Umbau der Catalyst SD-WAN-Fabric

Inhalt

Einleitung

In diesem Dokument wird die Wiederherstellung einer Cisco SD-WAN-Fabric beschrieben, einschließlich der Sicherung und Wiederherstellung der Controller-Konfigurationen für verschiedene Bereitstellungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Cisco Software Central
- Laden Sie die Controller-Software unter software.cisco.com herunter.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Voraussetzungen vor der Fabric-Wiederherstellung

- Neuer Satz von System-ips, Standort-IDs muss für die neue Fabric der Controller konfiguriert werden
- Stellen Sie sicher, dass Firewall-Regeln vorhanden sind, um die Kommunikation zwischen Controllern und Edges zu ermöglichen.
- Notieren Sie sich den Benutzernamen und das Kennwort neo4j(configuration-db) (dies muss

auf allen vManage-Knoten in einem Cluster identisch sein).
- Deaktivieren Sie Port-Hop an allen Edges.
- Erhöhen Sie die Neustartzeit auf 7 Tage.
- Löschen von Alarmen in Drittanbieter-Tools vor der Migration
- Verlaufsstatusdaten (Alarme, Ereignisse, Gerätestatistiken usw.) gehen verloren, es sei denn, es besteht eine vorherige Einrichtung zum Exportieren von Statistiken auf einen externen Server wie vAnalytics.
- Wenn Cloud OnRamp konfiguriert ist, stellen Sie sicher, dass Sie vor Beginn dieser Aktivität auf den in der Cloud bereitgestellten c8000v zugreifen können.
- Wenn Sie SDAVC in der alten Fabric aktiviert haben, stellen Sie sicher, dass die neue Fabric aktiviert ist (für Cluster muss sie nur auf einem einzelnen Knoten aktiviert sein).
- Die Wiederherstellung der Konfigurationsdatenbank wird nur auf derselben Version wie die ursprüngliche Fabric unterstützt.
- Bestätigen Sie die Person, die für die Controller verwendet wird. Wir unterstützen COMPUTE_DATA und DATA (Details unter jedem Abschnitt)
- Für die Enterprise-CA muss das von der Enterprise-CA ausgestellte Root-Zertifikat verwendet werden, das im vorhandenen Overlay verwendet wird. Das Zertifikat wird mit dem Enterprise-CA-Server signiert und für alle Controller über die Benutzeroberfläche installiert.

Bereitstellungsoptionen

vManage-Bereitstellung

- Standalone (1 Knoten)
- Cluster (3-Node oder 6-Node)

DR-Optionen

- Kein DR
- DR mit einem Knoten
- Standby-DR-Cluster (manuell/vom Administrator ausgelöst)

Anmerkung: Weitere Informationen zur Art der Notfallwiederherstellung finden Sie unter diesem Link

---

Kombinationen:

Nr.	vManage-Einrichtung	DR-Option
1	Standalone (1 Knoten)	Kein DR
2	Standalone (1 Knoten)	DR mit einem Knoten
3	Cluster (3-Node oder 6-Node)	Kein DR
4	Cluster (3-Node oder 6-Node)	Standby-DR-Cluster

Allgemeine Schritte für alle Kombinationen

Diese Schritte gelten für alle Bereitstellungskombinationen. Sie behandeln das Aufrufen von VM-Instanzen und das Anwenden einer grundlegenden CLI-Konfiguration. In jedem Kombinationsabschnitt wird angegeben, wie viele Instanzen bereitgestellt werden müssen und welche zusätzlichen Schritte ausgeführt werden müssen.

Installation und Aktivierung von SD-WAN-Controllern (Manager, Validator, Controller)

Anmerkung: Cisco hat bestimmte Begriffe umbenannt, sodass diese austauschbar sind. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst Controller

---

Laden Sie die OVA-Dateien für SD-WAN-Controller von der Cisco Software-Download-Seite hier herunter:

- Wählen Sie vEDGE Cloud aus, und laden Sie die vBond OVA für die erforderliche Softwareversion herunter.
- Wählen Sie vManage-Software aus, und laden Sie vManage OVA für die erforderliche Softwareversion herunter.
- Wählen Sie vSmart Software aus, und laden Sie vSmart OVA für die erforderliche Softwareversion herunter.

Anmerkung: Aktivieren Sie auf den ESXi/Cloud-Plattformen vSmart, vBond und vManage Controller mithilfe der OVA-Datei. Lesen Sie das verknüpfte Dokument, und stellen Sie sicher, dass je nach SD-WAN-Bereitstellungstyp ausreichend CPU, RAM und Festplatten allen Controllern zugewiesen sind. Navigieren Sie hier, um weitere Informationen zu erhalten. Weisen Sie dem vManage-Knoten unbedingt eine sekundäre Festplatte zu, wie in der Spalte Storage Size* in der verknüpften Computing-Anleitung angegeben.

Aufrufen eines Cisco Manager-Knoten

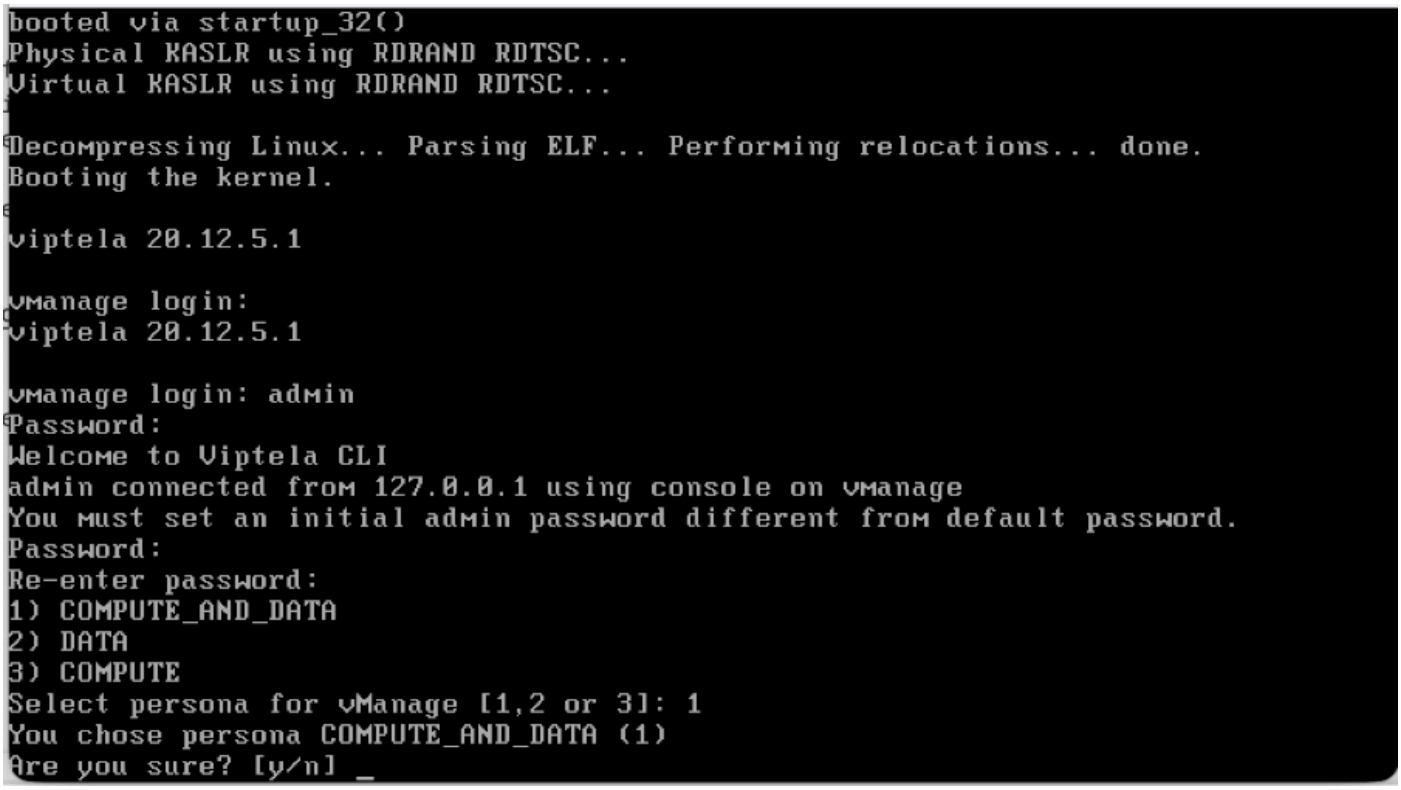
- Sobald der Cisco Manager oder vManage VM bereitgestellt wurde und der Zugriff auf die Konsole des Managers möglich ist, warten Sie, bis der Startvorgang abgeschlossen ist. Ein Hinweis ist, dass ein Meldesystem bereit ist und zur Eingabe von Benutzername und Kennwort aufgefordert wird.
- Geben Sie den Benutzernamen für die Standardbenutzerinformationen als admin und das Kennwort als admin ein. Geben Sie an, dass der Benutzer aufgefordert wird, das Kennwort zu ändern. Legen Sie das Kennwort fest, das vom Benutzer-Administrator nach Ihrer Wahl

benötigt wird.

- Anschließend wird der Benutzer aufgefordert, die Person zu wählen. Dies ist ein wichtiger Schritt, wenn ein vManage-Cluster vorhanden sein soll. Bitte wählen Sie die Persona, wie hier gezeigt Szenarien:

```
For a standalone vManage, choose the persona as COMPUTE_AND_DATA.
For a 3 node cluster, on 3 vManage nodes, the persona is set to COMPUTE_AND_DATA.
For a 6 node cluster, on 3 vManage nodes the persona is COMPUTE_AND_DATA and on rest 3 vManage nodes pe
```

Beispiel:Wählen Sie 1 für COMPUTE_AND_DATA



Wählen Sie die sekundäre Festplatte wie abgebildet aus:

```
2) DATA
3) COMPUTE
Select persona for vManage [1,2 or 3]: 1
You chose persona COMPUTE_AND_DATA (1)
Are you sure? [y/n] y
Available storage devices:
sdb     100GB
1) sdb
Select storage device to use: 1
Would you like to format sdb? (y/n): y
umount: /dev/sdb: not mounted.
mke2fs 1.45.7 (28-Jan-2021)
Discarding device blocks: done
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 5a94db1f-71c4-4e25-a6d1-8ef2495c1de2
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

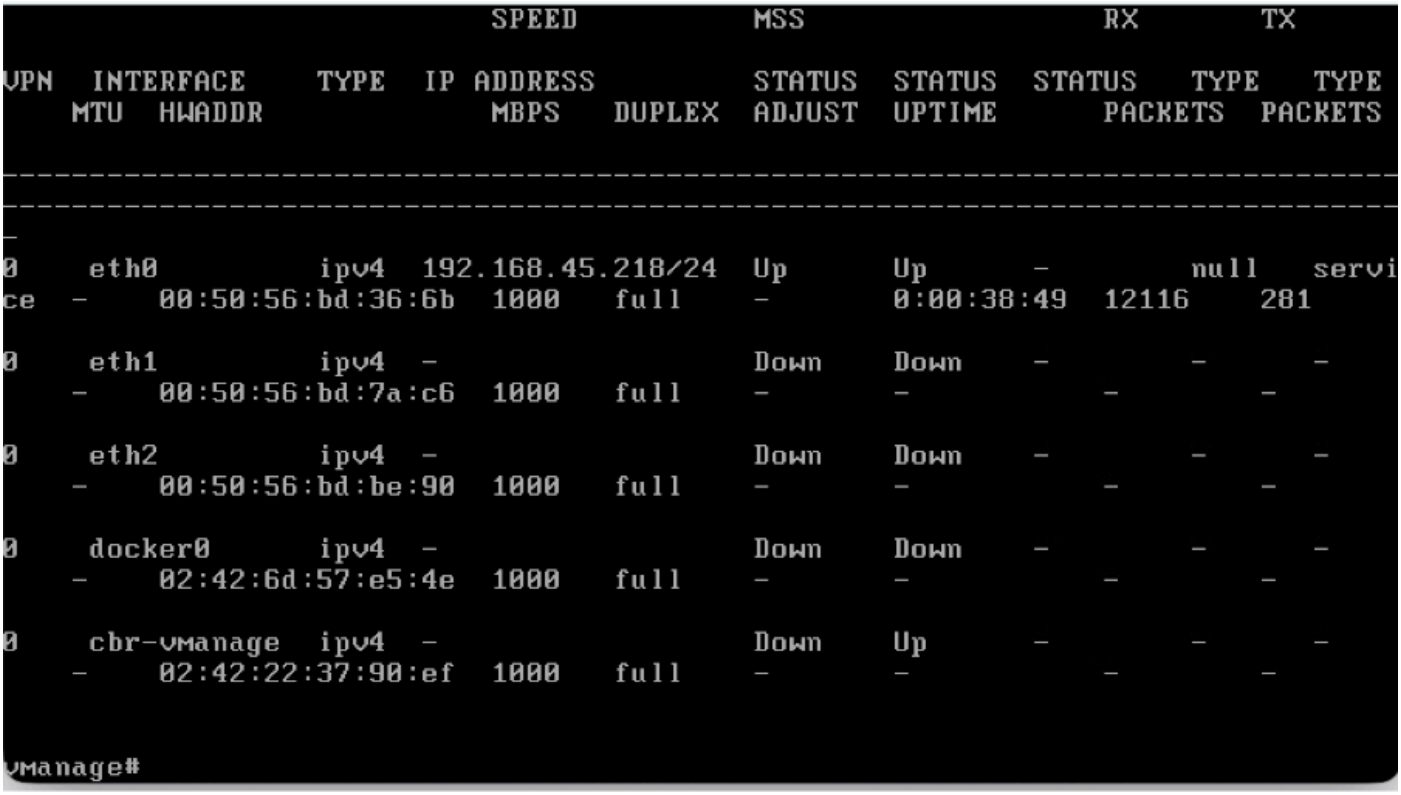
- Wählen Sie den sekundären Datenträger aus, und geben Sie zur Bestätigung Y ein.
- Cisco Manager wird neu geladen. Geben Sie nach dem Start den Benutzernamen und das Kennwort mit dem neuen Kennwort ein, das Sie neu konfiguriert haben.

```
early console in extract_kernel
input_data: 0x0000000021753b4
input_len: 0x000000000121c7f3
output: 0x0000000001000000
output_len: 0x000000000237ea6c
kernel_total_size: 0x0000000001fb0000
booted via startup_32()
Physical KASLR using RDRAND RDTSC...
Virtual KASLR using RDRAND RDTSC...

Decompressing Linux... Parsing ELF... Performing relocations... done.
Booting the kernel.

viptela 20.12.5.1

vmanage login:
viptela 20.12.5.1

vmanage login: admin
Password:
Last login: Wed Feb 18 10:52:47 UTC 2026 on tty0
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
vmanage#
```

- Sie können die VPN 512-Managementschnittstelle konfigurieren, um den Out-of-Band-Managementzugriff auf den Controller zu ermöglichen.
- Verwenden Sie den Befehl show interface. |, um die VPNs zu überprüfen, denen derzeit Schnittstellen zugeordnet sind.

- Konfigurieren Sie die Schnittstellen entsprechend.

Beispiel



```
                            SPEED          MSS                  RX       TX

VPN   INTERFACE    TYPE   IP ADDRESS        STATUS  STATUS  STATUS    TYPE    TYPE
    MTU  HWADDR             MBPS   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS

--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
_
0     eth0          ipv4  192.168.45.218/24  Up      Up      -         null    servi
ce  -     00:50:56:bd:36:6b  1000   full    -       0:00:38:49  12116     281

0     eth1          ipv4  -                 Down    Down    -         -       -
    -     00:50:56:bd:7a:c6  1000   full    -       -           -         -

0     eth2          ipv4  -                 Down    Down    -         -       -
    -     00:50:56:bd:be:90  1000   full    -       -           -         -

0     docker0       ipv4  -                 Down    Down    -         -       -
    -     02:42:6d:57:e5:4e  1000   full    -       -           -         -

0     cbr-vmanage   ipv4  -                 Down    Up      -         -       -
    -     02:42:22:37:90:ef  1000   full    -       -           -         -


vManage#
```

Anmerkung: Sie können die Konfiguration aus dem vorhandenen vManage-System heranziehen und das gleiche IP-Adressschema hier konfigurieren.

Konfigurationen der Management-Schnittstelle (VPN 512)

- Wenn eine Schnittstelle von VPN 0 auf VPN 512 verschoben werden muss, verwenden Sie diese Befehle, und konfigurieren Sie dann die IP-Adresse auf der Schnittstelle.

```
Conf t
vpn 0
 no interface eth0
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0
```

!

Validator aufrufen

- Konfigurieren Sie auf dem Hypervisor die erforderliche Rechenleistung (CPU, RAM und Festplatte) für den vBond-Knoten, und schalten Sie ihn ein.
- Sobald auf die Konsole zugegriffen werden kann, warten Sie, bis vBond vollständig gestartet ist. Warten Sie auf die Meldung System Ready (System bereit).
- Das System fordert Sie dann zur Eingabe von Benutzername und Kennwort auf. Geben Sie den Benutzernamen als admin und das Kennwort als admin ein. Anschließend fordert es den Benutzer auf, das Kennwort zu ändern. Legen Sie das Kennwort fest, das für den Benutzer admin benötigt wird.
- Sie können die VPN 512-Managementschnittstelle konfigurieren, um den Out-of-Band-Managementzugriff auf den Controller zu ermöglichen.
- Verwenden Sie den Befehl show interface. |, um die VPNs zu überprüfen, denen derzeit Schnittstellen zugeordnet sind.
- Konfigurieren Sie die Schnittstellen entsprechend.

Beispiel:

```
admin connected from 127.0.0.1 using console on vbond-01
vbond-01# sh int | tab

                                        IF      IF      IF
                                          TCP
               AF                       ADMIN   OPER    TRACKER  ENCAP
                         SPEED            MSS                  RX       TX
VPN  INTERFACE  TYPE  IP ADDRESS        STATUS  STATUS  STATUS   TYPE    PORT TYP
E  MTU  HWADDR             MBPS   DUPLEX  ADJUST  UPTIME      PACKETS  PACKETS
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
0    ge0/0      ipv4  10.106.51.184/24  Up      Up      -        null   transpor
t  -    00:50:56:bd:be:68  1000   full    -       0:04:39:15  1838     1843
0    ge0/1      ipv4  -                 Down    Down    -        -      -
   -    00:50:56:bd:04:8e  1000   full    -       -           -        -
0    ge0/2      ipv4  -                 Down    Down    -        -      -
   -    00:50:56:bd:f1:d5  1000   full    -       -           -        -
0    system     ipv4  1.1.1.4/32        Up      Up      -        null   loopback
   -    -                  1000   full    -       0:04:40:46  0        0
0    loopback1  ipv4  192.168.51.15/32  Up      Up      -        null   loopback
   -    -                  1000   full    -       0:04:39:18  0        0
512  eth0       ipv4  10.106.51.169/24  Up      Up      -        null   mgmt
   -    00:50:56:bd:3c:9b  1000   full    -       0:04:39:18  1839     1839

vbond-01#
```

Anmerkung: Verweisen Sie auf die Konfiguration des vorhandenen vBond, und konfigurieren Sie hier dieselben Konfigurationen.

Konfigurationen der Management-Schnittstelle (VPN 512)

- Wenn eine Schnittstelle von VPN 0 auf VPN 512 verschoben werden muss, verwenden Sie diese Befehle, und konfigurieren Sie dann die IP-Adresse auf der Schnittstelle.

```
Conf t
vpn 0
 no interface eth0
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0



!
commit
```

Aufrufen eines Controller-Knotens (vSmart)

- Führen Sie die gleichen Schritte wie beim Validator-Programm aus, um den vSmart-Knoten zu aktivieren.
- Nach der Konfiguration der VPN 512-IP-Adresse auf allen SD-WAN-Controllern können Sie über SSH auf die IP-Adresse des VPN 512 zugreifen.

CLI-Basiskonfiguration auf allen Controllern

Wenn Sie SSH-Zugriff auf alle Controller haben, konfigurieren Sie diese CLI-Konfigurationen auf jedem Controller.

Systemkonfiguration

```
config t
system
 host-name


 system-ip


 site-id


 organization-name


 vbond


commit
```

Hinweis: Wenn wir eine URL als vBond-Adresse verwenden, stellen Sie sicher, dass die IP-Adressen des DNS-Servers in der VPN 0-Konfiguration konfiguriert sind, oder dass sie aufgelöst werden können.

Konfiguration der Transportschnittstelle (VPN 0)

Diese Konfigurationen werden auf allen Controllern benötigt, damit die Transportschnittstelle Steuerverbindungen zu den Routern und den übrigen Controllern herstellen kann.

```
config t
vpn 0
 dns
```

```
        primary
 dns



         secondary
 interface eth1
  ip address



  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0



commit
```

Hinweis: Sie können die Konfigurationen Ihres vorhandenen Controllers heranziehen. Wenn die Konfiguration vorhanden ist, können Sie diese den neuen Controllern hinzufügen.

Konfigurieren Sie das Steuerungsprotokoll nur dann als TLS, wenn Router sichere Steuerverbindungen mit den vManage-Knoten mithilfe von TLS herstellen müssen. Standardmäßig stellen alle Controller und Router eine Steuerverbindung mithilfe von DTLS her. Dies ist eine optionale Konfiguration, die je nach Anforderung nur für vSmart- und vManage-Knoten erforderlich ist.

```
Conf t
security
 control
  protocol tls
Commit
```

Kombination 1: Standalone vManage + Kein DR

Erforderliche Instanzen:

- 1 vManage (COMPUTE_AND_DATA)
- 1 oder mehr vBond
- 1 oder mehr vSmart

Schritte:

1. Aufrufen aller Instanzen mithilfe der allgemeinen Schritte
2. Vorabprüfungen
3. Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller
4. Sicherung/Wiederherstellung der Konfig.-DB
5. Nachprüfungen

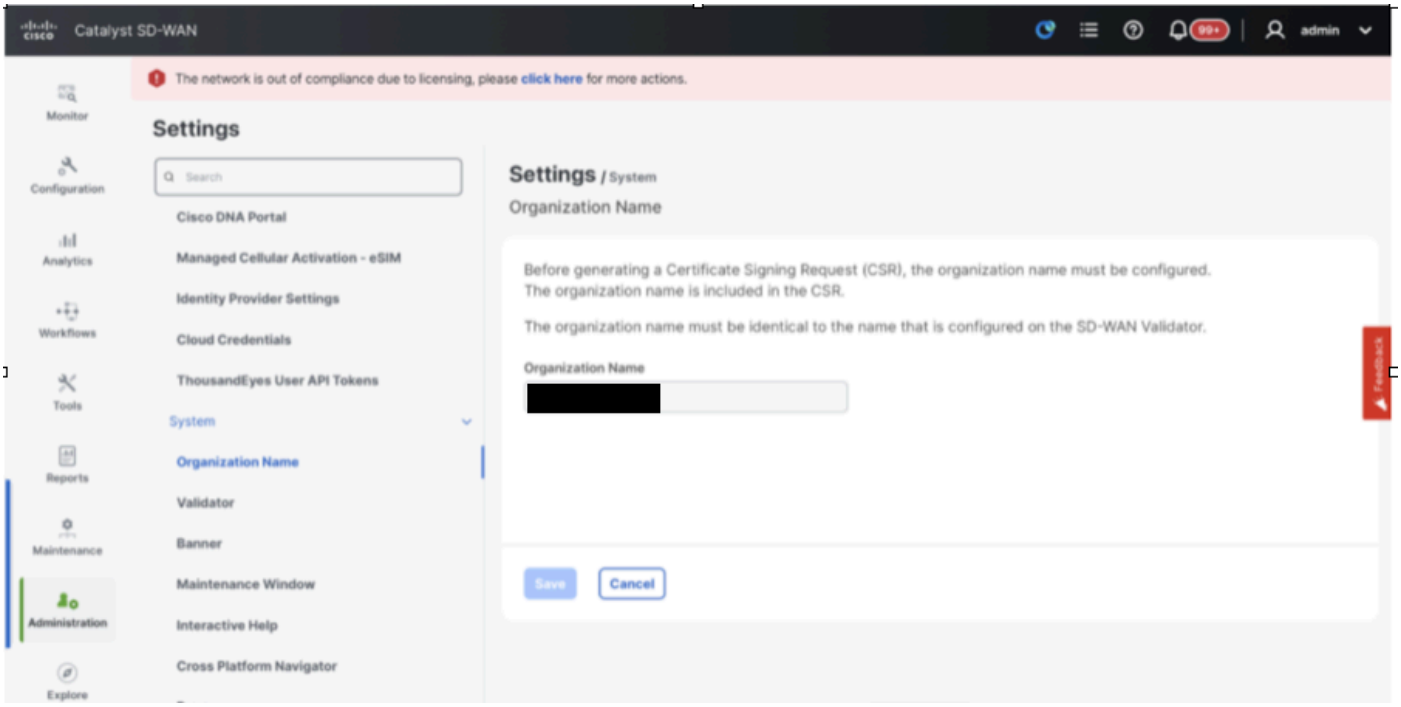
Schritt 1: Vorabprüfungen

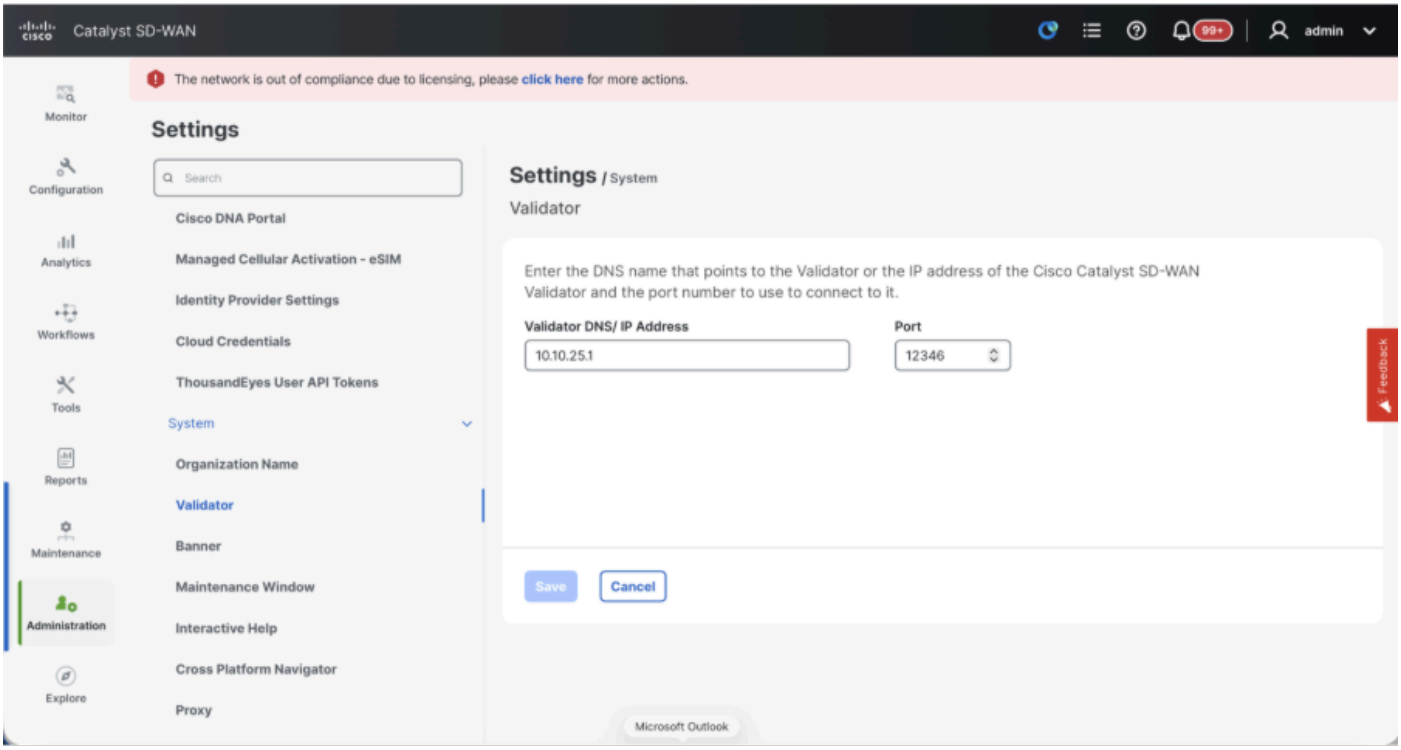
- Stellen Sie sicher, dass die Anzahl der aktiven Cisco SD-WAN Manager-Instanzen mit der Anzahl der neu installierten Cisco SD-WAN Manager-Instanzen identisch ist.
- Stellen Sie sicher, dass auf allen aktiven und neuen Cisco SD-WAN Manager-Instanzen dieselbe Softwareversion ausgeführt wird.
- Stellen Sie sicher, dass alle aktiven und neuen Cisco SD-WAN Manager-Instanzen die Management-IP-Adresse des Cisco SD-WAN Validators erreichen können.
- Stellen Sie sicher, dass die Zertifikate auf den neu installierten Cisco SD-WAN Manager-Instanzen installiert wurden.
- Stellen Sie sicher, dass die Uhren auf allen Cisco Catalyst SD-WAN-Geräten, einschließlich der neu installierten Cisco SD-WAN Manager-Instanzen, synchronisiert sind.
- Stellen Sie sicher, dass auf den neu installierten Cisco SD-WAN Manager-Instanzen ein neuer Satz von System-IPs und Standort-IDs konfiguriert und die gleiche grundlegende Konfiguration wie im aktiven Cluster verwendet wird.

Phase 2: Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller

Aktualisieren der Konfigurationen der vManage-Benutzeroberfläche

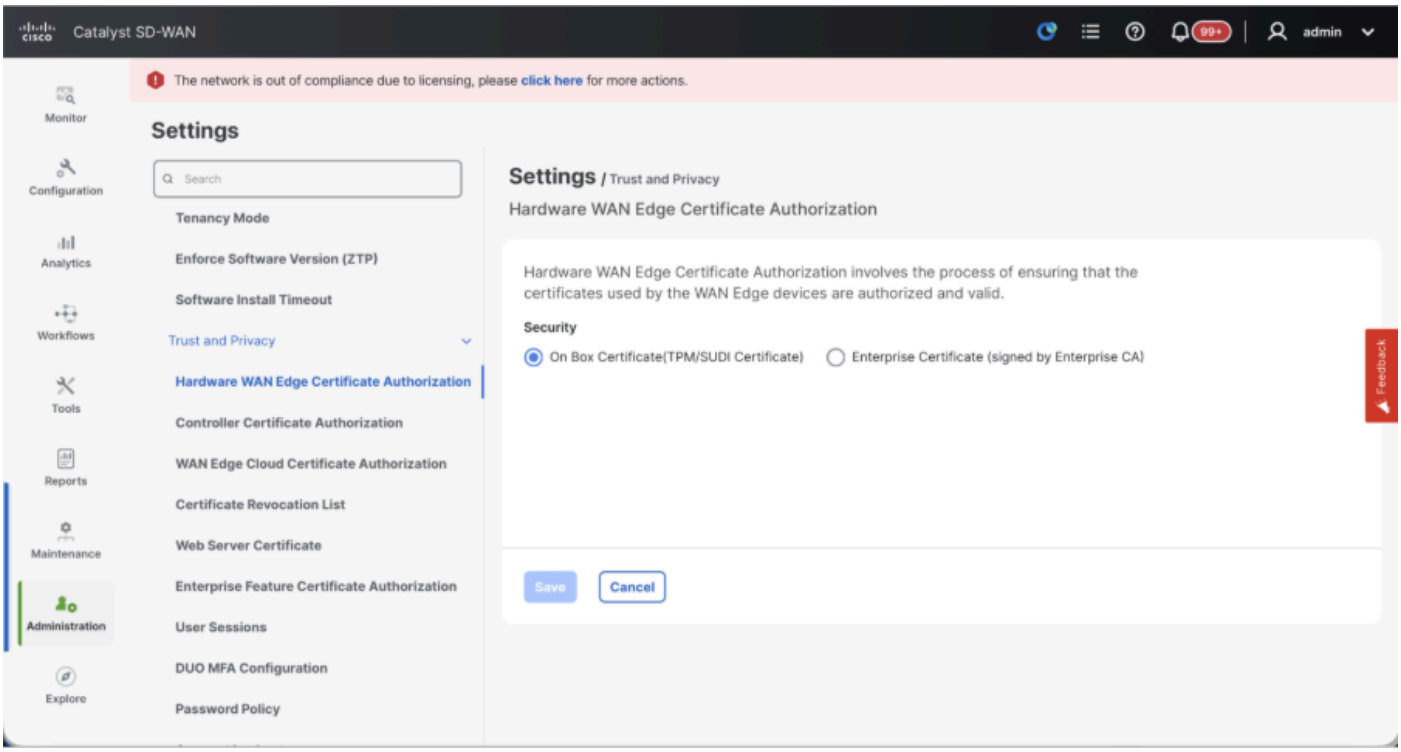
- Sobald die Konfigurationen in Schritt 1 in der CLI aller Controller hinzugefügt wurden, können wir über die URL https://<vmanage-ip> in Ihrem Browser auf die Web-UI von vManage zugreifen. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManage-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Administration > Settings, und führen Sie diese Schritte aus.
- Konfigurieren Sie den Organisationsnamen und die Validator-/vBond-URL/IP-Adresse. Konfigurieren Sie den gleichen Wert wie in der CLI des vManage-Knotens.
- In vManage 20.15/20.18 sind diese Konfigurationen im Abschnitt System verfügbar.



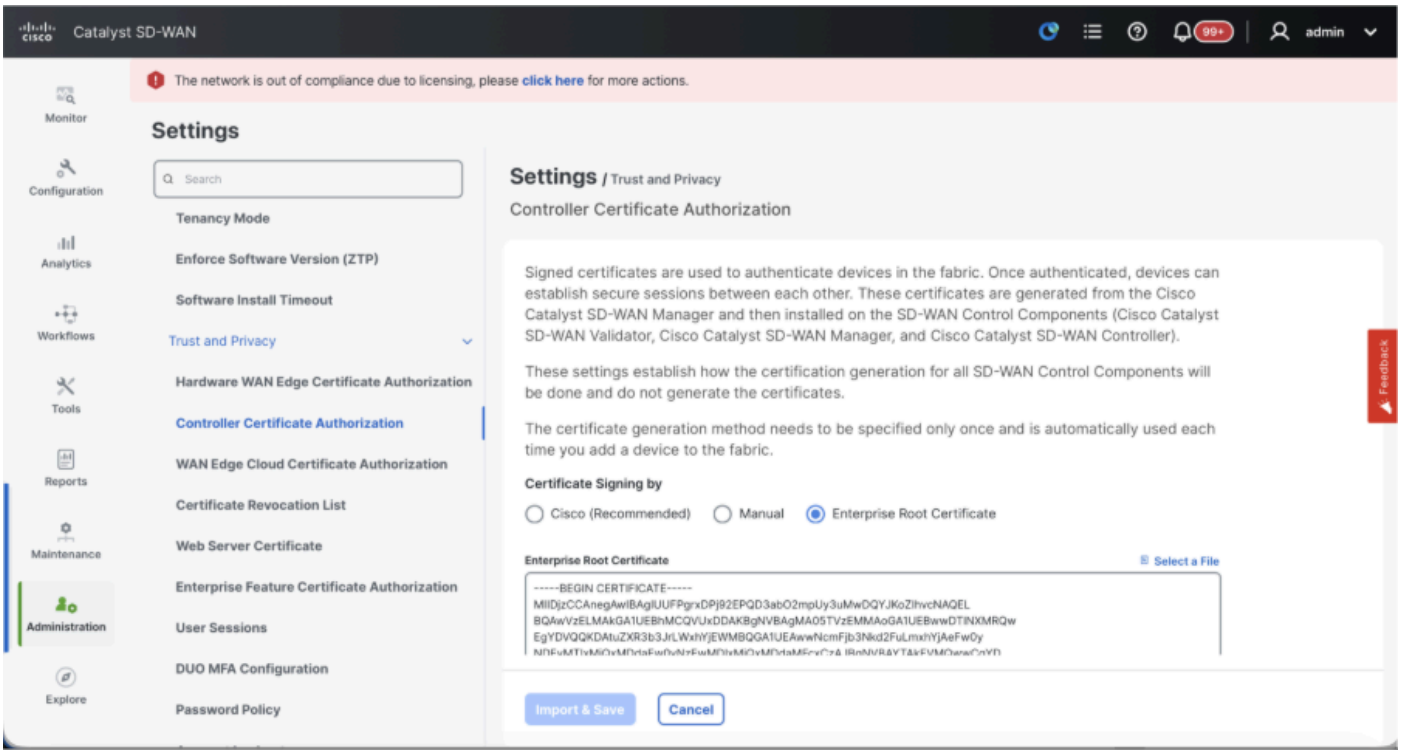


- Überprüfen Sie die Konfigurationen für die Zertifizierungsstelle (Certificate Authorization, CA), die die zum Signieren der Zertifikate verwendete Zertifizierungsstelle bestimmt. Hier sehen wir 3 Optionen:

1. Hardware WAN Edge Certificate Authorization (Hardware-WAN-Edge-Zertifikatsautorisierung): bestimmt die Zertifizierungsstelle für Hardware-SD-WAN-Edge-Router.
    - On Box Certificate (TPM/SUDI Certificate) - Mit dieser Option wird das vorinstallierte Zertifikat auf der Router-Hardware verwendet, um die Steuerverbindungen (TLS-/DTLS-Verbindungen) herzustellen.
    - Enterprise-Zertifikat (von der Enterprise-Zertifizierungsstelle signiert) - Bei dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

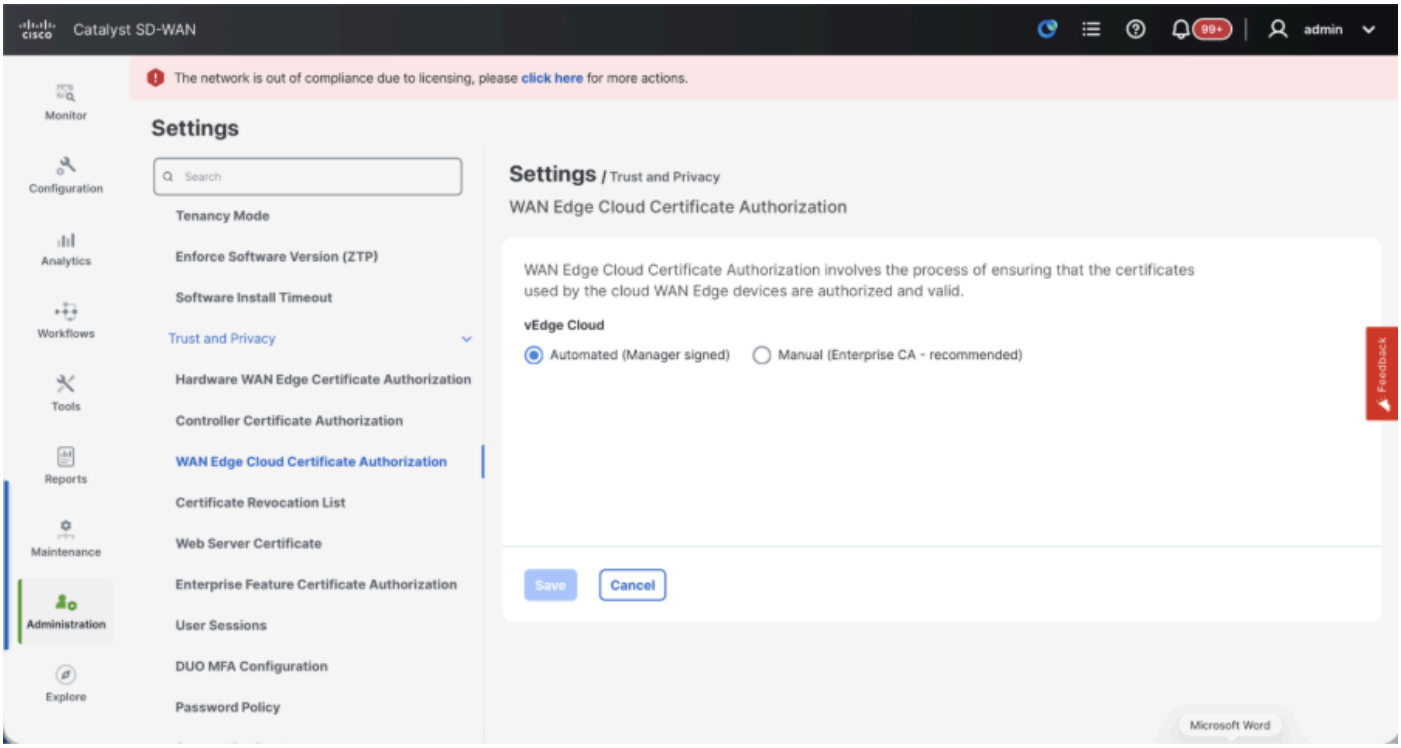


2. Controller Certificate Authorization (Controller-Zertifikatautorisierung): bestimmt die Zertifizierungsstelle für SD-WAN-Controller
    - Cisco (empfohlen) - Controller verwenden die von der Cisco PKI signierten Zertifikate. vManage kontaktiert das PNP-Portal automatisch mit den Smart Account-Anmeldedaten, die auf dem vManage konfiguriert sind. Das Zertifikat wird signiert und auf dem Controller installiert.
    - Manual (Manuell) - Controller verwenden die von der Cisco PKI signierten Zertifikate. Signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren.
    - Enterprise-Stammzertifikat - Mit dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

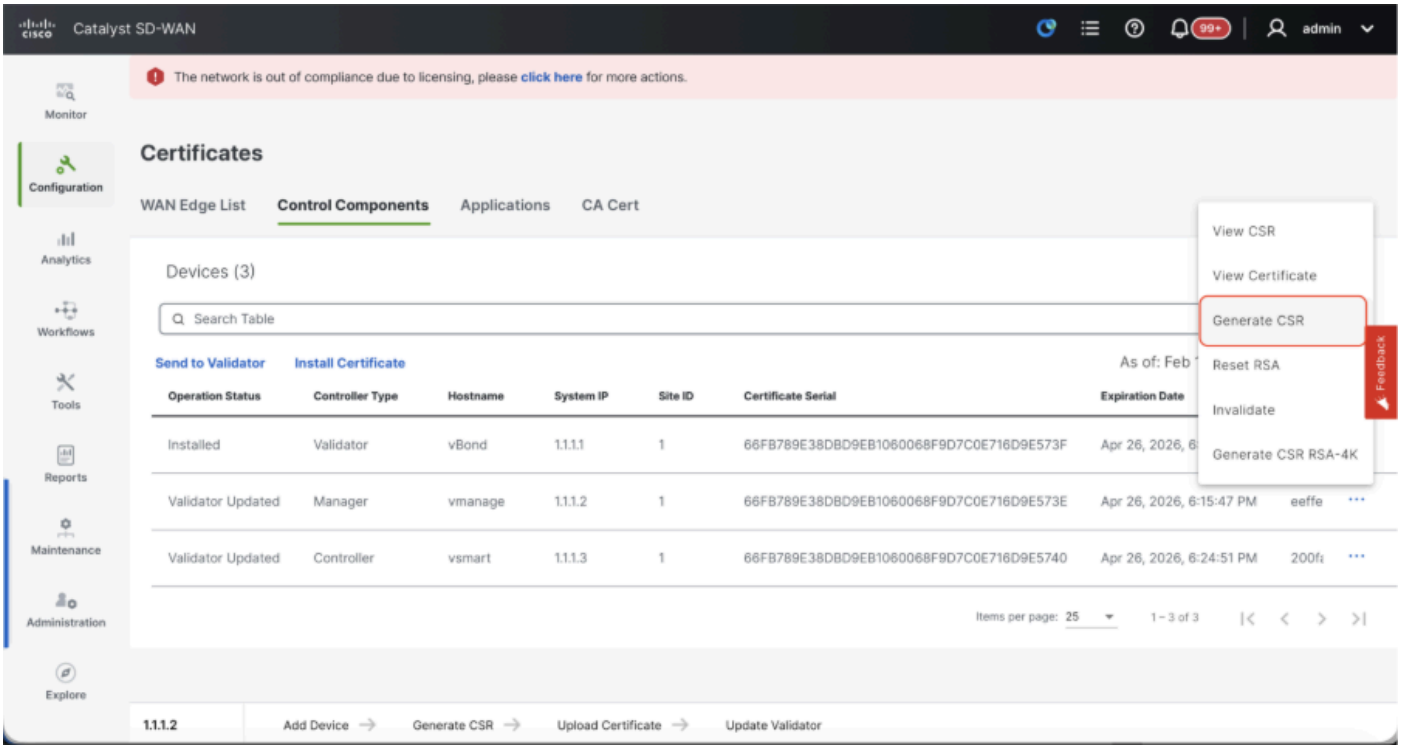


3. WAN-Edge-Cloud-Zertifikatautorisierung - bestimmt die Zertifizierungsstelle für virtuelle SD-WAN-Edge-Router (CSR1000v, C8000v, vEdge-Cloud)
    - Automated (vManage signiert) - vManage signiert automatisch den CSR für die virtuellen Edge-Router und installiert das Zertifikat auf dem Router.
    - Manuell (Enterprise CA - empfohlen) - Virtuelle Router verwenden Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

Wenn Sie eine eigene Zertifizierungsstelle (CA) oder eine Enterprise-Zertifizierungsstelle verwenden, wählen Sie Enterprise aus.



- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller
- Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

Integration von vBond/Validator und vSmart/Controller in vManage

Navigieren Sie zu Configuration > Devices > Control Components (Konfiguration > Geräte > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei Versionen 20.9/20.12: Konfiguration > Geräte > Controller

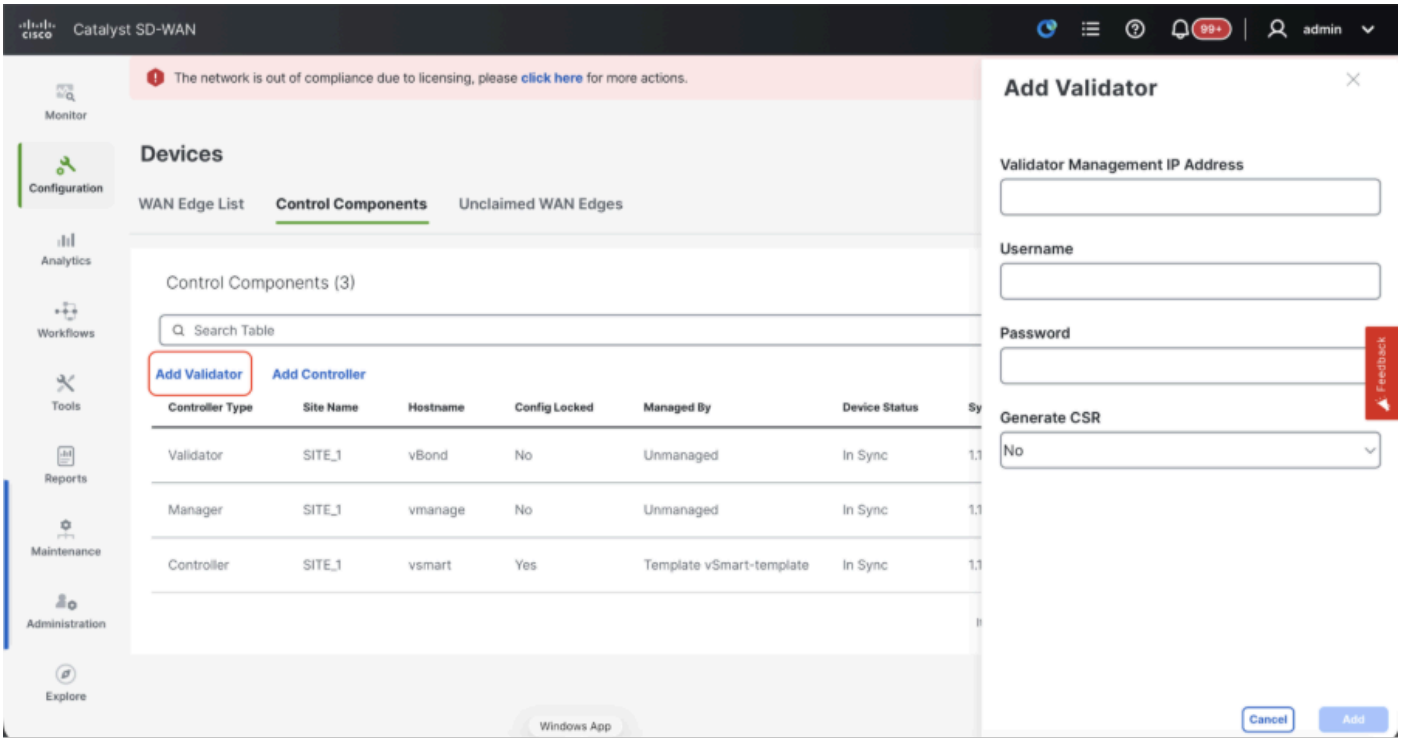
IntegrierenvBond/Validator

- Klicken Sie auf AdvBond.bei 20.12vManagerValidator hinzufügenim Fall von

20.15/20.18vManage. Ein Popup-Fenster wird geöffnet, und geben Sie den VPN 0-Transport-IP von vBond, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, falls dies über die CLI von vManagementvBondIP zulässig ist.
- Geben Sie die Anmeldeinformationen für den Benutzer von vBond ein.

Hinweis: Wir müssen Admin-Anmeldedaten von vBond oder einem Benutzerteil von netadmingroup verwenden. Dies können Sie in der CLI von vBond überprüfen. Wählen Sie im Dropdown-Menü "CSR generieren" die Option Ja, wenn ein neues Zertifikat für vBond installiert werden muss.

Anmerkung: Wenn sich vBond hinter einem NAT-Gerät bzw. einer NAT-Firewall befindet, überprüfen Sie, ob die IP-Adresse der vBond VPN 0-Schnittstelle in eine öffentliche IP-Adresse übersetzt wurde. Wenn die IP-Adresse der VPN 0-Schnittstelle von vManage aus nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der VPN 0-Schnittstelle.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vBond installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal.

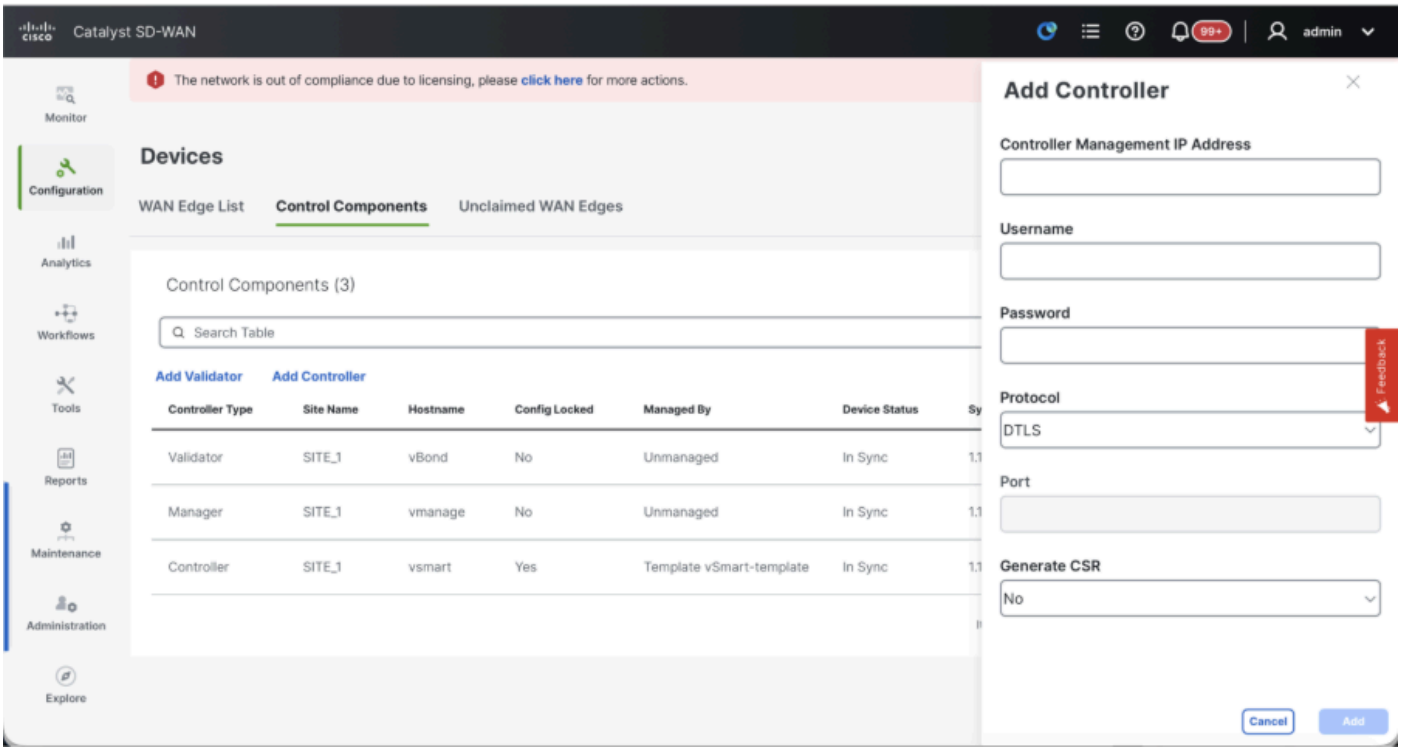
Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

- Wenn mehrere vBonds vorhanden sind, wiederholen Sie die gleichen Schritte.

Integration von vSmart/Controller

- Klicken Sie auf Add vSmart (vSmart hinzufügen), wenn es sich um 20.12 vManage handelt, oder auf Add Controller (Controller hinzufügen), wenn es sich um 20.15/20.18 vManage handelt.
- Geben Sie in einem Popup-Fenster die VPN 0-Transport-IP von vSmart ein, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, wenn dies von der CLI von vManage zu vSmart IP zulässig ist.
- Geben Sie die Benutzeranmeldeinformationen für vSmart Note ein, die von vSmart oder einem Benutzer der netadmin-Gruppe verwendet werden müssen.
- Sie können dies in der CLI des vSmart überprüfen.
- Legen Sie das Protokoll auf TLS fest, wenn TLS für Router verwendet werden soll, um Steuerverbindungen mit vSmart herzustellen. Diese Konfiguration muss auch für CLI von vSmarts- und vManage-Knoten konfiguriert werden.
- Wählen Sie im Dropdown-Menü "Generate CSR" (CSR generieren) die Option Yes (Ja) aus, wenn ein neues Zertifikat für vSmart installiert werden muss.

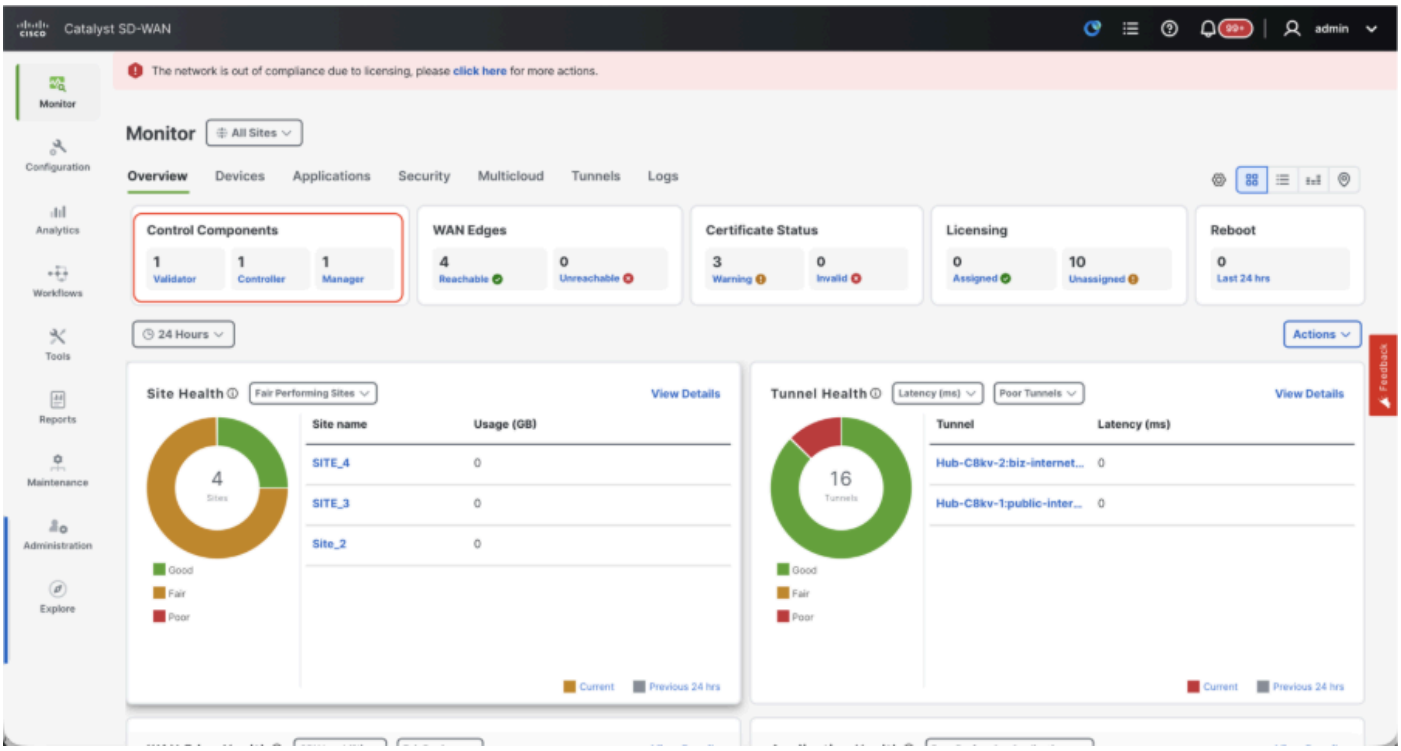
Hinweis: Wenn sich vSmart hinter dem NAT-Gerät/der Firewall befindet, prüfen Sie, ob die IP-Adresse der vSmart VPN 0-Schnittstelle in eine öffentliche IP übersetzt wurde. Wenn die IP-Adresse der VPN 0-Schnittstelle von vManage nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der IP-Adresse der VPN 0-Schnittstelle.



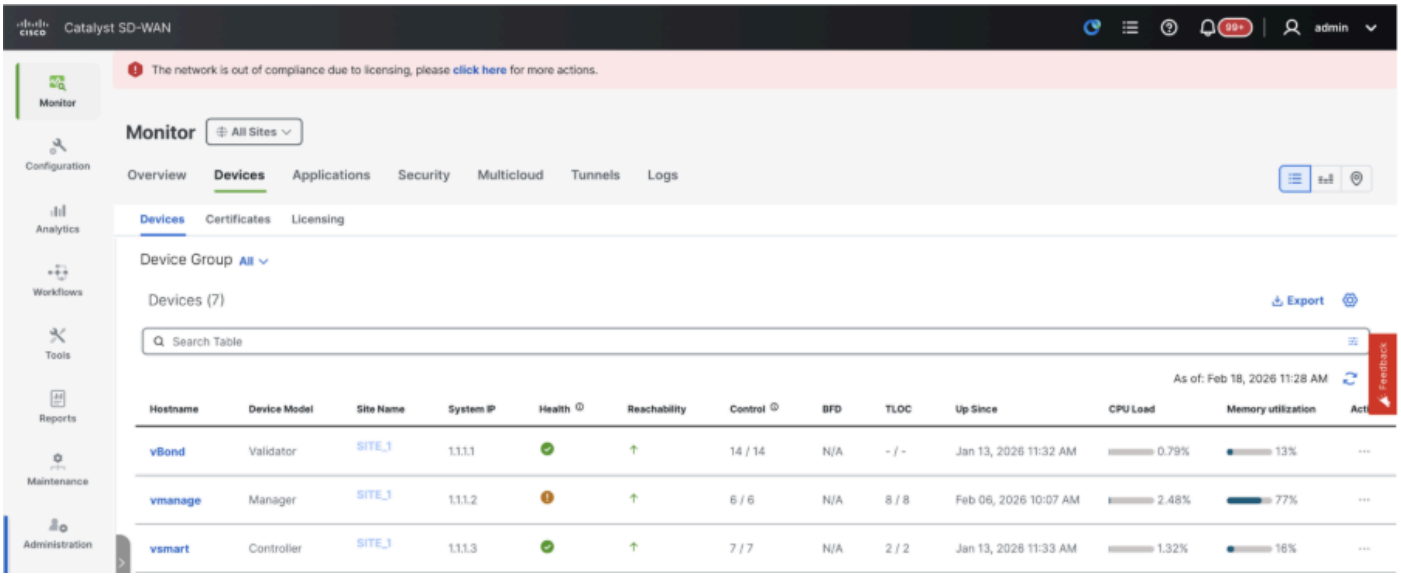
- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf dem vSmart installiert.
- Wenn Manual (Manuell) ausgewählt ist, signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren. Dasselbe Verfahren gilt für die Verwendung des Digicert- und Enterprise-Root-Zertifikats.
- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.
- Wenn mehrere vSmarts vorhanden sind, wiederholen Sie die gleichen Schritte.

Verifizierung

Überprüfen Sie nach Abschluss aller Schritte, ob alle Steuerungskomponenten unter Monitor>Dashboard erreichbar sind.



- Klicken Sie auf die jeweiligen Steuerungskomponenten, und vergewissern Sie sich, dass sie alle erreichbar sind.
- Navigieren Sie zu Überwachen > Geräte, und stellen Sie sicher, dass alle Steuerungskomponenten erreichbar sind.



Schritt 3: Sicherung/Wiederherstellung der Konfig.-DB

Sammeln von vManage-Konfigurations-DB-Backups und Wiederherstellen auf einem anderen vManage-Knoten

Sammeln der Konfiguration - DB-Backup:

- In der derzeit verwendeten SD-WAN-Fabric können Sie ein Konfigurations-DB-Backup

sowohl auf eigenständigen vManage- als auch auf vManage-Cluster-Konfigurationen erstellen.
- Bei eigenständigem vManage ist dieser vManager selbst der führende Anbieter von Konfigurationsdatenbanken.

Vergewissern Sie sich, dass configuration-db auf dem vManage-Knoten ausgeführt wird.

Sie können dies mit dem Befehl request nms configuration-db status onvManageCLI überprüfen. Die Ausgabe erfolgt wie dargestellt

```
vmanage# request nms configuration-db status
NMS configuration database
        Enabled: true
        Status: running PID:32632 for 1066085s
        Native metrics status: ENABLED
        Server-load metrics status: ENABLED
vmanage#
```

Verwenden Sie diesen Befehl, um das Backup configuration-db vom angegebenen Konfigurationsdb-Leader "vManage" zu erfassen.

