Ricostruzione del fabric Catalyst SD-WAN

Sommario

Introduzione

Questo documento descrive come ricostruire una struttura Cisco SD-WAN, incluso il backup e il ripristino delle configurazioni dei controller per diverse implementazioni.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Software Cisco Defined Wide Area Network (SD-WAN)
- Cisco Software Central
- Scaricare il software Controller da software.cisco.com

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prerequisiti prima della ricostruzione dell'infrastruttura

- È necessario configurare il nuovo set di IP sistema e ID sito per il nuovo fabric per i controller
- Assicurarsi che siano presenti regole firewall per consentire la comunicazione tra i controller e i bordi
- Notare il nome utente e la password neo4j(configuration-db) (devono essere gli stessi in tutti i nodi vManage di un cluster)
- Disabilitare l'hop della porta su tutti i bordi
- Aumentare i timer di riavvio a 7 giorni

- Cancellazione degli allarmi negli strumenti 3rdparty prima della migrazione
- I dati relativi alle statistiche cronologiche (allarmi, eventi, statistiche dei dispositivi e così via) vengono persi a meno che non sia stata precedentemente configurata l'esportazione delle statistiche in un server esterno, ad esempio vAnalytics
- Se Cloud onRamp è configurato, assicurarsi di avere la raggiungibilità al c8000v distribuito nel cloud prima dell'inizio di questa attività
- Se SDAVC è abilitato sul vecchio fabric, verificare che il nuovo fabric lo abbia abilitato (per il cluster, deve essere abilitato solo su un singolo nodo)
- Il ripristino del database di configurazione è supportato solo sulla stessa versione del fabric originale
- Confermare la persona utilizzata per i controller. Supportiamo COMPUTE_DATA e la persona DATA (dettagli in ciascuna sezione)
- Per le CA dell'organizzazione (enterprise), è necessario utilizzare il certificato radice rilasciato dalla CA dell'organizzazione (enterprise), utilizzato nella sovrapposizione esistente, e il certificato è firmato utilizzando il server CA dell'organizzazione (enterprise) e installato per tutti i controller tramite interfaccia utente

Opzioni di implementazione

Distribuzione vManage

- Indipendente (1 nodo)
- Cluster (a 3 o 6 nodi)

Opzioni DR

- Nessun ripristino di emergenza
- DR. a nodo singolo
- Cluster DR in standby (attivato manualmente/dall'amministratore)

Nota: Per ulteriori dettagli sul tipo di ripristino di emergenza, fare riferimento a questo collegamento

---

Combinazioni:

N.	Installazione di vManage	Opzione DR
1	Indipendente (1 nodo)	Nessun ripristino di emergenza
2	Indipendente (1 nodo)	DR. a nodo singolo
3	Cluster (a 3 o 6 nodi)	Nessun ripristino di emergenza
4	Cluster (a 3 o 6 nodi)	Cluster DR in standby

Operazioni comuni a tutte le combinazioni

Questi passaggi sono comuni a tutte le combinazioni di distribuzione. Coprono il processo di attivazione delle istanze di VM e di applicazione della configurazione CLI di base. In ogni sezione combinata viene indicato il numero di istanze da distribuire e i passaggi aggiuntivi da completare.

Installare e attivare i controller SD-WAN (Manager, Validator, Controller)

Nota: Cisco ha rinominato alcuni termini, quindi sono intercambiabili. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst Controller

---

Scaricare i file OVA per i controller SD-WAN dalla pagina di download del software Cisco qui:

- Scegliere vEDGE Cloud e scaricare vBond OVA per la versione software richiesta.
- Scegliere vManage software e scaricare vManage OVA per la versione software richiesta.
- Scegliere vSmart software e scaricare vSmart OVA per la versione software richiesta.

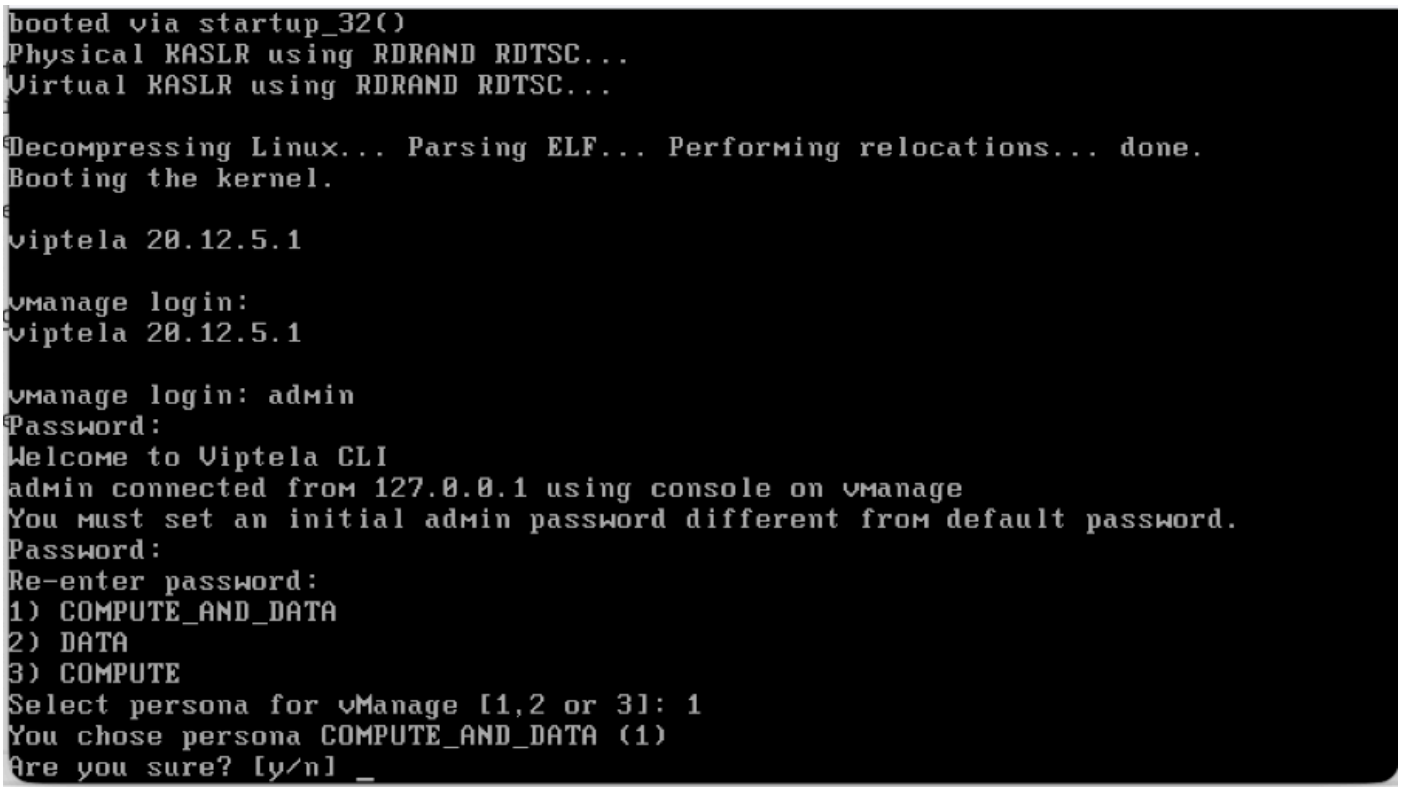
Nota: Sulle piattaforme ESXi/cloud, eseguire lo spin up dei controller vSmart, vBond e vManage utilizzando il file OVA. Fare riferimento al documento collegato e assicurarsi che CPU, RAM e dischi siano allocati in misura sufficiente a tutti i controller a seconda del tipo di distribuzione SD-WAN. Fare clic qui per ulteriori informazioni. Assicurarsi di assegnare il disco secondario al nodo vManage come indicato nella colonna Dimensione memoria* nella guida al calcolo collegata.

Visualizza un nodo di Cisco Manager

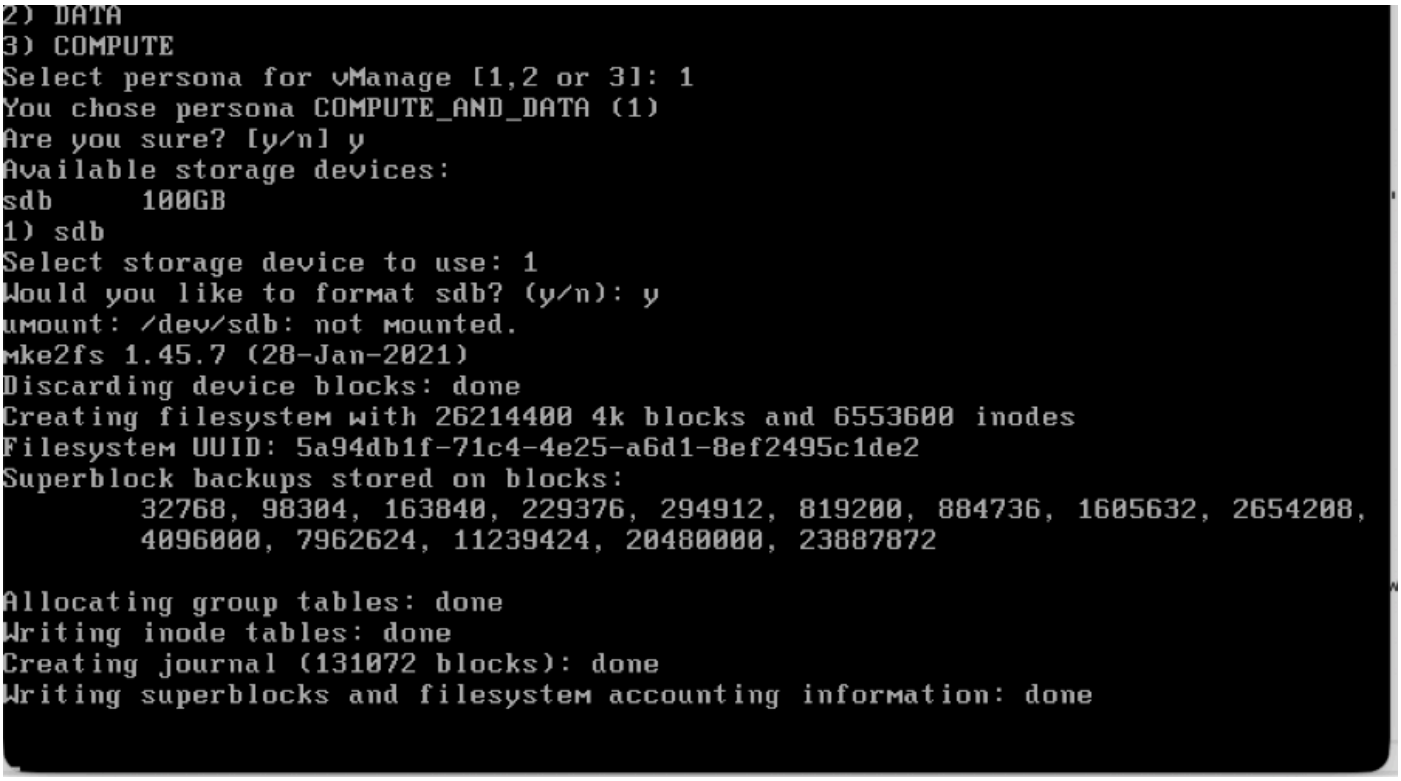
- Una volta implementata la VM Cisco Manager o vManage e dopo aver reso accessibile la console di gestione, attendere il completamento dell'avvio. Una indicazione è che vediamo un sistema di messaggi pronto e richiede il nome utente e la password.
- Immettere il nome utente delle credenziali utente predefinite come admin e la password come admin. Viene richiesto all'utente di cambiare la password, impostare la password necessaria per l'amministratore utente in base alla propria scelta.
- Viene quindi richiesto all'utente di selezionare la persona. Si tratta di un passaggio critico se si intende disporre di un cluster vManage. Scegliere l'utente come illustrato di seguito:

```
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
```

Esempio:scegliere 1 per COMPUTE_AND_DATA



Scegliere il disco secondario come illustrato:



- Scegliere il disco secondario e digitare Y per confermare.
- Cisco Manager viene ricaricato. Una volta avviato, immettere il nome utente e la password con la nuova password appena configurata.

```
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#
```

- È possibile configurare l'interfaccia di gestione VPN 512 per abilitare l'accesso di gestione fuori banda al controller.
- Usare il comando show interface | per controllare i VPN a cui sono attualmente mappate le interfacce.
- configurare le interfacce in modo appropriato.

Esempio

```
                              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#
```

Nota: È possibile fare riferimento alla configurazione dal vManage esistente e configurare qui lo stesso schema di indirizzi IP.

Configurazioni dell'interfaccia di gestione (VPN 512)

- Se è necessario spostare un'interfaccia dalla VPN 0 alla VPN 512, utilizzare questi comandi e configurare l'indirizzo IP sull'interfaccia

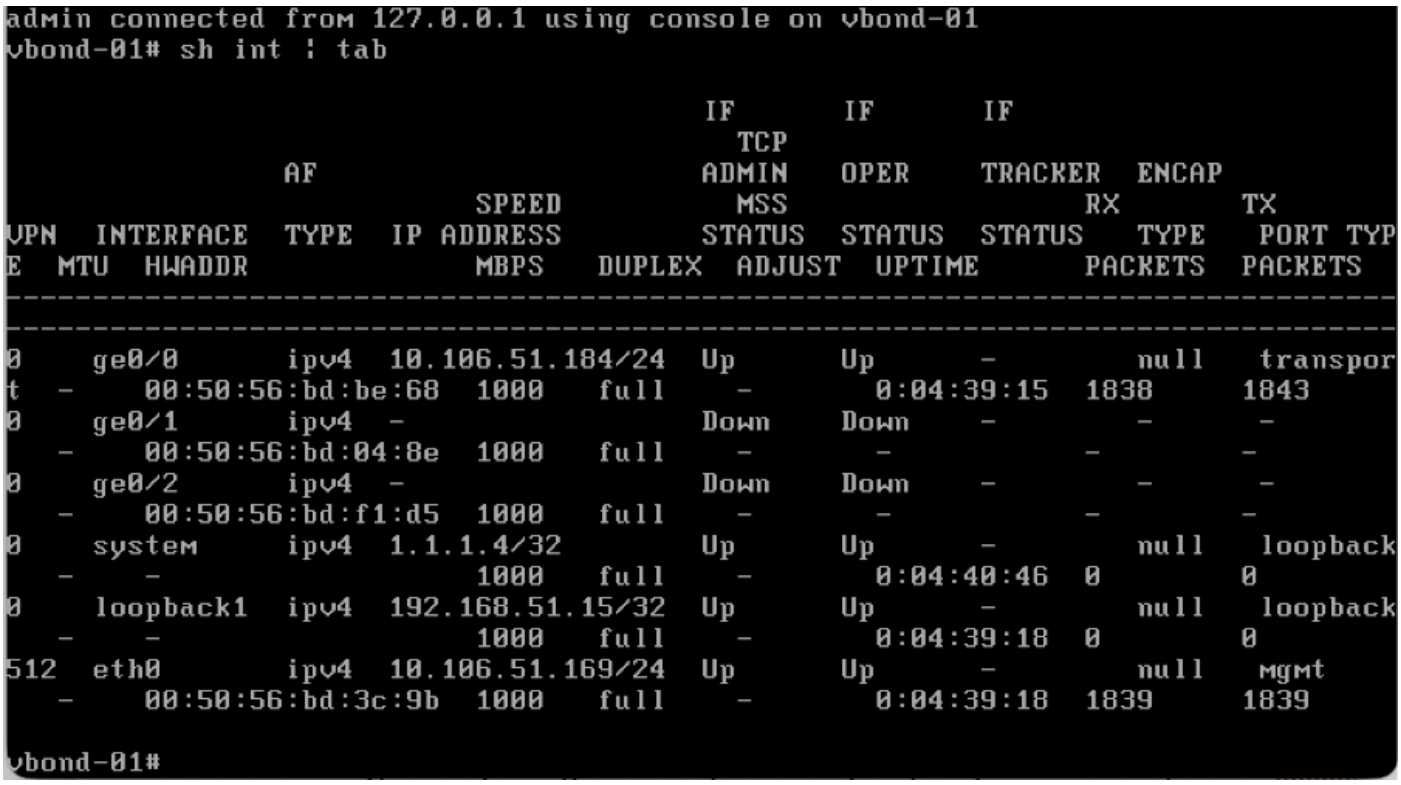
```
Conf t
vpn 0
 no interface eth0
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0



!
```

Visualizza la Convalida

- Sull'hypervisor, configurare il computer richiesto (CPU, RAM e disco) per il nodo vBond e accenderlo.
- Una volta che la console è accessibile, attendere che vBond si avvii completamente. Attendere il messaggio System Ready (Sistema pronto).
- Il sistema richiede quindi il nome utente e la password. Immettere le credenziali utente predefinite admin e password admin. Quindi, all'utente viene richiesto di modificare la password, impostare la password necessaria per l'amministratore utente in base alla propria scelta.
- È possibile configurare l'interfaccia di gestione VPN 512 per abilitare l'accesso di gestione fuori banda al controller.
- Usare il comando show interface | per controllare i VPN a cui sono attualmente mappate le interfacce.

- Configurare le interfacce di conseguenza.

Esempio:



```
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#
```

Nota: È possibile fare riferimento alla configurazione dal vBond esistente e configurare qui le stesse configurazioni.

Configurazioni dell'interfaccia di gestione (VPN 512)

- Se è necessario spostare un'interfaccia dalla VPN 0 alla VPN 512, utilizzare questi comandi e configurare l'indirizzo IP sull'interfaccia.

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




  no shutdown
 !
 ip route 0.0.0.0/0
```

```
!
commit
```

Attiva un nodo controller (vSmart)

- Eseguire gli stessi passaggi di Validator per visualizzare il nodo vSmart.
- Una volta configurato l'indirizzo IP VPN 512 su tutti i controller SD-WAN, è possibile accedervi utilizzando SSH sull'indirizzo IP VPN 512.

Configurazione CLI di base su tutti i controller

Una volta ottenuto l'accesso SSH a tutti i controller, configurare queste configurazioni CLI su ciascun controller.

Configurazione del sistema

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Nota: se si utilizza URL come indirizzo vBond, verificare di configurare gli indirizzi IP dei server DNS nella configurazione VPN 0 o di risolverli.

Configurazione interfaccia di trasporto (VPN 0)

Queste configurazioni sono necessarie su tutti i controller per abilitare l'interfaccia di trasporto utilizzata per stabilire le connessioni di controllo con i router e gli altri controller.

```
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
```

Nota: è possibile fare riferimento alle configurazioni del controller esistente e, se la configurazione è presente, è possibile aggiungerla ai nuovi controller.

Configurare il protocollo di controllo come TLS solo se è necessario che i router stabiliscano connessioni di controllo protette con i nodi vManage che utilizzano TLS. Per impostazione predefinita, tutti i controller e i router stabiliscono una connessione di controllo utilizzando DTLS. Si tratta di una configurazione opzionale richiesta solo sui nodi vSmart e vManage a seconda delle esigenze.

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

Combinazione 1: vManage standalone + senza ripristino di emergenza

Istanze necessarie:

- 1 vManage (COMPUTE_AND_DATA)
- 1 o più vBond
- 1 o più vSmart

Passaggi:

1. Visualizzare tutte le istanze utilizzando l'opzione Passi comuni (Common Steps)
2. Controlli preliminari
3. Configurazione di interfaccia utente, certificati e controller integrati vManage
4. Backup/ripristino di Config-db
5. Registra assegni

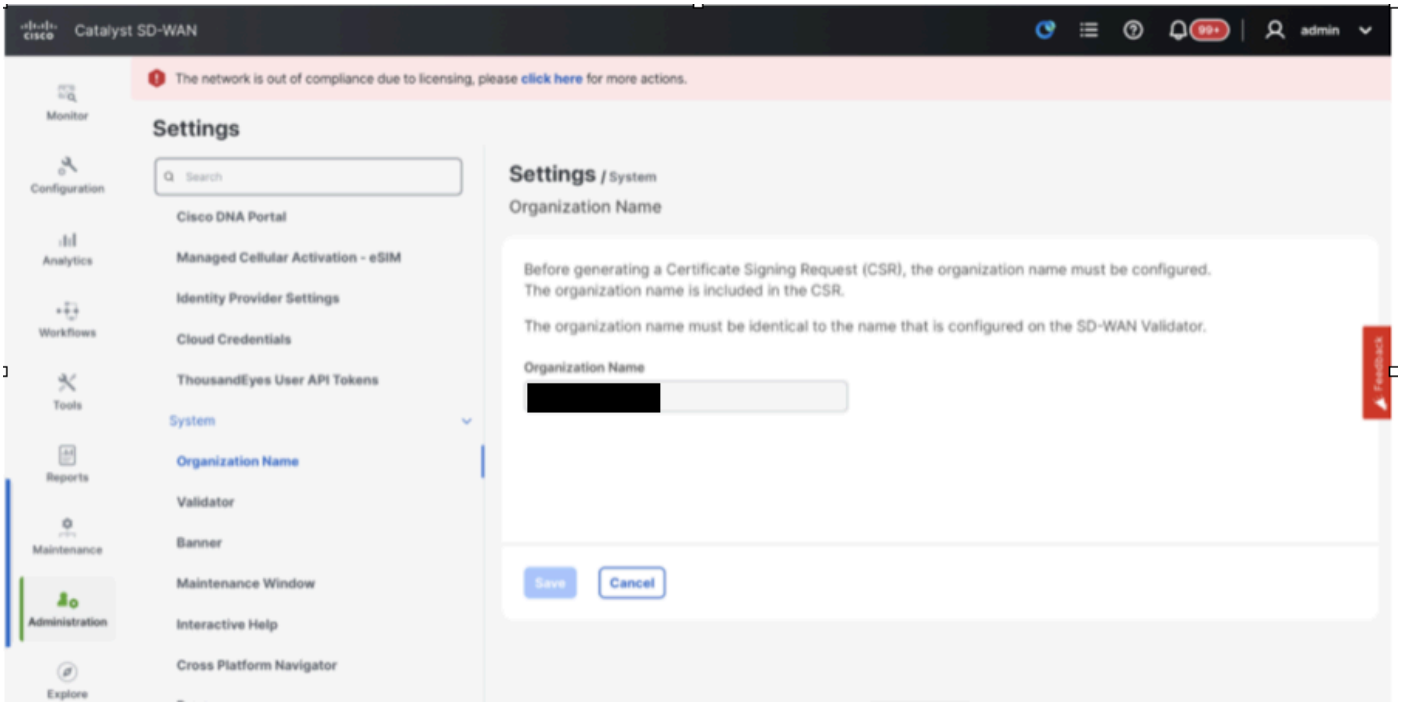
Passaggio 1: Controlli preliminari

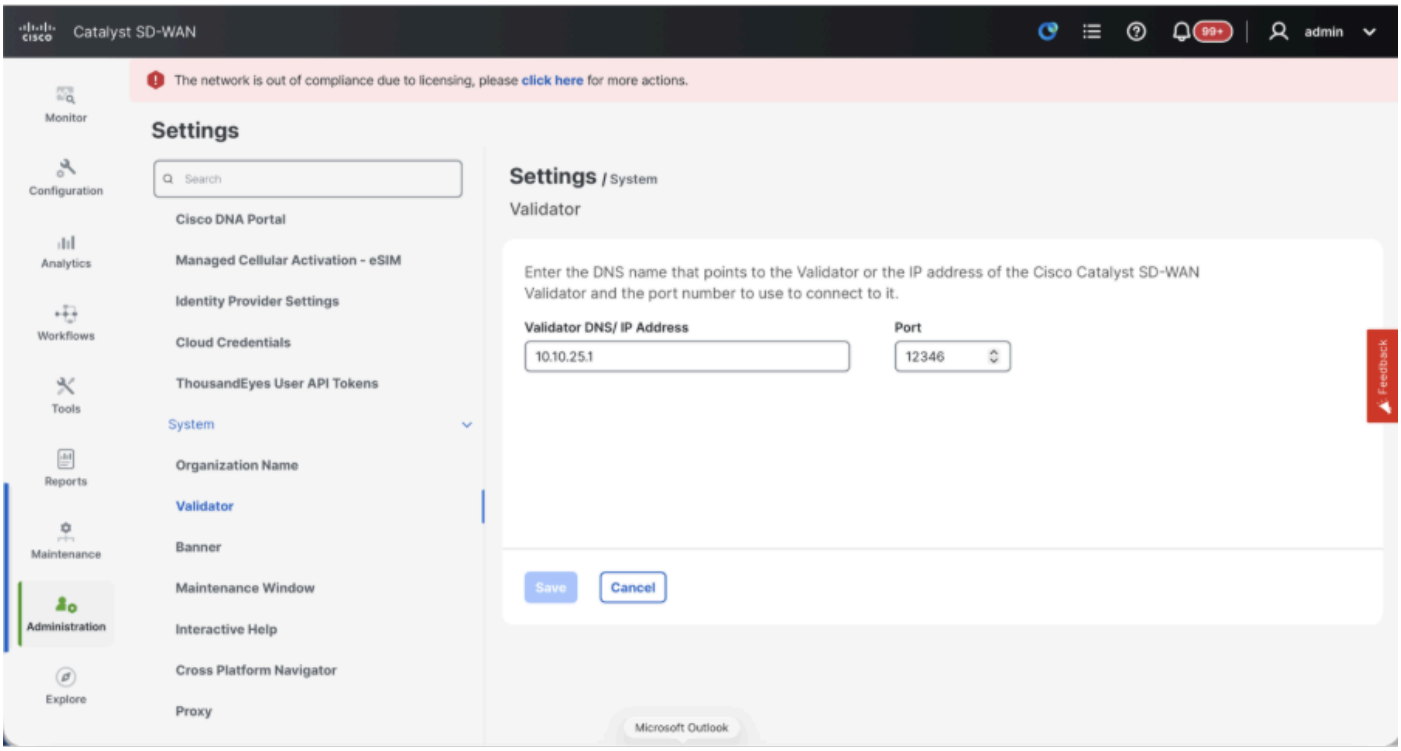
- Verificare che il numero delle istanze attive di Cisco SD-WAN Manager sia identico al numero delle nuove istanze di Cisco SD-WAN Manager installate.
- Accertarsi che tutte le istanze Cisco SD-WAN Manager attive e nuove eseguano la stessa versione del software.
- Verificare che tutte le istanze Cisco SD-WAN Manager nuove e attive siano in grado di raggiungere l'indirizzo IP di gestione di Cisco SD-WAN Validator.
- Verificare che i certificati siano stati installati nelle istanze di Cisco SD-WAN Manager appena installate.
- Verificare che gli orologi di tutti i dispositivi Cisco Catalyst SD-WAN, incluse le nuove istanze di Cisco SD-WAN Manager installate, siano sincronizzati.
- Verificare che nelle istanze di Cisco SD-WAN Manager appena installate sia configurato un nuovo set di IP di sistema e ID di sito, insieme alla stessa configurazione di base del cluster attivo.

Passaggio 2: Configurazione di interfaccia utente, certificati e controller integrati vManage

Aggiornare le configurazioni nell'interfaccia utente di vManage

- Una volta aggiunte le configurazioni al passo 1 nella CLI di tutti i controller, possiamo accedere alla webUI di vManage, usando l'URL https://<vmanage-ip> nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi nodi vManage. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Amministrazione > Impostazioni e completare i seguenti passaggi.
- Configurare il nome dell'organizzazione e l'URL/indirizzo IP di Validator/vBond. Configurare lo stesso valore presente nella CLI del nodo vManage.
- In vManage 20.15/20.18 queste configurazioni sono disponibili nella sezione Sistema.

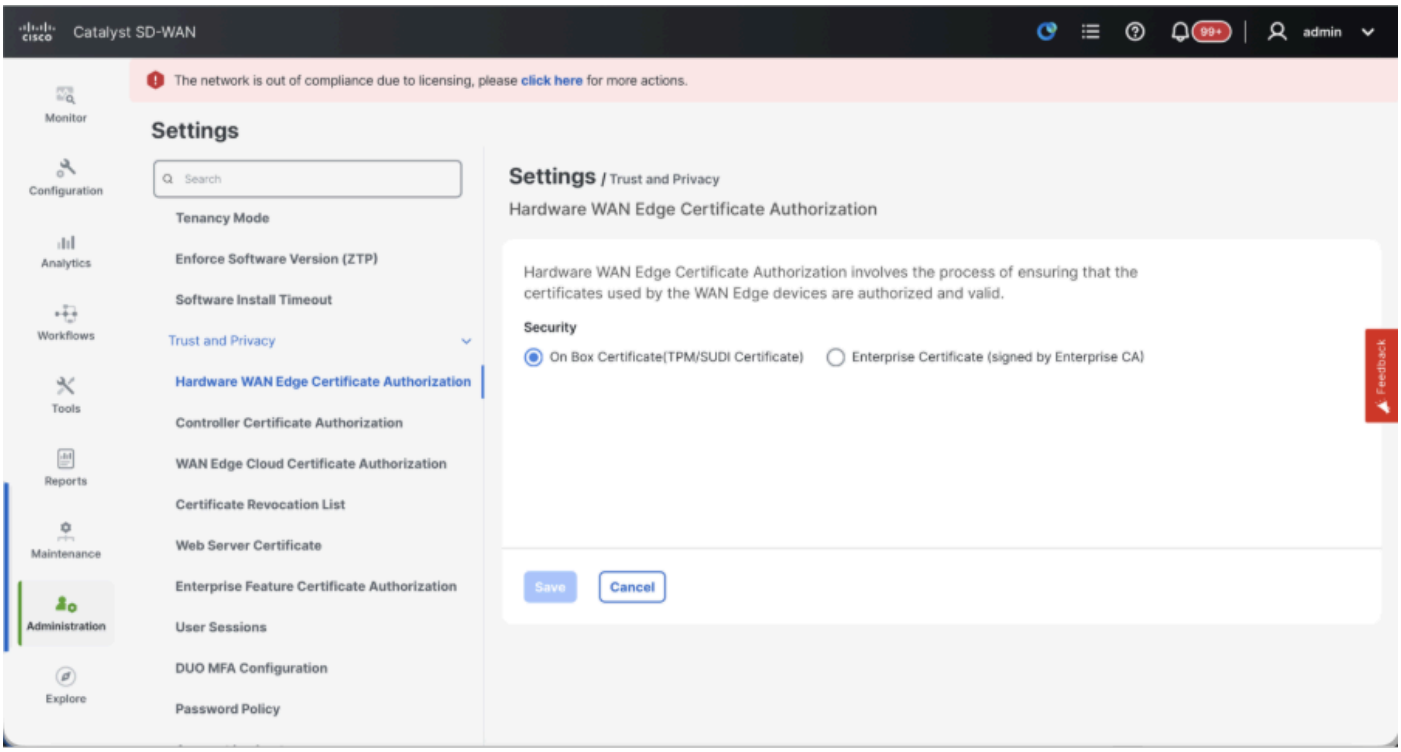




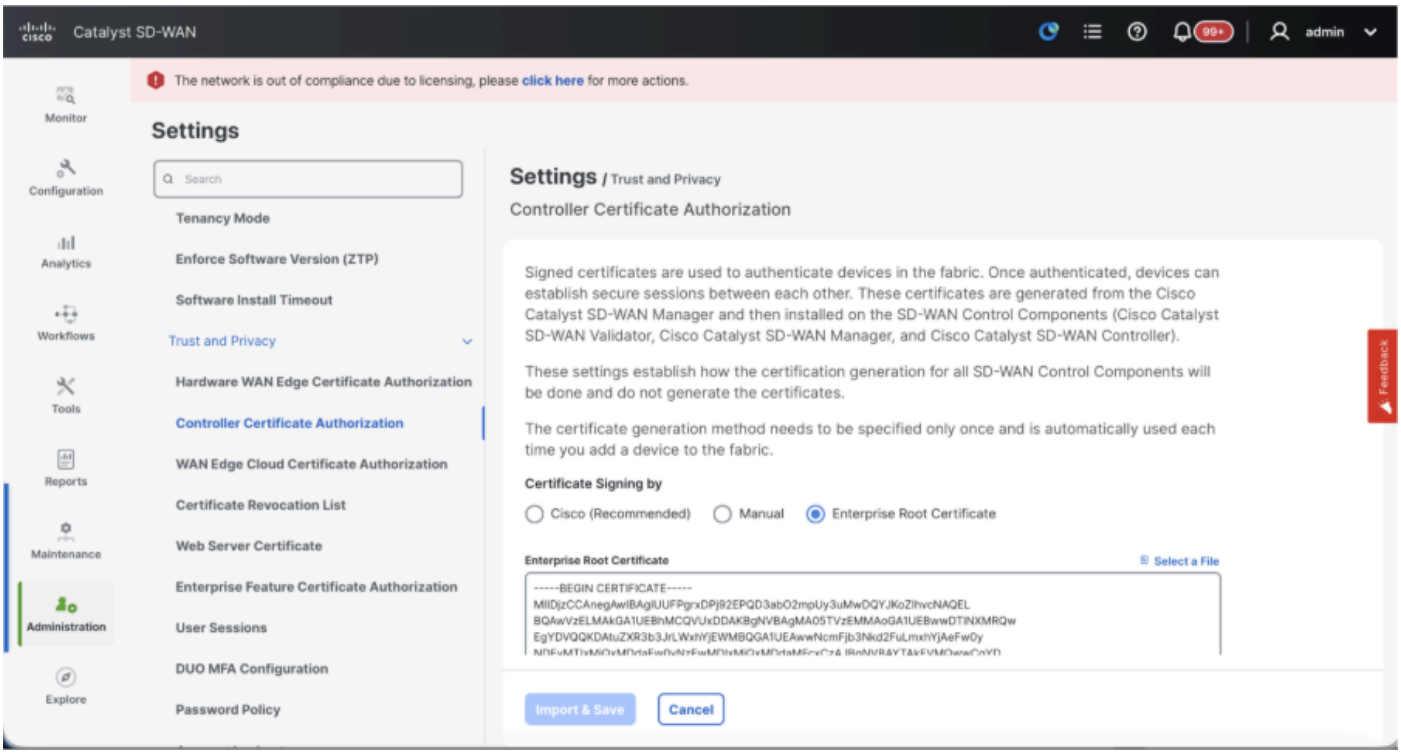
- Verificare le configurazioni per l'Autorità di certificazione (CA), che decide l'Autorità di certificazione utilizzata per firmare i certificati. Sono disponibili 3 opzioni:

1. Autorizzazione certificato perimetro WAN hardware - Decide la CA per i router perimetrali SD-WAN hardware.
    - Certificato On-Box (certificato TPM/SUDI): con questa opzione, il certificato preinstallato sull'hardware del router viene utilizzato per stabilire le connessioni di controllo (connessioni TLS/DTLS)
    - Certificato organizzazione (firmato dall'autorità di certificazione dell'organizzazione): questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario

aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

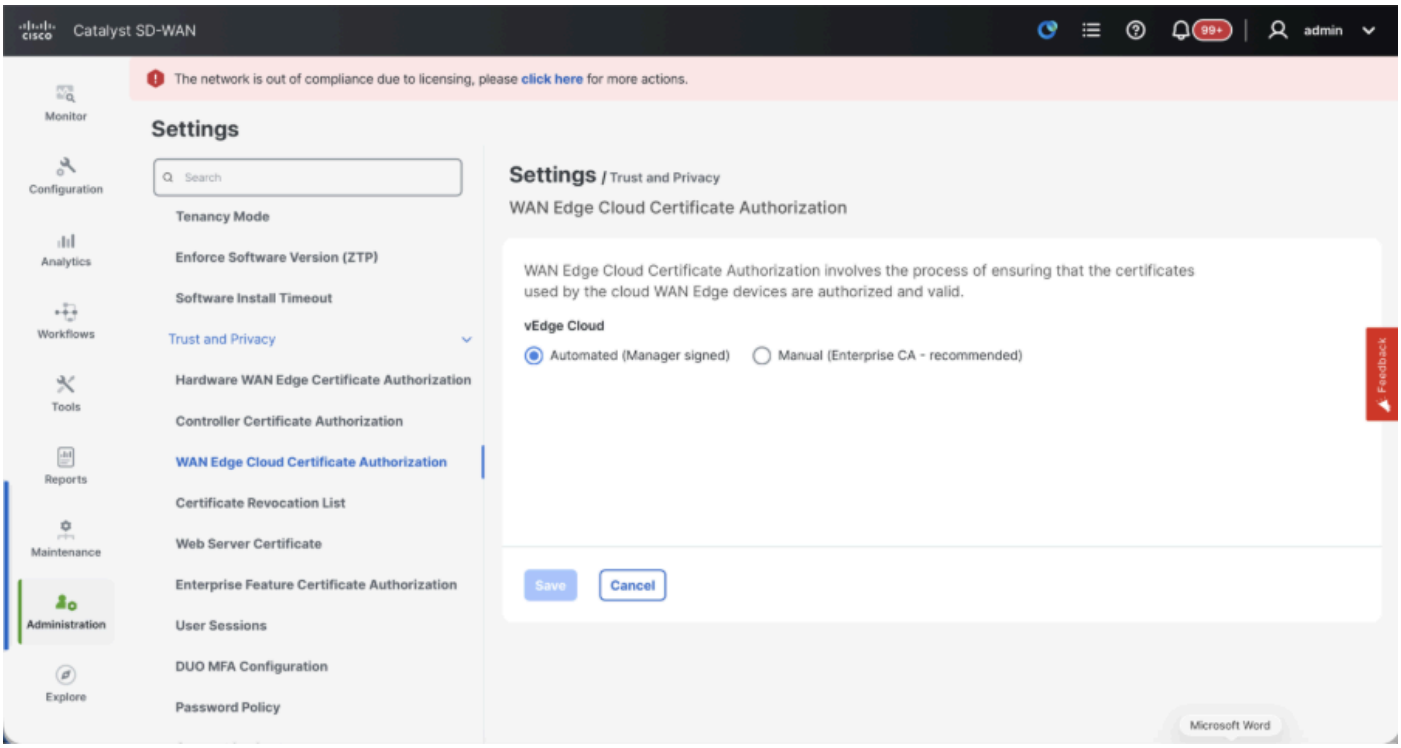


2. Controller Certificate Authorization - Decide la CA per i controller SD-WAN.
    - Cisco (scelta consigliata) - I controller utilizzano i certificati firmati da Cisco PKI. vManage contatta automaticamente il portale PNP utilizzando le credenziali dello smart account configurate in vManage e ottiene la firma del certificato che viene installato nel controller.
    - Manuale: i controller utilizzano i certificati firmati da Cisco PKI. Firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
    - Certificato radice dell'organizzazione: questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

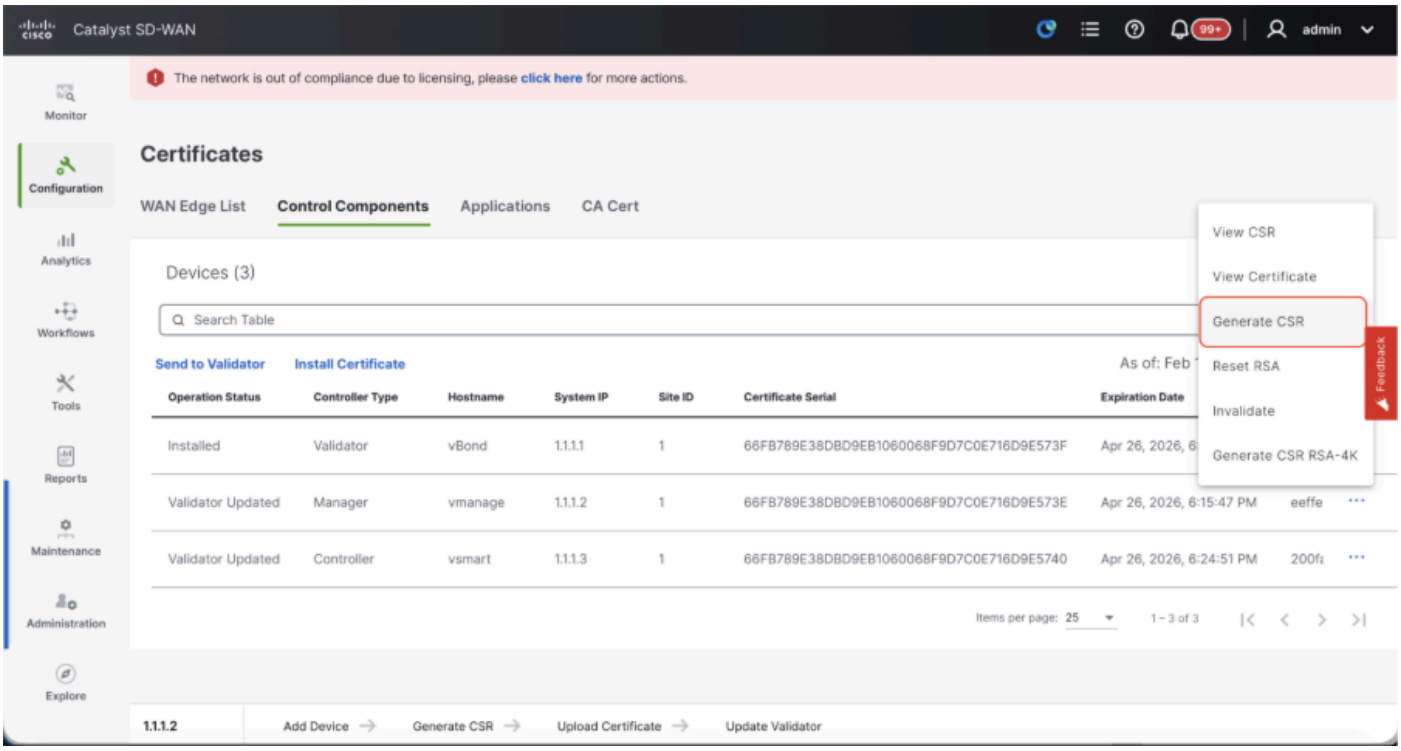


3. Autorizzazione certificato cloud perimetrale WAN - Decide la CA per i router perimetrali SD-WAN virtuali (CSR1000v, C8000v, vEdge cloud)
    - Automatizzato (vManage firmato): vManage firma automaticamente il CSR per i router perimetrali virtuali e installa il certificato sul router.
    - Manuale (Autorità di certificazione dell'organizzazione - consigliata) - I router virtuali utilizzano certificati firmati dall'Autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

Nel caso in cui si utilizzi la propria CA, Autorità di certificazione dell'organizzazione (enterprise), scegliere Enterprise.



- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller
- Fare clic su ... per Manager/vManage e fare clic su Generate CSR (Genera CSR).



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco

passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.

Caricamento di vBond/Validator e vSmart/Controller in vManage

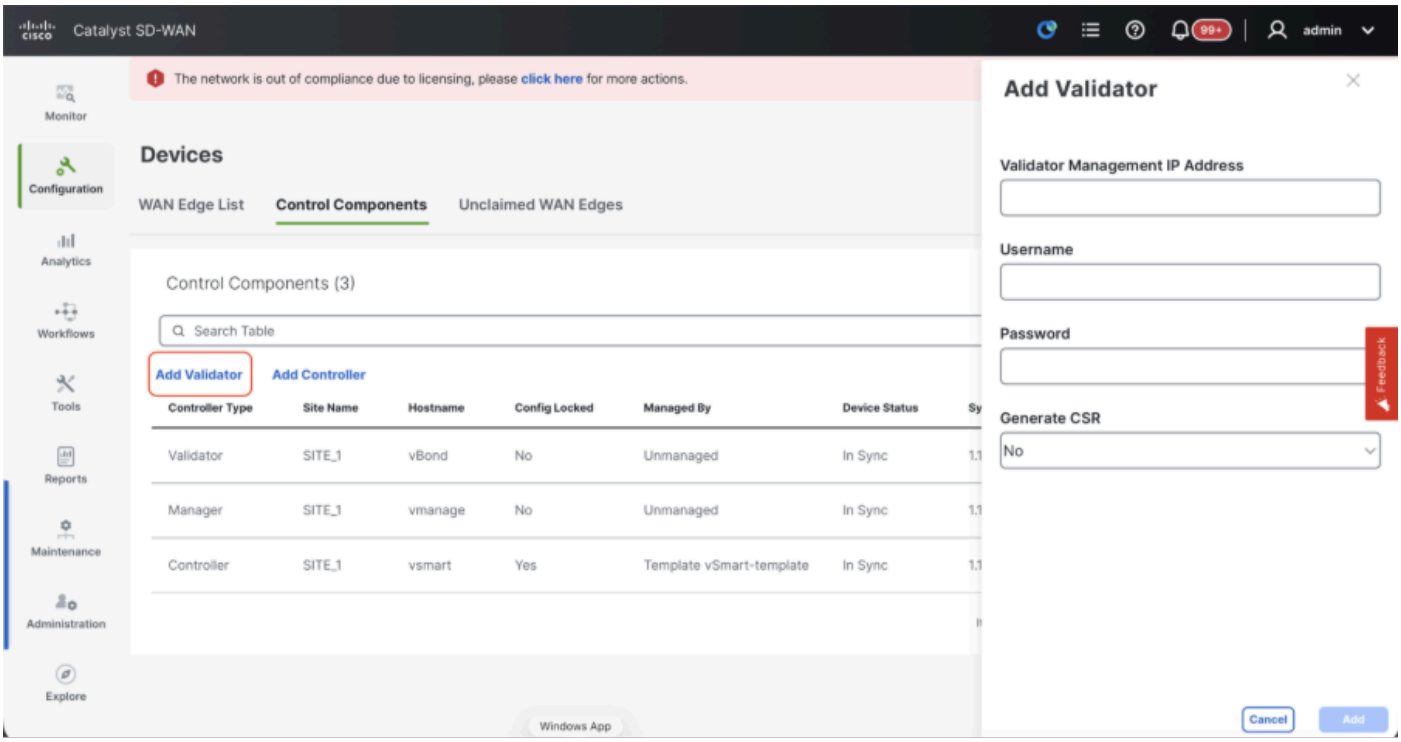
Passare a Configurazione > Dispositivi > Controllo componenti nel caso di nodi vManage 20.15/20.18. In caso di versioni 20.9/20.12, Configurazione > Dispositivi > Controller

vBond/Convalida onboarding

- Fare clic su AddvBondnel caso di 20.12vManagerAggiungi validatornel caso di 20.15/20.18vManage. Viene visualizzato un popup, immettere il IP di trasporto VPN 0 di vBondraggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping se consentito dalla CLI di vManagetovBondIP.
- Immettere le credenziali utente di vBond.

Nota: è necessario utilizzare le credenziali di amministratore di vBondor una parte utente di netadmingroup. È possibile verificare questa condizione nella CLI di vBond. Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vBond.

Nota: Se vBond è dietro un dispositivo/firewall NAT, verificare se l'IP dell'interfaccia VPN 0 di vBond è convertito in un IP pubblico. Se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, in questo passaggio utilizzare l'indirizzo IP pubblico dell'interfaccia VPN 0.



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vBond.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vBonds, ripetere gli stessi passaggi.

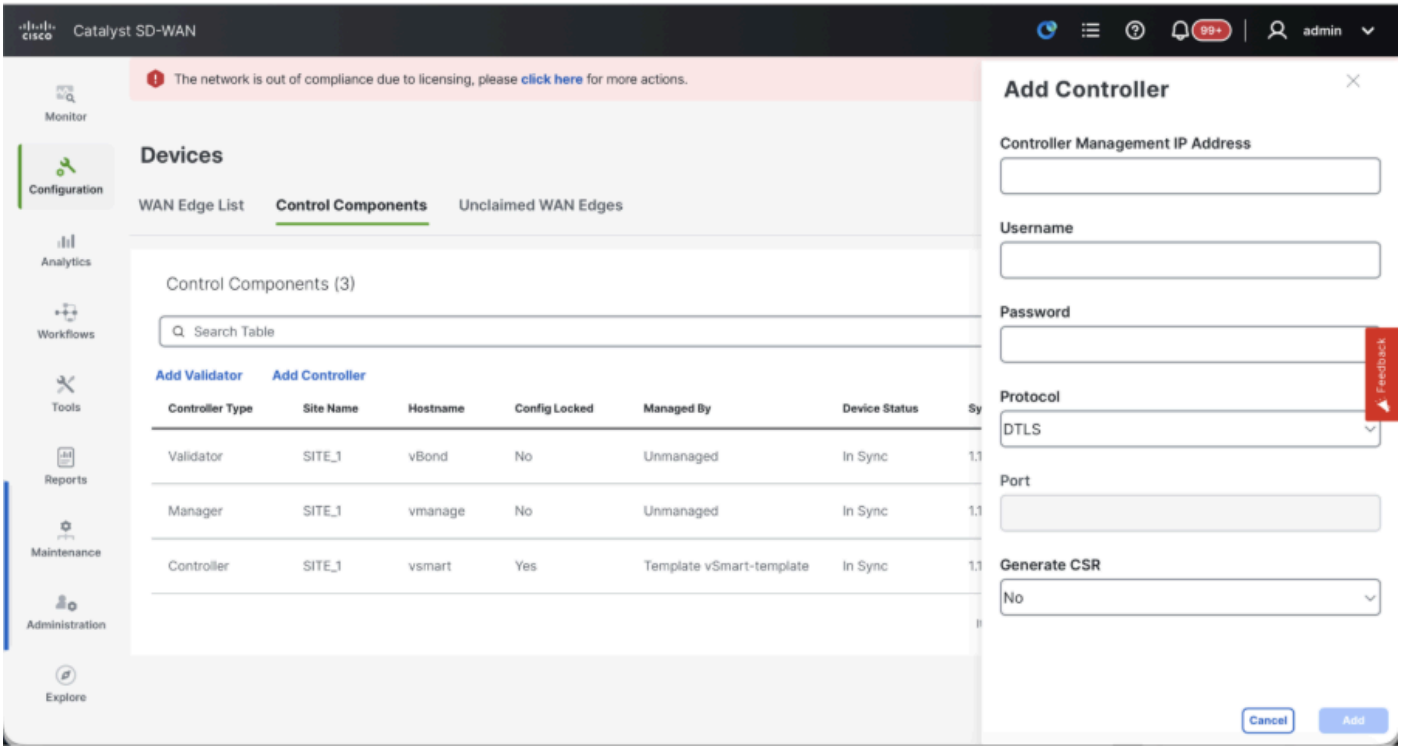
vSmart/Controller integrato

- Fare clic su Add vSmart in caso di vManage 20.12 o Add Controller in caso di vManage 20.15/20.18.
- Viene visualizzato un popup. Immettere l'IP di trasporto VPN 0 di vSmart raggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping, se consentito dalla CLI di vManage a vSmart IP.
- Immettere le credenziali utente di vSmart Note che è necessario utilizzare le credenziali di amministratore di vSmart o di un utente appartenente al gruppo netadmin.
- È possibile verificare questa condizione nella CLI di vSmart.
- Impostare il protocollo su TLS se si intende utilizzare TLS per i router per stabilire

connessioni di controllo con vSmart. Questa configurazione deve essere configurata anche sulla CLI dei nodi vSmarts e vManage.

- Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vSmart.

Nota: se vSmart è dietro un dispositivo/firewall NAT, verificare se l'indirizzo IP dell'interfaccia vSmart VPN 0 è convertito in un indirizzo IP pubblico e se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, utilizzare l'indirizzo IP pubblico dell'indirizzo IP dell'interfaccia VPN 0 in questo passaggio.

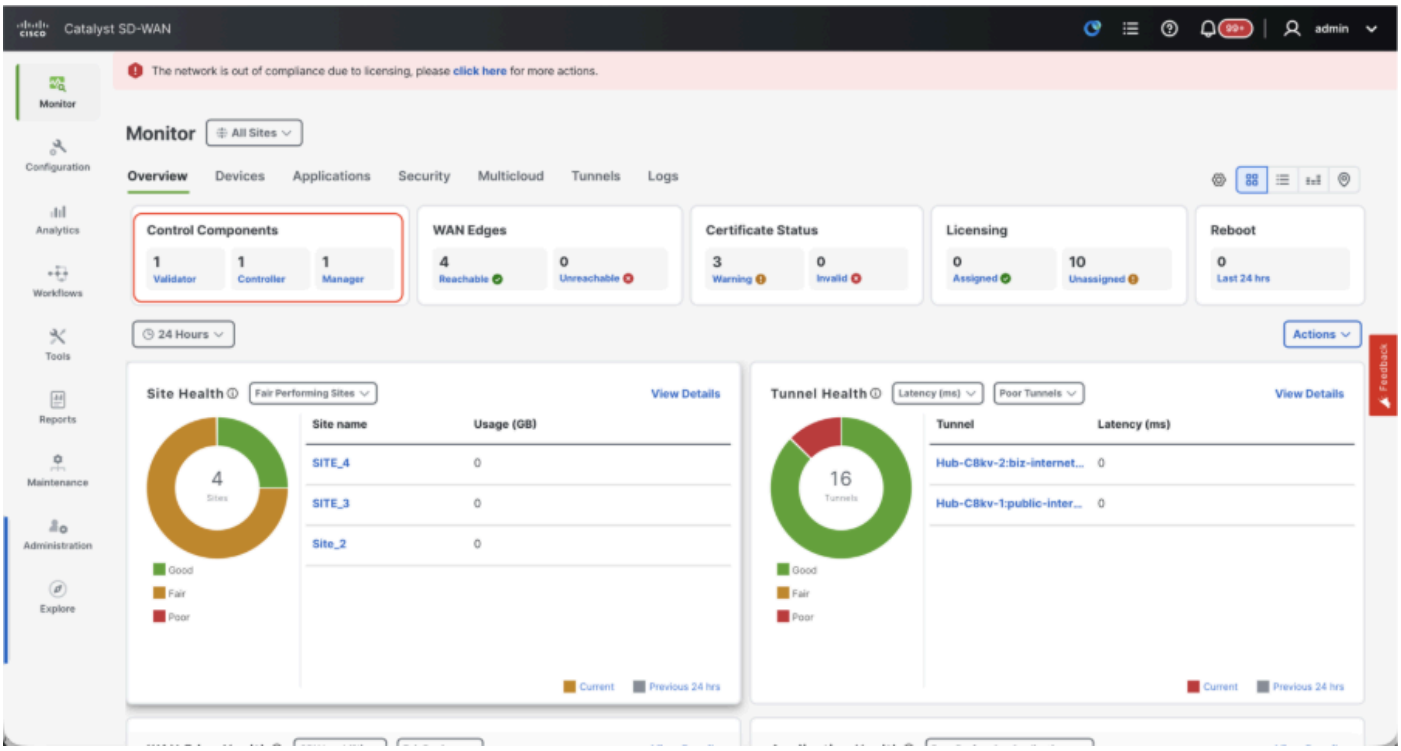


- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vSmart.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della relativa sovrapposizione SD-WAN. La stessa procedura è applicabile se si utilizza il certificato radice Digicert ed Enterprise.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- Se sono presenti più vSmarts, ripetere gli stessi passaggi.

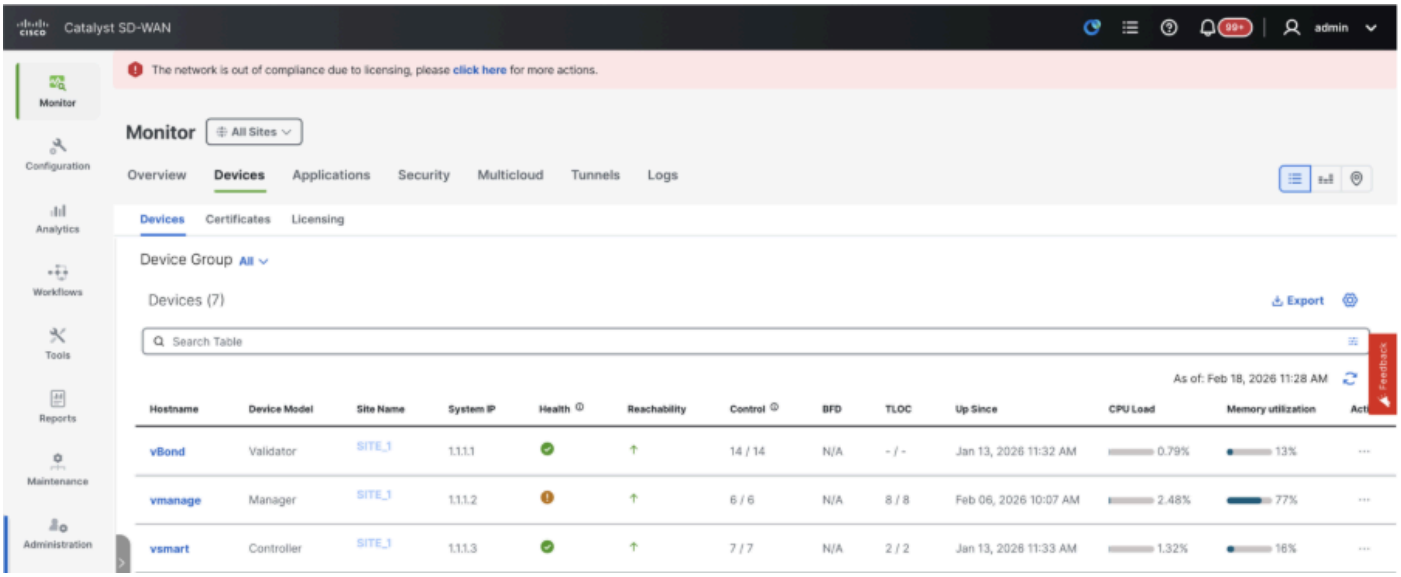
Verifica

Una volta completati tutti i passaggi, verificare che tutti i componenti di controllo siano raggiungibili

in Monitor>Dashboard



- Fate clic sui rispettivi componenti di controllo e verificate che siano tutti raggiungibili.
- Passare a Monitor > Dispositivi e verificare che tutti i componenti di controllo siano raggiungibili.



Passaggio 3: Backup/ripristino di Config-db

Raccolta del backup e del ripristino vManage configuration-db in un altro nodo vManage

Raccolta backup del database di configurazione:

- Nel fabric SD-WAN attualmente in uso, è possibile generare il backup del database di configurazione sia su vManage che su vManage di installazione del cluster.

- Per vManage standalone, vManage è il leader del database di configurazione.

Verificare che configuration-db sia in esecuzione nel nodo vManage.

Per verificare lo stesso comportamento, usare il comando request nms configuration-db status su vManageCLI. L'output è il seguente

