Uw Catalyst SD-WAN-verbinding opnieuw opbouwen

Inhoud

Inleiding

In dit document wordt beschreven hoe u een Cisco SD-WAN-fabric opnieuw kunt maken, inclusief back-ups maken van controllerconfiguraties en deze herstellen voor verschillende implementaties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Cisco Software Central
- Download de Controllers software van software.cisco.com

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Voorwaarden voor de wederopbouw van de stof

- Nieuwe set systeem-ips, site-ids moeten worden geconfigureerd voor de nieuwe structuur voor de controllers
- Zorg ervoor dat er firewallregels zijn ingesteld om communicatie tussen de controllers en de randen mogelijk te maken
- Noteer de neo4j (configuratie-db) gebruikersnaam en wachtwoord (het moet hetzelfde zijn op alle vManage-knooppunten in een cluster)
- Port-hop op alle randen uitschakelen
- Verhoog de sierlijke herstarttimers tot 7 dagen

- Alarmen wissen in 3reparty tools voor migratie
- Historische statusgegevens (Alarmen, Gebeurtenissen, Apparaatstatussen, enzovoort) gaan verloren, tenzij er een eerdere installatie is om statistieken naar een externe server zoals vAnalytics te exporteren
- Als Cloud OnRamp is geconfigureerd, moet u ervoor zorgen dat u bereikbaar bent voor de c8000v die vóór het begin van deze activiteit in de cloud is geïmplementeerd
- Als u SDAVC hebt ingeschakeld op de oude structuur, moet u ervoor zorgen dat de nieuwe structuur is ingeschakeld (voor clusters moet deze alleen op één node zijn ingeschakeld)
- Configuratie-db-herstel wordt alleen ondersteund op dezelfde versie als de oorspronkelijke structuur
- Bevestig de persoon die voor de controllers is gebruikt. Wij ondersteunen op COMPUTE_DATA en DATA persona (details onder elke sectie)
- Voor Enterprise CA moet u het root-certificaat gebruiken dat is uitgegeven door de Enterprise CA en dat wordt gebruikt in de bestaande overlay. CERT wordt ondertekend met de Enterprise CA-server en geïnstalleerd voor alle controllers via UI

Implementatieopties

vManage-implementatie

- Standalone (1 node)
- Cluster (3 of 6 knooppunten)

NH-opties

- Geen DR
- Single Node DR
- Standby DR-cluster (handmatig / getriggerd voor beheer)

Opmerking: raadpleeg deze link voor meer informatie over het type noodherstel

---

Combinaties:

#	vManage Setup	NH-optie
1	Standalone (1 node)	Geen DR
2	Standalone (1 node)	Single Node DR
3	Cluster (3 of 6 knooppunten)	Geen DR
4	Cluster (3 of 6 knooppunten)	Standby DR-cluster

Gemeenschappelijke stappen die van toepassing zijn op alle combinaties

Deze stappen zijn gebruikelijk voor alle implementatiecombinaties. Ze hebben betrekking op het proces om VM-instanties naar voren te brengen en de basis-CLI-configuratie toe te passen. In elk combinatiegedeelte wordt aangegeven hoeveel instanties moeten worden geïmplementeerd en welke extra stappen moeten worden uitgevoerd.

SD-WAN-controllers installeren en installeren (beheer, validator, controller)

Opmerking: Cisco heeft bepaalde termen omgedoopt, dus deze termen zijn uitwisselbaar. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst Controller

---

Download hier de OVA-bestanden voor SD-WAN-controllers van de downloadpagina voor Cisco-software:

- Kies vEDGE Cloud en download de vBond OVA voor de vereiste softwareversie.
- Kies vManage-software en download de vManage OVA voor de vereiste softwareversie.
- Kies vSmart-software en download de vSmart OVA voor de vereiste softwareversie.

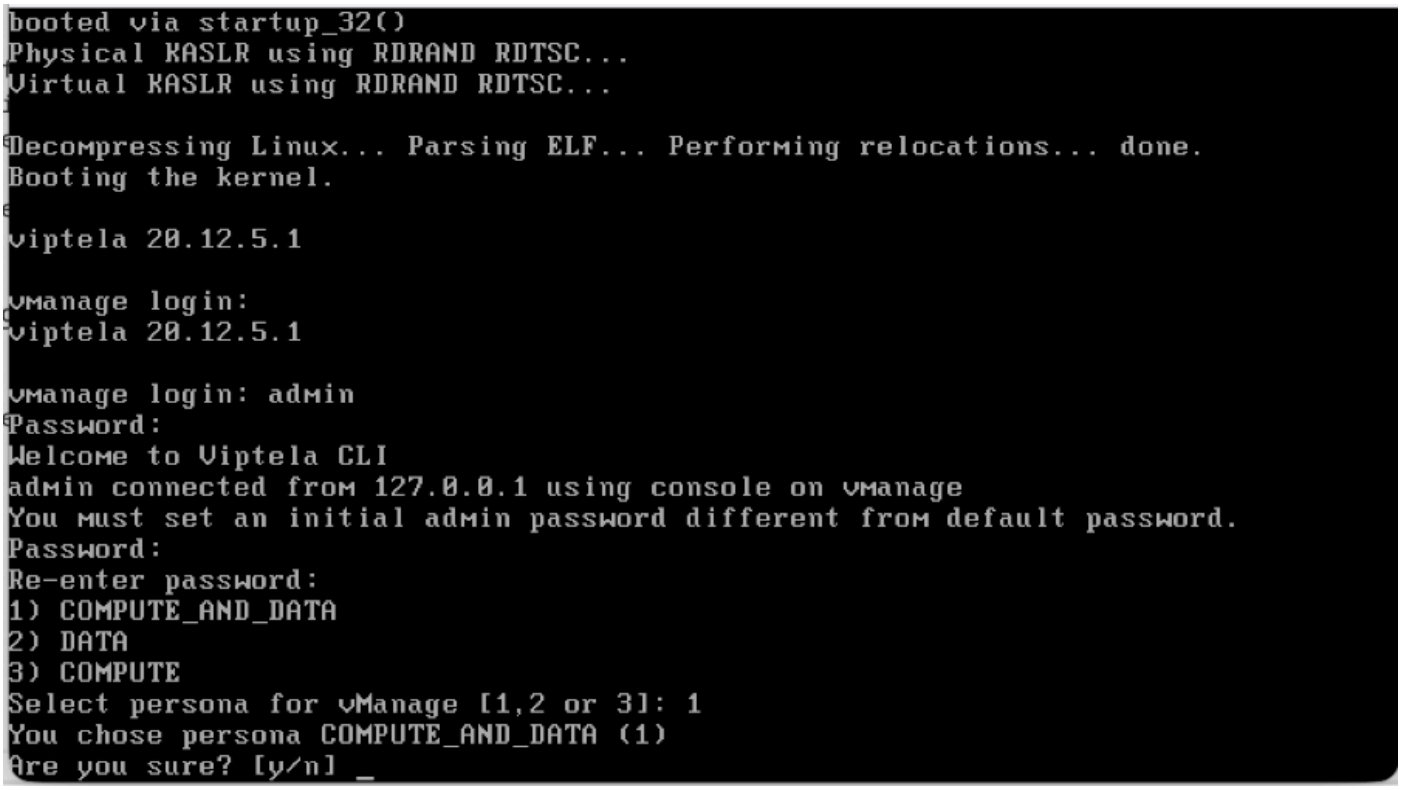
Opmerking: Op de ESXi / cloud-platforms, spin-up vSmart, vBond en vManage Controllers met behulp van de OVA-bestand. Raadpleeg het gekoppelde document en zorg ervoor dat voldoende CPU, RAM en schijven zijn toegewezen aan alle controllers, afhankelijk van het SD-WAN-implementatietype. Navigeer hier voor meer informatie. Zorg ervoor dat u de secundaire schijf toewijst aan de vManage-node, zoals vermeld in de kolom Opslaggrootte* in de gekoppelde computerhandleiding.

Een Cisco Manager-node openen

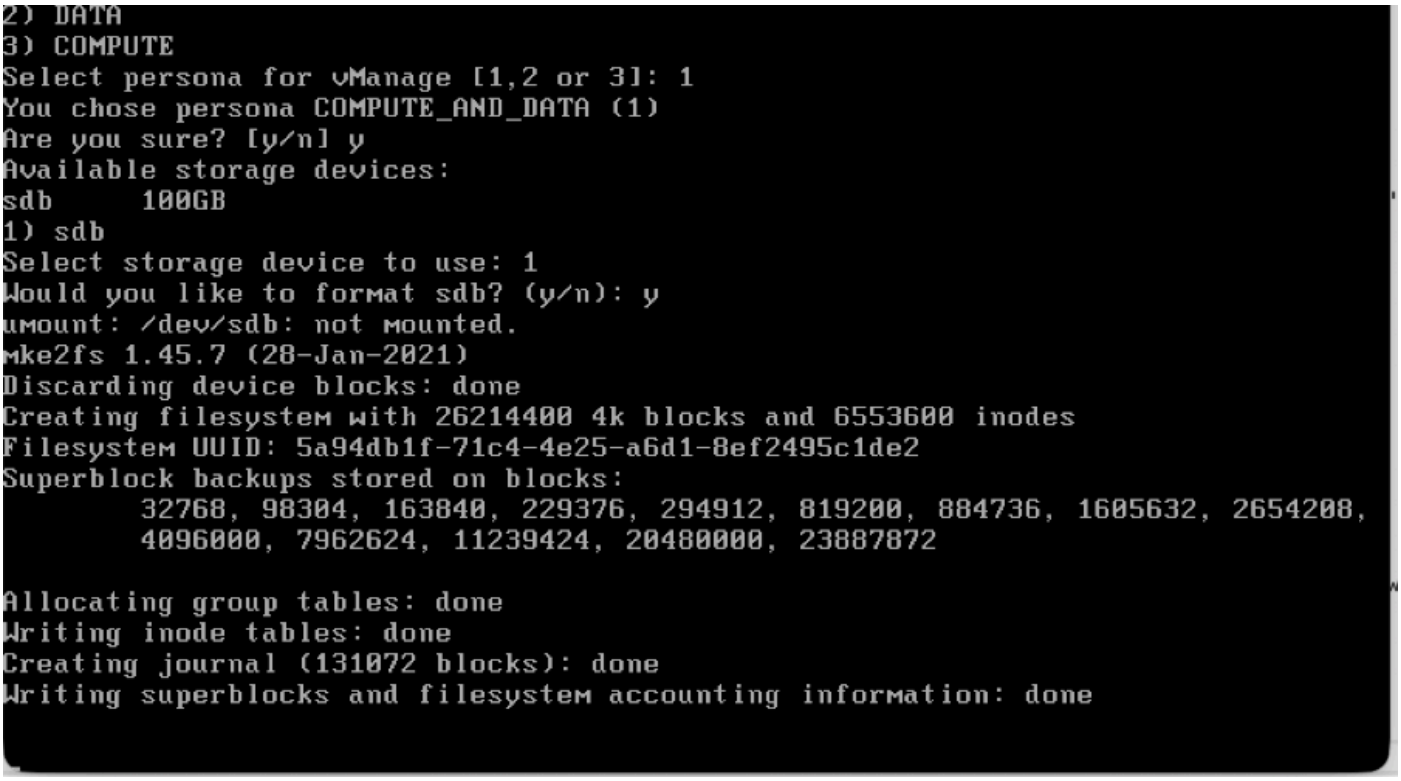
- Nadat Cisco Manager of vManage VM is geïmplementeerd en de console van de manager is geopend, wacht u tot het opstarten is voltooid. Een indicatie is dat we zien dat een berichtensysteem klaar is en vraagt om de gebruikersnaam en het wachtwoord.
- Voer de standaardgebruikersreferenties in als gebruikersnaam als beheerder en wachtwoord als beheerder. Post dat het de gebruiker vraagt om het wachtwoord te wijzigen, stel het wachtwoord in dat nodig is voor gebruikersbeheer volgens uw keuze.
- Vervolgens wordt de gebruiker gevraagd om de persona te selecteren. Dit is een cruciale stap als het de bedoeling is om een vManage-cluster te hebben. Kies de persona volgens de hier getoonde scenario's:

```
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
```

Voorbeeld: Kies 1 voor COMPUTE_AND_DATA



Kies de secundaire schijf zoals weergegeven:



- Kies de secundaire schijf en typ Y om te bevestigen.
- Cisco Manager wordt opnieuw geladen. Zodra het is opgestart, voert u de gebruikersnaam en het wachtwoord in met het nieuwe wachtwoord dat onlangs is geconfigureerd.

```
early console in extract_kernel
input_data: 0x00000000021753b4
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#
```

- U kunt de VPN 512-beheerinterface configureren om out-of-band beheertoegang tot de controller mogelijk te maken.
- Gebruik het tabblad Command Show Interface | om te controleren aan welke VPN-interfaces momenteel is toegewezen.
- Configureer de interfaces dienovereenkomstig.

Voorbeeld

```
                              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#
```

Opmerking: u kunt de configuratie van het bestaande vManage-systeem raadplegen en hetzelfde IP-adresschema hier configureren.

Configuraties van de beheerinterface (VPN 512)

- Als een interface moet worden verplaatst van VPN 0 naar VPN 512, gebruikt u deze opdrachten en configureert u het IP-adres op de interface

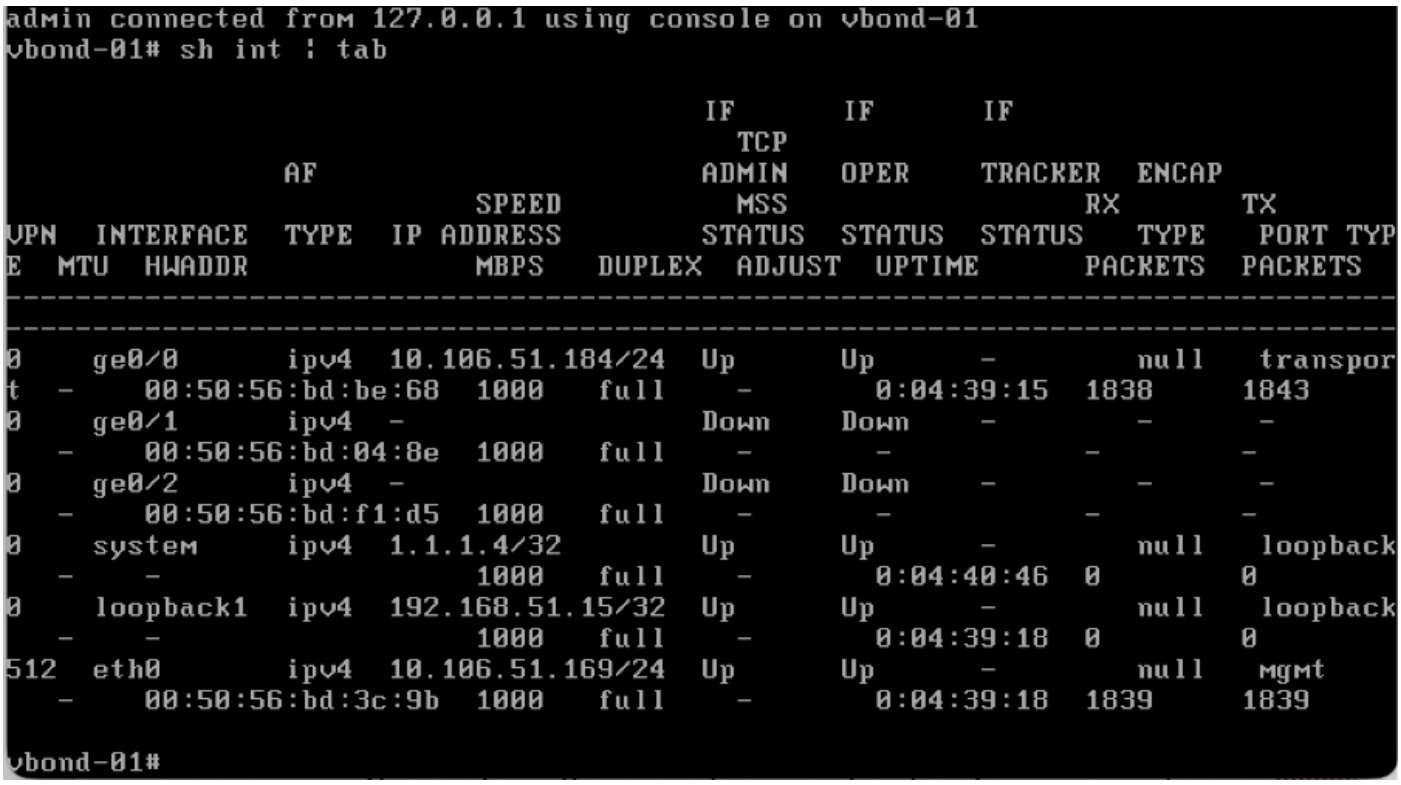
```
Conf t
vpn 0
 no interface eth0
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
```

Breng de validator naar voren

- Configureer op de hypervisor de vereiste computer (CPU, RAM en schijf) voor de vBond-node en schakel deze in.
- Zodra de console toegankelijk is, wacht u tot de vBond volledig is opgestart. Wacht op het bericht System Ready (Systeemklaar).
- Het systeem vraagt vervolgens om gebruikersnaam en wachtwoord. Voer de standaardgebruikersreferenties in als gebruikersnaam als beheerder en wachtwoord als beheerder. Daarna wordt de gebruiker gevraagd om het wachtwoord te wijzigen, stelt u het wachtwoord in dat nodig is voor gebruikersbeheer volgens uw keuze.
- U kunt de VPN 512-beheerinterface configureren om out-of-band beheertoegang tot de controller mogelijk te maken.
- Gebruik het tabblad Command Show Interface | om te controleren aan welke VPN-interfaces momenteel is toegewezen.

- Configureer de interfaces dienovereenkomstig.

Voorbeeld:



```
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#
```

Opmerking: u kunt de configuratie van de bestaande vBond raadplegen en hier dezelfde configuraties configureren.

Configuraties van de beheerinterface (VPN 512)

- Als een interface moet worden verplaatst van VPN 0 naar VPN 512, gebruikt u deze opdrachten en configureert u het IP-adres op de interface.

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




  no shutdown
 !
 ip route 0.0.0.0/0
```

```
!
commit
```

Een knooppunt voor de controller (vSmart)

- Voer dezelfde stappen uit als de validator om de vSmart-node te openen.
- Zodra het VPN 512 IP-adres is geconfigureerd op alle SD-WAN-controllers, kunt u deze openen met SSH op het VPN 512 IP-adres.

Basic CLI-configuratie op alle controllers

Zodra u SSH-toegang hebt tot alle controllers, configureert u deze CLI-configuraties op elke controller.

Systeemconfiguratie

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Opmerking: Als we URL als vBond-adres gebruiken, moet u de IP-adressen van de DNS-server configureren in VPN 0-configuratie of ervoor zorgen dat deze kunnen worden opgelost.

Configuratie van de transportinterface (VPN 0)

Deze configuraties zijn nodig op alle controllers om de transportinterface die wordt gebruikt om besturingsverbindingen met de routers en de rest van de controllers tot stand te brengen, mogelijk te maken.

```
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
```

Opmerking: u kunt verwijzen naar de configuraties van uw bestaande controller en als de configuratie aanwezig is, kunt u deze configuratie toevoegen aan de nieuwe controllers.

Configureer het controleprotocol alleen als TLS als routers verplicht zijn om beveiligde controleverbindingen met de vManage-knooppunten tot stand te brengen met behulp van TLS. Standaard maken alle controllers en routers een controleverbinding met behulp van DTLS. Dit is een optionele configuratie die alleen vereist is voor vSmart- en vManage-knooppunten, afhankelijk van uw vereisten.

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

Combinatie 1: Standalone vManage + geen DR

Benodigde gevallen:

- 1 vManage (COMPUTE_AND_DATA)
- 1 of meer vBond
- 1 of meer vSmart

Stappen:

1. Alle instanties weergeven met de gemeenschappelijke stappen
2. Controles vooraf
3. Configureren van vManage UI, certificaten en onboard controllers
4. Config-db back-up/terugzetbewerking
5. Controles achteraf

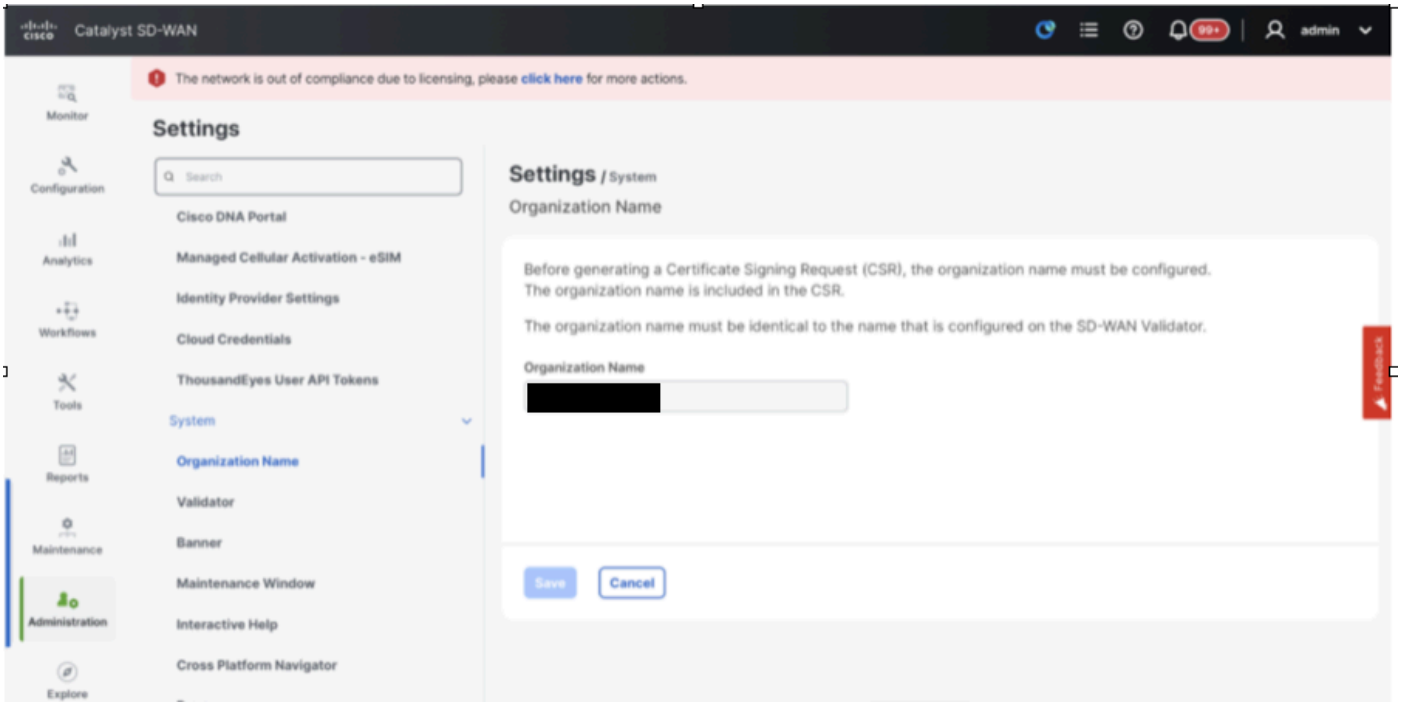
Stap 1: Controles vooraf

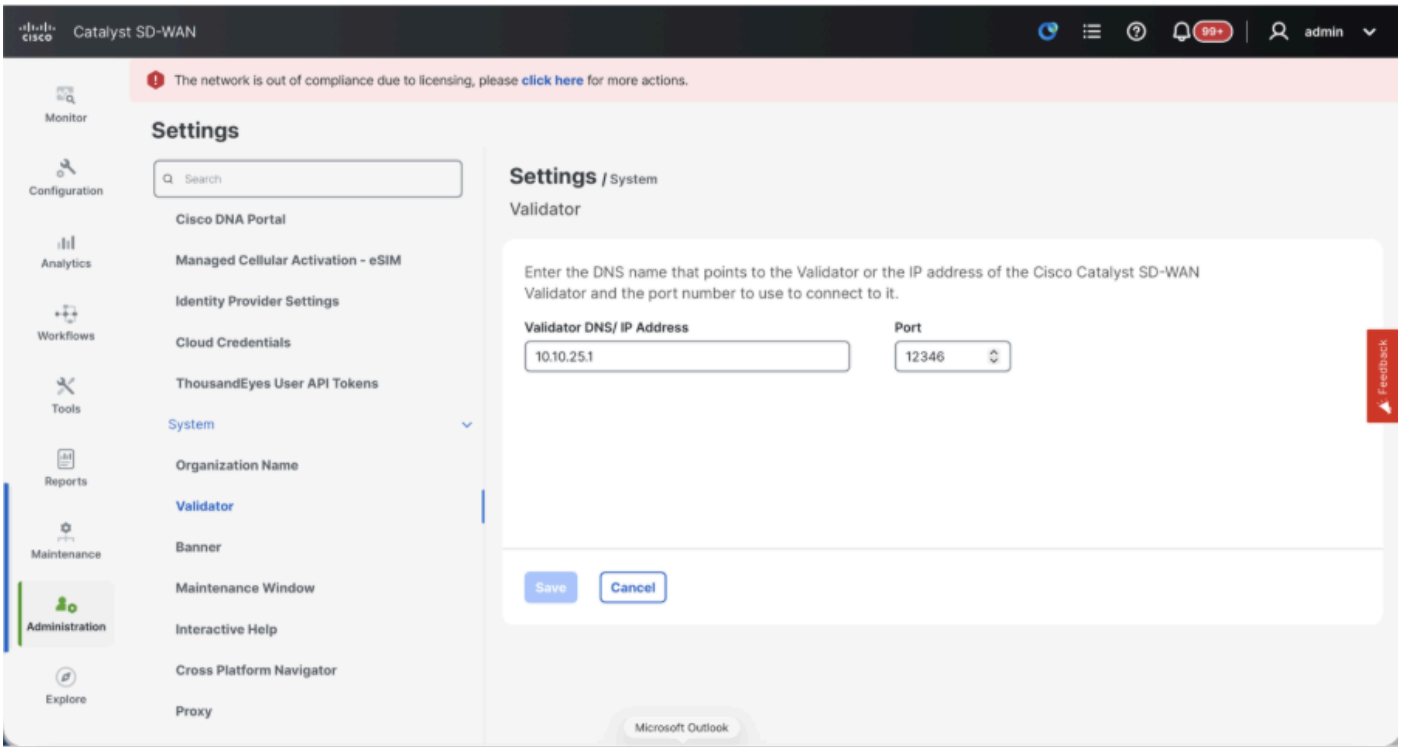
- Zorg ervoor dat het aantal actieve Cisco SD-WAN Manager-instanties identiek is aan het aantal nieuw geïnstalleerde Cisco SD-WAN Manager-instanties.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties dezelfde softwareversie uitvoeren.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties het IP-beheeradres van de Cisco SD-WAN Validator kunnen bereiken.
- Controleer of certificaten zijn geïnstalleerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties.
- Zorg ervoor dat de klokken op alle Cisco Catalyst SD-WAN-apparaten, inclusief de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, worden gesynchroniseerd.
- Zorg ervoor dat een nieuwe set van systeem-IP's en site-ID's is geconfigureerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, samen met dezelfde basisconfiguratie als het actieve cluster.

Stap 2: vManage UI, certificaten en ingebouwde controllers configureren

De configuraties op de vManage-gebruikersinterface bijwerken

- Zodra de configuraties in stap 1 zijn toegevoegd aan de CLI van alle controllers, hebben we toegang tot de webUI van vManage, met behulp van de URL https://<vmanage-ip> in uw browser. Gebruik het VPN 512 IP-adres van de respectieve vManage-knooppunten. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Beheer > Instellingen en voer deze stappen uit.
- Configureer de naam van de organisatie en het URL/IP-adres van de validator/vBond. Configureer dezelfde waarde als in de CLI van de vManage-node.
- In vManage 20.15/20.18 zijn deze configuraties beschikbaar onder de sectie Systeem.

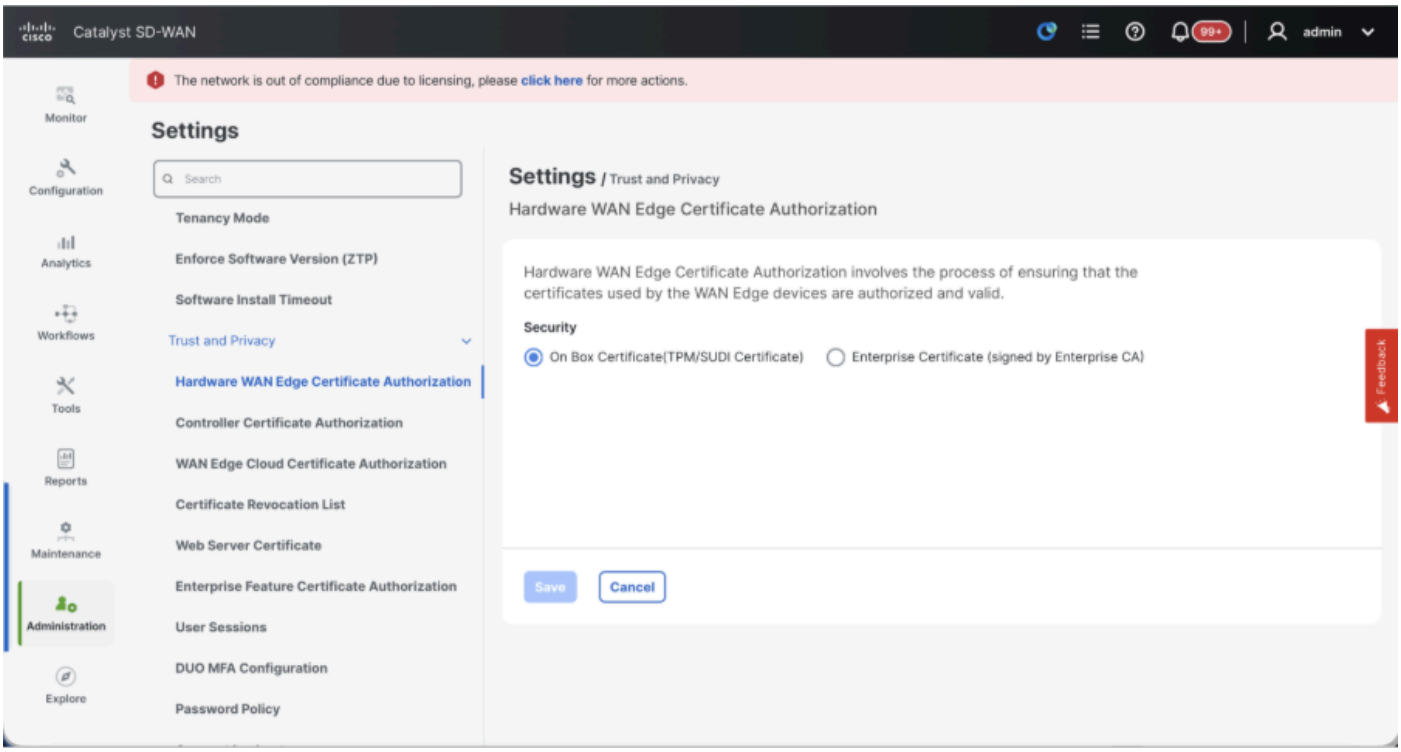




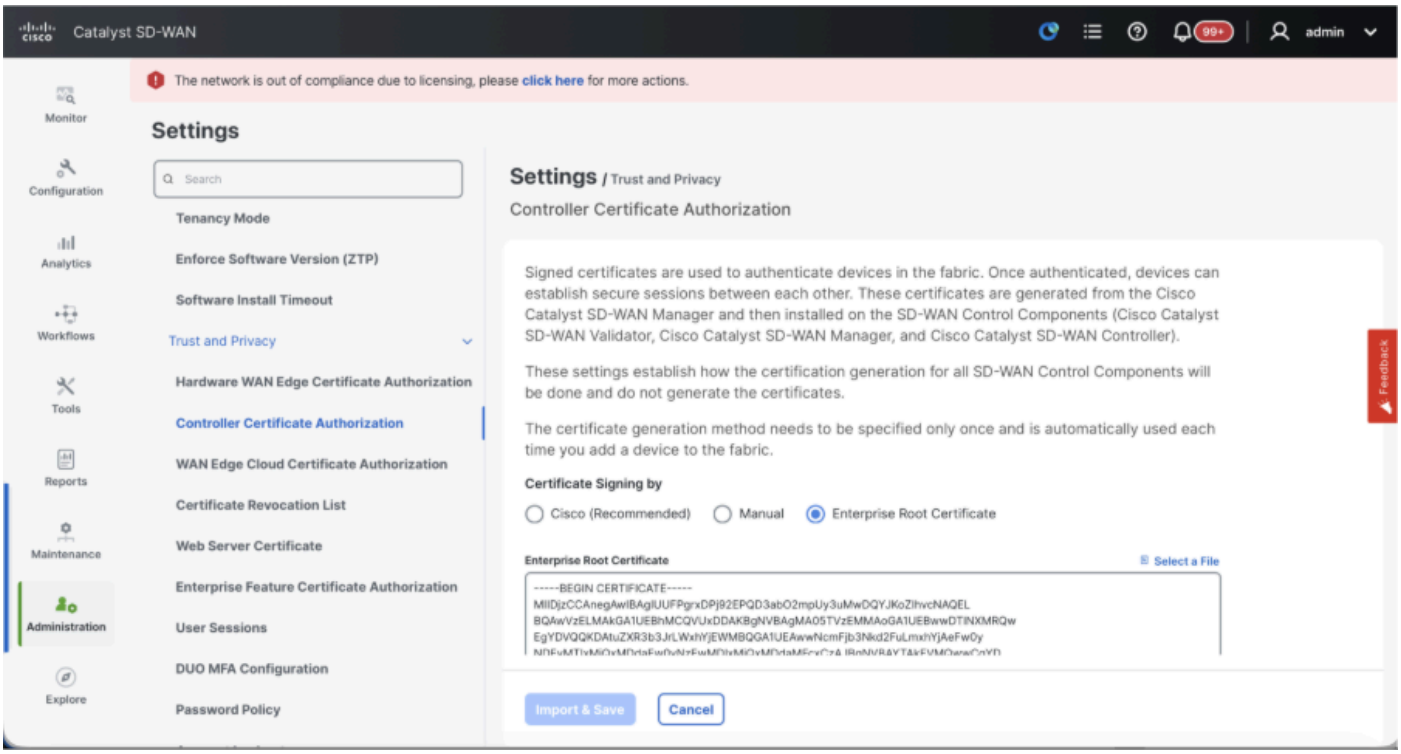
- Controleer de configuraties voor Certificaatautorisatie (CA), die bepaalt welke Certificaatautoriteit wordt gebruikt voor het ondertekenen van de certificaten. We zien daar 3 mogelijkheden:

1. Hardware WAN Edge Certificate Authorization - Bepaalt de CA voor hardware SD-WAN Edge-routers.
    - On Box Certificate (TPM/SUDI-certificaat) - Met deze optie wordt het vooraf geïnstalleerde certificaat op de hardware van de router gebruikt om de Controleverbindingen (TLS/DTLS-verbindingen) tot stand te brengen
    - Enterprise Certificate (ondertekend door Enterprise CA) - Met deze optie gebruiken de routers certificaten die zijn ondertekend door Enterprise-certificeringsinstantie van uw

organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

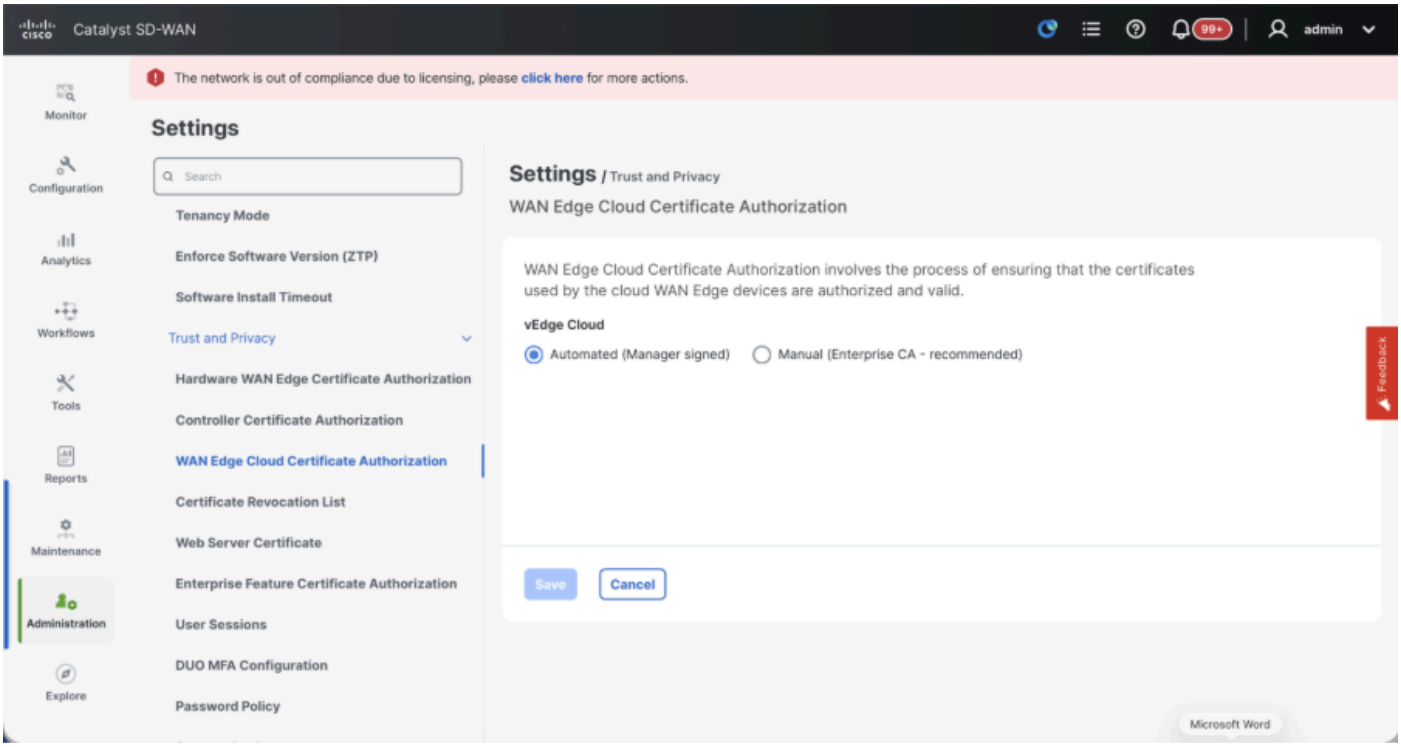


2. Controllercertificaatautorisatie - bepaalt de CA voor SD-WAN-controllers.
    - Cisco (aanbevolen) - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. vManage neemt automatisch contact op met het PNP-portaal met behulp van de referenties voor slimme accounts die zijn geconfigureerd op de vManage en laat het certificaat ondertekenen en installeren op de controller.
    - Handleiding - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. Handmatig ondertekenen van de CSR met behulp van de Cisco PNP portal door te navigeren naar smart account en virtuele account van de respectieve SD-WAN overlay.
    - Enterprise Root Certificate - Met deze optie gebruiken de routers certificaten die zijn ondertekend door de Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

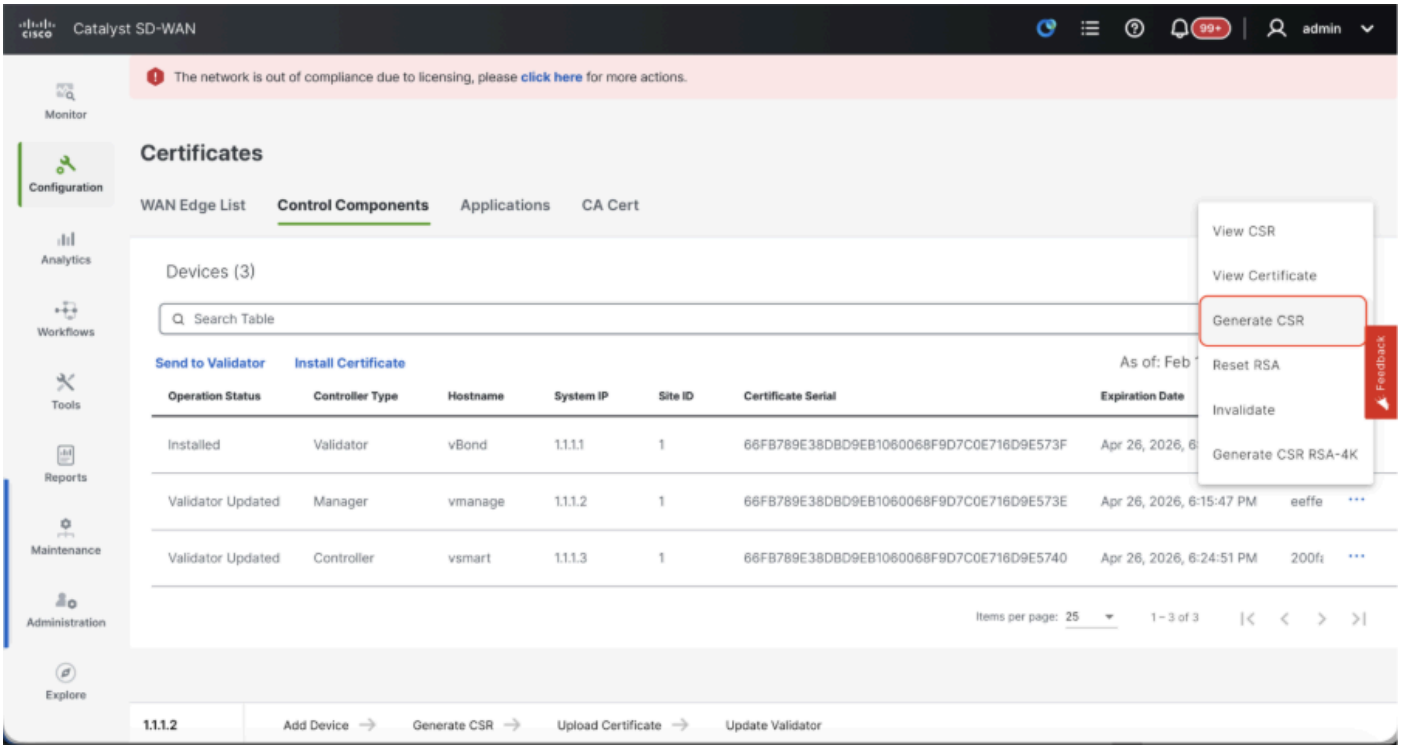


3. WAN Edge Cloud Certificate Authorization - Bepaalt de CA voor virtuele SD-WAN Edge-routers (CSR1000v, C8000v, vEdge cloud)
    - Geautomatiseerd (vManage ondertekend) - vManage ondertekent automatisch de CSR voor de virtuele Edge-routers en installeert het certificaat op de router.
    - Handmatig (Enterprise CA - aanbevolen) - Virtuele routers gebruiken certificaten die zijn ondertekend door de certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

Als we onze eigen CA, Enterprise-certificeringsinstantie, gebruiken, kiest u in dat geval Enterprise.



- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers
- Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

Onboarding vBond/Validator en vSmart/Controller naar de vManage

Navigeer naar Configuratie > Apparaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

OnboardingVbond/validator

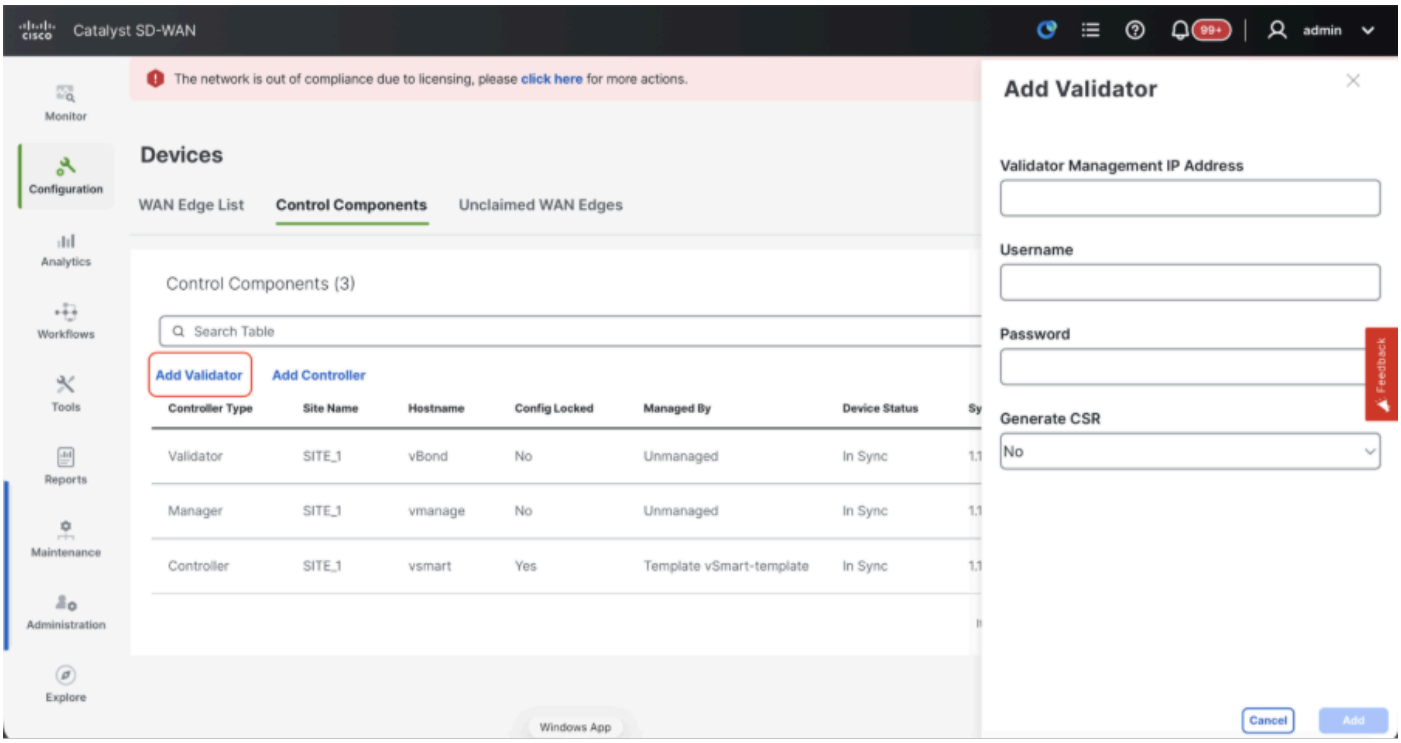
- Klik op AdvBondin geval van 12 .12vManagerValidator toevoegenin geval van 20.15/20.18vManage. Er wordt een pop-upvenster geopend. Voer de VPN 0 transporteert IP

van vBond die bereikbaar is vanaf de vManage.

- Controleer de bereikbaarheid met behulp van ping indien toegestaan vanuit de CLI van vManagetovBondIP.
- Voer de gebruikersreferenties van vBond in.

Opmerking: We moeten beheerdersreferenties gebruiken van vBond of een gebruikersonderdeel van netadminggroup. U kunt dit controleren in de CLI van de vBond. Kies Ja in de drop-down van "Genereer CSR" als we een nieuw certificaat voor vBond moeten installeren.

Opmerking: Als de vBond zich achter een NAT-apparaat/firewall bevindt, controleert u of de vBond VPN 0-interface IP is vertaald naar een openbaar IP-adres. Als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u in deze stap het openbare IP-adres van de VPN 0-interface.



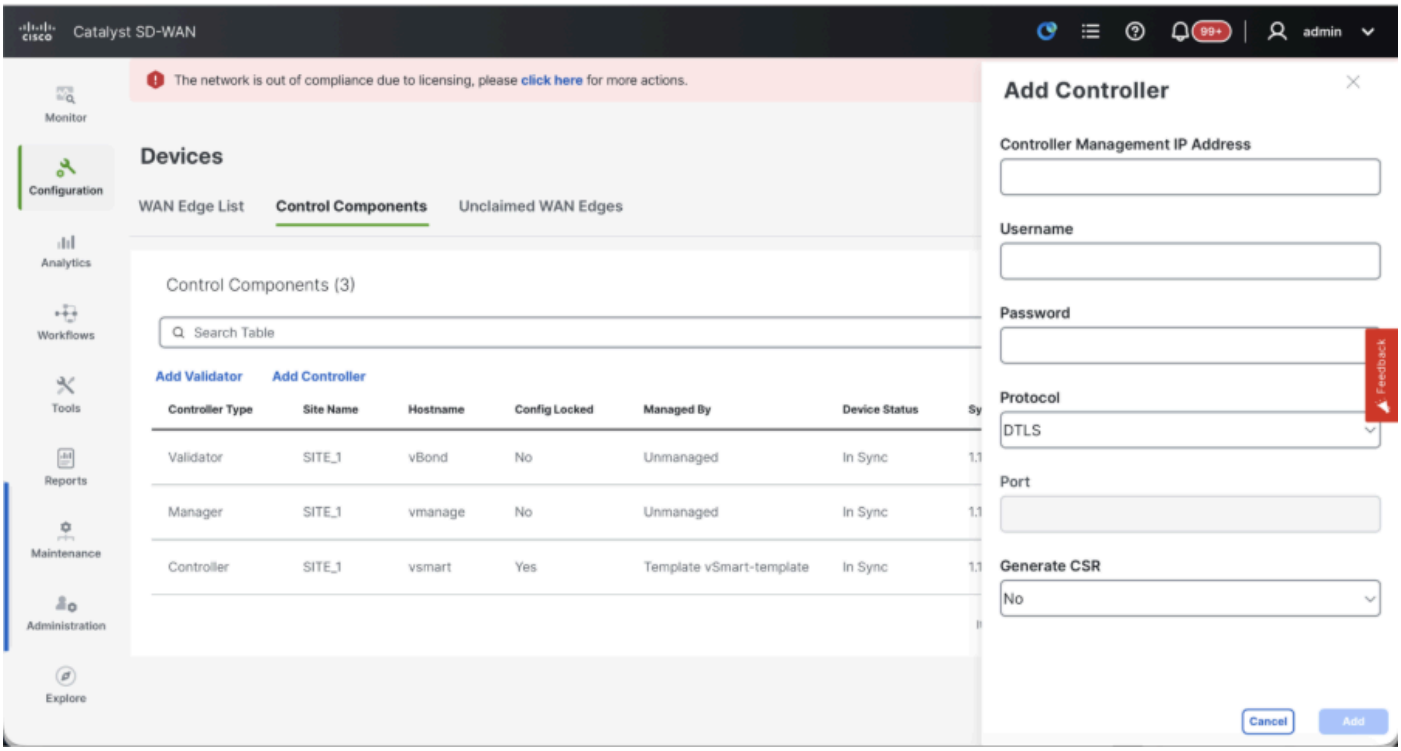
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door de vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vBond geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u

op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vBonds zijn, herhaalt u dezelfde stappen.

Onboarding vSmart/controller

- Klik op Add vSmart in geval van 10 .12 vManage of Add Controller in geval van 20.15/20.18 vManage.
- Als er een pop-upvenster wordt geopend, voert u het VPN 0-transport IP van vSmart in dat bereikbaar is via vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan van CLI van vManage naar vSmart IP.
- Voer de gebruikersreferenties van vSmart Note in die we nodig hebben om beheerdersreferenties van vSmart of een gebruikersdeel van de netadmin-groep te gebruiken.
- U kunt dit controleren in de CLI van de vSmart.
- Stel het protocol in op TLS als we TLS willen gebruiken voor routers om controleverbindingen met vSmart tot stand te brengen. Deze configuratie moet ook worden geconfigureerd op CLI van vSmarts- en vManage-knooppunten.
- Kies Ja in de keuzelijst "MVO genereren" als we een nieuw certificaat voor vSmart moeten installeren.

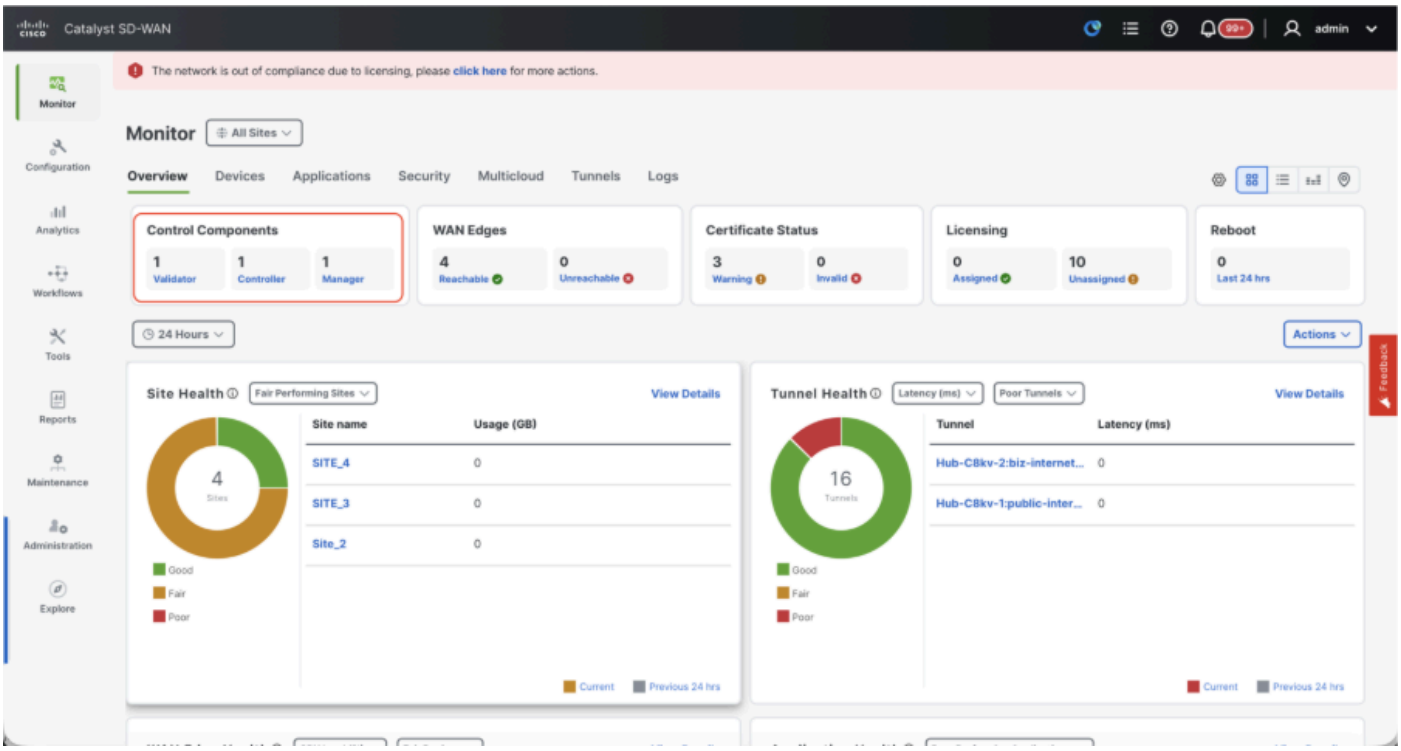
Opmerking: Als de vSmart zich achter NAT-apparaat/firewall bevindt, controleert u of de vSmart VPN 0-interface IP is vertaald naar een openbaar IP-adres en als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u in deze stap het openbare IP-adres van de VPN 0-interface IP.



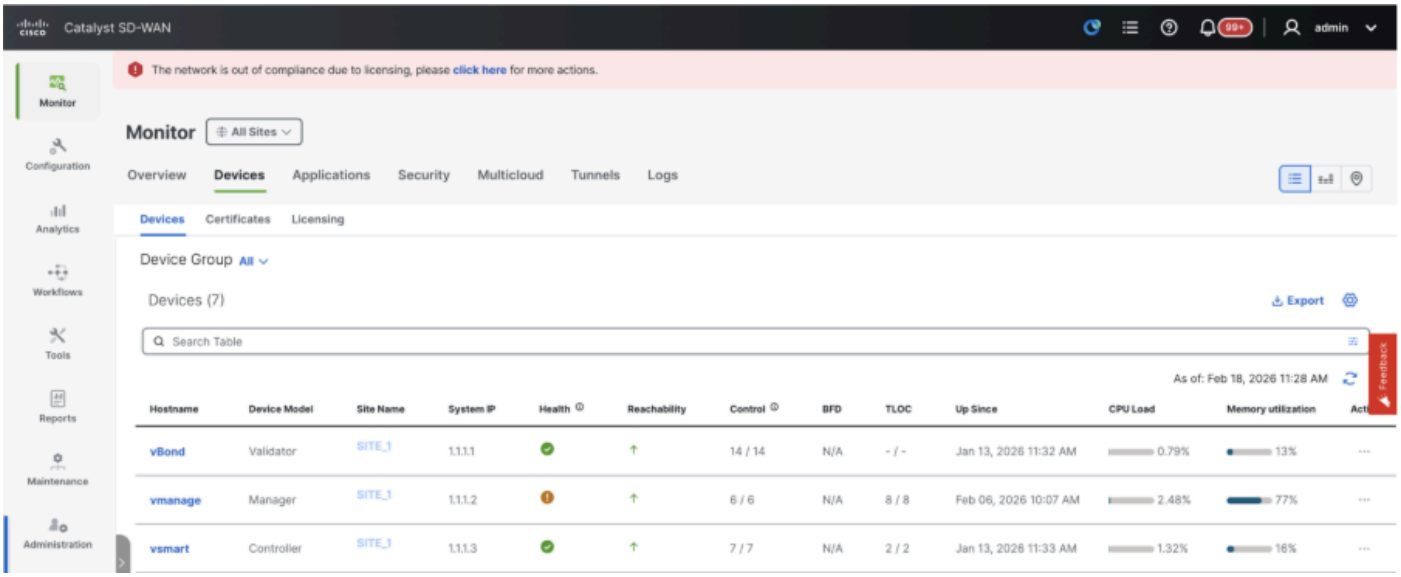
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vSmart geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.
- Als er meerdere vSmarts zijn, herhaalt u dezelfde stappen.

Verificatie

Controleer na voltooiing van alle stappen of alle besturingscomponenten bereikbaar zijn in Monitor>Dashboard



- Klik op de betreffende besturingscomponenten en bevestig dat ze allemaal bereikbaar zijn.
- Navigeer naar Monitor > Apparaten en controleer of alle besturingscomponenten bereikbaar zijn.



Stap 3: Config-DB Backup/Restore

Configuratie-db-back-up en terugzetbewerkingen op een andere vManage-node verzamelen

Configuratie-DB-back-up verzamelen:

- In de SD-WAN-fabric die momenteel in gebruik is, kunt u configuratie-db-back-ups genereren op zowel standalone vManage- als vManage-clusterinstellingen.
- Voor standalone vManage is dat vManage zelf de leider op het gebied van configuratie-db.

Bevestig dat de configuratie-db wordt uitgevoerd op de vManage-node.

U kunt hetzelfde controleren met behulp van de opdracht request nms configuration-db status onvManageCLI. De output is zoals getoond

