Reconstruya su fabric Catalyst SD-WAN

Contenido

Introducción

En este documento se describe cómo reconstruir un fabric SD-WAN de Cisco, incluidas las copias de seguridad y la restauración de las configuraciones del controlador para varias implementaciones.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) de Cisco
- Cisco Software Central
- Descargue el software Controllers de software.cisco.com

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Prerrequisitos Antes de Reconstruir el Fabric

- Se debe configurar un nuevo conjunto de id de sitio e ip del sistema para el nuevo fabric de los controladores
- Asegúrese de que las reglas de firewall estén en su lugar para habilitar la comunicación entre los controladores y los extremos
- Observe el nombre de usuario y la contraseña neo4j(configuration-db) (deben ser iguales en todos los nodos de vManage de un clúster)

- Inhabilite el salto de puerto en todos los bordes
- Aumentar los temporizadores de graceful restart a 7 días
- Borrado de alarmas en herramientas de 3rdparty antes de la migración
- Los datos de estadísticas históricas (alarmas, eventos, estadísticas de dispositivos, etc.) se pierden a menos que exista una configuración previa para exportar estadísticas a un servidor externo, como vAnalytics
- Si se configura Cloud OnRamp, asegúrese de que puede acceder al c8000v implementado en la nube antes de iniciar esta actividad
- Si tiene SDAVC activado en el fabric antiguo, asegúrese de que el nuevo fabric lo tiene activado (para el clúster, debe activarse en un solo nodo)
- La restauración de la base de datos de configuración sólo se admite en la misma versión que el fabric original
- Confirme la persona utilizada para los controladores. Ofrecemos soporte para COMPUTE_DATA y DATA persona (detalles en cada sección)
- Para la CA empresarial, debe utilizar el certificado raíz emitido por la CA empresarial, que se utiliza en la superposición existente, y el certificado se firma mediante el servidor de la CA empresarial y se instala para todos los controladores mediante la interfaz de usuario

Opciones de implementación

Implementación de vManage

- Independiente (1 nodo)
- Clúster (3 nodos o 6 nodos)

Opciones de DR

- No hay DR
- DR de nodo único
- Clúster de recuperación ante desastres en espera (manual/activado por el administrador)

Nota: Para obtener más detalles sobre el tipo de recuperación ante desastres, consulte este enlace

---

Combinaciones:

#	Configuración de vManage	Opción DR
1	Independiente (1 nodo)	No hay DR
2	Independiente (1 nodo)	DR de nodo único
3	Clúster (3 nodos o 6 nodos)	No hay DR
4	Clúster (3 nodos o 6 nodos)	Clúster de DR en espera

Pasos comunes aplicables a todas las combinaciones

Estos pasos son comunes a todas las combinaciones de implementación. Cubren el proceso de activar instancias de VM y aplicar la configuración básica de CLI. Cada sección de combinación indica cuántas instancias se deben implementar y qué pasos adicionales se deben completar.

Instalar y activar los controladores SD-WAN (administrador, validador, controlador)

Nota: Cisco ha cambiado la marca de determinados términos, por lo que estos son intercambiables. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst Controller

---

Descargue los archivos OVA para los controladores SD-WAN de la página de descarga de software de Cisco aquí:

- Elija vEDGE Cloud y descargue el OVA de vBond para la versión de software requerida.
- Elija vManage software y descargue el vManage OVA para la versión de software requerida.
- Elija vSmart software y descargue el vSmart OVA para la versión de software requerida.

Nota: En las plataformas ESXi/en la nube, active los controladores vSmart, vBond y vManage mediante el archivo OVA. Consulte el documento vinculado y asegúrese de que se asignen suficientes CPU, RAM y discos a todos los controladores, según el tipo de implementación de SD-WAN. Navegue aquí para obtener información adicional. Asegúrese de asignar un disco secundario al nodo vManage como se menciona en la columna Storage Size* (Tamaño de almacenamiento) de la guía informática vinculada.