```
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#
```

Utilizzare questo comando per raccogliere il backup del database di configurazione dal nodo vManage leader del database di configurazione identificato.

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

L'output previsto è il seguente:

```
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#
```

- Prendere nota delle credenziali di configuration-db se sono state aggiornate.
- Se non si è a conoscenza delle credenziali del database di configurazione, contattare TAC per recuperare le credenziali del database di configurazione dai nodi vManage esistenti.

- Le credenziali di configuration-db predefinite sono nome utente: neo4j e password: password

Ripristinare il backup di Configuration-db in un altro nodo vManage

Copiare il backup del database di configurazione nella directory /home/admin/ di vManage utilizzando SCP.

Output di esempio del comando scp:

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

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

Per ripristinare il backup del database di configurazione, è necessario innanzitutto configurare le credenziali del database di configurazione. Se le credenziali del database di configurazione sono predefinite (neo4j/password), è possibile ignorare questo passaggio.

Per configurare le credenziali configuration-db, utilizzare il comando request nms configuration-db update-admin-user. Utilizzare il nome utente e la password desiderati.

Notare che il server applicazioni di vManage è stato riavviato. A causa della quale l'interfaccia utente di vManage diventa inaccessibile per un breve periodo.

```
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 in cui è possibile procedere al ripristino del backup del database di configurazione:

È possibile utilizzare il comando request nms configuration-db restore path /home/admin/< > per ripristinare configuration-db nel nuovo 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
```

Una volta ripristinato il database di configurazione, verificare che l'interfaccia utente di vManage sia accessibile. Attendere circa 5 minuti e quindi tentare di accedere all'interfaccia utente.

Dopo aver eseguito correttamente il login all'interfaccia utente, verificare che l'elenco dei router perimetrali, il modello, i criteri e tutte le altre configurazioni presenti nell'interfaccia utente vManage precedente o esistente siano riflessi nella nuova interfaccia utente vManage.

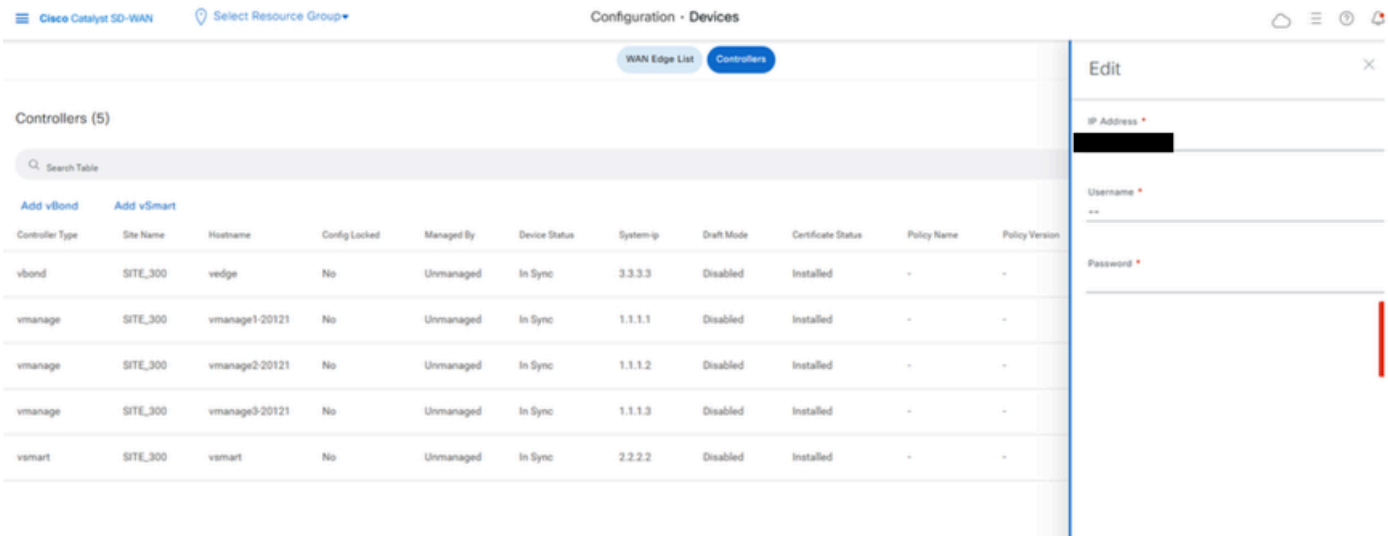
Passaggio 4: Riautenticazione dei controller e annullamento della convalida dei controller precedenti

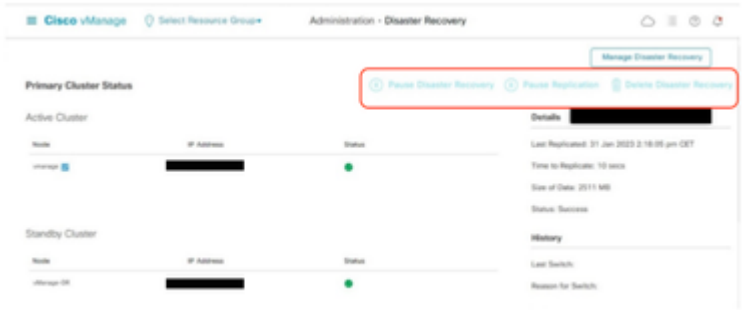
Una volta ripristinato il database di configurazione, è necessario riautenticare tutti i nuovi controller (manage/vsmart/vbond) nel fabric.

Nota: nella produzione effettiva, se l'IP dell'interfaccia utilizzato per la riautenticazione è l'IP dell'interfaccia del tunnel, è necessario garantire che il servizio NETCONF sia consentito sull'interfaccia del tunnel di vManage, vSmart e vBond e anche sui firewall lungo il percorso. La porta firewall da aprire è la porta TCP 830 come regola bidirezionale dal cluster DR a tutti i vBonds e vSmarts.

Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller

- Fare clic sui tre punti accanto a ciascun controller e scegliere Modifica





- Sostituire l'indirizzo ip (ip del sistema del controller) con l'indirizzo ip vpn 0 (interfaccia tunnel) del trasporto. Immettere il nome utente e la password e fare clic su Salva
- Eseguire la stessa operazione per tutti i nuovi controller nel fabric

Sincronizza la catena di certificati radice

Una volta caricati tutti i controller, attenersi a questa procedura:

Su qualsiasi server Cisco SD-WAN Manager nel cluster appena attivo, eseguire le seguenti azioni:

Immettere questo comando per sincronizzare il certificato radice con tutti i dispositivi Cisco Catalyst SD-WAN nel cluster appena attivo:

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

Immettere questo comando per sincronizzare l'UUID di Cisco SD-WAN Manager con Cisco SD-WAN Validator:

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

Una volta ripristinata la struttura e attivate le sessioni bfd e di controllo per tutti i bordi e i controller della struttura, è necessario invalidare i vecchi controller (vmanage/vsmart/vbond) dall'interfaccia utente

- In gestisci interfaccia utente fare clic su Configurazione > Certificati > Controller
- Fare clic su Controller

- Fare clic sui tre punti sul lato destro del controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su invalida
- Fare clic su Invia a vbond
- Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller
- Fare clic sui tre punti sul lato destro del controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su Elimina

Passaggio 5: Registra assegni

Nota: Continuare con la sezione Controlli successivi mostrata qui, che è comune a tutte le combinazioni di distribuzione.

Combinazione 2: vManage standalone + DR a nodo singolo

Istanze necessarie:

- 1 vManage (principale, COMPUTE_AND_DATA)
- 1 vManage (DR standby, COMPUTE_AND_DATA)
- 1 o più vBond
- 1 o più vSmart

Passaggi:

1. Visualizzare tutte le istanze utilizzando l'opzione Passi comuni (Common Steps)
2. Controlli preliminari
3. Configurazione di interfaccia utente, certificati e controller integrati vManage
4. Configurazione DR a nodo singolo
5. Backup/ripristino di Config-db
6. Registra assegni

Passaggio 1: Controlli preliminari

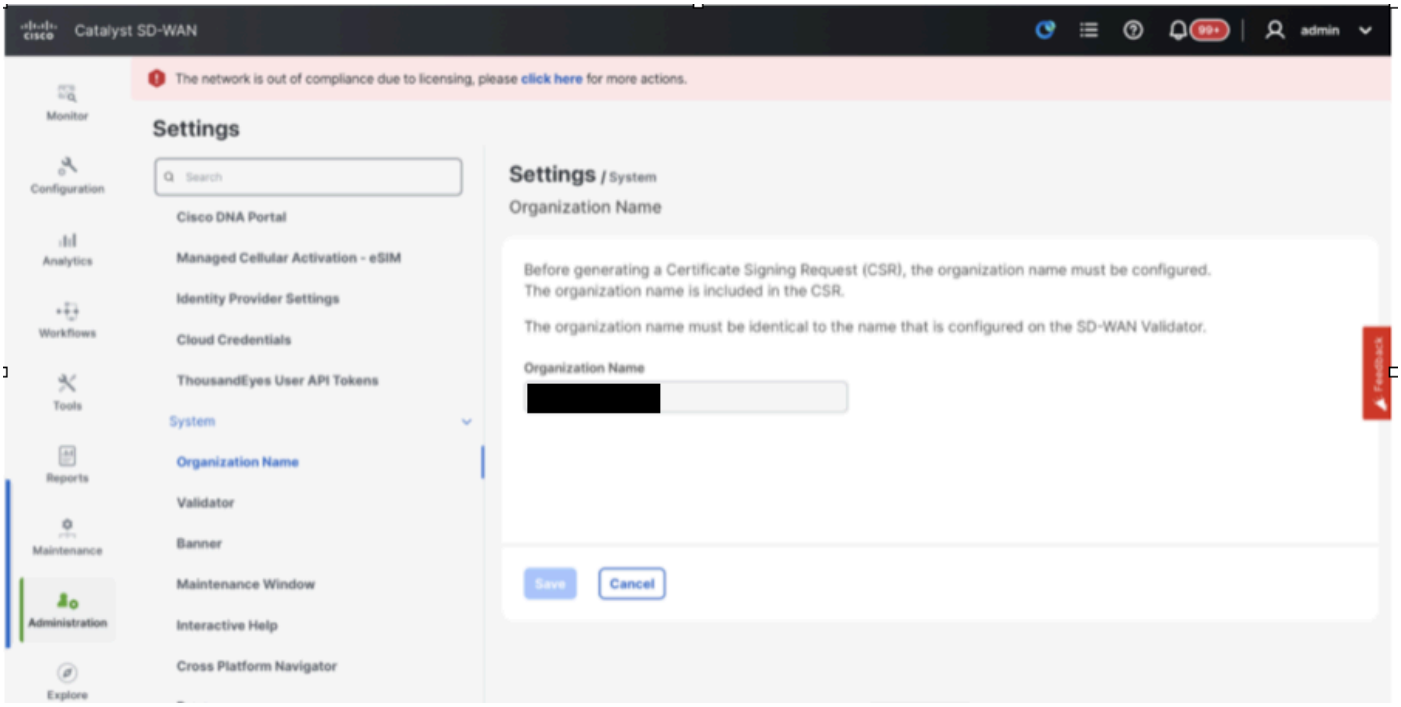
- Verificare che il numero delle istanze attive di Cisco SD-WAN Manager sia identico al numero delle nuove istanze di Cisco SD-WAN Manager installate.
- Accertarsi che tutte le istanze Cisco SD-WAN Manager attive e nuove eseguano la stessa versione del software.
- Verificare che tutte le istanze Cisco SD-WAN Manager nuove e attive siano in grado di raggiungere l'indirizzo IP di gestione di Cisco SD-WAN Validator.
- Verificare che i certificati siano stati installati nelle istanze di Cisco SD-WAN Manager appena installate.

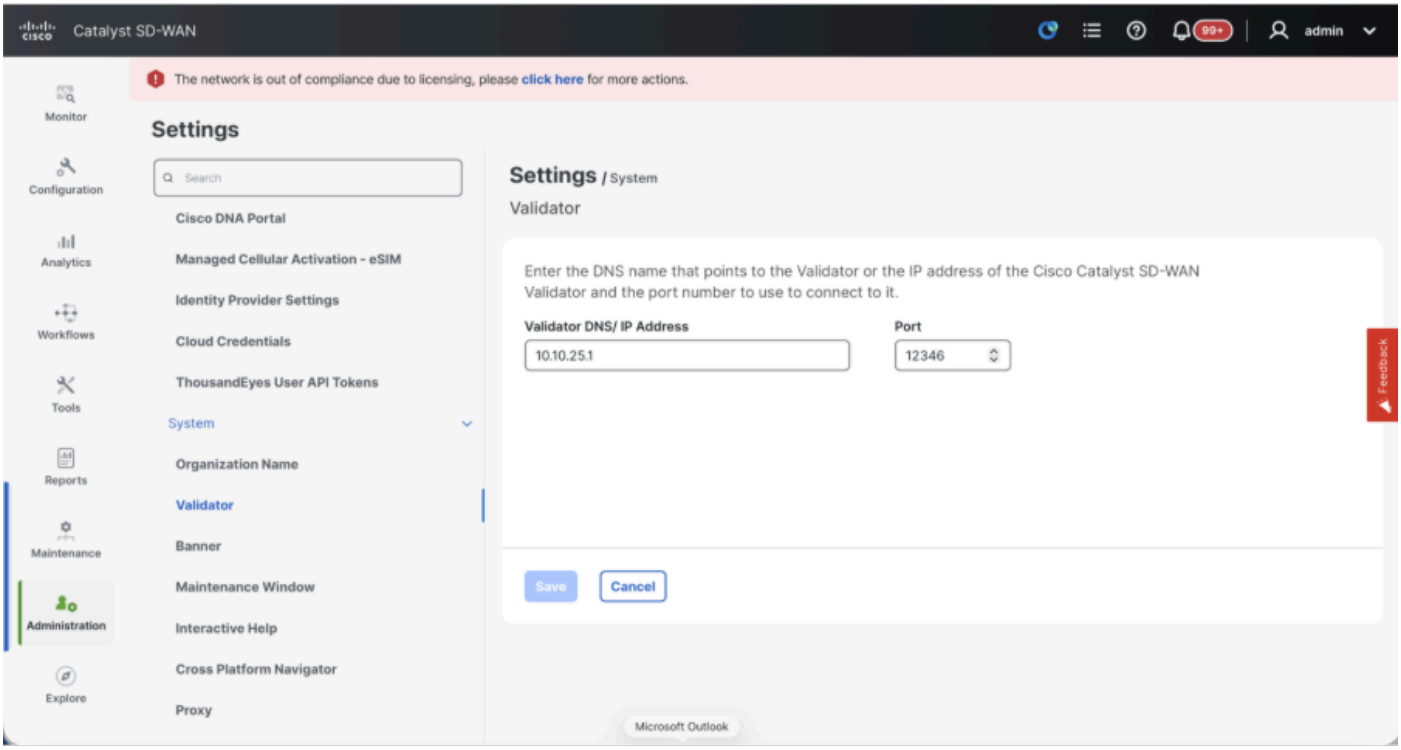
- Verificare che gli orologi di tutti i dispositivi Cisco Catalyst SD-WAN, incluse le nuove istanze di Cisco SD-WAN Manager installate, siano sincronizzati.
- Verificare che nelle istanze di Cisco SD-WAN Manager appena installate sia configurato un nuovo set di IP di sistema e ID di sito, insieme alla stessa configurazione di base del cluster attivo.

Passaggio 2: Configurazione di interfaccia utente, certificati e controller integrati vManage

Aggiornare le configurazioni nell'interfaccia utente di vManage

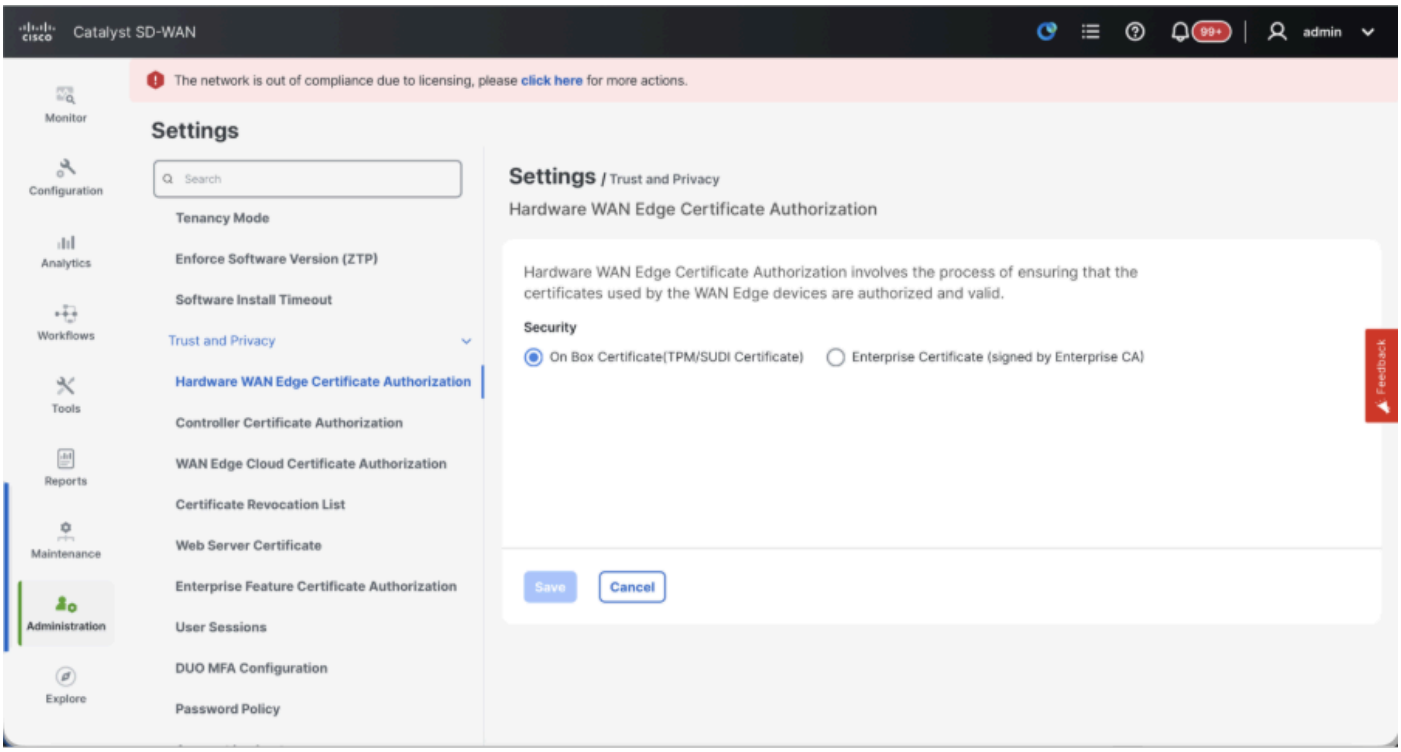
- Una volta aggiunte le configurazioni al passo 1 nella CLI di tutti i controller, possiamo accedere alla webUI di vManage, usando l'URL https://<vmanage-ip> nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi nodi vManage. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Amministrazione > Impostazioni e completare i seguenti passaggi.
- Configurare il nome dell'organizzazione e l'URL/indirizzo IP di Validator/vBond. Configurare lo stesso valore presente nella CLI del nodo vManage.
- In vManage 20.15/20.18 queste configurazioni sono disponibili nella sezione Sistema.



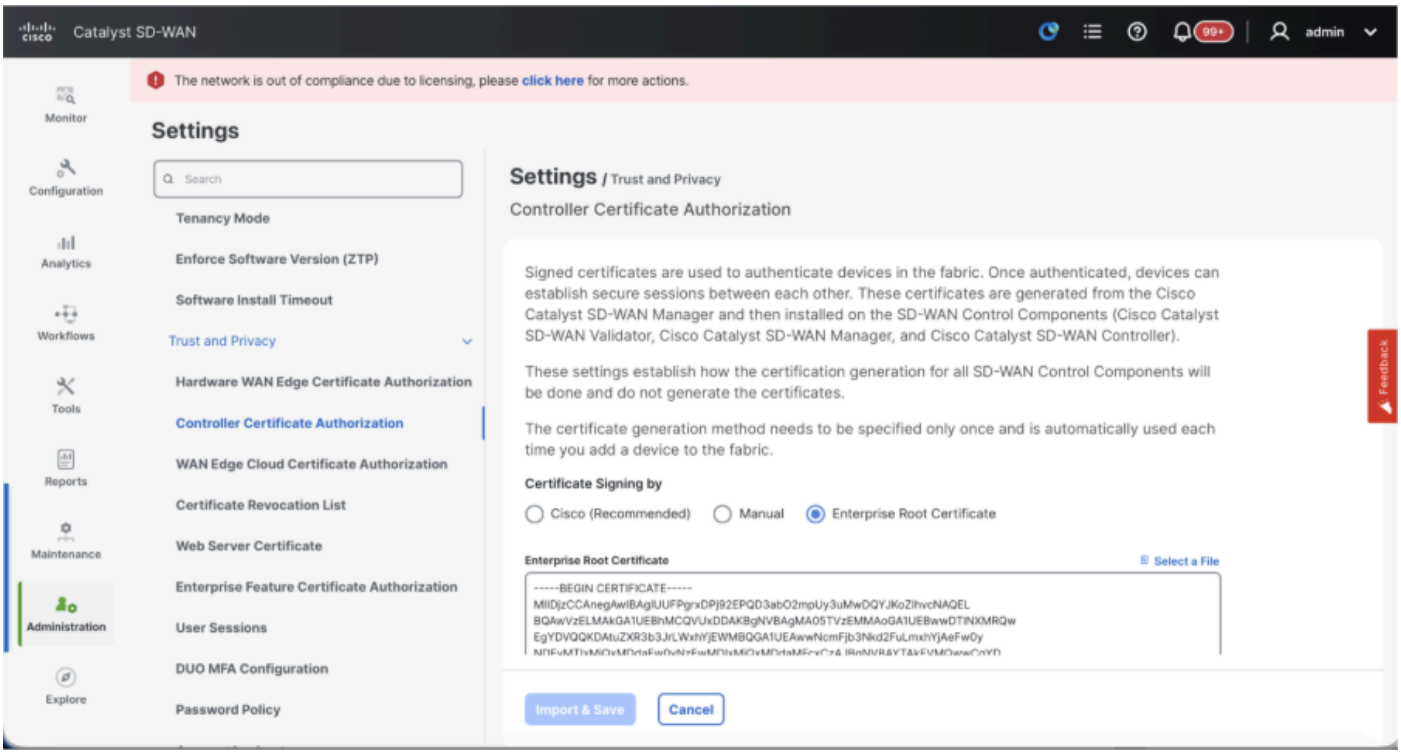


- Verificare le configurazioni per l'Autorità di certificazione (CA), che decide l'Autorità di certificazione utilizzata per firmare i certificati. Sono disponibili 3 opzioni:

1. Autorizzazione certificato perimetro WAN hardware - Decide la CA per i router perimetrali SD-WAN hardware.
    - Certificato On-Box (certificato TPM/SUDI): con questa opzione, il certificato preinstallato sull'hardware del router viene utilizzato per stabilire le connessioni di controllo (connessioni TLS/DTLS)
    - Certificato organizzazione (firmato dall'autorità di certificazione dell'organizzazione): questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

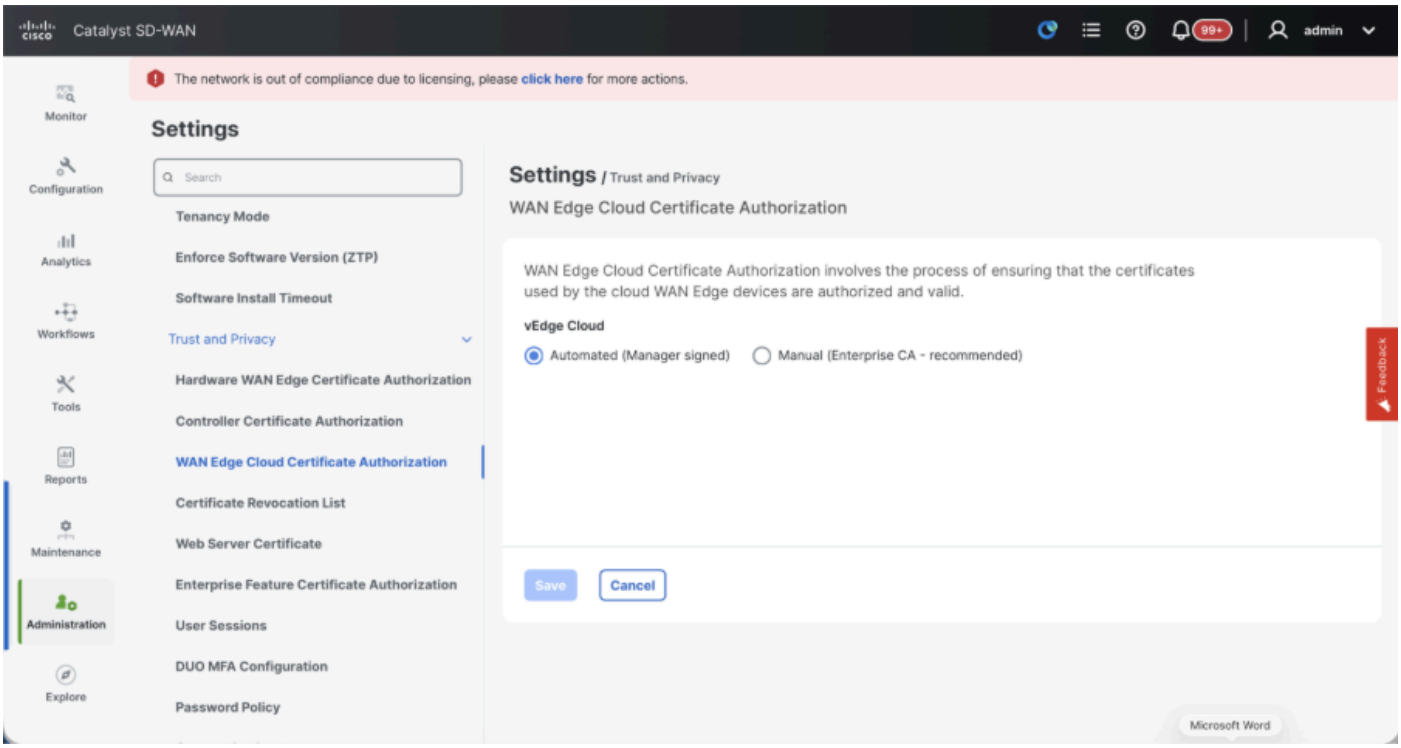


2. Controller Certificate Authorization - Decide la CA per i controller SD-WAN.
    - Cisco (scelta consigliata) - I controller utilizzano i certificati firmati da Cisco PKI. vManage contatta automaticamente il portale PNP utilizzando le credenziali dello smart account configurate in vManage e ottiene la firma del certificato che viene installato nel controller.
    - Manuale: i controller utilizzano i certificati firmati da Cisco PKI. Firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
    - Certificato radice dell'organizzazione: questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

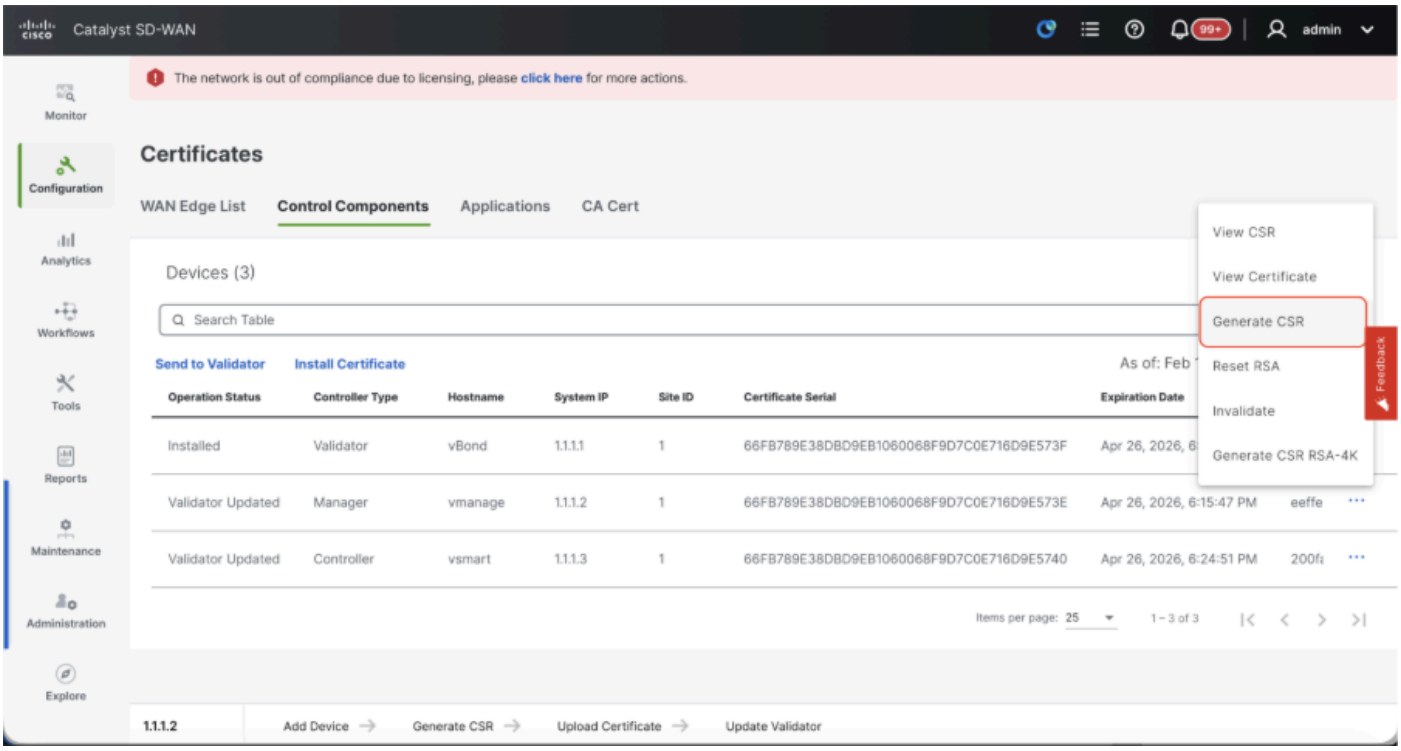


3. Autorizzazione certificato cloud perimetrale WAN - Decide la CA per i router perimetrali SD-WAN virtuali (CSR1000v, C8000v, vEdge cloud)
    - Automatizzato (vManage firmato): vManage firma automaticamente il CSR per i router perimetrali virtuali e installa il certificato sul router.
    - Manuale (Autorità di certificazione dell'organizzazione - consigliata) - I router virtuali utilizzano certificati firmati dall'Autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

Nel caso in cui si utilizzi la propria CA, Autorità di certificazione dell'organizzazione (enterprise), scegliere Enterprise.



- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller
- Fare clic su ... per Manager/vManage e fare clic su Generate CSR (Genera CSR).



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco

passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.

Caricamento di vBond/Validator e vSmart/Controller in vManage

Passare a Configurazione > Dispositivi > Controllo componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

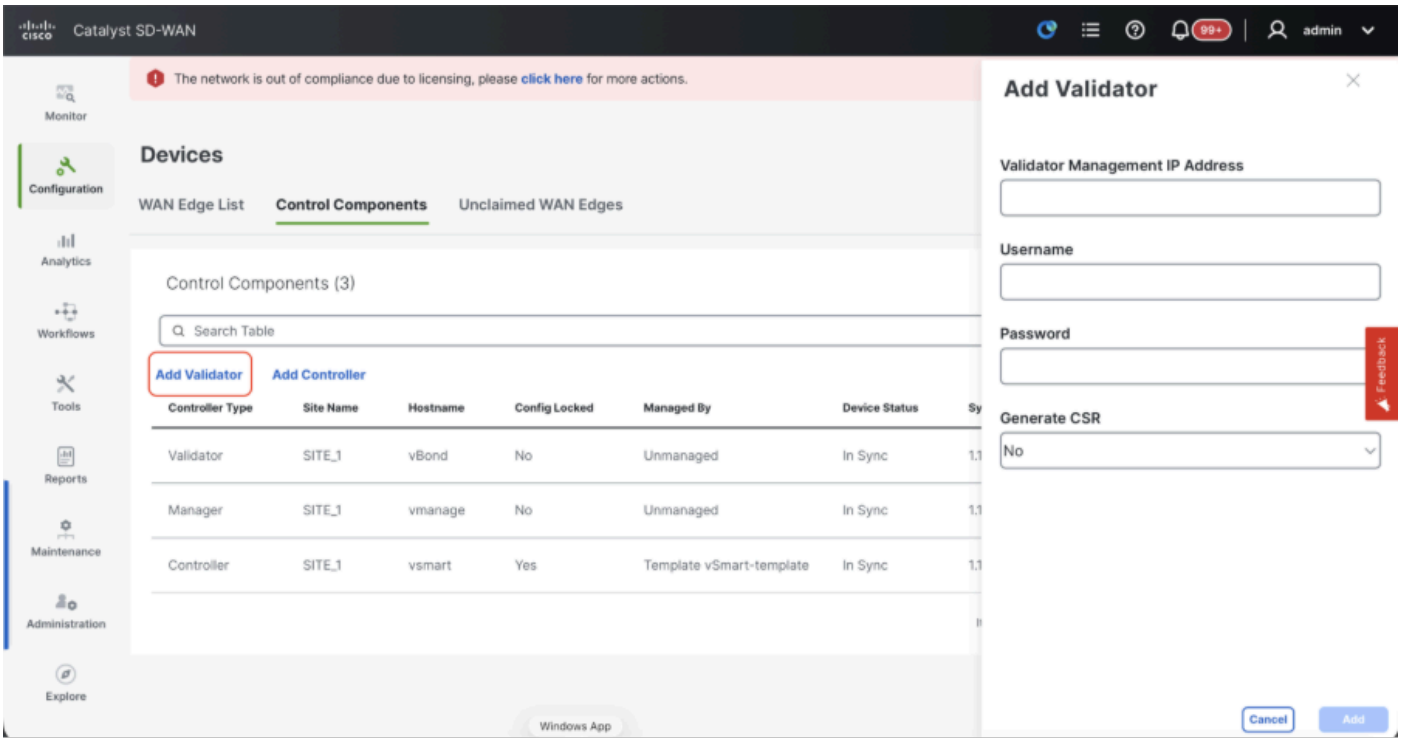
vBond/Convalida onboarding

- Fare clic su AddvBondnel caso di 20.12vManagerAggiungi validatornel caso di 20.15/20.18vManage. Viene visualizzato un popup, immettere il IP di trasporto VPN 0 di vBondraggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping se consentito dalla CLI di vManagetovBondIP.
- Immettere le credenziali utente di vBond.

Nota: è necessario utilizzare le credenziali di amministratore di vBondor una parte utente di netadmingroup. È possibile verificare questa condizione nella CLI di vBond. Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vBond

---

Nota: Se vBond è dietro un dispositivo/firewall NAT, verificare se l'IP dell'interfaccia VPN 0 di vBond è convertito in un IP pubblico. Se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, in questo passaggio utilizzare l'indirizzo IP pubblico dell'interfaccia VPN 0



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vBond.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vBonds, ripetere gli stessi passaggi.

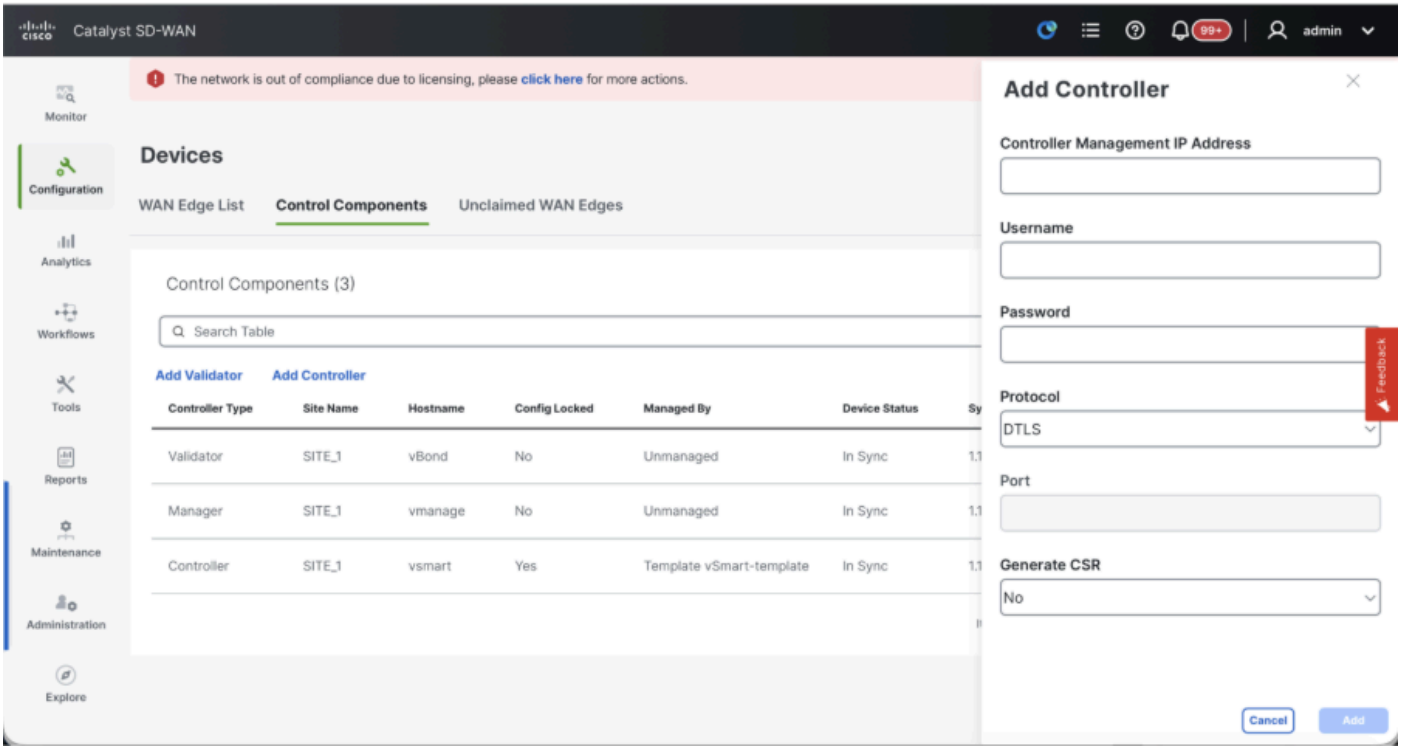
vSmart/Controller integrato

- Fare clic su Add vSmart in caso di vManage 20.12 o Add Controller in caso di vManage 20.15/20.18.
- Viene visualizzato un popup. Immettere l'IP di trasporto VPN 0 di vSmart raggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping, se consentito dalla CLI di vManage a vSmart IP.
- Immettere le credenziali utente di vSmart Note che è necessario utilizzare le credenziali di amministratore di vSmart o di un utente appartenente al gruppo netadmin.
- È possibile verificare questa condizione nella CLI di vSmart.
- Impostare il protocollo su TLS se si intende utilizzare TLS per i router per stabilire

connessioni di controllo con vSmart. Questa configurazione deve essere configurata anche sulla CLI dei nodi vSmarts e vManage.

- Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vSmart.

Nota: se vSmart è dietro un dispositivo/firewall NAT, verificare se l'indirizzo IP dell'interfaccia vSmart VPN 0 è convertito in un indirizzo IP pubblico e se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, utilizzare l'indirizzo IP pubblico dell'indirizzo IP dell'interfaccia VPN 0 in questo passaggio.

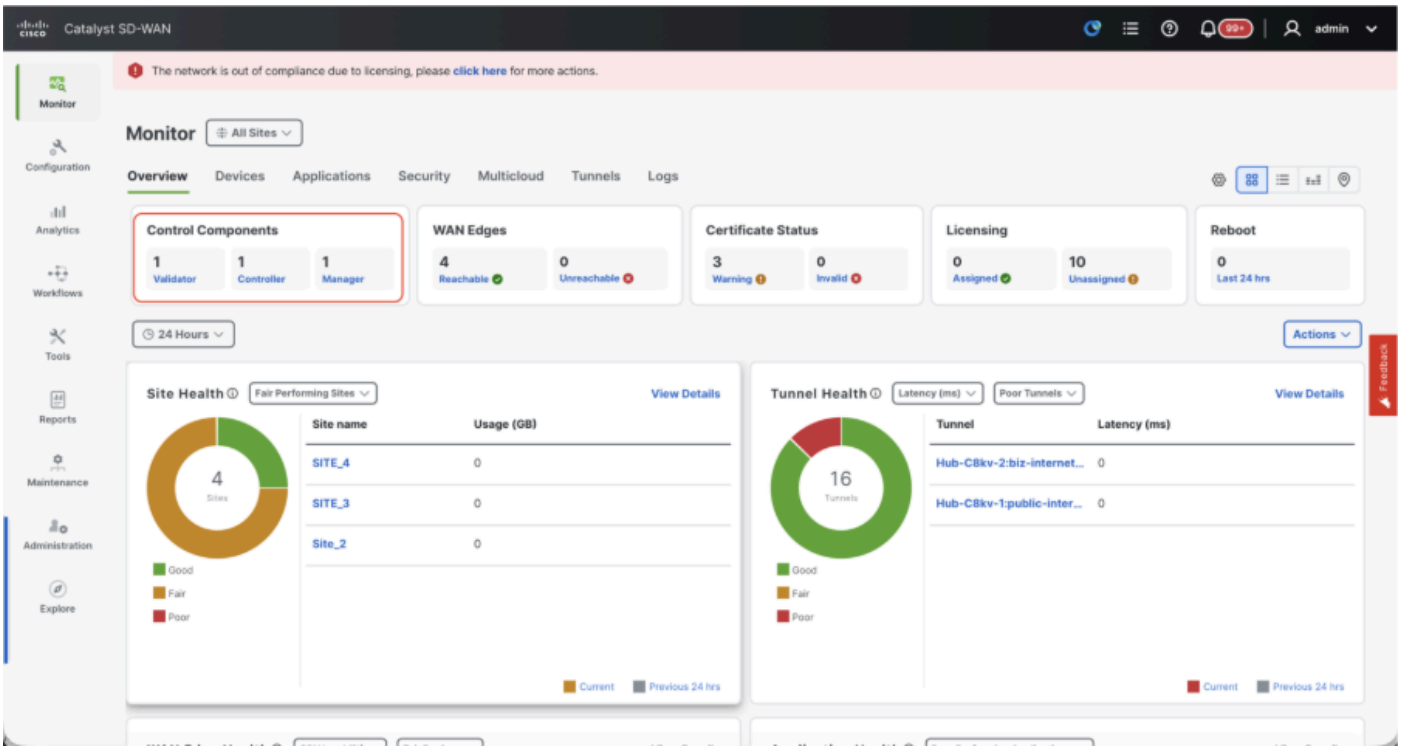


- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vSmart.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della relativa sovrapposizione SD-WAN. La stessa procedura è applicabile se si utilizza il certificato radice Digicert ed Enterprise.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- Se sono presenti più vSmarts, ripetere gli stessi passaggi.

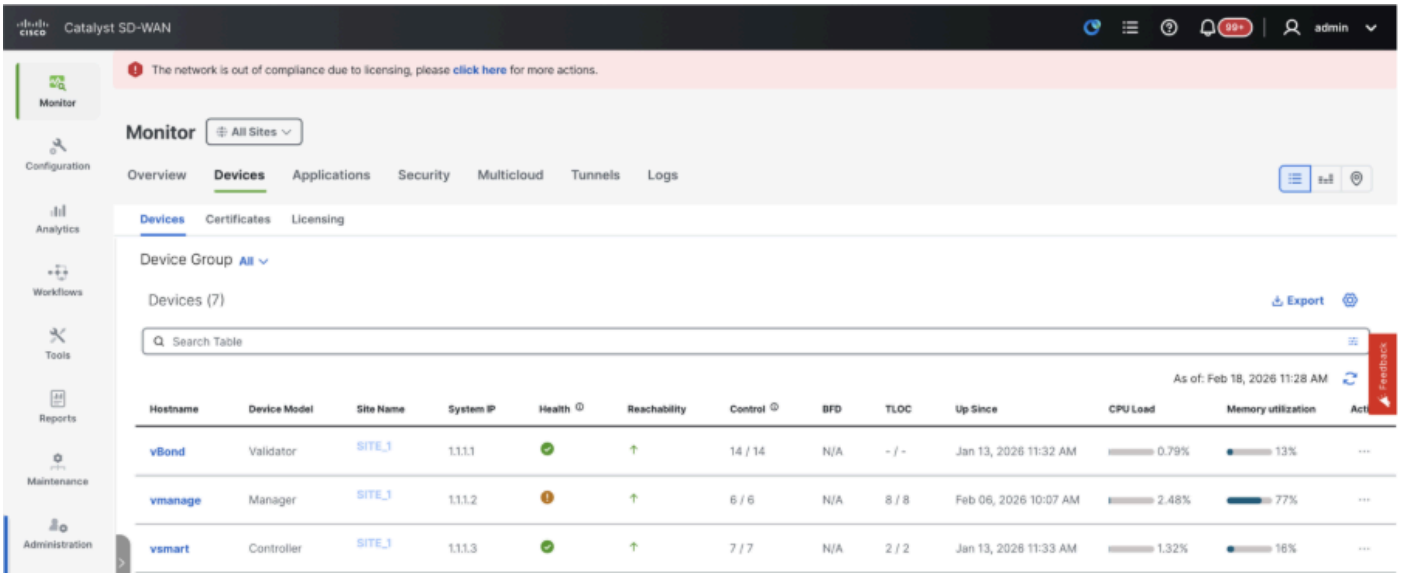
Verifica

Una volta completati tutti i passaggi, verificare che tutti i componenti di controllo siano raggiungibili

in Monitor>Dashboard



- Fate clic sui rispettivi componenti di controllo e verificate che siano tutti raggiungibili.
- Passare a Monitor > Dispositivi e verificare che tutti i componenti di controllo siano raggiungibili.



Passaggio 3: Backup/ripristino di Config-db

Raccolta del backup e del ripristino vManage configuration-db in un altro nodo vManage

---

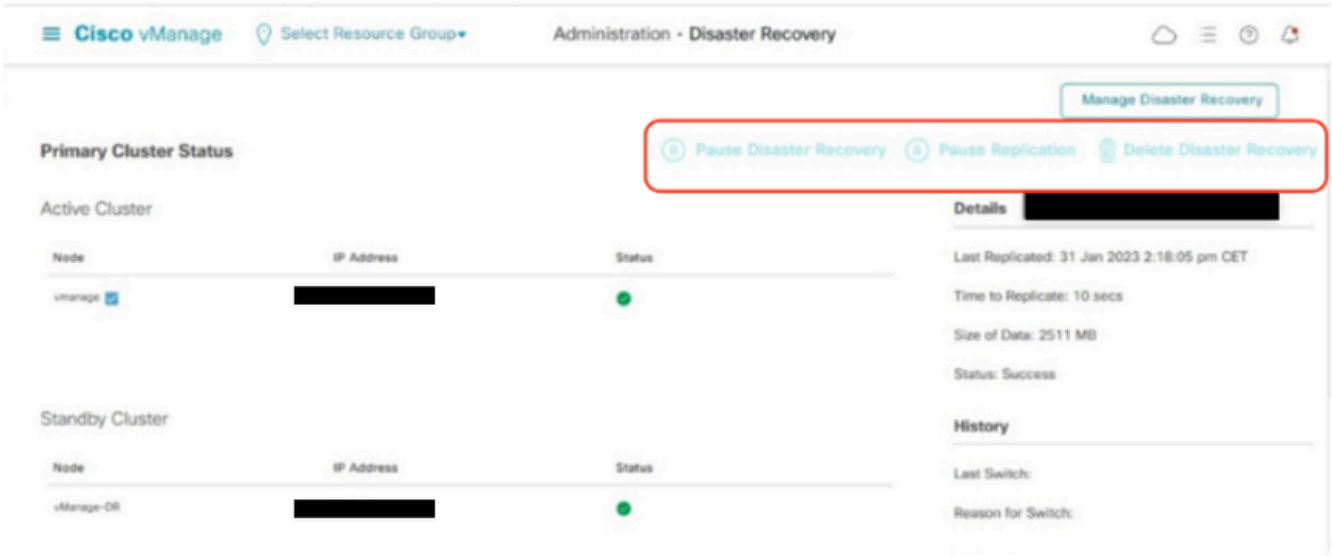
Nota: Durante la raccolta del backup del database di configurazione dal nodo vManage esistente in cui è abilitato il ripristino di emergenza, assicurarsi che venga raccolto dopo

---

che il ripristino di emergenza su tale nodo è stato sospeso ed eliminato.

Confermare che non è in corso la replica per il disaster recovery. Selezionare Amministrazione > Disaster Recovery e verificare che lo stato sia Operazione riuscita e non in uno stato transitorio, ad esempio Importazione in sospeso, Esportazione in sospeso o Download in sospeso. Se lo stato non ha esito positivo, contattare Cisco TAC e verificare la corretta replica prima di sospendere il ripristino di emergenza.

Sospendere innanzitutto il ripristino di emergenza e assicurarsi che l'attività sia completata. Eliminare quindi il ripristino di emergenza e verificare che l'attività sia stata completata.



Contattare Cisco TAC per garantire la corretta pulizia del dispositivo di ripristino di emergenza.

Raccolta backup del database di configurazione:

- Nel fabric SD-WAN attualmente in uso, è possibile generare il backup del database di configurazione sia su vManage che su vManage di installazione del cluster.
- Per vManage standalone, vManage è il leader del database di configurazione.

Verificare che configuration-db sia in esecuzione nel nodo vManage.

È possibile verificare la stessa condizione utilizzando il comando request nms configuration-db statusonvManageCLI. L'output è il seguente

