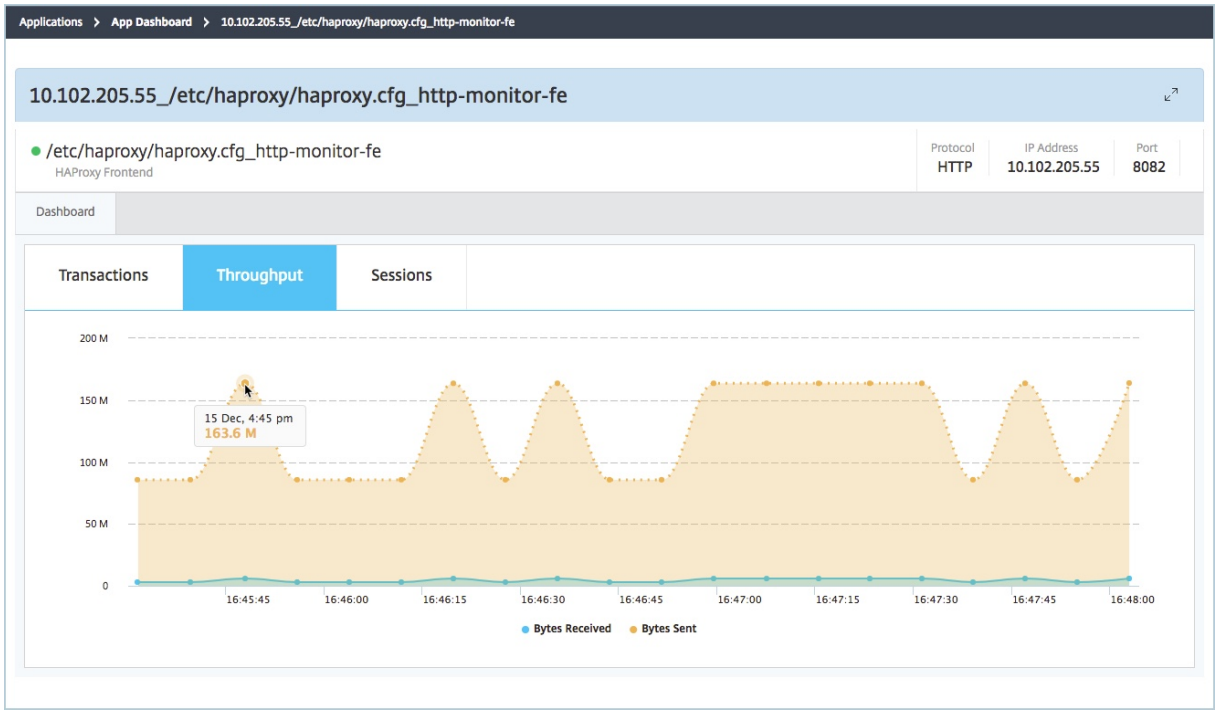


Standardmäßig ist die Registerkarte **Transaktionen** ausgewählt, und die Echtzeit-Transaktionen, die von der Anwendung ausgeführt werden, werden angezeigt.

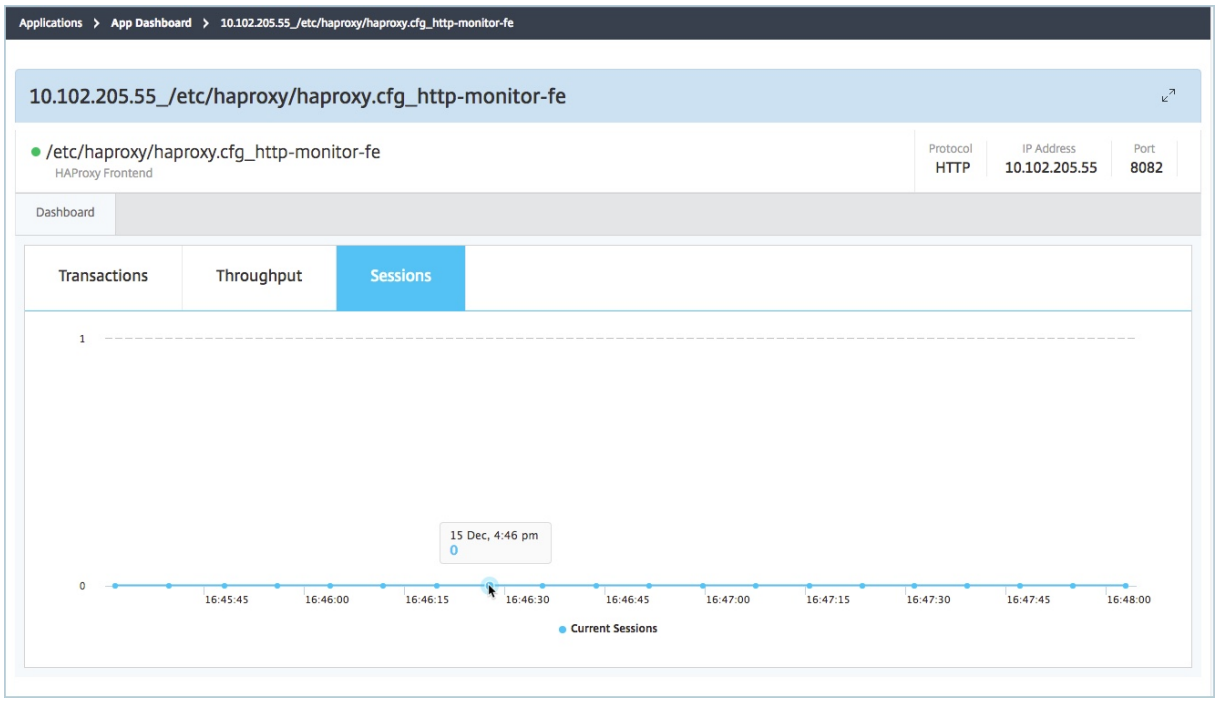


Um den Echtzeitdurchsatz der Anwendung anzuzeigen, klicken Sie auf die Registerkarte **Durchsatz**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Sie können auf die Registerkarte **Sitzungen** klicken, um die Anzahl der Sitzungen anzuzeigen, die von der Anwendung in Echtzeit eingerichtet wurden.



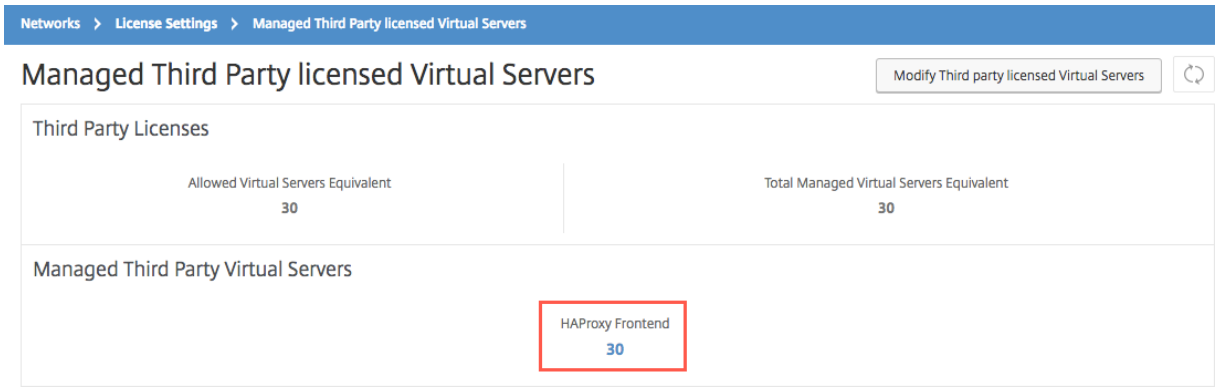
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 zusätzliche Frontends sind in virtuellen Serverpaketen zu 100 verfügbar. Sie können eine gültige Lizenz abrufen und die Lizenz mit der NetScaler ADM GUI installieren.

Installieren der Lizenzen von Drittanbietern

Sie können eine Lizenz auf NetScaler ADM installieren, um die Anwendungsstatistiken von mehr als 30 erkannten Anwendungen anzuzeigen.

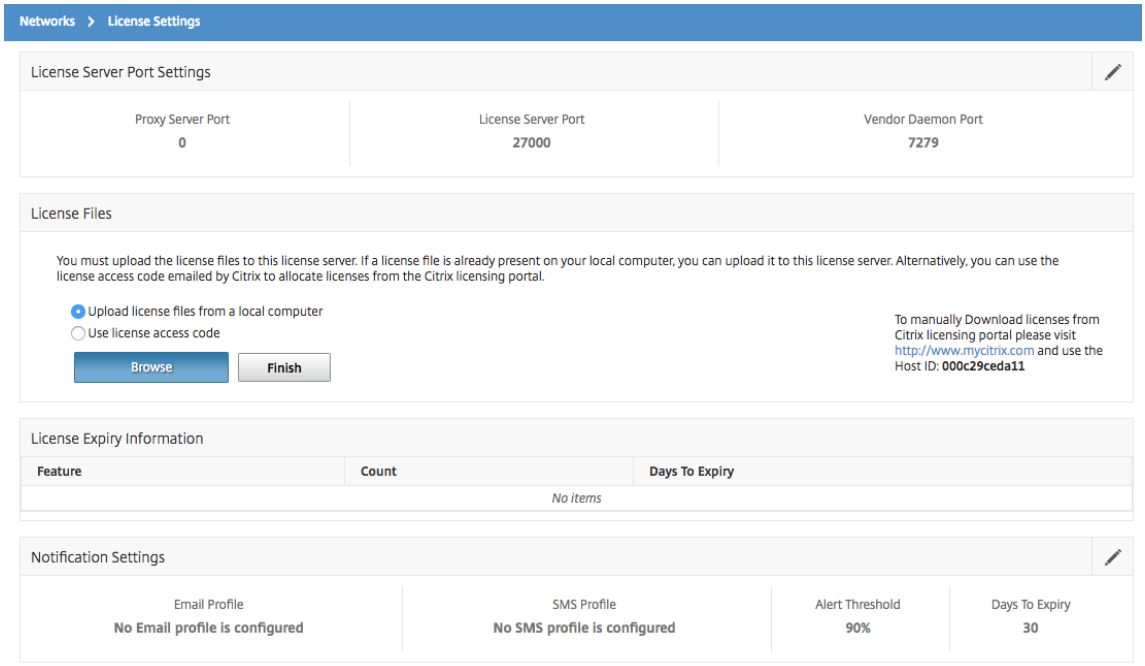
So installieren Sie eine Lizenz:

1. Geben Sie in einem Webbrowser die IP-Adresse des **NetScaler Management and Analytics System** 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:

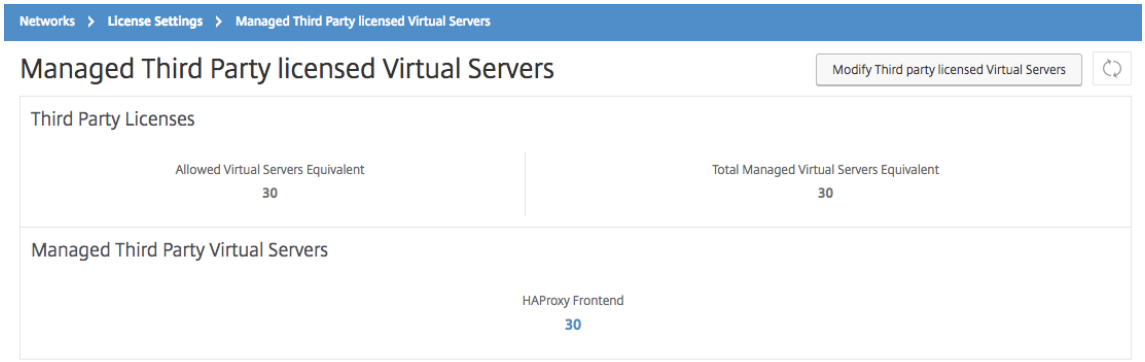
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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 eine E-Mail an die LAC für die erworbene Lizenz. Geben Sie die LAC in das Textfeld ein, und klicken Sie dann auf **Lizenzen abrufen**.

> **Hinweis**
>
> Wenn Sie diese Option auswählen, muss das NetScaler Management and Analytics System 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.



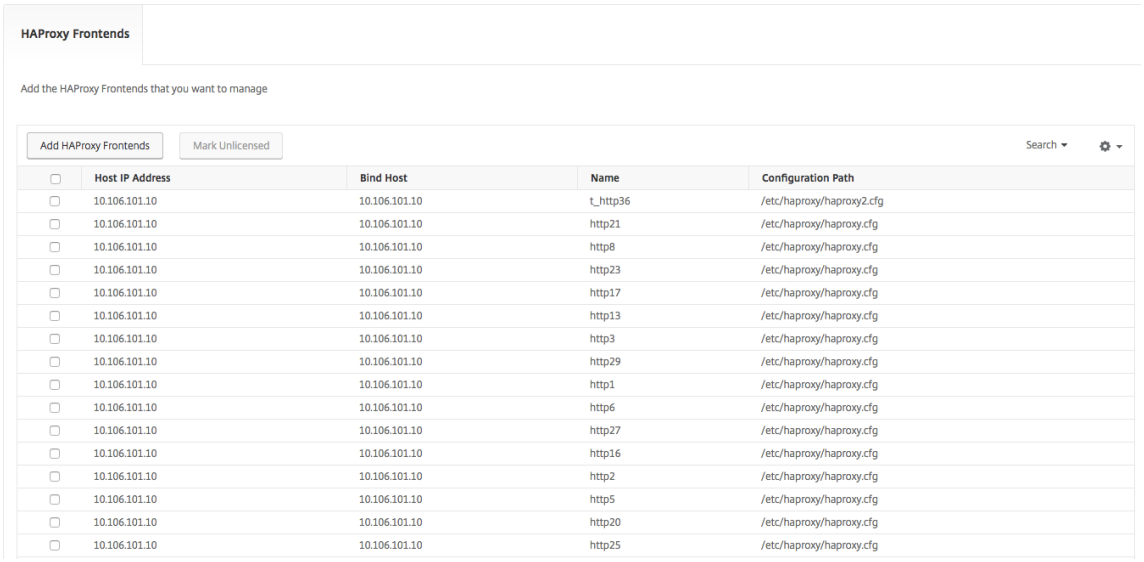
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwalten der Lizenzen von Drittanbietern

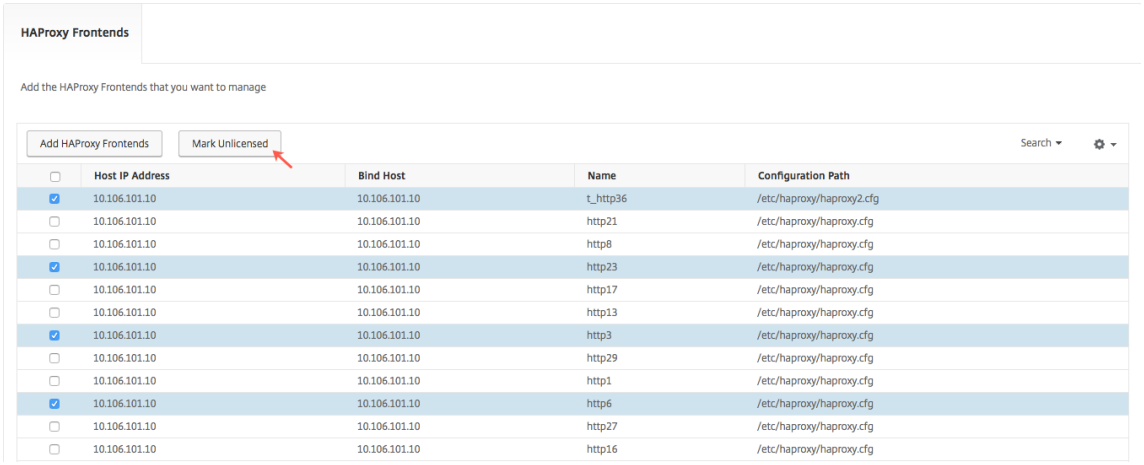
NetScaler ADM wählt die erkannten Anwendungen in den HAProxy-Instanzen nach dem Zufallsprinzip aus und lizenziert sie automatisch. Wenn Sie die ausgewählten erkannten Anwendungen ändern möchten, müssen Sie die Lizenzierung der lizenzierten erkannten Anwendungen manuell aufheben und dann die Lizenzen 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.

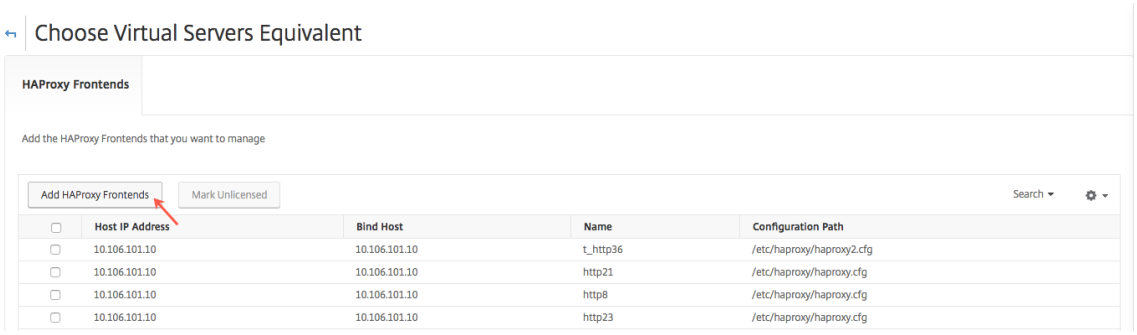


2. Wählen Sie die Frontends aus der Liste, **Als Nicht lizenziert markieren**, und klicken Sie auf **Fertig stellen**, um die Lizenzen freizugeben.

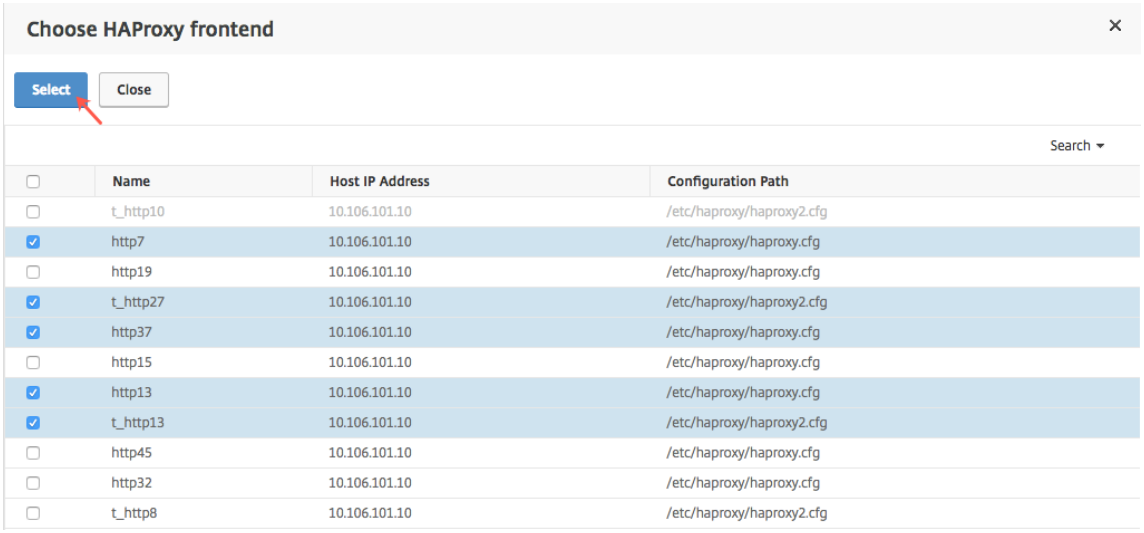


3. Nachdem Sie die Lizenzen freigegeben haben oder bereits Lizenzen verfügbar sind, klicken Sie auf **HAProxy-Frontends hinzufügen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. **Wählen Sie im Dialogfeld HAProxy-Frontend** auswählen die nicht lizenzierten Frontends 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

