重建Catalyst SD-WAN交換矩陣

目錄

簡介

本文檔介紹如何重建Cisco SD-WAN交換矩陣，包括備份和恢復各種部署的控制器配置。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- Cisco Software Central
- 從software.cisco.com下載控制器軟體

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

重建交換矩陣之前的先決條件

- 必須為控制器的新交換矩陣配置一組新的系統IPS、站點ID
- 確保防火牆規則到位，以啟用控制器與邊緣之間的通訊
- 請注意neo4j(configuration-db)使用者名稱和密碼（在群集中的所有vManage節點上必須相同）
- 在所有邊緣上禁用埠躍點
- 將正常重啟計時器增加至7天
- 在遷移前清除三方工具中的警報
- 除非預先設定將統計資訊匯出到外部伺服器（如asvAnalytics），否則歷史統計資訊（警報、事件、裝置統計資訊等）將會丟失
- 如果配置了Cloud OnRamp，請確保您在本練習開始之前能夠訪問在雲中部署的c8000v
- 如果在舊交換矩陣上啟用了SDAVC，請確保新交換矩陣已啟用（對於集群，只需在單個節點上啟用）
- 僅在與原始交換矩陣相同的版本上支援Configuration-db恢復

- 確認用於控制器的角色。我們支援COMPUTE_DATA和DATA角色（每個部分下的詳細資訊）
- 對於企業CA，需要使用由企業CA頒發的根證書（該證書用於現有重疊中），並且證書使用企業CA伺服器簽名並通過UI為所有控制器安裝

部署選項

vManage部署

- 獨立（1個節點）
- 集群（3節點或6節點）

DR選項

- 無DR
- 單節點DR
- 備用DR群集（手動/管理觸發）

附註：有關災難恢復型別的更多詳細資訊，請參閱此連結

組合：

#	vManage設定	DR選項
1	獨立（1個節點）	無DR
2	獨立（1個節點）	單節點DR
3	集群（3節點或6節點）	無DR
4	集群（3節點或6節點）	備用DR群集

適用於所有組合的常見步驟

這些步驟對所有部署組合都是通用的。它們涵蓋啟動VM例項和應用基本CLI配置的過程。每個組合部分都會告訴您要部署的例項數以及要完成的其他步驟。

安裝並啟動SD-WAN控制器（管理器、驗證器、控制器）

附註：思科重新命名了某些術語，因此這些術語可以互換。Cisco vManage = Cisco Catalyst Manager、Cisco vBond = Cisco Catalyst Validator、Cisco vSmart = Cisco Catalyst Controller

---

從思科軟體下載頁面下載SD-WAN控制器的OVA檔案：

- 選擇vEDGE Cloud，然後下載所需軟體版本的vBond OVA。
- 選擇vManage軟體並下載所需軟體版本的vManage OVA。
- 選擇vSmart軟體並下載所需軟體版本的vSmart OVA。

附註：在ESXi/雲平台上使用OVA檔案啟動vSmart、vBond和vManage控制器。請參閱連結的文檔，並確保根據SD-WAN部署型別為所有控制器分配了足夠的CPU、RAM和磁碟。導航到此處以獲取其他資訊。請確保將輔助磁碟分配給vManage節點，如連結計算指南的「儲存大小*」列中所述。

啟動Cisco Manager節點

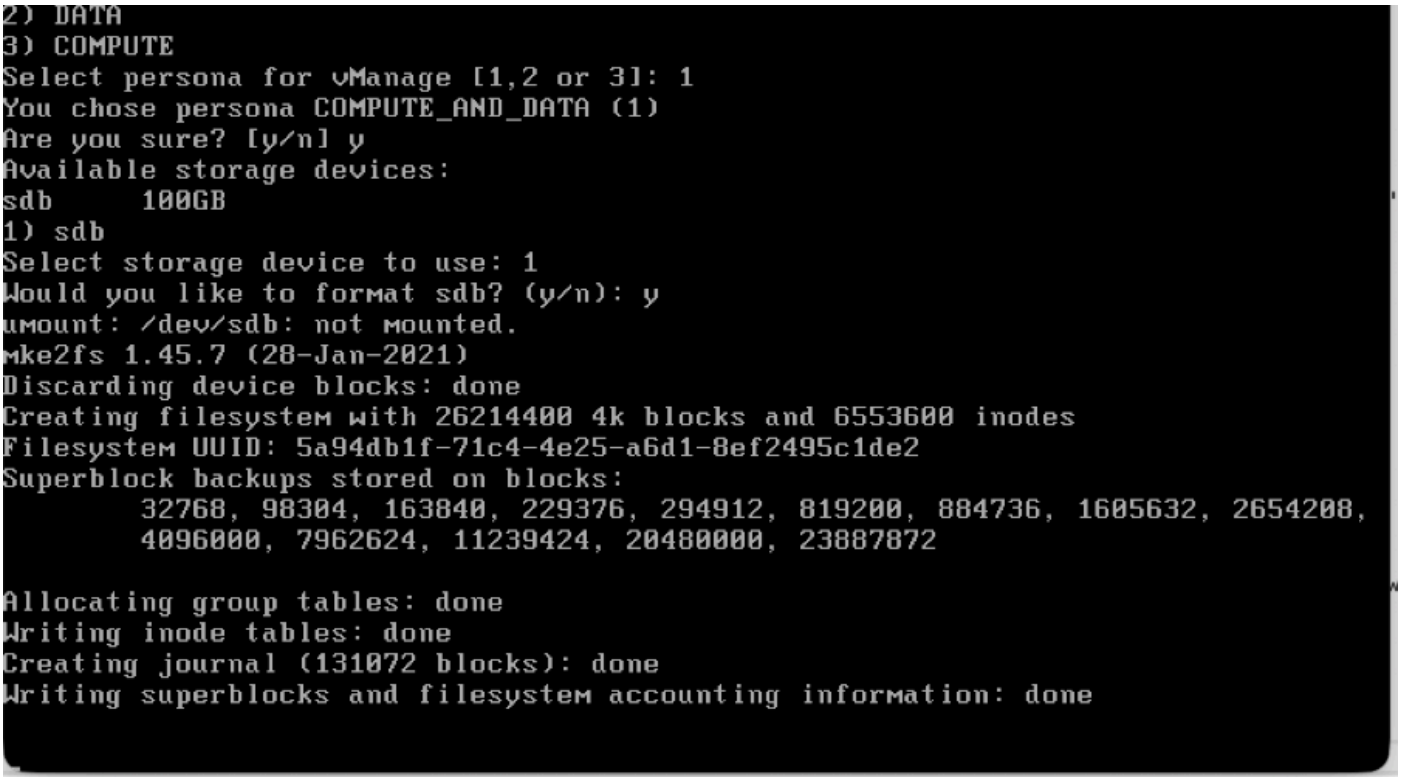
- 部署Cisco Manager或vManage VM且可以訪問Manager的控制檯後，等待啟動完成。一個指示是，我們看到消息系統已準備就緒，並提示輸入使用者名稱和密碼。
- 輸入默認使用者憑據使用者名稱admin和密碼admin。發佈它提示使用者更改密碼，根據您的選擇設定使用者admin所需的密碼。
- 然後提示使用者選擇角色。如果希望擁有vManage集群，則這是關鍵步驟。請根據此處顯示的場景選擇角色：

```
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
```

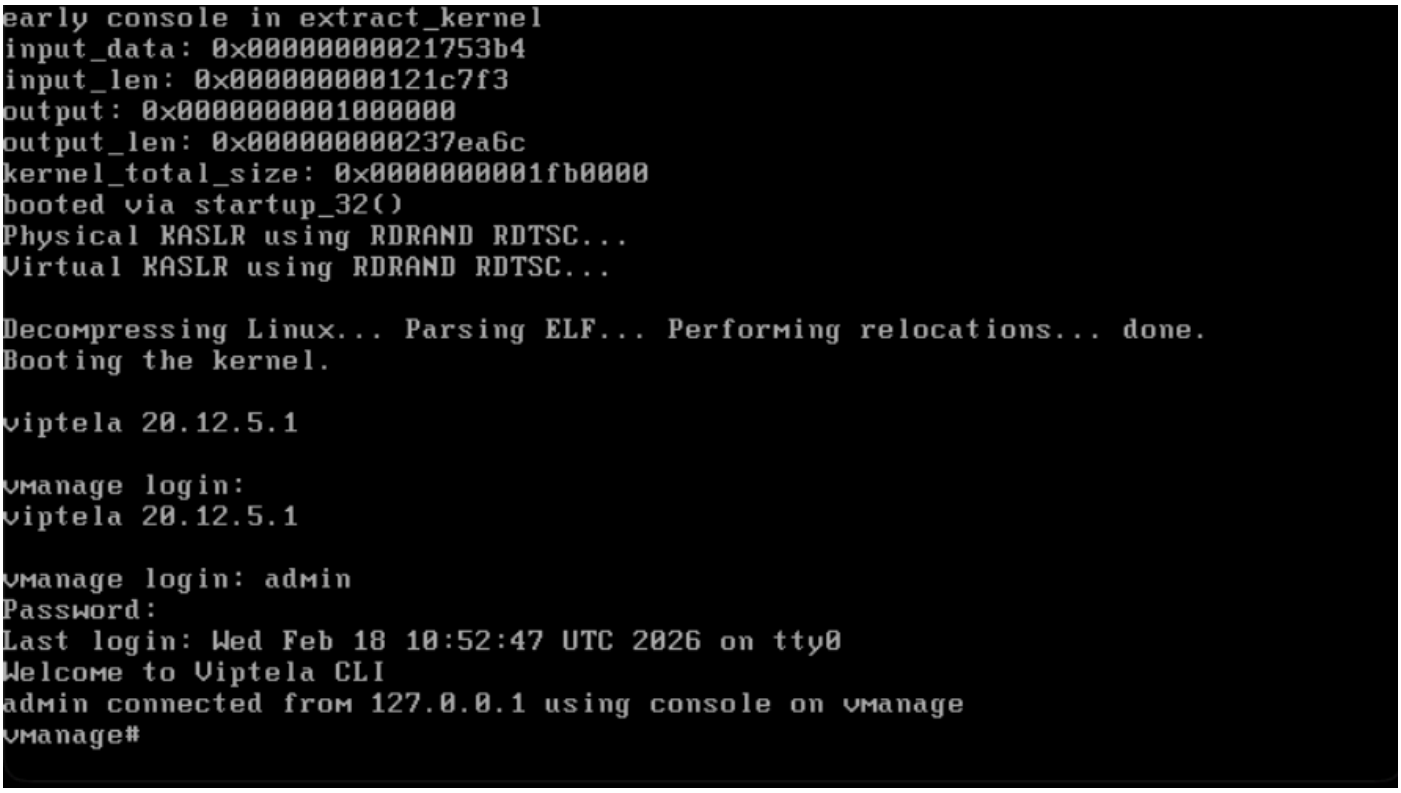
示例：為COMPUTE_AND_DATA選擇1

```
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:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
You must set an initial admin password different from default password.
Password:
Re-enter password:
1) COMPUTE_AND_DATA
2) DATA
3) COMPUTE
Select persona for vManage [1,2 or 3]: 1
You chose persona COMPUTE_AND_DATA (1)
Are you sure? [y/n] _
```

選擇輔助磁碟，如下所示：



- 選擇輔助磁碟並鍵入Y進行確認。
- Cisco Manager重新載入。啟動後，使用新配置的新密碼輸入使用者名稱和密碼。



- 您可以配置VPN 512 management interface以啟用對控制器的帶外管理訪問。
- 使用命令show interface |選項卡，用於檢查介面當前對映到的VPN。
- 相應地配置介面。

範例

```
                                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#
```

附註：您可以在此處參考現有vManage的配置並配置相同的IP地址方案。

管理介面(VPN 512)配置

- 如果需要將介面從VPN 0移動到VPN 512，請使用這些命令，然後配置介面上的IP地址

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




  no shutdown
 !
 ip route 0.0.0.0/0



!
```

啟動驗證器

- 在hypervisor上，為vBond節點配置所需的計算（CPU、RAM和磁碟）並開啟電源。
- 一旦控制檯可以訪問，請等待vBond完全啟動。等待出現「System Ready（系統就緒）」資訊。
- 然後系統提示輸入使用者名稱和密碼。輸入預設使用者憑據使用者名稱admin和密碼admin。在此之後，系統會提示使用者更改密碼，並根據您的選擇設定使用者admin所需的密碼。
- 您可以配置VPN 512管理介面以啟用對控制器的帶外管理訪問。
- 使用命令show interface |選項卡，用於檢查介面當前對映到的VPN。
- 相應地配置介面。

範例：

```
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#
```

附註：您可以從現有vBond中引用配置，並在此處配置相同的配置。

管理介面(VPN 512)配置

- 如果需要將介面從VPN 0移動到VPN 512，請使用這些命令，然後配置介面上的IP地址。

```
Conf t
vpn 0
```

```
 no interface eth0
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
commit
```

啟動控制器(vSmart)節點

- 執行與驗證程式相同的步驟以啟動vSmart節點。
- 在所有SD-WAN控制器上配置VPN 512 IP地址後，即可使用VPN 512 IP地址上的SSH訪問它們。

所有控制器上的基本CLI配置

一旦您對所有控制器具有SSH訪問許可權，請在每個控制器上配置這些CLI配置。

系統配置

```
config t
system
 host-name




 system-ip




 site-id




 organization-name
```

```
 vbond



commit
```

注意:如果使用URL作為vBond地址，請確保在VPN 0配置中配置DNS伺服器IP地址或確保可以解析這些地址。

傳輸介面(VPN 0)配置

所有控制器上都需要這些配置，才能啟用傳輸介面，該介面用於與路由器和其餘控制器建立控制連線。

```
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
```

注意：您可以參考現有控制器的配置，如果配置存在，則您可以將此配置新增到新控制器。

僅當需要路由器使用TLS與vManage節點建立安全控制連線時，才將控制協定配置為TLS。預設情況下，所有控制器和路由器都使用DTLS建立控制連接。根據您的要求，此可選配置僅在vSmart和vManage節點上需要。

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

組合1:獨立vManage +無DR

所需例項：

- 1個vManage(COMPUTE_AND_DATA)
- 1個或多個vBond
- 1個或多個vSmart

步驟:

1. 使用通用步驟調出所有例項
2. 預先檢查
3. 配置vManage UI、證書和板載控制器
4. Config-db backup/restore
5. 過帳支票

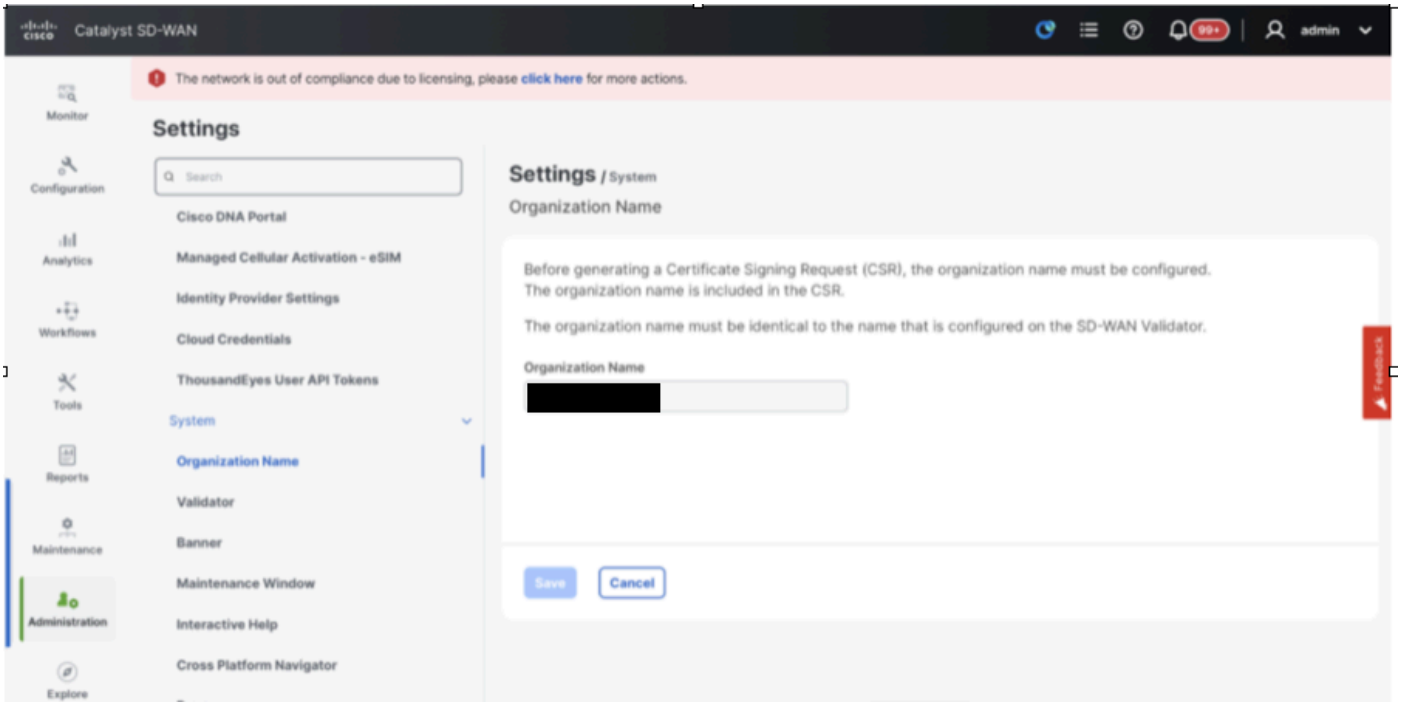
步驟 1:預先檢查

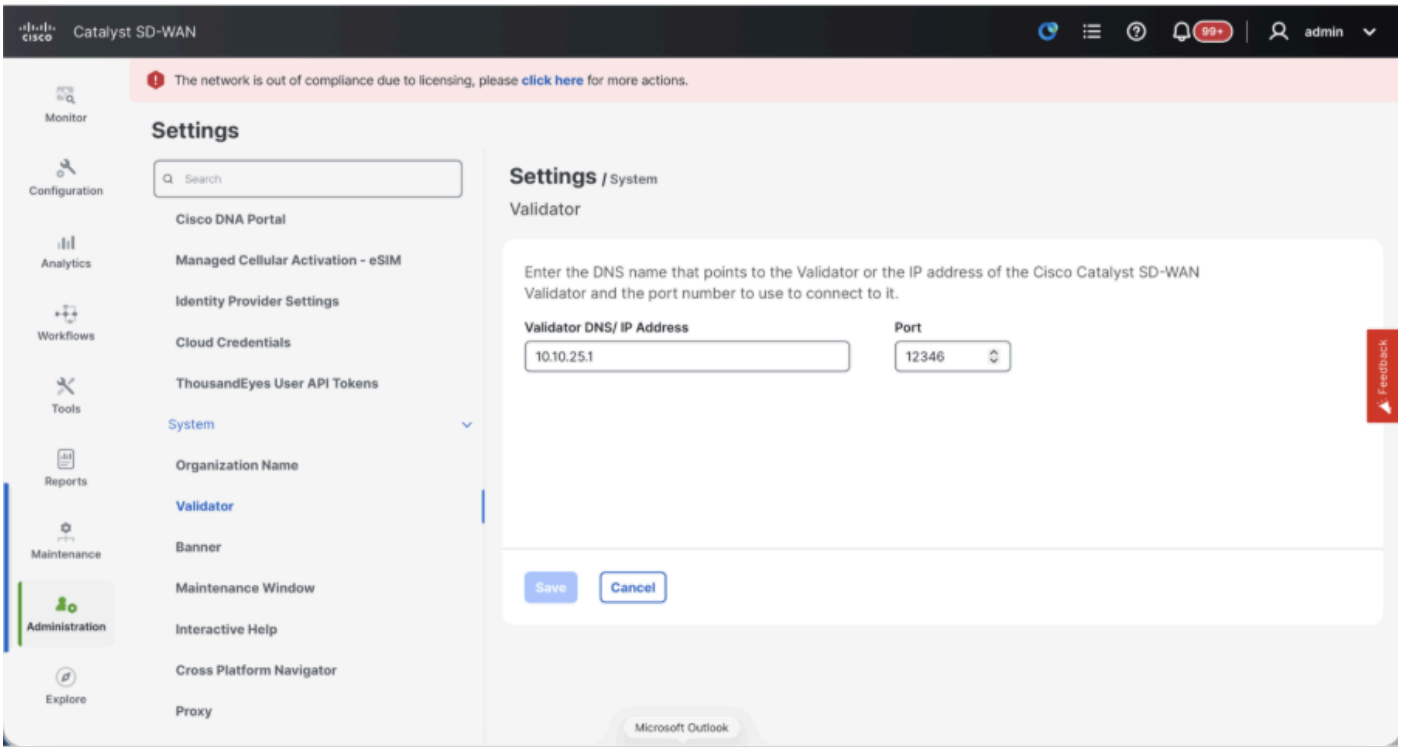
- 確保活動的Cisco SD-WAN Manager例項數與新安裝的Cisco SD-WAN Manager實例數相同。
- 確保所有活動的和新的Cisco SD-WAN Manager例項運行相同的軟體版本。
- 確保所有活動的和新的Cisco SD-WAN Manager例項都能到達Cisco SD-WAN Validator的管理IP地址。
- 確保證書已安裝在新安裝的Cisco SD-WAN Manager例項上。
- 確保所有Cisco Catalyst SD-WAN 裝置(包括新安裝的Cisco SD-WAN Manager例項)上的時鐘都同步。
- 確保在新安裝的Cisco SD-WAN Manager例項上配置一組新的系統IP和站點ID，並與活動群集配置相同的基本配置。

步驟 2:配置vManage UI、證書和板載控制器

更新vManage UI上的配置

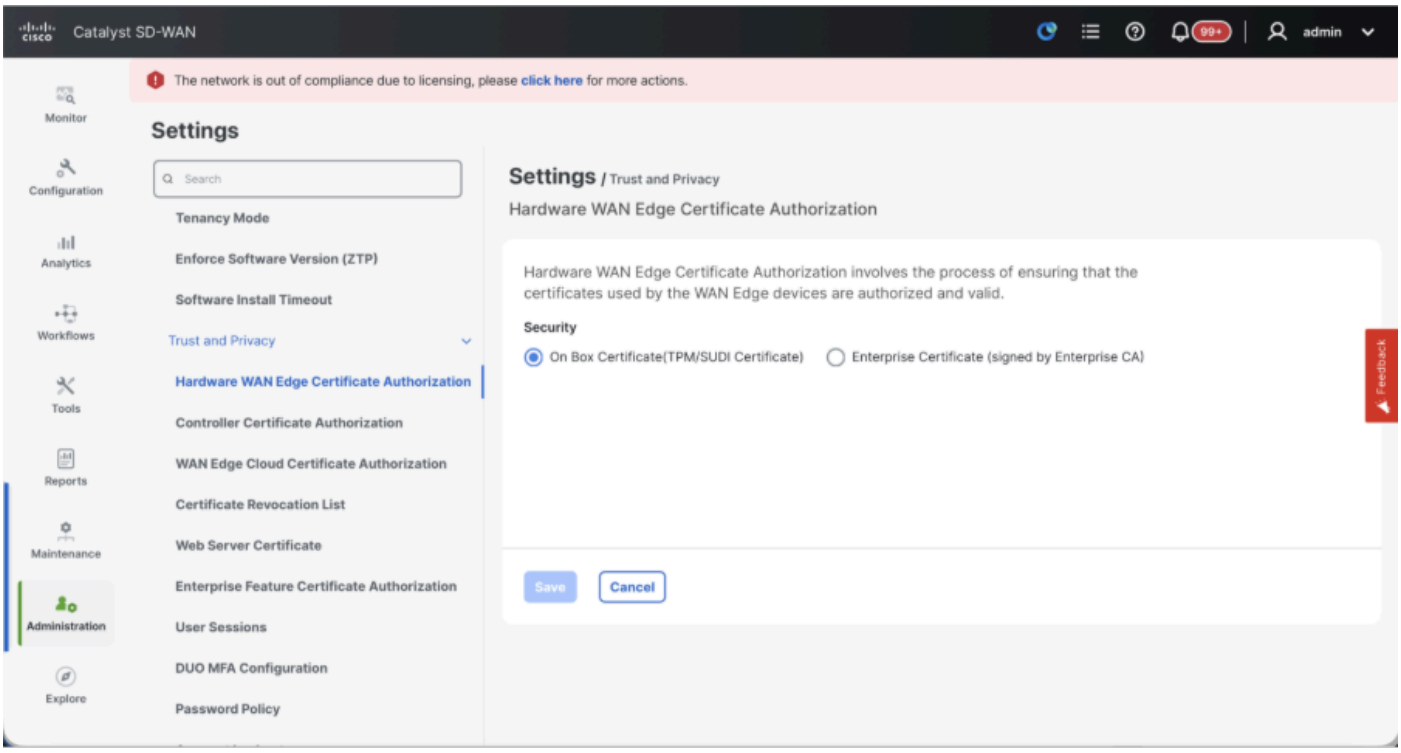
- 將步驟1中的組態新增到所有控制器的CLI上後，我們可以使用瀏覽器中的https://<vmanage-ip>URL存取vManage的WebUI。使用各個vManage節點的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 導覽至Administration > Settings，然後完成以下步驟。
- 配置組織名稱和驗證器/vBond URL/IP地址。配置與vManage節點的CLI中相同的值。
- 在vManage 20.15/20.18中，這些配置可在System部分中找到。



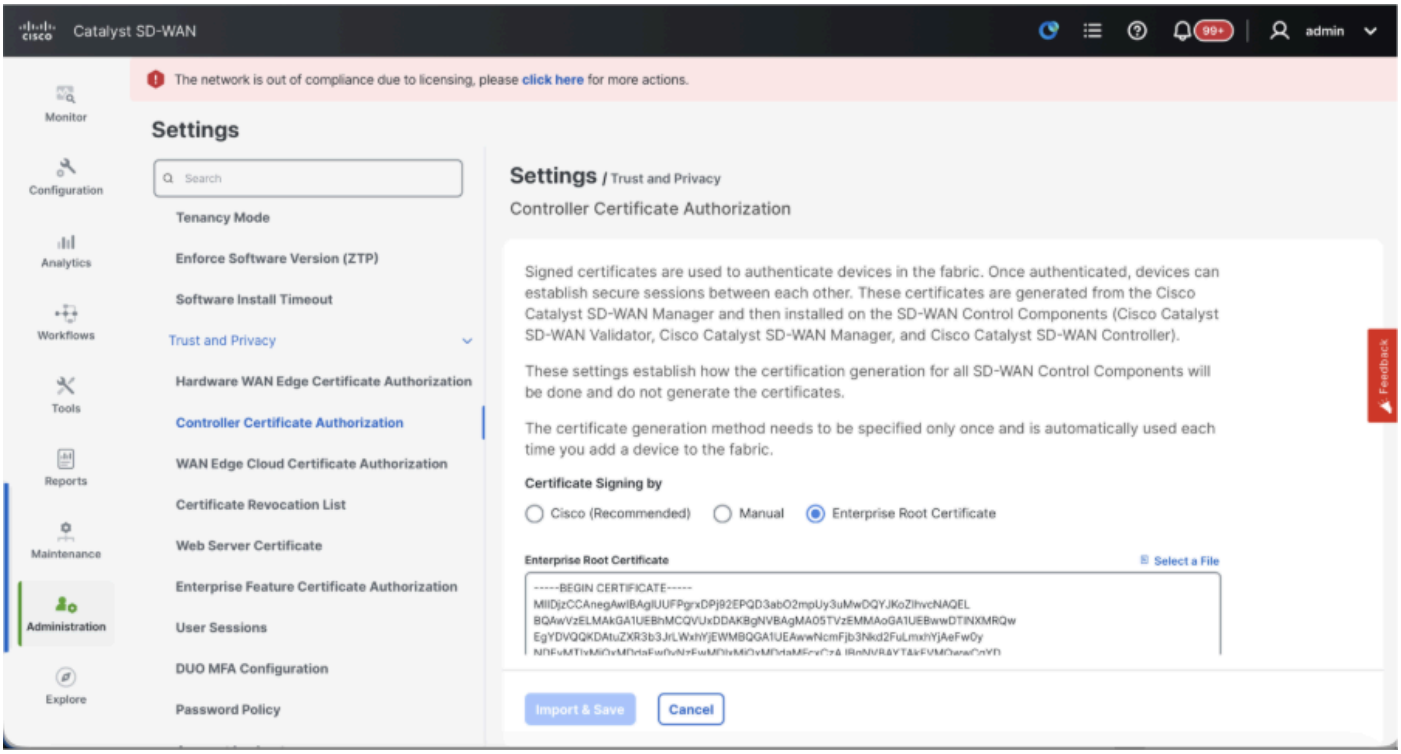


- 驗證證書授權(CA)的配置，CA決定用於簽署證書的證書授權。我們可以看到3個選項：

1. 硬體WAN邊緣證書授權 — 決定硬體SD-WAN邊緣路由器的CA。
    - 開箱證書（TPM/SUDI證書） — 使用此選項，路由器硬體上預安裝的證書用於建立控制連線（TLS/DTLS連線）
    - 企業證書（由企業CA簽署） — 使用此選項時，路由器使用由組織的企業證書頒發機構簽署的證書。選擇此選項時，必須在此處更新企業CA的根證書。



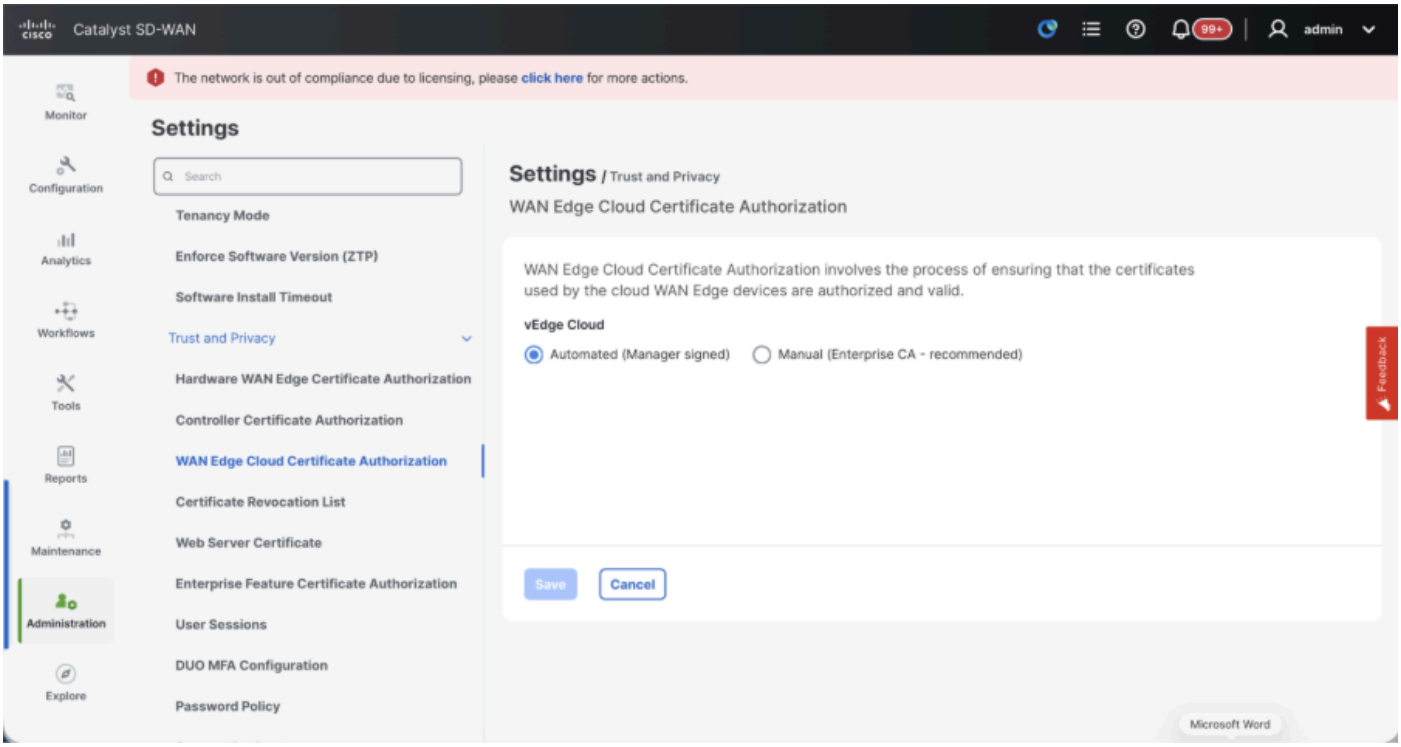
2. Controller Certificate Authorization — 決定SD-WAN控制器的CA。
   - 思科（推薦） — 控制器使用由Cisco PKI簽名的證書。vManage使用vManage上配置的智慧帳戶憑據自動聯絡PNP門戶，並簽署證書並將其安裝在控制器上。
   - 手動 — 控制器使用由Cisco PKI簽名的證書。導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
   - Enterprise Root Certificate — 使用此選項時，路由器使用由您組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。



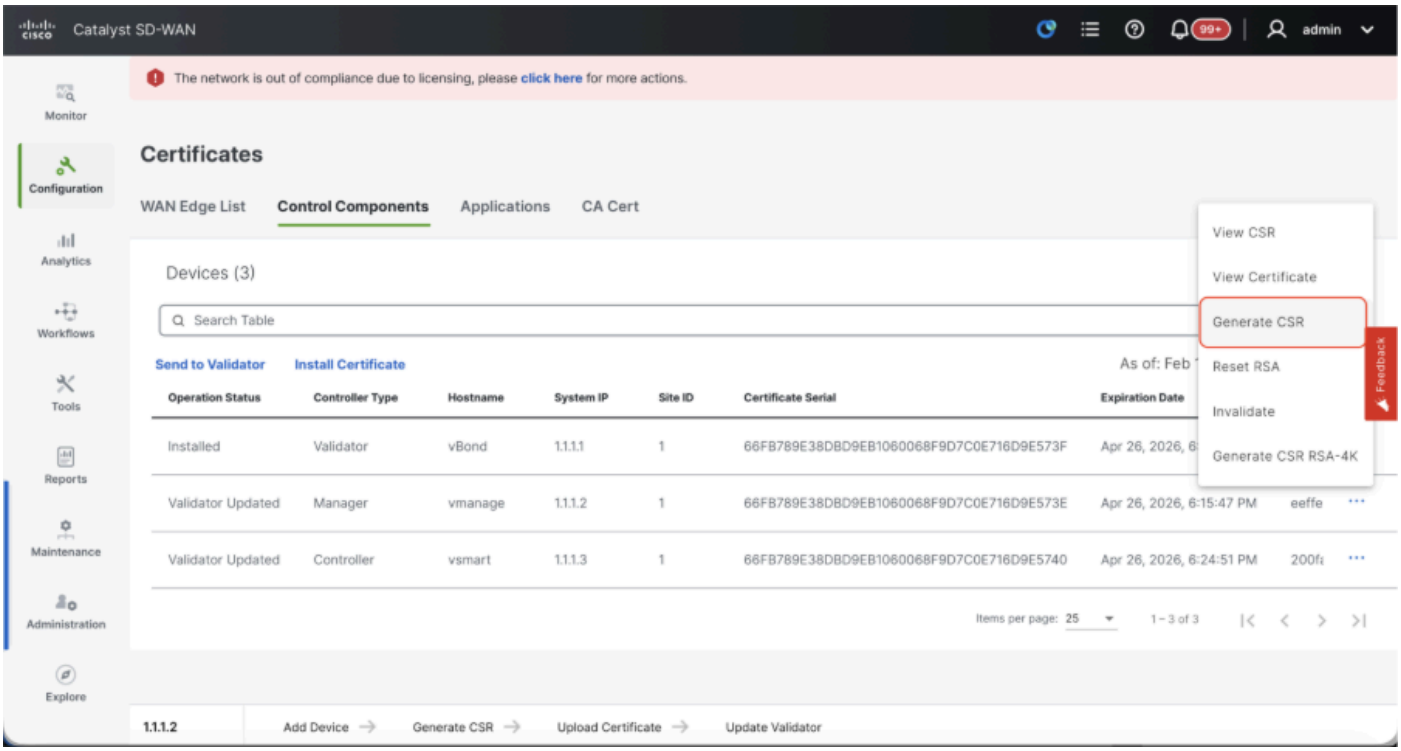
3. WAN邊緣雲證書授權 — 確定虛擬SD-WAN邊緣路由器（CSR1000v、C8000v、vEdge雲）的CA

- 自動（vManage簽名） — vManage自動對虛擬邊緣路由器的CSR進行簽名，並在路由器上安裝證書。
- 手動（企業CA — 推薦） — 虛擬路由器使用由組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。

如果使用CA（企業證書頒發機構），請選擇Enterprise。



- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers
- 點選Manager/vManage的……並點選Generate CSR。



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。

將vBond/Validator和vSmart/Controller註冊到vManage

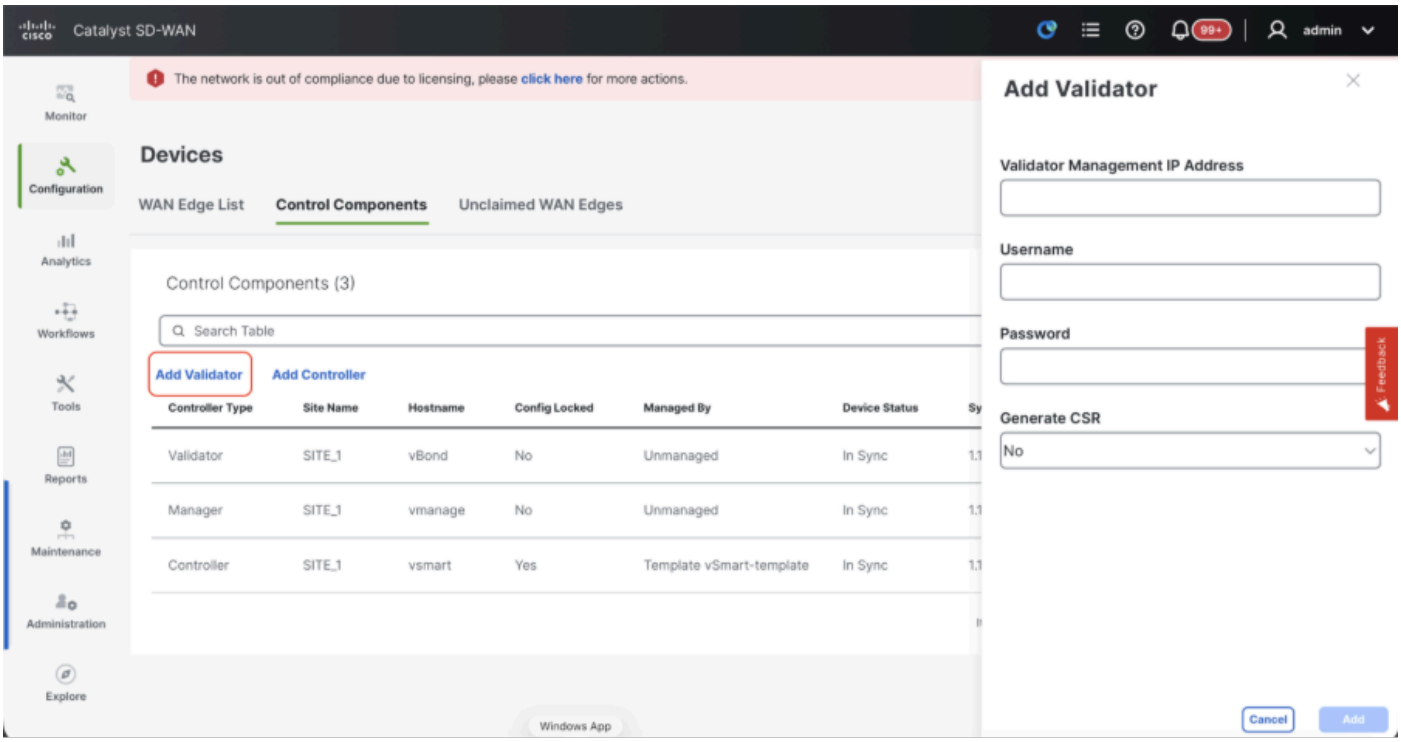
如果是20.15/20.18 vManage節點，請導航到Configuration > Devices > Control Components。在20.9/20.12版本的情況下，Configuration > Devices > Controllers

OnboardingvBond/驗證器

- 按一下AddvBond在20.12vManageor的情況下新增驗證程式在20.15/20.18 vManage的情況下。系統開啟一個彈出視窗，輸入 從vManage可訪問的vBond的VPN 0傳輸IP。
- 如果允許，請從vManagetovBondIP的CLI使用ping檢查可連接性。
- 輸入vBond的使用者憑據。

注意:我們需要使用vBondor的admin憑據作為netadmingroup的使用者部分。您可以在vBond的CLI中驗證這一點。如需安裝vBond的新憑證，請在「產生CSR」下拉式清單中選擇「是」。

附註：如果vBond位於NAT裝置/防火牆之後，請檢查vBond VPN 0介面IP是否已轉換為公共IP。如果無法從vManage訪問VPN 0介面IP，則在此步驟中使用VPN 0介面的公用IP地址。

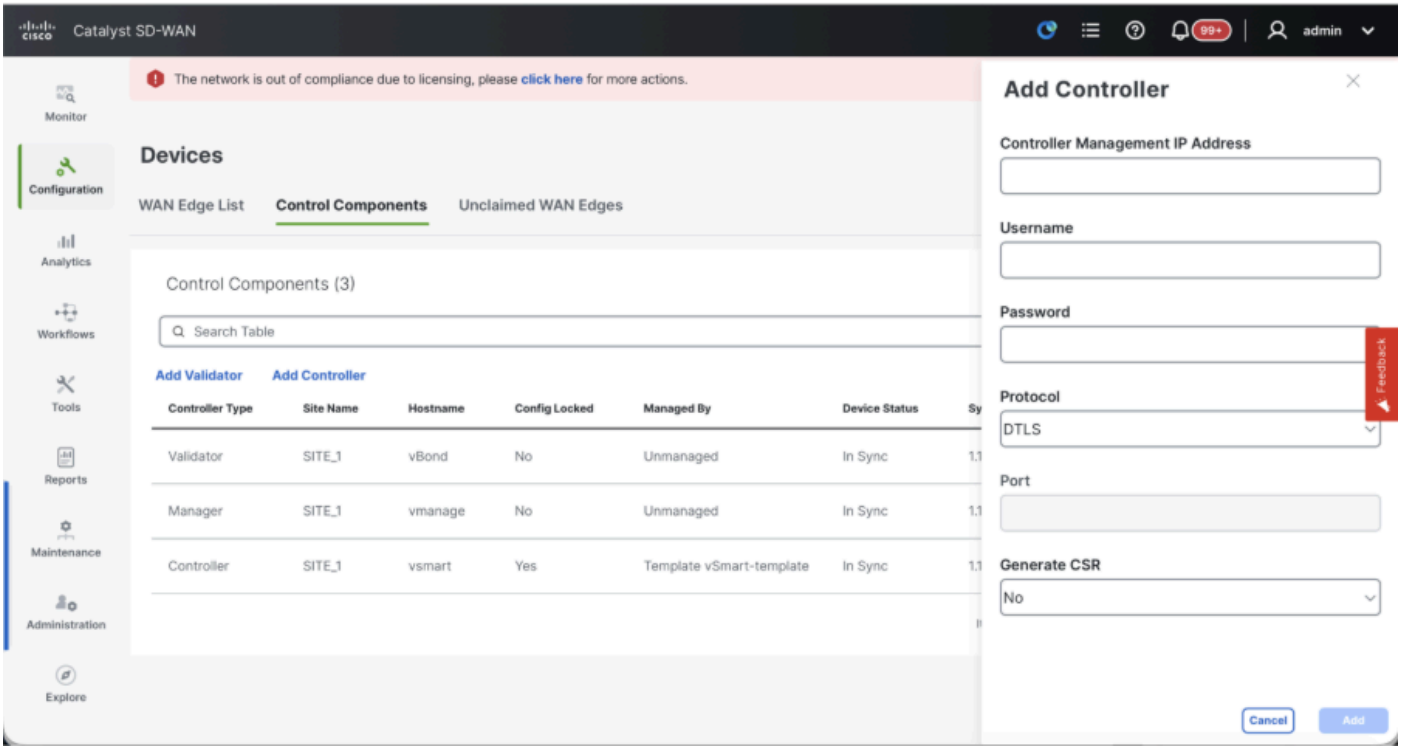


- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇思科（推薦），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vBond上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vBonds，請重複相同的步驟。

自註冊vSmart/控制器

- 在20.12 vManage的情況下按一下Add vSmart，在20.15/20.18 vManage的情況下按一下Add Controller。
- 系統開啟一個彈出視窗，輸入vSmart的VPN 0傳輸IP（可從vManage訪問）。
- 如果允許，請從vManage的CLI到vSmart IP使用ping檢查可達性。
- 輸入vSmart Note的使用者憑據，我們需要使用vSmart的管理員憑據或netadmin組的使用者部分。
- 您可以在vSmart的CLI中驗證這一點。
- 如果希望路由器使用TLS來建立與vSmart的控制連線，請將協定設定為TLS。此配置也需要在vSmarts和vManage節點的CLI上配置。
- 如需安裝vSmart的新憑證，請在「產生CSR」下拉式清單中選擇「是」。

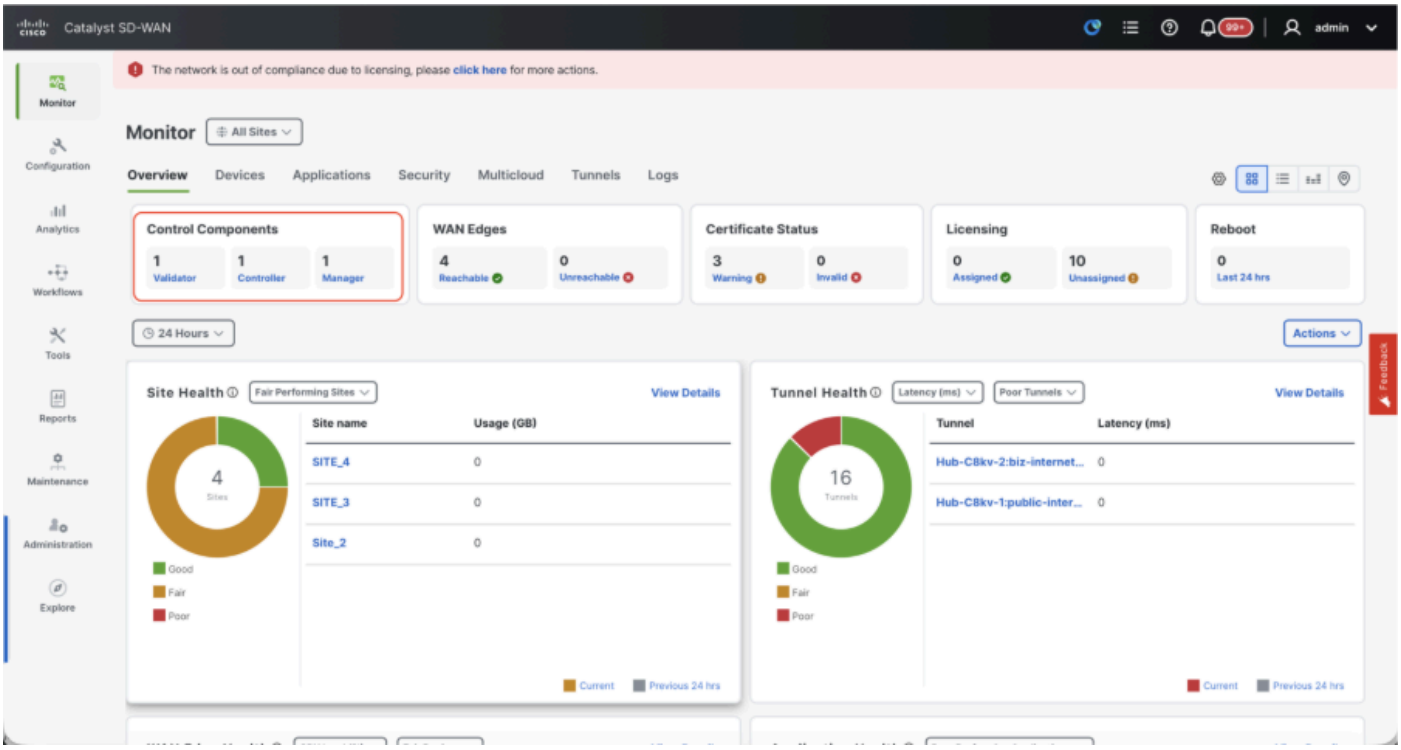
註：如果vSmart位於NAT裝置/防火牆之後，請檢查vSmart VPN 0介面IP是否已轉換為公共IP，如果無法從vManage訪問VPN 0介面IP，請在此步驟中使用VPN 0介面IP的公共IP地址。



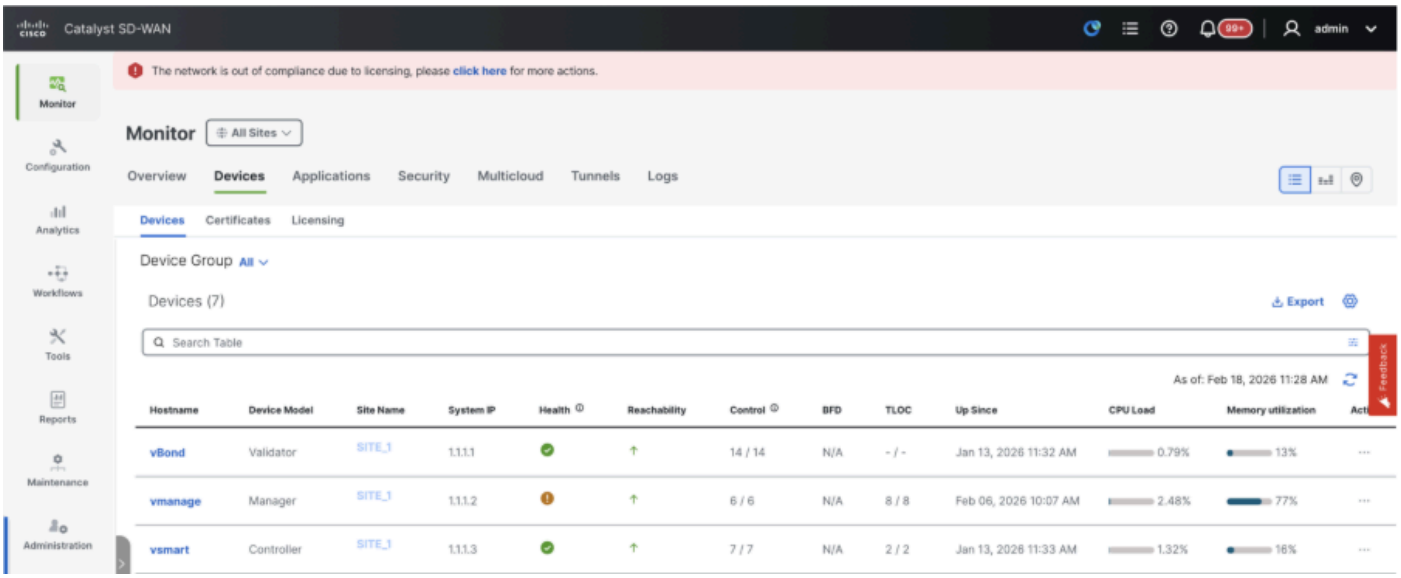
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vSmart上。
- 如果選擇「手動」，請導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，以使用思科PNP門戶手動簽署CSR。如果使用Digicert和企業根證書，則適用相同的程式。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果有多個vSmarts ，請重複相同的步驟。

驗證

完成所有步驟後，驗證是否可以在Monitor>Dashboard中訪問所有控制元件



- 按一下相應的控制元件，確認它們都可以訪問。
- 導覽至Monitor >Devices，確認所有控制元件均可連線。



步驟 3:Config-db備份/還原

在另一個vManage節點上收集vManage configuration-db備份和還原

收集Configuration-DB備份：

- 在當前正在使用的SD-WAN交換矩陣中，可以在獨立vManage和vManage群集設定上生成配置資料庫備份。
- 對於獨立vManage，該vManage本身是配置資料庫的領導者。

確認configuration-db正在vManage節點上運行。

您可以在vManageCLI上使用request nms configuration-db status命令進行驗證。輸出如下