```
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#
```

Gebruik deze opdracht om de configuratie-db-back-up te verzamelen van de geïdentificeerde configuratie-db leader vManage-node.

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

De verwachte output is als volgt:

```
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#
```

- Noteer de configuratie-db-referenties als deze is bijgewerkt.
- Als u de configuratie-db-referenties niet kent, neemt u contact op met TAC om de configuratie-db-referenties op te halen uit de bestaande vManage-knooppunten.
- Standaardconfiguratie-db-referenties zijn gebruikersnaam: neo4j en wachtwoord: wachtwoord

Configuration-db Backup terugzetten naar een andere vManage-node

Kopieer de configuratie-db back-up naar /home/admin/ directory van vManage met behulp van SCP.

Voorbeeld van scp-opdrachtuitvoer:

```
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
```

Om de configuratie-db back-up te herstellen, moeten we eerst de configuratie-db referenties configureren. Als uw configuratie-db-referenties standaard zijn (neo4j / wachtwoord), kunnen we deze stap overslaan.

Als u configuratie-db-referenties wilt configureren, gebruikt u de opdracht request nms configuration-db update-admin-user. Gebruik de gebruikersnaam en het wachtwoord van uw keuze.

Houd er rekening mee dat de toepassingsserver van vManage opnieuw wordt gestart. Hierdoor wordt de gebruikersinterface van vManage korte tijd ontoegankelijk.

```
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#
```

Post waarin we kunnen doorgaan met het herstellen van de configuratie-db back-up:

We kunnen de opdracht request nms configuration-db restore path /home/admin/< > gebruiken om de configuratie-db te herstellen naar de nieuwe vManage:

```
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
```

Zodra de configuratie-db is hersteld, moet u ervoor zorgen dat de vManage UI toegankelijk is. Wacht ongeveer 5 minuten en probeer vervolgens toegang te krijgen tot de gebruikersinterface.

Als u eenmaal met succes bent ingelogd op de gebruikersinterface, moet u ervoor zorgen dat de lijst met Edge-routers, het sjabloon, het beleid en alle andere configuraties die aanwezig waren op uw vorige of bestaande vManage-gebruikersinterface, worden weergegeven in de nieuwe vManage-gebruikersinterface.

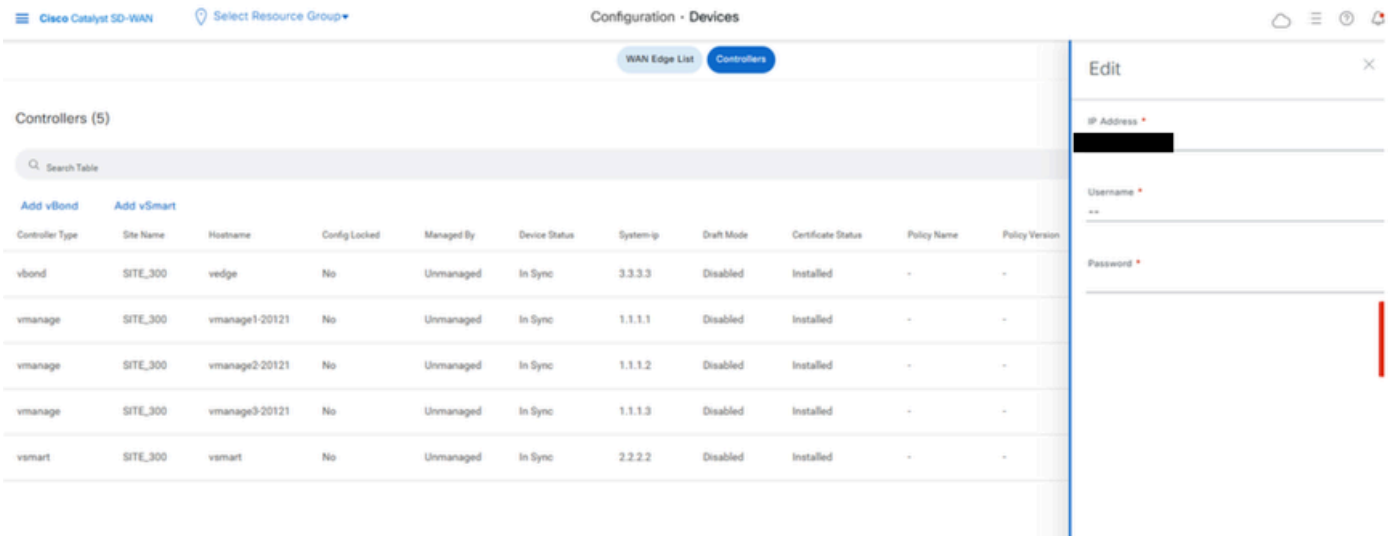
Stap 4: Reauthenticatie van controllers en ongeldigverklaring van oude controllers

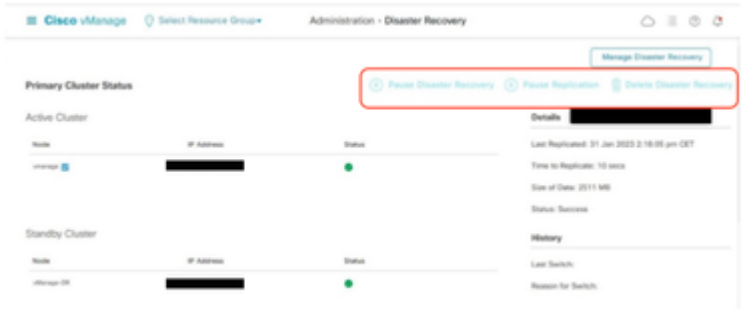
Zodra configuratie-db is hersteld, moeten we alle nieuwe controllers (vmanage/vsmart/vbond) in de fabric opnieuw verifiëren.

Opmerking: Als de IP-interface die wordt gebruikt om opnieuw te verifiëren de tunnelinterface IP is, moet u ervoor zorgen dat de NETCONF-service is toegestaan op de tunnelinterface van de vManage, vSmart en vBond en ook op de firewalls langs het pad. De firewallpoort die moet worden geopend, is TCP-poort 830 als bidirectionele regel van DR-cluster naar alle vBonds en vSmarts.

Klik in vmanage UI op Configuration > Devices > Controllers

- Klik op de drie puntjes bij elke controller en klik op Bewerken





- Vervang het ip-adres (system-ip van de controller) door het transport vpn 0 (tunnelinterface) ip-adres. Voer de gebruikersnaam en het wachtwoord in en klik op Opslaan
- Doe hetzelfde voor alle nieuwe controllers in de stof

Synchroniseer de Root-cert-keten

Als alle controllers zijn geïnstalleerd, voert u deze stap uit:

Voer op elke Cisco SD-WAN Manager-server in het nieuw actieve cluster de volgende acties uit:

Voer deze opdracht in om het rootcertificaat te synchroniseren met alle Cisco Catalyst SD-WAN-apparaten in het nieuw actieve cluster:

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

Voer deze opdracht in om de Cisco SD-WAN Manager UUID te synchroniseren met de Cisco SD-WAN Validator:

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

Zodra de fabric is hersteld en de controle- en bfd-sessies zijn ingesteld voor alle randen en controllers in de fabric, moeten we de oude controllers (vmanage/vsmart/vbond) van de gebruikersinterface ongeldig maken

- Klik in vmanage UI op Configuration > Certificates > Controllers
- Klik op Controllers

- Klik op de drie puntjes in de rechterkant van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Ongeldig maken
- Klik op verzenden naar vbond
- Klik in vmanage UI op Configuration > Devices > Controllers
- Klik op de drie puntjes in de rechterkant van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Verwijderen

Stap 5: Controles achteraf

Opmerking: ga verder met het gedeelte Controles achteraf dat hier wordt weergegeven en dat voor alle implementatiecombinaties geldt.

Combinatie 2: standalone vManage + DR met één node

Benodigde gevallen:

- 1 vManage (primair, COMPUTE_AND_DATA)
- 1 vManage (DR standby, COMPUTE_AND_DATA)
- 1 of meer vBond
- 1 of meer vSmart

Stappen:

1. Alle instanties weergeven met de gemeenschappelijke stappen
2. Voorcontroles
3. Configureren van vManage UI, certificaten en onboard controllers
4. DR-installatie met één node
5. Config-db back-up/terugzetbewerking
6. Controles achteraf

Stap 1: Controles vooraf

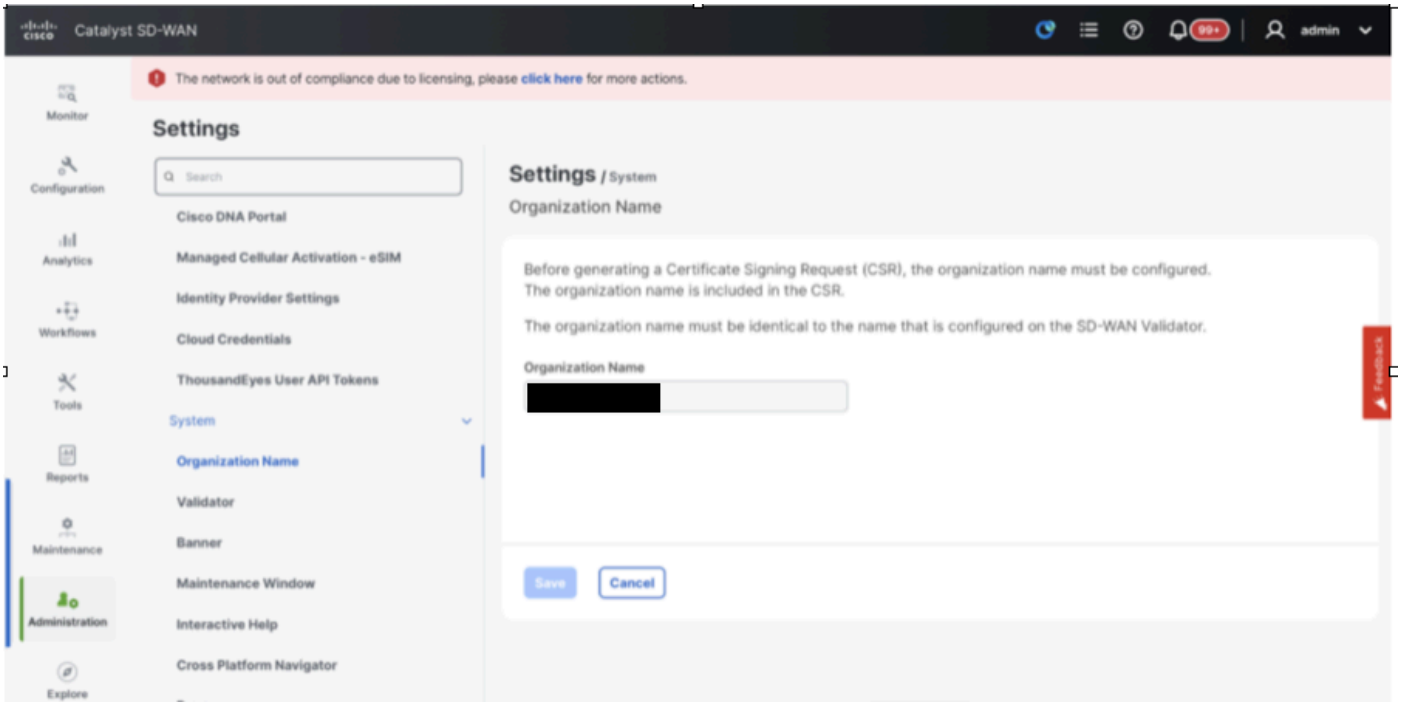
- Zorg ervoor dat het aantal actieve Cisco SD-WAN Managerinstances gelijk is aan het aantal nieuw geïnstalleerde Cisco SD-WAN Managerinstances.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties dezelfde softwareversie uitvoeren.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties het IP-beheeradres van de Cisco SD-WAN Validator kunnen bereiken.
- Controleer of certificaten zijn geïnstalleerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties.

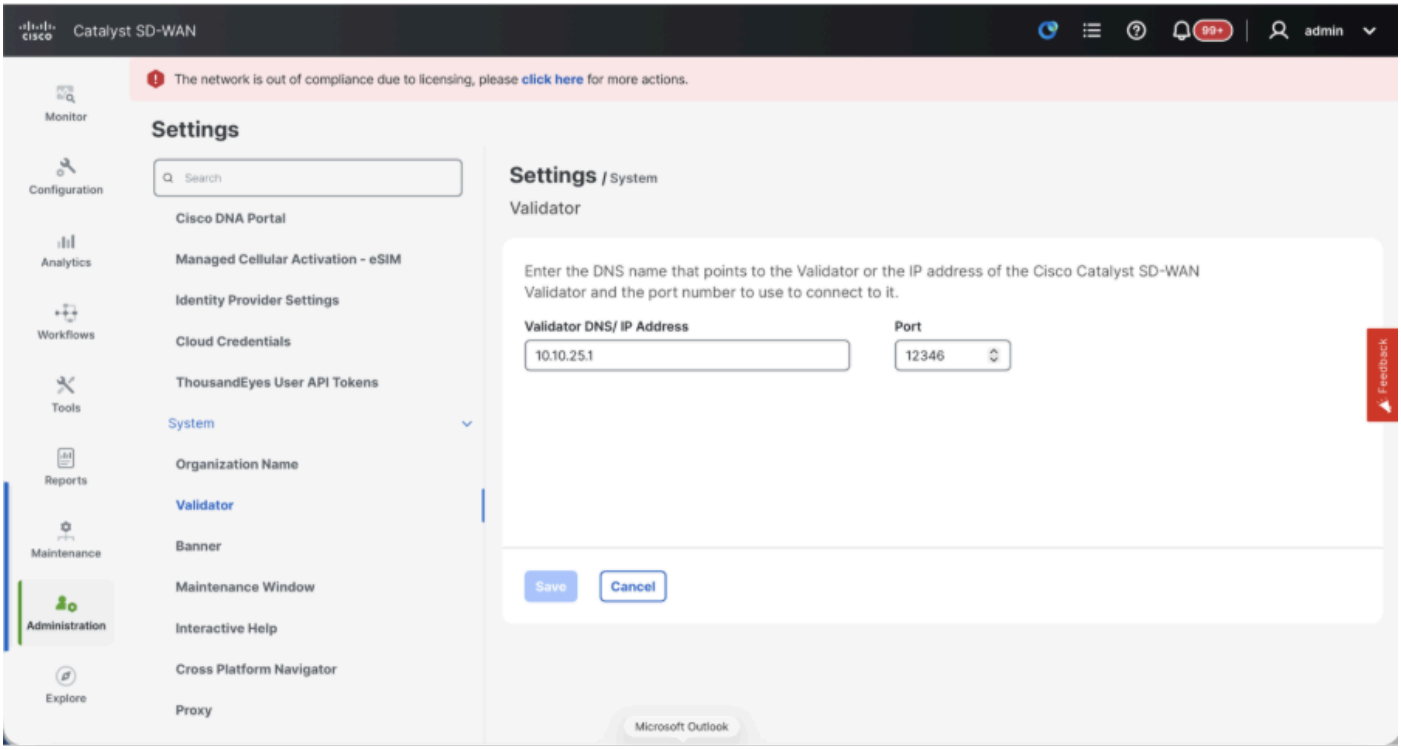
- Zorg ervoor dat de klokken op alle Cisco Catalyst SD-WAN-apparaten, inclusief de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, worden gesynchroniseerd.
- Zorg ervoor dat een nieuwe set van systeem-IP's en site-ID's is geconfigureerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, samen met dezelfde basisconfiguratie als het actieve cluster.

Stap 2: vManage UI, certificaten en ingebouwde controllers configureren

De configuraties op de vManage-gebruikersinterface bijwerken

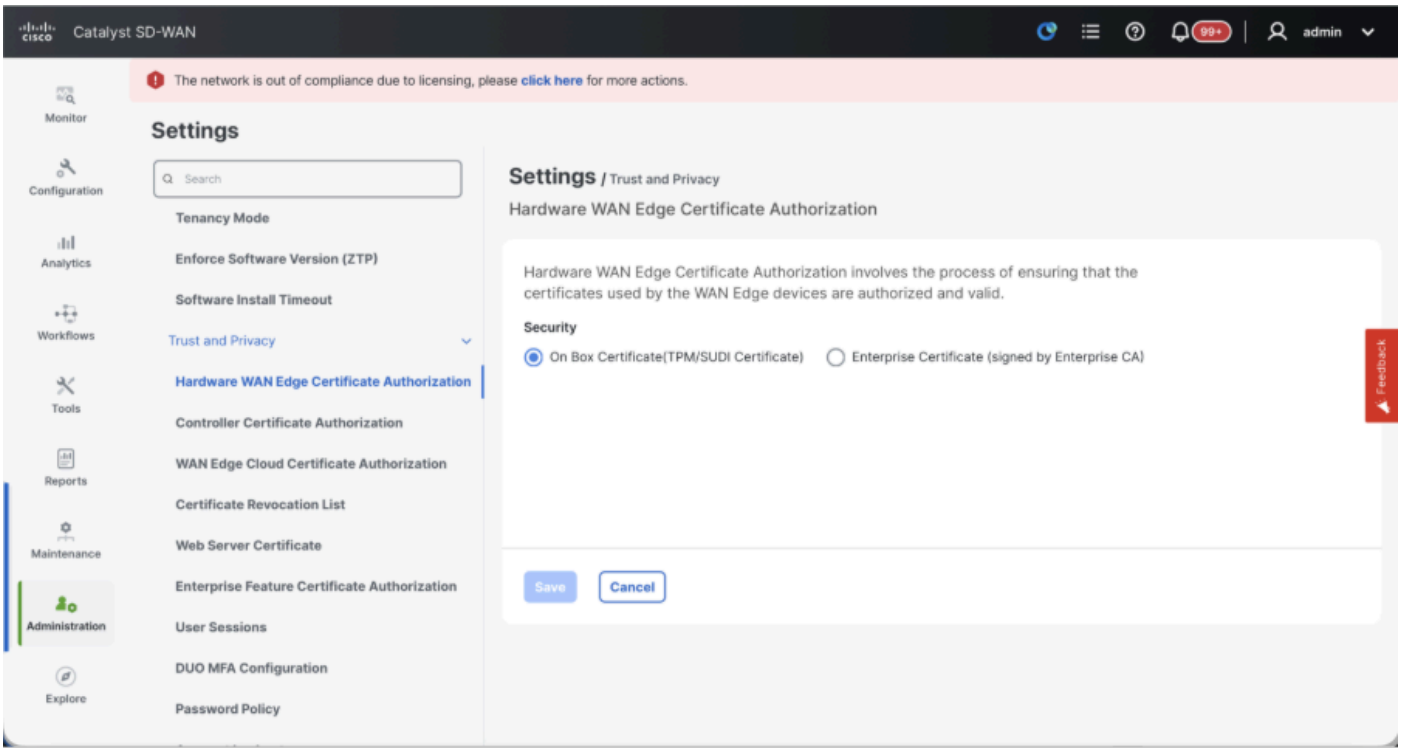
- Zodra de configuraties in stap 1 zijn toegevoegd aan de CLI van alle controllers, hebben we toegang tot de webUI van vManage, met behulp van de URL https://<vmanage-ip> in uw browser. Gebruik het VPN 512 IP-adres van de respectieve vManage-knooppunten. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Beheer > Instellingen en voer deze stappen uit.
- Configureer de naam van de organisatie en het URL/IP-adres van de validator/vBond. Configureer dezelfde waarde als in de CLI van de vManage-node.
- In vManage 20.15/20.18 zijn deze configuraties beschikbaar onder de sectie Systeem.



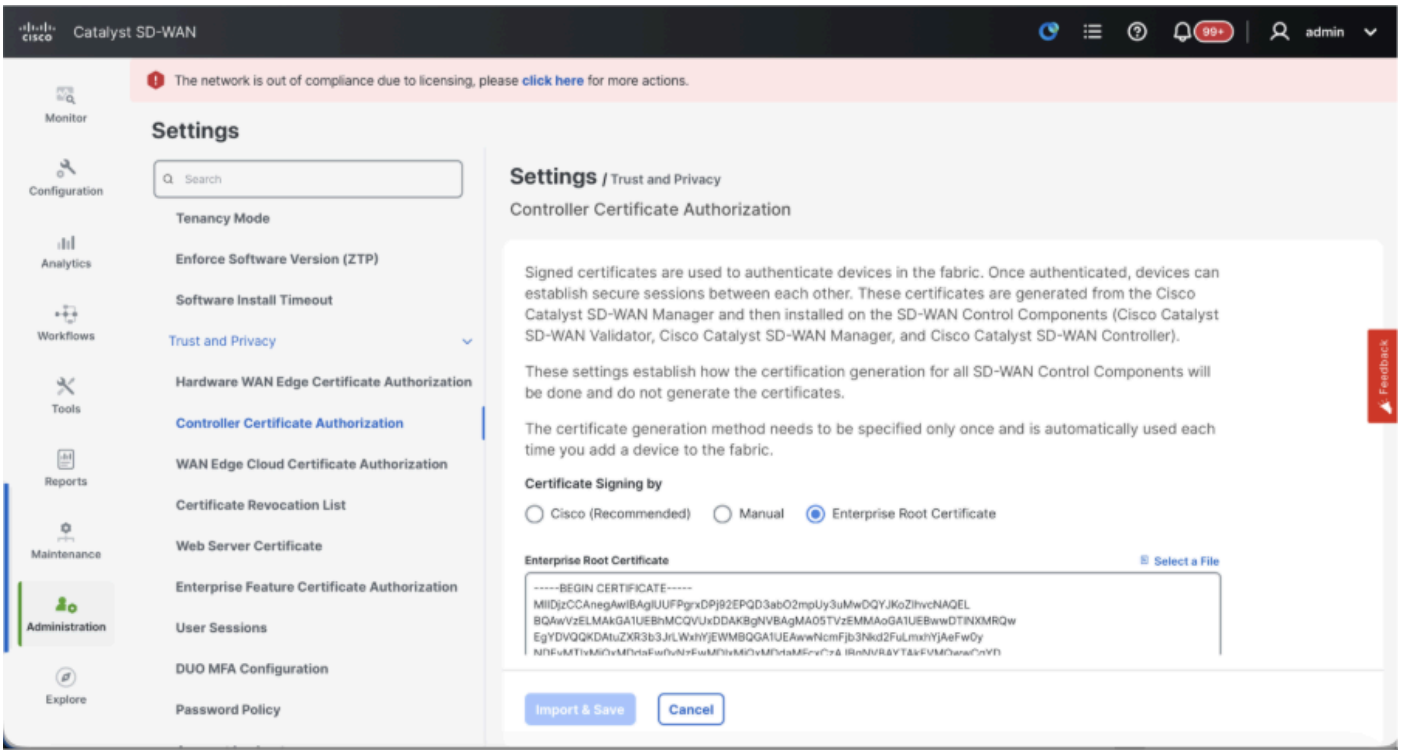


- Controleer de configuraties voor Certificaatautorisatie (CA), die bepaalt welke Certificaatautoriteit wordt gebruikt voor het ondertekenen van de certificaten. We zien daar 3 mogelijkheden:

1. Hardware WAN Edge Certificate Authorization - Bepaalt de CA voor hardware SD-WAN Edge-routers.
    - On Box Certificate (TPM/SUDI-certificaat) - Met deze optie wordt het vooraf geïnstalleerde certificaat op de hardware van de router gebruikt om de Controleverbindingen (TLS/DTLS-verbindingen) tot stand te brengen
    - Enterprise Certificate (ondertekend door Enterprise CA) - Met deze optie gebruiken de routers certificaten die zijn ondertekend door Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

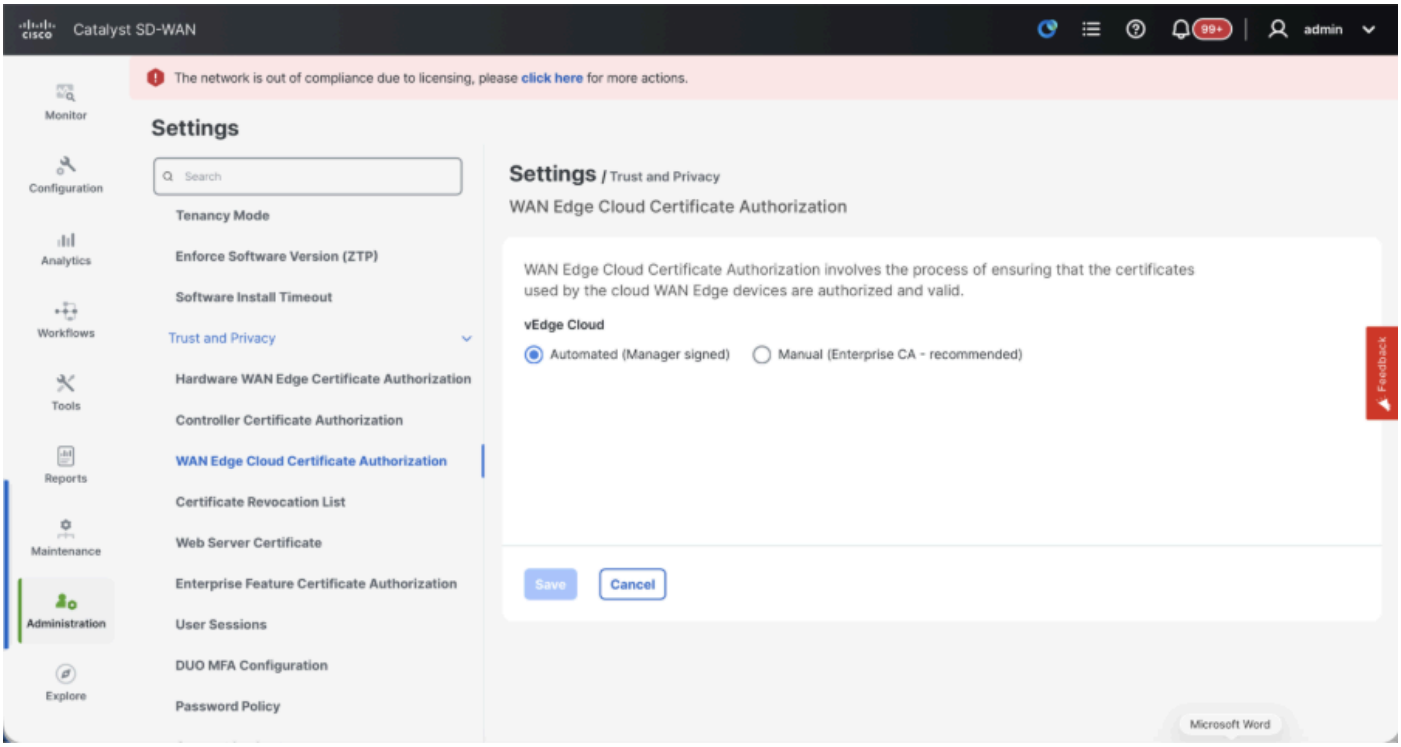


2. Controllercertificaatautorisatie - bepaalt de CA voor SD-WAN-controllers.
    - Cisco (aanbevolen) - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. vManage neemt automatisch contact op met het PNP-portaal met behulp van de referenties voor slimme accounts die zijn geconfigureerd op de vManage en laat het certificaat ondertekenen en installeren op de controller.
    - Handleiding - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. Handmatig ondertekenen van de CSR met behulp van de Cisco PNP portal door te navigeren naar smart account en virtuele account van de respectieve SD-WAN overlay.
    - Enterprise Root Certificate - Met deze optie gebruiken de routers certificaten die zijn ondertekend door de Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

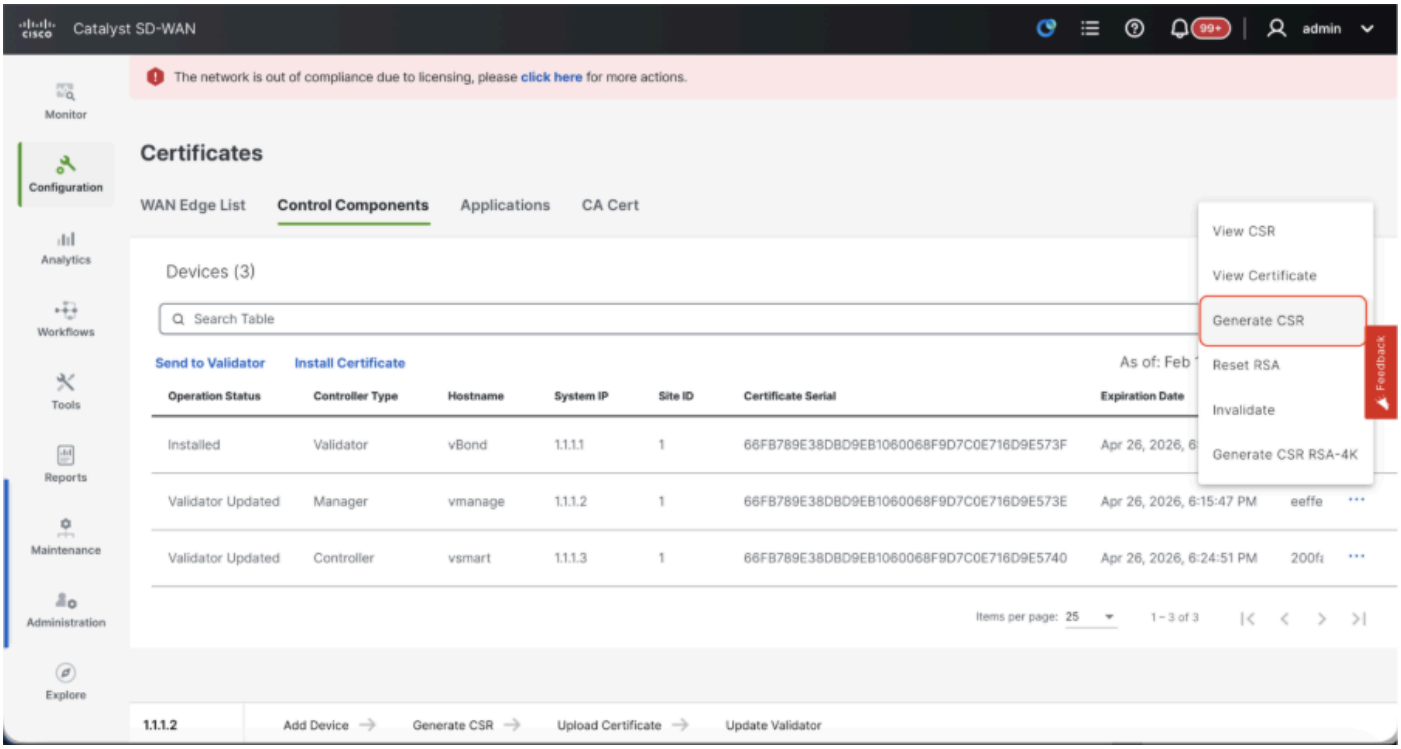


3. WAN Edge Cloud Certificate Authorization - Bepaalt de CA voor virtuele SD-WAN Edge-routers (CSR1000v, C8000v, vEdge cloud)
    - Geautomatiseerd (vManage ondertekend) - vManage ondertekent automatisch de CSR voor de virtuele Edge-routers en installeert het certificaat op de router.
    - Handmatig (Enterprise CA - aanbevolen) - Virtuele routers gebruiken certificaten die zijn ondertekend door de certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

Als we onze eigen CA, Enterprise-certificeringsinstantie, gebruiken, kiest u in dat geval Enterprise.



- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers
- Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

Onboarding vBond/Validator en vSmart/Controller naar de vManage

Navigeer naar Configuratie > Apparaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

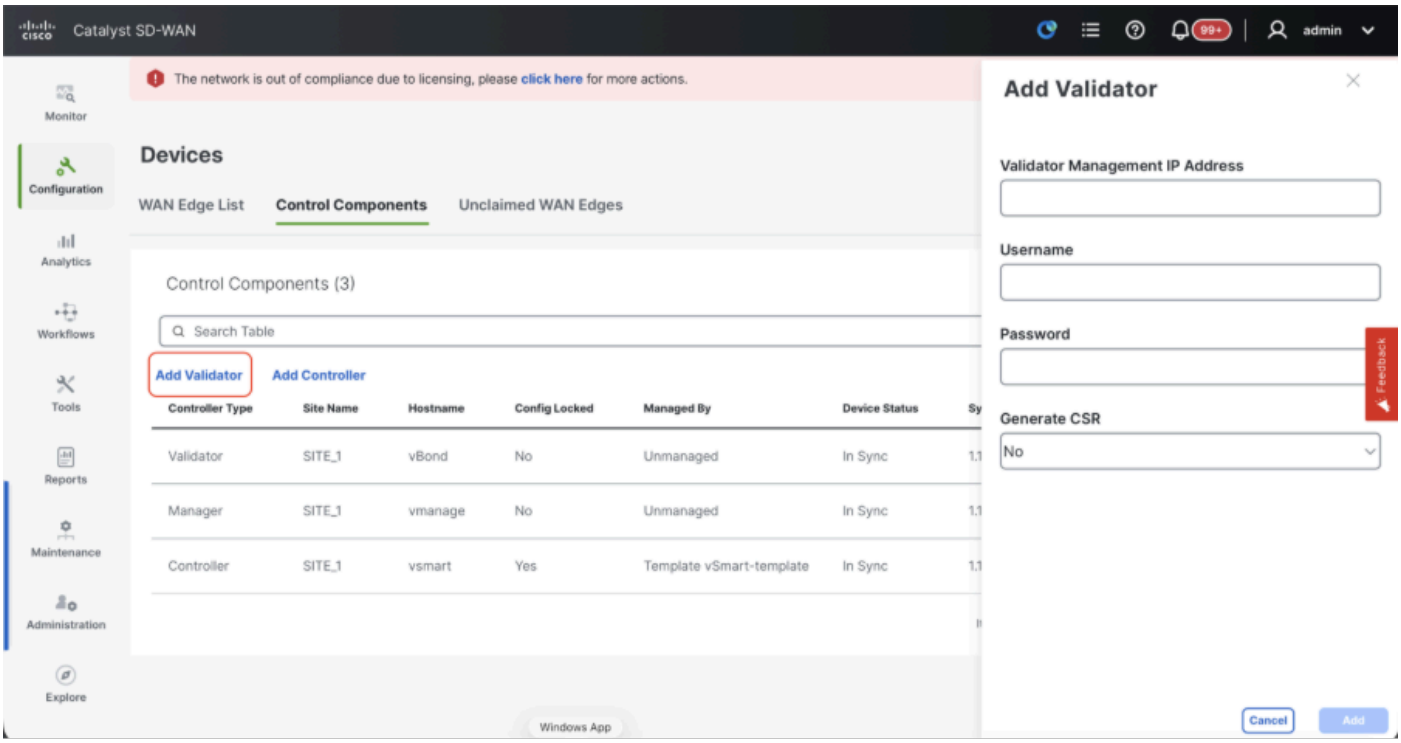
OnboardingVbond/validator

- Klik op AdvBondin geval van 12 .12vManagerValidator toevoegenin geval van 20.15/20.18vManage. Er wordt een pop-upvenster geopend. Voer de VPN 0 transporteert IP

van vBonds dat bereikbaar is vanaf de vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan vanuit de CLI van vManagetovBondIP.
- Voer de gebruikersreferenties van vBond in.

Opmerking: We moeten beheerdersreferenties gebruiken van vBond of een gebruikersonderdeel van netadminggroup. U kunt dit controleren in de CLI van de vBond. Kies Ja in de drop-down van "Genereer CSR" als we een nieuw certificaat voor vBond moeten installeren

Opmerking: Als de vBond zich achter een NAT-apparaat/firewall bevindt, controleert u of de vBond VPN 0-interface IP is vertaald naar een openbaar IP-adres. Als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u het openbare IP-adres van de VPN 0-interface in deze stap



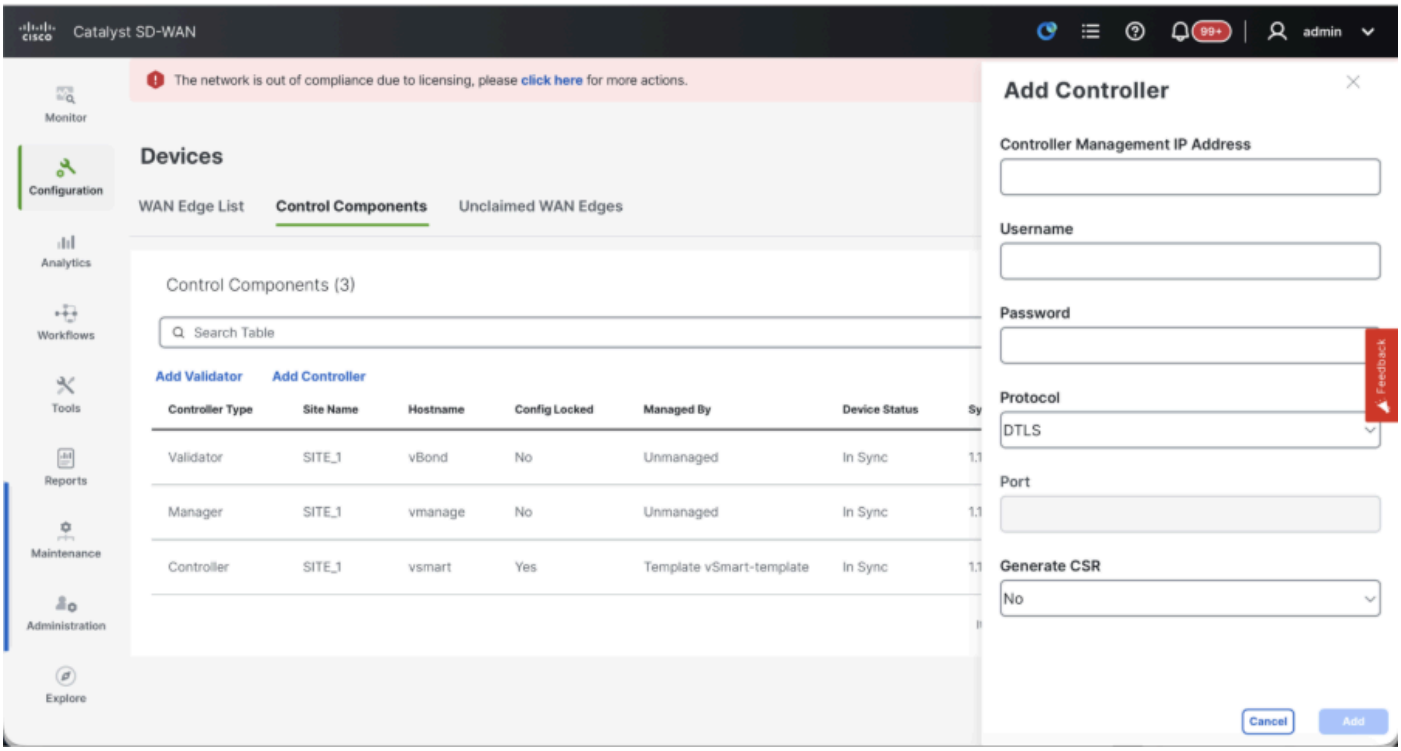
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door de vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vBond geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u

op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vBonds zijn, herhaalt u dezelfde stappen.

Onboarding vSmart/controller

- Klik op Add vSmart in geval van 10 .12 vManage of Add Controller in geval van 20.15/20.18 vManage.
- Als er een pop-upvenster wordt geopend, voert u het VPN 0-transport IP van vSmart in dat bereikbaar is via vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan van CLI van vManage naar vSmart IP.
- Voer de gebruikersreferenties van vSmart Note in die we nodig hebben om beheerdersreferenties van vSmart of een gebruikersdeel van de netadmin-groep te gebruiken.
- U kunt dit controleren in de CLI van de vSmart.
- Stel het protocol in op TLS als we TLS willen gebruiken voor routers om controleverbindingen met vSmart tot stand te brengen. Deze configuratie moet ook worden geconfigureerd op CLI van vSmarts- en vManage-knooppunten.
- Kies Ja in de keuzelijst "MVO genereren" als we een nieuw certificaat voor vSmart moeten installeren.

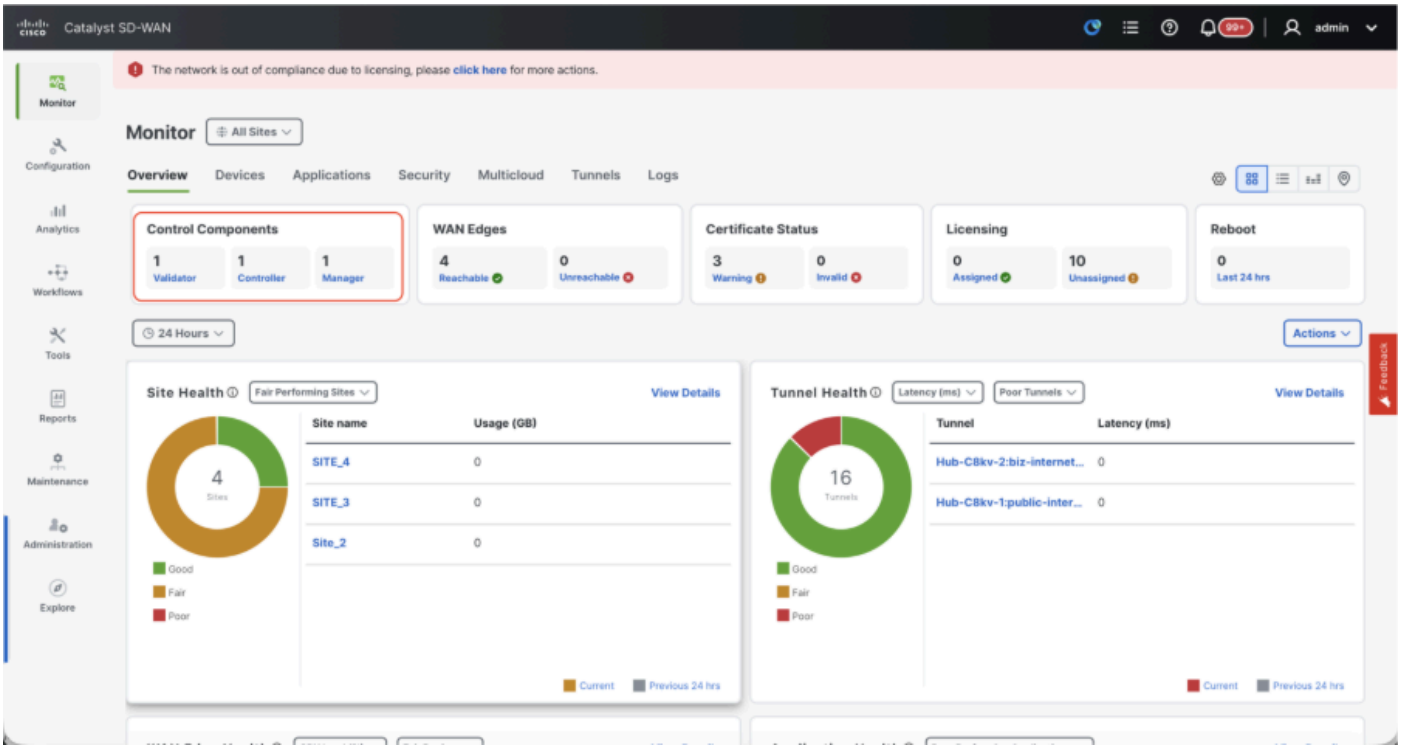
Opmerking: Als de vSmart zich achter NAT-apparaat/firewall bevindt, controleert u of de vSmart VPN 0-interface IP is vertaald naar een openbaar IP-adres en als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u in deze stap het openbare IP-adres van de VPN 0-interface IP.



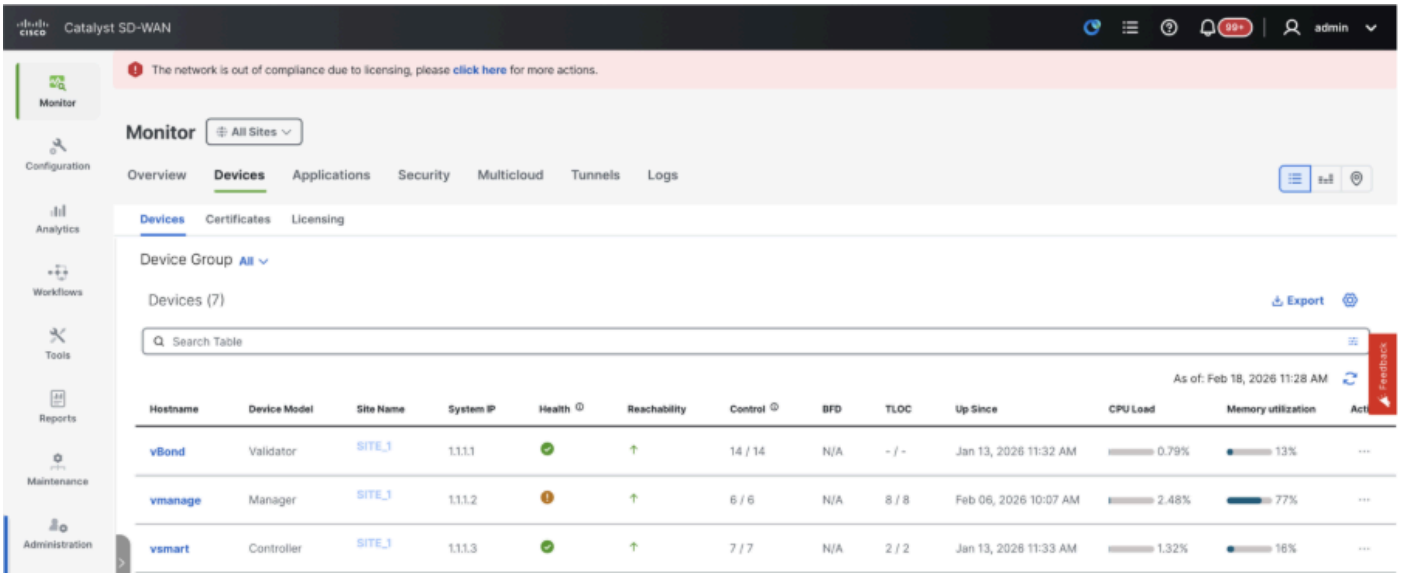
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vSmart geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.
- Als er meerdere vSmarts zijn, herhaalt u dezelfde stappen.

Verificatie

Controleer na voltooiing van alle stappen of alle besturingscomponenten bereikbaar zijn in Monitor>Dashboard



- Klik op de betreffende besturingscomponenten en bevestig dat ze allemaal bereikbaar zijn.
- Navigeer naar Monitor > Apparaten en controleer of alle besturingscomponenten bereikbaar zijn.



Stap 3: Config-DB Backup/Restore

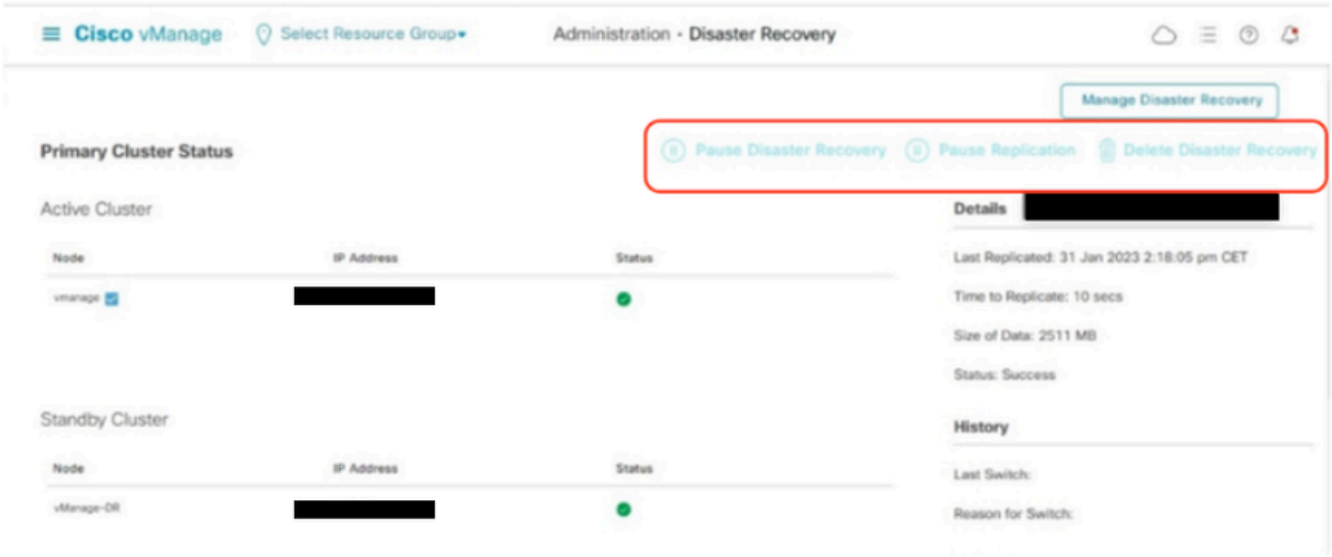
Configuratie-db-back-up en terugzetbewerkingen op een andere vManage-node verzamelen

---

Opmerking: Als u back-ups van de configuratiedatabase verzamelt van de bestaande vManage-node waarvoor Disaster Recovery is ingeschakeld, moet u ervoor zorgen dat deze worden verzameld nadat de Disaster Recovery op die node is gepauzeerd en verwijderd.

Bevestig dat er geen doorlopende Disaster Recovery-replicatie is. Navigeer naar Beheer > Disaster Recovery en Zorg ervoor dat de status Succesvol is en niet in een tijdelijke staat zoals Import Pending, Export Pending of Download Pending. Als de status niet succesvol is, neemt u contact op met Cisco TAC en zorgt u ervoor dat replicatie succesvol is voordat u doorgaat met het pauzeren van de Disaster Recovery.

Pauzeer eerst de Disaster Recovery en zorg ervoor dat de taak is voltooid. Verwijder vervolgens de Disaster Recovery en bevestig dat de taak is voltooid.



Neem contact op met Cisco TAC om ervoor te zorgen dat de Disaster Recovery met succes wordt opgeruimd.

Configuratie-DB-back-up verzamelen:

- In de SD-WAN-fabric die momenteel in gebruik is, kunt u configuratie-db-back-ups genereren op zowel standalone vManage- als vManage-clusterinstellingen.
- Voor standalone vManage is dat vManage zelf de leider op het gebied van configuratie-db.

Bevestig dat de configuratie-db wordt uitgevoerd op de vManage-node.

U kunt hetzelfde controleren met behulp van de opdrachtaanvraag nms configuration-db statusonvManageCLI. De output is zoals getoond