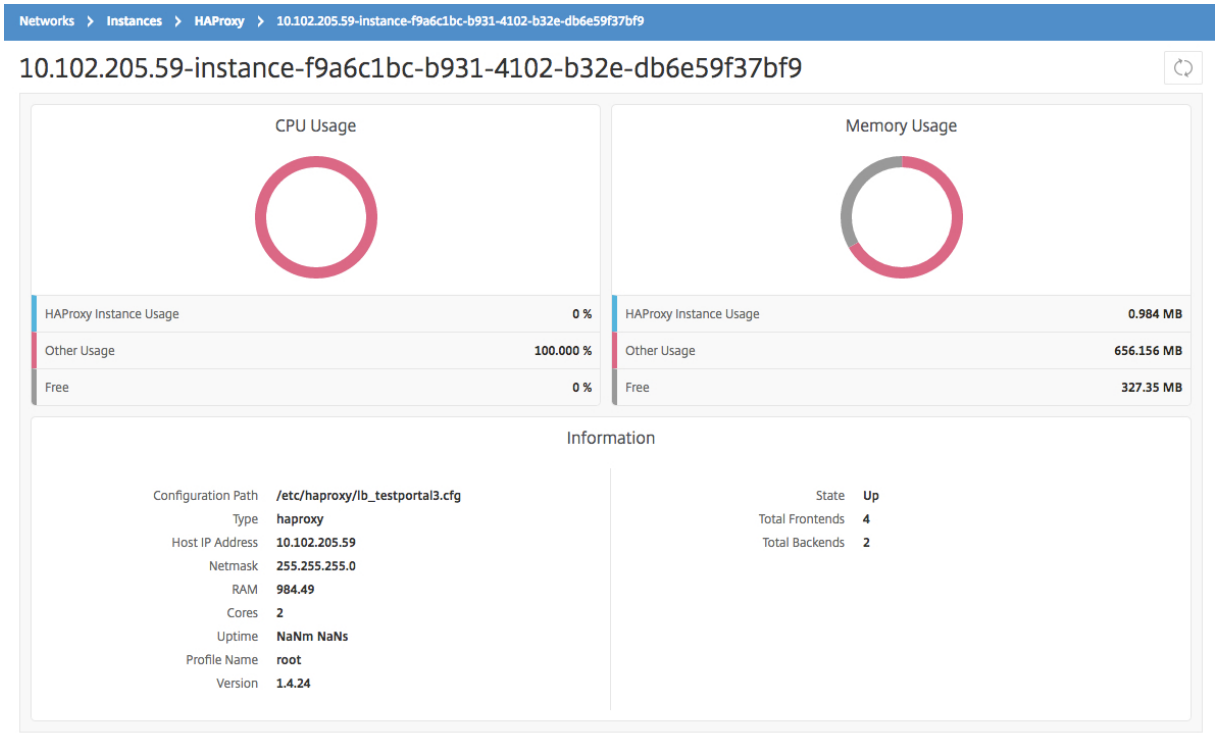
HAProxy-Instanzen überwachen

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**.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Details der auf HAProxy-Instanzen konfigurierten Frontends anzeigen

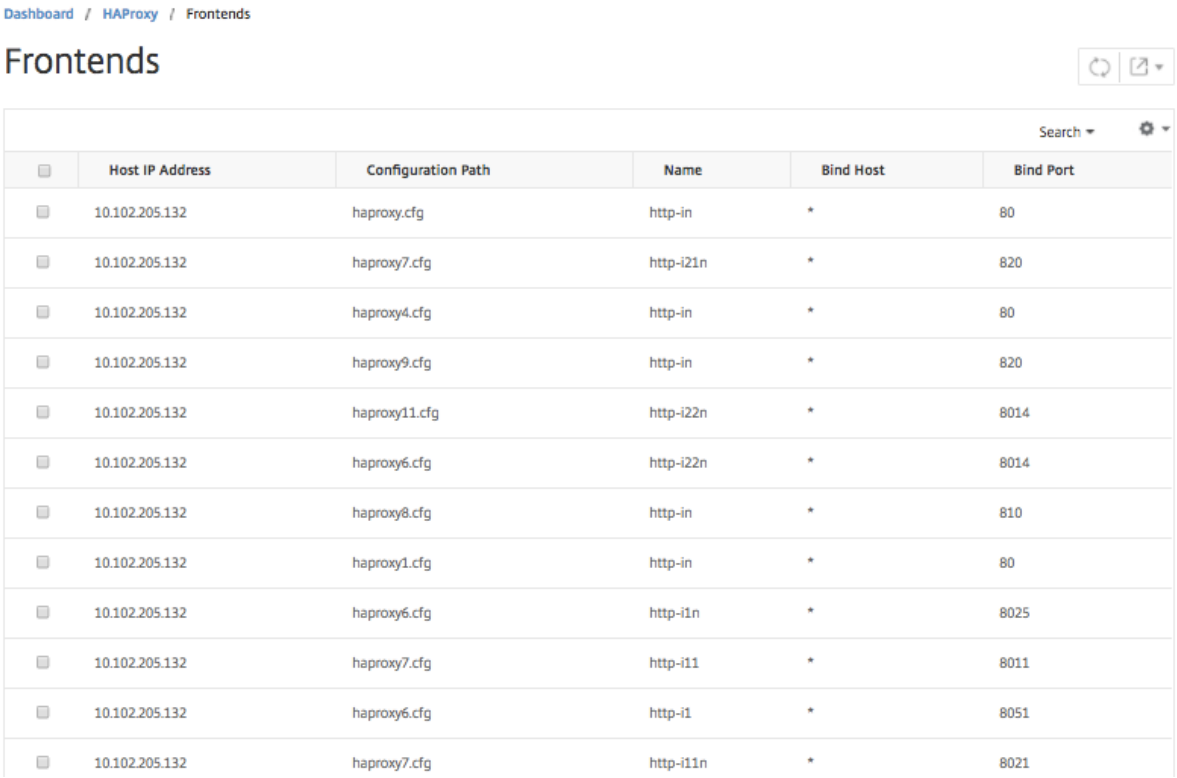
February 5, 2024

Citrix Application Delivery Management (Citrix ADM) meldet die folgenden Details des Frontend, das auf einer HAProxy-Instanz konfiguriert ist:

- **Host-IP-Adresse**. IP-Adresse des Hosts
- **Konfigurationspfad**.Absoluter Konfigurationspfad der HAProxy-Instanz auf dem Host.
- **Name**. Name des Frontend, das den eingehenden Datenverkehr verarbeitet.
- **Host binden**. IP-Adresse, an die das Frontend gebunden ist.
- **Port binden**. Port, an den das Frontend gebunden ist.

So zeigen Sie das Frontend an, das auf den HAProxy-Instanzen konfiguriert ist:

Navigieren Sie in NetScaler ADM zu **Netzwerke > Netzwerkfunktionen > HAProxy > Frontends**.



Host IP Address	Configuration Path	Name	Bind Host	Bind Port
10.102.205.132	haproxy.cfg	http-in	*	80
10.102.205.132	haproxy7.cfg	http-i21n	*	820
10.102.205.132	haproxy4.cfg	http-in	*	80
10.102.205.132	haproxy9.cfg	http-in	*	820
10.102.205.132	haproxy11.cfg	http-i22n	*	8014
10.102.205.132	haproxy6.cfg	http-i22n	*	8014
10.102.205.132	haproxy8.cfg	http-in	*	810
10.102.205.132	haproxy1.cfg	http-in	*	80
10.102.205.132	haproxy6.cfg	http-i1n	*	8025
10.102.205.132	haproxy7.cfg	http-i11	*	8011
10.102.205.132	haproxy6.cfg	http-i1	*	8051
10.102.205.132	haproxy7.cfg	http-i11n	*	8021

Details der auf HAProxy-Instanzen konfigurierten Backends anzeigen

February 5, 2024

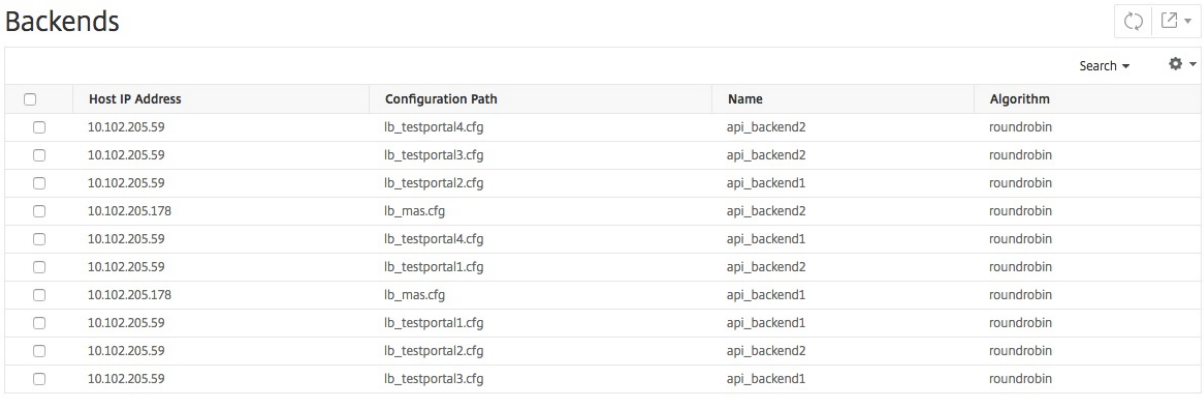
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Application Delivery Management (Citrix ADM) meldet die folgenden Details einer Backend-Anwendung, 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 Datenverkehr weitergeleitet wird.
- **Algorithmus**. Lastausgleichsalgorithmus, der zum Ausgleich des Datenverkehrs verwendet wird.

So zeigen Sie das Backend an, das auf den HAProxy-Instanzen konfiguriert ist:

Navigieren Sie in NetScaler ADM zu **Netzwerke** > **Netzwerkfunktionen** > **HAProxy** > **Backends**.



Details der auf HAProxy-Instanzen konfigurierten Server anzeigen

February 5, 2024

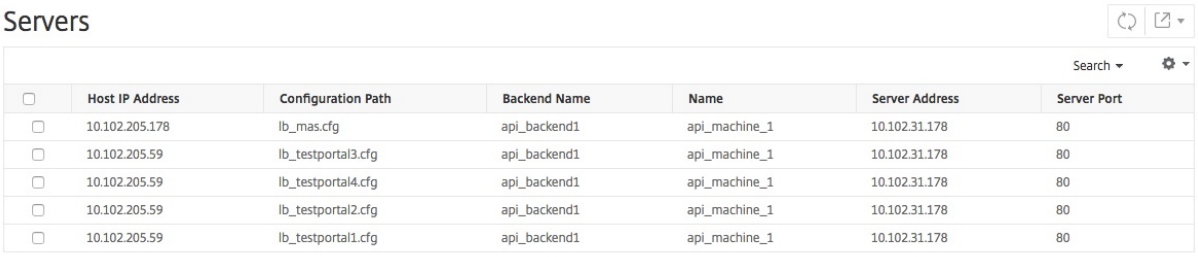
Citrix Application Delivery Management (Citrix ADM) meldet die folgenden Details zu Servern, die auf einer HAProxy-Instanz konfiguriert sind:

- **Host-IP-Adresse**. Name des Hosts.
- **Konfigurationspfad**.Absoluter Pfad der HAProxy-Instanzkonfigurationsdatei auf dem Host.
- **Backend-Name**. 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

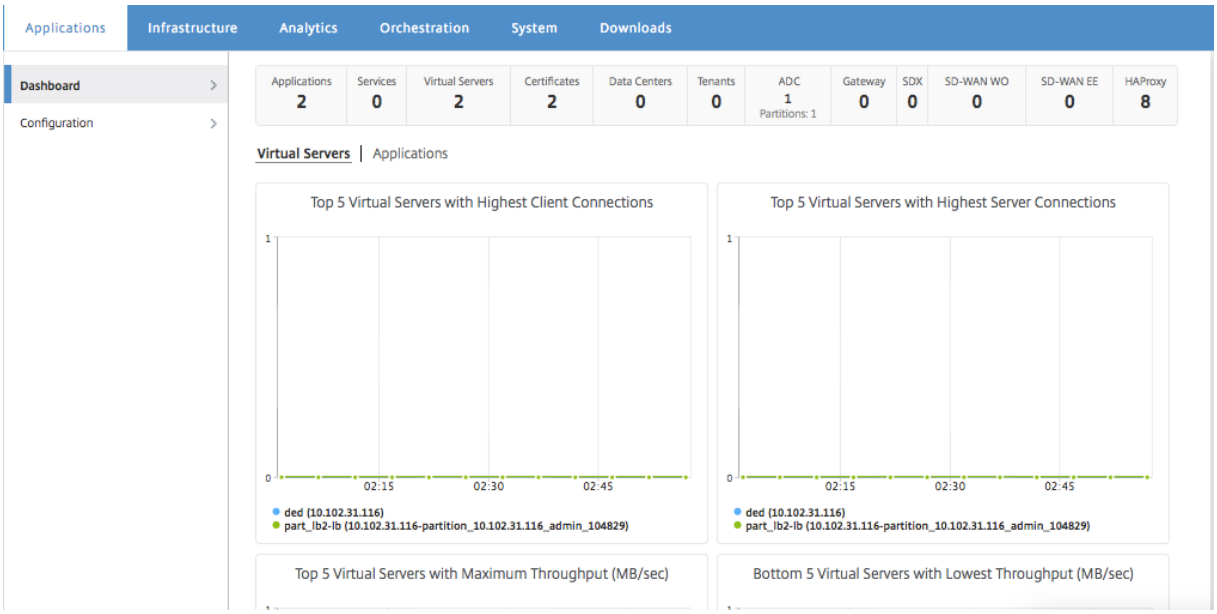


Anzeigen der HAProxy-Instanzen mit der höchsten Anzahl von Frontends oder Servern

February 5, 2024

Im Application Dashboard zeigt Citrix Application Delivery Management (Citrix ADM) die Anzahl der erfundenen HAProxy-Instanzen an und listet die fünf häufigsten HAProxy-Instanzen auf, die mit der höchsten Anzahl von Frontends oder Servern konfiguriert sind.

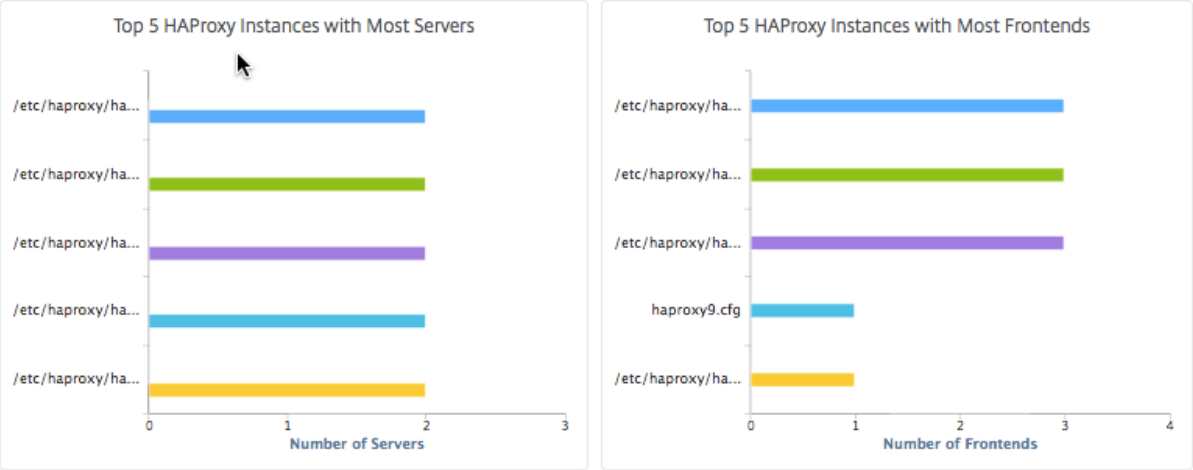
Um das Anwendungs-Dashboard anzuzeigen, navigieren Sie in Citrix ADM zu **Anwendungen** > **Dashboard**.



Die Anzahl der von Citrix ADM erkannten HAProxy-Instanzen wird in der obersten Zeile angezeigt, wie unten dargestellt:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Um die Liste der fünf wichtigsten HAProxy-Instanzen anzuzeigen, die mit der höchsten Anzahl von Frontends 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

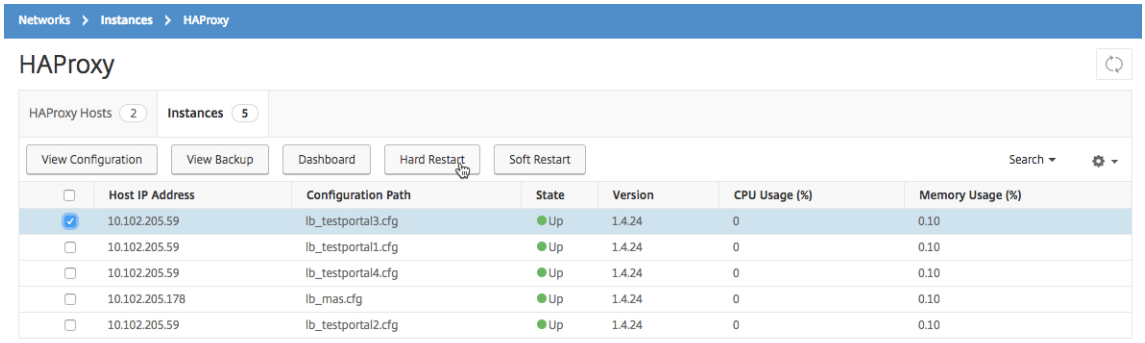
Der Softrestart hetzt den HAProxy-Prozess vom Listening-Port auf, aber der HAProxy-Prozess verarbeitet weiterhin bestehende Verbindungen, bis sie schließen. Ein neuer HAProxy-Prozess wird erstellt, um neue Verbindungen zu verarbeiten.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.



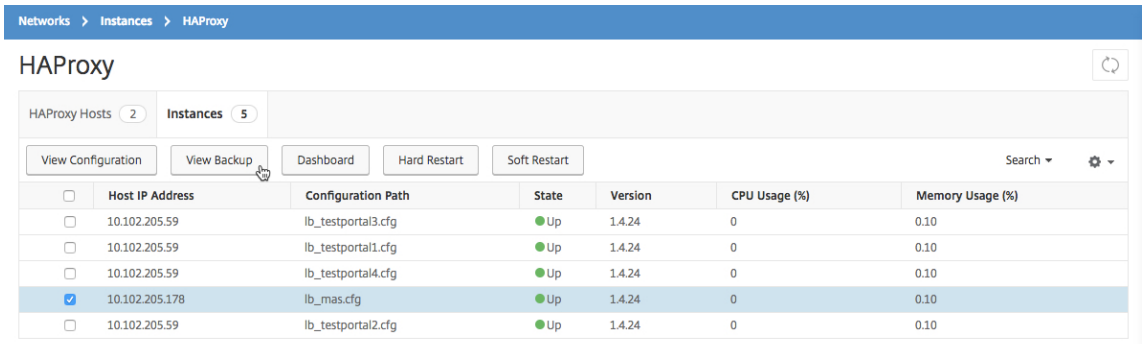
Backup und Wiederherstellen einer HAProxy-Instanz

February 5, 2024

Sie können den aktuellen Status einer HAProxy-Instanz in einer HAProxy-Konfigurationsdatei sichern. Wenn die Instanz instabil wird, können Sie die Datei backedup verwenden, um die Instanz in den stabilen Zustand wiederherzustellen.

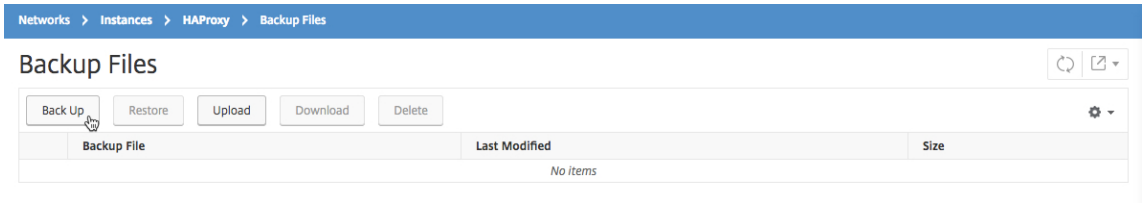
So sichern Sie eine HAProxy-Instanz mithilfe von NetScaler ADM:

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**.

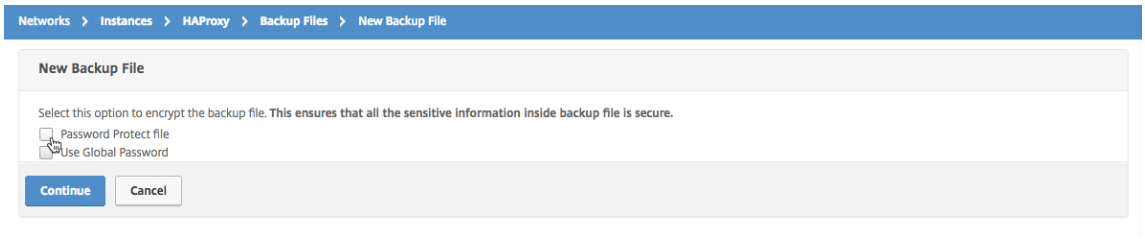


4. Klicken Sie auf der Seite **Backup-Dateienauf Sichern.**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



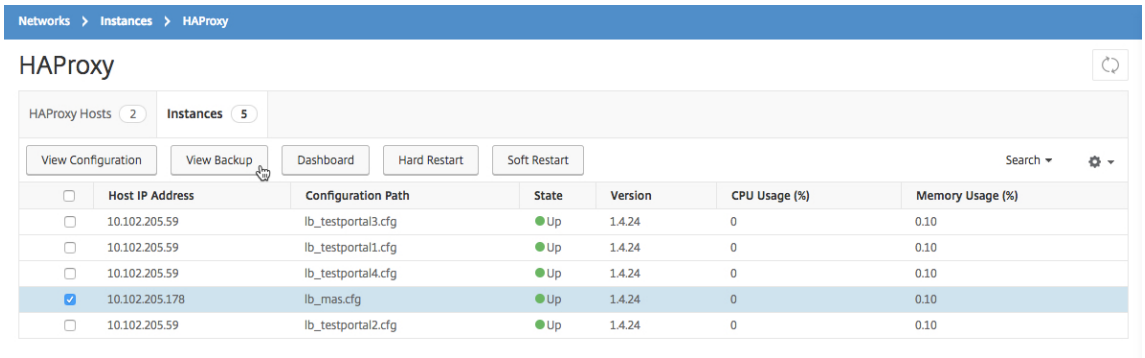
5. Sie können Ihre Backupdatei für zusätzliche Sicherheit verschlüsseln.



