Citrix SD-WAN Center 11

Machine translated content

Disclaimer

Contents

Systemanforderungen und Installation

February 16, 2022

Stellen Sie vor der Installation von Citrix SD-WAN Center auf einer VM sicher, dass Sie die Hardware- und Softwareanforderungen kennen und die Voraussetzungen erfüllt haben müssen.

> **Hinweis**
>
> Die Systemanforderungen gelten sowohl für ein einzelnes Netzwerk als auch für ein mutliregionales Netzwerk.

Hardwareanforderungen

Citrix SD-WAN Center verfügt über die folgenden Hardwareanforderungen.

Prozessor

- 4 Core, 3 GHz (oder gleichwertiger) Prozessor oder besser für einen Server, der bis zu 64 Standorte verwaltet.
- 8 Core, 3 GHz (oder gleichwertiger) Prozessor oder besser für einen Server, der bis zu 128 Standorte verwaltet.
- 16 Core, 3 GHz (oder gleichwertiger) Prozessor oder besser für einen Server, der bis zu 256 Standorte verwaltet.
- 32 Kerne, 3 GHz (oder gleichwertiger) Prozessor oder besser für einen Server, der bis zu 550 Standorte verwaltet.

Speicher

- Für eine VM, die bis zu 64 Standorte verwaltet, wird dringend empfohlen, mindestens 8 GB RAM.
- Für eine VM, die bis zu 128 Standorte verwaltet, wird dringend empfohlen, mindestens 16 GB RAM.
- Für eine VM, die bis zu 256 Standorte verwaltet, wird dringend empfohlen, mindestens 32 GB RAM.
- Für eine VM, die bis zu 550 Standorte verwaltet, wird dringend empfohlen, mindestens 32 GB RAM.

Erforderlicher Speicherplatz

Die folgende Tabelle enthält einige Richtlinien zum Bestimmen der Anforderungen an den Speicherplatz für den Citrix SD-WAN Center-Datenspeicher. Verwenden Sie Direktzugriffsspeicher mit SSD mit 5000 bis 10000 IOPS.

Geschätzter Speicherplatzbedarf

# Client-Sites	Durchschnittliche Anzahl an WAN-Links pro Standort	Durchschnittliche Anzahl Intranet-/Internet-Dienste pro Standort	Durchschnittliche Anzahl virtueller Pfade pro Site	Datenbankgröße (TB) für 1 Jahr
32	2	2	2	1,2 T
32	4	4	4	1,8 T
32	8	8	8	5,3 T
64	2	2	2	1,5 T
64	4	4	4	2,6 T
64	8	8	8	9,6 T
96	2	2	2	1,8 T
96	4	4	4	3,3 T
96	8	8	8	14,0T
128	2	2	2	2,0 T
128	4	4	4	4,1 T
128	8	8	8	18,0T
192	2	2	2	2,6 T
192	4	4	4	5,6 T
192	8	8	8	27,0T
256	2	2	2	3,0 T
256	4	4	4	7,2 T
256	8	8	8	35,0T
550	2	2	2	15,9 T
550	4	4	4	41,9 T
550	8	8	8	195,6 T

Netzwerkbandbreite

Die folgende Tabelle enthält einige Richtlinien zum Bestimmen der Netzwerkbandbreitenanforderungen für die Citrix SD-WAN Center VM.

Geschätzte Anforderungen an Netzwerkbandbreite

# Client-Sites	Durchschnittliche # WAN-Links	Durchschnittliche Anzahl virtueller Pfade pro Site	Gesamte VWAN-Daten pro 5-Minuten-Umfrage (MB)	Zu konfigurierende Bandbreitenrate pro 5-Minuten-Umfrage (Kbit/s)
32	2	2	1.2	Standard 1000
32	4	4	3.6	Standard 1000
32	8	8	20.0	Standard 1000
64	2	2	2.3	Standard 1000
64	4	4	7.2	Standard 1000
64	8	8	40.0	2000
96	2	2	3,5	Standard 1000
96	4	4	10.8	Standard 1000
96	8	8	60.0	3000
128	2	2	4.6	Standard 1000
128	4	4	14.4	Standard 1000
128	8	8	80.0	4000
192	2	2	6.9	Standard 1000
192	4	4	21,6	2000
192	8	8	120.0	6000
256	2	2	9.2	Standard 1000
256	4	4	28,8	2000
256	8	8	160	10000
550	2	2	34,0	2000
550	4	4	89,3	6000
550	8	8	415.7	24000

Software

Citrix SD-WAN Center VPX kann auf folgenden Plattformen konfiguriert werden:

Hypervisor

- VMware ESXi-Server Version 6.5
- Citrix XenServer 6.5 oder höher.
- Microsoft Hyper-V 2012 R2 oder höher.

Cloud-Plattform

- Microsoft Azure
- Amazon Web Services

Browser müssen Cookies aktiviert und JavaScript installiert und aktiviert haben.

Die Citrix SD-WAN Center Webschnittstelle wird von den folgenden Browsern unterstützt:

- Google Chrome 40.0+
- Microsoft Internet Explorer 11 +
- Mozilla Firefox 41.0+

Voraussetzungen

Im Folgenden sind die Voraussetzungen für die Installation und Bereitstellung von Citrix SD-WAN Center aufgeführt:

- Der SD-WAN Master Control Node (MCN) und die vorhandenen Client-Knoten müssen auf die neueste Citrix SD-WAN-Softwareversion aktualisiert werden.
- Es wird empfohlen, einen DHCP-Server im SD-WAN-Netzwerk zur Verfügung zu stellen und zu konfigurieren.
- Sie müssen über die Installationsdateien für Citrix SD-WAN Center verfügen.

> **Hinweis**
>
> Sie können keine Software von Drittanbietern in Citrix SD-WAN Center anpassen oder installieren. Sie können jedoch die vCPU, den Arbeitsspeicher und die Speichereinstellungen ändern.

Descargar de Citrix SD-WAN Center software

Laden Sie die Softwareinstallationsdateien der Citrix SD-WAN Center Management Console für das erforderliche Release und die erforderliche Plattform von der Downloads-Seite herunter .

Die Installationsdateien für Citrix SD-WAN Center verwenden die folgende Namenskonvention:

ctx-sdwc-version_number-platform.extension

- *version_number* ist die Versionsnummer der Citrix SD-WAN Center.
- *platform* ist der Plattformtyp, Hypervisor oder Cloud-Plattformname.
- *extension* ist die Erweiterung der Installationsdatei.

Plattform	Dateierweiterung
Citrix XenServer	XVA
VMware ESXi	-vmware.ova
Microsoft Hyper-V	-hyperv.vhd.zip
Microsoft Azure	-azure.vhd.zip

Sammeln der Installations- und Konfigurationsinformationen für Citrix SD-WAN Center

Dieser Abschnitt enthält eine Checkliste mit den Informationen, die Sie für die Installation und Bereitstellung von Citrix SD-WAN Center benötigen.

Sammeln oder bestimmen Sie die folgenden Informationen:

- Die IP-Adresse des ESXi-Servers, XenServer, Hyper-V-Servers oder Azure, auf dem die Citrix SD-WAN Center Virtual Machine (VM) gehostet wird.
- Ein eindeutiger Name, der der Citrix SD-WAN Center VM zugewiesen werden soll.
- Die Speichermenge, die für die Citrix SD-WAN Center-VM zugewiesen werden soll.
- Die Menge der Datenträgerkapazität, die für das virtuelle Laufwerk für die VM zugewiesen werden soll.
- Die Gateway-IP-Adresse, die das Citrix SD-WAN Center für die Kommunikation mit externen Netzwerken verwendet.
- Die Subnetzmaske für das Netzwerk, in dem die Citrix SD-WAN Center-VM installiert wird.

Installieren und Konfigurieren von Citrix SD-WAN Center auf ESXi Server

April 13, 2021

Installieren des VMware vSphere-Clients

Im Folgenden finden Sie die grundlegenden Anweisungen zum Herunterladen und Installieren des VMware vSphere-Clients, mit dem Sie die Citrix SD-WAN Center Virtual Machine erstellen und bereitstellen. Weitere Informationen finden Sie in der Dokumentation zu VMware vSphere Client.

Gehen Sie folgendermaßen vor, um VMware vSphere Client herunterzuladen und zu installieren:

1. Öffnen Sie einen Browser und navigieren Sie zu dem ESXi-Server, der den vSphere-Client und die Citrix SD-WAN Center Virtual Machine-Instanz (VM) hostet.

   Die VMware ESXi-Willkommensseite wird angezeigt.

2. Klicken Sie auf den Link **vSphere Client** herunterladen, um die vSphere Client-Installationsdatei herunterzuladen.

3. Installieren Sie den vSphere Client.

   Führen Sie die heruntergeladene vSphere Client-Installationsdatei aus, und akzeptieren Sie alle Standardoptionen, wenn Sie dazu aufgefordert werden.

4. Starten Sie nach Abschluss der Installation das vSphere Client-Programm.

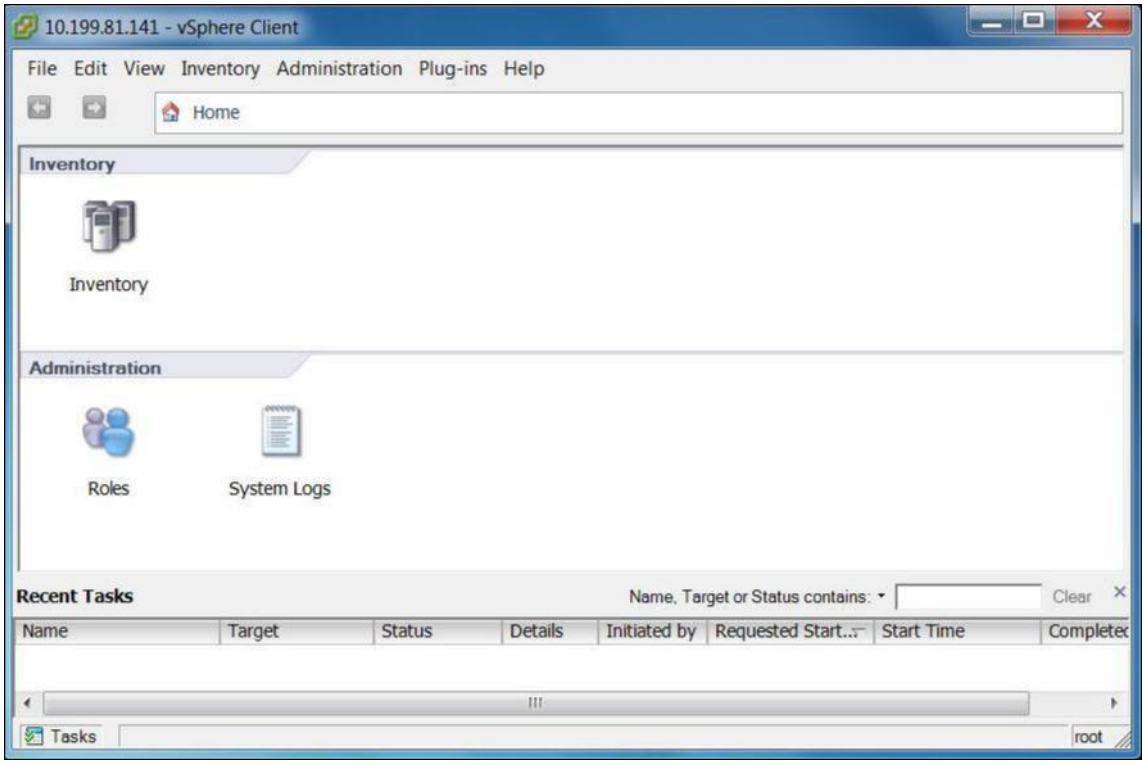
   Die VMware vSphere Client-Anmeldeseite wird angezeigt, in der Sie aufgefordert werden, die Anmeldeinformationen des ESXi-Servers einzugeben.

5. Geben Sie die Anmeldeinformationen des ESXi-Servers ein:

   - **IP Address / Name:** Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des ESXi-Servers ein, auf dem die Citrix SD-WAN Center-VM-Instanz ausgeführt wird.
   - **Benutzername**: Geben Sie den Serveradministratorkontonamen ein. Der Standardwert ist root.
   - **Kennwort**: Geben Sie das Kennwort ein, das diesem Administratorkonto zugeordnet ist.

6. Klicken Sie auf **Login**.

   Die vSphere Client-Hauptseite wird angezeigt.



Erstellen der Citrix SD-WAN Center-VM mithilfe der OVF-Vorlage

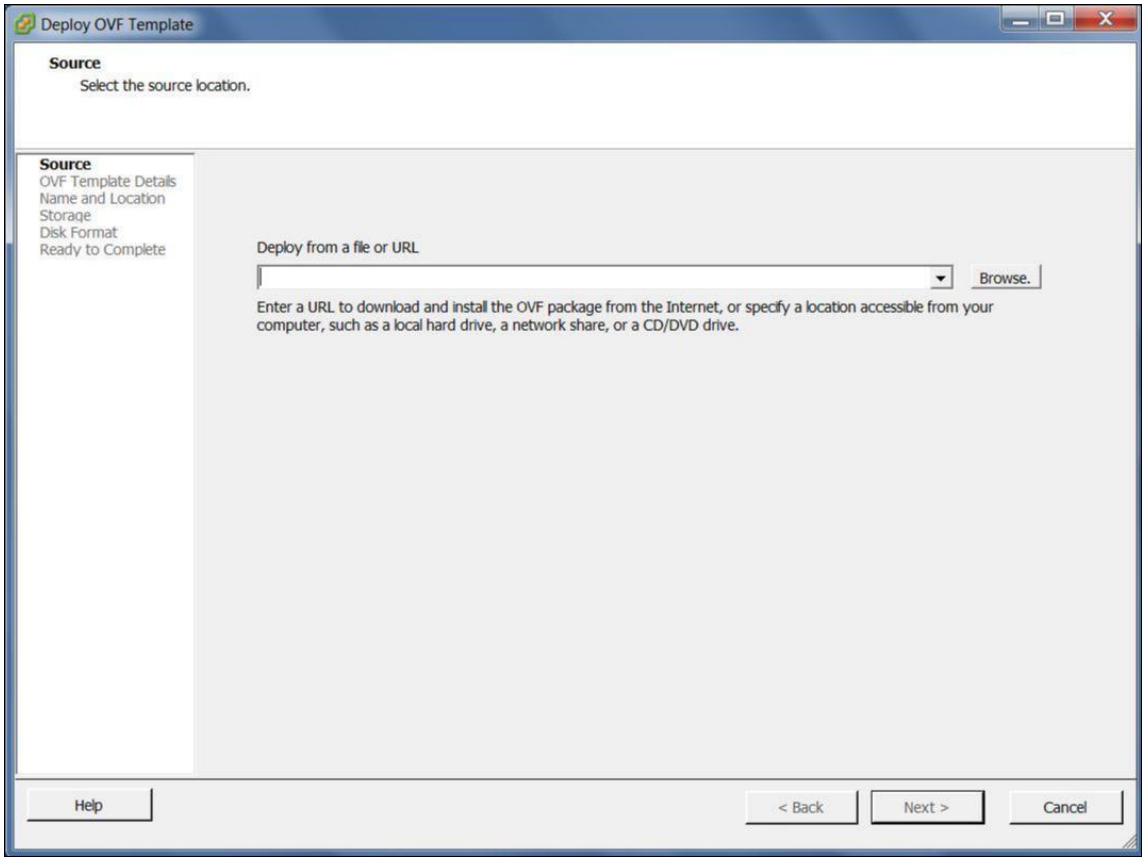
Erstellen Sie nach der Installation des VMware vSphere-Clients die virtuelle Citrix SD-WAN Center-Maschine.

1. Wenn Sie dies noch nicht getan haben, laden Sie die OVF-Vorlagendatei für Citrix SD-WAN Center (.ova-Datei) auf den lokalen PC herunter.

   Weitere Informationen finden Sie unter Systemanforderungen und Installation.

2. Klicken Sie im vSphere Client auf **Datei**, und wählen Sie dann im Dropdownmenü **OVF-Vorlage bereitstellen**aus.

   Der Assistent für die **OVF-Vorlage** wird angezeigt.

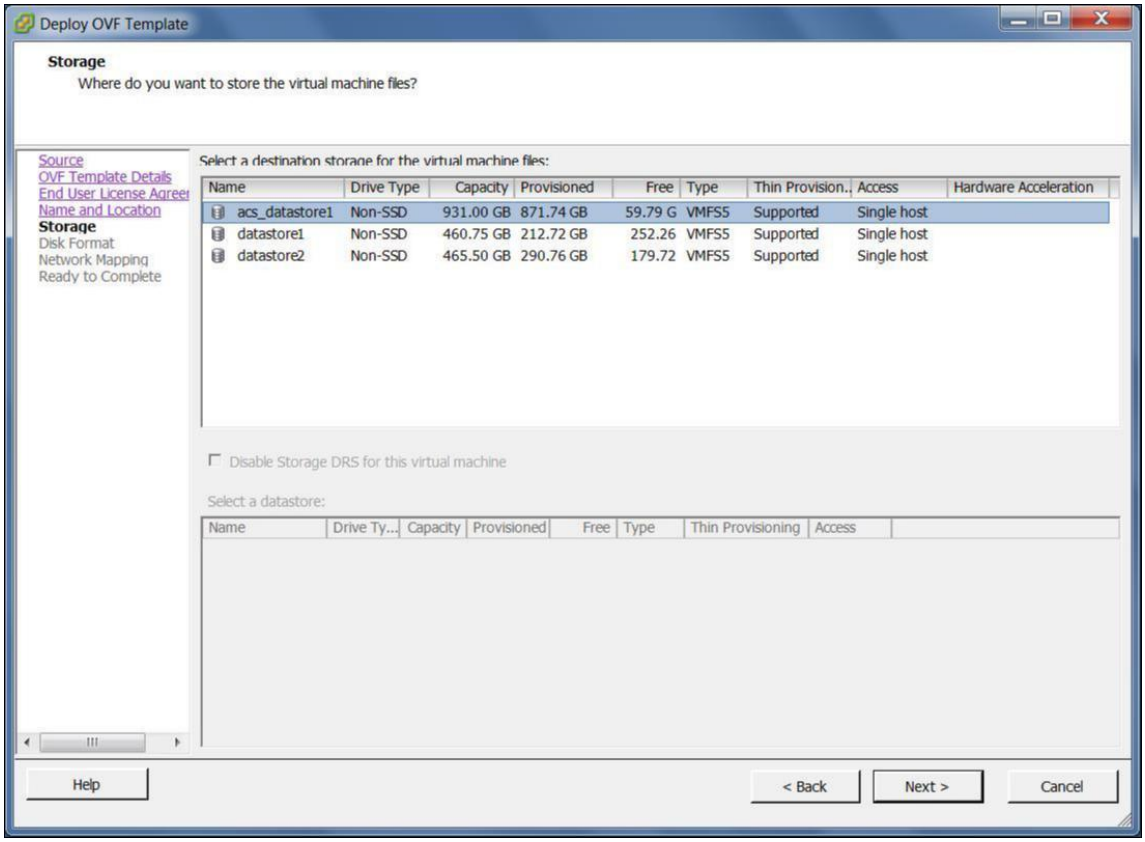


3. Klicken Sie auf **Durchsuchen**, und wählen Sie die Citrix SD-WAN Center OVF-Vorlage (.ova-Datei) aus, die Sie installieren möchten.
4. Klicken Sie auf **Weiter**.

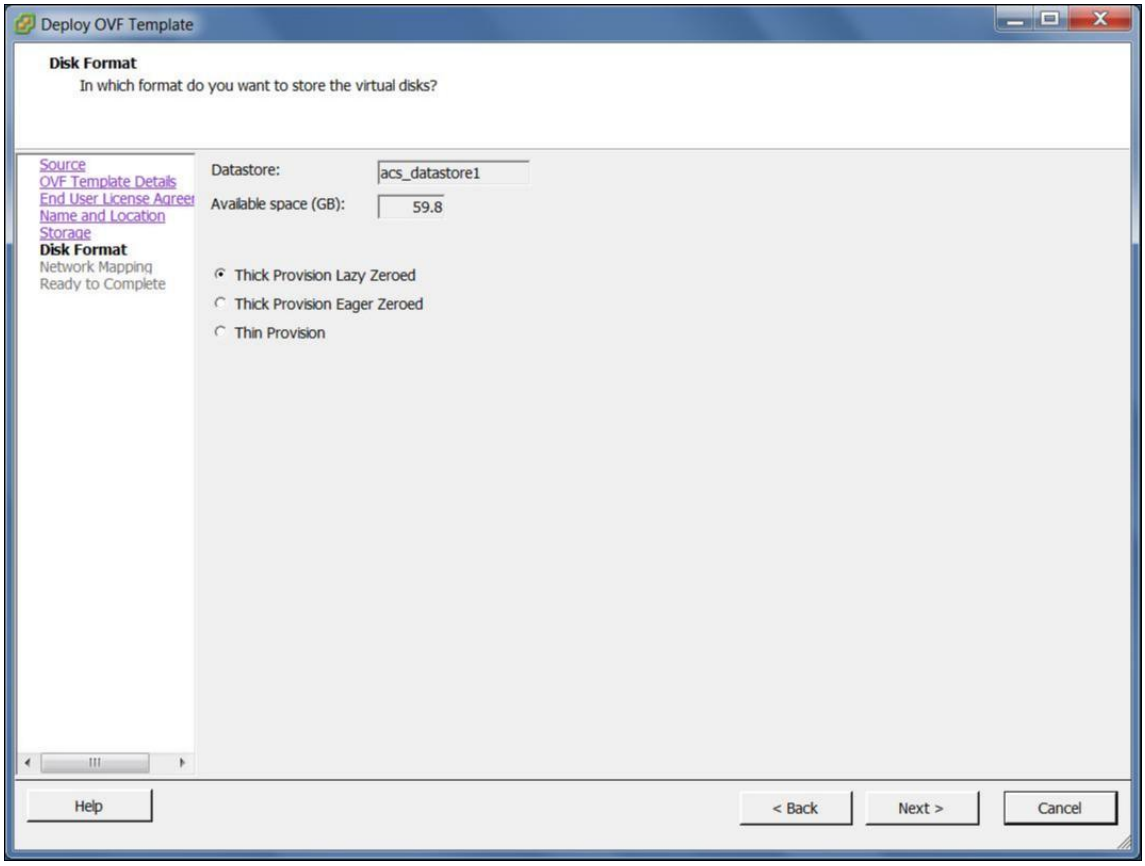
   Die ova-Datei wird importiert, und die Seite Details der OVF-Vorlage wird angezeigt.
5. Klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite Endbenutzer-Lizenzvertrag auf **Akzeptieren**, und klicken Sie dann auf **Weiter**.
7. Geben Sie auf der Seite Name und Speicherort einen eindeutigen Namen für die neue VM ein (oder übernehmen Sie den Standardwert).

   Der Name muss innerhalb des aktuellen **Inventory**-Ordners eindeutig sein und kann bis zu 80 Zeichen lang sein.
8. Klicken Sie auf **Weiter**.

   Die Seite Speicher wird angezeigt.



9. Akzeptieren Sie jetzt die Standardspeicherressource, indem Sie auf **Weiter** klicken. Sie können den Datenspeicher auch konfigurieren. Weitere Informationen finden Sie unter Hinzufügen und Konfigurieren des Datenspeichers auf dem ESXi-Server.



10. Übernehmen Sie auf der Seite Datenträgerformat die Standardeinstellungen, und klicken Sie auf **Weiter**.
11. Übernehmen Sie auf der Seite Netzwerkzuordnung den Standardwert (VM-Netzwerk), und klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite Bereit zum Abschluss auf **Fertig stellen**, um die VM zu erstellen.

    > **Hinweis**:
    >
    > Das Dekomprimieren des Datenträgerimages auf den Server kann einige Minuten dauern.

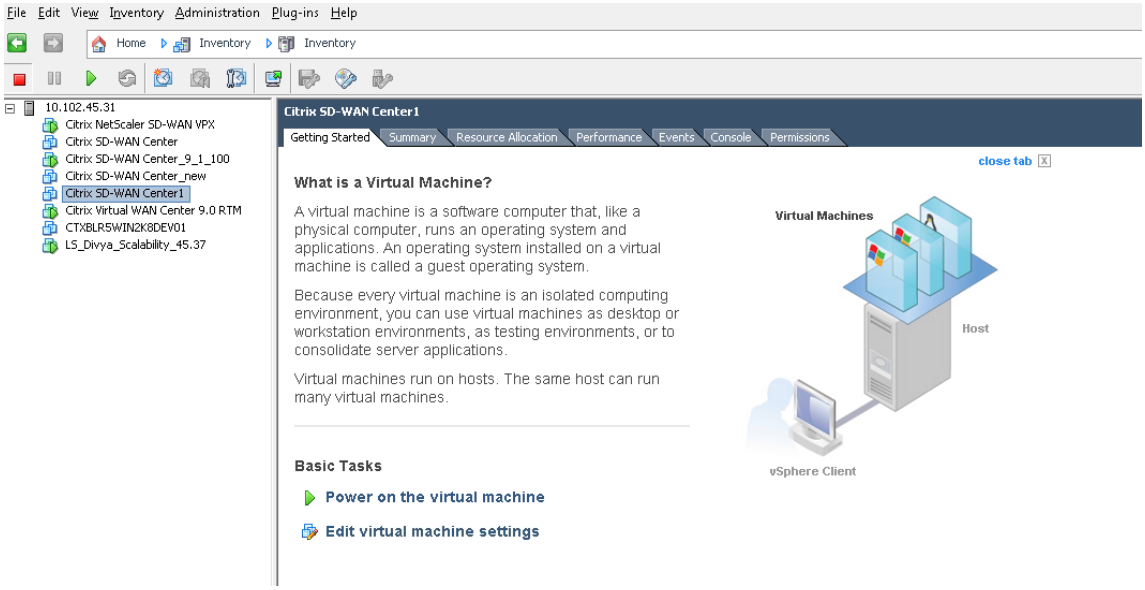
13. Klicken Sie auf **Schließen**.

Anzeigen und Aufzeichnen der Management-IP-Adresse auf dem ESXi-Server

Die Management-IP-Adresse ist die IP-Adresse der SD-WAN Center-VM. Verwenden Sie diese IP-Adresse, um sich bei der Citrix SD-WAN Center Web-Benutzeroberfläche anzumelden.

Gehen Sie folgendermaßen vor, um die Management-IP-Adresse anzuzeigen:

1. Wählen Sie auf der Seite “Inventory”des vSphere-Clients die neue Citrix SD-WAN Center-VM in der **Bestandsstruktur** (linker Fensterbereich) aus.

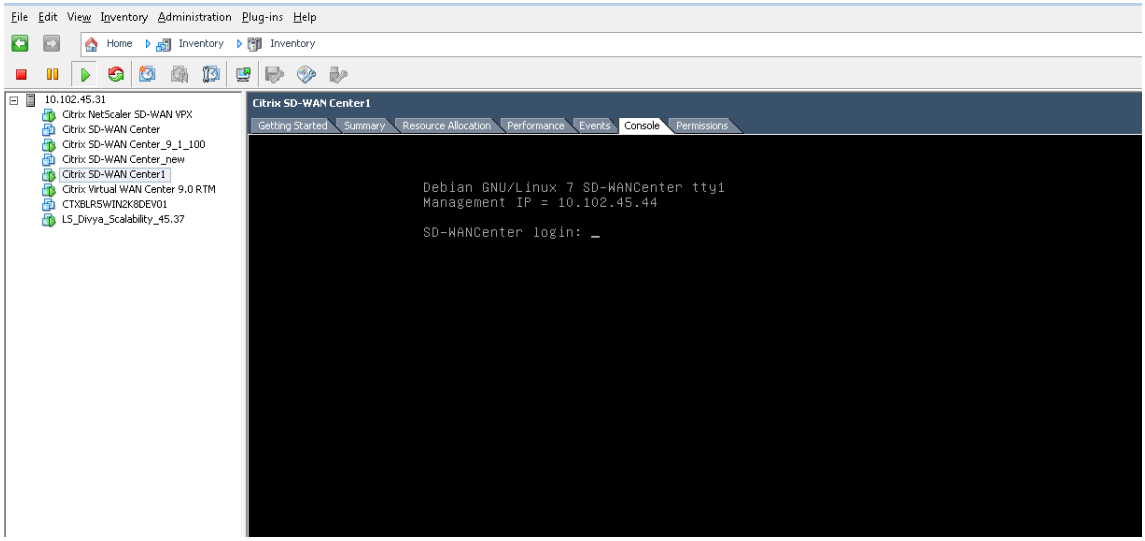


2. Klicken Sie auf der Seite Citrix SD-WAN Center unter Einfache Aufgaben auf **Virtuelle Maschine einschalten**.
3. Wählen Sie die Registerkarte **Konsole** aus, und klicken Sie dann auf eine beliebige Stelle im Konsolenbereich, um in den Konsolenmodus zu wechseln.

   Dadurch wird die Steuerung des Mauszeigers auf die VM-Konsole verschoben.

   > **Hinweis:**
   >
   > Um die Konsolensteuerung des Cursors freizugeben, drücken Sie gleichzeitig die Tasten <Strg> und <Alt>.

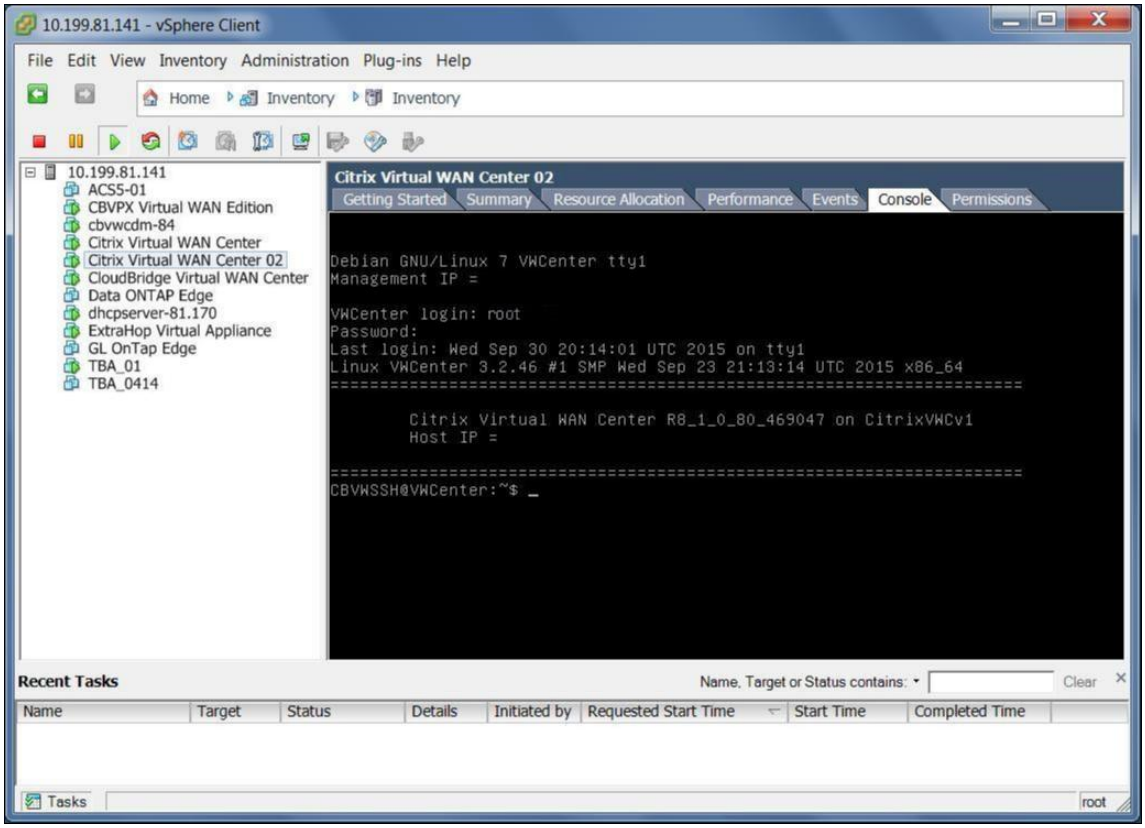
4. Drücken Sie die **Eingabetaste**, um die Anmeldeaufforderung für die Konsole anzuzeigen.



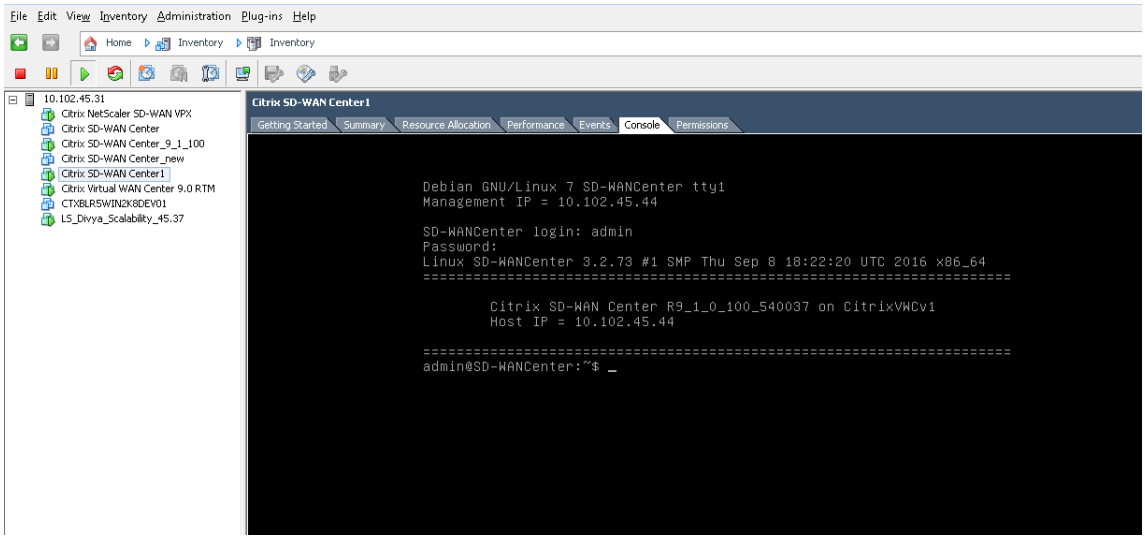
5. Melden Sie sich bei der VM-Konsole an.

Die Anmeldeinformationen für die neue Citrix SD-WAN Center-VM lauten wie folgt:

- Anmeldung: admin
- Kennwort: password



6. Zeichnen Sie die Management-IP-Adresse der Citrix SD-WAN Center VM auf, die als Host-IP-Adresse in einer Willkommensmeldung angezeigt wird, die bei der Anmeldung angezeigt wird.



> **Hinweis**
>
> Der DHCP-Server muss vorhanden und im SD-WAN-Netzwerk verfügbar sein, anderenfalls kann dieser Schritt nicht abgeschlossen werden.

Wenn der DHCP-Server nicht im SD-WAN-Netzwerk konfiguriert ist, müssen Sie manuell eine statische IP-Adresse eingeben.

So konfigurieren Sie eine statische IP-Adresse als Management-IP-Adresse:

1. Wenn die VM gestartet wird, klicken Sie auf die Registerkarte **Konsole**.
2. Melden Sie sich bei der VM an. Die Anmeldeinformationen für die neue Citrix SD-WAN Center-VM lauten wie folgt:

   Login: admin

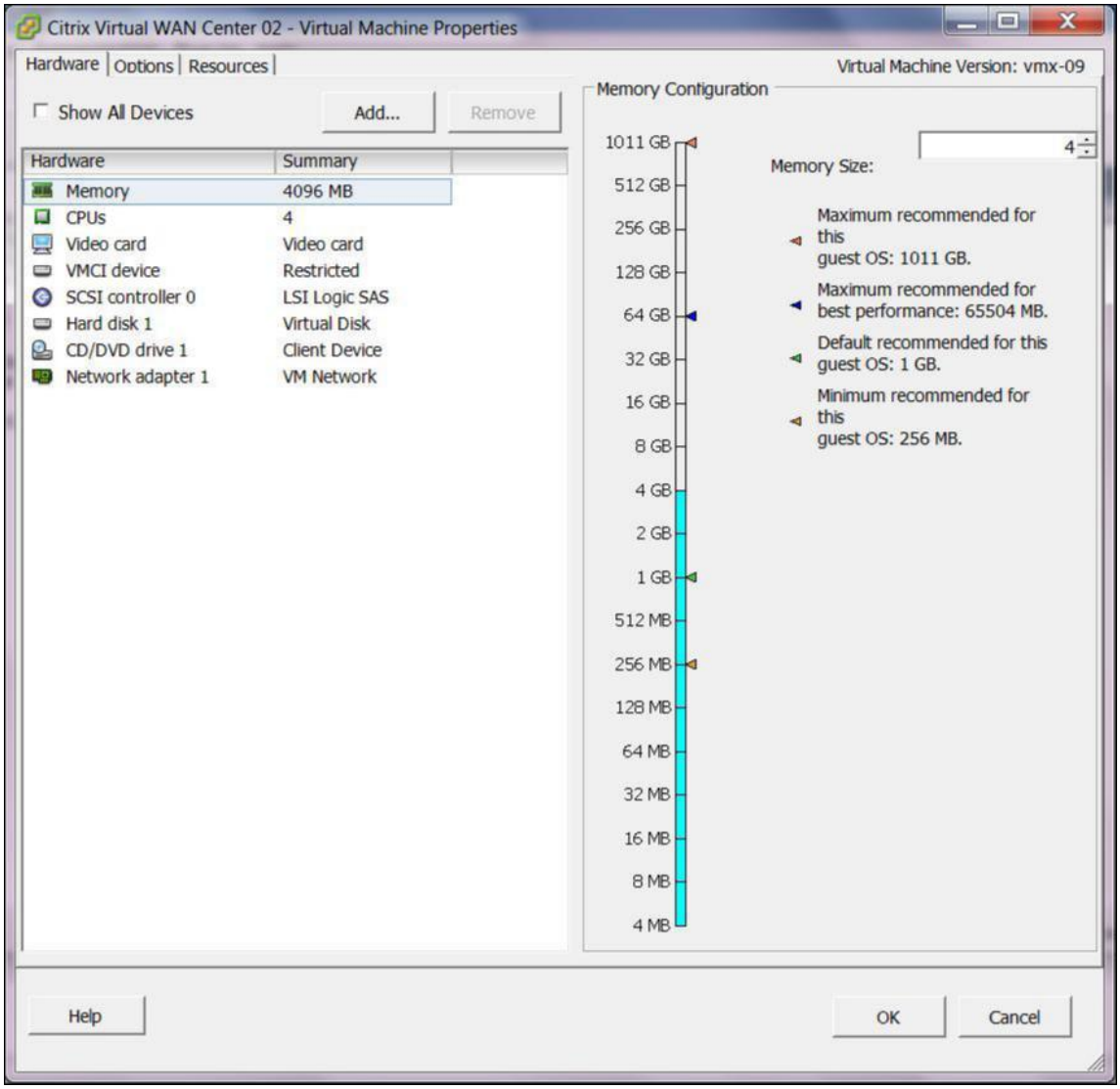
   Kennwort: password
3. Geben Sie in der Konsole den CLI-Befehl **management_ip**ein.
4. Geben Sie die Befehlssatzschnittstelle ein <ipaddress> <subnetmask> <gateway>, um Management-IP zu konfigurieren.**

Hinzufügen und Konfigurieren des Datenspeichers auf einem ESXi-Server

Sie können Datenspeicher hinzufügen und konfigurieren, um Statistiken über Citrix SD-WAN Center zu speichern.

So fügen Sie den Datenspeicher hinzu und konfigurieren sie:

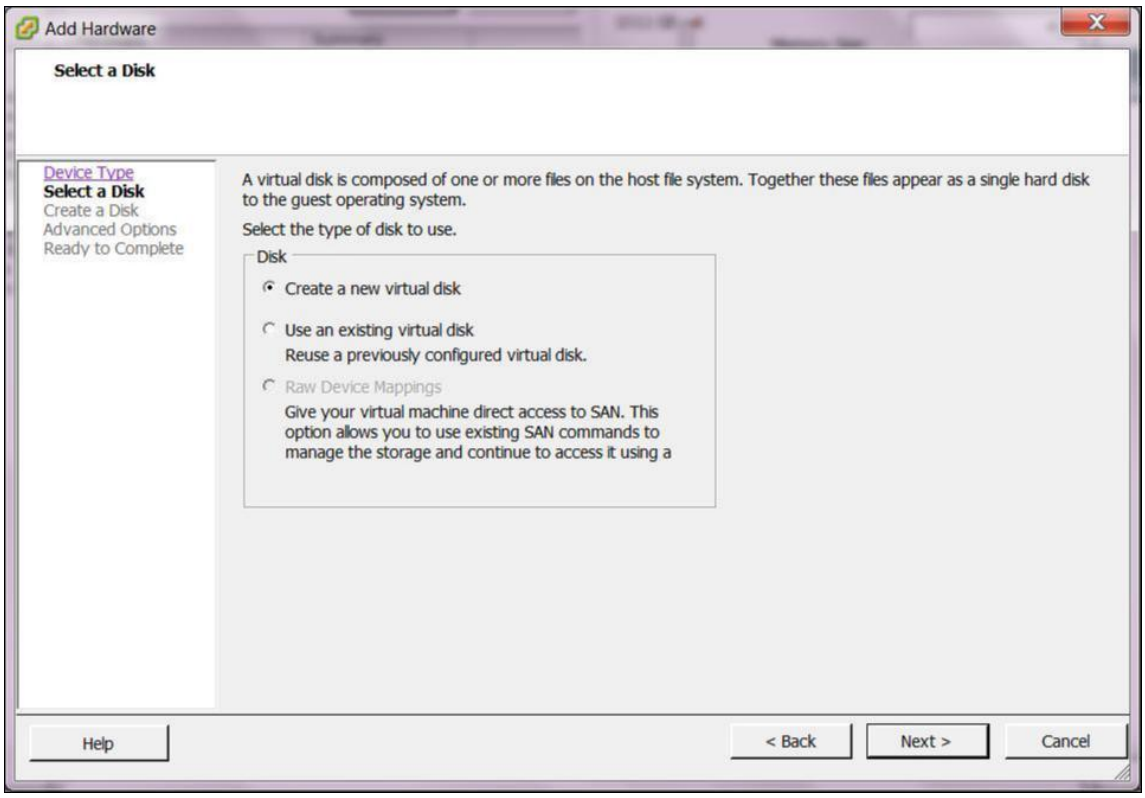
1. Klicken Sie im vSphere-Client auf das **Inventar** -Symbol, um die Seite Lagerbestand zu öffnen.
2. Erweitern Sie den Zweig **Bestandsstruktur** für den Citrix SD-WAN Center VM-Hostserver.
3. Klicken Sie im linken Bereich auf **+** neben der IP-Adresse des Servers, der die von Ihnen erstellte Citrix SD-WAN Center-VM hostet.
4. Öffnen Sie die neue Citrix SD-WAN Center VM zum Bearbeiten.
5. Klicken Sie in der **Bestandsstruktur** mit der rechten Maustaste auf den Namen der Citrix SD-WAN Center-VM, die Sie erstellt haben, und wählen Sie im Dropdownmenü **Einstellung bearbeiten**.



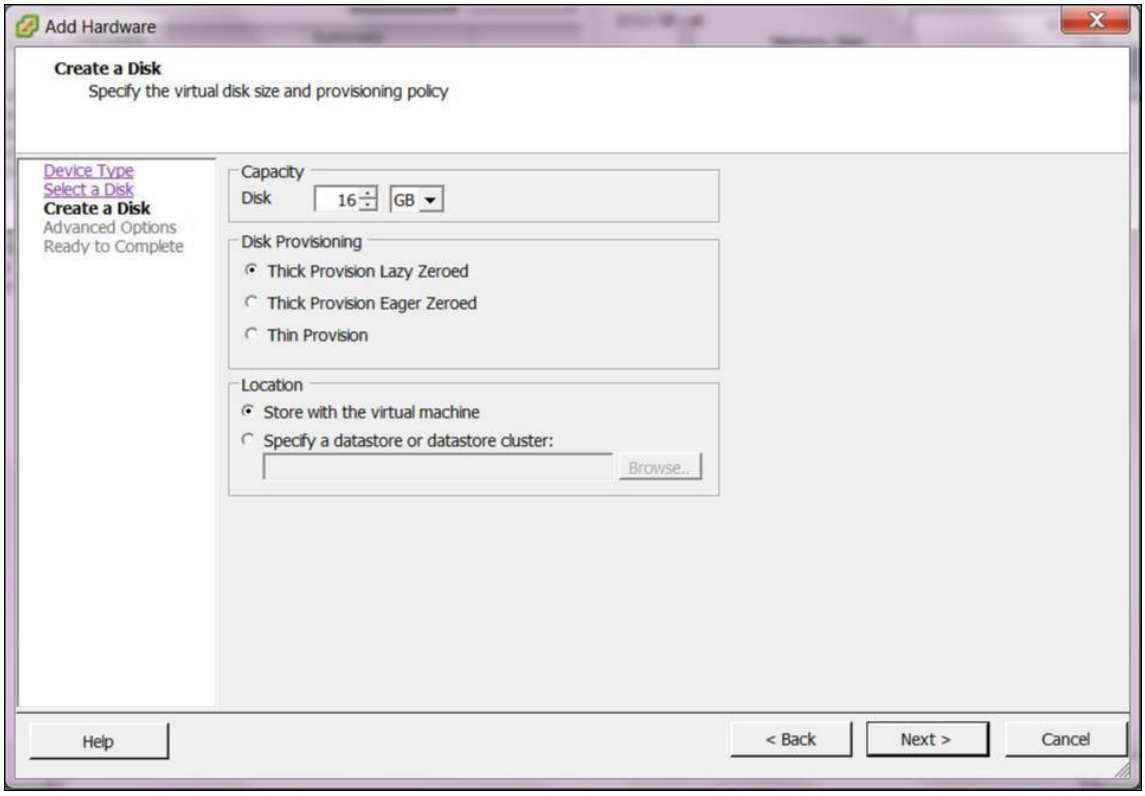
6. Geben Sie im Feld Speichergröße die Speichermenge ein, die dieser VM zugewiesen werden soll.

   Weitere Informationen finden Sie unter Speicheranforderungen.

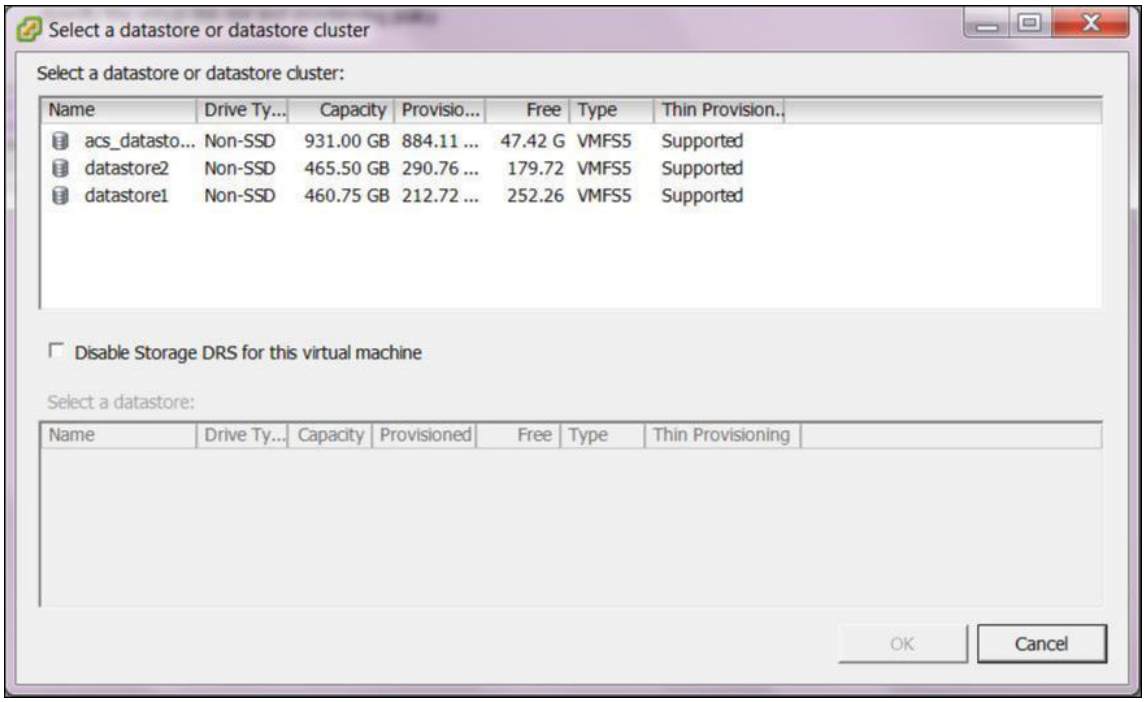
7. Klicken Sie auf **Hinzufügen**.
8. Wählen Sie auf der Seite Gerätetyp des Assistenten Hardware hinzufügen die Option **Festplatte** aus, und klicken Sie dann auf **Weiter**.



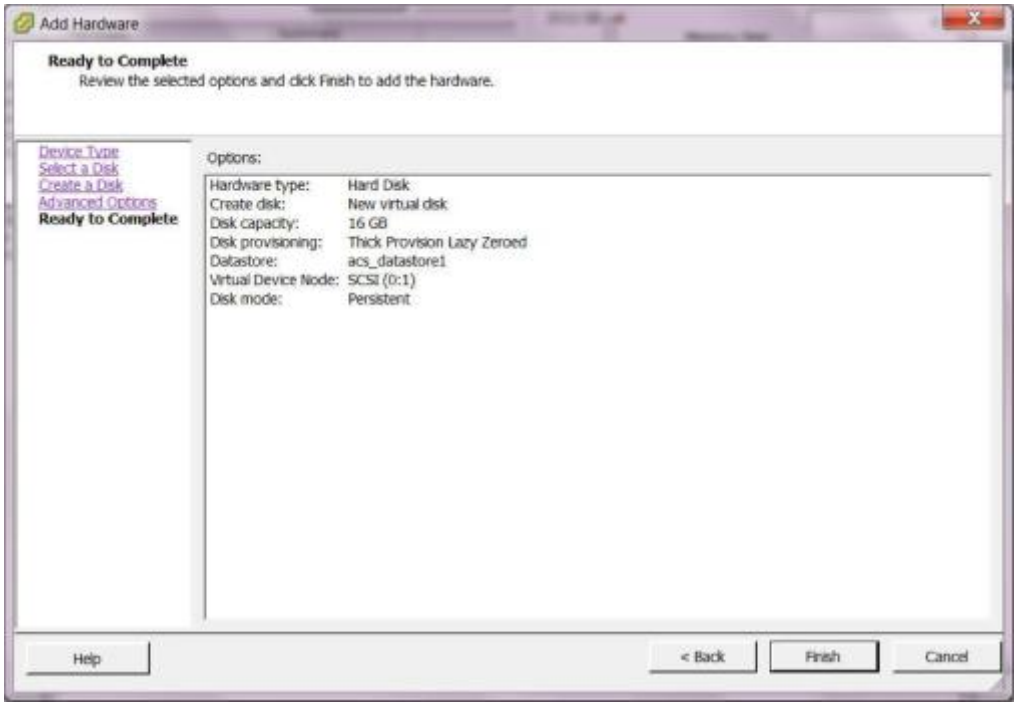
9. Wählen Sie auf der Seite Datenträger auswählen die Option **Neues virtuelles Laufwerk erstellen** aus, und klicken Sie auf **Weiter**.



10. Wählen Sie auf der Seite Datenträger erstellen im Abschnitt **Kapazität** die Festplattenkapazität für das neue virtuelle Laufwerk aus.
11. Wählen Sie im Abschnitt Datenträgerbereitstellung die Option **Thick Provisioning Lazy Zeroed** (Standardeinstellung) aus.
12. Wählen Sie im Abschnitt Speicherort die Option **Datenspeicher oder Datenspeicher-Cluster angeben**aus.
13. Klicken Sie auf **Durchsuchen**.



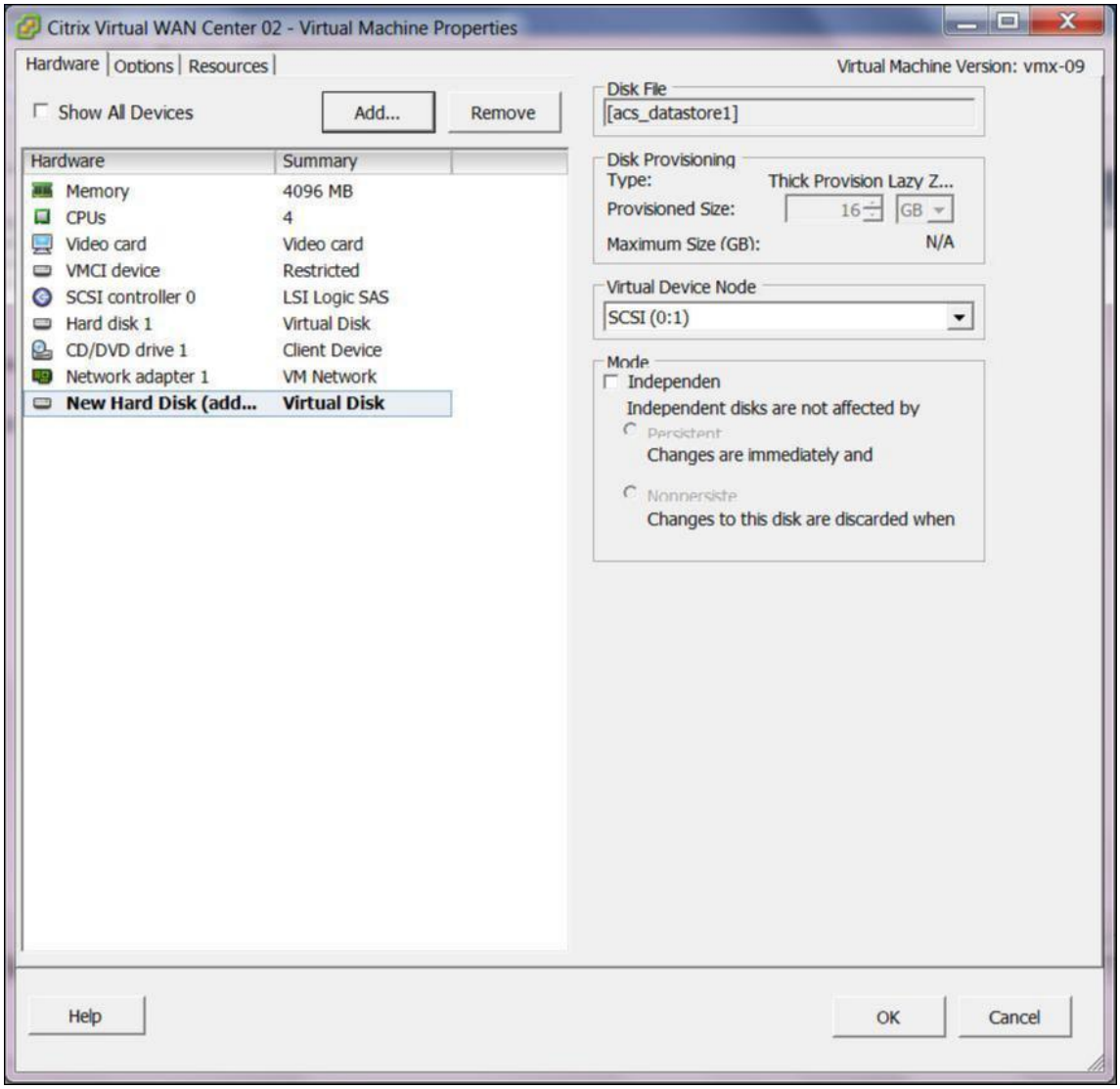
14. Wählen Sie einen Datenspeicher mit ausreichend verfügbarem Speicherplatz aus, und klicken Sie auf **OK**.
15. Klicken Sie auf **Weiter**.
16. Übernehmen Sie auf der Seite Erweiterte Optionen die Standardeinstellungen **für erweiterte Optionen**, und klicken Sie auf **Weiter**.



17. Klicken Sie auf **Fertig stellen**.

    Dadurch wird das neue virtuelle Laufwerk hinzugefügt, der Assistent zum Hinzufügen von Hardware wird beendet und Sie kehren zur Seite Eigenschaften des virtuellen Computers zurück.

18. Klicken Sie auf **OK**.



Installieren und Konfigurieren von Citrix SD-WAN Center auf XenServer

April 13, 2021

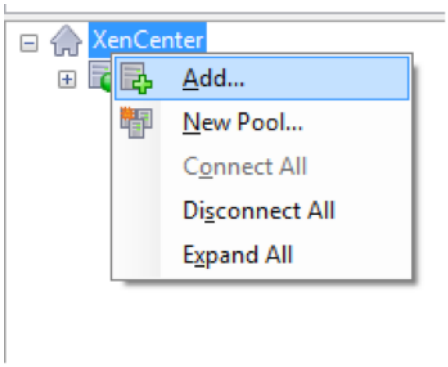
Sammeln Sie vor der Installation der virtuellen Citrix SD-WAN Center-Maschine auf einem XenServer-Server die erforderlichen Informationen wie unter Installations- und Konfigurationsinformationen für Citrix SD-WAN Center erfassen beschrieben.

Installieren des XenServer-Servers

Um den Citrix XenServer-Server zu installieren, auf dem Sie die virtuelle Citrix SD-WAN Center-Maschine bereitstellen möchten, muss XenCenter auf Ihrem Computer installiert sein. Wenn Sie dies noch nicht getan haben, laden Sie XenCenter herunter und installieren Sie es.

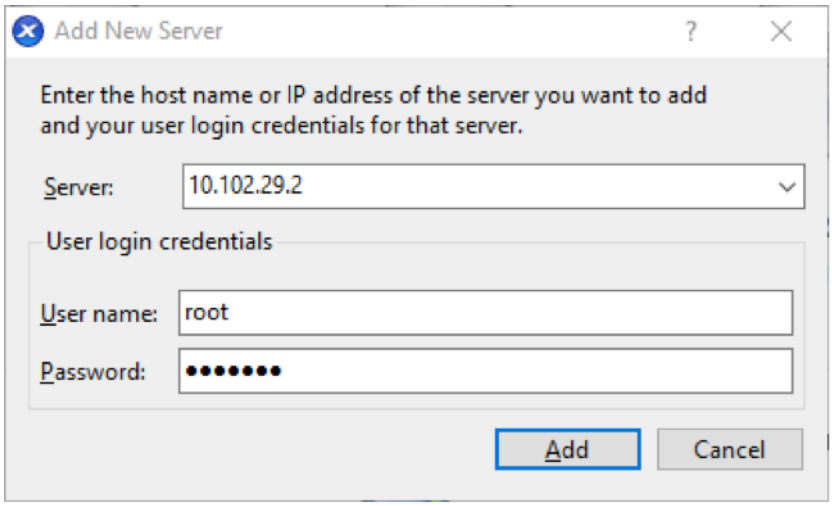
So installieren Sie einen XenServer-Server:

1. Öffnen Sie die XenCenter-Anwendung auf Ihrem Computer.
2. Klicken Sie im linken Strukturbereich mit der rechten Maustaste auf **XenCenter** und wählen Sie **Hinzufügen** aus.



3. Geben **Sie im Fenster "Neuen Server hinzufügen** "die erforderlichen Informationen in die folgenden Felder ein:

   - **Server**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des XenServer-Servers ein, auf dem die Citrix SD-WAN Center-VM-Instanz gehostet wird.
   - **Benutzername**: Geben Sie den Serveradministratorkontonamen ein. Der Standardwert ist root.
   - **Kennwort**: Geben Sie das Kennwort ein, das diesem Administratorkonto zugeordnet ist.



4. Klicken Sie auf **Hinzufügen**.

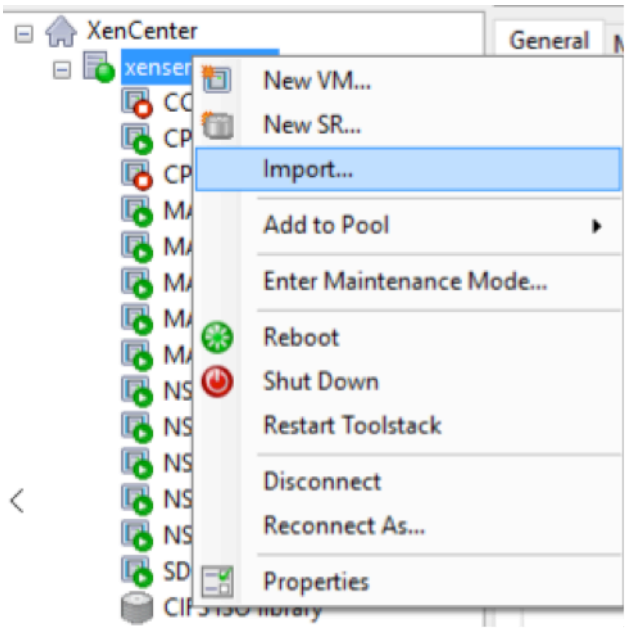
   Die IP-Adresse des neuen Servers wird im linken Bereich angezeigt.

Erstellen der Citrix SD-WAN Center-VM mit der XVA-Datei

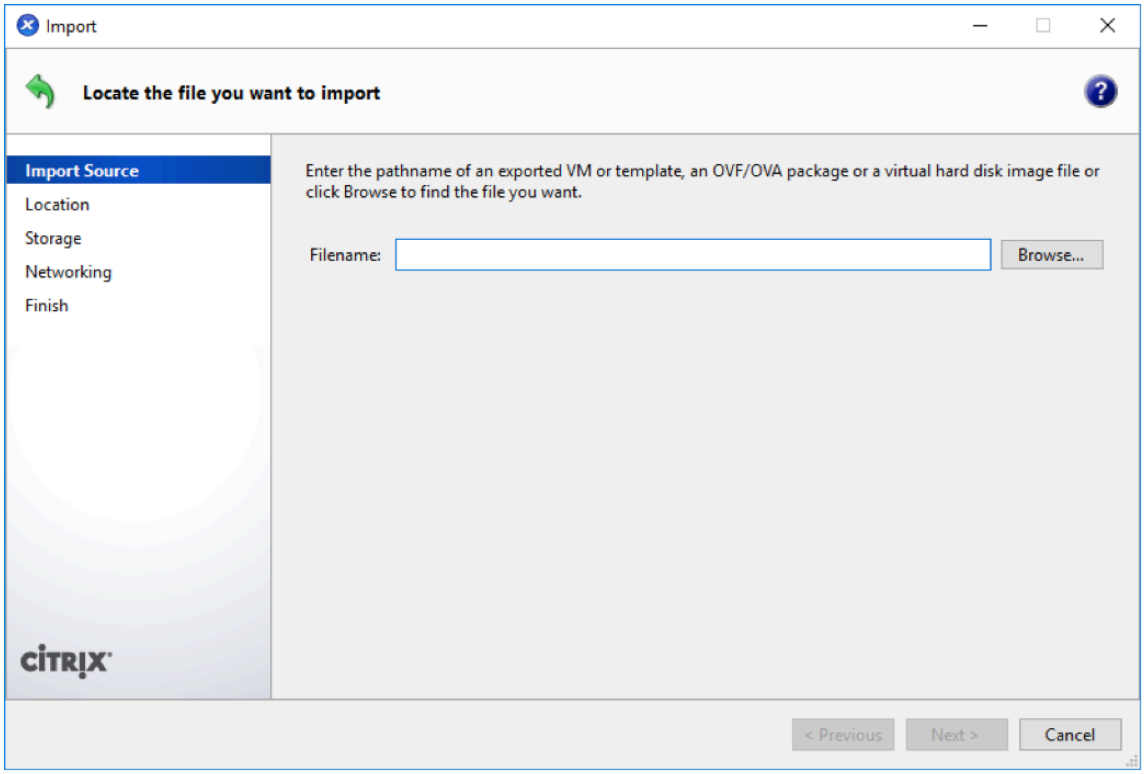
Die Software für virtuelle Citrix SD-WAN Center wird als XVA-Datei verteilt. Wenn Sie dies noch nicht getan haben, laden Sie die XVA-Datei herunter. Weitere Informationen finden Sie unter Systemanforderungen und Installation.

So erstellen Sie die Citrix SD-WAN Center VM:

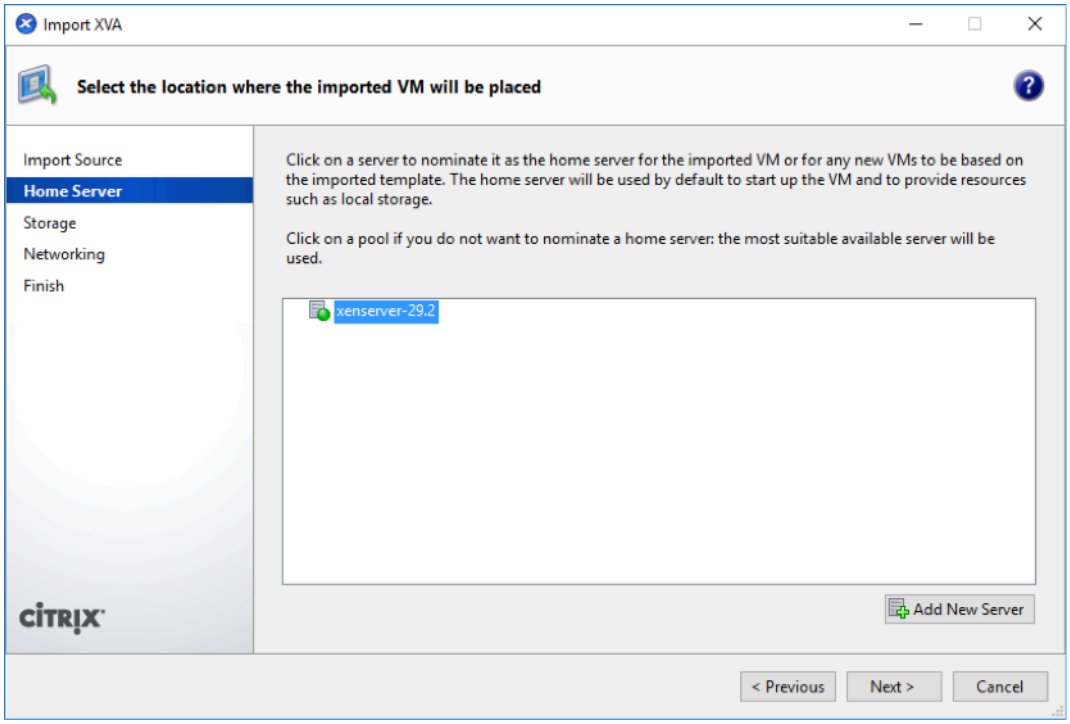
1. Klicken Sie in XenCenter mit der rechten Maustaste auf **XenServer**, und klicken Sie auf **Importieren**.



2. Navigieren Sie zur heruntergeladenen XVA-Datei, wählen Sie sie aus, und klicken Sie auf **Weiter**.

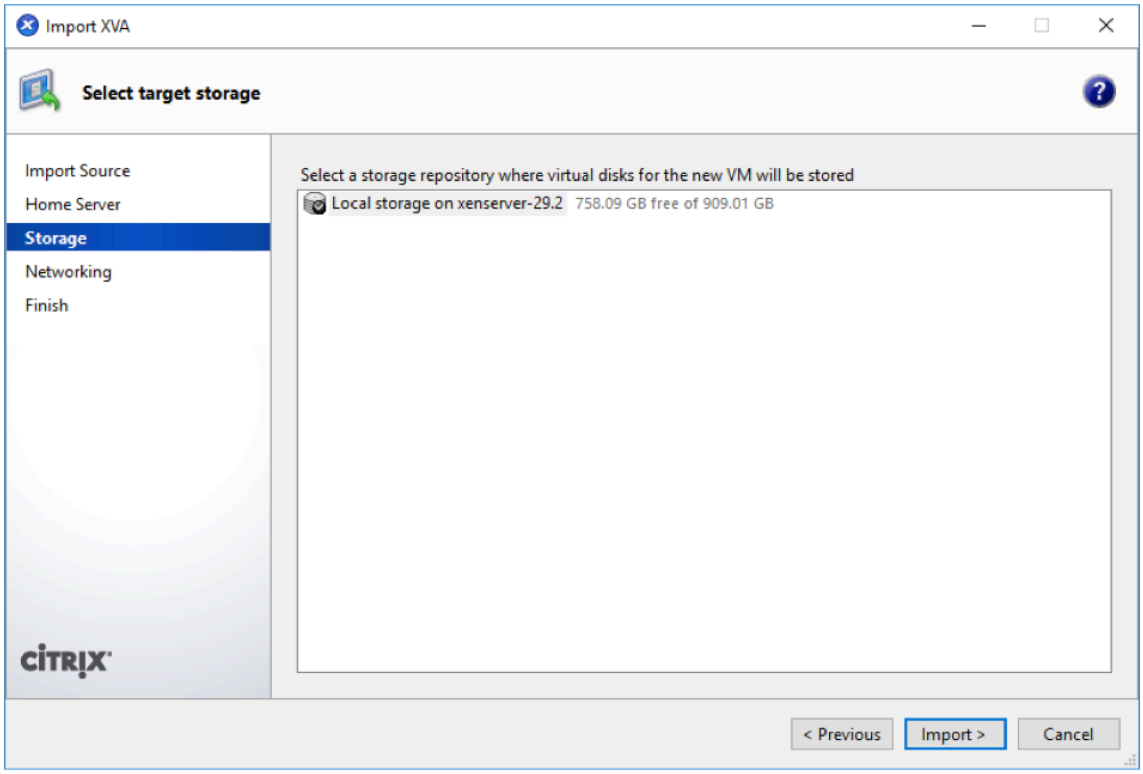


3. Wählen Sie einen zuvor erstellten XenServer-Server als Speicherort aus, in den die VM importiert werden soll, und klicken Sie auf **Weiter**.



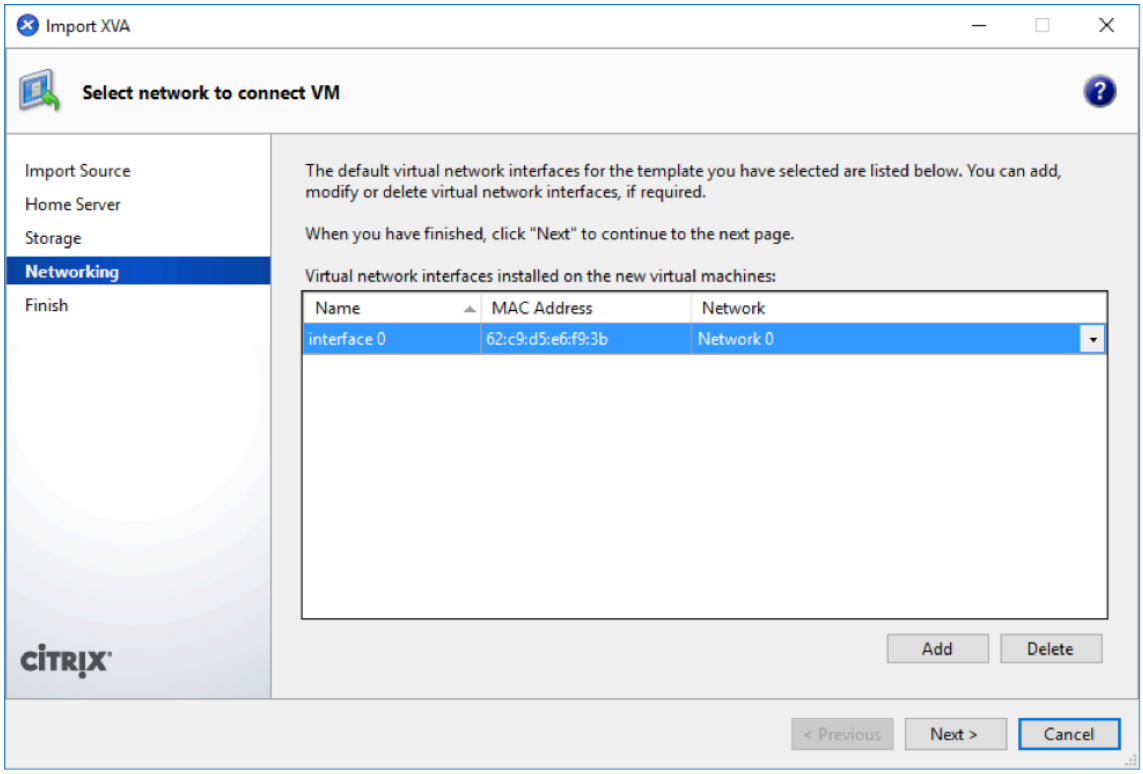
4. Wählen Sie ein Speicher-Repository aus, in dem der virtuelle Datenträger für die neue VM gespeichert wird, und klicken Sie auf **Import.**

Vorerst können Sie die Standard-Speicherressource akzeptieren. Oder Sie können den Datenspeicher konfigurieren. Weitere Informationen finden Sie unter **Hinzufügen und Konfigurieren des Datenspeichers in XenServer**.



Die importierte Citrix SD-WAN Center-VM wird im linken Bereich angezeigt.

5. Wählen Sie ein Netzwerk aus, mit dem die VM verbunden werden soll, und klicken Sie auf **Weiter**.



6. Klicken Sie auf **Fertig stellen**.

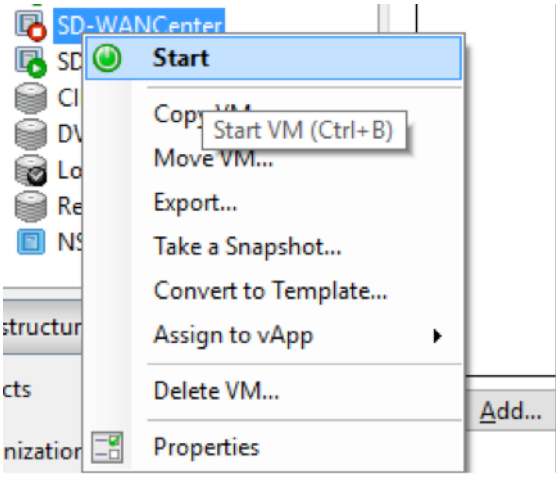
Anzeigen und Aufzeichnen der Management-IP-Adresse auf XenServer

Die Management-IP-Adresse ist die IP-Adresse der Citrix SD-WAN Center VM. Verwenden Sie diese IP-Adresse, um sich bei der Citrix SD-WAN Center Web-Benutzeroberfläche anzumelden.

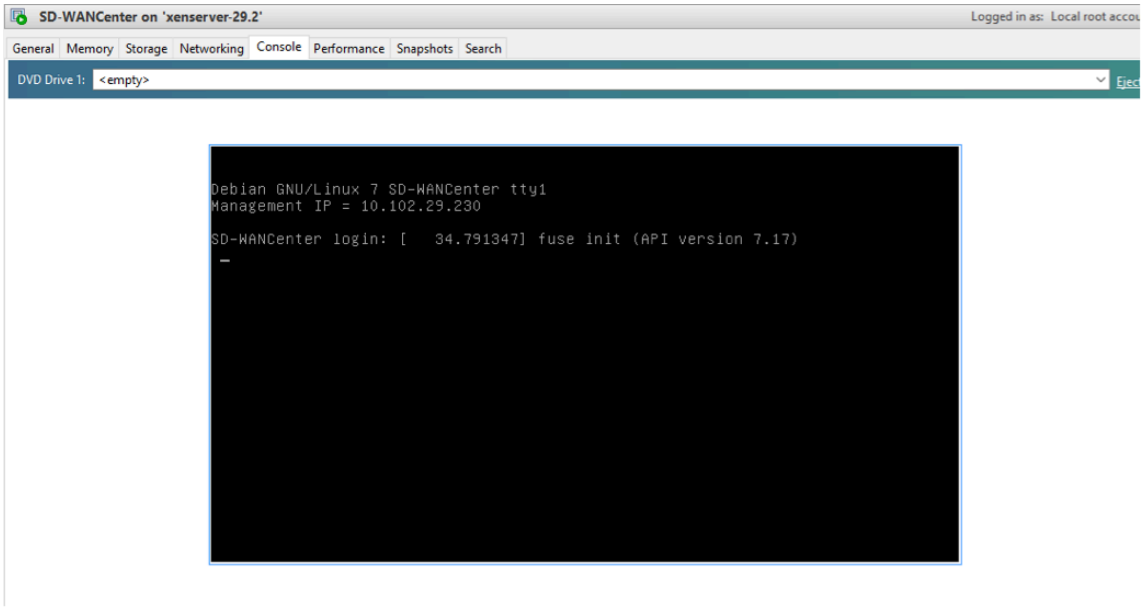
> **Hinweis**
>
> Der DHCP-Server muss vorhanden und im SD-WAN-Netzwerk verfügbar sein.

So zeigen Sie die Management-IP-Adresse an:

1. Klicken Sie in der XenCenter-Schnittstelle im linken Fensterbereich mit der rechten Maustaste auf die neue Citrix SD-WAN Center-VM, und wählen Sie **Start**aus.



2. Wenn die VM gestartet wird, klicken Sie auf die Registerkarte **Konsole**.



3. Notieren Sie sich die Management-IP-Adresse.

> **Hinweis**
>
> Der DHCP-Server muss vorhanden und im SD-WAN-Netzwerk verfügbar sein, anderenfalls kann dieser Schritt nicht abgeschlossen werden.

4. Melden Sie sich bei der VM an. Die Anmeldeinformationen für die neue Citrix SD-WAN Center-VM lauten wie folgt:

   Anmeldung: admin

   Kennwort: password

   Wenn der DHCP-Server nicht im Citrix SD-WAN-Netzwerk konfiguriert ist, müssen Sie manuell eine statische IP-Adresse eingeben.

So konfigurieren Sie eine statische IP-Adresse als Management-IP-Adresse:

1. Wenn die VM gestartet wird, klicken Sie auf die Registerkarte **Konsole**.
2. Melden Sie sich bei der VM an. Die Anmeldeinformationen für die neue Citrix SD-WAN Center-VM lauten wie folgt:

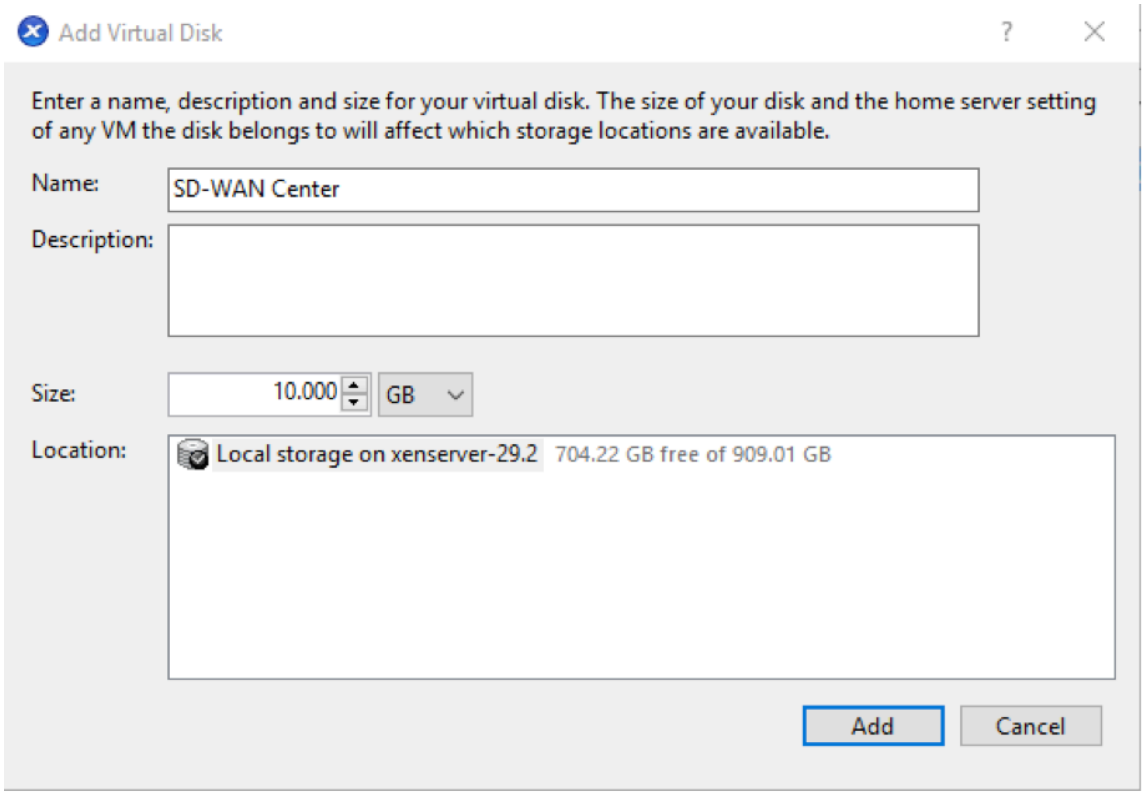
   Login: admin
   , **Kennwort**: password
3. Geben Sie in der Konsole den CLI-Befehl **management_ip** ein.
4. Geben Sie die Befehlssatzschnittstelle ein <ipaddress> <subnetmask> <gateway>, um Management-IP zu konfigurieren.**

Hinzufügen und Konfigurieren von Datenspeicher für einen XenServer-Server

Sie können Datenspeicher hinzufügen und konfigurieren, um Statistiken über Citrix SD-WAN Center zu speichern.

So fügen Sie die Datenspeicherung hinzu und konfigurieren sie:

1. Fahren Sie in XenCenter die Citrix SD-WAN Center-VM herunter.
2. Klicken Sie auf der Registerkarte **Speicher** auf **Hinzufügen**.



3. Geben Sie im Feld **Name** einen Namen für das virtuelle Laufwerk ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung des virtuellen Laufwerks ein.
5. Wählen Sie im Feld **Größe** die gewünschte Größe aus.
6. Wählen Sie im Feld **Standort** den lokalen Speicher aus.
7. Klicken Sie auf **Hinzufügen**.

Installieren und Konfigurieren von Citrix SD-WAN Center unter Microsoft Hyper-V

April 13, 2021

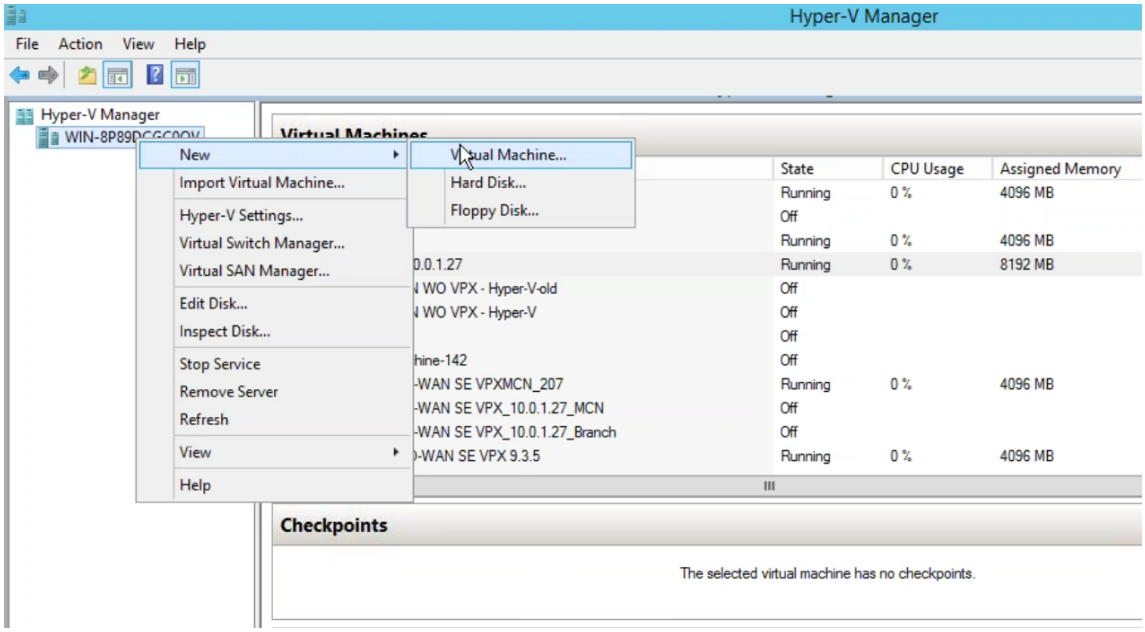
Sammeln Sie vor der Installation der virtuellen Maschine (VM) von Citrix SD-WAN Center auf dem Microsoft Hyper-V-Server die erforderlichen Informationen wie unter beschriebenSystemanforderungen und Installation.

Laden Sie die SD-WAN Center-Software für Hyper-V herunter, wie im Abschnitt Citrix SD-WAN Center Software herunterladen von beschriebenSystemanforderungen und Installation/en-us/citrix-sd-wan-center/11/system-requirements-and-installation.html.[()]

Stellen Sie sicher, dass das Hyper-V-Feature und das Verwaltungstool auf Ihrem Windows-Server aktiviert sind.

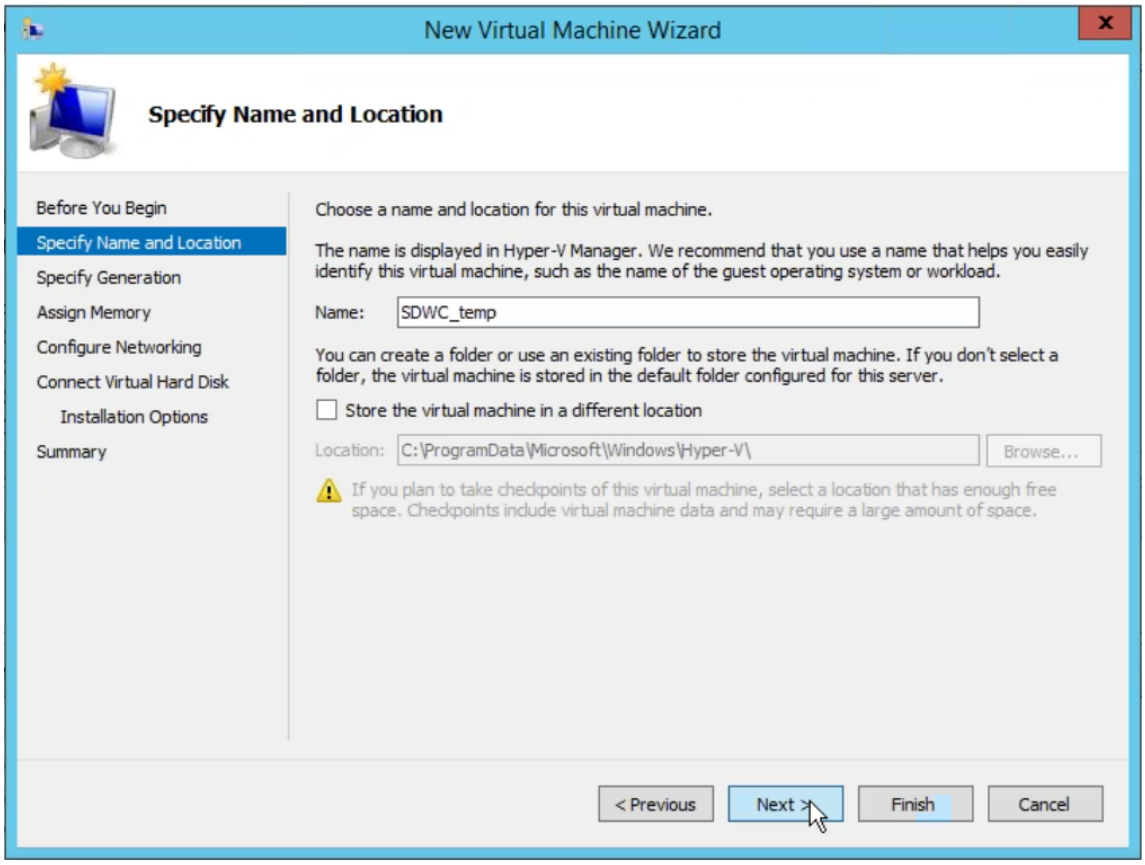
So erstellen Sie die SD-WAN Center-VM auf dem Hyper-V-Server:

1. Klicken Sie im Hyper-V-Manager mit der rechten Maustaste auf den Hyper-V-Server, und wählen Sie **Neu** > **Virtueller Computer** aus.



Der **Assistent für neue virtuelle Computer** wird angezeigt. Klicken Sie auf **Weiter**.

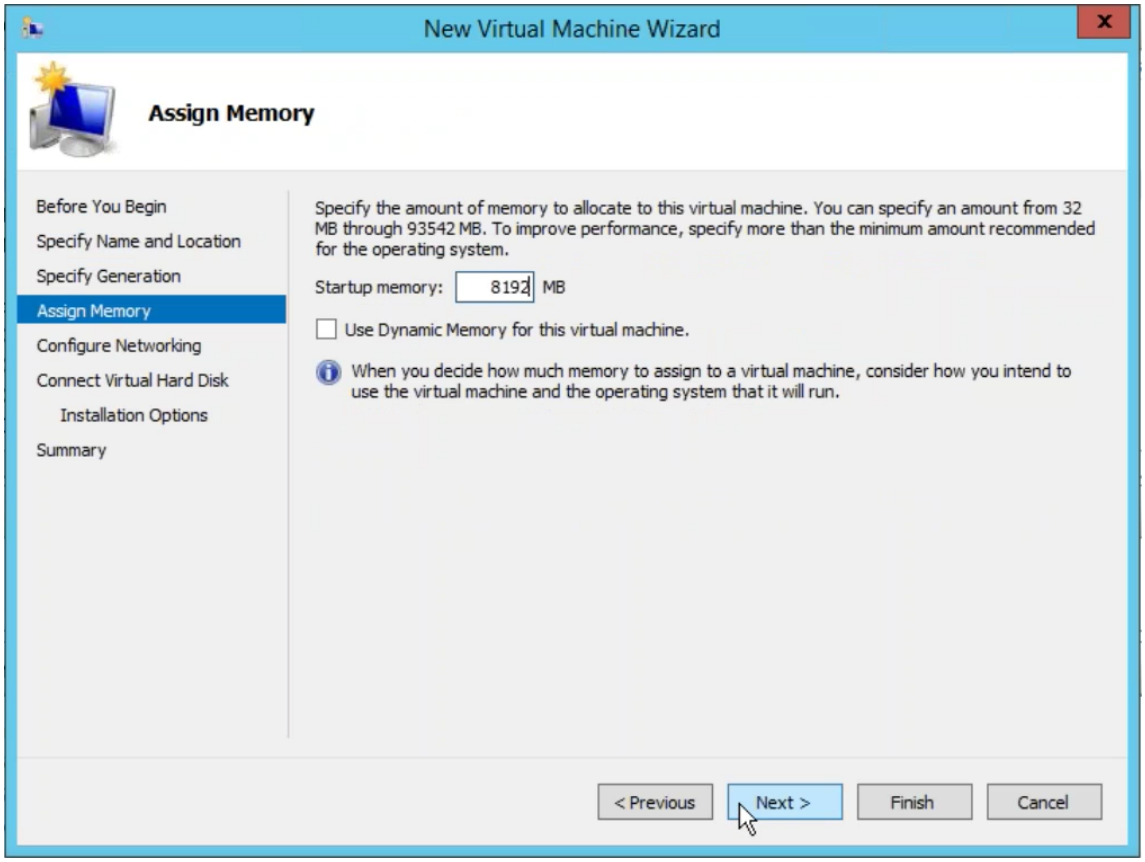
2. Geben Sie einen Namen für Ihre SD-WAN-Center-VM an, und ändern Sie ggf. den Speicherort des VM-Speicherorts.Klicken Sie auf **Weiter**.



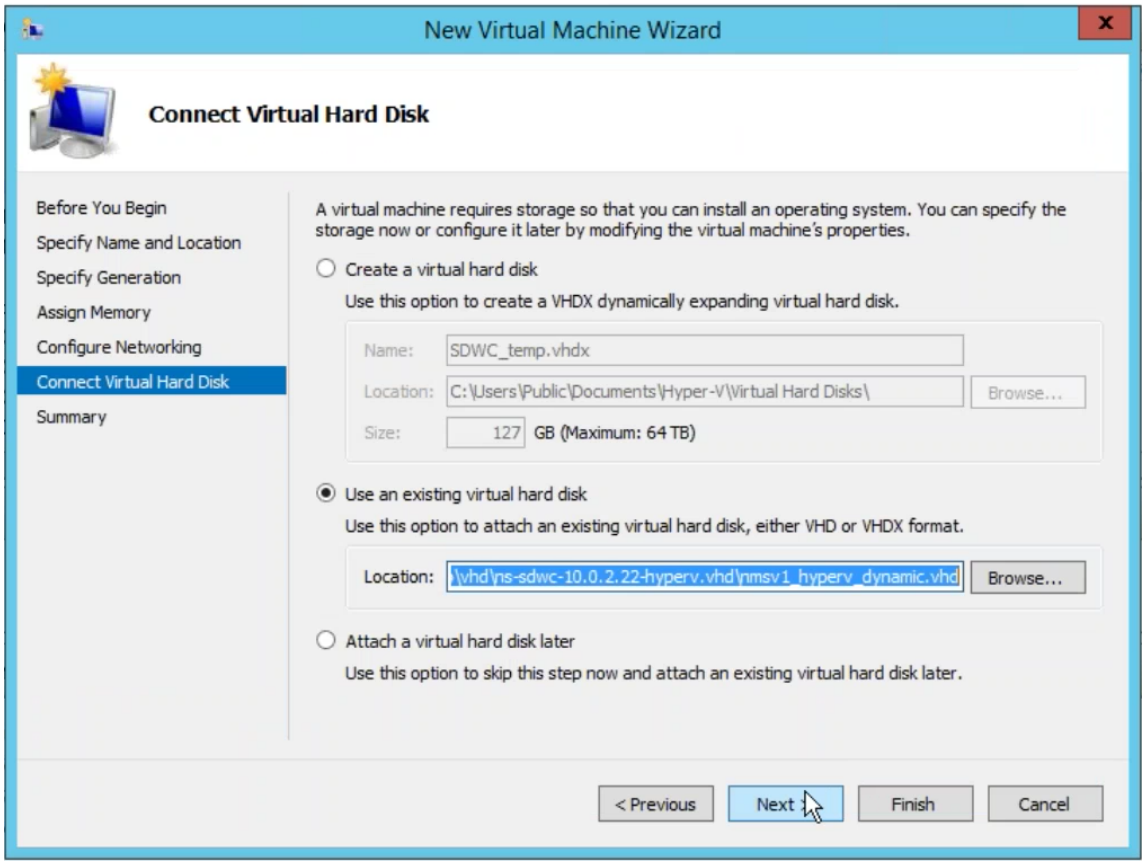
3. Wählen Sie die erforderliche VM-Generierung aus. Klicken Sie auf **Weiter**.

4. Weisen Sie der VM einen Arbeitsspeicher von 8 GB zu. Klicken Sie auf **Weiter**.

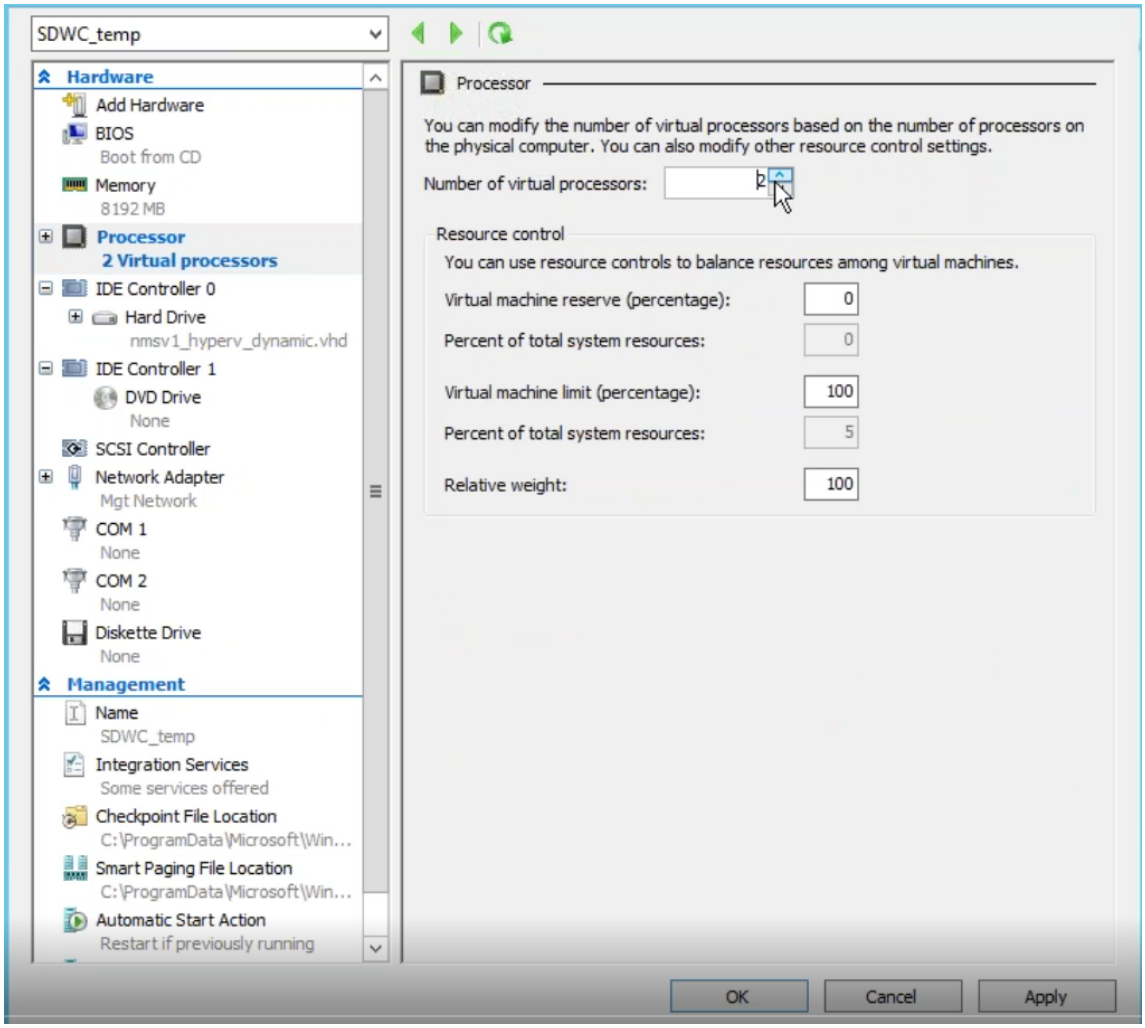
> **Hinweis**
>
> Die Citrix SD-WAN Center VM benötigt mindestens 8 GB Arbeitsspeicher, um bis zu 64 Standorte zu verwalten.Weitere Hinweise zum Speicher für die Anzahl der Standortzuordnungen finden Sie unterSystemanforderungen und Installation.



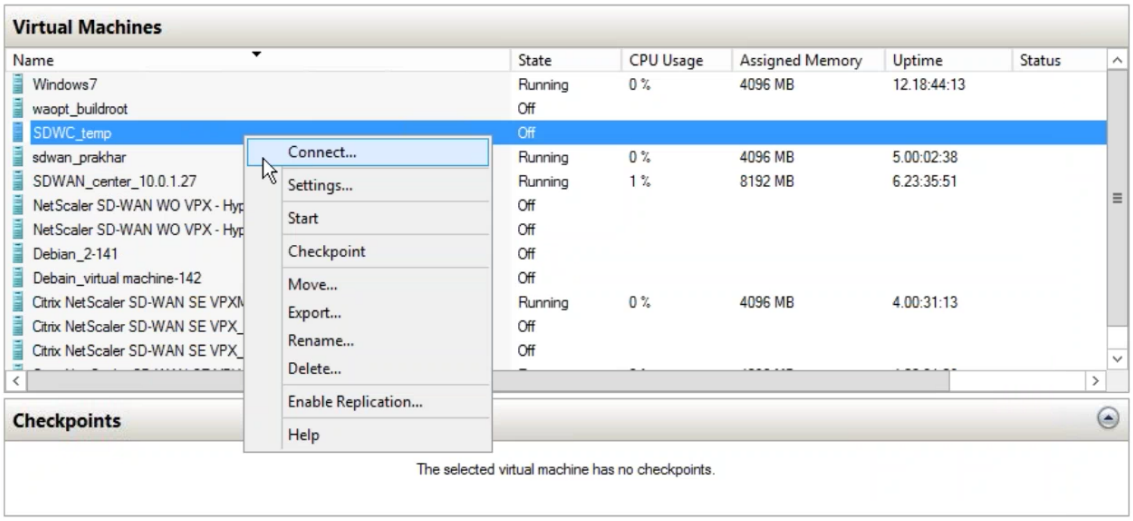
5. Wählen Sie den virtuellen Switch, der vom Netzwerkadapter der VM verwendet werden soll, Klicken Sie auf **Weiter**.
6. Wählen Sie **Vorhandene virtuelle Festplatte verwenden**aus, navigieren Sie und wählen Sie die heruntergeladene SD-WAN Center VHD-Datei aus. Klicken Sie auf **Weiter**.



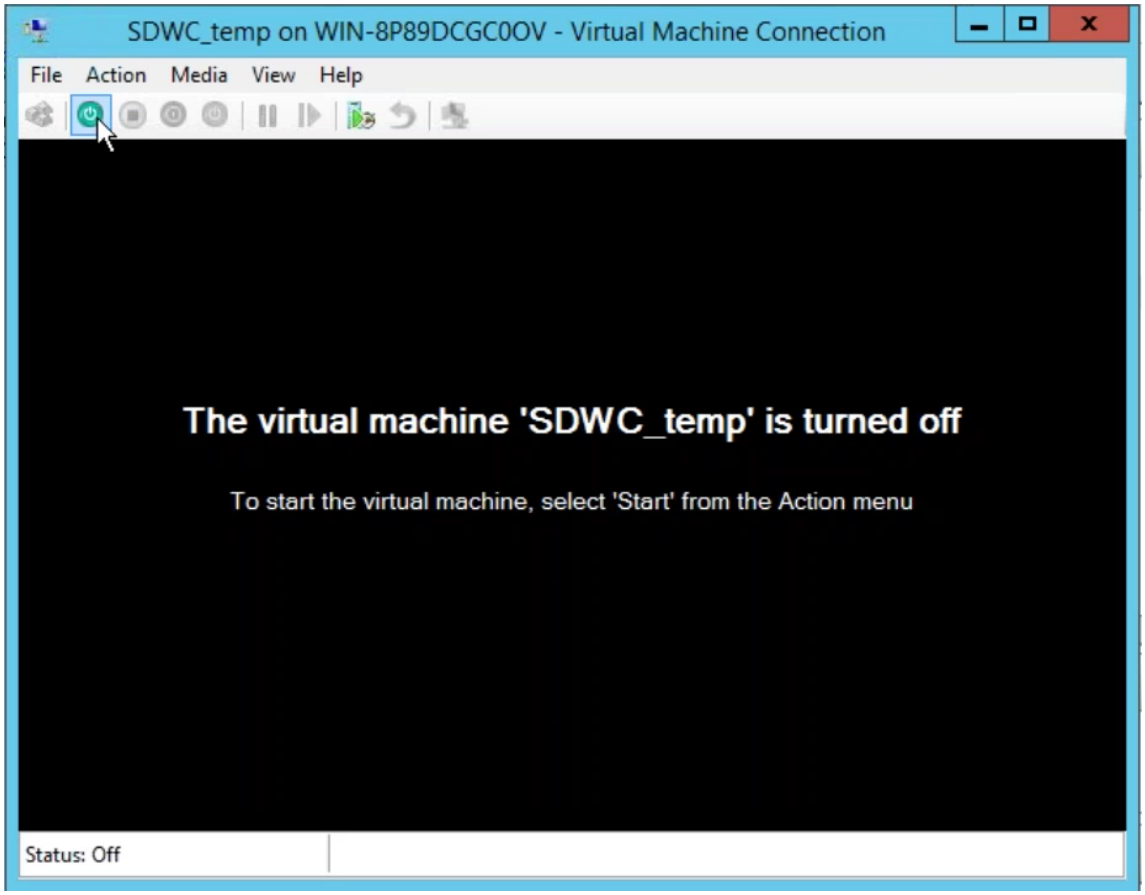
7. Überprüfen Sie die VM-Zusammenfassung, und ändern Sie ggf. die Einstellungen, andernfalls klicken Sie auf **Fertig stellen**.Die SD-WAN Center-VM wird erstellt und im Abschnitt **Virtuelle Maschinen** aufgeführt.
8. Klicken Sie mit der rechten Maustaste auf die SD-WAN Center-VM, und wählen Sie **Einstellungen**aus. Legen Sie die Anzahl der virtuellen Prozessoren auf vier fest, und klicken Sie auf **Übernehmen**.



9. Klicken Sie mit der rechten Maustaste auf die SD-WAN Center VM, und klicken Sie auf **Verbinden**.

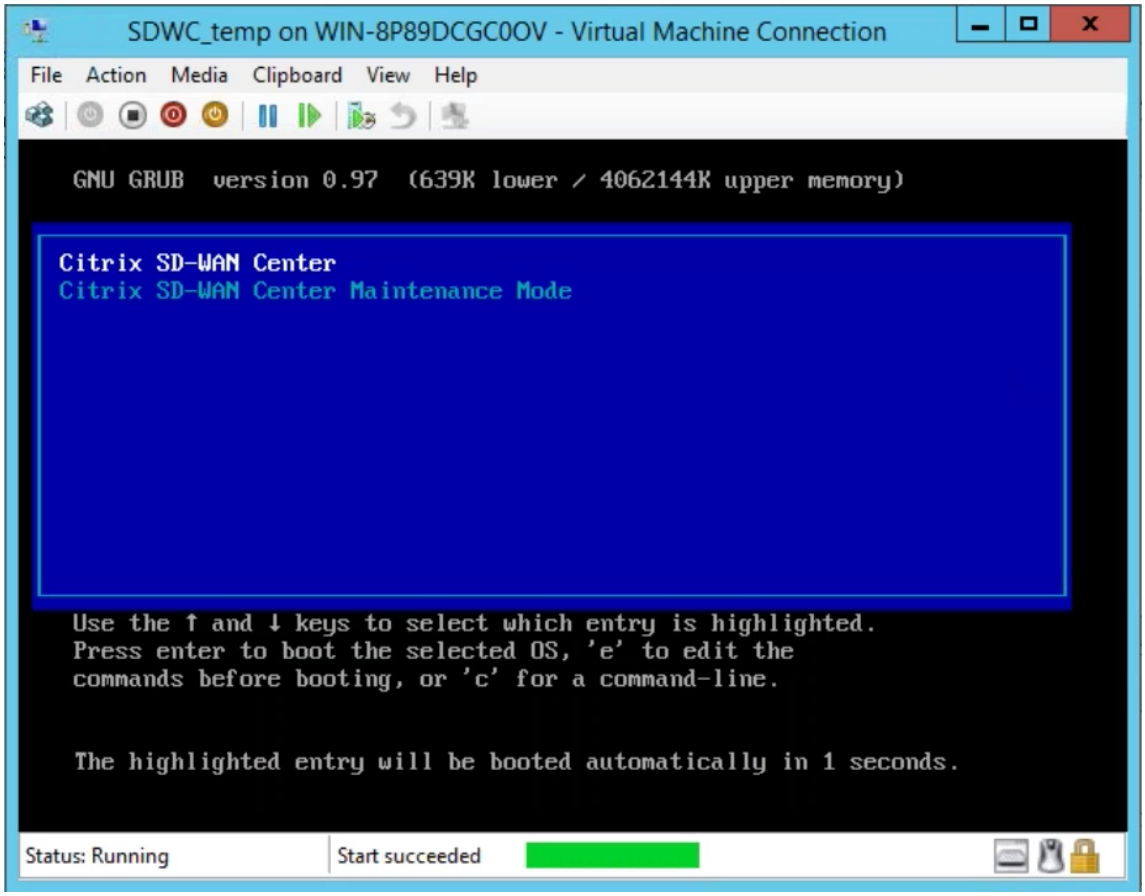


10. Klicken Sie auf die Schaltfläche **Start**.



> **Hinweis**
>
> Die Erstinstallation kann bis zu 50 Minuten dauern, abhängig von der Anzahl der CPUs und RAM, die Sie konfiguriert haben.

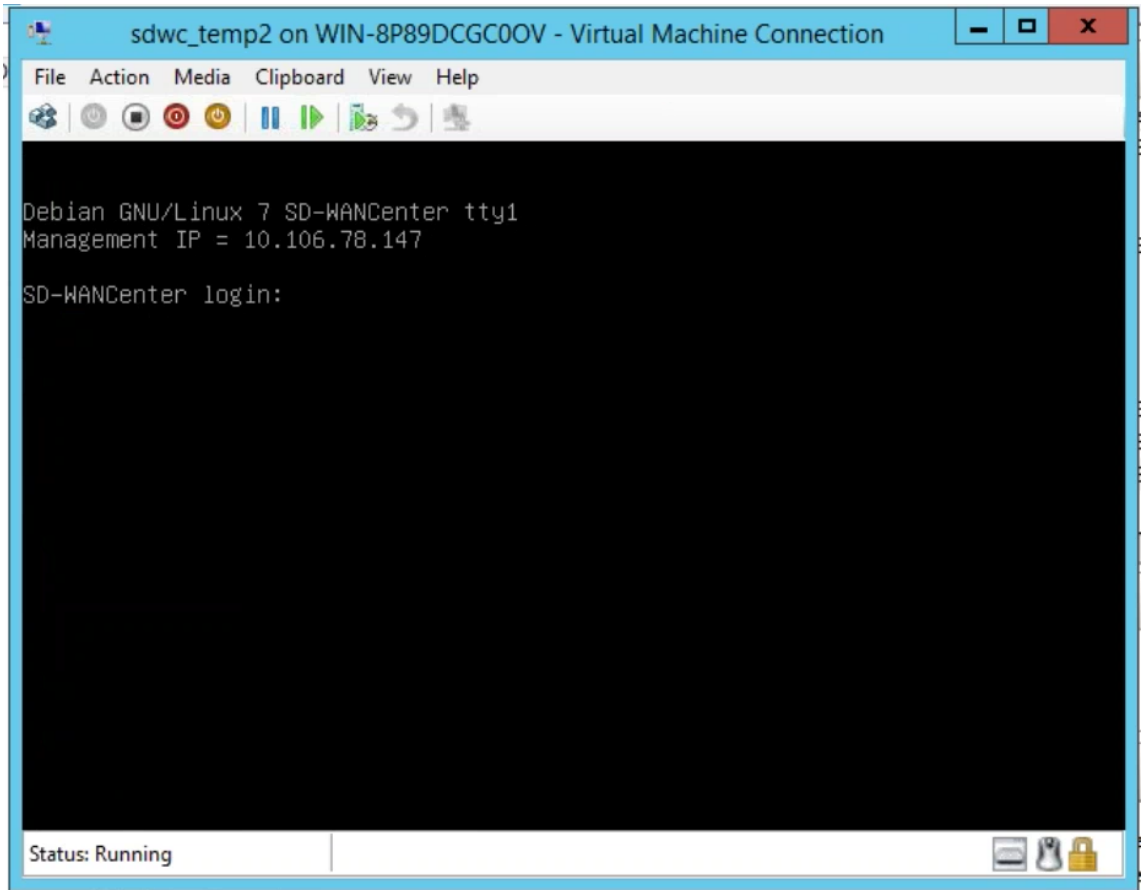
11. Nachdem die VM gestartet wurde, wählen Sie Citrix SD-WAN Center aus und drücken Sie die Eingabetaste.



12. Melden Sie sich bei der VM an. Die Standardanmeldedaten für die neue SD-WAN Center VM lauten wie folgt:

    Anmeldung: admin

    Kennwort: password



Die Management-IP-Adresse wird in der Konsole angezeigt. Verwenden Sie diese IP-Adresse, um auf die SD-WAN Center-Weboberfläche zuzugreifen.

> **Hinweis**
>
> Wenn DHCP im SD-WAN-Netzwerk nicht konfiguriert ist, müssen Sie manuell eine statische IP-Adresse eingeben.

So konfigurieren Sie eine statische IP-Adresse als Management-IP-Adresse:

1. Melden Sie sich bei der VM an. Die Standardanmeldedaten für die neue SD-WAN Center VM lauten wie folgt:

   Anmeldung: admin

   Kennwort: password

2. Geben Sie in der Konsole den CLI-Befehl ***management_ip***ein.
3. Geben Sie die Befehlssatzschnittstelle ein <ipaddress> <subnetmask> <gateway>, um die Management-IP zu konfigurieren.**

Verwenden Sie die Management-IP, um auf die Citrix SD-WAN Center-Webschnittstelle zuzugreifen.

Citrix SD-WAN Center auf Azure Marketplace mit Lösungsvorlage

April 13, 2021

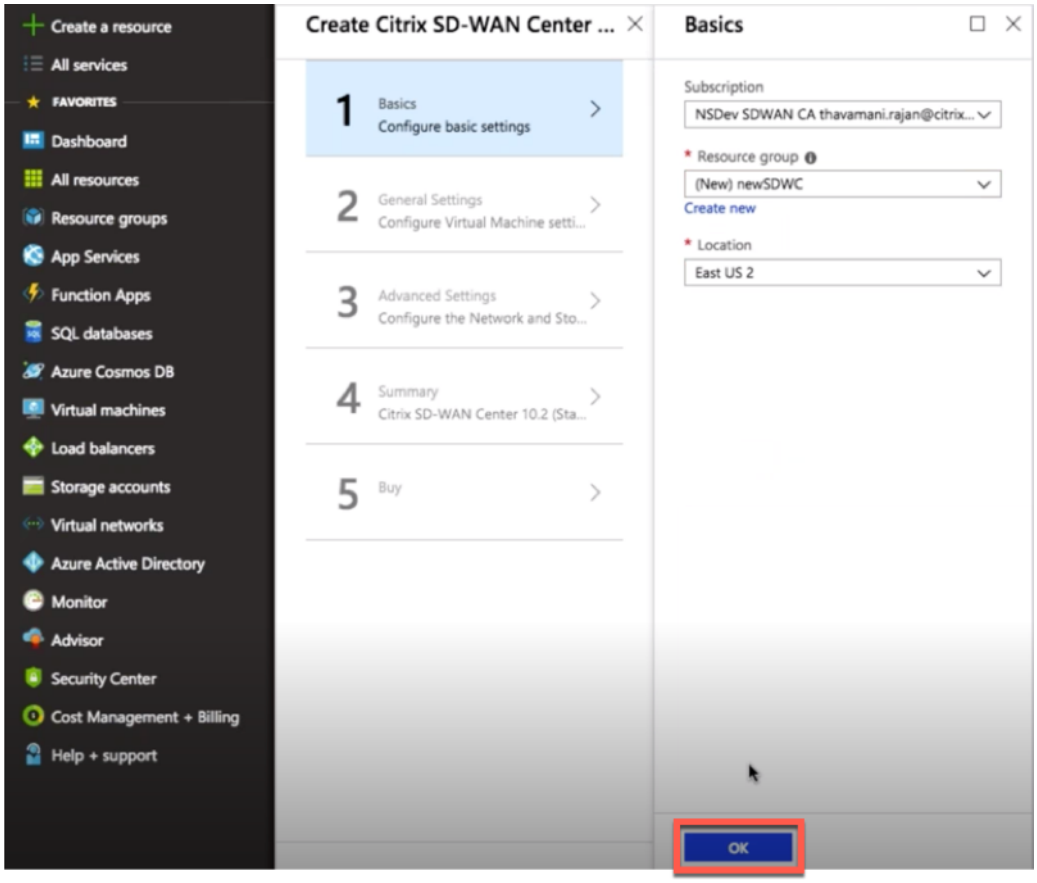
Citrix SD-WAN Center ist jetzt im Azure Marketplace verfügbar. Sie können Citrix SD-WAN Center als virtuelle Maschine (VM) in Azure Cloud mithilfe der Lösungsvorlage bereitstellen.

Sammeln Sie vor der Installation der virtuellen Maschine (VM) von Citrix SD-WAN Center auf Microsoft Azure die erforderlichen Informationen wie unter beschriebenSystemanforderungen und Installation.

Stellen Sie sicher, dass Sie Zugriff auf Microsoft Azure haben.

So stellen Sie Citrix SD-WAN Center VPX unter Microsoft Azure bereit:

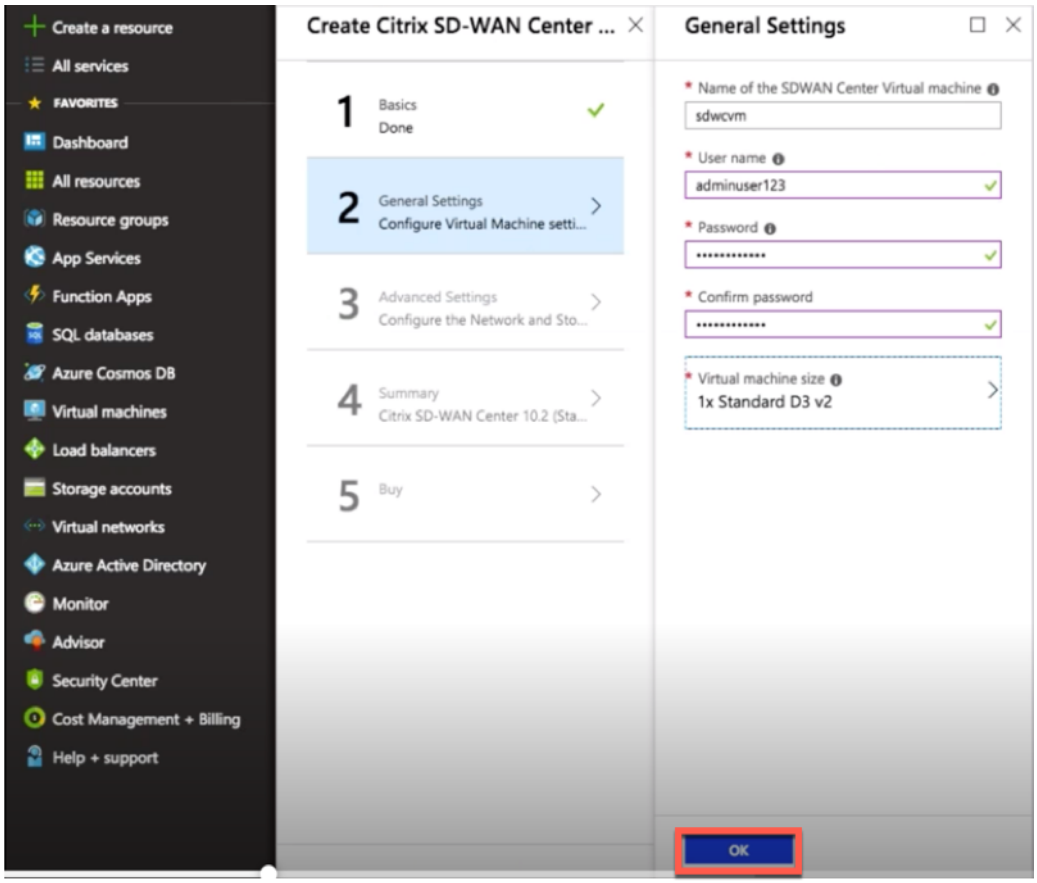
1. Navigieren Sie in Microsoft Azure zu **Startseite > Marketplace**. Suchen Sie das **Citrix SD-WAN Center**, und wählen Sie es aus.
2. Klicken Sie auf der Seite **Citrix SD-WAN Center** auf **Erstellen**. Die Seite **Citrix SD-WAN Center erstellen** wird angezeigt.
3. Wählen Sie im Abschnitt **Grundlagen** den Abonnementtyp, die Ressourcengruppe und den Speicherort aus. Klicken Sie auf **OK**.



> **HINWEIS:**
>
> Eine Ressourcengruppe ist ein Container, der zugehörige Ressourcen für eine Azure-Lösung enthält. Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten. Sie können auf der Grundlage Ihrer Bereitstellung festlegen, wie Ressourcen Ressourcengruppen zugewiesen werden sollen.

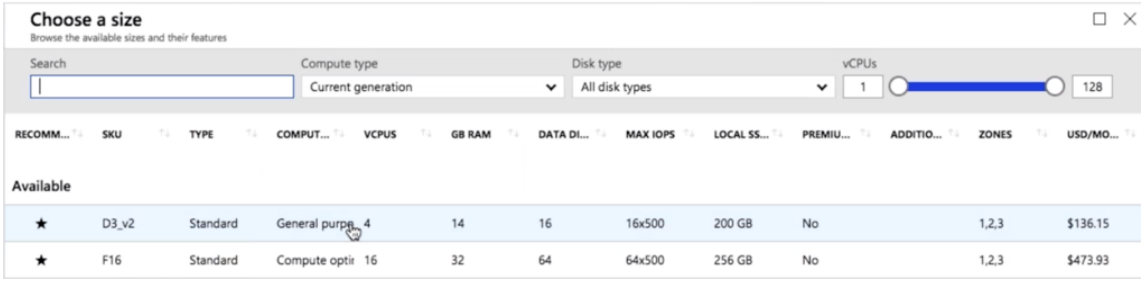
4. Geben Sie im Abschnitt **Allgemeine Einstellungen** den Namen und die Anmeldeinformationen ein, die Zugriff auf Administratorebene oder Berechtigungen für die virtuelle Citrix SD-WAN Center-Maschine bereitstellen.

   Anmeldeinformationen, die in diesem Schritt 4 bereitgestellt werden, werden auch verwendet, um das Kennwort für **Administrator-** Benutzeranmeldekonto festzulegen (standardmäßiges Administratorkonto Kennwort kann mit diesem Kennwort Anmeldeinformationen geändert werden). Klicken Sie auf **OK**.

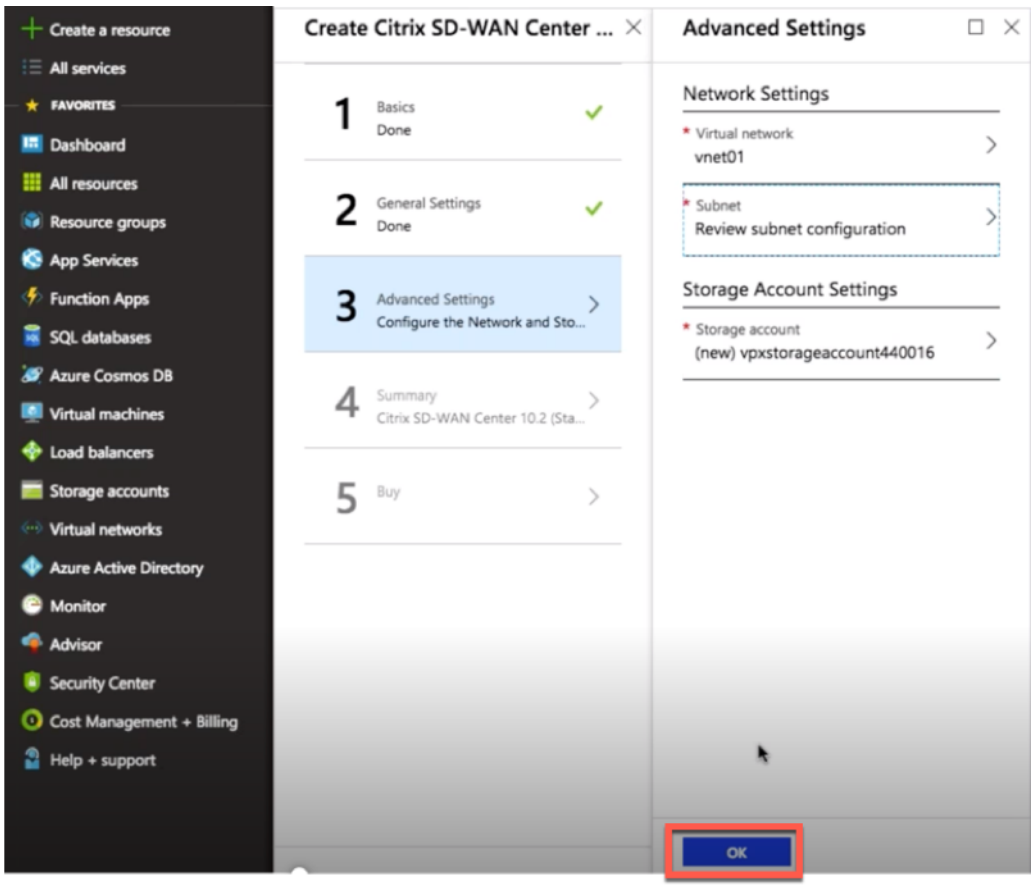


> **HINWEIS:**
>
> Derzeit stehen zwei Größen zur Verfügung: **Standard_D3_v2** und **Standard_F16**. Die D3_v2-Instanz kann verwendet werden, um ein Netzwerk mit bis zu 64 Standorten zu

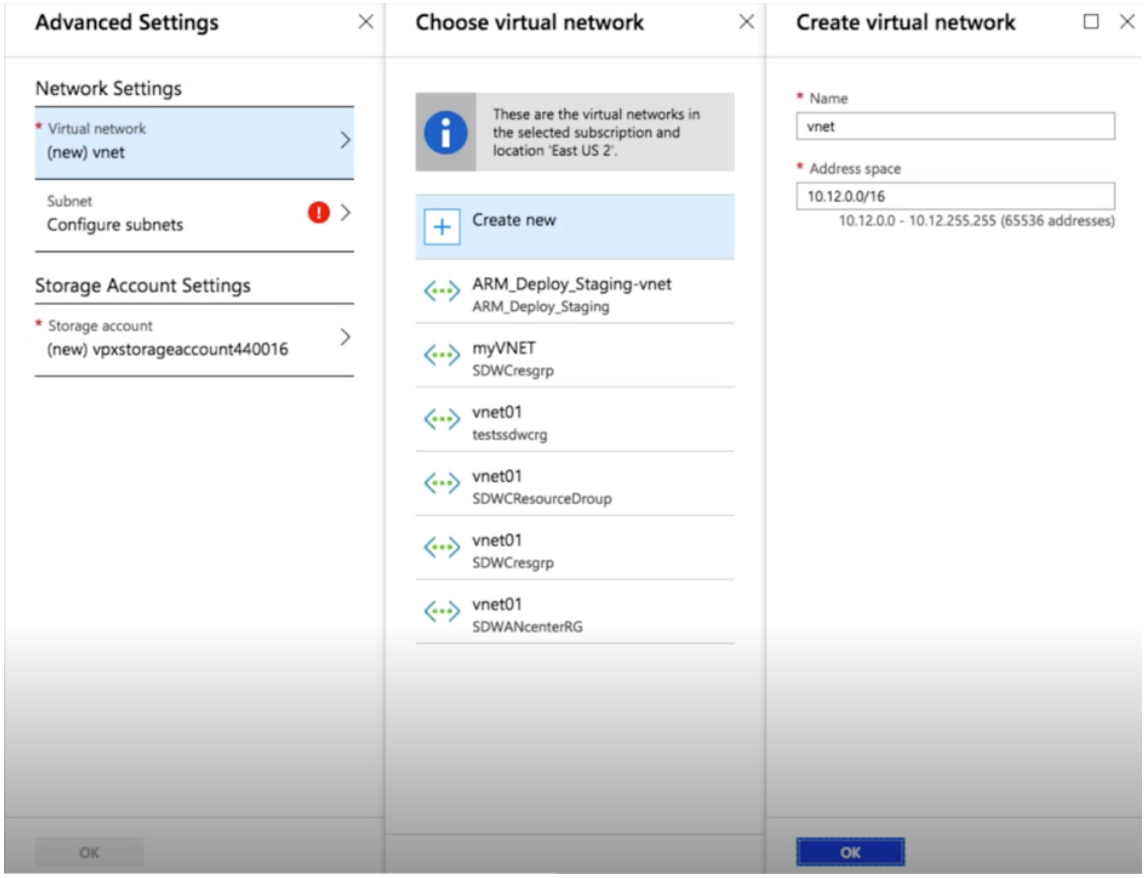
> überwachen. Die F16-Instanz ist nützlich, um ein Netzwerk mit bis zu 128 Standorten zu überwachen. Sie können auch eine verfügbare Größe der virtuellen Maschine suchen und auswählen.



5. Konfigurieren Sie im Abschnitt **Erweiterte Einstellungen** die **Netzwerk- und Speicherkontoeinstellung** für **Citrix SD-WAN Center VPX** basierend auf der Anzahl der zu überwachenden Sites.

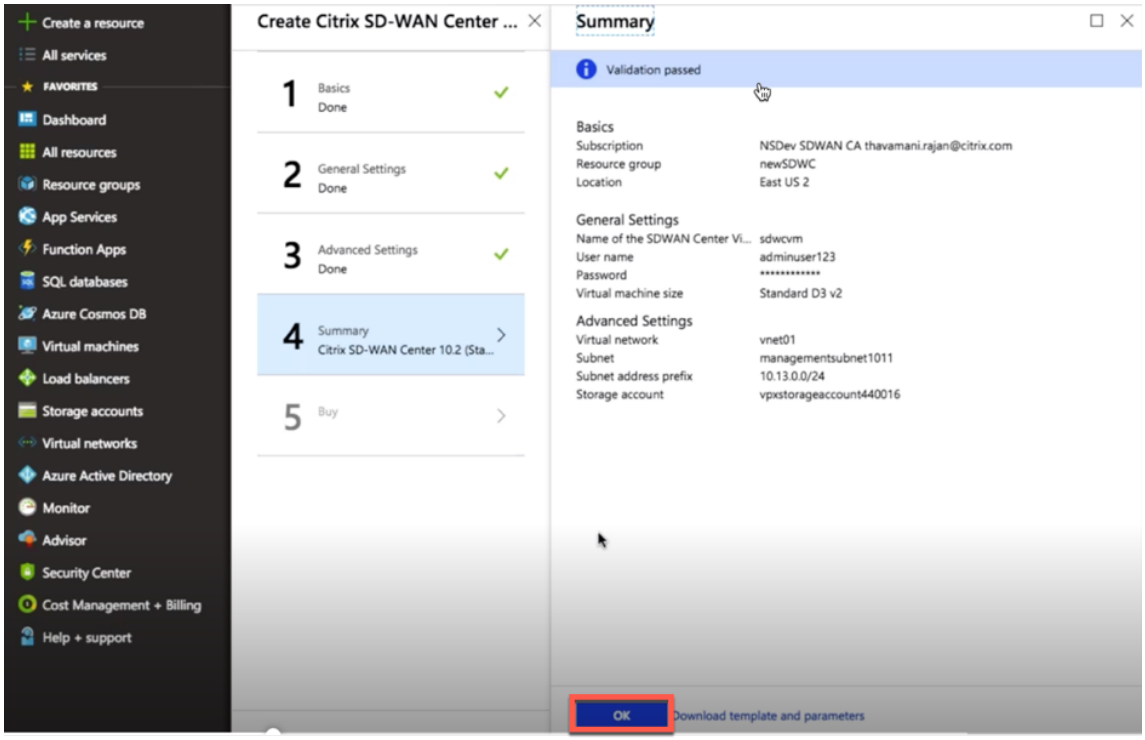


Wählen Sie ein virtuelles Netzwerk aus der verfügbaren Liste aus, oder Sie können ein neues virtuelles Netzwerk erstellen, indem Sie einen **Namen** und einen **Adressraum angeben**.

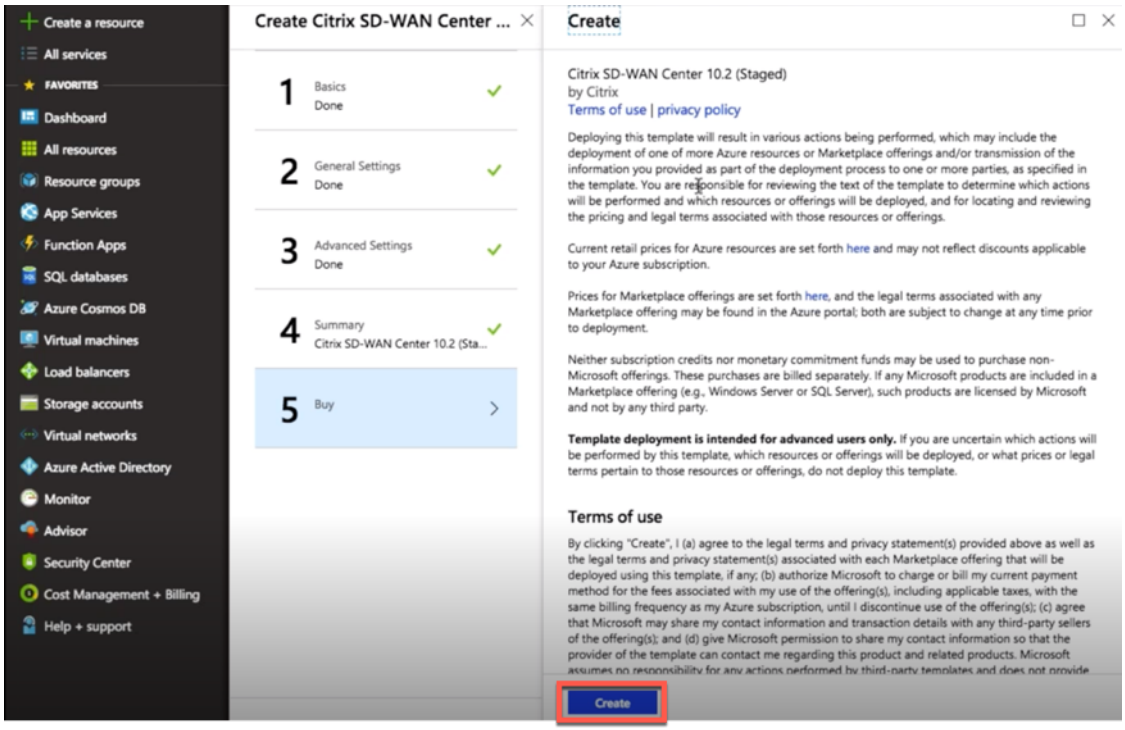


Wählen Sie **Subnetz** aus der Dropdownliste aus. Erstellen Sie ein **Speicherkonto**, und klicken Sie auf **OK**.

6. Die Konfiguration, die Sie in den vorherigen Schritten angegeben haben, wird überprüft und angewendet. Wenn Sie richtig konfiguriert haben, wird die Bestätigungsmeldung angezeigt. Klicken Sie auf **OK**.



7. Nach erfolgreicher Bereitstellung wird die Seite **Erstellen** angezeigt. Lesen Sie die **Nutzungsbedingungen und Datenschutzrichtlinien** sorgfältig durch und klicken Sie auf **Erstellen**.



Warten Sie, bis die VM-Bereitstellung abgeschlossen ist, und melden Sie sich dann mit der IP-Adresse an, die dieser VM zugewiesen wurde (indem Sie den Netzwerkabschnitt überprüfen und die Admin-

istratoranmeldeinformationen verwenden (die in Schritt 4 festgelegt wurden), und befolgen Sie die allgemeinen Bereitstellungsrichtlinien für SD-WAN Center.

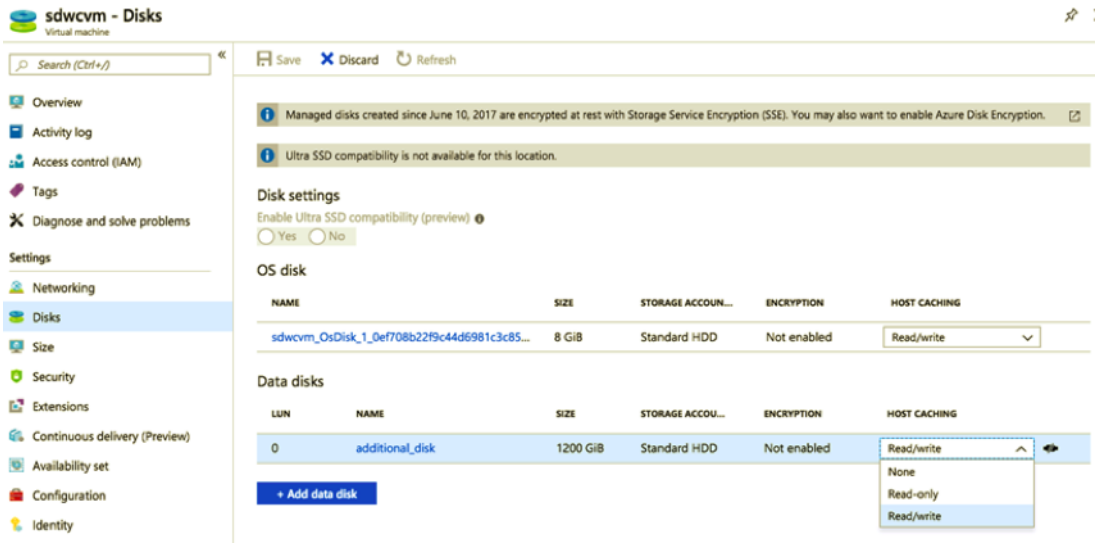
Datendatenträger hinzufügen

In diesem Abschnitt wird beschrieben, wie Sie mithilfe von eine neue verwaltete Datenfestplatte an eine virtuelle Maschine (VM) anfügenAzure-Portal. Die Größe des virtuellen Rechners bestimmt, wie viele Datendatenträger Sie anhängen können.

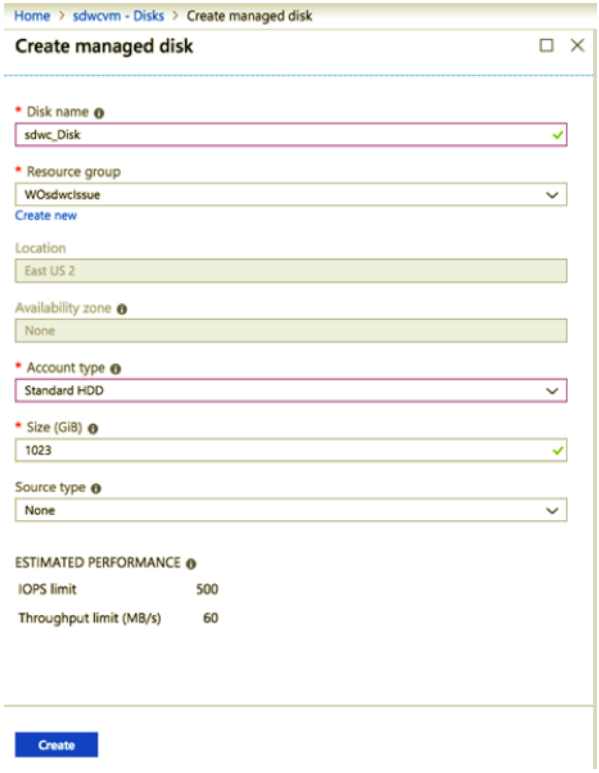
Wählen Sie im Azure-Portal im Menü auf der linken Seite die Option **Virtuelle Maschinen** aus, und wählen Sie eine virtuelle Maschine aus der Liste aus.

Führen Sie die folgenden Aktionen aus, um zusätzlichen Datenträger in Azure SD-WAN Center hinzuzufügen:

1. Fahren Sie die VM herunter.
2. Wählen Sie im VM-Dashboard unter **Einstellungen** die Option **Festplatten** aus.



3. Klicken Sie auf **+ Datenträger hinzufügen** und erstellen Sie einen neuen Datenträger mit Lese- und Schreibberechtigung.



Schließen Sie eine Festplatte an, indem Sie die folgenden obligatorischen Details ausfüllen:

- **Datenträgername** —Geben Sie einen Namen für das SD-WAN-Center-Datenträger an.
- **Ressourcengruppe** —Wählen Sie eine Ressourcengruppe aus der Dropdownliste aus.
- **Kontotyp** —Wählen Sie einen Kontotyp aus der Dropdownliste aus.
- **Größe (GIB)** —Geben Sie eine Größe in Gibibyte an.
- **Speichertyp** - Wählen Sie einen Quelltyp aus der Dropdownliste aus.

4. Wenn Sie fertig sind, klicken Sie auf **OK**.

Um die VM zu aktivieren, verweisen Sie auf dasWechseln des aktiven Speichers auf einen neuen DatenspeicherThema.

Citrix SD-WAN Center in AWS im VM importierbaren Image-Format

April 13, 2021

Das Citrix SD-WAN Center ist ein zentralisiertes Managementsystem oder eine einzige Glasverwaltungslösung, mit der Unternehmen alle Citrix SD-WAN-Appliances in ihrem WAN konfigurieren, überwachen und analysieren können.

Instanziieren einer virtuellen SD-WAN Center Appliance (AMI) in AWS

Sie benötigen ein AWS-Konto, um eine virtuelle SD-WAN Center-Appliance in einer AWS-VPC zu installieren. Sie können ein AWS-Konto erstellenhier. SD-WAN Center ist als Amazon Machine Image (AMI) im AWS Marketplace verfügbar.