```
request nms configuration-db backup path /opt/data/backup/
```

Die erwartete Ausgabe lautet wie folgt:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Notieren Sie sich die Anmeldeinformationen für die Konfigurationsdatenbank, wenn diese aktualisiert wurde.
- Wenn Sie die Anmeldeinformationen für die Konfigurationsdatenbank nicht kennen, wenden Sie sich an das TAC, um die Anmeldeinformationen für die Konfigurationsdatenbank von den vorhandenen vManage-Knoten abzurufen.

- Die Standardanmeldeinformationen für die -db-Konfiguration sind Benutzername: neo4j und Passwort: Kennwort

Wiederherstellen der Konfiguration - db-Sicherung auf einem anderen vManage-Knoten

Kopieren Sie das Sicherungsverzeichnis configuration-db mithilfe von SCP in das Verzeichnis /home/admin/ von vManage.

Beispielausgabe des Befehls scp:

```
XXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Zum Wiederherstellen des "configuration-db"-Backups müssen wir zunächst die "configuration-db"-Anmeldeinformationen konfigurieren. Wenn Ihre Anmeldeinformationen für configuration-db default(neo4j/password) sind, können wir diesen Schritt überspringen.

Um die Anmeldeinformationen für configuration-db zu konfigurieren, verwenden Sie den Befehl request nms configuration-db update-admin-user. Verwenden Sie den Benutzernamen und das Kennwort Ihrer Wahl.

Bitte beachten Sie, dass der Anwendungsserver von vManage neu gestartet wurde. Aufgrund dessen kann auf die vManage-Benutzeroberfläche für kurze Zeit nicht mehr zugegriffen werden.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operati
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Nach dem wir fortfahren können, die Konfiguration-db-Backup wiederherzustellen:

Wir können den Befehl request nms configuration-db restore path /home/admin/< > verwenden, um configuration-db auf dem neuen vManage wiederherzustellen:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Reseting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Sobald die Konfigurationsdatenbank wiederhergestellt ist, stellen Sie sicher, dass auf die vManage-Benutzeroberfläche zugegriffen werden kann. Warten Sie etwa 5 Minuten, und versuchen Sie dann, auf die Benutzeroberfläche zuzugreifen.

Nachdem Sie sich erfolgreich bei der Benutzeroberfläche angemeldet haben, stellen Sie sicher, dass die Liste der Edge-Router, die Vorlage, die Richtlinien und alle anderen Konfigurationen, die auf der vorherigen oder vorhandenen vManage-Benutzeroberfläche vorhanden waren, auf der neuen vManage-Benutzeroberfläche wiedergegeben werden.

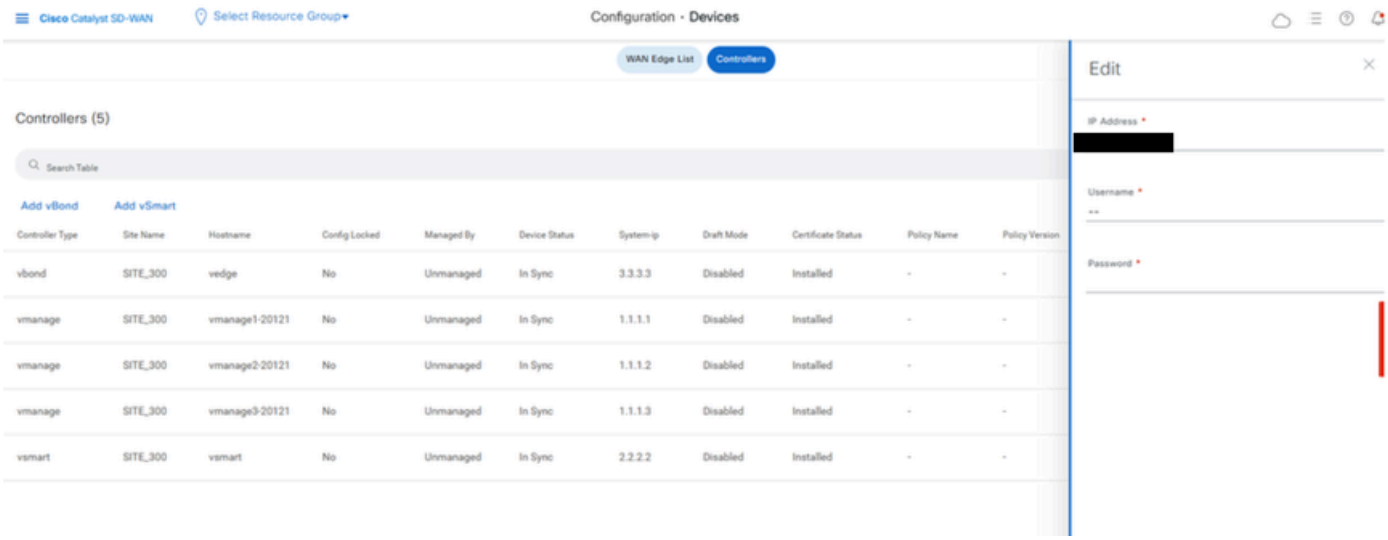
Schritt 4: Neuauthentifizierung von Controllern und Ungültigerklärung alter Controller

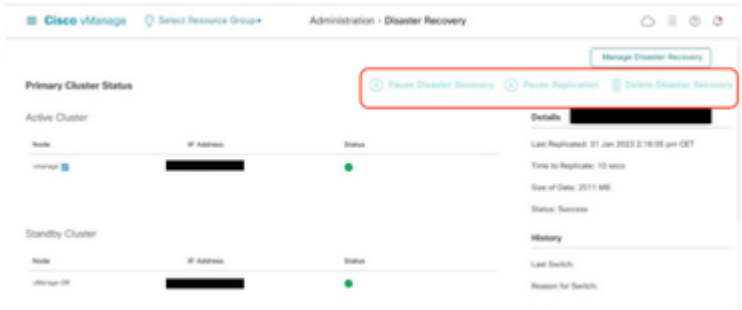
Nach der Wiederherstellung von configuration-db müssen alle neuen Controller (vmanage/vsmart/vbond) in der Fabric erneut authentifiziert werden.

Hinweis: Wenn in der Produktion die zur erneuten Authentifizierung verwendete Schnittstellen-IP die Tunnel-Schnittstellen-IP ist, müssen Sie sicherstellen, dass der NETCONF-Dienst auf der Tunnelschnittstelle von vManage, vSmart und vBond sowie auf den Firewalls entlang des Pfads zugelassen ist. Der zu öffnende Firewall-Port ist der TCP-Port 830 als bidirektionale Regel vom DR-Cluster zu allen vBonds und vSmarts.

Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.

- Klicken Sie auf die drei Punkte in der Nähe der einzelnen Controller, und klicken Sie dann auf Bearbeiten.





- Ersetzen Sie die IP-Adresse (System-IP des Controllers) durch die IP-Adresse des Transport-VPNs 0 (Tunnelschnittstelle). Geben Sie Benutzername und Kennwort ein, und klicken Sie auf "Speichern".
- Gleiches für alle neuen Controller im Fabric tun

Synchronisieren der Root-Zertifikatskette

Führen Sie diesen Schritt aus, nachdem alle Controller integriert wurden:

Führen Sie auf einem Cisco SD-WAN Manager-Server im neu aktiven Cluster die folgenden Aktionen aus:

Geben Sie diesen Befehl ein, um das Root-Zertifikat mit allen Cisco Catalyst SD-WAN-Geräten im neu aktiven Cluster zu synchronisieren:

https://vmanage-url/dataservice/system/device/sync/rootcertchain

Geben Sie diesen Befehl ein, um die UUID des Cisco SD-WAN-Managers mit dem Cisco SD-WAN Validator zu synchronisieren:

https://vmanage-url/dataservice/certificate/syncvbond

Sobald die Fabric wiederhergestellt ist und die Steuerungs- und BFD-Sitzungen für alle Edges und Controller in der Fabric verfügbar sind, müssen die alten Controller (vmanage/vsmart/vbond) in der Benutzeroberfläche ungültig gemacht werden.

- Klicken Sie in der verwalteten Benutzeroberfläche auf Configuration > Certificates > Controllers.
- Auf Controller klicken
- Klicken Sie auf die drei Punkte auf der rechten Seite des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Ungültig
- Klicken Sie auf Senden,
- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.
- Klicken Sie auf die drei Punkte auf der rechten Seite des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Löschen

Schritt 5: Nachprüfungen

Anmerkung: Fahren Sie mit dem hier abgebildeten Abschnitt "Nachprüfungen" fort, der für alle Bereitstellungskombinationen gilt.

Kombination 2: Standalone vManage + Single Node DR

Erforderliche Instanzen:

- 1 vManage (primär, COMPUTE_AND_DATA)
- 1 vManage (DR-Standby, COMPUTE_AND_DATA)
- 1 oder mehr vBond
- 1 oder mehr vSmart

Schritte:

1. Aufrufen aller Instanzen mithilfe der allgemeinen Schritte
2. Vorabprüfungen
3. Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller
4. DR-Einrichtung für einen Knoten
5. Sicherung/Wiederherstellung der Konfig.-DB
6. Nachprüfungen

Schritt 1: Vorabprüfungen

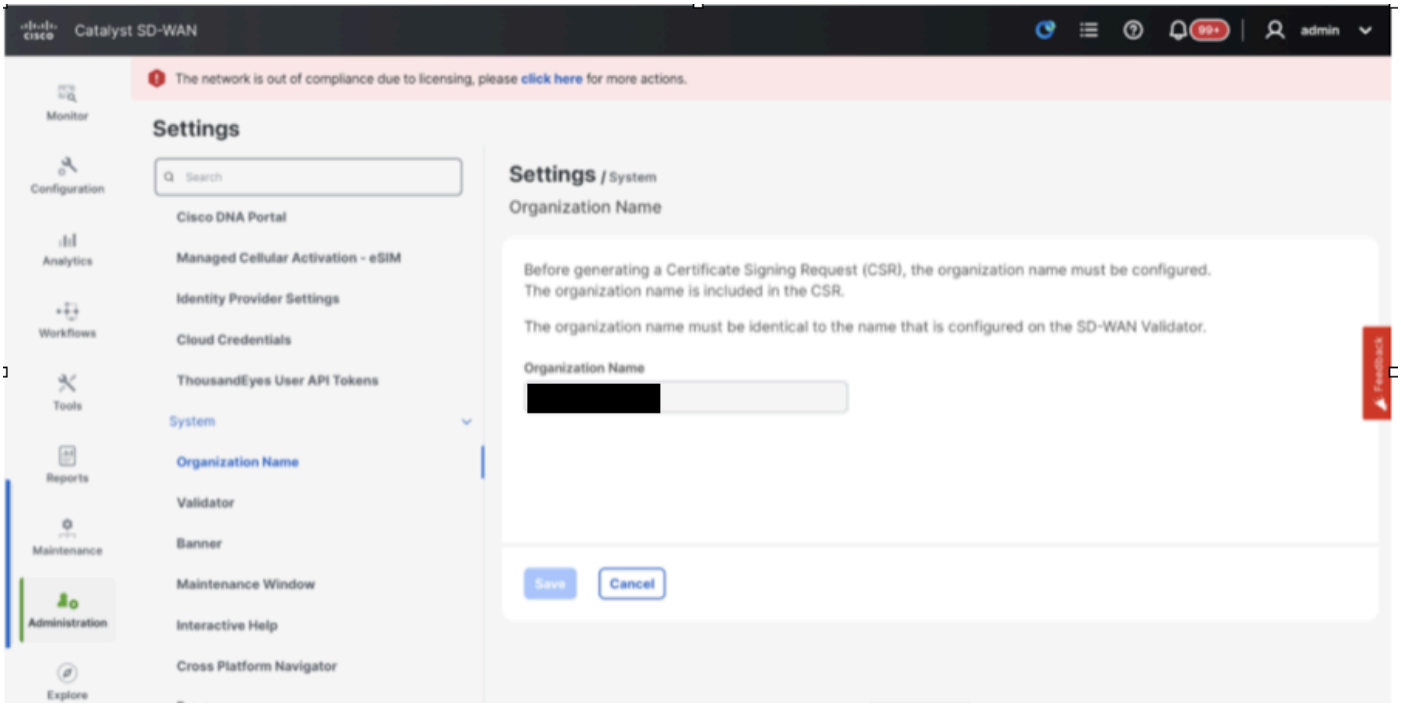
- Stellen Sie sicher, dass die Anzahl der aktiven Cisco SD-WAN Manager-Instanzen mit der Anzahl der neu installierten Cisco SD-WAN Manager-Instanzen identisch ist.
- Stellen Sie sicher, dass auf allen aktiven und neuen Cisco SD-WAN Manager-Instanzen dieselbe Softwareversion ausgeführt wird.
- Stellen Sie sicher, dass alle aktiven und neuen Cisco SD-WAN Manager-Instanzen die Management-IP-Adresse des Cisco SD-WAN Validators erreichen können.

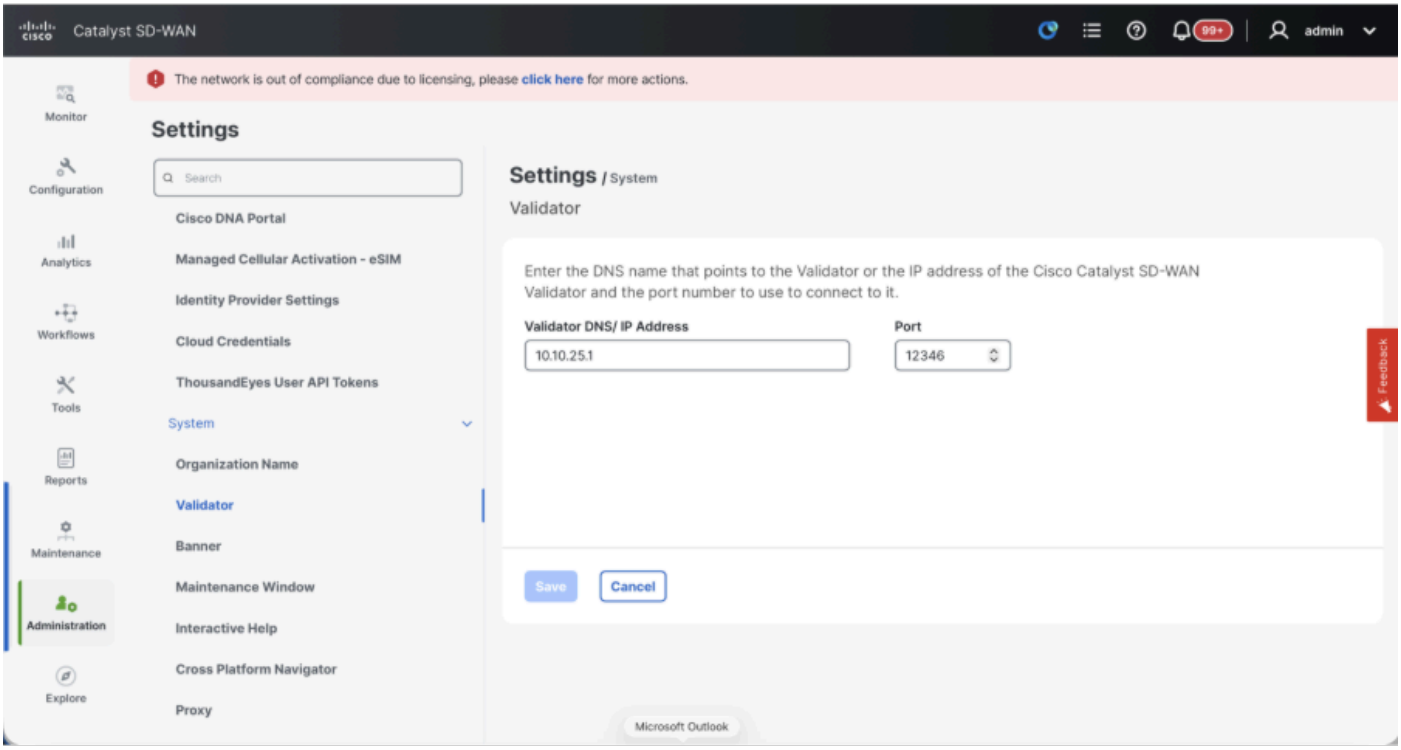
- Stellen Sie sicher, dass die Zertifikate auf den neu installierten Cisco SD-WAN Manager-Instanzen installiert wurden.
- Stellen Sie sicher, dass die Uhren auf allen Cisco Catalyst SD-WAN-Geräten, einschließlich der neu installierten Cisco SD-WAN Manager-Instanzen, synchronisiert sind.
- Stellen Sie sicher, dass auf den neu installierten Cisco SD-WAN Manager-Instanzen ein neuer Satz von System-IPs und Standort-IDs konfiguriert und die gleiche grundlegende Konfiguration wie im aktiven Cluster verwendet wird.

Phase 2: Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller

Aktualisieren der Konfigurationen der vManage-Benutzeroberfläche

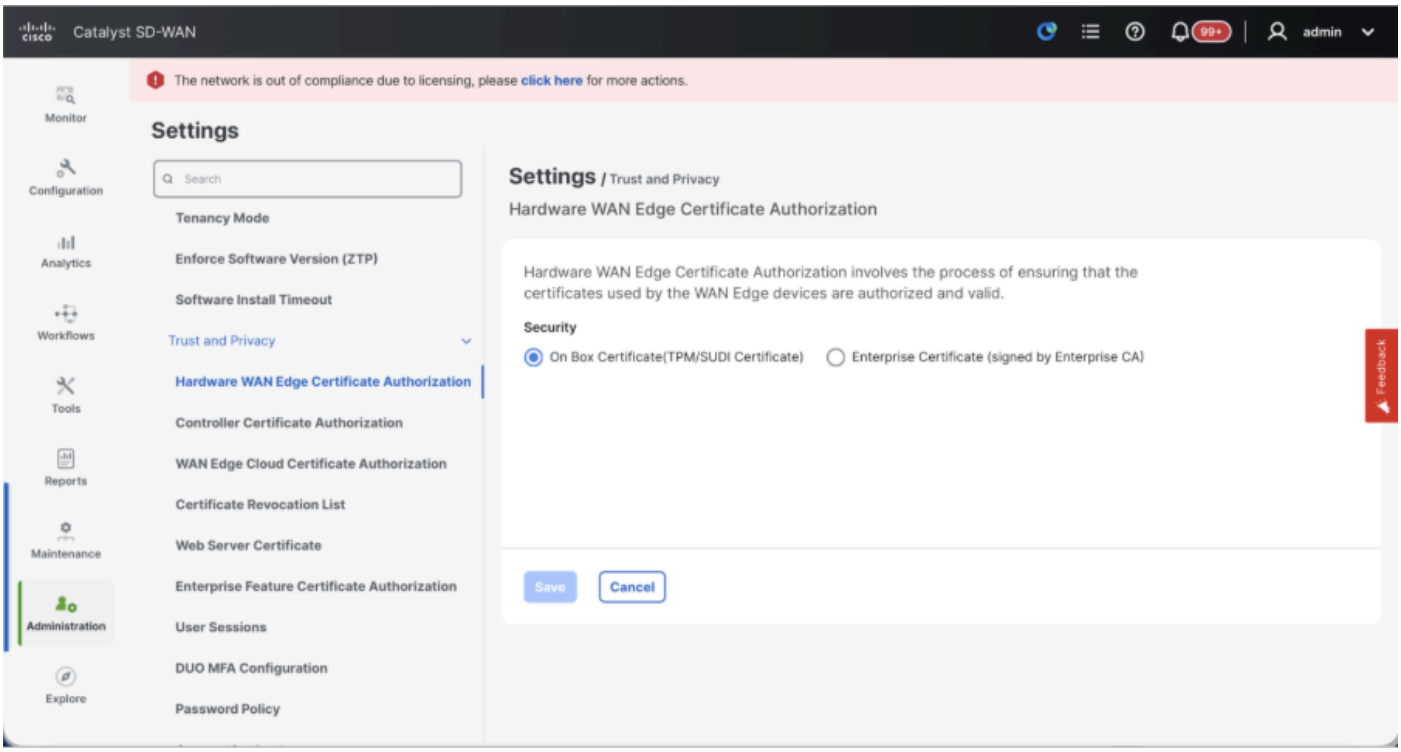
- Sobald die Konfigurationen in Schritt 1 in der CLI aller Controller hinzugefügt wurden, können wir über die URL https://<vmanage-ip> in Ihrem Browser auf die Web-UI von vManage zugreifen. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManage-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Administration > Settings, und führen Sie diese Schritte aus.
- Konfigurieren Sie den Organisationsnamen und die Validator-/vBond-URL/IP-Adresse. Konfigurieren Sie den gleichen Wert wie in der CLI des vManage-Knotens.
- In vManage 20.15/20.18 sind diese Konfigurationen im Abschnitt System verfügbar.



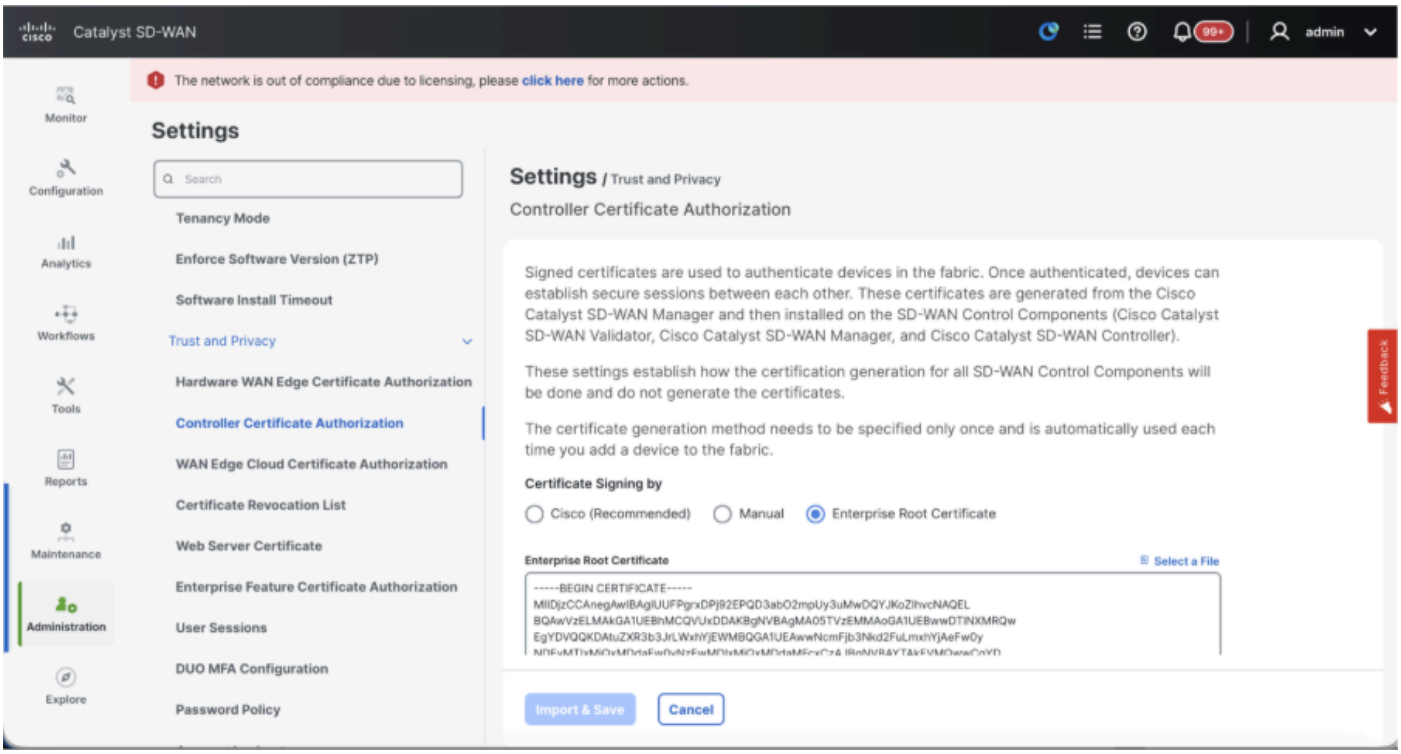


- Überprüfen Sie die Konfigurationen für die Zertifizierungsstelle (Certificate Authorization, CA), die die zum Signieren der Zertifikate verwendete Zertifizierungsstelle bestimmt. Hier sehen wir 3 Optionen:

1. Hardware WAN Edge Certificate Authorization (Hardware-WAN-Edge-Zertifikatsautorisierung): bestimmt die Zertifizierungsstelle für Hardware-SD-WAN-Edge-Router.
    - On Box Certificate (TPM/SUDI Certificate) - Mit dieser Option wird das vorinstallierte Zertifikat auf der Router-Hardware verwendet, um die Steuerverbindungen (TLS-/DTLS-Verbindungen) herzustellen.
    - Enterprise-Zertifikat (von der Enterprise-Zertifizierungsstelle signiert) - Bei dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

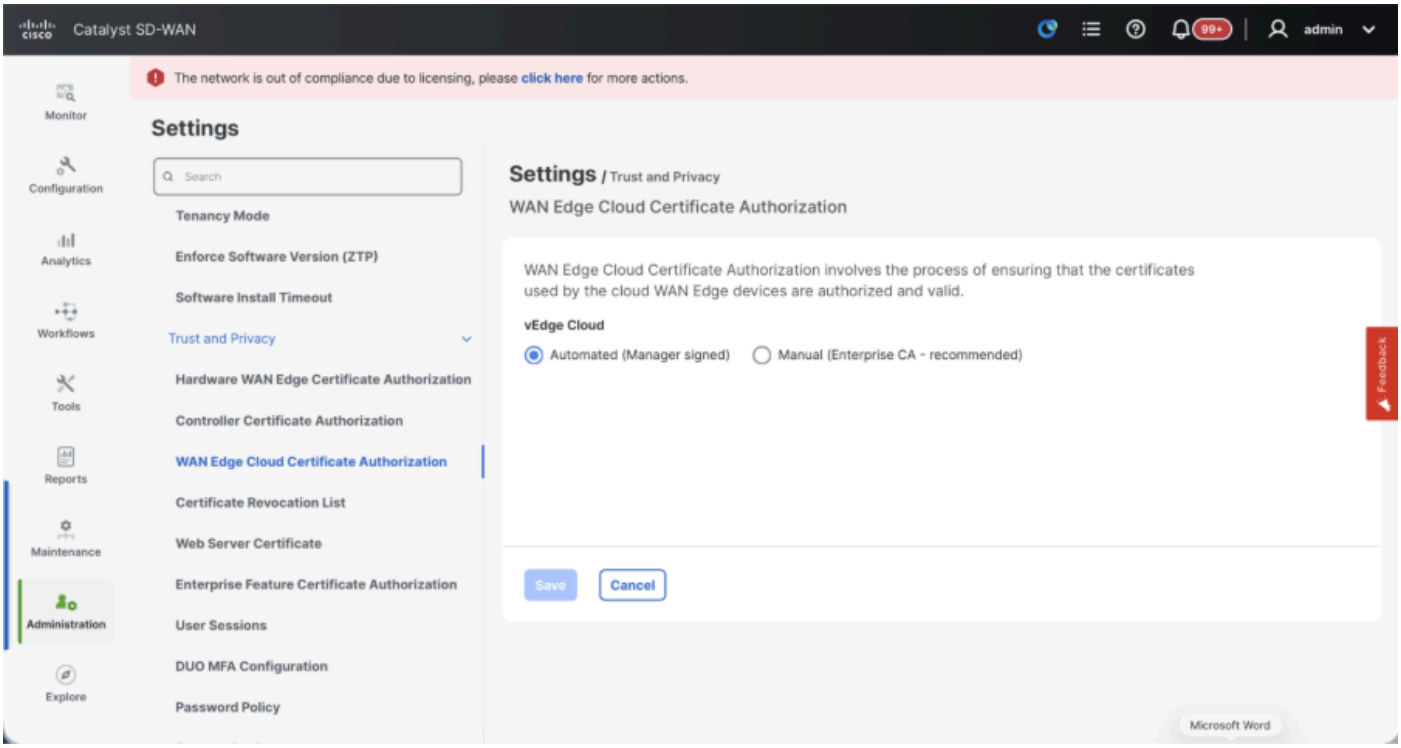


2. Controller Certificate Authorization (Controller-Zertifikatautorisierung): bestimmt die Zertifizierungsstelle für SD-WAN-Controller
    - Cisco (empfohlen) - Controller verwenden die von der Cisco PKI signierten Zertifikate. vManage kontaktiert das PNP-Portal automatisch mit den Smart Account-Anmeldedaten, die auf dem vManage konfiguriert sind. Das Zertifikat wird signiert und auf dem Controller installiert.
    - Manual (Manuell) - Controller verwenden die von der Cisco PKI signierten Zertifikate. Signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren.
    - Enterprise-Stammzertifikat - Mit dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

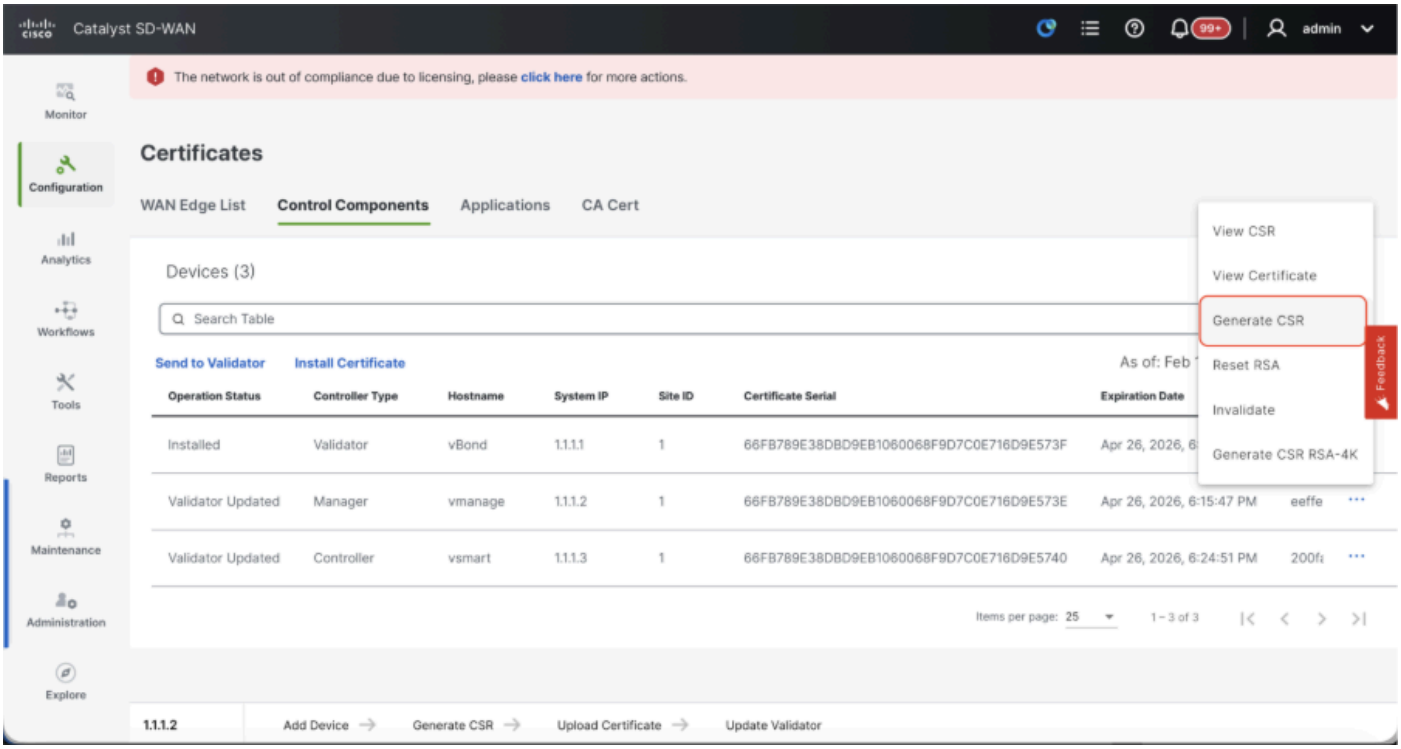


3. WAN-Edge-Cloud-Zertifikatautorisierung - bestimmt die Zertifizierungsstelle für virtuelle SD-WAN-Edge-Router (CSR1000v, C8000v, vEdge-Cloud)
    - Automated (vManage signiert) - vManage signiert automatisch den CSR für die virtuellen Edge-Router und installiert das Zertifikat auf dem Router.
    - Manuell (Enterprise CA - empfohlen) - Virtuelle Router verwenden Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

Wenn Sie eine eigene Zertifizierungsstelle (CA) oder eine Enterprise-Zertifizierungsstelle verwenden, wählen Sie Enterprise aus.



- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller
- Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

Integration von vBond/Validator und vSmart/Controller in vManage

Navigieren Sie zu Configuration > Devices > Control Components (Konfiguration > Geräte > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

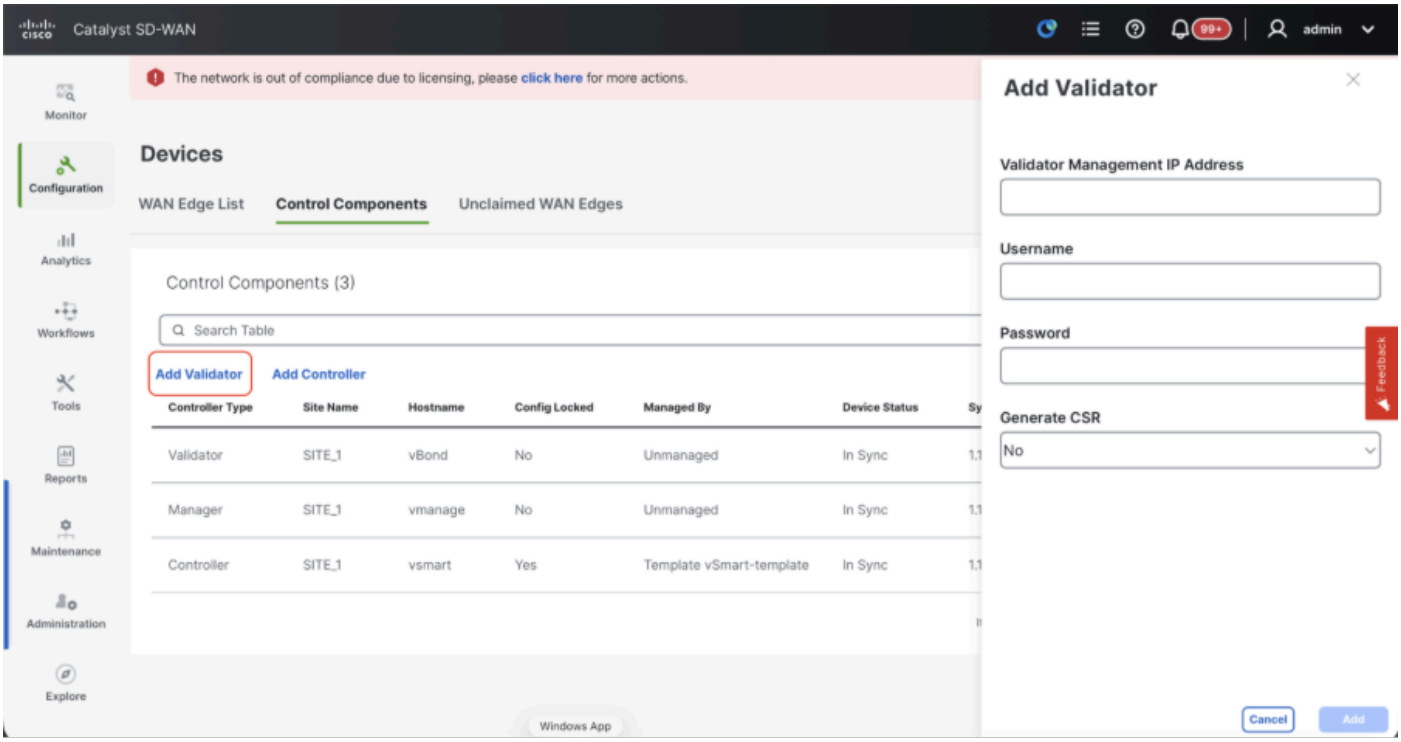
IntegrierenvBond/Validator

- Klicken Sie auf AdvBond.bei 20.12vManagerValidator hinzufügenim Fall von

20.15/20.18vManage. Ein Popup-Fenster wird geöffnet, und geben Sie den VPN 0-Transport-IP von vBond, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, falls dies über die CLI von vManagementvBondIP zulässig ist.
- Geben Sie die Anmeldeinformationen für den Benutzer von vBond ein.

Hinweis: Wir müssen Admin-Anmeldedaten von vBond oder einem Benutzerteil von netadmingroup verwenden. Dies können Sie in der CLI von vBond überprüfen. Wählen Sie im Dropdown-Menü "CSR generieren" die Option "Ja", wenn ein neues Zertifikat für vBond installiert werden soll.

Anmerkung: Wenn sich vBond hinter einem NAT-Gerät bzw. einer NAT-Firewall befindet, überprüfen Sie, ob die IP-Adresse der vBond VPN 0-Schnittstelle in eine öffentliche IP-Adresse übersetzt wurde. Wenn die VPN 0-Schnittstellen-IP von vManage aus nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der VPN 0-Schnittstelle.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vBond installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal.

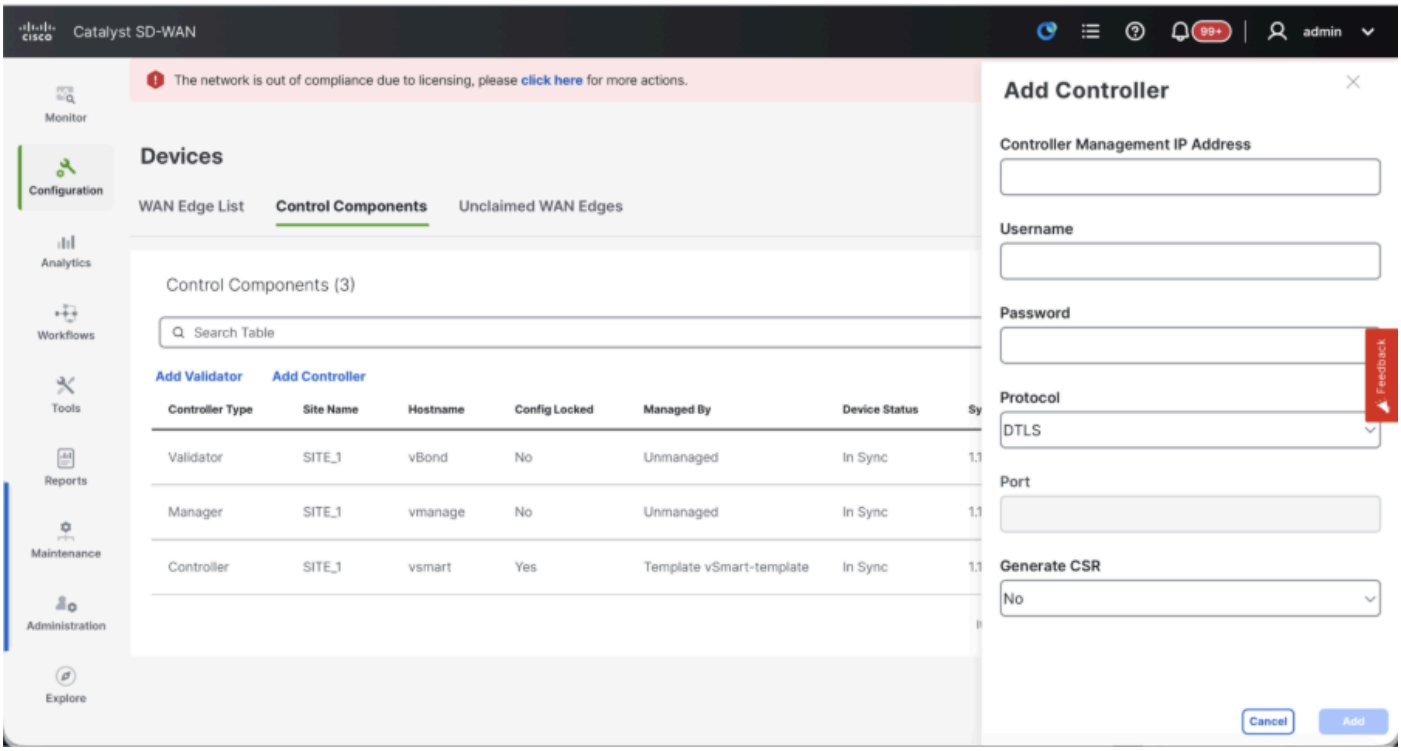
Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

- Wenn mehrere vBonds vorhanden sind, wiederholen Sie die gleichen Schritte.

Integration von vSmart/Controller

- Klicken Sie auf Add vSmart (vSmart hinzufügen), wenn es sich um 20.12 vManage handelt, oder auf Add Controller (Controller hinzufügen), wenn es sich um 20.15/20.18 vManage handelt.
- Geben Sie in einem Popup-Fenster die VPN 0-Transport-IP von vSmart ein, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, wenn dies von der CLI von vManage zu vSmart IP zulässig ist.
- Geben Sie die Benutzeranmeldeinformationen für vSmart Note ein, die von vSmart oder einem Benutzer der netadmin-Gruppe verwendet werden müssen.
- Sie können dies in der CLI des vSmart überprüfen.
- Legen Sie das Protokoll auf TLS fest, wenn TLS für Router verwendet werden soll, um Steuerverbindungen mit vSmart herzustellen. Diese Konfiguration muss auch für CLI von vSmarts- und vManage-Knoten konfiguriert werden.
- Wählen Sie im Dropdown-Menü "Generate CSR" (CSR generieren) die Option Yes (Ja) aus, wenn ein neues Zertifikat für vSmart installiert werden muss.

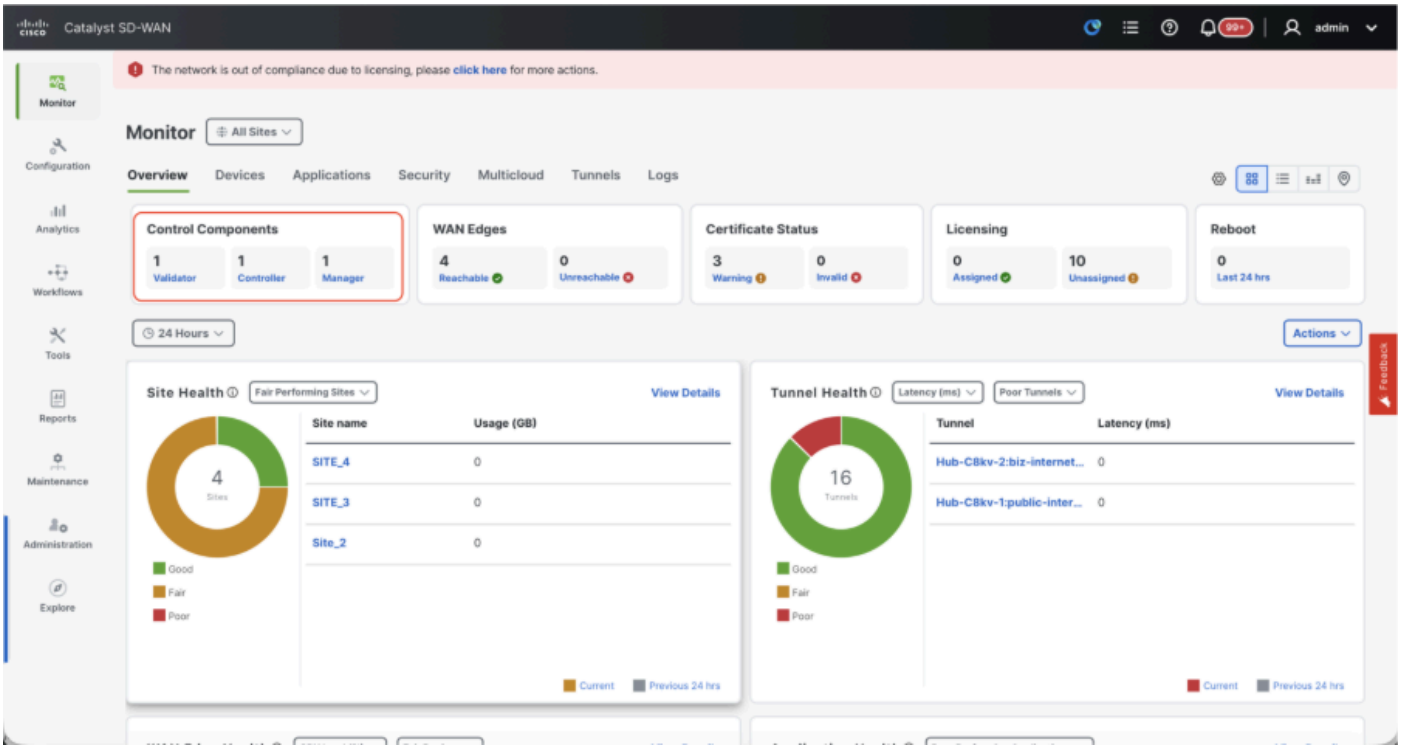
Hinweis: Wenn sich vSmart hinter dem NAT-Gerät/der Firewall befindet, prüfen Sie, ob die IP-Adresse der vSmart VPN 0-Schnittstelle in eine öffentliche IP übersetzt wurde. Wenn die IP-Adresse der VPN 0-Schnittstelle von vManage nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der IP-Adresse der VPN 0-Schnittstelle.