```
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#
```

Utilizzare questo comando per raccogliere il backup del database di configurazione dal nodo vManage leader del database di configurazione identificato.

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

L'output previsto è il seguente:

```
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#
```

- Prendere nota delle credenziali di configuration-db se sono state aggiornate.
- Se non si è a conoscenza delle credenziali del database di configurazione, contattare TAC per recuperare le credenziali del database di configurazione dai nodi vManage esistenti.
- Le credenziali di configuration-db predefinite sono nome utente: neo4j e password: password

Ripristinare il backup di Configuration-db in un altro nodo vManage

Copiare il backup del database di configurazione nella directory /home/admin/ di vManage utilizzando SCP.

Output di esempio del comando scp:

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

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

Per ripristinare il backup del database di configurazione, è necessario innanzitutto configurare le credenziali del database di configurazione. Se le credenziali del database di configurazione sono

predefinite (neo4j/password), è possibile ignorare questo passaggio.

Per configurare le credenziali configuration-db, utilizzare il comando request nms configuration-db update-admin-user.Utilizzare il nome utente e la password desiderati.

Notare che il server applicazioni di vManage è stato riavviato. A causa della quale l'interfaccia utente di vManage diventa inaccessibile per un breve periodo.

```
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 in cui è possibile procedere al ripristino del backup del database di configurazione:

È possibile utilizzare il comando request nms configuration-db restore path /home/admin/< > per ripristinare configuration-db nel nuovo 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
```

Una volta ripristinato il database di configurazione, verificare che l'interfaccia utente di vManage

sia accessibile. Attendere circa 5 minuti e quindi tentare di accedere all'interfaccia utente.

Dopo aver eseguito correttamente il login all'interfaccia utente, verificare che l'elenco dei router perimetrali, il modello, i criteri e tutte le altre configurazioni presenti nell'interfaccia utente vManage precedente o esistente siano riflessi nella nuova interfaccia utente vManage.

Passaggio 4: Configurazione DR a nodo singolo

Fare riferimento al passaggio 2: Controlli preliminari nella combinazione 2: vManage standalone + ripristino di emergenza a nodo singolo e verifica di aver completato tutti i requisiti prima di procedere con l'abilitazione del ripristino di emergenza.

DR. a nodo singolo

Prerequisiti

- Verificare che il nodo primario e il nodo secondario siano raggiungibili da HTTPS su una VPN di trasporto (VPN 0).

- Verificare che il nodo primario e il nodo secondario Cisco vManage eseguano la stessa versione di Cisco vManage.

Interfaccia cluster fuori banda nella VPN 0

1. Per ogni istanza vManage all'interno di un cluster, è necessaria una terza interfaccia (collegamento cluster) oltre alle interfacce utilizzate per VPN 0 (trasporto) e VPN 512 (gestione).
2. Questa interfaccia viene utilizzata per la comunicazione e la sincronizzazione tra i server vManage all'interno del cluster.
3. Questa interfaccia deve essere di almeno 1 Gbps e avere una latenza di 4 ms o inferiore. Si consiglia un'interfaccia di 10 Gbps.
4. Entrambi i nodi vManage devono essere in grado di raggiungere l'uno l'altro tramite questa interfaccia: che si tratti di un segmento di livello 2 o di un instradamento di livello 3.

- Verificare che tutti i servizi (application-server, configuration-db, messaging server, coordination server e statistics-db) siano abilitati su entrambi i nodi Cisco vManage.
- Distribuire tutti i controller, inclusi i Cisco vBond Orchestrator, nei centri dati principali e secondari. Verificare che questi controller siano raggiungibili dai nodi Cisco vManage distribuiti nei centri dati. I controller si connettono solo al nodo Cisco vManage primario.
- Verificare che non siano in corso altre operazioni nel nodo Cisco vManage attivo (primario) e in standby (secondario). Verificare, ad esempio, che nessun server sia in fase di aggiornamento o che nessun modello sia in fase di collegamento dei modelli ai dispositivi.

- Disabilitare il server proxy HTTP/HTTPS Cisco vManage, se abilitato. Se non si disabilita il server proxy, Cisco vManage tenta di stabilire la comunicazione per il ripristino di emergenza tramite l'indirizzo IP proxy, anche se gli indirizzi IP dei cluster fuori banda di Cisco vManage sono raggiungibili direttamente. È possibile riattivare il server proxy Cisco vManage HTTP/HTTPS al termine della registrazione del ripristino di emergenza.

- Prima di avviare il processo di registrazione per il ripristino di emergenza, passare alla finestra Strumenti → Riconosci rete sul nodo principale Cisco vManage e riscoprire i Cisco vBond Orchestrator.

Configurazione

Configurare le configurazioni CLI di tutti i nodi vManage che agiscono come nodi di ripristino di emergenza

Configurazione minima bare per vManageprima della registrazione del ripristino di emergenza è come mostrato

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Nota: se si utilizza URL come indirizzo vBond, verificare di configurare gli indirizzi IP dei server DNS nella configurazione VPN 0 o di risolverli.

Queste configurazioni sono necessarie per abilitare l'interfaccia di trasporto utilizzata per stabilire le connessioni di controllo con i router e gli altri controller

```
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
```

Configurare inoltre l'interfaccia di gestione VPN 512 per consentire l'accesso di gestione fuori

banda al controller.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
commit
```

Configurare l'interfaccia del servizio su DR vManage

Configurare l'interfaccia di servizio nel nodo vManage. Questa interfaccia viene utilizzata per la comunicazione DR,

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Verificare che per l'interfaccia di servizio sul server vManage principale e sul server vManage primario venga utilizzata la stessa subnet IP

Aggiornare le configurazioni nell'interfaccia utente di vManage

- Una volta aggiunte le configurazioni alla CLI di tutti i controller, è possibile accedere alla

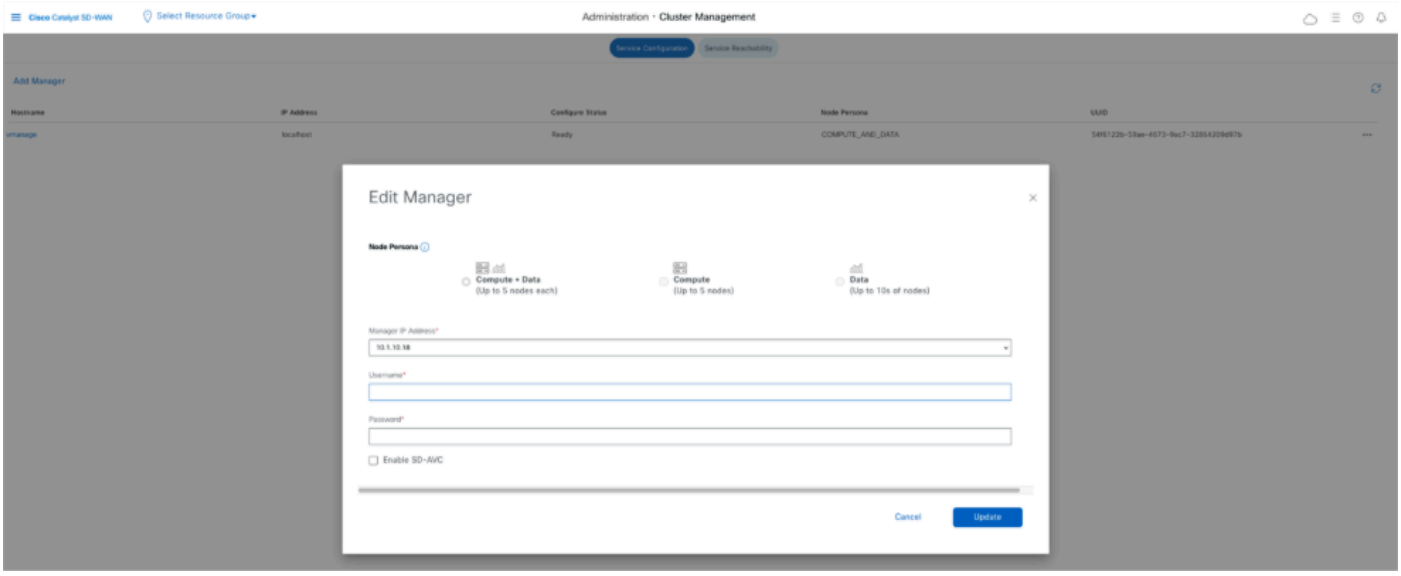
webUI di vManage, utilizzando l'URL https://<vmanage-ip> nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi nodi vManage. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Amministrazione > Impostazioni e completare i seguenti passaggi.
- Configurare il nome dell'organizzazione. Configurare lo stesso valore presente nella CLI del nodo vManage.
- In vManage 20.15/20.18 queste configurazioni sono disponibili nella sezione Sistema.

Installazione del certificato su DR vManage

Procedere come indicato nella sezione Combinazione 2: vManage standalone + DR a nodo singolo Fase 3: Configurare l'interfaccia utente, i certificati e i controller integrati di vManage per installare il certificato in vManage di Disaster Recovery.

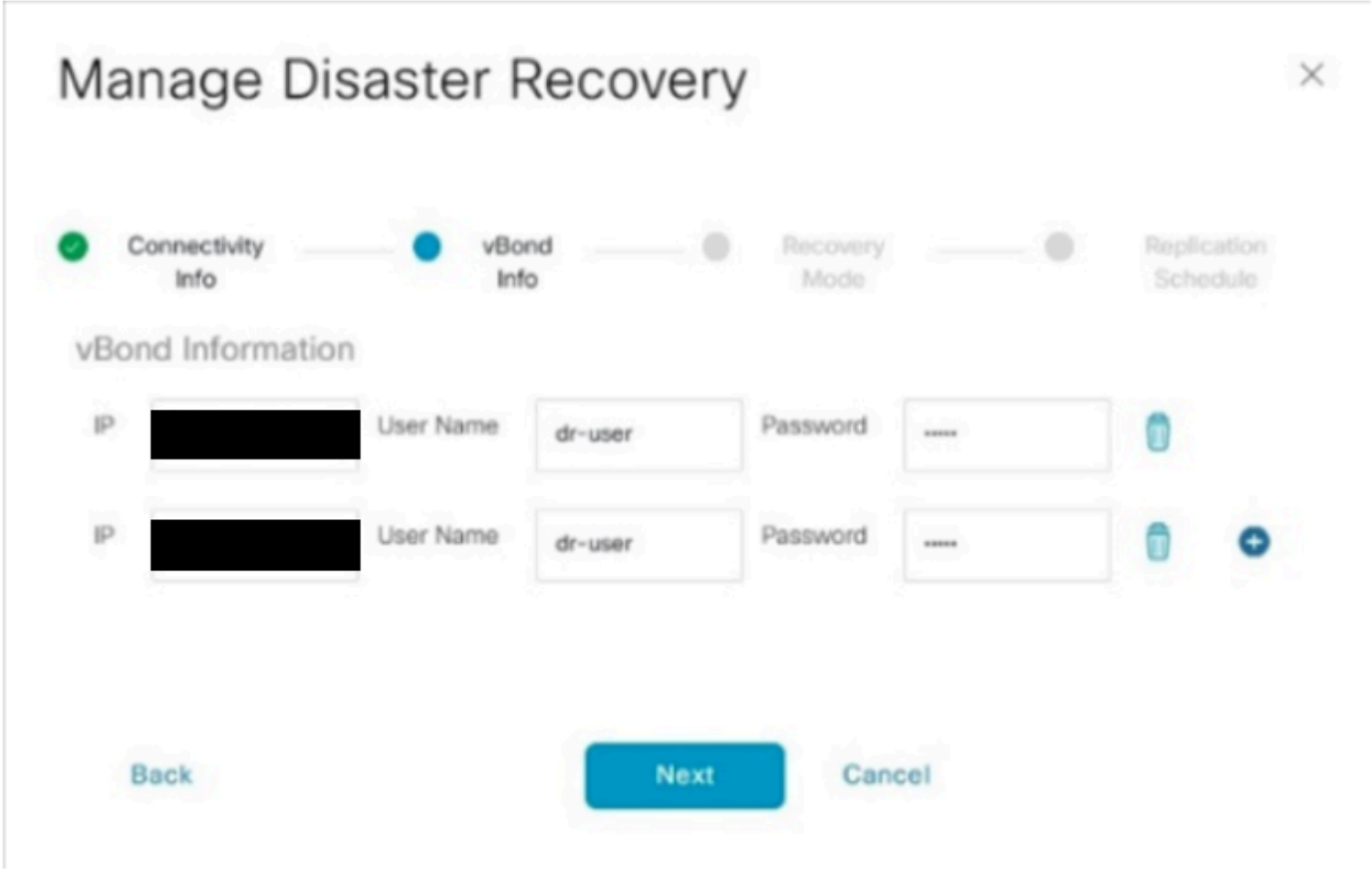
Aggiunta della configurazione del ripristino di emergenza

- Per questa operazione, passare alla versione principale di vManage.
- Passare a Amministrazione → Gestione cluster e indicare l'indirizzo IP dell'interfaccia fuori banda dopo aver fatto clic sui tre punti sul lato destro della voce vManage. Includere nome utente e password. Per questa configurazione è consigliabile creare un utente locale separato, ad esempio dradmin, sia sul server primario che su DR manage.



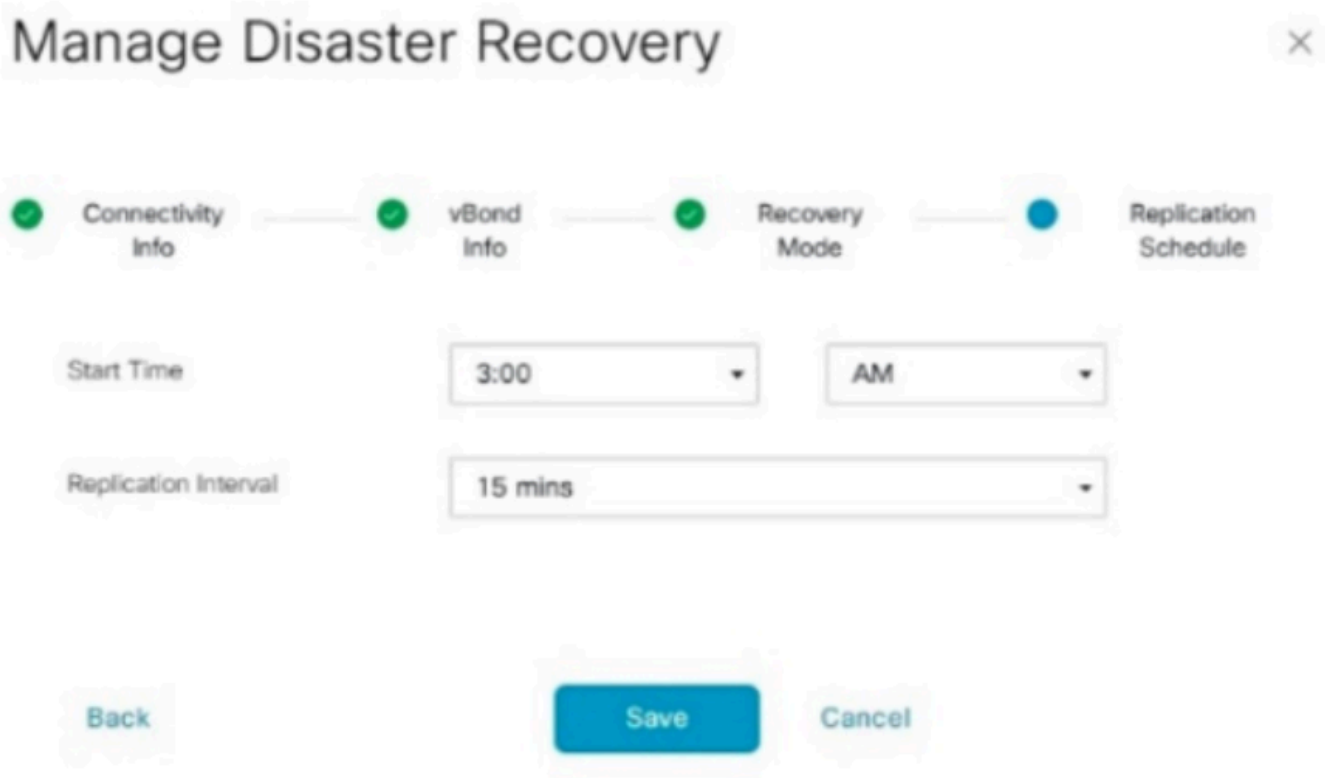
- VManage viene riavviato dopo questa modifica.
- Dopo l'accensione di vManage principale, passare a Amministrazione → Disaster Recovery. Fare clic su 'Manage Disaster Recovery' (Gestione ripristino di emergenza).
- Nella finestra popup, immettere i dettagli per vManage principale e secondario.
- Gli indirizzi IP da indicare sono gli indirizzi IP delle interfacce cluster fuori banda (eth2).
- Le credenziali devono essere quelle di un utente netadmin (dradmin) e non devono essere modificate una volta configurato il ripristino di emergenza. È possibile utilizzare una credenziale utente locale vManage separata per il ripristino di emergenza. È necessario verificare che l'utente locale vManage faccia parte del gruppo netadmin. È possibile utilizzare anche le credenziali di amministratore.

- Una volta compilato, fai clic su "Successivo".
- Specificare i dettagli dei controller vBond.
- I controller vBond devono essere raggiungibili nell'indirizzo IP specificato tramite Netconf.
- Le credenziali devono essere quelle di un utente netadmin (dradmin) e non devono essere modificate una volta configurato il ripristino di emergenza.
- Per questo motivo, è consigliabile che vBond disponga di questo utente dradmin configurato localmente oppure è possibile utilizzare l'utente admin per aggiungere il vBond.



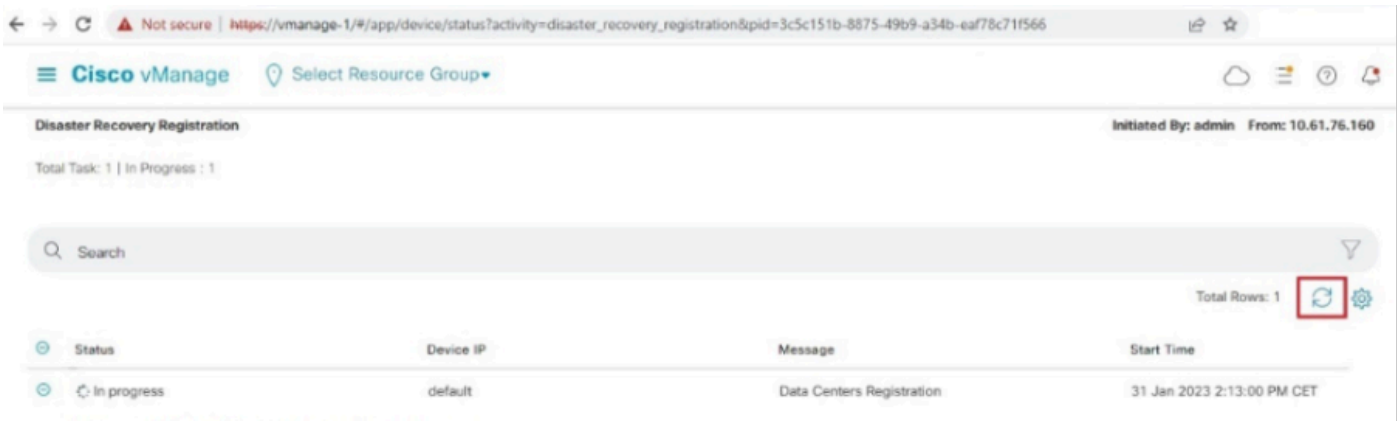
- Una volta compilato, fai clic su "Successivo".
- In modalità di ripristino, scegliere "Manuale". Fare clic su "Avanti".

Nella pianificazione della replica, impostare l'intervallo di replica".Ogni intervallo di replica, i dati vengono replicati dal database primario vManageto vManage secondario. Il valore minimo configurabile è 15 minuti.

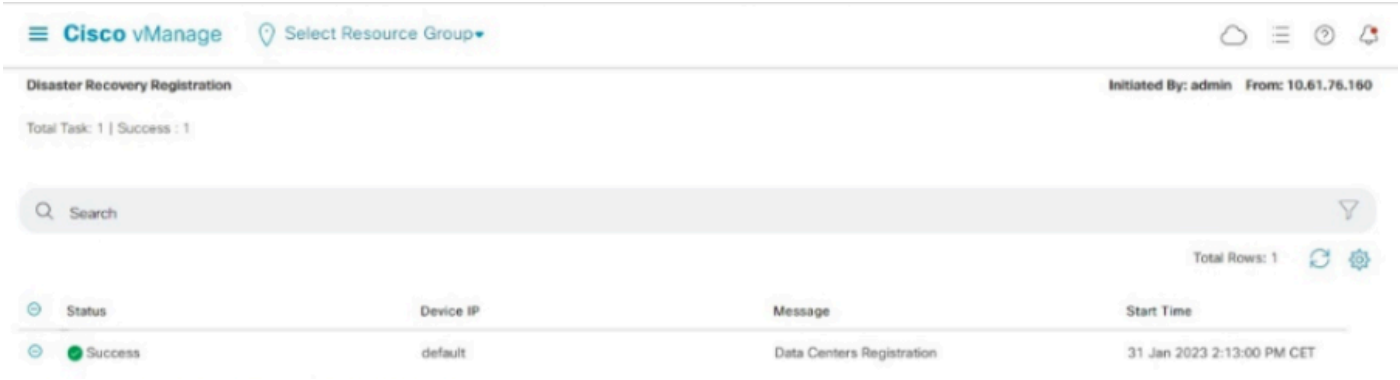


- Impostare il valore e fare clic su ‘Save’ (Salva).
- La registrazione del ripristino di emergenza inizia ora. Fare clic sul pulsante Aggiorna per aggiornare manualmente lo stato e i registri di stato. Questo processo può richiedere fino a

20-30 minuti.

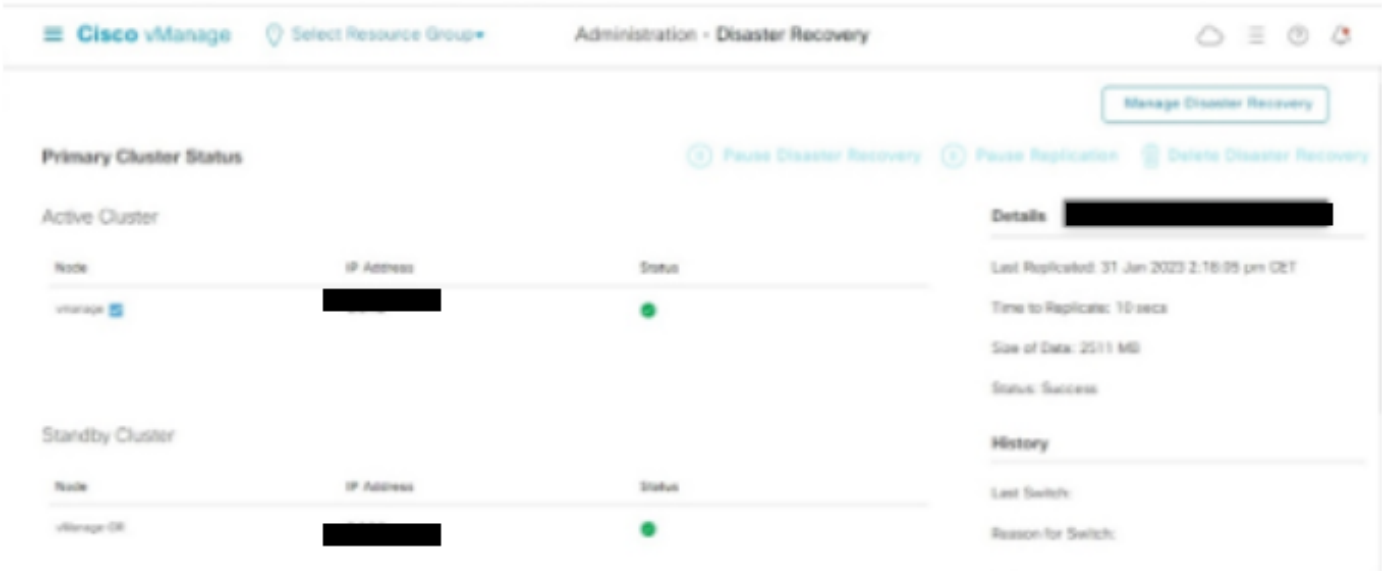


- Si noti che l'interfaccia utente grafica di vManage viene riavviata durante questo processo.
- Al termine, è necessario visualizzare lo stato Operazione completata.



Verifica

Passare a Amministrazione → Disaster Recoveryper verificare lo stato del ripristino di emergenza e la data dell'ultima replica dei dati.



Passaggio 5: Riautenticazione dei controller e annullamento della convalida dei controller precedenti

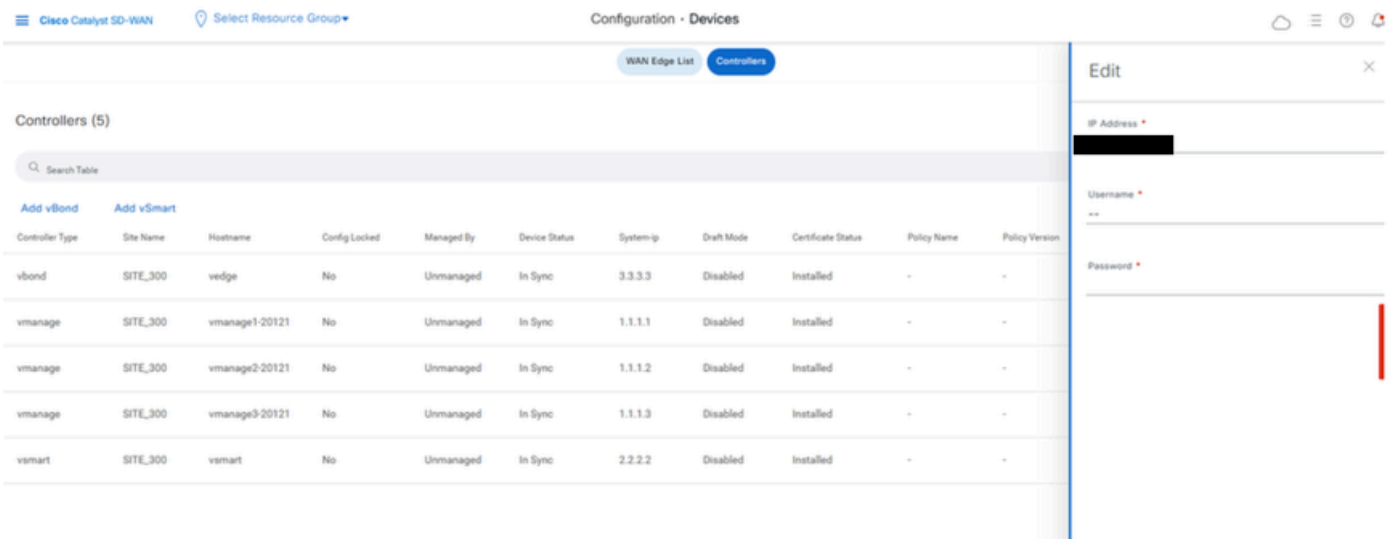
Una volta ripristinato il database di configurazione, è necessario riautenticare tutti i nuovi controller (manage/vsmart/vbond) nel fabric

---

Nota: nella produzione effettiva, se l'IP dell'interfaccia utilizzato per la riautenticazione è l'IP dell'interfaccia del tunnel, è necessario garantire che il servizio NETCONF sia consentito sull'interfaccia del tunnel di vManage, vSmart e vBond e anche sui firewall lungo il percorso. La porta firewall da aprire è la porta TCP 830 come regola bidirezionale dal cluster DR a tutti i vBonds e vSmarts.

Su vmanage UI, fare clic su Configurazione > Dispositivi > Controller

- Fare clic sui tre punti accanto a ciascun controller e scegliere Modifica



- Sostituire l'indirizzo ip (ip di sistema del controller) con l'indirizzo ip vpn 0 (interfaccia tunnel) del trasporto. Immettere il nome utente e la password e fare clic su Salva
- Eseguire la stessa operazione per tutti i nuovi controller nel fabric

Sincronizza la catena di certificati radice

Una volta caricati tutti i controller, attenersi a questa procedura:

Su qualsiasi server Cisco SD-WAN Manager nel cluster appena attivo, eseguire le seguenti azioni:

Immettere questo comando per sincronizzare il certificato radice con tutti i dispositivi Cisco Catalyst SD-WAN nel cluster appena attivo:

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

Immettere questo comando per sincronizzare l'UUID di Cisco SD-WAN Manager con Cisco SD-

WAN Validator:

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

Una volta ripristinata la struttura e attivate le sessioni bfd e di controllo per tutti i bordi e i controller della struttura, è necessario invalidare i vecchi controller (vmanage/vsmart/vbond) dall'interfaccia utente

- Su vmanage UI, fare clic su Configurazione > Dispositivi > Certificati
- Fare clic su Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su invalida
- Fare clic su Invia a vbond
- Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su Elimina

Passaggio 6: Registra assegni

Nota: Continuare con la sezione Controlli successivi mostrata qui, che è comune a tutte le combinazioni di distribuzione.

Combinazione 3: vManage Cluster + senza DR

Istanze necessarie:

- 3 vManage (cluster a 3 nodi, tutti COMPUTE_AND_DATA) o 6 vManage (3 COMPUTE_AND_DATA + 3 DATA)
- 1 o più vBond
- 1 o più vSmart

Passaggi:

1. Visualizzare tutte le istanze utilizzando l'opzione Passi comuni (Common Steps)
2. Controlli preliminari
3. Configurazione di interfaccia utente, certificati e controller integrati vManage
4. Crea cluster vManage
5. Backup/ripristino di Config-db
6. Registra assegni

Passaggio 1: Controlli preliminari

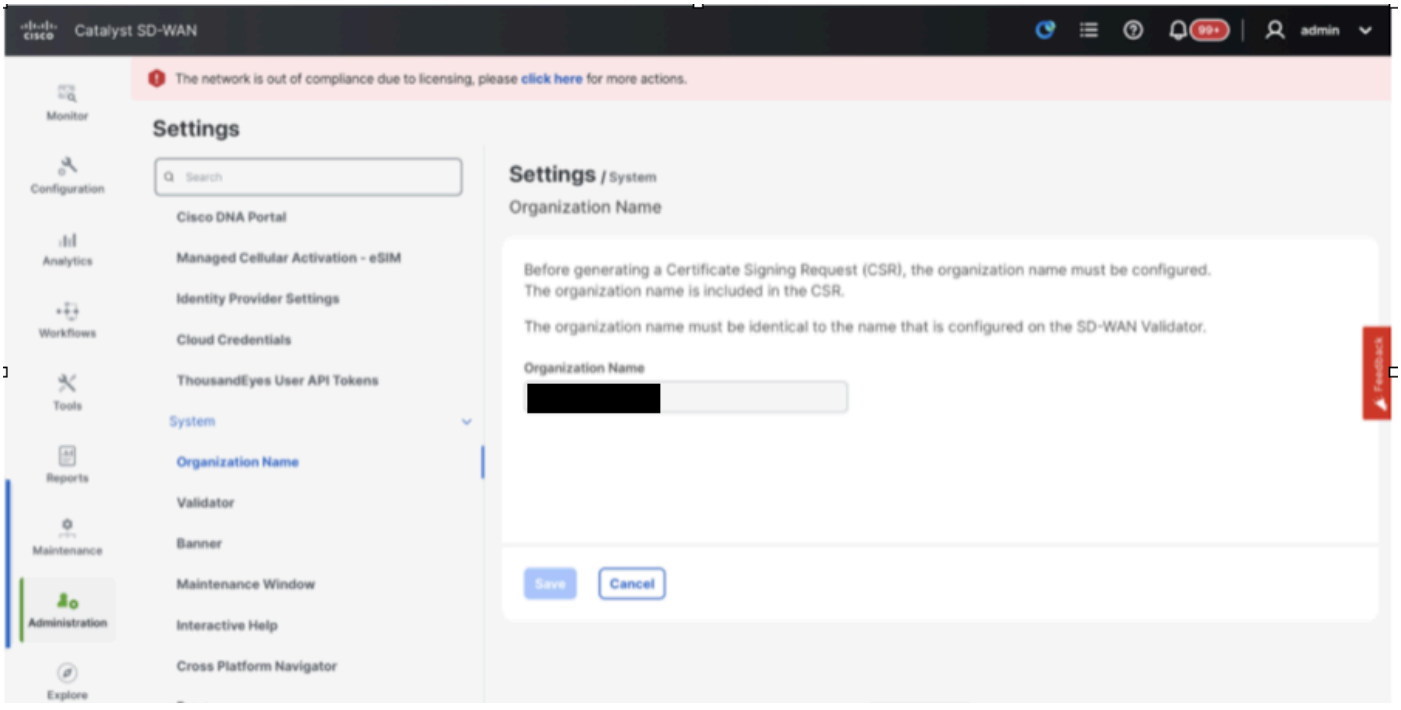
- Verificare che il numero delle istanze attive di Cisco SD-WAN Manager sia identico al numero delle nuove istanze di Cisco SD-WAN Manager installate.

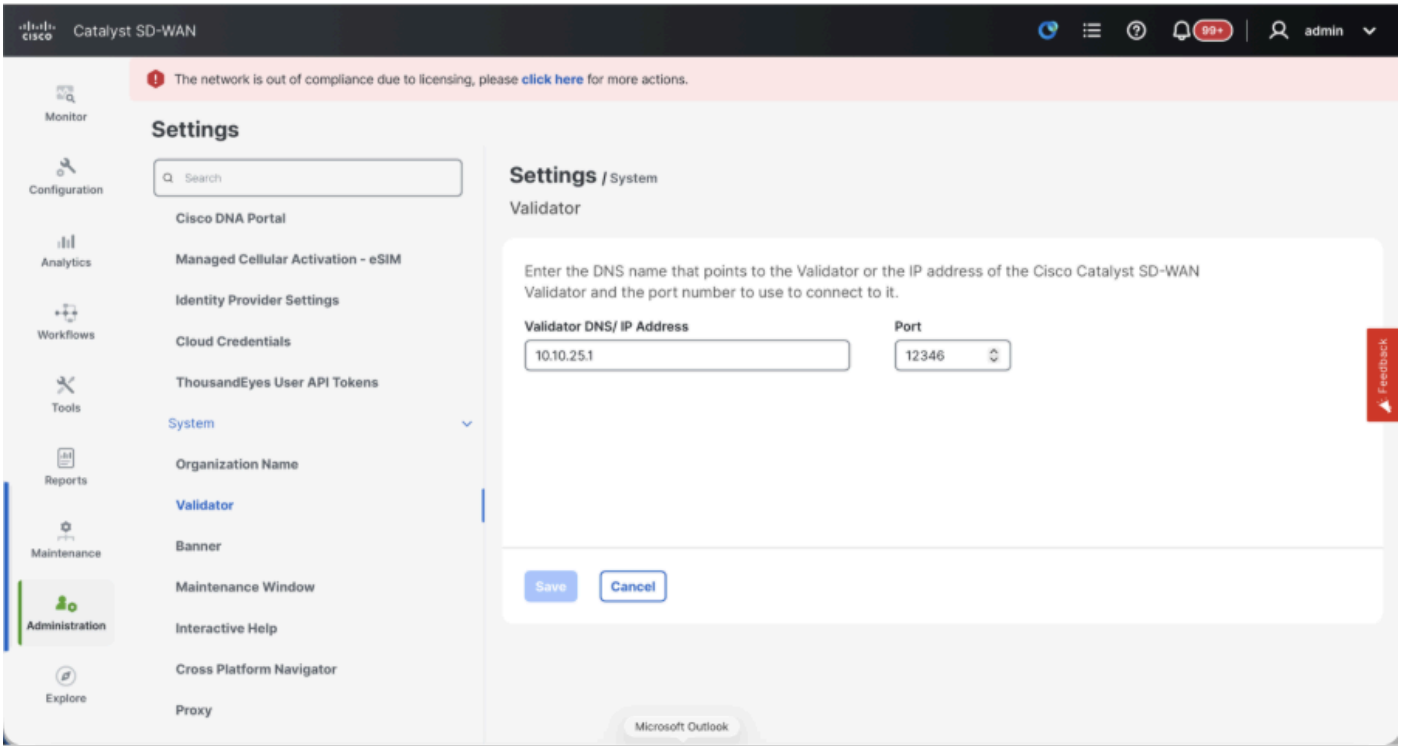
- Accertarsi che tutte le istanze Cisco SD-WAN Manager attive e nuove eseguano la stessa versione del software.
- Verificare che tutte le istanze Cisco SD-WAN Manager nuove e attive siano in grado di raggiungere l'indirizzo IP di gestione di Cisco SD-WAN Validator.
- Verificare che i certificati siano stati installati nelle istanze di Cisco SD-WAN Manager appena installate.
- Verificare che gli orologi di tutti i dispositivi Cisco Catalyst SD-WAN, incluse le nuove istanze di Cisco SD-WAN Manager installate, siano sincronizzati.
- Verificare che nelle istanze di Cisco SD-WAN Manager appena installate sia configurato un nuovo set di IP di sistema e ID di sito, insieme alla stessa configurazione di base del cluster attivo.