```
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#
```

Gebruik deze opdracht om de configuratie-db-back-up te verzamelen van de geïdentificeerde configuratie-db leader vManage-node.

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

De verwachte output is als volgt:

```
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#
```

- Noteer de configuratie-db-referenties als deze is bijgewerkt.
- Als u de configuratie-db-referenties niet kent, neemt u contact op met TAC om de configuratie-db-referenties op te halen uit de bestaande vManage-knooppunten.
- Standaardconfiguratie-db-referenties zijn gebruikersnaam: neo4j en wachtwoord: wachtwoord

Configuration-db Backup terugzetten naar een andere vManage-node

Kopieer de configuratie-db back-up naar /home/admin/ directory van vManage met behulp van SCP.

Voorbeeld van scp-opdrachtuitvoer:

```
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
```

Om de configuratie-db back-up te herstellen, moeten we eerst de configuratie-db referenties configureren. Als uw configuratie-db-referenties standaard zijn (neo4j / wachtwoord), kunnen we deze stap overslaan.

Als u configuratie-db-referenties wilt configureren, gebruikt u de opdracht request nms configuration-db update-admin-user. Gebruik de gebruikersnaam en het wachtwoord van uw keuze.

Houd er rekening mee dat de toepassingsserver van vManage opnieuw wordt gestart. Hierdoor wordt de gebruikersinterface van vManage korte tijd ontoegankelijk.

```
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#
```

Post waarin we kunnen doorgaan met het herstellen van de configuratie-db back-up:

We kunnen de opdracht request nms configuration-db restore path /home/admin/< > gebruiken om de configuratie-db te herstellen naar de nieuwe vManage:

```
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
```

Zodra de configuratie-db is hersteld, moet u ervoor zorgen dat de vManage UI toegankelijk is. Wacht ongeveer 5 minuten en probeer vervolgens toegang te krijgen tot de gebruikersinterface.

Als u eenmaal met succes bent ingelogd op de gebruikersinterface, moet u ervoor zorgen dat de lijst met Edge-routers, het sjabloon, het beleid en alle andere configuraties die aanwezig waren op uw vorige of bestaande vManage-gebruikersinterface, worden weergegeven in de nieuwe vManage-gebruikersinterface.

Stap 4: DR-installatie met één node

Raadpleeg Stap 2: Voorcontroles in Combinatie 2: Standalone vManage + Single Node DR en zorg ervoor dat we alle vereisten hebben voltooid voordat we doorgaan om Disaster Recovery in te schakelen.

Single Node DR

Voorwaarden

- Zorg ervoor dat de primaire en de secundaire node bereikbaar zijn via HTTPS op een transport VPN (VPN 0).

- Zorg ervoor dat de primaire node en de secundaire node van Cisco vManage dezelfde Cisco vManage-versie gebruiken.

Out-of-band clusterinterface in VPN 0

1. Voor elke vManage-instantie in een cluster is een derde interface (clusterkoppeling) vereist naast de interfaces die worden gebruikt voor VPN 0 (transport) en VPN 512 (beheer).
2. Deze interface wordt gebruikt voor communicatie en synchronisatie tussen de vManage-servers in het cluster.
3. Deze interface moet ten minste 1 Gbps zijn en een latentie van 4 ms of minder hebben. Een interface van 10 Gbps wordt aanbevolen.
4. Beide vManage-knooppunten moeten elkaar via deze interface kunnen bereiken: of het nu een laag 2-segment is of via laag 3-routering.

- Zorg ervoor dat alle services (toepassingsserver, configuratie-db, berichtenserver, coördinatieserver en statistiek-db) zijn ingeschakeld op beide Cisco vManage-knooppunten.
- Verdeel alle controllers, inclusief Cisco vBond Orchestrators, over zowel primaire als secundaire datacenters. Zorg ervoor dat deze controllers bereikbaar zijn voor Cisco vManage-knooppunten die over deze datacenters zijn verdeeld. De controllers maken alleen verbinding met de primaire Cisco vManage-node.
- Zorg ervoor dat er geen andere bewerkingen worden uitgevoerd in de actieve (primaire) en de standby (secundaire) Cisco vManage-node. Zorg er bijvoorbeeld voor dat er geen servers bezig zijn met het upgraden of dat er geen sjablonen worden gekoppeld aan apparaten.

- Schakel de Cisco vManage HTTP/HTTPS-proxyserver uit als deze is ingeschakeld. Als u de proxyserver niet uitschakelt, probeert Cisco vManage een noodherstelcommunicatie tot stand te brengen via het IP-adres van de proxy, zelfs als de IP-adressen van Cisco vManage out-of-band clusters direct bereikbaar zijn. U kunt de Cisco vManage HTTP/HTTPS-proxyserver opnieuw inschakelen nadat de registratie voor Disaster Recovery is voltooid.

- Voordat u het registratieproces voor noodherstel start, gaat u naar het venster Tools → Rediscover Network op de primaire Cisco vManage-node en herontdekt u de Cisco vBond Orchestrators.

Configuratie

Configureer de CLI-configuraties van alle vManage-knooppunten die fungeren als Disaster Recovery-knooppunt

De minimale configuratie voor vManagevoorafgaand aan de registratie voor Disaster Recovery wordt weergegeven

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Opmerking: Als we URL als vBond-adres gebruiken, moet u de IP-adressen van de DNS-server configureren in VPN 0-configuratie of ervoor zorgen dat deze kunnen worden opgelost.

Deze configuraties zijn nodig om de transportinterface die wordt gebruikt om besturingsverbindingen met de routers en de rest van de controllers tot stand te brengen, mogelijk te maken

```
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
```

Configureer ook de VPN 512management interface om out-of-band management toegang tot de controller mogelijk te maken.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
commit
```

Serviceinterface configureren op de DR vManage

Configureer de service-interface op de vManage-node. Deze interface wordt gebruikt voor DR-communicatie,

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Zorg ervoor dat hetzelfde IP-subnet wordt gebruikt voor de service-interface op de primaire vManage en DR vManage

De configuraties op de vManage-gebruikersinterface bijwerken

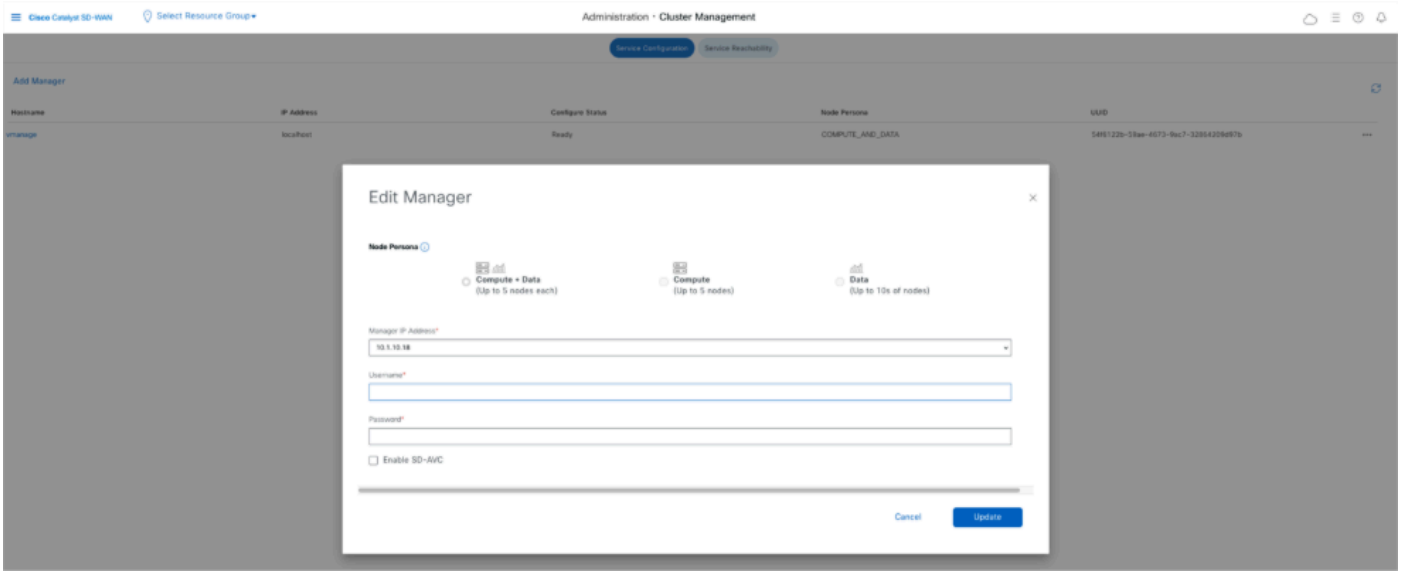
- Zodra de configuraties zijn toegevoegd aan de CLI van alle controllers, hebben we toegang tot de webUI van vManage, met behulp van de URL https://<vmanage-ip> in uw browser. Gebruik het VPN 512 IP-adres van de respectieve vManage-knooppunten. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Beheer > Instellingen en voer deze stappen uit.
- Configureer de naam van de organisatie. Configureer dezelfde waarde als in de CLI van de vManage-node.
- In vManage 20.15/20.18 zijn deze configuraties beschikbaar onder de sectie Systeem.

Certificaat installeren op DR vManage

Ga verder met de stappen die worden beschreven in sectie Combinatie 2: Standalone vManage + Single Node DR Stap 3: vManage UI, Certificaten en Onboard Controllers configureren om het certificaat op de Disaster Recovery vManage te installeren.

De configuratie voor Disaster Recovery toevoegen

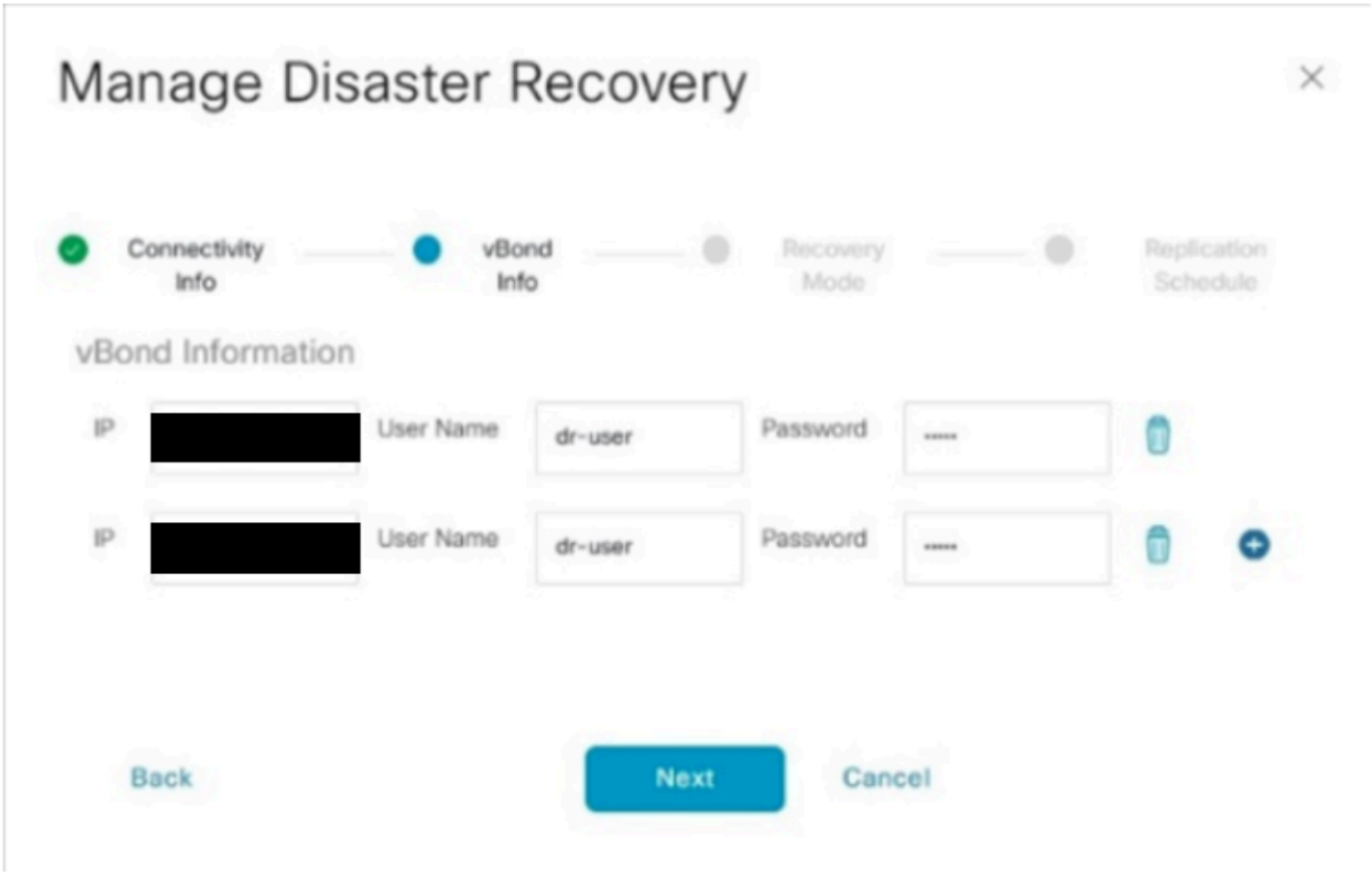
- Ga hiervoor naar de primaire vManage.
- Navigeer naar Beheer → Clusterbeheer en geef het IP-adres van de out-of-band-interface aan nadat u op de drie punten aan de rechterkant van het vManage-item hebt geklikt en voeg gebruikersnaam en wachtwoord toe. Het wordt aanbevolen om voor deze configuratie een afzonderlijke lokale gebruiker te maken, bijvoorbeeld dradmin op zowel primaire als DR vmanage.



- VManage wordt na deze wijziging opnieuw opgestart.
- Nadat het primaire vManage-bestand is verschenen, gaat u naar Beheer → Disaster Recovery. Klik op 'Disaster Recovery beheren'.
- Vul in het pop-upvenster de gegevens voor zowel primaire als secundaire vManage in.
- De aan te geven IP-adressen zijn de out-of-band clusterinterfaces (eth2) IP-adressen.
- De referenties moeten afkomstig zijn van een netadmin-gebruiker (dradmin) en mogen niet worden gewijzigd zodra de DR is geconfigureerd. Er kan een afzonderlijke vManage-referenties voor lokale gebruikers voor Disaster Recovery worden gebruikt. We moeten

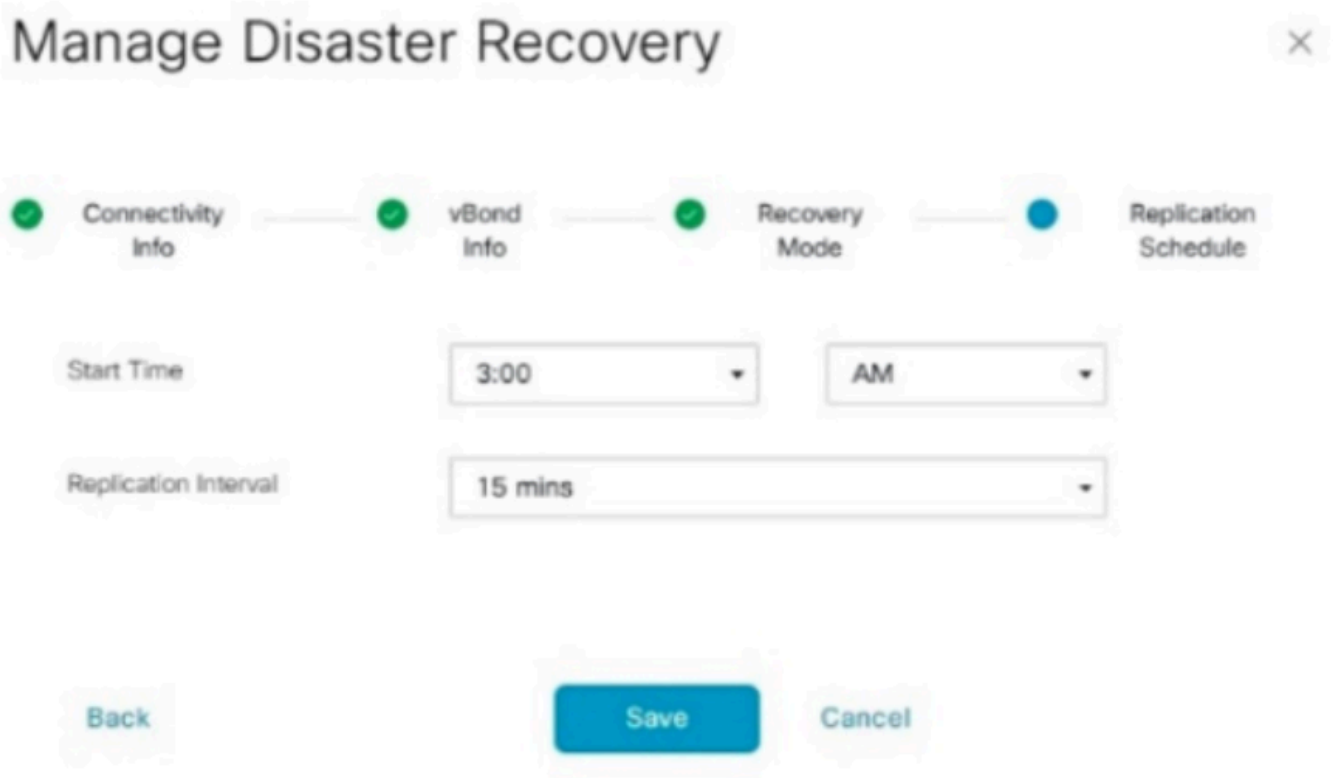
ervoor zorgen dat de lokale vManage-gebruiker deel uitmaakt van de netadmin-groep. Zelfs de admin-inloggegevens kunnen hier worden gebruikt.

- Klik na het invullen op ‘Volgende’.
- Vul de gegevens van de vBond-controllers in.
- De vBond-controllers moeten bereikbaar zijn via het opgegeven IP-adres via Netconf.
- De referenties moeten afkomstig zijn van een netadmin-gebruiker (dradmin) en mogen niet worden gewijzigd zodra de DR is geconfigureerd.
- Hiervoor is het aan te raden dat vBond deze dradmin gebruiker lokaal laat configureren of je kunt de admin gebruiker gebruiken om de vBond toe te voegen.

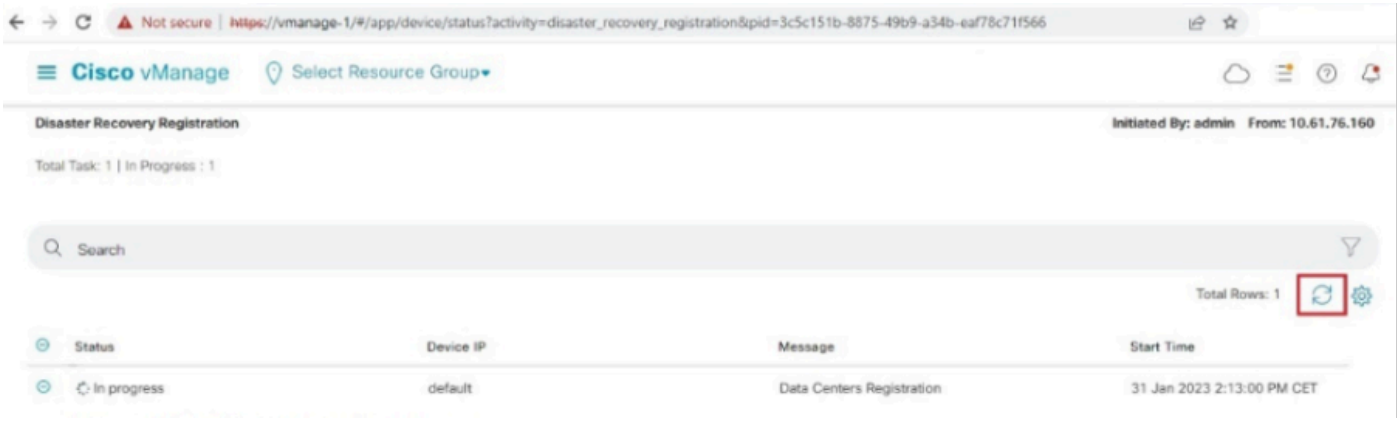


- Klik na het invullen op ‘Volgende’.
- Kies in de herstelmodus ‘Handmatig’. Klik op ‘Volgende’.

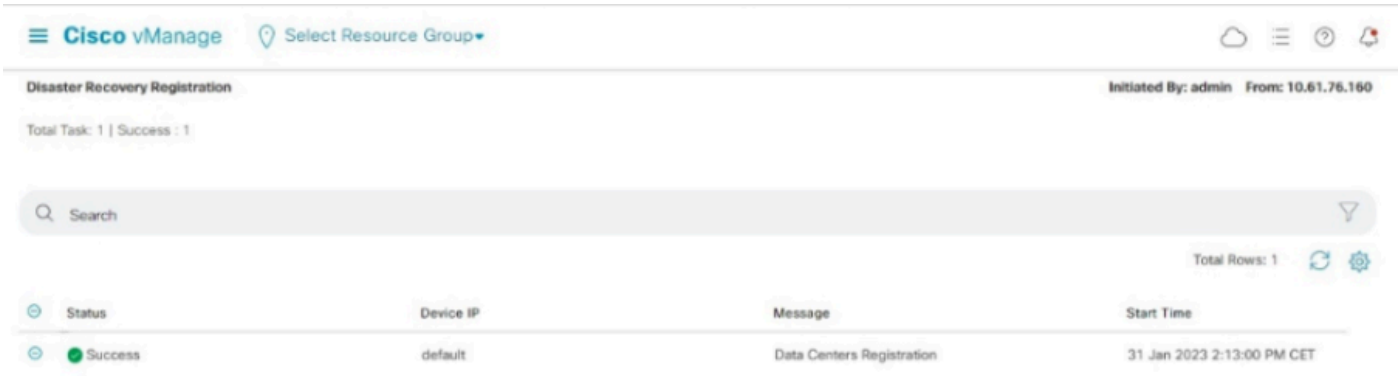
Stel in het Replicatieschema het ‘Replicatie-interval".Elke replicatie-intervaltijd worden de gegevens gerepliceerd vanaf primaire vManage naar secundair vManage. De minimale configureerbare waarde is 15 minuten.



- Stel de waarde in en klik op ‘Opslaan’.
- De registratie van DR begint nu. Klik op de knop Vernieuwen om de status en de voortgangslogboeken handmatig te vernieuwen. Dit proces kan tot 20-30 minuten duren.

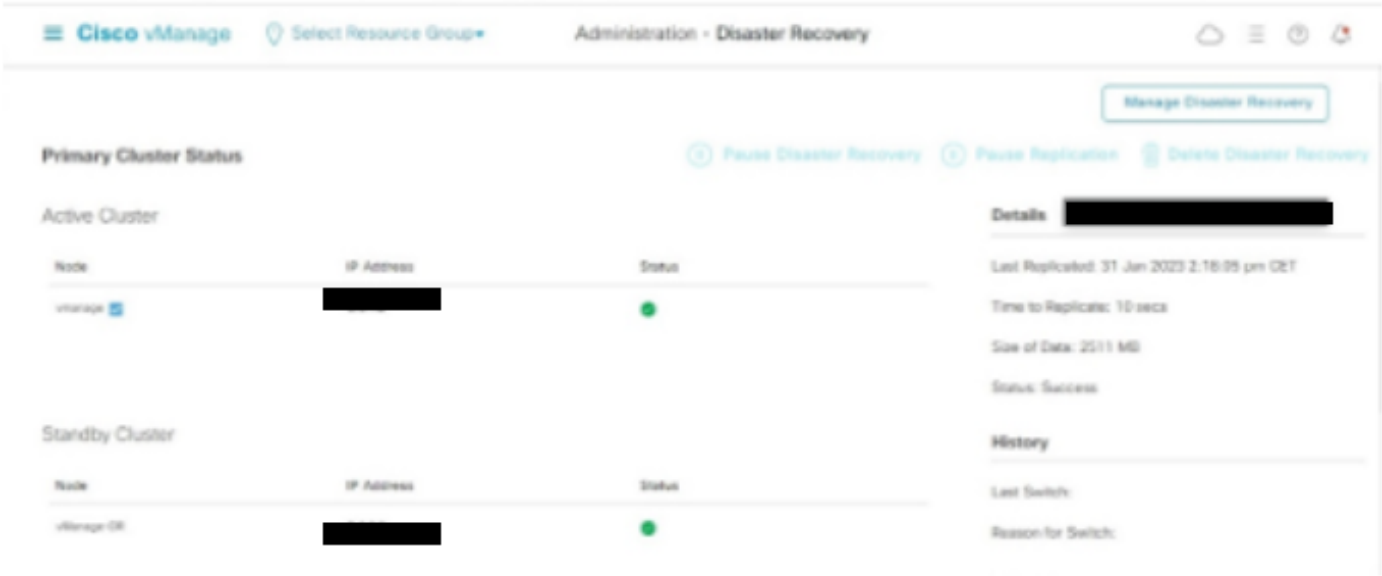


- Merk op dat de vManage GUI tijdens dit proces opnieuw wordt opgestart.
- Eenmaal voltooid, moet een status van succes worden gezien.



Verifiëren

Navigeer naar Beheer → Disaster Recoveryom de Disaster Recovery-status te zien en wanneer de gegevens de laatste keer zijn gerepliceerd.



Stap 5: Reauthenticatie van controllers en ongeldigverklaring van oude controllers

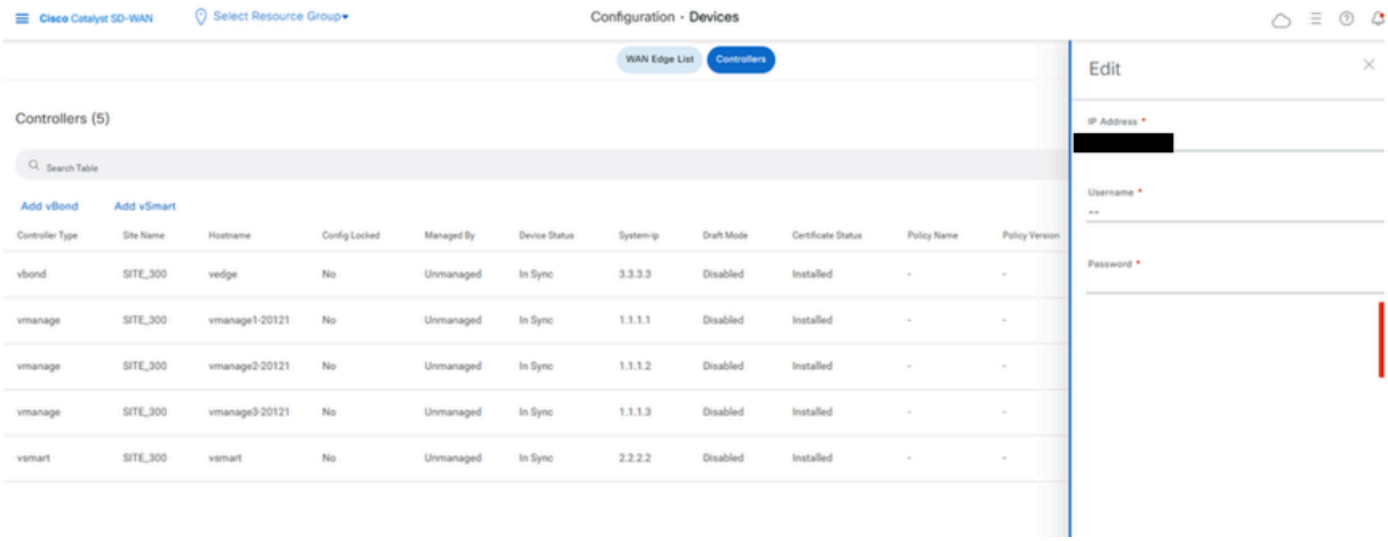
Zodra configuratie-db is hersteld, moeten we alle nieuwe controllers (vmanage/vsmart/vbond) in de fabric opnieuw verifiëren

---

Opmerking: Als de IP-interface die wordt gebruikt om opnieuw te verifiëren de tunnelinterface IP is, moet u ervoor zorgen dat de NETCONF-service is toegestaan op de tunnelinterface van de vManage, vSmart en vBond en ook op de firewalls langs het pad. De firewallpoort die moet worden geopend is TCP-poort 830 als bidirectionele regel van DR-cluster naar alle vBonds en vSmarts.

Klik in vmanage UI op Configuration > Devices > Controllers

- Klik op de drie puntjes bij elke controller en klik op Bewerken



- Vervang het ip-adres (system-ip van de controller) door het transport vpn 0 (tunnel interface) ip-adres .Voer de gebruikersnaam en het wachtwoord in en klik op opslaan
- Doe hetzelfde voor alle nieuwe controllers in de stof

Synchroniseer de Root-cert-keten

Als alle controllers zijn geïnstalleerd, voert u deze stap uit:

Voer op elke Cisco SD-WAN Manager-server in het nieuw actieve cluster de volgende acties uit:

Voer deze opdracht in om het rootcertificaat te synchroniseren met alle Cisco Catalyst SD-WAN-apparaten in het nieuw actieve cluster:

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

Voer deze opdracht in om de Cisco SD-WAN Manager UUID te synchroniseren met de Cisco SD-WAN Validator:

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

Zodra de fabric is hersteld en de controle- en bfd-sessies zijn ingesteld voor alle randen en controllers in de fabric, moeten we de oude controllers (vmanage/vsmart/vbond) van de gebruikersinterface ongeldig maken

- Klik op Configuratie > Apparaten > Certificaten in vmanage UI
- Klik op Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Ongeldig maken
- Klik op verzenden naar vbond
- Klik in vmanage UI op Configuration > Devices > Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Verwijderen

Stap 6: Controles achteraf

Opmerking: ga verder met het gedeelte Controles achteraf dat hier wordt weergegeven en dat voor alle implementatiecombinaties geldt.

Combinatie 3: vManage Cluster + No DR

Benodigde gevallen:

- 3 vManage (cluster met 3 knooppunten, alle COMPUTE_AND_DATA) of 6 vManage (3 COMPUTE_AND_DATA + 3 DATA)
- 1 of meer vBond
- 1 of meer vSmart

Stappen:

1. Alle instanties weergeven met de gemeenschappelijke stappen
2. Voorcontroles
3. Configureren van vManage UI, certificaten en onboard controllers
4. vManage-cluster samenstellen
5. Config-db back-up/terugzetbewerking
6. Controles achteraf

Stap 1: Controles vooraf

- Zorg ervoor dat het aantal actieve Cisco SD-WAN Managerinstances gelijk is aan het aantal nieuw geïnstalleerde Cisco SD-WAN Managerinstances.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties dezelfde softwareversie uitvoeren.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties het IP-

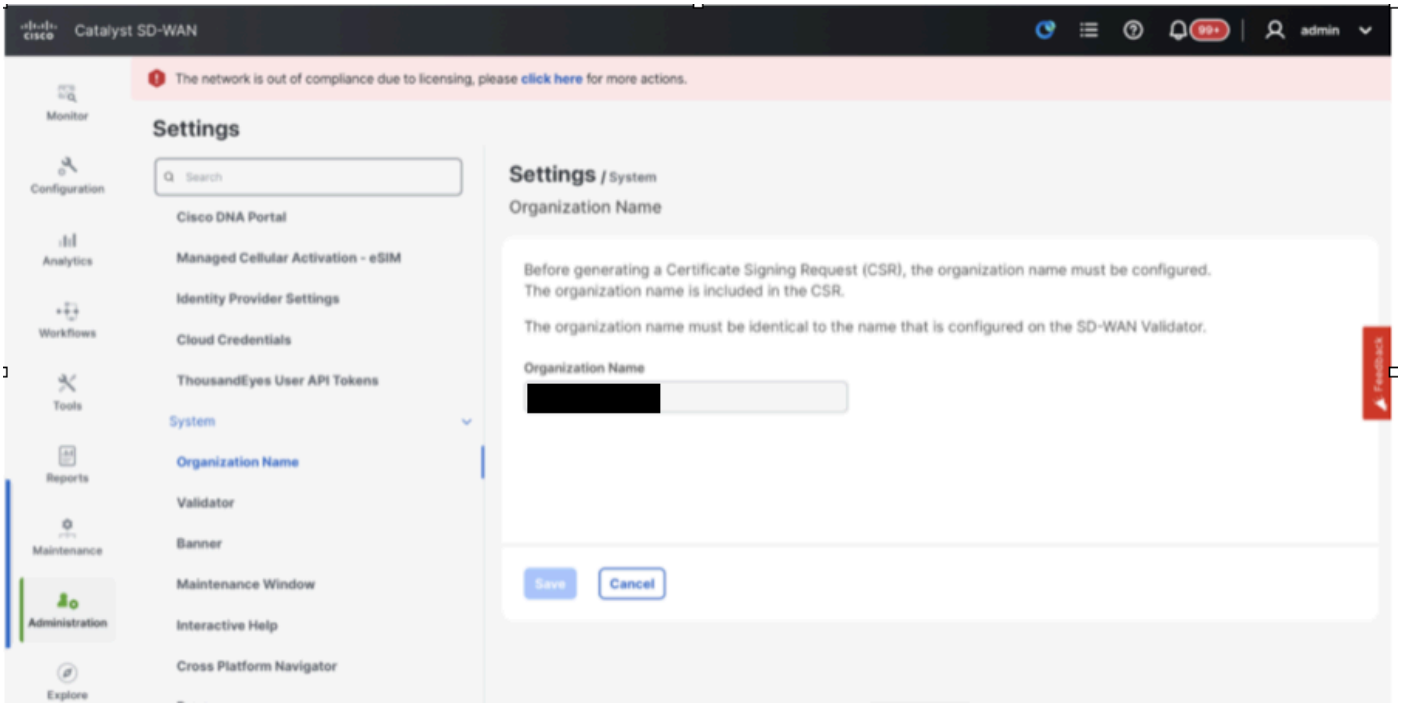
beheeradres van de Cisco SD-WAN Validator kunnen bereiken.

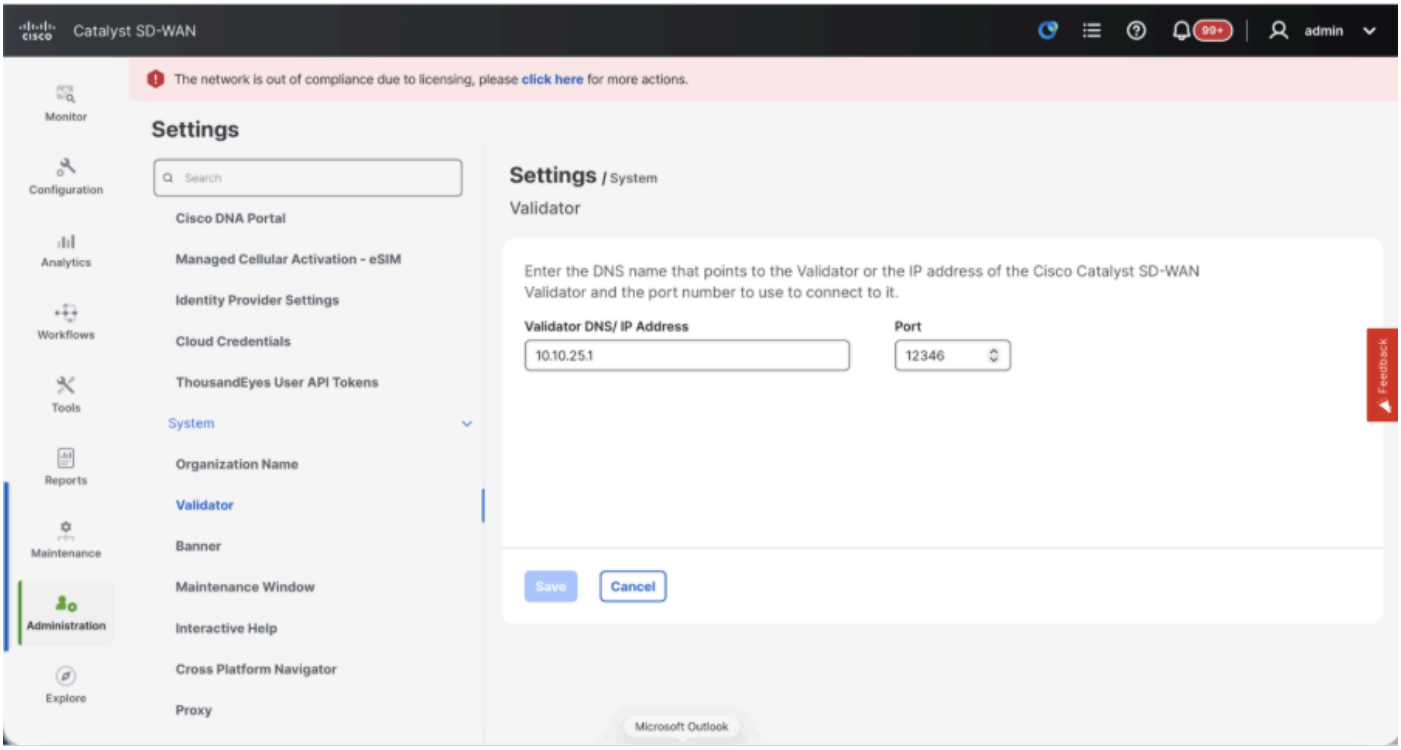
- Controleer of certificaten zijn geïnstalleerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties.
- Zorg ervoor dat de klokken op alle Cisco Catalyst SD-WAN-apparaten, inclusief de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, worden gesynchroniseerd.
- Zorg ervoor dat een nieuwe set van systeem-IP's en site-ID's is geconfigureerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, samen met dezelfde basisconfiguratie als het actieve cluster.

Stap 2: vManage UI, certificaten en ingebouwde controllers configureren

De configuraties op de vManage-gebruikersinterface bijwerken

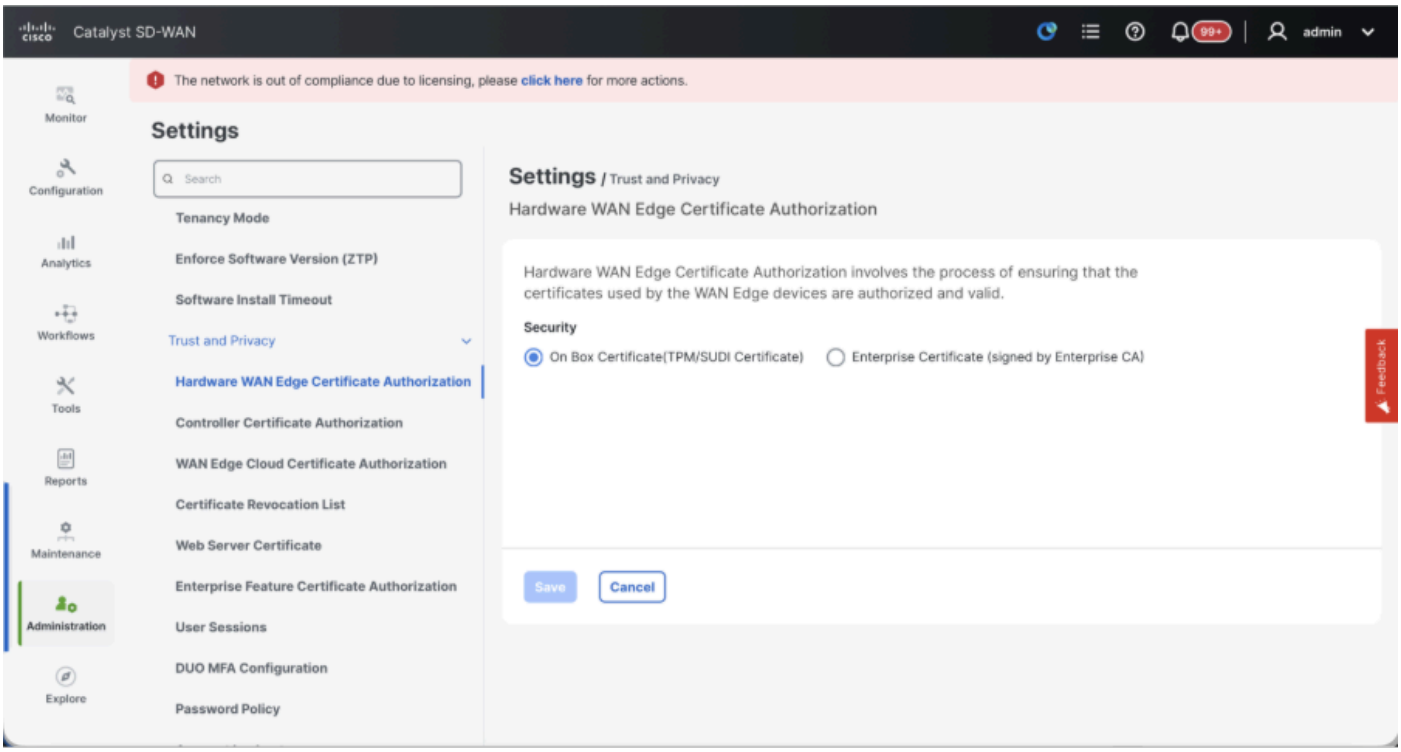
- Zodra de configuraties in stap 1 zijn toegevoegd aan de CLI van alle controllers, hebben we toegang tot de webUI van vManage, met behulp van de URL https://<vmanage-ip> in uw browser. Gebruik het VPN 512 IP-adres van de respectieve vManage-knooppunten. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Beheer > Instellingen en voer deze stappen uit.
- Configureer de naam van de organisatie en het URL/IP-adres van de validator/vBond. Configureer dezelfde waarde als in de CLI van de vManage-node.
- In vManage 20.15/20.18 zijn deze configuraties beschikbaar onder de sectie Systeem.