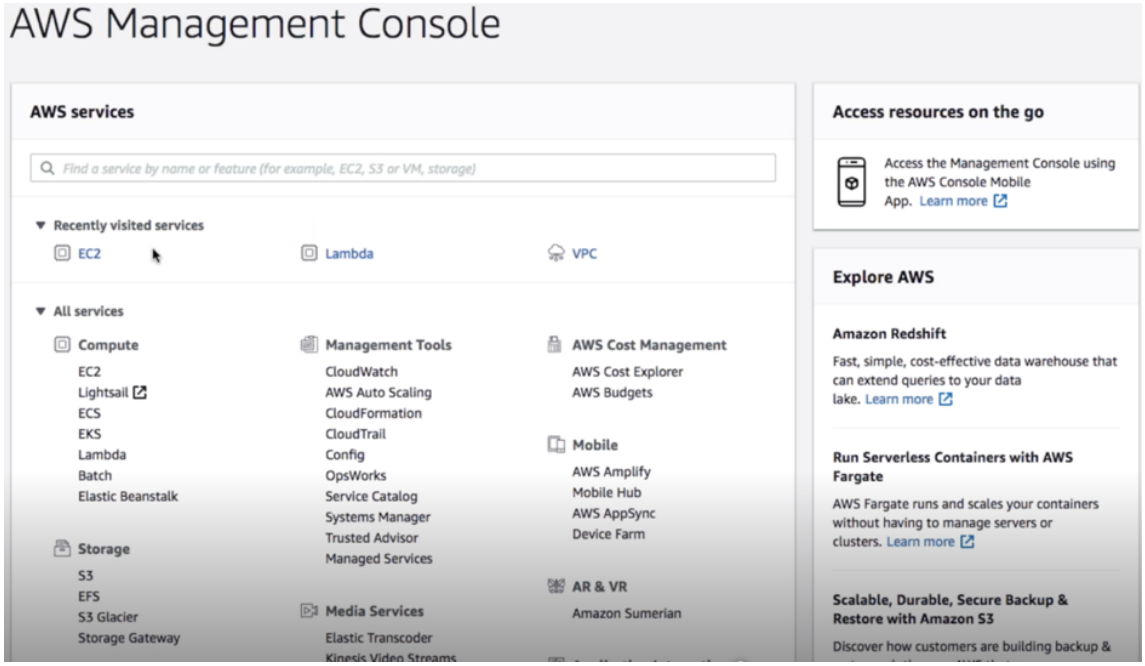
> **Hinweis:**
>
> Amazon nimmt häufig Änderungen an seinen AWS-Seiten vor, daher sind die folgenden Anweisungen möglicherweise nicht aktuell.

Es gibt zwei Ansätze, um eine virtuelle SD-WAN Center Appliance (AMI) in AWS zu instanziieren:

1. **Erster Ansatz:** Geben Sie in einem Webbrowser ein http://aws.amazon.com/. Wählen Sie AWS Management Console unter Mein Konto aus, um die Amazon Web Services (AWS) zu öffnen.

   Zweiter Ansatz:
   Geben Sie http://console.aws.amazon.com in einem Webbrowser ein, um die **Amazon Web Services** zu öffnen.

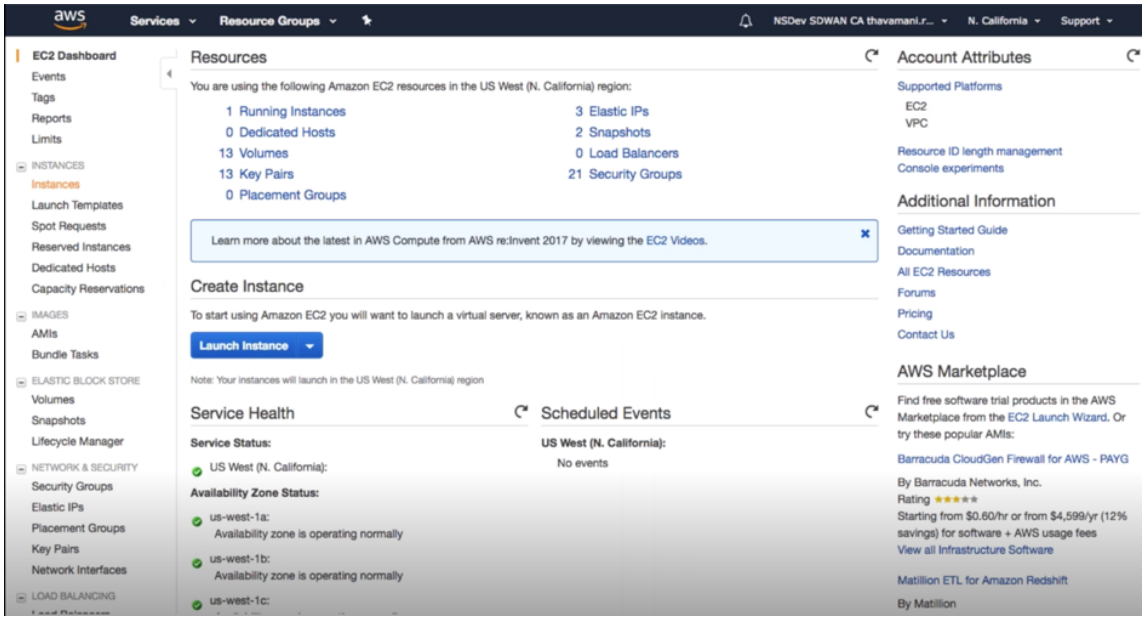
2. Verwenden Sie Ihre AWS-Kontoanmeldeinformationen, um sich anzumelden. Die Seite **Amazon Web Services** wird angezeigt. Sie können die Liste **Zuletzt besuchte Dienste** zusammen mit allen anderen Diensten anzeigen.

   Citrix SD-WAN Center-Appliances bieten die EC2 als AWS-Service-Instanzs an.

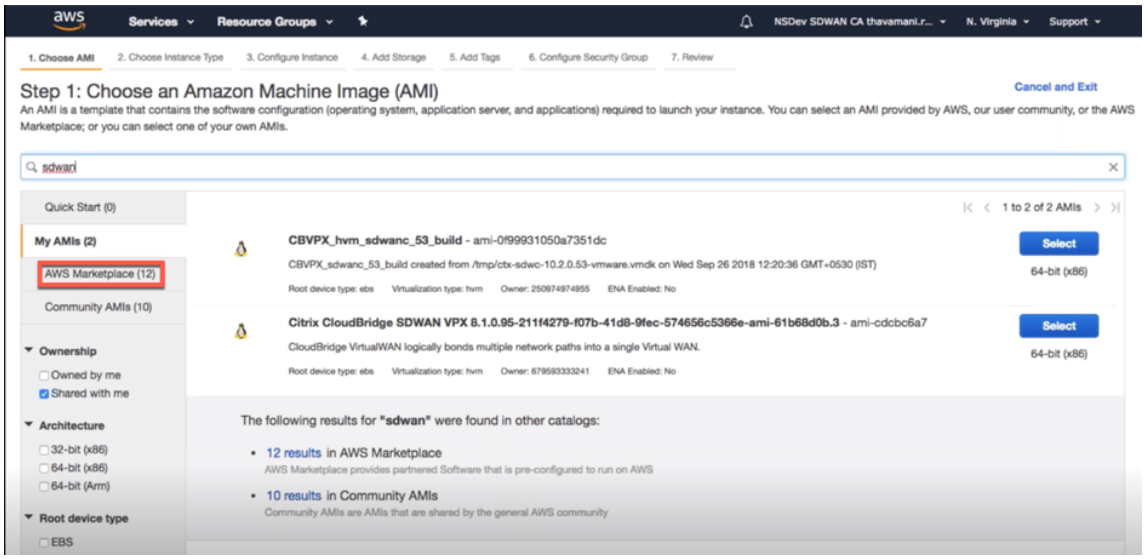
   - **EC2-Dashboard:** elastische Compute-Cloud, erweiterbare virtuelle Dienste/Instanzen

3. Klicken Sie im Abschnitt **Compute** auf **EC2**, und wählen Sie dann **Instanz starten** aus.



Sie können entweder die Option **Launch Instance** auswählen oder manuell zum Fenster **Instance** gelangen, indem Sie auf der linken Seite unter **Instances** den Speicherort der Option **INSTANCES** auswählen (siehe oben Screenshot).

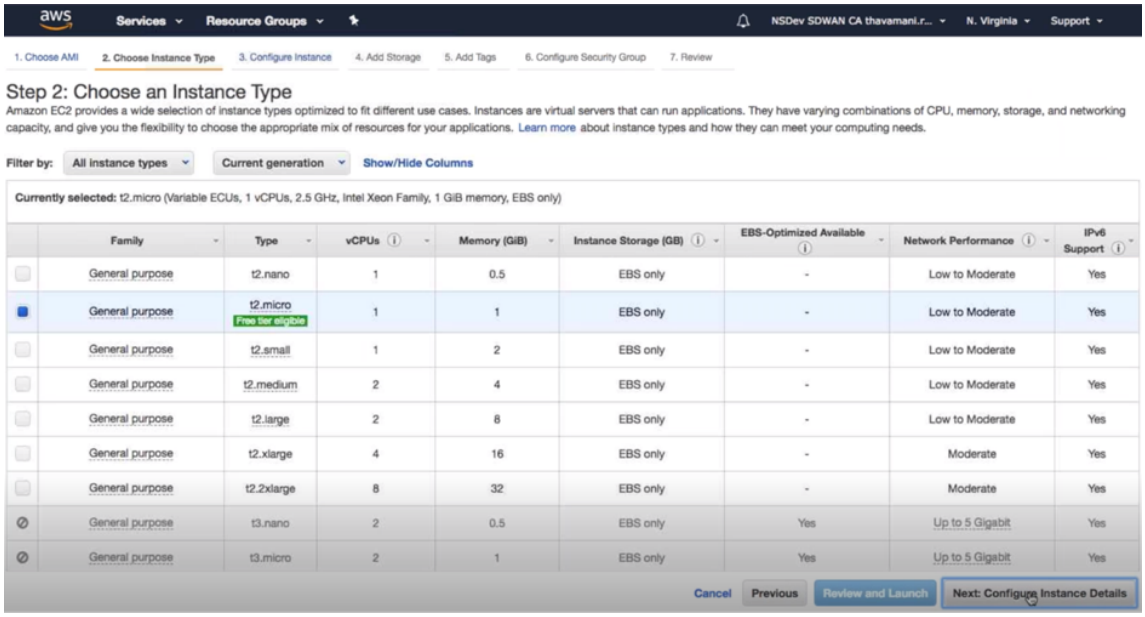
4. Klicken Sie auf der Seite **AMI auswählen** auf **AWS Marketplace**.
5. Geben Sie im Textfeld Suche SD-WAN ein, um nach dem SD-WAN-AMI zu suchen, und klicken Sie auf **Suchen**.



Wählen Sie auf der Suchergebnisseite eines der Citrix SD-WAN Center AMI mit der neuesten Version aus, und klicken Sie auf **Auswählen**.

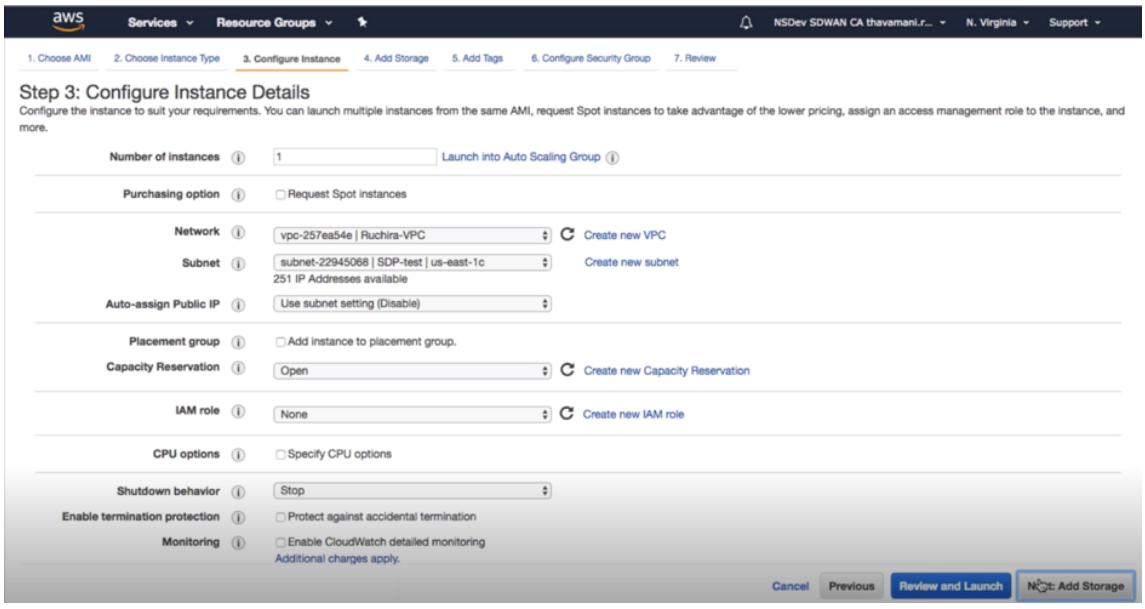
Eine **AMI-** Vorlage enthält die Softwarekonfiguration einschließlich Betriebssystem, Anwendungsserver und Anwendungen. Diese Vorlage ist erforderlich, um Instanzen zu starten.

6. Wählen Sie einen Instanztyp aus, und wählen Sie **Weiter: Instanzdetails konfigurieren**. Sie können Ihre Suche filtern, indem Sie einen bestimmten Instanztyp oder den gesamten Instanztyp mit aktueller Generierung auswählen.



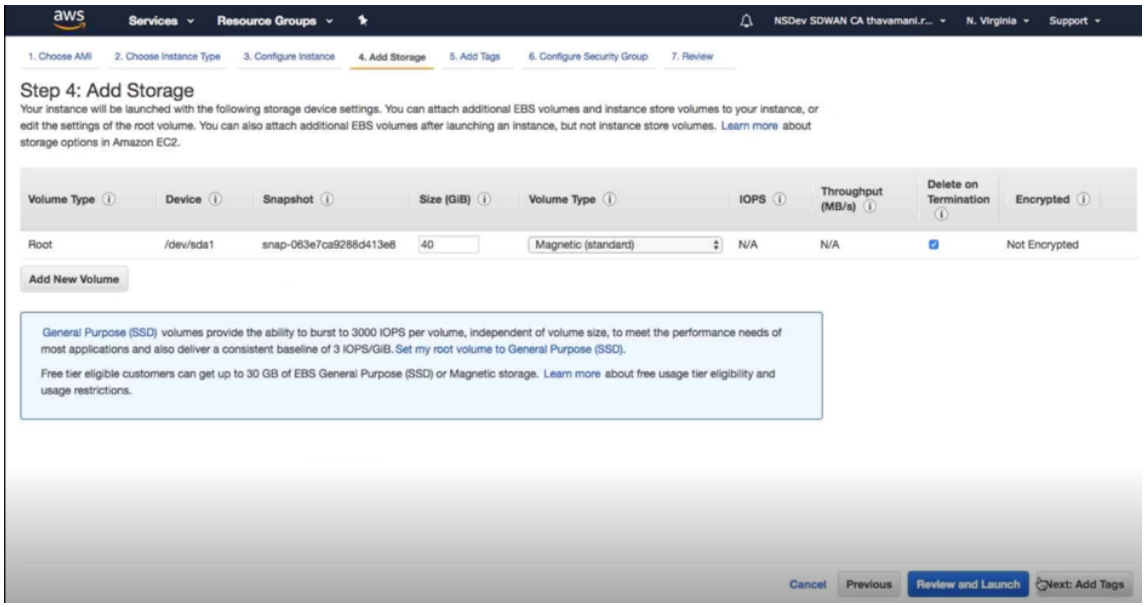
Amazon EC2 bietet eine große Auswahl an Instanz-Typen, die für verschiedene Anwendungsfälle optimiert wurden. Instanzen sind virtuelle Server, auf denen Anwendungen ausgeführt werden können.

7. Geben Sie auf der Seite **Instanz konfigurieren** in das Textfeld **Anzahl der Instanzen** 1 ein, und füllen Sie die anderen Details wie Netzwerk, Subnetz usw. für eine bestimmte Instanz nach Bedarf aus. Klicken Sie auf **Weiter: Speicher hinzufügen**.

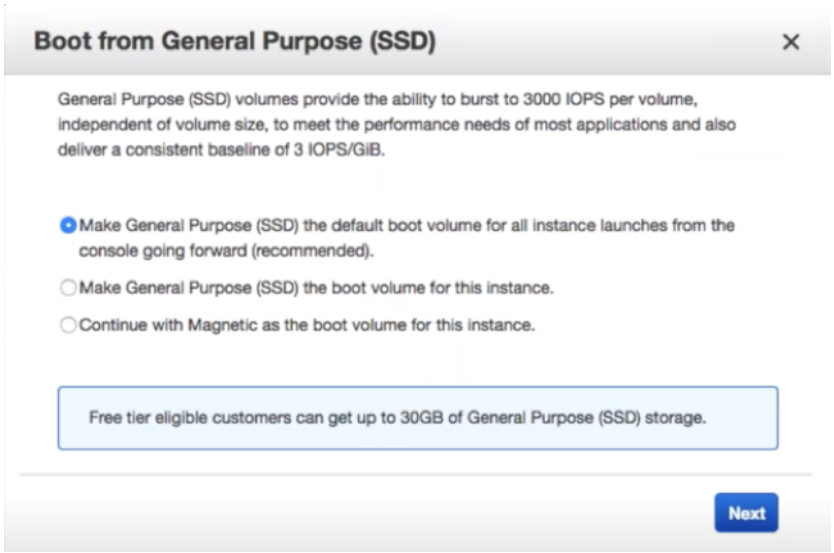


8. Die Instanz wird mit den Speichergeräteeinstellungen gestartet. Sie können ein neues Volume

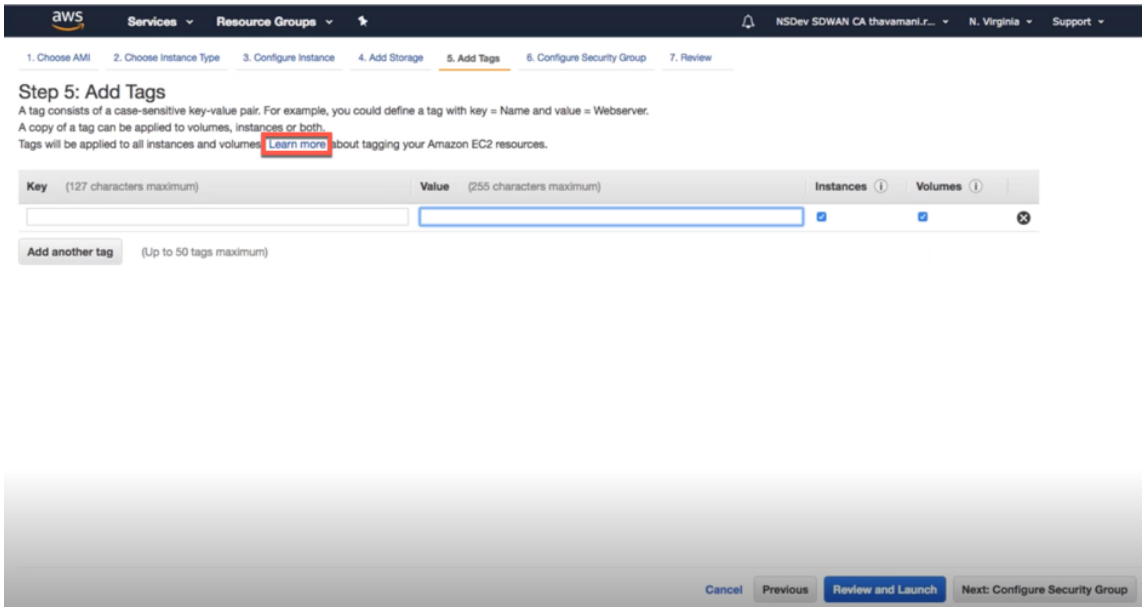
separat hinzufügen, sobald die Instanz bereitgestellt wurde.



9. Klicken Sie auf **Überprüfen und Starten**, um die Option Startvolume gemäß Ihrer Anforderung auszuwählen. Klicken Sie auf **Weiter**.



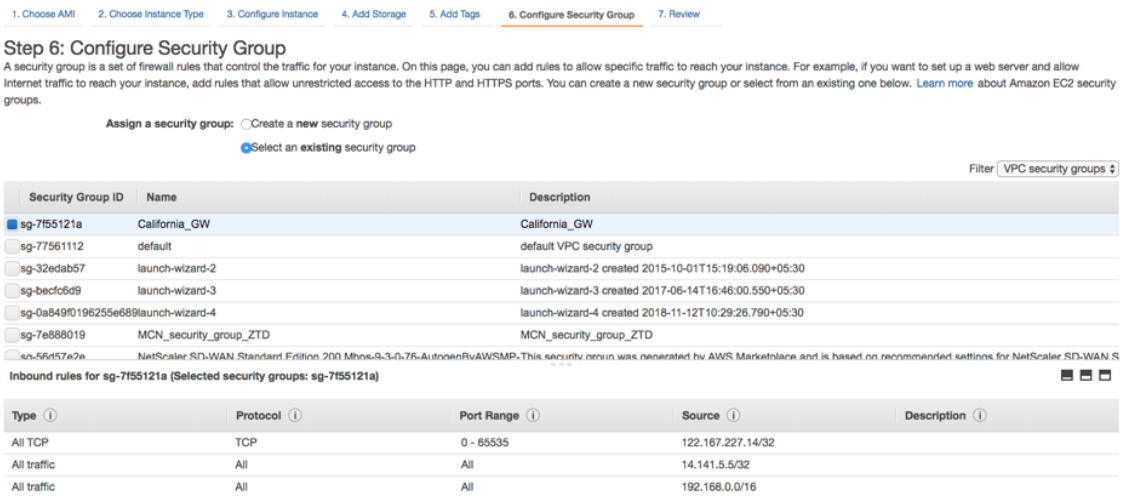
10. Fügen Sie ein Tag mit einem **Schlüsselnamen** und einem **Wert** hinzu oder definieren Sie es. Klicken Sie auf **Weitere** Informationen, um mehr über Tagging zu erfahren. Sie können maximal 50 Tags hinzufügen. Klicken Sie auf **Weiter: Sicherheitsgruppe konfigurieren**.



> **Hinweis:**
>
> HINWEIS: Eine Tag-Schlüssellänge muss zwischen 1 und 127 Zeichen betragen.

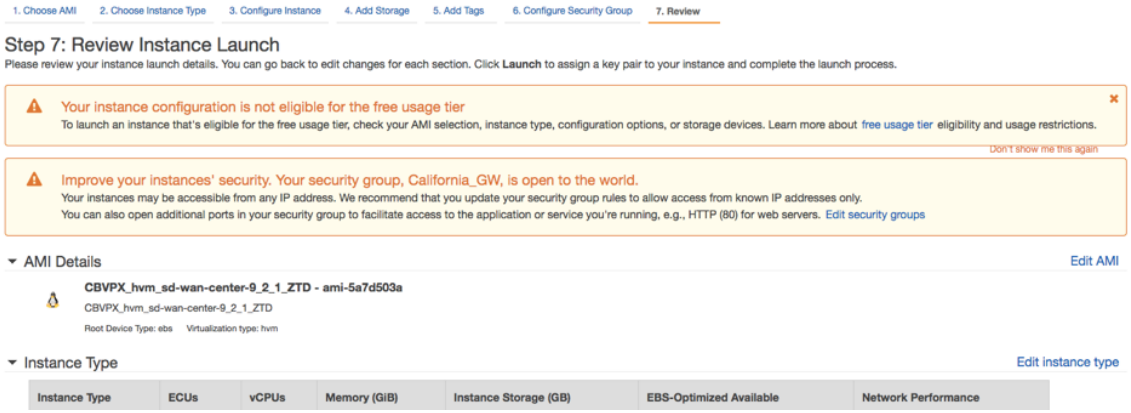
11. Sie können eine allgemeine Sicherheitsgruppe erstellen, die hilft, den Datenverkehr für die Instanz zu steuern. Sie können eine neue Sicherheitsgruppe erstellen oder eine vorhandene Sicherheitsgruppe aus der Liste auswählen.

> **Hinweis:**
>
> Stellen Sie sicher, dass die Sicherheitsgruppe es zulässt, dass eingehende Verbindungen über 2156 Port Daten von Citrix SD-WAN-Appliances sammelt.



12. Überprüfen Sie die Details zum Instanzstart, und klicken Sie dann auf **Starten**. Es erscheint ein Popup-Feld, in dem Sie aufgefordert werden, ein Schlüsselpaar zu erstellen. Es ist zwingend

erforderlich, ein Schlüsselpaar für die Instanz zu erstellen.



Zweistufige Authentifizierung

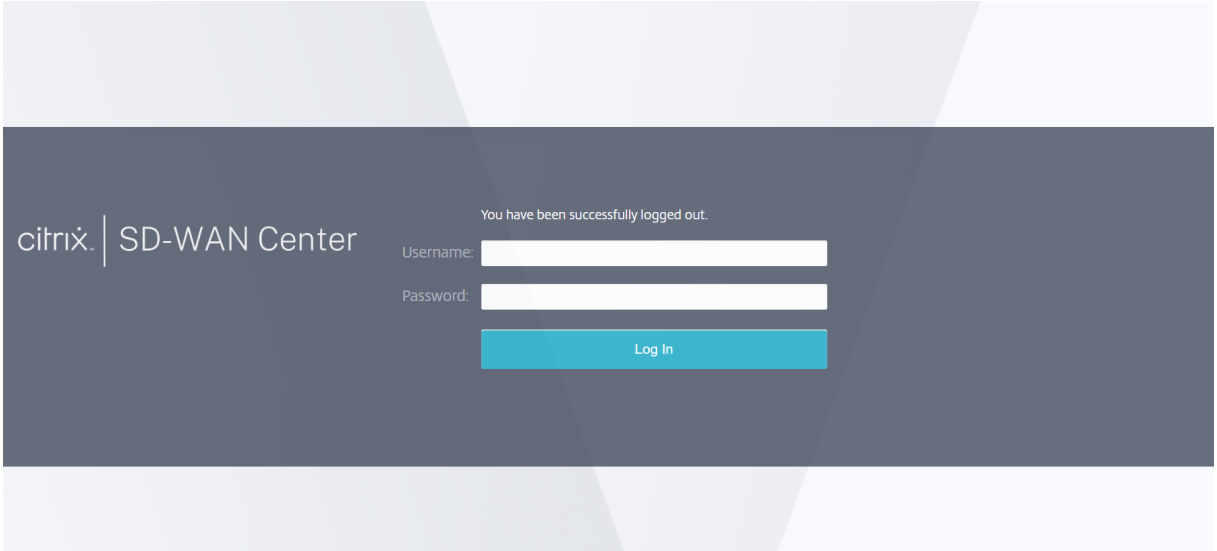
April 13, 2021

Die Zwei-Faktor-Authentifizierung (TFA) stellt zwei Authentifizierungsfaktoren für den Zugriff auf Citrix SD-WAN Center sowohl für lokale als auch für Remote-Benutzerkonten dar. Es führt eine zusätzliche Sicherheitsebene in der Citrix SD-WAN Center-Anmeldesequenz ein.

Die erste Authentifizierungsstufe für ein lokales Benutzerkonto wird mithilfe des in Citrix SD-WAN Center konfigurierten Kennworts erreicht. Weitere Informationen finden Sie unter Benutzerkonten.

Die erste Authentifizierungsstufe für ein Remote-Benutzerkonto wird mithilfe des primären RADIUS- oder TACACS + -Authentifizierungsservers erreicht. Weitere Informationen finden Sie unter Primäre Authentifizierung.

Ein zusätzlicher sekundärer RADIUS- oder TACACS + -Authentifizierungsserver kann sowohl für lokale als auch für Remote-Benutzerkonten konfiguriert werden, um die Zwei-Faktor-Authentifizierung zu aktivieren. Weitere Informationen finden Sie unter Sekundäre Authentifizierung.



Anmeldeinformationen für Citrix SD-WAN Center:

- **Benutzername**: Der im SD-WAN Center oder auf dem primären Authentifizierungsserver konfigurierte Benutzername.
- **Kennwort**: Das Kennwort, das auf dem SD-WAN Center oder dem primären Authentifizierungsserver konfiguriert ist.
- **Sekundäres Kennwort**: Das Kennwort, das auf dem sekundären Authentifizierungsserver konfiguriert ist.

> **Hinweis**
>
> Die Option **Sekundäres Kennwort** wird nur angezeigt, wenn der sekundäre Authentifizierungsserver konfiguriert ist.

Primäre Authentifizierung

April 13, 2021

Sie können Authentifizierungsserver wie RADIUS oder TACACS + konfigurieren, um Remotebenutzer zu authentifizieren, die sich bei Citrix SD-WAN Center anmelden. Die primäre Authentifizierung ist der erste Authentifizierungsfaktor für Remotebenutzer, wenn die Zwei-Faktor-Authentifizierung aktiviert ist. Weitere Informationen finden Sie unter Zweistufige Authentifizierung.

> **Hinweis**

> Stellen Sie sicher, dass Benutzerkonten auf den erforderlichen Authentifizierungsservern erstellt werden.

RADIUS-Authentifizierungsserver

Um die RADIUS-Authentifizierung zu verwenden, müssen Sie mindestens einen RADIUS-Server angeben und konfigurieren. Optional können Sie redundante Backup-Server mit bis zu drei RADIUS-Servern konfigurieren. Die Server werden sequenziell überprüft, beginnend mit dem Server, der zuerst im Abschnitt **Server** aufgeführt ist. Stellen Sie sicher, dass die erforderlichen Benutzerkonten auf dem RADIUS-Authentifizierungsserver erstellt werden.

So aktivieren und konfigurieren Sie die RADIUS-Authentifizierung:

1. Navigieren Sie in der Citrix SD-WAN Center-Weboberfläche zu **Administration** > **Benutzer-/Authentifizierungseinstellungen**.
2. Aktivieren Sie im Abschnitt **Primäre Authentifizierung** > **RADIUS-Authentifizierung** das Kontrollkästchen **RADIUS-Authentifizierung aktivieren**.

   > **Hinweis**
   >
   > Wenn die TACACS + -Authentifizierung bereits aktiviert ist, wird sie deaktiviert.

3. Geben Sie im Feld **Timeout** das Zeitintervall (in Sekunden) ein, das auf eine Authentifizierungsantwort vom RADIUS-Server gewartet werden soll.

   Der Zeitüberschreitungswert sollte kleiner oder gleich 10 Sekunden sein.
4. Geben Sie im Feld **Serverschlüssel** einen geheimen Schlüssel ein, der beim Herstellen einer Verbindung mit den RADIUS-Servern verwendet werden soll.
5. Geben Sie in die Felder **Serverschlüssel bestätigen** den geheimen Schlüssel erneut ein.

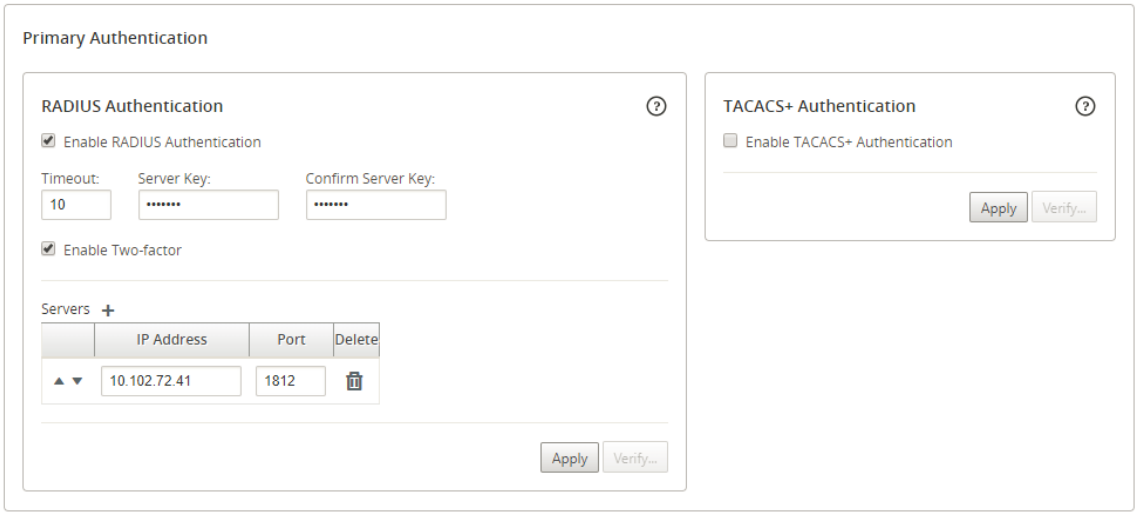
   > **Hinweis**
   >
   > Die Einstellungen **für Timeout** und **Serverschlüssel** werden auf alle konfigurierten Server angewendet**.**

6. Wählen Sie **Zwei-Faktor-Authentifizierung aktivieren** aus, um die Zwei-Faktor-Authentifizierung zu aktivieren.

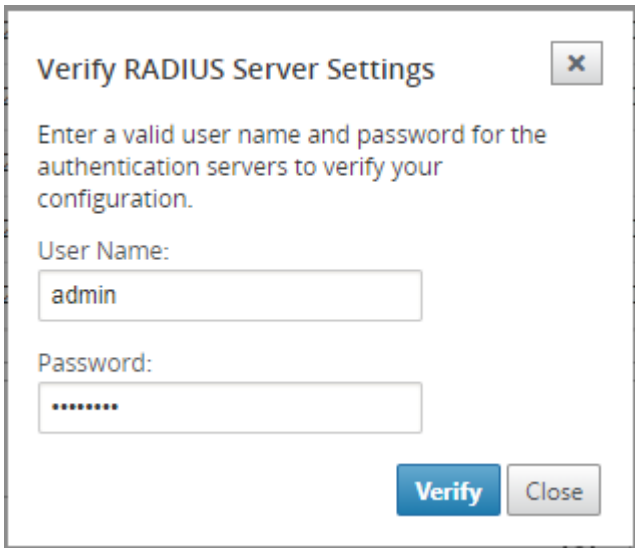
   > **Hinweis**
   >
   > Die Option **Zwei-Faktor-aktivieren** wird nur angezeigt, wenn der sekundäre Authentifizierungsserver konfiguriert ist.

> Konfigurieren Sie einen sekundären Authentifizierungsserver, entweder RADIUS oder TACAS +. Weitere Informationen finden Sie unter Sekundäre Authentifizierung.

7. Klicken Sie auf das Plussymbol (+) neben **Server**, um einen RADIUS-Server hinzuzufügen.
8. Geben Sie im Feld **IP-Adresse** die Host-IP-Adresse für den RADIUS-Server ein.
9. Geben Sie im Feld **Port** die Portnummer für den RADIUS-Server ein. Die Standardportnummer lautet 1812.



10. Klicken Sie auf **Apply**.
11. Klicken Sie auf **Überprüfen**, um die Verbindung zum RADIUS-Server zu überprüfen. Das Dialogfeld **RADIUS-Servereinstellungen überprüfen** wird angezeigt.



12. Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Authentifizierungsserver ein, und klicken Sie auf **Überprüfen**.

Um weitere Server zu konfigurieren, wiederholen Sie die Schritte 7 bis 12.

TACACS + Authentifizierungsserver

Um TACACS + zu verwenden, müssen Sie mindestens einen TACACS + -Server angeben und konfigurieren. Optional können Sie redundante Backup-Server mit bis zu drei TACACS + -Servern konfigurieren. Die Server werden sequenziell überprüft, beginnend mit dem Server, der zuerst im Abschnitt **Server** aufgeführt ist. Stellen Sie sicher, dass die erforderlichen Benutzerkonten auf dem TACACS + Authentifizierungsserver erstellt werden.

So aktivieren und konfigurieren Sie die TACACS + -Authentifizierung:

1. Navigieren Sie in der Citrix SD-WAN Center-Weboberfläche zu **Administration** > **Benutzer-/Authentifizierungseinstellungen**.
2. Aktivieren Sie im Abschnitt **Primäre Authentifizierung> TACACS+-Authentifizierung**das Kontrollkästchen**TACACS+-Authentifizierung aktivieren**.

   > **Hinweis**
   >
   > Wenn die RADIUS-Authentifizierung bereits aktiviert ist, wird sie deaktiviert.

3. Geben Sie im Feld **Timeout** das Zeitintervall (in Sekunden) ein, das auf eine Authentifizierungsantwort vom TACACS + -Server gewartet werden soll.

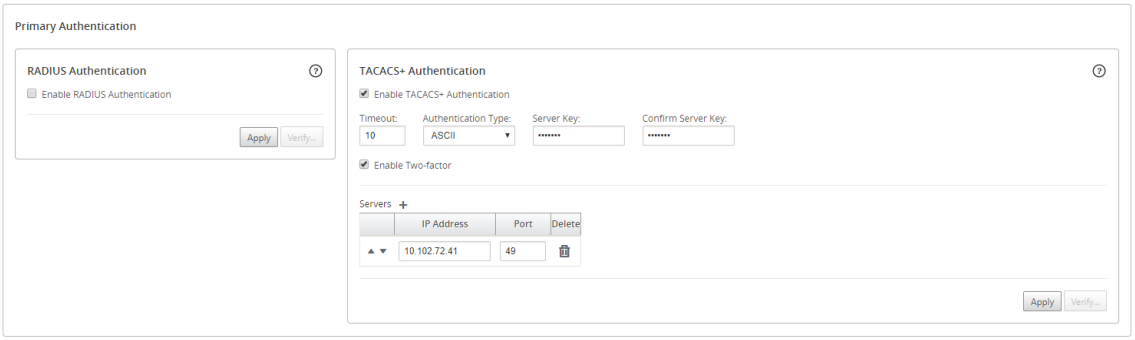
   Der Zeitüberschreitungswert sollte kleiner oder gleich 10 Sekunden sein.
4. Wählen Sie im Feld **Authentifizierungstyp** die Verschlüsselungsmethode aus, die verwendet werden soll, um den Benutzernamen und das Kennwort an den TACACS +-Server zu senden.
5. Geben Sie im Feld **Serverschlüssel** einen geheimen Schlüssel ein, der beim Herstellen einer Verbindung mit den TACACS +-Servern verwendet werden soll.
6. Geben Sie in die Felder **Serverschlüssel bestätigen** den geheimen Schlüssel erneut ein.

   > **Hinweis**
   >
   > Die Einstellungen **für Timeout**, **Authentifizierungstyp** und **Serverschlüssel** werden auf alle konfigurierten Server angewendet.

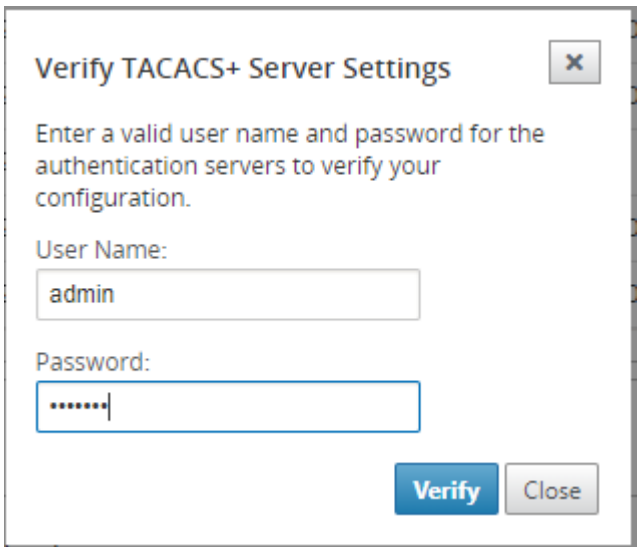
7. Wählen Sie **Zwei-Faktor-Authentifizierung aktivieren** aus, um die Zwei-Faktor-Authentifizierung zu aktivieren.

   > **Hinweis**
   >
   > Die Option **Zwei-Faktor-aktivieren** wird nur angezeigt, wenn der sekundäre Authentifizierungsserver konfiguriert ist.
   >
   > Konfigurieren Sie einen sekundären Authentifizierungsserver, entweder RADIUS oder TACAS +. Weitere Informationen finden Sie unter Sekundäre Authentifizierung.

8. Klicken Sie auf das Plus-Symbol (+) neben **Server**, um einen TACACS + -Server hinzuzufügen.
9. Geben Sie im Feld **IP-Adresse** die Host-IP-Adresse für den TACACS + -Server ein.
10. Geben Sie im Feld **Port** die Portnummer für TACACS + -Server ein. Die Standardportnummer ist 49.



11. Klicken Sie auf **Apply**.
12. Klicken Sie auf **Überprüfen**, um die Verbindung zum RADIUS-Server zu überprüfen. Das Dialogfeld **TACACS + Servereinstellungen überprüfen** wird angezeigt.



13. Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Authentifizierungsserver ein, und klicken Sie auf **Überprüfen**.

    Um weitere Server zu konfigurieren, wiederholen Sie die Schritte 8 bis 13.

Sekundäre Authentifizierung

April 13, 2021

Die sekundäre Authentifizierung ist so konfiguriert, dass die Zwei-Faktor-Authentifizierung für lokale und Remotebenutzerkonten aktiviert wird. Sie können entweder den RADIUS- oder TACACS + -Authentifizierungsserver als sekundären Authentifizierungsdienst konfigurieren. Weitere Informationen finden Sie unter Zweistufige Authentifizierung.

> **Hinweis**
>
> Stellen Sie sicher, dass Benutzerkonten auf den erforderlichen Authentifizierungsservern erstellt werden. Das Kennwort für das Benutzerkonto ist als zweiter Faktor in der Anmeldesequenz von Citrix SD-WAN Center zu verwenden.

Sekundärer RADIUS-Authentifizierungsserver

Um die RADIUS-Authentifizierung zu verwenden, müssen Sie mindestens einen RADIUS-Server angeben und konfigurieren. Optional können Sie redundante Backup-Server mit bis zu drei RADIUS-Servern konfigurieren. Die Server werden sequenziell überprüft, beginnend mit dem Server, der zuerst im Abschnitt **Server** aufgeführt ist. Stellen Sie sicher, dass die erforderlichen Benutzerkonten auf dem RADIUS-Authentifizierungsserver erstellt werden.

So aktivieren und konfigurieren Sie die RADIUS-Authentifizierung:

1. Navigieren Sie in der Citrix SD-WAN Center-Weboberfläche zu **Administration** > **Benutzer-/Authentifizierungseinstellungen**.
2. Aktivieren Sie im Abschnitt **Sekundäre Authentifizierung> RADIUS-Authentifizierung**das Kontrollkästchen**Sekundäre RADIUS-Authentifizierung aktivieren**.

   > **Hinweis**
   >
   > Wenn die TACACS + -Authentifizierung bereits aktiviert ist, wird sie deaktiviert.

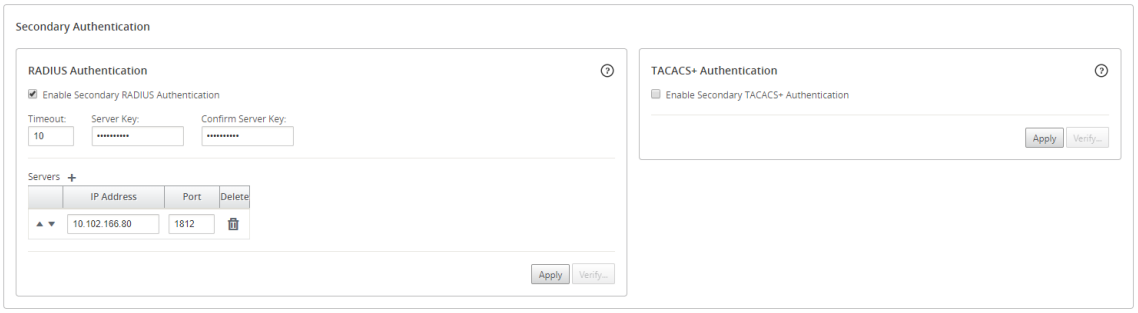
3. Geben Sie im Feld **Timeout** das Zeitintervall (in Sekunden) ein, das auf eine Authentifizierungsantwort vom RADIUS-Server gewartet werden soll.

   Der Zeitüberschreitungswert sollte kleiner oder gleich 10 Sekunden sein.
4. Geben Sie im Feld **Serverschlüssel** einen geheimen Schlüssel ein, der beim Herstellen einer Verbindung mit den RADIUS-Servern verwendet werden soll.
5. Geben Sie in die Felder **Serverschlüssel bestätigen** den geheimen Schlüssel erneut ein.

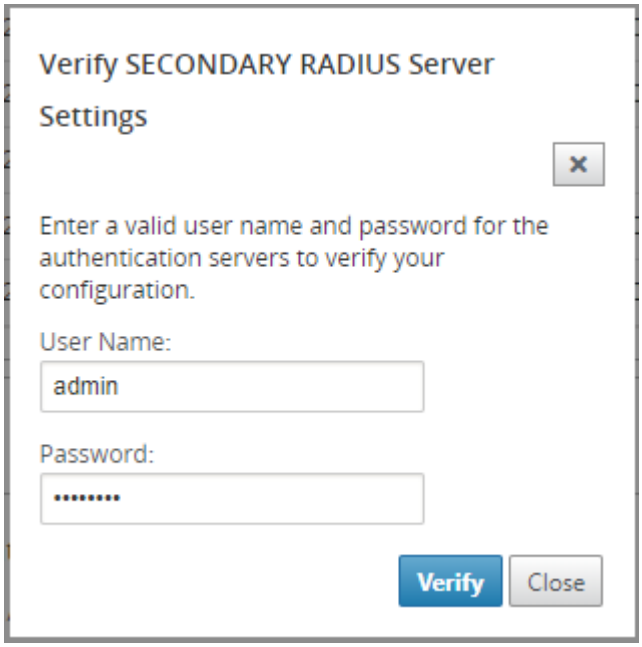
   > **Hinweis**
   >
   > Die Einstellungen **für Timeout** und **Serverschlüssel** werden auf alle konfigurierten Server angewendet**.**

6. Klicken Sie auf das Plussymbol (+) neben **Server**, um einen RADIUS-Server hinzuzufügen.

7. Geben Sie im Feld **IP-Adresse** die Host-IP-Adresse für den RADIUS-Server ein.
8. Geben Sie im Feld **Port** die Portnummer für den RADIUS-Server ein. Die Standardportnummer lautet 1812.



9. Klicken Sie auf **Apply**.
10. Klicken Sie auf **Überprüfen**, um die Verbindung zum RADIUS-Server zu überprüfen. Das Dialogfeld **Secondary RADIUS-Servereinstellungen überprüfen** wird angezeigt.



11. Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Authentifizierungsserver ein, und klicken Sie auf **Überprüfen**.

Um weitere Server zu konfigurieren, wiederholen Sie die Schritte 6 bis 11.

Sekundärer TACACS + Authentifizierungsserver

Um TACACS + zu verwenden, müssen Sie mindestens einen TACACS + -Server angeben und konfigurieren. Optional können Sie redundante Backup-Server mit bis zu drei TACACS + -Servern konfigurieren.

Die Server werden sequenziell überprüft, beginnend mit dem Server, der zuerst im Abschnitt **Server** aufgeführt ist. Stellen Sie sicher, dass die erforderlichen Benutzerkonten auf dem TACACS + Authentifizierungsserver erstellt werden.

So aktivieren und konfigurieren Sie die TACACS + -Authentifizierung:

1. Navigieren Sie in der SD-WAN Center-Weboberfläche zu **Administration** > **Benutzer-/Authentifizierungseinstellungen**.
2. Aktivieren Sie im Abschnitt **Sekundäre Authentifizierung** > **TACACS+-Authentifizierung** das Kontrollkästchen **Sekundäre TACACS+-Authentifizierung aktivieren**.

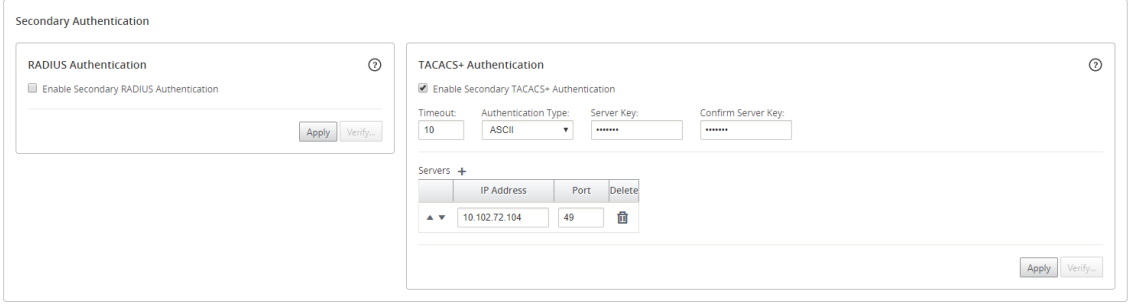
   > **Hinweis**
   >
   > Wenn die RADIUS-Authentifizierung bereits aktiviert ist, wird sie deaktiviert.

3. Geben Sie im Feld **Timeout** das Zeitintervall (in Sekunden) ein, das auf eine Authentifizierungsantwort vom TACACS + -Server gewartet werden soll.

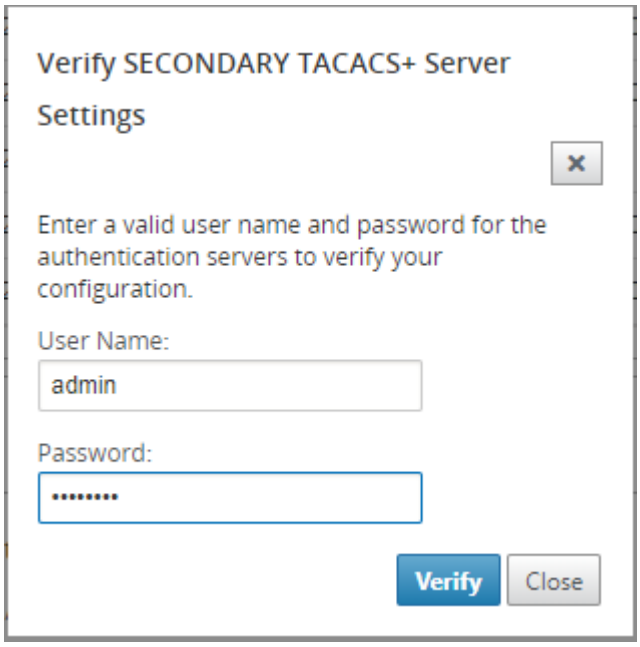
   Der Zeitüberschreitungswert sollte kleiner oder gleich 10 Sekunden sein.
4. Wählen Sie im Feld **Authentifizierungstyp** die Verschlüsselungsmethode aus, die verwendet werden soll, um den Benutzernamen und das Kennwort an den TACACS +-Server zu senden.
5. Geben Sie im Feld **Serverschlüssel** einen geheimen Schlüssel ein, der beim Herstellen einer Verbindung mit den TACACS +-Servern verwendet werden soll.
6. Geben Sie in die Felder **Serverschlüssel bestätigen** den geheimen Schlüssel erneut ein.

   > **Hinweis**
   >
   > Die Einstellungen **für Timeout**, **Authentifizierungstyp** und **Serverschlüssel** werden auf alle konfigurierten Server angewendet.

7. Klicken Sie auf das Plus-Symbol (+) neben **Server**, um einen TACACS + -Server hinzuzufügen.
8. Geben Sie im Feld **IP-Adresse** die Host-IP-Adresse für den TACACS + -Server ein.
9. Geben Sie im Feld **Port** die Portnummer für TACACS + -Server ein. Die Standardportnummer ist 49



10. Klicken Sie auf **Apply**.
11. Klicken Sie auf **Überprüfen**, um die Verbindung zum RADIUS-Server zu überprüfen. Das Dialogfeld **TACACS + Servereinstellungen überprüfen** wird angezeigt.



12. Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Authentifizierungsserver ein, und klicken Sie auf **Überprüfen**.

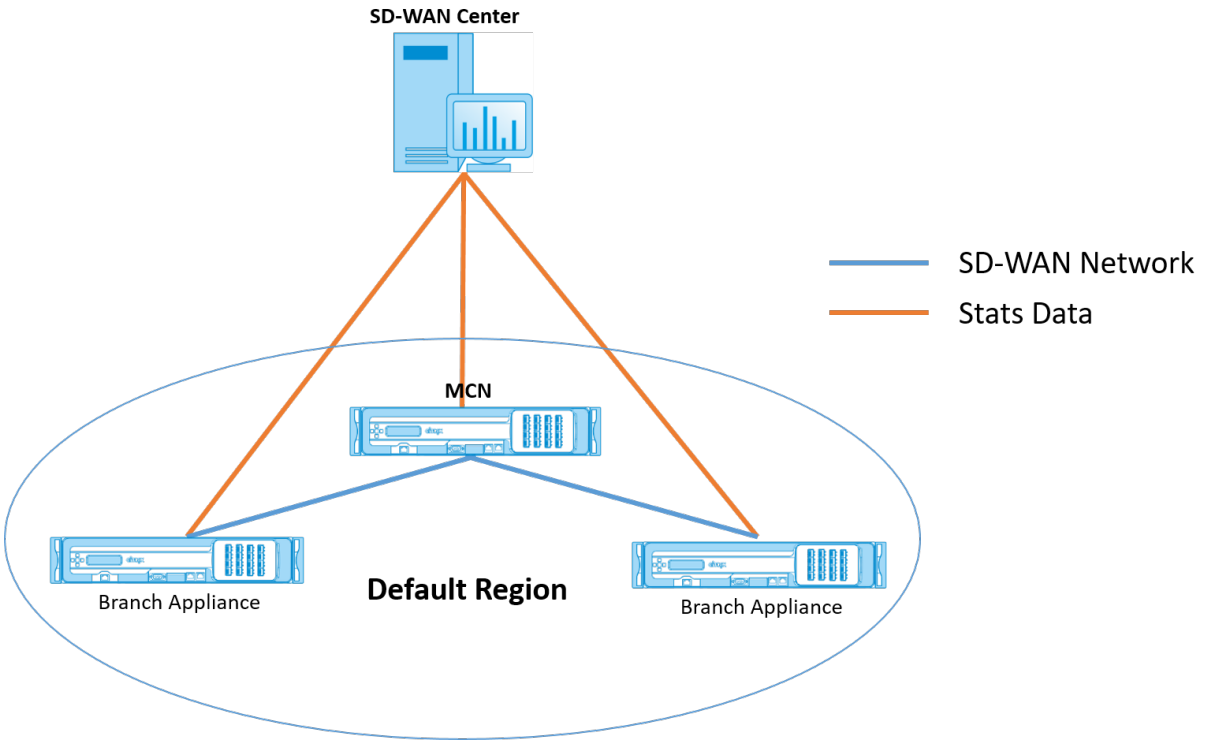
    Um weitere Server zu konfigurieren, wiederholen Sie die Schritte 7 bis 12.

Netzwerkbereitstellung in einer Region

April 13, 2021

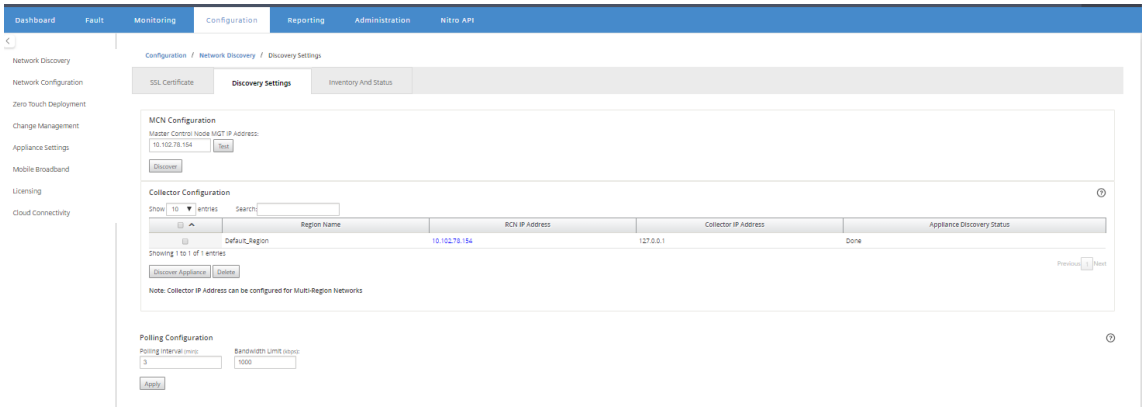
Wenn Ihr Unternehmen über ein kleines Netzwerk verfügt, das eine einzige administrative (oder geografische) Grenze umfasst, können Sie Citrix SD-WAN Center im Standardmodus verwenden (mit einer einzigen “Standardregion”). Eine Region kann maximal 550 Standorte unterstützen.

Ein einzelnes Regionennetzwerk verfügt über einen Master Control Node (MCN) für die zentrale Steuerung und Citrix SD-WAN Center für die zentrale Verwaltung. Der mit dem MCN verknüpfte und von ihm kontrollierte Bereich wird als Standardregion bezeichnet. Das Citrix SD-WAN Center fragt den MCN und alle Zweiggeräte im Standardbereich ab.



So stellen Sie Citrix SD-WAN Center für eine Region bereit:

1. Laden Sie die Citrix SD-WAN Center Software herunter. Weitere Informationen finden Sie unter Systemanforderungen und Installation.
2. [Installieren Sie das Citrix SD-WAN Center aufESXi-Server[],XenServer,[]Hyper-V()oderAzure[].]
3. Konfigurieren der Verwaltungsschnittstelleneinstellungen. Weitere Informationen finden Sie unter Konfigurieren der Verwaltungsschnittstelleneinstellungen.
4. Generieren, herunterladen und installieren Sie das SD-WAN MCN SSL-Zertifikat auf dem SD-WAN Center. Weitere Informationen finden Sie unter Installieren des Citrix SD-WAN SSL-Zertifikats.
5. Generieren, herunterladen und installieren Sie das SD-WAN Center SSL-Zertifikat auf der MCN-Appliance. Weitere Informationen finden Sie unter Installieren des Citrix SD-WAN Center SSL-Zertifikats.
6. Navigieren Sie in der Benutzeroberfläche von Citrix SD-WAN Center zu **Konfiguration** > **Netzwerkerkennung** > **Discoveryeinstellungen**.
7. Geben Sie im Feld **Master Controller Node MGT IP Address** die MCN-IP-Adresse ein, und klicken Sie auf **Test**. Dadurch wird eine Verbindung zwischen dem MCN und dem Citrix SD-WAN Center hergestellt.



8. Klicken Sie auf **Entdecken**. Wenn Sie bereits ein MCN entdeckt haben, ändert sich diese Option in **Rediscover**.

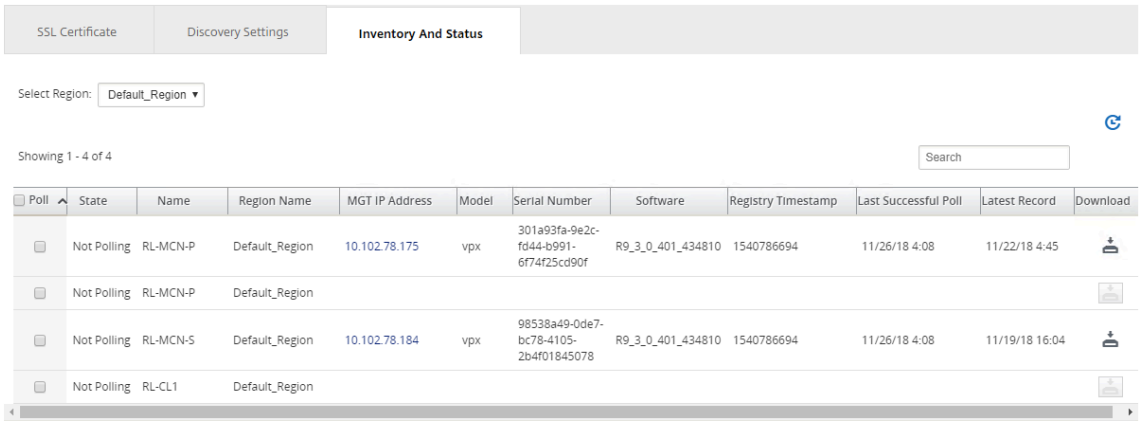
   > **Hinweis**
   >
   > Der MCN muss aktiv sein und der SD-WAN-Dienst sollte aktiviert sein. Weitere Informationen finden Sie unter Aktivieren des SD-WAN-Dienstes.

9. Klicken Sie nach Abschluss des Ermittlungsvorgangs auf die Registerkarte **Inventar und Status**.

   In der Tabelle **Inventory und Status** werden die Statusinformationen für alle erkannten Citrix SD-WAN-Appliances angezeigt.

10. Aktivieren Sie das Kontrollkästchen **Abfragen** in der oberen linken Ecke der Tabellenüberschrift.

    Dadurch wird das Kontrollkästchen **Abfragen** für jede in der Tabelle aufgelistete Appliance aktiviert. Deaktivieren Sie das Kontrollkästchen, um eine Appliance aus der Abfrageliste auszuschließen.



11. Klicken Sie auf **Apply**.

    > **Tipp**
    >
    > Sie können die Speichergröße des Citrix SD-WAN Center erhöhen, indem Sie einen Data Store auf der virtuellen Maschine erstellen und den Data Store wechseln. Weitere Informa-

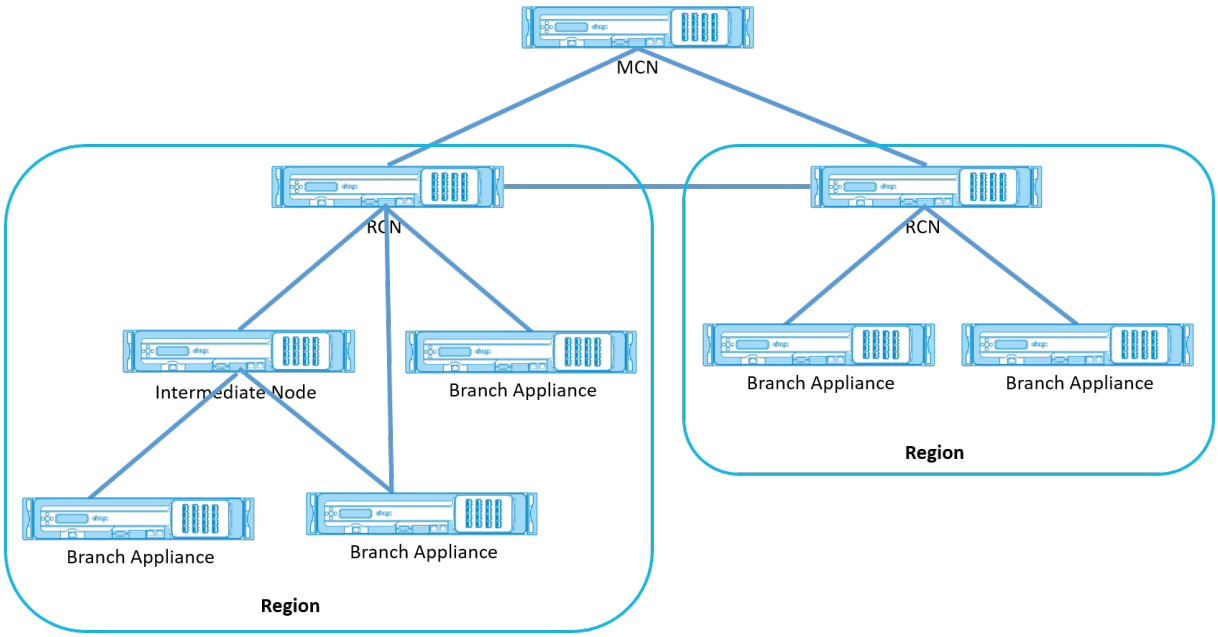
> tionen, siehe Wechseln des aktiven Speichers auf einen neuen Datenspeicher.

Netzwerkbereitstellung in mehreren Regionen

April 13, 2021

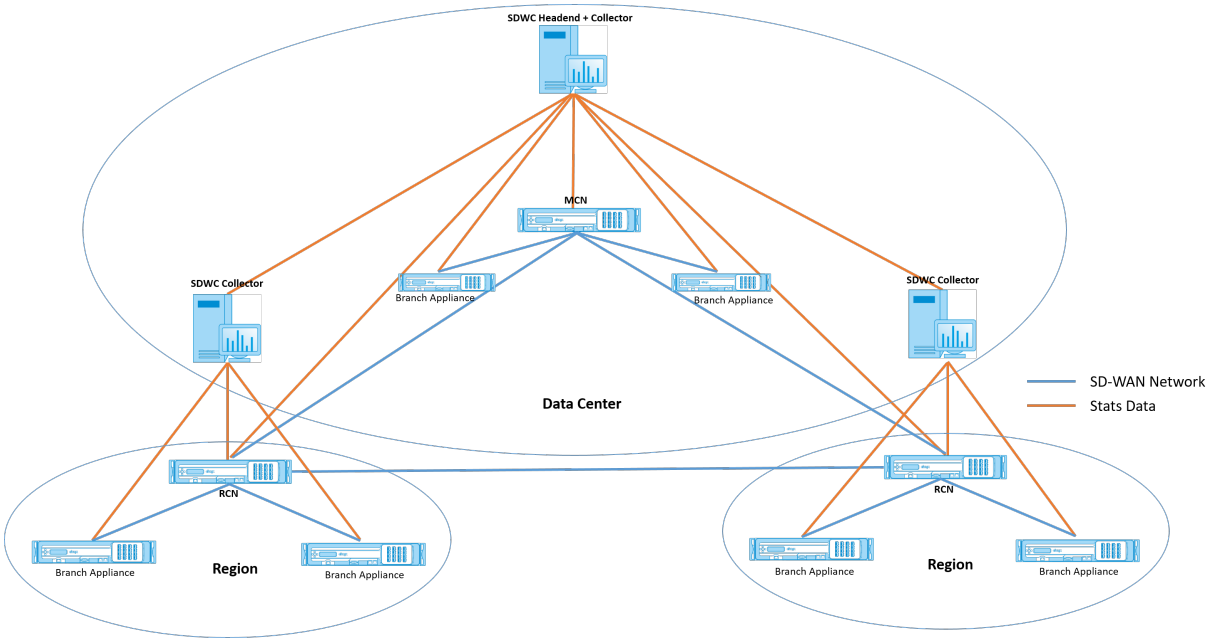
Wenn Ihr Unternehmen über ein großes Netzwerk verfügt, das mehrere administrative (oder geografische) Grenzen umfasst, können Sie Citrix SD-WAN Center im Modus mit mehreren Regionen verwenden, wobei jede Region maximal 550 Standorte unterstützt.

Das Netzwerk mit mehreren Regionen unterstützt eine hierarchische Architektur mit einem Master Control Node (MCN), der mehrere Regional Control Nodes (RCNs) steuert. Jeder RCN steuert wiederum mehrere Client-Sites. Das MCN kann optional auch verwendet werden, um einige Client-Standorte direkt als Teil der "Standardregion"zu steuern. Diese hierarchische und verteilte Architektur ermöglicht einen höheren Maßstab und eine effektive Delegierung der regionalen Verwaltung.



Das Citrix SD-WAN Center fragt MCN, RCNs und alle zugehörigen Zweigstellen ab.

Für die mehrregionale Citrix SD-WAN Center-Architektur ist ein Kollektor pro Region erforderlich, um Daten und Statistiken auf Regionsebene zu erfassen und zu speichern. Diese verteilte Architektur ermöglicht eine höhere Skalierung über mehrere Regionen hinweg, während die "Single Pane of Glass" -Ansicht für die Verwaltung des gesamten Netzwerks beibehalten wird.



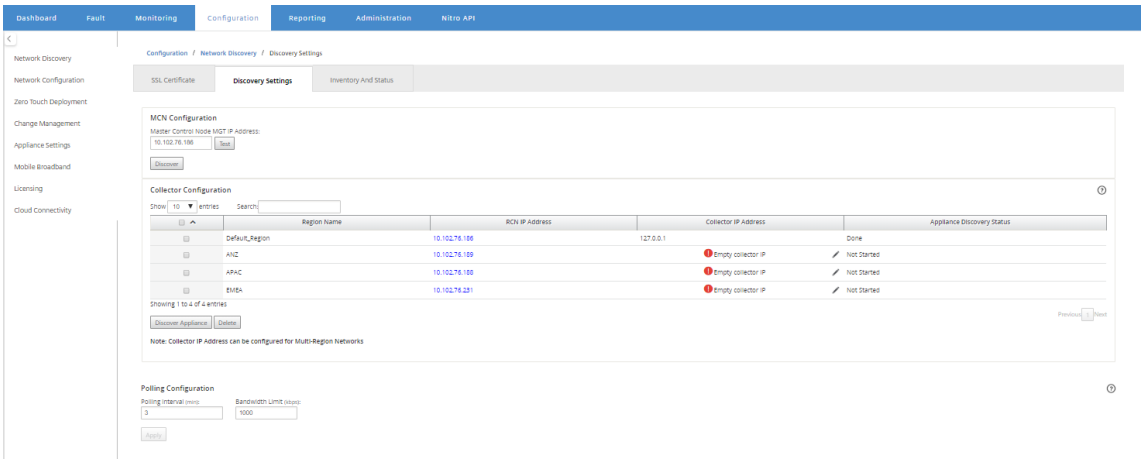
> **Hinweis**
>
> Bei einer Bereitstellung mit mehreren Regionen enthalten die Standardregionsstatistiken Statistiken aller Standorte, die vom MCN und dem RCN verwaltet werden. Die RCN-Daten werden jedoch nicht auf dem SD-WAN Center Collector gespeichert. Der SD-WAN Center Collector holt die RCN-Standortdaten von den jeweiligen regionalen Kollektoren ab.

So stellen Sie Citrix SD-WAN Center für mehrere Regionen bereit:

1. Laden Sie die Citrix SD-WAN Center Software herunter. Weitere Informationen finden Sie unter Systemanforderungen und Installation.
2. [Installieren Sie das Citrix SD-WAN Center aufESXi-Server,[]XenServer,[]Hyper-V()oderAzure.[]]
3. Konfigurieren der Verwaltungsschnittstelleneinstellungen. Weitere Informationen siehe Konfigurieren der Verwaltungsschnittstelleneinstellungen.
4. Generieren, herunterladen und installieren Sie das SD-WAN MCN SSL-Zertifikat auf dem SD-WAN Center. Weitere Informationen finden Sie unter Installieren des Citrix SD-WAN SSL-Zertifikats.
5. Generieren, herunterladen und installieren Sie das SD-WAN Center SSL-Zertifikat auf der MCN-Appliance. Weitere Informationen finden Sie unter Installieren des Citrix SD-WAN Center SSL-Zertifikats.
6. Navigieren Sie in der Benutzeroberfläche von Citrix SD-WAN Center zu **Konfiguration** > **Netzwerkerkennung** > **Discoveryeinstellungen**.
7. Geben Sie im Feld **Master Controller Node MGT IP Address** die MCN-IP-Adresse ein, und klicken Sie auf **Test**. Dadurch wird eine Verbindung zwischen dem MCN und dem Citrix SD-WAN Center hergestellt.

8. Klicken Sie auf **Entdecken**. Eine Liste aller mit dem MCN verbundenen RCNs wird im Abschnitt **Collector Configuration** angezeigt. Um die nicht standardmäßigen Regionssites zu ermitteln, benötigen Sie einen aktiven RCN mit aktiven Pfaden zu MCN.

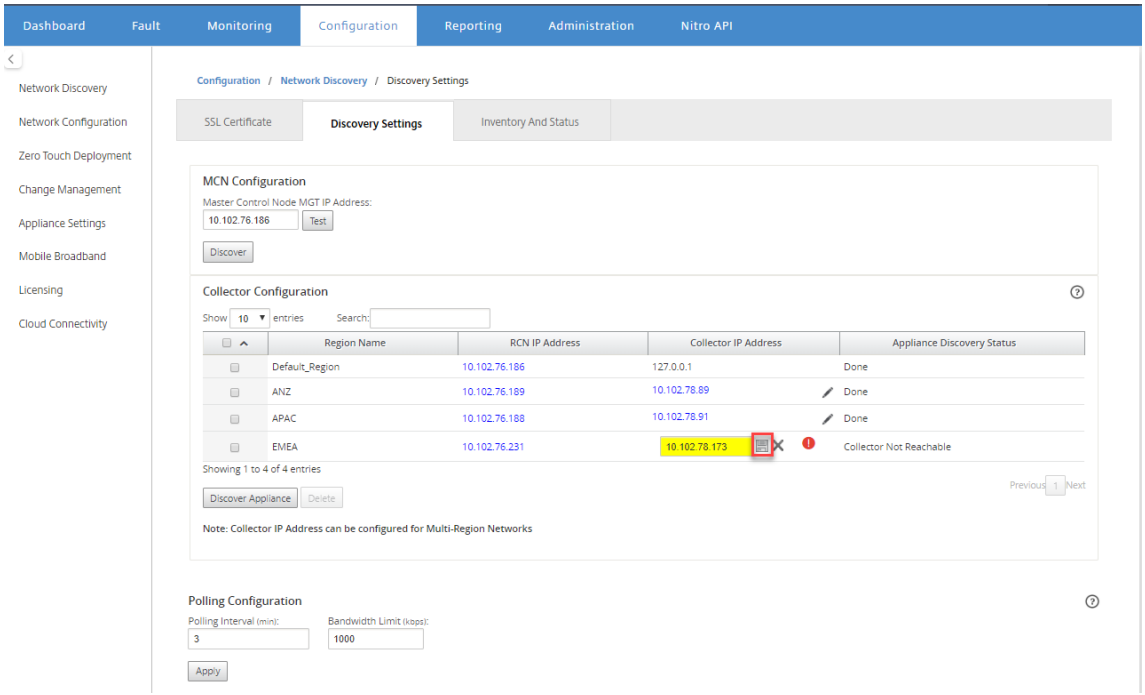
> **Hinweis**
>
> Das Citrix SD-WAN Center fungiert als Collector für den Standardbereich.



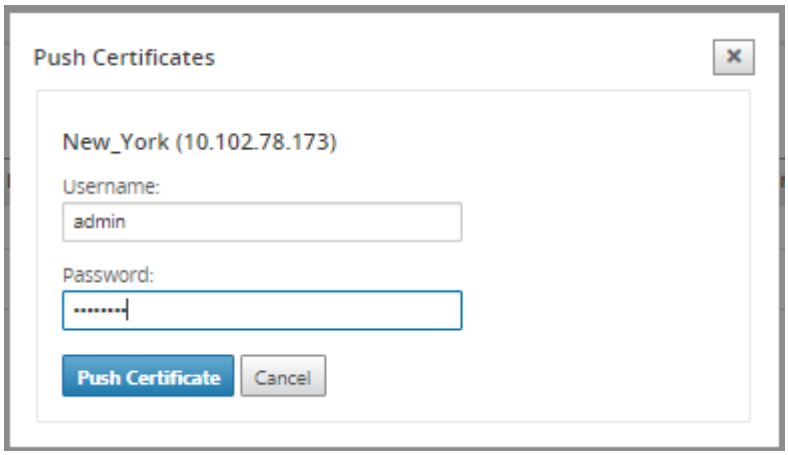
9. Klicken Sie auf das Symbol Bearbeiten, und geben Sie im Feld **Collector IP** die IP-Adresse des Citrix SD-WAN Center ein, das Sie als Collector für eine Region konfigurieren möchten.

> **Hinweis**
>
> Installieren Sie zum Einrichten eines Collectors eine Citrix SD-WAN Center-VM und konfigurieren Sie die Management-IP-Adresse. Die Management-IP-Adresse dieses Citrix SD-WAN Centers ist die Collector-IP-Adresse.

10. Klicken Sie auf das Symbol Speichern, um die Collector-IP-Adresse zu speichern und das Certificate-Key-Paar an das RCN zu übertragen.

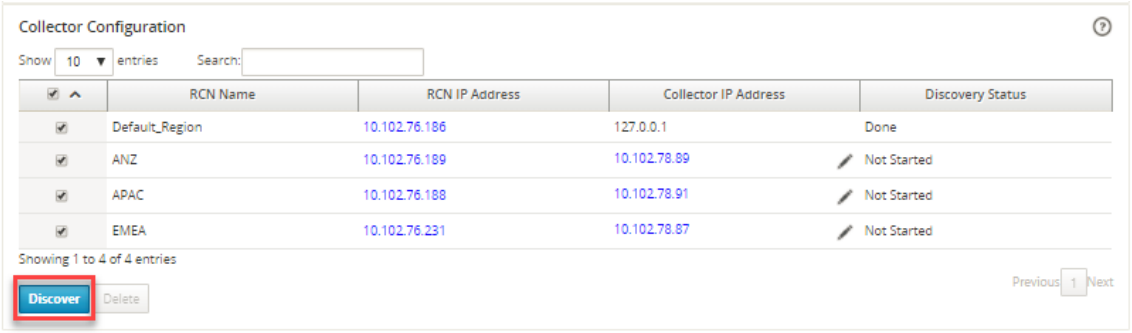


11. Geben Sie die Anmeldeinformationen für den RCN ein, und klicken Sie auf **Push Certificate**.

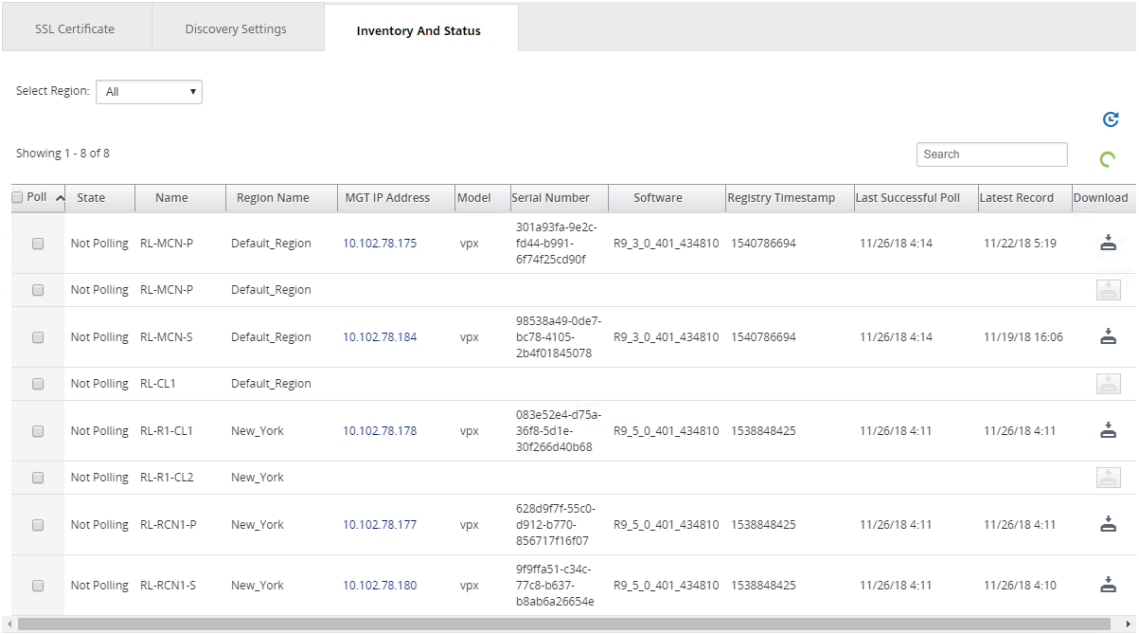


12. Konfigurieren Sie in ähnlicher Weise die Collector-IP-Adresse für alle RCNs.

> **Hinweis**
>
> Die Appliances werden automatisch alle 30 Minuten erkannt. Wenn neue RCNs zum Netzwerk hinzugefügt werden und eine Änderungsverwaltung abgeschlossen ist, können Sie die Appliance auswählen und auf **Discover Appliance** klicken, um die Appliance sofort zu ermitteln.



Nachdem der **Ermittlungsstatus** in **Fertig** geändert wurde, können Sie die erkannten Sites auf der Seite **"Inventar und Status** "anzeigen.



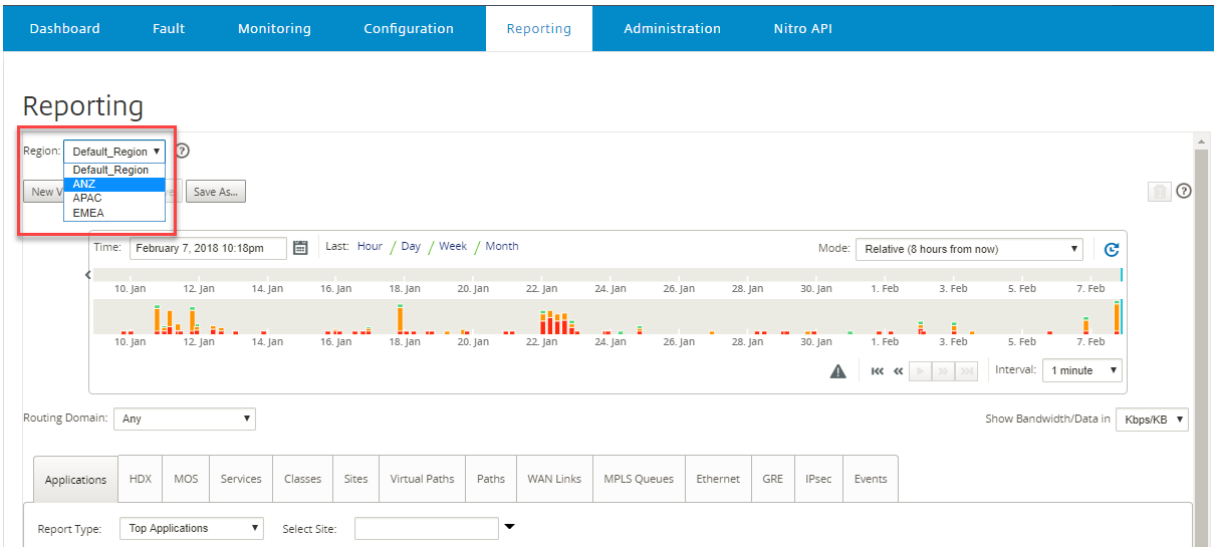
> **Tipp**
>
> Sie können die Sites basierend auf dem Namen der Region filtern. **Wählen Sie im Feld Region** auswählen die Region aus.

13. Wählen **Sie auf der Seite "Lagerbestand und Status** "die Sites aus, die Sie mit der Abfrage beginnen möchten, und klicken Sie auf **Übernehmen**.

> **Tipp**
>
> Sie können die Speichergröße des Collectors erhöhen, indem Sie einen Datenspeicher auf der virtuellen Maschine erstellen. Weitere Informationen, siehe Wechseln des aktiven Speichers auf einen neuen Datenspeicher.

Sie können bestimmte Regionen auswählen, um Ereignis- und Statistikberichte anzuzeigen.

Die Ereignis- und Statistikberichte werden aus dem Kollektor der jeweiligen Region abgerufen.



Konfiguration

April 13, 2021

Die ersten Schritte zum Konfigurieren von Citrix SD-WAN Center sind sowohl für ein einzelnes Netzwerk als auch für ein mehrregionales Netzwerk üblich. Im Folgenden finden Sie eine Liste der gängigen Konfigurationsverfahren:

- Konfigurieren der Verwaltungsschnittstelleneinstellungen
- Installieren Sie die Citrix SD-WAN Center-Zertifikate.
- Wechseln Sie den aktiven Speicher auf einen neuen Datenspeicher.

Konfigurieren der Verwaltungsschnittstelleneinstellungen

April 13, 2021

Sie können die Einstellungen der Verwaltungsschnittstelle mit der Citrix SD-WAN Center-Webschnittstelle konfigurieren.

Die Einstellungen der Verwaltungsschnittstelle umfassen Folgendes:

- IP-Adresse der Citrix SD-WAN-Center-Verwaltung
- Gateway-IP-Adresse

- Subnetzmaske
- Primärer DNS
- Sekundäres DNS

So konfigurieren Sie die Einstellungen der Verwaltungsschnittstelle:

1. Wählen Sie in der Citrix SD-WAN Center-Weboberfläche die Registerkarte **Administration** aus.

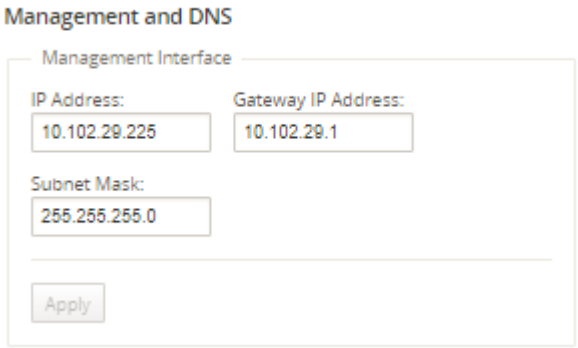
   Standardmäßig wird die Seite **Benutzer-/Authentifizierungseinstellungen** angezeigt.

2. Wählen Sie in der Navigationsstruktur **Globale Einstellungen**aus.

3. Konfigurieren Sie die Verwaltungs- und DNS-Einstellungen.

   Fügen Sie im Abschnitt **Verwaltung und DNS** die erforderlichen Informationen zu den folgenden Feldern hinzu:

   - **IP-Adresse**: Geben Sie die IP-Adresse für das Citirx SD-WAN Center ein.
   - **Gateway-IP-Adresse**: Geben Sie die Gateway-IP-Adresse ein, die die Citrix SD-WAN Center-VM für die Kommunikation mit externen Netzwerken verwendet.
   - **Subnetzmaske**: Geben Sie die Subnetzmaske ein, um das Netzwerk zu definieren, in dem sich die Citrix SD-WAN Center-VM befindet.



4. Klicken Sie auf **Anwenden.**

> **Hinweis**
>
> Die Verbindung zum Citrix SD-WAN Center wird beendet, wenn Ihre Änderungen übernommen werden.

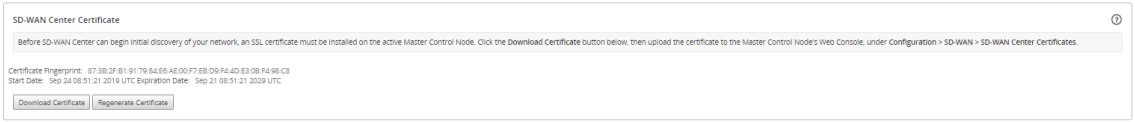
Installieren Sie das SD-WAN Center SSL-Zertifikat

April 13, 2021

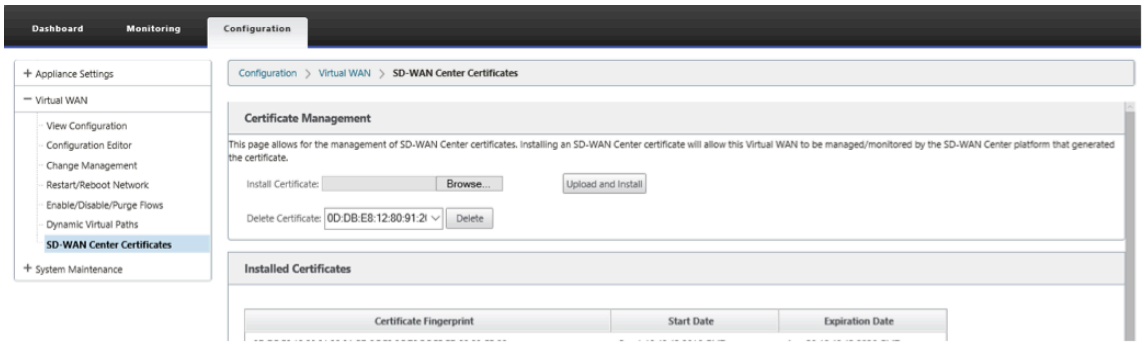
Zum Herstellen einer Verbindung zwischen Citrix SD-WAN Center und Citrix SD-WAN Master Control Node (MCN) laden Sie das SSL-Zertifikat aus dem SD-WAN Center herunter und installieren Sie es auf dem MCN.

So generieren und installieren Sie das Citrix SD-WAN Center-Zertifikat:

1. Navigieren Sie in der Webschnittstelle von Citrix SD-WAN Center zu **Konfiguration** > **Netzwerkerkennung** > **SSL-Zertifikat** > **SD-WAN Center-Zertifikat**.
2. Klicken Sie auf **Zertifikat neu generieren**, um ein neues SSL-Zertifikat zu generieren, um die Kommunikation mit dem MCN herzustellen.



3. Klicken Sie auf **Zertifikat herunterladen**. Navigieren Sie zum gewünschten Speicherort, und speichern Sie das Zertifikat.
4. Navigieren Sie in der Citrix SD-WAN MCN-Webschnittstelle zu **Konfiguration** > **Virtuelles WAN** > **SD-WAN Center-Zertifikate** > **SD-WAN Center Certificate Management**.



5. Klicken Sie auf **Datei auswählen**, durchsuchen und wählen Sie das heruntergeladene SD-WAN Center SSL-Zertifikat aus.

6. Klicken Sie auf **Hochladen und Installieren**, wird das SD-WAN-Center SSL-Zertifikat in den MCN hochgeladen und eine Erfolgsmeldung angezeigt, wenn die Installation abgeschlossen ist.

Installieren des Citrix SD-WAN SSL-Zertifikats

April 13, 2021

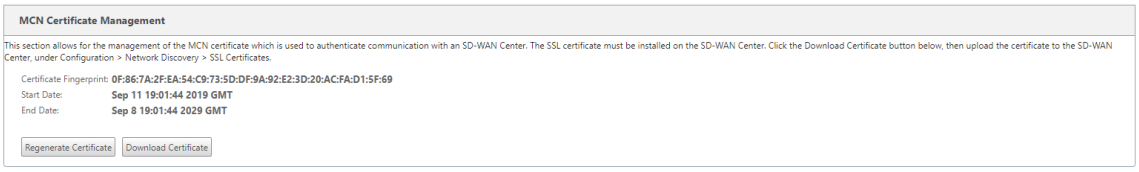
Um eine Verbindung zwischen Citrix SD-WAN MCN und Citrix SD-WAN Center herzustellen, laden Sie das SSL-Zertifikat von der MCN SD-WAN-Appliance herunter und installieren Sie es im SD-WAN Center.

Sie können das Appliance-Zertifikat auf dem MCN regenerieren, das das vordefinierte Zertifikat ersetzt, und es dann im SD-WAN Center installieren.

Die Installation des Appliance-Zertifikats im SD-WAN-Center ist für neue Bereitstellungen und für die SSL-Kommunikation obligatorisch. MCN generiert ein Netzwerkzertifikat und verteilt das Zertifikat mit einem privaten Schlüssel über den Zertifikatmanager an alle Knoten. Die Zertifikate werden von jedem Zweig verwendet, um das SD-WAN Center zu authentifizieren.

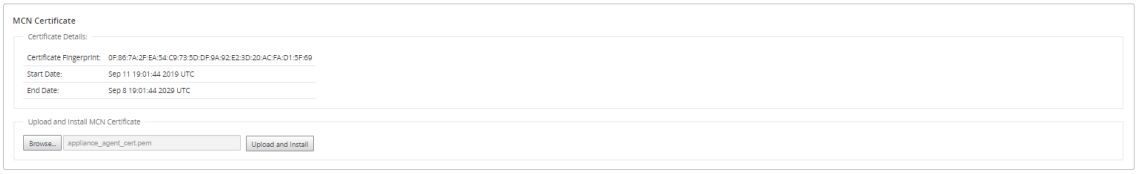
So generieren und installieren Sie das SD-WAN-Zertifikat:

1. Navigieren Sie in der MCN SD-WAN-Appliance zu **Konfiguration** > **Virtuelles WAN** > **SD-WAN Center-Zertifikate** > **MCN Certificate Management**.
2. Klicken Sie auf **Zertifikat neu generieren**, um ein neues SSL-Zertifikat zu generieren, um die Kommunikation mit dem SD-WAN Center herzustellen.

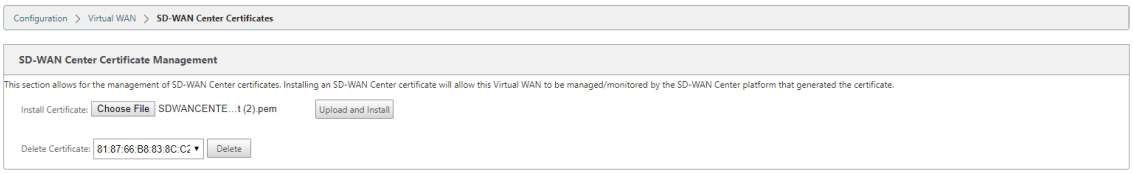


> **Hinweis:**
>
> Wenn Sie das SSL-Zertifikat neu generieren, verwendet die SD-WAN-Appliance das neue Zertifikat sofort für die Kommunikation mit dem erkannten SD-WAN Center. Die Kommunikation mit den Appliances wird jedoch erst hergestellt, wenn Sie das neu generierte Zertifikat im SD-WAN Center herunterladen und installieren.

3. Klicken Sie auf **Zertifikat herunterladen**. Navigieren Sie zum gewünschten Speicherort, und speichern Sie das Zertifikat.
4. Navigieren Sie in der Webschnittstelle von Citrix SD-WAN Center zu **Konfiguration** > **SSL-Zertifikat** > **MCN-Zertifikat**.



5. Klicken Sie auf **Durchsuchen**, und wählen Sie das heruntergeladene MCN SSL-Zertifikat aus.



6. Klicken Sie auf **Hochladen und Installieren**, es lädt das MCN SSL-Zertifikat in das SD-WAN Center hoch.

Wechseln des aktiven Speichers auf einen neuen Datenspeicher

April 13, 2021

In Citrix SD-WAN Center können Sie den aktiven Speicher in den Datenspeicher wechseln, den Sie auf dem virtuellen Server erstellt haben. Auf diese Weise können Sie weitere Statistikdaten speichern, die durch Abfragen aller Citrix SD-WAN-Appliances im WAN erhalten wurden. Weitere Informationen zum Erstellen eines Datenspeichers auf dem ESXi-Server finden Sie unter Hinzufügen und Konfigurieren des Datenspeichers auf ESXi Server. Informationen zum Erstellen eines Datenspeichers auf XenServer finden Sie unter Hinzufügen und Konfigurieren des Datenspeichers auf XenServer

So geben Sie den aktiven Speicher für die Citrix SD-WAN Center-VM an:

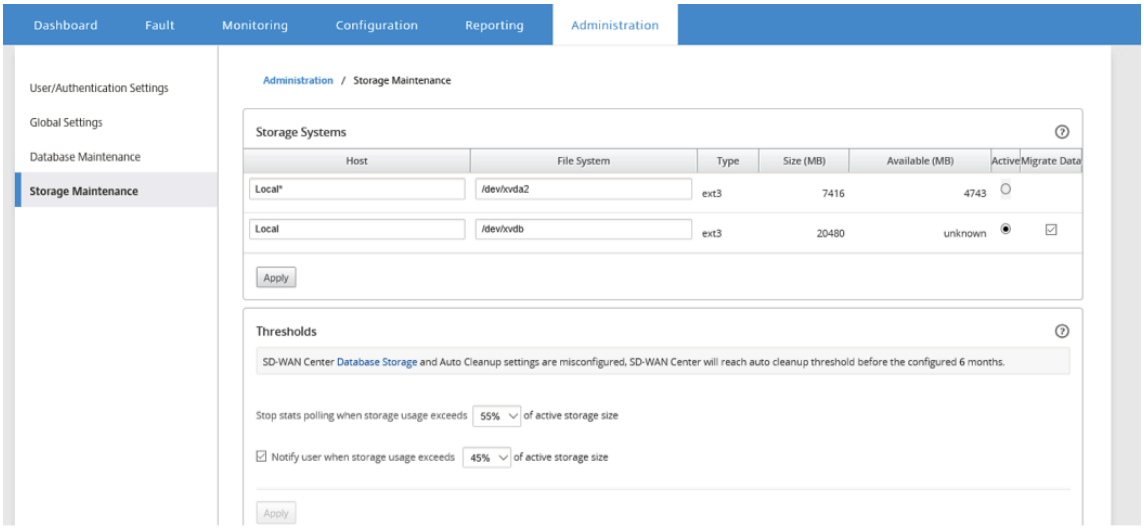
1. Melden Sie sich bei Citrix SD-WAN Center VM an.

   Die Standardanmeldedaten für Citrix SD-WAN Center lauten wie folgt:

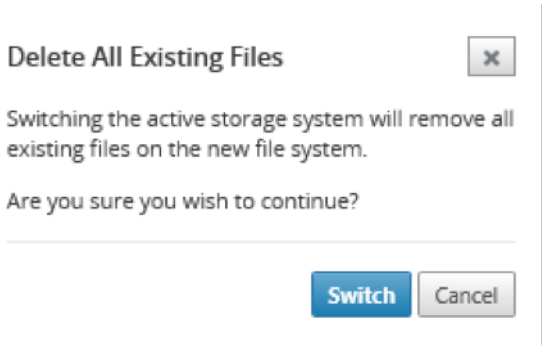
   Anmeldung: admin

   Kennwort: password

2. Klicken Sie auf die Registerkarte **Administration** und dann auf **Speicherwartung**.



3. Wählen Sie in der Spalte **Aktiv** der Tabelle Speichersysteme den erstellten Speicher aus.
4. Wählen Sie **Daten migrieren** aus, und klicken Sie auf **Anwenden**.
5. Die Meldung **Alle vorhandenen Dateien löschen** wird angezeigt und klicken Sie auf **Wechseln**.



   Dadurch wird Citrix SD-WAN Center in den **Wartungsmodus versetzt** und eine Fortschrittsanzeige im Hauptseitenbereich angezeigt.

6. Wenn die Aktivierung abgeschlossen ist, klicken Sie auf **Weiter**.

   Dadurch wird der Fortschrittsbalken verworfen und zur Hauptseite der **Speicherwartung** zurückgekehrt.

Bereitstellen der Citrix SD-WAN-Appliance

April 13, 2021

Sie können Citrix SD-WAN Center verwenden, um die Appliance-Konfigurations- oder Appliance-Einstellungsdatei zu erstellen und den Änderungsverwaltungsassistenten verwenden, um die

Konfiguration an die Appliances im Netzwerk zu übertragen. Weitere Informationen finden Sie unter Konfigurieren von Citrix SD-WAN-Appliances.

Sie können Citrix SD-WAN Center so konfigurieren, dass er als zentraler Lizenzserver fungiert und Lizenzierungsdienste für alle Knoten im Netzwerk bereitstellt. Dadurch entfällt die Notwendigkeit, Lizenzen auf einzelnen Knoten lokal zu installieren. Weitere Informationen finden Sie unter Citrix SD-WAN Center als Lizenzserver.

Sie können Citrix SD-WAN Center verwenden, um den Bereitstellungsprozess der SD-WAN-Anwendungen in Zweigstellen mithilfe der Zero Touch-Bereitstellungsfunktion zu optimieren. Weitere Informationen finden Sie unter Zero Touch-Bereitstellung.

Konfigurieren von Citrix SD-WAN-Appliances

April 13, 2021

Verwenden Sie den Konfigurationseditor, um die Konfigurationseinstellungen zu bearbeiten und das Konfigurationspaket in das MCN zu exportieren. Weitere Informationen, siehe Konfigurationseditor.

Sie können den Änderungsverwaltungsassistenten der MCN-Appliance über Citrix SD-WAN Center verwenden. Weitere Informationen, siehe Änderungsverwaltungs-Assistent.

Sie können die Appliance-Einstellung im Citrix SD-WAN Center konfigurieren und in einen Satz verwalteter Citrix SD-WAN-Appliances in Ihrem SD-WAN-Netzwerk exportieren.Weitere Informationen finden Sie unter,Appliance-Einstellungen.

Konfigurationseditor

April 13, 2021

Der Konfigurationseditor ist als Komponente der Citrix SD-WAN Center Webschnittstelle und in der Citrix SD-WAN-Verwaltungswebschnittstelle verfügbar, die auf dem Master Control Node (MCN) des SD-WAN-Netzwerks ausgeführt wird.

> **Hinweis**
>
> Konfigurationen können nicht direkt über Citrix SD-WAN Center an die erkannten Appliances übertragen werden. Sie können den Konfigurationseditor verwenden, um die Konfigurationseinstellungen zu bearbeiten und ein Konfigurationspaket zu erstellen. Wenn das Konfigura-

> tionspaket erstellt wurde, können Sie es in das MCN exportieren und installieren. Die Änderungen werden dann im MCN wiedergegeben.
>
> Sie müssen sich mit Administratorrechten an der Citrix SD-WAN Center-Appliance und dem MCN anmelden, die Konfigurationen im Citrix SD-WAN-Center bearbeiten und die Konfigurationen auf dem MCN exportieren und installieren.

Ausführliche Anweisungen zur Verwendung des Konfigurationseditors zum Konfigurieren Ihres Citrix SD-WAN finden Sie in derCitrix SD-WAN 10.1/en-us/citrix-sd-wan/10-1.html [()]Dokumentation.

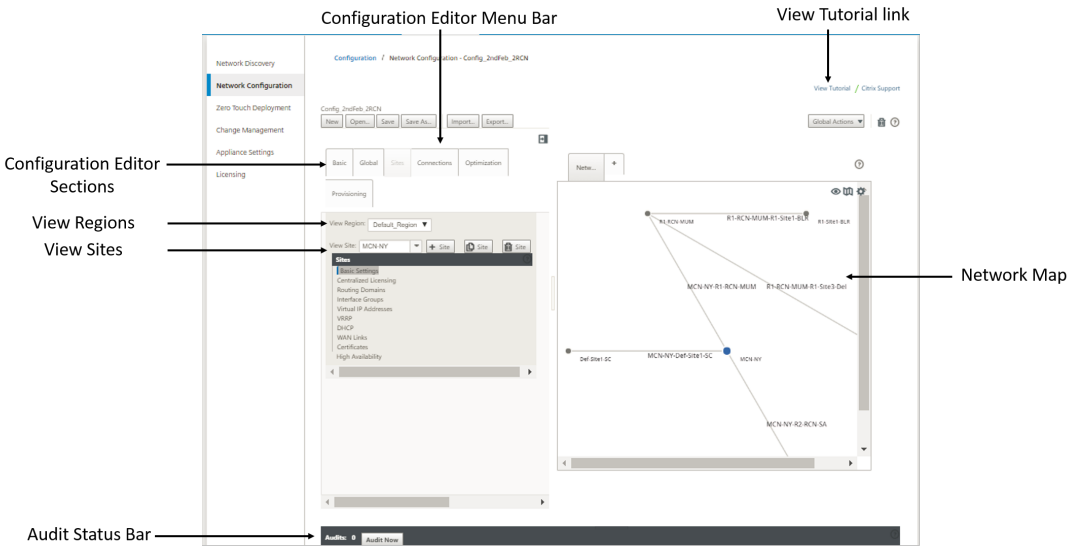
Mit dem Konfigurationseditor können Sie Folgendes tun:

- Hinzufügen und Konfigurieren von Citrix SD-WAN Appliance-Sites und -Verbindungen.
- Stellen Sie die Citrix SD-WAN-Appliance bereit.
- Erstellen und definieren Sie die Citrix SD-WAN-Konfiguration.
- Definieren und sehen Sie Netzwerkkarten Ihres SD-WAN-Systems an.

So öffnen Sie den Konfigurationseditor:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf **Netzwerkkonfiguration**.

   Die folgende Abbildung beschreibt die grundlegenden Navigations- und Seitenelemente des **Konfigurationseditors**sowie die in diesem Handbuch verwendete Terminologie.



   Der primäre Bildschirm des Konfigurationseditors verfügt über die folgenden Navigationselemente:

- **Konfigurationseditor Menüleiste**: Enthält die primären Aktivitätsschaltflächen für Konfigurationseditor-Vorgänge. Darüber hinaus befindet sich am rechten Rand der Menüleiste

die Linkschaltfläche **Tutorial anzeigen**, um das Tutorial zum Konfigurationseditor zu initiieren. Das Lernprogramm führt Sie durch eine Reihe von Blasenbeschreibungen für jedes Element der Anzeige des Konfigurationseditors.

- **Configuration Editor-Abschnitte** : Jede Registerkarte stellt einen Abschnitt der obersten Ebene dar. Es gibt sechs Abschnitte: **Basic**, **Global**, **Sites**, **Verbindungen**, **Optimierung**und **Provisioning**. Klicken Sie auf eine Abschnittsregisterkarte, um die Konfigurationsstruktur für diesen Abschnitt anzuzeigen.
- **Region anzeigen**: Für die Bereitstellung mit mehreren Regionen werden alle konfigurierten Regionen aufgelistet. Bei einer Bereitstellung mit einer Region wird standardmäßig die Standardregion angezeigt. Um die Sites in einer Region anzuzeigen, wählen Sie eine Region aus der Dropdownliste aus.
- **Sites anzeigen:** Listet die Standortknoten auf, die der Konfiguration hinzugefügt wurden und derzeit im Konfigurationseditor geöffnet werden. Um die Standortkonfiguration anzuzeigen, wählen Sie einen Standort aus der Von-Down-Liste aus.
- **Netzwerkkarte:** Bietet eine schematische Ansicht des SD-WAN-Netzwerks.Bewegen Sie den Mauszeiger über die Sites oder den Pfad, um weitere Details anzuzeigen. Klicken Sie auf die Sites, um Berichtsoptionen anzuzeigen.
- **Überwachungsstatusleiste**: Die dunkelgraue Leiste am unteren Rand der Seite des Konfigurationseditors und erstreckt sich über die gesamte Breite der Seite Konfigurationseditor. Die Statusleiste **Audits** ist nur verfügbar, wenn der **Konfigurationseditor** geöffnet ist. Ein Audit-Warnsymbol (roter Punkt oder Goldrute Delta) ganz links in der Statusleiste zeigt einen oder mehrere Fehler an, die in der aktuell geöffneten Konfiguration vorhanden sind. Klicken Sie auf die Statusleiste, um eine vollständige Liste aller nicht aufgelösten Überwachungswarnungen für diese Konfiguration anzuzeigen.

Änderungsverwaltungs-Assistent

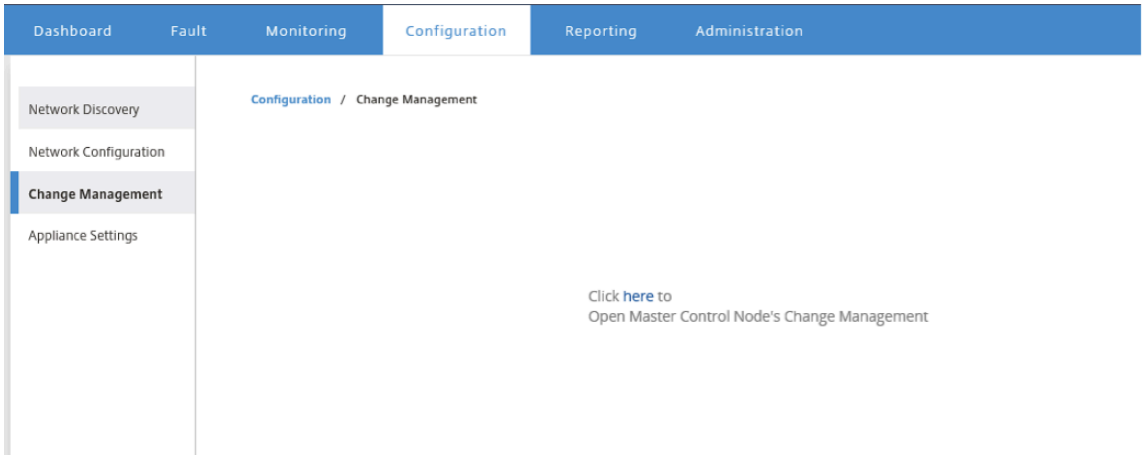
April 13, 2021

Der Änderungsverwaltungs-Assistent führt Sie durch das Hochladen, Herunterladen, Staging und Aktivieren der Citrix SD-WAN-Software und Konfiguration auf der Master Control Node (MCN) -Appliance und Client-Appliances.

Der Änderungsverwaltungs-Assistent ist eine Komponente der Citrix SD-WAN-Verwaltungswebschnittstelle, die auf dem MCN ausgeführt wird, und ist nicht Teil des Citrix SD-WAN Centers. Sie können jedoch das Citrix SD-WAN Center verwenden, um eine Verbindung mit dem angegebenen MCN herzustellen und auf den Änderungsverwaltungs-Assistenten zuzugreifen.

So öffnen Sie den Änderungsverwaltungs-Assistenten:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf **Änderungsverwaltung**.



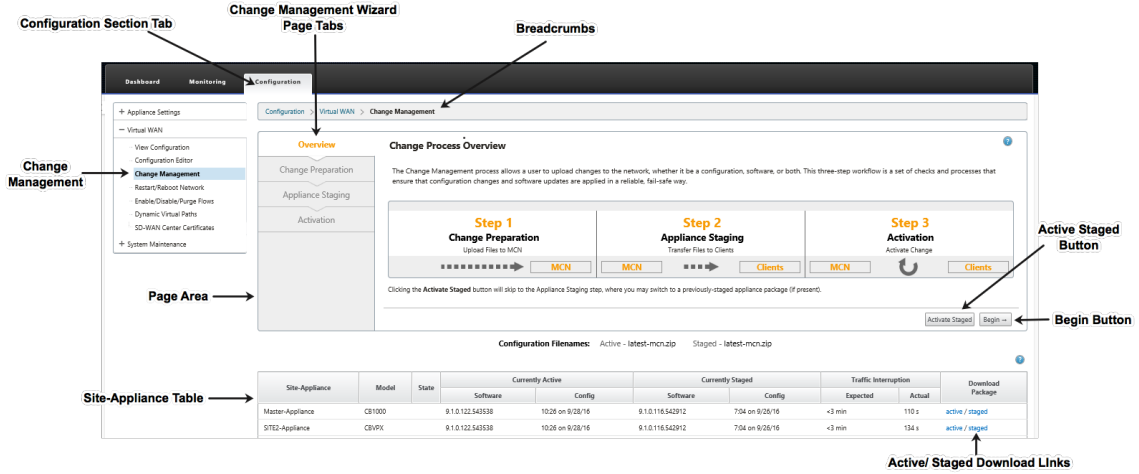
3. **Klicken Sie in der Eingabeaufforderung Klicken Sie hier, um die Änderungsverwaltung des Hauptkontrollknotens zu öffnen** auf den Link **Hier**.

   Sie werden automatisch in der MCN GUI eingeloggt.

   > **Hinweis**
   >
   > Sie müssen sich nicht mit den MCN-Anmeldeinformationen bei der MCN-GUI anmelden, die automatische Anmeldefunktion aktiviert einmaliges Anmelden.

4. Klicken Sie in der MCN-Management-Weboberfläche auf die Registerkarte **Konfiguration**.
5. Klicken Sie in der Navigationsstruktur (linker Bereich) neben dem **Virtual WAN-** Zweig auf **+**, um diesen Zweig zu erweitern.
6. Klicken Sie auf **Änderungsverwaltung**.

   Dies zeigt die erste Seite des Assistenten für die **Änderungsverwaltung** an, die Seite **Änderungsprozessübersicht**, wie in der folgenden Abbildung dargestellt.



7. Klicken Sie auf Starten, um den Assistenten **zu starten**.

> **Hinweis**
>
> Ausführliche Anweisungen zur Verwendung des Assistenten zum Hochladen, Aktivieren und Aktivieren der SD-WAN-Software und der Konfiguration auf den Appliances finden Sie im SD-WAN 9.1.0 Benutzerhandbuch.

Der **Änderungsverwaltungs** -Assistent verfügt über die folgenden Navigationselemente:

- **Seitenbereich**: Zeigt die Formulare, Tabellen und Aktivitätsschaltflächen für jede Seite des **Änderungsverwaltungsassistenten** an.
- **Registerkarten des Änderungsverwaltungsassistenten**: Auf der linken Seite des Seitenbereichs werden auf jeder Seite des Assistenten Registerkarten in der Reihenfolge aufgeführt, in der die entsprechenden Schritte im Assistentenprozess ausgeführt werden. Wenn eine Registerkarte aktiv ist, können Sie darauf klicken, um zu einer vorherigen Seite im Assistenten zurückzukehren. Eine aktive Registerkarte zeigt seinen Namen in einer blauen Schriftart an. Eine graue Schrift zeigt eine inaktive Registerkarte an. Registerkarten sind inaktiv, bis alle Abhängigkeiten (vorherige Schritte) fehlerfrei erfüllt wurden.
- **Appliance-Site-Tabelle**: Am unteren Rand des Seitenbereichs des Assistenten enthält diese Tabelle Informationen zu den einzelnen konfigurierten Appliance-Standorten und Links zum Herunterladen der aktiven oder bereitgestellten Appliance-Pakete für dieses Appliance-Modell und diese Site. Ein Paket in diesem Kontext ist ein ZIP-Datei-Bundle, das das entsprechende SD-WAN-Softwarepaket für dieses Appliance-Modell und das angegebene Konfigurationspaket enthält. Der Abschnitt Konfigurationsdateinamen oberhalb der Tabelle zeigt den Paketnamen für die aktuellen aktiven und bereitgestellten Pakete auf der lokalen Appliance.
- **Aktiv/Staged Download-Links**: Im Feld **Download-Paket**(ganz rechts) jedes Eintrags in der **Appliance-Site-**Tabelle können Sie auf einen Link in einem Eintrag klicken, um das aktive oder bereitgestellte Paket für die Site dieser Appliance herunterzuladen.

- **Schaltfläche Start**: Klicken Sie auf **Beginnen**, um den Prozess des **Änderungsverwaltungsassistenten** zu starten und zur Registerkarte **Änderungsvorbereitung**fortzufahren.
- **Schaltfläche "Staged aktivieren"**: Wenn es sich nicht um eine anfängliche Bereitstellung handelt und Sie die aktuell bereitgestellten Konfiguration aktivieren möchten, haben Sie die Möglichkeit, direkt mit dem **Aktivierungsschritt** fortzufahren. Klicken Sie auf **Staged aktivieren**, um direkt zur Seite **Aktivierung** zu gelangen und die Aktivierung der aktuell bereitgestellten Konfiguration zu initiieren.

Appliance-Einstellungen

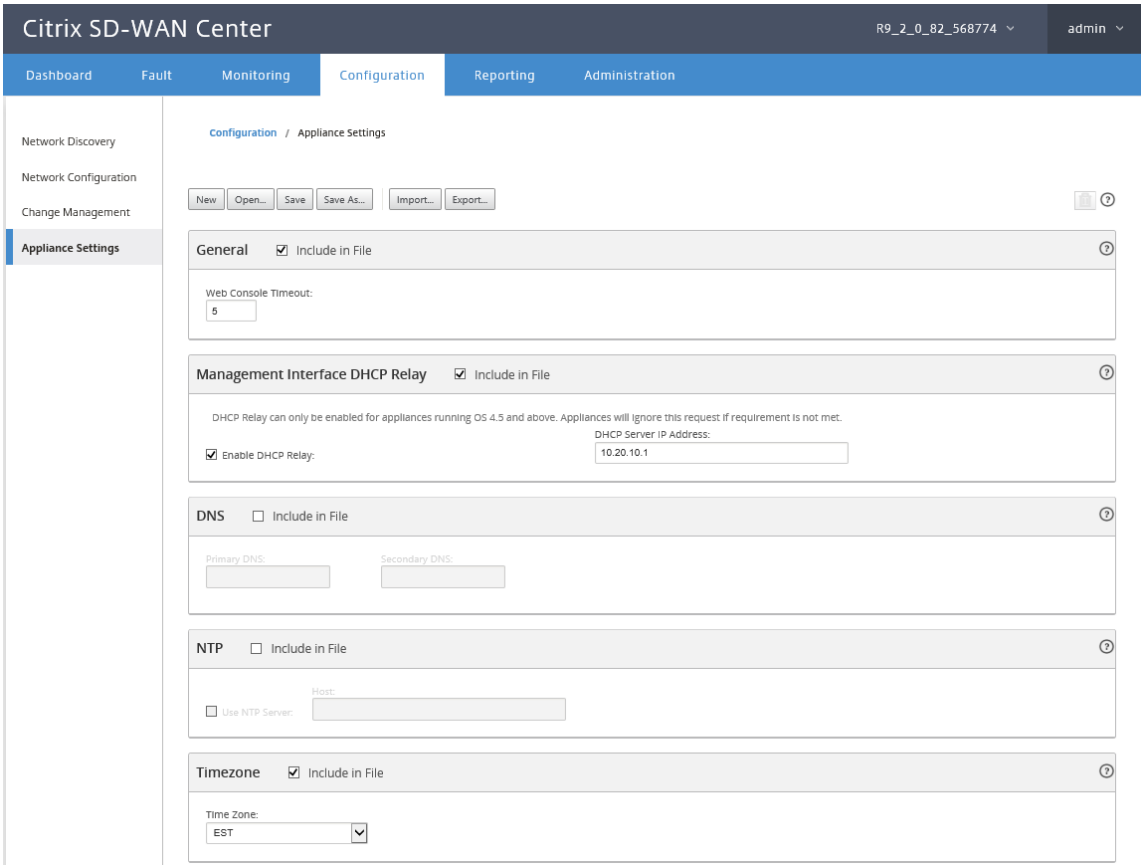
April 13, 2021

Sie können die Appliance-Einstellung im Citrix SD-WAN Center konfigurieren und in einen Satz verwalteter Citrix SD-WAN-Appliances in Ihrem SD-WAN-Netzwerk exportieren.Auf der Seite **Appliance-Einstellungen** können Sie die folgenden Aktionen ausführen:

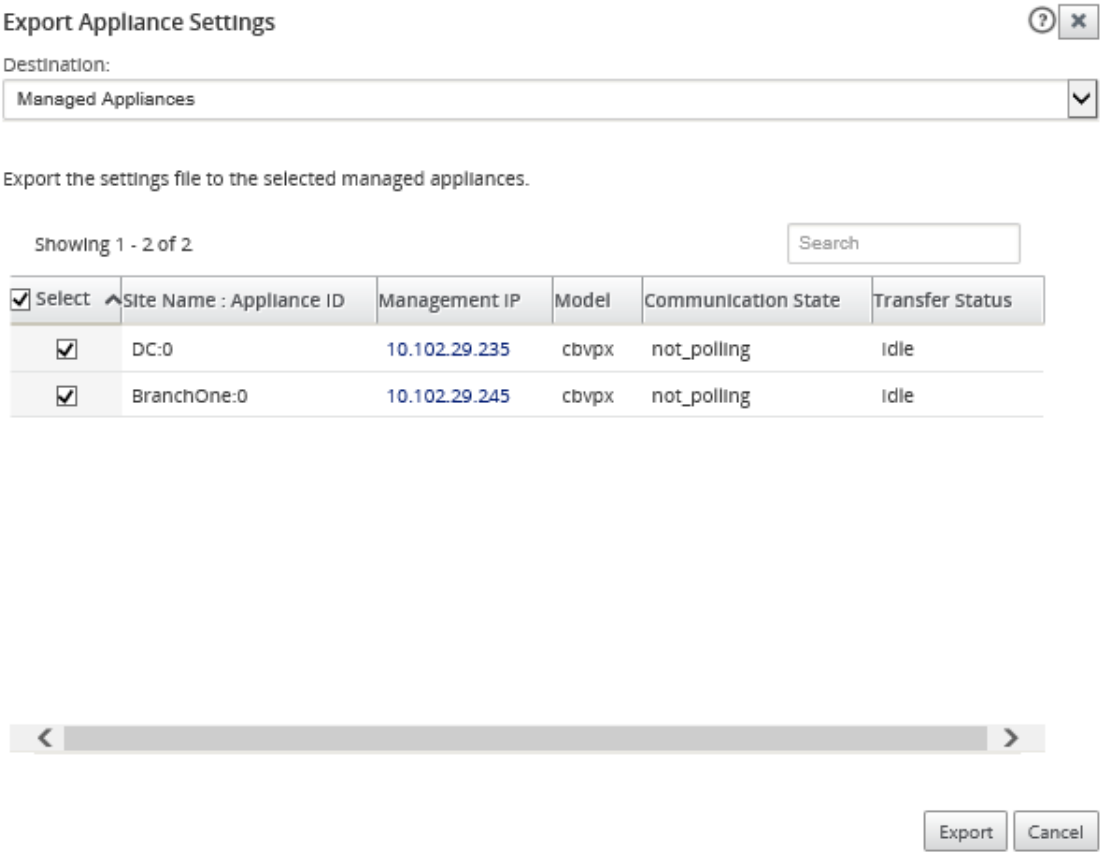
- Erstellen Sie eine neue Appliance-Einstellungsdatei.
- Öffnen und bearbeiten Sie eine vorhandene Appliance-Einstellungsdatei.
- Importieren Sie eine Appliance-Einstellungsdatei von Ihrem lokalen Computer.
- Laden Sie eine Appliance-Einstellungsdatei auf Ihren lokalen Computer herunter.
- Exportieren Sie eine Appliance-Einstellungsdatei in die verwalteten Appliances.

So erstellen Sie eine Appliance-Einstellungsdatei und exportieren sie in verwaltete Appliances:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf **Einheiteneinstellungen** und dann auf **Neu**.



3. Wählen Sie **In Datei einschließen** für die erforderlichen Einstellungen aus, und geben Sie die Parameterwerte für die Einstellungen an. Weitere Informationen finden Sie unter Appliance-Einstellungstabelle.
4. Klicken Sie auf **Exportieren**. Geben **Sie im Dialogfeld Speichern** unter einen Namen für die Appliance-Einstellungsdatei ein, und klicken Sie auf **Speichern**. Das Dialogfeld "**Appliance-Einstellungen exportieren** "wird angezeigt.
5. Wählen Sie im Feld **Ziel** die Option **Verwaltete Appliances** aus, und wählen Sie die Appliances aus, in die Sie die Appliance-Einstellungen exportieren möchten.



> **Hinweis**
>
> Um die Appliance-Einstellungen auf Ihren lokalen Computer herunterzuladen, wählen Sie im Feld **Ziel** die Option **Dateidownload** aus.

6. Klicken Sie auf **Exportieren**.

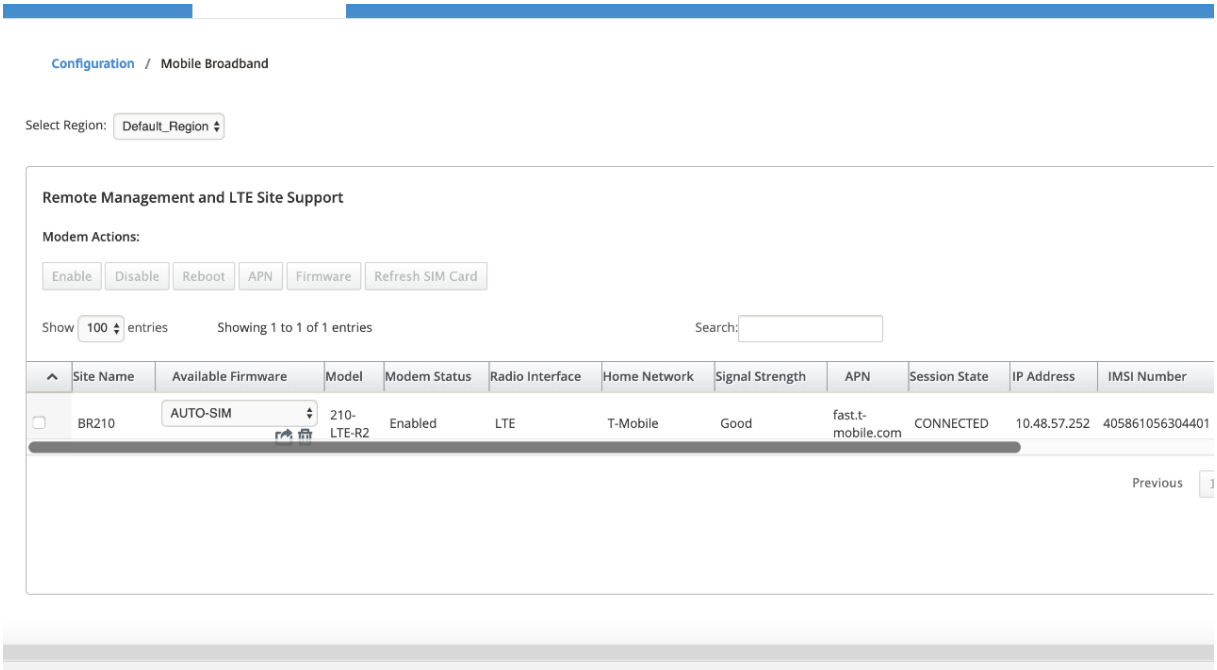
Remote LTE-Standortverwaltung

April 13, 2021

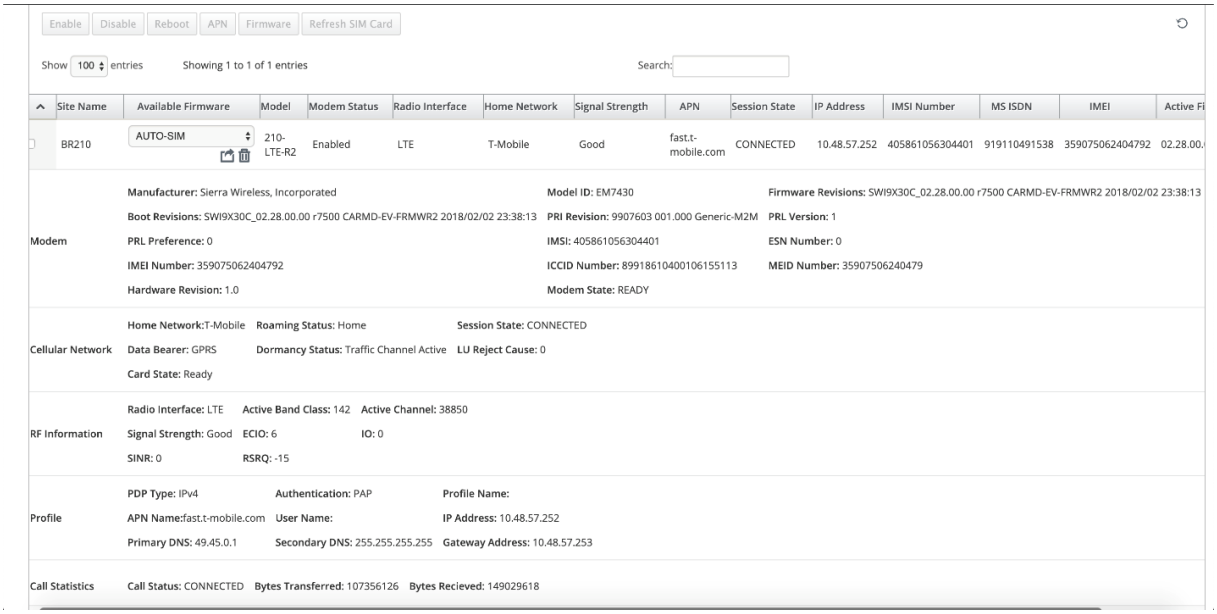
Mit Citrix SD-WAN Center können Sie alle LTE-Standorte in Ihrem Netzwerk remote anzeigen und verwalten. In der LTE-Zusammenfassungstabelle sind die Citrix SD-WAN 210-SE LTE-Appliances aufgeführt, die in Ihrem Netzwerk verwendet werden.

Um die LTE-Standorte in Ihrem Netzwerk remote zu verwalten, navigieren Sie in der Benutzeroberfläche des SD-WAN Centers zu **Konfiguration > Mobiles Breitband**.

Bei einer Bereitstellung mit mehreren Regionen können Sie eine Region auswählen, für die Sie die LTE-Standorte verwalten möchten. Standardmäßig ist die Standardeinstellung “Default_Region”ausgewählt.



Klicken Sie auf **+**, um die Details anzuzeigen.



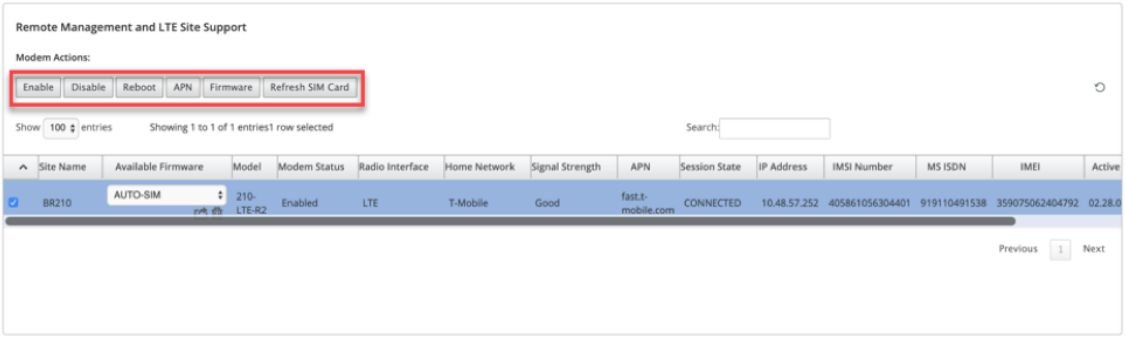
Sie können entweder eine einzelne Appliance oder mehrere Appliances auswählen, um den folgenden LTE-Modemvorgang auszuführen:

- **Enable:** Modem an den ausgewählten Sites aktivieren.
- **Disable:** Deaktivieren Sie das Modem an den ausgewählten Sites.

- **Reboot:** Starten Sie das Modem der ausgewählten Sites neu.
- **APN**: Konfigurieren Sie die APN-Einstellungen für die ausgewählten Sites. Weitere Informationen finden Sie unter Konfigurieren von APN-Einstellungen.
- **Firmware**: Durchsuchen und wählen Sie die erforderliche Firmware. Sie können die Firmware-Datei nur hochladen oder hochladen und auf den ausgewählten Sites anwenden. Aus der Liste der verfügbaren Firmware können Sie auswählen, ob Sie sie anwenden oder löschen möchten.

  > **Hinweis**
  >
  > Bei Bereitstellungen mit mehreren Regionen können Firmwarevorgänge für Nicht-Standardregionsites nicht über das SD-WAN Center-Headend ausgeführt werden. Firmwarevorgänge können über das Collector SD-WAN Center der jeweiligen Region durchgeführt werden.

- **SIM-Karte aktualisieren**: Aktualisieren Sie die SIM-Karte, indem Sie sie ausschalten und an den ausgewählten Standorten wieder einschalten. Dieser Vorgang wird ausgeführt, um die neue SIM-Karte zu erkennen, die in das 210 SE LTE-Modem eingelegt ist.



Sie können die LTE-Funktionalität auch auf einzelnen LTE-Appliances konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der LTE-Funktionalität auf 210 SE LTE.

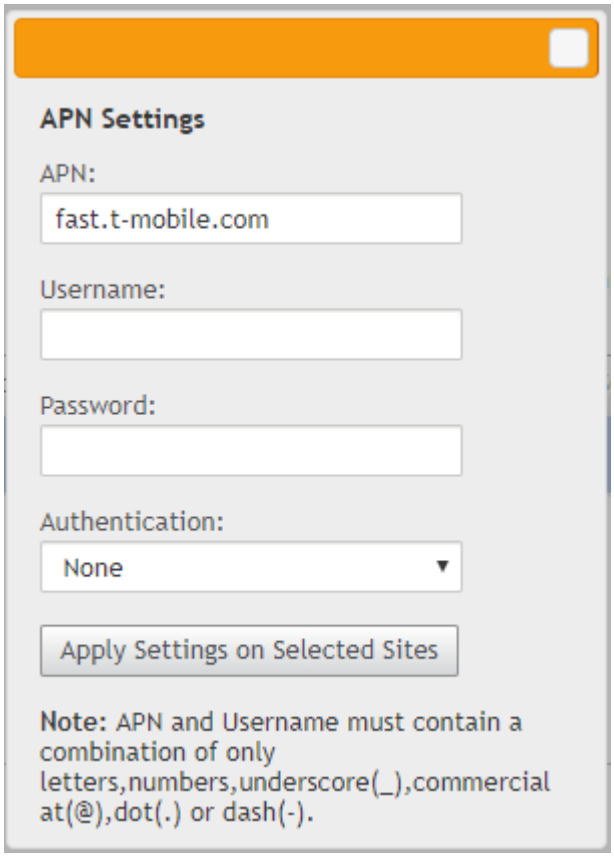
APN-Einstellungen

APN ist der Name der Einstellungen, die Ihre Appliance liest, um eine Verbindung zum Gateway zwischen dem Mobilfunknetz des Mobilfunknetzes und dem öffentlichen Internet einzurichten. Sie können die APN-Informationen vom Netzanbieter abrufen und die **APN-Einstellungen** auf einer oder mehreren LTE-Appliances remote konfigurieren.

> **Hinweis:**
> DieAPN-Einstellungen variieren je nach Netzanbieter.

So konfigurieren Sie APN-Einstellungen:

1. Navigieren Sie in der Benutzeroberfläche des SD-WAN Centers zu **Konfiguration > Mobiles Breitband**. Wählen Sie die LTE-Sites aus, für die Sie APN-Einstellungen konfigurieren möchten, und klicken Sie auf **APN**.



2. Geben Sie den **APN-Namen**, den **Benutzernamen**, das **Kennwort** und die **Authentifizierung** ein, die vom Netzbetreiber bereitgestellt wurden. Sie können zwischen PAP, CHAP, PAPCHAP Authentifizierungsprotokollen wählen. Wenn der Netzbetreiber keinen Authentifizierungstyp angegeben hat, setzen Sie ihn auf **Keine**.
3. Klicken Sie auf **Einstellungen für ausgewählte Sites anwenden**.

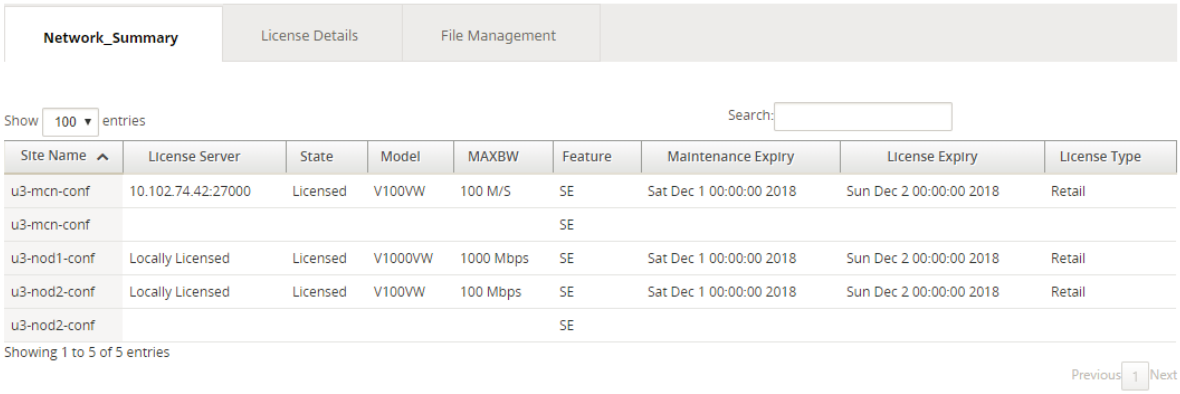
Citrix SD-WAN Center als Lizenzserver

April 13, 2021

Sie können die Lizenzen für die Appliances in Ihrem Netzwerk erwerben, sie hochladen und in SD-WAN Center installieren. Um SD-WAN Center als Remote-Lizenzserver zu verwenden, konfigurieren Sie die IP-Adresse von SD-WAN Center als Remote-Server für die zentrale Lizenzverwaltung. Weitere Informationen, siehe Zentrales Lizenzmanagement.

Nachdem Sie die Netzwerkkonfiguration über den Änderungsverwaltungsprozess an die Standorte übertragen haben und die Konfiguration aktiviert ist, erhalten die Zweigstellen-Appliances automatisch die Lizenzen vom SD-WAN-Center.
Damit diese Lizenzen verwendet werden können, muss man die Lizenzen dem Host des SD-WAN Centers selbst zuweisen.

Um die Lizenzdetails aller vom SD-WAN Center erkannten Appliances anzuzeigen, navigieren Sie zu **Konfiguration** > **Lizenzierung** > **Netzwerkübersicht.**



Folgende Parameter werden angezeigt:

- **Sitename**: Der Name der Site.
- **Lizenzserver**: Die IP-Adresse und die Portnummer des Lizenzservers. Wenn die Lizenz lokal auf der Appliance installiert wurde, wird sie als “Lokal lizenziert”angezeigt.
- **Status**: Der aktuelle Lizenzstatus der Appliance, Lizenziert oder Nicht lizenziert.
- **Modell**: Das Appliance-Modell, das von der Lizenz unterstützt wird.
- **MAXBW**: Die maximale Bandbreite, die von der Lizenz erlaubt ist.
- **Feature**: Die Citrix SD-WAN-Edition, die von der Lizenz unterstützt wird.
- **Wartungsablauf**: Das Ablaufdatum von Citrix Subscription Advantage.

  > **Hinweis**
  >
  > Wenn das Software-Builddatum während des Software-Upgrades höher als das Ablaufdatum der Wartung ist, ist das Software-Upgrade nicht zulässig.

- **Lizenzablauf**: Das Ablaufdatum der Lizenz.
- **Lizenztyp**: Der Typ der Lizenz.

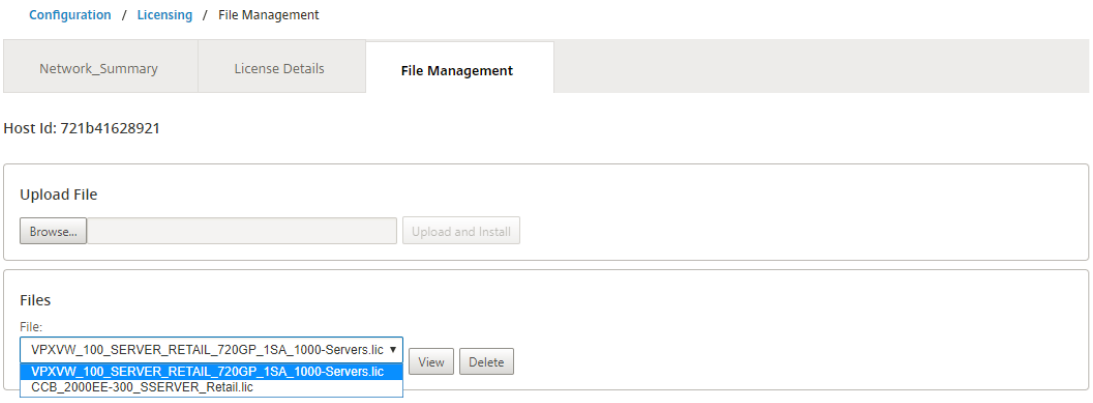
So laden Sie Lizenzdateien in SD-WAN Center hoch und installieren Sie sie:

1. Erwerben Sie die Lizenz für die Citrix SD-WAN-Appliances, und speichern Sie sie auf Ihrem lokalen Computer.

   > **Hinweis**
   >
   > Weitere Informationen zum Erhalt einer Citrix SD-WAN-Softwarelizenz erhalten Sie beim Citrix SD-WAN-Kundendienst.

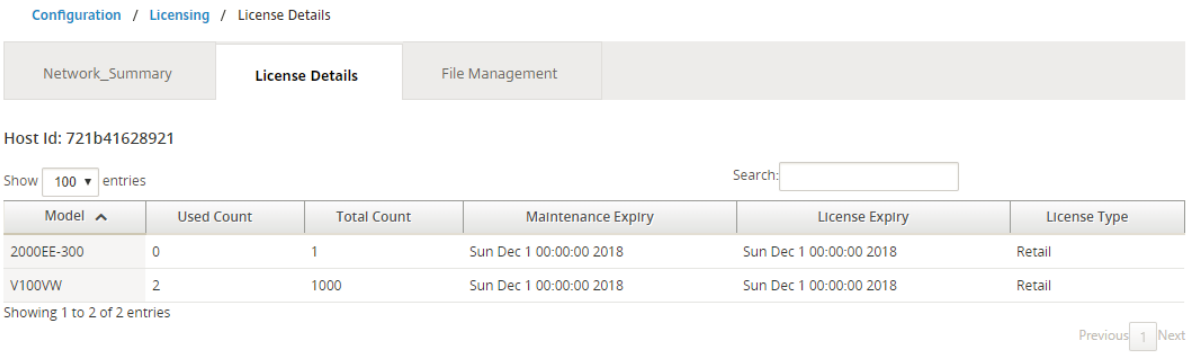
2. Navigieren Sie in der SD-WAN Center GUI zu **Lizenzierung** > **Dateiverwaltung**.
3. Klicken **Sie im Abschnitt Datei hochladen** auf **Durchsuchen**. Wählen Sie die Lizenzdatei von Ihrem lokalen Computer aus und klicken Sie auf **Hochladen und Installieren**.

   Die installierten Lizenzdateien werden im Dropdownmenü **Dateien** aufgeführt. Sie können die Lizenzdateien anzeigen oder löschen.



> **Hinweis**
>
> Die Host-ID ist die SD-WAN Center-Host-ID, die zum Generieren der Lizenzdateien verwendet wird. Die Lizenzdateien, die mit einer anderen Host-ID generiert wurden, können nicht auf Citrix SD-WAN Center hochgeladen und installiert werden.

Sie können die Details aller in Citrix SD-WAN Center hochgeladenen und installierten Lizenzdateien auf einen Blick anzeigen, indem Sie zu **Konfiguration** > **Lizenzierung** > **Lizenzdetails** navigieren.



Folgende Parameter werden angezeigt:

- **Modell:** Das Gerätemodell, das die Lizenz unterstützt.
- **Anzahl der verwendeten Einheiten:** Die Anzahl der Appliances, auf denen diese Lizenz installiert ist.
- **Gesamtanzahl:** Die Gesamtzahl der Appliances, auf denen diese Lizenz installiert werden kann.
- **Wartungsablauf**: Das Ablaufdatum von Citrix Subscription Advantage.
- **Lizenzablauf**: Das Ablaufdatum der Lizenz.
- **Lizenztyp**: Der Typ der Lizenz.

Bereitstellen von Citrix SD-WAN in Azure über Citrix SD-WAN Center

April 13, 2021

Citrix SD-WAN für Azure ermöglicht Organisationen eine direkte sichere Verbindung von jeder Zweigstelle zu den in Azure gehosteten Anwendungen. Dadurch müssen Cloudgebundener Datenverkehr nicht über ein Rechenzentrum zurückgeholt werden.