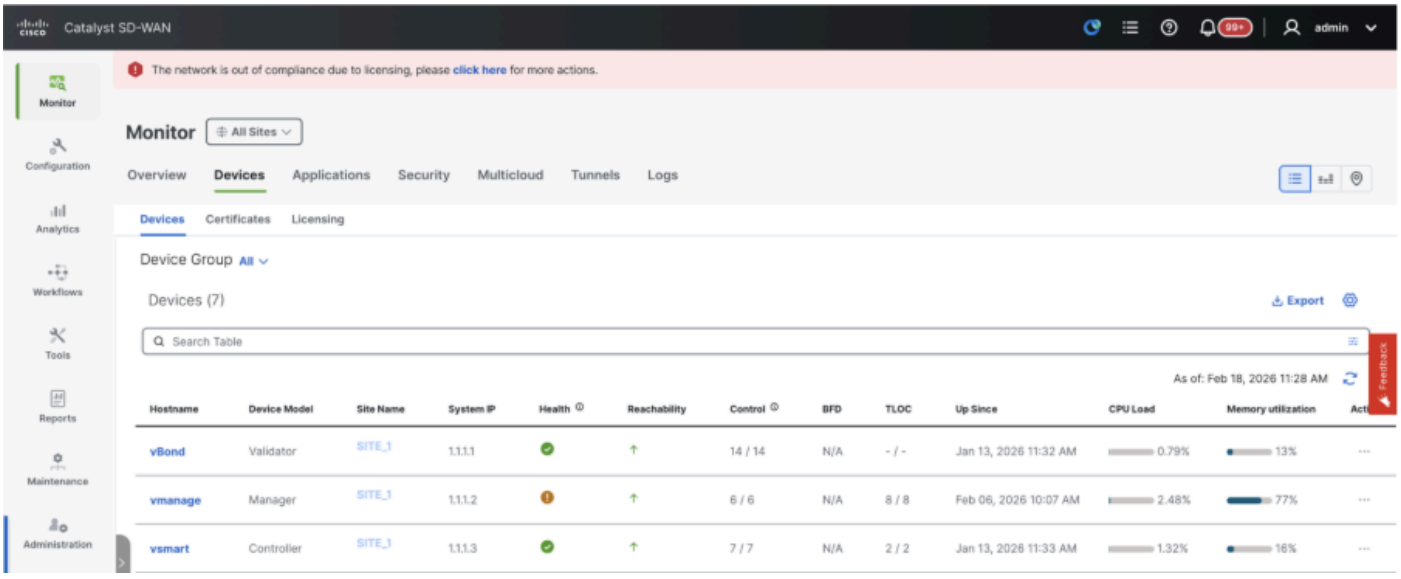
- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf dem vSmart installiert.
- Wenn Manual (Manuell) ausgewählt ist, signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren. Dasselbe Verfahren gilt für die Verwendung des Digicert- und Enterprise-Root-Zertifikats.
- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.
- Wenn mehrere vSmarts vorhanden sind, wiederholen Sie die gleichen Schritte.

Verifizierung

Überprüfen Sie nach Abschluss aller Schritte, ob alle Steuerungskomponenten unter Monitor>Dashboard erreichbar sind.



- Klicken Sie auf die jeweiligen Steuerungskomponenten, und vergewissern Sie sich, dass sie alle erreichbar sind.
- Navigieren Sie zu Überwachen > Geräte, und stellen Sie sicher, dass alle Steuerungskomponenten erreichbar sind.



Schritt 3: Sicherung/Wiederherstellung der Konfig.-DB

Sammeln von vManage-Konfigurations-DB-Backups und Wiederherstellen auf einem anderen vManage-Knoten

---

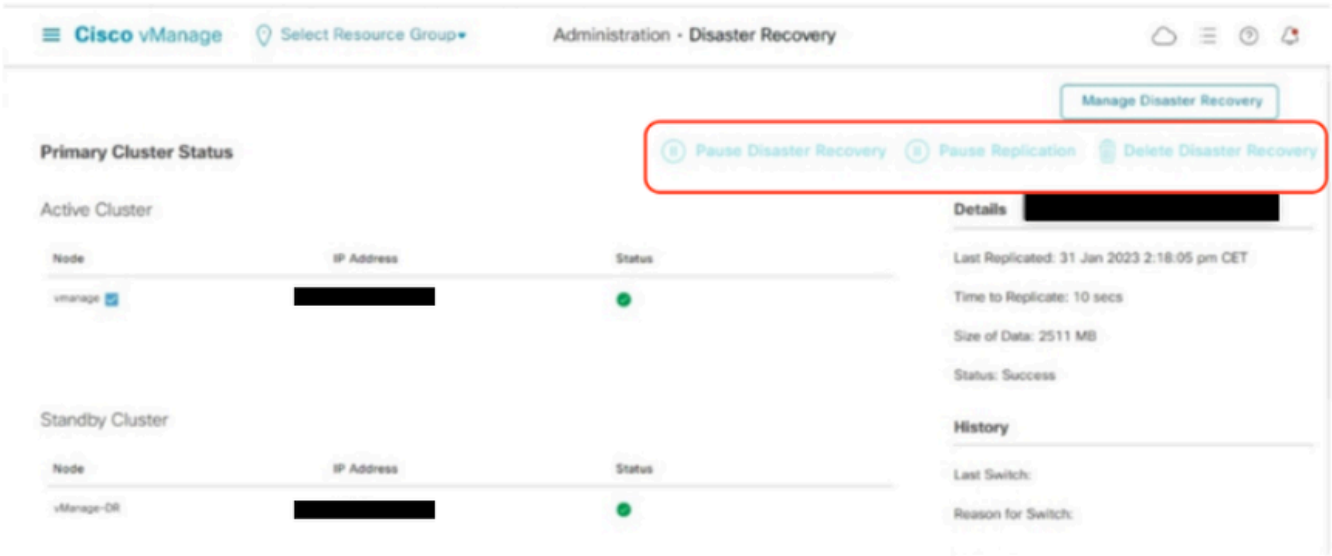
Anmerkung: Stellen Sie beim Sammeln des Konfigurations-Datenbank-Backups vom vorhandenen vManage-Knoten, auf dem die Notfallwiederherstellung aktiviert ist, sicher,

---

dass das Backup gesammelt wird, nachdem die Notfallwiederherstellung auf diesem Knoten angehalten und gelöscht wurde.

Bestätigen Sie, dass keine laufende Disaster Recovery-Replikation vorhanden ist. Navigieren Sie zu Administration > Disaster Recovery und Vergewissern Sie sich, dass der Status "Success" lautet und sich nicht in einem vorübergehenden Status wie "Import Pending" (Ausstehend), "Export Pending" (Ausstehend) oder "Download Pending" (Ausstehend) befindet. Wenn der Status nicht erfolgreich ist, wenden Sie sich an das Cisco TAC, und stellen Sie sicher, dass die Replikation erfolgreich ist, bevor Sie die Disaster Recovery anhalten.

Halten Sie zunächst die Notfallwiederherstellung an, und stellen Sie sicher, dass die Aufgabe abgeschlossen ist. Löschen Sie anschließend die Notfallwiederherstellung, und bestätigen Sie, dass die Aufgabe abgeschlossen ist.



Wenden Sie sich an das Cisco TAC, um sicherzustellen, dass die Notfallwiederherstellung erfolgreich beseitigt wird.

Sammeln der Konfiguration - DB-Backup:

- In der derzeit verwendeten SD-WAN-Fabric können Sie ein Konfigurations-DB-Backup sowohl auf eigenständigen vManage- als auch auf vManage-Cluster-Konfigurationen erstellen.
- Bei eigenständigem vManage ist dieser vManager selbst der führende Anbieter von Konfigurationsdatenbanken.

Vergewissern Sie sich, dass configuration-db auf dem vManage-Knoten ausgeführt wird.

Sie können dies mit dem Befehl request nms configuration-db statusonvManageCLI überprüfen. Die Ausgabe erfolgt wie dargestellt

```
vmanage# request nms configuration-db status
NMS configuration database
        Enabled: true
        Status: running PID:32632 for 1066085s
        Native metrics status: ENABLED
        Server-load metrics status: ENABLED
vmanage#
```

Verwenden Sie diesen Befehl, um das Backup configuration-db vom angegebenen Konfigurationsdb-Leader "vManage" zu erfassen.

```
request nms configuration-db backup path /opt/data/backup/
```

Die erwartete Ausgabe lautet wie folgt:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Notieren Sie sich die Anmeldeinformationen für die Konfigurationsdatenbank, wenn diese aktualisiert wurde.
- Wenn Sie die Anmeldeinformationen für die Konfigurationsdatenbank nicht kennen, wenden Sie sich an das TAC, um die Anmeldeinformationen für die Konfigurationsdatenbank von den vorhandenen vManage-Knoten abzurufen.
- Die Standardanmeldeinformationen für die -db-Konfiguration sind Benutzername: neo4j und Passwort: Kennwort

Wiederherstellen der Konfiguration - db-Sicherung auf einem anderen vManage-Knoten

Kopieren Sie das Sicherungsverzeichnis configuration-db mithilfe von SCP in das Verzeichnis /home/admin/ von vManage.

Beispielausgabe des Befehls scp:

```
XXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
```

```
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Zum Wiederherstellen des "configuration-db"-Backups müssen wir zunächst die "configuration-db"-Anmeldeinformationen konfigurieren. Wenn Ihre Anmeldeinformationen für configuration-db default(neo4j/password) sind, können wir diesen Schritt überspringen.

Um die Anmeldeinformationen für configuration-db zu konfigurieren, verwenden Sie den Befehl request nms configuration-db update-admin-user.Use the username and password of your choice.

Bitte beachten Sie, dass der Anwendungsserver von vManage neu gestartet wurde. Aufgrund dessen kann auf die vManage-Benutzeroberfläche für kurze Zeit nicht mehr zugegriffen werden.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operati
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Nach dem wir fortfahren können, die Konfiguration-db-Backup wiederherzustellen:

Wir können den Befehl request nms configuration-db restore path /home/admin/< > verwenden, um configuration-db auf dem neuen vManage wiederherzustellen:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Reseting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
```

```
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Sobald die Konfigurationsdatenbank wiederhergestellt ist, stellen Sie sicher, dass auf die vManage-Benutzeroberfläche zugegriffen werden kann. Warten Sie etwa 5 Minuten, und versuchen Sie dann, auf die Benutzeroberfläche zuzugreifen.

Nachdem Sie sich erfolgreich bei der Benutzeroberfläche angemeldet haben, stellen Sie sicher, dass die Liste der Edge-Router, die Vorlage, die Richtlinien und alle anderen Konfigurationen, die auf der vorherigen oder vorhandenen vManage-Benutzeroberfläche vorhanden waren, auf der neuen vManage-Benutzeroberfläche wiedergegeben werden.

Schritt 4: DR-Einrichtung für einen Knoten

Siehe Schritt 2: Vorprüfungen in Kombination 2: Standalone vManage + Single Node DR und stellen Sie sicher, dass wir alle Anforderungen erfüllt haben, bevor wir mit der Disaster Recovery fortfahren.

DR mit einem Knoten

Voraussetzungen

- Stellen Sie sicher, dass der primäre und der sekundäre Knoten über HTTPS über ein Transport-VPN (VPN 0) erreichbar sind.
- Stellen Sie sicher, dass auf dem primären und sekundären Cisco vManage-Knoten dieselbe Cisco vManage-Version ausgeführt wird.

Out-of-Band-Cluster-Schnittstelle in VPN 0

1. Für jede vManage-Instanz innerhalb eines Clusters ist neben den für VPN 0 (Transport) und VPN 512 (Management) verwendeten Schnittstellen eine dritte Schnittstelle (Cluster-Verbindung) erforderlich.
2. Diese Schnittstelle wird für die Kommunikation und Synchronisierung zwischen den vManage-Servern im Cluster verwendet.
3. Diese Schnittstelle muss mindestens 1 Gbit/s betragen und eine Latenz von maximal 4 ms aufweisen. Eine Schnittstelle mit 10 Gbit/s wird empfohlen.
4. Beide vManage-Knoten müssen sich über diese Schnittstelle erreichen können: sei es ein Layer-2-Segment oder durch Layer-3-Routing.

- Stellen Sie sicher, dass alle Services (Anwendungsserver, Konfigurationsdatenbank, Messaging-Server, Koordinierungsserver und Statistikdatenbank) auf beiden Cisco vManage-Knoten aktiviert sind.

- Verteilung aller Controller, einschließlich Cisco vBond Orchestrator, auf primäre und sekundäre Rechenzentren Stellen Sie sicher, dass diese Controller über Cisco vManage-Knoten erreichbar sind, die über diese Rechenzentren verteilt sind. Die Controller sind nur mit dem primären Cisco vManage-Knoten verbunden.
- Vergewissern Sie sich, dass im aktiven (primären) und im Standby-Knoten (sekundären) Cisco vManage keine weiteren Vorgänge ausgeführt werden. Stellen Sie z. B. sicher, dass keine Server aktualisiert werden oder dass keine Vorlagen an die Geräte angehängt werden.

- Deaktivieren Sie den Cisco vManage HTTP/HTTPS-Proxyserver, wenn er aktiviert ist. Wenn Sie den Proxyserver nicht deaktivieren, versucht Cisco vManage, eine Notfallwiederherstellungs-Kommunikation über die Proxy-IP-Adresse herzustellen, selbst wenn die Out-of-Band-Cluster-IP-Adressen von Cisco vManage direkt erreichbar sind. Sie können den Cisco vManage HTTP/HTTPS-Proxyserver nach Abschluss der Disaster Recovery-Registrierung erneut aktivieren.

- Bevor Sie mit der Registrierung für die Notfallwiederherstellung beginnen, rufen Sie das Fenster Extras → Netzwerk neu erkennen auf, das sich auf dem primären Cisco vManage-Knoten befindet, und suchen Sie erneut nach Cisco vBond Orchestrator.

Konfiguration

Konfigurieren der CLI-Konfigurationen des vManage-Knotens, der als Notfallwiederherstellungsknoten fungiert

Die absolute Mindestkonfiguration für vManagevor der Registrierung für die Notfallwiederherstellung ist wie folgt

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond
```

```
commit
```

Hinweis: Wenn wir eine URL als vBond-Adresse verwenden, stellen Sie sicher, dass die IP-Adressen des DNS-Servers in der VPN 0-Konfiguration konfiguriert sind, oder dass sie aufgelöst werden können.

Diese Konfigurationen werden benötigt, um die Transportschnittstelle zu aktivieren, die zum Herstellen von Steuerverbindungen mit den Routern und den übrigen Controllern verwendet wird

```
config t
vpn 0
 dns


        primary
 dns


         secondary
 interface eth1
  ip address



  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
```

```
 !
 ip route 0.0.0.0/0



commit
```

Konfigurieren Sie außerdem die VPN 512Management-Schnittstelle, um den Out-of-Band-Management-Zugriff auf den Controller zu ermöglichen.

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
commit
```

Konfigurieren Sie die Service-Schnittstelle auf DR vManage.

Konfigurieren Sie die Service-Schnittstelle auf dem vManage-Knoten. Diese Schnittstelle wird für die DR-Kommunikation verwendet.

```
conf t
 interface eth2
  ip address
```

```
  no shutdown
commit
```

Stellen Sie sicher, dass dasselbe IP-Subnetz für die Service-Schnittstelle auf dem primären vManage und DR vManage verwendet wird.

Aktualisieren der Konfigurationen der vManage-Benutzeroberfläche

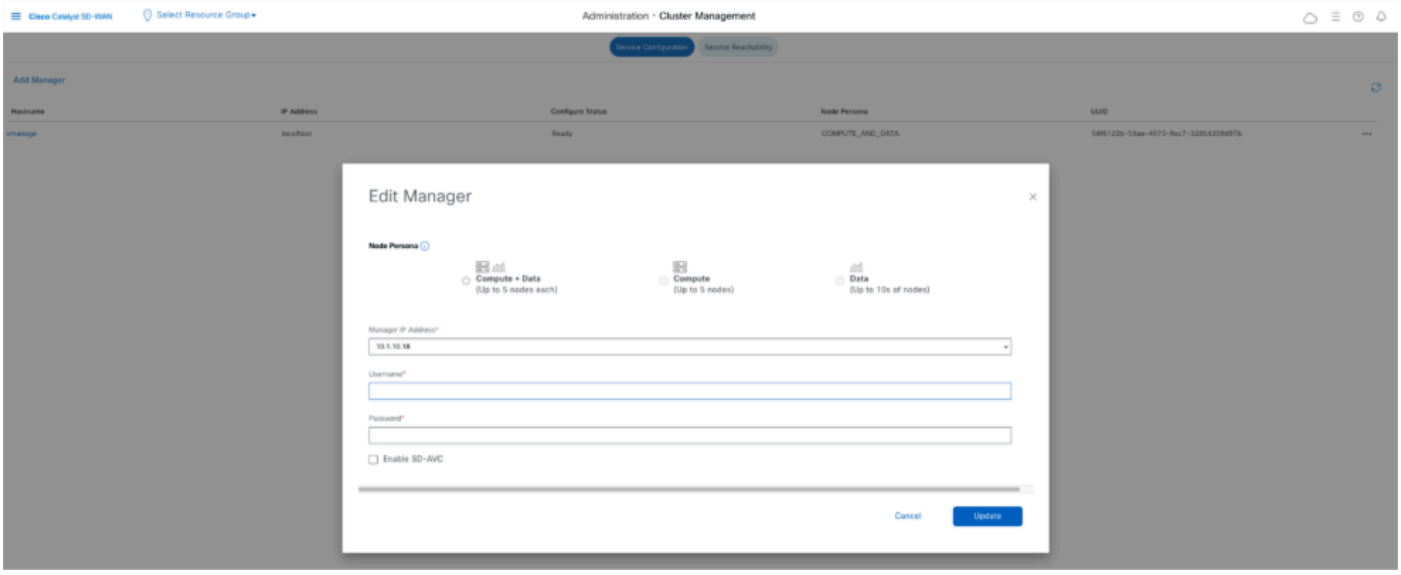
- Sobald die Konfigurationen der CLI aller Controller hinzugefügt wurden, können wir über die URL https://<vmanage-ip> in Ihrem Browser auf die Web-UI von vManage zugreifen. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManage-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Administration > Settings, und führen Sie diese Schritte aus.
- Organisationsname konfigurieren. Konfigurieren Sie den gleichen Wert wie in der CLI des vManage-Knotens.
- In vManage 20.15/20.18 sind diese Konfigurationen im Abschnitt System verfügbar.

Installieren des Zertifikats auf DR vManage

Gehen Sie wie unter Abschnitt Kombination 2 beschrieben vor: Standalone vManage + Single Node DR Schritt 3: Konfigurieren Sie die vManage-Benutzeroberfläche, -Zertifikate und -Onboard-Controller, um das Zertifikat auf dem Disaster Recovery vManage zu installieren.

Hinzufügen der Disaster Recovery-Konfiguration

- Rufen Sie hierzu den primären vManager auf.
- Navigieren Sie zu Administration → Cluster Management, und geben Sie die IP-Adresse der Out-of-Band-Schnittstelle an, nachdem Sie auf die drei Punkte auf der rechten Seite des vManage-Eintrags geklickt haben. Fügen Sie Benutzername und Kennwort ein. Es wird empfohlen, für diese Konfiguration einen separaten lokalen Benutzer zu erstellen, z. B. dradmin auf dem primären und DR-Manager.



- VManage wird nach dieser Änderung neu gestartet.
- Navigieren Sie nach dem Aktivieren von Primary vManage zu Administration → Disaster Recovery. Klicken Sie auf "Verwalten der Notfallwiederherstellung".
- Geben Sie im Popup-Fenster die Details für den primären und sekundären vManage ein.
- Die anzuzeigenden IP-Adressen sind die Out-of-Band-Cluster-Schnittstellen(eth2).
- Die Anmeldedaten müssen die eines Netzwerkadministratorbenutzers (dradmin) sein und dürfen nicht geändert werden, nachdem der Notfallwiederherstellungsmechanismus konfiguriert wurde. Für die Notfallwiederherstellung können separate Anmeldeinformationen für lokale Benutzer von vManage verwendet werden. Wir müssen sicherstellen, dass der lokale vManage-Benutzer Teil der netadmin-Gruppe ist. Hier können sogar Administratoranmeldeinformationen verwendet werden.

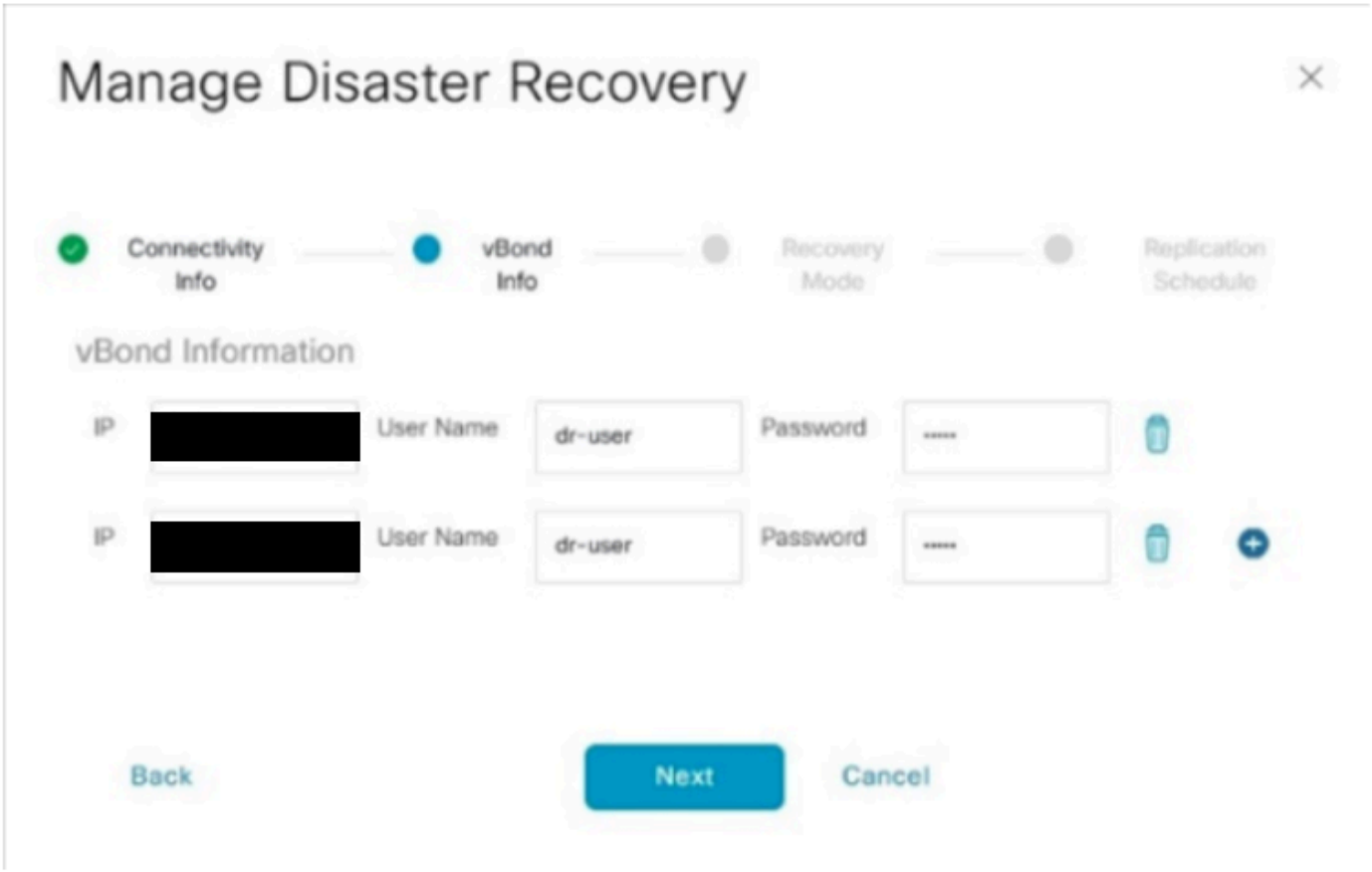
- Klicken Sie nach dem Ausfüllen auf "Weiter".

- Füllen Sie die Details der vBond-Controller aus.

- Die vBond-Controller müssen über Netconf in der angegebenen IP-Adresse erreichbar sein.

- Die Anmeldedaten müssen die eines Netzwerkadministratorbenutzers (dradmin) sein und dürfen nach der Konfiguration des DR nicht mehr geändert werden.

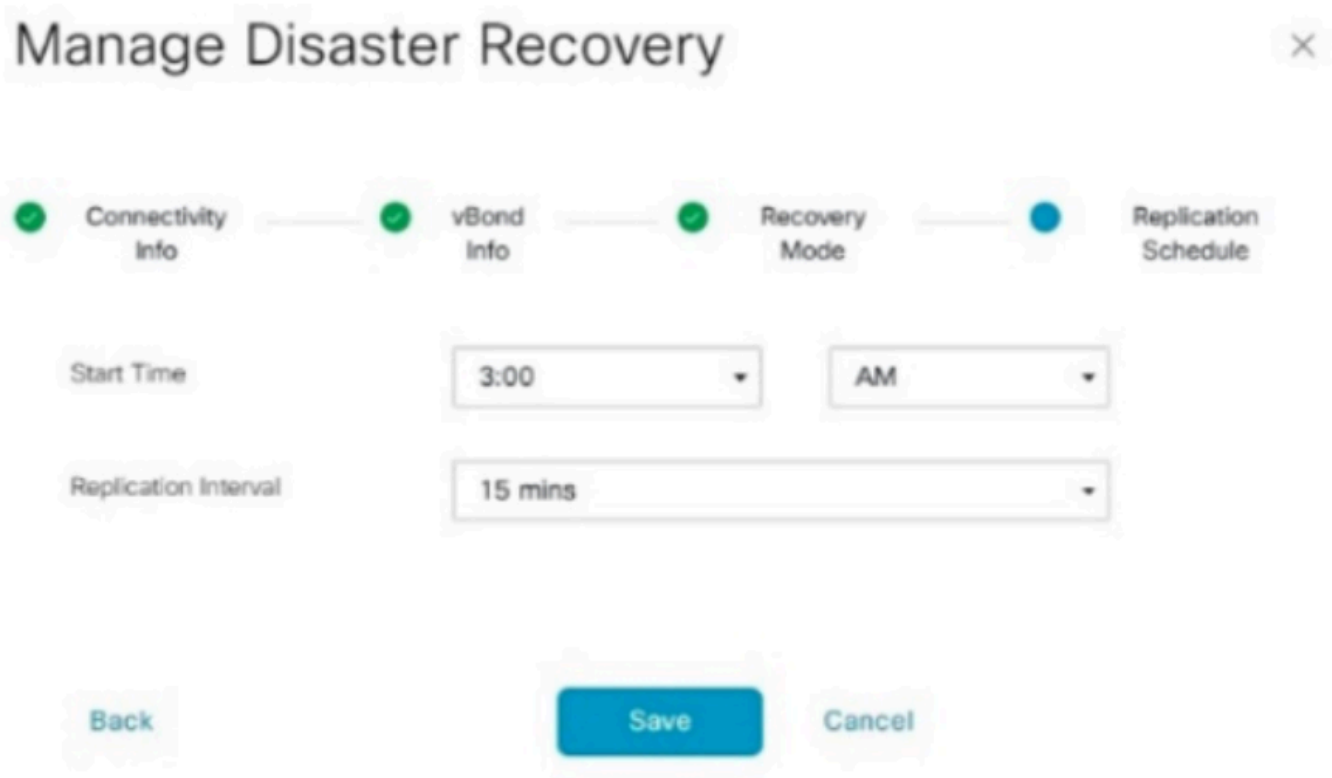
- Zu diesem Zweck wird empfohlen, dass vBond diesen Dradmin-Benutzer lokal konfiguriert. Alternativ können Sie den Admin-Benutzer verwenden, um vBond hinzuzufügen.



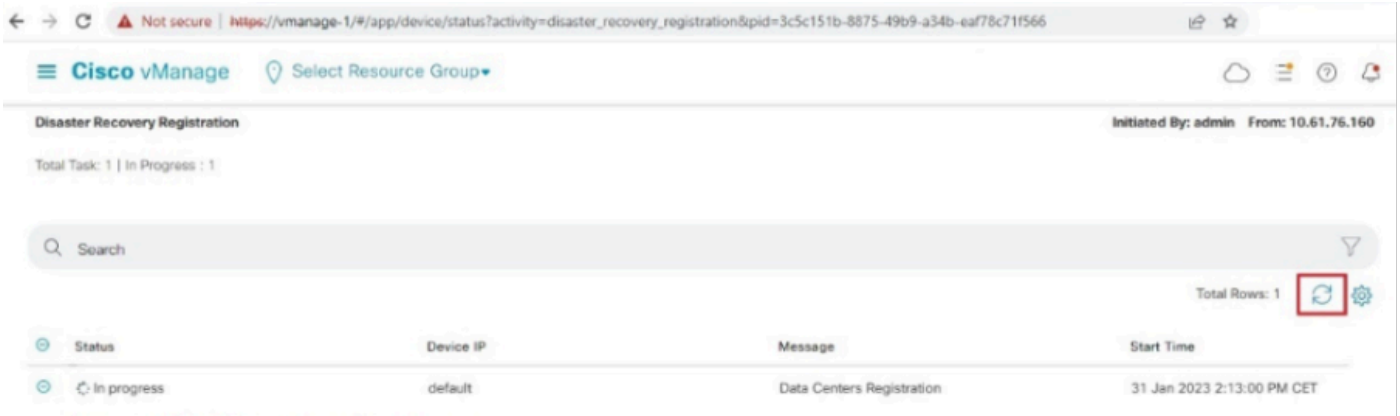
- Klicken Sie nach dem Ausfüllen auf "Weiter".
- Wählen Sie im Wiederherstellungsmodus "Manuell" aus. Klicken Sie auf "Weiter".

Legen Sie im Replikationszeitplan den Wert "Replication Interval" (Replikationsintervall)'.Bei jedem Replikationsintervall werden die Daten von der primären vManageTo sekundärer vManage.

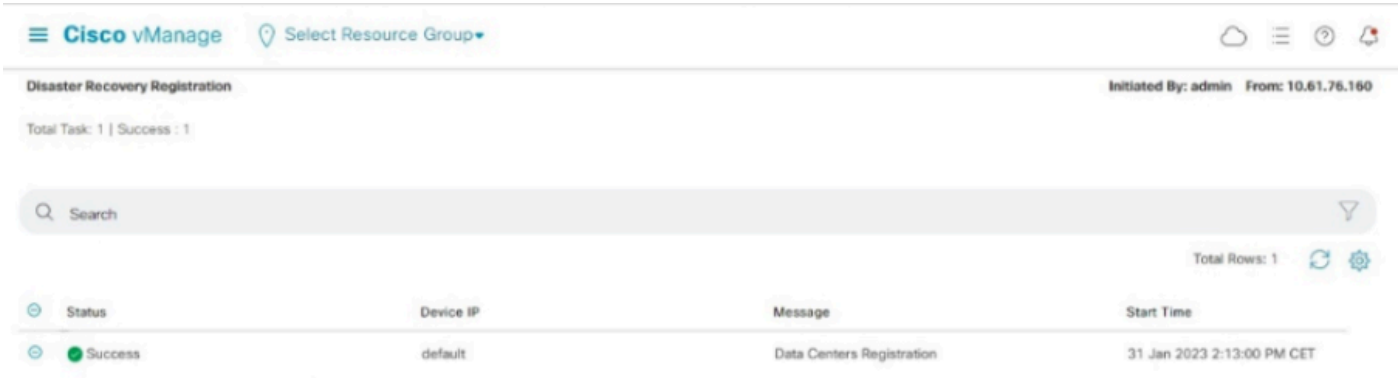
Der konfigurierbare Mindestwert beträgt 15 Minuten.



- Legen Sie den Wert fest, und klicken Sie auf "Speichern".
- Die DR-Registrierung beginnt jetzt. Klicken Sie auf die Aktualisierungsschaltfläche, um den Status und die Fortschrittsprotokolle manuell zu aktualisieren. Dieser Vorgang kann 20-30 Minuten dauern.

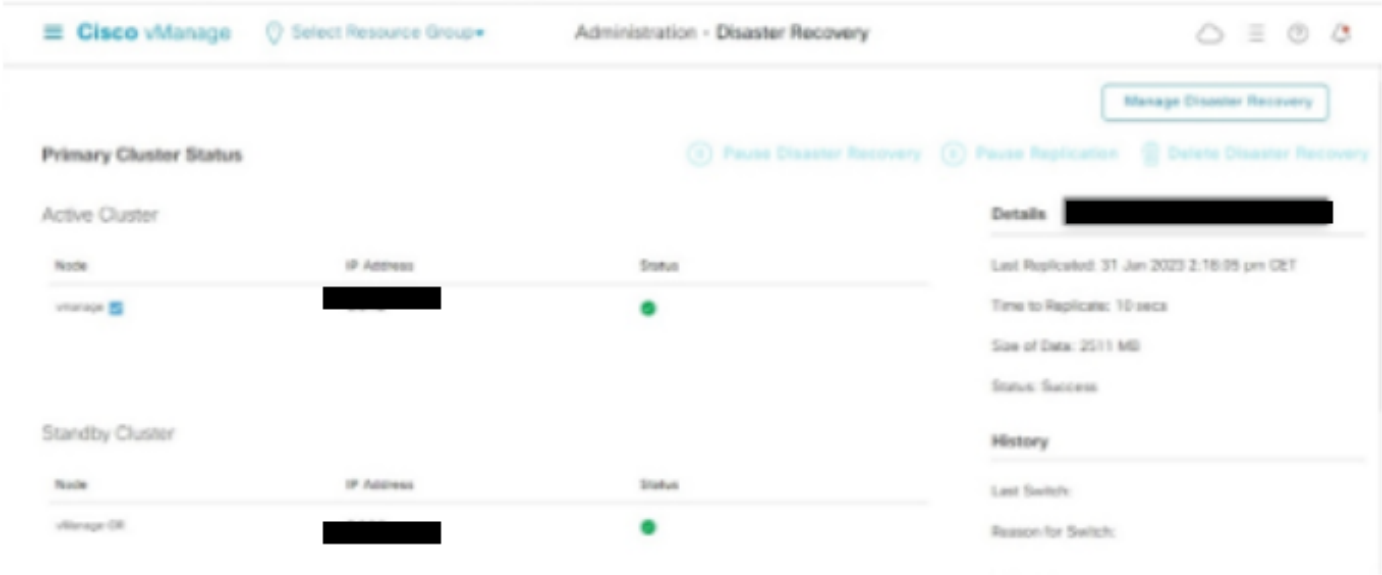


- Beachten Sie, dass die grafische Benutzeroberfläche von vManage während dieses Vorgangs neu gestartet wird.
- Nach Abschluss dieses Vorgangs muss der Status "Success" angezeigt werden.



Überprüfung

Navigieren Sie zuAdministration → Disaster Recoveryum den Status der Notfallwiederherstellung und den Zeitpunkt der letzten Replikation der Daten anzuzeigen.



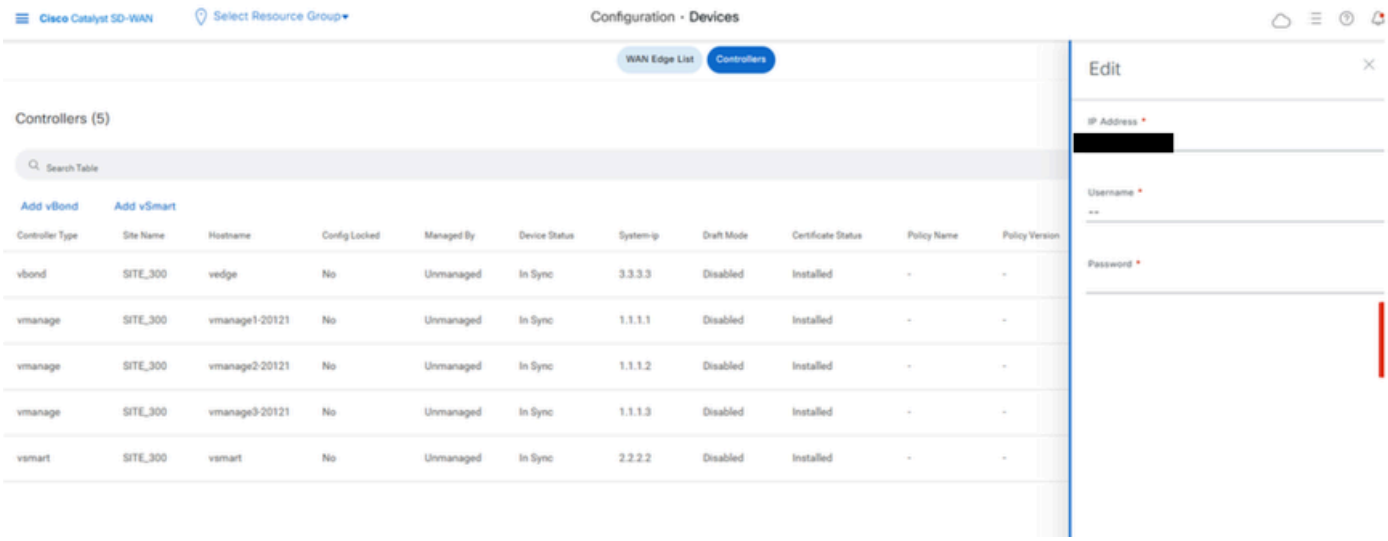
Schritt 5: Neuauthentifizierung von Controllern und Ungültigerklärung alter Controller

Nach der Wiederherstellung der Konfigurationsdatenbank müssen alle neuen Controller (vmanage/vsmart/vbond) im Fabric erneut authentifiziert werden.

Hinweis: Wenn in der Produktion die zur erneuten Authentifizierung verwendete Schnittstellen-IP die Tunnel-Schnittstellen-IP ist, müssen Sie sicherstellen, dass der NETCONF-Dienst auf der Tunnelschnittstelle von vManage, vSmart und vBond sowie auf den Firewalls entlang des Pfads zugelassen ist. Der zu öffnende Firewall-Port ist der TCP-Port 830 als bidirektionale Regel vom DR-Cluster zu allen vBonds und vSmarts .

Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.

- Klicken Sie auf die drei Punkte in der Nähe der einzelnen Controller, und klicken Sie dann auf Bearbeiten.



- Ersetzen Sie die IP-Adresse (System-IP des Controllers) durch die IP-Adresse des Transport-VPN 0 (Tunnelschnittstelle). Geben Sie Benutzername und Kennwort ein, und klicken Sie auf "Save" (Speichern).
- Gleiches für alle neuen Controller im Fabric tun

Synchronisieren der Root-Zertifikatskette

Führen Sie diesen Schritt aus, nachdem alle Controller integriert wurden:

Führen Sie auf einem Cisco SD-WAN Manager-Server im neu aktiven Cluster die folgenden Aktionen aus:

Geben Sie diesen Befehl ein, um das Root-Zertifikat mit allen Cisco Catalyst SD-WAN-Geräten im neu aktiven Cluster zu synchronisieren:

https://vmanage-url/dataservice/system/device/sync/rootcertchain

Geben Sie diesen Befehl ein, um die UUID des Cisco SD-WAN-Managers mit dem Cisco SD-WAN Validator zu synchronisieren:

https://vmanage-url/dataservice/certificate/syncvbond

Sobald die Fabric wiederhergestellt ist und die Steuerungs- und BFD-Sitzungen für alle Edges und Controller in der Fabric verfügbar sind, müssen die alten Controller (vmanage/vsmart/vbond) in der Benutzeroberfläche ungültig gemacht werden.

- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Zertifikate.
- Auf Controller klicken
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Ungültig
- Klicken Sie auf Senden,

- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Löschen

Schritt 6: Nachprüfungen

Anmerkung: Fahren Sie mit dem hier abgebildeten Abschnitt "Nachprüfungen" fort, der für alle Bereitstellungskombinationen gilt.

Kombination 3: vCluster verwalten + Keine DR

Erforderliche Instanzen:

- 3 vManage (Cluster mit 3 Knoten, alle COMPUTE_AND_DATA) oder 6 vManage (3 COMPUTE_AND_DATA + 3 DATA)
- 1 oder mehr vBond
- 1 oder mehr vSmart

Schritte:

1. Aufrufen aller Instanzen mithilfe der allgemeinen Schritte
2. Vorabprüfungen
3. Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller
4. vManage-Cluster erstellen
5. Sicherung/Wiederherstellung der Konfig.-DB
6. Nachprüfungen

Schritt 1: Vorabprüfungen

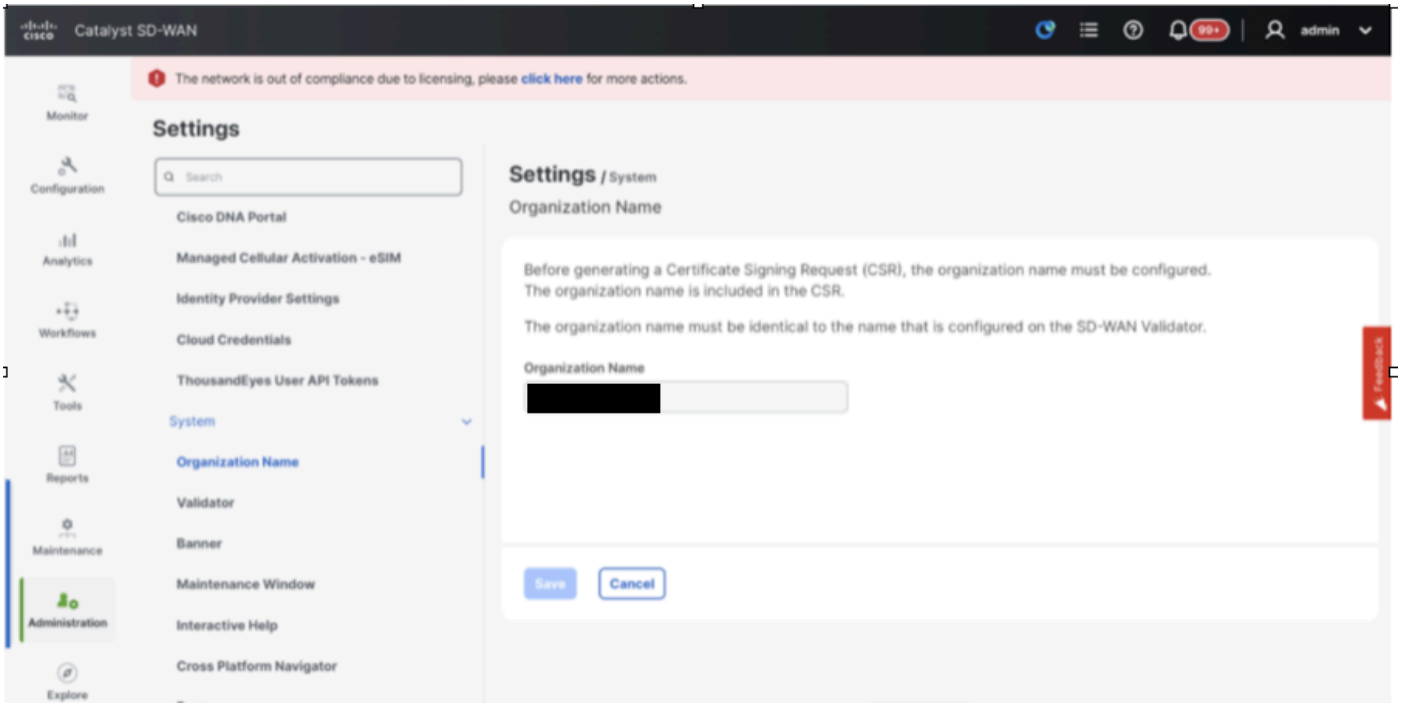
- Stellen Sie sicher, dass die Anzahl der aktiven Cisco SD-WAN Manager-Instanzen mit der Anzahl der neu installierten Cisco SD-WAN Manager-Instanzen identisch ist.
- Stellen Sie sicher, dass auf allen aktiven und neuen Cisco SD-WAN Manager-Instanzen dieselbe Softwareversion ausgeführt wird.
- Stellen Sie sicher, dass alle aktiven und neuen Cisco SD-WAN Manager-Instanzen die Management-IP-Adresse des Cisco SD-WAN Validators erreichen können.
- Stellen Sie sicher, dass die Zertifikate auf den neu installierten Cisco SD-WAN Manager-Instanzen installiert wurden.
- Stellen Sie sicher, dass die Uhren auf allen Cisco Catalyst SD-WAN-Geräten, einschließlich der neu installierten Cisco SD-WAN Manager-Instanzen, synchronisiert sind.
- Stellen Sie sicher, dass auf den neu installierten Cisco SD-WAN Manager-Instanzen ein

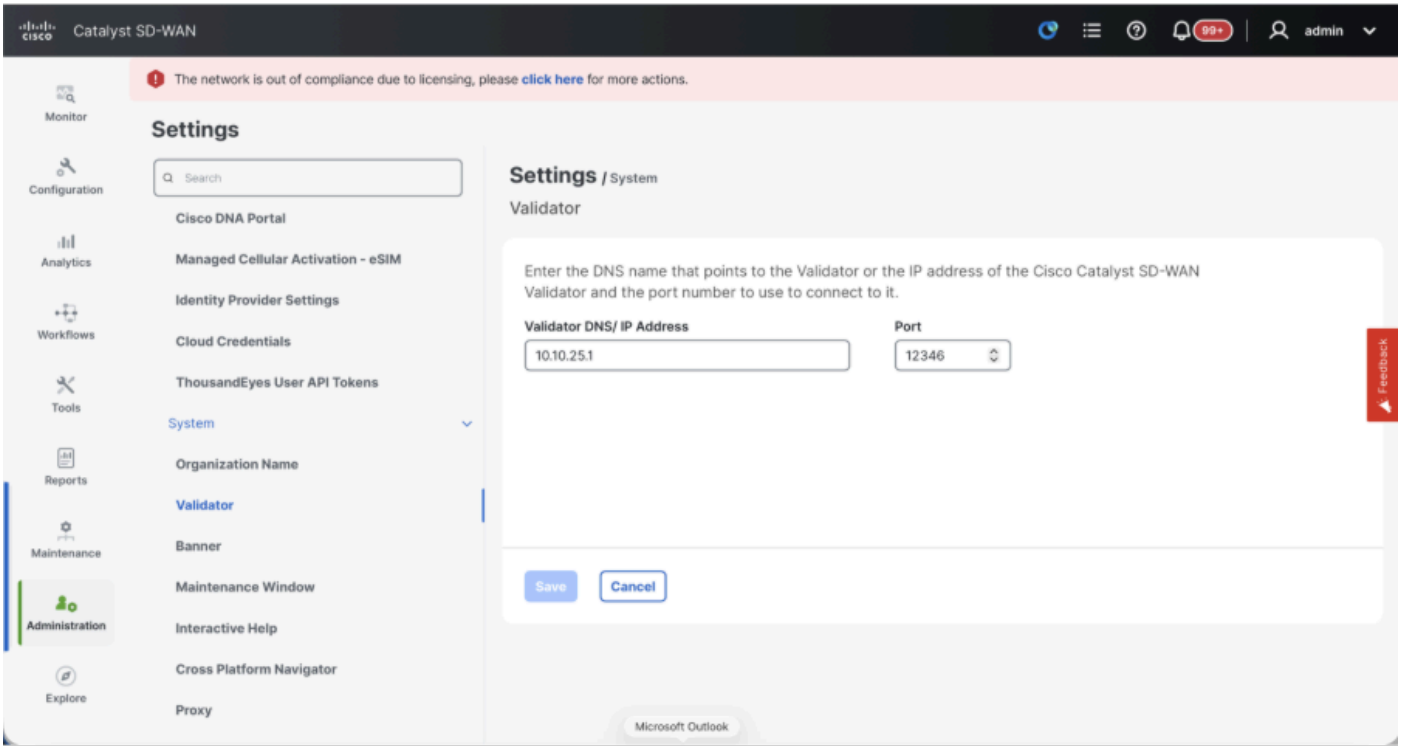
neuer Satz von System-IPs und Standort-IDs konfiguriert und die gleiche grundlegende Konfiguration wie im aktiven Cluster verwendet wird.

Phase 2: Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller

Aktualisieren der Konfigurationen der vManage-Benutzeroberfläche

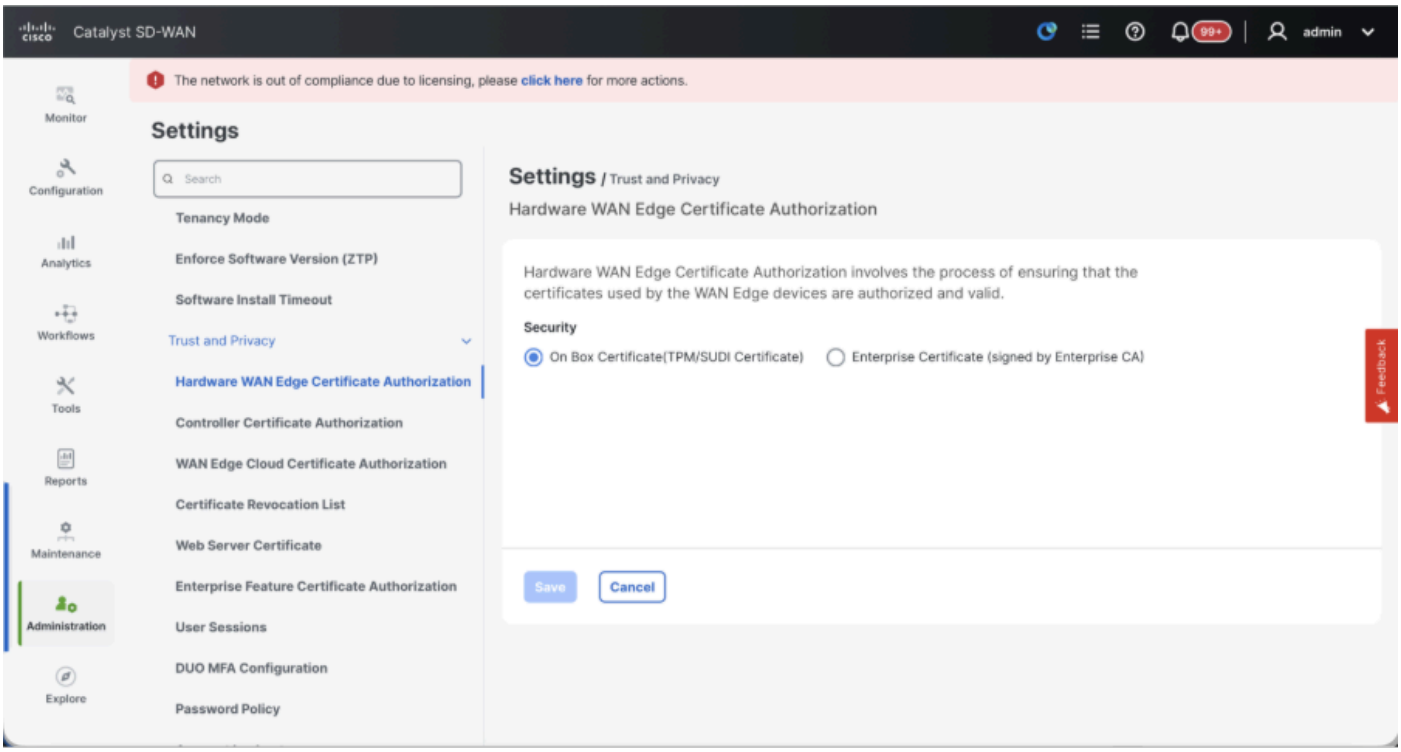
- Sobald die Konfigurationen in Schritt 1 in der CLI aller Controller hinzugefügt wurden, können wir über die URL https://<vmanage-ip> in Ihrem Browser auf die Web-UI von vManage zugreifen. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManage-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Administration > Settings, und führen Sie diese Schritte aus.
- Konfigurieren Sie den Organisationsnamen und die Validator-/vBond-URL/IP-Adresse. Konfigurieren Sie den gleichen Wert wie in der CLI des vManage-Knotens.
- In vManage 20.15/20.18 sind diese Konfigurationen im Abschnitt System verfügbar.



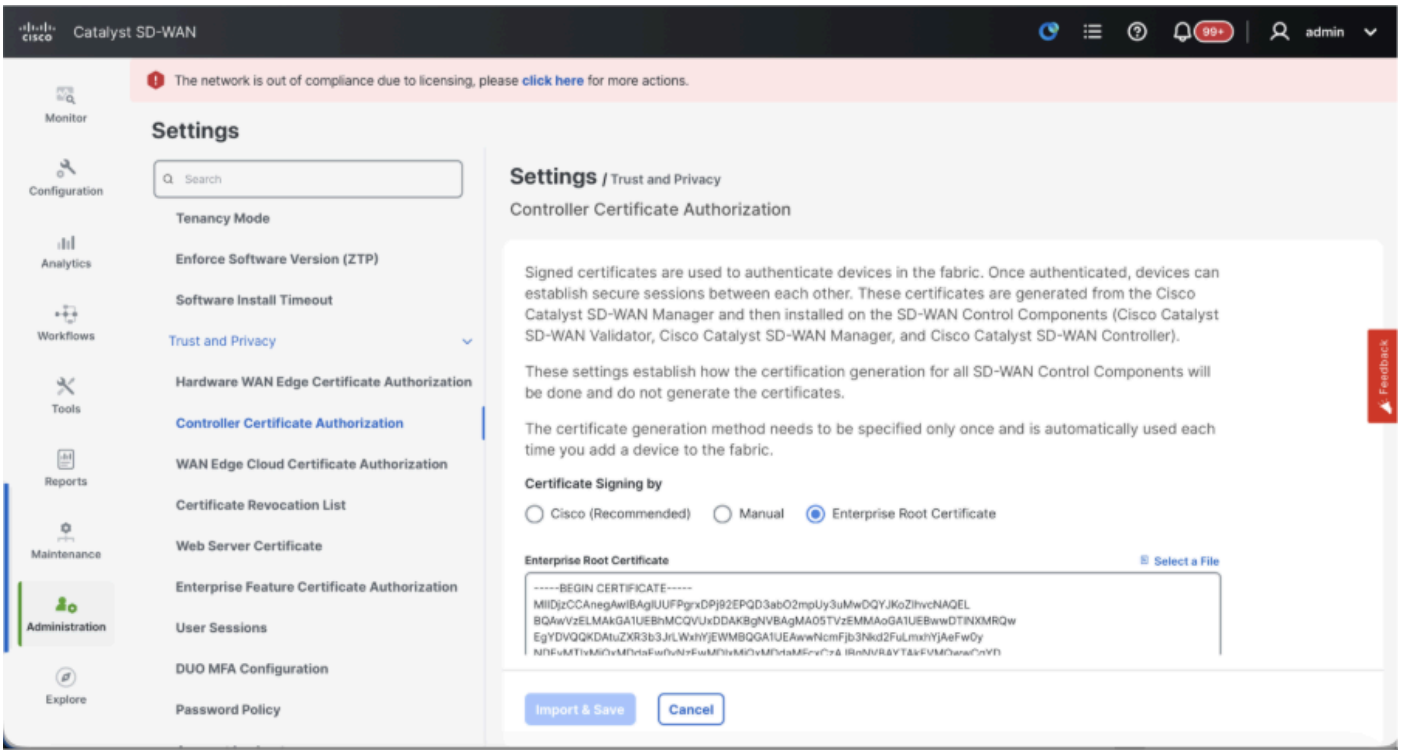


- Überprüfen Sie die Konfigurationen für die Zertifizierungsstelle (Certificate Authorization, CA), die die zum Signieren der Zertifikate verwendete Zertifizierungsstelle bestimmt. Hier sehen wir 3 Optionen:

1. Hardware WAN Edge Certificate Authorization (Hardware-WAN-Edge-Zertifikatsautorisierung): bestimmt die Zertifizierungsstelle für Hardware-SD-WAN-Edge-Router.
    - On Box Certificate (TPM/SUDI Certificate) - Mit dieser Option wird das vorinstallierte Zertifikat auf der Router-Hardware verwendet, um die Steuerverbindungen (TLS-/DTLS-Verbindungen) herzustellen.
    - Enterprise-Zertifikat (von der Enterprise-Zertifizierungsstelle signiert) - Bei dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

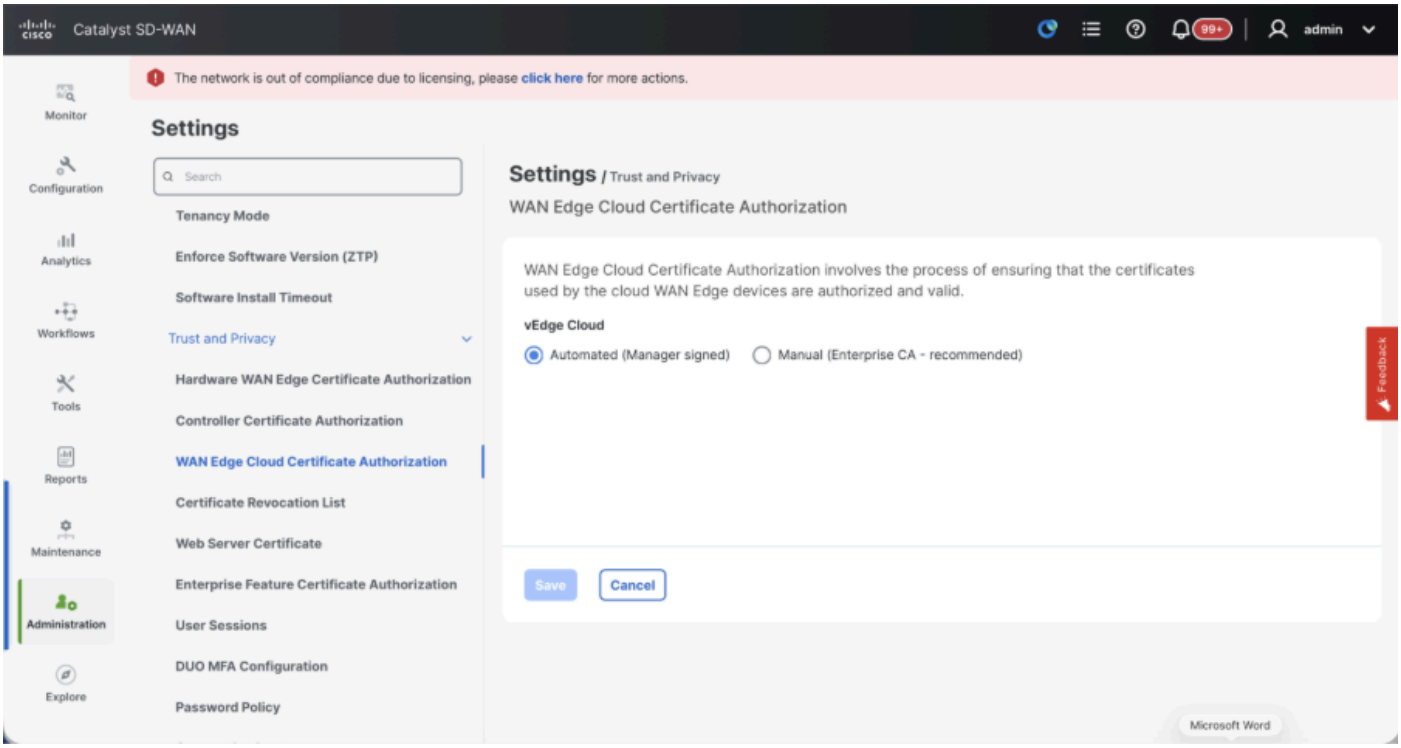


2. Controller Certificate Authorization (Controller-Zertifikatautorisierung): bestimmt die Zertifizierungsstelle für SD-WAN-Controller
    - Cisco (empfohlen) - Controller verwenden die von der Cisco PKI signierten Zertifikate. vManage kontaktiert das PNP-Portal automatisch mit den Smart Account-Anmeldedaten, die auf dem vManage konfiguriert sind. Das Zertifikat wird signiert und auf dem Controller installiert.
    - Manual (Manuell) - Controller verwenden die von der Cisco PKI signierten Zertifikate. Signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren.
    - Enterprise-Stammzertifikat - Mit dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

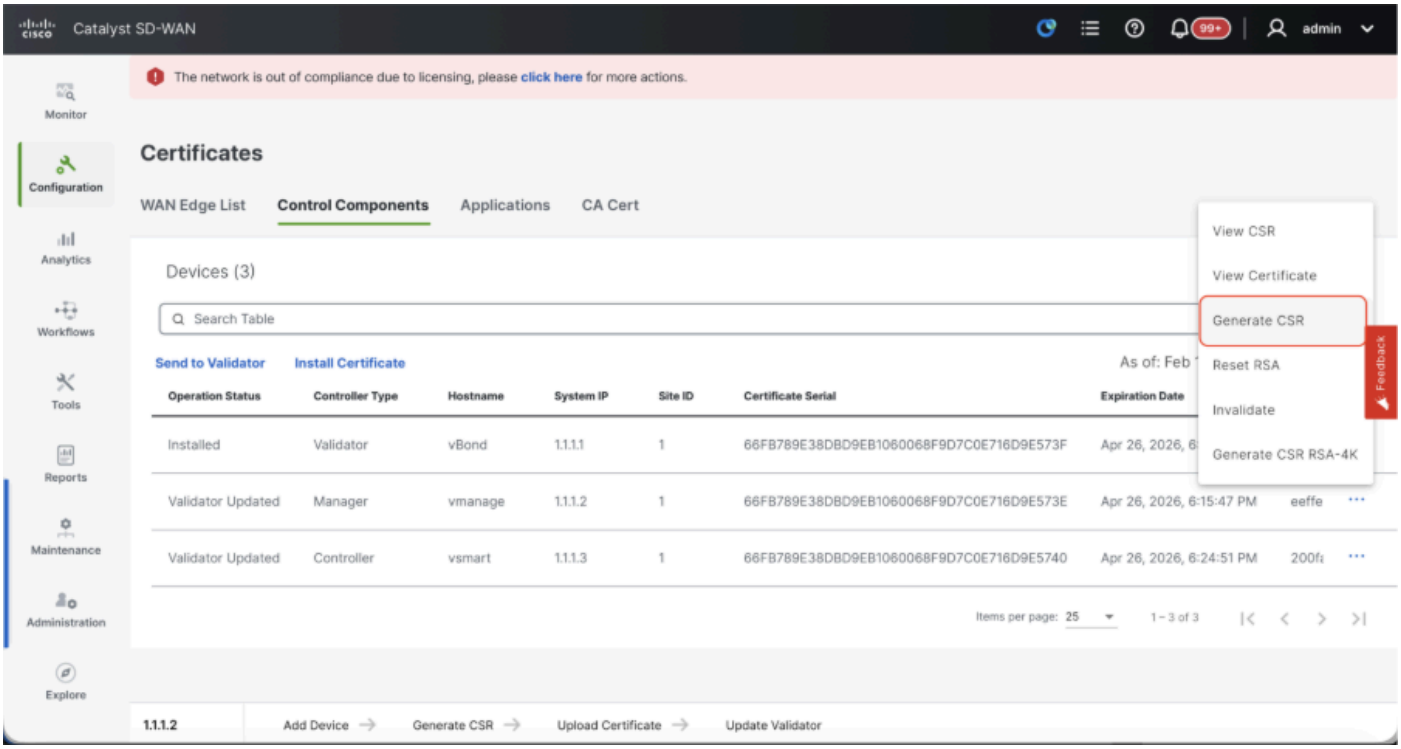


3. WAN-Edge-Cloud-Zertifikatautorisierung - bestimmt die Zertifizierungsstelle für virtuelle SD-WAN-Edge-Router (CSR1000v, C8000v, vEdge-Cloud)
    - Automated (vManage signiert) - vManage signiert automatisch den CSR für die virtuellen Edge-Router und installiert das Zertifikat auf dem Router.
    - Manuell (Enterprise CA - empfohlen) - Virtuelle Router verwenden Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

Wenn Sie eine eigene Zertifizierungsstelle (CA) oder eine Enterprise-Zertifizierungsstelle verwenden, wählen Sie Enterprise aus.



- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller
- Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

Integration von vBond/Validator und vSmart/Controller in vManage

Navigieren Sie zu Configuration > Devices > Control Components (Konfiguration > Geräte > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

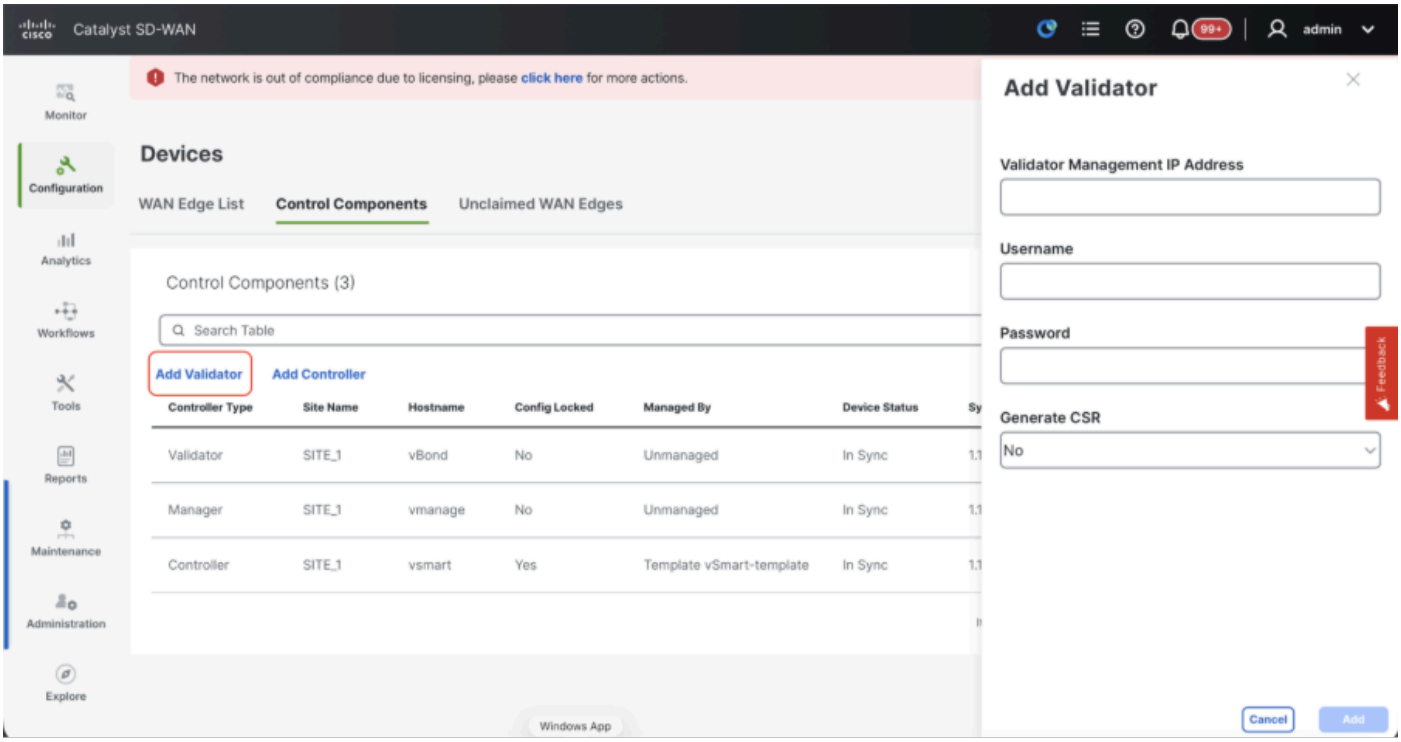
IntegrierenvBond/Validator

- Klicken Sie auf AdvBond.bei 20.12vManagerValidator hinzufügenim Fall von

20.15/20.18vManage. Ein Popup-Fenster wird geöffnet, und geben Sie den VPN 0-Transport-IP von vBond, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, falls dies über die CLI von vManagementvBondIP zulässig ist.
- Geben Sie die Anmeldeinformationen für den Benutzer von vBond ein.

Hinweis: Wir müssen Admin-Anmeldedaten von vBond oder einem Benutzerteil von netadmingroup verwenden. Dies können Sie in der CLI von vBond überprüfen. Wählen Sie im Dropdown-Menü "CSR generieren" die Option "Ja", wenn ein neues Zertifikat für vBond installiert werden soll.

Anmerkung: Wenn sich vBond hinter einem NAT-Gerät bzw. einer NAT-Firewall befindet, überprüfen Sie, ob die IP-Adresse der vBond VPN 0-Schnittstelle in eine öffentliche IP-Adresse übersetzt wurde. Wenn die VPN 0-Schnittstellen-IP von vManage aus nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der VPN 0-Schnittstelle.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vBond installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal.

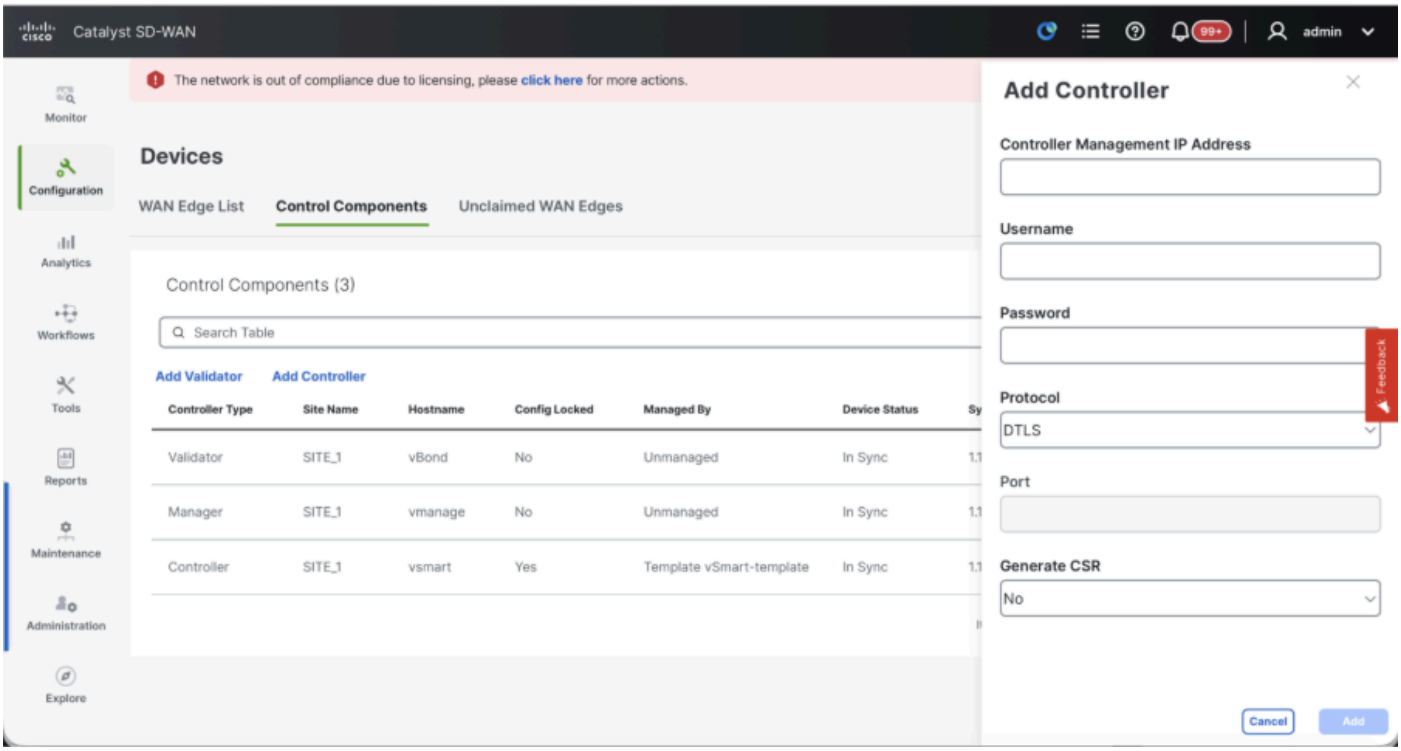
Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

- Wenn mehrere vBonds vorhanden sind, wiederholen Sie die gleichen Schritte.

Integration von vSmart/Controller

- Klicken Sie auf Add vSmart (vSmart hinzufügen), wenn es sich um 20.12 vManage handelt, oder auf Add Controller (Controller hinzufügen), wenn es sich um 20.15/20.18 vManage handelt.
- Geben Sie in einem Popup-Fenster die VPN 0-Transport-IP von vSmart ein, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, wenn dies von der CLI von vManage zu vSmart IP zulässig ist.
- Geben Sie die Benutzeranmeldeinformationen für vSmart Note ein, die von vSmart oder einem Benutzer der netadmin-Gruppe verwendet werden müssen.
- Sie können dies in der CLI des vSmart überprüfen.
- Legen Sie das Protokoll auf TLS fest, wenn TLS für Router verwendet werden soll, um Steuerverbindungen mit vSmart herzustellen. Diese Konfiguration muss auch für CLI von vSmarts- und vManage-Knoten konfiguriert werden.
- Wählen Sie im Dropdown-Menü "Generate CSR" (CSR generieren) die Option Yes (Ja) aus, wenn ein neues Zertifikat für vSmart installiert werden muss.

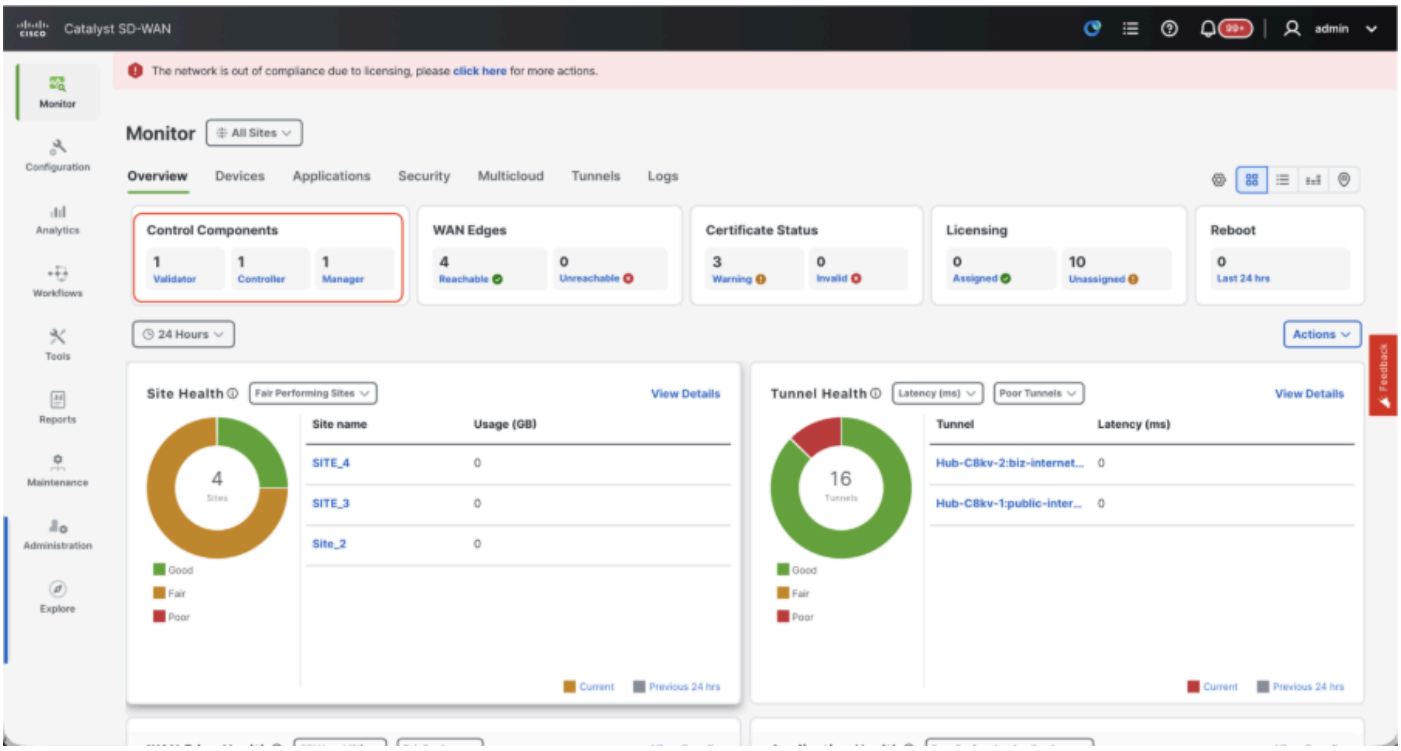
Hinweis: Wenn sich vSmart hinter dem NAT-Gerät/der Firewall befindet, prüfen Sie, ob die IP-Adresse der vSmart VPN 0-Schnittstelle in eine öffentliche IP übersetzt wurde. Wenn die IP-Adresse der VPN 0-Schnittstelle von vManage nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der IP-Adresse der VPN 0-Schnittstelle.



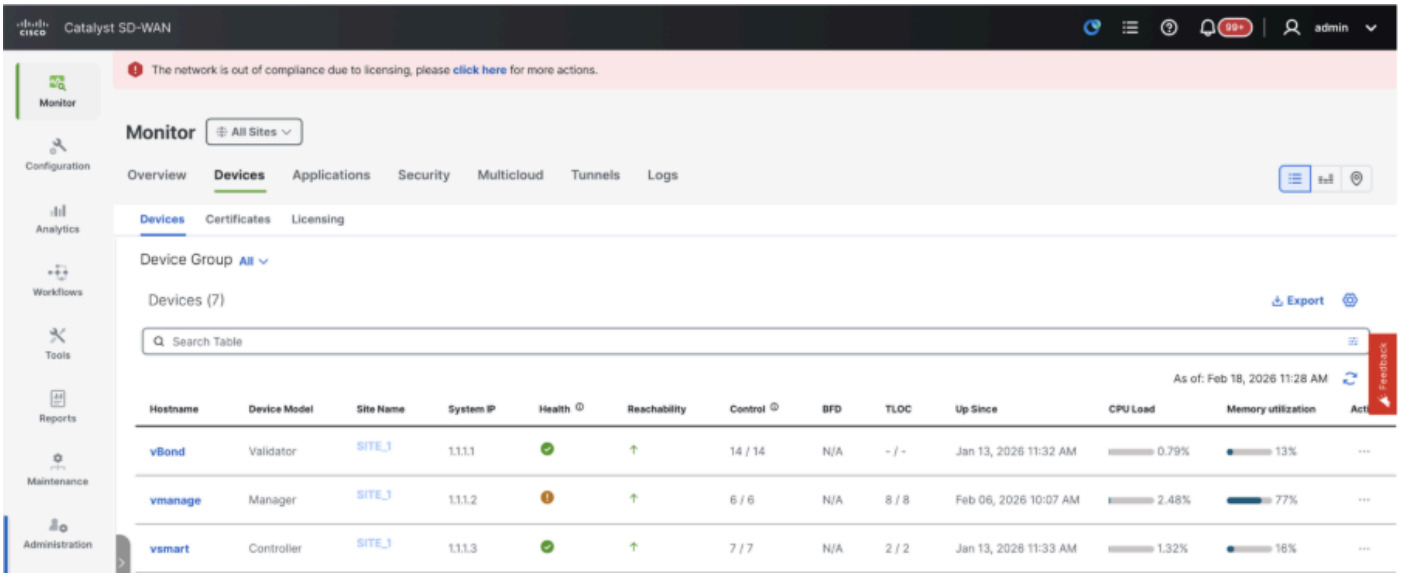
- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf dem vSmart installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays.
- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.
- Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.
- Wenn mehrere vSmarts vorhanden sind, wiederholen Sie die gleichen Schritte.

Verifizierung

Überprüfen Sie nach Abschluss aller Schritte, ob alle Steuerungskomponenten unter Monitor>Dashboard erreichbar sind.



- Klicken Sie auf die jeweiligen Steuerungskomponenten, und vergewissern Sie sich, dass sie alle erreichbar sind.
- Navigieren Sie zu Überwachen > Geräte, und stellen Sie sicher, dass alle Steuerungskomponenten erreichbar sind.



Schritt 3: vManage-Cluster erstellen

Integrierte SD-WAN-Fabric mit vManage Cluster im SD-WAN-Overlay

---

Hinweis: Der vManage-Cluster kann je nach Anzahl der in die SD-WAN-Fabric integrierten Standorte mit drei vManage-Knoten oder mit sechs vManage-Knoten konfiguriert werden. Verweisen Sie auf Ihren vorhandenen vManage-Cluster, und wählen Sie die Anzahl der

---

Knoten aus.

Konfigurieren der CLI-Konfigurationen aller vManage-Knoten im Cluster

Konfiguration der Systemkonfiguration auf allen vManage-Knoten

- Konfigurieren Sie den Rest der vManage-Knoten. Im Falle eines Clusters mit drei Knoten müssen Sie noch zwei Knoten konfigurieren, im Falle eines Clusters mit sechs Knoten müssen Sie fünf Knoten konfigurieren.
- Konfigurieren Sie die Systemkonfigurationen wie folgt:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Hinweis: Wenn wir eine URL als vBond-Adresse verwenden, stellen Sie sicher, dass die IP-Adressen des DNS-Servers in der VPN 0-Konfiguration konfiguriert sind, oder dass sie aufgelöst werden können.

Konfigurieren der Transportschnittstelle auf allen vManage-Knoten

Diese Konfigurationen werden benötigt, um die Transportschnittstelle zu aktivieren, über die Steuerverbindungen mit den Routern und den übrigen Controllern hergestellt werden.