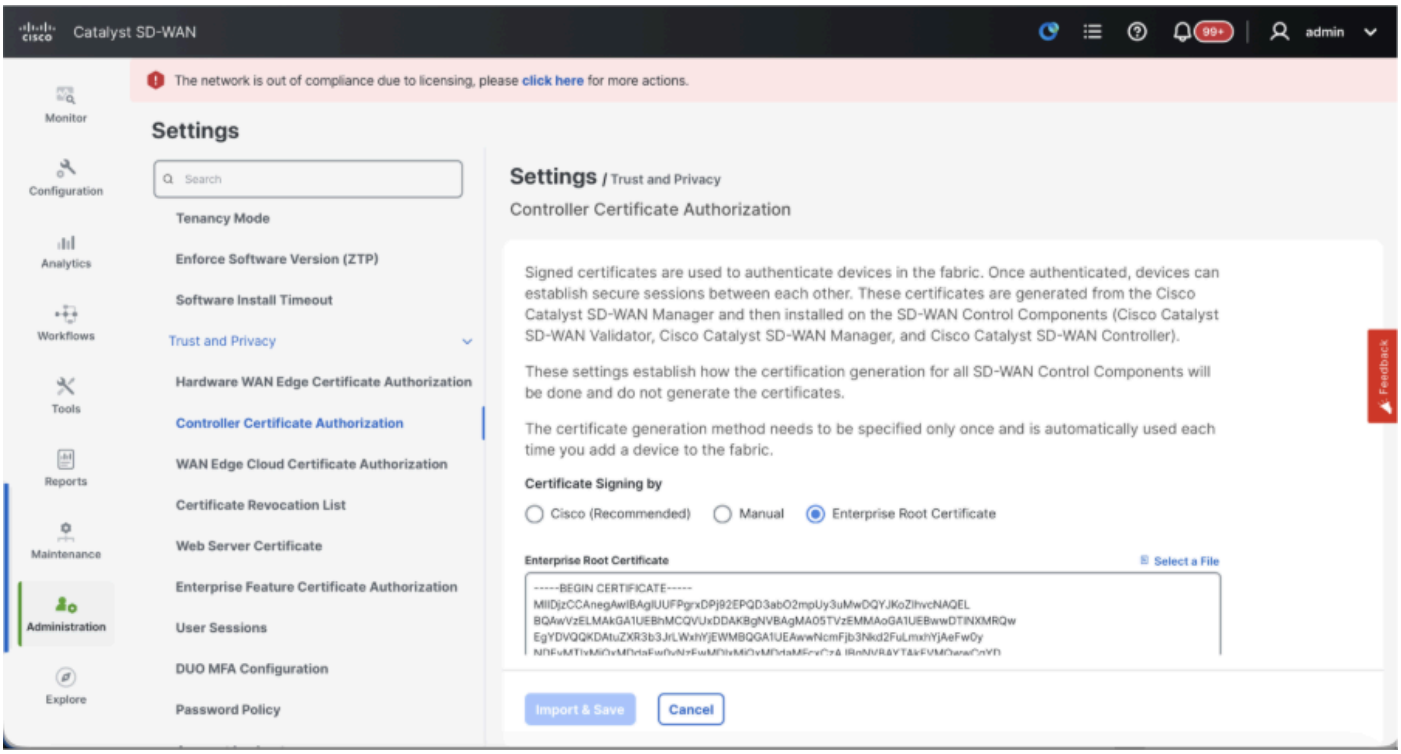


- Controleer de configuraties voor Certificaatautorisatie (CA), die bepaalt welke Certificaatautoriteit wordt gebruikt voor het ondertekenen van de certificaten. We zien daar 3 mogelijkheden:

1. Hardware WAN Edge Certificate Authorization - Bepaalt de CA voor hardware SD-WAN Edge-routers.
    - On Box Certificate (TPM/SUDI-certificaat) - Met deze optie wordt het vooraf geïnstalleerde certificaat op de hardware van de router gebruikt om de Controleverbindingen (TLS/DTLS-verbindingen) tot stand te brengen
    - Enterprise Certificate (ondertekend door Enterprise CA) - Met deze optie gebruiken de routers certificaten die zijn ondertekend door Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

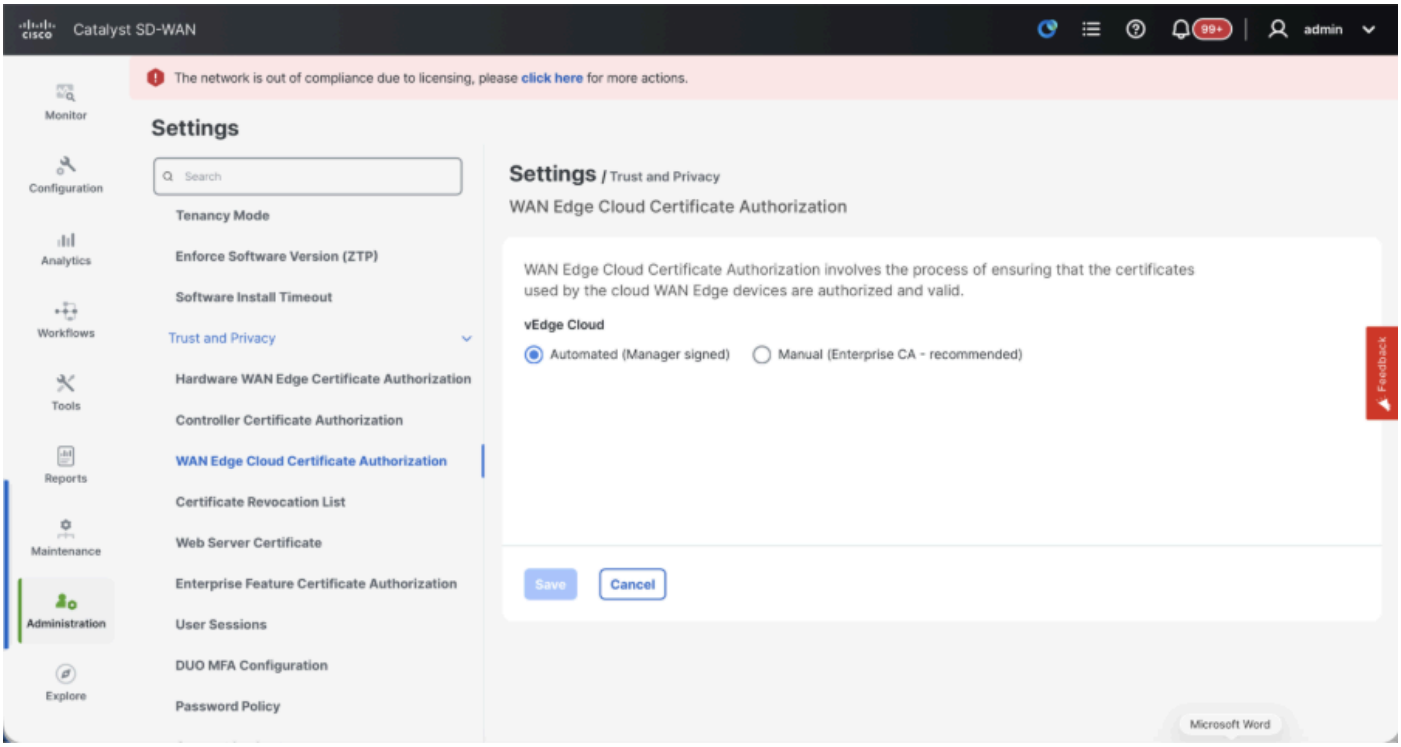


2. Controllercertificaatautorisatie - bepaalt de CA voor SD-WAN-controllers.
    - Cisco (aanbevolen) - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. vManage neemt automatisch contact op met het PNP-portaal met behulp van de referenties voor slimme accounts die zijn geconfigureerd op de vManage en laat het certificaat ondertekenen en installeren op de controller.
    - Handleiding - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. Handmatig ondertekenen van de CSR met behulp van de Cisco PNP portal door te navigeren naar smart account en virtuele account van de respectieve SD-WAN overlay.
    - Enterprise Root Certificate - Met deze optie gebruiken de routers certificaten die zijn ondertekend door de Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

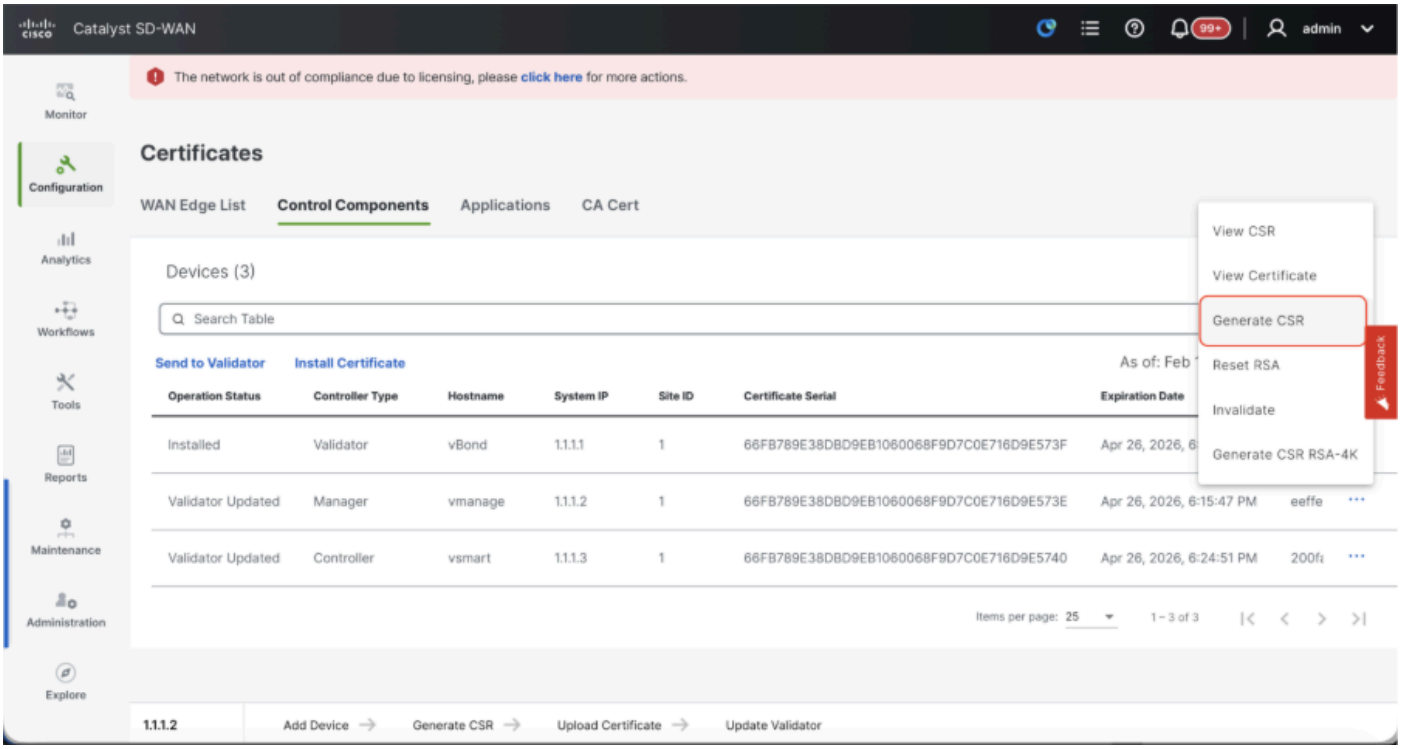


3. WAN Edge Cloud Certificate Authorization - Bepaalt de CA voor virtuele SD-WAN Edge-routers (CSR1000v, C8000v, vEdge cloud)
    - Geautomatiseerd (vManage ondertekend) - vManage ondertekent automatisch de CSR voor de virtuele Edge-routers en installeert het certificaat op de router.
    - Handmatig (Enterprise CA - aanbevolen) - Virtuele routers gebruiken certificaten die zijn ondertekend door de certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

Als we onze eigen CA, Enterprise-certificeringsinstantie, gebruiken, kiest u in dat geval Enterprise.



- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers
- Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

Onboarding vBond/Validator en vSmart/Controller naar de vManage

Navigeer naar Configuratie > Apparaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

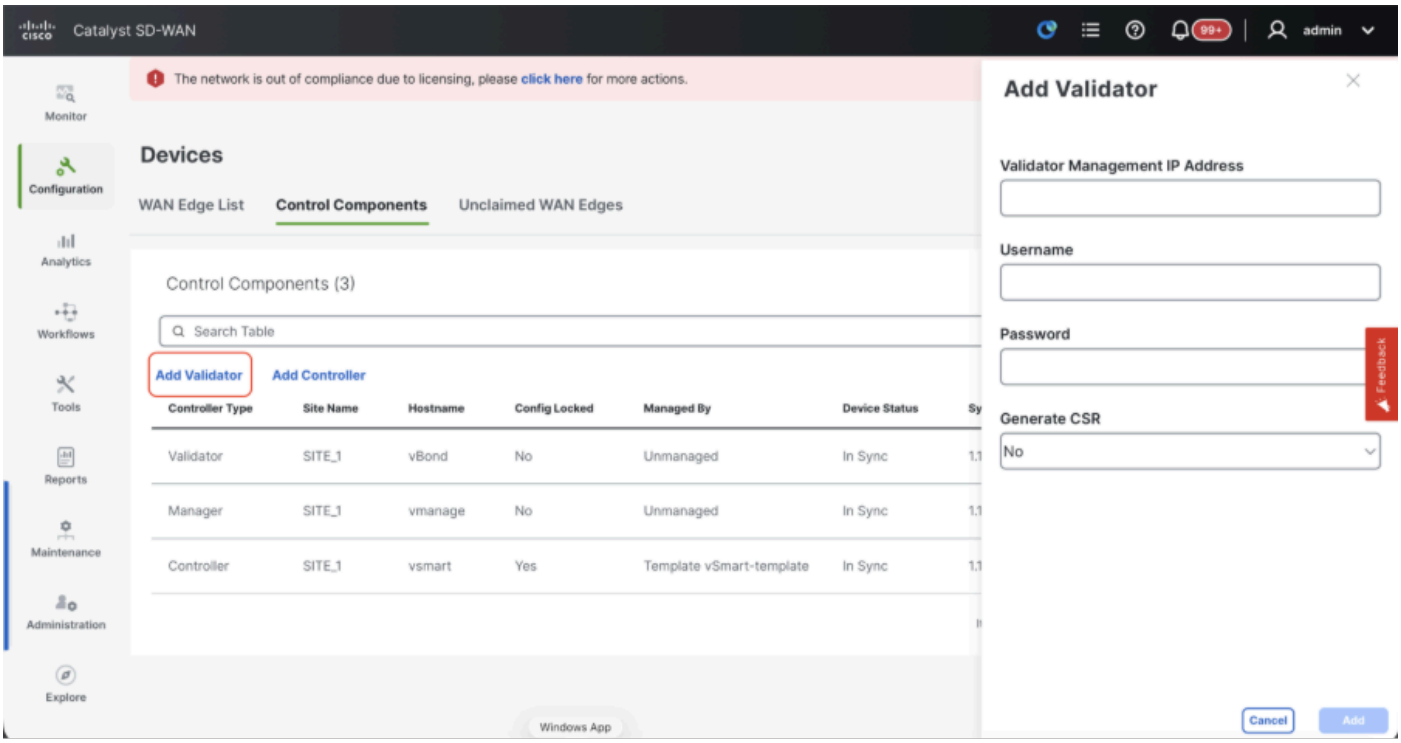
OnboardingVbond/validator

- Klik op AdvBondin geval van 12 .12vManagerValidator toevoegenin geval van 20.15/20.18vManage. Er wordt een pop-upvenster geopend. Voer de VPN 0 transporteert IP

van vBonds dat bereikbaar is vanaf de vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan vanuit de CLI van vManagetovBondIP.
- Voer de gebruikersreferenties van vBond in.

Opmerking: We moeten beheerdersreferenties gebruiken van vBond of een gebruikersonderdeel van netadminggroup. U kunt dit controleren in de CLI van de vBond. Kies Ja in de drop-down van "Genereer CSR" als we een nieuw certificaat voor vBond moeten installeren

Opmerking: Als de vBond zich achter een NAT-apparaat/firewall bevindt, controleert u of de vBond VPN 0-interface IP is vertaald naar een openbaar IP-adres. Als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u het openbare IP-adres van de VPN 0-interface in deze stap



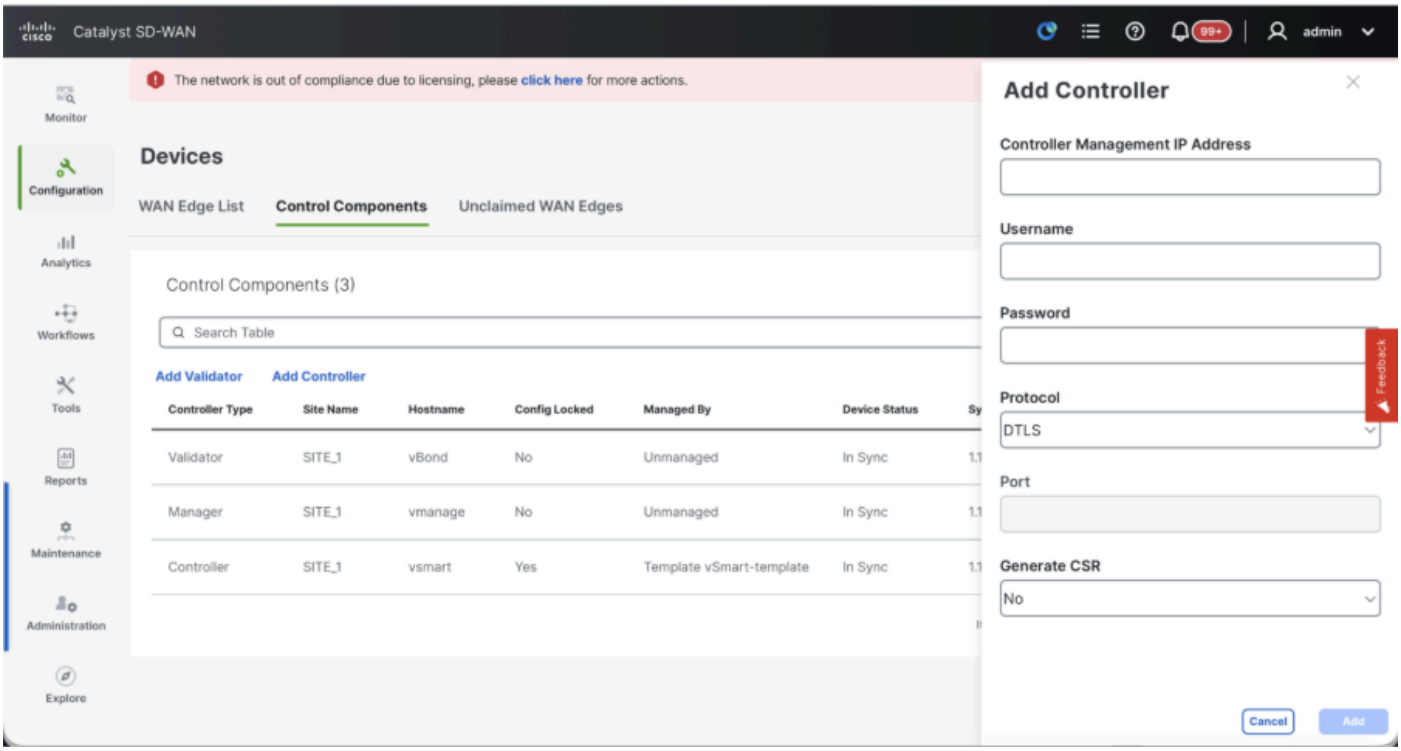
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door de vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vBond geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u

op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vBonds zijn, herhaalt u dezelfde stappen.

Onboarding vSmart/controller

- Klik op Add vSmart in geval van 10 .12 vManage of Add Controller in geval van 20.15/20.18 vManage.
- Als er een pop-upvenster wordt geopend, voert u het VPN 0-transport IP van vSmart in dat bereikbaar is via vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan van CLI van vManage naar vSmart IP.
- Voer de gebruikersreferenties van vSmart Note in die we nodig hebben om beheerdersreferenties van vSmart of een gebruikersdeel van de netadmin-groep te gebruiken.
- U kunt dit controleren in de CLI van de vSmart.
- Stel het protocol in op TLS als we TLS willen gebruiken voor routers om controleverbindingen met vSmart tot stand te brengen. Deze configuratie moet ook worden geconfigureerd op CLI van vSmarts- en vManage-knooppunten.
- Kies Ja in de keuzelijst "MVO genereren" als we een nieuw certificaat voor vSmart moeten installeren.

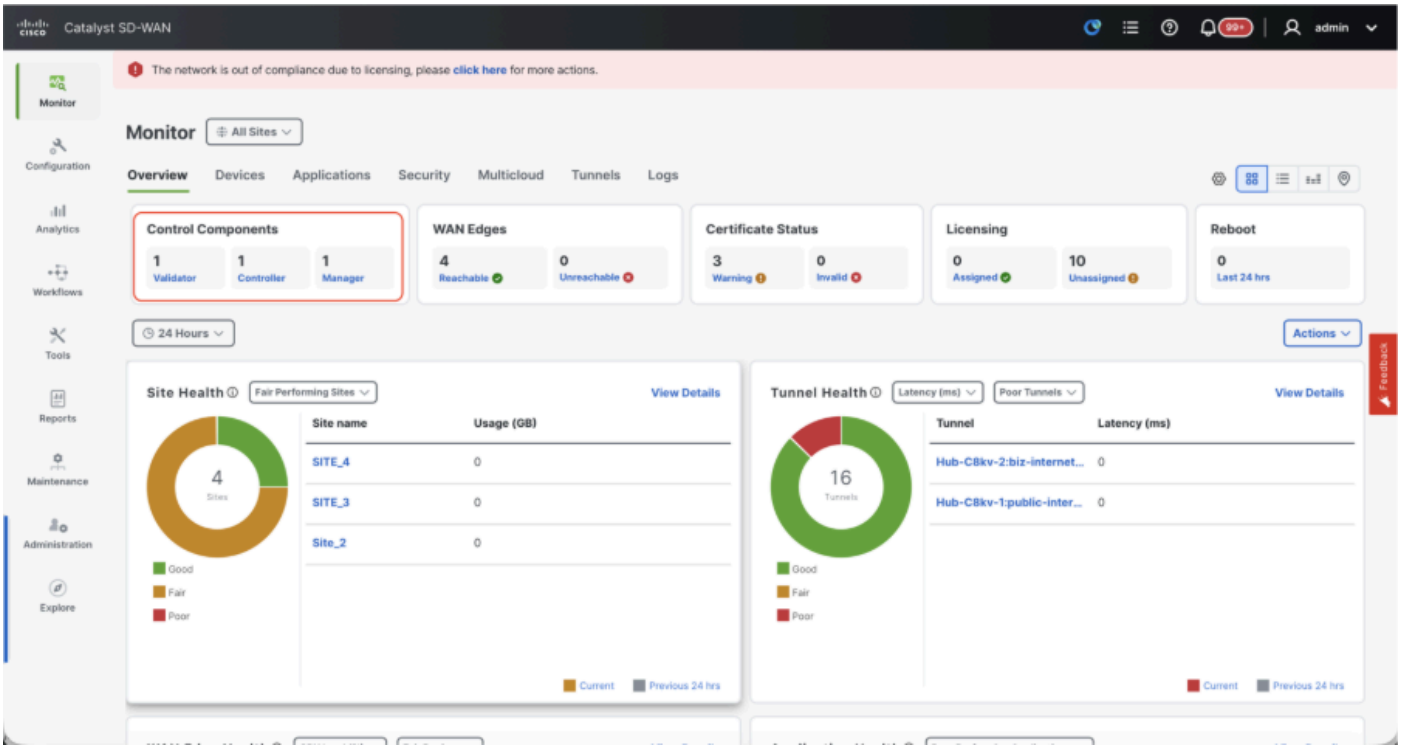
Opmerking: Als de vSmart zich achter NAT-apparaat/firewall bevindt, controleert u of de vSmart VPN 0-interface IP is vertaald naar een openbaar IP-adres en als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u in deze stap het openbare IP-adres van de VPN 0-interface IP.



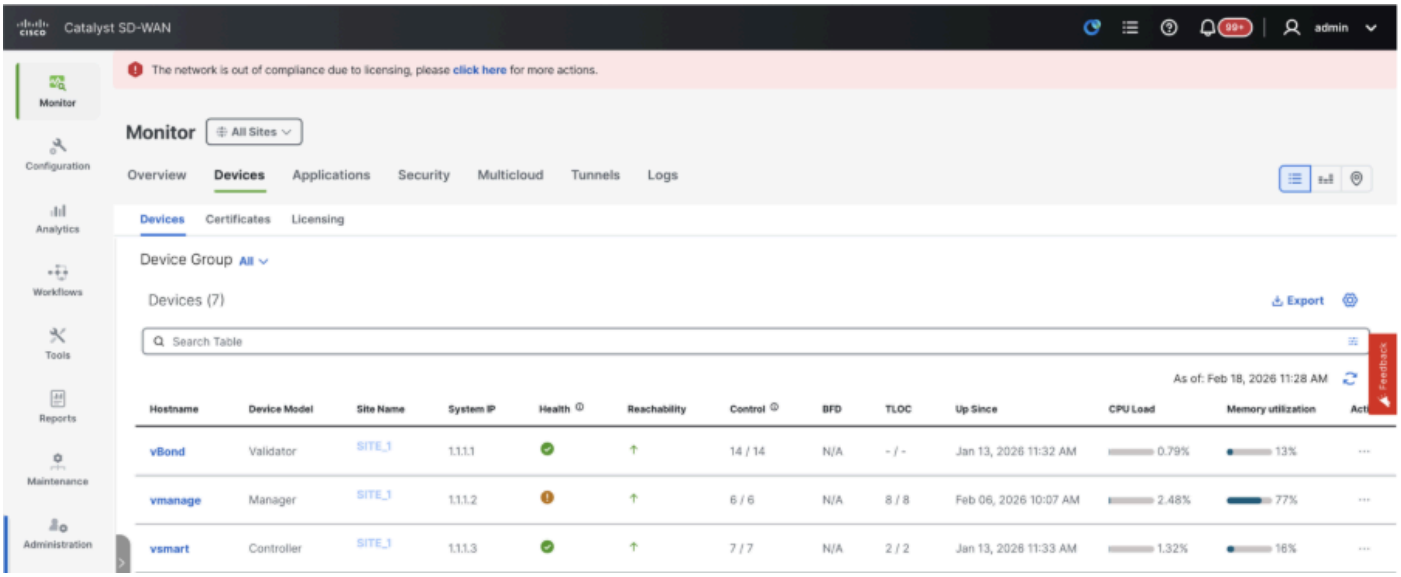
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vSmart geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren.
- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.
- Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vSmarts zijn, herhaalt u dezelfde stappen.

Verificatie

Controleer na voltooiing van alle stappen of alle besturingscomponenten bereikbaar zijn in Monitor>Dashboard



- Klik op de betreffende besturingscomponenten en bevestig dat ze allemaal bereikbaar zijn.
- Navigeer naar Monitor > Apparaten en controleer of alle besturingscomponenten bereikbaar zijn.



Stap 3: vManage-cluster samenstellen

Onboard SD-WAN-verbinding met een vManage-cluster in de SD-WAN-overlay

---

Opmerking: vManage Cluster kan worden geconfigureerd met 3 vManage-knooppunten of 6 vManage-knooppunten, afhankelijk van het aantal sites dat aan boord is van de SD-WAN-verbinding. Raadpleeg uw bestaande vManage-cluster en kies het aantal knooppunten volgens hetzelfde.

De CLI-configuraties configureren van alle vManage-knooppunten die deel uitmaken van het cluster

Systeemconfiguratie configureren voor alle vManage-knooppunten

- De rest van de vManage-knooppunten configureren. In het geval van een cluster met drie knooppunten moet u nog twee knooppunten configureren, in het geval van een cluster met zes knooppunten moet u vijf knooppunten configureren.
- Systeemconfiguraties configureren zoals wordt weergegeven:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Opmerking: Als we URL als vBond-adres gebruiken, moet u de IP-adressen van de DNS-

server configureren in VPN 0-configuratie of ervoor zorgen dat deze kunnen worden opgelost.

De transportinterface op alle vManage-knooppunten configureren

Deze configuraties zijn nodig om de transportinterface die wordt gebruikt om besturingsverbindingen met de routers en de rest van de controllers tot stand te brengen.

```
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
```

Beheerinterface configureren op alle vManage-knooppunten

Configureer ook de VPN 512management interface om out-of-band management toegang tot de controller mogelijk te maken.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Optionele configuratie:

- U kunt verwijzen naar de configuraties van uw bestaande controller en als de hier vermelde configuratie aanwezig is, kunt u deze configuratie toevoegen aan de nieuwe controllers.
- Configureer het controleprotocol alleen als TLS als routers verplicht zijn om beveiligde controleverbindingen met de vManage-knooppunten tot stand te brengen met behulp van TLS. Standaard maken alle controllers en routers een controleverbinding met behulp van DTLS. Dit is een optionele configuratie die alleen vereist is voor vSmart- en vManage-knooppunten, afhankelijk van uw vereisten.

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

Serviceinterface configureren op alle vManage-knooppunten

Configureer de service-interface op alle vManagenodes, inclusief vManage-1, die al aan boord is.

Deze interface wordt gebruikt voor clustercommunicatie, wat communicatie tussen de vManagenodes in het cluster betekent.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Zorg ervoor dat hetzelfde IP-subnet wordt gebruikt voor de service-interface voor alle knooppunten in het vManagecluster.

Clusterreferenties configureren

We kunnen dezelfde beheerdersreferenties van de vManageodes gebruiken om het vManagecluster te configureren. Anders kunnen we een nieuwe gebruikersreferentie configureren die deel uitmaakt van netadminggroup. De configuraties voor het configureren van nieuwe gebruikersreferenties worden weergegeven

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

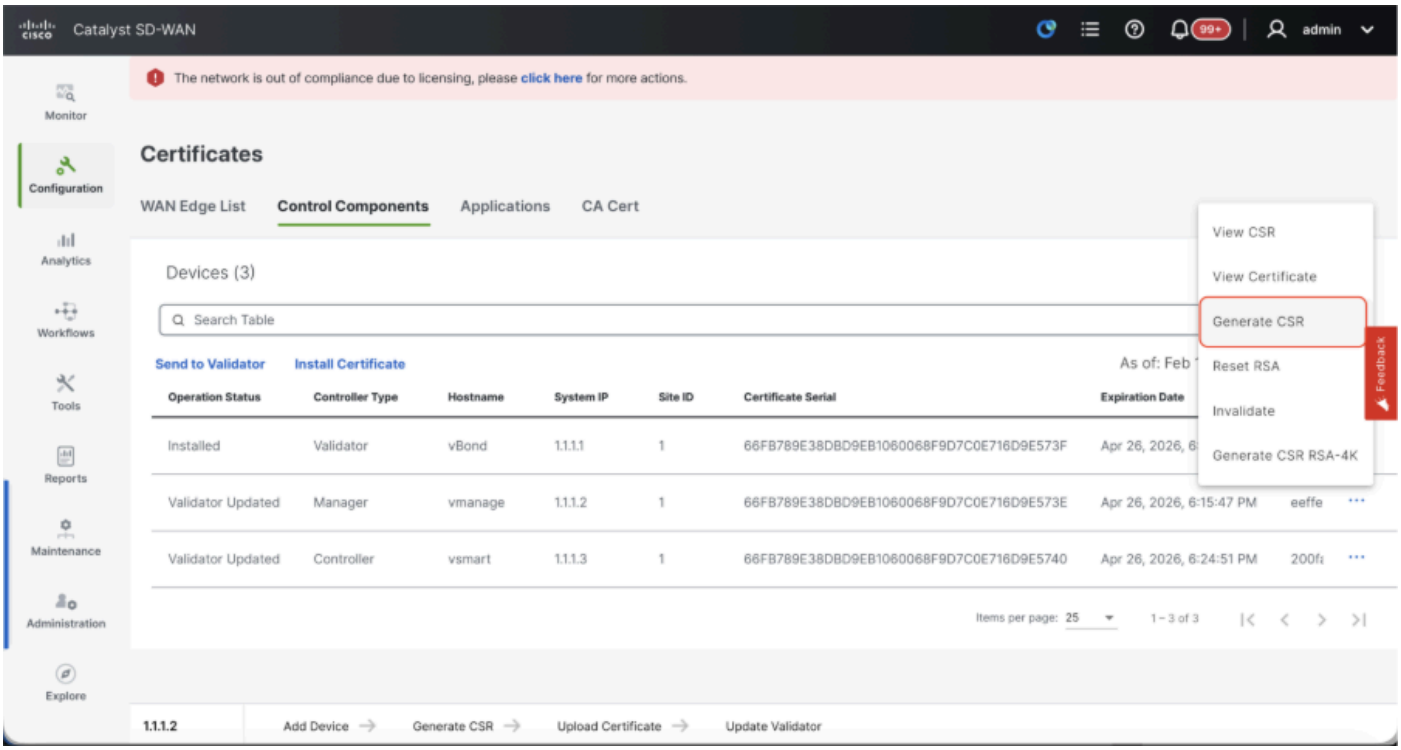
Zorg ervoor dat u dezelfde gebruikersreferenties configureert voor alle vManagenodes die deel uitmaken van het cluster. Als we besluiten beheerdersreferenties te gebruiken, moet het dezelfde

gebruikersnaam/wachtwoord zijn voor alle vManagenodes.

Apparaatcertificaat installeren op alle vManage-knooppunten

- Meld u aan bij vManageUI van alle vManagenodes met behulp van de URL https://<vmanage-ip>in uw browser. Gebruik het VPN 512 IP-adres van de respectievelijke vManagenodes. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

  Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.

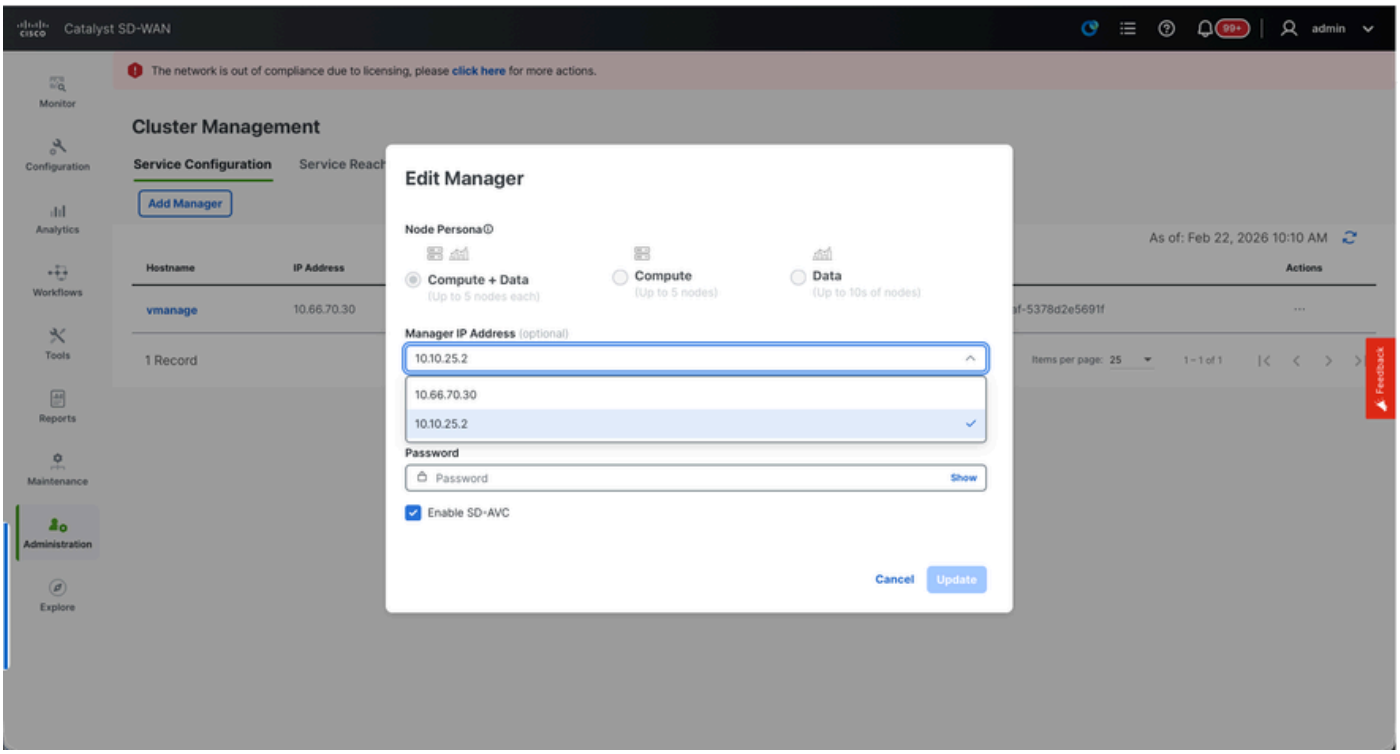
- Voltooi deze stap voor alle vManage-knooppunten die deel uitmaken van het cluster.

Klaar om het vManage-cluster te bouwen

- Navigeer op de webUI van vManage-1 naar Beheer > Clusterbeheer, klik op ... onder Acties voor vManage-1, kies Bewerken.
- De nodepersona wordt automatisch gekozen op basis van de persona die we hebben gekozen terwijl de VM werd aangemaakt.

Opmerking: voor een cluster met drie knooppunten worden alle drie vManage-knooppunten met compute+data als persona weergegeven.

- Voor een cluster met 6 knooppunten worden 3 vManage-knooppunten met compute+data opgevoed, terwijl de persona en 3 vManage-knooppunten met data als persona worden opgevoed.
- Zorg ervoor dat u in de vervolgkeuzelijst voor IP-adres van Manager serviceinterface IP van vManage kiest.

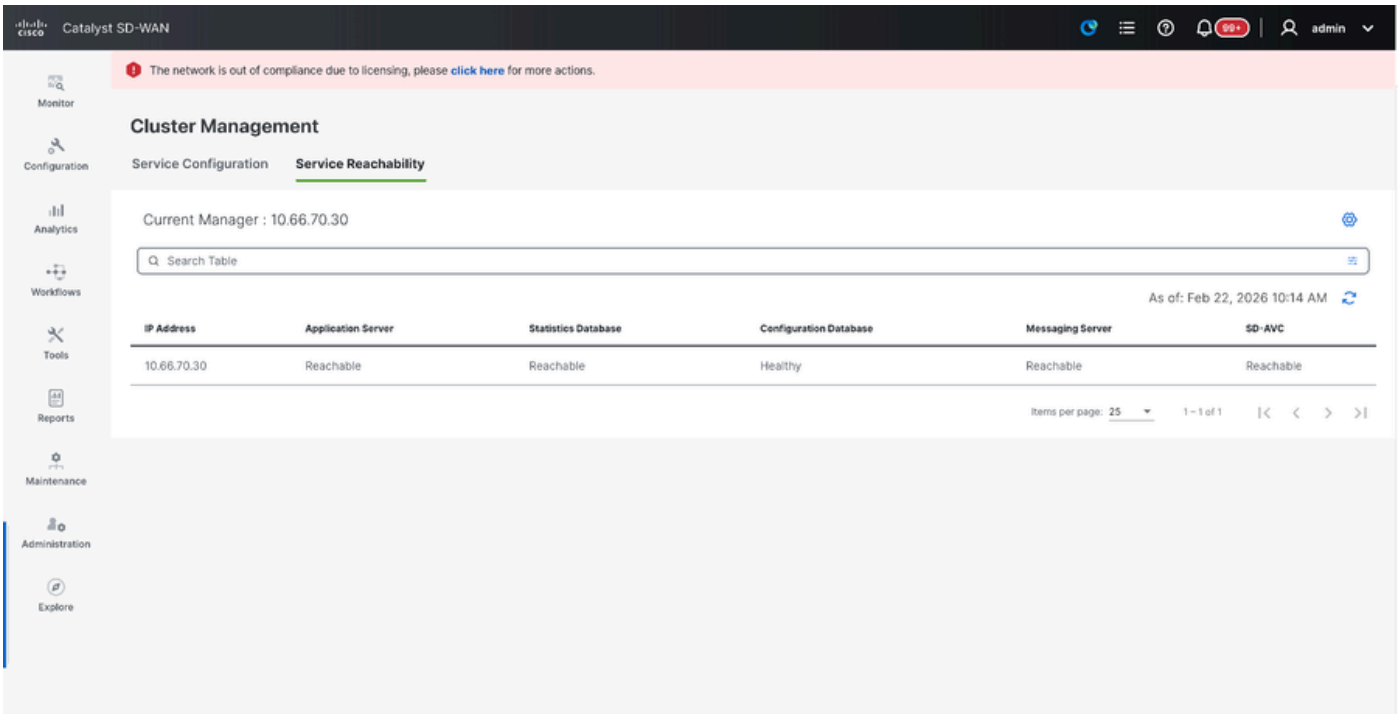


- Voer de gebruikersnaam en het wachtwoord in die we willen gebruiken om vManage-cluster in te schakelen. Dit wordt clusterreferenties genoemd.
- Zoals eerder vermeld, moeten dezelfde referenties worden geconfigureerd op alle vManage-knooppunten en moeten deze worden gebruikt terwijl alle knooppunten aan het cluster worden toegevoegd.

Opmerking: raadpleeg deze configuratie in uw bestaande cluster om SDAVC in te schakelen. U hoeft alleen te worden gecontroleerd als dit vereist is en alleen op één vManage-node van het cluster nodig is.

Klik op Update.

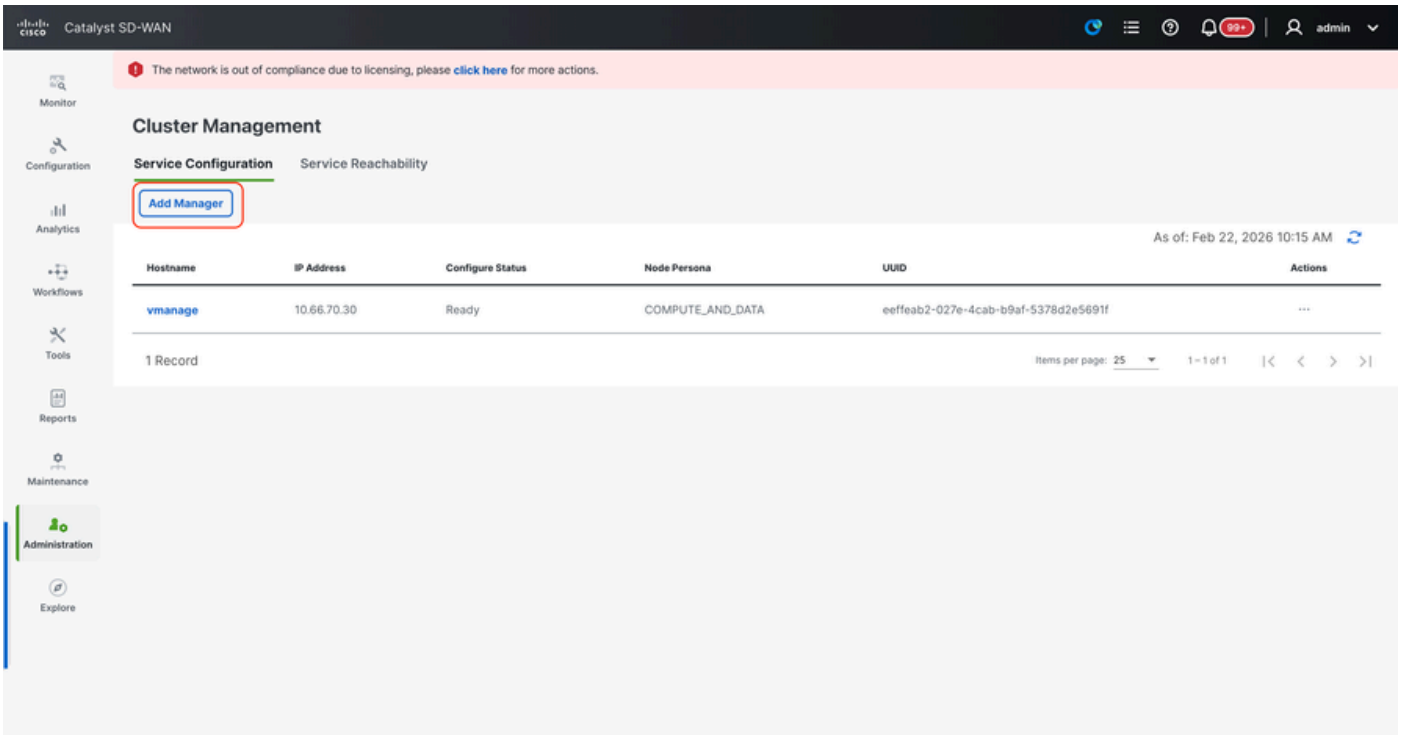
- Na dit bericht start de vManage NMS-services opnieuw op de achtergrond op en is de gebruikersinterface gedurende een paar minuten van ongeveer 5 tot 10 minuten niet beschikbaar. Gedurende deze periode is CLI-toegang van vManage beschikbaar.
- Zodra de vManage-1 UI toegankelijk is, navigeert u naar Beheer > Clusterbeheer en zorgt u ervoor dat de serviceinterface van IP vManage wordt weergegeven onder IP-adres,De status configureren is gereed en de nodepersona wordt correct weergegeven.
- Switch naar service bereikbaarheid sectie op dezelfde pagina en zorg ervoor dat alle diensten bereikbaar zijn.

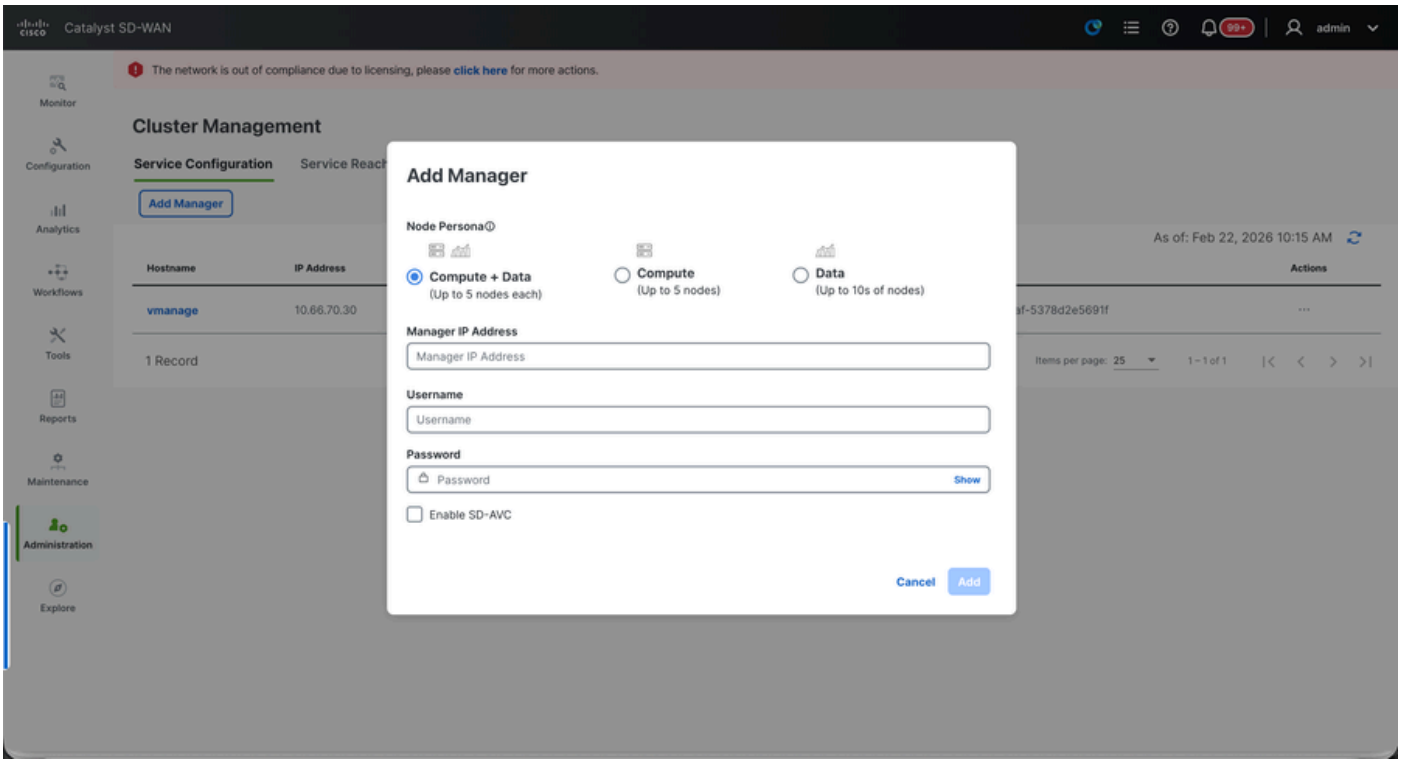


- Als we zien dat een van de services nog niet bereikbaar is, wacht dan even. Meestal duurt het ongeveer 20 tot 30 minuten.