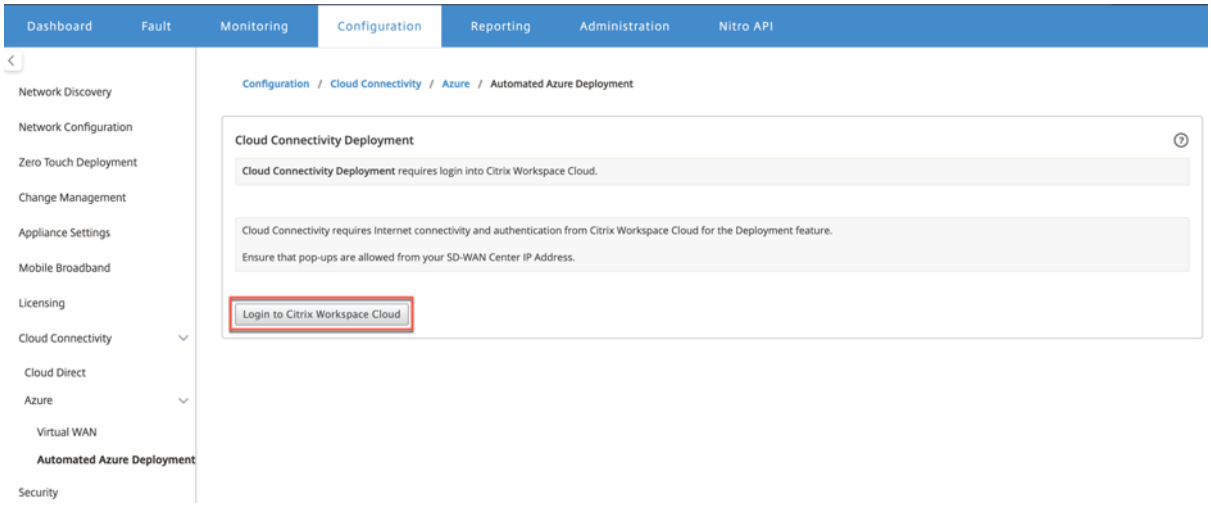
Voraussetzungen

- Citrix Workspace Cloud-Anmeldeinformationen.
- Azure-Abonnementanmeldeinformationen
- Azure-Anwendungs- und Dienstprinzipal mit der rollenbasierten Zugriffskontrolle finden Sie unter Vorgehensweise: Verwenden des Portals zum Erstellen einer Azure AD-Anwendung und Dienstprinzipal, die auf Ressourcen zugreifen können.
- Nachdem der Dienstprinzipal erstellt wurde, notieren Sie sich die folgenden Details:
  - Azure-Abonnenten-ID
  - Mandanten-ID

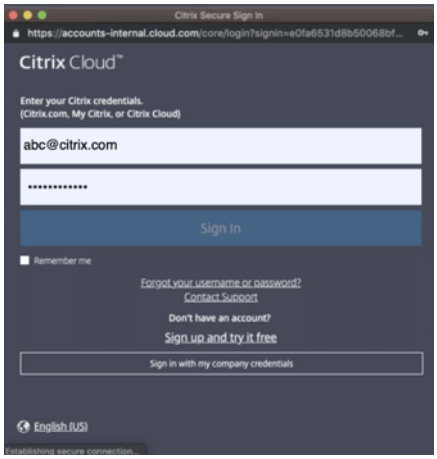
  - Anwendungs-ID
  - Geheimer Schlüssel

- Führen Sie die Änderungsverwaltung im MCN/SD -WAN Center mithilfe der ctx-sdw-sw-xxxxxxx.zip durch.
- Ermitteln Sie im Citrix SD-WAN Center das MCN und ziehen Sie die aktive Konfiguration.

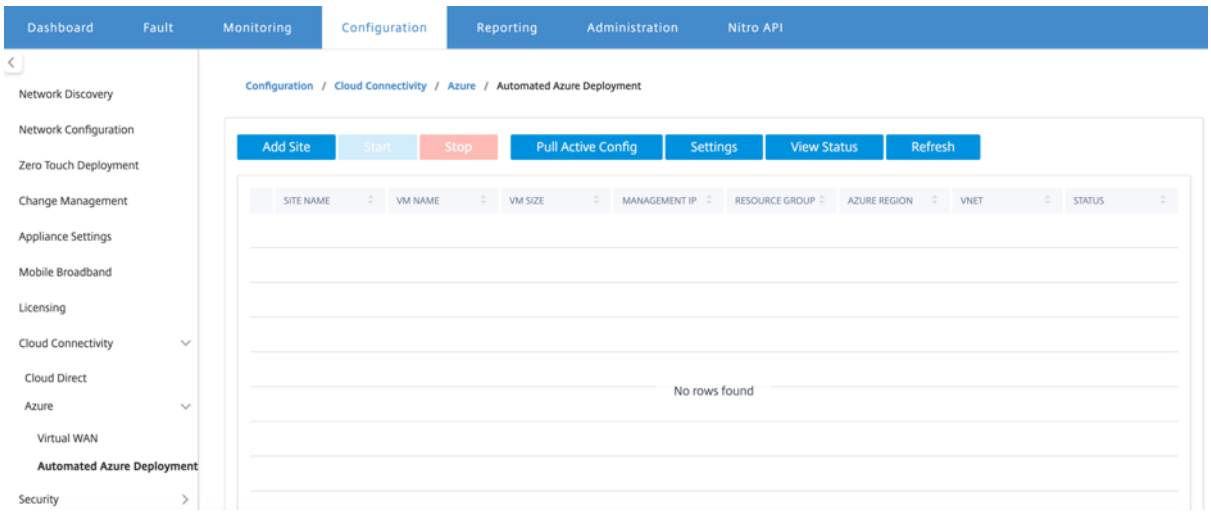
Um Citrix SD-WAN in Azure über SD-WAN Center bereitzustellen, navigieren Sie zu **Konfiguration > Cloud-Konnektivität > Azure > Automated Azure-Bereitstellung**.



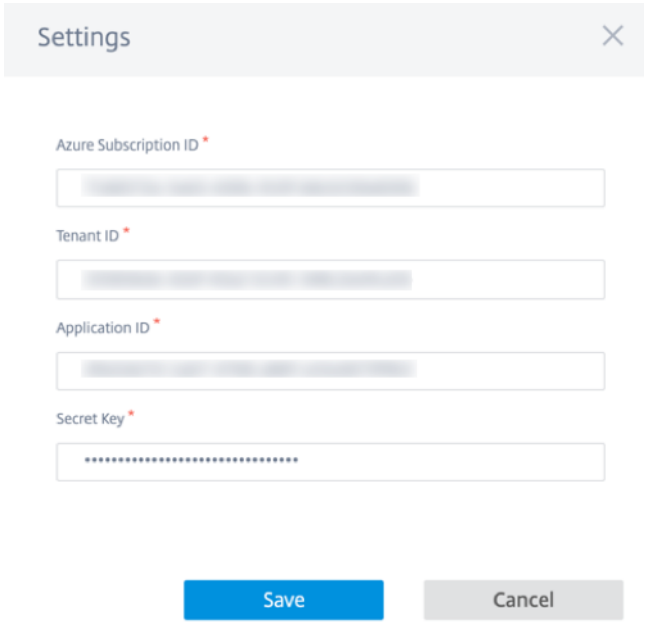
Melden Sie sich mit den Citrix Cloud-Anmeldeinformationen an.



Automatisierte Azure-Bereitstellung



Klicken Sie auf **die Option Einstellungen**, und geben Sie die Details zum Azure-Abonnement an. Klicken Sie auf Option Aktive Konfiguration abrufen, um die aktive ausgeführte Konfiguration aus dem MCN abzurufen.



Bereitstellen von Citrix SD-WAN in Azure

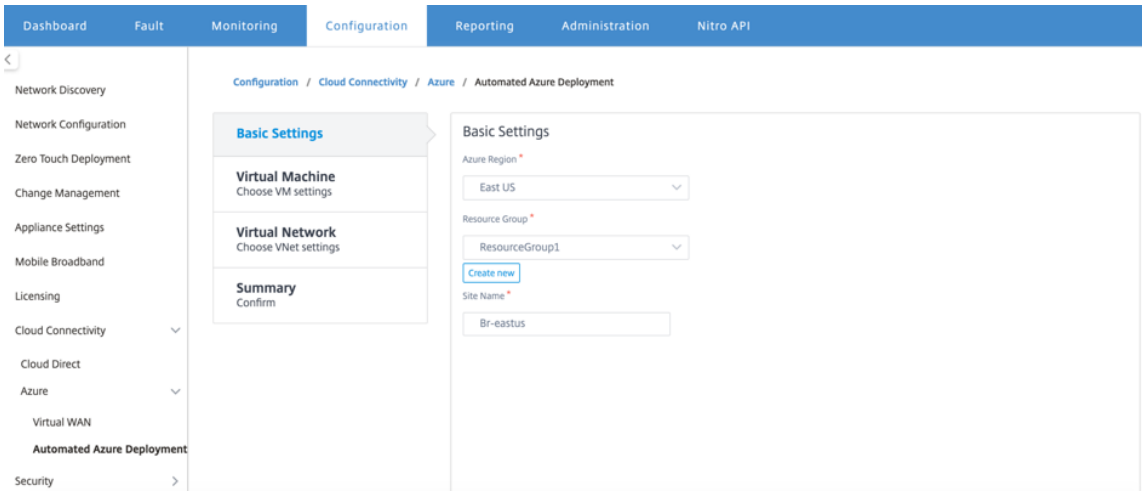
So stellen Sie das Citrix SD-WAN in Microsoft Azure bereit:

1. Klicken Sie auf **Site hinzufügen**, um eine neue SD-WAN-Instanz hinzuzufügen. Es initiiert die Erstellung einer virtuellen SD-WAN-Maschine in Azure unter Ihrem aktuellen Abonnement.

   Im Rahmen dieser Bereitstellung werden auch folgende Punkte bereitgestellt:

- Fügt der aktuellen aktiven MCN-Konfiguration automatisch die SD-WAN-Konfiguration für den neu hinzugefügten Standort hinzu.
- Führt das Änderungsmanagement aus.
- Wenden Sie die Softwareversion und Konfiguration des MCN auf diese neue Site an.

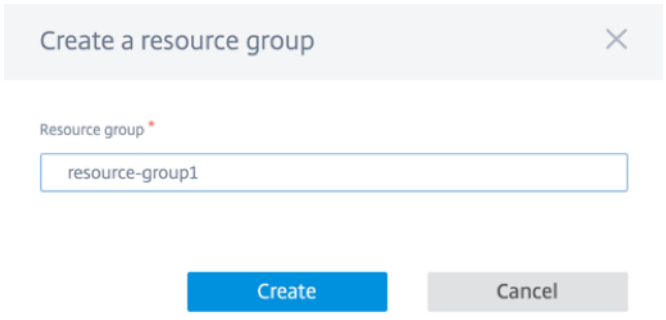
Führen Sie die **Standardeinstellungen, die virtuelle Maschine** und das **virtuelle Netzwerk** aus.



Wählen Sie unter Grundeinstellungen die Region und die Ressourcengruppe aus der Dropdownliste aus. Sobald die Region ausgewählt ist, werden in der Dropdownliste Ressourcengruppen alle vorhandenen Ressourcengruppen in dieser Region unter diesem Abonnement angezeigt.

> **HINWEIS:**
>
> Um einen Standort hinzuzufügen, muss die Ressourcengruppe leer sein.

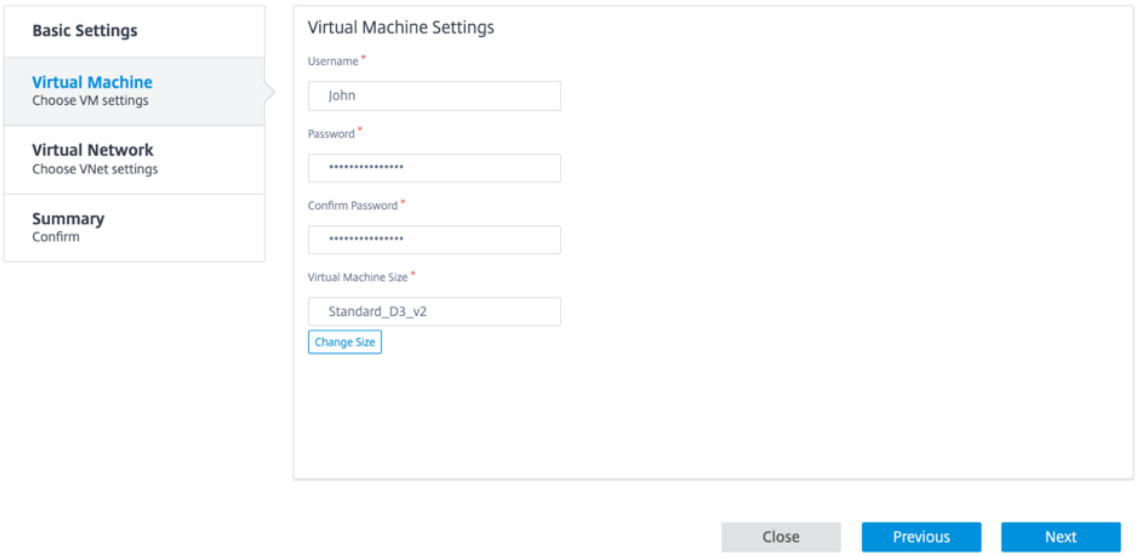
Sie können eine vorhandene leere Ressourcengruppe auswählen oder auf die Option **Neu erstellen** klicken, um eine neue zu erstellen.



2. Der Standortname wird automatisch mit dem Namen der Region generiert. Sie können den Site-Namen weiterhin nach Bedarf bearbeiten.

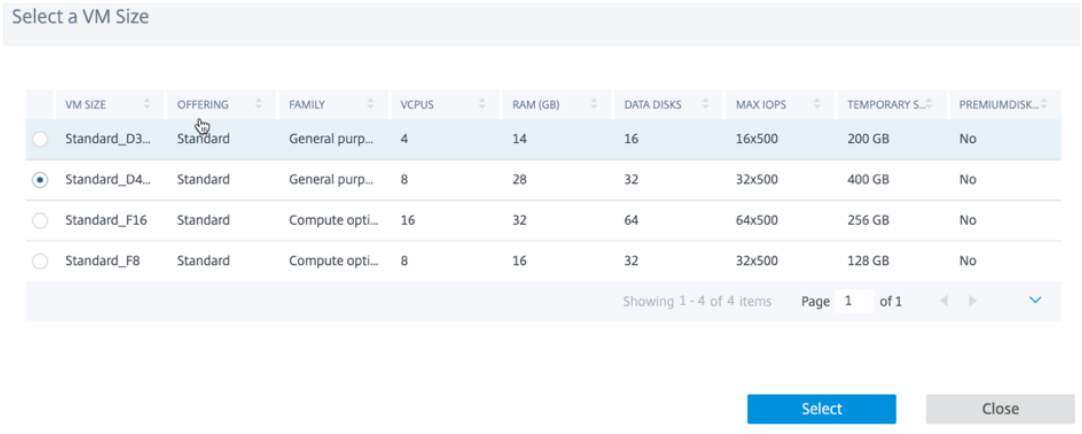
> **HINWEIS:**
>
> Stellen Sie sicher, dass der Standortname die Anforderungen an den SD-WAN-Standortnamen erfüllt und im SD-WAN-Netzwerk eindeutig ist.
>
> Der Azure-VM-Name wird aus dem Sitename im Format **AZ-regionname-sitename** generiert.

3. Klicken Sie auf **Weiter**, um die virtuelle Maschine zu konfigurieren.

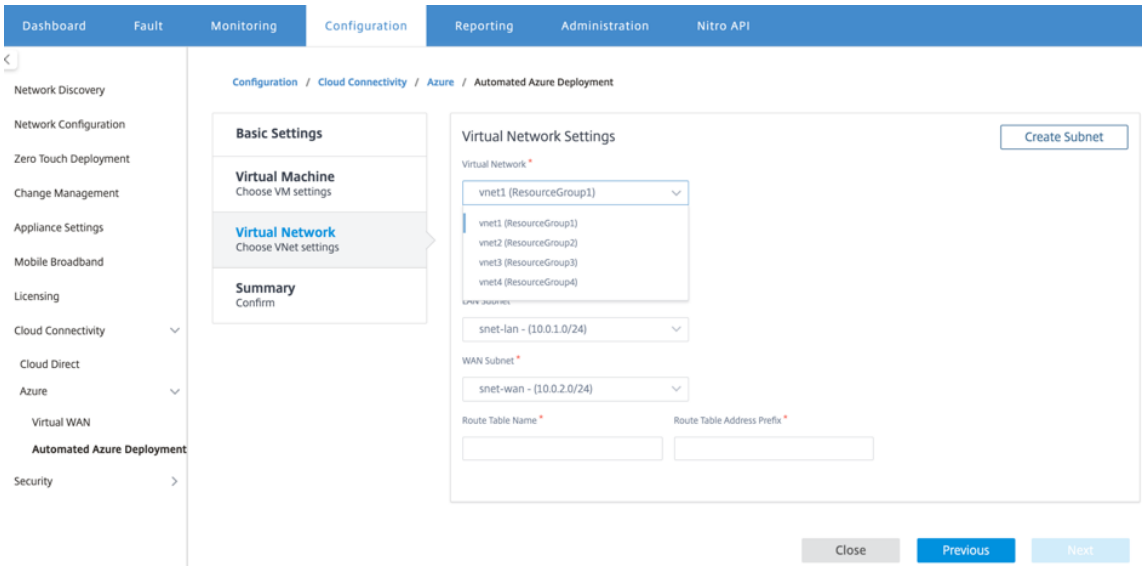


Geben Sie Benutzername, Kennwort und Kennwort bestätigen an. Standardmäßig ist die VM-Größe automatisch mit der Standardgröße gefüllt. Klicken Sie auf **Größe ändern**, um bei Bedarf eine andere VM-Größe auszuwählen.

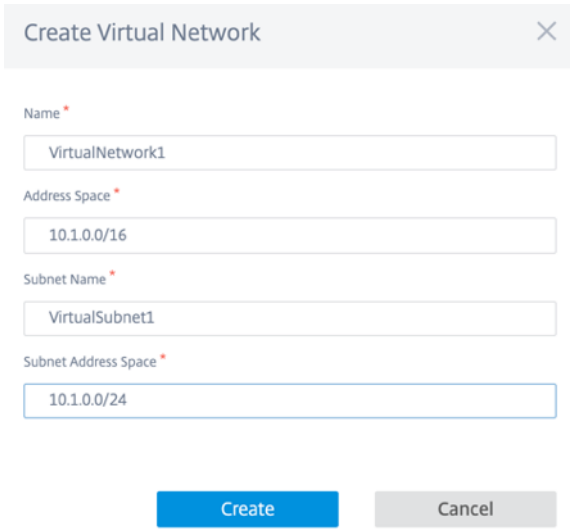
> **HINWEIS:**
>
> Diese während der Bereitstellung bereitgestellten Benutzeranmeldeinformationen verfügen über schreibgeschützten Zugriff auf das Azure SD-WAN. Verwenden Sie für Administratorberechtigungen Administratoranmeldeinformationen.



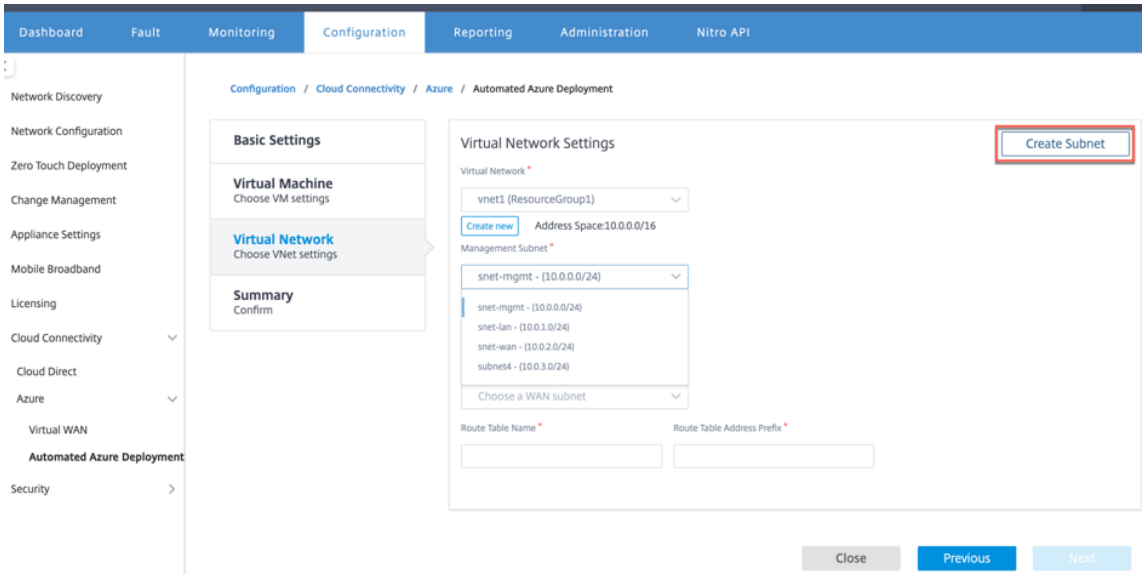
4. Klicken Sie auf **Weiter**, um die Einstellungen für das virtuelle Netzwerk durchzuführen.
5. Wählen Sie in der Dropdownliste das virtuelle Netzwerk aus. Die Liste enthält das gesamte virtuelle Netzwerk in der ausgewählten Azure-Region.



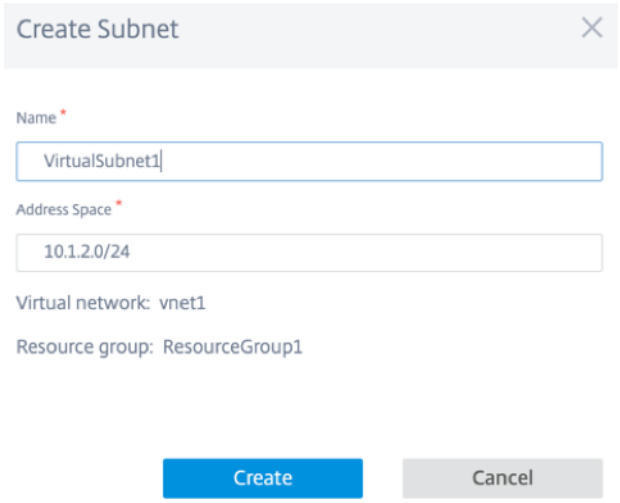
Sie können die Site in einem vorhandenen virtuellen Netzwerk bereitstellen oder ein neues virtuelles Netzwerk erstellen. Klicken Sie auf **Neu erstellen**, um ein neues virtuelles Netzwerk zu erstellen. Geben Sie den Namen des virtuellen Netzwerks, den Adressraum (geben Sie einen benutzerdefinierten privaten IP-Adressraum an), den Subnetznamen und den Subnetzadressraum an.



6. Wählen Sie ein Subnetz für die Verwaltung aus.



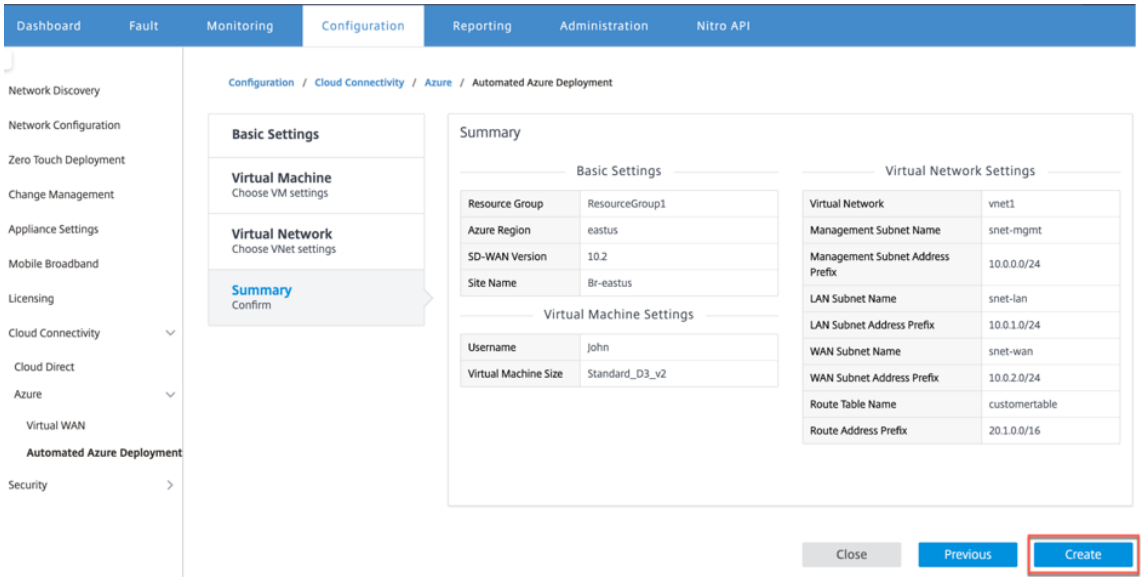
7. Sie können ein Subnetz auch mit der Option **Subnetz erstellen** (in der oberen rechten Ecke) erstellen.



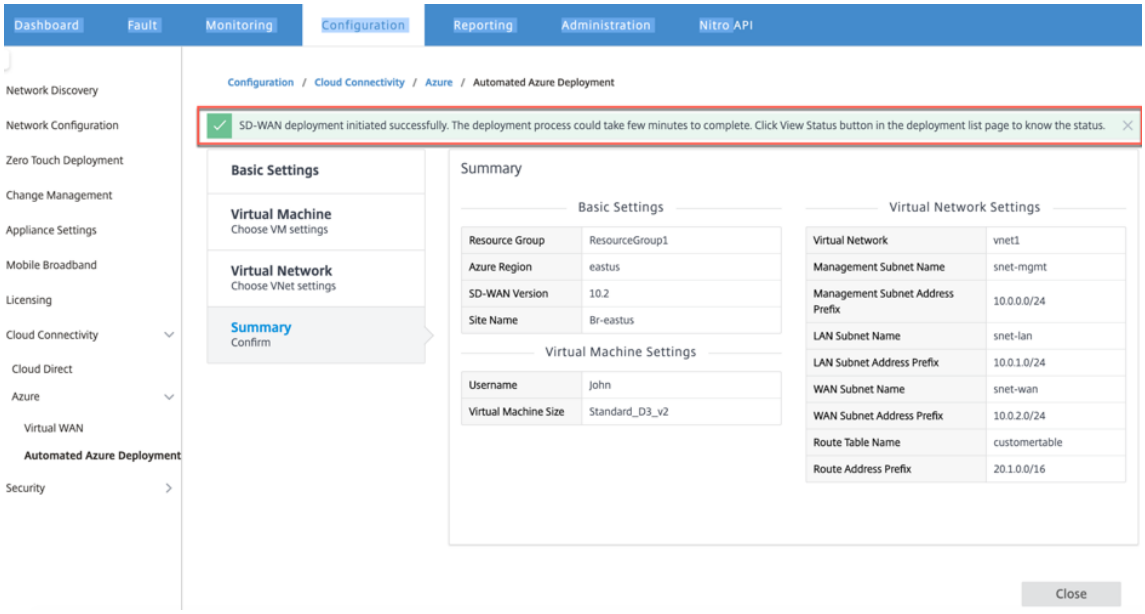
8. Wählen Sie in der Dropdownliste ein anderes Subnetz für LAN und WAN aus, und geben Sie den **Routingtabellennamen** zusammen mit dem **Adresspräfix Routingtabelle** an. Das **Routing Table Address Prefix** ist der Zieladressraum, der an diese SD-WAN-Appliance umgeleitet wird. Andere Zieladresse wird von Azure-Routing umgeleitet.

> **HINWEIS:**
>
> Die Routingtabelle ist dem LAN-Subnetz zugeordnet. Wenn dem gewählten LAN-Subnetz bereits eine Routentabelle zugeordnet ist, wird diese Routentabelle angezeigt und kann nicht geändert werden. Andernfalls können Sie den Namen der Routingtabelle angeben.

9. Klicken Sie auf **Weiter**, um die Einstellungsdetails zu überprüfen und zu bestätigen, und klicken Sie auf **Erstellen**.



Oben wird eine Statusmeldung angezeigt, die besagt, dass die Bereitstellung erfolgreich initiiert wurde.



Die Bereitstellung kann einige Zeit in Anspruch nehmen, daher wird empfohlen, dass Sie auf **Status anzeigen** klicken, um das neueste Update zum Bereitstellungsstatus zu erhalten.

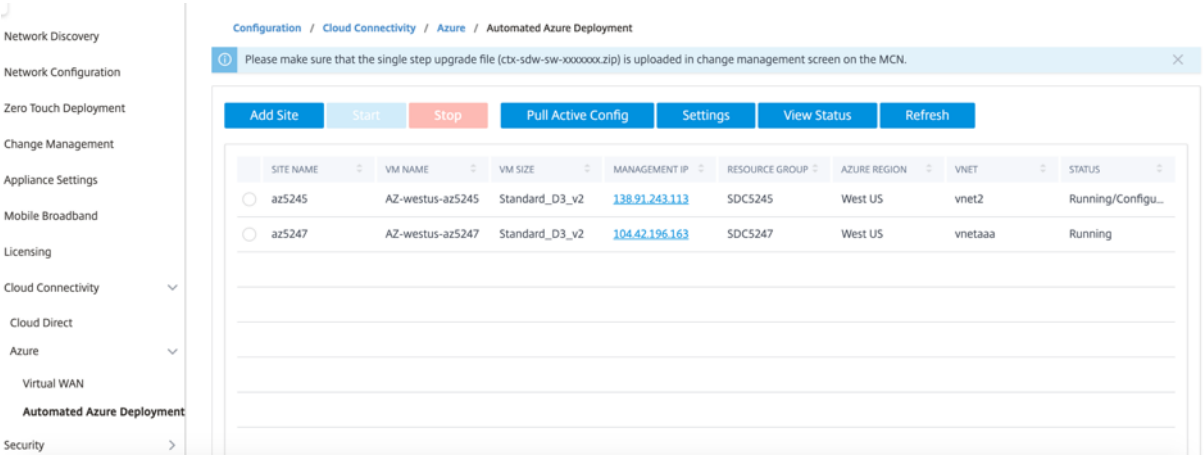
Im Rahmen der Bereitstellung:

- Die virtuelle Maschine wird in der ausgewählten Azure-Region erstellt.
- Eine Site wird automatisch zur aktiven SD-WAN-Konfiguration im SD-WAN hinzugefügt.
- Die Änderungsverwaltung wird auf der neu bereitgestellten Azure-VM durchgeführt.

Sobald die Bereitstellung erfolgreich ist, werden die virtuellen Pfade zwischen der MCN- und Azure-Site gebildet. Wenn bei der Bereitstellung ein Fehler auftritt, wird der Prozess zurückgesetzt und alle

automatisch erstellten Ressourcen werden zurückgesetzt.

Standardmäßig wird die Site als Teil der Standard-Routingdomäne platziert. Er gehört zur Standard-region, die die standardmäßige automatische Pfadgruppe verwendet.



- **Sitename**: Name der Citrix SD-WAN-Site. Dieser Sitename wird in der Citrix SD-WAN-Konfiguration verwendet.
- **VM-Name**: Name der virtuellen Maschine (VM), die in Azure bereitgestellt wird.
- **VM-Größe**: Die VM-Größe, die beim Erstellen der Site ausgewählt wurde.
- **Management-IP**: Management-IP-Adresse, die der neu erstellten SD-WAN-VM zugewiesen wurde.
- **Ressourcengruppe**: Ressourcengruppen sind logische Konstrukte und der Datenaustausch über Ressourcengruppen hinweg ist immer möglich. Die virtuelle Azure-Maschine gehört zu dieser Ressourcengruppe. Die neuen Ressourcen, die während der Bereitstellung des Citrix SD-WAN erstellt wurden, werden unter dieser Ressourcengruppe gruppiert. Wenn während der Bereitstellung ein Fehler auftritt, werden die in dieser Ressourcengruppe erstellten Ressourcen gelöscht.
- **Azure-Region**: Stellt den Speicherort der Ressourcengruppe und ihrer Ressourcen dar.
- **VNet**: Virtuelles Netzwerk, das von der Site verwendet wird.
- **Status**: Gibt den Status der VM an.

Klicken Sie auf **Aktualisieren**, um den aktuellen Standortstatus abzurufen. Sie können die VM jederzeit für die ausgewählte Site **starten** oder **stoppen**. Sie können jeweils nur eine Site auswählen.

Melden Sie sich nach Abschluss der Bereitstellung bei MCN oder Citrix SD-WAN Center an, um den Status virtueller Pfade anzuzeigen.

Zero Touch-Bereitstellung

April 13, 2021

> **Hinweis**
>
> Der Zero Touch-Bereitstellungsdienst wird nur auf ausgewählten Citrix SD-WAN-Appliances unterstützt:
>
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition (Reimaging erforderlich)
> - SD-WAN 1000 Enterprise Edition (Premium Edition) (Reimaging erforderlich)
> - SD-WAN 1100 Standard Edition
> - SD-WAN 1100 Premium (Enterprise) Edition
> - SD-WAN 2000 Standard Edition (Reimaging erforderlich)
> - SD-WAN 2000 Enterprise Edition (Premium Edition) (Reimaging erforderlich)
>   - SD-WAN AWS VPX-Instanz

Zero Touch Deployment (ZTD) Service ist ein von Citrix betriebener und verwalteter Cloud-Service, der die Erkennung neuer Appliances im Citrix SD-WAN-Netzwerk ermöglicht und den Bereitstellungsprozess für Zweigstellen automatisiert. Der ZTD Cloud Service ist von jedem Knoten im Netzwerk über das Internet und über das SSL-Protokoll (Secure Socket Layer) zugänglich.

Der ZTD Cloud Service kommuniziert sicher mit Backend-Citrix Network-Services und speichert die Identifikation von Kunden, die Zero Touch-fähige Geräte erworben haben (z. B. SD-WAN 410-SE, 2100-SE).Die Backend-Services sind vorhanden, um jede Zero Touch-Bereitstellungsanforderung zu authentifizieren und die Zuordnung zwischen dem Kundenkonto und den Seriennummern von Citrix SD-WAN-Appliances ordnungsgemäß zu validieren.

ZTD High-Level-Architektur und Workflow

Rechenzentrums-Standort

Citrix SD-WAN-Administrator —Ein Benutzer mit Administratorrechten für die SD-WAN-Umgebung mit den folgenden primären Zuständigkeiten:

- Konfigurationserstellung mit dem Citrix SD-WAN Center Network Configuration Tool oder Import der Konfiguration von der Master Control Node (MCN) SD-WAN-Appliance
- Citrix Cloud Login, um den Zero Touch Deployment Service für die Bereitstellung neuer Standortknoten zu initiieren.

> **Hinweis**
>
> Wenn Ihr SD-WAN Center über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Server-Einstellungen im SD-WAN Center konfigurieren. Weitere Informationen siehe Proxy-Server-Einstellungen für Zero Touch-Bereitstellung.

Netzwerkadministrator —Ein Benutzer, der für die Netzwerkverwaltung in Unternehmen zuständig ist (DHCP, DNS, Internet, Firewall usw.)

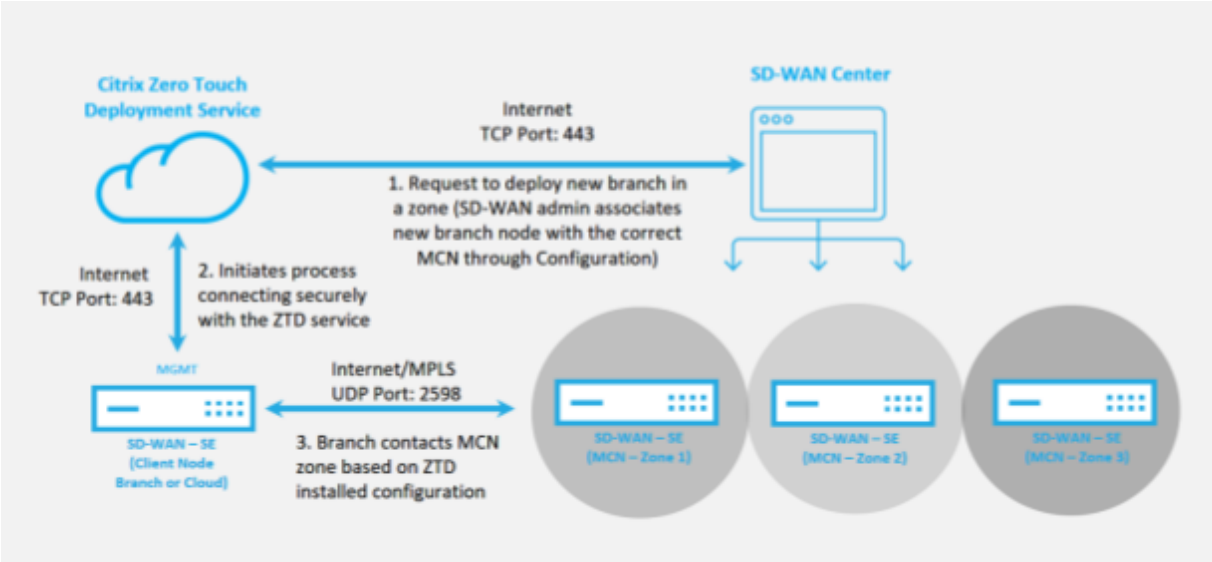
- Konfigurieren Sie ggf. Firewalls für die ausgehende Kommunikation mit dem FQDN ***sd-wanzt.citrixnetworkapi.net*** vom SD-WAN Center.

Remote-Standort

Installateur vor Ort —Ein lokaler Ansprechpartner oder ein angeheuerter Installateur für Aktivitäten vor Ort mit den folgenden Hauptaufgaben:

- Physisch die Citrix SD-WAN-Appliance auspacken.
- Reimaging nicht-ZTD-fähiger Appliances.
  - Benötigt für: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - Nicht erforderlich für: SD-WAN 410-SE, 2100-SE
- Stromkabel der Appliance anschließen.
- Verkabeln der Appliance für die Internetverbindung über die Verwaltungsschnittstelle (z. B. MGMT oder 0/1).
- Verkabeln der Appliance für WAN-Link-Konnektivität auf den Datenschnittstellen (z. B.apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5 usw.).

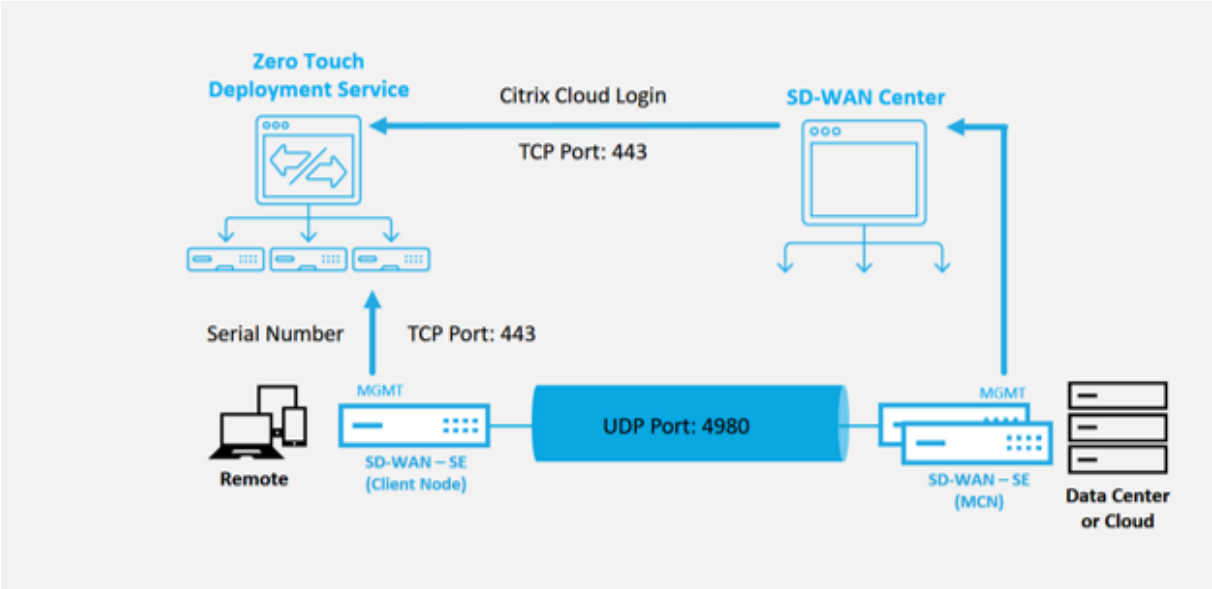
> **Hinweis**
>
> Das Schnittstellenlayout unterscheidet sich von jedem Modell. Bitte beachten Sie daher die Dokumentation zur Identifizierung von Daten- und Management-Ports.



Die folgenden Voraussetzungen sind erforderlich, bevor Sie einen Zero Touch-Bereitstellungsdienst starten:

- Aktive Ausführung von SD-WAN auf Master Control Node (MCN) heraufgestuft.
- Aktive Ausführung von SD-WAN Center mit Verbindung zum MCN über Virtual Path.
- Citrix Cloud Anmeldeinformationen, die am erstellt wurdenhttps://onboarding.cloud.com(siehe unten die Anleitung zur Kontoerstellung).
- Verwaltungsnetzwerkkonnektivität (SD-WAN Center und SD-WAN-Appliance) mit dem Internet an Port 443, entweder direkt oder über einen Proxy-Server.
- Internet-Konnektivität an Port 443 für den Zugriff auf das SD-WAN Center Webportal für die ZTD-Ersteinrichtung.
- (optional) Mindestens eine aktiv ausgeführte SD-WAN-Appliance, die in einer Zweigstelle im Client-Modus mit gültiger Virtual Path-Konnektivität zu MCN betrieben wird, um die erfolgreiche Pfadeinrichtung im bestehenden Unterlagernetzwerk zu überprüfen.

Die letzte Voraussetzung ist keine Anforderung, sondern ermöglicht es dem SD-WAN-Administrator, zu überprüfen, ob das Unterlagernetzwerk virtuelle Pfade eingerichtet werden kann, wenn die Zero Touch Deployment mit einem neu hinzugefügten Standort abgeschlossen ist.In erster Linie wird überprüft, ob die entsprechenden Firewall- und Route-Richtlinien für den NAT-Datenverkehr entsprechend eingerichtet sind oder ob der UDP-Port 4980 erfolgreich in das Netzwerk eindringen kann, um das MCN zu erreichen.



Zero Touch-Bereitstellungsdienst —Überblick

Der Zero Touch Deployment Service arbeitet zusammen mit dem SD-WAN Center, um eine einfachere Bereitstellung von SD-WAN-Appliances in Zweigstellen zu ermöglichen. Das SD-WAN Center wird als zentrales Management-Tool für die SD-WAN Standard und Enterprise (Premium) Edition Appliances konfiguriert und verwendet.Um den Zero Touch Deployment Service (oder ZTD Cloud Service) nutzen zu können, muss ein Administrator zunächst das erste SD-WAN-Gerät in der Umgebung bereitstellen und dann das SD-WAN-Center als zentralen Verwaltungspunkt konfigurieren und bereitstellen.Wenn das SD-WAN-Center, Version 9.1 oder höher, mit Verbindung zum öffentlichen Internet an Port 443 installiert ist, initiiert SD-WAN Center automatisch den Cloud-Dienst und installiert die erforderlichen Komponenten, um die Zero Touch Deployment Features zu entsperren und die Zero Touch Deployment Option in der GUI verfügbar zu machen des SD-WAN Centers.Zero Touch Deployment ist in der SD-WAN Center-Software standardmäßig nicht verfügbar.Dies wurde speziell darauf ausgelegt, sicherzustellen, dass die richtigen vorläufigen Komponenten im Unterlagernetzwerk vorhanden sind, bevor ein Administrator jede Vor-Ort-Aktivität mit Zero Touch Deployment einleiten kann.

Nachdem eine funktionierende SD-WAN-Umgebung eingerichtet wurde und die Registrierung beim Zero Touch Deployment Service ausgeführt wurde, erfolgt durch Erstellen eines Citrix Cloud-Kontos.Da SD-WAN Center mit dem ZTD-Dienst kommunizieren kann, stellt die GUI die Zero Touch Deployment Optionen auf der Registerkarte Konfiguration zur Verfügung.Die Anmeldung beim Zero Touch Service authentifiziert die Kunden-ID, die mit der jeweiligen SD-WAN-Umgebung verknüpft ist, und registriert das SD-WAN-Center, zusätzlich zum Entsperren des Kontos für die weitere Authentifizierung von ZTD-Appliance-Bereitstellungen.

Mit dem Tool Netzwerkkonfiguration im SD-WAN Center muss der SD-WAN-Administrator dann die Vorlagen oder die Funktion zum Klonen der Site verwenden, um die SD-WAN-Konfiguration

zum Hinzufügen neuer Sites zu erstellen.Die neue Konfiguration wird vom SD-WAN-Center verwendet, um die Bereitstellung von ZTD für die neu hinzugefügten Standorte zu initiieren.Wenn der SD-WAN-Administrator eine Site für die Bereitstellung mithilfe des ZTD-Prozesses initiiert, hat er die Möglichkeit, die für ZTD zu verwendende Appliance vorab zu authentifizieren, indem er die Seriennummer vorausgefüllt und die E-Mail-Kommunikation mit dem Vor-Ort-Installationsprogramm initiiert, um die Vor-Ort-Aktivitäten zu starten.

Der Onsite-Installer erhält E-Mail-Kommunikation, dass der Standort für die Zero Touch Deployment bereit ist, und kann mit dem Installationsvorgang für das Einschalten und Verkabeln der Appliance für die DHCP-IP-Adresszuweisung und den Internetzugriff über den MGMT-Anschluss beginnen.Auch Verkabelung in allen LAN- und WAN-Ports.Alles andere wird vom ZTD Service initiiert und der Fortschritt wird durch die Verwendung der Aktivierungs-URL überwacht. Falls es sich bei dem zu installierenden Remote-Knoten um eine Cloud-Instanz handelt, startet das Öffnen der Aktivierungs-URL den Workflow, um die Instanz automatisch in der dafür vorgesehenen Cloud-Umgebung zu installieren. Ein lokaler Installer benötigt keine Aktion.

Der Zero Touch Deployment Cloud Service automatisiert die folgenden Aktionen:

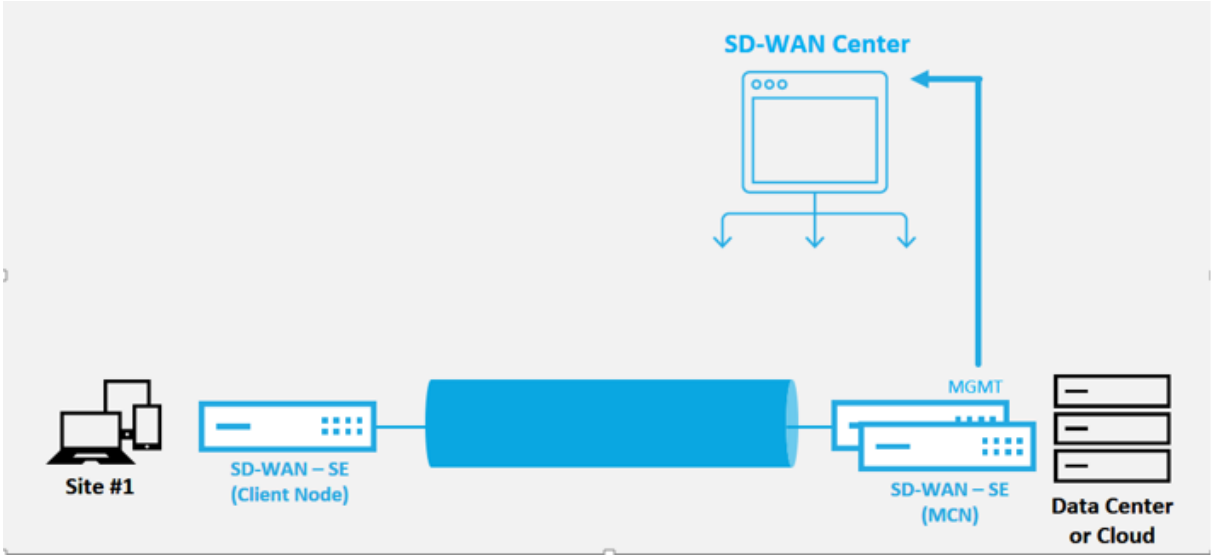
Laden Sie den ZTD Agent herunter und aktualisieren Sie, wenn neue Funktionen auf der Zweigstellenappliance verfügbar sind.

- Authentifizieren Sie die Zweigstellenappliance, indem Sie die Seriennummer überprüfen.
- Authentifizieren Sie, dass der SD-WAN-Administrator die Site für ZTD mit dem SD-WAN-Center akzeptiert hat.
- Ziehen Sie die für die Ziel-Appliance spezifische Konfigurationsdatei aus dem SD-WAN-Center.
- Push die für die Ziel-Appliance spezifische Konfigurationsdatei an die Zweigstellenappliance.
- Installieren Sie die Konfigurationsdatei auf der Zweigstellenappliance.
- Verschieben Sie alle fehlenden SD-WAN-Softwarekomponenten oder erforderlichen Updates an die Zweigstellenappliance.
- Push einer temporären 10-Mbit/s-Lizenzdatei zum Bestätigen der Herstellung virtueller Pfade zur Zweigstellenappliance.
- Aktivieren Sie den SD-WAN-Dienst auf der Zweigstellenappliance.

Der SD-WAN-Administrator benötigt weitere Schritte, um eine permanente Lizenzdatei auf der Appliance zu installieren.

Zero Touch-Bereitstellungsdienstverfahren

Im folgenden Verfahren werden die Schritte beschrieben, die erforderlich sind, um eine neue Site mithilfe des Zero Touch Deployment Service bereitzustellen.Ein laufendes MCN und ein Client-Knoten arbeiten bereits mit der richtigen Kommunikation zum SD-WAN Center, sowie etablierte virtuelle Pfade, die die Konnektivität über das Unterlagernetzwerk bestätigen. Die folgenden Schritte sind für den SD-WAN-Administrator erforderlich, um die Bereitstellung von Zero Touch zu initiieren:



Konfigurieren des Zero Touch-Bereitstellungsdiensts

Das SD-WAN-Center verfügt über die Funktionalität, um Anforderungen von neu verbundenen Appliances zu akzeptieren, um dem SD-WAN Enterprise-Netzwerk beizutreten. Die Anforderung wird über den Null-Touch-Bereitstellungsdienst an die Weboberfläche weitergeleitet. Sobald sich die Appliance mit dem Dienst verbindet, werden Konfigurationspakete und Software-Upgrade-Pakete heruntergeladen.

Konfigurationsworkflow:

- Öffnen Sie **SD-WAN Center** > **Neue Standortkonfiguration erstellen** oder vorhandene Konfiguration importieren und speichern Sie sie.
- Melden Sie sich bei Citrix Workspace Cloud an, um den ZTD-Dienst zu aktivieren. Die Menüoption Zero Touch Deployment wird nun in der Web-Verwaltungsschnittstelle des SD-WAN Center angezeigt.
- Navigieren Sie in SD-WAN Center zu **Konfiguration** > **Zero Touch-Bereitstellung** > **Neue Site bereitstellen**.
- Wählen Sie eine Appliance aus, klicken Sie auf Aktivieren und dann auf **Bereitstellen**.
- Installer erhält Aktivierungs-E-Mail > Geben Sie die Seriennummer ein > **Aktivieren** > Appliance wurde erfolgreich bereitgestellt.

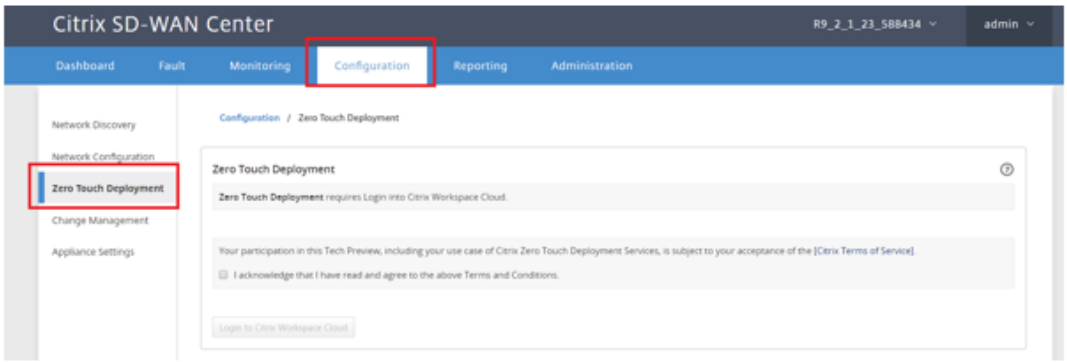
So konfigurieren Sie Zero Touch-Bereitstellungsdienst:

1. Installieren Sie SD-WAN Center mit aktivierten Zero Touch Deployment Funktionen.
    a) Installieren Sie SD-WAN Center mit DHCP zugewiesener IP-Adresse.
    b) Stellen Sie sicher, dass das SD-WAN Center eine ordnungsgemäße Management-IP-Adresse und Netzwerk-DNS-Adresse mit Konnektivität zum öffentlichen Internet im

Verwaltungsnetzwerk zuweist.

c) Aktualisieren Sie das SD-WAN Center auf die neueste Version der SD-WAN-Software.

d) Bei ordnungsgemäßer Internetverbindung initiiert das SD-WAN-Center den Zero Touch Deployment (ZTD) Cloud Service und lädt automatisch alle für ZTD spezifischen Firmware-Updates herunter und installiert sie. Wenn diese Call-Home-Prozedur fehlschlägt, ist die folgende Zero Touch Deployment Option in der GUI nicht verfügbar.



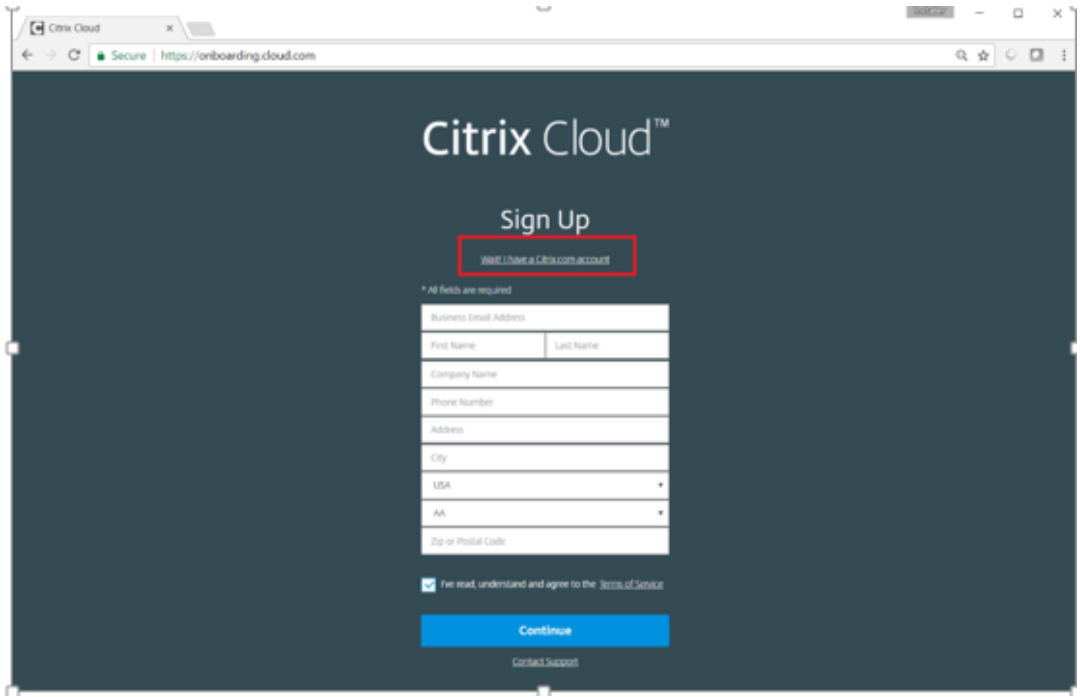
e) Lesen Sie die Allgemeinen Geschäftsbedingungen und wählen Sie dann **Ich bestätige, dass ich die oben genannten Geschäftsbedingungen gelesen habe und damit einverstanden bin**.

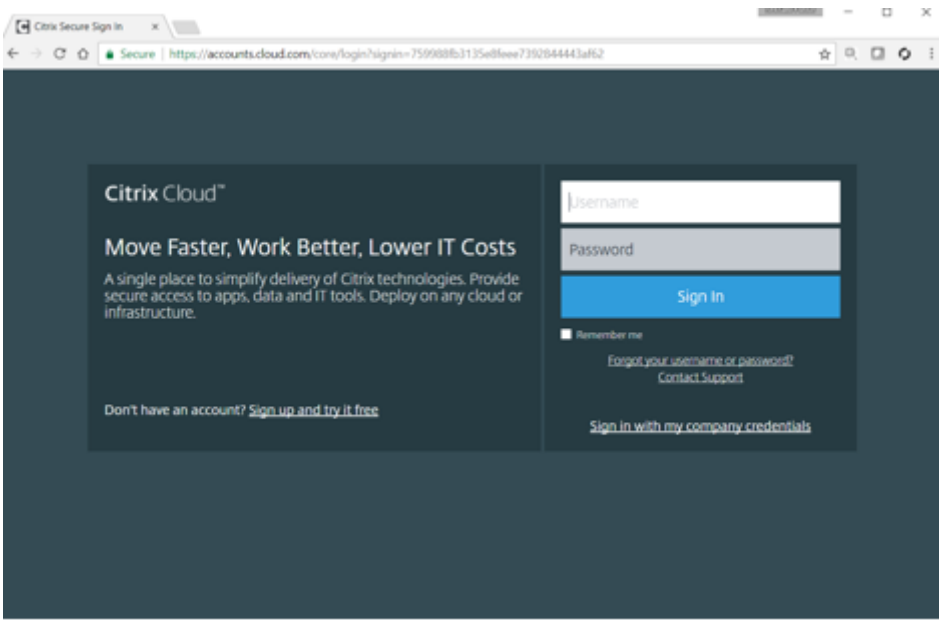
f) Klicken Sie auf die Schaltfläche **Anmelden bei Citrix Workspace Cloud**, wenn bereits ein Citrix Cloud-Konto erstellt wurde.

g) Melden Sie sich im Citrix Cloud-Konto an, und wenn Sie die folgende Meldung über die erfolgreiche Anmeldung erhalten haben, **schließen Sie bitte dieses Fenster NICHT. Der Prozess benötigt weitere ~20 Sekunden, damit die grafische Benutzeroberfläche des SD-WAN CENTER aktualisiert wird.** Das Fenster sollte sich selbst schließen, wenn es abgeschlossen ist.**

h) Gehen Sie folgendermaßen vor, um ein Cloud Login-Konto zu erstellen:

- Öffnen Sie einen Webbrowser, umhttps://onboarding.cloud.com
- Klicken Sie auf den Link für **Moment, ich habe ein Citrix.com Konto**.





i) Melden Sie sich mit einem vorhandenen Citrix Konto an.

j) Sobald Sie sich bei der SD-WAN Center Zero Touch Deployment Seite angemeldet haben, stellen Sie möglicherweise fest, dass keine Sites für die ZTD-Bereitstellung verfügbar sind, aus folgenden Gründen:

- Die aktive Konfiguration wurde nicht im Dropdownmenü Konfiguration ausgewählt.
- Alle Sites für die aktuelle aktive Konfiguration wurden bereits bereitgestellt
- Die Konfiguration wurde nicht mit dem SD-WAN Center erstellt, sondern mit dem Konfigurationseditor, der im MCN

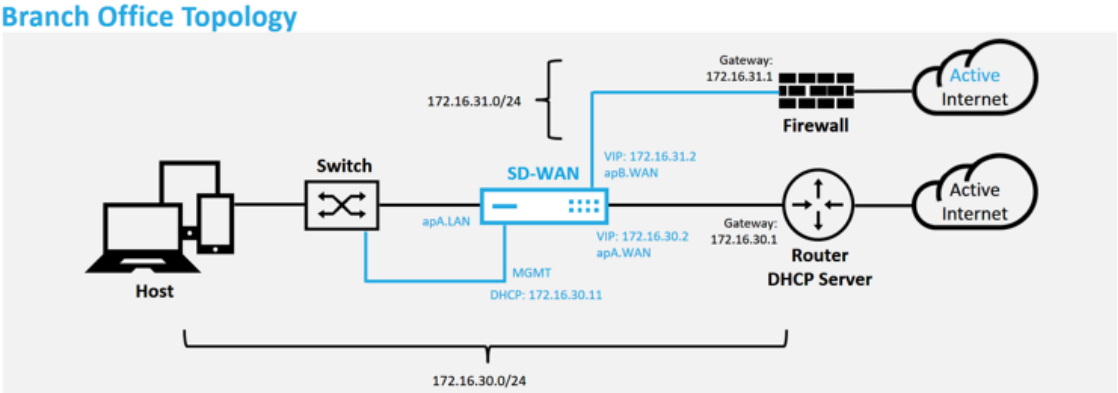
- Sites wurden nicht in der Konfiguration eingebaut, die Null-touch-fähige Geräte referenziert (z. B. 410-SE, 2100-SE, Cloud VPX)

2. Aktualisieren Sie die Konfiguration, um einen **neuen Remote-** Standort mit einer **ZTD-fähigen SD-WAN-Appliance** mithilfe der SD-WAN-Center-Netzwerkkonfiguration hinzuzufügen.

   Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkkonfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center.Für die Zero Touch Deployment Funktion muss der SD-WAN-Administrator die Konfiguration mithilfe von SD-WAN Center erstellen.Das folgende Verfahren sollte verwendet werden, um eine neue Site hinzuzufügen, die für die Null-Touch-Bereitstellung vorgesehen ist.

   Entwerfen Sie die neue Site für die SD-WAN-Appliance-Bereitstellung, indem Sie zunächst die Details der neuen Site skizzieren (Appliance-Modell, Verwendung von Schnittstellengruppen, virtuelle IP-Adressen, WAN-Verbindungen mit Bandbreite und deren jeweiligen Gateways).

   > **Wichtig**
   >
   > Möglicherweise bemerken Sie jeden Standortknoten, auf dem VPX ausgewählt wurde, als das Modell ebenfalls aufgeführt ist, aber derzeit ist ZTD-Unterstützung nur für die AWS VPX-Instanz verfügbar.
   >
   > **Hinweis**
   >
   > - Stellen Sie sicher, dass Sie einen Support-Webbrowser für Citrix SD-WAN Center verwenden
   > - Stellen Sie sicher, dass der Webbrowser während der Citrix Workspace-Anmeldung keine Popupfenster blockiert.

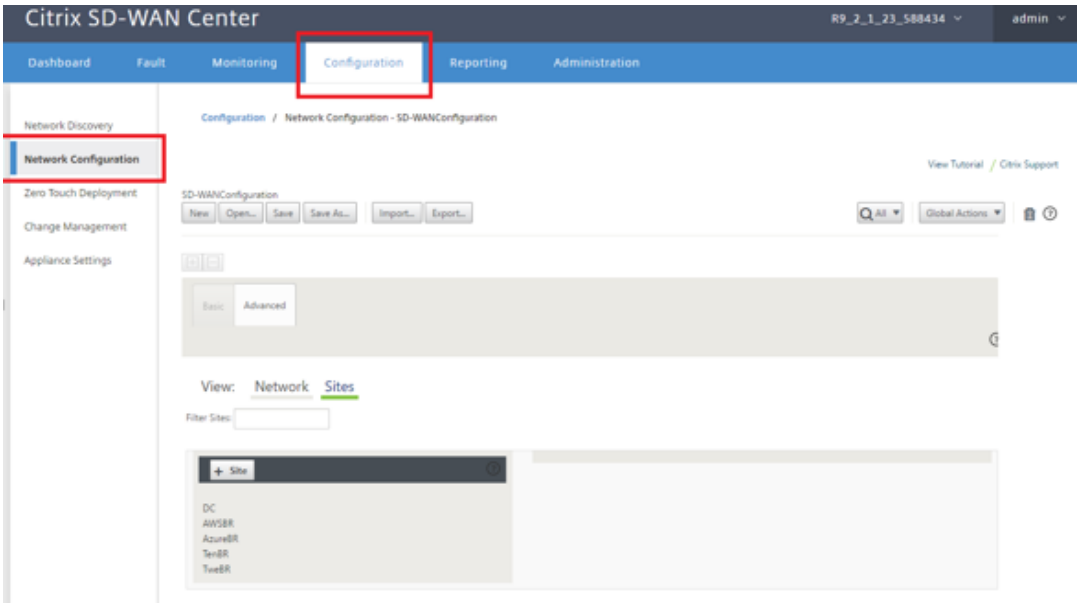
   Dies ist ein Beispiel für die Bereitstellung eines Zweigstellenstandorts, die SD-WAN-Appliance wird physisch im Pfad der vorhandenen MPLS-WAN-Verbindung über ein 172.16.30.0/24 -Netzwerk bereitgestellt und eine vorhandene Sicherungsverbindung verwendet, indem sie in einen aktiven Zustand aktiviert und diese zweite WAN-Verbindung direkt in die SD-WAN-Appliance auf ein anderes Subnetz 172.16.31.0/24.

Hinweis

Die SD-WAN-Appliances weisen automatisch eine Standard-IP-Adresse von 192.168.100.1/16 zu.Wenn DHCP standardmäßig aktiviert ist, stellt der DHCP-Server im Netzwerk der Appliance möglicherweise eine zweite IP-Adresse in einem Subnetz zur Verfügung, die den Standardwert überlappt.Dies kann möglicherweise zu einem Routingproblem auf der Appliance führen, bei dem die Appliance möglicherweise keine Verbindung zum ZTD Cloud Service herstellen kann. Konfigurieren Sie den DHCP-Server so, dass IP-Adressen außerhalb des Bereichs 192.168.0.0/16 zugewiesen werden.

Für die SD-WAN-Produktplatzierung in einem Netzwerk stehen verschiedene Bereitstellungsmodi zur Verfügung. Im obigen Beispiel wird SD-WAN als Overlay auf der vorhandenen Netzwerkinfrastruktur bereitgestellt.Bei neuen Sites können SD-WAN-Administratoren das SD-WAN im Edge- oder Gateway-Modus bereitstellen, wodurch ein WAN-Edge-Router und eine Firewall entfällt und die Netzwerkanforderungen für Edge-Routing und Firewall auf der SD-WAN-Lösung konsolidiert werden.

a) Öffnen Sie die **SD-WAN Center-Webverwaltungsoberfläche** und navigieren Sie zur Seite **Configuration** > **Network Configuration**.



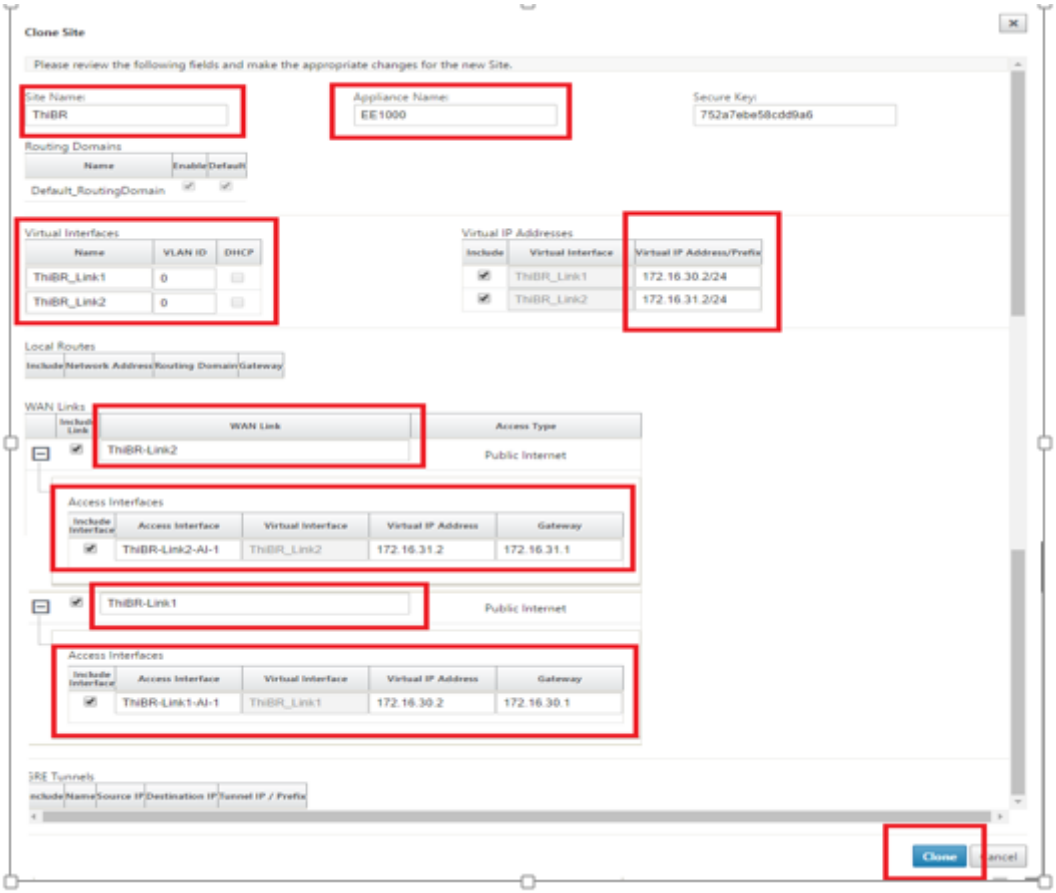
b) Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration aus dem MCN.

c) Navigieren Sie zur Registerkarte Erweitert, um eine Site zu erstellen.

d) Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.

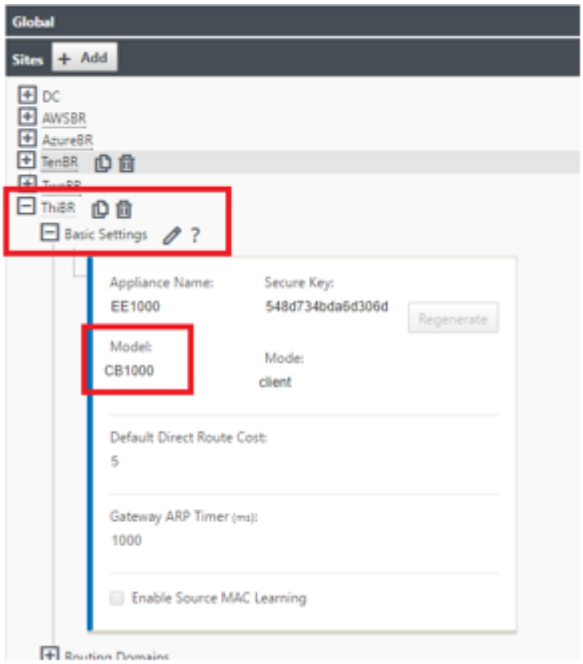
e) Schnelle Konfiguration für die neue Site mithilfe der Clone-Funktion einer vorhandenen Site erstellt.

f) Füllen Sie alle erforderlichen Felder aus der für diesen neuen Zweigstandort entworfenen Topologie aus.



g) Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen**der Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-

Dienst unterstützen würde.



h) Das SD-WAN-Modell für die Site kann aktualisiert werden. Beachten Sie jedoch, dass die Schnittstellengruppen möglicherweise neu definiert werden müssen, da die aktualisierte Appliance möglicherweise ein neues Schnittstellenlayout hat, das zum Klonen verwendet wurde.

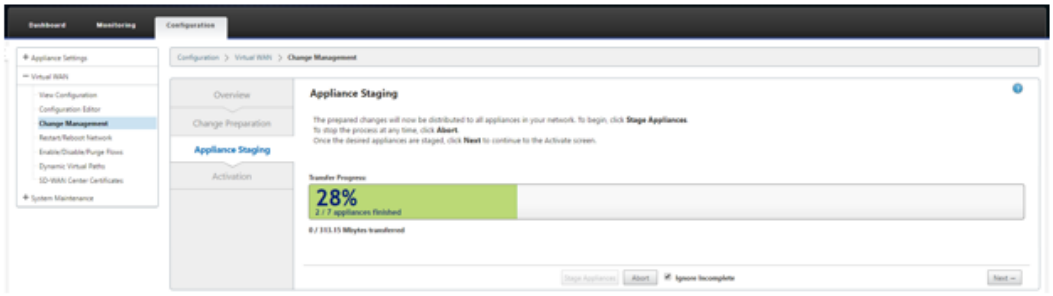
i) Speichern Sie die neue Konfiguration im SD-WAN Center, und verwenden Sie den Export in die Option **Change Management Posteingang**, um die Konfiguration mithilfe der Änderungsverwaltung zu verschieben.

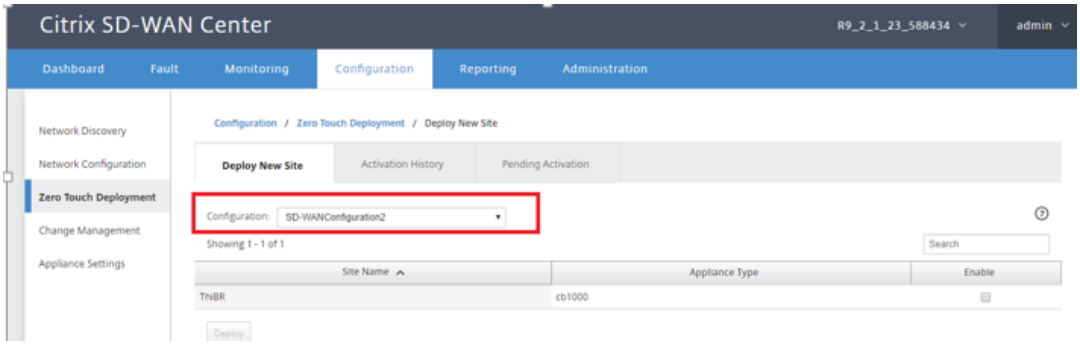
j) Befolgen Sie das Änderungsverwaltungsverfahren, um die neue Konfiguration ordnungsgemäß zu implementieren, wodurch die vorhandenen SD-WAN-Geräte über die neue Site informiert werden, die per Zero Touch bereitgestellt werden soll. Sie müssen die Option Unvollständig ignorieren verwenden, um den Versuch zu überspringen, die Konfiguration auf die neue Site zu übertragen, die noch benötigt wird. durch den ZTD-Workflow.

3. Navigieren Sie zurück zur Seite Zero Touch Deployment von SD-WAN Center, und wenn die neue aktive Konfiguration ausgeführt wird, steht die neue Site für die Bereitstellung zur Verfügung.

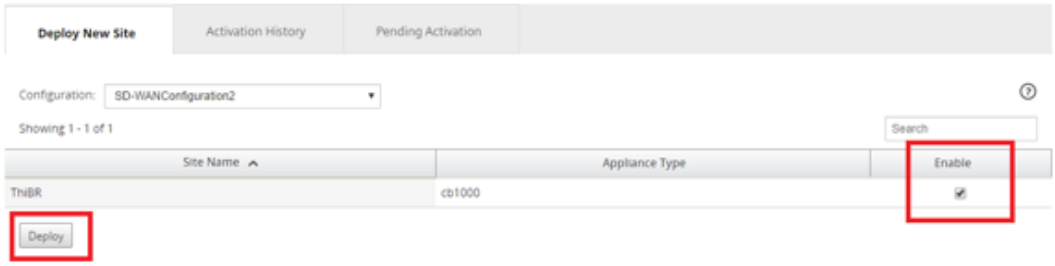
   a) Wählen Sie auf der Seite Zero Touch-Bereitstellung unter der Registerkarte **Neue Site bereitstellen** die ausgeführte Netzwerkkonfigurationsdatei

   b) Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit nicht bereitgestellten SD-WAN-Geräten angezeigt, die für Zero Touch unterstützt werden.

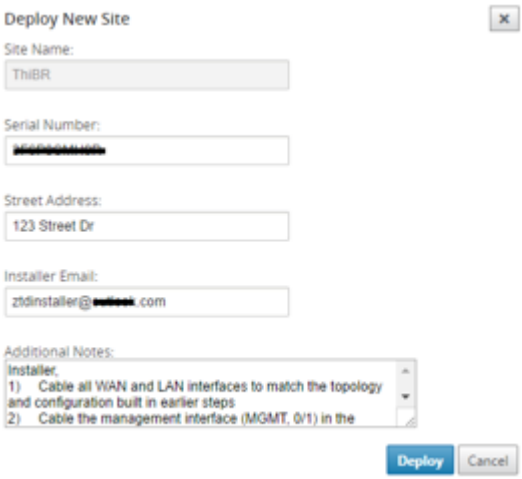




c) Wählen Sie die Zweigsites aus, die Sie für den Zero Touch-Dienst konfigurieren möchten, klicken Sie auf **Aktivieren**und dann **Bereitstellen**.



d) Es wird ein Popupfenster Neue Site bereitstellen angezeigt, in dem der Administrator bei Bedarf die Seriennummer, die Straßenadresse der Zweigstelle, die E-Mail-Adresse des Installers und weitere Hinweise angeben kann.

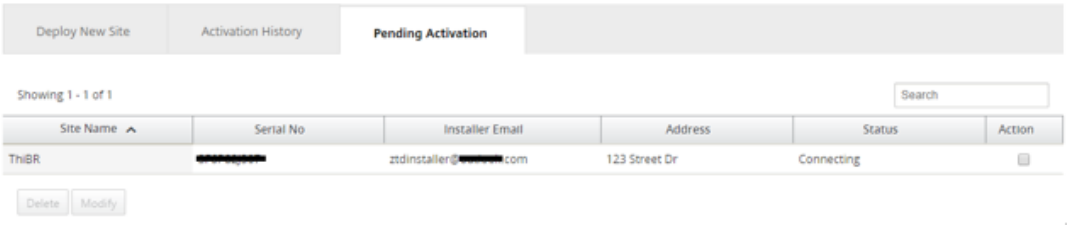


> **Hinweis**
>
> - Das Eingabefeld Seriennummer ist optional und führt je nachdem, ob es ausgefüllt ist oder nicht, zu einer Änderung der Vor-Ort-Aktivitäten, für die der Installer verantwortlich ist.
> - Wenn das Feld Seriennummer ausgefüllt ist —Das Installationsprogramm muss keine Seriennummer in die Aktivierungs-URL eingeben, die mit dem Befehl "site bereitstellen"generiert wurde.
> - Wenn das Feld "Seriennummer"schwarz bleibt —Das Installationsprogramm ist dafür verantwortlich, die korrekte Seriennummer der Appliance in die Aktivierungs-URL einzugeben, die mit dem Befehl "Bereitstellen"generiert wurde.

a) Nachdem Sie auf die Schaltfläche **Bereitstellen** geklickt haben, wird eine Meldung angezeigt, dass Die Standortkonfiguration wurde bereitgestellt.

b) Diese Aktion veranlasst das SD-WAN Center, das zuvor beim ZTD Cloud Service registriert wurde, die Konfiguration dieser bestimmten Site als temporär im ZTD Cloud Service gespeichert zu teilen.

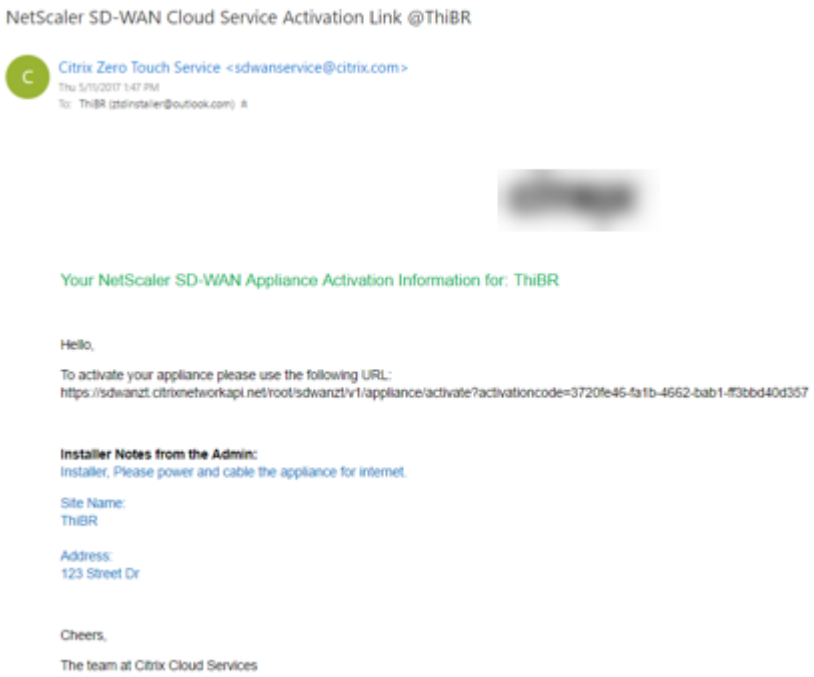
c) Navigieren Sie zur Registerkarte Ausstehende Aktivierung, um zu bestätigen, dass die Informationen der Zweigstandsite-Site erfolgreich ausgefüllt wurden und in den Status der ausstehenden Installationsaktivität versetzt wurden.



> **Hinweis**
>
> Eine Null-Touch-Bereitstellung im Status Ausstehende Aktivierung kann optional auf Löschen oder Ändern gewählt werden, wenn die Informationen falsch sind. Wenn eine Site von der ausstehenden Aktivierungsseite gelöscht wird, kann sie auf der Registerkarte Neue Site bereitstellen bereitgestellt werden. Sobald Sie die Zweig-Site aus der ausstehenden Aktivierung löschen möchten, wird der Aktivierungslink, der an das Installationsprogramm gesendet wird, ungültig.
>
> Wenn das Feld Seriennummer nicht vom SD-WAN-Administrator ausgefüllt wurde, zeigt das Statusfeld Warten auf Installer anstelle von Verbinden.

4. Die nächste Reihe von Aktivitäten wird vom Vor-Ort-Installateur durchgeführt.

   a) Das Installationsprogramm überprüft das Postfach auf die E-Mail-Adresse, die der SD-WAN-Administrator beim Bereitstellen der Site verwendet hat.


NetScaler SD-WAN Cloud Service Activation Link @ThiBR

Citrix Zero Touch Service <sdwanservice@citrix.com>

Your NetScaler SD-WAN Appliance Activation Information for: ThiBR

Hello,

To activate your appliance please use the following URL:
https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate?activationcode=3720fe46-fa1b-4662-bab1-ff3bbd40d357

Installer Notes from the Admin:
Installer, Please power and cable the appliance for internet.

Site Name:
ThiBR

Address:
123 Street Dr

Cheers,

The team at Citrix Cloud Services

   b) Öffnen Sie die Aktivierungs-URL für die Zero Touch-Bereitstellung in einem Internetbrowserfenster.

   c) Wenn der SD-WAN-Administrator die Seriennummer im Schritt Bereitstellungsstandort nicht vorausgefüllt hat, ist der Installer dafür verantwortlich, die Seriennummer auf der physischen Appliance zu finden und die Seriennummer manuell in die Aktivierungs-URL einzugeben, und klicken Sie dann auf die Schaltfläche **Aktivieren**.

d) Wenn der Administrator die Seriennummerninformationen vorab ausfüllt, ist die Aktivierungs-URL bereits zum nächsten Schritt weitergegangen.

e) Der Installer muss physisch vor Ort sein, um die folgenden Aktionen auszuführen:

- Verkabeln Sie alle WAN- und LAN-Schnittstellen an die Topologie und Konfiguration, die in früheren Schritten erstellt wurden.
- Verkabeln Sie die Verwaltungsschnittstelle (MGMT, 0/1) im Segment des Netzwerks, das DHCP-IP-Adresse und -Konnektivität mit dem Internet mit DNS- und FQDN zu IP-Adressenauflösung bereitstellt.
- Netzkabel der SD-WAN-Appliance.
- Schalten Sie den Netzschalter der Appliance ein.

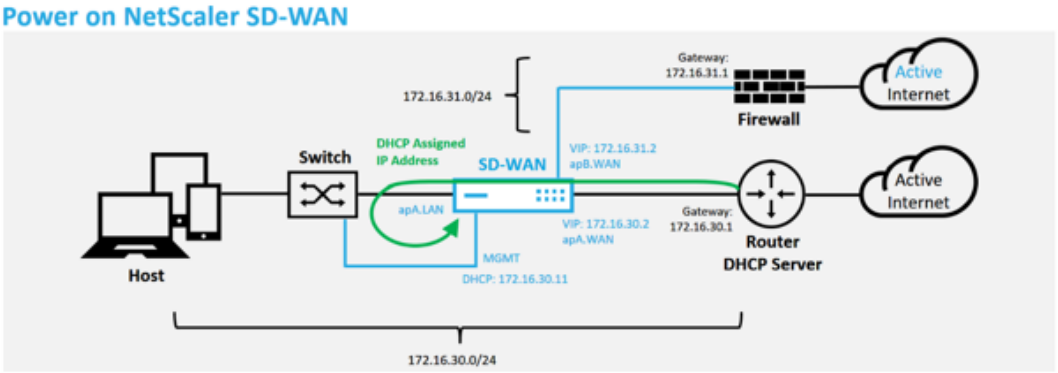
> **Hinweis**
>
> Die meisten Appliances schaltet sich automatisch ein, wenn das Netzkabel angeschlossen ist.Einige Geräte müssen möglicherweise über den Netzschalter an der Vorderseite des Geräts eingeschaltet werden, andere haben den Netzschalter auf der Rückseite des Geräts.Einige Netzschalter müssen den Netzschalter gedrückt halten, bis das Gerät eingeschaltet ist.

5. Die nächste Reihe von Schritten wird mit Hilfe des Zero Touch Deployment Service automatisiert, erfordert jedoch, dass die folgenden Voraussetzungen zur Verfügung stehen.

- Die Branch-Appliance sollte hochgefahren werden
- DHCP muss im vorhandenen Netzwerk verfügbar sein, um Verwaltungs- und DNS-IP-Adresse zuzuweisen
- Jede DHCP-zugewiesene IP-Adresse erfordert eine Verbindung zum Internet mit der Fähigkeit, FQDNs aufzulösen

- IP-Zuweisung kann manuell konfiguriert werden, solange die anderen Voraussetzungen erfüllt sind

a) Die Appliance erhält eine IP-Adresse vom Netzwerk DHCP-Server. In dieser Beispieltopologie wird dies über die umgangenen Datenschnittstellen einer werkseitigen Standardzustandsanwendung erreicht.

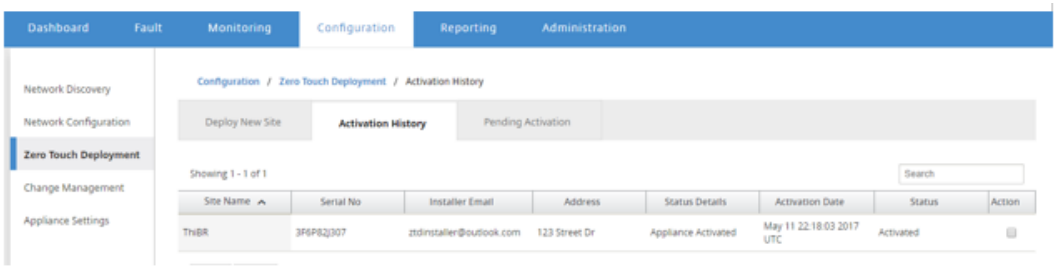


b) Wenn die Appliance die Webverwaltungs- und DNS-IP-Adressen vom DHCP-Server des Unterlagernetzwerks abruft, initiiert die Appliance den Zero Touch Deployment Service und lädt alle mit ZTD zusammenhängenden Softwareupdates herunter.

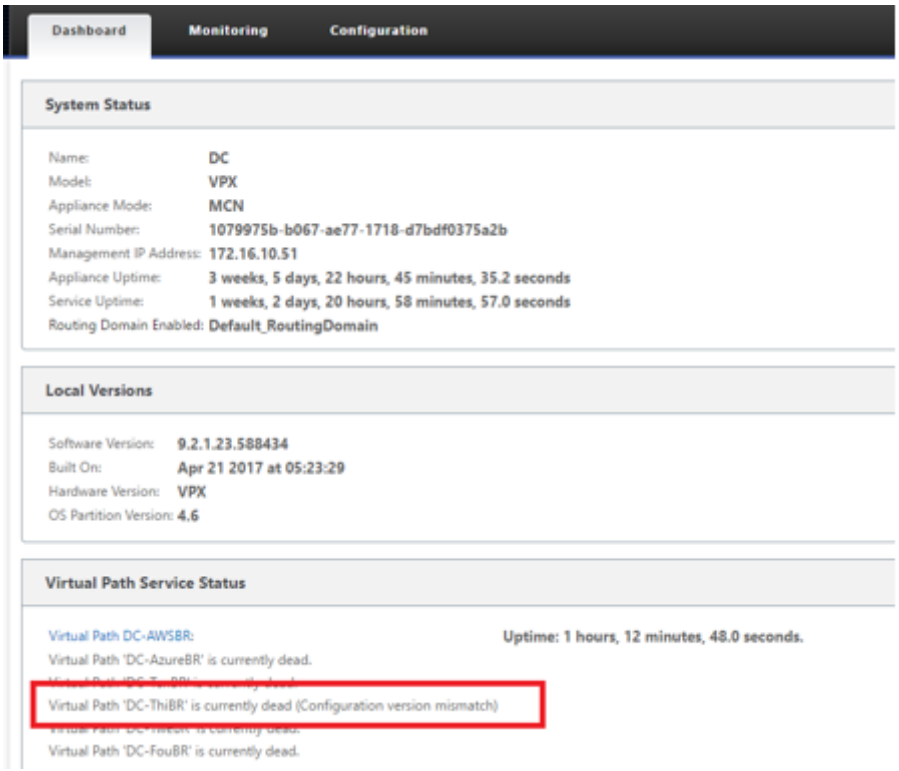
c) Bei erfolgreicher Konnektivität zum ZTD Cloud Service führt der Bereitstellungsprozess automatisch folgende Schritte aus:

- Laden Sie die Konfigurationsdatei herunter, die zuvor vom SD-WAN-Center gespeichert wurde
- Anwenden der Konfiguration auf die lokale Appliance
- Laden Sie eine temporäre Lizenzdatei mit 10 MB herunter und installieren Sie sie
- Herunterladen und Installieren von Softwareupdates bei Bedarf
- Aktivieren Sie den SD-WAN-Dienst

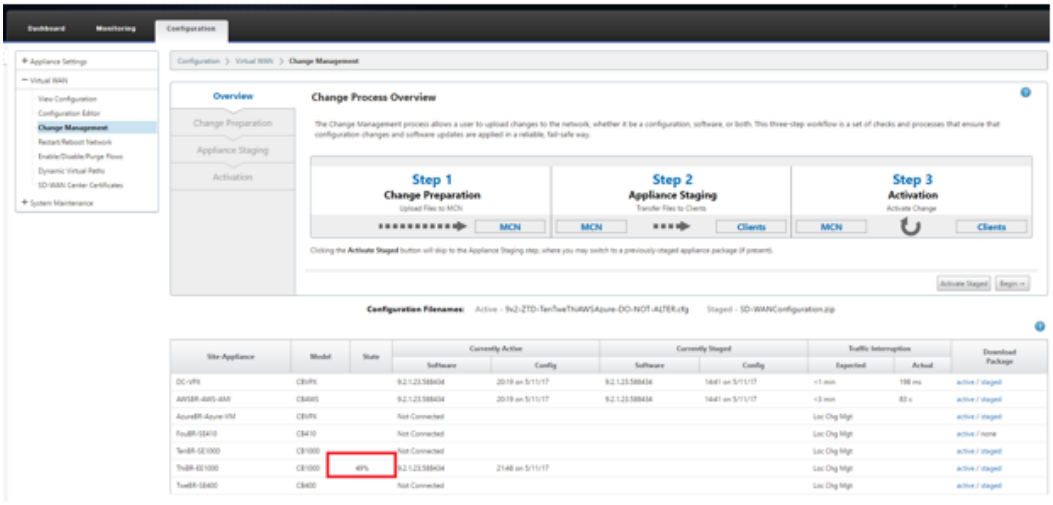
d) Eine weitere Bestätigung kann in der Web-Management-Oberfläche des SD-WAN Center erfolgen, das Zero Touch Deployment Menü zeigt erfolgreich aktivierte Appliances auf der Registerkarte **Aktivierungsverlauf an**.



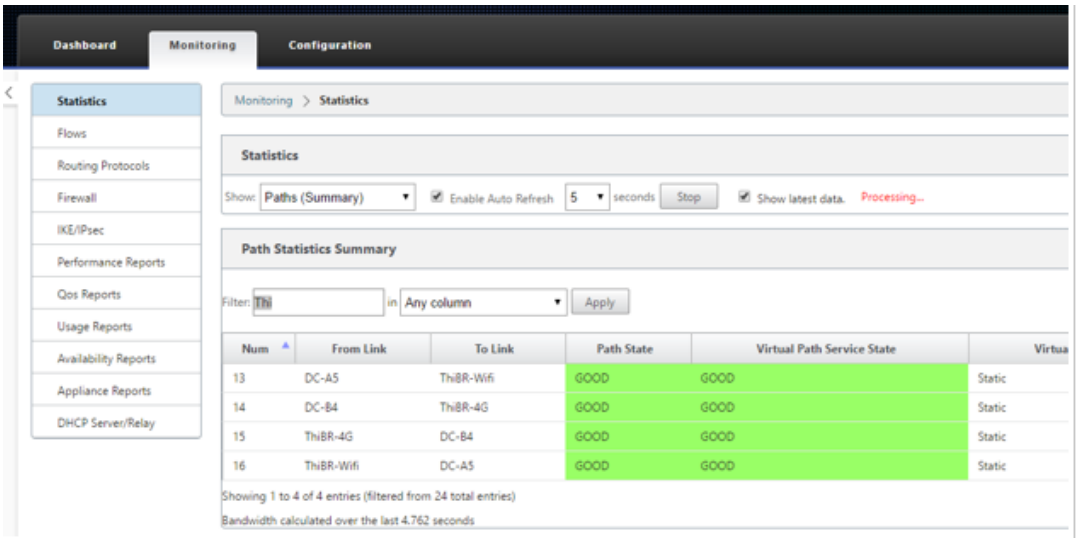
e) Die virtuellen Pfade werden möglicherweise nicht sofort in einem verbundenen Zustand angezeigt, da das MCN der Konfiguration nicht vertraut, die vom ZTD Cloud Service übergeben wird, und meldet Konfigurationsversion mismatch im MCN Dashboard.



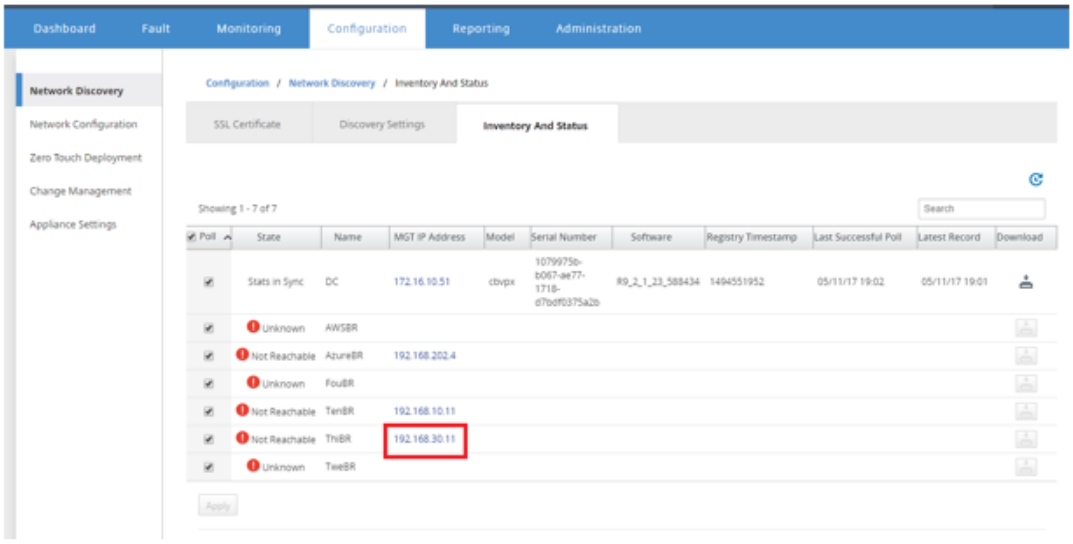
f) Die Konfiguration wird erneut an die neu installierte Zweigstellen-Appliance übermittelt und der Status wird auf der Seite **MCN** > **Konfiguration** > **Virtuelles WAN** > **Änderungsmanagement** überwacht (dieser Vorgang kann einige Minuten dauern).



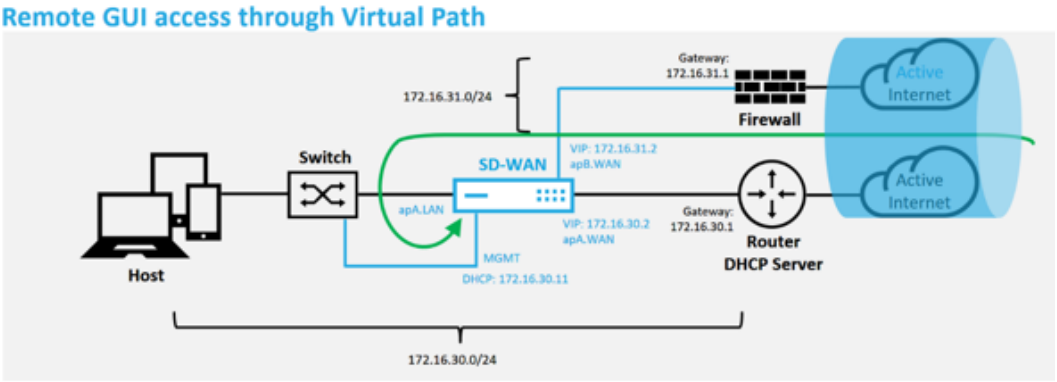
g) Der SD-WAN-Administrator kann die Head-End-MCN-Webverwaltungsseite für die etablierten virtuellen Pfade der Remotesite überwachen.



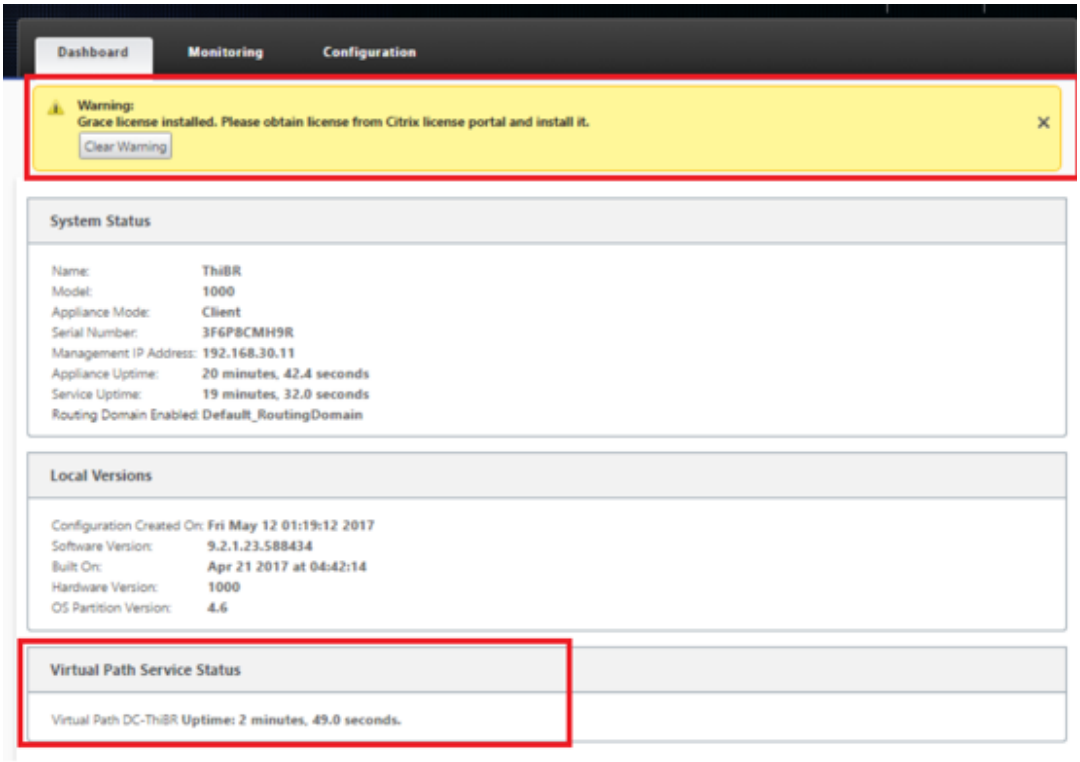
h) Das SD-WAN-Center kann auch verwendet werden, um die DHCP-zugewiesene IP-Adresse der Vor-Ort-Appliance auf der Seite **Konfiguration** > **Netzwerkerkennung** > **Bestandsliste und Status** zu identifizieren.



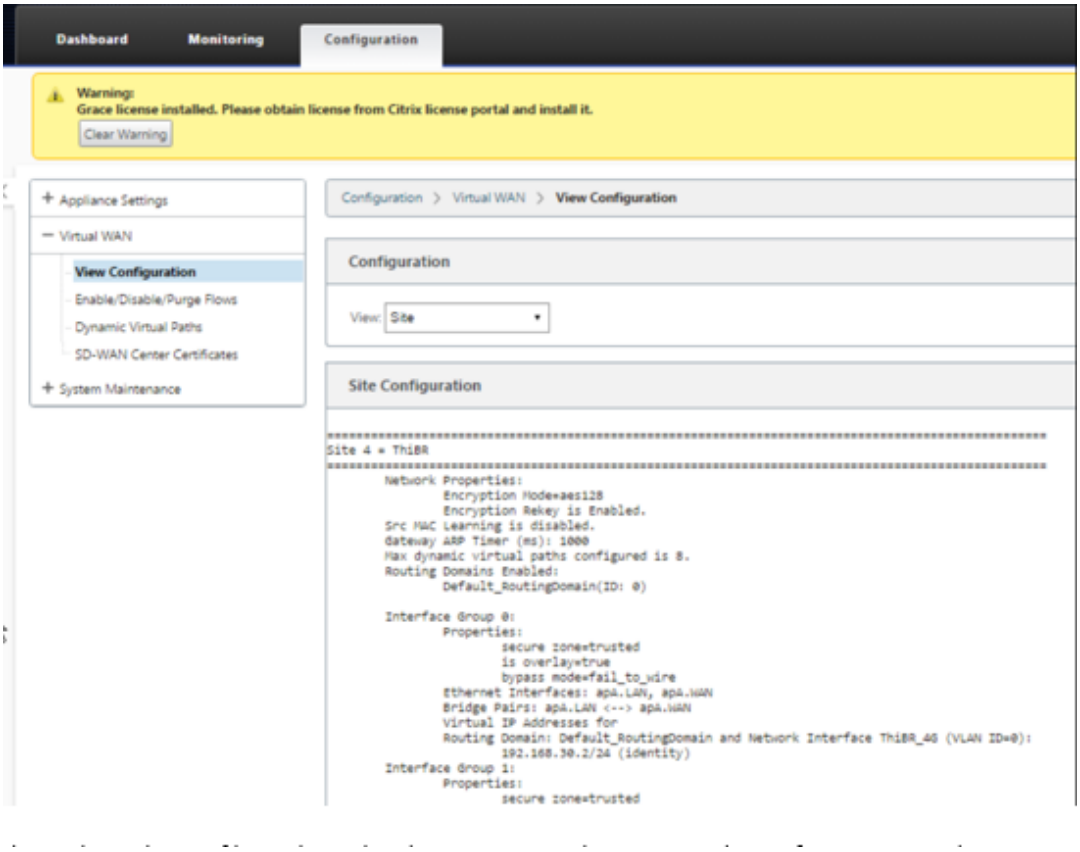
i) Zu diesem Zeitpunkt kann der SD-WAN-Netzwerkadministrator über das SD-WAN-Overlay-Netzwerk auf die Vor-Ort-Appliance zugreifen.



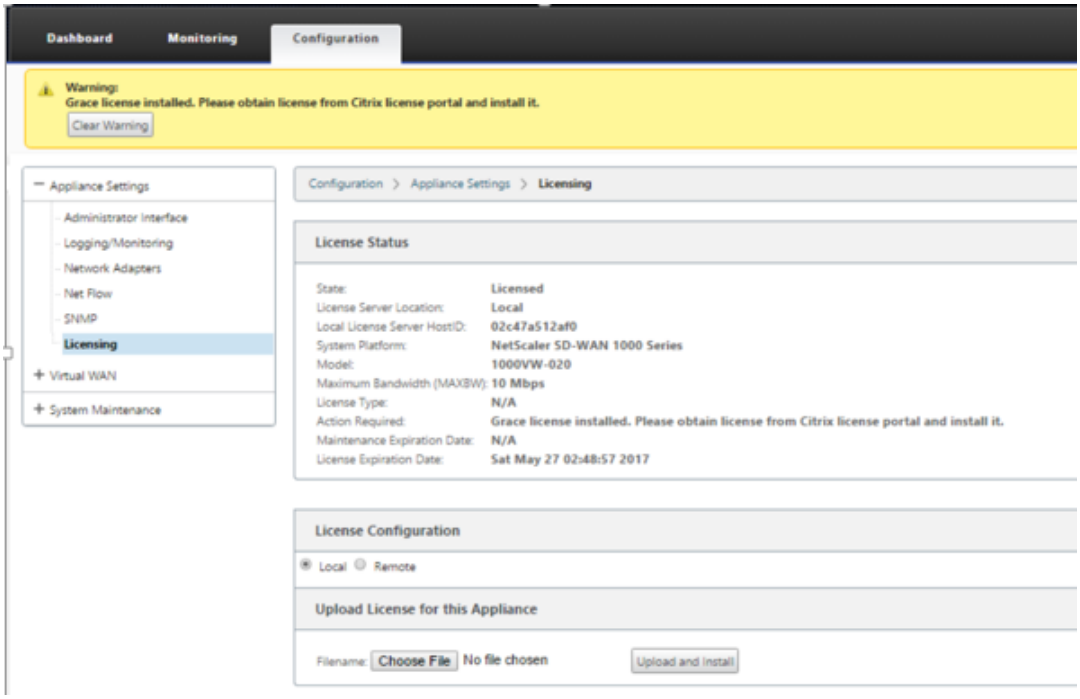
j) Der Webverwaltungszugriff auf die Remote-Standort-Appliance zeigt an, dass die Appliance mit einer temporären Gnadenlizenz von 10 Mbit/s installiert wurde, wodurch der Status des Virtual Path Service als aktiv gemeldet werden kann.



k) Die Appliance-Konfiguration kann über die Seite **Konfiguration** > **Virtuelles WAN** > **Konfiguration anzeigen** validiert werden.



l) Die Appliance-Lizenzdatei kann auf der Seite **Konfiguration** > **Appliance-Einstellungen** > **Lizenzierung** auf eine permanente Lizenz aktualisiert werden.



m) Nach dem Hochladen und Installieren der permanenten Lizenzdatei verschwindet

das Warnbanner von Grace License und während der Lizenzinstallation wird kein Verbindungsverlust mit der Remote-Site auftreten (keine Pings werden gelöscht).

On-Prem Zero-Touch

April 13, 2021

Anweisungen zum Bereitstellen einer SD-WAN-Appliance mit Zero Touch Service finden Sie im Thema;Konfigurieren des Zero Touch-Bereitstellungsdiensts.

AWS

April 13, 2021

Bereitstellen in AWS

Mit SD-WAN Version 9.3 wurden die Null-Touch-Bereitstellungsfunktionen auf Cloud-Instanzs erweitert.Das Verfahren zur Bereitstellung von Zero Touch-Bereitstellungsprozess vier Cloud-Instanzen unterscheidet sich geringfügig von der Appliance-Bereitstellung für Zero Touch-Dienst.

1. Aktualisieren Sie die Konfiguration, um mithilfe der SD-WAN-Center-Netzwerkkonfiguration einen neuen Remote-Standort mit einem ZTD-fähigen SD-WAN-Cloud-Gerät hinzuzufügen.

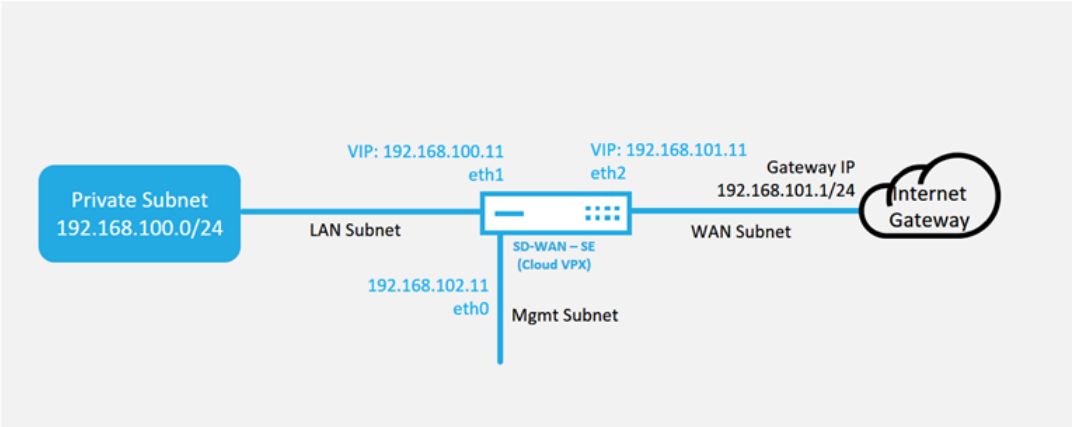
   Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkkonfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center.Für die Zero Touch Deployment Funktion muss der SD-WAN-Administrator die Konfiguration mithilfe von SD-WAN Center erstellen.Das folgende Verfahren sollte verwendet werden, um einen neuen Cloud-Knoten hinzuzufügen, der für die Null-Touch-Bereitstellung vorgesehen ist.

   a) Entwerfen Sie die neue Site für die SD-WAN-Cloud-Bereitstellung, indem Sie zunächst die Details der neuen Site skizzieren (z. B. die VPX-Größe, die Verwendung von Schnittstellengruppen, virtuelle IP-Adressen, WAN-Link (s) mit Bandbreite und deren jeweiligen Gateways).

      > **Hinweis**
      >
      > - In der Cloud bereitgestellte SD-WAN-Instanzen müssen im Edge/Gateway -Modus

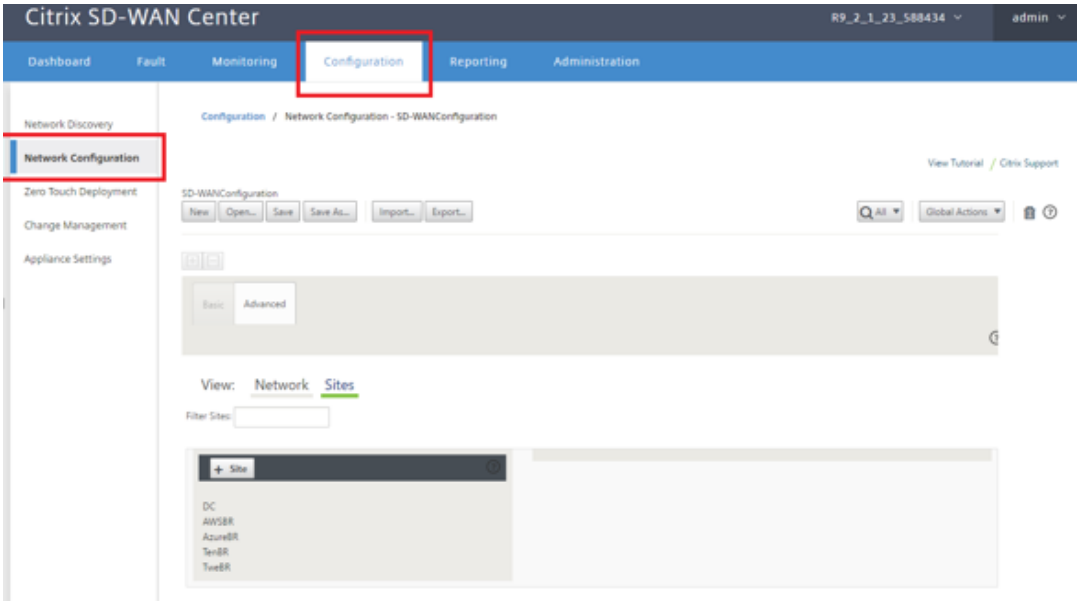
> bereitgestellt werden.
> - Die Vorlage für die Cloud-Instanz ist auf drei Schnittstellen beschränkt: Management, LAN und WAN (in dieser Reihenfolge).
> - Die verfügbaren Cloud-Vorlagen für SD-WAN VPX sind derzeit hart festgelegt, um die #. #. #.11 IP-Adresse der verfügbaren Subnetze in der VPC zu erhalten.

Cloud Topology with NetScaler SD-WAN



Dies ist ein Beispiel für die Bereitstellung einer SD-WAN-Cloud bereitgestellten Site. Das Citrix SD-WAN-Gerät wird als Edge-Gerät bereitgestellt, das eine einzelne Internet-WAN-Verbindung in diesem Cloud-Netzwerk bedient.Remote-Standorte können mehrere unterschiedliche Internet-WAN-Verbindungen nutzen, die mit demselben Internet-Gateway für die Cloud verbunden sind, wodurch Ausfallsicherheit und aggregierte Bandbreitenkonnektivität von jedem SD-WAN-Bereitstellungsstandort zur Cloud-Infrastruktur bereitgestellt werden.Dies ermöglicht eine kostengünstige und äußerst zuverlässige Konnektivität zur Cloud.

b) Öffnen Sie die Web-Management-Schnittstelle des SD-WAN Center, und navigieren Sie zur Seite **Konfiguration** > **Netzwerkkonfiguration**.

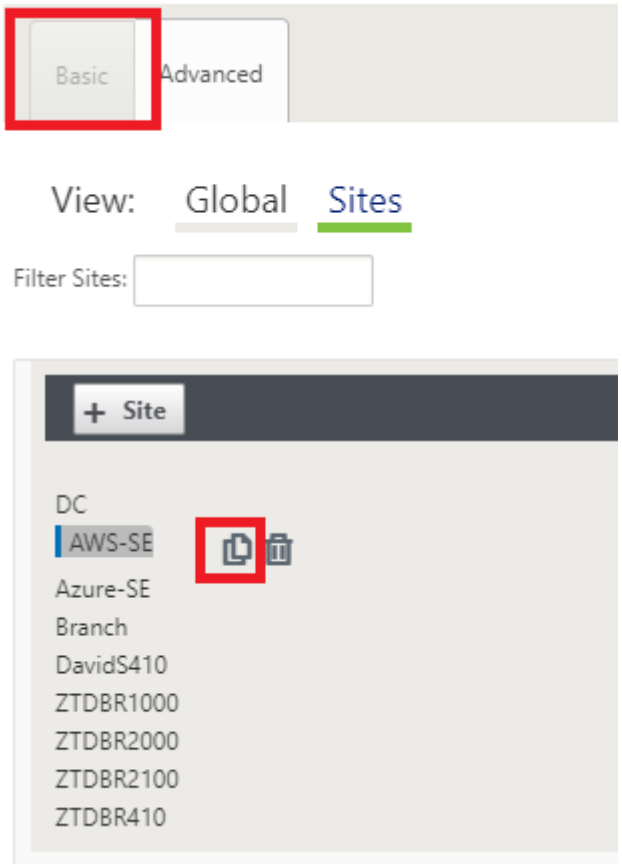


c) Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration aus dem MCN.

d) Navigieren Sie zur Registerkarte Basic, um eine neue Site zu erstellen.

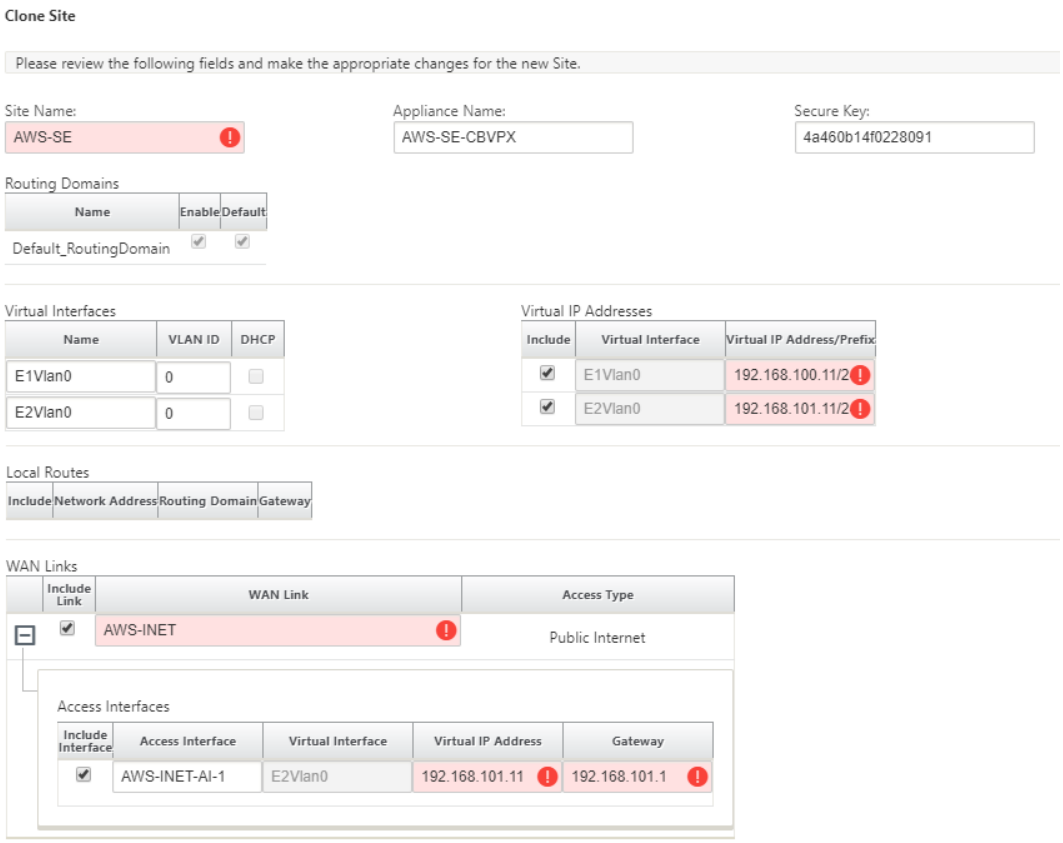
e) Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.

f) Erstellen Sie schnell die Konfiguration für die neue Cloud-Site, indem Sie die Clone-Funktion einer vorhandenen Site verwenden oder manuell eine neue Site erstellen.

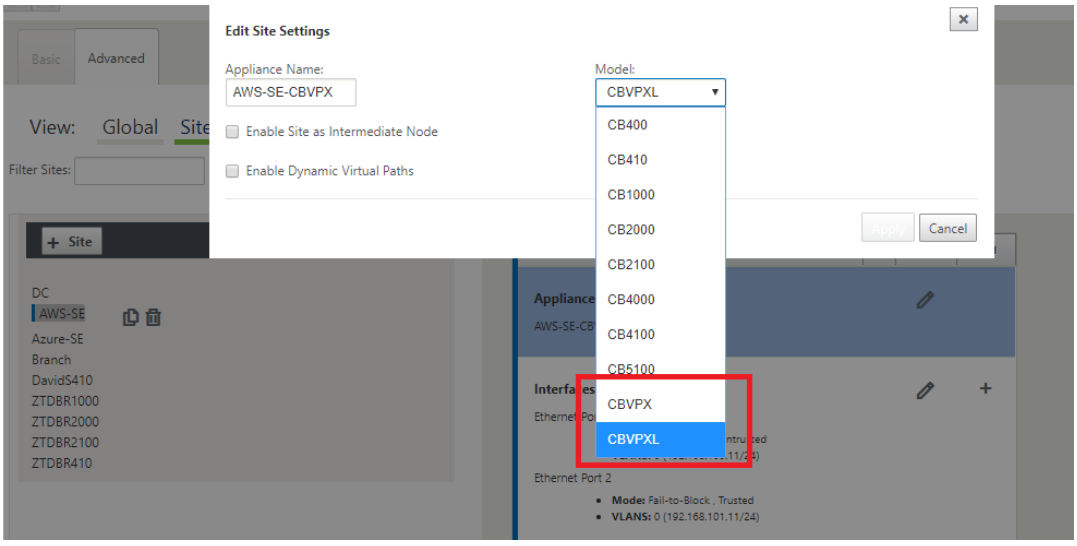


g) Füllen Sie alle erforderlichen Felder aus der zuvor für diese neue Cloud-Site entwickelten Topologie aus.

   Beachten Sie, dass die für Cloud-ZTD-Bereitstellungen verfügbare Vorlage fest festgelegt ist, um die #.#.#.11-IP-Adresse für die Mgmt-, LAN- und WAN-Subnetze zu verwenden.Wenn die Konfiguration nicht so eingestellt ist, dass sie mit der erwarteten .11-IP-Host-Adresse für jede Schnittstelle übereinstimmt, kann das Gerät ARP für die Cloud-Umgebung Gateways und IP-Konnektivität zum virtuellen Pfad des MCN nicht ordnungsgemäß einrichten.

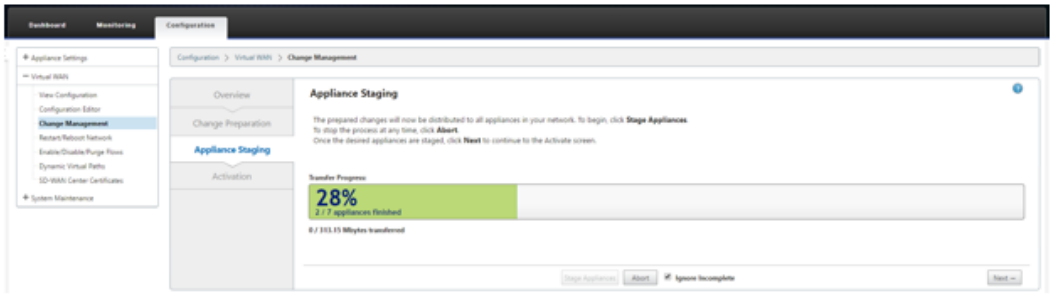


h) Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen** der Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-Dienst unterstützen würde.



i) Speichern Sie die neue Konfiguration im SD-WAN Center, und verwenden Sie den Export in die Option **Change Management Posteingang**, um die Konfiguration mithilfe der Änderungsverwaltung zu verschieben.

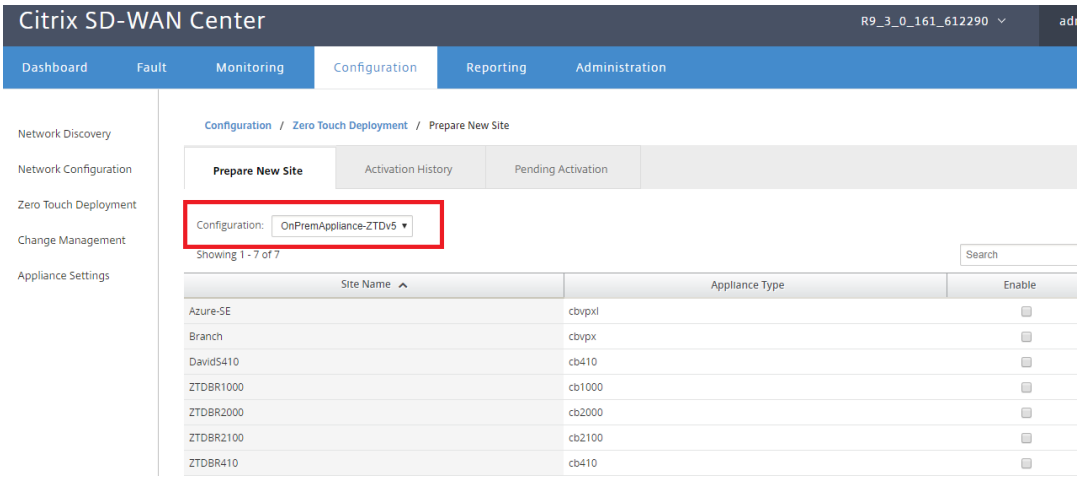
j) Befolgen Sie das Änderungsverwaltungsverfahren, um die neue Konfiguration ordnungsgemäß zu implementieren, wodurch die vorhandenen SD-WAN-Geräte über die neue Site informiert werden, die per Zero Touch bereitgestellt werden soll. Sie müssen die Option *Unvollständig ignorieren* verwenden, um den Versuch zu überspringen, die Konfiguration auf die neue Site zu übertragen, die muss noch den ZTD-Workflow durchlaufen.



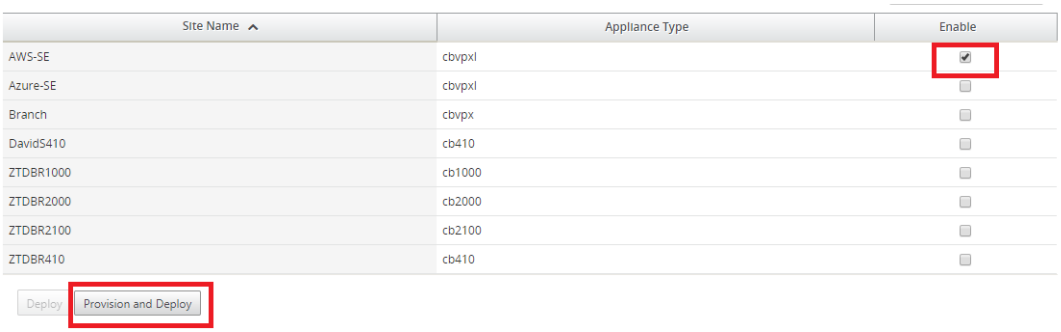
2. Navigieren Sie zurück zur Seite Zero Touch Deployment von SD-WAN Center. Wenn die neue aktive Konfiguration ausgeführt wird, steht die neue Site für die Bereitstellung zur Verfügung.

a) Wählen Sie auf der Seite Zero Touch-Bereitstellung unter der Registerkarte **Neue Site bereitstellen** die ausgeführte Netzwerkkonfigurationsdatei aus.

b) Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit nicht bereitgestellten Citrix SD-WAN-Geräten angezeigt, die für Zero Touch unterstützt werden.

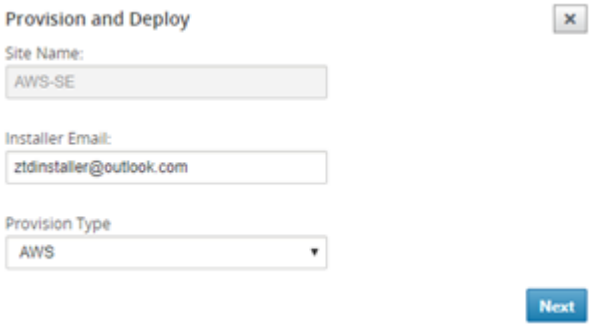


c) Wählen Sie die Ziel-Cloud-Site aus, die Sie mit dem Zero Touch-Dienst bereitstellen möchten, klicken Sie auf**Aktivieren**und dann auf **Bereitstellen und bereitstellen**.

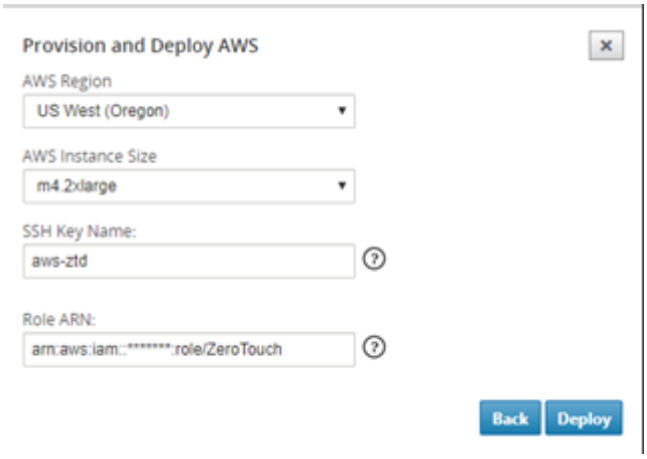


d) Es erscheint ein Popup-Fenster, in dem der Citrix SD-WAN Admin die Bereitstellung für Zero Touch initiieren kann.

Geben Sie eine E-Mail-Adresse ein, an die die Aktivierungs-URL übermittelt werden kann, und wählen Sie den **Bereitstellungstyp** für die gewünschte Cloud aus.



e) Nachdem Sie auf **Weiter** geklickt haben und die entsprechende Region und Instanzgröße gewählt, füllen Sie die Felder SSH-Schlüsselname und Rollen-ARN entsprechend aus.

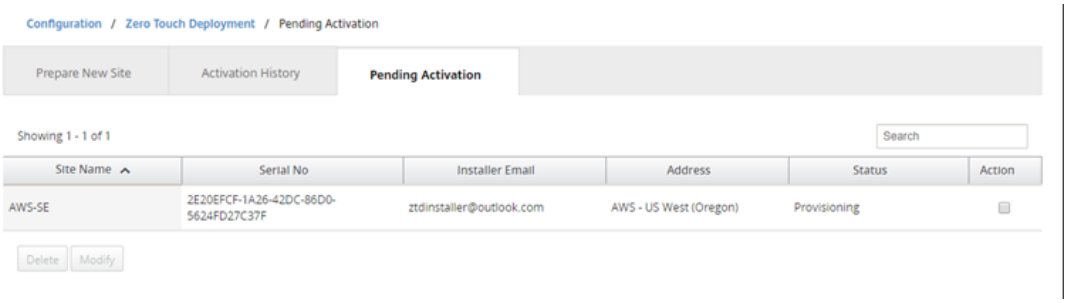


> **Hinweis**
>
> Nutzen Sie die Hilfe-Links, um Anleitungen zum Einrichten des SSH-Schlüssels und der Rollen-ARN für das Cloud-Konto zu erhalten. Stellen Sie außerdem sicher, dass die ausgewählte Region mit dem übereinstimmt, was auf dem Konto verfügbar ist

> und dass die ausgewählte Instanzgröße VPX oder VPXL als ausgewähltes Modell in der SD-WAN-Konfiguration übereinstimmt.

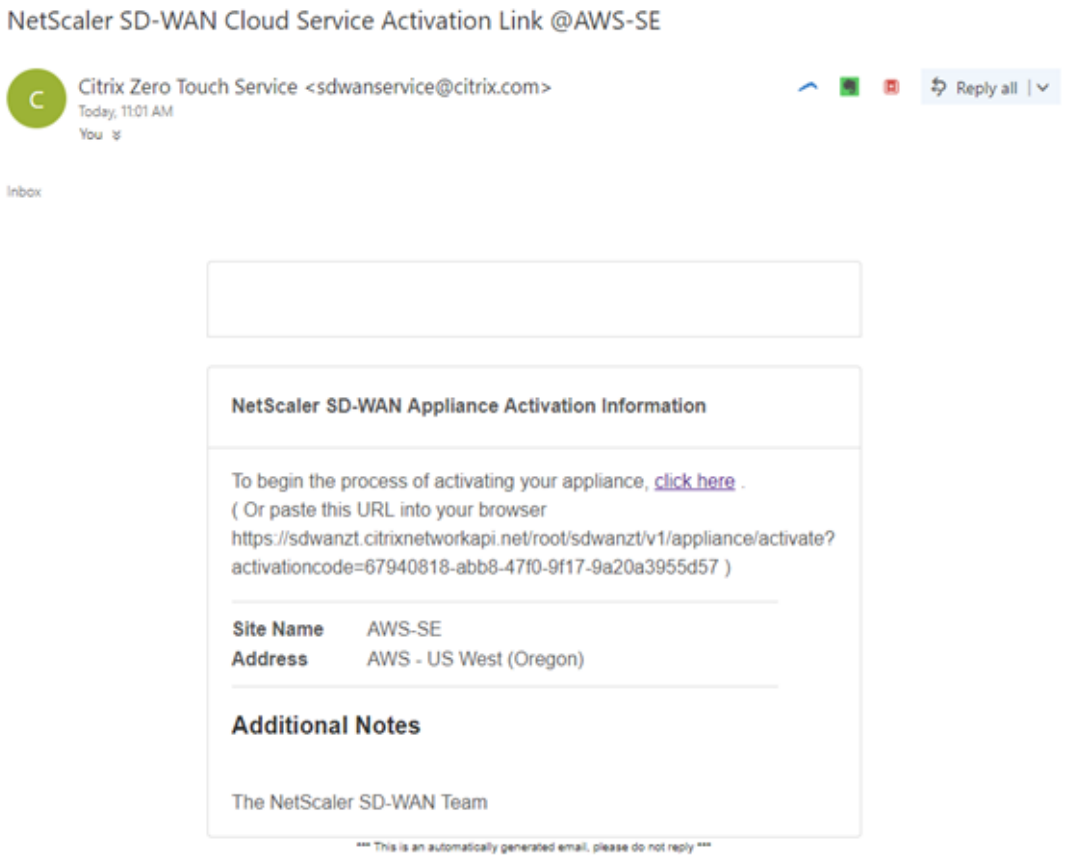
f) Klicken Sie auf **Deploy**und lösen Sie das SD-WAN Center aus, das zuvor beim ZTD Cloud Service registriert wurde, um die Konfiguration dieser Site so freizugeben, dass sie temporär im ZTD Cloud Service gespeichert ist.

g) Navigieren Sie zur Registerkarte **Ausstehende Aktivierung**, um zu bestätigen, dass die Standortinformationen erfolgreich ausgefüllt wurden und in einen Bereitstellungsstatus versetzt wurden.



3. Starten Sie den Zero Touch-Bereitstellungsprozess als Cloud-Administrator.

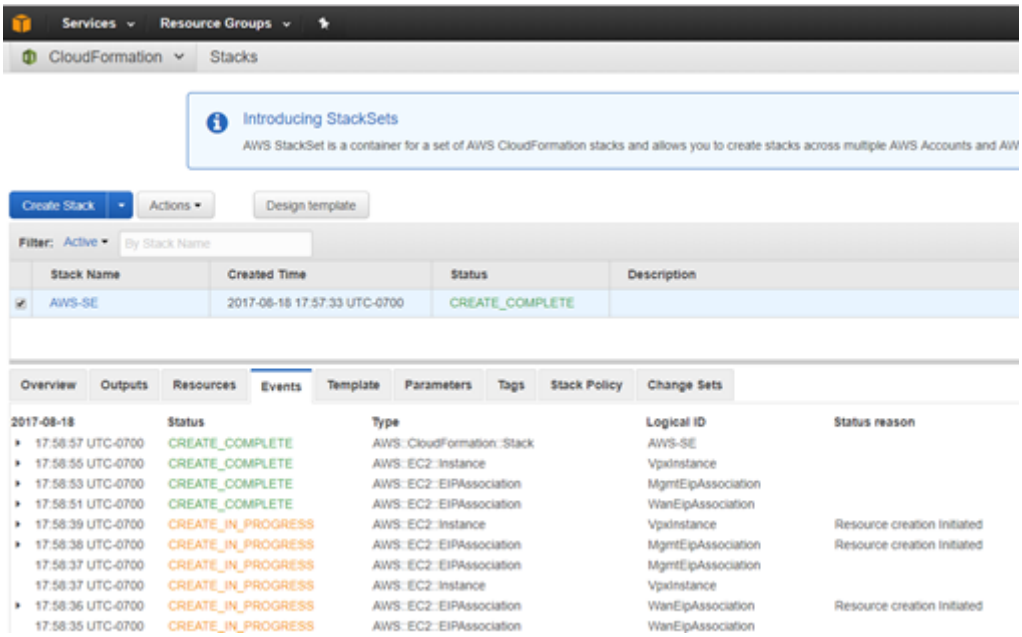
a) Der Installer muss das Postfach der E-Mail-Adresse überprüfen, die der SD-WAN-Administrator bei der Bereitstellung der Site verwendet hat.



b) Öffnen Sie die Aktivierungs-URL in der E-Mail in einem Internet-Browser-Fenster.

c) Wenn der SSH-Schlüssel und die Rollen-ARN ordnungsgemäß eingegeben werden, beginnt der Zero Touch-Bereitstellungsdienst sofort mit der Bereitstellung der SD-WAN-Instanz. Andernfalls werden Verbindungsfehler sofort angezeigt.

d) Zur weiteren Fehlerbehebung in der AWS-Konsole kann der Cloud Formation-Dienst zum Abfangen von Ereignissen verwendet werden, die während des Bereitstellungsvorgangs auftreten.

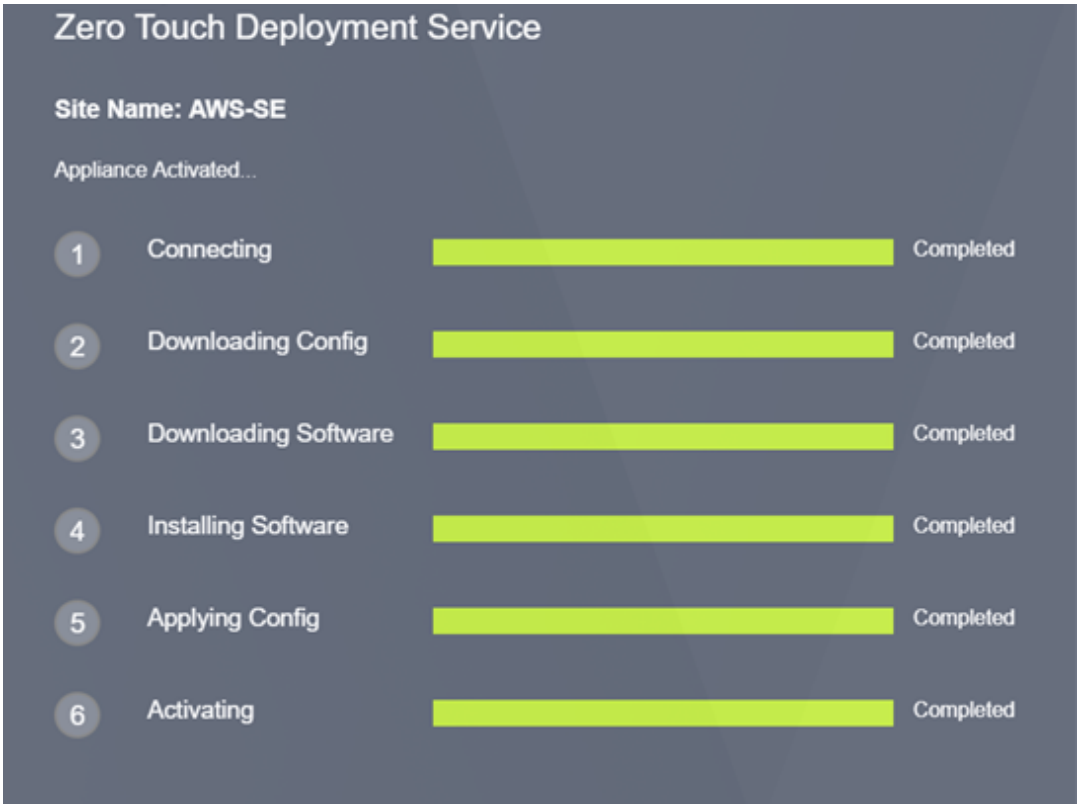


e) Erlauben Sie den Bereitstellungsprozess ca. 8-10 Minuten und die Aktivierung weiterer ~ 3-5 Minuten, um vollständig abzuschließen.