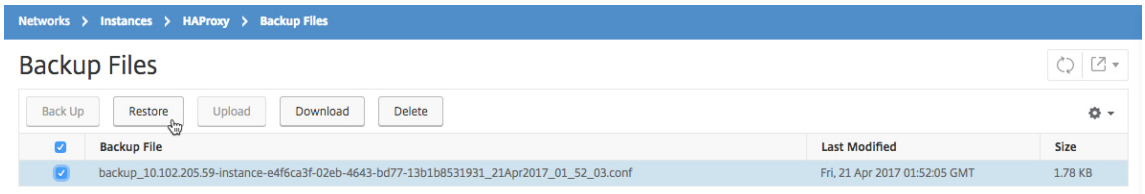
6. Klicken Sie auf **Weiter**.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> neu.

HAProxy-Konfigurationsdatei bearbeiten

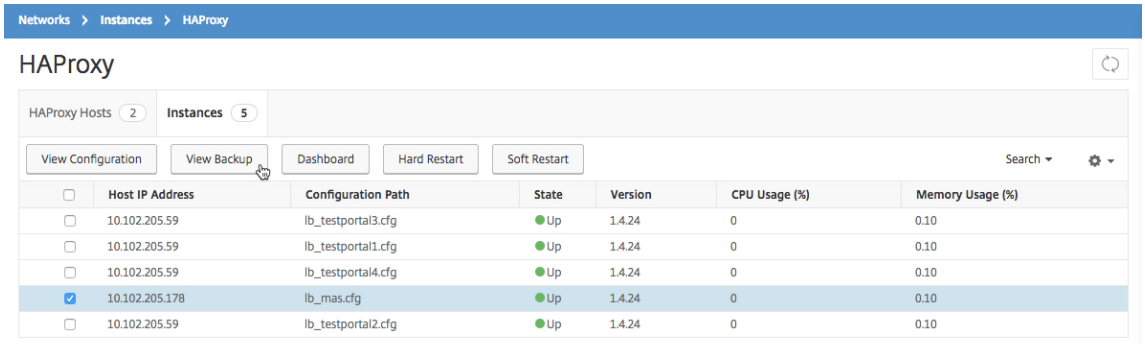
February 5, 2024

Sie können Frontend, Backend, Server und andere Einstellungen in der vorhandenen HAProxy-Konfigurationsdatei aktualisieren. So bearbeiten Sie die HAProxy-Konfigurationsdatei:

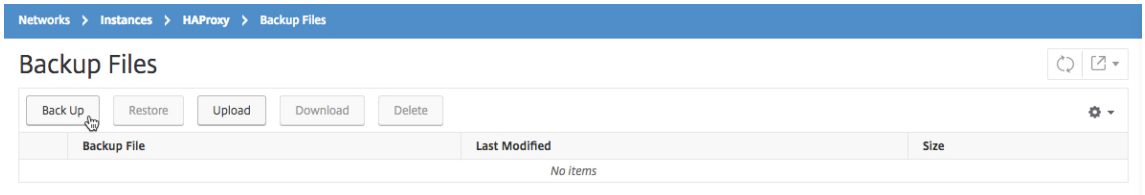
- Sichern Sie die HAProxy-Konfigurationsdatei.
- Laden Sie das Backup der HAProxy-Konfigurationsdatei herunter und bearbeiten Sie sie offline.
- Hochladen der aktualisierten HAProxy-Konfigurationsdatei in Citrix Application Delivery Management (Citrix ADM)
- Stellen Sie die HAProxy-Instanz mit der aktualisierten 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**.

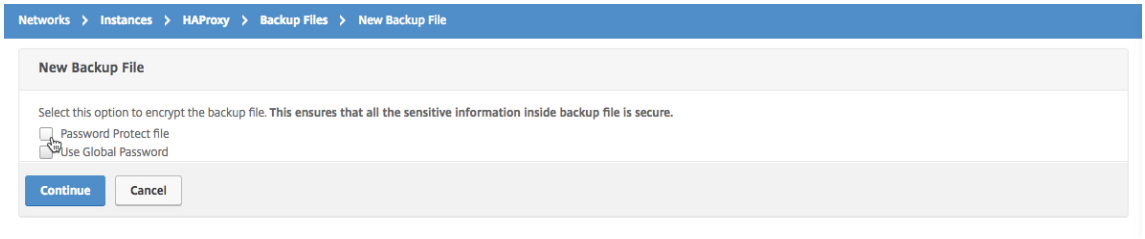


4. Klicken Sie auf der Seite **Backupdateien** auf **Sichern**.



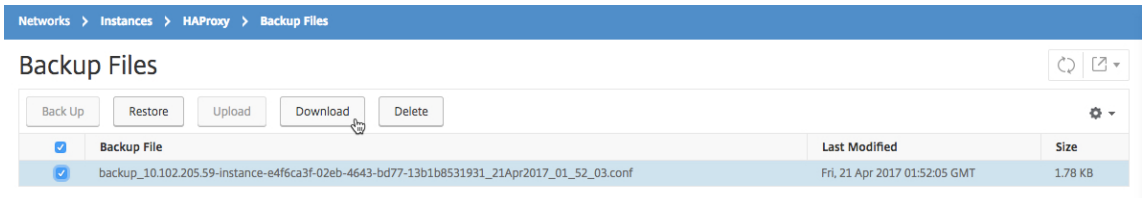
5. Klicken Sie auf **Weiter**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

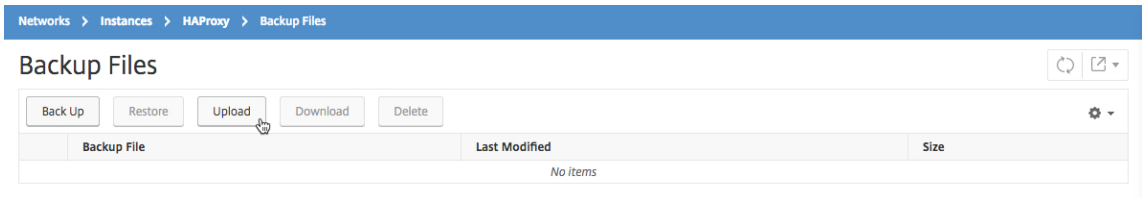


> **Hinweis**
>
> Verschlüsseln Sie die Backupdatei nicht.

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 beschrieben, wie Sie die Systemeinstellungen auf Ihrem Citrix ADM konfigurieren.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn du willst…	Mach das…
Nachricht des Tages konfigurieren	Sie können jetzt eine Willkommensnachricht in Citrix ADM erstellen. Mit dieser Funktion können Sie Erinnerungsmeldungen für sich selbst oder den Benutzer festlegen, der sich bei NetScaler ADM anmeldet. Navigieren Sie zu **System** > **Systemeinstellungen** und klicken Sie auf **Nachricht des Tages konfigurieren**. Klicken Sie auf **Nachricht aktivieren**, geben Sie die Nachricht in das Meldungsfeld ein und klicken Sie auf **OK** .
Fahren Sie Citrix ADM herunter	Navigieren Sie zu **System** > **Systemadministration**. Sie können auf **Citrix ADM herunterfahren** klicken, um Citrix ADM vollständig herunterzufahren. **Hinweis**: Sobald Sie Citrix ADM heruntergefahren haben, können Sie Citrix ADM nur von dem Hypervisor aus erneut starten, auf dem Sie es installiert haben.
Konfigurieren Sie die Einstellungen des Einrichtungsassistenten	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Citrix ADM** einrichten die **Einstellungen** des Setupassistenten aus. Sie können die Option **Citrix ADM Network** auswählen, um Netzwerkeinstellungen wie die IP-Adresse von Citrix ADM und das Kennwort zu ändern. Sie können auf **Systemeinstellungen** klicken, um den Hostnamen, den Kommunikationsmodus mit den Instanzen oder die lokale Zeitzone zu ändern.
Konfigurieren Sie die Netzwerkeinstellungen	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Citrix ADM** einrichten die Option **Netzwerkkonfiguration** aus. Die GUI zeigt die auf dem Citrix ADM installierten SSL-Zertifikate und Schlüssel an.
SSL-Zertifikat anzeigen	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Citrix ADM einrichten** die Option **SSL-Zertifikat anzeigen** aus. Die GUI zeigt die auf dem Citrix ADM installierten SSL-Zertifikate und Schlüssel an.
Zeitzone ändern	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Systemeinstellungen** die Option **Zeitzone ändern** aus. Wählen Sie in der Dropdownliste **Zeitzone** die Zeitzone für die Uhr Ihrer Citrix ADM Appliance aus.
Hostnamen ändern	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Systemeinstellungen** die Option **Hostname ändern** aus. Geben Sie einen Hostnamen ein, der zur Identifizierung Ihres Citrix ADM verwendet wird, sodass der Hostname in der Lizenz angezeigt wird, wenn Sie die Universallizenz für Citrix ADM Gateway generieren.
Ändern Sie die Systemeinstellungen	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Systemeinstellungen** die Option **Systemeinstellungen ändern** aus. Aktivieren oder deaktivieren Sie dann die Kontrollkästchen, um die folgenden Funktionen zu aktivieren oder zu deaktivieren: Nur sicherer Zugriff, Sitzungstimeout aktivieren, Standardauthentifizierung zulassen, NSRECOVER-Anmeldung aktivieren, Zertifikatsdownload aktivieren, Shell-Zugriff für Benutzer ohne NSROOT aktivieren, Benutzeranmeldeinformationen für Instanzanmeldung abfragen
Konfigurieren Sie die SSL-Einstellungen	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Systemeinstellungen** die Option **SSL-Einstellungen konfigurieren** aus, um

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

die aktuellen Protokolleinstellungen und die verwendeten Verschlüsselungssammlungen anzuzeigen. Wenn Sie eine der Einstellungen ändern möchten, wählen Sie unter **Einstellungen bearbeiten** die Option **Protokolleinstellungen** oder **Cipher Suites** aus. |
Aktivieren Sie die Einstellungsfunktion zur Verbesserung der Benutzererfahrung	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Systemeinstellungen** die Option Einstellungen zur **Verbesserung der Benutzerfreundlichkeit konfigurieren** aus, und aktivieren Sie dann das Kontrollkästchen **CUXIP aktivieren**. Wenn Sie dieses Kontrollkästchen aktivieren, werden Nutzungsstatistiken ausschließlich zur Verbesserung der grafischen Benutzeroberfläche erfasst. Die empfangenen Daten werden nur von Citrix-Technikern verwendet und an niemanden weitergegeben.
Upgrade von NetScaler ADM	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter der Unterüberschrift **Systemadministration** die Option **Citrix ADM aktualisieren** aus, und wählen Sie dann die neue Imagedatei aus. Sie können eine Datei auswählen, die sich bereits auf der virtuellen Citrix ADM Appliance befindet, oder Sie können eine Datei von Ihrem lokalen Computer hochladen.
Starten Sie Citrix ADM neu	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter der Unterüberschrift **Systemadministration** die Option **Citrix ADM neu starten** aus. Es erscheint ein Dialogfenster, in dem Sie aufgefordert werden, Ihre Aktion zu bestätigen. Klicken Sie auf **Ja**.
Systembereinigungseinstellungen konfigurieren (zum Bereinigen alter Daten)	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Prune Settings** die Option **System Prune Settings** aus. Geben Sie im Feld Zu speichernde Daten (Tage) die Anzahl der Tage ein, für die Daten im System aufbewahrt werden sollen.
Konfigurieren Sie die System-Backup-Einstellungen	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Backup-Einstellungen** die Option **Systemsicherungseinstellungen** aus und geben Sie dann die Anzahl der Systemsicherungen ein, die auf der Citrix ADM Appliance aufbewahrt werden sollen. Sie können sich auch dafür entscheiden, die Sicherungsdateien zu verschlüsseln, und Sie können einen externen Speicherort angeben, an den sie übertragen werden sollen. Übertragene Sicherungsdateien können auf dem System aufbewahrt oder aus dem System gelöscht werden.
Konfiguration der Instanz-Backup-Einstellungen	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Backup-Einstellungen** die Option **Instanz-Backup-Einstellungen** aus und geben Sie das Zeitintervall (in Stunden) ein, in dem eine Sicherungsdatei erstellt werden soll, die alle vom Citrix ADM verwalteten Instanzen sichert. Sie können die Anzahl der Sicherungsdateien angeben, die aufbewahrt werden sollen, und ob sie verschlüsselt werden sollen, sodass ohne Kennwort nicht auf sie zugegriffen werden kann.
Sehen Sie sich die Systemstatistiken an	Navigieren Sie zu **System** > **Statistik**. Ein Liniendiagramm zeigt Informationen wie CPU-Auslastung, Speichernutzung und Festplattennutzung an.
Sitzungen anzeigen und verwalten	Navigieren Sie zu **System** > **Sitzungen**. Sie können

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

dann alle aktiven Sitzungen mit Details sehen. Um eine Sitzung zu beenden, aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie auf **Sitzung abbrechen**. |
Einen Mandanten hinzufügen oder ändern	Navigieren Sie zu **System** > **Mandanten** und fügen Sie einen neuen Mandanten hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen Mandanten. Sie können zusätzliche Informationen angeben, z. B. den Namen einer Organisationseinheit, eine Abteilung und eine URL für den Mandanten.
Ändern Sie die Benutzersperrrichtlinie	Navigieren Sie zu **System** > **Benutzerverwaltung**. Wählen Sie unter **Benutzerkonfiguration** die Option **Konfiguration der Benutzersperrung** aus, und aktivieren Sie dann das Kontrollkästchen **Benutzersperre aktivieren**. Sie können die Anzahl der ungültigen Versuche angeben, die ein Benutzer unternehmen kann, bevor sein Konto deaktiviert wird, und wie lange die Benutzersperrrichtlinie aktiv ist.
Ändern Sie die Komplexität des Kennworts	Navigieren Sie zu **System** > **Benutzerverwaltung**. Wählen Sie unter **Benutzerkonfiguration** die Option **Kennwortrichtlinie** aus, und aktivieren Sie dann das Kontrollkästchen **Kennwortkomplexität aktivieren**. Geben Sie im Feld **Mindestkennwortlänge** die Mindestanzahl von Zeichen ein, die für ein Kennwort auf dem Citrix ADM erforderlich sind.
Einen Benutzer hinzufügen oder ändern	Navigieren Sie zu **System** > **Benutzerverwaltung > Benutzer**. Fügen Sie unter Benutzer einen neuen Benutzer hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen Benutzer. Wenn Sie einen Benutzer hinzufügen, können Sie Optionen wie externe Authentifizierung, Sitzungstimeout und die Zuweisung des Benutzers zu bestimmten Gruppen aktivieren.
Benutzergruppe hinzufügen oder ändern	Navigieren Sie zu **System** > **Benutzeradministration** > **Gruppen**. Fügen Sie unter **Gruppen** eine neue Gruppe hinzu oder bearbeiten Sie die Einstellungen für eine vorhandene Gruppe. Wenn Sie eine Gruppe hinzufügen, können Sie Optionen wie das Zuweisen von Berechtigungen für die Gruppe, das Konfigurieren eines Sitzungstimeouts, das Zuweisen von Benutzern zur Gruppe und das Zulassen des Zugriffs auf bestimmte oder alle Anwendungen im Citrix ADM aktivieren.
Ändern Sie die Authentifizierungskonfiguration	Navigieren Sie zu **System** > **Authentifizierung** > **Authentifizierung** . Wählen Sie unter **Authentifizierung** die **Option** Authentifizierungskonfiguration aus, und wählen Sie den Typ des Authentifizierungsservers aus.
RADIUS-Server hinzufügen oder ändern	Navigieren Sie zu **System** > **Authentifizierung** > **RADIUS** . Fügen Sie unter **RADIUS** einen neuen RADIUS-Server hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen RADIUS-Server, indem Sie die Netzwerkparameter eingeben oder ändern.
Einen LDAP-Server hinzufügen oder ändern	Navigieren Sie zu System > Authentifizierung > LDAP. Fügen Sie unter LDAP einen neuen LDAP-Server hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen LDAP-Server, indem Sie die Netzwerkparameter eingeben oder ändern.
Einen TACACS-Server hinzufügen oder ändern	Navigieren Sie zu **System** > **Authentifizierung** > **TACACS** . Fügen Sie unter **TACACS** einen neuen TACACS-Server hinzu oder bearbeiten Sie die

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Einstellungen für einen vorhandenen TACACS-Server, indem Sie die Netzwerkparameter eingeben oder ändern. |
Einen Syslog-Server hinzufügen oder ändern	Navigieren Sie zu **System** > **Überwachung** > **Syslog-Server** . Fügen Sie unter **Syslog**-Server einen neuen Syslog-Server hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen Syslog-Server, indem Sie die Netzwerkparameter eingeben oder ändern. Sie können zusätzliche Informationen bereitstellen, indem Sie die Art der Log-Levels auswählen, die Sie überwachen möchten.
Syslog-Meldungen lesen	Navigieren Sie zu **System** > **Auditing** . Wählen Sie unter **Audit-Meldungen** die Option **Syslog-Nachrichten** aus. Zusammenfassungen aller Systemprotokolldateien werden im Syslog Viewer angezeigt. Sie können die Syslog-Datei, die Sie anzeigen möchten, aus der Dropdownoption Datei auswählen. Darüber hinaus können Syslog-Dateien weiter nach Modul, Ereignistyp und Schweregrad gefiltert werden.
Konfigurieren Sie die Syslog-Bereinigungseinstellungen	Navigieren Sie zu **System** > **Auditing** . Wählen Sie unter **Einstellungen** die Option Syslog-Löscheinstellungen aus, und geben Sie dann die Anzahl der Tage ein, für die Syslog-Daten aufbewahrt werden sollen, bevor sie aus dem Citrix ADM gelöscht werden.****
Systemereignisse anzeigen	Navigieren Sie zu **System** > **Ereignisse** . Sie können dann alle aktuellen Ereignisse mit Details sehen.
Einen NTP-Server hinzufügen oder ändern	Navigieren Sie zu **System** > **NTP-Server**. Fügen Sie einen neuen NTP-Server hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen NTP-Server.
NTP-Parameter konfigurieren	Navigieren Sie zu **System** > **NTP-Server**. Klicken Sie auf **NTP-Parameter** und geben Sie die Konfigurationsdetails des Servers in die dafür vorgesehenen Felder ein.
NTP-Synchronisierung aktivieren	Navigieren Sie zu **System** > **NTP-Server**. Um die auf dem NTP-Server angezeigte Uhrzeit mit Ihrer lokalen Uhr zu synchronisieren, aktivieren Sie das Kontrollkästchen **NTP-Synchronisierung aktivieren**.
Verschlüsselungsgruppen hinzufügen oder ändern	Navigieren Sie zu **System** > **Verschlüsselungsgruppen**, um eine neue Verschlüsselungsgruppe hinzuzufügen oder die Einstellungen einer vorhandenen Verschlüsselungsgruppe zu bearbeiten. Sie müssen eine Beschreibung Ihrer Verschlüsselungsgruppe eingeben und sie einer Verschlüsselungssuite zuweisen.
Benachrichtigungseinstellungen konfigurieren	Navigieren Sie zu **System** > **Benachrichtigungen**. Wählen Sie unter **Einstellungen** die Option **Benachrichtigungseinstellungen ändern** aus. Wählen Sie die Aktionen aus, für die Sie die Benachrichtigungen senden möchten, und wählen Sie **E-Mail**, **SMS** oder beides aus.
Event-Digest-Einstellungen konfigurieren	Navigieren Sie zu **System** > **Benachrichtigungen**. Wählen Sie unter **Einstellungen** die Option **Event Digest-Einstellungen konfigurieren** aus. Nachdem Sie das Kontrollkästchen **Event Digest deaktivieren** deaktiviert haben, können Sie einen Wiederholungszeitraum festlegen und eine E-Mail-Verteilerliste für den Versand von Event-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Digest-Benachrichtigungen auswählen. |
E-Mail-Server hinzufügen oder ändern	Navigieren Sie zu **System** > **Benachrichtigungen** > E-**Mail** . Wählen Sie unter E-**Mail** die Registerkarte E-**Mail**-Server aus, um einen neuen E-Mail-Server hinzuzufügen oder die Einstellungen für einen vorhandenen E-Mail-Server zu bearbeiten. Sie können zusätzliche Prüfungen aktivieren, um sicherzustellen, dass für den Zugriff auf den E-Mail-Server eine Authentifizierung erforderlich ist, oder um anzugeben, dass Ihr E-Mail-Server die SSL-Authentifizierung unterstützt.
E-Mail-Verteilerlisten hinzufügen oder ändern	Navigieren Sie zu **System** > **Benachrichtigungen** > E-**Mail** . Wählen Sie unter **E**-**Mail** die Registerkarte E-Mail-Verteilerliste aus, um eine neue E-Mail-Verteilerliste hinzuzufügen oder die Einstellungen für eine vorhandene E-Mail-Verteilerliste zu bearbeiten.
SMS-Server hinzufügen oder ändern	Navigieren Sie zu **System** > **Benachrichtigungen** > **SMS** . Wählen Sie unter **SMS** die Registerkarte **SMS-Server** aus, um einen neuen SMS-Server hinzuzufügen oder die Einstellungen für einen vorhandenen SMS-Server zu bearbeiten .
SMS-Verteilerlisten hinzufügen oder ändern	Navigieren Sie zu **System** > **Benachrichtigungen** > **SMS** . Wählen Sie unter **SMS** die Registerkarte **SMS-Verteilerliste** aus, um eine neue SMS-Verteilerliste hinzuzufügen oder die Einstellungen für eine vorhandene SMS-Verteilerliste zu bearbeiten.
SNMP-Engine-ID konfigurieren	Navigieren Sie zu **System** > **SNMP**. Wählen Sie unter **Einstellungen** die Option **Engine-ID konfigurieren** aus und geben Sie die Engine-ID an.
SNMP MIB konfigurieren	Navigieren Sie zu **System** > **SNMP**. Wählen Sie unter **Einstellungen** die Option **SNMP MIB konfigurieren** aus und geben Sie die SNMP MIB-Details ein.
SNMP-Traps konfigurieren	Navigieren Sie zu **System** > **SNMP** > **Trap-Ziele**. Fügen Sie unter **SNMP-Traps** ein neues SNMP-Trap-Ziel hinzu oder bearbeiten Sie die Einstellungen für ein vorhandenes SNMP-Trap-Ziel.
Einen SNMP-Manager hinzufügen oder ändern	Navigieren Sie zu **System** > **SNMP** > **Manager**. Fügen Sie unter **SNMP Manager** einen neuen SNMP-Manager hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen SNMP-Manager.
Einen SNMP-Benutzer hinzufügen oder ändern	Navigieren Sie zu **System** > **SNMP** > **Benutzer**. Fügen Sie unter **SNMP-Benutzer** einen neuen SNMP-Benutzer hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen SNMP-Benutzer.
SNMP-Ansichten hinzufügen oder ändern	Navigieren Sie zu **System** > **SNMP** > **Views** . Fügen Sie unter **SNMP-Ansicht** eine neue SNMP-Ansicht hinzu oder bearbeiten Sie die Einstellungen für eine vorhandene SNMP-Ansicht.
Alarme ändern	Navigieren Sie zu **System** > **Alarme** und wählen Sie den Alarm aus, dessen Einstellungen Sie ändern möchten. Alarme helfen Ihnen dabei, den Zustand Ihres Citrix ADM Servers zu überwachen.
Sehen Sie sich das Task-Protokoll an	****Navigieren Sie zu **System** > **Diagnose** > Aufgabenprotokolle . Sie können dann alle Aufgabenprotokolle mit Details sehen. Sie können zusätzliche