Bouw het vManage-cluster

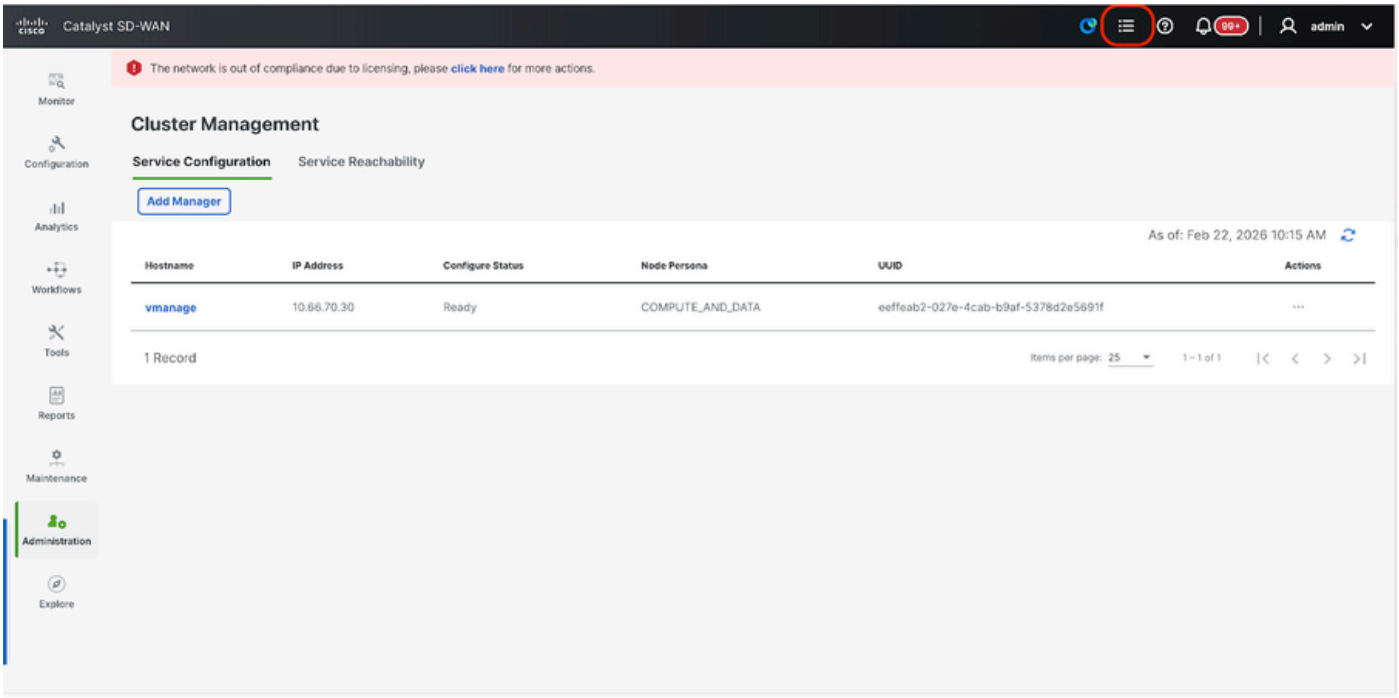
- Navigeer op de webUI van vManage-1 naar Beheer > Clusterbeheer, in de sectie Serviceconfiguratie,
- Klik op Add Manager, er verschijnt een pop-upvenster:





- Kies de Node-persona op basis van de persona-configuraties die zijn uitgevoerd terwijl de vManage – 2-node werd gesponnen.
- Voer de serviceinterface van IP vManage-2 in onder IP-adres voor beheer
- Voer de gebruikersnaam en het wachtwoord in, dat dezelfde referenties zijn als die we in stap 6 hebben gebruikt.
- Schakel SDAVC in - Wordt niet aangevinkt omdat we het al op vManage-1 zouden hebben ingeschakeld
- Klik op Toevoegen.
- Nadat u dit bericht hebt geplaatst, start de vManage NMS-services opnieuw op de

achtergrond voor vManage 1- en 2-knooppunten. De gebruikersinterface is niet beschikbaar voor een paar minuten van ongeveer 5 tot 10 minuten voor vManage 1 en 2.
- Gedurende deze periode is CLI-toegang van vManage 1 en 2 beschikbaar.
- Zodra de vManage-1 UI toegankelijk is, navigeert u naar Beheer > Clusterbeheer, zorgt u ervoor dat de IP-serviceinterface van zowel vManage wordt weergegeven onder IP-adres, Configuratiestatus is gereed en nodepersona correct wordt weergegeven.
- Switch-naar-service bereikbaarheid gedeelte op dezelfde pagina en zorg ervoor dat alle services bereikbaar zijn voor zowel de vManage-knooppunten.
- Als we zien dat een van de services nog niet bereikbaar is, wacht dan even. Meestal duurt het ongeveer 5 tot 10 minuten.
- U kunt de status van het proces voor het toevoegen van clusters controleren in de takenlijst die beschikbaar is in de rechterbovenhoek van de vManage-gebruikersinterface.



- U kunt opzoeken naar de actieve takenlijst en als de taak nog steeds wordt vermeld onder de actieve takenlijst, geeft dit aan dat de taak nog niet is voltooid.
- U kunt op de taak klikken om de voortgang van hetzelfde te controleren. Als de taak niet wordt vermeld onder de lijst Actieve taken, switch dan naar Voltooid en zorg ervoor dat de taak succesvol is afgerond.
- Pas nadat deze punten zijn gevalideerd, gaat u verder met de volgende stap.

Met deze punten moet rekening worden gehouden voordat het volgende knooppunt aan het cluster wordt toegevoegd:

Controleer deze punten op alle UI's van de vManage-knooppunten die tot nu toe aan het cluster zijn toegevoegd:

- Navigeer naar Monitor > Overzicht van de vManage-gebruikersinterface en zorg ervoor dat het aantal vManage-knooppunten correct wordt weergegeven en bereikbaar is, afhankelijk van het aantal knooppunten dat aan het cluster is toegevoegd.

- Navigeer naar Beheer > Clusterbeheer en zorg ervoor dat de IP-serviceinterface van zowel vManage wordt weergegeven onder IP-adres, Configuratiestatus is gereed en nodepersona correct wordt weergegeven.
- Switch-naar-service bereikbaarheid gedeelte op dezelfde pagina en zorg ervoor dat alle services bereikbaar zijn voor zowel de vManage-knooppunten.

- Telkens wanneer een node aan het cluster wordt toegevoegd, worden de NMS-services van alle nodes in het cluster opnieuw gestart, waardoor de UI van al die nodes enige tijd onbereikbaar wordt.
- Afhankelijk van het aantal knooppunten in het cluster kan het langer duren voordat de gebruikersinterface een back-up heeft gemaakt en alle services bereikbaar zijn.
- U kunt de taak controleren onder Taaklijst die beschikbaar is in de rechterbovenhoek van de vManage UI.
- Op de vManage UI van elk knooppunt dat aan het cluster is toegevoegd, moeten we alle routers, sjablonen en beleidsregels zien als ze beschikbaar waren in vManage-1.
- Als die configuraties niet aanwezig waren op vManage-1, moeten de vBonds- en vSmarts-configuraties die zijn toegevoegd aan vManage-1 en ook de configuraties Beheer > Instellingen voor Organisatienaam, vBond, Certificaatautorisatie worden weergegeven op de rest van de vManage-knooppunten die aan het cluster zijn toegevoegd.
- Herhaal dezelfde stappen voor de overige vManage-knooppunten.

Als alle controllers zijn geïnstalleerd, voert u deze stap uit:

Stap 4: Config-DB Backup/Restore

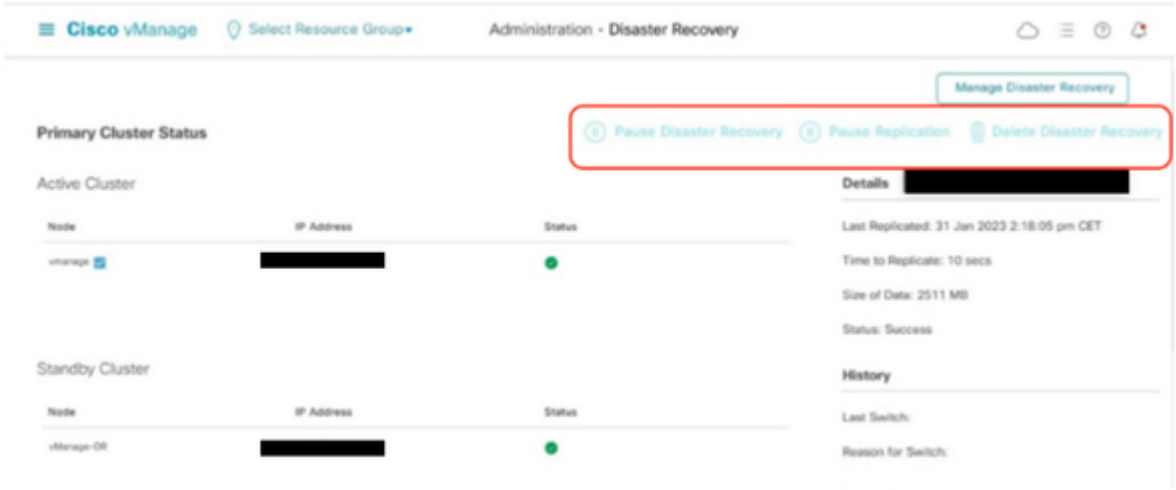
Configuratie-db-back-up en terugzetbewerkingen op een andere vManage-node verzamelen

---

Opmerking: Als u back-ups van de configuratiedatabase verzamelt van het bestaande vManage-cluster waarvoor Disaster Recovery is ingeschakeld, moet u ervoor zorgen dat deze worden verzameld nadat de Disaster Recovery op die node is gepauzeerd en verwijderd.

Bevestig dat er geen doorlopende Disaster Recovery-replicatie is. Navigeer naar Beheer > Disaster Recovery en Zorg ervoor dat de status Succesvol is en niet in een tijdelijke staat zoals Import Pending, Export Pending of Download Pending. Als de status niet succesvol is, neemt u contact op met Cisco TAC en zorgt u ervoor dat replicatie succesvol is voordat u doorgaat met het pauzeren van de Disaster Recovery.

Pauzeer eerst de Disaster Recovery en zorg ervoor dat de taak is voltooid. Verwijder vervolgens de Disaster Recovery en bevestig dat de taak is voltooid.



Neem contact op met Cisco TAC om ervoor te zorgen dat de Disaster Recovery met succes wordt opgeruimd.

Configuratie-DB-back-up verzamelen:

- In de SD-WAN-fabric die momenteel wordt gebruikt, kunt u configuratie-db-back-up genereren vanuit het vManage-cluster.
- Houd er rekening mee dat we configuratie-db-back-up alleen moeten genereren op één node van het vManage-cluster, die de configuratie-db-leider is.

- Voor standalone vManage is dat vManage zelf de leider op het gebied van configuratie-db.
- Identificeer in het vManage-cluster de configuratie-db-leiderknooppunt met behulp van de diagnostiek command request nms configuration-db.U kunt deze opdracht uitvoeren op alle knooppunten van het vManage-cluster met drie knooppunten.
- In een cluster met 6 knooppunten moet u deze opdracht uitvoeren op de vManage-knooppunten waar configuratie-db is ingeschakeld om de leader-node te identificeren. Navigeer naar Beheer > Clusterbeheer om hetzelfde te controleren:
- Zoals we in de schermafbeelding zien, hebben de knooppunten die zijn geconfigureerd met persona COMPUTE_AND_DATA configuratie-db uitgevoerd.

U kunt hetzelfde controleren met de opdracht requestNmsconfiguration-dbstatus op vManageCLI. De output is zoals getoond

```
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#
```

- Zodra u het commando uitvoertVraag NMS Configuration-DB Diagnostics aan op deze knooppunten, de uitvoer is als volgt:

- Zoek naar het gemarkeerde veld voor "IsLeader". Als het is ingesteld op 1, geeft dit aan dat node de leader node is en we kunnen daar configuratie-db back-up van verzamelen.

```
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     .
```

Gebruik deze opdracht om de configuratie-db-back-up te verzamelen van de geïdentificeerde configuratie-db leader vManage-node.

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

De verwachte output is als volgt:

```
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#
```

- Noteer de configuratie-db-referenties als deze is bijgewerkt.
- Als u de configuratie-db-referenties niet kent, neemt u contact op met TAC om de configuratie-db-referenties op te halen uit de bestaande vManage-knooppunten.
- Standaardconfiguratie-db-referenties zijn gebruikersnaam: neo4j en wachtwoord: wachtwoord

Configuration-db Backup terugzetten naar een andere vManage-node

Kopieer de configuratie-db back-up naar /home/admin/ directory van vManage met behulp van SCP.

Voorbeeld van scp-opdrachtuitvoer:

```
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
```

Om de configuratie-db back-up te herstellen, moeten we eerst de configuratie-db referenties configureren. Als uw configuratie-db-referenties standaard zijn (neo4j / wachtwoord), kunnen we deze stap overslaan.

Als u configuratie-db-referenties wilt configureren, gebruikt u de opdracht request nms configuration-db update-admin-user. Gebruik de gebruikersnaam en het wachtwoord van uw keuze.

Houd er rekening mee dat de toepassingsserver van vManage opnieuw wordt gestart. Hierdoor wordt de gebruikersinterface van vManage korte tijd ontoegankelijk.

```
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#
```

Post waarin we kunnen doorgaan met het herstellen van de configuratie-db back-up:

We kunnen de opdracht request nms configuration-db restore path /home/admin/< > gebruiken om de configuratie-db te herstellen naar de nieuwe vManage:

```
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
```

Zodra de configuratie-db is hersteld, moet u ervoor zorgen dat de vManage UI toegankelijk is. Wacht ongeveer 5 minuten en probeer vervolgens toegang te krijgen tot de gebruikersinterface.

Als u eenmaal met succes bent ingelogd op de gebruikersinterface, moet u ervoor zorgen dat de lijst met Edge-routers, het sjabloon, het beleid en alle andere configuraties die aanwezig waren op uw vorige of bestaande vManage-gebruikersinterface, worden weergegeven in de nieuwe vManage-gebruikersinterface.

Stap 5: Reauthenticatie van controllers en ongeldigverklaring van oude controllers

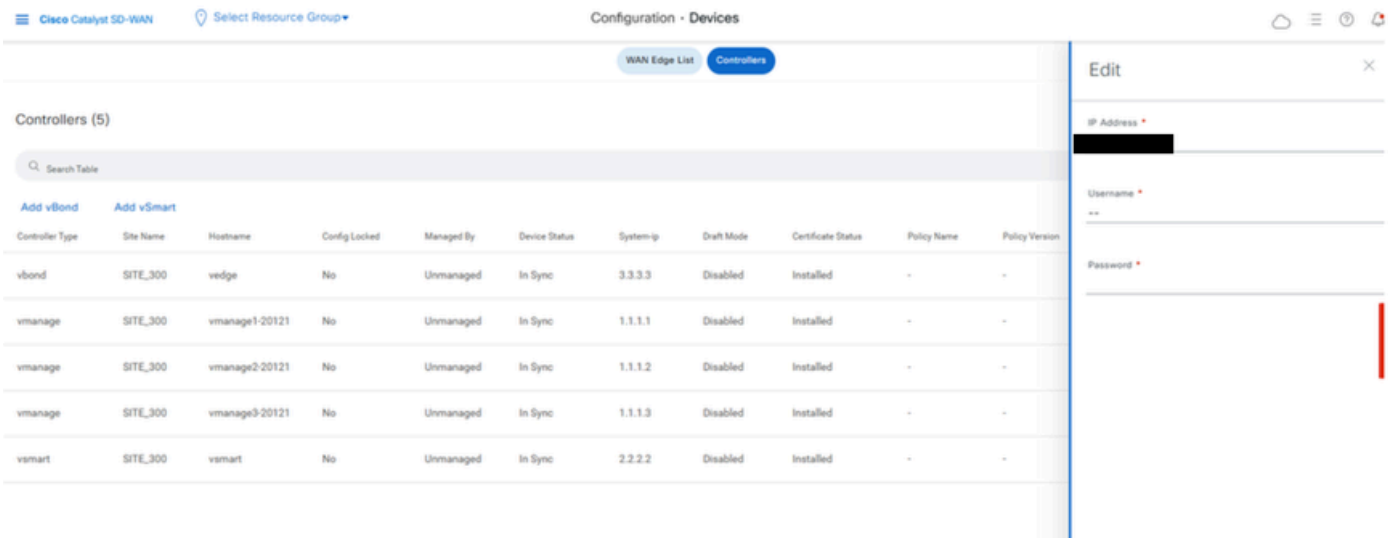
Zodra configuratie-db is hersteld, moeten we alle nieuwe controllers (vmanage/vsmart/vbond) in de fabric opnieuw verifiëren

---

Opmerking: Als de IP-interface die wordt gebruikt om opnieuw te verifiëren de tunnelinterface IP is, moet u ervoor zorgen dat de NETCONF-service is toegestaan op de tunnelinterface van de vManage, vSmart en vBond en ook op de firewalls langs het pad. De firewallpoort die moet worden geopend is TCP-poort 830 als bidirectionele regel van DR-cluster naar alle vBonds en vSmarts.

Klik in vmanage UI op Configuration > Devices > Controllers

- Klik op de drie puntjes bij elke controller en klik op Bewerken



- Vervang het ip-adres (system-ip van de controller) door het transport vpn 0 (tunnel interface)

ip-adres .Voer de gebruikersnaam en het wachtwoord in en klik op opslaan
- Doe hetzelfde voor alle nieuwe controllers in de stof

Synchroniseer de Root-cert-keten

Als alle controllers zijn geïnstalleerd, voert u deze stap uit:

Voer op elke Cisco SD-WAN Manager-server in het nieuw actieve cluster de volgende acties uit:

Voer deze opdracht in om het rootcertificaat te synchroniseren met alle Cisco Catalyst SD-WAN-apparaten in het nieuw actieve cluster:

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

Voer deze opdracht in om de Cisco SD-WAN Manager UUID te synchroniseren met de Cisco SD-WAN Validator:

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

Zodra de fabric is hersteld en de controle- en bfd-sessies zijn ingesteld voor alle randen en controllers in de fabric, moeten we de oude controllers (vmanage/vsmart/vbond) van de gebruikersinterface ongeldig maken

- Klik op Configuratie > Apparaten > Certificaten in vmanage UI
- Klik op Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Ongeldig maken
- Klik op verzenden naar vbond
- Klik in vmanage UI op Configuration > Devices > Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Verwijderen.

Stap 6: Controles achteraf

Opmerking: ga verder met het gedeelte Controles achteraf dat hier wordt weergegeven en dat voor alle implementatiecombinaties geldt.

Combinatie 4: vManage Cluster + Manual/Cold Standby DR

Wat is Manual/Cold Standby DR? De back-up van de SD-WAN Manager-server of het SD-WAN Manager-cluster wordt in koude stand-bytoestand afgesloten.

Regelmatige back-ups van de actieve database worden gemaakt en als de primaire SD-WAN Manager of SD-WAN Manager-cluster uitvalt, wordt de stand-by SD-WAN Manager of SD-WAN Manager-cluster handmatig naar boven gebracht en wordt de back-updatabase hersteld.

Benodigde gevallen:

- 3 of 6 vManage (primair cluster)
- 3 of 6 vManage (DR standby-cluster)
- 1 of meer vBond (verdeeld over primaire en DR-datacenters)
- 1 of meer vSmart (verdeeld over primaire en NH-datacenters)

Stappen:

1. Alle instanties weergeven met de gemeenschappelijke stappen
2. Voorcontroles
3. Configureren van vManage UI, certificaten en onboard controllers
4. vManage-cluster samenstellen
5. Cold Standby DR-clusterconfiguratie
6. Config-db back-up/terugzetbewerking
7. Controles achteraf

Stap 1: Controles vooraf

- Zorg ervoor dat het aantal actieve Cisco SD-WAN Managerinstances gelijk is aan het aantal nieuw geïnstalleerde Cisco SD-WAN Managerinstances.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties dezelfde softwareversie uitvoeren.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties het IP-beheeradres van de Cisco SD-WAN Validator kunnen bereiken.
- Controleer of certificaten zijn geïnstalleerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties.
- Zorg ervoor dat de klokken op alle Cisco Catalyst SD-WAN-apparaten, inclusief de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, worden gesynchroniseerd.
- Zorg ervoor dat een nieuwe set van systeem-IP's en site-ID's is geconfigureerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, samen met dezelfde basisconfiguratie als het actieve cluster.

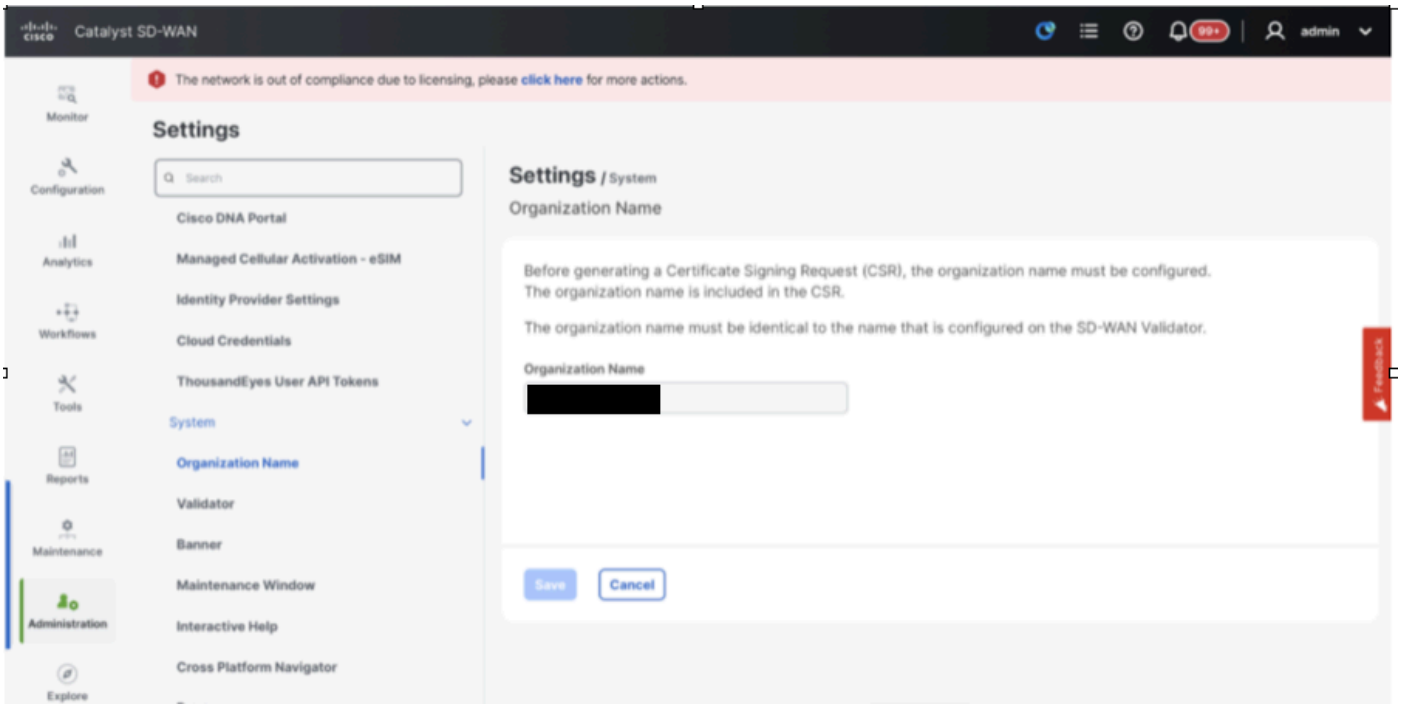
Stap 2: vManage UI, certificaten en ingebouwde controllers configureren

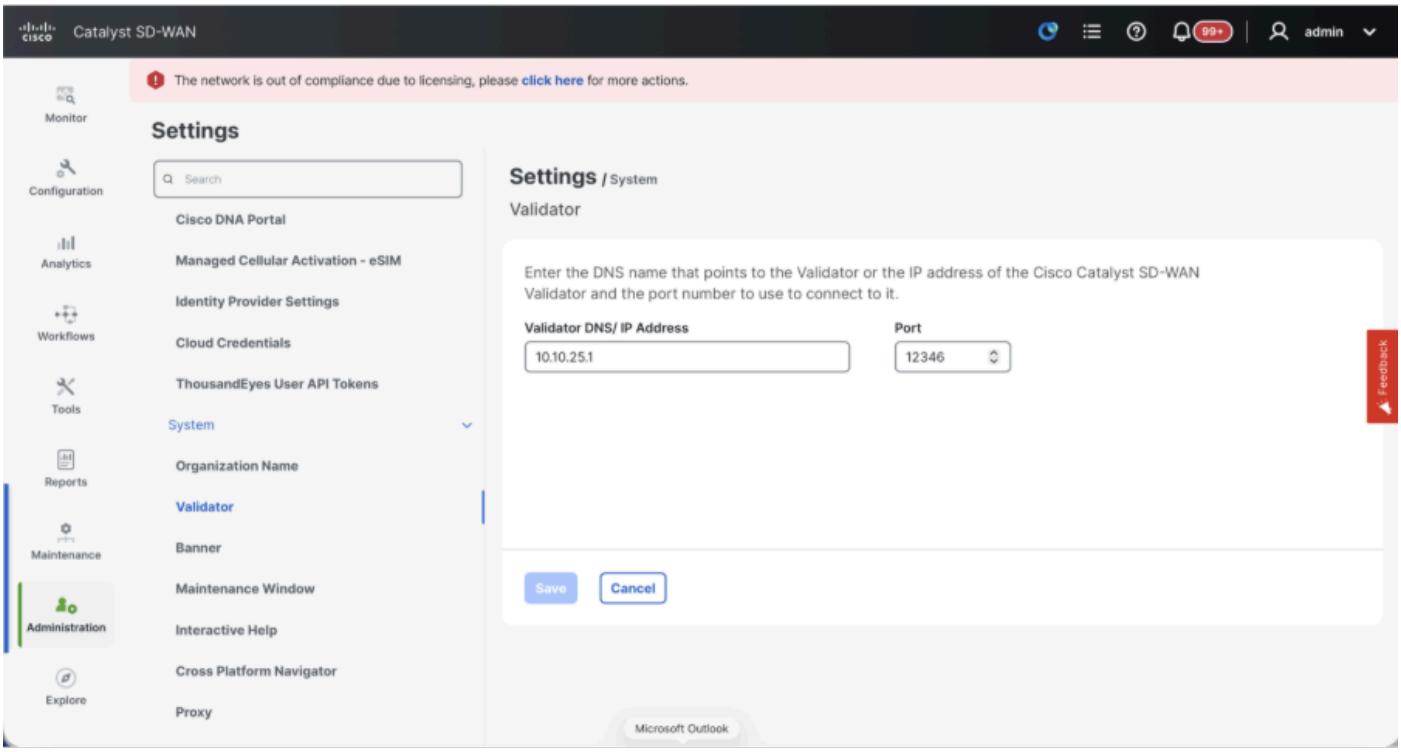
De configuraties op de vManage-gebruikersinterface bijwerken

- Zodra de configuraties in stap 1 zijn toegevoegd aan de CLI van alle controllers, hebben we toegang tot de webUI van vManage, met behulp van de URL https://<vmanage-ip> in uw browser. Gebruik het VPN 512 IP-adres van de respectieve vManage-knooppunten. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Beheer > Instellingen en voer deze stappen uit.
- Configureer de naam van de organisatie en het URL/IP-adres van de validator/vBond.

Configureer dezelfde waarde als in de CLI van de vManage-node.

- In vManage 20.15/20.18 zijn deze configuraties beschikbaar onder de sectie Systeem.



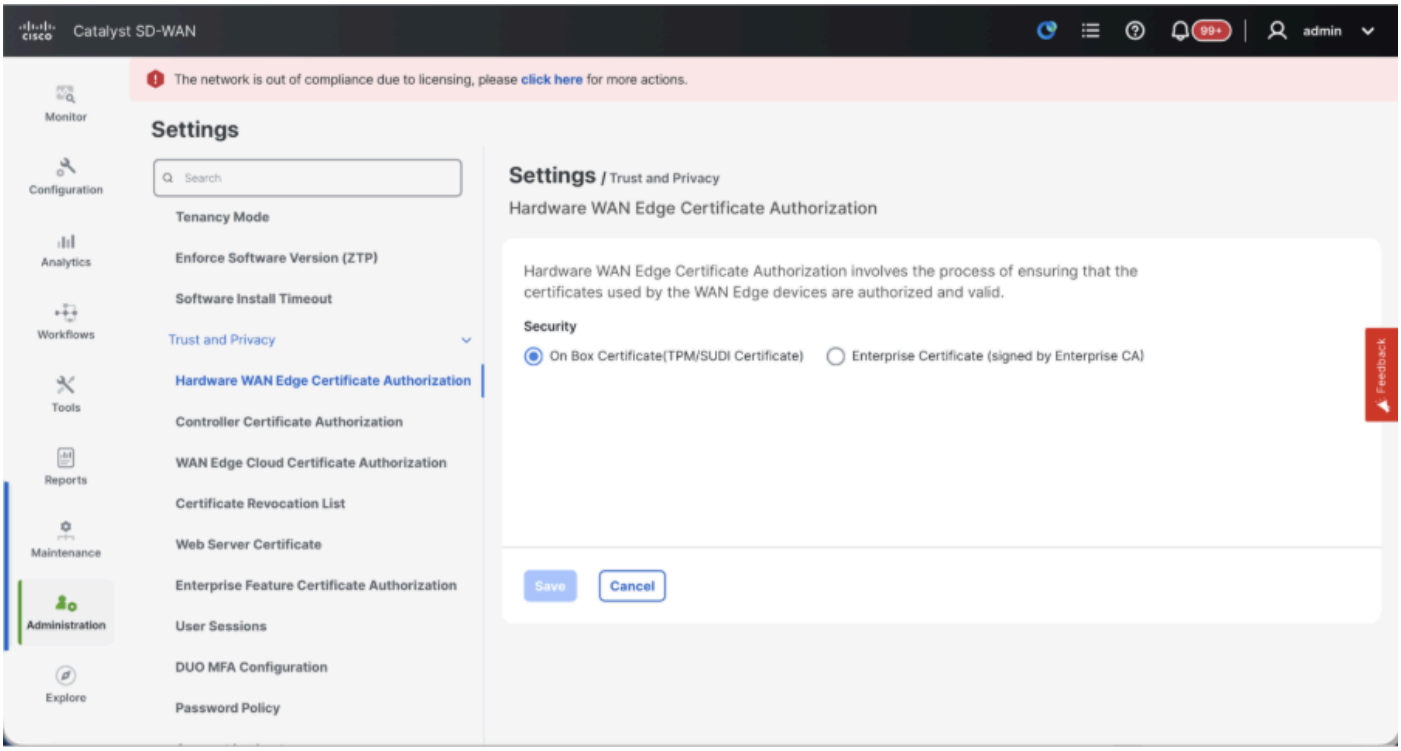


- Controleer de configuraties voor Certificaatautorisatie (CA), die bepaalt welke Certificaatautoriteit wordt gebruikt voor het ondertekenen van de certificaten. We zien daar 3 mogelijkheden:

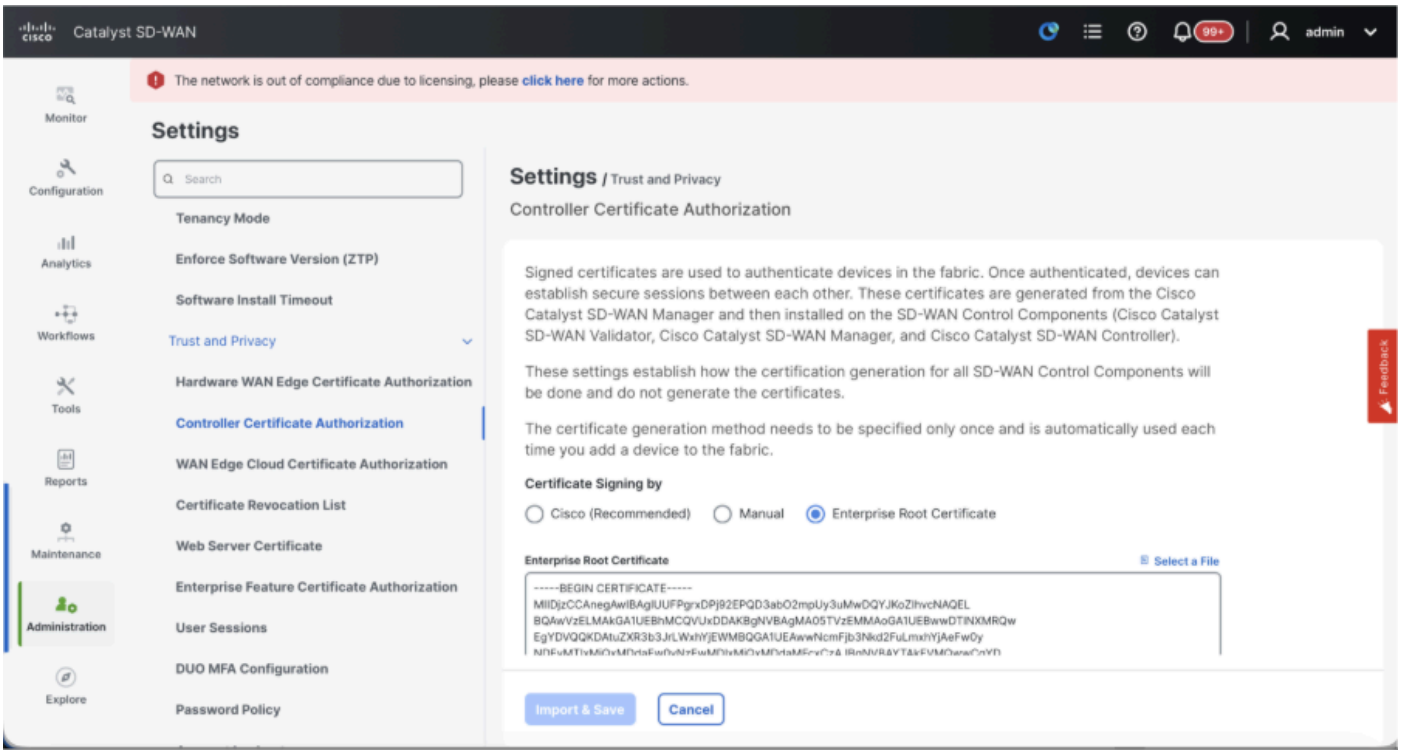
1. Hardware WAN Edge Certificate Authorization - Bepaalt de CA voor hardware SD-WAN Edge-routers.
    - On Box Certificate (TPM/SUDI-certificaat) - Met deze optie wordt het vooraf geïnstalleerde certificaat op de hardware van de router gebruikt om de

Controleverbindingen (TLS/DTLS-verbindingen) tot stand te brengen

- Enterprise Certificate (ondertekend door Enterprise CA) - Met deze optie gebruiken de routers certificaten die zijn ondertekend door Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

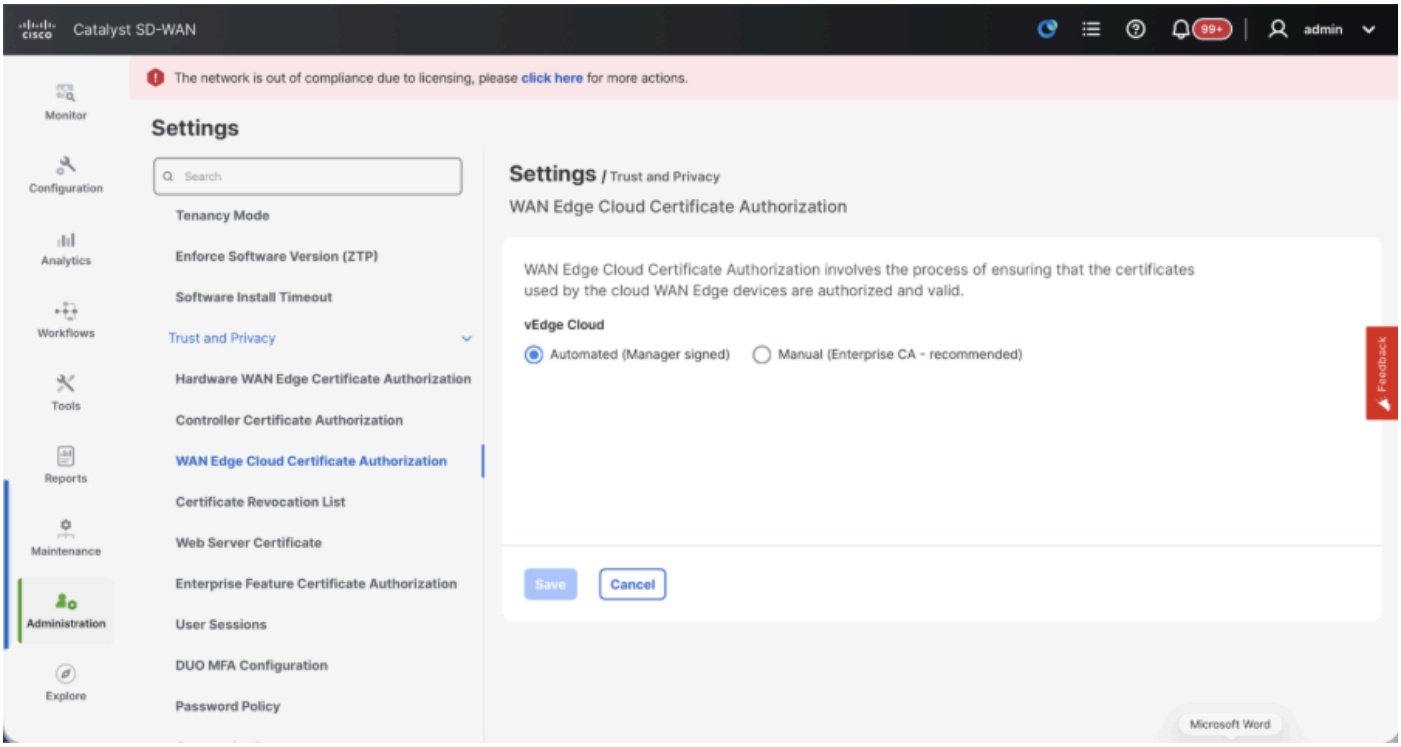


2. Controllercertificaatautorisatie - bepaalt de CA voor SD-WAN-controllers.
    - Cisco (aanbevolen) - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. vManage neemt automatisch contact op met het PNP-portaal met behulp van de referenties voor slimme accounts die zijn geconfigureerd op de vManage en laat het certificaat ondertekenen en installeren op de controller.
    - Handleiding - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. Handmatig ondertekenen van de CSR met behulp van de Cisco PNP portal door te navigeren naar smart account en virtuele account van de respectieve SD-WAN overlay.
    - Enterprise Root Certificate - Met deze optie gebruiken de routers certificaten die zijn ondertekend door de Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

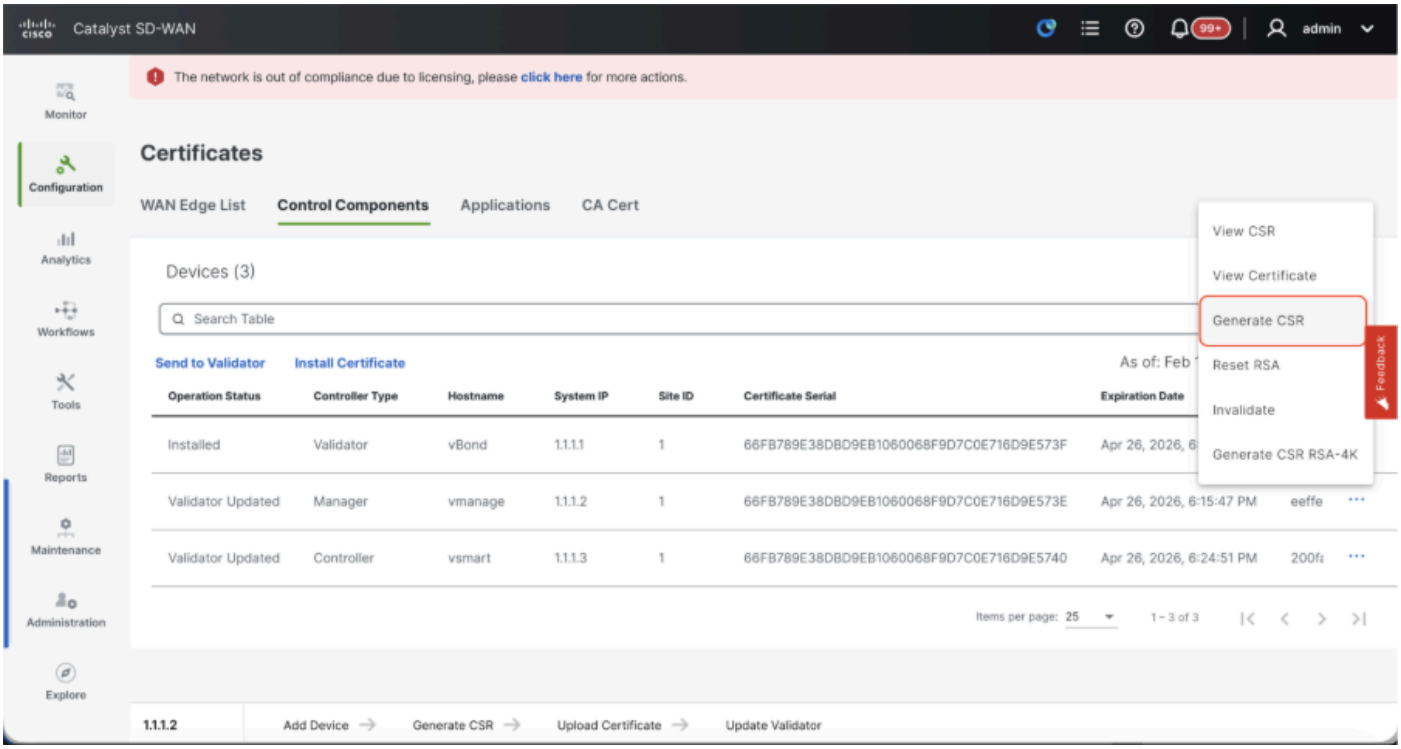


3. WAN Edge Cloud Certificate Authorization - Bepaalt de CA voor virtuele SD-WAN Edge-routers (CSR1000v, C8000v, vEdge cloud)
    - Geautomatiseerd (vManage ondertekend) - vManage ondertekent automatisch de CSR voor de virtuele Edge-routers en installeert het certificaat op de router.
    - Handmatig (Enterprise CA - aanbevolen) - Virtuele routers gebruiken certificaten die zijn ondertekend door de certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

Als we onze eigen CA, Enterprise-certificeringsinstantie, gebruiken, kiest u in dat geval Enterprise.



- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers
- Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

Onboarding vBond/Validator en vSmart/Controller naar de vManage

Navigeer naar Configuratie > Apparaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

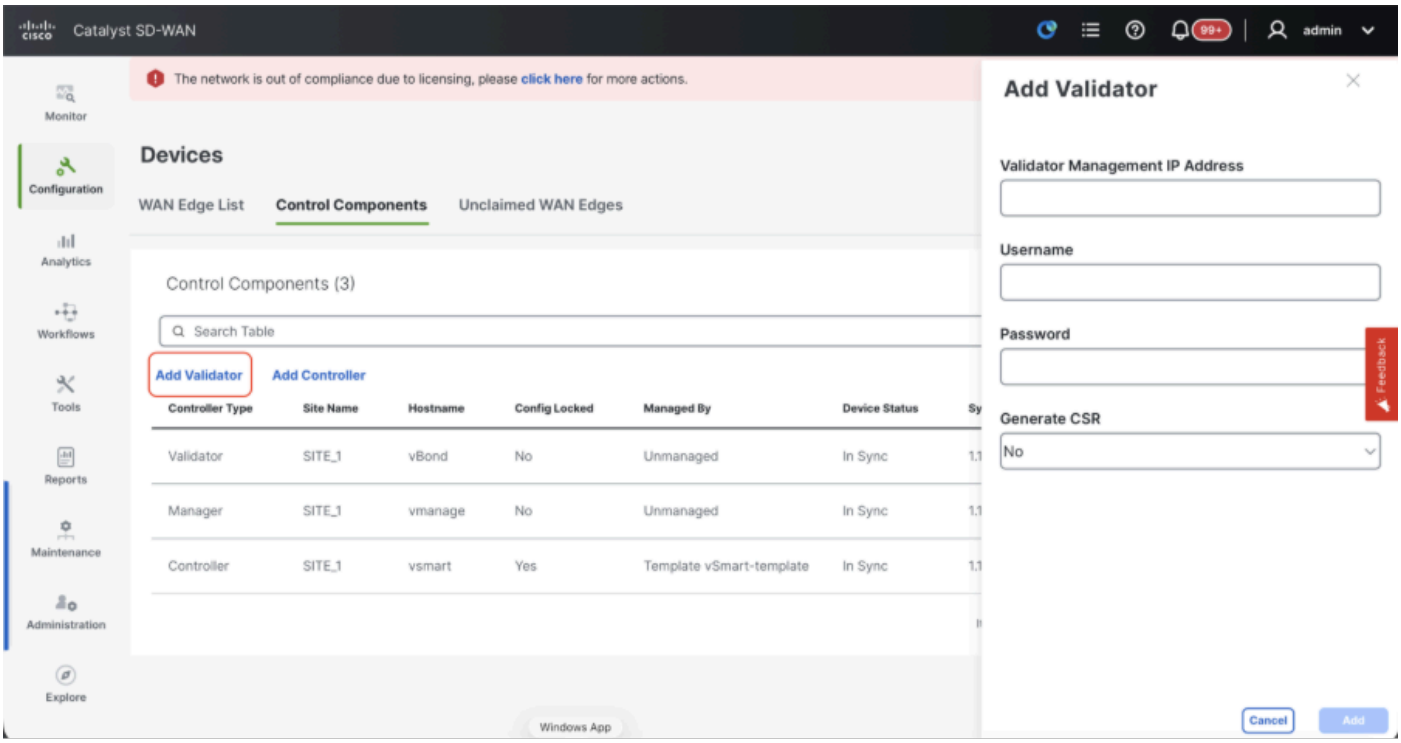
OnboardingVbond/validator

- Klik op AdvBondin geval van 12 .12vManagerValidator toevoegenin geval van 20.15/20.18vManage. Er wordt een pop-upvenster geopend. Voer de VPN 0 transporteert IP

van vBonds dat bereikbaar is vanaf de vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan vanuit de CLI van vManagetovBondIP.
- Voer de gebruikersreferenties van vBond in.

