重建Catalyst SD-WAN交换矩阵

目录

简介

本文档介绍如何重建Cisco SD-WAN交换矩阵，包括备份和恢复各种部署的控制器配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- 思科软件中心
- 从software.cisco.com下载控制器软件

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

重建交换矩阵之前的必备条件

- 必须为控制器的新交换矩阵配置一组新的系统ips、站点ID
- 确保防火墙规则到位，以启用控制器与边缘之间的通信
- 注意neo4j(configuration-db)用户名和密码（在集群中的所有vManage节点上必须相同）
- 在所有边缘上禁用端口跃点
- 将平稳重启计时器增加到7天
- 在迁移之前清除三方工具中的警报
- 历史统计信息数据（警报、事件、设备统计信息等）将丢失，除非事先设置要将统计信息导出到外部服务器(如asvAnalytics)
- 如果配置了Cloud OnRamp，请确保您在本练习开始之前能够访问在云中部署的c8000v
- 如果在旧交换矩阵上启用了SDAVC，请确保新交换矩阵已启用它（对于集群，它只需在单个节点上启用）
- 只有与原始交换矩阵相同的版本才支持Configuration-db恢复
- 确认用于控制器的角色。我们支持COMPUTE_DATA和DATA角色（每个部分下的详细信息）

- 对于企业CA，需要使用由企业CA颁发的根证书（用于现有重叠），证书使用企业CA服务器签名并通过UI为所有控制器安装

部署选项

vManage部署

- 独立（1个节点）
- 集群（3节点或6节点）

DR选项

- 无DR
- 单节点DR
- 备用DR群集（手动/管理触发）

注意：有关灾难恢复类型的更多详细信息，请参阅此链接

组合：

#	vManage设置	DR选项
1	独立（1个节点）	无DR
2	独立（1个节点）	单节点DR
3	集群（3节点或6节点）	无DR
4	集群（3节点或6节点）	备用DR群集

适用于所有组合的通用步骤

这些步骤对所有部署组合都通用。它们涵盖启动VM实例和应用基本CLI配置的过程。每个组合部分都会告诉您要部署多少实例以及要完成的其他步骤。

安装和启用SD-WAN控制器（管理器、验证器、控制器）

注意：思科已更改某些术语的品牌，因此这些术语可以互换。Cisco vManage = Cisco Catalyst Manager、Cisco vBond = Cisco Catalyst Validator、Cisco vSmart = Cisco Catalyst Controller

---

从Cisco软件下载页面下载SD-WAN控制器的OVA文件此处:

- 选择vEDGE Cloud并下载所需软件版本的vBond OVA。
- 选择vManage软件并下载所需软件版本的vManage OVA。
- 选择vSmart软件并下载所需软件版本的vSmart OVA。

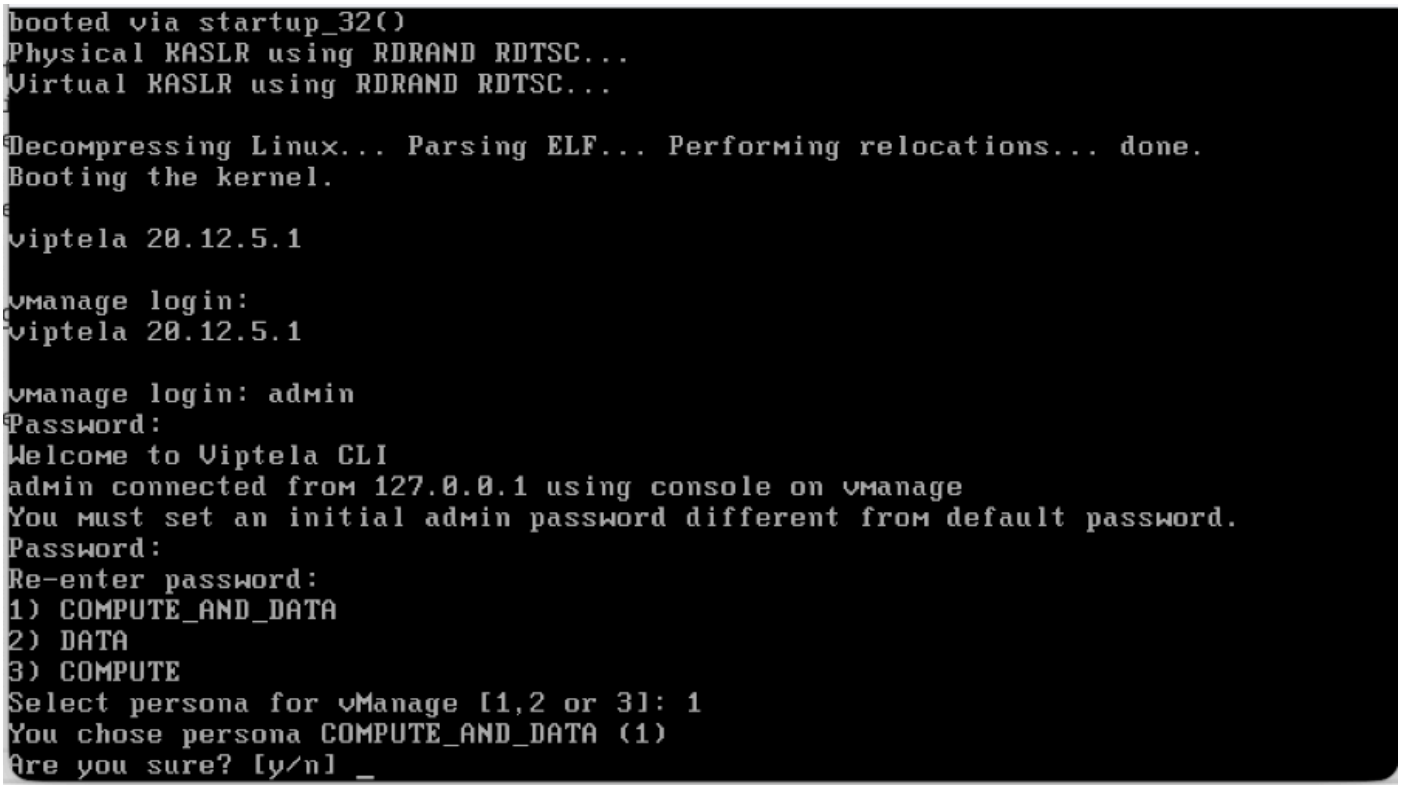
注意：在ESXi/云平台上使用OVA文件启动vSmart、vBond和vManage控制器。请参阅链接文档，并确保根据SD-WAN部署类型为所有控制器分配足够的CPU、RAM和磁盘。导航到此处以获取其他信息。请确保将辅助磁盘分配给vManage节点，如链接的计算指南的“存储大小*”列中所述。

启动Cisco Manager节点

- 部署Cisco Manager或vManage VM且可以访问Manager的控制台后，等待启动完成。一个迹象是，我们看到消息系统已准备就绪，并会提示输入用户名和密码。
- 输入默认用户凭证用户名admin和密码admin。发布提示用户更改密码，根据您的选择设置用户admin所需的密码。
- 然后提示用户选择角色。如果打算使用vManage集群，这是关键步骤。请根据此处所示的场景选择角色：

```
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：为COMPUTE_AND_DATA选择1



选择辅助磁盘，如下所示：

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

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

- 选择辅助磁盘并键入Y进行确认。
- 重新加载Cisco Manager。启动后，使用新配置的新密码输入用户名和密码。

```
early console in extract_kernel
input_data: 0x00000000021753b4
input_len: 0x000000000121c7f3
output: 0x0000000001000000
output_len: 0x000000000237ea6c
kernel_total_size: 0x0000000001fb0000
booted via startup_32()
Physical KASLR using RDRAND RDTSC...
Virtual KASLR using RDRAND RDTSC...

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

viptela 20.12.5.1

vmanage login:
viptela 20.12.5.1

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

- 您可以配置VPN 512 management interface以启用对控制器的带外管理访问。
- 使用命令show interface |选项卡，用于检查接口当前映射到的VPN。
- 相应地配置接口。

示例

```
                                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#
```

注意：您可以在此处引用现有vManage的配置并配置相同的IP地址方案。

管理接口(VPN 512)配置

- 如果需要将接口从VPN 0移动到VPN 512，请使用以下命令，然后在该接口上配置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



!
```

启动验证器

- 在虚拟机监控程序上，为vBond节点配置所需的计算（CPU、RAM和磁盘），然后打开电源。
- 一旦控制台可以访问，请等待vBond完全启动。等待出现“System Ready（系统就绪）”信息。

- 然后，系统提示输入用户名和密码。输入默认用户凭据用户名admin和密码admin。在此之后，系统将提示用户更改密码，并根据您的选择设置用户admin所需的密码。
- 您可以配置VPN 512管理接口以启用对控制器的带外管理访问。
- 使用命令show interface |选项卡，用于检查接口当前映射到的VPN。
- 相应地配置接口。

示例：

```
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#
```

注意：您可以参考现有vBond中的配置，并在此处配置相同的配置。

管理接口(VPN 512)配置

- 如果需要将接口从VPN 0移动到VPN 512，请使用以下命令，然后配置接口上的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
```

启动控制器(vSmart)节点

- 执行与验证程序相同的步骤以启动vSmart节点。
- 一旦在所有SD-WAN控制器上配置了VPN 512 IP地址，您就可以使用VPN 512 IP地址上的SSH访问它们。

所有控制器上的基本CLI配置

一旦您拥有对所有控制器的SSH访问权限，请在每个控制器上配置这些CLI配置。

系统配置

```
config t
system
 host-name



 system-ip



 site-id
```

```
 organization-name


 vbond


commit
```

注意:如果我们使用URL作为vBond地址，请确保在VPN 0配置中配置DNS服务器IP地址或确保可以解析这些地址。

传输接口(VPN 0)配置

所有控制器上都需要这些配置，才能启用传输接口，该接口用于与路由器和其余控制器建立控制连接。

```
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：您可以参考现有控制器的配置，如果配置存在，则您可以将此配置添加到新控制器。

仅当需要路由器使用TLS与vManage节点建立安全控制连接时，才将控制协议配置为TLS。默认情况下，所有控制器和路由器都使用DTLS建立控制连接。根据您的要求，此配置是仅在vSmart和vManage节点上必需的可选配置。

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

组合1:独立vManage +无DR

所需实例：

- 1个vManage(COMPUTE_AND_DATA)
- 1个或多个vBond
- 1个或多个vSmart

步骤:

1. 使用通用步骤启动所有实例
2. 预检查
3. 配置vManage UI、证书和板载控制器
4. Config-db备份/恢复
5. 过帐检查

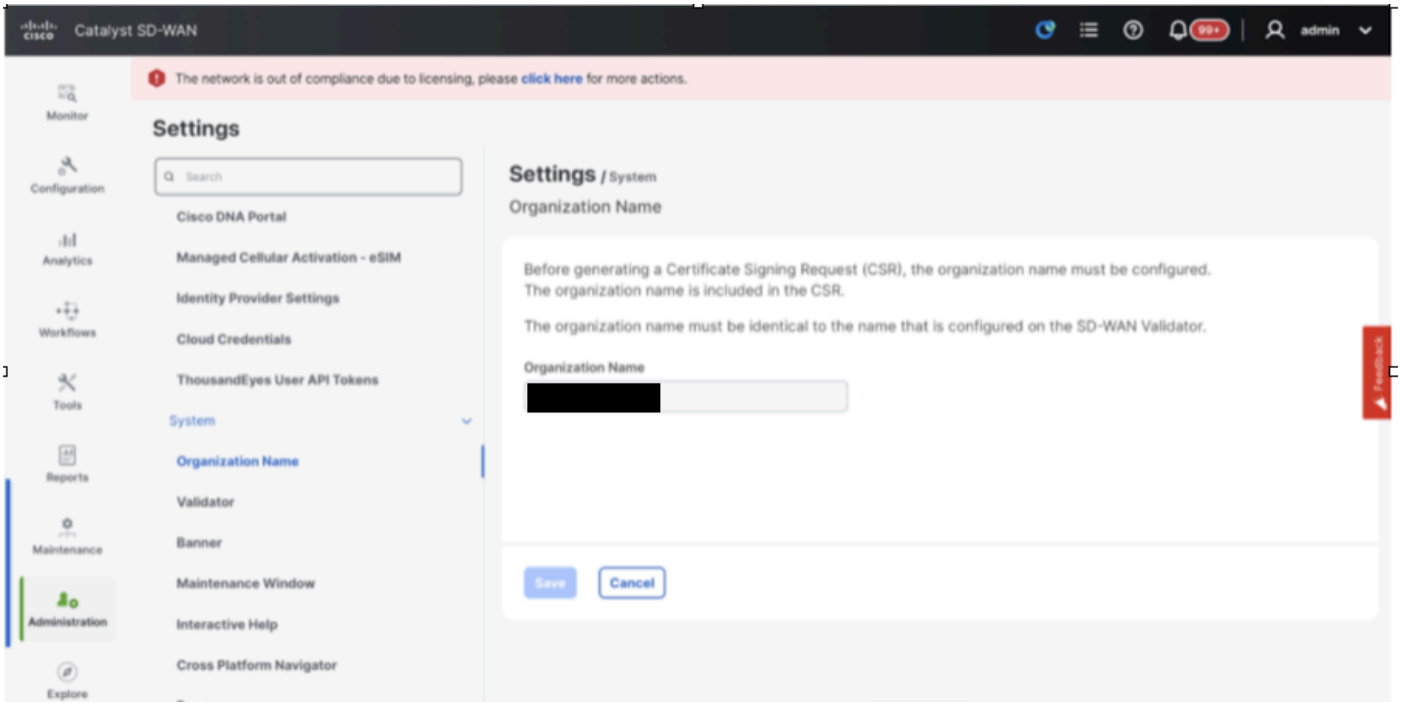
步骤 1：预检查

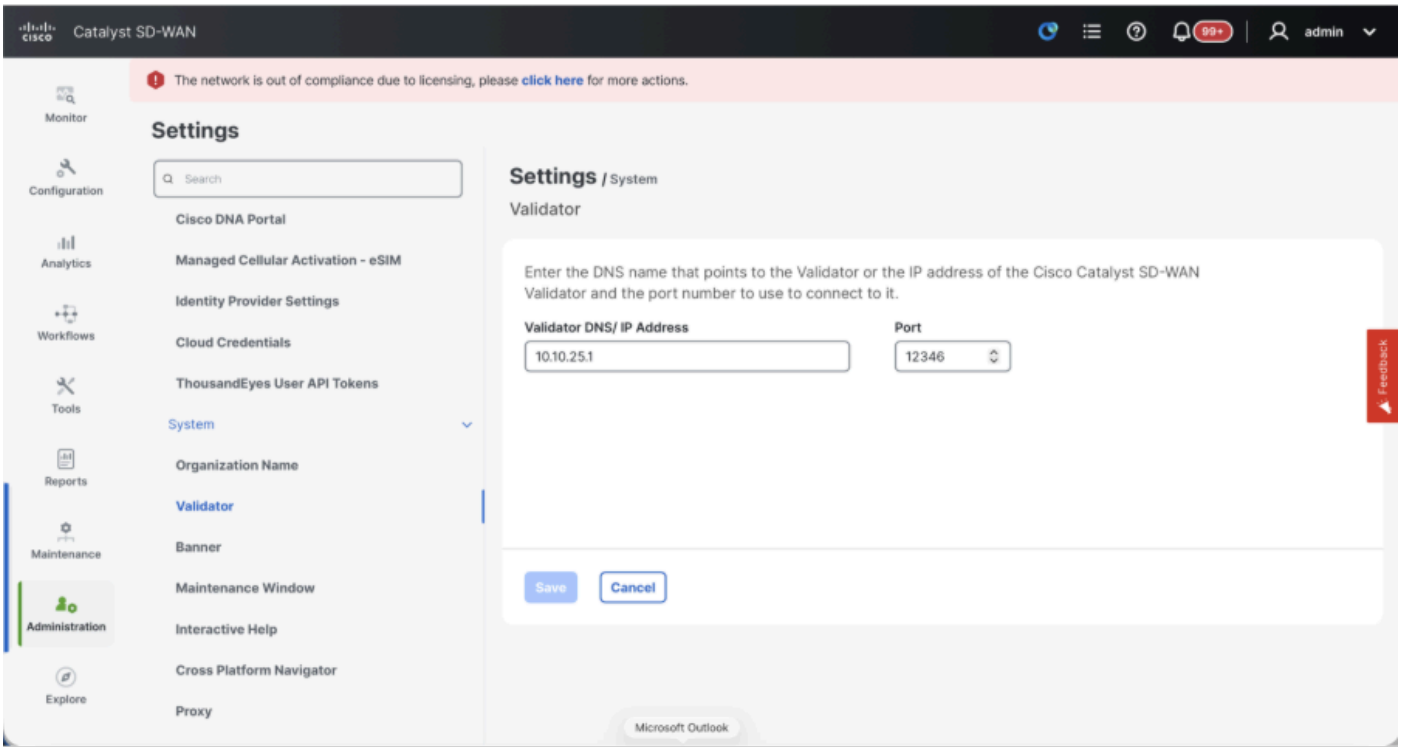
- 确保活动的Cisco SD-WAN Manager实例数与新安装的Cisco SD-WAN Manager实例数相同。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例都运行相同的软件版本。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例能够到达Cisco SD-WAN Validator的管理IP地址。
- 确保证书已安装在新安装的Cisco SD-WAN Manager实例上。
- 确保所有Cisco Catalyst SD-WAN设备(包括新安装的Cisco SD-WAN Manager)上的时钟都同步。
- 确保在新安装的Cisco SD-WAN Manager实例上配置一组新的系统IP和站点ID，同时配置与活动集群相同的基本配置。

步骤 2：配置vManage UI、证书和板载控制器

更新vManage UI上的配置

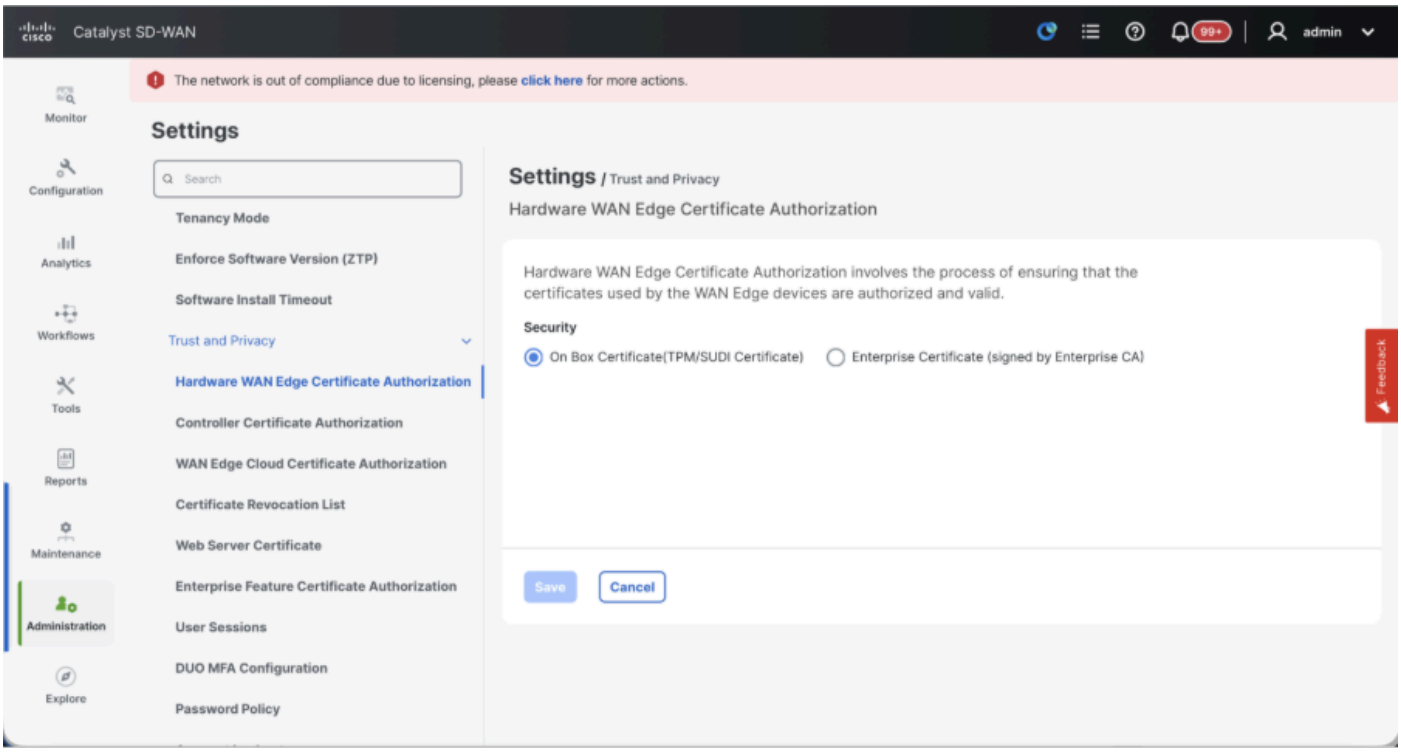
- 一旦将步骤1中的配置添加到所有控制器的CLI中，我们就可以使用浏览器中的URL https://<vmanage-ip>访问vManage的WebUI。使用各个vManage节点的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 导航到管理>设置并完成以下步骤。
- 配置组织名称和验证器/vBond URL/IP地址。配置与vManage节点的CLI中相同的值。
- 在vManage 20.15/20.18中，这些配置在System部分下提供。



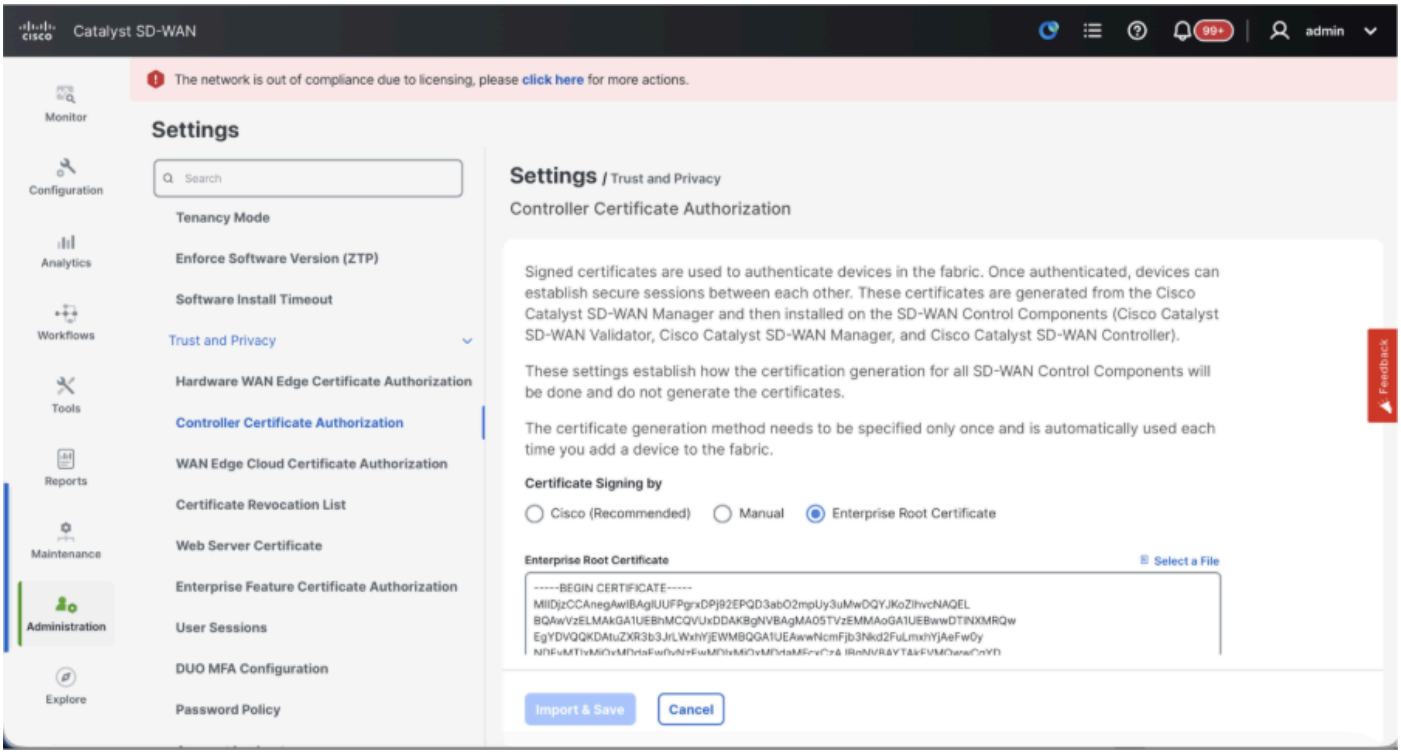


- 验证证书授权(CA)的配置，CA决定用于证书签名的证书颁发机构。我们可以看到3个选项：

1. 硬件WAN边缘证书授权 — 确定硬件SD-WAN边缘路由器的CA。
    - 开箱证书（TPM/SUDI证书）— 使用此选项，路由器硬件上预安装的证书用于建立控制连接（TLS/DTLS连接）
    - 企业证书（由企业CA签署）— 使用此选项时，路由器使用由组织的企业证书颁发机构签署的证书。选择此选项时，必须在此处更新企业CA的根证书。



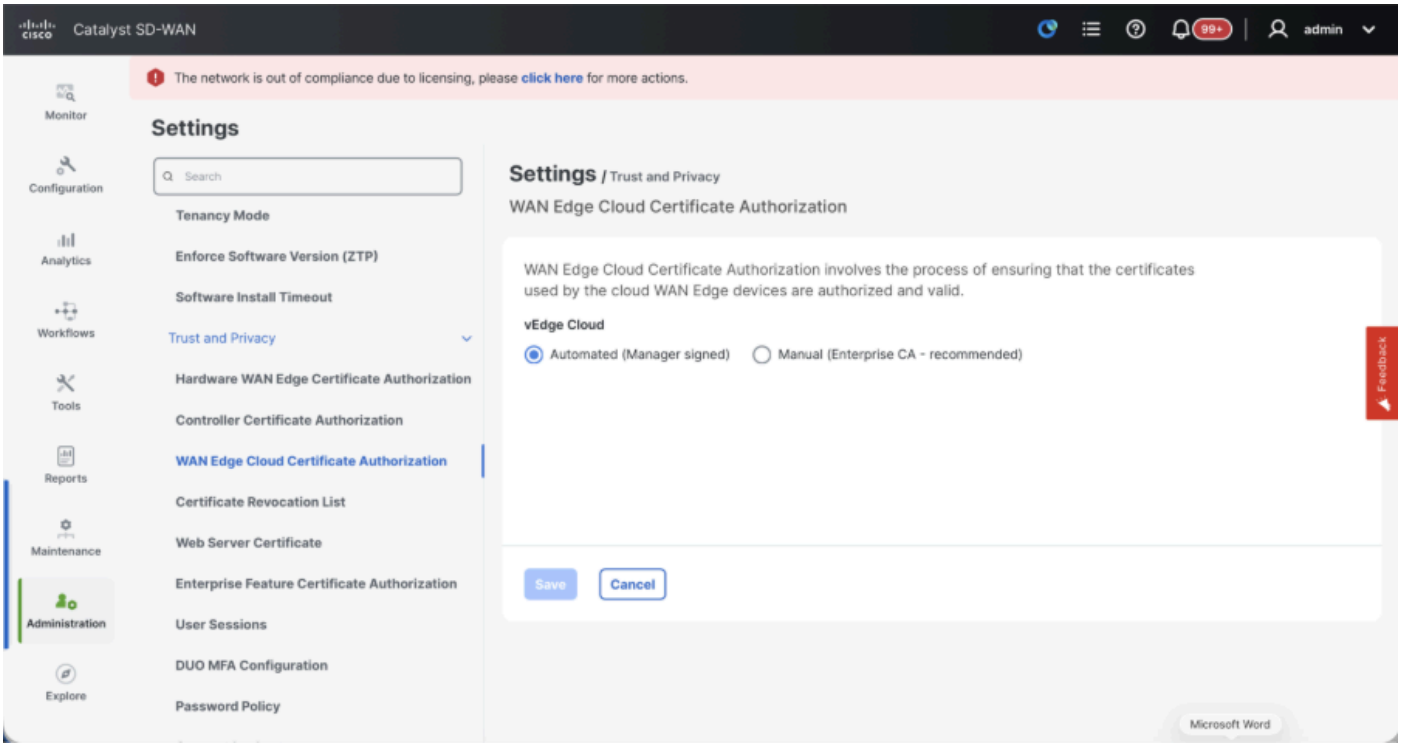
2. 控制器证书授权 — 决定SD-WAN控制器的CA。
   - 思科（推荐） — 控制器使用思科PKI签名的证书。vManage使用vManage上配置的智能帐户凭证自动联系PNP门户，并获取证书签名并安装在控制器上。
   - 手动 — 控制器使用由Cisco PKI签名的证书。使用思科PNP门户手动签署CSR，方法是导航到相应SD-WAN重叠的智能帐户和虚拟帐户。
   - 企业根证书 — 通过此选项，路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。



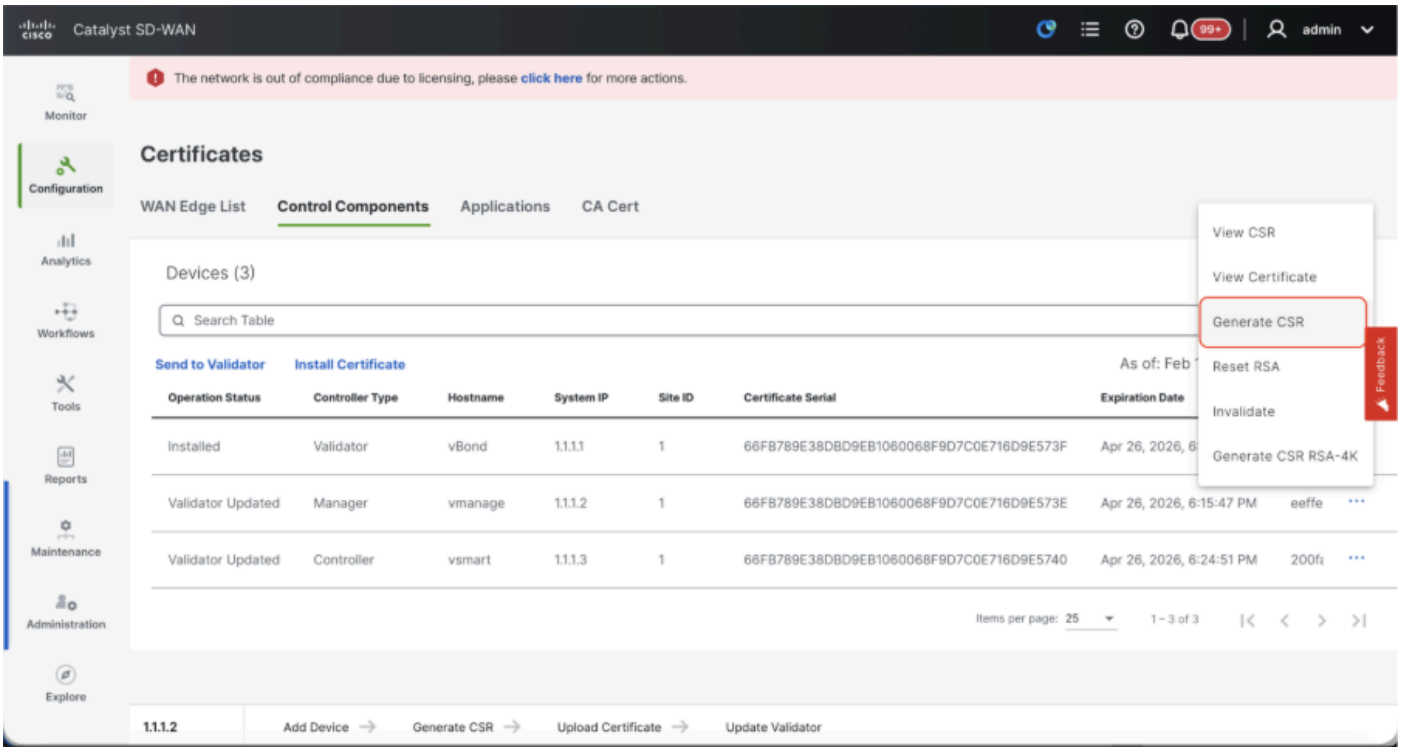
3. 广域网边缘云证书授权 — 确定虚拟SD — 广域网边缘路由器（CSR1000v、C8000v、vEdge云）的CA

- 自动（vManage签名）— vManage自动为虚拟边缘路由器签署CSR并在路由器上安装证书。
- 手动（企业CA — 推荐）— 虚拟路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

例如，如果我们使用自己的CA（企业证书颁发机构），请选择Enterprise。



- 如果是20.15/20.18 vManage节点，请导航到配置>证书>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers
- 为Manager/vManage点击……，然后点击Generate CSR。



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

将vBond/Validator和vSmart/Controller注册到vManage

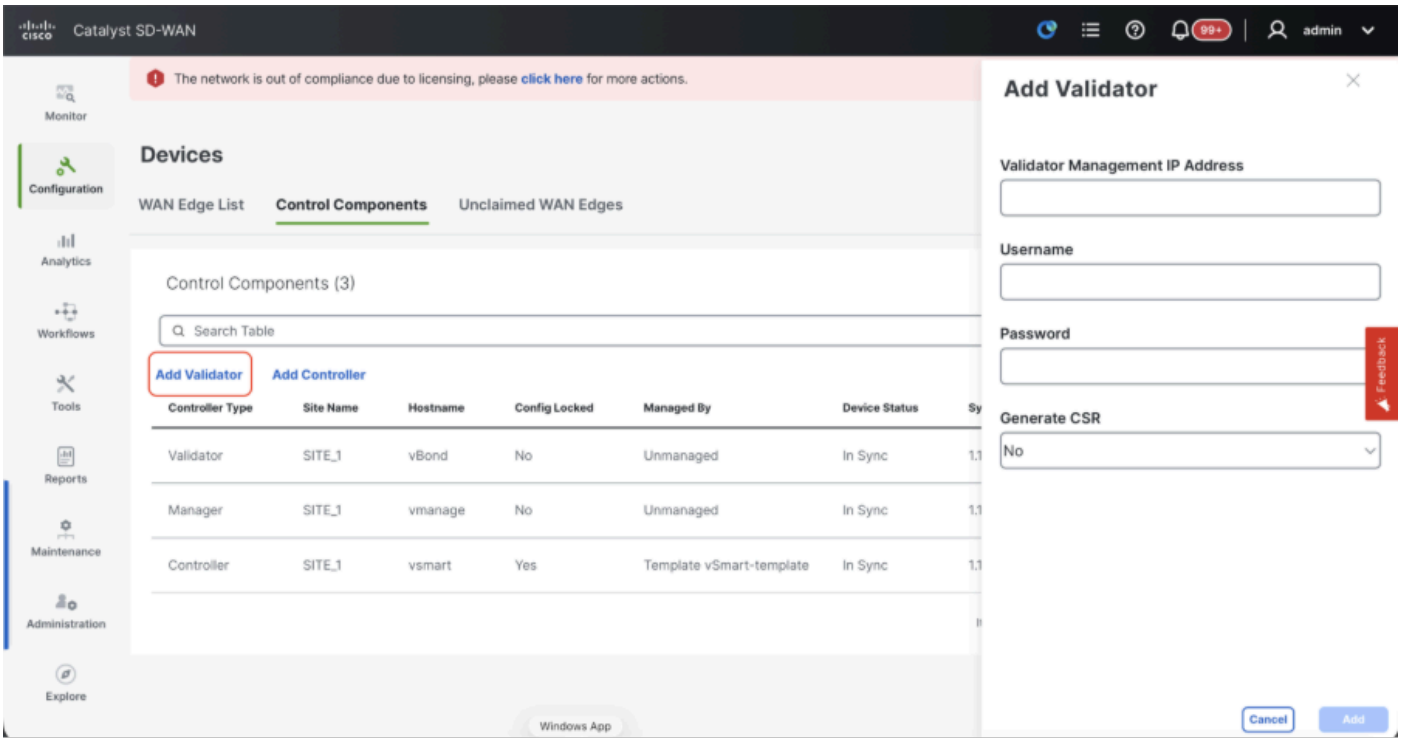
如果是20.15/20.18 vManage节点，请导航到配置>设备>控制组件。对于20.9/20.12版本，请选择Configuration > Devices > Controllers

OnboardingvBond/验证器

- 单击AddvBond对于20.12vManageor的情况添加验证程序20.15/20.18vManage。系统打开一个弹出窗口，输入 vBond的VPN 0传输IP，可从vManage访问。
- 如果允许，请从vManagetovBondIP的CLI使用ping检查可接通性。
- 输入vBond的用户凭证。

注意：我们需要将vBondor的管理凭据用作netadmingroup的用户部分。您可以在vBond的CLI中验证这一点。如果我们需要为vBond安装新证书，请在“生成CSR”的下拉列表中选择是。

注意：如果vBond位于NAT设备/防火墙之后，请检查vBond VPN 0接口IP是否已转换为公共IP。如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口的公用IP地址。

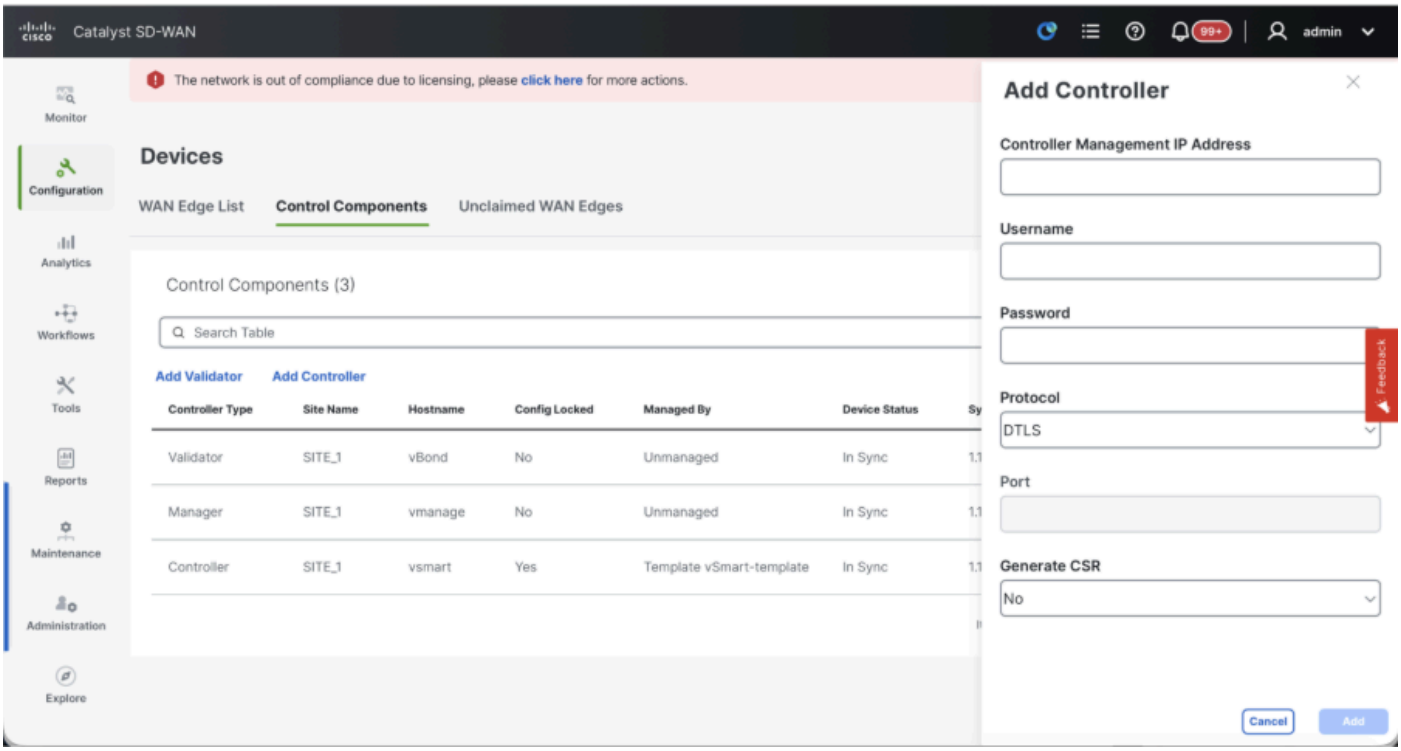


- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vBond上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 如果有多个vBonds，请重复相同的步骤。

自注册vSmart/控制器

- 在20.12 vManage中点击Add vSmart，在20.15/20.18 vManage中点击Add Controller。
- 系统打开一个弹出窗口，输入vSmart的VPN 0传输IP，可从vManage访问。
- 如果允许从vManage的CLI到vSmart IP，请使用ping检查可达性。
- 输入vSmart Note的用户凭据，我们需要使用vSmart的管理员凭据或netadmin组的用户部分。
- 您可以在vSmart的CLI中验证这一点。
- 如果打算对路由器使用TLS来建立与vSmart的控制连接，请将协议设置为TLS。此配置也需要在vSmarts和vManage节点的CLI上进行配置。
- 如果需要为vSmart安装新证书，请在生成CSR"的下拉列表中选择Yes。

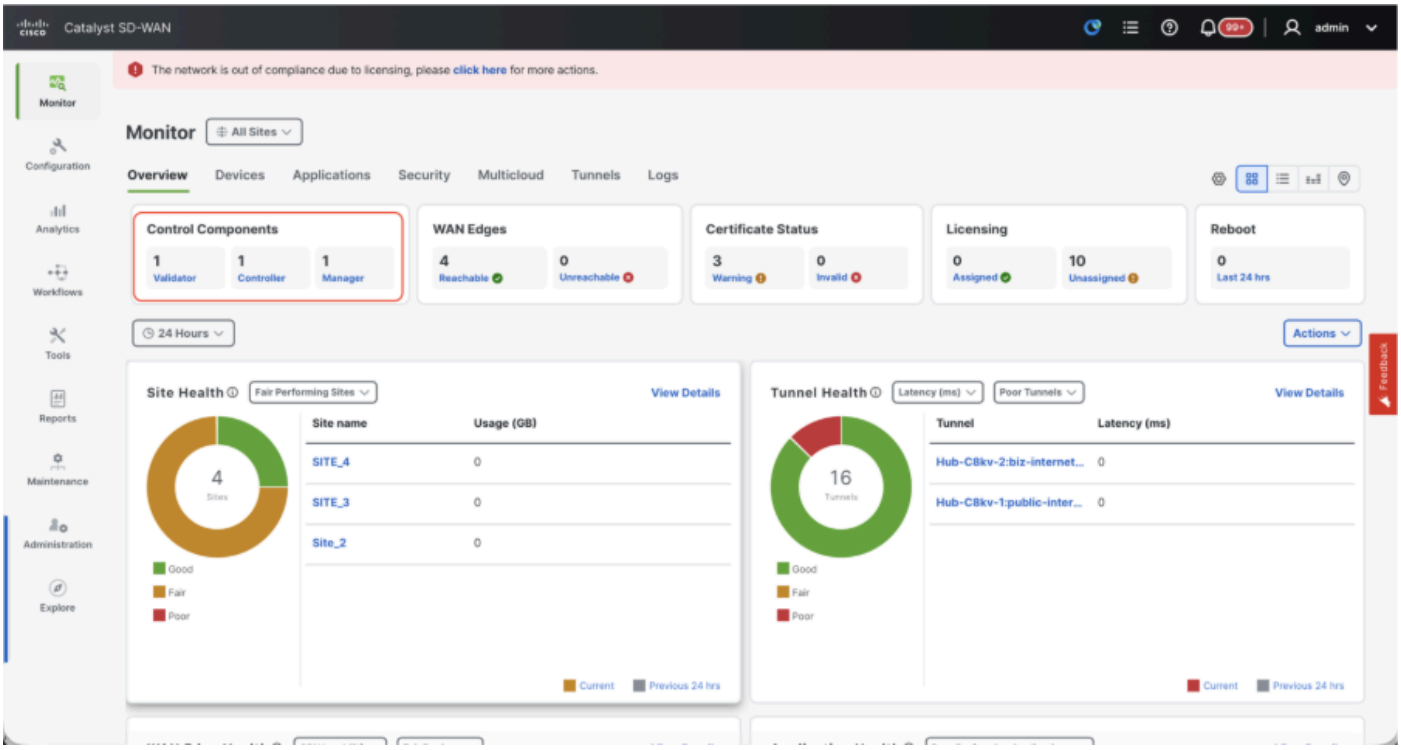
注意：如果vSmart位于NAT设备/防火墙之后，请检查vSmart VPN 0接口IP是否已转换为公共IP，如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口IP的公共IP地址。



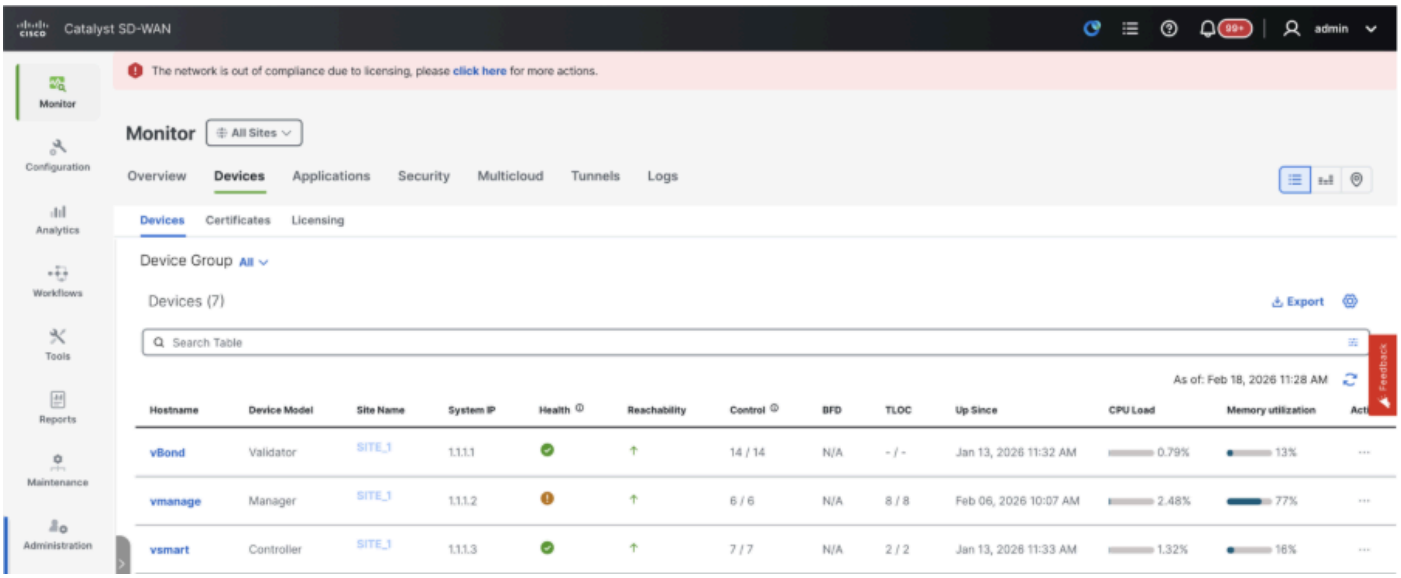
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装在vSmart上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。如果使用Digicert和企业根证书，则适用相同步骤。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果有多个vSmarts，请重复相同的步骤。

确认

完成所有步骤后，在Monitor>Dashboard中确认所有控制组件均可访问



- 单击相应的控制组件，确认它们都可访问。
- 导航到监控>设备，确认所有控制组件均可访问。



步骤 3：Config-db备份/恢复

在另一个vManage节点上收集vManage configuration-db备份和恢复

收集Configuration-DB备份：

- 在当前正在使用的SD-WAN交换矩阵中，您可以在独立vManage和vManage集群设置上生成配置数据库备份。
- 对于独立vManage，该vManage本身是配置数据库领导者。

确认configuration-db正在vManage节点上运行。

您可以使用request nms configuration-db status命令在vManageCLI上检验相同配置。输出如下所示