```
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#
```

使用此命令從標識的configuration-db領導vManage節點收集configuration-db備份。

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

預期輸出如下：

```
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#
```

- 如果已更新configuration-db憑證，請記下該憑證。
- 如果您不知道配置資料庫憑據，請聯絡TAC以從現有vManage節點檢索配置資料庫憑據。
- 預設的configuration-db憑證是使用者名稱：neo4j和密碼：密碼

將Configuration-db備份還原到另一個vManage節點

使用SCP將configuration-db backup複製到vManage的/home/admin/目錄。

scp命令輸出示例：

```
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
```

要恢復configuration-db備份，首先需要配置configuration-db憑據。如果您的配置資料庫憑據是預設值(neo4j/password)，則可以跳過此步驟。

要配置configuration-db憑據，請使用命令request nms configuration-db update-admin-user。使用您選擇的使用者名稱和密碼。

請注意，vManage的應用程式伺服器已重新啟動。由於vManage UI將在短時間內不可訪問。

```
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#
```

可以繼續還原配置資料庫備份的開機自檢：

我們可以使用命令request nms configuration-db restore path /home/admin/< >將configuration-db還原到新的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
```

恢復configuration-db後，確保vManage UI可訪問。等待約5分鐘，然後嘗試訪問UI。

成功登入到UI後，請確保邊緣路由器清單、模板、策略以及以前或現有vManage UI上存在的所有其餘配置都反映在新的vManage UI上。

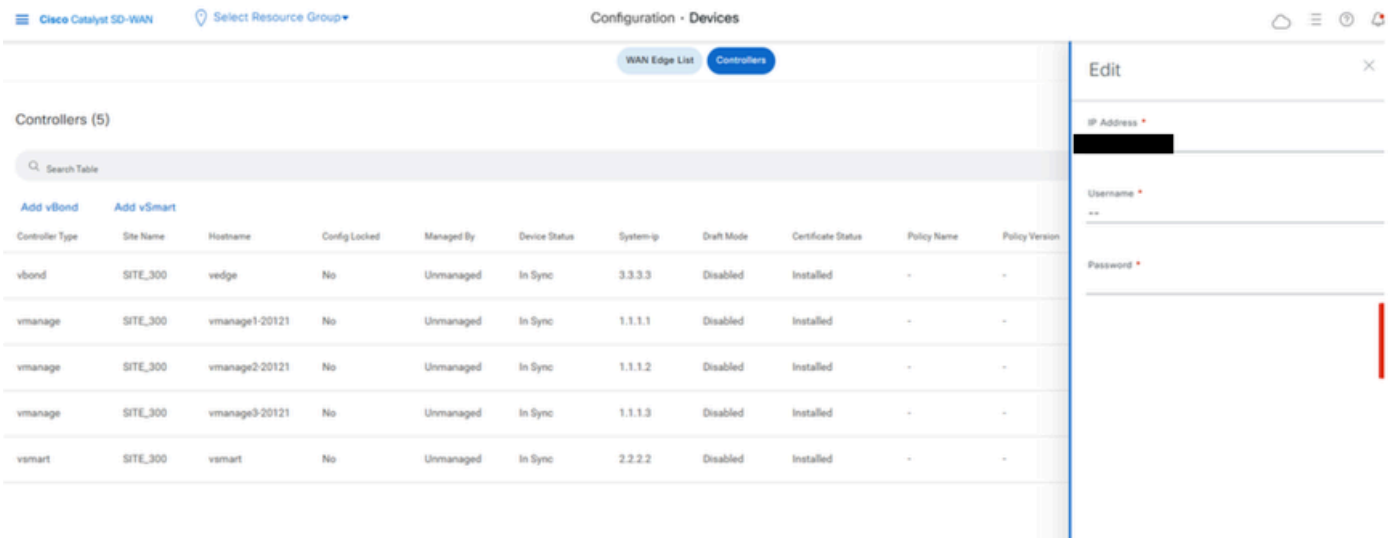
步驟 4:控制器的重新驗證和舊控制器的失效

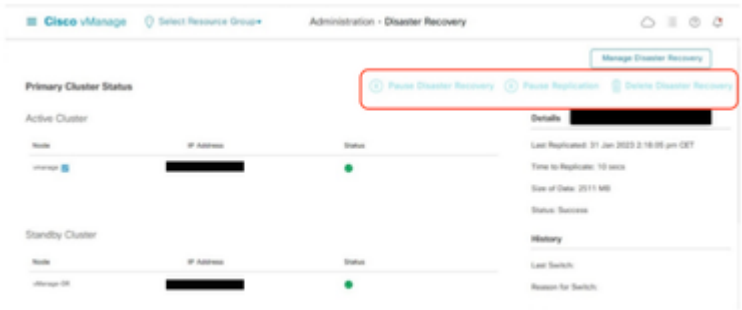
恢復configuration-db後，我們需要重新驗證交換矩陣中的所有新控制器(vmanage/vsmart/vbond)。

註：在實際生產中，如果用於重新身份驗證的介面IP是隧道介面IP，則需要確保在vManage、vSmart和vBond的隧道介面以及路徑沿途的防火牆上允許NETCONF服務。要開啟的防火牆埠是作為從DR群集到所有vBonds和vSmarts的雙向規則的TCP埠830。

在vmanage UI上，點選Configuration > Devices > Controllers

- 按一下每個控制器附近的三個點，然後按一下「Edit（編輯）」





- 將ip-address（控制器的系統ip）替換為傳輸vpn 0（隧道介面）ip地址。輸入使用者名稱和密碼，然後按一下儲存
- 對交換矩陣中的所有新控制器執行相同操作

同步根證書鏈

載入所有控制器後，完成以下步驟：

在新活動群集中的任何Cisco SD-WAN Manager伺服器上，執行以下操作：

輸入以下命令將根證書與新活動群集中的所有Cisco Catalyst SD-WAN裝置同步：

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

輸入以下命令將Cisco SD-WAN Manager UUID與Cisco SD-WAN驗證器同步：

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

在交換矩陣恢復後，交換矩陣中的所有邊緣和控制器的控制和bfd會話均已啟動，我們需要從UI使舊控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，點選Configuration > Certificates > Controllers
- 按一下「Controllers（控制器）」
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)右側的三個點。按一下「invalidate（失效）」
- 點選send to vbond
- 在vmanage UI上，點選Configuration > Devices > Controllers
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)右側的三個域。點選刪除(Delete)

步驟 5:過帳支票

附註：繼續使用此處顯示的「後檢查」部分，它對所有部署組合都是通用的。

組合2:獨立vManage +單節點DR

所需例項：

- 1個vManage（主、COMPUTE_AND_DATA）
- 1個vManage(DR standby、COMPUTE_AND_DATA)
- 1個或多個vBond
- 1個或多個vSmart

步驟:

1. 使用通用步驟調出所有例項
2. 預先檢查
3. 配置vManage UI、證書和板載控制器
4. 單節點DR設定
5. Config-db backup/restore

6. 過帳支票

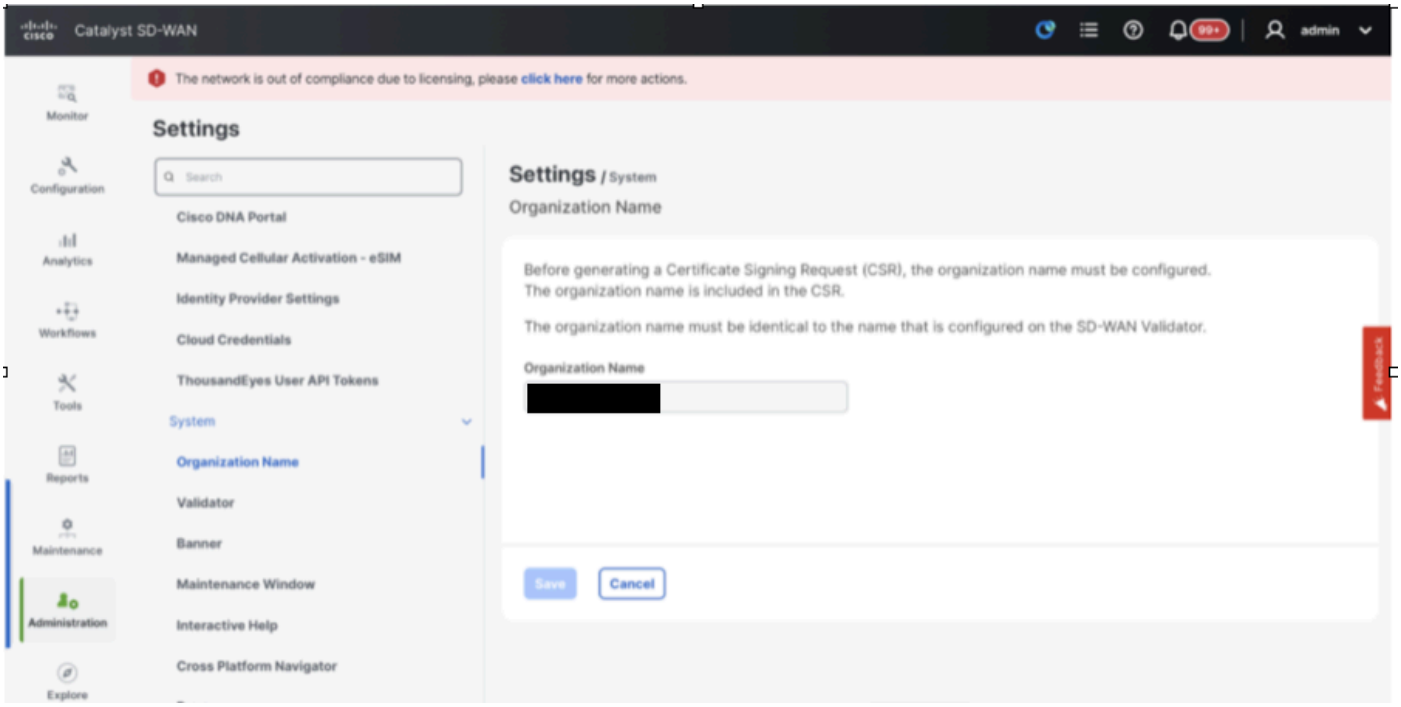
步驟 1:預先檢查

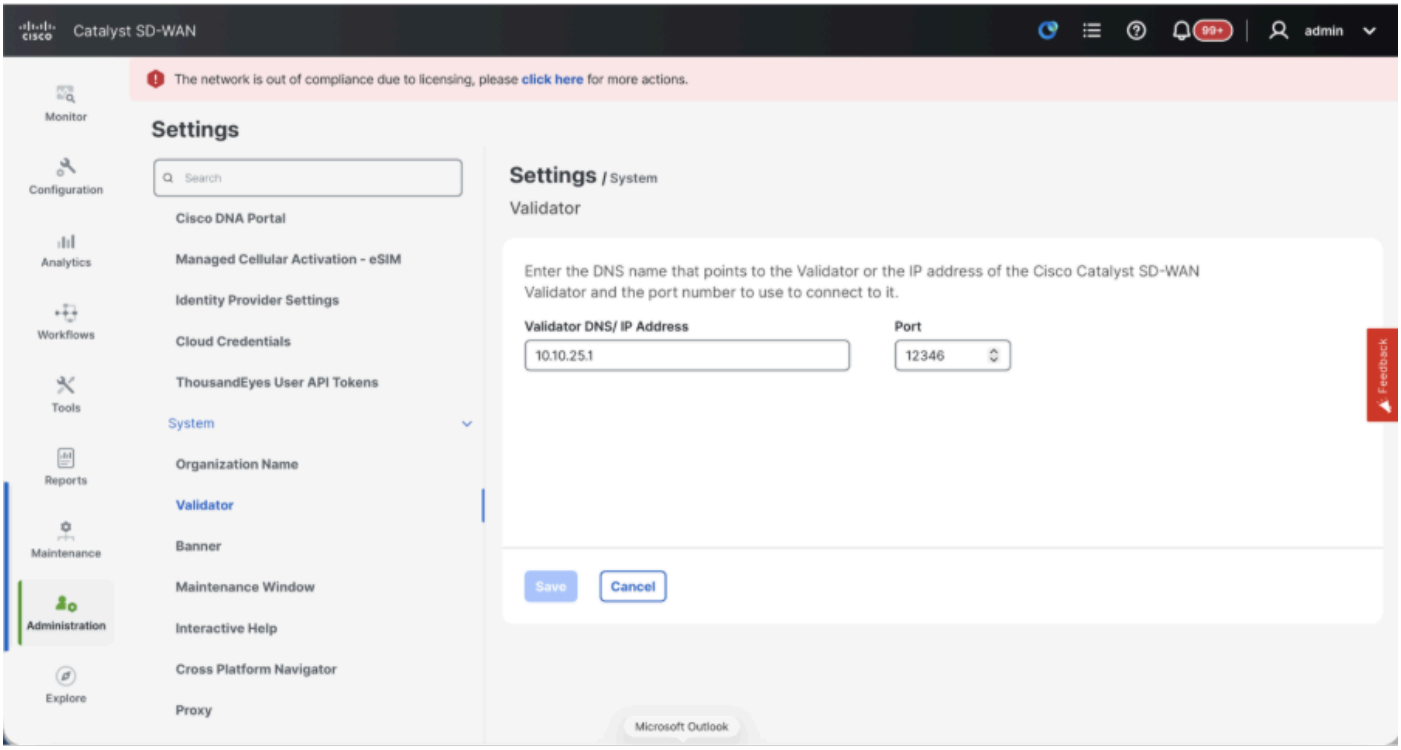
- 確保活動的Cisco SD-WAN Manager例項數與新安裝的Cisco SD-WAN Manager例項數相同。
- 確保所有活動的和新的Cisco SD-WAN Manager例項運行相同的軟體版本。
- 確保所有活動的和新的Cisco SD-WAN Manager例項都能到達Cisco SD-WAN Validator的管理IP地址。
- 確保證書已安裝在新安裝的Cisco SD-WAN Manager例項上。
- 確保所有Cisco Catalyst SD-WAN 裝置(包括新安裝的Cisco SD-WAN Manager例項)上的時鐘都同步。
- 確保在新安裝的Cisco SD-WAN Manager例項上配置一組新的系統IP和站點ID，並與活動群集配置相同的基本配置。

步驟 2:配置vManage UI、證書和板載控制器

更新vManage UI上的配置

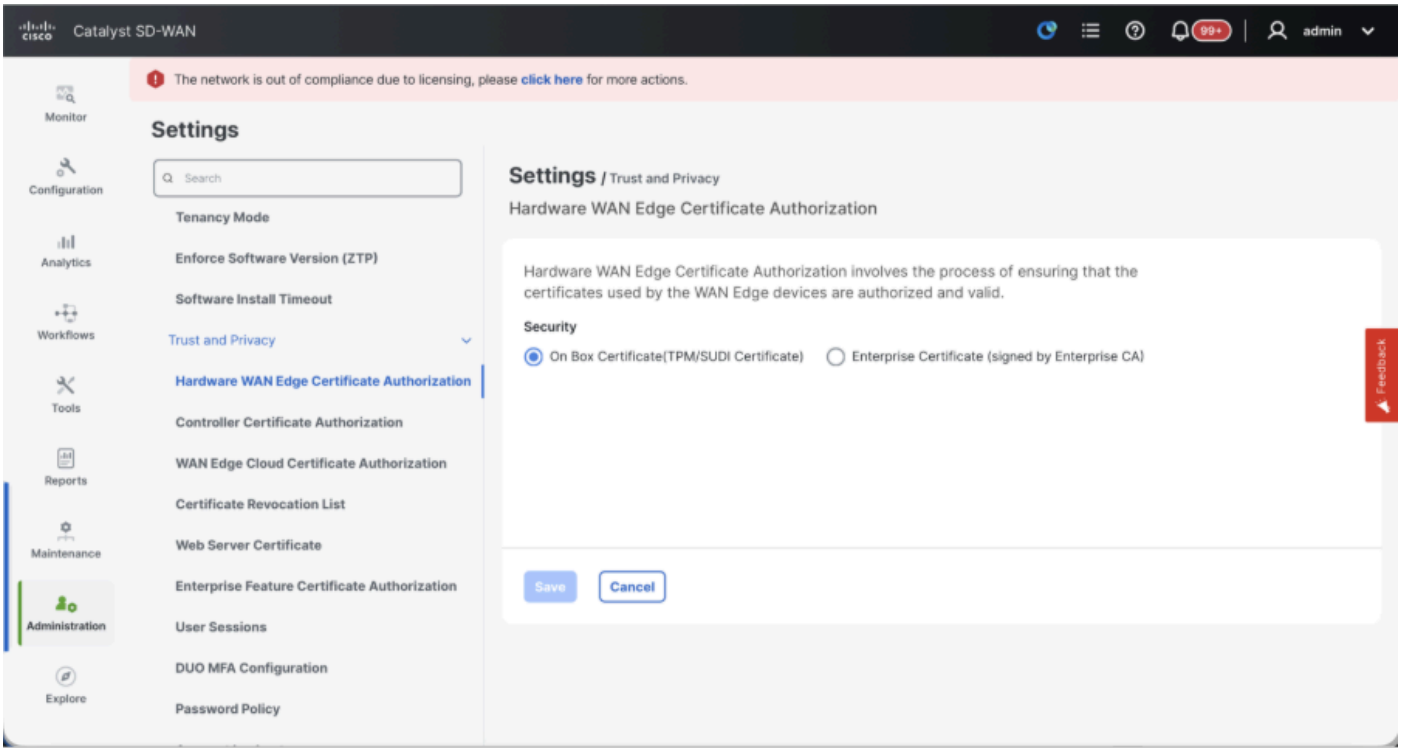
- 將步驟1中的組態新增到所有控制器的CLI上後，我們可以使用瀏覽器中的https://<vmanage-ip>URL存取vManage的WebUI。使用各個vManage節點的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 導覽至Administration > Settings，然後完成以下步驟。
- 配置組織名稱和驗證器/vBond URL/IP地址。配置與vManage節點的CLI中相同的值。
- 在vManage 20.15/20.18中，這些配置可在System部分中找到。





- 驗證證書授權(CA)的配置，CA決定用於簽署證書的證書授權。我們可以看到3個選項：

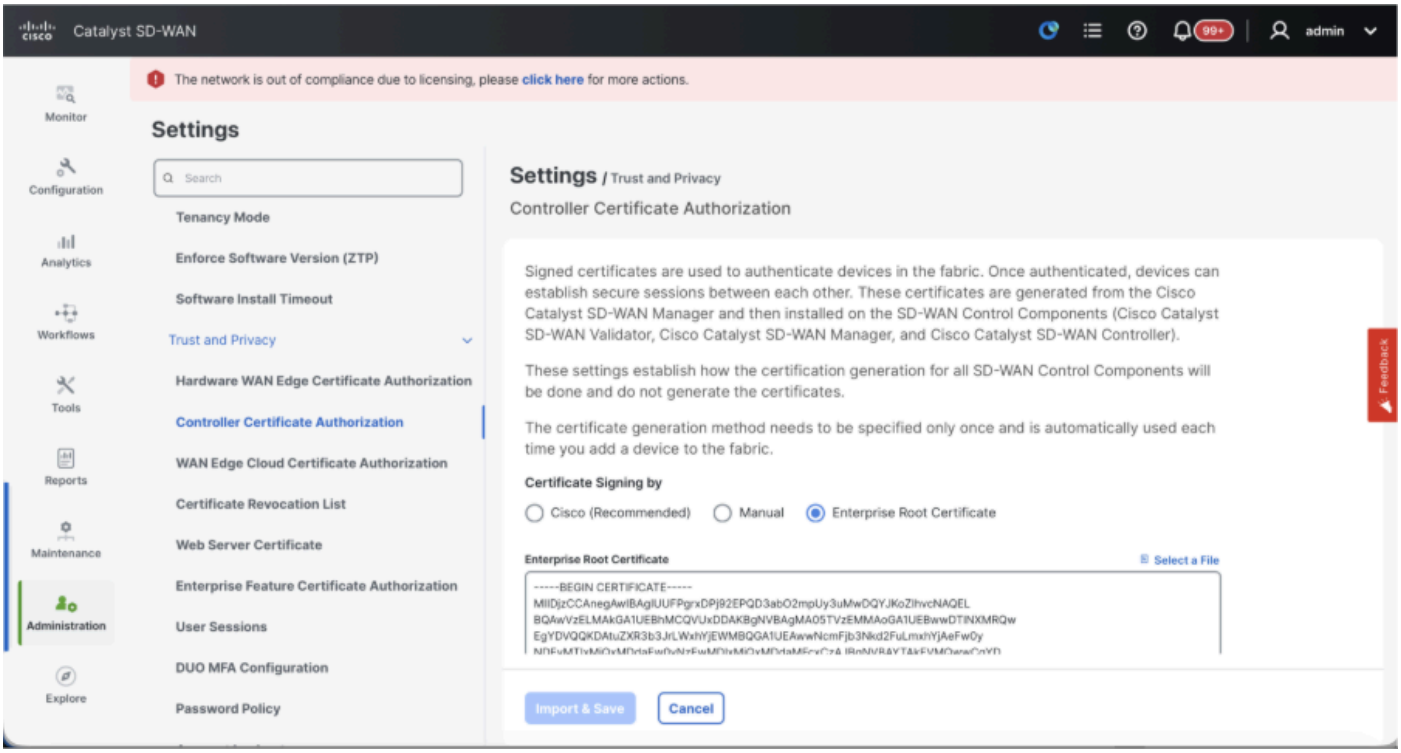
1. 硬體WAN邊緣證書授權 — 決定硬體SD-WAN邊緣路由器的CA。
    - 開箱證書（TPM/SUDI證書） — 使用此選項，路由器硬體上預安裝的證書用於建立控制連線（TLS/DTLS連線）
    - 企業證書（由企業CA簽署） — 使用此選項時，路由器使用由組織的企業證書頒發機構簽署的證書。選擇此選項時，必須在此處更新企業CA的根證書。



2. Controller Certificate Authorization — 決定SD-WAN控制器的CA。
    - 思科（推薦） — 控制器使用由Cisco PKI簽名的證書。vManage使用vManage上配置的

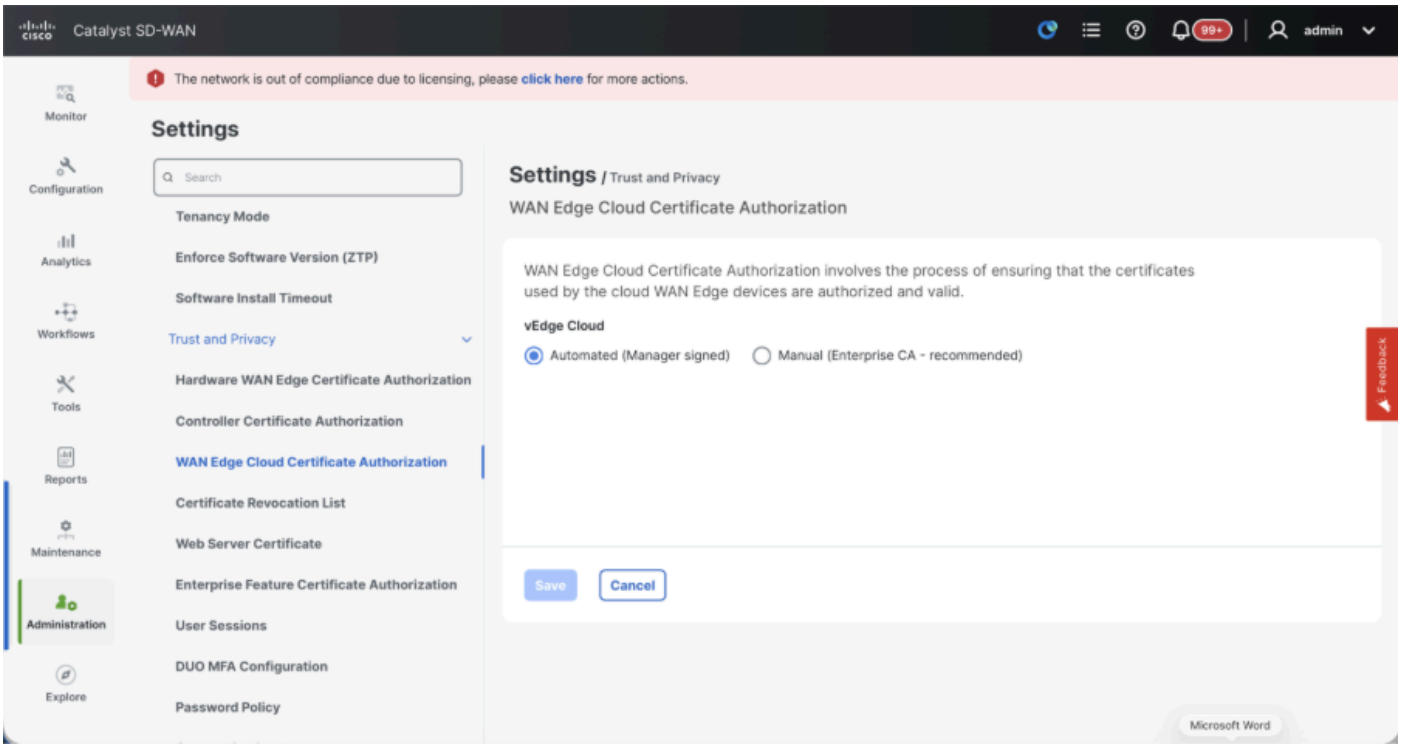
智慧帳戶憑據自動聯絡PNP門戶，並簽署證書並將其安裝在控制器上。

- 手動 — 控制器使用由Cisco PKI簽名的證書。導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
- Enterprise Root Certificate — 使用此選項時，路由器使用由您組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。

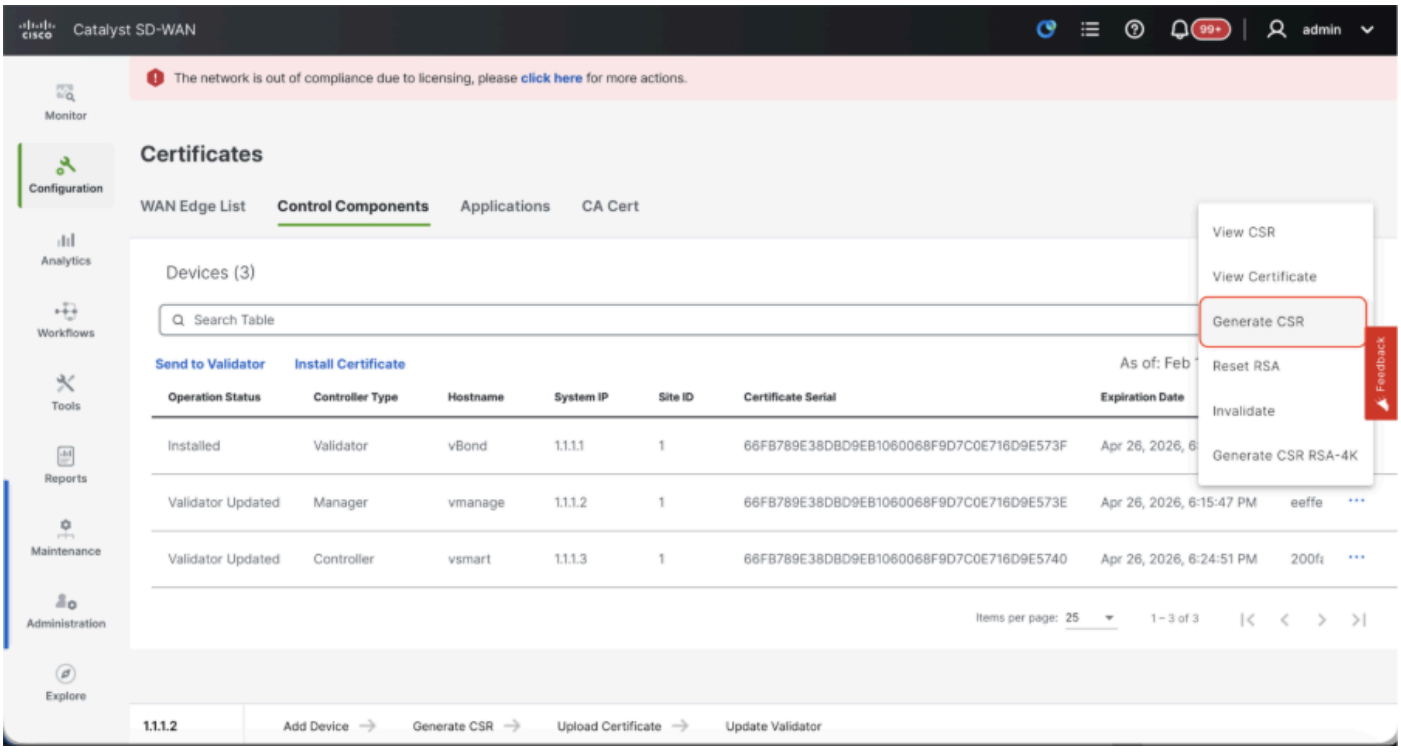


3. WAN邊緣雲證書授權 — 確定虛擬SD-WAN邊緣路由器（CSR1000v、C8000v、vEdge雲）的CA
    - 自動（vManage簽名） — vManage自動對虛擬邊緣路由器的CSR進行簽名，並在路由器上安裝證書。
    - 手動（企業CA — 推薦） — 虛擬路由器使用由組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。

如果使用CA（企業證書頒發機構），請選擇Enterprise。



- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers
- 點選Manager/vManage的……並點選Generate CSR。



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相

同的步驟。

將vBond/Validator和vSmart/Controller註冊到vManage

如果是20.15/20.18 vManage節點，請導航到Configuration > Devices > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

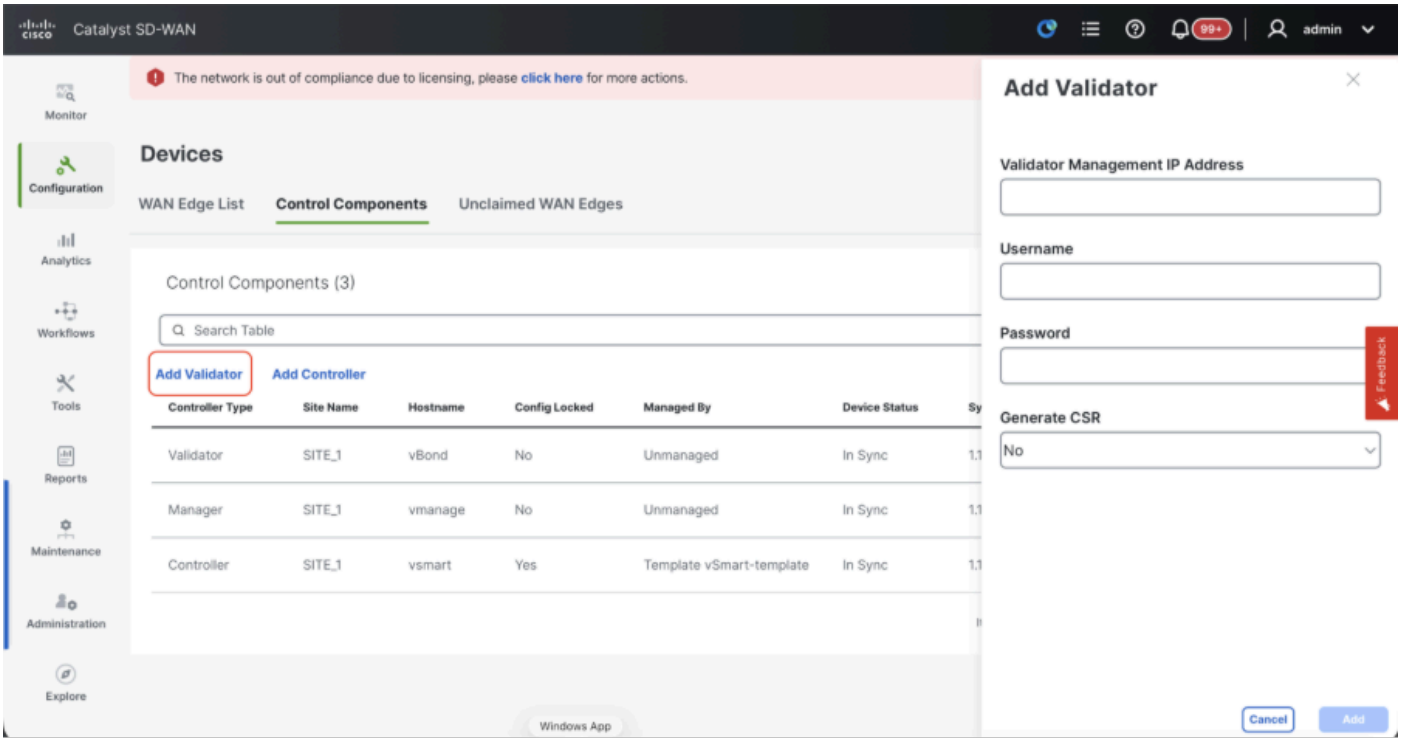
OnboardingvBond/驗證器

- 按一下AddvBond在20.12vManageor的情況下新增驗證程式在20.15/20.18 vManage的情況下。系統開啟一個彈出視窗，輸入 從vManage可訪問的vBond的VPN 0傳輸IP。
- 如果允許，請從vManagetovBondIP的CLI使用ping檢查可連接性。
- 輸入vBond的使用者憑據。

注意:我們需要使用vBondor的admin憑據作為netadmingroup的使用者部分。您可以在vBond的CLI中驗證這一點。如需安裝vBond的新憑證，請在「產生CSR」下拉式清單中選擇Yes

---

附註：如果vBond位於NAT裝置/防火牆之後，請檢查vBond VPN 0介面IP是否已轉換為公共IP。如果無法從vManage訪問VPN 0介面IP，則在此步驟中使用VPN 0介面的公用IP地址



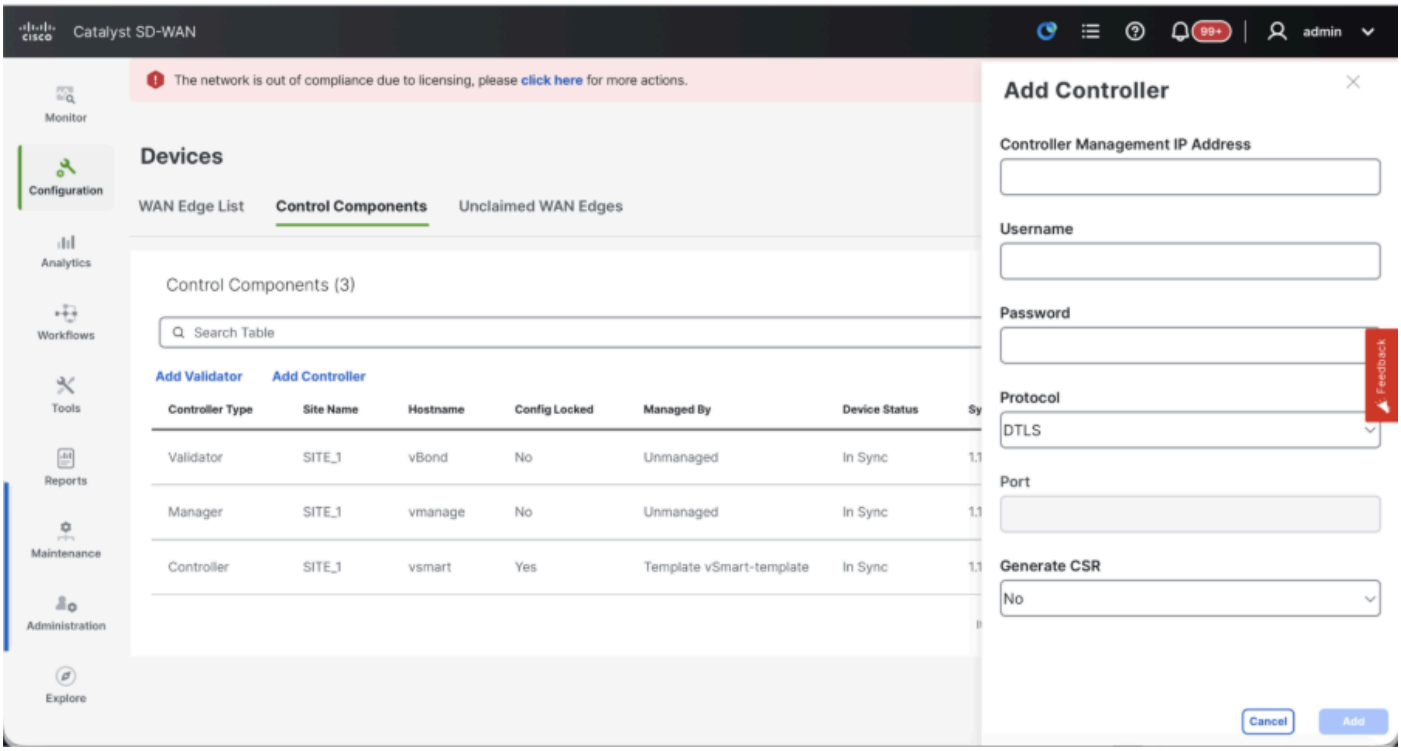
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇思科（推薦），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vBond上。

- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vBonds，請重複相同的步驟。

自註冊vSmart/控制器

- 在20.12 vManage的情況下按一下Add vSmart，在20.15/20.18 vManage的情況下按一下Add Controller。
- 系統開啟一個彈出視窗，輸入vSmart的VPN 0傳輸IP（可從vManage訪問）。
- 如果允許，請從vManage的CLI到vSmart IP使用ping檢查可達性。
- 輸入vSmart Note的使用者憑據，我們需要使用vSmart的管理員憑據或netadmin組的使用者部分。
- 您可以在vSmart的CLI中驗證這一點。
- 如果希望路由器使用TLS來建立與vSmart的控制連線，請將協定設定為TLS。此配置也需要在vSmarts和vManage節點的CLI上配置。
- 如需安裝vSmart的新憑證，請在「產生CSR」下拉式清單中選擇「是」。