Opmerking: We moeten beheerdersreferenties gebruiken van vBond of een gebruikersonderdeel van netadminggroup. U kunt dit controleren in de CLI van de vBond. Kies Ja in de drop-down van "Genereer CSR" als we een nieuw certificaat voor vBond moeten installeren

Opmerking: Als de vBond zich achter een NAT-apparaat/firewall bevindt, controleert u of de vBond VPN 0-interface IP is vertaald naar een openbaar IP-adres. Als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u het openbare IP-adres van de VPN 0-interface in deze stap



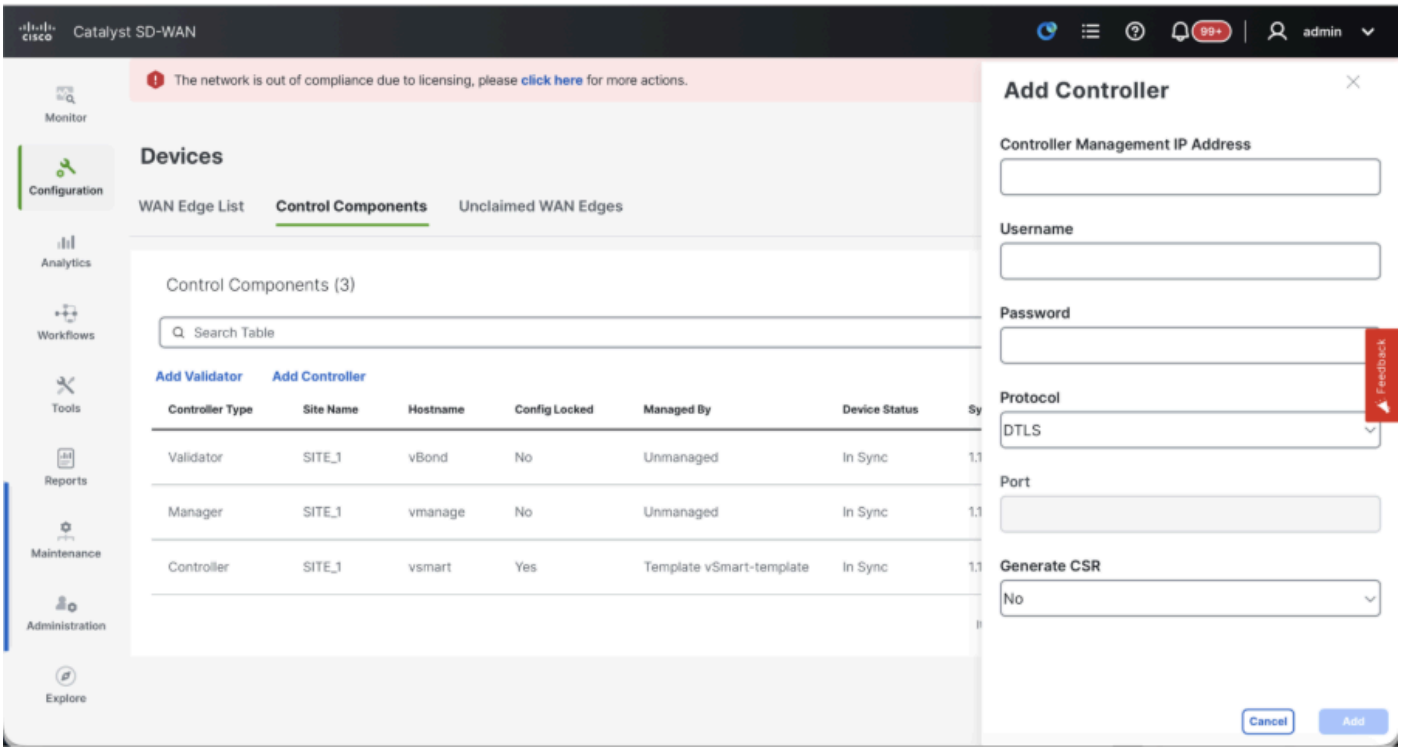
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door de vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vBond geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u

op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vBonds zijn, herhaalt u dezelfde stappen.

Onboarding vSmart/controller:

- Klik op Add vSmart in geval van 10 .12 vManage of Add Controller in geval van 20.15/20.18 vManage.
- Als er een pop-upvenster wordt geopend, voert u het VPN 0-transport IP van vSmart in dat bereikbaar is via vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan van CLI van vManage naar vSmart IP.
- Voer de gebruikersreferenties van vSmart Note in die we nodig hebben om beheerdersreferenties van vSmart of een gebruikersdeel van de netadmin-groep te gebruiken.
- U kunt dit controleren in de CLI van de vSmart.
- Stel het protocol in op TLS als we TLS willen gebruiken voor routers om controleverbindingen met vSmart tot stand te brengen. Deze configuratie moet ook worden geconfigureerd op CLI van vSmarts- en vManage-knooppunten.
- Kies Ja in de keuzelijst "MVO genereren" als we een nieuw certificaat voor vSmart moeten installeren.

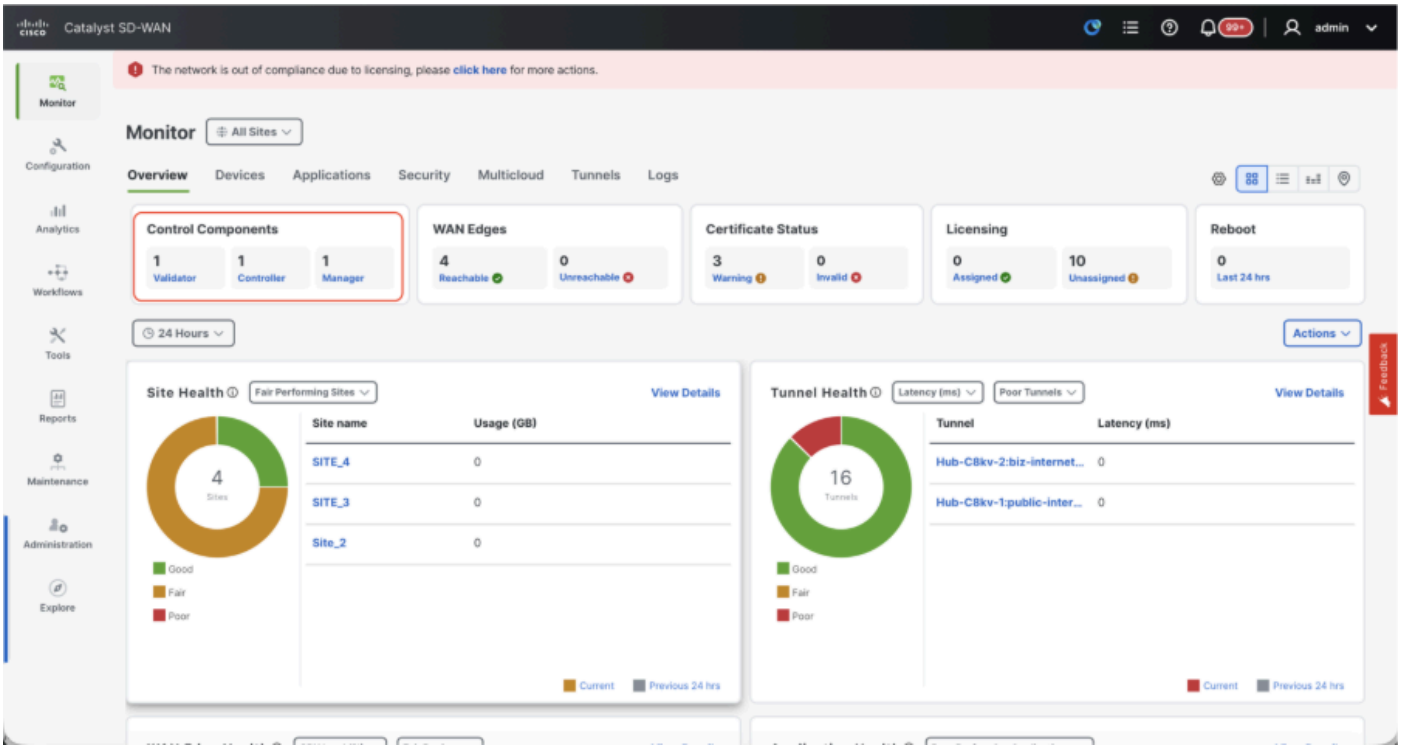
Opmerking: Als de vSmart zich achter NAT-apparaat/firewall bevindt, controleert u of de vSmart VPN 0-interface IP is vertaald naar een openbaar IP-adres en als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u in deze stap het openbare IP-adres van de VPN 0-interface IP.



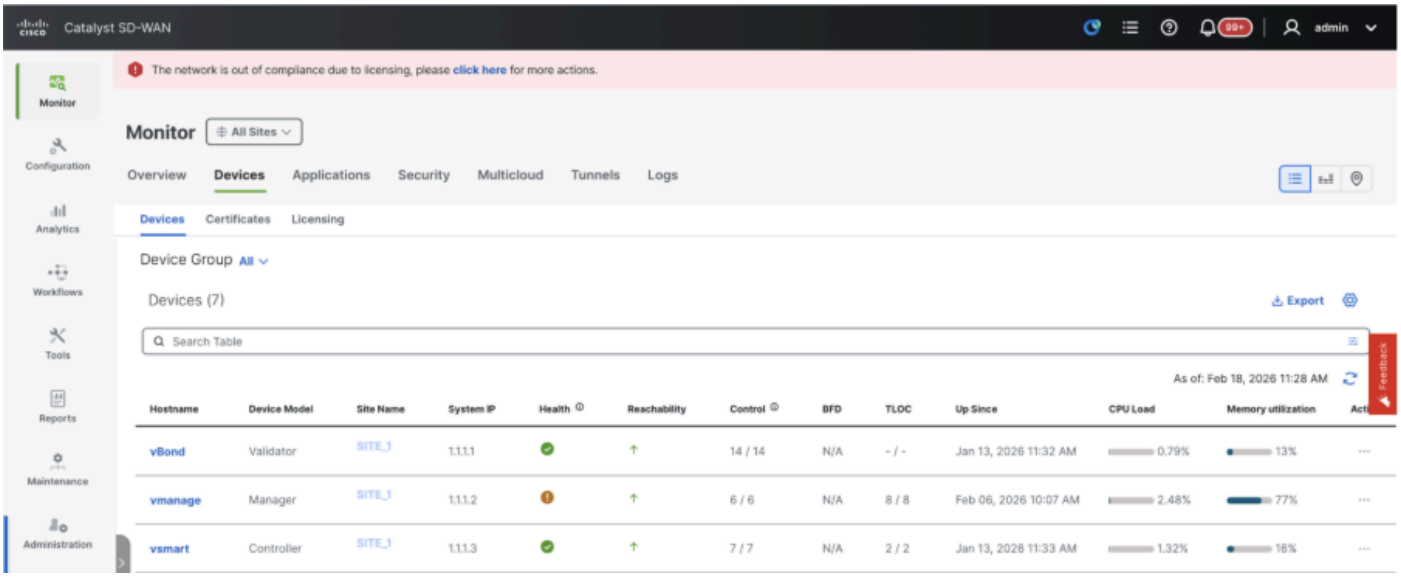
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vSmart geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren.
- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.
- Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vSmarts zijn, herhaalt u dezelfde stappen.

Verificatie

Controleer na voltooiing van alle stappen of alle besturingscomponenten bereikbaar zijn in Monitor>Dashboard



- Klik op de betreffende besturingscomponenten en bevestig dat ze allemaal bereikbaar zijn.
- Navigeer naar Monitor > Apparaten en controleer of alle besturingscomponenten bereikbaar zijn.



Stap 3: vManage-cluster samenstellen

Onboard SD-WAN-verbinding met een vManage-cluster in de SD-WAN-overlay

---

Opmerking: vManage Cluster kan worden geconfigureerd met 3 vManage-knooppunten of 6 vManage-knooppunten, afhankelijk van het aantal sites dat aan boord is van de SD-WAN-verbinding

---

Aan boord van alle SD-WAN-controllers met één vManage-node

Ga verder met de stappen die worden gedeeld in "Onboard SD-WAN-controllers met een enkele node vManage in de SD-WAN-overlay" om eerst de SD-WAN-fabric met één vManage-node en alle vereiste Validators (vBond) en Controllers (vSmart) aan boord te brengen.

De CLI-configuraties configureren van alle vManage-knooppunten die deel uitmaken van het cluster

- De rest van de vManage-knooppunten configureren. In het geval van een cluster met drie knooppunten moet u nog twee knooppunten configureren, in het geval van een cluster met zes knooppunten moet u vijf knooppunten configureren.
- Systeemconfiguraties configureren zoals wordt weergegeven:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Opmerking: Als we URL als vBond-adres gebruiken, moet u de IP-adressen van de DNS-server configureren in VPN 0-configuratie of ervoor zorgen dat deze kunnen worden opgelost.

Deze configuraties zijn nodig om de transportinterface die wordt gebruikt om besturingsverbindingen met de routers en de rest van de controllers tot stand te brengen.

```
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
```

Configureer ook de VPN 512management interface om out-of-band management toegang tot de controller mogelijk te maken.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Optionele configuratie:

- U kunt verwijzen naar de configuraties van uw bestaande controller en als de hier vermelde configuratie aanwezig is, kunt u deze configuratie toevoegen aan de nieuwe controllers.
- Configureer het controleprotocol alleen als TLS als routers verplicht zijn om beveiligde controleverbindingen met de vManage-knooppunten tot stand te brengen met behulp van TLS. Standaard maken alle controllers en routers een controleverbinding met behulp van DTLS. Dit is een optionele configuratie die alleen vereist is voor vSmart- en vManage-knooppunten, afhankelijk van uw vereisten.

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

Serviceinterface configureren op alle vManage-knooppunten

Configureer de service-interface op alle vManagenodes, inclusief vManage-1, die al aan boord is. Deze interface wordt gebruikt voor clustercommunicatie, wat communicatie tussen de vManagenodes in het cluster betekent.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Zorg ervoor dat hetzelfde IP-subnet wordt gebruikt voor de service-interface voor alle knooppunten in het vManagecluster.

Clusterreferenties configureren

We kunnen dezelfde beheerdersreferenties van de vManageodes gebruiken om het vManagecluster te configureren. Anders kunnen we een nieuwe gebruikersreferentie configureren die deel uitmaakt van netadminggroup. De configuraties voor het configureren van nieuwe gebruikersreferenties worden weergegeven

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

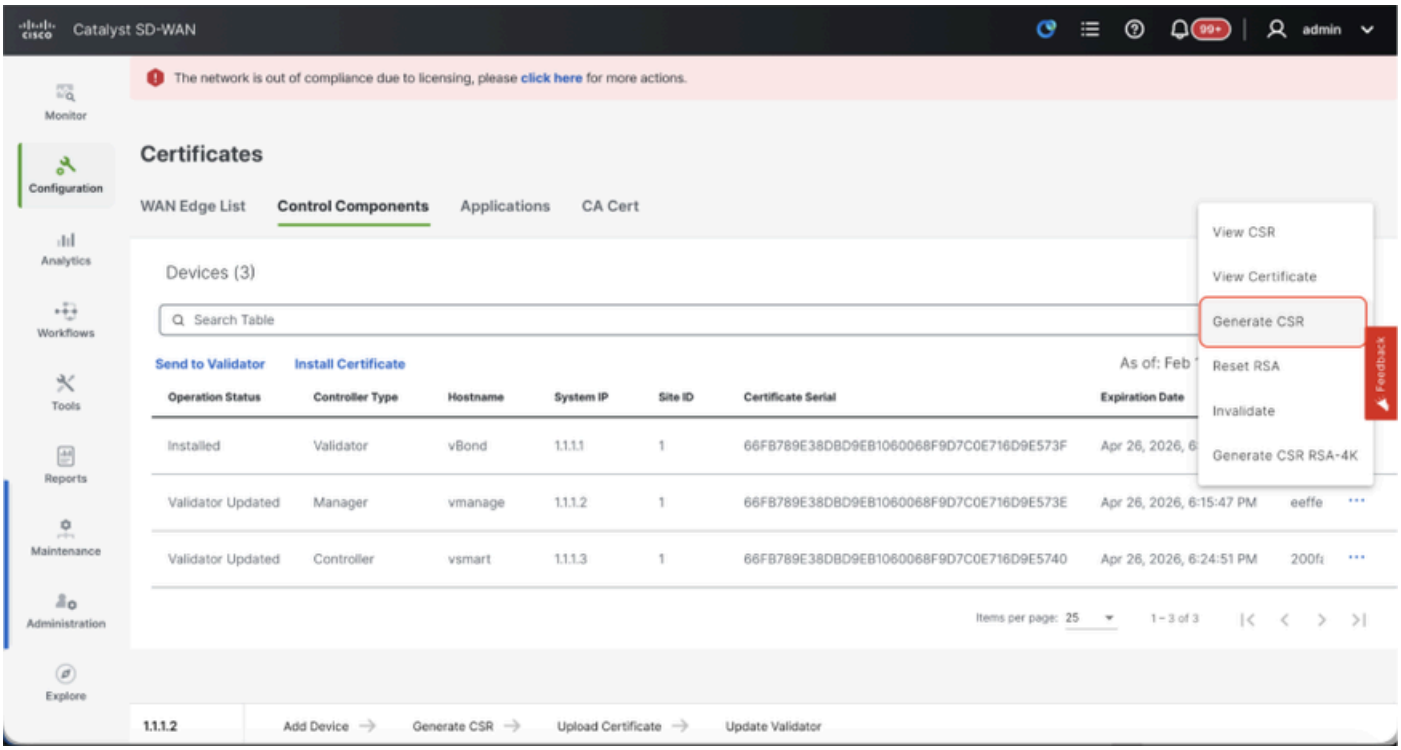
Zorg ervoor dat u dezelfde gebruikersreferenties configureert voor alle vManagenodes die deel uitmaken van het cluster. Als we besluiten beheerdersreferenties te gebruiken, moet het dezelfde gebruikersnaam/wachtwoord zijn voor alle vManagenodes.

Apparaatcertificaat installeren op alle vManage-knooppunten

- Meld u aan bij vManageUI van alle vManagenodes met behulp van de URL https://<vmanage-ip>in uw browser. Gebruik het VPN 512 IP-adres van de respectievelijke vManagenodes. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.

- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

  Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.

- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren.

- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.

- Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

- Voltooi deze stap voor alle vManage-knooppunten die deel uitmaken van het cluster.

Klaar om het vManage-cluster te bouwen

- Navigeer op de webUI van vManage-1 naar Beheer > Clusterbeheer, klik op ... onder Acties voor vManage-1, kies Bewerken.
- De nodepersona wordt automatisch gekozen op basis van de persona die we hebben gekozen terwijl de VM werd aangemaakt.

Opmerking: voor een cluster met drie knooppunten worden alle drie vManage-knooppunten met compute+data als persona weergegeven.

- Voor een cluster met 6 knooppunten worden 3 vManage-knooppunten met compute+data opgevoed, terwijl de persona en 3 vManage-knooppunten met data als persona worden opgevoed.
- Zorg ervoor dat u in de vervolgkeuzelijst voor IP-adres van Manager serviceinterface IP van vManage kiest.
- Voer de gebruikersnaam en het wachtwoord in die we willen gebruiken om vManage-cluster in te schakelen. Dit wordt clusterreferenties genoemd.
- Zoals eerder vermeld, moeten dezelfde referenties worden geconfigureerd op alle vManage-knooppunten en moeten deze worden gebruikt terwijl alle knooppunten aan het cluster worden toegevoegd.

Optionele configuratie:

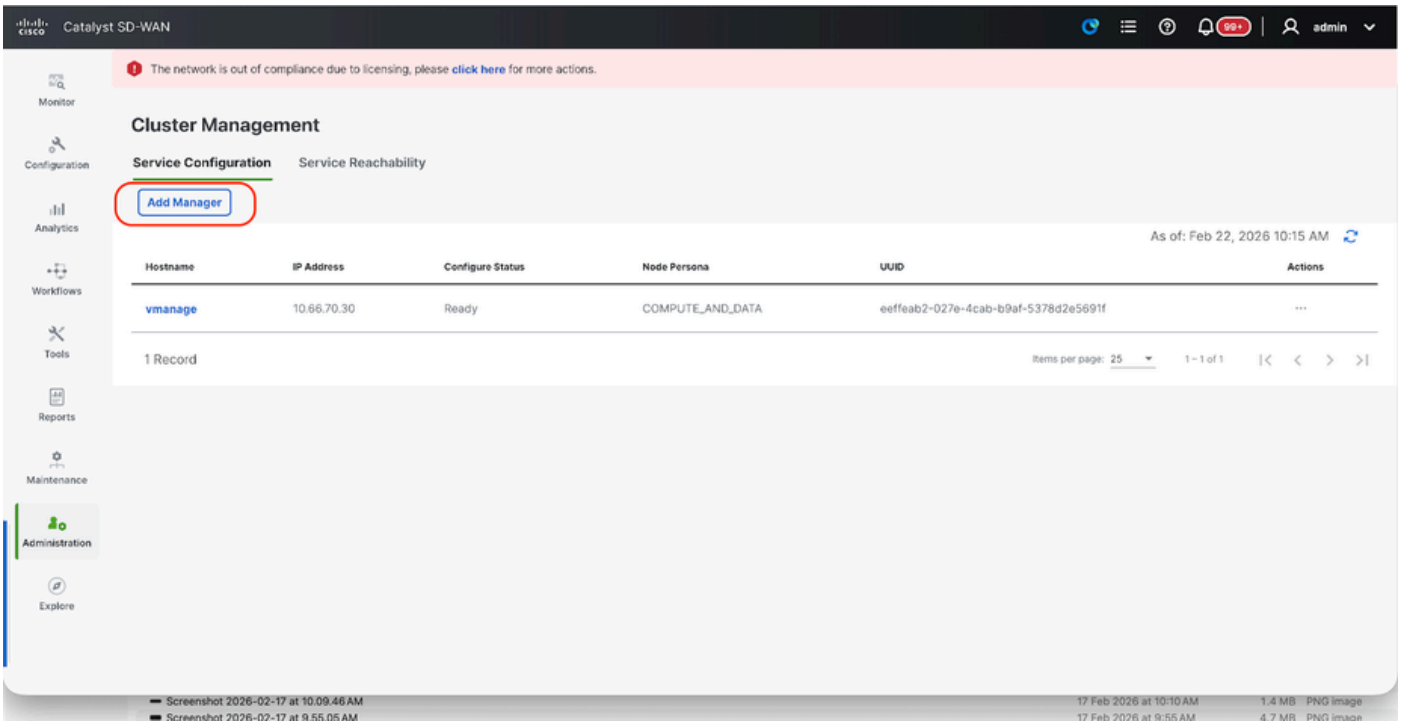
Raadpleeg deze configuratie in uw bestaande cluster om SDAVC in te schakelen - U hoeft alleen te worden gecontroleerd als dit vereist is en alleen nodig is op één vManage-node van het cluster.

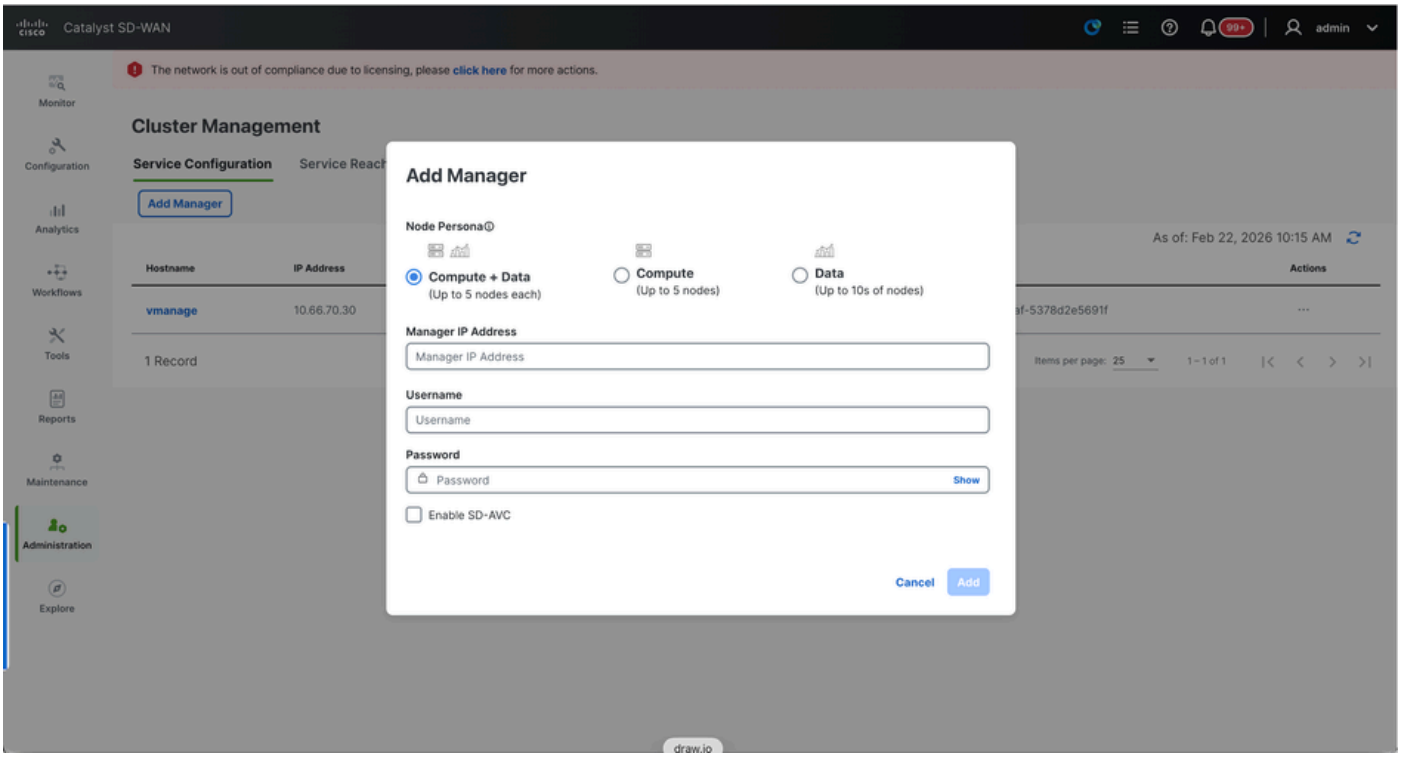
Klik op Update.

- Na dit bericht start de vManage NMS-services opnieuw op de achtergrond op en is de gebruikersinterface gedurende een paar minuten van ongeveer 5 tot 10 minuten niet beschikbaar. Gedurende deze periode is CLI-toegang van vManage beschikbaar.
- Zodra de vManage-1 UI toegankelijk is, navigeert u naar Beheer > Clusterbeheer, zorgt u ervoor dat de serviceinterface van IP vManage wordt weergegeven onder IP-adres,De status configureren is gereed en de nodepersona wordt correct weergegeven. Switch naar service bereikbaarheid sectie op dezelfde pagina en zorg ervoor dat alle diensten bereikbaar zijn.
- Als we zien dat een van de services nog niet bereikbaar is, wacht dan even. Meestal duurt het ongeveer 20 tot 30 minuten.

Bouw het vManage-cluster

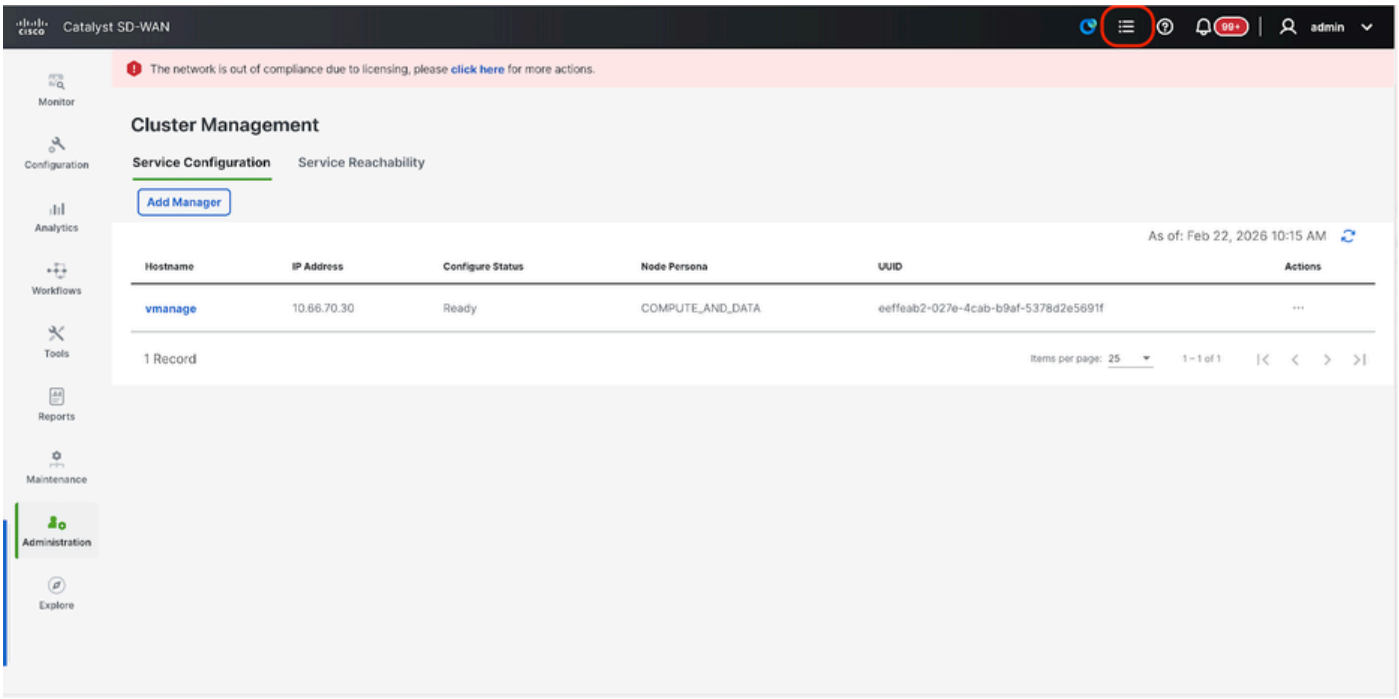
- Navigeer op de webUI van vManage-1 naar Beheer > Clusterbeheer, in de sectie Serviceconfiguratie,
- Klik op Add Manager, er verschijnt een pop-upvenster:





- Kies de Node-persona op basis van de persona-configuraties die zijn uitgevoerd terwijl de vManage – 2-node werd gesponnen.
- Voer de serviceinterface van IP vManage-2 in onder IP-adres voor beheer
- Voer de gebruikersnaam en het wachtwoord in, dat dezelfde referenties zijn als die we in stap 6 hebben gebruikt.
- Schakel SDAVC in - Wordt niet aangevinkt omdat we het al op vManage-1 zouden hebben ingeschakeld
- Klik op Toevoegen.
- Nadat u dit bericht hebt geplaatst, start de vManage NMS-services opnieuw op de achtergrond voor vManage 1- en 2-knooppunten. De gebruikersinterface is niet beschikbaar

voor een paar minuten van ongeveer 5 tot 10 minuten voor vManage 1 en 2.
- Gedurende deze periode is CLI-toegang van vManage 1 en 2 beschikbaar.
- Zodra de vManage-1 UI toegankelijk is, navigeert u naar Beheer > Clusterbeheer, zorgt u ervoor dat de IP-serviceinterface van zowel vManage wordt weergegeven onder IP-adres, Configuratiestatus is gereed en nodepersona correct wordt weergegeven.
- Switch-naar-service bereikbaarheid op dezelfde pagina en zorg ervoor dat alle services bereikbaar zijn voor beide vManage-knooppunten.
- Als we zien dat een van de services nog niet bereikbaar is, wacht dan even. Meestal duurt het ongeveer 5 tot 10 minuten.
- U kunt de status van het proces voor het toevoegen van clusters controleren in de takenlijst die beschikbaar is in de rechterbovenhoek van de vManage-gebruikersinterface.



- U kunt opzoeken naar de actieve takenlijst en als de taak nog steeds wordt vermeld onder de actieve takenlijst, geeft dit aan dat de taak nog niet is voltooid.
- U kunt op de taak klikken om de voortgang van hetzelfde te controleren. Als de taak niet wordt vermeld onder de lijst Actieve taken, switch dan naar Voltooid en zorg ervoor dat de taak succesvol is afgerond.
- Pas nadat deze punten zijn gevalideerd, gaat u verder met de volgende stap.

Met deze punten moet rekening worden gehouden voordat het volgende knooppunt aan het cluster wordt toegevoegd:

Controleer deze punten op alle UI's van de vManage-knooppunten die tot nu toe aan het cluster zijn toegevoegd:

- Navigeer naar Monitor > Overzicht van de vManage-gebruikersinterface en zorg ervoor dat het aantal vManage-knooppunten correct wordt weergegeven en bereikbaar is, afhankelijk van het aantal knooppunten dat aan het cluster is toegevoegd.

- Navigeer naar Beheer > Clusterbeheer en zorg ervoor dat de IP-serviceinterface van zowel

vManage wordt weergegeven onder IP-adres, Configuratiestatus is gereed en nodepersona correct wordt weergegeven.
- Switch-naar-service bereikbaarheid gedeelte op dezelfde pagina en zorg ervoor dat alle services bereikbaar zijn voor zowel de vManage-knooppunten.

- Telkens wanneer een node aan het cluster wordt toegevoegd, worden de NMS-services van alle nodes in het cluster opnieuw gestart, waardoor de UI van al die nodes enige tijd onbereikbaar wordt.
- Afhankelijk van het aantal knooppunten in het cluster kan het langer duren voordat de gebruikersinterface een back-up heeft gemaakt en alle services bereikbaar zijn.
- U kunt de taak controleren onder Taaklijst die beschikbaar is in de rechterbovenhoek van de vManage UI.
- Op de vManage UI van elk knooppunt dat aan het cluster is toegevoegd, moeten we alle routers, sjablonen en beleidsregels zien als ze beschikbaar waren in vManage-1.
- Als die configuraties niet aanwezig waren op vManage-1, moeten de vBonds- en vSmarts-configuraties die zijn toegevoegd aan vManage-1 en ook de configuraties Beheer > Instellingen voor Organisatienaam, vBond, Certificaatautorisatie worden weergegeven op de rest van de vManage-knooppunten die aan het cluster zijn toegevoegd.
- Herhaal dezelfde stappen voor de overige vManage-knooppunten.

Stap 4: Cold Standby DR Cluster Setup

Cold Standby DR-clusterconfiguratie

U kunt nog een vManage-cluster instellen met de stappen die worden beschreven in stap 4: vManage-cluster samenstellen. Post die de in stap 6 beschreven stappen voltooit: Config-db Backup/Restore om de config-db-back-up in het stand-bycluster te herstellen.

Stap 5: Config-DB Backup/Restore

Configuratie-db-back-up en terugzetbewerkingen op een andere vManage-node verzamelen

Configuratie-DB-back-up verzamelen:

- In de SD-WAN-fabric die momenteel wordt gebruikt, kunt u configuratie-db-back-up genereren vanuit het vManage-cluster.
- Houd er rekening mee dat we configuratie-db-back-up alleen moeten genereren op één node van het vManage-cluster, die de configuratie-db-leider is.

- Voor standalone vManage is dat vManage zelf de leider op het gebied van configuratie-db.
- Identificeer in het vManage-cluster de configuratie-db-leiderknooppunt met behulp van de diagnostiek command request nms configuration-db.U kunt deze opdracht uitvoeren op alle knooppunten van het vManage-cluster met drie knooppunten.
- In een cluster met 6 knooppunten moet u deze opdracht uitvoeren op de vManage-knooppunten waar configuratie-db is ingeschakeld om de leader-node te identificeren. Navigeer naar Beheer > Clusterbeheer om hetzelfde te controleren:

- Zoals we in de schermafbeelding zien, hebben de knooppunten die zijn geconfigureerd met persona COMPUTE_AND_DATA configuratie-db uitgevoerd.

U kunt hetzelfde controleren met de opdracht requestNmsconfiguration-dbstatus op vManageCLI. De output is zoals getoond

```
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#
```

- Zodra u het commando uitvoertVraag NMS Configuration-DB Diagnostics aan op deze knooppunten, de uitvoer is als volgt:
- Zoek naar het gemarkeerde veld voor "IsLeader". Als het is ingesteld op 1, geeft dit aan dat node de leader node is en we kunnen daar configuratie-db back-up van verzamelen.

```
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     .
```

Gebruik deze opdracht om de configuratie-db-back-up te verzamelen van de geïdentificeerde configuratie-db leader vManage-node.

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

De verwachte output is als volgt:

```
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#
```

- Noteer de configuratie-db-referenties als deze is bijgewerkt.
- Als u de configuratie-db-referenties niet kent, neemt u contact op met TAC om de configuratie-db-referenties op te halen uit de bestaande vManage-knooppunten.
- Standaardconfiguratie-db-referenties zijn gebruikersnaam: neo4j en wachtwoord: wachtwoord

Configuration-db Backup terugzetten naar een andere vManage-node

Kopieer de configuratie-db back-up naar /home/admin/ directory van vManage met behulp van SCP.

Voorbeeld van scp-opdrachtuitvoer:

```
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
```

Om de configuratie-db back-up te herstellen, moeten we eerst de configuratie-db referenties configureren. Als uw configuratie-db-referenties standaard zijn (neo4j / wachtwoord), kunnen we deze stap overslaan.

Als u configuratie-db-referenties wilt configureren, gebruikt u de opdracht request nms configuration-db update-admin-user. Gebruik de gebruikersnaam en het wachtwoord van uw keuze.

Houd er rekening mee dat de toepassingsserver van vManage opnieuw wordt gestart. Hierdoor wordt de gebruikersinterface van vManage korte tijd ontoegankelijk.

```
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#
```

Post waarin we kunnen doorgaan met het herstellen van de configuratie-db back-up:

We kunnen de opdracht request nms configuration-db restore path /home/admin/< > gebruiken om de configuratie-db te herstellen naar de nieuwe vManage:

```
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
```

Zodra de configuratie-db is hersteld, moet u ervoor zorgen dat de vManage UI toegankelijk is. Wacht ongeveer 5 minuten en probeer vervolgens toegang te krijgen tot de gebruikersinterface.

Als u eenmaal met succes bent ingelogd op de gebruikersinterface, moet u ervoor zorgen dat de lijst met Edge-routers, het sjabloon, het beleid en alle andere configuraties die aanwezig waren op uw vorige of bestaande vManage-gebruikersinterface, worden weergegeven in de nieuwe vManage-gebruikersinterface.

Stap 6: Reauthenticatie van controllers en ongeldigverklaring van oude controllers

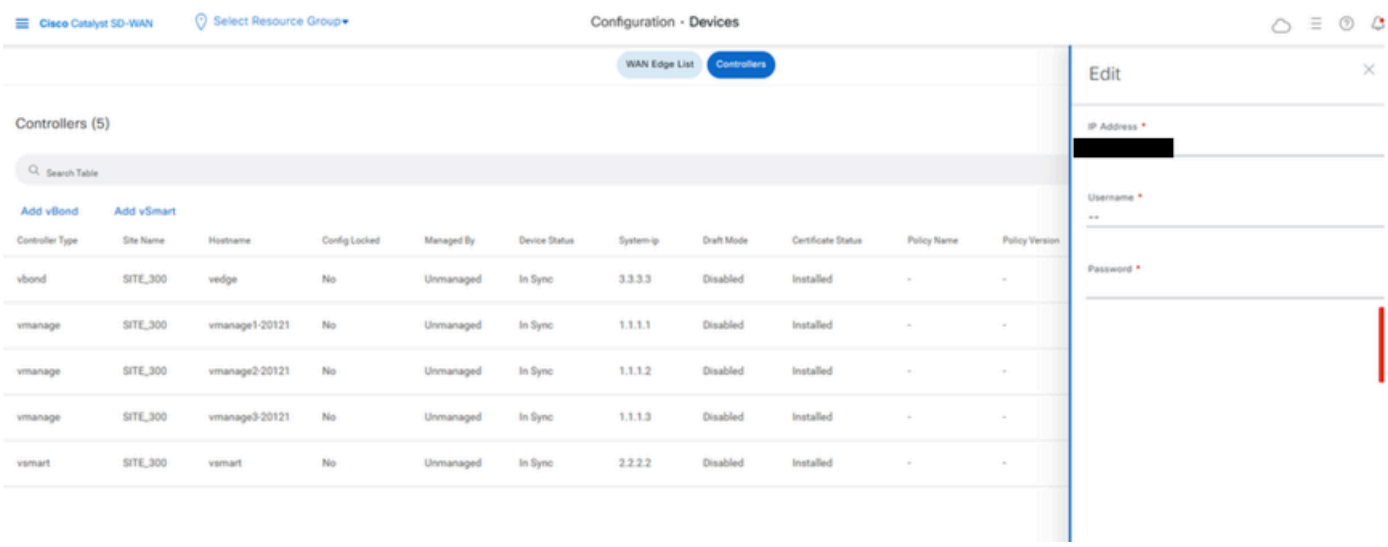
Zodra configuratie-db is hersteld, moeten we alle nieuwe controllers (vmanage/vsmart/vbond) in de fabric opnieuw verifiëren

---

Opmerking: Als de IP-interface die wordt gebruikt om opnieuw te verifiëren de tunnelinterface IP is, moet u ervoor zorgen dat de NETCONF-service is toegestaan op de tunnelinterface van de vManage, vSmart en vBond en ook op de firewalls langs het pad. De firewallpoort die moet worden geopend is TCP-poort 830 als bidirectionele regel van DR-cluster naar alle vBonds en vSmarts.

Klik in vmanage UI op Configuration > Devices > Controllers

- Klik op de drie puntjes bij elke controller en klik op Bewerken



- Vervang het ip-adres (system-ip van de controller) door het transport vpn 0 (tunnel interface) ip-adres .Voer de gebruikersnaam en het wachtwoord in en klik op opslaan
- Doe hetzelfde voor alle nieuwe controllers in de stof

Synchroniseer de Root-cert-keten

Als alle controllers zijn geïnstalleerd, voert u deze stap uit:

Voer op elke Cisco SD-WAN Manager-server in het nieuw actieve cluster de volgende acties uit:

Voer deze opdracht in om het rootcertificaat te synchroniseren met alle Cisco Catalyst SD-WAN-apparaten in het nieuw actieve cluster:

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

Voer deze opdracht in om de Cisco SD-WAN Manager UUID te synchroniseren met de Cisco SD-WAN Validator:

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

Zodra de fabric is hersteld en de controle- en bfd-sessies zijn ingesteld voor alle randen en controllers in de fabric, moeten we de oude controllers (vmanage/vsmart/vbond) van de gebruikersinterface ongeldig maken

- Klik op Configuratie > Apparaten > Certificaten in vmanage UI
- Klik op Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Ongeldig maken
- Klik op verzenden naar vbond
- Klik in vmanage UI op Configuration > Devices > Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Verwijderen

Stap 7: Controles achteraf

Opmerking: ga verder met het gedeelte Controles achteraf dat hier wordt weergegeven en dat voor alle implementatiecombinaties geldt.

Combinatie 5: vManage Cluster + NH ingeschakeld

Benodigde gevallen:

- 3 of 6 vManage (primair cluster)
- 3 of 6 vManage (DR standby-cluster)
- 1 of meer vBond (verdeeld over primaire en DR-datacenters)
- 1 of meer vSmart (verdeeld over primaire en NH-datacenters)

Stappen:

1. Alle instanties weergeven met de gemeenschappelijke stappen
2. Voorcontroles
3. Configureren van vManage UI, certificaten en onboard controllers
4. vManage-cluster samenstellen
5. Cold Standby DR-clusterconfiguratie
6. Config-db back-up/terugzetbewerking
7. Controles achteraf

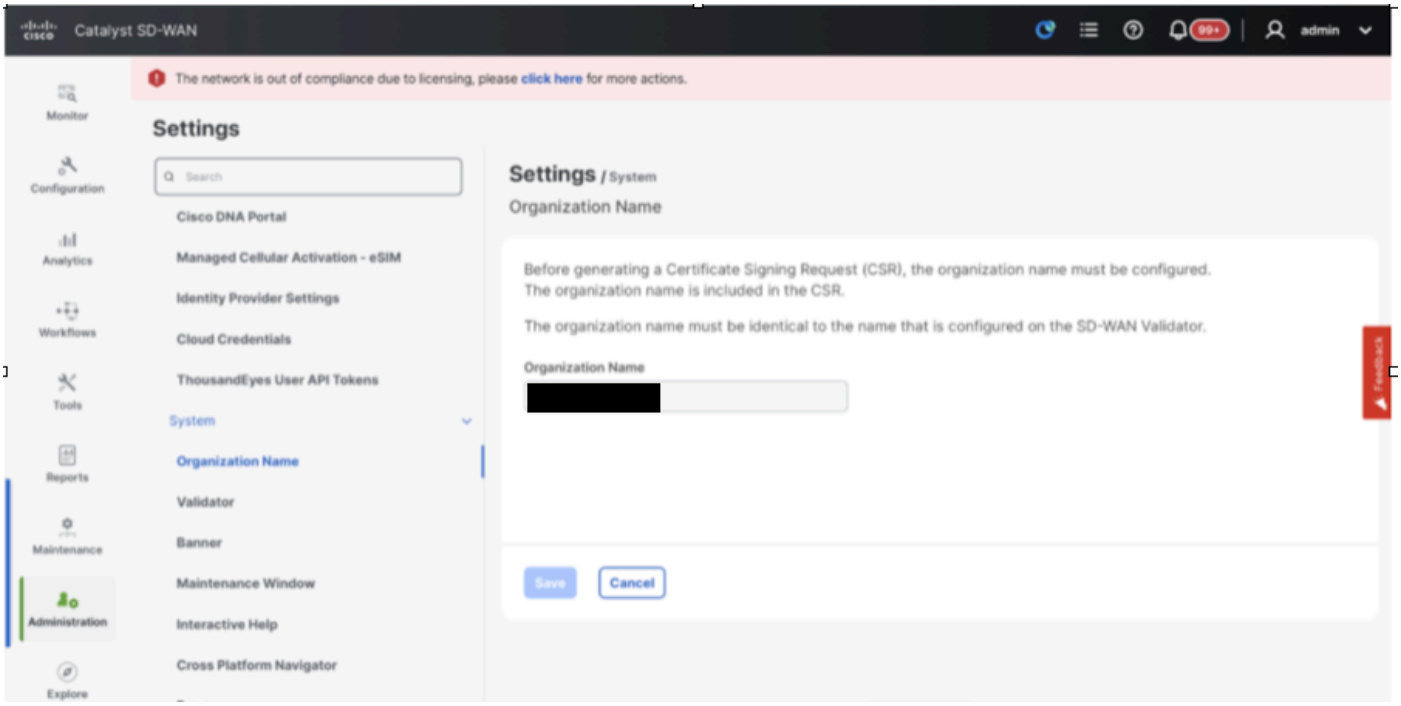
Stap 1: Controles vooraf

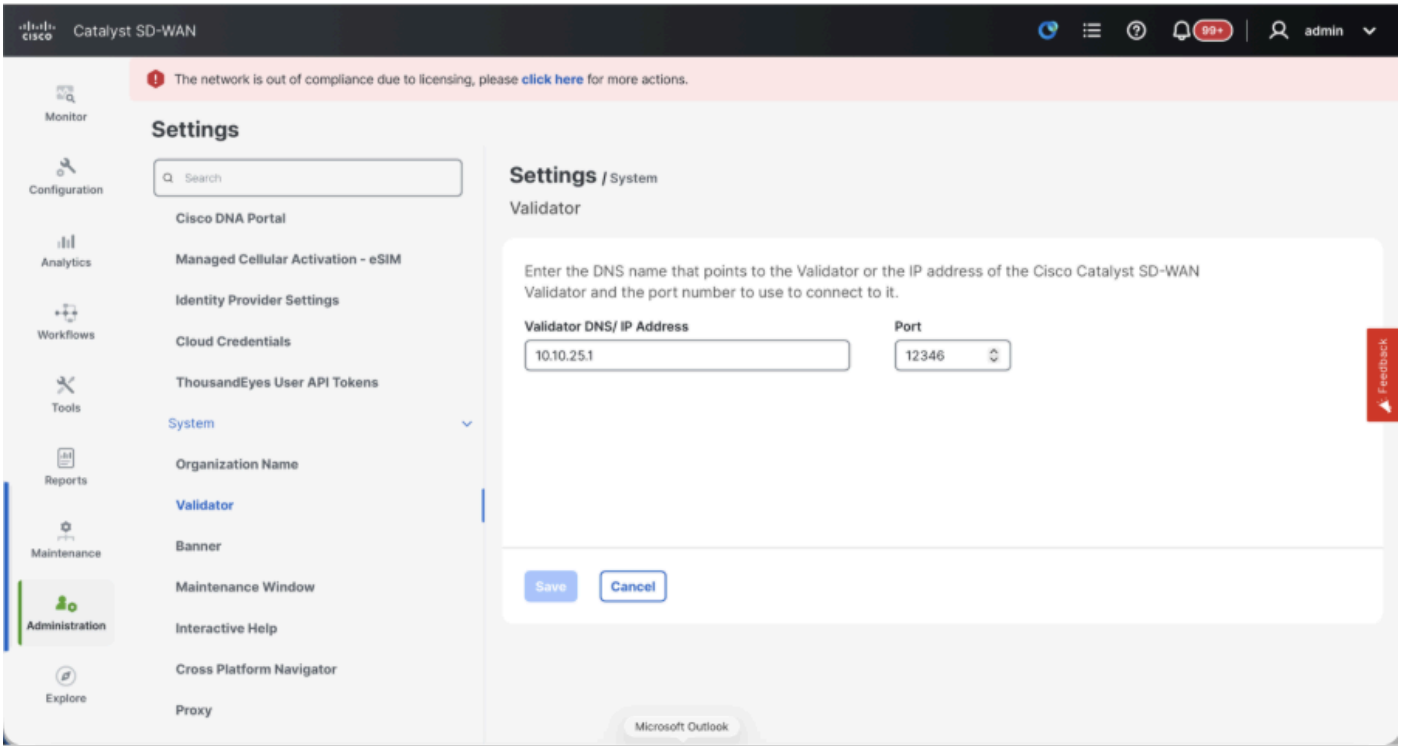
- Zorg ervoor dat het aantal actieve Cisco SD-WAN Managerinstances gelijk is aan het aantal nieuw geïnstalleerde Cisco SD-WAN Managerinstances.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties dezelfde softwareversie uitvoeren.
- Zorg ervoor dat alle actieve en nieuwe Cisco SD-WAN Manager-instanties het IP-beheeradres van de Cisco SD-WAN Validator kunnen bereiken.
- Controleer of certificaten zijn geïnstalleerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties.
- Zorg ervoor dat de klokken op alle Cisco Catalyst SD-WAN-apparaten, inclusief de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, worden gesynchroniseerd.
- Zorg ervoor dat een nieuwe set van systeem-IP's en site-ID's is geconfigureerd op de nieuw geïnstalleerde Cisco SD-WAN Manager-instanties, samen met dezelfde basisconfiguratie als het actieve cluster.