Passaggio 2: Configurazione di interfaccia utente, certificati e controller integrati vManage

Aggiornare le configurazioni nell'interfaccia utente di vManage

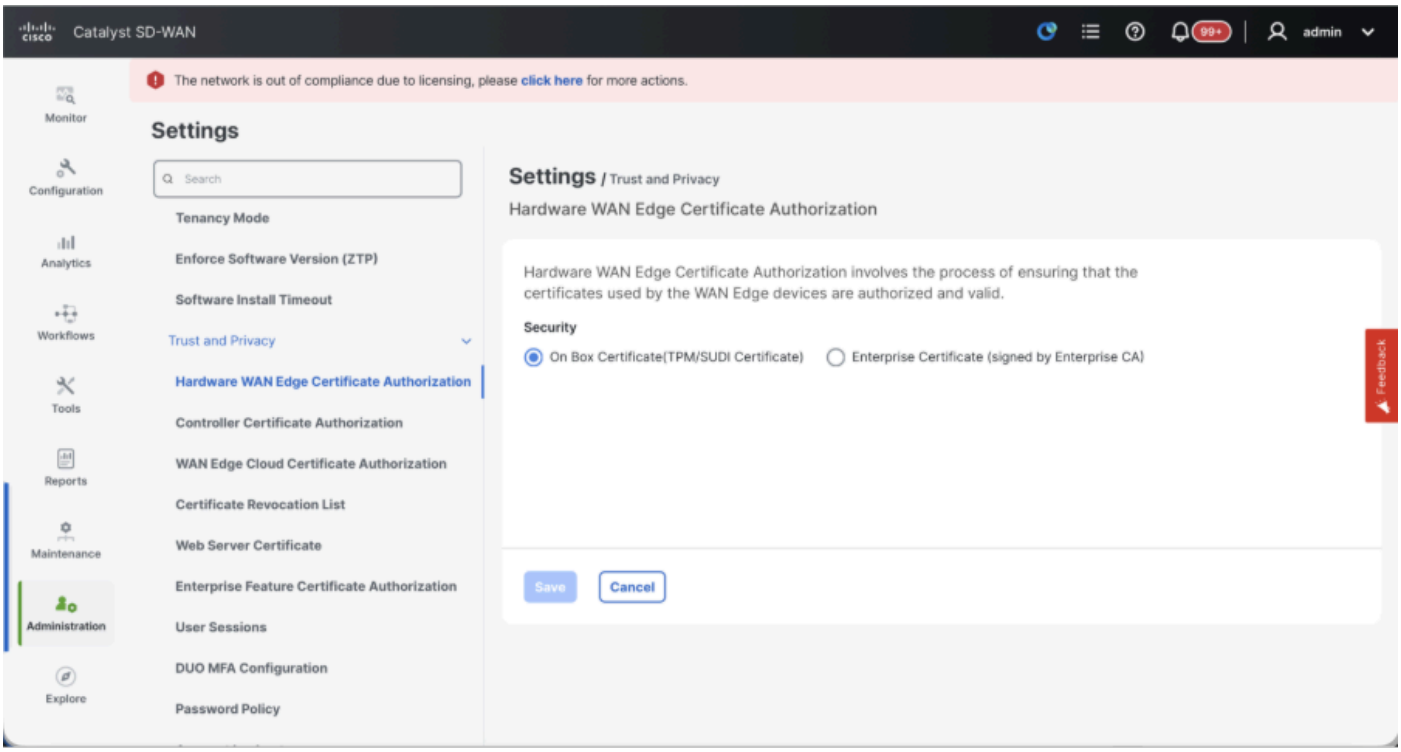
- Una volta aggiunte le configurazioni al passo 1 nella CLI di tutti i controller, possiamo accedere alla webUI di vManage, usando l'URL https://<vmanage-ip> nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi nodi vManage. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Amministrazione > Impostazioni e completare i seguenti passaggi.
- Configurare il nome dell'organizzazione e l'URL/indirizzo IP di Validator/vBond. Configurare lo stesso valore presente nella CLI del nodo vManage.
- In vManage 20.15/20.18 queste configurazioni sono disponibili nella sezione Sistema.



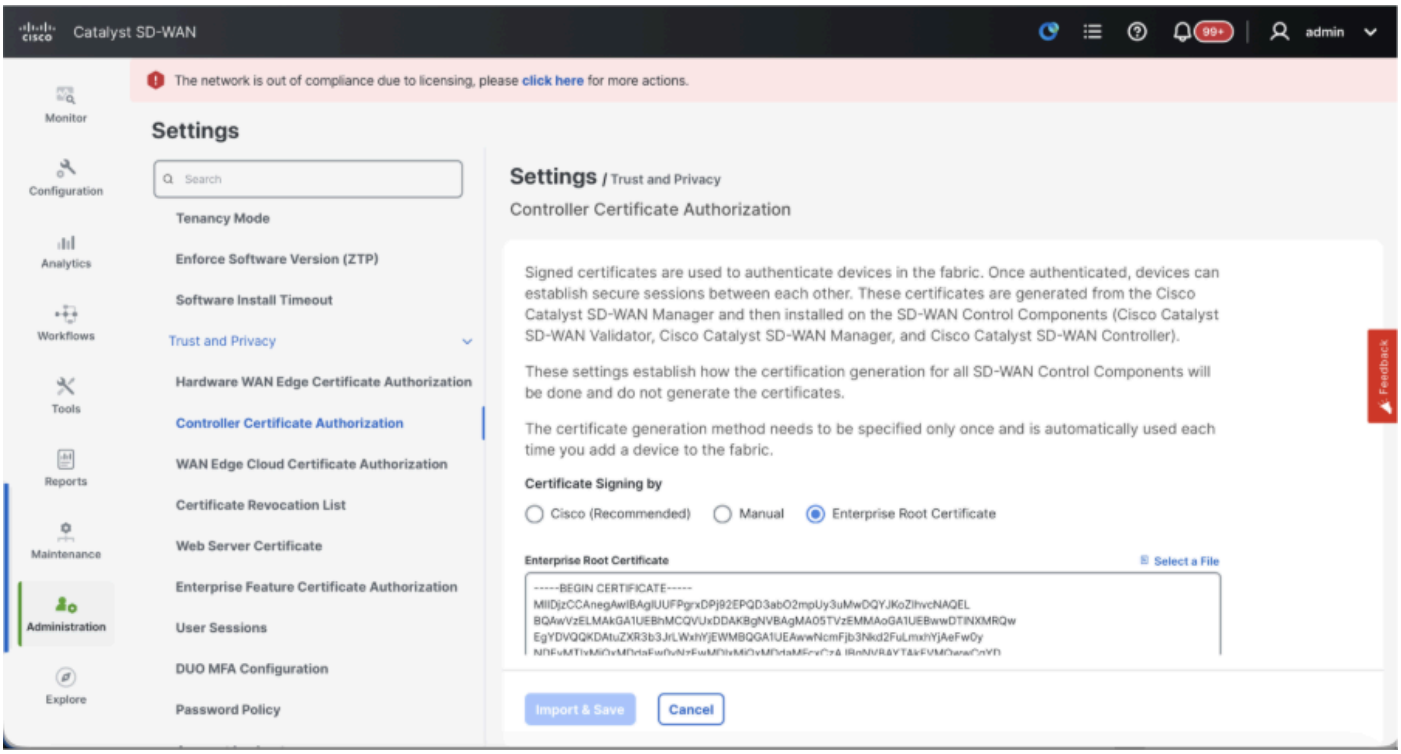


- Verificare le configurazioni per l'Autorità di certificazione (CA), che decide l'Autorità di certificazione utilizzata per firmare i certificati. Sono disponibili 3 opzioni:

1. Autorizzazione certificato perimetro WAN hardware - Decide la CA per i router perimetrali SD-WAN hardware.
    - Certificato On-Box (certificato TPM/SUDI): con questa opzione, il certificato preinstallato sull'hardware del router viene utilizzato per stabilire le connessioni di controllo (connessioni TLS/DTLS)
    - Certificato organizzazione (firmato dall'autorità di certificazione dell'organizzazione): questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

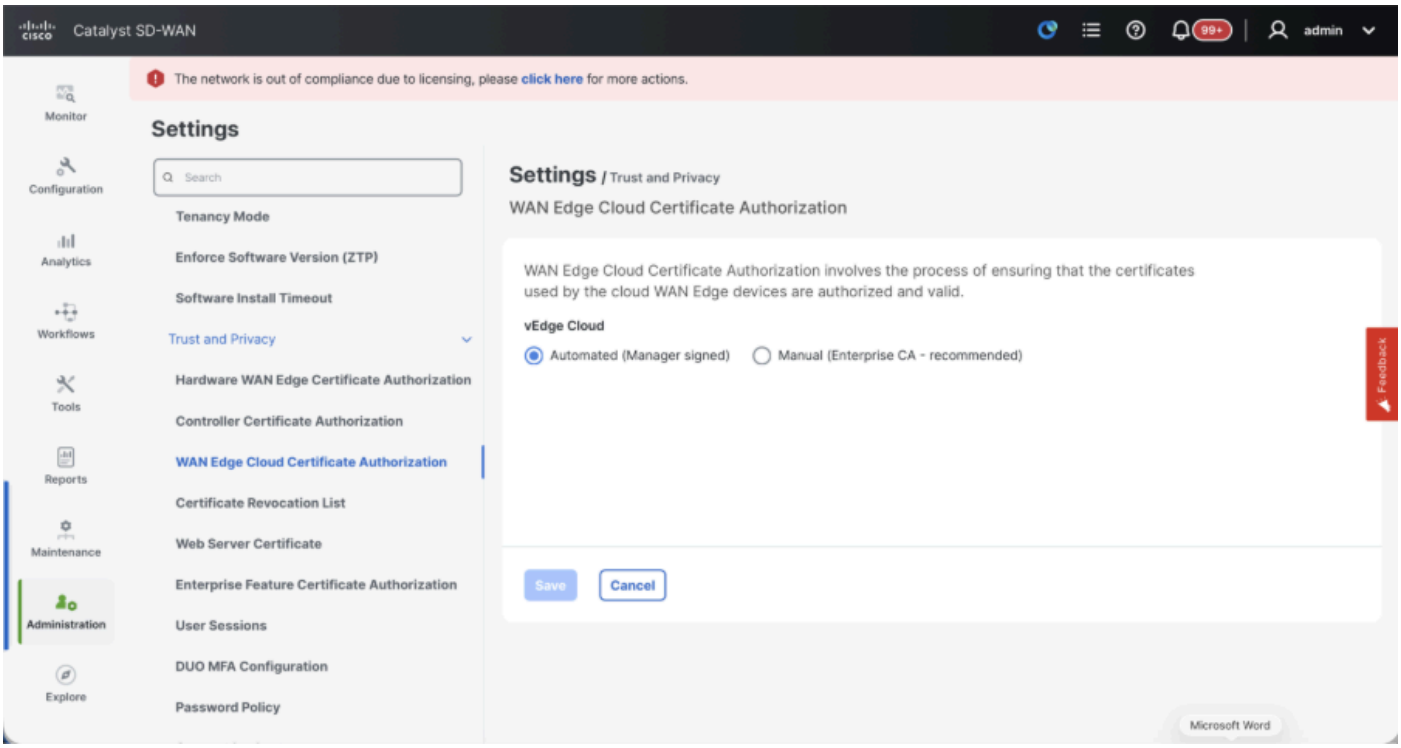


2. Controller Certificate Authorization - Decide la CA per i controller SD-WAN.
    - Cisco (scelta consigliata) - I controller utilizzano i certificati firmati da Cisco PKI. vManage contatta automaticamente il portale PNP utilizzando le credenziali dello smart account configurate in vManage e ottiene la firma del certificato che viene installato nel controller.
    - Manuale: i controller utilizzano i certificati firmati da Cisco PKI. Firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
    - Certificato radice dell'organizzazione: questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

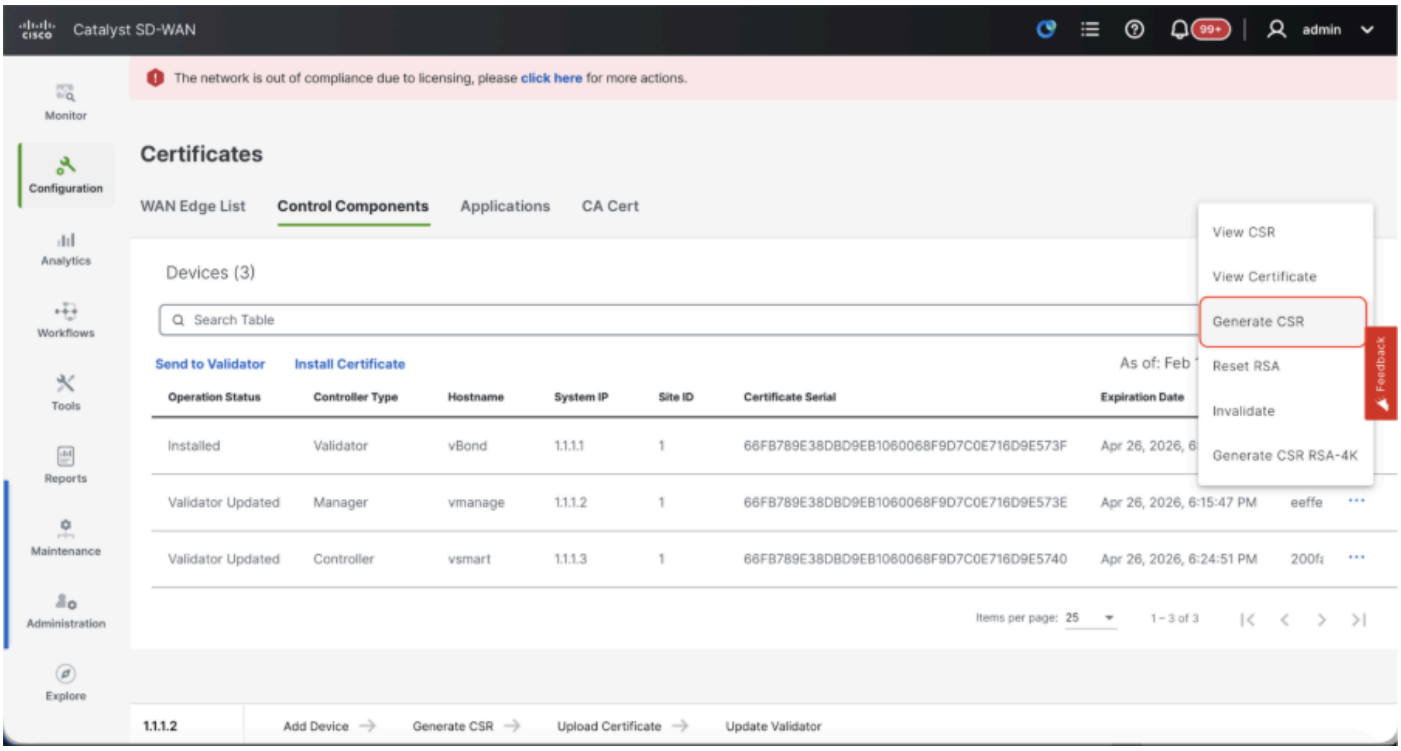


3. Autorizzazione certificato cloud perimetrale WAN - Decide la CA per i router perimetrali SD-WAN virtuali (CSR1000v, C8000v, vEdge cloud)
    - Automatizzato (vManage firmato): vManage firma automaticamente il CSR per i router perimetrali virtuali e installa il certificato sul router.
    - Manuale (Autorità di certificazione dell'organizzazione - consigliata) - I router virtuali utilizzano certificati firmati dall'Autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

Nel caso in cui si utilizzi la propria CA, Autorità di certificazione dell'organizzazione (enterprise), scegliere Enterprise.



- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller
- Fare clic su ... per Manager/vManage e fare clic su Generate CSR (Genera CSR).



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco

passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.

Caricamento di vBond/Validator e vSmart/Controller in vManage

Passare a Configurazione > Dispositivi > Controllo componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

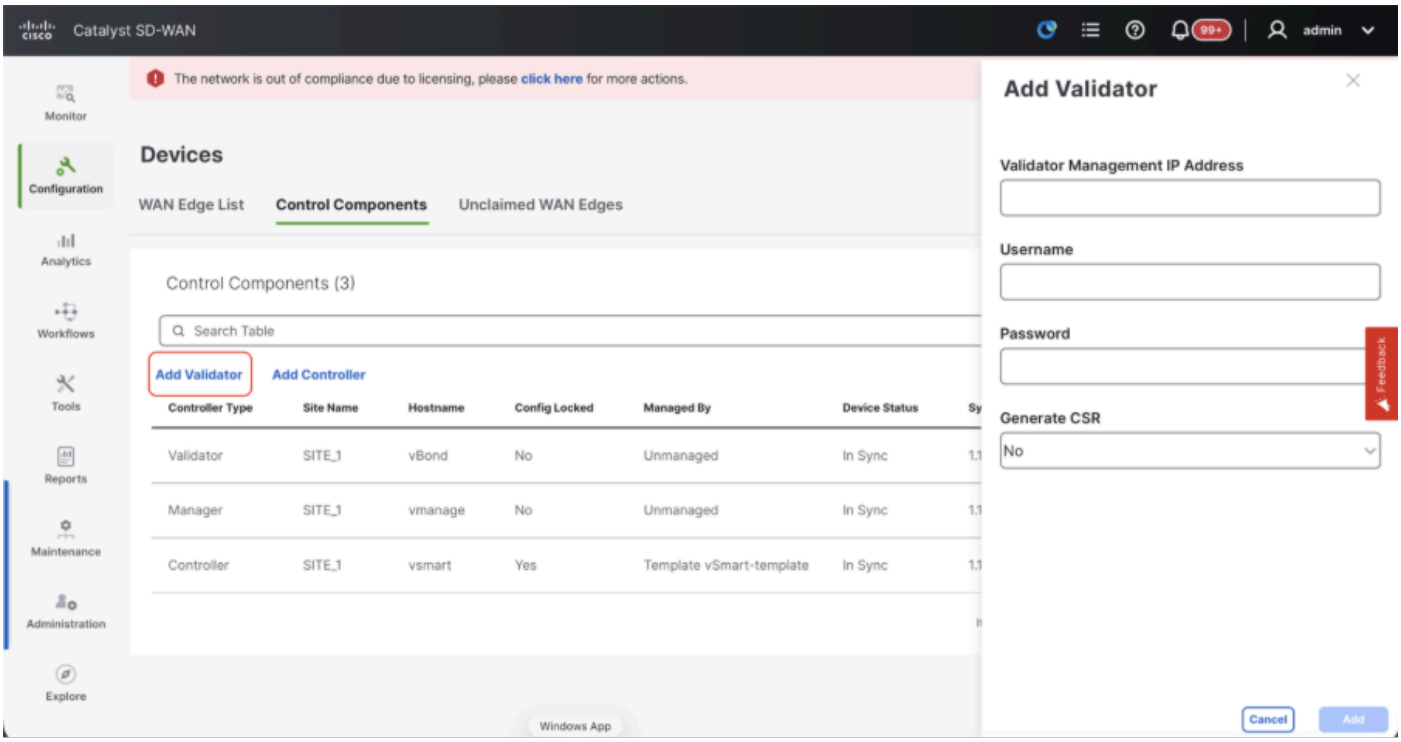
vBond/Convalida onboarding

- Fare clic su AddvBondnel caso di 20.12vManagerAggiungi validatornel caso di 20.15/20.18vManage. Viene visualizzato un popup, immettere il IP di trasporto VPN 0 di vBondraggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping se consentito dalla CLI di vManagetovBondIP.
- Immettere le credenziali utente di vBond.

Nota: è necessario utilizzare le credenziali di amministratore di vBondor una parte utente di netadmingroup. È possibile verificare questa condizione nella CLI di vBond. Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vBond

---

Nota: Se vBond è dietro un dispositivo/firewall NAT, verificare se l'IP dell'interfaccia VPN 0 di vBond è convertito in un IP pubblico. Se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, in questo passaggio utilizzare l'indirizzo IP pubblico dell'interfaccia VPN 0



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vBond.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vBonds, ripetere gli stessi passaggi.

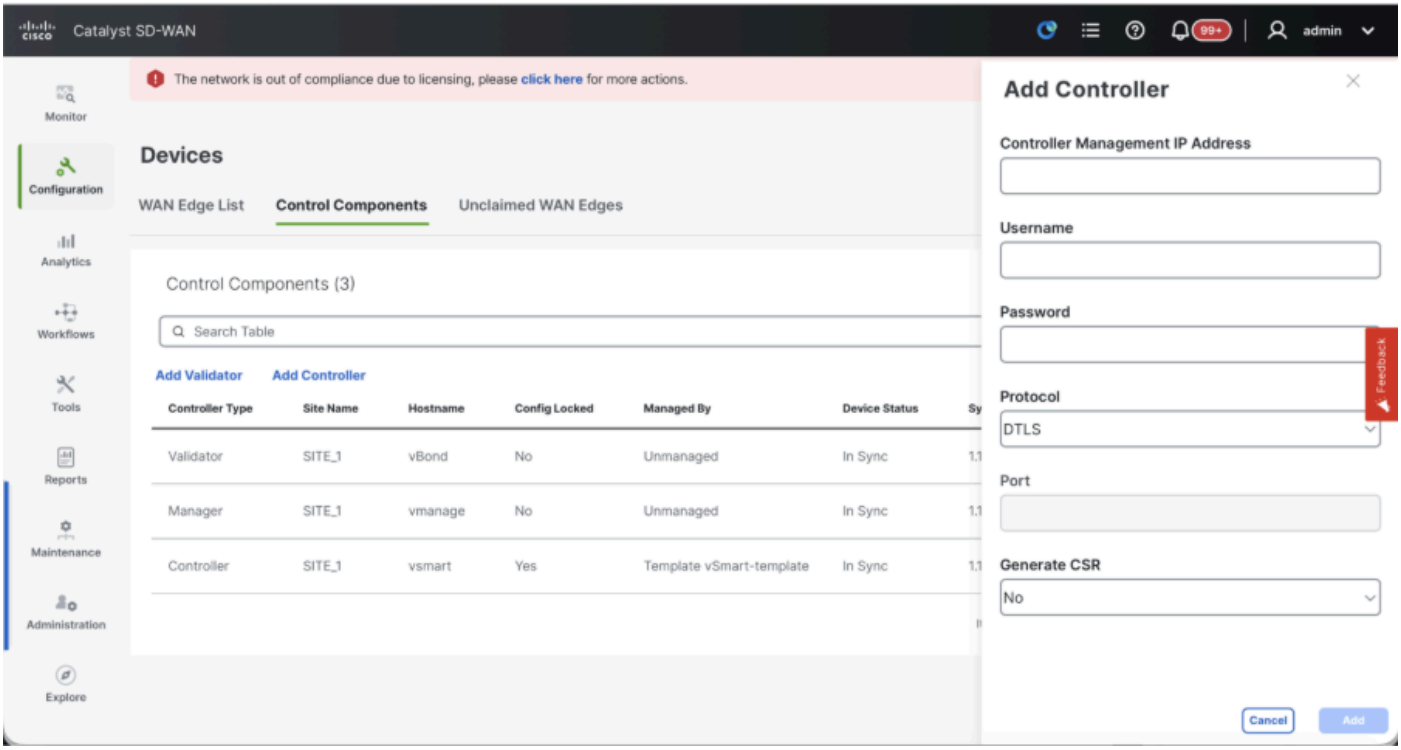
vSmart/Controller integrato

- Fare clic su Add vSmart in caso di vManage 20.12 o Add Controller in caso di vManage 20.15/20.18.
- Viene visualizzato un popup. Immettere l'IP di trasporto VPN 0 di vSmart raggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping, se consentito dalla CLI di vManage a vSmart IP.
- Immettere le credenziali utente di vSmart Note che è necessario utilizzare le credenziali di amministratore di vSmart o di un utente appartenente al gruppo netadmin.
- È possibile verificare questa condizione nella CLI di vSmart.
- Impostare il protocollo su TLS se si intende utilizzare TLS per i router per stabilire

connessioni di controllo con vSmart. Questa configurazione deve essere configurata anche sulla CLI dei nodi vSmarts e vManage.

- Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vSmart.

Nota: se vSmart è dietro un dispositivo/firewall NAT, verificare se l'indirizzo IP dell'interfaccia vSmart VPN 0 è convertito in un indirizzo IP pubblico e se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, utilizzare l'indirizzo IP pubblico dell'indirizzo IP dell'interfaccia VPN 0 in questo passaggio.

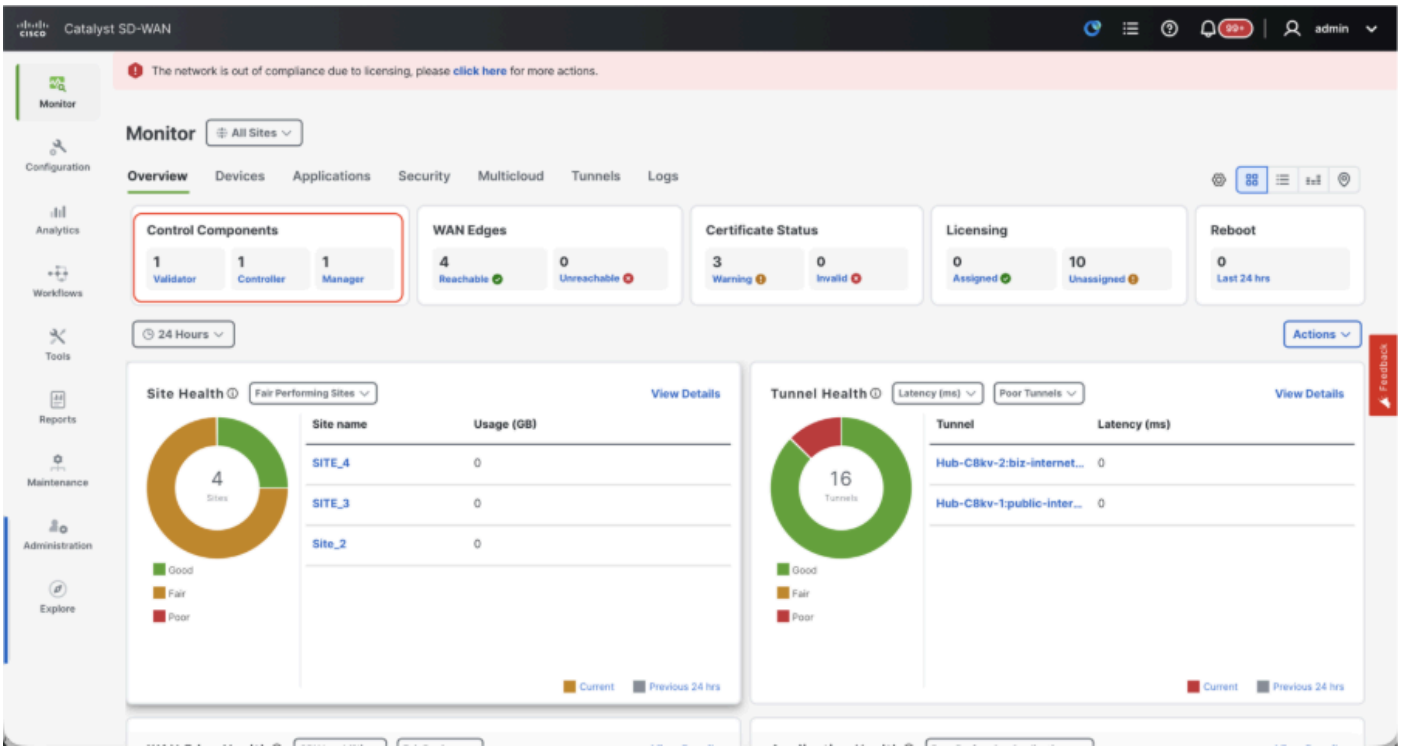


- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vSmart.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vSmarts, ripetere gli stessi passaggi.

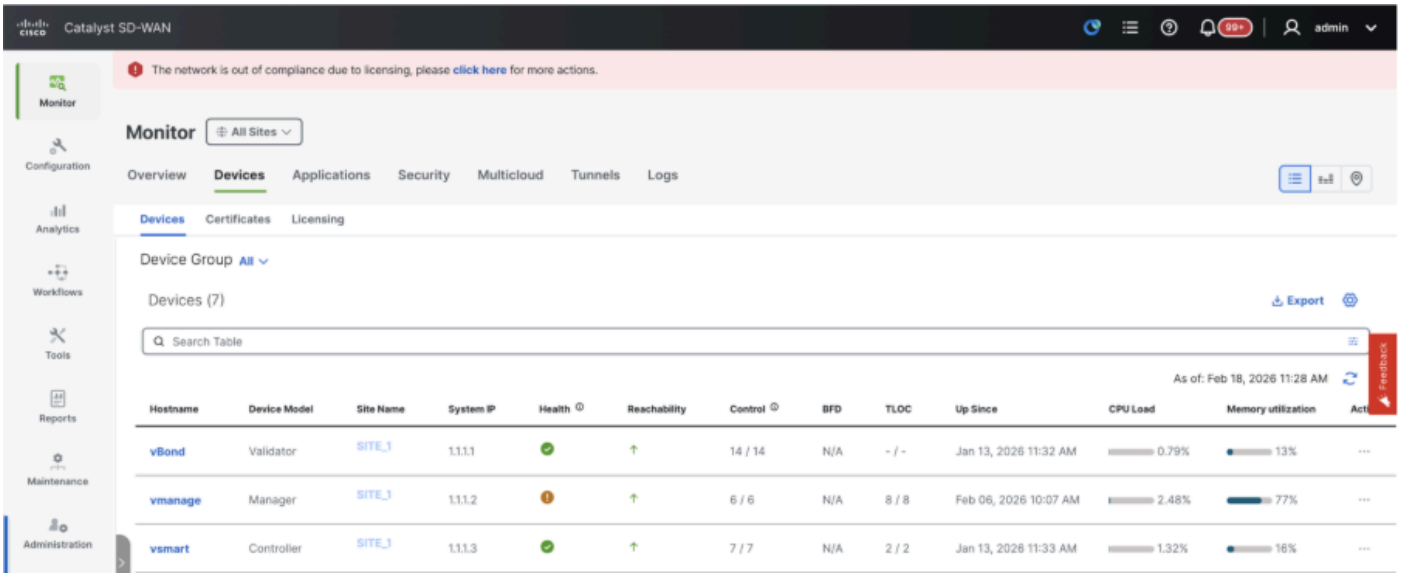
Verifica

Una volta completati tutti i passaggi, verificare che tutti i componenti di controllo siano raggiungibili

in Monitor>Dashboard



- Fate clic sui rispettivi componenti di controllo e verificate che siano tutti raggiungibili.
- Passare a Monitor > Dispositivi e verificare che tutti i componenti di controllo siano raggiungibili.



Passaggio 3: Crea cluster vManage

Fabric SD-WAN integrato con un cluster vManage nella sovrapposizione SD-WAN

Nota: il cluster vManage può essere configurato con 3 nodi vManage o 6 nodi vManage a seconda del numero di siti collegati all'infrastruttura SD-WAN. Fare riferimento al cluster

---

vManage esistente e scegliere il numero di nodi in base allo stesso.

Configurare le configurazioni CLI di tutti i nodi vManage appartenenti al cluster

Configura configurazione di sistema in tutti i nodi vManage

- Configurare gli altri nodi vManage. In caso di cluster a 3 nodi, sono disponibili 2 nodi da configurare, in caso di cluster a 6 nodi sono disponibili 5 nodi da configurare.
- Configurare le configurazioni di sistema come mostrato:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Nota: se si utilizza URL come indirizzo vBond, verificare di configurare gli indirizzi IP dei server DNS nella configurazione VPN 0 o di risolverli.

Configura interfaccia di trasporto su tutti i nodi vManage

Queste configurazioni sono necessarie per abilitare l'interfaccia di trasporto utilizzata per stabilire le connessioni di controllo con i router e gli altri controller.

```
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
```

Configura interfaccia di gestione su tutti i nodi vManage

Configurare inoltre l'interfaccia di gestione VPN 512 per consentire l'accesso di gestione fuori banda al controller.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Configurazione facoltativa:

- È possibile fare riferimento alle configurazioni del controller esistente e, se la configurazione indicata è presente, è possibile aggiungerla ai nuovi controller.
- Configurare il protocollo di controllo come TLS solo se i router devono stabilire connessioni di controllo protette con i nodi vManage che utilizzano TLS. Per impostazione predefinita, tutti i controller e i router stabiliscono una connessione di controllo utilizzando il protocollo DTLS. Si tratta di una configurazione opzionale richiesta solo sui nodi vSmart e vManage a seconda delle esigenze.

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

Configura interfaccia di servizio in tutti i nodi vManage

Configurare l'interfaccia del servizio su tutti i vManagenodes, incluso vManage-1 che è già stato

caricato. Questa interfaccia viene utilizzata per la comunicazione del cluster, ovvero la comunicazione tra i vManagenodes nel cluster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Verificare che per l'interfaccia di servizio in tutti i nodi del cluster vManagement venga utilizzata la stessa subnet IP.

Configura credenziali cluster

È possibile utilizzare le stesse credenziali di amministrazione dei nodi vManage per configurare il cluster vManage. In caso contrario, è possibile configurare una nuova credenziale utente che faccia parte di netadmingroup. Le configurazioni per la configurazione delle nuove credenziali utente sono le seguenti

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

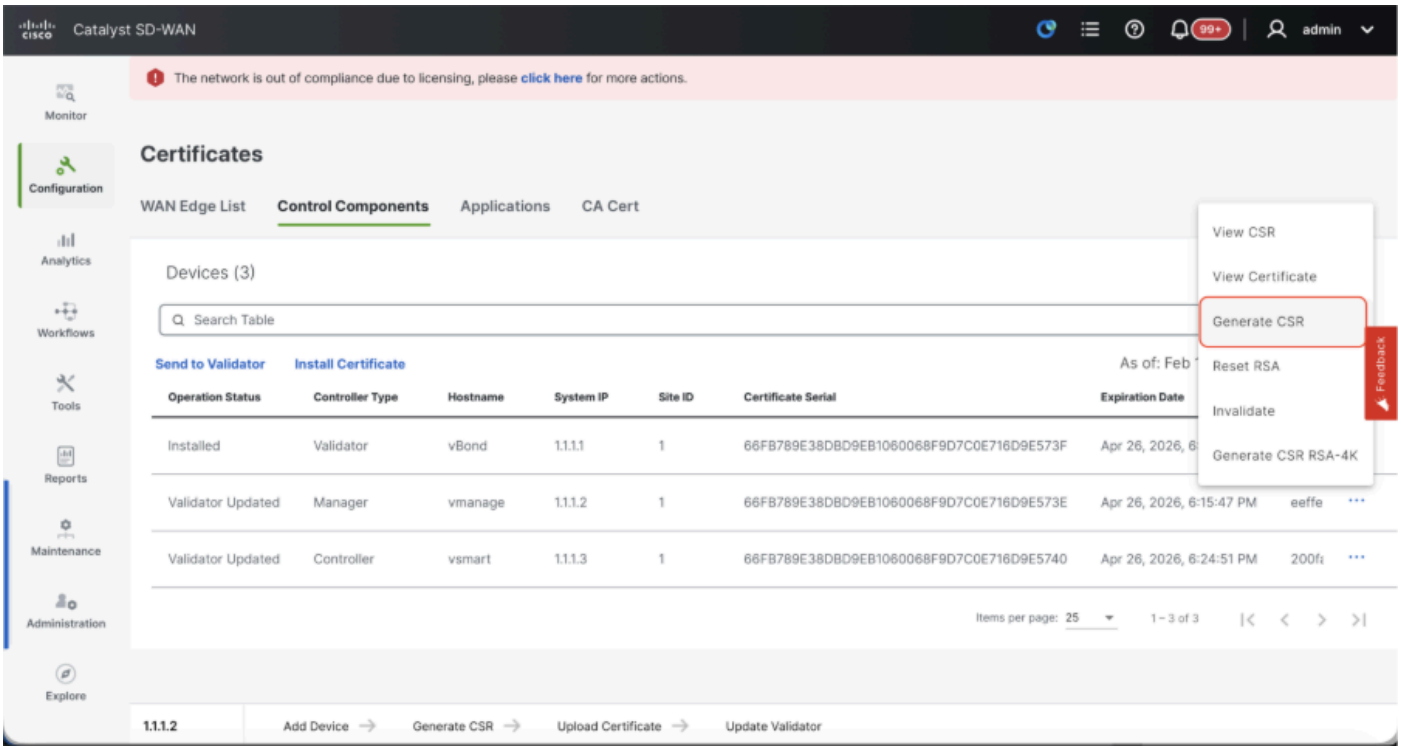
Assicurarsi di configurare le stesse credenziali utente in tutti gli vManagenodesche fanno parte del cluster.Se si decide di utilizzare le credenziali di amministratore, è necessario che siano lo stesso

nome utente/password in tutti gli vManagenodes.

Installa certificato dispositivo in tutti i nodi vManage

- Accedere a vManageUI di tutti i vManagenodes utilizzando l'URL https://<vmanage-ip>nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi vManagenode. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

  Fare clic su ... per Manager/vManage e fare clic su Generate CSR.



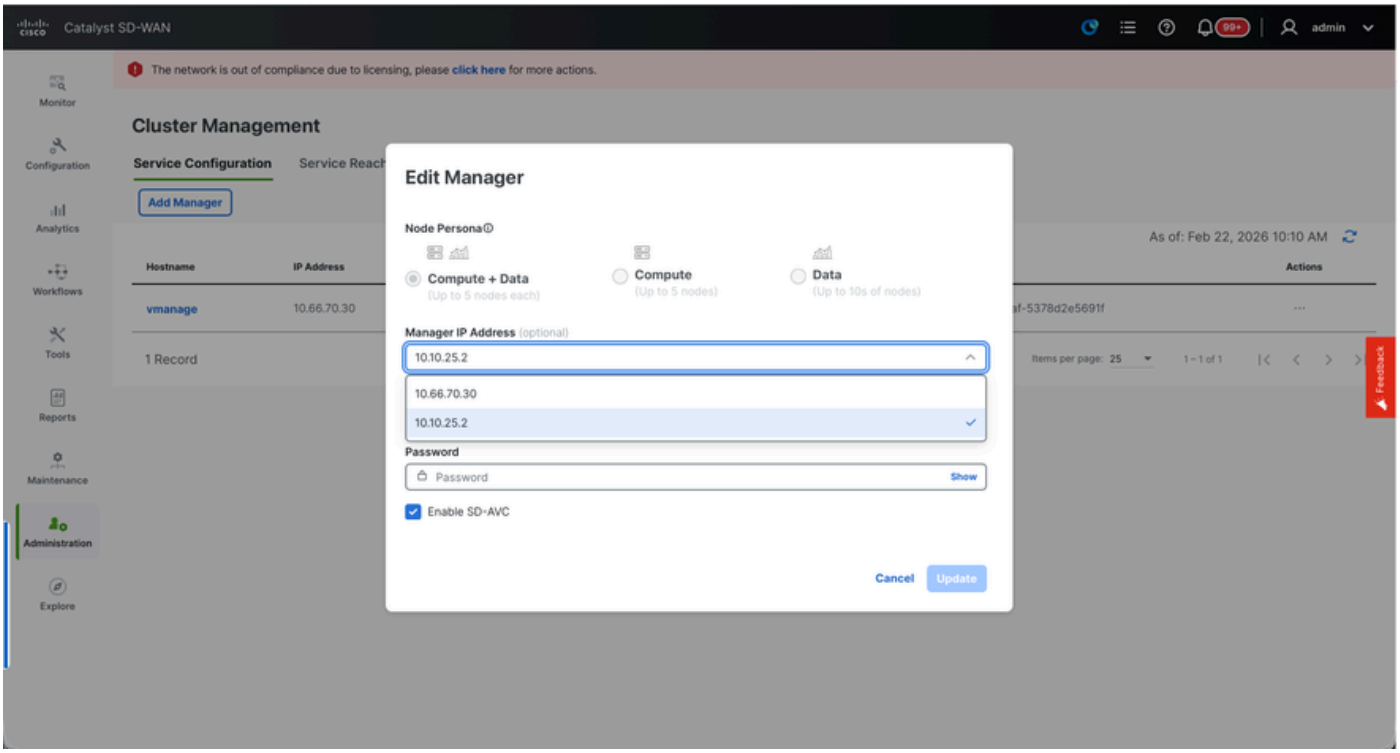
- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della relativa sovrapposizione SD-WAN. La stessa procedura è applicabile se si utilizza il certificato radice Digicert ed Enterprise.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- Completare questo passaggio in tutti i nodi vManage che fanno parte del cluster.

Preparare la creazione del cluster vManage

- Sul WebUI di vManage-1, selezionare Amministrazione > Gestione cluster, fare clic su ... in Azioni per vManage-1, scegliere Modifica.
- La persona del nodo viene scelta automaticamente in base alla persona scelta durante lo spun up della VM.

Nota: Per un cluster a 3 nodi, tutti e 3 i nodi vManage vengono visualizzati con compute+data come persona.

- Per un cluster a 6 nodi, vengono visualizzati 3 nodi vManage con dati di tipo compute+data come utente e 3 nodi vManage come utente.
- Dall'elenco a discesa per l'indirizzo IP di Manager, assicurarsi di scegliere l'indirizzo IP dell'interfaccia di servizio di vManage.

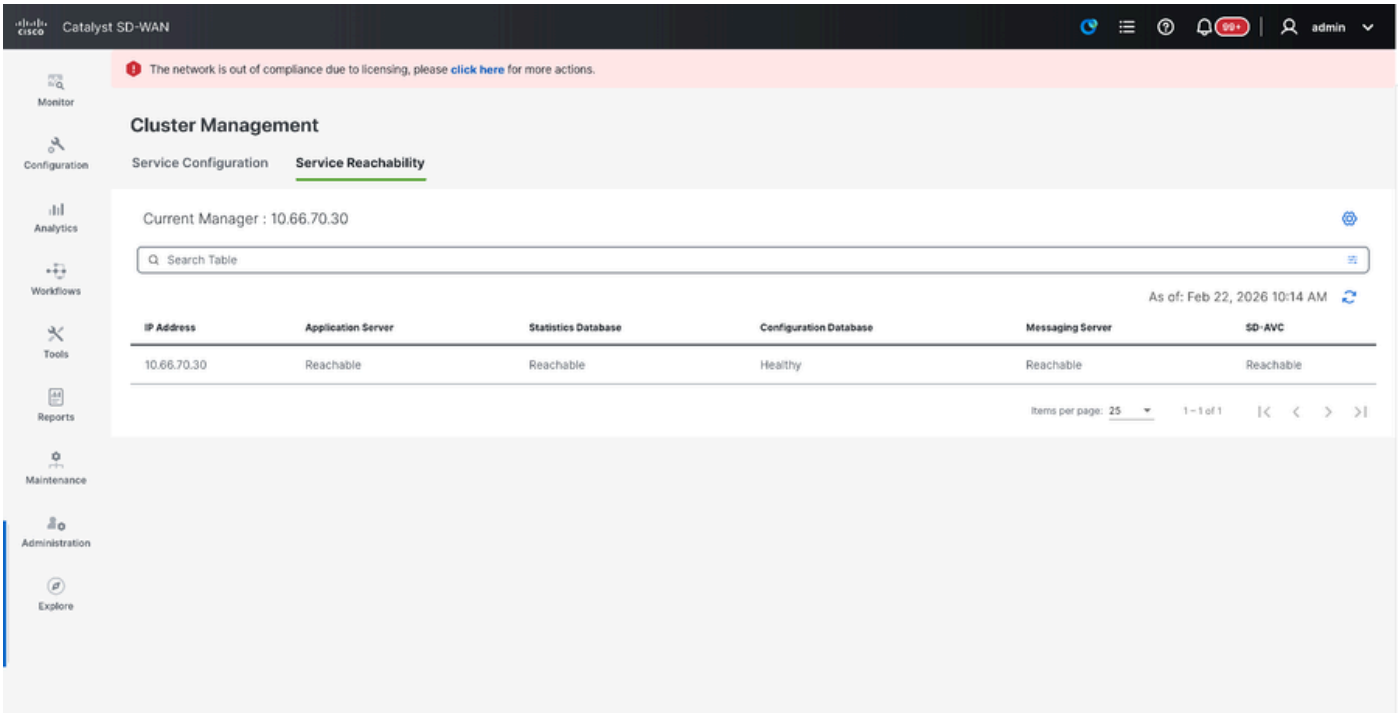


- Immettere il nome utente e la password che si desidera utilizzare per abilitare il cluster vManage, definito credenziali del cluster.
- Come accennato in precedenza, è necessario configurare le stesse credenziali su tutti i nodi vManage e utilizzarle durante l'aggiunta di tutti i nodi al cluster.

Nota: Fare riferimento a questa configurazione nel cluster esistente per abilitare SDAVC. Deve essere verificata solo se è richiesta ed è necessaria solo su un nodo vManage del cluster.

Fare clic su Aggiorna.

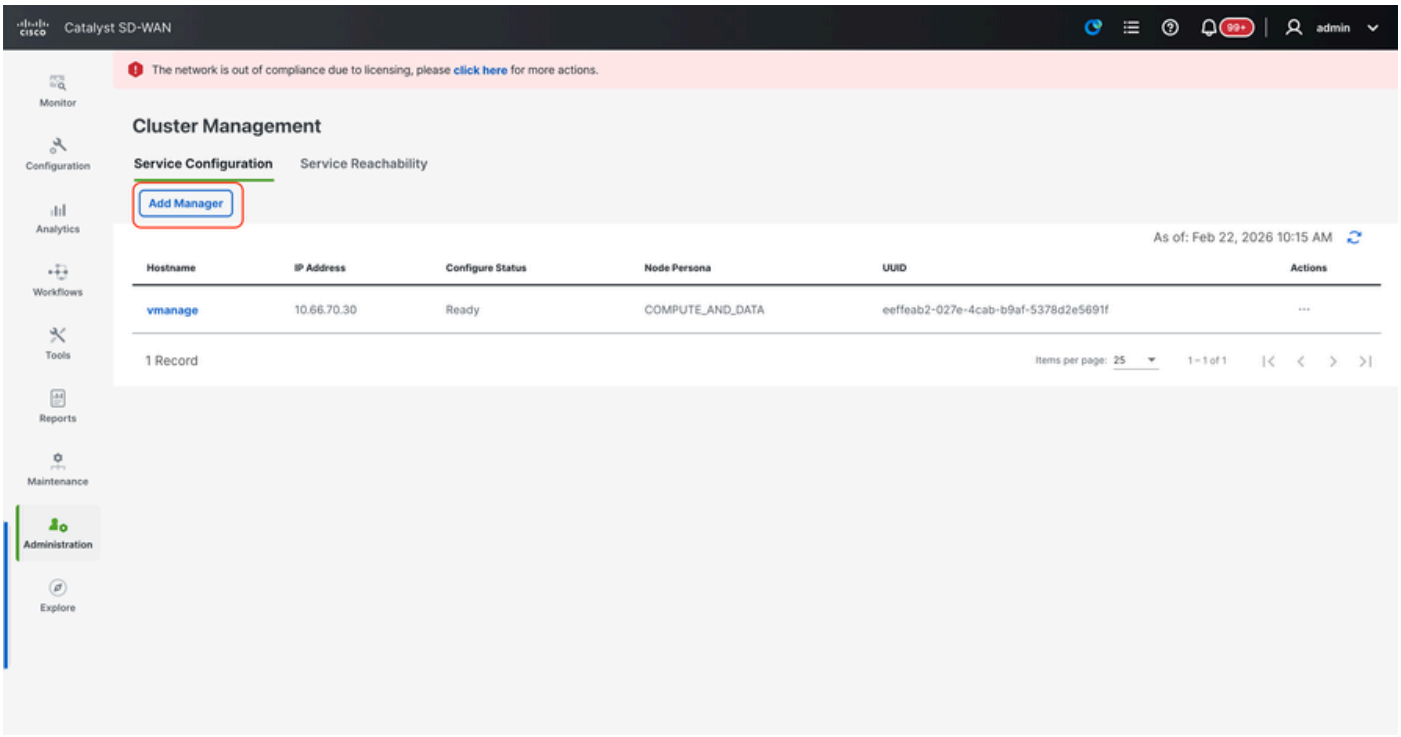
- In seguito, i servizi vManage NMS vengono riavviati in background e l'interfaccia utente non è disponibile per alcuni minuti, dai 5 ai 10 minuti circa. Durante questo periodo, l'accesso CLI di vManage è disponibile.
- Una volta che l'interfaccia utente di vManage-1 è accessibile, passare a Amministrazione > Gestione cluster, assicurarsi che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP,Lo stato della configurazione è Pronto e la persona del nodo viene riflessa correttamente.
- Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili.