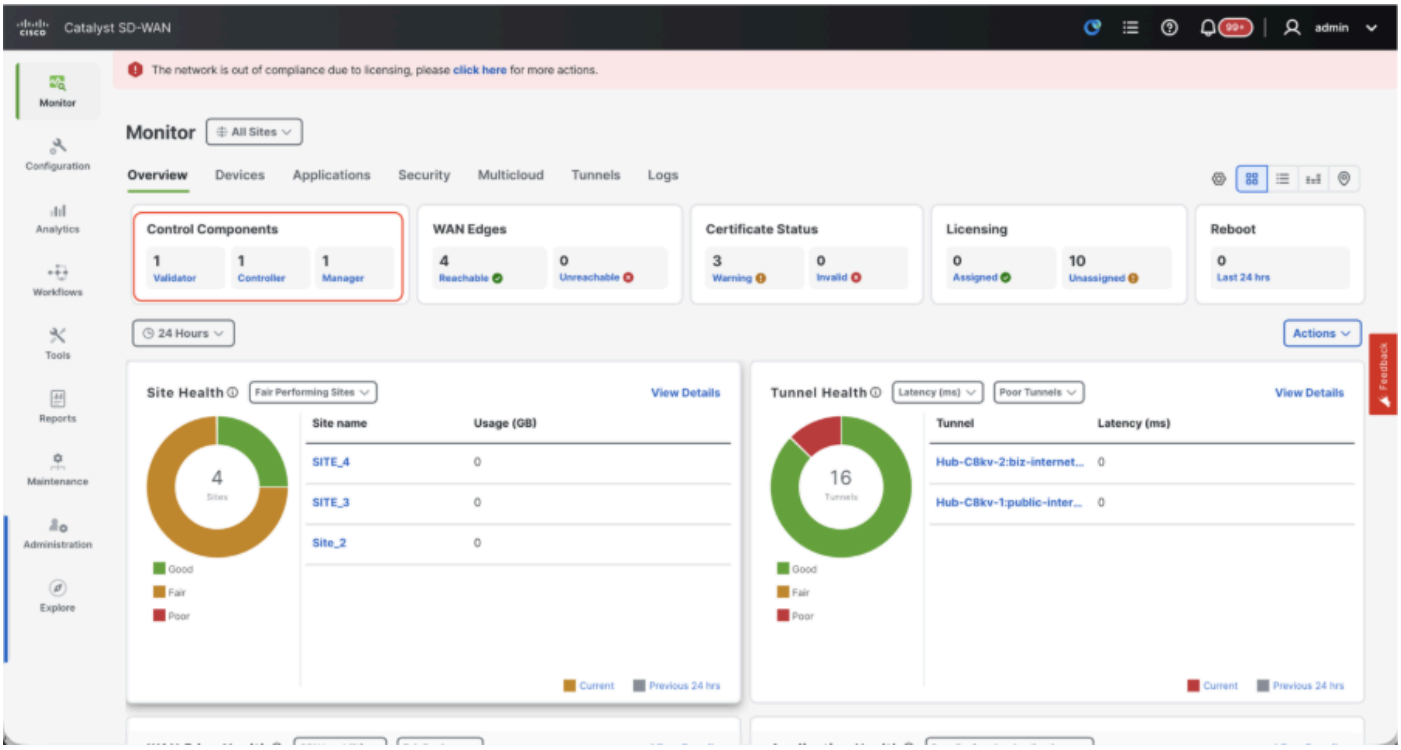
註：如果vSmart位於NAT裝置/防火牆之後，請檢查vSmart VPN 0介面IP是否已轉換為公共IP，如果無法從vManage訪問VPN 0介面IP，請在此步驟中使用VPN 0介面IP的公共IP地址。



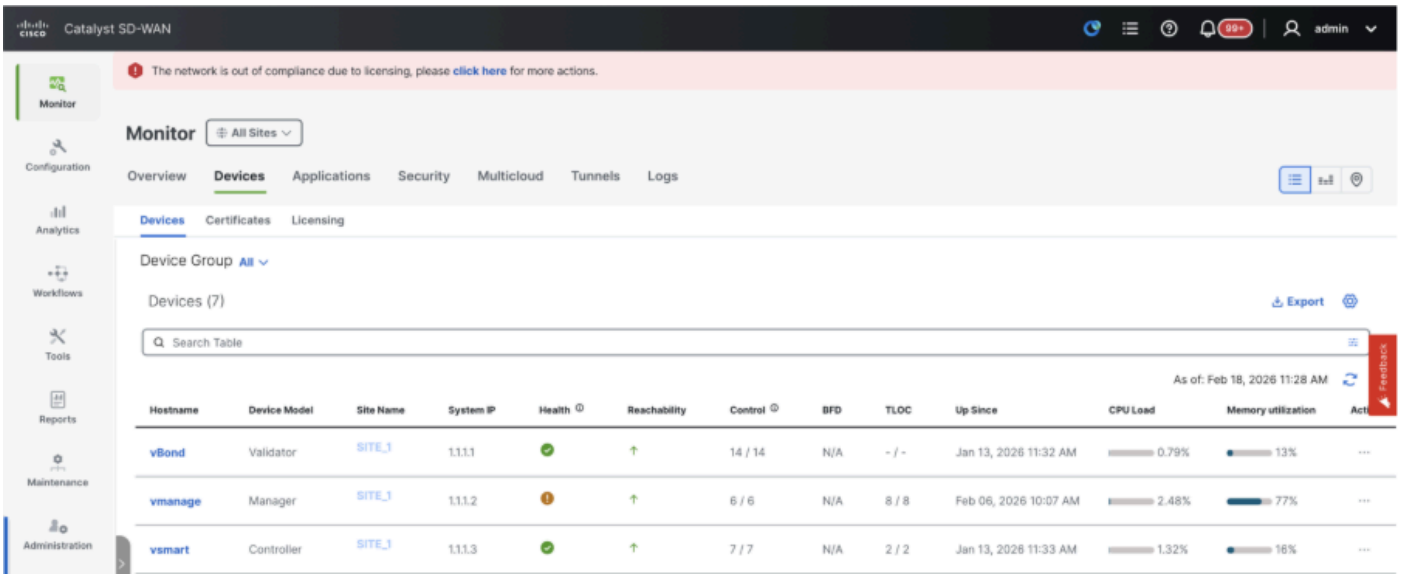
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vSmart上。
- 如果選擇「手動」，請導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，以使用思科PNP門戶手動簽署CSR。如果使用Digicert和企業根證書，則適用相同的程式。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果有多個vSmarts ，請重複相同的步驟。

驗證

完成所有步驟後，驗證是否可以在Monitor>Dashboard中訪問所有控制元件



- 按一下相應的控制元件，確認它們都可以訪問。
- 導覽至Monitor >Devices，確認所有控制元件均可連線。



步驟 3:Config-db備份/還原

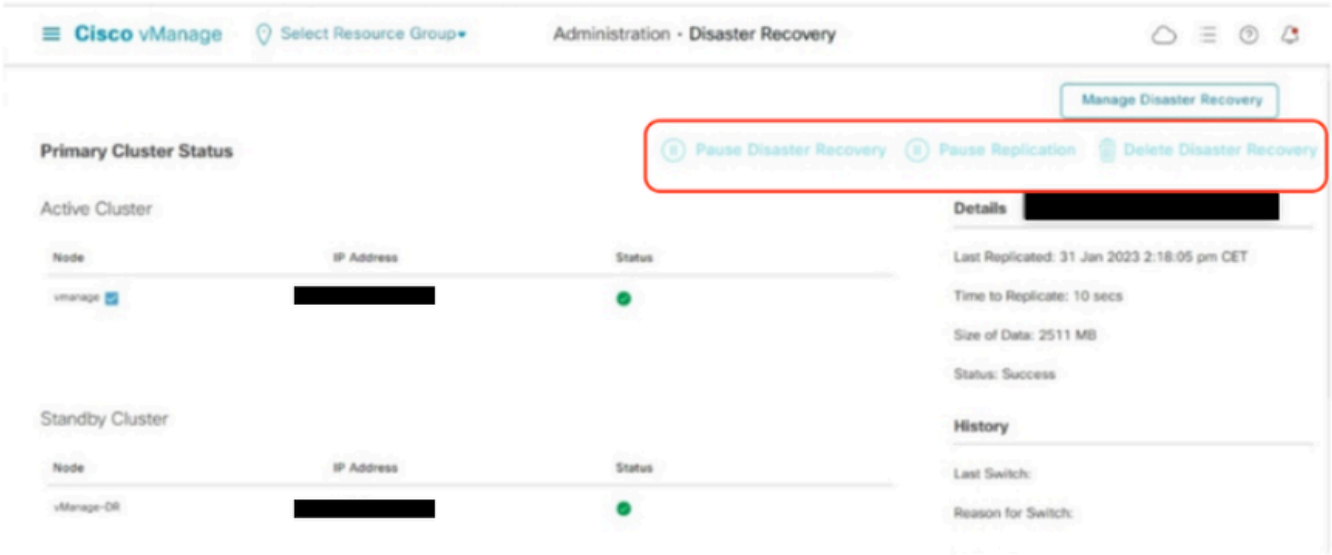
在另一個vManage節點上收集vManage configuration-db備份和還原

附註：從已啟用災難恢復的現有vManage節點收集配置資料庫備份時，請確保在該節點上的災難恢復暫停並刪除後收集該備份。

確認沒有正在進行的災難恢復複製。導航到管理>災難恢復和 確保狀態為「成功」，而不是處於「

匯入掛起」、「匯出掛起」或「下載掛起」等暫時狀態。如果狀態不成功，請聯絡Cisco TAC並確保複製成功，然後繼續暫停災難恢復。

首先暫停災難恢復並確保任務完成。然後刪除災難恢復並確認任務已完成。



聯絡Cisco TAC，確保已成功清理災難恢復。

收集Configuration-DB備份：

- 在當前正在使用的SD-WAN交換矩陣中，可以在獨立vManage和vManage群集設定上生成配置資料庫備份。
- 對於獨立vManage，該vManage本身是配置資料庫的領導者。

確認configuration-db正在vManage節點上運行。

您可以使用commandrequest nms configuration-db statusonvManageCLI驗證相同內容。輸出如下

```
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#
```

使用此命令從標識的configuration-db領導vManage節點收集configuration-db備份。

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

預期輸出如下：

```
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#
```

- 如果已更新configuration-db憑證，請記下該憑證。
- 如果您不知道配置資料庫憑據，請聯絡TAC以從現有vManage節點檢索配置資料庫憑據。
- 預設的configuration-db憑證是使用者名稱：neo4j和密碼：密碼

將Configuration-db備份還原到另一個vManage節點

使用SCP將configuration-db backup複製到vManage的/home/admin/目錄。

scp命令輸出示例：

```
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
```

要恢復configuration-db備份，首先需要配置configuration-db憑據。如果您的配置資料庫憑據是預設值(neo4j/password)，則可以跳過此步驟。

要配置configuration-db憑據，請使用request nms configuration-db update-admin-user命令。使用您選擇的使用者名稱和密碼。

請注意，vManage的應用程式伺服器已重新啟動。由於vManage UI將在短時間內不可訪問。

```
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#
```

可以繼續還原配置資料庫備份的開機自檢：

我們可以使用命令request nms configuration-db restore path /home/admin/< >將configuration-db還原到新的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
```

恢復configuration-db後，確保vManage UI可訪問。等待約5分鐘，然後嘗試訪問UI。

成功登入到UI後，請確保邊緣路由器清單、模板、策略以及以前或現有vManage UI上存在的所有其餘配置都反映在新的vManage UI上。

步驟 4:單節點DR設定

請參閱步驟2:Combination 2:中的預檢查獨立式vManage +單節點災難恢復，並確保我們已經完成所有要求，然後我們開始啟用災難恢復。

單節點DR

必要條件

- 確保在傳輸VPN(VPN 0)上通過HTTPS可以訪問主節點和輔助節點。

- 確保Cisco vManage主節點和輔助節點運行相同的Cisco vManage版本。

VPN 0中的帶外群集介面

1. 對於集群內的每個vManage例項，除了用於VPN 0（傳輸）和VPN 512（管理）的介面之外，還需要第三個介面（集群鏈路）。
2. 此介面用於群集內vManage伺服器之間的通訊和同步。
3. 此介面必須至少為1 Gbps，並且延遲為4毫秒或更短。建議使用10 Gbps介面。
4. 兩個vManage節點必須能夠通過此介面相互連線：無論是第2層網段還是通過第3層路由。

- 確保在兩個Cisco vManage節點上啟用所有服務（應用伺服器、配置資料庫、消息伺服器、協調伺服器和統計資訊資料庫）。
- 在主資料中心和輔助資料中心之間分發所有控制器，包括Cisco vBond協調器。確保這些控制器可通過分佈在這些資料中心的Cisco vManage節點訪問。控制器僅連線到主Cisco vManage節點。
- 確保主用（主）和備用（輔助）Cisco vManage節點中沒有其他操作正在進行。例如，確保沒有伺服器正在升級，或者沒有模板正在將模板附加到裝置。

- 如果已啟用Cisco vManage HTTP/HTTPS代理伺服器，請將其禁用。如果不禁用代理伺服器，Cisco vManage將嘗試通過代理IP地址建立災難恢復通訊，即使Cisco vManage帶外群集IP地址可直接訪問。災難恢復註冊完成後，您可以重新啟用Cisco vManage HTTP/HTTPS代理伺服器。

- 開始災難恢復註冊過程之前，請轉至主Cisco vManage節點上的Tools → Rediscover Network視窗，並重新發現Cisco vBond Orchestrator。

組態

配置作為災難恢復節點的所有vManage節點的CLI配置

vManage的最低配置災難恢復註冊之前，如下所示

```
config t
system
 host-name



 system-ip



 site-id



 organization-name
```

```
 vbond



commit
```

注意:如果使用URL作為vBond地址，請確保在VPN 0配置中配置DNS伺服器IP地址或確保可以解析這些地址。

啟用傳輸介面時，需要使用這些配置來建立與路由器和其餘控制器的控制連線

```
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
```

另外配置VPN 512management介面以啟用對控制器的帶外管理訪問。

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
commit
```

在DR vManage上配置服務介面

在vManage節點上配置服務介面。此介面用於DR通訊，

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

```
  no shutdown
commit
```

確保同一IP子網用於主vManage和DR vManage上的服務介面。

更新vManage UI上的配置

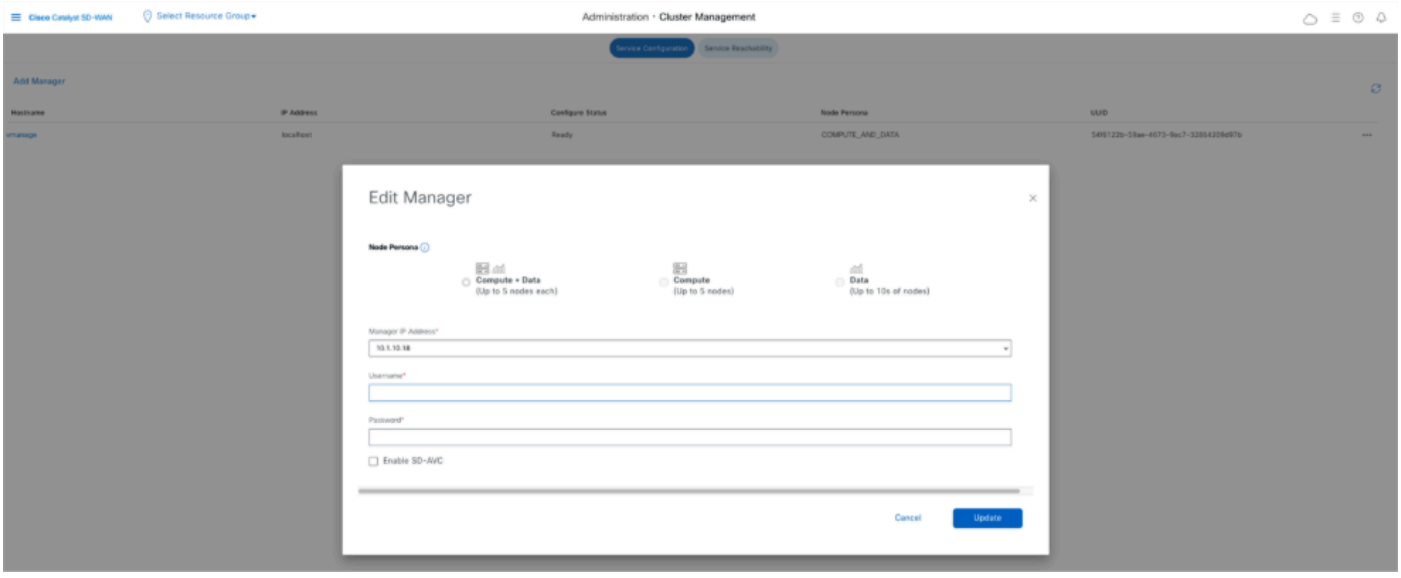
- 在所有控制器的CLI上新增配置後，我們就可以使用瀏覽器中的https://<vmanage-ip>訪問vManage的WebUI。使用各個vManage節點的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 導覽至Administration > Settings，然後完成以下步驟。
- 配置組織名稱。配置與vManage節點的CLI中相同的值。
- 在vManage 20.15/20.18中，這些配置可在System部分中找到。

在DR vManage上安裝證書

繼續執行Combination 2部分中提供的步驟：獨立vManage +單節點DR第3步：配置vManage UI、證書和板載控制器，以在災難恢復vManage上安裝該證書。

新增災難恢復配置

- 為此，請轉至主vManage。
- 點選vManage條目右側的三個點，導航到Administration → Cluster Management，指示帶外介面的IP地址，並包括使用者名稱和密碼。建議為此配置在主要和DR vmanage上建立單獨的本地使用者，例如dradmin。



- VManage在此更改後重新啟動。

- 主vManage啟動後，導航至管理→災難恢復。按一下「管理災難恢復」。
- 在彈出視窗中，填寫主要和輔助vManage的詳細資訊。
- 要指示的IP地址是帶外群集介面(eth2)的IP地址。
- 憑證必須是netadmin使用者(dradmin)的憑證，並且配置DR後不得更改這些憑證。可以使用單獨的vManage本地使用者憑據進行災難恢復。我們需要確保vManage本地使用者是netadmin組的一部分。此處也可以使用管理員憑據。

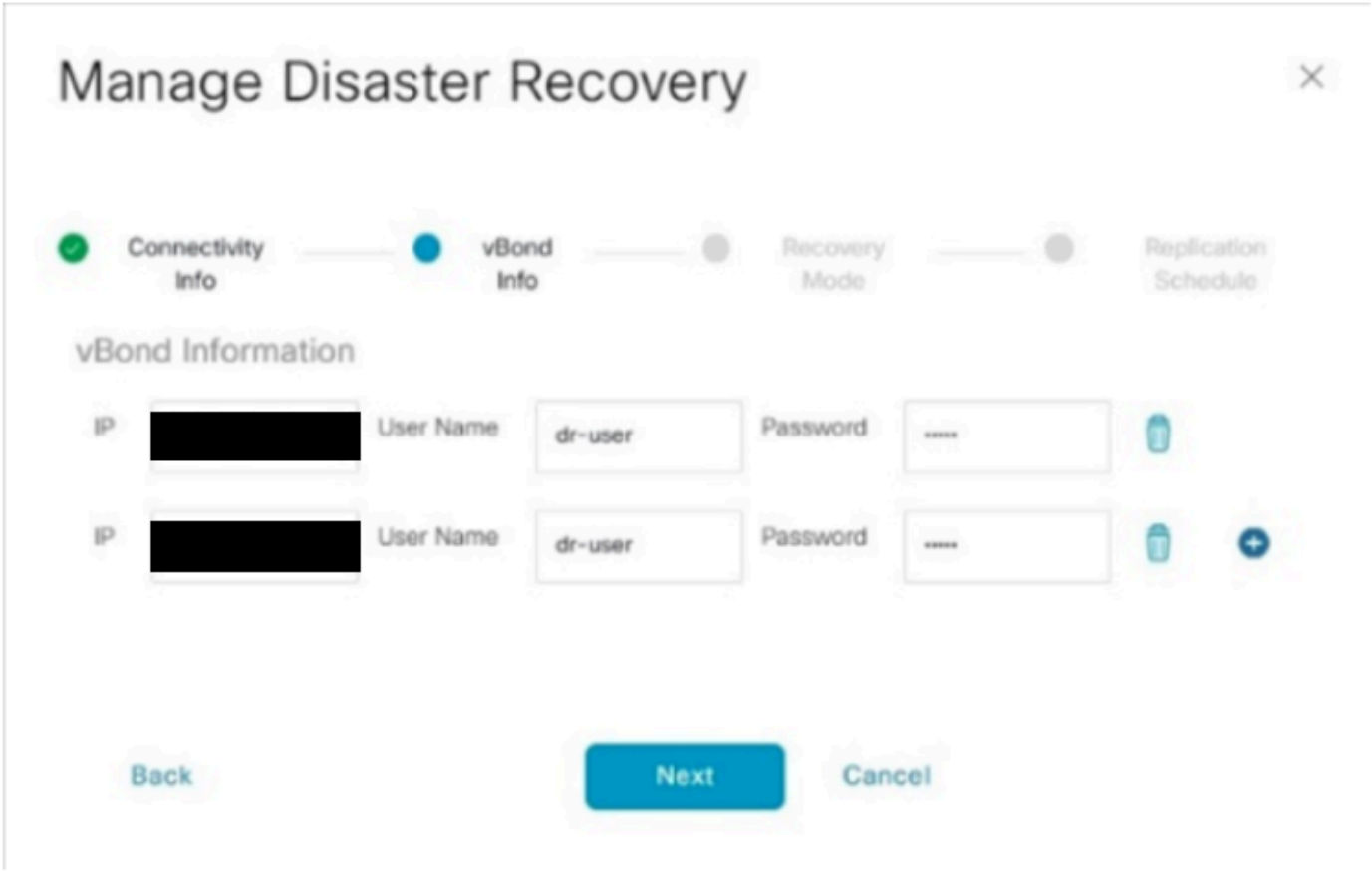
- 填寫完畢後，按一下「下一步」。

- 填寫vBond控制器的詳細資訊。

- vBond控制器必須能夠通過Netconf以指定的IP地址訪問。

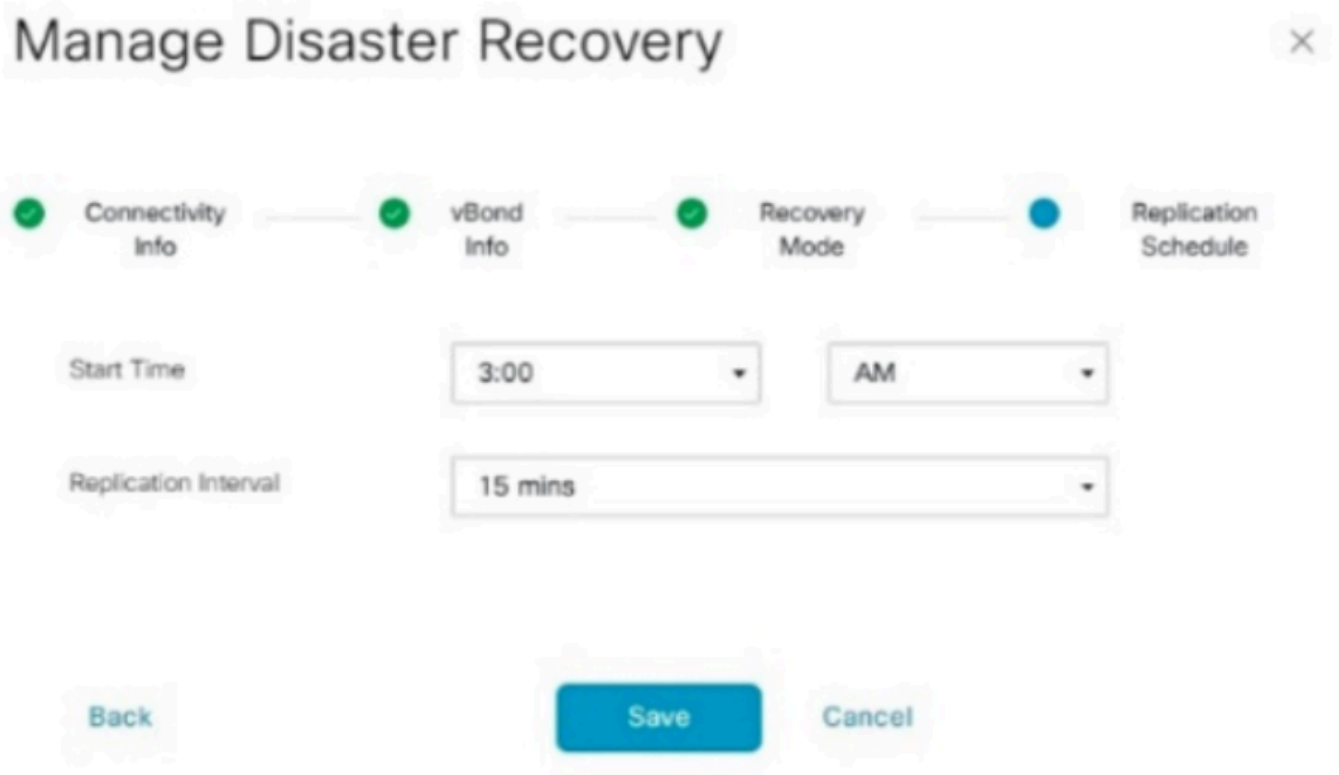
- 憑據必須是netadmin使用者(dradmin)的憑據，並且配置DR後不能更改這些憑據。

- 為此，建議在本地配置此dradmin使用者，或者可以使用admin使用者新增vBond。

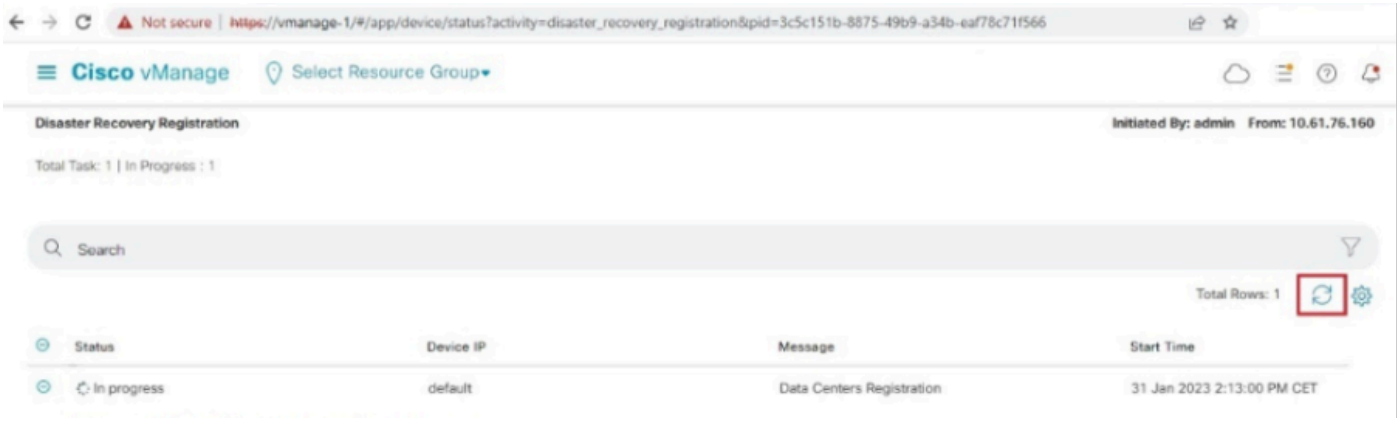


- 填寫完畢後，按一下「下一步」。
- 在「恢復模式」中，選擇「手動」。按一下「下一步」。

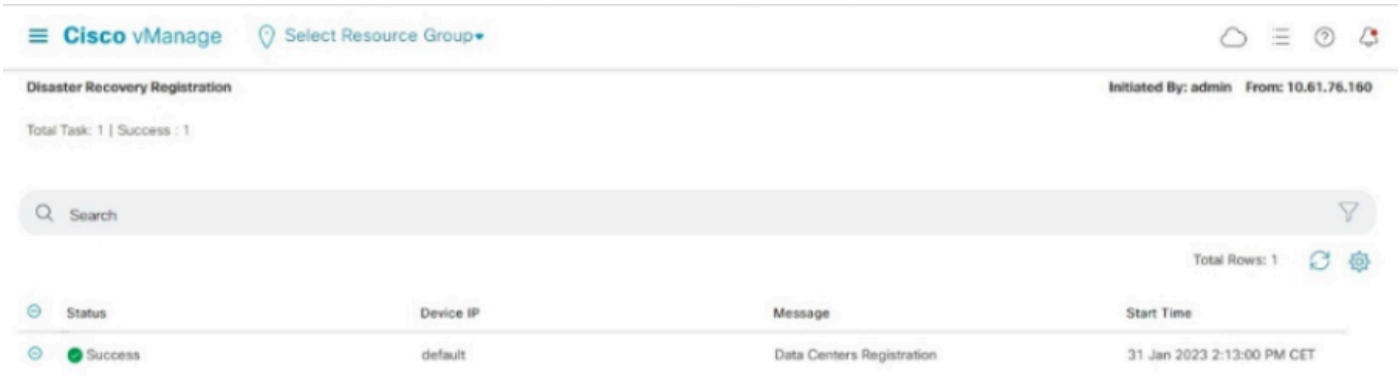
在複製計畫中，設定「複製間隔」'。每次複製間隔時間，資料都會從主節點複製 vManagement到輔助vManage。最小可配置值為15分鐘。



- 設定該值並按一下「Save」。
- DR註冊現在開始。按一下刷新按鈕以手動刷新狀態和進度日誌。此過程可能需要20-30分鐘。

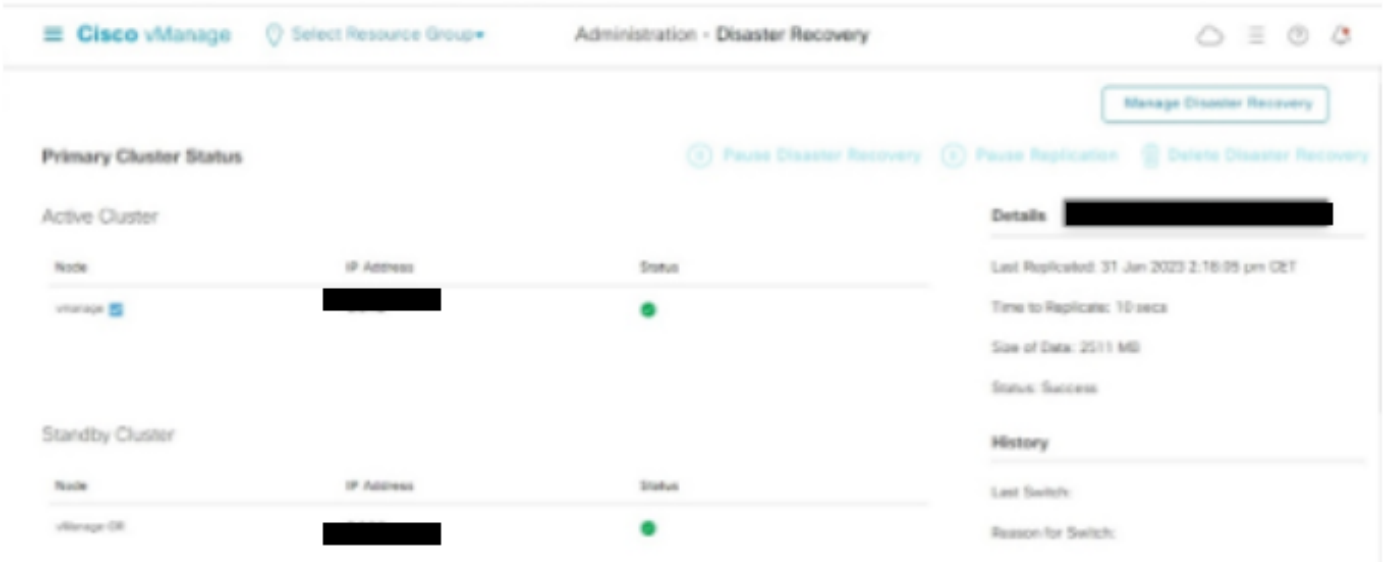


- 請注意，vManage GUI在此過程中重新啟動。
- 完成後，必須看到Success狀態。



驗證

導覽至管理→ 災難恢復檢視災難恢復狀態以及上次複製資料的時間。



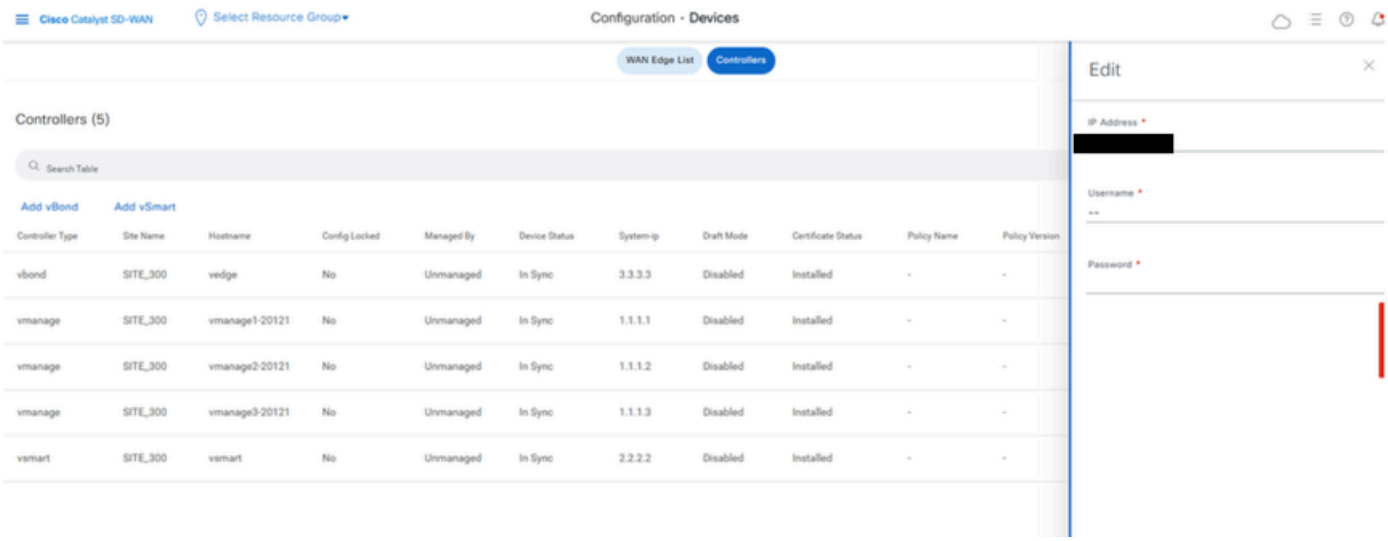
步驟 5:控制器的重新驗證和舊控制器的失效

恢復configuration-db後，我們需要重新驗證交換矩陣中的所有新控制器(vmanage/vsmart/vbond)

註：在實際生產中，如果用於重新身份驗證的介面IP是隧道介面IP，則需要確保在vManage、vSmart和vBond的隧道介面以及路徑沿途的防火牆上允許NETCONF服務。要開啟的防火牆埠是作為從DR群集到所有vBonds和vSmarts的雙向規則的TCP埠830。

在vmanage UI上，點選Configuration > Devices > Controllers

- 按一下每個控制器附近的三個點，然後按一下「Edit（編輯）」



- 將ip-address（控制器的系統ip）替換為transport vpn 0（隧道介面）ip地址。輸入使用者名稱和密碼，然後按一下save
- 對交換矩陣中的所有新控制器執行相同操作

同步根證書鏈

載入所有控制器後，完成以下步驟：

在新活動群集中的任何Cisco SD-WAN Manager伺服器上，執行以下操作：

輸入以下命令將根證書與新活動群集中的所有Cisco Catalyst SD-WAN裝置同步：

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

輸入以下命令將Cisco SD-WAN Manager UUID與Cisco SD-WAN驗證器同步：

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

在交換矩陣恢復後，交換矩陣中的所有邊緣和控制器的控制和bfd會話均已啟動，我們需要從UI使舊控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，點選Configuration > Devices > Certificates
- 按一下「Controllers（控制器）」
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。按一下「invalidate（失

效）」
- 點選send to vbond
- 在vmanage UI上，點選Configuration > Devices > Controllers
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。點選刪除(Delete)

步驟 6:過帳支票

附註：繼續使用此處顯示的「後檢查」部分，它對所有部署組合都是通用的。

組合3:vManage Cluster +無DR

所需例項：

- 3個vManage（3節點集群，所有COMPUTE_AND_DATA）或6個vManage（3個COMPUTE_AND_DATA + 3個資料）
- 1個或多個vBond
- 1個或多個vSmart

步驟:

1. 使用通用步驟調出所有例項
2. 預先檢查
3. 配置vManage UI、證書和板載控制器
4. 構建vManage群集
5. Config-db backup/restore
6. 過帳支票

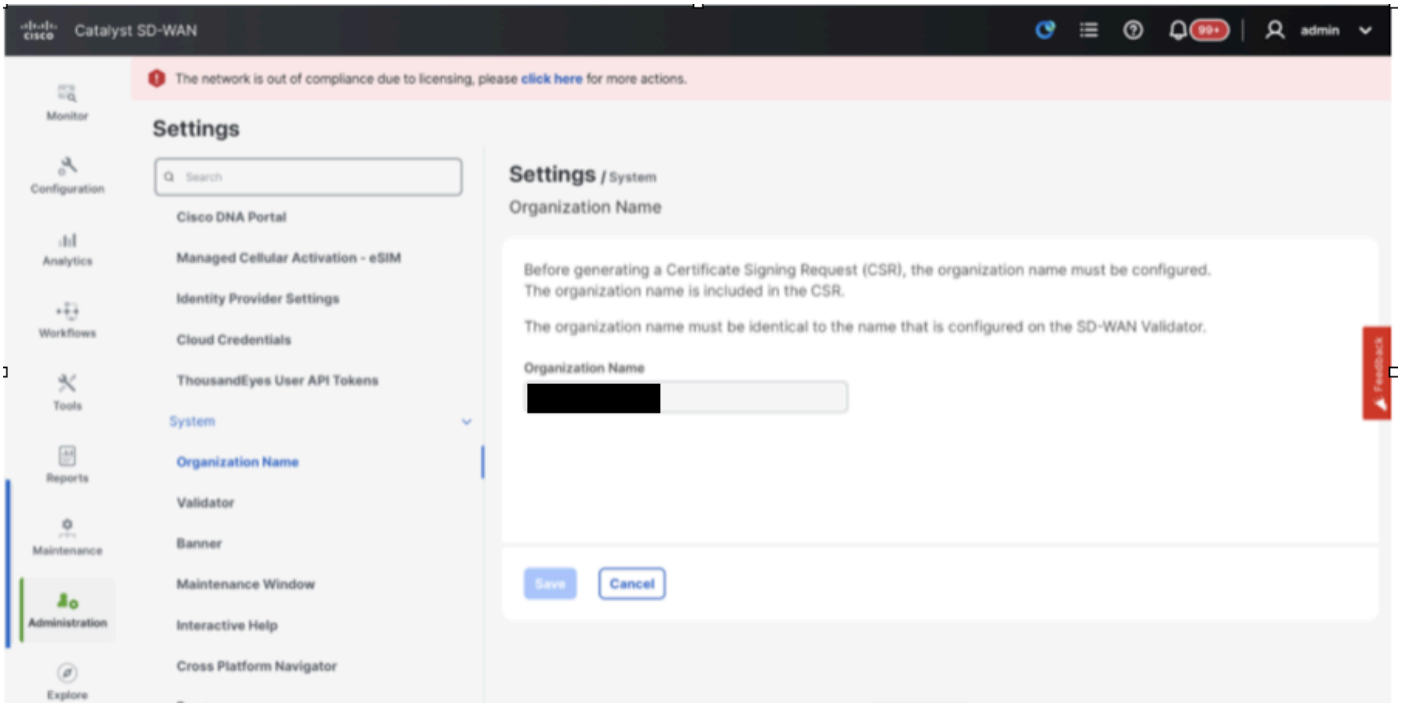
步驟 1:預先檢查

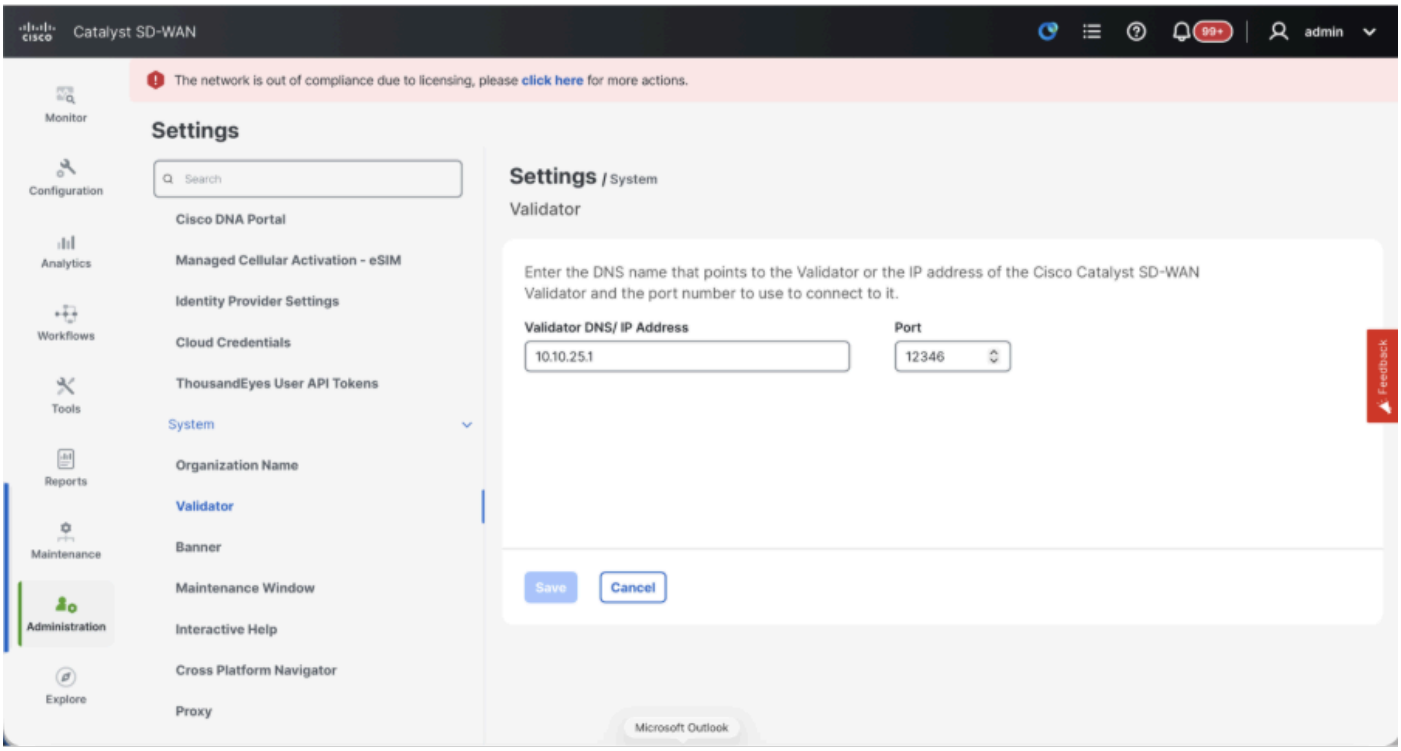
- 確保活動的Cisco SD-WAN Manager例項數與新安裝的Cisco SD-WAN Manager例項數相同。
- 確保所有活動的和新的Cisco SD-WAN Manager例項運行相同的軟體版本。
- 確保所有活動的和新的Cisco SD-WAN Manager例項都能到達Cisco SD-WAN Validator的管理IP地址。
- 確保證書已安裝在新安裝的Cisco SD-WAN Manager例項上。
- 確保所有Cisco Catalyst SD-WAN 裝置(包括新安裝的Cisco SD-WAN Manager例項)上的時鐘都同步。
- 確保在新安裝的Cisco SD-WAN Manager例項上配置一組新的系統IP和站點ID，並與活動群集配置相同的基本配置。

步驟 2:配置vManage UI、證書和板載控制器

更新vManage UI上的配置

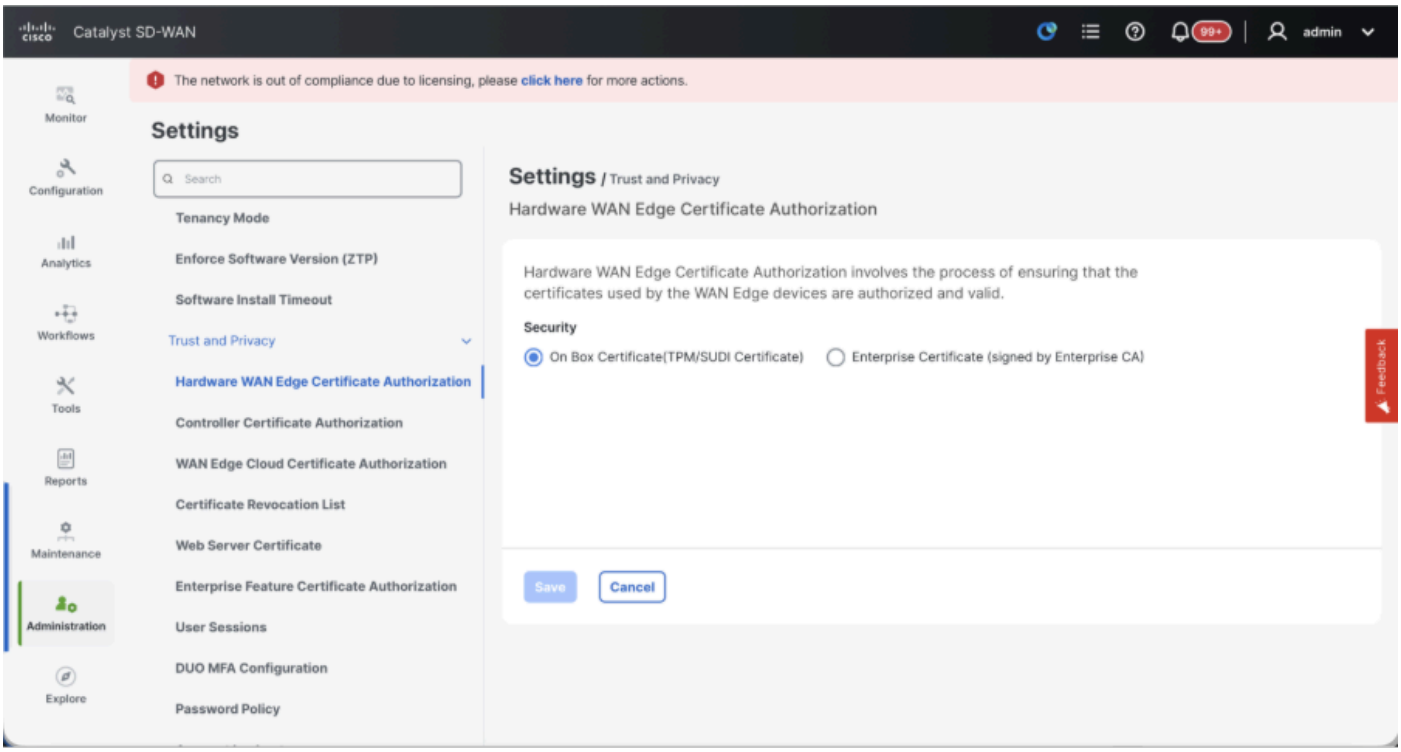
- 將步驟1中的組態新增到所有控制器的CLI上後，我們可以使用瀏覽器中的https://<vmanage-ip>URL存取vManage的WebUI。使用各個vManage節點的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 導覽至Administration > Settings，然後完成以下步驟。
- 配置組織名稱和驗證器/vBond URL/IP地址。配置與vManage節點的CLI中相同的值。
- 在vManage 20.15/20.18中，這些配置可在System部分中找到。