```
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#
```

使用此命令从已确定的configuration-db领导vManage节点收集configuration-db备份。

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

预期输出如下所示：

```
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凭证，请记下该凭证。
- 如果您不知道配置数据库凭证，请联系TAC从现有vManage节点检索配置数据库凭证。
- 默认的configuration-db凭证是用户名：neo4j和密码：密码

将Configuration-db备份恢复到另一个vManage节点

使用SCP将configuration-db备份复制到vManage的/home/admin/目录。

scp命令输出示例：

```
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
```

要恢复configuration-db备份，首先需要配置configuration-db凭据。如果您的配置数据库凭证是默认凭证(neo4j/password)，我们可以跳过此步骤。

要配置configuration-db凭证，请使用命令request nms configuration-db update-admin-user。使用您选择的用户名和密码。

请注意，vManage的应用服务器已重新启动。由于此vManage UI在短时间内变得不可访问。

```
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#
```

发布后，我们可以继续恢复configuration-db备份：

我们可以使用命令request nms configuration-db restore path /home/admin/< >将配置数据库恢复到新的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
```

恢复configuration-db后，请确保vManage UI可访问。等待约5分钟，然后尝试访问UI。

成功登录UI后，请确保边缘路由器列表、模板、策略以及之前或现有vManage UI上存在的所有其余配置都反映在新的vManage UI上。

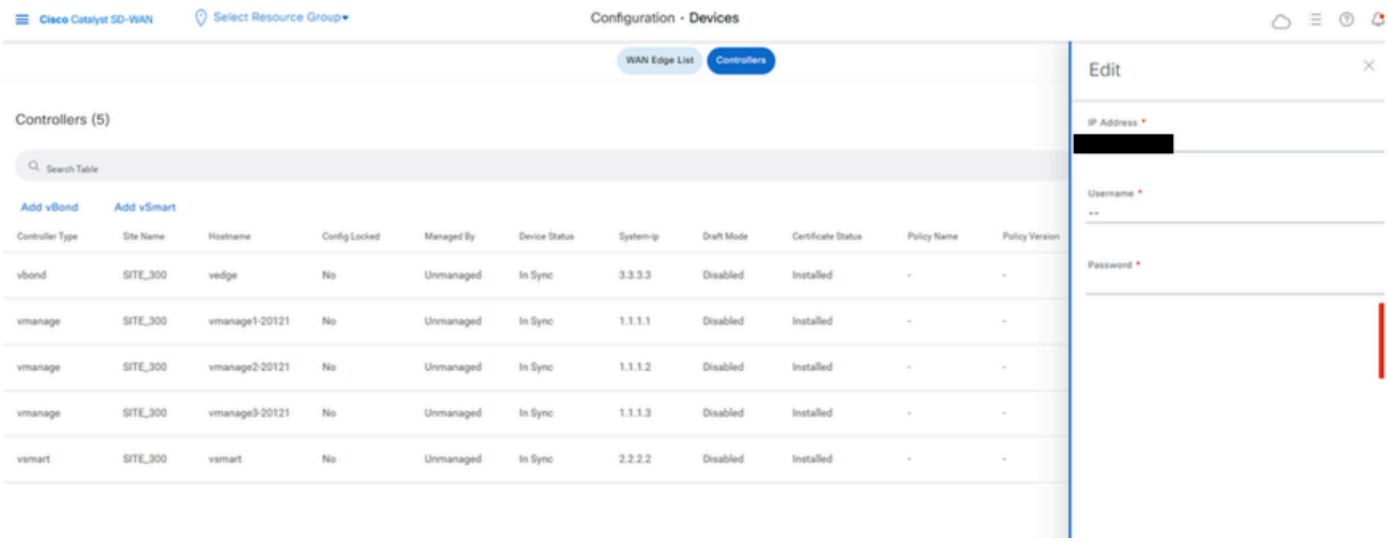
步骤 4：控制器重新验证和旧控制器失效

恢复configuration-db后，我们需要重新验证交换矩阵中的所有新控制器(vmanage/vsmart/vbond)。

注：在实际生产中，如果用于重新身份验证的接口IP是隧道接口IP，则需要确保在vManage、vSmart和vBond的隧道接口以及路径沿途的防火墙上允许NETCONF服务。要打开的防火墙端口是从DR群集到所有vBonds和vSmarts的双向规则的TCP端口830。

在vmanage UI上，点击Configuration > Devices > Controllers

- 点击每个控制器附近的三个点，然后点击Edit



- 将ip-address（控制器的系统ip）替换为传输vpn 0（隧道接口）ip地址。输入用户名和密码，然后点击save
- 对交换矩阵中的所有新控制器执行相同操作

同步根证书链

所有控制器入网后，请完成以下步骤：

在新活动集群中的任何Cisco SD-WAN Manager服务器上，执行以下操作：

输入以下命令将根证书与新活动集群中的所有Cisco Catalyst SD-WAN设备同步：

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

输入以下命令将Cisco SD-WAN Manager UUID与Cisco SD-WAN Validator同步：

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

一旦交换矩阵恢复，并且交换矩阵中的所有边缘和控制器的控制和bfd会话都已启动，我们就需要从UI使旧控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，点击Configuration > Certificates > Controllers
- 点击“控制器”
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)右侧的三个点。点击invalidate（失效）
- 点击send to vbond
- 在vmanage UI上，点击Configuration > Devices > Controllers
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)右侧的三个域。点击Delete

步骤 5：过帐检查

注意：继续此处所示的“后检查”部分，它适用于所有部署组合。

组合2:独立vManage +单节点DR

所需实例：

- 1个vManage（主、COMPUTE_AND_DATA）
- 1个vManage（DR备用、COMPUTE_AND_DATA）
- 1个或多个vBond
- 1个或多个vSmart

步骤:

1. 使用通用步骤启动所有实例
2. 预检查
3. 配置vManage UI、证书和板载控制器
4. 单节点DR设置
5. Config-db备份/恢复
6. 过帐检查

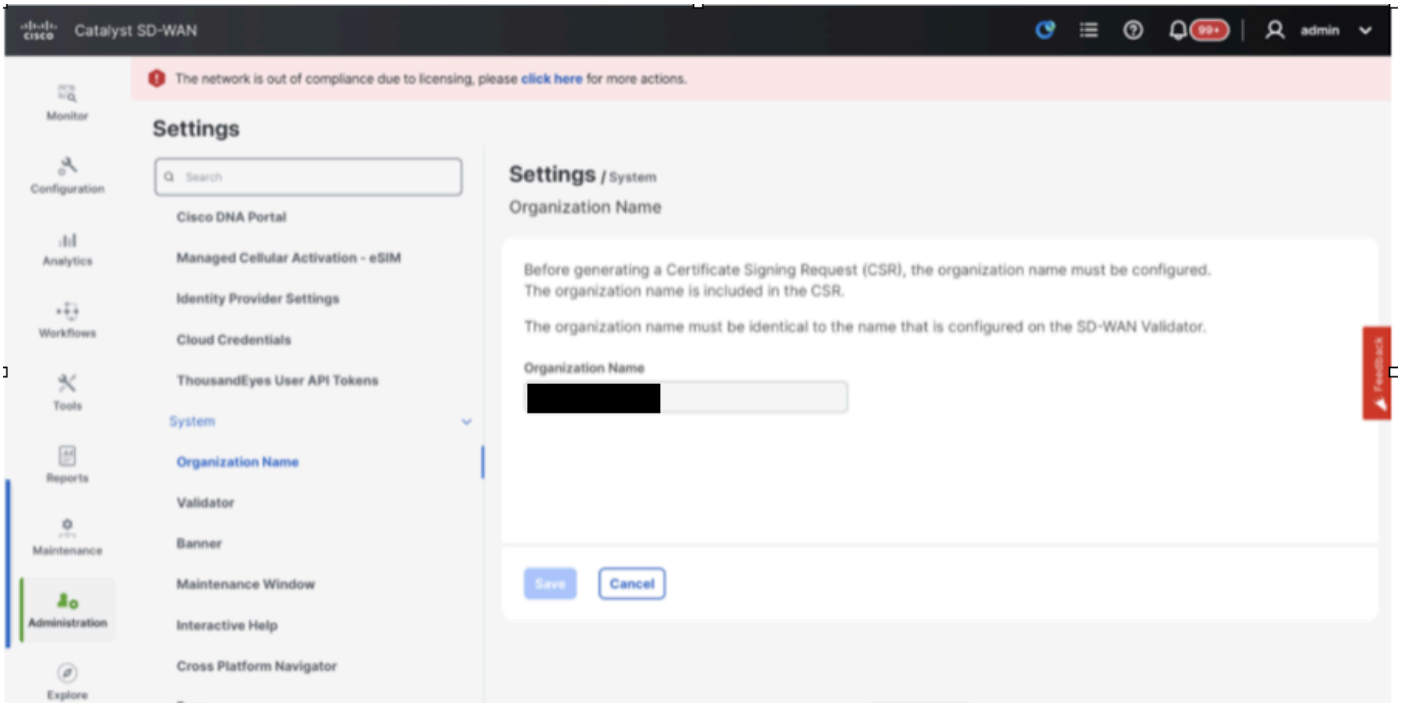
步骤 1：预检查

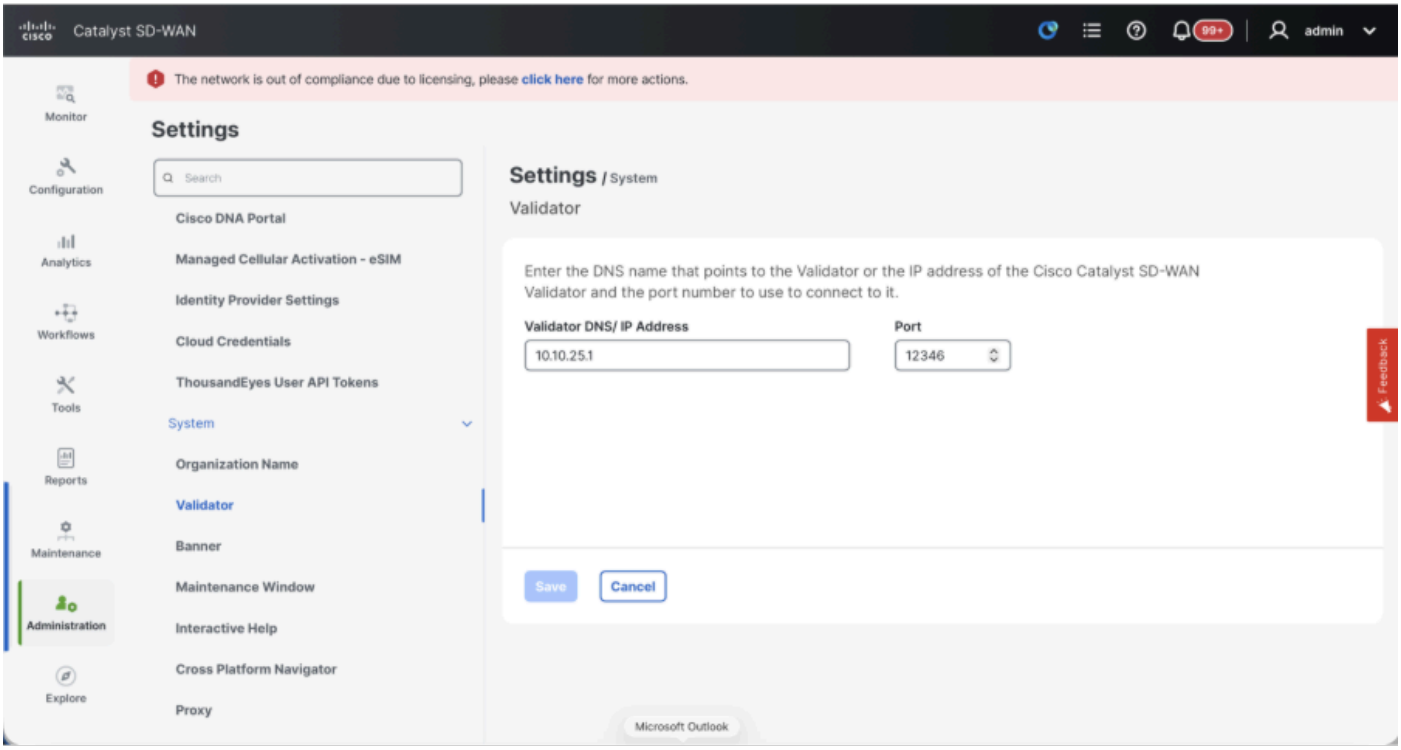
- 确保活动的Cisco SD-WAN Manager实例数与新安装的Cisco SD-WAN Manager实例数相同。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例都运行相同的软件版本。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例能够到达Cisco SD-WAN Validator的管理IP地址。
- 确保证书已安装在新安装的Cisco SD-WAN Manager实例上。
- 确保所有Cisco Catalyst SD-WAN设备(包括新安装的Cisco SD-WAN Manager)上的时钟都同步。
- 确保在新安装的Cisco SD-WAN Manager实例上配置一组新的系统IP和站点ID，同时配置与活动集群相同的基本配置。

步骤 2：配置vManage UI、证书和板载控制器

更新vManage UI上的配置

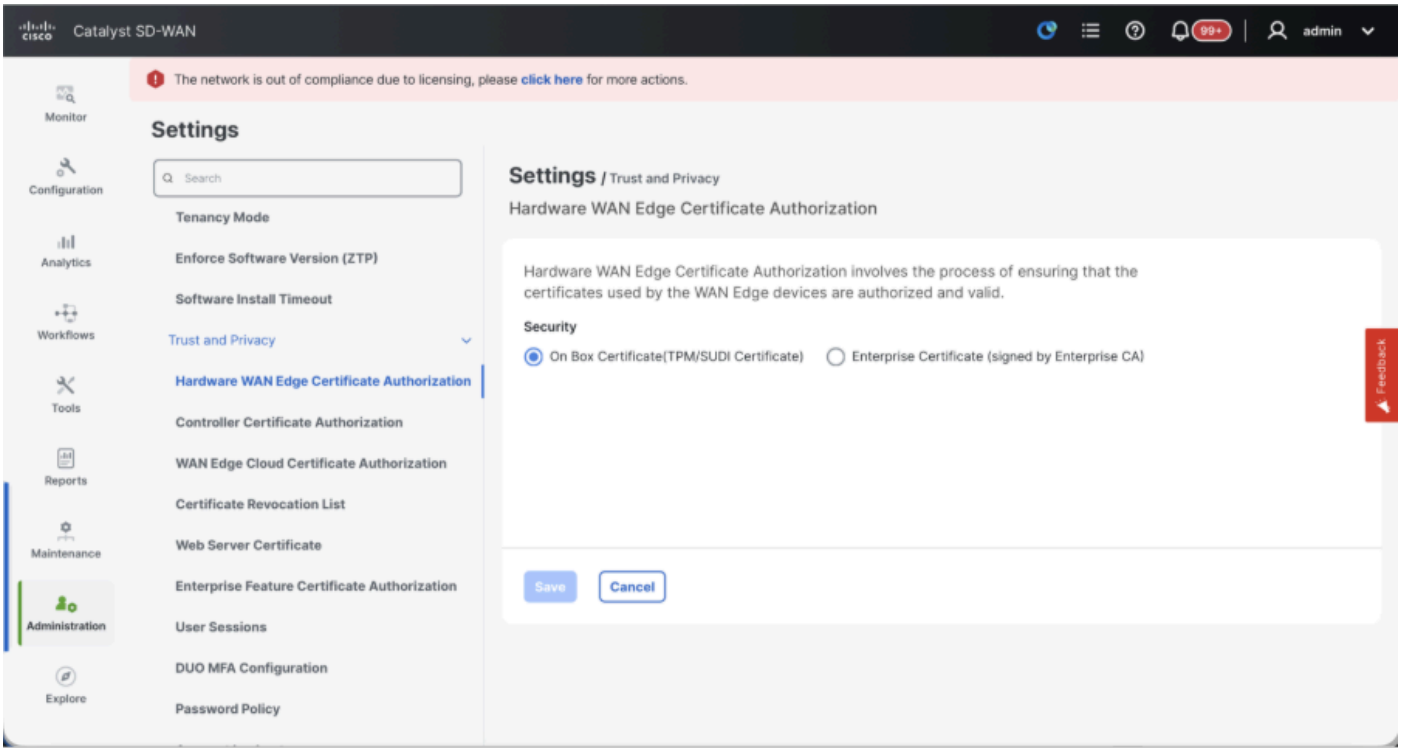
- 一旦将步骤1中的配置添加到所有控制器的CLI中，我们就可以使用浏览器中的URL https://<vmanage-ip>访问vManage的WebUI。使用各个vManage节点的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 导航到管理>设置并完成以下步骤。
- 配置组织名称和验证器/vBond URL/IP地址。配置与vManage节点的CLI中相同的值。
- 在vManage 20.15/20.18中，这些配置在System部分下提供。





- 验证证书授权(CA)的配置，CA决定用于证书签名的证书颁发机构。我们可以看到3个选项：

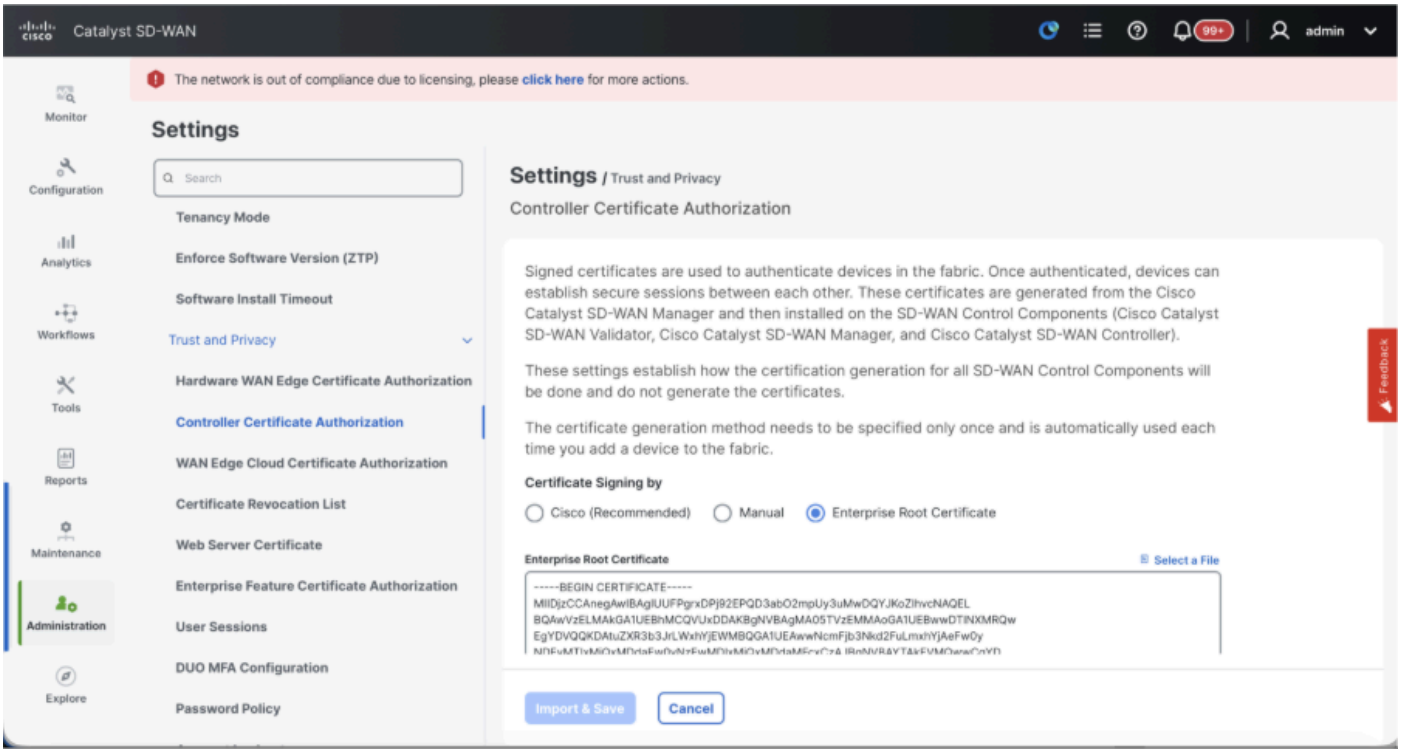
1. 硬件WAN边缘证书授权 — 确定硬件SD-WAN边缘路由器的CA。
    - 开箱证书（TPM/SUDI证书）— 使用此选项，路由器硬件上预安装的证书用于建立控制连接（TLS/DTLS连接）
    - 企业证书（由企业CA签署）— 使用此选项时，路由器使用由组织的企业证书颁发机构签署的证书。选择此选项时，必须在此处更新企业CA的根证书。



2. 控制器证书授权 — 决定SD-WAN控制器的CA。
    - 思科（推荐）— 控制器使用思科PKI签名的证书。vManage使用vManage上配置的智能

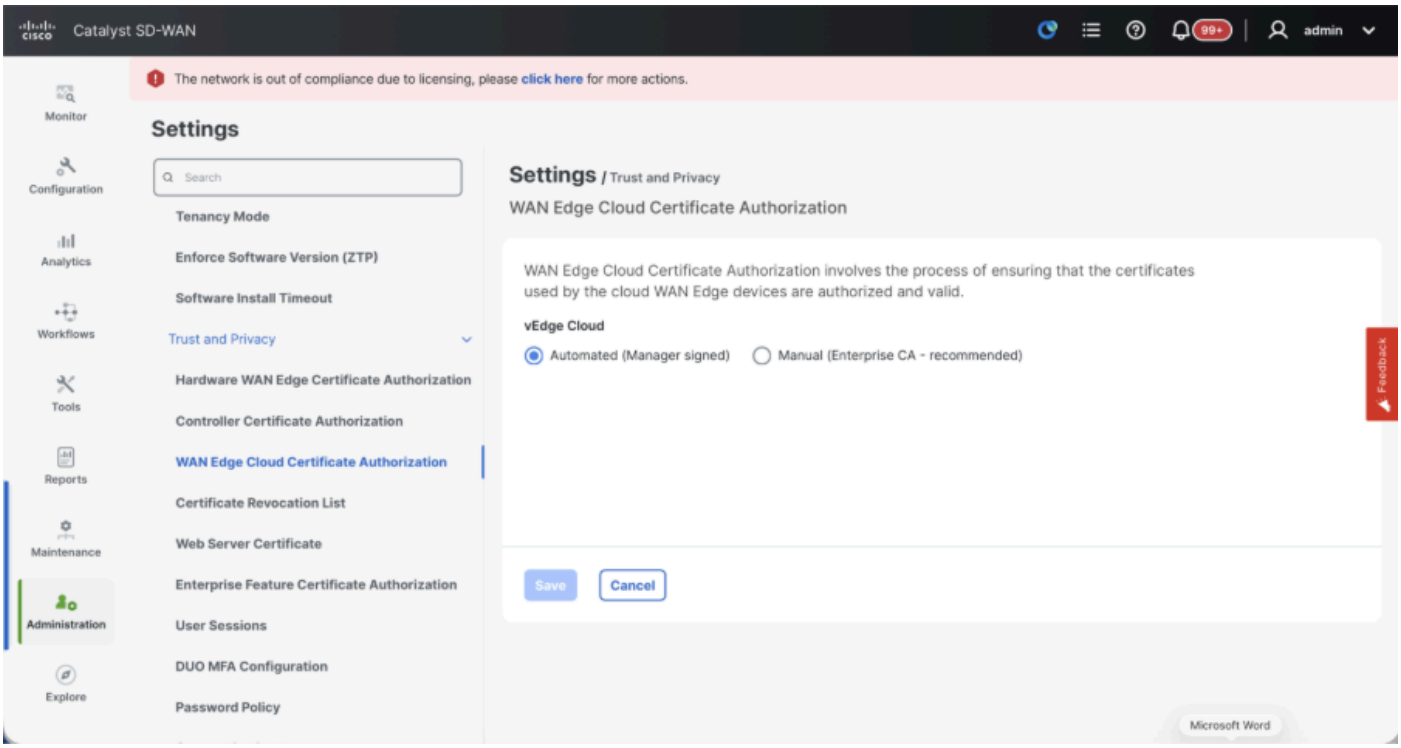
帐户凭证自动联系PNP门户，并获取证书签名并安装在控制器上。

- 手动 — 控制器使用由Cisco PKI签名的证书。使用思科PNP门户手动签署CSR，方法是导航到相应SD-WAN重叠的智能帐户和虚拟帐户。
- 企业根证书 — 通过此选项，路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

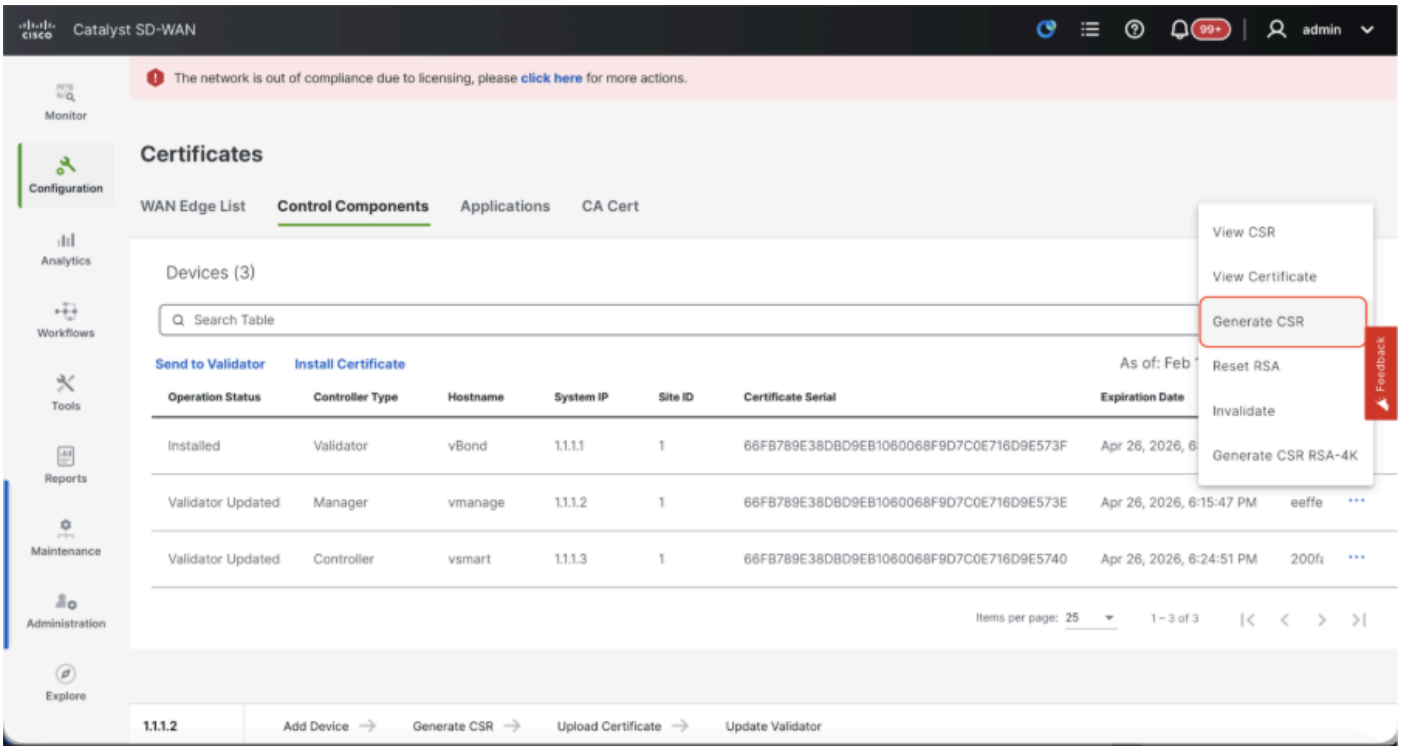


3. 广域网边缘云证书授权 — 确定虚拟SD — 广域网边缘路由器（CSR1000v、C8000v、vEdge云）的CA
    - 自动（vManage签名） — vManage自动为虚拟边缘路由器签署CSR并在路由器上安装证书。
    - 手动（企业CA — 推荐） — 虚拟路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

例如，如果我们使用自己的CA（企业证书颁发机构），请选择Enterprise。



- 如果是20.15/20.18 vManage节点，请导航到配置>证书>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers
- 为Manager/vManage点击……，然后点击Generate CSR。



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

将vBond/Validator和vSmart/Controller注册到vManage

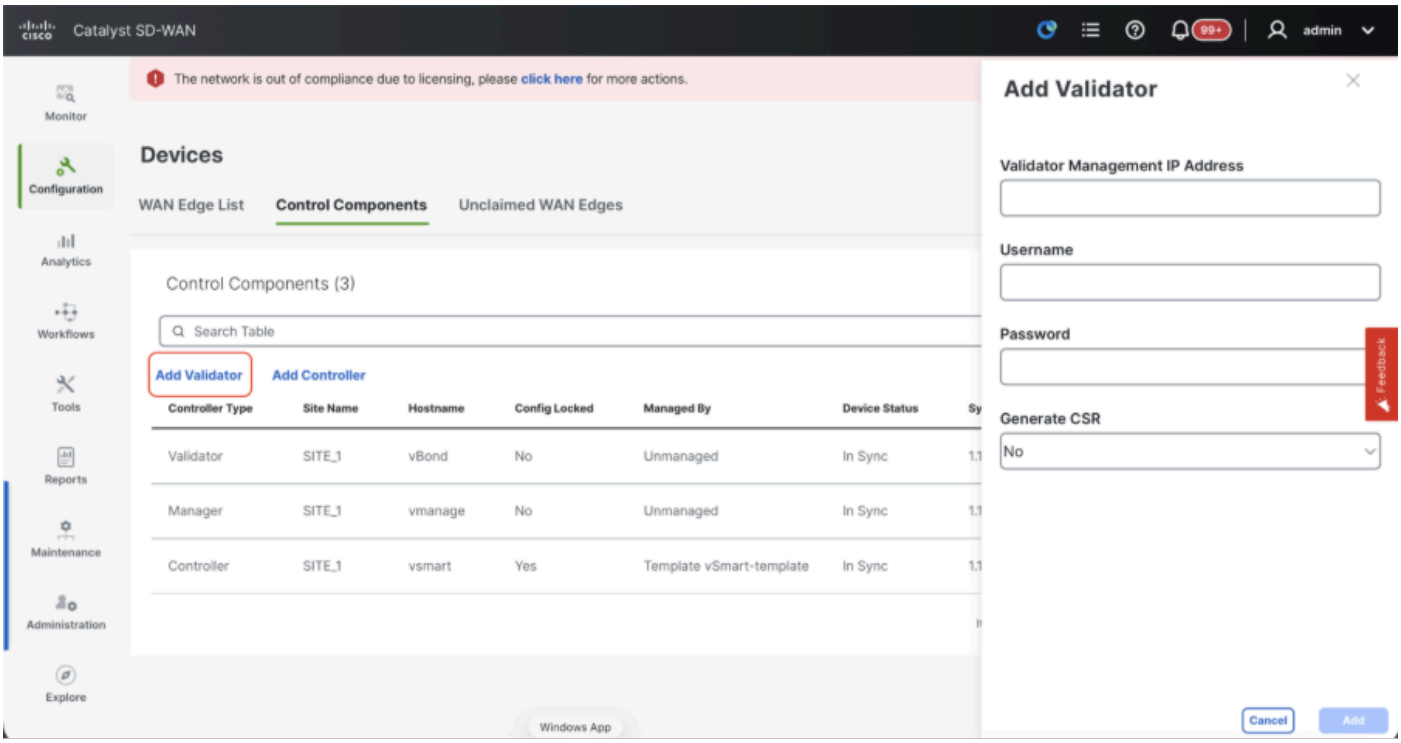
如果是20.15/20.18 vManage节点，请导航到配置>设备>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers

OnboardingvBond/验证器

- 单击AddvBond对于20.12vManageor的情况添加验证程序20.15/20.18vManage。系统打开一个弹出窗口，输入 vBond的VPN 0传输IP，可从vManage访问。
- 如果允许，请从vManagetovBondIP的CLI使用ping检查可接通性。
- 输入vBond的用户凭证。

注意：我们需要将vBondor的管理凭据用作netadmingroup的用户部分。您可以在vBond的CLI中验证这一点。如果我们需要为vBond安装新证书，请在“生成CSR”的下拉列表中选择是

注意：如果vBond位于NAT设备/防火墙之后，请检查vBond VPN 0接口IP是否已转换为公共IP。如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口的公用IP地址



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vBond上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户

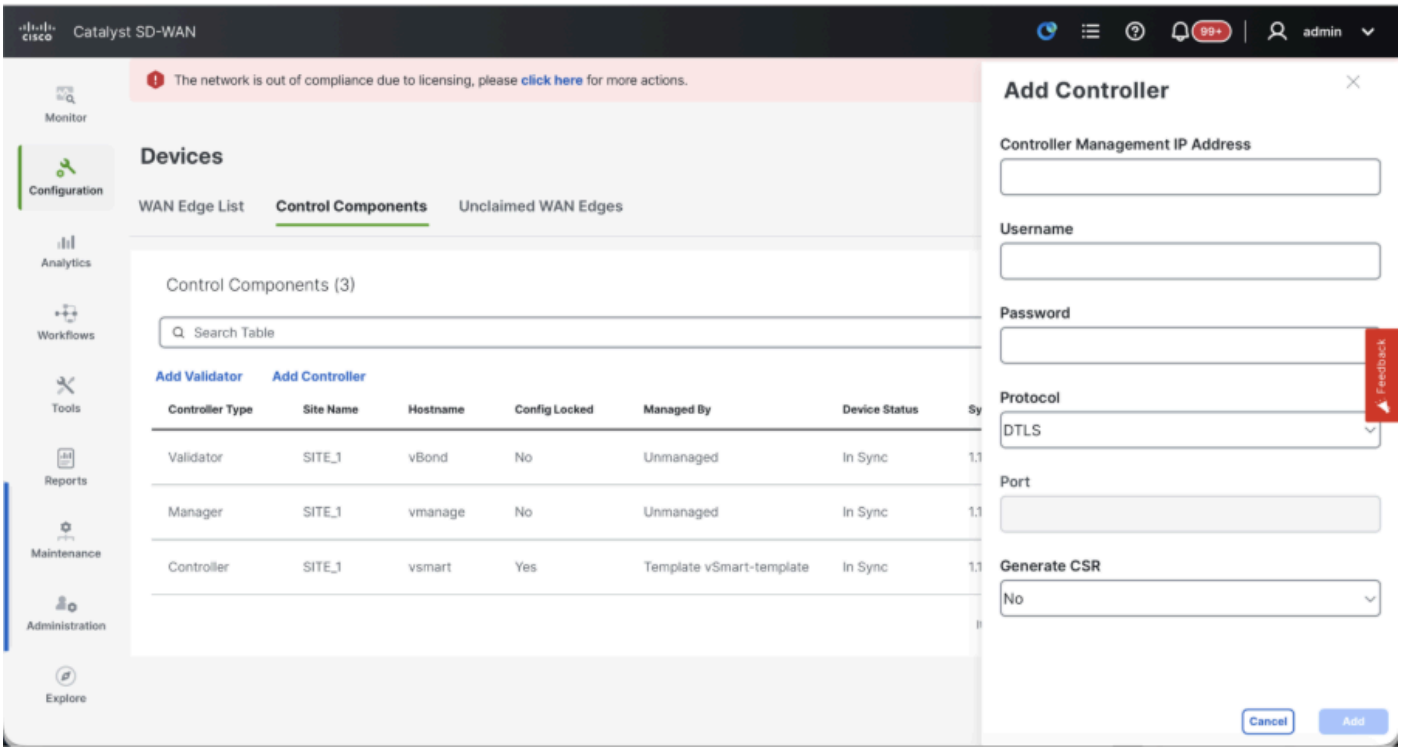
手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

- 如果有多个vBonds，请重复相同的步骤。

自注册vSmart/控制器

- 在20.12 vManage中点击Add vSmart，在20.15/20.18 vManage中点击Add Controller。
- 系统打开一个弹出窗口，输入vSmart的VPN 0传输IP，可从vManage访问。
- 如果允许从vManage的CLI到vSmart IP，请使用ping检查可达性。
- 输入vSmart Note的用户凭据，我们需要使用vSmart的管理员凭据或netadmin组的用户部分。
- 您可以在vSmart的CLI中验证这一点。
- 如果打算对路由器使用TLS来建立与vSmart的控制连接，请将协议设置为TLS。此配置也需要在vSmarts和vManage节点的CLI上进行配置。
- 如果需要为vSmart安装新证书，请在生成CSR"的下拉列表中选择Yes。

注意：如果vSmart位于NAT设备/防火墙之后，请检查vSmart VPN 0接口IP是否已转换为公共IP，如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口IP的公共IP地址。



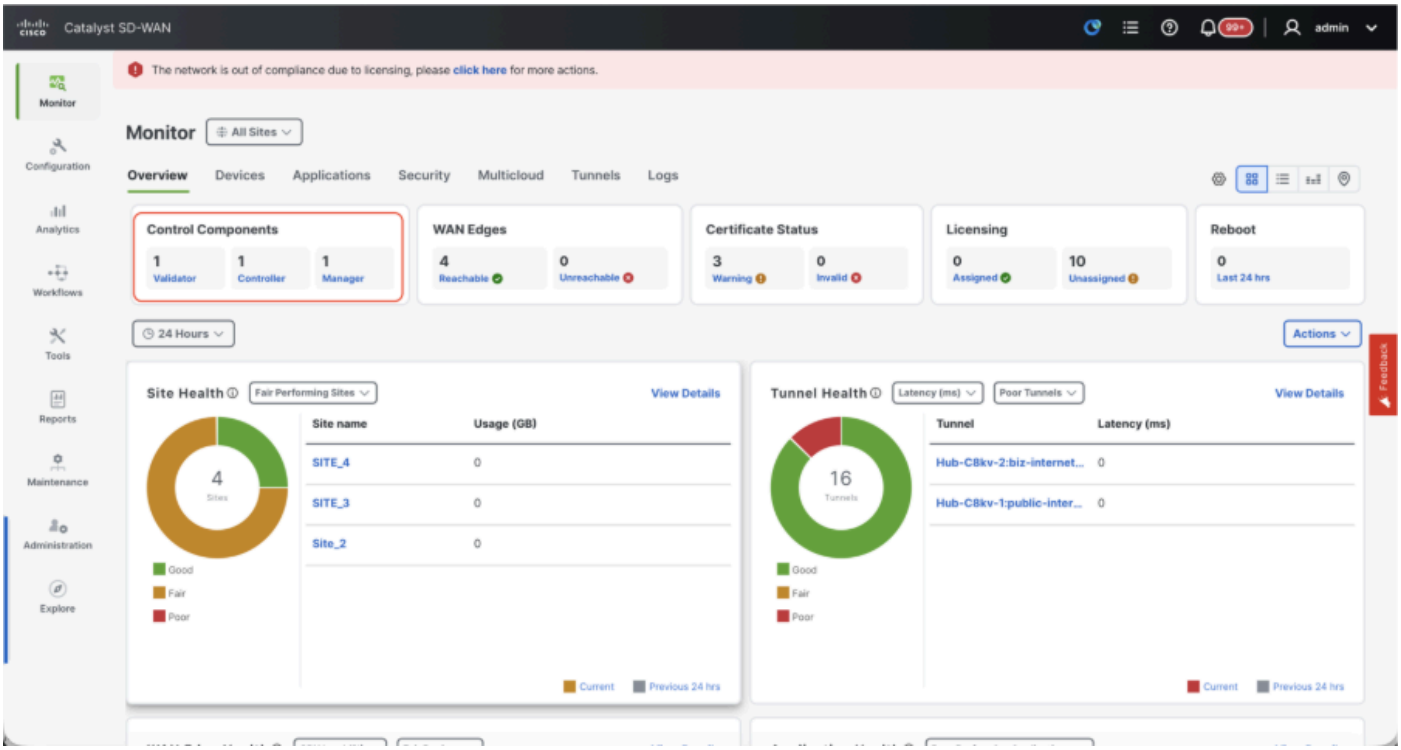
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将

CSR上传到PNP门户，并且证书签名后，会自动将其安装在vSmart上。

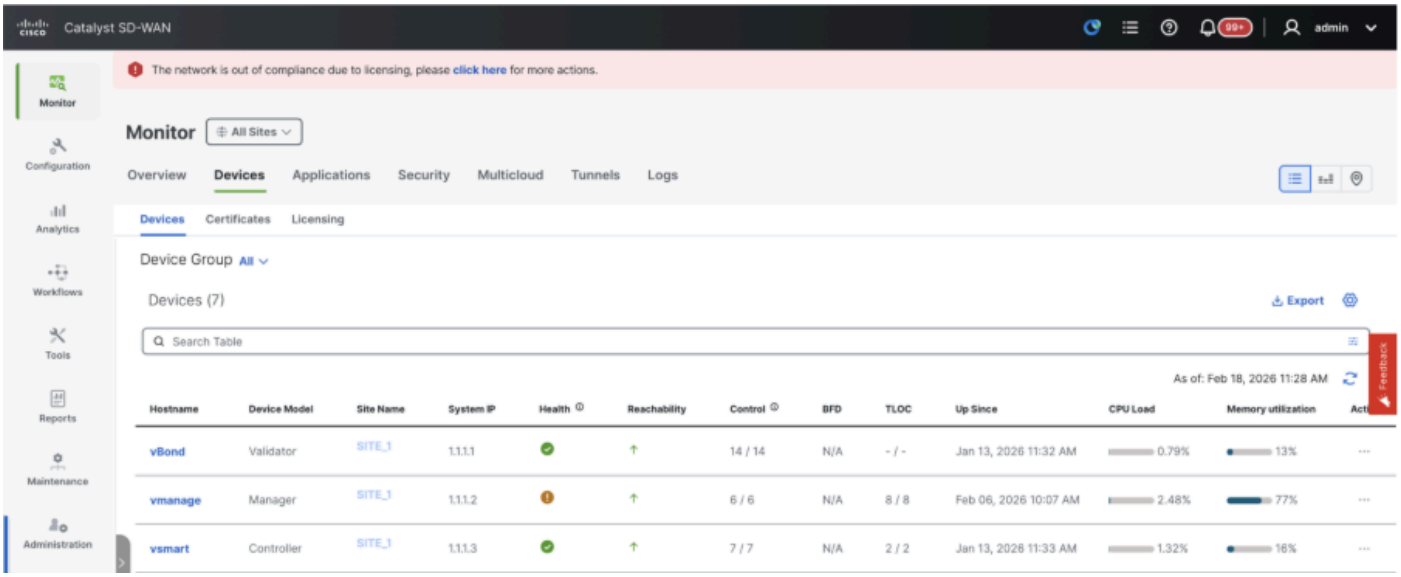
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。如果使用Digicert和企业根证书，则适用相同步骤。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果有多个vSmarts，请重复相同的步骤。

确认

完成所有步骤后，在Monitor>Dashboard中确认所有控制组件均可访问



- 单击相应的控制组件，确认它们都可访问。
- 导航到监控>设备，确认所有控制组件均可访问。



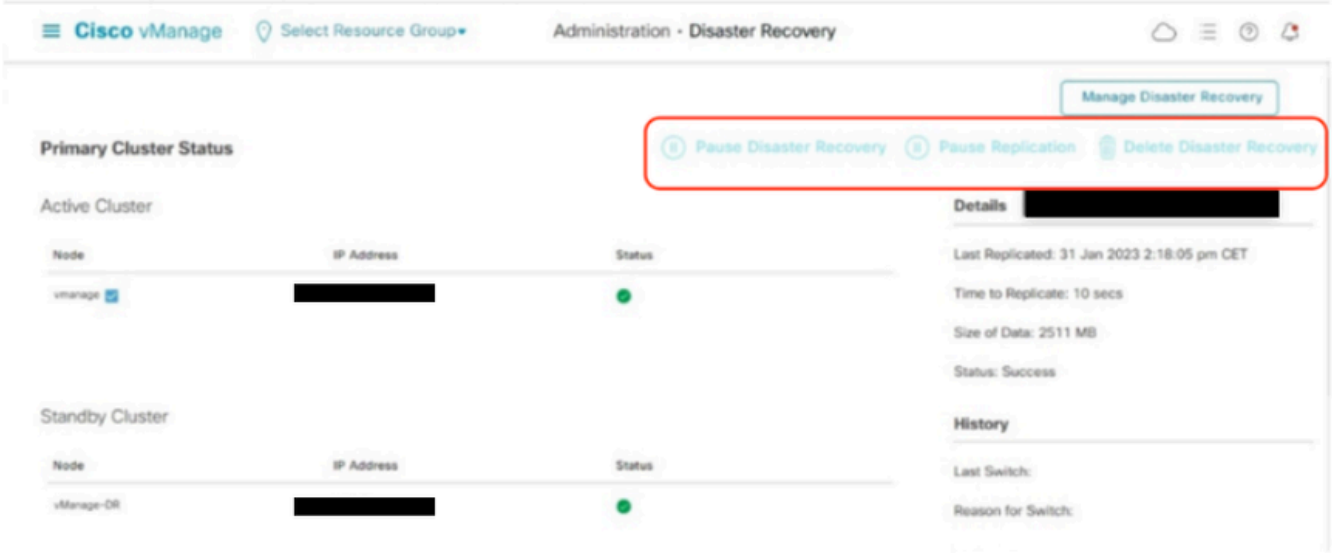
步骤 3：Config-db备份/恢复

在另一个vManage节点上收集vManage configuration-db备份和恢复

注意：从已启用灾难恢复的现有vManage节点收集配置数据库备份时，请确保在该节点的灾难恢复暂停和删除后收集配置数据库备份。

确认没有正在进行的灾难恢复复制。导航到管理>灾难恢复和 确保状态为Success且未处于Import Pending、Export Pending或Download Pending等暂时状态。如果状态未成功，请联系Cisco TAC并确保复制成功，然后继续暂停灾难恢复。

首先暂停灾难恢复并确保任务完成。然后删除灾难恢复并确认任务已完成。



联系思科TAC以确保成功清理灾难恢复。

收集Configuration-DB备份：

- 在当前正在使用的SD-WAN交换矩阵中，您可以在独立vManage和vManage集群设置上生成配置数据库备份。
- 对于独立vManage，该vManage本身是配置数据库领导者。

确认configuration-db正在vManage节点上运行。

您可以使用commandrequest nms configuration-db statusonvManageCLI验证相同配置。输出如下所示