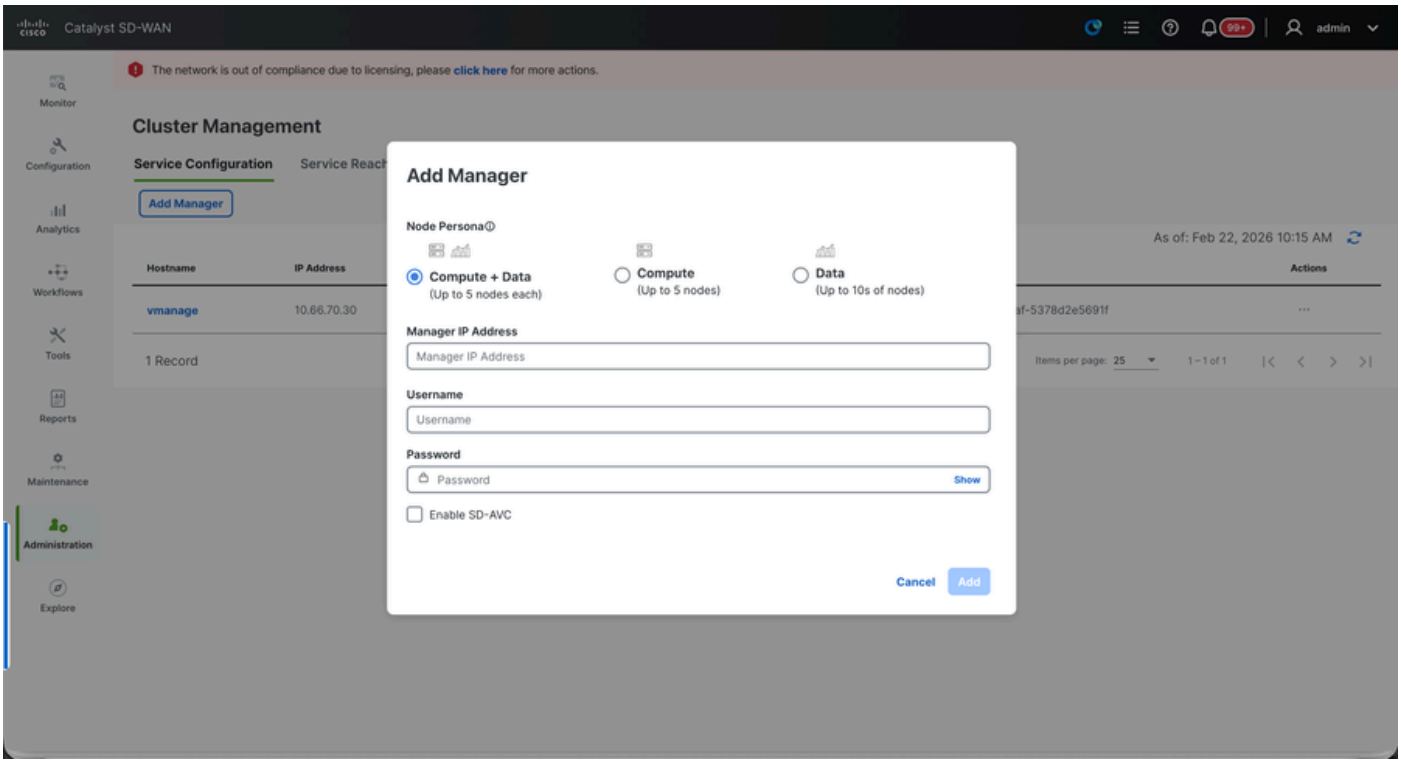


- Se si rileva che uno dei servizi non è ancora raggiungibile, attendere. Di solito ci vogliono dai 20 ai 30 minuti.

Crea il cluster vManage

- Sul WebUI di vManage-1, selezionare Amministrazione > Gestione cluster, nella sezione Configurazione servizio,
- Fare clic su Add Manager, viene visualizzata una finestra popup:

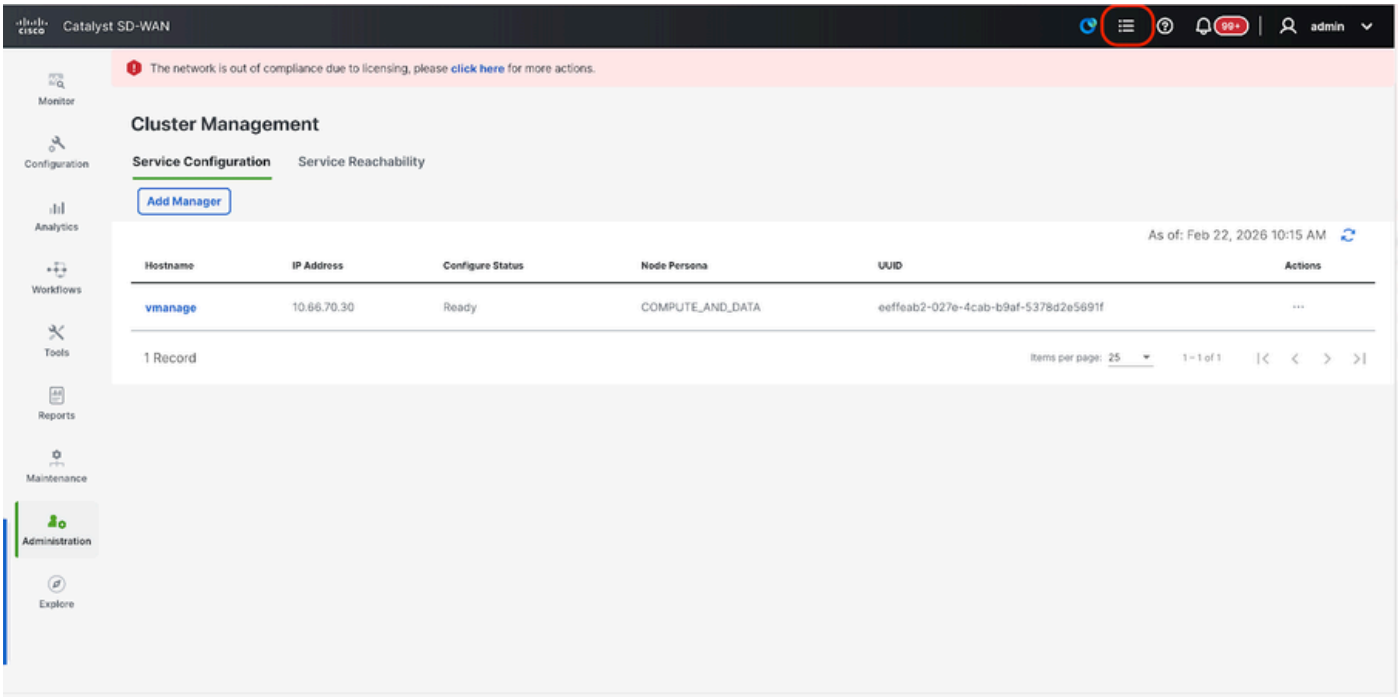




- Scegliere la persona Nodo in base alle configurazioni della persona eseguite durante l'esecuzione dello spun-up del nodo vManage - 2.
- Immettere l'indirizzo IP dell'interfaccia di servizio di vManage-2 in Indirizzo IP manager
- Immettere il nome utente e la password, ovvero le stesse credenziali utilizzate nel passaggio 6.
- Abilita SDAVC - Da lasciare deselezionato come avremmo già abilitato su vManage-1
- Fare clic su Aggiungi.
- In seguito, i servizi vManage NMS vengono riavviati in background per i nodi vManage 1 e 2. L'interfaccia utente non è disponibile per alcuni minuti, dai 5 ai 10 minuti circa, per vManage

1 e 2.

- Durante questo periodo, è disponibile l'accesso CLI di vManage 1 e 2.
- Una volta che l'interfaccia utente di vManage-1 è accessibile, passare a Amministrazione > Gestione cluster, verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP, Configura stato sia Pronto e che la persona del nodo sia indicata correttamente.
- Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili per entrambi i nodi vManage.
- Se si rileva che uno dei servizi non è ancora raggiungibile, attendere. Di solito ci vogliono dai 5 ai 10 minuti.
- È possibile controllare lo stato del processo di aggiunta cluster nell'elenco Attività disponibile nell'angolo superiore destro dell'interfaccia utente di vManage.



- È possibile cercare Elenco attività attivo e se l'attività è ancora elencata in Elenco attività attivo, indica che l'attività non è stata ancora completata.
- È possibile fare clic sull'attività per verificarne lo stato di avanzamento. Se l'attività non è elencata in Elenco attività attivo, passare a Completato e assicurarsi che l'attività sia stata completata correttamente.
- Solo dopo la convalida di questi punti, procedere al passaggio successivo.

Prima di aggiungere il nodo successivo al cluster, è necessario prendere in considerazione i seguenti punti:

Verificare questi punti in tutte le interfacce utente dei nodi vManage aggiunti al cluster:

- Passare a Monitoraggio > Panoramica dell'interfaccia utente di vManage e verificare che il numero di nodi vManage sia indicato correttamente e che sia raggiungibile a seconda del numero di nodi aggiunti al cluster.

- Passare a Amministrazione > Gestione cluster e verificare che l'indirizzo IP dell'interfaccia di

servizio di vManage sia indicato in Indirizzo IP, che Configura stato sia Pronto e che la persona del nodo sia indicata correttamente.
- Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili per entrambi i nodi vManage.

- Ogni volta che un nodo viene aggiunto al cluster, i servizi NMS di tutti i nodi nel cluster vengono riavviati, pertanto l'interfaccia utente di tutti questi nodi diventa irraggiungibile per un certo periodo di tempo.
- A seconda del numero di nodi nel cluster, il backup dell'interfaccia utente e la raggiungibilità di tutti i servizi possono richiedere più tempo.
- È possibile monitorare l'attività in Elenco attività disponibile nell'angolo superiore destro dell'interfaccia utente di vManage.
- Nell'interfaccia utente di vManage di ogni nodo aggiunto al cluster, è necessario visualizzare tutti i router, i modelli e i criteri, se disponibili in vManage-1.
- Se tali configurazioni non erano presenti in vManage-1, le configurazioni vBonds e vSmarts aggiunte a vManage-1 e anche Amministrazione > Impostazioni per Nome organizzazione, vBond, Autorizzazione certificato devono essere riflesse sul resto dei nodi vManage aggiunti al cluster.
- Ripetere gli stessi passaggi per gli altri nodi vManage.

Una volta caricati tutti i controller, attenersi a questa procedura:

Passaggio 4: Backup/ripristino di Config-db

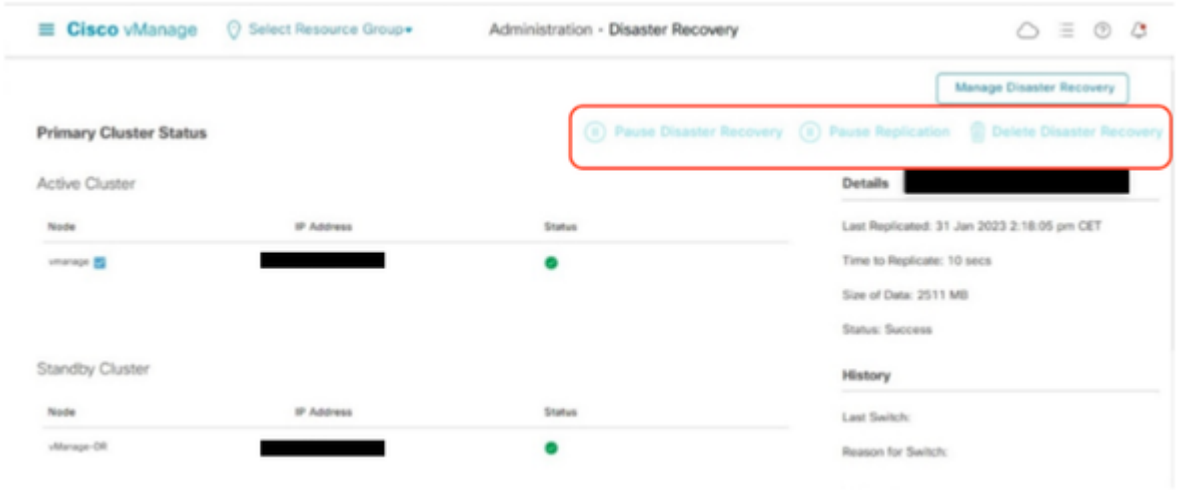
Raccolta del backup e del ripristino vManage configuration-db in un altro nodo vManage

---

Nota: Durante la raccolta del backup del database di configurazione dal cluster vManage esistente in cui è abilitato il ripristino di emergenza, assicurarsi che venga raccolto dopo che il ripristino di emergenza in tale nodo è stato sospeso ed eliminato.

Confermare che non è in corso la replica per il disaster recovery. Selezionare Amministrazione > Disaster Recovery e verificare che lo stato sia Operazione riuscita e non in uno stato transitorio, ad esempio Importazione in sospeso, Esportazione in sospeso o Download in sospeso. Se lo stato non ha esito positivo, contattare Cisco TAC e verificare la corretta replica prima di sospendere il ripristino di emergenza.

Sospendere innanzitutto il ripristino di emergenza e assicurarsi che l'attività sia completata. Eliminare quindi il ripristino di emergenza e verificare che l'attività sia stata completata.



Contattare Cisco TAC per garantire la corretta pulizia del dispositivo di ripristino di emergenza.

Raccolta backup del database di configurazione:

- Nell'infrastruttura SD-WAN attualmente in uso, è possibile generare il backup del database di configurazione dal cluster vManage.
- Si noti che è necessario generare il backup del database di configurazione solo su un nodo del cluster vManage che è il leader del database di configurazione.

- Per vManage standalone, vManage è il leader del database di configurazione.
- In cluster vManage, identificare il nodo della linea guida configuration-db utilizzando il comando request nms configuration-db diagnostics.È possibile eseguire questo comando su tutti i nodi del cluster vManage a 3 nodi.
- In un cluster a 6 nodi, assicurarsi di eseguire questo comando sui nodi vManage in cui configuration-db è abilitato per identificare il nodo principale. Passare a Amministrazione > Gestione cluster per verificare quanto segue:
- Come si può vedere nello screenshot, sui nodi configurati con la persona COMPUTE_AND_DATA è in esecuzione configuration-db.

È possibile verificare la stessa condizione utilizzando il comando requestnmsconfiguration-dbstatus in vManageCLI. L'output è il seguente

```
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#
```

- Una volta eseguito il comandorequest nms configuration-db diagnostics su questi nodi, l'output è il seguente:
- Cercare il campo evidenziato per "IsLeader". Se è impostato su 1, indica che il nodo è il

nodo della linea guida e da esso è possibile raccogliere il backup del database di configurazione.

```
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     .
```

Utilizzare questo comando per raccogliere il backup del database di configurazione dal nodo vManage leader del database di configurazione identificato.

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

L'output previsto è il seguente:

```
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#
```

- Prendere nota delle credenziali di configuration-db se sono state aggiornate.
- Se non si è a conoscenza delle credenziali del database di configurazione, contattare TAC per recuperare le credenziali del database di configurazione dai nodi vManage esistenti.
- Le credenziali di configuration-db predefinite sono nome utente: neo4j e password: password

Ripristinare il backup di Configuration-db in un altro nodo vManage

Copiare il backup del database di configurazione nella directory /home/admin/ di vManage utilizzando SCP.

Output di esempio del comando scp:

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

```
viptela 20.15.4.1

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

Per ripristinare il backup del database di configurazione, è necessario innanzitutto configurare le credenziali del database di configurazione. Se le credenziali del database di configurazione sono predefinite (neo4j/password), è possibile ignorare questo passaggio.

Per configurare le credenziali configuration-db, utilizzare il comando request nms configuration-db update-admin-user.Utilizzare il nome utente e la password desiderati.

Notare che il server applicazioni di vManage è stato riavviato. A causa della quale l'interfaccia utente di vManage diventa inaccessibile per un breve periodo.

```
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 in cui è possibile procedere al ripristino del backup del database di configurazione:

È possibile utilizzare il comando request nms configuration-db restore path /home/admin/< > per ripristinare configuration-db nel nuovo 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
```

Una volta ripristinato il database di configurazione, verificare che l'interfaccia utente di vManage sia accessibile. Attendere circa 5 minuti e quindi tentare di accedere all'interfaccia utente.

Dopo aver eseguito correttamente il login all'interfaccia utente, verificare che l'elenco dei router perimetrali, il modello, i criteri e tutte le altre configurazioni presenti nell'interfaccia utente vManage precedente o esistente siano riflessi nella nuova interfaccia utente vManage.

Passaggio 5: Riautenticazione dei controller e annullamento della convalida dei controller precedenti

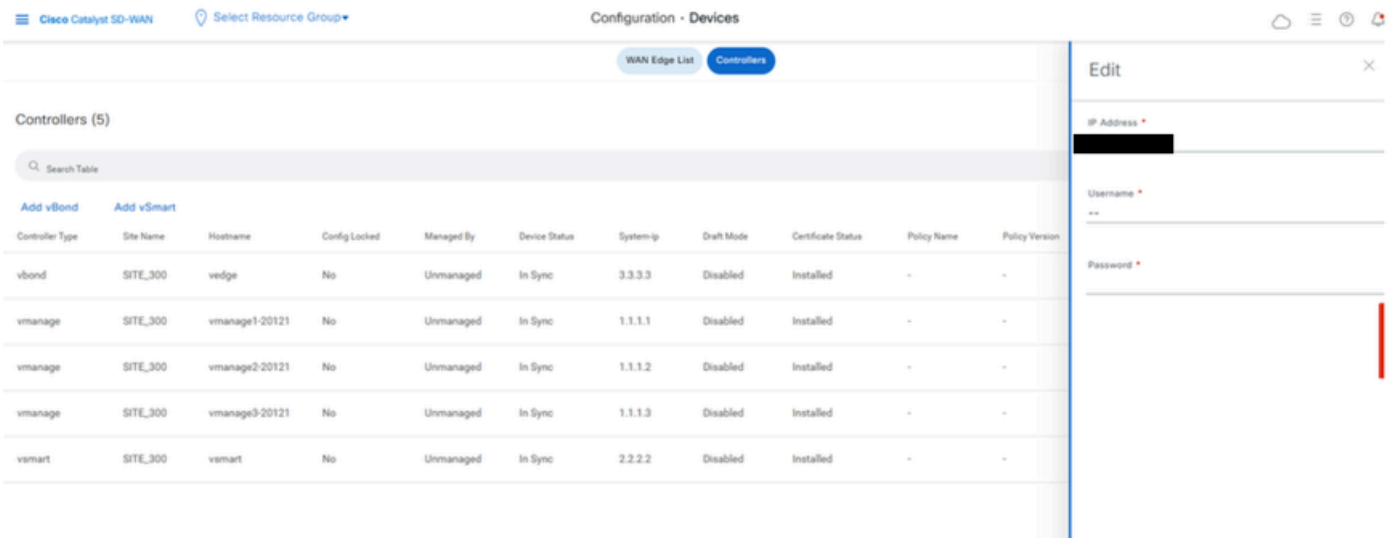
Una volta ripristinato il database di configurazione, è necessario riautenticare tutti i nuovi controller (manage/vsmart/vbond) nel fabric

---

Nota: nella produzione effettiva, se l'IP dell'interfaccia utilizzato per la riautenticazione è l'IP dell'interfaccia del tunnel, è necessario garantire che il servizio NETCONF sia consentito sull'interfaccia del tunnel di vManage, vSmart e vBond e anche sui firewall lungo il percorso. La porta firewall da aprire è la porta TCP 830 come regola bidirezionale dal cluster DR a tutti i vBonds e vSmarts.

Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller

- Fare clic sui tre punti accanto a ciascun controller e scegliere Modifica



- Sostituire l'indirizzo ip (ip di sistema del controller) con l'indirizzo ip vpn 0 (interfaccia tunnel) del trasporto. Immettere il nome utente e la password e fare clic su Salva

- Eseguire la stessa operazione per tutti i nuovi controller nel fabric

Sincronizza la catena di certificati radice

Una volta caricati tutti i controller, attenersi a questa procedura:

Su qualsiasi server Cisco SD-WAN Manager nel cluster appena attivo, eseguire le seguenti azioni:

Immettere questo comando per sincronizzare il certificato radice con tutti i dispositivi Cisco Catalyst SD-WAN nel cluster appena attivo:

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

Immettere questo comando per sincronizzare l'UUID di Cisco SD-WAN Manager con Cisco SD-WAN Validator:

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

Una volta ripristinata la struttura e attivate le sessioni bfd e di controllo per tutti i bordi e i controller della struttura, è necessario invalidare i vecchi controller (vmanage/vsmart/vbond) dall'interfaccia utente

- Su vmanage UI, fare clic su Configurazione > Dispositivi > Certificati
- Fare clic su Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su invalida
- Fare clic su Invia a vbond
- Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su Elimina.

Passaggio 6: Registra assegni

Nota: Continuare con la sezione Controlli successivi mostrata qui, che è comune a tutte le combinazioni di distribuzione.

Combinazione 4: vManage Cluster + DR standby manuale/a freddo

Cos'è il ripristino di emergenza in standby manuale/a freddo? Il server di backup SD-WAN Manager o il cluster SD-WAN Manager viene mantenuto in stato di standby a freddo.

Vengono eseguiti backup regolari del database attivo e se il cluster primario SD-WAN Manager o SD-WAN Manager non funziona, il cluster in standby SD-WAN Manager o SD-WAN Manager viene attivato manualmente e il database di backup viene ripristinato.

Istanze necessarie:

- 3 o 6 vManage (cluster primario)
- 3 o 6 vManage (cluster DR in standby)
- 1 o più vBond (distribuiti tra data center principali e DR)
- 1 o più vSmart (distribuiti tra data center principali e di disaster recovery)

Passaggi:

1. Visualizzare tutte le istanze utilizzando l'opzione Passi comuni (Common Steps)
2. Controlli preliminari
3. Configurazione di interfaccia utente, certificati e controller integrati vManage
4. Crea cluster vManage
5. Installazione cluster DR in standby a freddo
6. Backup/ripristino di Config-db
7. Registra assegni

Passaggio 1: Controlli preliminari

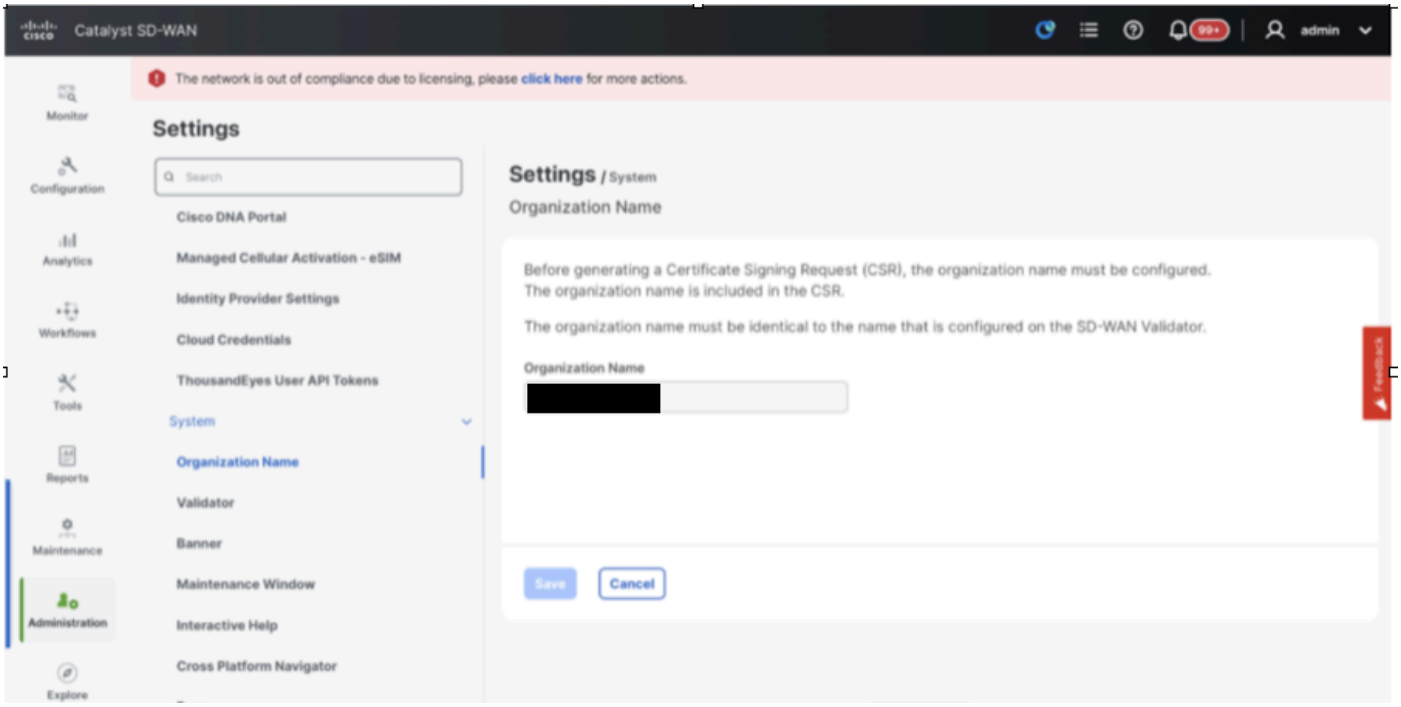
- Verificare che il numero delle istanze attive di Cisco SD-WAN Manager sia identico al numero delle nuove istanze di Cisco SD-WAN Manager.
- Accertarsi che tutte le istanze Cisco SD-WAN Manager attive e nuove eseguano la stessa versione del software.
- Verificare che tutte le istanze Cisco SD-WAN Manager nuove e attive siano in grado di raggiungere l'indirizzo IP di gestione di Cisco SD-WAN Validator.
- Verificare che i certificati siano stati installati nelle istanze di Cisco SD-WAN Manager appena installate.
- Verificare che gli orologi di tutti i dispositivi Cisco Catalyst SD-WAN, incluse le nuove istanze di Cisco SD-WAN Manager installate, siano sincronizzati.
- Verificare che nelle istanze di Cisco SD-WAN Manager appena installate sia configurato un nuovo set di IP di sistema e ID di sito, insieme alla stessa configurazione di base del cluster attivo.

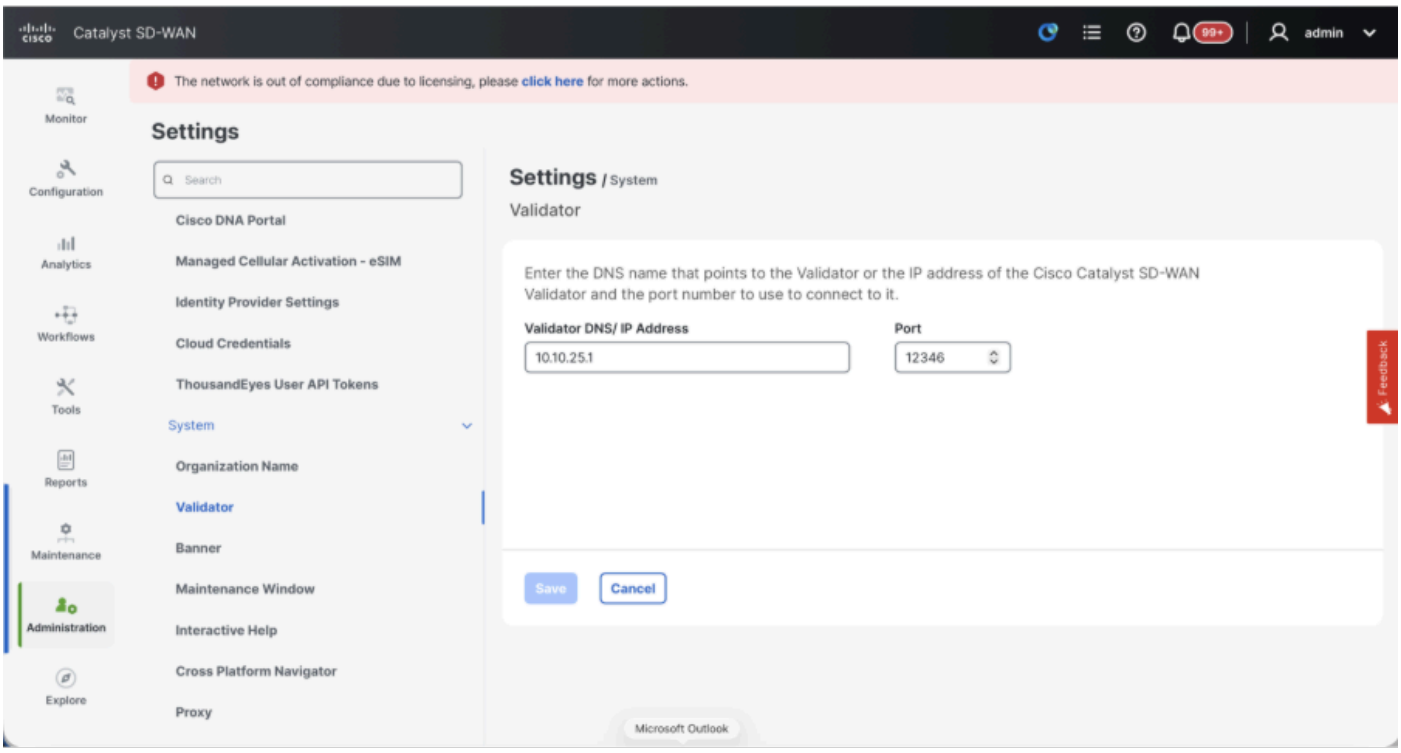
Passaggio 2: Configurazione di interfaccia utente, certificati e controller integrati vManage

Aggiornare le configurazioni nell'interfaccia utente di vManage

- Una volta aggiunte le configurazioni al passo 1 nella CLI di tutti i controller, possiamo accedere alla webUI di vManage, usando l'URL https://<vmanage-ip> nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi nodi vManage. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Amministrazione > Impostazioni e completare i seguenti passaggi.

- Configurare il nome dell'organizzazione e l'URL/indirizzo IP di Validator/vBond. Configurare lo stesso valore presente nella CLI del nodo vManage.
- In vManage 20.15/20.18 queste configurazioni sono disponibili nella sezione Sistema.



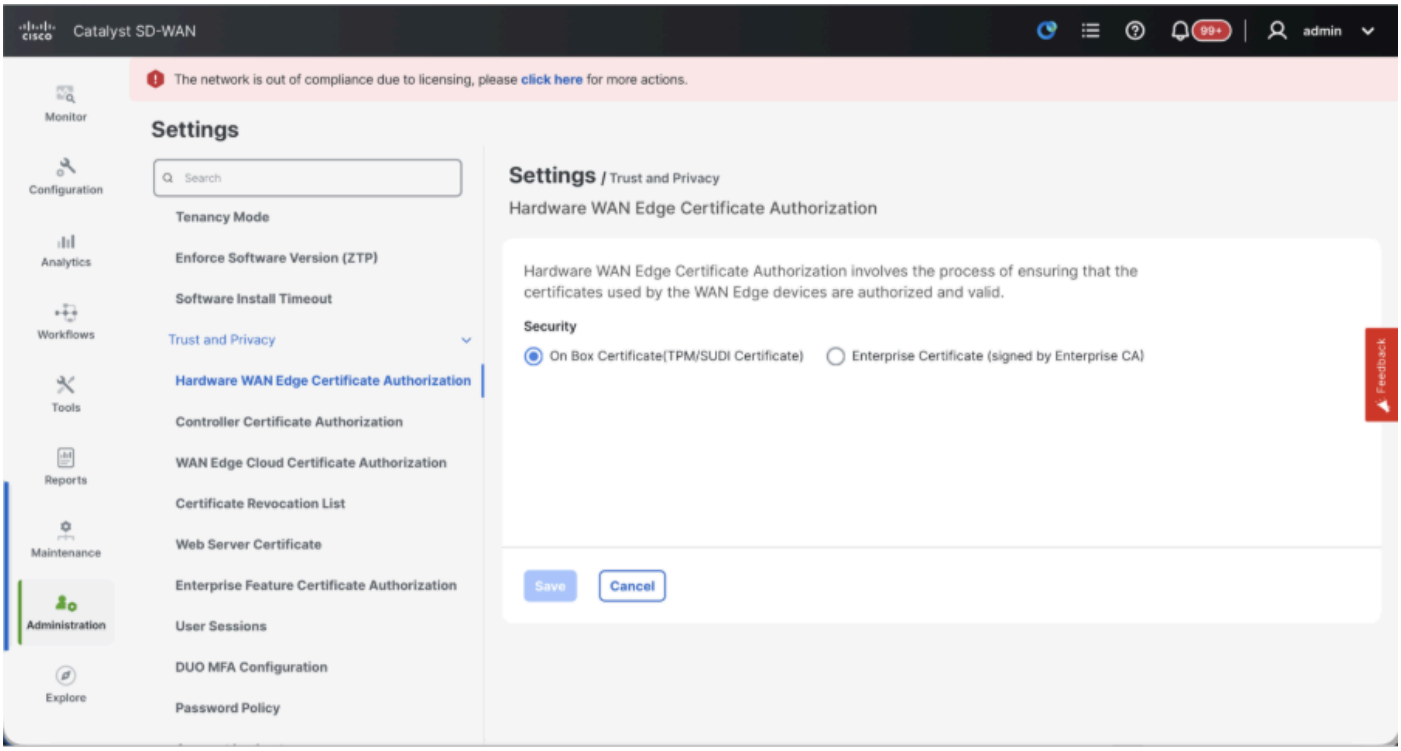


- Verificare le configurazioni per l'Autorità di certificazione (CA), che decide l'Autorità di certificazione utilizzata per firmare i certificati. Sono disponibili 3 opzioni:

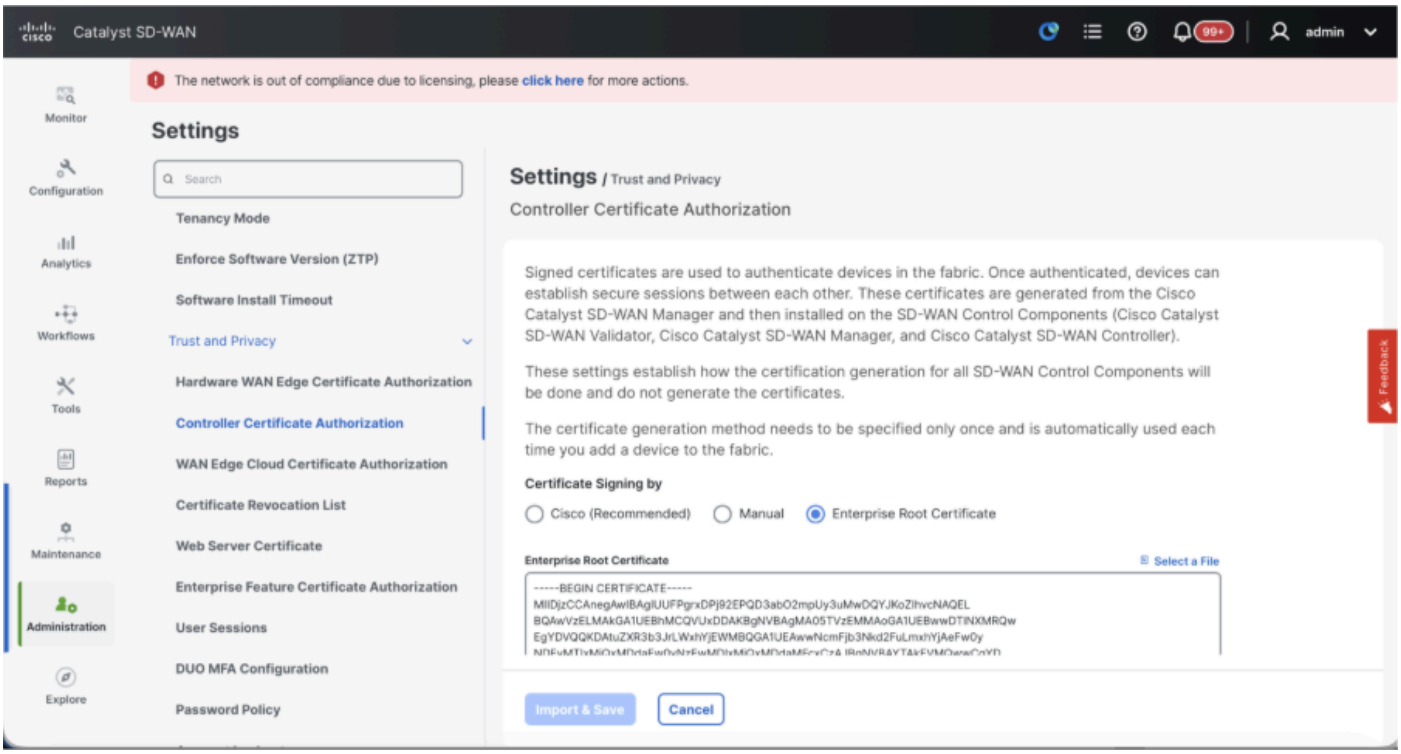
1. Autorizzazione certificato perimetro WAN hardware - Decide la CA per i router perimetrali SD-WAN hardware.
    - Certificato On-Box (certificato TPM/SUDI): con questa opzione, il certificato preinstallato sull'hardware del router viene utilizzato per stabilire le connessioni di

controllo (connessioni TLS/DTLS)

- Certificato organizzazione (firmato dall'autorità di certificazione dell'organizzazione): questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

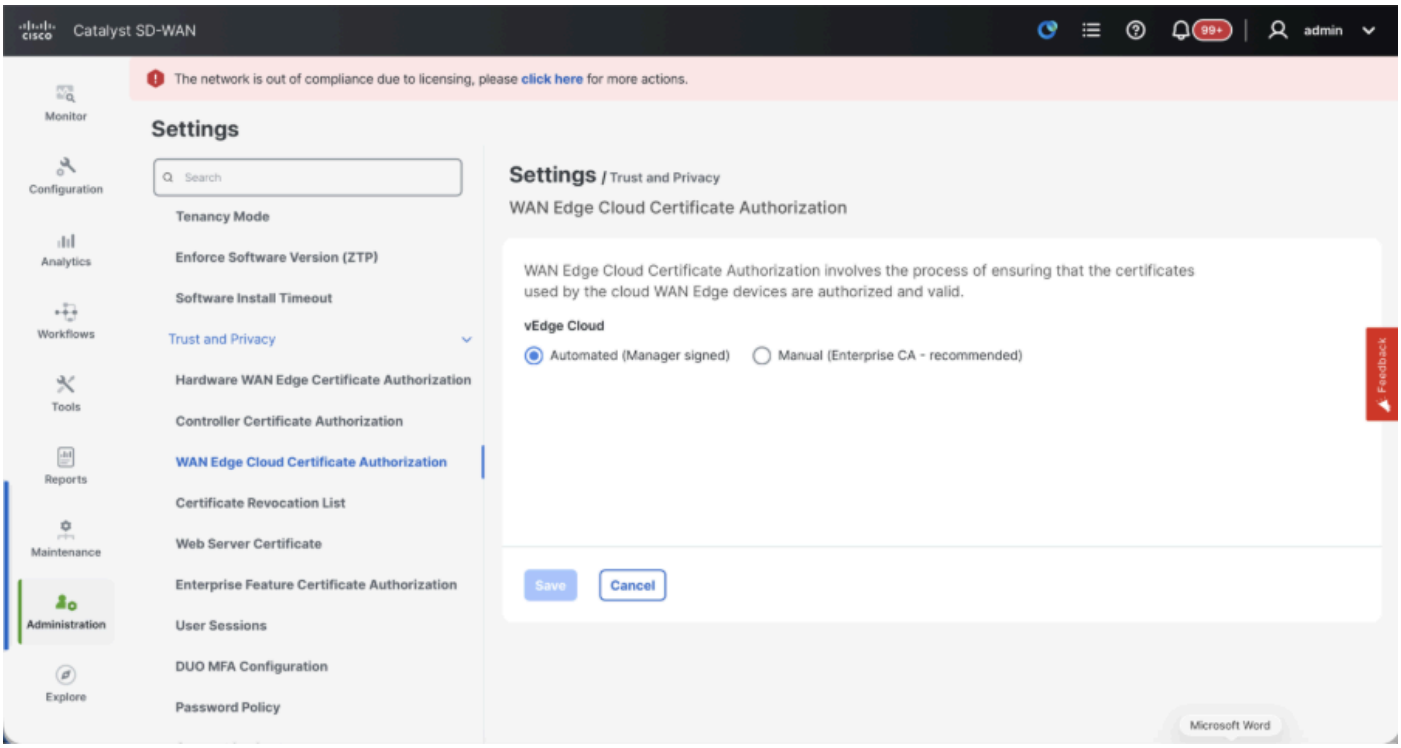


2. Controller Certificate Authorization - Decide la CA per i controller SD-WAN.
    - Cisco (scelta consigliata) - I controller utilizzano i certificati firmati da Cisco PKI. vManage contatta automaticamente il portale PNP utilizzando le credenziali dello smart account configurate in vManage e ottiene la firma del certificato che viene installato nel controller.
    - Manuale: i controller utilizzano i certificati firmati da Cisco PKI. Firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
    - Certificato radice dell'organizzazione: questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

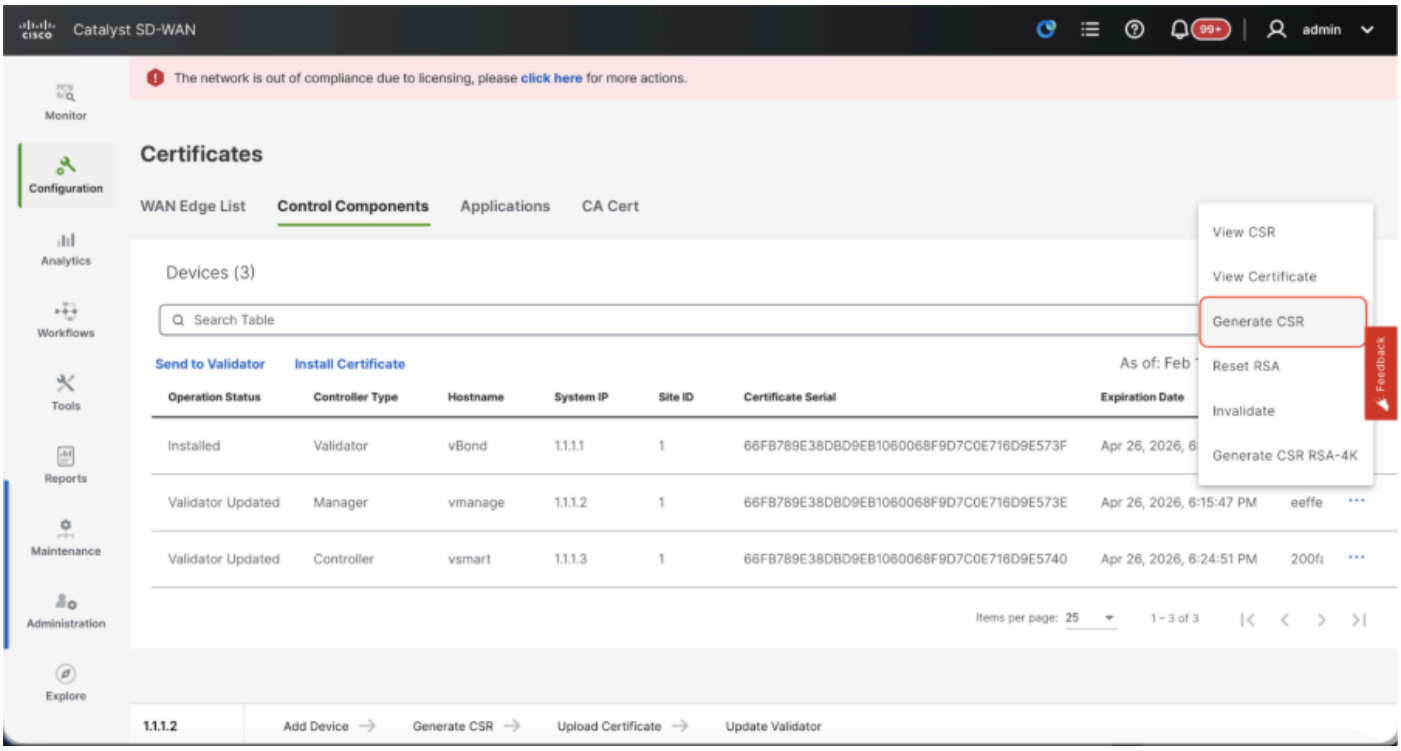


3. Autorizzazione certificato cloud perimetrale WAN - Decide la CA per i router perimetrali SD-WAN virtuali (CSR1000v, C8000v, vEdge cloud)
    - Automatizzato (vManage firmato): vManage firma automaticamente il CSR per i router perimetrali virtuali e installa il certificato sul router.
    - Manuale (Autorità di certificazione dell'organizzazione - consigliata) - I router virtuali utilizzano certificati firmati dall'Autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

Nel caso in cui si utilizzi la propria CA, Autorità di certificazione dell'organizzazione (enterprise), scegliere Enterprise.



- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller
- Fare clic su ... per Manager/vManage e fare clic su Generate CSR (Genera CSR).



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco

passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.

Caricamento di vBond/Validator e vSmart/Controller in vManage

Passare a Configurazione > Dispositivi > Controllo componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

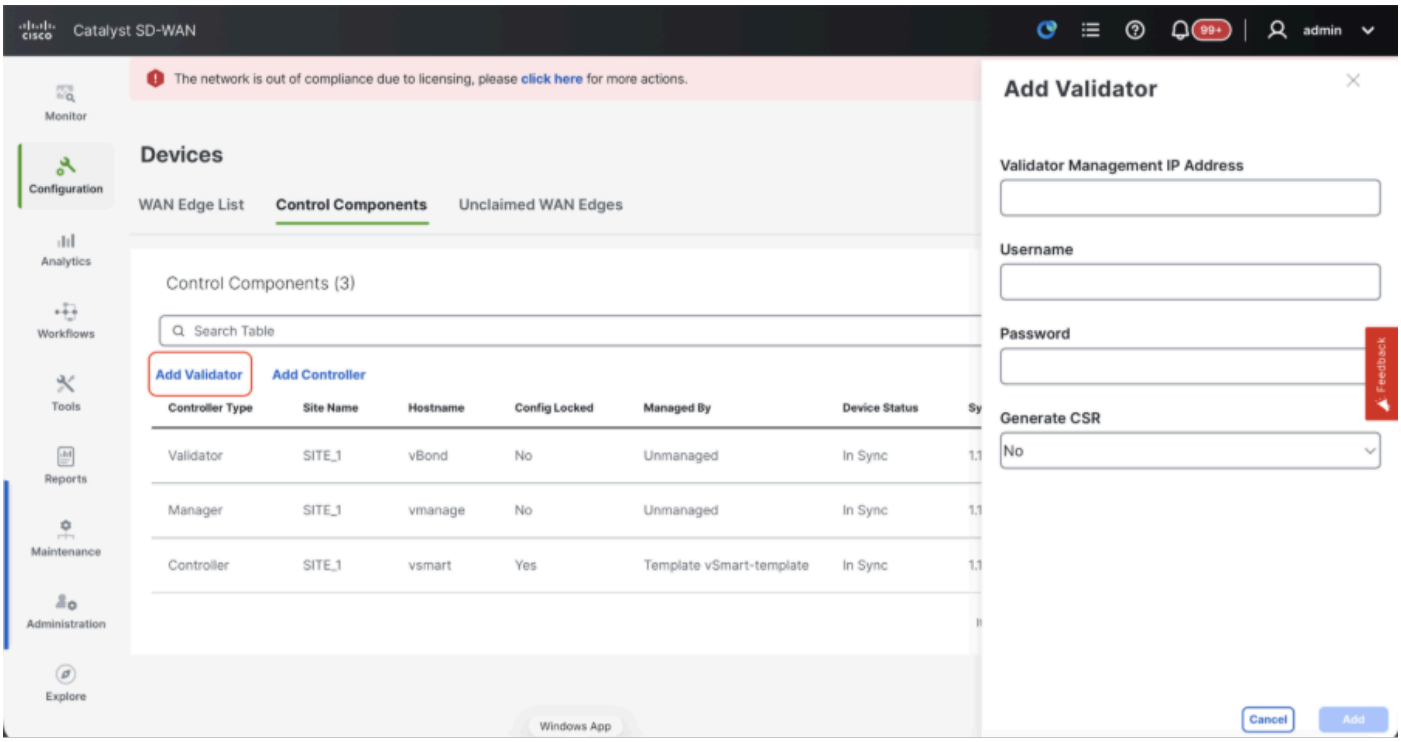
vBond/Convalida onboarding

- Fare clic su AddvBondnel caso di 20.12vManagerAggiungi validatornel caso di 20.15/20.18vManage. Viene visualizzato un popup, immettere il IP di trasporto VPN 0 di vBondraggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping se consentito dalla CLI di vManagetovBondIP.
- Immettere le credenziali utente di vBond.

Nota: è necessario utilizzare le credenziali di amministratore di vBondor una parte utente di netadmingroup. È possibile verificare questa condizione nella CLI di vBond. Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vBond

---

Nota: Se vBond è dietro un dispositivo/firewall NAT, verificare se l'IP dell'interfaccia VPN 0 di vBond è convertito in un IP pubblico. Se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, in questo passaggio utilizzare l'indirizzo IP pubblico dell'interfaccia VPN 0



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vBond.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vBonds, ripetere gli stessi passaggi.

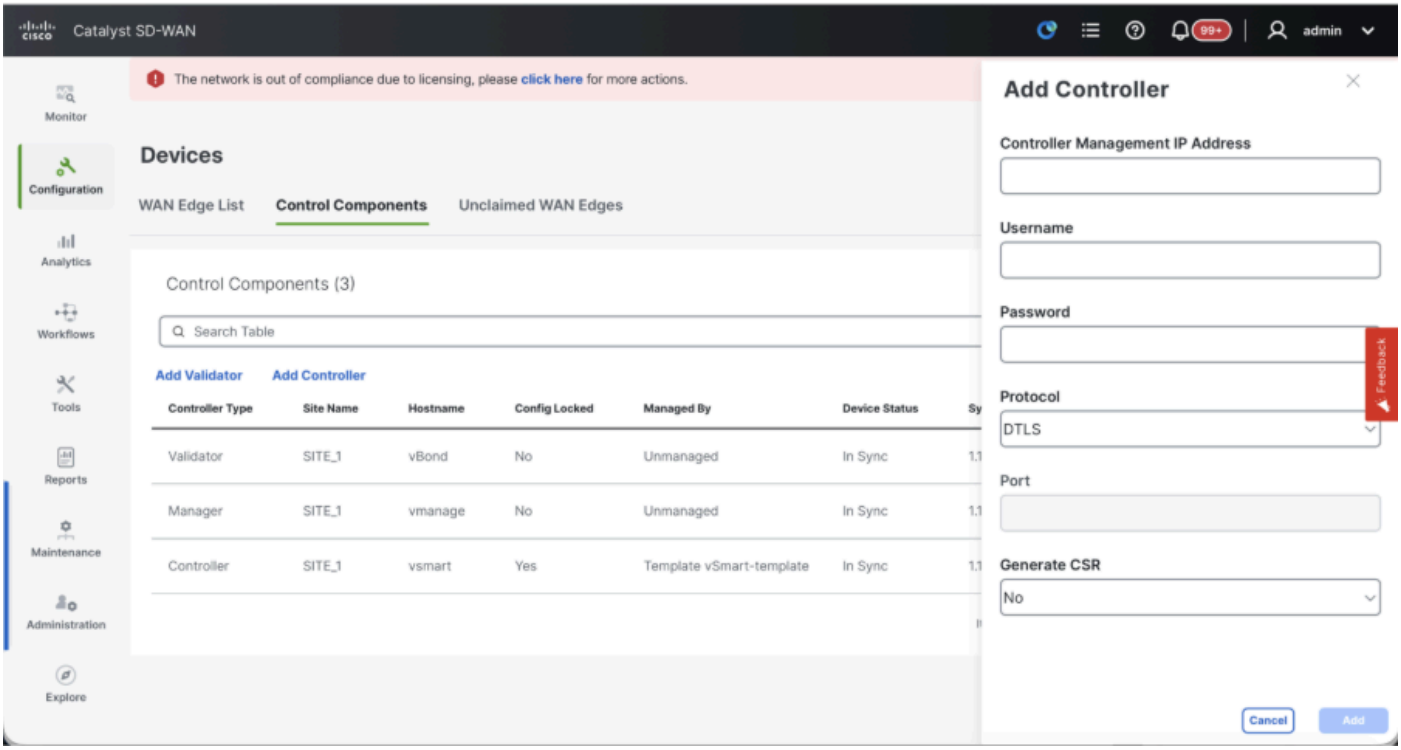
vSmart/Controller integrato:

- Fare clic su Add vSmart in caso di vManage 20.12 o Add Controller in caso di vManage 20.15/20.18.
- Viene visualizzato un popup. Immettere l'IP di trasporto VPN 0 di vSmart raggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping, se consentito dalla CLI di vManage a vSmart IP.
- Immettere le credenziali utente di vSmart Note che è necessario utilizzare le credenziali di amministratore di vSmart o di un utente appartenente al gruppo netadmin.
- È possibile verificare questa condizione nella CLI di vSmart.
- Impostare il protocollo su TLS se si intende utilizzare TLS per i router per stabilire

connessioni di controllo con vSmart. Questa configurazione deve essere configurata anche sulla CLI dei nodi vSmarts e vManage.

- Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vSmart.

Nota: se vSmart è dietro un dispositivo/firewall NAT, verificare se l'indirizzo IP dell'interfaccia vSmart VPN 0 è convertito in un indirizzo IP pubblico e se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, utilizzare l'indirizzo IP pubblico dell'indirizzo IP dell'interfaccia VPN 0 in questo passaggio.

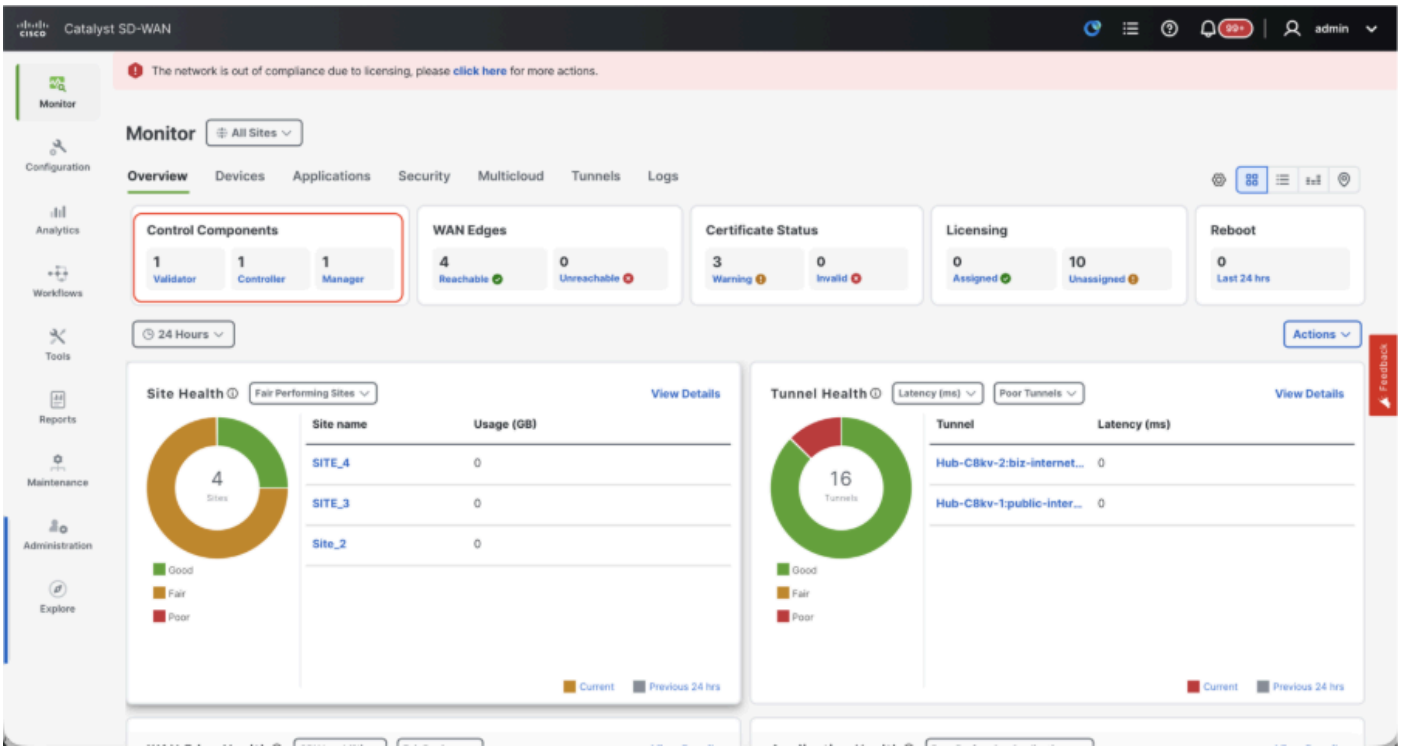


- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vSmart.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vSmarts, ripetere gli stessi passaggi.

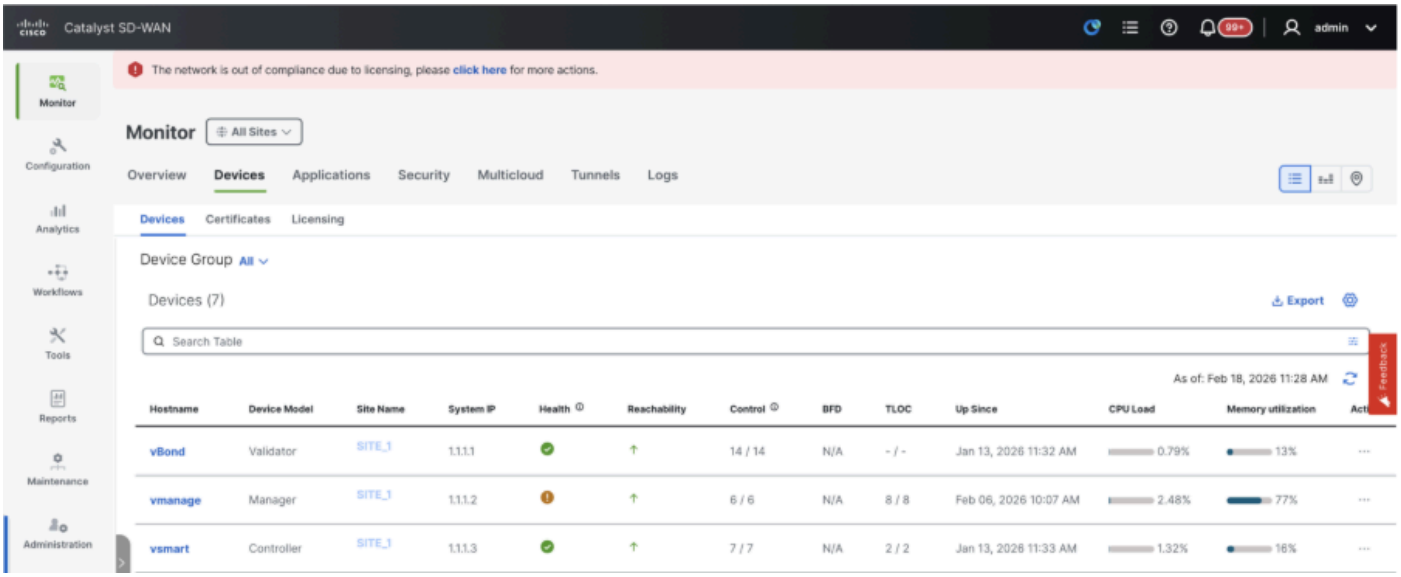
Verifica

Una volta completati tutti i passaggi, verificare che tutti i componenti di controllo siano raggiungibili

in Monitor>Dashboard



- Fate clic sui rispettivi componenti di controllo e verificate che siano tutti raggiungibili.
- Passare a Monitor > Dispositivi e verificare che tutti i componenti di controllo siano raggiungibili.



Passaggio 3: Crea cluster vManage

Fabric SD-WAN integrato con un cluster vManage nella sovrapposizione SD-WAN

Nota: il cluster vManage può essere configurato con 3 nodi vManage o 6 nodi vManage a seconda del numero di siti collegati all'infrastruttura SD-WAN

Integrazione di tutti i controller SD-WAN con un unico nodo vManage

Procedere con i passaggi condivisi in "Controller SD-WAN integrati con un singolo nodo vManage nella sovrapposizione SD-WAN" per avviare prima il fabric SD-WAN con un nodo vManage e incorporare tutti i validatori (vBond) e i controller (vSmart) richiesti.

Configurare le configurazioni CLI di tutti i nodi vManage appartenenti al cluster

- Configurare gli altri nodi vManage. In caso di cluster a 3 nodi, sono disponibili 2 nodi da configurare, in caso di cluster a 6 nodi sono disponibili 5 nodi da configurare.
- Configurare le configurazioni di sistema come mostrato:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Nota: se si utilizza URL come indirizzo vBond, verificare di configurare gli indirizzi IP dei server DNS nella configurazione VPN 0 o di risolverli.

Queste configurazioni sono necessarie per abilitare l'interfaccia di trasporto utilizzata per stabilire le connessioni di controllo con i router e gli altri controller.