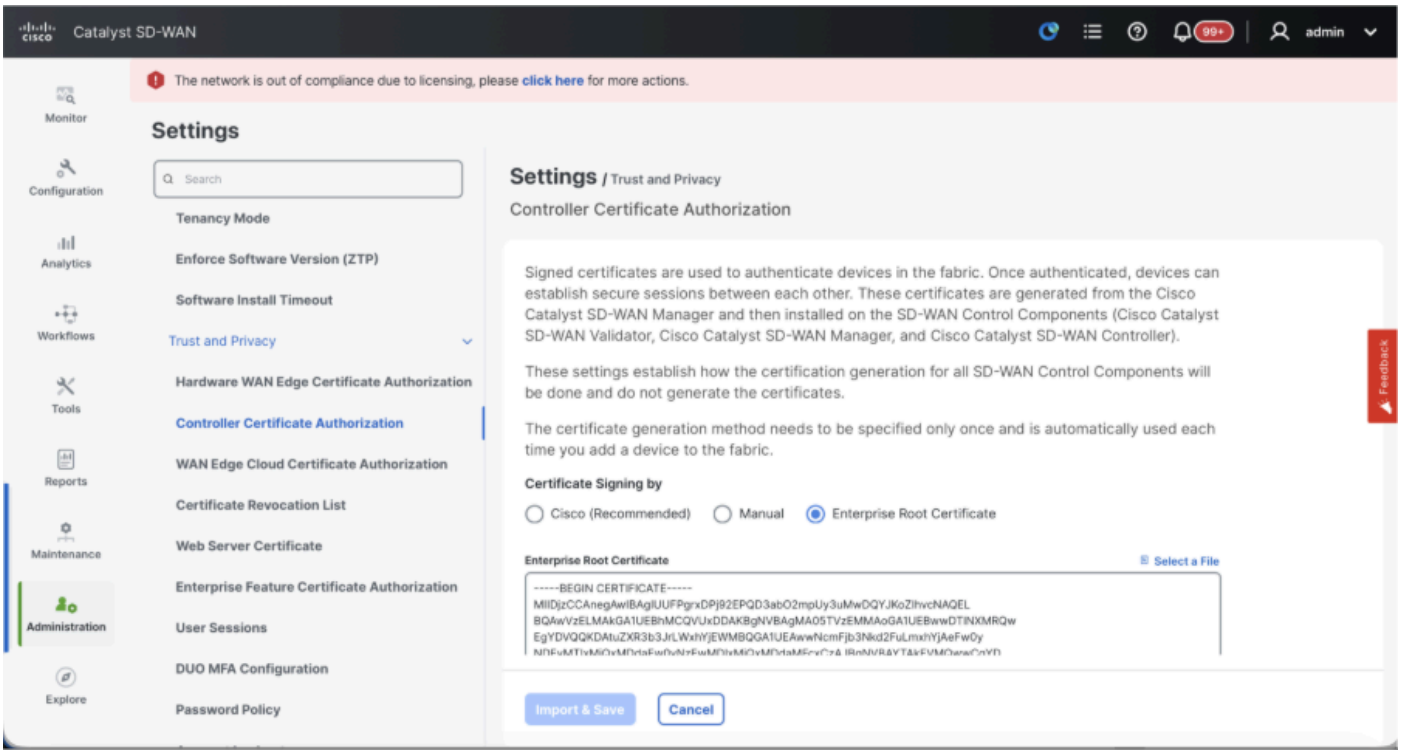


- 驗證證書授權(CA)的配置，CA決定用於簽署證書的證書授權。我們可以看到3個選項：

1. 硬體WAN邊緣證書授權 — 決定硬體SD-WAN邊緣路由器的CA。
    - 開箱證書（TPM/SUDI證書） — 使用此選項，路由器硬體上預安裝的證書用於建立控制連線（TLS/DTLS連線）
    - 企業證書（由企業CA簽署） — 使用此選項時，路由器使用由組織的企業證書頒發機構簽署的證書。選擇此選項時，必須在此處更新企業CA的根證書。

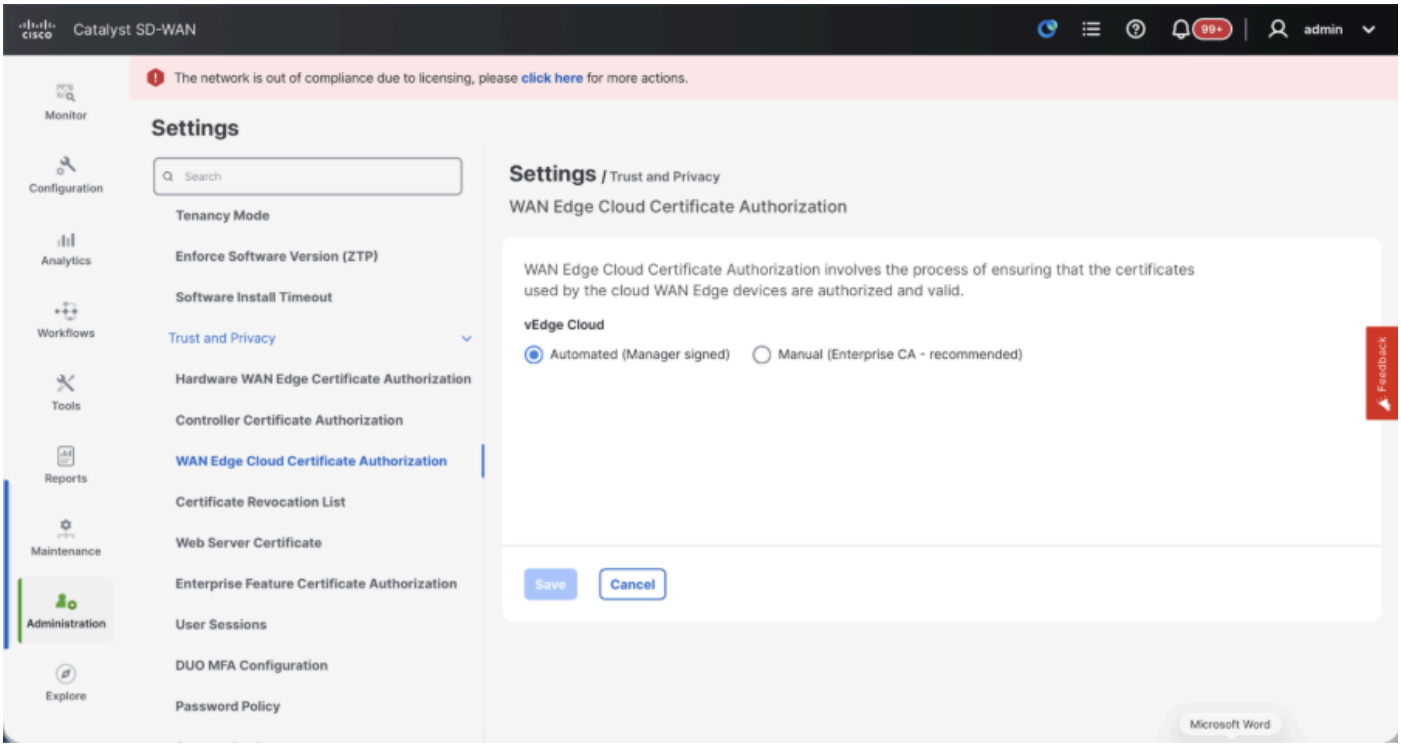


2. Controller Certificate Authorization — 決定SD-WAN控制器的CA。
    - 思科（推薦） — 控制器使用由Cisco PKI簽名的證書。vManage使用vManage上配置的智慧帳戶憑據自動聯絡PNP門戶，並簽署證書並將其安裝在控制器上。
    - 手動 — 控制器使用由Cisco PKI簽名的證書。導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
    - Enterprise Root Certificate — 使用此選項時，路由器使用由您組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。



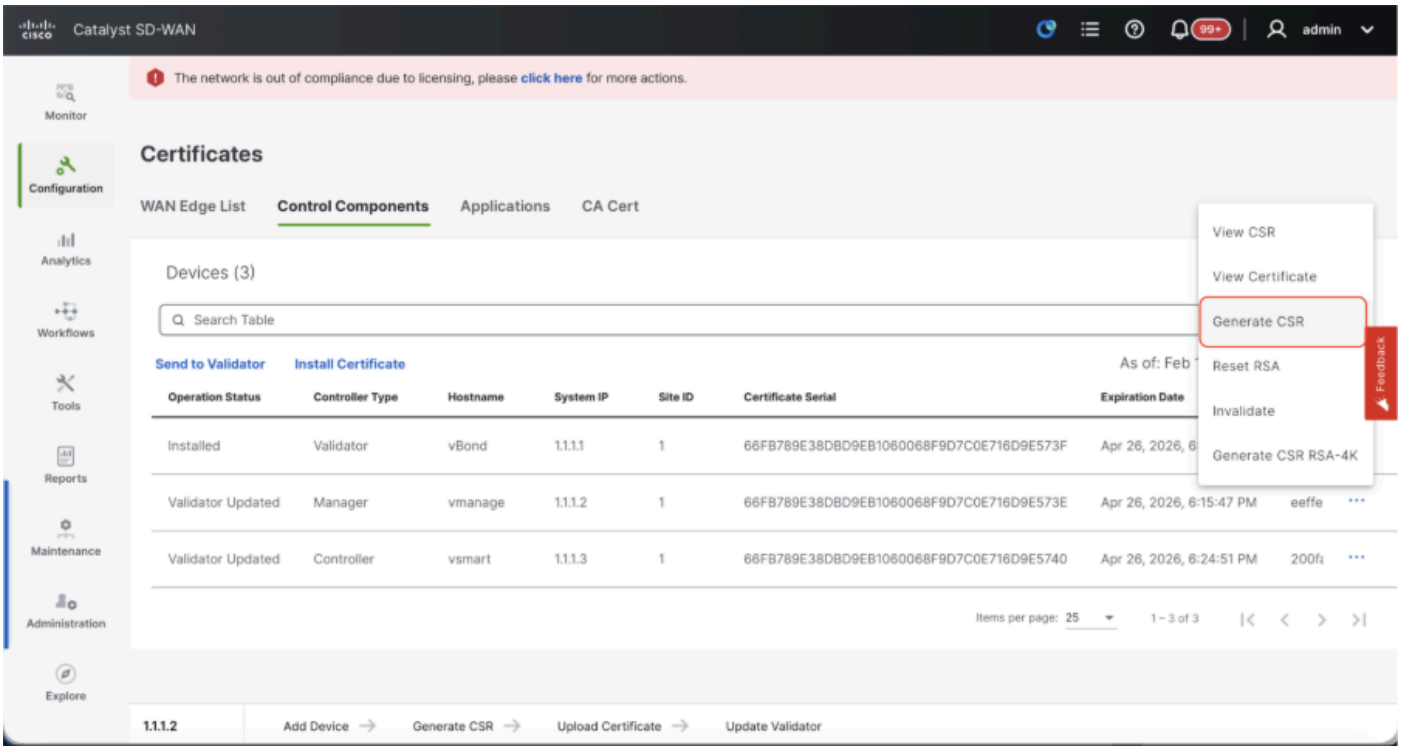
3. WAN邊緣雲證書授權 — 確定虛擬SD-WAN邊緣路由器（CSR1000v、C8000v、vEdge雲）的CA
    - 自動（vManage簽名） — vManage自動對虛擬邊緣路由器的CSR進行簽名，並在路由器上安裝證書。
    - 手動（企業CA — 推薦） — 虛擬路由器使用由組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。

如果使用CA（企業證書頒發機構），請選擇Enterprise。



- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control

Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers
- 點選Manager/vManage的……並點選Generate CSR。



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。

將vBond/Validator和vSmart/Controller註冊到vManage

如果是20.15/20.18 vManage節點，請導航到Configuration > Devices > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

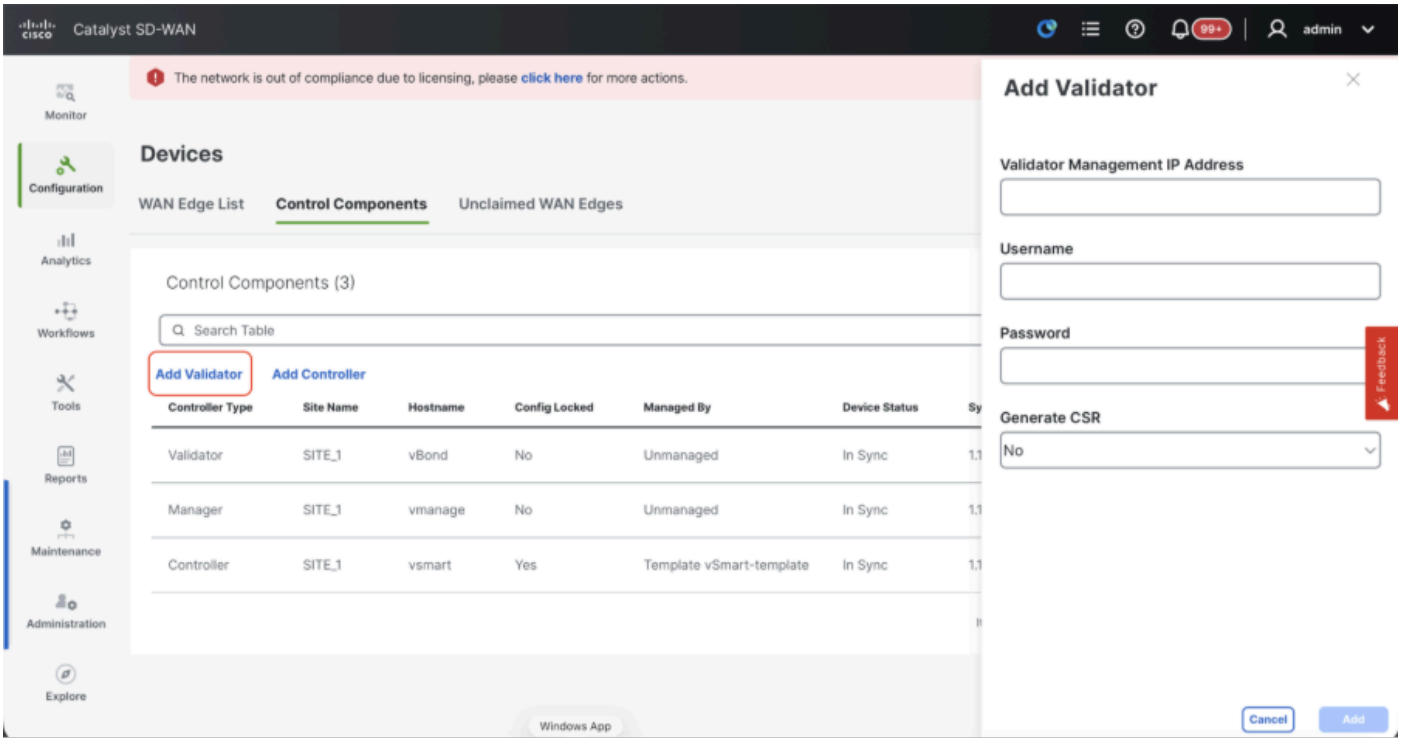
OnboardingvBond/驗證器

- 按一下AddvBond在20.12vManageor的情況下新增驗證程式在20.15/20.18 vManage的情況下。系統開啟一個彈出視窗，輸入 從vManage可訪問的vBond的VPN 0傳輸IP。
- 如果允許，請從vManagetovBondIP的CLI使用ping檢查可連接性。
- 輸入vBond的使用者憑據。

注意:我們需要使用vBondor的admin憑據作為netadmingroup的使用者部分。您可以在vBond的CLI中驗證這一點。如需安裝vBond的新憑證，請在「產生CSR」下拉式清單中選擇Yes

---

附註：如果vBond位於NAT裝置/防火牆之後，請檢查vBond VPN 0介面IP是否已轉換為公共IP。如果無法從vManage訪問VPN 0介面IP，則在此步驟中使用VPN 0介面的公用IP地址



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇思科（推薦），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vBond上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vBonds，請重複相同的步驟。

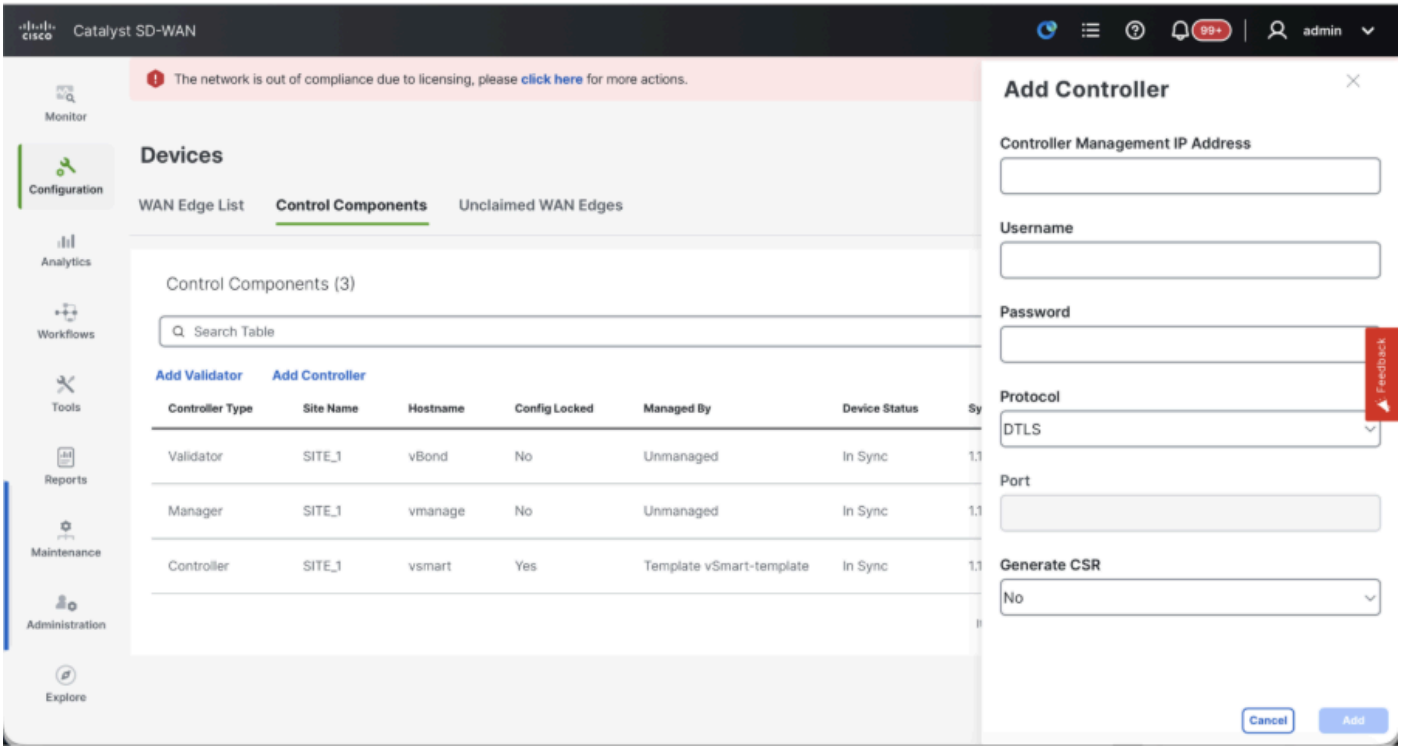
自註冊vSmart/控制器

- 在20.12 vManage的情況下按一下Add vSmart，在20.15/20.18 vManage的情況下按一下Add Controller。
- 系統開啟一個彈出視窗，輸入vSmart的VPN 0傳輸IP（可從vManage訪問）。
- 如果允許，請從vManage的CLI到vSmart IP使用ping檢查可達性。
- 輸入vSmart Note的使用者憑據，我們需要使用vSmart的管理員憑據或netadmin組的使用者部分。
- 您可以在vSmart的CLI中驗證這一點。
- 如果希望路由器使用TLS來建立與vSmart的控制連線，請將協定設定為TLS。此配置也需要在

vSmarts和vManage節點的CLI上配置。

- 如需安裝vSmart的新憑證，請在「產生CSR」下拉式清單中選擇「是」。

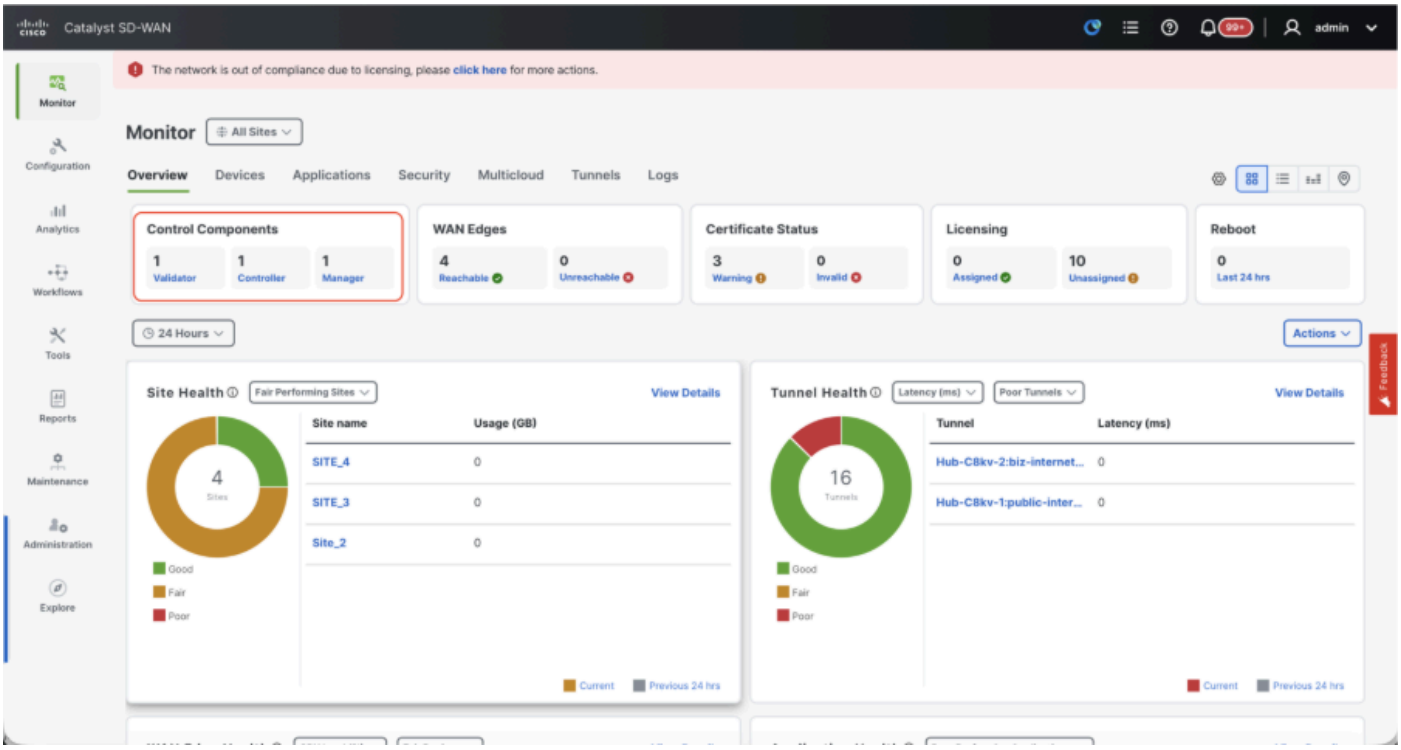
註：如果vSmart位於NAT裝置/防火牆之後，請檢查vSmart VPN 0介面IP是否已轉換為公共IP，如果無法從vManage訪問VPN 0介面IP，請在此步驟中使用VPN 0介面IP的公共IP地址。



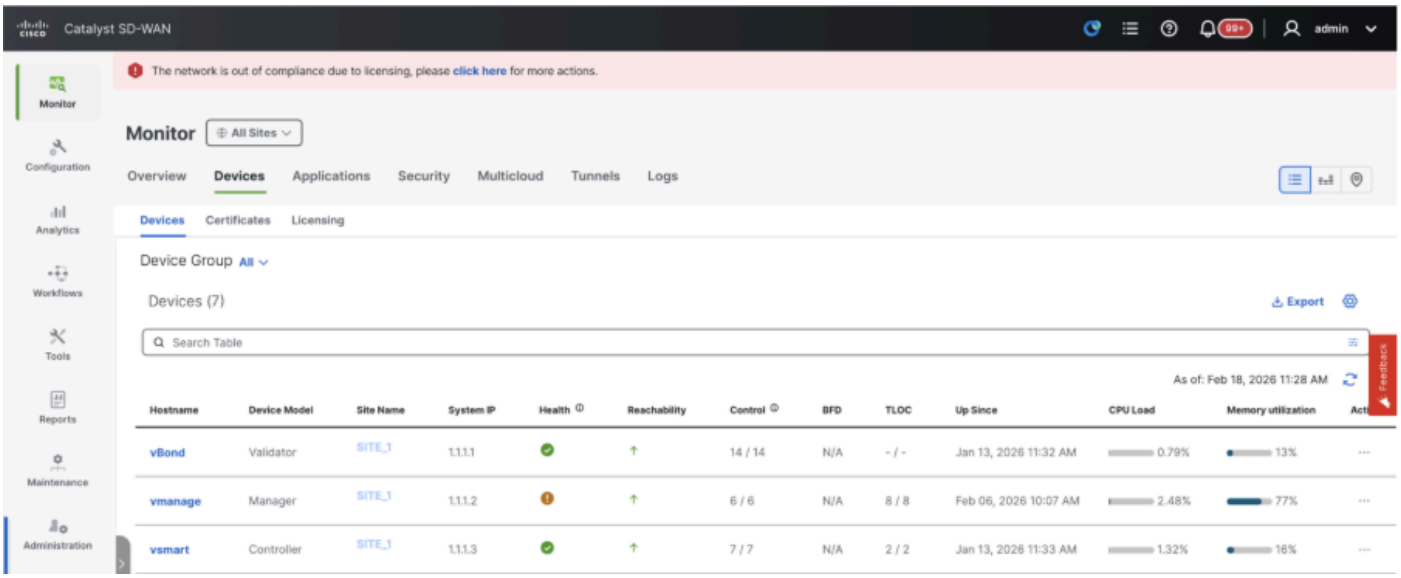
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vSmart上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vSmarts ，請重複相同的步驟。

驗證

完成所有步驟後，驗證是否可以在Monitor>Dashboard中訪問所有控制元件



- 按一下相應的控制元件，確認它們都可以訪問。
- 導覽至Monitor >Devices，確認所有控制元件均可連線。



步驟 3:構建vManage群集

板載SD-WAN交換矩陣，在SD-WAN重疊中帶有vManage集群

注意:vManage集群可以配置3個vManage節點或6個vManage節點，具體取決於註冊到SD-WAN交換矩陣的站點數量。請參考現有的vManage集群，並根據該集群選擇節點數。

配置屬於群集的所有vManage節點的CLI配置

在所有vManage節點上配置系統配置

- 配置vManage節點的其餘節點。對於3個節點集群，您有其餘2個要配置的節點；對於6個節點集群，您有5個要配置的節點。
- 配置系統配置，如下所示：

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注意:如果使用URL作為vBond地址，請確保在VPN 0配置中配置DNS伺服器IP地址或確保可以解析這些地址。

在所有vManage節點上配置傳輸介面

需要這些配置來啟用傳輸介面，該介面用於與路由器和其餘控制器建立控制連線。

```
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
```

在所有vManage節點上配置管理介面

另外配置VPN 512management介面以啟用對控制器的帶外管理訪問。

```
Conf t
```

```
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

可選配置：

- 您可以參考現有控制器的配置，如果此處列出的配置存在，您可以將此配置新增到新控制器中。
- 僅當需要路由器使用TLS與vManage節點建立安全控制連線時，才將控制協定配置為TLS。預設情況下，所有控制器和路由器都使用DTLS建立控制連線。根據您的要求，此可選配置僅在vSmart和vManage節點上需要。

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

在所有vManage節點上配置服務介面

在已登入的所有vManagenodes（包括vManage-1）上配置服務介面。此介面用於集群通訊，表示集群中vManagenodes之間的通訊。

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

確保同一IP子網用於vManagecluster中所有節點上的服務介面。

配置群集憑據

我們可以使用vManagenodes的相同管理憑據來配置vManagecluster。否則，我們可以配置作為netadmingroup一部分的新使用者憑據。配置新使用者憑據的配置如下所示

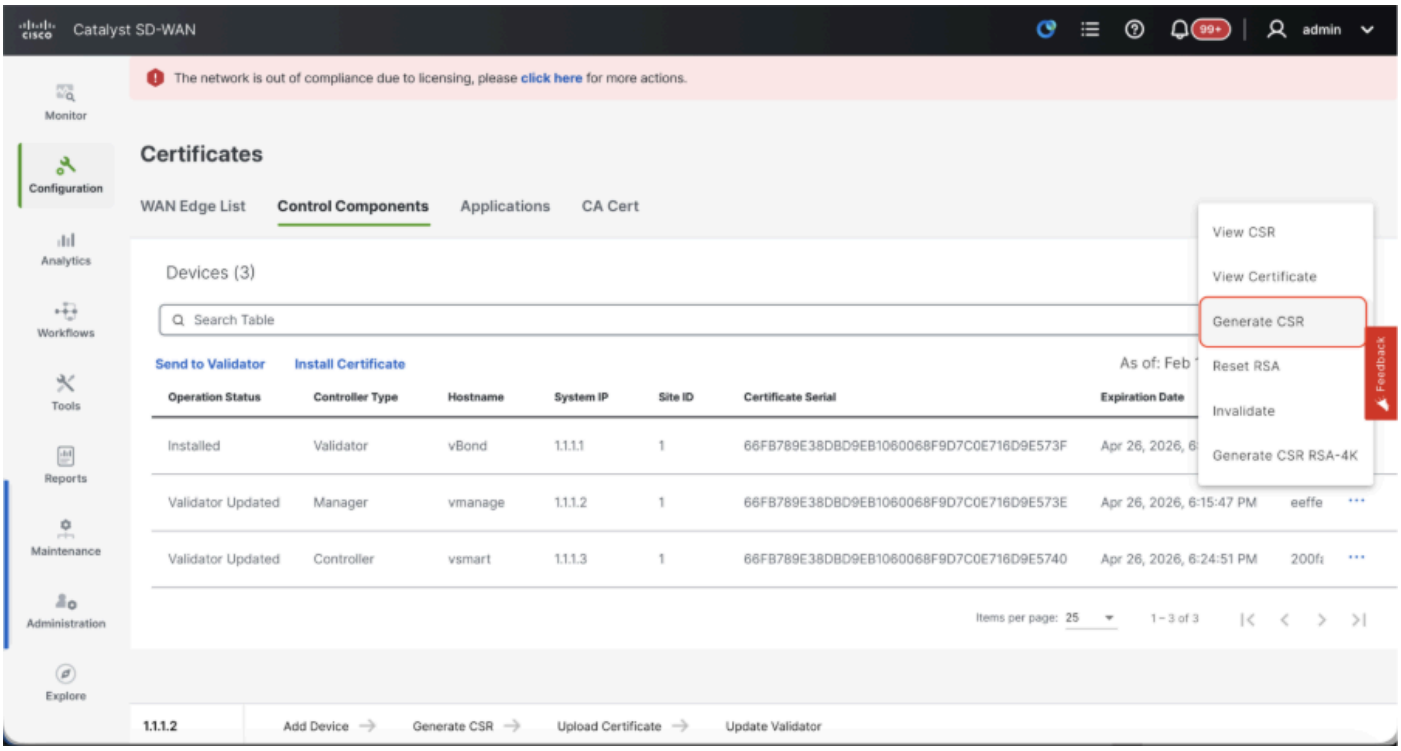
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

確保在屬於群集的所有vManagenode上配置相同的使用者憑據。如果我們決定使用管理員憑據，則必須在所有vManagenode上配置相同的使用者名稱/密碼。

在所有vManage節點上安裝裝置證書

- 使用瀏覽器中的URL https://<vmanage-ip>登入所有vManagenodes的tovManageUI。使用各自的vManagenodes的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

  按一下Manager/vManage的……並按一下Generate CSR。



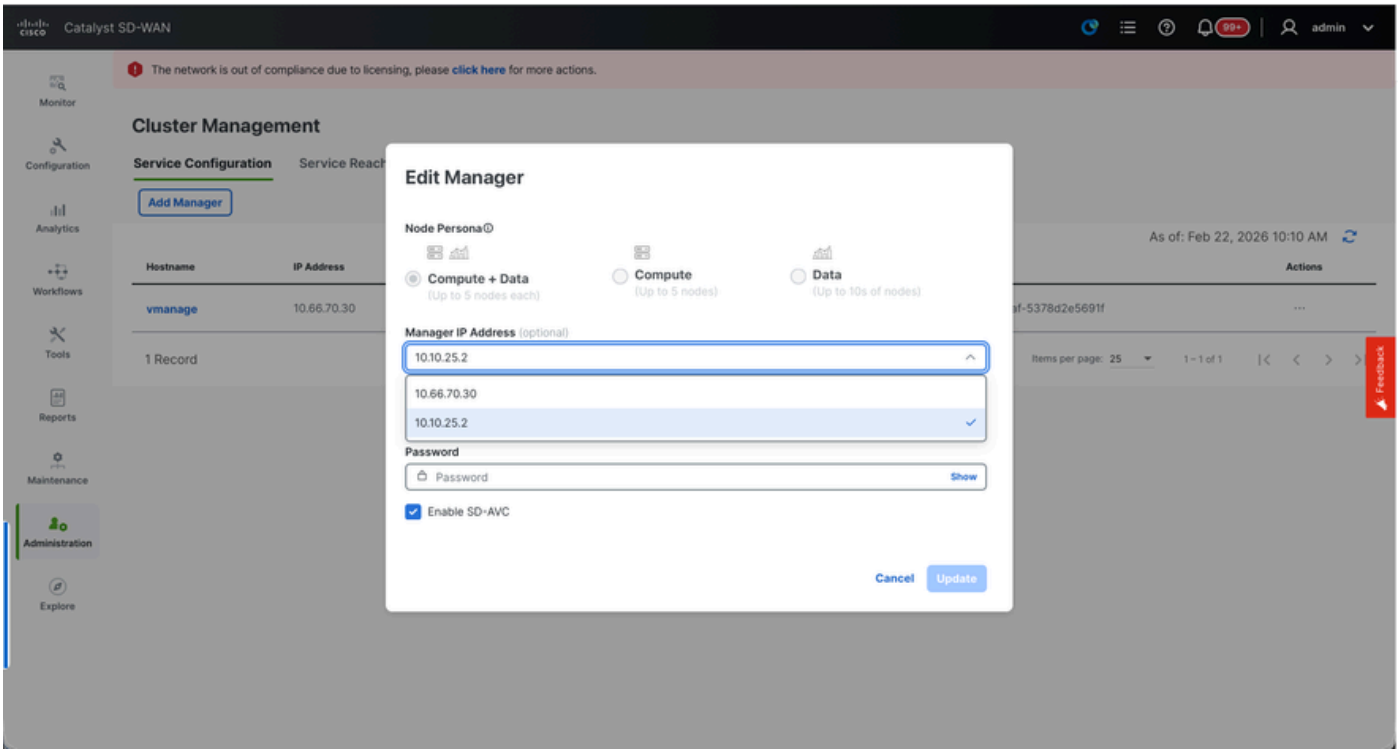
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，以使用思科PNP門戶手動簽署CSR。如果使用Digicert和企業根證書，則適用相同的程式。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 跨屬於群集的所有vManage節點完成此步驟。

準備構建vManage群集

- 在vManage-1的WebUI上，導航到Administration > Cluster Management，在vManage-1的Actions下按一下……，然後選擇Edit。
- 在虛擬機器啟動時，根據我們選擇的角色自動選擇節點角色。

附註：對於一個3節點群集，所有3個vManage節點都以compute+data作為角色。

- 對於6節點群集，3個vManage節點將compute+data作為角色建立，3個vManage節點將資料作為角色建立。
- 從Manager IP地址下拉選單中，確保選擇vManage的服務接口IP。

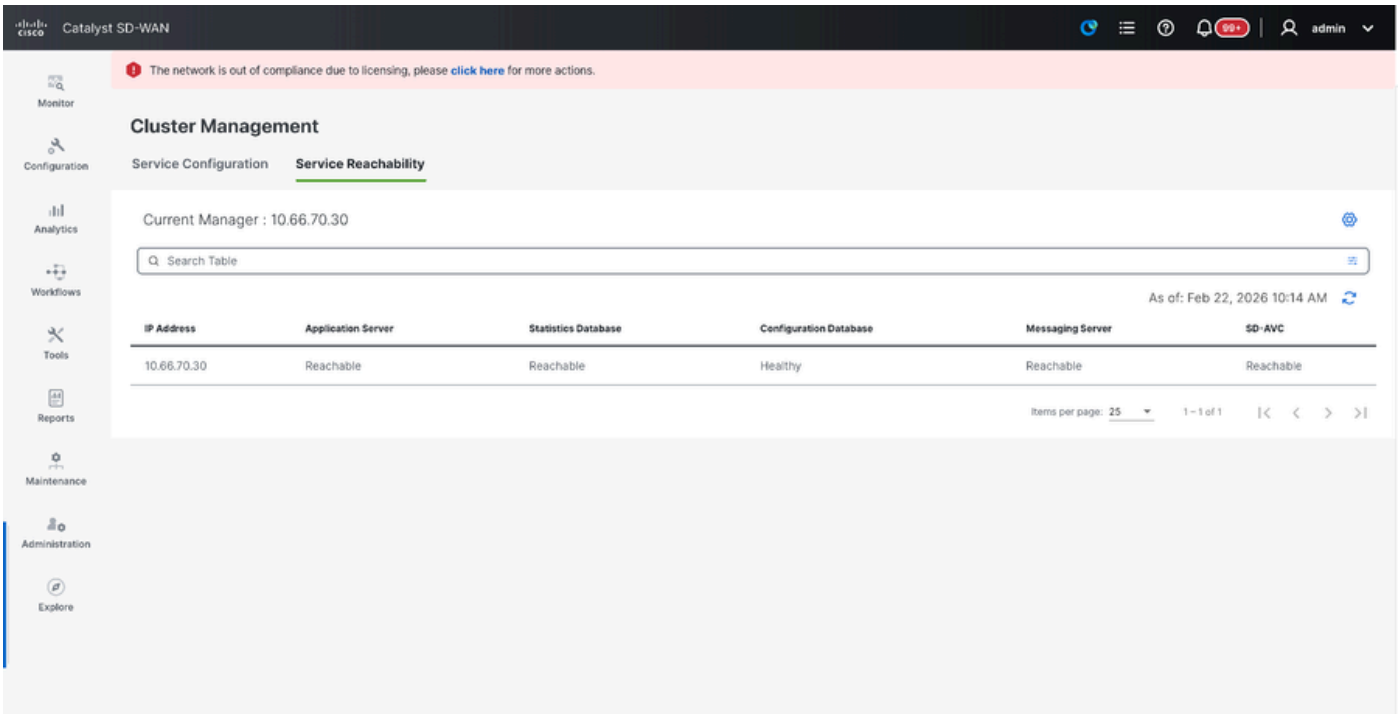


- 輸入我們希望用來啟用vManage群集的使用者名稱和密碼，該群集稱為群集憑據。
- 如前所述，必須在所有vManage節點上配置相同的憑證，並且在將所有節點新增到群集時必須使用相同的憑證。

附註：請參考現有群集中的此配置以啟用SDAVC — 僅當需要並且僅需要在群集的一個vManage節點上時，才需要選中。

按一下「更新」。

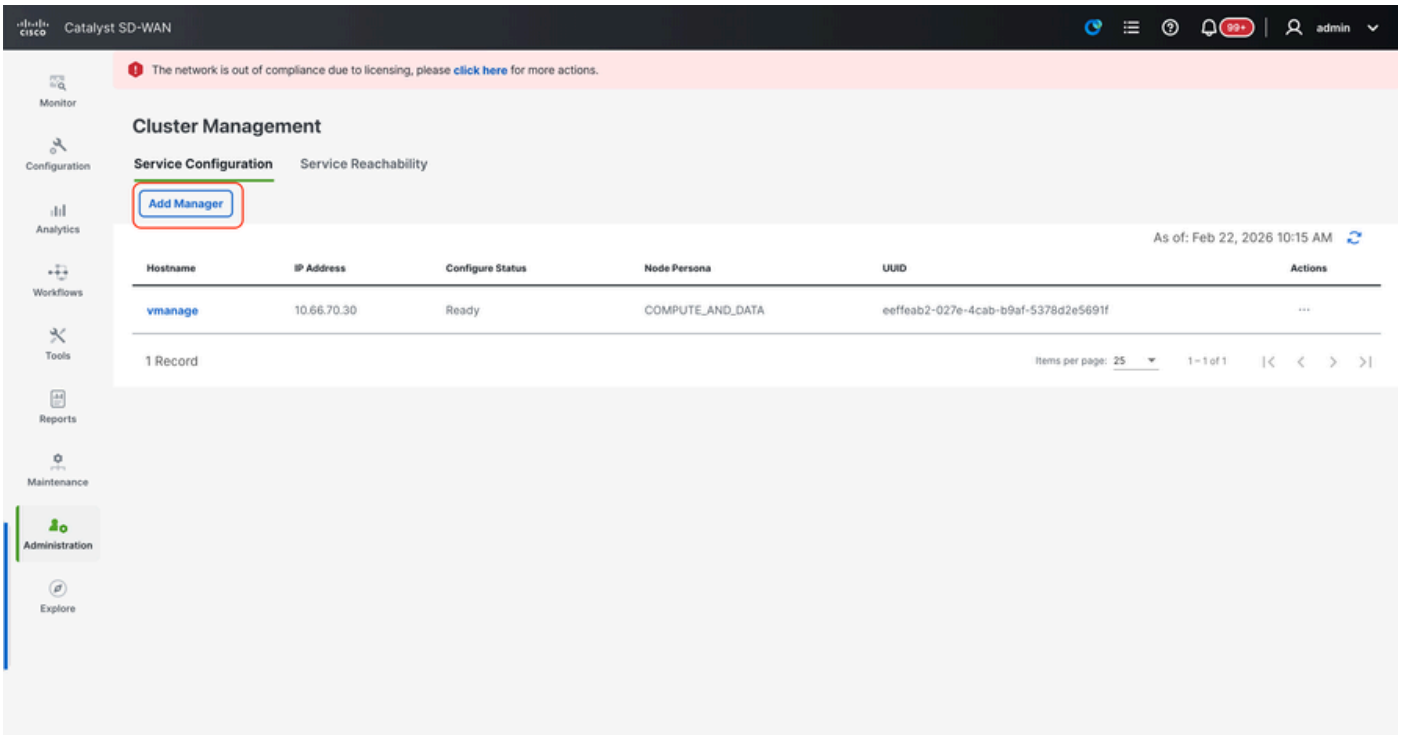
- 發佈此消息後，vManage NMS服務在後台重新啟動，該UI在大約5至10分鐘的時間內不可用。在此期間，可使用vManage的CLI訪問。
- 在vManage-1 UI可以訪問之後，導航到Administration > Cluster Management，確保vManage的服務介面IP反映在IP地址下，配置狀態為就緒且正確反映節點角色。
- 切換至同一頁面中的「服務可接通性」部分，並確保所有服務均可訪問。

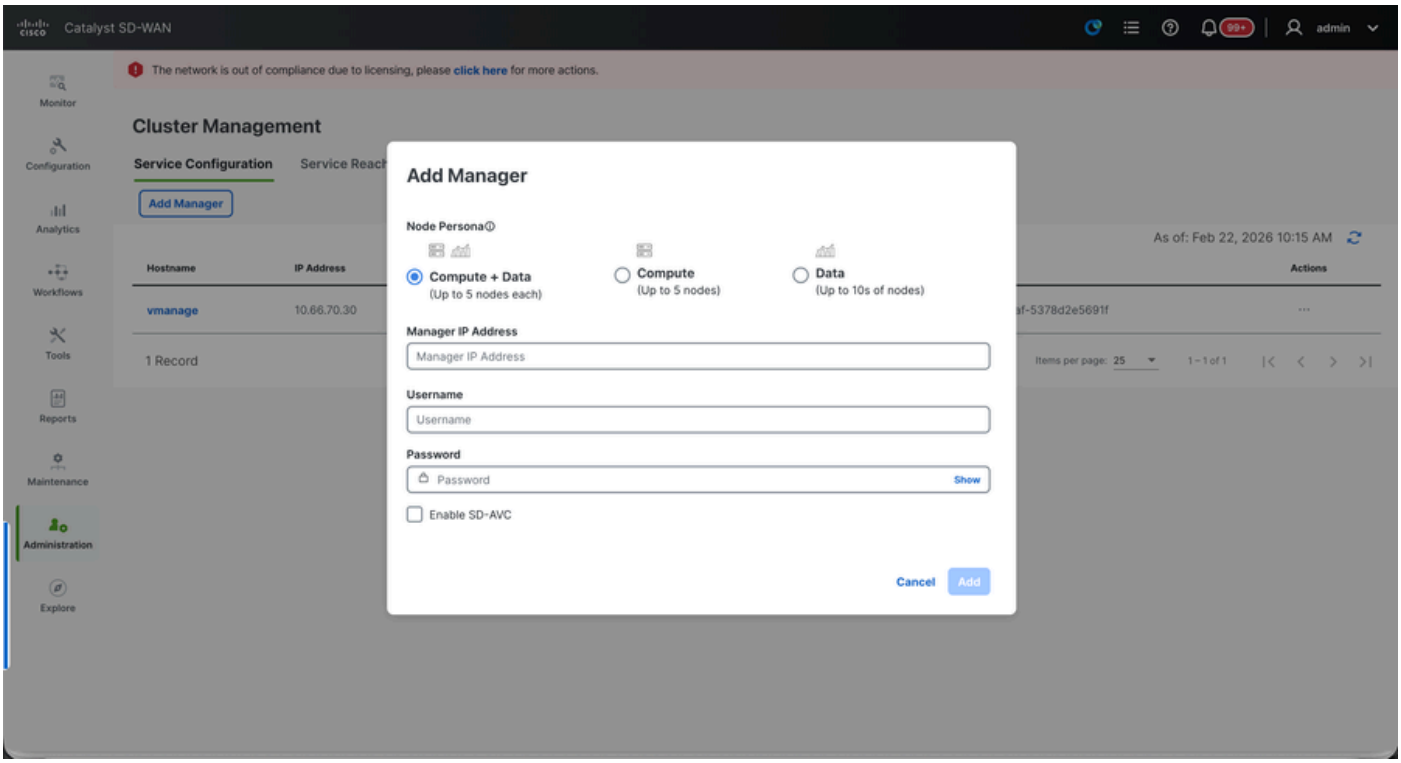


- 如果尚未看到任何服務，請稍候。通常需要20到30分鐘。

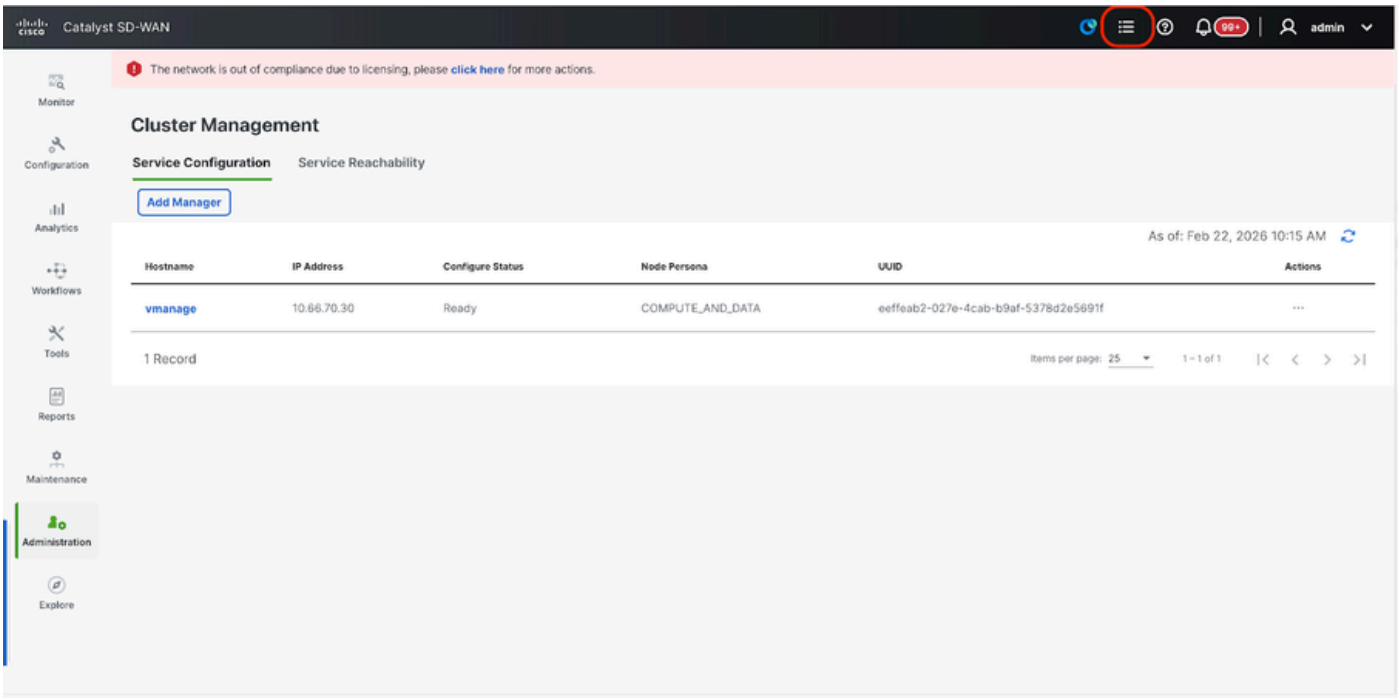
構建vManage群集

- 在vManage-1的WebUI上，導航到Administration > Cluster Management，在Service Configuration部分中，
- 按一下Add Manager，出現一個彈出視窗：





- 根據在vManage - 2節點旋轉時完成的角色配置選擇節點角色。
- 在Manager IP地址下輸入vManage-2的服務介面IP
- 輸入使用者名稱和密碼，該使用者名稱和密碼與我們在步驟6中使用的憑據相同。
- 啟用SDAVC — 保持未選中狀態，因為我們會在vManage-1上啟用它
- 點選Add。
- 之後，vManage 1和2節點的vManage NMS服務在後台重新啟動。對於vManage 1和2，該UI的可用時間大約為5到10分鐘。
- 在此期間，可使用vManage 1和2的CLI訪問。
- 可以訪問vManage-1 UI後，請導航至Administration > Cluster Management，確保vManage和vManage的服務介面IP反映在IP地址下，Configure Status is Ready且節點角色反映正確。
- 切換到同一頁中的「服務可接通性」部分，並確保兩個vManage節點的所有服務均可訪問。
- 如果尚未看到任何服務，請稍候。通常需要5到10分鐘。
- 您可以在vManage UI右上角的Task-list中檢查集群新增進程的狀態。



- 您可以查詢「活動」任務清單，如果該任務仍列在「活動」任務清單下，則表示該任務尚未完成。
- 您可以按一下該任務檢查其進度。如果該任務未列在「活動」任務清單下，請切換到「已完成」並確保任務成功完成。
- 只有在這些點經過驗證後，才能繼續下一步。

將下一個節點新增到群集之前，需要考慮以下幾點:

請在已新增到群集的所有vManage節點的UI上驗證這些點：

- 導航到Monitor > Overview of vManage UI，確保正確反映了vManage節點的數量，且根據新增到群集的節點數量可以看到。

- 導航到Administration > Cluster Management，並確保兩個vManage的服務介面IP都反映在IP地址下，Configure Status is Ready且節點角色正確反映。
- 切換到同一頁中的「服務可接通性」部分，並確保兩個vManage節點的所有服務均可訪問。

- 每次向群集中新增節點時，群集中所有節點的NMS服務都會重新啟動，因此在一段時間內，這些節點的UI將變得不可達。
- 根據群集中的節點數，可能需要較長的時間才能備份UI以及訪問所有服務。
- 您可以在vManage UI右上角的Task-list下監視任務。
- 在新增到群集的每個節點的vManage UI上，我們需要檢視所有路由器、模板和策略（如果它們在vManage-1中可用）。
- 如果這些配置不存在於vManage-1上，則新增到vManage-1中的vBonds和vSmarts以及組織— 名稱、vBond、證書授權的管理>設定配置必須反映在新增到群集的其餘vManage節點上。

- 對其餘vManage節點重複相同步驟。

載入所有控制器後，完成以下步驟：

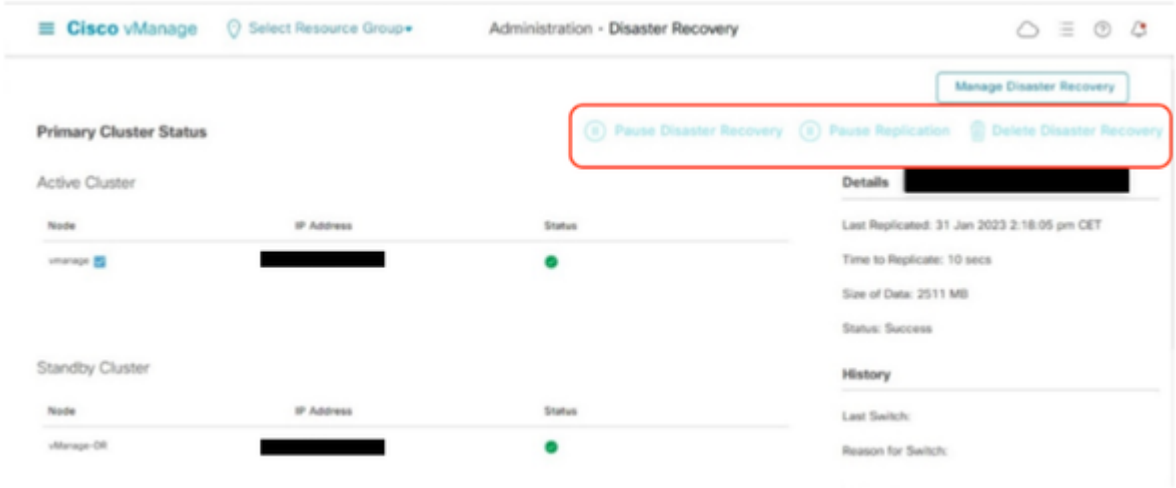
步驟 4:Config-db備份/還原

在另一個vManage節點上收集vManage configuration-db備份和還原

附註：從已啟用災難恢復的現有vManage群集收集配置資料庫備份時，請確保在該節點上的災難恢復暫停並刪除後收集該備份。

確認沒有正在進行的災難恢復複製。導航到管理>災難恢復和 確保狀態為「成功」，而不是處於「匯入掛起」、「匯出掛起」或「下載掛起」等暫時狀態。如果狀態不成功，請聯絡Cisco TAC並確保複製成功，然後繼續暫停災難恢復。

首先暫停災難恢復並確保任務完成。然後刪除災難恢復並確認任務已完成。



聯絡Cisco TAC，確保已成功清理災難恢復。

收集Configuration-DB備份：

- 在當前正在使用的SD-WAN交換矩陣中，可以從vManage群集生成配置資料庫備份。
- 請注意，我們只能在vManage群集中的一個節點（該節點是configuration-db領導者）上生成configuration-db備份。

- 對於獨立vManage，該vManage本身是配置資料庫的領導者。
- 在vManage群集中，使用命令request nms configuration-db diagnostics標識configuration-db領導節點。您可以在3節點vManage群集的所有節點上運行此命令。
- 在6節點集群中，確保在啟用了configuration-db的vManage節點上運行此命令，以標識領導節點。 導覽至Administration > Cluster Management以驗證相同內容：
- 如螢幕截圖所示，配置了persona COMPUTE_AND_DATA的節點正在運行configuration-db。

您可以在vManageCLI上使用requestnmsconfiguration-dbstatus命令進行驗證。輸出如下