```
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#
```

使用此命令从已确定的configuration-db领导vManage节点收集configuration-db备份。

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

预期输出如下所示：

```
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凭证，请记下该凭证。
- 如果您不知道配置数据库凭证，请联系TAC从现有vManage节点检索配置数据库凭证。
- 默认的configuration-db凭证是用户名：neo4j和密码：密码

将Configuration-db备份恢复到另一个vManage节点

使用SCP将configuration-db备份复制到vManage的/home/admin/目录。

scp命令输出示例：

```
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
```

要恢复configuration-db备份，首先需要配置configuration-db凭据。如果您的配置数据库凭证是默认凭证(neo4j/password)，我们可以跳过此步骤。

要配置configuration-db凭据，请使用命令request nms configuration-db update-admin-user。使用您选择的用户名和密码。

请注意，vManage的应用服务器已重新启动。由于此vManage UI在短时间内变得不可访问。

```
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#
```

发布后，我们可以继续恢复configuration-db备份：

我们可以使用命令request nms configuration-db restore path /home/admin/< >将配置数据库恢复到新的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
```

恢复configuration-db后，请确保vManage UI可访问。等待约5分钟，然后尝试访问UI。

成功登录UI后，请确保边缘路由器列表、模板、策略以及之前或现有vManage UI上存在的所有其余配置都反映在新的vManage UI上。

步骤 4：单节点DR设置

请参阅步骤2:组合2中的预检查：独立式vManage +单节点DR，并确保我们已经完成所有要求，然后继续启用灾难恢复。

单节点DR

先决条件

- 确保在传输VPN(VPN 0)上通过HTTPS可以访问主节点和辅助节点。
- 确保Cisco vManage主节点和辅助节点运行相同的Cisco vManage版本。

VPN 0中的带外集群接口

1. 对于集群中的每个vManage实例，除用于VPN 0（传输）和VPN 512（管理）的接口外，还需要第三个接口（集群链路）。
2. 此接口用于集群内的vManage服务器之间的通信和同步。
3. 此接口必须至少为1 Gbps，并且延迟为4毫秒或更短。建议使用10 Gbps接口。
4. 两个vManage节点必须能够通过此接口相互连接：无论是第2层网段还是通过第3层路由。

- 确保在两个Cisco vManage节点上启用所有服务（应用服务器、配置数据库、消息服务器、协调服务器和统计数据库）。
- 跨主要和辅助数据中心分发所有控制器，包括思科vBond协调器。确保分布在这些数据中心中的Cisco vManage节点可以访问这些控制器。控制器仅连接到主Cisco vManage节点。
- 确保主用（主要）和备用（辅助）Cisco vManage节点中没有其他操作正在进行。例如，确保没有服务器正在升级，或者没有模板正在将模板附加到设备。

- 如果已启用Cisco vManage HTTP/HTTPS代理服务器，请将其禁用。如果不禁用代理服务器，Cisco vManage会尝试通过代理IP地址建立灾难恢复通信，即使Cisco vManage带外集群IP地址可直接访问。您可以在灾难恢复注册完成后重新启用Cisco vManage HTTP/HTTPS代理服务器。

- 在开始灾难恢复注册过程之前，请转至主Cisco vManage节点上的Tools → Rediscover Network窗口，并重新发现Cisco vBond Orchestrator。

配置

配置作为灾难恢复节点的所有vManage节点的CLI配置

vManage的最小配置，如图所示

```
config t
system
 host-name



 system-ip
```

```
 site-id


 organization-name


 vbond


commit
```

注意:如果我们使用URL作为vBond地址，请确保在VPN 0配置中配置DNS服务器IP地址或确保可以解析这些地址。

需要使用这些配置来启用传输接口，该接口用于与路由器和控制器的其余部分建立控制连接

```
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
```

还要配置VPN 512管理接口以启用对控制器的带外管理访问。

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
commit
```

在DR vManage上配置服务接口

在vManage节点上配置服务接口。此接口用于DR通信，

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

确保主vManage和DR vManage上的服务接口使用相同的IP子网

更新vManage UI上的配置

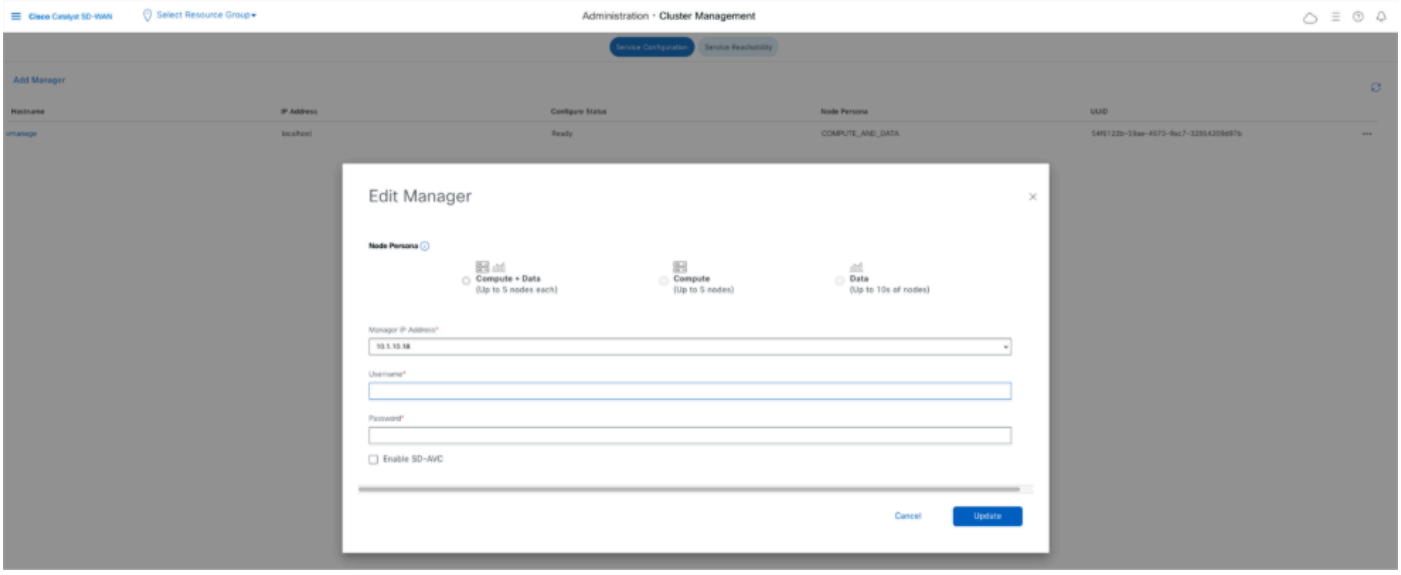
- 在所有控制器的CLI上添加配置后，我们可以使用浏览器中的URL https://<vmanage-ip>访问vManage的WebUI。使用各个vManage节点的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 导航到管理>设置并完成以下步骤。
- 配置组织名称。配置与vManage节点的CLI中相同的值。
- 在vManage 20.15/20.18中，这些配置在System部分下提供。

在DR vManage上安装证书

继续执行Combination 2部分下给出的步骤：独立vManage +单节点DR第3步：配置vManage UI、证书和板载控制器，以在灾难恢复vManage上安装证书。

添加灾难恢复配置

- 为此，请转至主vManage。
- 点击vManage条目右侧的三个点并包含用户名和密码后，导航到Administration → Cluster Management并指示带外接口的IP地址。建议为此配置创建一个单独的本地用户，例如，主要和DR vmanage上的dradmin。



- VManage在此更改后重新启动。
- 在Primary vManage启动后，导航到Administration → Disaster Recovery。点击“管理灾难恢复”。
- 在弹出窗口中，填写主要和辅助vManage的详细信息。
- 要指示的IP地址是带外集群接口(eth2)的IP地址。
- 凭证必须是netadmin用户(dradmin)的凭证，并且配置DR后不得更改这些凭证。可以使用单独的用于灾难恢复的vManage本地用户凭据。我们需要确保vManage本地用户是netadmin组的一部分。此处可使用管理员凭据。

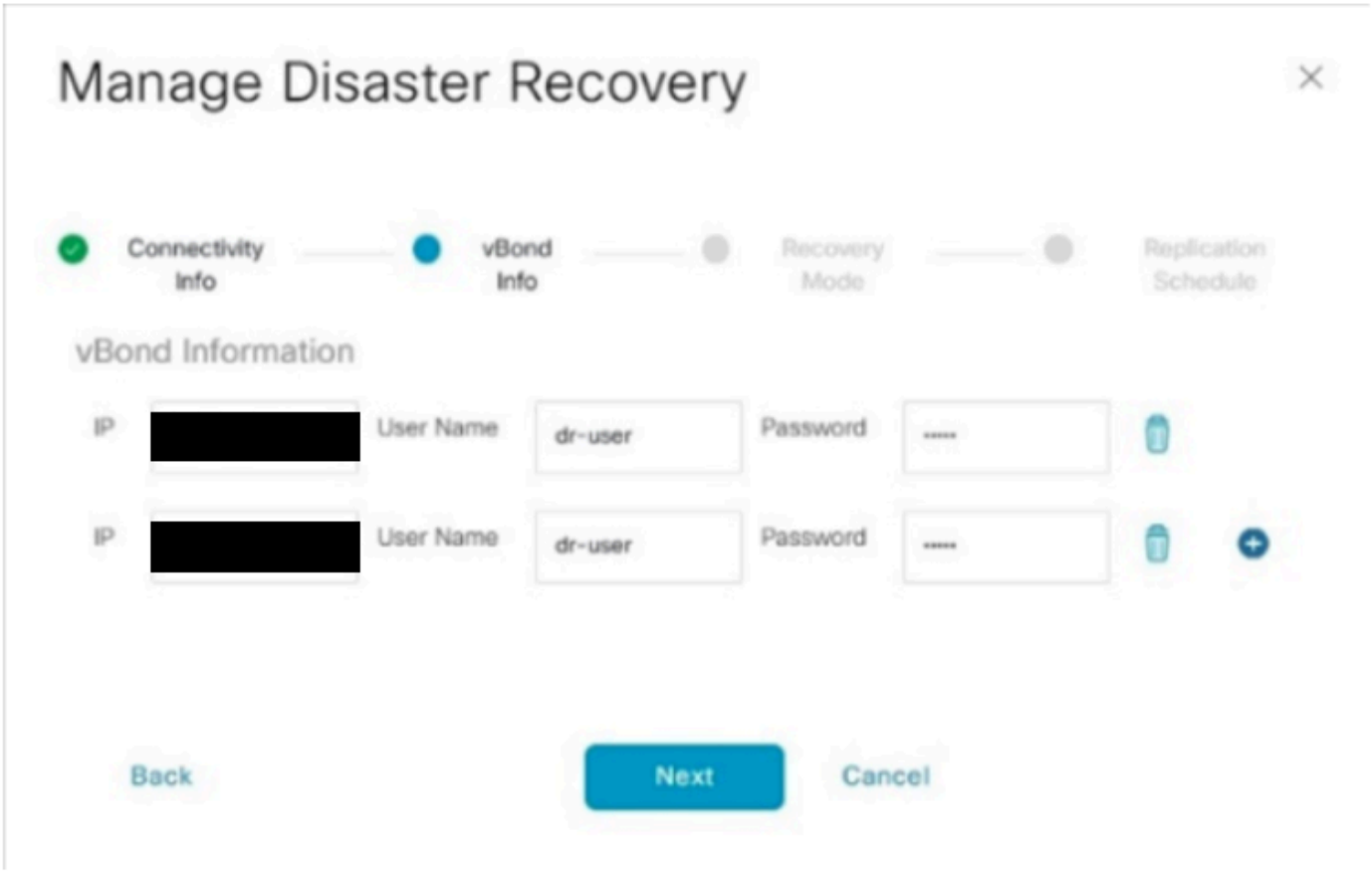
- 填写完毕后，单击“下一步”。

- 填写vBond控制器详细信息。

- vBond控制器必须在指定的IP地址中通过Netconf到达。

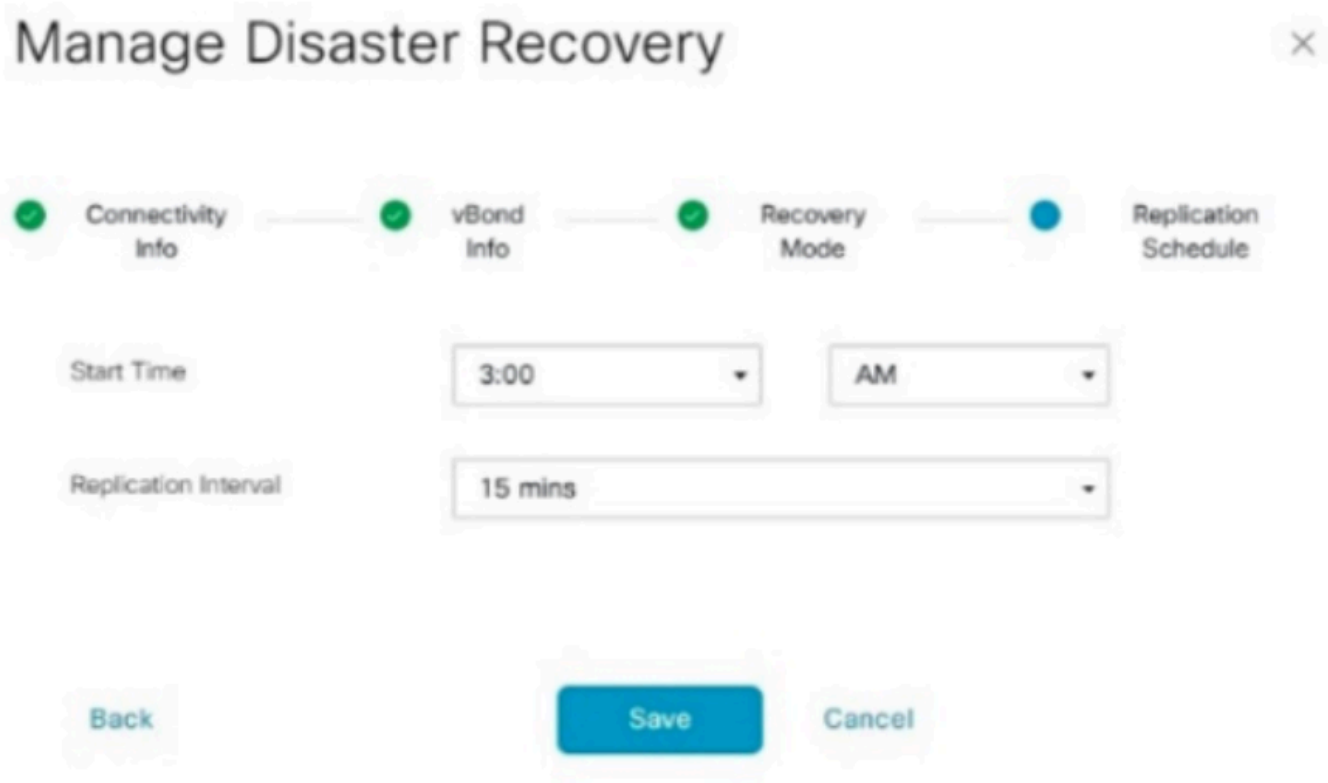
- 凭证必须是netadmin用户(dradmin)的凭证，并且配置DR后不得更改这些凭证。

- 为此，建议vBond在本地配置此dadmin用户，或者您可以使用管理员用户添加vBond。

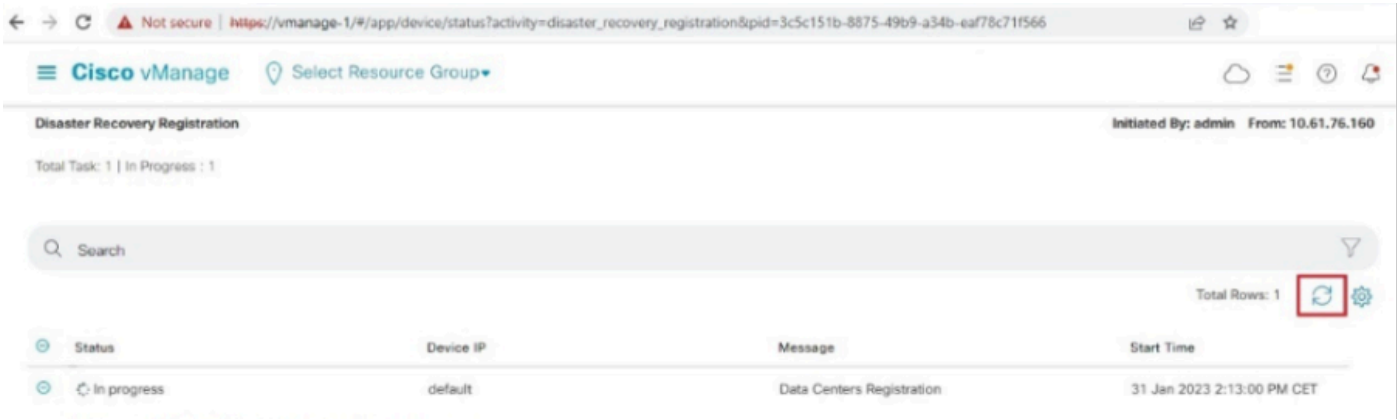


- 填写完毕后，单击“下一步”。
- 在恢复模式下，选择“手动”。单击“下一步”。

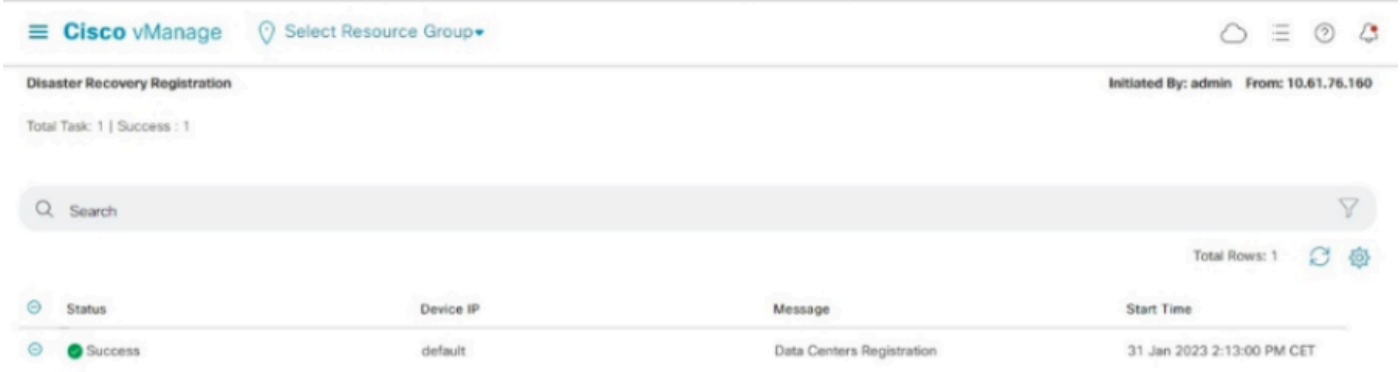
在复制计划中，设置“复制间隔”'.每次复制间隔时间，都会从主复制数据 vManageto辅助vManage。最小可配置值为15分钟。



- 设置值，然后单击“Save”。
- DR注册现在开始。点击refresh按钮手动刷新状态和进度日志。此过程可能需要20-30分钟。

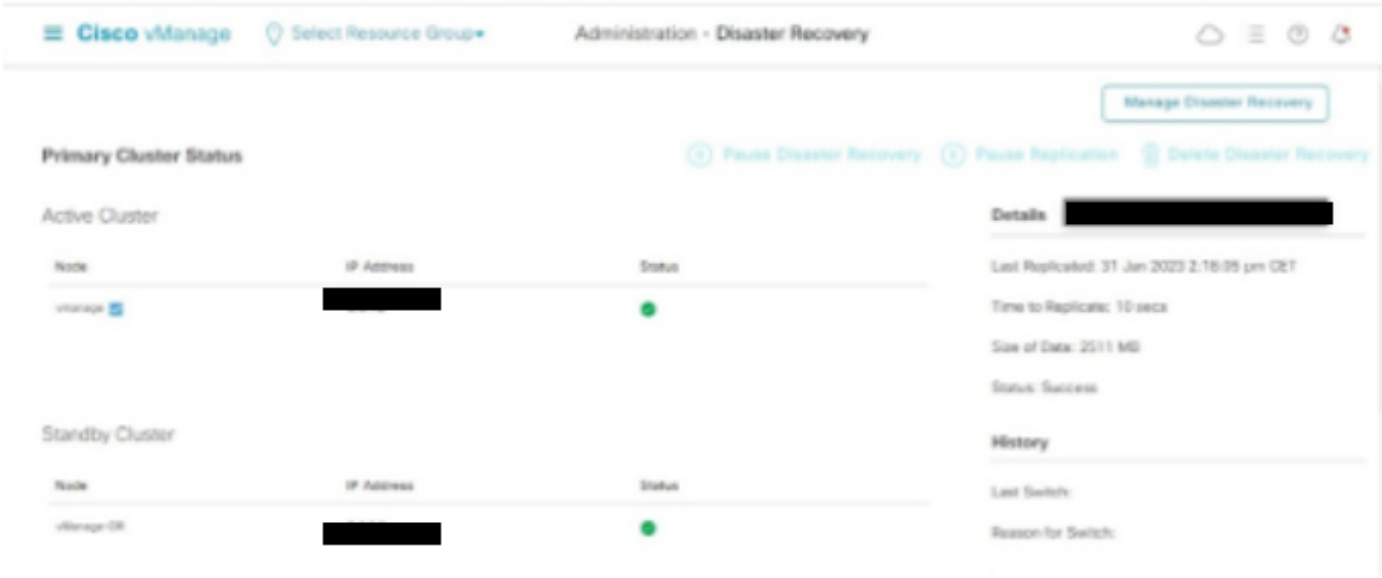


- 请注意，vManage GUI在此过程中重新启动。
- 完成后，必须看到Success状态。



验证

导航到管理→灾难恢复查看灾难恢复状态以及上次复制数据的时间。



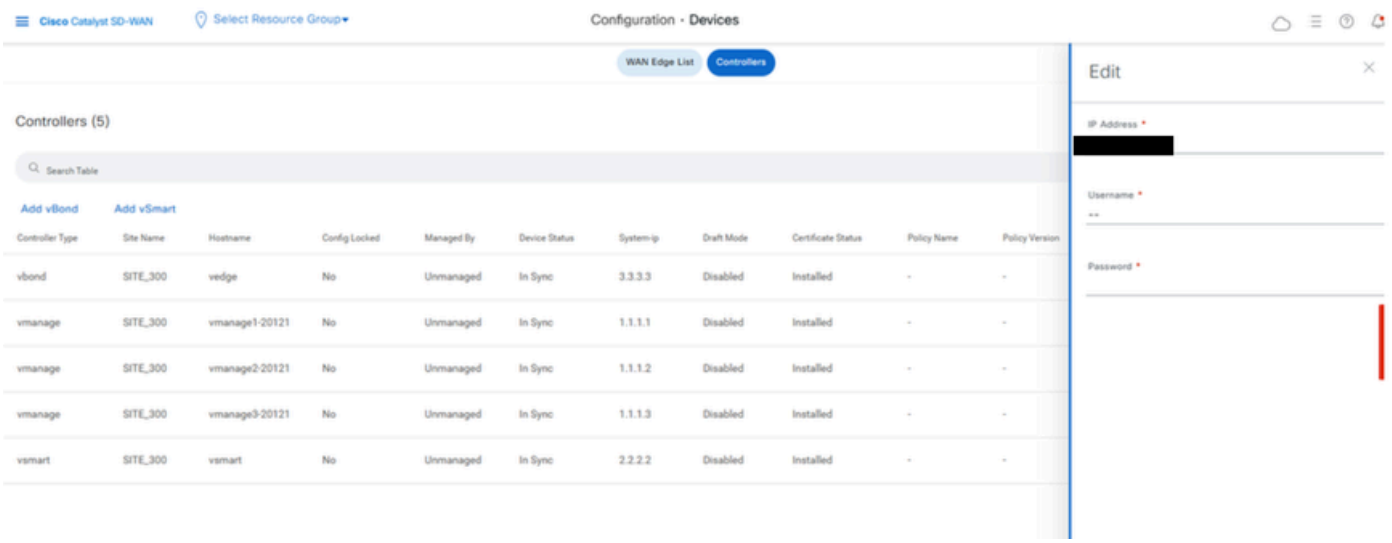
步骤 5：控制器重新验证和旧控制器失效

恢复configuration-db后，我们需要重新验证交换矩阵中的所有新控制器(vmanage/vsmart/vbond)

注：在实际生产中，如果用于重新身份验证的接口IP是隧道接口IP，则需要确保在vManage、vSmart和vBond的隧道接口以及路径沿途的防火墙上允许NETCONF服务。要打开的防火墙端口是从DR群集到所有vBonds和vSmarts的双向规则的TCP端口830。

在vmanage UI上，点击Configuration > Devices > Controllers

- 点击每个控制器附近的三个点，然后点击Edit



- 将ip-address（控制器的系统ip）替换为transport vpn 0（隧道接口）ip地址。输入用户名和密码，然后点击save
- 对交换矩阵中的所有新控制器执行相同操作

同步根证书链

所有控制器入网后，请完成以下步骤：

在新活动集群中的任何Cisco SD-WAN Manager服务器上，执行以下操作：

输入以下命令将根证书与新活动集群中的所有Cisco Catalyst SD-WAN设备同步：

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

输入以下命令将Cisco SD-WAN Manager UUID与Cisco SD-WAN Validator同步：

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

一旦交换矩阵恢复，并且交换矩阵中的所有边缘和控制器的控制和bfd会话都已启动，我们就需要从UI使旧控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，点击Configuration > Devices > Certificates
- 点击“控制器”
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击invalidate（失效）
- 点击send to vbond
- 在vmanage UI上，点击Configuration > Devices > Controllers
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击Delete

步骤 6：过帐检查

注意：继续此处所示的“后检查”部分，它适用于所有部署组合。

组合3:vManage Cluster +无DR

所需实例：

- 3个vManage（3节点集群，所有COMPUTE_AND_DATA）或6个vManage（3个COMPUTE_AND_DATA + 3个数据）
- 1个或多个vBond
- 1个或多个vSmart

步骤:

1. 使用通用步骤启动所有实例
2. 预检查
3. 配置vManage UI、证书和板载控制器

4. 构建vManage集群
5. Config-db备份/恢复
6. 过帐检查

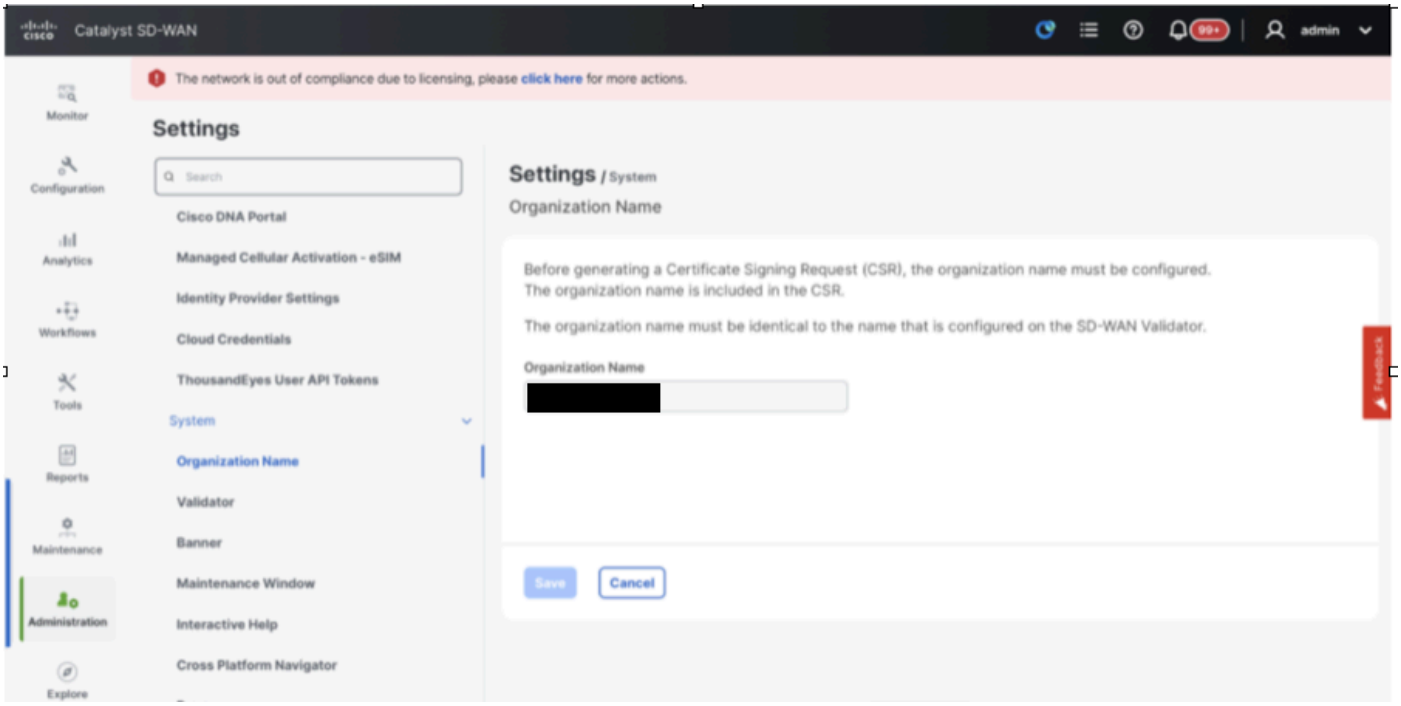
步骤 1：预检查

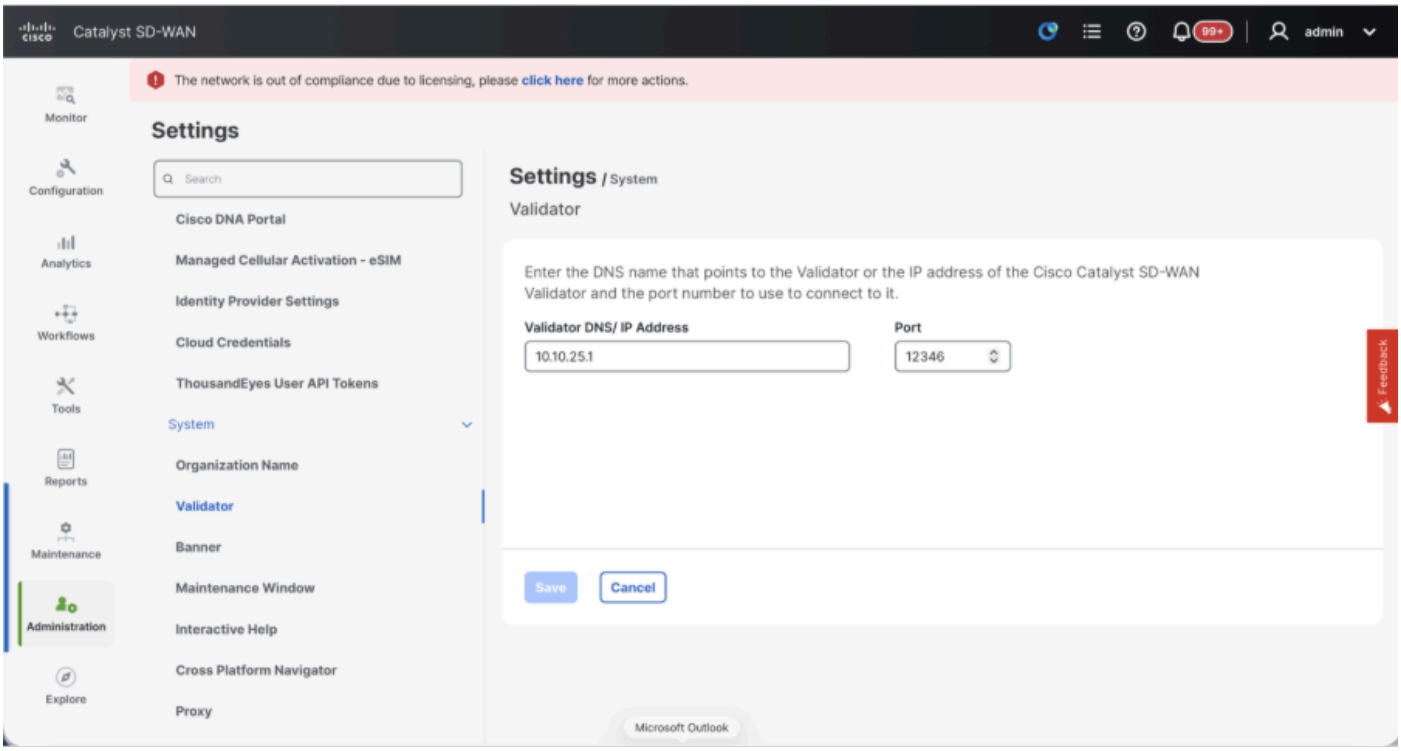
- 确保活动的Cisco SD-WAN Manager实例数与新安装的Cisco SD-WAN Manager实例数相同。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例都运行相同的软件版本。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例能够到达Cisco SD-WAN Validator的管理IP地址。
- 确保证书已安装在新安装的Cisco SD-WAN Manager实例上。
- 确保所有Cisco Catalyst SD-WAN设备(包括新安装的Cisco SD-WAN Manager)上的时钟都同步。
- 确保在新安装的Cisco SD-WAN Manager实例上配置一组新的系统IP和站点ID，同时配置与活动集群相同的基本配置。

步骤 2：配置vManage UI、证书和板载控制器

更新vManage UI上的配置

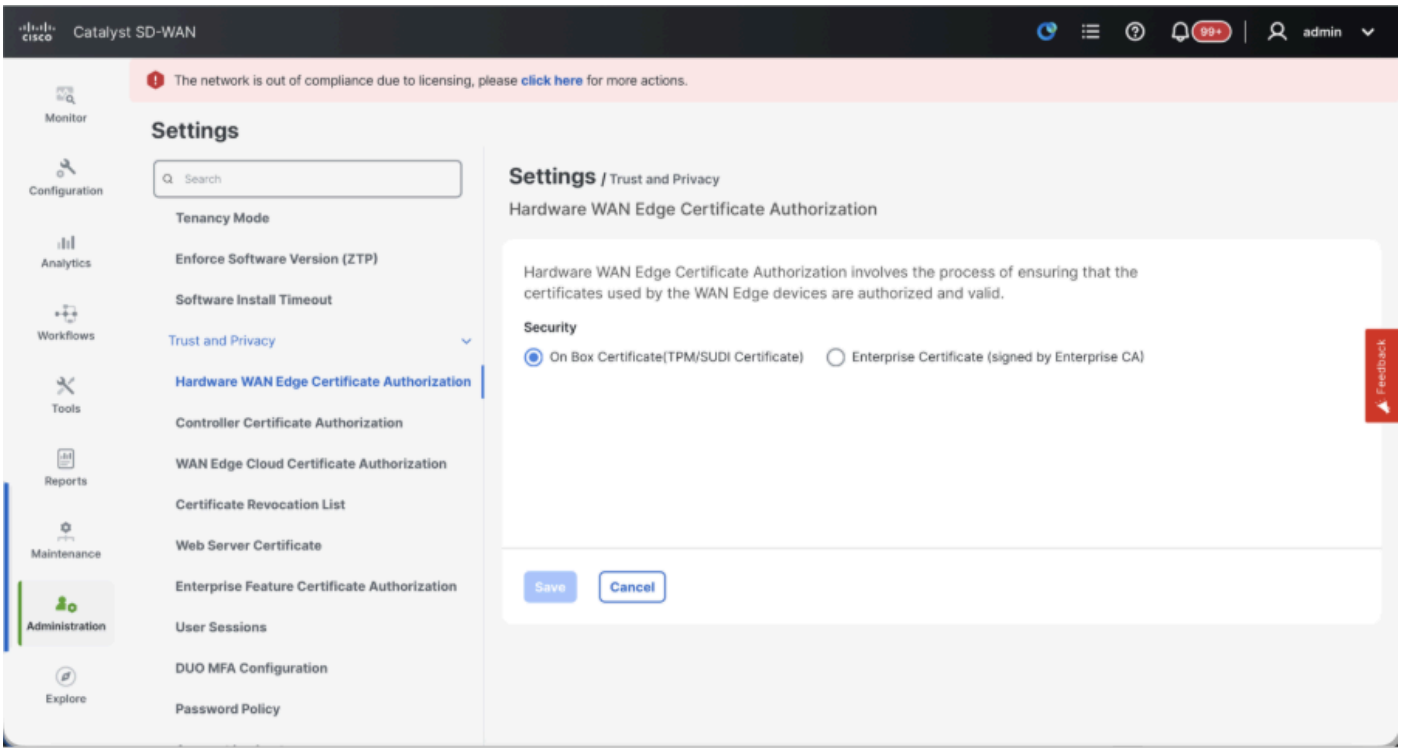
- 一旦将步骤1中的配置添加到所有控制器的CLI中，我们就可以使用浏览器中的URL https://<vmanage-ip>访问vManage的WebUI。使用各个vManage节点的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 导航到管理>设置并完成以下步骤。
- 配置组织名称和验证器/vBond URL/IP地址。配置与vManage节点的CLI中相同的值。
- 在vManage 20.15/20.18中，这些配置在System部分下提供。



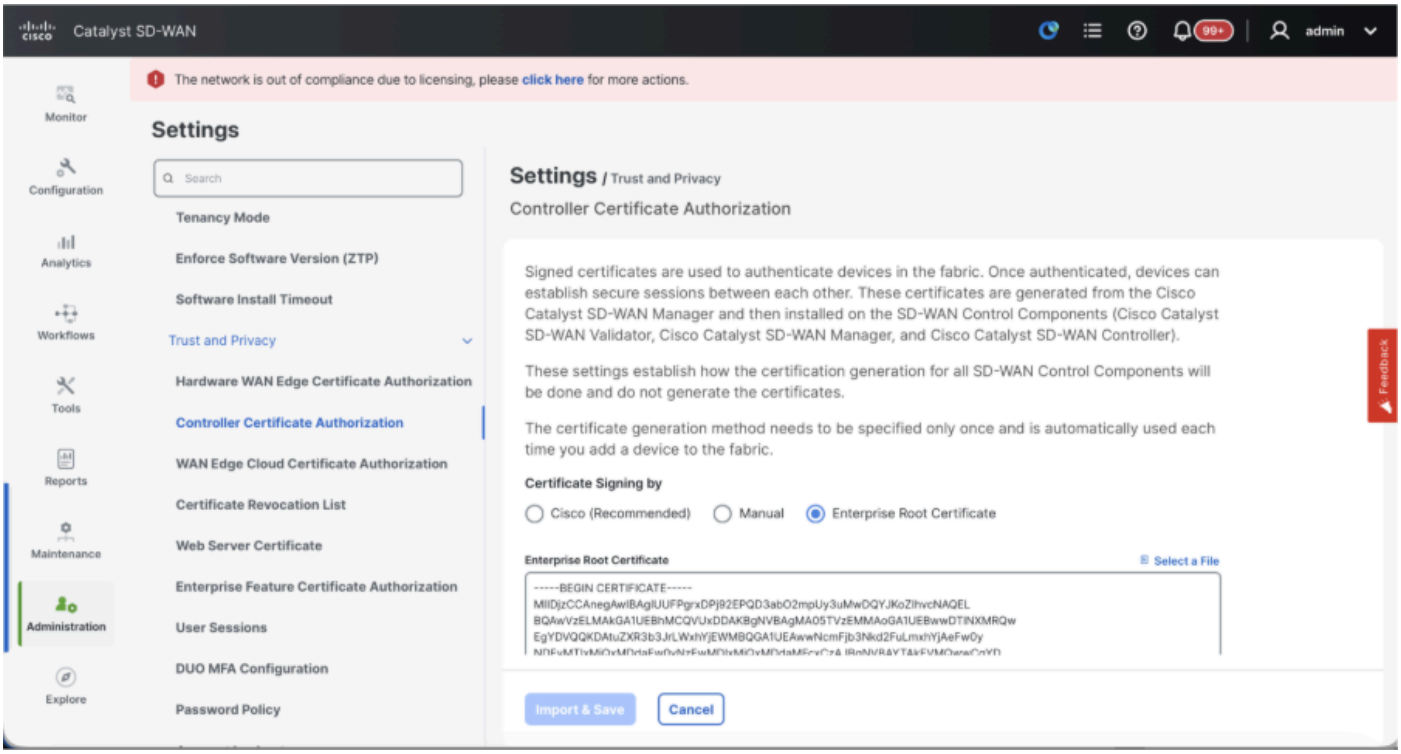


- 验证证书授权(CA)的配置，CA决定用于证书签名的证书颁发机构。我们可以看到3个选项：

1. 硬件WAN边缘证书授权 — 确定硬件SD-WAN边缘路由器的CA。
    - 开箱证书（TPM/SUDI证书）— 使用此选项，路由器硬件上预安装的证书用于建立控制连接（TLS/DTLS连接）
    - 企业证书（由企业CA签署）— 使用此选项时，路由器使用由组织的企业证书颁发机构签署的证书。选择此选项时，必须在此处更新企业CA的根证书。