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Informationen anzeigen, indem Sie ein Task-Protokoll auswählen und dessen Geräteprotokoll anzeigen und dann das Befehlsprotokoll für das ausgewählte Geräteprotokoll anzeigen. |
Generieren Sie die Datei für den technischen Support	Navigieren Sie zu **System** > **Diagnose** > **Technischer Support** . Klicken Sie unter **Technischer Support** auf **Datei für technischen Support** generieren, um ein Archiv (TAR-Datei) der Citrix ADM-Daten und -Statistiken zu generieren, das Sie an den Citrix Support senden können , um Hilfe beim Debuggen eines Problems zu erhalten.
Zeitzoneneinstellungen für Dashboard-Berichte konfigurieren	Navigieren Sie zu **System** > **Analytics-Einstellungen**. Wählen Sie unter **Analytics-Einstellungen** die Option **Dashboard-Berichtszeitzoneneinstellungen konfigurieren** aus, um Ihre Ortszeit oder GMT-Zone als Standard für die in Ihrem Dashboard angezeigten Berichte festzulegen.
Timeout für ICA-Sitzungen konfigurieren	Navigieren Sie zu **System** > **Analytics-Einstellungen**. Wählen Sie unter **Analytics-Einstellungen** die Option **ICA-Sitzungstimeout konfigurieren** aus und geben Sie den Zeitraum ein, für den eine ICA-Sitzung im Leerlauf bleiben kann, bevor sie beendet wird.
Analytics-Funktionen konfigurieren	Navigieren Sie zu **System** > **Analytics-Einstellungen**. Wählen Sie unter **Analytics-Einstellungen** die Option **Funktionen konfigurieren** aus, um Multihop-Einstellungen und adaptive Schwellenwerteinstellungen zu aktivieren. Wenn Sie das Kontrollkästchen **Multihop aktivieren** aktivieren , erfasst und korreliert Citrix ADM die AppFlow-Datensätze von allen Appliances, die mit mehr als einer Citrix ADC-Instanz zwischen einem Client und einem Server bereitgestellt werden. Wenn Sie das Kontrollkästchen **Adaptiven Schwellenwert aktivieren** aktivieren , wird eine Syslog-Meldung an den Syslog-Server gesendet, wenn die Anzahl der Treffer auf einer URL den Schwellenwert überschreitet.
Datenbankeinstellungen konfigurieren	Navigieren Sie zu **System** > **Analytics-Einstellungen**. Wählen Sie unter **Analytics-Einstellungen** die Option **Funktionen konfigurieren** aus, um die Datenbankindexeinstellungen und die Einstellungen für die Datenbankbereinigung zu aktivieren. Indem Sie das Kontrollkästchen Datenbankindizierung **aktivieren** aktivieren , können Sie eine effiziente Abfrage der Citrix ADM-Datenbank ermöglichen. Wenn Sie das Kontrollkästchen **Datenbankbereinigung aktivieren** aktivieren , wird der Versuch, die Datenbank zu bereinigen, wiederholt, wenn eine hohe Belastung des Citrix ADM die Bereinigung zum regelmäßig geplanten Zeitpunkt verhindert.
Datenbank-Cache-Einstellungen konfigurieren	Navigieren Sie zu **System** > **Analytics-Einstellungen**. Wählen Sie unter **Analytics-Einstellungen** die Option Datenbank-**Cache-Einstellungen konfigurieren** aus, um den Datenbankinhalt lokal im Cache zu speichern, sodass Sie diesen Inhalt anzeigen können, ohne Zugriff auf den Datenbankserver zu benötigen.
Konfiguration der Datensatzeinstellungen	Wählen Sie in den **Analytics-Einstellungen** die Option **Datensatzeinstellungen konfigurieren** aus. Sie können Funktionen für die folgenden Einstellungen aktivieren: Einstellungen für das Datensatzprotokoll, Einstellungen für die Persistenz der Datendauer, Web Insight-Berichtseinstellungen, Web Insight SLA-Datenerfassungseinstellungen, Web Insight-URL-Datenerfassungseinstellungen, URL-Parametereinstellungen

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SLA-Management für bestimmte Citrix ADC IP-Adressen konfigurieren	Navigieren Sie zu **System** > **Analytics-Einstellungen** > **SLA-Verwaltung**. Wählen Sie aus der angezeigten Liste die Citrix ADC IP-Adresse einer Appliance aus, auf der Sie SLA über Serverantwortzeit, Treffer/Sekunde und Bandbreitennutzung verwalten möchten.
Konfigurieren Sie die Dauer, für die Datenbankdatensätze für jede Insight-Zusammenfassungsebene aufbewahrt werden sollen	Navigieren Sie zu **System** > **Analytics-Einstellungen** > **Datenbankzusammenfassung**. Geben Sie die Dauer an, für die Sie Insight-Daten auf Citrix ADM aufbewahren möchten. Sie können wählen, ob Sie diese Daten stündlich, täglich oder einmal pro Minute speichern möchten.
Adaptive Schwellenwerte hinzufügen oder ändern	Navigieren Sie zu **System** > **Analytics-Einstellungen** > **Adaptive Schwellenwerte**. Fügen Sie unter **Adaptive Schwellenwerte** einen neuen adaptiven Schwellenwert hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen adaptiven Schwellenwert. 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 höher ist als der für die URL festgelegte Schwellenwert, wird eine Syslog-Meldung an einen externen Syslog-Server gesendet. Das Schwellenwertintervall kann entweder Tage oder Wochen betragen.
Schwellenwert und Warnmeldungen hinzufügen oder ändern	Navigieren Sie zu **System** > **Analytics-Einstellungen** > **Schwellenwerte**. Fügen Sie unter **Schwellenwerte** ein neues Limit hinzu oder bearbeiten Sie die Einstellungen für einen vorhandenen Schwellenwert. Sie können beim Erstellen oder Ändern eines Schwellenwerts zusätzliche Aktionselemente bereitstellen, z. B. ihn aktivieren, Benachrichtigungen per E-Mail oder SMS senden oder eine Regel für den Schwellenwert konfigurieren.
Laden Sie SSL-Zertifikatsdateien und SSL-Schlüssel hoch	Navigieren Sie zu **System** > **Erweiterte Einstellungen** > **SSL-Zertifikatsdateien**. Wählen Sie unter SSL-Zertifikatsdateien die Registerkarte **SSL-Zertifikate** aus, um ein neues **SSL-Zertifikat** hochzuladen. Wählen Sie auf ähnliche Weise unter SSL-Zertifikatsdateien die Registerkarte **SSL-Schlüssel** aus, um einen neuen **SSL-Schlüssel** hochzuladen.
Zeitplan (en) für den Export von Berichten anzeigen oder bearbeiten	Navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Zeitpläne exportieren**. Sie können dann alle Exportpläne mit Details sehen. Sie können jeden Exportplan aus der hier angezeigten Liste bearbeiten.
Einen Berichtsexport planen	Navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Zeitpläne exportieren**. Um einen neuen Zeitplan hinzuzufügen, klicken Sie auf die Schaltfläche ganz rechts und wählen Sie die Registerkarte **Zeitplanexport**. Geben Sie die Details an und klicken Sie auf **Planen**.
Verwenden Sie die Backup- und Wiederherstellungsfunktionen	Navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Sicherungsdateien**, um eine Sicherungskopie der aktuellen Einstellungen von Citrix ADM zu erstellen. Sie können diese gesicherten Dateien später verwenden, um das Citrix ADM in den Zustand zurückzusetzen, den Sie gesichert haben. Citrix empfiehlt, diese

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Funktion vor der Durchführung eines Upgrades und generell als Vorsichtsmaßnahme zu verwenden. |
Installieren eines SSL-Zertifikats	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Citrix ADM** einrichten die Option **SSL-Zertifikat installieren** aus. Sie können eine Zertifikatsdatei und eine SSL-Schlüsseldatei auswählen, die sich bereits auf der virtuellen Citrix ADM Appliance befinden, oder Sie können die Dateien von Ihrem lokalen Computer hochladen. Sie müssen das Citrix ADM Kennwort in das Feld Kennwort eingeben, um das SSL-Zertifikat erfolgreich zu installieren.
Anmeldedaten für die Instanzanmeldung abfragen	**Navigieren Sie zu**System**> Systemeinstellungen ändern** . Aktivieren Sie **Prompt Credentials for Instance Login** , um Benutzer bei jedem Konfigurationsvorgang auf Citrix ADC-Instanzen zur Eingabe ihrer Instanzanmeldeinformationen aufzufordern.
Automatische Datenlöschung aktivieren	Navigieren Sie zu **System** > **Systemadministration**. Wählen Sie unter **Prune Settings** die Option **System Prune Settings** aus. Wählen Sie das Kontrollkästchen **Automatische Datenlöschung aktivieren**, damit Citrix ADM die Daten löschen kann, wenn die Festplattennutzung den festgelegten Schwellenwert erreicht. Wenn diese Funktion aktiviert ist, löscht Citrix ADM Daten zu Ereignissen, Syslogs, Leistungsberichten und Analysen, bis die Festplattennutzung den festgelegten Schwellenwert unterschreitet. Klicken Sie auf das Bearbeitungssymbol, um den Schwellenwert für die Festplattennutzung zu ändern.

Einstellungen für das Systembackup konfigurieren

February 5, 2024

Sie sollten die anfänglichen Systembackupeinstellungen festlegen, bevor Sie das Citrix Application Delivery Management (ADM) -System sichern und wiederherstellen müssen.

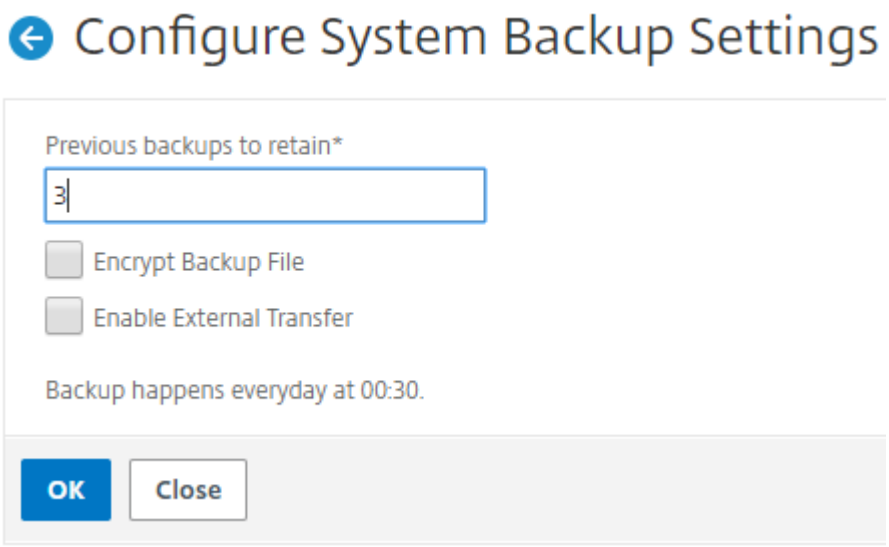
1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter**Backupeinstellungen**auf**Systemback**
2. Geben Sie auf der Seite **„Systemsicherungseinstellungen konfigurieren** “Folgendes an:

    - Anzahl der zu speichernden Backups. Sie können nur bis zu 10 Backups aufbewahren.
    - 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Übertragung finden Sie unter Übertragen einer Citrix ADM Backup-Datei 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 das Mindestabfrageintervall beispielsweise 64 Sekunden betragen soll, was als 2^6 ausgedrückt werden kann, geben Sie 6 ein

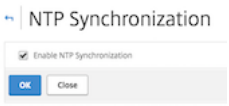
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

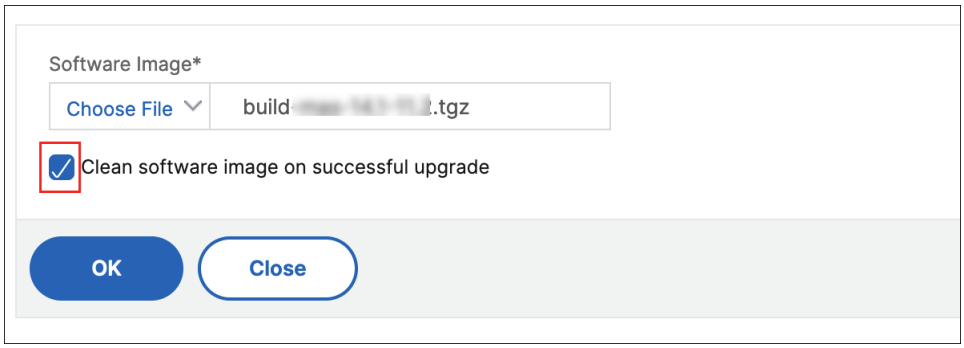
Upgrade von NetScaler ADM

February 5, 2024

Jede Version von Citrix Application Delivery Management (ADM) 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 **Citrix ADM aktualisieren**.
2. Laden Sie auf der Seite Citrix ADM aktualisieren eine neue Imagedatei hoch, indem Sie entweder **Lokal** (Ihre lokale Maschine) oder **Gerät** auswählen (die Zertifikatdatei muss auf der virtuellen Citrix ADM-Appliance vorhanden sein).
   Standardmäßig wird das Softwareimage nach einem erfolgreichen Upgrade bereinigt.
3. Klicken Sie auf **OK**.



Kennwort für NetScaler ADM zurücksetzen

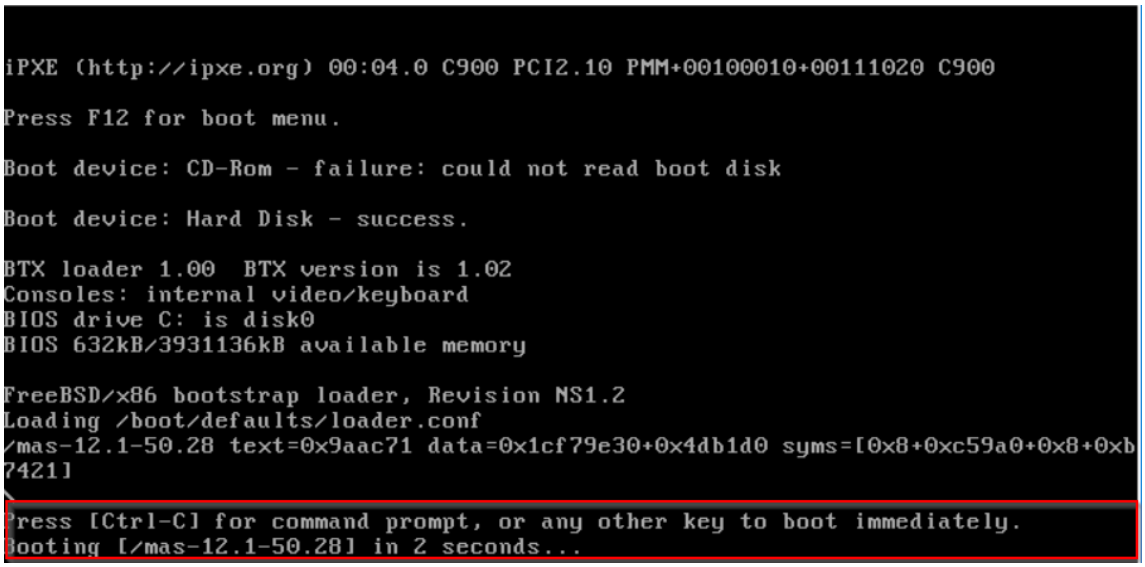
February 5, 2024

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.