```
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#
```

- 一旦您執行命令請求nms configuration-db對這些節點進行診斷，輸出如下：
- 查詢「IsLeader」的突出顯示的欄位。如果設定為1，則表示節點是領導節點，我們可以從中收集配置資料庫備份。

```
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     .
```

使用此命令從標識的configuration-db領導vManage節點收集configuration-db備份。

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

預期輸出如下：

```
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#
```

- 如果已更新configuration-db憑證，請記下該憑證。
- 如果您不知道配置資料庫憑據，請聯絡TAC以從現有vManage節點檢索配置資料庫憑據。

- 預設的configuration-db憑證是使用者名稱：neo4j和密碼：密碼

將Configuration-db備份還原到另一個vManage節點

使用SCP將configuration-db backup複製到vManage的/home/admin/目錄。

scp命令輸出示例：

```
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
```

要恢復configuration-db備份，首先需要配置configuration-db憑據。如果您的配置資料庫憑據是預設值(neo4j/password)，則可以跳過此步驟。

要配置configuration-db憑據，請使用request nms configuration-db update-admin-user命令。使用您選擇的使用者名稱和密碼。

請注意，vManage的應用程式伺服器已重新啟動。由於vManage UI將在短時間內不可訪問。

```
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#
```

可以繼續還原配置資料庫備份的開機自檢：

我們可以使用命令request nms configuration-db restore path /home/admin/< >將configuration-db還原到新的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
```

恢復configuration-db後，確保vManage UI可訪問。等待約5分鐘，然後嘗試訪問UI。

成功登入到UI後，請確保邊緣路由器清單、模板、策略以及以前或現有vManage UI上存在的所有其餘配置都反映在新的vManage UI上。

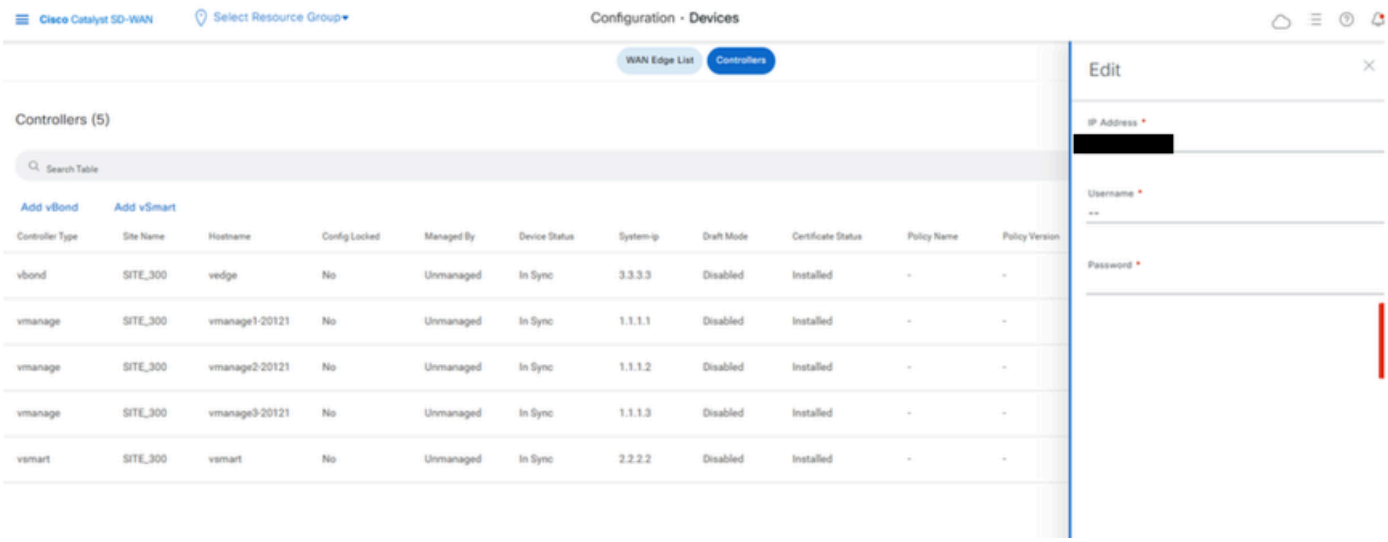
步驟 5:控制器的重新驗證和舊控制器的失效

恢復configuration-db後，我們需要重新驗證交換矩陣中的所有新控制器(vmanage/vsmart/vbond)

註：在實際生產中，如果用於重新身份驗證的介面IP是隧道介面IP，則需要確保在vManage、vSmart和vBond的隧道介面以及路徑沿途的防火牆上允許NETCONF服務。要開啟的防火牆埠是作為從DR群集到所有vBonds和vSmarts的雙向規則的TCP埠830。

在vmanage UI上，點選Configuration > Devices > Controllers

- 按一下每個控制器附近的三個點，然後按一下「Edit（編輯）」



- 將ip-address（控制器的系統ip）替換為transport vpn 0（隧道介面）ip地址。輸入使用者名稱和密碼，然後按一下save
- 對交換矩陣中的所有新控制器執行相同操作

同步根證書鏈

載入所有控制器後，完成以下步驟：

在新活動群集中的任何Cisco SD-WAN Manager伺服器上，執行以下操作：

輸入以下命令將根證書與新活動群集中的所有Cisco Catalyst SD-WAN裝置同步：

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

輸入以下命令將Cisco SD-WAN Manager UUID與Cisco SD-WAN驗證器同步：

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

在交換矩陣恢復後，交換矩陣中的所有邊緣和控制器的控制和bfd會話均已啟動，我們需要從UI使舊控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，點選Configuration > Devices > Certificates
- 按一下「Controllers（控制器）」
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。按一下「invalidate（失效）」
- 點選send to vbond
- 在vmanage UI上，點選Configuration > Devices > Controllers
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。點選刪除(Delete)。

步驟 6:過帳支票

附註：繼續使用此處顯示的「後檢查」部分，它對所有部署組合都是通用的。

組合4:vManage Cluster +手動/冷備份DR

什麼是手動/冷備份DR — 備份SD-WAN Manager伺服器或SD-WAN Manager群集在冷備份狀態下保持關閉。

對活動資料庫進行常規備份，如果主SD-WAN Manager或SD-WAN Manager群集關閉，則手動啟動備用SD-WAN Manager或SD-WAN Manager群集，並在其上恢復備份資料庫。

所需例項：

- 3或6個vManage（主群集）
- 3或6個vManage（DR備用群集）
- 1個或多個vBond（分佈於主資料中心和DR資料中心）
- 1個或多個vSmart（分佈於主資料中心和DR資料中心）

步驟:

1. 使用通用步驟調出所有例項
2. 預先檢查

3. 配置vManage UI、證書和板載控制器
4. 構建vManage群集
5. 冷備用DR群集設定
6. Config-db backup/restore
7. 過帳支票

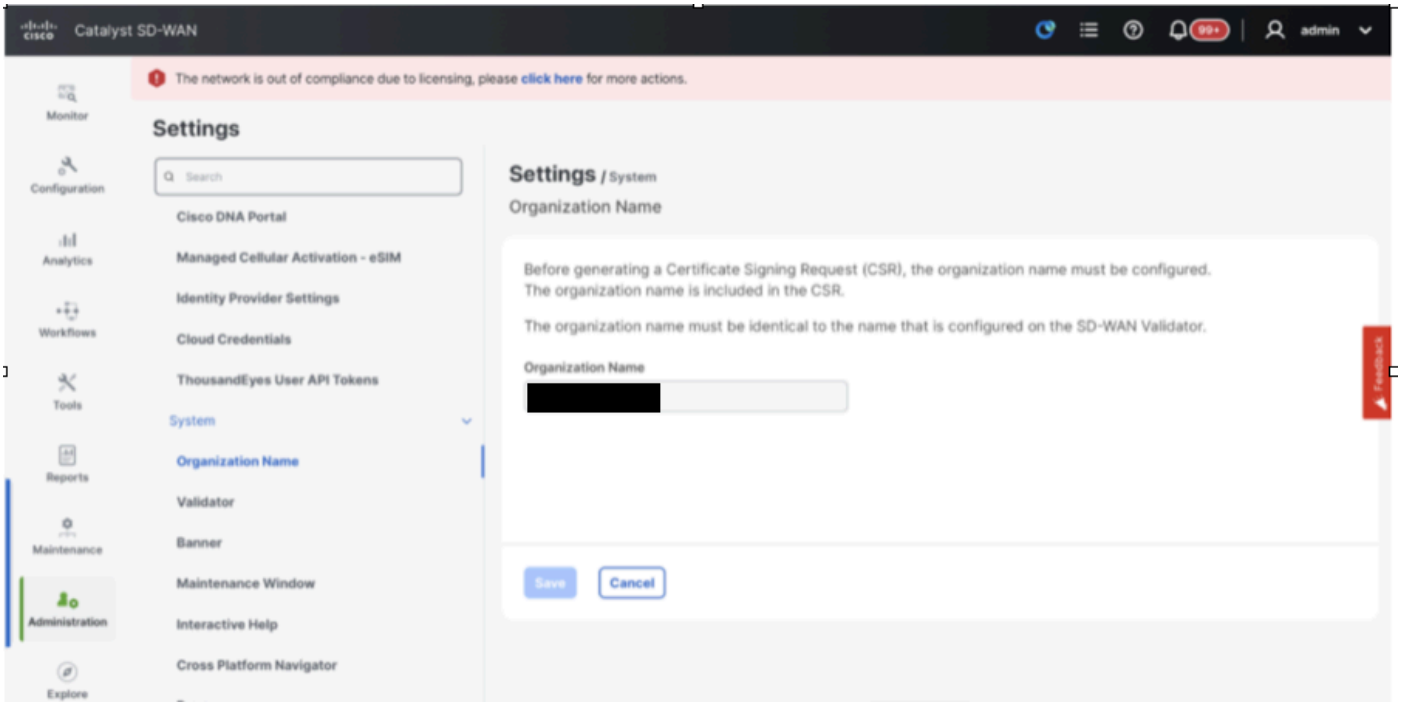
步驟 1:預先檢查

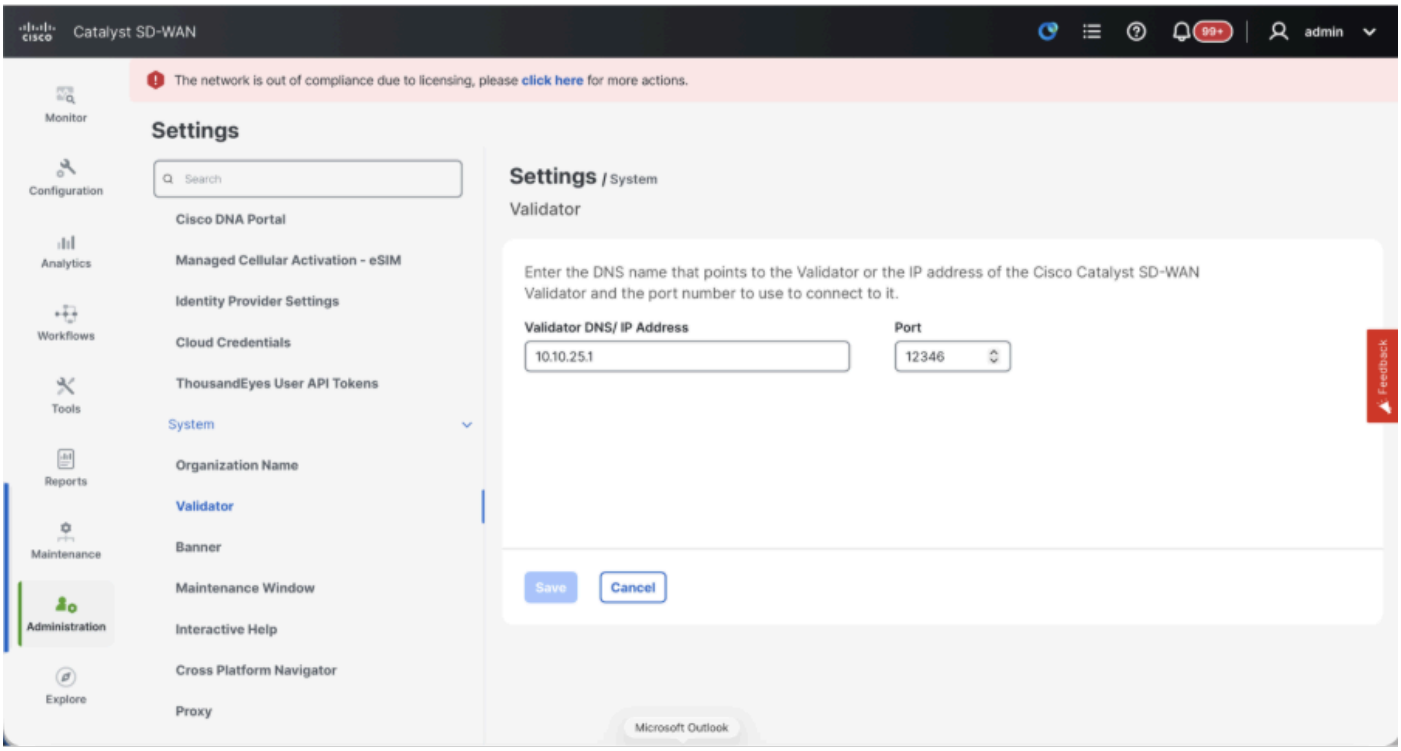
- 確保活動的Cisco SD-WAN Manager例項數與新安裝的Cisco SD-WAN Manager實例數相同。
- 確保所有活動的和新的Cisco SD-WAN Manager例項運行相同的軟體版本。
- 確保所有活動的和新的Cisco SD-WAN Manager例項都能到達Cisco SD-WAN Validator的管理IP地址。
- 確保證書已安裝在新安裝的Cisco SD-WAN Manager例項上。
- 確保所有Cisco Catalyst SD-WAN 裝置(包括新安裝的Cisco SD-WAN Manager例項)上的時鐘都同步。
- 確保在新安裝的Cisco SD-WAN Manager例項上配置一組新的系統IP和站點ID，並與活動群集配置相同的基本配置。

步驟 2:配置vManage UI、證書和板載控制器

更新vManage UI上的配置

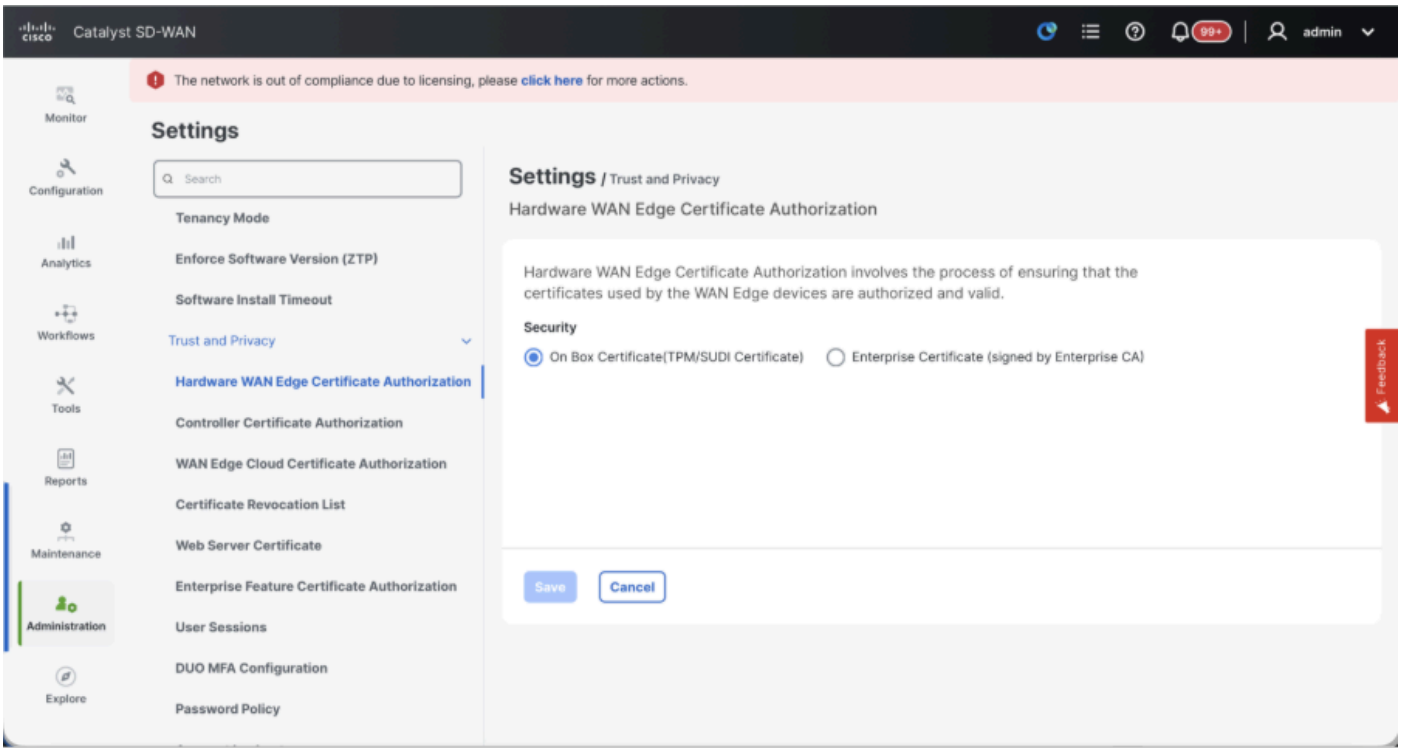
- 將步驟1中的組態新增到所有控制器的CLI上後，我們可以使用瀏覽器中的https://<vmanage-ip>URL存取vManage的WebUI。使用各個vManage節點的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 導覽至Administration > Settings，然後完成以下步驟。
- 配置組織名稱和驗證器/vBond URL/IP地址。配置與vManage節點的CLI中相同的值。
- 在vManage 20.15/20.18中，這些配置可在System部分中找到。



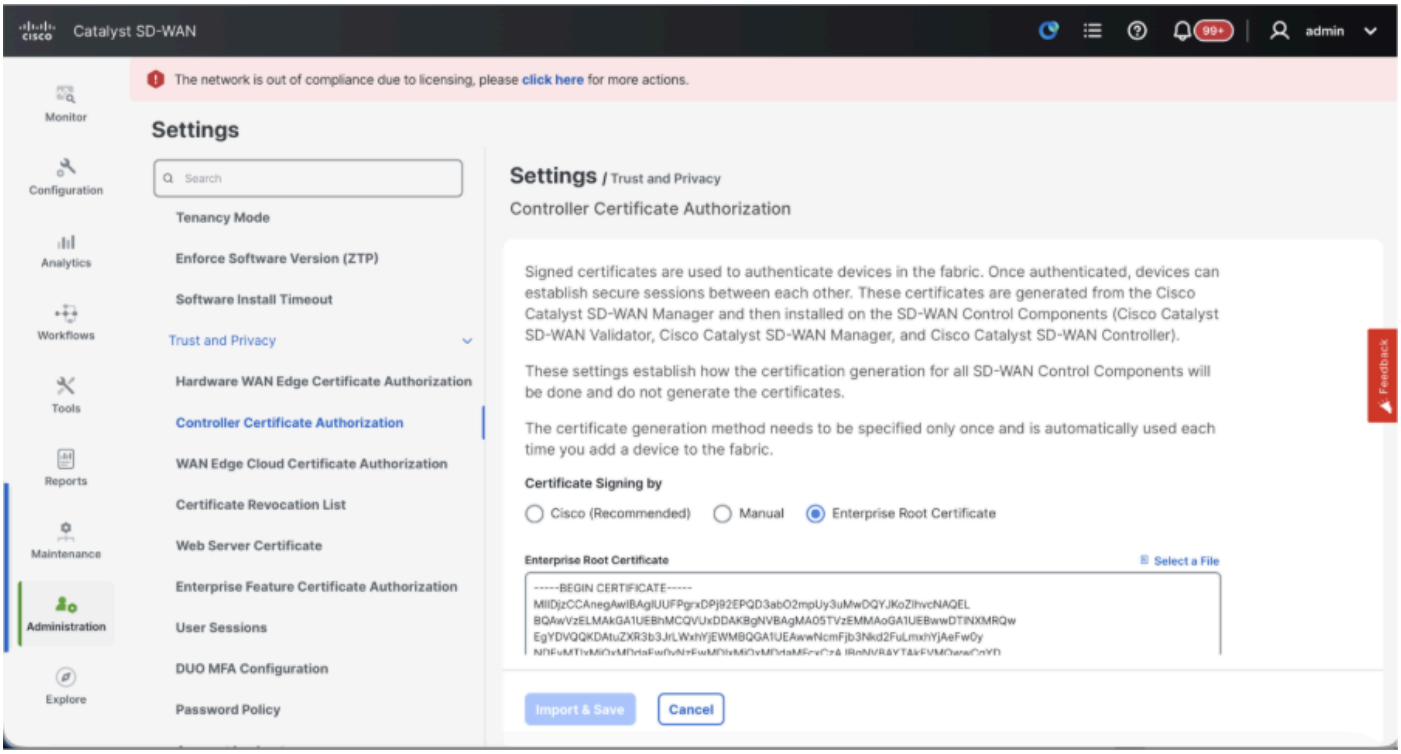


- 驗證證書授權(CA)的配置，CA決定用於簽署證書的證書授權。我們可以看到3個選項：

1. 硬體WAN邊緣證書授權 — 決定硬體SD-WAN邊緣路由器的CA。
    - 開箱證書（TPM/SUDI證書） — 使用此選項，路由器硬體上預安裝的證書用於建立控制連線（TLS/DTLS連線）
    - 企業證書（由企業CA簽署） — 使用此選項時，路由器使用由組織的企業證書頒發機構簽署的證書。選擇此選項時，必須在此處更新企業CA的根證書。



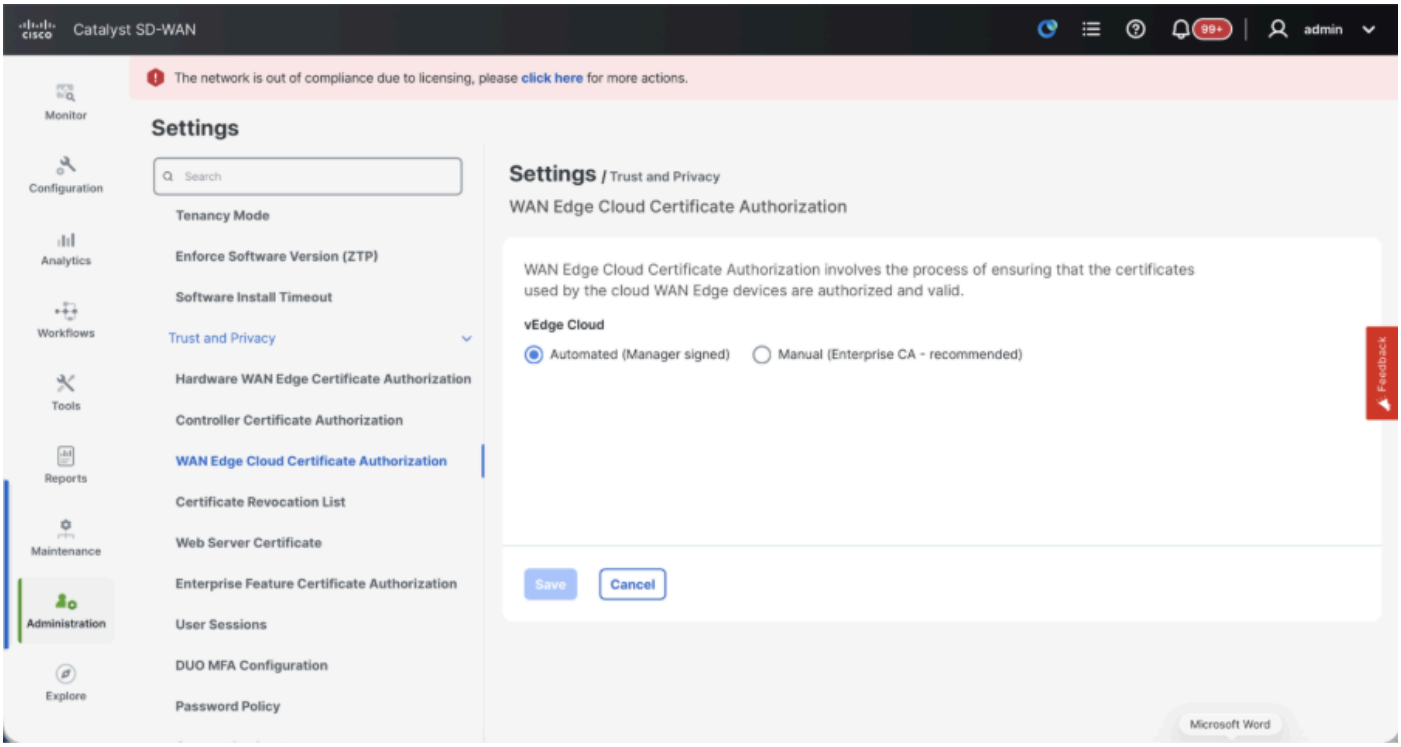
2. Controller Certificate Authorization — 決定SD-WAN控制器的CA。
   - 思科（推薦） — 控制器使用由Cisco PKI簽名的證書。vManage使用vManage上配置的智慧帳戶憑據自動聯絡PNP門戶，並簽署證書並將其安裝在控制器上。
   - 手動 — 控制器使用由Cisco PKI簽名的證書。導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
   - Enterprise Root Certificate — 使用此選項時，路由器使用由您組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。



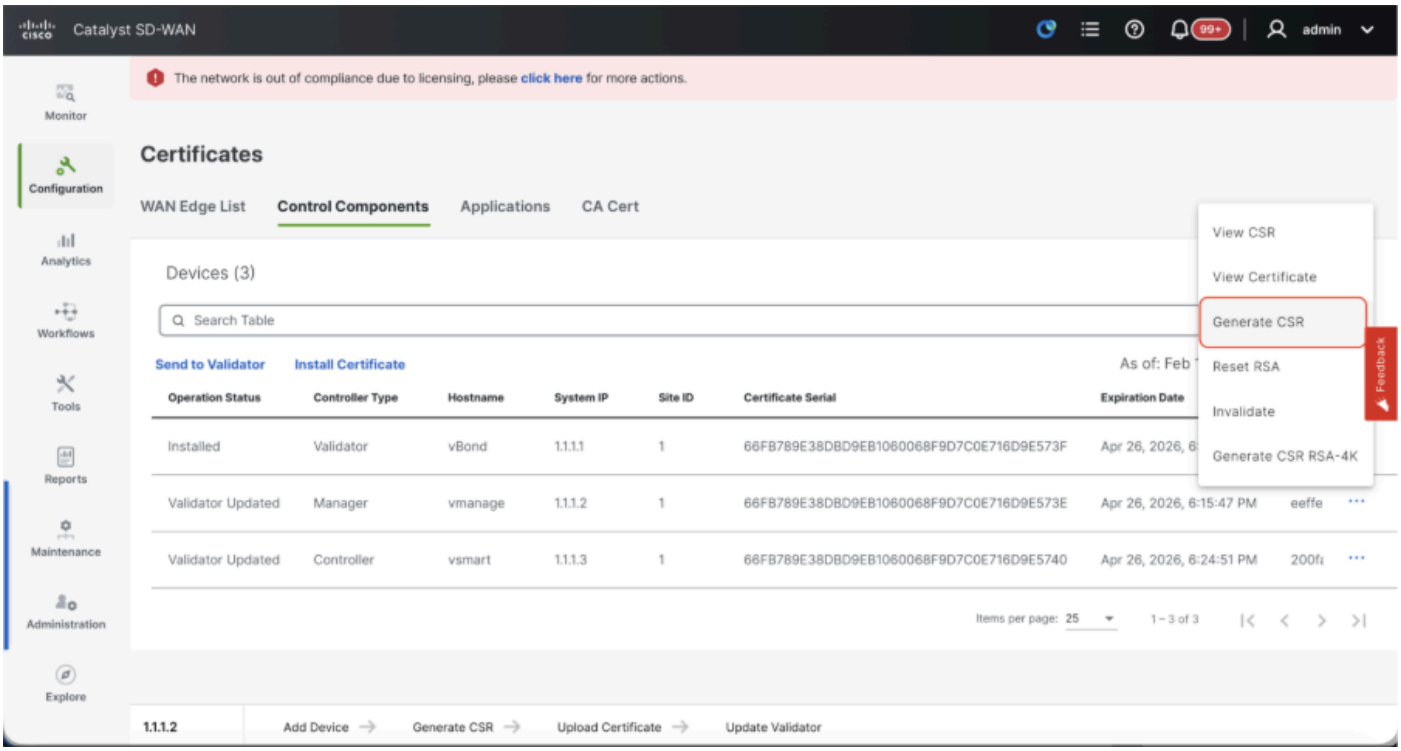
3. WAN邊緣雲證書授權 — 確定虛擬SD-WAN邊緣路由器（CSR1000v、C8000v、vEdge雲）的CA

- 自動（vManage簽名） — vManage自動對虛擬邊緣路由器的CSR進行簽名，並在路由器上安裝證書。
- 手動（企業CA — 推薦） — 虛擬路由器使用由組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。

如果使用CA（企業證書頒發機構），請選擇Enterprise。



- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers
- 點選Manager/vManage的……並點選Generate CSR。



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。

將vBond/Validator和vSmart/Controller註冊到vManage

如果是20.15/20.18 vManage節點，請導航到Configuration > Devices > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

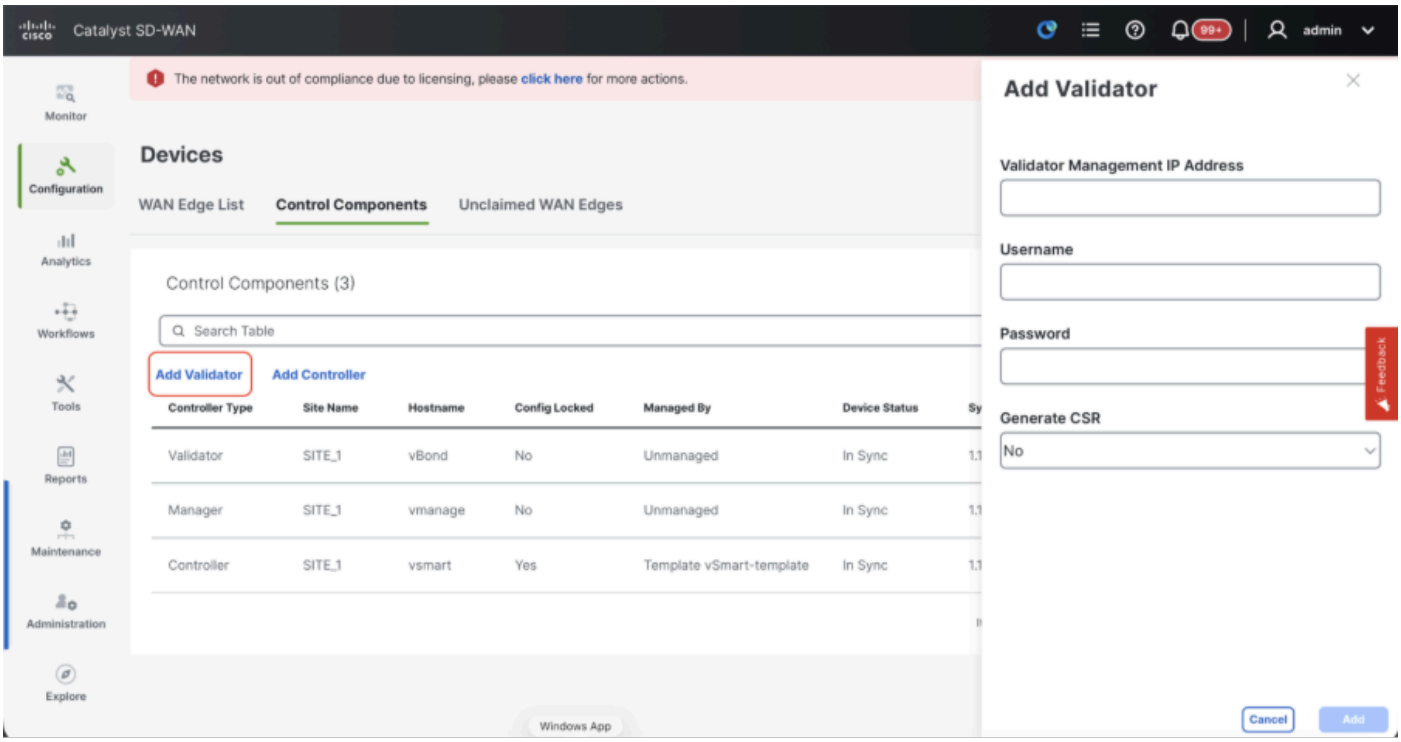
OnboardingvBond/驗證器

- 按一下AddvBond在20.12vManageor的情況下新增驗證程式在20.15/20.18 vManage的情況下。系統開啟一個彈出視窗，輸入 從vManage可訪問的vBond的VPN 0傳輸IP。
- 如果允許，請從vManagetovBondIP的CLI使用ping檢查可連接性。
- 輸入vBond的使用者憑據。

注意:我們需要使用vBondor的admin憑據作為netadmingroup的使用者部分。您可以在vBond的CLI中驗證這一點。如需安裝vBond的新憑證，請在「產生CSR」下拉式清單中選擇Yes

---

附註：如果vBond位於NAT裝置/防火牆之後，請檢查vBond VPN 0介面IP是否已轉換為公共IP。如果無法從vManage訪問VPN 0介面IP，則在此步驟中使用VPN 0介面的公用IP地址