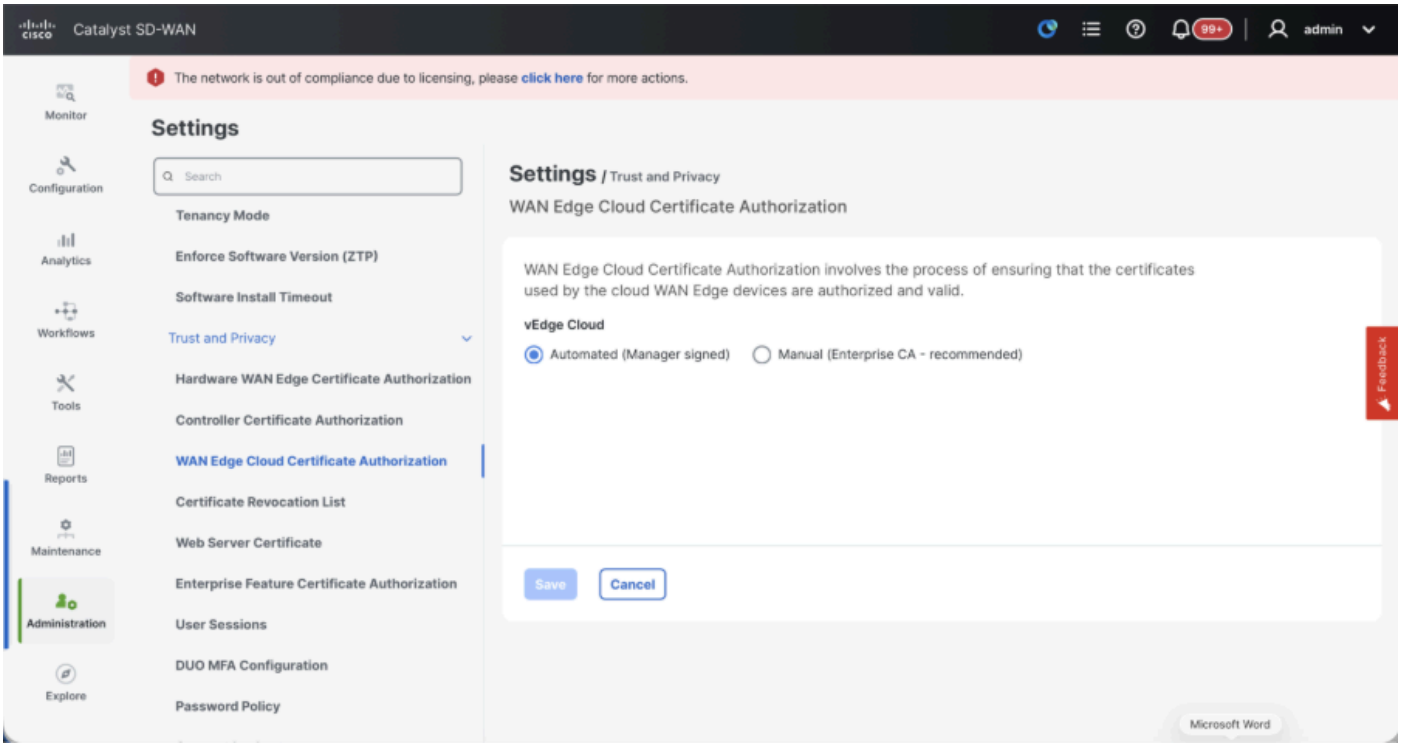
2. 控制器证书授权 — 决定SD-WAN控制器的CA。
   - 思科（推荐） — 控制器使用思科PKI签名的证书。vManage使用vManage上配置的智能帐户凭证自动联系PNP门户，并获取证书签名并安装在控制器上。
   - 手动 — 控制器使用由Cisco PKI签名的证书。使用思科PNP门户手动签署CSR，方法是导航到相应SD-WAN重叠的智能帐户和虚拟帐户。
   - 企业根证书 — 通过此选项，路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。



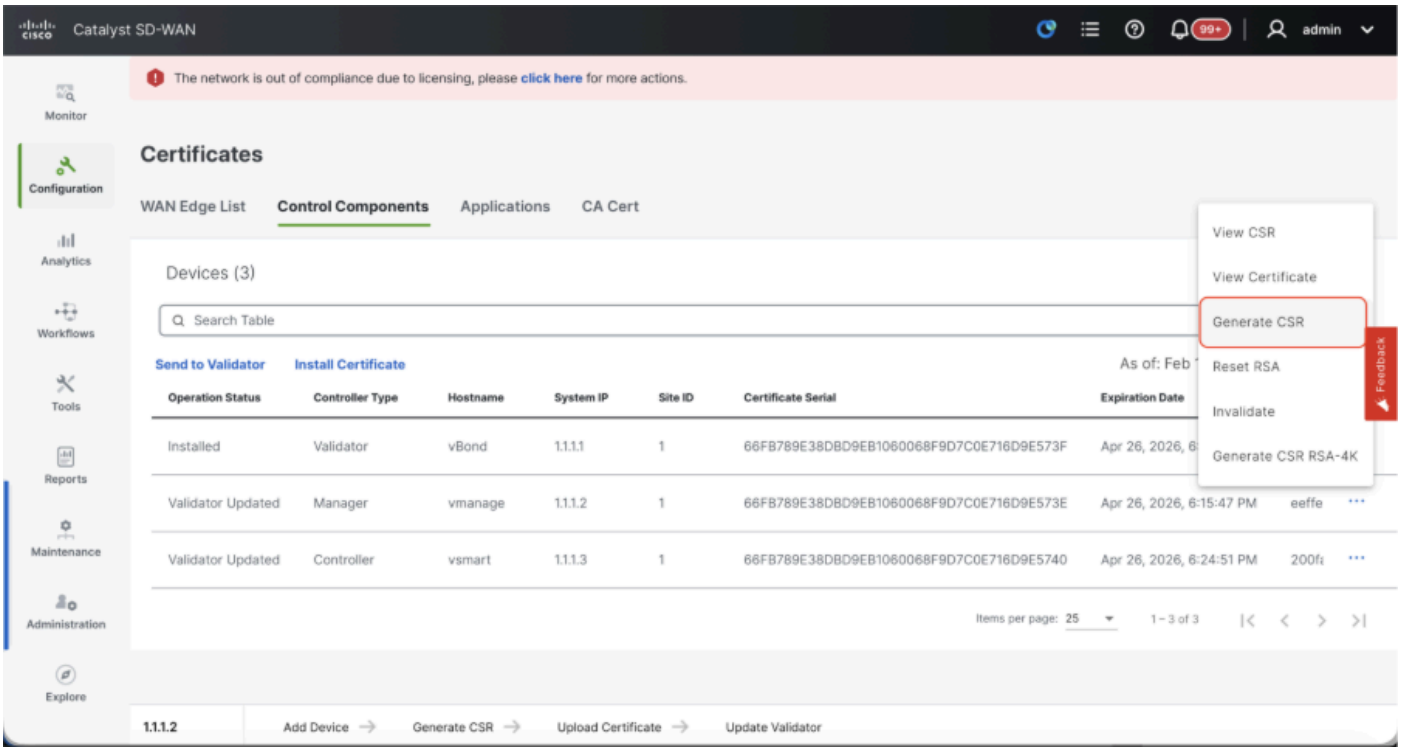
3. 广域网边缘云证书授权 — 确定虚拟SD — 广域网边缘路由器（CSR1000v、C8000v、vEdge云）的CA

- 自动（vManage签名）— vManage自动为虚拟边缘路由器签署CSR并在路由器上安装证书。
- 手动（企业CA — 推荐）— 虚拟路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

例如，如果我们使用自己的CA（企业证书颁发机构），请选择Enterprise。



- 如果是20.15/20.18 vManage节点，请导航到配置>证书>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers
- 为Manager/vManage点击……，然后点击Generate CSR。



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

将vBond/Validator和vSmart/Controller注册到vManage

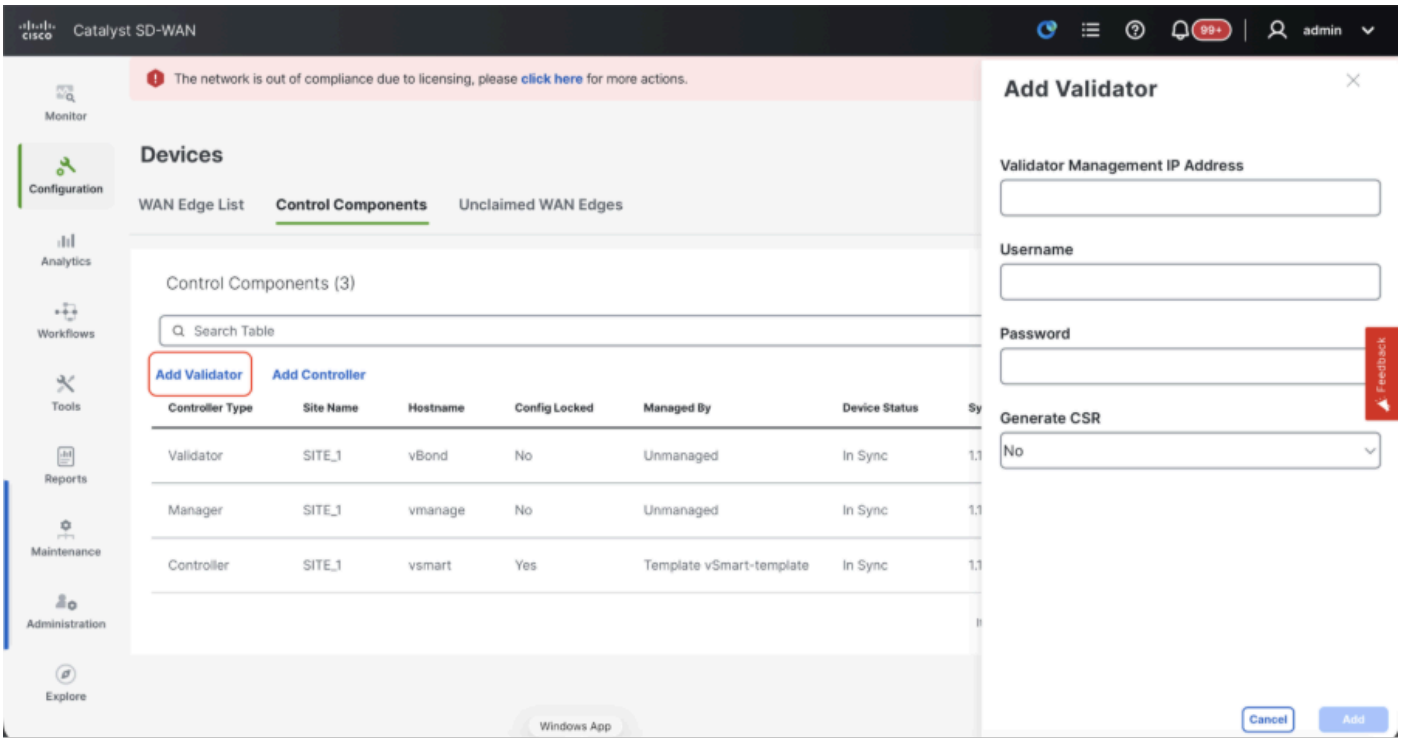
如果是20.15/20.18 vManage节点，请导航到配置>设备>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers

OnboardingvBond/验证器

- 单击AddvBond对于20.12vManageor的情况添加验证程序20.15/20.18vManage。系统打开一个弹出窗口，输入 vBond的VPN 0传输IP，可从vManage访问。
- 如果允许，请从vManagetovBondIP的CLI使用ping检查可接通性。
- 输入vBond的用户凭证。

注意：我们需要将vBondor的管理凭据用作netadmingroup的用户部分。您可以在vBond的CLI中验证这一点。如果我们需要为vBond安装新证书，请在“生成CSR”的下拉列表中选择是

注意：如果vBond位于NAT设备/防火墙之后，请检查vBond VPN 0接口IP是否已转换为公共IP。如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口的公用IP地址

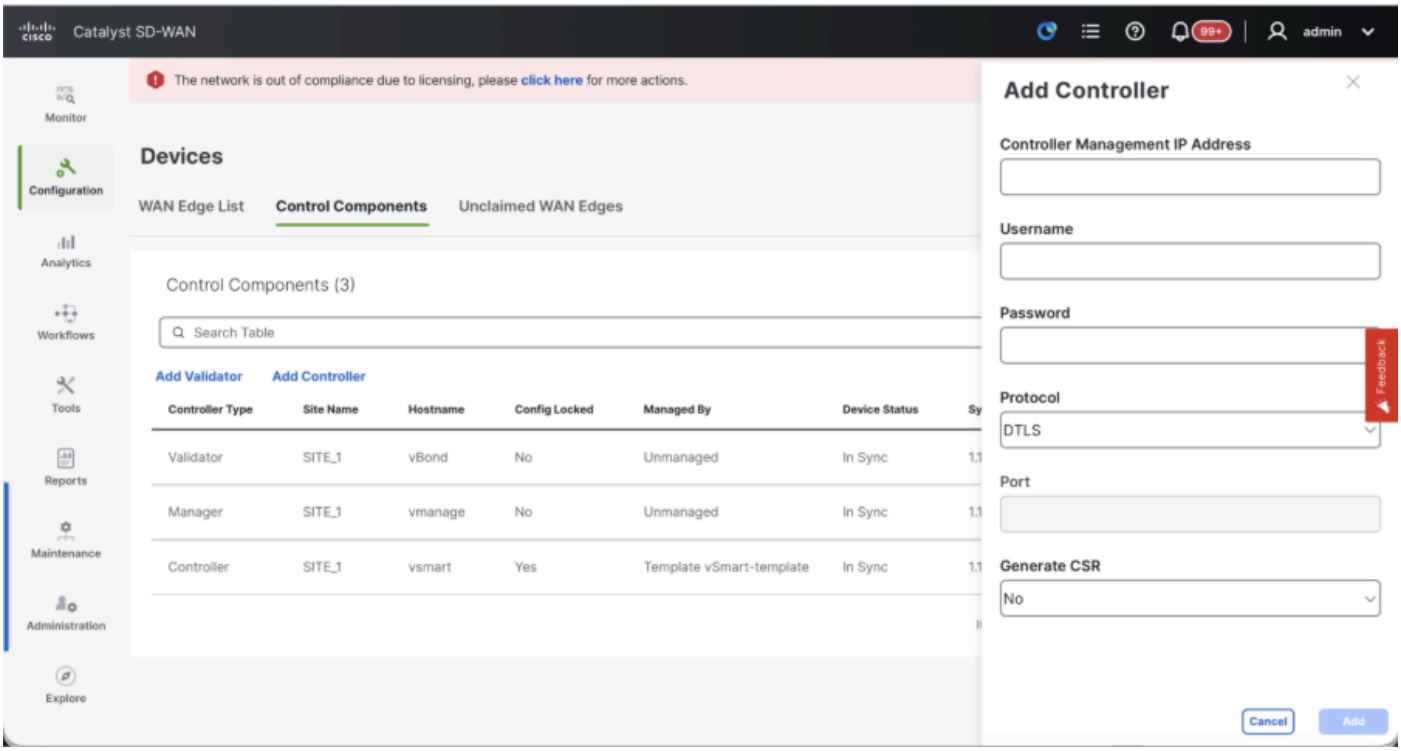


- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vBond上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 如果有多个vBonds，请重复相同的步骤。

自注册vSmart/控制器

- 在20.12 vManage中点击Add vSmart，在20.15/20.18 vManage中点击Add Controller。
- 系统打开一个弹出窗口，输入vSmart的VPN 0传输IP，可从vManage访问。
- 如果允许从vManage的CLI到vSmart IP，请使用ping检查可达性。
- 输入vSmart Note的用户凭据，我们需要使用vSmart的管理员凭据或netadmin组的用户部分。
- 您可以在vSmart的CLI中验证这一点。
- 如果打算对路由器使用TLS来建立与vSmart的控制连接，请将协议设置为TLS。此配置也需要在vSmarts和vManage节点的CLI上进行配置。
- 如果需要为vSmart安装新证书，请在生成CSR"的下拉列表中选择Yes。

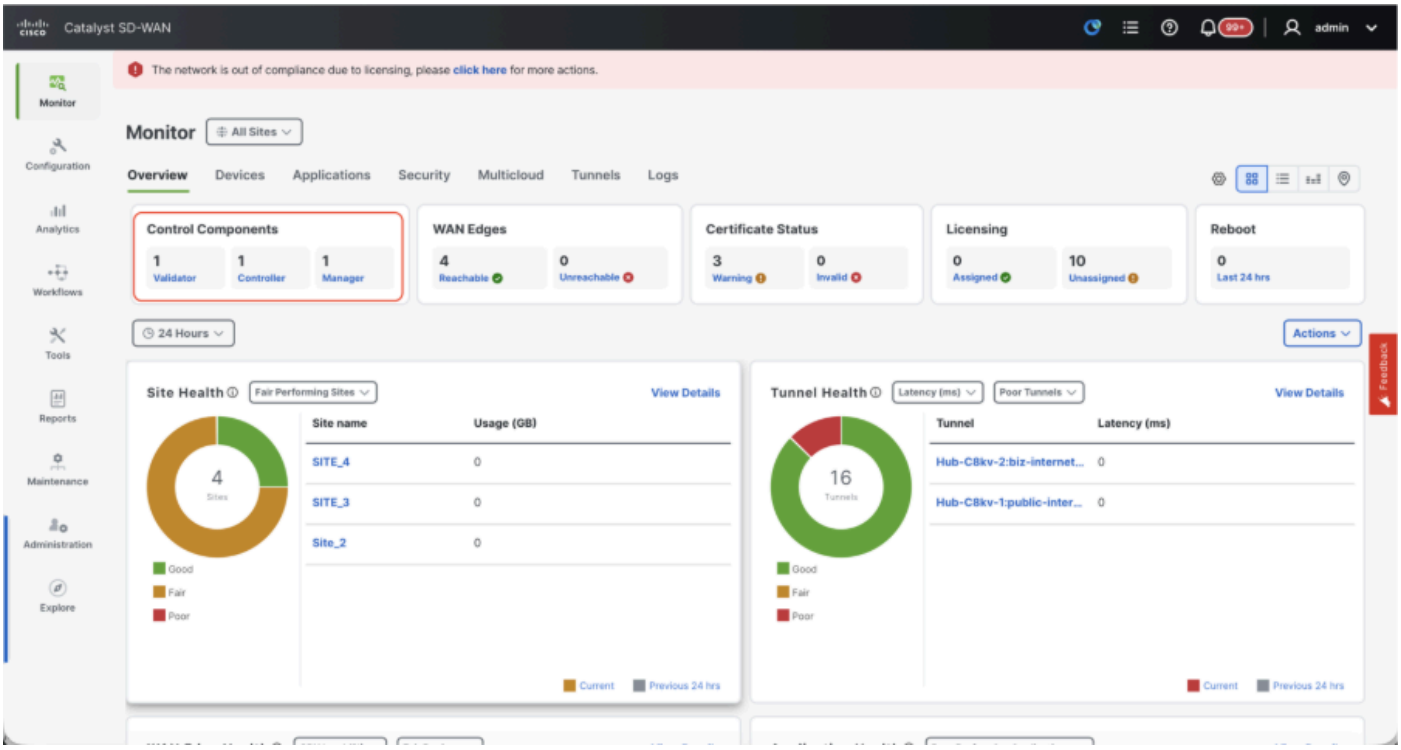
注意：如果vSmart位于NAT设备/防火墙之后，请检查vSmart VPN 0接口IP是否已转换为公共IP，如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口IP的公共IP地址。



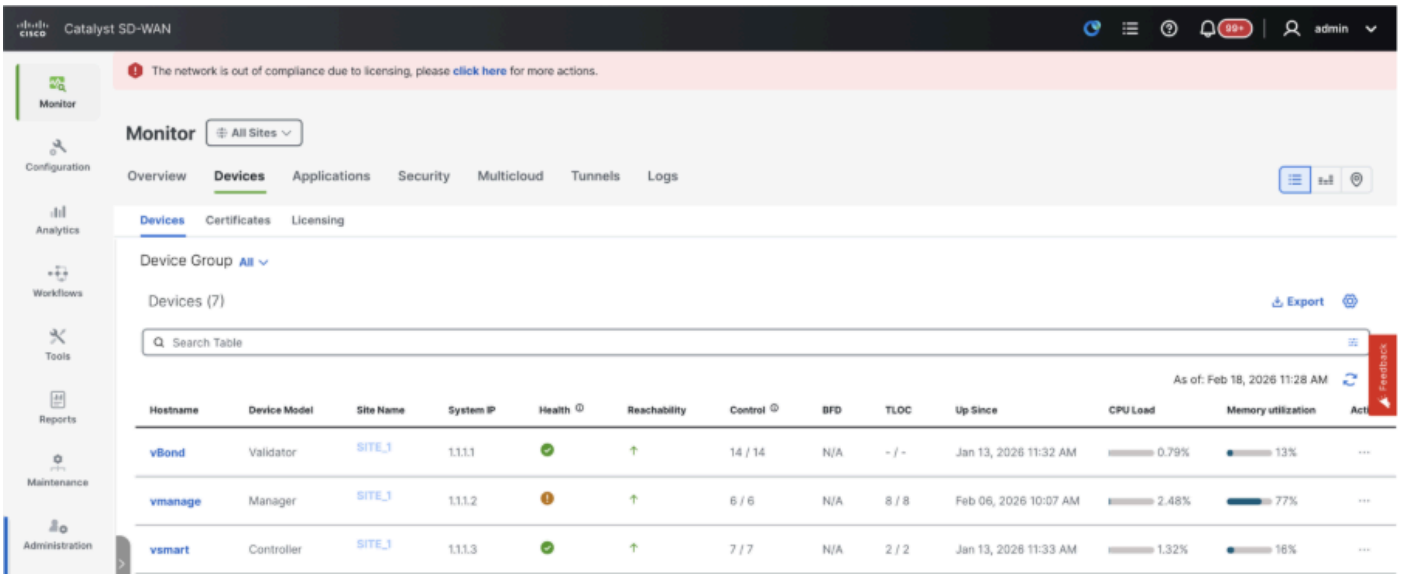
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装在vSmart上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 如果有多个vSmarts，请重复相同的步骤。

确认

完成所有步骤后，在Monitor>Dashboard中确认所有控制组件均可访问



- 单击相应的控制组件，确认它们都可访问。
- 导航到监控>设备，确认所有控制组件均可访问。



步骤 3：构建vManage集群

板载SD-WAN交换矩阵，在SD-WAN重叠中带有vManage集群

注意:vManage集群可以配置3个vManage节点或6个vManage节点，具体取决于注册到SD-WAN交换矩阵的站点数量。请参考现有的vManage集群，并根据该集群选择节点数。

配置属于集群的所有vManage节点的CLI配置

在所有vManage节点上配置系统配置

- 配置vManage节点的其余节点。对于3个节点集群，您有剩余的2个要配置的节点；对于6个节点集群，您有5个要配置的节点。
- 配置系统配置，如下所示：

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注意:如果我们使用URL作为vBond地址，请确保在VPN 0配置中配置DNS服务器IP地址或确保可以解析这些地址。

在所有vManage节点上配置传输接口

需要使用这些配置来启用传输接口，该接口用于与路由器和其余控制器建立控制连接。

```
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节点上配置管理接口

还要配置VPN 512管理接口以启用对控制器的带外管理访问。

```
Conf t
```

```
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

可选配置：

- 您可以参考现有控制器的配置，如果此处列出的配置存在，您可以将此配置添加到新控制器。
- 仅当路由器需要使用TLS与vManage节点建立安全控制连接时，才将控制协议配置为TLS。默认情况下，所有控制器和路由器都使用DTLS建立控制连接。根据您的要求，此配置是仅在vSmart和vManage节点上必需的可选配置。

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

在所有vManage节点上配置服务接口

在所有vManagenode(包括已注册的vManage-1)上配置服务接口。此接口用于集群通信，即集群中vManagenodes之间的通信。

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

确保同一IP子网用于vManagecluster中所有节点上的服务接口。

配置集群凭证

我们可以使用与vManagenode相同的管理凭据配置vManagecluster。否则，我们可以配置作为netadmingroup一部分的新用户凭据。配置新用户凭据的配置如下所示

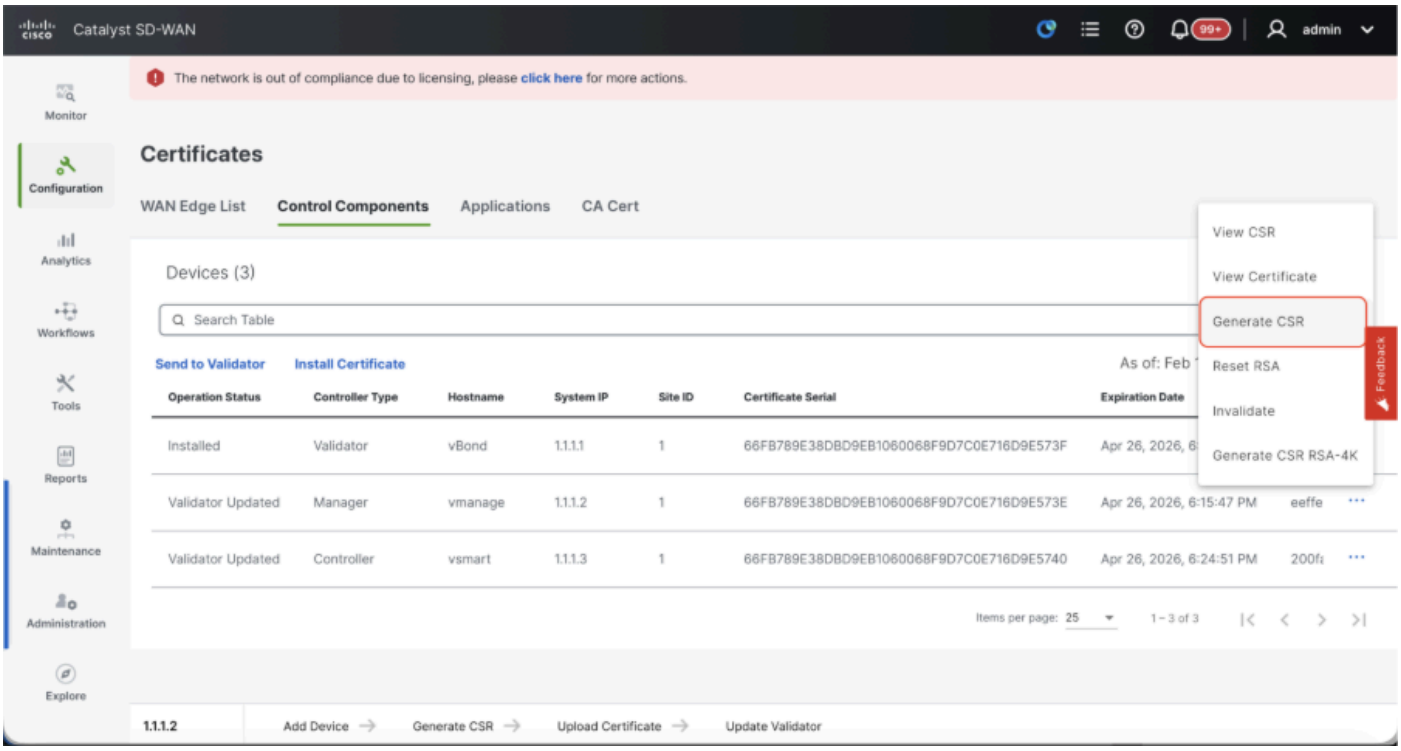
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

确保在属于群集的所有vManagenode上配置相同的用户凭据。如果我们决定使用管理员凭据，则必须在所有vManagenode上配置相同的用户名/密码。

在所有vManage节点上安装设备证书

- 使用浏览器中的URL https://<vmanage-ip>登录所有vManagenode的tovManageUI。使用各个vManagenode的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 如果是20.15/20.18 vManage节点，请导航到Configuration > Certificates > Control Components 。对于20.9/20.12版本，Configuration > Devices > Controllers

  单击Manager/vManage的……并单击Generate CSR。



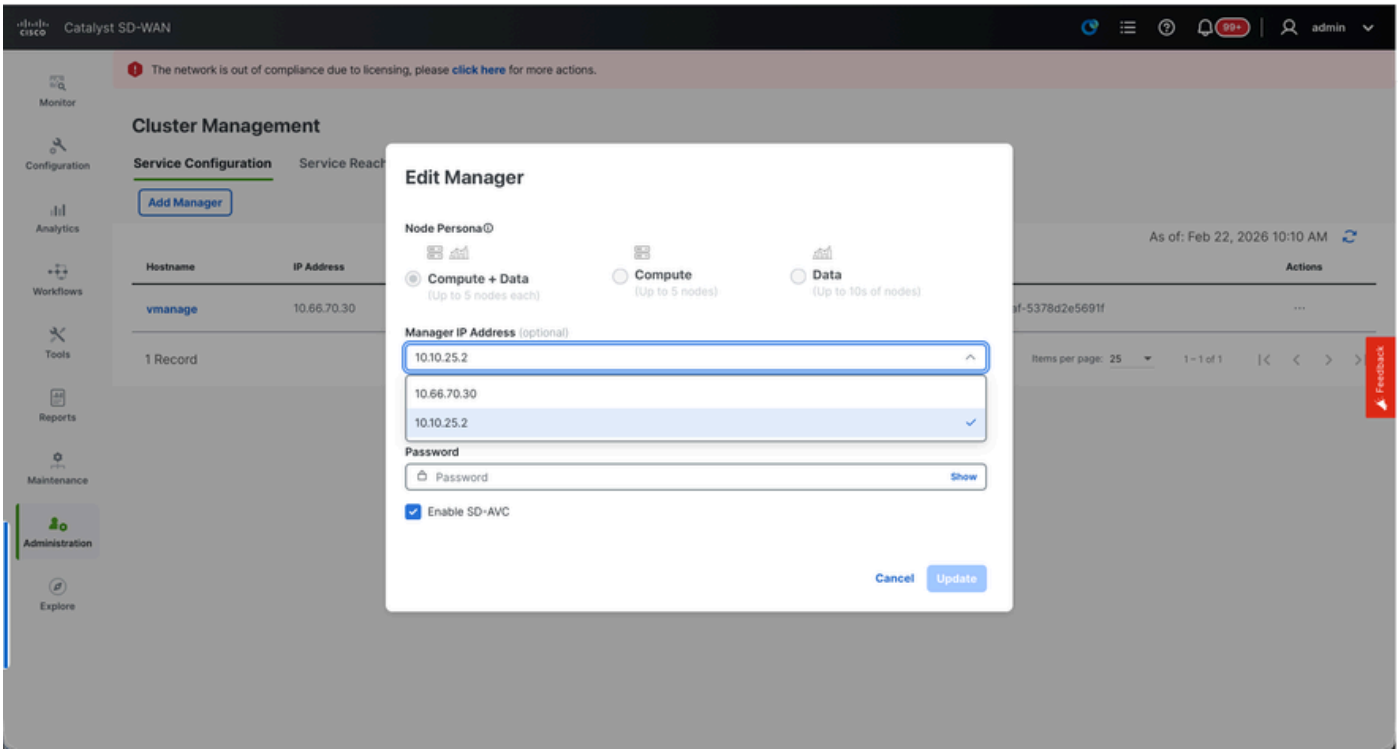
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。如果使用Digicert和企业根证书，则适用相同步骤。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 跨属于集群的所有vManage节点完成此步骤。

准备构建vManage集群

- 在vManage-1的WebUI上，导航到Administration > Cluster Management，在vManage-1的Actions下点击……，选择Edit。
- 系统会根据在VM启动时选择的角色自动选择节点角色。

注意：对于有3个节点的集群，所有3个vManage节点都以计算+数据作为角色。

- 对于6节点集群，3个vManage节点采用计算+数据作为角色，3个vManage节点采用数据作为角色。
- 从Manager IP地址下拉列表中，确保选择vManage的服务接口IP。

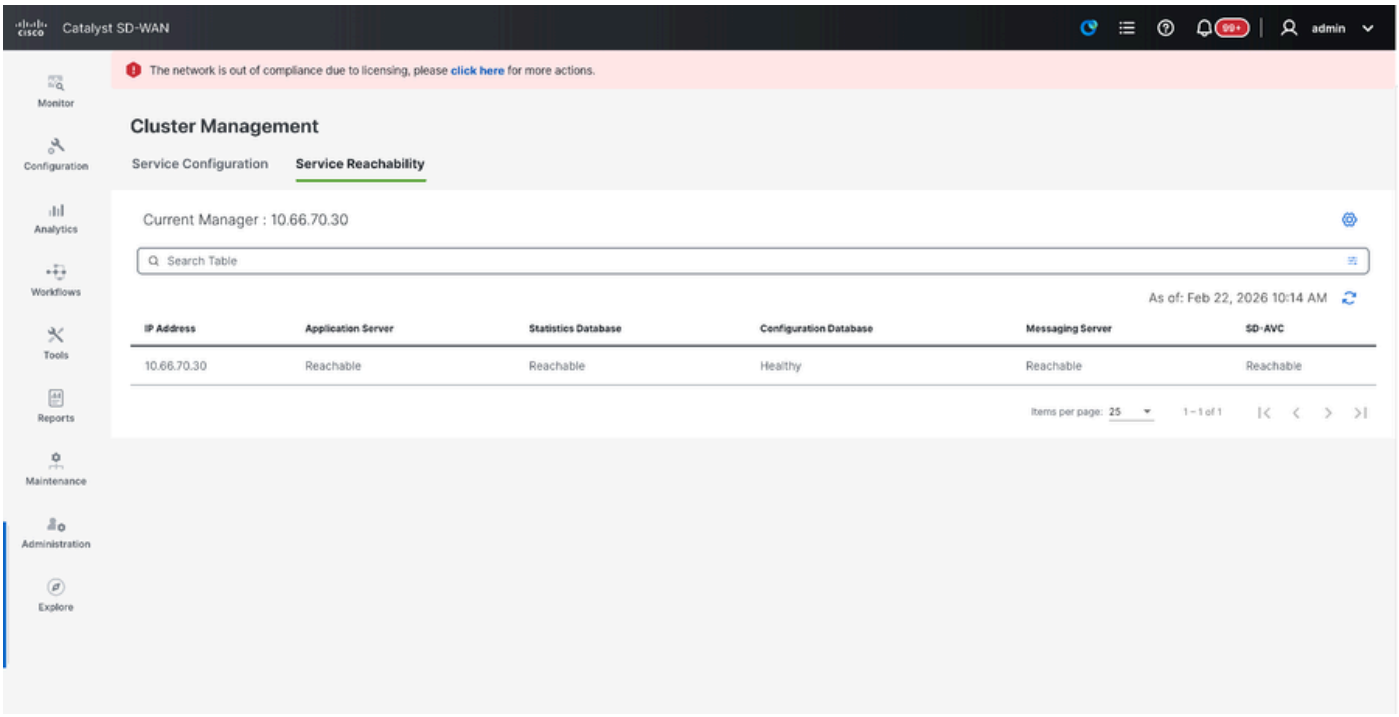


- 输入用于启用vManage集群（称为集群凭证）所需的用户名和密码。
- 如前所述，必须在所有vManage节点上配置相同的凭证，并且必须在将所有节点添加到集群时使用。

注意：请参阅现有集群中的此配置以启用SDAVC — 仅当需要且仅在集群的一个vManage节点上需要时，才需要选中。

点击Update。

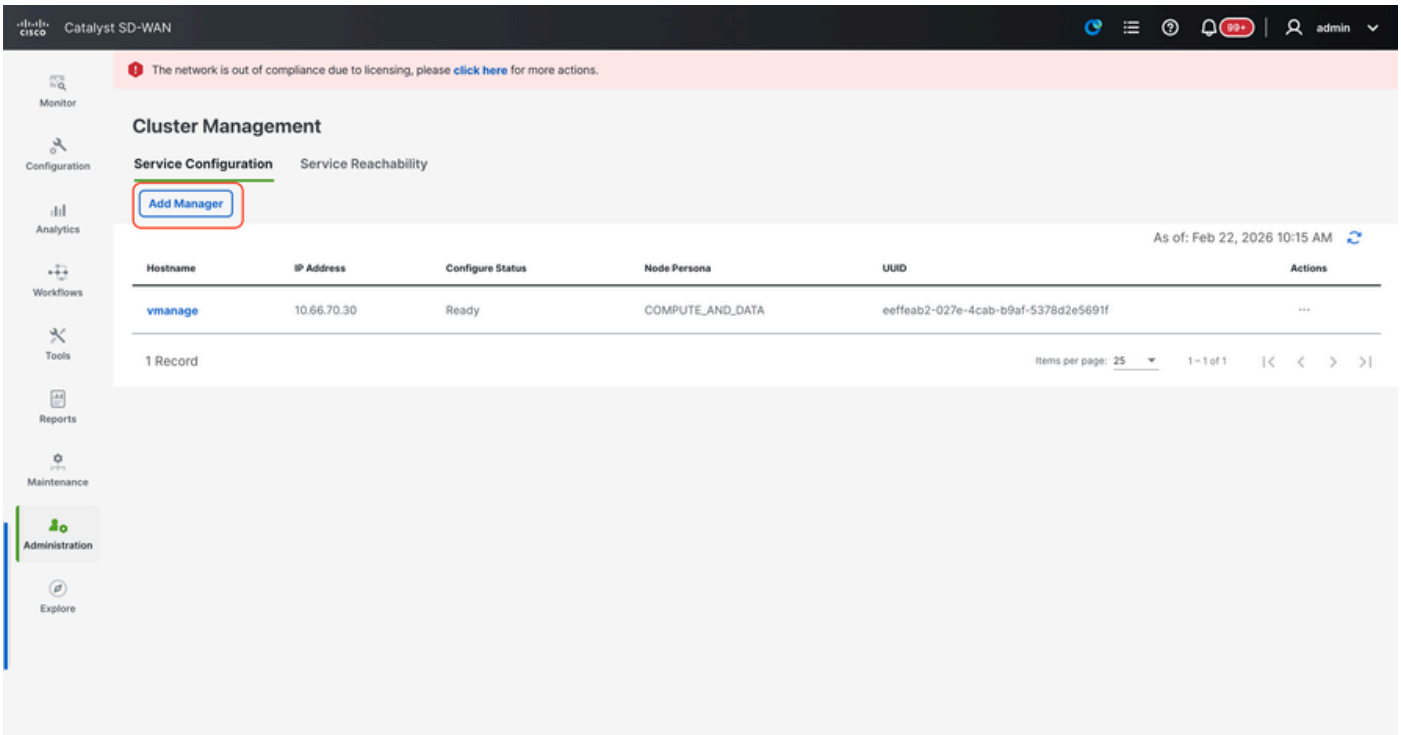
- 之后，vManage NMS服务在后台重新启动，UI在大约5至10分钟的几分钟内不可用。在此期间，vManage的CLI访问可用。
- 可访问vManage-1 UI后，导航到Administration > Cluster Management，确保vManage的服务接口IP反映在IP地址下，Configure Status is Ready，节点角色正确反映。
- 切换至同一页面中的服务可达性部分，并确保所有服务均可访问。

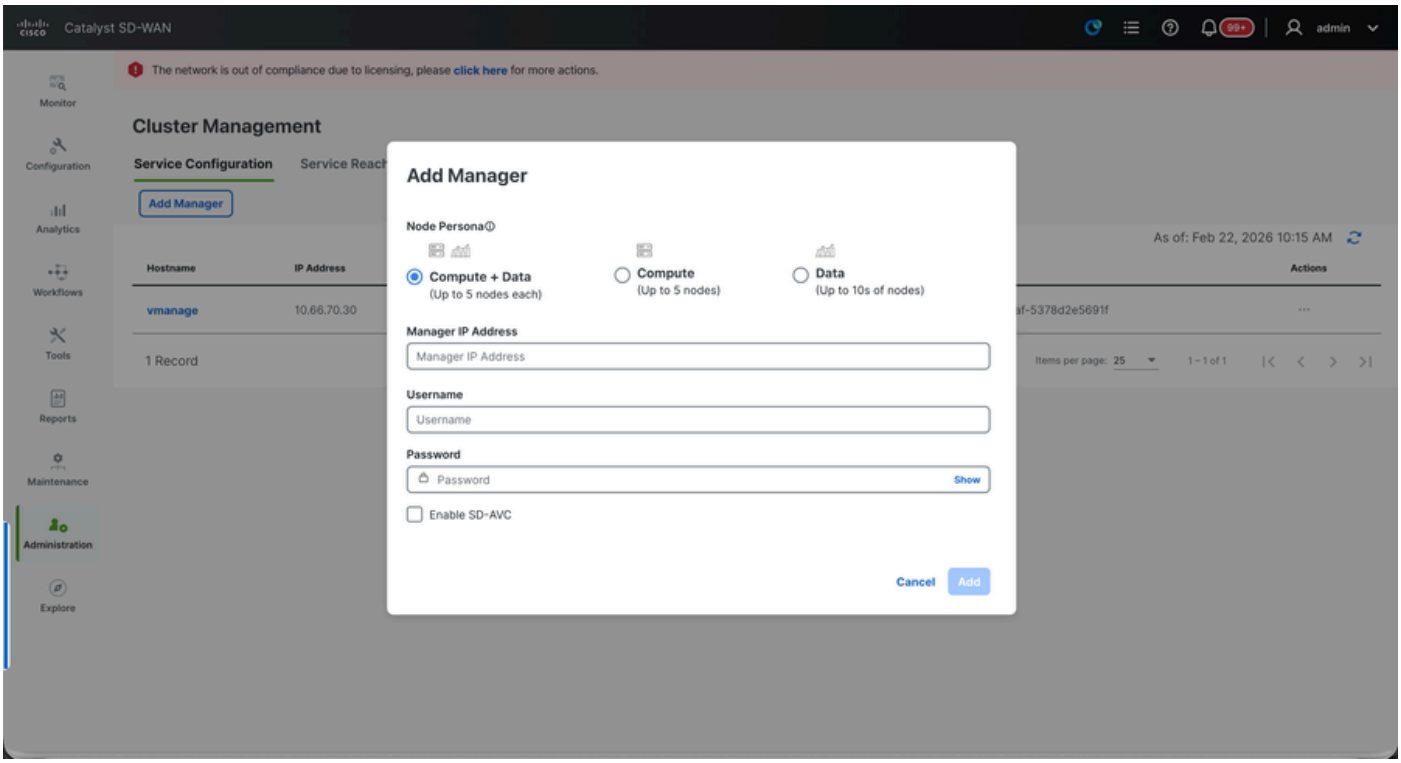


- 如果我们发现任何服务尚未到达，请稍候。通常需要20到30分钟。

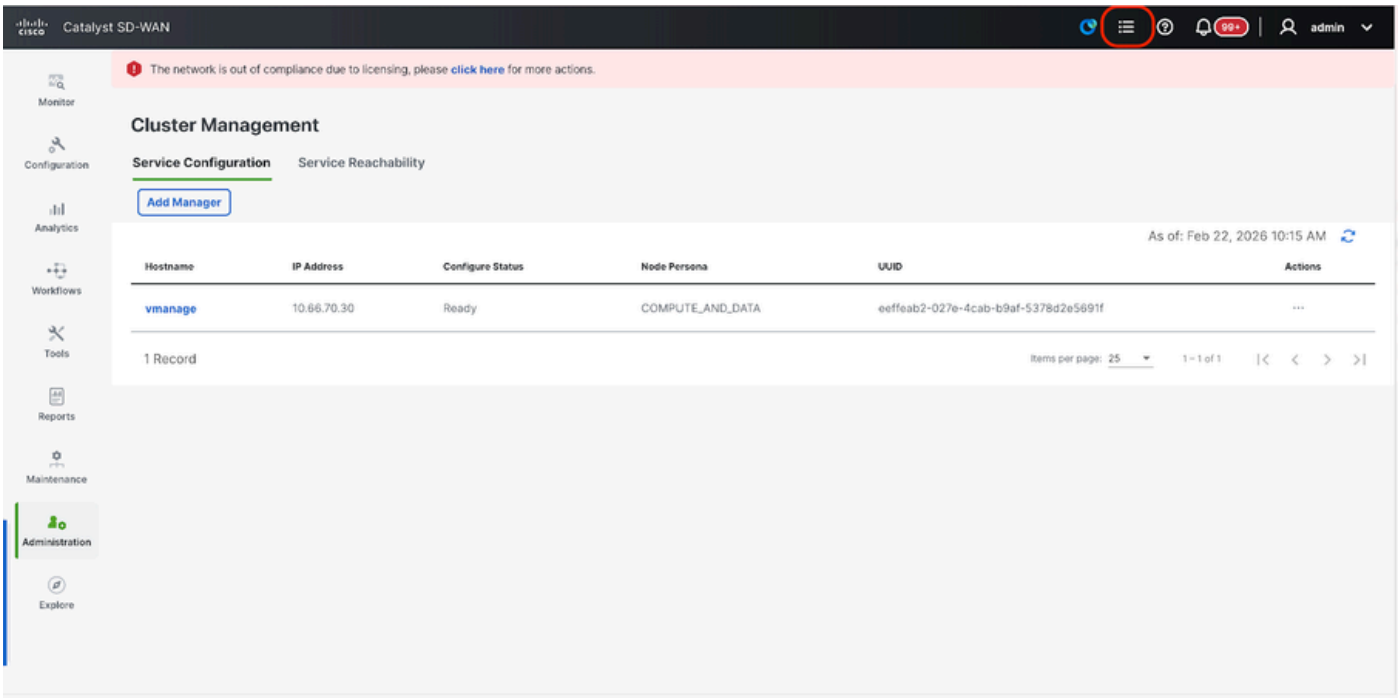
构建vManage集群

- 在vManage-1的WebUI上，导航到Administration > Cluster Management，在Service Configuration部分，
- 单击Add Manager，将出现一个弹出窗口：