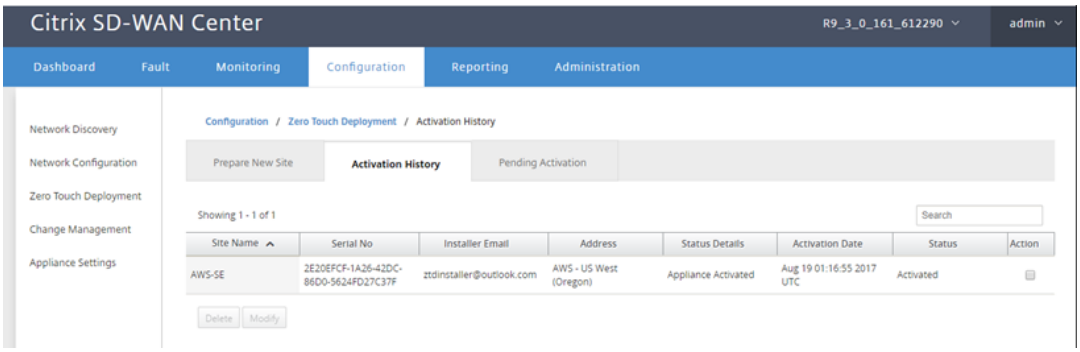
f) Bei erfolgreicher Konnektivität der SD-WAN-Cloud-Instanz mit dem ZTD Cloud Service

führt der Dienst automatisch Folgendes aus:

- Laden Sie die standortspezifische Konfigurationsdatei herunter, die zuvor vom SD-WAN-Center gespeichert wurde.
- Anwenden der Konfiguration auf die lokale Instanz
- Laden Sie eine temporäre Lizenzdatei mit 10 MB herunter und installieren Sie sie
- Herunterladen und Installieren von Softwareupdates bei Bedarf
- Aktivieren Sie den SD-WAN-Dienst

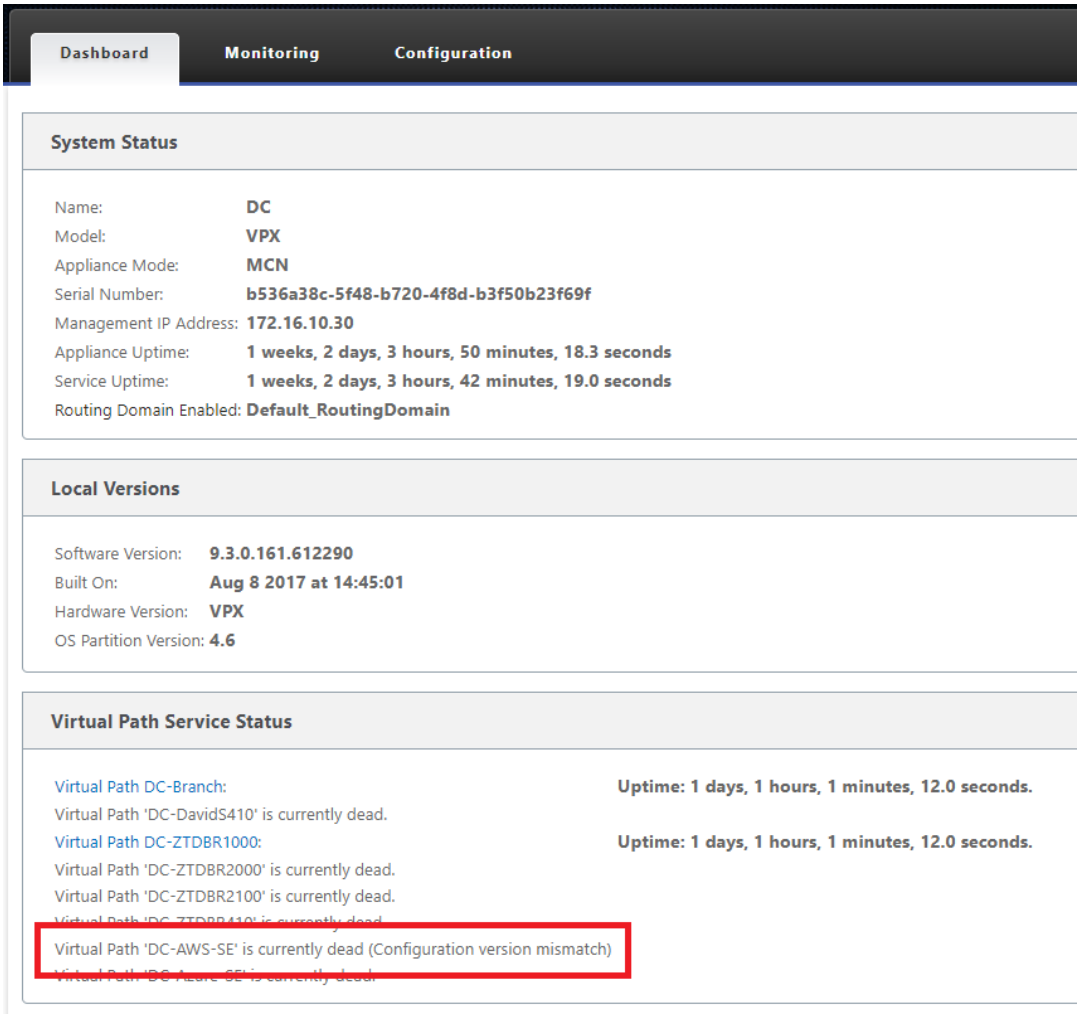


g) Eine weitere Bestätigung kann über die Webverwaltungsschnittstelle des SD-WAN Center erfolgen. Im Zero Touch Deployment Menü werden erfolgreich aktivierte Appliances auf der Registerkarte **Aktivierungsverlauf** angezeigt.

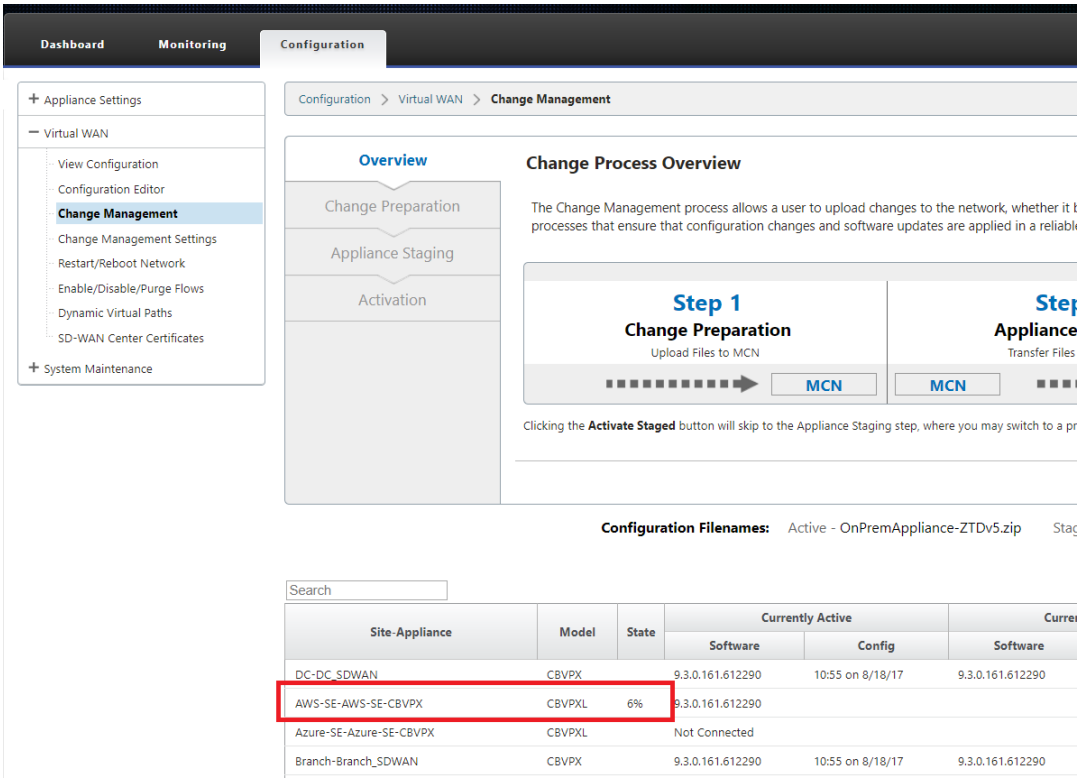


h) Die virtuellen Pfade werden möglicherweise nicht sofort in einem verbundenen Zustand

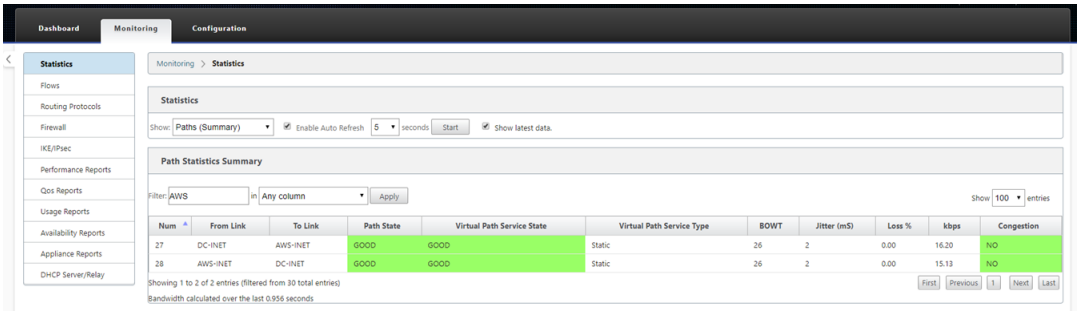
angezeigt. Dies liegt daran, dass das MCN der Konfiguration nicht vertraut, die vom ZTD Cloud Service übergeben wird, und meldet *Konfigurationsversion mismatch* im MCN Dashboard.



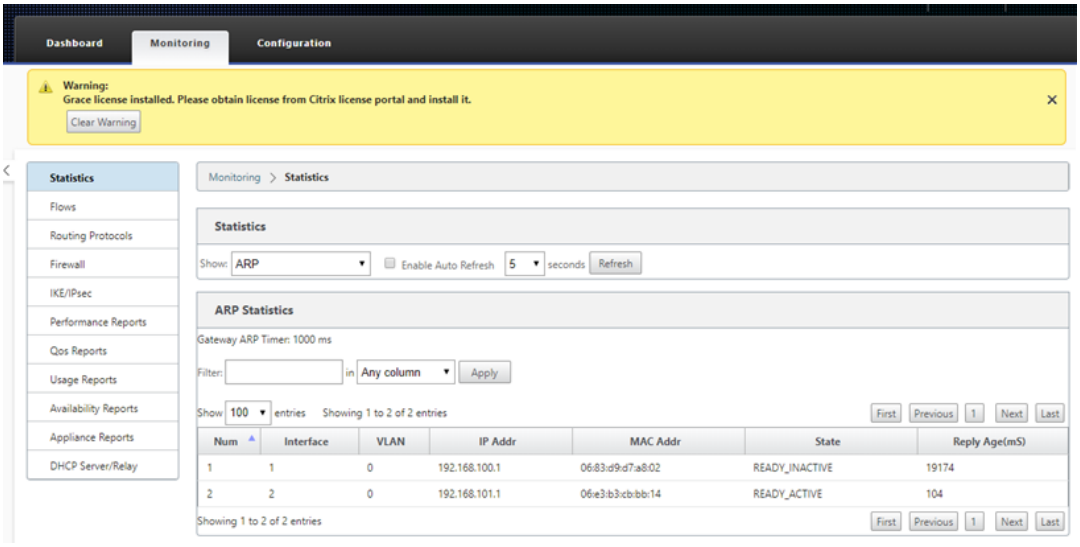
i) Die Konfiguration wird automatisch an die neu installierte Zweigstellen-Appliance übertragen. Der Status dieser Konfiguration kann auf der Seite **MCN** > **Konfiguration** > **Virtual WAN** > **Change Management** überwacht werden (abhängig von der Konnektivität dieser Prozess kann einige Minuten dauern).



j) Der SD-WAN-Administrator kann die Head-End-MCN-Webverwaltungsseite für die etablierten virtuellen Pfade der neu hinzugefügten Cloud-Site überwachen.



k) Wenn eine Fehlerbehebung erforderlich ist, öffnen Sie die Benutzeroberfläche von SD-WAN-Instanzs mit der öffentlichen IP-Adresse, die von der Cloud-Umgebung während der Bereitstellung zugewiesen wurde, und verwenden Sie die ARP-Tabelle auf der Seite **Überwachung** > **Statistiken**, um Probleme zu identifizieren, die mit den erwarteten Gateways verbunden sind, oder verwenden Sie die Optionen zur Verfolgung von Routen und Paketerfassung in der Diagnose.



Azure

April 13, 2021

Mit SD-WAN Version 9.3 wurden die Null-Touch-Bereitstellungsfunktionen auf Cloud-Instanzs erweitert. Das Verfahren zum Bereitstellen von Zero Touch-Bereitstellungsprozess für Cloud-Instanzs unterscheidet sich geringfügig von der Appliance-Bereitstellung für Zero Touch-Dienst.

Aktualisieren der Konfiguration zum Hinzufügen eines neuen Remote-Standorts mit einem ZTD-fähigen SD-WAN-Cloud-Gerät mithilfe der SD-WAN-Center-Netzwerkkonfiguration

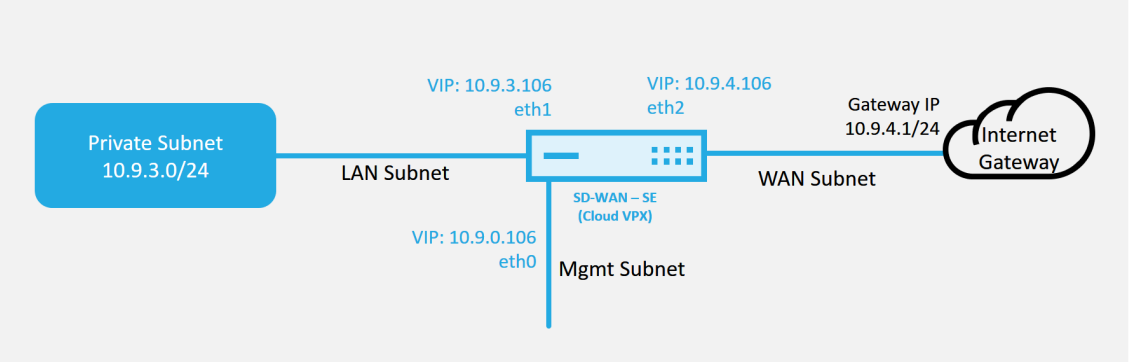
Wenn die SD-WAN-Konfiguration nicht mit der SD-WAN-Center-Netzwerkkonfiguration erstellt wurde, importieren Sie die aktive Konfiguration aus dem MCN und beginnen Sie mit der Änderung der Konfiguration mit dem SD-WAN Center. Für die Zero Touch-Bereitstellung muss der SD-WAN-Administrator die Konfiguration mithilfe des SD-WAN-Centers erstellen. Das folgende Verfahren sollte verwendet werden, um einen neuen Cloud-Knoten hinzuzufügen, der für die Null-Touch-Bereitstellung vorgesehen ist.

1. Entwerfen Sie die neue Site für die SD-WAN-Cloud-Bereitstellung, indem Sie zunächst die Details der neuen Site skizzieren (z. B. die VPX-Größe, die Verwendung von Schnittstellengruppen, virtuelle IP-Adressen, WAN-Link (s) mit Bandbreite und deren jeweiligen Gateways).

Hinweis

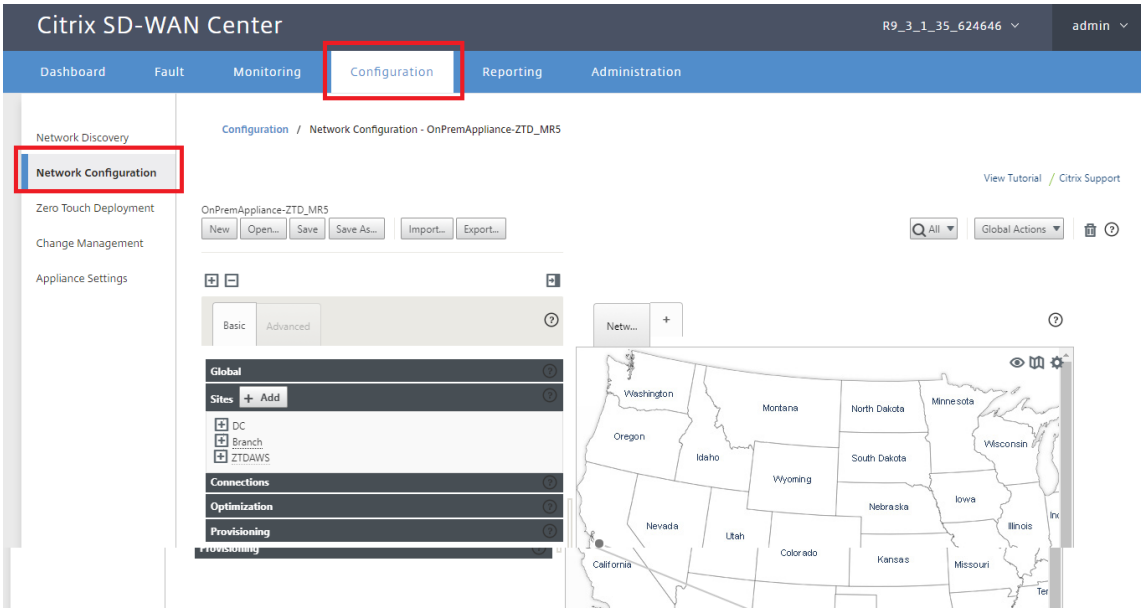
- In der Cloud bereitgestellte SD-WAN-Instanzen müssen im Edge/Gateway -Modus bereitgestellt werden.
- Die Vorlage für die Cloud-Instanz ist auf drei Schnittstellen beschränkt: Management, LAN und WAN (in dieser Reihenfolge).
- Die verfügbaren Azure-Cloudvorlagen für SD-WAN VPX sind derzeit hart festgelegt, um die 10.9.4.106 IP für das WAN, 10.9.3.106 IP für das LAN und 10.9.0.16 IP für die Verwaltungsadresse zu erhalten.Die SD-WAN-Konfiguration für den Azure-Knoten für Zero Touch muss mit diesem Layout übereinstimmen.
- Der Azure-Site-Name in der Konfiguration muss alle Kleinbuchstaben ohne Sonderzeichen enthalten (z. B. ztdazure).

Azure Cloud Topology with NetScaler SD-WAN

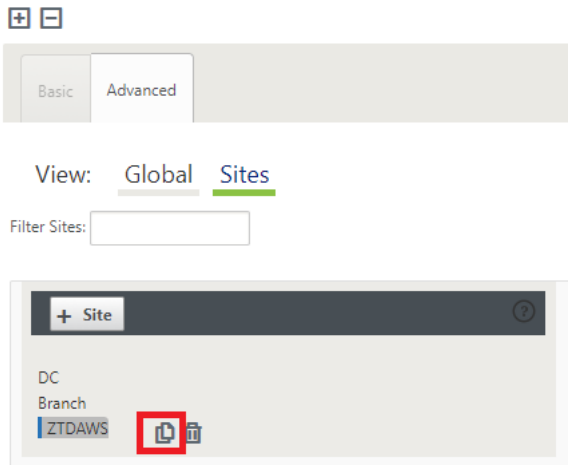


Dies ist ein Beispiel für die Bereitstellung einer SD-WAN-Cloud bereitgestellten Site. Das Citrix SD-WAN-Gerät wird als Edge-Gerät bereitgestellt, das eine einzelne Internet-WAN-Verbindung in diesem Cloud-Netzwerk bedient.Remote-Standorte können mehrere unterschiedliche Internet-WAN-Verbindungen nutzen, die mit demselben Internet-Gateway für die Cloud verbunden sind, wodurch Ausfallsicherheit und aggregierte Bandbreitenkonnektivität von jedem SD-WAN-Bereitstellungsstandort zur Cloud-Infrastruktur bereitgestellt werden.Dies ermöglicht eine kostengünstige und äußerst zuverlässige Konnektivität zur Cloud.

2. Öffnen Sie die Web-Management-Schnittstelle des SD-WAN Center, und navigieren Sie zur Seite **Konfiguration** > **Netzwerkkonfiguration**.



3. Stellen Sie sicher, dass bereits eine funktionierende Konfiguration vorhanden ist, oder importieren Sie die Konfiguration aus dem MCN.
4. Navigieren Sie zur Registerkarte Basic, um eine neue Site zu erstellen.
5. Öffnen Sie die Kachel Sites, um die aktuell konfigurierten Sites anzuzeigen.
6. Erstellen Sie schnell die Konfiguration für die neue Cloud-Site, indem Sie die Clone-Funktion einer vorhandenen Site verwenden oder manuell eine neue Site erstellen.

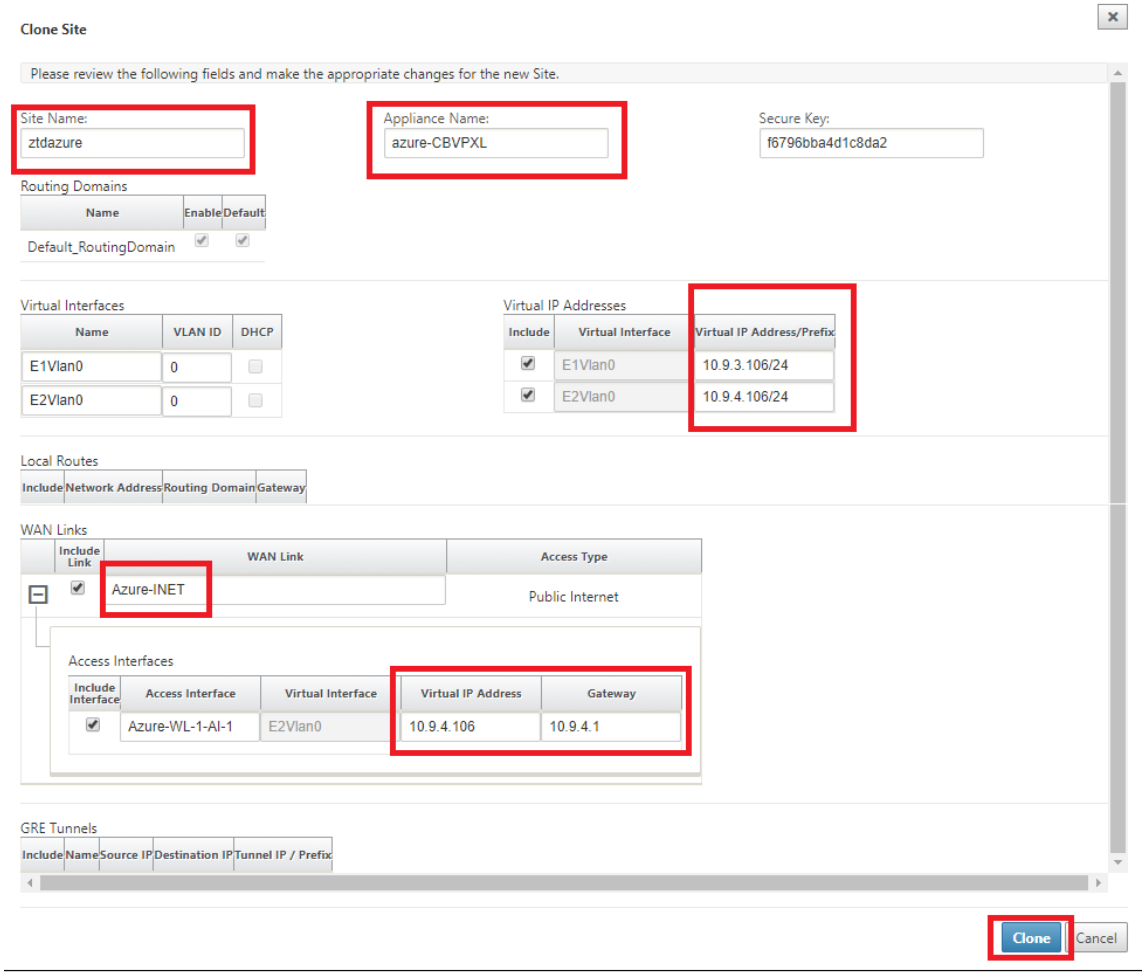


7. Füllen Sie alle erforderlichen Felder aus der zuvor für diese neue Cloud-Site entwickelten Topologie aus.

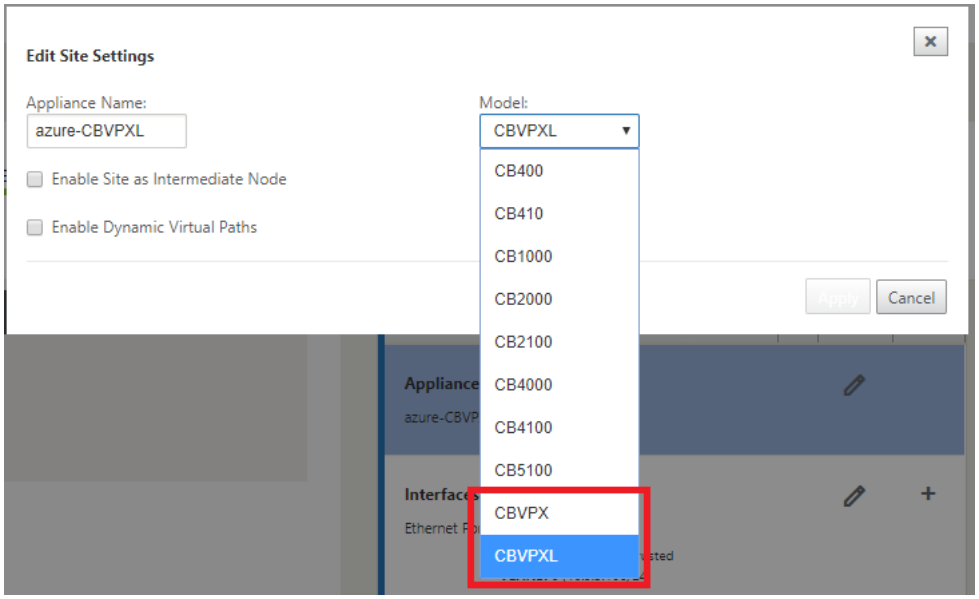
   Beachten Sie, dass die für Azure Cloud ZTD-Bereitstellungen verfügbare Vorlage derzeit fest festgelegt ist, um die 10.9.4.106 IP für das WAN, 10.9.3.106 IP für das LAN und 10.9.0.16 IP für die Verwaltungsadresse zu erhalten. Wenn die Konfiguration nicht so eingestellt ist, dass sie mit der erwarteten VIP-Adresse für jede Schnittstelle übereinstimmt, kann das Gerät ARP für die Cloud-

Umgebung Gateways und IP-Konnektivität zum virtuellen Pfad des MCN nicht ordnungsgemäß einrichten.

Es wird importiert, dass der Sitename mit dem übereinstimmt, was Azure erwartet.Der Site-Name muss in Kleinbuchstaben, mindestens 6 Zeichen, ohne Sonderzeichen, er muss dem folgenden regulären Ausdruck bestätigen **^[a-z] [a-z0-9-]{1,61}[a-z0-9]$.**

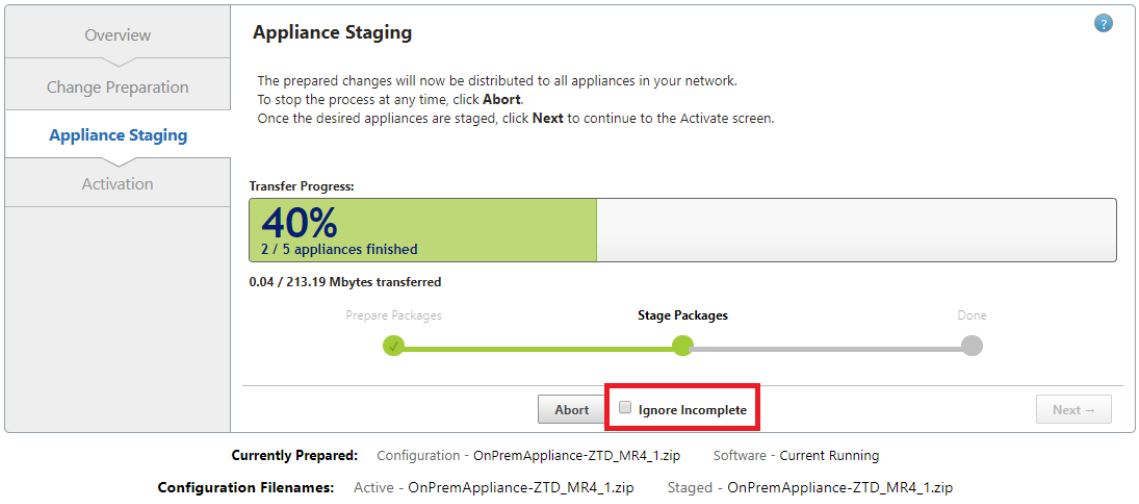


8. Navigieren Sie nach dem Klonen einer neuen Site zu den **Grundeinstellungen** der Site, und überprüfen Sie, ob das SD-WAN-Modell korrekt ausgewählt ist, was den Null-Touch-Dienst unterstützen würde.



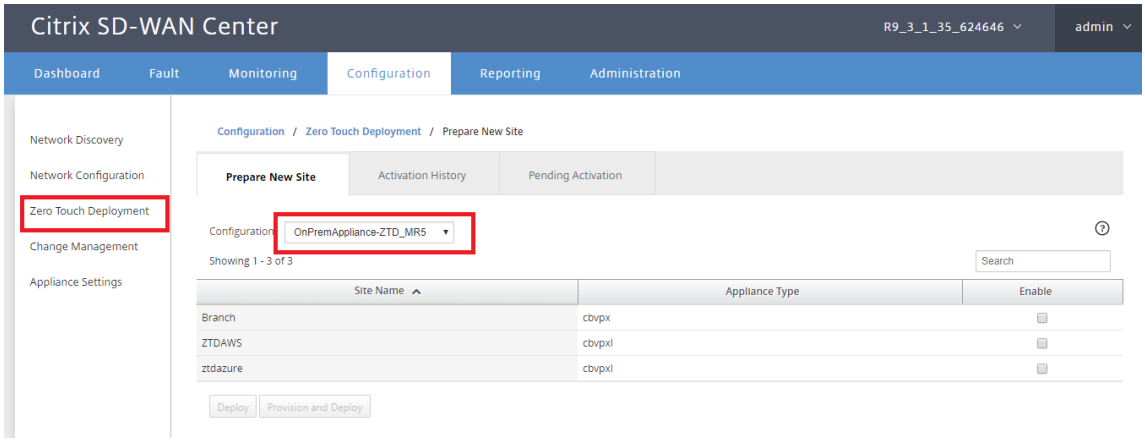
9. Speichern Sie die neue Konfiguration im SD-WAN Center, und verwenden Sie den Export in die Option **Change Management Posteingang**, um die Konfiguration mithilfe der Änderungsverwaltung zu verschieben.

10. Befolgen Sie das Änderungsverwaltungsverfahren, um die neue Konfiguration ordnungsgemäß zu implementieren, wodurch die vorhandenen SD-WAN-Geräte über die neue Site informiert werden, die per Zero Touch bereitgestellt werden soll. Sie müssen die Option *Unvollständig ignorieren* verwenden, um den Versuch zu überspringen, die Konfiguration auf die neue Site zu übertragen, die muss noch den ZTD-Workflow durchlaufen.

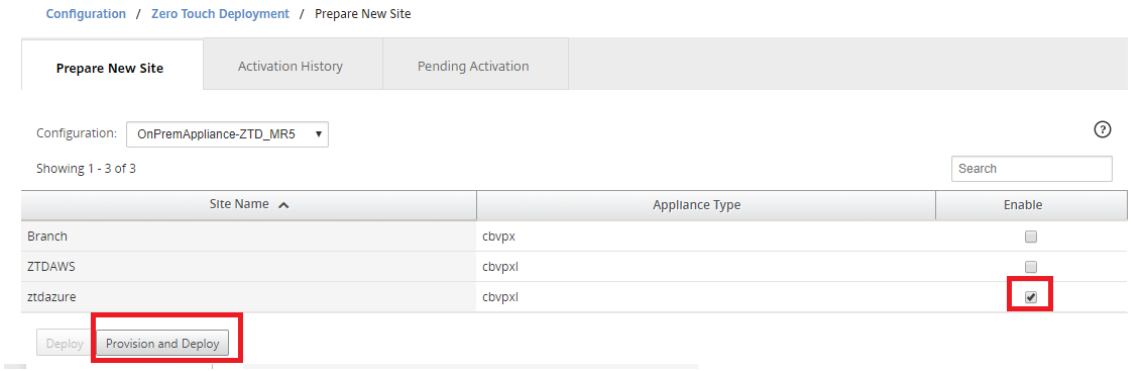


Navigieren Sie zur Zero Touch Deployment Seite des SD-WAN Centers, und wenn die neue aktive Konfiguration ausgeführt wird, wird die neue Site für die Bereitstellung und Bereitstellung von Azure SD-WAN Center verfügbar sein (Schritt 1 von 2)

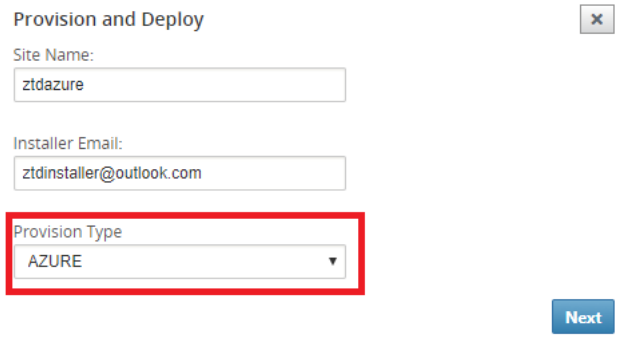
1. Melden Sie sich auf der Seite Zero Touch Deployment mit den Anmeldeinformationen Ihres Citrix Kontos an. Wählen **Sie auf der Registerkarte Neue Site bereitstellen** die ausgeführte Netzwerkkonfigurationsdatei aus.
2. Nachdem die ausgeführte Konfigurationsdatei ausgewählt wurde, wird die Liste aller Zweigstandorte mit ZTD-fähigen Citrix SD-WAN-Geräten angezeigt.



3. Wählen Sie die Ziel-Cloud-Site aus, die Sie mit dem Zero Touch-Dienst bereitstellen möchten, klicken Sie auf**Aktivieren**und dann auf **Bereitstellen und bereitstellen**.

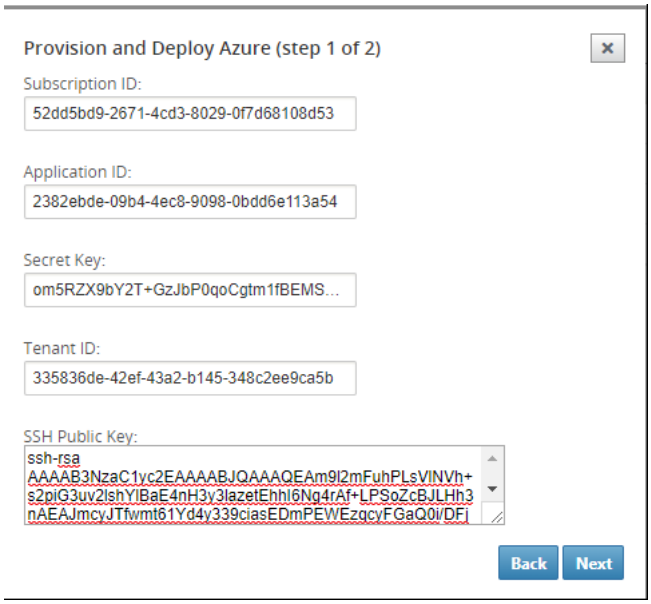


4. Es erscheint ein Popupfenster, in dem der Citrix SD-WAN Admin die Bereitstellung für Zero Touch initiieren kann. Überprüfen Sie, ob der Site-Name den Anforderungen in Azure entspricht (Kleinbuchstaben ohne Sonderzeichen). Geben Sie eine E-Mail-Adresse an, an die die Aktivierungs-URL übermittelt werden kann, und wählen Sie Azure als **Bereitstellungstyp** für die gewünschte Cloud aus, bevor Sie auf **Weiter** klicken.

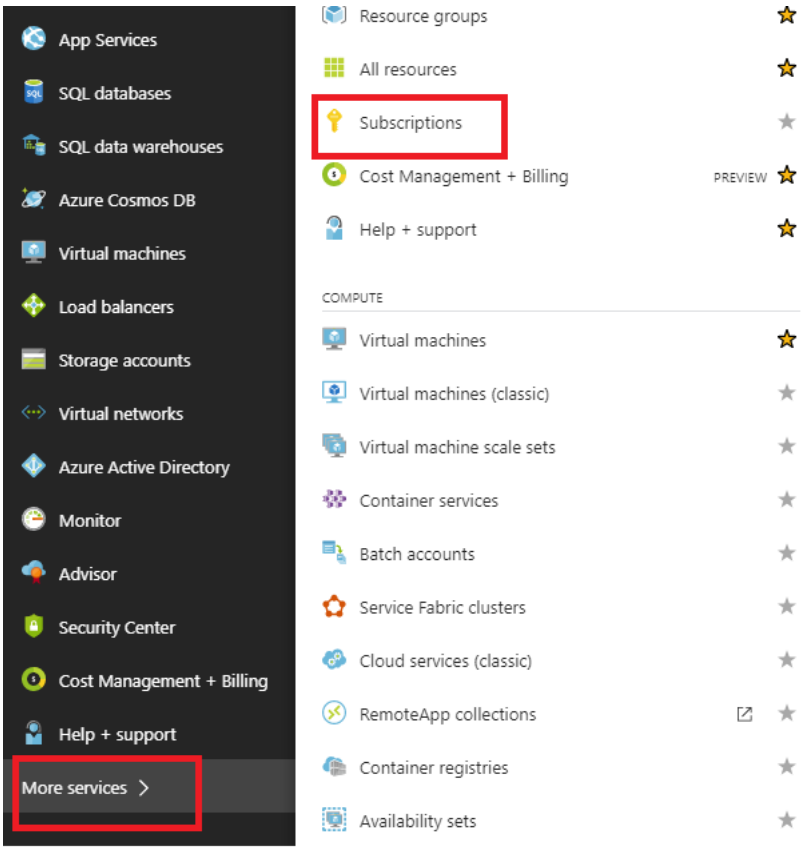


5. Nachdem Sie auf **Weiter** geklickt haben, erfordert das Fenster Bereitstellen und Bereitstellen von Azure (Schritt 1 von 2) eine Eingabe von, die vom Azure-Konto abgerufen wurde.

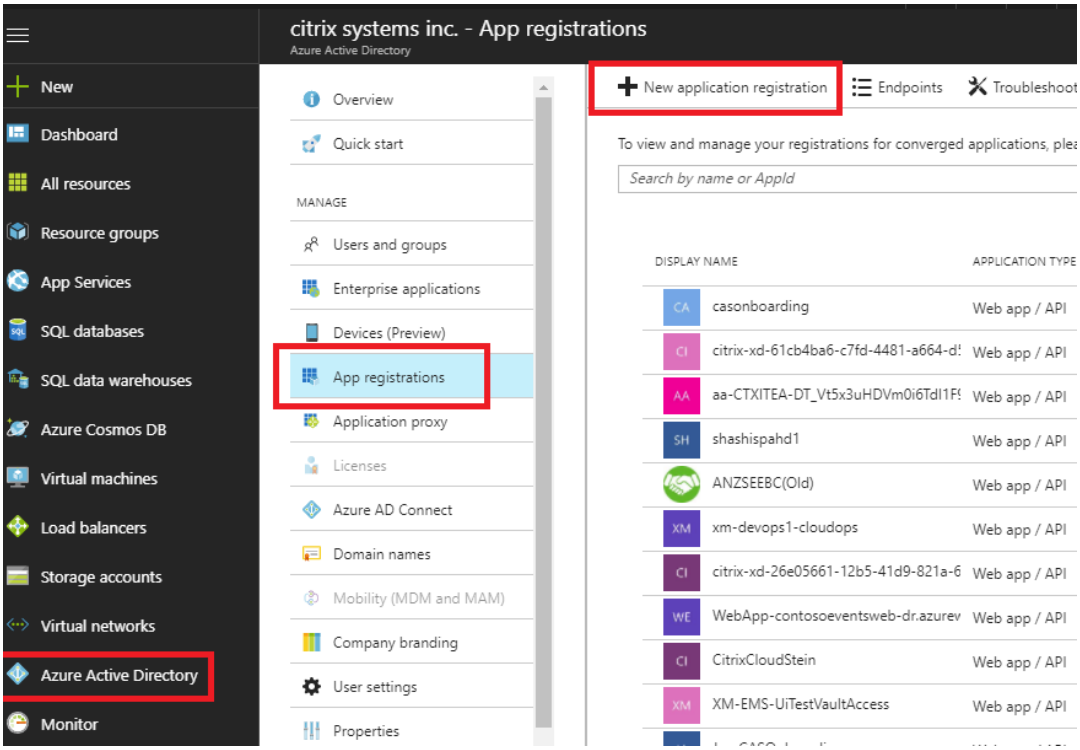
   Kopieren Sie alle erforderlichen Felder, nachdem Sie die Informationen von Ihrem Azure-Konto erhalten haben, und fügen Sie sie ein. In den folgenden Schritten wird beschrieben, wie Sie die erforderliche Abonnement-ID, die Anwendungs-ID, den geheimen Schlüssel und die Mandanten-ID von Ihrem Azure-Konto erhalten, und klicken Sie dann auf **Weiter**.



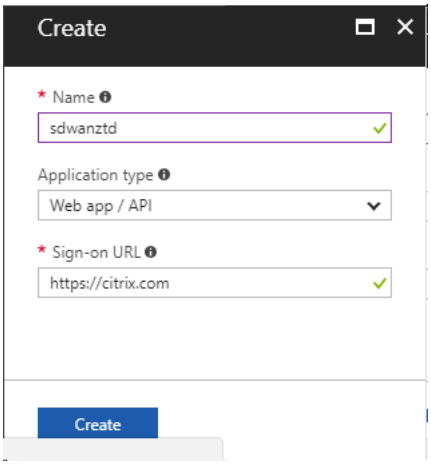
   a) Auf dem Azure-Konto können wir die erforderliche ***Abonnement-ID*** identifizieren, indem Sie zu “Weitere Dienste”navigieren und **Abonnements auswählen.**



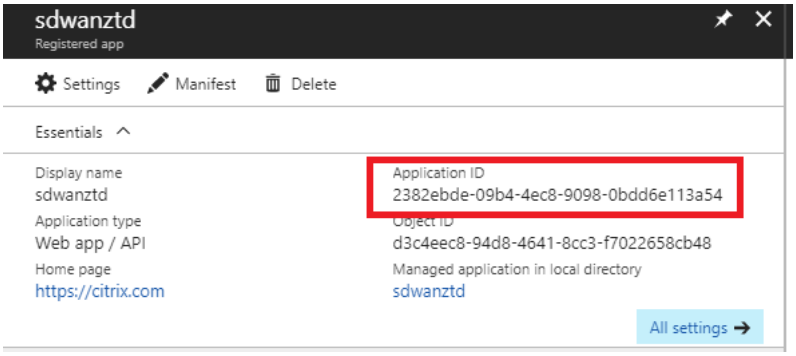
b) Um die erforderliche ***Anwendungs-ID*** zu identifizieren, navigieren Sie zu Azure Active Directory, Anwendungsregistrierungen, und klicken Sie auf **New application registration**.



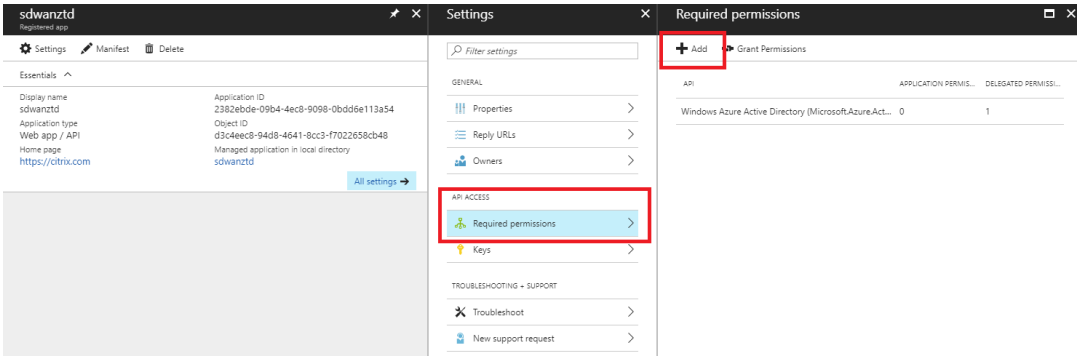
c) Geben Sie im Menü zum Erstellen der App-Registrierung einen Namen und eine Anmelde-URL ein (dies kann eine beliebige URL sein, die einzige Voraussetzung ist, dass sie gültig sein muss) und klicken Sie dann auf **Erstellen**.



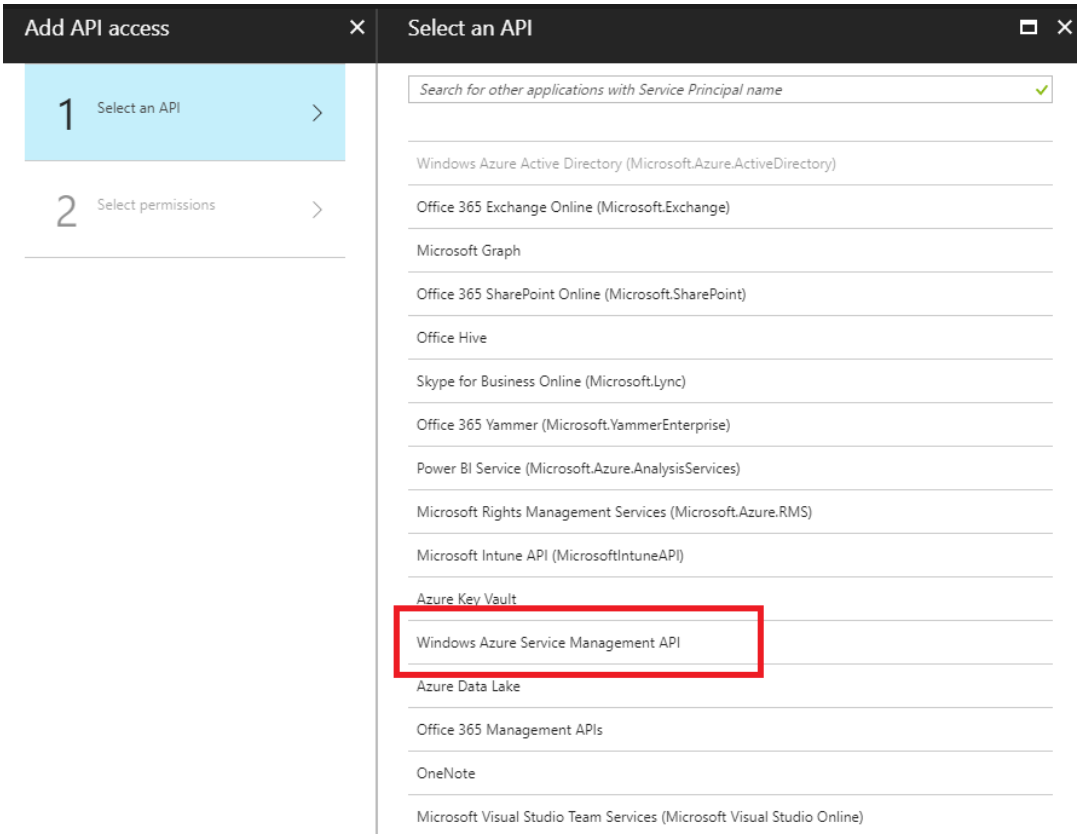
d) Suchen Sie nach der neu erstellten registrierten App und öffnen Sie sie, und notieren Sie sich die Anwendungs-ID.



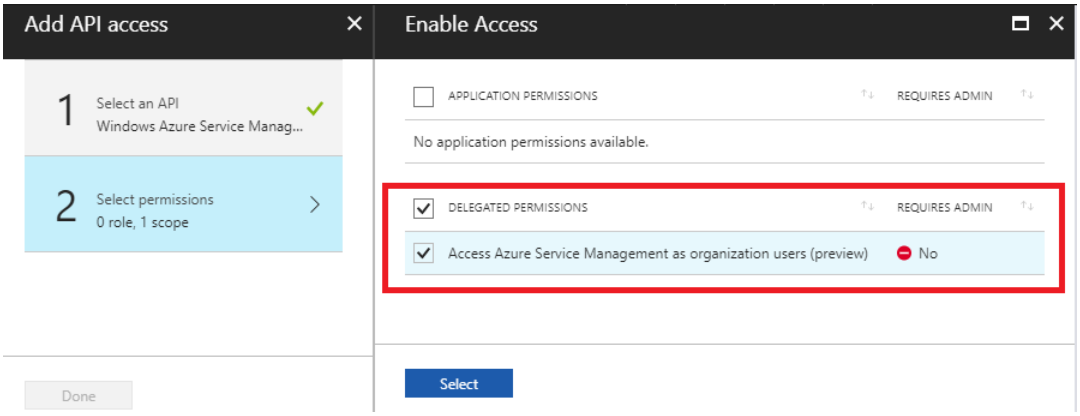
e) Öffnen Sie erneut die neu erstellte Registrierungs-App, und um den erforderlichen *Sicherheitsschlüssel* zu identifizieren, wählen Sie unter API-Zugriff **Erforderliche Berechtigungen** aus, um einem Drittanbieter die Bereitstellung und Instanzierung zu ermöglichen. Wählen Sie dann **Hinzufügen** aus.



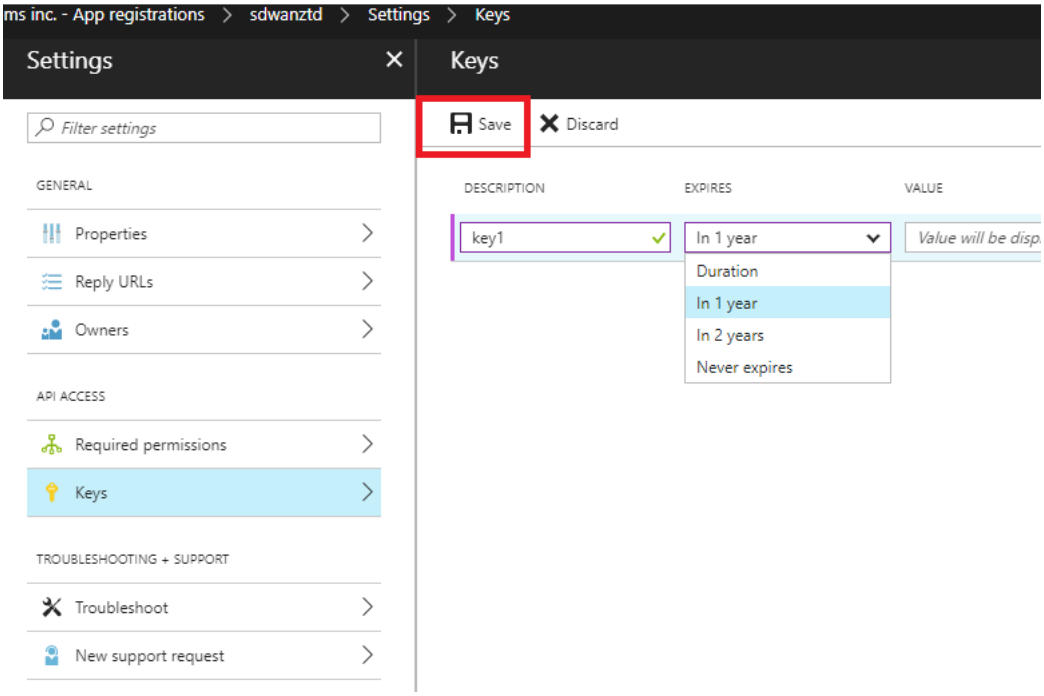
f) Wenn Sie die erforderlichen Berechtigungen hinzufügen, wählen Sie eine **API** aus, und markieren Sie dann die **Windows Azure-Dienstverwaltungs-API**.



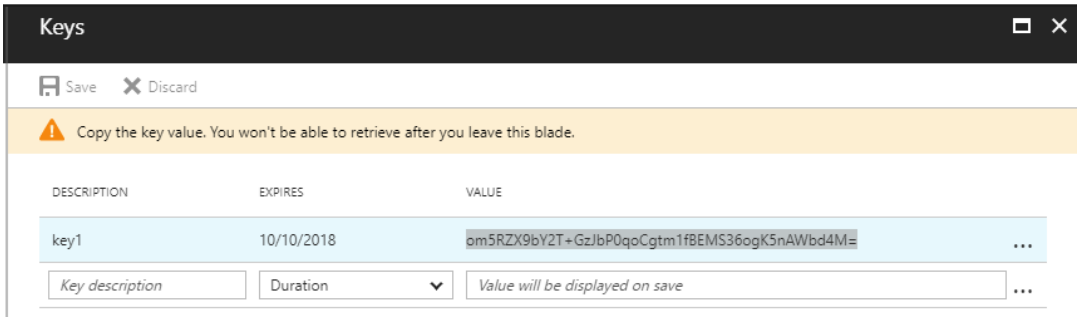
g) Aktivieren Sie **Stellvertreterberechtigungen**, um Instanzen bereitzustellen, und klicken Sie dann auf **Auswählen** und **Fertig**.



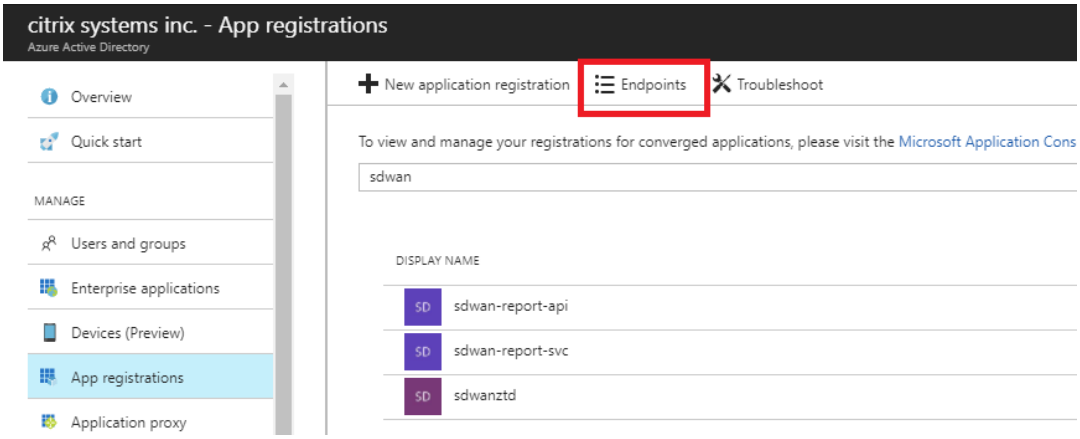
h) Wählen Sie für diese registrierte App unter API-Zugriff die Option **Schlüssel** aus, und erstellen Sie eine geheime **Schlüsselbeschreibung** und die gewünschte **Dauer** für die Gültigkeit des Schlüssels.Klicken Sie dann auf **Speichern**, um einen **geheimen Schlüssel** zu erzeugen (der Schlüssel ist nur für den Provisioning-Prozess erforderlich, er kann gelöscht werden, nachdem die Instanz verfügbar ist).



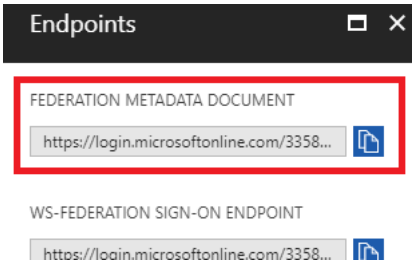
i) Kopieren und speichern Sie den geheimen Schlüssel (beachten Sie, dass Sie diesen später nicht abrufen können).



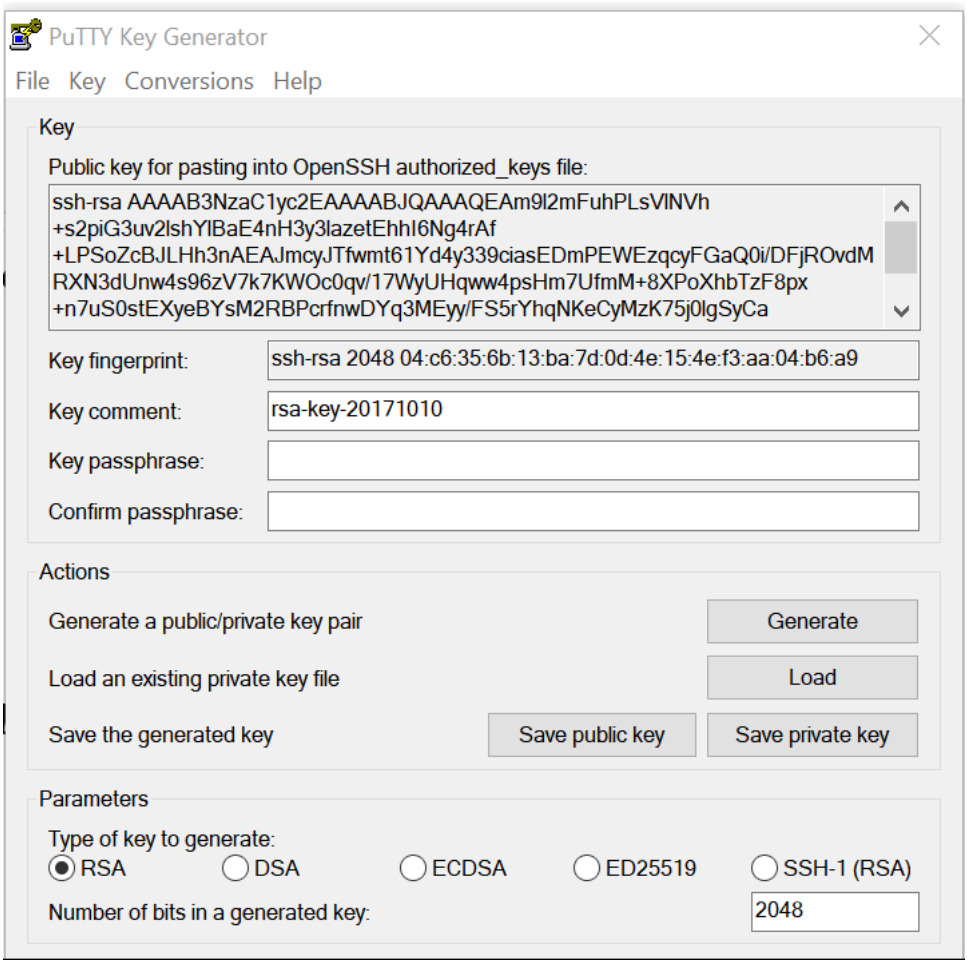
j) Um die erforderliche **Mandanten-ID** zu identifizieren, gehen Sie zurück zum App-Registrierungsbereich und wählen Sie **Endpunkte** aus.



k) Kopieren Sie das **Verbundmetadatendokument**, um Ihre Mandanten-ID zu identifizieren (beachten Sie, dass die Mandanten-ID 36 Zeichen ist, die sich zwischen online.com / und dem / federation in der URL befindet).

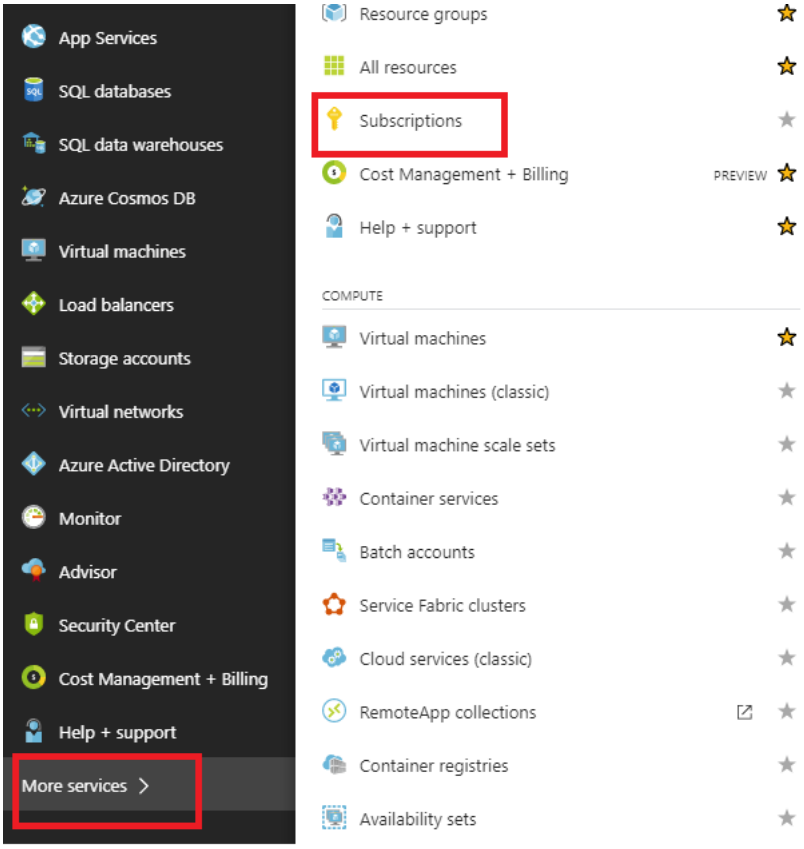


l) Das letzte benötigte Element ist der ***SSH Public Key***.Dies kann mit Putty Key Generator oder ssh-keygen erstellt werden und wird für die Authentifizierung verwendet, wodurch sich Passwörter nicht anmelden müssen.Der öffentliche SSH-Schlüssel kann kopiert werden (einschließlich der Überschrift ssh-rsa und nachfolgende rsa-Schlüsselzeichenfolgen).Dieser öffentliche Schlüssel wird über die SD-WAN Center-Eingabe für den Citrix Zero Touch Deployment Service freigegeben.

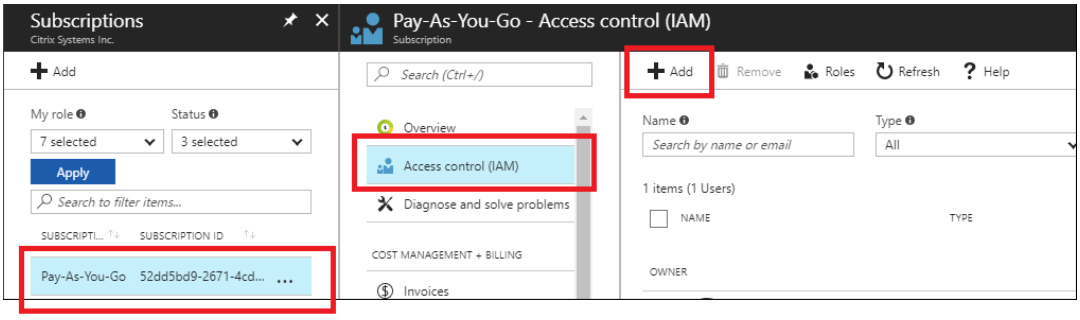


m) Zusätzliche Schritte sind erforderlich, um der Anwendung eine Rolle zuzuweisen.Navigieren

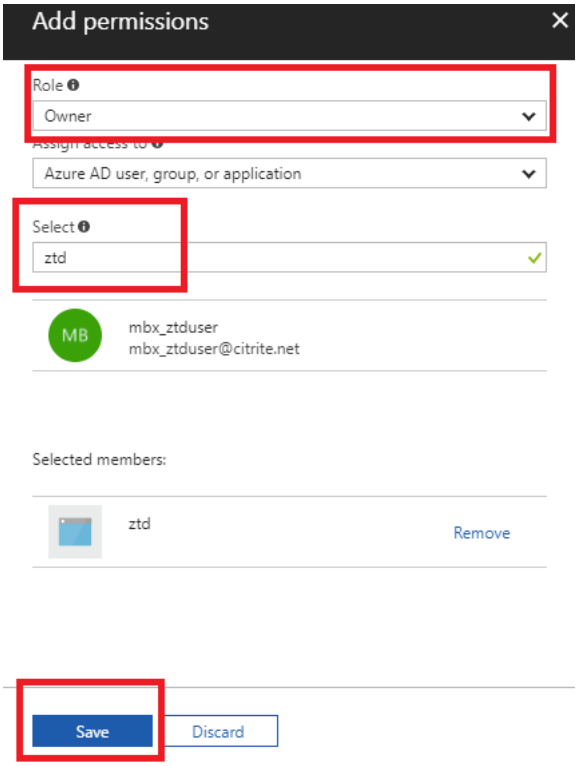
Sie zurück zu Weitere Dienste und dann Abonnements.



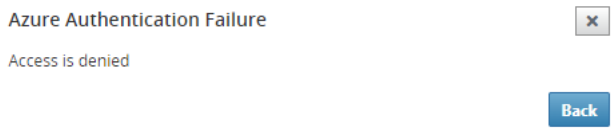
n) Wählen Sie das aktive Abonnement aus, dann **Zugriffskontrolle (AIM)**, und klicken Sie dann auf **Hinzufügen**.



o) Wählen Sie im Bereich Berechtigungen hinzufügen die Rolle "**Besitzer**"aus, weisen Sie den Zugriff auf **"Azure AD-Benutzer, Gruppe oder Anwendung"**zu und suchen Sie im **Feld Auswählen**nach der registrierten App, damit der Zero Touch Deployment Cloud Service die Instanz in Azure erstellen und konfigurieren kann Abonnement.Sobald die App identifiziert wurde, wählen Sie sie aus, und stellen Sie sicher, dass sie als ausgewähltes Element ausgefüllt wird, bevor **Sie auf Speichern**klicken.

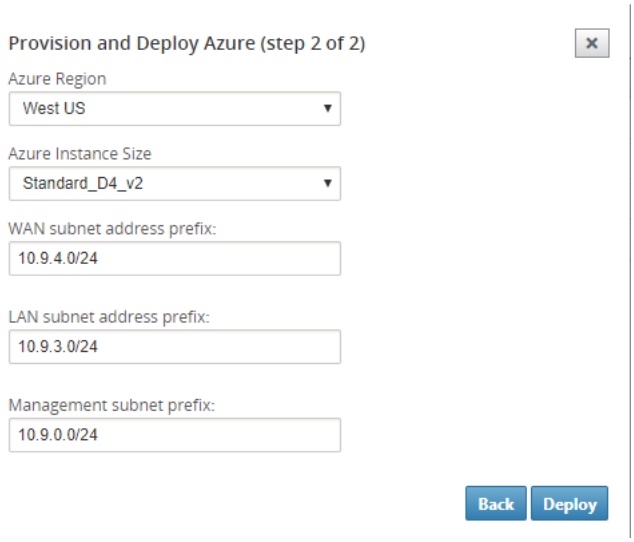


p) Nachdem Sie die erforderlichen Eingaben gesammelt und in das SD-WAN Center eingegeben haben, klicken Sie auf **Weiter**.Wenn die Eingaben nicht korrekt sind, tritt ein Authentifizierungsfehler auf.

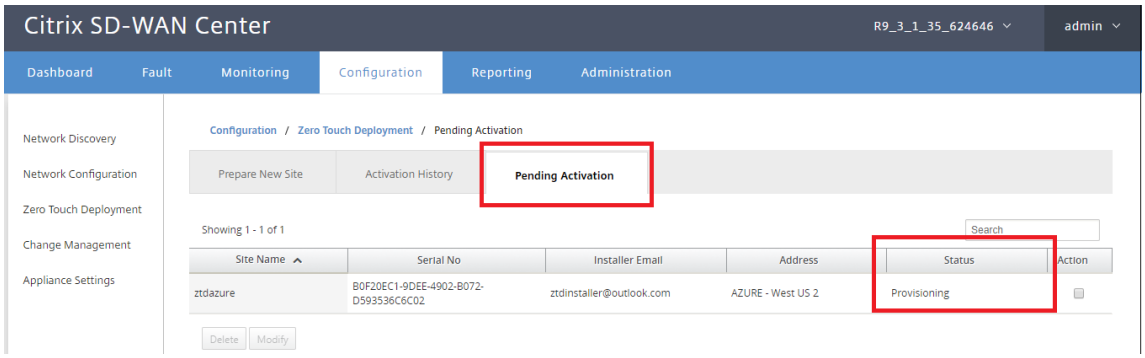


SD-WAN Center Bereitstellung und Bereitstellung von Azure (Schritt 2 von 2)

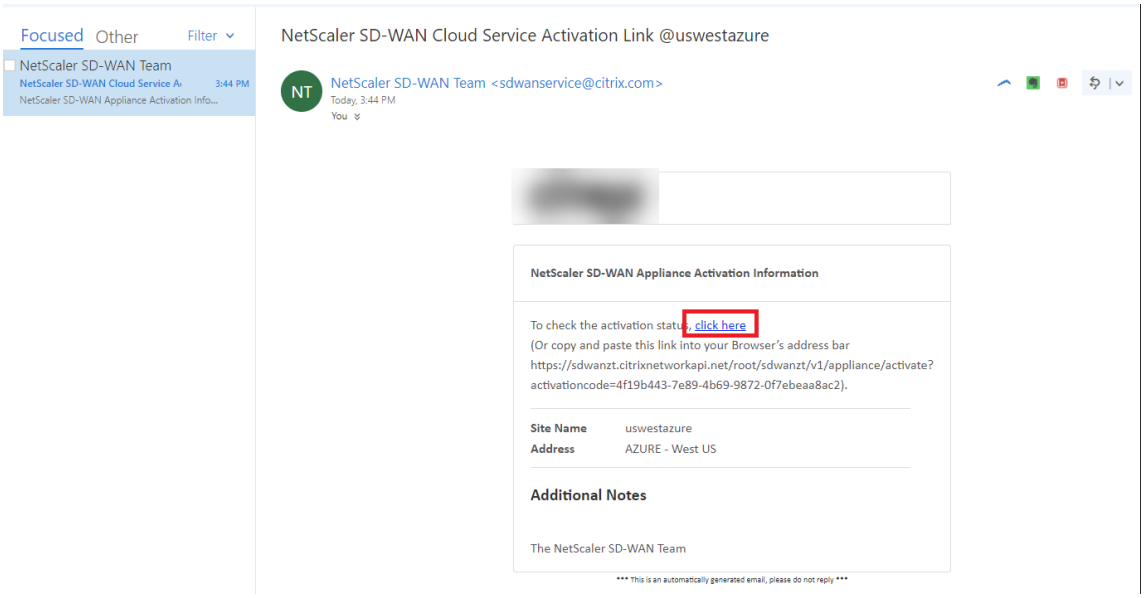
1. Sobald die Azure-Authentifizierung erfolgreich ist, füllen Sie die entsprechenden Felder aus, um die gewünschte Azure-Region und die entsprechende Instanzgröße auszuwählen, und klicken Sie dann auf **Bereitstellen**.



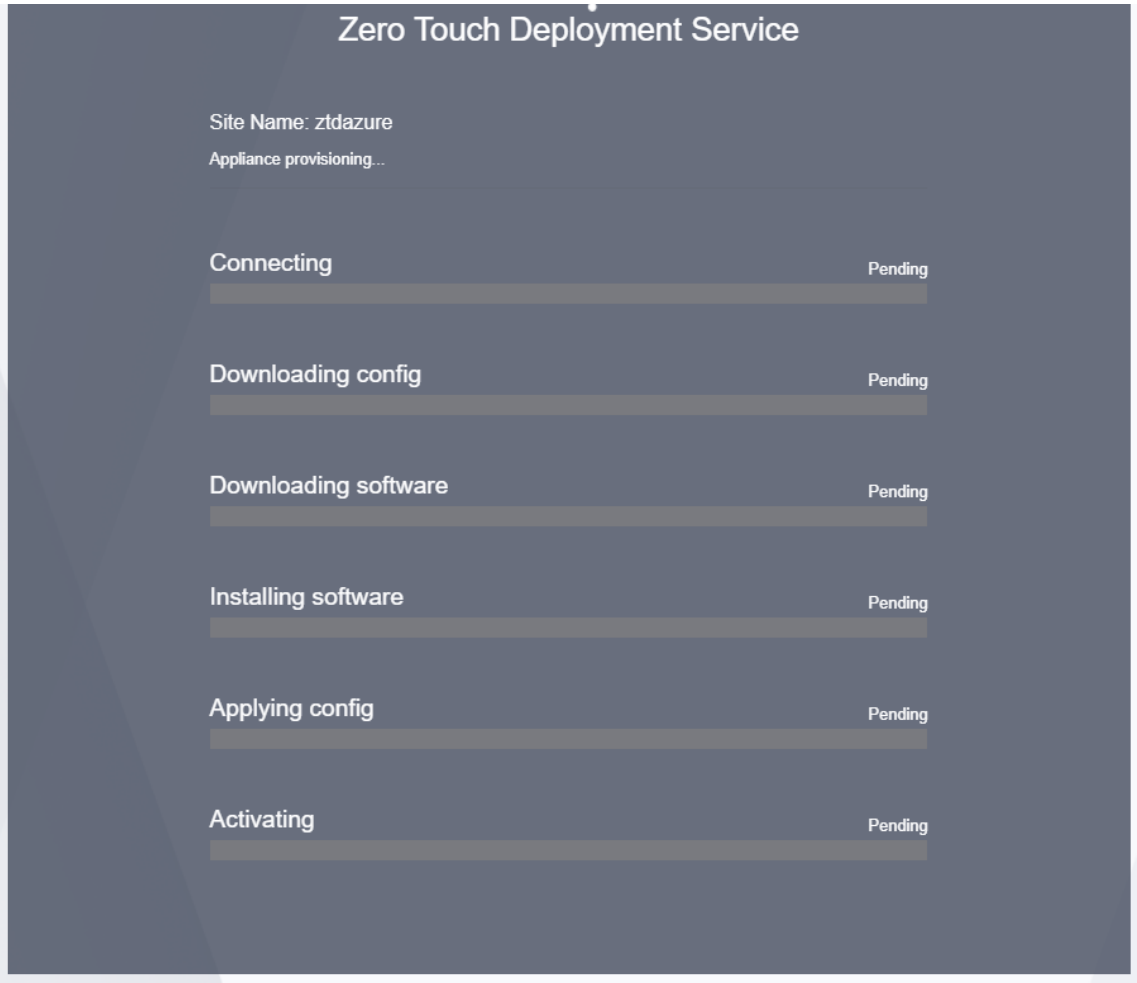
2. Navigieren Sie zur Registerkarte **Ausstehende Aktivierung** im SD-WAN Center, um den aktuellen Status der Bereitstellung zu verfolgen.



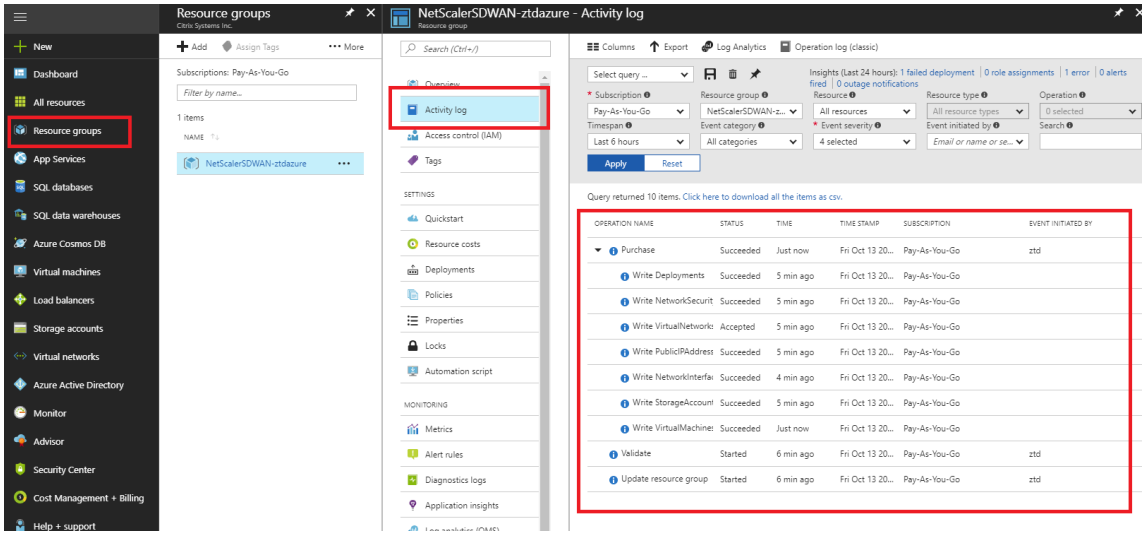
3. Eine E-Mail mit einem Aktivierungscode wird an die in Schritt 1 eingegebene E-Mail-Adresse gesendet, die E-Mail abgerufen und die **Aktivierungs-URL** geöffnet, um den Prozess auszulösen und den Aktivierungsstatus zu überprüfen.



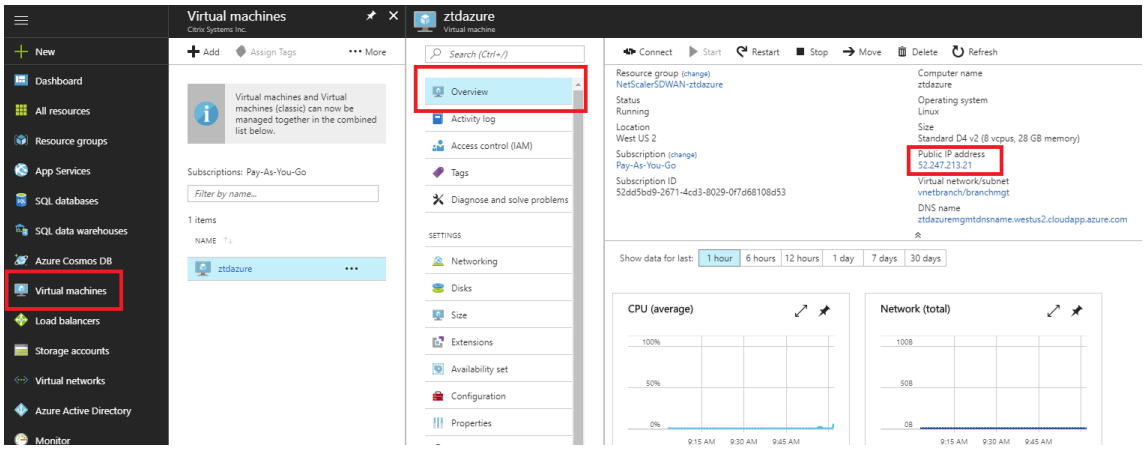
4. Eine E-Mail mit einer Aktivierungs-URL wird an die in Schritt 1 eingegebene E-Mail-Adresse gesendet.Holen Sie sich die E-Mail und öffnen Sie die **Aktivierungs-URL**, um den Prozess auszulösen und den Aktivierungsstatus zu überprüfen.



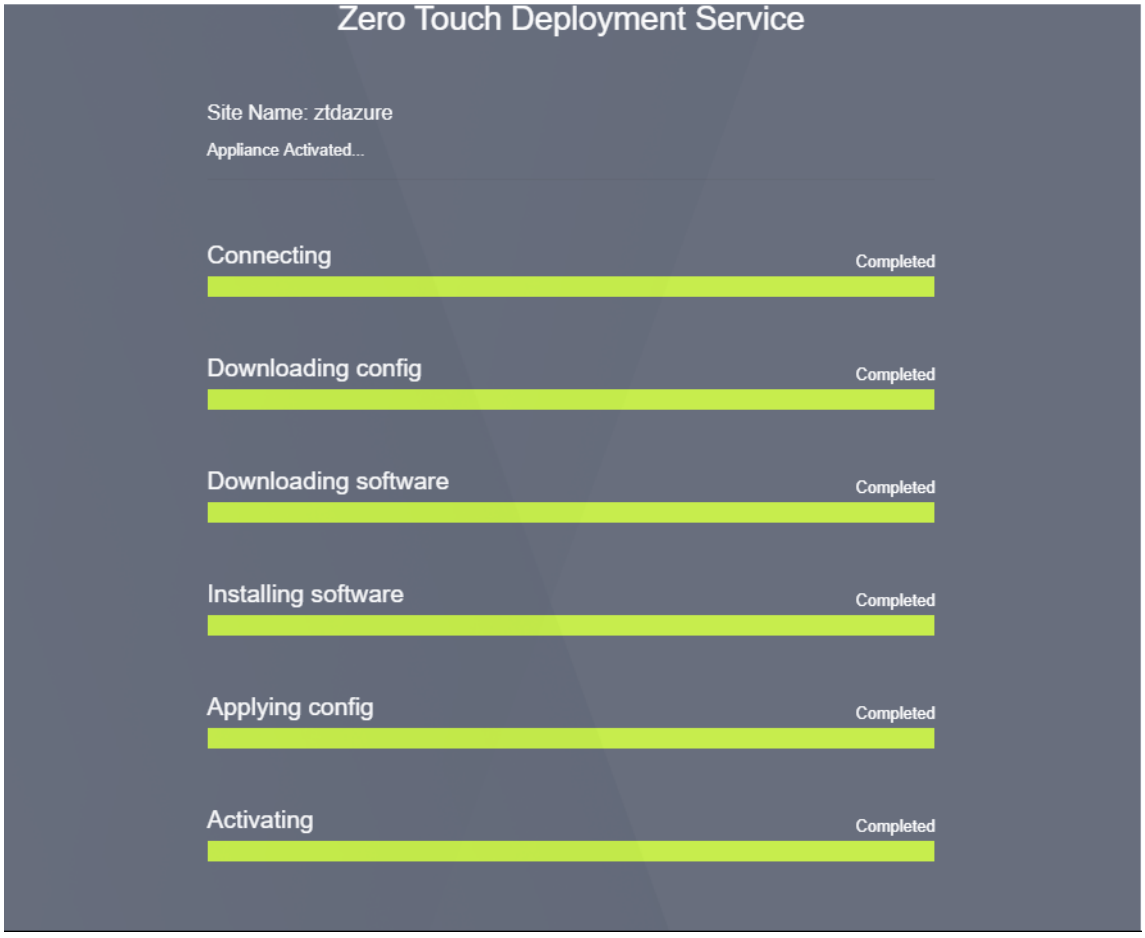
5. Es dauert einige Minuten, bis die Instanz vom SD-WAN Cloud Service bereitgestellt wird.Sie können die Aktivität im Azure-Portal unter **Aktivitätsprotokoll** für die automatisch erstellte **Ressourcengruppe** überwachen.Alle Probleme oder Fehler bei der Bereitstellung werden hier aufgefüllt und im Aktivierungsstatus auf SD-WAN Center repliziert.



6. Im Azure-Portal ist die erfolgreich gestartete Instanz unter **Virtuelle Maschinen verfügbar**. Um die zugewiesene öffentliche IP abzurufen, navigieren Sie zur Übersicht für die Instanz.

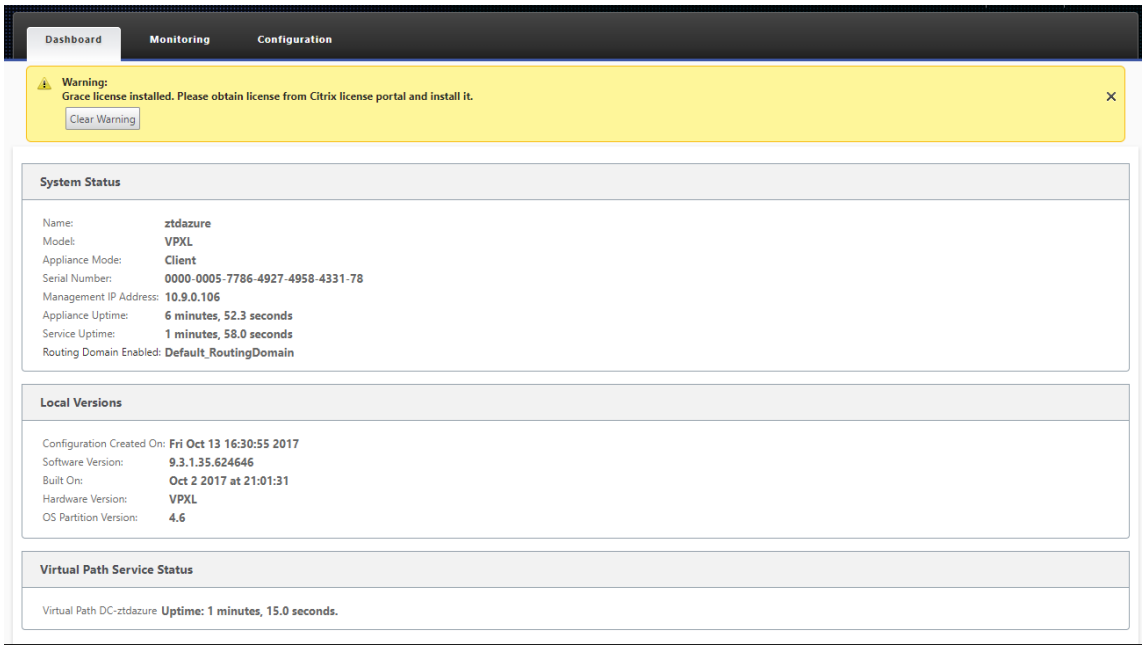


7. Nachdem sich die VM in einem laufenden Zustand befindet, geben Sie sie eine Minute, bevor der Dienst sich anspricht und den Prozess des Herunterladens der Konfiguration, der Software und der Lizenz startet.

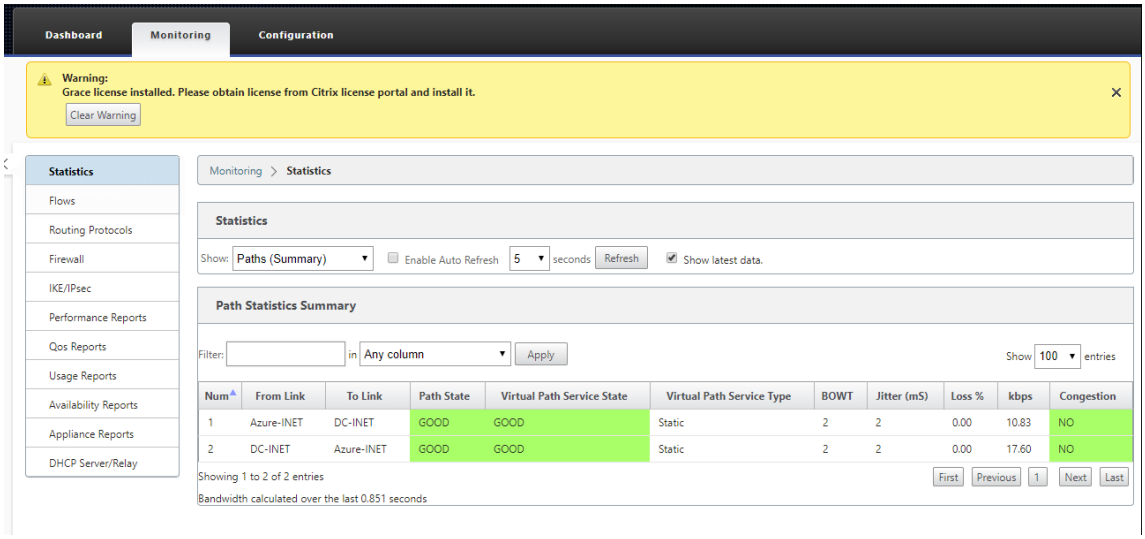


8. Nachdem die einzelnen SD-WAN-Cloud-Dienstschritte automatisch kompliziert sind, melden

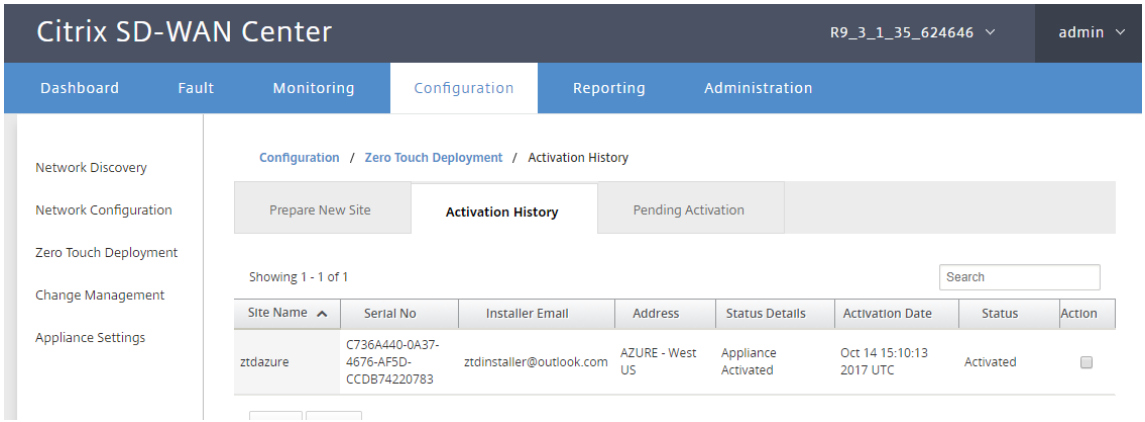
Sie sich bei der Webschnittstelle von SD-WAN-Instanzs mit der öffentlichen IP-Adresse an, die vom Azure-Portal abgerufen wurde.



9. Auf der Seite Citrix SD-WAN-Überwachungsstatistiken werden erfolgreiche Konnektivität vom MCN zur SD-WAN-Instanz in Azure identifiziert.



10. Darüber hinaus wird der erfolgreiche (oder erfolglose) Bereitstellungsversuch auf der Aktivierungsverlaufsseite des SD-WAN-Centers protokolliert.



Proxy-Server-Einstellungen für Null-Touch-Bereitstellung

April 13, 2021

Als Voraussetzung für die Zero Touch Deployment sollte das Citrix SD-WAN Center mit dem Internet verbunden sein. Wenn Ihr Citrix SD-WAN Center über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Server-Einstellungen im Citrix SD-WAN Center konfigurieren.

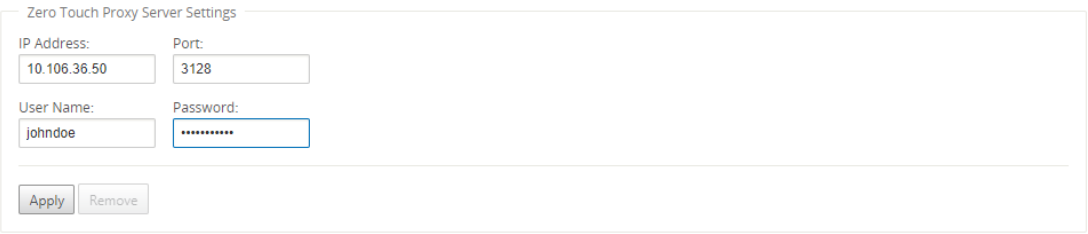
> **Hinweis**
>
> Diese Proxyservereinstellung wird nur für Zero Touch Deployment verwendet.

So konfigurieren Sie Null-Touch-Proxy-Server-Einstellungen:

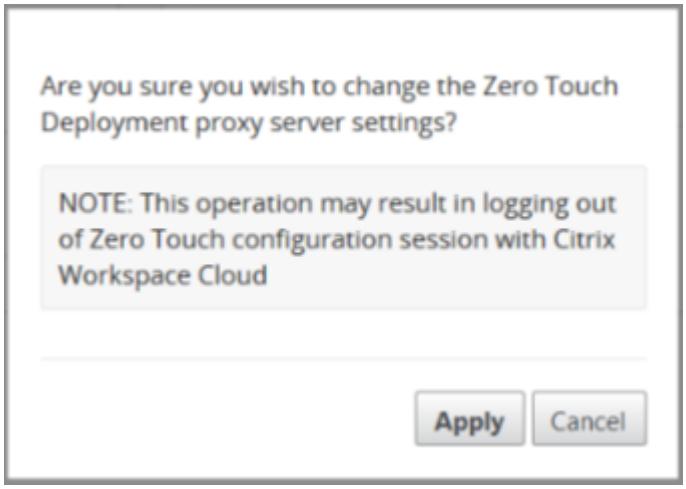
1. Navigieren Sie in der SD-WAN Center-Weboberfläche zu **Administration** > **Globale Einstellungen** > **Verwaltungsschnittstelle**.
2. Geben Sie im Abschnitt **Zero Touch Proxy Server Setting** Werte für die folgenden Felder ein:

   - **IP-Adresse: Die**IP-Adresse des Proxy-Servers.
   - **Port**: Die Netzwerkportnummer, auf der der Proxyserver Verbindungen akzeptiert.
   - **Benutzername**: Der Proxy-Server-Benutzername
   - **Kennwort**: Das Kennwort für den Proxy-Server.

   > **Hinweis**
   >
   > Sie können das Feld **Benutzername** und **Kennwort** leer lassen, wenn auf dem Proxyserver keine Authentifizierung konfiguriert ist.



3. Klicken Sie auf **Übernehmen**, ein Bestätigungsdialogfeld wird angezeigt.

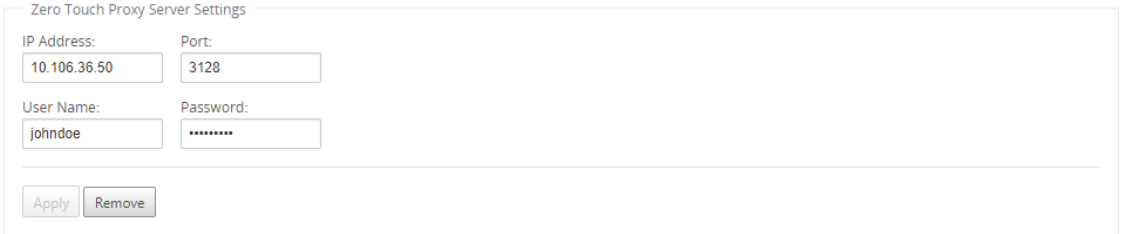


4. Klicken Sie auf **Apply**.

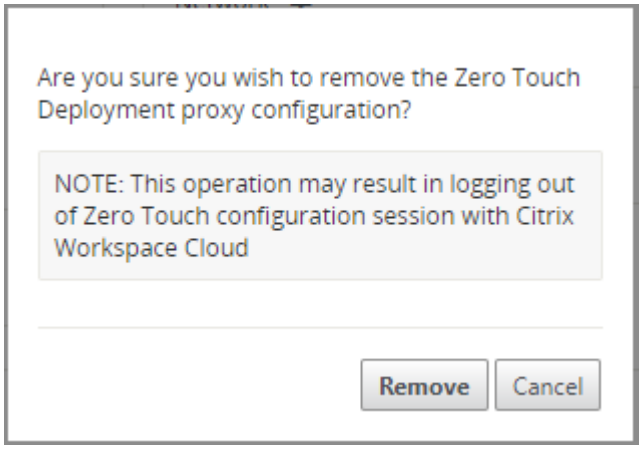
> **Hinweis**
>
> Sie können die Proxy-Server-Einstellungen ganz entfernen, wenn das Citrix SD-WAN Center direkt mit dem Internet verbunden ist. Sie können die Proxy-Server-Einstellungen auch entfernen und ggf. einen anderen Proxy-Server konfigurieren.

So entfernen Sie Proxy-Server-Einstellungen:

1. Navigieren Sie in der Citrix SD-WAN Center-Weboberfläche zu **Administration** > **Globale Einstellungen** > **Verwaltungsschnittstelle**.
2. Klicken Sie im Abschnitt **Zero Touch Proxy-Server-Einstellung** auf **Entfernen**.



3. Klicken Sie auf **Entfernen**, ein Bestätigungsdialogfeld wird angezeigt.



4. Klicken Sie auf **Entfernen**.

Palo Alto Netzwerkintegration

April 13, 2021

Palo Alto Netzwerke bieten cloudbasierte Sicherheitsinfrastruktur zum Schutz von Remote-Netzwerken. Es bietet Sicherheit, da Organisationen regionale, cloudbasierte Firewalls einrichten können, die die SD-WAN-Fabric schützen.

Mit dem Prisma Access Service für Remote-Netzwerke können Sie Remote-Netzwerkstandorte einbinden und den Benutzern Sicherheit bieten. Es beseitigt die Komplexität bei der Konfiguration und Verwaltung von Geräten an jedem Remote-Standort. Der Service bietet eine effiziente Möglichkeit, neue Remote-Netzwerkstandorte einfach hinzuzufügen und die betrieblichen Herausforderungen zu minimieren, indem sichergestellt wird, dass die Benutzer an diesen Standorten immer verbunden und sicher sind, und ermöglicht es Ihnen, Richtlinien zentral über Panorama zu verwalten, um eine konsistente und optimierte Sicherheit für Ihr Remote-Netzwerk zu gewährleisten. Netzwerkstandorte.

Um Ihre Remote-Netzwerkstandorte mit dem Prisma Access-Dienst zu verbinden, können Sie die Palo Alto Networks Firewall der nächsten Generation oder ein IPSec-kompatibles Gerät eines Drittanbieters einschließlich
SD-WAN verwenden, das einen IPSec-Tunnel für den Dienst einrichten kann.

- Planen des Prisma Access Service für Remote-Netzwerke
- Konfigurieren des Prisma Access Service für Remote-Netzwerke
- Onboard-Remote-Netzwerke mit Konfigurationsimport

Die Citrix SD-WAN Lösung bot bereits die Möglichkeit, den Internetverkehr von der Zweigstelle zu trennen. Dies ist entscheidend, um eine zuverlässigere Benutzererfahrung mit geringer Latenz zu er-

möglichen und gleichzeitig die Einführung eines teuren Sicherheits-Stacks in jedem Zweig zu vermeiden. Citrix SD-WAN und Palo Alto Networks bieten nun verteilten Unternehmen eine zuverlässigere und sicherere Möglichkeit, Benutzer in Zweigstellen mit Anwendungen in der Cloud zu verbinden.

Citrix SD-WAN Appliances können über IPSec-Tunnel von SD-WAN-Appliances Standorten mit minimaler Konfiguration mit dem Palo Alto Cloud-Dienst-Netzwerk (Prisma Access Service) verbunden werden. Sie können das Palo Alto Netzwerk in Citrix SD-WAN Center konfigurieren.

Bevor Sie mit der Konfiguration des Prisma Access Service für Remote Networks beginnen, stellen Sie sicher, dass Sie die folgende Konfiguration bereit haben, um sicherzustellen, dass Sie den Dienst erfolgreich aktivieren und Richtlinien für Benutzer in Ihren Remote-Netzwerkstandorten erzwingen können:

1. **Dienstverbindung**—Wenn Ihre Remote-Netzwerkstandorte Zugriff auf die Infrastruktur in Ihrer Unternehmenszentrale benötigen, um Benutzer zu authentifizieren oder den Zugriff auf wichtige Netzwerkressourcen zu ermöglichen, müssen Sie den Zugriff auf Ihr Unternehmensnetzwerk so einrichten, dass die Zentrale und die Remote-Netzwerkstandorte verbunden.

Wenn der Remote-Netzwerkstandort autonom ist und an anderen Standorten nicht auf die Infrastruktur zugreifen muss, müssen Sie die Dienstverbindung nicht einrichten (es sei denn, Ihre mobilen Benutzer benötigen Zugriff).

1. **Vorlage**—Der Prisma Access-Dienst erstellt automatisch einen Vorlagenstapel (Remote_Network_Template_
und eine oberste Vorlage (Remote_Network_Template) für den Prisma Access-Dienst für Remote-Netzwerke. Um den Prisma Access Service für Remote Networks zu konfigurieren, konfigurieren Sie die oberste Vorlage von Grund auf neu oder nutzen Ihre vorhandene Konfiguration, wenn Sie bereits eine Palo Alto Networks Firewall vor Ort ausführen.

   Die Vorlage erfordert die Einstellungen zum Einrichten der IPSec-Tunnel- und IKE-Konfiguration (Internet Key Exchange) für die Protokollaushandlung zwischen Ihrem Remote-Netzwerkstandort und dem Prisma Access-Dienst für Remote-Netzwerke, Zonen, die Sie in der Sicherheitsrichtlinie referenzieren können, und ein Protokollweiterleitungsprofil, damit Sie kann Protokolle vom Prisma Access-Dienst für Remote-Netzwerke an den Protokollierungsdienst weiterleiten.
2. **Übergeordnete Gerätegruppe**—Der Prisma Access-Dienst für Remote-Netzwerke erfordert, dass Sie eine übergeordnete Gerätegruppe angeben, die Ihre Sicherheitsrichtlinie, Sicherheitsprofile und andere Richtlinienobjekte (wie Anwendungsgruppen und Objekte und Adressgruppen) sowie Authentifizierungsrichtlinie enthält, damit Der Prisma Access-Dienst für Remote-Netzwerke kann Richtlinien für Datenverkehr durchsetzen, der durch den IPSec-Tunnel an den Prisma Access-Dienst für Remote-Netzwerke weitergeleitet wird. Sie müssen entweder Richtlinienregeln und -objekte in Panorama definieren oder eine vorhandene Gerätegruppe verwenden, um Benutzer am Remote-Netzwerkstandort zu schützen.

> **Hinweis:**
>
> Wenn Sie eine vorhandene Gerätegruppe verwenden, die auf Zonen verweist, müssen Sie die entsprechende Vorlage, die die Zonen definiert, dem Remote_Network_Template_Stack hinzufügen.

Auf diese Weise können Sie die Zonenzuordnung abschließen, wenn Sie den Prisma Access Service für Remote Networks konfigurieren.

3. **IP-Subnetze**—Damit der Prisma Access-Dienst Datenverkehr an Ihre Remote-Netzwerke weiterleitet, müssen Sie Routinginformationen für die Teilnetze bereitstellen, die Sie mit dem Prisma Access-Dienst sichern möchten. Sie können entweder eine statische Route zu jedem Teilnetz am Remote-Netzwerkstandort definieren oder BGP zwischen den Dienstverbindungsstandorten und dem Prisma Access-Dienst konfigurieren oder eine Kombination beider Methoden verwenden.

   Wenn Sie beide statischen Routen konfigurieren und BGP aktivieren, haben die statischen Routen Vorrang. Zwar ist es praktisch, statische Routen zu verwenden, wenn Sie nur wenige Teilnetze an Ihren Remote-Netzwerkstandorten haben, in einer großen Bereitstellung mit vielen Remote-Netzwerken mit überlappenden Subnetzen, ermöglicht BGP Ihnen eine einfachere Skalierung.

Netzwerk Palo Alto in SD-WAN Center

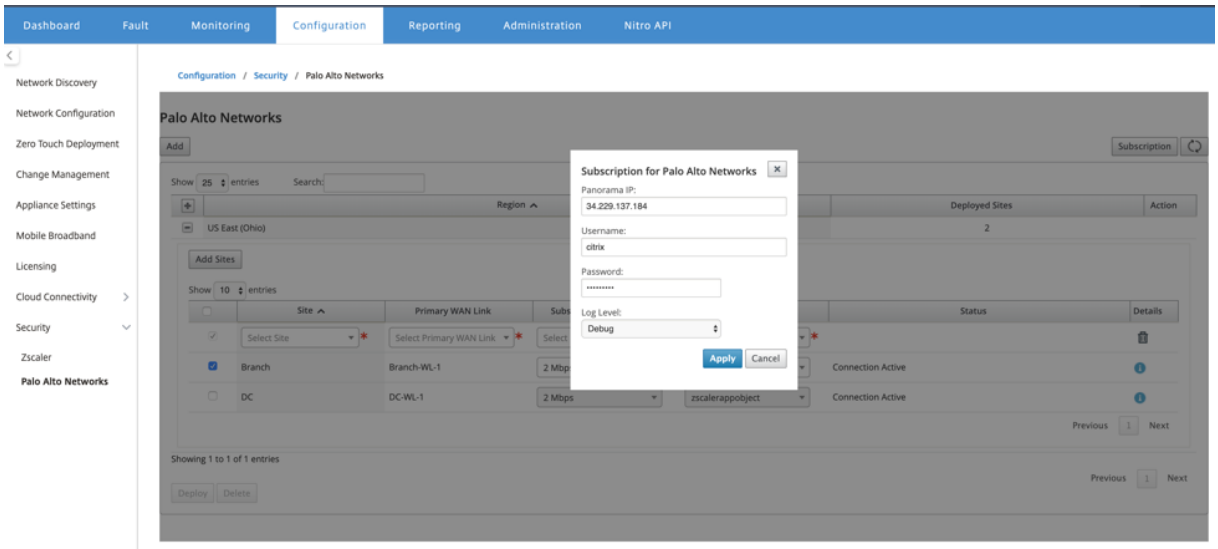
Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Rufen Sie die Panorama-IP-Adresse vom PRISMA ACCESS-Service ab.
- Rufen Sie Benutzernamen und Kennwortbenutzer im PRISMA ACCESS-Service ab.
- Konfigurieren Sie IPSec-Tunnel in der Benutzeroberfläche der SD-WAN-Appliance.
- Stellen Sie sicher, dass die Site nicht in eine Region integriert ist, in der bereits eine andere Site mit anderen ike/ipsec-Profilen als Citrix-ike-crypto-default/Citrix-IPsec-crypto-default konfiguriert ist.
- Stellen Sie sicher, dass die Prisma Access-Konfiguration nicht manuell geändert wird, wenn die Konfiguration vom SD-WAN Center aktualisiert wird.

Geben Sie in der Benutzeroberfläche des Citrix SD-WAN Centers Palo Alto Abonnementinformationen an.

- Konfigurieren Sie die Panorama-IP-Adresse. Diese IP-Adresse erhalten Sie von Palo Alto (PRISMA ACCESS Dienst).

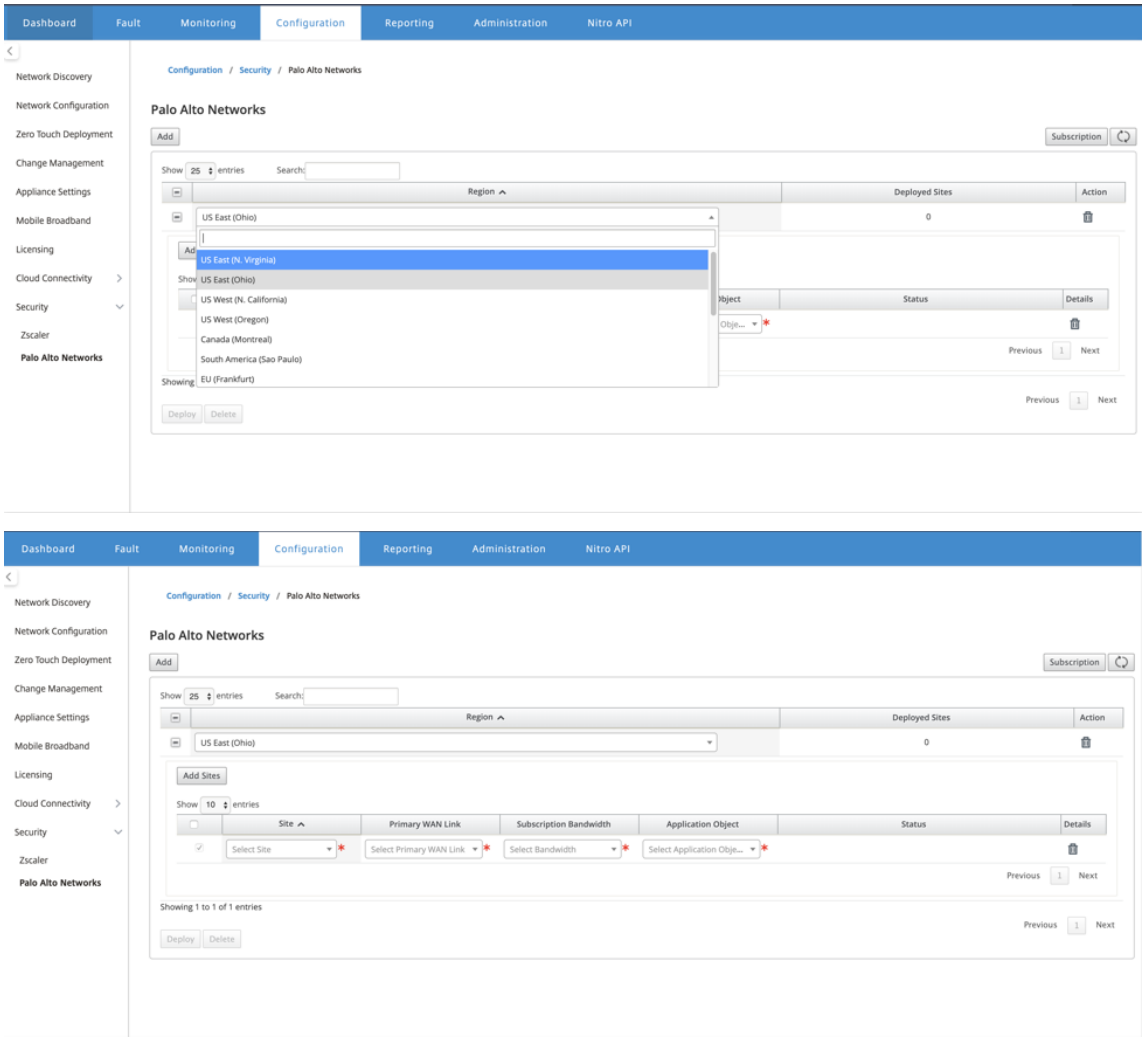
- Konfigurieren Sie den Benutzernamen und das Kennwort, die im PRISMA ACCESS-Dienst verwendet werden.



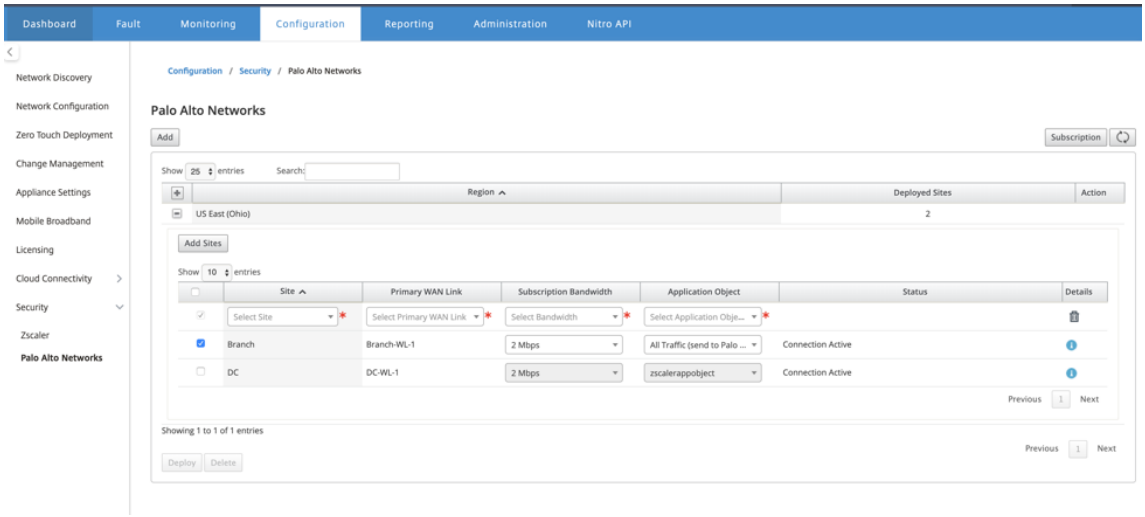
Hinzufügen und Bereitstellen von Sites

1. Um die Sites bereitzustellen, wählen Sie die PRISMA ACCESS-Netzwerkregion und die SD-WAN-Site aus, die für die Prisma Access-Region konfiguriert werden soll, und wählen Sie dann die Standort-WAN-Link, die Bandbreite und das Anwendungsobjekt für die Datenverkehrsauswahl aus.

   > **Hinweis:**
   >
   > Der Datenfluss wird beeinträchtigt, wenn die ausgewählte Bandbreite den verfügbaren Bandbreitenbereich überschreitet.
   >
   > Sie können den gesamten internetgebundenen Datenverkehr an den PRISMA ACCESS-Service umleiten, indem Sie unter der Objektauswahl Anwendung die Option **Alle Datenverkehr** auswählen.

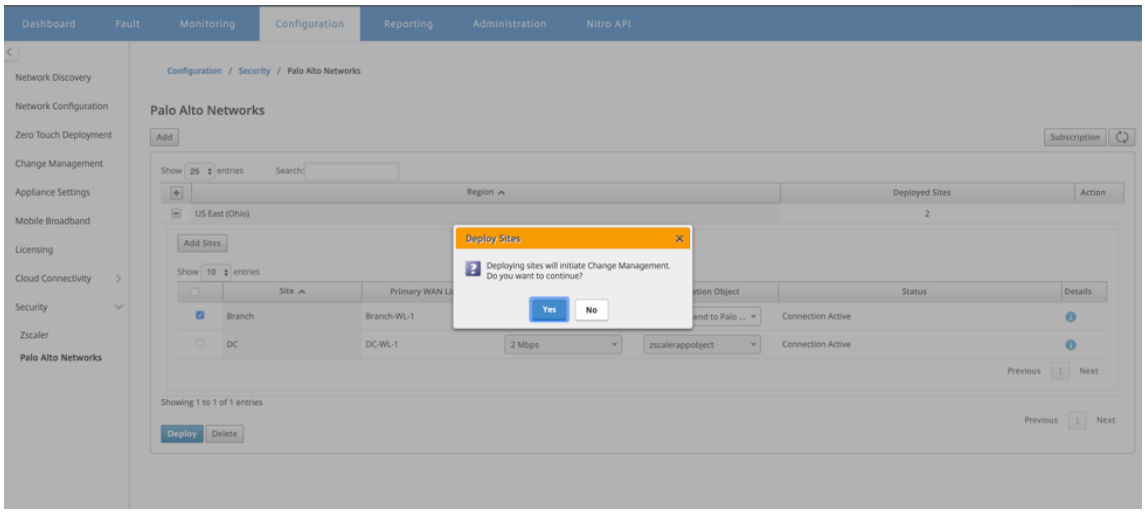


2. Sie können nach Bedarf weitere SD-WAN-Zweigstellen hinzufügen.

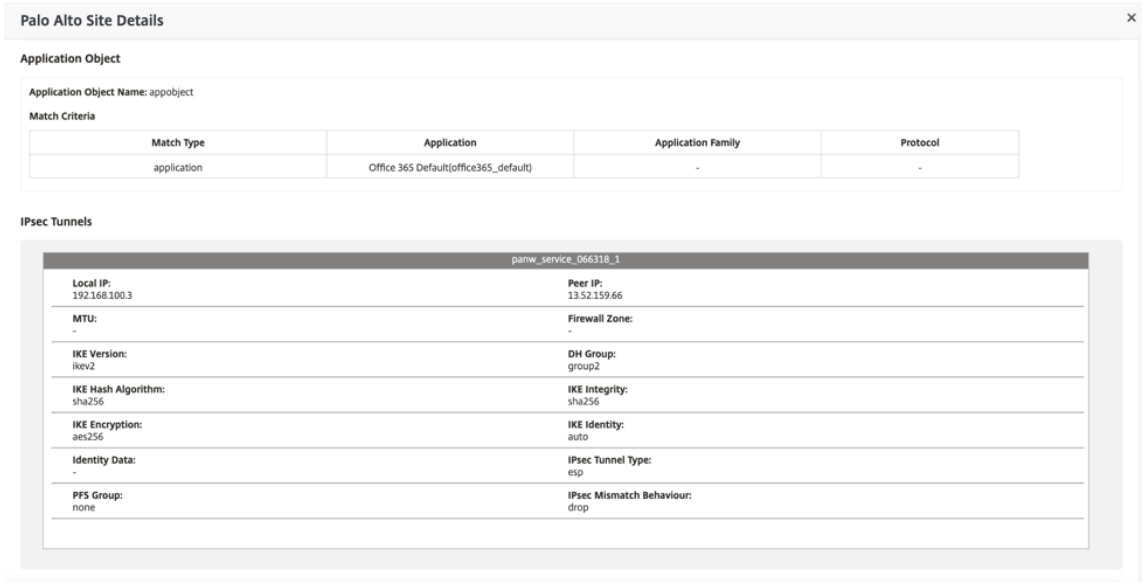


3. Klicken Sie auf **Bereitstellen**. Der Änderungsmanagement-Prozess wird initiiert. Klicken Sie

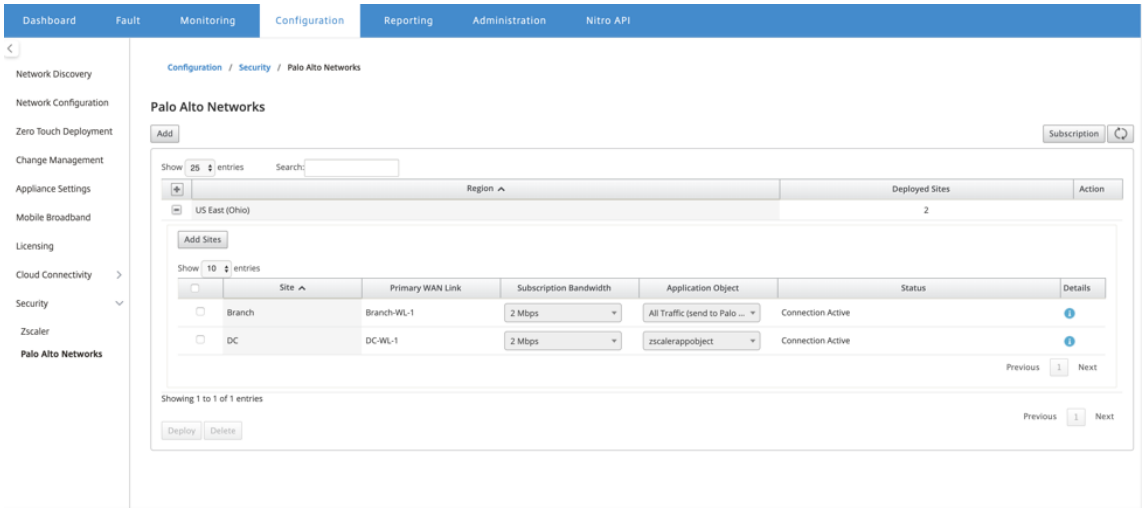
auf **Ja**, um fortzufahren.



Nach der Bereitstellung ist die IPSec-Tunnelkonfiguration, die zum Einrichten der Tunnel verwendet wird, wie folgt.



Die Zielseite zeigt die Liste aller Sites an, die unter verschiedenen SD-WAN-Regionen konfiguriert und gruppiert sind.



Überprüfen Sie die End-to-End-Datenverkehrsverbindung:

- Aus dem LAN-Subnetz der Zweigstelle, greifen Sie auf Internetressourcen zu.
- Stellen Sie sicher, dass der Datenverkehr über den Citrix SD-WAN IPSec-Tunnel zum Palo Alto Prisma Access geht.
- Überprüfen Sie, ob die Sicherheitsrichtlinie von Palo Alto auf den Datenverkehr auf der Registerkarte Überwachung angewendet wird.
- Überprüfen Sie, ob die Antwort von Internet zu Host in einem Zweig durchläuft.

Microsoft Azure Virtual WAN

April 13, 2021

Microsoft Azure Virtual WAN und Citrix SD-WAN bieten vereinfachte Netzwerkkonnektivität und zentralisierte Verwaltung über hybride Cloud-Workloads hinweg. Sie können die Konfiguration von Zweiganwendungen automatisieren, um eine Verbindung mit dem Azure-WAN herzustellen und Richtlinien für die Verwaltung von Zweigstellen entsprechend Ihren geschäftlichen Anforderungen konfigurieren. Die integrierte Dashboard-Schnittstelle bietet sofortige Einblicke in die Problembehandlung, die Zeit sparen und Transparenz für große Site-zu-Site-Konnektivität bietet.

Mit Microsoft Azure Virtual WAN können Sie vereinfachte Konnektivität zu Azure Cloud-Arbeitslasten aktivieren und Datenverkehr über das Azure-Backbone-Netzwerk und darüber hinaus weiterleiten. Azure bietet über 54 Regionen und mehrere Anwesenheitspunkte auf der ganzen Welt dienen Azure Regionen als Hubs, die Sie für eine Verbindung mit den Zweigen auswählen können. Nachdem die Zweige verbunden sind, verwenden Sie den Azure-Clouddienst über Hub-zu-Hub-Konnektivität. Sie

können die Konnektivität vereinfachen, indem Sie mehrere Azure-Dienste einschließlich Hub-Peering mit Azure VNETs anwenden. Hubs dienen als Verkehrs-Gateways für die Filialen.

Microsoft Azure Virtual WAN bietet folgende Vorteile:

- Integrierte Konnektivitätslösungen in Hub and Spoke —Automatisieren Sie die Standort-zu-Standort-Konnektivität und Konfiguration zwischen lokal und dem Azure-Hub aus verschiedenen Quellen, einschließlich vernetzter Partnerlösungen.
- Automatisierte Einrichtung und Konfiguration —Verbinden Sie Ihre virtuellen Netzwerke nahtlos mit dem Azure-Hub.
- Intuitive Problembehandlung —Sie können den End-to-End-Ablauf in Azure anzeigen und diese Informationen verwenden, um erforderliche Aktionen durchzuführen.

Verwenden von Citrix SD-WAN zum Herstellen einer Verbindung mit Microsoft Azure Virtual WAN

February 16, 2022

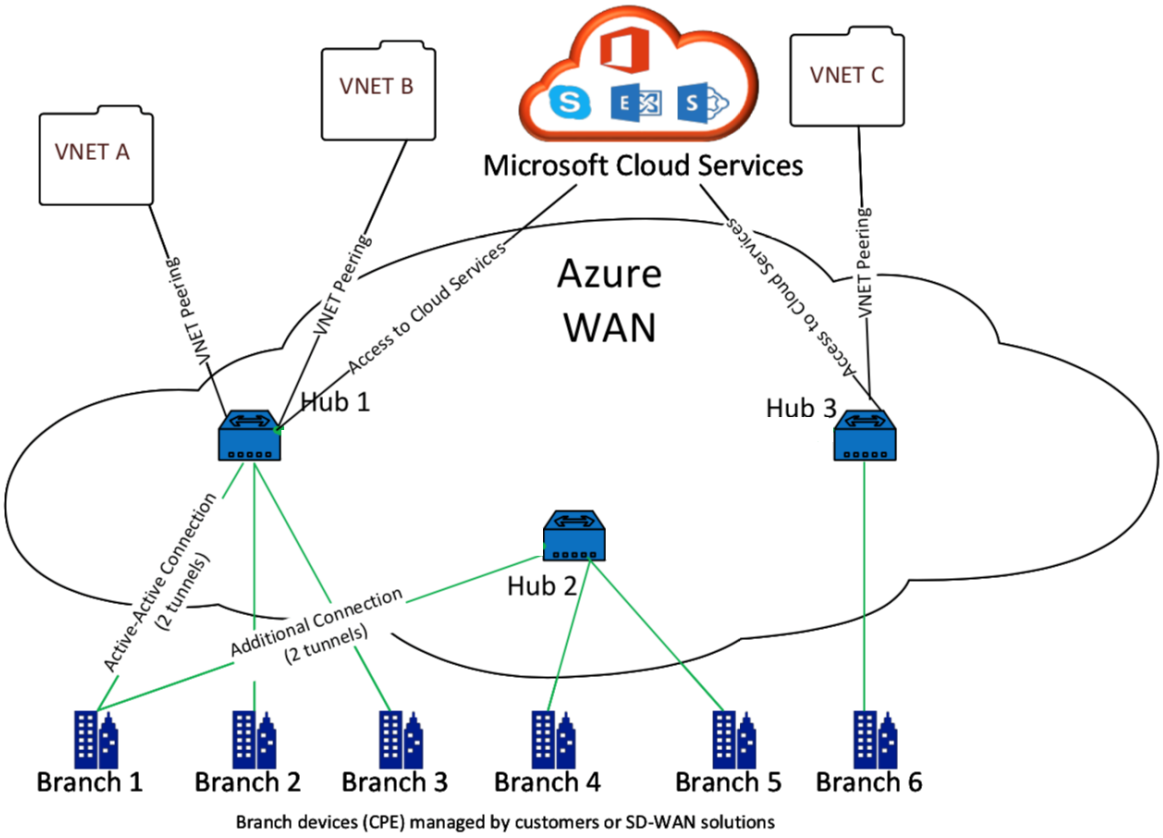
Damit lokale Geräte eine Verbindung mit Azure herstellen können, ist ein Controller erforderlich. Ein Controller erfasst Azure-APIs, um Standortkonnektivität mit dem Azure-WAN und einem Hub herzustellen.

Microsoft Azure Virtual WAN enthält die folgenden Komponenten und Ressourcen:

- WAN: Stellt das gesamte Netzwerk in Microsoft Azure dar. Es enthält Links zu allen Hubs, die Sie in diesem WAN haben möchten. WANs sind voneinander isoliert und können keinen gemeinsamen Hub oder Verbindungen zwischen zwei Hubs in verschiedenen WANs enthalten.
- Site: Stellt Ihr lokales VPN-Gerät und seine Einstellungen dar. Eine Site kann sich mit mehreren Hubs verbinden. Mit Citrix SD-WAN können Sie über eine integrierte Lösung verfügen, um diese Informationen automatisch in Azure zu exportieren.
- Hub: Stellt den Kern Ihres Netzwerks in einer bestimmten Region dar. Der Hub enthält verschiedene Service-Endpunkte, um Konnektivität und andere Lösungen für Ihr lokales Netzwerk zu ermöglichen. Standort-zu-Site-Verbindungen werden zwischen den Sites zu einem Hubs-VPN-Endpunkt hergestellt.
- Virtuelle Hub-Netzwerkverbindung: Hub-Netzwerk verbindet den Azure Virtual WAN Hub nahtlos mit Ihrem virtuellen Netzwerk. Derzeit ist eine Konnektivität zu virtuellen Netzwerken verfügbar, die sich innerhalb derselben Virtual Hub-Region befinden.

- Zweig: Die Zweigstellen sind die lokalen Citrix SD-WAN-Appliances, die in Kundenstandorten vorhanden sind. Ein SD-WAN-Controller verwaltet die Zweige zentral. Die Verbindung stammt von hinter diesen Zweigen und endet in Azure. Der SD-WAN-Controller ist dafür verantwortlich, die erforderliche Konfiguration auf diese Zweige und auf Azure Hubs anzuwenden.

In der folgenden Abbildung werden die Virtual WAN-Komponenten beschrieben:



Wie funktioniert Microsoft Azure Virtual WAN?

1. Das SD-WAN-Center wird mithilfe von Dienstprinzipal, Prinzipal oder rollenbasierten Zugriffsfunktionen authentifiziert, die in der Azure-Benutzeroberfläche aktiviert ist.
2. Das SD-WAN-Center ruft die Azure-Konnektivitätskonfiguration ab und aktualisiert das lokale Gerät. Dadurch wird das Herunterladen, Bearbeiten und Aktualisieren der Konfiguration des lokalen Geräts automatisiert.
3. Nachdem das Gerät über die richtige Azure-Konfiguration verfügt, wird eine Standort-zu-Standort-Verbindung (zwei aktive IPSec-Tunnel) mit dem Azure-WAN hergestellt. Azure erfordert den Zweiggeräteconnector, um IKEv2-Einstellungen zu unterstützen. Die BGP-Konfiguration ist optional.

Hinweis: IPSec-Parameter für die Einrichtung von IPSec-Tunneln sind standardisiert.

IPSec-Eigenschaft	Parameter
Ike Verschlüsselungsalgorithmus	AES-256
Ike Integritätsalgorithmus	SHA 256
Dh Gruppe	DH2
IPsec-Verschlüsselungsalgorithmus	GCM AES 256
IPSec-Integritätsalgorithmus	GCM AES 256
PFS Gruppe	Ohne

Azure Virtual WAN automatisiert die Konnektivität zwischen dem virtuellen Netzwerk der Arbeitslast und dem Hub. Wenn Sie eine virtuelle Hubnetzwerkverbindung erstellen, wird die entsprechende Konfiguration zwischen dem bereitgestellten Hub und dem virtuellen Netzwerk (VNET) der Arbeitslasten festgelegt.

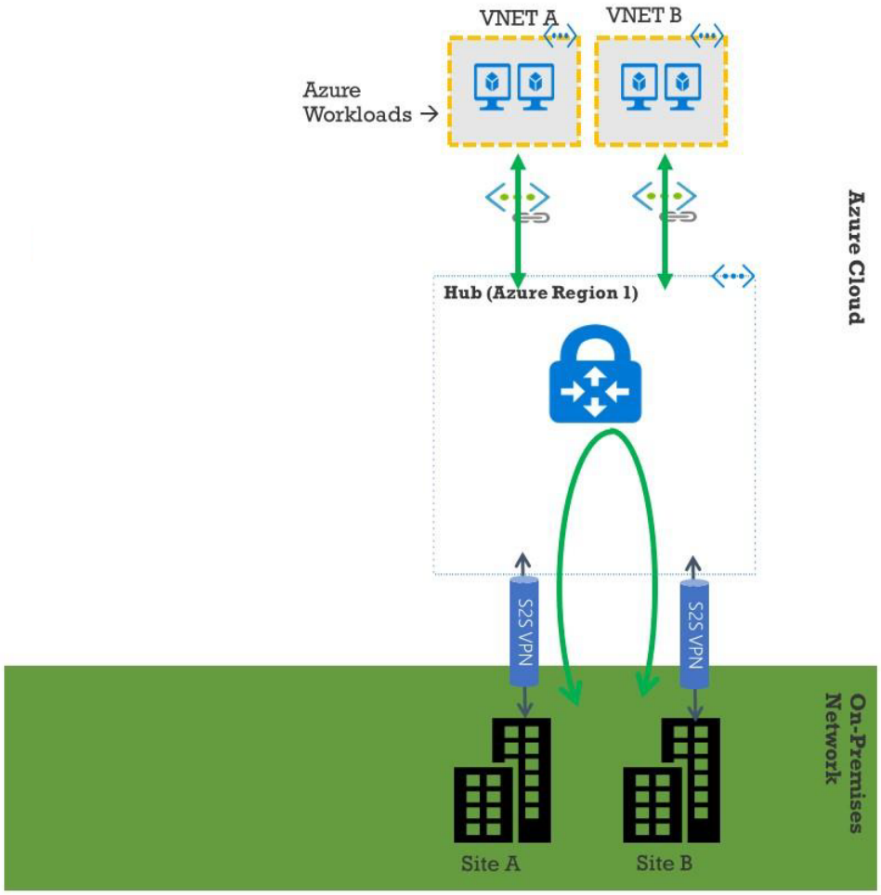
Voraussetzungen und Anforderungen

Lesen Sie die folgenden Anforderungen, bevor Sie mit der Konfiguration von Azure und SD-WAN zum Verwalten von Zweigsites, die eine Verbindung zu Azure-Hubs herstellen, fortfahren.

1. Azure-Abonnement für Virtual WAN auf die Positivliste gesetzt haben.
2. Verfügen Sie über eine lokale Appliance wie eine SD-WAN-Appliance, um IPSec in Azure-Ressourcen einzurichten.
3. Haben Sie Internet-Links mit öffentlichen IP-Adressen. Obwohl eine einzelne Internetverbindung ausreicht, um eine Verbindung mit Azure herzustellen, benötigen Sie zwei IPSec-Tunnel, um dieselbe WAN-Verbindung zu verwenden.
4. SD-WAN-Controller: Ein Controller ist die Schnittstelle, die für die Konfiguration von SD-WAN-Appliances für die Verbindung mit Azure zuständig ist.
5. Ein VNET in Azure mit mindestens einer Arbeitslast. Zum Beispiel eine VM, die einen Dienst hostet. Berücksichtigen Sie die folgenden Punkte:

    a) Das virtuelle Netzwerk sollte nicht über ein Azure VPN- oder Express Route-Gateway oder eine virtuelle Netzwerk-Appliance verfügen.
    b) Das virtuelle Netzwerk sollte keine benutzerdefinierte Route haben, die den Datenverkehr für die Arbeitslast, auf die von einem lokalen Zweig aus zugegriffen wird, an ein nicht virtuelles WAN-Netzwerk weiterleitet.
    c) Die entsprechenden Berechtigungen für den Zugriff auf die Arbeitslast müssen konfiguriert werden. Zum Beispiel Port 22 SSH-Zugriff für eine Ubuntu-VM.

Das folgende Diagramm veranschaulicht ein Netzwerk mit zwei Standorten und zwei virtuellen Netzwerken in Microsoft Azure.



Microsoft Azure Virtual WAN einrichten

Damit lokale SD-WAN-Zweige eine Verbindung zu Azure herstellen und über IPSec-Tunnel auf die Ressourcen zugreifen können, sollten die folgenden Schritte ausgeführt werden.

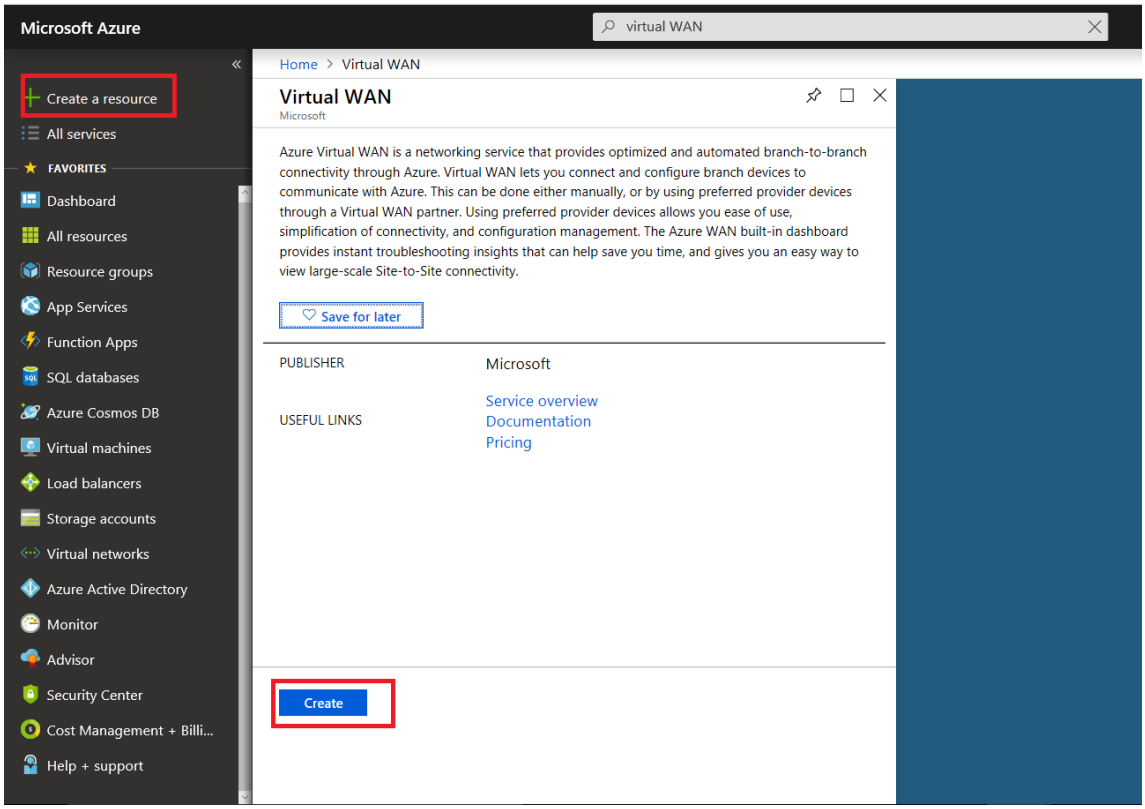
1. Konfigurieren von WAN-Ressourcen.
2. Aktivieren von SD-WAN-Zweigen für die Verbindung mit Azure mithilfe von IPSec-Tunneln.

Konfigurieren Sie Azure-Netzwerk, bevor Sie das SD-WAN-Netzwerk konfigurieren, da die für die Verbindung mit SD-WAN-Appliances erforderlichen Azure-Ressourcen vorher verfügbar sein müssen. Sie können jedoch die SD-WAN-Konfiguration konfigurieren, bevor Sie Azure-Ressourcen konfigurieren. In diesem Thema wird zuerst das Einrichten des Azure Virtual WAN-Netzwerks vor der Konfiguration von SD-WAN-Appliances erörtert. https://microsoft.com azurblaues virtuelles WAN.

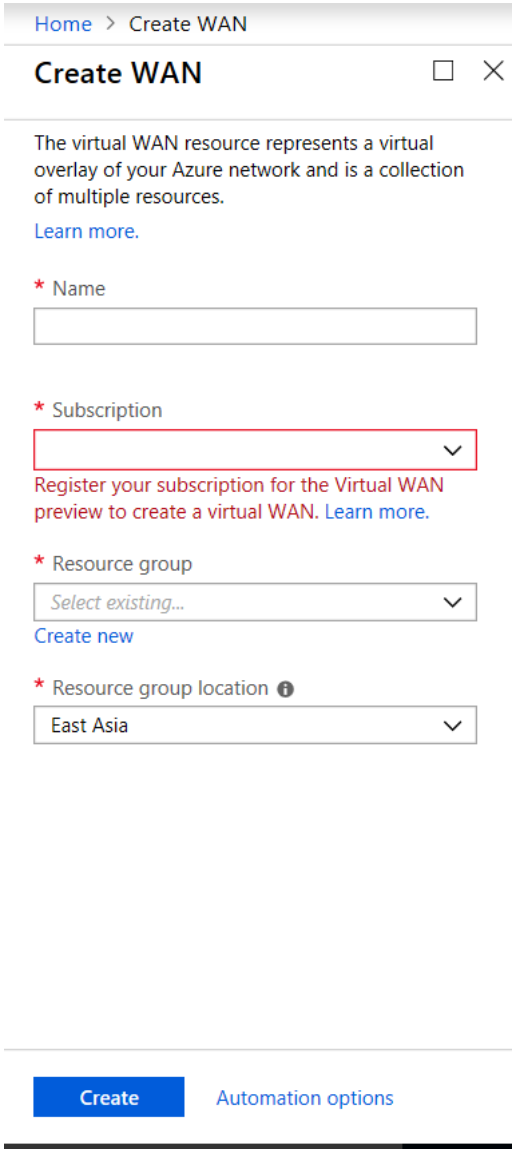
Erstellen einer WAN-Ressource

So verwenden Sie Virtual WAN-Funktionen und verbinden die on-premises Zweig-Appliance mit Azure:

1. Melden Sie sich bei Azure Marketplacean, rufen Sie die Virtual WAN-App auf und wählen Sie **WAN erstellen**aus.



2. Geben Sie einen Namen für das WAN ein und wählen Sie das Abonnement aus, das Sie für WAN verwenden möchten.



3. Wählen Sie eine vorhandene Ressourcengruppe aus, oder erstellen Sie eine neue Ressourcengruppe. Ressourcengruppen sind logische Konstrukte und der Datenaustausch über Ressourcengruppen hinweg ist immer möglich.
4. Wählen Sie den Speicherort aus, an dem sich die Ressourcengruppe befinden soll. WAN ist eine globale Ressource, die keinen Standort hat. Sie müssen jedoch einen Speicherort für die Ressourcengruppe eingeben, der Metadaten für die WAN-Ressource enthält.
5. Klicken Sie auf **Erstellen**. Dadurch wird der Prozess zum Überprüfen und Bereitstellen der Einstellungen gestartet.

Site erstellen

Sie können eine Site über einen bevorzugten Anbieter erstellen. Der bevorzugte Anbieter sendet die Informationen zu Ihrem Gerät und Ihrer Site an Azure oder Sie können entscheiden, das Gerät selbst zu verwalten. Wenn Sie das Gerät verwalten möchten, müssen Sie die Site in Azure Portal erstellen.

SD-WAN-Netzwerk und Microsoft Azure Virtual WAN-Workflow

Konfigurieren der SD-WAN-Appliance:

1. Bereitstellen einer Citrix SD-WAN-Appliance
    - Verbinden Sie die SD-WAN-Zweigeinheit mit der MCN-Appliance.
2. Konfigurieren der SD-WAN-Appliance
    - Konfigurieren Sie die Intranetdienste für die Active-Active Verbindung.

Konfigurieren Sie das SD-WAN-Center:

- Konfigurieren Sie SD-WAN Center für die Verbindung mit Microsoft Azure.

Konfigurieren von Azure-Einstellungen:

- Geben Sie Mandanten-ID, Client-ID, Secure Key, Subscriber-ID und Ressourcengruppe an.

Konfigurieren Sie den Zweigstandort zu WAN-Zuordnung:

1. Ordnen Sie einer Zweigstelle eine WAN-Ressource zu. Der gleiche Standort kann nicht mit mehreren WANs verbunden werden.
2. Klicken Sie auf **Neu**, um Site-WAN-Zuordnung zu konfigurieren.
3. Wählen Sie **Azure WAN-Ressourcen**aus.
4. Wählen Sie **Dienste** (Intranet) für die Site aus. Wählen Sie zwei Dienste für Active-Standby-Unterstützung aus.
5. Wählen Sie **Sitenamen** aus, die den WAN-Ressourcen zugeordnet werden sollen.
6. Klicken Sie auf **Bereitstellen**, um die Zuordnung zu bestätigen.
7. Warten Sie, bis der Status in **Tunnel bereitgestellt** geändert wurde, um die **IPsec**-Tunneleinstellungen anzuzeigen.
8. Verwenden Sie die Ansicht SD-WAN Center Reporting, um den Status der jeweiligen IPSec-Tunnel zu überprüfen.

Konfigurieren des Citrix SD-WAN-Netzwerks

MCN:

Das MCN dient als Verteilungspunkt für die anfängliche Systemkonfiguration und nachfolgende Konfigurationsänderungen. In einem virtuellen WAN kann nur ein aktives MCN vorhanden sein. Standardmäßig haben Appliances die vorab zugewiesene Rolle des Clients. Um eine Appliance als MCN einzurichten, müssen Sie zuerst die Site als MCN hinzufügen und konfigurieren. Die Benutzeroberfläche für die Netzwerkkonfiguration wird verfügbar, nachdem ein Standort als MCN konfiguriert wurde. Upgrades und Konfigurationsänderungen müssen nur über das MCN- oder SD-WAN-Center durchgeführt werden.

Rolle von MCN:

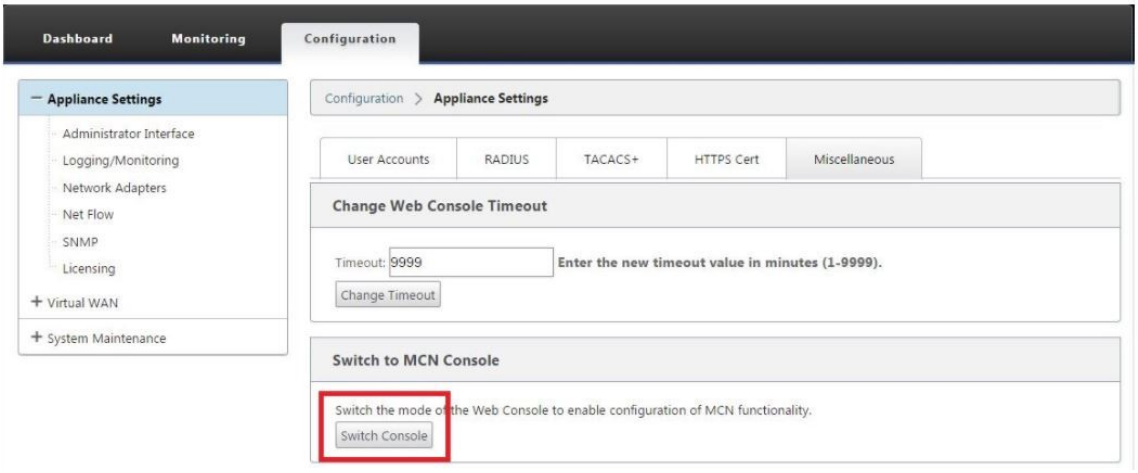
Der MCN ist der zentrale Knoten, der als Controller eines SD-WAN-Netzwerks fungiert, und der zentrale Verwaltungspunkt für die Client-Knoten. Alle Konfigurationsaktivitäten und die Vorbereitung von Firmware-Paketen und deren Verteilung an die Clients werden auf dem MCN konfiguriert. Darüber hinaus sind Überwachungsinformationen nur auf dem MCN verfügbar. Das MCN kann das gesamte SD-WAN-Netzwerk überwachen, während Client-Knoten nur die lokalen Intranets und einige Informationen für diese Clients überwachen können, mit denen sie verbunden sind. Der Hauptzweck des MCN besteht darin, Overlay-Verbindungen (virtuelle Pfade) mit einem oder mehreren Client-Knoten im SD-WAN-Netzwerk für die Unternehmens-Standort-zu-Standort-Kommunikation herzustellen. Ein MCN kann virtuelle Pfade zu mehreren Client-Knoten verwalten und haben. Es kann mehr als ein MCN geben, aber nur eine kann zu einem bestimmten Zeitpunkt aktiv sein. Die folgende Abbildung veranschaulicht das grundlegende Diagramm der MCN- und Client- (Zweigknoten) -Appliances für ein kleines Netzwerk von zwei Standorten.