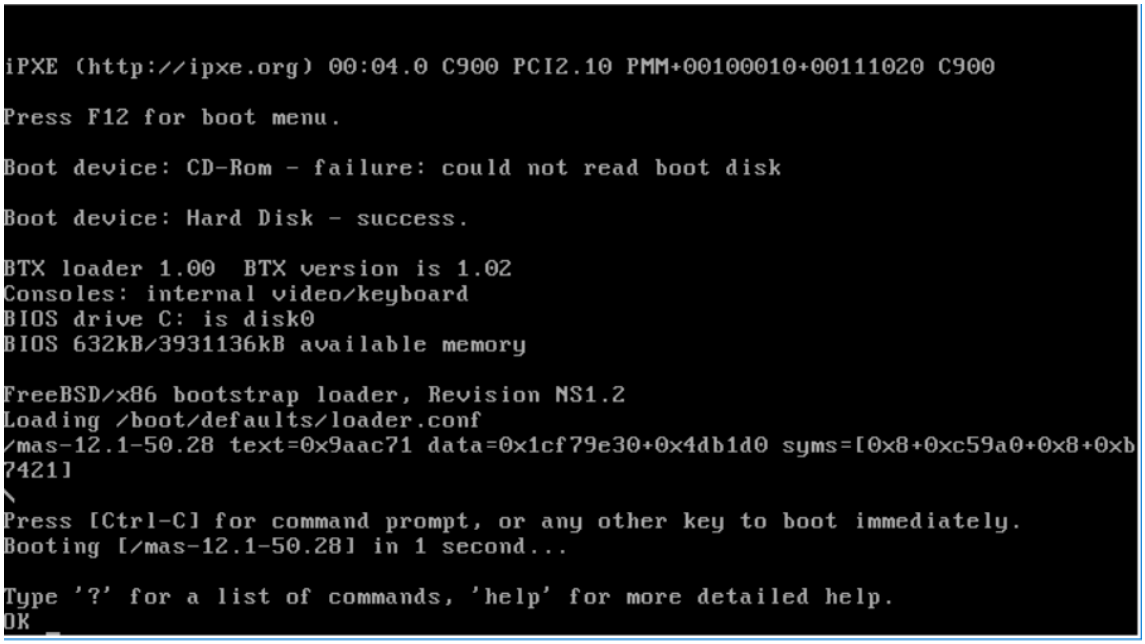
Citrix Hypervisor mit XenCenter:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

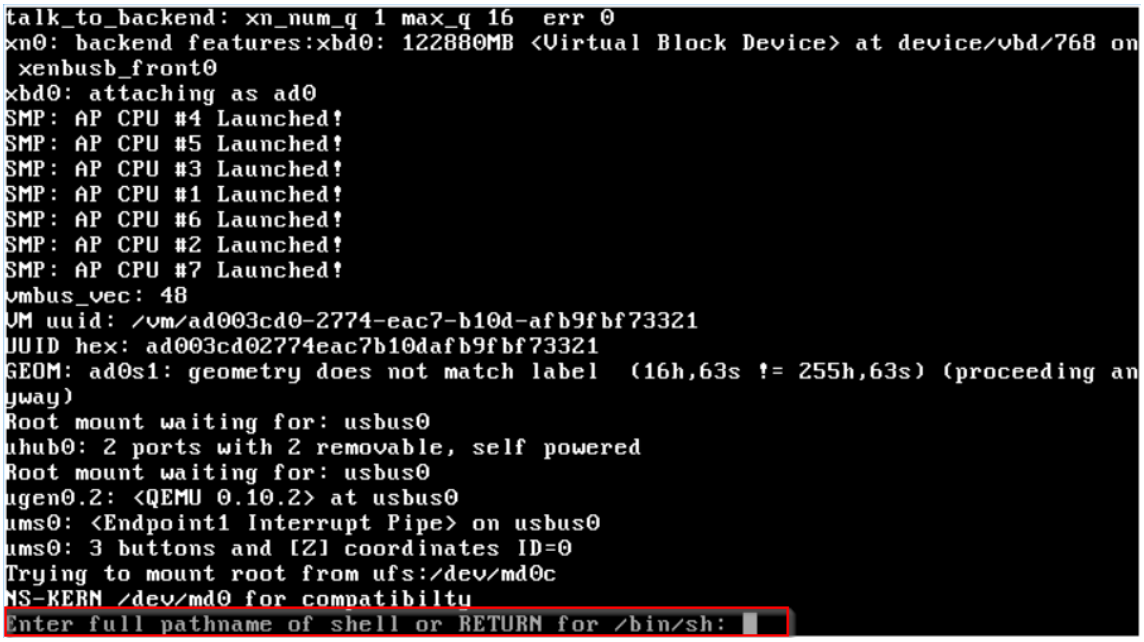


4. Führen Sie den Befehl **boot -s** an der Eingabeaufforderung OK

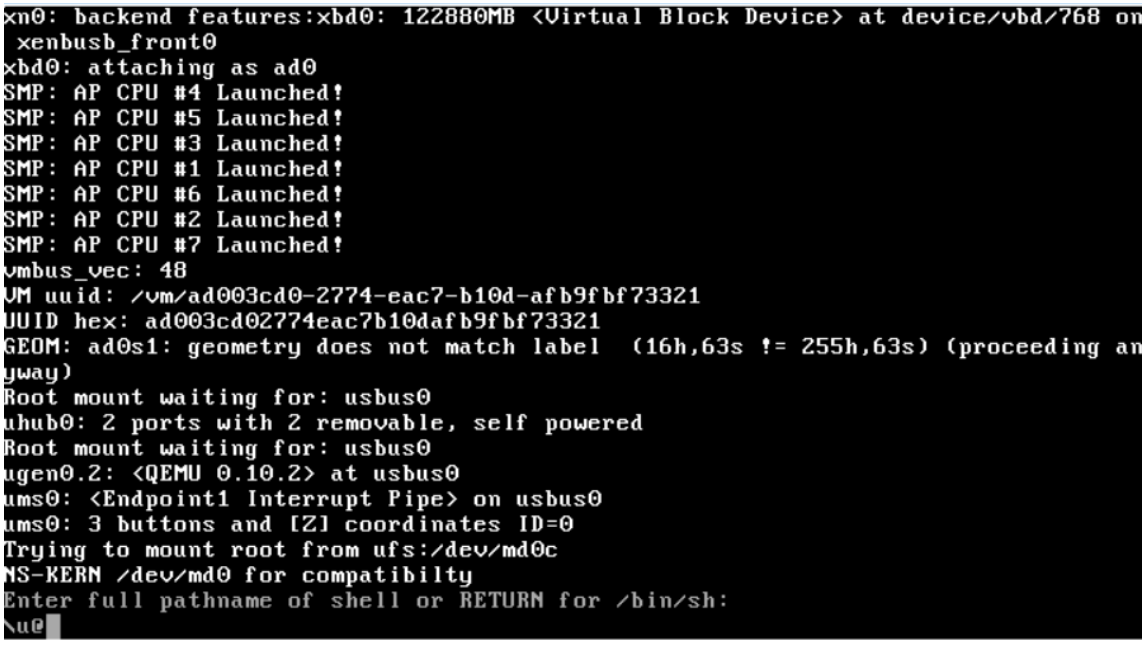


NetScaler ADM wird neu gestartet und zeigt die folgende Meldung an:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



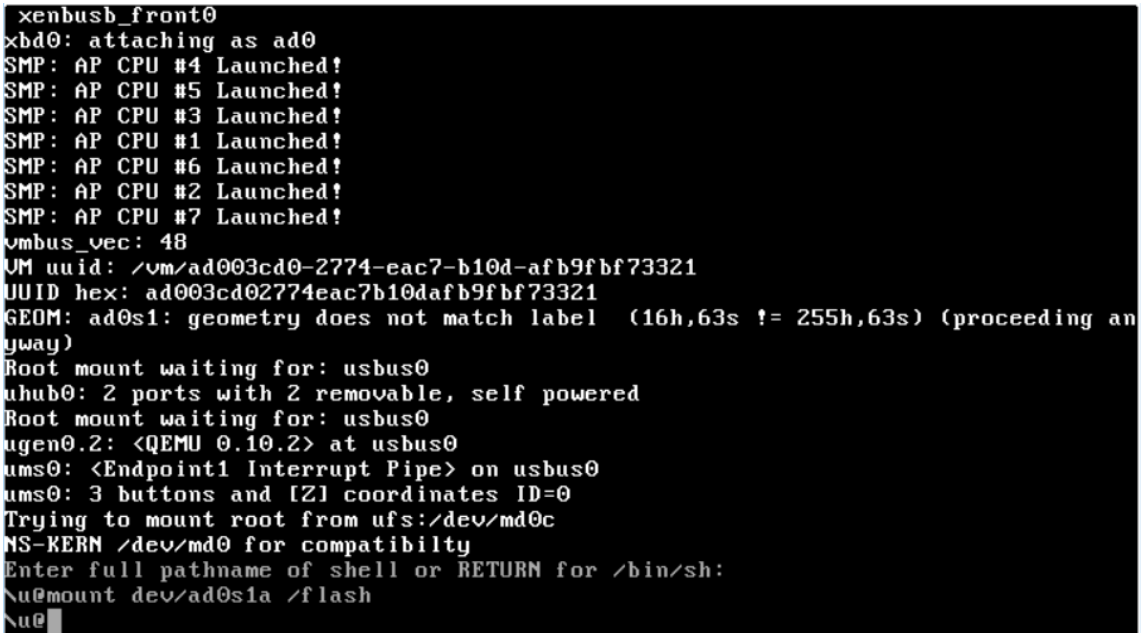
5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.



6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

```
mount dev/ad0s1a /flash
```

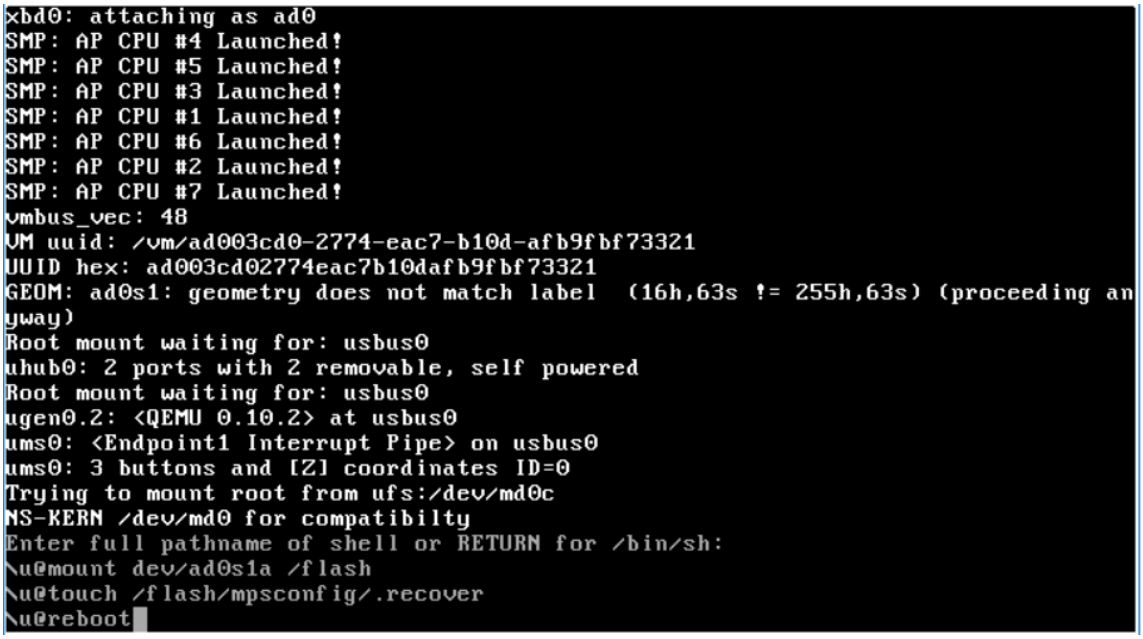
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm –rf /etc/passwd`
9. Erstellen Sie eine Datei mit dem folgenden Befehl:

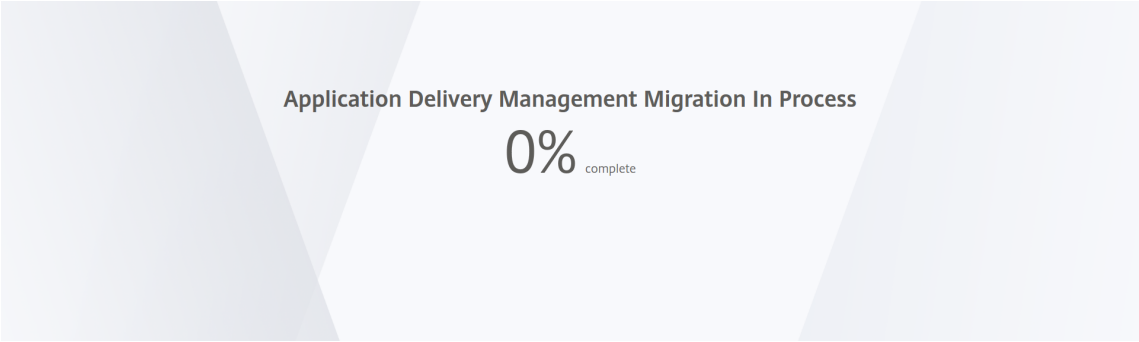
   `touch /flash/mpsconfig/.recover`

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.
10. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.



11. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.

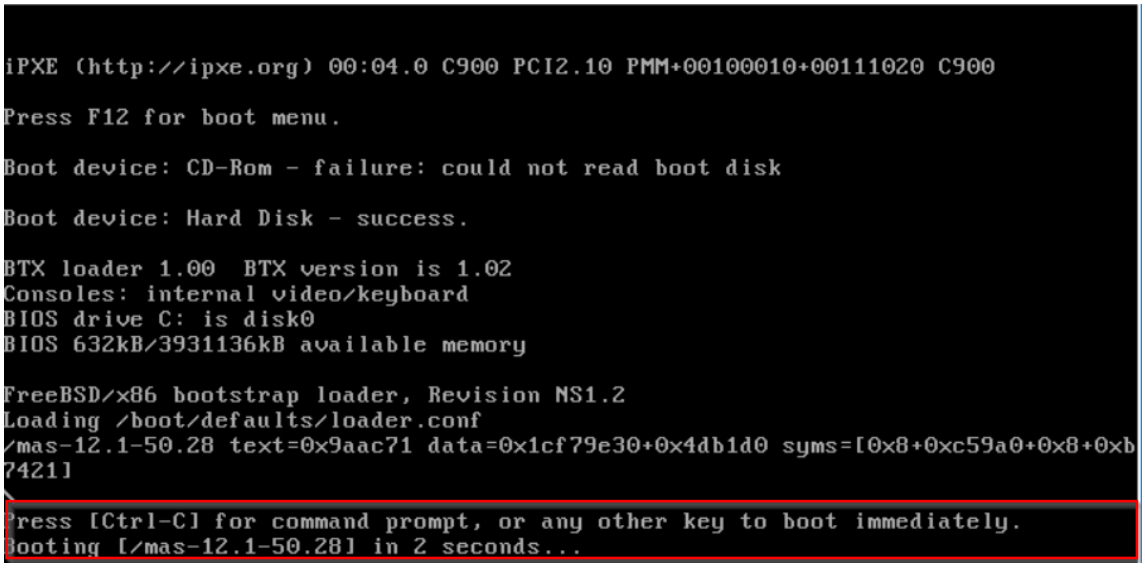
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom Hypervisor anzumelden.

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. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm –rf /etc/passwd`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

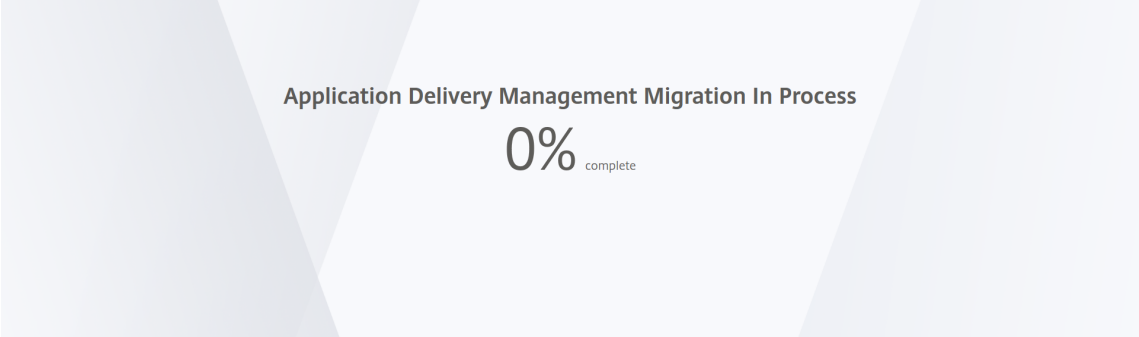
9. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.

10. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.

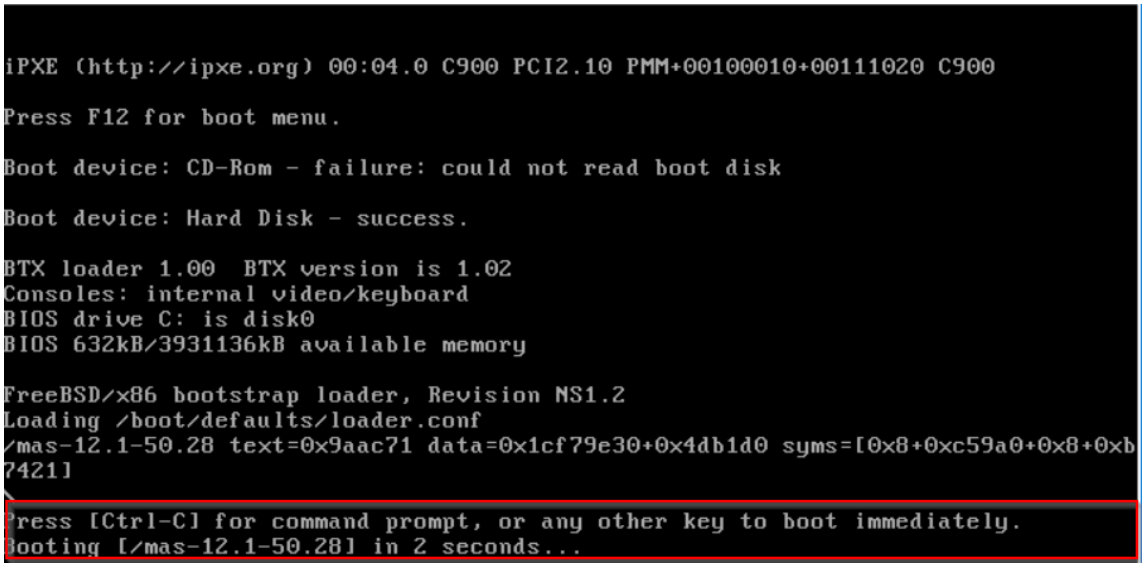
11. Greifen Sie auf die NetScaler ADM GUI zu und warten Sie, bis der Neustart abgeschlossen ist.



   Sie können jetzt *nsroot/nsroot* Anmeldeinformationen verwenden, um sich von der GUI anzumelden, und *nsrecover/nsroot*, um sich vom ESX-Server anzumelden.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

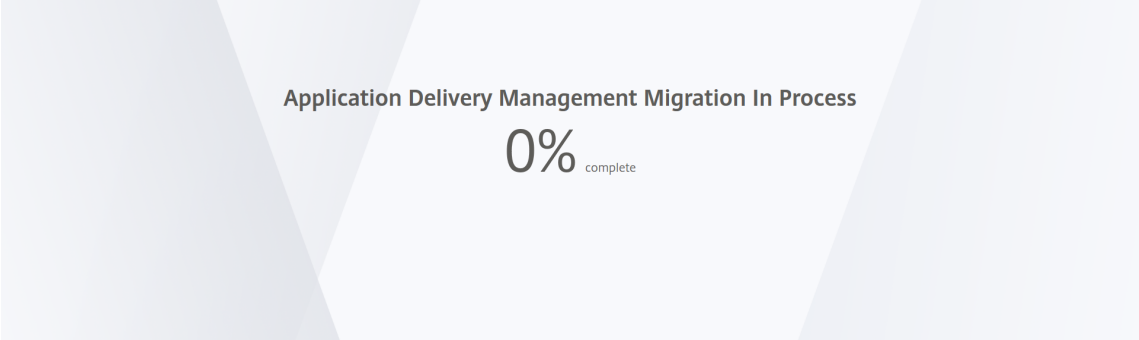
5. Drücken Sie die **Eingabetaste**, um die Eingabeaufforderung /u @ zu erhalten.
6. Mounten Sie die Flash-Partition mit dem folgenden Befehl:

   ```
   mount dev/ad0s1a /flash
   ```

7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm –rf /etc/passwd`
9. Erstellen Sie eine Datei mit dem folgenden Befehl:

   ```
   touch /flash/mpsconfig/.recover
   ```

   Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.
10. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
11. 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.