- 根据在vManage - 2节点旋转时完成的角色配置选择节点角色。
- 在Manager IP address下输入vManage-2的服务接口IP
- 输入用户名和密码，该凭证与我们在步骤6中使用的凭证相同。
- 启用SDAVC — 保持未选中状态，因为我们本可以在vManage-1上启用它
- 点击Add。
- 之后，vManage 1和2节点的vManage NMS服务在后台重新启动。对于vManage 1和2,UI在大约5至10分钟的时间内不可用。
- 在此期间，vManage 1和2的CLI访问可用。
- 可以访问vManage-1 UI后，导航到Administration > Cluster Management，确保两个vManage的服务接口IP都反映在IP地址下，Configure Status is Ready，并且节点角色正确反映。
- 切换到同一页中的“服务可接通性”部分，并确保两个vManage节点的所有服务均可访问。
- 如果我们发现任何服务尚未到达，请稍候。通常需要5到10分钟。
- 您可以在vManage UI右上角可用的任务列表中检查集群添加进程的状态。



- 您可以查找“活动”任务列表，如果该任务仍列在“活动”任务列表下，则表明该任务尚未完成。
- 您可以单击任务来检查相同任务的进度。如果该任务未列在“活动任务”列表下，请切换到“已完成”，并确保任务成功完成。
- 只有在验证这些点后，才能继续下一步。

在将下一个节点添加到集群之前，需要考虑以下几点:

请验证到目前为止已添加到集群的vManage节点的所有UI上的以下点：

- 导航到Monitor > Overview of vManage UI，确保正确反映了vManage节点的数量，且根据添加到集群的节点数量可以看到。

- 导航到Administration > Cluster Management，并确保两个vManage的服务接口IP均反映在IP地址下，Configure Status is Ready且节点角色正确反映。
- 切换到同一页中的“服务可接通性”部分，并确保两个vManage节点的所有服务均可访问。

- 每次向集群中添加节点时，集群中所有节点的NMS服务都会重新启动，因此在一段时间内，所有这些节点的UI都变得不可达。
- 根据群集中的节点数量，可能需要较长的时间才能备份UI和访问所有服务。
- 您可以在vManage UI右上角的Task-list下监控任务。
- 在添加到集群的每个节点的vManage UI上，我们需要查看所有路由器、模板和策略（如果它们在vManage-1中可用）。
- 如果这些配置不存在于vManage-1上，则添加到vManage-1中的vBonds和vSmarts以及组织 — 名称、vBond、证书授权的Administration > Settings配置必须反映在添加到集群的其他vManage节点上。
- 对其余vManage节点重复相同步骤。

所有控制器入网后，请完成以下步骤：

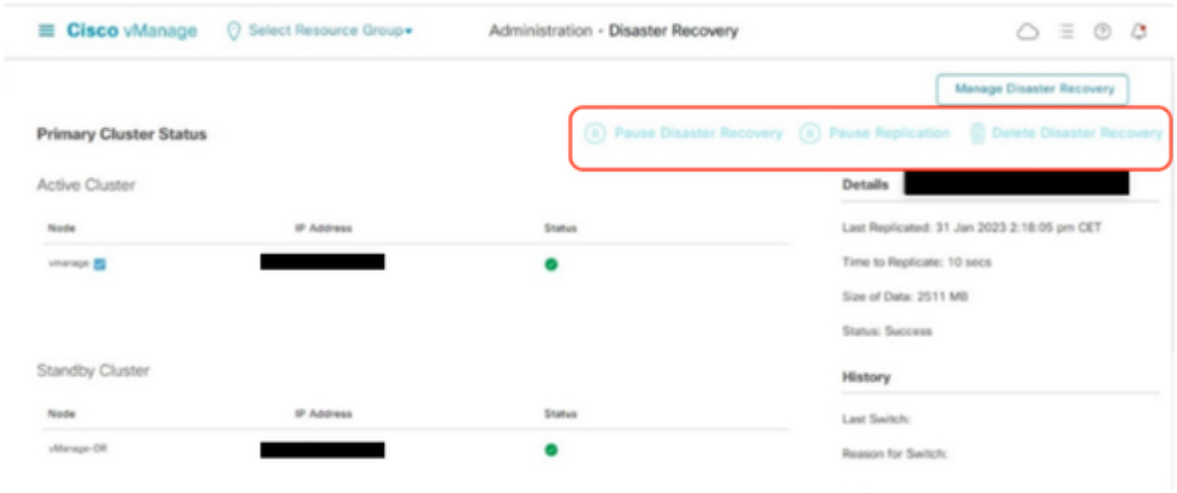
步骤 4：Config-db备份/恢复

在另一个vManage节点上收集vManage configuration-db备份和恢复

注意：从已启用灾难恢复的现有vManage群集收集配置数据库备份时，请确保在该节点上的灾难恢复暂停并删除后收集配置数据库备份。

确认没有正在进行的灾难恢复复制。导航到管理>灾难恢复和 确保状态为Success且未处于Import Pending、Export Pending或Download Pending等暂时状态。如果状态未成功，请联系Cisco TAC并确保复制成功，然后继续暂停灾难恢复。

首先暂停灾难恢复并确保任务完成。然后删除灾难恢复并确认任务已完成。



联系思科TAC以确保成功清理灾难恢复。

收集Configuration-DB备份：

- 在当前正在使用的SD-WAN交换矩阵中，可以从vManage集群生成configuration-db备份。
- 请注意，我们只能在vManage群集的其中一个节点（即configuration-db领导者）上生成configuration-db backup。

- 对于独立vManage，该vManage本身是配置数据库领导者。
- 在vManage集群中，使用命令request nms configuration-db diagnostics确定configuration-db领导节点。您可以在3节点vManage集群的所有节点上运行此命令。
- 在6节点集群中，请确保在启用了configuration-db的vManage节点上运行此命令以标识领导节点。 导航到管理>集群管理以验证相同内容：
- 如屏幕截图所示，配置了persona COMPUTE_AND_DATA的节点正在运行configuration-db。

您可以在vManageCLI上使用requestnmsconfiguration-dbstatus命令验证相同。输出如下所示

```
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#
```

- 执行命令后，在这些节点上请求nms configuration-db diagnostics，输出如下所示：
- 查找“IsLeader”的突出显示的字段。如果设置为1，则表明节点是领导节点，我们可以从中收集configuration-db备份。

```
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     .
```

使用此命令从已确定的configuration-db领导vManage节点收集configuration-db备份。

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

预期输出如下所示：

```
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凭证，请记下该凭证。
- 如果您不知道配置数据库凭证，请联系TAC从现有vManage节点检索配置数据库凭证。
- 默认的configuration-db凭证是用户名：neo4j和密码：密码

将Configuration-db备份恢复到另一个vManage节点

使用SCP将configuration-db备份复制到vManage的/home/admin/目录。

scp命令输出示例：

```
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
```

要恢复configuration-db备份，首先需要配置configuration-db凭据。如果您的配置数据库凭证是默认凭证(neo4j/password)，我们可以跳过此步骤。

要配置configuration-db凭据，请使用命令request nms configuration-db update-admin-user。使用您选择的用户名和密码。

请注意，vManage的应用服务器已重新启动。由于此vManage UI在短时间内变得不可访问。

```
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#
```

发布后，我们可以继续恢复configuration-db备份：

我们可以使用命令request nms configuration-db restore path /home/admin/< >将配置数据库恢复到新的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
```

恢复configuration-db后，请确保vManage UI可访问。等待约5分钟，然后尝试访问UI。

成功登录UI后，请确保边缘路由器列表、模板、策略以及之前或现有vManage UI上存在的所有其余配置都反映在新的vManage UI上。

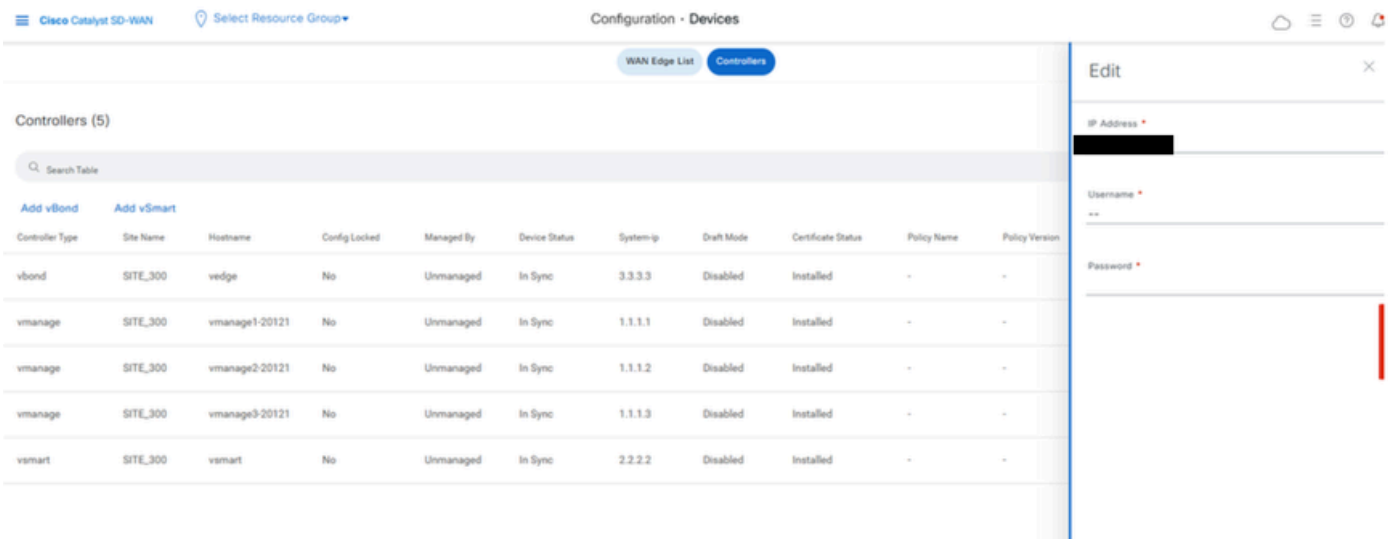
步骤 5：控制器重新验证和旧控制器失效

恢复configuration-db后，我们需要重新验证交换矩阵中的所有新控制器(vmanage/vsmart/vbond)

注：在实际生产中，如果用于重新身份验证的接口IP是隧道接口IP，则需要确保在vManage、vSmart和vBond的隧道接口以及路径沿途的防火墙上允许NETCONF服务。要打开的防火墙端口是从DR群集到所有vBonds和vSmarts的双向规则的TCP端口830。

在vmanage UI上，点击Configuration > Devices > Controllers

- 点击每个控制器附近的三个点，然后点击Edit



- 将ip-address（控制器的系统ip）替换为transport vpn 0（隧道接口）ip地址。输入用户名和密码，然后点击save
- 对交换矩阵中的所有新控制器执行相同操作

同步根证书链

所有控制器入网后，请完成以下步骤：

在新活动集群中的任何Cisco SD-WAN Manager服务器上，执行以下操作：

输入以下命令将根证书与新活动集群中的所有Cisco Catalyst SD-WAN设备同步：

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

输入以下命令将Cisco SD-WAN Manager UUID与Cisco SD-WAN Validator同步：

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

一旦交换矩阵恢复，并且交换矩阵中的所有边缘和控制器的控制和bfd会话都已启动，我们就需要从UI使旧控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，点击Configuration > Devices > Certificates
- 点击“控制器”
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击invalidate（失效）
- 点击send to vbond
- 在vmanage UI上，点击Configuration > Devices > Controllers
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。单击删除。

步骤 6：过帐检查

注意：继续此处所示的“后检查”部分，它适用于所有部署组合。

组合4:vManage Cluster +手动/冷备份DR

什么是手动/冷备份DR — 备份SD-WAN Manager服务器或SD-WAN Manager群集在冷备份状态下保持关闭。

对活动数据库进行定期备份，如果主SD-WAN Manager或SD-WAN Manager集群发生故障，则手动启动备用SD-WAN Manager或SD-WAN Manager集群，并在其中恢复备份数据库。

所需实例：

- 3或6个vManage（主集群）
- 3或6个vManage（DR备用集群）
- 1个或多个vBond（分布于主数据中心和DR数据中心）
- 1个或多个vSmart（分布于主数据中心和DR数据中心）

步骤:

1. 使用通用步骤启动所有实例
2. 预检查
3. 配置vManage UI、证书和板载控制器
4. 构建vManage集群
5. 冷备用DR集群设置
6. Config-db备份/恢复
7. 过帐检查

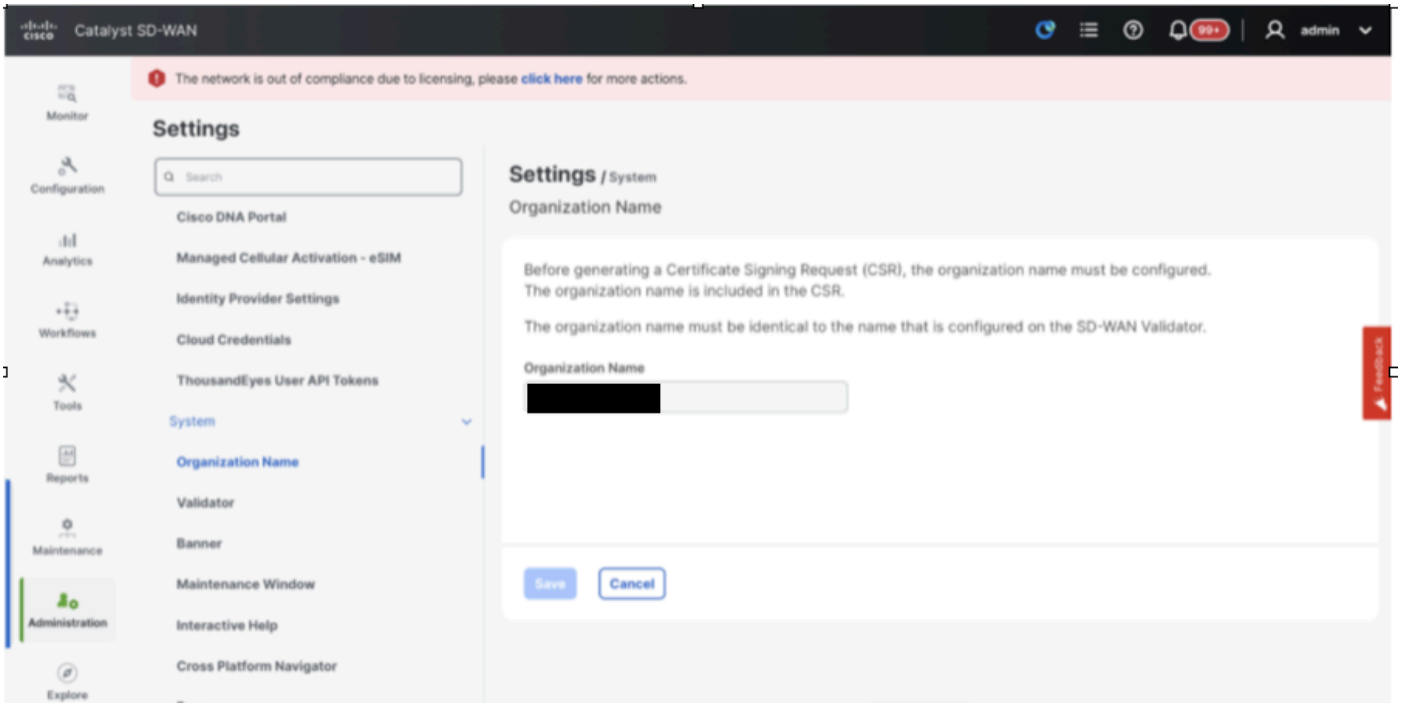
步骤 1：预检查

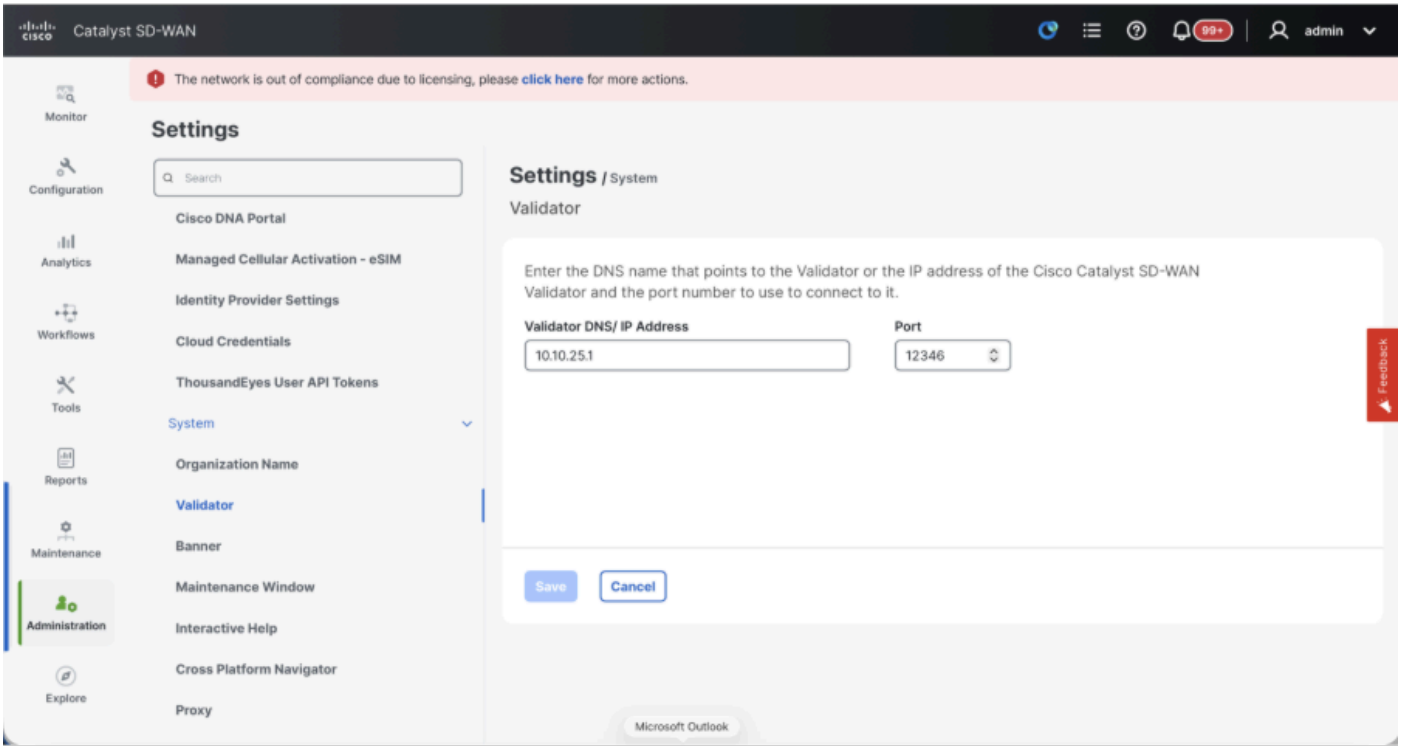
- 确保活动的Cisco SD-WAN Manager实例数与新安装的Cisco SD-WAN Manager实例数相同。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例都运行相同的软件版本。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例能够到达Cisco SD-WAN Validator的管理IP地址。
- 确保证书已安装在新安装的Cisco SD-WAN Manager实例上。
- 确保所有Cisco Catalyst SD-WAN设备(包括新安装的Cisco SD-WAN Manager)上的时钟都同步。
- 确保在新安装的Cisco SD-WAN Manager实例上配置一组新的系统IP和站点ID，同时配置与活动集群相同的基本配置。

步骤 2：配置vManage UI、证书和板载控制器

更新vManage UI上的配置

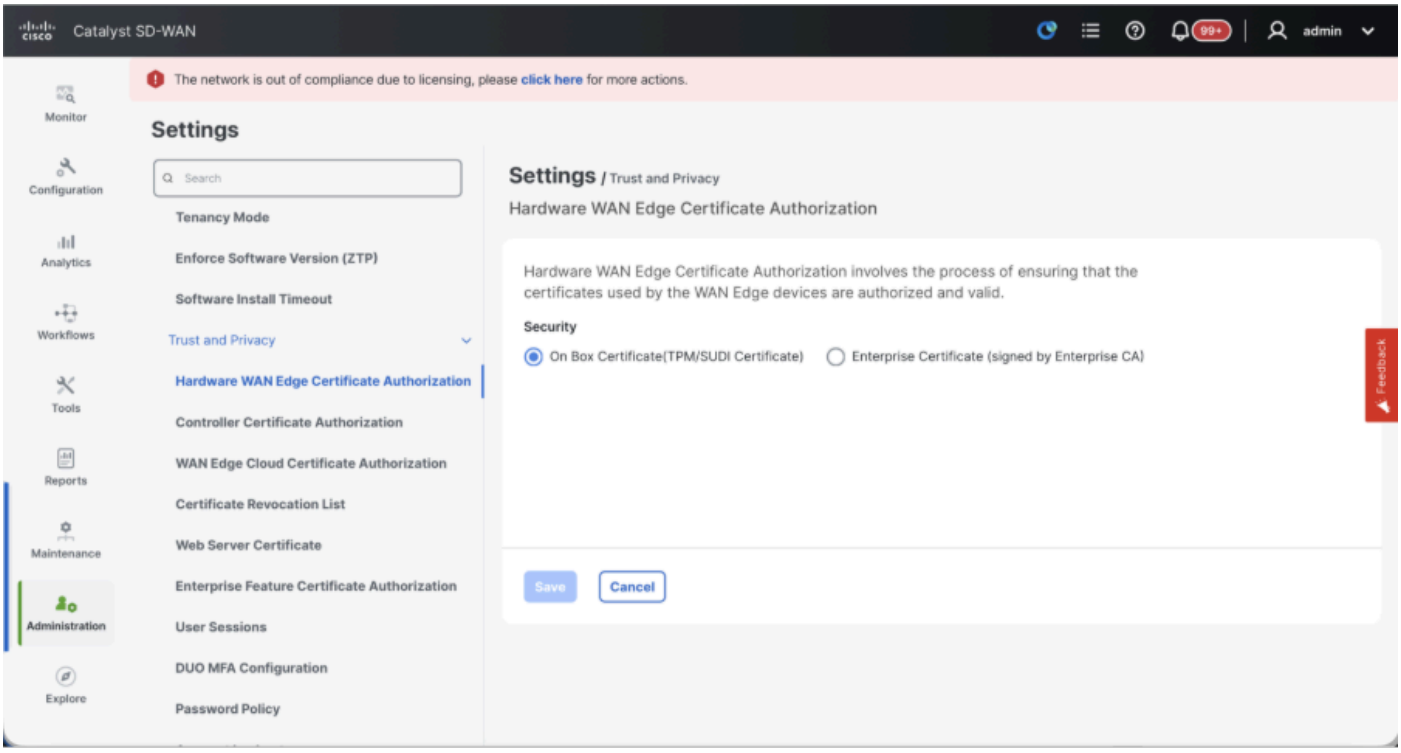
- 一旦将步骤1中的配置添加到所有控制器的CLI中，我们就可以使用浏览器中的URL https://<vmanage-ip>访问vManage的WebUI。使用各个vManage节点的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 导航到管理>设置并完成以下步骤。
- 配置组织名称和验证器/vBond URL/IP地址。配置与vManage节点的CLI中相同的值。
- 在vManage 20.15/20.18中，这些配置在System部分下提供。





- 验证证书授权(CA)的配置，CA决定用于证书签名的证书颁发机构。我们可以看到3个选项：

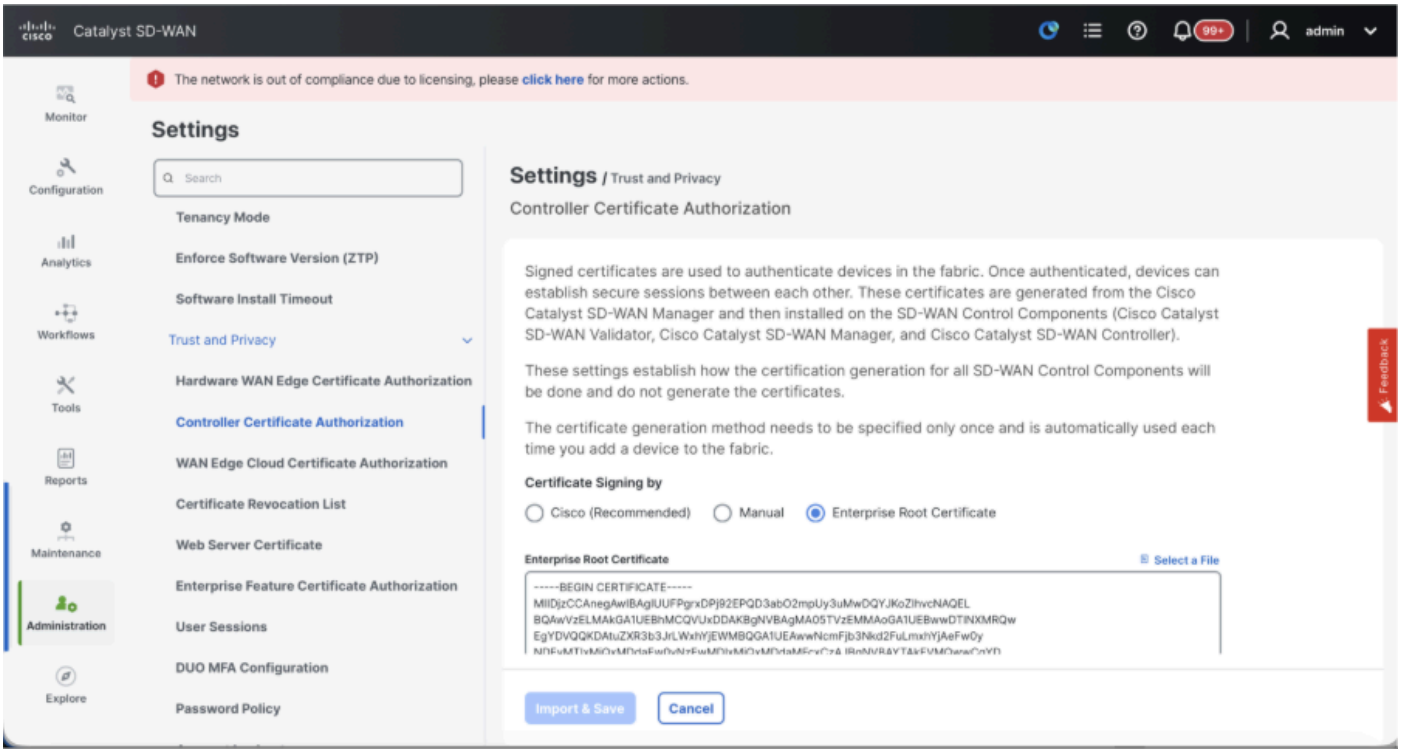
1. 硬件WAN边缘证书授权 — 确定硬件SD-WAN边缘路由器的CA。
    - 开箱证书（TPM/SUDI证书）— 使用此选项，路由器硬件上预安装的证书用于建立控制连接（TLS/DTLS连接）
    - 企业证书（由企业CA签署）— 使用此选项时，路由器使用由组织的企业证书颁发机构签署的证书。选择此选项时，必须在此处更新企业CA的根证书。



2. 控制器证书授权 — 决定SD-WAN控制器的CA。
    - 思科（推荐）— 控制器使用思科PKI签名的证书。vManage使用vManage上配置的智能

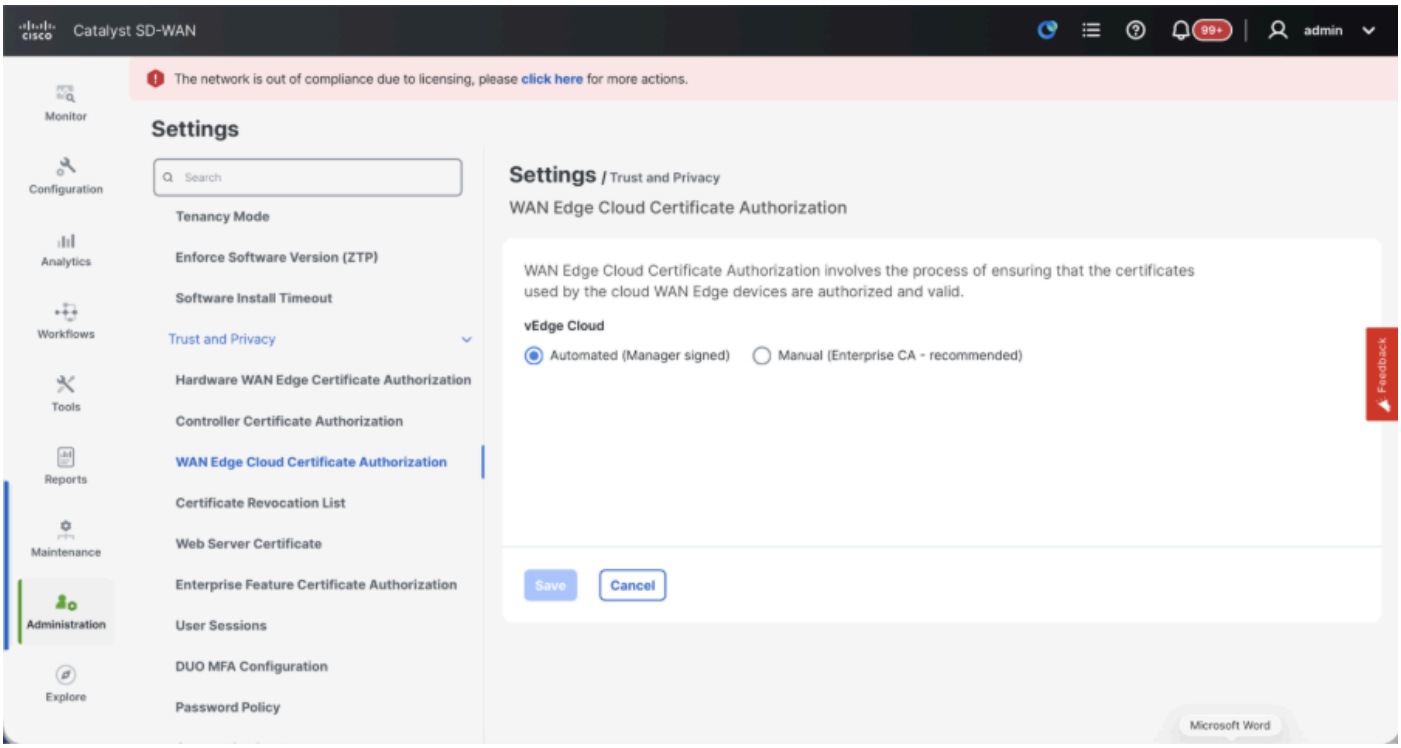
帐户凭证自动联系PNP门户，并获取证书签名并安装在控制器上。

- 手动 — 控制器使用由Cisco PKI签名的证书。使用思科PNP门户手动签署CSR，方法是导航到相应SD-WAN重叠的智能帐户和虚拟帐户。
- 企业根证书 — 通过此选项，路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

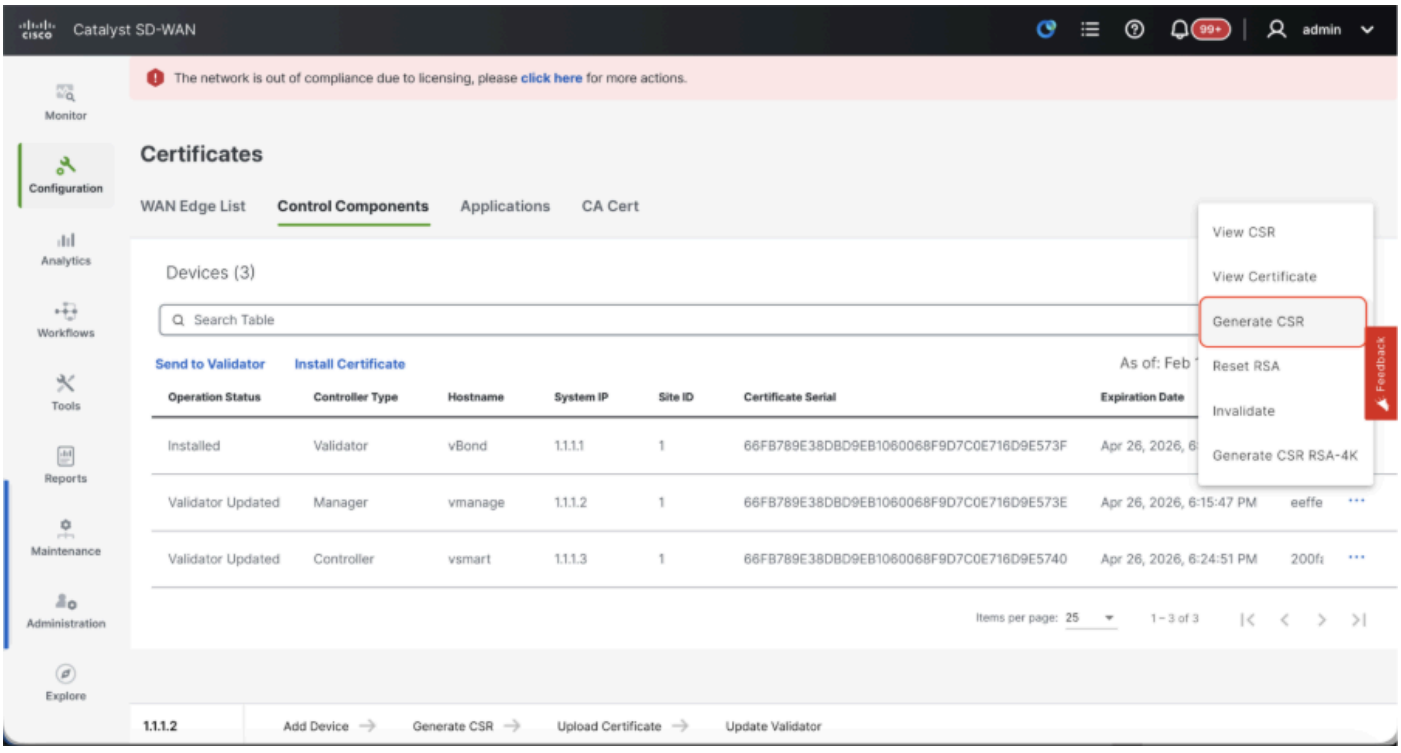


3. 广域网边缘云证书授权 — 确定虚拟SD — 广域网边缘路由器（CSR1000v、C8000v、vEdge云）的CA
    - 自动（vManage签名） — vManage自动为虚拟边缘路由器签署CSR并在路由器上安装证书。
    - 手动（企业CA — 推荐） — 虚拟路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

例如，如果我们使用自己的CA（企业证书颁发机构），请选择Enterprise。



- 如果是20.15/20.18 vManage节点，请导航到配置>证书>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers
- 为Manager/vManage点击……，然后点击Generate CSR。



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

将vBond/Validator和vSmart/Controller注册到vManage

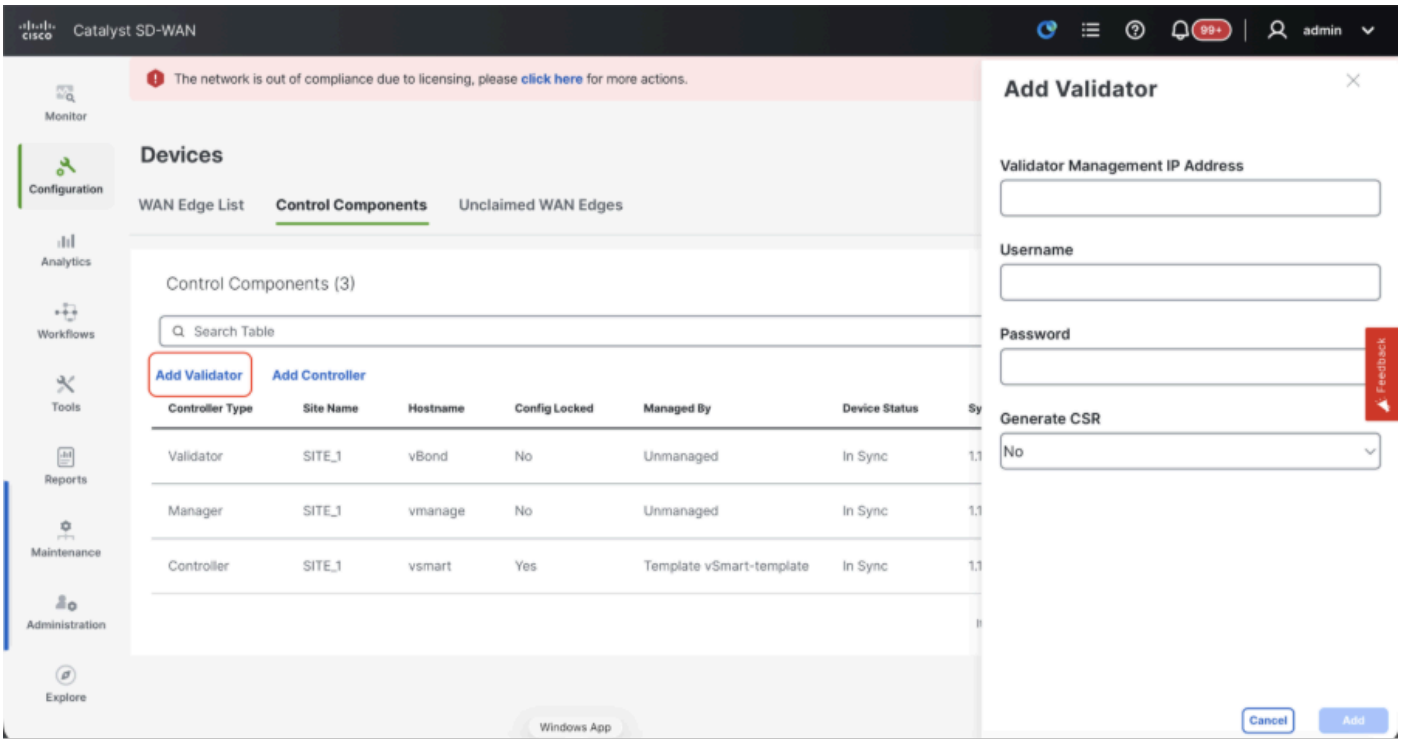
如果是20.15/20.18 vManage节点，请导航到配置>设备>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers

OnboardingvBond/验证器

- 单击AddvBond对于20.12vManageor的情况添加验证程序20.15/20.18vManage。系统打开一个弹出窗口，输入 vBond的VPN 0传输IP，可从vManage访问。
- 如果允许，请从vManagetovBondIP的CLI使用ping检查可接通性。
- 输入vBond的用户凭证。

注意：我们需要将vBondor的管理凭据用作netadmingroup的用户部分。您可以在vBond的CLI中验证这一点。如果我们需要为vBond安装新证书，请在“生成CSR”的下拉列表中选择是

注意：如果vBond位于NAT设备/防火墙之后，请检查vBond VPN 0接口IP是否已转换为公共IP。如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口的公用IP地址



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vBond上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户

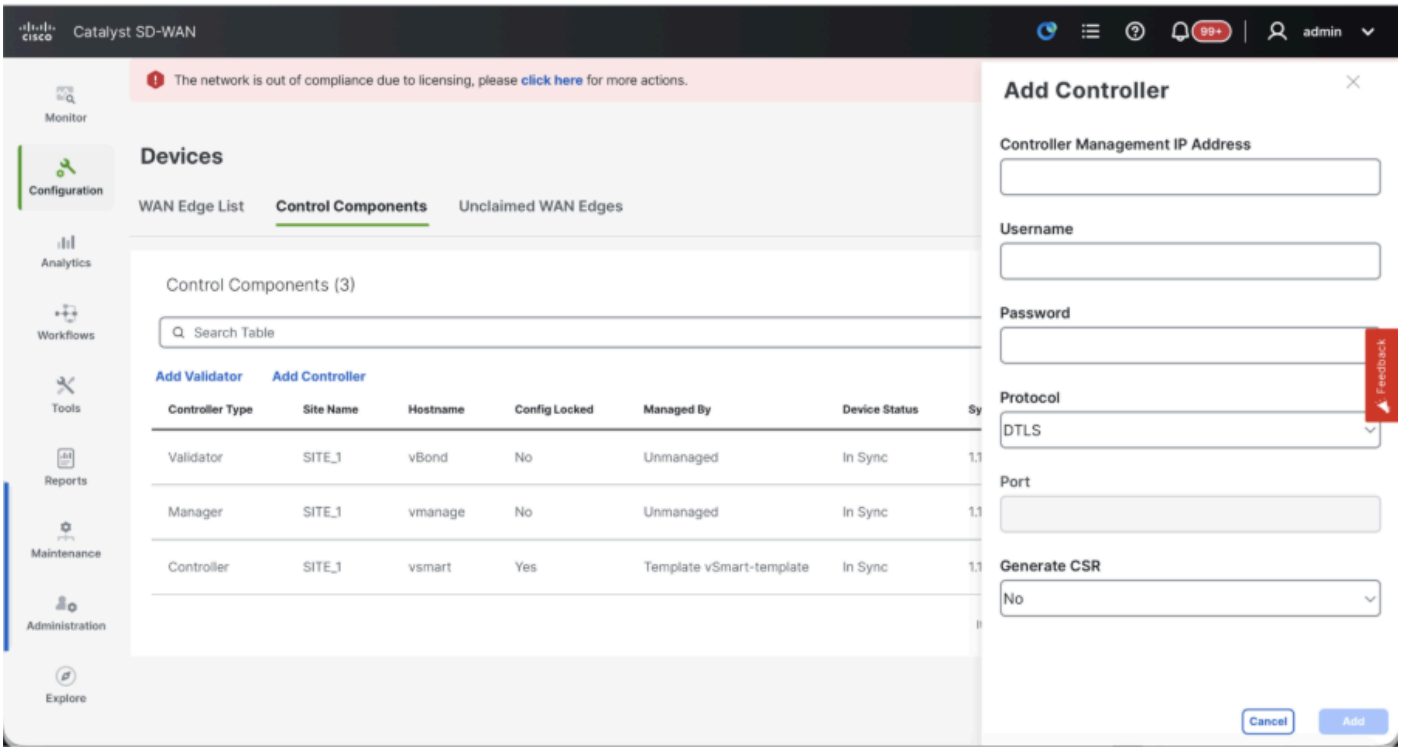
手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

- 如果有多个vBonds，请重复相同的步骤。

自注册vSmart/控制器：

- 在20.12 vManage中点击Add vSmart，在20.15/20.18 vManage中点击Add Controller。
- 系统打开一个弹出窗口，输入vSmart的VPN 0传输IP，可从vManage访问。
- 如果允许从vManage的CLI到vSmart IP，请使用ping检查可达性。
- 输入vSmart Note的用户凭据，我们需要使用vSmart的管理员凭据或netadmin组的用户部分。
- 您可以在vSmart的CLI中验证这一点。
- 如果打算对路由器使用TLS来建立与vSmart的控制连接，请将协议设置为TLS。此配置也需要在vSmarts和vManage节点的CLI上进行配置。
- 如果需要为vSmart安装新证书，请在生成CSR"的下拉列表中选择Yes。

注意：如果vSmart位于NAT设备/防火墙之后，请检查vSmart VPN 0接口IP是否已转换为公共IP，如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口IP的公共IP地址。