```
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
```

Configurare inoltre l'interfaccia di gestione VPN 512 per consentire l'accesso di gestione fuori

banda al controller.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Configurazione facoltativa:

- È possibile fare riferimento alle configurazioni del controller esistente e, se la configurazione indicata è presente, è possibile aggiungerla ai nuovi controller.
- Configurare il protocollo di controllo come TLS solo se i router devono stabilire connessioni di controllo protette con i nodi vManage che utilizzano TLS. Per impostazione predefinita, tutti i controller e i router stabiliscono una connessione di controllo utilizzando il protocollo DTLS. Si tratta di una configurazione opzionale richiesta solo sui nodi vSmart e vManage a seconda delle esigenze.

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

Configura interfaccia di servizio in tutti i nodi vManage

Configurare l'interfaccia del servizio su tutti i vManagenodes, incluso vManage-1 che è già stato caricato. Questa interfaccia viene utilizzata per la comunicazione del cluster, ovvero la comunicazione tra i vManagenodes nel cluster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Verificare che per l'interfaccia di servizio in tutti i nodi del cluster vManagement venga utilizzata la stessa subnet IP.

Configura credenziali cluster

È possibile utilizzare le stesse credenziali di amministrazione dei nodi vManage per configurare il cluster vManage. In caso contrario, è possibile configurare una nuova credenziale utente che faccia parte di netadmingroup. Le configurazioni per la configurazione delle nuove credenziali utente sono le seguenti

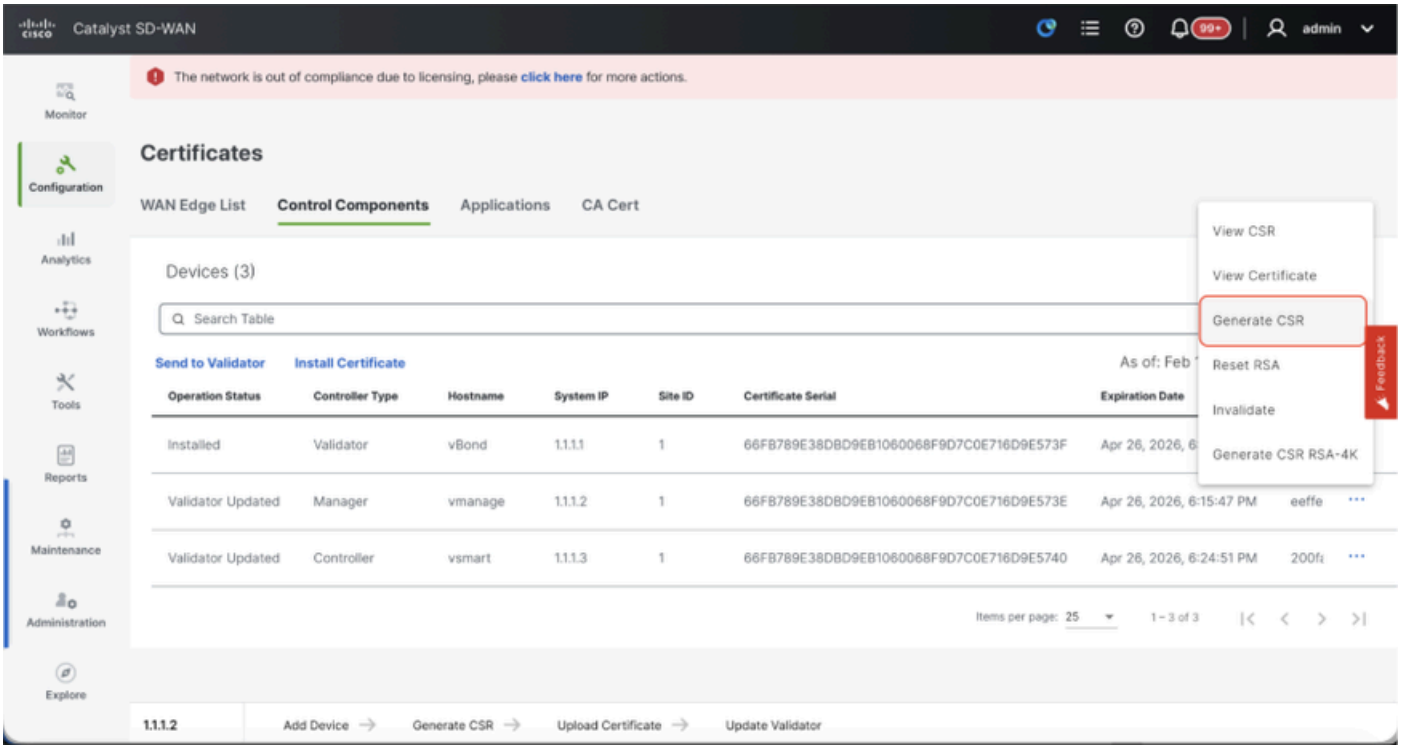
```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

Assicurarsi di configurare le stesse credenziali utente in tutti gli vManagenodeche fanno parte del cluster.Se si decide di utilizzare le credenziali di amministratore, è necessario che siano lo stesso nome utente/password in tutti gli vManagenodes.

Installa certificato dispositivo in tutti i nodi vManage

- Accedere a vManageUI di tutti i vManagenodes utilizzando l'URL https://<vmanage-ip>nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi vManagenode. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

  Fare clic su ... per Manager/vManage e fare clic su Generate CSR.



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Completare questo passaggio in tutti i nodi vManage che fanno parte del cluster.

Preparare la creazione del cluster vManage

- Sul WebUI di vManage-1, selezionare Amministrazione > Gestione cluster, fare clic su ... in Azioni per vManage-1, scegliere Modifica.
- La persona del nodo viene scelta automaticamente in base alla persona scelta durante

lo spun up della VM.

Nota: Per un cluster a 3 nodi, tutti e 3 i nodi vManage vengono visualizzati con compute+data come persona.

- Per un cluster a 6 nodi, vengono visualizzati 3 nodi vManage con dati di tipo compute+data come utente e 3 nodi vManage come utente.
- Dall'elenco a discesa per l'indirizzo IP di Manager, assicurarsi di scegliere l'indirizzo IP dell'interfaccia di servizio di vManage.
- Immettere il nome utente e la password che si desidera utilizzare per abilitare il cluster vManage, definito credenziali del cluster.
- Come accennato in precedenza, è necessario configurare le stesse credenziali su tutti i nodi vManage e utilizzarle durante l'aggiunta di tutti i nodi al cluster.

Configurazione facoltativa:

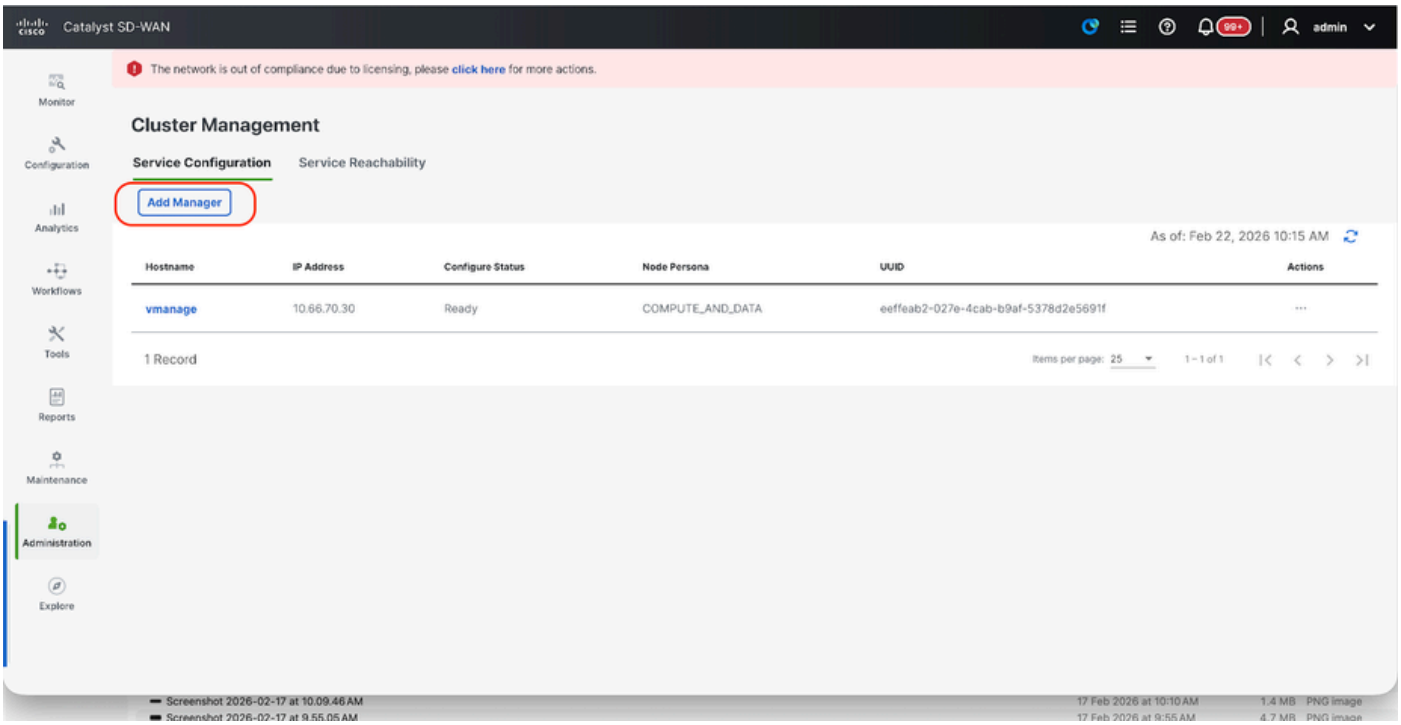
Fare riferimento a questa configurazione nel cluster esistente per Abilitare SDAVC: deve essere verificata solo se è necessaria ed è necessaria solo su un nodo vManage del cluster.

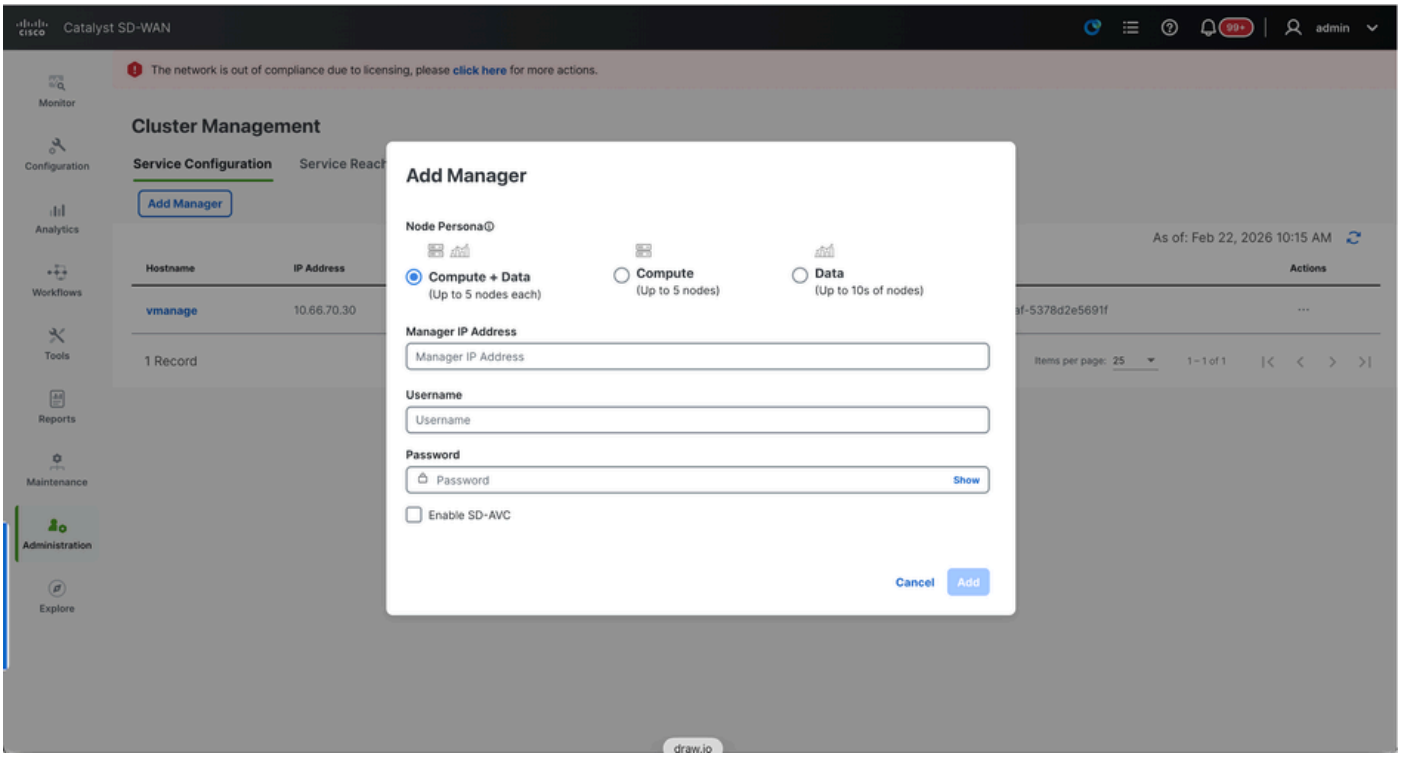
Fare clic su Aggiorna.

- In seguito, i servizi vManage NMS vengono riavviati in background e l'interfaccia utente non è disponibile per alcuni minuti, dai 5 ai 10 minuti circa. Durante questo periodo, l'accesso CLI di vManage è disponibile.
- Una volta che l'interfaccia utente di vManage-1 è accessibile, passare a Amministrazione > Gestione cluster, verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP,Lo stato della configurazione è Pronto e la persona del nodo viene riflessa correttamente. Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili.
- Se si rileva che uno dei servizi non è ancora raggiungibile, attendere. Di solito ci vogliono dai 20 ai 30 minuti.

Crea il cluster vManage

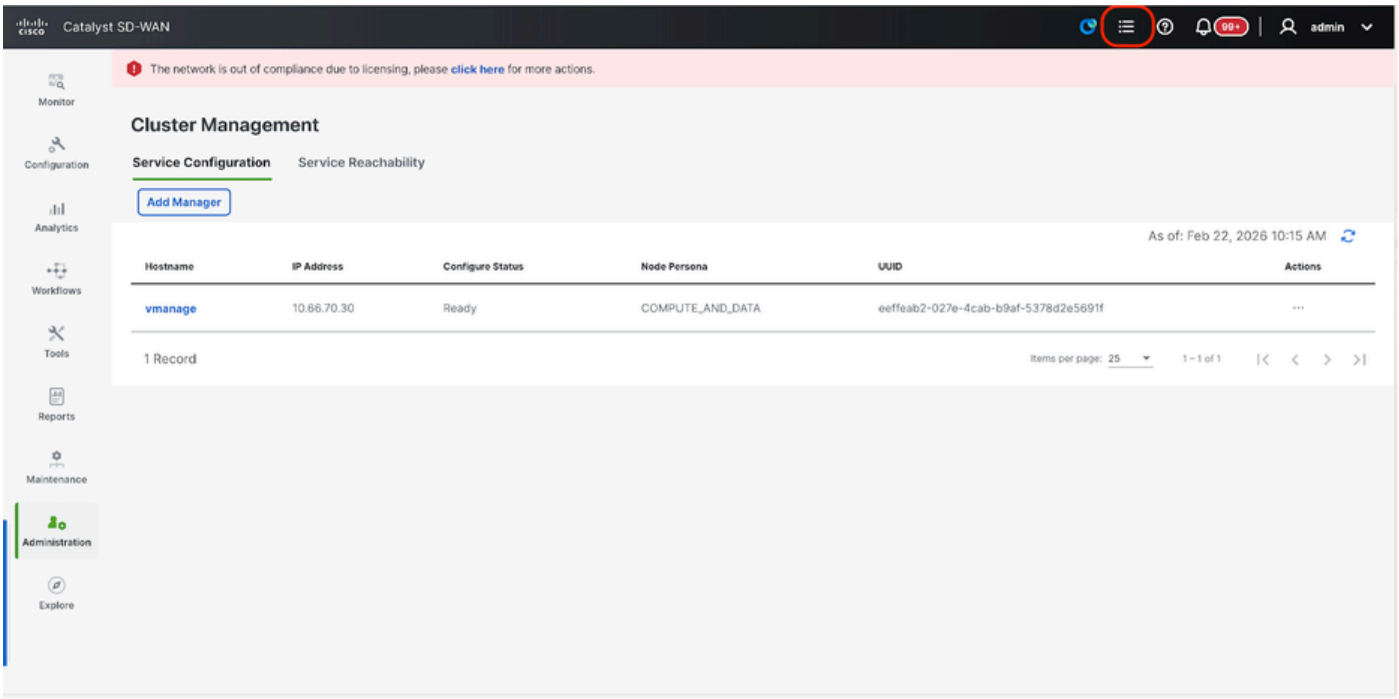
- Sul WebUI di vManage-1, selezionare Amministrazione > Gestione cluster, nella sezione Configurazione servizio,
- Fare clic su Add Manager, viene visualizzata una finestra popup:





- Scegliere la persona Nodo in base alle configurazioni della persona eseguite durante l'esecuzione dello spun-up del nodo vManage - 2.
- Immettere l'indirizzo IP dell'interfaccia di servizio di vManage-2 in Indirizzo IP manager
- Immettere il nome utente e la password, ovvero le stesse credenziali utilizzate nel passaggio 6.
- Abilita SDAVC - Da lasciare deselezionato come avremmo già abilitato su vManage-1
- Fare clic su Aggiungi.
- In seguito, i servizi vManage NMS vengono riavviati in background per i nodi vManage 1 e 2. L'interfaccia utente non è disponibile per alcuni minuti, dai 5 ai 10 minuti circa, per vManage 1 e 2.

- Durante questo periodo, è disponibile l'accesso CLI di vManage 1 e 2.
- Una volta che l'interfaccia utente di vManage-1 è accessibile, passare a Amministrazione > Gestione cluster, verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP, Configura stato sia Pronto e che la persona del nodo sia indicata correttamente.
- Passare alla sezione Raggiungibilità servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili per entrambi i nodi vManage.
- Se si rileva che uno dei servizi non è ancora raggiungibile, attendere. Di solito ci vogliono dai 5 ai 10 minuti.
- È possibile controllare lo stato del processo di aggiunta cluster nell'elenco Attività disponibile nell'angolo superiore destro dell'interfaccia utente di vManage.



- È possibile cercare Elenco attività attivo e se l'attività è ancora elencata in Elenco attività attivo, indica che l'attività non è stata ancora completata.
- È possibile fare clic sull'attività per verificarne lo stato di avanzamento. Se l'attività non è elencata in Elenco attività attivo, passare a Completato e assicurarsi che l'attività sia stata completata correttamente.
- Solo dopo la convalida di questi punti, procedere al passaggio successivo.

Prima di aggiungere il nodo successivo al cluster, è necessario prendere in considerazione i seguenti punti:

Verificare questi punti in tutte le interfacce utente dei nodi vManage aggiunti al cluster:

- Passare a Monitoraggio > Panoramica dell'interfaccia utente di vManage e verificare che il numero di nodi vManage sia indicato correttamente e che sia raggiungibile a seconda del numero di nodi aggiunti al cluster.

- Passare a Amministrazione > Gestione cluster e verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP, che Configura stato sia Pronto e che la

persona del nodo sia indicata correttamente.
- Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili per entrambi i nodi vManage.

- Ogni volta che un nodo viene aggiunto al cluster, i servizi NMS di tutti i nodi nel cluster vengono riavviati, pertanto l'interfaccia utente di tutti questi nodi diventa irraggiungibile per un certo periodo di tempo.
- A seconda del numero di nodi nel cluster, il backup dell'interfaccia utente e la raggiungibilità di tutti i servizi possono richiedere più tempo.
- È possibile monitorare l'attività in Elenco attività disponibile nell'angolo superiore destro dell'interfaccia utente di vManage.
- Nell'interfaccia utente di vManage di ogni nodo aggiunto al cluster, è necessario visualizzare tutti i router, i modelli e i criteri, se disponibili in vManage-1.
- Se tali configurazioni non erano presenti in vManage-1, le configurazioni vBonds e vSmarts aggiunte a vManage-1 e anche Amministrazione > Impostazioni per Nome organizzazione, vBond, Autorizzazione certificato devono essere riflesse sul resto dei nodi vManage aggiunti al cluster.
- Ripetere gli stessi passaggi per gli altri nodi vManage.

Passaggio 4: Installazione cluster DR in standby a freddo

Installazione cluster DR in standby a freddo

È possibile attivare un altro cluster vManage eseguendo la procedura descritta nel passo 4: Creare un cluster vManage. Post che completano i passaggi descritti nel Passaggio 6: Backup/Ripristino config-db per ripristinare il backup config-db nel cluster in standby.

Passaggio 5: Backup/ripristino di Config-db

Raccolta del backup e del ripristino vManage configuration-db in un altro nodo vManage

Raccolta backup del database di configurazione:

- Nell'infrastruttura SD-WAN attualmente in uso, è possibile generare il backup del database di configurazione dal cluster vManage.
- Si noti che è necessario generare il backup del database di configurazione solo su un nodo del cluster vManage che è il leader del database di configurazione.

- Per vManage standalone, vManage è il leader del database di configurazione.
- In cluster vManage, identificare il nodo della linea guida configuration-db utilizzando il comando request nms configuration-db diagnostics.È possibile eseguire questo comando su tutti i nodi del cluster vManage a 3 nodi.
- In un cluster a 6 nodi, assicurarsi di eseguire questo comando sui nodi vManage in cui configuration-db è abilitato per identificare il nodo principale. Passare a Amministrazione > Gestione cluster per verificare quanto segue:
- Come si può vedere nello screenshot, sui nodi configurati con la persona

COMPUTE_AND_DATA è in esecuzione configuration-db.

È possibile verificare la stessa condizione utilizzando il comando requestnmsconfiguration-dbstatus in vManageCLI. L'output è il seguente

```
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#
```

- Una volta eseguito il comandorequest nms configuration-db diagnostics su questi nodi, l'output è il seguente:
- Cercare il campo evidenziato per "IsLeader". Se è impostato su 1, indica che il nodo è il nodo della linea guida e da esso è possibile raccogliere il backup del database di configurazione.

```
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     .
```

Utilizzare questo comando per raccogliere il backup del database di configurazione dal nodo vManage leader del database di configurazione identificato.

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

L'output previsto è il seguente:

```
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#
```

- Prendere nota delle credenziali di configuration-db se sono state aggiornate.
- Se non si è a conoscenza delle credenziali del database di configurazione, contattare TAC per recuperare le credenziali del database di configurazione dai nodi vManage esistenti.
- Le credenziali di configuration-db predefinite sono nome utente: neo4j e password: password

Ripristinare il backup di Configuration-db in un altro nodo vManage

Copiare il backup del database di configurazione nella directory /home/admin/ di vManage utilizzando SCP.

Output di esempio del comando scp:

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

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

Per ripristinare il backup del database di configurazione, è necessario innanzitutto configurare le credenziali del database di configurazione. Se le credenziali del database di configurazione sono predefinite (neo4j/password), è possibile ignorare questo passaggio.

Per configurare le credenziali configuration-db, utilizzare il comando request nms configuration-db update-admin-user.Utilizzare il nome utente e la password desiderati.

Notare che il server applicazioni di vManage è stato riavviato. A causa della quale l'interfaccia utente di vManage diventa inaccessibile per un breve periodo.

```
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 in cui è possibile procedere al ripristino del backup del database di configurazione:

È possibile utilizzare il comando request nms configuration-db restore path /home/admin/< >

per ripristinare configuration-db nel nuovo 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
```

Una volta ripristinato il database di configurazione, verificare che l'interfaccia utente di vManage sia accessibile. Attendere circa 5 minuti e quindi tentare di accedere all'interfaccia utente.

Dopo aver eseguito correttamente il login all'interfaccia utente, verificare che l'elenco dei router perimetrali, il modello, i criteri e tutte le altre configurazioni presenti nell'interfaccia utente vManage precedente o esistente siano riflessi nella nuova interfaccia utente vManage.

Passaggio 6: Riautenticazione dei controller e annullamento della convalida dei controller precedenti

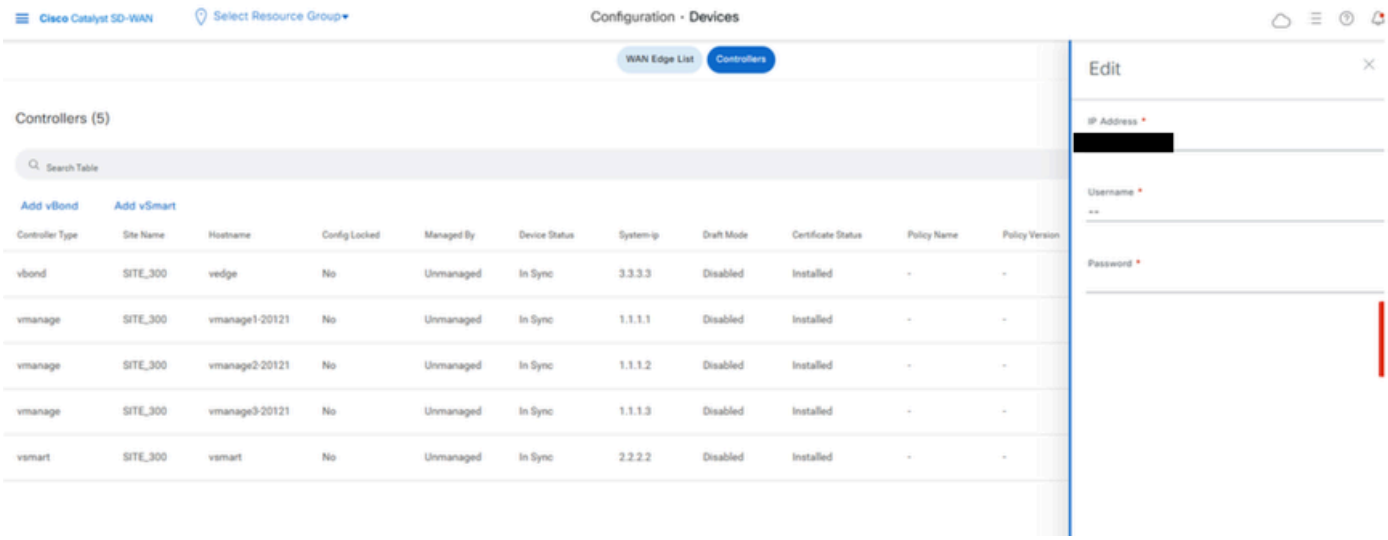
Una volta ripristinato il database di configurazione, è necessario riautenticare tutti i nuovi controller (manage/vsmart/vbond) nel fabric

---

Nota: nella produzione effettiva, se l'IP dell'interfaccia utilizzato per la riautenticazione è l'IP dell'interfaccia del tunnel, è necessario garantire che il servizio NETCONF sia consentito sull'interfaccia del tunnel di vManage, vSmart e vBond e anche sui firewall lungo il percorso. La porta firewall da aprire è la porta TCP 830 come regola bidirezionale dal cluster DR a tutti i vBonds e vSmarts.

Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller

- Fare clic sui tre punti accanto a ciascun controller e scegliere Modifica



- Sostituire l'indirizzo ip (ip di sistema del controller) con l'indirizzo ip vpn 0 (interfaccia tunnel) del trasporto. Immettere il nome utente e la password e fare clic su Salva
- Eseguire la stessa operazione per tutti i nuovi controller nel fabric

Sincronizza la catena di certificati radice

Una volta caricati tutti i controller, attenersi a questa procedura:

Su qualsiasi server Cisco SD-WAN Manager nel cluster appena attivo, eseguire le seguenti azioni:

Immettere questo comando per sincronizzare il certificato radice con tutti i dispositivi Cisco Catalyst SD-WAN nel cluster appena attivo:

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

Immettere questo comando per sincronizzare l'UUID di Cisco SD-WAN Manager con Cisco SD-WAN Validator:

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

Una volta ripristinata la struttura e attivate le sessioni bfd e di controllo per tutti i bordi e i controller della struttura, è necessario invalidare i vecchi controller (vmanage/vsmart/vbond) dall'interfaccia utente

- Su vmanage UI, fare clic su Configurazione > Dispositivi > Certificati
- Fare clic su Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su invalida
- Fare clic su Invia a vbond
- Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su Elimina

Passaggio 7: Registra assegni

Nota: Continuare con la sezione Controlli successivi mostrata qui, che è comune a tutte le combinazioni di distribuzione.

Combinazione 5: vManage Cluster + DR abilitato

Istanze necessarie:

- 3 o 6 vManage (cluster primario)
- 3 o 6 vManage (cluster DR in standby)
- 1 o più vBond (distribuiti tra data center principali e DR)
- 1 o più vSmart (distribuiti tra data center principali e di disaster recovery)

Passaggi:

1. Visualizzare tutte le istanze utilizzando l'opzione Passi comuni (Common Steps)
2. Controlli preliminari
3. Configurazione di interfaccia utente, certificati e controller integrati vManage
4. Crea cluster vManage
5. Installazione cluster DR in standby a freddo
6. Backup/ripristino di Config-db
7. Registra assegni

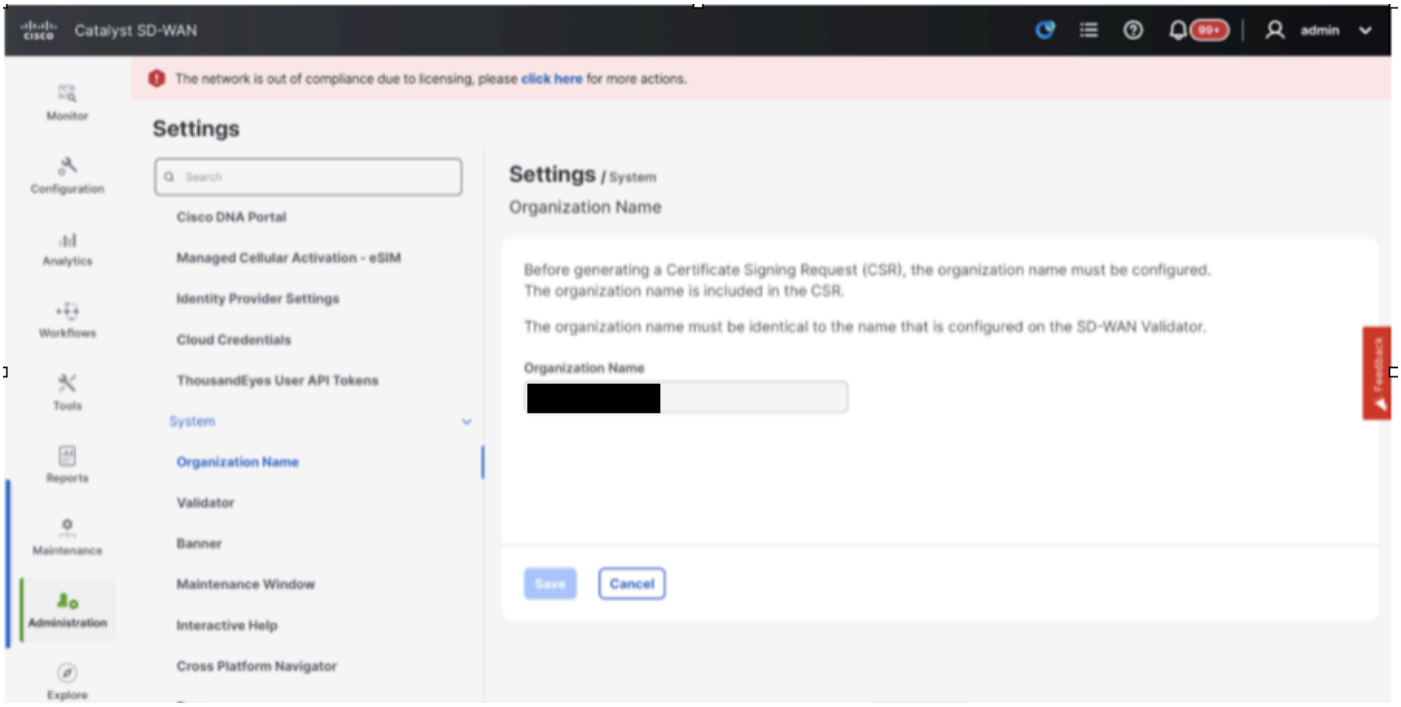
Passaggio 1: Controlli preliminari

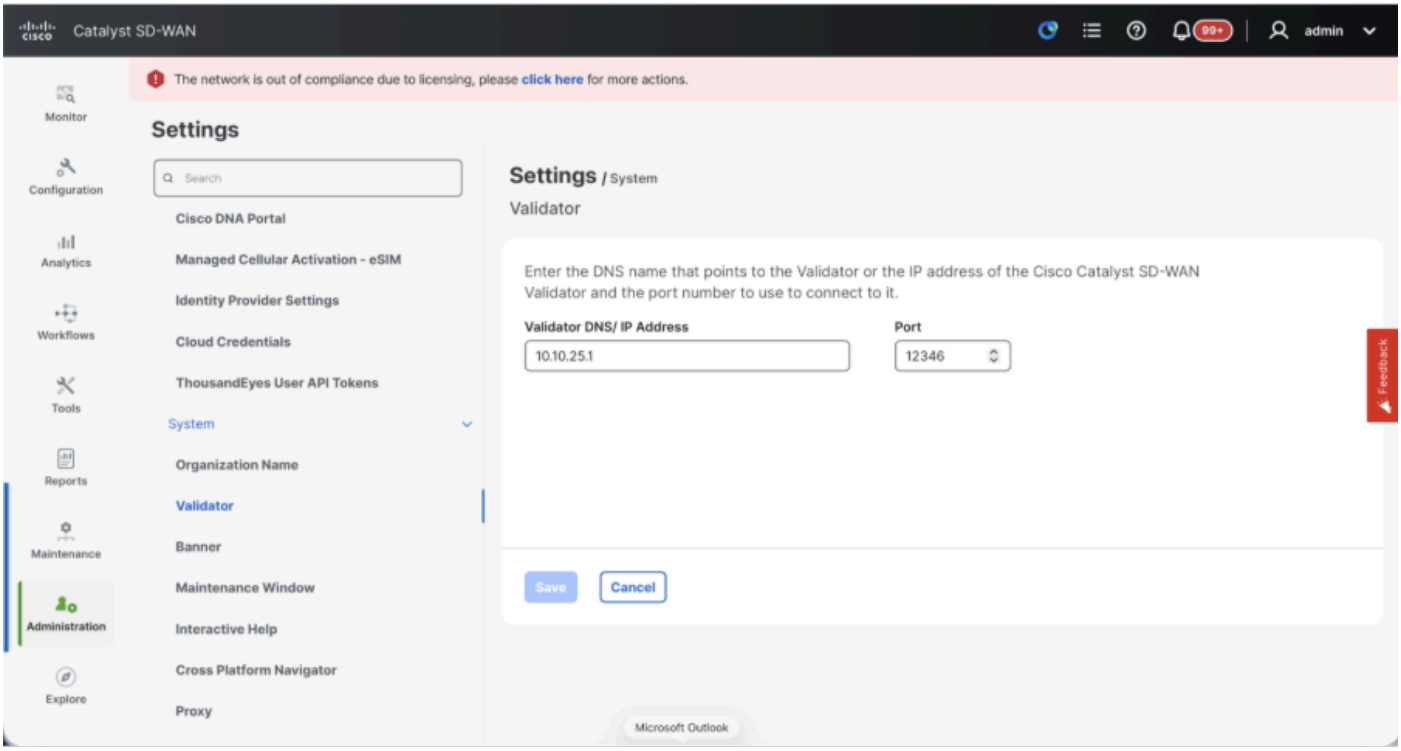
- Verificare che il numero delle istanze attive di Cisco SD-WAN Manager sia identico al numero delle nuove istanze di Cisco SD-WAN Manager.
- Accertarsi che tutte le istanze Cisco SD-WAN Manager attive e nuove eseguano la stessa versione del software.
- Verificare che tutte le istanze Cisco SD-WAN Manager nuove e attive siano in grado di raggiungere l'indirizzo IP di gestione di Cisco SD-WAN Validator.
- Verificare che i certificati siano stati installati nelle istanze di Cisco SD-WAN Manager appena installate.
- Verificare che gli orologi di tutti i dispositivi Cisco Catalyst SD-WAN, incluse le nuove istanze di Cisco SD-WAN Manager installate, siano sincronizzati.
- Verificare che nelle istanze di Cisco SD-WAN Manager appena installate sia configurato un nuovo set di IP di sistema e ID di sito, insieme alla stessa configurazione di base del cluster attivo.