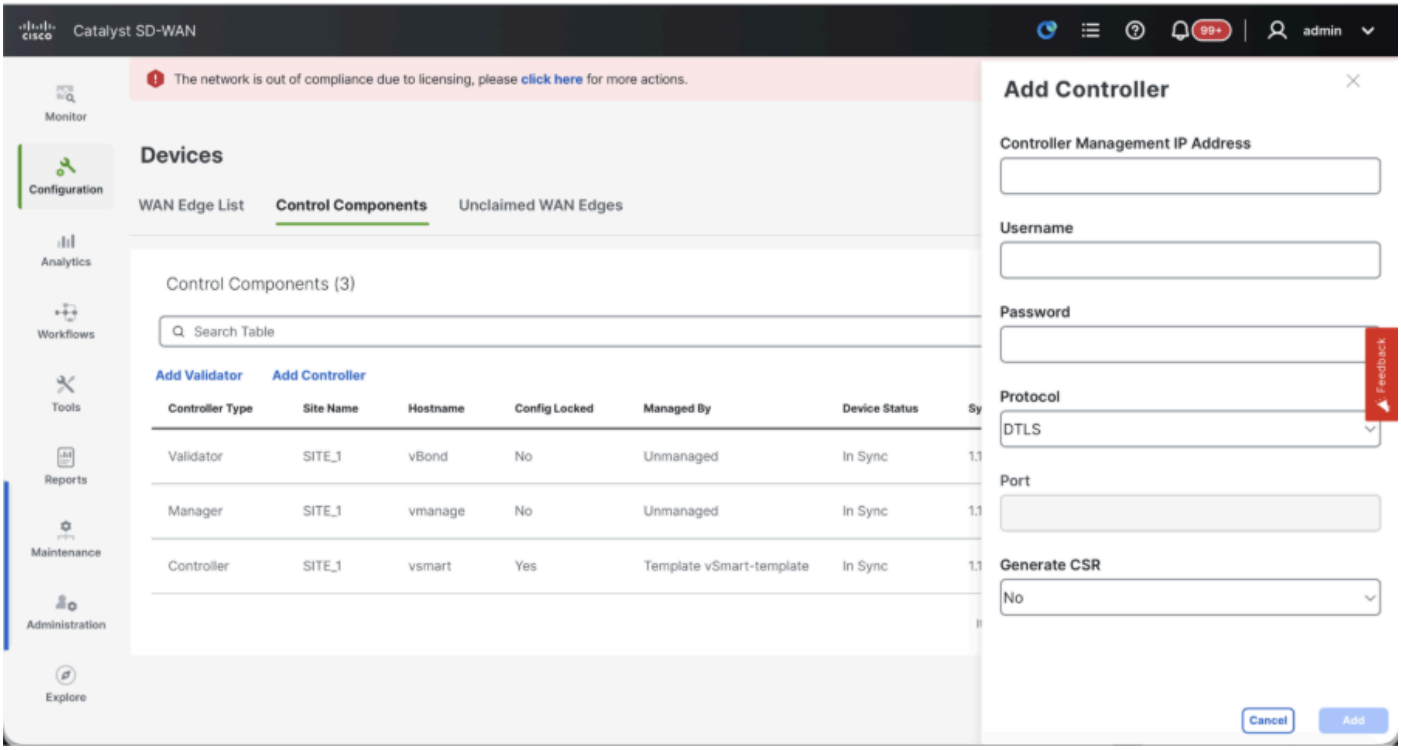


- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇思科（推薦），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vBond上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vBonds，請重複相同的步驟。

自註冊vSmart/控制器：

- 在20.12 vManage的情況下按一下Add vSmart，在20.15/20.18 vManage的情況下按一下Add Controller。
- 系統開啟一個彈出視窗，輸入vSmart的VPN 0傳輸IP（可從vManage訪問）。
- 如果允許，請從vManage的CLI到vSmart IP使用ping檢查可達性。
- 輸入vSmart Note的使用者憑據，我們需要使用vSmart的管理員憑據或netadmin組的使用者部分。
- 您可以在vSmart的CLI中驗證這一點。
- 如果希望路由器使用TLS來建立與vSmart的控制連線，請將協定設定為TLS。此配置也需要在vSmarts和vManage節點的CLI上配置。
- 如需安裝vSmart的新憑證，請在「產生CSR」下拉式清單中選擇「是」。

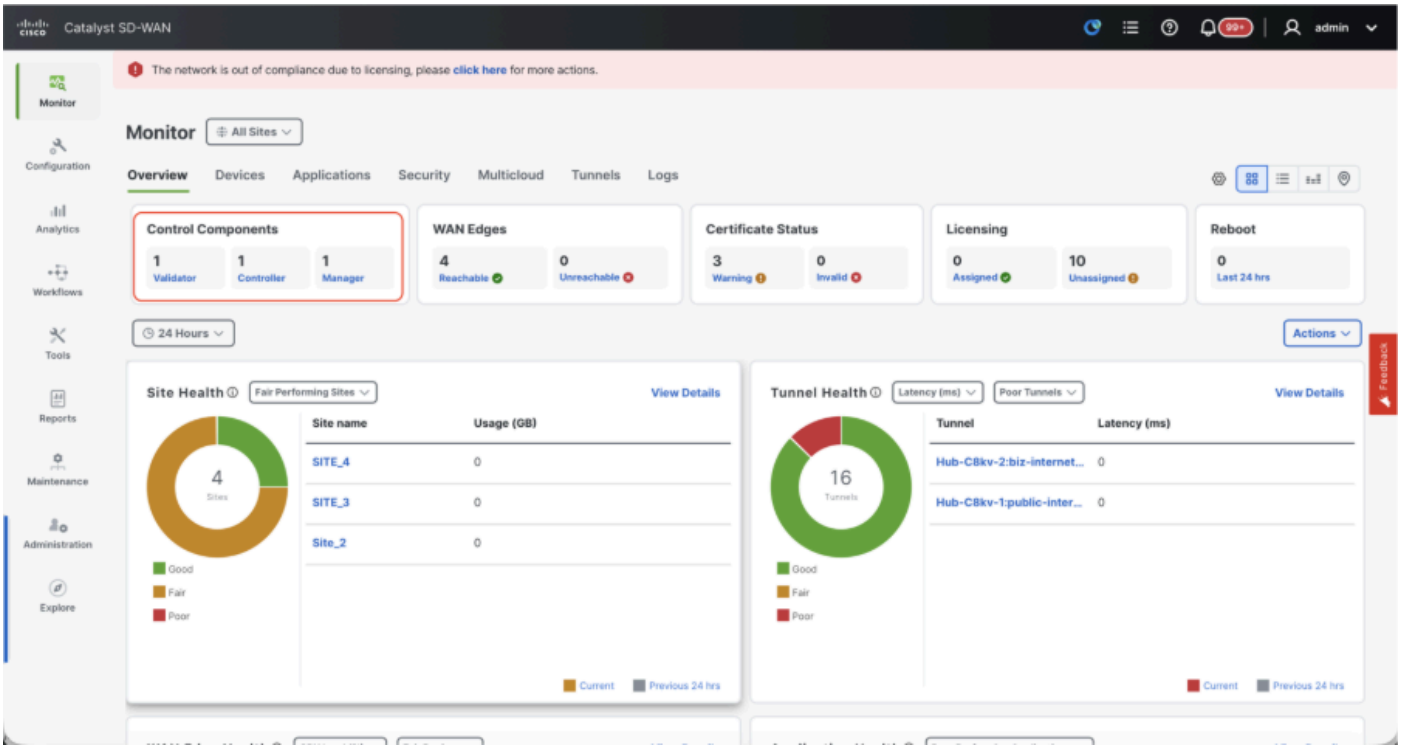
註：如果vSmart位於NAT裝置/防火牆之後，請檢查vSmart VPN 0介面IP是否已轉換為公共IP，如果無法從vManage訪問VPN 0介面IP，請在此步驟中使用VPN 0介面IP的公共IP地址。



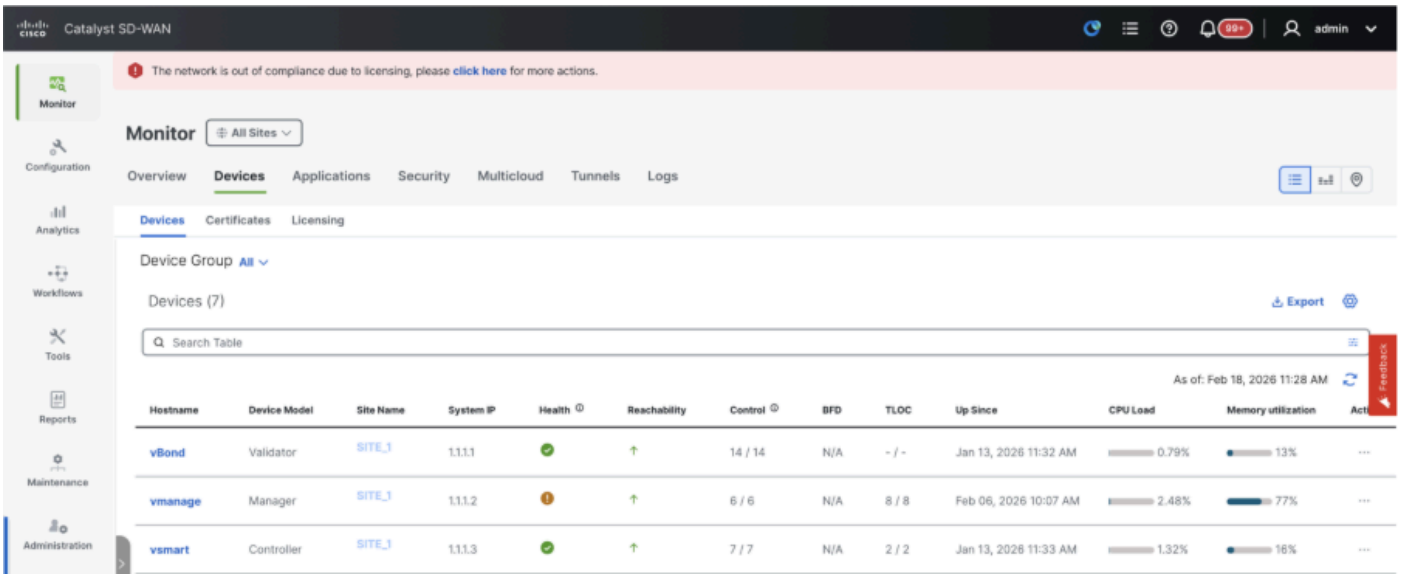
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vSmart上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vSmarts ，請重複相同的步驟。

驗證

完成所有步驟後，驗證是否可以在Monitor>Dashboard中訪問所有控制元件



- 按一下相應的控制元件，確認它們都可以訪問。
- 導覽至Monitor >Devices，確認所有控制元件均可連線。



步驟 3:構建vManage群集

板載SD-WAN交換矩陣，在SD-WAN重疊中帶有vManage集群

注意:vManage集群可以配置3個vManage節點或6個vManage節點，具體取決於註冊到SD-WAN交換矩陣的站點數量

通過單個vManage節點加入所有SD-WAN控制器

繼續執行「在SD-WAN重疊中帶單節點vManage的板載SD-WAN控制器」中共用的步驟，首先啟用帶一個vManage節點的SD-WAN交換矩陣，並加入所有必需的驗證器(vBond)和控制器(vSmart)。

配置屬於群集的所有vManage節點的CLI配置

- 配置vManage節點的其餘節點。對於3個節點集群，您有其餘2個要配置的節點；對於6個節點集群，您有5個要配置的節點。
- 配置系統配置，如下所示：

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注意:如果使用URL作為vBond地址，請確保在VPN 0配置中配置DNS伺服器IP地址或確保可以解析這些地址。

需要這些配置來啟用傳輸介面，該介面用於與路由器和其餘控制器建立控制連線。

```
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
```

另外配置VPN 512management介面以啟用對控制器的帶外管理訪問。

```
Conf t
vpn 512
 interface eth0
  ip address
```

```
  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

可選配置：

- 您可以參考現有控制器的配置，如果此處列出的配置存在，您可以將此配置新增到新控制器中。
- 僅當需要路由器使用TLS與vManage節點建立安全控制連線時，才將控制協定配置為TLS。預設情況下，所有控制器和路由器都使用DTLS建立控制連線。根據您的要求，此可選配置僅在vSmart和vManage節點上需要。

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

在所有vManage節點上配置服務介面

在已登入的所有vManagenodes（包括vManage-1）上配置服務介面。此介面用於集群通訊，表示集群中vManagenodes之間的通訊。

```
conf t
 interface eth2
  ip address



  no shutdown
commit
```

確保同一IP子網用於vManagecluster中所有節點上的服務介面。

配置群集憑據

我們可以使用vManagenodes的相同管理憑據來配置vManagecluster。否則，我們可以配置作為netadmingroup一部分的新使用者憑據。配置新使用者憑據的配置如下所示

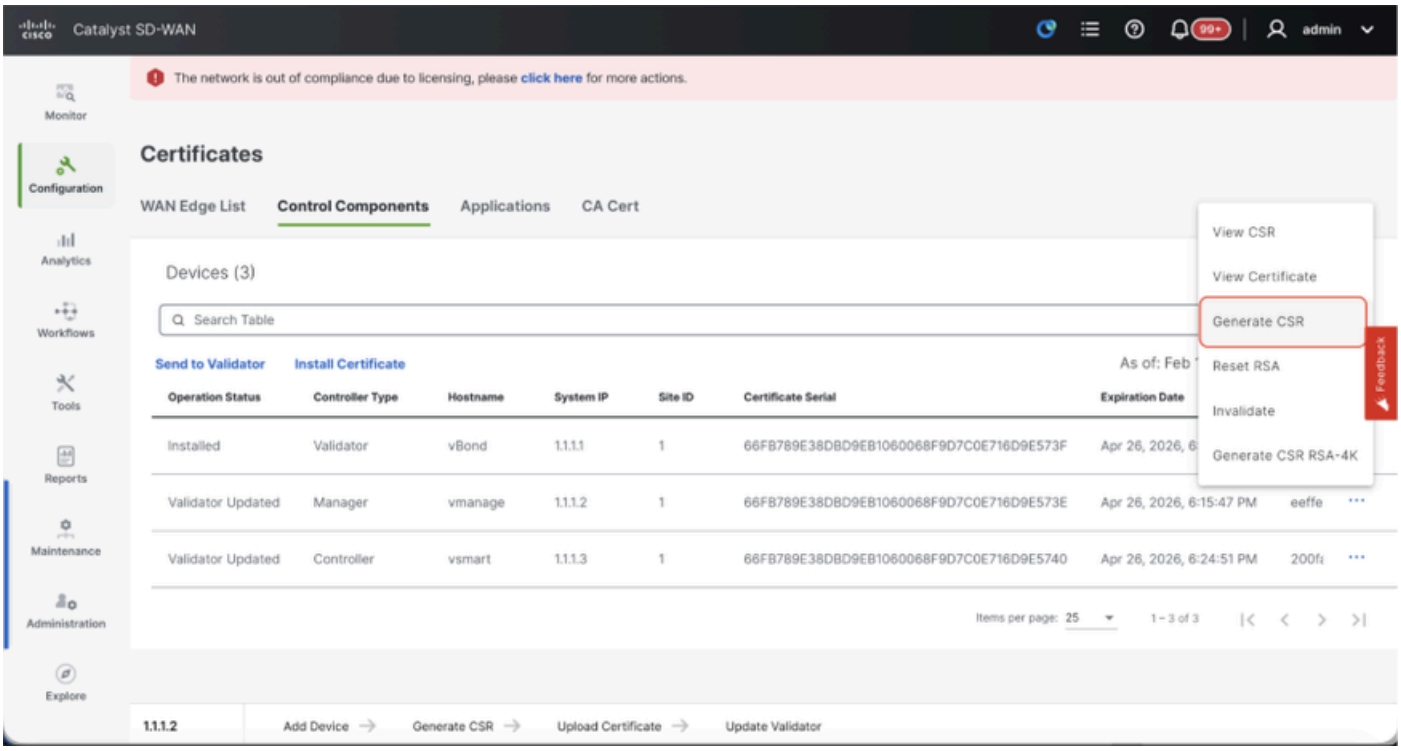
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

確保在屬於群集的所有vManagenode上配置相同的使用者憑據。如果我們決定使用管理員憑據，則必須在所有vManagenode上配置相同的使用者名稱/密碼。

在所有vManage節點上安裝裝置證書

- 使用瀏覽器中的URL https://<vmanage-ip>登入所有vManagenodes的tovManageUI。使用各自的vManagenodes的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

  按一下Manager/vManage的……並按一下Generate CSR。



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 跨屬於群集的所有vManage節點完成此步驟。

準備構建vManage群集

- 在vManage-1的WebUI上，導航到Administration > Cluster Management，在vManage-1的Actions下按一下……，然後選擇Edit。
- 在虛擬機器啟動時，根據我們選擇的角色自動選擇節點角色。

附註：對於一個3節點群集，所有3個vManage節點都以compute+data作為角色。

- 對於6節點群集，3個vManage節點將compute+data作為角色建立，3個vManage節點將資料作為角色建立。
- 從Manager IP地址下拉選單中，確保選擇vManage的服務接口IP。
- 輸入我們希望用來啟用vManage群集的使用者名稱和密碼，該群集稱為群集憑據。
- 如前所述，必須在所有vManage節點上配置相同的憑證，並且在將所有節點新增到群集時必

須使用相同的憑證。

可選配置：

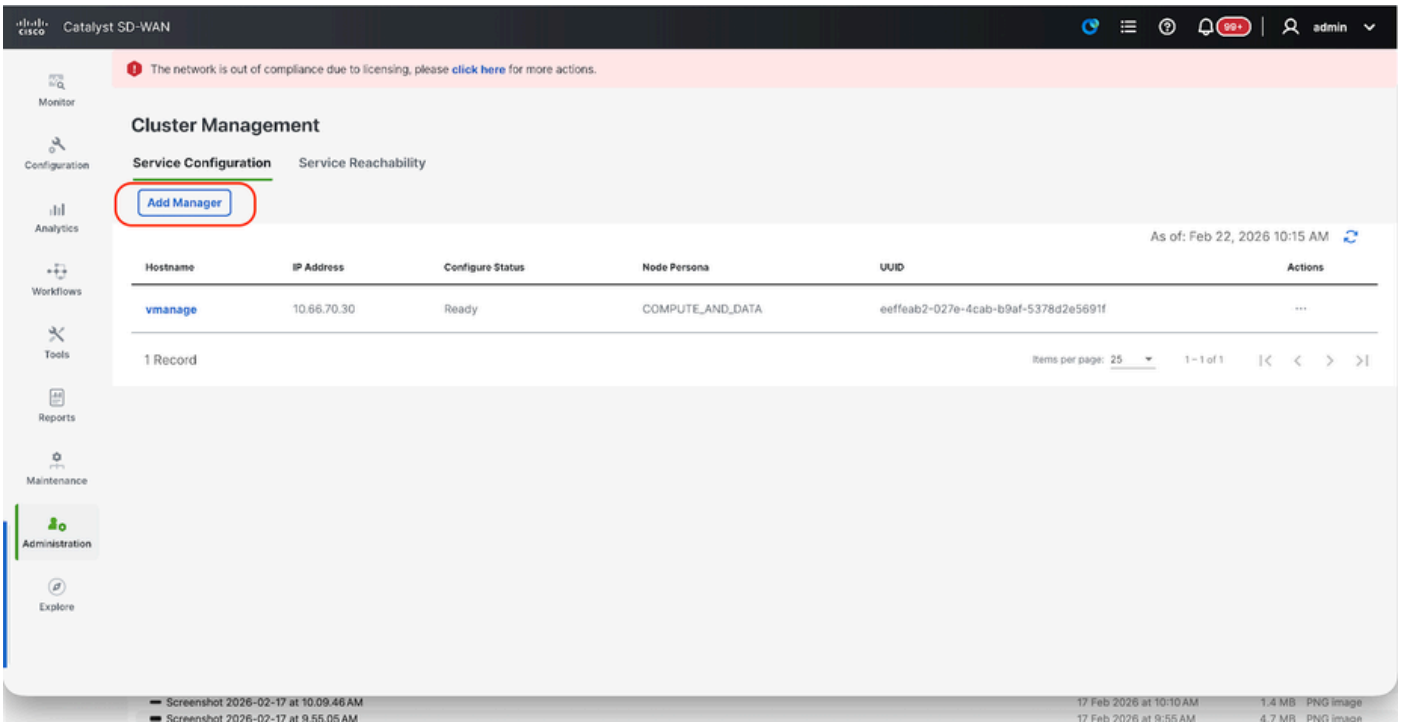
請參考現有群集中的此配置，以啟用SDAVC — 僅當需要且僅在群集的一個vManage節點上需要時，才需要選中。

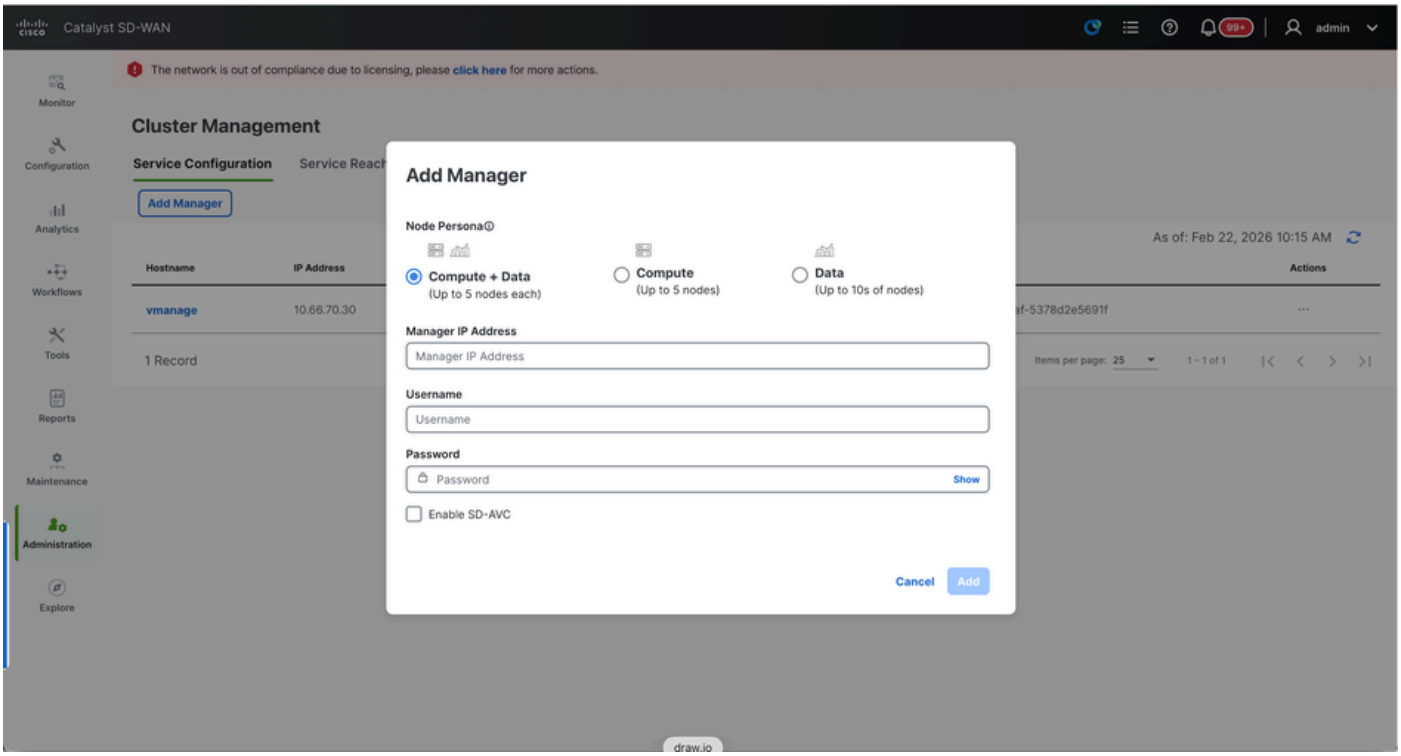
按一下「更新」。

- 發佈此消息後，vManage NMS服務在後台重新啟動，該UI在大約5至10分鐘的時間內不可用。在此期間，可使用vManage的CLI訪問。
- 可以訪問vManage-1 UI後，導航到Administration > Cluster Management，確保vManage的服務介面IP反映在IP地址下，配置狀態為就緒且正確反映節點角色。切換至同一頁面中的「服務可接通性」部分，並確保所有服務均可訪問。
- 如果尚未看到任何服務，請稍候。通常需要20到30分鐘。

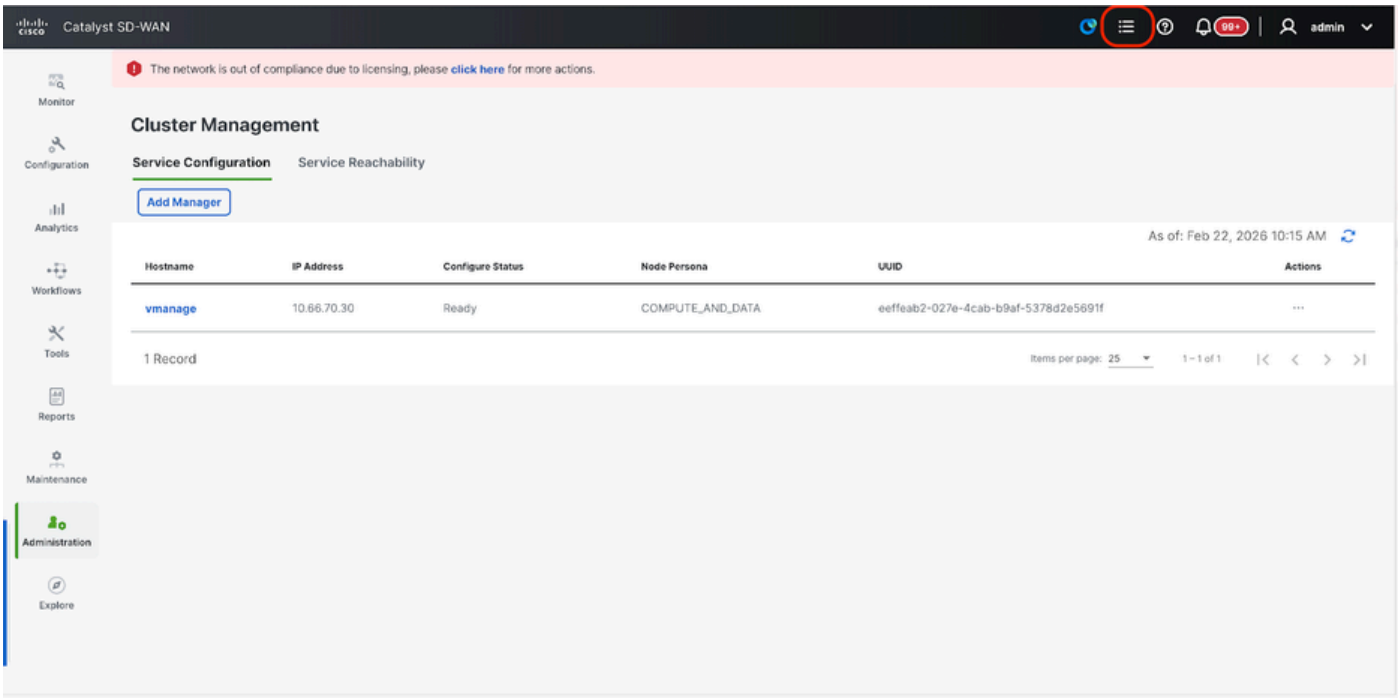
構建vManage群集

- 在vManage-1的WebUI上，導航到Administration > Cluster Management，在Service Configuration部分中，
- 按一下Add Manager，出現一個彈出視窗：





- 根據在vManage - 2節點旋轉時完成的角色配置選擇節點角色。
- 在Manager IP地址下輸入vManage-2的服務介面IP
- 輸入使用者名稱和密碼，該使用者名稱和密碼與我們在步驟6中使用的憑據相同。
- 啟用SDAVC — 保持未選中狀態，因為我們會在vManage-1上啟用它
- 點選Add。
- 之後，vManage 1和2節點的vManage NMS服務在後台重新啟動。對於vManage 1和2，該UI的可用時間大約為5到10分鐘。
- 在此期間，可使用vManage 1和2的CLI訪問。
- 可以訪問vManage-1 UI後，請導航至Administration > Cluster Management，確保vManage和vManage的服務介面IP反映在IP地址下，Configure Status is Ready且節點角色反映正確。
- 切換到同一頁中的「服務可接通性」部分，並確保兩個vManage節點的所有服務均可訪問。
- 如果尚未看到任何服務，請稍候。通常需要5到10分鐘。
- 您可以在vManage UI右上角的Task-list中檢查集群新增進程的狀態。



- 您可以查詢「活動」任務清單，如果該任務仍列在「活動」任務清單下，則表示該任務尚未完成。
- 您可以按一下該任務檢查其進度。如果該任務未列在「活動」任務清單下，請切換到「已完成」並確保任務成功完成。
- 只有在這些點經過驗證後，才能繼續下一步。

將下一個節點新增到群集之前，需要考慮以下幾點:

請在已新增到群集的所有vManage節點的UI上驗證這些點：

- 導航到Monitor > Overview of vManage UI，確保正確反映了vManage節點的數量，且根據新增到群集的節點數量可以看到。

- 導航到Administration > Cluster Management，並確保兩個vManage的服務介面IP都反映在IP地址下，Configure Status is Ready且節點角色正確反映。
- 切換到同一頁中的「服務可接通性」部分，並確保兩個vManage節點的所有服務均可訪問。

- 每次向群集中新增節點時，群集中所有節點的NMS服務都會重新啟動，因此在一段時間內，這些節點的UI將變得不可達。
- 根據群集中的節點數，可能需要較長的時間才能備份UI以及訪問所有服務。
- 您可以在vManage UI右上角的Task-list下監視任務。
- 在新增到群集的每個節點的vManage UI上，我們需要檢視所有路由器、模板和策略（如果它們在vManage-1中可用）。
- 如果這些配置不存在於vManage-1上，則新增到vManage-1中的vBonds和vSmarts以及組織— 名稱、vBond、證書授權的管理>設定配置必須反映在新增到群集的其餘vManage節點上。

- 對其餘vManage節點重複相同步驟。

步驟 4:冷備用DR群集設定

冷備用DR群集設定

您可以使用步驟4中介紹的步驟來啟動多個vManage集群：生成vManage群集。開機自檢，完成步驟6中所述的步驟：Config-db Backup/Restore，恢復備用群集中的config-db備份。

步驟 5:Config-db備份/還原

在另一個vManage節點上收集vManage configuration-db備份和還原

收集Configuration-DB備份：

- 在當前正在使用的SD-WAN交換矩陣中，可以從vManage群集生成配置資料庫備份。
- 請注意，我們只能在vManage群集中的一個節點（該節點是configuration-db領導者）上生成configuration-db備份。

- 對於獨立vManage，該vManage本身是配置資料庫的領導者。
- 在vManage群集中，使用命令request nms configuration-db diagnostics標識configuration-db領導節點。您可以在3節點vManage群集的所有節點上運行此命令。
- 在6節點集群中，確保在啟用了configuration-db的vManage節點上運行此命令，以標識領導節點。 導覽至Administration > Cluster Management以驗證相同內容：
- 如螢幕截圖所示，配置了persona COMPUTE_AND_DATA的節點正在運行configuration-db。

您可以在vManageCLI上使用requestnmsconfiguration-dbstatus命令進行驗證。輸出如下

```
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#
```

- 一旦您執行命令請求nms configuration-db對這些節點進行診斷，輸出如下：
- 查詢「IsLeader」的突出顯示的欄位。如果設定為1，則表示節點是領導節點，我們可以從中收集配置資料庫備份。

```
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     .
```

使用此命令從標識的configuration-db領導vManage節點收集configuration-db備份。

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

預期輸出如下：

```
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#
```

- 如果已更新configuration-db憑證，請記下該憑證。
- 如果您不知道配置資料庫憑據，請聯絡TAC以從現有vManage節點檢索配置資料庫憑據。
- 預設的configuration-db憑證是使用者名稱：neo4j和密碼：密碼

將Configuration-db備份還原到另一個vManage節點

使用SCP將configuration-db backup複製到vManage的/home/admin/目錄。

scp命令輸出示例：

```
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
```

要恢復configuration-db備份，首先需要配置configuration-db憑據。如果您的配置資料庫憑據是預設值(neo4j/password)，則可以跳過此步驟。

要配置configuration-db憑據，請使用request nms configuration-db update-admin-user命令。使用您選擇的使用者名稱和密碼。

請注意，vManage的應用程式伺服器已重新啟動。由於vManage UI將在短時間內不可訪問。

```
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#
```

可以繼續還原配置資料庫備份的開機自檢：

我們可以使用命令request nms configuration-db restore path /home/admin/< >將configuration-db還原到新的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
```

恢復configuration-db後，確保vManage UI可訪問。等待約5分鐘，然後嘗試訪問UI。

成功登入到UI後，請確保邊緣路由器清單、模板、策略以及以前或現有vManage UI上存在的所有其餘配置都反映在新的vManage UI上。

步驟 6:控制器的重新驗證和舊控制器的失效

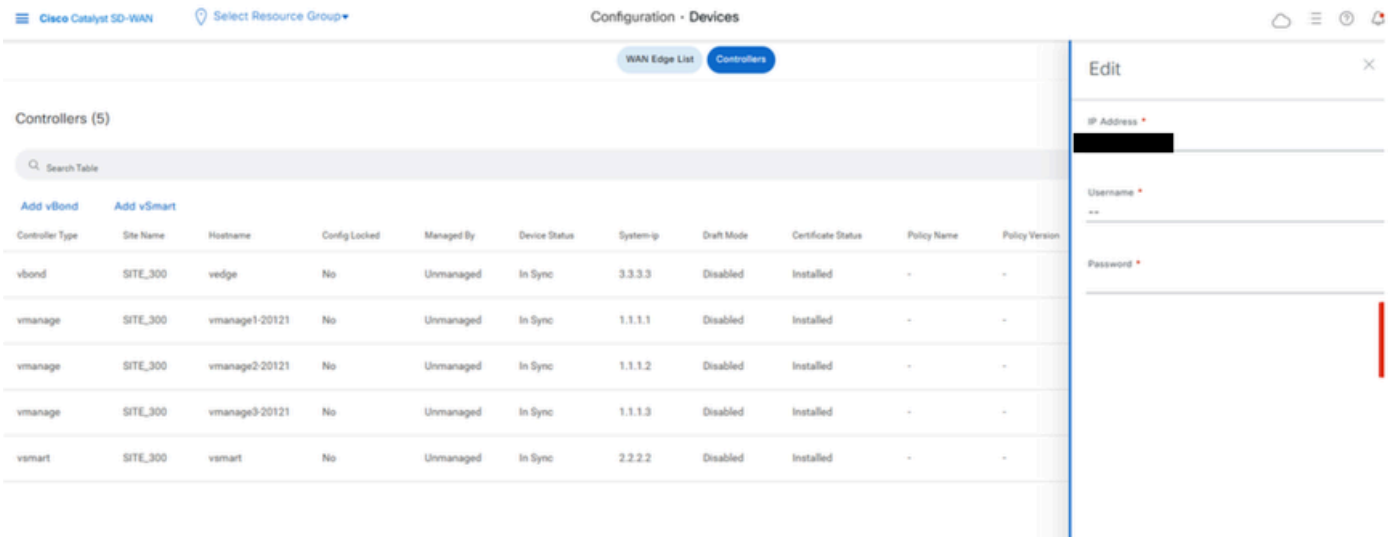
恢復configuration-db後，我們需要重新驗證交換矩陣中的所有新控制器(vmanage/vsmart/vbond)

註：在實際生產中，如果用於重新身份驗證的介面IP是隧道介面IP，則需要確保在vManage、vSmart和vBond的隧道介面以及路徑沿途的防火牆上允許NETCONF服務。要開

啟的防火牆埠是作為從DR群集到所有vBonds和vSmarts的雙向規則的TCP埠830。

在vmanage UI上，點選Configuration > Devices > Controllers

- 按一下每個控制器附近的三個點，然後按一下「Edit（編輯）」



- 將ip-address（控制器的系統ip）替換為transport vpn 0（隧道介面）ip地址。輸入使用者名稱和密碼，然後按一下save
- 對交換矩陣中的所有新控制器執行相同操作

同步根證書鏈

載入所有控制器後，完成以下步驟：

在新活動群集中的任何Cisco SD-WAN Manager伺服器上，執行以下操作：

輸入以下命令將根證書與新活動群集中的所有Cisco Catalyst SD-WAN裝置同步：

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

輸入以下命令將Cisco SD-WAN Manager UUID與Cisco SD-WAN驗證器同步：

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

在交換矩陣恢復後，交換矩陣中的所有邊緣和控制器的控制和bfd會話均已啟動，我們需要從UI使舊控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，點選Configuration > Devices > Certificates
- 按一下「Controllers（控制器）」
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。按一下「invalidate（失效）」
- 點選send to vbond
- 在vmanage UI上，點選Configuration > Devices > Controllers

- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。點選刪除(Delete)

步驟 7:過帳支票

附註：繼續使用此處顯示的「後檢查」部分，它對所有部署組合都是通用的。

組合5:vManage Cluster + DR已啟用

所需例項：

- 3或6個vManage（主群集）
- 3或6個vManage（DR備用群集）
- 1個或多個vBond（分佈於主資料中心和DR資料中心）
- 1個或多個vSmart（分佈於主資料中心和DR資料中心）

步驟:

1. 使用通用步驟調出所有例項
2. 預先檢查
3. 配置vManage UI、證書和板載控制器
4. 構建vManage群集
5. 冷備用DR群集設定
6. Config-db backup/restore
7. 過帳支票

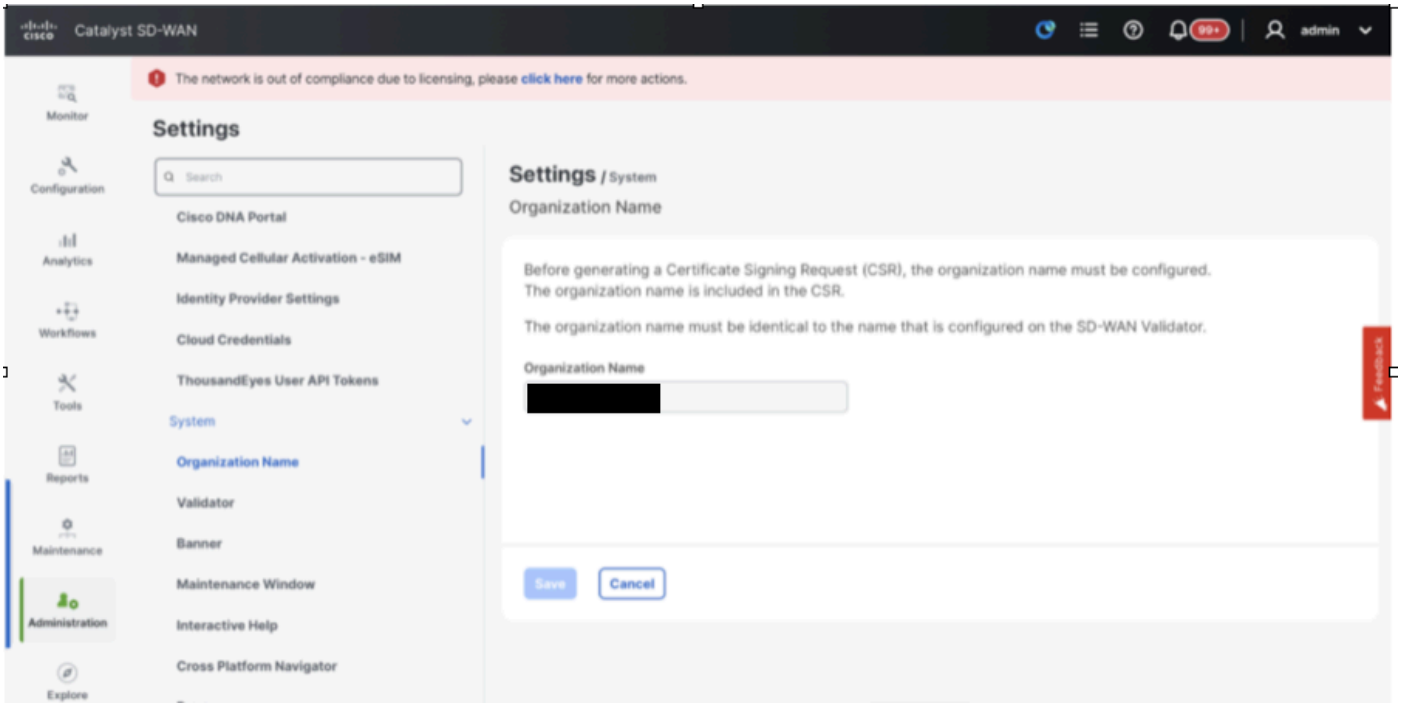
步驟 1:預先檢查

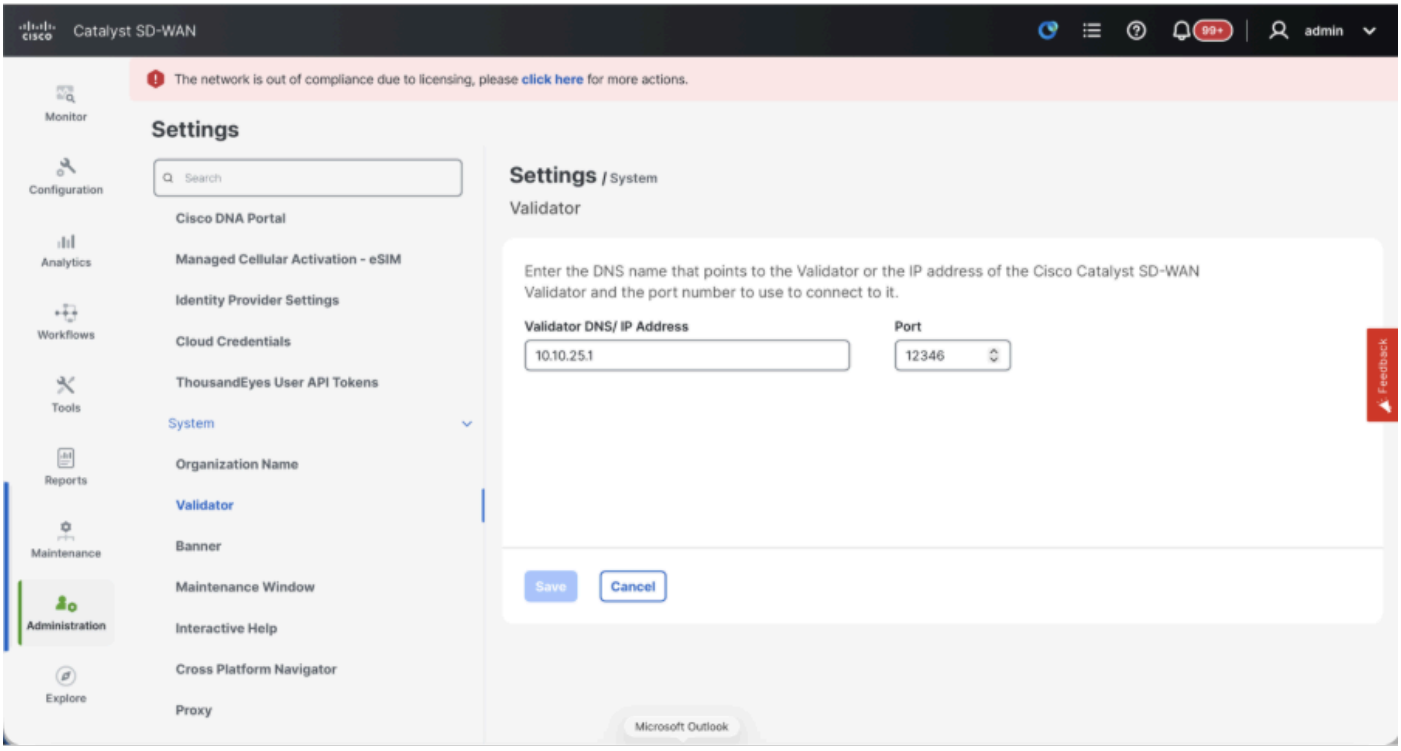
- 確保活動的Cisco SD-WAN Manager例項數與新安裝的Cisco SD-WAN Manager實例數相同。
- 確保所有活動的和新的Cisco SD-WAN Manager例項運行相同的軟體版本。
- 確保所有活動的和新的Cisco SD-WAN Manager例項都能到達Cisco SD-WAN Validator的管理IP地址。
- 確保證書已安裝在新安裝的Cisco SD-WAN Manager例項上。
- 確保所有Cisco Catalyst SD-WAN 裝置(包括新安裝的Cisco SD-WAN Manager例項)上的時鐘都同步。
- 確保在新安裝的Cisco SD-WAN Manager例項上配置一組新的系統IP和站點ID，並與活動群集配置相同的基本配置。