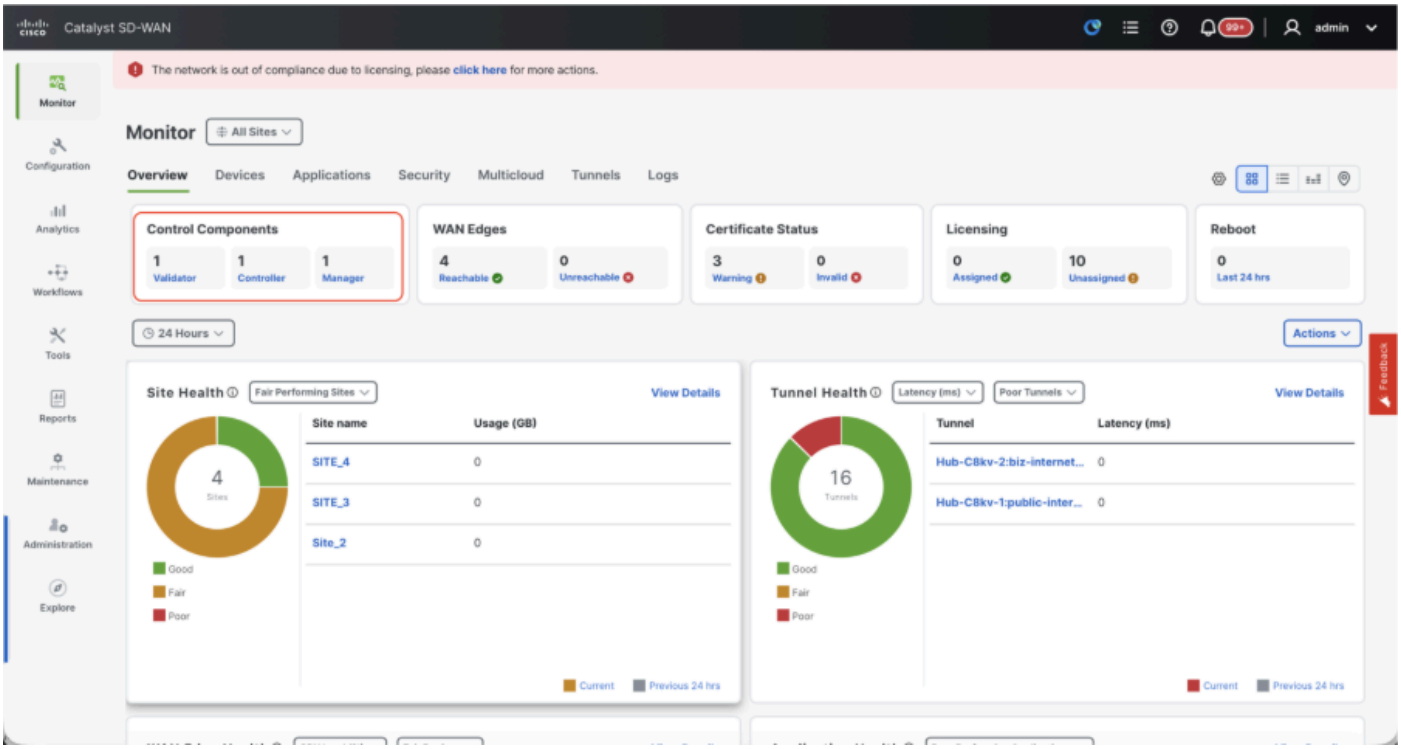
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将

CSR上传到PNP门户，并且证书签名后，会自动将其安装在vSmart上。

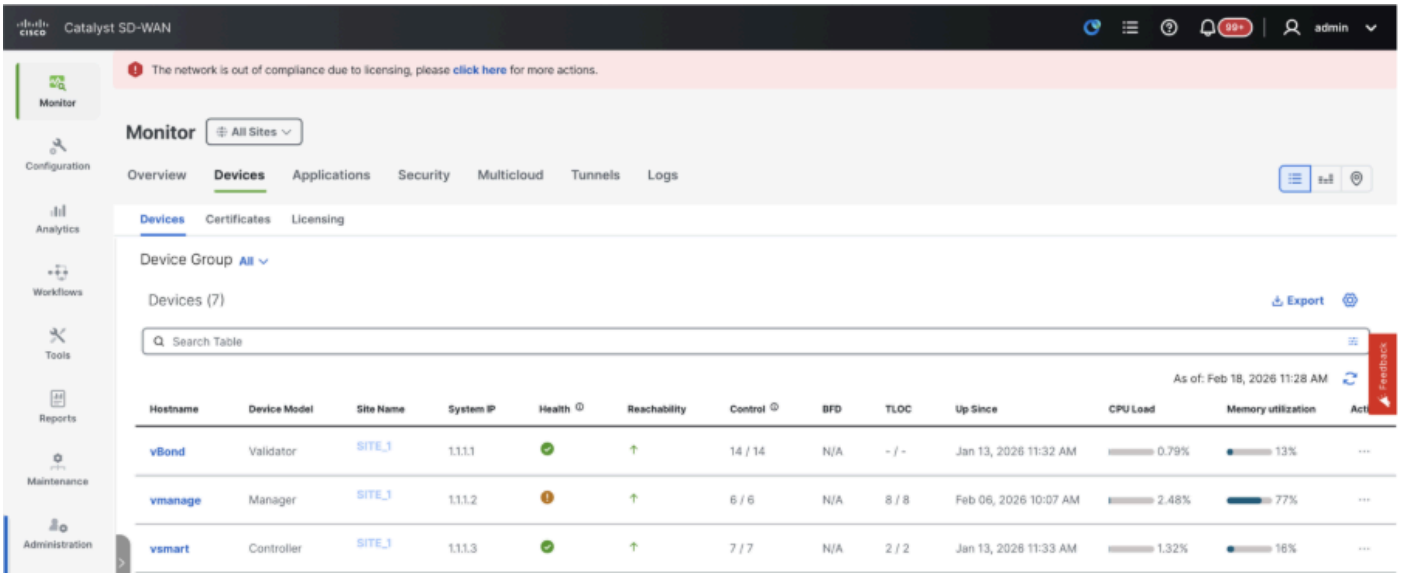
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 如果有多个vSmarts，请重复相同的步骤。

确认

完成所有步骤后，在Monitor>Dashboard中确认所有控制组件均可访问



- 单击相应的控制组件，确认它们都可访问。
- 导航到监控>设备，确认所有控制组件均可访问。



步骤 3：构建vManage集群

板载SD-WAN交换矩阵，在SD-WAN重叠中带有vManage集群

注意:vManage集群可以配置3个vManage节点或6个vManage节点，具体取决于注册到SD-WAN交换矩阵的站点数量

通过单个vManage节点加入所有SD-WAN控制器

继续执行“在SD-WAN重叠中带单节点vManage的板载SD-WAN控制器”中共享的步骤，首先启用带一个vManage节点的SD-WAN交换矩阵，然后板载所有所需的验证器(vBond)和控制器(vSmart)。

配置属于集群的所有vManage节点的CLI配置

- 配置vManage节点的其余节点。对于3个节点集群，您有剩余的2个要配置的节点；对于6个节点集群，您有5个要配置的节点。
- 配置系统配置，如下所示：

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注意:如果我们使用URL作为vBond地址，请确保在VPN 0配置中配置DNS服务器IP地址或确保可以解析这些地址。

需要使用这些配置来启用传输接口，该接口用于与路由器和其余控制器建立控制连接。

```
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
```

还要配置VPN 512管理接口以启用对控制器的带外管理访问。

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

可选配置：

- 您可以参考现有控制器的配置，如果此处列出的配置存在，您可以将此配置添加到新控制器。
- 仅当路由器需要使用TLS与vManage节点建立安全控制连接时，才将控制协议配置为TLS。默认情况下，所有控制器和路由器都使用DTLS建立控制连接。根据您的要求，此配置是仅在vSmart和vManage节点上必需的可选配置。

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

在所有vManage节点上配置服务接口

在所有vManagenode(包括已注册的vManage-1)上配置服务接口。此接口用于集群通信，即集群中vManagenodes之间的通信。

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

确保同一IP子网用于vManagecluster中所有节点上的服务接口。

配置集群凭证

我们可以使用与vManagenode相同的管理凭据配置vManagecluster。否则，我们可以配置作为netadmingroup一部分的新用户凭据。配置新用户凭据的配置如下所示

```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

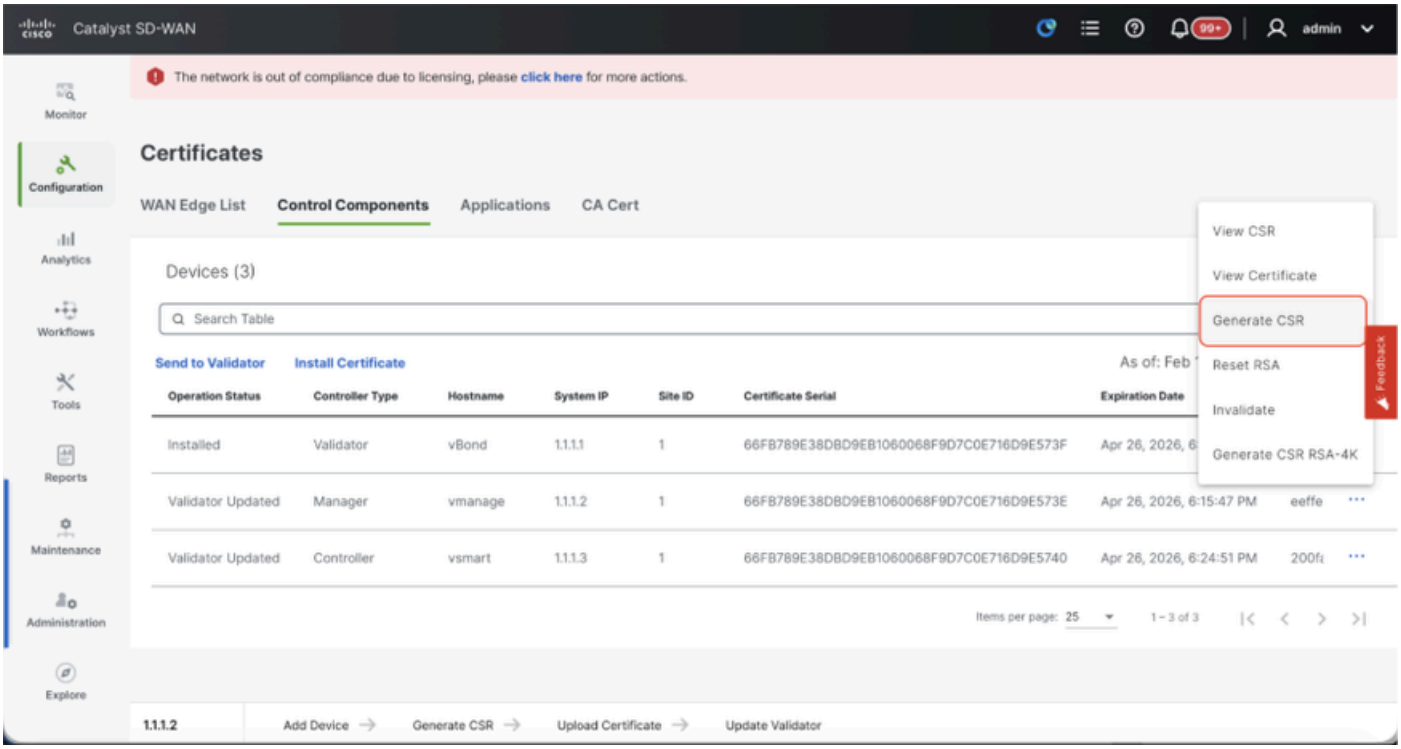
确保在属于群集的所有vManagenode上配置相同的用户凭据。如果我们决定使用管理员凭据，则必须在所有vManagenode上配置相同的用户名/密码。

在所有vManage节点上安装设备证书

- 使用浏览器中的URL https://<vmanage-ip>登录所有vManagenode的tovManageUI。使用各个vManagenode的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 如果是20.15/20.18 vManage节点，请导航到Configuration > Certificates > Control

Components 。对于20.9/20.12版本，Configuration > Devices > Controllers

单击Manager/vManage的……并单击Generate CSR。



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 跨属于集群的所有vManage节点完成此步骤。

准备构建vManage集群

- 在vManage-1的WebUI上，导航到Administration > Cluster Management，在vManage-1的Actions下点击……，选择Edit。
- 系统会根据在VM启动时选择的角色自动选择节点角色。

注意：对于有3个节点的集群，所有3个vManage节点都以计算+数据作为角色。

- 对于6节点集群，3个vManage节点采用计算+数据作为角色，3个vManage节点采用数据作为角色。

- 从Manager IP地址下拉列表中，确保选择vManage的服务接口IP。
- 输入用于启用vManage集群（称为集群凭证）所需的用户名和密码。
- 如前所述，必须在所有vManage节点上配置相同的凭证，并且必须在将所有节点添加到集群时使用。

可选配置：

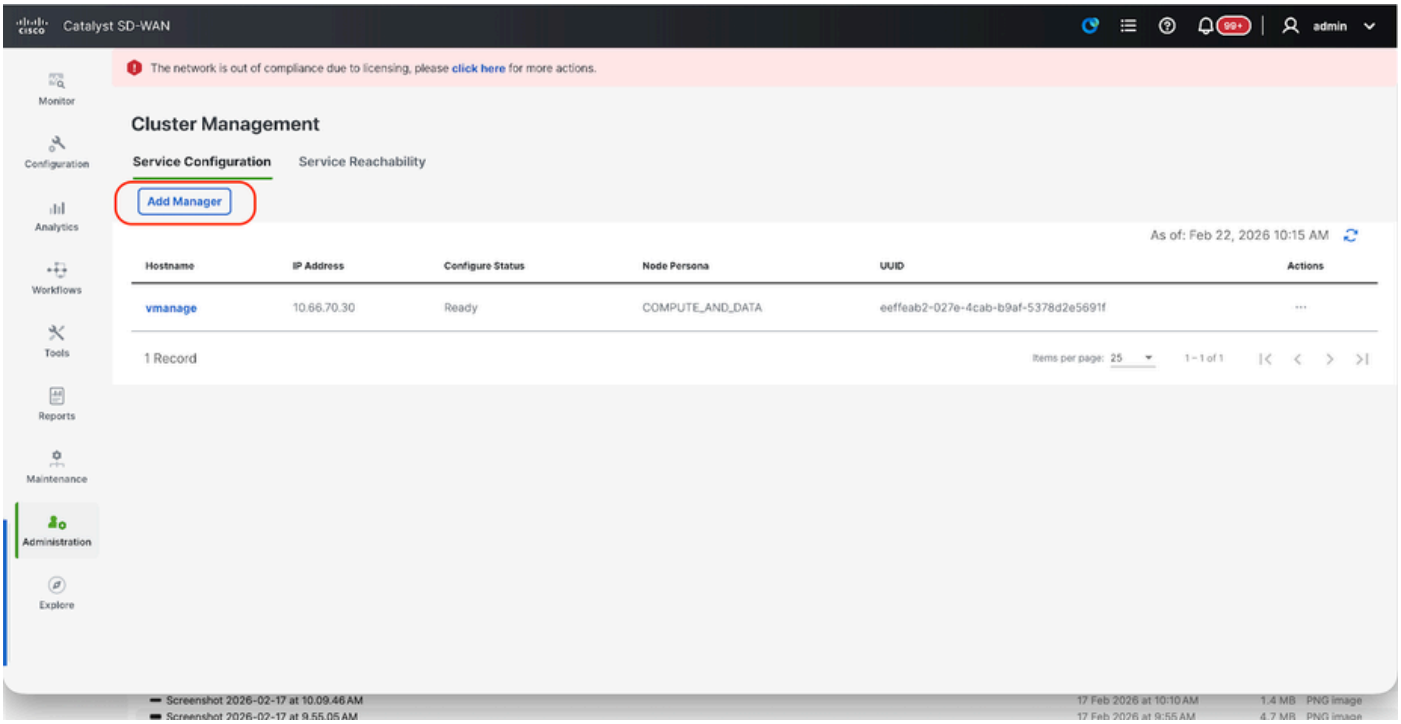
请参阅现有集群中的此配置以启用SDAVC — 仅当需要且仅在集群的一个vManage节点上需要时，才需要选中。

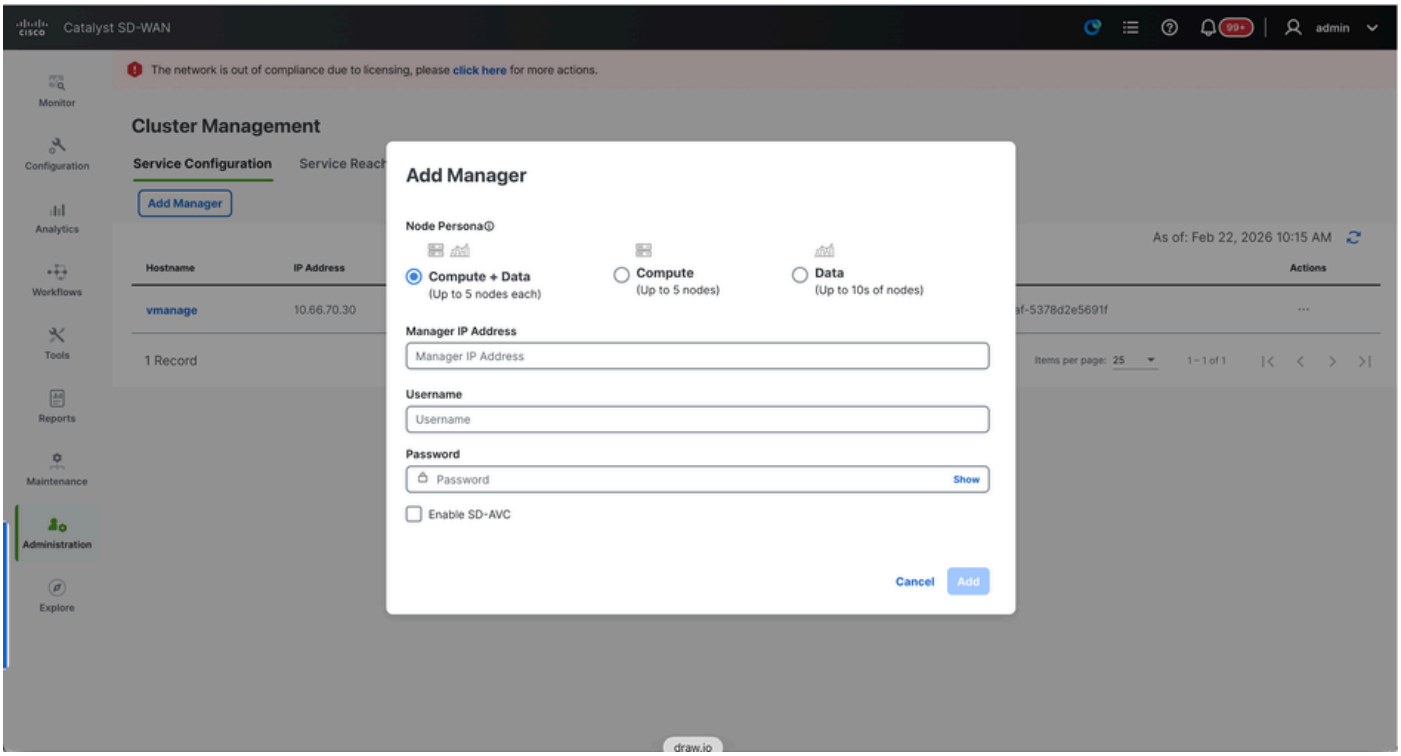
点击Update。

- 之后，vManage NMS服务在后台重新启动，UI在大约5至10分钟的几分钟内不可用。在此期间，vManage的CLI访问可用。
- 可以访问vManage-1 UI后，导航到Administration > Cluster Management，确保vManage的服务接口IP反映在IP地址下，Configure Status is Ready，节点角色正确反映。切换至同一页面中的服务可达性部分，并确保所有服务均可访问。
- 如果我们发现任何服务尚未到达，请稍候。通常需要20到30分钟。

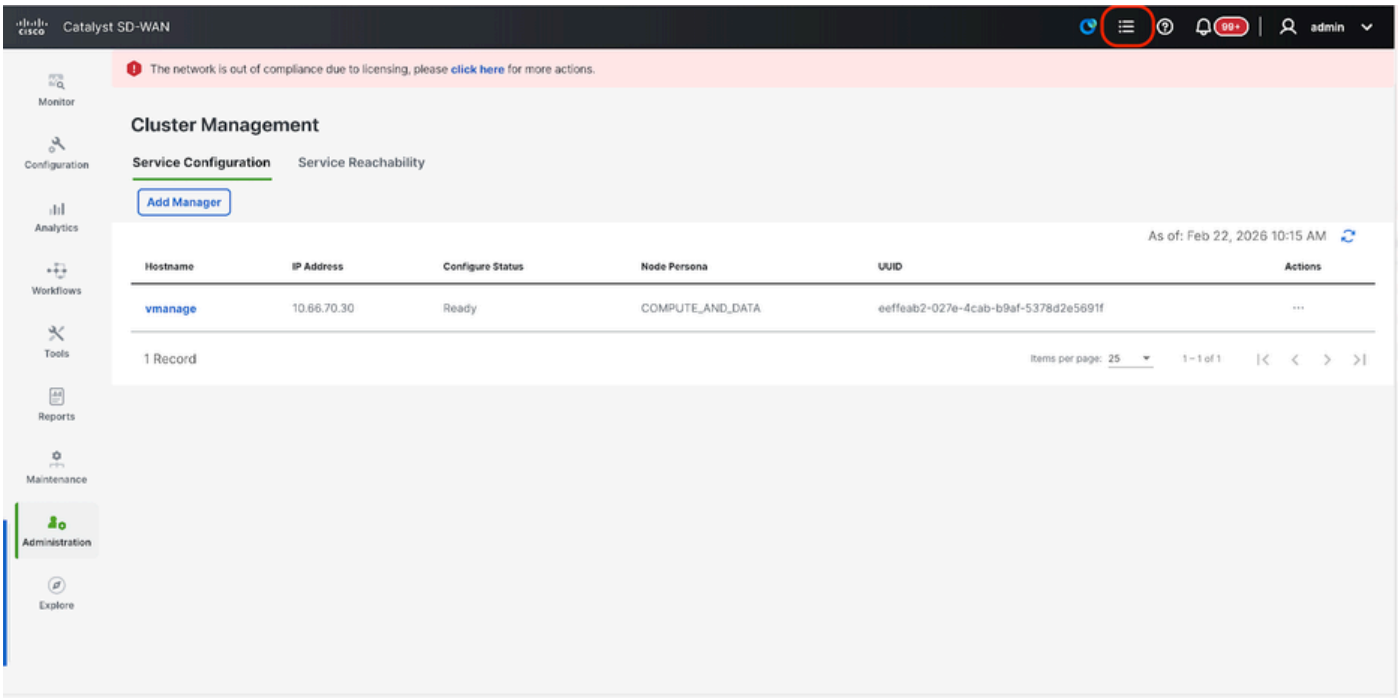
构建vManage集群

- 在vManage-1的WebUI上，导航到Administration > Cluster Management，在Service Configuration部分，
- 单击Add Manager，将出现一个弹出窗口：





- 根据在vManage - 2节点旋转时完成的角色配置选择节点角色。
- 在Manager IP address下输入vManage-2的服务接口IP
- 输入用户名和密码，该凭证与我们在步骤6中使用的凭证相同。
- 启用SDAVC — 保持未选中状态，因为我们本可以在vManage-1上启用它
- 点击Add。
- 之后，vManage 1和2节点的vManage NMS服务在后台重新启动。对于vManage 1和2,UI在大约5至10分钟的时间内不可用。
- 在此期间，vManage 1和2的CLI访问可用。
- 可以访问vManage-1 UI后，导航到Administration > Cluster Management，确保两个vManage的服务接口IP都反映在IP地址下，Configure Status is Ready，并且节点角色正确反映。
- 切换至同一页面中的“服务可达性”部分，并确保两个vManage节点的所有服务均可访问。
- 如果我们发现任何服务尚未到达，请稍候。通常需要5到10分钟。
- 您可以在vManage UI右上角可用的任务列表中检查集群添加进程的状态。



- 您可以查找“活动”任务列表，如果该任务仍列在“活动”任务列表下，则表明该任务尚未完成。
- 您可以单击任务来检查相同任务的进度。如果该任务未列在“活动任务”列表下，请切换到“已完成”，并确保任务成功完成。
- 只有在验证这些点后，才能继续下一步。

在将下一个节点添加到集群之前，需要考虑以下几点:

请验证到目前为止已添加到集群的vManage节点的所有UI上的以下点：

- 导航到Monitor > Overview of vManage UI，确保正确反映了vManage节点的数量，且根据添加到集群的节点数量可以看到。

- 导航到Administration > Cluster Management，并确保两个vManage的服务接口IP均反映在IP地址下，Configure Status is Ready且节点角色正确反映。
- 切换到同一页中的“服务可接通性”部分，并确保两个vManage节点的所有服务均可访问。

- 每次向集群中添加节点时，集群中所有节点的NMS服务都会重新启动，因此在一段时间内，所有这些节点的UI都变得不可达。
- 根据群集中的节点数量，可能需要较长的时间才能备份UI和访问所有服务。
- 您可以在vManage UI右上角的Task-list下监控任务。
- 在添加到集群的每个节点的vManage UI上，我们需要查看所有路由器、模板和策略（如果它们在vManage-1中可用）。
- 如果这些配置不存在于vManage-1上，则添加到vManage-1中的vBonds和vSmarts以及组织 — 名称、vBond、证书授权的Administration > Settings配置必须反映在添加到集群的其他vManage节点上。
- 对其余vManage节点重复相同步骤。

步骤 4：冷备用DR集群设置

冷备用DR集群设置

您可以使用第4步中介绍的步骤启动一个或多个vManage集群：构建vManage集群。完成步骤6中所述的步骤的开机自检：Config-db Backup/Restore，恢复备用群集中的config-db备份。

步骤 5：Config-db备份/恢复

在另一个vManage节点上收集vManage configuration-db备份和恢复

收集Configuration-DB备份：

- 在当前正在使用的SD-WAN交换矩阵中，可以从vManage集群生成configuration-db备份。
- 请注意，我们只能在vManage群集的其中一个节点（即configuration-db领导者）上生成configuration-db backup。

- 对于独立vManage，该vManage本身是配置数据库领导者。
- 在vManage集群中，使用命令request nms configuration-db diagnostics确定configuration-db领导节点。您可以在3节点vManage集群的所有节点上运行此命令。
- 在6节点集群中，请确保在启用了configuration-db的vManage节点上运行此命令以标识领导节点。 导航到管理>集群管理以验证相同内容：
- 如屏幕截图所示，配置了persona COMPUTE_AND_DATA的节点正在运行configuration-db。

您可以在vManageCLI上使用requestnmsconfiguration-dbstatus命令验证相同。输出如下所示

```
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#
```

- 执行命令后，在这些节点上请求nms configuration-db diagnostics，输出如下所示：
- 查找“IsLeader”的突出显示的字段。如果设置为1，则表明节点是领导节点，我们可以从中收集configuration-db备份。

```
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     .
```

使用此命令从已确定的configuration-db领导vManage节点收集configuration-db备份。

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

预期输出如下所示：

```
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凭证，请记下该凭证。
- 如果您不知道配置数据库凭证，请联系TAC从现有vManage节点检索配置数据库凭证。
- 默认的configuration-db凭证是用户名：neo4j和密码：密码

将Configuration-db备份恢复到另一个vManage节点

使用SCP将configuration-db备份复制到vManage的/home/admin/目录。

scp命令输出示例：

```
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
```

要恢复configuration-db备份，首先需要配置configuration-db凭据。如果您的配置数据库凭证是默认凭证(neo4j/password)，我们可以跳过此步骤。

要配置configuration-db凭据，请使用命令request nms configuration-db update-admin-user。使用您选择的用户名和密码。

请注意，vManage的应用服务器已重新启动。由于此vManage UI在短时间内变得不可访问。

```
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#
```