Konfigurieren der SD-WAN-Appliance als MCN

Um das MCN hinzuzufügen und zu konfigurieren, müssen Sie sich zuerst bei der Management-Webschnittstelle auf der Appliance anmelden, die Sie als MCN festlegen, und die Management-Webschnittstelle in den MCN-Konsolenmodus wechseln. Der MCN-Konsolenmodus ermöglicht den Zugriff auf den Konfigurationseditor im Management-Webinterface, mit dem Sie derzeit verbunden sind. Sie können dann den Konfigurationseditor verwenden, um die MCN-Site hinzuzufügen und zu konfigurieren.

Gehen Sie wie folgt vor, um das Management-Webinterface in den MCN-Konsolenmodus umzuschalten:

1. Melden Sie sich bei der SD-WAN-Management-Weboberfläche der Appliance an, die Sie als MCN konfigurieren möchten.
2. Klicken Sie in der Hauptmenüleiste des Hauptbildschirms des Management Webinterface auf **Konfiguration** (blauer Balken oben auf der Seite).
3. Öffnen Sie in der Navigationsstruktur (linker Bereich) den Zweig **Applianceeinstellungen** und klicken Sie auf **Administratorschnittstelle**.
4. Wählen Sie die Registerkarte **Verschiedenes**. Die Seite mit den verschiedenen administrativen Einstellungen wird geöffnet.



   Am unteren Rand der Registerkarte **Verschiedenes** befindet sich der Abschnitt **Switch to [Client, MCN] Console**. Dieser Abschnitt enthält die Schaltfläche **Konsole wechseln**, um zwischen den Konsolenmodi der Appliance umzuschalten.

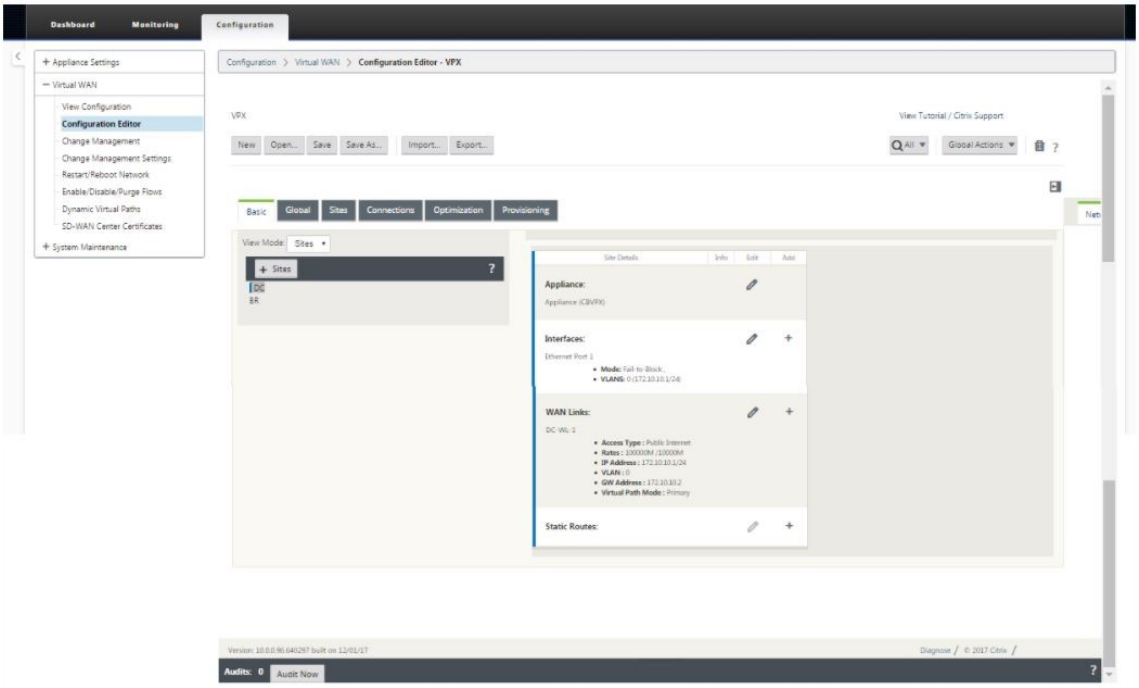
Die Abschnittsüberschrift zeigt den aktuellen Konsolenmodus wie folgt an:

- Im Client-Konsolenmodus (Standard) lautet die Abschnittsüberschrift Switch to MCN Console.
- Im MCN-Konsolenmodus lautet die Abschnittsüberschrift Switch to Client Console.

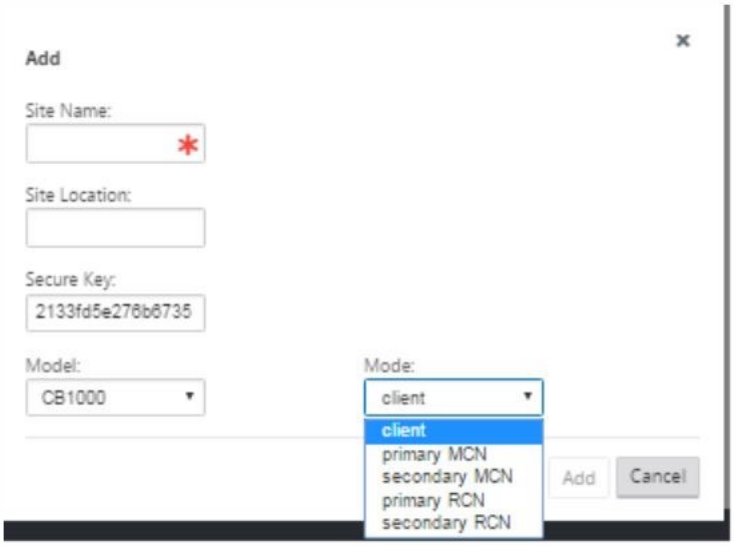
Standardmäßig befindet sich eine neue Appliance im Client-Konsolenmodus. Im MCN-Konsolenmodus wird die Ansicht des Konfigurationseditors in der Navigationsstruktur aktiviert. Der Konfigurationseditor ist nur auf der MCN-Appliance verfügbar.

MCN konfigurieren Gehen Sie folgendermaßen vor, um die MCN-Appliance-Site hinzuzufügen und mit der Konfiguration zu beginnen:

1. Navigieren Sie in der SD-WAN-Appliance-GUI zu **Virtual WAN** > **Konfigurationseditor**.

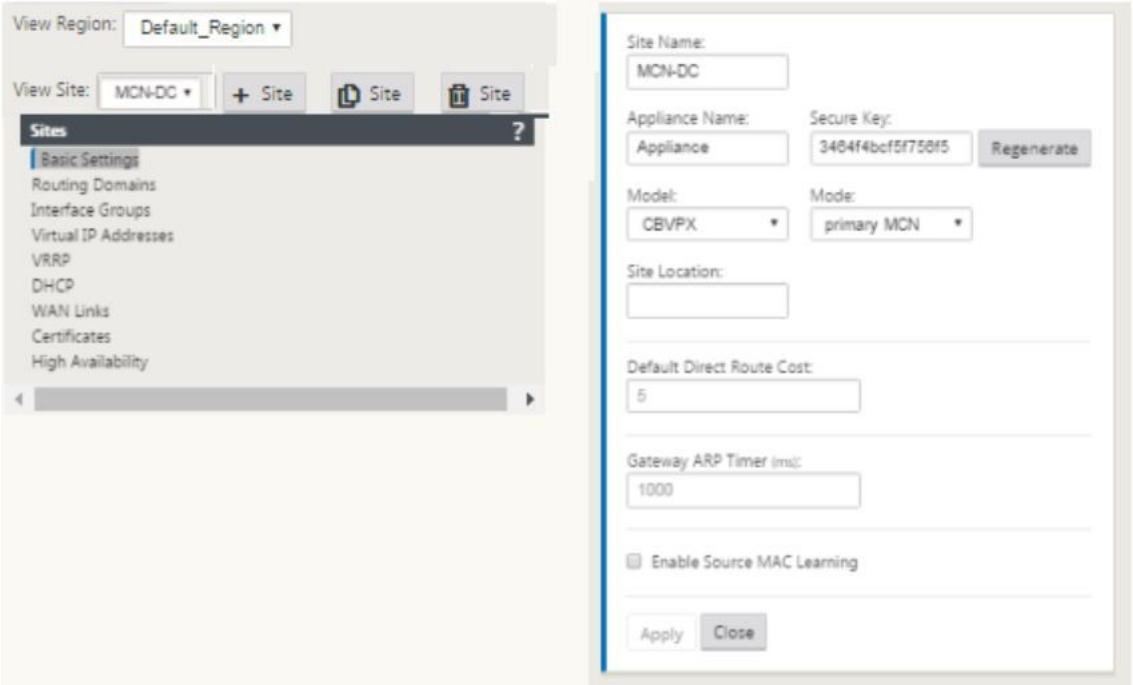


2. Klicken Sie in der Seitenleiste auf **+ Sites**, um mit dem Hinzufügen und Konfigurieren der MCN-Site zu beginnen. Das Dialogfeld **Site hinzufügen** wird angezeigt.

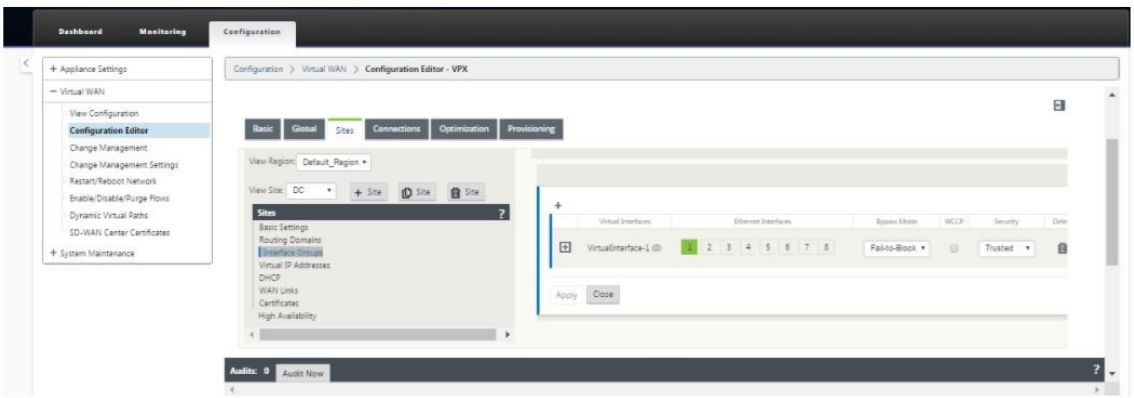


3. Geben Sie einen Standortnamen ein, mit dem Sie den geografischen Standort und die Rolle der Appliance (DC/Secondary DC) bestimmen können. Wählen Sie das richtige Einheitenmodell aus. Die Auswahl der richtigen Appliance ist entscheidend, da sich die Hardwareplattformen hinsichtlich Rechenleistung und Lizenzierung voneinander unterscheiden. Da wir diese Appliance als primäre Head-End-Appliance konfigurieren, wählen Sie den Modus als primäre MCN und klicken Sie auf **Hinzufügen**.
4. Dadurch wird die neue Site zur Site-Struktur hinzugefügt, und die Standardansicht zeigt die Kon-

figurationsseite für grundlegende Einstellungen, wie unten dargestellt:

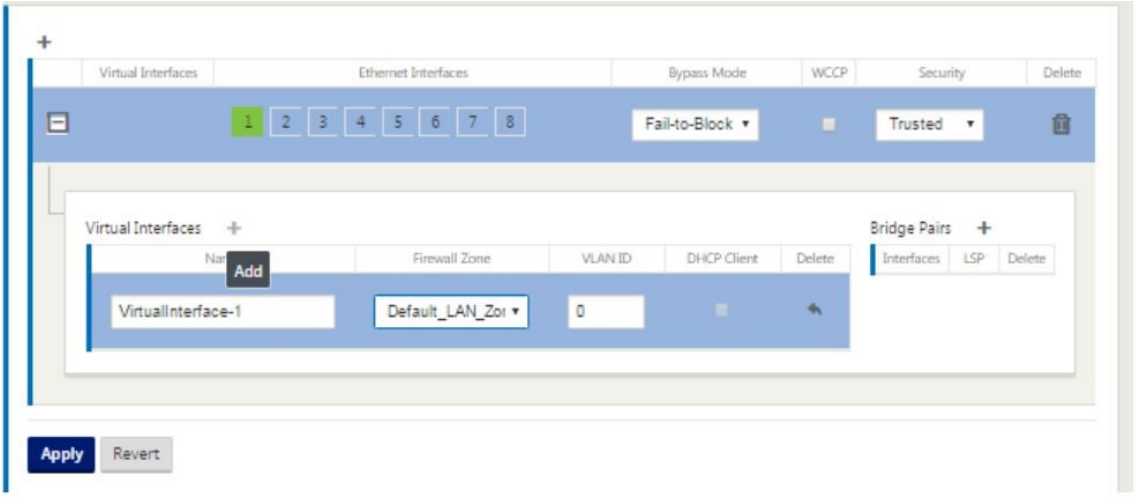


5. Geben Sie die grundlegenden Einstellungen wie Standort, Standortname ein.
6. Konfigurieren Sie die Appliance so, dass sie Datenverkehr vom Internet/MPLS/Breitband akzeptieren kann. Definieren Sie die Schnittstellen, auf denen die Links beendet werden. Dies hängt davon ab, ob sich die Appliance im Overlay- oder Unterlagermodus befindet.
7. Klicken Sie auf **“Interface groups”,** um die Schnittstellen zu definieren.

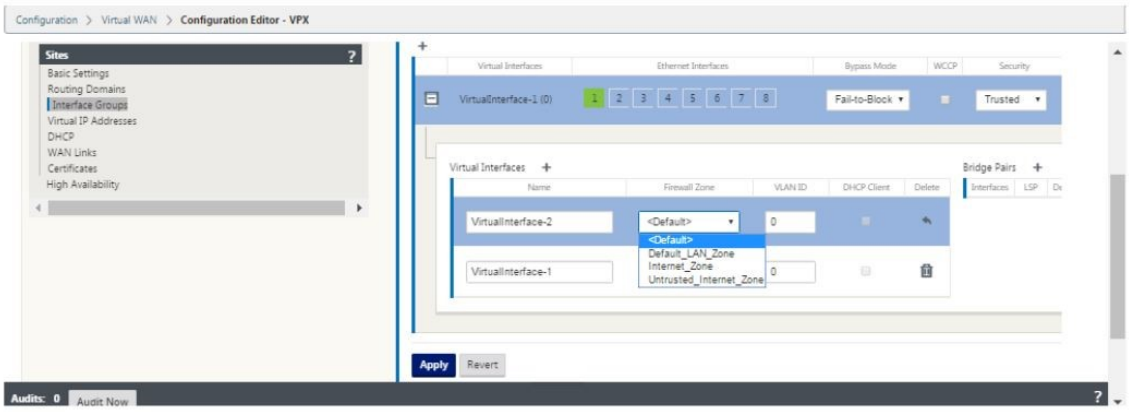


8. Klicken Sie auf +, um virtuelle Schnittstellengruppen hinzuzufügen. Dadurch wird eine neue virtuelle Schnittstellengruppe hinzugefügt. Die Anzahl der virtuellen Schnittstellen hängt von den Links ab, die die Appliance verarbeiten soll. Die Anzahl der Verknüpfungen, die eine Appliance verarbeiten kann, variiert von Einheitenmodell zu Modell, und die maximale Anzahl von Links kann bis zu acht sein.

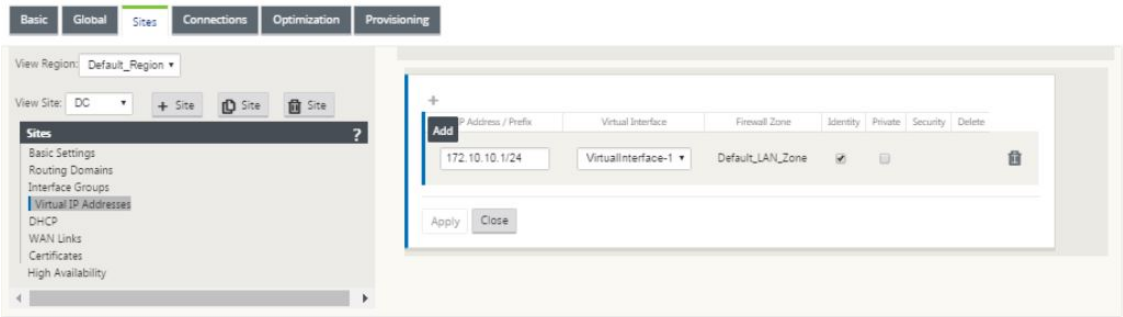
9. Klicken Sie auf + rechts neben virtuellen Schnittstellen, um den Bildschirm wie unten gezeigt anzuzeigen.

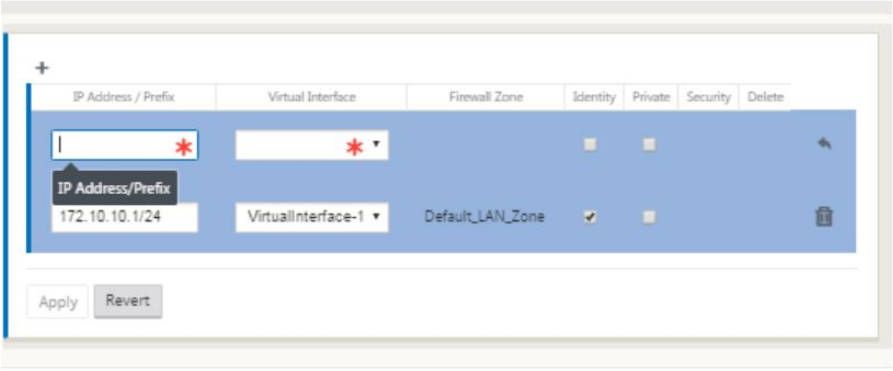


10. Wählen Sie die **Ethernet-Schnittstellen**aus, die den Teil dieser virtuellen Schnittstelle bilden. Abhängig vom Plattformmodell verfügen Appliances über ein vorkonfiguriertes Paar Fail-to-Wire-Schnittstellen. Wenn Sie Fail-to-Wire für Appliances aktivieren möchten, stellen Sie sicher, dass Sie das richtige Schnittstellenpaar auswählen, und stellen Sie sicher, dass Sie in der Spalte **Bypass-Modus** die Option Fail-to-Wire wählen.
11. Wählen Sie die Sicherheitsstufe aus der Dropdownliste aus. Der vertrauenswürdige Modus wird gewählt, wenn die Schnittstelle MPLS-Links bereitstellt und Nicht vertrauenswürdig gewählt wird, wenn Internetlinks auf den jeweiligen Schnittstellen verwendet werden.
12. Klicken Sie auf + rechts neben der Bezeichnung "virtuelle Schnittstellen". Hier werden Name, Firewallzone und VLAN-IDs angezeigt. Geben Sie den **Namen und die VLAN-ID** für diese virtuelle Schnittstellengruppe ein. VLAN-ID dient zum Identifizieren und Markieren von Datenverkehr zu und von der virtuellen Schnittstelle, verwenden Sie 0 (Null) für native/nicht getaggte Datenverkehr.



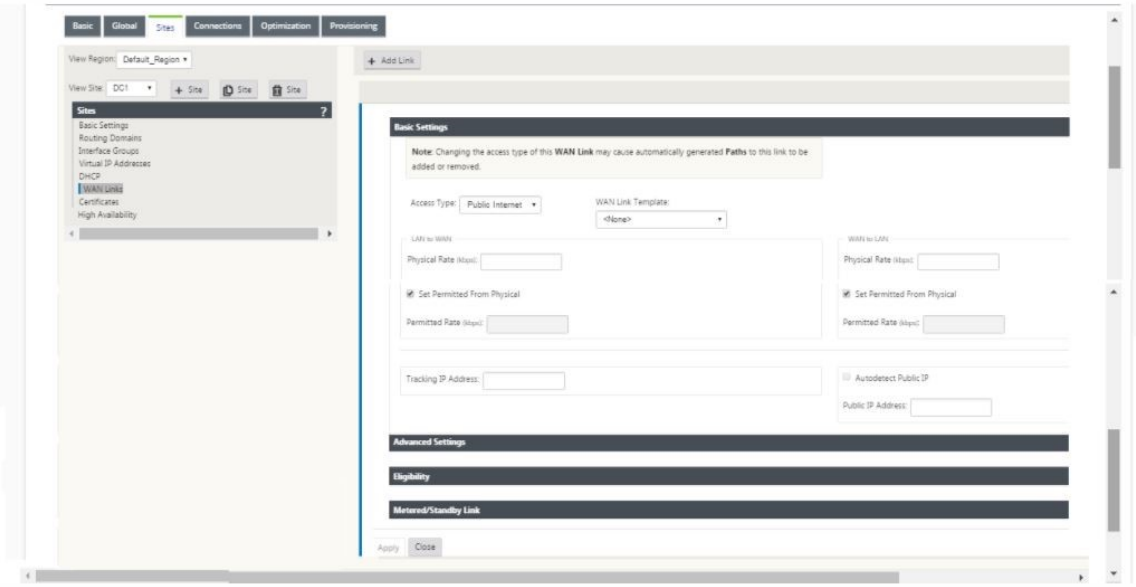
13. Zum Konfigurieren von Schnittstellen ohne Kabel klicken Sie auf "Bridge-Paare". Dies fügt ein neues Bridge-Paar hinzu und ermöglicht die Bearbeitung. Klicken Sie auf **Übernehmen**, um diese Einstellungen zu bestätigen.
14. Um weitere virtuelle Schnittstellengruppen hinzuzufügen, klicken Sie rechts neben dem Zweig der Schnittstellengruppen auf + und fahren Sie wie oben fort.
15. Nachdem die Schnittstellen ausgewählt wurden, besteht der nächste Schritt darin, IP-Adressen auf diesen Schnittstellen zu konfigurieren. In der Citrix SD-WAN-Terminologie wird dies als VIP (Virtual IP) bezeichnet.
16. Fahren Sie in der Siteansicht fort und klicken Sie auf die virtuelle IP-Adresse, um die Schnittstellen zum Konfigurieren von VIP anzuzeigen.



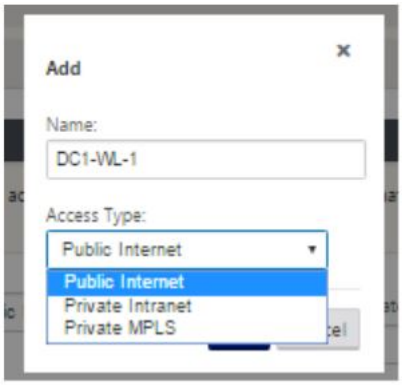


17. Geben Sie die IP-Adresse/Präfix-Informationen ein und wählen Sie die **virtuelle Schnittstelle** aus, mit der die Adresse verknüpft ist. Die virtuelle IP-Adresse muss die vollständige Hostadresse und die Netzmaske enthalten. Wählen Sie die gewünschten Einstellungen für die virtuelle IP-Adresse aus, z. B. die Firewallzone, Identität, Privat und Sicherheit. Klicken Sie auf **Anwenden**. Dadurch werden die Adressinformationen zur Site hinzugefügt und in die Tabelle Virtuelle IP-Adressen der Site aufgenommen. Um weitere virtuelle IP-Adressen hinzuzufügen, klicken Sie rechts neben den Virtuellen IP-Adressen auf +, und fahren Sie wie oben beschrieben fort.

18. Fahren Sie im Abschnitt Standorte fort, um WAN-Links für die Site zu konfigurieren.

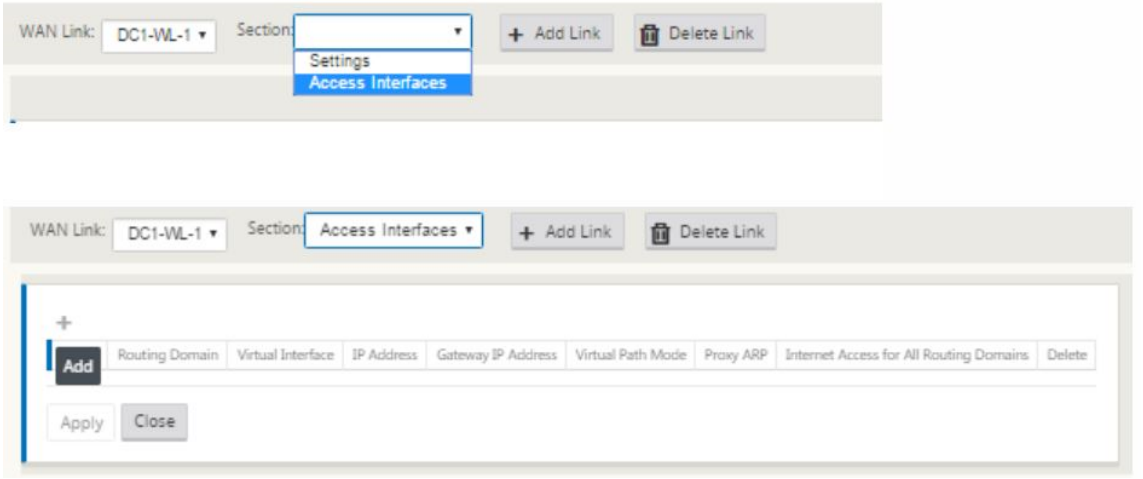


19. Klicken Sie auf **Link hinzufügen**, oben im Bedienfeld auf der rechten Seite. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den zu konfigurierenden Linktyp auswählen können.



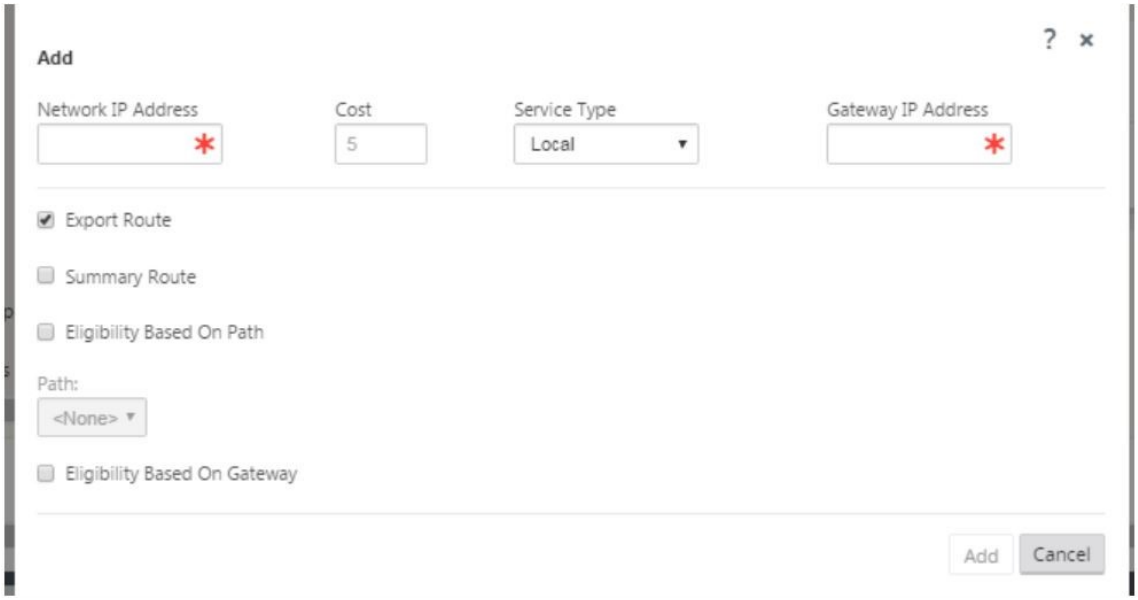
20. Öffentliches Internet ist für Internet/Breitband/DSL/ADSL -Links, während private MPLS für MPLS-Links ist. Private Intranet ist auch für MPLS-Links. Der Unterschied zwischen privaten MPLS und privaten Intranet-Links besteht darin, dass private MPLS die QoS-Richtlinien von MPLS-Links beibehalten kann.

21. Wenn Sie das öffentliche Internet auswählen und die IPs über DHCP zugewiesen werden, wählen Sie die Option IP automatisch erkennen.
22. Wählen Sie **auf der Konfigurationsseite der WAN-Link-Konfiguration die Option Access Interfaces** aus. Dadurch wird die Ansicht Access Interfaces für die Site geöffnet. Fügen Sie die VIP- und Gateway-IP für jeden der Links hinzu und konfigurieren Sie sie wie unten gezeigt.



23. Klicken Sie auf **+**, um eine Schnittstelle hinzuzufügen. Dadurch wird der Tabelle ein leerer Eintrag hinzugefügt und zur Bearbeitung geöffnet.
24. Geben Sie den Namen ein, den Sie dieser Schnittstelle zuweisen möchten. Sie können den Namen basierend auf dem Linktyp und dem Speicherort wählen. Halten Sie die Routingdomäne als Standard bei, wenn Sie keine Netzwerke trennen und der Schnittstelle eine IP zuweisen möchten.
25. Stellen Sie sicher, dass Sie eine öffentlich erreichbare Gateway IP-Adresse angeben, wenn es sich bei dem Link um einen Internetlink oder eine private IP-Adresse handelt, wenn es sich um einen MPLS-Link handelt. Behalten Sie den virtuellen Pfadmodus als primär, da Sie diesen Link benötigen, um einen virtuellen Pfad zu bilden.

    Hinweis: Aktivieren Sie Proxy ARP, wenn die Appliance auf ARP-Anfragen für die Gateway-IP-Adresse antwortet, wenn das Gateway nicht erreichbar ist.
26. Klicken Sie auf **Übernehmen**, um die Konfiguration der WAN-Link abzuschließen. Wenn Sie weitere WAN-Links konfigurieren möchten, wiederholen Sie die Schritte für einen anderen Link.
27. Konfigurieren Sie Routen für die Site. Klicken Sie auf “Verbindungsansicht”und wählen Sie Routen aus.
28. Klicken Sie auf +, um Routen hinzuzufügen, öffnet dies ein Dialogfeld, wie unten gezeigt.



29. Geben Sie die folgenden Informationen für die neue Route zur Verfügung stehen:

    - Netzwerk-IP-Adresse
    - Kosten —Die Kosten bestimmen, welche Route Vorrang vor der anderen hat. Pfade mit niedrigeren Kosten haben Vorrang vor höheren Kosten Routen. Der Standardwert ist fünf.
    - Diensttyp —Wählen Sie den Dienst aus, ein Dienst kann einer der folgenden sein:
        - Virtueller Pfad
        - Intranet
        - Internet
        - Passthrough
        - Lokal
        - GRE Tunnel
        - LAN IPsec-Tunnel

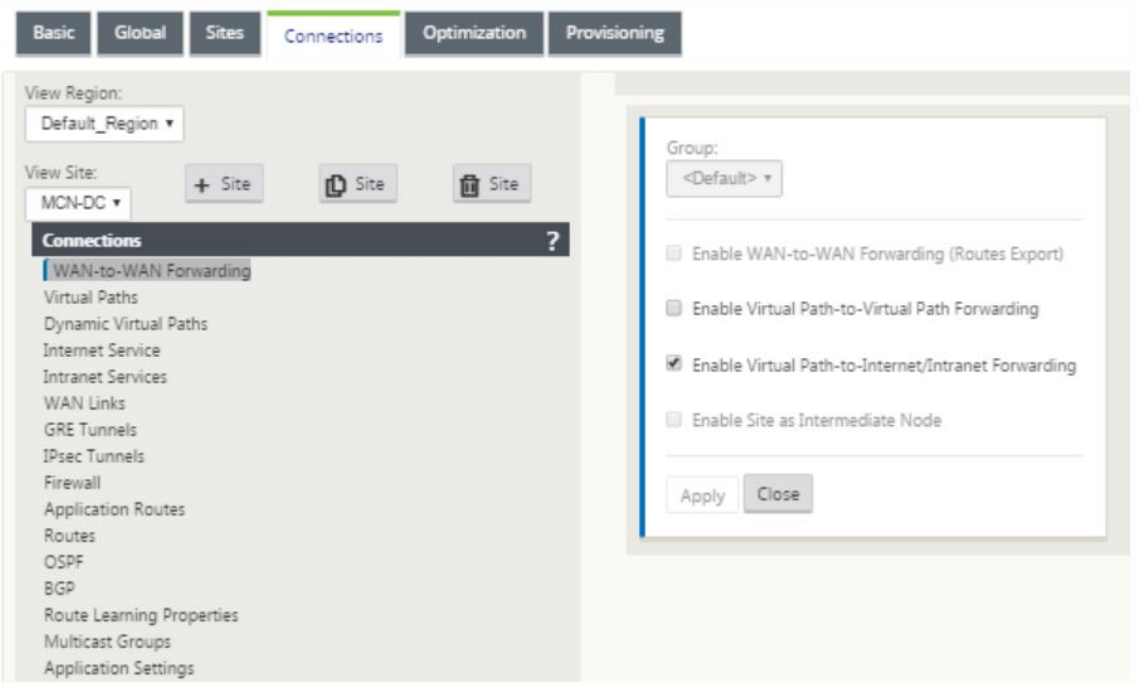
30. Klicken Sie auf **Anwenden**.

Um weitere Routen für die Site hinzuzufügen, klicken Sie auf + rechts neben dem Streckenzweig und fahren Sie wie oben beschrieben fort. Weitere Informationen finden Sie unter MCN konfigurieren.

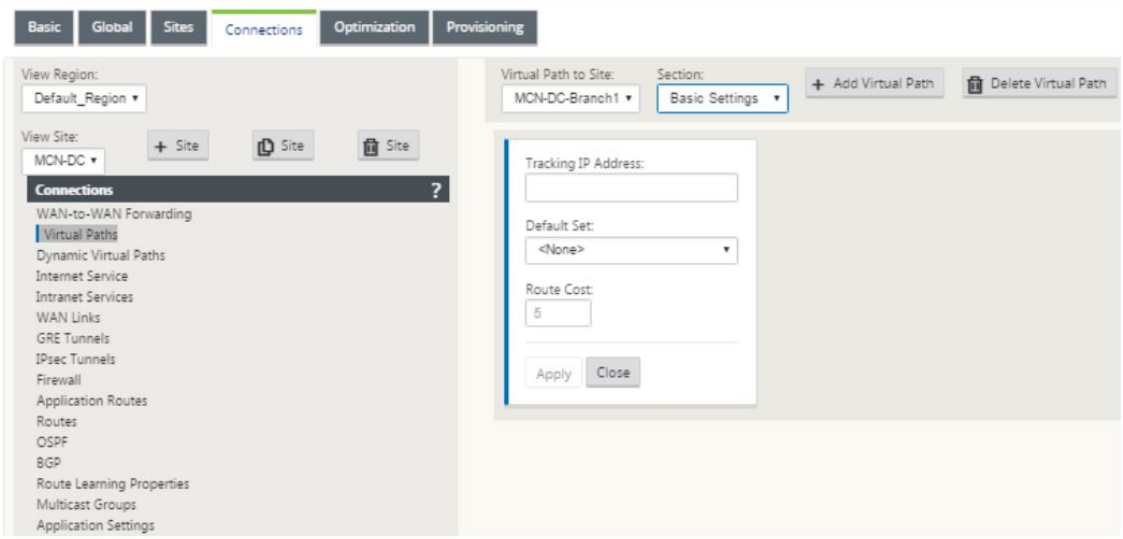
Konfigurieren des virtuellen Pfads zwischen MCN und Zweigstandorten Stellen Sie die Konnektivität zwischen dem MCN und dem Zweigknoten her. Sie können dies tun, indem Sie einen virtuellen Pfad zwischen diesen beiden Sites konfigurieren. Navigieren Sie in der Konfigurationsstruktur des Konfigurationseditors zur Registerkarte **Verbindungen**.

1. Klicken Sie im Konfigurationsabschnitt auf die Registerkarte **Verbindungen**. Daraufhin wird der Abschnitt Verbindungen der Konfigurationsstruktur angezeigt.

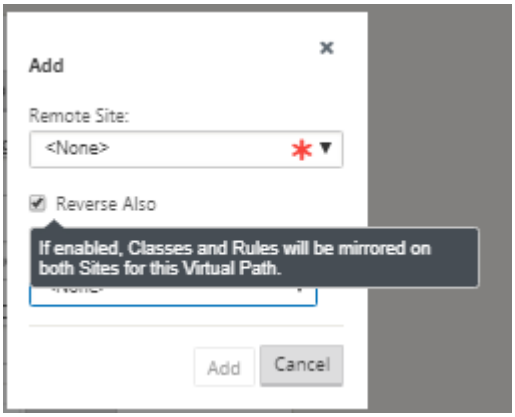
2. Wählen Sie auf der Abschnittseite **Verbindungen** das Dropdownmenü **MCN** aus Ansicht Site aus.



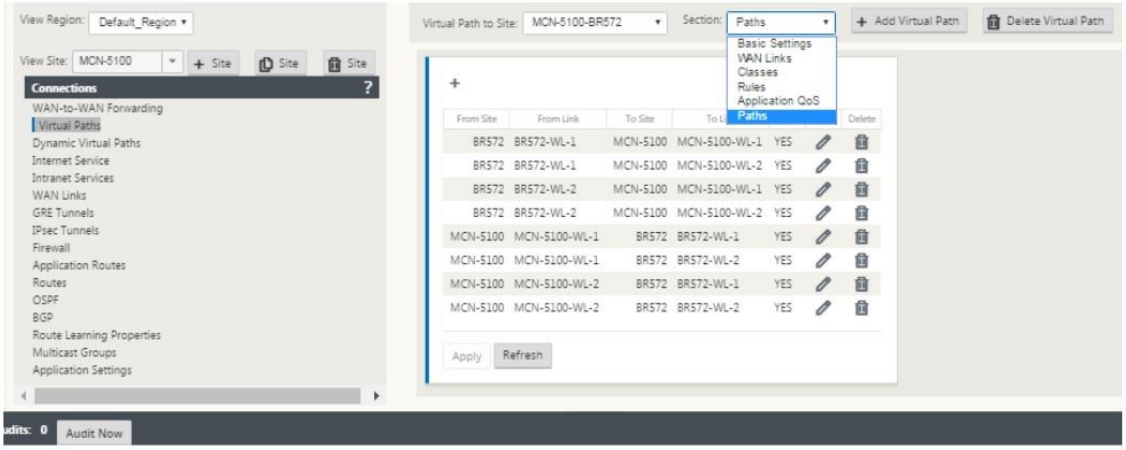
3. Wählen Sie unter der Registerkarte Verbindungen den virtuellen Pfad aus, um einen virtuellen Pfad zwischen den MCN- und Zweigstandorten zu erstellen.



4. Klicken Sie im Abschnitt "**Virtuellen Pfad hinzufügen** "neben dem Namen des statischen virtuellen Pfads auf Virtuellen Pfad. Dies öffnet sich ein Dialogfeld, wie unten gezeigt. Wählen Sie den Zweig aus, für den der virtuelle Pfad konfiguriert werden soll. Sie müssen dies unter der Bezeichnung "remote site"konfigurieren. Wählen Sie den Knoten "Branch"aus dieser Dropdownliste aus und klicken Sie auf das Kontrollkästchen **Reverse Also.**



Verkehrsklassifizierung und Steuerung werden auf beiden Seiten des virtuellen Pfades gespiegelt. Nachdem dies abgeschlossen ist, wählen Sie Pfade aus dem Dropdownmenü unter dem Label namens Abschnitt wie unten gezeigt.



5. Klicken Sie über der Pfadtabelle auf **+ Hinzufügen**, in der das Dialogfeld Pfad hinzufügen angezeigt wird. Geben Sie die Endpunkte an, in denen der virtuelle Pfad konfiguriert werden muss. Klicken Sie nun auf **Hinzufügen**, um den Pfad zu erstellen, und klicken Sie auf **das Kontrollkästchen Umkehren**.

   Hinweis: Citrix SD-WAN misst die Verbindungsqualität in beide Richtungen. Dies bedeutet, dass Punkt A zu Punkt B ein Pfad ist und Punkt B zu Punkt A ein anderer Pfad ist. Mit Hilfe der unidirektionalen Messung der Verbindungsbedingungen kann das SD-WAN die beste Route wählen, um den Verkehr zu senden. Dies unterscheidet sich von Messgrößen wie RTT, bei denen es sich um eine bidirektionale Metrik zur Messung der Latenz handelt. Beispielsweise wird eine Verbindung zwischen Punkt A und Punkt B als zwei Pfade angezeigt, und für jeden von ihnen werden die Verbindungsleistungsmetriken unabhängig berechnet.

Diese Einstellung reicht aus, um die virtuellen Pfade zwischen dem MCN und dem Zweig nach oben zu bringen, weitere Konfigurationsoptionen sind ebenfalls verfügbar. Weitere Informationen finden Sie unter

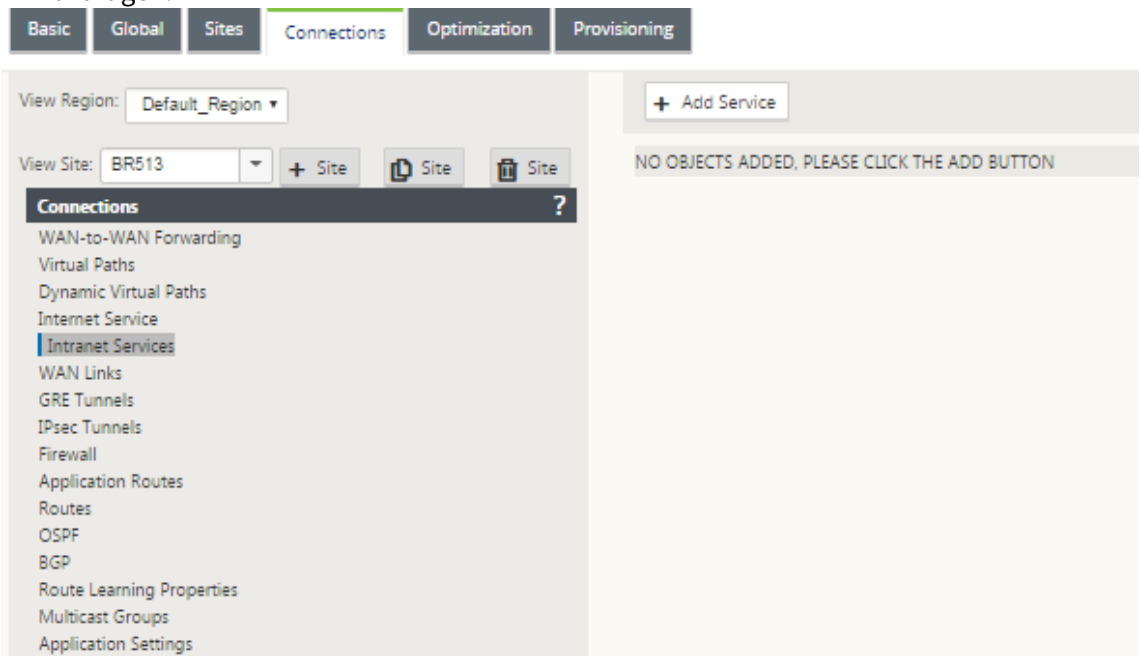
Konfigurieren des virtuellen Pfaddienstes zwischen MCN und Client-Sites.

MCN-Konfiguration bereitstellen Der nächste Schritt besteht darin, die Konfiguration bereitzustellen. Hierbei handelt es sich um die folgenden zwei Schritte:

1. Exportieren Sie das SD-WAN-Konfigurationspaket in Change Management.
    - Bevor Sie die Appliance-Pakete generieren können, müssen Sie zuerst das fertige Konfigurationspaket aus dem **Konfigurationseditor** in den globalen **Change Management-Staging-Posteingang** auf dem MCN exportieren. Beachten Sie die Schritte im Abschnitt Änderungsmanagement durchführen.
2. Generieren und Stage der Appliance-Pakete.
    - Nachdem Sie das neue Konfigurationspaket zum Change Management-Posteingang hinzugefügt haben, können Sie die Appliance-Pakete auf den Zweigstandorten generieren und bereitstellen. Dazu verwenden Sie den Änderungsverwaltungs-Assistenten in der Management-Weboberfläche auf dem MCN. Beziehen Sie sich auf die Schritte im Abschnitt Stage Appliance-Pakete.

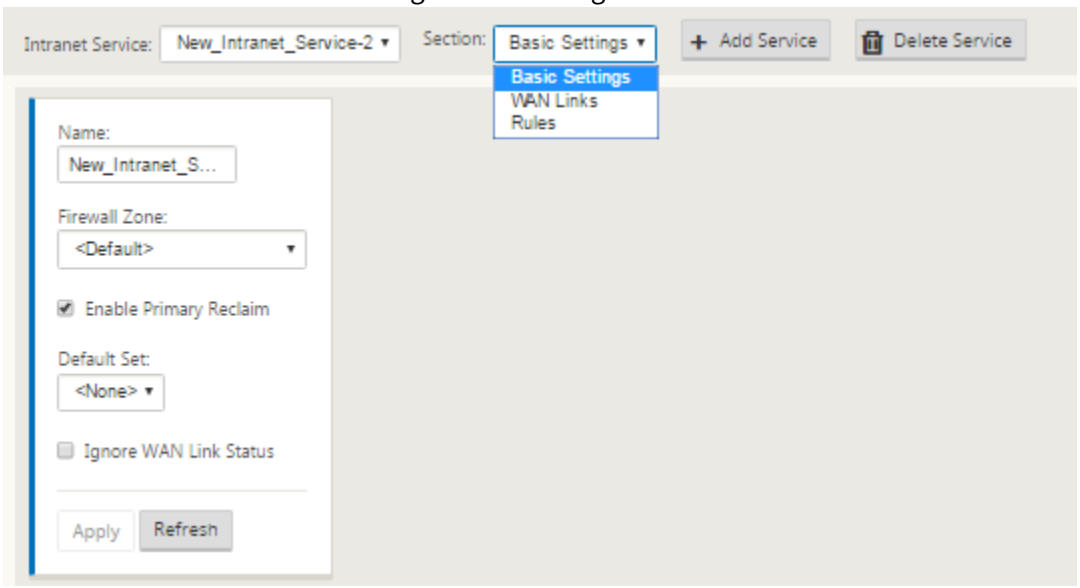
Konfigurieren von Intranetdiensten für die Verbindung mit Azure WAN-Ressourcen

1. Gehen Sie in der SD-WAN-Appliance-GUI zum **Konfigurationseditor**. Navigieren Sie zur Kachel **Verbindungen** . Klicken Sie auf **+ Dienst hinzufügen**, um einen Intranetdienst für diese Site hinzuzufügen.



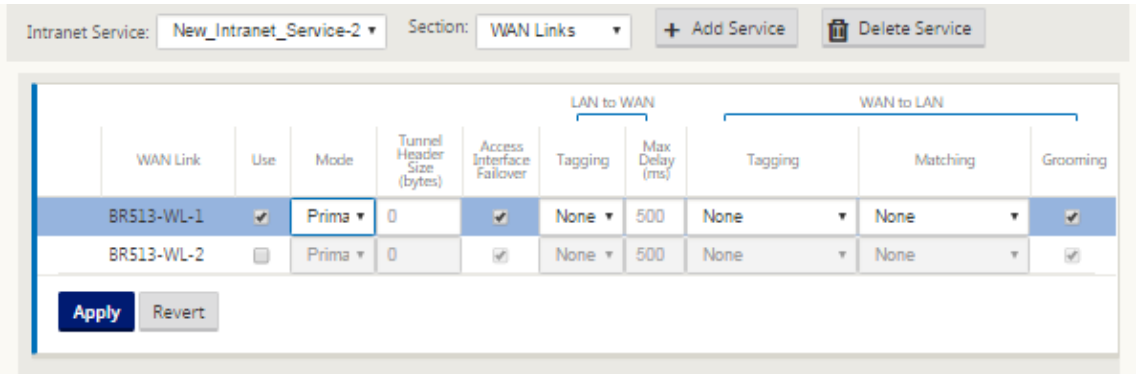
2. In den **Grundeinstellungen** für den Intranetdienst gibt es mehrere Möglichkeiten, wie sich der Intranetdienst während der Nichtverfügbarkeit von WAN-Verbindungen verhalten soll.

   - **Primäre Rückforderung aktivieren** —Aktivieren Sie dieses Kontrollkästchen, wenn der ausgewählte primäre Link nach dem Failover übernommen werden soll. Wenn Sie diese Option jedoch nicht aktivieren, wird der sekundäre Link weiterhin Verkehr senden.
   - **WAN-Link-Status ignorieren** —Wenn diese Option aktiviert ist, verwenden Pakete, die für diesen Intranetdienst bestimmt sind, diesen Dienst auch dann weiterhin, wenn die konstituierenden WAN-Verbindungen nicht verfügbar sind.

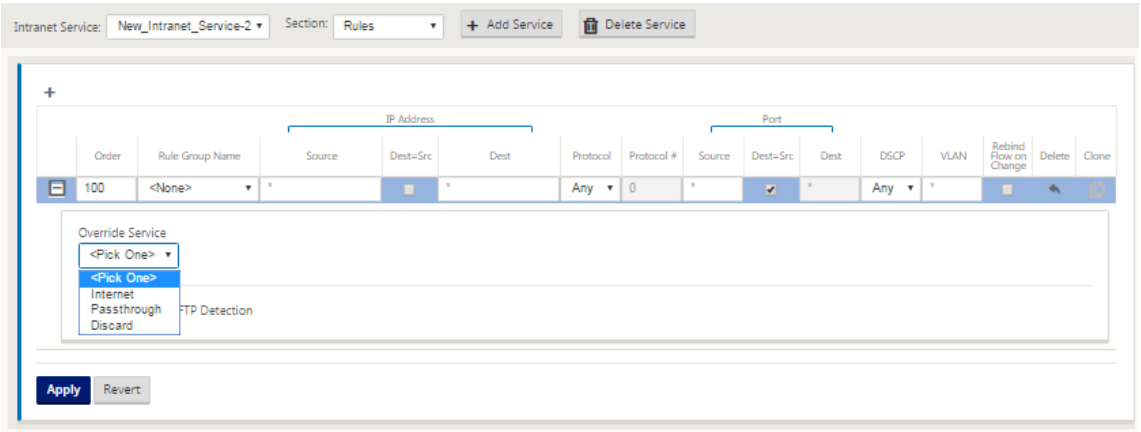


3. Nach der Konfiguration der Grundeinstellungen besteht der nächste Schritt darin, die konstituierenden WAN-Links für diesen Dienst auszuwählen. Maximal zwei Links werden für einen Intranetdienst ausgewählt. Um die WAN-Links auszuwählen, wählen Sie die Option “WAN-Links” aus der Dropdownliste “Section”. Die WAN-Links funktionieren im primären und sekundären Modus und nur eine Verbindung wird als primäre WAN-Verbindung ausgewählt.

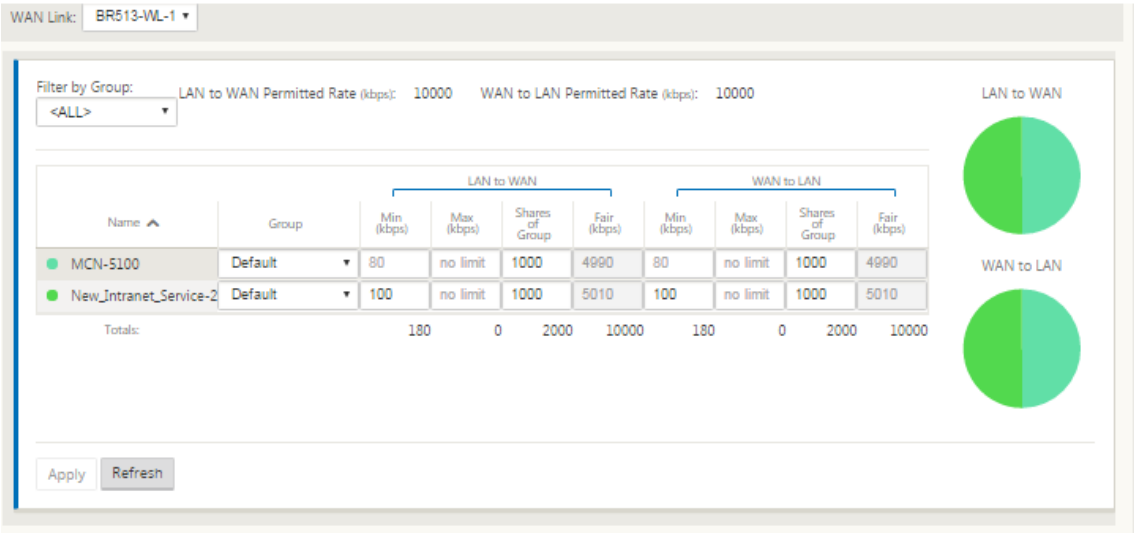
   Hinweis: Wenn ein zweiter Intranetdienst erstellt wird, muss er über die primäre und sekundäre WAN-Link-Zuordnung verfügen.



4. Zweigstandortspezifische Regeln sind verfügbar, die die Anpassung der einzelnen Zweigstandorts ermöglichen, alle allgemeinen Einstellungen, die im globalen Standardsatz konfiguriert sind, eindeutig außer Kraft zu setzen. Modi umfassen die gewünschte Zustellung über eine bestimmte WAN-Verbindung oder als Override-Dienst, der die Durchleitung oder das Verwerfen des gefilterten Datenverkehrs ermöglicht. Wenn beispielsweise Traffic vorhanden ist, den Sie nicht über den Intranetdienst übertragen möchten, können Sie eine Regel schreiben, um diesen Datenverkehr zu verwerfen oder ihn über einen anderen Dienst (Internet oder Durchlauf) zu senden.

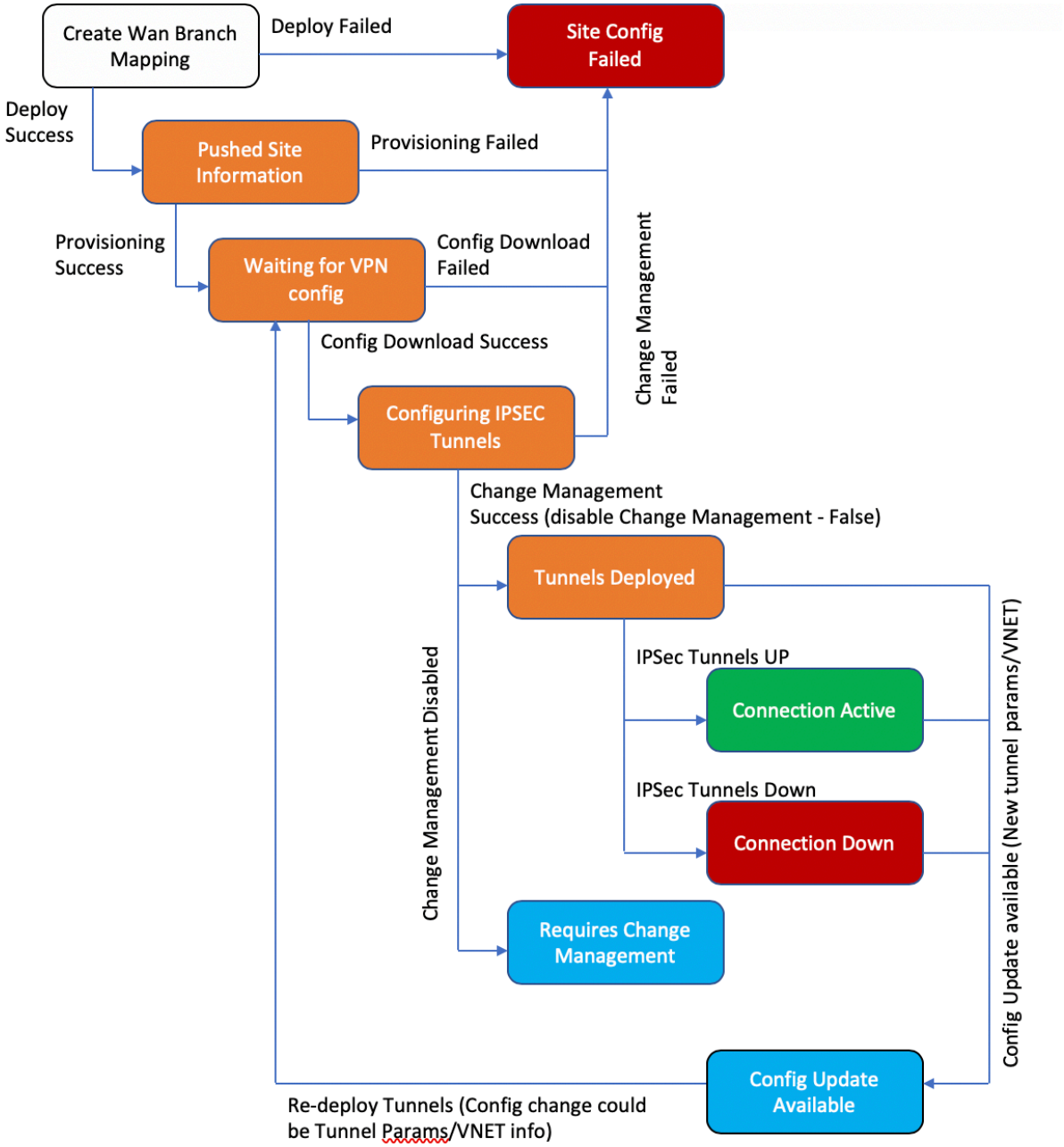


5. Wenn der Intranetdienst für einen Standort aktiviert ist, wird die **Provisioning-Kachel** zur Verfügung gestellt, um die bidirektionale Verteilung der Bandbreite (LAN zu WAN/WAN zu LAN) für eine WAN-Verbindung zwischen den verschiedenen Diensten über die WAN-Verbindung zu ermöglichen. Im Abschnitt "**Dienste** "können Sie die Bandbreitenzuweisung weiter optimieren. Darüber hinaus kann Fair Share aktiviert werden, so dass Services ihre minimale reservierte Bandbreite erhalten können, bevor eine faire Verteilung erfolgt.



SD-WAN Center konfigurieren

Im folgenden Diagramm werden der high-level Workflow des SD-WAN Center und Azure Virtual WAN-Verbindung sowie die entsprechenden Zustandsübergänge der Bereitstellung beschrieben.



Konfigurieren von Azure-Einstellungen:

- Geben Sie Azure Mandanten-ID, Anwendungs-ID, geheimen Schlüssel und Abonnement-ID

(auch Dienstprinzipal genannt) an.

Konfigurieren Sie den Zweigstandort zu WAN-Zuordnung:

- Ordnen Sie einer WAN-Ressource einen Zweigstandort zu. Der gleiche Standort kann nicht mit mehreren WANs verbunden werden.
- Klicken Sie auf **Neu**, um Site-WAN-Zuordnung zu konfigurieren.
- Wählen Sie **Azure WAN-Ressourcen** aus.
- Wählen Sie **Sitenamen** aus, die den WAN-Ressourcen zugeordnet werden sollen.
- Klicken Sie auf **Bereitstellen**, um die Zuordnung zu bestätigen. Die WAN-Verbindungen, die für die Tunnelbereitstellung verwendet werden sollen, werden automatisch mit den für die optimale Verbindungskapazität aufgefüllt.
- Warten Sie, bis der Status zu „Tunnel bereitgestellt“wechselt, um die **IPSec-Tunneleinstellungen** anzuzeigen.
- Verwenden Sie die Ansicht SD-WAN Center Reporting, um den Status der jeweiligen IPSec-Tunnel zu überprüfen. Der IPSec-Tunnelstatus sollte GRÜN sein, damit der Datenverkehr fließt, der besagt, dass die Verbindung aktiv ist.

Bereitstellen von SD-WAN-Center:

SD-WAN-Center ist das Management- und Reporting-Tool für Citrix SD-WAN. Die erforderliche Konfiguration für Virtual WAN wird im SD-WAN Center durchgeführt. SD-WAN Center ist nur als virtueller Formfaktor (VPX) verfügbar und muss auf einem VMware ESXi oder einem XenServer Hypervisor installiert werden. Für die Konfiguration einer SD-WAN-Center-Appliance sind mindestens 8 GB RAM und 4 CPU-Kerne erforderlich. Hier sind die Schritte zum Installieren und Konfigurieren einer SD-WAN-Center-VM.

Konfigurieren von SD-WAN Center für Azure-Konnektivität

Lesen Sie Erstellen Sie einen Service Principal für weitere Informationen.

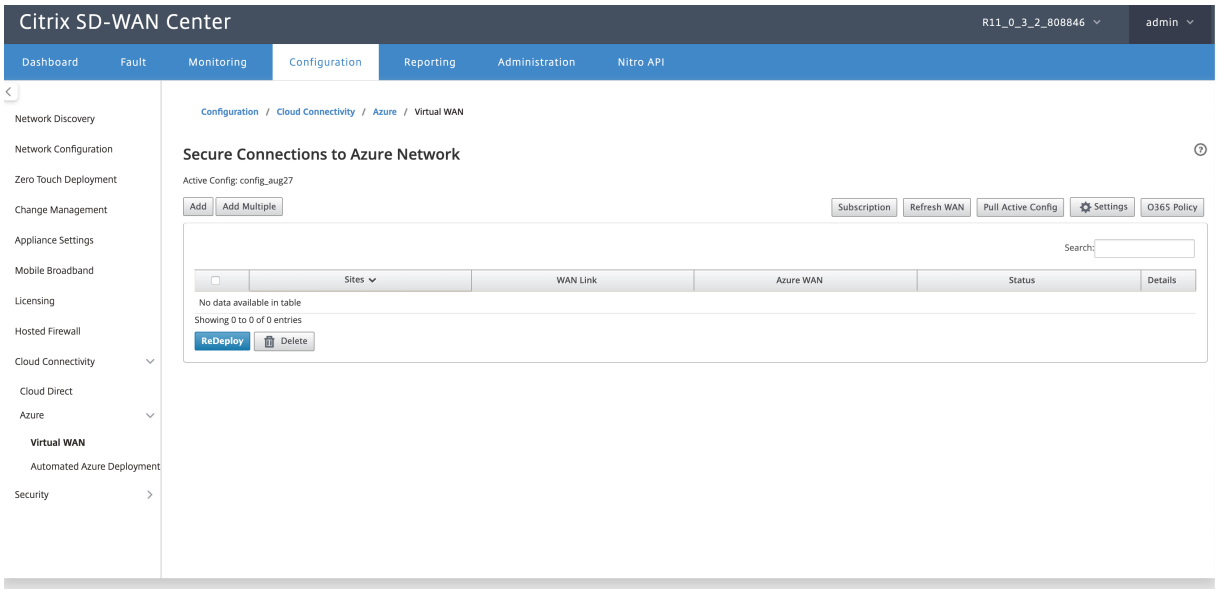
Um SD-WAN-Center mit Azure erfolgreich zu authentifizieren, sollten die folgenden Parameter verfügbar sein:

- Verzeichnis (Mandanten-ID)
- Anwendung (Client-ID)
- Sicherer Schlüssel (Client Secret)
- Teilnehmer-ID

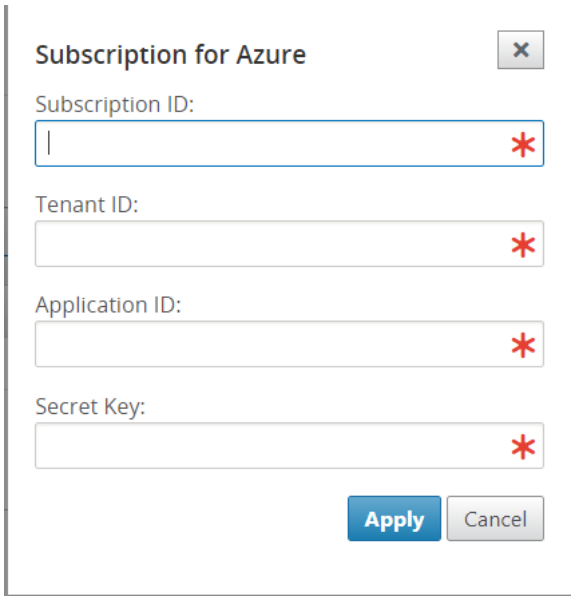
Authentifizieren des SD-WAN-Centers:

Navigieren Sie in der Benutzeroberfläche des SD-WAN Centers zu **Konfiguration** > **Cloud-Konnektivität** > **Azure** > **Virtual WAN**. Konfigurieren Sie Azure-Verbindungseinstellungen. Unter

dem folgenden Link finden Sie weitere Informationen zum Konfigurieren der Azure VPN-Verbindung, Azure Resource Manager.



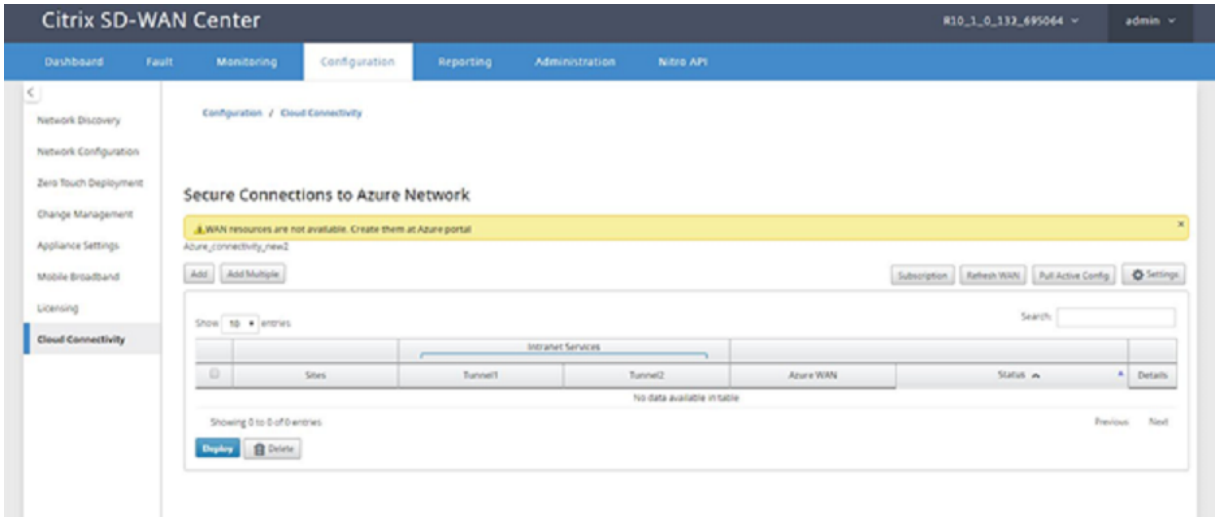
Geben Sie die **Abonnement-ID**, die **Mandanten-ID**, die **Anwendungs-ID** und den **sicheren Schlüssel** ein. Dieser Schritt ist erforderlich, um SD-WAN-Center mit Azure zu authentifizieren. Wenn die oben eingegebenen Anmeldeinformationen nicht korrekt sind, schlägt die Authentifizierung fehl und weitere Aktionen sind nicht zulässig. Klicken Sie auf **Anwenden**.



Das Feld **Speicherkonto** bezieht sich auf das Speicherkonto, das Sie in Azure erstellt haben. Wenn Sie kein Speicherkonto erstellt haben, wird automatisch ein neues Speicherkonto in Ihrem Abonnement erstellt, wenn Sie auf **Übernehmen**klicken.

Erhalten Sie Azure Virtual WAN-Ressourcen:

Nach erfolgreicher Authentifizierung fragt Citrix SD-WAN Azure ab, um eine Liste der Azure Virtual WAN-Ressourcen zu erhalten, die Sie im ersten Schritt nach der Anmeldung beim Azure-Portal erstellt haben. Die WAN-Ressourcen repräsentieren Ihr gesamtes Netzwerk in Azure. Es enthält Links zu allen Hubs, die Sie in diesem WAN haben möchten. WANs sind voneinander isoliert und können keinen gemeinsamen Hub oder Verbindungen zwischen zwei verschiedenen Hubs in verschiedenen WAN-Ressourcen enthalten.



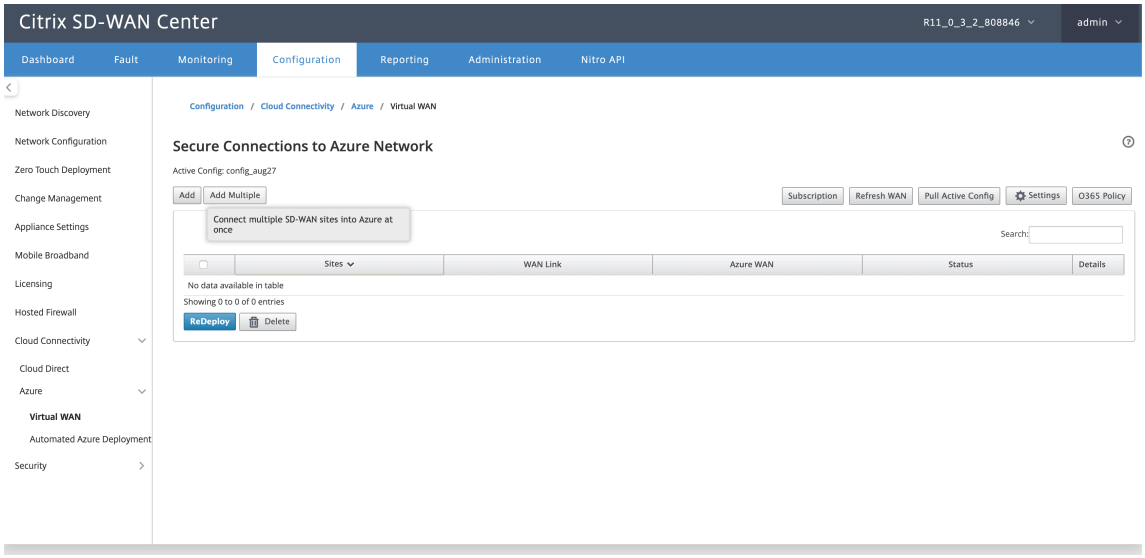
So ordnen Sie Zweigstandorte und Azure WAN-Ressourcen zu:

Ein Zweigstandort muss Azure WAN-Ressourcen zugeordnet werden, um IPsec-Tunnel einzurichten. Ein Zweig kann mit mehreren Hubs innerhalb einer virtuellen Azure-WAN-Ressource verbunden werden, und eine virtuelle Azure-WAN-Ressource kann mit mehreren lokalen Zweigstellen verbunden werden. Erstellen Sie einzelne Zeilen für jeden Zweig der Azure Virtual WAN-Ressourcenbereitstellung.

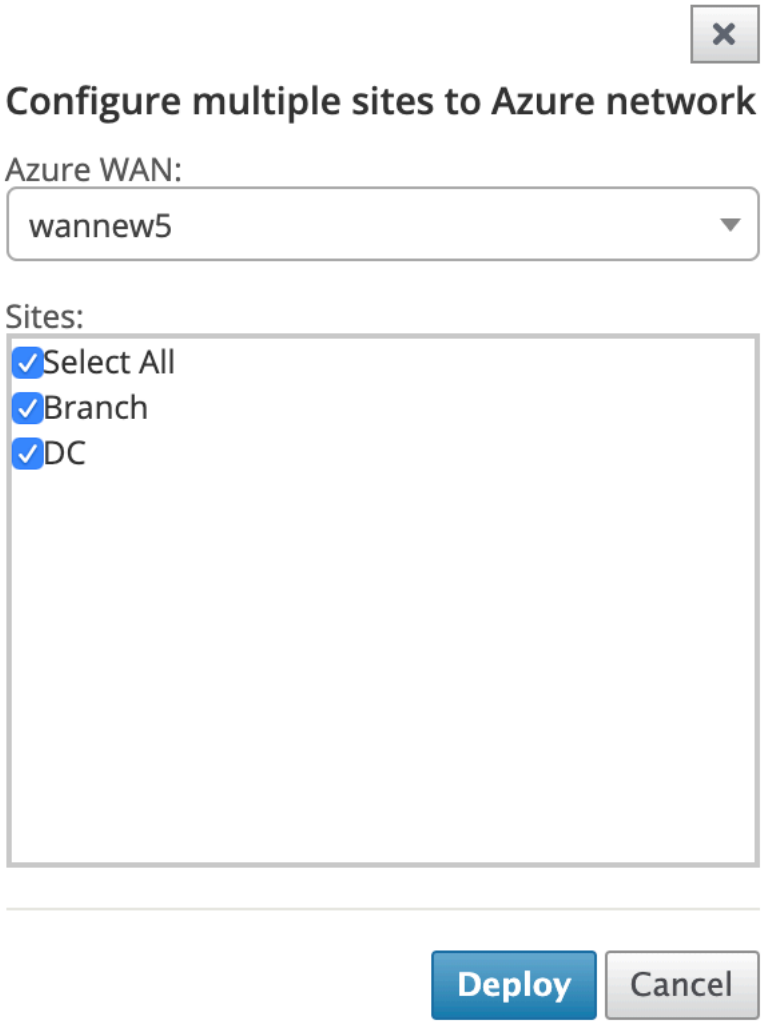
So fügen Sie mehrere Sites hinzu:

Sie können auswählen, dass alle entsprechenden Sites hinzugefügt und mit den ausgewählten einzelnen WAN-Ressourcen verknüpft werden sollen.

1. Klicken Sie auf **“Mehrere hinzufügen”,** um alle Sites hinzuzufügen, die den ausgewählten WAN-Ressourcen zugeordnet werden müssen.



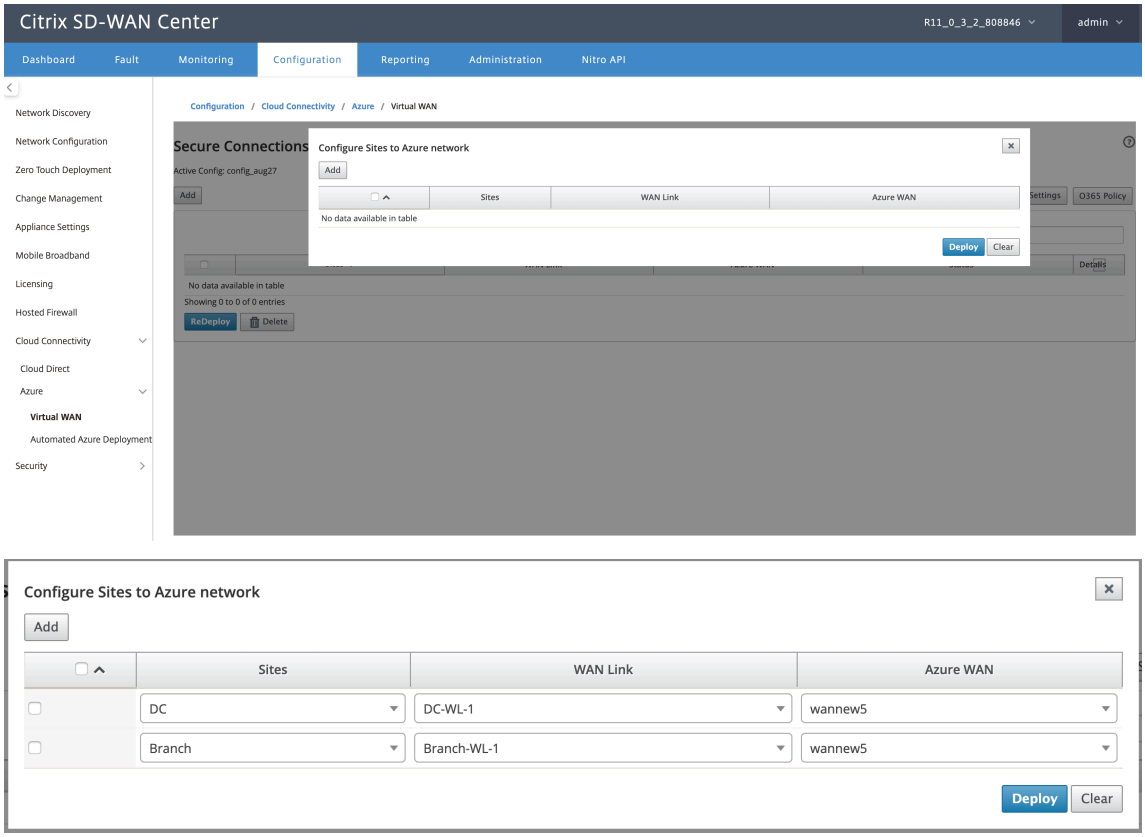
2. Die Dropdownliste Azure WAN-Ressourcen (siehe unten) wird mit den Ressourcen ihres Azure Kontos vorausgefüllt. Wenn keine WAN-Ressourcen erstellt wurden, ist diese Liste leer und Sie müssen zum Azure Portal navigieren, um die Ressourcen zu erstellen. Wenn die Liste mit WAN-Ressourcen gefüllt ist, wählen Sie die **Azure-WAN-Ressource** aus, mit der die Zweigstandorte verbunden werden sollen.
3. Wählen Sie einen oder alle Zweigstandorte aus, um den Prozess der IPSec-Tunneleinrichtung zu initiieren. Die öffentlichen Internet-Wanlinks mit der besten Kapazität der Site werden automatisch ausgewählt, um die IPSec-Tunnel zu den Azure VPN-Gateways einzurichten.



So fügen Sie eine einzelne Site hinzu:

Sie können auch festlegen, dass Sites einzeln (einzeln) hinzugefügt werden und wenn Ihr Netzwerk wächst, oder wenn Sie eine Standort-für-Standort-Bereitstellung durchführen, können Sie mehrere Standorte hinzufügen, wie oben beschrieben.

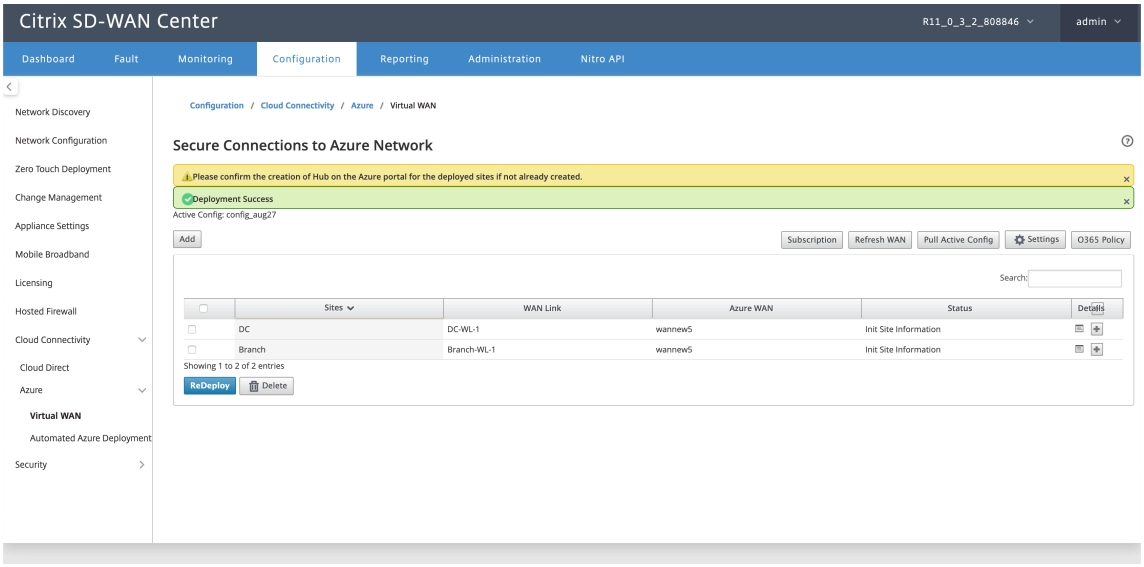
1. Klicken Sie auf **Neuen Eintrag hinzufügen**, um einen Site-Namen für die Site-Wan-Zuordnung auszuwählen. Fügen Sie Sites im Dialogfeld Sites zu **Azure-Netzwerk** konfigurieren hinzu.



2. Wählen Sie den Zweigstandort aus, der für das Azure Virtual WAN-Netzwerk konfiguriert werden soll.
3. Wählen Sie den WAN-Link aus, der mit der Site verknüpft ist (die Links des öffentlichen Internettyps werden in der Reihenfolge der besten physischen Verknüpfungskapazität aufgeführt).
4. Wählen Sie im Dropdownmenü **Azure Virtual WANs** die WAN-Ressource aus, der die Site zugeordnet werden soll.
5. Klicken Sie auf **Bereitstellen**, um die Zuordnung zu bestätigen. Der Status („Init-Site-Informationen „Push-Site-Informationen“und „Warten auf VPN-Konfiguration“) wird aktualisiert, um Sie über den Vorgang zu informieren.

Der Bereitstellungsprozess umfasst den folgenden Status:

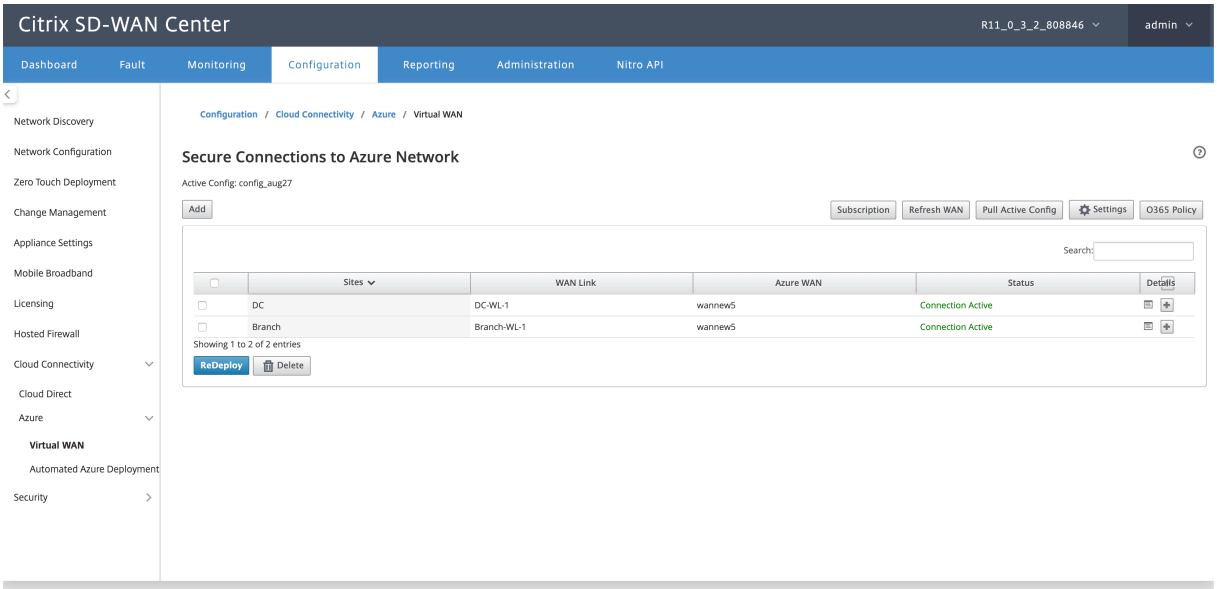
- Push-Site-Informationen
- Warten auf VPN-Konfiguration
- Bereitgestellte Tunnel
- Verbindung aktiv (IPSec-Tunnel ist hochgefahren) oder Verbindung heruntergefahren (IPSec-Tunnel ist heruntergefahren)

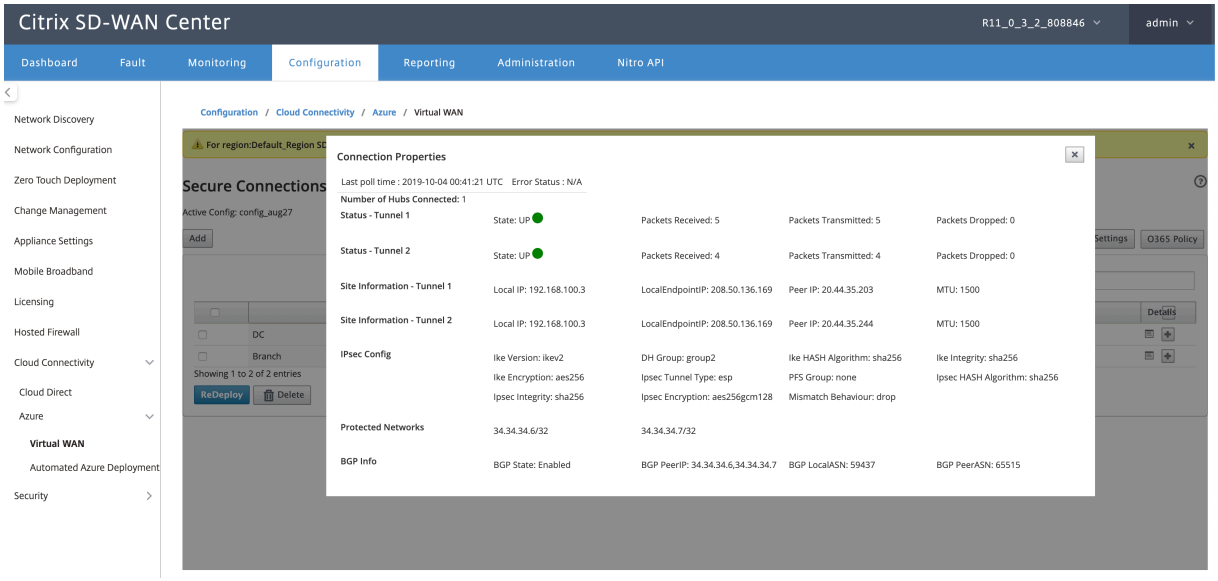


Zuordnungen von Standort-Wan-Ressourcenzuordnungen (Azure-Portal):

Ordnen Sie die bereitgestellten Sites im Azure-Portal den virtuellen Hubs zu, die unter der Azure Virtual WAN-Ressource erstellt wurden. Einem Zweigstandort können ein oder mehrere virtuelle Hubs zugeordnet werden. Jeder virtuelle Hub wird in einer bestimmten Region erstellt, und bestimmte Arbeitslasten können den virtuellen Hubs zugeordnet werden, indem virtuelle Netzwerkverbindungen erstellt werden. Erst nachdem die Zuordnung von Branch Site zu Virtual Hub erfolgreich ist, werden die VPN-Konfigurationen heruntergeladen und die entsprechenden IPsec-Tunnel werden von site zu VPN Gateways erstellt.

Warten Sie, bis der Status in Tunnel Deployed oder Connection Active geändert wurde, um die **IPSec-Tunneleinstellungen** anzuzeigen. Zeigen Sie IPSec-Einstellungen an, die den ausgewählten Diensten zugeordnet sind.

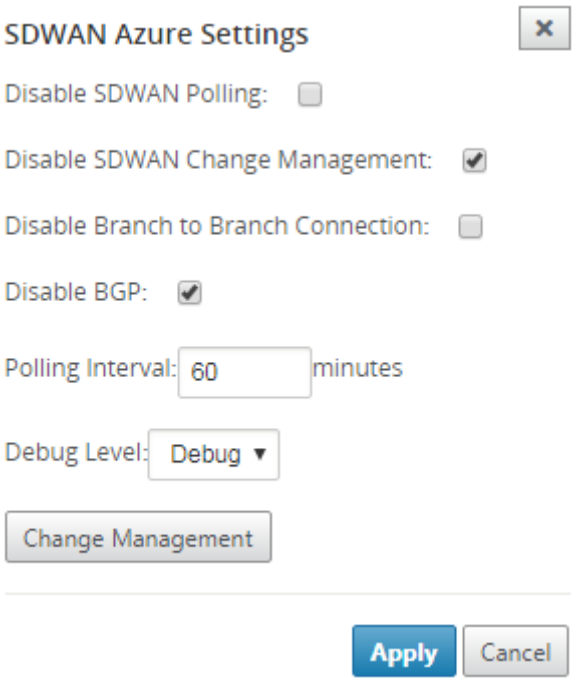




SD-WAN Azure-Einstellungen:

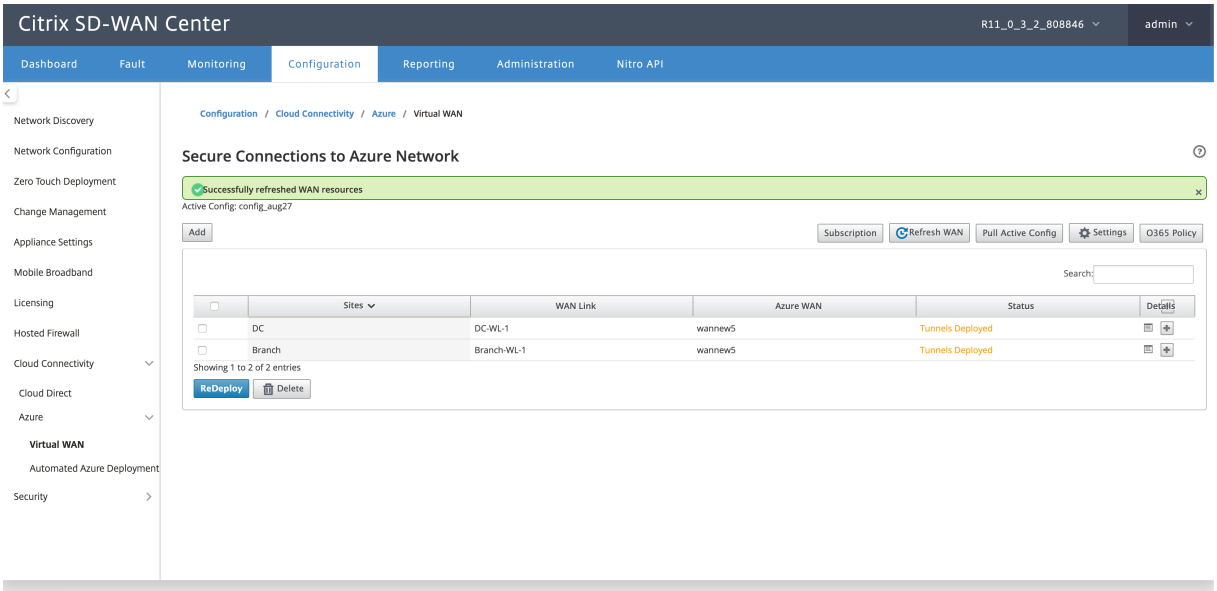
- **Deaktivieren des SD-WAN-Änderungsmanagements** —Standardmäßig wird der Change Management-Prozess automatisiert. Das bedeutet, dass SD-WAN Center jederzeit eine neue Konfiguration in der Azure Virtual WAN-Infrastruktur verfügbar ist, diese abruft und automatisch auf Zweige angewendet wird. Dieses Verhalten wird jedoch gesteuert, wenn Sie steuern möchten, wann eine Konfiguration auf einen Fall angewendet werden muss. Ein Vorteil der Deaktivierung des automatischen Änderungsmanagements besteht darin, dass die Konfiguration für diese Funktion und andere SD-WAN-Funktionen unabhängig voneinander verwaltet wird.
- **SDWAN-Polling deaktivieren**—Deaktiviert alle neuen SD-WAN Azure-Bereitstellungen und Abfragen in vorhandenen Bereitstellungen.
- **Abrufintervall** —Option Abfrageintervall steuert das Intervall für die Suche nach Konfigurationsupdates in der Azure Virtual WAN- Die empfohlene Zeit für das Abfrageintervall beträgt 1 Stunde.
- **Verbindung zwischen Zweig und Zweig deaktivieren** —Deaktiviert die Kommunikation zwischen Zweig und Zweig über Azure Virtual WAN-Infrastruktur. Standardmäßig ist diese Option deaktiviert. Sobald Sie dies aktiviert haben, bedeutet dies, dass lokale Niederlassungen miteinander und mit den Ressourcen hinter den Zweigen über IPSec über Virtual WAN Infra von Azure kommunizieren können. Dies hat keine Auswirkung auf die Branch-to-Branch-Kommunikation über den virtuellen SD-WAN-Pfad, Zweige können miteinander und ihre jeweiligen Ressourcen/Endpunkte über den virtuellen Pfad kommunizieren, selbst wenn diese Option deaktiviert ist.
- **BGP deaktivieren** —Dies deaktiviert BGP over IP, standardmäßig ist es deaktiviert. Nach der Aktivierung werden die Standortrouten über BGP angekündigt.

- **Debug-Ebene** —Ermöglicht das Erfassen von Protokollen, um bei Verbindungsproblemen zu debuggen.

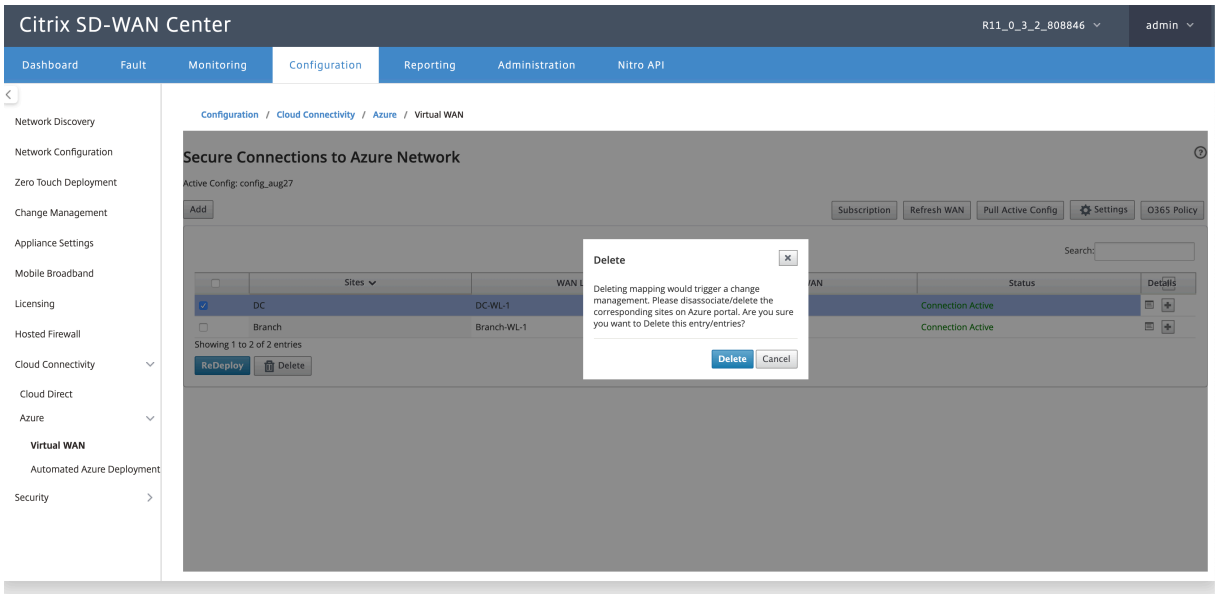


WAN-Ressourcen aktualisieren:

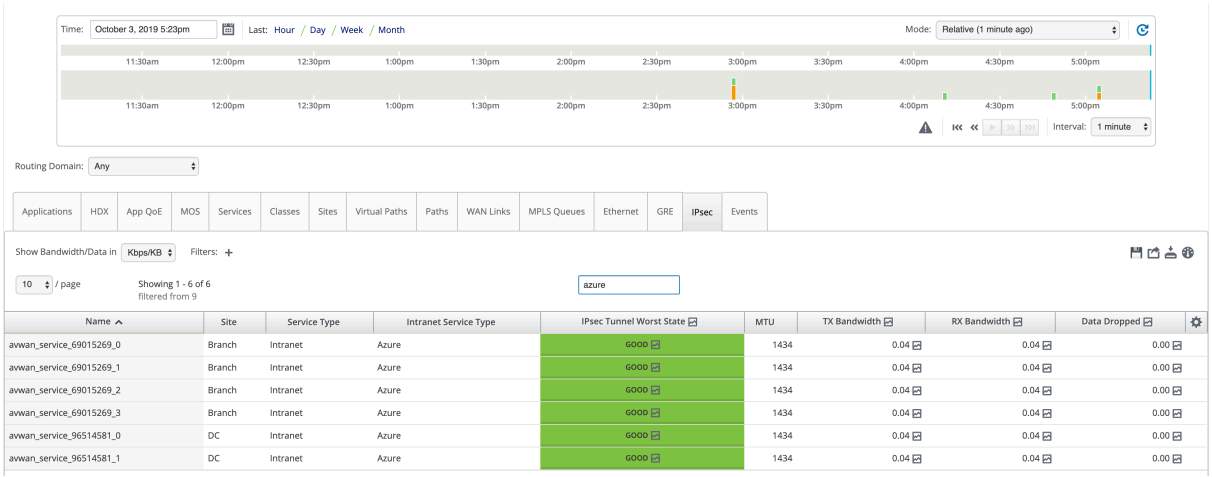
Klicken Sie auf das Symbol **Aktualisieren**, um die neuesten WAN-Ressourcen abzurufen, die Sie im Azure-Portal aktualisiert haben. Nach Abschluss des Aktualisierungsvorgangs wird eine Meldung angezeigt, dass die WAN-Ressourcen erfolgreich aktualisiert wurden.



Standort-WAN-Ressourcenzuordnung entfernen Wählen Sie eine oder mehrere Zuordnungen aus, um das Löschen durchzuführen. Intern wird der Änderungsverwaltungsprozess der SD-WAN-Appliance ausgelöst, und bis er erfolgreich ist, ist die Option Löschen deaktiviert, um zu verhindern, dass weitere Löschungen durchgeführt werden. Zum Löschen der Zuordnung müssen Sie die Zuordnung der entsprechenden Sites im Azure-Portal aufheben oder löschen. Der Benutzer muss diesen Vorgang manuell ausführen.



Überwachung von IPsec-Tunneln Navigieren Sie in der Benutzeroberfläche des SD-WAN Centers zu **Reporting** > **IPsec**, um den Status von IPSec-Tunneln zu überprüfen. Der Tunnelstatus sollte GRÜN sein, damit der Datenverkehr fließen kann.



Cloud Direct Service

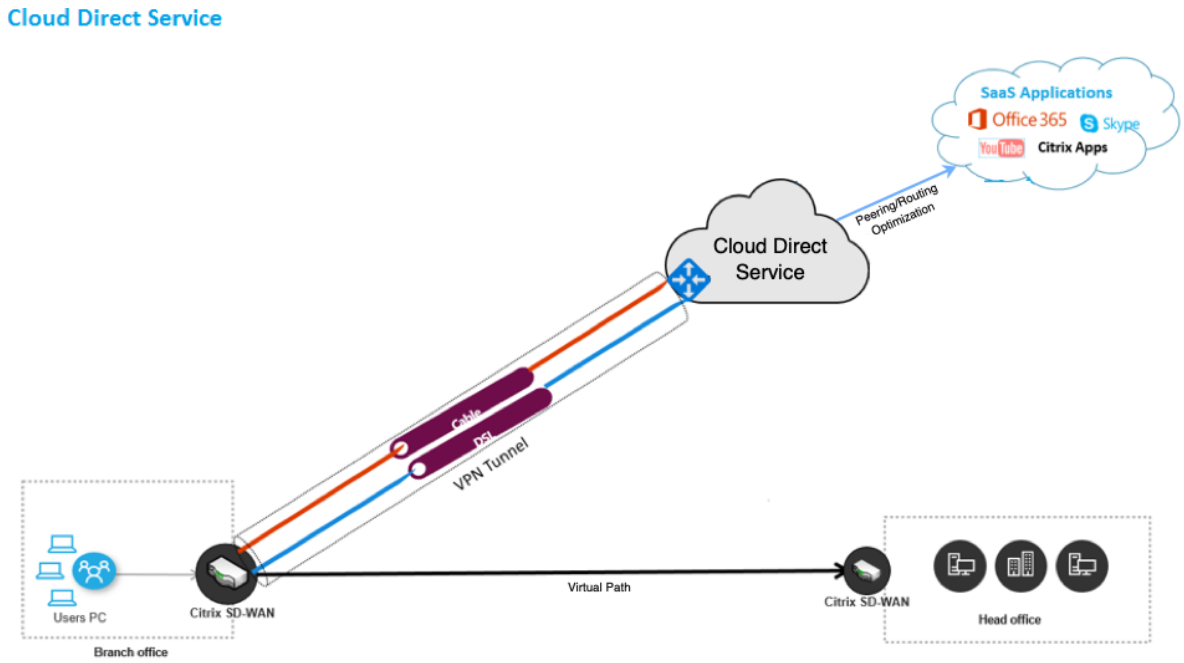
April 13, 2021

Der Cloud Direct-Dienst bietet SD-WAN-Funktionen als Cloud-Service durch zuverlässige und sichere Bereitstellung für den gesamten internetbasierten Datenverkehr unabhängig von der Hostumgebung (Rechenzentrum, Cloud und Internet). Es verbessert die Netzwerksichtbarkeit und -verwaltung. Damit können Partner ihren Endkunden verwaltete SD-WAN-Services für geschäftskritische SaaS-Anwendungen anbieten.

Cloud Direct Service bietet folgende Vorteile:

- Redundanz: Verwendet mehrere Internet-WAN-Verbindungen und ermöglicht ein nahtloses Failover.
- Link-Aggregation - Verwendet alle Internet-WAN-Links gleichzeitig.
- Intelligenter Lastausgleich über WAN-Verbindungen verschiedener Anbieter:
  - Messung von Paketverlust, Jitter und Durchsatz.
  - Benutzerdefinierte Anwendungsidentifikation.
  - Anwendungsanforderungen und Schaltungsleistungsabgleich (Anpassung an Echtzeit-Netzwerkbedingungen).
- SLA-Grade Dynamic QoS-Fähigkeit zur Internetschaltung:
  - Passt sich dynamisch an den variierenden Kreisdurchsatz an.
  - Anpassung durch Tunnel an Ein- und Ausgangsendpunkten.
- Umleiten von VOIP-Anrufen zwischen Schaltungen, ohne den Anruf zu löschen.
- End-to-End-Überwachung und Sichtbarkeit.

Cloud Direct Service Workflow



Bevor Sie mit der Bereitstellung des Cloud Direct Service beginnen, stellen Sie sicher, dass die folgenden Schritte abgeschlossen sind:

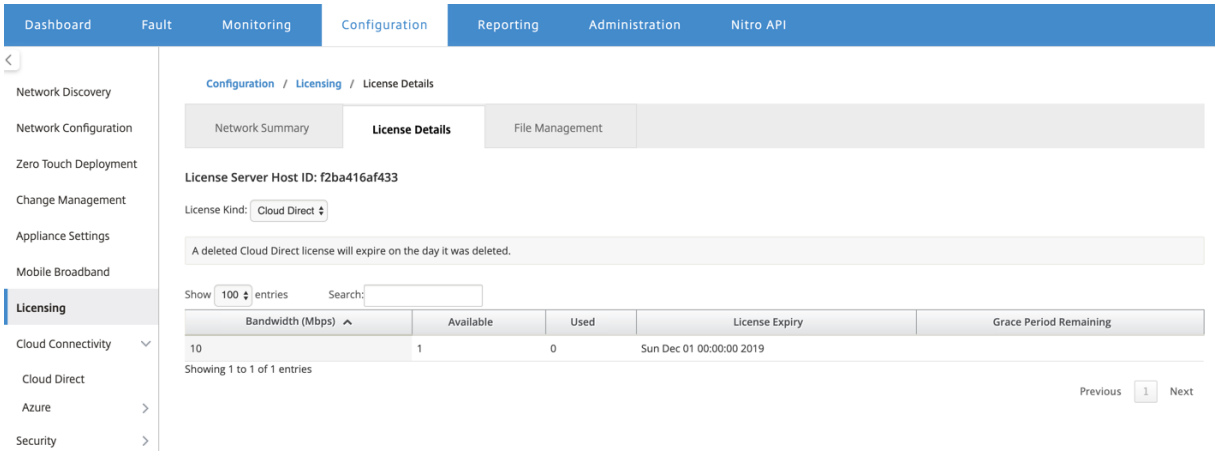
1. Sie verfügen über eine 410-SE, 210-SE oder 1100-SE/PE Edition. Wenn die werkseitig ausgelieferte SD-WAN-Version der Appliance älter als 9.3.5 ist, müssen Sie das USB-Reimaging Verfahren ausführen, um die Appliance auf das neueste Versandbasis-Image zu aktualisieren.
2. Führen Sie eine Upgrade in einem Schritt-Prozedur aus, um die Softwareversion zu installieren, die Cloud Direct Service unterstützt.
3. Konfigurieren Sie die MCN-Appliance und richten Sie die virtuellen Pfade mit ihren Zweigen ein:
    - Konfigurieren Sie den Zweigstandort. Weitere Informationen finden Sie unter Zweig konfigurieren.
    - Erstellen Sie Anwendungsobjekte für anwendungsbasierte Routen.
        - Wenn Sie beabsichtigen, die Anwendungen selektiv über den Cloud-Direktdienst zu steuern, erstellen Sie die Anwendungsobjekte, indem Sie die entsprechenden Anwendungen einschließen (siehe Erstellen: Anwendungsobjekte), die über den Cloud Direct Service. Um den internetgebundenen Datenverkehr zu verwalten, muss der Internetdienst über den Appliance-Konfigurationseditor erstellt werden. Weitere Informationen finden Sie unter Internet Service.
        - Wenn Sie beabsichtigen, den gesamten internetgebundenen Datenverkehr über den

Citrix Cloud-Direktdienst zu steuern, können Sie die Erstellung der spezifischen Anwendungsobjekte überspringen.

Lizenzierung

Cloud Direct Service Funktion wird unabhängig von den Basislizenzen von SD-WAN lizenziert. Stellen Sie sicher, dass Sie die erforderlichen Lizenzen für den Cloud Direct-Dienst im SD-WAN Center installiert haben. Weitere Informationen finden Sie unter Citrix SD-WAN Center als Lizenzserver.sd-wan-center-as-license-server.

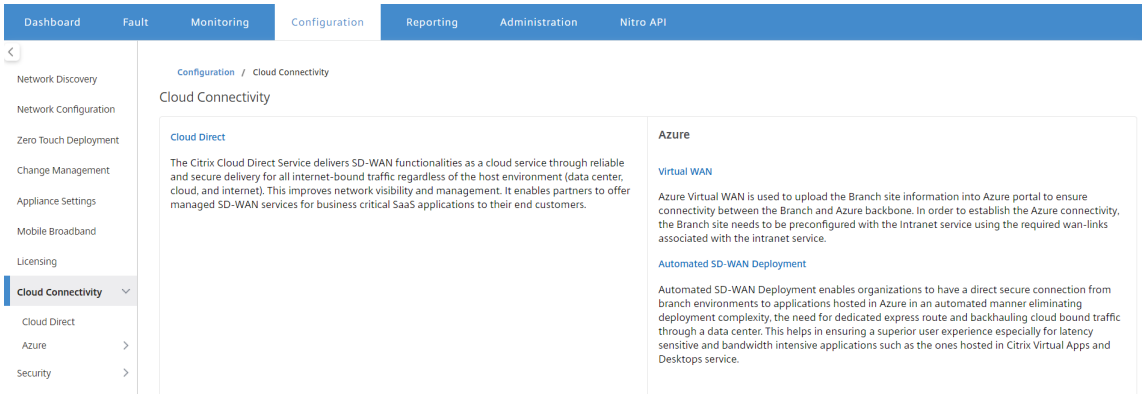
Die Seite Lizenzierung enthält Details zu den installierten Cloud Direct-Dienstlizenzinformationen.



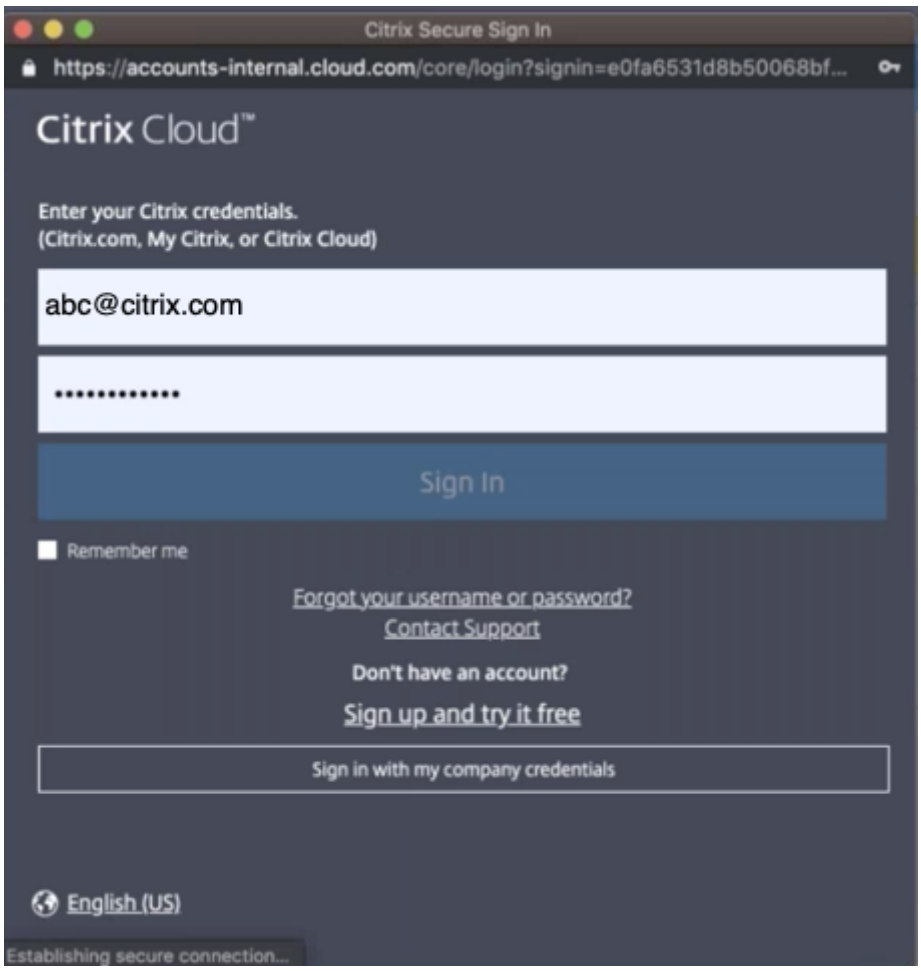
> **Hinweis:**
> Für die abgelaufenen oder gelöschten Cloud Direct-Lizenzen gibt es eine Nachfrist von 30 Tagen, vor der Sie die gültigen Lizenzen installieren müssen, damit die bereitgestellten Cloud Direct-Sites funktionsfähig sind. Wenn vor Ablauf des Grace-Zeitraums keine gültigen Lizenzen installiert werden, deaktiviert SD-WAN Center den Cloud Direct-Dienst vor Ort unter Verwendung der abgelaufenen Lizenz.

Konfigurieren des Cloud-Direktdiensts im SD-WAN Center

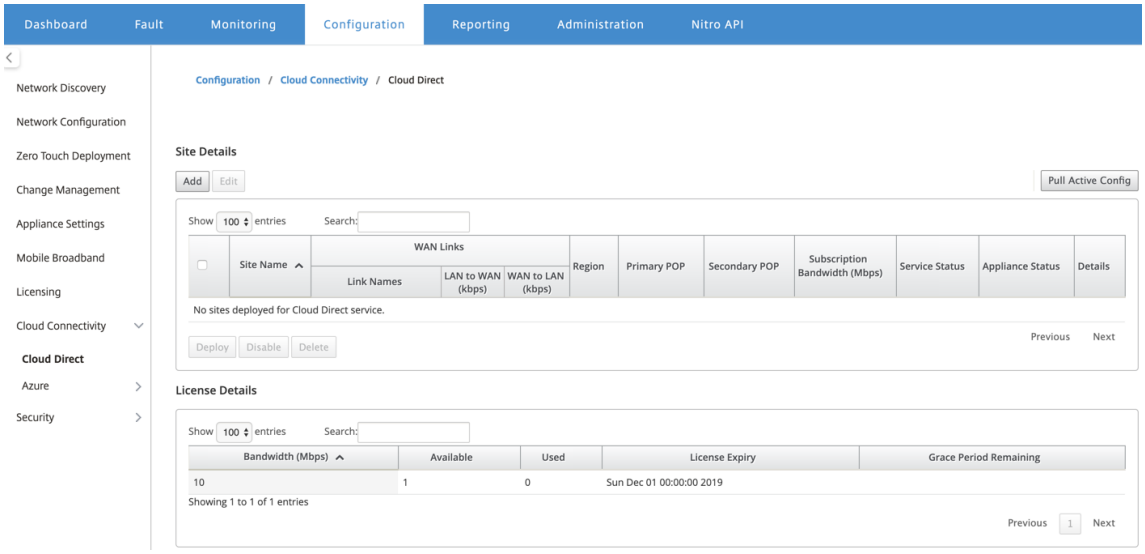
1. Navigieren Sie in der Benutzeroberfläche des SD-WAN Centers zu **Konfiguration** > **Cloud-Konnektivität** > **Cloud Direct**.



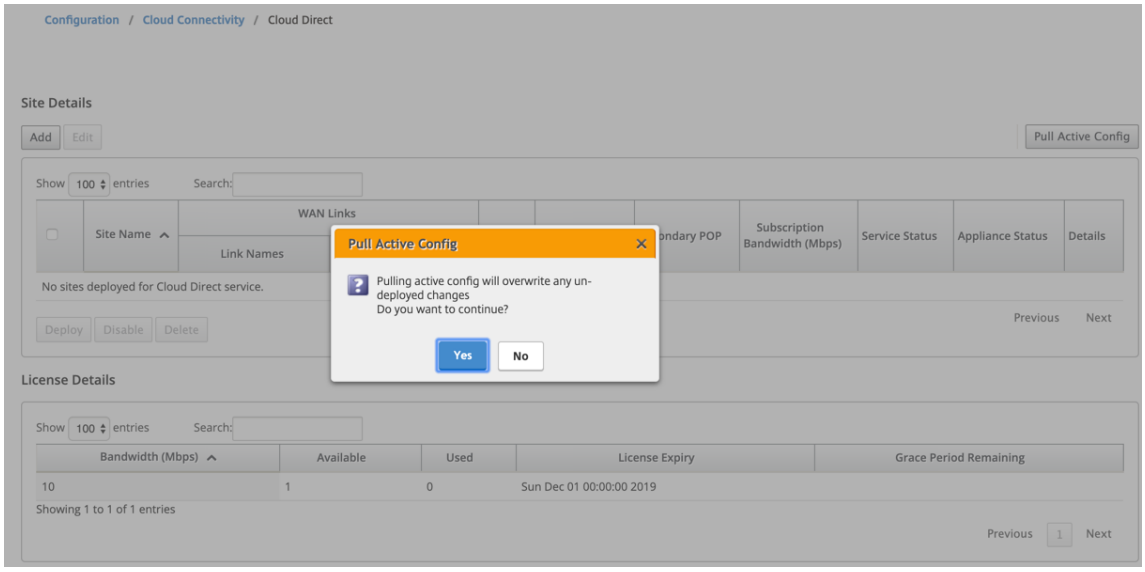
2. Melden Sie sich mit den Citrix Cloud-Anmeldeinformationen an.



Die Cloud Direct-Homepage wird angezeigt, nachdem Sie sich erfolgreich beim Citrix Cloud Service angemeldet haben.

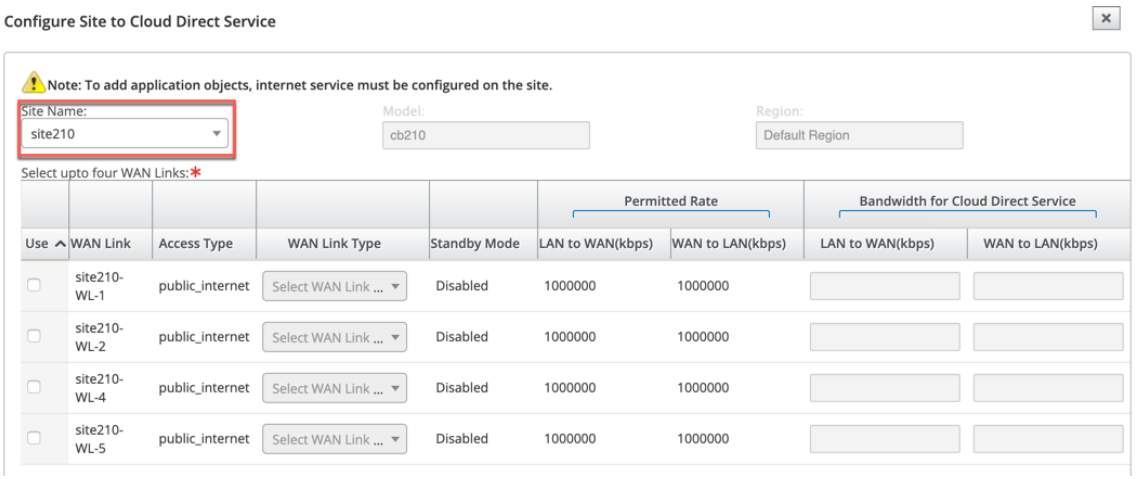


3. Klicken Sie auf **Aktive Konfiguration** abrufen, um die neueste aktive MCN-Konfiguration abzurufen.



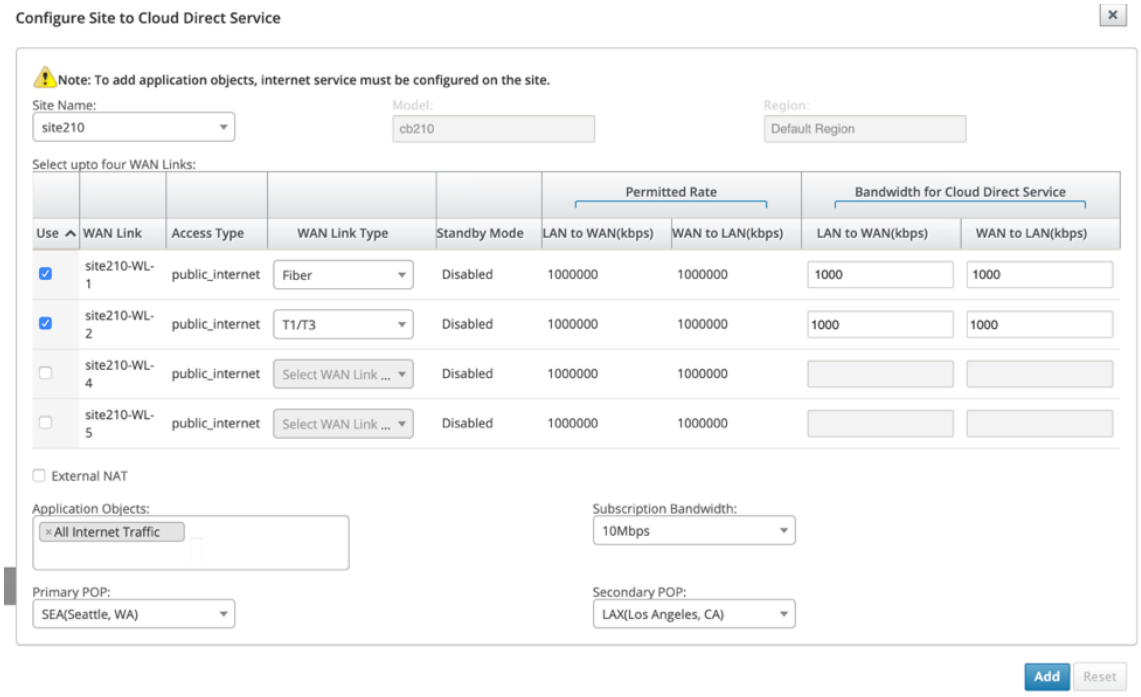
4. Klicken Sie auf **Neue Site hinzufügen**. Sites, die für die Bereitstellung des Cloud Direct-Dienstes in Frage kommen, werden im Menü angezeigt.

> **Hinweis:**
> Die Cloud Direct-Dienstfunktion wird auf Hardware-Appliances 210, 410 und 1100 unterstützt.



5. Wenn ein Standort ausgewählt wird, werden die öffentlichen Internet-WAN-Verbindungen angezeigt, die dem ausgewählten Standort zugeordnet sind, zusammen mit den Appliance-Modellinformationen und der Region, in der die Appliance bereitgestellt wird.
6. Wählen Sie die WAN-Links aus, die Sie für den Cloud Direct-Dienst verwenden möchten, zusammen mit den Optionen **WAN-Link-Typ**, **Anwendungsobjekte**, **Abonnementbandbreite**, **primärer POP** und **sekundärer POP**.

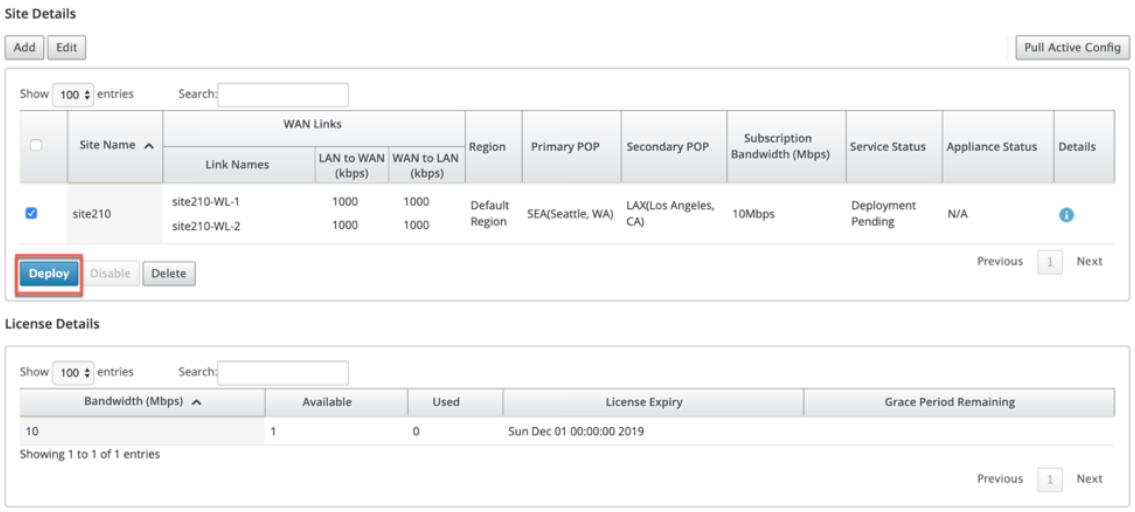
> **Hinweis**
>
> Bis zu vier WAN-Verbindungen werden für den Cloud Direct-Dienst unterstützt.



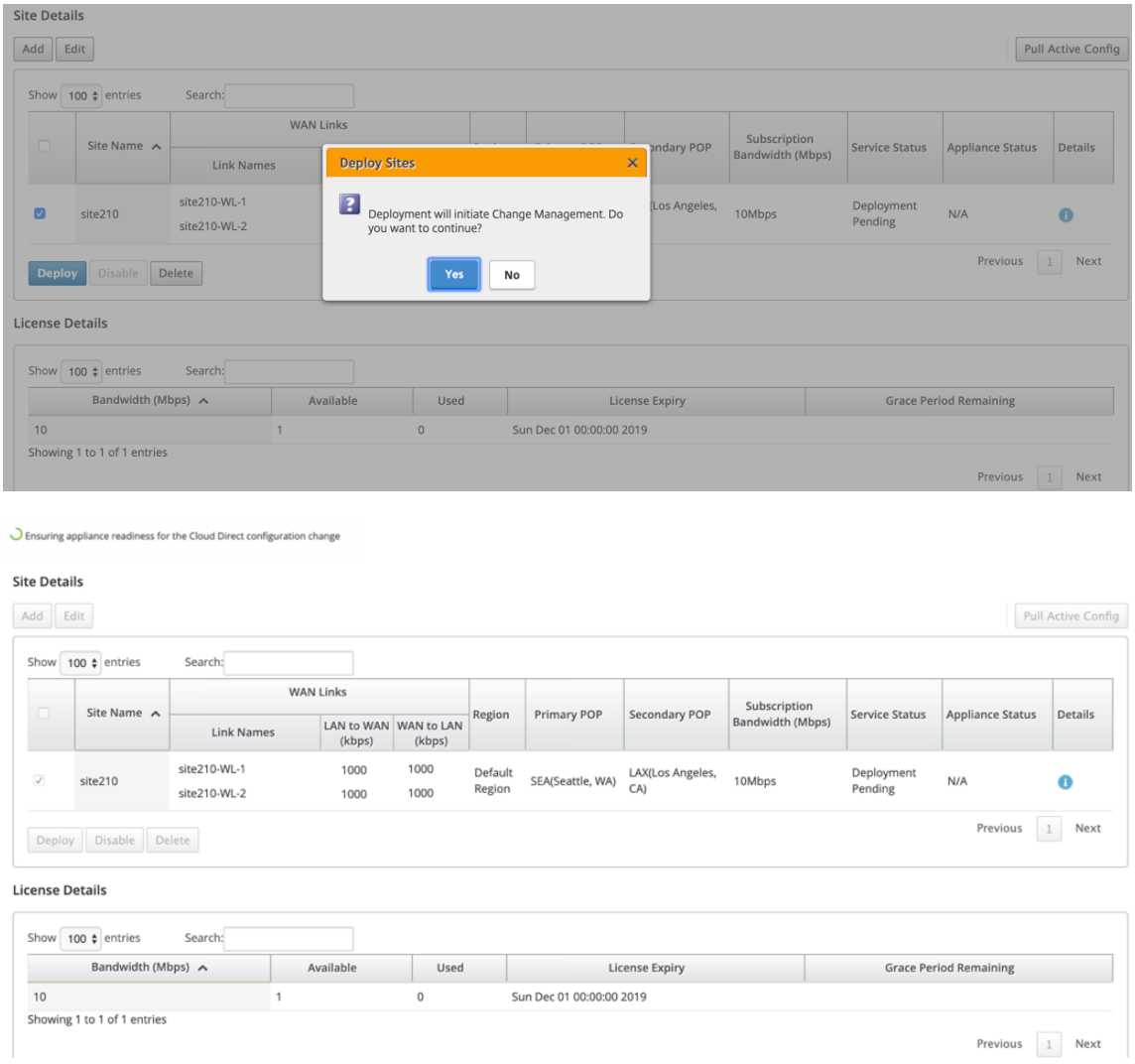
- **Site-Name**: Zeigt die Sites an, die für die Bereitstellung der Cloud Direct-Funktion in Frage kommen.

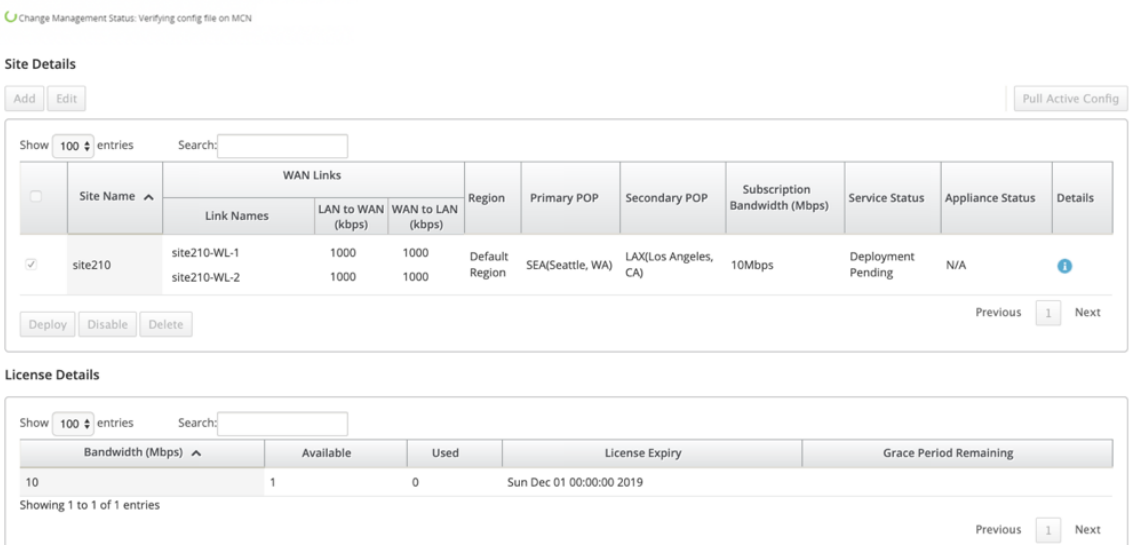
- **Modell**: Für die ausgewählte Site wird der entsprechende Appliance-Modellname automatisch ausgefüllt.
- **Region**: Für den ausgewählten Standort werden die Details der Appliance-spezifischen bereitgestellten Region automatisch aufgefüllt.
- **WAN-Link**: Für die ausgewählte Site werden die zugehörigen öffentlichen WAN-Links angezeigt.
- **WAN-Link-Typ**: Wählen Sie den WAN-Link-Typ aus dem Menü.
- **Standby-Modus**: Der Standbymodus wird aus der WAN-Link-Konfiguration abgerufen.
- **Bandbreite für Cloud Direct Service**: Geben Sie die Bandbreite ein, die der Cloud Direct Service ausschließlich nutzen kann. Die ausgewählte Bandbreite muss kleiner als die konfigurierte zulässige Bandbreite sein und steht nicht für die Verwendung durch die Dienste virtueller Pfad, Internet und Intranet zur Verfügung.
- **Externe NAT**: Es ist erforderlich, dass der öffentliche Internetverkehr, der aus dem Filial-LAN-Netzwerk stammt, Quell-NAT von einer bestimmten IP-Adresse ist. Standardmäßig wird dies automatisch durchgeführt und im Rahmen der SD-WAN-Netzwerkkonfiguration gepflegt. Wenn Sie die NAT-IP (LAN-Netzwerk) außerhalb des SD-WAN-Geräts konfigurieren möchten (z. B. in einer externen Firewall), können Sie bei der Bereitstellung von Standorten die Option Externe NAT-Option auswählen. Die IP, zu der der LAN-Datenverkehr die Quell-NAT sein muss, ist auf der **Detailseite** der bereitgestellten Cloud Direct-Site verfügbar.
- **Anwendungsobjekte**: Sie können bestimmte Anwendungsobjekte auswählen oder “Alle Internetverkehrs”auswählen, um über den Cloud Direct-Dienst umgeleitet zu werden. Wenn die spezifischen Anwendungsobjekte ausgewählt sind, wird der Datenverkehr für diese Anwendungen über den Cloud Direct-Dienst gesendet, und der Rest des Datenverkehrs wird über den auf der Appliance konfigurierten Internetdienst gesteuert.
- **Abonnementbandbreite**: Abonnementbandbreite ist mit der Lizenzierung für den Cloud-Direktdienst verknüpft.
- **Primär/Sekundär POP**: Stellen Sie sicher, dass der primäre und sekundäre POP nicht identisch sind. Wählen Sie die POPs abhängig von der Standortnähe aus. Klicken Sie auf **Hinzufügen**.

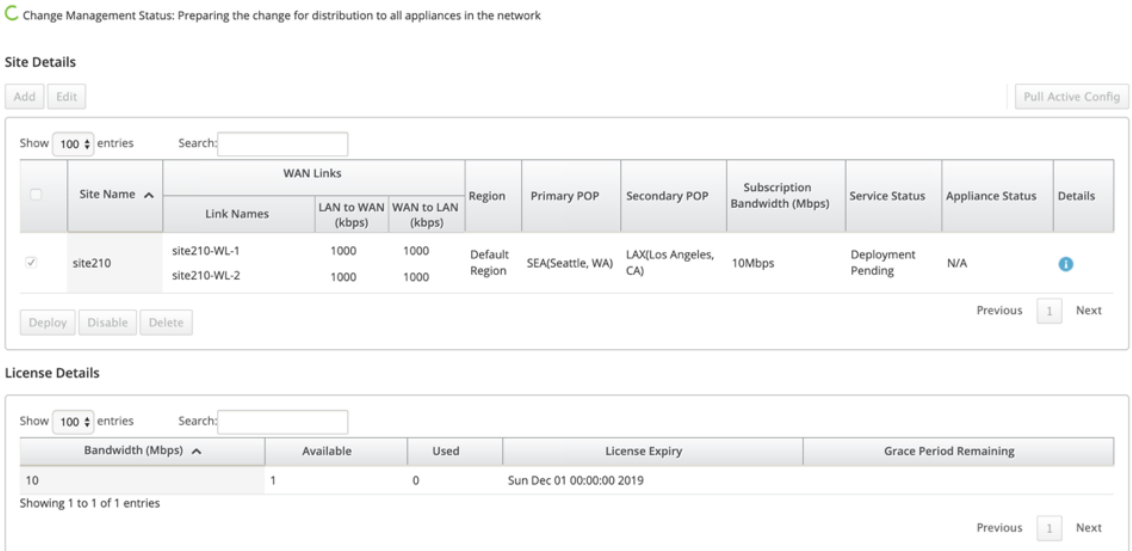
7. Nachdem die Sites hinzugefügt wurden, wird der Dienststatus als **Bereitstellung ausstehend**angezeigt. Wählen Sie die Site aus, für die Sie den Cloud Direct-Dienst bereitstellen möchten, und klicken Sie auf **Bereitstellen**.

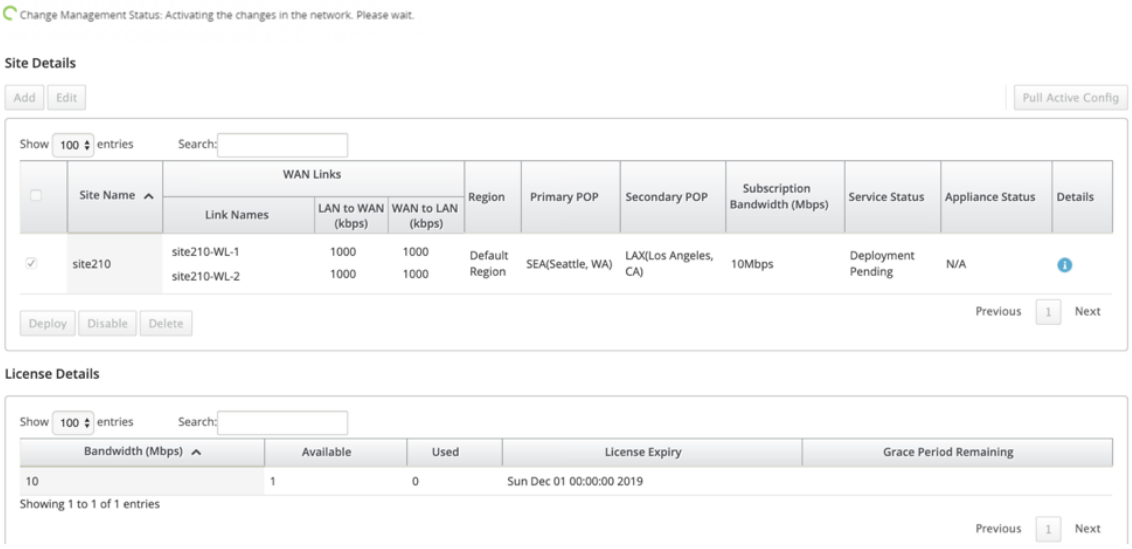


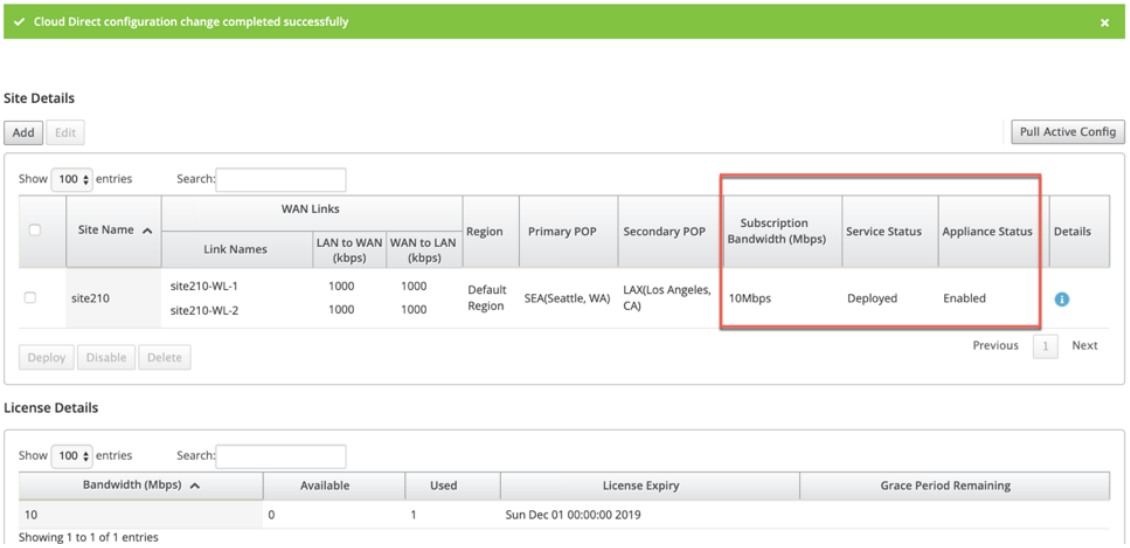
Es wird eine Benachrichtigung angezeigt, die besagt, dass der Bereitstellungsvorgang eine Änderungsverwaltung auf der MCN-Appliance initiiert. Sie können auf **Ja** oder **Nein**klicken.









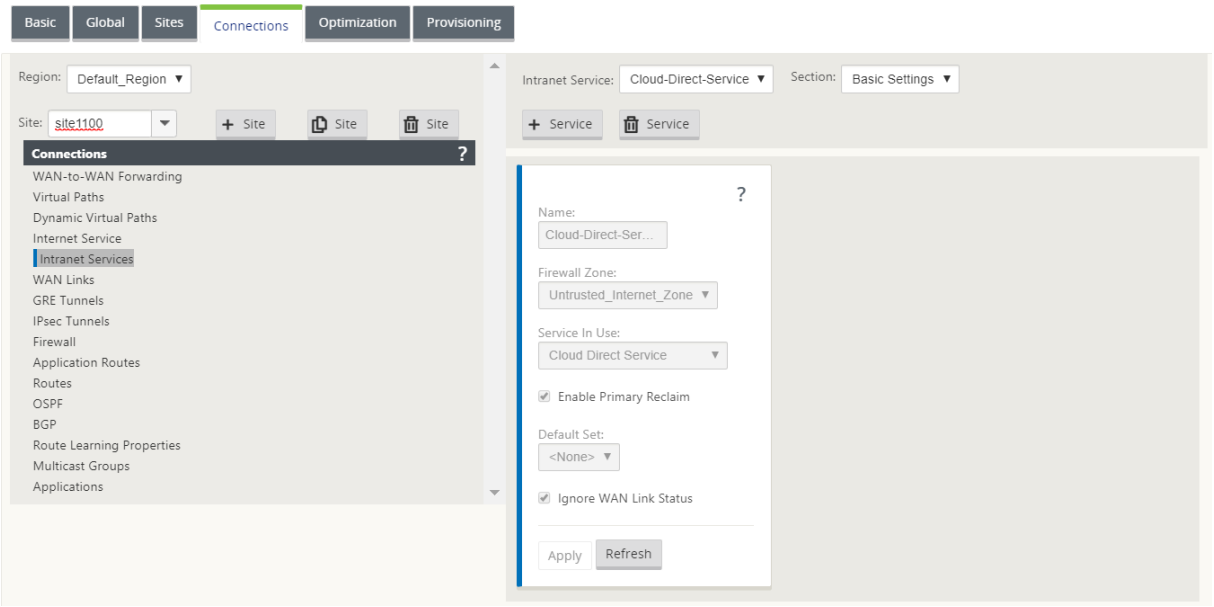


Nach der erfolgreichen Bereitstellung der Sites wird auf der Cloud Direct Service-Seite Folgendes angezeigt:

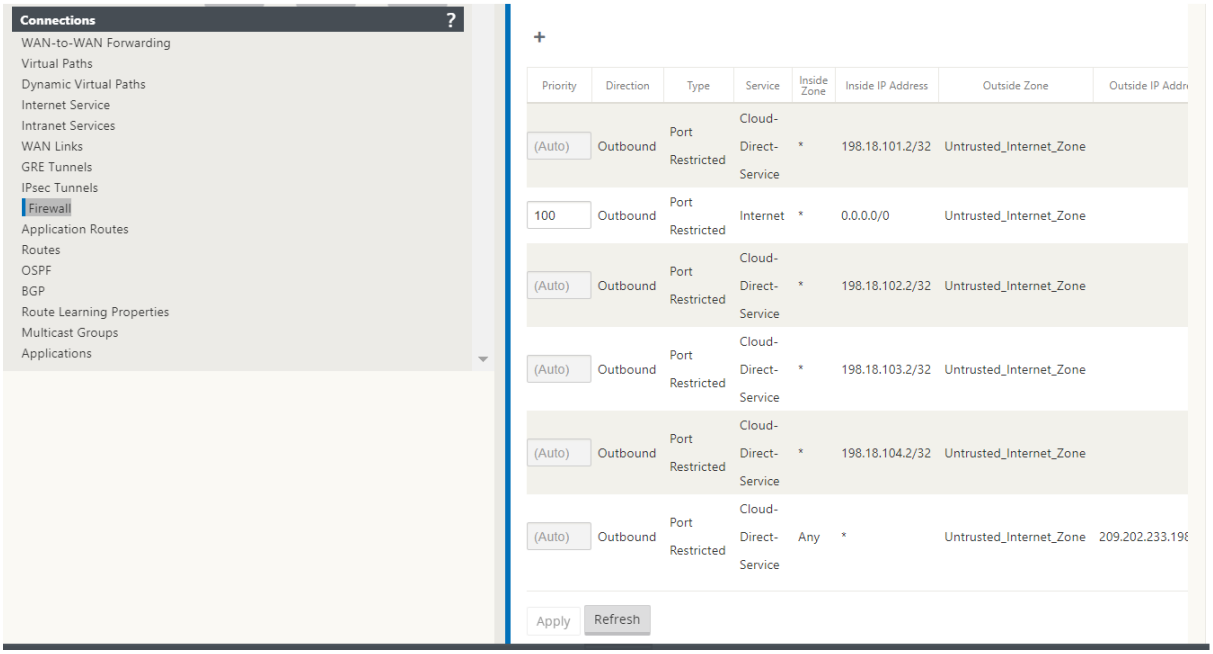
- **Dienststatus**: Bereitgestellt
- **Appliance-Status**: Aktiviert
- **Abonnementbandbreite (Mbit/s)**: 10 Mbit/s
- **Verbraucht die installierte Lizenz**

Der obige Änderungsverwaltungsschritt generiert automatisch die benötigten Cloud Direct-Dienstkonfigurationen und fügt der laufenden Konfiguration hinzu.