步驟 2:配置vManage UI、證書和板載控制器

更新vManage UI上的配置

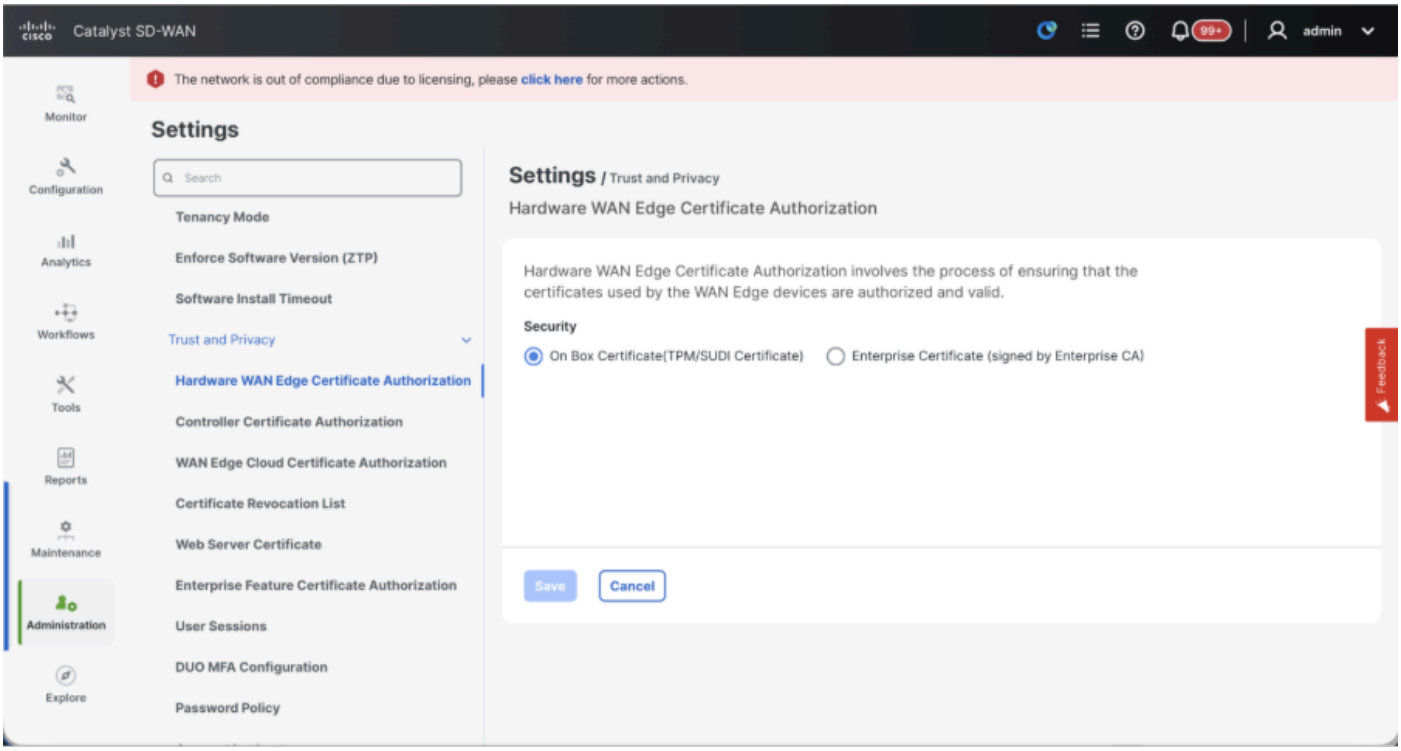
- 將步驟1中的組態新增到所有控制器的CLI上後，我們可以使用瀏覽器中的https://<vmanage-ip>URL存取vManage的WebUI。使用各個vManage節點的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 導覽至Administration > Settings，然後完成以下步驟。
- 配置組織名稱和驗證器/vBond URL/IP地址。配置與vManage節點的CLI中相同的值。
- 在vManage 20.15/20.18中，這些配置可在System部分中找到。



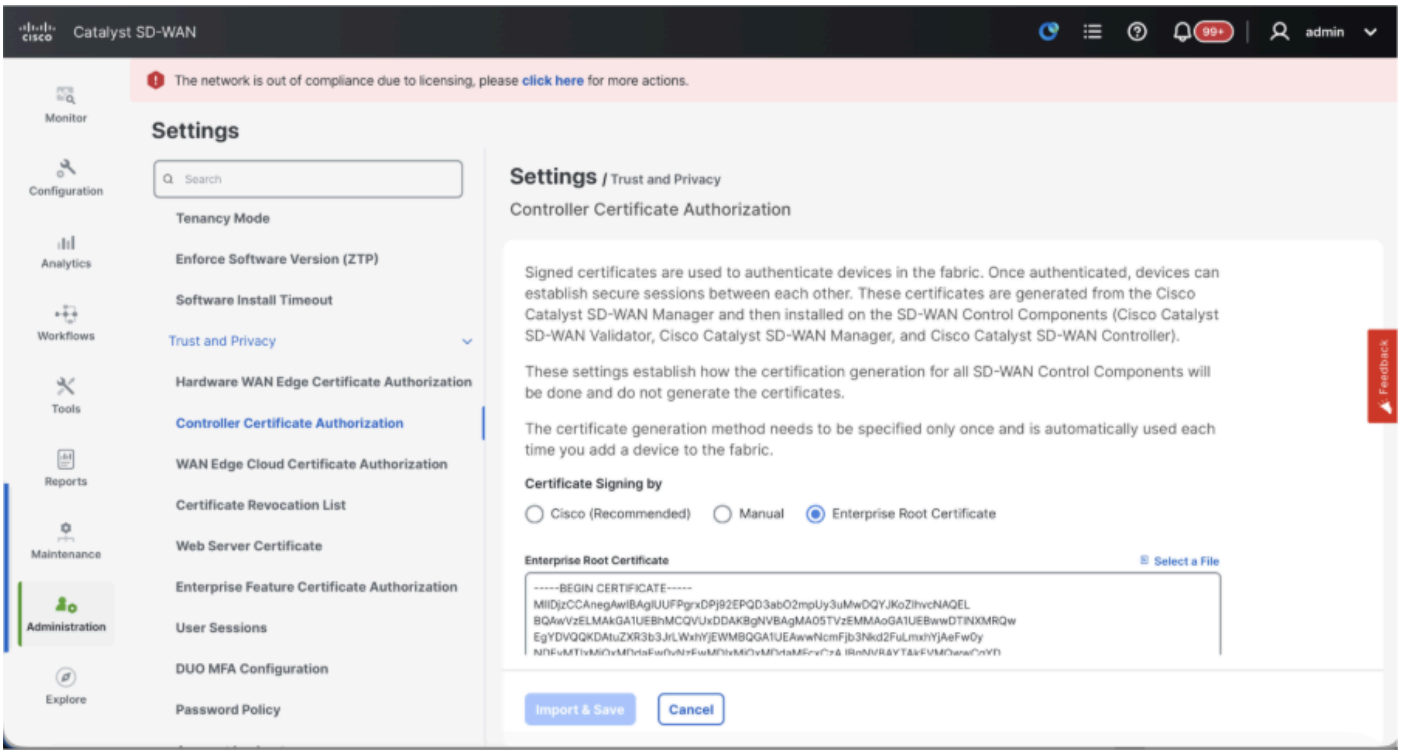


- 驗證證書授權(CA)的配置，CA決定用於簽署證書的證書授權。我們可以看到3個選項：

1. 硬體WAN邊緣證書授權 — 決定硬體SD-WAN邊緣路由器的CA。
    - 開箱證書（TPM/SUDI證書） — 使用此選項，路由器硬體上預安裝的證書用於建立控制連線（TLS/DTLS連線）
    - 企業證書（由企業CA簽署） — 使用此選項時，路由器使用由組織的企業證書頒發機構簽署的證書。選擇此選項時，必須在此處更新企業CA的根證書。

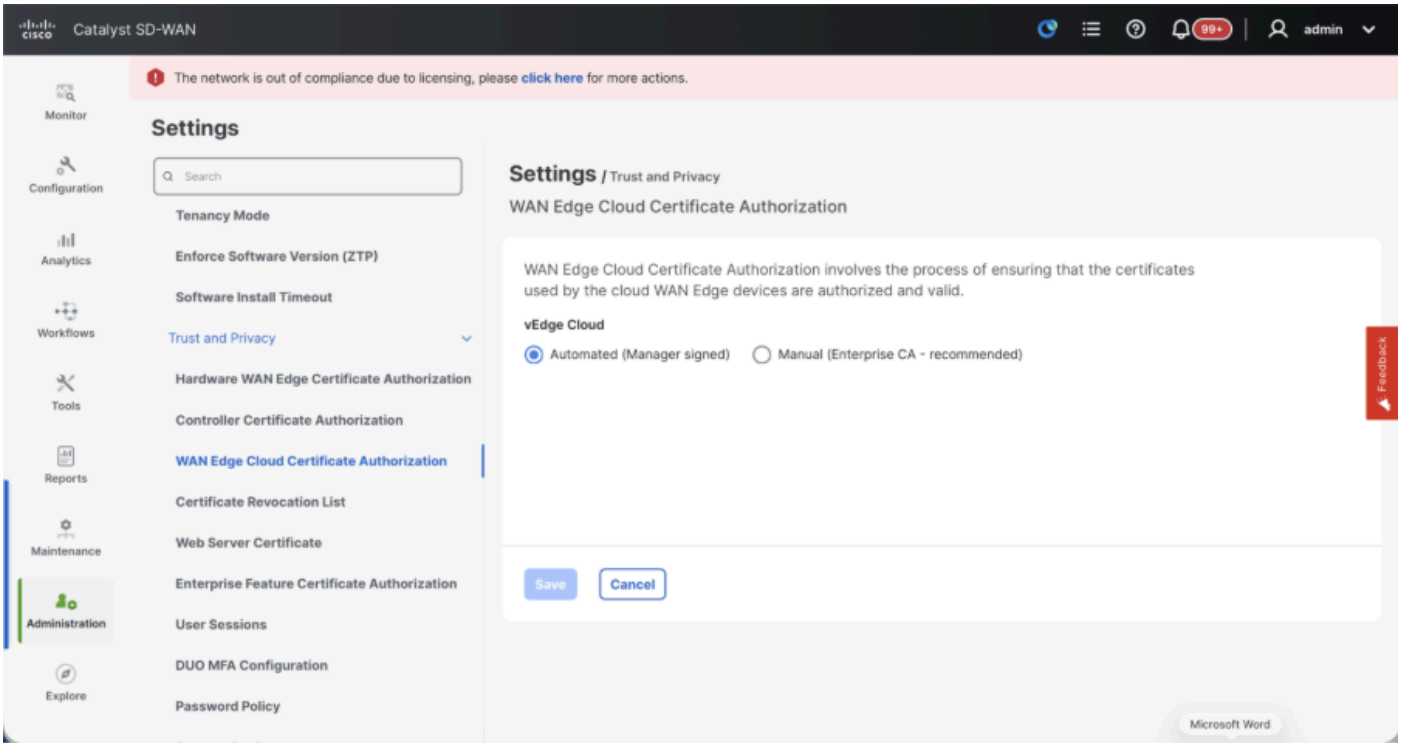


2. Controller Certificate Authorization — 決定SD-WAN控制器的CA。
    - 思科（推薦） — 控制器使用由Cisco PKI簽名的證書。vManage使用vManage上配置的智慧帳戶憑據自動聯絡PNP門戶，並簽署證書並將其安裝在控制器上。
    - 手動 — 控制器使用由Cisco PKI簽名的證書。導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
    - Enterprise Root Certificate — 使用此選項時，路由器使用由您組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。



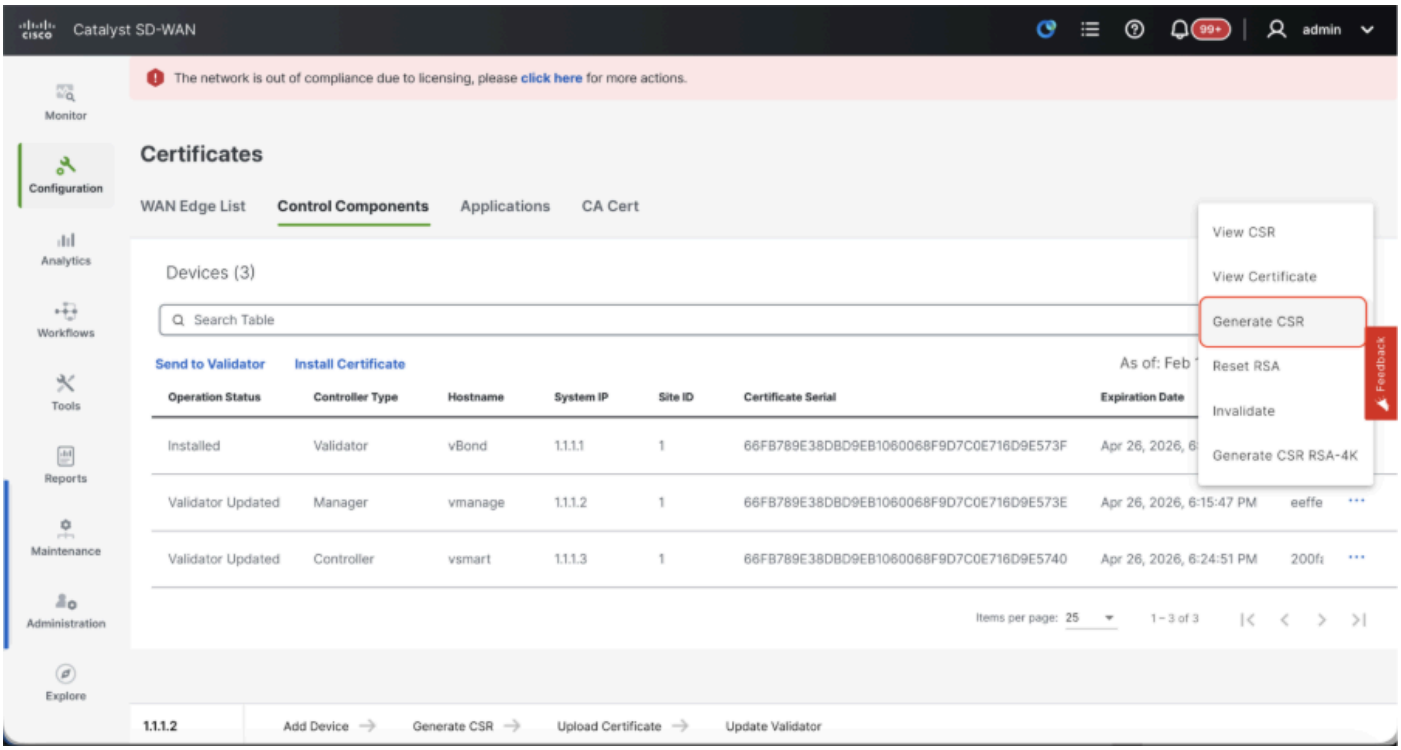
3. WAN邊緣雲證書授權 — 確定虛擬SD-WAN邊緣路由器（CSR1000v、C8000v、vEdge雲）的CA
    - 自動（vManage簽名） — vManage自動對虛擬邊緣路由器的CSR進行簽名，並在路由器上安裝證書。
    - 手動（企業CA — 推薦） — 虛擬路由器使用由組織的企業證書頒發機構簽名的證書。選擇此選項時，必須在此處更新企業CA的根證書。

如果使用CA（企業證書頒發機構），請選擇Enterprise。



- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control

Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers
- 點選Manager/vManage的……並點選Generate CSR。



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。

將vBond/Validator和vSmart/Controller註冊到vManage

如果是20.15/20.18 vManage節點，請導航到Configuration > Devices > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

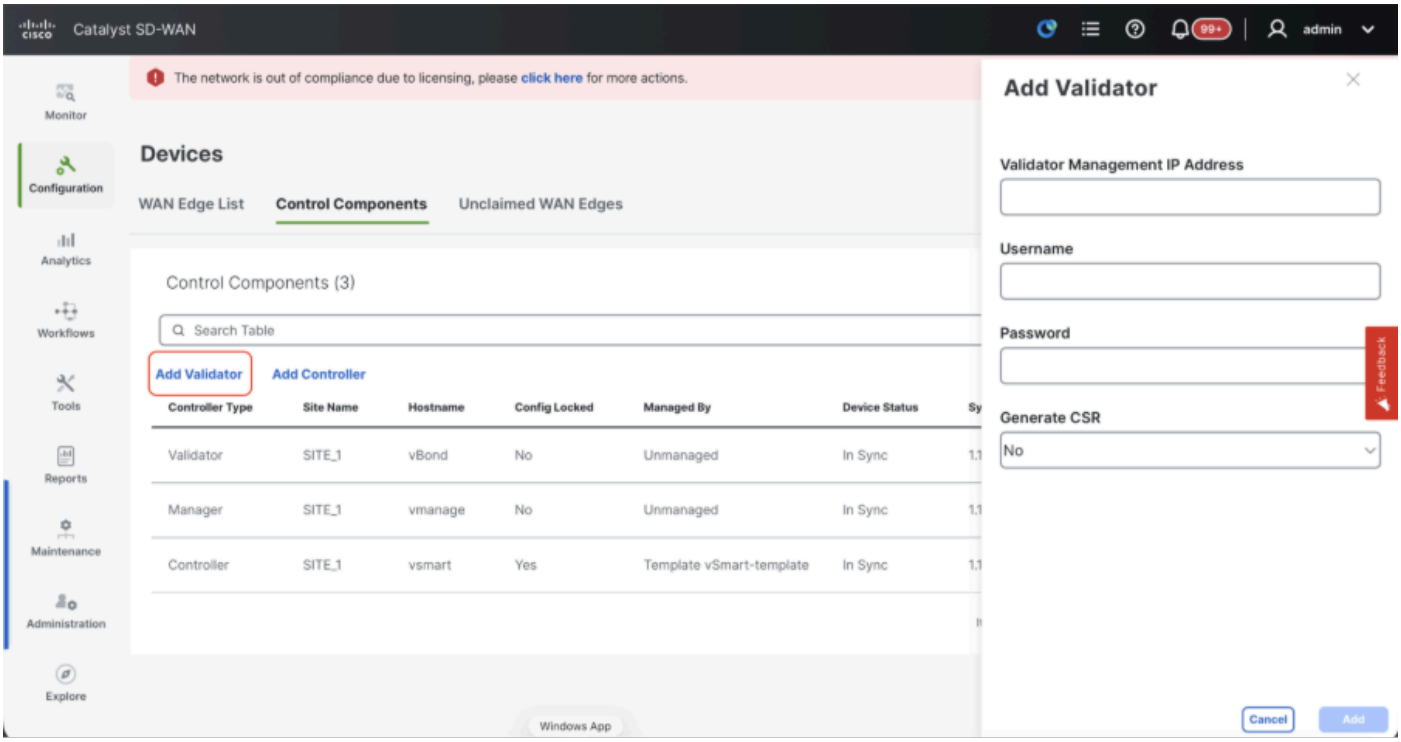
OnboardingvBond/驗證器

- 按一下AddvBond在20.12vManageor的情況下新增驗證程式在20.15/20.18 vManage的情況下。系統開啟一個彈出視窗，輸入 從vManage可訪問的vBond的VPN 0傳輸IP。
- 如果允許，請從vManagetovBondIP的CLI使用ping檢查可連接性。
- 輸入vBond的使用者憑據。

注意:我們需要使用vBondor的admin憑據作為netadmingroup的使用者部分。您可以在vBond的CLI中驗證這一點。如需安裝vBond的新憑證，請在「產生CSR」下拉式清單中選擇Yes

---

附註：如果vBond位於NAT裝置/防火牆之後，請檢查vBond VPN 0介面IP是否已轉換為公共IP。如果無法從vManage訪問VPN 0介面IP，則在此步驟中使用VPN 0介面的公用IP地址



- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇思科（推薦），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vBond上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vBonds，請重複相同的步驟。

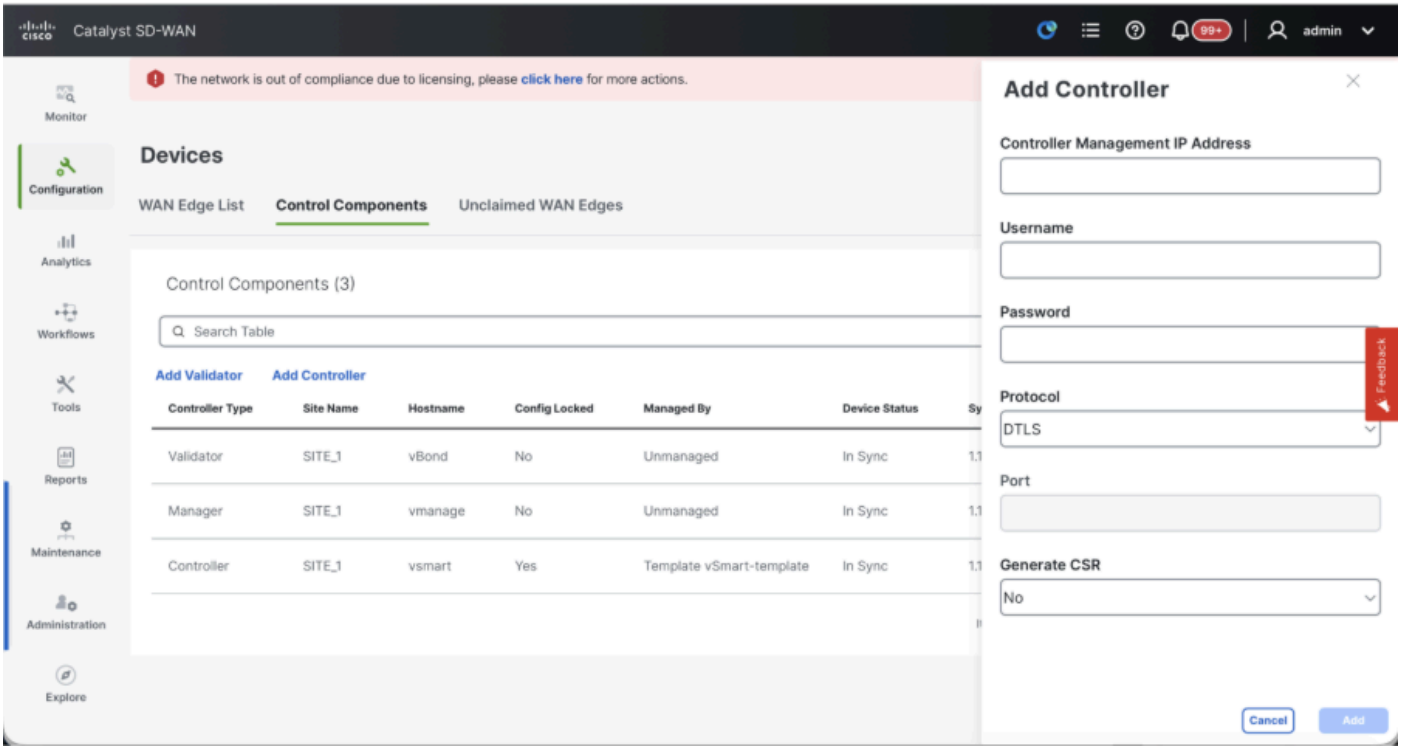
自註冊vSmart/控制器：

- 在20.12 vManage的情況下按一下Add vSmart，在20.15/20.18 vManage的情況下按一下Add Controller。
- 系統開啟一個彈出視窗，輸入vSmart的VPN 0傳輸IP（可從vManage訪問）。
- 如果允許，請從vManage的CLI到vSmart IP使用ping檢查可達性。
- 輸入vSmart Note的使用者憑據，我們需要使用vSmart的管理員憑據或netadmin組的使用者部分。
- 您可以在vSmart的CLI中驗證這一點。
- 如果希望路由器使用TLS來建立與vSmart的控制連線，請將協定設定為TLS。此配置也需要在

vSmarts和vManage節點的CLI上配置。

- 如需安裝vSmart的新憑證，請在「產生CSR」下拉式清單中選擇「是」。

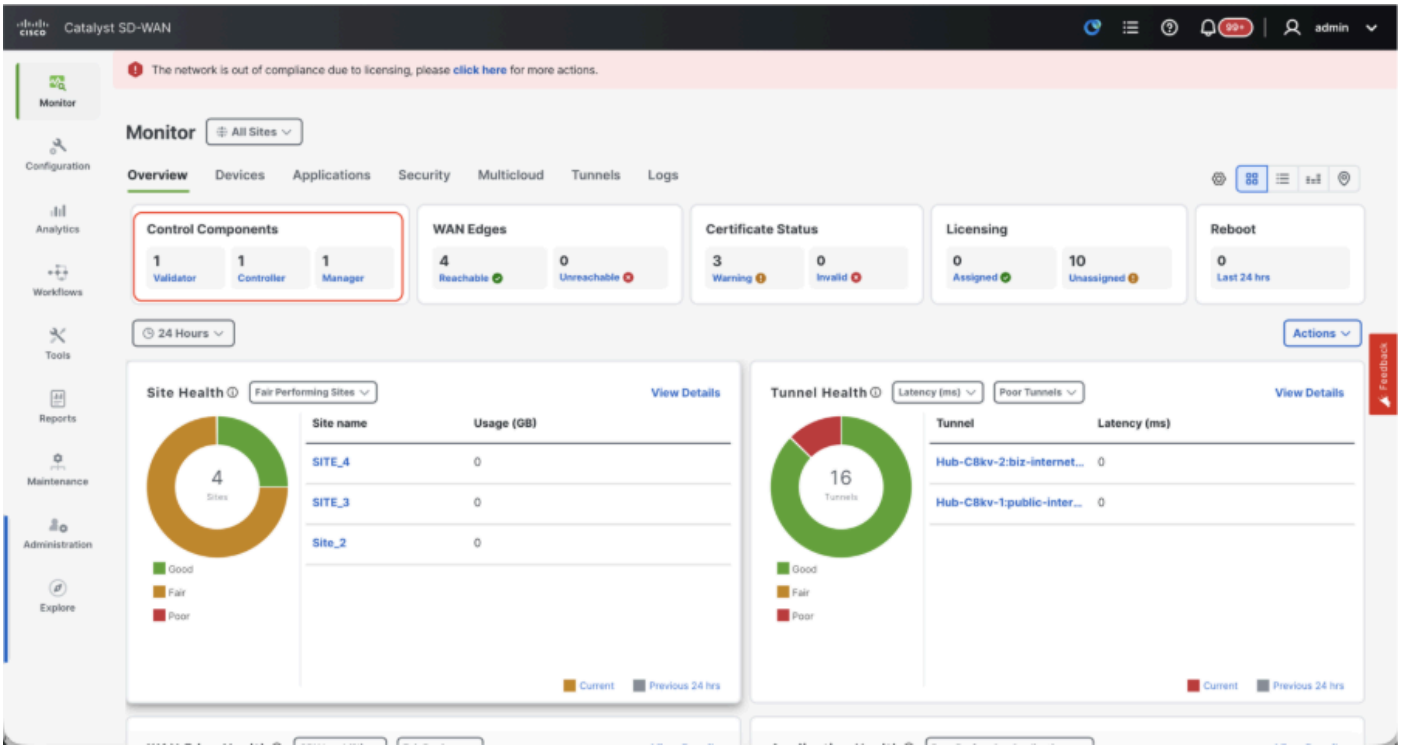
註：如果vSmart位於NAT裝置/防火牆之後，請檢查vSmart VPN 0介面IP是否已轉換為公共IP，如果無法從vManage訪問VPN 0介面IP，請在此步驟中使用VPN 0介面IP的公共IP地址。



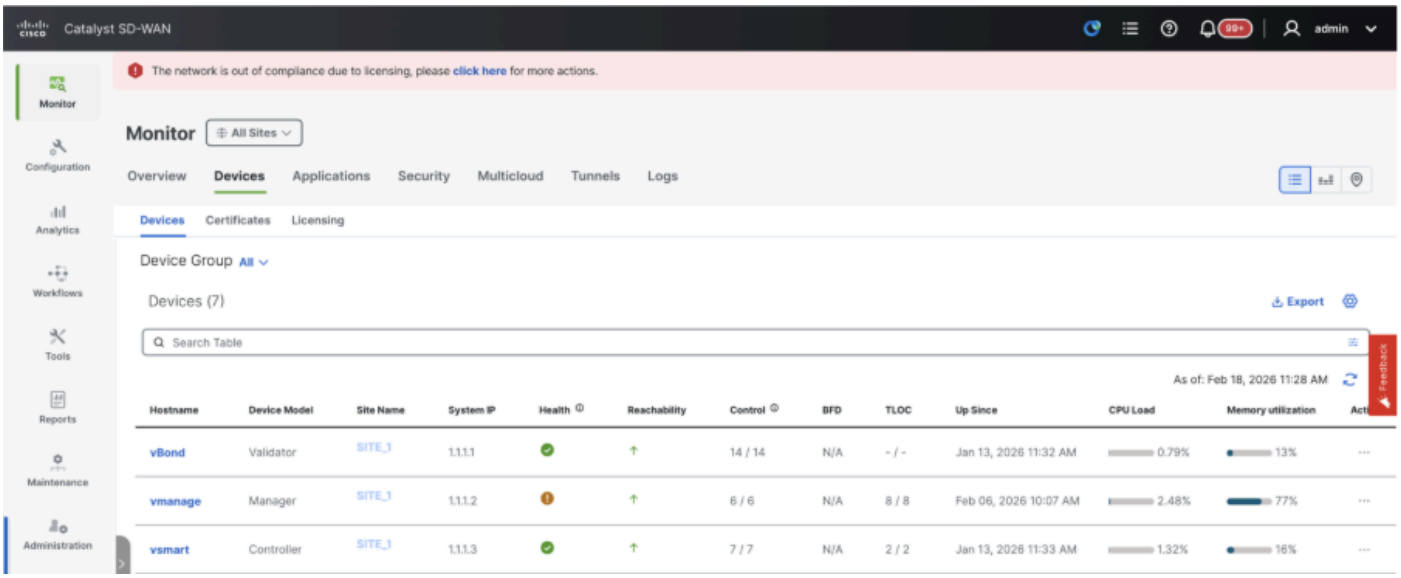
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vSmart上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 如果有多個vSmarts ，請重複相同的步驟。

驗證

完成所有步驟後，驗證是否可以在Monitor>Dashboard中訪問所有控制元件



- 按一下相應的控制元件，確認它們都可以訪問。
- 導覽至Monitor >Devices，確認所有控制元件均可連線。



步驟 3:構建vManage群集

板載SD-WAN交換矩陣，在SD-WAN重疊中帶有vManage集群

注意:vManage集群可以配置3個vManage節點或6個vManage節點，具體取決於註冊到SD-WAN交換矩陣的站點數量

通過單個vManage節點加入所有SD-WAN控制器

繼續執行「在SD-WAN重疊中帶單節點vManage的板載SD-WAN控制器」中共用的步驟，首先啟用帶一個vManage節點的SD-WAN交換矩陣，並加入所有必需的驗證器(vBond)和控制器(vSmart)。

配置屬於群集的所有vManage節點的CLI配置

- 配置vManage節點的其餘節點。對於3個節點集群，您有其餘2個要配置的節點；對於6個節點集群，您有5個要配置的節點。
- 配置系統配置，如下所示：

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注意:如果使用URL作為vBond地址，請確保在VPN 0配置中配置DNS伺服器IP地址或確保可以解析這些地址。

需要這些配置來啟用傳輸介面，該介面用於與路由器和其餘控制器建立控制連線。

```
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
```

另外配置VPN 512management介面以啟用對控制器的帶外管理訪問。

```
Conf t
vpn 512
 interface eth0
  ip address
```

```
  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

可選配置：

- 您可以參考現有控制器的配置，如果此處列出的配置存在，您可以將此配置新增到新控制器中。
- 僅當需要路由器使用TLS與vManage節點建立安全控制連線時，才將控制協定配置為TLS。預設情況下，所有控制器和路由器都使用DTLS建立控制連線。根據您的要求，此可選配置僅在vSmart和vManage節點上需要。

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

在所有vManage節點上配置服務介面

在已登入的所有vManagenodes（包括vManage-1）上配置服務介面。此介面用於集群通訊，表示集群中vManagenodes之間的通訊。

```
conf t
 interface eth2
  ip address



  no shutdown
commit
```

確保同一IP子網用於vManagecluster中所有節點上的服務介面。

配置群集憑據

我們可以使用vManagenodes的相同管理憑據來配置vManagecluster。否則，我們可以配置作為netadmingroup一部分的新使用者憑據。配置新使用者憑據的配置如下所示

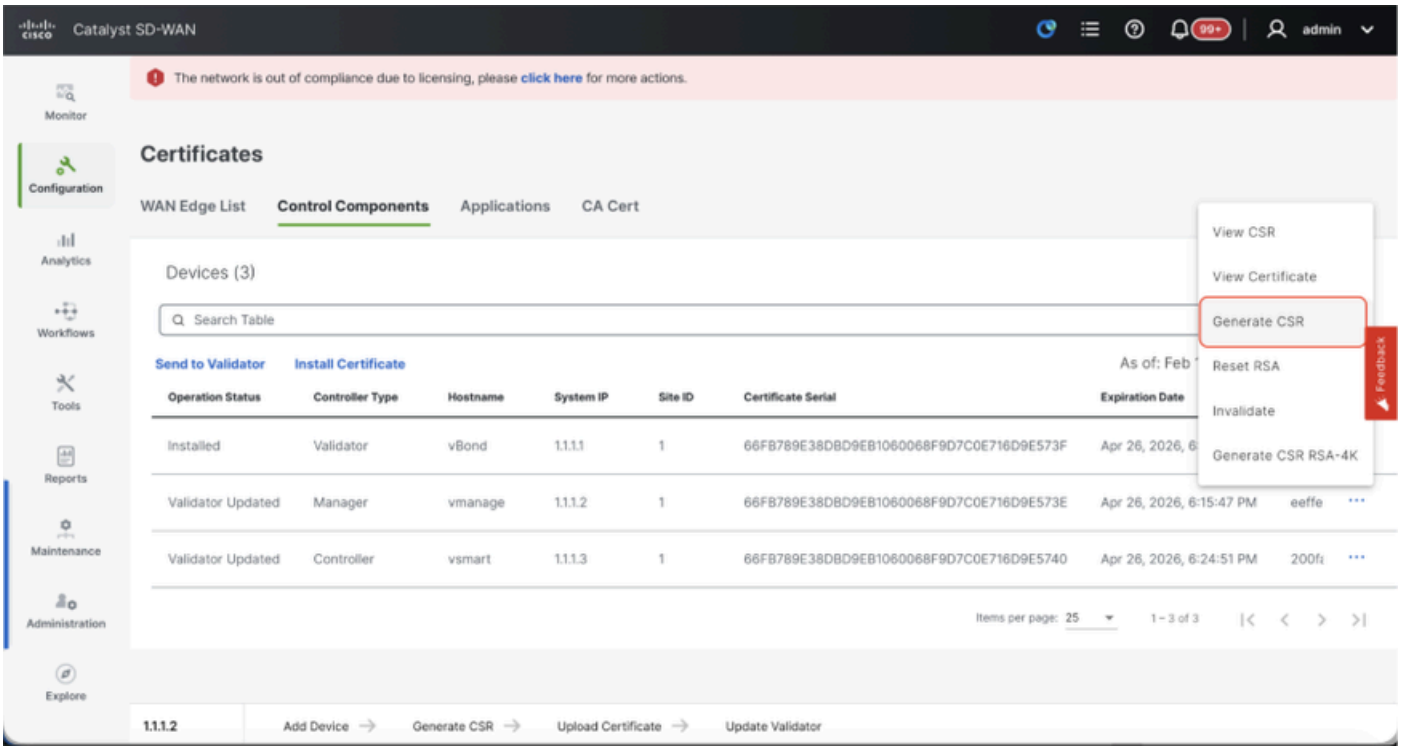
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

確保在屬於群集的所有vManagenode上配置相同的使用者憑據。如果我們決定使用管理員憑據，則必須在所有vManagenode上配置相同的使用者名稱/密碼。

在所有vManage節點上安裝裝置證書

- 使用瀏覽器中的URL https://<vmanage-ip>登入所有vManagenodes的tovManageUI。使用各自的vManagenodes的VPN 512 IP地址。您可以使用管理員使用者名稱和密碼登入。
- 如果是20.15/20.18 vManage節點，請導航到Configuration > Certificates > Control Components。若為20.9/20.12版本，請輸入Configuration > Devices > Controllers

  按一下Manager/vManage的……並按一下Generate CSR。



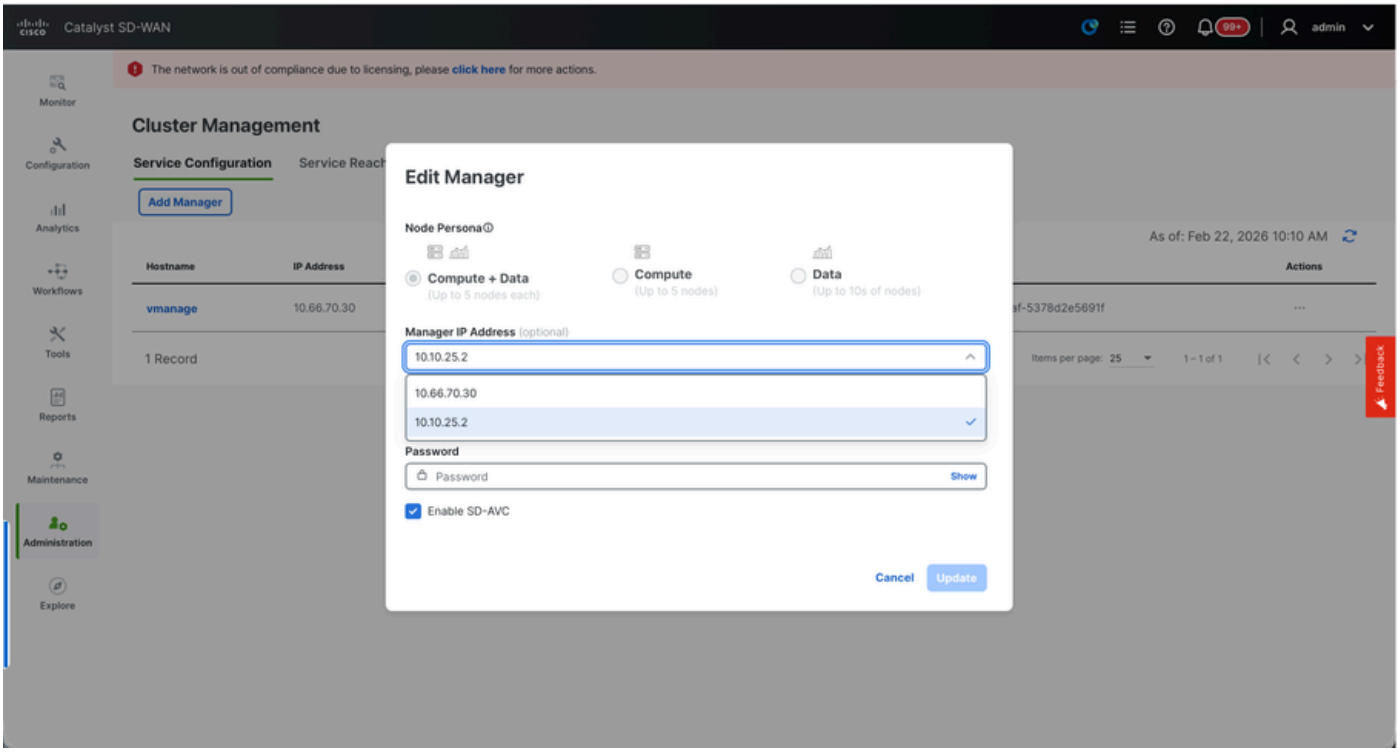
- 產生CSR後，您可以下載CSR，並根據為控制器選擇的憑證授權進行簽名。您可以在管理>設定>控制器憑證授權中驗證此組態。如果選擇Cisco（建議），則vManage會自動將CSR上傳到PNP門戶，並且證書簽署後，會自動將其安裝在vManage上。
- 如果選擇「手動」，請通過導航到相應SD-WAN重疊的智慧帳戶和虛擬帳戶，使用思科PNP門戶手動簽署CSR。
- 證書從PNP門戶可用後，在vManage的同一部分中按一下安裝證書，然後上傳證書並安裝證書。
- 如果我們使用Digicert和Enterprise Root Certificate ，則適用相同的步驟。
- 跨屬於群集的所有vManage節點完成此步驟。

準備構建vManage群集

- 在vManage-1的WebUI上，導航到Administration > Cluster Management，在vManage-1的Actions下按一下……，然後選擇Edit。
- 在虛擬機器啟動時，根據我們選擇的角色自動選擇節點角色。

附註：對於一個3節點群集，所有3個vManage節點都以compute+data作為角色。對於6節點群集，3個vManage節點將compute+data作為角色建立，3個vManage節點將資料作為角色建立。

- 從Manager IP地址下拉選單中，確保選擇vManage的服務接口IP。



- 輸入我們希望用來啟用vManage群集的使用者名稱和密碼，該群集稱為群集憑據。
- 如前所述，必須在所有vManage節點上配置相同的憑證，並且在將所有節點新增到群集時必須使用相同的憑證。

可選配置：

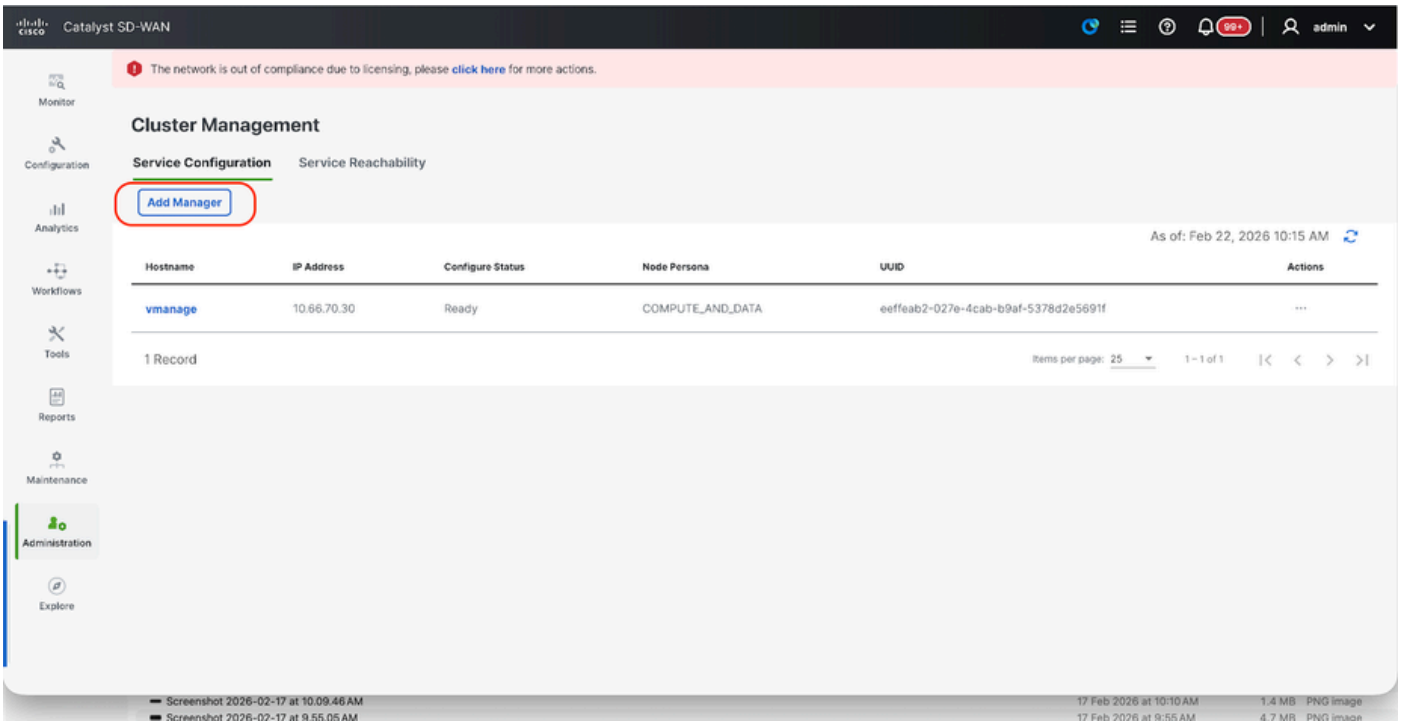
請參考現有群集中的此配置，以啟用SDAVC — 僅當需要且僅在群集的一個vManage節點上需要時，才需要選中。

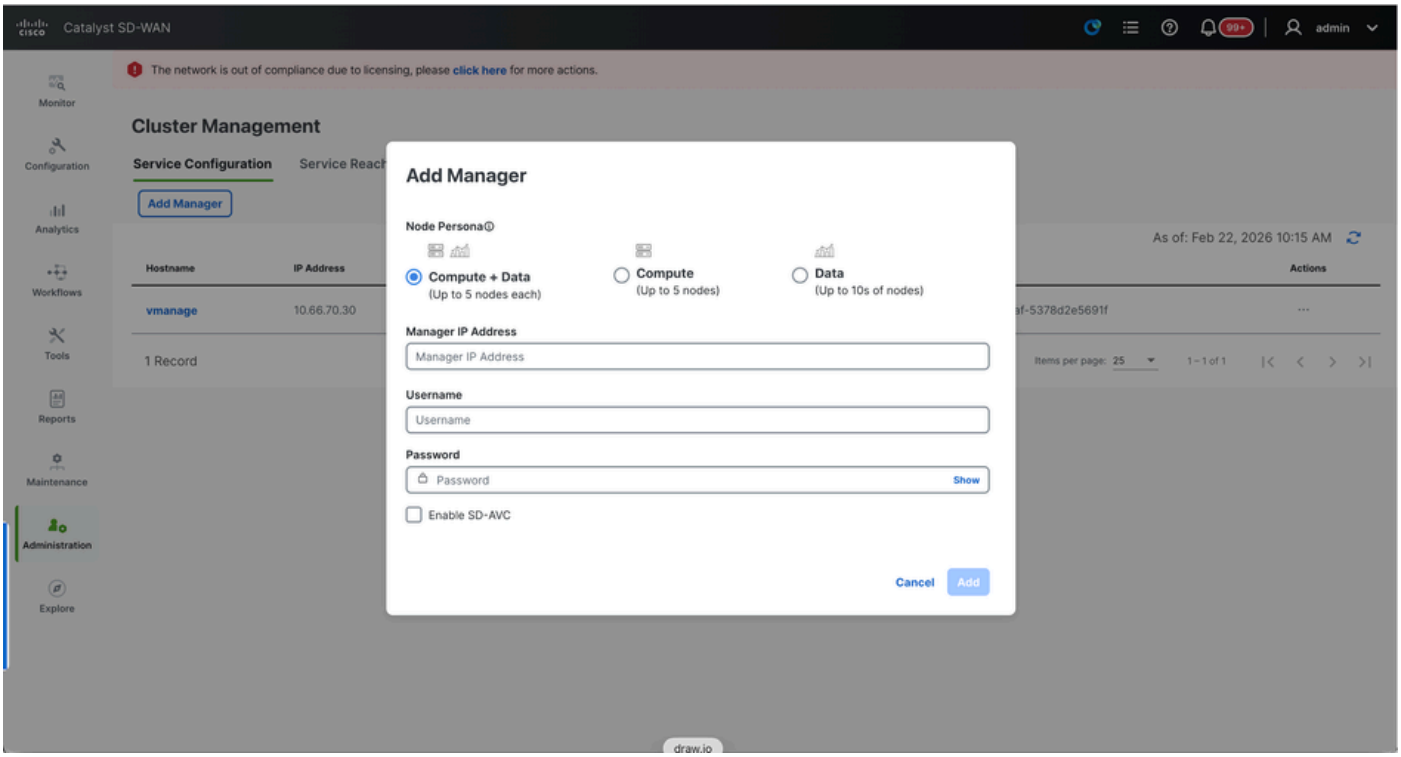
按一下「更新」。

- 發佈此消息後，vManage NMS服務在後台重新啟動，該UI在大約5至10分鐘的時間內不可用。在此期間，可使用vManage的CLI訪問。
- 可以訪問vManage-1 UI後，導航到Administration > Cluster Management，確保vManage的服務介面IP反映在IP地址下，配置狀態為就緒且正確反映節點角色。切換到相同頁面中的Service Reachability部分，並確保所有服務均可訪問。
- 如果尚未看到任何服務，請稍候。通常需要20到30分鐘。

構建vManage群集

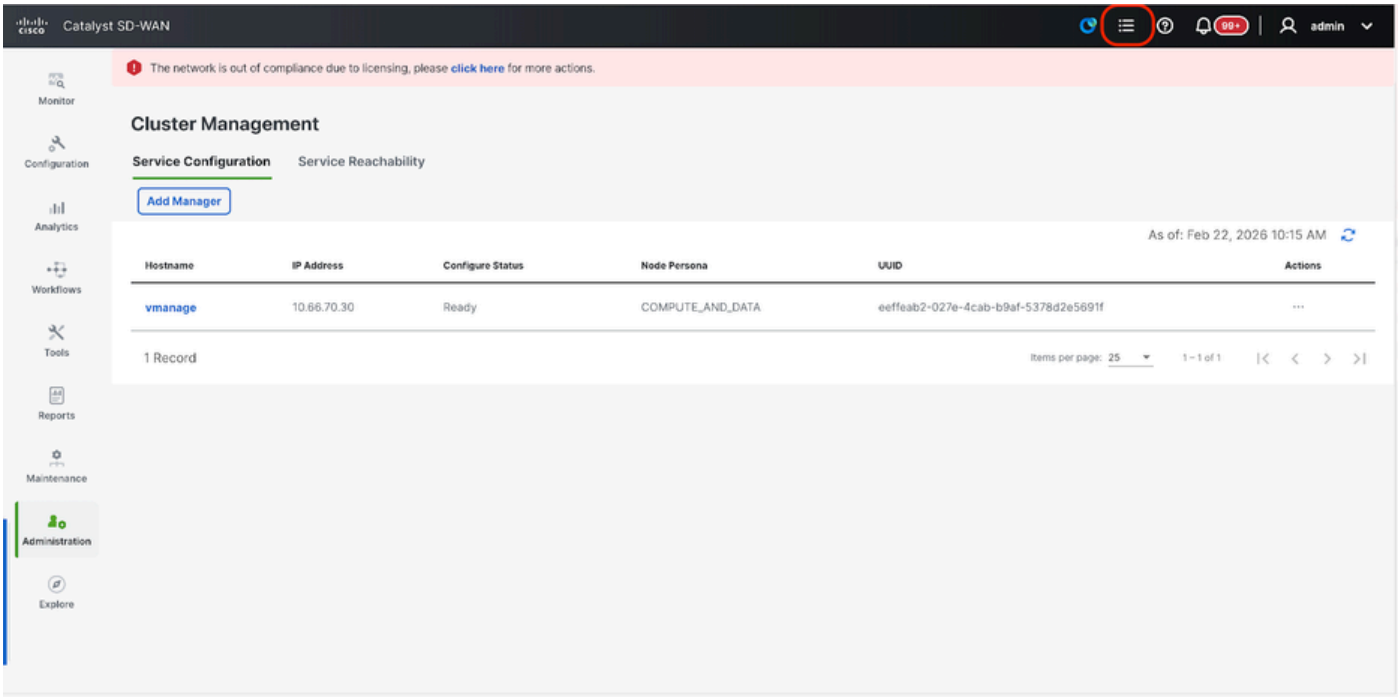
- 在vManage-1的WebUI上，導航到Administration > Cluster Management，在Service Configuration部分中，
- 按一下Add Manager，出現一個彈出視窗：





- 根據在vManage - 2節點旋轉時完成的角色配置選擇節點角色。
- 在Manager IP地址下輸入vManage-2的服務介面IP
- 輸入使用者名稱和密碼，該使用者名稱和密碼與我們在步驟6中使用的憑據相同。
- 啟用SDAVC — 保持未選中狀態，因為我們會在vManage-1上啟用它
- 點選Add。
- 之後，vManage 1和2節點的vManage NMS服務在後台重新啟動。對於vManage 1和2，該UI的可用時間大約為5到10分鐘。
- 在此期間，可使用vManage 1和2的CLI訪問。
- 可以訪問vManage-1 UI後，請導航至Administration > Cluster Management，確保vManage和vManage的服務介面IP反映在IP地址下，Configure Status is Ready且節點角色反

映正確。
- 切換到同一頁中的「服務可接通性」部分，並確保兩個vManage節點的所有服務均可訪問。
- 如果尚未看到任何服務，請稍候。通常需要5到10分鐘。
- 您可以在vManage UI右上角的Task-list中檢查集群新增進程的狀態。



- 您可以查詢「活動」任務清單，如果該任務仍列在「活動」任務清單下，則表示該任務尚未完成。
- 您可以按一下該任務檢查其進度。如果該任務未列在「活動」任務清單下，請切換到「已完成」並確保任務成功完成。
- 只有在這些點經過驗證後，才能繼續下一步。

將下一個節點新增到群集之前，需要考慮以下幾點:

請在已新增到群集的所有vManage節點的UI上驗證這些點：

- 導航到Monitor > Overview of vManage UI，確保正確反映了vManage節點的數量，且根據新增到群集的節點數量可以看到。

- 導航到Administration > Cluster Management，並確保兩個vManage的服務介面IP都反映在IP地址下，Configure Status is Ready且節點角色正確反映。
- 切換到同一頁中的「服務可接通性」部分，並確保兩個vManage節點的所有服務均可訪問。

- 每次向群集中新增節點時，群集中所有節點的NMS服務都會重新啟動，因此在一段時間內，這些節點的UI將變得不可達。
- 根據群集中的節點數，可能需要較長的時間才能備份UI以及訪問所有服務。
- 您可以在vManage UI右上角的Task-list下監視任務。
- 在新增到群集的每個節點的vManage UI上，我們需要檢視所有路由器、模板和策略（如果它們在vManage-1中可用）。
- 如果這些配置不存在於vManage-1上，則新增到vManage-1中的vBonds和vSmarts以及組織— 名稱、vBond、證書授權的管理>設定配置必須反映在新增到群集的其餘vManage節點上。

- 對其餘vManage節點重複相同步驟。

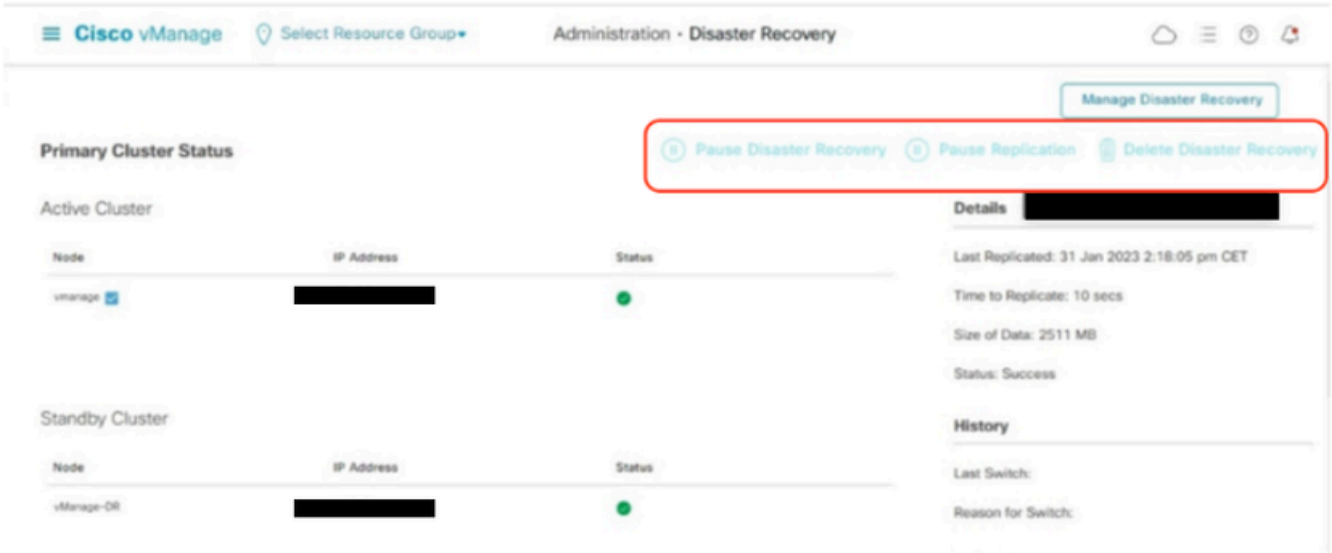
步驟 4:Config-db備份/還原

在另一個vManage節點上收集vManage configuration-db備份和還原

附註：從已啟用災難恢復的現有vManage群集收集配置資料庫備份時，請確保在該節點上的災難恢復暫停並刪除後收集該備份。

確認沒有正在進行的災難恢復複製。導航到管理>災難恢復和 確保狀態為「成功」，而不是處於「匯入掛起」、「匯出掛起」或「下載掛起」等暫時狀態。如果狀態不成功，請聯絡Cisco TAC並確保複製成功，然後繼續暫停災難恢復。

首先暫停災難恢復並確保任務完成。然後刪除災難恢復並確認任務已完成。



聯絡Cisco TAC，確保已成功清理災難恢復。

收集Configuration-DB備份：

- 在當前正在使用的SD-WAN交換矩陣中，可以從vManage群集生成配置資料庫備份。
- 請注意，我們只能在vManage群集中的一個節點（該節點是configuration-db領導者）上生成configuration-db備份。

- 對於獨立vManage，該vManage本身是配置資料庫的領導者。
- 在vManage群集中，使用命令request nms configuration-db diagnostics標識configuration-db領導節點。您可以在3節點vManage群集的所有節點上運行此命令。
- 在6節點集群中，確保在啟用了configuration-db的vManage節點上運行此命令，以標識領導節點。 導覽至Administration > Cluster Management以驗證相同內容：
- 如螢幕截圖所示，配置了persona COMPUTE_AND_DATA的節點正在運行configuration-db。

您可以在vManageCLI上使用requestnmsconfiguration-dbstatus命令進行驗證。輸出如下