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:

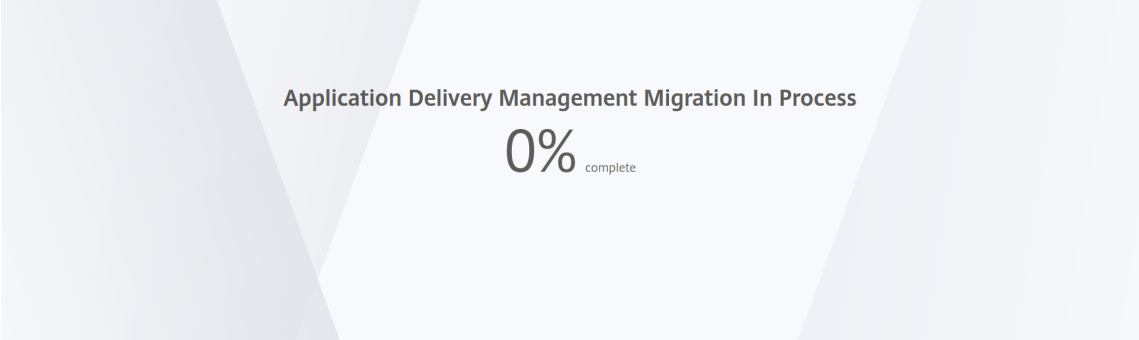
   ```
   mount dev/vtbd0s1a /flash
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. `Delete /flash/mpsconfig/master.passwd`
9. `Delete rm –rf /etc/passwd`
10. Erstellen Sie eine Datei mit dem folgenden Befehl:

    `touch /flash/mpsconfig/.recover`

    Das Kennwort wird nun auf das Standardkennwort zurückgesetzt.
11. Führen Sie den Befehl **Neustart** aus, um NetScaler ADM neu zu starten.
12. 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.

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 Syslog-Daten gelöscht werden sollen.Sie können die Anzahl der Tage angeben, nach denen die folgenden Syslog-Daten aus der NetScaler Application Delivery Management (ADM) gelöscht werden:

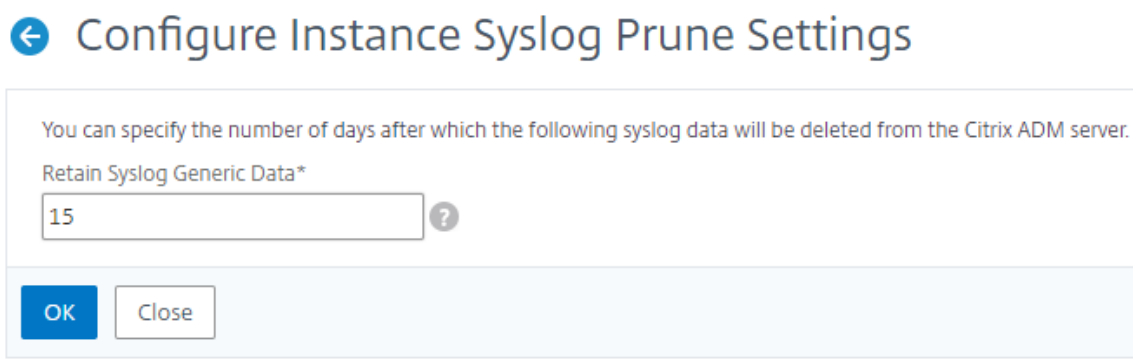
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Generische Syslog-Daten
- AppFirewall-Daten
- NetScaler Gateway Daten

Sie können das Citrix Gateway-Bereinigungsintervall auch nach Syslog-Typ konfigurieren. Dieses Bereinigungsintervall hat Vorrang vor dem Bereinigungsintervall, das für die Aufbewahrung von Citrix Gateway-Daten konfiguriert ist.

So konfigurieren Sie die Einstellungen für das Syslog-Löschintervall für Citrix ADM:

1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter **Prune Settings** auf **Instance Syslog Prune Settings**.
2. Geben Sie auf der Seite **Syslog-Löscheinstellungen für Instanzen konfigurieren** die Option **Generische Syslog-Daten beibehalten** an. Geben Sie die Anzahl der Tage ein, für die NetScaler ADM generische Syslog-Nachrichten aufbewahrt.



Einstellungen für Systemausfall konfigurieren

February 5, 2024

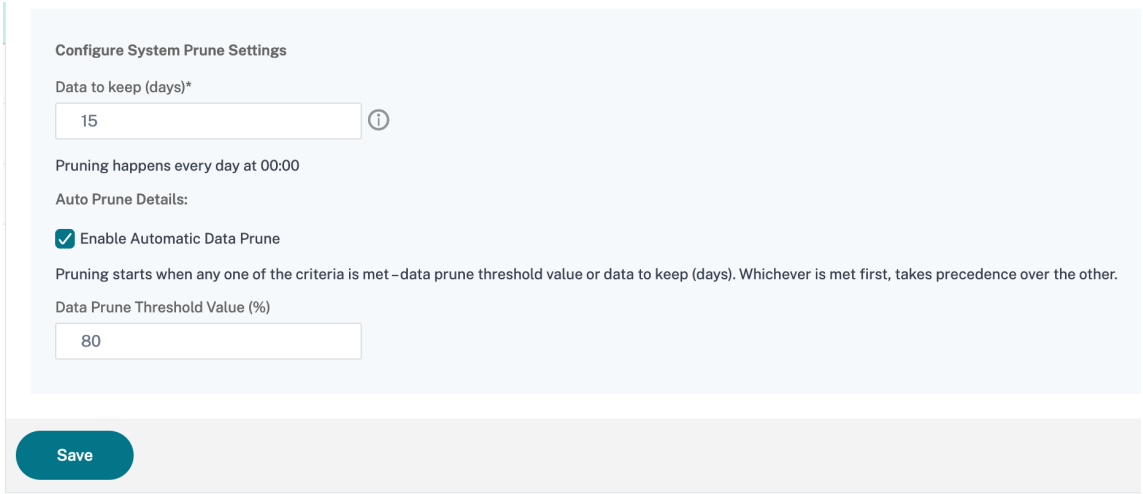
Um die Menge der Berichtsdaten zu begrenzen, die in der Datenbank der Citrix Application Delivery Management -Software (ADM) gespeichert werden, können Sie sie beschneiden. Sie können das Intervall angeben, für das NetScaler ADM Netzwerkberichtsdaten, Ereignisse, Überwachungsprotokolle und Aufgabenprotokolle 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Navigieren Sie zu **System** > **Systemadministration**. Klicken Sie unter **Prune Settings** auf **System Prune Settings** .
2. Geben Sie auf der Seite **Systemausfalleinstellungen konfigurieren** die Anzahl der Tage an, für die Daten gespeichert werden sollen, und klicken Sie auf**OK**.

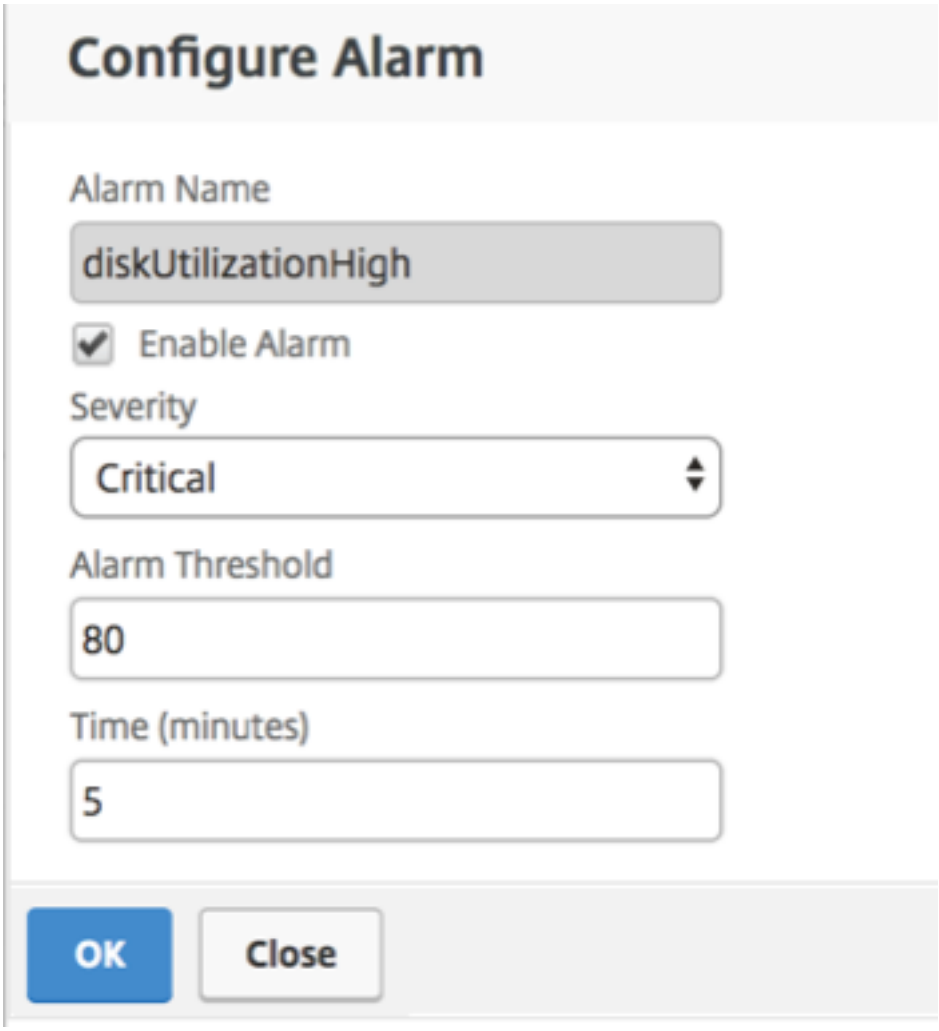


Sie können das automatische Löschen aktivieren, indem Sie das Kontrollkästchen **Automatische** Datenlöschung aktivieren aktivieren . **Ein Alarm wird ausgelöst, wenn die Festplattennutzung den konfigurierten Schwellenwert für die Datenlöschung überschreitet .**

Sie können den Alarm **diskUtilizationHigh** konfigurieren und aktivieren (standardmäßig) und Folgendes angeben:

- **Schweregrad,** z. B. Kritisch.
- **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.
    - **Enable nsrecover Login** - Aktivieren Sie nsrecover login auf Management Service.
    - **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verwenden des Citrix ADM Datenbankwiederherstellungsskripts für eine eigenständige Citrix ADM-Bereitstellung

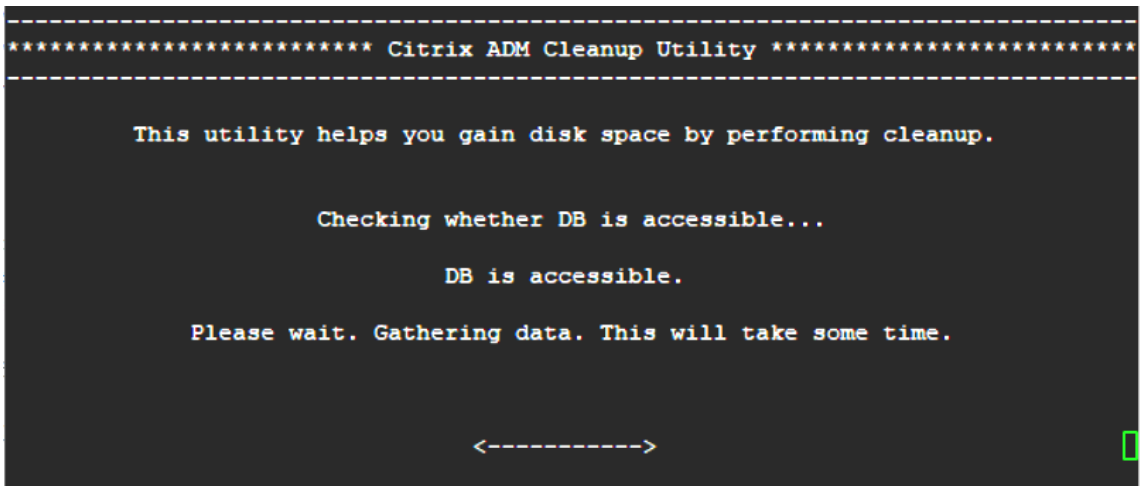
Verwenden Sie das folgende Verfahren in einer NetScaler ADM Bereitstellung für einen Server, um eine Verbindung mit dem Dateisystem herzustellen, einige Komponenten zu löschen, die Datenbank zugänglich zu machen und dann die Wiederherstellungsvorgänge durchzuführen.

1. Melden Sie sich mit einem SSH-Client oder der Konsole Ihres Hypervisors bei Citrix ADM an und geben Sie den folgenden Befehl ein:

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

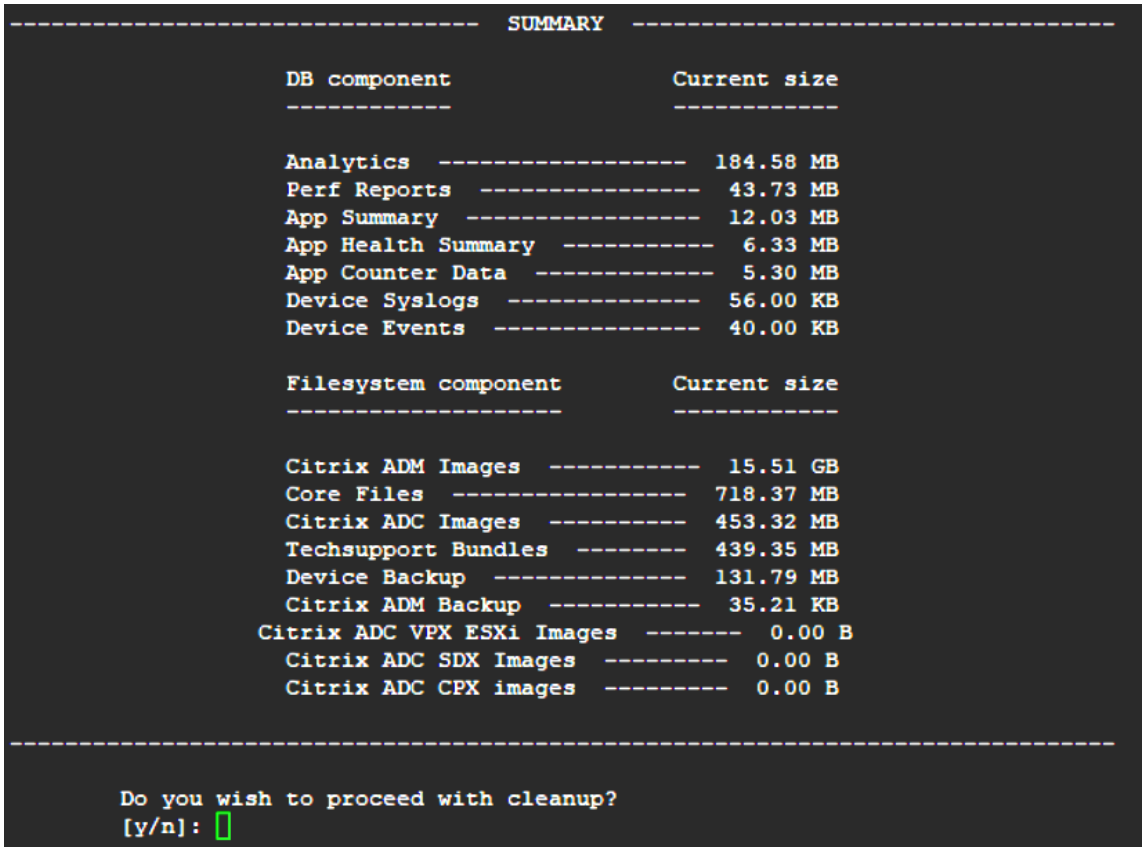
2. Wenn auf dem Bildschirm eine Warnmeldung zum Beenden einiger NetScaler ADM Prozesse angezeigt wird, geben Sie “y”ein, und drücken **Sie die Eingabetaste**.

   Der folgende Bildschirm wird angezeigt, während das System bestimmt, welche Komponenten der Datenbank Sie löschen können, ohne dass sich auf die Kerndateien des Systems auswirkt.



3. Auf dem Bildschirm wird die Liste der Dateien in der Datenbank angezeigt. Geben Sie “y”ein und drücken Sie die Eingabetaste, um den Bereinigungsprozess zu starten.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

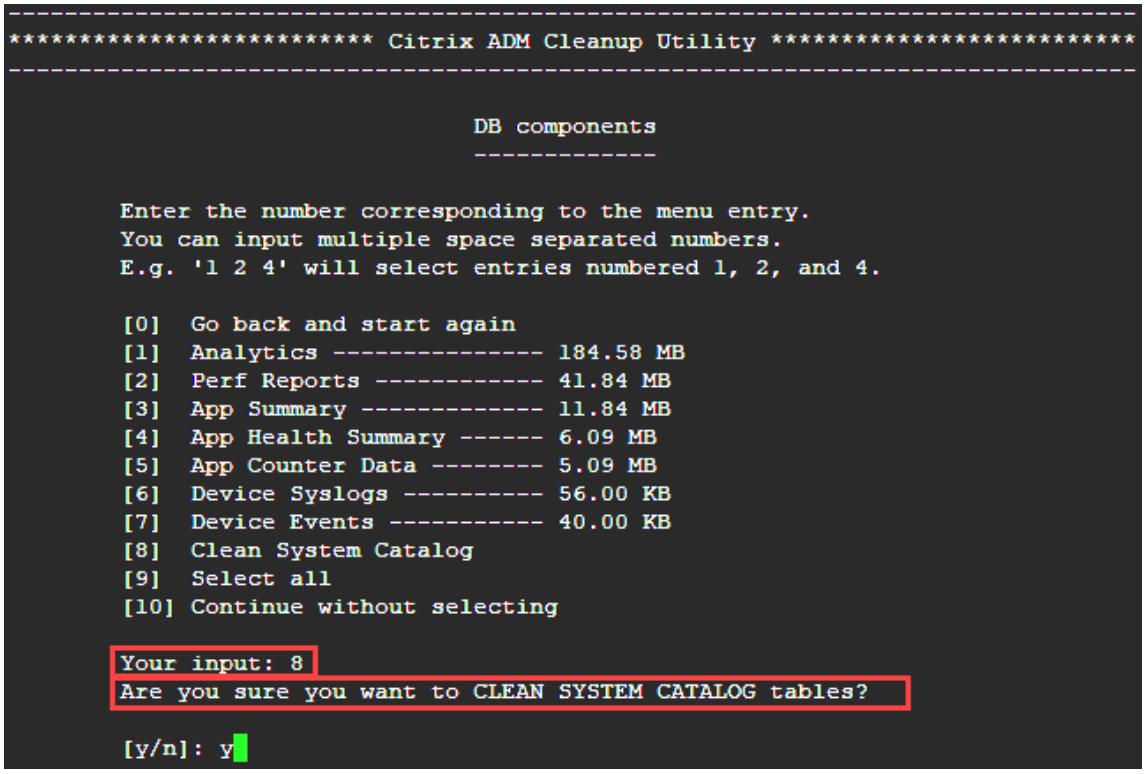


4. Sie können die spezifische Datenbankkomponente auswählen, die gereinigt werden muss, und die entsprechende Nummer eingeben. Drücken Sie die **Eingabetaste**.

   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.

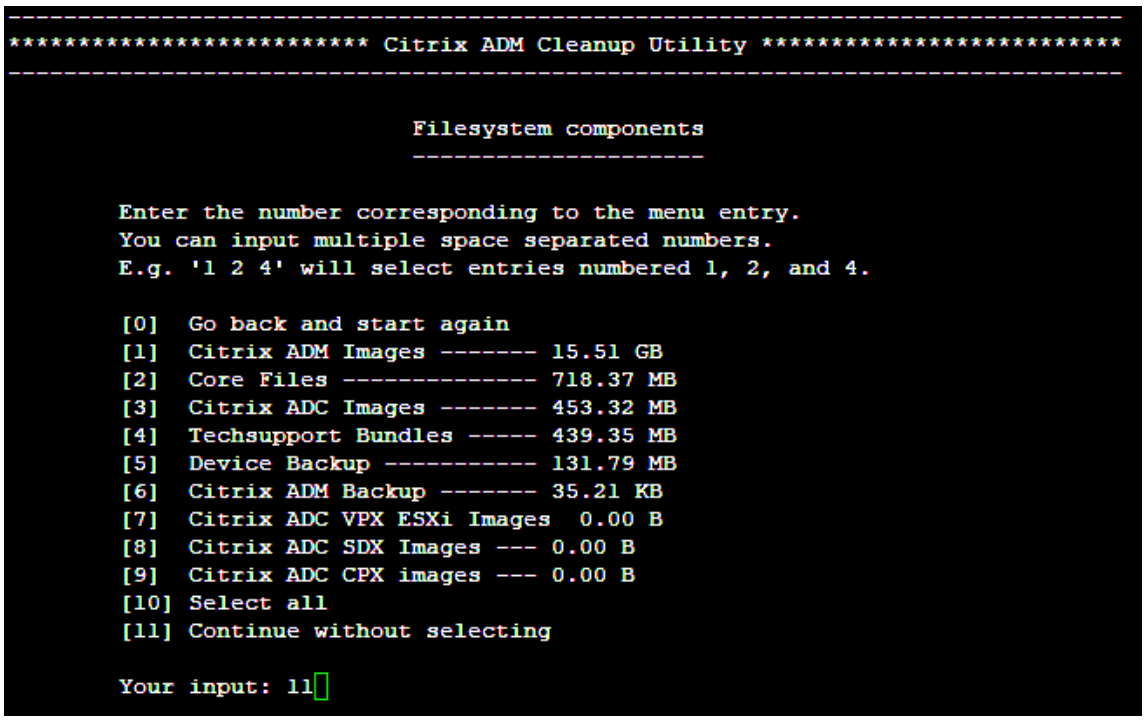
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



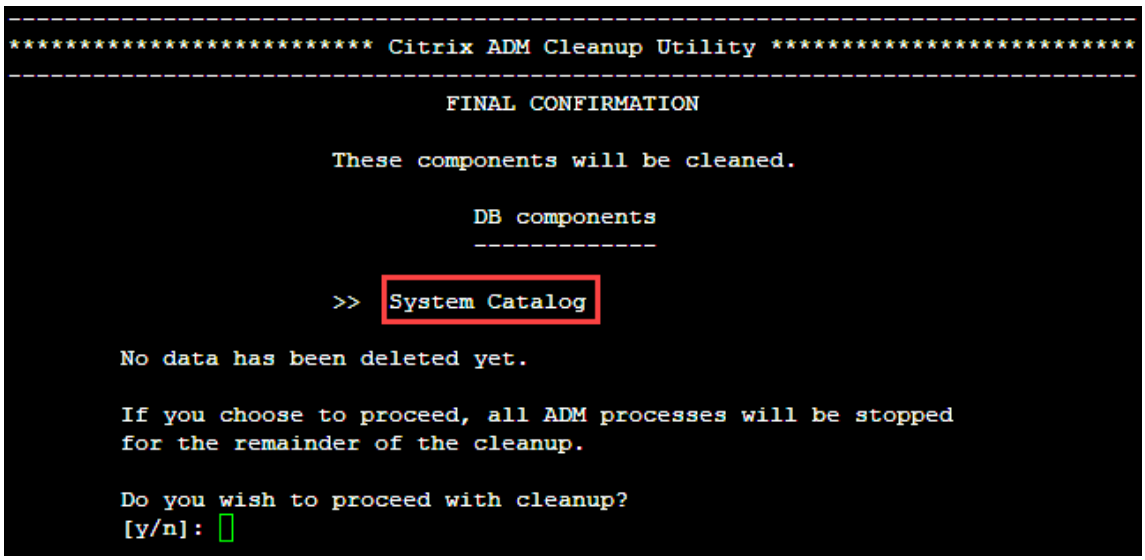
Das Cleanup-Hilfsprogramm bietet Ihnen die Möglichkeit, Datenbankkomponenten und Dateikomponenten zu bereinigen. Sie können eine beliebige Dateikomponente auswählen, indem Sie eine Zahl zwischen „1“und „9“eingeben oder „11”eingeben und die Eingabetaste drücken, um die Datenbankkomponente zu reinigen.

> **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”.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

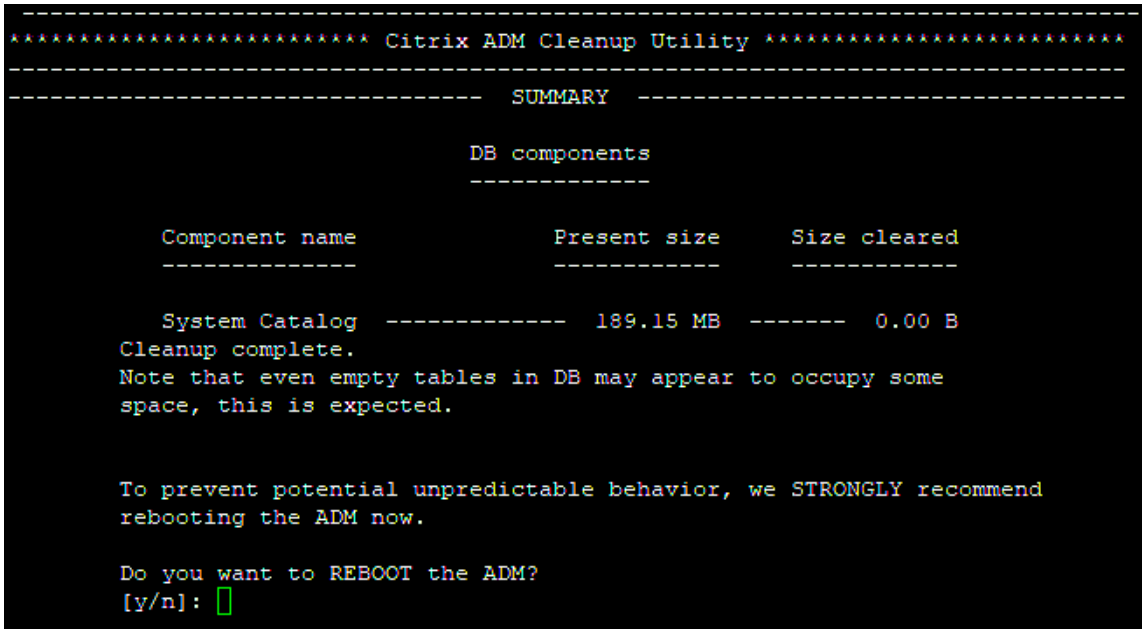


5. Geben Sie “y”ein und drücken Sie im letzten Bestätigungsbildschirm erneut die **Eingabetaste**.



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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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 müssen dann in der Lage sein, eine Verbindung zur Citrix ADM-Datenbank herzustellen. Wenn nicht, führen Sie das Wiederherstellungsskript erneut aus, um mehr Speicherplatz freizugeben. Wenn Citrix ADM läuft, muss 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

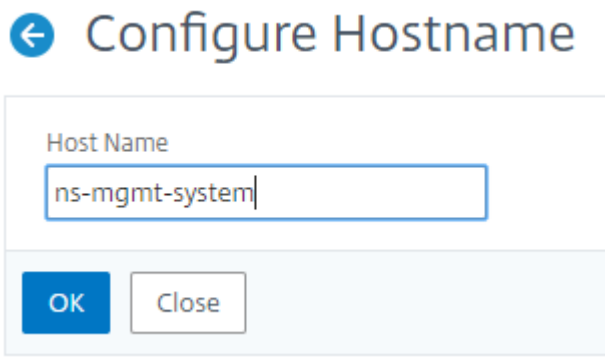
Hostnamen zu einem NetScaler ADM-Server zuweisen

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. Sichern Sie vor dem Upgrade die ADM-Serverkonfigurationsdateien aus Sicherheitsgründen.

Das Backup umfasst die folgenden Komponenten:

- Citrix ADM Konfigurationsdateien:
  - SNMP
  - Syslog-Serverkonfigurationsdateien
  - NTP-Dateien

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 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.

> **Hinweis**
>
> Analytics-Daten, Ereignisse und Syslog-Nachrichten werden von Backups 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.

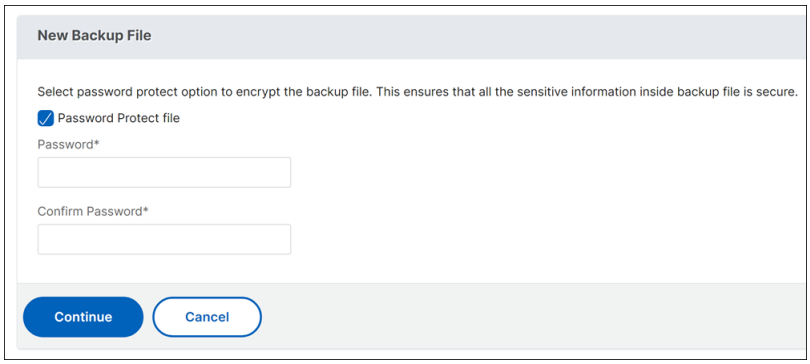
Das Backup wird als komprimierte TAR-Datei gespeichert, die auch verschlüsselt werden kann. Standardmäßig werden drei Sicherungsdateien auf dem Server aufbewahrt. Um Probleme mit geringem Speicherplatz zu vermeiden, können Sie maximal 10 Backupdateien auf dem NetScaler ADM -Server speichern. Citrix empfiehlt jedoch, einige Kopien Ihrer Backupdateien auf dem Server zu speichern oder die Dateien vorsorglich auf ein anderes System zu übertragen .

So sichern Sie eine NetScaler ADM Konfiguration:

1. Navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Backupdateien**, und klicken Sie dann auf **Backup**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Um die Backupdatei zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Kennwortschutzdatei**, und geben Sie dann ein Kennwort zum Verschlüsseln der Datei ein.



> **Hinweis**
>
> Sie können eine Backupdatei für die Verschlüsselung auch festlegen, indem Sie zu **System** > **Systembackupeinstellungen**navigieren und dann **Backupdatei verschlüsseln**auswählen.

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.

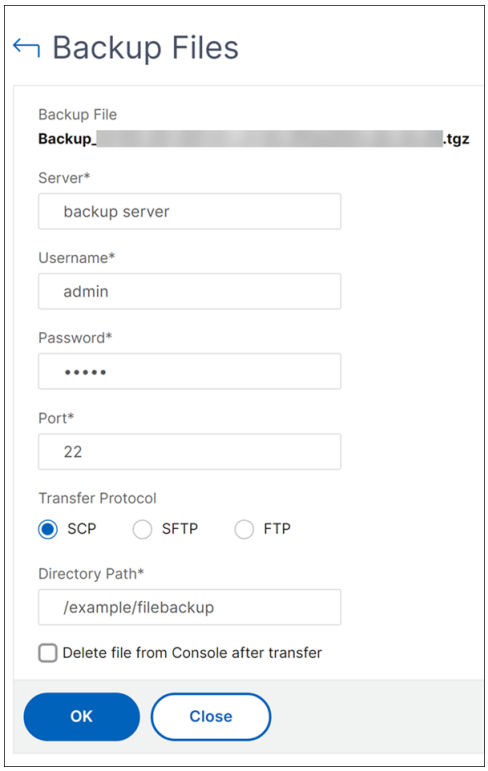
So übertragen Sie eine Citrix ADM Backupdatei:

1. Navigieren Sie zu**System**>**Erweiterte Einstellungen**>**Backupdateien**.
2. Wählen Sie die Backupdatei aus, die Sie auf ein anderes System verschieben möchten, und klicken Sie dann auf**Übertragen**.
3. Geben Sie auf der Seite **Backup-Dateien** die folgenden Parameter an:
   - **Server** —IP-Adresse des Systems, auf das Sie die gesicherte Datei übertragen möchten.
   - **Benutzername und Kennwort** —Benutzeranmeldedaten des neuen Systems, in das die gesicherten Dateien kopiert werden.
   - **Port** —Portnummer des Systems, auf das die Dateien übertragen werden.
   - **Übertragungsprotokoll** —Protokoll, das für die Übertragung der Sicherungsdatei verwendet wird. Sie können die Protokolle SCP, SFTP oder FTP auswählen, um die gesicherte Datei zu übertragen.
   - **Verzeichnispfad** - Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Alternativ können Sie auch die Details zu externen Systemen festlegen, indem Sie zu **System** > **Systembackupeinstellungen** navigieren.

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 auf Ihrem lokalen System zu speichern, navigieren Sie zu **System** > **Erweiterte Einstellungen** > **Backupdateien**, wählen Sie die Datei aus, die Sie kopieren möchten, und klicken Sie dann auf **Herunterladen**.

Wiederherstellen der NetScaler ADM Konfiguration aus einer Backupdatei

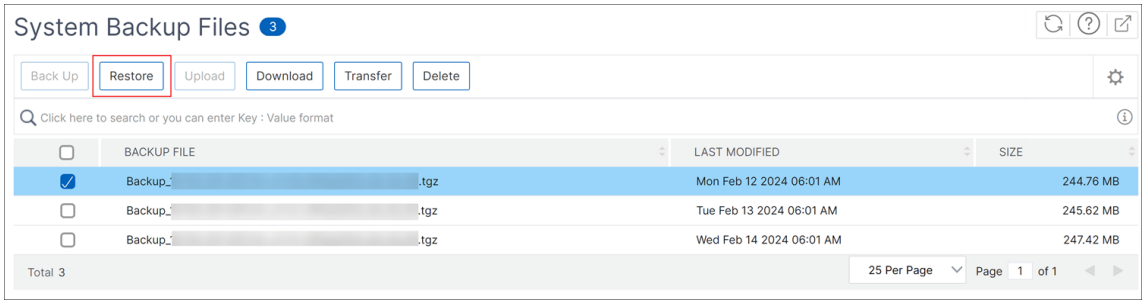
Wenn Sie die Citrix ADM Konfiguration aus einer zuvor gesicherten Datei wiederherstellen, wird die Backupdatei durch den Wiederherstellungsvorgang aufgehoben und anschließend die Konfiguration wiederhergestellt. Der Wiederherstellungsvorgang löscht die vorhandene Konfiguration und ersetzt sie durch die Konfiguration in der Sicherungsdatei.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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** > **Erweiterte Einstellungen** > **Sicherungsdateien**.