```
config t
vpn 0
 dns



        primary
 dns



         secondary
 interface eth1
  ip address



  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0



commit
```

Managementschnittstelle auf allen vManage-Knoten konfigurieren

Konfigurieren Sie außerdem die VPN 512Management-Schnittstelle, um den Out-of-Band-Management-Zugriff auf den Controller zu ermöglichen.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Optionale Konfiguration:

- Sie können die Konfigurationen Ihres vorhandenen Controllers anzeigen. Wenn die hier aufgeführte Konfiguration vorhanden ist, können Sie diese Konfiguration den neuen Controllern hinzufügen.
- Konfigurieren Sie das Steuerungsprotokoll nur dann als TLS, wenn Router sichere Steuerverbindungen mit den vManage-Knoten herstellen müssen, die TLS verwenden. Standardmäßig stellen alle Controller und Router eine Kontrollverbindung mithilfe von DTLS her. Dies ist eine optionale Konfiguration, die je nach Anforderung nur für vSmart- und vManage-Knoten erforderlich ist.

```
Conf t
security
 control
  protocol tls
commit
```

Serviceschnittstelle auf allen vManage-Knoten konfigurieren

Konfigurieren Sie die Service-Schnittstelle auf allen vManager-Knoten, einschließlich vManage-1, das bereits integriert wurde. Diese Schnittstelle wird für die Cluster-Kommunikation verwendet, d. h. die Kommunikation zwischen den vManager-Knoten im Cluster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Stellen Sie sicher, dass dasselbe IP-Subnetz für die Service-Schnittstelle an allen Knoten im vManagement-Cluster verwendet wird.

Cluster-Anmeldeinformationen konfigurieren

Wir können die gleichen Admin-Anmeldedaten von vManagerNodes verwenden, um vManagerCluster zu konfigurieren. Andernfalls können wir eine neue Benutzeranmeldeinformation konfigurieren, die Teil derNetAdmingroup ist. Die Konfigurationen für die Konfiguration neuer Benutzeranmeldeinformationen sind wie folgt:

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

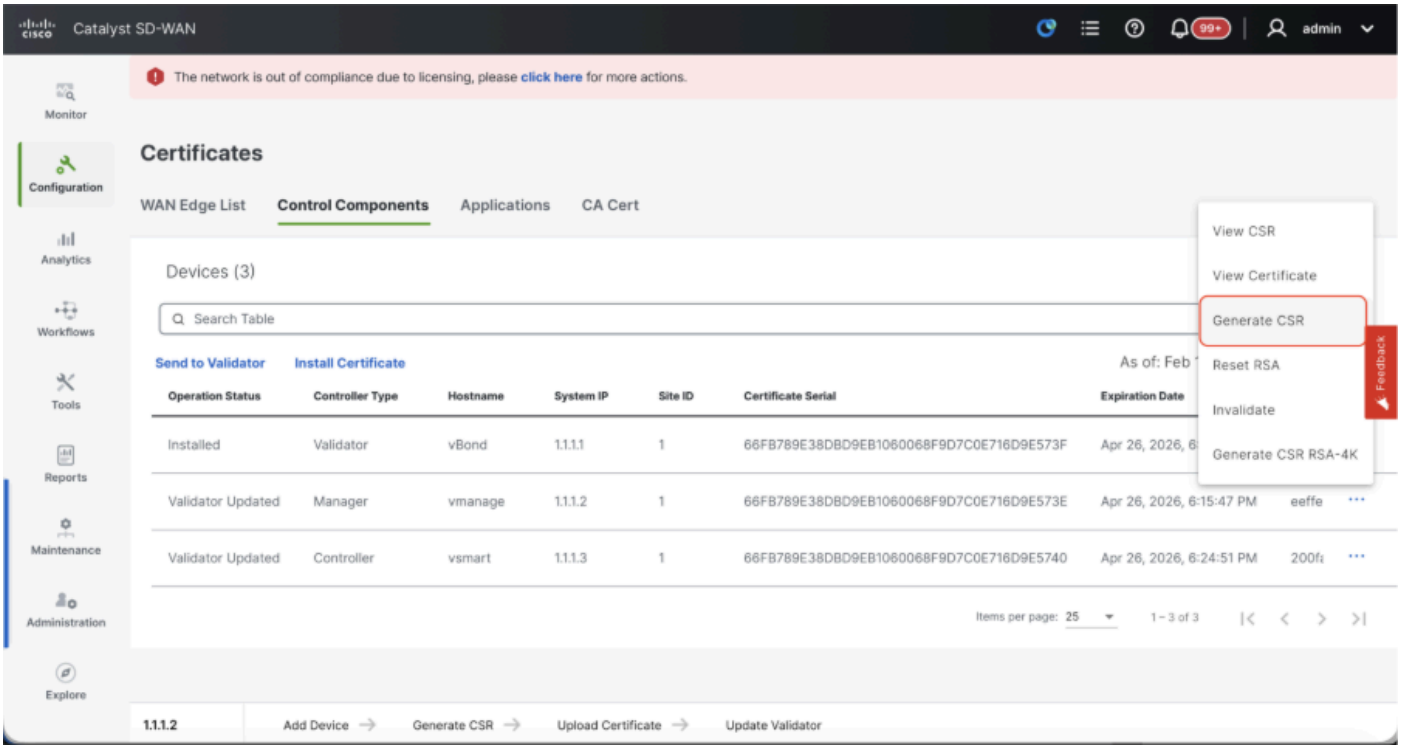
Achten Sie darauf, in allen vManager-Knoten, die Teil des Clusters sind, dieselben

Benutzeranmeldeinformationen zu konfigurieren.Wenn wir die Admin-Anmeldedaten verwenden möchten, müssen in allen vManager-Knoten dieselben Benutzernamen und Kennwörter verwendet werden.

Gerätezertifikat auf allen vManage-Knoten installieren

- Melden Sie sich bei der vManageUI aller vManager-Knoten über die URL https://<vmanage-ip>in Ihrem Browser an. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManager-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

  Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.
- Wenn Manual (Manuell) ausgewählt ist, signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren. Dasselbe Verfahren gilt für die Verwendung des Digicert- und Enterprise-Root-Zertifikats.

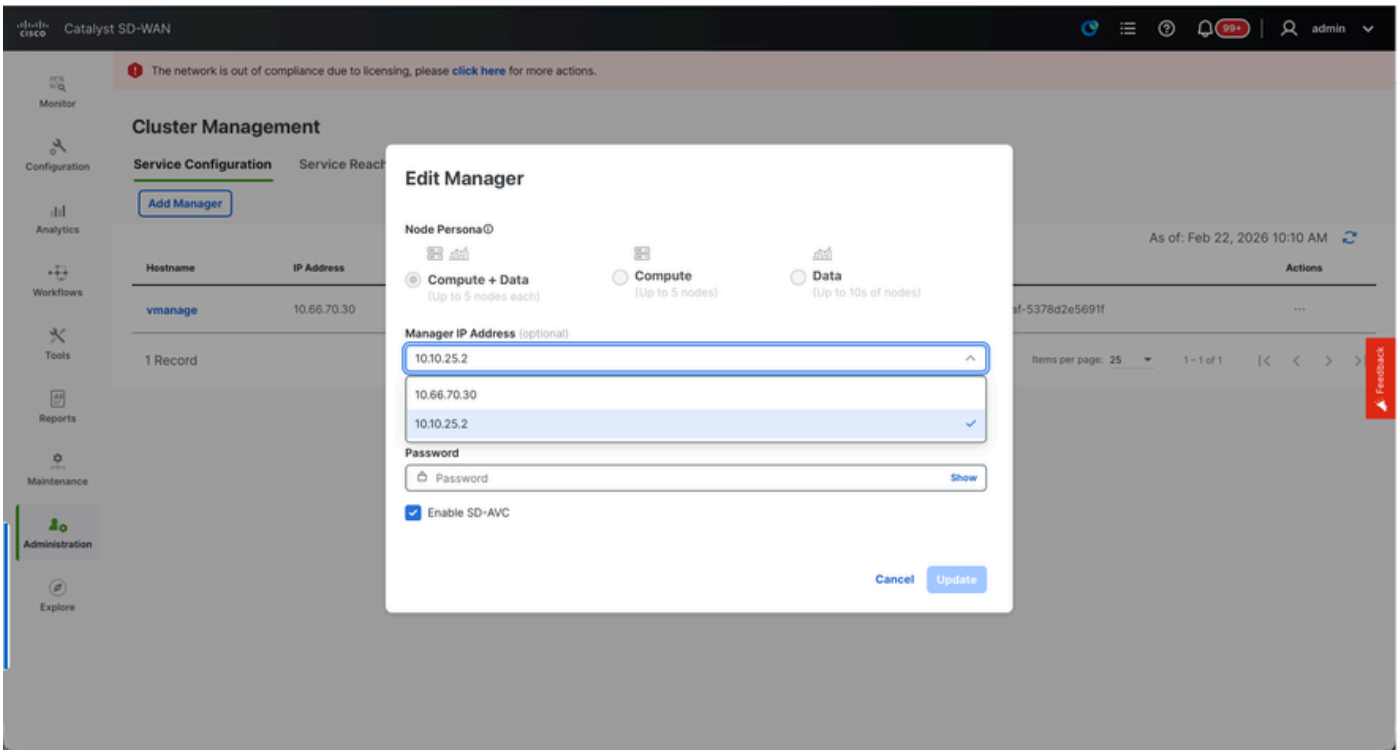
- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.
- Führen Sie diesen Schritt für alle vManage-Knoten aus, die Teil des Clusters sind.

Vorbereiten des vManage-Clusters

- Navigieren Sie auf der Web-UI von vManage-1 zu Administration > Cluster Management, klicken Sie auf ... unter Actions for vManage-1 (Aktionen für vManage-1) und wählen Sie Edit (Bearbeiten).
- Die Knoten-Persona wird automatisch auf Basis der Persona ausgewählt, die wir beim Hochfahren der VM ausgewählt haben.

Anmerkung: Bei einem Cluster mit drei Knoten werden alle drei vManage-Knoten mit "compute+data" als Rolle aufgerufen.

- Bei einem Cluster mit sechs Knoten werden drei vManage-Knoten mit "compute+data" als persona und drei vManage-Knoten mit "data" als persona aktiviert.
- Wählen Sie aus dem Dropdown-Menü für die Manager-IP-Adresse die Service-Schnittstellen-IP von vManage aus.

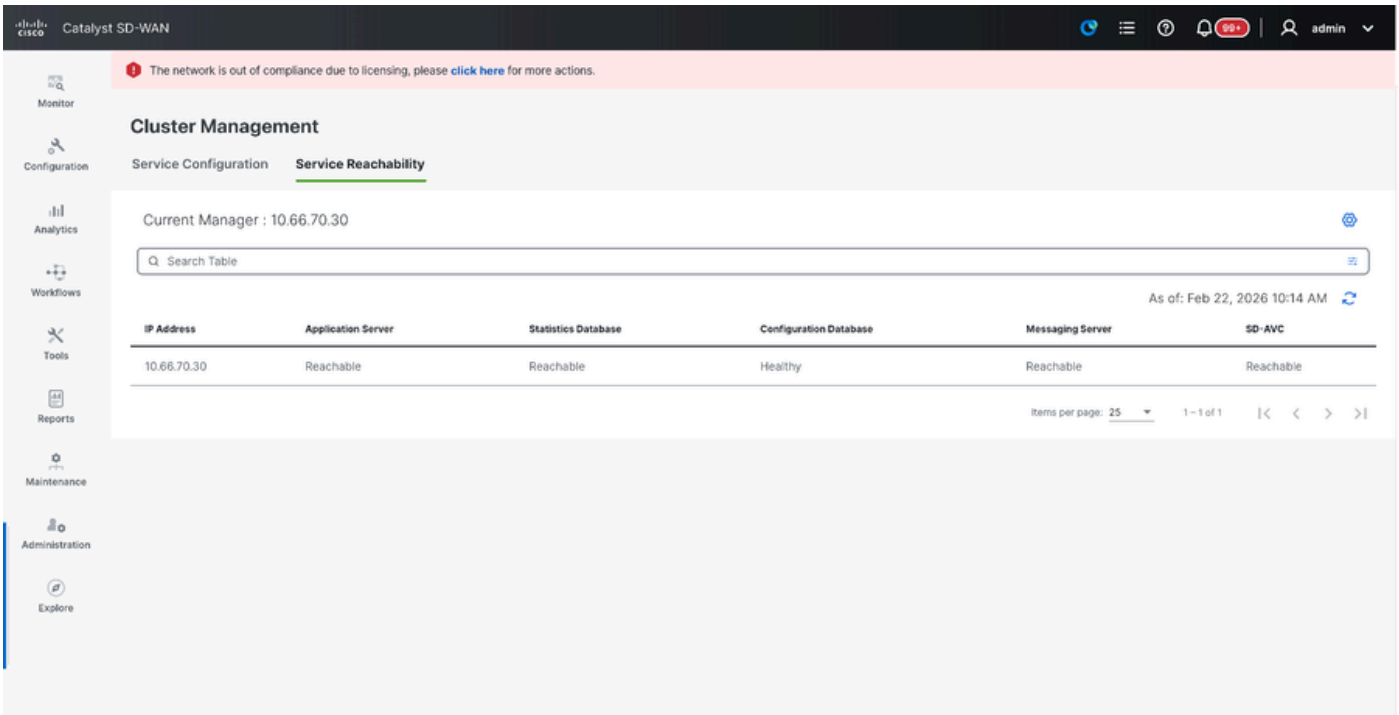


- Geben Sie den Benutzernamen und das Passwort ein, mit denen Sie den vManage-Cluster aktivieren möchten, der als Cluster-Anmeldedaten bezeichnet wird.
- Wie bereits erwähnt, müssen auf allen vManage-Knoten dieselben Anmeldeinformationen konfiguriert und beim Hinzufügen aller Knoten zum Cluster verwendet werden.

Anmerkung: Informationen zur Aktivierung von SDAVC finden Sie in der Konfiguration Ihres vorhandenen Clusters. Sie müssen nur aktiviert werden, wenn dies erforderlich ist und nur auf einem vManage-Knoten des Clusters erforderlich ist.

Klicken Sie auf Aktualisieren.

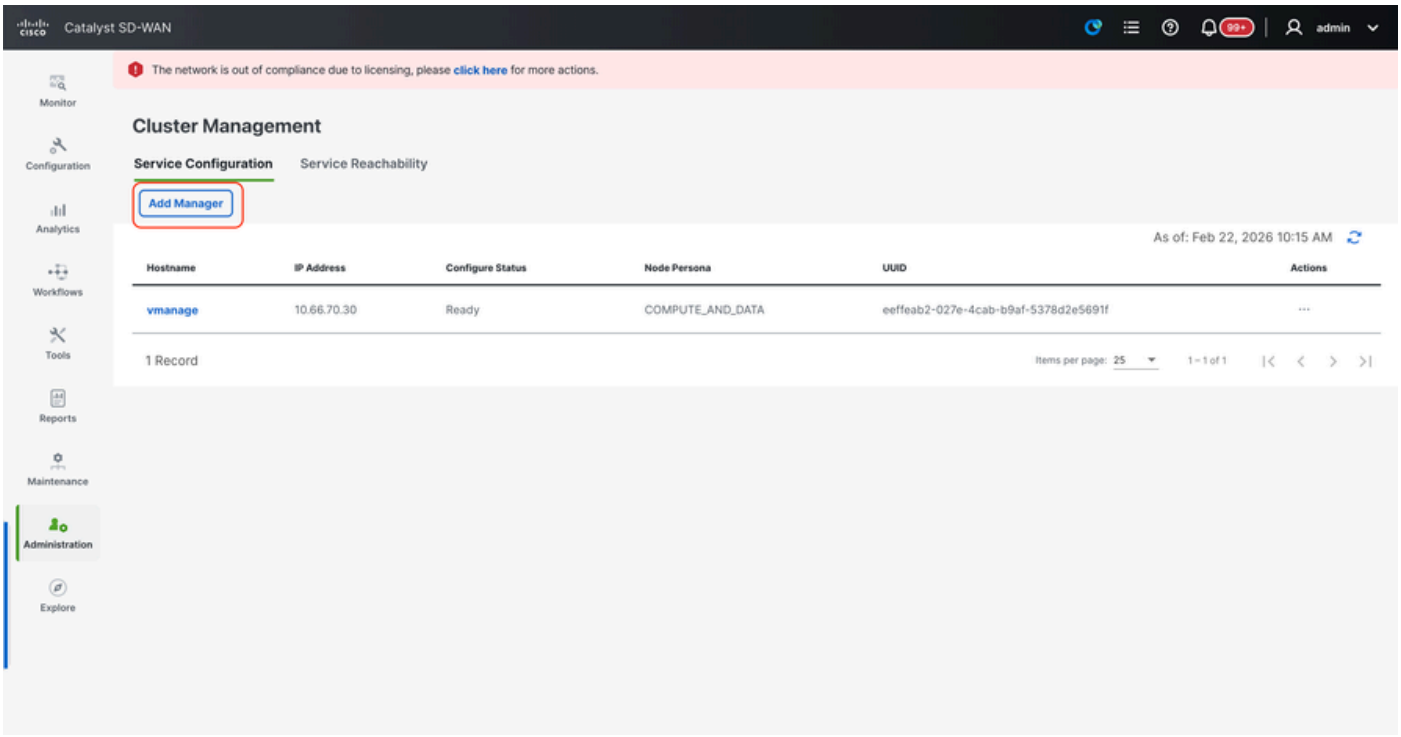
- Nach diesem Vorgang wird der vManage NMS-Dienst im Hintergrund neu gestartet, und die Benutzeroberfläche ist für einige Minuten (etwa 5 bis 10 Minuten) nicht verfügbar. Während dieser Zeit ist der CLI-Zugriff von vManage verfügbar.
- Sobald auf die vManage-1-Benutzeroberfläche zugegriffen werden kann, navigieren Sie zu Administration > Cluster Management, stellen Sie sicher, dass die IP-Adresse der Service-Schnittstelle von vManage unter der IP-Adresse angezeigt wird.Der Konfigurationsstatus lautet "Ready", und die Node-Persona wird korrekt wiedergegeben.
- Wechseln Sie zum Abschnitt "Erreichbarkeit von Services" auf derselben Seite, und stellen Sie sicher, dass alle Services erreichbar sind.

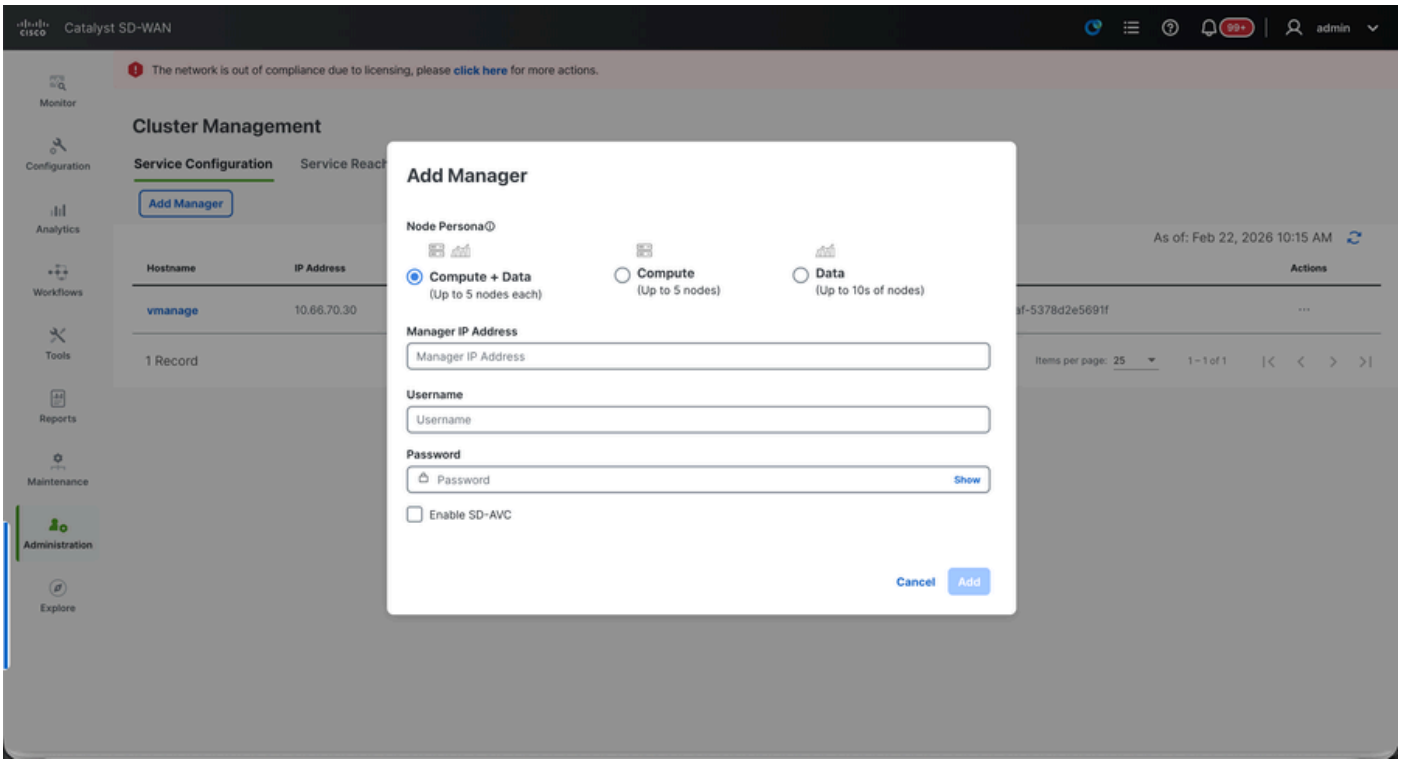


- Wenn wir sehen, dass einer der Dienste noch nicht erreichbar ist, warten Sie bitte. In der Regel dauert etwa 20 bis 30 Minuten.

Aufbau des vManage-Clusters

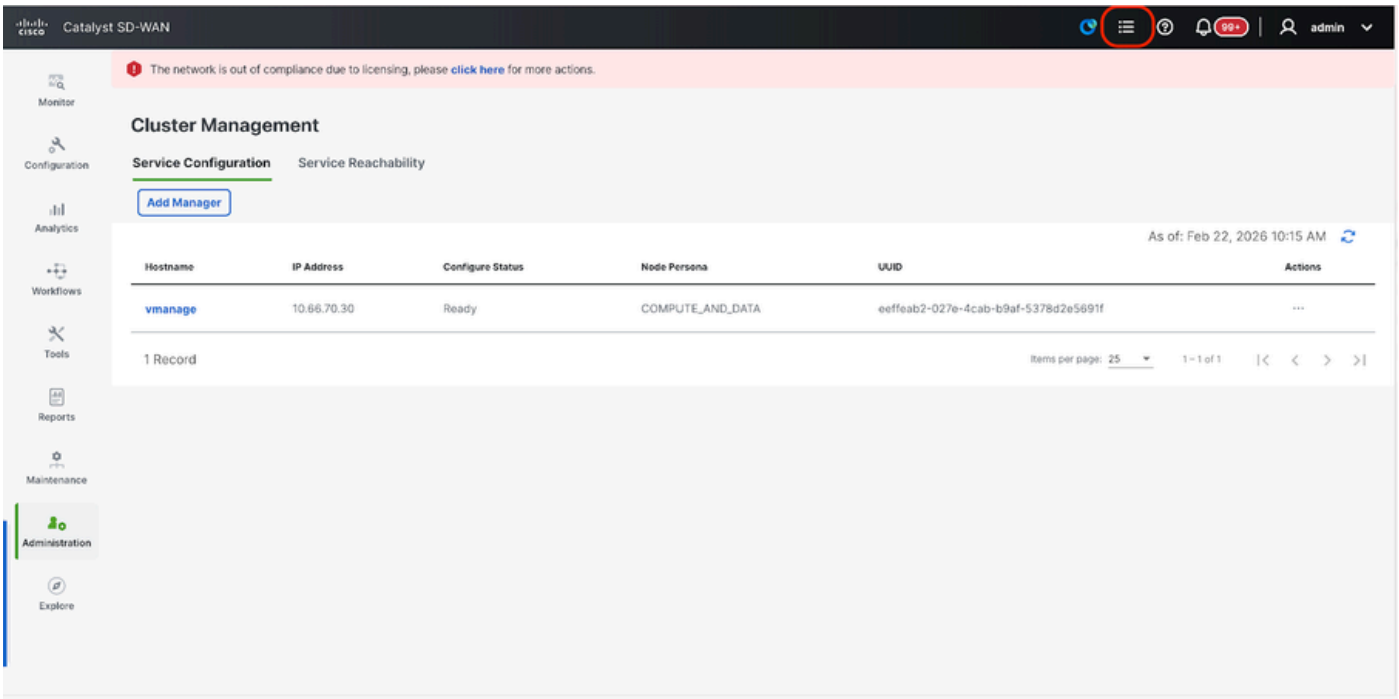
- Navigieren Sie auf der Web-Benutzeroberfläche von vManage-1 zu Administration > Cluster Management, im Abschnitt Service Configuration,
- Klicken Sie auf Add Manager, um ein Popup-Fenster anzuzeigen:





- Wählen Sie den Knoten persona basierend auf den persönlichen Konfigurationen aus, die während der Aktivierung von vManage - 2 durchgeführt wurden.
- Geben Sie die IP-Adresse der Service-Schnittstelle von vManage-2 unter der Manager-IP-Adresse ein.
- Geben Sie den Benutzernamen und das Kennwort ein. Dies sind die gleichen Anmeldeinformationen wie in Schritt 6.
- SDAVC aktivieren: Deaktivieren Sie diese Option, da sie bereits in vManage-1 aktiviert ist.
- Klicken Sie auf Hinzufügen.
- Nach diesem Schritt werden die vManage NMS-Dienste für vManage 1- und 2-Knoten im

Hintergrund neu gestartet. Die Benutzeroberfläche ist für einige Minuten von etwa 5 bis 10 Minuten für vManage 1 und 2 nicht verfügbar.
- Während dieser Zeit ist der CLI-Zugriff von vManage 1 und 2 verfügbar.
- Sobald auf die vManage-1-Benutzeroberfläche zugegriffen werden kann, navigieren Sie zu Administration > Cluster Management, stellen Sie sicher, dass die Service-Schnittstellen-IP des vManage unter der IP-Adresse angezeigt wird, der Konfigurationsstatus "Ready" lautet und die Knoten-IP-Adresse korrekt wiedergegeben wird.
- Wechseln Sie zum Abschnitt "Service-Erreichbarkeit" auf derselben Seite, und stellen Sie sicher, dass alle Services für beide vManage-Knoten erreichbar sind.
- Wenn wir sehen, dass einer der Dienste noch nicht erreichbar ist, warten Sie bitte. In der Regel dauert etwa 5 bis 10 Minuten.
- Sie können den Status des Cluster-Hinzufügevorgangs in der Aufgabenliste überprüfen, die oben rechts auf der vManage-Benutzeroberfläche zur Verfügung steht.



- Sie können nach der Liste "Aktive Task" suchen. Wenn die Task immer noch in der Liste "Aktive Task" aufgeführt ist, weist dies darauf hin, dass die Task noch nicht abgeschlossen ist.
- Sie können auf die Aufgabe klicken, um den Fortschritt der gleichen Aufgabe zu überprüfen. Wenn die Aufgabe nicht in der Liste "Aktive Aufgabe" aufgeführt ist, wechseln Sie zu "Abgeschlossen", und stellen Sie sicher, dass die Aufgabe erfolgreich abgeschlossen wurde.
- Fahren Sie erst mit dem nächsten Schritt fort, nachdem diese Punkte validiert wurden.

Diese Punkte müssen berücksichtigt werden, bevor der nächste Knoten zum Cluster hinzugefügt wird:

Überprüfen Sie diese Punkte auf allen UIs der vManage-Knoten, die dem Cluster bisher hinzugefügt wurden:

- Navigieren Sie zu Monitor > Overview of vManage UI, und stellen Sie sicher, dass die

Anzahl der vManage-Knoten korrekt wiedergegeben wird und in Abhängigkeit von der Anzahl der Knoten, die dem Cluster hinzugefügt wurden, als erreichbar angezeigt wird.

- Navigieren Sie zu Administration > Cluster Management, und stellen Sie sicher, dass die Service-Schnittstellen-IP des vManage unter IP-Adresse, Configure Status is Ready und Node-Personal korrekt wiedergegeben wird.
- Wechseln Sie zum Abschnitt "Service-Erreichbarkeit" auf derselben Seite, und stellen Sie sicher, dass alle Services für beide vManage-Knoten erreichbar sind.

- Bei jedem Hinzufügen eines Knotens zum Cluster werden die NMS-Dienste aller Knoten im Cluster neu gestartet, sodass die Benutzeroberfläche all dieser Knoten für einige Zeit nicht erreichbar ist.
- Je nach Anzahl der Knoten im Cluster kann es länger dauern, bis die Benutzeroberfläche gesichert ist und alle Dienste erreichbar sind.
- Sie können die Aufgabe in der Aufgabenliste oben rechts in der vManage-Benutzeroberfläche überwachen.
- Auf der vManage-Benutzeroberfläche jedes Knotens, der dem Cluster hinzugefügt wurde, müssen alle Router, Vorlagen und Richtlinien angezeigt werden, wenn sie in vManage-1 verfügbar waren.
- Wenn diese Konfigurationen in vManage-1 nicht vorhanden waren, müssen die vBonds und vSmarts, die zu vManage-1 hinzugefügt wurden, sowie die Konfigurationen Administration > Settings für Organisationsname, vBond, Certificate Authorization (Administration > Einstellungskonfigurationen für Organisationsname, vBond, Zertifikatsautorisierung) auf den übrigen vManage-Knoten, die dem Cluster hinzugefügt wurden, angezeigt werden.
- Wiederholen Sie die gleichen Schritte für die übrigen vManage-Knoten.

Führen Sie diesen Schritt aus, nachdem alle Controller integriert wurden:

Schritt 4: Sicherung/Wiederherstellung der Konfig.-DB

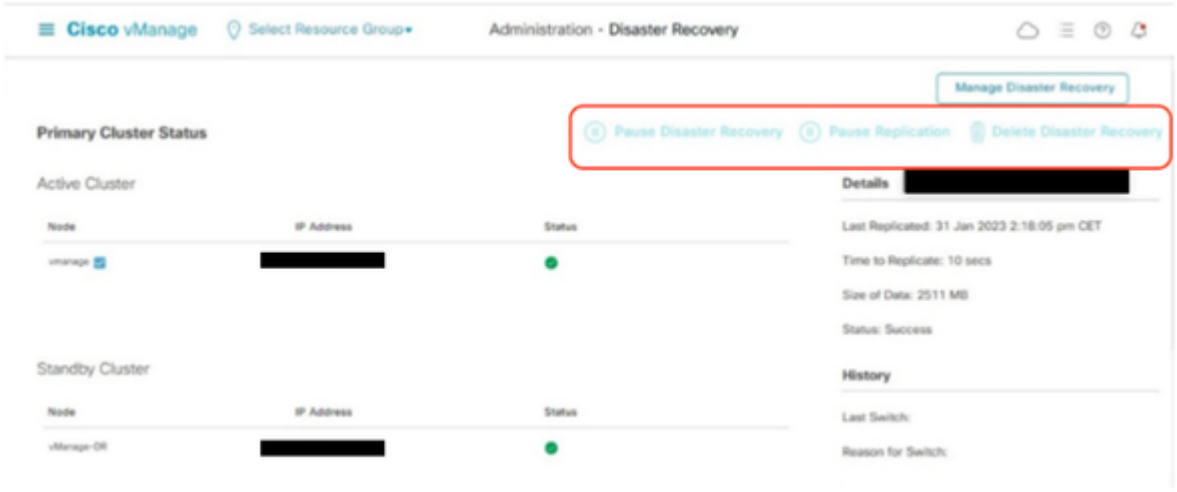
Sammeln von vManage-Konfigurations-DB-Backups und Wiederherstellen auf einem anderen vManage-Knoten

---

Anmerkung: Stellen Sie beim Sammeln des Konfigurations-Datenbank-Backups aus dem vorhandenen vManage-Cluster, in dem die Notfallwiederherstellung aktiviert ist, sicher, dass das Backup gesammelt wird, nachdem die Notfallwiederherstellung auf diesem Knoten angehalten und gelöscht wurde.

Bestätigen Sie, dass keine laufende Disaster Recovery-Replikation vorhanden ist. Navigieren Sie zu Administration > Disaster Recovery und Vergewissern Sie sich, dass der Status "Success" lautet und sich nicht in einem vorübergehenden Status wie "Import Pending" (Ausstehend), "Export Pending" (Ausstehend) oder "Download Pending" (Ausstehend) befindet. Wenn der Status nicht erfolgreich ist, wenden Sie sich an das Cisco TAC, und stellen Sie sicher, dass die Replikation erfolgreich ist, bevor Sie die Disaster Recovery anhalten.

Halten Sie zunächst die Notfallwiederherstellung an, und stellen Sie sicher, dass die Aufgabe abgeschlossen ist. Löschen Sie anschließend die Notfallwiederherstellung, und bestätigen Sie, dass die Aufgabe abgeschlossen ist.



Wenden Sie sich an das Cisco TAC, um sicherzustellen, dass die Notfallwiederherstellung erfolgreich beseitigt wird.

Sammeln der Konfiguration - DB-Backup:

- In der derzeit verwendeten SD-WAN-Fabric können Sie ein Backup der Konfigurationsdatenbank vom vManage-Cluster generieren.
- Bitte beachten Sie, dass wir ein Backup der Konfigurationsdatenbank nur auf einem Knoten des vManage-Clusters generieren müssen, der der führende Konfigurationsdatenbank ist.

- Bei eigenständigem vManage ist dieser vManager selbst der führende Anbieter von Konfigurationsdatenbanken.
- Identifizieren Sie im vManage-Cluster mithilfe des Befehls request nms configuration-db diagnostics den Knoten configuration-db leader.Sie können diesen Befehl auf allen Knoten des vManage-Clusters mit drei Knoten ausführen.
- In einem Cluster mit sechs Knoten muss dieser Befehl auf den vManage-Knoten ausgeführt werden, auf denen configuration-db aktiviert ist, um den Leader-Knoten zu identifizieren. Navigieren Sie zu Administration > Cluster Management, um dies zu überprüfen:
- Wie wir im Screenshot sehen, laufen bei den Knoten, die mit persona COMPUTE_AND_DATA konfiguriert sind, configuration-db.

Dasselbe können Sie mit dem Befehl requestnmsconfiguration-dbstatus in vManageCLI überprüfen. Die Ausgabe erfolgt wie dargestellt

```
vmanage# request nms configuration-db status
NMS configuration database
        Enabled: true
        Status: running PID:32632 for 1066085s
        Native metrics status: ENABLED
```

```
        Server-load metrics status: ENABLED
vmanage#
```

- Nach der Ausführung des Befehlsrequest nms configuration-db diagnostics on these nodes, die Ausgabe ist wie folgt:
- Suchen Sie das hervorgehobene Feld für "IsLeader". Wenn es auf 1 gesetzt ist, bedeutet dies, dass der Knoten der führende Knoten ist, und wir können die Sicherung der Konfigurationsdatenbank von ihm erfassen.