Stap 2: vManage UI, certificaten en ingebouwde controllers configureren

De configuraties op de vManage-gebruikersinterface bijwerken

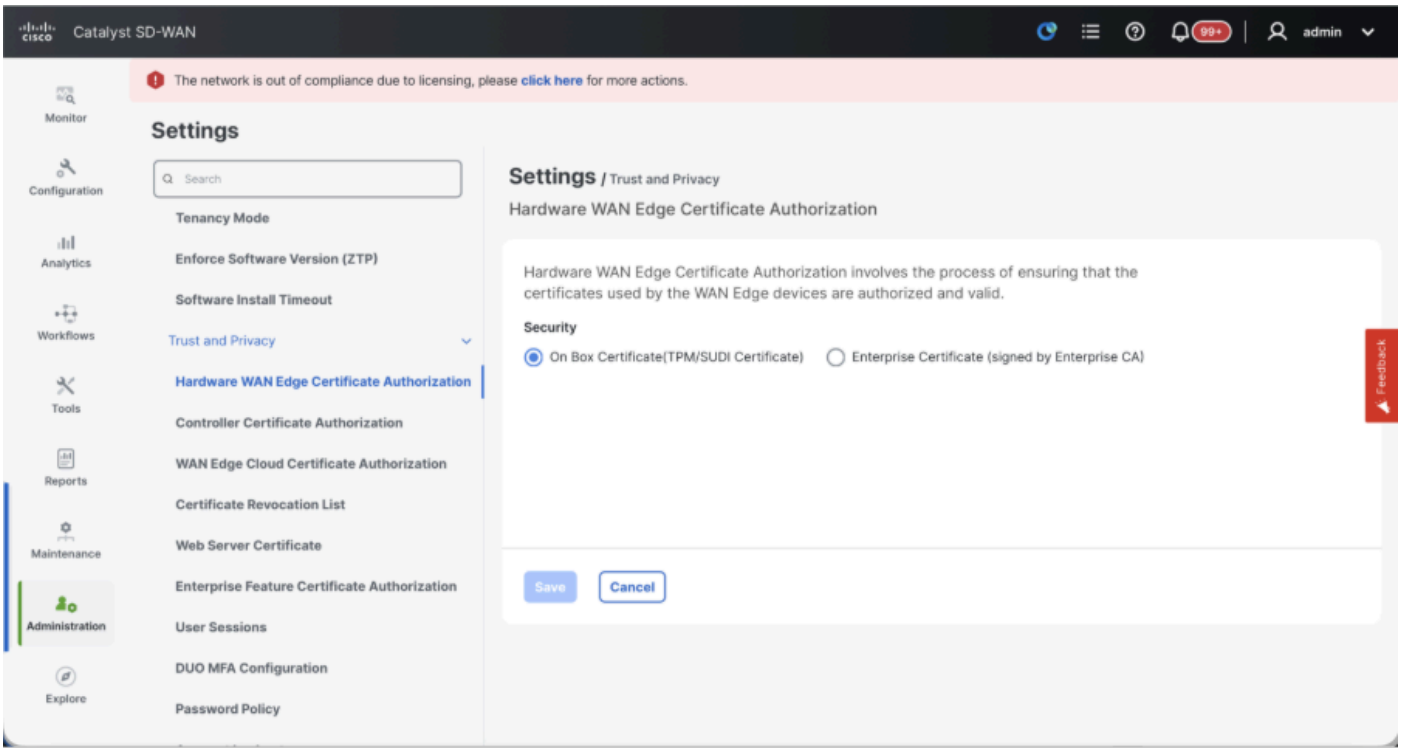
- Zodra de configuraties in stap 1 zijn toegevoegd aan de CLI van alle controllers, hebben we toegang tot de webUI van vManage, met behulp van de URL https://<vmanage-ip> in uw browser. Gebruik het VPN 512 IP-adres van de respectieve vManage-knooppunten. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.
- Navigeer naar Beheer > Instellingen en voer deze stappen uit.
- Configureer de naam van de organisatie en het URL/IP-adres van de validator/vBond. Configureer dezelfde waarde als in de CLI van de vManage-node.
- In vManage 20.15/20.18 zijn deze configuraties beschikbaar onder de sectie Systeem.



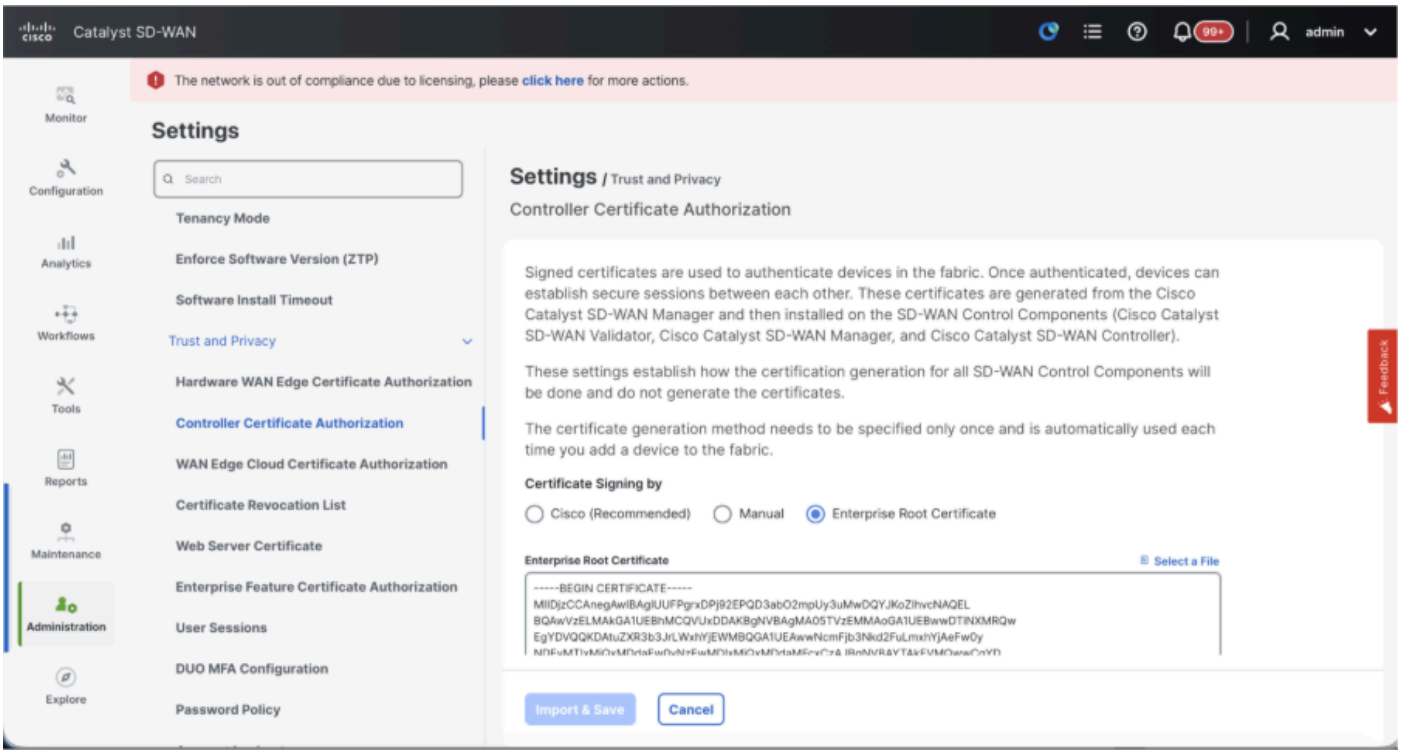


- Controleer de configuraties voor Certificaatautorisatie (CA), die bepaalt welke Certificaatautoriteit wordt gebruikt voor het ondertekenen van de certificaten. We zien daar 3 mogelijkheden:

1. Hardware WAN Edge Certificate Authorization - Bepaalt de CA voor hardware SD-WAN Edge-routers.
    - On Box Certificate (TPM/SUDI-certificaat) - Met deze optie wordt het vooraf geïnstalleerde certificaat op de hardware van de router gebruikt om de Controleverbindingen (TLS/DTLS-verbindingen) tot stand te brengen
    - Enterprise Certificate (ondertekend door Enterprise CA) - Met deze optie gebruiken de routers certificaten die zijn ondertekend door Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

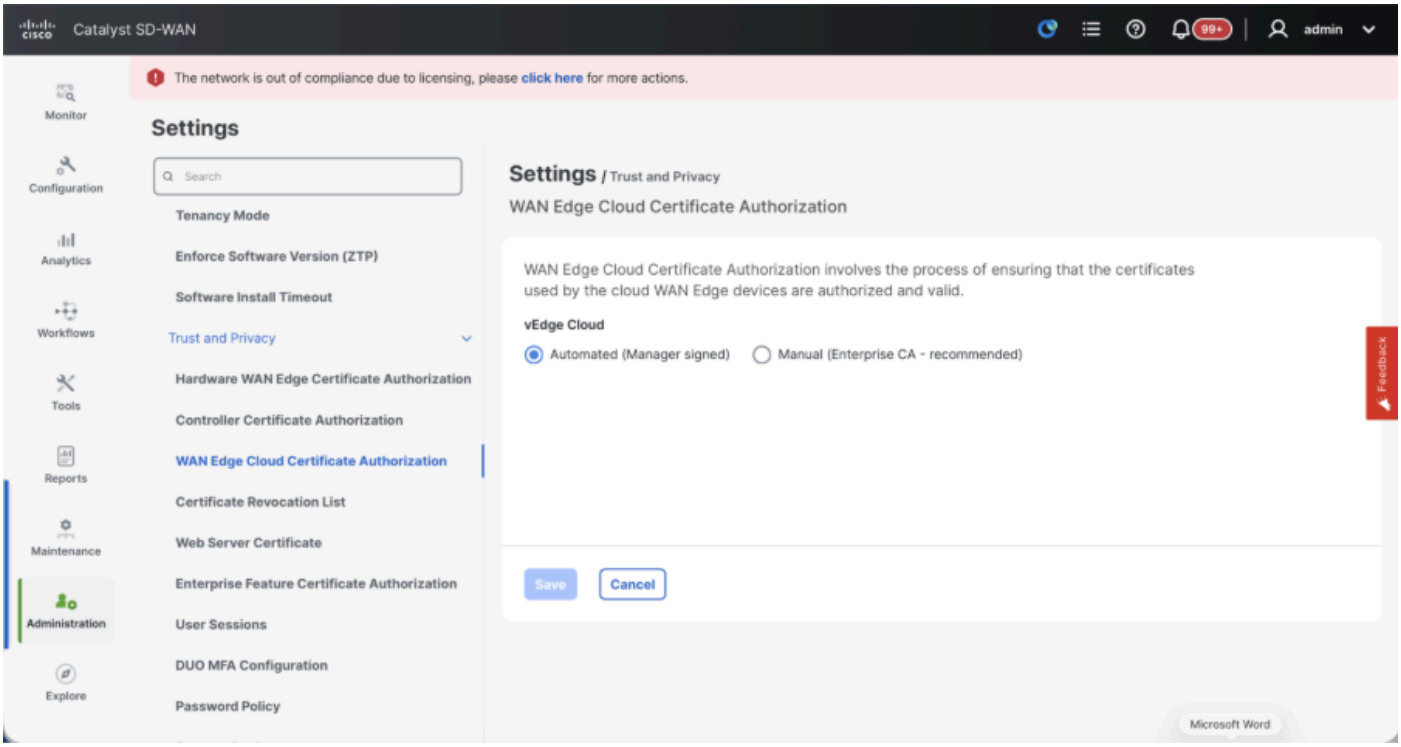


2. Controllercertificaatautorisatie - bepaalt de CA voor SD-WAN-controllers.
    - Cisco (aanbevolen) - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. vManage neemt automatisch contact op met het PNP-portaal met behulp van de referenties voor slimme accounts die zijn geconfigureerd op de vManage en laat het certificaat ondertekenen en installeren op de controller.
    - Handleiding - Controllers gebruiken de certificaten die zijn ondertekend door Cisco PKI. Handmatig ondertekenen van de CSR met behulp van de Cisco PNP portal door te navigeren naar smart account en virtuele account van de respectieve SD-WAN overlay.
    - Enterprise Root Certificate - Met deze optie gebruiken de routers certificaten die zijn ondertekend door de Enterprise-certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

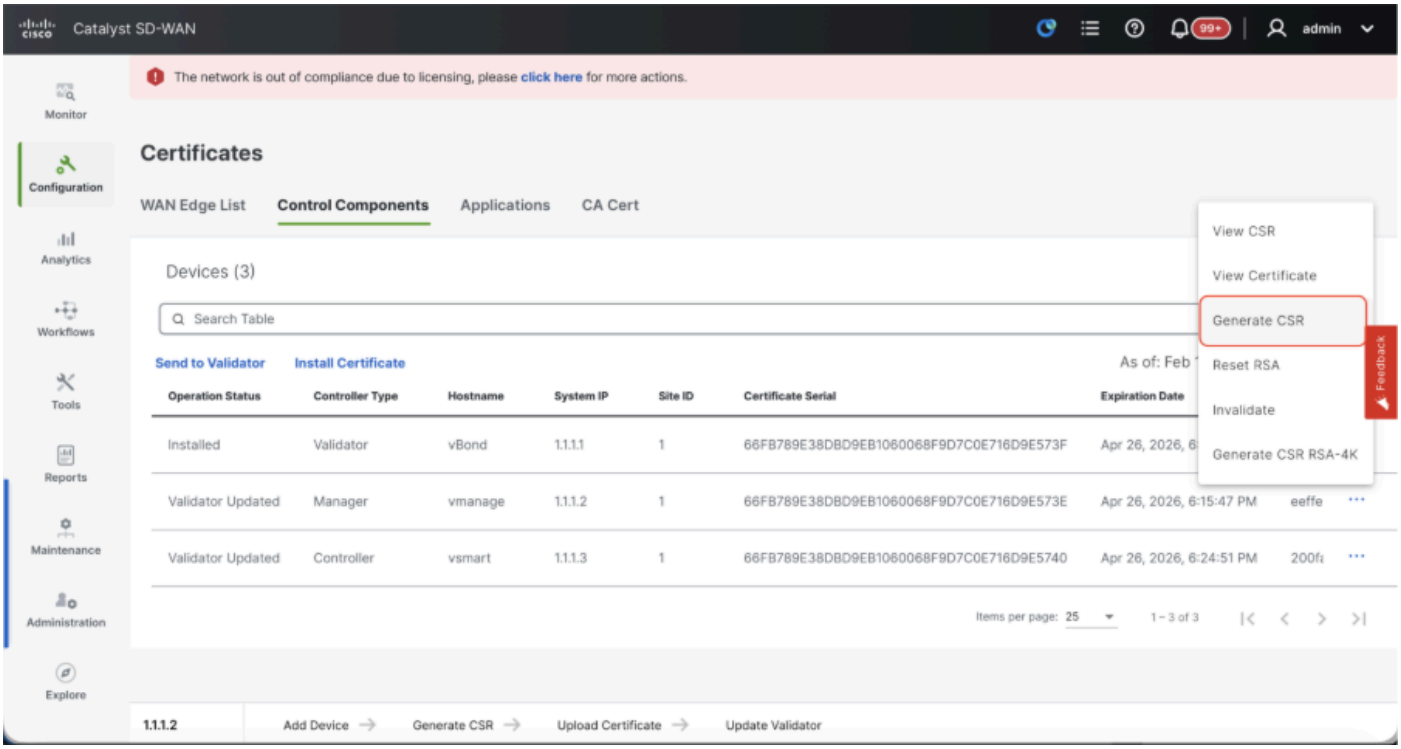


3. WAN Edge Cloud Certificate Authorization - Bepaalt de CA voor virtuele SD-WAN Edge-routers (CSR1000v, C8000v, vEdge cloud)
    - Geautomatiseerd (vManage ondertekend) - vManage ondertekent automatisch de CSR voor de virtuele Edge-routers en installeert het certificaat op de router.
    - Handmatig (Enterprise CA - aanbevolen) - Virtuele routers gebruiken certificaten die zijn ondertekend door de certificeringsinstantie van uw organisatie. Als u deze optie kiest, moet het basiscertificaat van Enterprise CA hier worden bijgewerkt.

Als we onze eigen CA, Enterprise-certificeringsinstantie, gebruiken, kiest u in dat geval Enterprise.



- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers
- Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

Onboarding vBond/Validator en vSmart/Controller naar de vManage

Navigeer naar Configuratie > Apparaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

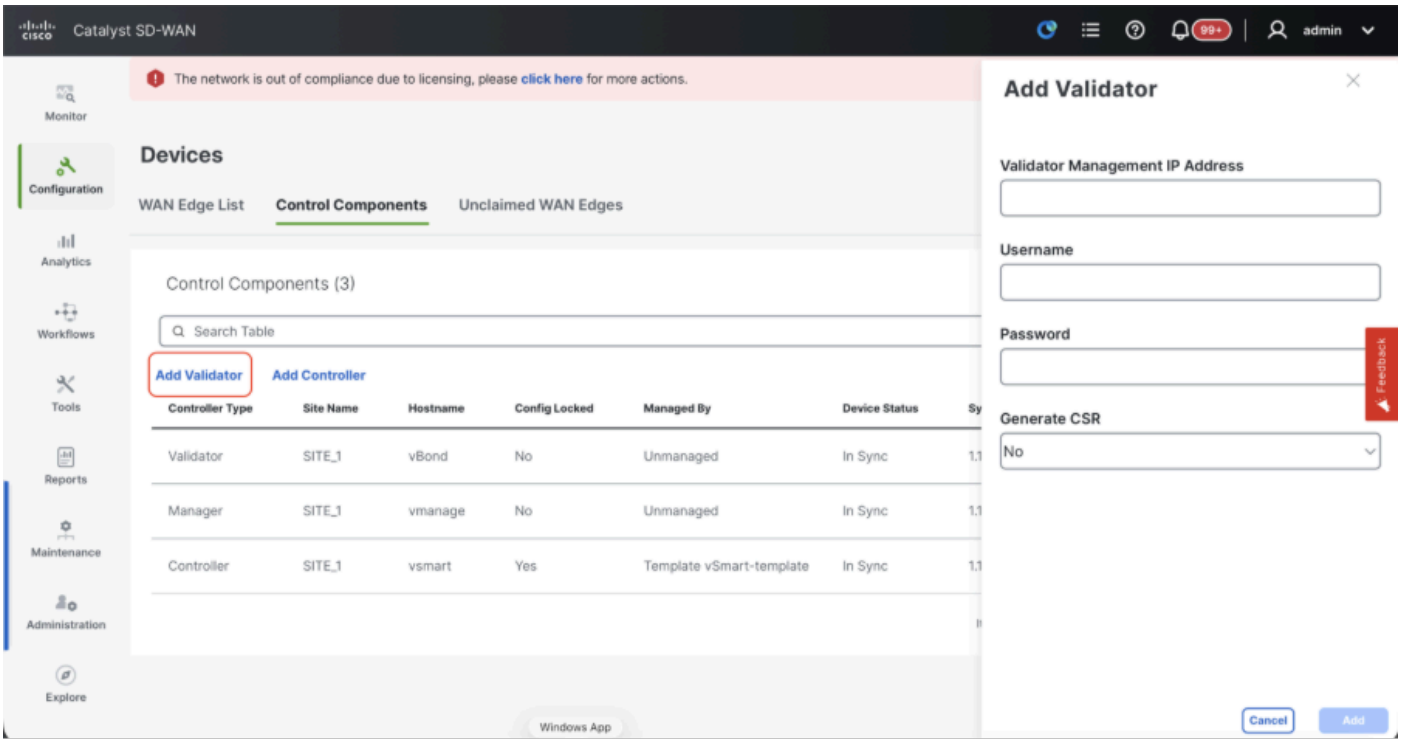
OnboardingVbond/validator

- Klik op AdvBondin geval van 12 .12vManagerValidator toevoegenin geval van 20.15/20.18vManage. Er wordt een pop-upvenster geopend. Voer de VPN 0 transporteert IP

van vBonds dat bereikbaar is vanaf de vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan vanuit de CLI van vManagetovBondIP.
- Voer de gebruikersreferenties van vBond in.

Opmerking: We moeten beheerdersreferenties gebruiken van vBond of een gebruikersonderdeel van netadminggroup. U kunt dit controleren in de CLI van de vBond. Kies Ja in de drop-down van "Genereer CSR" als we een nieuw certificaat voor vBond moeten installeren

Opmerking: Als de vBond zich achter een NAT-apparaat/firewall bevindt, controleert u of de vBond VPN 0-interface IP is vertaald naar een openbaar IP-adres. Als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u het openbare IP-adres van de VPN 0-interface in deze stap



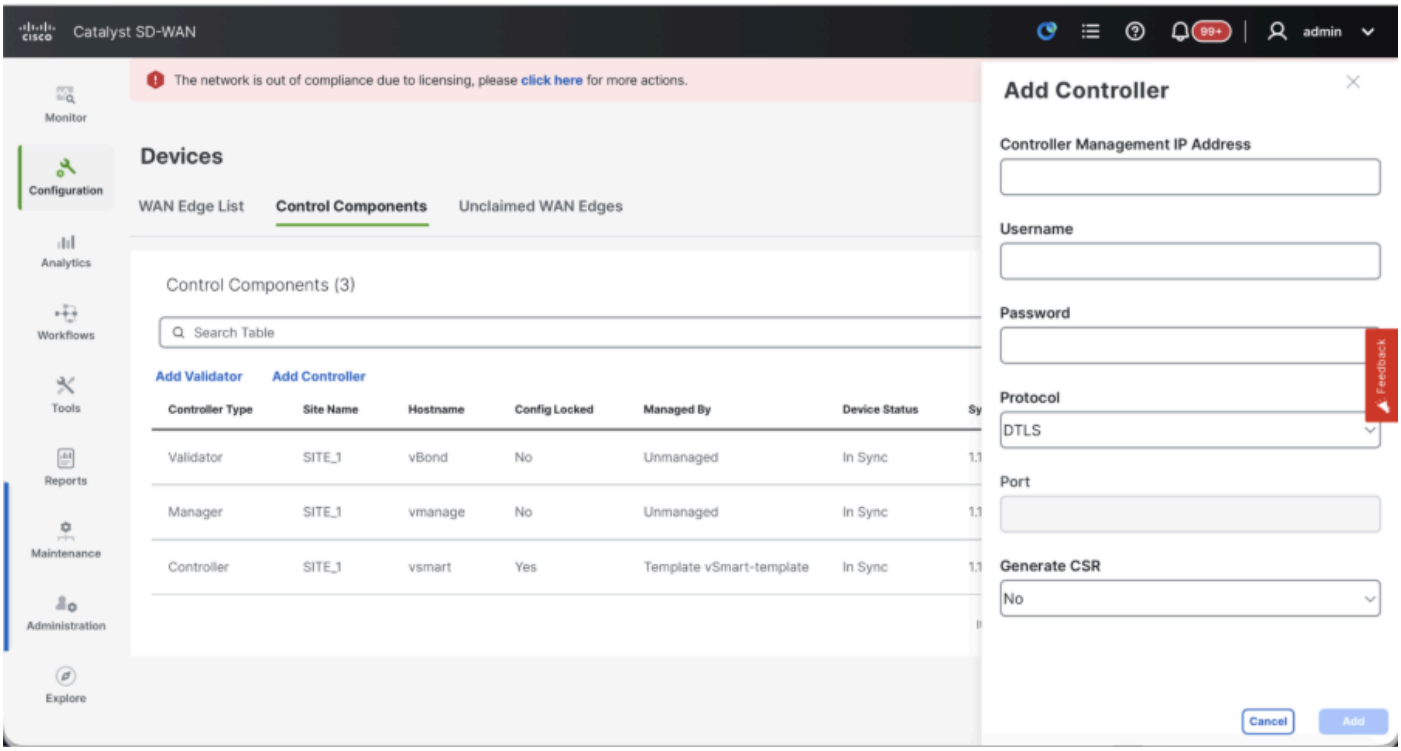
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door de vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vBond geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren. Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u

op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat. Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vBonds zijn, herhaalt u dezelfde stappen.

Onboarding vSmart/controller:

- Klik op Add vSmart in geval van 10 .12 vManage of Add Controller in geval van 20.15/20.18 vManage.
- Als er een pop-upvenster wordt geopend, voert u het VPN 0-transport IP van vSmart in dat bereikbaar is via vManage.
- Controleer de bereikbaarheid met behulp van ping indien toegestaan van CLI van vManage naar vSmart IP.
- Voer de gebruikersreferenties van vSmart Note in die we nodig hebben om beheerdersreferenties van vSmart of een gebruikersdeel van de netadmin-groep te gebruiken.
- U kunt dit controleren in de CLI van de vSmart.
- Stel het protocol in op TLS als we TLS willen gebruiken voor routers om controleverbindingen met vSmart tot stand te brengen. Deze configuratie moet ook worden geconfigureerd op CLI van vSmarts- en vManage-knooppunten.
- Kies Ja in de keuzelijst "MVO genereren" als we een nieuw certificaat voor vSmart moeten installeren.

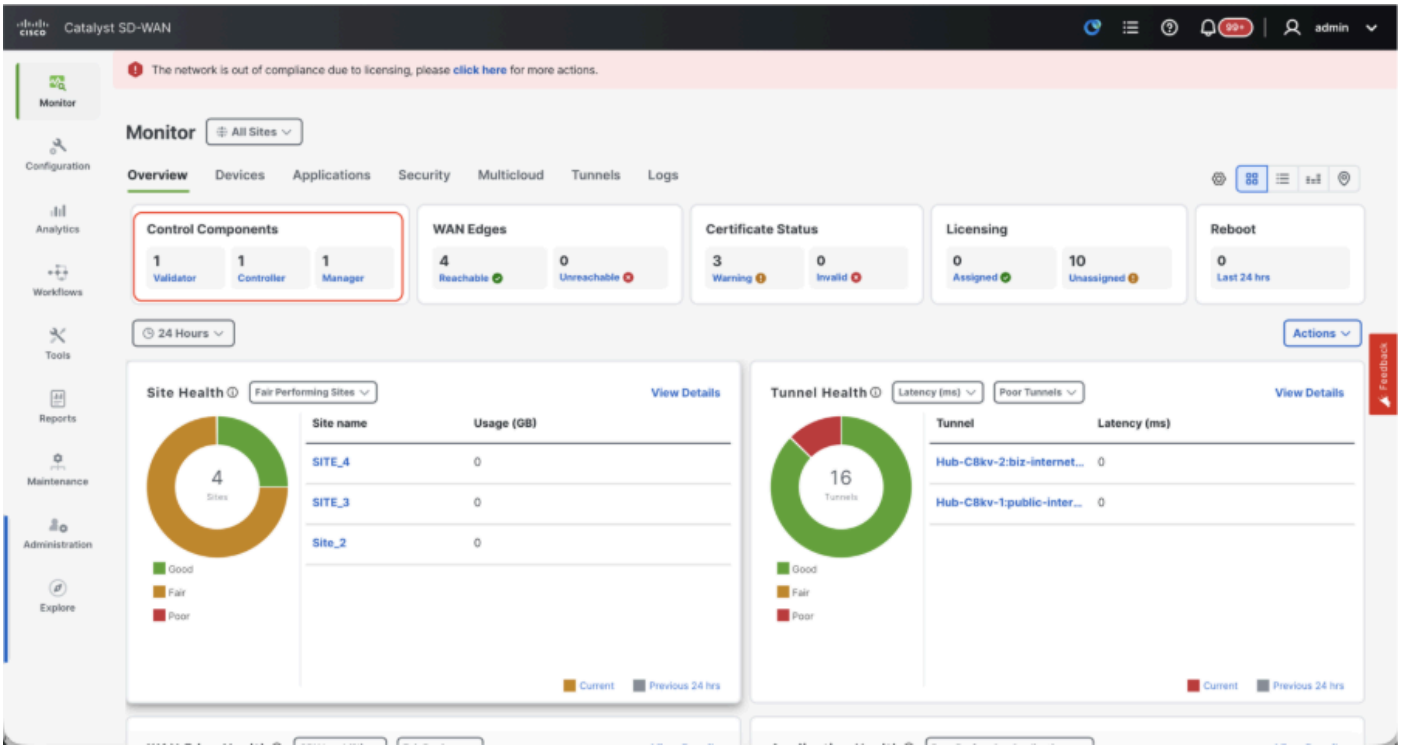
Opmerking: Als de vSmart zich achter NAT-apparaat/firewall bevindt, controleert u of de vSmart VPN 0-interface IP is vertaald naar een openbaar IP-adres en als de VPN 0-interface IP niet bereikbaar is via vManage, gebruikt u in deze stap het openbare IP-adres van de VPN 0-interface IP.



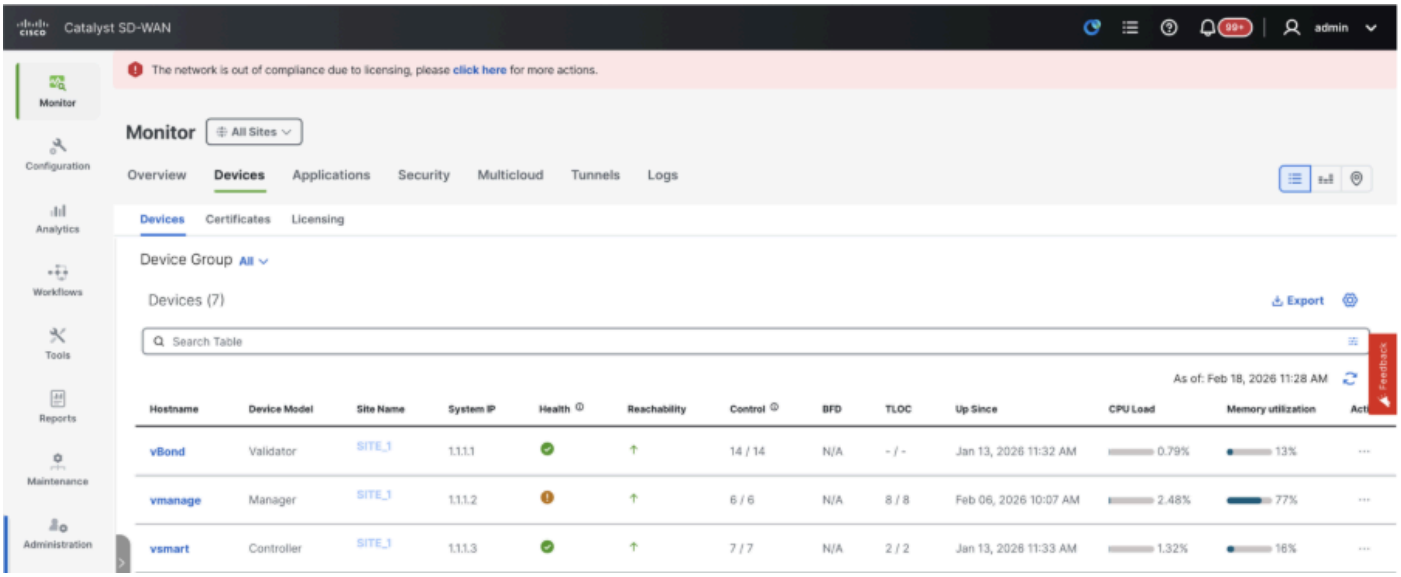
- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op de vSmart geïnstalleerd.
- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren.
- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.
- Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.
- Als er meerdere vSmarts zijn, herhaalt u dezelfde stappen.

Verificatie

Controleer na voltooiing van alle stappen of alle besturingscomponenten bereikbaar zijn in Monitor>Dashboard



- Klik op de betreffende besturingscomponenten en bevestig dat ze allemaal bereikbaar zijn.
- Navigeer naar Monitor > Apparaten en controleer of alle besturingscomponenten bereikbaar zijn.



Stap 3: vManage-cluster samenstellen

Onboard SD-WAN-verbinding met een vManage-cluster in de SD-WAN-overlay

---

Opmerking: vManage Cluster kan worden geconfigureerd met 3 vManage-knooppunten of 6 vManage-knooppunten, afhankelijk van het aantal sites dat aan boord is van de SD-WAN-verbinding

---

Aan boord van alle SD-WAN-controllers met één vManage-node

Ga verder met de stappen die worden gedeeld in "Onboard SD-WAN-controllers met een enkele node vManage in de SD-WAN-overlay" om eerst de SD-WAN-fabric met één vManage-node en alle vereiste Validators (vBond) en Controllers (vSmart) aan boord te brengen.

De CLI-configuraties configureren van alle vManage-knooppunten die deel uitmaken van het cluster

- De rest van de vManage-knooppunten configureren. In het geval van een cluster met drie knooppunten moet u nog twee knooppunten configureren, in het geval van een cluster met zes knooppunten moet u vijf knooppunten configureren.
- Systeemconfiguraties configureren zoals wordt weergegeven:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Opmerking: Als we URL als vBond-adres gebruiken, moet u de IP-adressen van de DNS-server configureren in VPN 0-configuratie of ervoor zorgen dat deze kunnen worden opgelost.

Deze configuraties zijn nodig om de transportinterface die wordt gebruikt om besturingsverbindingen met de routers en de rest van de controllers tot stand te brengen.

```
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
```

Configureer ook de VPN 512management interface om out-of-band management toegang tot de controller mogelijk te maken.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Optionele configuratie:

- U kunt verwijzen naar de configuraties van uw bestaande controller en als de hier vermelde configuratie aanwezig is, kunt u deze configuratie toevoegen aan de nieuwe controllers.
- Configureer het controleprotocol alleen als TLS als routers verplicht zijn om beveiligde controleverbindingen met de vManage-knooppunten tot stand te brengen met behulp van TLS. Standaard maken alle controllers en routers een controleverbinding met behulp van DTLS. Dit is een optionele configuratie die alleen vereist is voor vSmart- en vManage-knooppunten, afhankelijk van uw vereisten.

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

Serviceinterface configureren op alle vManage-knooppunten

Configureer de service-interface op alle vManagenodes, inclusief vManage-1, die al aan boord is. Deze interface wordt gebruikt voor clustercommunicatie, wat communicatie tussen de vManagenodes in het cluster betekent.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Zorg ervoor dat hetzelfde IP-subnet wordt gebruikt voor de service-interface voor alle knooppunten in het vManagecluster.

Clusterreferenties configureren

We kunnen dezelfde beheerdersreferenties van de vManageodes gebruiken om het vManagecluster te configureren. Anders kunnen we een nieuwe gebruikersreferentie configureren die deel uitmaakt van netadminggroup. De configuraties voor het configureren van nieuwe gebruikersreferenties worden weergegeven

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

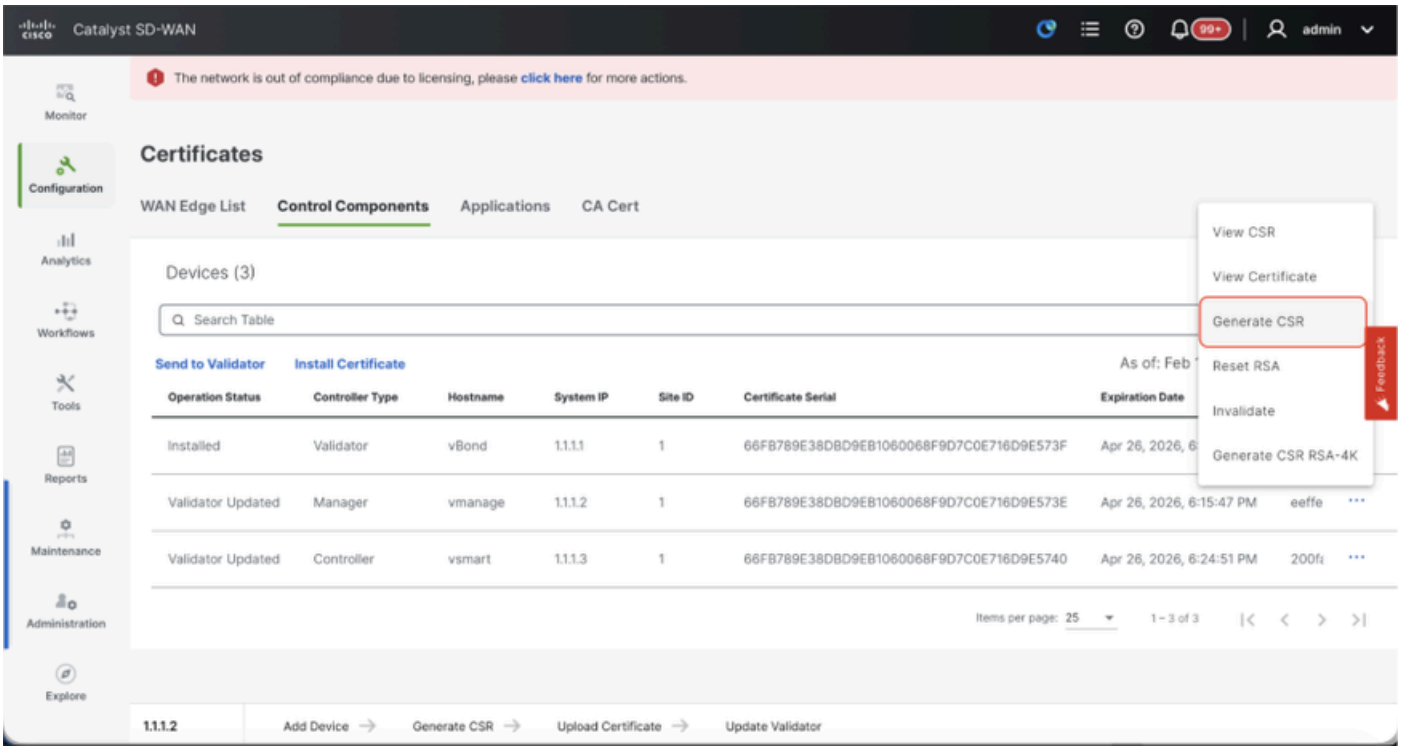
Zorg ervoor dat u dezelfde gebruikersreferenties configureert voor alle vManagenodes die deel uitmaken van het cluster. Als we besluiten beheerdersreferenties te gebruiken, moet het dezelfde gebruikersnaam/wachtwoord zijn voor alle vManagenodes.

Apparaatcertificaat installeren op alle vManage-knooppunten

- Meld u aan bij vManageUI van alle vManagenodes met behulp van de URL https://<vmanage-ip>in uw browser. Gebruik het VPN 512 IP-adres van de respectievelijke vManagenodes. U kunt inloggen met de gebruikersnaam en het wachtwoord van de beheerder.

- Navigeer naar Configuratie > Certificaten > Besturingscomponenten in het geval van 20.15/20.18 vManage-knooppunten. In het geval van 20.9/20 .12 versies, Configuratie > Apparaten > Controllers

  Klik op ... voor Manager/vManage en klik op CSR genereren.



- Zodra de CSR is gegenereerd, kunt u de CSR downloaden en laten ondertekenen op basis van de certificeringsinstantie die is gekozen voor controllers. U kunt deze configuratie controleren in Beheer > Instellingen > Autorisatie voor controllercertificaat. Als Cisco (Recommended) wordt gekozen, wordt de CSR automatisch door vManage naar het PNP-portaal geüpload en zodra het certificaat is ondertekend, wordt het automatisch op vManage geïnstalleerd.

- Als Handmatig wordt gekozen, ondertekent u de CSR handmatig met behulp van het Cisco PNP-portaal door naar het slimme account en het virtuele account van de respectieve SD-WAN-overlay te navigeren.

- Zodra het certificaat beschikbaar is via het PNP-portaal, klikt u op het certificaat installeren in hetzelfde gedeelte van vManage en uploadt u het certificaat en installeert u het certificaat.

- Dezelfde procedure is van toepassing als we gebruik maken van Digicert en Enterprise Root Certificate.

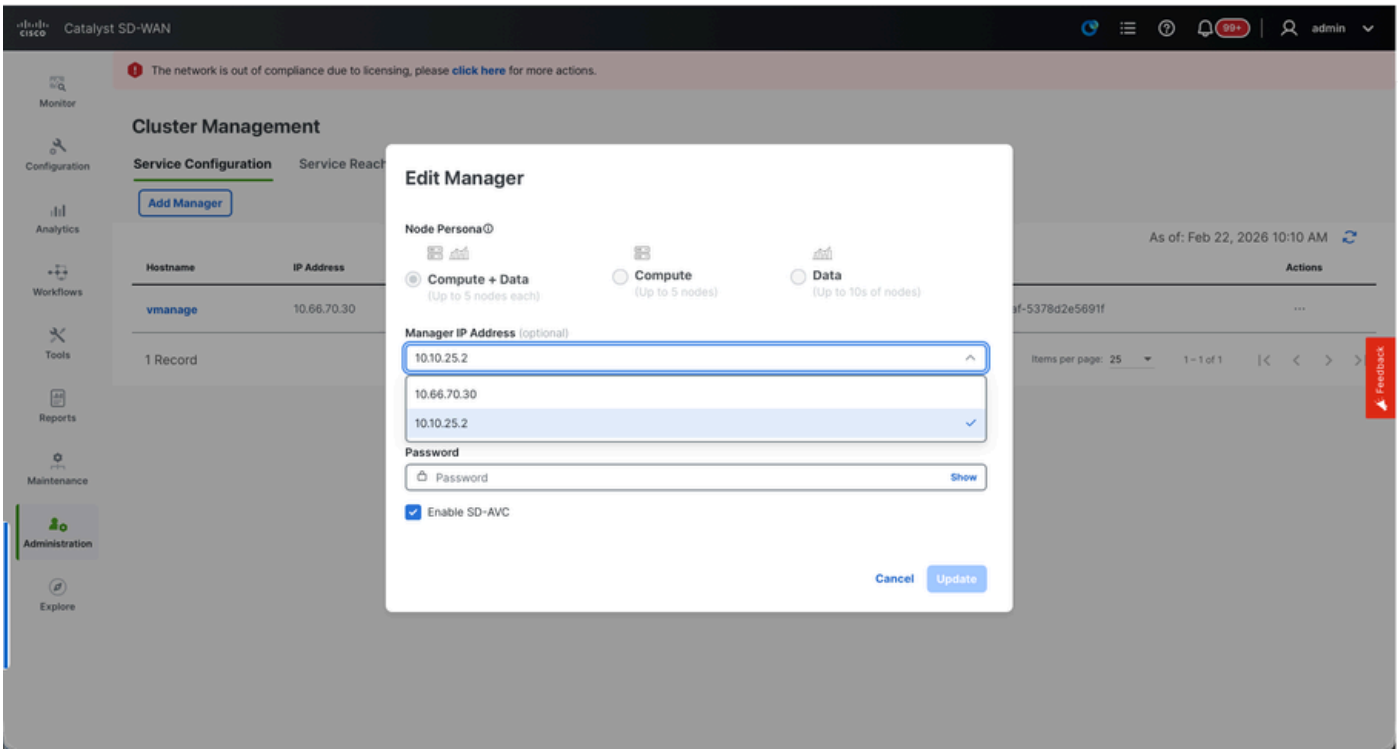
- Voltooi deze stap voor alle vManage-knooppunten die deel uitmaken van het cluster.

Klaar om het vManage-cluster te bouwen

- Navigeer op de webUI van vManage-1 naar Beheer > Clusterbeheer, klik op ... onder Acties voor vManage-1, kies Bewerken.
- De nodepersona wordt automatisch gekozen op basis van de persona die we hebben gekozen terwijl de VM werd aangemaakt.

Opmerking: voor een cluster met drie knooppunten worden alle drie vManage-knooppunten met compute+data als persona weergegeven. Voor een cluster met zes knooppunten worden drie vManage-knooppunten met compute+data aangesproken, terwijl de persona en drie vManage-knooppunten met de persona worden aangesproken.

- Zorg ervoor dat u in de vervolgkeuzelijst voor IP-adres van Manager serviceinterface IP van vManage kiest.



- Voer de gebruikersnaam en het wachtwoord in die we willen gebruiken om vManage-cluster in te schakelen. Dit wordt clusterreferenties genoemd.
- Zoals eerder vermeld, moeten dezelfde referenties worden geconfigureerd op alle vManage-knooppunten en moeten deze worden gebruikt terwijl alle knooppunten aan het cluster worden toegevoegd.

Optionele configuratie:

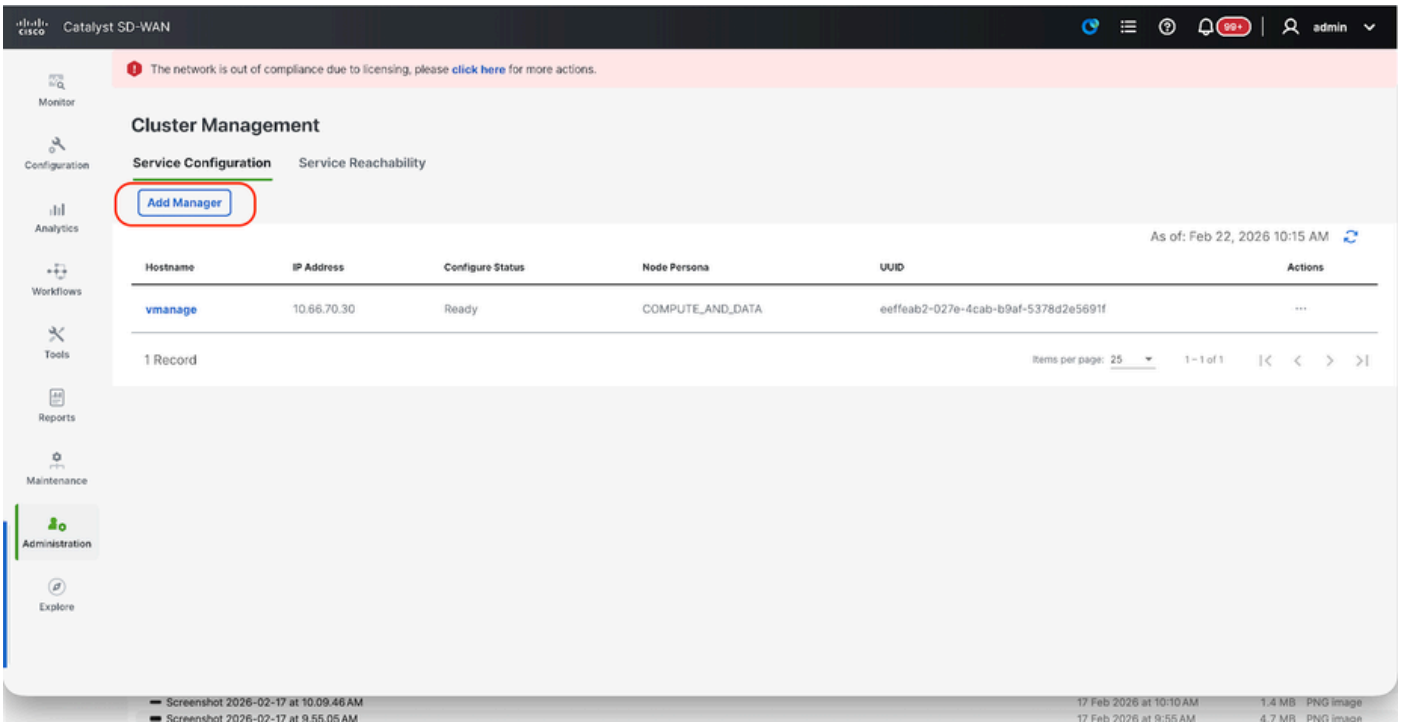
Raadpleeg deze configuratie in uw bestaande cluster om SDAVC in te schakelen - U hoeft alleen te worden gecontroleerd als dit vereist is en alleen nodig is op één vManage-node van het cluster.

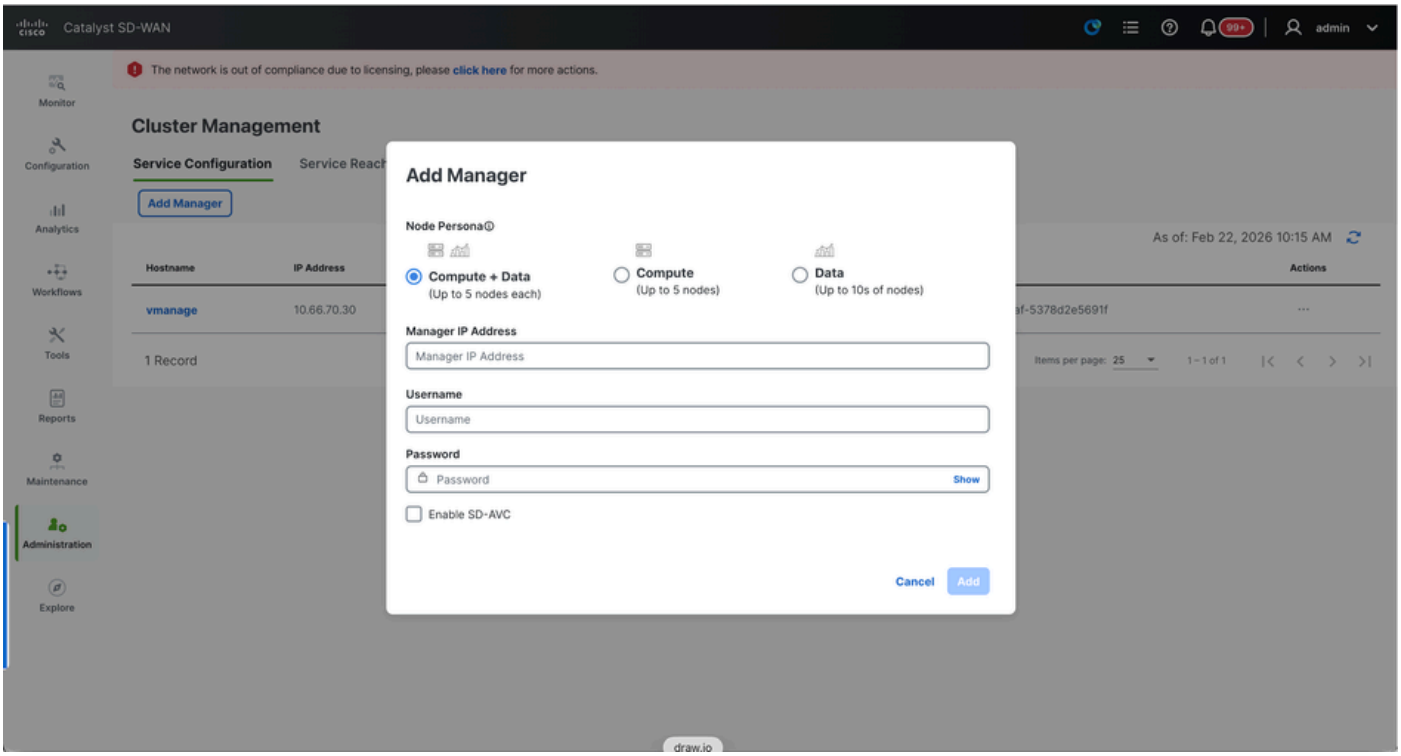
Klik op Update.