Passaggio 2: Configurazione di interfaccia utente, certificati e controller integrati vManage

Aggiornare le configurazioni nell'interfaccia utente di vManage

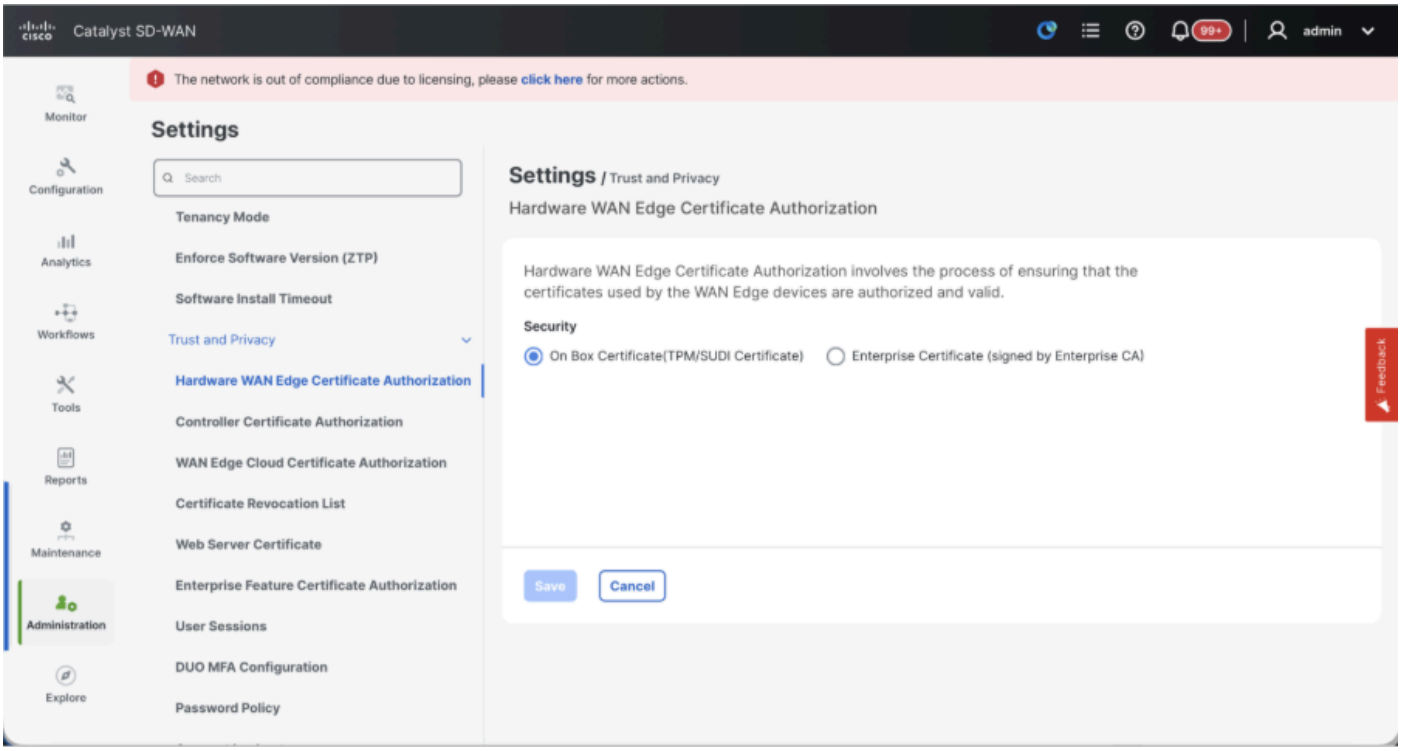
- Una volta aggiunte le configurazioni al passo 1 nella CLI di tutti i controller, possiamo accedere alla webUI di vManage, usando l'URL https://<vmanage-ip> nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi nodi vManage. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Amministrazione > Impostazioni e completare i seguenti passaggi.
- Configurare il nome dell'organizzazione e l'URL/indirizzo IP di Validator/vBond. Configurare lo stesso valore presente nella CLI del nodo vManage.
- In vManage 20.15/20.18 queste configurazioni sono disponibili nella sezione Sistema.



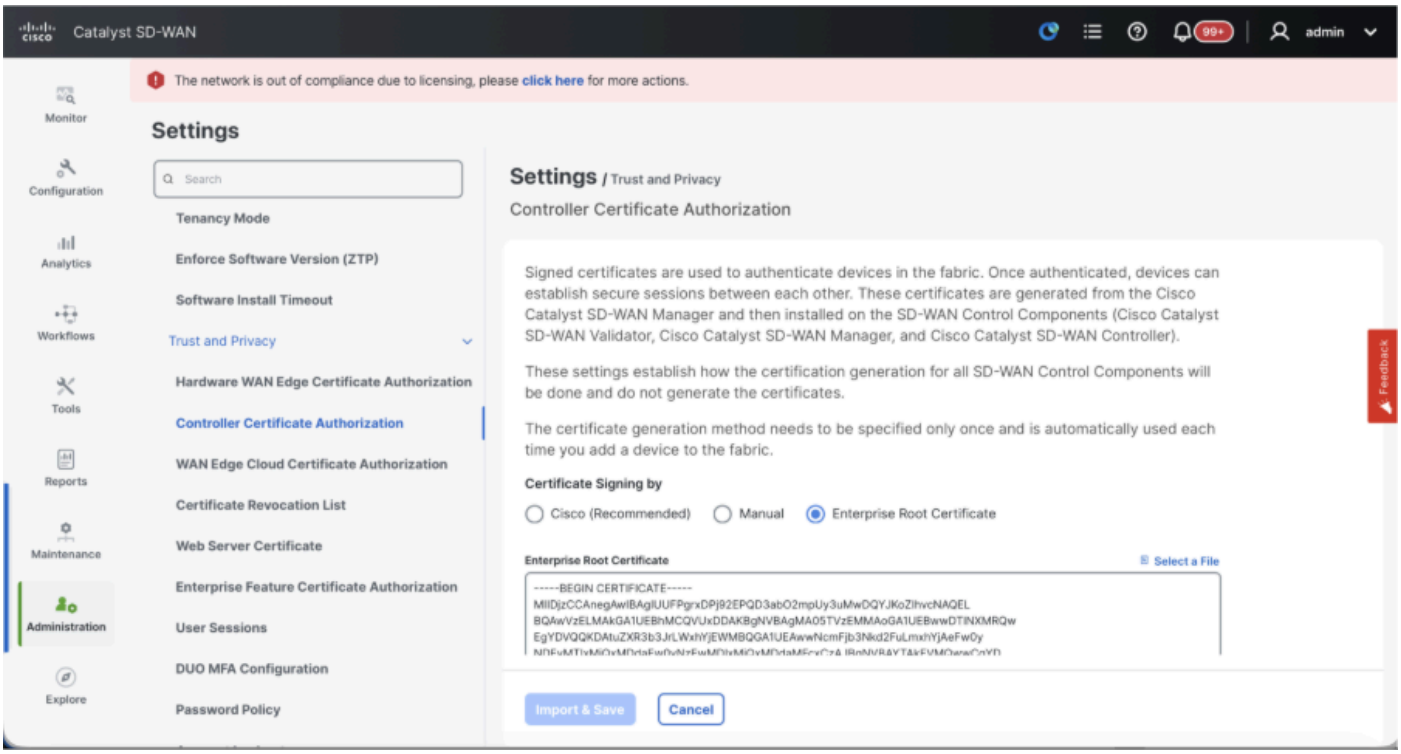


- Verificare le configurazioni per l'Autorità di certificazione (CA), che decide l'Autorità di certificazione utilizzata per firmare i certificati. Sono disponibili 3 opzioni:

1. Autorizzazione certificato perimetro WAN hardware - Decide la CA per i router perimetrali SD-WAN hardware.
    - Certificato On-Box (certificato TPM/SUDI): con questa opzione, il certificato preinstallato sull'hardware del router viene utilizzato per stabilire le connessioni di controllo (connessioni TLS/DTLS)
    - Certificato organizzazione (firmato dall'autorità di certificazione dell'organizzazione): questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

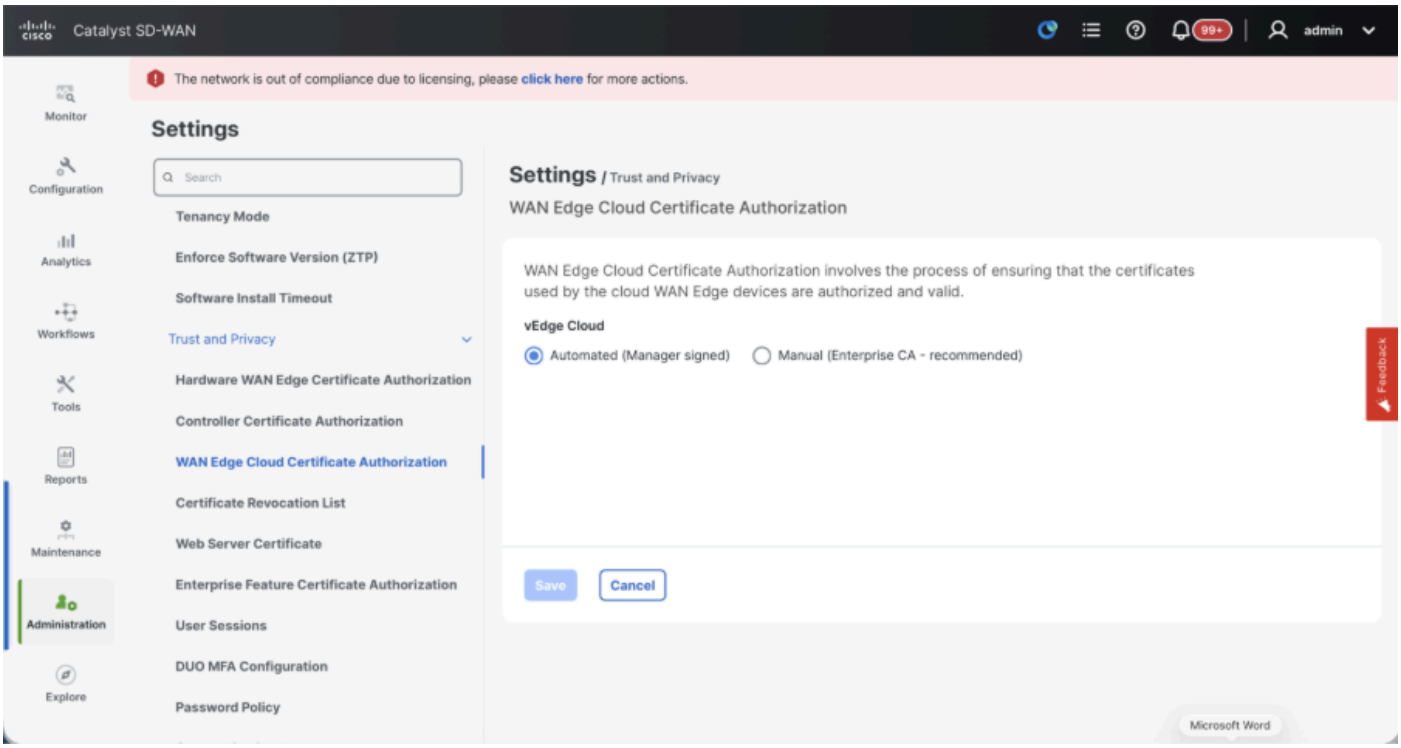


2. Controller Certificate Authorization - Decide la CA per i controller SD-WAN.
    - Cisco (scelta consigliata) - I controller utilizzano i certificati firmati da Cisco PKI. vManage contatta automaticamente il portale PNP utilizzando le credenziali dello smart account configurate in vManage e ottiene la firma del certificato che viene installato nel controller.
    - Manuale: i controller utilizzano i certificati firmati da Cisco PKI. Firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
    - Certificato radice dell'organizzazione: questa opzione consente ai router di utilizzare certificati firmati dall'autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

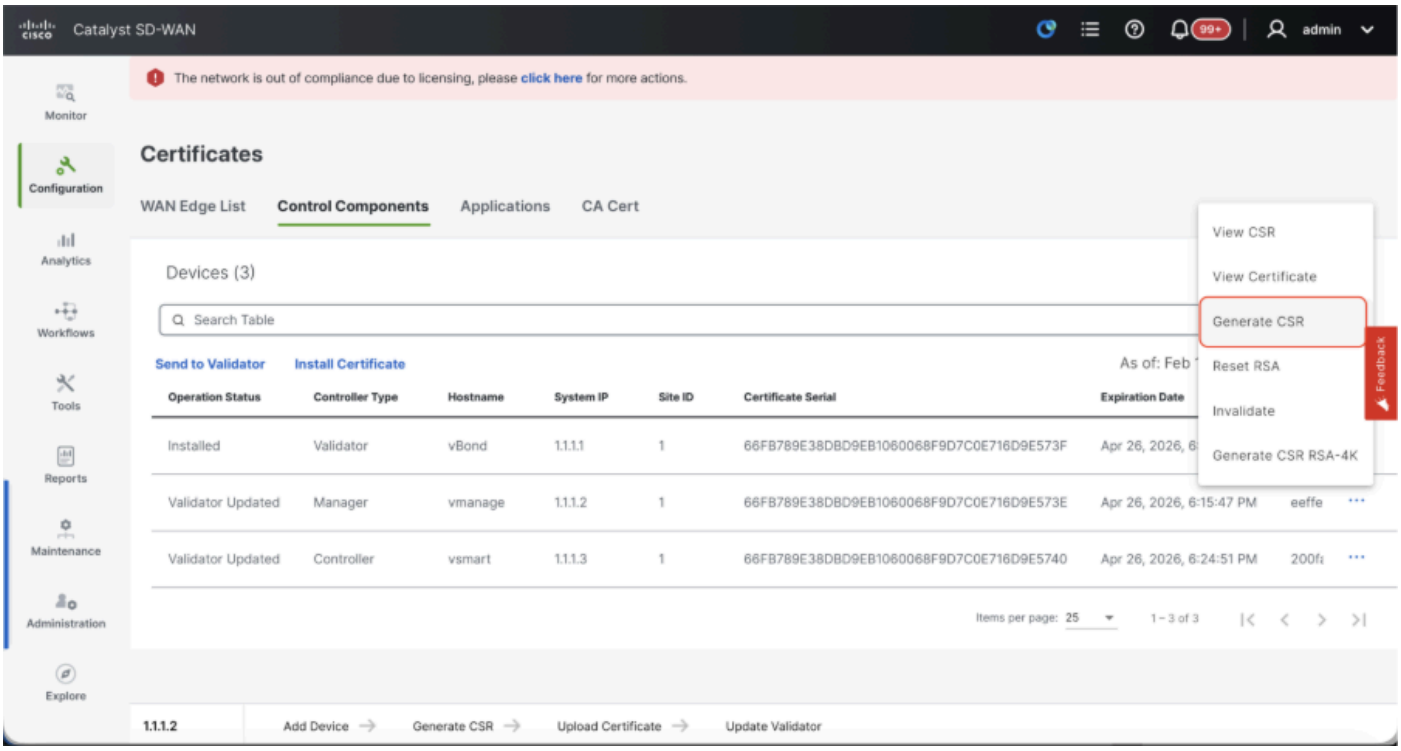


3. Autorizzazione certificato cloud perimetrale WAN - Decide la CA per i router perimetrali SD-WAN virtuali (CSR1000v, C8000v, vEdge cloud)
    - Automatizzato (vManage firmato): vManage firma automaticamente il CSR per i router perimetrali virtuali e installa il certificato sul router.
    - Manuale (Autorità di certificazione dell'organizzazione - consigliata) - I router virtuali utilizzano certificati firmati dall'Autorità di certificazione dell'organizzazione. Quando si sceglie questa opzione, è necessario aggiornare qui il certificato radice dell'autorità di certificazione dell'organizzazione (enterprise).

Nel caso in cui si utilizzi la propria CA, Autorità di certificazione dell'organizzazione (enterprise), scegliere Enterprise.



- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller
- Fare clic su ... per Manager/vManage e fare clic su Generate CSR (Genera CSR).



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco

passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.

Caricamento di vBond/Validator e vSmart/Controller in vManage

Passare a Configurazione > Dispositivi > Controllo componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

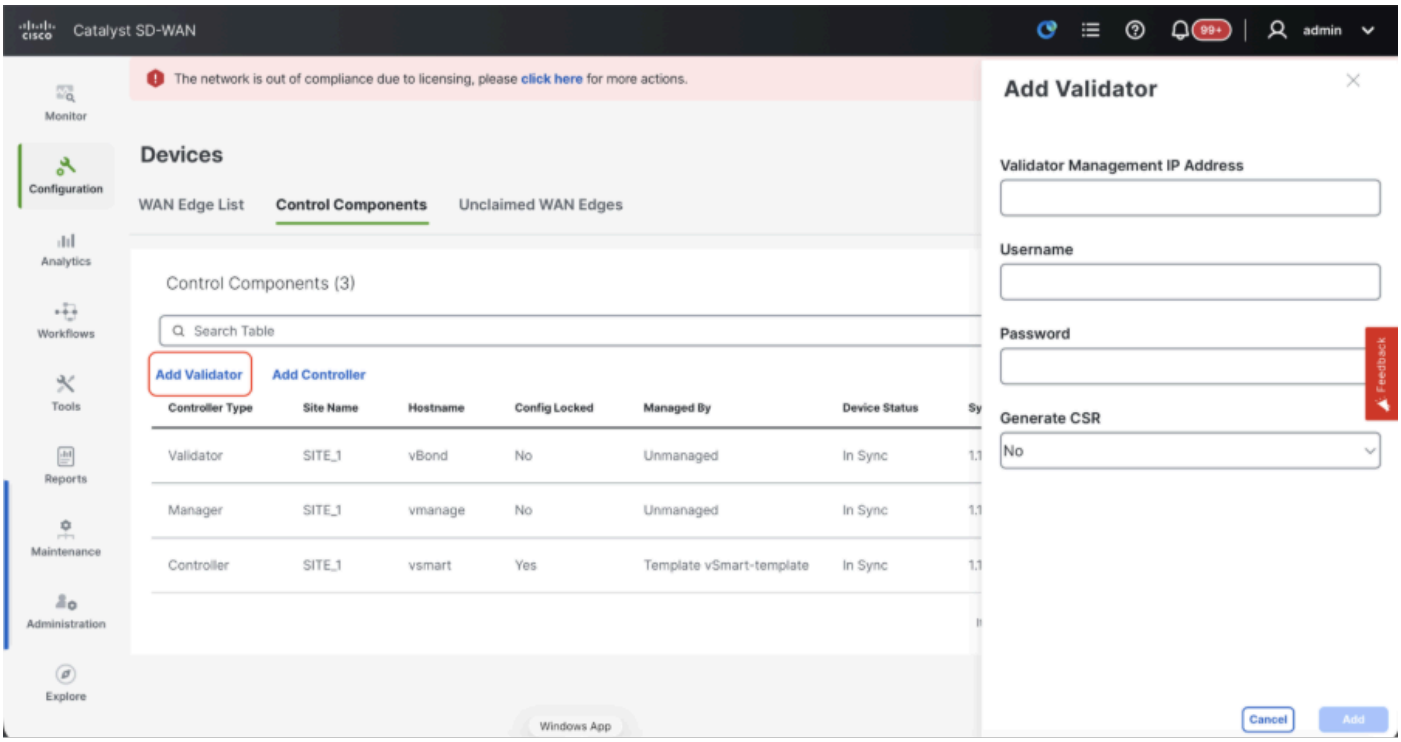
vBond/Convalida onboarding

- Fare clic su AddvBondnel caso di 20.12vManagerAggiungi validatornel caso di 20.15/20.18vManage. Viene visualizzato un popup, immettere il IP di trasporto VPN 0 di vBondraggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping se consentito dalla CLI di vManagetovBondIP.
- Immettere le credenziali utente di vBond.

Nota: è necessario utilizzare le credenziali di amministratore di vBondor una parte utente di netadmingroup. È possibile verificare questa condizione nella CLI di vBond. Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vBond

---

Nota: Se vBond è dietro un dispositivo/firewall NAT, verificare se l'IP dell'interfaccia VPN 0 di vBond è convertito in un IP pubblico. Se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, in questo passaggio utilizzare l'indirizzo IP pubblico dell'interfaccia VPN 0



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vBond.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN. Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo. La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vBonds, ripetere gli stessi passaggi.

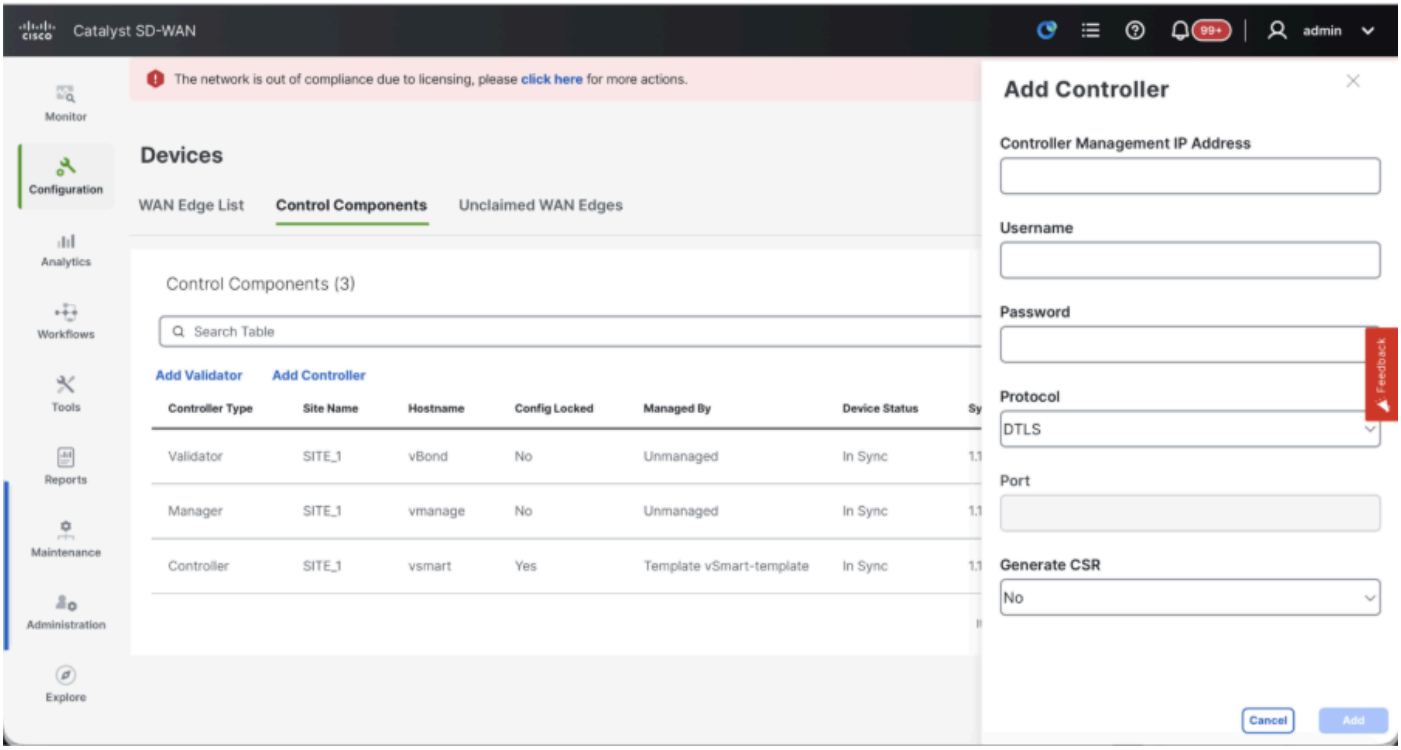
vSmart/Controller integrato:

- Fare clic su Add vSmart in caso di vManage 20.12 o Add Controller in caso di vManage 20.15/20.18.
- Viene visualizzato un popup. Immettere l'IP di trasporto VPN 0 di vSmart raggiungibile da vManage.
- Verificare la raggiungibilità usando il comando ping, se consentito dalla CLI di vManage a vSmart IP.
- Immettere le credenziali utente di vSmart Note che è necessario utilizzare le credenziali di amministratore di vSmart o di un utente appartenente al gruppo netadmin.
- È possibile verificare questa condizione nella CLI di vSmart.
- Impostare il protocollo su TLS se si intende utilizzare TLS per i router per stabilire

connessioni di controllo con vSmart. Questa configurazione deve essere configurata anche sulla CLI dei nodi vSmarts e vManage.

- Scegliere Sì nell'elenco a discesa "Generate CSR" se è necessario installare un nuovo certificato per vSmart.

Nota: se vSmart è dietro un dispositivo/firewall NAT, verificare se l'indirizzo IP dell'interfaccia vSmart VPN 0 è convertito in un indirizzo IP pubblico e se l'indirizzo IP dell'interfaccia VPN 0 non è raggiungibile da vManage, utilizzare l'indirizzo IP pubblico dell'indirizzo IP dell'interfaccia VPN 0 in questo passaggio.

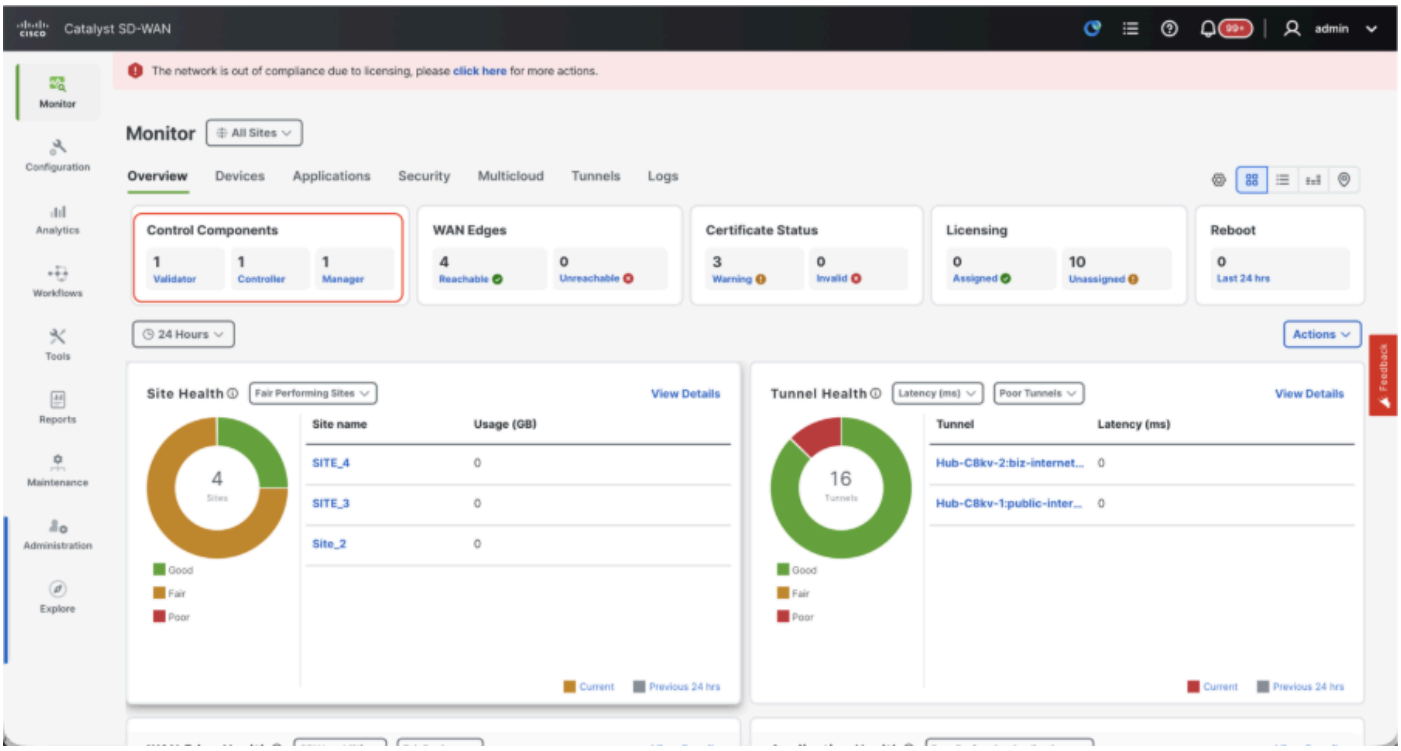


- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente sul portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente su vSmart.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Se sono presenti più vSmarts, ripetere gli stessi passaggi.

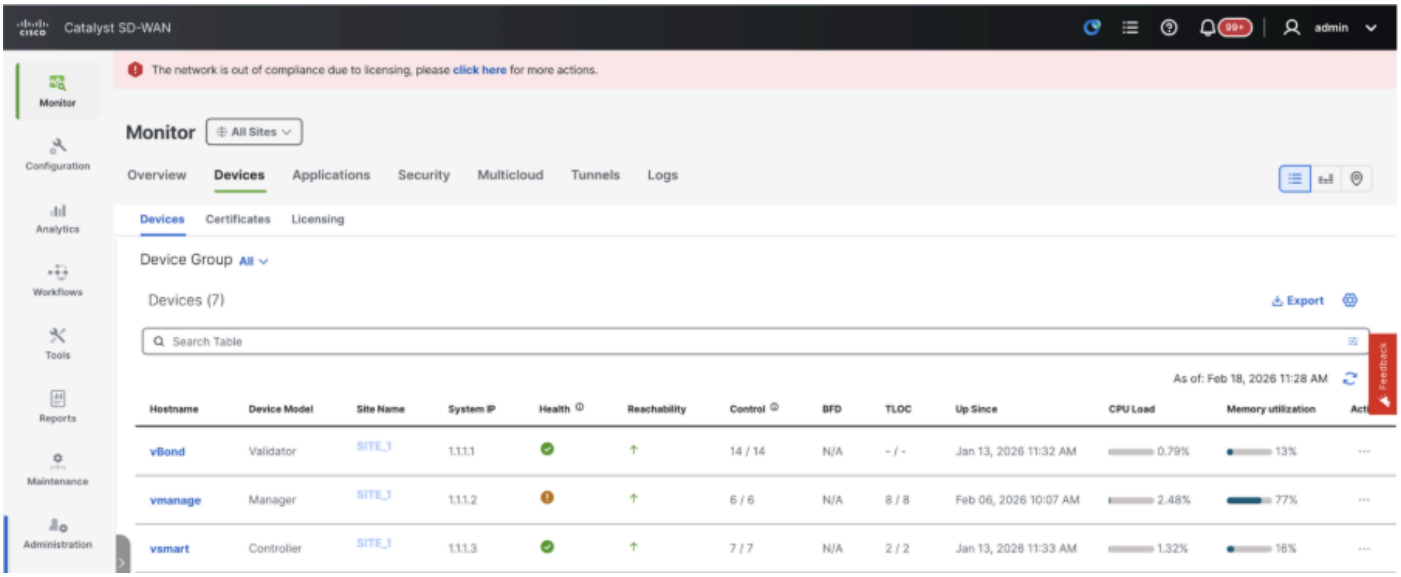
Verifica

Una volta completati tutti i passaggi, verificare che tutti i componenti di controllo siano raggiungibili

in Monitor>Dashboard



- Fate clic sui rispettivi componenti di controllo e verificate che siano tutti raggiungibili.
- Passare a Monitor > Dispositivi e verificare che tutti i componenti di controllo siano raggiungibili.



Passaggio 3: Crea cluster vManage

Fabric SD-WAN integrato con un cluster vManage nella sovrapposizione SD-WAN

Nota: il cluster vManage può essere configurato con 3 nodi vManage o 6 nodi vManage a seconda del numero di siti collegati all'infrastruttura SD-WAN

Integrazione di tutti i controller SD-WAN con un unico nodo vManage

Procedere con i passaggi condivisi in "Controller SD-WAN integrati con un singolo nodo vManage nella sovrapposizione SD-WAN" per avviare prima il fabric SD-WAN con un nodo vManage e incorporare tutti i validatori (vBond) e i controller (vSmart) richiesti.

Configurare le configurazioni CLI di tutti i nodi vManage appartenenti al cluster

- Configurare gli altri nodi vManage. In caso di cluster a 3 nodi, sono disponibili 2 nodi da configurare, in caso di cluster a 6 nodi sono disponibili 5 nodi da configurare.
- Configurare le configurazioni di sistema come mostrato:

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Nota: se si utilizza URL come indirizzo vBond, verificare di configurare gli indirizzi IP dei server DNS nella configurazione VPN 0 o di risolverli.

Queste configurazioni sono necessarie per abilitare l'interfaccia di trasporto utilizzata per stabilire le connessioni di controllo con i router e gli altri controller.

```
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
```

Configurare inoltre l'interfaccia di gestione VPN 512 per consentire l'accesso di gestione fuori

banda al controller.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

Configurazione facoltativa:

- È possibile fare riferimento alle configurazioni del controller esistente e, se la configurazione indicata è presente, è possibile aggiungerla ai nuovi controller.
- Configurare il protocollo di controllo come TLS solo se i router devono stabilire connessioni di controllo protette con i nodi vManage che utilizzano TLS. Per impostazione predefinita, tutti i controller e i router stabiliscono una connessione di controllo utilizzando il protocollo DTLS. Si tratta di una configurazione opzionale richiesta solo sui nodi vSmart e vManage a seconda delle esigenze.

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

Configura interfaccia di servizio in tutti i nodi vManage

Configurare l'interfaccia del servizio su tutti i vManagenodes, incluso vManage-1 che è già stato caricato. Questa interfaccia viene utilizzata per la comunicazione del cluster, ovvero la comunicazione tra i vManagenodes nel cluster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Verificare che per l'interfaccia di servizio in tutti i nodi del cluster vManagement venga utilizzata la stessa subnet IP.

Configura credenziali cluster

È possibile utilizzare le stesse credenziali di amministrazione dei nodi vManage per configurare il cluster vManage. In caso contrario, è possibile configurare una nuova credenziale utente che faccia parte di netadmingroup. Le configurazioni per la configurazione delle nuove credenziali utente sono le seguenti