```
vManage-3# request nms configuration-db diagnostics
NMS configuration database
Checking cluster connectivity for ports 7687,7474 ...
Pinging vManage  node 0 on 169.254.1.5:7687,7474...
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2026-02-18 12:41 UTC
SENT (0.0013s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (0.0022s) Handshake with 169.254.1.5:7474 completed
SENT (1.0024s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (1.0028s) Handshake with 169.254.1.5:7687 completed
SENT (2.0044s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (2.0050s) Handshake with 169.254.1.5:7474 completed
SENT (3.0064s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (3.0072s) Handshake with 169.254.1.5:7687 completed
SENT (4.0083s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (4.0091s) Handshake with 169.254.1.5:7474 completed
SENT (5.0106s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (5.0115s) Handshake with 169.254.1.5:7687 completed
Max rtt: 0.906ms | Min rtt: 0.392ms | Avg rtt: 0.724ms
TCP connection attempts: 6 | Successful connections: 6 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 5.01 seconds
Pinging vManage  node 1 on 169.254.2.5:7687,7474...
========== SNIP ==========
Connecting to 10.10.10.3...
+-------------------------------------------------------------------------------------+
| type             | row                                    | attributes[row]["value"] |
+-------------------------------------------------------------------------------------+
| "StoreSizes"     | "TotalStoreSize"                       | 85828934                 |
| "PageCache"      | "Flush"                                | 4268666                  |
| "PageCache"      | "EvictionExceptions"                   | 0                        |
| "PageCache"      | "UsageRatio"                           | 0.09724264705882353      |
| "PageCache"      | "Eviction"                             | 2068                     |
| "PageCache"      | "HitRatio"                             | 1.0                      |
| "ID Allocations" | "NumberOfRelationshipIdsInUse"         | 2068                     |
| "ID Allocations" | "NumberOfPropertyIdsInUse"             | 56151                    |
| "ID Allocations" | "NumberOfNodeIdsInUse"                 | 7561                     |
| "ID Allocations" | "NumberOfRelationshipTypeIdsInUse"     | 31                       |
| "Transactions"   | "LastCommittedTxId"                    | 214273                   |
| "Transactions"   | "NumberOfOpenTransactions"             | 1                        |
| "Transactions"   | "NumberOfOpenedTransactions"           | 441742                   |
| "Transactions"   | "PeakNumberOfConcurrentTransactions"   | 11                       |
| "Transactions"   | "NumberOfCommittedTransactions"        | 414568                   |
| "Causal Cluster" | "IsLeader"                             | 1         >>>>>>>>>      |
| "Causal Cluster" | "MsgProcessDelay"                      | 0                        |
| "Causal Cluster" | "InFlightCacheTotalBytes"              | 0                        |
+-------------------------------------------------------------------------------------+
18 rows
ready to start consuming query after 388 ms, results consumed after another 13 ms
```

```
Completed
Connecting to 10.10.10.3...
Displaying the Neo4j Cluster Status
+-----------------------------------------------------------------------------------------------------------------
| name     | aliases | access       | address            | role       | requestedStatus | currentStatus
+-----------------------------------------------------------------------------------------------------------------
| "neo4j"  | []      | "read-write" | "169.254.3.5:7687" | "leader"   | "online"        | "online"
| "neo4j"  | []      | "read-write" | "169.254.2.5:7687" | "follower" | "online"        | "online"
| "neo4j"  | []      | "read-write" | "169.254.1.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.3.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.2.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.1.5:7687" | "leader"   | "online"        | "online"
+-----------------------------------------------------------------------------------------------------------------
6 rows
ready to start consuming query after 256 ms, results consumed after another 3 ms
Completed
Total disk space used by configuration-db:
60M     .
```

Verwenden Sie diesen Befehl, um das Backup configuration-db vom angegebenen Konfigurationsdb-Leader "vManage" zu erfassen.

```
request nms configuration-db backup path /opt/data/backup/
```

Die erwartete Ausgabe lautet wie folgt:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Notieren Sie sich die Anmeldeinformationen für die Konfigurationsdatenbank, wenn diese aktualisiert wurde.
- Wenn Sie die Anmeldeinformationen für die Konfigurationsdatenbank nicht kennen, wenden Sie sich an das TAC, um die Anmeldeinformationen für die Konfigurationsdatenbank von den vorhandenen vManage-Knoten abzurufen.

- Die Standardanmeldeinformationen für die -db-Konfiguration sind Benutzername: neo4j und Passwort: Kennwort

Wiederherstellen der Konfiguration - db-Sicherung auf einem anderen vManage-Knoten

Kopieren Sie das Sicherungsverzeichnis configuration-db mithilfe von SCP in das Verzeichnis /home/admin/ von vManage.

Beispielausgabe des Befehls scp:

```
XXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Zum Wiederherstellen des "configuration-db"-Backups müssen wir zunächst die "configuration-db"-Anmeldeinformationen konfigurieren. Wenn Ihre Anmeldeinformationen für configuration-db default(neo4j/password) sind, können wir diesen Schritt überspringen.

Um die Anmeldeinformationen für configuration-db zu konfigurieren, verwenden Sie den Befehl request nms configuration-db update-admin-user.Use the username and password of your choice.

Bitte beachten Sie, dass der Anwendungsserver von vManage neu gestartet wurde. Aufgrund dessen kann auf die vManage-Benutzeroberfläche für kurze Zeit nicht mehr zugegriffen werden.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operati
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Nach dem wir fortfahren können, die Konfiguration-db-Backup wiederherzustellen:

Wir können den Befehl request nms configuration-db restore path /home/admin/< > verwenden, um configuration-db auf dem neuen vManage wiederherzustellen:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
```

```
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Reseting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Sobald die Konfigurationsdatenbank wiederhergestellt ist, stellen Sie sicher, dass auf die vManage-Benutzeroberfläche zugegriffen werden kann. Warten Sie etwa 5 Minuten, und versuchen Sie dann, auf die Benutzeroberfläche zuzugreifen.

Nachdem Sie sich erfolgreich bei der Benutzeroberfläche angemeldet haben, stellen Sie sicher, dass die Liste der Edge-Router, die Vorlage, die Richtlinien und alle anderen Konfigurationen, die auf der vorherigen oder vorhandenen vManage-Benutzeroberfläche vorhanden waren, auf der neuen vManage-Benutzeroberfläche wiedergegeben werden.

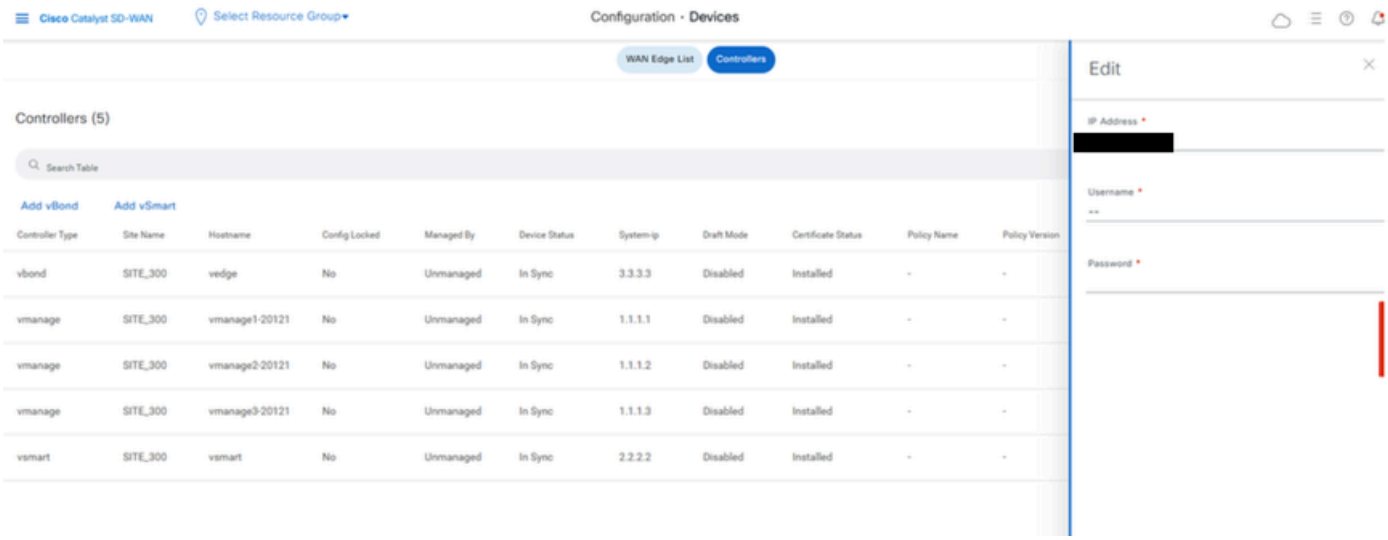
Schritt 5: Neuauthentifizierung von Controllern und Ungültigerklärung alter Controller

Nach der Wiederherstellung der Konfigurationsdatenbank müssen alle neuen Controller (vmanage/vsmart/vbond) im Fabric erneut authentifiziert werden.

Hinweis: Wenn in der Produktion die zur erneuten Authentifizierung verwendete Schnittstellen-IP die Tunnel-Schnittstellen-IP ist, müssen Sie sicherstellen, dass der NETCONF-Dienst auf der Tunnelschnittstelle von vManage, vSmart und vBond sowie auf den Firewalls entlang des Pfads zugelassen ist. Der zu öffnende Firewall-Port ist der TCP-Port 830 als bidirektionale Regel vom DR-Cluster zu allen vBonds und vSmarts .

Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.

- Klicken Sie auf die drei Punkte in der Nähe der einzelnen Controller, und klicken Sie dann auf Bearbeiten.



- Ersetzen Sie die IP-Adresse (System-IP des Controllers) durch die IP-Adresse des Transport-VPN 0 (Tunnelschnittstelle). Geben Sie Benutzername und Kennwort ein, und klicken Sie auf "Save" (Speichern).
- Gleiches für alle neuen Controller im Fabric tun

Synchronisieren der Root-Zertifikatskette

Führen Sie diesen Schritt aus, nachdem alle Controller integriert wurden:

Führen Sie auf einem Cisco SD-WAN Manager-Server im neu aktiven Cluster die folgenden Aktionen aus:

Geben Sie diesen Befehl ein, um das Root-Zertifikat mit allen Cisco Catalyst SD-WAN-Geräten im neu aktiven Cluster zu synchronisieren:

https://vmanage-url/dataservice/system/device/sync/rootcertchain

Geben Sie diesen Befehl ein, um die UUID des Cisco SD-WAN-Managers mit dem Cisco SD-WAN Validator zu synchronisieren:

https://vmanage-url/dataservice/certificate/syncvbond

Sobald die Fabric wiederhergestellt ist und die Steuerungs- und BFD-Sitzungen für alle Edges und Controller in der Fabric verfügbar sind, müssen die alten Controller (vmanage/vsmart/vbond) in der Benutzeroberfläche ungültig gemacht werden.

- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Zertifikate.
- Auf Controller klicken
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Ungültig
- Klicken Sie auf Senden,
- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Löschen.

Schritt 6: Nachprüfungen

Anmerkung: Fahren Sie mit dem hier abgebildeten Abschnitt "Nachprüfungen" fort, der für alle Bereitstellungskombinationen gilt.

Kombination 4: vCluster verwalten + Manuell/Kalt Standby-DR

Was ist Manual/Cold Standby DR ? Der SD-WAN Manager-Backup-Server oder das SD-WAN Manager-Cluster wird im Cold-Standby-Zustand heruntergefahren.

Es werden regelmäßige Sicherungen der aktiven Datenbank durchgeführt. Wenn der primäre SD-WAN-Manager- oder SD-WAN-Manager-Cluster ausfällt, wird der SD-WAN-Manager- oder SD-WAN-Manager-Standby-Cluster manuell aktiviert und die Backup-Datenbank darauf wiederhergestellt.

Erforderliche Instanzen:

- 3 oder 6 vManage (primäres Cluster)
- 3 oder 6 vManage (DR-Standby-Cluster)
- 1 oder mehr vBond (verteilt auf primäre und DR-Rechenzentren)
- 1 oder mehr vSmart (verteilt auf primäre und DR-Rechenzentren)

Schritte:

1. Aufrufen aller Instanzen mithilfe der allgemeinen Schritte
2. Vorabprüfungen
3. Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller
4. vManage-Cluster erstellen
5. Einrichtung des Cold Standby DR-Clusters
6. Sicherung/Wiederherstellung der Konfig.-DB
7. Nachprüfungen

Schritt 1: Vorabprüfungen

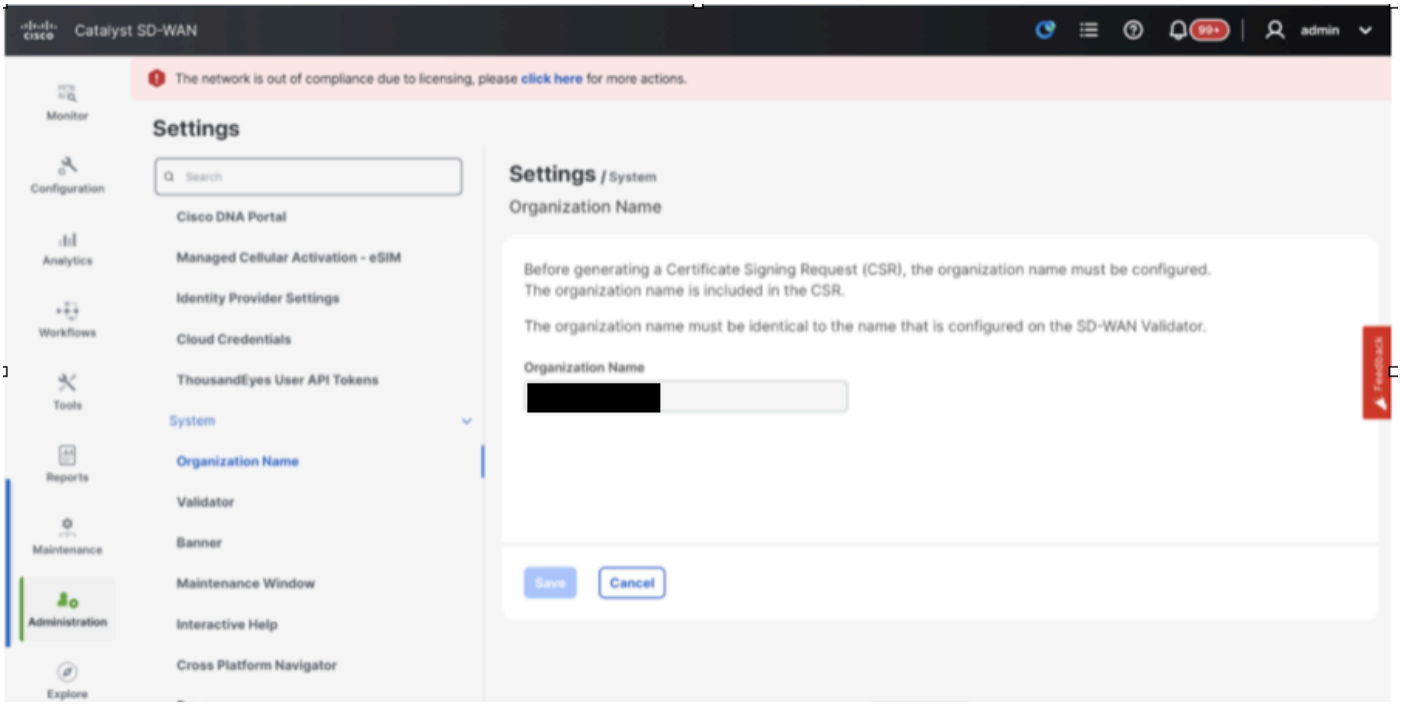
- Stellen Sie sicher, dass die Anzahl der aktiven Cisco SD-WAN Manager-Instanzen mit der Anzahl der neu installierten Cisco SD-WAN Manager-Instanzen identisch ist.
- Stellen Sie sicher, dass auf allen aktiven und neuen Cisco SD-WAN Manager-Instanzen dieselbe Softwareversion ausgeführt wird.
- Stellen Sie sicher, dass alle aktiven und neuen Cisco SD-WAN Manager-Instanzen die Management-IP-Adresse des Cisco SD-WAN Validators erreichen können.
- Stellen Sie sicher, dass die Zertifikate auf den neu installierten Cisco SD-WAN Manager-Instanzen installiert wurden.

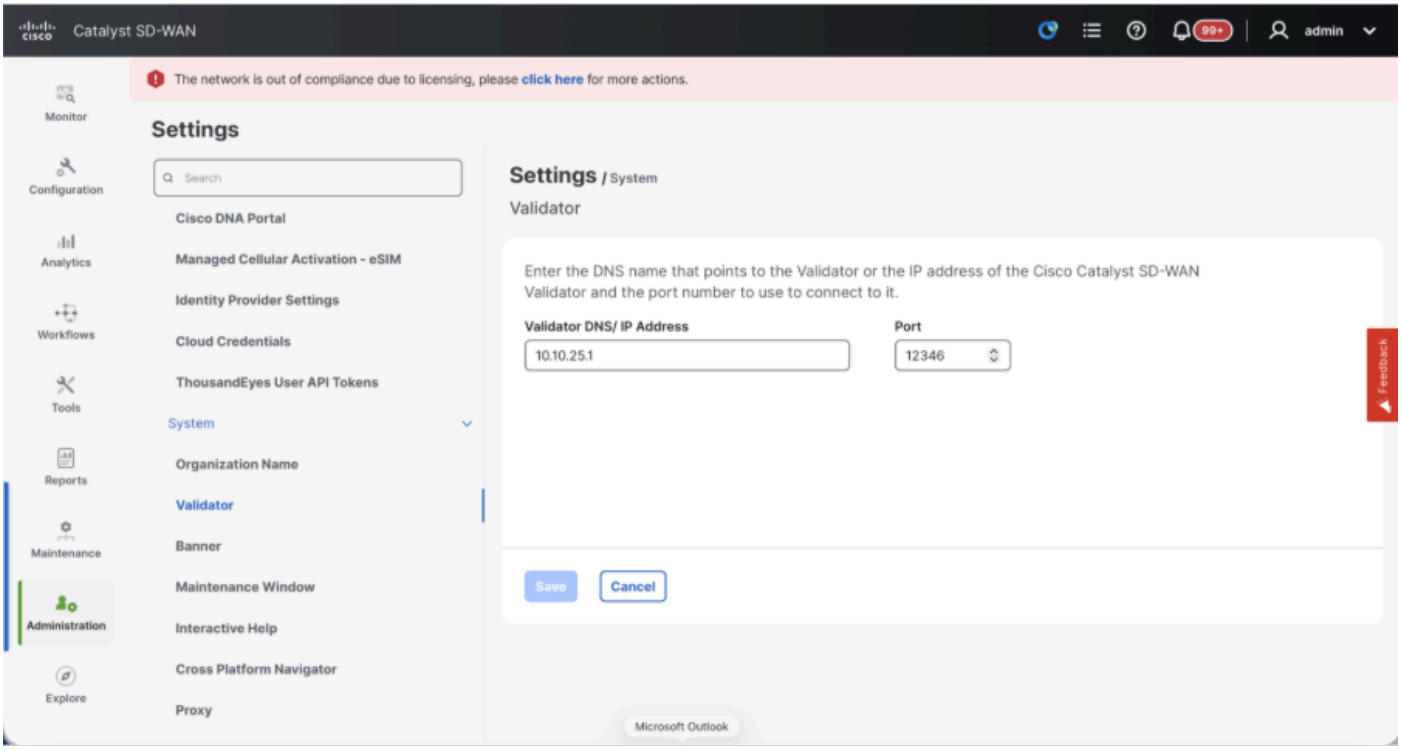
- Stellen Sie sicher, dass die Uhren auf allen Cisco Catalyst SD-WAN-Geräten, einschließlich der neu installierten Cisco SD-WAN Manager-Instanzen, synchronisiert sind.
- Stellen Sie sicher, dass auf den neu installierten Cisco SD-WAN Manager-Instanzen ein neuer Satz von System-IPs und Standort-IDs konfiguriert und die gleiche grundlegende Konfiguration wie im aktiven Cluster verwendet wird.

Phase 2: Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller

Aktualisieren der Konfigurationen der vManage-Benutzeroberfläche

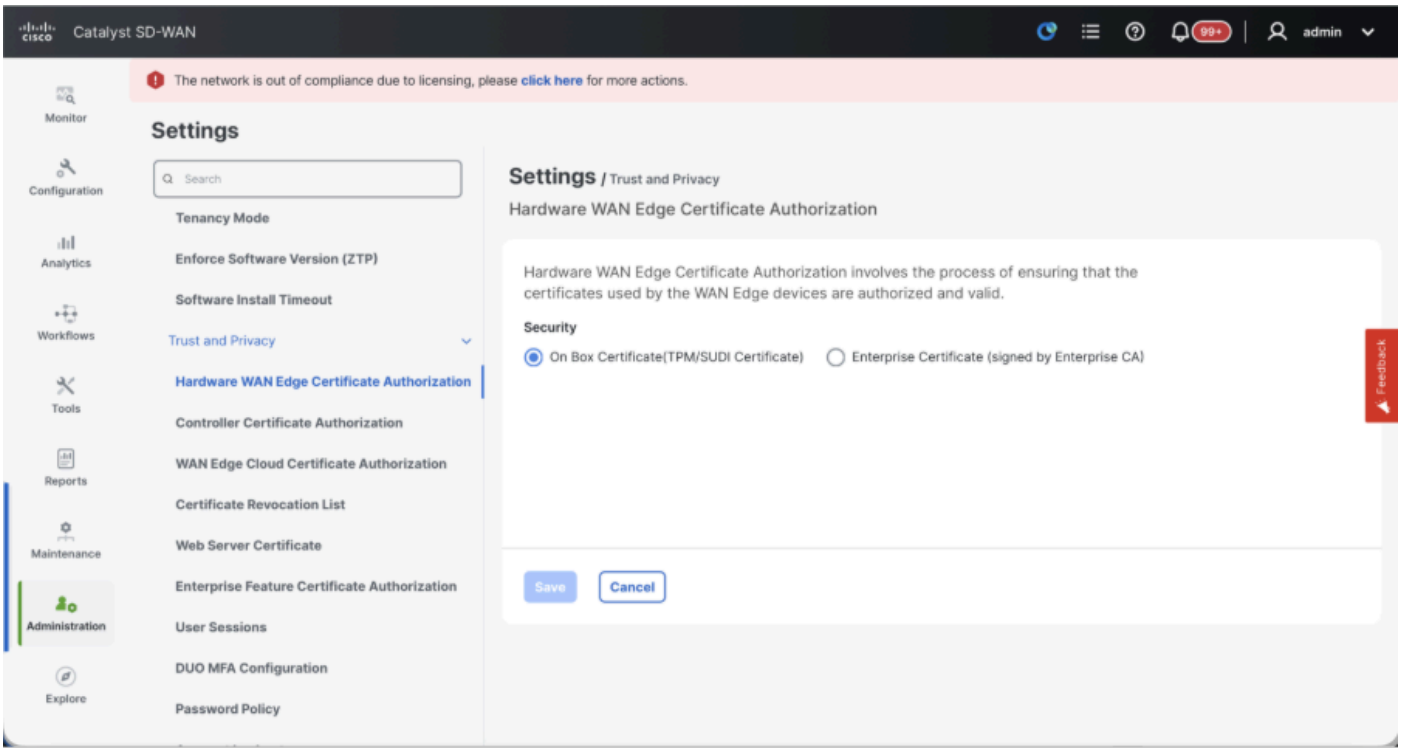
- Sobald die Konfigurationen in Schritt 1 in der CLI aller Controller hinzugefügt wurden, können wir über die URL https://<vmanage-ip> in Ihrem Browser auf die Web-UI von vManage zugreifen. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManage-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Administration > Settings, und führen Sie diese Schritte aus.
- Konfigurieren Sie den Organisationsnamen und die Validator-/vBond-URL/IP-Adresse. Konfigurieren Sie den gleichen Wert wie in der CLI des vManage-Knotens.
- In vManage 20.15/20.18 sind diese Konfigurationen im Abschnitt System verfügbar.



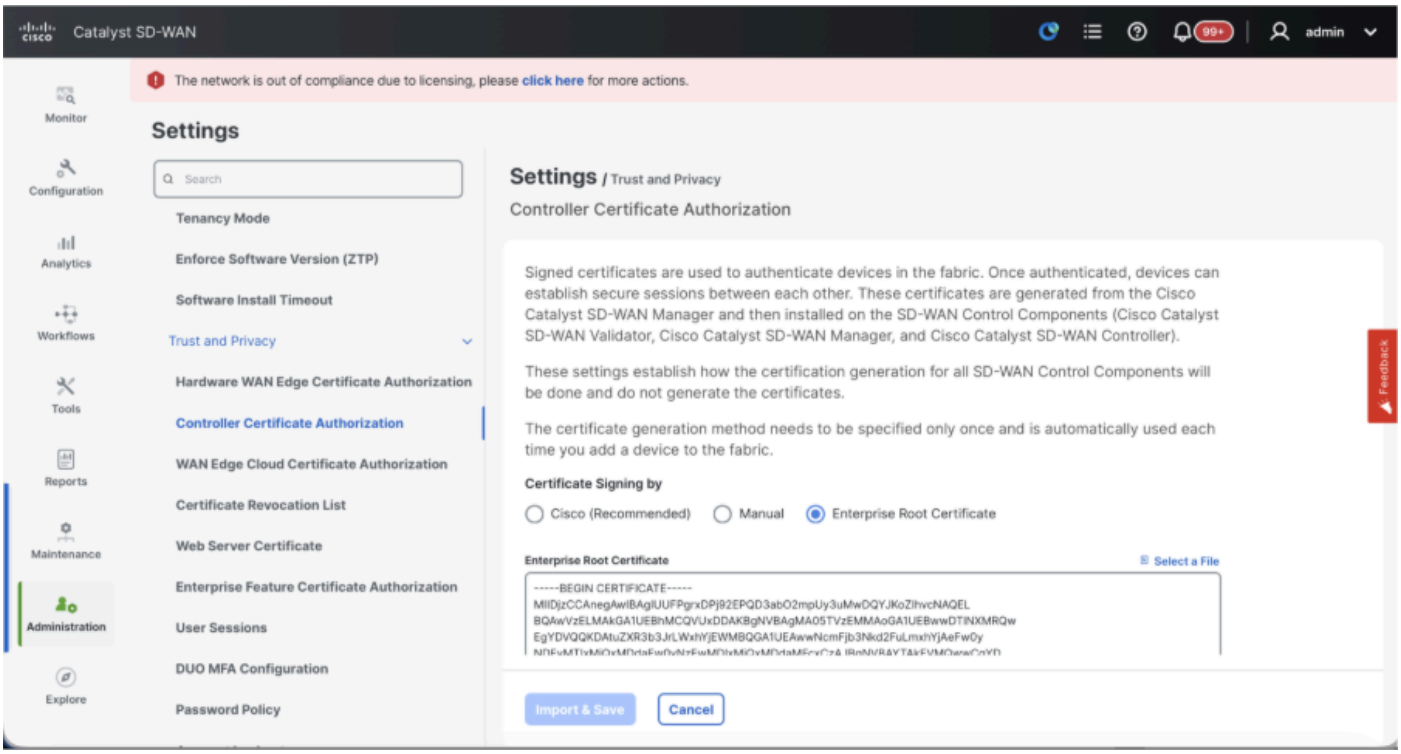


- Überprüfen Sie die Konfigurationen für die Zertifizierungsstelle (Certificate Authorization, CA), die die zum Signieren der Zertifikate verwendete Zertifizierungsstelle bestimmt. Hier sehen wir 3 Optionen:

1. Hardware WAN Edge Certificate Authorization (Hardware-WAN-Edge-Zertifikatsautorisierung): bestimmt die Zertifizierungsstelle für Hardware-SD-WAN-Edge-Router.
    - On Box Certificate (TPM/SUDI Certificate) - Mit dieser Option wird das vorinstallierte Zertifikat auf der Router-Hardware verwendet, um die Steuerverbindungen (TLS-/DTLS-Verbindungen) herzustellen.
    - Enterprise-Zertifikat (von der Enterprise-Zertifizierungsstelle signiert) - Bei dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

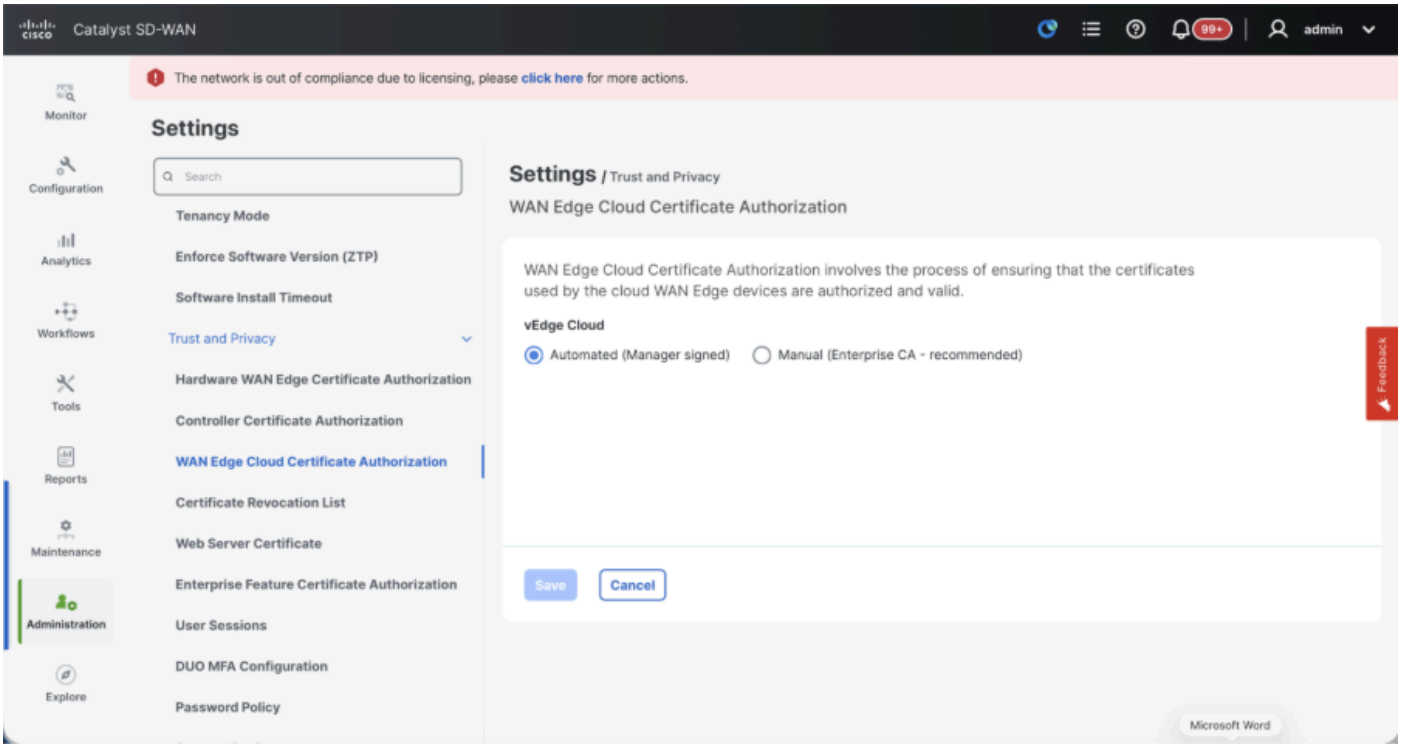


2. Controller Certificate Authorization (Controller-Zertifikatautorisierung): bestimmt die Zertifizierungsstelle für SD-WAN-Controller
    - Cisco (empfohlen) - Controller verwenden die von der Cisco PKI signierten Zertifikate. vManage kontaktiert das PNP-Portal automatisch mit den Smart Account-Anmeldedaten, die auf dem vManage konfiguriert sind. Das Zertifikat wird signiert und auf dem Controller installiert.
    - Manual (Manuell) - Controller verwenden die von der Cisco PKI signierten Zertifikate. Signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren.
    - Enterprise-Stammzertifikat - Mit dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

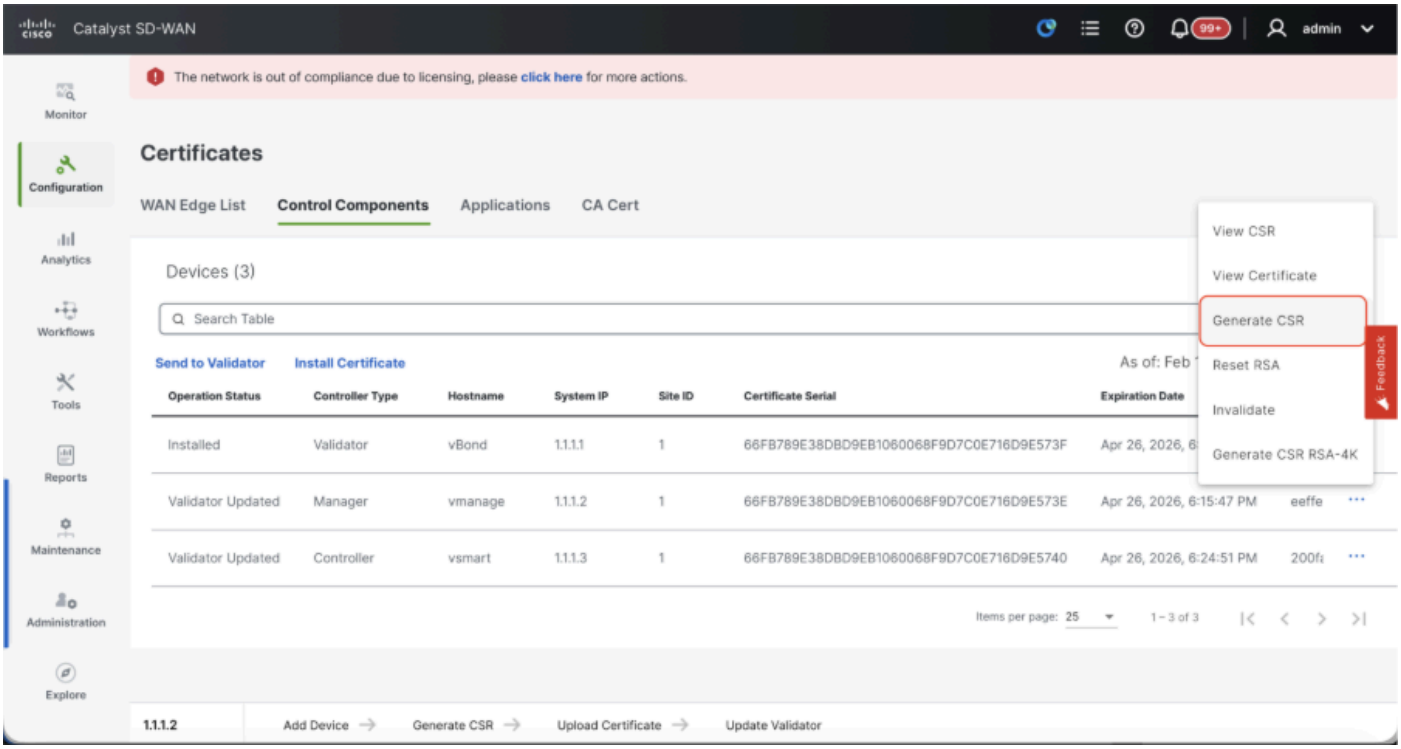


3. WAN-Edge-Cloud-Zertifikatautorisierung - bestimmt die Zertifizierungsstelle für virtuelle SD-WAN-Edge-Router (CSR1000v, C8000v, vEdge-Cloud)
    - Automated (vManage signiert) - vManage signiert automatisch den CSR für die virtuellen Edge-Router und installiert das Zertifikat auf dem Router.
    - Manuell (Enterprise CA - empfohlen) - Virtuelle Router verwenden Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

Wenn Sie eine eigene Zertifizierungsstelle (CA) oder eine Enterprise-Zertifizierungsstelle verwenden, wählen Sie Enterprise aus.



- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller
- Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

Integration von vBond/Validator und vSmart/Controller in vManage

Navigieren Sie zu Configuration > Devices > Control Components (Konfiguration > Geräte > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

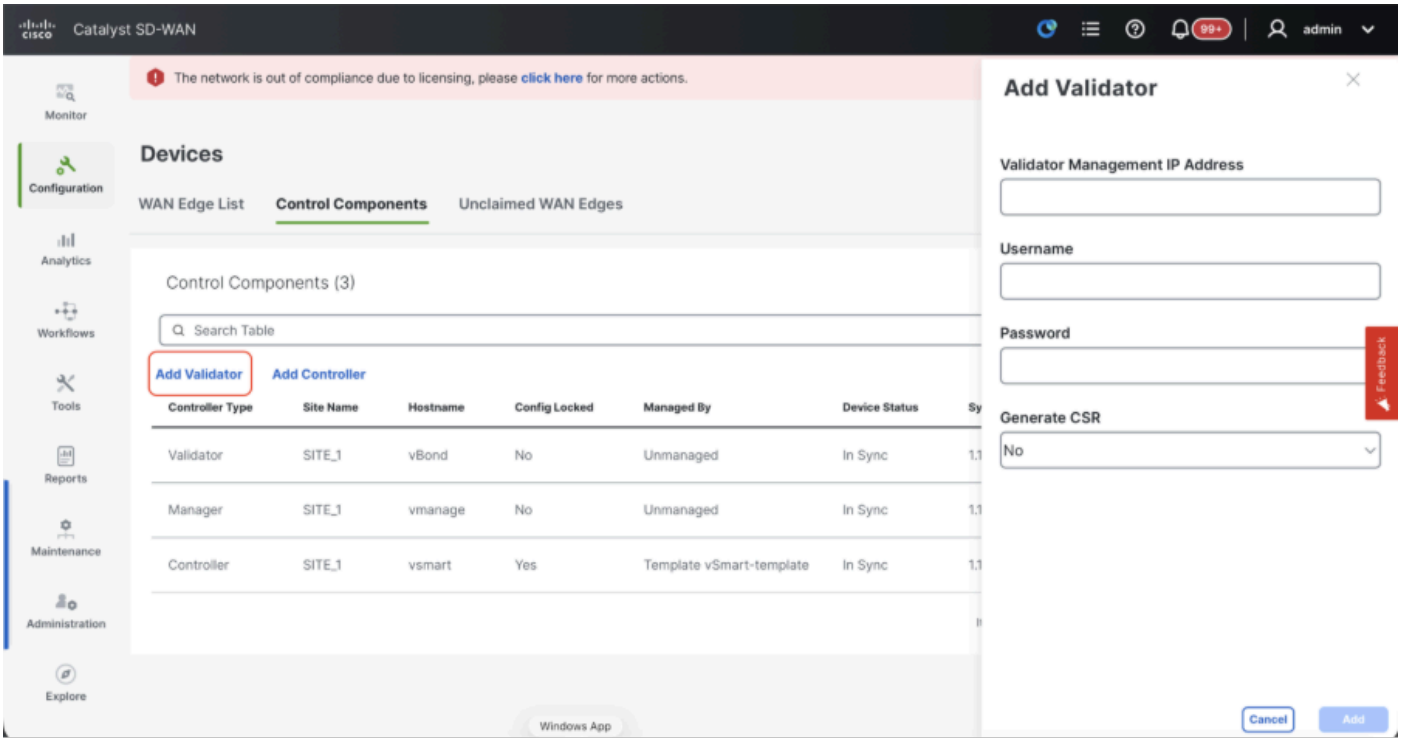
IntegrierenvBond/Validator

- Klicken Sie auf AdvBond.bei 20.12vManagerValidator hinzufügenim Fall von

20.15/20.18vManage. Ein Popup-Fenster wird geöffnet, und geben Sie den VPN 0-Transport-IP von vBond, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, falls dies über die CLI von vManagementvBondIP zulässig ist.
- Geben Sie die Anmeldeinformationen für den Benutzer von vBond ein.

Hinweis: Wir müssen Admin-Anmeldedaten von vBond oder einem Benutzerteil von netadmingroup verwenden. Dies können Sie in der CLI von vBond überprüfen. Wählen Sie im Dropdown-Menü "CSR generieren" die Option "Ja", wenn ein neues Zertifikat für vBond installiert werden soll.

Anmerkung: Wenn sich vBond hinter einem NAT-Gerät bzw. einer NAT-Firewall befindet, überprüfen Sie, ob die IP-Adresse der vBond VPN 0-Schnittstelle in eine öffentliche IP-Adresse übersetzt wurde. Wenn die VPN 0-Schnittstellen-IP von vManage aus nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der VPN 0-Schnittstelle.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vBond installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal.

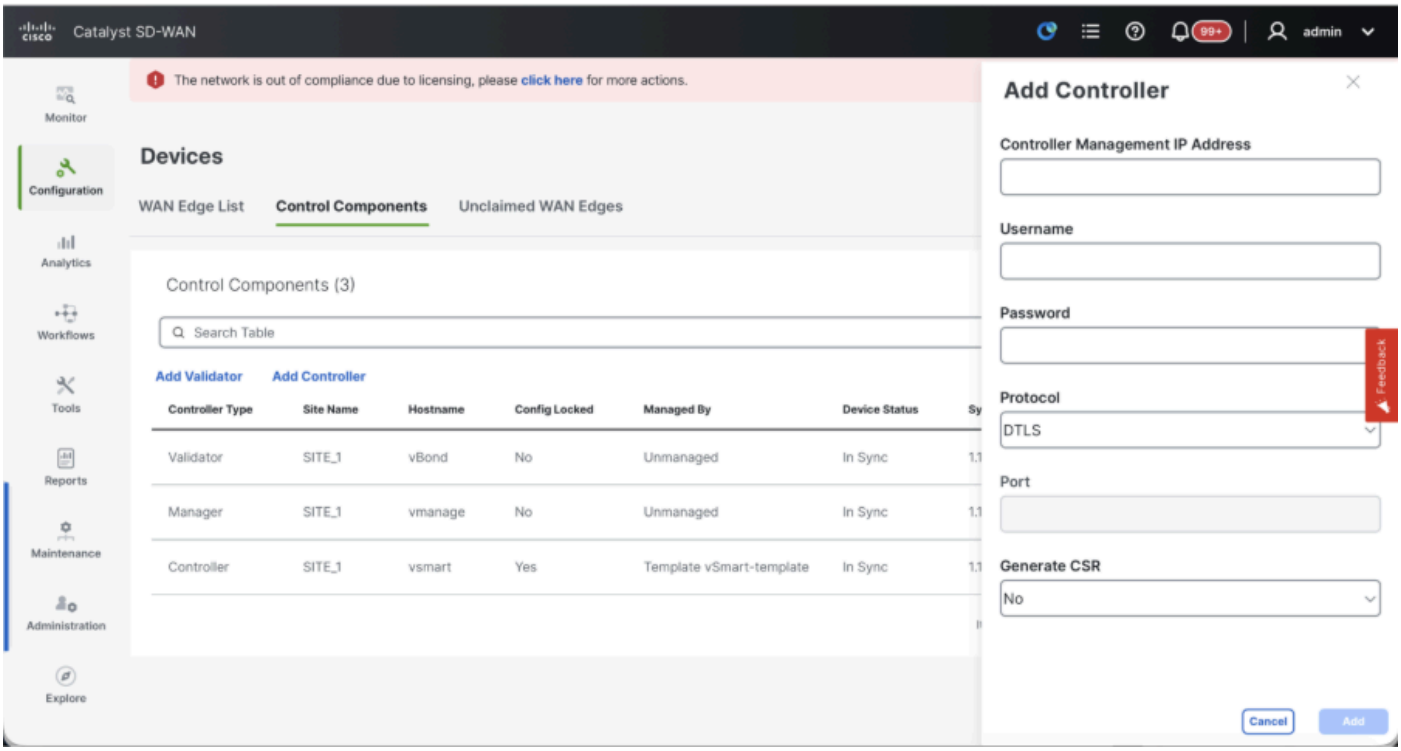
Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

- Wenn mehrere vBonds vorhanden sind, wiederholen Sie die gleichen Schritte.

Integration von vSmart/Controller:

- Klicken Sie auf Add vSmart (vSmart hinzufügen), wenn es sich um 20.12 vManage handelt, oder auf Add Controller (Controller hinzufügen), wenn es sich um 20.15/20.18 vManage handelt.
- Geben Sie in einem Popup-Fenster die VPN 0-Transport-IP von vSmart ein, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, wenn dies von der CLI von vManage zu vSmart IP zulässig ist.
- Geben Sie die Benutzeranmeldeinformationen für vSmart Note ein, die von vSmart oder einem Benutzer der netadmin-Gruppe verwendet werden müssen.
- Sie können dies in der CLI des vSmart überprüfen.
- Legen Sie das Protokoll auf TLS fest, wenn TLS für Router verwendet werden soll, um Steuerverbindungen mit vSmart herzustellen. Diese Konfiguration muss auch für CLI von vSmarts- und vManage-Knoten konfiguriert werden.
- Wählen Sie im Dropdown-Menü "Generate CSR" (CSR generieren) die Option Yes (Ja) aus, wenn ein neues Zertifikat für vSmart installiert werden muss.

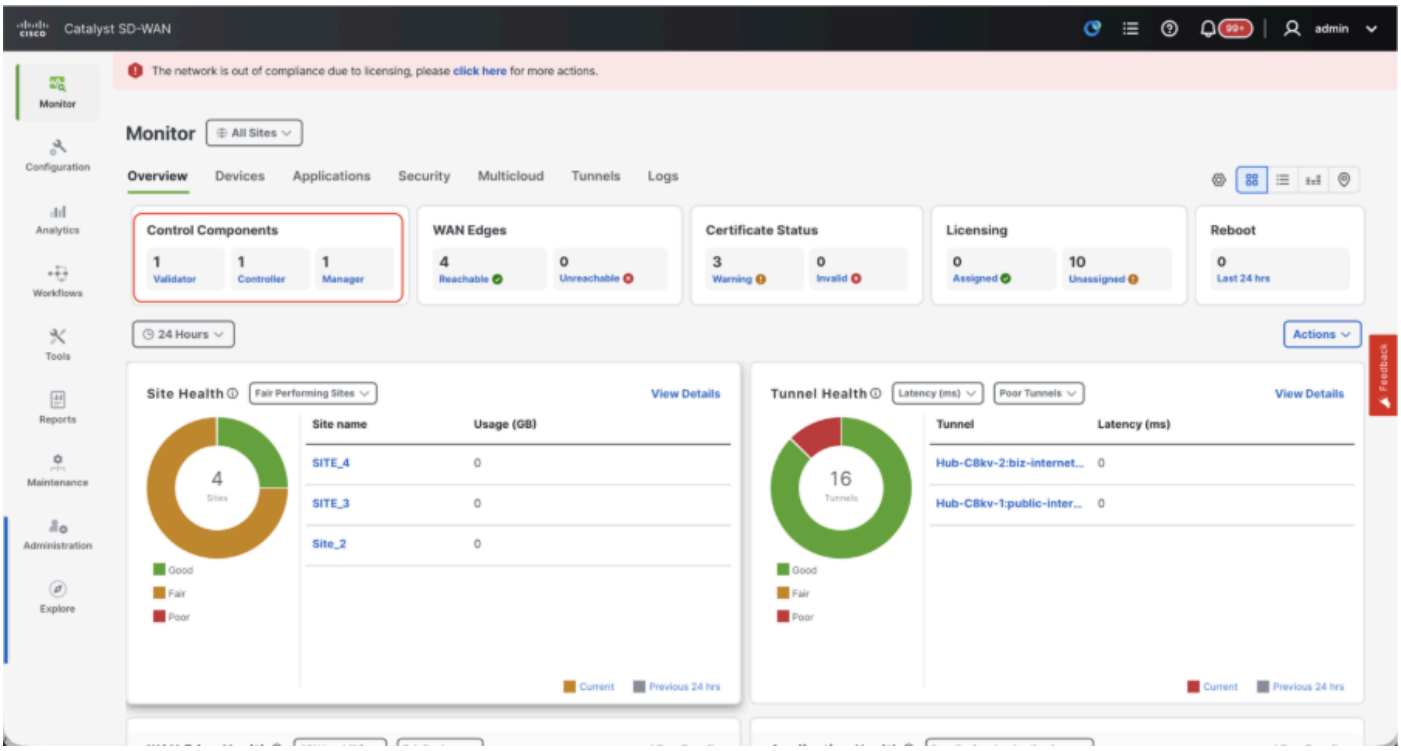
Hinweis: Wenn sich vSmart hinter dem NAT-Gerät/der Firewall befindet, prüfen Sie, ob die IP-Adresse der vSmart VPN 0-Schnittstelle in eine öffentliche IP übersetzt wurde. Wenn die IP-Adresse der VPN 0-Schnittstelle von vManage nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der IP-Adresse der VPN 0-Schnittstelle.