- Na dit bericht start de vManage NMS-services opnieuw op de achtergrond op en is de gebruikersinterface gedurende een paar minuten van ongeveer 5 tot 10 minuten niet beschikbaar. Gedurende deze periode is CLI-toegang van vManage beschikbaar.
- Zodra de vManage-1 UI toegankelijk is, navigeert u naar Beheer > Clusterbeheer, zorgt u ervoor dat de serviceinterface van IP vManage wordt weergegeven onder IP-adres,De status configureren is gereed en de nodepersona wordt correct weergegeven. Switch naar service bereikbaarheid sectie op dezelfde pagina en zorg ervoor dat alle diensten bereikbaar zijn.
- Als we zien dat een van de services nog niet bereikbaar is, wacht dan even. Meestal duurt het ongeveer 20 tot 30 minuten.

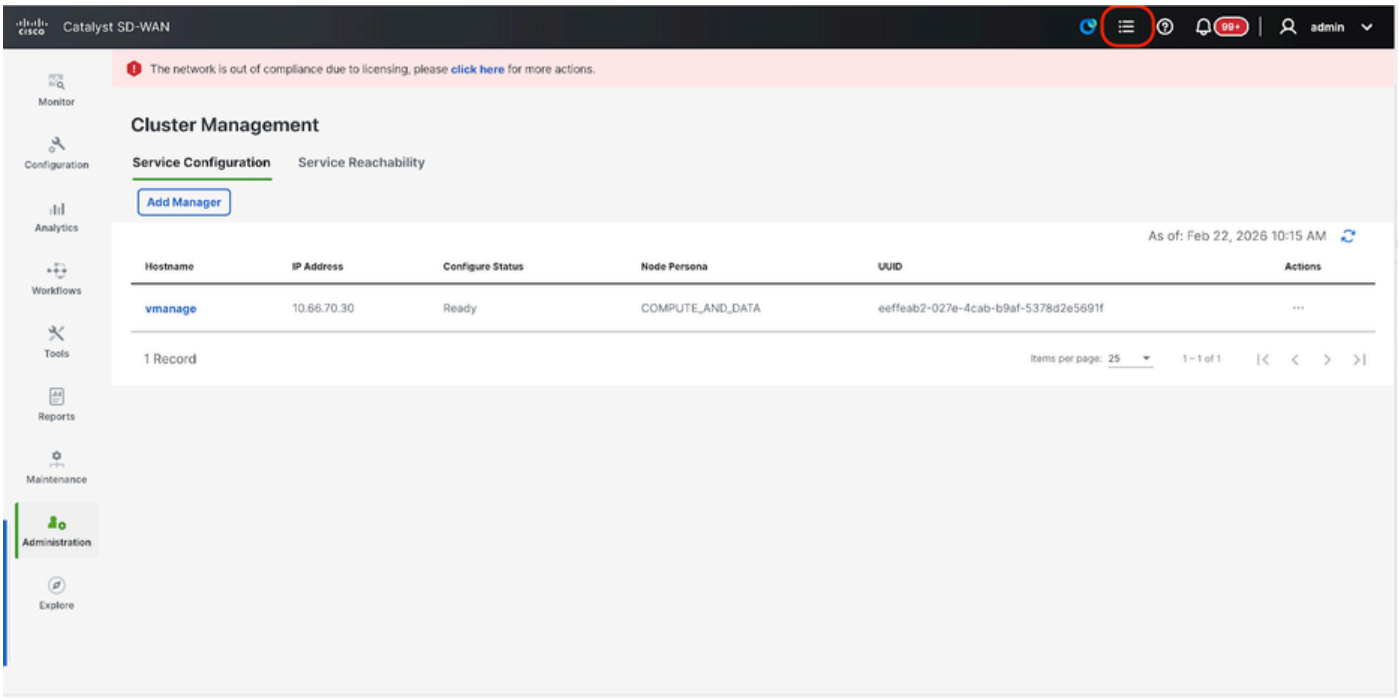
Bouw het vManage-cluster

- Navigeer op de webUI van vManage-1 naar Beheer > Clusterbeheer, in de sectie Serviceconfiguratie,
- Klik op Add Manager, er verschijnt een pop-upvenster:





- Kies de Node-persona op basis van de persona-configuraties die zijn uitgevoerd terwijl de vManage – 2-node werd gesponnen.
- Voer de serviceinterface van IP vManage-2 in onder IP-adres voor beheer
- Voer de gebruikersnaam en het wachtwoord in, dat dezelfde referenties zijn als die we in stap 6 hebben gebruikt.
- Schakel SDAVC in - Wordt niet aangevinkt omdat we het al op vManage-1 zouden hebben ingeschakeld
- Klik op Toevoegen.
- Nadat u dit bericht hebt geplaatst, start de vManage NMS-services opnieuw op de achtergrond voor vManage 1- en 2-knooppunten. De gebruikersinterface is niet beschikbaar voor een paar minuten van ongeveer 5 tot 10 minuten voor vManage 1 en 2.
- Gedurende deze periode is CLI-toegang van vManage 1 en 2 beschikbaar.
- Zodra de vManage-1 UI toegankelijk is, navigeert u naar Beheer > Clusterbeheer, zorgt u ervoor dat de IP-serviceinterface van zowel vManage wordt weergegeven onder IP-adres, Configuratiestatus is gereed en nodepersona correct wordt weergegeven.
- Switch-naar-service bereikbaarheid op dezelfde pagina en zorg ervoor dat alle services bereikbaar zijn voor beide vManage-knooppunten.
- Als we zien dat een van de services nog niet bereikbaar is, wacht dan even. Meestal duurt het ongeveer 5 tot 10 minuten.
- U kunt de status van het proces voor het toevoegen van clusters controleren in de takenlijst die beschikbaar is in de rechterbovenhoek van de vManage-gebruikersinterface.



- U kunt opzoeken naar de actieve takenlijst en als de taak nog steeds wordt vermeld onder de actieve takenlijst, geeft dit aan dat de taak nog niet is voltooid.
- U kunt op de taak klikken om de voortgang van hetzelfde te controleren. Als de taak niet wordt vermeld onder de lijst Actieve taken, switch dan naar Voltooid en zorg ervoor dat de taak succesvol is afgerond.
- Pas nadat deze punten zijn gevalideerd, gaat u verder met de volgende stap.

Met deze punten moet rekening worden gehouden voordat het volgende knooppunt aan het cluster wordt toegevoegd:

Controleer deze punten op alle UI's van de vManage-knooppunten die tot nu toe aan het cluster zijn toegevoegd:

- Navigeer naar Monitor > Overzicht van de vManage-gebruikersinterface en zorg ervoor dat het aantal vManage-knooppunten correct wordt weergegeven en bereikbaar is, afhankelijk van het aantal knooppunten dat aan het cluster is toegevoegd.

- Navigeer naar Beheer > Clusterbeheer en zorg ervoor dat de IP-serviceinterface van zowel vManage wordt weergegeven onder IP-adres, Configuratiestatus is gereed en nodepersona correct wordt weergegeven.
- Switch-naar-service bereikbaarheid gedeelte op dezelfde pagina en zorg ervoor dat alle services bereikbaar zijn voor zowel de vManage-knooppunten.

- Telkens wanneer een node aan het cluster wordt toegevoegd, worden de NMS-services van alle nodes in het cluster opnieuw gestart, waardoor de UI van al die nodes enige tijd onbereikbaar wordt.
- Afhankelijk van het aantal knooppunten in het cluster kan het langer duren voordat de gebruikersinterface een back-up heeft gemaakt en alle services bereikbaar zijn.
- U kunt de taak controleren onder Taaklijst die beschikbaar is in de rechterbovenhoek van de vManage UI.

- Op de vManage UI van elk knooppunt dat aan het cluster is toegevoegd, moeten we alle routers, sjablonen en beleidsregels zien als ze beschikbaar waren in vManage-1.
- Als die configuraties niet aanwezig waren op vManage-1, moeten de vBonds- en vSmarts-configuraties die zijn toegevoegd aan vManage-1 en ook de configuraties Beheer > Instellingen voor Organisatienaam, vBond, Certificaatautorisatie worden weergegeven op de rest van de vManage-knooppunten die aan het cluster zijn toegevoegd.
- Herhaal dezelfde stappen voor de overige vManage-knooppunten.

Stap 4: Config-DB Backup/Restore

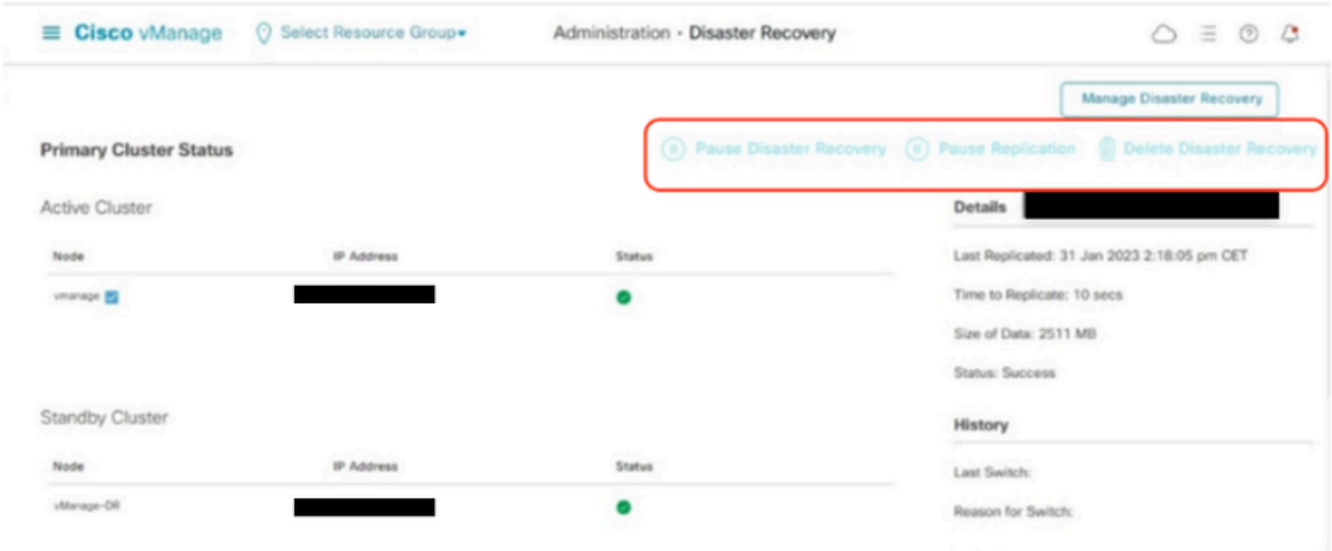
Configuratie-db-back-up en terugzetbewerkingen op een andere vManage-node verzamelen

---

Opmerking: Als u back-ups van de configuratiedatabase verzamelt van het bestaande vManage-cluster waarvoor Disaster Recovery is ingeschakeld, moet u ervoor zorgen dat deze worden verzameld nadat de Disaster Recovery op die node is gepauzeerd en verwijderd.

Bevestig dat er geen doorlopende Disaster Recovery-replicatie is. Navigeer naar Beheer > Disaster Recovery en Zorg ervoor dat de status Succesvol is en niet in een tijdelijke staat zoals Import Pending, Export Pending of Download Pending. Als de status niet succesvol is, neemt u contact op met Cisco TAC en zorgt u ervoor dat replicatie succesvol is voordat u doorgaat met het pauzeren van de Disaster Recovery.

Pauzeer eerst de Disaster Recovery en zorg ervoor dat de taak is voltooid. Verwijder vervolgens de Disaster Recovery en bevestig dat de taak is voltooid.



Neem contact op met Cisco TAC om ervoor te zorgen dat de Disaster Recovery met succes wordt opgeruimd.

Configuratie-DB-back-up verzamelen:

- In de SD-WAN-fabric die momenteel wordt gebruikt, kunt u configuratie-db-back-up genereren vanuit het vManage-cluster.
- Houd er rekening mee dat we configuratie-db-back-up alleen moeten genereren op één node van het vManage-cluster, die de configuratie-db-leider is.

- Voor standalone vManage is dat vManage zelf de leider op het gebied van configuratie-db.
- Identificeer in het vManage-cluster de configuratie-db-leiderknooppunt met behulp van de diagnostiek command request nms configuration-db.U kunt deze opdracht uitvoeren op alle knooppunten van het vManage-cluster met drie knooppunten.
- In een cluster met 6 knooppunten moet u deze opdracht uitvoeren op de vManage-knooppunten waar configuratie-db is ingeschakeld om de leader-node te identificeren. Navigeer naar Beheer > Clusterbeheer om hetzelfde te controleren:
- Zoals we in de schermafbeelding zien, hebben de knooppunten die zijn geconfigureerd met persona COMPUTE_AND_DATA configuratie-db uitgevoerd.

U kunt hetzelfde controleren met de opdracht requestNmsconfiguration-dbstatus op vManageCLI. De output is zoals getoond

```
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#
```

- Zodra u het commando uitvoertVraag NMS Configuration-DB Diagnostics aan op deze knooppunten, de uitvoer is als volgt:
- Zoek naar het gemarkeerde veld voor "IsLeader". Als het is ingesteld op 1, geeft dit aan dat node de leader node is en we kunnen daar configuratie-db back-up van verzamelen.

```
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     .
```

Gebruik deze opdracht om de configuratie-db-back-up te verzamelen van de geïdentificeerde configuratie-db leader vManage-node.

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

De verwachte output is als volgt:

```
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#
```

- Noteer de configuratie-db-referenties als deze is bijgewerkt.
- Als u de configuratie-db-referenties niet kent, neemt u contact op met TAC om de configuratie-db-referenties op te halen uit de bestaande vManage-knooppunten.
- Standaardconfiguratie-db-referenties zijn gebruikersnaam: neo4j en wachtwoord: wachtwoord

Configuration-db Backup terugzetten naar een andere vManage-node

Kopieer de configuratie-db back-up naar /home/admin/ directory van vManage met behulp van SCP.

Voorbeeld van scp-opdrachtuitvoer:

```
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
```

Om de configuratie-db back-up te herstellen, moeten we eerst de configuratie-db referenties configureren. Als uw configuratie-db-referenties standaard zijn (neo4j / wachtwoord), kunnen we deze stap overslaan.

Als u configuratie-db-referenties wilt configureren, gebruikt u de opdracht request nms configuration-db update-admin-user. Gebruik de gebruikersnaam en het wachtwoord van uw keuze.

Houd er rekening mee dat de toepassingsserver van vManage opnieuw wordt gestart. Hierdoor wordt de gebruikersinterface van vManage korte tijd ontoegankelijk.

```
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#
```

Post waarin we kunnen doorgaan met het herstellen van de configuratie-db back-up:

We kunnen de opdracht request nms configuration-db restore path /home/admin/< > gebruiken om de configuratie-db te herstellen naar de nieuwe vManage:

```
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
```

Zodra de configuratie-db is hersteld, moet u ervoor zorgen dat de vManage UI toegankelijk is. Wacht ongeveer 5 minuten en probeer vervolgens toegang te krijgen tot de gebruikersinterface.

Als u eenmaal met succes bent ingelogd op de gebruikersinterface, moet u ervoor zorgen dat de lijst met Edge-routers, het sjabloon, het beleid en alle andere configuraties die aanwezig waren op uw vorige of bestaande vManage-gebruikersinterface, worden weergegeven in de nieuwe vManage-gebruikersinterface.

Stap 5: Disaster Recovery inschakelen in een vManage-cluster

Belangrijke voorcontroles

Er moeten twee afzonderlijke vManage-clusters met drie knooppunten worden geconfigureerd en operationeel zijn om door te gaan met noodherstel. Op het actieve cluster moeten validators en controllers zijn geïnstalleerd. Als u validators en controllers op de DR-site hebt staan, moeten deze ook op het actieve cluster worden geïnstalleerd en niet op het DR vManage-cluster.

Cisco raadt u aan om aan de volgende vereisten te voldoen voordat u Disaster Recovery registreert:

- Zorg ervoor dat de primaire en de secundaire node bereikbaar zijn via HTTPS op een transport VPN (VPN 0).
- Zorg ervoor dat Cisco vSmart Controllers en Cisco vBond Orchestrators op de secundaire setup zijn aangesloten op de primaire setup.
- Zorg ervoor dat de primaire node en de secundaire node van Cisco vManage dezelfde Cisco vManage-versie gebruiken.
- Out-of-band clusterinterface (service-interface) in VPN 0.
- Voor elke vManage-instantie in een cluster is een derde interface (clusterkoppeling) vereist naast de interfaces die worden gebruikt voor VPN 0 (transport) en VPN 512 (beheer).
- Deze interface wordt gebruikt voor communicatie en synchronisatie tussen de vManage-servers in het cluster.
- Deze interface moet ten minste 1 Gbps zijn en een latentie van 4 ms of minder hebben. Een interface van 10 Gbps wordt aanbevolen.
- Beide vManage-knooppunten moeten elkaar via deze interface kunnen bereiken: of het nu een laag 2-segment is of via laag 3-routering.
- In elke vManage moet deze interface in de GUI worden geconfigureerd als een clusterinterface (Beheer > Clusterbeheer – geef uw eigen IP-adres, gebruiker en wachtwoord voor de out-of-band clusterinterface aan).
- Om Cisco vManage-knooppunten in staat te stellen met elkaar te communiceren via datacenters, schakelt u de TCP-poorten 8443 en 830 in op uw firewalls voor datacenters.
- Zorg ervoor dat alle services (toepassingsserver, configuratie-db, berichtenserver, coördinatieserver en statistiek-db) zijn ingeschakeld op beide Cisco vManage-knooppunten.
- Verdeel alle controllers, inclusief Cisco vBond Orchestrators, over zowel primaire als secundaire datacenters. Zorg ervoor dat deze controllers bereikbaar zijn voor Cisco vManage-knooppunten die over deze datacenters zijn verdeeld. De controllers maken alleen verbinding met de primaire Cisco vManage-node.
- Zorg ervoor dat er geen andere bewerkingen worden uitgevoerd in de actieve (primaire) en de standby (secundaire) Cisco vManage-node. Zorg er bijvoorbeeld voor dat er geen servers

bezig zijn met het upgraden of koppelen van sjablonen aan apparaten.

- Schakel de Cisco vManage HTTP/HTTPS-proxyserver uit als deze is ingeschakeld. Zie HTTP/HTTPS-proxyserver voor Cisco vManage-communicatie met externe servers. Als u de proxyserver niet uitschakelt, probeert Cisco vManage een noodherstelcommunicatie tot stand te brengen via het IP-adres van de proxy, zelfs als de IP-adressen van Cisco vManage out-of-band clusters direct bereikbaar zijn. U kunt de Cisco vManage HTTP/HTTPS-proxyserver opnieuw inschakelen nadat de registratie voor Disaster Recovery is voltooid.
- Voordat u het registratieproces voor noodherstel start, gaat u naar het venster Extra > Netwerk opnieuw ontdekken op het primaire Cisco vManage-knooppunt en herontdekt u de Cisco vBond Orchestrators.

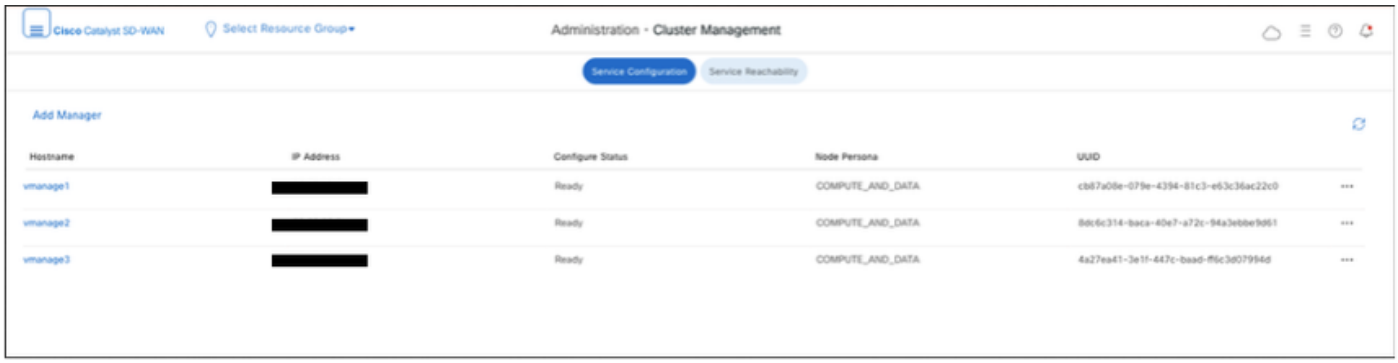
Configuraties

Raadpleeg deze link voor meer informatie over vManage Disaster Recovery.

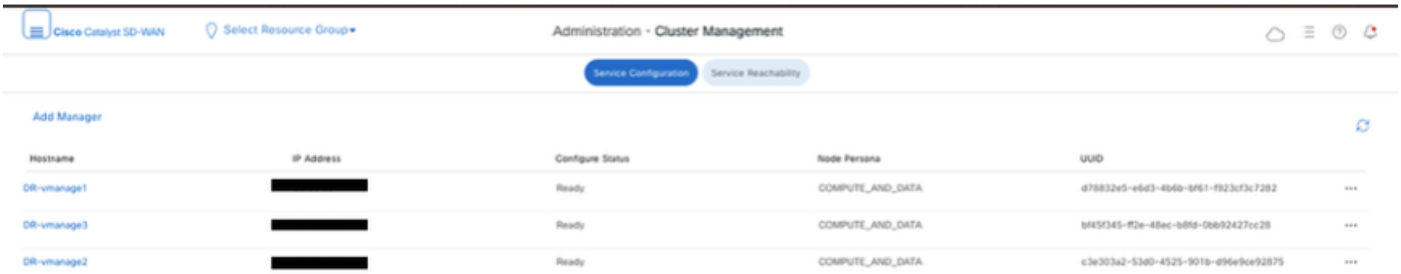
De twee afzonderlijke clusters met drie knooppunten zijn al gemaakt, ervan uitgaande dat elke SD-WAN-beheerder een minimale configuratie heeft en dat het certificeringsgedeelte is voltooid.

Navigeer naar Beheer > Clusterbeheer op beide clusters en controleer of alle knooppunten klaar zijn.

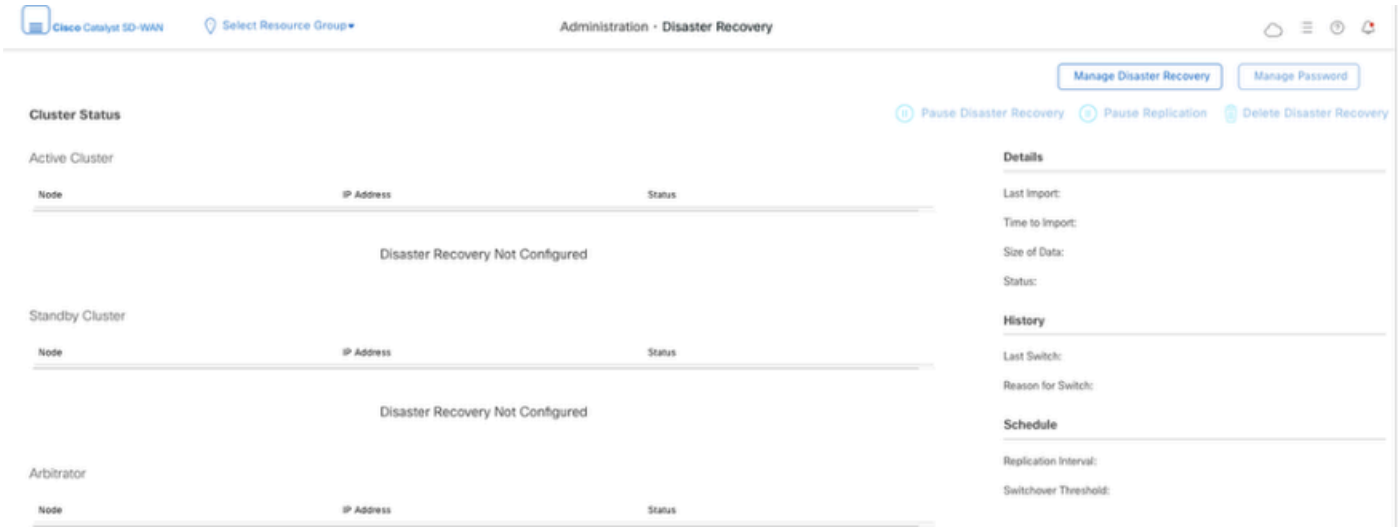
DC vManage



DR vmanage



Navigeer naar Beheer>Disaster Recovery of Primary vManage Cluster. Klik op Disaster Recovery beheren.



Vul in het pop-upvenster de gegevens voor zowel primaire als secundaire vManage in.

De aan te geven IP-adressen zijn de out-of-band clusterinterfaces en IP-adressen. Gebruik bij voorkeur het IP-adres van de VPN 0-serviceinterface van vManage-1 in elk van de clusters.

De referenties moeten afkomstig zijn van een netadmin-gebruiker en mogen niet worden gewijzigd zodra de DR is geconfigureerd, tenzij deze wordt verwijderd. Er kan een afzonderlijke vManage-referenties voor lokale gebruikers voor Disaster Recovery worden gebruikt. We moeten ervoor zorgen dat de lokale vManage-gebruiker deel uitmaakt van de netadmin-groep. Zelfs de admin-inloggegevens kunnen hier worden gebruikt.

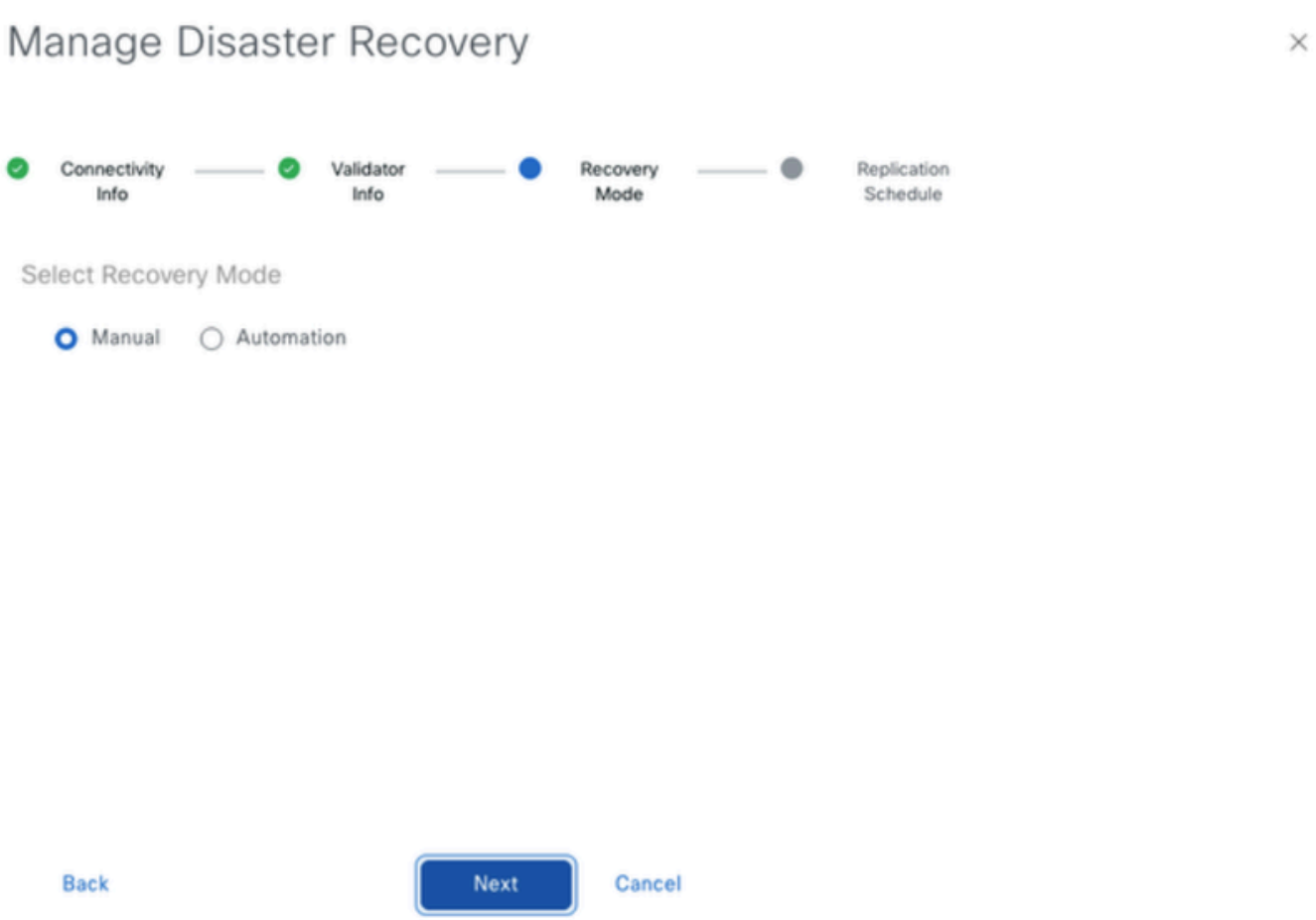
Klik op Volgende zodra u deze hebt ingevuld.

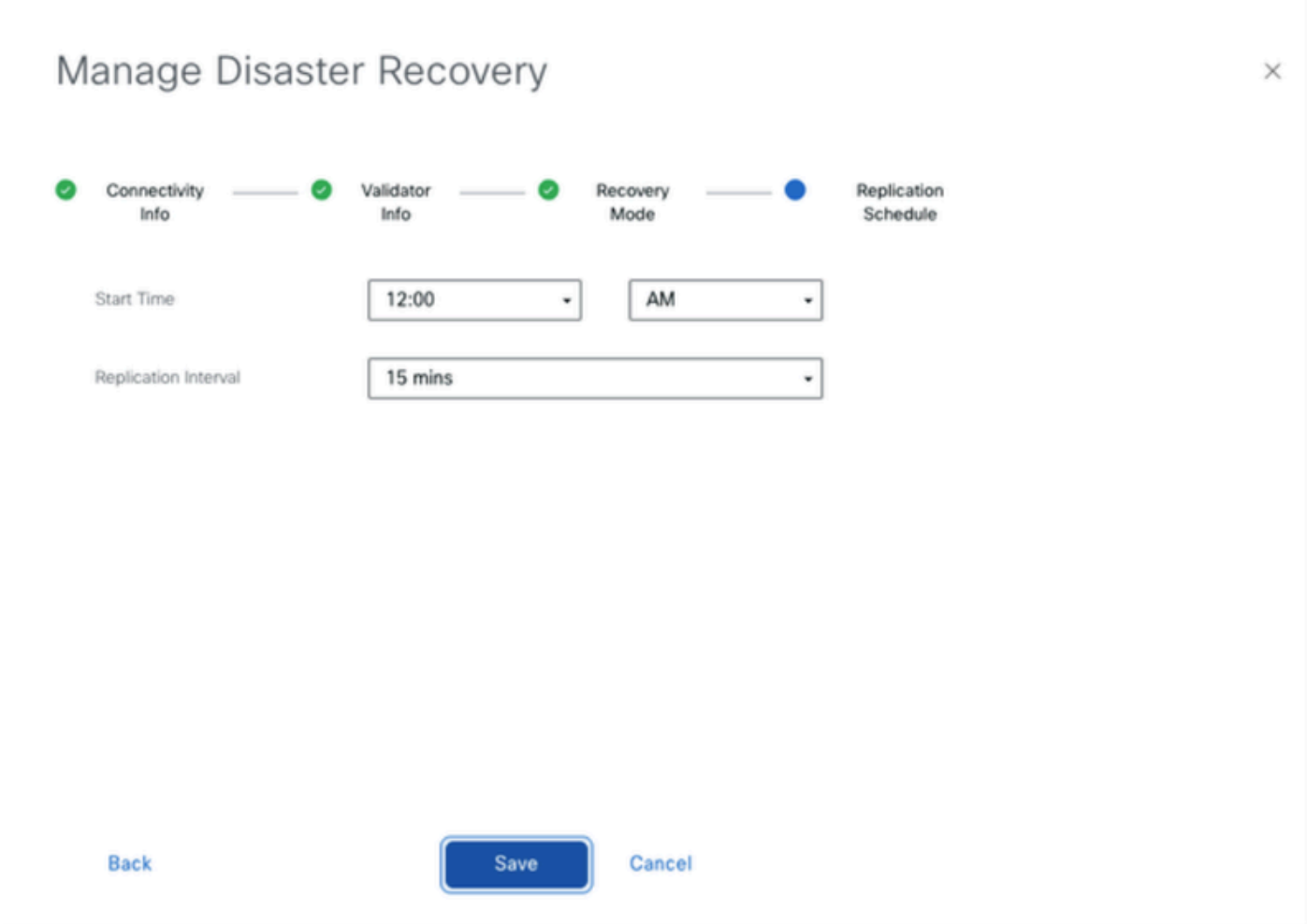
- Vul de gegevens van de vBond-controllers in.

De vBond-controllers moeten bereikbaar zijn via het opgegeven IP-adres via Netconf.

Klik op Volgende zodra u deze hebt ingevuld.

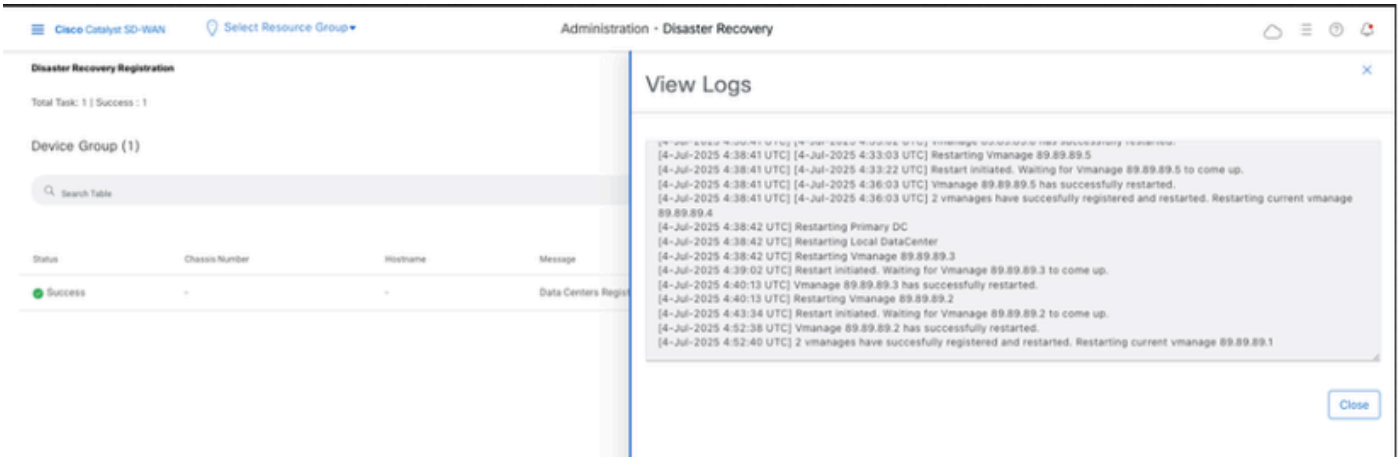
- Kies in de herstelmodus Handmatig. De automatische modus is uitgeschakeld. Klik op Next (Volgende).


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



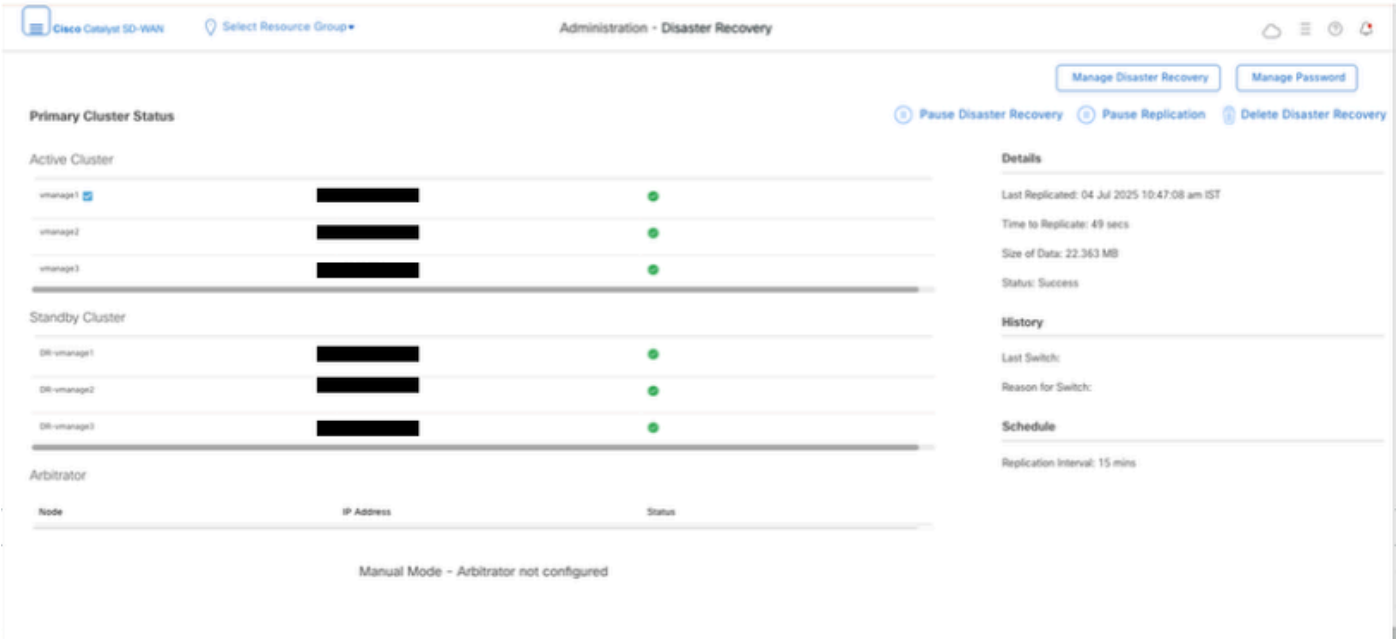
Stel de waarde in en klik op Opslaan.

- De registratie van DR begint nu. Klik op de knop Vernieuwen om de status en de voortgangslogboeken handmatig te vernieuwen. Dit proces kan tot 20-30 minuten duren.



Verificatie

Navigeer naar Beheer>Disaster Recovery om de status Disaster Recovery te bekijken en te zien wanneer de gegevens de laatste keer zijn gerepliceerd.



Opmerking: Replicatie kan enkele uren duren, afhankelijk van de grootte van de database. Bovendien kan het enkele cycli vereisen om een succesvolle replicatie te bereiken.

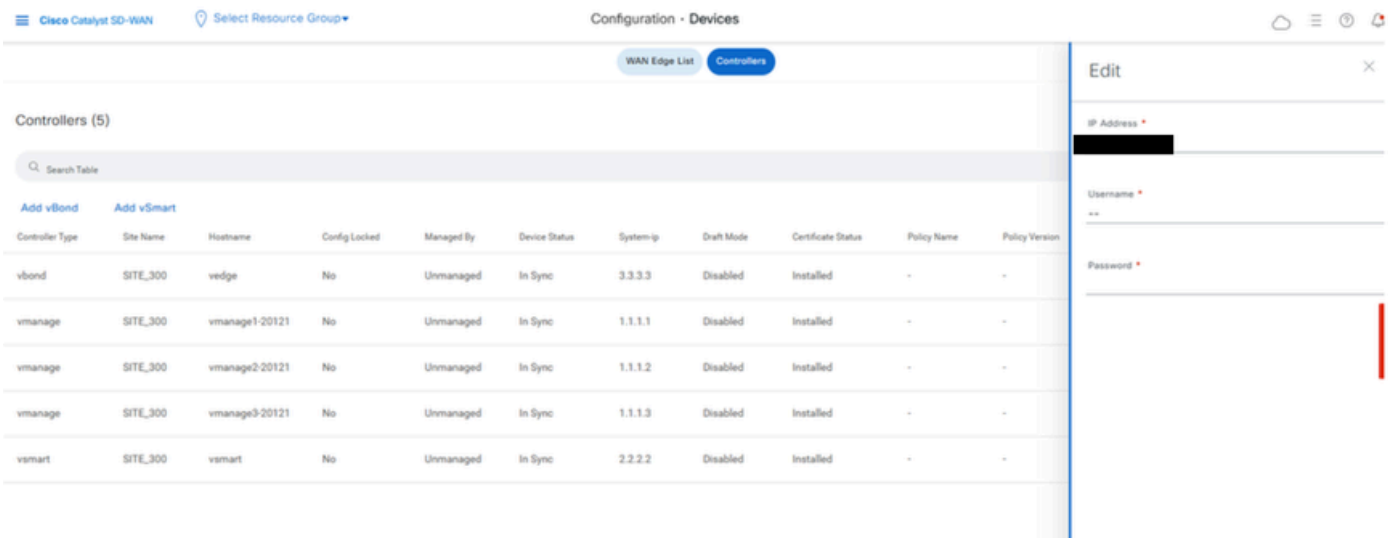
Stap 6: Reauthenticatie van controllers en ongeldigverklaring van oude controllers

Zodra configuratie-db is hersteld, moeten we alle nieuwe controllers (vmanage/vsmart/vbond) in de fabric opnieuw verifiëren

Opmerking: Als de IP-interface die wordt gebruikt om opnieuw te verifiëren de tunnelinterface IP is, moet u ervoor zorgen dat de NETCONF-service is toegestaan op de tunnelinterface van de vManage, vSmart en vBond en ook op de firewalls langs het pad. De firewallpoort die moet worden geopend is TCP-poort 830 als bidirectionele regel van DR-cluster naar alle vBonds en vSmarts.

Klik in vmanage UI op Configuration > Devices > Controllers

- Klik op de drie puntjes bij elke controller en klik op Bewerken



- Vervang het ip-adres (system-ip van de controller) door het transport vpn 0 (tunnel interface) ip-adres .Voer de gebruikersnaam en het wachtwoord in en klik op opslaan
- Doe hetzelfde voor alle nieuwe controllers in de stof

Synchroniseer de Root-cert-keten

Als alle controllers zijn geïnstalleerd, voert u deze stap uit:

Voer op elke Cisco SD-WAN Manager-server in het nieuw actieve cluster de volgende acties uit:

Voer deze opdracht in om het rootcertificaat te synchroniseren met alle Cisco Catalyst SD-WAN-apparaten in het nieuw actieve cluster:

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

Voer deze opdracht in om de Cisco SD-WAN Manager UUID te synchroniseren met de Cisco SD-WAN Validator:

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

Zodra de fabric is hersteld en de controle- en bfd-sessies zijn ingesteld voor alle randen en controllers in de fabric, moeten we de oude controllers (vmanage/vsmart/vbond) van de gebruikersinterface ongeldig maken

- Klik op Configuratie > Apparaten > Certificaten in vmanage UI
- Klik op Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Ongeldig maken
- Klik op verzenden naar vbond
- Klik in vmanage UI op Configuration > Devices > Controllers
- Klik op de drie puntjes in de buurt van de controller (vmanage/vsmart/vbond) van de oude stof. Klik op Verwijderen

Controles achteraf

Deze postcontroles zijn van toepassing op alle implementatiecombinaties.

Cloud Edge-routers opnieuw activeren:

- Als C8000v deel uitmaakt van de overlay en is ondertekend met vmanaged, moeten ze opnieuw worden geverifieerd, dat wil zeggen:

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

        token
```

- Controleverbindingen en BFD-sessies bevestigen
- Bevestigen dat het toepassingsverkeer van begin tot eind verloopt
- Als er wijzigingen zijn aangebracht in de port-hop voordat de stof opnieuw op de randen wordt gebouwd, moeten deze worden teruggedraaid

- Controleer of de objecten worden weergegeven zoals verwacht:
    - Sjablonen
    - Beleid
    - Apparaatpagina (beide tabbladen)WAN vEdge List en Controllers

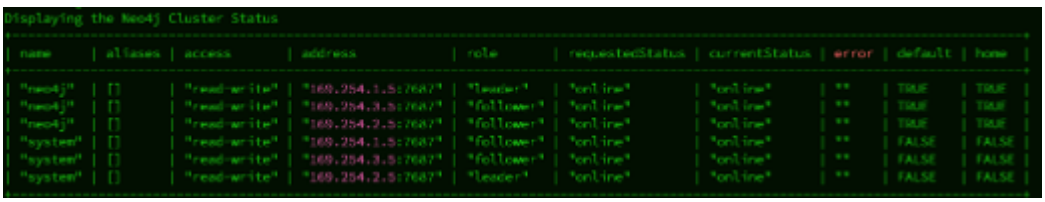
  vControles achteraf beheren

- Toepasselijk voor vManage-knooppunten:

  Configuration-DB(Neo4j) controleert:

  Voer de opdracht "request nms configuration-db diagnostics" uit op alle vManage-knooppunten:

  1. Controleer voor Node online en Leadership status: (niet beschikbaar voor alle versies)



"Neo4j" moet 3 knooppunten online tonen en 1 leider en 2 volgers. "systeem" moet ook 3 knooppunten online en 1 leider en 2 volgers weergeven, maar omdat dit niet de standaard Db is, is de standaardvlag vals. Als er minder dan 3 vermeldingen in elke neo4j en systeem betekent knooppunt viel uit cluster. Neem contact op met Cisco TAC om hetzelfde probleem op te lossen.

2. Controleer of een node "quarantaine" is.

```
##############################################
##############################################
Running quarantine check
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Check if Neo4j Nodes are Quarantined
None of the neo4j nodes is quarantined
None of the neo4j nodes is quarantined
None of the neo4j nodes is quarantined
##############################################
```

Geen van de knooppunten moet in quarantaine-toestand zijn.

3. De validatie van het schema moet "succesvol" zijn.

```
##############################################
Running schema violation pre-check script
WARNING: sun.reflect.Reflection.getCallerClass is not supported. This will impact performance.
Validating Schema from the configuration-db
Successfully validated configuration-db schema
written to file /opt/data/containers/mounts/upgrade-coordinator/schema.json
Contents of /opt/data/containers/mounts/upgrade-coordinator/schema.json:
{
  "check_name": "Validating configuration-db admin names",
  "check_result": "SUCCESSFUL",
  "check_analysis": "Successfully validated configuration-db schema",
  "check_action": ""
}
##############################################
##############################################
```

4. Verzamel een configuratie-db back-up met behulp van de opdracht "Request NMS Configuration-db Diagnostics" en zorg ervoor dat het succesvol is.

```
vmanage_2013# request nms configuration-db backup path /opt/data/backup/9thSepBackup.tar.gz
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/9thSepBackup.tar.gz.tar.gz
sha256sum: 9d43addcf6c43f18c32b833295a6318fa0a63a7bf7456965140dcb9a61118b5e
Removing the temp staging dir :/opt/data/backup/staging
vmanage_2013#
```

Als er inconsistenties of fouten worden gezien, neemt u contact op met Cisco TAC voor probleemoplossing.

Als alternatief kunnen we deze API-aanroepen uitvoeren om de vmanage-knooppuntstatus voor een cluster te bevestigen (voor alle COMPUTE+DATA-knooppunten) - werkt alleen op versie 10 .12 en later

```
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
```

Zorg ervoor dat in een cluster slechts één leider is voor zowel neo4j als het systeem en rust als volgers .Zorg ervoor dat alle knooppunten online zijn .Als u 3 knooppuntencluster hebt (alle drie zijn COMPUTE+DATA), moet er slechts één leider zijn voor zowel neo4j als het systeem .Elke afwijking, moet u contact opnemen met TAC

5. Controleer op /var/log/kern.log of er schijf-, Mem-, IO-fouten zijn. Dit moet worden gecontroleerd op alle vManage-knooppunten.

6.Controleer de stap wanneer u een nieuw cluster vormt voor vmanage die geen CC tussen elke node heeft
Voer ssh uit als vmanage-admin van node 1 naar andere nodes cluster ip en vice versa, om te controleren of de publieke sleutel is uitgewisseld en het wachtwoord minder ssh werkt
[Toestemmingstoken is vereist voor de hier weergegeven stappen]

```
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:
```

Als de uitvoer vraagt om het wachtwoord in te voeren, neem dan contact op met TAC

Controleur Postcontroles:

Toepasbaar voor alle SD-WAN-controllers (vBond, vManage, vSmart):

Voer de opdrachten uit op alle controllers in de overlay en controleer of de UUID en serienummers van vManage die worden weergegeven, geldig zijn voor de huidige structuur:

vBond-opdrachten:

Orchestrator valid-vSmarts weergeven

Orchestrator valid-vmanage-id weergeven

vManage/vSmart-opdrachten:

Besturingselement geldige v-smarts weergeven

Validig besturingselement-vManage-ID weergeven

Houd er rekening mee dat de uitvoer van geldige vSmarts-besturingselementen de serienummers van zowel vSmarts- als vManage-knooppunten bevat.

Vergelijk het met de functies die in vManage UI worden weergegeven. Navigeer naar de sectie Configuratie > Certificaten > Controllers.

Als er extra items worden weergegeven voor het UUID/serienummer die momenteel niet aan boord van de verbinding zijn, moeten we deze verwijderen. U kunt hiervoor contact opnemen met Cisco TAC.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.