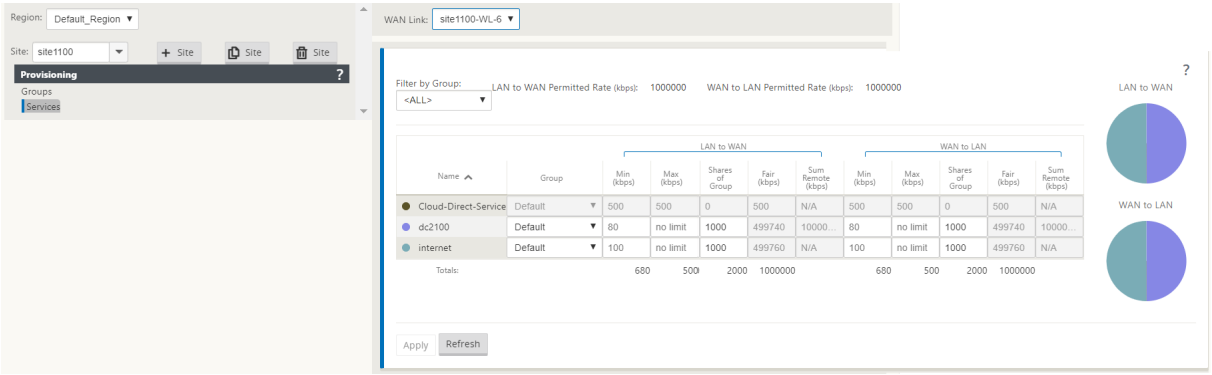
> **Hinweis:**
>
> Der automatisch erstellte **Cloud Direct Service** (Intranetdienst) ist der Default_RoutingDomain zugeordnet.



Firewalleinstellungen

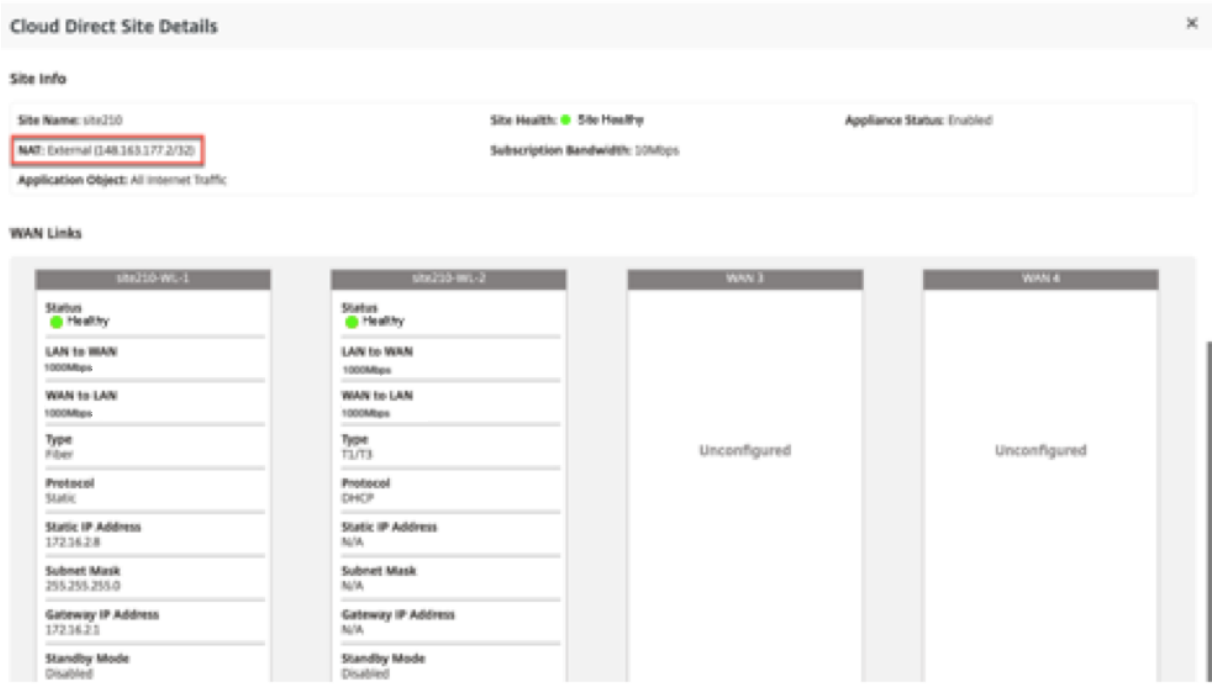


Provisioning von Sites über die Benutzeroberfläche der SD-WAN-Anwendung

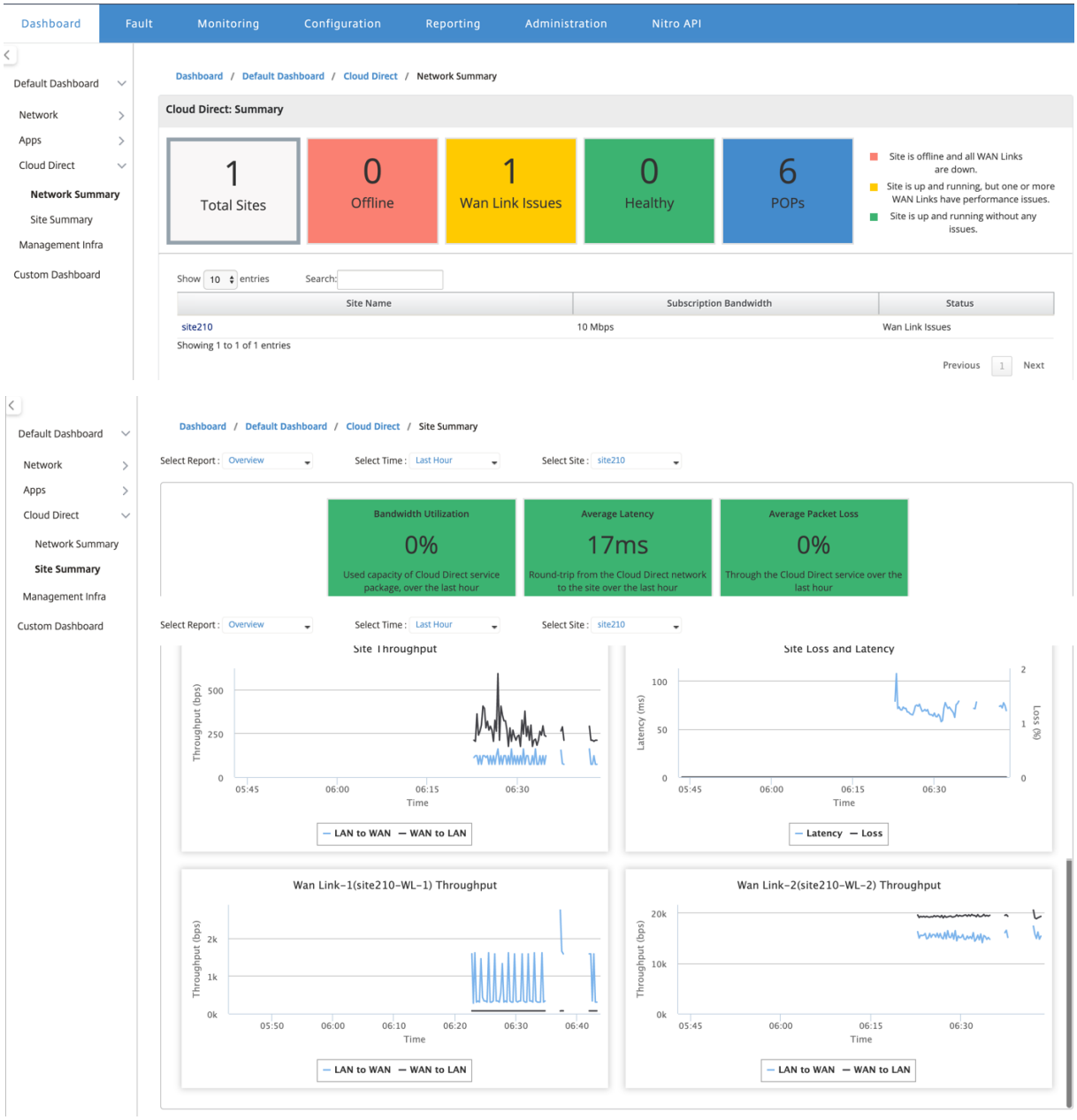


Überwachung des Cloud Direct-Dienstes

Sie können den konfigurierten Cloud Direct-Dienst anzeigen, nachdem die Standorte bereitgestellt und aktiviert wurden. Klicken Sie auf das Ausrufe-Symbol in der Spalte **Details**, um die Website-Details anzuzeigen.



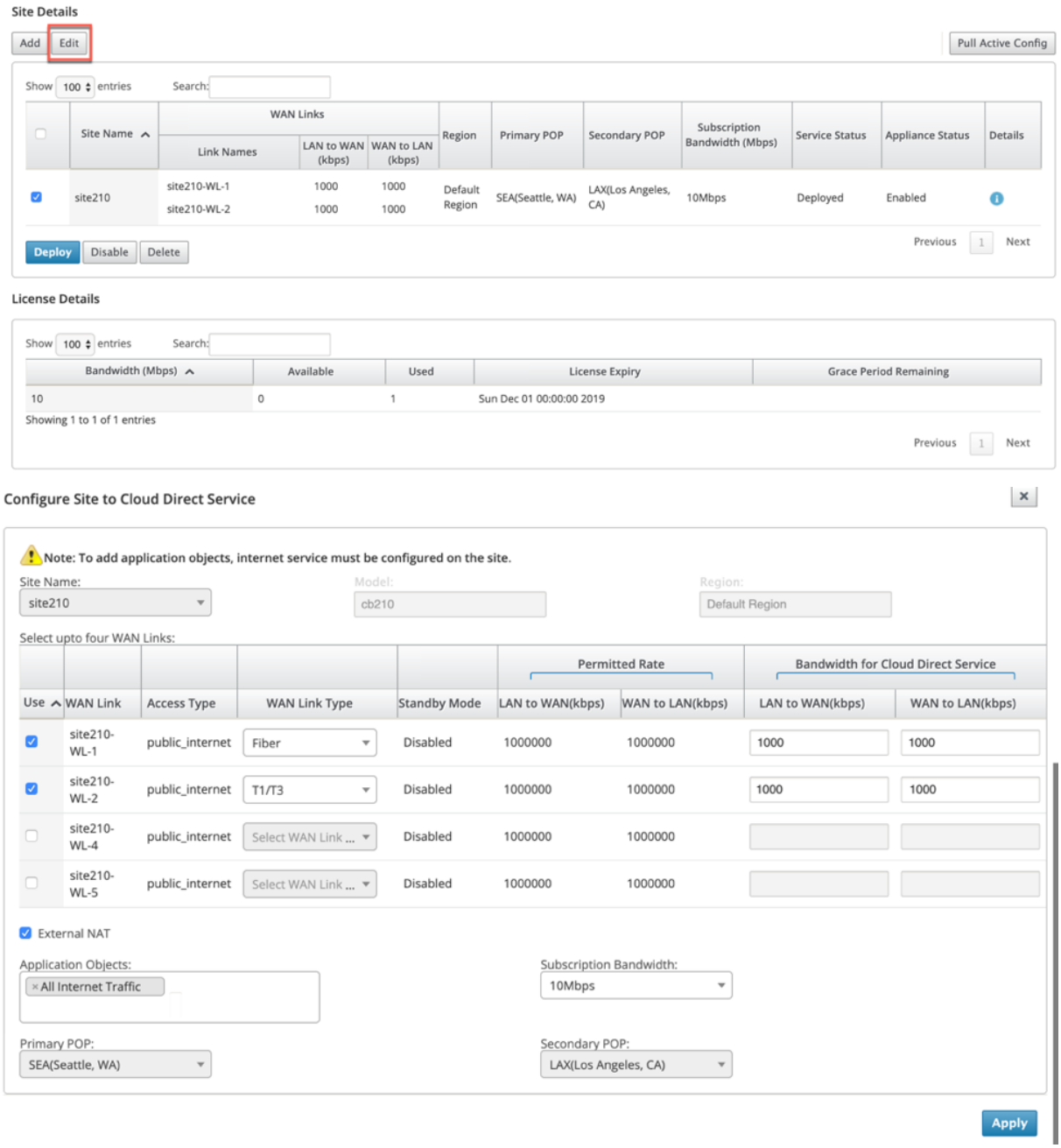
Sie können die Siteübersichtsdiagramme anzeigen, indem Sie zu **Dashboard** > **Cloud Direct** > **Netzwerkübersicht** und **Standortübersicht** navigieren.

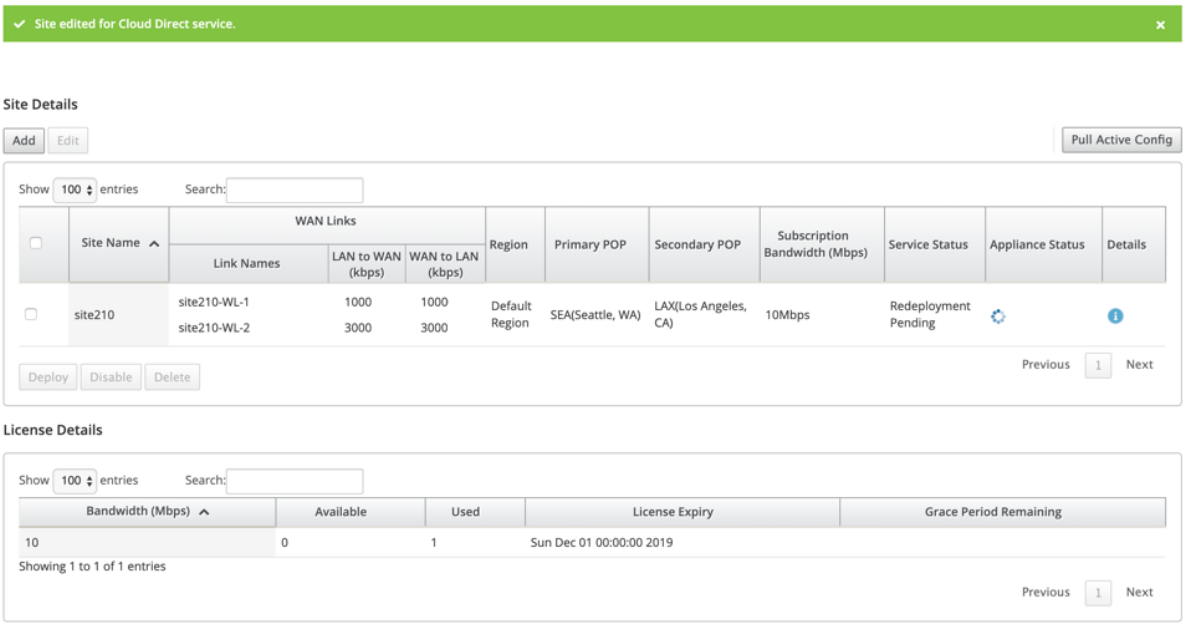


Bearbeiten der Site im SD-WAN Center

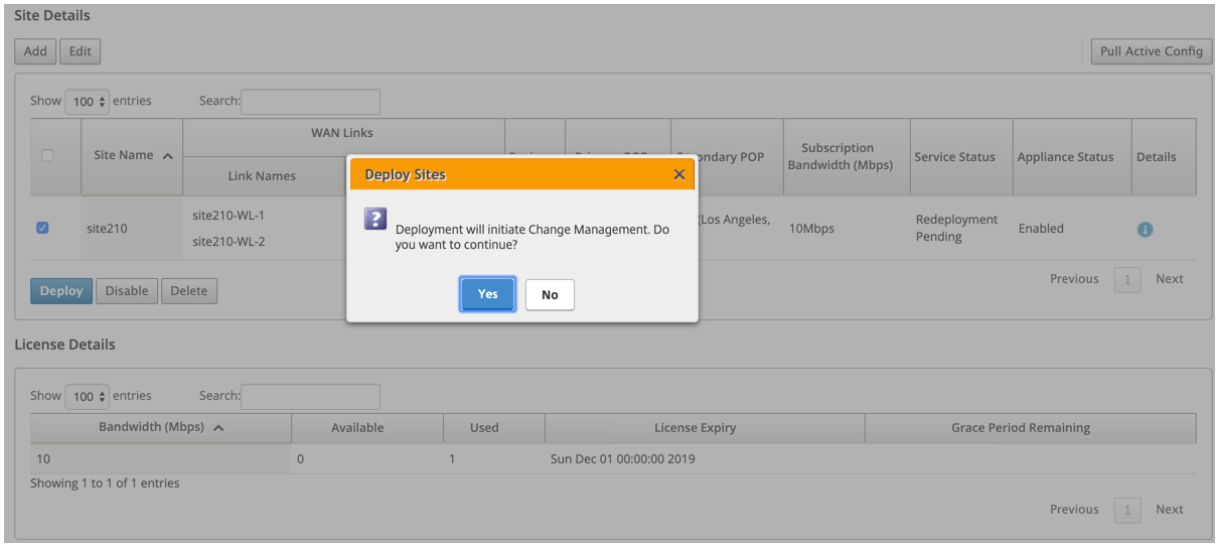
Sie können die Sites bearbeiten, um Bandbreite und WAN-Link-Typ zu ändern.

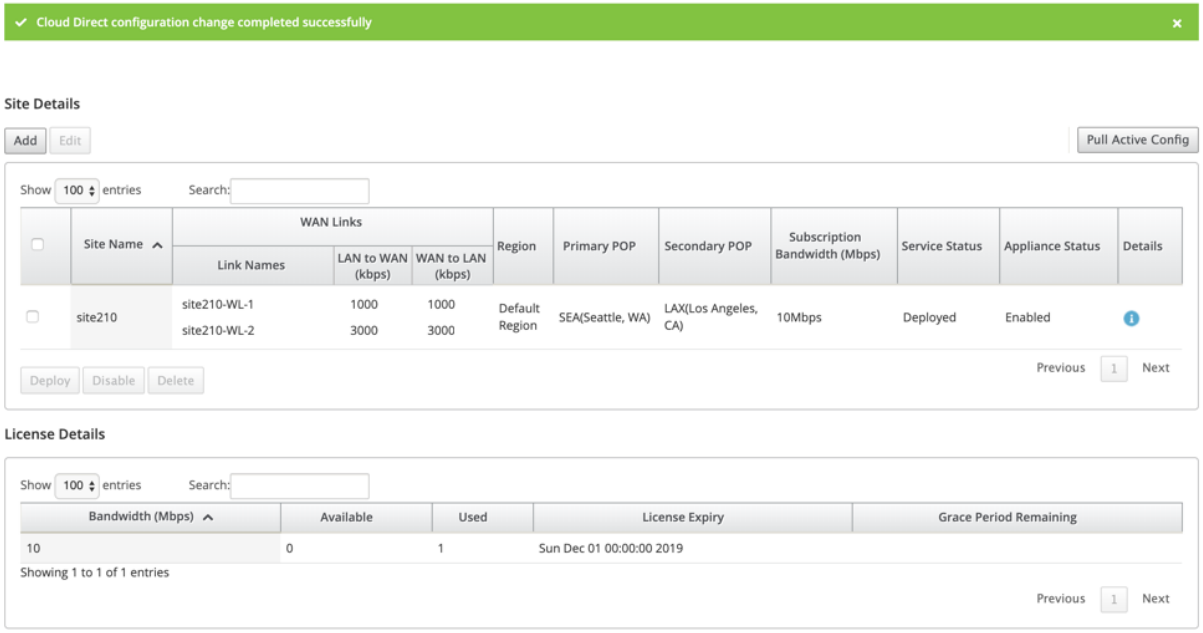
> **Hinweis**
>
> POP-Auswahlen können nicht bearbeitet werden.





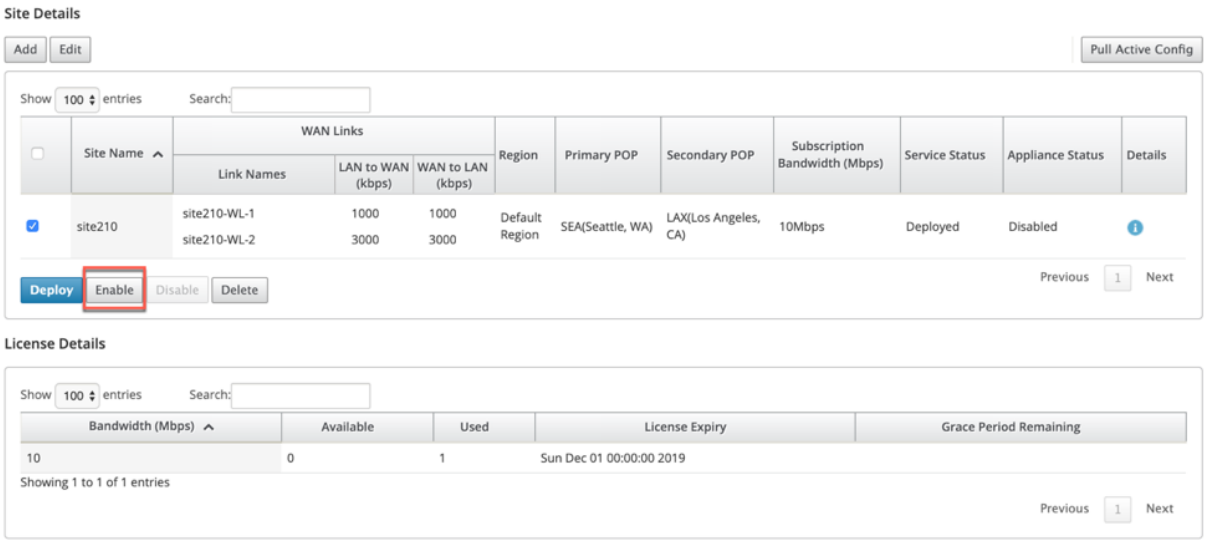
Der Dienststatus wird als Neubereitstellung ausstehend angezeigt. Stellen Sie die Site bereit. Der Bereitstellungsprozess ist für die bearbeitete Site abgeschlossen.

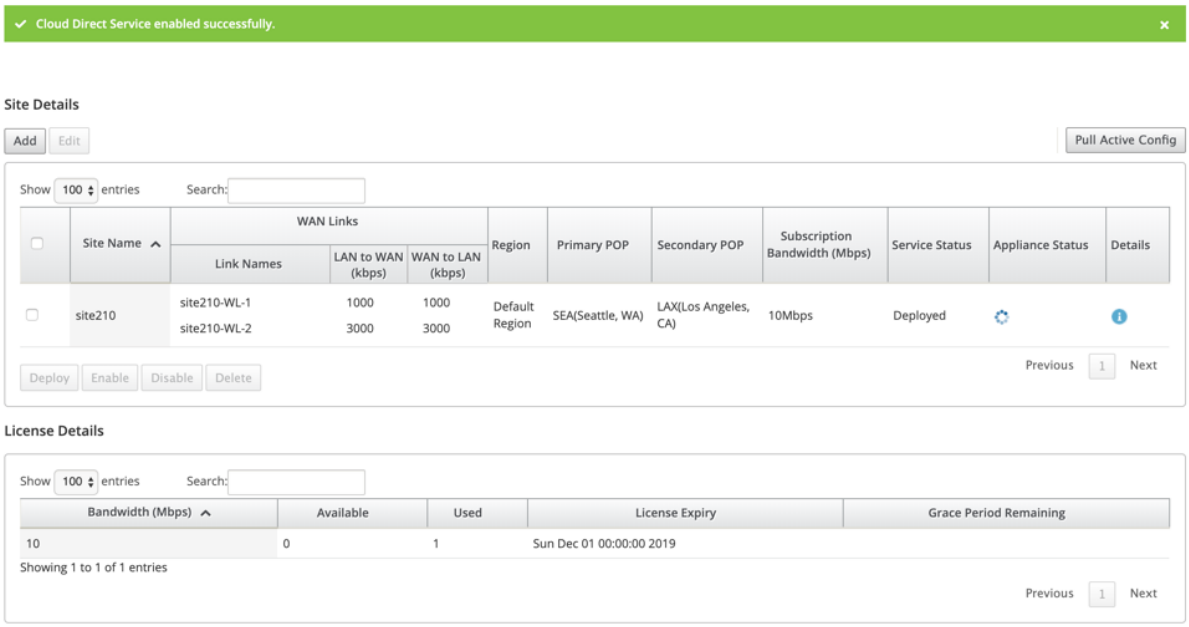




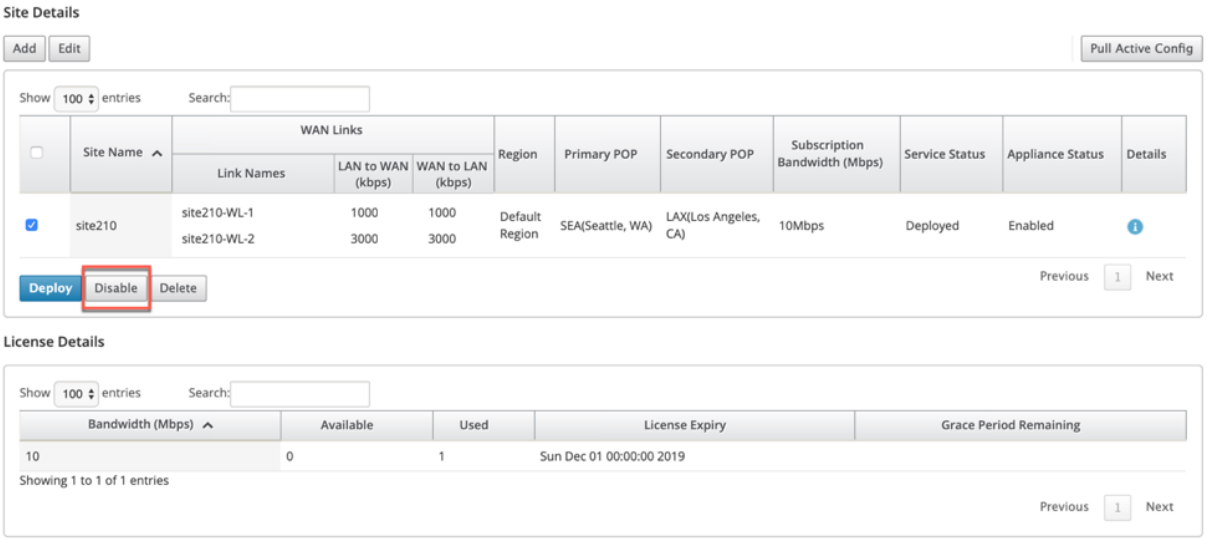
Site aktivieren und deaktivieren

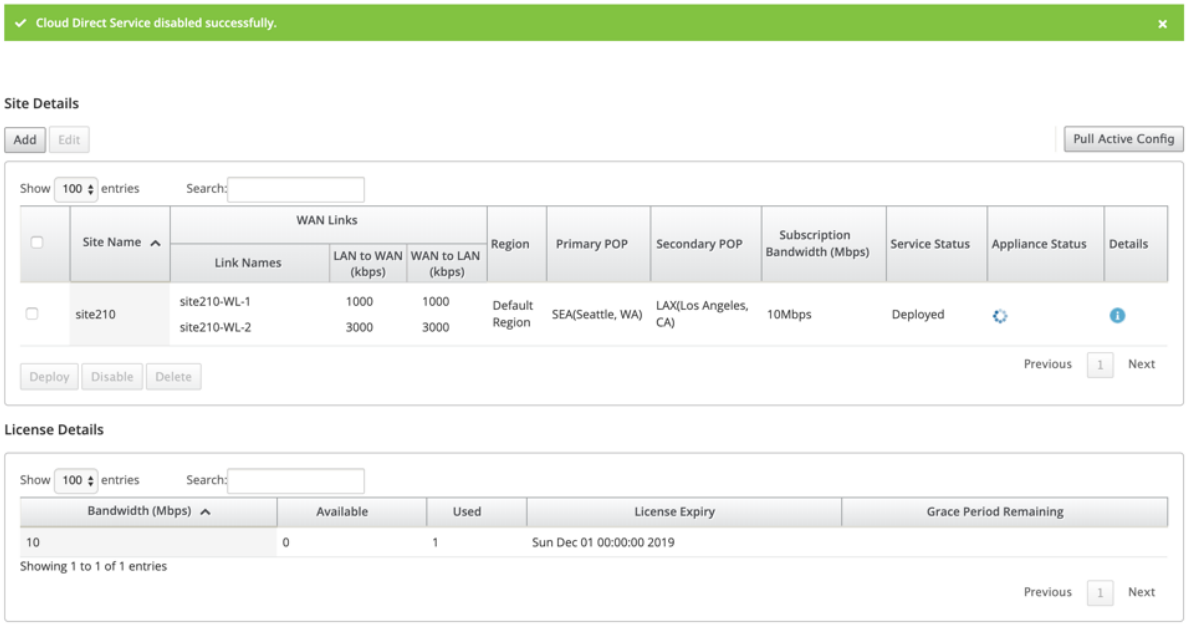
Sie können einen bereitgestellten Standort aktivieren, dessen Appliance-Status als deaktiviert angezeigt wird. Klicken Sie zum Aktivieren der Site auf **Aktivieren**.





Klicken Sie auf **Deaktivieren**, um eine bereitgestellte Site zu deaktivieren. Die Deaktivierung der Site würde den Cloud-Direktdienst nicht mehr verwenden, um den Internetverkehr zu steuern. Der gesamte Datenverkehr wird über den Internetdienst umgeleitet, wenn er auf der Appliance konfiguriert ist.

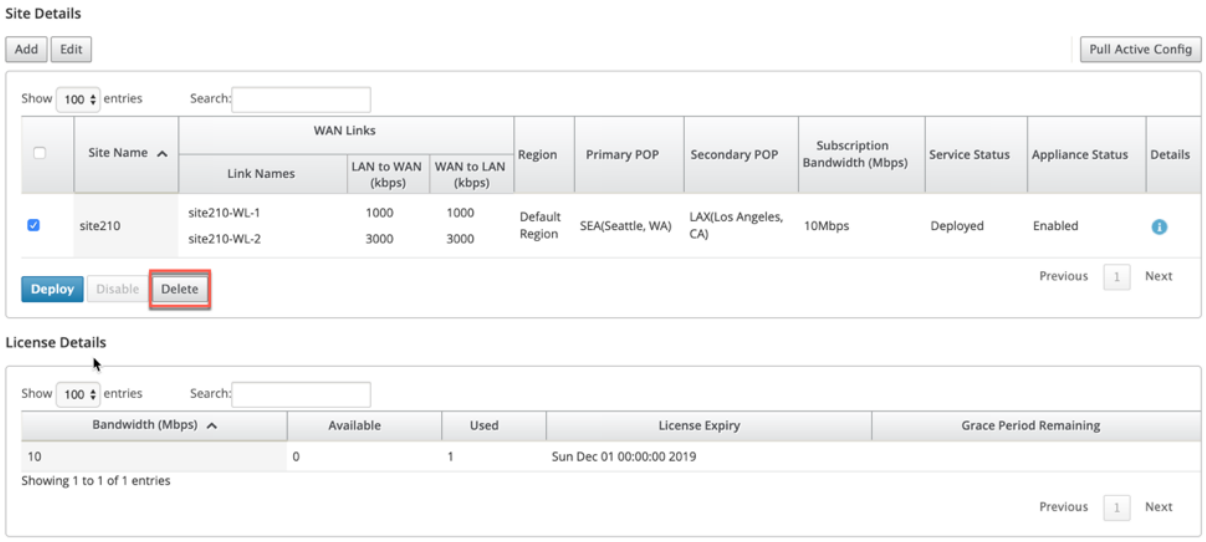


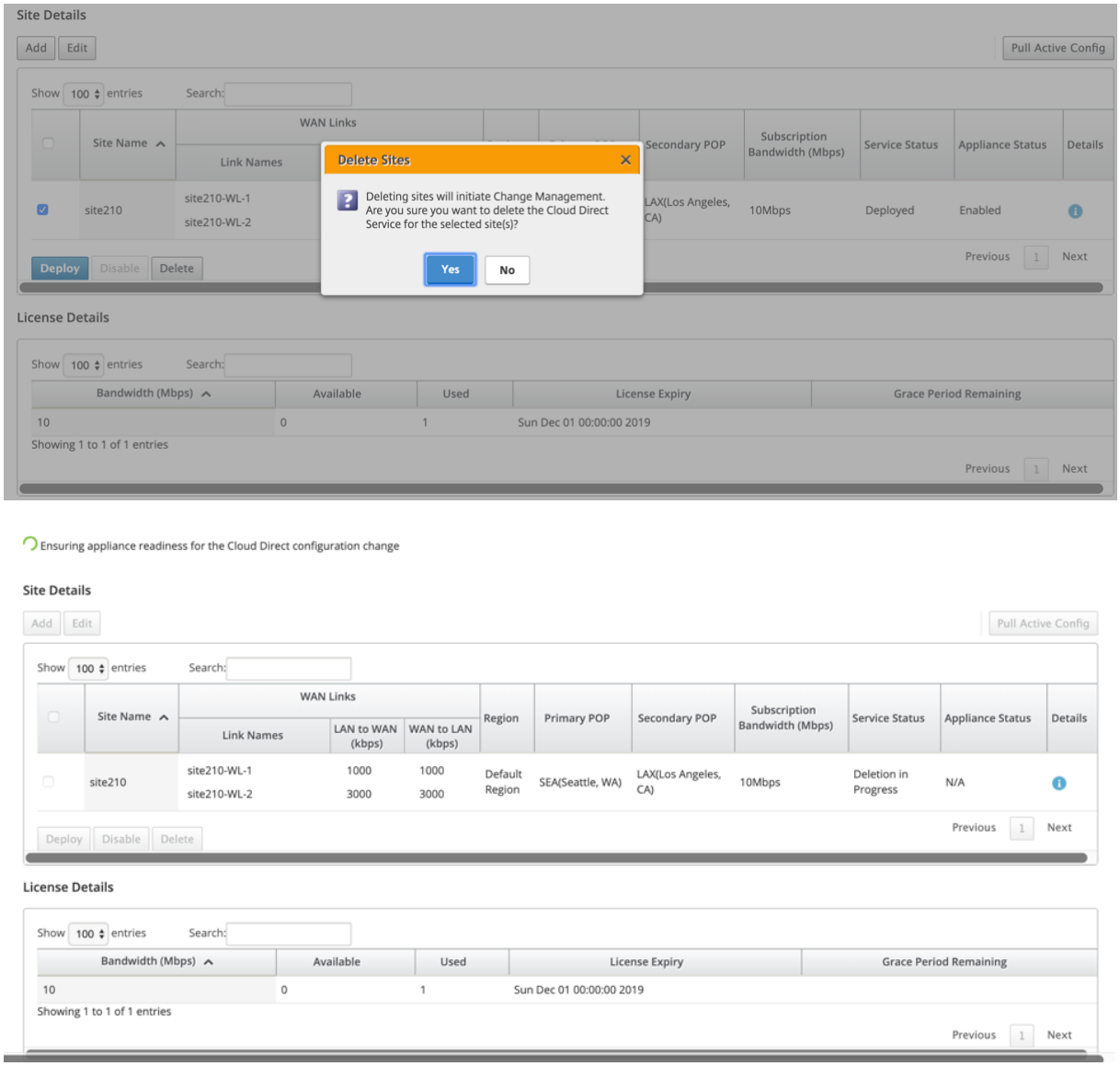


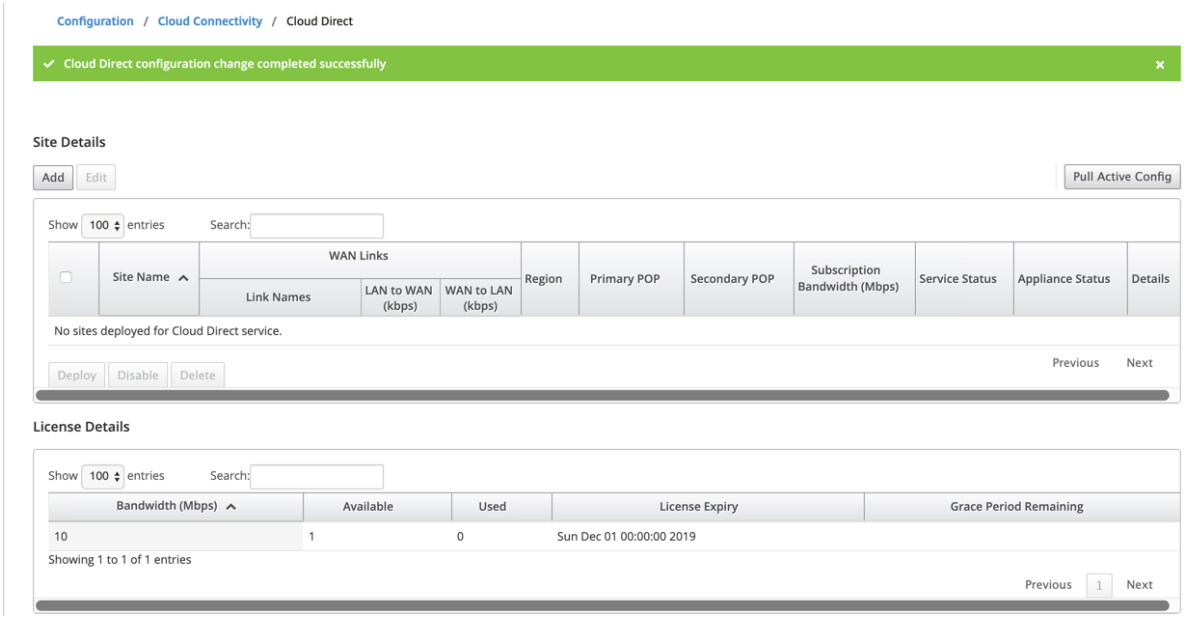
Site löschen

Sie können die Sites löschen, für die keine Cloud Direct-Konnektivität mehr erforderlich ist. Um Sites zu löschen, wählen Sie die Site aus, und klicken Sie auf **Löschen**. Eine Bestätigungsmeldung zum Löschen von Sites wird angezeigt.

Die gesamte Cloud-Direktdienstkonfiguration wird durch den Änderungsmanagement-Prozess entfernt.



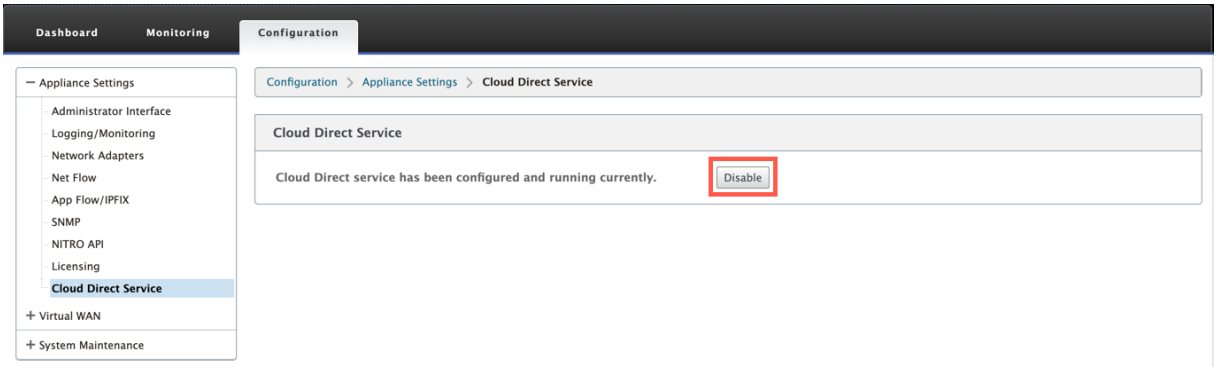




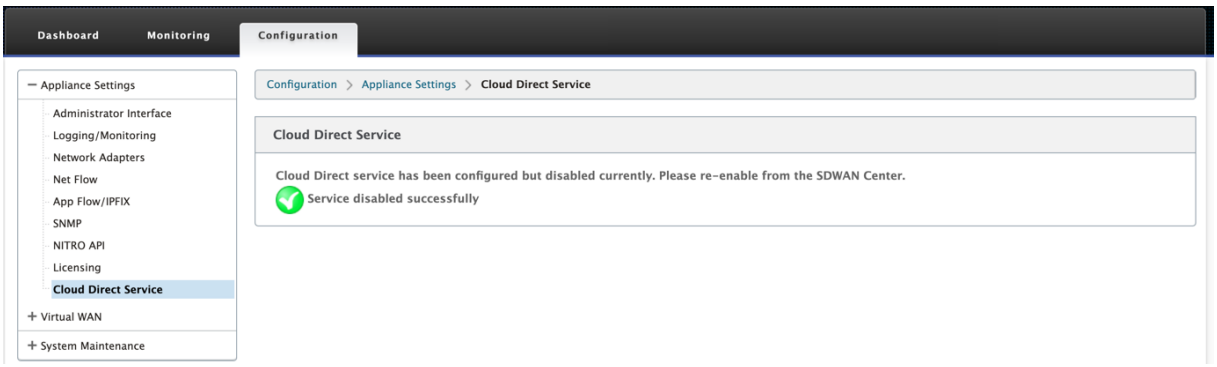
Status des Cloud Direct Service auf Citrix SD-WAN

Sie können den Cloud Direct-Dienststatus auf einer lokalen SD-WAN-Appliance überprüfen.

Gehen Sie zur Citrix SD-WAN GUI, navigieren Sie zu **Konfiguration** > erweitern Sie die **Appliance-Einstellungen** > wählen Sie **Cloud Direct Service** aus.



Klicken Sie auf **Deaktivieren**, um den Cloud Direct-Dienst zu deaktivieren.



Problembehandlung

Die häufigsten Fehlermeldungen, die bei der Bereitstellung des Cloud Direct-Dienstes auf SD-WAN Center auftreten können, sind wie folgt.

Fehler-/Statusmeldungen werden im SDWAN Center unter **Konfiguration** > **Cloud-Konnektivität** > **Cloud Direct** angezeigt.

'Cloud Direct License error! Please upload additional license for {bandwidth} Mbps bandwidth'

- Laden Sie eine gültige Cloud Direct-Lizenz auf SDWAN Center hoch, indem Sie zu **Konfiguration** > **Lizenzierung** > **Dateiverwaltungsoption** navigieren und dann mit der Bereitstellung dieser Funktion fortfahren.

'Cloud Direct configuration HA due to Citrix Cloud Workspace login issue'

- Geben Sie die Anmeldeinformationen für die Citrix Cloud Workspace-Anmeldung im SDWAN Center erneut ein, indem Sie zu **Konfiguration** > **Cloud-Konnektivitätsoption** navigieren.

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) is not reachable or is missing Cloud Direct support'

- Überprüfen Sie, ob die SD-WAN-Appliance oder -Appliances (im Falle einer HA-Bereitstellung) am Management-Port erreichbar sind.

'Cloud Direct configuration HA Config Check error for site: {site_name}'

- Überprüfen Sie die Konnektivität beider Appliances im HA-Paar, das dem bereitgestellten Standort entspricht.

'Both the HA Pair Appliances have to be reachable to perform Cloud Direct Configuration'

- Bei der Bereitstellung des Cloud Direct-Dienstes auf SD-WAN-Appliances im HA-Paar müssen sowohl sekundäre als auch primäre Appliances über den Verwaltungsport erreichbar sein.

‘Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) has SSO Login Issue’

- Überprüfen Sie, ob die SD-WAN-Appliance betriebsbereit ist und über den Management-Port erreichbar ist. Dieser Fehler wird angezeigt, wenn SD-WAN Center die einmalige Anmeldung bei der SDWAN-Appliance nicht durchführen kann.

‘Internal error encountered during Cloud Direct configuration processing’

- Dies kann aufgrund mehrerer Fehlerbedingungen während der Konfigurationsüberprüfung oder des restlichen Verarbeitungsvorgangs auftreten. Benutzer müssen möglicherweise die Protokolle überprüfen und den Vorgang erneut ausführen.

‘Cloud Direct configuration processing canceled! MCN is not ready for change management’

- Überprüfen Sie, ob MCN zugänglich ist und ausgeführt wird und ob der Änderungsverwaltungsstatus “network_staging”ist.

‘Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) does not have Cloud Direct support. Führen Sie ein Upgrade in einem Schritt durch, um eine Cloud Direct-Unterstützung zu haben’

- Führen Sie ein Software-Upgrade auf der SD-WAN-Appliance über **MCN** > **Change Management** durch. Versuchen Sie nach diesem Verfahren erneut, den Cloud Direct-Dienst für diese Site bereitzustellen.

‘Cloud Direct configuration processing error! SD WAN change management operation failed’

- Change Management-Operation war irgendwie nicht erfolgreich. Weitere Informationen finden Sie in den SDWAN Center-Protokollen.

‘Cloud Direct configuration processing error! Enabling service at site: {site_name} failed’

- Der Cloud Direct-Dienst kann nicht auf der SD-WAN-Appliance aktiviert werden. Überprüfen Sie, ob eine bestimmte Appliance oder ein HA-Paar angeschlossen ist oder ob Probleme beim einmaligen Anmelden auftreten. Überprüfen Sie die Protokolle auf dem SD-WAN Center und der Appliance, um weitere Informationen zu erhalten.

‘Cloud Direct configuration processing error! Disabling service at site: {site_name} failed’

- Cloud Direct-Dienst auf der SD-WAN-Appliance kann nicht deaktiviert werden. Prüfen Sie, ob eine bestimmte Appliance oder ein HA-Paar angeschlossen ist oder ob Probleme beim einmaligen Anmelden auftreten. Überprüfen Sie die Protokolle auf dem SD-WAN Center und der Appliance, um weitere Informationen zu erhalten.

‘Cloud Direct configuration processing error! Config image push to site: {site_name} failed’

- Das dienstspezifische Image kann nicht über die REST-API auf die Appliance hochgeladen werden oder kann nicht auf beide Appliances im HA-Paar zugreifen.

‘Cloud Direct Service encountered an error during configuration processing. Audit errors found in the SD WAN config!’

- Beim Versuch, die SDWAN-Konfiguration zu kompilieren, wurden Überwachungsfehler gefunden. Weitere Informationen finden Sie in den Protokollen des SD-WAN Centers.

‘Cloud Direct configuration processing error! Create Site failed for Site: {site_name}’

- Dienstseitiger Fehler beim Erstellen einer Site für die entsprechende SDWAN-Appliance. Weitere Informationen finden Sie in den SDWAN Center-Protokollen.

‘Cloud Direct configuration processing error! Update Site failed for Site: {site_name}’

- Dienstseitiger Fehler beim Ändern der sitebezogenen Einstellungen für die entsprechende SDWAN-Appliance. Weitere Informationen finden Sie in den SDWAN Center-Protokollen.

Fehlermeldungen in Protokollen (SDWAN_Common.log)

Im Folgenden finden Sie einige Szenarien, in denen Cloud Direct-Dienst auf der SD-WAN-Appliance bereitgestellt wird, aber möglicherweise nicht wie erwartet funktioniert. Sie können die Protokolle auf der lokalen SDWAN-Appliance mit SDWAN_common.log herunterladen und überprüfen, um weitere Informationen zu erhalten.

Szenario 1

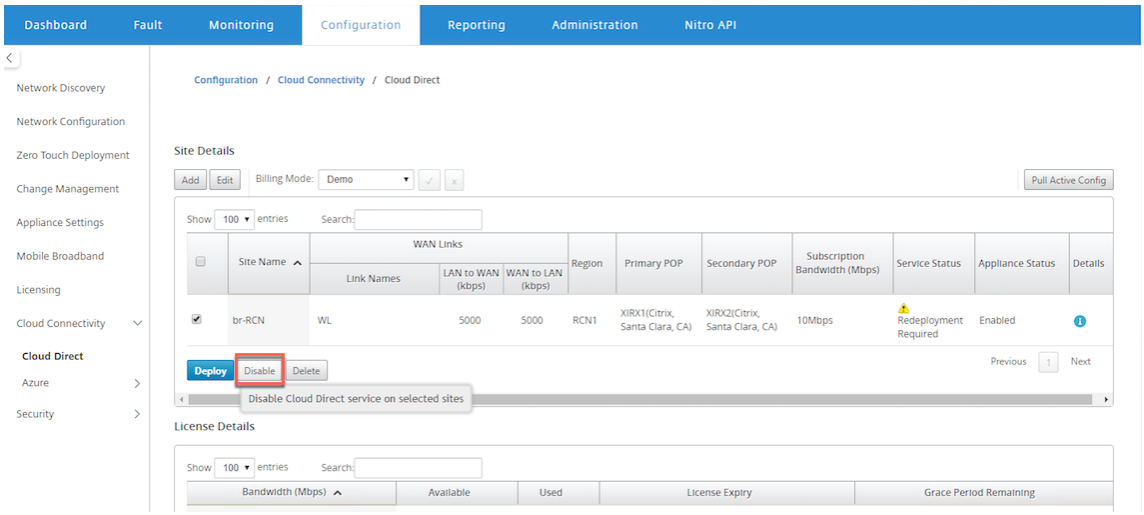
“Detected Cloud Direct VM is not responding …Disabling Cloud Direct Service now!”“Cloud Direct service has been disabled.” Die zugrunde liegende KVM, die auf der lokalen SDWAN-Appliance ausgeführt wird, funktioniert nicht erwartungsgemäß. In diesem Fall ist die Cloud Direct-Dienstfunktionalität auf der Appliance deaktiviert.

Szenario 2

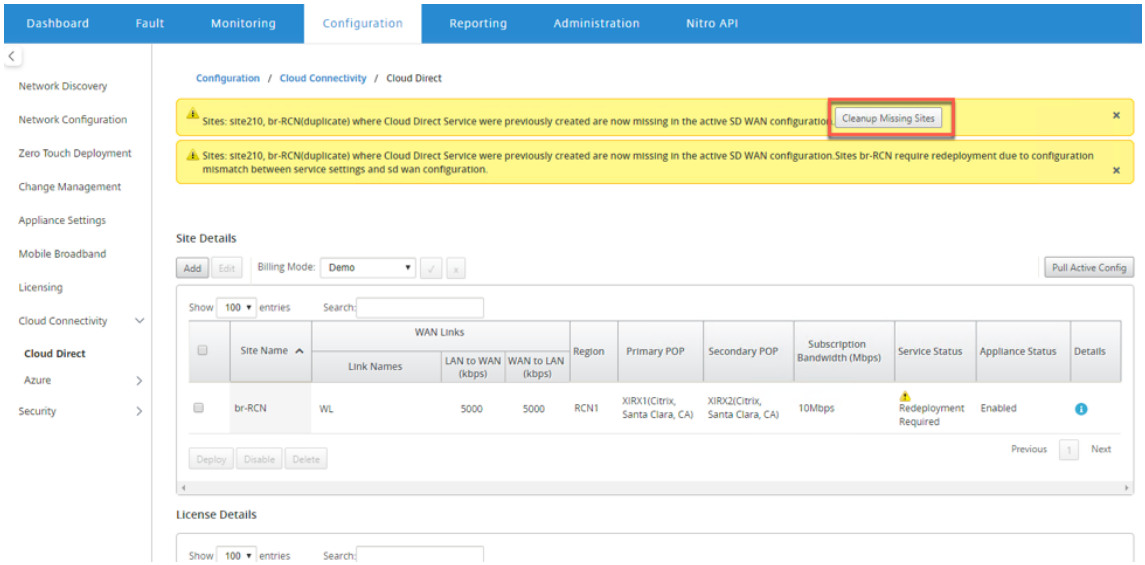
“No tunneled packets seen for past 5 mins …Disabling Cloud Direct Service now!”“Cloud Direct service has been disabled.” Zwischen der SD-WAN-Appliance und dem Tunnelendpunkt, der für den Cloud Direct-Dienst verwendet wird, ist kein Tunnel eingerichtet. Dies kann auf Fehlkonfiguration von wan-link, fehlende Internetkonnektivität über konfiguriertes wan-link, inkompatibles oder ungültiges Daten/Config-Image, das an die Appliance übertragen wird, oder auf eine Firewall-Regel zurückzuführen sein, die UDP-Tunnelpakete löschen könnte, wenn sie über wan-link empfangen werden. In diesem Fall ist die Cloud Direct-Dienstfunktionalität auf der Appliance deaktiviert.

Wenn Sie eine Konfiguration auf MCN mit unterschiedlicher Cloud Direct-Konfiguration aktivieren (Zum Beispiel: NAT-Konfiguration wird für Cloud Direct geändert) und dies kann zu einer permanenten Unterbrechung des Datenverkehrs führen. Um diesen Block zu überwinden, können Sie einen der folgenden Schritte ausführen, um die verschiedenen Routen auf der Appliance auszuwählen:

1. Navigieren Sie in der Benutzeroberfläche des SD-WAN Centers zu **Konfiguration** > **Cloud-Konnektivität** > **Cloud Direct**. Wählen Sie die Cloud Direct Appliance aus, und klicken Sie auf **Deaktivieren**, um den Cloud-Direktdienst zu deaktivieren.



2. Navigieren Sie zu **Konfiguration** > **Cloud-Konnektivität** > **Cloud Direct** und ziehen Sie die aktive Konfiguration ab, um die Bereinigungsbenachrichtigung zu erhalten. Sie können auf die Benachrichtigungsschaltfläche für **fehlende Sites bereinigen** klicken, die für die betroffene Cloud Direct Appliance angezeigt wird. Dieser Vorgang deaktiviert den Cloud Direct-Dienst, der auf der Appliance ausgeführt wird.



3. Stellen Sie den Cloud Direct-Dienst erneut im SD-WAN Center bereit, um den Cloud Direct-Dienst für betroffene Appliances zu verwenden.

Integrieren von Citrix SD-WAN und Zscaler mit Citrix SD-WAN Center

April 13, 2021

Citrix SD-WAN und Zscaler helfen Unternehmen, ihr WAN für die Cloud-Migration zu transformieren, indem sie sichere lokale Unterbrechungen für Anwendungen und Ressourcen bereitstellen, die im Internet gehostet werden. Neue WAN-Infrastrukturtechnologien wie SD-WAN erhöhen die Agilität und Skalierung des Netzwerks und senken gleichzeitig Kosten und Komplexität für eine verbesserte Benutzererfahrung in verteilten Unternehmen.

SD-WAN-Lösungen vereinfachen das Routing, da Datenverkehr, der für die Cloud bestimmt ist, lokal ins Internet gebracht werden kann. SD-WAN bietet Flexibilität beim Routing des Datenverkehrs an das Internet (Entfernen der zentralen DC-Umgebung) mithilfe von Anwendungssteuerungsfunktionen. Die Aussetzung des Netzwerks im Internet birgt jedoch erhebliche Sicherheitsrisiken. Ein zentralisierter Ansatz zur Sicherung lokaler Ausbrüche durch einen Cloud-Service eliminiert den Aufwand für die Wartung der Sicherheitsinfrastruktur in den Filialen. Der gesamte Datenverkehr wird zuverlässig und sicher an Zscaler (cloudbasierte Sicherheitsplattform) mit Citrix SD-WAN im Zweignetz weitergeleitet. Sie können kostspielige Infrastruktur eliminieren und Ihr Netzwerk vor Bedrohungen und Schwachstellen schützen.

Citrix SD-WAN

Citrix SD-WAN unterstützt Unternehmen beim Wechsel in die Cloud, indem lokale Branch-zu-Internet-Breakouts mit einer integrierten Stateful-Firewall sicher aktiviert werden, um Richtlinien zu erstellen, die den Internetzugriff direkt aus der Zweigstelle ermöglichen oder verweigern können. Citrix SD-WAN identifiziert Anwendungen durch eine Kombination aus einer integrierten Datenbank mit mehr als 4.000 Anwendungen, einschließlich einzelner SaaS-Anwendungen, und verwendet Deep Packet Inspection Technologie für die Echtzeiterkennung und Klassifizierung von Anwendungen. Es nutzt dieses Anwendungswissen, um den Datenverkehr von der Zweigstelle in das Internet, die Cloud oder SaaS zu steuern.

Zscaler

Zscaler ist die führende cloudbasierte Sicherheitsplattform, die überragende Sicherheit bietet, ohne dass lokale Hardware, Appliances oder Software benötigt werden. Zscaler legt einen Umfang um das Internet herum, so dass Unternehmen nicht in jedem Büro einen Sicherheitsbereich setzen müssen. Die Zscaler Cloud Security Platform fungiert als eine Reihe von Sicherheitskontrollen in mehr als 100 Rechenzentren auf der ganzen Welt. Durch die Umleitung des Internetverkehrs an Zscaler können Unternehmen Geschäfte, Filialen und Remote-Standorte sofort sichern. Zscaler verbindet Benutzer mit dem Internet und überprüft jedes Byte des Datenverkehrs —selbst wenn es verschlüsselt oder komprimiert ist—so dass Benutzer sicher sind und alle versteckten Bedrohungen identifiziert werden, bevor sie das Unternehmensnetzwerk infiltrieren können.

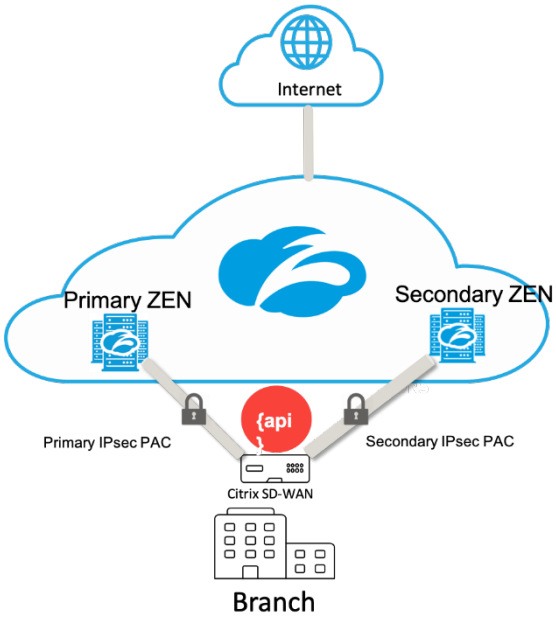
Citrix SD-WAN ermöglicht das Erstellen von Richtlinien, die einen direkten Internetausbruch aus der Zweigstelle ermöglichen, und die Cloud Security Platform von Zscaler sorgt für Sicherheit für die IT, indem der gesamte internetgebundene Datenverkehr in einem Cloud-Dienst in der Nähe des Verbindungsnetzes überprüft wird.

Zscaler Erzwingungsknoten (ZENs)

Citrix SD-WAN unterstützt Zscaler-APIs zur Automatisierung der Erstellung von IPSec-Tunneln zwischen Citrix SD-WAN und Zscaler Enforcement Nodes (ZENs) im Cloud-Netzwerk von Zscaler. ZENs sind voll funktionsfähige Inline-Internet-Sicherheits-Gateways, die den gesamten Internetverkehr bidirektional auf Malware untersuchen und Sicherheits- und Compliance-Richtlinien durchsetzen.

Die Zscaler-API stellt die beiden nächstgelegenen Rechenzentrumsstandorte jeder Filiale zur Verfügung, sodass SD-WAN den Datenverkehr effektiv steuern kann. Organisationen können zulassen, dass Zscaler automatisch das dem Zweigstellen nächstgelegene ZEN auswählt, indem es die IP-Adressen von WAN-Links sucht, die auf Citrix SD-WAN konfiguriert sind, oder manuell die **ZENs**auswählen.

> **Hinweis**
>
> Beide Routen befinden sich immer im aktiven Modus, wenn der Tunnel UP ist. Wenn ein Tunnel hinuntergeht, wird die entsprechende Route nicht erreichbar und die andere Route bleibt in diesem Fall UP.



Vorteile

Die Vorteile der Integration von Citrix SD-WAN und Zscaler umfassen:

- Schnellere Einführung von SaaS und Cloud in einem verteilten Unternehmen.
  - Die Zentralisierung der Sicherheit als Cloud-Dienst macht die Notwendigkeit, sie in jedem Zweig zu haben.
  - Es ist überflüssig, internetgesteuerten Datenverkehr zu hinterlegen, sodass lokale Internetausbrüche in der Zweigstelle möglich sind.
- Vereinfachte IT-Verwaltung mit automatischer Verbindung mit einer Secure Web Gateway.
  - API-Unterstützung automatisiert die Konfiguration von sicheren Tunneln zu Zscaler
- Verbesserte Benutzerfreundlichkeit durch Reduzierung der Latenz durch Backhauling SaaS-Datenverkehr.
  - Eliminiert Hub-and-Spoke-Modellabhängigkeit aus Sicherheitsgründen
- Eliminierung kostspieliger Sicherheitsstapel in Zweigstellen

  - Reduzieren Sie den Aufwand für die Bereitstellung und Verwaltung von Firewalls in den Filialen.

- Gewissheit, dass internetgebundener Datenverkehr immer sicher ist.
  - Sicherheitsrichtlinien binden Benutzer nicht an einen physischen Standort.
  - Bietet Sandboxing, Überprüfung aller Ports und Protokolle, einschließlich SSL, URL-Filterung, erweiterter Bedrohungsschutz und mehr zum Schutz vor Zero-Day-Angriffen.

Unterstützte Funktionen

Eine Zscaler-Bereitstellung mit SD-WAN-Appliances unterstützt die folgenden Funktionen:

- Weiterleiten des benutzerdefinierten Internetverkehrs an Zscaler, wodurch ein direkter Internetausbruch möglich ist.
- Direkter Internetzugang (DIA) mit Zscaler pro Kundenstandort.
  - Auf einigen Sites sollten Sie DIA mit lokalen Sicherheitsgeräten bereitstellen und Zscaler nicht verwenden.
  - Auf einigen Sites können Sie den Datenverkehr einer anderen Kundenseite für den Internetzugang zurückholen.
- Virtuelle Routing- und Weiterleitungsbereitstellungen.
- Ein WAN-Link als Teil von Internetdiensten.

Zscaler ist ein Cloud-Dienst. Sie müssen es als Service einrichten und die zugrunde liegenden WAN-Links definieren:

- Konfigurieren Sie einen vertrauenswürdigen öffentlichen Internet-WAN-Link im Rechenzentrum und an den Zweigstellen.
- Automatische Konfiguration von IPSec-Tunneln für Intranetdienste.

Bereitstellen von Zscaler im Citrix SD-WAN Center-Workflow

Im Folgenden werden die High-Level-Schritte beschrieben, die den Workflow für die Bereitstellung von Zscaler in SD-WAN Center definieren.

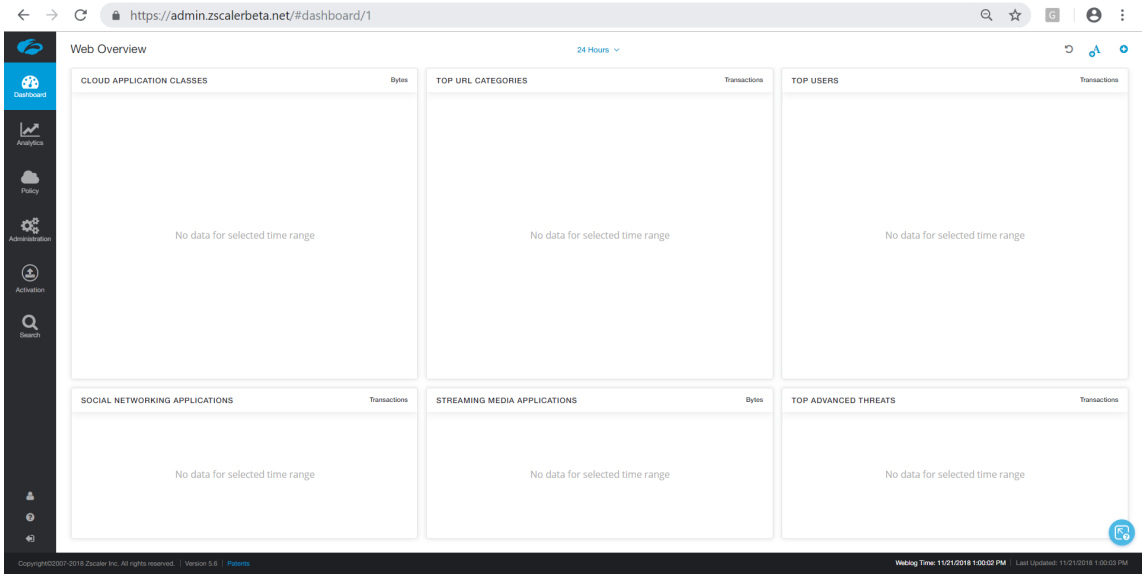
1. Konfigurieren Sie das Zscaler-Abonnement für SD-WAN Center (einmalig). Melden Sie sich bei derZscalerSite an, um Abonnementinformationen zu erhalten.
2. Wählen Sie In Citrix SD-WAN Center GUI **bereitstellen** aus.
   - Stellen Sie die Konfiguration für die Site mithilfe von Internet-WAN-Link und vorkonfiguriertem Anwendungsobjekt bereit.

- Konnektivität herstellen.
- Abrufen/Aktualisieren des IPSec-Status.

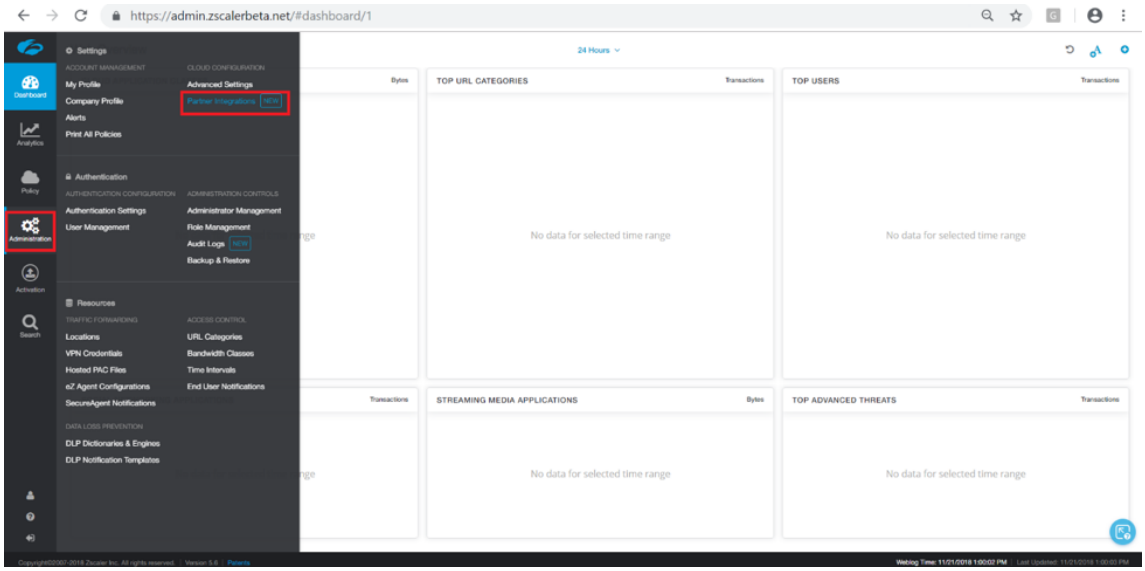
Zscaler-Abonnement

Bevor Sie mit der Konfiguration von Zscaler im SD-WAN Center fortfahren, müssen Sie sich im Zscaler-Portal anmelden.

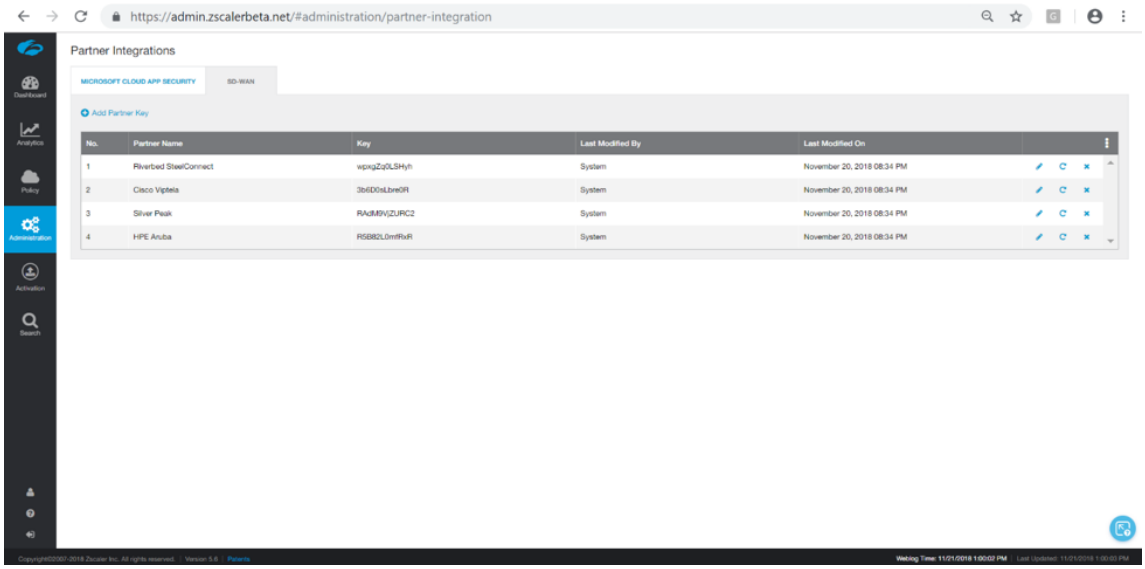
1. Melden Sie sich bei derZscalerSite an, um Abonnementinformationen zu erhalten. Die Seite Dashboard wird geöffnet.

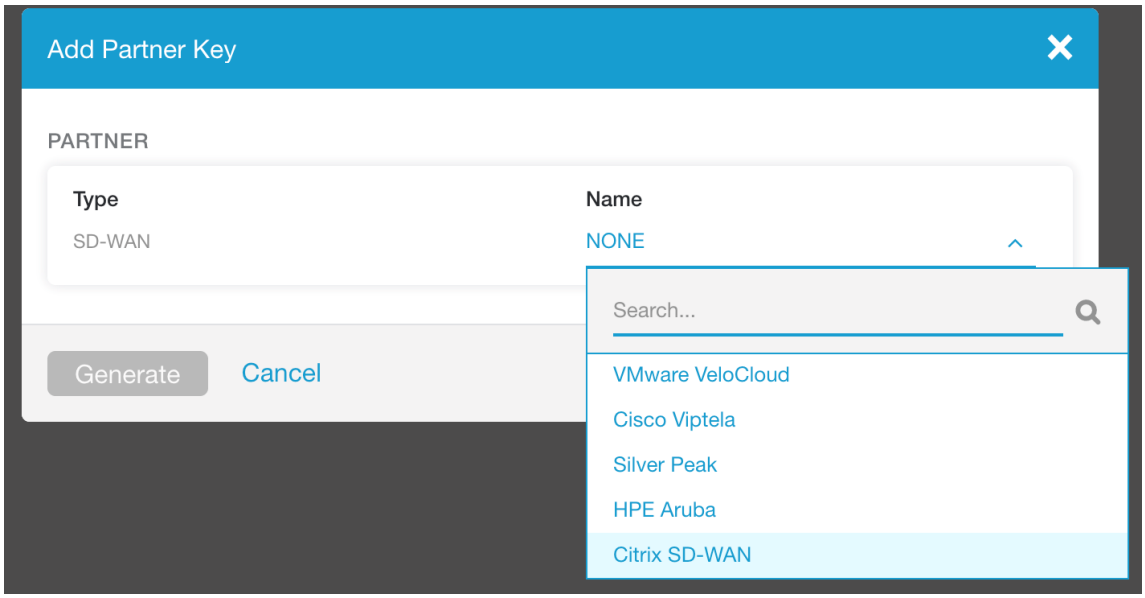


2. Klicken Sie auf **Administration > Partnerintegrationen**.



3. Wählen Sie auf der Seite **Partnerintegrationen** die Option **SD-WAN** aus. Klicken Sie auf **Partnerschlüssel hinzufügen**.



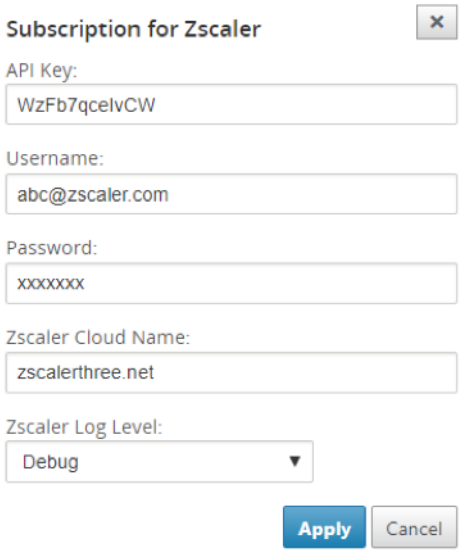


4. Wählen Sie **Citrix SDWAN** als Partnerschlüssel aus, und klicken Sie auf **Generieren**. Speichern Sie den Schlüssel.

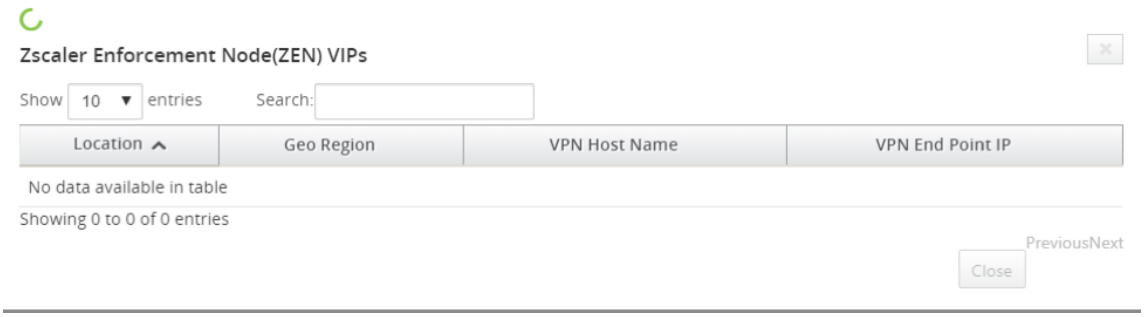
Konfigurieren von Zscaler in Citrix SD-WAN Center

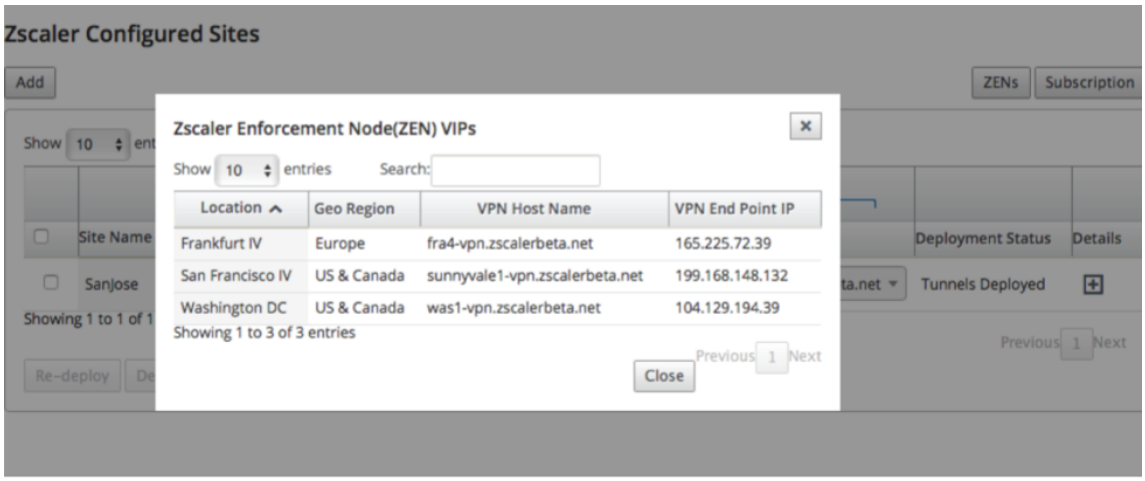
1. Navigieren Sie in der Citrix SD-WAN Center GUI zur Seite **Konfiguration > Sicherheit**. Die Seite **Zscaler Konfigurierte Sites** wird geöffnet.
2. Klicken Sie auf **Abonnement**. Geben Sie die Zscaler API (Partnerschlüssel) ein, die in den vorangegangenen Schritten erstellt wurde. Geben Sie für Zscaler **Benutzernamen** und **Kennwort**

ein. Wählen Sie **Zscaler Cloud Name**, **Zscaler Log Level**, und klicken Sie auf **Übernehmen**.

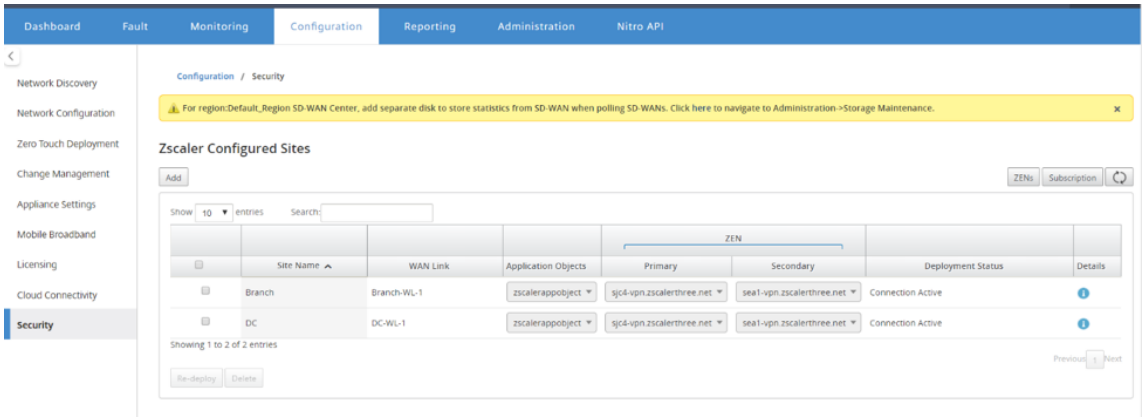


3. Zens stellt die Liste der verfügbaren VPN-Endpunkte für dieses Zscaler Cloud-Abonnement bereit.

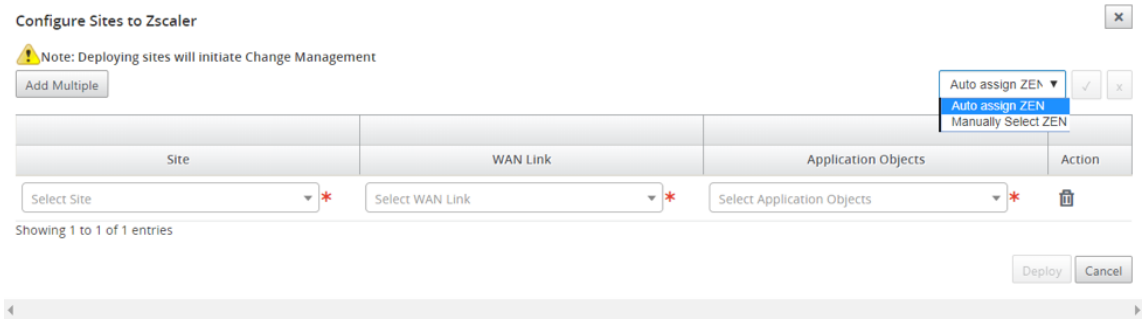




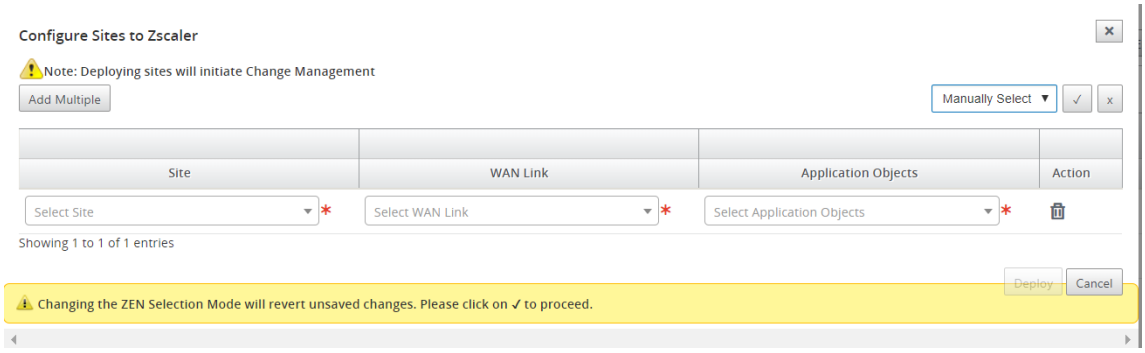
4. Nachdem Sie das Zscaler-Abonnement und die ZEN-Details eingegeben haben, können Sie mit dem Hinzufügen von Sites zu Zscaler beginnen. Klicken Sie auf **Hinzufügen**.



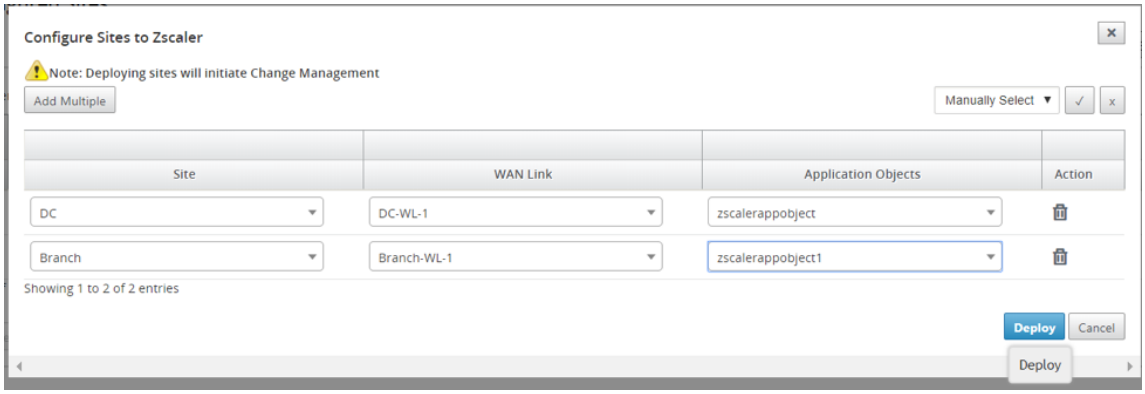
5. Fügen Sie im Dialogfeld **Sites für Zscaler konfigurieren** die **Site**, den WAN-Link und **Application Objects** hinzu. Standardmäßig ist die Option **ZEN automatisch zuweisen** ausgewählt.

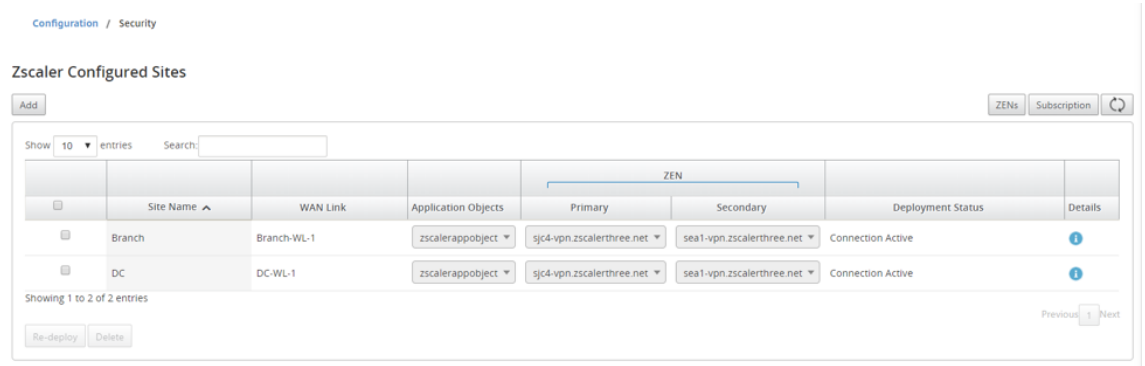


Sie können **ZEN manuell auswählen**. Die folgende Meldung wird jedoch angezeigt, dass nicht gespeicherte Änderungen verloren gehen.



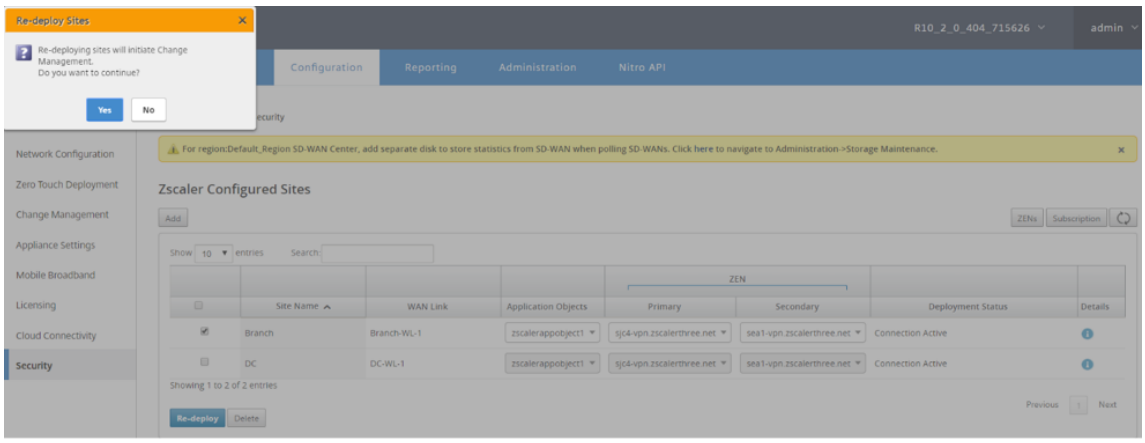
6. Wählen Sie die gewünschten Sites aus, und klicken Sie auf **Bereitstellen**. Sie können mehrere Sites hinzufügen, indem Sie **Mehrere hinzufügen**auswählen. Die ausgewählten Sites werden bereitgestellt und die Konfigurationsseite wird angezeigt.



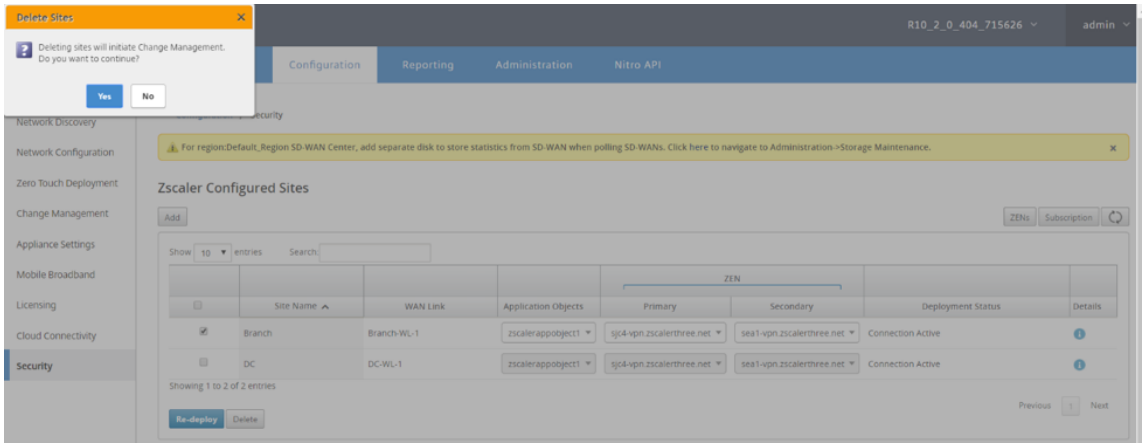


Beachten Sie, dass die primären und sekundären ZEN-IP-Adressen ausgefüllt sind und der Bereitstellungsstatus **Verbindung aktiv**ist.

7. Klicken Sie auf **Erneut bereitstellen**, wenn Sie Änderungen an den VPN-Endpunkten oder Anwendungsobjekten der konfigurierten Site vornehmen. Alle Änderungen an den konfigurierten Standorten im SD-WAN-Center lösen einen **Änderungsverwaltungsprozess** für die Appliances aus, die an den Zweigstandorten und DC-Sites konfiguriert sind.

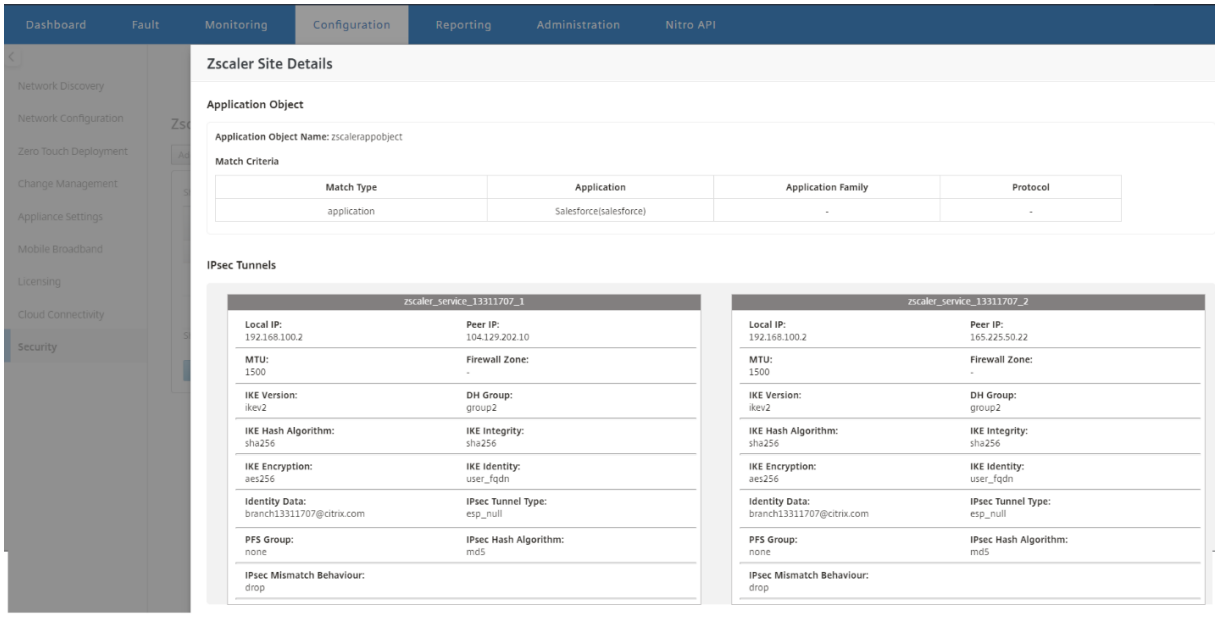


Durch das Löschen von Sites wird auch der Änderungsverwaltungsprozess ausgelöst.



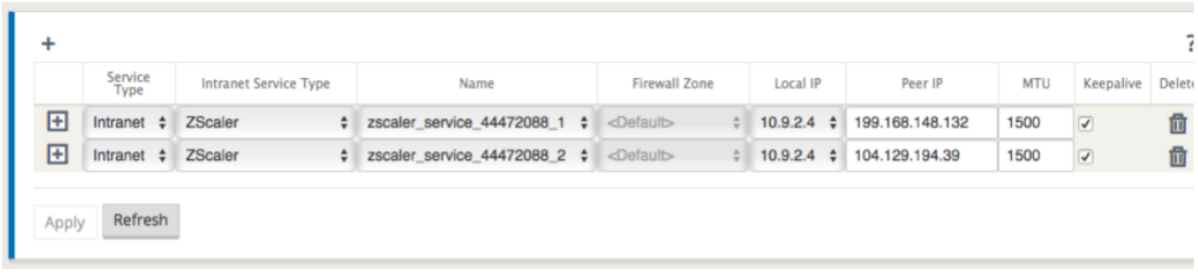
Überwachung und Fehlersuche

Wählen Sie konfigurierte Sites aus, um weitere Informationen zu Anwendungsobjekten und primären/sekundären IP-Adressen anzuzeigen. Durch Klicken auf das Symbol **Details** können Sie vollständige Informationen über die konfigurierten Sites anzeigen.



IPSec-Tunnelkonfiguration

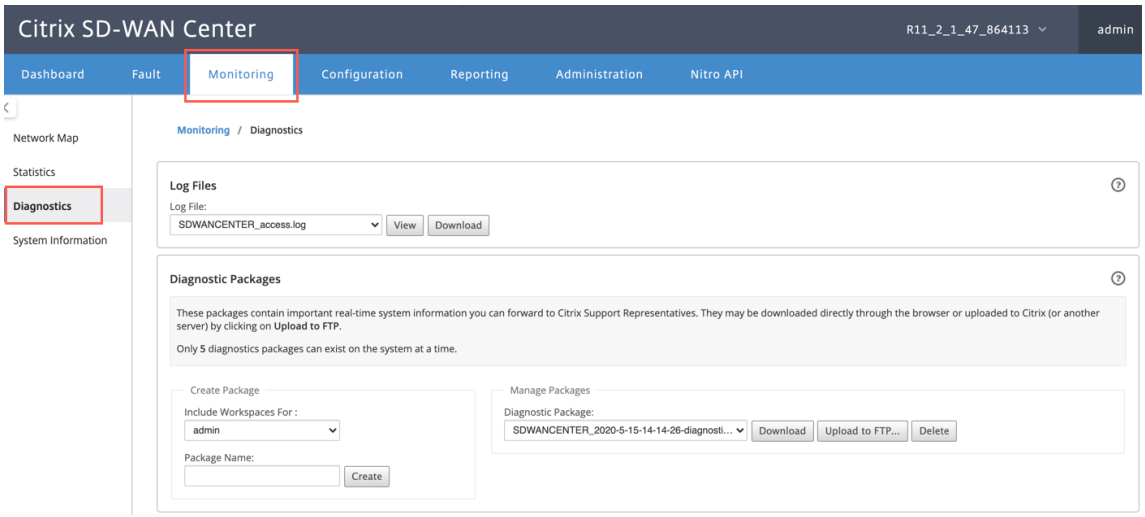
Die Seite Details in der SD-WAN Center GUI enthält Informationen zur IPSec-Tunnelkonfiguration für primäre und sekundäre Endpunkte. Die Peer-IP wird von Zscaler abgerufen. Überprüfen Sie die IPSec-Tunnelkonfiguration im GUI-Konfigurationseditor der SD-WAN-Appliance.



Sie können die Zscaler-Protokolle anzeigen und herunterladen, mit denen Probleme im Citrix SD-WAN Center behandelt werden.

Anzeigen von Zscaler-Protokolldateien:

1. Klicken Sie Citrix SD-WAN Center-Webinterface auf die Registerkarte **Überwachung** > **Diagnose**.



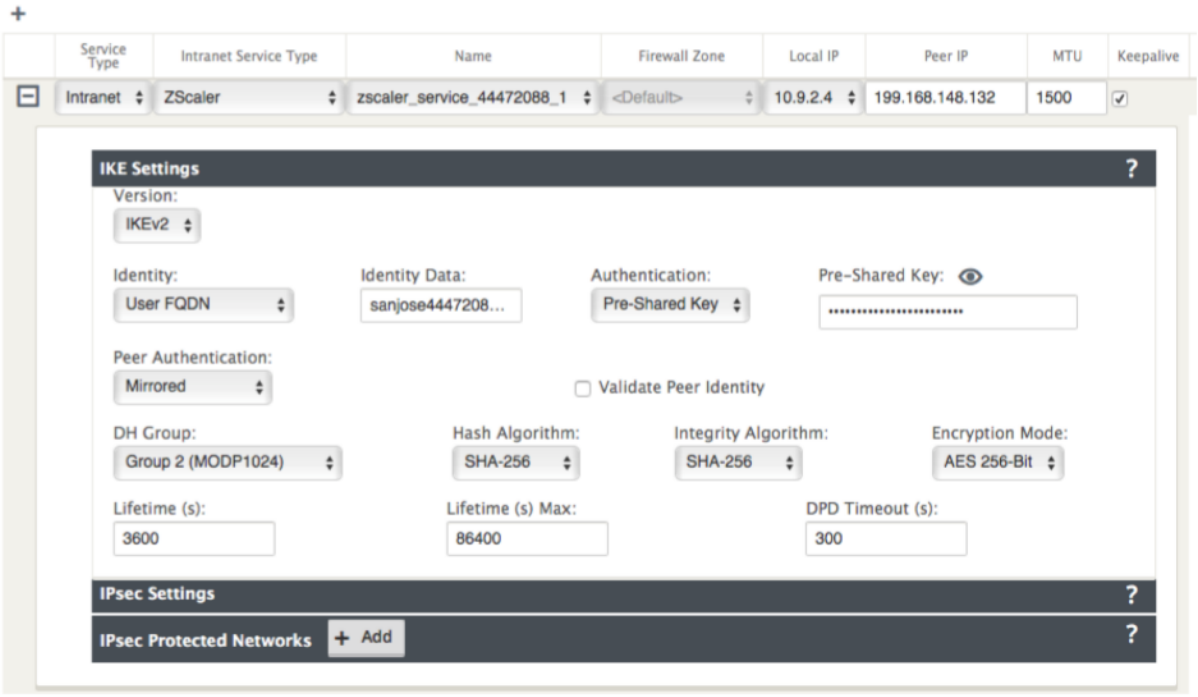
2. Wählen Sie in der Dropdownliste **Protokolldatei** die Zscaler-Protokolldatei aus, die Sie anzeigen möchten. Klicken Sie **auf Ansicht**.
3. Wenn Sie die Protokolldateien auf Ihren Computer herunterladen möchten, klicken Sie auf **Herunterladen**.

IKE-Einstellungen

Die folgenden IKE/IPsec -Einstellungen werden für die IPSec-Tunnelkonfiguration in der SD-WAN-Appliance ausgewählt. Weitere Informationen zum Konfigurieren von IPSec-Tunnel —IKE-Einstellungen finden Sie unter;Konfigurieren des IPSec-Tunnels zwischen SD-WAN und Drittanbieter-GerätenThema.

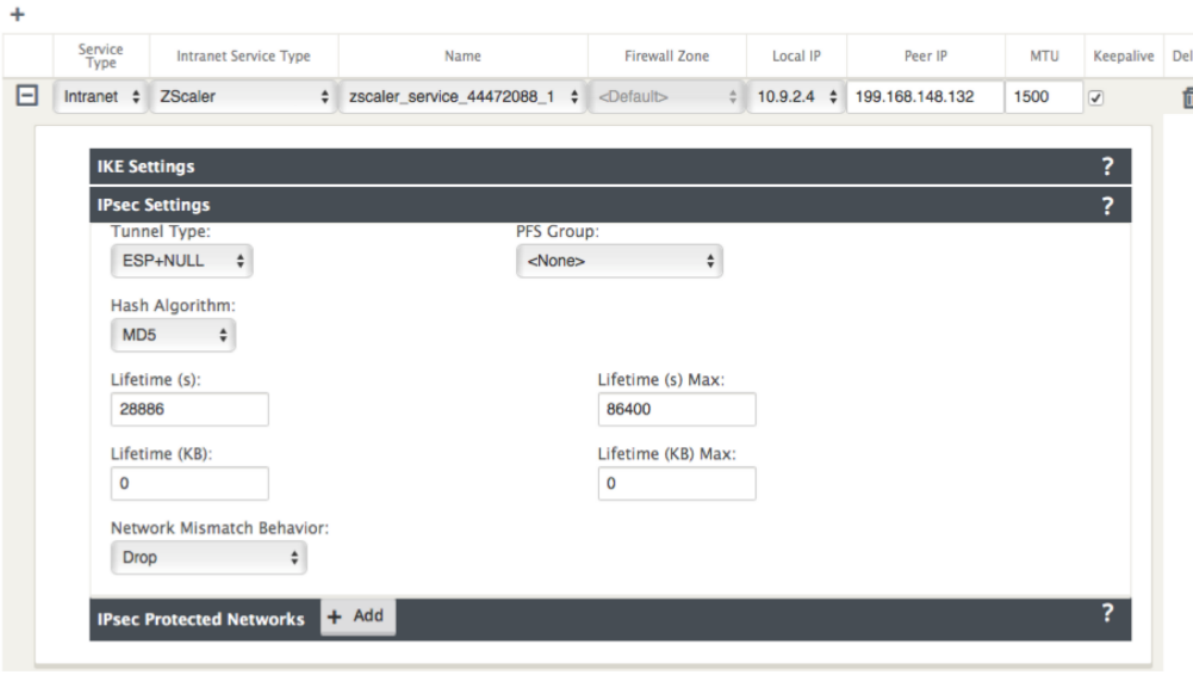
- IKE-Version - IKEv2
- IKE-Identität —Benutzer-FQDN
- Hashalgorithmus - SHA-256

- Integritätsalgorithmus —SHA-256
- Verschlüsselungsmodus —AES 256 Bits
- IPsec —Tunnelmodus
- IPSec-Verschlüsselung —Null



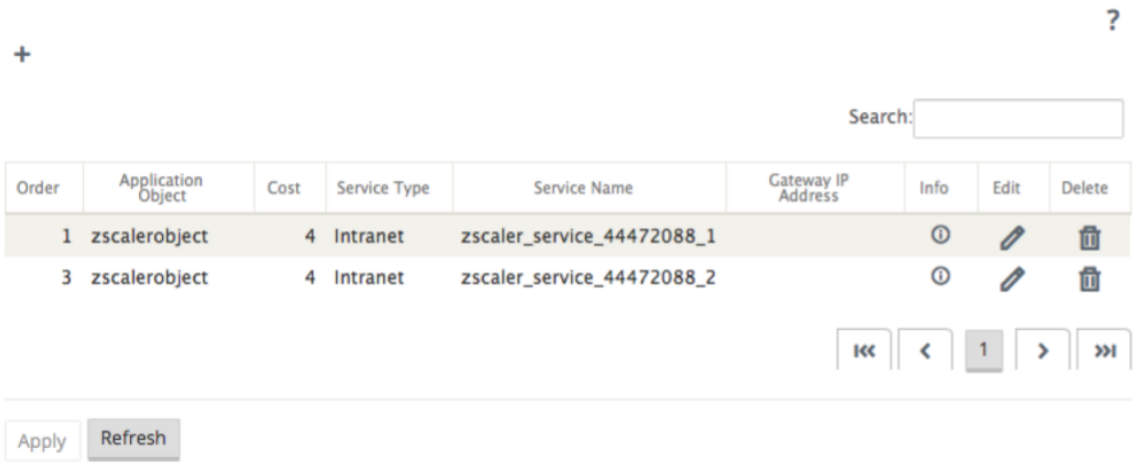
IPsec-Einstellungen

Weitere Informationen zum Konfigurieren der IPSec-Tunneleinstellungen finden Sie unter Konfigurieren des IPSec-Tunnels zwischen SD-WAN und Drittanbieter-Geräten.



Anwendungsobjekte

Stellen Sie sicher, dass Anwendungsobjekte konfiguriert sind. Weitere Informationen zum Konfigurieren von Anwendungsrouten finden Sie unter Anwendungsklassifizierung.



> **Hinweis**
>
> Die GRE-Tunnelkonfiguration wird nicht als Teil des automatisierten Workflows unterstützt. Die manuelle Konfiguration ist jedoch weiterhin zulässig. Weitere Informationen finden Sie unter Zscaler Integration mit GRE-Tunneln und IPsec-Tunneln.

Überwachen

April 13, 2021

Mit dem Citrix SD-WAN Center Dashboard können Sie die SD-WAN-Netzwerkstatistiken und -diagramme in einem einzigen Bereich anzeigen. Weitere Informationen finden Sie unter Dashboard.

Sie können auch das SD-WAN-NetzwerkEreignisseundBerichtein Citrix SD-WAN Center anzeigen.

Monitoring verwandte Artikel:

Diagnose-Pakete

Ereignisbenachrichtigungen

Protokolldateien

Speicherabbilder

Abrufintervall

Statistik

Systeminformationen

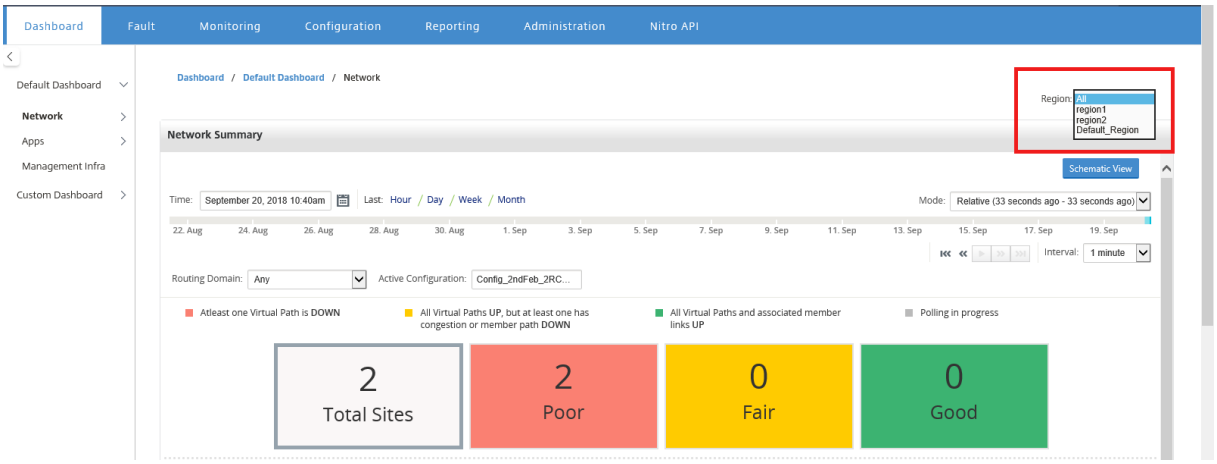
Dashboard

April 13, 2021

Das Citrix SD-WAN Center Dashboard zeigt eine Teilmenge der allgemeinen Statistiken auf einen Blick an. Für eine Bereitstellung mit einer einzelnen Region werden die Statistiken vom MCN abgerufen, das in Citrix SD-WAN Center erkannt wird. Für eine Bereitstellung mit mehreren Regionen werden die Statistiken von allen regionalen Citrix SD-WAN Center Collectors für das ausgewählte Zeitintervall abgerufen. Sie können die folgenden Statistiken anzeigen:

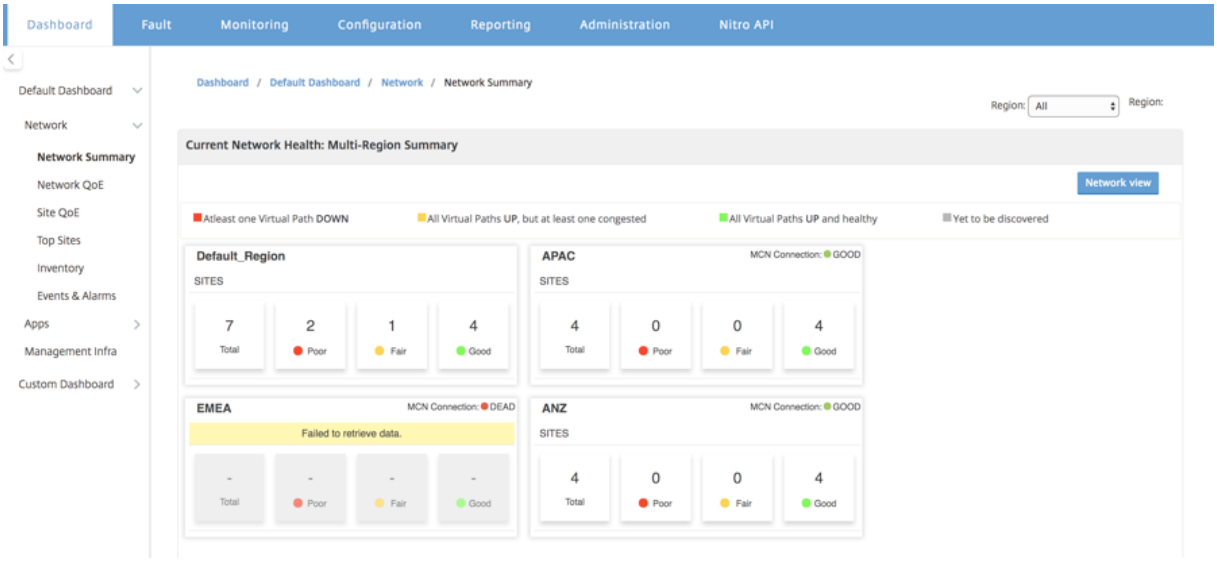
- Netzwerkübersicht
- Netzwerk QoE
- Topsites
- Inventar
- Ereignisse und Alarme
- Top-Apps
- HDX QoE
- Verwaltungsinfra

Bei einer Bereitstellung mit einer einzelnen Region werden die Standardregionsstatistiken auf dem Dashboard angezeigt. Bei einer Bereitstellung mit mehreren Regionen können Sie das Dashboard mit mehreren Regionen oder das regionale Dashboard anzeigen. Um das Dashboard mit mehreren Regionen anzuzeigen, wählen Sie im Menü **Region** die Option **Alle** aus.



Sie können den MCN-Verbindungsstatus auf jeder Regionskachel anzeigen. Der MCN-Verbindungsstatus ist der Integritätsstatus des virtuellen Pfads zwischen einem RCN und dem MCN.

> **Hinweis**
>
> Bei einer Bereitstellung mit mehreren Regionen enthalten die Standardregionsstatistiken Statistiken aller vom MCN verwalteten Standorte. Es kann auch RCN-Statistiken enthalten, da die RCNs virtuelle Pfade zum MCN haben.
>
> Das Dropdownmenü **Region** ist in Citrix SD-WAN Center Collectors nicht verfügbar.



Das Citrix SD-WAN Center Dashboard wird basierend auf dem konfigurierten Abrufintervall aktualisiert. Das Standardabrufintervall beträgt fünf Minuten. Weitere Informationen finden Sie unter

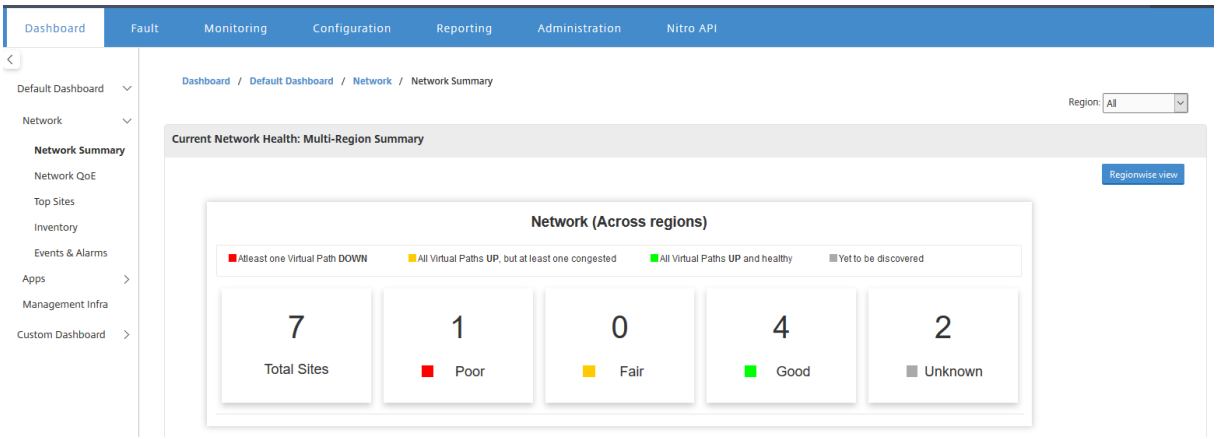
Abrufintervall.

Netzwerkübersicht

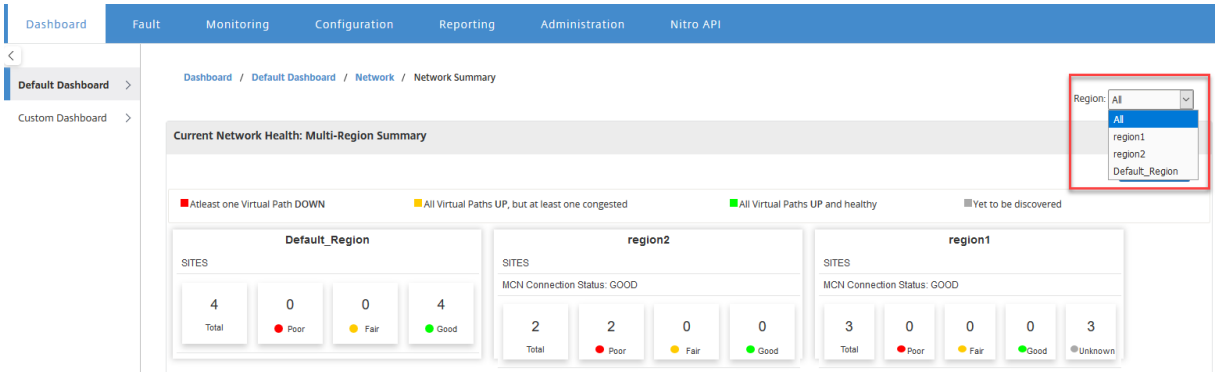
Bei einer Bereitstellung mit mehreren Regionen bietet das Widget "**Netzwerkübersicht"** einen Überblick über den Netzwerkzustand in allen Regionen. Eine Regionskarte für jede Region im Netzwerk wird mit folgenden Informationen angezeigt:

- Die Gesamtzahl der Standorte in der Region.
- Die Anzahl der Standorte im Status "Schlecht". Eine Site hat den Status "Schlecht", wenn mindestens ein virtueller Pfad "DOWN"ist.
- Die Anzahl der Standorte im Status "Fair". Eine Site hat den Status "Fair", wenn alle virtuellen Pfade in der Site UP sind, aber mindestens ein Pfad hat ein Überlastungsproblem oder ein Mitgliedspfad ist DOWN.
- Die Anzahl der Standorte im Status "Gut". Eine Site hat den Status Gut, wenn alle virtuellen Pfade und die zugeordneten Elementpfade UP sind.
- Die Anzahl der Sites im Status Unbekannt. Eine Site hat den Status Unbekannt, wenn die Abfrage ausgeführt wird.

Um die Netzwerkzusammenfassung mit mehreren Regionen anzuzeigen, navigieren Sie zu **Dash** board > **Standard-Dashboard** > **Netzwerk** > **Netzwerkübersicht**, und wählen Sie im Dropdownmenü **Region** die Option **Alle** aus.



Standardmäßig wird der Bildschirm in der **Netzwerkansicht**angezeigt. Sie können den aktuellen Netzwerkzustand der Netzwerkzusammenfassung mit mehreren Regionen anzeigen, indem Sie auf die **Regionsansicht**klicken. Sie können auch den MCN-Verbindungsstatus auf jeder Regionskachel anzeigen.



Klicken Sie auf eine Regionskarte, um einen Drilldown in das regionale Dashboard anzuzeigen.

Für eine einzelne Region bietet das Widget **Netzwerkübersicht** einen Überblick über den Netzwerkzustand der ausgewählten Region.

Um die regionale Netzwerkzusammenfassung anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk**> **Netzwerkübersicht**, und wählen Sie im Dropdownmenü **Region** eine **Region** aus.

Sie können die regionale Netzwerkübersicht entweder in der Kachelansicht oder in der Schemaansicht anzeigen.

Sie können das Timeline-Control verwenden, um die Netzwerkstatusübersicht für einen ausgewählten Zeitraum anzuzeigen. Sie können den Netzwerkstatus auch über einen Zeitraum abspielen oder pausieren.

Modus hilft, die Zeit als ein relatives oder ein absolutes Konzept zu sehen.

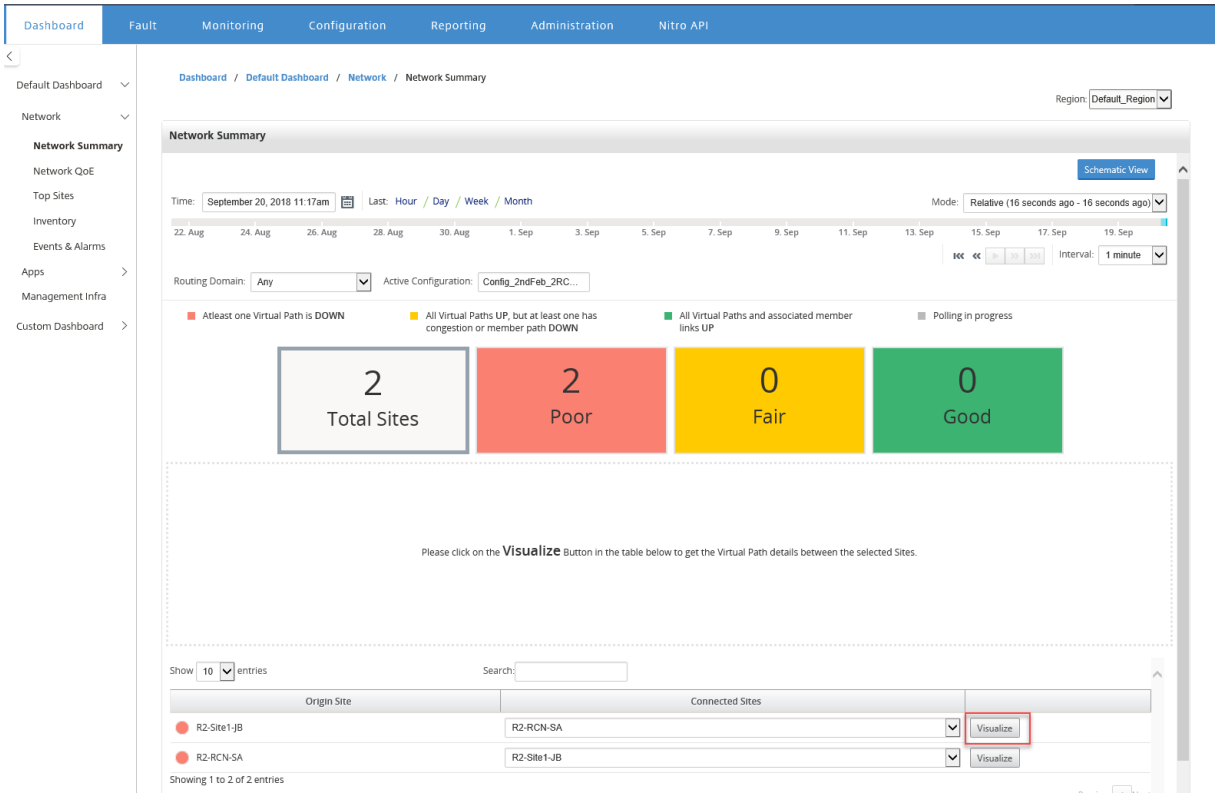
Weitere Informationen zu Zeitleiste und Modus finden Sie unterZeitleisten-Steuerelemente.

Kachelansicht

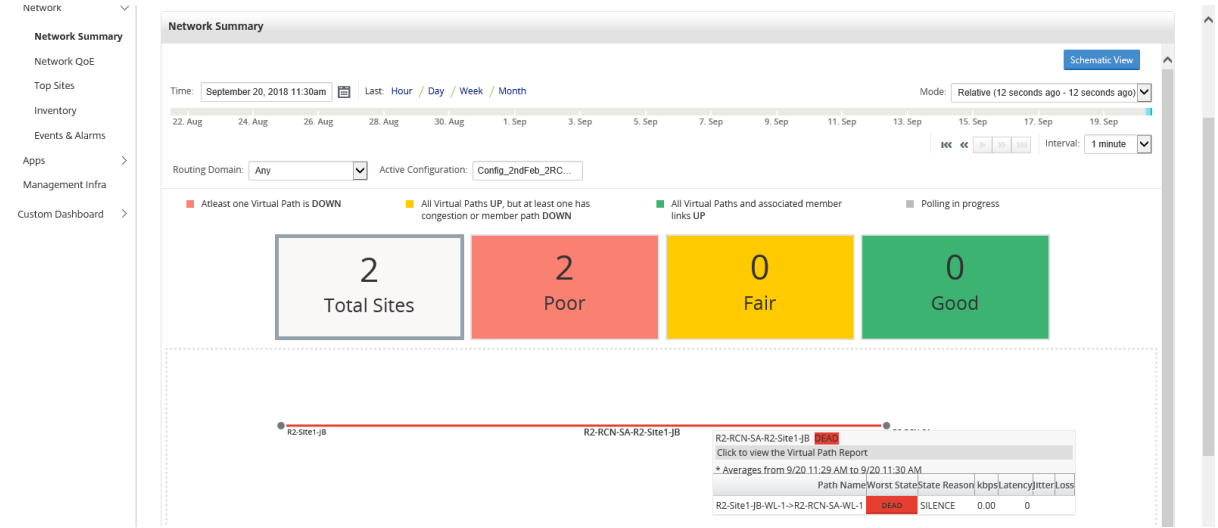
Die Kachelansicht enthält folgende Informationen:

- Die Gesamtzahl der Standorte in der Region.
- Die Anzahl der Standorte im Status “Schlecht”. Eine Site hat den Status “Schlecht”, wenn mindestens ein virtueller Pfad “DOWN”ist.
- Die Anzahl der Standorte im Status “Fair”. Eine Site hat den Status “Fair”, wenn alle virtuellen Pfade in der Site UP sind, aber mindestens ein Pfad hat ein Überlastungsproblem oder ein Mitgliedspfad ist DOWN.
- Die Anzahl der Standorte im Status “Gut”. Eine Site hat den Status Gut, wenn alle virtuellen Pfade und die zugeordneten Elementpfade UP sind.
- Die Anzahl der Sites im Status Unbekannt. Eine Site hat den Status Unbekannt, wenn die Abfrage ausgeführt wird.

Um eine grafische Darstellung eines Pfades zwischen zwei Standorten anzuzeigen, wählen Sie den Pfad aus und klicken Sie auf **Visualisieren**.



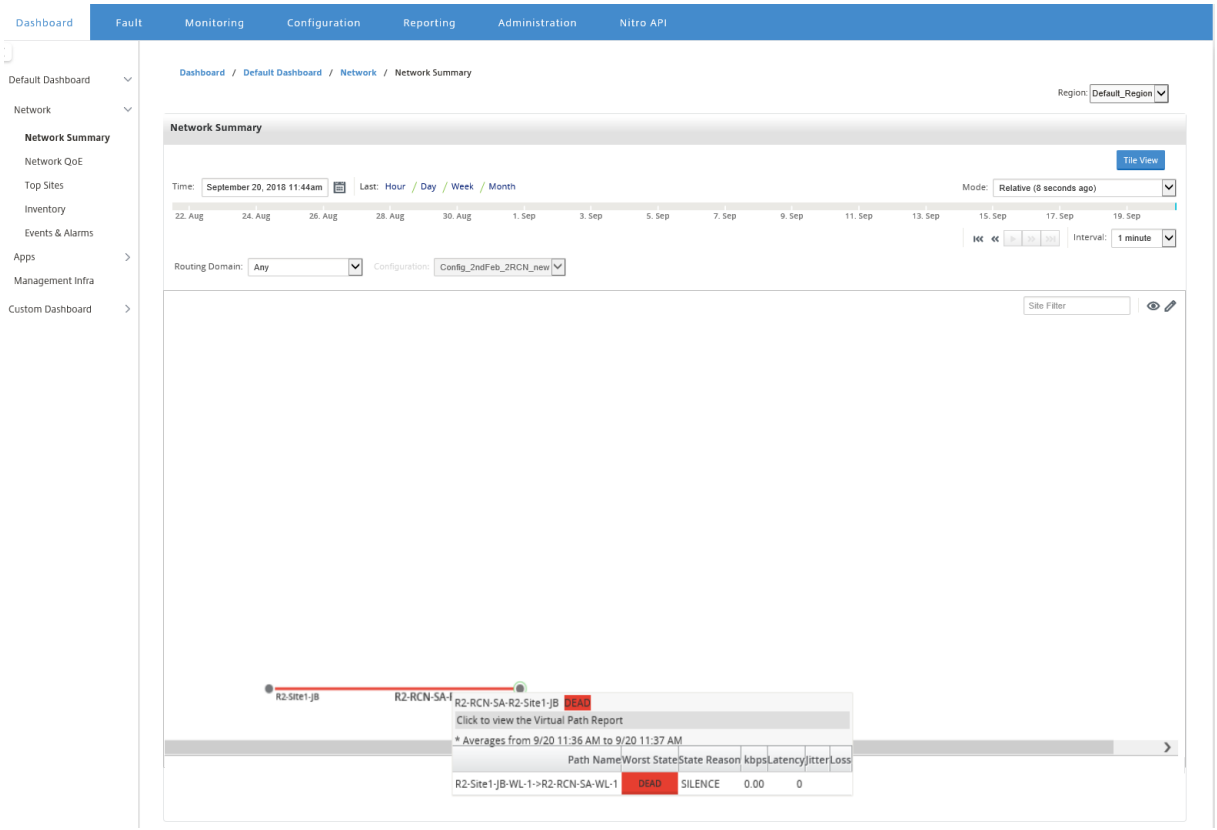
Bewegen Sie den Mauszeiger über die Sites oder den Pfad, um weitere Details anzuzeigen. Klicken Sie auf die Sites, um Berichtsoptionen anzuzeigen und auszuwählen.



Schematische Ansicht

Die schematische Ansicht bietet eine grafische Ansicht des SD-WAN-Netzwerks. Die in diesem Abschnitt angezeigten Informationen werden je nach ausgewählter Konfiguration und Routingdomäne aktualisiert. Um hier eine Netzwerkzuordnung anzuzeigen, müssen Sie die Netzwerkkonfiguration und Netzwerkzuordnungen aus dem Master Controller Node (MCN) importieren. Weitere Informationen siehe MCN-Konfiguration importieren.

Bewegen Sie den Mauszeiger über die Sites oder den Pfad, um weitere Details anzuzeigen. Klicken Sie auf die Sites, um Berichtsoptionen anzuzeigen.

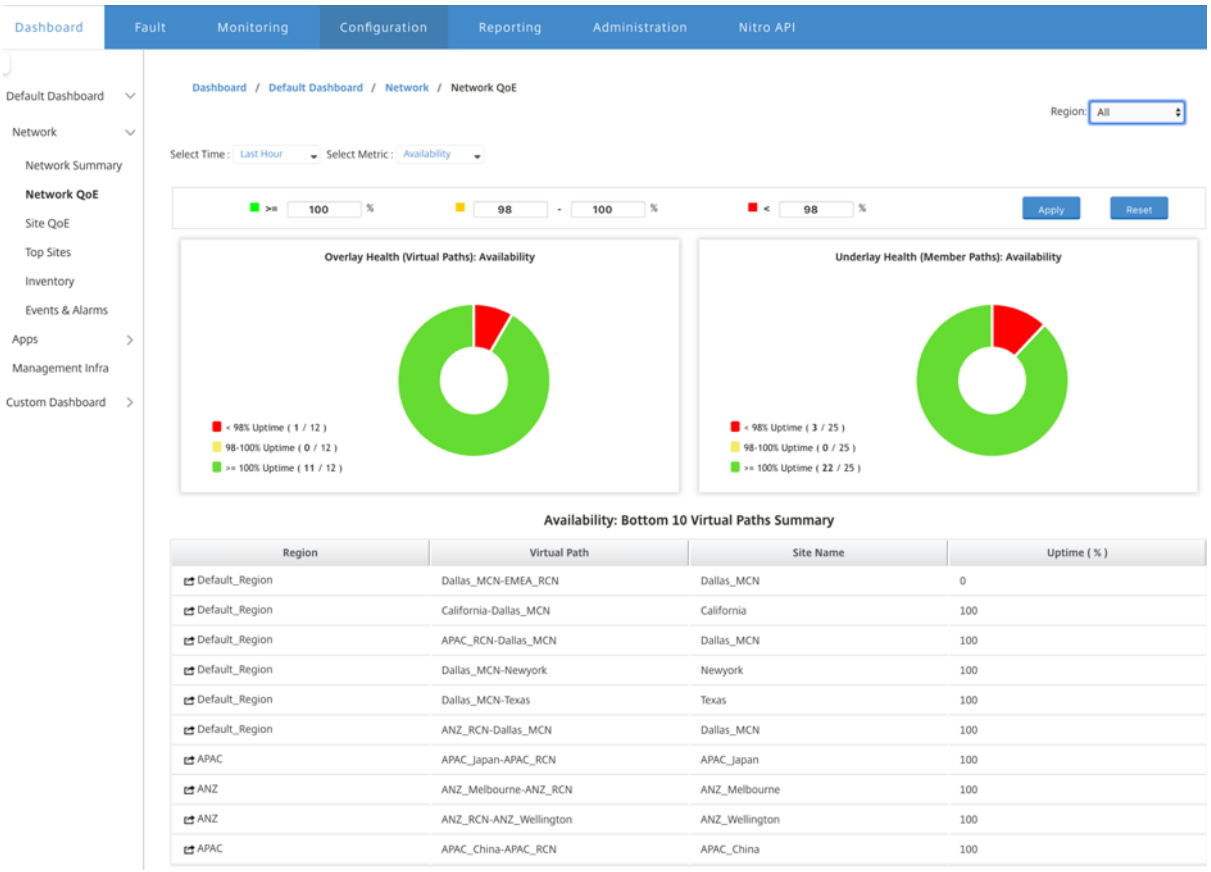


Netzwerk QoE

Das **Netzwerk-QoE-** Widget bietet eine grafische Darstellung der Verfügbarkeits-, Verlust-, Latenz- und Jitter-Parameter eines virtuellen Pfads. Es stellt die Statistiken sowohl für den überlagerten virtuellen Pfad als auch für die unterlagerten Elementpfade bereit.

Bei einer Bereitstellung mit mehreren Regionen können Sie je nach ausgewählter Metrik eine Liste der unteren 10 virtuellen Pfade anzeigen. Die virtuellen Pfaddaten werden von allen regionalen Kollektoren für das ausgewählte Zeitintervall erfasst. Sie können die Bandbreiten-, Jitter-, Verlust- und Überlastungsdetails der virtuellen Pfade anzeigen, die Ihre Aufmerksamkeit am meisten erfordern.

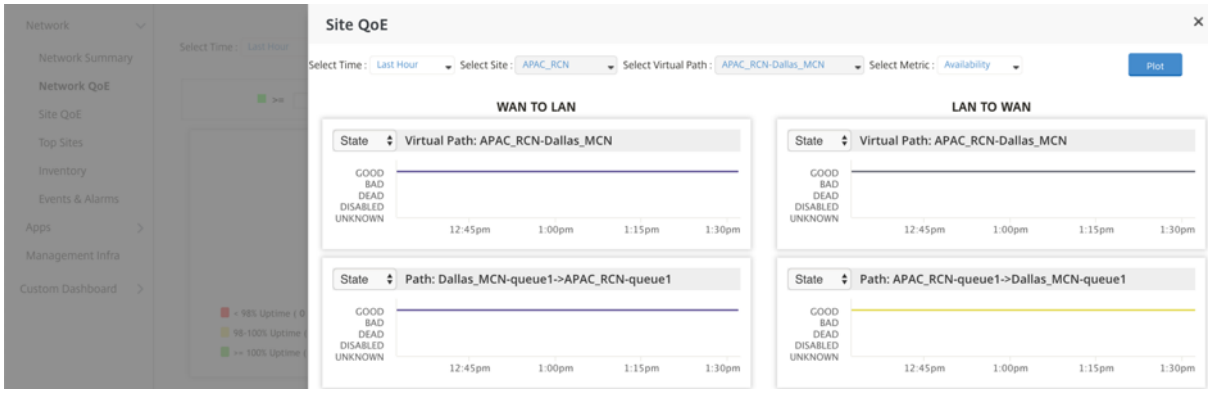
Um die Integrität virtueller Pfade für mehrere Regionen anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk** > **Netzwerk-QoE** und wählen Sie im Dropdownmenü **Region** die Option **Alle** aus.



Für eine einzelne Region können Sie je nach ausgewählter Metrik eine Liste der unteren 10 virtuellen Pfade anzeigen. Die Statistiken werden für das ausgewählte Zeitintervall erfasst. Sie können die Bandbreiten-, Jitter-, Verlust- und Überlastungsdetails der virtuellen Pfade anzeigen, die Ihre Aufmerksamkeit am meisten erfordern.

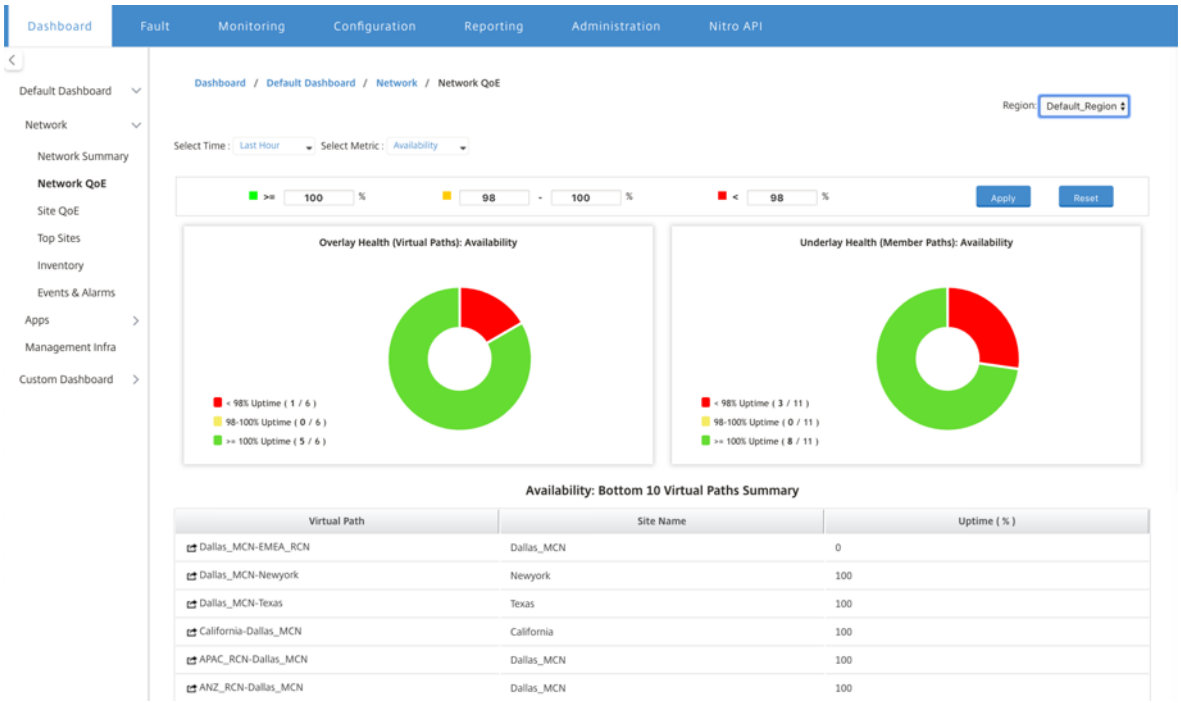
Sie können die Overlay- und Underlay-Pfade für die ausgewählte Metrik (Verfügbarkeit, Verlust, Jitter, Latenz) über das ausgewählte Zeitintervall vergleichen. Sie können auch benutzerdefinierte Schwellenwerte für die Metriken festlegen und diese speichern, wenn Sie auf **Übernehmen** klicken. Klicken Sie auf **Zurücksetzen**, um die Standardgrenzwerte zu speichern.

Der Benutzer kann auch einen Drilldown zu einem beliebigen virtuellen Pfad in der Tabelle verwenden, indem er auf der **Drilldown-** Schaltfläche links neben jeder Zeile verwendet. Ein **Site-QoE** wird mit dem detaillierten Vergleich zwischen dem Conduit und den zugrunde liegenden Elementpfaden angezeigt.



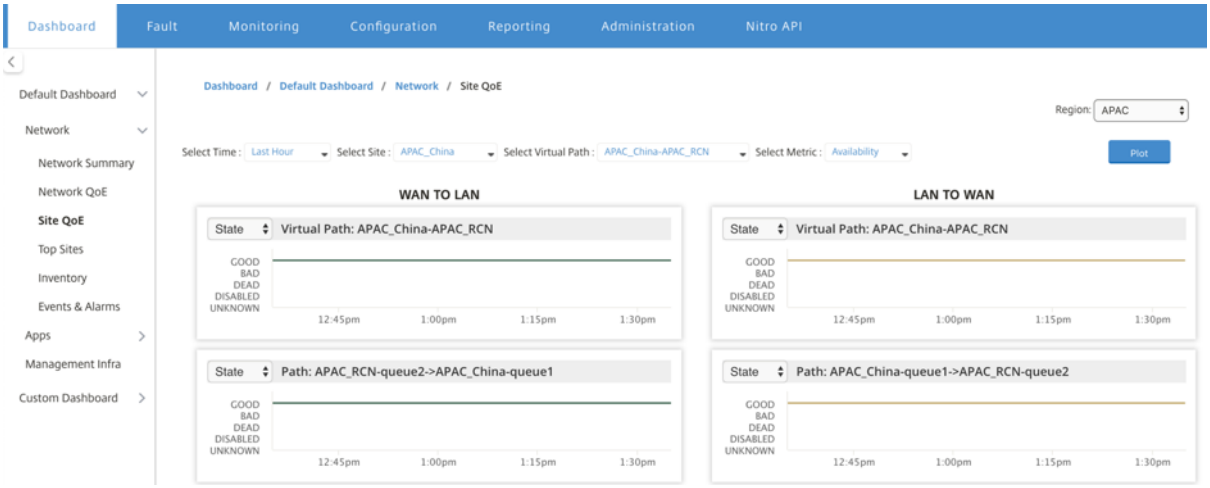
Im Schieberegler werden der Sitename und der virtuelle Pfad standardmäßig ausgewählt, abhängig von der Zeile, auf die Sie geklickt haben, und er wird deaktiviert. Der Benutzer kann jedoch einen anderen Zeitbereich und eine andere Metrik auswählen und auf die Option **Plot** klicken, um die neuen Diagramme zu plotten.

Um regionale Gesundheitsstatistiken für virtuelle Pfade anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk**> **Netzwerk-QoE** und wählen Sie im Dropdownmenü **Region** eine Region aus.



Standort QoE

Sie können Site QoE als Werkzeug verwenden, um den virtuellen Pfad mit den zugrunde liegenden Elementpfaden zu vergleichen. Sie müssen eine Site und einen beliebigen virtuellen Pfad von dieser Site und Metrik auswählen.Klicken Sie auf **Plot**.

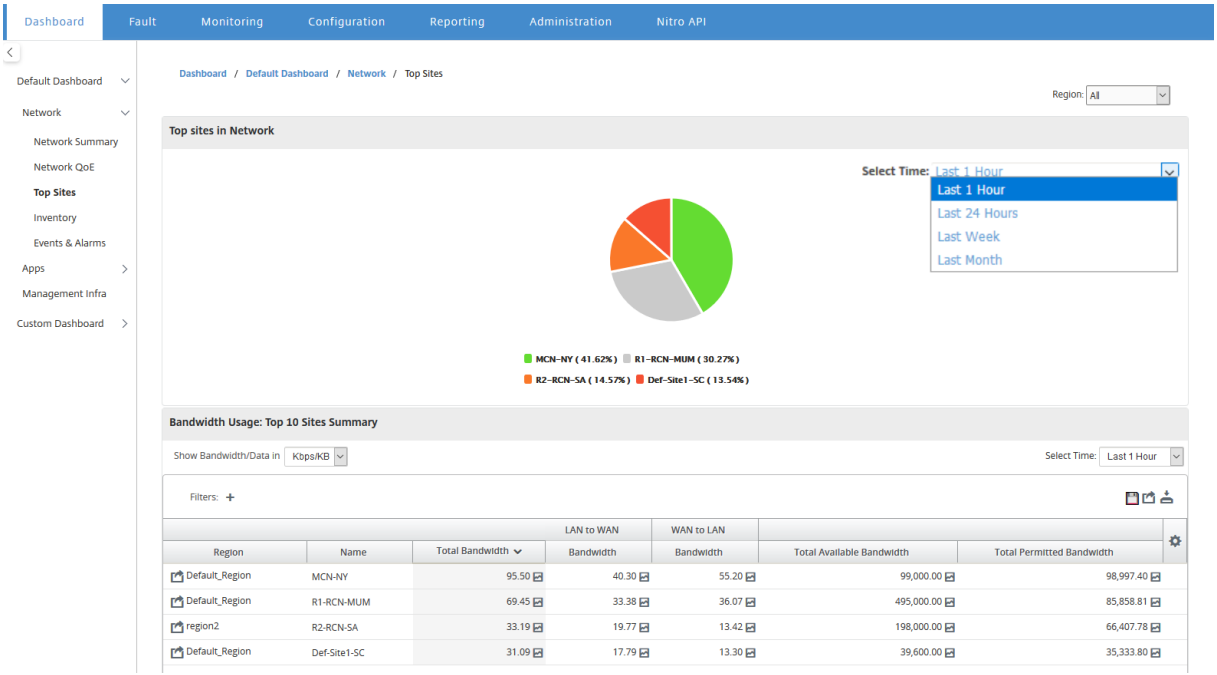


Im ersten Abschnitt werden die Statistiken der virtuellen Pfade in **WAN zu LAN** und **LAN zu WAN** dargestellt. Im folgenden Abschnitt werden alle zugrunde liegenden Elementpfade Diagramme dargestellt. Beide Dinge sind sowohl auf regionaler als auch auf Netzwerkebene präsent.