发布后，我们可以继续恢复configuration-db备份：

我们可以使用命令request nms configuration-db restore path /home/admin/< >将配置数据库恢复到新的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
```

恢复configuration-db后，请确保vManage UI可访问。等待约5分钟，然后尝试访问UI。

成功登录UI后，请确保边缘路由器列表、模板、策略以及之前或现有vManage UI上存在的所有其余配置都反映在新的vManage UI上。

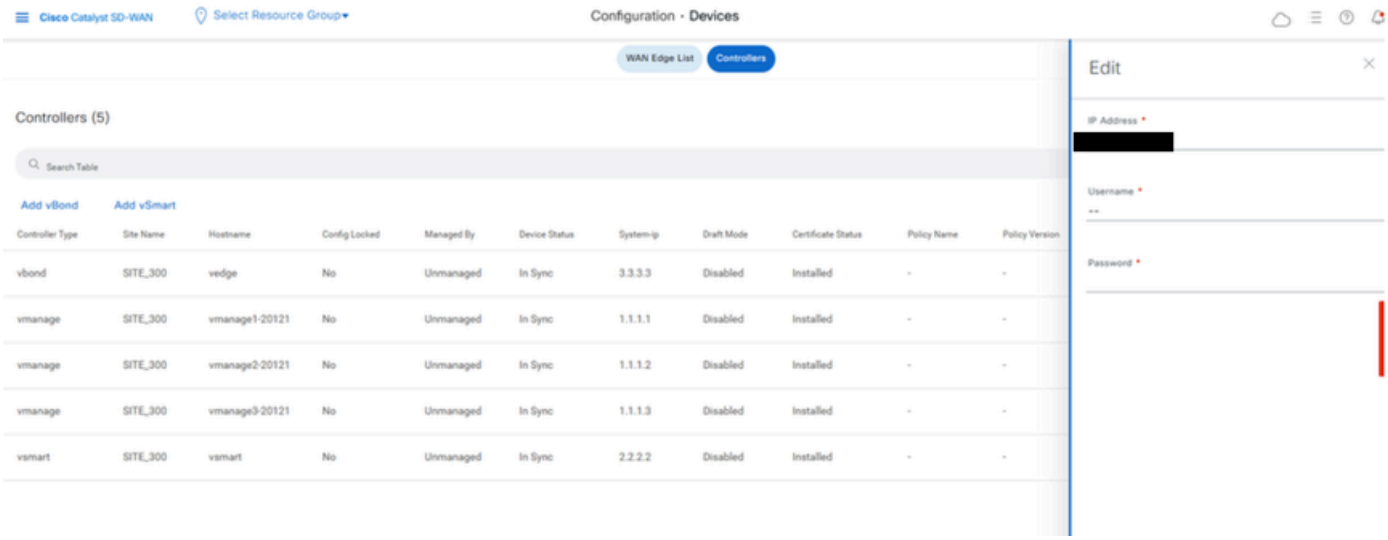
步骤 6：控制器重新验证和旧控制器失效

恢复configuration-db后，我们需要重新验证交换矩阵中的所有新控制器(vmanage/vsmart/vbond)

注：在实际生产中，如果用于重新身份验证的接口IP是隧道接口IP，则需要确保在vManage、vSmart和vBond的隧道接口以及路径沿途的防火墙上允许NETCONF服务。要打开的防火墙端口是从DR群集到所有vBonds和vSmarts的双向规则的TCP端口830。

在vmanage UI上，点击Configuration > Devices > Controllers

- 点击每个控制器附近的三个点，然后点击Edit



- 将ip-address（控制器的系统ip）替换为transport vpn 0（隧道接口）ip地址。输入用户名和密码，然后点击save
- 对交换矩阵中的所有新控制器执行相同操作

同步根证书链

所有控制器入网后，请完成以下步骤：

在新活动集群中的任何Cisco SD-WAN Manager服务器上，执行以下操作：

输入以下命令将根证书与新活动集群中的所有Cisco Catalyst SD-WAN设备同步：

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

输入以下命令将Cisco SD-WAN Manager UUID与Cisco SD-WAN Validator同步：

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

一旦交换矩阵恢复，并且交换矩阵中的所有边缘和控制器的控制和bfd会话都已启动，我们就需要从UI使旧控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，点击Configuration > Devices > Certificates
- 点击“控制器”
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击invalidate（失效）
- 点击send to vbond
- 在vmanage UI上，点击Configuration > Devices > Controllers
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击Delete

步骤 7：过帐检查

注意：继续此处所示的“后检查”部分，它适用于所有部署组合。

组合5:vManage Cluster + DR已启用

所需实例：

- 3或6个vManage（主集群）
- 3或6个vManage（DR备用集群）
- 1个或多个vBond（分布于主数据中心和DR数据中心）
- 1个或多个vSmart（分布于主数据中心和DR数据中心）

步骤:

1. 使用通用步骤启动所有实例
2. 预检查
3. 配置vManage UI、证书和板载控制器
4. 构建vManage集群
5. 冷备用DR集群设置
6. Config-db备份/恢复
7. 过帐检查

步骤 1：预检查

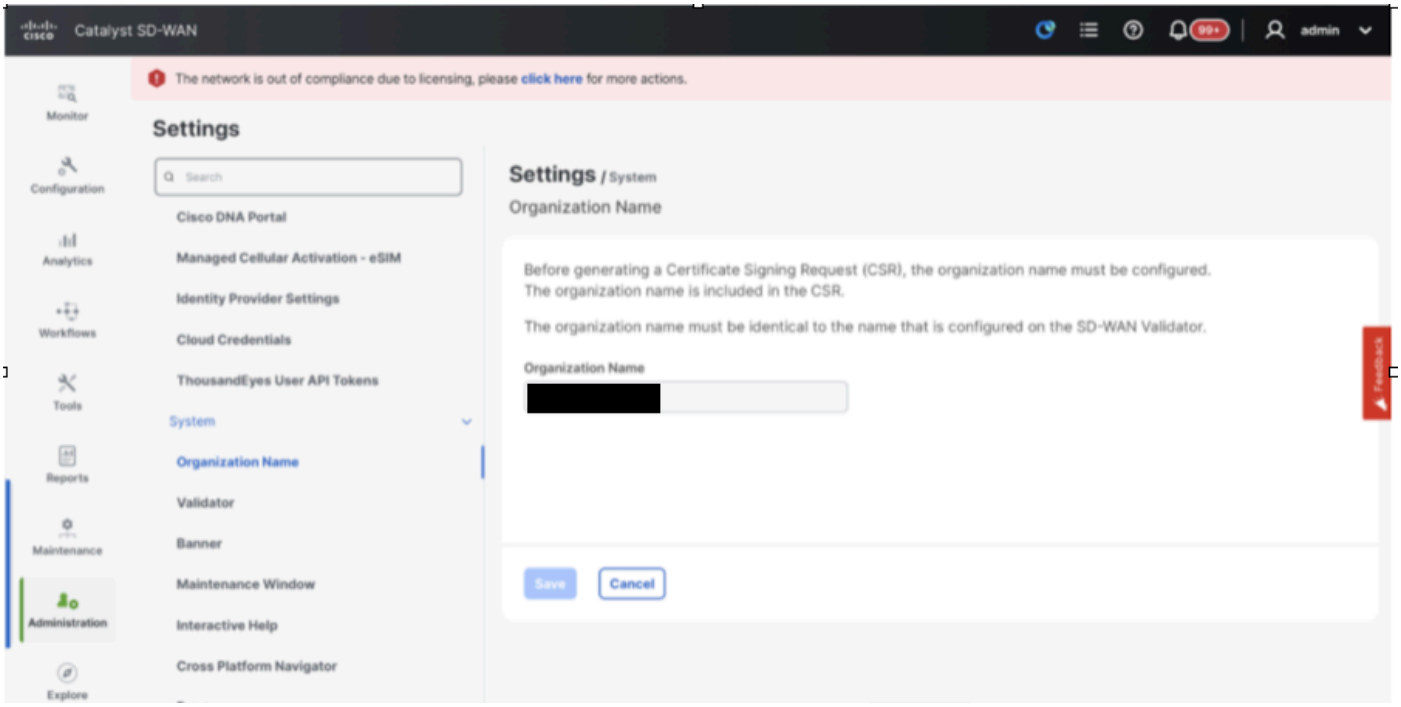
- 确保活动的Cisco SD-WAN Manager实例数与新安装的Cisco SD-WAN Manager实例数相同。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例都运行相同的软件版本。
- 确保所有活动实例和新的Cisco SD-WAN Manager实例能够到达Cisco SD-WAN Validator的管理IP地址。
- 确保证书已安装在新安装的Cisco SD-WAN Manager实例上。
- 确保所有Cisco Catalyst SD-WAN设备(包括新安装的Cisco SD-WAN Manager)上的时钟都同步。
- 确保在新安装的Cisco SD-WAN Manager实例上配置一组新的系统IP和站点ID，同时配置与活动集群相同的基本配置。

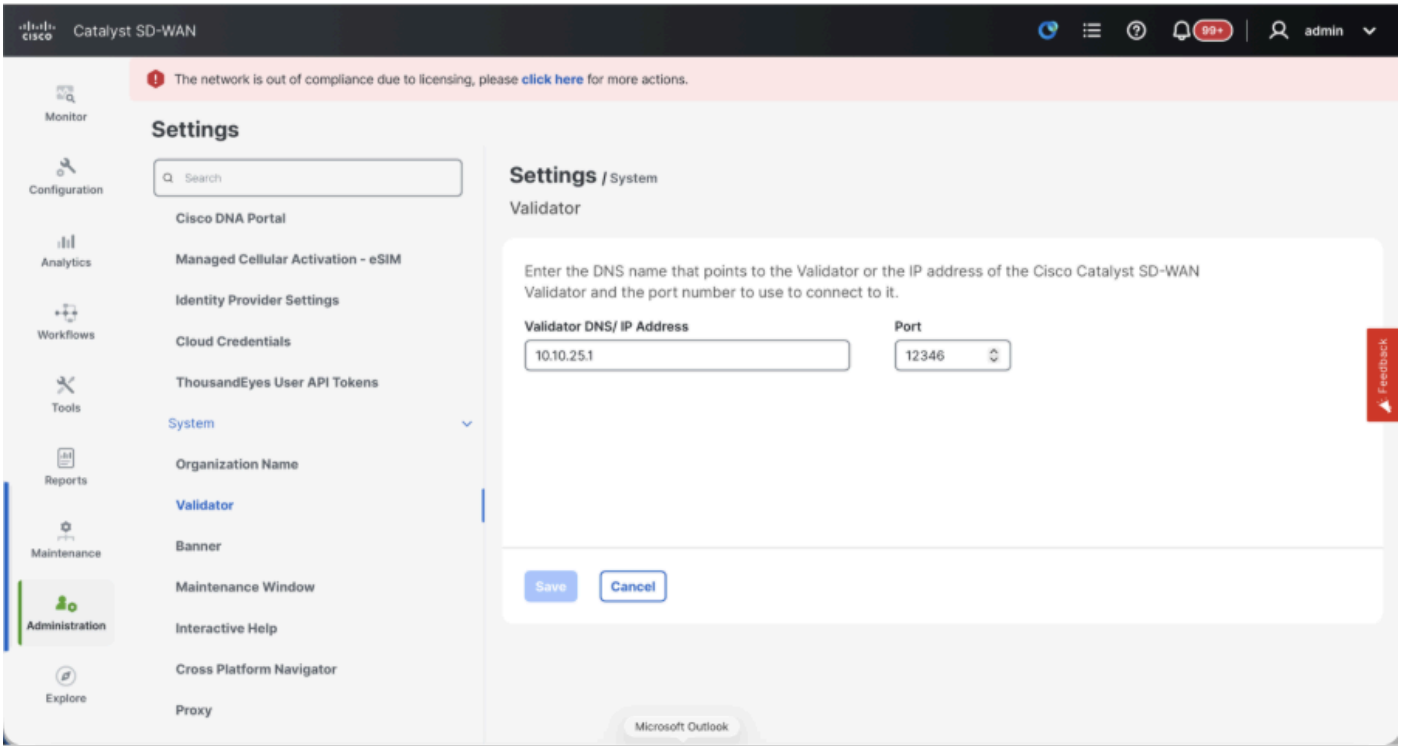
步骤 2：配置vManage UI、证书和板载控制器

更新vManage UI上的配置

- 一旦将步骤1中的配置添加到所有控制器的CLI中，我们就可以使用浏览器中的URL https://<vmanage-ip>访问vManage的WebUI。使用各个vManage节点的VPN 512 IP地址。您可以使用管理员用户名和密码登录。

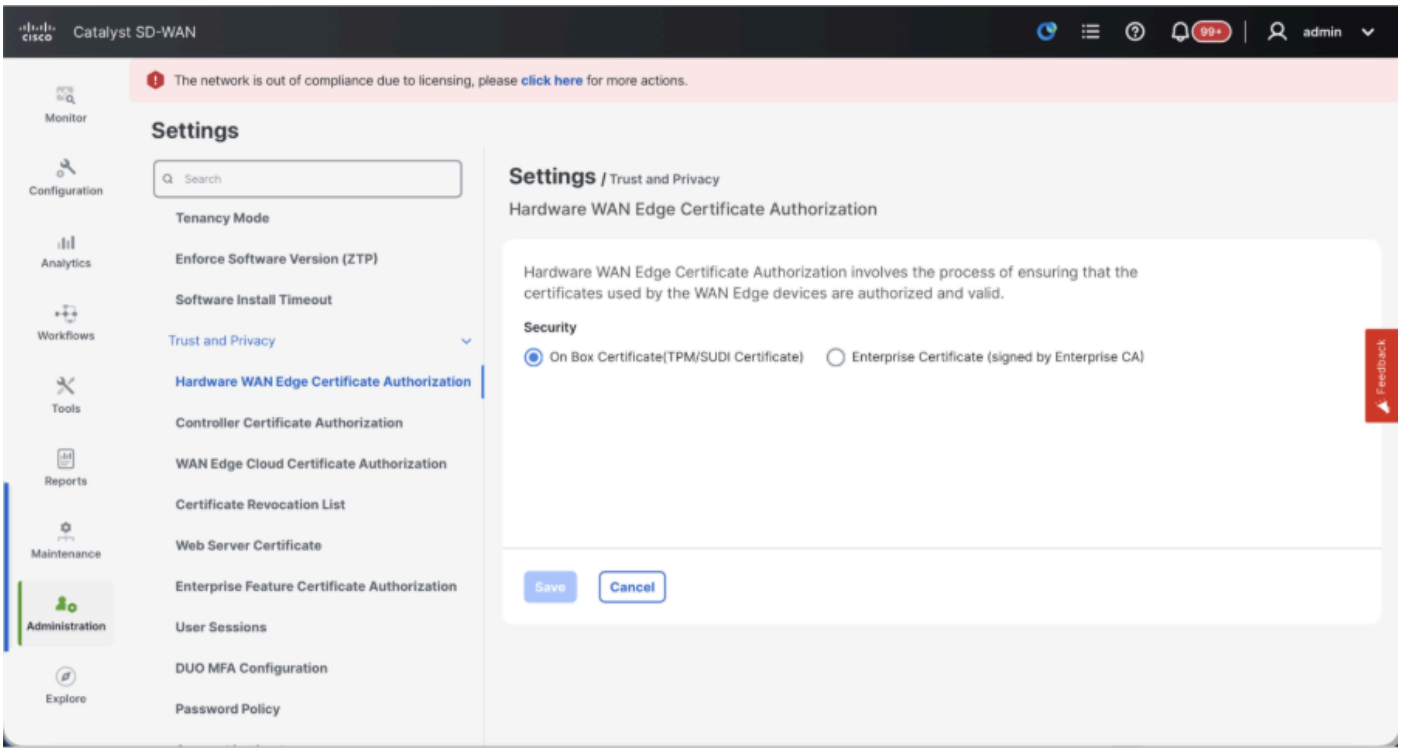
- 导航到管理>设置并完成以下步骤。
- 配置组织名称和验证器/vBond URL/IP地址。配置与vManage节点的CLI中相同的值。
- 在vManage 20.15/20.18中，这些配置在System部分下提供。



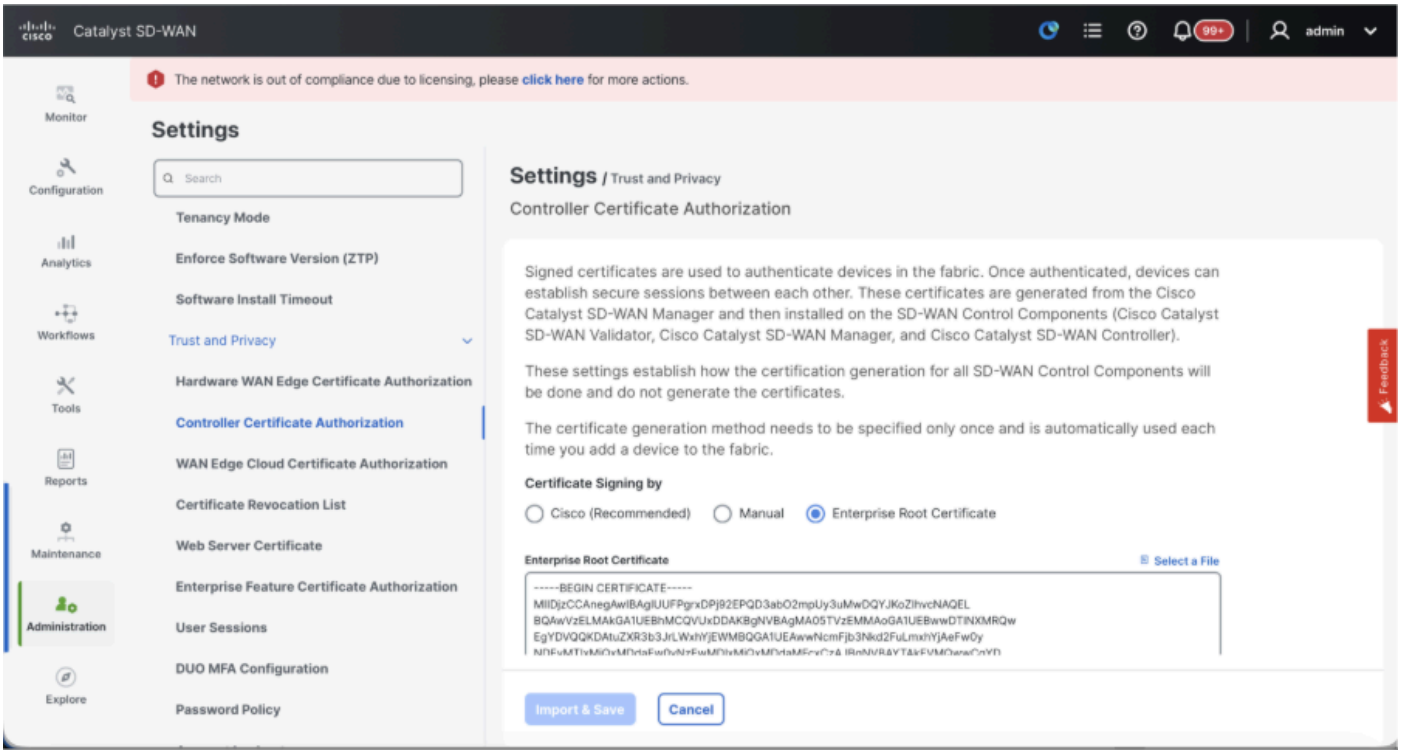


- 验证证书授权(CA)的配置，CA决定用于证书签名的证书颁发机构。我们可以看到3个选项：

1. 硬件WAN边缘证书授权 — 确定硬件SD-WAN边缘路由器的CA。
    - 开箱证书（TPM/SUDI证书）— 使用此选项，路由器硬件上预安装的证书用于建立控制连接（TLS/DTLS连接）
    - 企业证书（由企业CA签署）— 使用此选项时，路由器使用由组织的企业证书颁发机构签署的证书。选择此选项时，必须在此处更新企业CA的根证书。



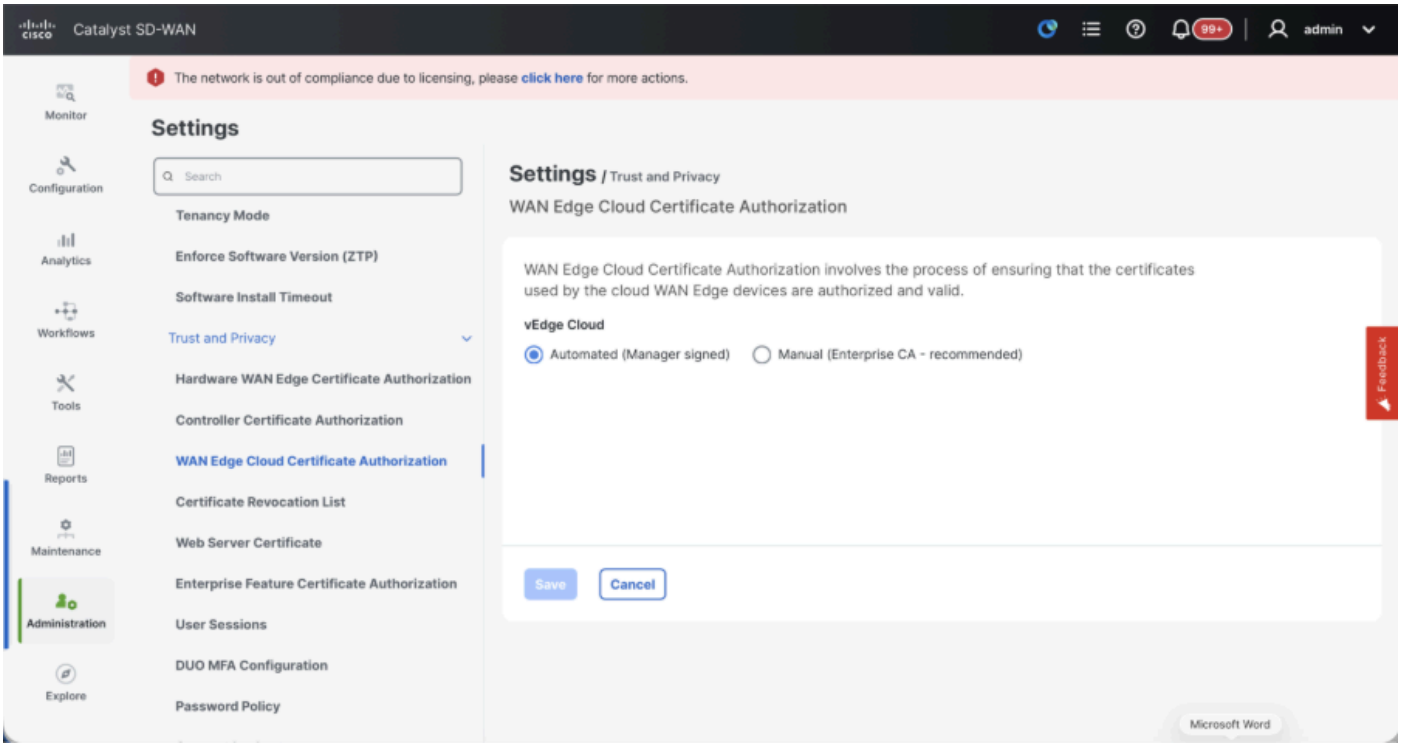
2. 控制器证书授权 — 决定SD-WAN控制器的CA。
   - 思科（推荐） — 控制器使用思科PKI签名的证书。vManage使用vManage上配置的智能帐户凭证自动联系PNP门户，并获取证书签名并安装在控制器上。
   - 手动 — 控制器使用由Cisco PKI签名的证书。使用思科PNP门户手动签署CSR，方法是导航到相应SD-WAN重叠的智能帐户和虚拟帐户。
   - 企业根证书 — 通过此选项，路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。



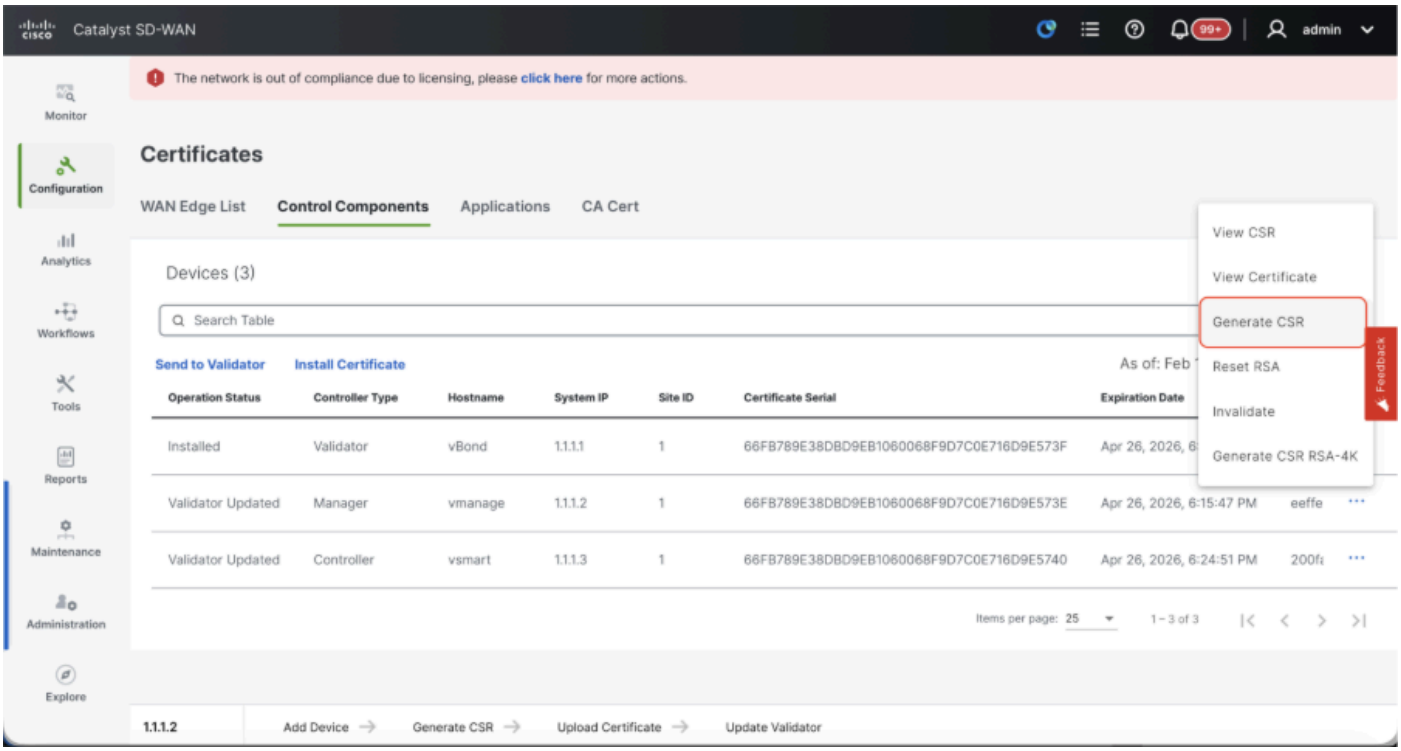
3. 广域网边缘云证书授权 — 确定虚拟SD — 广域网边缘路由器（CSR1000v、C8000v、vEdge云）的CA

- 自动（vManage签名）— vManage自动为虚拟边缘路由器签署CSR并在路由器上安装证书。
- 手动（企业CA — 推荐）— 虚拟路由器使用由组织的企业证书颁发机构签名的证书。选择此选项时，必须在此处更新企业CA的根证书。

例如，如果我们使用自己的CA（企业证书颁发机构），请选择Enterprise。



- 如果是20.15/20.18 vManage节点，请导航到配置>证书>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers
- 为Manager/vManage点击……，然后点击Generate CSR。



- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。

将vBond/Validator和vSmart/Controller注册到vManage

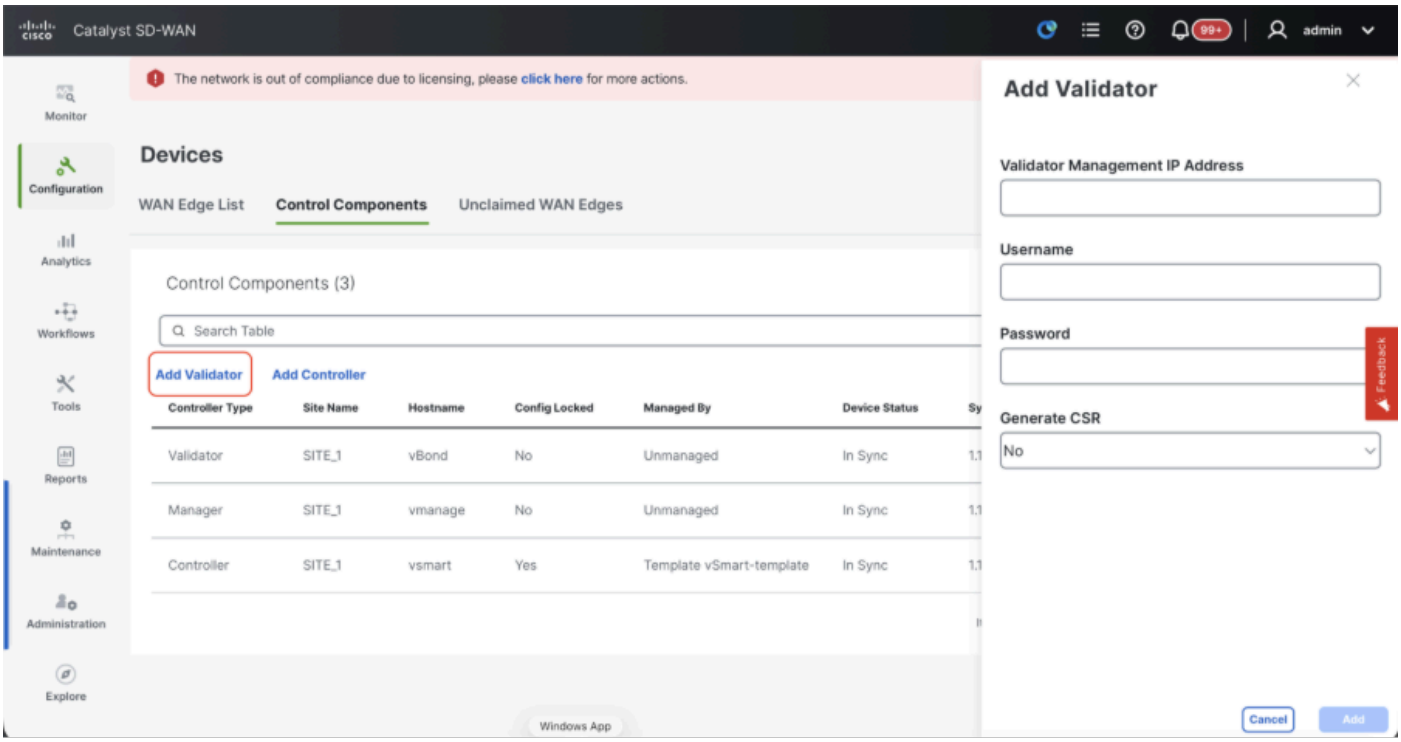
如果是20.15/20.18 vManage节点，请导航到配置>设备>控制组件。对于20.9/20.12版本，Configuration > Devices > Controllers

OnboardingvBond/验证器

- 单击AddvBond对于20.12vManageor的情况添加验证程序20.15/20.18vManage。系统打开一个弹出窗口，输入 vBond的VPN 0传输IP，可从vManage访问。
- 如果允许，请从vManagetovBondIP的CLI使用ping检查可接通性。
- 输入vBond的用户凭证。

注意：我们需要将vBondor的管理凭据用作netadmingroup的用户部分。您可以在vBond的CLI中验证这一点。如果我们需要为vBond安装新证书，请在“生成CSR”的下拉列表中选择是

注意：如果vBond位于NAT设备/防火墙之后，请检查vBond VPN 0接口IP是否已转换为公共IP。如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口的公用IP地址

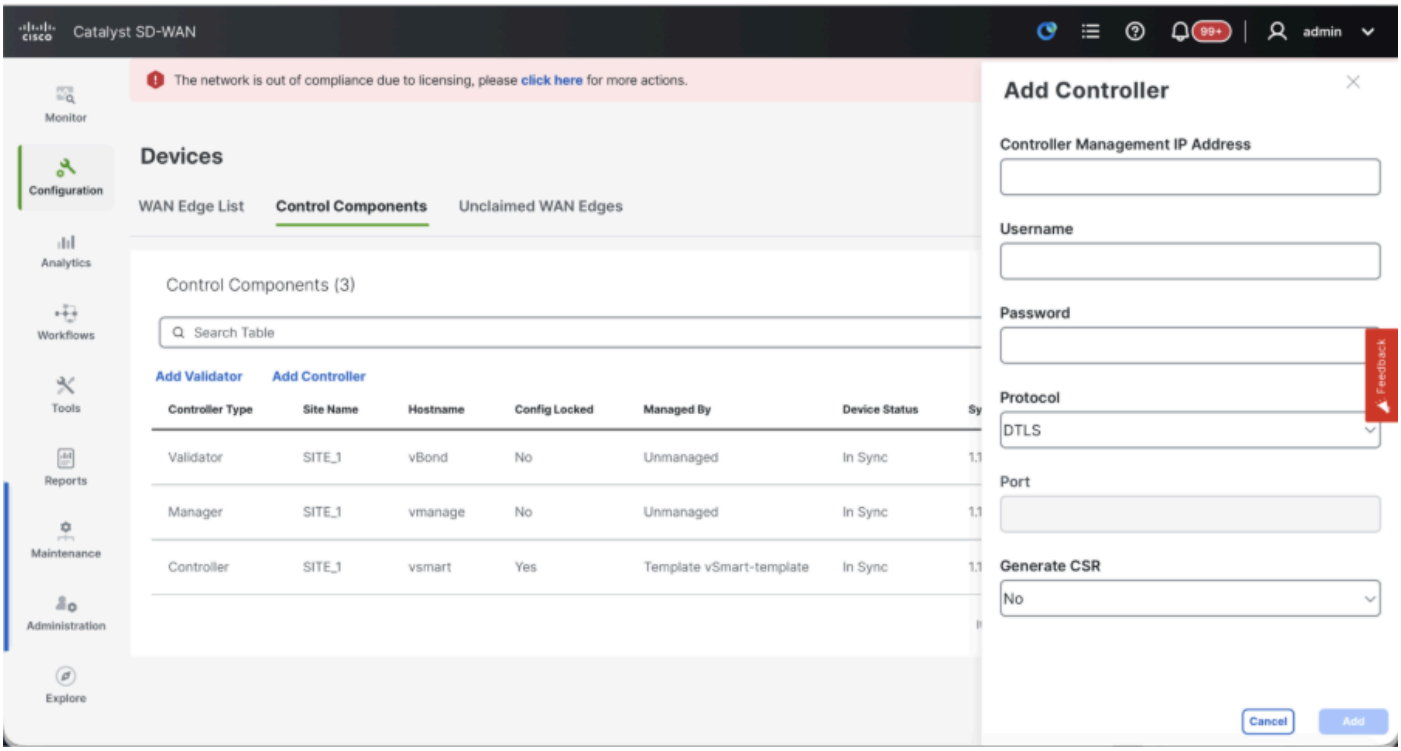


- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vBond上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 如果有多个vBonds，请重复相同的步骤。

自注册vSmart/控制器：

- 在20.12 vManage中点击Add vSmart，在20.15/20.18 vManage中点击Add Controller。
- 系统打开一个弹出窗口，输入vSmart的VPN 0传输IP，可从vManage访问。
- 如果允许从vManage的CLI到vSmart IP，请使用ping检查可达性。
- 输入vSmart Note的用户凭据，我们需要使用vSmart的管理员凭据或netadmin组的用户部分。
- 您可以在vSmart的CLI中验证这一点。
- 如果打算对路由器使用TLS来建立与vSmart的控制连接，请将协议设置为TLS。此配置也需要在vSmarts和vManage节点的CLI上进行配置。
- 如果需要为vSmart安装新证书，请在生成CSR"的下拉列表中选择Yes。

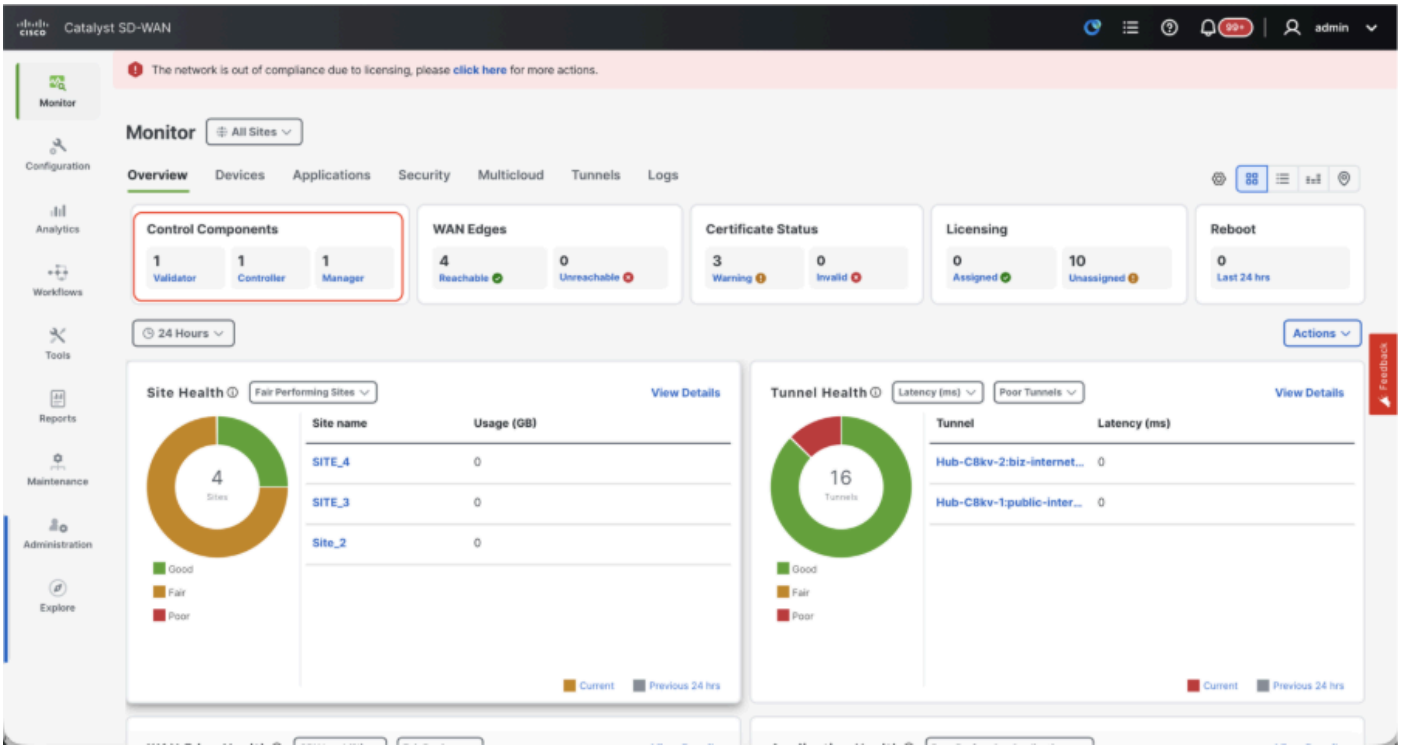
注意：如果vSmart位于NAT设备/防火墙之后，请检查vSmart VPN 0接口IP是否已转换为公共IP，如果无法从vManage访问VPN 0接口IP，请在此步骤中使用VPN 0接口IP的公共IP地址。



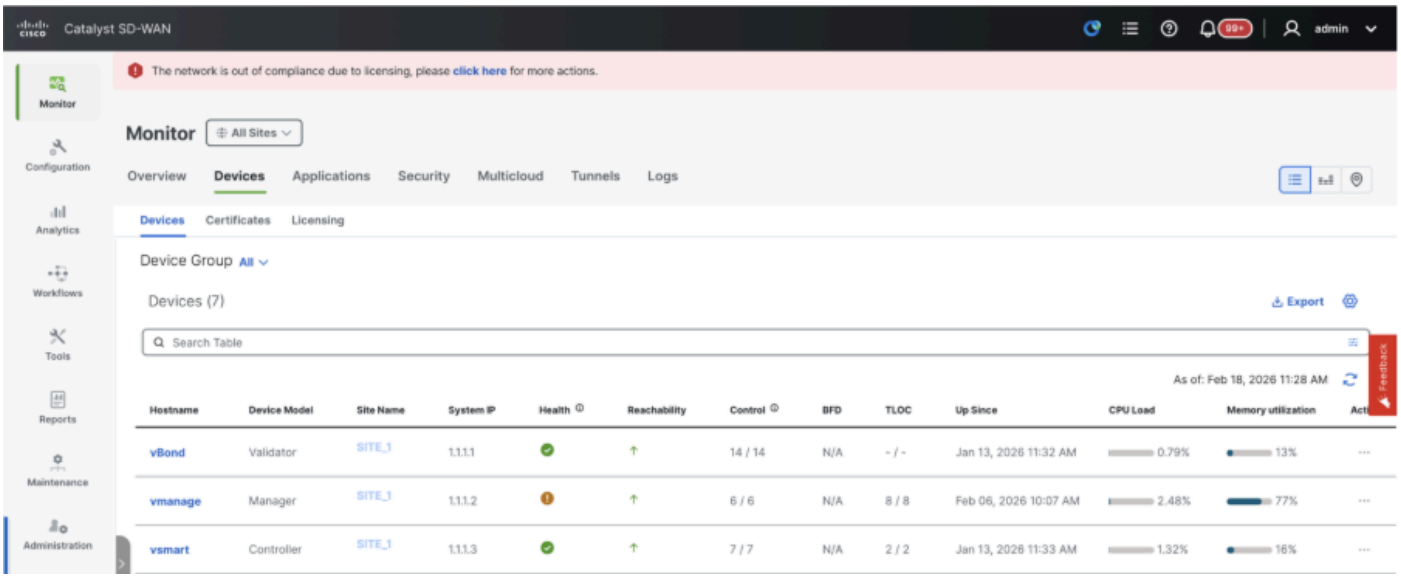
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装在vSmart上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 如果有多个vSmarts，请重复相同的步骤。

确认

完成所有步骤后，在Monitor>Dashboard中确认所有控制组件均可访问



- 单击相应的控制组件，确认它们都可访问。
- 导航到监控>设备，确认所有控制组件均可访问。



步骤 3：构建vManage集群

板载SD-WAN交换矩阵，在SD-WAN重叠中带有vManage集群

注意:vManage集群可以配置3个vManage节点或6个vManage节点，具体取决于注册到SD-WAN交换矩阵的站点数量

通过单个vManage节点加入所有SD-WAN控制器

继续执行“在SD-WAN重叠中带单节点vManage的板载SD-WAN控制器”中共享的步骤，首先启用带一个vManage节点的SD-WAN交换矩阵，然后板载所有所需的验证器(vBond)和控制器(vSmart)。

配置属于集群的所有vManage节点的CLI配置

- 配置vManage节点的其余节点。对于3个节点集群，您有剩余的2个要配置的节点；对于6个节点集群，您有5个要配置的节点。
- 配置系统配置，如下所示：

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注意:如果我们使用URL作为vBond地址，请确保在VPN 0配置中配置DNS服务器IP地址或确保可以解析这些地址。

需要使用这些配置来启用传输接口，该接口用于与路由器和其余控制器建立控制连接。

```
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
```

还要配置VPN 512管理接口以启用对控制器的带外管理访问。

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

```
  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

可选配置：

- 您可以参考现有控制器的配置，如果此处列出的配置存在，您可以将此配置添加到新控制器。
- 仅当路由器需要使用TLS与vManage节点建立安全控制连接时，才将控制协议配置为TLS。默认情况下，所有控制器和路由器都使用DTLS建立控制连接。根据您的要求，此配置是仅在vSmart和vManage节点上必需的可选配置。

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

在所有vManage节点上配置服务接口

在所有vManagenode(包括已注册的vManage-1)上配置服务接口。此接口用于集群通信，即集群中vManagenodes之间的通信。

```
conf t
 interface eth2
  ip address



  no shutdown
commit
```

确保同一IP子网用于vManagecluster中所有节点上的服务接口。

配置集群凭证

我们可以使用与vManagenode相同的管理凭据配置vManagecluster。否则，我们可以配置作为netadmingroup一部分的新用户凭据。配置新用户凭据的配置如下所示

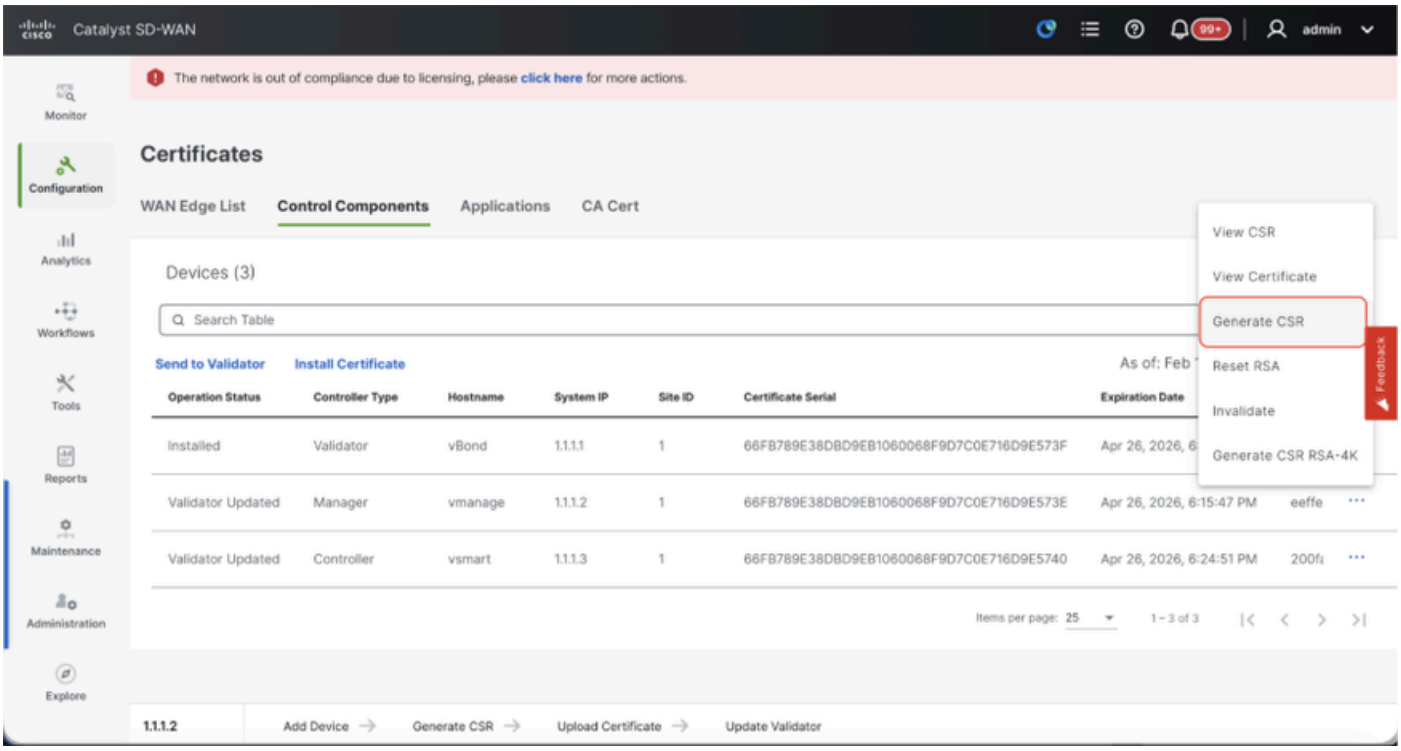
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

确保在属于群集的所有vManagenode上配置相同的用户凭据。如果我们决定使用管理员凭据，则必须在所有vManagenode上配置相同的用户名/密码。

在所有vManage节点上安装设备证书

- 使用浏览器中的URL https://<vmanage-ip>登录所有vManagenode的tovManageUI。使用各个vManagenode的VPN 512 IP地址。您可以使用管理员用户名和密码登录。
- 如果是20.15/20.18 vManage节点，请导航到Configuration > Certificates > Control Components 。对于20.9/20.12版本，Configuration > Devices > Controllers

  单击Manager/vManage的……并单击Generate CSR。



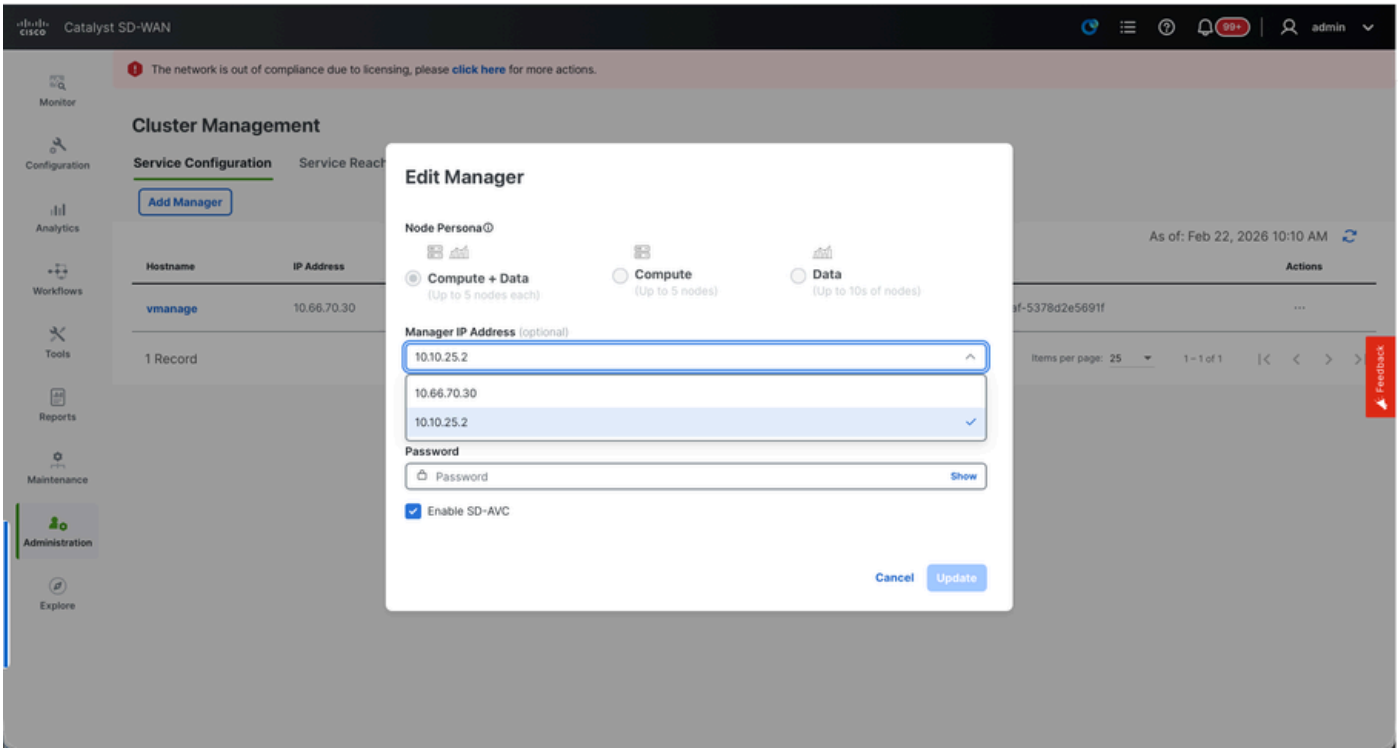
- 生成CSR后，您可以下载CSR并根据为控制器选择的证书颁发机构对其进行签名。您可以在管理>设置>控制器证书授权中验证此配置。如果选择思科（推荐），则vManage会自动将CSR上传到PNP门户，并且证书签名后，会自动将其安装到vManage上。
- 如果选择“手动”，请通过导航到相应SD-WAN重叠的智能帐户和虚拟帐户，使用思科PNP门户手动签署CSR。
- 证书从PNP门户可用后，点击vManage同一部分的安装证书，然后上传证书并安装证书。
- 如果我们使用Digicert和Enterprise Root Certificate，则适用相同的步骤。
- 跨属于集群的所有vManage节点完成此步骤。

准备构建vManage集群

- 在vManage-1的WebUI上，导航到Administration > Cluster Management，在vManage-1的Actions下点击……，选择Edit。
- 系统会根据在VM启动时选择的角色自动选择节点角色。

注意：对于有3个节点的集群，所有3个vManage节点都以计算+数据作为角色。对于6节点集群，3个vManage节点采用计算+数据作为角色，3个vManage节点采用数据作为角色。

- 从Manager IP地址下拉列表中，确保选择vManage的服务接口IP。



- 输入用于启用vManage集群（称为集群凭证）所需的用户名和密码。
- 如前所述，必须在所有vManage节点上配置相同的凭证，并且必须在将所有节点添加到集群时使用。

可选配置：

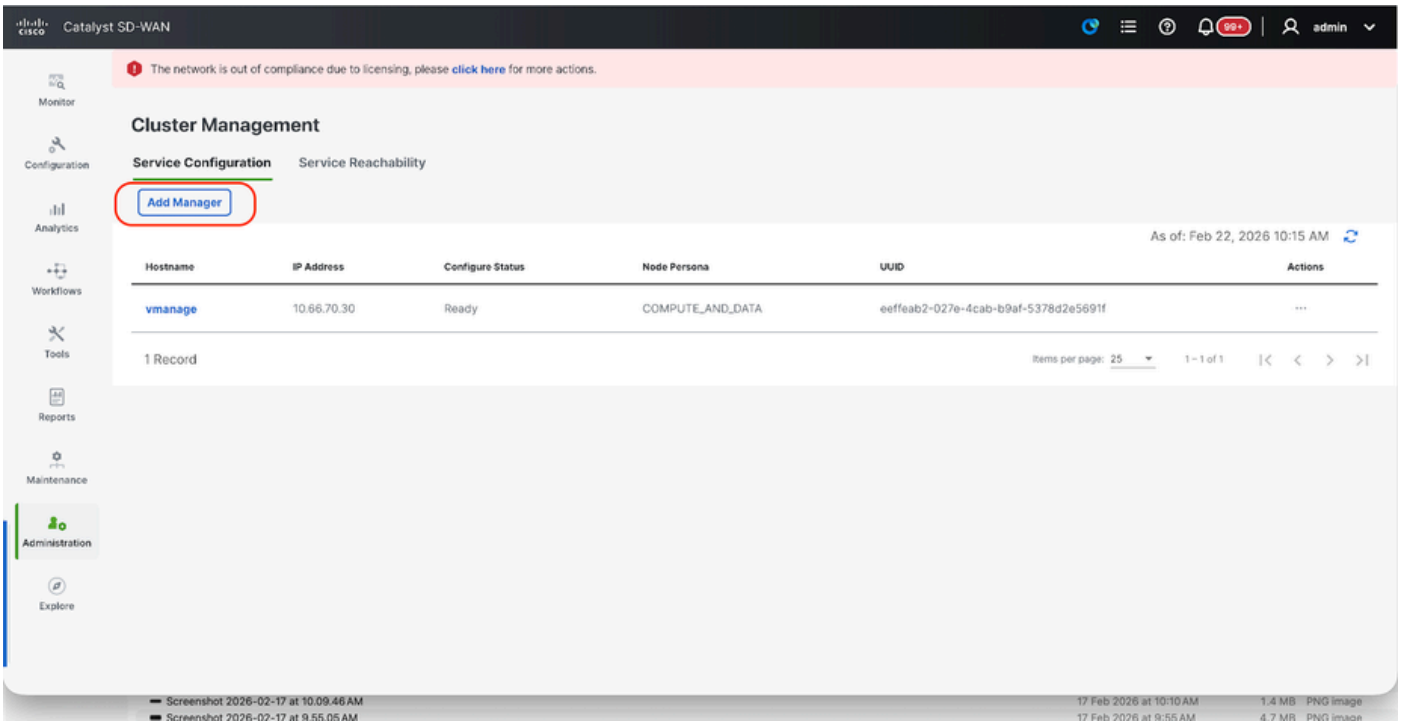
请参阅现有集群中的此配置以启用SDAVC — 仅当需要且仅在集群的一个vManage节点上需要时，才需要选中。

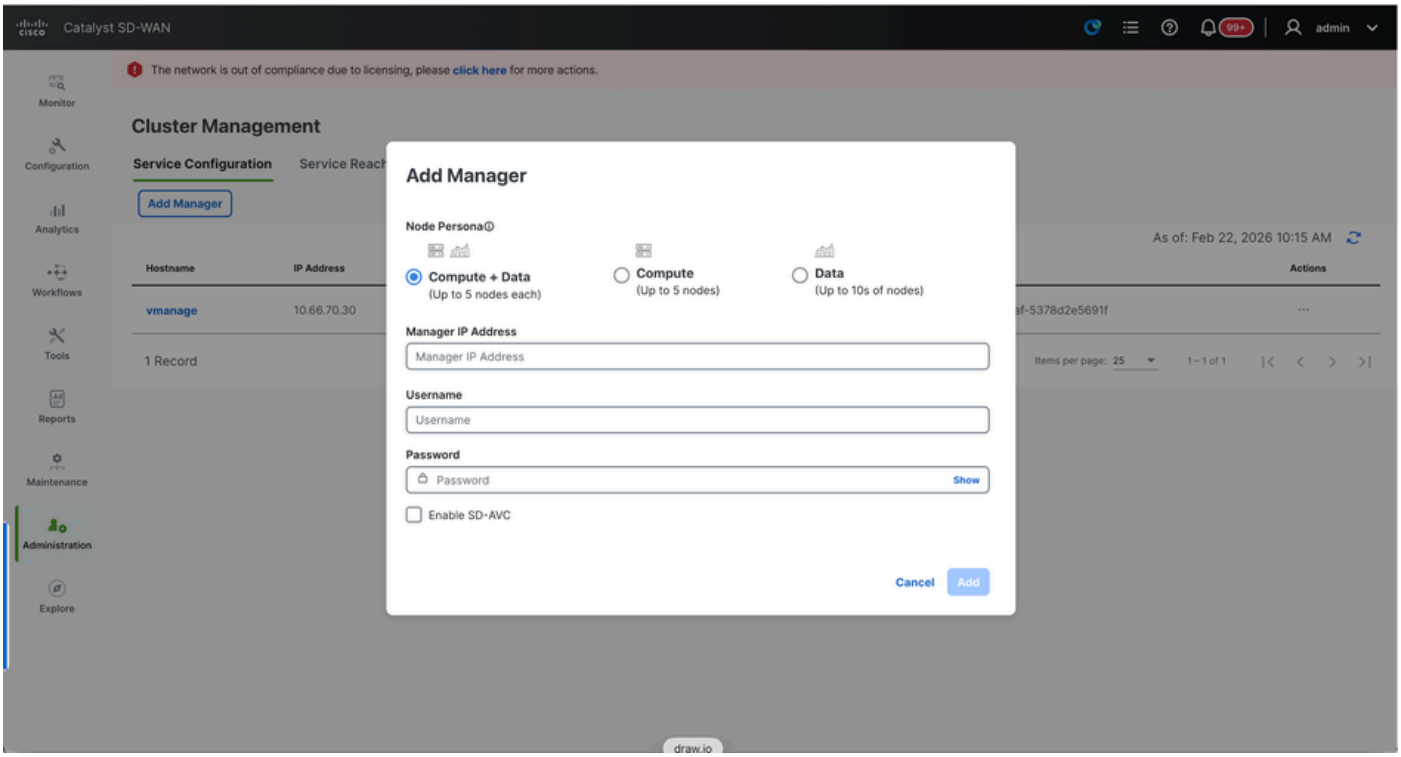
点击Update。

- 之后，vManage NMS服务在后台重新启动，UI在大约5至10分钟的几分钟内不可用。在此期间，vManage的CLI访问可用。
- 可以访问vManage-1 UI后，导航到Administration > Cluster Management，确保vManage的服务接口IP反映在IP地址下，Configure Status is Ready，节点角色正确反映。在同一页切换到Service Reachability部分，并确保所有服务均可访问。
- 如果我们发现任何服务尚未到达，请稍候。通常需要20到30分钟。

构建vManage集群

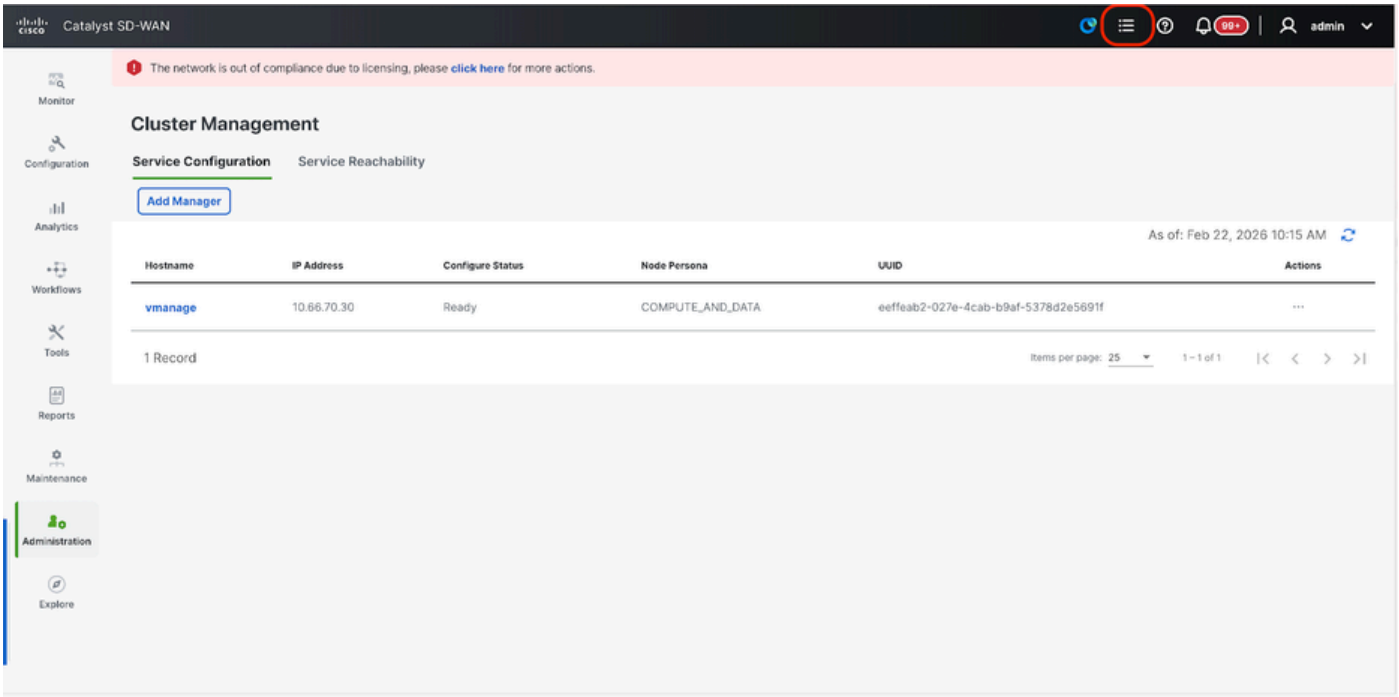
- 在vManage-1的WebUI上，导航到Administration > Cluster Management，在Service Configuration部分，
- 单击Add Manager，将出现一个弹出窗口：