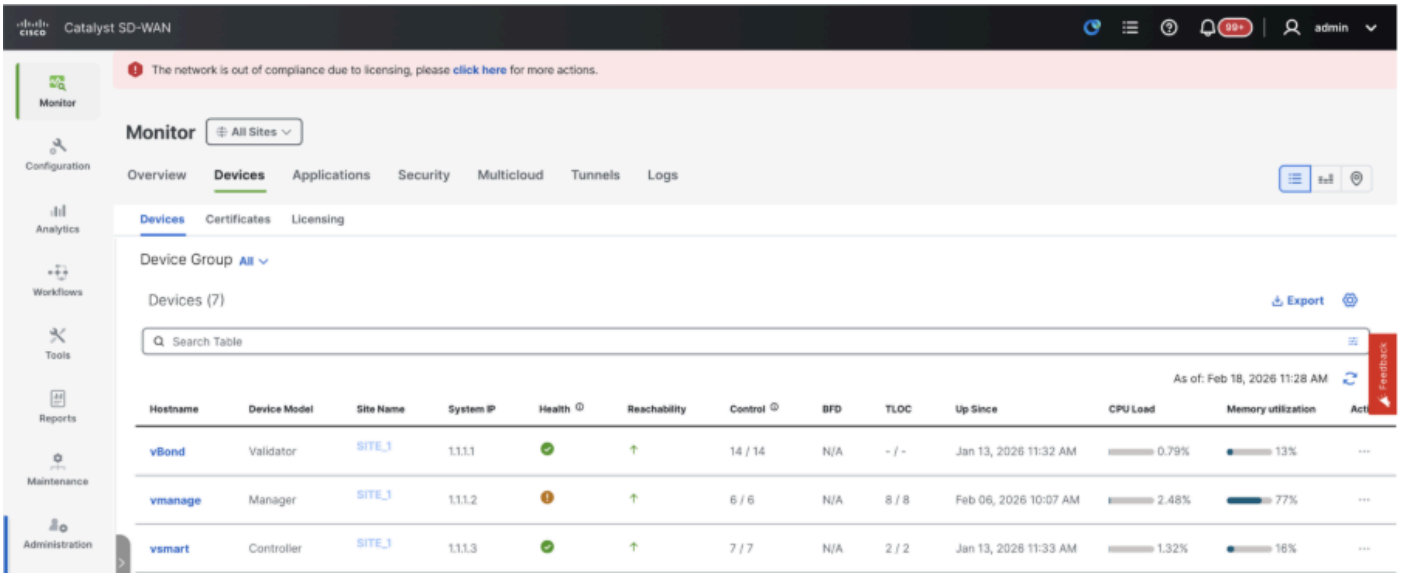
- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf dem vSmart installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays.
- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.
- Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.
- Wenn mehrere vSmarts vorhanden sind, wiederholen Sie die gleichen Schritte.

Verifizierung

Überprüfen Sie nach Abschluss aller Schritte, ob alle Steuerungskomponenten unter Monitor>Dashboard erreichbar sind.



- Klicken Sie auf die jeweiligen Steuerungskomponenten, und vergewissern Sie sich, dass sie alle erreichbar sind.
- Navigieren Sie zu Überwachen > Geräte, und stellen Sie sicher, dass alle Steuerungskomponenten erreichbar sind.



Schritt 3: vManage-Cluster erstellen

Integrierte SD-WAN-Fabric mit vManage Cluster im SD-WAN-Overlay

---

Hinweis: Der vManage-Cluster kann je nach Anzahl der in die SD-WAN-Fabric integrierten Standorte mit drei vManage-Knoten oder mit sechs vManage-Knoten konfiguriert werden.

Integrieren Sie alle SD-WAN-Controller mit einem einzigen vManage-Knoten.

Fahren Sie mit den unter "Integrierte SD-WAN-Controller mit einem einzelnen Knoten vManage im SD-WAN-Overlay" gemeinsam genutzten Schritten fort, um zunächst die SD-WAN-Fabric mit einem vManage-Knoten zu aktivieren und alle erforderlichen Validatoren (vBond) und Controller (vSmart) zu integrieren.

Konfigurieren der CLI-Konfigurationen aller vManage-Knoten im Cluster

- Konfigurieren Sie den Rest der vManage-Knoten. Im Falle eines Clusters mit drei Knoten müssen Sie noch zwei Knoten konfigurieren, im Falle eines Clusters mit sechs Knoten müssen Sie fünf Knoten konfigurieren.
- Konfigurieren Sie die Systemkonfigurationen wie folgt:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Hinweis: Wenn wir eine URL als vBond-Adresse verwenden, stellen Sie sicher, dass die IP-Adressen des DNS-Servers in der VPN 0-Konfiguration konfiguriert sind, oder dass sie aufgelöst werden können.

Diese Konfigurationen werden benötigt, um die Transportschnittstelle zu aktivieren, über die Steuerverbindungen mit den Routern und den übrigen Controllern hergestellt werden.

```
config t
vpn 0
 dns



        primary
 dns



         secondary
 interface eth1
  ip address




  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0



commit
```

Konfigurieren Sie außerdem die VPN 512Management-Schnittstelle, um den Out-of-Band-Management-Zugriff auf den Controller zu ermöglichen.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Optionale Konfiguration:

- Sie können die Konfigurationen Ihres vorhandenen Controllers anzeigen. Wenn die hier aufgeführte Konfiguration vorhanden ist, können Sie diese Konfiguration den neuen Controllern hinzufügen.
- Konfigurieren Sie das Steuerungsprotokoll nur dann als TLS, wenn Router sichere Steuerverbindungen mit den vManage-Knoten herstellen müssen, die TLS verwenden. Standardmäßig stellen alle Controller und Router eine Kontrollverbindung mithilfe von DTLS her. Dies ist eine optionale Konfiguration, die je nach Anforderung nur für vSmart- und vManage-Knoten erforderlich ist.

```
Conf t
security
 control
  protocol tls
commit
```

Serviceschnittstelle auf allen vManage-Knoten konfigurieren

Konfigurieren Sie die Service-Schnittstelle auf allen vManager-Knoten, einschließlich vManage-1, das bereits integriert wurde. Diese Schnittstelle wird für die Cluster-Kommunikation verwendet, d. h. die Kommunikation zwischen den vManager-Knoten im Cluster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Stellen Sie sicher, dass dasselbe IP-Subnetz für die Service-Schnittstelle an allen Knoten im vManagement-Cluster verwendet wird.

Cluster-Anmeldeinformationen konfigurieren

Wir können die gleichen Admin-Anmeldedaten von vManagerNodes verwenden, um vManagerCluster zu konfigurieren. Andernfalls können wir eine neue Benutzeranmeldeinformation konfigurieren, die Teil derNetAdmingroup ist. Die Konfigurationen für die Konfiguration neuer Benutzeranmeldeinformationen sind wie folgt:

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

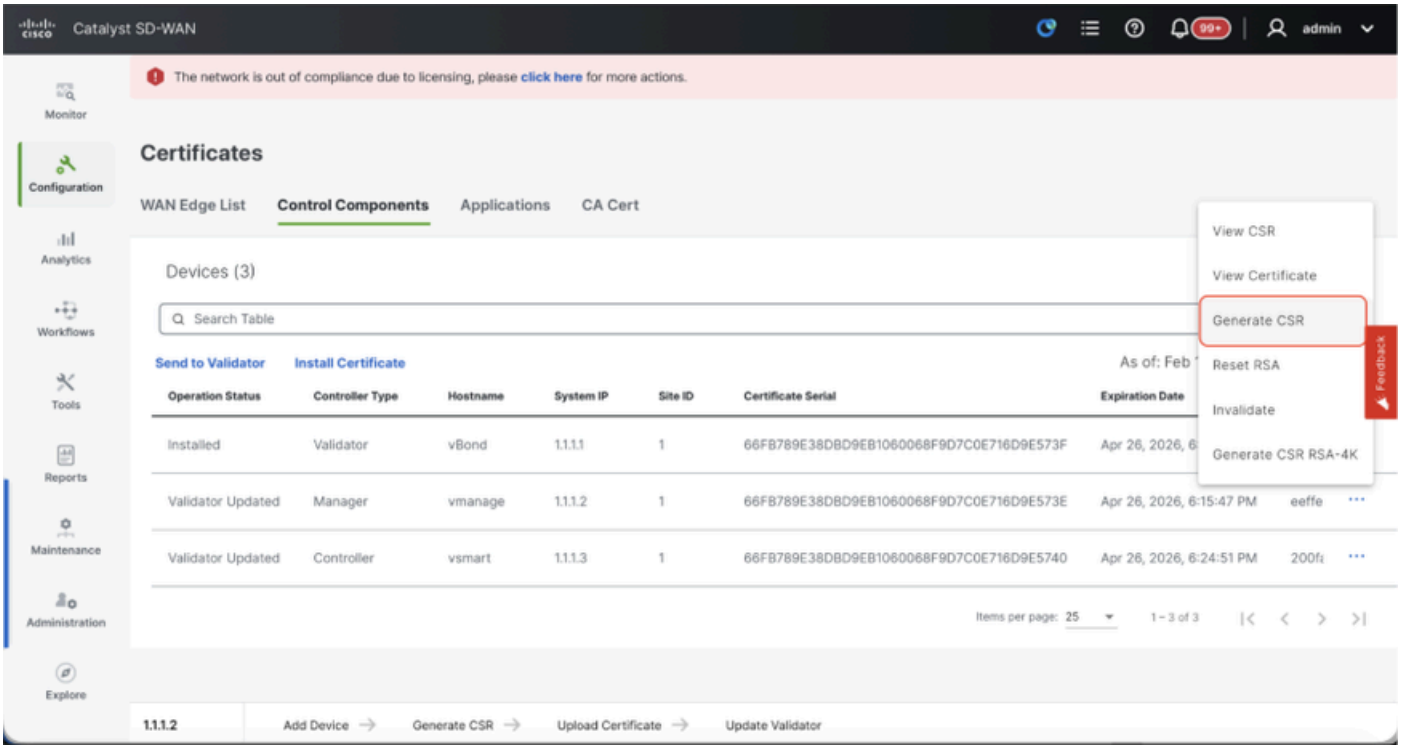
Stellen Sie sicher, dass Sie in allen Managementcodes, die Teil des Clusters sind, dieselben Benutzeranmeldeinformationen konfigurieren.Wenn Sie die Administratoranmeldeinformationen verwenden möchten, müssen Sie in allen Managementcodes denselben Benutzernamen und dasselbe Kennwort verwenden.

Gerätezertifikat auf allen vManage-Knoten installieren

- Melden Sie sich bei der vManageUI aller vManager-Knoten über die URL https://<vmanage-ip>in Ihrem Browser an. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManager-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.

- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

  Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.

- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays.

- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.

- Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.
- Führen Sie diesen Schritt für alle vManage-Knoten aus, die Teil des Clusters sind.

Vorbereiten des vManage-Clusters

- Navigieren Sie auf der Web-UI von vManage-1 zu Administration > Cluster Management, klicken Sie auf ... unter Actions for vManage-1 (Aktionen für vManage-1) und wählen Sie Edit (Bearbeiten).
- Die Knoten-Persona wird automatisch auf Basis der Persona ausgewählt, die wir beim Hochfahren der VM ausgewählt haben.

Anmerkung: Bei einem Cluster mit drei Knoten werden alle drei vManage-Knoten mit "compute+data" als Rolle aufgerufen.

- Bei einem Cluster mit sechs Knoten werden drei vManage-Knoten mit "compute+data" als persona und drei vManage-Knoten mit "data" als persona aktiviert.
- Wählen Sie aus dem Dropdown-Menü für die Manager-IP-Adresse die Service-Schnittstellen-IP von vManage aus.
- Geben Sie den Benutzernamen und das Passwort ein, mit denen Sie den vManage-Cluster aktivieren möchten, der als Cluster-Anmeldedaten bezeichnet wird.
- Wie bereits erwähnt, müssen auf allen vManage-Knoten dieselben Anmeldeinformationen konfiguriert und beim Hinzufügen aller Knoten zum Cluster verwendet werden.

Optionale Konfiguration:

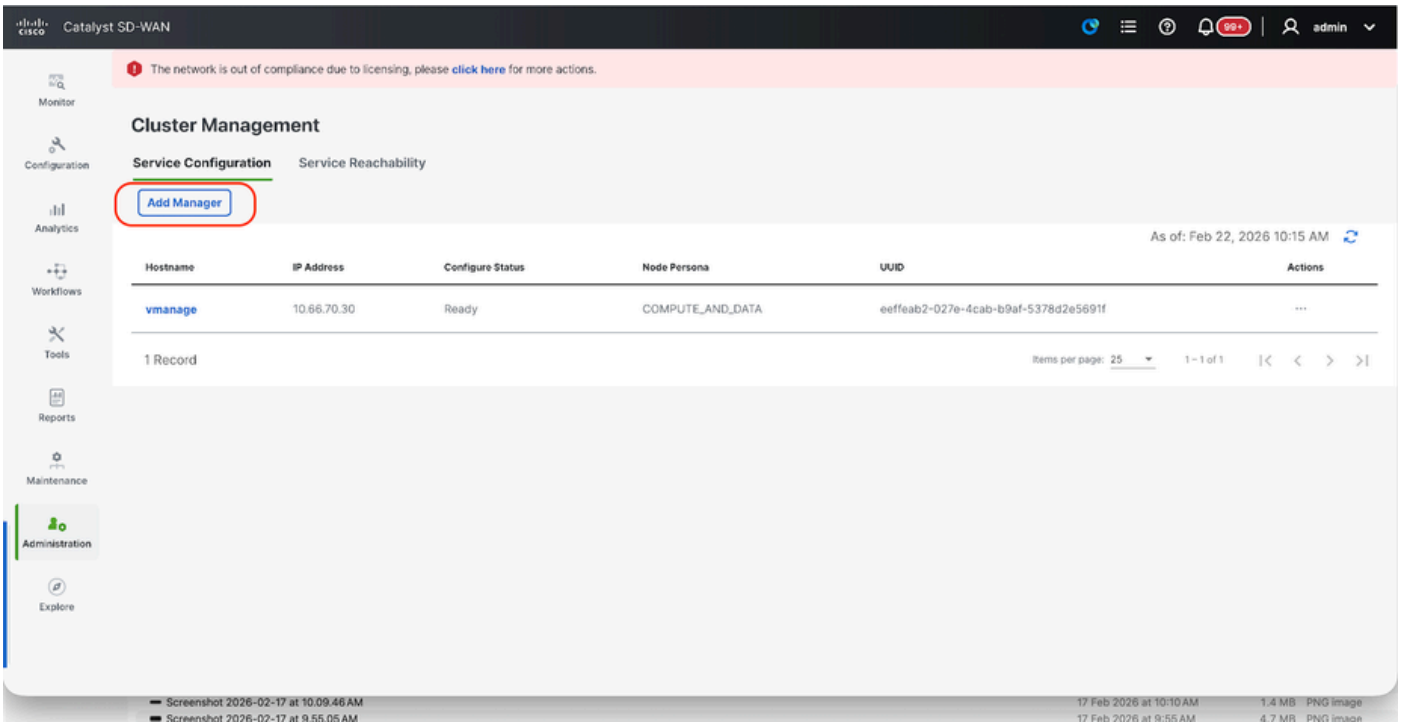
Lesen Sie diese Konfiguration in Ihrem vorhandenen Cluster, um SDAVC zu aktivieren - Muss nur überprüft werden, wenn dies erforderlich ist und nur auf einem vManage-Knoten des Clusters erforderlich ist.

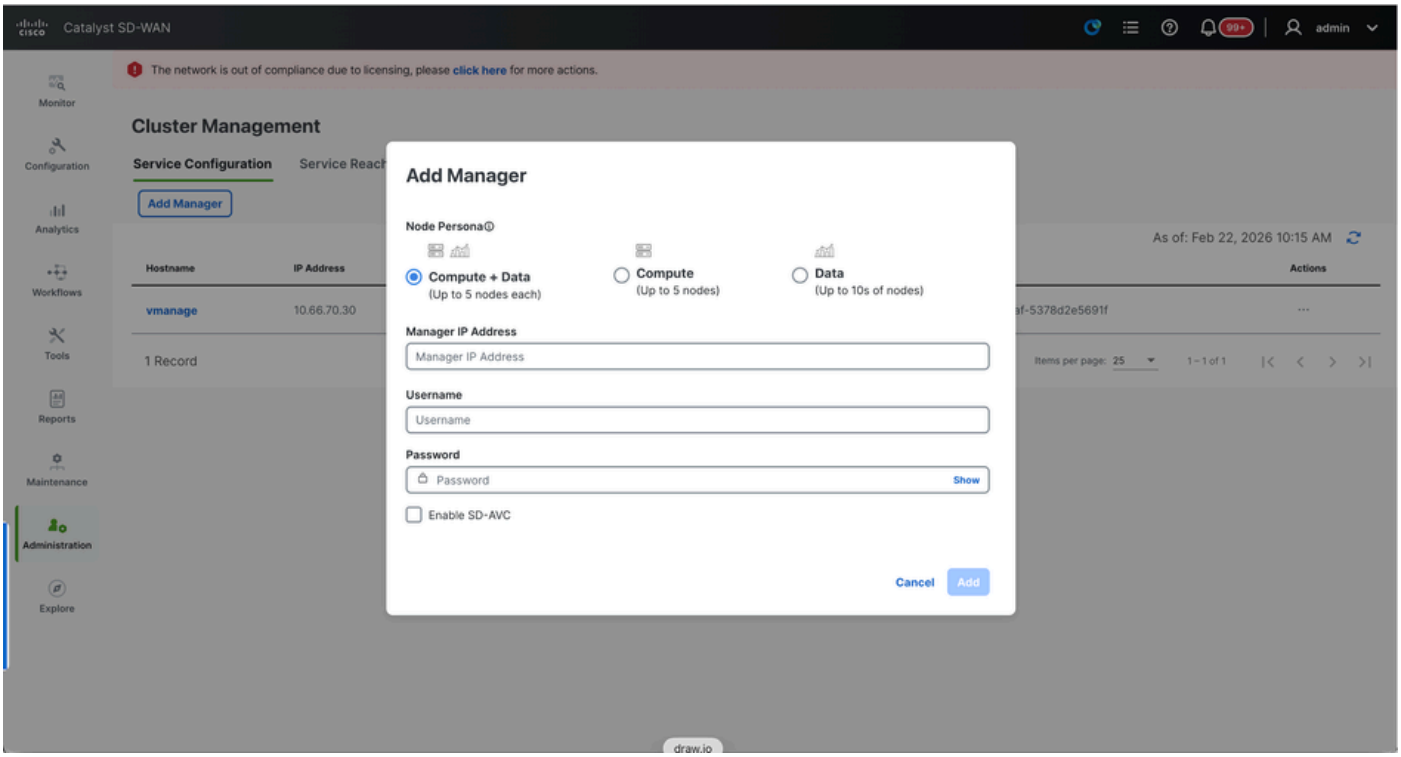
Klicken Sie auf Aktualisieren.

- Nach diesem Vorgang wird der vManage NMS-Dienst im Hintergrund neu gestartet, und die Benutzeroberfläche ist für einige Minuten (etwa 5 bis 10 Minuten) nicht verfügbar. Während dieser Zeit ist der CLI-Zugriff von vManage verfügbar.
- Sobald auf die vManage-1-Benutzeroberfläche zugegriffen werden kann, navigieren Sie zu Administration > Cluster Management, und stellen Sie sicher, dass die IP-Adresse der Service-Schnittstelle von vManage unter der IP-Adresse angezeigt wird.Der Konfigurationsstatus lautet "Ready", und die Node-Persona wird korrekt wiedergegeben. Wechseln Sie zum Abschnitt "Erreichbarkeit von Services" auf derselben Seite, und stellen Sie sicher, dass alle Services erreichbar sind.
- Wenn wir sehen, dass einer der Dienste noch nicht erreichbar ist, warten Sie bitte. In der Regel dauert etwa 20 bis 30 Minuten.

Aufbau des vManage-Clusters

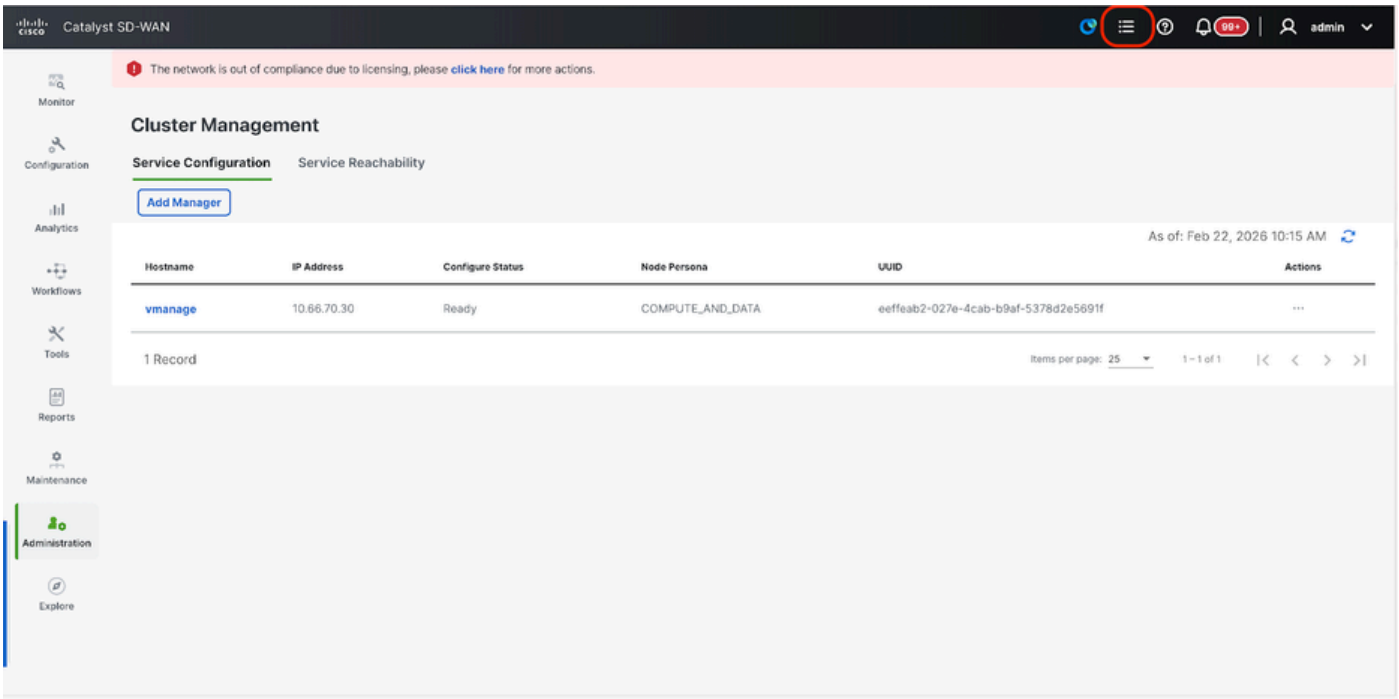
- Navigieren Sie auf der Web-Benutzeroberfläche von vManage-1 zu Administration > Cluster Management, im Abschnitt Service Configuration,
- Klicken Sie auf Add Manager, um ein Popup-Fenster anzuzeigen:





- Wählen Sie den Knoten persona basierend auf den persönlichen Konfigurationen aus, die während der Aktivierung von vManage - 2 durchgeführt wurden.
- Geben Sie die IP-Adresse der Service-Schnittstelle von vManage-2 unter der Manager-IP-Adresse ein.

- Geben Sie den Benutzernamen und das Kennwort ein. Dies sind die gleichen Anmeldeinformationen wie in Schritt 6.
- SDAVC aktivieren: Deaktivieren Sie diese Option, da sie bereits in vManage-1 aktiviert ist.
- Klicken Sie auf Hinzufügen.
- Nach diesem Schritt werden die vManage NMS-Dienste für vManage 1- und 2-Knoten im Hintergrund neu gestartet. Die Benutzeroberfläche ist für einige Minuten von etwa 5 bis 10 Minuten für vManage 1 und 2 nicht verfügbar.
- Während dieser Zeit ist der CLI-Zugriff von vManage 1 und 2 verfügbar.
- Sobald auf die vManage-1-Benutzeroberfläche zugegriffen werden kann, navigieren Sie zu Administration > Cluster Management, stellen Sie sicher, dass die Service-Schnittstellen-IP des vManage unter der IP-Adresse angezeigt wird, der Konfigurationsstatus "Ready" lautet und die Knoten-IP-Adresse korrekt wiedergegeben wird.
- Wechseln Sie zum Abschnitt "Service-Erreichbarkeit" auf derselben Seite, und stellen Sie sicher, dass alle Services für beide vManage-Knoten erreichbar sind.
- Wenn wir sehen, dass einer der Dienste noch nicht erreichbar ist, warten Sie bitte. In der Regel dauert etwa 5 bis 10 Minuten.
- Sie können den Status des Cluster-Hinzufügevorgangs in der Aufgabenliste überprüfen, die oben rechts auf der vManage-Benutzeroberfläche zur Verfügung steht.



- Sie können nach der Liste "Aktive Task" suchen. Wenn die Task immer noch in der Liste "Aktive Task" aufgeführt ist, weist dies darauf hin, dass die Task noch nicht abgeschlossen ist.
- Sie können auf die Aufgabe klicken, um den Fortschritt der gleichen Aufgabe zu überprüfen. Wenn die Aufgabe nicht in der Liste "Aktive Aufgabe" aufgeführt ist, wechseln Sie zu "Abgeschlossen", und stellen Sie sicher, dass die Aufgabe erfolgreich abgeschlossen wurde.
- Fahren Sie erst mit dem nächsten Schritt fort, nachdem diese Punkte validiert wurden.

Diese Punkte müssen berücksichtigt werden, bevor der nächste Knoten zum Cluster hinzugefügt

wird:

Überprüfen Sie diese Punkte auf allen UIs der vManage-Knoten, die dem Cluster bisher hinzugefügt wurden:

- Navigieren Sie zu Monitor > Overview of vManage UI, und stellen Sie sicher, dass die Anzahl der vManage-Knoten korrekt wiedergegeben wird und in Abhängigkeit von der Anzahl der Knoten, die dem Cluster hinzugefügt wurden, als erreichbar angezeigt wird.

- Navigieren Sie zu Administration > Cluster Management, und stellen Sie sicher, dass die Service-Schnittstellen-IP des vManage unter IP-Adresse, Configure Status is Ready und Node-Personal korrekt wiedergegeben wird.
- Wechseln Sie zum Abschnitt "Service-Erreichbarkeit" auf derselben Seite, und stellen Sie sicher, dass alle Services für beide vManage-Knoten erreichbar sind.

- Bei jedem Hinzufügen eines Knotens zum Cluster werden die NMS-Dienste aller Knoten im Cluster neu gestartet, sodass die Benutzeroberfläche all dieser Knoten für einige Zeit nicht erreichbar ist.
- Je nach Anzahl der Knoten im Cluster kann es länger dauern, bis die Benutzeroberfläche gesichert ist und alle Dienste erreichbar sind.
- Sie können die Aufgabe in der Aufgabenliste oben rechts in der vManage-Benutzeroberfläche überwachen.
- Auf der vManage-Benutzeroberfläche jedes Knotens, der dem Cluster hinzugefügt wurde, müssen alle Router, Vorlagen und Richtlinien angezeigt werden, wenn sie in vManage-1 verfügbar waren.
- Wenn diese Konfigurationen in vManage-1 nicht vorhanden waren, müssen die vBonds und vSmarts, die zu vManage-1 hinzugefügt wurden, sowie die Konfigurationen Administration > Settings für Organisationsname, vBond, Certificate Authorization (Administration > Einstellungskonfigurationen für Organisationsname, vBond, Zertifikatsautorisierung) auf den übrigen vManage-Knoten, die dem Cluster hinzugefügt wurden, angezeigt werden.
- Wiederholen Sie die gleichen Schritte für die übrigen vManage-Knoten.

Schritt 4: Einrichtung des Cold Standby DR-Clusters

Einrichtung des Cold Standby DR-Clusters

Sie können einen weiteren vManage-Cluster mit den in Schritt 4 beschriebenen Schritten aufrufen: vManage-Cluster erstellen. Führen Sie einen Post aus, in dem Sie die in Schritt 6 beschriebenen Schritte durchführen: "Config-db Backup/Restore" zum Wiederherstellen der "config-db"-Sicherung im Standby-Cluster.

Schritt 5: Sicherung/Wiederherstellung der Konfig.-DB

Sammeln von vManage-Konfigurations-DB-Backups und Wiederherstellen auf einem anderen vManage-Knoten

Sammeln der Konfiguration - DB-Backup:

- In der derzeit verwendeten SD-WAN-Fabric können Sie ein Backup der Konfigurationsdatenbank vom vManage-Cluster generieren.
- Bitte beachten Sie, dass wir ein Backup der Konfigurationsdatenbank nur auf einem Knoten des vManage-Clusters generieren müssen, der der führende Konfigurationsdatenbank ist.

- Bei eigenständigem vManage ist dieser vManager selbst der führende Anbieter von Konfigurationsdatenbanken.
- Identifizieren Sie im vManage-Cluster mithilfe des Befehls request nms configuration-db diagnostics den Knoten configuration-db leader.Sie können diesen Befehl auf allen Knoten des vManage-Clusters mit drei Knoten ausführen.
- In einem Cluster mit sechs Knoten muss dieser Befehl auf den vManage-Knoten ausgeführt werden, auf denen configuration-db aktiviert ist, um den Leader-Knoten zu identifizieren. Navigieren Sie zu Administration > Cluster Management, um dies zu überprüfen:
- Wie wir im Screenshot sehen, laufen bei den Knoten, die mit persona COMPUTE_AND_DATA konfiguriert sind, configuration-db.

Dasselbe können Sie mit dem Befehl requestnmsconfiguration-dbstatus in vManageCLI überprüfen. Die Ausgabe erfolgt wie dargestellt

```
vmanage# request nms configuration-db status
NMS configuration database
        Enabled: true
        Status: running PID:32632 for 1066085s
        Native metrics status: ENABLED
        Server-load metrics status: ENABLED
vmanage#
```

- Nach der Ausführung des Befehlsrequest nms configuration-db diagnostics on these nodes, die Ausgabe ist wie folgt:
- Suchen Sie das hervorgehobene Feld für "IsLeader". Wenn es auf 1 gesetzt ist, bedeutet dies, dass der Knoten der führende Knoten ist, und wir können die Sicherung der Konfigurationsdatenbank von ihm erfassen.

```
vManage-3# request nms configuration-db diagnostics
NMS configuration database
Checking cluster connectivity for ports 7687,7474 ...
Pinging vManage  node 0 on 169.254.1.5:7687,7474...
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2026-02-18 12:41 UTC
SENT (0.0013s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (0.0022s) Handshake with 169.254.1.5:7474 completed
SENT (1.0024s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (1.0028s) Handshake with 169.254.1.5:7687 completed
SENT (2.0044s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (2.0050s) Handshake with 169.254.1.5:7474 completed
SENT (3.0064s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (3.0072s) Handshake with 169.254.1.5:7687 completed
SENT (4.0083s) Starting TCP Handshake > 169.254.1.5:7474
```

```
RCVD (4.0091s) Handshake with 169.254.1.5:7474 completed
SENT (5.0106s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (5.0115s) Handshake with 169.254.1.5:7687 completed
Max rtt: 0.906ms | Min rtt: 0.392ms | Avg rtt: 0.724ms
TCP connection attempts: 6 | Successful connections: 6 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 5.01 seconds
Pinging vManage  node 1 on 169.254.2.5:7687,7474...
========== SNIP ==========
Connecting to 10.10.10.3...
+-------------------------------------------------------------------------------------+
| type             | row                                    | attributes[row]["value"] |
+-------------------------------------------------------------------------------------+
| "StoreSizes"     | "TotalStoreSize"                       | 85828934                 |
| "PageCache"      | "Flush"                                | 4268666                  |
| "PageCache"      | "EvictionExceptions"                   | 0                        |
| "PageCache"      | "UsageRatio"                           | 0.09724264705882353      |
| "PageCache"      | "Eviction"                             | 2068                     |
| "PageCache"      | "HitRatio"                             | 1.0                      |
| "ID Allocations" | "NumberOfRelationshipIdsInUse"         | 2068                     |
| "ID Allocations" | "NumberOfPropertyIdsInUse"             | 56151                    |
| "ID Allocations" | "NumberOfNodeIdsInUse"                 | 7561                     |
| "ID Allocations" | "NumberOfRelationshipTypeIdsInUse"     | 31                       |
| "Transactions"   | "LastCommittedTxId"                    | 214273                   |
| "Transactions"   | "NumberOfOpenTransactions"             | 1                        |
| "Transactions"   | "NumberOfOpenedTransactions"           | 441742                   |
| "Transactions"   | "PeakNumberOfConcurrentTransactions"   | 11                       |
| "Transactions"   | "NumberOfCommittedTransactions"        | 414568                   |
| "Causal Cluster" | "IsLeader"                             | 1         >>>>>>>>>      |
| "Causal Cluster" | "MsgProcessDelay"                      | 0                        |
| "Causal Cluster" | "InFlightCacheTotalBytes"              | 0                        |
+-------------------------------------------------------------------------------------+
18 rows
ready to start consuming query after 388 ms, results consumed after another 13 ms
Completed
Connecting to 10.10.10.3...
Displaying the Neo4j Cluster Status
+-------------------------------------------------------------------------------------------------------------------
| name     | aliases | access       | address             | role       | requestedStatus | currentStatus
+-------------------------------------------------------------------------------------------------------------------
| "neo4j"  | []      | "read-write" | "169.254.3.5:7687" | "leader"   | "online"        | "online"
| "neo4j"  | []      | "read-write" | "169.254.2.5:7687" | "follower" | "online"        | "online"
| "neo4j"  | []      | "read-write" | "169.254.1.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.3.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.2.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.1.5:7687" | "leader"   | "online"        | "online"
+-------------------------------------------------------------------------------------------------------------------
6 rows
ready to start consuming query after 256 ms, results consumed after another 3 ms
Completed
Total disk space used by configuration-db:
60M     .
```

Verwenden Sie diesen Befehl, um das Backup configuration-db vom angegebenen Konfigurationsdb-Leader "vManage" zu erfassen.

```
request nms configuration-db backup path /opt/data/backup/
```

Die erwartete Ausgabe lautet wie folgt:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Notieren Sie sich die Anmeldeinformationen für die Konfigurationsdatenbank, wenn diese aktualisiert wurde.
- Wenn Sie die Anmeldeinformationen für die Konfigurationsdatenbank nicht kennen, wenden Sie sich an das TAC, um die Anmeldeinformationen für die Konfigurationsdatenbank von den vorhandenen vManage-Knoten abzurufen.
- Die Standardanmeldeinformationen für die -db-Konfiguration sind Benutzername: neo4j und Passwort: Kennwort

  Wiederherstellen der Konfiguration - db-Sicherung auf einem anderen vManage-Knoten

  Kopieren Sie das Sicherungsverzeichnis configuration-db mithilfe von SCP in das Verzeichnis /home/admin/ von vManage.

  Beispielausgabe des Befehls scp:

  ```
  XXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
  viptela 20.15.4.1

  (admin@10.66.62.27) Password:
  (admin@10.66.62.27) Password:
  june18th.tar.gz
  ```

  Zum Wiederherstellen des "configuration-db"-Backups müssen wir zunächst die "configuration-db"-Anmeldeinformationen konfigurieren. Wenn Ihre Anmeldeinformationen für configuration-db default(neo4j/password) sind, können wir diesen Schritt überspringen.

  Um die Anmeldeinformationen für configuration-db zu konfigurieren, verwenden Sie den Befehl request nms configuration-db update-admin-user.Use the username and password of your choice.

Bitte beachten Sie, dass der Anwendungsserver von vManage neu gestartet wurde. Aufgrund dessen kann auf die vManage-Benutzeroberfläche für kurze Zeit nicht mehr zugegriffen werden.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same op
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Nach dem wir fortfahren können, die Konfiguration-db-Backup wiederherzustellen:

Wir können den Befehl request nms configuration-db restore path /home/admin/< > verwenden, um configuration-db auf dem neuen vManage wiederherzustellen:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Reseting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Sobald die Konfigurationsdatenbank wiederhergestellt ist, stellen Sie sicher, dass auf die vManage-Benutzeroberfläche zugegriffen werden kann. Warten Sie etwa 5 Minuten, und versuchen Sie dann, auf die Benutzeroberfläche zuzugreifen.

Nachdem Sie sich erfolgreich bei der Benutzeroberfläche angemeldet haben, stellen Sie sicher,

dass die Liste der Edge-Router, die Vorlage, die Richtlinien und alle anderen Konfigurationen, die auf der vorherigen oder vorhandenen vManage-Benutzeroberfläche vorhanden waren, auf der neuen vManage-Benutzeroberfläche wiedergegeben werden.

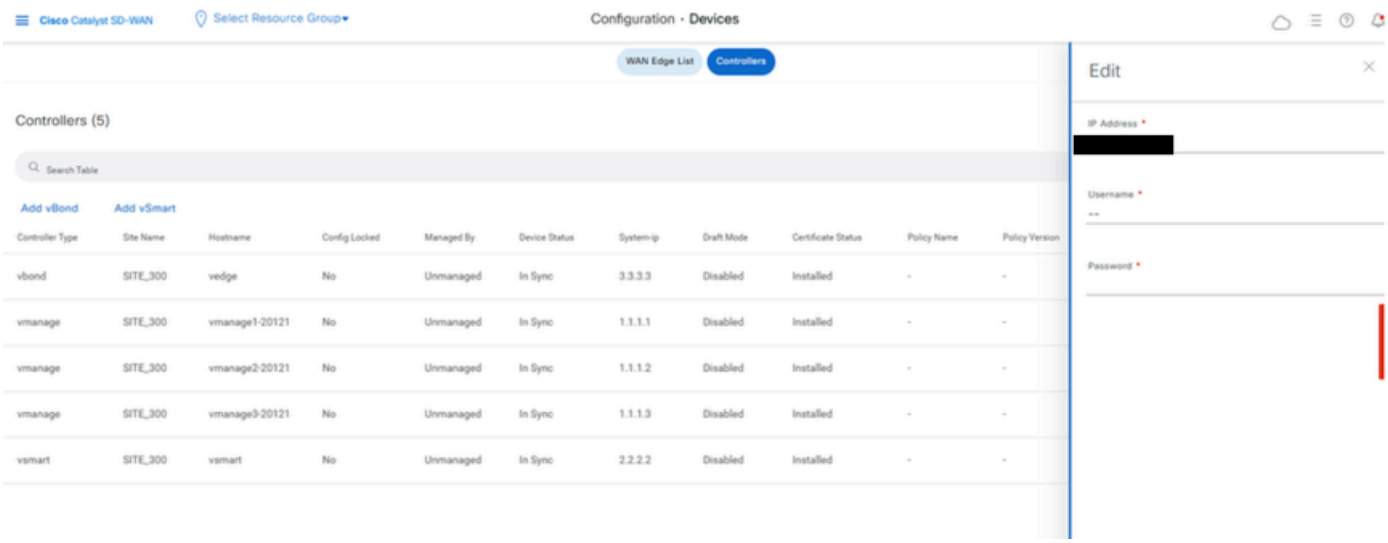
Schritt 6: Neuauthentifizierung von Controllern und Ungültigerklärung alter Controller

Nach der Wiederherstellung der Konfigurationsdatenbank müssen alle neuen Controller (vmanage/vsmart/vbond) im Fabric erneut authentifiziert werden.

Hinweis: Wenn in der Produktion die zur erneuten Authentifizierung verwendete Schnittstellen-IP die Tunnel-Schnittstellen-IP ist, müssen Sie sicherstellen, dass der NETCONF-Dienst auf der Tunnelschnittstelle von vManage, vSmart und vBond sowie auf den Firewalls entlang des Pfads zugelassen ist. Der zu öffnende Firewall-Port ist der TCP-Port 830 als bidirektionale Regel vom DR-Cluster zu allen vBonds und vSmarts .

Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.

- Klicken Sie auf die drei Punkte in der Nähe der einzelnen Controller, und klicken Sie dann auf Bearbeiten.



- Ersetzen Sie die IP-Adresse (System-IP des Controllers) durch die IP-Adresse des Transport-VPN 0 (Tunnelschnittstelle). Geben Sie Benutzername und Kennwort ein, und klicken Sie auf "Save" (Speichern).
- Gleiches für alle neuen Controller im Fabric tun

Synchronisieren der Root-Zertifikatskette

Führen Sie diesen Schritt aus, nachdem alle Controller integriert wurden:

Führen Sie auf einem Cisco SD-WAN Manager-Server im neu aktiven Cluster die folgenden

Aktionen aus:

Geben Sie diesen Befehl ein, um das Root-Zertifikat mit allen Cisco Catalyst SD-WAN-Geräten im neu aktiven Cluster zu synchronisieren:

https://vmanage-url/dataservice/system/device/sync/rootcertchain

Geben Sie diesen Befehl ein, um die UUID des Cisco SD-WAN-Managers mit dem Cisco SD-WAN Validator zu synchronisieren:

https://vmanage-url/dataservice/certificate/syncvbond

Sobald die Fabric wiederhergestellt ist und die Steuerungs- und BFD-Sitzungen für alle Edges und Controller in der Fabric verfügbar sind, müssen die alten Controller (vmanage/vsmart/vbond) in der Benutzeroberfläche ungültig gemacht werden.

- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Zertifikate.
- Auf Controller klicken
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Ungültig
- Klicken Sie auf Senden,
- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Löschen

Schritt 7: Nachprüfungen

Anmerkung: Fahren Sie mit dem hier abgebildeten Abschnitt "Nachprüfungen" fort, der für alle Bereitstellungskombinationen gilt.

Kombination 5: vCluster verwalten + DR aktiviert

Erforderliche Instanzen:

- 3 oder 6 vManage (primäres Cluster)
- 3 oder 6 vManage (DR-Standby-Cluster)
- 1 oder mehr vBond (verteilt auf primäre und DR-Rechenzentren)
- 1 oder mehr vSmart (verteilt auf primäre und DR-Rechenzentren)

Schritte:

1. Aufrufen aller Instanzen mithilfe der allgemeinen Schritte
2. Vorabprüfungen
3. Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller
4. vManage-Cluster erstellen
5. Einrichtung des Cold Standby DR-Clusters

6. Sicherung/Wiederherstellung der Konfig.-DB
7. Nachprüfungen

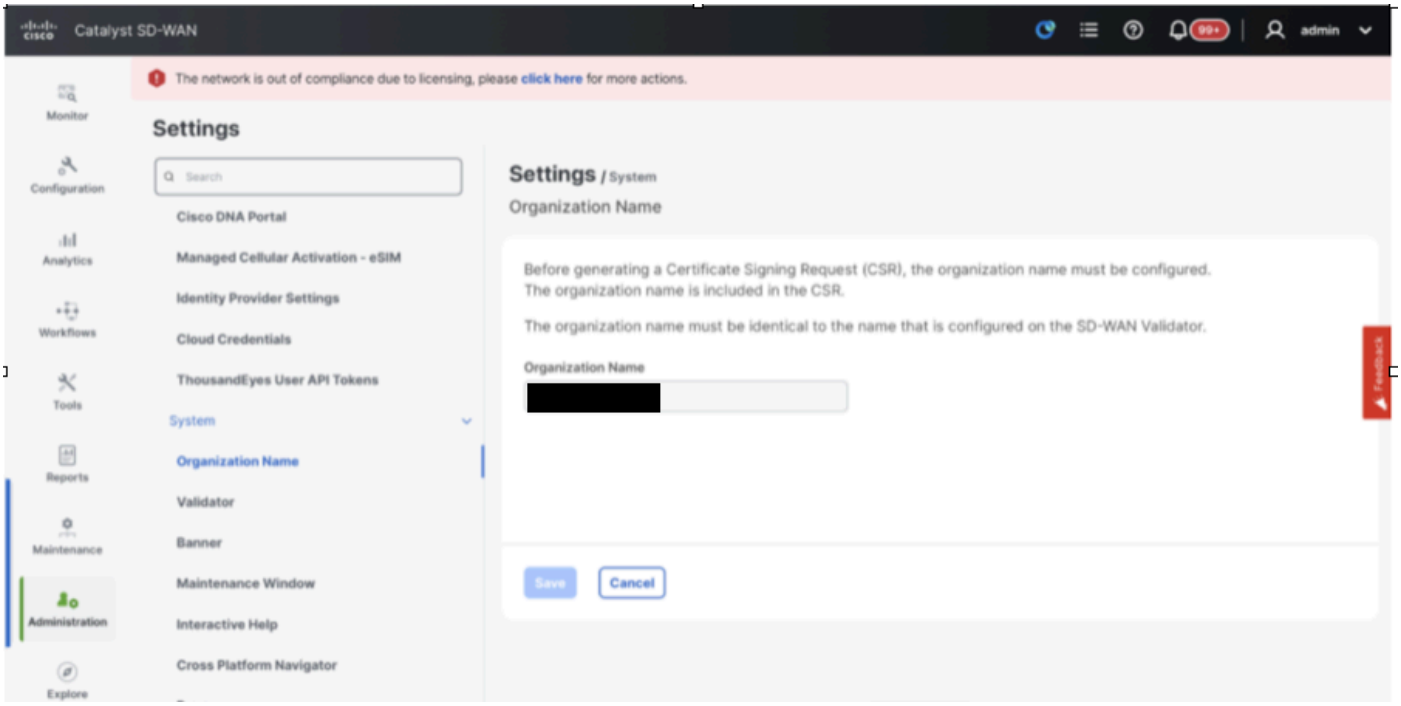
Schritt 1: Vorabprüfungen

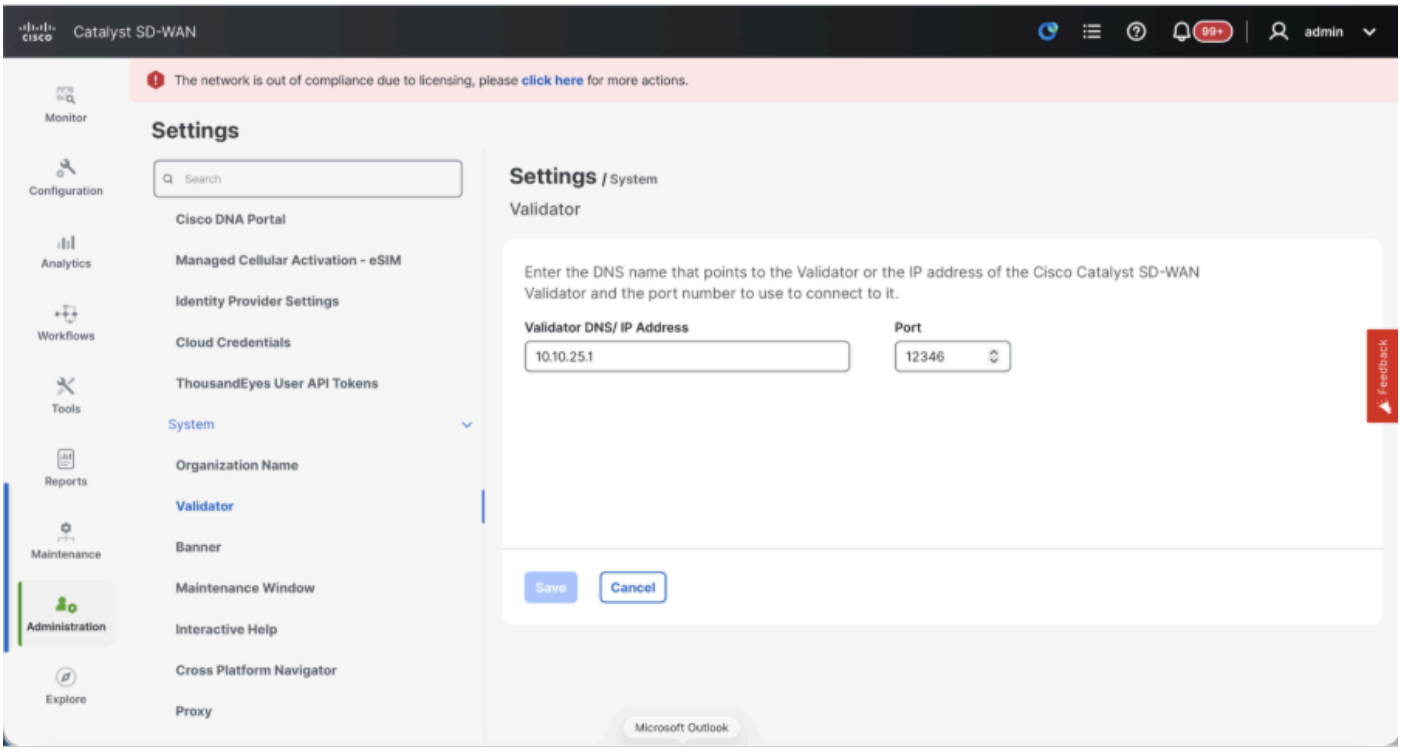
- Stellen Sie sicher, dass die Anzahl der aktiven Cisco SD-WAN Manager-Instanzen mit der Anzahl der neu installierten Cisco SD-WAN Manager-Instanzen identisch ist.
- Stellen Sie sicher, dass auf allen aktiven und neuen Cisco SD-WAN Manager-Instanzen dieselbe Softwareversion ausgeführt wird.
- Stellen Sie sicher, dass alle aktiven und neuen Cisco SD-WAN Manager-Instanzen die Management-IP-Adresse des Cisco SD-WAN Validators erreichen können.
- Stellen Sie sicher, dass die Zertifikate auf den neu installierten Cisco SD-WAN Manager-Instanzen installiert wurden.
- Stellen Sie sicher, dass die Uhren auf allen Cisco Catalyst SD-WAN-Geräten, einschließlich der neu installierten Cisco SD-WAN Manager-Instanzen, synchronisiert sind.
- Stellen Sie sicher, dass auf den neu installierten Cisco SD-WAN Manager-Instanzen ein neuer Satz von System-IPs und Standort-IDs konfiguriert und die gleiche grundlegende Konfiguration wie im aktiven Cluster verwendet wird.

Phase 2: Konfigurieren der vManage-Benutzeroberfläche, -Zertifikate und der integrierten Controller

Aktualisieren der Konfigurationen der vManage-Benutzeroberfläche

- Sobald die Konfigurationen in Schritt 1 in der CLI aller Controller hinzugefügt wurden, können wir über die URL https://<vmanage-ip> in Ihrem Browser auf die Web-UI von vManage zugreifen. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManage-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.
- Navigieren Sie zu Administration > Settings, und führen Sie diese Schritte aus.
- Konfigurieren Sie den Organisationsnamen und die Validator-/vBond-URL/IP-Adresse. Konfigurieren Sie den gleichen Wert wie in der CLI des vManage-Knotens.
- In vManage 20.15/20.18 sind diese Konfigurationen im Abschnitt System verfügbar.