Topsites

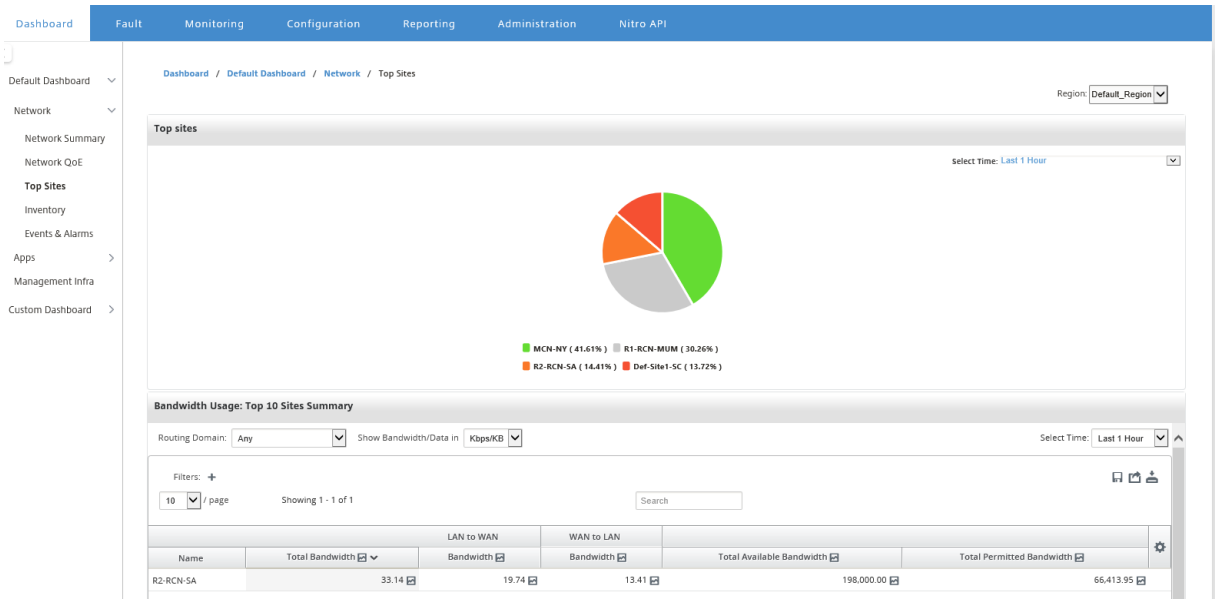
Bei einer Bereitstellung mit mehreren Regionen listet das Widget **Top Sites** die Top 10 Sites in allen Regionen mit der höchsten Bandbreitennutzung im ausgewählten Zeitintervall auf.

Um die obersten Sites in allen Regionen anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk** > **Top Sites** und wählen Sie im Dropdownmenü **Region** die Option **Alle** aus.



Klicken Sie auf eine Site oder Metrik, um detaillierte Berichte und Statistiken anzuzeigen.

Für eine einzelne Region zeigt das Widget “Top Sites”die Statistiken zur Bandbreitennutzung für alle Sites in der Region an. Die Statistiken werden für das ausgewählte Zeitintervall erfasst. Sie können die Standorte basierend auf der Routingdomäne filtern.



Inventar

Alle 30 Minuten sammelt der Inventory Manager die Hardwareinformationen aller Citrix SD-WAN-Appliances, die in Citrix SD-WAN Center entdeckt werden.

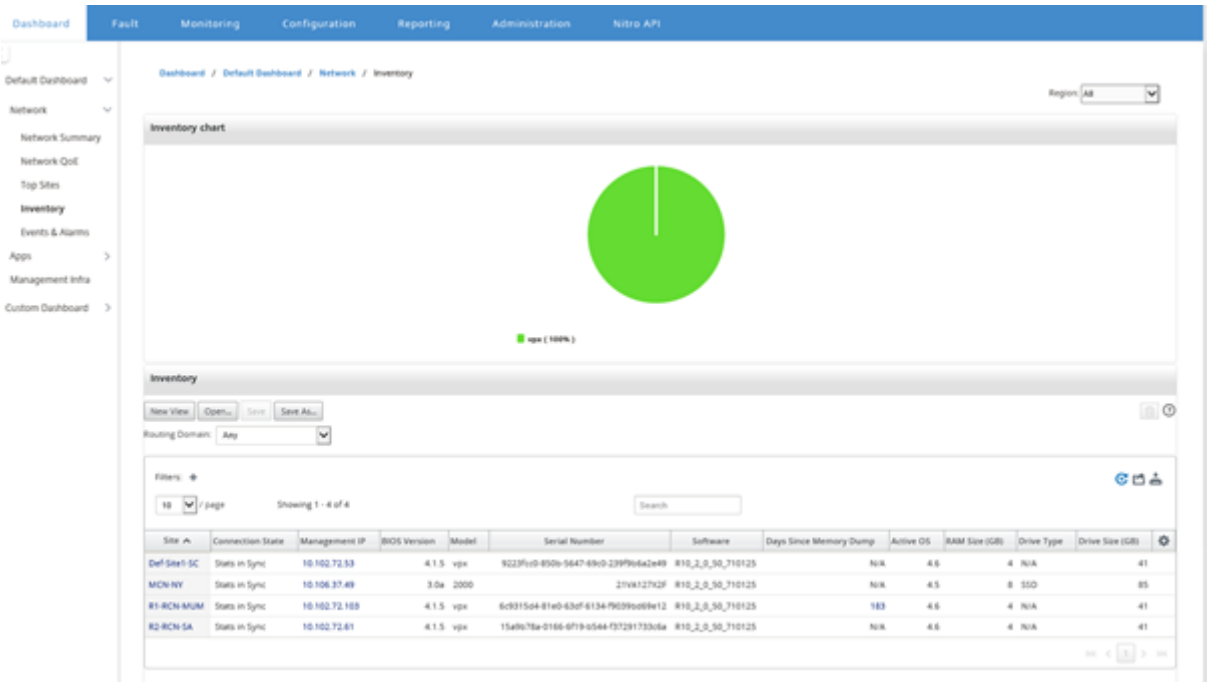
Um die mehrteiligen Inventarstatistiken anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk** > **Lagerbestand** und wählen Sie im Dropdownmenü **Region** die Option aus.

Um die Bestandsstatistiken einer bestimmten Region anzuzeigen, wählen Sie im Dropdown-menü Region die Region aus.

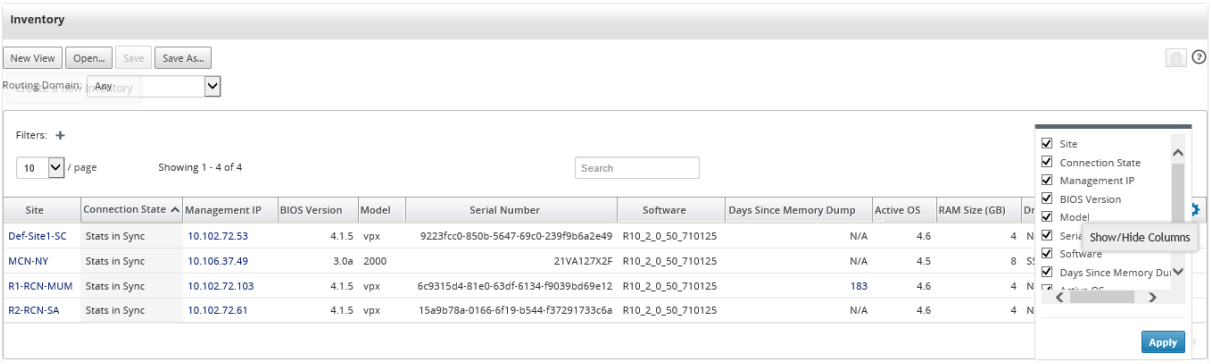
Sie können die folgenden Bestandsstatistiken anzeigen:

- **Site**: Name der Site, die in der Konfiguration gefunden wurde, die im MCN ausgeführt wird. Wenn es sich bei der Appliance um ein sekundäres MCN handelt, wird neben dem Namen “(sekundär)”angezeigt. Sie können auf den Namen klicken, um auf die Appliance-Webkonsole zuzugreifen.
- **Verbindungsstatus**: Konnektivitätsstatus zur Appliance. Ein rotes Symbol wird angezeigt, wenn die Verbindung nicht erreichbar oder nicht authentifiziert ist.
- **Management-IP**: Management-IP-Adresse der Appliance. Sie können auf die IP-Adresse klicken, um auf die Appliance-Webkonsole zuzugreifen.

- **BIOS-Version**: BIOS-Version der Appliance.
- **Modell**: Hardware-Modell des Geräts.
- **Seriennummer**: Seriennummer der Einheit.
- **Software**; Versionsnummer der SD-WAN-Software.
- **Tage seit Speicherabbild**: Zeit seit dem letzten Systemfehler Speicherabbild. Wenn die Appliance ihren Speicher in den letzten vier Tagen abgelegt hat, wird neben der Uhrzeit ein Fehlersymbol angezeigt. Wenn das Speicherabbild zwischen 5 und 10 Tagen aufgetreten ist, wird ein Warnsymbol angezeigt. N/A wird angezeigt, wenn kein Dump verfügbar ist. Durch Klicken auf die Uhrzeit wird die Log-Seite des SD-WAN geöffnet.
- **Aktive Betriebssysteme**: Das Betriebssystem, das derzeit auf der Appliance ausgeführt wird.
- **RAM-Größe (GB)**: Menge an RAM, der derzeit auf der Appliance in GB installiert ist.
- **Laufwerkstyp**: Typ des auf der Appliance installierten Datenspeicherlaufwerks. Der Wert kann SSD (Solid State Drive) oder HDD (Festplatte) sein.
- **Laufwerksgröße (GB)**: Größe des derzeit auf der Appliance installierten Datenspeicherlaufwerks in GB.



> **Hinweis**
>
> Sie können die Spalten für die Inventarstatistiktabelle anordnen, indem Sie die Option **Spalten ein-/ausblenden** verwenden.



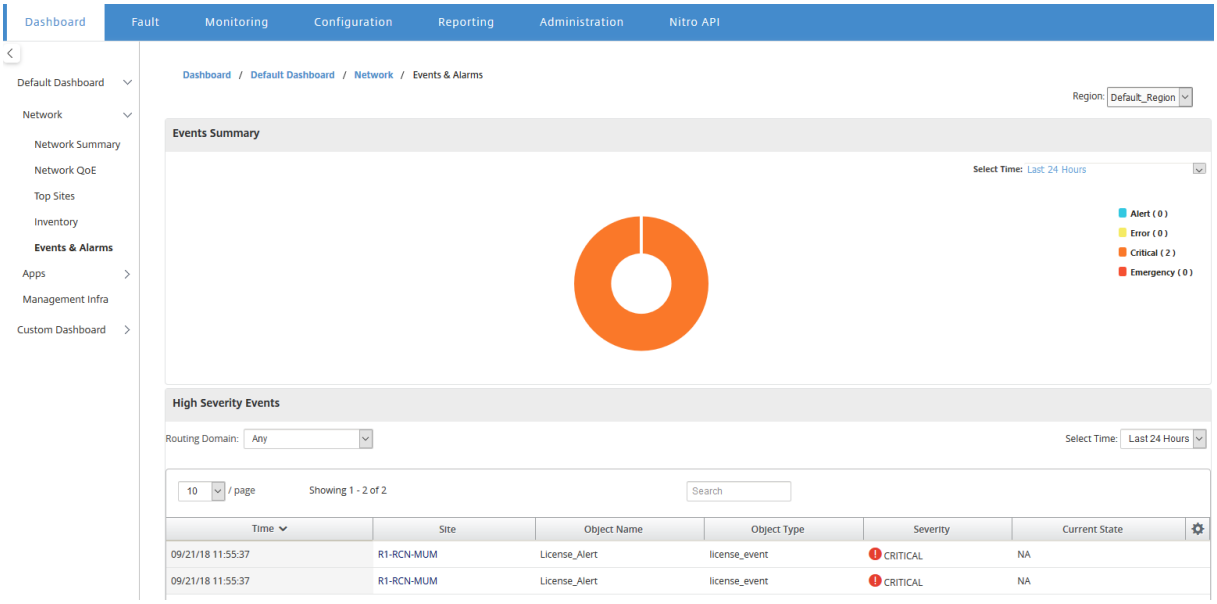
Ereignisse und Alarme

Bei einer Bereitstellung mit mehreren Regionen können Sie die Ereignisse und Alarme aller Regionen im Netzwerk anzeigen. Diese Informationen werden für das ausgewählte Zeitintervall erfasst. Um Ereignisse und Statistiken mit mehreren Regionen anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk** > **Ereignisse und Alarme** und wählen Sie im Dropdownmenü **Region** die Option **Alle** aus.

Sie können auch alle Ereignisse und Alarme einer einzelnen Region anzeigen. Diese Informationen werden für das ausgewählte Zeitintervall erfasst. Um Ereignisse und Alarmstatistiken anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Netzwerk** > **Ereignisse und Alarme** und wählen Sie im Dropdownmenü **Region** eine Region aus.

Der Abschnitt **Ereignisübersicht** gibt einen grafischen Überblick über den Ereignistyp und die Anzahl der Ereignisse. Sie können auf das Diagramm klicken, um die Ereignisse auf der Seite **Fehler** anzuzeigen. Die Anzeige zeigt auch, wie viele Ereignisse in jeder Kategorie sind. Alarmauslöser können auf den einzelnen SD-WAN Appliances konfiguriert werden. Weitere Informationen, siehe Ereignisbenachrichtigungen.

Im Abschnitt **Ereignisse mit hohem Schweregrad** wird eine Liste der schwerwiegenden Ereignisse angezeigt. Sie können die Ereignisse basierend auf der Routingdomäne filtern. Die in diesem Abschnitt angezeigten Informationen werden über die Registerkarte **Fehler** erfasst. Weitere Informationen finden Sie unter Ereignisse.

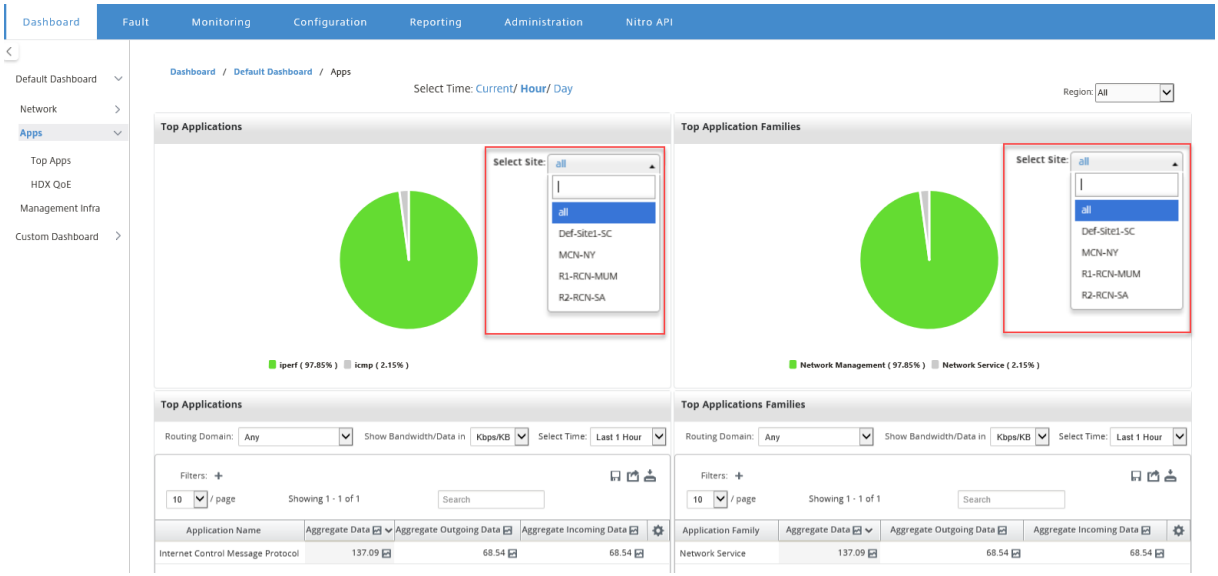


Anwendungen

Top Apps

Deep Packet Inspection (DPI) ermöglicht es der SD-WAN-Appliance, den durchgehenden Datenverkehr zu analysieren und die Anwendungs- und Anwendungsfamilientypen zu identifizieren. Bei einer Bereitstellung mit mehreren Regionen können Sie die wichtigsten Anwendungen und die wichtigsten Anwendungsfamilien in allen Regionen des Netzwerks anzeigen. Diese Informationen werden für das ausgewählte Zeitintervall erfasst.

Um die Statistiken der wichtigsten Anwendungen in allen Regionen im Netzwerk anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Apps > Top-Apps** und wählen Sie im Dropdownmenü **Region** die Option **Alle** aus.

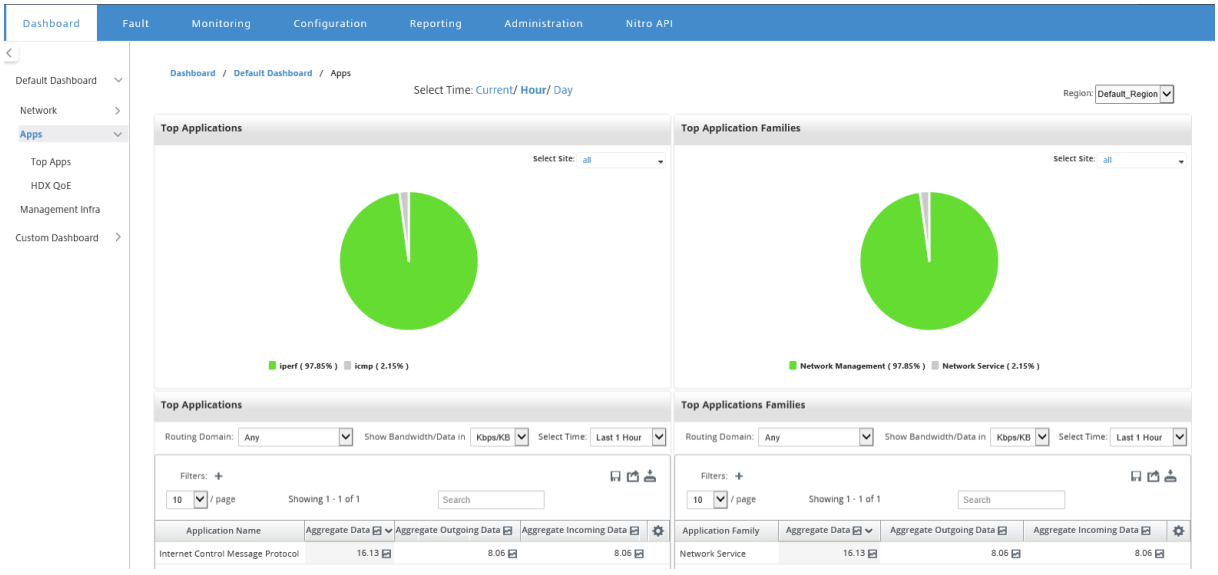


Sie können das durchsuchbare Dropdownmenü für die Siteauswahl sowohl für die **Top-Anwendungs**familien als auch für die **Top-Anwendungsfamilien** anzeigen.

Sie können auch die Top-Anwendungen und Top-Anwendungsfamilien einer bestimmten Region anzeigen.

Um die Anwendungsstatistiken einer Region anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard**> **Apps > Top-Apps** und wählen Sie im Dropdownmenü **Region** eine Region aus**.**

Sie können den Standort und das Zeitintervall als letzte 24 Stunden, letzte 1 Stunde oder aktuell auswählen.

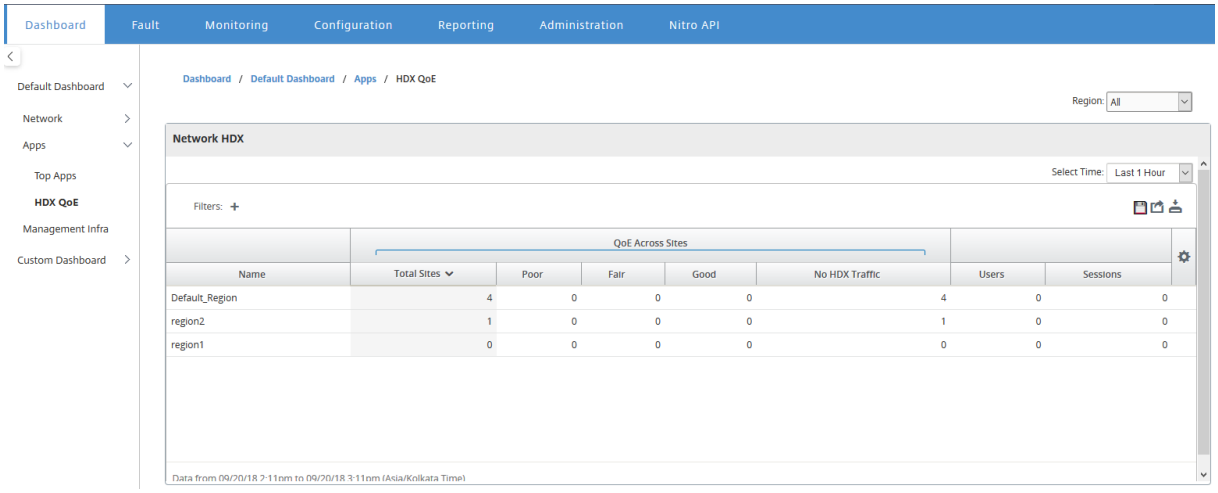


HDX QoE

Quality of Experience (QoE) ist ein berechneter Index, der Ihnen hilft, Ihre ICA-Erfahrung zu verstehen. Dieser Index wird für den gesamten ICA-Anwendungsdatenverkehr berechnet, der vom WAN zum Standort durchquert wird. Statistiken über Paketabwurf, Jitter und Latenz werden in der QoE-Berechnung verwendet. Die QoE ist eine ganze Zahl zwischen [0, 100], je höher die Zahl, desto besser die Benutzererfahrung.Die Jitter-, Latenz- und Paketablagestatistiken werden während der Paketverarbeitung auf Datenpfaden verfolgt.

Sites im gesamten Netzwerk werden basierend auf dem QoE des HDX-Datenverkehrs als gut, fair, schlecht oder gar kein HDX-Datenverkehr kategorisiert. Weitere Informationen finden Sie unter HDX QoE.

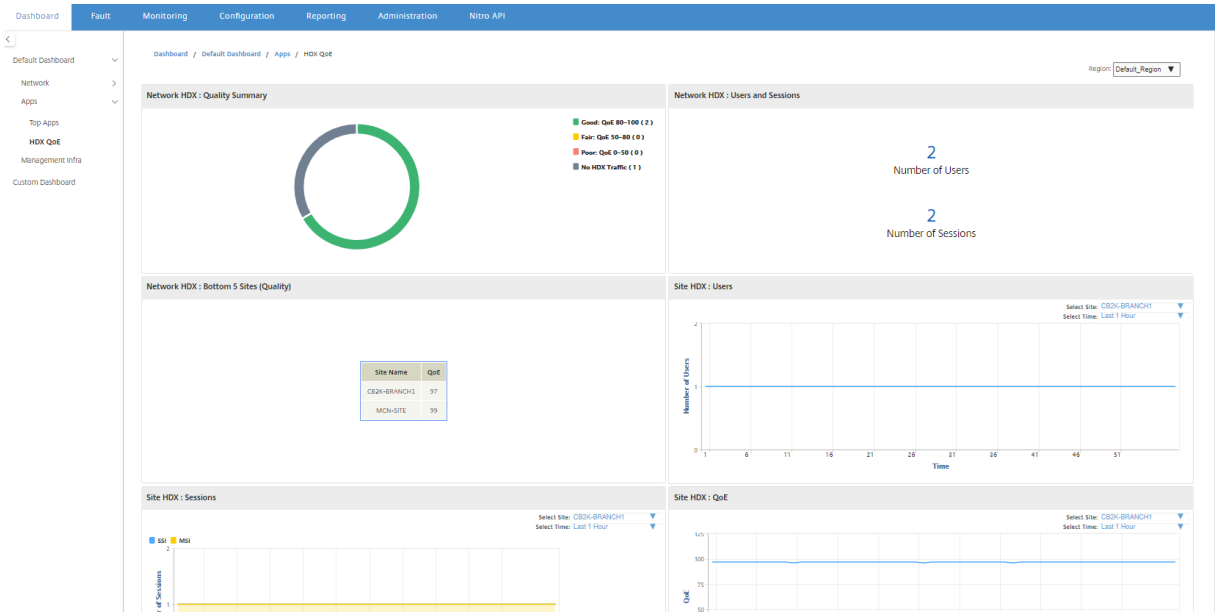
Um HDX QoE von Sites in allen Regionen des Netzwerks anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Apps > HDX QoE,** und wählen Sie im Dropdownmenü **Region** die Option **Alle aus.**



Sie können die folgenden HDX-QoE-Metriken für die einzelnen Regionen anzeigen.

- Netzwerk-HDX: Qualitätsübersicht
- Netzwerk HDX: Benutzer und Sitzungen
- Netzwerk HDX: Bottom fünf Standorte (Qualität)
- Standort HDX: Benutzer
- Standort HDX: Sitzungen
- Site HDX: Qualität der Erfahrung

Um HDX QoE-Statistiken anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard**> **Apps > HDX QoE** und wählen Sie im Dropdownmenü **Region** eine Region aus.

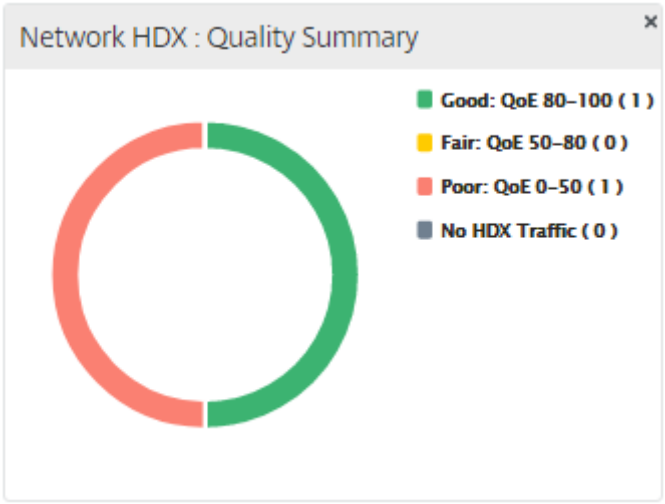


> **Hinweis**
>
> Manchmal scheinen die HDX-Dashboard-Daten und HDX-Berichte von verschiedenen Standorten nicht synchron zu sein, da jede Standortstatistik unabhängig abgefragt wird.
>
> Bei HDX-Dashboard-Widgets sehen Sie möglicherweise eine Site ohne HDX-Datenverkehr, es kann jedoch eine Anzahl von HDX-Sitzungen und -Benutzern ungleich Null sein. Dies geschieht, wenn die HDX-Sitzungen für diesen Abrufzeitraum im Leerlauf bleiben und weiterhin im offenen Zustand bleiben.

Netzwerk-HDX: Zusammenfassung der Qualität

Der HDX-Datenverkehr wird in die folgenden Qualitätskategorien eingeteilt:

Qualität	QoE-Reihe
Gut	80–100
Fair	50–80
Schlecht	0–50
Kein HDX-Datenverkehr	Nicht zutreffend

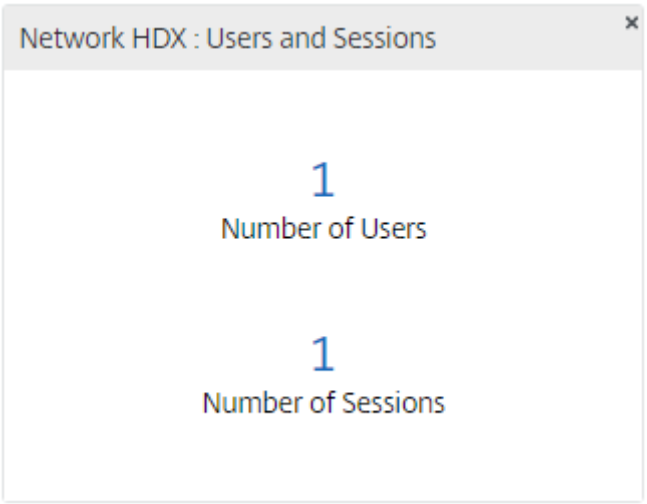


Sie können auf das Diagramm klicken, um HDX-Berichte pro Standort anzuzeigen. Weitere Informationen finden Sie unter Anzeigen von HDX-Berichten.

Netzwerk HDX: Benutzer und Sitzungen

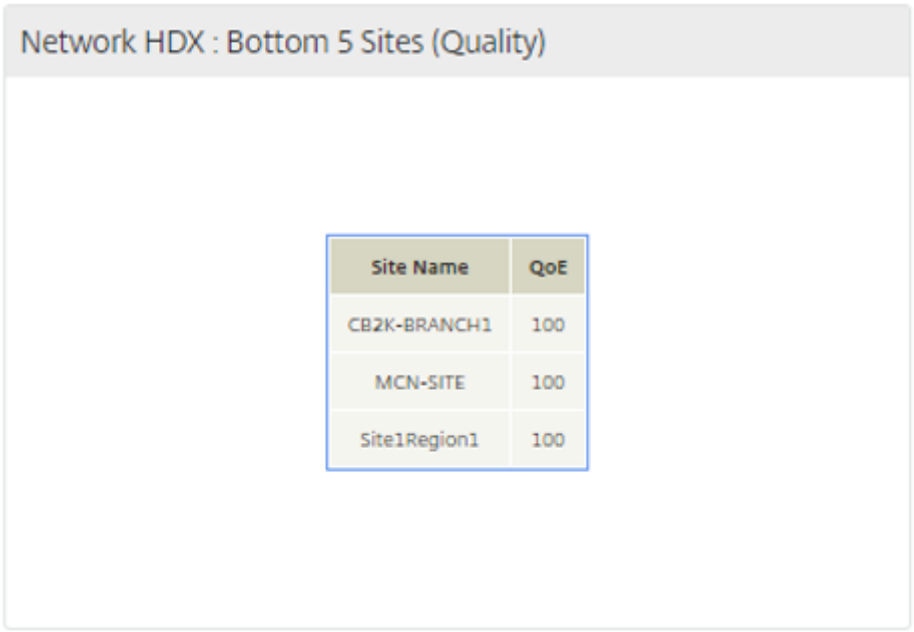
Dieses Widget enthält Informationen über die Anzahl der aktiven HDX-Benutzer und -Sitzungen. Die Anzahl der Sitzungen ist die Gesamtzahl der aktiven Single Session ICA (SSI) und Multi-Session ICA (MSI-Sitzung) Sitzungen.

> **Hinweis**
>
> In der aktuellen Version basiert die Anzahl der Benutzer nicht auf eindeutigen Benutzernamen. Das heißt, zwei Sitzungen, die von einem einzelnen Benutzer auf zwei verschiedenen Computern gestartet wurden, werden als zwei Benutzer gezählt.



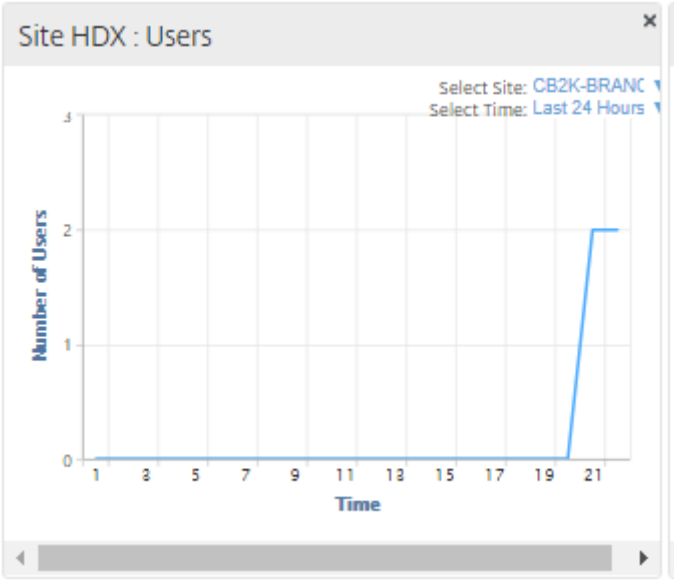
Netzwerk HDX: Bottom 5 Standorte (Qualität)

Dieses Widget bietet eine Liste der unteren 5 Sites, die den geringsten QoE-Wert haben. Es trägt dazu bei, Initiativen zur Verbesserung der Benutzererfahrung zu fördern.



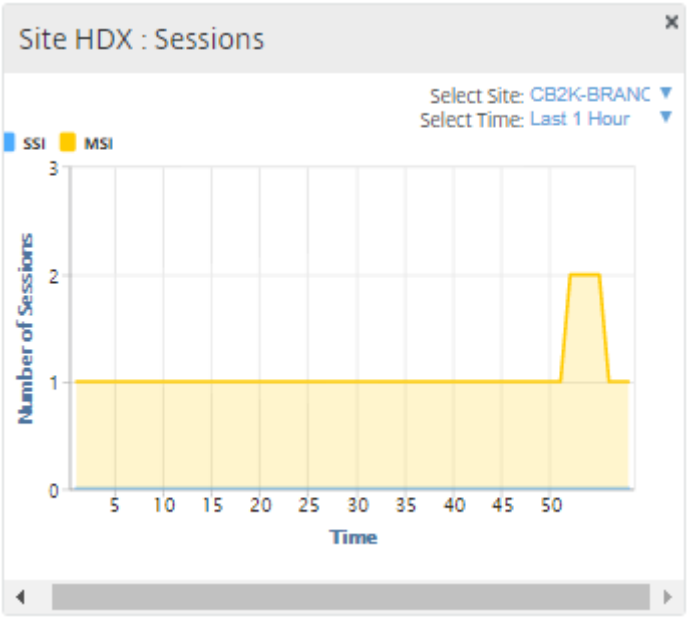
Standort HDX: Benutzer

Dieses Widget bietet eine grafische Darstellung der Anzahl der Benutzer, die für das ausgewählte Zeitintervall an einer bestimmten Site aktiv waren.Sie können die Site und das Zeitintervall als letzte 24 Stunden, letzte 1 Stunde oder letzte 5 Minuten auswählen.



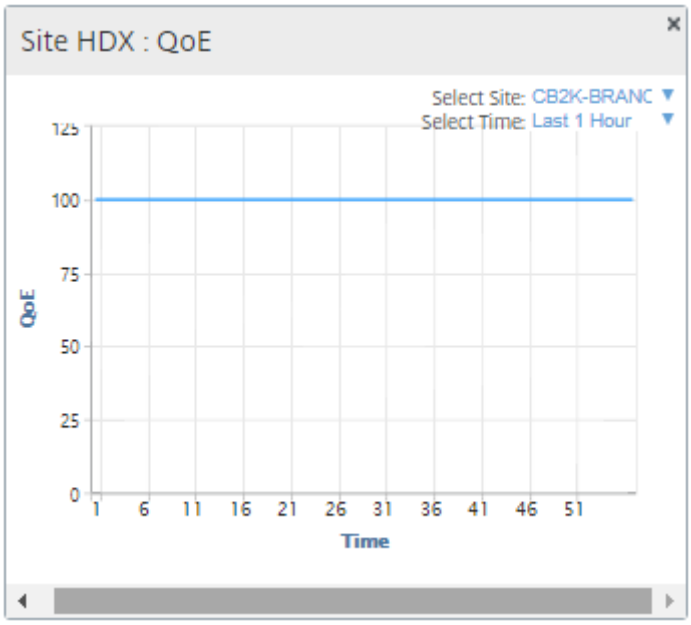
Standort HDX: Sitzungen

Dieses Widget bietet eine grafische Darstellung der Anzahl der MSI- und SSI-Sitzungen, die an einem bestimmten Standort für das ausgewählte Zeitintervall aktiv sind.Sie können die Site und das Zeitintervall als letzte 24 Stunden, letzte 1 Stunde oder letzte 5 Minuten auswählen.



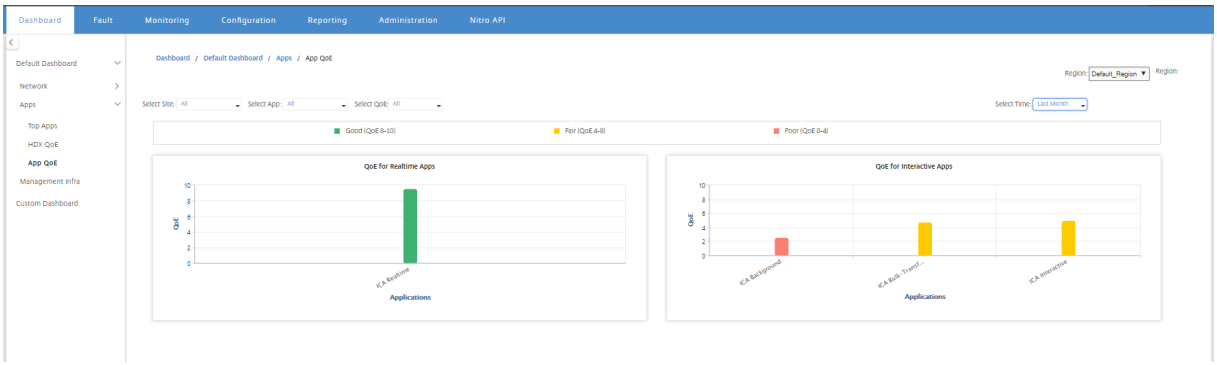
Site HDX: Qualität der Erfahrung

Dieses Widget bietet eine grafische Darstellung des gesamten QoE an einem bestimmten Standort für das ausgewählte Zeitintervall.Sie können die Site und das Zeitintervall als letzte 24 Stunden, letzte 1 Stunde oder letzte 5 Minuten auswählen.



Anwendung QoE

Anwendungs-QoE ist ein Maß für die Qualität der Benutzererfahrung für eine Anwendung. Der Anwendungs-QoE-Punktebereich beträgt 0-10, wobei 10 eine ausgezeichnete Qualität und 0 eine schlechte Qualität darstellt. Weitere Informationen finden Sie unter Anwendung QoE. Sie können die QoE-Punktzahl der Anwendung für Echtzeit- und interaktive Datenverkehr anzeigen.



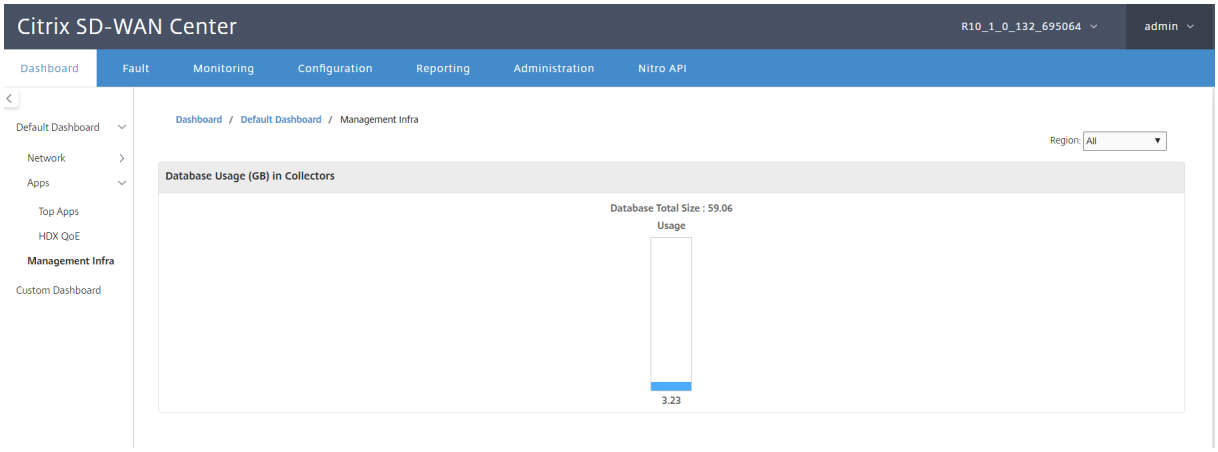
Sie können die QoE-Statistiken der Anwendung nach Standort, Anwendung oder QoE-Art filtern.

Managementinfra

Auf der Seite “Management Infra”können Sie die Statistiken zur Nutzung und Speicherung der Citrix SD-WAN Center-Datenbank anzeigen.

Bei einer Bereitstellung mit mehreren Regionen können Sie die Datenbankverwendung aller Kollektoren im Netzwerk anzeigen. Um Statistiken über mehrere Regionen anzuzeigen, navigieren Sie zu

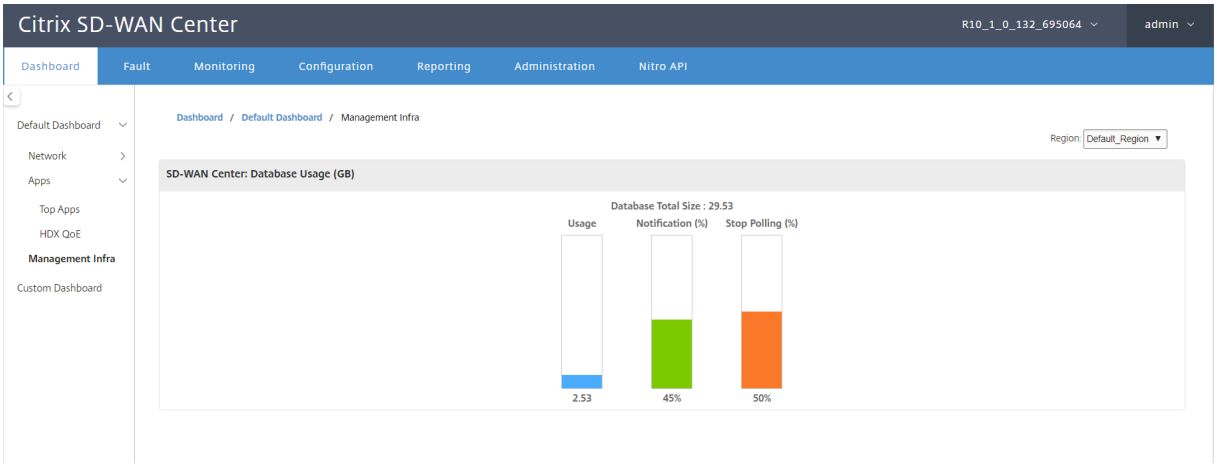
Dashboard > **Standard-Dashboard** > **Management Infra** und wählen Sie im Dropdownmenü **Region** die Option **Alle**.



Um Citrix SD-WAN Center-Datenbankstatistiken für eine bestimmte Region anzuzeigen, navigieren Sie zu **Dashboard** > **Standard-Dashboard** > **Management-Infra**, und wählen Sie im Dropdownmenü **Region** eine Region aus.

Im Abschnitt **Datenbankverwendung** wird eine grafische Übersicht über die Ressourcennutzung der Datenbank und die Schwellenwerte für das Senden von Benachrichtigungen oder das Anhalten der Datenerfassung angezeigt. Sie können auf das Diagramm klicken, um die Details auf der Seite Datenbankpflege anzuzeigen.

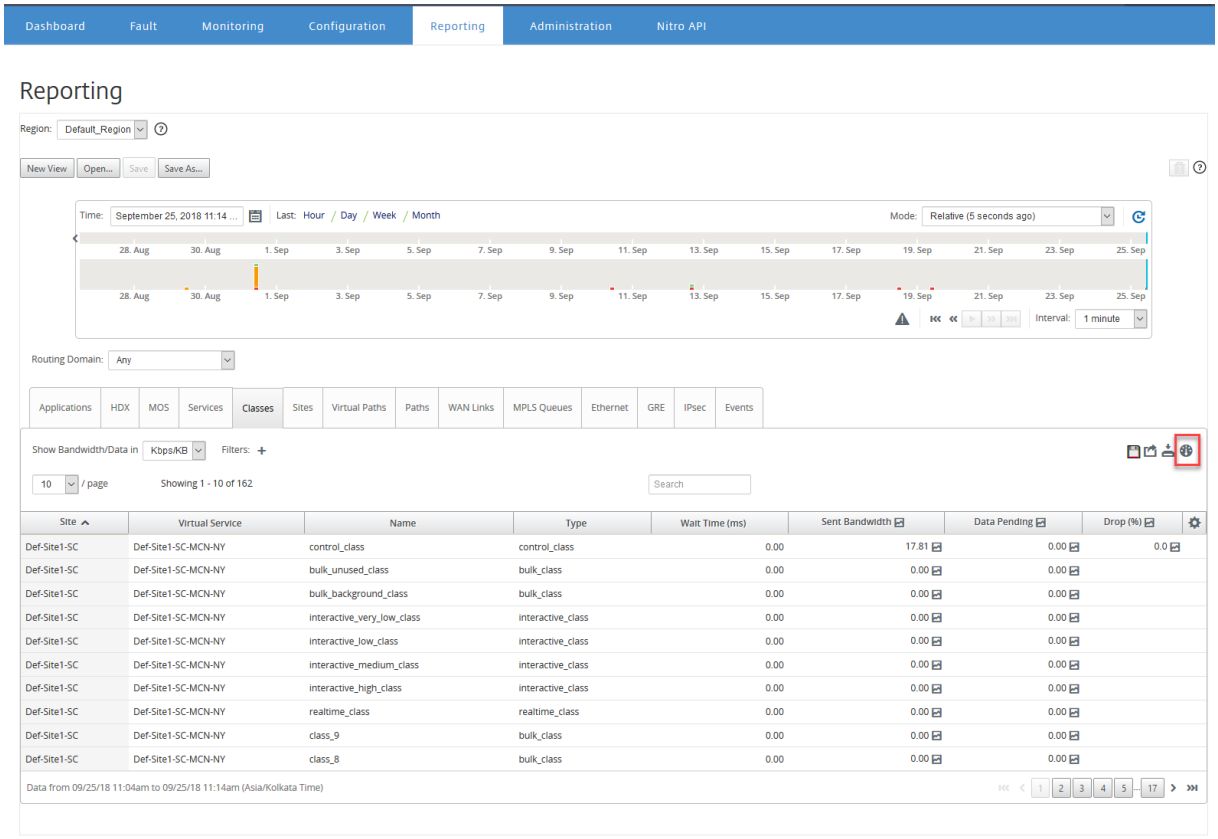
- **Auslastung**: Derzeit verwendete Datenbankkapazität in GB.
- **Benachrichtigung**: Schwellenwert für die Erstellung einer Benachrichtigung über die Datenbankverwendung. Der Schwellenwert ist ein Prozentsatz der maximalen Größe der Datenbank. Wenn eine E-Mail-Benachrichtigung konfiguriert ist, wird eine E-Mail-Benachrichtigung gesendet, wenn die Größe der Datenbank diesen Schwellenwert überschreitet. Weitere Informationen finden Sie unter Ereignisbenachrichtigungen.
- **Polling beenden**: Schwellenwert für das Anhalten der Statistikabfrage. Der Schwellenwert ist ein Prozentsatz der maximalen Größe der Datenbank. Die Abfrage wird beendet, wenn die Größe der Datenbank diesen Schwellenwert überschreitet. Weitere Information finden Sie unter Datenbank verwalten.



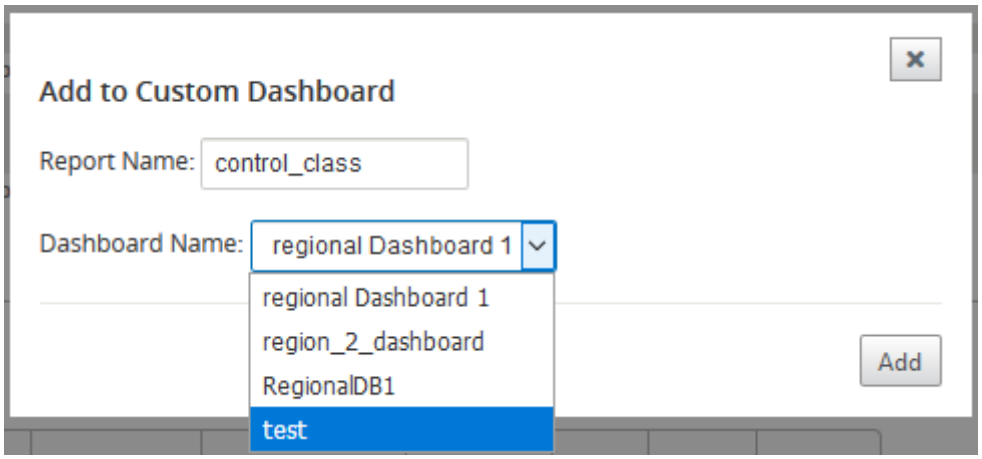
Benutzerdefiniertes Dashboard

Sie können das Citrix SD-WAN Center-Dashboard anpassen und die Statistiken auswählen, die Sie auf dem Dashboard basierend auf Ihren analytischen Anforderungen anzeigen möchten. Erstellen Sie ein benutzerdefiniertes Dashboard mit regionalen Details oder eine globale Zusammenfassung. Sie können auch einen vorhandenen Bericht anpassen.

> **Hinweis**
>
> Sie können jetzt einen Bericht als Widget an Ihr benutzerdefiniertes Dashboard anheften, indem Sie die Option **Zum Dashboard hinzufügen** auf der Seite “Berichte”verwenden.



Geben Sie den Berichtsnamen ein, und wählen Sie das benutzerdefinierte Dashboard aus.



Für das benutzerdefinierte Dashboard “Regionale Details”können Sie aus den folgenden Widgets auf Bereichsebene wählen:

- Siteübersicht
- Virtueller Pfad
- Veranstaltungen in der Region
- Regionsalarm - Übersicht
- Lagerverwaltung (pro Region)

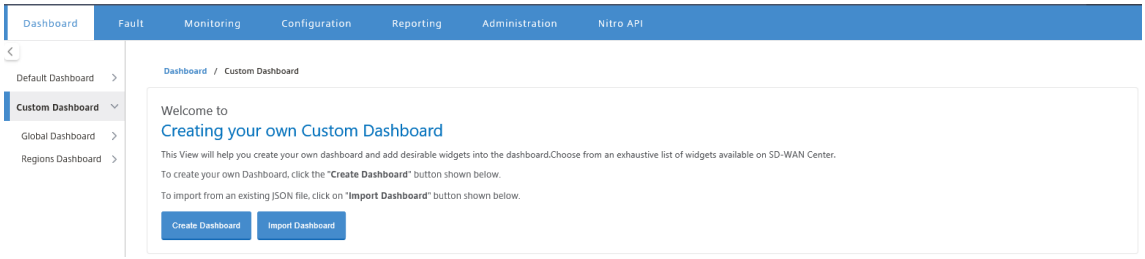
- Top Sites pro Region
- Pfade
- MPLS-Warteschlangen
- Ethernet
- LAN GRE Tunnel
- IPSec-Tunnel
- Serviceübersicht
- Klassen
- Siteereignisse
- Top Anwendungen pro Region
- Top-Anwendungsfamilie pro Region
- Standort HDX: Benutzer
- Standort HDX: Sitzungen
- Standort HDX: QoE
- MOS-Anwendungen
- Datenbankverwendung

Für ein benutzerdefiniertes Dashboard mit globaler Zusammenfassung können Sie aus den folgenden Widgets auf Netzwerkebene wählen:

- Übersicht über mehrere Regionen
- Virtual Path Health im Netzwerk
- Ereignisse
- Alarmübersicht
- Lagerbestands-Manager
- Top Sites im Netzwerk
- Netzwerk HDX
- Datenbankverwendung in Collectors
- Top Anwendungen
- Top Anwendungsfamilien

So erstellen Sie ein benutzerdefiniertes Dashboard:

1. Navigieren Sie zu **Dashboard** > **Benutzerdefiniertes Dashboard**, und klicken Sie auf **Dashboard erstellen**.

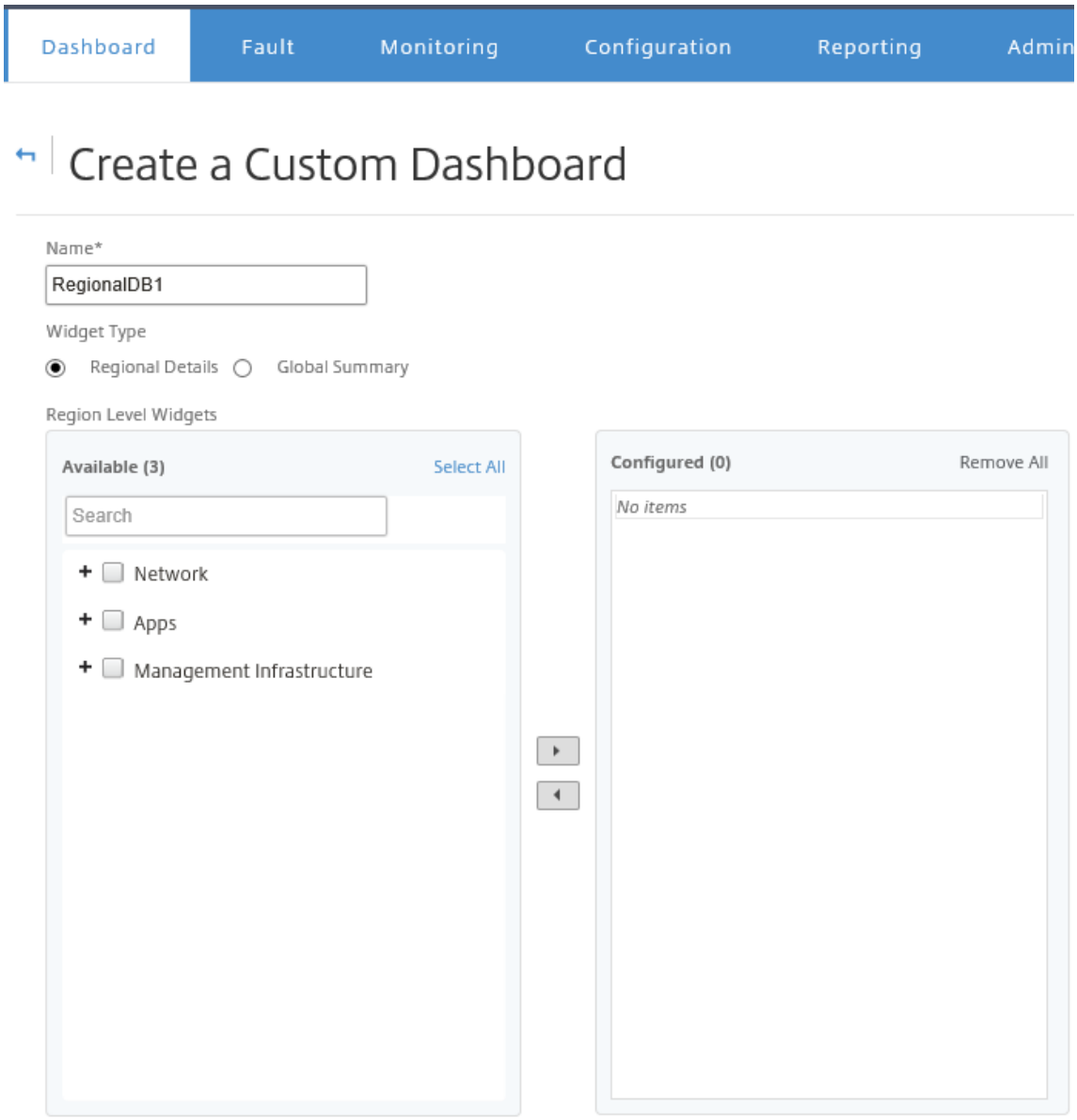


> **Hinweis**
>
> Sie können ein vorhandenes Dashboard auch im JSON-Format importieren, indem Sie auf **Dashboard importieren** klicken.

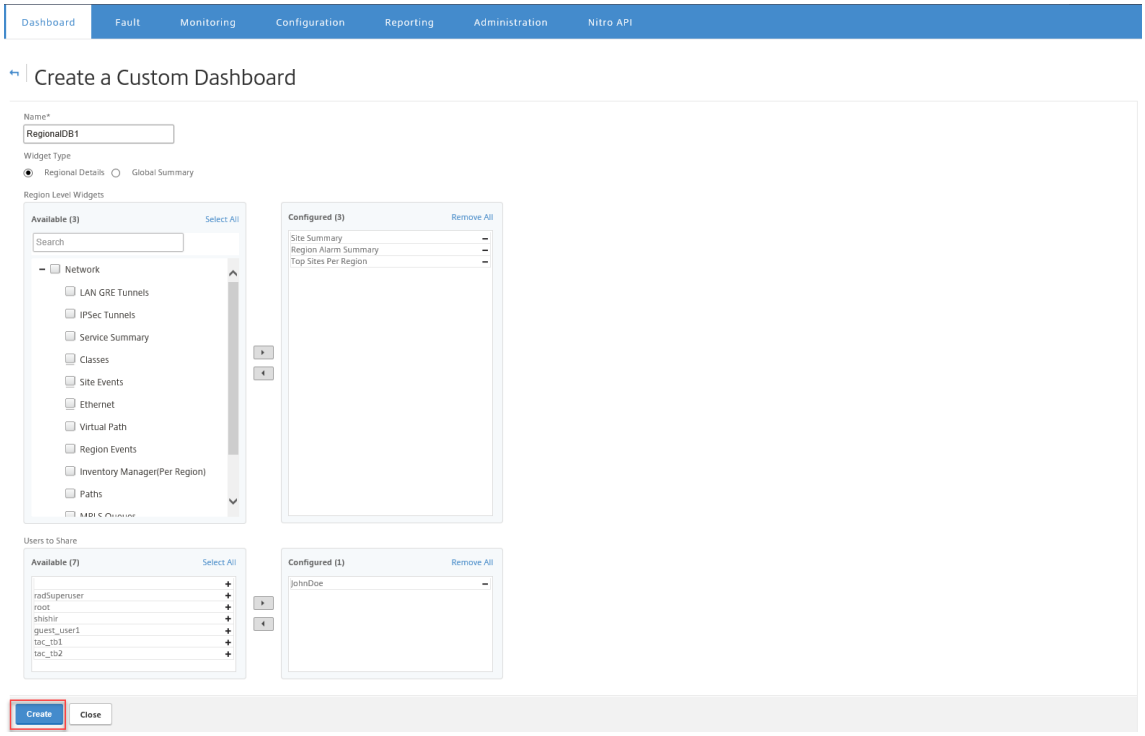
2. Geben Sie im Feld **Name** einen Namen für das benutzerdefinierte Dashboard ein.
3. Wählen Sie den Widget-Typ aus. Wählen Sie **Globale Zusammenfassung**, um Widgets auf Netzwerkebene anzuzeigen, und wählen Sie **Regionale Details** aus, um Widgets auf regionaler Ebene anzuzeigen.

4. Klicken Sie auf **Hinzufügen** und wählen Sie die erforderlichen Widgets aus.

   Die Widgets sind in drei Ebenen unterteilt: Netzwerk, Apps und Management-Infrastruktur.



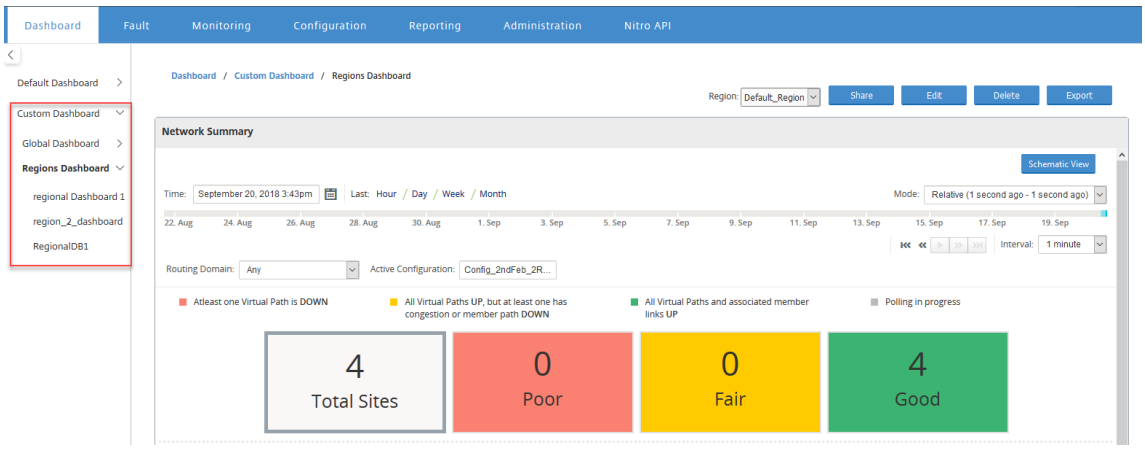
> Hinweis
>
> Bei einer Bereitstellung mit einer **Region sind nur Widgets auf Regionsebene** verfügbar.



Sie können das benutzerdefinierte Dashboard auch für mehrere Benutzer freigeben. Weitere Informationen zu Benutzern finden Sie unter[Benutzerkonten](#).

5. Klicken Sie auf **Erstellen**. Das neu erstellte benutzerdefinierte Dashboard wird unter **Benutzerdefiniertes Dashboard** aufgelistet.

> **Tipp**
>
> Sie können das benutzerdefinierte Dashboard bearbeiten oder löschen.



Diagnose-Pakete

April 13, 2021

Ein Diagnosepaket besteht aus allen Systemprotokolldateien, Systeminformationen und anderen erforderlichen Details, die das Citrix SD-WAN-Supportteam bei der Diagnose und Behebung von Problemen mit Ihrem System unterstützen.

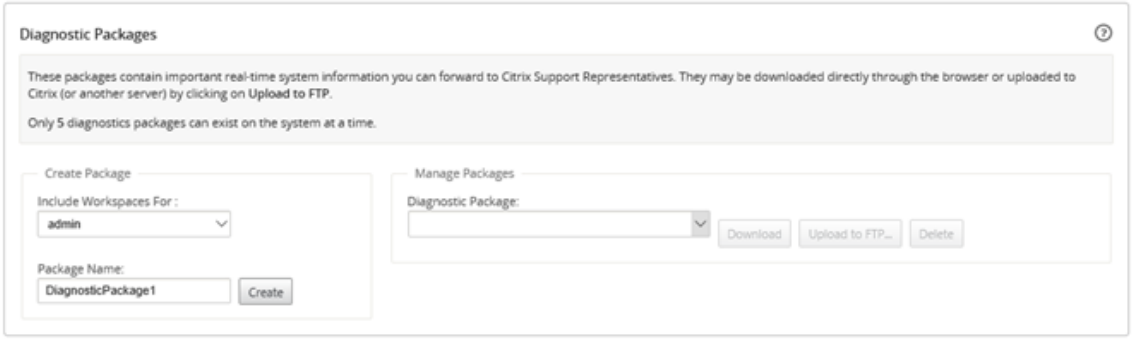
Nachdem Sie das Paket erstellt haben, können Sie es auf Ihren Computer herunterladen und dann das Diagnosepaket an den Citrix Customer Support senden. Alternativ können Sie es direkt auf den Citrix Customer Support Server (oder einen anderen Server) hochladen.

> **Hinweis**
>
> Citrix SD-WAN Center kann maximal fünf Diagnosepakete gleichzeitig speichern.

So erstellen Sie ein Diagnosepaket:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Überwachung**, und klicken Sie dann auf **Diagnose**.
2. Wählen Sie im Abschnitt **Diagnose-Pakete** unter **Paket erstellen** aus der Dropdownliste **Workspaces einschließen für** einen Benutzer aus, dessen Arbeitsbereiche in die Diagnose kopiert werden sollen.

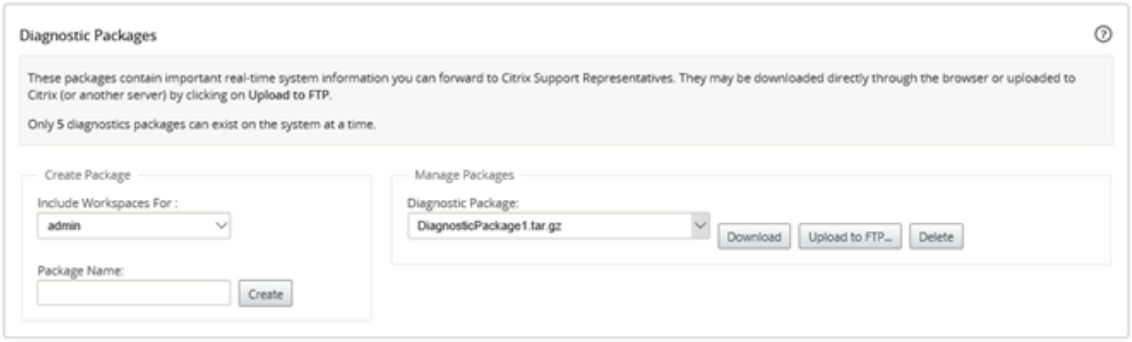
   > **Hinweis**
   >
   > Das Diagnose-Paket enthält die fünf Konfigurationen, die zuletzt vom ausgewählten Benutzer geändert wurden.

3. Geben Sie im Feld **Paketname** einen Namen für das Diagnosepaket ein.
4. Klicken Sie auf **Erstellen**. Dadurch wird eine Systemdiagnose ausgeführt und ein Diagnosepaket generiert.

So laden Sie ein Diagnosepaket herunter:

1. Wählen Sie im Abschnitt **Diagnose-Pakete** unter **Paket verwalten** aus der Dropdownliste **Diagnose-Pakete** das Paket aus, das Sie herunterladen möchten.



2. Klicken Sie auf **Download**. Das Diagnosepaket wird auf Ihren lokalen Computer heruntergeladen.

So laden Sie ein Diagnosepaket auf einen FTP-Server hoch:

1. Wählen Sie im Abschnitt **Diagnose-Pakete** unter **Paket verwalten** aus der Dropdownliste **Diagnose-Pakete** ein Paket aus, das Sie hochladen möchten.
2. Klicken Sie auf **Zu FTP hochladen**. Dadurch wird das Dialogfeld "Auf **FTP-Server hochladen** "geöffnet, in dem Sie Ihre FTP-Authentifizierungsinformationen angeben und das Paket auf den Citrix Customer Support FTP-Server oder auf einen anderen FTP-Host hochladen können.

3. Geben Sie im Feld **Kundenname** einen Namen ein, der den Citrix SD-WAN-Support bei der Identifizierung der Diagnosepakete unterstützt.
   Ein Verzeichnis mit diesem Namen wird auf dem Citrix FTP-Server erstellt, und Ihre Dateien werden an diesen Speicherort hochgeladen.

4. Geben Sie im Feld **FTP-Host** die IP-Adresse oder den Hostnamen (falls DNS konfiguriert ist) des FTP-Servers ein.
5. Geben Sie im Feld **Benutzername** einen Benutzernamen ein, der für die Anmeldung am FTP-Server verwendet werden soll.
6. Geben Sie im Feld **Kennwort** das Kennwort ein, das dem Benutzernamen zugeordnet ist.
7. Klicken Sie auf **Upload**.

> **Hinweis**
>
> Es wird empfohlen, alte Diagnose-Pakete regelmäßig zu löschen, um zu verhindern, dass die Grenze für die maximal zulässigen Pakete überschritten wird. Um ein vorhandenes Diagnosepaket zu löschen, wählen Sie in der Dropdownliste **Diagnosepaket** ein Diagnosepaket aus, und klicken Sie dann auf **Löschen**.

Ereignisse

April 13, 2021

Citrix SD-WAN Center erfasst Ereignisinformationen von allen erkannten Appliances im Netzwerk. Diese Ereignisinformationen können gefiltert und auf der Seite **Ereignisanzeige** angezeigt werden.

Die Ereignisdetails enthalten die folgenden Informationen.

- **Zeit:** Die Zeit, zu der das Ereignis generiert wurde.
- **Site:** Der Name der Site, von der das Ereignis stammt.
- **Einheiten-ID:** Zeigt an, ob es sich bei der Appliance, von der das Ereignis stammt, um eine primäre (**0**) oder sekundäre (**1**) -Appliance handelt.

  > **Hinweis**
  >
  > Die Spalte Einheiten-ID ist standardmäßig ausgeblendet. Um die Spalte anzuzeigen, klicken Sie auf **Einblenden/Ausblenden** (Zahnradsymbol) und aktivieren Sie im Dropdownmenü das Kontrollkästchen **Einheiten-ID**

- **Objektname:** Der Name des Objekts, das das Ereignis generiert.
- **Objekttyp:** Der Objekttyp, der das Ereignis generiert.
- **Schweregrad:** Der Schweregrad des Ereignisses.
- **Vorheriger Status:** Der Status des Objekts vor dem Ereignis. Der Status wird als **unbekannt** aufgeführt, wenn er nicht zutreffend ist.

- **Aktueller Status:** Der Status des Objekts zum Zeitpunkt des Ereignisses.
- **Beschreibung:** Textbeschreibung des Ereignisses.

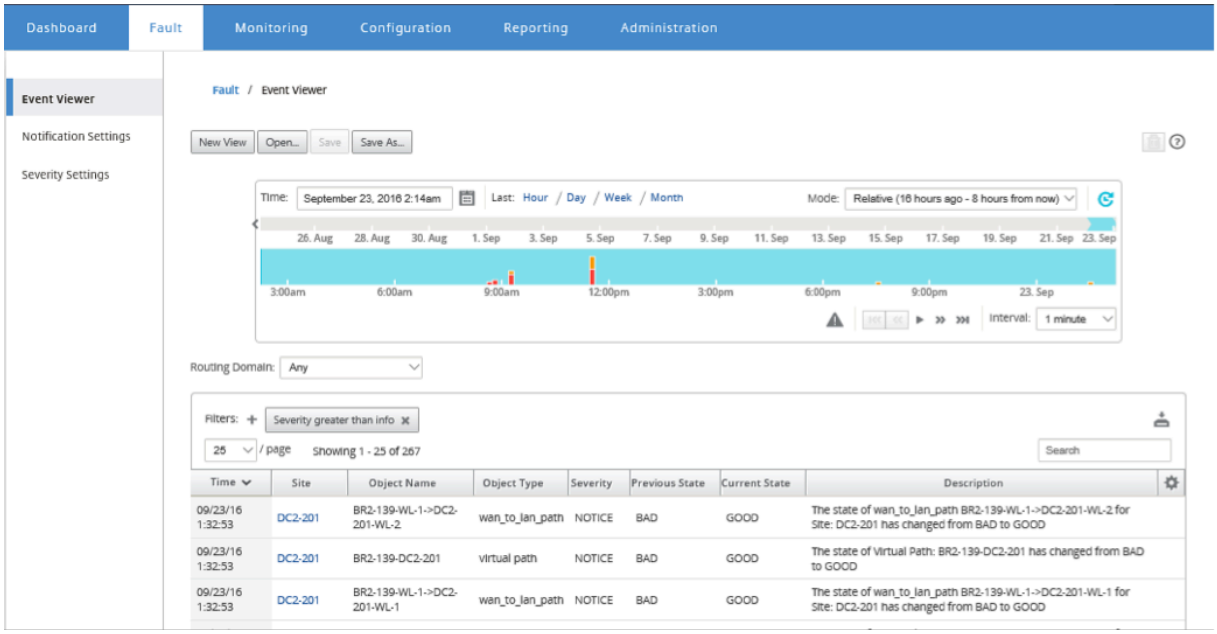
Anzeigen von Ereignissen

Sie können die Ereignisse anzeigen, filtern und von der Ereignisanzeige herunterladen.

Zugriff auf die Ereignisanzeige-Seite.

Klicken Sie im Citrix SD-WAN Center-Webinterface auf die Registerkarte **“Fault”.**

Die Seite Ereignisanzeige wird standardmäßig angezeigt.



Sie können Berichte eines bestimmten Zeitraums auswählen und anzeigen, indem Sie die Zeitachsen-Steuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

> **Hinweis**
>
> Sie können die Ereignisdaten der letzten 30 Tage anzeigen. Jegliche Daten über diesen Zeitraum hinaus werden automatisch aus dem SD-WAN Center Collector und den jeweiligen regionalen Collectors entfernt.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.

Verwenden von Filtern

Sie können benutzerdefinierte Filter erstellen, um die Ergebnisse der Ereignistabelle einzugrenzen.

So erstellen Sie und wenden Sie einen Filter an:

1. Klicken Sie rechts neben der Bereichsbezeichnung für **Filter** auf das Pluszeichen **+.**
2. Wählen Sie im Dropdownmenü eine Kategorie aus.

   Folgende Optionen stehen zur Verfügung:

   - Größe
   - Objektname
   - Objekttyp
   - Schweregrad
   - Vorheriger Status
   - Aktueller Status
3. Wählen Sie im mittleren Dropdownmenü einen Operator aus.

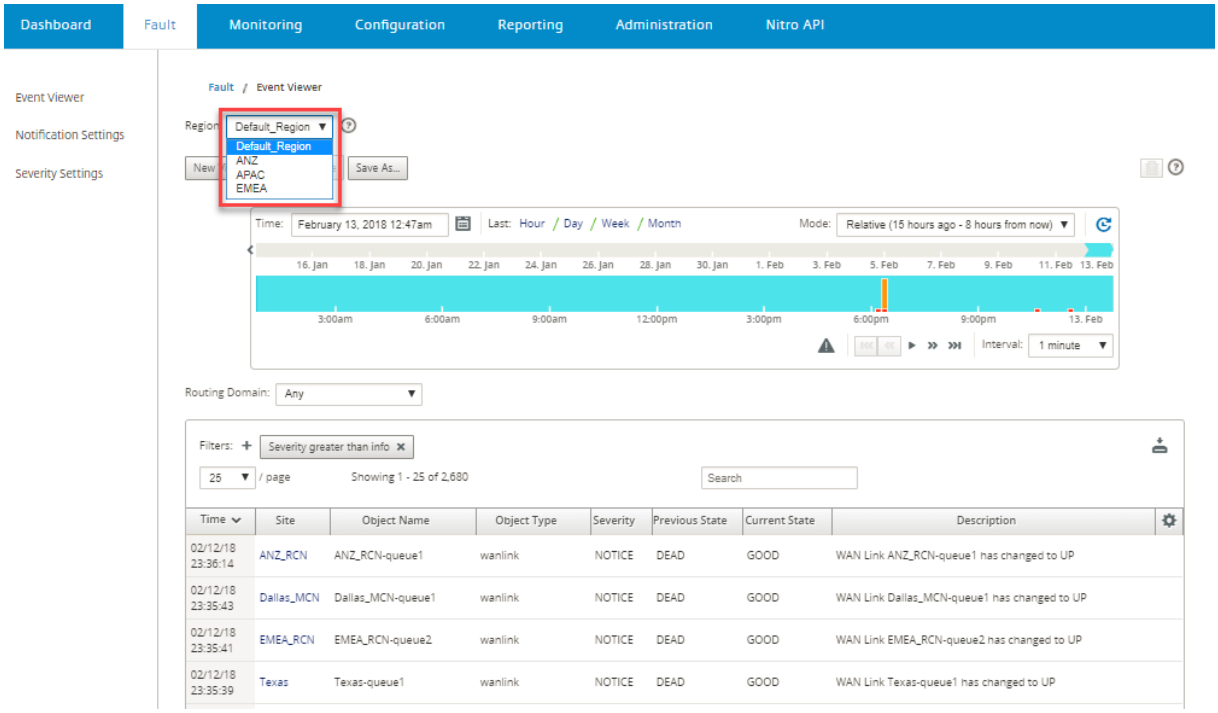
   Die folgenden Optionen stehen zur Auswahl:

   - is
   - is not
   - is one of
   - contains
   - does not contain
   - less than
   - less than or equal to
   - greater than
   - greater than or equal to
4. Geben Sie die Zeichenfolge oder den Wert ein, um den Filter zu trennen.

> **Hinweis**
>
> Bei diesem Feld wird die Groß- und Kleinschreibung beachtet.

> **Hinweis**
>
> Sie können mehrere Filter erstellen und anwenden.
> Für Netzwerk mit mehreren Regionen können Sie bestimmte Regionen auswählen, um das Ereignis anzuzeigen.

Die Ereignisdaten werden aus dem Kollektor der jeweiligen Region abgerufen.



> **Hinweis**
>
> Bei einer Netzwerkbereitstellung mit einer Region ist die Dropdownliste **“Region”** nicht verfügbar.

So laden Sie die Ereignistabelle als CSV-Datei herunter:

Klicken Sie auf das Download-Symbol in der oberen rechten Ecke der Ereignistabelle.

Weitere Informationen zu Ereignisstatistiken finden Sie unterEreignisbericht.

Sie können Citrix SD-WAN Center so konfigurieren, dass externe Ereignisbenachrichtigungen für verschiedene Ereignistypen wie E-Mail, SNMP-Traps oder Syslog-Nachrichten gesendet werden. Weitere Informationen finden Sie unter Ereignisbenachrichtigungen.

Ereignisbenachrichtigungen

April 13, 2021

Sie können Citrix SD-WAN Center so konfigurieren, dass Ereignisbenachrichtigungen für verschiedene Ereignistypen wie E-Mail, SNMP-Traps oder Syslog-Nachrichten gesendet werden. Nachdem Sie die Benachrichtigungseinstellungen für E-Mail, SNMP und Syslog konfiguriert haben, können Sie den Schweregrad für verschiedene Ereignistypen auswählen und den Modus (E-Mail, SNMP, Syslog) zum Senden von Ereignisbenachrichtigungen auswählen. Benachrichtigungen werden für Ereignisse

generiert, die dem angegebenen Schweregrad für den Ereignistyp entsprechen oder darüber liegen.

Die verfügbaren Schweregrade sind in absteigender Reihenfolge des Schweregrads wie folgt:

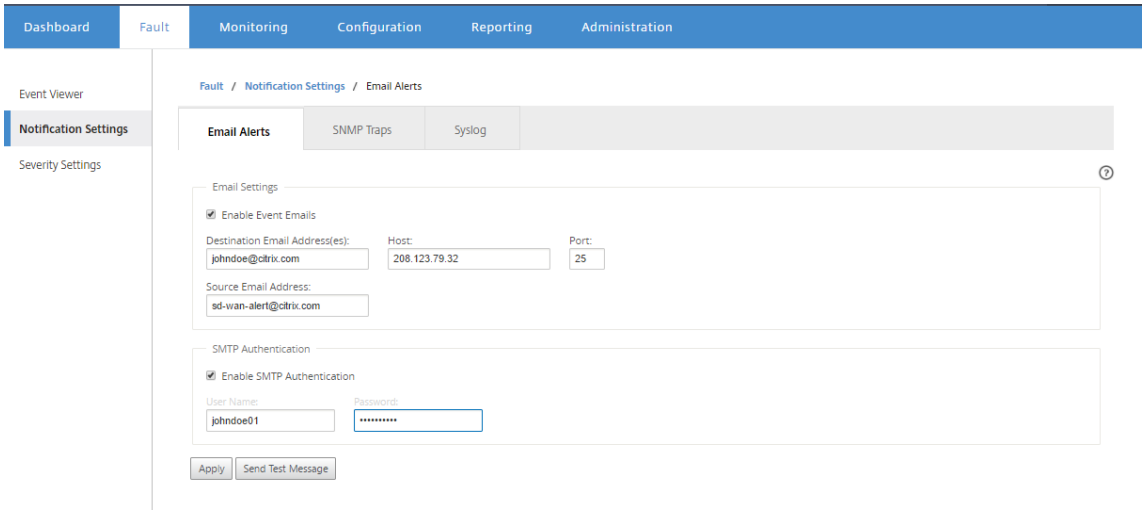
- NOTFALL
- BENACHRICHTIGUNG
- KRITISCH
- ERROR
- WARNUNG
- HINWEIS
- INFORMATIV
- DEBUG

> **Tipp**
>
> Sie können Benachrichtigungseinstellungen konfigurieren, um Ereigniswarnungen per E-Mail, SNMP-Traps oder Syslog-Nachrichten sowohl in Citrix SD-WAN Center als auch in den einzelnen Citrix SD-WAN-Appliances in Ihrem Netzwerk zu empfangen.
>
> Wenn Sie Benachrichtigungen im Citrix SD-WAN Center aktivieren, können Sie jedoch Ereignisbenachrichtigungen für das gesamte Citrix SD-WAN-Netzwerk (d. h. MCN und alle Sites) erhalten. Wenn Sie Benachrichtigungen auf den Citrix SD-WAN-Appliances aktivieren, können Sie jedoch nur Benachrichtigungen von den einzelnen Appliances empfangen.
>
> Es wird empfohlen, Benachrichtigungen nur im Citrix SD-WAN Center zu aktivieren, um redundante Benachrichtigungen von den anderen Citrix SD-WAN-Appliances in Ihrem Netzwerk zu vermeiden.

Konfigurieren von E-Mail-Benachrichtigungseinstellungen

So konfigurieren Sie E-Mail-Benachrichtigungseinstellungen:

1. Navigieren Sie in der Webverwaltungsschnittstelle von Citrix SD-WAN Center zu **Fehler** > **Benachrichtigungseinstellungen** > **E-Mail-Benachrichtigungen.**



2. Wählen Sie **Ereignis-E-Mails aktivieren aus**.
3. Geben **Sie im Feld Ziel-E-Mail-Adresse (n)** die E-Mail-Adresse ein, an die Warnbenachrichtigungen gesendet werden sollen.

   > **Hinweis**
   >
   > Sie können mehrere E-Mail-Adressen durch Semikolons getrennt eingeben.

4. Geben Sie im Feld **Host** die IP-Adresse oder den Hostnamen eines externen SMTP-Servers ein, um E-Mail-Nachrichten an das Internet weiterzuleiten.
5. Geben Sie im Feld **Port** die Portnummer ein, die für die SMTP-Verbindung verwendet werden soll. Der Standardport ist 25.
6. Geben Sie im Feld **Quell-E-Mail-Adresse** die E-Mail-Adresse ein, von der E-Mail-Benachrichtigungen gesendet werden.
7. Wählen Sie **SMTP-Authentifizierung aktivieren** aus.
8. Geben Sie im Feld **Benutzername** einen Benutzernamen für den für die Authentifizierung verwendeten SMTP-Server ein.
9. Geben Sie im Feld **Kennwort** das Kennwort ein, das dem Benutzernamen des für die Authentifizierung verwendeten SMTP-Servers zugeordnet ist.

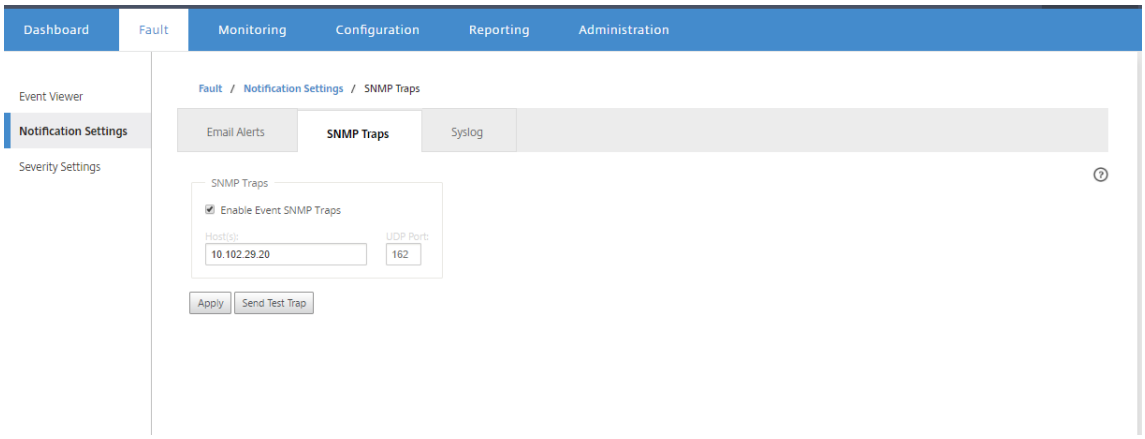
   > **Hinweis**
   >
   > Klicken Sie auf **Testnachricht senden,** um eine E-Mail-Beispielwarnung an die konfigurierten Empfänger zu senden.

10. Klicken Sie auf **Apply**.

Konfigurieren der SNMP-Trap-Benachrichtigungseinstellungen

So konfigurieren Sie SNMP-Trap-Benachrichtigungseinstellungen:

1. Navigieren Sie in der Webverwaltungsschnittstelle von Citrix SD-WAN Center zu **Fehler** > **Benachrichtigungseinstellungen** > **SNMP-Traps**.
2. Wählen Sie **Ereignis-SNMP-Traps aktivieren aus.**



3. Geben Sie im Feld **Host (s)** die IP-Adresse oder den Hostnamen eines externen SNMP-Systems ein. Dieser Host empfängt die Ereignisse als SNMP-Traps.

> **Hinweis**
>
> Sie können mehrere IP-Adressen oder Hostnamen durch Semikolons getrennt eingeben.

4. Geben Sie im Feld **UDP-Port** den UDP-Port ein, der zum Senden der SNMP-Traps verwendet werden soll. Standardmäßig ist der UDP-Port auf 162 festgelegt.
5. Klicken Sie auf **Über** nehmen, um die Benachrichtigungseinstellungen für SNMP-Traps anzuwenden.

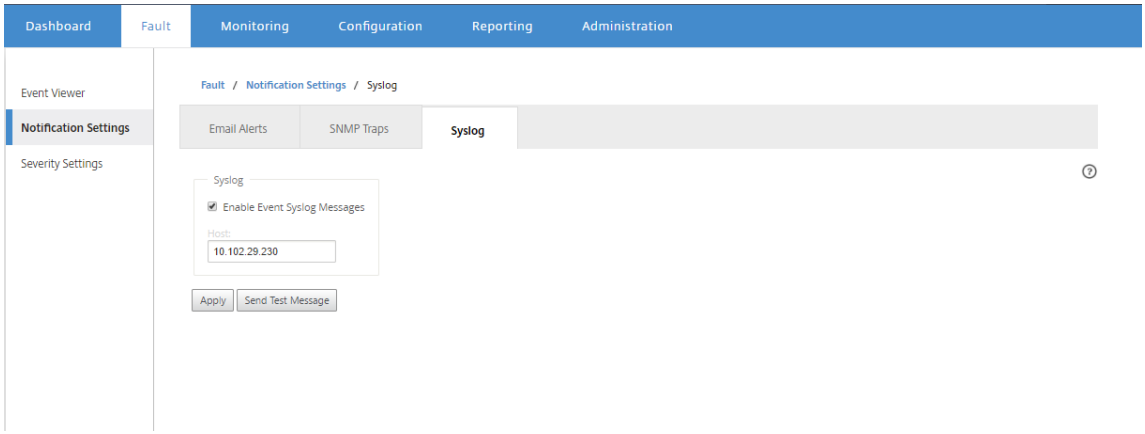
> **Hinweis**
>
> Klicken Sie alternativ auf **Test-Trap senden**, um zu überprüfen, ob das System in der Lage ist, ein SNMP-Trap an das konfigurierte Ziel zu senden.

Konfigurieren der Syslog-Benachrichtigungseinstellungen

So konfigurieren Sie Syslog-Benachrichtigungseinstellungen:

1. Navigieren Sie in der Webverwaltungsschnittstelle von Citrix SD-WAN Center zu **Fehler** > **Benachrichtigungseinstellungen** > **Syslog**.

2. Wählen Sie **Ereignissyslog-Meldungen aktivieren aus.**



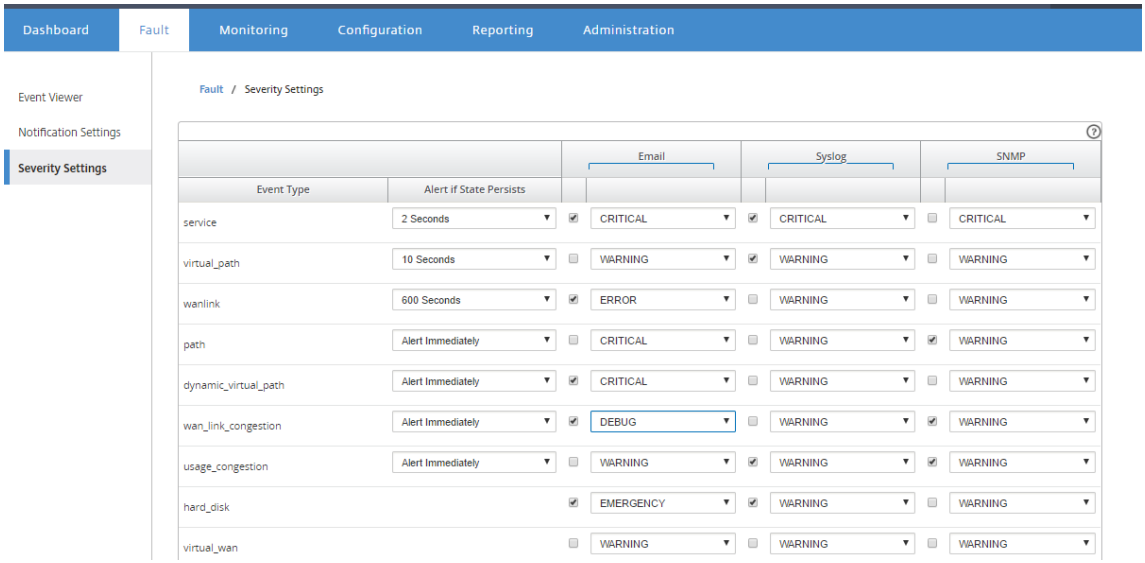
3. Geben Sie im Feld **Host** die IP-Adresse oder den Hostnamen eines externen Syslog-Servers ein, der zum Empfangen von Ereignissen als Syslog-Nachrichten verwendet wird.
4. Klicken Sie auf **Über** nehmen, um die Syslog-Benachrichtigungseinstellungen anzuwenden.

> **Hinweis**
>
> Klicken Sie alternativ auf **Testnachricht senden**, um zu überprüfen, ob das System eine Syslog-Nachricht an den konfigurierten Host senden kann.

Konfigurieren von Ereignisbenachrichtigungen

So konfigurieren Sie Ereignisbenachrichtigungen:

1. Navigieren Sie in der Webverwaltungsschnittstelle von Citrix SD-WAN Center zu **Fehler** > **Schweregrad-Einstellungen**.
2. Wählen Sie im Feld **Warnung, wenn Sate weiterhin besteht**, die Zeitdauer aus, nach der eine Benachrichtigung gesendet wird, wenn das Ereignis weiterhin besteht.



3. Wählen Sie für jeden Ereignistyp die Benachrichtigungsoption und wählen Sie den Schweregrad aus.

> **Hinweis**
>
> Die Benachrichtigungsoptionen E-Mail, Syslog und SNMP werden erst nach der Konfiguration der entsprechenden Benachrichtigungseinstellungen aktiviert.

4. Klicken Sie auf **Apply**.

Konfigurieren von Alarmen

Sie können auch Alarme in Citrix SD-WAN Center konfigurieren und auf einzelne Appliances übertragen.

Um den Alarm in Citrix SD-WAN Center zu konfigurieren, navigieren Sie zu **Konfiguration** > **Appliance-Einstellungen** > **Benachrichtigungseinstellungen** > **Alarmkonfiguration** und klicken Sie auf **+**.

Wählen Sie Werte für die folgenden Felder aus, oder geben Sie sie ein:

- **Ereignistyp**: Die Citrix SD-WAN-Appliance kann Alarme für bestimmte Subsysteme oder Objekte im Netzwerk auslösen. Diese werden als Ereignistypen bezeichnet. Die verfügbaren Ereignistypen sind SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH,

WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL, and IPSEC_TUNNEL.

- **Triggerstatus:** Der Ereignisstatus, der einen Alarm für einen Ereignistyp auslöst. Die verfügbaren Optionen für den Triggerstatus hängen vom gewählten Ereignistyp ab.
- **Triggerdauer**: Die Dauer in Sekunden bestimmt, wie schnell die Appliance einen Alarm auslöst. Geben Sie 0 ein, um sofortige Warnungen zu erhalten, oder geben Sie einen Wert zwischen 15-7200 Sekunden ein.Alarme werden nicht ausgelöst, wenn innerhalb der Triggerdauer zusätzliche Ereignisse auf demselben Objekt auftreten. Zusätzliche Alarme werden nur ausgelöst, wenn ein Ereignis länger als die Dauer der Triggerdauer ist.
- **Clear State**: Der Ereignisstatus, der einen Alarm für einen Ereignistyp löscht, nachdem der Alarm ausgelöst wurde. Die verfügbaren Optionen für den Clear State sind vom gewählten Triggerstatus abhängig.
- **Dauer löschen:** Die Dauer in Sekunden, die bestimmt, wie lange gewartet werden soll, bevor ein Alarm gelöscht wird.Geben Sie "0"ein, um den Alarm sofort zu löschen, oder geben Sie einen Wert zwischen 15-7200 Sekunden ein. Der Alarm wird nicht gelöscht, wenn innerhalb der angegebenen Zeit ein weiteres Clear-State-Ereignis am selben Objekt auftritt.
- **Schweregrad**: Ein benutzerdefiniertes Feld, das bestimmt, wie dringend ein Alarm ist. Der Schweregrad wird in den Alerts, die bei Auslösung oder Löschvorgang des Alarms gesendet werden, und in der Zusammenfassung der ausgelösten Alarme angezeigt.
- **E-Mail**: Alarmauslöser und Löschwarnungen für den Ereignistyp werden per E-Mail gesendet.
- **Syslog**: Alarmauslöser und Clear Alerts für den Ereignistyp werden über Syslog gesendet.
- **SNMP**: Alarmauslöser und klare Alarme für den Ereignistyp werden über SNMP-Trap gesendet.

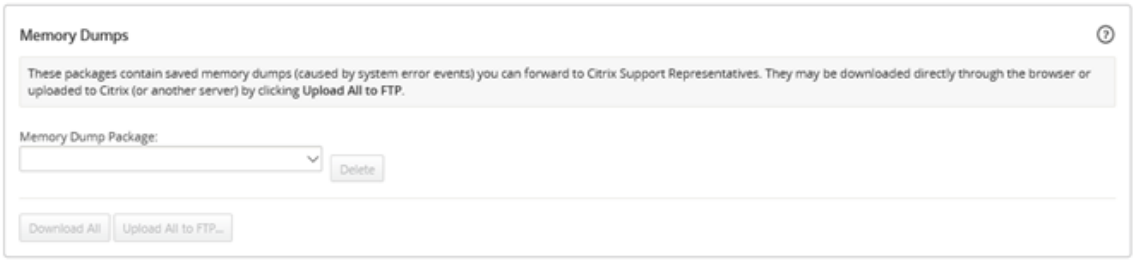
Speicherabbilder

April 13, 2021

Ein Speicherabbild wird generiert, wenn ein Prozess abstürzt. Alle Speicherabbilder, die derzeit auf dem System verfügbar sind, können in einem kombinierten Paket heruntergeladen und zur Prüfung durch das Citrix Support-Team auf einen FTP-Server hochgeladen werden. Sie können jedoch einzelne Speicherabbilder löschen.

So laden Sie Speicherabbilder herunter:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Überwachung**, und klicken Sie dann auf **Diagnose**.
2. Wählen Sie im Abschnitt **Speicherabbilder** aus der Dropdownliste **Speicherabbildpaket** ein Speicherabbildpaket aus.



3. Klicken Sie auf **Alle herunterladen**. Speichern Sie das Speicherabbildpaket auf Ihrem lokalen Computer.

So laden Sie ein Speicherabbildpaket auf einen FTP-Server hoch:

1. Wählen Sie im Abschnitt **Speicherabbilder** aus der Dropdownliste **Speicherabbildpaket** ein Speicherabbildpaket aus.
2. Klicken Sie auf **Auf FTP-Server hochladen**. Dadurch wird das Dialogfeld "**Alle auf FTP hochladen** "geöffnet, in dem Sie Ihre FTP-Authentifizierungsinformationen angeben und das Paket auf den Citrix Customer Support FTP-Server oder auf einen anderen FTP-Host hochladen können.

3. Geben Sie im Feld **Kundenname** einen Namen ein, der den Citrix SD-WAN-Support bei der Identifizierung der Diagnosepakete unterstützt.

   Ein Verzeichnis mit diesem Namen wird auf dem Citrix FTP-Server erstellt, und Ihre Dateien werden an diesen Speicherort hochgeladen.

4. Geben Sie im Feld **FTP-Host** die IP-Adresse oder den Hostnamen (falls DNS konfiguriert ist) des FTP-Servers ein.

5. Geben Sie im Feld **Benutzername** einen Benutzernamen ein, der für die Anmeldung am FTP-Server verwendet werden soll.
6. Geben Sie im Feld **Kennwort** das Kennwort ein, das dem Benutzernamen zugeordnet ist.
7. Klicken Sie auf **Upload**.

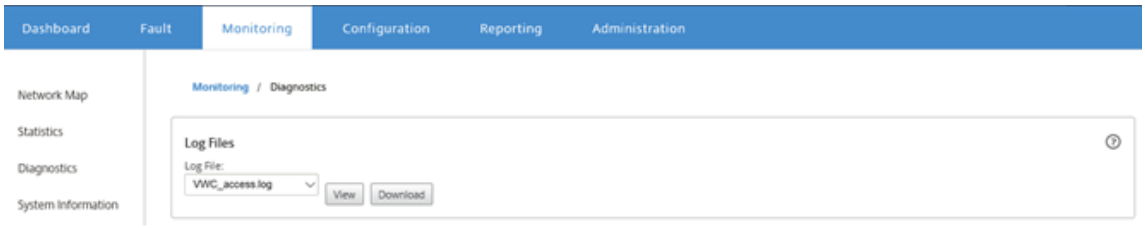
Protokolldateien

April 13, 2021

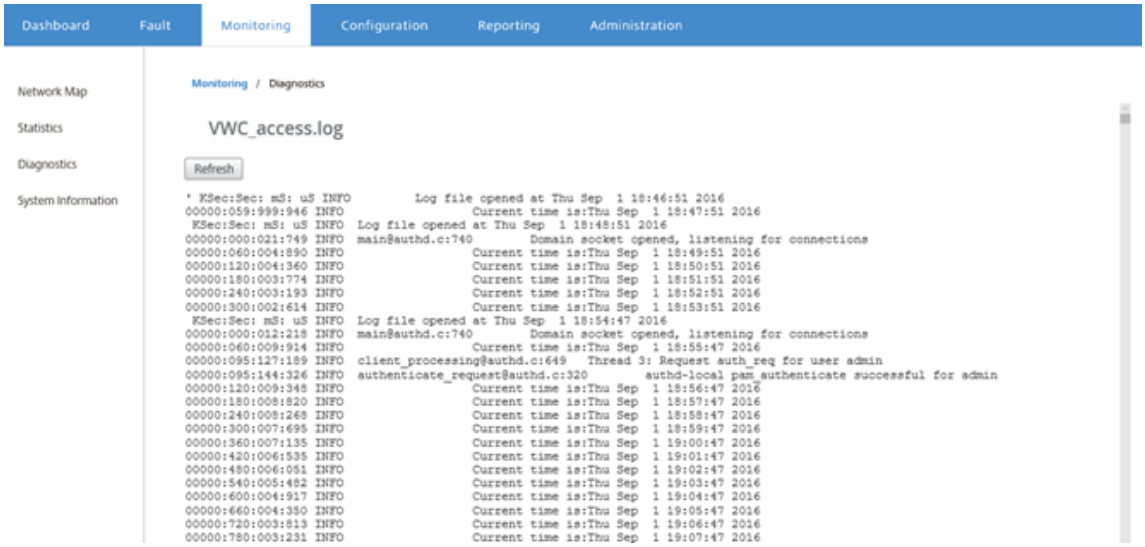
In den Protokolldateien werden Informationen über die Webkonsole, Benutzeroberflächenausnahmen, interne Abstürze usw. gesammelt. Diese Protokolle können zur Behebung von Problemen im Citrix SD-WAN Center verwendet werden.

So zeigen Sie Protokolldateien an:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Überwachung**.
2. Klicken Sie auf **Diagnose**.
3. Wählen **Sie in der Dropdownliste Protokolldatei** die Protokolldatei aus, die Sie anzeigen möchten.



4. Klicken Sie **auf Ansicht**. Der Inhalt der Protokolldatei wird angezeigt.



5. Wenn Sie die Protokolldateien auf Ihren Computer herunterladen möchten, klicken Sie auf **Herunterladen**.

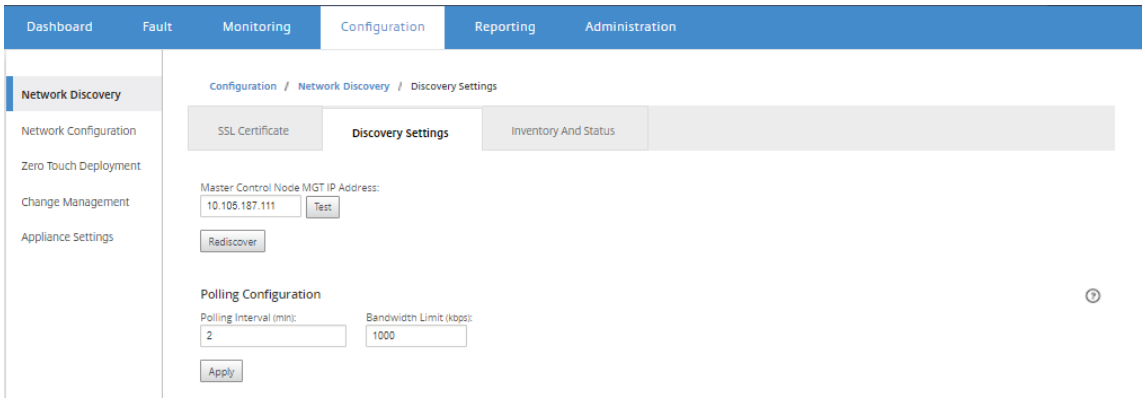
Abfrageintervall

April 13, 2021

Polling bezieht sich auf das Sammeln von Statistiken aus der erkannten Appliance. Sie können das Intervall und die Bandbreitenbegrenzung für Abrufvorgänge konfigurieren, nachdem Sie die Appliances entdeckt haben. Weitere Informationen zum Erkennen der Appliance finden Sie unterNetzwerkbereitstellung in einer RegionoderNetzwerkbereitstellung in mehreren Regionen.

So führen Sie die Abrufkonfiguration durch:

1. Navigieren Sie in der Citrix SD-WAN Center-Weboberfläche zu **Konfiguration** > **Netzwerkerkennung> Discoveryeinstellungen**.



2. Geben Sie im Feld **Abrufintervall** die Abruffrequenz in Minuten ein. Die Reichweite beträgt 2 —60 Minuten. Der Standardwert beträgt 5 Minuten.
3. Geben Sie im Feld **Bandbreitenlimit** den Grenzwert für die Abrufbandbreite in kbps ein. Das MCN beschränkt die Bandbreite auf den angegebenen Wert, wenn Abrufstatistiken von der Appliance an das Citrix SD-WAN Center übertragen werden. Der Bereich beträgt 100 Kbp —1 Gbit/s. Der Standardwert ist 1 Mbps.
4. Klicken Sie auf **Apply**.

Statistik

April 13, 2021

Sie können die vom Citrix SD-WAN Center erfassten Statistiken als Diagramme anzeigen. Diese Diagramme werden als Zeitachse und Verwendung dargestellt, sodass Sie die Verwendungstrends verschiedener Netzwerkobjekteigenschaften verstehen können. Sie können Diagramme für netzwerkweite Anwendungsstatistiken anzeigen. Für jeden Standort im SD-WAN-Netzwerk können Sie Diagramme für die folgenden Netzwerkparameter anzeigen:

- Bandbreite
- QoS
- Virtueller Pfad
- Internetdienste
- Intranetdienste
- Passthrough-Dienste
- WAN-Links
- Ethernet-Schnittstellen
- GRE Tunnel
- IPSec-Tunnel
- Anwendungen
- Anwendungsfamilien

> **Tipp**
>
> Sie können Ansichten nach Ihren Anforderungen erstellen, speichern und vorhandene Ansichten öffnen.

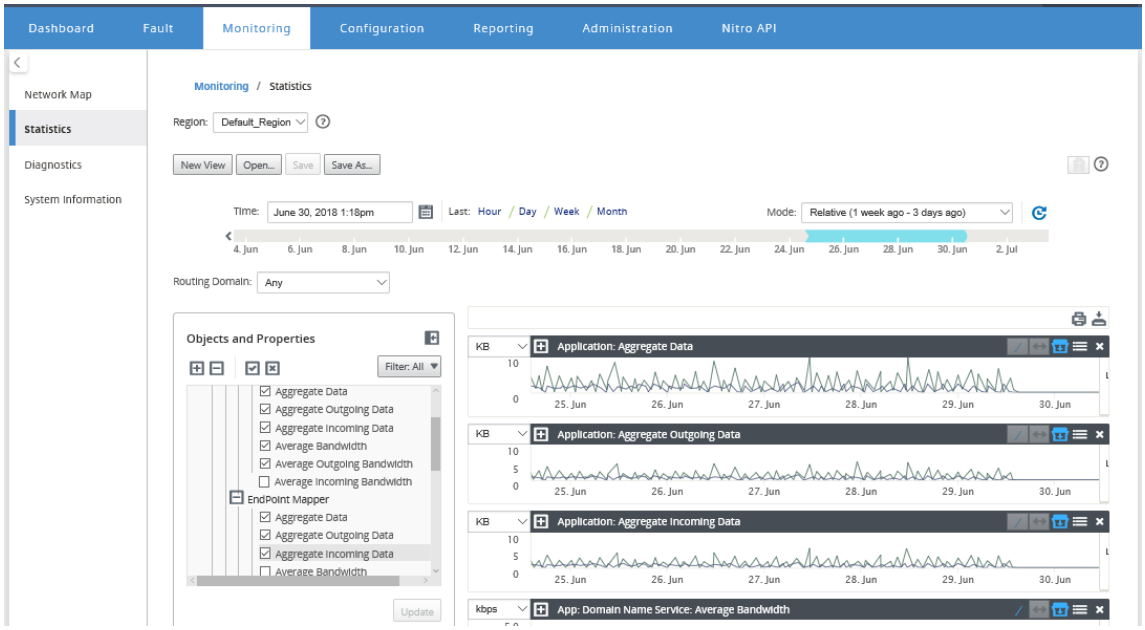
So zeigen Sie statistische Diagramme an:

1. Navigieren Sie in der Citrix SD-WAN Center Web-Benutzeroberfläche zu **Überwachung** > **Statistik**.

2. Wählen Sie eine Region und eine Routingdomäne aus.
3. Suchen **und wählen Sie im hierarchischen Baum Objekte** und Eigenschaften die gewünschten Eigenschaften aus.

> **Tipp**
>
> Sie können auch das Dropdownmenü **Filter** und das Menü **Voreinstellungen** verwenden, um das Suchen und Auswählen von Eigenschaften zu vereinfachen.

4. Klicken Sie auf **Aktualisieren**, um Diagramme für die ausgewählten Eigenschaften anzuzeigen.

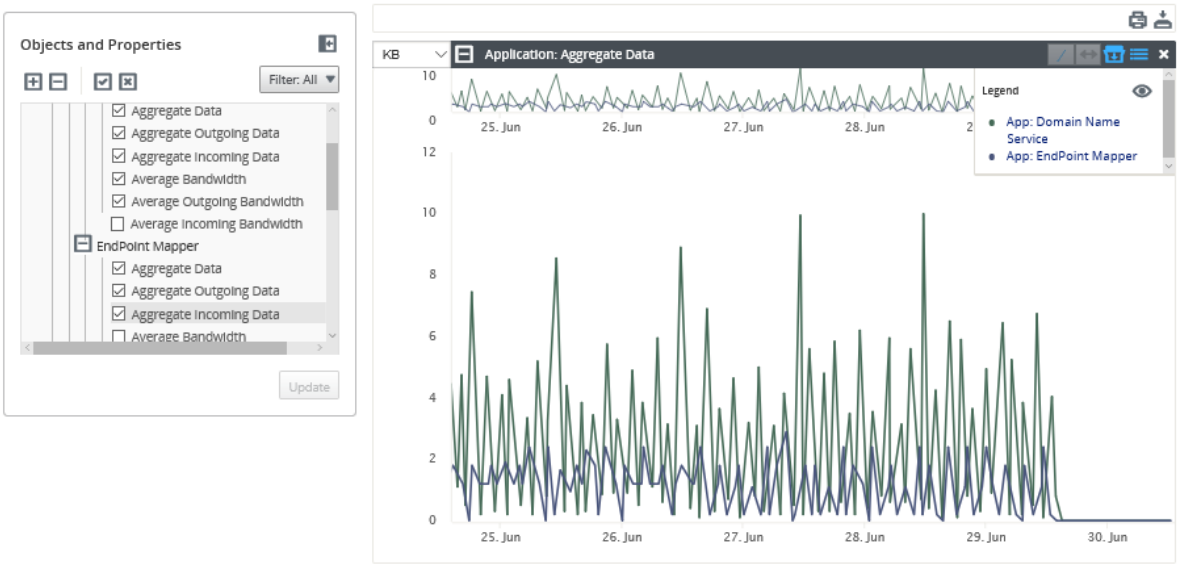


> **Tipp**
>
> Deaktivieren Sie eine Eigenschaft, und klicken Sie auf **Aktualisieren**, um das Diagramm für diese Eigenschaft aus dem Bereich Diagrammanzeige zu entfernen.

5. Wählen Sie einen Zeitraum für die aktuelle Ansicht aus. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente

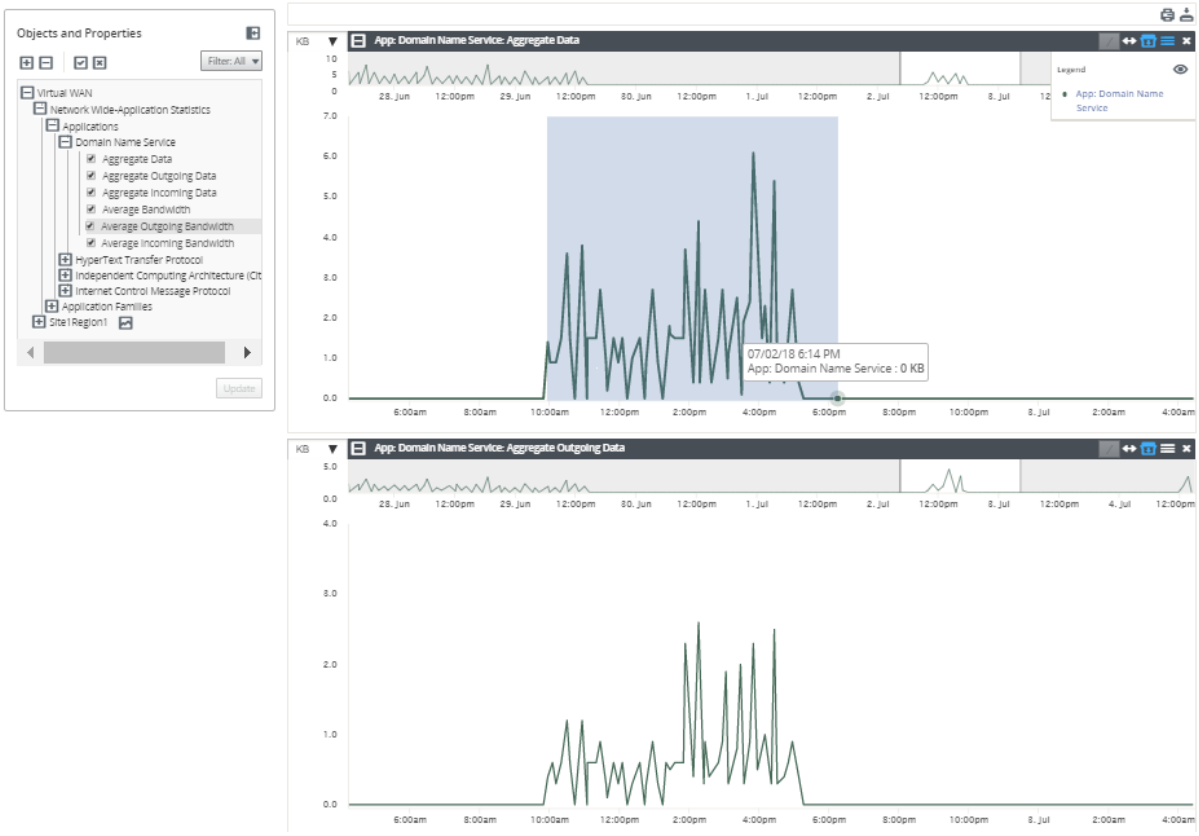
   Die Diagramme werden basierend auf den ausgewählten Eigenschaften angezeigt.

> **Tipp**
>
> Wenn Sie mehrere Eigenschaften auswählen, werden die Diagramme im **Trendansicht**-Modus angezeigt, um vertikalen Platz zu sparen. Klicken Sie auf eine Diagrammüberschrift, um das vollständig erweiterte Diagramm ein- und auszublenden. Sie können auch die Trendansicht und Legenden in den Diagrammen ein- und ausblenden.

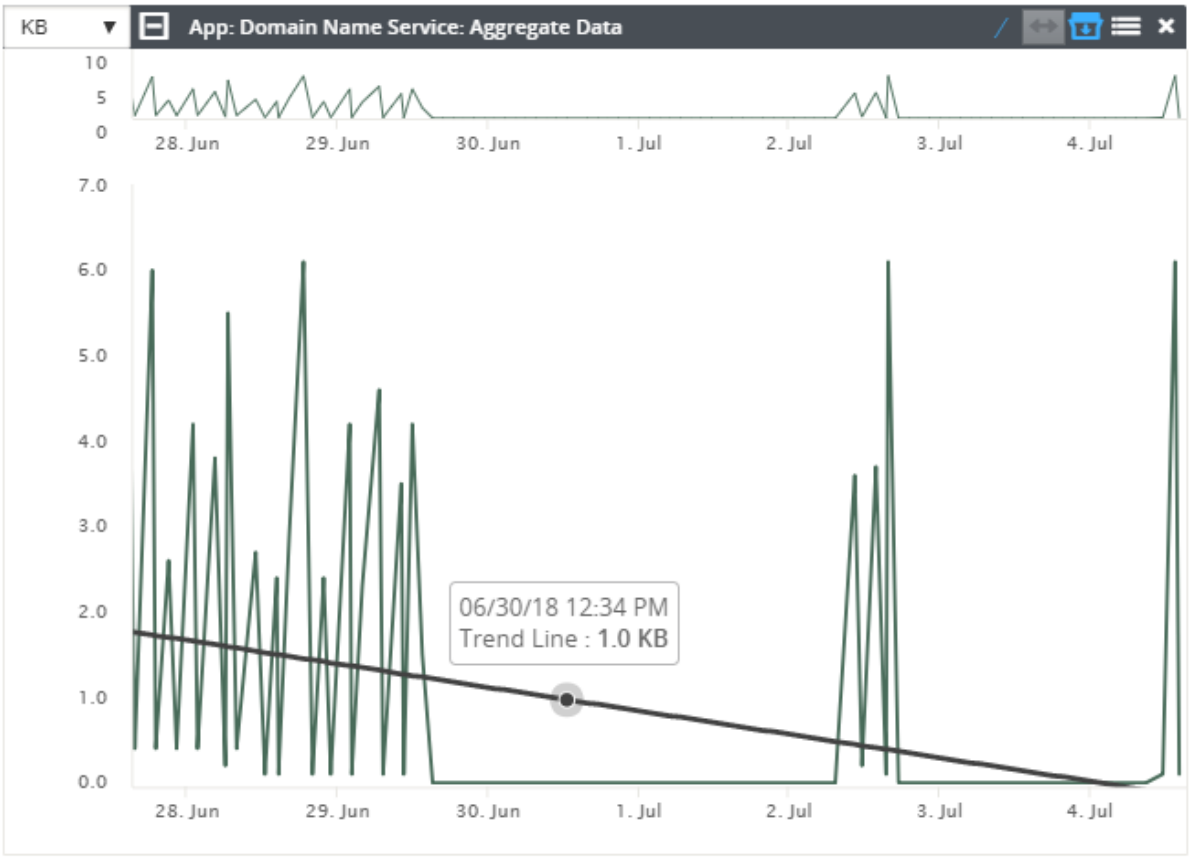


Tipp

Um ein Diagramm zu zoomen, klicken Sie auf den Diagrammplot und ziehen Sie ihn. Durch das Zoomen auf einem Diagramm werden alle Diagramme auf die ausgewählte Zeit gezoomt, um eine einheitliche Ansicht beizubehalten. Klicken Sie auf das Reset-Symbol (↔), um den Zoom zurückzusetzen.



> **Tipp**
>
> Sie können die Trendlinie ein- und ausblenden, indem Sie auf das Symbol (/) klicken.



> **Hinweis**
>
> Sie können die Grafiken drucken oder den Diagrammsatz als CSV-Datei herunterladen.

Systeminformationen

April 13, 2021

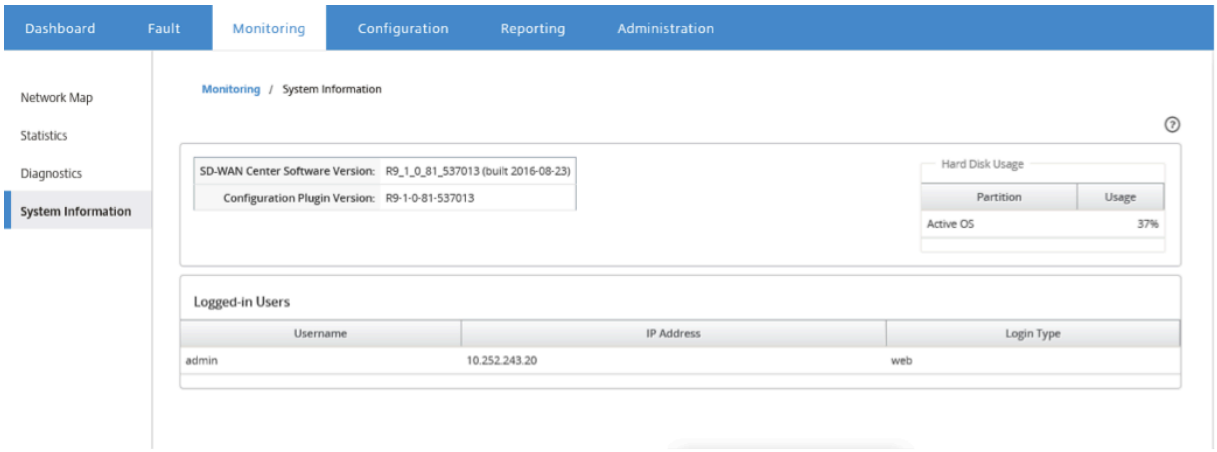
Die folgenden Informationen werden auf der Systeminformationsseite angezeigt:

- **Citrix SD-WAN Center Softwareversion**: Die Citrix SD-WAN Center-Softwareversion, die derzeit auf dieser virtuellen Maschine installiert ist und ausgeführt wird.
- **Version des Konfigurations-Plug-ins**: Die Version des Konfigurationseditor-Plug-Ins, die derzeit auf dieser virtuellen Citrix SD-WAN Center-Maschine installiert und ausgeführt wird.

- **Festplattennutzung**: Die Menge des Festplattenspeichers, der vom Betriebssystem und von Datenpartitionen verwendet wird.
- An@@**gemeldete Benutzer**: Benutzername, IP-Adresse und Anmeldetyp für jeden Benutzer, der sich derzeit an dieser virtuellen Citrix SD-WAN Center-Maschine angemeldet hat.

So zeigen Sie die Systeminformationen an:

Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Überwachung**, und klicken Sie dann auf **Systeminformationen**.



Berichterstellung

April 13, 2021

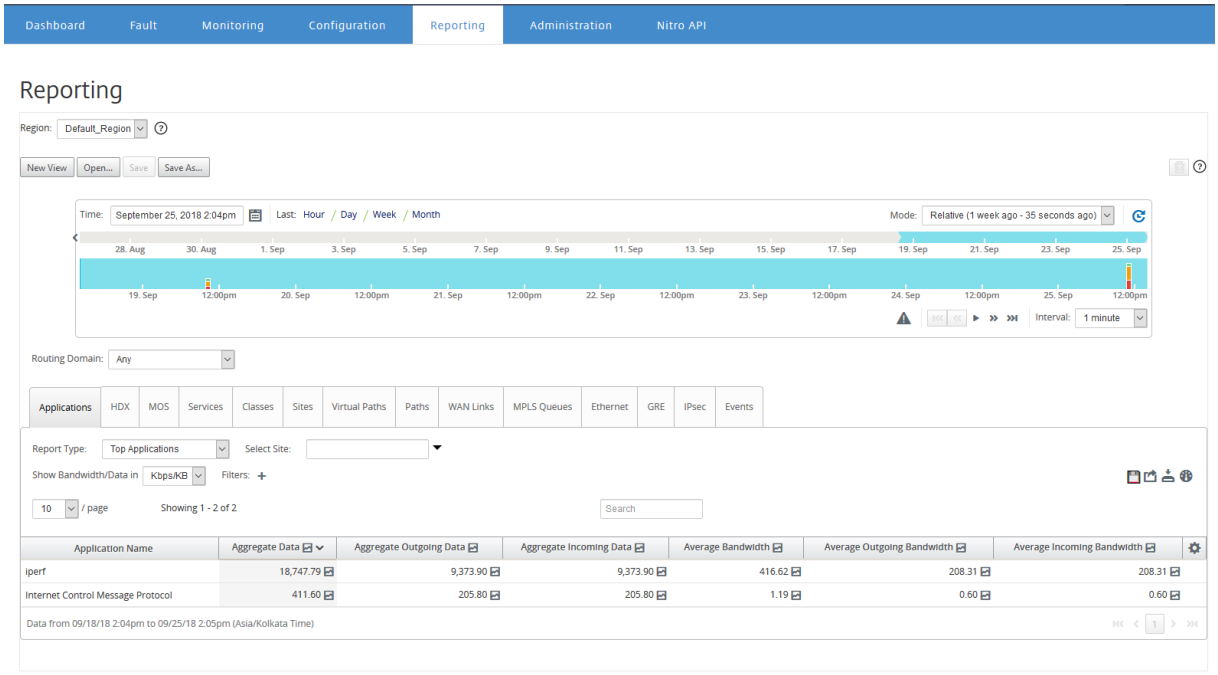
Citrix SD-WAN Center bietet die folgenden Berichte:

- **Anwendungen:** Zeigt Details über eingehenden Datenverkehr, ausgehenden Datenverkehr und den gesamten Datenverkehr der wichtigsten Anwendungen, Sites und Anwendungsfamilien an.
- **HDX**: Zeigt detaillierte HDX-Daten für jeden Standort an.
- **Sites:** Zeigt Statistiken auf Siteebene für jede Site im virtuellen WAN an. Sites Zeilen werden erweitert, um die Tabelle **Services** anzuzeigen, die für die Site gefiltert wurde.
- **Service:** Zeigt zusammenfassende Statistiken nach Diensttyp (Virtual Path, Internet, Intranet und Pass-Through) für jede Site im Virtual WAN an. Dienstzeilen werden erweitert, um die einzelnen Dienste für den Diensttyp anzuzeigen.
- **Virtuelle Pfade:** Zeigt Statistiken über virtuelle Pfadebene für jeden virtuellen Pfad im SD-WAN an. Virtuelle Pfade Zeilen werden erweitert, um die im virtuellen Pfad enthaltenen Pfade anzuzeigen.

> **Hinweis**
>
> Virtuelle Pfaddaten werden aus der Perspektive beider Endpunkte aufgezeichnet. Jeder virtuelle Pfad kann zwei Zeilen aufweisen, die von der Site identifiziert wurden, auf der die Statistiken aufgezeichnet wurden.

- **Pfade:** Zeigt Statistiken auf Pfadebene für jeden Pfad im virtuellen WAN an.
- **WAN-Links:** Zeigt Statistiken auf WAN-Link-Ebene für jeden WAN-Link an jeder Site im virtuellen WAN an. WAN-Verknüpfungszeilen werden erweitert, um eine Nutzungsübersicht für jeden Diensttyp für diesen WAN-Link anzuzeigen. Jede Diensttypzeile wird dann erweitert, um Verwendungen für jeden Dienst dieses Typs anzuzeigen. Wenn es sich bei der WAN-Verbindung um einen privaten MPLS-Link handelt, wird eine zweite Tabelle mit den MPLS-Warteschlangen für den WAN-Link angezeigt.
- **MPLS-Warteschlangen:** Die MPLS-Warteschlangenzeilen werden erweitert, um eine Nutzungszusammenfassung für jeden Diensttyp für diese Warteschlange anzuzeigen. Jede Diensttypzeile wird dann erweitert, um Verwendungen für jeden Dienst dieses Typs anzuzeigen.
- **Klassen:** Zeigt Statistiken auf Klassenebene für jede Klasse für jeden virtuellen Pfad im virtuellen WAN an.
- **MOS Score**: Der Mean Opinion Score (MOS) liefert ein numerisches Maß für die Qualität der Erfahrung, die eine Anwendung für Endbenutzer liefert.
- **Ethernet-Schnittstellen:** Zeigt Statistiken auf Ethernet-Schnittstellenebene für jede Schnittstelle an jedem Standort im virtuellen WAN an.
- **GRE Tunnel:** Zeigt Statistiken aller LAN GRE Tunnel an jedem Standort im WAN an.
- **IPsec-Tunnel:** Zeigt Statistiken aller IP-Sicherheitstunnel an jedem Standort im WAN an.
- **Ereignisse:** Zeigt zusammenfassende Anzahl der Ereignisse an, die an jeder Site im virtuellen WAN auftreten. **Ereigniszeilen** werden erweitert, um die Zusammenfassungsanzahl nach Objekttyp für diese Site anzuzeigen. Jeder Objekttyp wird dann erweitert, um Zusammenfassungszählungen für jedes Objekt dieses Typs anzuzeigen.

Auf der Registerkarte **Reporting** der Citrix SD-WAN Center-Weboberfläche können Sie alle Berichte oder ausgewählte Berichte anzeigen. Sie können auch Berichte herunterladen.

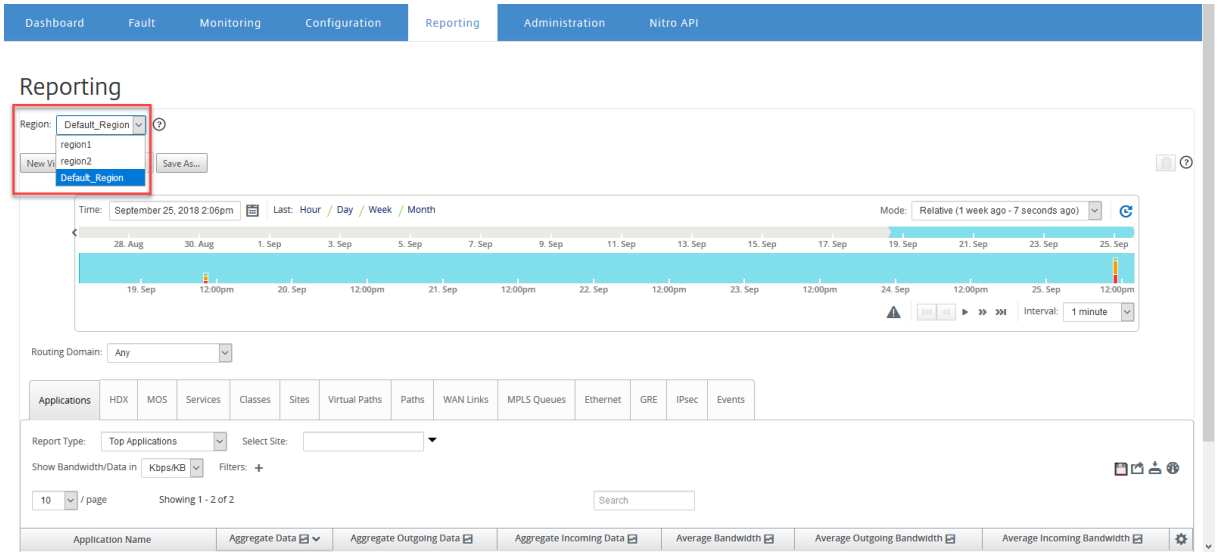


Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.

Für Netzwerk mit mehreren Regionen können Sie bestimmte Regionen auswählen, um Statistikberichte anzuzeigen.

Die Berichtsdaten werden aus dem Kollektor der jeweiligen Region abgerufen.



> **Hinweis**
>
> Bei einer Netzwerkbereitstellung mit einer **Region** ist die Dropdownliste “Region”nicht verfügbar.

Weitere Informationen zum Anzeigen verschiedener Berichte finden Sie in den folgenden Themen:

Anwendungsbericht

Bandbreitenbericht

Klassenbericht

Ethernet-Schnittstellenbericht

Ereignisbericht

GRE Tunnelbericht

HDX-Bericht

IPSec-Tunnelbericht

Verknüpfungsleistungsbericht

MOS für Anwendungen

MPLS-Warteschlangenbericht

Anwendungsbericht

April 13, 2021

Deep Packet Inspection (DPI) ermöglicht es der SD-WAN-Appliance, den durchgehenden Datenverkehr zu analysieren und die Anwendungs- und Anwendungsfamilientypen zu identifizieren. Die Citrix SD-WAN-Appliance zeichnet die Anzahl der Bytes und die Bandbreite des eingehenden und ausgehenden Datenverkehrs jeder Anwendung auf. SD-WAN Center fragt die SD-WAN-Appliance im definierten Abrufintervall ab, ruft diese Daten ab und zeigt sie im Dashboard und als Berichte an.

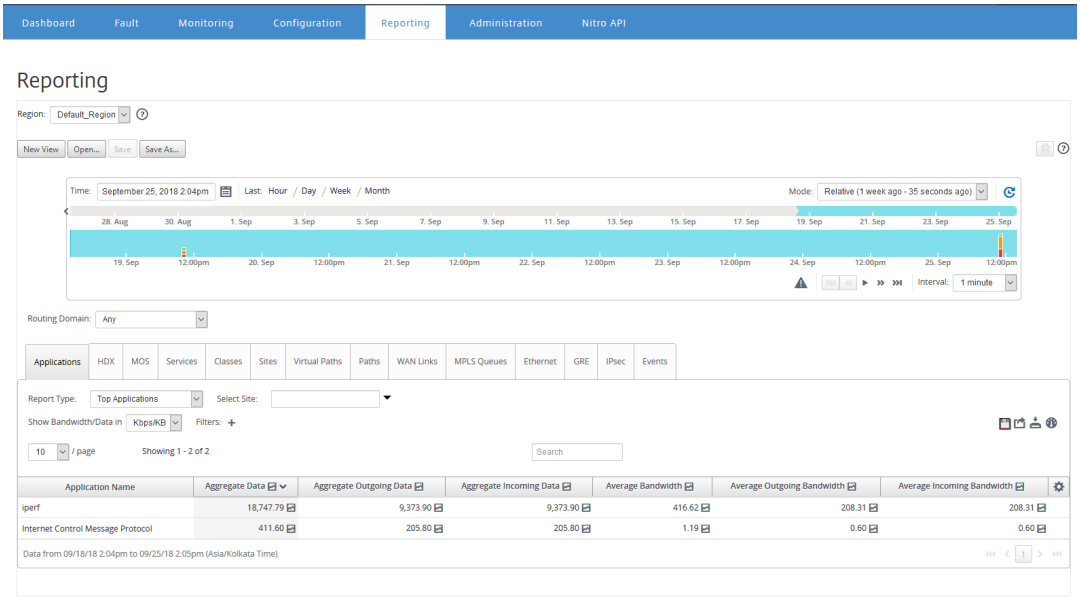
Sie können Top-Anwendungen, Top-Sites und Berichte der Top-Anwendungsfamilien anzeigen. Diese Berichte enthalten Details zu den Gesamtdaten, eingehenden und ausgehenden Daten und Bandbreite.

So zeigen Sie Anwendungsberichte in Citrix SD-WAN Center an:

1. Navigieren Sie in der Citrix SD-WAN Center Web-Benutzeroberfläche zu **Berichterstellung** > **Anwendungen**.

2. Wählen Sie im Zeitzeilen-Steuerelement das Zeitintervall aus. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.
3. Wählen Sie die Einheit aus, um die Daten anzuzeigen. Sie können Berichtsdaten in Einheiten von Kbps, Mbit/s oder Gbit/s anzeigen.
4. Wählen Sie in der Dropdownliste **Berichtstyp** einen der folgenden Berichtstypen aus:

    - **Top Applications**: Die Top-Anwendungen, die im Netzwerk für das ausgewählte Zeitintervall verwendet werden. Sie können die oberste Anwendung nach Sitename filtern. Standardmäßig werden die Top-Anwendungen für alle Sites angezeigt.
    - **Top Anwendungsfamilien**: Die wichtigsten Anwendungsfamilien, die im Netzwerk verwendet werden. Sie können die wichtigsten Anwendungsfamilien nach Sitename filtern. Standardmäßig werden die wichtigsten Anwendungsfamilien für alle Sites angezeigt.
    - **Top-Sites**: Traffic an den obersten Sites für das ausgewählte Zeitintervall. Sie können Top-Sites nach dem Namen der Anwendung oder der Anwendungsfamilie filtern.



Für jeden Berichtstyp können Sie die folgenden Daten anzeigen:

- **Aggregierte eingehende Daten**: Anwendungsdaten, die aus dem WAN in die Site gelangen.
- **Aggregierte ausgehende Daten**: Anwendungsdaten, die von der Site an das WAN gesendet werden.
- **Aggregierte Daten**: Summe des eingehenden und ausgehenden Datenverkehrs.
- **Durchschnittliche eingehende Bandbreite**: Bandbreite des eingehenden Anwendungsdatenverkehrs.
- **Durchschnittliche ausgehende Bandbreite**: Bandbreite des ausgehenden Anwendungsdatenverkehrs.

- **Durchschnittliche Bandbreite**: Gesamtbandbreite, die vom eingehenden und ausgehenden Anwendungsverkehr verbraucht wird.

> **Tipp**
>
> Für jeden Wert können Sie den Mauszeiger über das Diagrammsymbol bewegen, um eine Mini-Grafik anzuzeigen, oder klicken Sie auf, um die Diagrammansicht in einem anderen Fenster zu öffnen. Weitere Informationen finden Sie unter Statistik.

Anwendungs-QoE-Bericht

April 13, 2021

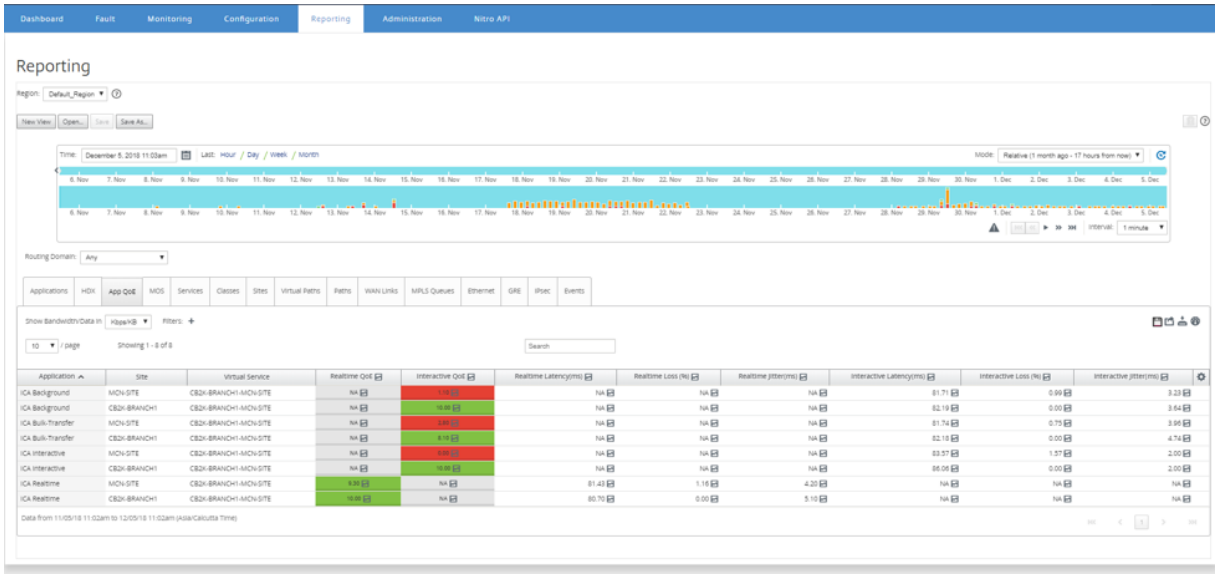
Anwendungs-QoE ist ein Maß für die Qualität der Benutzererfahrung für eine Anwendung. Der Anwendungs-QoE-Punktebereich beträgt 0 —10, wobei 10 eine ausgezeichnete Qualität und 0 eine schlechte Qualität darstellt. Weitere Informationen finden Sie im Abschnitt **Application QoE**.

So zeigen Sie die Auswertung “Anwendungs-QoE”an:

Navigieren Sie in Citrix SD-WAN Center zu **Reporting > App QoE**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitraums auswählen und anzeigen, indem Sie die Zeitachsen-Steuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Application:** Name der Anwendung oder des Anwendungsobjekts.
- **Site**: Der Name der Site.
- **Virtueller Dienst**: Der verwendete virtuelle Pfaddienst.
- **Echtzeit-QoE**: Der QoE-Wert für Echtzeit-Traffic.
- **Interaktives QoE**: Der QoE-Wert für interaktives Traffic.
- **Echtzeit-Latenz**: Die Latenz in Millisekunden für Echtzeitverkehr.
- **Echtzeitverlust**: Der Verlustprozentsatz für Echtzeitverkehr.
- **Echtzeit-Jitter**: Der in Millisekunden beobachtete Jitter für Echtzeitverkehr.
- **Interaktive Latenz**: Die Latenz in Millisekunden für interaktiven Datenverkehr.
- **Interaktiver Verlust**: Der Verlustprozentsatz für interaktiven Datenverkehr.
- **Interaktiver Jitter**: Der in Millisekunden beobachtete Jitter für interaktiven Verkehr.

> **TIPP**:
>
> Für jeden Wert können Sie den Mauszeiger über das Diagrammsymbol bewegen, um eine Mini-Grafik anzuzeigen, oder klicken Sie auf, um die Diagrammansicht in einem anderen Fenster zu öffnen.

Weitere Informationen finden Sie unter Statistik.

Bandbreitenbericht

April 13, 2021

Das Citrix SD-WAN Center bietet eine zentrale Ansicht der Bandbreitenstatistikdaten, die von verschiedenen Standorten in Ihrem SD-WAN-Netzwerk abgefragt werden.

In der Citrix SD-WAN-Konfiguration wird Datenverkehr, der durch die virtuellen Pfade fließt, als Zugehörigkeit zu Echtzeit-, interaktiven oder Massenklassentypen klassifiziert. Die Klassen sind vordefiniert, aber Sie können diese Klassen anpassen und Regeln auf sie anwenden. Weitere Informationen finden Sie unter Klasse anpassen und Regeln nach IP-Addess und Portnummer.

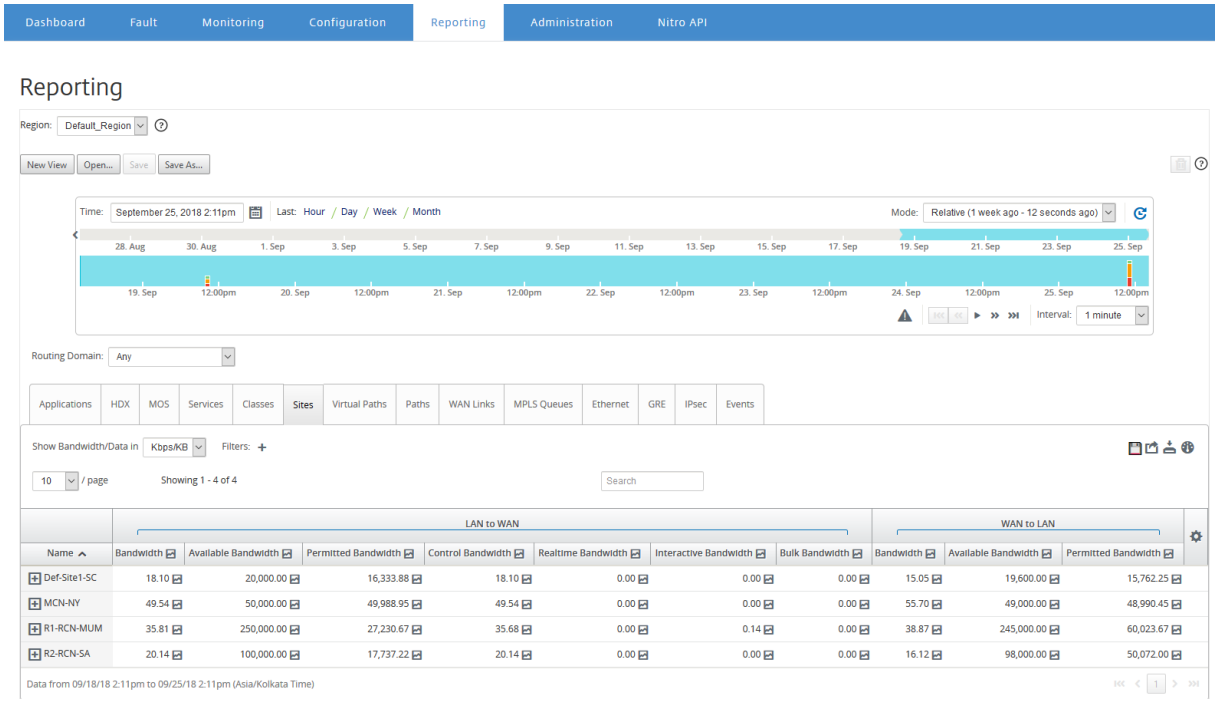
Mit Citrix SD-WAN Center können Sie zusammen mit den grundlegenden Bandbreitenstatistiken die Bandbreite anzeigen, die von Anwendungen dieser Klassen auf jeder Standort-, Pfad- oder WAN-Link-Ebene belegt wird.