```
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#
```

- 一旦您執行命令請求nms configuration-db對這些節點進行診斷，輸出如下：
- 查詢「IsLeader」的突出顯示的欄位。如果設定為1，則表示節點是領導節點，我們可以從中收集配置資料庫備份。

```
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     .
```

使用此命令從標識的configuration-db領導vManage節點收集configuration-db備份。

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

預期輸出如下：

```
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#
```

- 如果已更新configuration-db憑證，請記下該憑證。
- 如果您不知道配置資料庫憑據，請聯絡TAC以從現有vManage節點檢索配置資料庫憑據。

- 預設的configuration-db憑證是使用者名稱：neo4j和密碼：密碼

將Configuration-db備份還原到另一個vManage節點

使用SCP將configuration-db backup複製到vManage的/home/admin/目錄。

scp命令輸出示例：

```
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
```

要恢復configuration-db備份，首先需要配置configuration-db憑據。如果您的配置資料庫憑據是預設值(neo4j/password)，則可以跳過此步驟。

要配置configuration-db憑據，請使用request nms configuration-db update-admin-user命令。使用您選擇的使用者名稱和密碼。

請注意，vManage的應用程式伺服器已重新啟動。由於vManage UI將在短時間內不可訪問。

```
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#
```

可以繼續還原配置資料庫備份的開機自檢：

我們可以使用命令request nms configuration-db restore path /home/admin/< >將configuration-db還原到新的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
```

恢復configuration-db後，確保vManage UI可訪問。等待約5分鐘，然後嘗試訪問UI。

成功登入到UI後，請確保邊緣路由器清單、模板、策略以及以前或現有vManage UI上存在的所有其餘配置都反映在新的vManage UI上。

步驟 5:在vManage群集上啟用災難恢復

重要預檢查

必須配置兩個獨立的vManage 3節點群集並使其正常運行，才能繼續進行災難恢復。在活動群集上，必須安裝驗證器和控制器。如果您在DR站點上有驗證器和控制器，則這些控制器也必須在活動群集上而不是在DR vManage群集上被登入。

思科建議在註冊災難恢復之前，必須滿足以下要求：

- 確保在傳輸VPN(VPN 0)上通過HTTPS可以訪問主節點和輔助節點。
- 確保輔助設定中的Cisco vSmart控制器和Cisco vBond協調器連線到主設定。
- 確保Cisco vManage主節點和輔助節點運行相同的Cisco vManage版本。
- VPN 0中的帶外群集介面（服務介面）。
- 對於集群內的每個vManage例項，除了用於VPN 0（傳輸）和VPN 512（管理）的介面之外，還需要第三個介面（集群鏈路）。
- 此介面用於群集內vManage伺服器之間的通訊和同步。
- 此介面必須至少為1 Gbps，並且延遲為4毫秒或更短。建議使用10 Gbps介面。
- 兩個vManage節點必須能夠通過此介面相互連線：無論是第2層網段還是通過第3層路由。
- 在每個vManage中，必須在GUI中將此介面配置為群集介面(Administration > Cluster Management — 指示自己的帶外群集介面IP地址、使用者和密碼)。

- 為了允許Cisco vManage節點在資料中心之間相互通訊，請在資料中心防火牆上啟用TCP埠8443和830。
- 確保在兩個Cisco vManage節點上啟用所有服務（應用伺服器、配置資料庫、消息伺服器、協調伺服器和統計資訊資料庫）。
- 在主資料中心和輔助資料中心之間分發所有控制器，包括Cisco vBond協調器。確保這些控制器可通過分佈在這些資料中心的Cisco vManage節點訪問。控制器僅連線到主Cisco vManage節點。
- 確保主用（主）和備用（輔助）Cisco vManage節點中沒有其他操作正在進行。例如，確保沒有伺服器正在將模板升級或附加到裝置。
- 如果已啟用Cisco vManage HTTP/HTTPS代理伺服器，請將其禁用。請參閱HTTP/HTTPS代理伺服器以瞭解Cisco vManage與外部伺服器的通訊。如果不禁用代理伺服器，Cisco vManage將嘗試通過代理IP地址建立災難恢復通訊，即使Cisco vManage帶外群集IP地址可直接訪問。災難恢復註冊完成後，您可以重新啟用Cisco vManage HTTP/HTTPS代理伺服器。
- 開始災難恢復註冊過程之前，請導航至主Cisco vManage節點上的Tools > Rediscover Network視窗，並重新發現Cisco vBond Orchestrator。

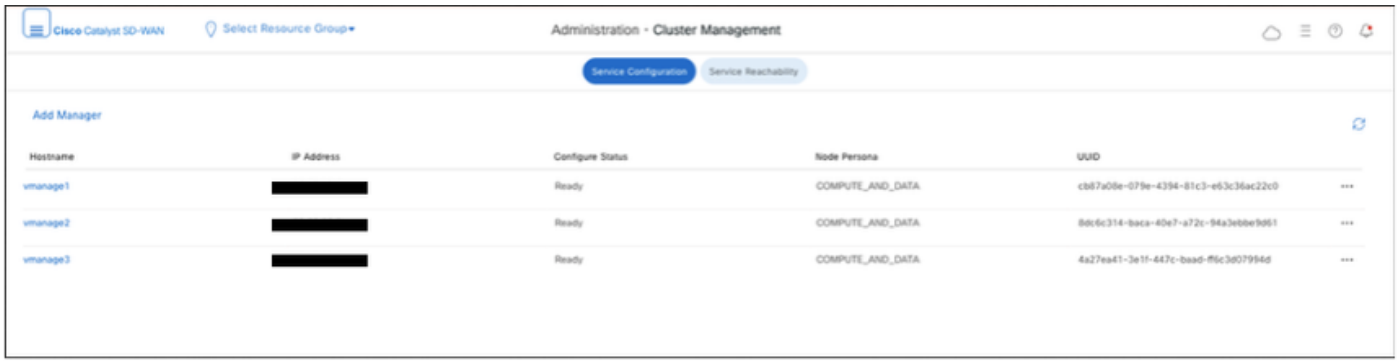
組態

有關vManage Disaster Recovery的詳細資訊，請參閱此鏈接。

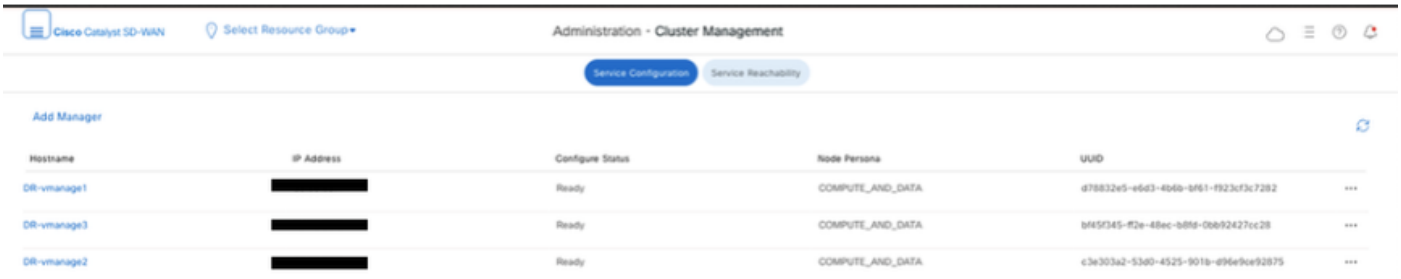
假設每個SD-WAN管理器具有最低配置且認證部分已完成，則已經建立了兩個單獨的3節點群集。

在兩個群集上導航到Administration > Cluster Management，並驗證所有節點是否處於就緒狀態。

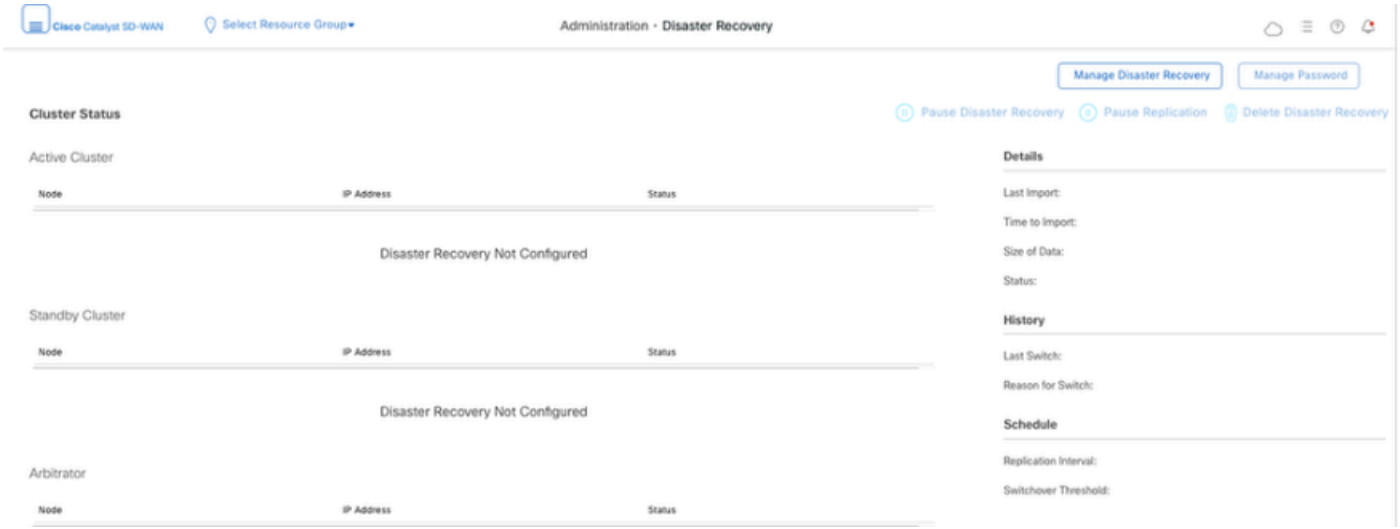
DC vManage



DR vmanage



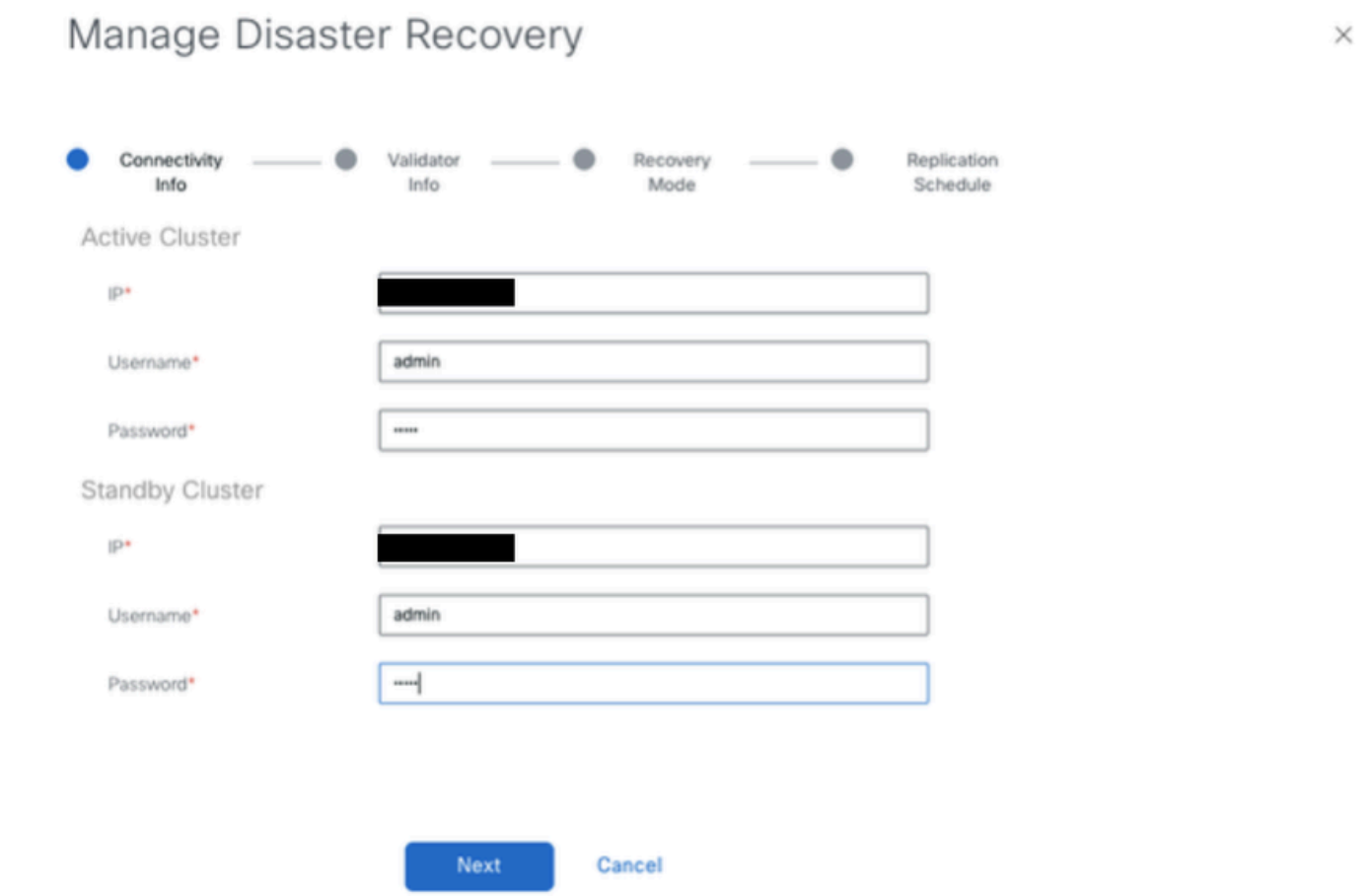
導航到Administration>Disaster Recovery of Primary vManage Cluster。按一下Manage Disaster Recovery。



在彈出視窗中，填寫主要和輔助vManage的詳細資訊。

要指示的IP地址是帶外群集介面的IP地址。 最好在每個集群中使用vManage-1的VPN 0服務介面的IP地址。

憑據必須是netadmin使用者的憑據，並且配置DR後不能更改這些憑據，除非將其刪除。 可以使用單獨的vManage本地使用者憑據進行災難恢復。我們需要確保vManage本地使用者是netadmin組的一部分。此處也可以使用管理員憑據。



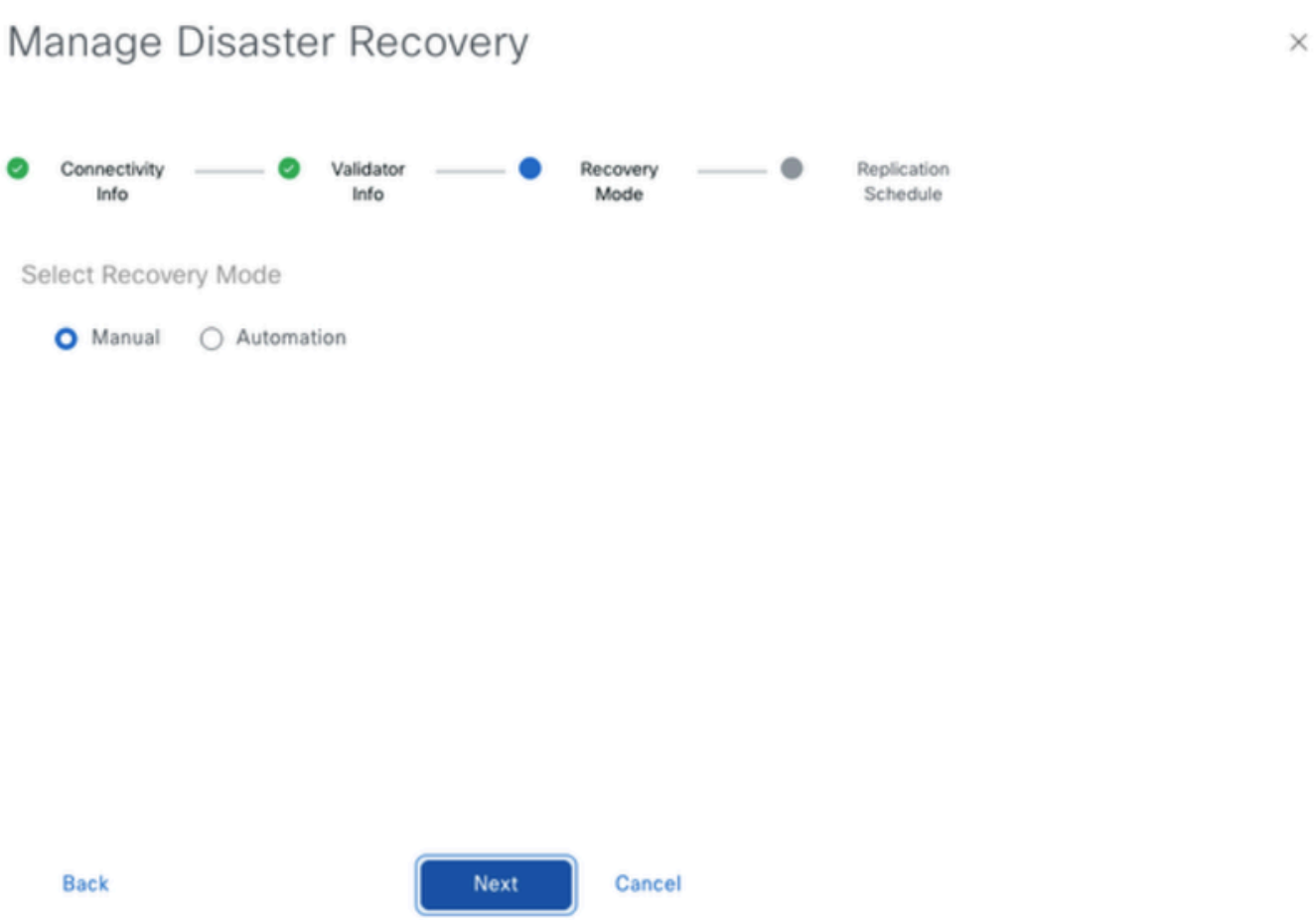
填寫完畢後，按一下下一步。

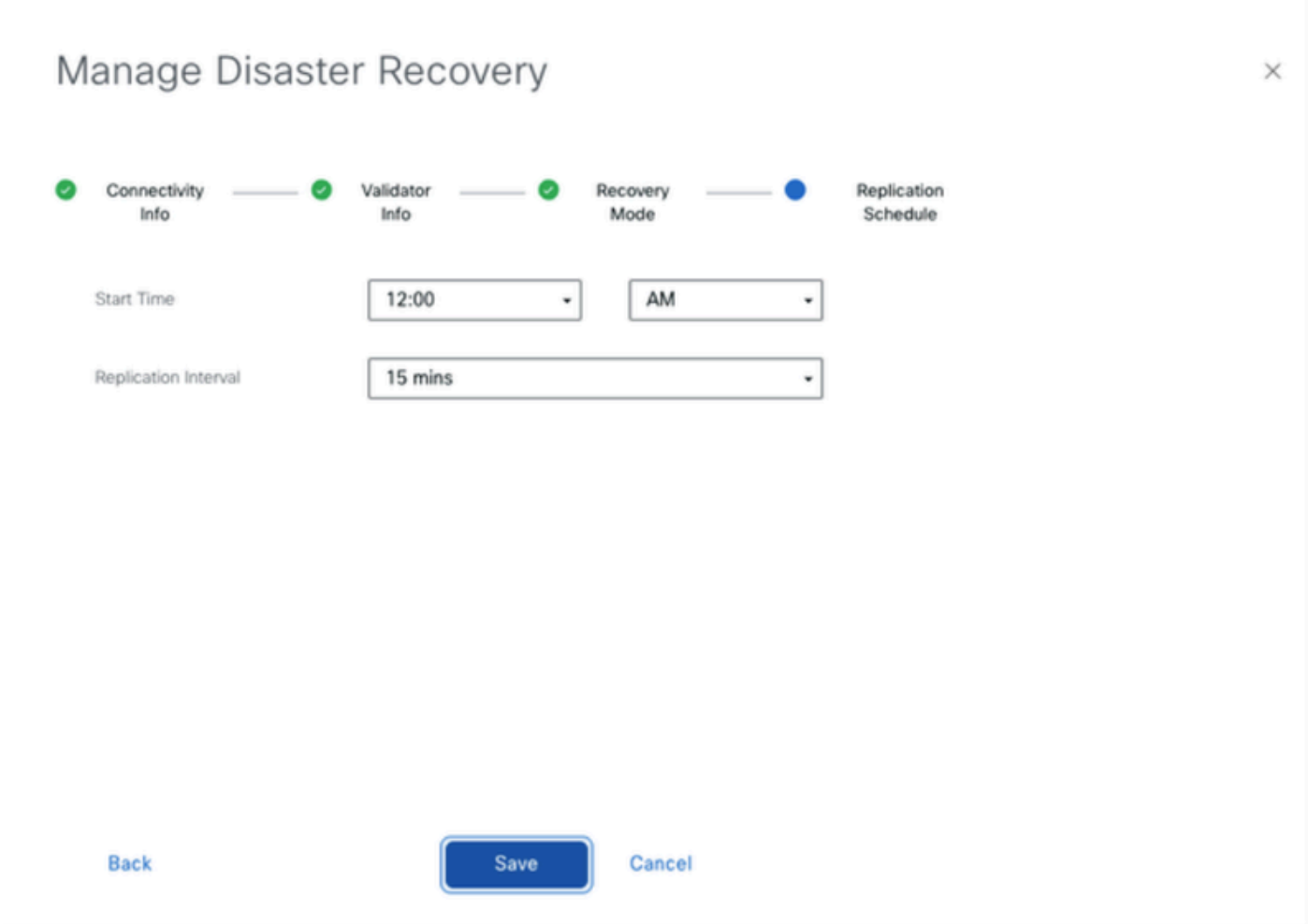
- 填寫vBond控制器的詳細資訊。

vBond控制器必須能夠通過Netconf以指定的IP地址訪問。

填寫完畢後，按一下下一步。

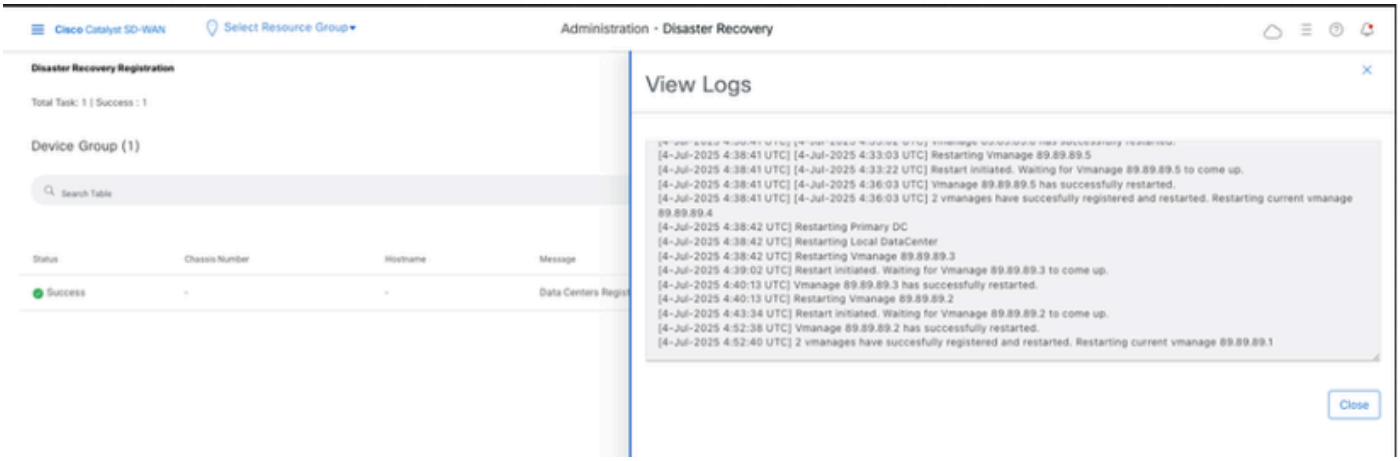
- 在「Recovery Mode（恢復模式）」中選擇Manual。自動化模式已棄用。按「Next」（下一步）。


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



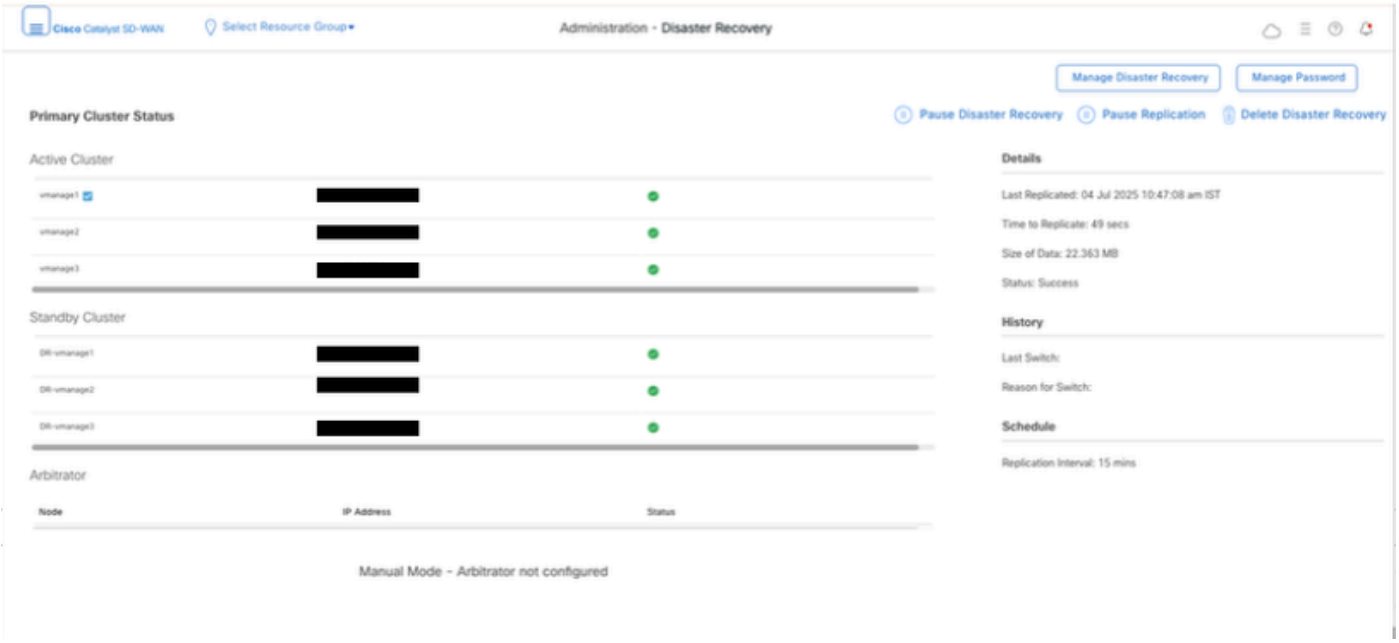
設定值，然後按一下Save。

- DR註冊現在開始。按一下刷新按鈕以手動刷新狀態和進度日誌。此過程可能需要20-30分鐘。



驗證

導航到管理>災難恢復，以檢視災難恢復狀態以及上次複製資料的時間。



附註：複製可能需要幾個小時，具體取決於資料庫大小。此外，它可能需要幾個週期才能成功完成複製。

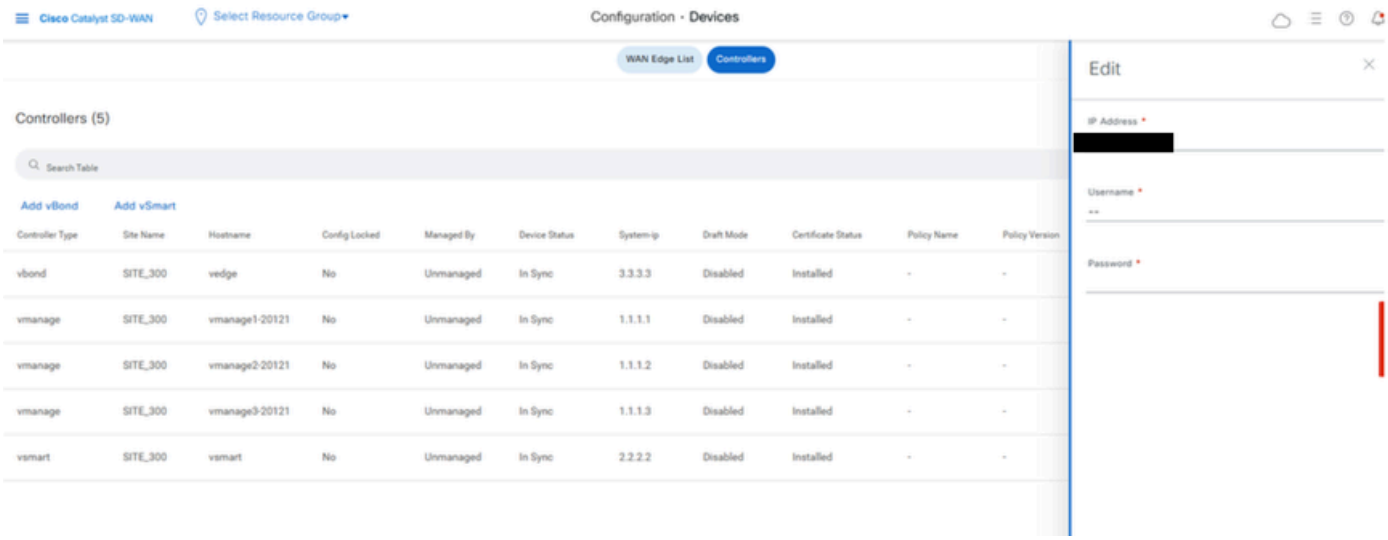
步驟 6:控制器的重新驗證和舊控制器的失效

恢復configuration-db後，我們需要重新驗證交換矩陣中的所有新控制器(vmanage/vsmart/vbond)

註：在實際生產中，如果用於重新身份驗證的介面IP是隧道介面IP，則需要確保在vManage、vSmart和vBond的隧道介面以及路徑沿途的防火牆上允許NETCONF服務。要開啟的防火牆埠是作為從DR群集到所有vBonds和vSmarts的雙向規則的TCP埠830。

在vmanage UI上，點選Configuration > Devices > Controllers

- 按一下每個控制器附近的三個點，然後按一下「Edit（編輯）」



- 將ip-address（控制器的系統ip）替換為transport vpn 0（隧道介面）ip地址。輸入使用者名稱和密碼，然後按一下save
- 對交換矩陣中的所有新控制器執行相同操作

同步根證書鏈

載入所有控制器後，完成以下步驟：

在新活動群集中的任何Cisco SD-WAN Manager伺服器上，執行以下操作：

輸入以下命令將根證書與新活動群集中的所有Cisco Catalyst SD-WAN裝置同步：

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

輸入以下命令將Cisco SD-WAN Manager UUID與Cisco SD-WAN驗證器同步：

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

在交換矩陣恢復後，交換矩陣中的所有邊緣和控制器的控制和bfd會話均已啟動，我們需要從UI使舊控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，點選Configuration > Devices > Certificates
- 按一下「Controllers（控制器）」
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。按一下「invalidate（失效）」
- 點選send to vbond
- 在vmanage UI上，點選Configuration > Devices > Controllers
- 從舊交換矩陣按一下控制器(vmanage/vsmart/vbond)附近的三個點。點選刪除(Delete)

過帳支票

這些後期檢查適用於所有部署組合。

重新啟用雲邊緣路由器：

- 如果C8000v是重疊和託管簽名的一部分，則需要重新進行身份驗證，即：

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

        token
```

- 確認控制連線和BFD會話已啟動
- 確認應用程式流量正在端到端流動
- 如果在邊緣上重建交換矩陣之前對埠躍點進行了更改，則必須恢復這些更改
- 驗證專案是否按預期顯示：
    - 模板
    - 政策
    - 裝置頁面（兩個頁籤）WAN vEdge機架控制器

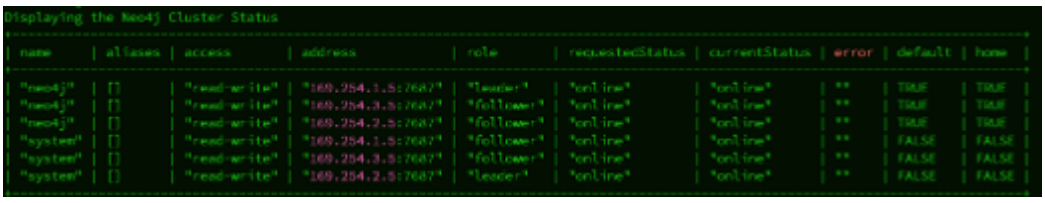
  vManage post checks

- 適用於vManage節點：

  Configuration-DB(Neo4j)檢查：

  在所有vManage節點上執行「request nms configuration-db diagnostics」命令：

  1.檢查節點聯機狀態和Leadership狀態：（不適用於所有版本）



「Neo4j」必須線上顯示3個節點、1個領導者和2個追隨者。「system」也必須顯示3個節點聯機，1個引導節點和2個跟隨者，但由於這不是預設的資料庫，因此預設標誌為false。如果每個neo4j中的條目少於3個，則系統表示節點從群集中脫落。請與Cisco TAC聯絡，進行相同疑難排解。

2.檢查是否有任何節點為「隔離」。

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

所有節點均不能處於隔離狀態。

3.架構驗證必須是「成功」。

```
##########################################
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.使用「request nms configuration-db diagnostics」命令收集configuration-db備份，並確保其成功。

```
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#
```

如果發現任何不一致或錯誤，請聯絡Cisco TAC進行故障排除。

或者，我們可以運行這些API呼叫以確認集群的vmanage節點狀態（對於所有COMPUTE+DATA節點） — 僅在20.12版及更高版本上運行

```
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
```

確保在一個集群中只有一個neo4j和系統的領導，並作為跟隨者駐留。確保所有節點都處於聯機狀態。如果有3個節點集群（所有三個節點都是COMPUTE+DATA），則對於neo4j和系統，必須只有一個領導。任何偏差，您必須聯絡TAC

5.在/var/log/kern.log中檢查所有磁碟、記憶體、IO錯誤。需要在所有vManage節點上檢查此項。

6.為在每個節點之間沒有CC的vmanage建立一個新群集時，請檢查該步驟
從節點1到其他節點cluster ip執行vmanage-admin的ssh，反之亦然，以檢查公鑰是否已交換，且密碼更少的ssh是否起作用[此處步驟需要同意令牌]

```
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:
```

如果輸出要求輸入密碼，請聯絡TAC

控制器開機自檢檢查：

適用於所有SD-WAN控制器(vBond、vManage、vSmart):

在重疊中的所有控制器上執行命令，並確認所看到的vManage UUID和序列號對當前交換矩陣有效：

vBond命令：

show orchestrator valid-vsmarts

show orchestrator valid-vmanage-id

vManage/vSmart命令：

show control valid-vsmarts

show control valid-vmanage-id

請注意，show control valid-vsmarts的輸出包括vSmarts和vManage節點的序列號。

請將其與vManage UI中顯示的內容進行比較。導覽至Configuration > Certificates > Controllers一節。

如果發現當前未註冊到交換矩陣的UUID/序列號有任何附加條目，我們必須將其刪除。您可以聯絡思科TAC取得相同結果。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。