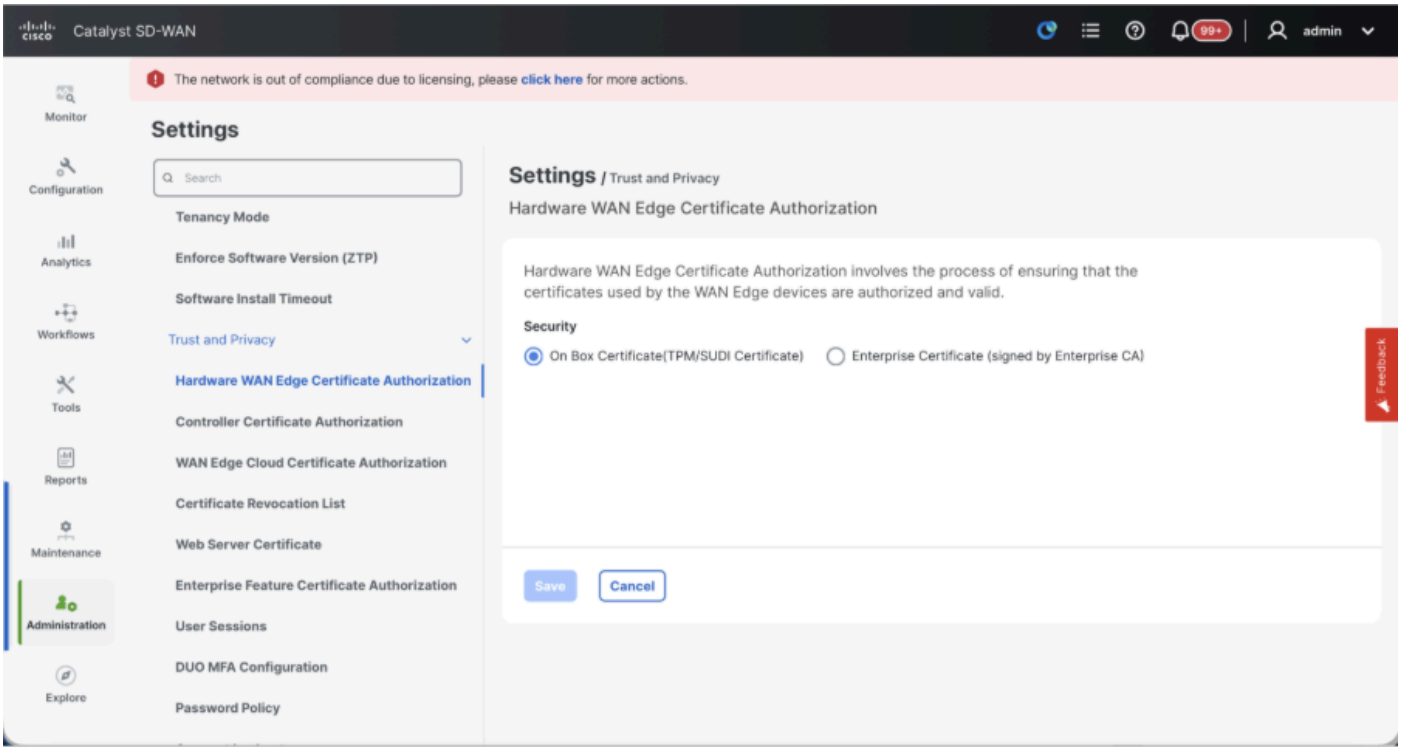




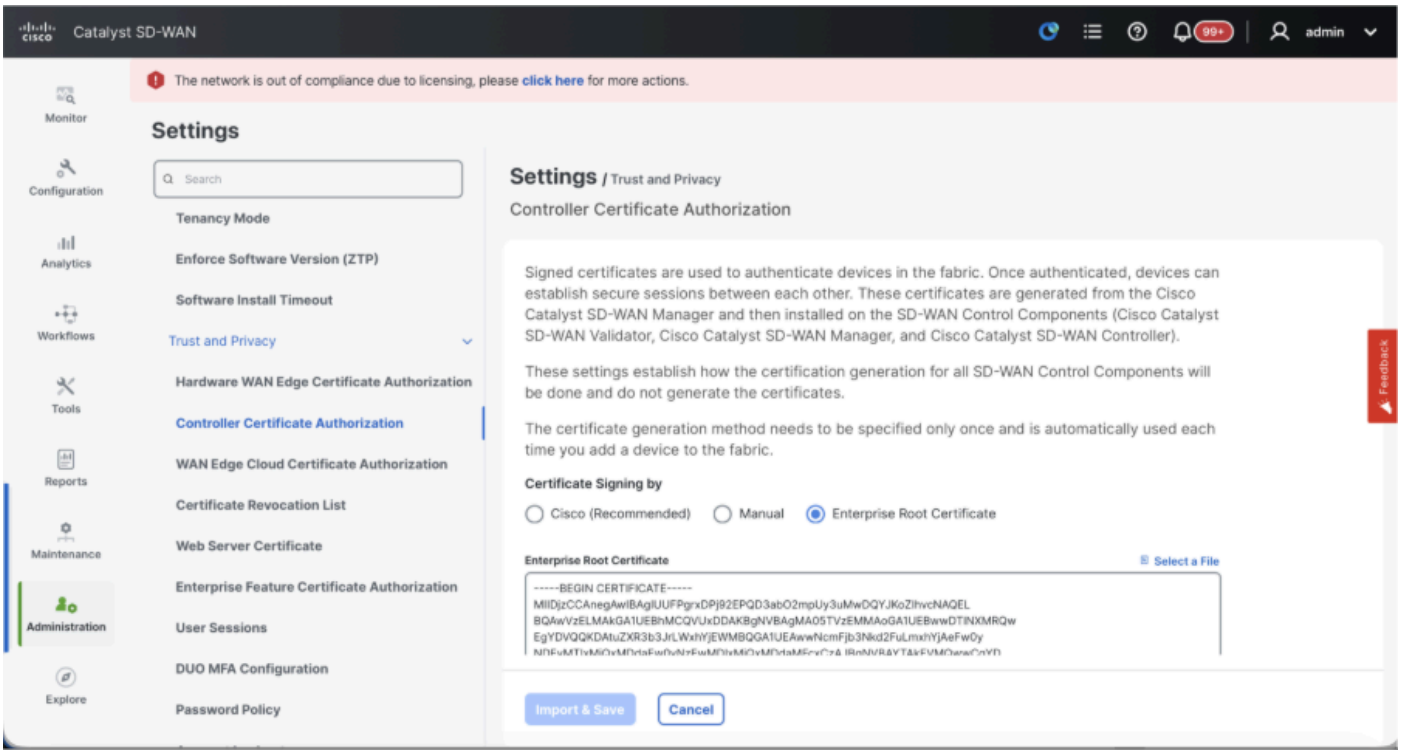
- Überprüfen Sie die Konfigurationen für die Zertifizierungsstelle (Certificate Authorization, CA), die die zum Signieren der Zertifikate verwendete Zertifizierungsstelle bestimmt. Hier sehen wir 3 Optionen:

1. Hardware WAN Edge Certificate Authorization (Hardware-WAN-Edge-Zertifikatsautorisierung): bestimmt die Zertifizierungsstelle für Hardware-SD-WAN-Edge-Router.
    - On Box Certificate (TPM/SUDI Certificate) - Mit dieser Option wird das vorinstallierte Zertifikat auf der Router-Hardware verwendet, um die Steuerverbindungen (TLS-/DTLS-Verbindungen) herzustellen.
    - Enterprise-Zertifikat (von der Enterprise-Zertifizierungsstelle signiert) - Bei dieser

Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

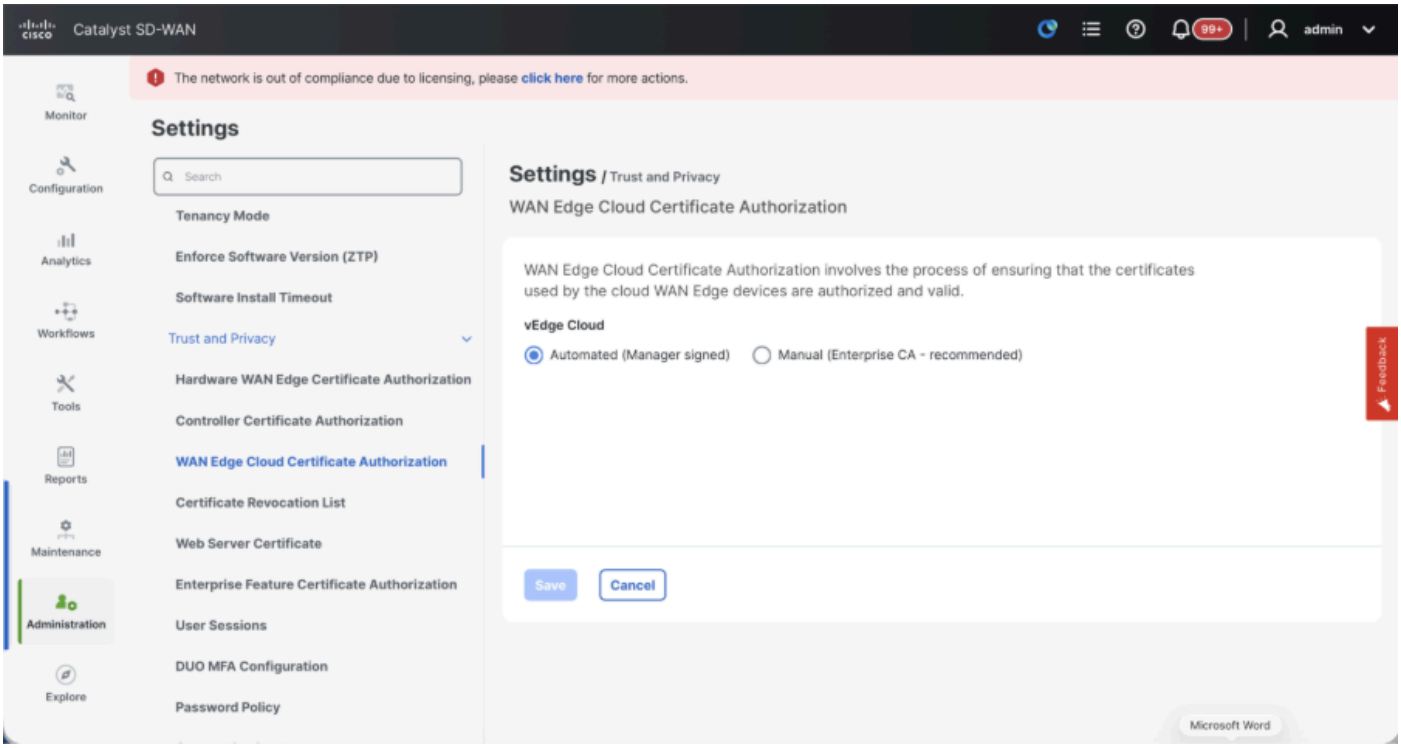


2. Controller Certificate Authorization (Controller-Zertifikatautorisierung): bestimmt die Zertifizierungsstelle für SD-WAN-Controller
    - Cisco (empfohlen) - Controller verwenden die von der Cisco PKI signierten Zertifikate. vManage kontaktiert das PNP-Portal automatisch mit den Smart Account-Anmeldedaten, die auf dem vManage konfiguriert sind. Das Zertifikat wird signiert und auf dem Controller installiert.
    - Manual (Manuell) - Controller verwenden die von der Cisco PKI signierten Zertifikate. Signieren Sie den CSR manuell über das Cisco PNP-Portal, indem Sie zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays navigieren.
    - Enterprise-Stammzertifikat - Mit dieser Option verwenden die Router Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

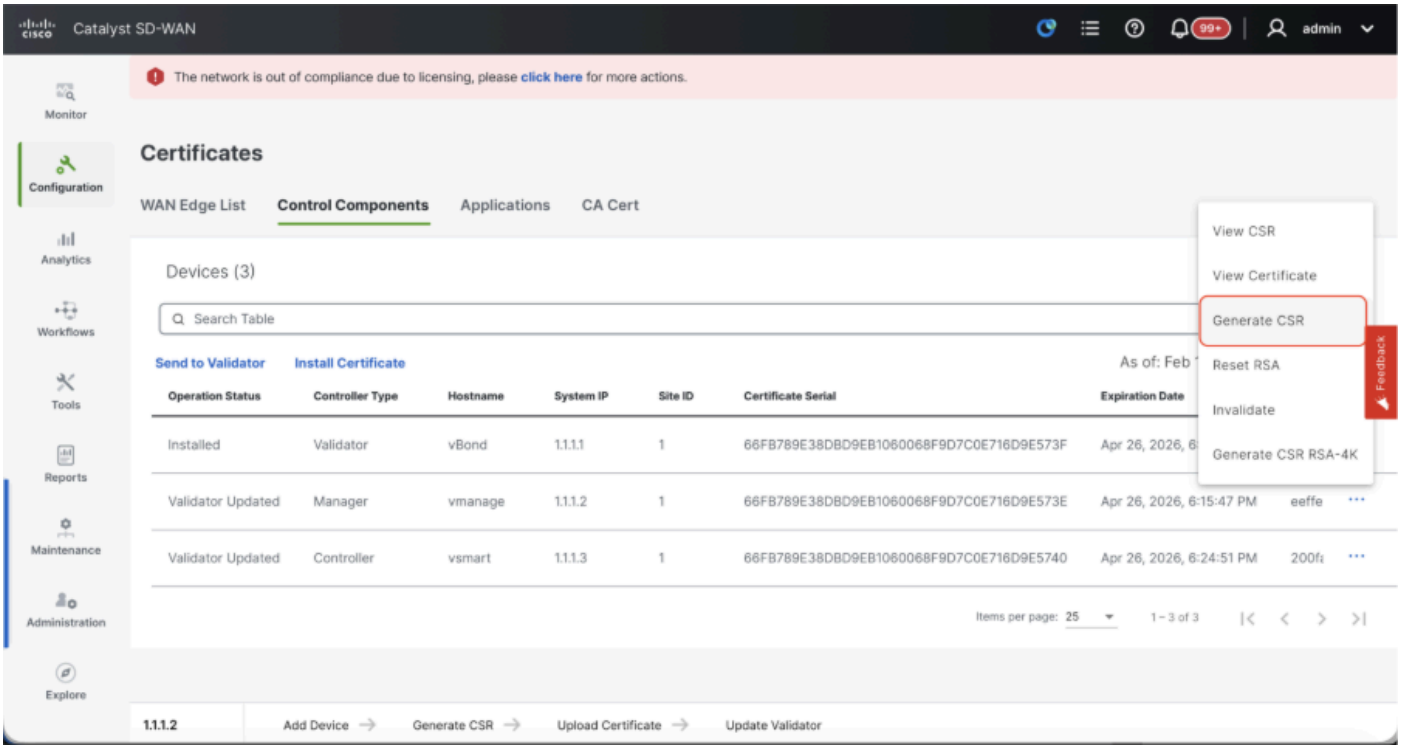


3. WAN-Edge-Cloud-Zertifikatautorisierung - bestimmt die Zertifizierungsstelle für virtuelle SD-WAN-Edge-Router (CSR1000v, C8000v, vEdge-Cloud)
    - Automated (vManage signiert) - vManage signiert automatisch den CSR für die virtuellen Edge-Router und installiert das Zertifikat auf dem Router.
    - Manuell (Enterprise CA - empfohlen) - Virtuelle Router verwenden Zertifikate, die von der Enterprise-Zertifizierungsstelle Ihrer Organisation signiert wurden. Bei Auswahl dieser Option muss das Stammzertifikat der Enterprise-CA hier aktualisiert werden.

Wenn Sie eine eigene Zertifizierungsstelle (CA) oder eine Enterprise-Zertifizierungsstelle verwenden, wählen Sie Enterprise aus.



- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller
- Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

Integration von vBond/Validator und vSmart/Controller in vManage

Navigieren Sie zu Configuration > Devices > Control Components (Konfiguration > Geräte > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

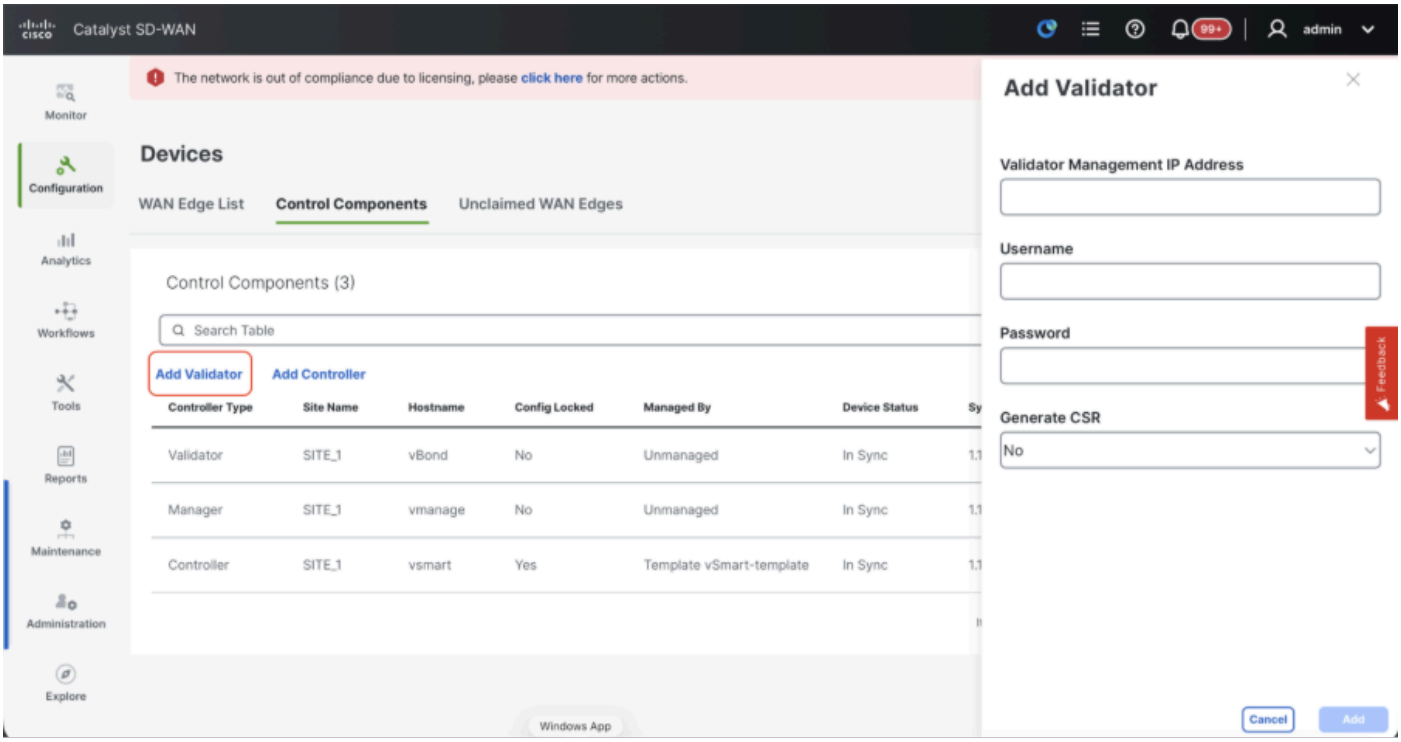
IntegrierenvBond/Validator

- Klicken Sie auf AdvBond.bei 20.12vManagerValidator hinzufügenim Fall von

20.15/20.18vManage. Ein Popup-Fenster wird geöffnet, und geben Sie den VPN 0-Transport-IP von vBond, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, falls dies über die CLI von vManagementvBondIP zulässig ist.
- Geben Sie die Anmeldeinformationen für den Benutzer von vBond ein.

Hinweis: Wir müssen Admin-Anmeldedaten von vBond oder einem Benutzerteil von netadmingroup verwenden. Dies können Sie in der CLI von vBond überprüfen. Wählen Sie im Dropdown-Menü "CSR generieren" die Option "Ja", wenn ein neues Zertifikat für vBond installiert werden soll.

Anmerkung: Wenn sich vBond hinter einem NAT-Gerät bzw. einer NAT-Firewall befindet, überprüfen Sie, ob die IP-Adresse der vBond VPN 0-Schnittstelle in eine öffentliche IP-Adresse übersetzt wurde. Wenn die VPN 0-Schnittstellen-IP von vManage aus nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der VPN 0-Schnittstelle.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vBond installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal.

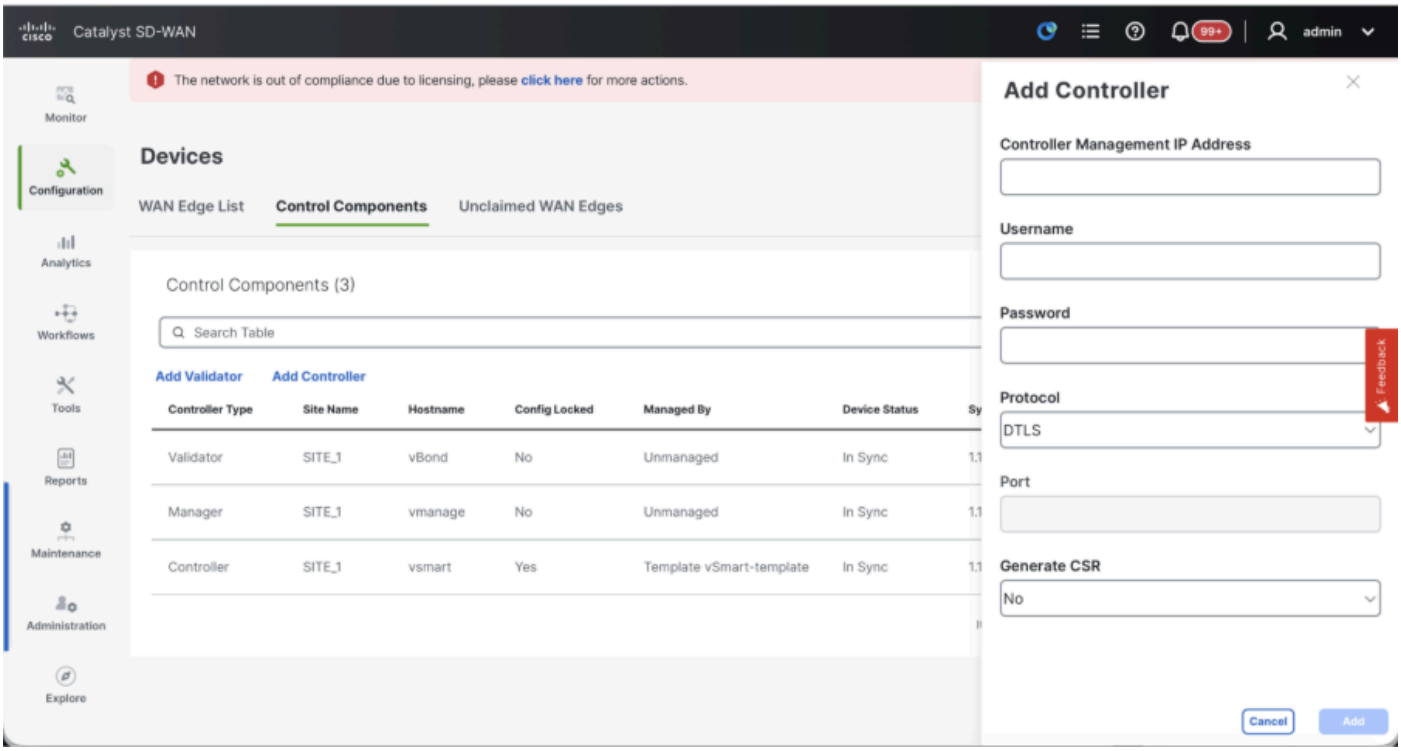
Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays. Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat. Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.

- Wenn mehrere vBonds vorhanden sind, wiederholen Sie die gleichen Schritte.

Integration von vSmart/Controller:

- Klicken Sie auf Add vSmart (vSmart hinzufügen), wenn es sich um 20.12 vManage handelt, oder auf Add Controller (Controller hinzufügen), wenn es sich um 20.15/20.18 vManage handelt.
- Geben Sie in einem Popup-Fenster die VPN 0-Transport-IP von vSmart ein, die über vManage erreichbar ist.
- Überprüfen Sie die Erreichbarkeit mithilfe des Ping-Befehls, wenn dies von der CLI von vManage zu vSmart IP zulässig ist.
- Geben Sie die Benutzeranmeldeinformationen für vSmart Note ein, die von vSmart oder einem Benutzer der netadmin-Gruppe verwendet werden müssen.
- Sie können dies in der CLI des vSmart überprüfen.
- Legen Sie das Protokoll auf TLS fest, wenn TLS für Router verwendet werden soll, um Steuerverbindungen mit vSmart herzustellen. Diese Konfiguration muss auch für CLI von vSmarts- und vManage-Knoten konfiguriert werden.
- Wählen Sie im Dropdown-Menü "Generate CSR" (CSR generieren) die Option Yes (Ja) aus, wenn ein neues Zertifikat für vSmart installiert werden muss.

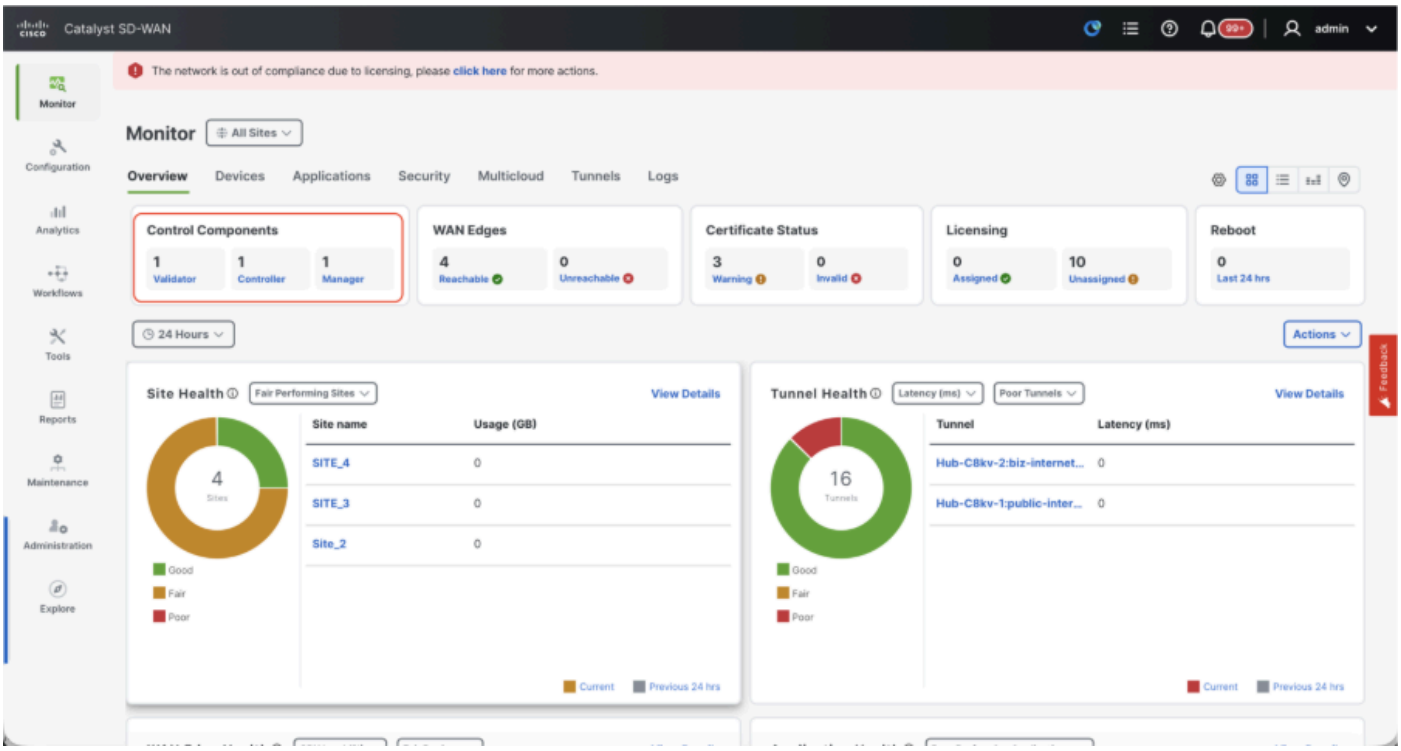
Hinweis: Wenn sich vSmart hinter dem NAT-Gerät/der Firewall befindet, prüfen Sie, ob die IP-Adresse der vSmart VPN 0-Schnittstelle in eine öffentliche IP übersetzt wurde. Wenn die IP-Adresse der VPN 0-Schnittstelle von vManage nicht erreichbar ist, verwenden Sie in diesem Schritt die öffentliche IP-Adresse der IP-Adresse der VPN 0-Schnittstelle.



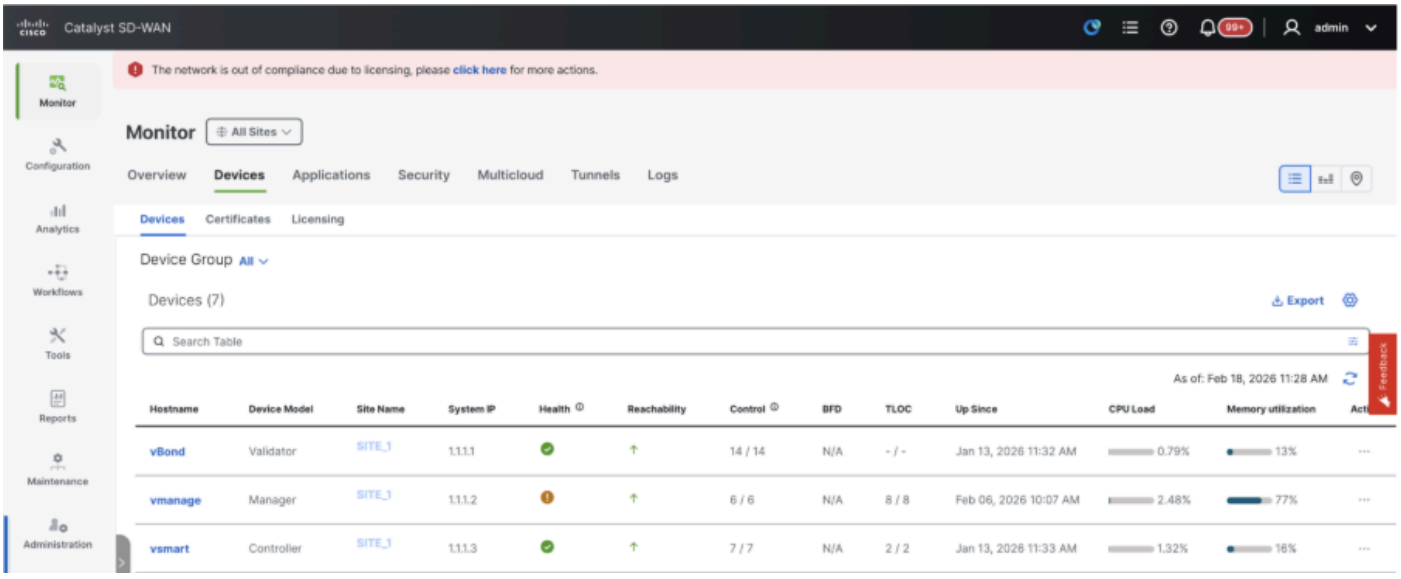
- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManager in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf dem vSmart installiert.
- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays.
- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.
- Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.
- Wenn mehrere vSmarts vorhanden sind, wiederholen Sie die gleichen Schritte.

Verifizierung

Überprüfen Sie nach Abschluss aller Schritte, ob alle Steuerungskomponenten unter Monitor>Dashboard erreichbar sind.



- Klicken Sie auf die jeweiligen Steuerungskomponenten, und vergewissern Sie sich, dass sie alle erreichbar sind.
- Navigieren Sie zu Überwachen > Geräte, und stellen Sie sicher, dass alle Steuerungskomponenten erreichbar sind.



Schritt 3: vManage-Cluster erstellen

Integrierte SD-WAN-Fabric mit vManage Cluster im SD-WAN-Overlay

---

Hinweis: Der vManage-Cluster kann je nach Anzahl der in die SD-WAN-Fabric integrierten Standorte mit drei vManage-Knoten oder mit sechs vManage-Knoten konfiguriert werden.

Integrieren Sie alle SD-WAN-Controller mit einem einzigen vManage-Knoten.

Fahren Sie mit den unter "Integrierte SD-WAN-Controller mit einem einzelnen Knoten vManage im SD-WAN-Overlay" gemeinsam genutzten Schritten fort, um zunächst die SD-WAN-Fabric mit einem vManage-Knoten zu aktivieren und alle erforderlichen Validatoren (vBond) und Controller (vSmart) zu integrieren.

Konfigurieren der CLI-Konfigurationen aller vManage-Knoten im Cluster

- Konfigurieren Sie den Rest der vManage-Knoten. Im Falle eines Clusters mit drei Knoten müssen Sie noch zwei Knoten konfigurieren, im Falle eines Clusters mit sechs Knoten müssen Sie fünf Knoten konfigurieren.
- Konfigurieren Sie die Systemkonfigurationen wie folgt:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Hinweis: Wenn wir eine URL als vBond-Adresse verwenden, stellen Sie sicher, dass die IP-Adressen des DNS-Servers in der VPN 0-Konfiguration konfiguriert sind, oder dass sie aufgelöst werden können.

Diese Konfigurationen werden benötigt, um die Transportschnittstelle zu aktivieren, über die Steuerverbindungen mit den Routern und den übrigen Controllern hergestellt werden.

```
config t
vpn 0
 dns



        primary
 dns



         secondary
 interface eth1
  ip address




  tunnel-interface
   allow-service all
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0



commit
```

Konfigurieren Sie außerdem die VPN 512Management-Schnittstelle, um den Out-of-Band-Management-Zugriff auf den Controller zu ermöglichen.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Optionale Konfiguration:

- Sie können die Konfigurationen Ihres vorhandenen Controllers anzeigen. Wenn die hier aufgeführte Konfiguration vorhanden ist, können Sie diese Konfiguration den neuen Controllern hinzufügen.
- Konfigurieren Sie das Steuerungsprotokoll nur dann als TLS, wenn Router sichere Steuerverbindungen mit den vManage-Knoten herstellen müssen, die TLS verwenden. Standardmäßig stellen alle Controller und Router eine Kontrollverbindung mithilfe von DTLS her. Dies ist eine optionale Konfiguration, die je nach Anforderung nur für vSmart- und vManage-Knoten erforderlich ist.

```
Conf t
security
 control
  protocol tls
commit
```

Serviceschnittstelle auf allen vManage-Knoten konfigurieren

Konfigurieren Sie die Service-Schnittstelle auf allen vManager-Knoten, einschließlich vManage-1, das bereits integriert wurde. Diese Schnittstelle wird für die Cluster-Kommunikation verwendet, d. h. die Kommunikation zwischen den vManager-Knoten im Cluster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Stellen Sie sicher, dass dasselbe IP-Subnetz für die Service-Schnittstelle an allen Knoten im vManagement-Cluster verwendet wird.

Cluster-Anmeldeinformationen konfigurieren

Wir können die gleichen Admin-Anmeldedaten von vManagerNodes verwenden, um vManagerCluster zu konfigurieren. Andernfalls können wir eine neue Benutzeranmeldeinformation konfigurieren, die Teil derNetAdmingroup ist. Die Konfigurationen für die Konfiguration neuer Benutzeranmeldeinformationen sind wie folgt:

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

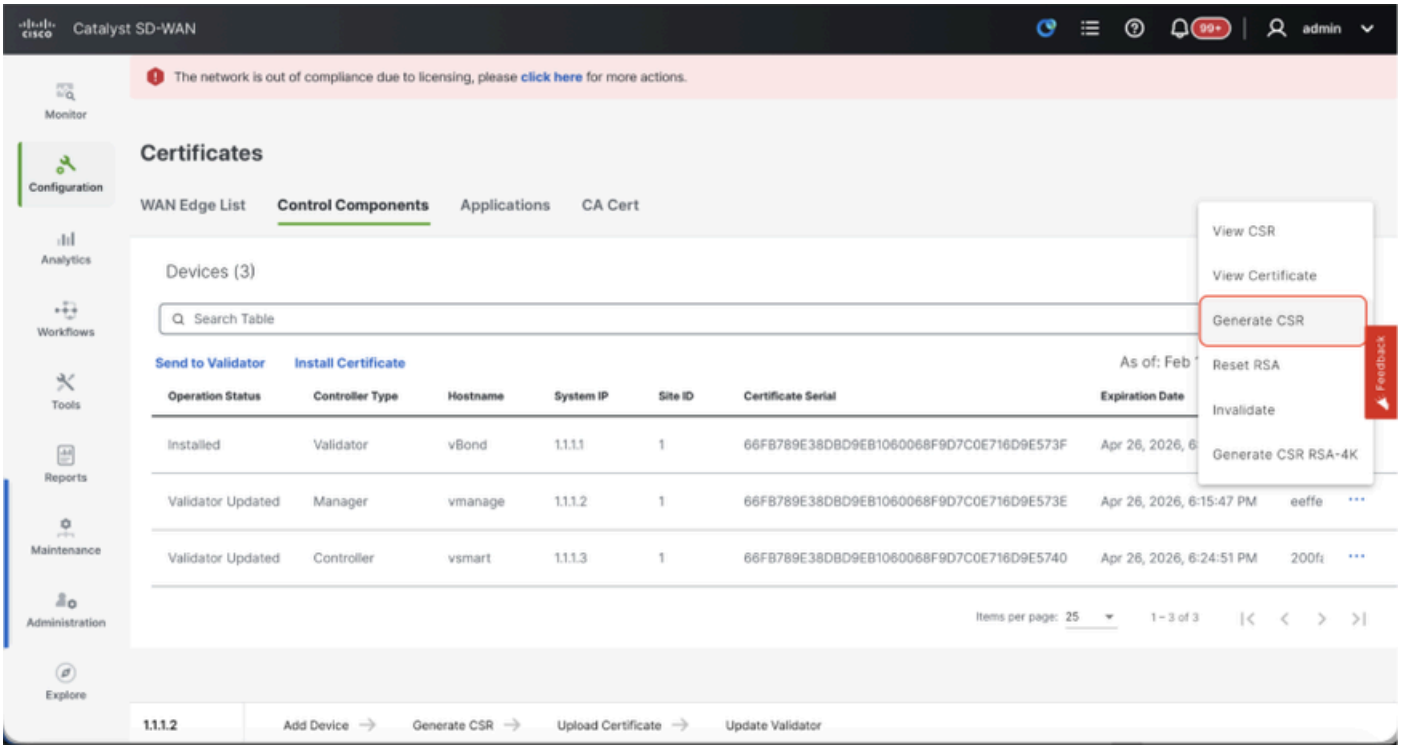
Stellen Sie sicher, dass Sie in allen Managementcodes, die Teil des Clusters sind, dieselben Benutzeranmeldeinformationen konfigurieren.Wenn Sie die Administratoranmeldeinformationen verwenden möchten, müssen Sie in allen Managementcodes denselben Benutzernamen und dasselbe Kennwort verwenden.

Gerätezertifikat auf allen vManage-Knoten installieren

- Melden Sie sich bei der vManageUI aller vManager-Knoten über die URL https://<vmanage-ip>in Ihrem Browser an. Verwenden Sie die VPN 512-IP-Adresse der jeweiligen vManager-Knoten. Sie können sich mit dem Benutzernamen und dem Kennwort des Administrators anmelden.

- Navigieren Sie zu Configuration > Certificates > Control Components (Konfiguration > Zertifikate > Steuerungskomponenten), falls es sich um 20.15/20.18 vManage-Knoten handelt. Bei den Versionen 20.9/20.12 finden Sie unter Konfiguration > Geräte > Controller

  Klicken Sie auf ... für Manager/vManage und dann auf CSR generieren.



- Sobald der CSR generiert wurde, können Sie den CSR herunterladen und anhand der für die Controller ausgewählten Zertifizierungsstelle signieren lassen. Sie können diese Konfiguration unter Administration > Settings > Controller Certificate Authorization (Verwaltung > Einstellungen > Controller-Zertifikatsautorisierung) überprüfen. Wenn Cisco (empfohlen) ausgewählt ist, wird der CSR automatisch vom vManage in das PNP-Portal hochgeladen. Sobald das Zertifikat signiert wurde, wird es automatisch auf vManage installiert.

- Bei manueller Auswahl signieren Sie den CSR manuell über das Cisco PNP-Portal. Navigieren Sie dazu zum Smart Account und zum Virtual Account des jeweiligen SD-WAN-Overlays.

- Sobald das Zertifikat im PNP-Portal verfügbar ist, klicken Sie im gleichen Abschnitt von vManage auf Install certificate (Zertifikat installieren), laden Sie das Zertifikat hoch, und installieren Sie das Zertifikat.

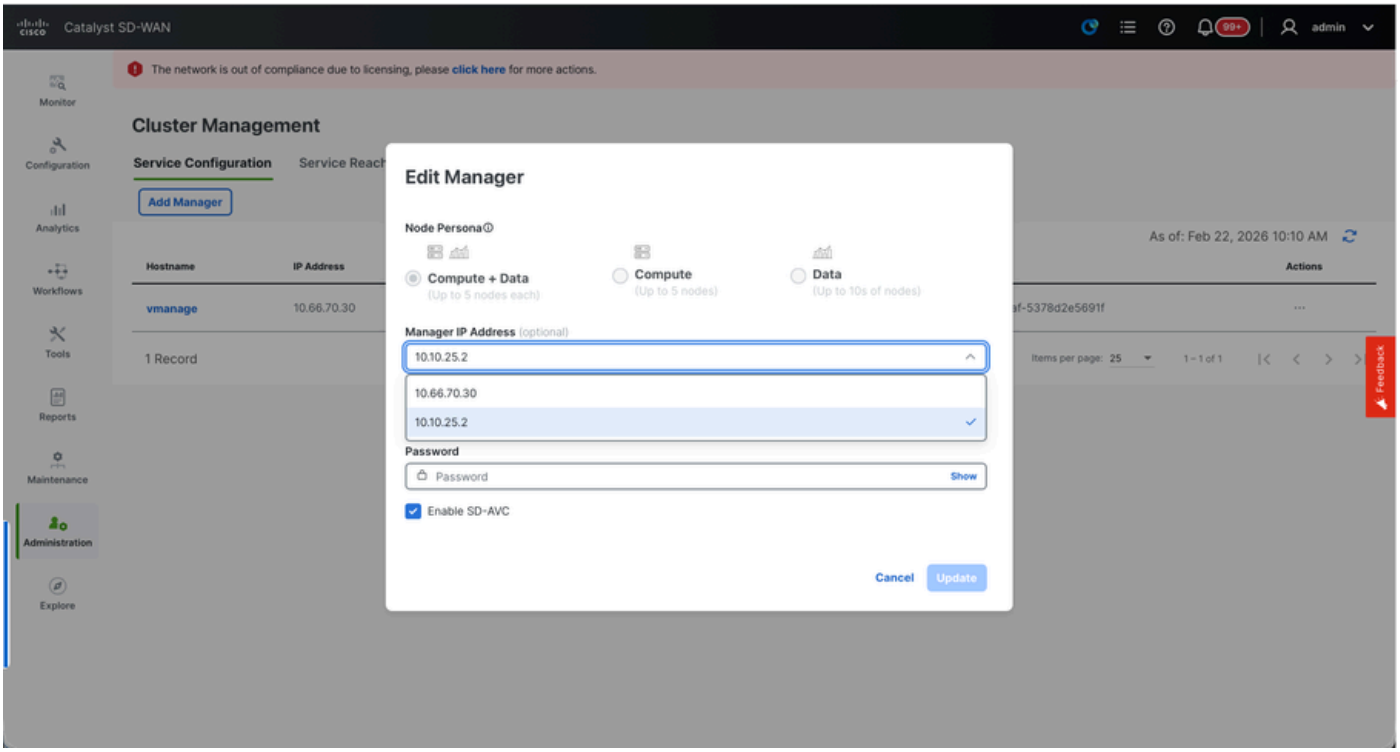
- Das gleiche Verfahren gilt, wenn wir das Digicert- und das Enterprise-Stammzertifikat verwenden.
- Führen Sie diesen Schritt für alle vManage-Knoten aus, die Teil des Clusters sind.

Vorbereiten des vManage-Clusters

- Navigieren Sie auf der Web-UI von vManage-1 zu Administration > Cluster Management, klicken Sie auf ... unter Actions for vManage-1 (Aktionen für vManage-1) und wählen Sie Edit (Bearbeiten).
- Die Knoten-Persona wird automatisch auf Basis der Persona ausgewählt, die wir beim Hochfahren der VM ausgewählt haben.

Anmerkung: Bei einem Cluster mit drei Knoten werden alle drei vManage-Knoten mit "compute+data" als Rolle aufgerufen. Bei einem Cluster mit sechs Knoten werden drei vManage-Knoten mit "compute+data" als persona und drei vManage-Knoten mit "data" als persona aktiviert.

- Wählen Sie aus dem Dropdown-Menü für die Manager-IP-Adresse die Service-Schnittstellen-IP von vManage aus.



- Geben Sie den Benutzernamen und das Passwort ein, mit denen Sie den vManage-Cluster aktivieren möchten, der als Cluster-Anmeldedaten bezeichnet wird.
- Wie bereits erwähnt, müssen auf allen vManage-Knoten dieselben Anmeldeinformationen konfiguriert und beim Hinzufügen aller Knoten zum Cluster verwendet werden.

Optionale Konfiguration:

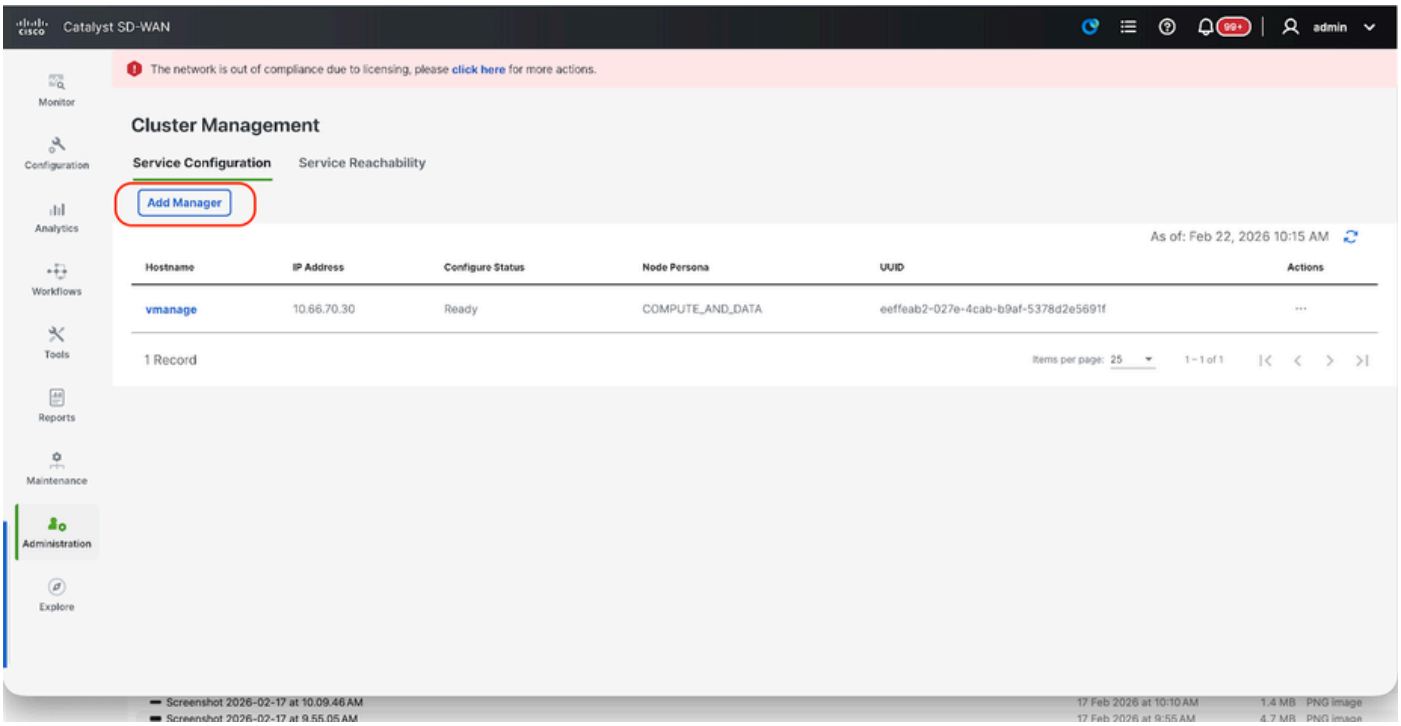
Lesen Sie diese Konfiguration in Ihrem vorhandenen Cluster, um SDAVC zu aktivieren - Muss nur überprüft werden, wenn dies erforderlich ist und nur auf einem vManage-Knoten des Clusters erforderlich ist.

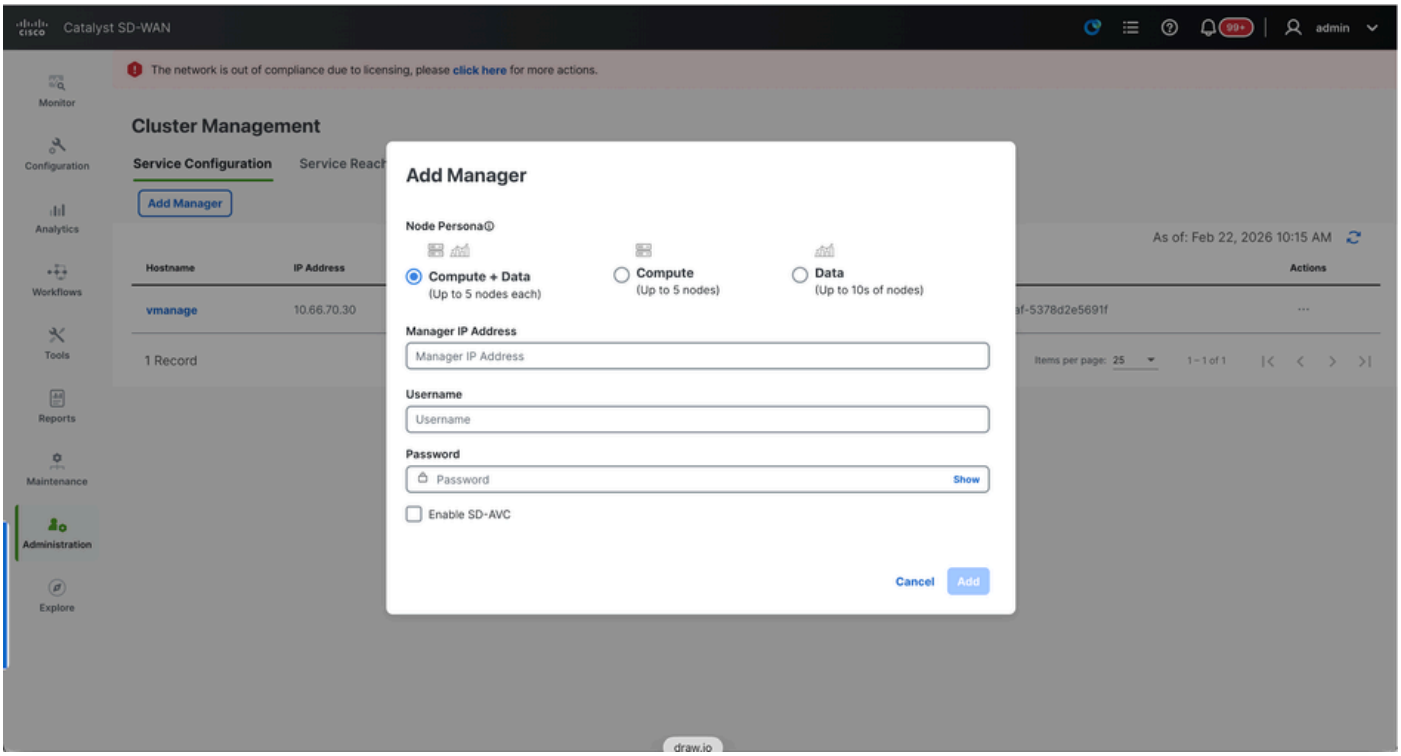
Klicken Sie auf Aktualisieren.

- Nach diesem Vorgang wird der vManage NMS-Dienst im Hintergrund neu gestartet, und die Benutzeroberfläche ist für einige Minuten (etwa 5 bis 10 Minuten) nicht verfügbar. Während dieser Zeit ist der CLI-Zugriff von vManage verfügbar.
- Sobald auf die vManage-1-Benutzeroberfläche zugegriffen werden kann, navigieren Sie zu Administration > Cluster Management, und stellen Sie sicher, dass die IP-Adresse der Service-Schnittstelle von vManage unter der IP-Adresse angezeigt wird.Der Konfigurationsstatus lautet "Ready", und die Node-Persona wird korrekt wiedergegeben. Wechseln Sie zum Abschnitt Erreichbarkeit von Services auf derselben Seite, und stellen Sie sicher, dass alle Services erreichbar sind.
- Wenn wir sehen, dass einer der Dienste noch nicht erreichbar ist, warten Sie bitte. In der Regel dauert etwa 20 bis 30 Minuten.

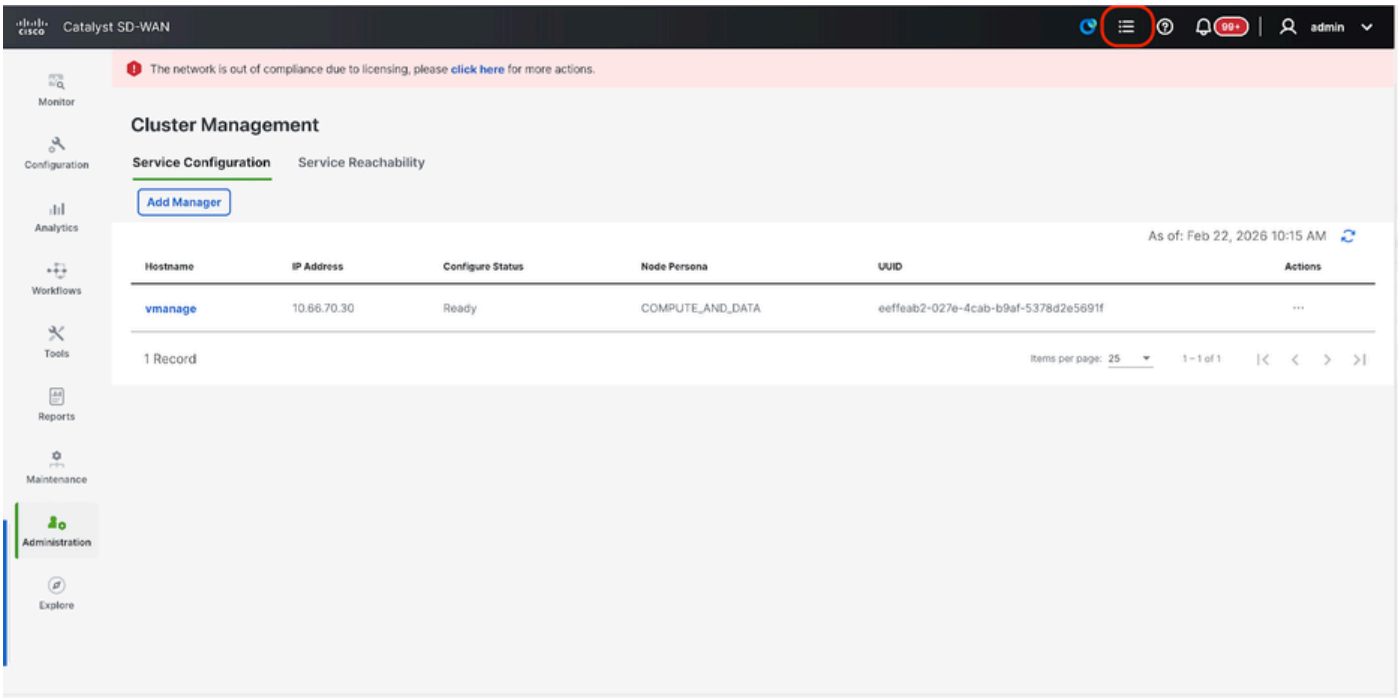
Aufbau des vManage-Clusters

- Navigieren Sie auf der Web-Benutzeroberfläche von vManage-1 zu Administration > Cluster Management, im Abschnitt Service Configuration,
- Klicken Sie auf Add Manager, um ein Popup-Fenster anzuzeigen:





- Wählen Sie den Knoten persona basierend auf den persönlichen Konfigurationen aus, die während der Aktivierung von vManage - 2 durchgeführt wurden.
- Geben Sie die IP-Adresse der Service-Schnittstelle von vManage-2 unter der Manager-IP-Adresse ein.
- Geben Sie den Benutzernamen und das Kennwort ein. Dies sind die gleichen Anmeldeinformationen wie in Schritt 6.
- SDAVC aktivieren: Deaktivieren Sie diese Option, da sie bereits in vManage-1 aktiviert ist.
- Klicken Sie auf Hinzufügen.
- Nach diesem Schritt werden die vManage NMS-Dienste für vManage 1- und 2-Knoten im Hintergrund neu gestartet. Die Benutzeroberfläche ist für einige Minuten von etwa 5 bis 10 Minuten für vManage 1 und 2 nicht verfügbar.
- Während dieser Zeit ist der CLI-Zugriff von vManage 1 und 2 verfügbar.
- Sobald auf die vManage-1-Benutzeroberfläche zugegriffen werden kann, navigieren Sie zu Administration > Cluster Management, stellen Sie sicher, dass die Service-Schnittstellen-IP des vManage unter der IP-Adresse angezeigt wird, der Konfigurationsstatus "Ready" lautet und die Knoten-IP-Adresse korrekt wiedergegeben wird.
- Wechseln Sie zum Abschnitt "Service-Erreichbarkeit" auf derselben Seite, und stellen Sie sicher, dass alle Services für beide vManage-Knoten erreichbar sind.
- Wenn wir sehen, dass einer der Dienste noch nicht erreichbar ist, warten Sie bitte. In der Regel dauert etwa 5 bis 10 Minuten.
- Sie können den Status des Cluster-Hinzufügevorgangs in der Aufgabenliste überprüfen, die oben rechts auf der vManage-Benutzeroberfläche zur Verfügung steht.