So zeigen Sie Bandbreitenstatistikenan:

Navigieren Sie in Citrix SD-WAN Center zu **Reporting** > **Sites**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Bandbreite**: Gesamtbandbreite, die von allen Pakettypen verbraucht wird. Bandbreite = Kontrolle der Bandbreite + Echtzeit-Bandbreite + Interaktive Bandbreite + Massenbandbreite. Zum Beispiel im obigen Screenshot, bei SITE2, Bandbreite = 1120,99 + 166,61 + 117,21 + 810,78 + 26.40
- **Verfügbare Bandbreite**: Gesamtbandbreite, die allen WAN-Links einer Site zugewiesen ist.
- **Kontrollbandbreite**: Bandbreite, die zum Übertragen von Steuerungspaketen verwendet wird, die Routing-, Planungs- und Verknüpfungsstatistikinformationen enthalten.
- **Zulässige Bandbreite**: Bandbreite zur Übertragung von Informationen.
- **Realtime Bandwidth:** Bandbreite, die von Anwendungen verbraucht wird, die zum Typ der Echtzeitklasse in der Citrix SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Interaktive Bandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der Citrix SD-WAN Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
- **Massenbandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die zum Massenklassentyp der Citrix SD-WAN-Konfiguration gehören. Diese Anwendungen erfordern sehr wenig menschliches Eingreifen und werden meist von den Systemen selbst gehandhabt (z. B.

FTP, Backup-Operationen).

Klassenbericht

April 13, 2021

Die virtuellen Dienste können bestimmten QoS-Klassen zugewiesen werden, und verschiedene Bandbreitenbeschränkungen können auf verschiedene Klassen angewendet werden. Eine Klasse kann einer von drei Grundtypen sein:

- **Echtzeitklassen**: Servieren Sie Datenverkehrsflüsse, die Prompt-Service bis zu einem bestimmten Bandbreitenlimit erfordern. Niedrige Latenz wird gegenüber dem aggregierten Durchsatz bevorzugt.
- **Interaktive Klassen**: Servieren Sie Datenverkehrsflüsse, die gegenüber Verlust und Latenz empfindlich sind. Interaktive Klassen haben eine niedrigere Priorität als in Echtzeit, haben jedoch absolute Priorität gegenüber Massenverkehr.
- **Massenklassen**: Servieren Sie Datenverkehrsflüsse, die eine hohe Bandbreite erfordern und verlustempfindlich sind. Massenklassen haben die niedrigste Priorität.

Durch die Angabe unterschiedlicher Bandbreitenanforderungen für verschiedene Klassen kann der virtuelle Pfadplaner konkurrierende Bandbreitenanforderungen aus mehreren Klassen desselben Typs festlegen. Der Scheduler verwendet den HFSC-Algorithmus (Hierarchical Fair Service Curve), um Fairness zwischen den Klassen zu erreichen.

Weitere Hinweise zum Anpassen von Klassen finden Sie unterAnpassen von Klassen.

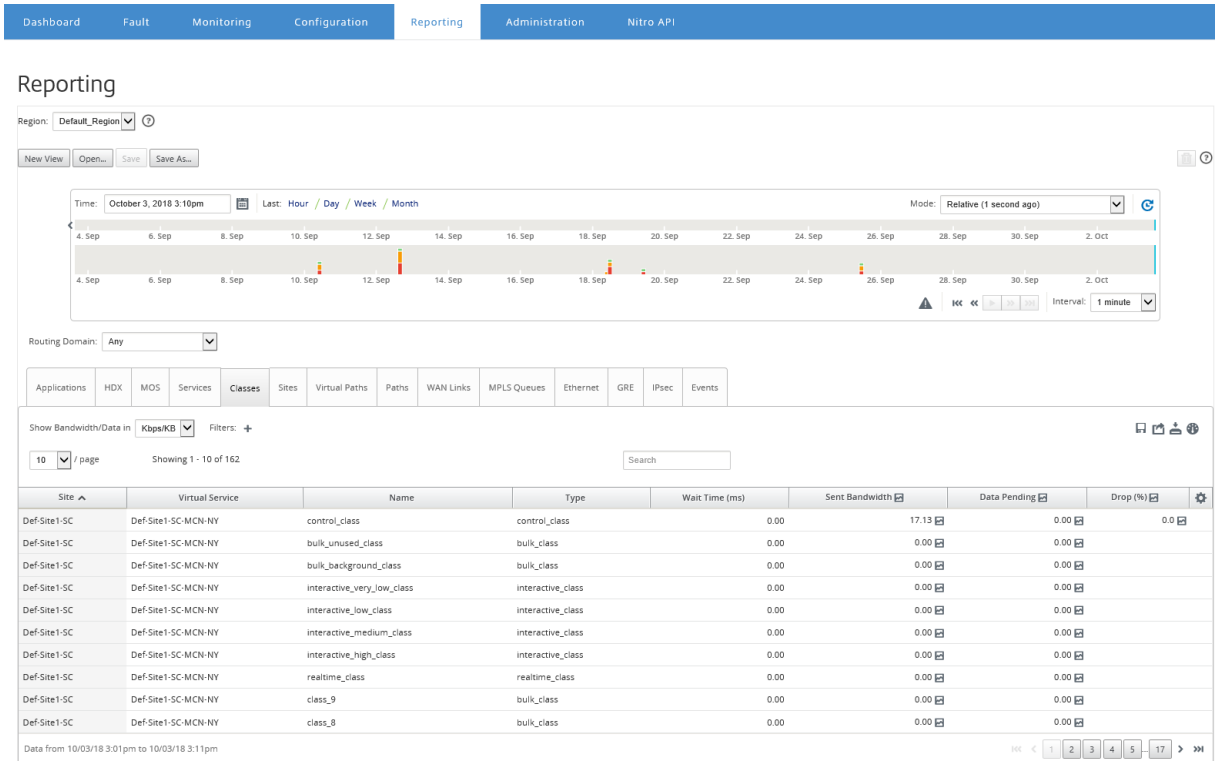
So zeigen Sie Klassenstatistikenan:

Navigieren Sie in Citrix SD-WAN Center zu **Berichte** > **Klassen**, und wählen Sie im Zeitplan-Steuerelement einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitraums auswählen und anzeigen, indem Sie die Zeitachsen-Steuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

> **Hinweis**
>
> Sie können die Klassendaten der letzten 30 Tage anzeigen. Jegliche Daten über diesen Zeitraum hinaus werden automatisch aus dem SD-WAN Center Collector und den jeweiligen regionalen Collectors entfernt.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Name**: Klassenname
- **Typ**: Klassentyp. Realtime, interaktiv oder Bulk.
- **Wartezeit**: Das Zeitintervall zwischen der Übertragung von Paketen in Millisekunden.
- **Gesendete Bandbreite**: Übertragene Bandbreite
- **Gesendete Daten**: Gesendete Daten in Kbps.
- **Gesendete Pakete**: Anzahl der gesendeten Pakete.
- **Daten ausstehend**: Zu sendende Daten in Kbps.
- **Ausstehende Pakete**: Anzahl der Pakete, die gesendet werden sollen.
- **Drop**: Prozentsatz der Daten, die gelöscht wurden.
- **Daten gelöscht**: Daten wurden gelöscht, in Kbps.
- **Verworfene Pakete**: Anzahl der Pakete, die aufgrund von Netzwerküberlastung gelöscht wurden.
- **Datenabdeckung**: Prozentsatz des ausgewählten Zeitraums, für den Daten verfügbar sind.

> **Hinweis**
>
> Klicken Sie auf das Einstellungssymbol, um die Metriken auszuwählen, die Sie anzeigen möchten.

Ethernet-Schnittstellenbericht

April 13, 2021

Das Citrix SD-WAN Center bietet eine zentrale Ansicht aller Ethernet-Schnittstellen auf den verschiedenen Citrix SD-WAN-Appliances in Ihrem SD-WAN-Netzwerk. Auf diese Weise können Sie bei der Fehlerbehebung schnell feststellen, ob einer der Ports ausfällt. Sie können auch die übertragene und empfangene Bandbreite oder Paketdetails an jedem Port anzeigen. Sie können auch die Anzahl der Fehler anzeigen, die während eines bestimmten Zeitraums auf diesen Schnittstellen aufgetreten sind.

Die Ethernet-Schnittstellen werden während der Einrichtung des SD-WAN-Netzwerks auf jeder Citrix SD-WAN-Appliance konfiguriert.

Hinweise zum Konfigurieren von Schnittstellengruppen für MCN-Sites finden Sie unterMCN konfigurieren/en-us/citrix-sd-wan/10-2/configuration/set-up-master-control-node/configure-mcn.html.[()]

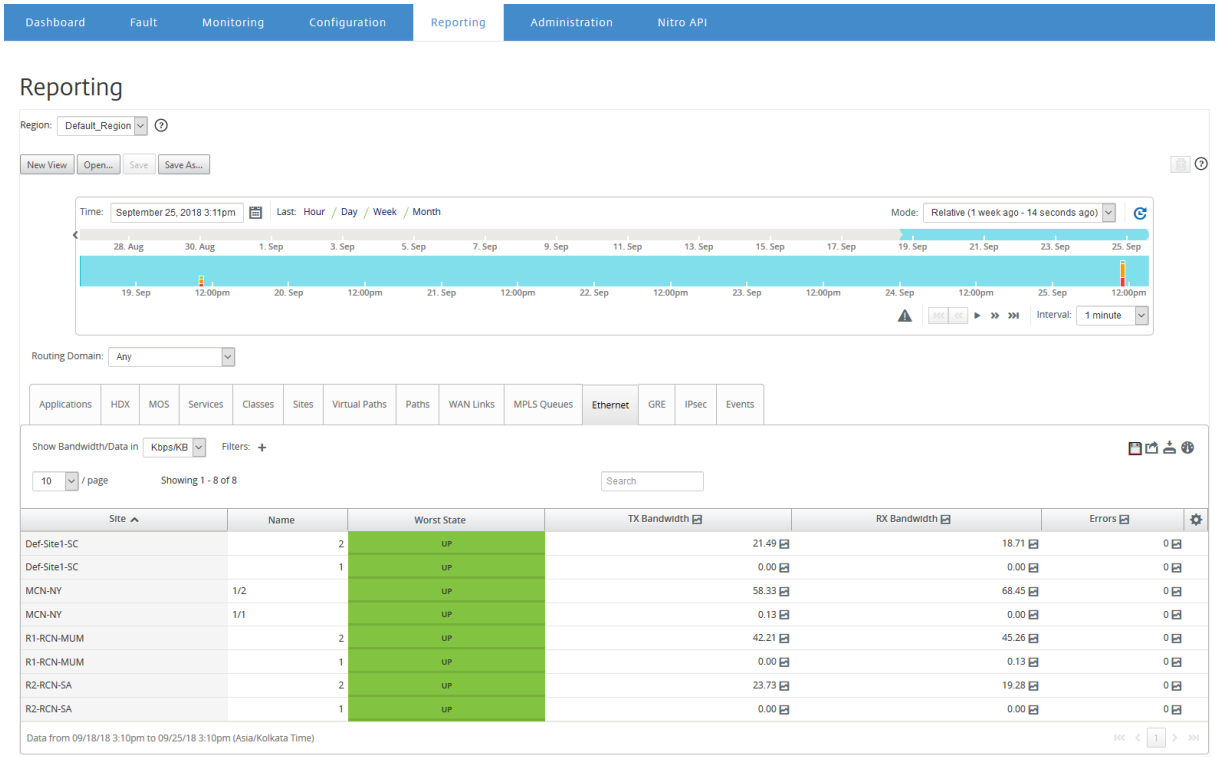
Hinweise zum Konfigurieren von Schnittstellengruppen für Zweigstandorte finden Sie unterZweigknoten konfigurieren.

So zeigen Sie Statistiken über die Ethernet-Schnittstellean:

Navigieren Sie in Citrix SD-WAN Center zu **Berichte** > **Ethernet**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Name**: Name der Ethernet-Schnittstelle.
- **Schlimmster Zustand**: Der schlechteste Zustand, der während des ausgewählten Zeitraums beobachtet wird.
- **TX-Bandbreite**: übertragene Bandbreite.
- **RX-Bandwidth**: empfangene Bandbreite.
- **TX-Pakete**: Anzahl der übertragenen Pakete.
- **RX-Pakete**: Anzahl der empfangenen Pakete.
- **Fehler**: Anzahl der während des ausgewählten Zeitraums beobachteten Fehler.
- **Datenabdeckung**: Prozentsatz des ausgewählten Zeitraums, für den Daten verfügbar sind.

> **Hinweis**
>
> Klicken Sie auf das Einstellungssymbol, um die Metriken auszuwählen, die Sie anzeigen möchten.

Ereignisbericht

April 13, 2021

Sie können die Anzahl der verschiedenen Ereignisse anzeigen, die an jedem Standort im SD-WAN-Netzwerk auftreten.

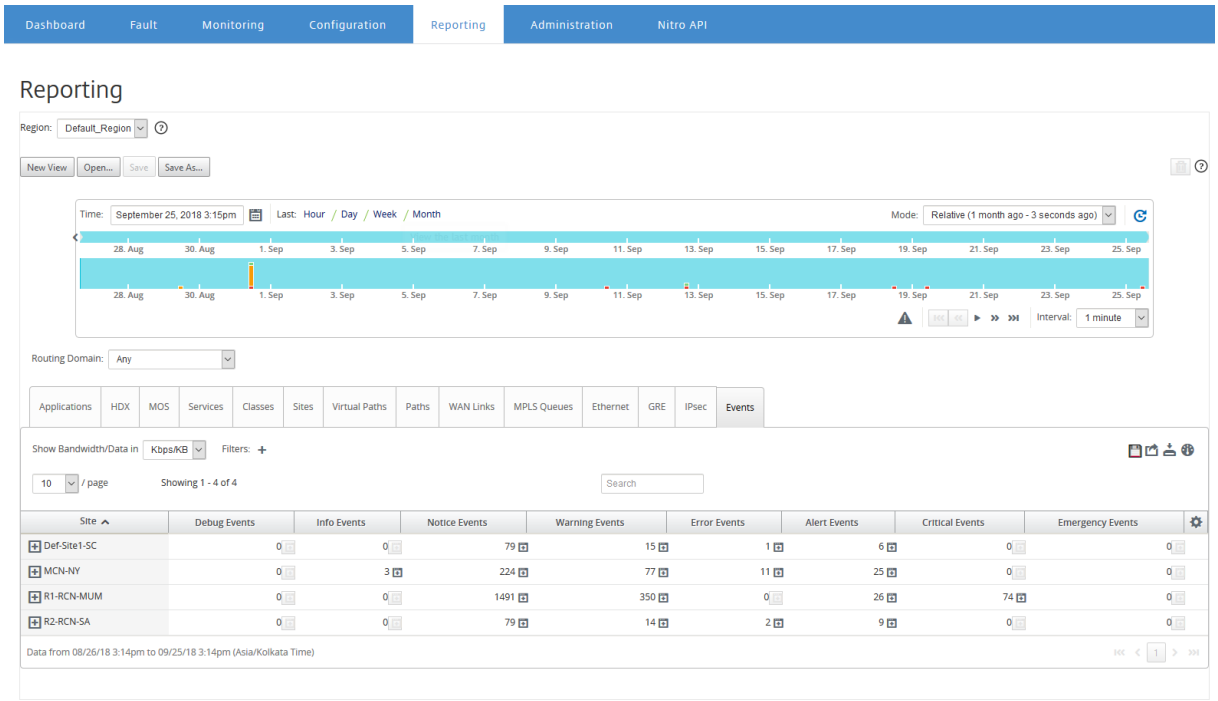
Weitere Hinweise zu Ereignissen finden Sie unterEreignisse.

So zeigen Sie Ereignisstatistikenan:

Navigieren Sie in Citrix SD-WAN Center zu **Berichte** > **Ereignisse**, und wählen Sie im Zeitplan-Steuerelement einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Info Events**: Anzahl der Informationsereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse auf niedriger Ebene.
- **Benachrichungsereignisse**: Anzahl der Benachrichungsereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse, über die der Administrator wissen sollte.
- **Warnungsereignisse**: Anzahl der Warnungsereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse, die in naher Zukunft Maßnahmen erfordern.
- **Fehlerereignisse**: Anzahl der Fehlerereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse, die auf eine Art von Fehler hinweisen.

- **Warnungsereignisse**: Anzahl der Warnungsereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse, die möglicherweise Maßnahmen erfordern.
- **Kritische Ereignisse**: Anzahl der kritischen Ereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse, die auf eine bevorstehende Krise hinweisen.
- **Notfallereignisse**: Anzahl der Notfallereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Dies sind Ereignisse, die auf eine sofortige Krise hinweisen (z. B. Stromversorgungsausfall, Lüfterausfall, Festplattenschwelle überschritten, Dienst deaktiviert).
- **Debug-Ereignisse**: Anzahl der Debug-Ereignisse, die während des ausgewählten Zeitraums aufgetreten sind. Debug-Ereignisse werden generiert, wenn Test-E-Mail oder Test Syslog auf den Citrix SD-WAN-Appliances verwendet werden.

> **Hinweis**
>
> Klicken Sie auf das Einstellungssymbol, um die Metriken auszuwählen, die Sie anzeigen möchten.

In der folgenden Tabelle sind einige Beispiele für Statusänderungen von Objekten aufgeführt, für die Ereignisse gemeldet werden.

Event	Object Type	Previous State	Current State
NOTICE	LAN to WAN path	BAD	GOOD
		GOOD	BAD
	WAN to LAN path	BAD	GOOD
		GOOD	BAD
	Dynamic virtual path	BAD	GOOD
		GOOD	BAD
WARNING	Virtual path	GOOD	BAD
	WAN link congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	Usage congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	LAN to WAN path	GOOD	DEAD
		BAD	DEAD
	WAN to LAN path	GOOD	DEAD
		BAD	DEAD
ALERT	Virtual path	BAD	DEAD
		DEAD	BAD
ERROR	WAN-link	GOOD	DEAD
	Ethernet	GOOD	UNDEFINED
		UNDEFINED	DEAD
INFO	Proxy-arp	UNDEFINED	ACTIVE
		UNDEFINED	STANDBY

Sie können Citrix SD-WAN Center so konfigurieren, dass externe Ereignisbenachrichtigungen für verschiedene Ereignistypen wie E-Mail, SNMP-Traps oder Syslog-Nachrichten gesendet werden. Weitere Informationen siehe Ereignisbenachrichtigungen.

GRE Tunnelbericht

April 13, 2021

Sie können einen Tunnelmechanismus verwenden, um Pakete eines Protokolls innerhalb eines anderen Protokolls zu transportieren. Das Protokoll, das das andere Protokoll trägt, wird als Transportprotokoll bezeichnet, und das mitgeführte Protokoll wird als Passagierprotokoll bezeichnet. Generic Routing Encapsulation (GRE) ist ein Tunnelmechanismus, der IP als Transportprotokoll verwendet und viele verschiedene Passagierprotokolle tragen kann.

Die Tunnelquelladresse und die Zieladresse werden verwendet, um die beiden Endpunkte der virtuellen Punkt-zu-Punkt-Verbindungen im Tunnel zu identifizieren.

Weitere Informationen zum Konfigurieren von GRE-Tunneln auf Citrix SD-WAN-Appliances finden Sie unter GRE Tunnel.

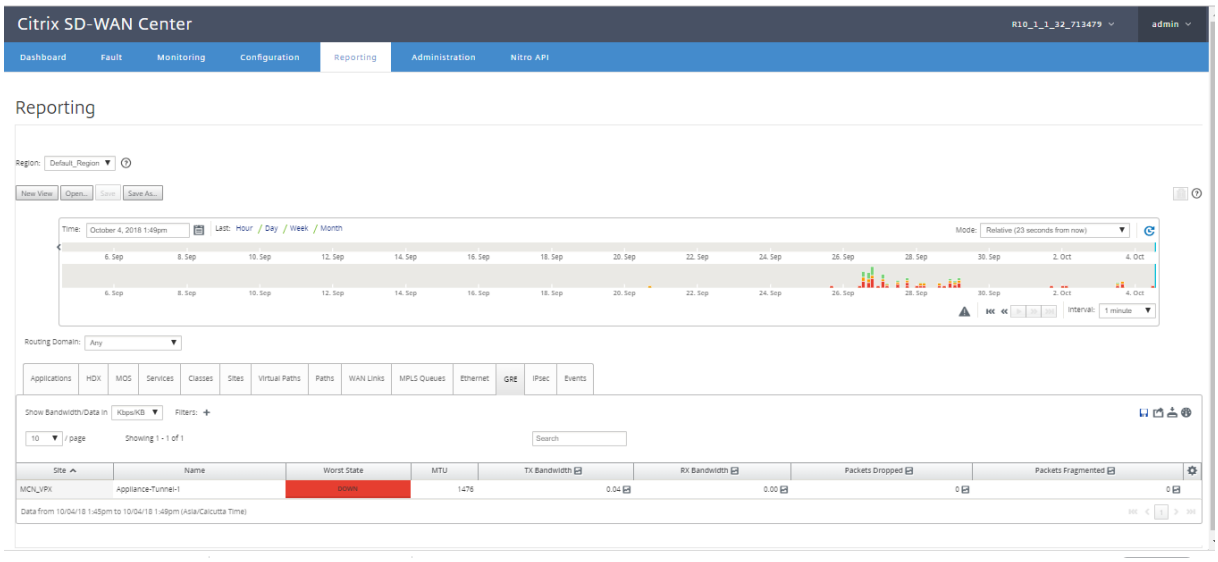
Citrix SD-WAN Center zeigt Ihnen den Status aller in Ihrem Citrix SD-WAN-Netzwerk konfigurierten GRE-Tunnel an.

So zeigen Sie GRE-Tunnelstatistikenan:

Navigieren Sie in Citrix SD-WAN Center zu **Reporting** > **GRE**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Schlimmster Zustand**: Der schlechteste Zustand, der während des ausgewählten Zeitraums beobachtet wird.
- **MTU**: Maximale Übertragungseinheit —die Größe des größten IP-Datagramms, das über eine bestimmte Verbindung übertragen werden kann.
- **TX-Bandbreite**: übertragene Bandbreite.
- **RX-Bandwidth**: empfangene Bandbreite.
- **TX-Pakete**: Anzahl der übertragenen Pakete.
- **RX-Pakete**: Anzahl der empfangenen Pakete.

- **Verworfene Pakete**: Anzahl der Pakete, die aufgrund von Netzwerküberlastung gelöscht wurden.
- **Pakete Fragmentiert**: Anzahl der fragmentierten Pakete. Pakete werden fragmentiert, um kleinere Pakete zu erstellen, die eine Verbindung mit einer MTU passieren können, die kleiner als das ursprüngliche Datagramm ist. Die Fragmente werden vom empfangenden Host wieder zusammengesetzt.
- **Datenabdeckung**: Prozentsatz des ausgewählten Zeitraums, für den Daten verfügbar sind.

> **Hinweis**
>
> Klicken Sie auf das Einstellungssymbol, um die Metriken auszuwählen, die Sie anzeigen möchten.

HDX-Bericht

April 13, 2021

Wählen Sie einen der folgenden Berichtstypen aus der Dropdownliste aus:

- HDX-Site-Statistiken
- HDX-Zusammenfassung (gilt sowohl für verfügbare HDX-Informationskanal als auch für nicht verfügbare Sitzungen)
- HDX-Benutzersitzungen (nur für HDX-Informationskanal verfügbar Sitzungen)
- HDX-Apps (nur für HDX-Informationskanal verfügbar Sitzungen)

HDX-Site-Statistiken

HDX-Bericht liefert detaillierte HDX-Daten pro Standort.Die Daten für jede Site werden in zwei Ansichten angezeigt.

Übersichtsansicht

In der Ansicht "Zusammenfassung"werden die folgenden Daten für eine Site angezeigt:

- **QoE-Index:** Quality of Experience (QoE) ist ein numerischer Wert zwischen 0 und 100. Je höher der Wert, desto besser die Benutzererfahrung.
- **Benutzer** —Die Anzahl der aktiven Benutzer auf der Site.
- **TCP-Flows:** Anzahl der aktiven HDX-Sitzungen in der Site, die das TCP-Protokoll verwenden.
- **UDP-Flows** —Die Anzahl der aktiven HDX-Sitzungen auf der Site, die das UDP-Protokoll verwenden.

- **Sitzungen:** Die Gesamtzahl aktiver HDX-Sitzungen auf der Site, die Sitzungen mit Small-Scale Integration (SSI) und Medium-Scale Integration (MSI) umfasst.

Detailansicht

Sie können auf eine einzelne Site klicken, um Details zu allen Variablen anzuzeigen, die QoE beeinflussen.Jedes Zeilenpaar zeigt die QoE-Faktoren für Daten, die auf lokalen und entfernten Seiten für einen bestimmten virtuellen Pfad berechnet werden.

Latenz-, Jitter- und Paket drop-Variablen, die sich auf den QoE auswirken, sind die effektive Zahl, die das Citrix SD-WAN Gerät gemessen. Beispielsweise könnte es einen größeren Prozentsatz des Paketabfalls im Netzwerk geben, da Citrix SD-WAN die Paketabfälle durch ein eigenes Protokoll korrigiert, wäre der effektive Paketverlust der Anwendung viel geringer, wodurch die QoE für HDX-Anwendungen verbessert wird.

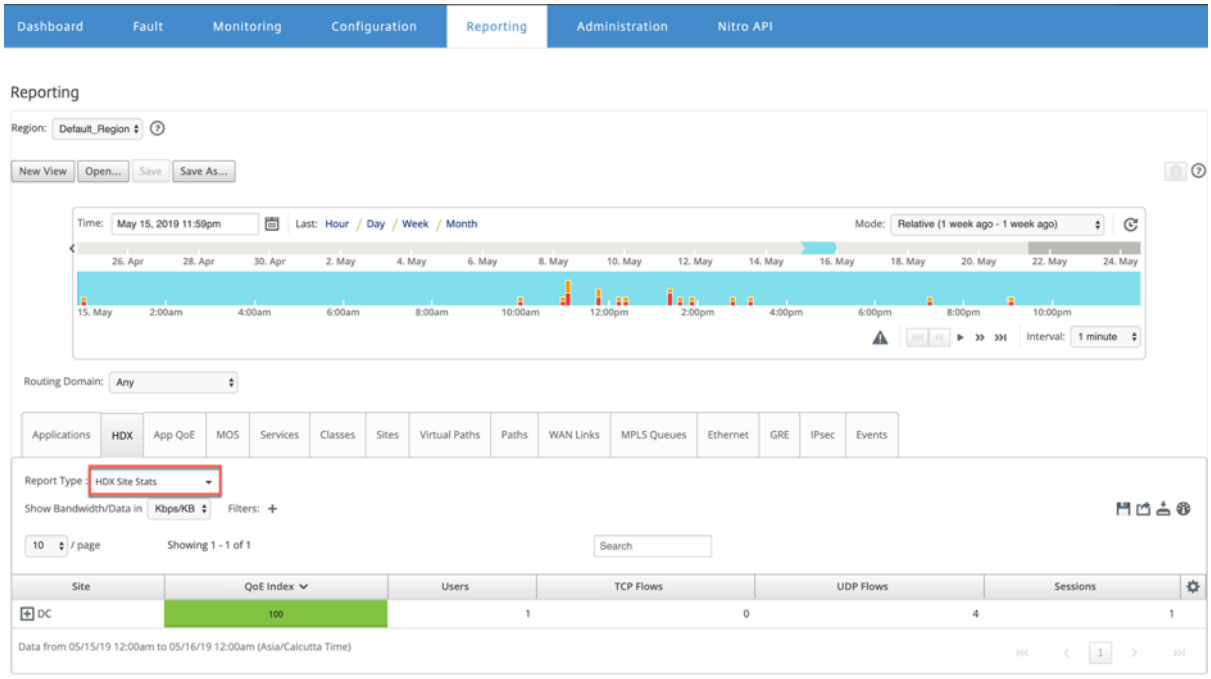
Ebenso verbessert die Latenzverbesserung durch Paketduplizierung auch die QoE für HDX-Anwendungen. Das heißt, Citrix SD-WAN verbessert die QoE für HDX-Datenverkehr, da die Faktoren verbessert werden, die sich auf den QoE auswirken. Weitere Informationen, siehe HDX QoE.

So zeigen Sie HDX-Berichtean:

Navigieren Sie im Citrix SD-WAN Center zu **Berichterstellung** > **HDX**und wählen Sie im Zeitachsensteuerungsfenster einen Zeitraum aus.

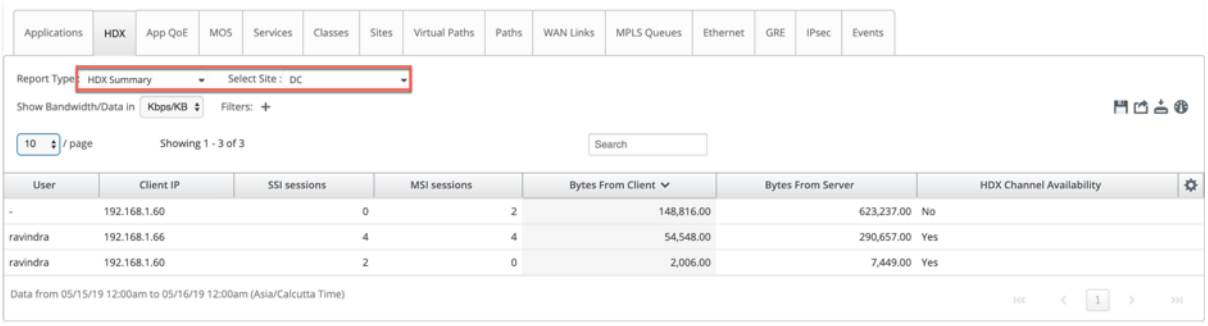
Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



HDX-Zusammenfassung

Wählen Sie den **HDX**-Übersichtsbericht und die Site aus der Dropdownliste aus. Der HDX-Zusammenfassungsbericht zeigt den Bericht jedes Benutzers an, der sich während des ausgewählten Zeitraums angemeldet hat.



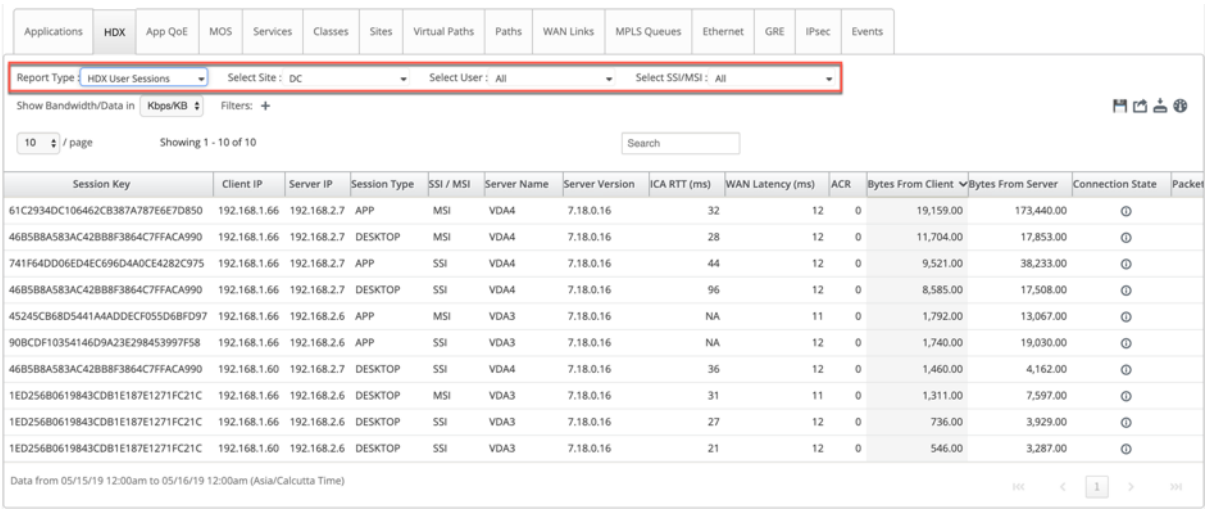
Im HDX-Zusammenfassungsbericht können Sie die folgenden Parameter anzeigen:

- **Benutzer**: Name des Benutzers.
- **Client-IP**: Client-IP-Adresse.
- **SSI-Sitzungen**: Anzahl der aktiven Single Stream ICA (SSI) -Sitzungen.
- **MSI-Sitzungen**: Anzahl der aktiven Multi Stream ICA (MSI-Sitzungen).
- **Bytes vom Client**: Größe in Bytes vom Client.
- **Bytes vom Server**: Größe in Bytes vom Server.
- **HDX-Kanalverfügbarkeit**: Gibt den Verfügbarkeitsstatus des HDX-Informationskanals **Ja/Nein**an. Wenn der Kanal nicht verfügbar ist, wird der Benutzername als Bindestrich (-)

angezeigt.

HDX-Benutzersitzungen

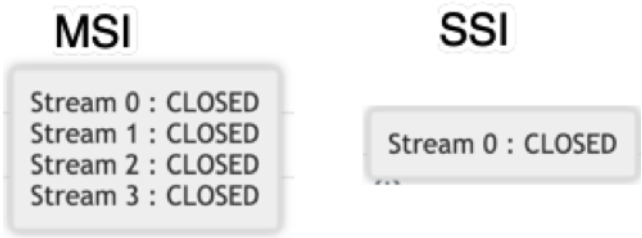
Im Bericht über HDX-Benutzersitzungen werden alle von den Benutzern verwendeten Sitzungsdetails angezeigt. Wählen Sie die Site, den Benutzer und SSI oder MSI aus der Dropdownliste aus. Standardmäßig werden in den Feldern **Benutzer auswählen**und **SSI/MSI** auswählen **ALLE** angezeigt.



Sie können über die Optionen **Suchen** oder **Filtern:+** die gewünschten Sitzungsinformationen ermitteln.

- **Sitzungsschlüssel**: Der Sitzungsschlüssel stellt die eindeutige Identität für eine ICA-Sitzung dar.
- **Client-IP**: Client-IP-Adresse für jede Sitzung.
- **Server-IP**: Server-IP-Adresse für jede Sitzung.
- **Sitzungstyp**: Typ der Sitzungen (Desktop, App).
- **SSI/MSI**: Zeigt an, ob es sich um eine SSI- oder MSI-Sitzung handelt.
- **Servername**: Zeigt den Namen des Servers an.
- **Serverversion:** Zeigt die Version des Servers an.
- **ICA RTT (ms)**: Zeigt die ICA Round Trip Time (RTT) in Millisekunden an. Dies ist eine End-to-End-Roundtripzeit zwischen Client und Server.
- **WAN-Latenz**: Latenz über das WAN, d.h. zwischen den beiden SD-WANs über den virtuellen Pfad. Diese Latenz schließt keine Client- oder serverseitige Netzwerklatenz ein.
- **ACR**: Zeigt die Anzahl der automatischen Clientwiederverbindung an.
- **Bytes vom Client**: Größe in Bytes vom Client.
- **Bytes vom Server**: Größe in Bytes vom Server.
- **Verbindungsstatus**: Bewegen Sie die Maus, um den Verbindungsstatus zu sehen.

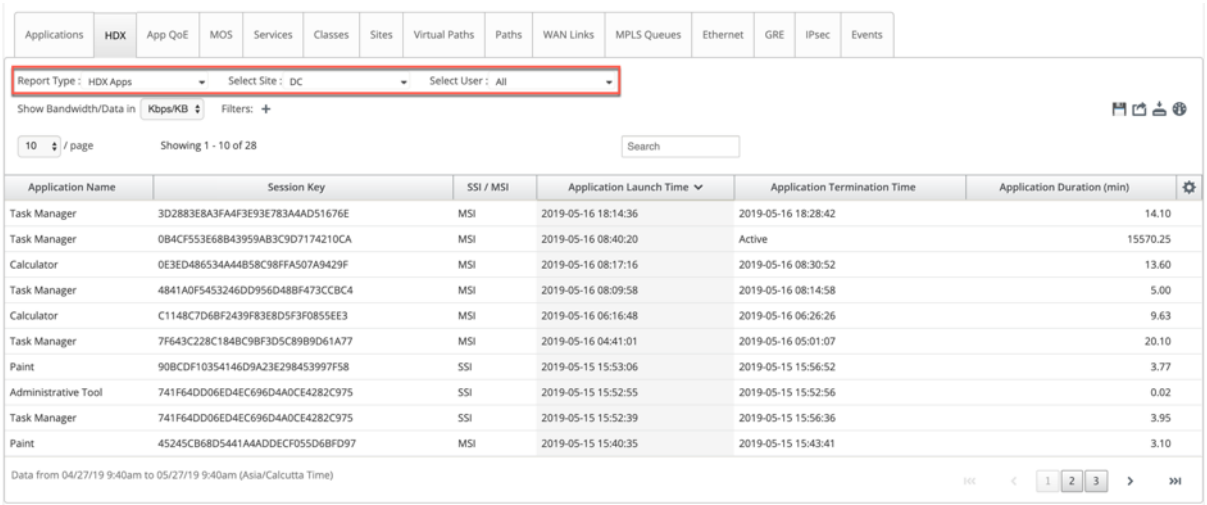
- Für MSI gibt es vier Verbindungen. Diese Verbindungen sind auf L4-Ebene (TCP/UDP-Zustand).
- Für SSI gibt es nur eine Verbindung.



- **Paket vom Client**: Anzahl der Pakete vom Client.
- **Paket vom Server**: Anzahl der Pakete vom Server.

HDX-Apps

Sie können alle Anwendungen sehen, die von einem bestimmten Benutzer oder von allen Benutzern verwendet werden. Wählen Sie die **Site** und den **Benutzer** aus, um die Anwendungsdetails anzuzeigen.



- **Anwendungsname**: Gibt den Namen der HDX-Anwendung an.
- **Sitzungsschlüssel**: Stellt den eindeutigen Sitzungsschlüssel bereit, der für diese bestimmte Anwendung verwendet wird.
- **SSI/MSI**: Zeigt an, ob es sich um eine SSI- oder MSI-Sitzung handelt.
- **Anwendungsstartzeit**: Gibt die Startzeit der Anwendung mit Datum an.
- **Anwendungsbeendigungszeit**: Gibt die Beendigungszeit der Anwendung mit Datum an. Wenn eine Anwendung aktiv ist, zeigt sie statt der Beendigungszeit aktiv an.
- **Anwendungsdauer (min)**: Gibt die Anwendungsdauer in Minuten an.

Hinweis

- Im Fall eines unbeabsichtigten Fehlers, z. B. wenn die HDX-Sitzungsinformationen auf dem Gerät nicht verfügbar sind, werden die benutzerbasierten HDX-Berichte nicht angezeigt, selbst wenn die **HDX-Benutzerberichterstellung** aktiviert ist. Einige Felder wie Benutzername, Servername, Serverversion, ICA RTT in den Berichten werden möglicherweise als **NA**angezeigt.
- Die Anwendungsbeendungszeit im **HDX-Apps-Bericht** wird nur angezeigt, wenn SD-WAN die **Anwendungsbeendungszeit** von Xen Application/Xen Desktop Server erhält. Ansonsten werden einige Anwendungen als aktiv gemeldet, selbst wenn sie geschlossen sind.
- Aufgrund der Beschränkung von Citrix Virtual Apps and Desktops (früher XenApp und XenDesktop) ist der **Anwendungsname**, der im Bericht HDX Apps angezeigt wird, auf nur 19 Zeichen beschränkt.

IPSec-Tunnelbericht

April 13, 2021

IP-Sicherheitsprotokolle (IPSec) bieten Sicherheitsdienste wie Verschlüsselung sensibler Daten, Authentifizierung, Schutz vor Wiederholung und Datenvertraulichkeit für IP-Pakete.Encapsulating Security Payload (ESP) und Authentication Header (AH) sind die beiden IPSec-Sicherheitsprotokolle, die zur Bereitstellung dieser Sicherheitsdienste verwendet werden.

Im IPSec-Tunnelmodus ist das gesamte ursprüngliche IP-Paket durch IPSec geschützt. Das ursprüngliche IP-Paket wird umhüllt und verschlüsselt, und ein neuer IP-Header wird hinzugefügt, bevor das Paket über den VPN-Tunnel übertragen wird.

Weitere Informationen zum Konfigurieren von IPsec-Tunneln auf Citrix SD-WAN-Geräten finden Sie unter IPSec-Tunnelterminierung .

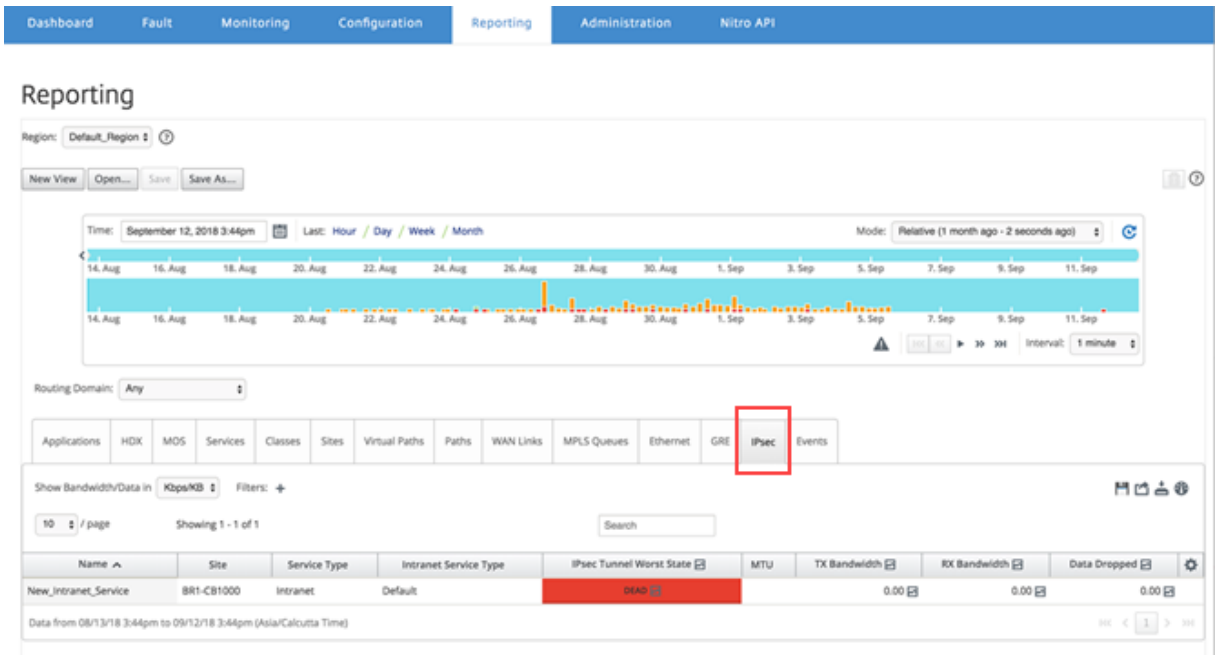
Citrix SD-WAN Center kann Ihnen den Status aller IPSec-Tunnel anzeigen, die in Ihrem Citrix SD-WAN-Netzwerk konfiguriert sind.

So zeigen Sie IPSec-Tunnelstatistikenan:

Navigieren Sie in Citrix SD-WAN Center zu **Reporting** > **IPSec-Tunnels**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Name**: Anwendungsname.
- **Site**: Name der Site.
- **Servicetyp**: Typ des Dienstes.
- **Intranetdiensttyp: Typ**des Intranetdiensts, der dem IPSec-Tunnel zugeordnet ist. Im Folgenden werden die Intranetdienste aufgeführt:
  - Standard
  - Microsoft Azure Virtual WAN
  - Zscaler
  - Citrix SaaS-Gateway
- **IPSec Worst State**: Der schlechteste Zustand, der während des ausgewählten Zeitraums beobachtet wurde.
- **MTU**: Maximale Übertragungseinheit —Größe des größten IP-Datagramms, das über eine bestimmte Verbindung übertragen werden kann.
- **TX-Bandbreite**: übertragene Bandbreite.
- **RX-Bandwidth**: empfangene Bandbreite.
- **TX-Pakete**: Anzahl der übertragenen Pakete.
- **RX-Pakete**: Anzahl der empfangenen Pakete.
- **Daten gelöscht**: Daten wurden gelöscht, in Kbps.
- **Verworfene Pakete**: Anzahl der verworfenen Pakete.

> **Hinweis**
>
> Klicken Sie auf das Einstellungssymbol, um die Metriken auszuwählen, die Sie anzeigen möchten.

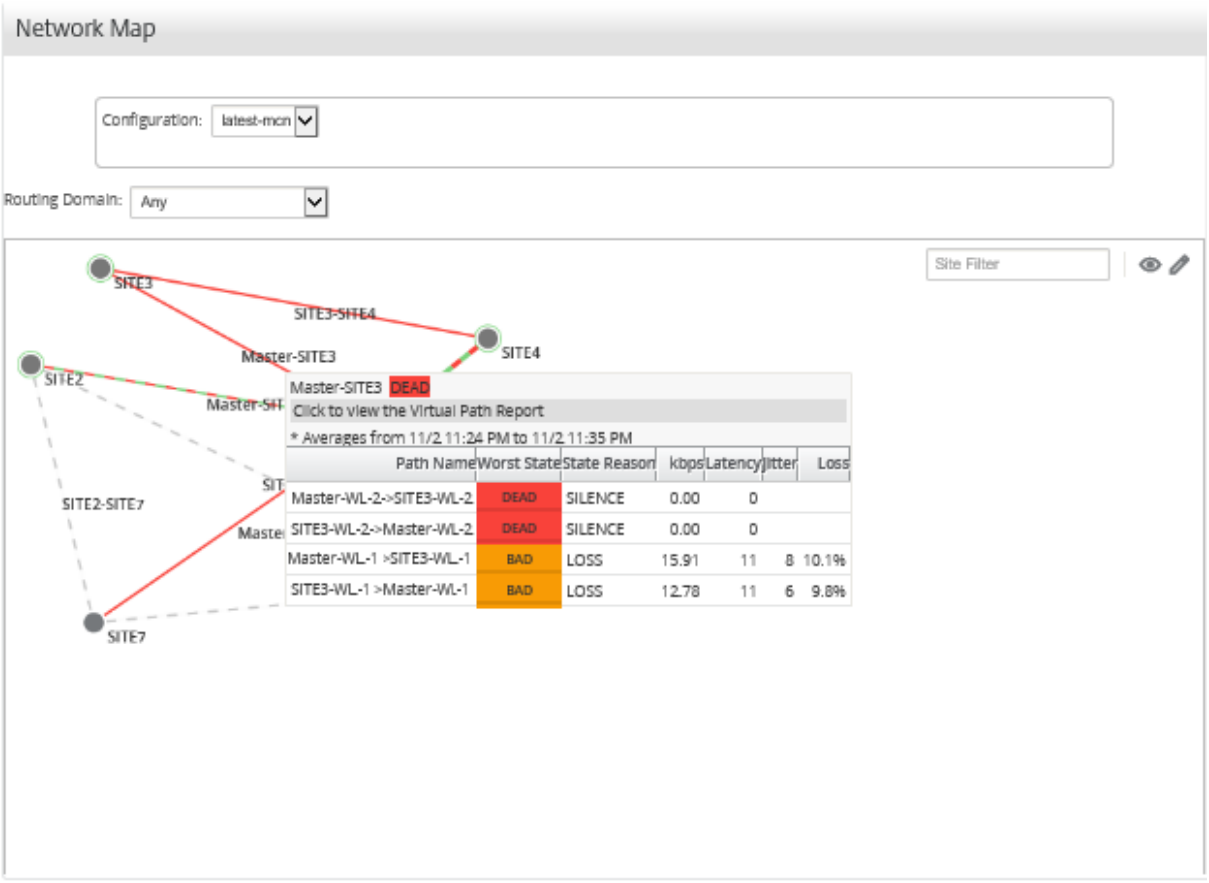
Verknüpfungsleistungsbericht

April 13, 2021

Citrix SD-WAN Center kann Leistungsstatistiken auf Standort-, Dienst-, virtuellen Pfad- oder WAN-Link-Ebene anzeigen.

Betrachten Sie ein Netzwerk, in dem Organisation ABC vier Niederlassungen hat. Bei SITE3 wurden Brownouts gemeldet. Das heißt, die Mitarbeiter sind manchmal nicht in der Lage, die Intranetseiten anzuzeigen. Sie vermuten, dass dies auf die Leistung der zugrunde liegenden Links zurückzuführen ist.

Sie können eine allgemeine Ansicht der Verknüpfungsstatistiken erhalten, indem Sie den Mauszeiger auf der Netzwerkkarte im Dashboard über den Pfad zwischen einer Site und dem Rechenzentrum bewegen.



Der obige Screenshot zeigt, dass es zwei WAN-Links (WL-1 und WL-2) zwischen SITE 3 und dem Master Controller Node (MCN) gibt, und zeigt Statistiken für die letzten 10 Minuten.

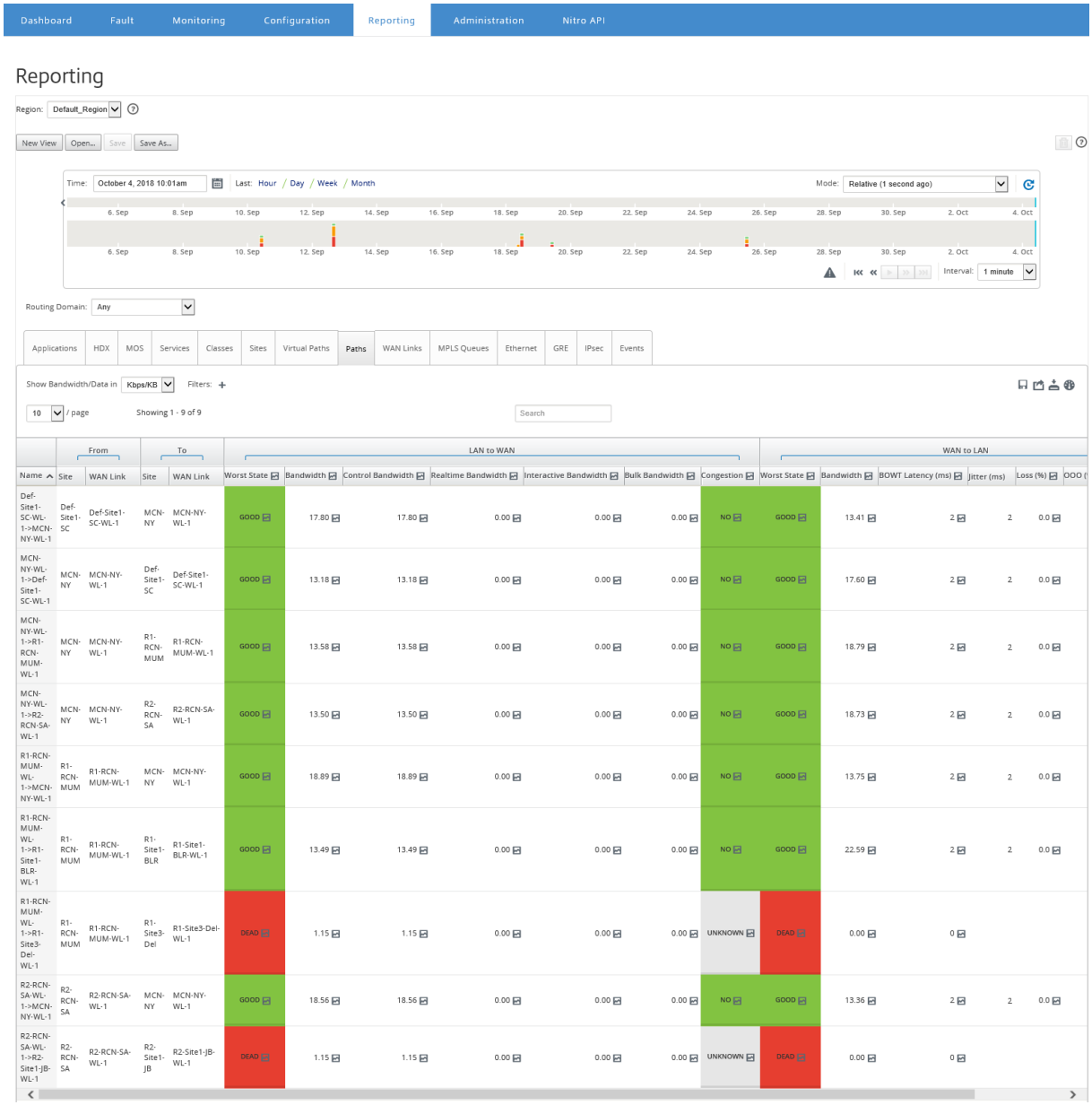
Die virtuellen Pfade Master-WL2- > SITE3-WL2 und SITE3-WL2 - > Master-WL2 funktionieren nicht, und alternative Pfade Master-WL1- > SITE3-WL1 und SITE3-WL1 - > Master-WL1 sind in einem schlechten Zustand und verlieren einen signifikanten Prozentsatz der übertragenen Daten. Dies ist die wahrscheinliche Ursache für die Brownout-Frage bei SITE3.

Alternativ können Sie die Verknüpfungsstatistiken anzeigen, indem Sie zu **Reporting** >**Pfade** navigieren.

Wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Name**: Der Pfadname.
- **Von (Site und WAN Link)**: Die Quell-Site und WAN-Link.
- **Nach (Standort- und WAN-Link)**: Der Zielstandort und WAN-Link.
- **LAN zu WAN**
  - **Arbeitsstatus**:
  - **Bandbreite**: Gesamtbandbreite, die von allen Pakettypen verbraucht wird. Bandbreite = Kontrolle der Bandbreite + Echtzeit-Bandbreite + Interaktive Bandbreite + Massenbandbreite.
  - **Kontrollbandbreite**: Bandbreite, die zum Übertragen von Steuerungspaketen verwendet

wird, die Routing-, Planungs- und Verknüpfungsstatistikinformationen enthalten.
  - **Echtzeitbandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die in der SD-WAN-Konfiguration zum Echtzeitklassentyp gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
  - **Interaktive Bandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
  - **Massenbandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die zum Massenklassentyp der SD-WAN-Konfiguration gehören. Diese Anwendungen erfordern sehr wenig menschliches Eingreifen und werden meist von den Systemen selbst gehandhabt (z. B. FTP, Backup-Operationen).
  - **Überlastung**: Überlastung durch erhöhten Datenverkehr oder unerwartete Verzögerung des Paketflusses im WAN.

- **WAN zu LAN**:
  - **Worst State**: Der schlechteste WAN-zu-LAN-Status, der während des Zeitraums beobachtet wurde.
  - **Bandbreite**:
  - **BOWT Latenz (ms)**: Die beste One-Way-Zeit (BOWT), die für ein Paket in Millisekunden von einem Punkt zum anderen verwendet wird.
  - **Jitter (ms)**: Variation der Verzögerung empfangener Pakete in Millisekunden.
  - **Verlust (%)**: Prozentsatz der verlorenen Pakete.
  - **OOO (%)**: Prozentsatz der Pakete, die nicht in der richtigen Reihenfolge oder außerhalb der Reihenfolge sind (OOO).
  - **Überlastung**: Überlastung durch erhöhten Datenverkehr oder unerwartete Verzögerung des Paketflusses im WAN.

Klicken Sie auf das Symbol **Einstellungen** und wählen Sie die Parameter aus, die Sie in Berichten anzeigen möchten.

MOS für Anwendungen

April 13, 2021

Der Mean Opinion Score (MOS) liefert ein numerisches Maß für die Qualität der Erfahrung, die eine Anwendung den Endbenutzern liefert. Es wird hauptsächlich für VoIP-Anwendungen verwendet. In

Citrix SD-WAN wird MOS auch verwendet, um die Qualität von Nicht-VoIP-Anwendungen zu bewerten, indem der Datenverkehr so beurteilt wird, als ob es sich um einen VoIP-Anruf handelte.

Citrix SD-WAN Center berechnet und zeigt MOS für den Datenverkehr an, der durch den virtuellen Pfad fließt. Aktivieren Sie die Option **MOS schätzen** für jede Anwendung auf jeder Citrix SD-WAN-Appliance, um die MOS-Werte dieser Anwendungen in Citrix SD-WAN Center anzuzeigen.

Weitere Informationen zum Aktivieren von MOS für Anwendungen in Citrix SD-WAN finden Sie unterRegelgruppen hinzufügen und MOS aktivieren.

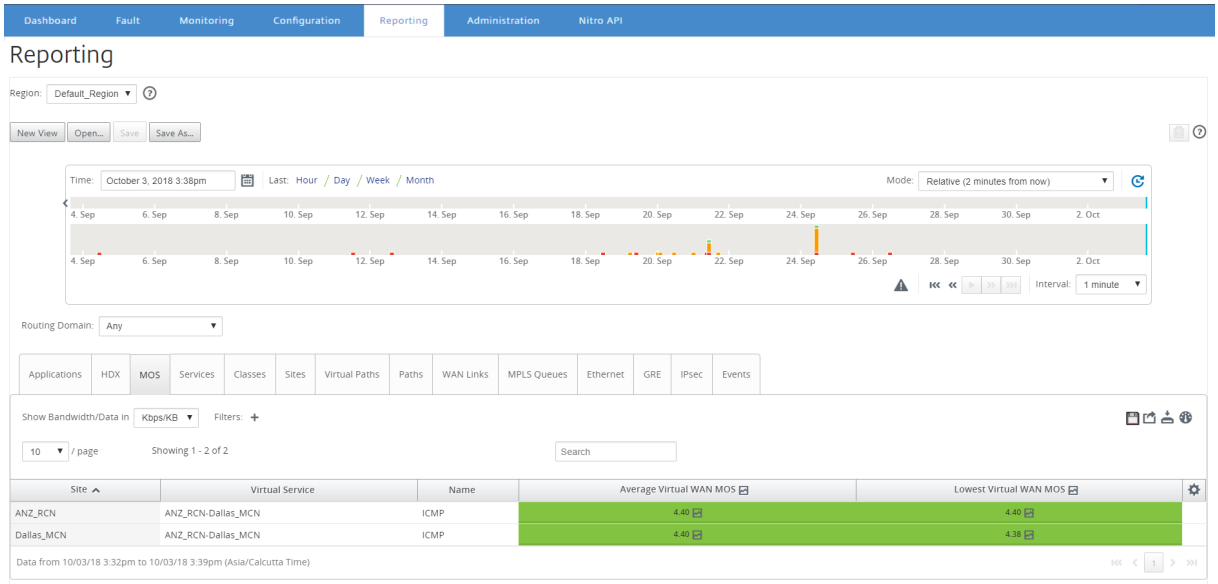
> **Hinweis**
>
> Aktivieren Sie unter Regeln die Option Performance verfolgen, um MOS für Anwendungen zu schätzen und in Citrix SD-WAN Center anzuzeigen. Weitere Informationen zu Regeln finden Sie unterRegeln nach IP-Adresse und Portnummer.

So zeigen Sie MOS für Anwendungenan:

Navigieren Sie in Citrix SD-WAN Center zu **Reporting** > **Anwendungen**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **Name**: Name der Anwendung.

- **Durchschnittlicher Virtual WAN MOS**: Durchschnittlicher Qualitätsfaktor, der über den ausgewählten Zeitraum berechnet wird.
- **Niedrigster Virtual WAN MOS**: Niedrigster Qualitätsfaktor, der innerhalb des ausgewählten Zeitraums berechnet wird.

Die Punktzahlen werden wie folgt bewertet:

- 5 —Benutzer sind sehr zufrieden.
- 4 —Benutzer sind zufrieden.
- 3 —Benutzer sind unzufrieden.
- 2 —Benutzer sind sehr unzufrieden.
- 1 —Nicht empfohlen.

MPLS-Warteschlangenbericht

April 13, 2021

MPLS-Warteschlangen stellen Dienstwarteschlangen bereit, die durch standardmäßige DSCP-Tags (Differentiated Services Code Point) gesteuert werden. Die Tags steuern die Servicequalität zwischen zwei Sites im virtuellen WAN.

MPLS-Warteschlangen ermöglichen MPLS-Anbietern, Datenverkehr anhand von DSCP-Markierungen zu identifizieren, sodass Dienstklasse vom Anbieter angewendet werden kann.

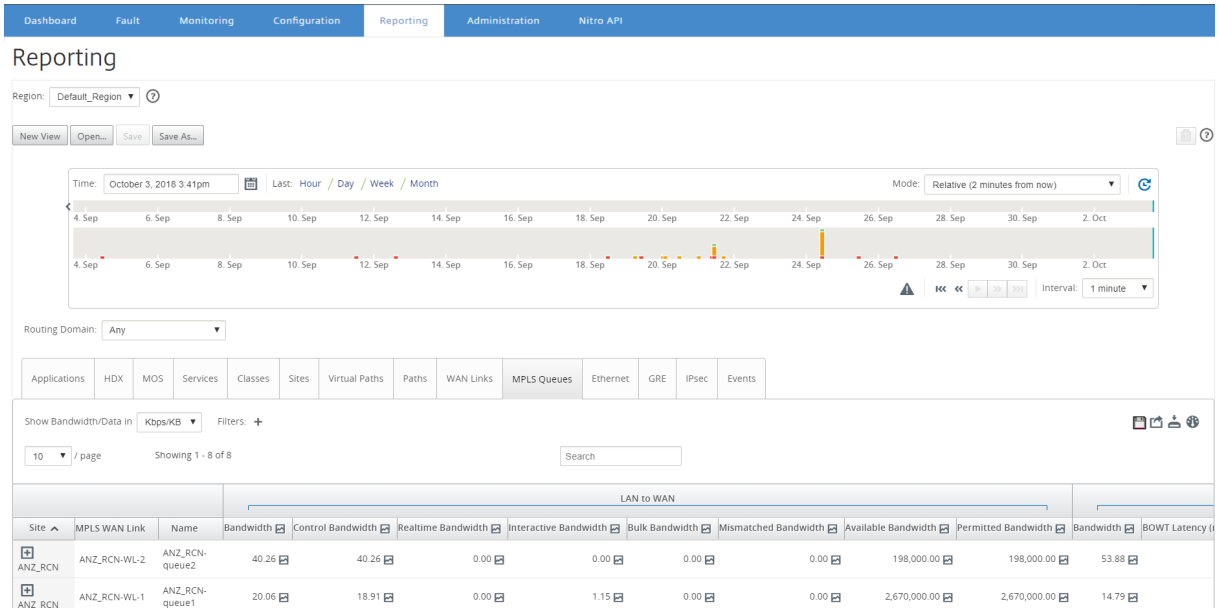
Weitere Informationen zum Konfigurieren privater MPLS-WAN-Links auf Citrix SD-WAN-Appliances finden Sie unterMPLS-Warteschlangen.

So zeigen Sie MPLS-Warteschlangenstatistiken an:

Navigieren Sie in Citrix SD-WAN Center zu **Berichte** > **MPLS-Warteschlangen**, und wählen Sie im Timeline-Control einen Zeitraum aus.

Sie können Berichte eines bestimmten Zeitrahmens auswählen und anzeigen, indem Sie die Zeitleistensteuerelemente verwenden. Weitere Informationen finden Sie unter Zeitleisten-Steuerelemente.

Sie können Berichtsansichten auch erstellen, speichern und öffnen. Weitere Informationen finden Sie unter Ansichten verwalten.



Sie können die folgenden Metriken anzeigen:

- **MPLS-WAN-Link**: Name der MPLS-WAN-Verknüpfung, der die MPLS-Warteschlange angehört.
- **Name**: Der DSCP-Tag-Name.
- **Bandbreite**: Gesamtbandbreite, die von allen Pakettypen verbraucht wird. Bandbreite = Kontrolle der Bandbreite + Echtzeit-Bandbreite + Interaktive Bandbreite + Massenbandbreite.
- **Kontrollbandbreite**: Bandbreite, die zum Übertragen von Steuerungspaketen verwendet wird, die Routing-, Planungs- und Verknüpfungsstatistikinformationen enthalten.
- **Realtime Bandwidth:** Bandbreite, die von Anwendungen verbraucht wird, die zum Typ der Echtzeitklasse in der Citrix SD-WAN-Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz ab. Ein verzögertes Paket ist schlechter als ein verlorenes Paket (z. B. VoIP, Skype for Business).
- **Interaktive Bandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die zum interaktiven Klassentyp in der Citrix SD-WAN Konfiguration gehören. Die Leistung solcher Anwendungen hängt weitgehend von der Netzwerklatenz und dem Paketverlust ab (z. B. XenDesktop, XenApp).
- **Massenbandbreite:** Bandbreite, die von Anwendungen verbraucht wird, die zum Massenklassentyp der Citrix SD-WAN-Konfiguration gehören. Diese Anwendungen erfordern sehr wenig menschliches Eingreifen und werden meist von den Systemen selbst gehandhabt (z. B. FTP, Backup-Operationen).
- Nicht**übereinstimmende Bandbreite**: Frames, die nicht mit den definierten DSCP-Tags übereinstimmen, werden einer Standardwarteschlange zugeordnet, die für nicht übereinstimmende Bandbreite bestimmt ist.
- **Verfügbare Bandbreite**: Die Summe der Bandbreite, die allen WAN-Links einer Site zugewiesen ist.

- **Zulässige Bandbreite**: Bandbreite zur Übertragung von Informationen.
- **BOWT-Latenz**: Die beste einmalige Zeit, die ein Paket in Millisekunden von einem Punkt zum anderen bewegt.
- **Jitter**: Variation der Verzögerung empfangener Pakete in Millisekunden.
- **Verlorene Pakete**: Anzahl der verlorenen Pakete.
- **Verlust**: Prozentsatz der verlorenen Pakete.
- **OOO**: Prozentsatz der Pakete, die nicht in der richtigen Reihenfolge sind.
- **Überlastung**: Überlastung durch erhöhten Datenverkehr oder unerwartete Verzögerung des Paketflusses im WAN.

> **Hinweis**
>
> Klicken Sie auf das Einstellungssymbol, um die Metriken auszuwählen, die Sie anzeigen möchten.

Verwaltung

April 13, 2021

Sie können Ihr Citrix SD-WAN Center VPX mit den folgenden Verwaltungsoptionen verwalten und verwalten.

Datum und Uhrzeit konfigurieren

HTTPS-Zertifikate

MCN-Konfiguration importieren

Datenbank verwalten

Ansichten verwalten

Software-Upgrade

Zeitleisten-Steuerelemente

Benutzerkonten

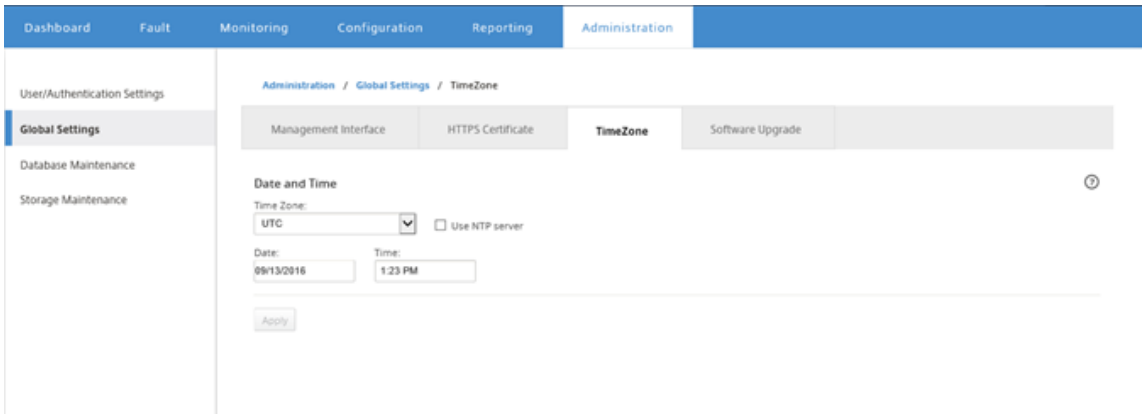
Datum und Uhrzeit konfigurieren

April 13, 2021

Sie können Datum und Uhrzeit des Citrix SD-WAN Center-Verwaltungssystems entweder manuell oder mithilfe eines NTP-Servers ändern.Wenn Sie die Option **NTP-Server verwenden** auswählen, können Sie kein aktuelles Datum und eine aktuelle Uhrzeit manuell eingeben.

So stellen Sie Datum und Uhrzeit manuell ein:

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.
2. Klicken Sie auf **Globale Einstellungen**, und klicken Sie dann auf **Zeitzone**.



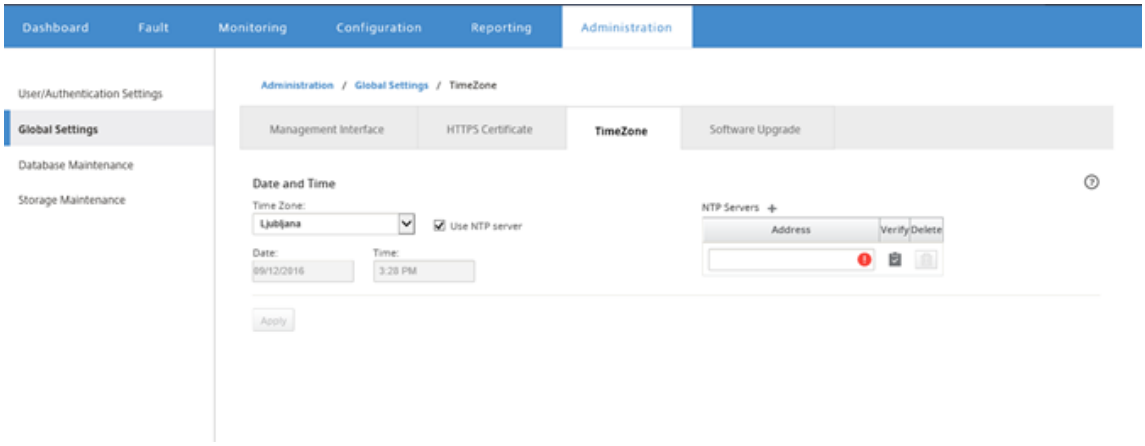
3. Wählen Sie im Feld **Zeitzone** eine **Stadt** in der aktuellen Zeitzone aus. Alternativ können Sie das aktuelle Datum und die aktuelle Uhrzeit für Ihre Zeitzone eingeben.
4. Klicken Sie auf **Apply**.

Sie können die Citrix SD-WAN Center-Uhr mit einem externen NTP-Server synchronisieren.

So legen Sie Datum und Uhrzeit mithilfe eines NTP-Servers fest:

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.
2. Klicken Sie auf **Globale Einstellungen** und dann auf **Zeitzone**.
3. Wählen Sie **NTP-Server verwenden**aus.

   Dadurch werden die Felder Datum und Uhrzeit deaktiviert und die Tabelle NTP-Server angezeigt.



4. Um einen neuen NTP-Server hinzuzufügen, klicken Sie auf das Symbol **+** neben NTP Server.
5. Geben Sie im Feld **Adresse** die **IP-Adresse** für den NTP -Server ein.

   Sie können bis zu drei NTP-Server angeben, aber Sie müssen mindestens einen angeben. Diese dienen als NTP-Sicherungsserver, wenn ein Server ausgeschaltet ist, synchronisiert das Citrix SD-WAN Center automatisch mit dem anderen NTP-Server.

   Wenn Sie einen Domänennamen für einen NTP-Server angeben, müssen Sie auch einen DNS-Server konfigurieren, sofern Sie dies nicht bereits getan haben.Um einen Servereintrag aus der Tabelle zu entfernen, klicken Sie in der Spalte **Löschen** des Eintrags auf das Symbol Löschen.
6. Klicken Sie auf **Überprüfen**, um zu überprüfen, ob der Server erreichbar ist, bevor Sie Ihre Einstellungen anwenden.
7. Klicken Sie auf **Apply**.

HTTPS-Zertifikate

April 13, 2021

HTTPS-Zertifikat ist für den Aufbau der HTTPS-Verbindung mit Citrix SD-WAN Center erforderlich.

Details zum installierten HTTPS-Zertifikat anzeigen

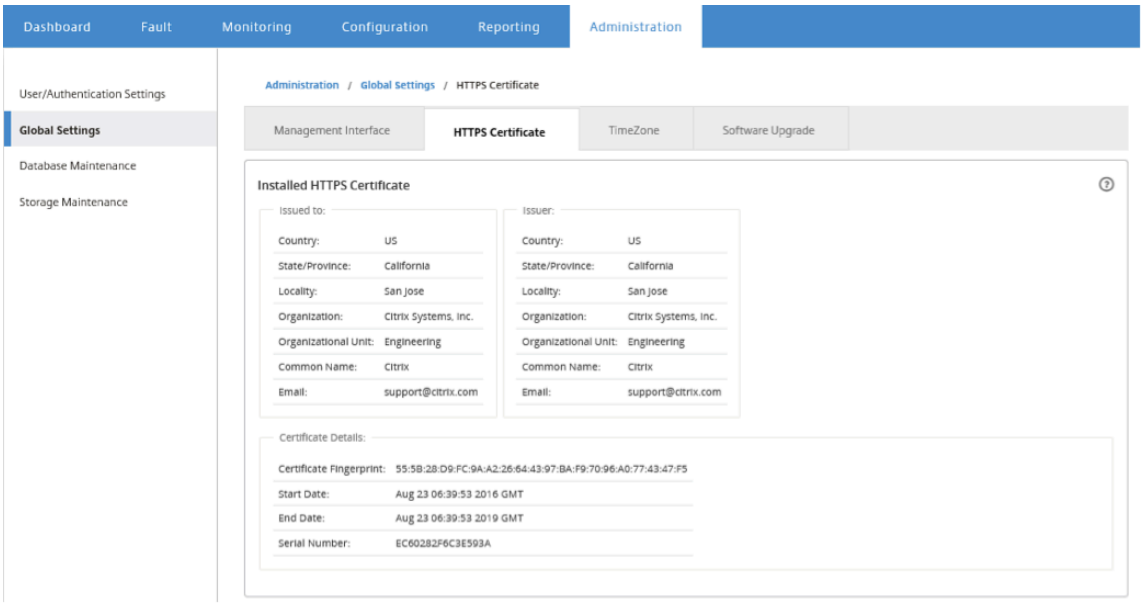
Citrix. Um das aktuelle Zertifikat auszuwerten, können Sie die Zertifikatdetails anzeigen.

So zeigen Sie die Details des bereits auf Citrix SD-WAN Center installierten HTTPS-Zertifikats an:

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.

2. Klicken Sie auf **Globale Einstellungen** und dann auf **HTTPS-Zertifikat**.

   Die HTTPS-Zertifikatdetails werden im Abschnitt **Installiertes HTTPS-Zertifikat** angezeigt.

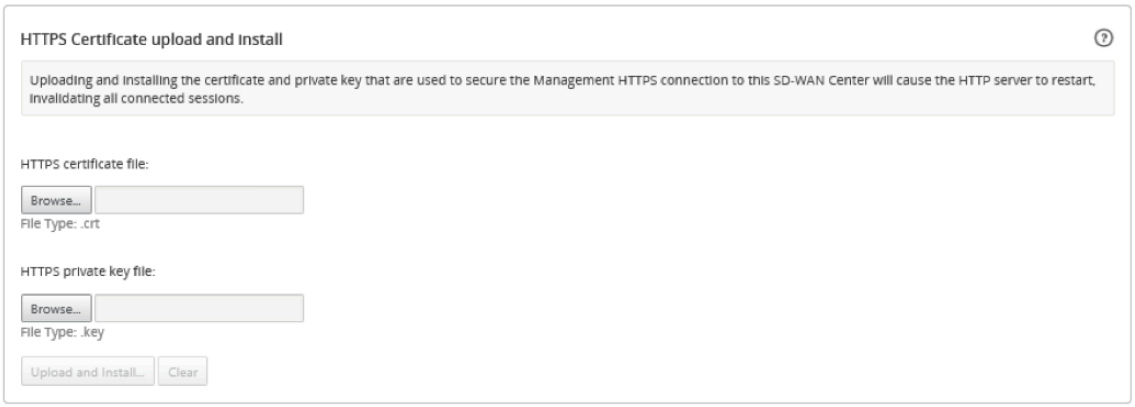


Hochladen und Installieren eines HTTPS-Zertifikats

Durch die Installation eines HTTPS-Zertifikats wird Citrix SD-WAN Center in den Wartungsmodus versetzt, bis der Vorgang abgeschlossen ist. Wenn der Vorgang abgeschlossen ist, wird der Webserver neu gestartet, wobei alle verbundenen Sitzungen ungültigen. Wenn die Verbindung zum Server beim Neustart des Webservers unterbrochen wird, lädt der Wartungsmodus automatisch die vorherige Seite neu und zeigt einen Sicherheitshinweis vom Browser an. Wenn der Bildschirm nicht neu geladen wird, klicken Sie auf **Weiter**, um die vorherige Seite neu zu laden.

So laden Sie das HTTPS-Zertifikat hoch und installieren Sie es:

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.
2. Klicken Sie auf **Globale Einstellungen** und dann auf **HTTPS-Zertifikate**.
3. Klicken Sie im Abschnitt **Hochladen und Installieren des HTTPS-Zertifikats** im Feld **HTTPS-Zertifikatdatei** auf **Durchsuchen**, und wählen Sie ein HTTPS-Zertifikat aus.
4. Klicken Sie für das Feld **HTTPS private Schlüsseldatei**auf **Durchsuchen**, und wählen Sie eine private HTTPS-Schlüsseldatei aus.
5. Klicken Sie auf **Hochladen und Installieren**.



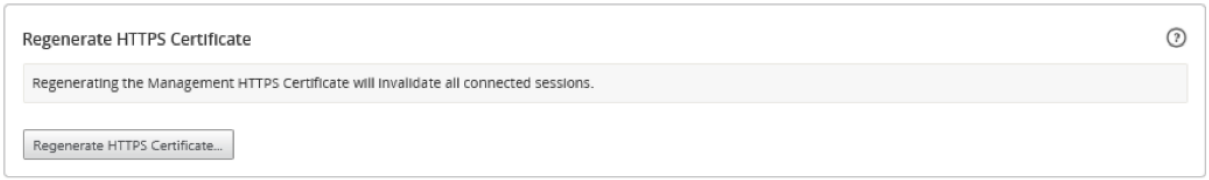
Wiederherstellen des HTTPS-Zertifikats

Sie können ein selbstsigniertes Zertifikat regenerieren, mit dem die Management-HTTPS-Verbindung mit Citrix SD-WAN Center gesichert wird. Durch die erneute Generierung des HTTPS-Zertifikats wird Citrix SD-WAN Center in den Wartungsmodus versetzt, bis der Vorgang abgeschlossen ist. Wenn der Vorgang abgeschlossen ist, wird der Webserver neu gestartet, wobei alle verbundenen Sitzungen ungültigen.

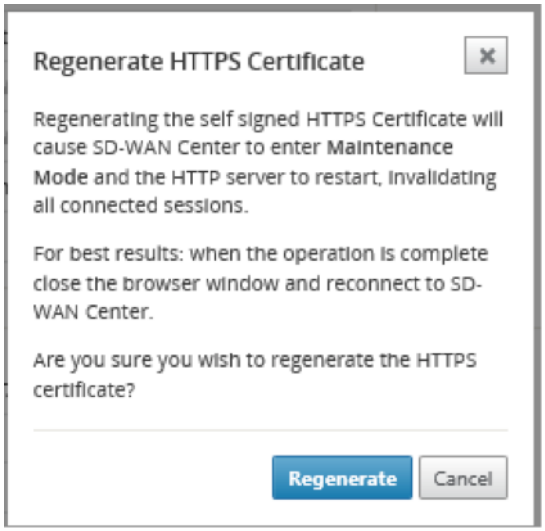
Wenn die Verbindung zum Server beim Neustart des Webservers unterbrochen wird, lädt der Wartungsmodus automatisch die vorherige Seite neu und zeigt einen Sicherheitshinweis vom Browser an. Wenn der Bildschirm nicht angezeigt wird, klicken Sie auf **Weiter**, um die vorherige Seite neu zu laden.

So generieren Sie das HTTPS-Zertifikat erneut:

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.
2. Klicken Sie auf **Globale Einstellungen** und dann auf **HTTPS-Zertifikate**.
3. Klicken **Sie im Abschnitt HTTPS-Zertifikatneu generieren auf HTTPS-Zertifikat** neu generieren.



Die Meldung “HTTPS-Zertifikat neu generieren”wird angezeigt. Klicken Sie auf **Regenerieren**.



MCN-Konfiguration importieren

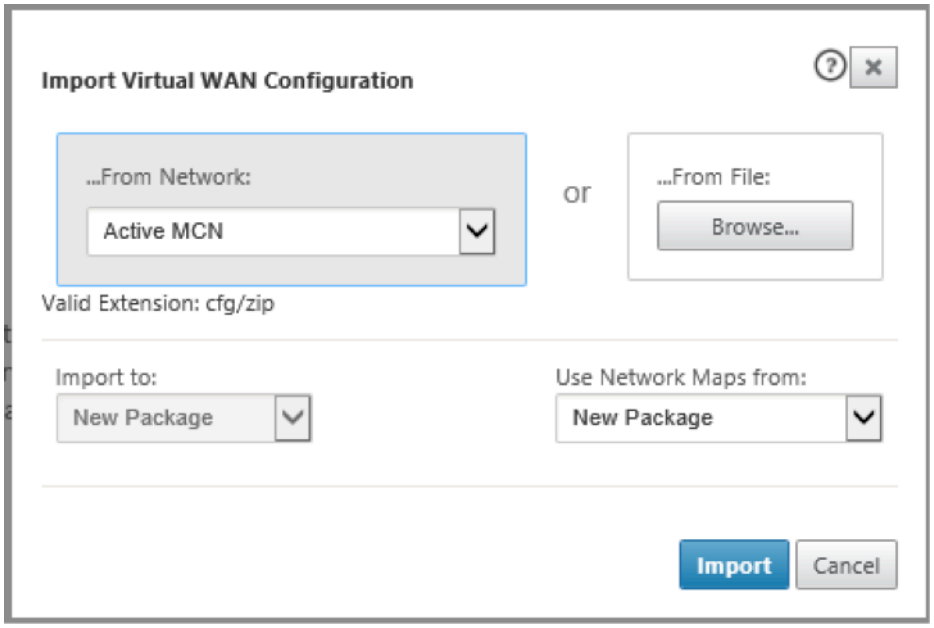
April 13, 2021

Wenn Citrix SD-WAN Center eingerichtet ist und eine Verbindung zwischen dem Master Control Node (MCN) und dem Citrix SD-WAN Center hergestellt wird, können Sie die MCN-Konfiguration in Citrix SD-WAN Center importieren und die Netzwerkzuordnungen anzeigen.

Die Funktion Importieren importiert eine Konfiguration in eine offene oder neue Citrix SD-WAN-Masterkonfiguration. Wenn eine Citrix SD-WAN-Masterkonfiguration geöffnet ist, wenn Sie die Importfunktion verwenden, werden sie und ihre Zuordnungen von der neuen Citrix SD-WAN-Masterkonfiguration überschrieben. Wenn keine Citrix SD-WAN-Masterkonfiguration geöffnet ist, wird ein Paket ohne Titel erstellt.

So importieren Sie die MCN-Konfiguration in Citrix SD-WAN Center:

1. Klicken Sie in der Citrix SD-WAN Center-Webschnittstelle auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf **Netzwerkkonfiguration** und dann auf **Importieren**.



3. Wählen Sie im Feld **Von Netzwerk** eine der folgenden Optionen aus:

   - **Aktive MCN**: Stellen Sie eine Verbindung zum aktiven MCN her und laden Sie die aktuelle Konfiguration herunter.
   - **Andere:**Stellen Sie eine Verbindung mit einer IP-Adresse eines anderen MCN her und laden Sie die aktuelle Konfiguration herunter. Möglicherweise müssen Sie das Sicherheitszertifikat von diesem Citrix SD-WAN Center im MCN installieren, bevor Sie die Konfiguration importieren können.

   Weitere Informationen finden Sie unter Installieren des Citrix SD-WAN Center-Zertifikats.

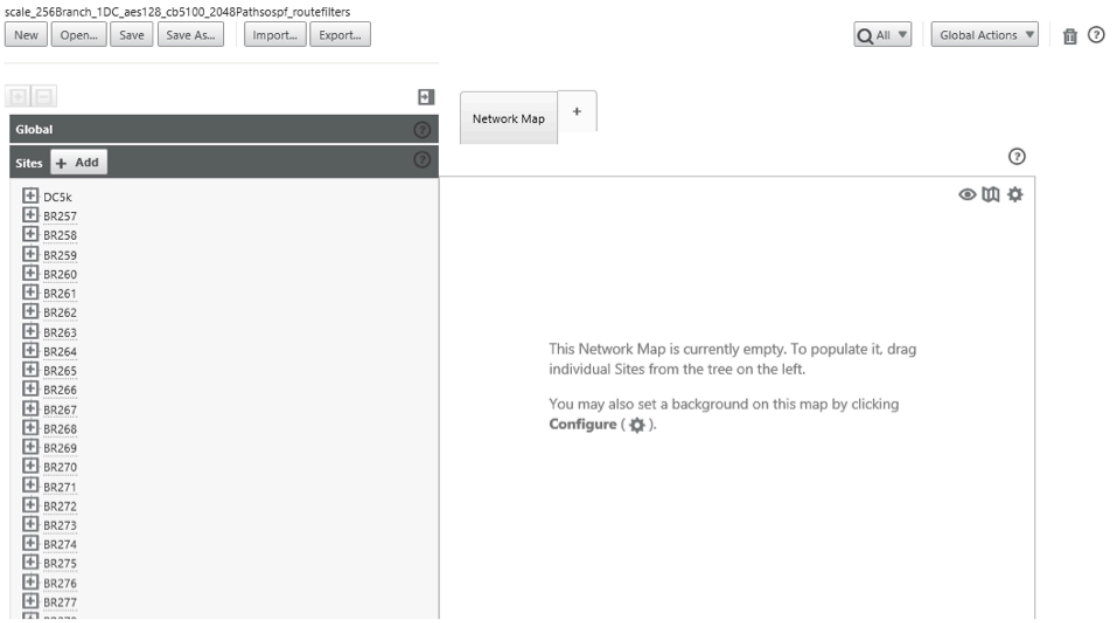
4. Alternativ können Sie im Abschnitt **Aus Datei** auf **Durchsuchen** klicken, und wählen Sie eine Konfiguration aus, die von Ihrem Computer hochgeladen werden soll.

5. Wählen Sie im Feld **Importieren** nach die Option **Aktuelles Paket** aus, um den Inhalt der ausgewählten Datei in das aktuelle geöffnete Paket zu importieren.

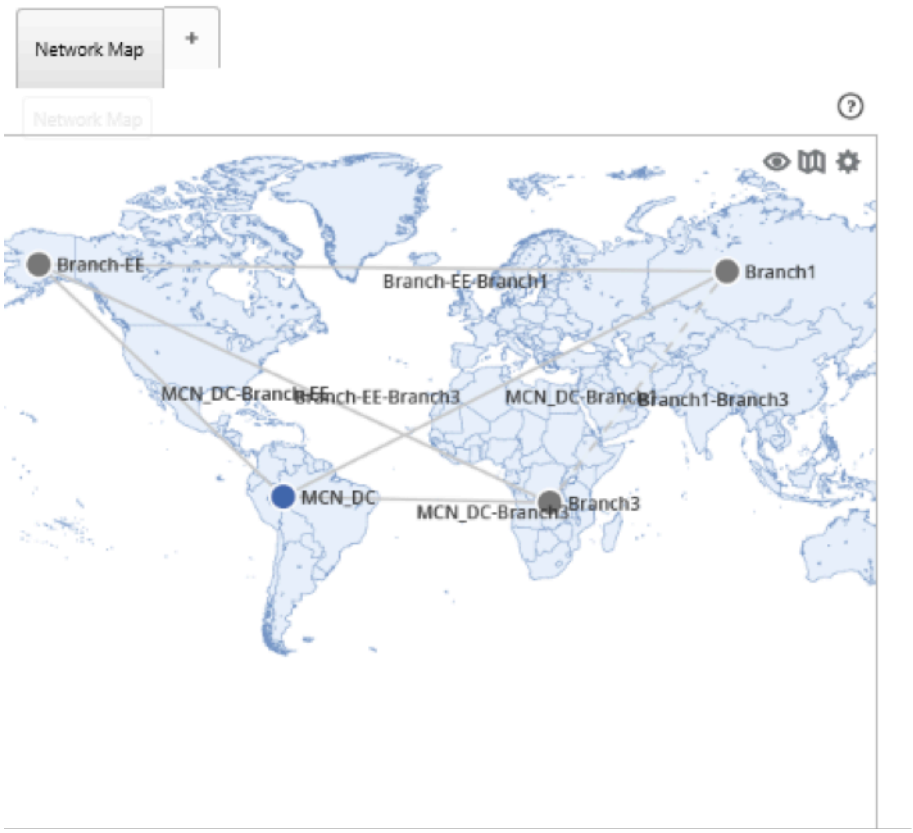
6. Wählen **Sie im Feld Netzwerkkarten verwenden von**eine der folgenden Optionen aus.

   - **Aktuelles Paket**: Behalten Sie den aktuell gespeicherten Satz von Netzwerkkarten nach dem Import bei.
   - **Neues Paket**: Verwenden Sie die Netzwerkkarten aus dem importierten Paket und verwerfen Sie den aktuellen Kartensatz.
   - **Beide Pakete**: Verwenden Sie die importierten Karten zusätzlich zu den aktuell gespeicherten Karten.

7. Klicken Sie auf **Importieren**. Die Konfiguration wird importiert.



8. Im Abschnitt **Netzwerkkarte**. Klicken Sie auf das Einstellungssymbol und wählen Sie **Automatisch ausfüllen** aus, um jede Site in der Konfiguration automatisch der Karte hinzuzufügen und anzuordnen.



Datenbank verwalten

April 13, 2021

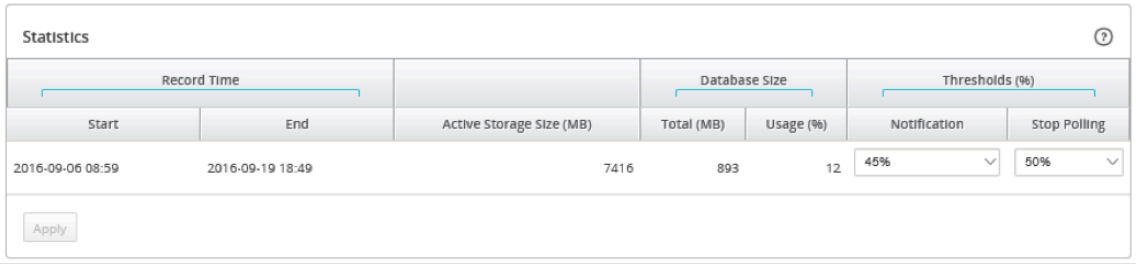
Sie können die Datenbank überwachen und verwalten, um sicherzustellen, dass genügend Speicherplatz verfügbar ist, um die Abrufdaten aller erkannten Appliances im Netzwerk zu speichern.

Anzeigen von Datenbankstatistiken

Die Tabelle **Statistik** zeigt die verfügbaren Datenbankstatistiken an und enthält Eingabefelder zum Festlegen der Schwellenwerte für die Datenbankfestplattennutzung für Benachrichtigungen und Abfragen.

So zeigen Sie Datenbankstatistiken an:

1. Klicken Sie in der Citrix SD-WAN Center Web UI auf die Registerkarte **Administration**.
2. Klicken Sie auf **Datenbankverwaltung**. Im Abschnitt **"Statistics"** werden folgende Informationen angezeigt.
    - **Datensatzzeit:** Zeigt Datum und Zeitstempel für die ältesten und letzten Datensätze in der Datenbank an. Diese Spalte enthält die folgenden Informationen:
        - **Start:** Zeigt Datum und Zeitstempel des ältesten Datensatzes in der Datenbank an.
        - **Ende**: Zeigt Datum und Zeitstempel des letzten Datensatzes in der Datenbank an.
    - **Aktive Speichergröße (MB)**: Zeigt den Speicherplatz des aktuellen aktiven Speichers an.
    - **Datenbankgröße (MB)**: Zeigt die aktuelle Datenbankgröße und Verwendungsinformationen an. Diese Spalte enthält die folgenden Informationen:
        - **Summe (MB)**: Zeigt die Gesamtgröße der Datenbank in MB an.
        - **Verwendung (%)**: Zeigt den Prozentsatz der Datenträgernutzung auf dem Festplattenspeicher des aktuell aktiven Speichers an.



So legen Sie den Benachrichtigungs- und Abrufschwellenwert fest:

1. Geben Sie im Feld **Benachrichtigung** den Prozentsatz der Datenbankgröße oder der aktiven Speichergröße ein, die als Schwellenwert für die Erstellung einer Benachrichtigung über die Datenbanknutzung verwendet werden soll. Eine E-Mail-Benachrichtigung wird gesendet, wenn die Datenbanknutzung diesen Schwellenwert überschreitet.
2. Geben Sie im Feld **Abruf beenden** den Schwellenwert für die Datenbankdatenträgerauslastung (Prozentsatz) ein, an dem die Statistikabfrage beendet werden soll. Wählen Sie im Dropdownmenü einen Wert von **10%** bis **50%** aus. Der Standardwert ist **50%**.
3. Klicken Sie auf **Apply**.

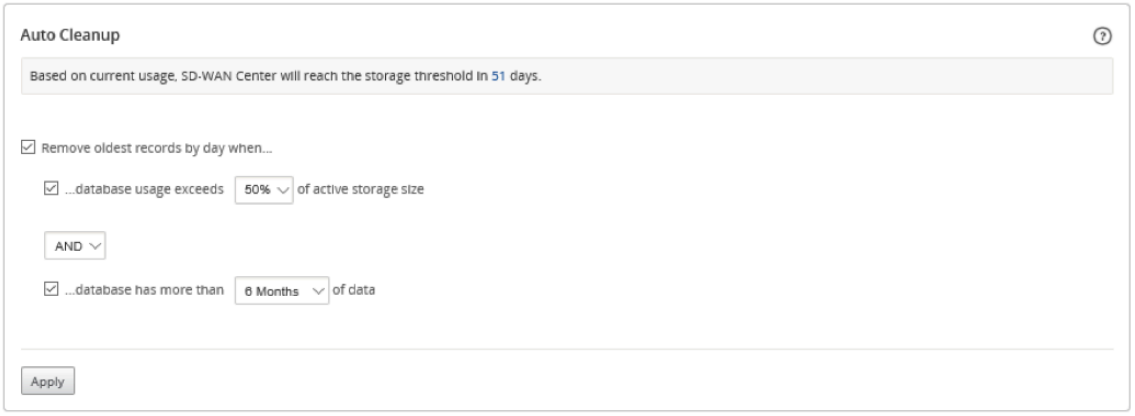
Konfigurieren der automatischen Bereinigung

Um die Datenbankdatenträgerauslastung unter Kontrolle zu halten, können Sie Schwellenwerte angeben, die bei Überschreiten das Entfernen älterer Datensätze aus der Datenbank auslösen.

So aktivieren Sie die Datenbankbereinigung und konfigurieren die Schwellenwerte:

1. Klicken Sie in der Citrix SD-WAN Center Web UI auf die Registerkarte **Administration**.
2. Klicken Sie auf **Datenbankverwaltung**.
3. Wählen Sie unter **Auto Cleanup** die Option **Älteste Datensätze nach Tag entfernen…, um die Datenbankbereinigung zu aktivieren.**

   Wenn diese Option aktiviert ist, wird die Datenbank täglich um 2:00 Uhr überprüft. Die Prüfung initiiert eine Datenbankbereinigung, wenn die angegebenen Schwellenwerte erreicht oder überschritten werden. Standardmäßig ist dies nicht aktiviert.



4. Wählen Sie**… Datenbanknutzung überschreitet (%) der aktiven Speichergröße** und wählen Sie dann einen Prozentsatz aus dem Dropdownmenü aus, um den Schwellenwert für eine Datenbankbereinigung anzugeben. Die Optionen sind von **10%** bis **50%** in Schritten von **5%**.
5. Wählen Sie **ANDoder**OR, einen Operator aus dem Dropdown-Menü zwischen „…Datenbank-Nutzung überschreitet…“und „…Datenbank hat mehr als…“-Schwellenwerte aus, um einen

Operator anzugeben, um diese Regel für diese Schwellenwerte anzuwenden. Der Standardwert ist**UND**.

6. Wählen Sie**.. Datenbank hat mehr als** [# Monate] **Monate an Daten** und wählen Sie dann die Anzahl der Monate aus dem Dropdownmenü, um den Zeitspanne Schwellenwert für eine Datenbankbereinigung anzugeben, für die Daten in der Datenbank gespeichert werden sollen. Die Optionen sind von **3 Monaten** bis **12 Monaten** in Schritten von einem Monat.
7. Klicken Sie auf **Apply**.

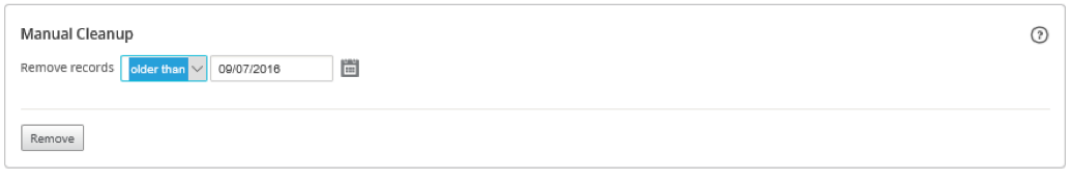
Konfigurieren der manuellen Bereinigung

Sie können Statistik- und Ereignisdatensätze basierend auf angegebenen Kriterien manuell aus der Datenbank entfernen.

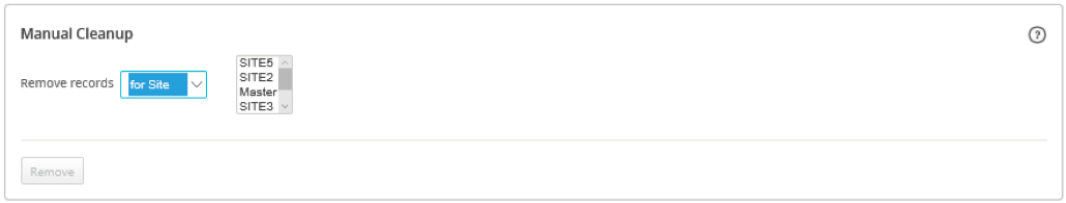
So führen Sie eine manuelle Datenbankbereinigung durch:

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.
2. Klicken Sie auf **Datenbankverwaltung**.
3. Wählen Sie **unter Manuelle Bereinigung** einen Filter aus dem Dropdownmenü **Datensätze entfernen** aus. Die Filteroptionen sind:

   - **älter als:** Entfernen Sie Datensätze, die vor einem angegebenen Datum gesammelt wurden. Wenn Sie diesen Filter auswählen, werden ein Datumsfeld und eine Kalenderauswahlschaltfläche angezeigt. Klicken Sie auf die Kalenderschaltfläche, um ein Datum auszuwählen. Alle Datensätze, die älter als das angegebene Datum sind, werden entfernt.

   - **für Site:** Entfernen Sie Datensätze, die vor einem angegebenen Datum gesammelt wurden. Wenn Sie diesen Filter auswählen, werden ein Datumsfeld und eine Kalenderauswahlschaltfläche angezeigt. Klicken Sie auf die Kalenderschaltfläche, um ein Datum auszuwählen. Alle Datensätze, die älter als das angegebene Datum sind, werden entfernt.

4. Klicken Sie auf **Entfernen**.

Ansichten verwalten

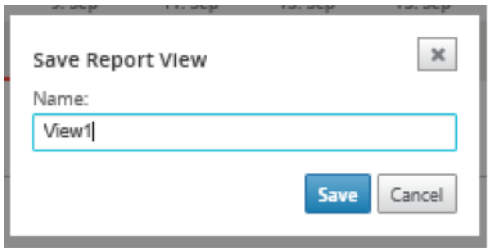
April 13, 2021

Auf der Seite Fehler, Berichterstellung, Netzwerkkarte und Statistiken können Sie die jeweiligen Ansichten erstellen, anzeigen, ändern und löschen.

> **Hinweis**
>
> Die Screenshots, die in der Prozedur verwendet werden, können je nach Art der Ansicht von der tatsächlichen Benutzeroberfläche abweichen.

So erstellen Sie eine neue Ansicht:

1. Klicken Sie auf **Neue Ansicht**. Dadurch wird eine neue, unbenannte Ansicht erstellt und die Zeitangabe auf die aktuelle Zeit zurückgesetzt.
2. Erstellen und Anwenden von Filtern oder nehmen Sie die erforderlichen Änderungen vor.
3. Klicken Sie auf **Speichern unter**.
4. Geben **Sie im Dialogfeld Ansicht speichern** einen Namen für Ihre Ansicht ein.
5. Klicken Sie auf **Save**.



So öffnen und ändern Sie eine vorhandene Ansicht:

1. Klicken Sie auf **Öffnen**.
2. Wählen **Sie im Dialogfeld Ansicht öffnen** eine Berichtsansicht aus der Dropdownliste aus.
3. Klicken Sie auf **Öffnen**. Die Ereignisansicht wird geöffnet.
4. Nehmen Sie die notwendige Änderung nach Bedarf vor.
5. Klicken Sie auf **Save**.

Um eine Ansicht zu löschen, öffnen Sie die Ansicht und klicken Sie auf das Symbol Löschen.

Software-Upgrade

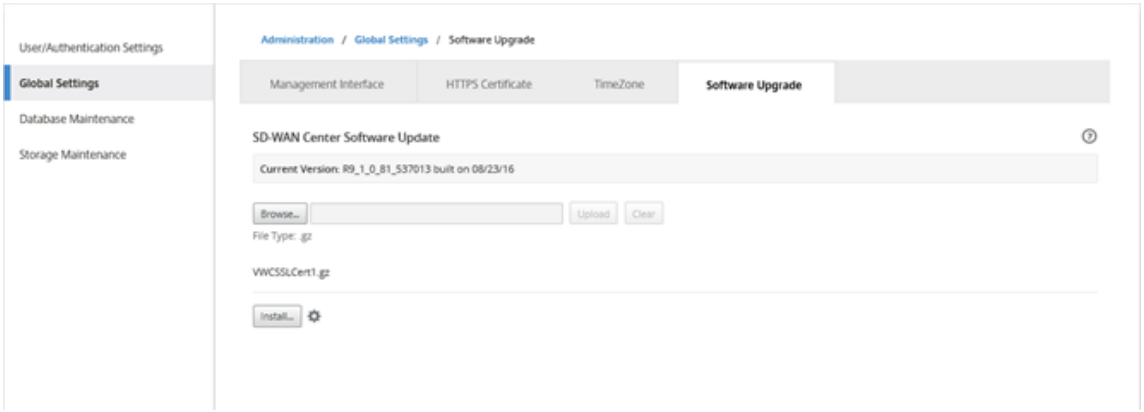
April 13, 2021

Sie können die Option Software-Upgrade verwenden, um Ihre Citrix SD-WAN Center-Software auf die neueste Version zu aktualisieren. Der Software-Upgradeprozess versetzt Citrix SD-WAN Center in den Wartungsmodus. Wenn eine Datenbankmigration erforderlich ist, kann dieser Vorgang mehrere Stunden dauern. Während dieser Zeit werden keine Statistikdaten aus dem Virtual WAN gesammelt, und alle Citrix SD-WAN Center-Funktionen sind nicht verfügbar.

> **Wichtig**
>
> Es wird empfohlen, das Upgrade während der Wartungszeiten auszuführen.
>
> **Hinweis**
>
> Laden Sie das entsprechende Citrix SD-WAN Center Softwarepaket auf Ihren lokalen Computer herunter. Sie können dieses Paket vonDownloadsSeite herunterladen.

So laden Sie eine neue Version der Citrix SD-WAN Center-Software hoch und installieren Sie sie

1. Klicken Sie in der Citrix SD-WAN Center-Weboberfläche auf die Registerkarte **Administration**.
2. Klicken Sie auf **Globale Einstellungen** und dann auf **Software-Upgrade**.



3. Klicken Sie auf **Durchsuchen**, um einen Dateibrowser zu öffnen, und wählen Sie das Softwarepaket aus, das Sie hochladen möchten.
4. Klicken Sie auf **Hoch** laden, um das ausgewählte Softwarepaket auf die aktuelle virtuelle Citrix SD-WAN Center-Maschine hochzuladen.
5. Klicken Sie nach Abschluss des Uploads auf **Installieren**.

6. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Installieren**.
7. Aktivieren Sie im angezeigten Dialogfeld das Kontrollkästchen **Ich akzeptiere den Endbenutzer-Lizenzvertrag**, und klicken Sie dann auf **Installieren**.

Zeitleisten-Steuerelemente

April 13, 2021

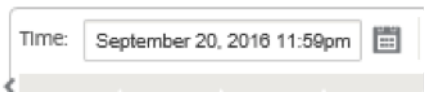
Die Zeitleiste oben auf der Seite “Fehler”, “Berichterstellung”, “Netzwerkkarte”und “Statistiken”enthält Steuerelemente, mit denen Sie den Zeitrahmen der aktuellen Ansicht einschränken können. Sie können einen Zeitrahmen von bis zu 30 Tagen Daten aus der aktuellen Datenbank anzeigen.

> **Hinweis**
>
> Basierend auf dem ausgewählten Zeitraum können Sie die historischen Daten unabhängig von der aktuellen Citrix SD-WAN-Netzwerkkonfiguration anzeigen.

Zeit

Sie können die folgenden Elemente verwenden, um einen Zeitrahmen für die aktuelle Ansicht festzulegen:

- **Time:** Geben Sie das Datum und die Uhrzeit in das Feld **Zeit** ein, um das Ergebnis auf ein bestimmtes Datum und eine bestimmte Uhrzeit einzugrenzen. Das Format kann eines der folgenden sein:
  - ***Month Day, Year Hour:Minutes*** [**am** / **pm**] For example: September 7, 2015 2:00pm.
  - ***MM/DD/YYYY HH:MM*** [**am** / **pm**] For example: 09/07/2015 8:36am.
  - ***M/D/YY H:MM*** [**am** / **pm**] For example: 9/7/15 10:14pm
- **Kalender** - (Kalendersymbol) Klicken Sie auf das Kalendersymbol rechts neben dem Feld Zeit, und wählen Sie ein Datum aus, um die Ansichtsergebnisse auf dieses Datum zu beschränken.



- **Zeitlinie** - Klicken Sie auf einen anderen Punkt auf einer Zeitachse, und ziehen Sie ihn an einen anderen Punkt, um einen Zeitrahmen von mindestens 30 Minuten auszuwählen.

- **Zuletzt: Stunden/Tag/Woche/Monat** - Klicken Sie auf eine Option (**Stunde**, **Tag**, **Woche** oder **Monat**), um die Ansichtsergebnisse auf diesen Zeitraum zu beschränken.

Modus

Der Zeitleistenmodus legt fest, wie die Zeitachse die Auswahl des Zeitrahmens interpretiert und wie automatische Aktualisierungen in der aktuellen Ansicht und im Dashboard widergespiegelt werden. Es gibt zwei Modusoptionen **Relativ** (*ausgewählter Zeitrahmen*) und **Absolute** (*ausgewählter Zeitrahmen*), wobei der ausgewählte Zeitrahmen der im Feld **Zeit** angegebene Zeitrahmen ist.

Zum Ändern des Zeitachsenmodus wählen Sie rechts oben in der Zeitachse im Dropdownmenü **“Modus”** die Option **“Relativ”** oder **“Absolut”.**

Relativer Modus

Wenn Sie den **relativen** Modus auswählen, wird mit der Zeitachse der Zeitrahmen **als** relativer Zeitraum behandelt. Wenn Sie die Ansicht speichern und später öffnen, sind die in der Ansicht dargestellten Informationen relativ zu dem Zeitpunkt, zu dem die Ansicht geöffnet wurde. Wenn Sie automatische Aktualisierungen aktiviert haben und eine Statistikaktualisierung erkannt wird, wird die Ansicht relativ zum zuletzt in der Datenbank aufgezeichneten Zeitpunkt aktualisiert.

Der aktuell angegebene Zeitrahmen wird in Klammern als Teil der Menüoption **“Relativ”** angezeigt. Wenn Sie beispielsweise **“Letzter Tag”** als Zeitraum auswählen, wird die Option **“Relativ”** angezeigt (1 Tag und dann 1 Minute).

Absoluter Modus

Wenn Sie **“Absoluter Modus”** auswählen, wird der für **Zeit**: festgelegte Zeitraum als absoluter (statischer) Punkt in der Zeit behandelt. Die Ansicht stellt immer die ausgewählte Zeit dar, auch wenn Sie die Ansicht speichern und zu einem späteren Zeitpunkt öffnen oder automatische Aktualisierungen aktivieren. Der aktuell angegebene Zeitrahmen wird in Klammern als Teil der Menüoption **“Absolute”** mit folgendem Format angezeigt:

Absolute (*start_date start_time - end_date end_time*)

Wenn Sie beispielsweise **Letzter: Tag** als Zeitraum auswählen und das aktuelle Datum und die Uhrzeit 9/7 4:43 PM sind, wird bei der Option **Absolute** Folgendes angezeigt: **Absolute (9/6 4:43 PM - 9/7 4:43 PM)**.

Benutzerkonten

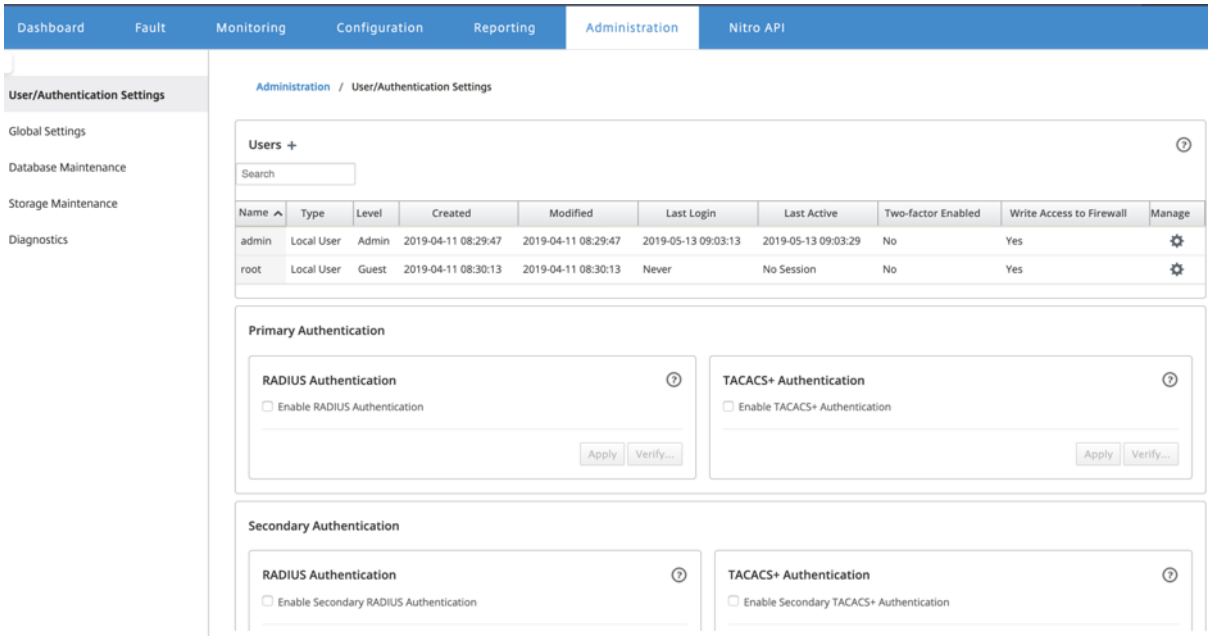
April 13, 2021

Sie können eine Liste aller lokalen und Remotebenutzerkonten anzeigen, die sich mindestens einmal bei der virtuellen Citrix SD-WAN Center-Maschine angemeldet haben. Remote-Benutzerkonten werden über RADIUS- oder TACACS + -Authentifizierungsserver authentifiziert. Sie können Citrix SD-WAN Center auch ein neues lokales Benutzerkonto hinzufügen.

> **Hinweis**
>
> Wenn ein Benutzerkonto auf einem Remoteauthentifizierungsserver verfügbar ist, aber nie zur Anmeldung bei Citrix SD-WAN Center verwendet wird, wird es nicht in der Liste **Benutzer** angezeigt.

Um Benutzerkonten in der SD-WAN Center-Weboberfläche anzuzeigen, navigieren Sie zu **Administration > Benutzer-/Authentifizierungseinstellungen**.

Eine Liste der Benutzerkonten wird im Abschnitt **Benutzer** angezeigt.



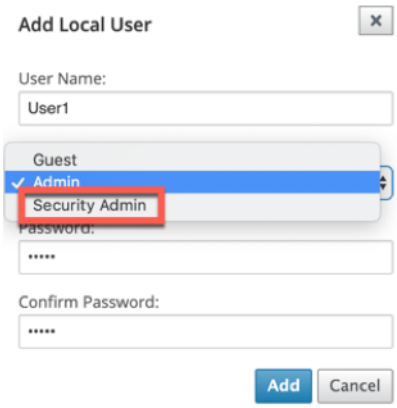
Folgende Informationen werden angezeigt:

- **Name:** Der Benutzername.
- **Typ**: Der Typ des Benutzerkontos kann einer der folgenden sein:
  - **Lokal:** Benutzerkonten, die lokal über die SD-WAN Center-Schnittstelle erstellt und verwaltet werden.

  - **RADIUS**: Vom RADIUS-Server authentifizierte Remote-Benutzerkonten.
  - **TACACS +**: Remote-Benutzerkonten, die vom TACACS + -Server authentifiziert wurden.

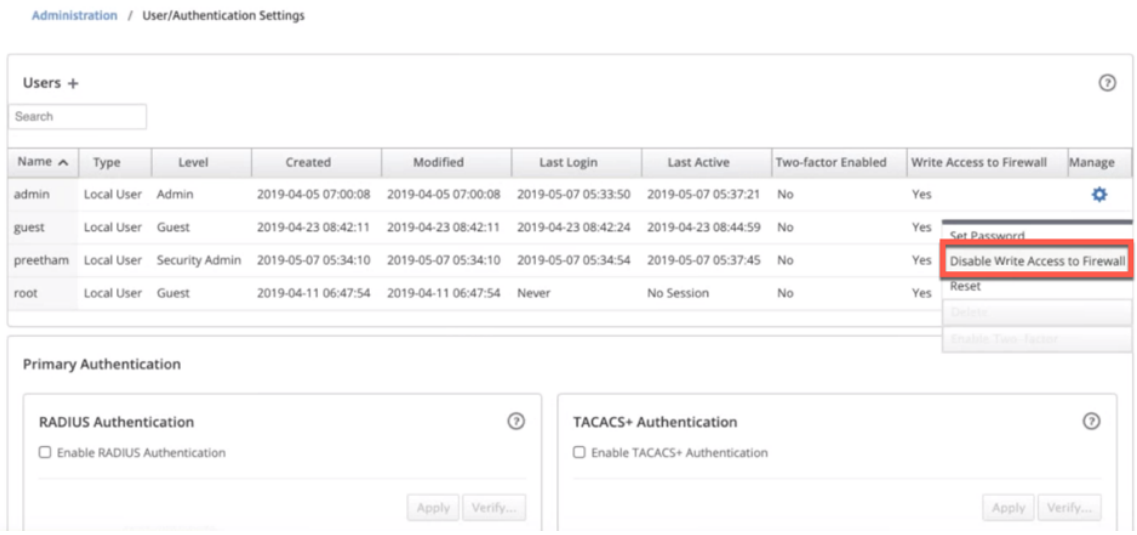
- **Ebene:** Die folgenden drei Stufen der Kontoberechtigung:

  - **Admin**: Administratorkonto verfügt über Administratorrechte. Es hat Lese-/Schreibzugriff auf alle Abschnitte.
  - **Gast**: Das Gastkonto ist ein schreibgeschütztes Konto mit Zugriff auf die Seite **Dashboard**, **Reporting**und **Überwachung**.
  - **Sicherheitsadministrator**: Ein **Sicherheitsadministrator** hat nur den Lese-/Schreibzugriff für die Firewall- und sicherheitsbezogenen Einstellungen im **Konfigurationseditor**, während er Lesezugriff auf die verbleibenden Abschnitte hat.

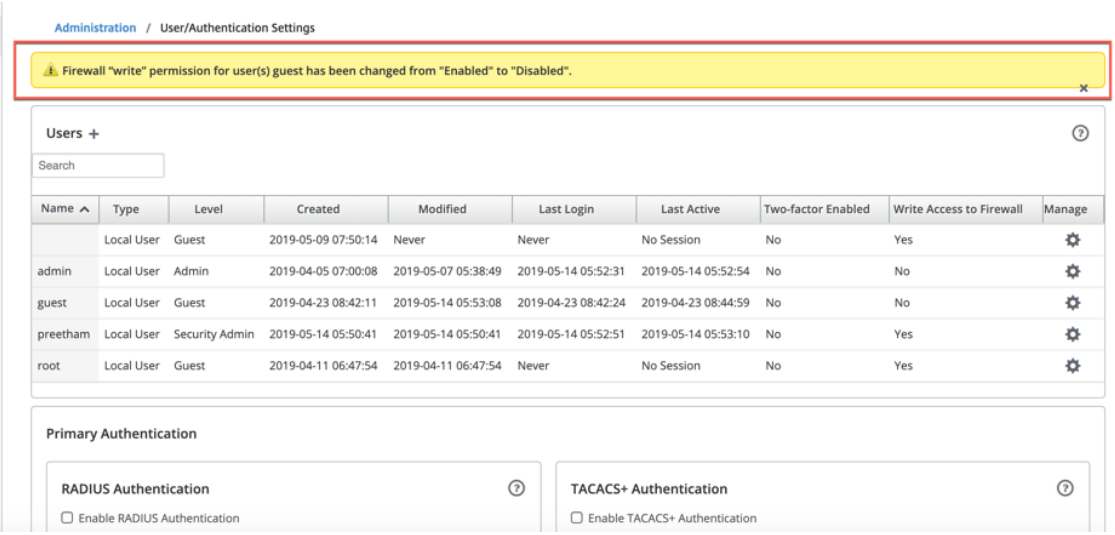


Der Administrator kann die Konfiguration erstellen und exportieren, und der Sicherheitsadministrator kann die Konfiguration importieren und die sicherheitsbezogenen Änderungen bei Bedarf vornehmen. Nur ein Sicherheitsadministrator kann die Konfiguration der Sicherheitsfunktion ändern oder ändern.

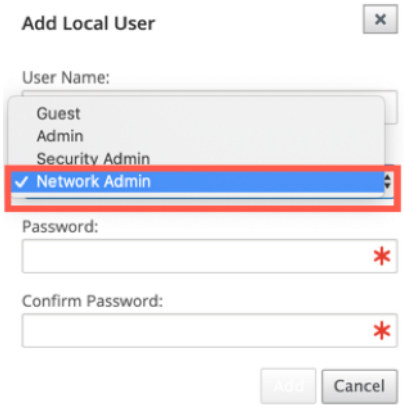
> **HINWEIS:**Der
> Sicherheitsadministrator hat die Berechtigung, den Schreibzugriff auf die Firewall für andere Benutzer (Admin/Guest) zu deaktivieren.



Eine Benachrichtigungsleiste wird allen Benutzern angezeigt, nachdem der Sicherheitsadministrator die Firewall-Schreibberechtigung für einen bestimmten Benutzer geändert hat. Diese Benachrichtigung wird pro Benutzer angezeigt und daher muss jeder angemeldete Benutzer die Warnung bestätigen, damit sie entfernt werden kann.



- **Netzwerkadministrator**: Ein **Netzwerkadministrator** hat keinen Zugriff auf die Firewall. Der Netzwerkadministrator hat nur Lese-/Schreibzugriff auf die Netzwerkeinstellungen, während er schreibgeschützt auf die verbleibenden Abschnitte zugreifen kann.



Der Knoten der gehosteten Firewall ist für den Netzwerkadministrator nicht verfügbar. In diesem Fall muss der Netzwerkadministrator eine neue Konfiguration importieren. Sowohl Netzwerk- als auch sicherheitsbezogene Einstellungen werden vom Superadministrator (Admin) verwaltet.

Der Netzwerk- und Sicherheitsadministrator kann nur Änderungen an der Konfiguration vornehmen, kann aber nur vom **Superadministrator (Admin)**auf das Netzwerk angewendet werden.

Ein Superadministrator (admin) hat die folgenden Berechtigungen:

- Kann die Konfiguration in den Posteingang zur Änderungsverwaltung exportieren, um eine Konfiguration und ein Softwareupdate im Netzwerk durchzuführen.
- Kann auch den Lese- und Schreibzugriff der Netzwerk- und Sicherheitsadministratoren umschalten.

- **Erstellt**: Bei lokalen Benutzerkonten das Datum, an dem das Benutzerkonto erstellt wurde. Bei einem Remotebenutzerkonto das Datum der ersten Anmeldesitzung.
- **Geändert**: Bei lokalen Benutzerkonten das Datum, an dem das Kennwort zuletzt geändert wurde. Für Remote-Benutzer das Datum der ersten Anmeldesitzung.
- **Letzter Login**: Das Datum, an dem sich der Benutzer zuletzt angemeldet hat. Eine QuickInfo zeigt die IP-Adresse des Geräts an, das zur Anmeldung verwendet wurde.
- **Zuletzt aktiv**: Das Datum, an dem die letzte Anforderung an den Server gestellt wurde. Eine QuickInfo zeigt die IP-Adresse des Geräts an, das zur Anmeldung verwendet wurde.
- **Verwalten:** Klicken Sie auf das Zahnradsymbol, um ein Menü mit den folgenden Optionen anzuzeigen:
  - **Kennwort festlegen**: Kennwort für das lokale Benutzerkonto ändern. Das aktuelle root-Kennwort ist erforderlich, um das root-Kennwort zu ändern. Sie können die Kennwörter von Remotebenutzerkonten nicht ändern.

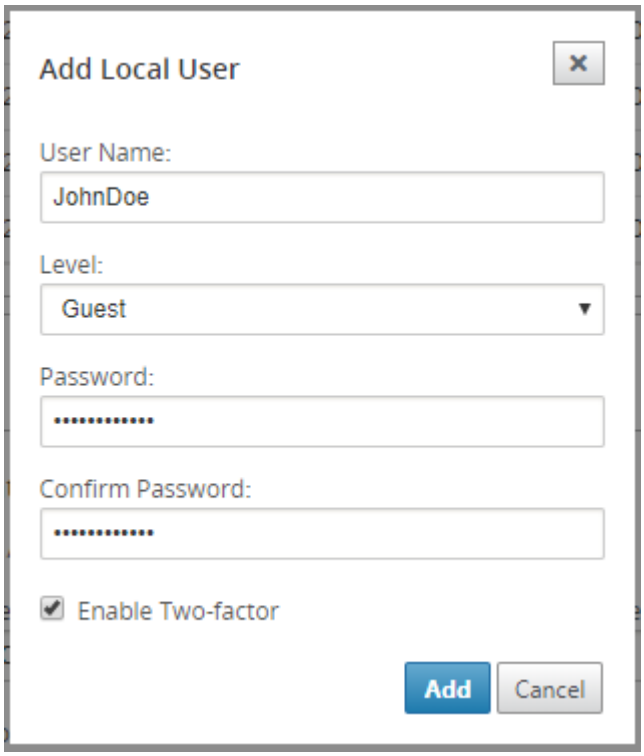
  - **Zurücksetzen**: Entfernen Sie die Arbeitsbereiche und Einstellungen für dieses Benutzerkonto.
  - **Löschen**: Löschen Sie das lokale Benutzerkonto, die Arbeitsbereiche und die Einstellungen aus dem SD-WAN Center. Sie können Remote- und Administratorkonten nicht löschen.
  - **Zwei-Faktor-Aktivierung:** Aktivieren Sie die Zwei-Faktor-Authentifizierung für das lokale und Remote-Benutzerkonto. Weitere Informationen finden Sie unter Zwei-Faktor-Authentifizierung.

- **Schreibzugriff auf Firewall**: Zeigt an, dass der Schreibzugriff auf Firewall aktiviert oder deaktiviert ist.

So fügen Sie dem Citrix SD-WAN Center ein neues lokales Benutzerkonto hinzu:

> **Hinweis**
>
> Die in Citrix SD-WAN Center lokal erstellten Benutzerkonten verfügen nicht über die Berechtigung, das Netzwerkkonfigurationspaket zu bearbeiten und in das MCN zu exportieren.

1. Klicken Sie auf das Symbol Hinzufügen + neben **Benutzer**. **Das Dialogfeld Lokalen Benutzer hinzufügen** wird angezeigt.



2. Geben Sie Werte für die folgenden Parameter ein:

   - **Benutzername**: Der Benutzername für das lokale Benutzerkonto.

- **Ebene**: Die Kontoberechtigung. Ein Gastbenutzerkonto ist ein schreibgeschütztes Konto, das auf das Anzeigen von Dashboards, Berichten und Statistiken beschränkt ist. Das Gastbenutzerkonto hat nicht die Berechtigung zum Bearbeiten und Exportieren des Netzwerkkonfigurationspakets in das MCN.
- **Kennwort**: Das Kennwort für das Benutzerkonto.
- **Kennwort bestätigen**: Geben Sie das Kennwort zur Bestätigung erneut ein.

3. Wählen Sie **Zwei-Faktor-** Authentifizierung aktivieren aus, um die Zwei-Faktor-Authentifizierung für das lokale Benutzerkonto zu aktivieren.

   > **Hinweis**
   >
   > Die Option **Zwei-Faktor-aktivieren** wird nur angezeigt, wenn der sekundäre Authentifizierungsserver konfiguriert ist.
   >
   > Konfigurieren Sie einen sekundären Authentifizierungsserver, entweder RADIUS- oder TACAS + -Authentifizierung. Stellen Sie sicher, dass das Benutzerkonto auf dem sekundären Authentifizierungsserver konfiguriert ist. Weitere Informationen finden Sie unter Sekundäre Authentifizierung.

4. Klicken Sie auf **Hinzufügen**.Das neue Benutzerkonto wird erstellt, und die Kontoinformationen werden der Tabelle **Benutzer** hinzugefügt.

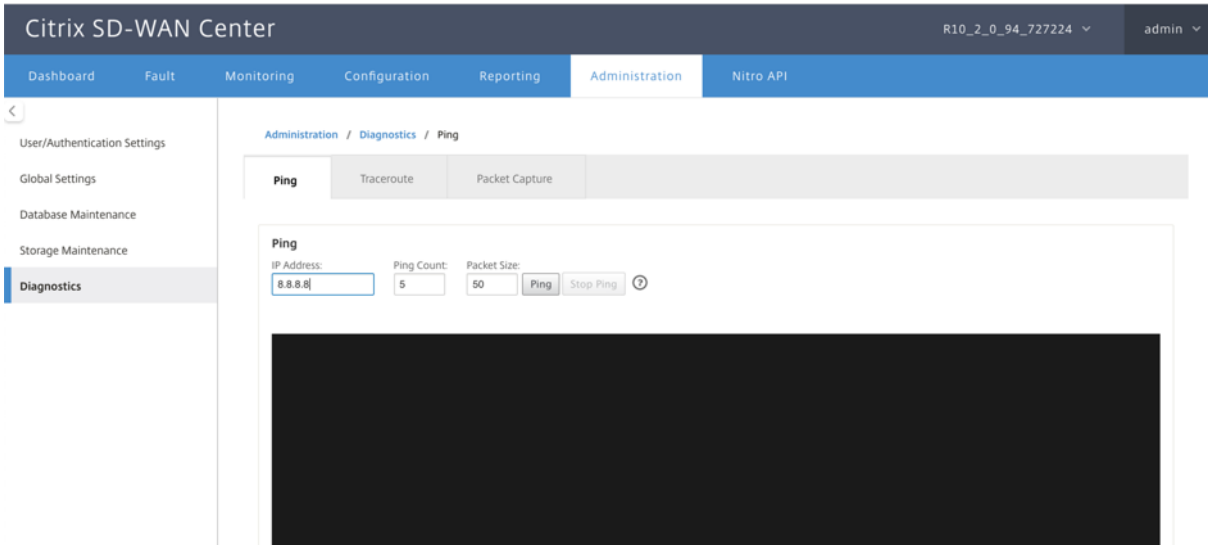
> **Hinweis**
>
> Das Citrix SD-WAN Center kann bis zu 600 lokale Benutzer haben.

Diagnose

April 13, 2021

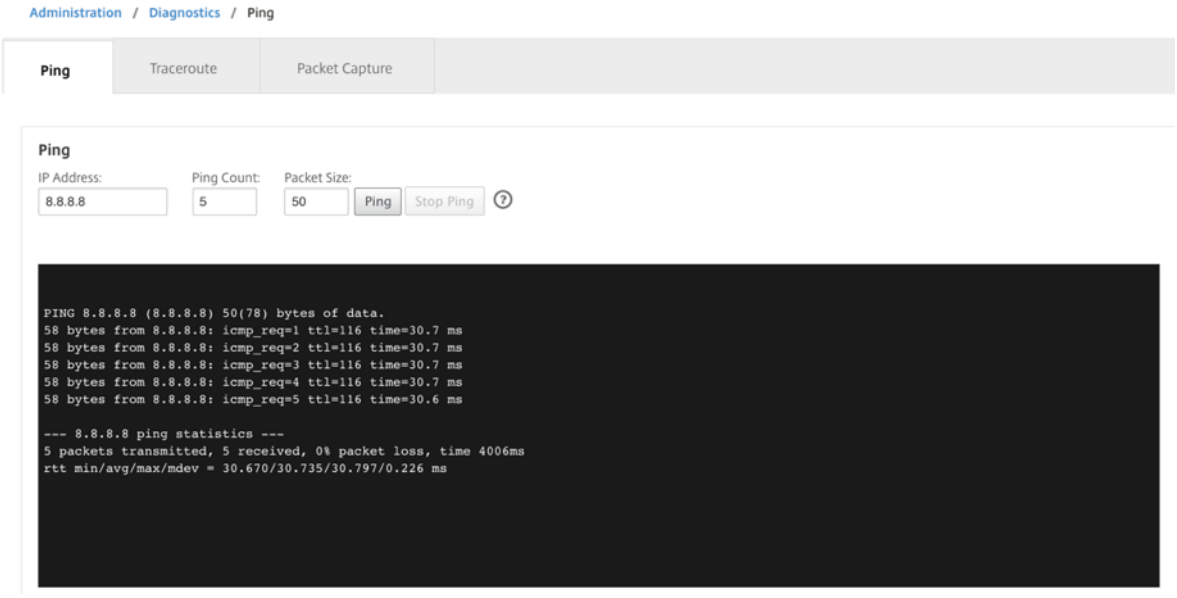
Citrix SD-WAN Center Diagnostics Utilities bieten Ping-, Traceroute- und Paketerfassungsfunktion zum Testen und Untersuchen von Verbindungsproblemen auf der Citrix SD-WAN Center-Appliance. Die Diagnoseoptionen im **Citrix SD-WAN Center Dashboard** steuern die Datensammlung.

Um das Diagnose-Tool zu verwenden, navigieren Sie zu **Administration > Diagnose**.



Ping

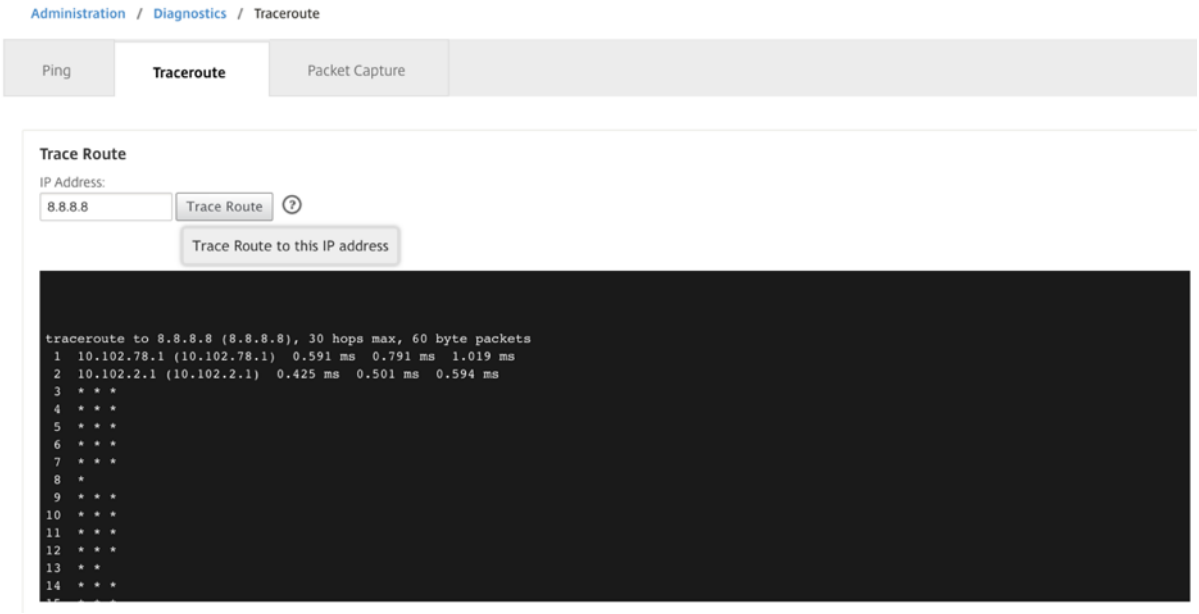
Mit der Option **Ping** können Sie eine beliebige Management-IP-Adresse im SD-WAN Center-Netzwerk anpingen.



Geben Sie eine gültige IP-Adresse zusammen mit der Anzahl der Ping-Zähler (wie oft die Ping-Anforderung gesendet werden soll) und der Paketgröße (Anzahl der Datenbytes) an. Klicken Sie auf **Ping beenden**, um eine laufende Pingsuche zu beenden.

Traceroute

Verwenden Sie die Option **Traceroute**, um sicherzustellen, dass die IP-Adressen erreichbar sind. Sie können jede Management-IP-Adresse im Netzwerk nachvollziehen, indem Sie die Route anzeigen und Transitverzögerungen von Paketen messen.

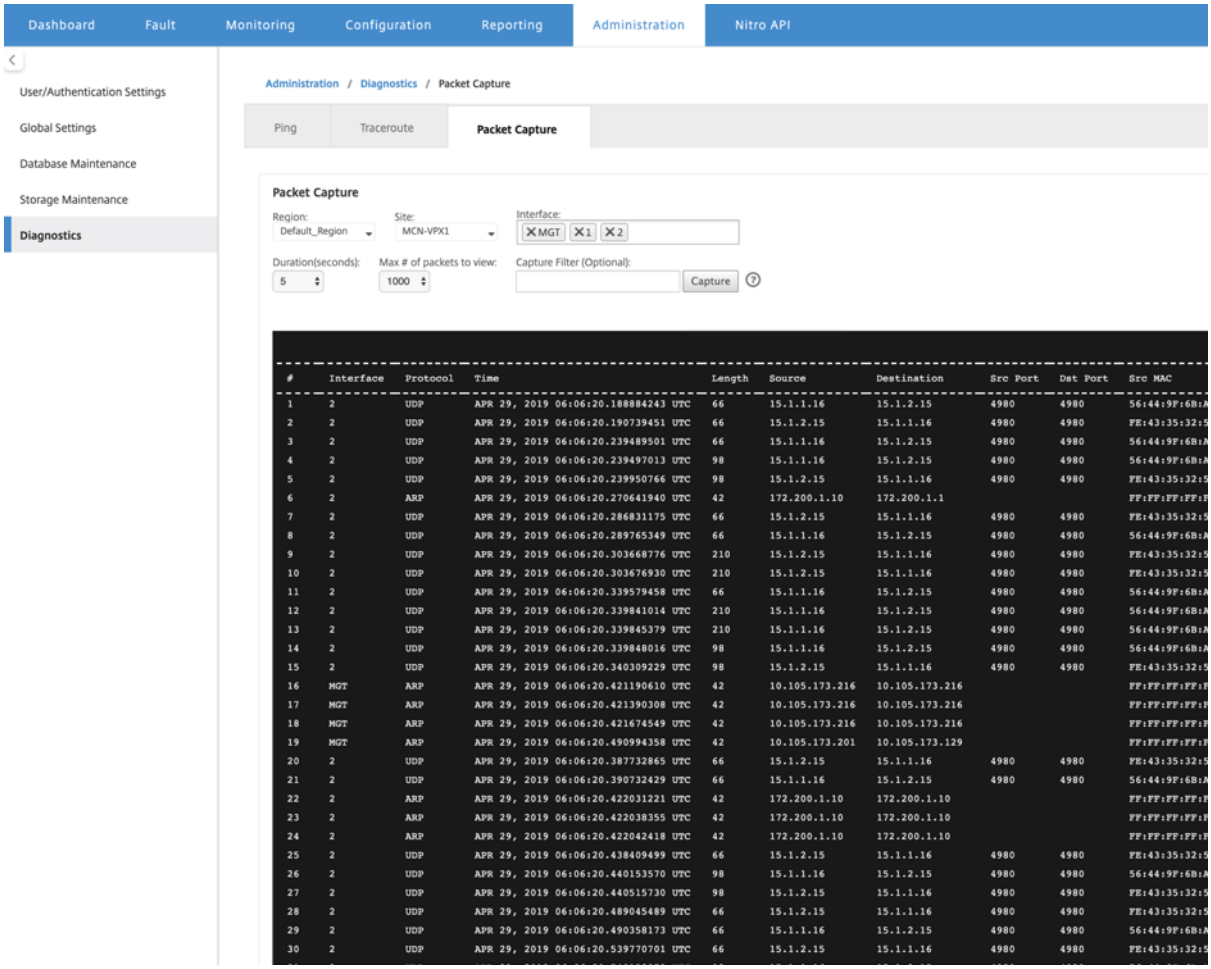


Geben Sie eine gültige Management-IP-Adresse für die Verfolgung der Route ein. Klicken Sie auf **Route verfolgen**.

> **HINWEIS:**
>
> Das Traceroute-Ergebnis zeigt maximal 30 Hops an.

Paketerfassung

Verwenden Sie die Option **Paketerfassung**, um das Datenpaket abzufangen, das über die ausgewählte aktive Schnittstelle in der ausgewählten Site durchläuft.



Geben Sie die folgenden Eingaben für den Paketerfassungsvorgang an:

- **Region** - Wählen Sie in der Dropdownliste eine Region aus, die vom SD-WAN-Center verwaltet wird.
- **Site** - Verfügbare Sites in der ausgewählten Region. Wählen Sie eine Site aus der Dropdownliste aus.
- **Schnittstelle** - Aktive Schnittstellen sind für die Paketerfassung in der ausgewählten Site verfügbar. Wählen Sie eine Schnittstelle aus oder fügen Sie Schnittstellen aus der Dropdownliste hinzu. Wählen Sie mindestens eine Schnittstelle aus, um eine Paketerfassung auszulösen.

  > **HINWEIS:**
  >
  > Die Möglichkeit, die Paketerfassung über alle Schnittstellen gleichzeitig auszuführen, hilft, die Problembehandlungsaufgabe zu beschleunigen.

- **Dauer (Sekunden)** —Dauer (in Sekunden), wie lange die Daten erfasst werden müssen.
- **Max. Anzahl der anzuzeigenden Pakete** - Maximale Anzahl der Pakete, die im Paketerfassungsergebnis angezeigt werden sollen.

- **Capture-Filter (Optional)** - Das optionale **Capturefilter**-Feld akzeptiert eine Filterzeichenfolge, die verwendet wird, um zu bestimmen, welche Pakete erfasst werden. Pakete werden mit der Filterzeichenfolge verglichen und wenn das Vergleichsergebnis wahr ist, wird das Paket erfasst. Wenn der Filter leer ist, werden alle Pakete erfasst. Weitere Informationen finden Sie unter Capture-Filter.

  Im Folgenden finden Sie einige Beispiele für diesen Capture-Filter:

  - **Ether proto\ARP** - Erfasst nur ARP-Pakete
  - **Ether proto\IP** - Erfasst nur IPv4-Pakete
  - **VLAN 100** - Erfasst nur Pakete mit einem VLAN von 100\
  - **Host 10.40.10.20** - Erfasst nur IPv4-Pakete zum oder vom Host mit der Adresse 10.40.10.20
  - **Net 10.40.10.0 Mask 255.255.255.0** - Erfasst nur IPv4-Pakete im Subnetz 10.40.10.0/24
  - **IP proto \ TCP** - Erfasst nur IPv4/TCP Pakete
  - **Port 80** - Erfasst nur IP-Pakete zu oder von Port 80
  - **Portbereich 20 —30** - Erfasst nur IP-Pakete zu oder von den Ports 20 bis 30
  - **Host 10.40.10.20 und Port 80 und TCP** - Erfasst nur IP-Pakete zum oder vom TCP-Port 80 auf dem Host 10.40.10.20

> **Hinweis:**
>
> Die maximale Größe der Aufnahmedatei beträgt bis zu 575 MB. Sobald die Paketaufnahmedatei diese Größe erreicht hat, wird die Paketerfassung gestoppt.

Klicken Sie auf **Erfassen**, um das Ergebnis der Paketerfassung anzuzeigen.