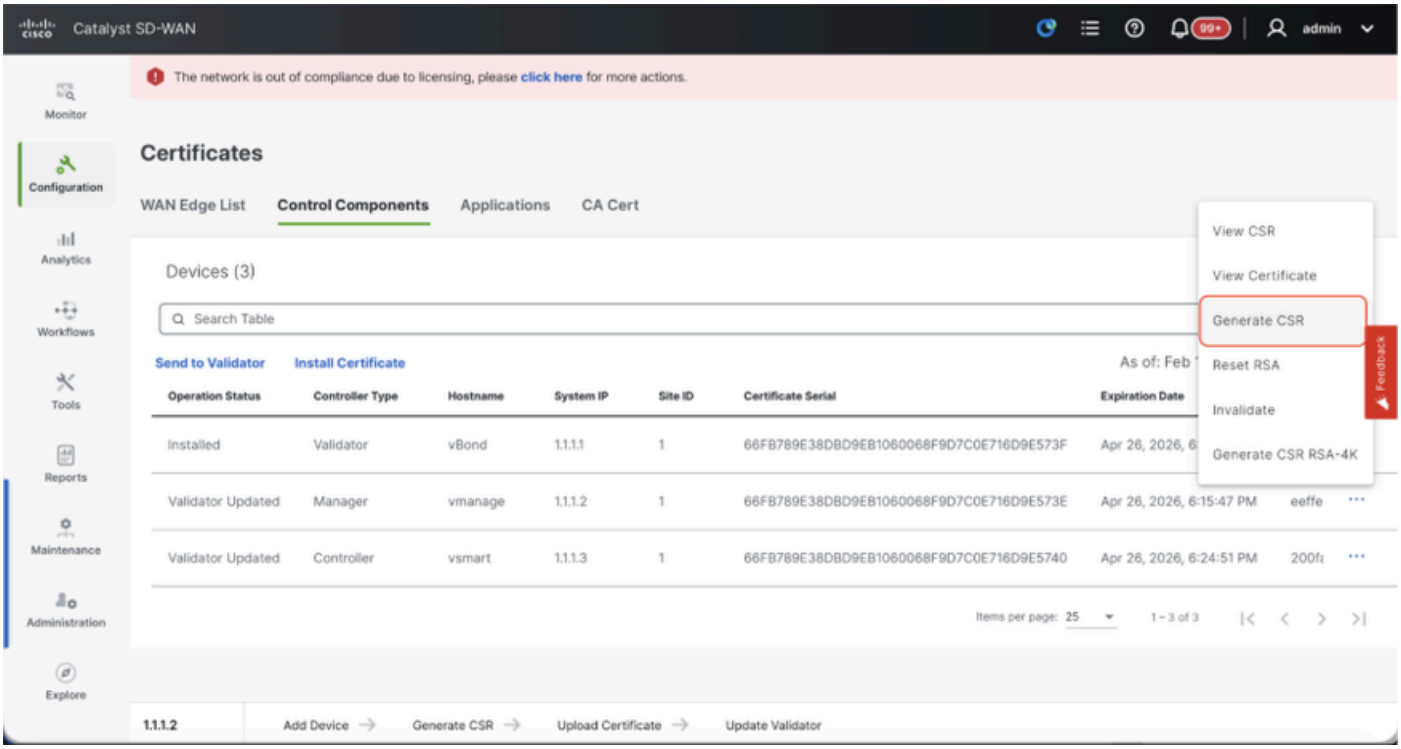
```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

Assicurarsi di configurare le stesse credenziali utente in tutti gli vManagenodeche fanno parte del cluster.Se si decide di utilizzare le credenziali di amministratore, è necessario che siano lo stesso nome utente/password in tutti gli vManagenodes.

Installa certificato dispositivo in tutti i nodi vManage

- Accedere a vManageUI di tutti i vManagenodes utilizzando l'URL https://<vmanage-ip>nel browser. Utilizzare l'indirizzo IP VPN 512 dei rispettivi vManagenode. È possibile eseguire l'accesso con il nome utente e la password admin.
- Passare a Configurazione > Certificati > Controlla componenti nel caso di nodi vManage 20.15/20.18. Nel caso delle versioni 20.9/20.12, Configurazione > Dispositivi > Controller

  Fare clic su ... per Manager/vManage e fare clic su Generate CSR.



- Una volta generato il CSR, è possibile scaricarlo e firmarlo in base all'autorità di certificazione scelta per i controller. È possibile verificare questa configurazione in Amministrazione > Impostazioni > Autorizzazione certificato controller. Se si sceglie Cisco (scelta consigliata), il CSR viene caricato automaticamente nel portale PNP da vManage e, una volta firmato, il certificato viene installato automaticamente in vManage.
- Se si sceglie Manuale, firmare manualmente il CSR utilizzando il portale PNP di Cisco passando allo smart account e all'account virtuale della rispettiva sovrapposizione SD-WAN.
- Una volta che il certificato è disponibile dal portale PNP, fare clic su installa certificato nella stessa sezione di vManage, quindi caricare il certificato e installarlo.
- La stessa procedura è applicabile se si utilizza un certificato radice Digicert ed Enterprise.
- Completare questo passaggio in tutti i nodi vManage che fanno parte del cluster.

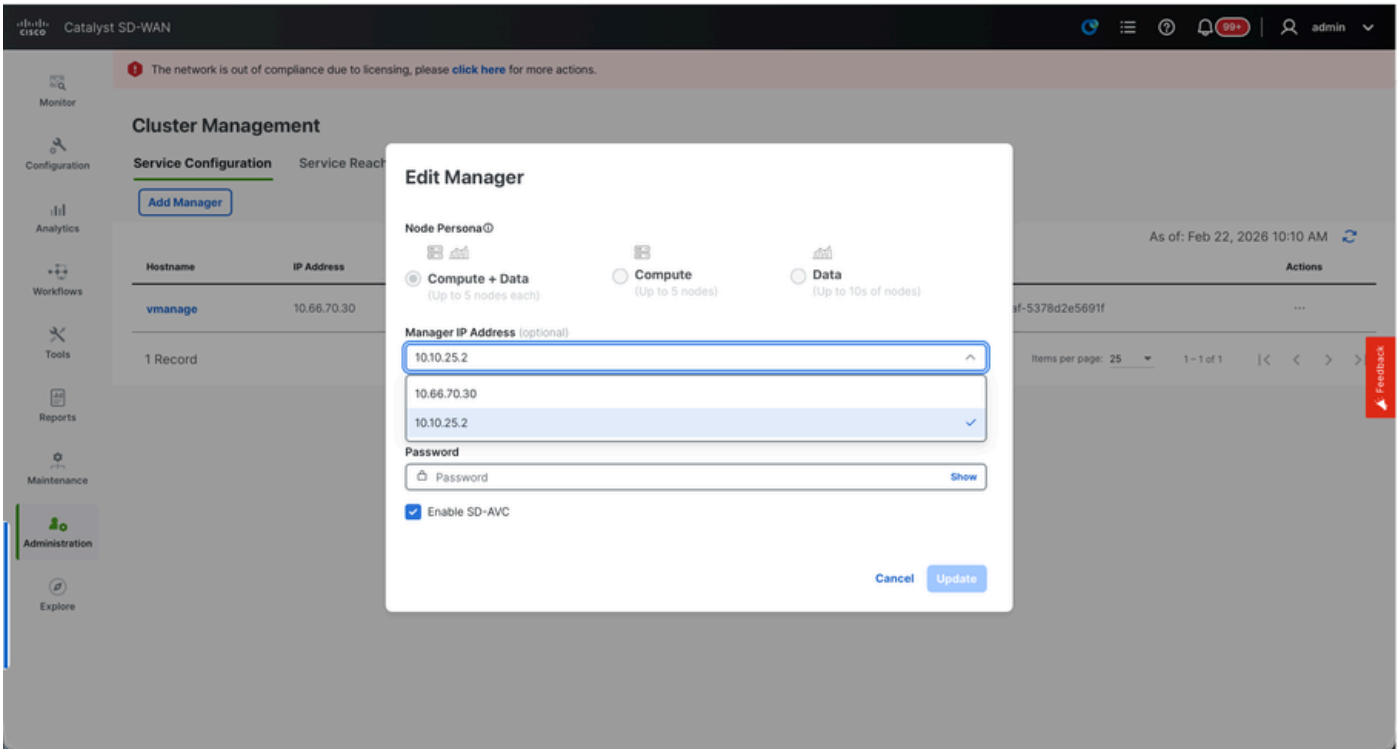
Preparare la creazione del cluster vManage

- Sul WebUI di vManage-1, selezionare Amministrazione > Gestione cluster, fare clic su ... in Azioni per vManage-1, scegliere Modifica.
- La persona del nodo viene scelta automaticamente in base alla persona scelta durante

lo spun up della VM.

Nota: Per un cluster a 3 nodi, tutti e 3 i nodi vManage vengono visualizzati con compute+data come persona. Per un cluster a 6 nodi, vengono visualizzati 3 nodi vManage con dati di tipo compute+data come utente e 3 nodi vManage come utente.

- Dall'elenco a discesa per l'indirizzo IP di Manager, assicurarsi di scegliere l'indirizzo IP dell'interfaccia di servizio di vManage.



- Immettere il nome utente e la password che si desidera utilizzare per abilitare il cluster vManage, definito credenziali del cluster.
- Come accennato in precedenza, è necessario configurare le stesse credenziali su tutti i nodi vManage e utilizzarle durante l'aggiunta di tutti i nodi al cluster.

Configurazione facoltativa:

Fare riferimento a questa configurazione nel cluster esistente per Abilitare SDAVC: deve essere verificata solo se è necessaria ed è necessaria solo su un nodo vManage del cluster.

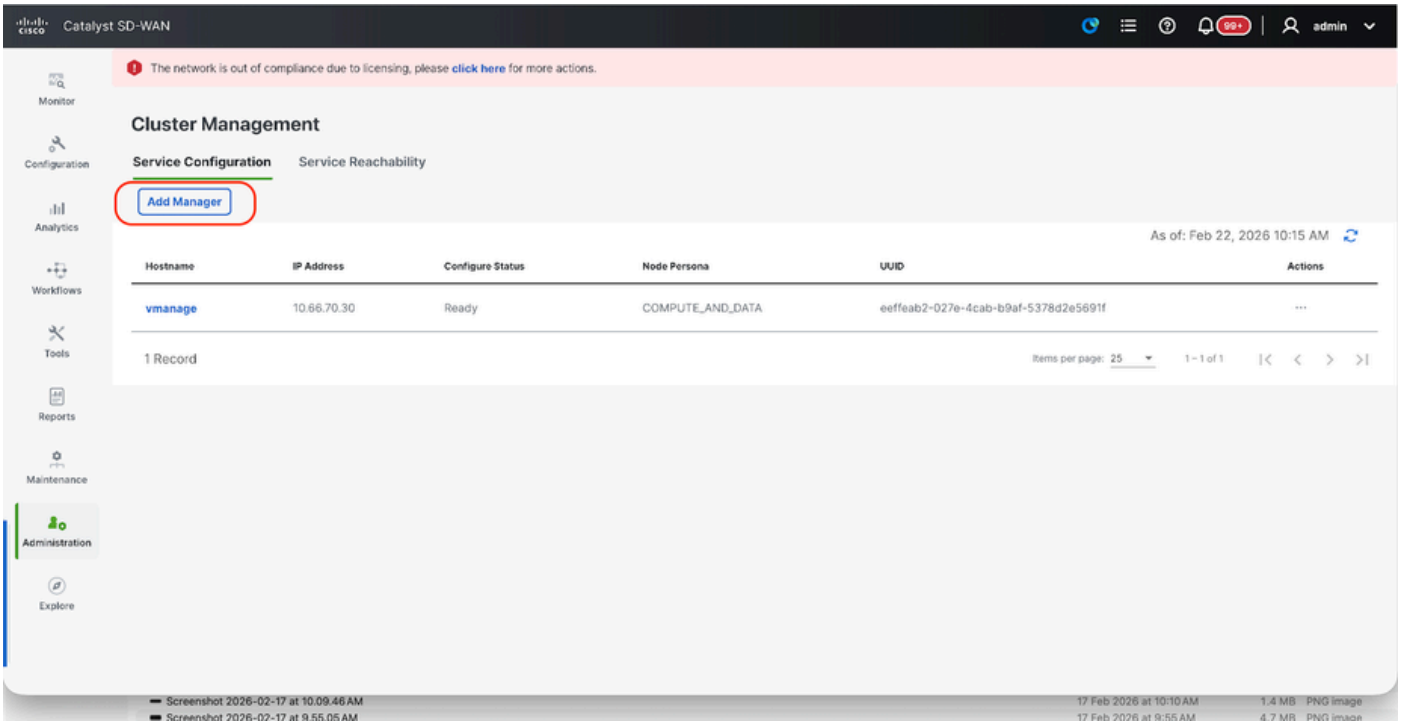
Fare clic su Aggiorna.

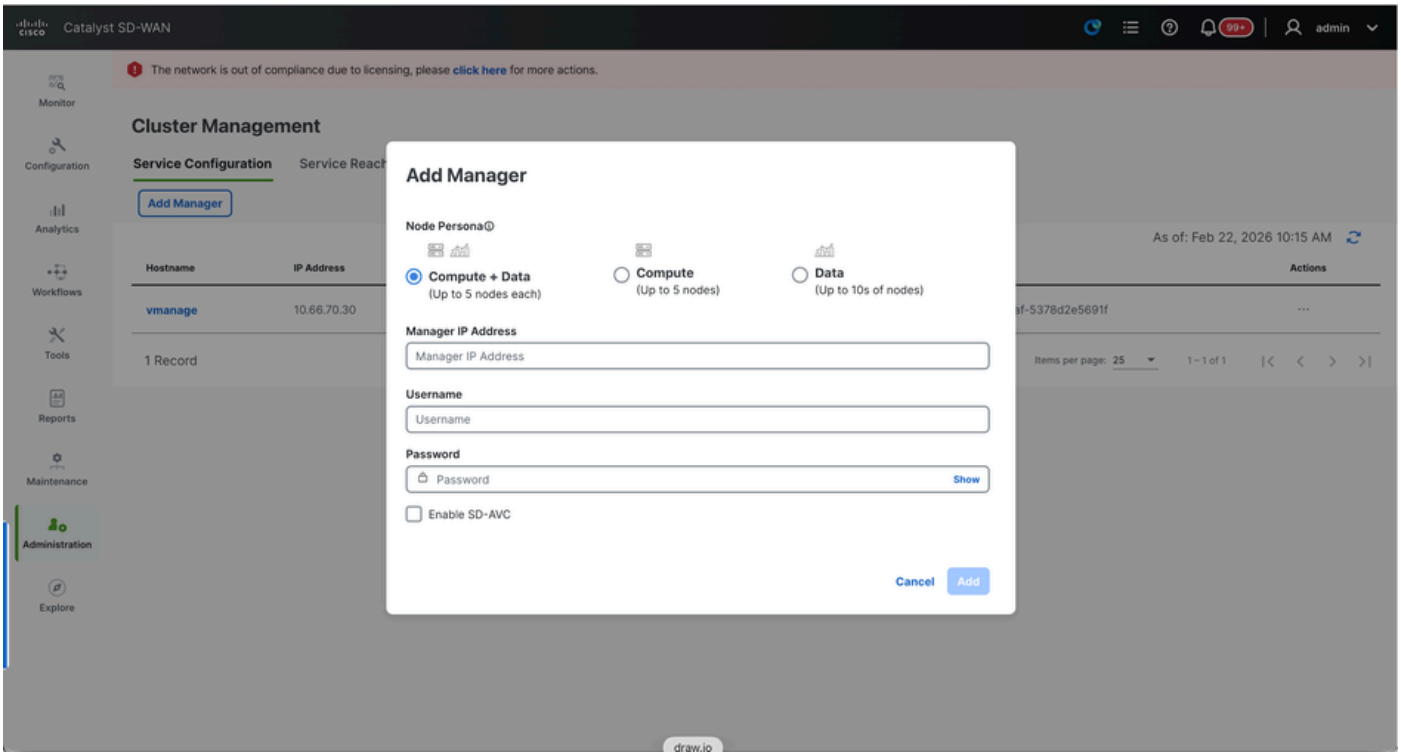
- In seguito, i servizi vManage NMS vengono riavviati in background e l'interfaccia utente non è disponibile per alcuni minuti, dai 5 ai 10 minuti circa. Durante questo periodo, l'accesso CLI di vManage è disponibile.
- Una volta che l'interfaccia utente di vManage-1 è accessibile, passare a Amministrazione > Gestione cluster, verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP,Lo stato della configurazione è Pronto e la persona del nodo viene

riflessa correttamente. Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili.
- Se si rileva che uno dei servizi non è ancora raggiungibile, attendere. Di solito ci vogliono dai 20 ai 30 minuti.

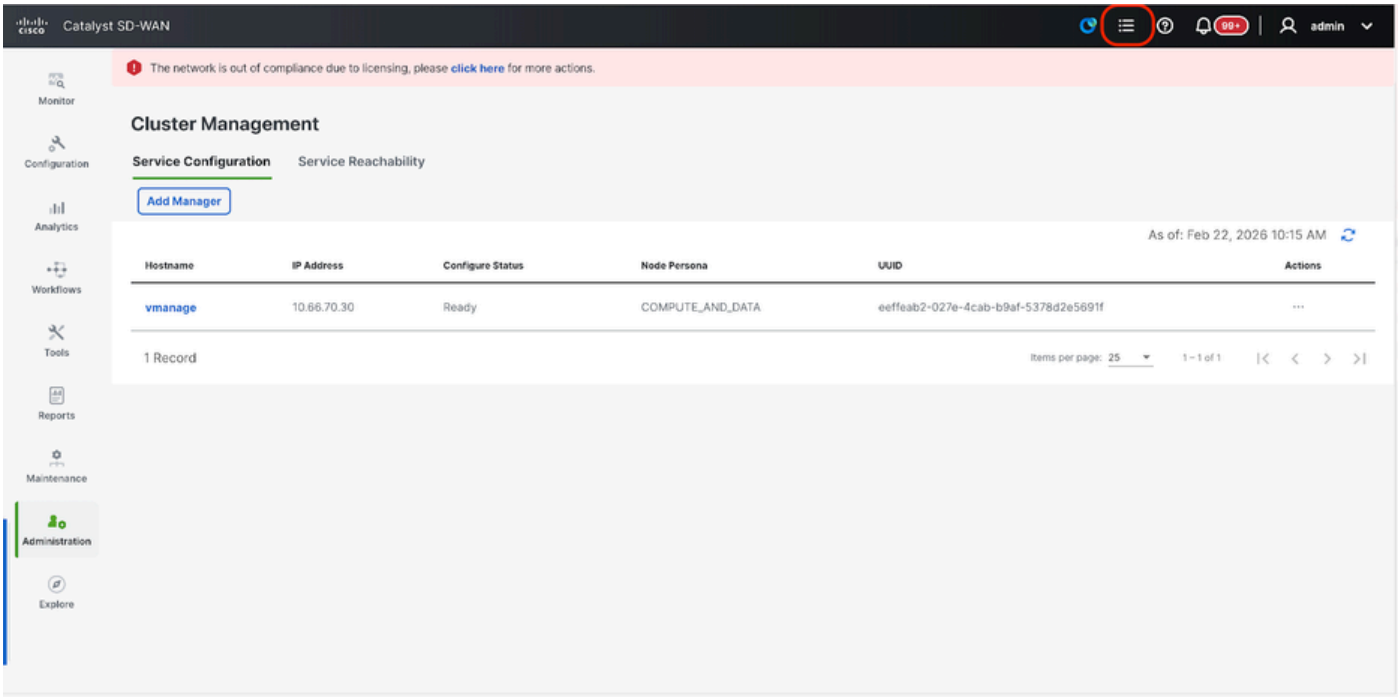
Crea il cluster vManage

- Sul WebUI di vManage-1, selezionare Amministrazione > Gestione cluster, nella sezione Configurazione servizio,
- Fare clic su Add Manager, viene visualizzata una finestra popup:





- Scegliere la persona Nodo in base alle configurazioni della persona eseguite durante l'esecuzione dello spun-up del nodo vManage - 2.
- Immettere l'indirizzo IP dell'interfaccia di servizio di vManage-2 in Indirizzo IP manager
- Immettere il nome utente e la password, ovvero le stesse credenziali utilizzate nel passaggio 6.
- Abilita SDAVC - Da lasciare deselezionato come avremmo già abilitato su vManage-1
- Fare clic su Aggiungi.
- In seguito, i servizi vManage NMS vengono riavviati in background per i nodi vManage 1 e 2. L'interfaccia utente non è disponibile per alcuni minuti, dai 5 ai 10 minuti circa, per vManage 1 e 2.
- Durante questo periodo, è disponibile l'accesso CLI di vManage 1 e 2.
- Una volta che l'interfaccia utente di vManage-1 è accessibile, passare a Amministrazione > Gestione cluster, verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP, Configura stato sia Pronto e che la persona del nodo sia indicata correttamente.
- Passare alla sezione Raggiungibilità servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili per entrambi i nodi vManage.
- Se si rileva che uno dei servizi non è ancora raggiungibile, attendere. Di solito ci vogliono dai 5 ai 10 minuti.
- È possibile controllare lo stato del processo di aggiunta cluster nell'elenco Attività disponibile nell'angolo superiore destro dell'interfaccia utente di vManage.



- È possibile cercare Elenco attività attivo e se l'attività è ancora elencata in Elenco attività attivo, indica che l'attività non è stata ancora completata.
- È possibile fare clic sull'attività per verificarne lo stato di avanzamento. Se l'attività non è elencata in Elenco attività attivo, passare a Completato e assicurarsi che l'attività sia stata completata correttamente.
- Solo dopo la convalida di questi punti, procedere al passaggio successivo.

Prima di aggiungere il nodo successivo al cluster, è necessario prendere in considerazione i seguenti punti:

Verificare questi punti in tutte le interfacce utente dei nodi vManage aggiunti al cluster:

- Passare a Monitoraggio > Panoramica dell'interfaccia utente di vManage e verificare che il numero di nodi vManage sia indicato correttamente e che sia raggiungibile a seconda del numero di nodi aggiunti al cluster.

- Passare a Amministrazione > Gestione cluster e verificare che l'indirizzo IP dell'interfaccia di servizio di vManage sia indicato in Indirizzo IP, che Configura stato sia Pronto e che la persona del nodo sia indicata correttamente.
- Passare alla sezione Raggiungibilità del servizio nella stessa pagina e verificare che tutti i servizi siano raggiungibili per entrambi i nodi vManage.

- Ogni volta che un nodo viene aggiunto al cluster, i servizi NMS di tutti i nodi nel cluster vengono riavviati, pertanto l'interfaccia utente di tutti questi nodi diventa irraggiungibile per un certo periodo di tempo.
- A seconda del numero di nodi nel cluster, il backup dell'interfaccia utente e la raggiungibilità di tutti i servizi possono richiedere più tempo.
- È possibile monitorare l'attività in Elenco attività disponibile nell'angolo superiore destro dell'interfaccia utente di vManage.
- Nell'interfaccia utente di vManage di ogni nodo aggiunto al cluster, è necessario visualizzare tutti i router, i modelli e i criteri, se disponibili in vManage-1.
- Se tali configurazioni non erano presenti in vManage-1, le configurazioni vBonds e vSmarts aggiunte a vManage-1 e anche Amministrazione > Impostazioni per Nome organizzazione, vBond, Autorizzazione certificato devono essere riflesse sul resto dei nodi vManage aggiunti al cluster.
- Ripetere gli stessi passaggi per gli altri nodi vManage.

Passaggio 4: Backup/ripristino di Config-db

Raccolta del backup e del ripristino vManage configuration-db in un altro nodo vManage

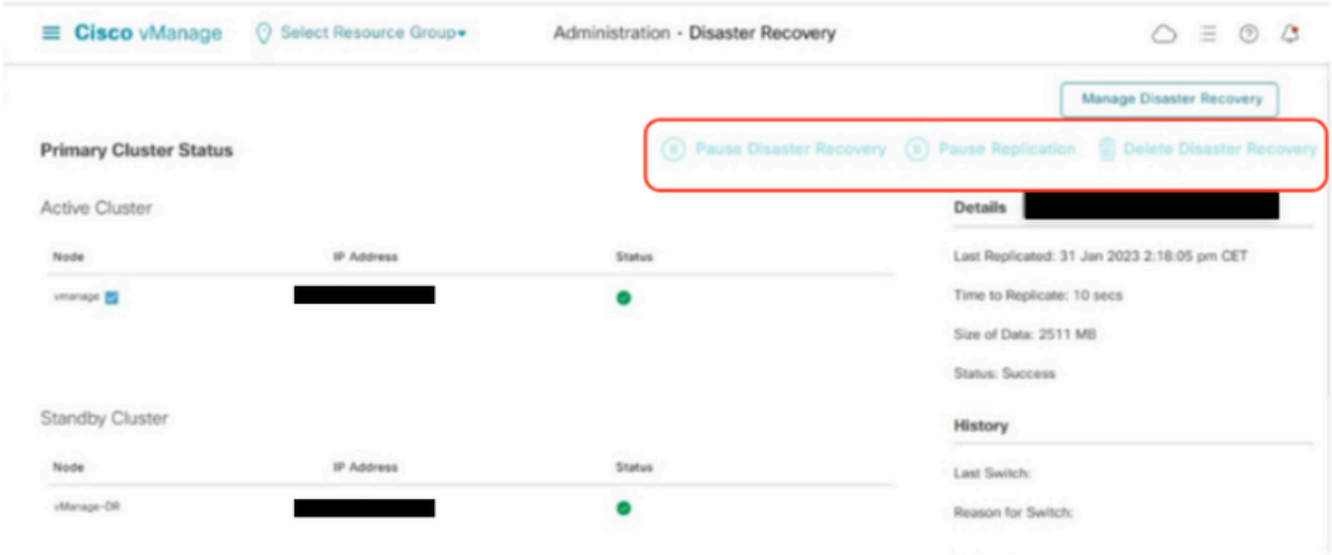
---

Nota: Durante la raccolta del backup del database di configurazione dal cluster vManage esistente in cui è abilitato il ripristino di emergenza, assicurarsi che venga raccolto dopo che il ripristino di emergenza in tale nodo è stato sospeso ed eliminato.

Confermare che non è in corso la replica per il disaster recovery. Selezionare Amministrazione > Disaster Recovery e verificare che lo stato sia Operazione riuscita e non in uno stato transitorio, ad esempio Importazione in sospeso, Esportazione in sospeso o Download in sospeso. Se lo stato non ha esito positivo, contattare Cisco TAC e verificare la corretta replica prima di sospendere il ripristino di emergenza.

Sospendere innanzitutto il ripristino di emergenza e assicurarsi che l'attività sia completata.

Eliminare quindi il ripristino di emergenza e verificare che l'attività sia stata completata.



Contattare Cisco TAC per garantire la corretta pulizia del dispositivo di ripristino di emergenza.

Raccolta backup del database di configurazione:

- Nell'infrastruttura SD-WAN attualmente in uso, è possibile generare il backup del database di configurazione dal cluster vManage.
- Si noti che è necessario generare il backup del database di configurazione solo su un nodo del cluster vManage che è il leader del database di configurazione.

- Per vManage standalone, vManage è il leader del database di configurazione.
- In cluster vManage, identificare il nodo della linea guida configuration-db utilizzando il comando request nms configuration-db diagnostics.È possibile eseguire questo comando su tutti i nodi del cluster vManage a 3 nodi.
- In un cluster a 6 nodi, assicurarsi di eseguire questo comando sui nodi vManage in cui configuration-db è abilitato per identificare il nodo principale. Passare a Amministrazione > Gestione cluster per verificare quanto segue:
- Come si può vedere nello screenshot, sui nodi configurati con la persona COMPUTE_AND_DATA è in esecuzione configuration-db.

È possibile verificare la stessa condizione utilizzando il comando requestnmsconfiguration-dbstatus in vManageCLI. L'output è il seguente

```
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#
```

- Una volta eseguito il comandorequest nms configuration-db diagnostics su questi nodi, l'output è il seguente:
- Cercare il campo evidenziato per "IsLeader". Se è impostato su 1, indica che il nodo è il nodo della linea guida e da esso è possibile raccogliere il backup del database di configurazione.

```
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     .
```

Utilizzare questo comando per raccogliere il backup del database di configurazione dal nodo vManage leader del database di configurazione identificato.

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

L'output previsto è il seguente:

```
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#
```

- Prendere nota delle credenziali di configuration-db se sono state aggiornate.
- Se non si è a conoscenza delle credenziali del database di configurazione, contattare TAC per recuperare le credenziali del database di configurazione dai nodi vManage esistenti.
- Le credenziali di configuration-db predefinite sono nome utente: neo4j e password: password

Ripristinare il backup di Configuration-db in un altro nodo vManage

Copiare il backup del database di configurazione nella directory /home/admin/ di vManage utilizzando SCP.

Output di esempio del comando scp:

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

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

Per ripristinare il backup del database di configurazione, è necessario innanzitutto configurare le credenziali del database di configurazione. Se le credenziali del database di configurazione sono predefinite (neo4j/password), è possibile ignorare questo passaggio.

Per configurare le credenziali configuration-db, utilizzare il comando request nms configuration-db update-admin-user.Utilizzare il nome utente e la password desiderati.

Notare che il server applicazioni di vManage è stato riavviato. A causa della quale l'interfaccia utente di vManage diventa inaccessibile per un breve periodo.

```
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 in cui è possibile procedere al ripristino del backup del database di configurazione:

È possibile utilizzare il comando request nms configuration-db restore path /home/admin/< > per ripristinare configuration-db nel nuovo 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
```

Una volta ripristinato il database di configurazione, verificare che l'interfaccia utente di vManage sia accessibile. Attendere circa 5 minuti e quindi tentare di accedere all'interfaccia utente.

Dopo aver eseguito correttamente il login all'interfaccia utente, verificare che l'elenco dei router perimetrali, il modello, i criteri e tutte le altre configurazioni presenti nell'interfaccia utente vManage precedente o esistente siano riflessi nella nuova interfaccia utente vManage.

Passaggio 5: Abilitare il ripristino di emergenza in un cluster vManage

Controlli preliminari importanti

Per procedere con il ripristino di emergenza, è necessario configurare e utilizzare due cluster vManage a 3 nodi separati. Nel cluster attivo è necessario che le convalide e i controller siano integrati. Nel caso in cui si disponga di validator e controller sul sito DR, è necessario che questi siano installati anche sul cluster attivo e non sul cluster DR vManage.

Cisco consiglia di soddisfare i seguenti requisiti prima di registrare il disaster recovery:

- Verificare che il nodo primario e il nodo secondario siano raggiungibili da HTTPS su una VPN di trasporto (VPN 0).
- Verificare che i Cisco vSmart Controller e i Cisco vBond Orchestrator sull'installazione secondaria siano collegati all'installazione primaria.
- Verificare che il nodo primario e il nodo secondario Cisco vManage eseguano la stessa versione di Cisco vManage.
- Interfaccia cluster fuori banda (interfaccia di servizio) nella VPN 0.
- Per ogni istanza vManage all'interno di un cluster, è necessaria una terza interfaccia (collegamento cluster) oltre alle interfacce utilizzate per VPN 0 (trasporto) e VPN 512 (gestione).
- Questa interfaccia viene utilizzata per la comunicazione e la sincronizzazione tra i server vManage all'interno del cluster.
- Questa interfaccia deve essere di almeno 1 Gbps e avere una latenza di 4 ms o inferiore. Si consiglia un'interfaccia di 10 Gbps.
- Entrambi i nodi vManage devono essere in grado di raggiungere l'uno l'altro tramite questa interfaccia: che si tratti di un segmento di livello 2 o di un instradamento di livello 3.

- In ogni vManage, questa interfaccia deve essere configurata nella GUI come interfaccia cluster (Amministrazione > Gestione cluster - indicare l'indirizzo IP, l'utente e la password dell'interfaccia cluster fuori banda).
- Per consentire ai nodi Cisco vManage di comunicare tra loro nei data center, abilitare le porte TCP 8443 e 830 sui firewall del data center.
- Verificare che tutti i servizi (application-server, configuration-db, messaging server, coordination server e statistics-db) siano abilitati su entrambi i nodi Cisco vManage.
- Distribuire tutti i controller, inclusi i Cisco vBond Orchestrator, nei centri dati principali e secondari. Verificare che questi controller siano raggiungibili dai nodi Cisco vManage distribuiti nei centri dati. I controller si connettono solo al nodo Cisco vManage primario.
- Verificare che non siano in corso altre operazioni nel nodo Cisco vManage attivo (primario) e in standby (secondario). Verificare, ad esempio, che nessun server stia aggiornando o collegando modelli ai dispositivi.
- Disabilitare il server proxy HTTP/HTTPS Cisco vManage, se abilitato. Vedere Server proxy HTTP/HTTPS per la comunicazione Cisco vManage con server esterni. Se non si disabilita il server proxy, Cisco vManage tenta di stabilire la comunicazione per il ripristino di emergenza tramite l'indirizzo IP proxy, anche se gli indirizzi IP dei cluster fuori banda di Cisco vManage sono raggiungibili direttamente. È possibile riattivare il server proxy Cisco vManage HTTP/HTTPS al termine della registrazione del ripristino di emergenza.
- Prima di avviare il processo di registrazione del ripristino di emergenza, passare alla finestra Strumenti > Riconosci rete sul nodo Cisco vManage principale e individuare nuovamente i Cisco vBond Orchestrator.

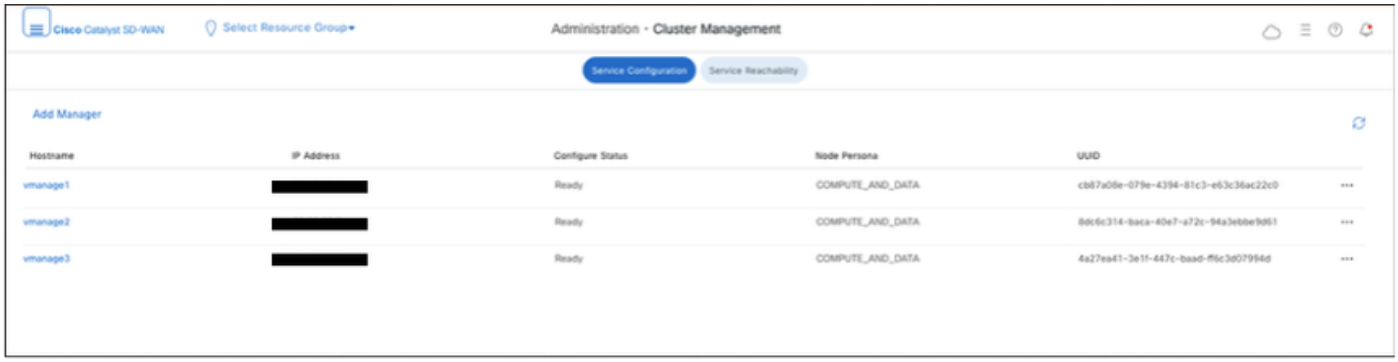
Configurazioni

Per ulteriori informazioni su vManage Disaster Recovery, fare riferimento a questo collegamento.

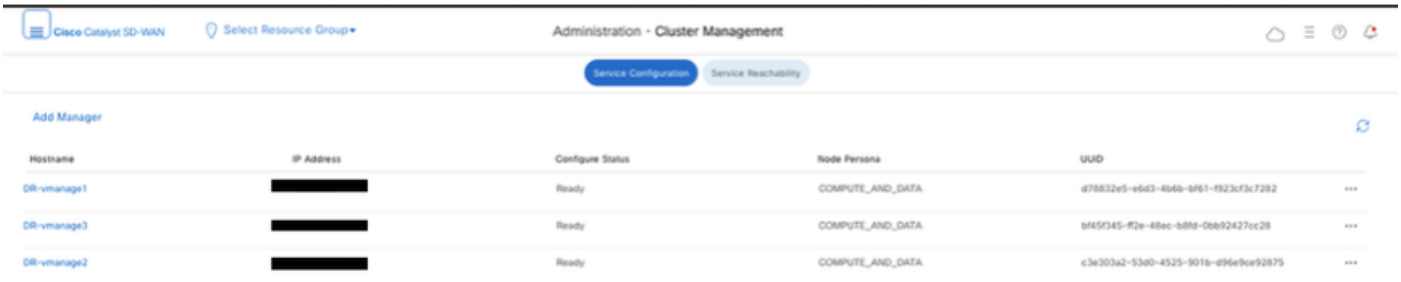
I due cluster a 3 nodi separati sono già stati creati, presupponendo che ciascun gestore SD-WAN disponga della configurazione minima e che la parte di certificazione sia stata completata.

Passare a Amministrazione > Gestione cluster in entrambi i cluster e verificare che tutti i nodi siano in stato Pronto.

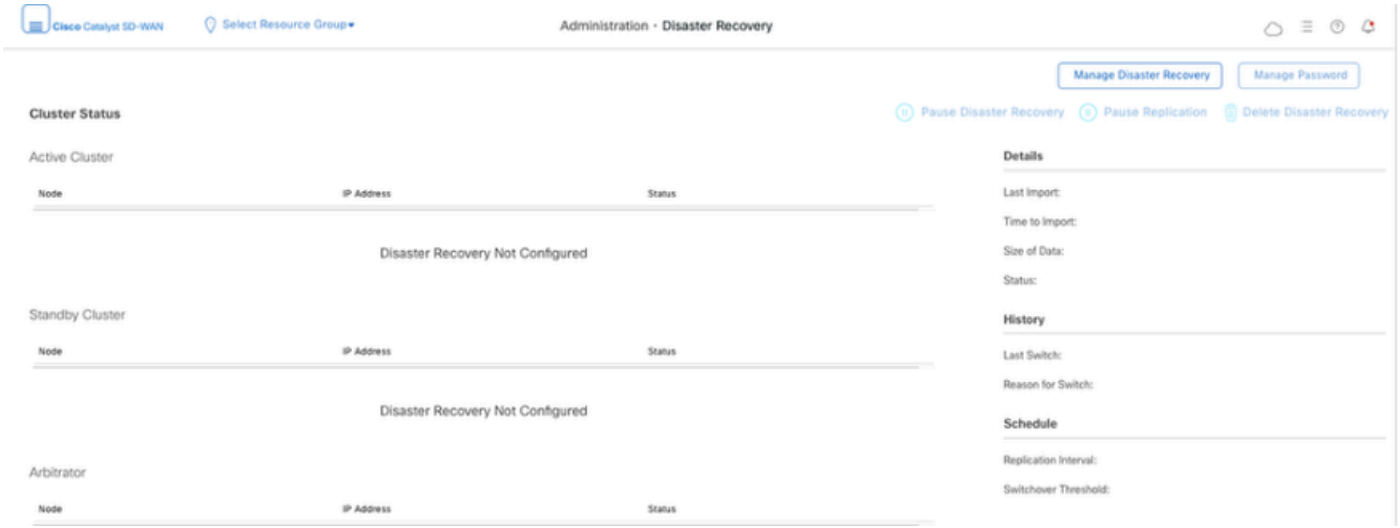
DC vManage



DR Manage



Passare a Amministrazione>Ripristino di emergenza del cluster vManage principale. Fare clic su Gestione ripristino di emergenza.



Nella finestra popup, immettere i dettagli per vManage principale e secondario.

Gli indirizzi IP da indicare sono gli indirizzi IP delle interfacce cluster fuori banda. È preferibile utilizzare l'indirizzo IP dell'interfaccia di servizio VPN 0 di vManage-1 in ogni cluster.

Le credenziali devono essere quelle di un utente netadmin e non devono essere modificate una volta configurato il DR, a meno che non venga eliminato. È possibile utilizzare una credenziale utente locale vManage separata per il ripristino di emergenza. È necessario verificare che l'utente locale vManage faccia parte del gruppo netadmin. È possibile utilizzare anche le credenziali di amministratore.

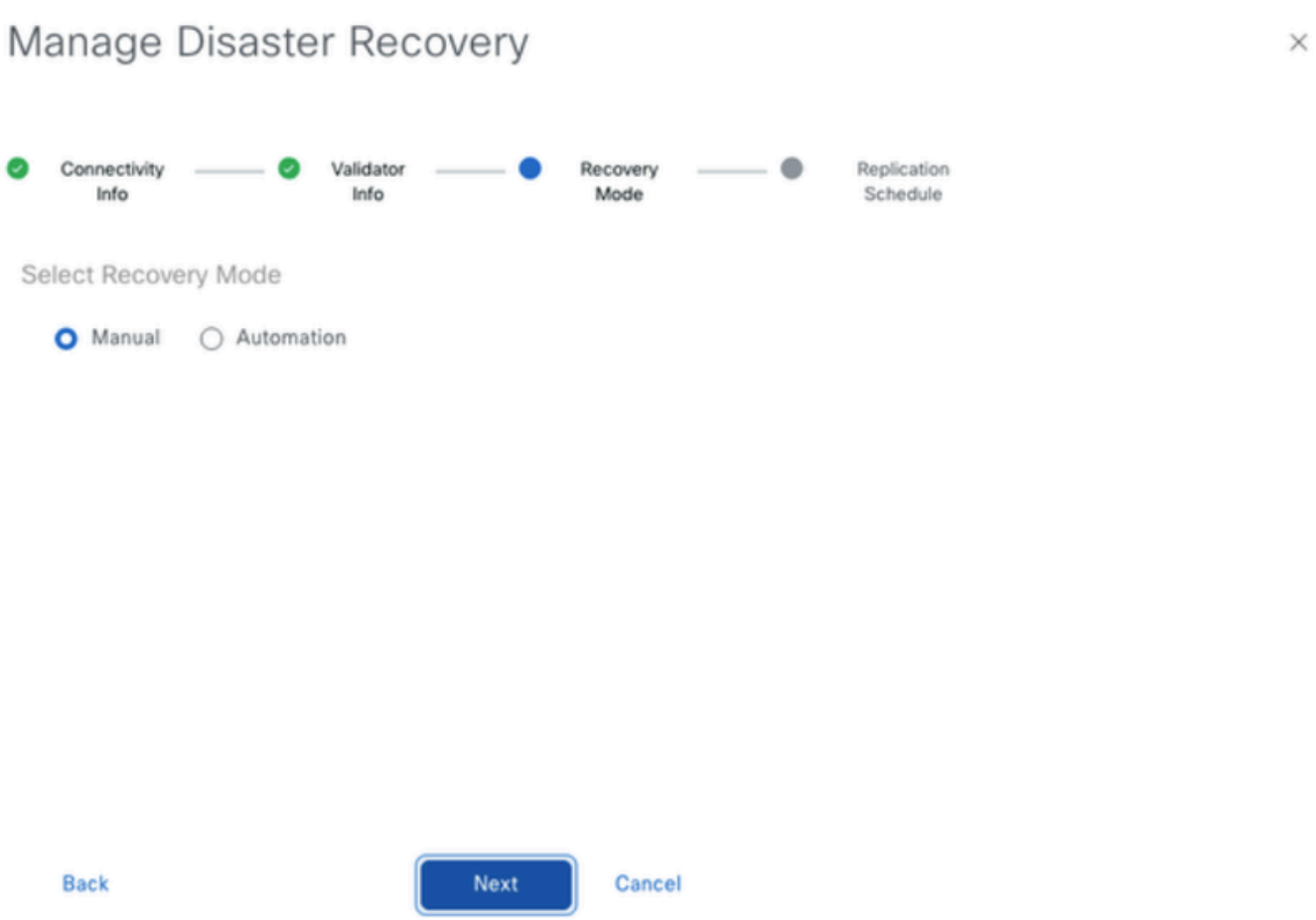
Una volta completate le impostazioni, fare clic su Avanti.

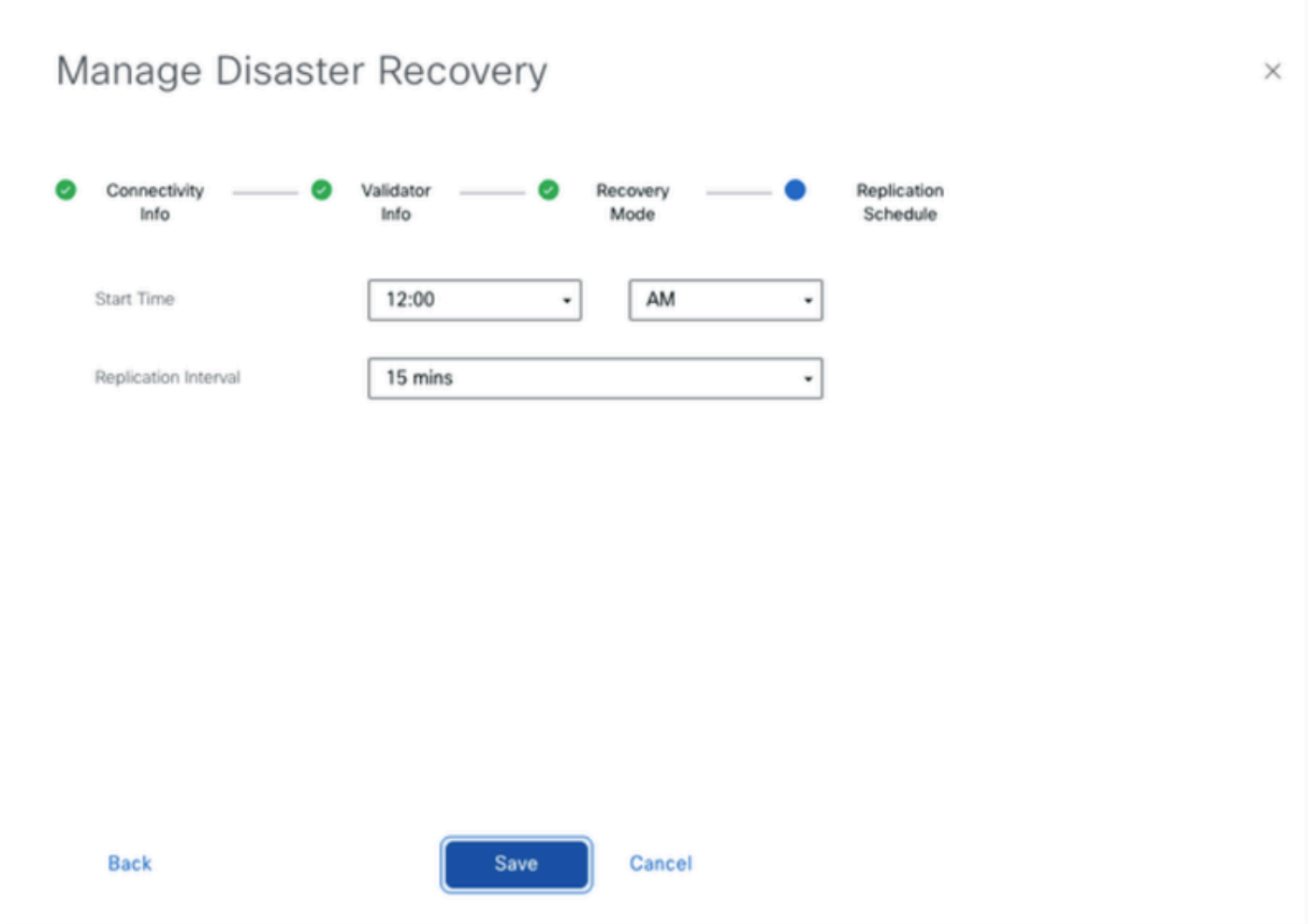
- Specificare i dettagli dei controller vBond.

I controller vBond devono essere raggiungibili nell'indirizzo IP specificato tramite Netconf.

Una volta completate le impostazioni, fare clic su Avanti.

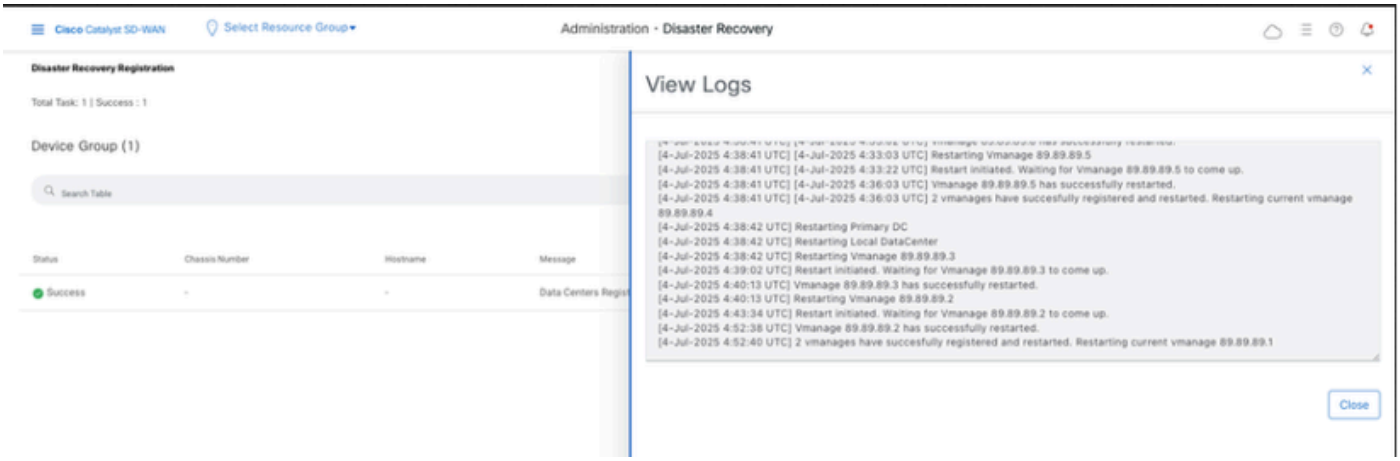
- In Modalità di ripristino, scegliere Manuale. La modalità di automazione è deprecata. Fare clic su Next (Avanti).


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



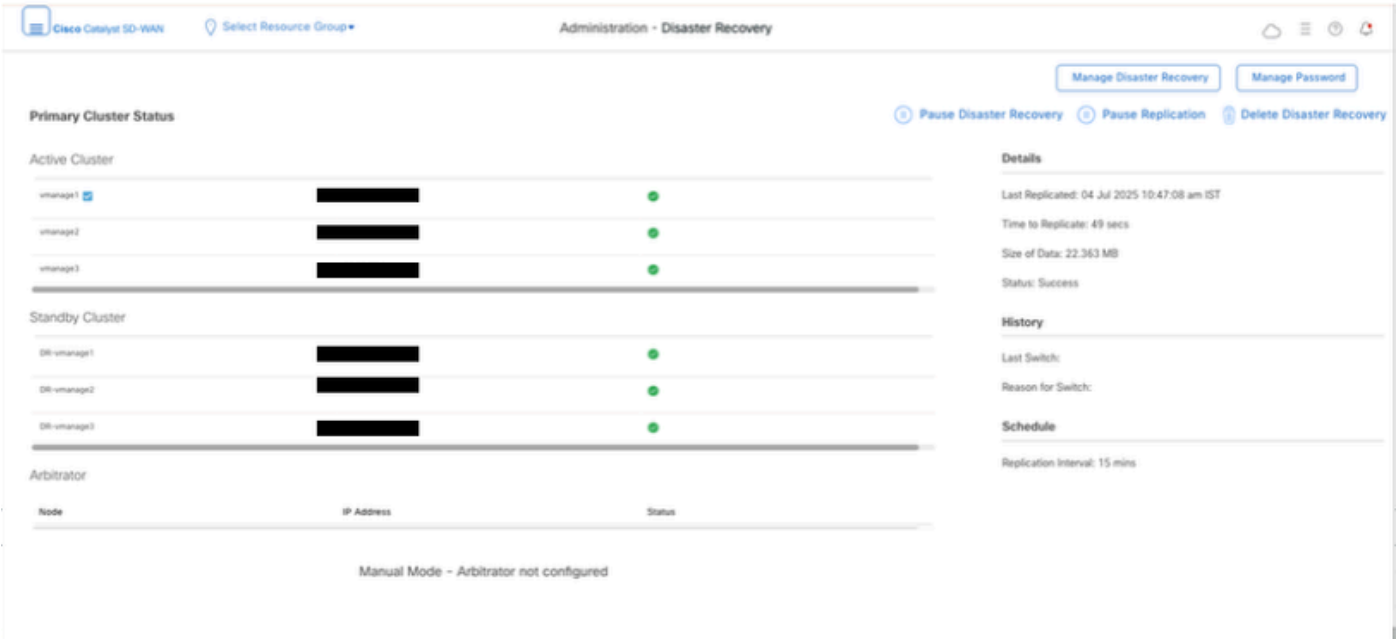
Impostare il valore e fare clic su Salva.

- La registrazione del ripristino di emergenza inizia ora. Fare clic sul pulsante Aggiorna per aggiornare manualmente lo stato e i registri di stato. Questo processo può richiedere fino a 20-30 minuti.



Verifica

Passare a Amministrazione>Disaster Recovery per verificare lo stato di Disaster Recovery e la data dell'ultima replica dei dati.



Nota: La replica può richiedere diverse ore a seconda delle dimensioni del database. Inoltre, può richiedere alcuni cicli per ottenere una replica corretta.

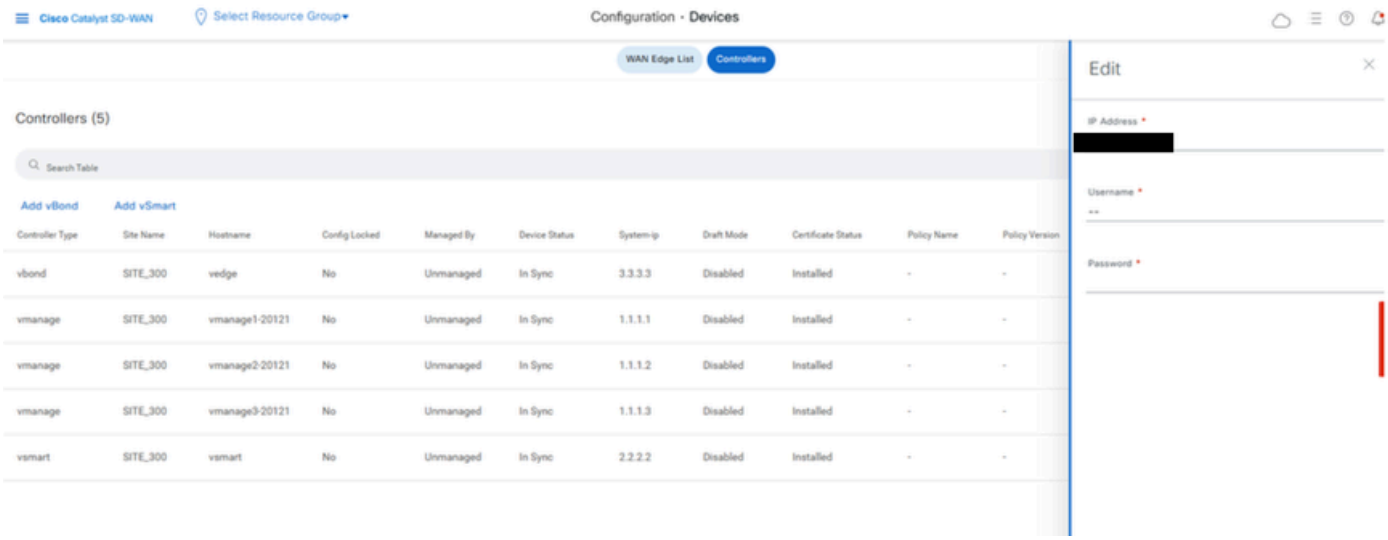
Passaggio 6: Riautenticazione dei controller e annullamento della convalida dei controller precedenti

Una volta ripristinato il database di configurazione, è necessario riautenticare tutti i nuovi controller (manage/vsmart/vbond) nel fabric

Nota: nella produzione effettiva, se l'IP dell'interfaccia utilizzato per la riautenticazione è l'IP dell'interfaccia del tunnel, è necessario garantire che il servizio NETCONF sia consentito sull'interfaccia del tunnel di vManage, vSmart e vBond e anche sui firewall lungo il percorso. La porta firewall da aprire è la porta TCP 830 come regola bidirezionale dal cluster DR a tutti i vBonds e vSmarts.

Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller

- Fare clic sui tre punti accanto a ciascun controller e scegliere Modifica



- Sostituire l'indirizzo ip (ip di sistema del controller) con l'indirizzo ip vpn 0 (interfaccia tunnel) del trasporto. Immettere il nome utente e la password e fare clic su Salva
- Eseguire la stessa operazione per tutti i nuovi controller nel fabric

Sincronizza la catena di certificati radice

Una volta caricati tutti i controller, attenersi a questa procedura:

Su qualsiasi server Cisco SD-WAN Manager nel cluster appena attivo, eseguire le seguenti azioni:

Immettere questo comando per sincronizzare il certificato radice con tutti i dispositivi Cisco Catalyst SD-WAN nel cluster appena attivo:

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

Immettere questo comando per sincronizzare l'UUID di Cisco SD-WAN Manager con Cisco SD-WAN Validator:

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

Una volta ripristinata la struttura e attivate le sessioni bfd e di controllo per tutti i bordi e i controller della struttura, è necessario invalidare i vecchi controller (vmanage/vsmart/vbond) dall'interfaccia utente

- Su vmanage UI, fare clic su Configurazione > Dispositivi > Certificati
- Fare clic su Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su invalida
- Fare clic su Invia a vbond
- Su gestisci interfaccia utente, fare clic su Configurazione > Dispositivi > Controller
- Fare clic sui tre punti vicino al controller (vmanage/vsmart/vbond) del vecchio fabric. Fare clic su Elimina

Registra assegni

Questi controlli successivi si applicano a tutte le combinazioni di distribuzione.

Riattiva router cloud Edge:

- Se C8000v fa parte della sovrapposizione e ha firmato gestito, è necessario riautenticarli, ovvero:

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

        token
```

- Conferma connessioni di controllo e sessioni DCF attive
- Confermare il flusso del traffico dell'applicazione da un'estremità all'altra
- Se le modifiche sono state apportate alla porta-hop prima della ricostruzione del fabric sui bordi, è necessario annullarle
- Verificare che gli elementi vengano visualizzati come previsto:
    - Modelli
    - Politiche
    - Pagina Dispositivo (entrambe le schede)WAN vEdge ListandController

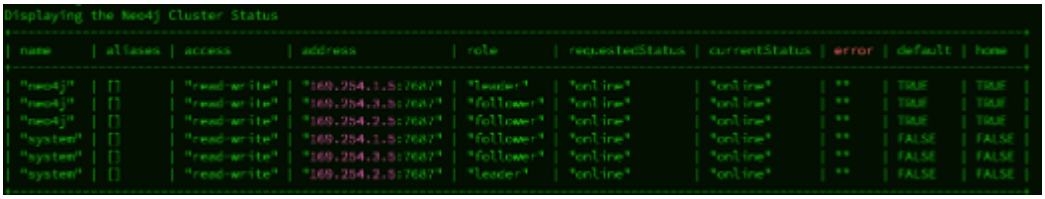
  vManage - controlli post

- Applicabile per i nodi vManage:

  Controlli di Configuration-DB(Neo4j):

  Eseguire il comando "request nms configuration-db diagnostics" su tutti i nodi vManage:

  1. Verificare lo stato online e di leadership del nodo (non disponibile per tutte le versioni):



"Neo4j" deve mostrare 3 nodi online e 1 leader e 2 follower. "system" deve anche mostrare 3 nodi online e 1 leader e 2 follower, tuttavia, poiché questo non è il Db predefinito, il flag predefinito è false. Se in ogni neo4j sono presenti meno di 3 voci e il sistema significa che il nodo è stato disattivato dal cluster. Per risolvere lo stesso problema, contattare Cisco TAC.

2. Verificare se un nodo è in "quarantena".

```
##############################################
##############################################
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
##############################################
```

Nessuno dei nodi deve essere in stato di quarantena.

3. La convalida dello schema deve avere esito positivo.

```
##########################################
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. Raccogliere un backup di configuration-db utilizzando il comando "request nms configuration-db diagnostics" e assicurarsi che abbia esito positivo.

```
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#
```

In caso di incoerenze o errori, rivolgersi a Cisco TAC per la risoluzione dei problemi.

In alternativa, è possibile eseguire queste chiamate API per confermare lo stato di gestione del nodo per un cluster (per tutti i nodi COMPUTE+DATA). Funziona solo nella versione 20.12 e successive

```
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
```

Assicurarsi che in un cluster sia presente un solo leader sia per neo4j che per system e rest come follower. Assicurarsi che tutti i nodi siano online. Se si dispone di un cluster a 3 nodi (tutti e tre sono COMPUTE+DATA), deve esistere un solo leader sia per neo4j che per system. Qualsiasi deviazione, è necessario contattare TAC

5. Verificare se in /var/log/kern.log si sono verificati errori di I/O, Mem e del disco. È necessario controllare questa impostazione su tutti i nodi vManage.

6.Controllare la fase quando si crea un nuovo cluster per vmanage che non dispone di CC tra ciascun nodo
Eseguire ssh come manage-admin dal nodo 1 agli altri nodi IP del cluster e viceversa, per verificare se la chiave pubblica è stata scambiata e se il protocollo ssh senza password funziona [il token di consenso è richiesto per i passaggi illustrati]

```
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:
```

Se il risultato chiede di immettere la password, contattare TAC

Controlli post controller:

Applicabile a tutti i controller SD-WAN (vBond, vManage, vSmart):

Eseguire i comandi su tutti i controller nella sovrapposizione e verificare che l'UUID vManage e i numeri di serie rilevati siano validi per l'infrastruttura corrente:

Comandi vBond:

show orchestrator valid-vsmarts

show orchestrator valid-manage-id

Comandi vManage/vSmart:

show control valid-vsmarts

show control valid-manage-id

Si noti l'output di show control valid-vsmarts include i numeri di serie dei nodi vSmarts e vManage.

Confrontare questo valore con quelli visualizzati nell'interfaccia utente di vManage. Passare alla sezione Configurazione > Certificati > Controller.

Se vengono rilevate voci aggiuntive per l'UUID o il numero di serie che non sono attualmente presenti nell'infrastruttura, è necessario eliminarle. A tal fine, è possibile contattare Cisco TAC.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).