- Sie können nach der Liste "Aktive Task" suchen. Wenn die Task immer noch in der Liste "Aktive Task" aufgeführt ist, weist dies darauf hin, dass die Task noch nicht abgeschlossen ist.
- Sie können auf die Aufgabe klicken, um den Fortschritt der gleichen Aufgabe zu überprüfen. Wenn die Aufgabe nicht in der Liste "Aktive Aufgabe" aufgeführt ist, wechseln Sie zu "Abgeschlossen", und stellen Sie sicher, dass die Aufgabe erfolgreich abgeschlossen wurde.
- Fahren Sie erst mit dem nächsten Schritt fort, nachdem diese Punkte validiert wurden.

Diese Punkte müssen berücksichtigt werden, bevor der nächste Knoten zum Cluster hinzugefügt wird:

Überprüfen Sie diese Punkte auf allen UIs der vManage-Knoten, die dem Cluster bisher hinzugefügt wurden:

- Navigieren Sie zu Monitor > Overview of vManage UI, und stellen Sie sicher, dass die Anzahl der vManage-Knoten korrekt wiedergegeben wird und in Abhängigkeit von der Anzahl der Knoten, die dem Cluster hinzugefügt wurden, als erreichbar angezeigt wird.

- Navigieren Sie zu Administration > Cluster Management, und stellen Sie sicher, dass die Service-Schnittstellen-IP des vManage unter IP-Adresse, Configure Status is Ready und Node-Personal korrekt wiedergegeben wird.
- Wechseln Sie zum Abschnitt "Service-Erreichbarkeit" auf derselben Seite, und stellen Sie sicher, dass alle Services für beide vManage-Knoten erreichbar sind.

- Bei jedem Hinzufügen eines Knotens zum Cluster werden die NMS-Dienste aller Knoten im Cluster neu gestartet, sodass die Benutzeroberfläche all dieser Knoten für einige Zeit nicht erreichbar ist.
- Je nach Anzahl der Knoten im Cluster kann es länger dauern, bis die Benutzeroberfläche gesichert ist und alle Dienste erreichbar sind.

- Sie können die Aufgabe in der Aufgabenliste oben rechts in der vManage-Benutzeroberfläche überwachen.
- Auf der vManage-Benutzeroberfläche jedes Knotens, der dem Cluster hinzugefügt wurde, müssen alle Router, Vorlagen und Richtlinien angezeigt werden, wenn sie in vManage-1 verfügbar waren.
- Wenn diese Konfigurationen in vManage-1 nicht vorhanden waren, müssen die vBonds und vSmarts, die zu vManage-1 hinzugefügt wurden, sowie die Konfigurationen Administration > Settings für Organisationsname, vBond, Certificate Authorization (Administration > Einstellungskonfigurationen für Organisationsname, vBond, Zertifikatsautorisierung) auf den übrigen vManage-Knoten, die dem Cluster hinzugefügt wurden, angezeigt werden.
- Wiederholen Sie die gleichen Schritte für die übrigen vManage-Knoten.

Schritt 4: Sicherung/Wiederherstellung der Konfig.-DB

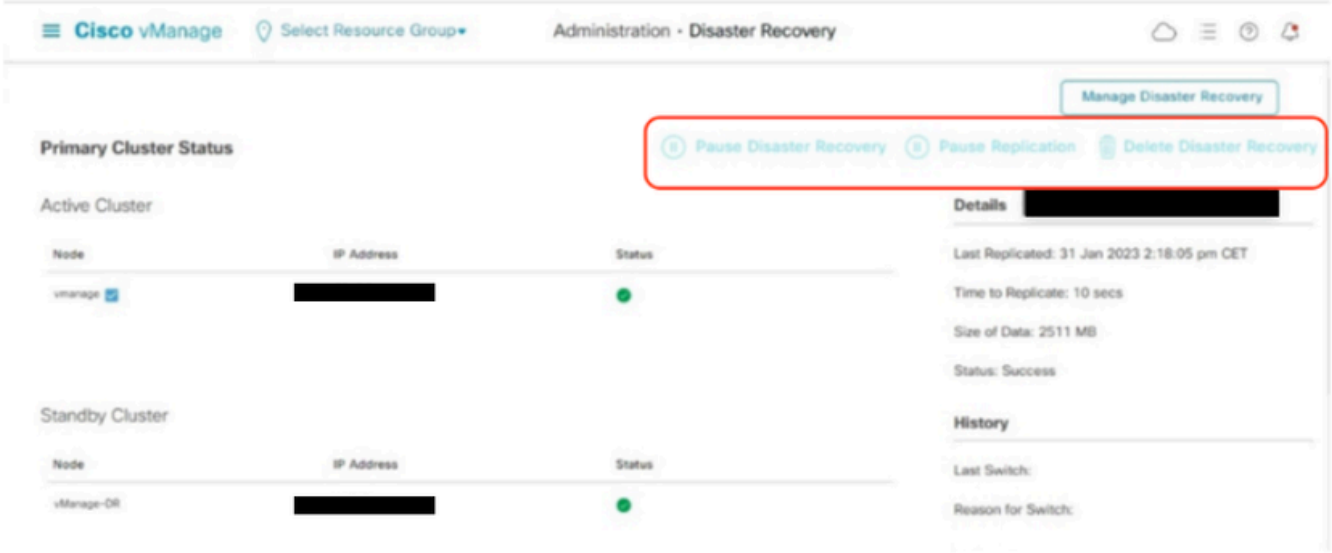
Sammeln von vManage-Konfigurations-DB-Backups und Wiederherstellen auf einem anderen vManage-Knoten

---

Anmerkung: Stellen Sie beim Sammeln des Konfigurations-Datenbank-Backups aus dem vorhandenen vManage-Cluster, in dem die Notfallwiederherstellung aktiviert ist, sicher, dass das Backup gesammelt wird, nachdem die Notfallwiederherstellung auf diesem Knoten angehalten und gelöscht wurde.

Bestätigen Sie, dass keine laufende Disaster Recovery-Replikation vorhanden ist. Navigieren Sie zu Administration > Disaster Recovery und Vergewissern Sie sich, dass der Status "Success" lautet und sich nicht in einem vorübergehenden Status wie "Import Pending" (Ausstehend), "Export Pending" (Ausstehend) oder "Download Pending" (Ausstehend) befindet. Wenn der Status nicht erfolgreich ist, wenden Sie sich an das Cisco TAC, und stellen Sie sicher, dass die Replikation erfolgreich ist, bevor Sie die Disaster Recovery anhalten.

Halten Sie zunächst die Notfallwiederherstellung an, und stellen Sie sicher, dass die Aufgabe abgeschlossen ist. Löschen Sie anschließend die Notfallwiederherstellung, und bestätigen Sie, dass die Aufgabe abgeschlossen ist.



Wenden Sie sich an das Cisco TAC, um sicherzustellen, dass die Notfallwiederherstellung erfolgreich beseitigt wird.

Sammeln der Konfiguration - DB-Backup:

- In der derzeit verwendeten SD-WAN-Fabric können Sie ein Backup der Konfigurationsdatenbank vom vManage-Cluster generieren.
- Bitte beachten Sie, dass wir ein Backup der Konfigurationsdatenbank nur auf einem Knoten des vManage-Clusters generieren müssen, der der führende Konfigurationsdatenbank ist.

- Bei eigenständigem vManage ist dieser vManager selbst der führende Anbieter von Konfigurationsdatenbanken.
- Identifizieren Sie im vManage-Cluster mithilfe des Befehls request nms configuration-db diagnostics den Knoten configuration-db leader.Sie können diesen Befehl auf allen Knoten des vManage-Clusters mit drei Knoten ausführen.
- In einem Cluster mit sechs Knoten muss dieser Befehl auf den vManage-Knoten ausgeführt werden, auf denen configuration-db aktiviert ist, um den Leader-Knoten zu identifizieren. Navigieren Sie zu Administration > Cluster Management, um dies zu überprüfen:
- Wie wir im Screenshot sehen, laufen bei den Knoten, die mit persona COMPUTE_AND_DATA konfiguriert sind, configuration-db.

Dasselbe können Sie mit dem Befehl requestnmsconfiguration-dbstatus in vManageCLI überprüfen. Die Ausgabe erfolgt wie dargestellt

```
vmanage# request nms configuration-db status
NMS configuration database
        Enabled: true
        Status: running PID:32632 for 1066085s
        Native metrics status: ENABLED
        Server-load metrics status: ENABLED
vmanage#
```

- Nach der Ausführung des Befehlsrequest nms configuration-db diagnostics on these nodes, die Ausgabe ist wie folgt:
- Suchen Sie das hervorgehobene Feld für "IsLeader". Wenn es auf 1 gesetzt ist, bedeutet dies, dass der Knoten der führende Knoten ist, und wir können die Sicherung der Konfigurationsdatenbank von ihm erfassen.

```
vManage-3# request nms configuration-db diagnostics
NMS configuration database
Checking cluster connectivity for ports 7687,7474 ...
Pinging vManage  node 0 on 169.254.1.5:7687,7474...
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2026-02-18 12:41 UTC
SENT (0.0013s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (0.0022s) Handshake with 169.254.1.5:7474 completed
SENT (1.0024s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (1.0028s) Handshake with 169.254.1.5:7687 completed
SENT (2.0044s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (2.0050s) Handshake with 169.254.1.5:7474 completed
SENT (3.0064s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (3.0072s) Handshake with 169.254.1.5:7687 completed
SENT (4.0083s) Starting TCP Handshake > 169.254.1.5:7474
RCVD (4.0091s) Handshake with 169.254.1.5:7474 completed
SENT (5.0106s) Starting TCP Handshake > 169.254.1.5:7687
RCVD (5.0115s) Handshake with 169.254.1.5:7687 completed
Max rtt: 0.906ms | Min rtt: 0.392ms | Avg rtt: 0.724ms
TCP connection attempts: 6 | Successful connections: 6 | Failed: 0 (0.00%)
Nping done: 1 IP address pinged in 5.01 seconds
Pinging vManage  node 1 on 169.254.2.5:7687,7474...
========== SNIP ==========
Connecting to 10.10.10.3...
+-------------------------------------------------------------------------------------+
| type             | row                                    | attributes[row]["value"] |
+-------------------------------------------------------------------------------------+
| "StoreSizes"     | "TotalStoreSize"                       | 85828934                 |
| "PageCache"      | "Flush"                                | 4268666                  |
| "PageCache"      | "EvictionExceptions"                   | 0                        |
| "PageCache"      | "UsageRatio"                           | 0.09724264705882353      |
| "PageCache"      | "Eviction"                             | 2068                     |
| "PageCache"      | "HitRatio"                             | 1.0                      |
| "ID Allocations" | "NumberOfRelationshipIdsInUse"         | 2068                     |
| "ID Allocations" | "NumberOfPropertyIdsInUse"             | 56151                    |
| "ID Allocations" | "NumberOfNodeIdsInUse"                 | 7561                     |
| "ID Allocations" | "NumberOfRelationshipTypeIdsInUse"     | 31                       |
| "Transactions"   | "LastCommittedTxId"                    | 214273                   |
| "Transactions"   | "NumberOfOpenTransactions"             | 1                        |
| "Transactions"   | "NumberOfOpenedTransactions"           | 441742                   |
| "Transactions"   | "PeakNumberOfConcurrentTransactions"   | 11                       |
| "Transactions"   | "NumberOfCommittedTransactions"        | 414568                   |
| "Causal Cluster" | "IsLeader"                             | 1         >>>>>>>>>      |
| "Causal Cluster" | "MsgProcessDelay"                      | 0                        |
| "Causal Cluster" | "InFlightCacheTotalBytes"              | 0                        |
+-------------------------------------------------------------------------------------+
18 rows
ready to start consuming query after 388 ms, results consumed after another 13 ms
Completed
Connecting to 10.10.10.3...
Displaying the Neo4j Cluster Status
+-----------------------------------------------------------------------------------------------------------
```

```
| name     | aliases | access       | address            | role       | requestedStatus | currentStatus
+-------------------------------------------------------------------------------------------------------------
| "neo4j"  | []      | "read-write" | "169.254.3.5:7687" | "leader"   | "online"        | "online"
| "neo4j"  | []      | "read-write" | "169.254.2.5:7687" | "follower" | "online"        | "online"
| "neo4j"  | []      | "read-write" | "169.254.1.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.3.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.2.5:7687" | "follower" | "online"        | "online"
| "system" | []      | "read-write" | "169.254.1.5:7687" | "leader"   | "online"        | "online"
+-------------------------------------------------------------------------------------------------------------
6 rows
ready to start consuming query after 256 ms, results consumed after another 3 ms
Completed
Total disk space used by configuration-db:
60M     .
```

Verwenden Sie diesen Befehl, um das Backup configuration-db vom angegebenen Konfigurationsdb-Leader "vManage" zu erfassen.

```
request nms configuration-db backup path /opt/data/backup/
```

Die erwartete Ausgabe lautet wie folgt:

```
vmanage# request nms configuration-db backup path /opt/data/backup/june18th
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/june18th.tar.gz
sha256sum: 8d0f5af8aee4e70f05e3858be6bdd5e6c136134ae47c383569ec883080f5d359
Removing the temp staging dir :/opt/data/backup/staging
vmanage#
```

- Notieren Sie sich die Anmeldeinformationen für die Konfigurationsdatenbank, wenn diese aktualisiert wurde.
- Wenn Sie die Anmeldeinformationen für die Konfigurationsdatenbank nicht kennen, wenden Sie sich an das TAC, um die Anmeldeinformationen für die Konfigurationsdatenbank von den vorhandenen vManage-Knoten abzurufen.
- Die Standardanmeldeinformationen für die -db-Konfiguration sind Benutzername: neo4j und Passwort: Kennwort

Wiederherstellen der Konfiguration - db-Sicherung auf einem anderen vManage-Knoten

Kopieren Sie das Sicherungsverzeichnis configuration-db mithilfe von SCP in das Verzeichnis

/home/admin/ von vManage.

Beispielausgabe des Befehls scp:

```
XXXXXXXXX Downloads % scp june18th.tar.gz admin@10.66.62.27:/home/admin/
viptela 20.15.4.1

(admin@10.66.62.27) Password:
(admin@10.66.62.27) Password:
june18th.tar.gz
```

Zum Wiederherstellen des "configuration-db"-Backups müssen wir zunächst die "configuration-db"-Anmeldeinformationen konfigurieren. Wenn Ihre Anmeldeinformationen für configuration-db default(neo4j/password) sind, können wir diesen Schritt überspringen.

Um die Anmeldeinformationen für configuration-db zu konfigurieren, verwenden Sie den Befehl request nms configuration-db update-admin-user.Use the username and password of your choice.

Bitte beachten Sie, dass der Anwendungsserver von vManage neu gestartet wurde. Aufgrund dessen kann auf die vManage-Benutzeroberfläche für kurze Zeit nicht mehr zugegriffen werden.

```
vmanage# request nms configuration-db update-admin-user
configuration-db
Enter current user name:neo4j
Enter current user password:password
Enter new user name:ciscoadmin
Enter new user password:ciscoadmin
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Successfully updated configuration database admin user(this is service node, please repeat same operati
Successfully restarted vManage Device Data Collector
Successfully restarted NMS application server
Successfully restarted NMS data collection agent
vmanage#
```

Nach dem wir fortfahren können, die Konfiguration-db-Backup wiederherzustellen:

Wir können den Befehl request nms configuration-db restore path /home/admin/< > verwenden, um configuration-db auf dem neuen vManage wiederherzustellen:

```
vmanage# request nms configuration-db restore path /home/admin/june18th.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Successfully backup database to /opt/data/backup/configdb-local-tmp-20230623-160954.tar.gz
Configuration database is running in a standalone mode
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
```

```
Successfully saved cluster configuration for localhost
Successfully saved vManage root CA information for device: "53f95156-f56b-472f-b713-d164561b25b7"
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Reseting NMS configuration database on localhost
Loading NMS configuration database on localhost
Starting NMS configuration database on localhost
Waiting for 180s or the instance to start...
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Successfully reinserted vmanage root ca information
Starting NMS application server on localhost
Waiting for 180s for the instance to start...
Successfully restored database
```

Sobald die Konfigurationsdatenbank wiederhergestellt ist, stellen Sie sicher, dass auf die vManage-Benutzeroberfläche zugegriffen werden kann. Warten Sie etwa 5 Minuten, und versuchen Sie dann, auf die Benutzeroberfläche zuzugreifen.

Nachdem Sie sich erfolgreich bei der Benutzeroberfläche angemeldet haben, stellen Sie sicher, dass die Liste der Edge-Router, die Vorlage, die Richtlinien und alle anderen Konfigurationen, die auf der vorherigen oder vorhandenen vManage-Benutzeroberfläche vorhanden waren, auf der neuen vManage-Benutzeroberfläche wiedergegeben werden.

Schritt 5: Disaster Recovery auf einem vManage-Cluster aktivieren

Wichtige Überprüfungen

Zwei separate vManage-Cluster mit drei Knoten müssen konfiguriert und betriebsbereit sein, um mit der Notfallwiederherstellung fortfahren zu können. Auf dem aktiven Cluster müssen Validierungssteuerungen und Controller integriert sein. Falls sich der Validator und die Controller am DR-Standort befinden, müssen sie auch im aktiven Cluster und nicht im DR vManage-Cluster integriert werden.

Cisco empfiehlt, vor der Registrierung der Disaster Recovery die folgenden Anforderungen zu erfüllen:

- Stellen Sie sicher, dass der primäre und der sekundäre Knoten über HTTPS über ein Transport-VPN (VPN 0) erreichbar sind.
- Stellen Sie sicher, dass die Cisco vSmart Controller und Cisco vBond Orchestrator der sekundären Einrichtung mit der primären Einrichtung verbunden sind.
- Stellen Sie sicher, dass auf dem primären und sekundären Cisco vManage-Knoten dieselbe Cisco vManage-Version ausgeführt wird.
- Out-of-Band-Cluster-Schnittstelle (Service-Schnittstelle) in VPN 0.
- Für jede vManage-Instanz innerhalb eines Clusters ist neben den für VPN 0 (Transport) und VPN 512 (Management) verwendeten Schnittstellen eine dritte Schnittstelle (Cluster-

Verbindung) erforderlich.

- Diese Schnittstelle wird für die Kommunikation und Synchronisierung zwischen den vManage-Servern im Cluster verwendet.
- Diese Schnittstelle muss mindestens 1 Gbit/s betragen und eine Latenz von maximal 4 ms aufweisen. Eine Schnittstelle mit 10 Gbit/s wird empfohlen.
- Beide vManage-Knoten müssen sich über diese Schnittstelle erreichen können: sei es ein Layer-2-Segment oder durch Layer-3-Routing.
- In jedem vManage muss diese Schnittstelle in der GUI als Cluster-Schnittstelle konfiguriert werden (Administration > Cluster Management - eigene Out-of-Band-Cluster-Schnittstellen-IP-Adresse, Benutzer und Kennwort angeben).
- Damit Cisco vManage-Knoten über mehrere Rechenzentren hinweg miteinander kommunizieren können, aktivieren Sie die TCP-Ports 8443 und 830 auf den Firewalls Ihres Rechenzentrums.
- Stellen Sie sicher, dass alle Services (Anwendungsserver, Konfigurationsdatenbank, Messaging-Server, Koordinierungsserver und Statistikdatenbank) auf beiden Cisco vManage-Knoten aktiviert sind.
- Verteilung aller Controller, einschließlich Cisco vBond Orchestrator, auf primäre und sekundäre Rechenzentren Stellen Sie sicher, dass diese Controller über Cisco vManage-Knoten erreichbar sind, die über diese Rechenzentren verteilt sind. Die Controller sind nur mit dem primären Cisco vManage-Knoten verbunden.
- Stellen Sie sicher, dass im aktiven (primären) und im Standby-Knoten (sekundären) Cisco vManage keine weiteren Vorgänge ausgeführt werden. Stellen Sie beispielsweise sicher, dass keine Server aktualisiert oder Vorlagen an Geräte angehängt werden.
- Deaktivieren Sie den Cisco vManage HTTP/HTTPS-Proxyserver, wenn er aktiviert ist. Informationen zur Cisco vManage-Kommunikation mit externen Servern finden Sie unter HTTP/HTTPS-Proxy-Server. Wenn Sie den Proxyserver nicht deaktivieren, versucht Cisco vManage, eine Notfallwiederherstellungs-Kommunikation über die Proxy-IP-Adresse herzustellen, selbst wenn die Out-of-Band-Cluster-IP-Adressen von Cisco vManage direkt erreichbar sind. Sie können den Cisco vManage HTTP/HTTPS-Proxyserver nach Abschluss der Disaster Recovery-Registrierung erneut aktivieren.
- Bevor Sie mit der Registrierung für die Notfallwiederherstellung beginnen, navigieren Sie zum Fenster Extras > Netzwerk neu erkennen auf dem primären Cisco vManage-Knoten, und suchen Sie erneut nach den Cisco vBond Orchestrator.

Konfigurationen

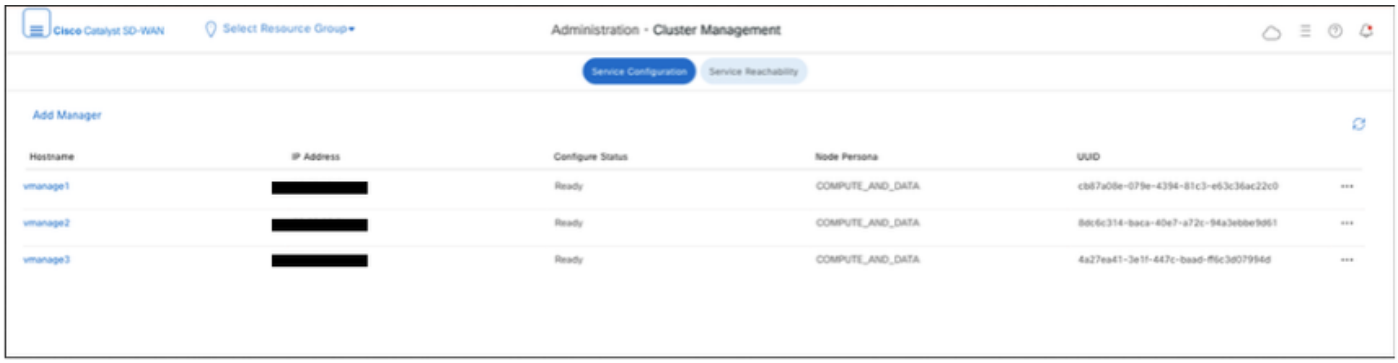
Weitere Informationen zu vManage Disaster Recovery finden Sie unter diesem Link.

Die beiden separaten Cluster mit drei Knoten wurden bereits erstellt. Dabei wird vorausgesetzt,

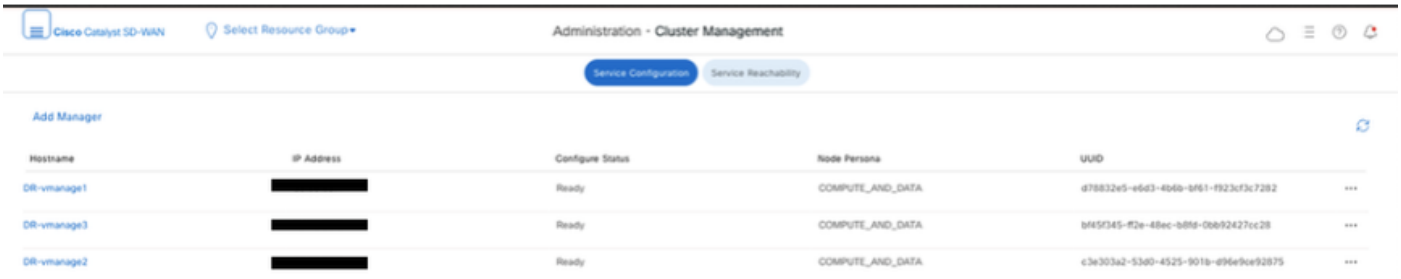
dass jeder SD-WAN-Manager über die absolute Mindestkonfiguration verfügt und die Zertifizierung abgeschlossen ist.

Navigieren Sie zu Administration > Cluster Management auf beiden Clustern, und überprüfen Sie, ob alle Knoten bereit sind.

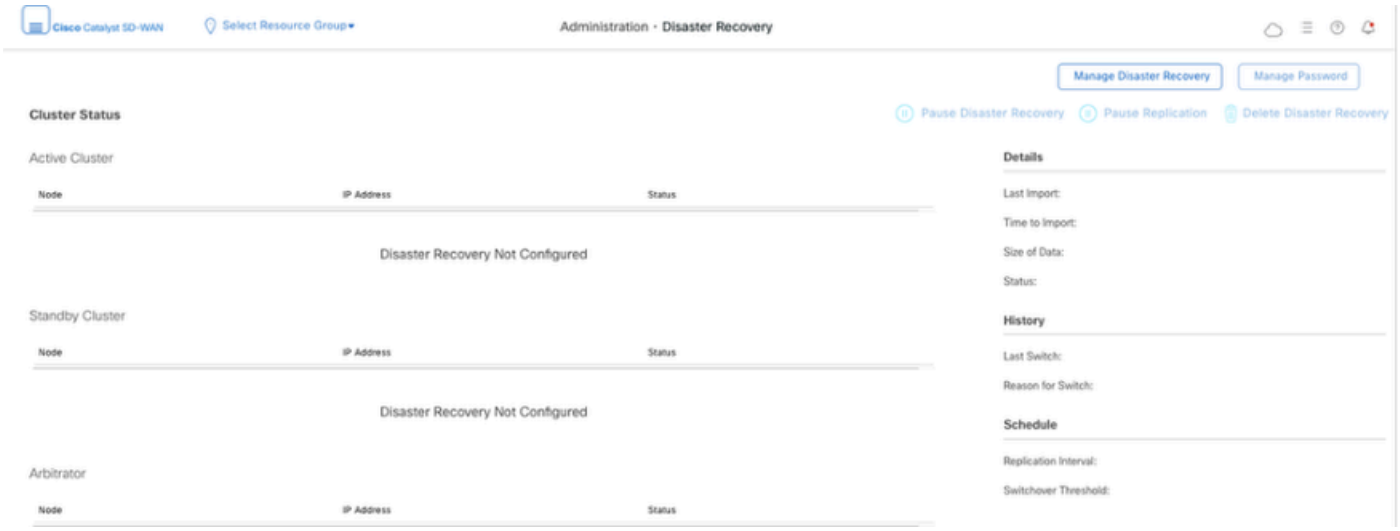
Rechenzentrums-vManagement



DR-Verwaltung



Navigieren Sie zu Administration > Disaster Recovery of Primary vManage Cluster. Klicken Sie auf Disaster Recovery verwalten.



Geben Sie im Popup-Fenster die Details für den primären und sekundären vManage ein.

Die anzuzeigenden IP-Adressen sind die IP-Adressen der Out-of-Band-Clusterschnittstellen.

Verwenden Sie vorzugsweise die IP-Adresse der VPN 0-Service-Schnittstelle von vManage-1 in jedem Cluster.

Die Anmeldedaten müssen die eines Netzwerkadministratorbenutzers sein und dürfen nach der Konfiguration der Notfallwiederherstellung nicht geändert werden, es sei denn, sie werden gelöscht. Für die Notfallwiederherstellung können separate vManage-Anmeldeinformationen für lokale Benutzer verwendet werden. Wir müssen sicherstellen, dass der lokale vManage-Benutzer Teil der netadmin-Gruppe ist. Hier können sogar Administratoranmeldeinformationen verwendet werden.

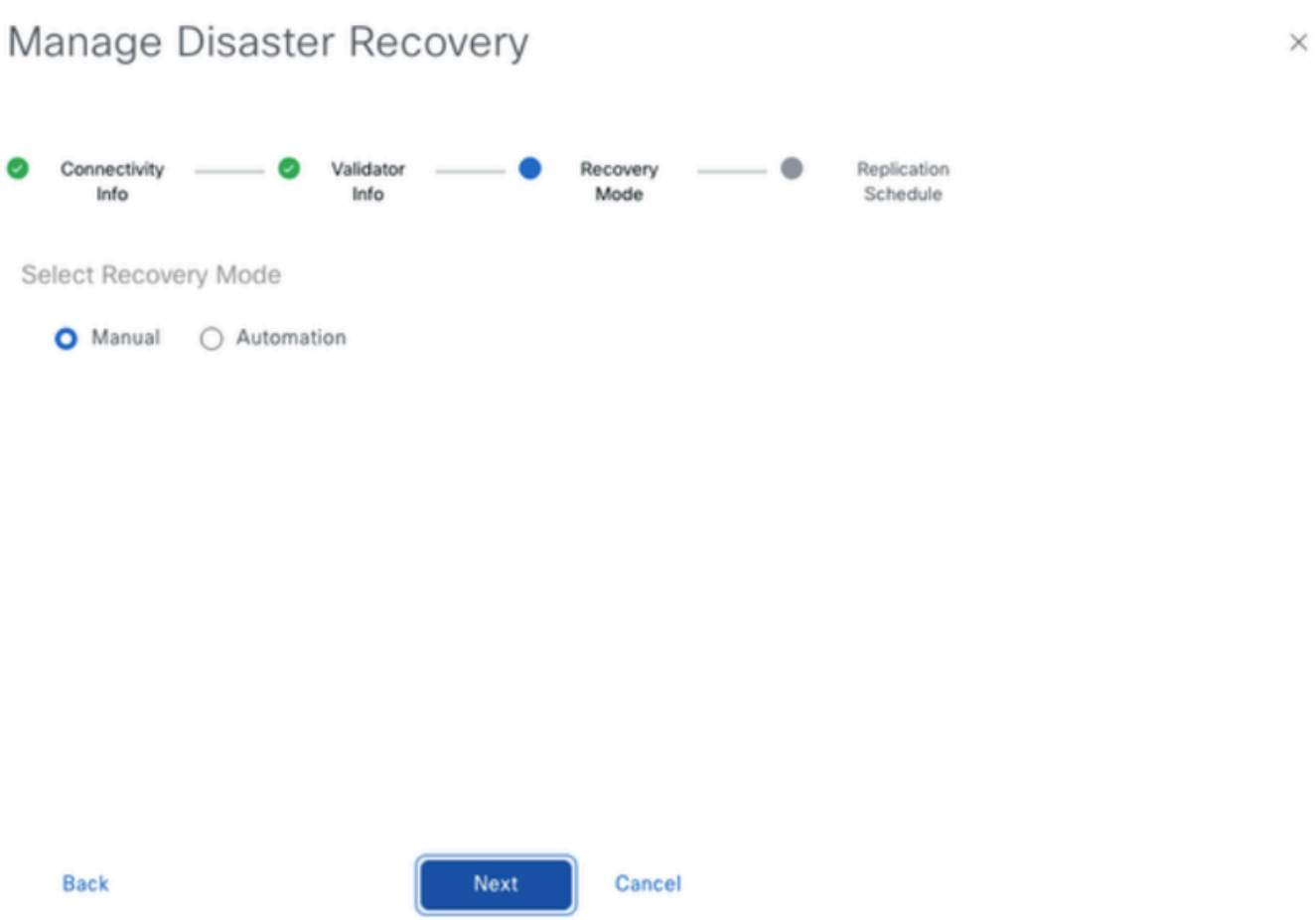
Klicken Sie nach dem Ausfüllen auf Weiter.

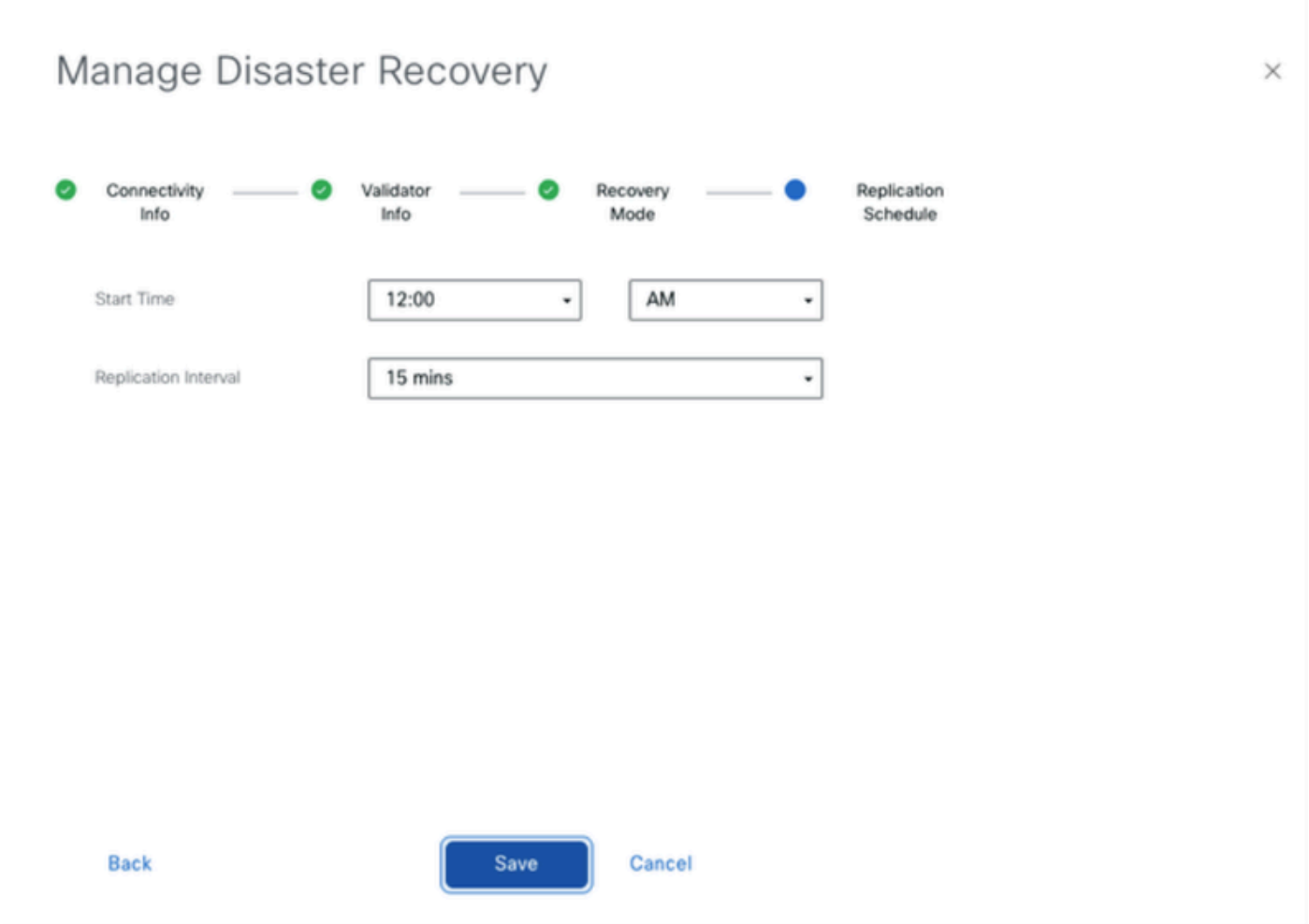
- Füllen Sie die Details der vBond-Controller aus.

Die vBond-Controller müssen über Netconf in der angegebenen IP-Adresse erreichbar sein.

Klicken Sie nach dem Ausfüllen auf Weiter.

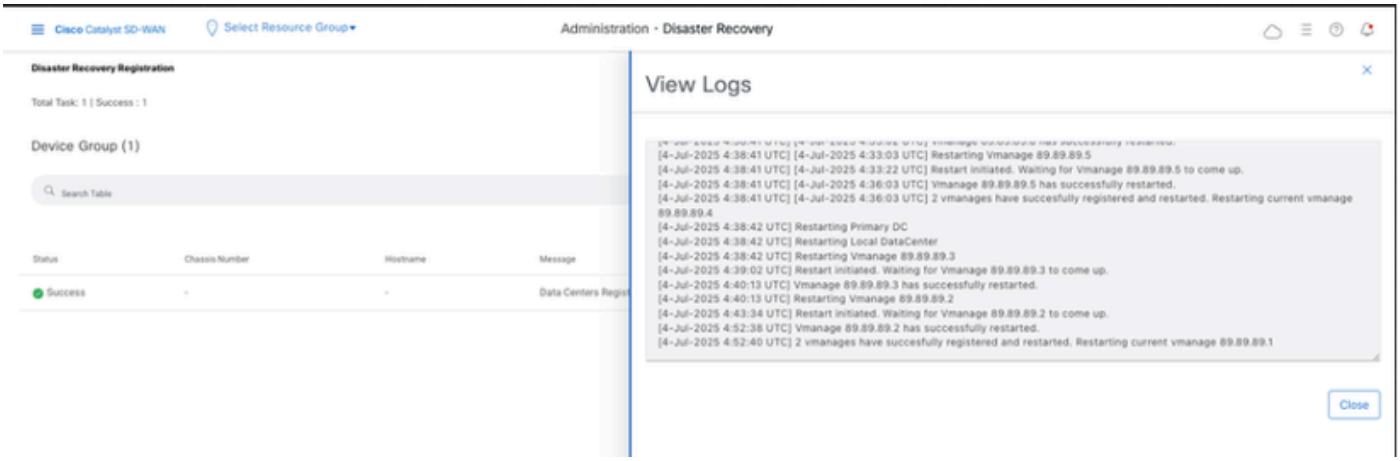
- Wählen Sie im Wiederherstellungsmodus die Option Manual (Manuell). Der Automatisierungsmodus ist veraltet. Klicken Sie auf Next (Weiter).


Manage Disaster Recovery
Connectivity Info
Validator Info
Recovery Mode
Replication Schedule
Select Recovery Mode
Manual
Automation
Back
Next
Cancel



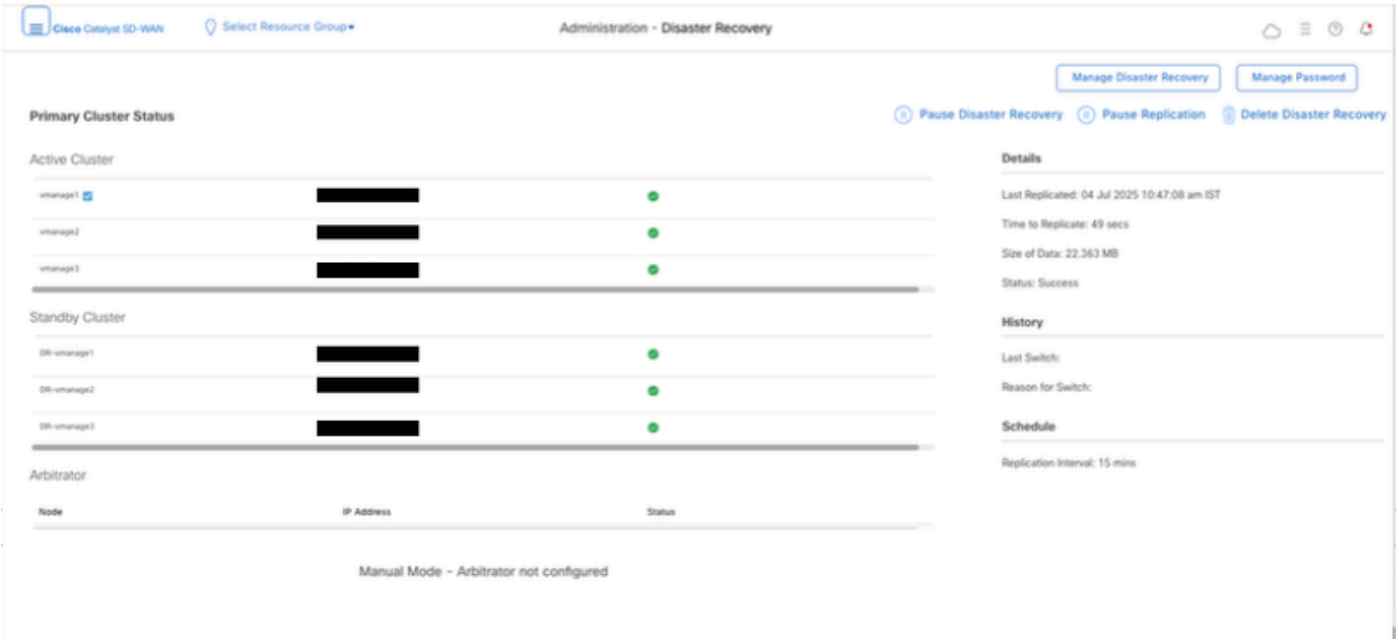
Legen Sie den Wert fest, und klicken Sie auf Speichern.

- Die DR-Registrierung beginnt jetzt. Klicken Sie auf die Aktualisierungsschaltfläche, um den Status und die Fortschrittsprotokolle manuell zu aktualisieren. Dieser Vorgang kann 20-30 Minuten dauern.



Verifizierung

Navigieren Sie zu Administration > Disaster Recovery, um den Status der Disaster Recovery und den Zeitpunkt der letzten Datenreplikation anzuzeigen.



Anmerkung: Die Replikation kann je nach Datenbankgröße mehrere Stunden dauern. Außerdem kann es einige Zyklen dauern, bis die Replikation erfolgreich abgeschlossen ist.

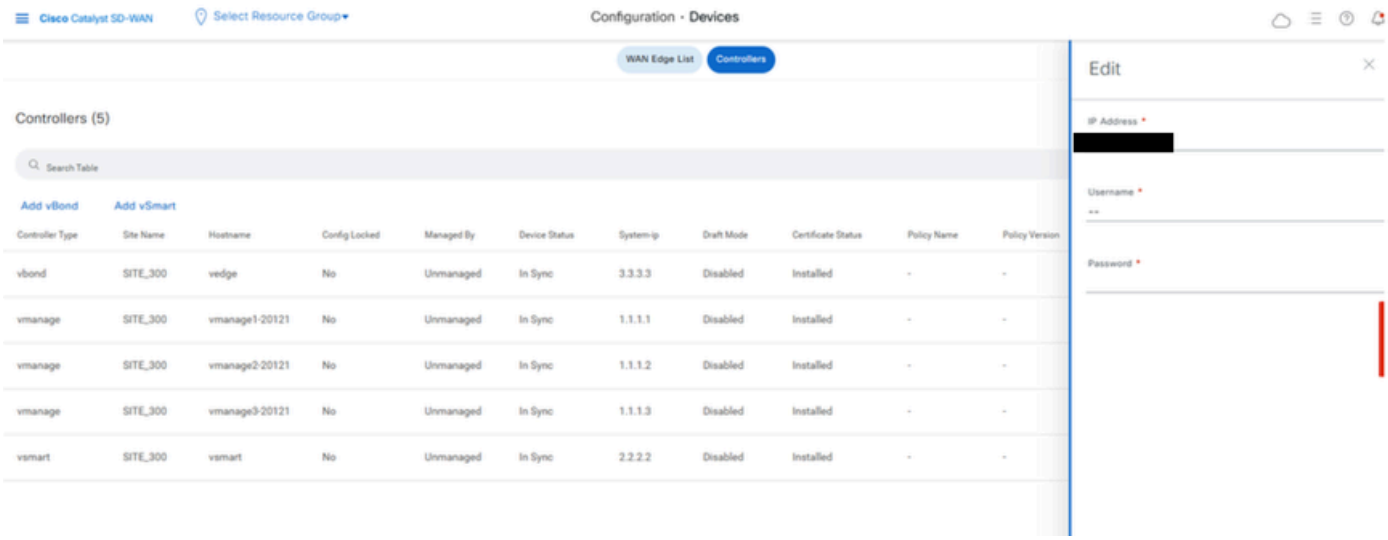
Schritt 6: Neuauthentifizierung von Controllern und Ungültigerklärung alter Controller

Nach der Wiederherstellung der Konfigurationsdatenbank müssen alle neuen Controller (vmanage/vsmart/vbond) im Fabric erneut authentifiziert werden.

Hinweis: Wenn in der Produktion die zur erneuten Authentifizierung verwendete Schnittstellen-IP die Tunnel-Schnittstellen-IP ist, müssen Sie sicherstellen, dass der NETCONF-Dienst auf der Tunnelschnittstelle von vManage, vSmart und vBond sowie auf den Firewalls entlang des Pfads zugelassen ist. Der zu öffnende Firewall-Port ist der TCP-Port 830 als bidirektionale Regel vom DR-Cluster zu allen vBonds und vSmarts .

Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.

- Klicken Sie auf die drei Punkte in der Nähe der einzelnen Controller, und klicken Sie dann auf Bearbeiten.



- Ersetzen Sie die IP-Adresse (System-IP des Controllers) durch die IP-Adresse des Transport-VPN 0 (Tunnelschnittstelle). Geben Sie Benutzername und Kennwort ein, und klicken Sie auf "Save" (Speichern).
- Gleiches für alle neuen Controller im Fabric tun

Synchronisieren der Root-Zertifikatskette

Führen Sie diesen Schritt aus, nachdem alle Controller integriert wurden:

Führen Sie auf einem Cisco SD-WAN Manager-Server im neu aktiven Cluster die folgenden Aktionen aus:

Geben Sie diesen Befehl ein, um das Root-Zertifikat mit allen Cisco Catalyst SD-WAN-Geräten im neu aktiven Cluster zu synchronisieren:

https://vmanage-url/dataservice/system/device/sync/rootcertchain

Geben Sie diesen Befehl ein, um die UUID des Cisco SD-WAN-Managers mit dem Cisco SD-WAN Validator zu synchronisieren:

https://vmanage-url/dataservice/certificate/syncvbond

Sobald die Fabric wiederhergestellt ist und die Steuerungs- und BFD-Sitzungen für alle Edges und Controller in der Fabric verfügbar sind, müssen die alten Controller (vmanage/vsmart/vbond) in der Benutzeroberfläche ungültig gemacht werden.

- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Zertifikate.
- Auf Controller klicken
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Ungültig
- Klicken Sie auf Senden,
- Klicken Sie auf der verwalteten Benutzeroberfläche auf Konfiguration > Geräte > Controller.
- Klicken Sie auf die drei Punkte in der Nähe des Controllers (vmanage/vsmart/vbond) aus der alten Fabric. Klicken Sie auf Löschen

Nachprüfungen

Diese Nachprüfungen gelten für alle Bereitstellungskombinationen.

Cloud-Edge-Router reaktivieren:

- Wenn C800v Teil des Overlays und verwaltete signierte Elemente sind, müssen sie erneut authentifiziert werden, d. h.:

```
request platform software sdwan vedge_cloud activate chassis-number

        token
```

- Bestätigen, dass die Steuerungsverbindungen und BFD-Sitzungen aktiv sind
- End-to-End-Datenverkehr der Anwendungen bestätigen
- Wenn vor der Neuerstellung der Fabric an den Edges Änderungen am Port-Hop vorgenommen wurden, müssen diese rückgängig gemacht werden.
- Stellen Sie sicher, dass die Elemente wie erwartet angezeigt werden:
    - Vorlagen
    - Richtlinien
    - Geräteseite (beide Registerkarten)WAN vEdge-Liste undController

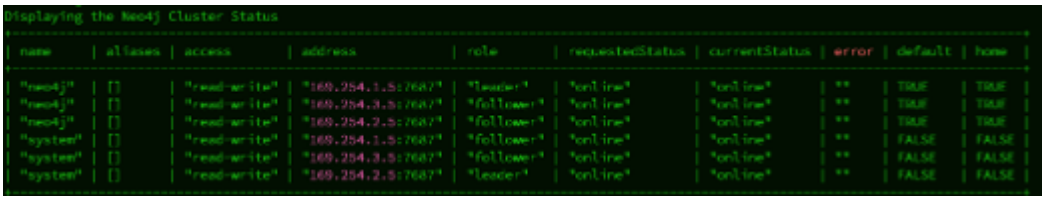
  vNachprüfungen verwalten

- Gilt für vManage-Knoten:

  Konfigurations-DB(Neo4j)-Prüfungen:

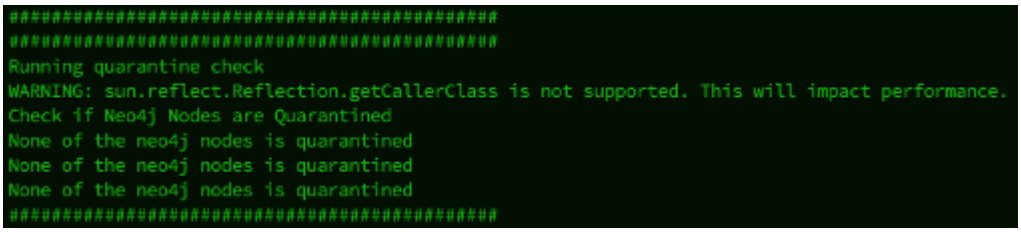
  Führen Sie den Befehl "request nms configuration-db diagnostics" auf allen vManage-Knoten aus:

  1. Node Online und Leadership Status prüfen:(nicht für alle Versionen verfügbar)



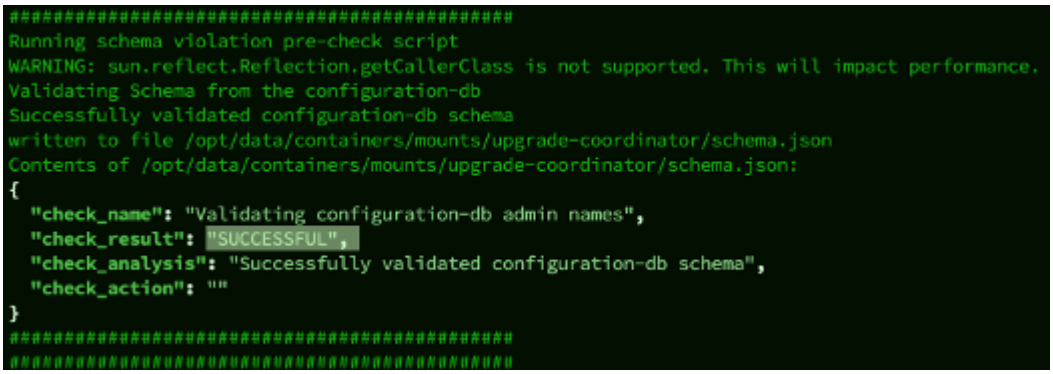
"Neo4j" muss 3 Nodes online und 1 Leader und 2 Follower zeigen. "system" muss auch 3 Knoten online und 1 Leader und 2 Follower anzeigen, da dies jedoch nicht der Standard-DB ist, ist das Standard-Flag falsch. Wenn es weniger als 3 Einträge in jedem neo4j und System bedeutet, dass Knoten aus Cluster gefallen. Wenden Sie sich zur Problembehebung an das Cisco TAC.

2. Überprüfen Sie, ob ein Knoten "quarantine" ist.

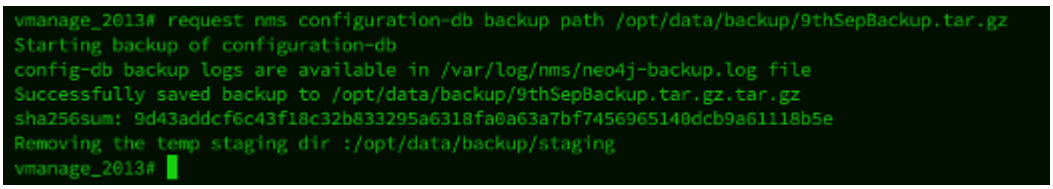


Keiner der Knoten darf sich im Quarantänestatus befinden.

3. Die Schemavalidierung muss "erfolgreich" sein.



4. Erstellen Sie mit dem Befehl "request nms configuration-db diagnostics" ein Sicherungs-Image für die Konfigurationsdatenbank, und stellen Sie sicher, dass es erfolgreich ist.



Wenden Sie sich bei Inkonsistenzen oder Fehlern zur Fehlerbehebung an das Cisco TAC.

Alternativ können wir diese API-Aufrufe ausführen, um den Status des verwalteten Knotens für einen Cluster zu bestätigen (für alle COMPUTE+DATA-Knoten) - funktioniert nur mit Version 20.12 und höher

```
go to vshell of the vmanage node ( to be done on all vmanages)
```

```
================================================================
curl -u

       :

          -H "Content-Type: application/json"   -d '{"statements":[{"statement":"call dbms.cluster.over

         :7474/db/neo4j/tx/commit | jq -r
curl -u

          :

             -H "Content-Type: application/json"   -d '{"statements":[{"statement":"show databases"}]}'

            :7474/db/neo4j/tx/commit | jq -r
```

Stellen Sie sicher, dass in einem Cluster nur ein Leader für neo4j und System und Rest als Follower vorhanden ist.Stellen Sie sicher, dass alle Knoten online sind.Wenn Sie 3 Node-Cluster haben (alle drei sind COMPUTE+DATA), darf es nur einen Leader für neo4j und System geben.Jede Abweichung,Sie müssen TAC kontaktieren

5. Suchen Sie in /var/log/kern.log nach Laufwerks-, Mem- oder E/A-Fehlern. Dies muss auf allen vManage-Knoten überprüft werden.

6.Überprüfen Sie den Schritt, wenn Sie ein neues Cluster für vmanage bilden, das zwischen den einzelnen Knoten kein CC hat.
Führen Sie ssh als vmanage-admin von Knoten 1 zu anderen Knoten Cluster-IP und vise versa aus, um zu überprüfen, ob ein öffentlicher Schlüssel ausgetauscht wird und passwortloses ssh funktioniert [Zustimmung Token ist für die hier abgebildeten Schritte erforderlich]

```
DR-vManage-1:~# ssh -i /etc/viptela/.ssh/id_dsa -p 830 vmanage-admin@



The authenticity of host '[192.168.50.5]:830 ([192.168.50.5]:830)' can't be established.
ECDSA key fingerprint is SHA256:rSpscoYCVC+yifUMHVTlxtjqmyrZSFg93msFdoSUieQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.50.5]:830' (ECDSA) to the list of known hosts.
viptela 20.9.3.0.31

Password:
```

Falls die Ausgabe die Eingabe des Kennworts verlangt, wenden Sie sich an das TAC.

Controller-Postprüfungen:

Gilt für alle SD-WAN-Controller (vBond, vManage, vSmart):

Führen Sie die Befehle auf allen Controllern im Overlay aus, und bestätigen Sie, dass die angezeigte vManage UUID und die Seriennummern für die aktuelle Fabric gültig sind:

vBond-Befehle:

show orchestrator gültiges-vsmarts

show orchestrator Gültig-vManage-ID

vManage/vSmart-Befehle:

show control valid-vsmarts

show control valid-vmanage-id

Beachten Sie, dass die Ausgabe von show control valid-vsmarts die Seriennummern von vSmarts- und vManage-Knoten enthält.

Vergleichen Sie sie mit denen in der vManage-Benutzeroberfläche. Navigieren Sie zum Abschnitt Konfiguration > Zertifikate > Controller.

Wenn zusätzliche Einträge für die UUID/Seriennummer angezeigt werden, die derzeit nicht in die Fabric integriert sind, müssen wir sie löschen. Sie können sich auch an das Cisco TAC wenden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.