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** > **Erweiterte Einstellungen** > **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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

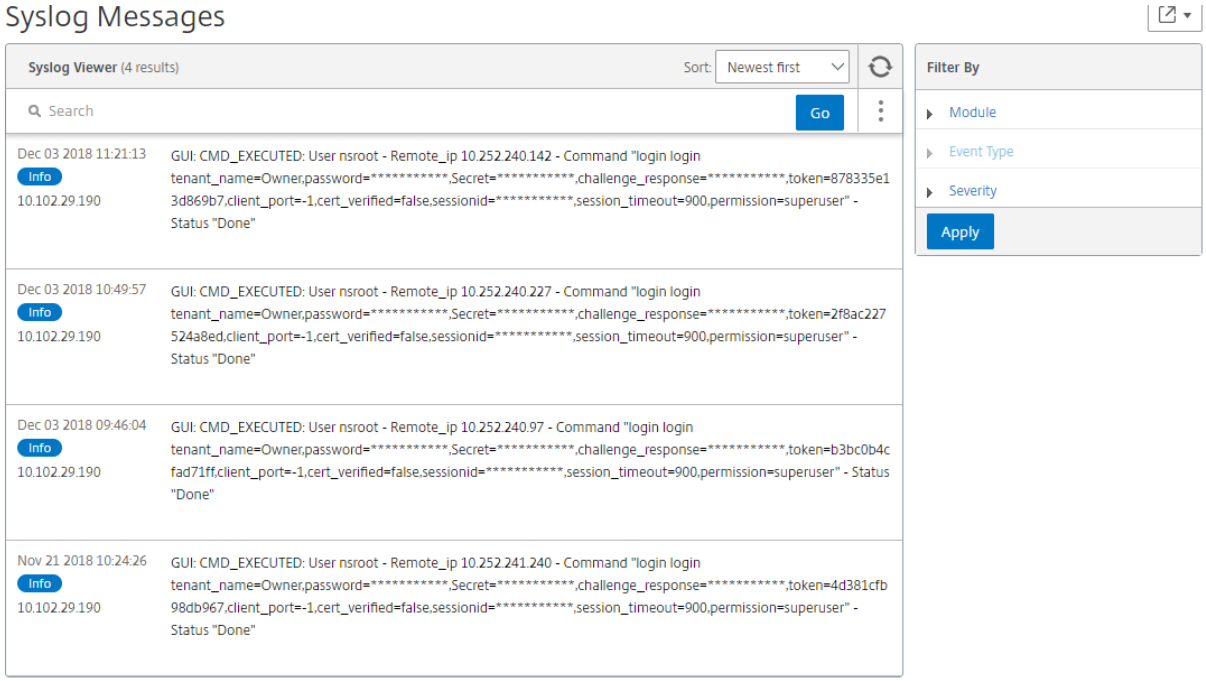
So zeigen Sie Syslog-Meldungen auf Citrix ADM an:

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Sicherheit-snetzwerkprotokolle, 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

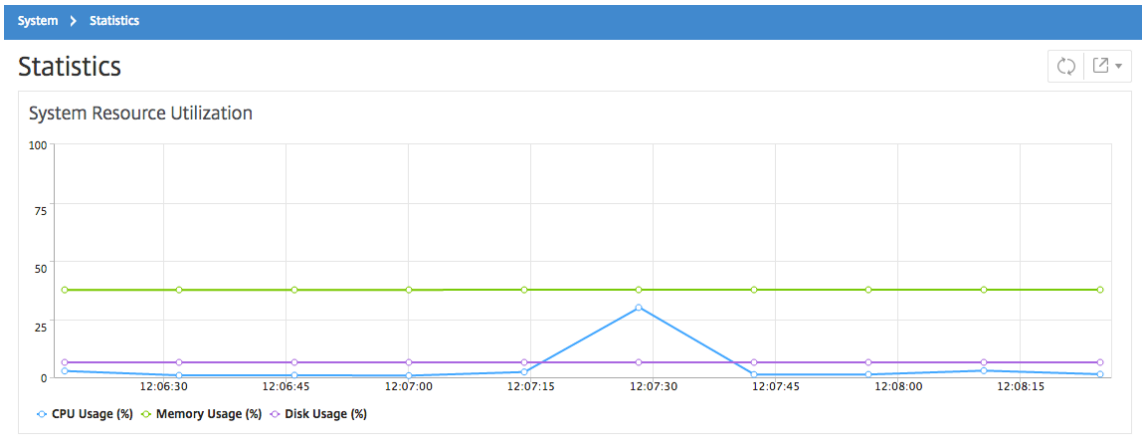
CPU-, Arbeitsspeicher- und Datenträgernutzung überwachen

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.

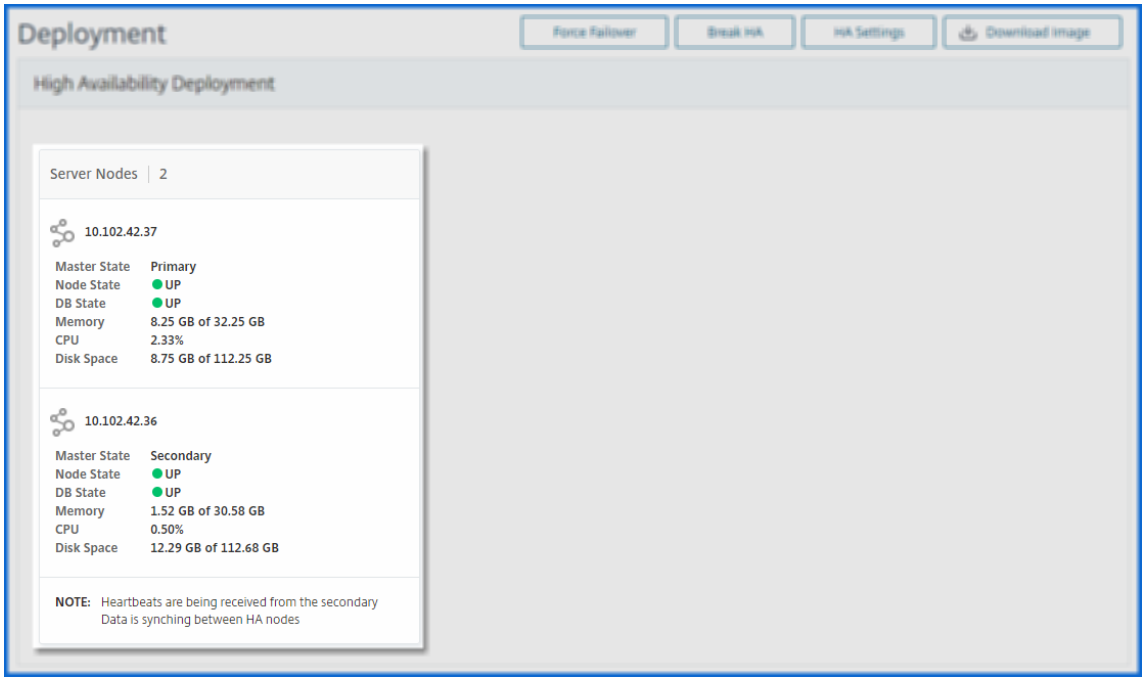
So überwachen Sie die CPU-, Speicher- und Datenträgernutzung:

- **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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Konfigurieren der Einstellungen für die Systembenachrichtigung

February 5, 2024

Sie können Benachrichtigungen an ausgewählte Benutzergruppen für eine Reihe von systembezogenen Funktionen senden. Diese Systemfunktionen sind in Ereigniskategorien wie SystemReboot, StatusPoll, SystemState usw. unterteilt. Sie können NetScaler Application Delivery Management (ADM) so konfigurieren, dass Sie Benachrichtigungen per E-Mail oder SMS senden. Sie müssen einen E-Mail-Server und/oder einen SMS-Gateway server (Short Message Service) konfigurieren, um E-Mail- und Textbenachrichtigungen an Benutzer zu senden.Dadurch wird sichergestellt, dass Sie über alle Aktivitäten auf Systemebene wie Benutzeranmeldung oder Systemneustart benachrichtigt werden.

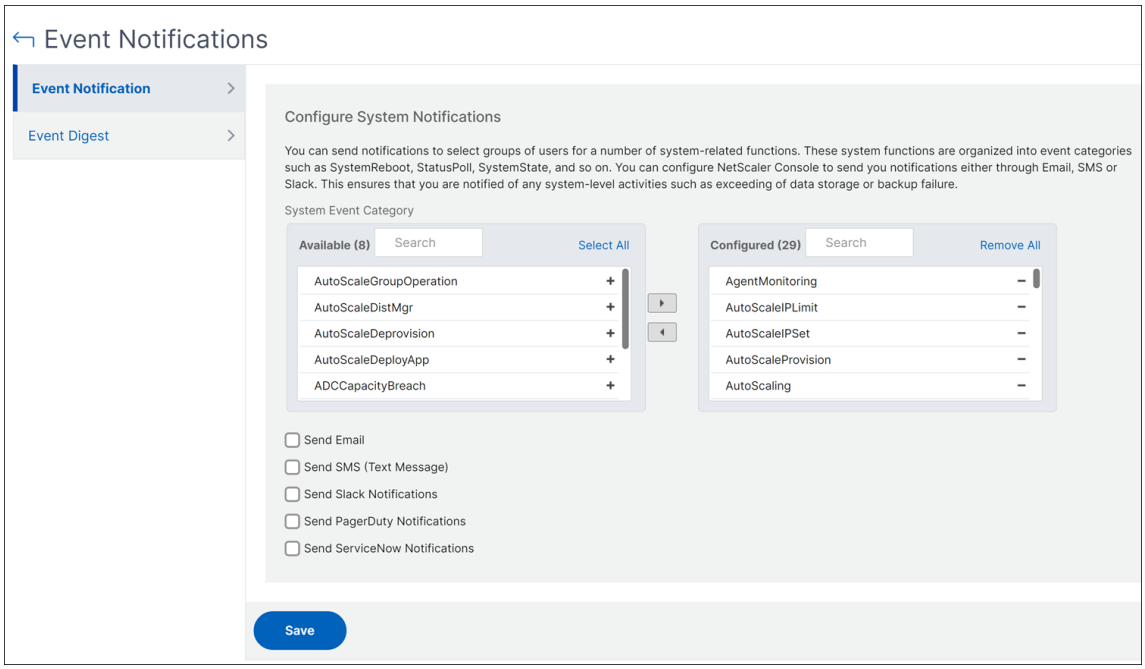
Sie können beispielsweise eine E-Mail-Benachrichtigung an zwei Benutzer senden, wenn jemand versucht, sich mit der CLI bei Citrix ADM anzumelden und der Anmeldeversuch fehlschlägt. Sie müssen die Systembenachrichtigung konfigurieren, indem Sie die Kategorie UserLogin auswählen und entweder einen E-Mail-Benachrichtigungsserver erstellen oder eine vorhandene E-Mail-Verteilerliste auswählen, an die die Benachrichtigung gesendet werden soll.

So konfigurieren Sie die Einstellungen für die Systembenachrichtigung in Citrix ADM:

1. Navigieren Sie zu **System** > **Benachrichtigungen**. Klicken Sie unter**Einstellungen**auf **Benachrichtigungseinstellungen ändern**.

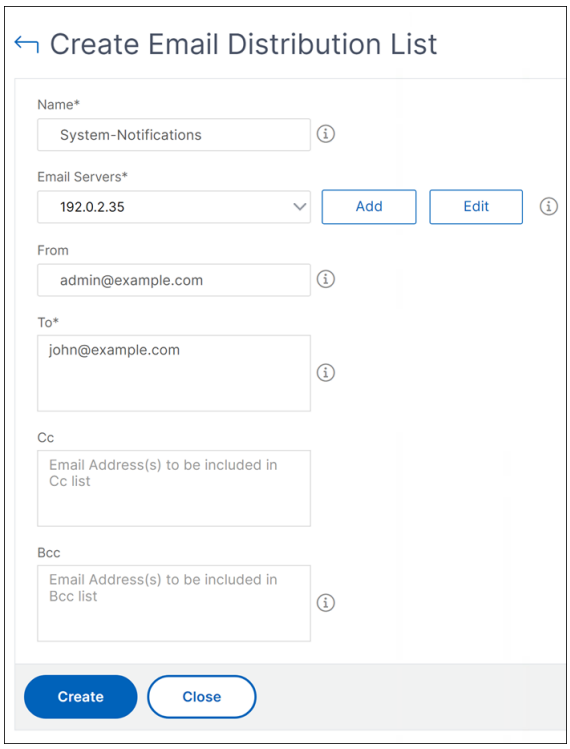
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Wählen Sie auf der Seite **Einstellungen für Systembenachrichtigungen konfigurieren** unter**Kategorie**eine Kategorie wie**UserLogin**aus.



3. Wählen Sie **E-Mail senden**aus, und wählen Sie entweder eine E-Mail-Verteilung aus der Dropdown-Liste aus, oder klicken Sie auf das Symbol "**+**", um eine neue E-Mail-Verteilerliste zu erstellen, wie in der folgenden Abbildung dargestellt. Wenn Sie Textbenachrichtigungen senden möchten, wählen Sie **SMS senden (Textnachricht)**und erstellen Sie eine SMS-Verteilerliste, indem Sie auf das Symbol „**+**"klicken und SMS-Serverdetails angeben.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Nachdem die Benachrichtigungen für bestimmte Ereigniskategorien festgelegt wurden, wird bei jedem Ereignis, das zu dieser Kategorie gehört, eine Benachrichtigung per E-Mail oder SMS an die Empfänger gesendet. In diesem Beispiel wird eine E-Mail-Benachrichtigung angezeigt, wenn sich ein Benutzer nicht mit der Befehlszeilenschnittstelle bei Citrix ADM anmelden kann.

Time: Mon, 24 Apr 2017 14:32:12 GMT
Category: UserLogin
Severity: Major
Information: Invalid "CLI" login for user nsroot from client IP Address 10.252.240.56
Action: No Action Required.

Systembenachrichtigungen werden für die folgenden Ereignisse gesendet:

Kategorie	Ursache
BackupFailure	Das System-Backup schlägt fehl
DataStorageExceeded	Der Datenbankspeicher überschreitet das in der Lizenz angegebene Limit
DeviceBackupFailure	Das Instanzbackup schlägt fehl

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Kategorie	Ursache
HAMonitoring	Das System-HA-Failover tritt auf, keine Heartbeats vom Peer-Knoten und Datenbank-Synchronisierungsfehler tritt auf
HealthMontoring	Die CPU-, RAM- oder Festplattenauslastung überschreitet den Schwellenwert
LicensePool	Der Lizenzpool überschreitet den Schwellenwert
Lizenzen	Lizenz schlägt fehl, wenn sie angewendet wird
PasswordRecovery	Die Kennwortwiederherstellung schlägt fehl oder ist erfolgreich
PerfCounterThresholdHigh	Der Wert des Leistungszählers überschreitet den Grenzwert
PerfCounterThresholdNormal	Der Wert des Leistungszählers ist normal
PolicyFailed	Jede der Systemrichtlinien schlägt fehl
RemoteDeviceBackupFailure	Das Backup der Remote-Instance schlägt fehl
RemoteSystemBackupFailure	Das Remote-System-Backup schlägt fehl
RemoteSystemBackupNormal	Das Remote-System-Backup ist erfolgreich
SSLCertThreshold	Der Schwellenwert für ein Zertifikat wurde überschritten
StatusPoll	Jede Änderung des Status einer Instanz
SubSystemState	Jede Änderung des Zustands des Teilsystems
SystemReboot	Das System wird neu gestartet
SystemState	Jede Änderung des Zustands des Systems
TrapConfigFailure	Beim Hinzufügen eines SNMP-Traps zu einer Instance tritt ein Fehler auf
UserLogin	Benutzerauthentifizierung schlägt fehl

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 be-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

heben. Das Archiv ist eine TAR-Datei, die Sie an das technische Support-Team senden können.

> **Hinweis**
>
> Für Citrix ADM -Server in einem Hochverfügbarkeitsmodus können Sie eine technische Supportdatei von einem der Server 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 sollen. 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 ein:

      /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-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

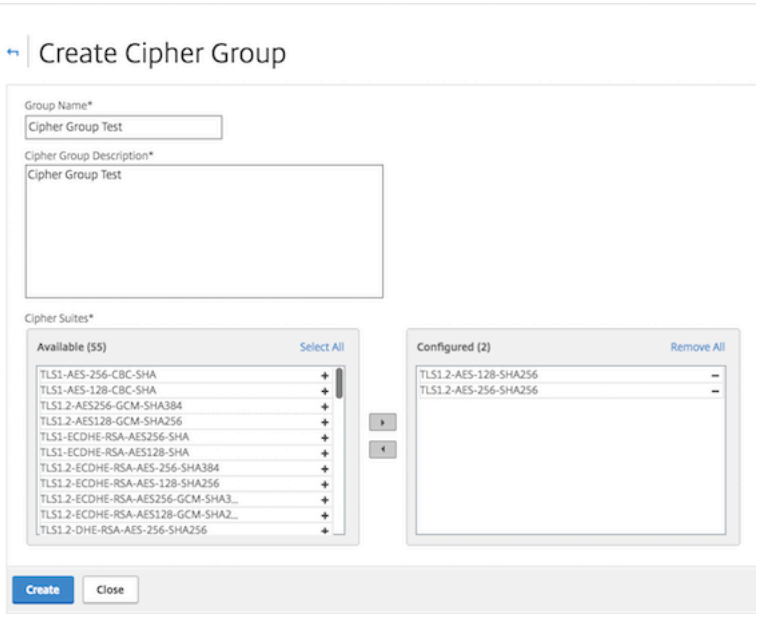
February 5, 2024

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 umfasst ein Protokoll, einen Schlüsselaustauschalgorithmus (Kx), einen Authentifizierungsalgorithmus (Au), einen Verschlüsselungsalgorithmus (Enc) und einen Nachrichtenauthentifizierungscode-Algorithmus (Mac).

So fügen Sie eine Verschlüsselungsgruppe in NetScaler ADM hinzu:

1. Navigieren Sie zu **System** > **Verschlüsselungsgruppen**, und klicken Sie dann auf **Hinzufügen**.
2. 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.
3. Klicken Sie auf **Erstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



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. 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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**.

So erstellen Sie einen SNMP-Benutzer:

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 sollten Systemalarme konfigurieren, um sicherzustellen, dass Sie kritische oder schwerwiegende Systemprobleme kennen. Sie möchten z. B. benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

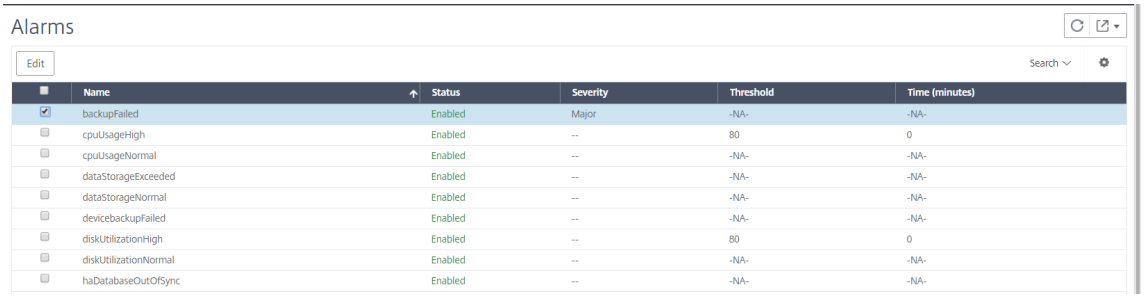
Sie können den Schweregrad eines Alarms zuweisen oder ändern. Die Schweregrade, die Sie zuweisen können, sind Kritisch, Groß, Geringfügig, Warnung und Informativ.

Betrachten Sie ein Szenario, in dem Sie überwachen möchten, wenn ein fehlgeschlagener Backupversuch vorliegt. Sie können den Alarm "BackupFailed"aktivieren und ihm einen Schweregrad zuweisen, z. B. "Major". 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** > **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**.

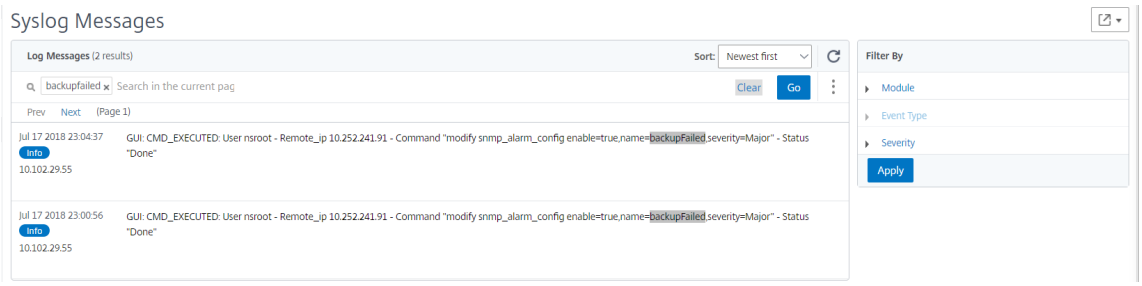
> **Hinweis**
>
> Für einige Alarme können Sie keinen Schwellenwert festlegen.
> Wenn der Alarm ausgelöst wird, können Sie das generierte Ereignis als Syslog-Meldung anzeigen.

So zeigen Sie das vom BackupFailed-Alarm mithilfe von Citrix ADM generierte Ereignis an:

1. Navigieren Sie zu**System** > **Überwachung**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

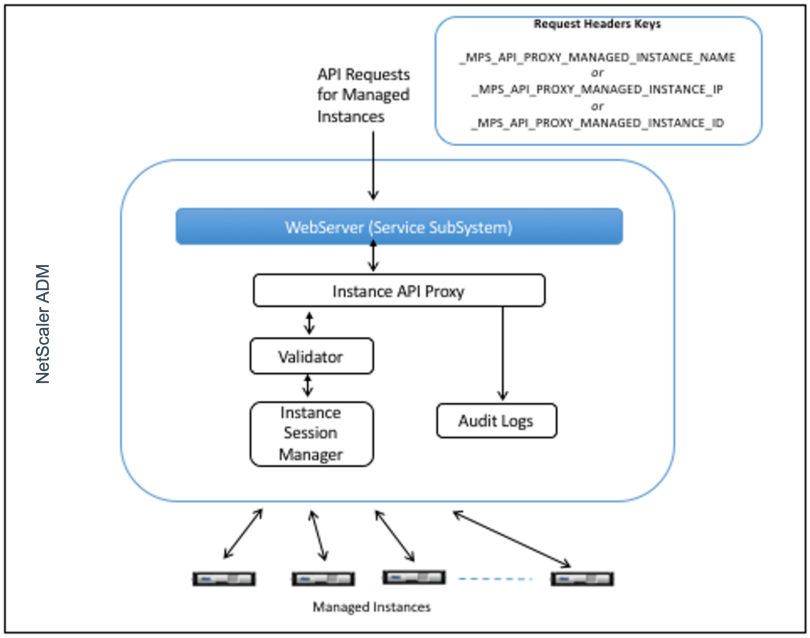
So funktioniert Citrix ADM als API-Proxyserver

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:

- _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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Wenn die API-Anforderung gültig ist und an die verwaltete Instanz weitergeleitet werden kann, identifiziert Citrix ADM eine Sitzung, die vom Instanzsitzungsmanager verwaltet wird, und sendet die Anforderung dann an die verwaltete Instanz.

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/v2/config/login HTTP/1.1
    Host: 192.0.2.5
    Content-Type: application/json
    Accept: application/json
    Cache-Control: no-cache

    {

        "login":
        {

            "username":"******",
            "password":"*******"
         }

     }

<!--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",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  "username": "***********",
  "tenant_name": "Owner",
  "resourceName": "******",
  "login": [
    {

      "tenant_name": "Owner",
      "permission": "superuser",
      "session_timeout": "36000",
      "challenge_token": "",
      "username": "",
      "login_type": "",
      "challenge": "",
      "client_ip": "",
      "client_port": "-1",
      "cert_verified": "false",
      "sessionid": "##
    D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
      "token": "b2f3f935e93db6a"
     }

  ]

 }

<!--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:

```
    GET /nitro/v1/stat/lbvserver HTTP/1.1
    Host: 192.0.2.5
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    Accept: application/json
    Cache-Control: no-cache
<!--NeedCopy-->
```

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 HTTP/1.1
    Host: 192.0.2.5
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
5      Content-Type: application/json
6      Accept: application/json
7      Cache-Control: no-cache
8
9      {
10   "lbvserver":{
11   "name":"sample_lbvserver","servicetype":"HTTP","ipv46":"10.102.1.11","
        port":"80" }
12    }
13
14 <!--NeedCopy-->
```

Beispiel 3: Ändern Sie einen virtuellen Lastausgleichsserver

Der Client muss NetScaler ADM eine API-Anforderung mit folgendem Formular senden:

```
1      PUT /nitro/v1/config/lbvserver HTTP/1.1
2      Host: 192.0.2.5
3      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5      Content-Type: application/json
6      Accept: application/json
7      Cache-Control: no-cache
8
9      {
10   "lbvserver":{
11   "name":"sample_lbvserver","appflowlog":"DISABLED" }
12    }
13
14 <!--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 HTTP/1.1
2      Host: 192.0.2.5
3      Cookie: SESSID=##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5      Cache-Control: no-cache
6
7  <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Muss ich den virtuellen EUEM-Kanal auf Citrix Gateway-Instanzen 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 verbleibenden HDX Insight Daten weiterhin in NetScaler ADM angezeigt.

Ein virtueller EUEM-Kanal ist ein Standarddienst, der auf Citrix Virtual Desktop-Anwendungen (VDA) ausgeführt wird. Wenn es nicht ausgeführt wird, starten Sie den Prozess “Citrix End User Experience Monitoring”in VDA-Diensten.

Wie aktiviere ich NetScaler ADM, um Webanwendungs- und Virtual-Desktop-Datenverkehr zu überwachen?

1. Navigieren Sie zu **Infrastruktur** > **Instanzen** und wählen Sie die Citrix Application Delivery Controller (Citrix ADC) -Instanz aus, auf der Sie Analysen aktivieren möchten.
2. Wählen Sie in der Dropdownliste **Aktion** die Option **Insight aktivieren/deaktivieren** aus.
3. Wählen Sie auf der Seite **Configure Insight** , die geöffnet wird, alle virtuellen Server aus, auf denen Sie Analytics aktivieren möchten, und klicken Sie auf **AppFlow aktivieren** . Weitere Informationen finden Sie unter So aktivieren Sie Analytics für Instanzen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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. Sie müssen zunächst Analysen auf den virtuellen Servern aktivieren, die in Citrix ADC Instanzen gehostet werden, die von Citrix ADM verwaltet werden. Weitere Informationen finden Sie unter So aktivieren Sie Analytics auf Instances .

Muss ich auf die einzelne Citrix ADC Appliance zugreifen, 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 füge ich eine zusätzliche Festplatte an Citrix ADM an?

So stellen Sie einen zusätzliche Datenträger für NetScaler ADM bereit:

1. Fahren Sie die virtuelle NetScaler ADM Maschine herunter.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Stellen Sie im Hypervisor einen zusätzlichen Datenträger mit der erforderlichen Datenträgergröße für die virtuellen 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 Festplattenspeicher von 200 GB anstelle von 80 GB anhängen. Neu zugeordnete 200 GB Speicherplatz werden zum Speichern von Datenbankdaten und NetScaler ADM Protokolldateien verwendet. Der vorhandene 120-GB-Festplattenspeicher 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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Warum müssen wir externe Authentifizierungsserver kaskadieren?

Kaskadierte externe Authentifizierungsserver bieten eine unterbrechungsfreie Authentifizierungsverarbeitung und ermöglichen legitimen Benutzern den Zugriff, wenn ein Authentifizierungsserver ausfällt. 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 könnten die externen Server nicht mehr erreichbar sein, oder die Anmeldeinformationen eines neuen Benutzers wurden möglicherweise auf 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 Extraktion externer 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix ADM an, erstellen Sie manuell dieselben Gruppeninformationen in Citrix ADM und weisen Sie diesen Gruppen Berechtigungen 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 Citrix ADM zum Löschen von Zertifikaten aus Citrix 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**.

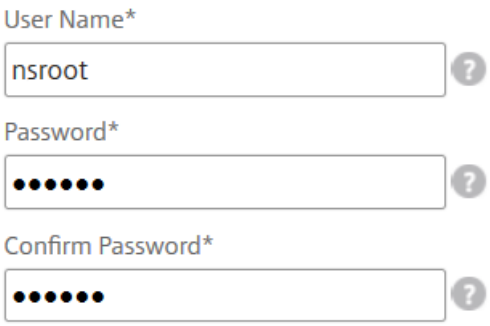
   Die Seite “Benutzer”wird angezeigt.

2. Wählen Sie den Benutzernamen **nsroot** aus, und klicken Sie auf **Bearbeiten**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Wie verhält es sich bei einem HA-Paar, wenn das Kennwort im primären Knoten geändert wird und die Option HA-Paar unterbrechen später ausgewählt wird?

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Unterstützt Citrix ADM zusätzliche Festplatten?

Ja. Bei einer Neuinstallation des NetScaler ADM HA-Paars werden standardmäßig 120 GB Speicher zugewiesen. Für mehr als 120 GB Speicher können Sie eine zusätzliche Festplatte für maximal 3 TB Speicher hinzufügen. Das Hinzufügen von mehr als einer zusätzlichen Festplatte 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sie können Instanzen entweder beim ersten Einrichten des NetScaler ADM -Servers oder zu einem späteren Zeitpunkt hinzufügen.

Was ist ein Instanzprofil?

Ein Instanzprofil wird von Citrix ADM verwendet, um auf eine bestimmte 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 > **Instances** > **NetScaler VPX,** wählen Sie die Instanzen aus, die Sie erneut erkennen möchten, und klicken Sie in der Dropdownliste **Aktion** auf **Rediscover**. Weitere Informationen finden Sie unter Wiederentdecken mehrerer VPX-Instanzen.

Kann NetScaler ADM auf Citrix SDX installiert werden?

Nein

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 mehr 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 Citrix ADC-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 SNMP-Einstellungen sichern. Wenn NetScaler ADM jemals instabil wird, können Sie die gesicherten Dateien verwenden, um NetScaler ADM in einen stabilen Zustand wiederherzustellen.

Um die Citrix ADM-Konfiguration zu sichern und wiederherzustellen, navigieren Sie zu **System** >**Erweiterte Einstellungen** > **Backupdateien** und klicken Sie auf **Backup** oder **Wiederherstellen**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Weitere Informationen finden Sie unter Sichern und Wiederherstellen der Konfiguration auf Citrix 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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) Citrix ADM Knoten prüft, ob der zuvor aktive Knoten als AppFlow Collector oder Syslog-Server konfiguriert wurde. Falls dies der Fall ist, fügt der neue primäre Knoten den

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

AppFlow Collector oder Syslog-Serverdetails zu den an die Instanzen gesendeten Informationen 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?

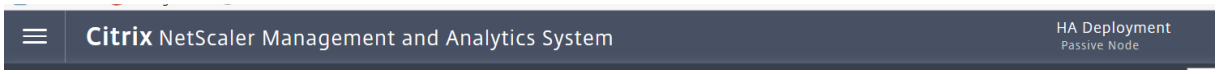
Alle NetScaler ADC-Instanzen werden vom primären NetScaler ADM Knoten verwaltet.

Wie werden virtuelle Serverlizenzen im Falle eines Citrix ADM HA-Failovers verwaltet?

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. Die Lizenzen müssen bis zum Ende der Nachfrist erneut auf der neuen Primärdatenbank beantragt werden. 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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/

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).