- 根据在vManage - 2节点旋转时完成的角色配置选择节点角色。
- 在Manager IP address下输入vManage-2的服务接口IP
- 输入用户名和密码，该凭证与我们在步骤6中使用的凭证相同。
- 启用SDAVC — 保持未选中状态，因为我们本可以在vManage-1上启用它
- 点击Add。
- 之后，vManage 1和2节点的vManage NMS服务在后台重新启动。对于vManage 1和2,UI在大约5至10分钟的时间内不可用。
- 在此期间，vManage 1和2的CLI访问可用。
- 可以访问vManage-1 UI后，导航到Administration > Cluster Management，确保两个vManage的服务接口IP都反映在IP地址下，Configure Status is Ready，并且节点角色正确反

映。
- 切换至同一页面中的“服务可达性”部分，并确保两个vManage节点的所有服务均可访问。
- 如果我们发现任何服务尚未到达，请稍候。通常需要5到10分钟。
- 您可以在vManage UI右上角可用的任务列表中检查集群添加进程的状态。



- 您可以查找“活动”任务列表，如果该任务仍列在“活动”任务列表下，则表明该任务尚未完成。
- 您可以单击任务来检查相同任务的进度。如果该任务未列在“活动任务”列表下，请切换到“已完成”，并确保任务成功完成。
- 只有在验证这些点后，才能继续下一步。

在将下一个节点添加到集群之前，需要考虑以下几点:

请验证到目前为止已添加到集群的vManage节点的所有UI上的以下点：

- 导航到Monitor > Overview of vManage UI，确保正确反映了vManage节点的数量，且根据添加到集群的节点数量可以看到。

- 导航到Administration > Cluster Management，并确保两个vManage的服务接口IP均反映在IP地址下，Configure Status is Ready且节点角色正确反映。
- 切换到同一页中的“服务可接通性”部分，并确保两个vManage节点的所有服务均可访问。

- 每次向集群中添加节点时，集群中所有节点的NMS服务都会重新启动，因此在一段时间内，所有这些节点的UI都变得不可达。
- 根据群集中的节点数量，可能需要较长的时间才能备份UI和访问所有服务。
- 您可以在vManage UI右上角的Task-list下监控任务。
- 在添加到集群的每个节点的vManage UI上，我们需要查看所有路由器、模板和策略（如果它们在vManage-1中可用）。
- 如果这些配置不存在于vManage-1上，则添加到vManage-1中的vBonds和vSmarts以及组织 — 名称、vBond、证书授权的Administration > Settings配置必须反映在添加到集群的其他vManage节点上。

- 对其余vManage节点重复相同步骤。

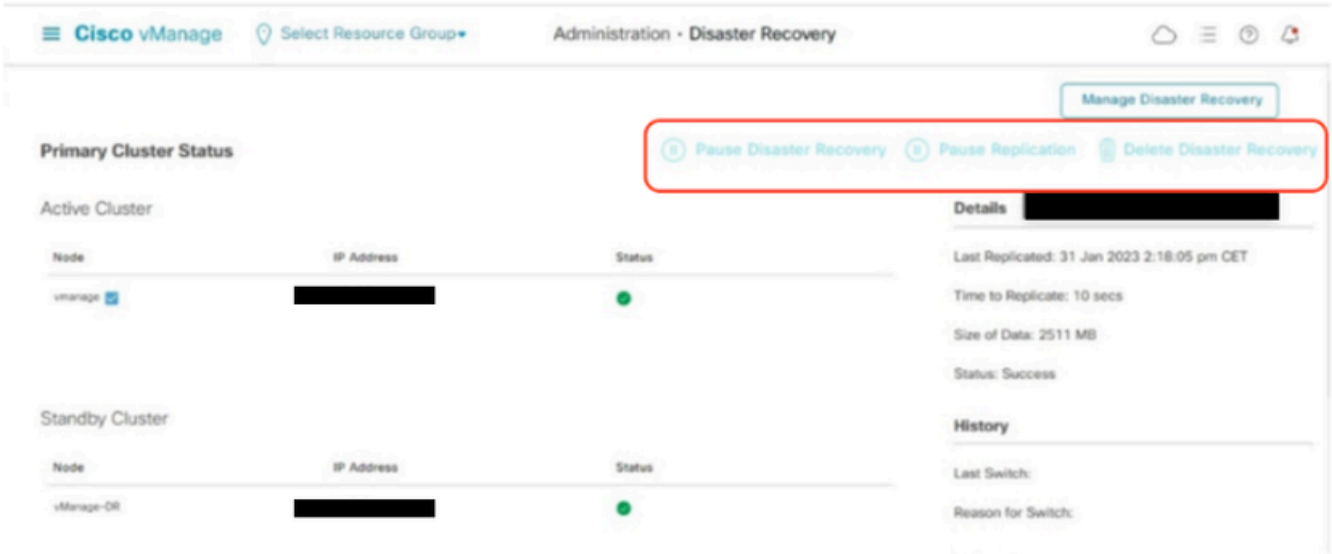
步骤 4：Config-db备份/恢复

在另一个vManage节点上收集vManage configuration-db备份和恢复

注意：从已启用灾难恢复的现有vManage群集收集配置数据库备份时，请确保在该节点上的灾难恢复暂停并删除后收集配置数据库备份。

确认没有正在进行的灾难恢复复制。导航到管理>灾难恢复和 确保状态为Success且未处于Import Pending、Export Pending或Download Pending等暂时状态。如果状态未成功，请联系Cisco TAC并确保复制成功，然后继续暂停灾难恢复。

首先暂停灾难恢复并确保任务完成。然后删除灾难恢复并确认任务已完成。



联系思科TAC以确保成功清理灾难恢复。

收集Configuration-DB备份：

- 在当前正在使用的SD-WAN交换矩阵中，可以从vManage集群生成configuration-db备份。
- 请注意，我们只能在vManage群集的其中一个节点（即configuration-db领导者）上生成configuration-db backup。

- 对于独立vManage，该vManage本身是配置数据库领导者。
- 在vManage集群中，使用命令request nms configuration-db diagnostics确定configuration-db领导节点。您可以在3节点vManage集群的所有节点上运行此命令。
- 在6节点集群中，请确保在启用了configuration-db的vManage节点上运行此命令以标识领导节点。 导航到管理>集群管理以验证相同内容：
- 如屏幕截图所示，配置了persona COMPUTE_AND_DATA的节点正在运行configuration-db。

您可以在vManageCLI上使用requestnmsconfiguration-dbstatus命令验证相同。输出如下所示

```
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#
```

- 执行命令后，在这些节点上请求nms configuration-db diagnostics，输出如下所示：
- 查找“IsLeader”的突出显示的字段。如果设置为1，则表明节点是领导节点，我们可以从中收集configuration-db备份。

```
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     .
```

使用此命令从已确定的configuration-db领导vManage节点收集configuration-db备份。

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

预期输出如下所示：

```
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凭证，请记下该凭证。
- 如果您不知道配置数据库凭证，请联系TAC从现有vManage节点检索配置数据库凭证。
- 默认的configuration-db凭证是用户名：neo4j和密码：密码

将Configuration-db备份恢复到另一个vManage节点

使用SCP将configuration-db备份复制到vManage的/home/admin/目录。

scp命令输出示例：

```
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
```

要恢复configuration-db备份，首先需要配置configuration-db凭据。如果您的配置数据库凭证是默认凭证(neo4j/password)，我们可以跳过此步骤。

要配置configuration-db凭据，请使用命令request nms configuration-db update-admin-user。使用您选择的用户名和密码。

请注意，vManage的应用服务器已重新启动。由于此vManage UI在短时间内变得不可访问。

```
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#
```

发布后，我们可以继续恢复configuration-db备份：

我们可以使用命令request nms configuration-db restore path /home/admin/< >将配置数据库恢复到新的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
```

恢复configuration-db后，请确保vManage UI可访问。等待约5分钟，然后尝试访问UI。

成功登录UI后，请确保边缘路由器列表、模板、策略以及之前或现有vManage UI上存在的所有其余配置都反映在新的vManage UI上。

步骤 5：在vManage群集上启用灾难恢复

重要预检查

两个单独的vManage 3节点群集必须配置且运行正常，才能继续进行灾难恢复。在活动群集上，必须注册验证器和控制器。如果您在DR站点上有验证器和控制器，则这些控制器也必须在活动群集上而不是在DR vManage群集上入网。

Cisco建议在注册灾难恢复之前必须满足以下要求：

- 确保在传输VPN(VPN 0)上通过HTTPS可以访问主节点和辅助节点。
- 确保辅助设置中的思科vSmart控制器和思科vBond协调器连接到主设置。
- 确保Cisco vManage主节点和辅助节点运行相同的Cisco vManage版本。
- VPN 0中的带外集群接口（服务接口）。
- 对于集群中的每个vManage实例，除用于VPN 0（传输）和VPN 512（管理）的接口外，还需要第三个接口（集群链路）。
- 此接口用于集群内的vManage服务器之间的通信和同步。
- 此接口必须至少为1 Gbps，并且延迟为4毫秒或更短。建议使用10 Gbps接口。
- 两个vManage节点必须能够通过此接口相互连接：无论是第2层网段还是通过第3层路由。
- 在每个vManage中，必须在GUI中将此接口配置为集群接口(Administration > Cluster Management — 指示自己的带外集群接口IP地址、用户和密码)。
- 要允许Cisco vManage节点在数据中心之间相互通信，请在数据中心防火墙上启用TCP端口8443和830。

- 确保在两个Cisco vManage节点上启用所有服务（应用服务器、配置数据库、消息服务器、协调服务器和统计数据库）。
- 跨主要和辅助数据中心分发所有控制器，包括思科vBond协调器。确保分布在这些数据中心中的Cisco vManage节点可以访问这些控制器。控制器仅连接到主Cisco vManage节点。
- 确保主用（主要）和备用（辅助）Cisco vManage节点中没有其他操作正在进行。例如，确保没有服务器正在升级模板或将模板附加到设备。
- 如果已启用Cisco vManage HTTP/HTTPS代理服务器，请将其禁用。请参阅HTTP/HTTPS代理服务器，以实现Cisco vManage与外部服务器的通信。如果不禁用代理服务器，Cisco vManage会尝试通过代理IP地址建立灾难恢复通信，即使Cisco vManage带外集群IP地址可直接访问。您可以在灾难恢复注册完成后重新启用Cisco vManage HTTP/HTTPS代理服务器。
- 在开始灾难恢复注册过程之前，导航到主Cisco vManage节点上的Tools > Rediscover Network窗口，并重新发现Cisco vBond Orchestrator。

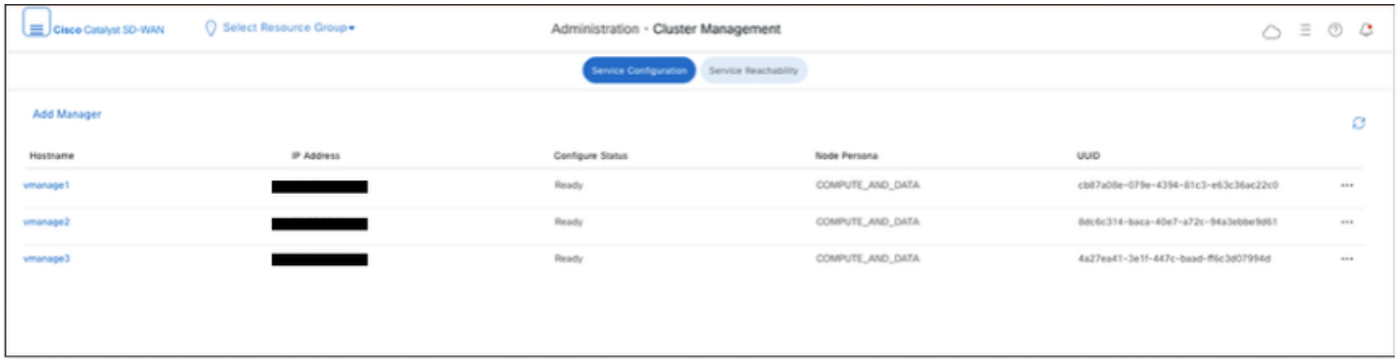
配置

有关vManage灾难恢复的详细信息，请参阅此链接。

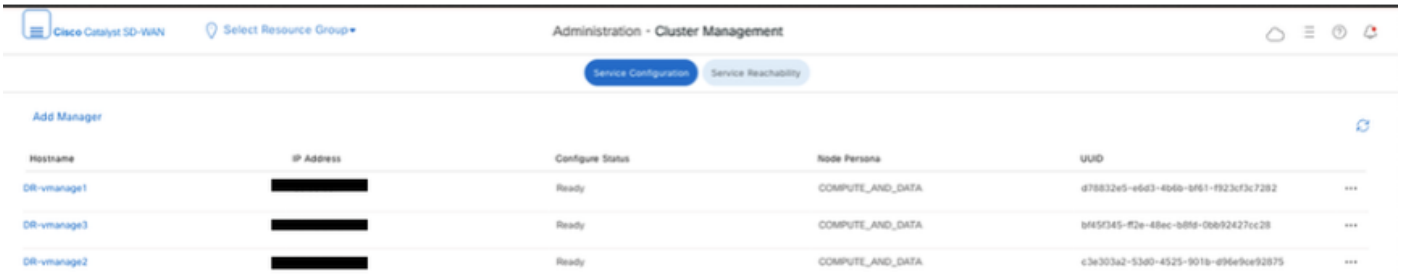
假设每个SD-WAN管理器具有最低配置并完成认证部分，则已创建两个单独的3节点集群。

在两个集群上导航到Administration > Cluster Management，并验证所有节点是否处于就绪状态。

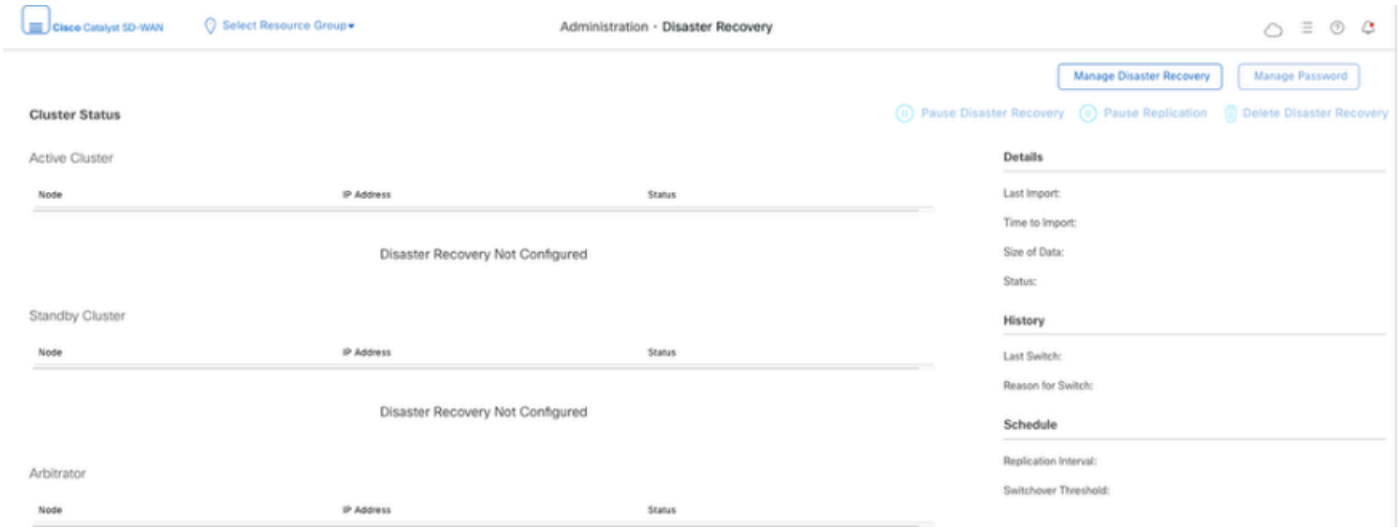
DC vManage



DR vmanage



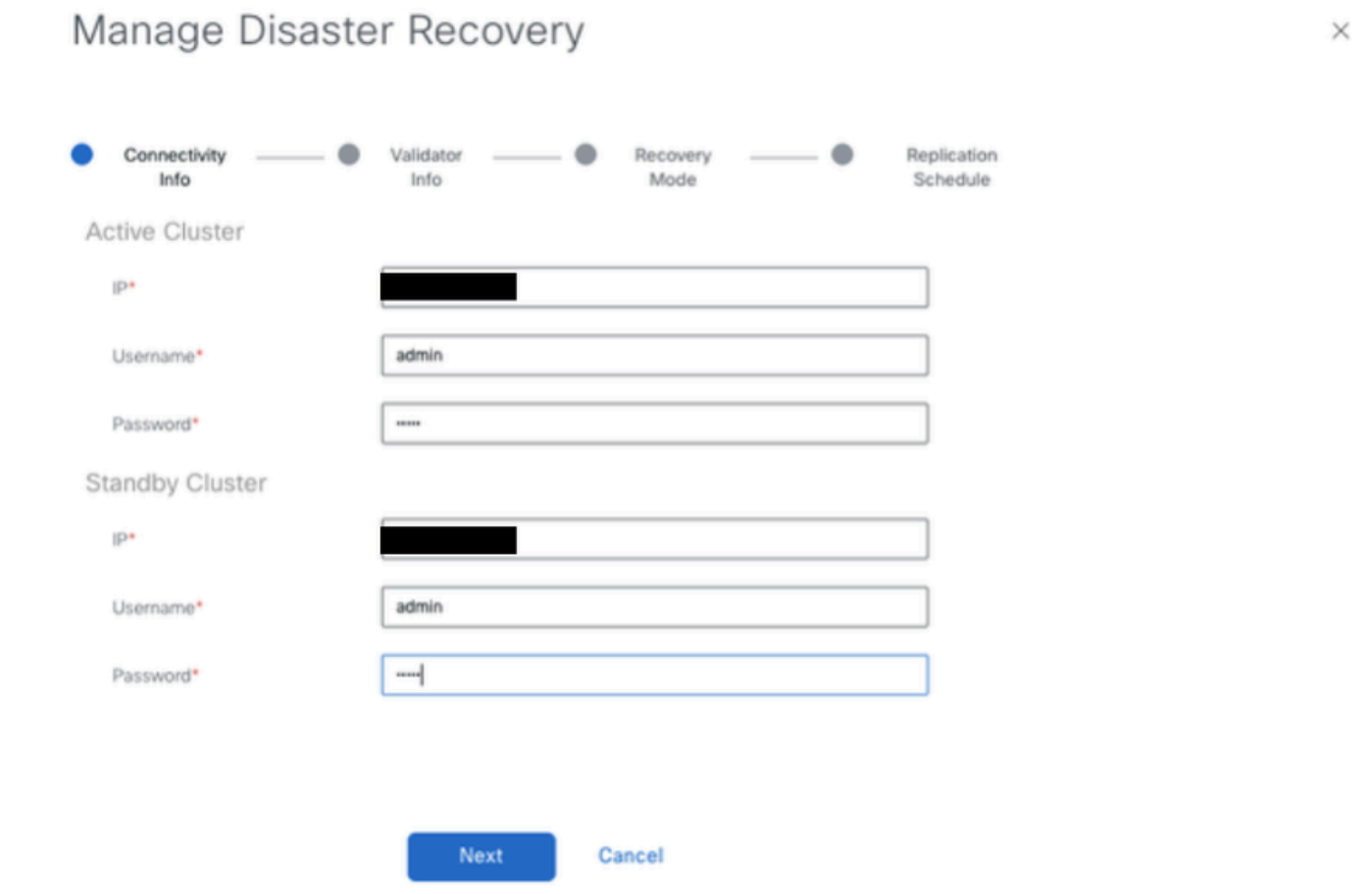
导航到Administration>Disaster Recovery of Primary vManage Cluster。单击管理灾难恢复。



在弹出窗口中，填写主要和辅助vManage的详细信息。

要指示的IP地址是带外集群接口IP地址。 最好在每个集群中使用vManage-1的VPN 0服务接口的IP地址。

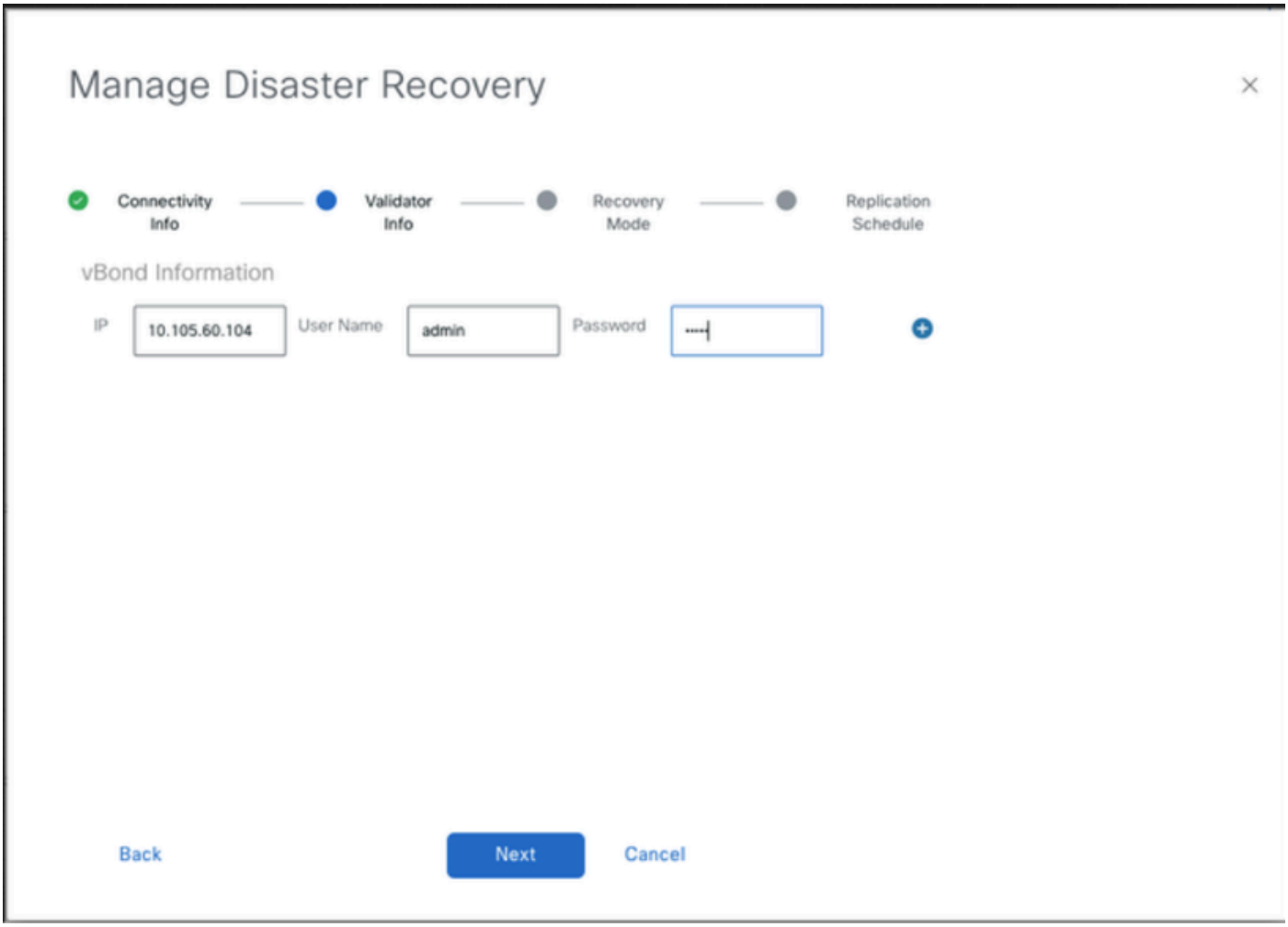
凭证必须是netadmin用户的凭证，配置DR后不得更改凭证，除非删除凭证。 可以使用独立的vManage本地用户凭证进行灾难恢复。我们需要确保vManage本地用户是netadmin组的一部分。此处可使用管理员凭据。



填满后，单击下一步。

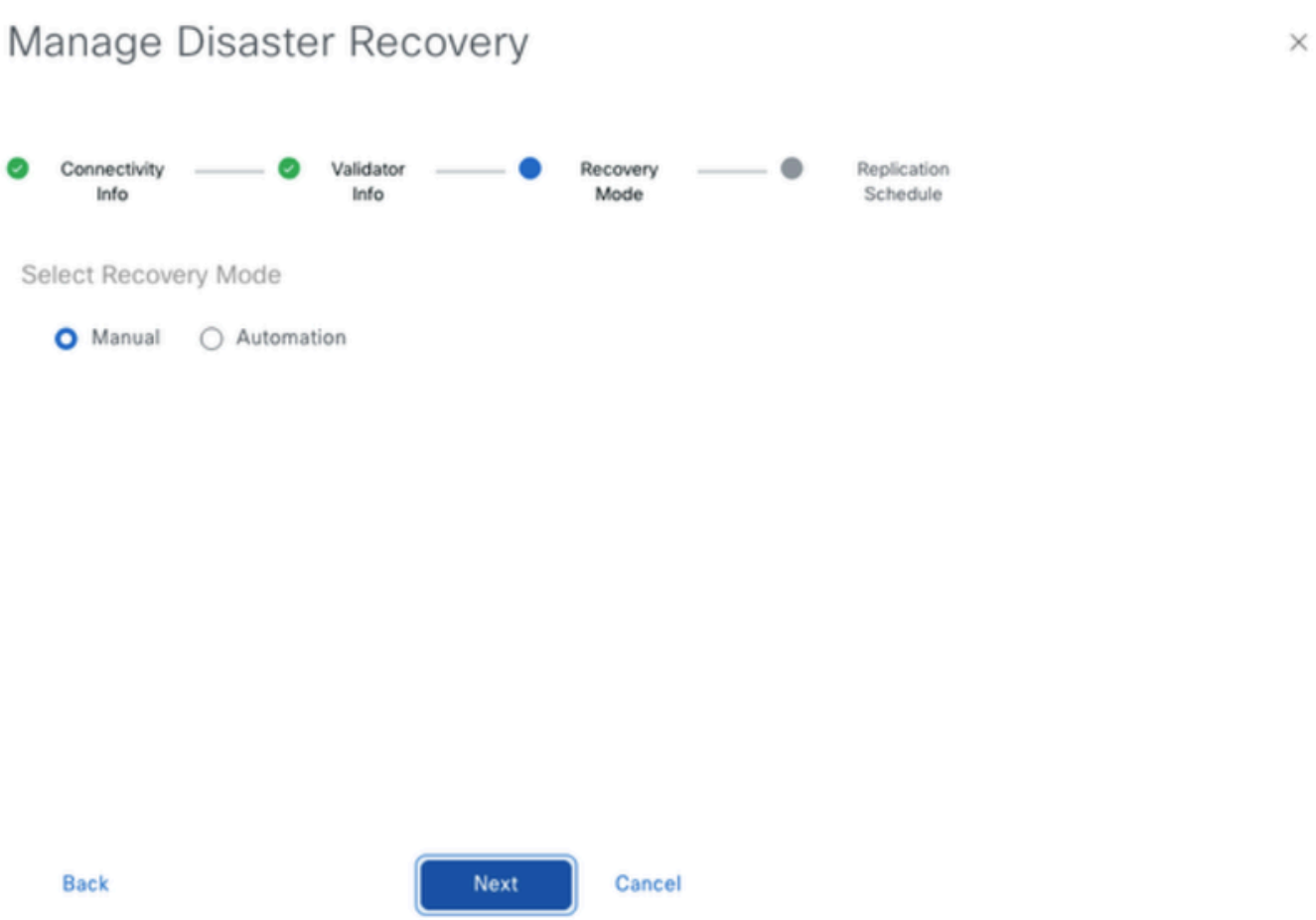
- 填写vBond控制器详细信息。

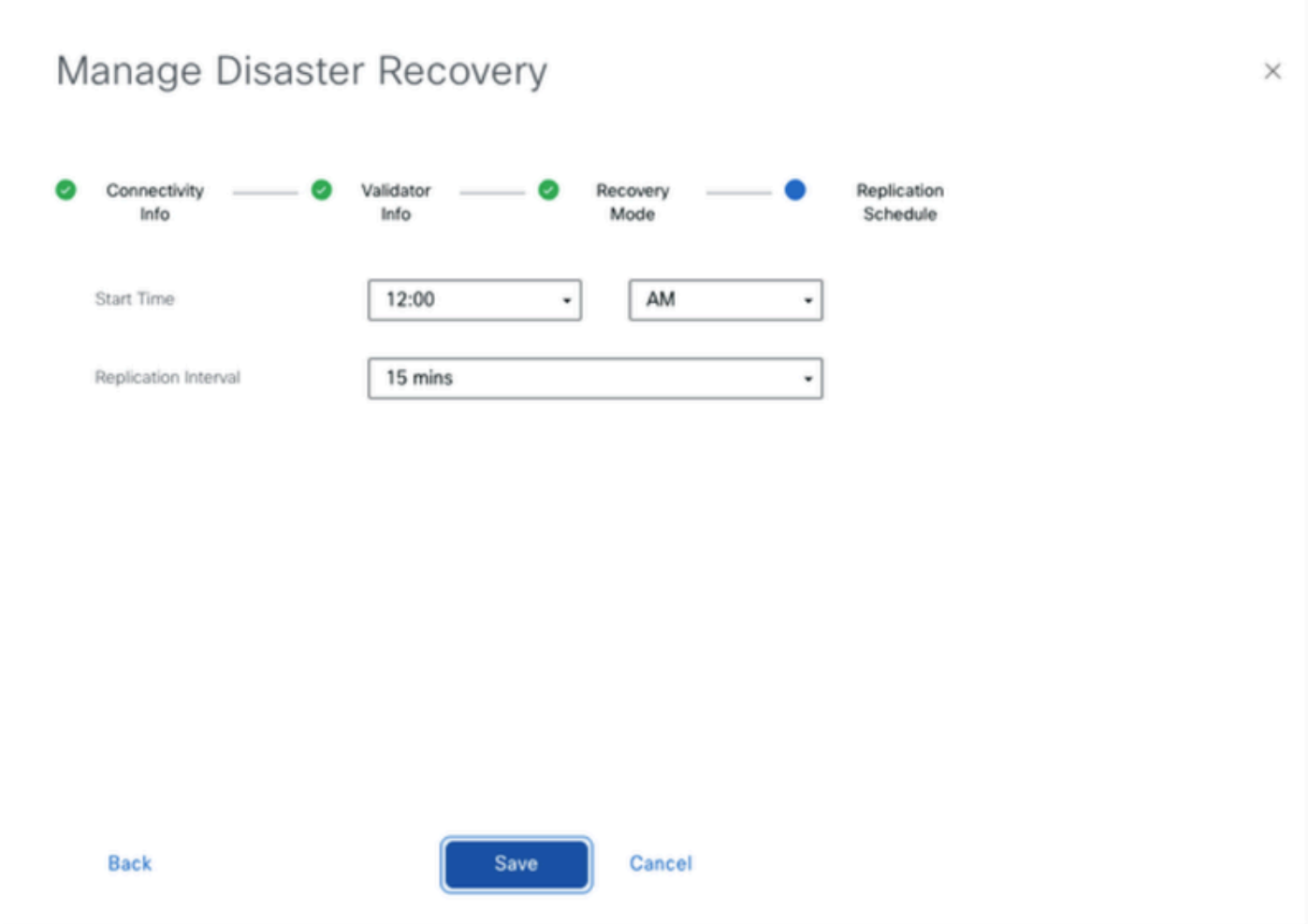
vBond控制器必须在指定的IP地址中通过Netconf到达。



填满后，单击下一步。

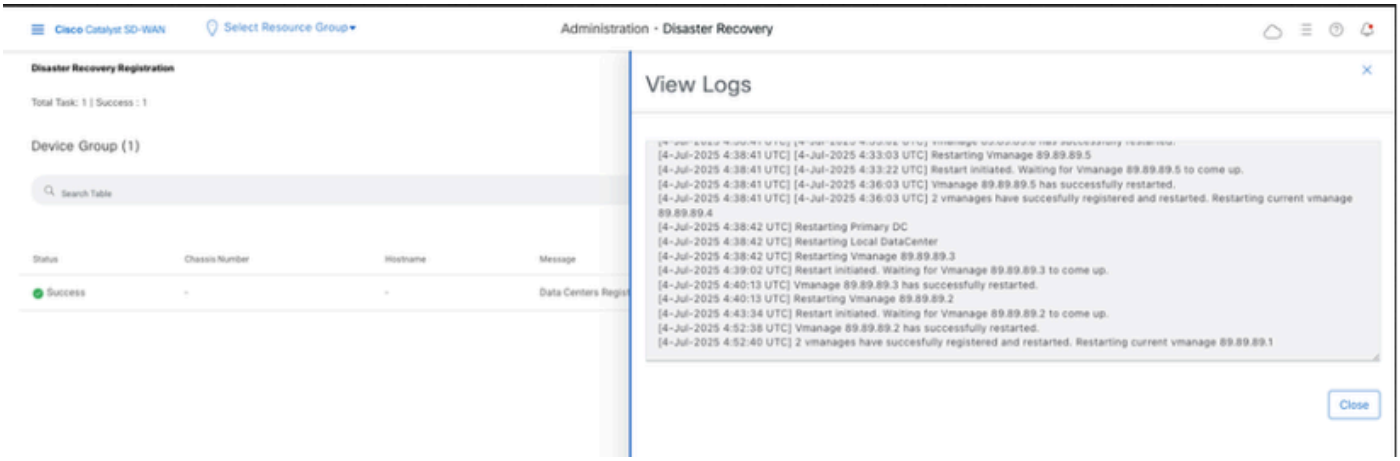
- 在恢复模式下，选择手动。自动化模式已弃用。单击 Next。


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



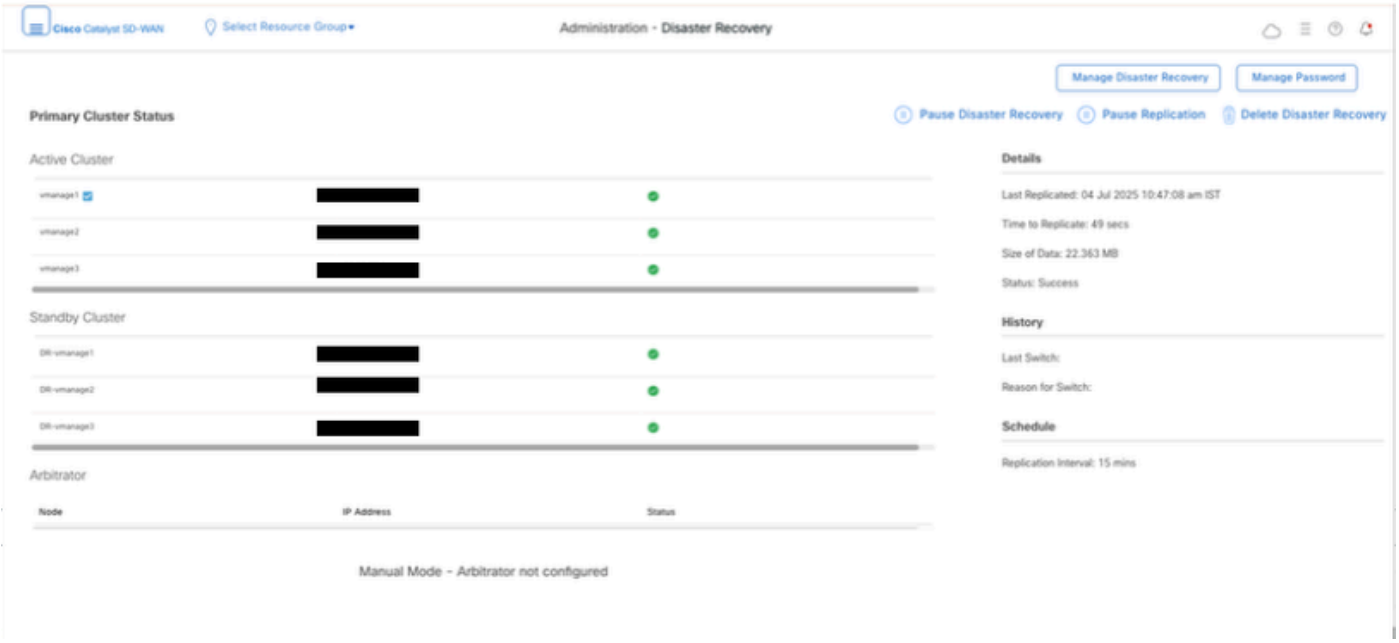
设置值，然后单击Save。

- DR注册现在开始。点击刷新按钮以手动刷新状态和进度日志。此过程可能需要20-30分钟。



确认

导航到管理>灾难恢复，以查看灾难恢复状态以及上次复制数据的时间。



注意：复制可能需要几个小时，具体取决于数据库大小。此外，它可能需要几个周期才能成功复制。

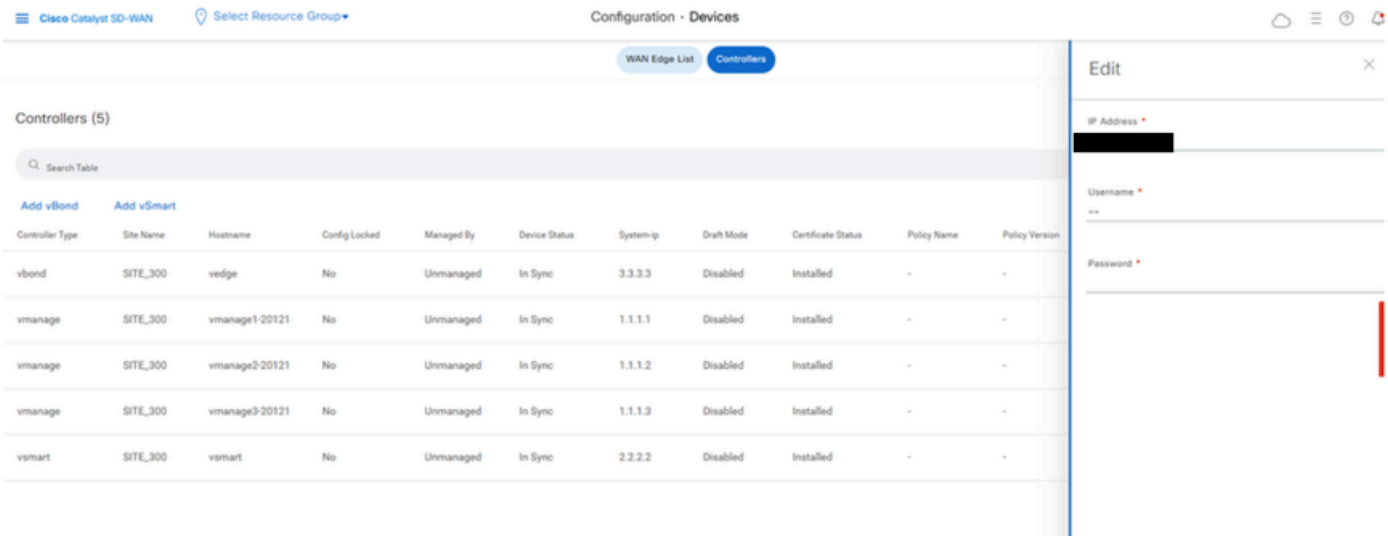
步骤 6：控制器重新验证和旧控制器失效

恢复configuration-db后，我们需要重新验证交换矩阵中的所有新控制器(vmanage/vsmart/vbond)

注：在实际生产中，如果用于重新身份验证的接口IP是隧道接口IP，则需要确保在vManage、vSmart和vBond的隧道接口以及路径沿途的防火墙上允许NETCONF服务。要打开的防火墙端口是从DR群集到所有vBonds和vSmarts的双向规则的TCP端口830。

在vmanage UI上，点击Configuration > Devices > Controllers

- 点击每个控制器附近的三个点，然后点击Edit



- 将ip-address（控制器的系统ip）替换为transport vpn 0（隧道接口）ip地址。输入用户名和密码，然后点击save
- 对交换矩阵中的所有新控制器执行相同操作

同步根证书链

所有控制器入网后，请完成以下步骤：

在新活动集群中的任何Cisco SD-WAN Manager服务器上，执行以下操作：

输入以下命令将根证书与新活动集群中的所有Cisco Catalyst SD-WAN设备同步：

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

输入以下命令将Cisco SD-WAN Manager UUID与Cisco SD-WAN Validator同步：

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

一旦交换矩阵恢复，并且交换矩阵中的所有边缘和控制器的控制和bfd会话都已启动，我们就需要从UI使旧控制器(vmanage/vsmart/vbond)失效

- 在vmanage UI上，点击Configuration > Devices > Certificates
- 点击“控制器”
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击invalidate（失效）
- 点击send to vbond
- 在vmanage UI上，点击Configuration > Devices > Controllers
- 点击旧交换矩阵中控制器(vmanage/vsmart/vbond)附近的三个点。点击Delete

过帐检查

这些后期检查适用于所有部署组合。

重新激活云边缘路由器：

- 如果C8000v属于重叠并受管签名，则需要重新进行身份验证，即：

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

        token
```

- 确认控制连接和BFD会话已启动
- 确认应用流量正在端到端流动
- 如果在边缘上重建交换矩阵之前对端口跃点进行了更改，则必须恢复这些更改
- 验证项目是否按预期显示：
    - 模板
    - 策略
    - 设备页面（两个选项卡）WAN vEdge ListandControllers

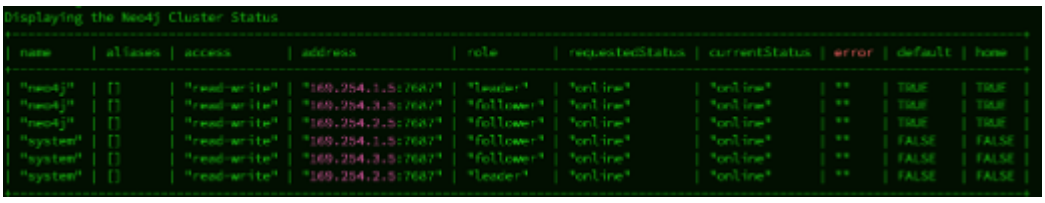
  vManage post checks

- 适用于vManage节点：

  Configuration-DB(Neo4j)检查：

  在所有vManage节点上执行命令“request nms configuration-db diagnostics”：

  1.检查节点在线状态和领导状态：（不适用于所有版本）



“Neo4j”必须在线显示3个节点，1个领导者和2个追随者。“system”还必须显示3个在线节点、1个引导节点和2个跟随者，但由于这不是默认数据库，因此默认标志为false。如果每个neo4j少于3个条目，则系统表示节点从集群中脱离。请联系Cisco TAC进行故障排除。

2.检查是否有任何节点为“隔离”。

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

所有节点都必须处于隔离状态。

3.架构验证必须“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.使用命令“request nms configuration-db diagnostics”收集configuration-db备份，并确保其成功。

```
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#
```

如果发现任何不一致或错误，请联系Cisco TAC进行故障排除。

或者，我们可以运行这些API调用以确认集群（用于所有COMPUTE+DATA节点）的vmanage节点状态 — 仅在20.12版及更高版本上运行

```
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
```

确保在一个集群中只有一个neo4j和系统的领导，其余为跟随者。确保所有节点均在线。如果您有3个节点集群（全部三个都是COMPUTE+DATA），neo4j和系统的领导者都必须只有一个。任何偏差，您必须联系TAC

5.在/var/log/kern.log中检查所有磁盘、内存、IO错误。这需要在所有vManage节点上检查。

6.为在每个节点之间没有CC的vmanage形成新集群时，请检查该步骤
从节点1到其他节点集群ip执行vmanage-admin作为ssh，反之亦然，以检查是否交换了公钥且未使用密码ssh [此处步骤需要同意令牌]

```
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:
```

如果输出要求输入密码，请联系TAC

控制器开机自检检查：

适用于所有SD-WAN控制器(vBond、vManage、vSmart):

在重叠中的所有控制器上执行命令，并确认所看到的vManage UUID和序列号对当前交换矩阵有效：

虚拟绑定命令：

show orchestrator valid-vsmarts

show orchestrator valid-vmanage-id

vManage/vSmart命令：

show control valid-vsmarts

show control valid-vmanage-id

请注意，show control valid-vsmarts的输出包括vSmarts和vManage节点的序列号。

请将其与vManage UI中看到的进行比较。导航到配置>证书>控制器部分。

如果发现当前未注册到交换矩阵的UUID/序列号的其它条目，则必须将其删除。您也可以与思科TAC联系。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。