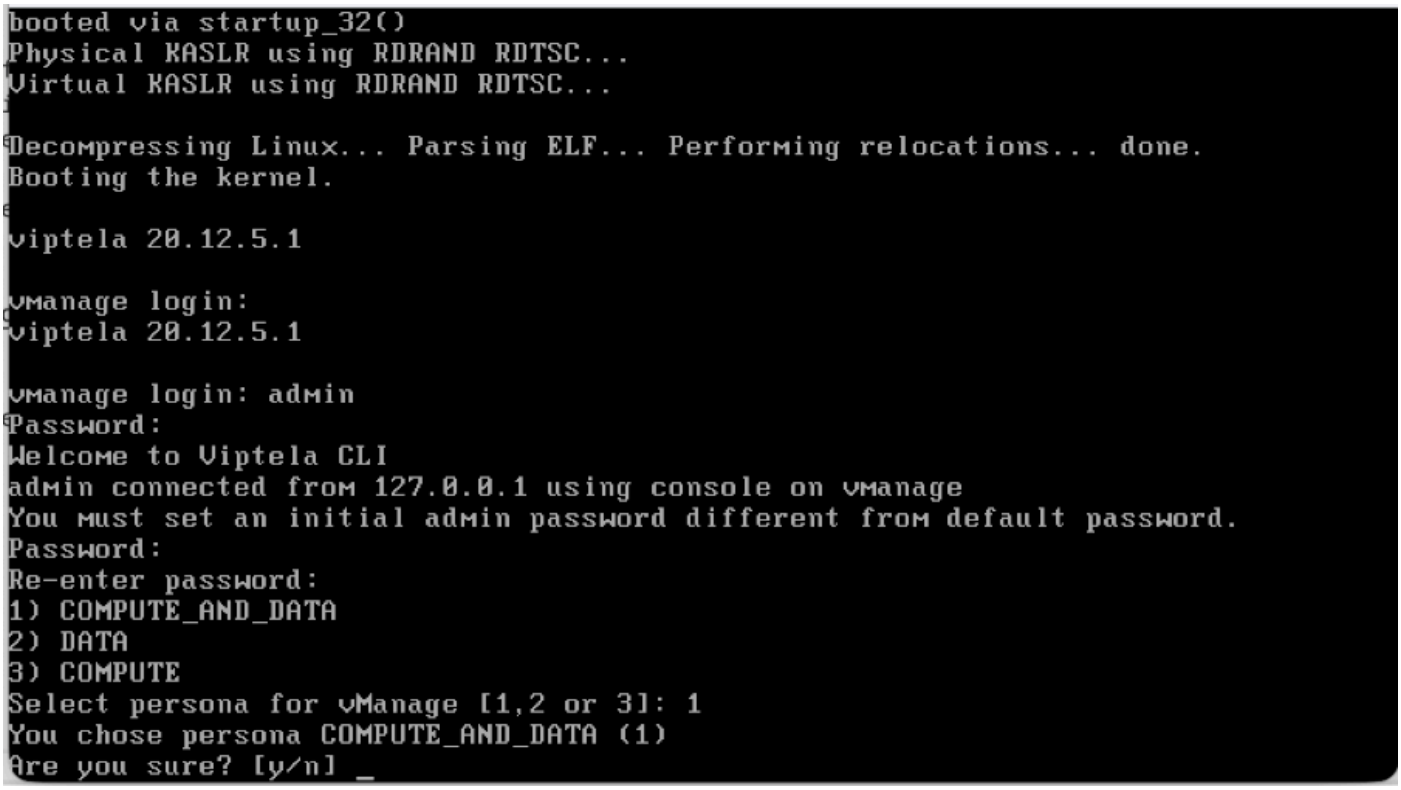
Activar un nodo de Cisco Manager

- Una vez que se haya implementado Cisco Manager o vManage VM y se pueda acceder a la consola del administrador, espere a que finalice el arranque. Una indicación es que vemos que un sistema de mensajes está listo y solicita el nombre de usuario y la contraseña.
- Introduzca las credenciales de usuario predeterminadas nombre de usuario como admin y contraseña como admin. Exponga que solicita al usuario que cambie la contraseña, establezca la contraseña que necesita el administrador de usuarios según su elección.
- A continuación, solicita al usuario que seleccione la persona. Este es un paso crítico si la intención es tener un clúster de vManage. Seleccione el personaje según se muestra a continuación:

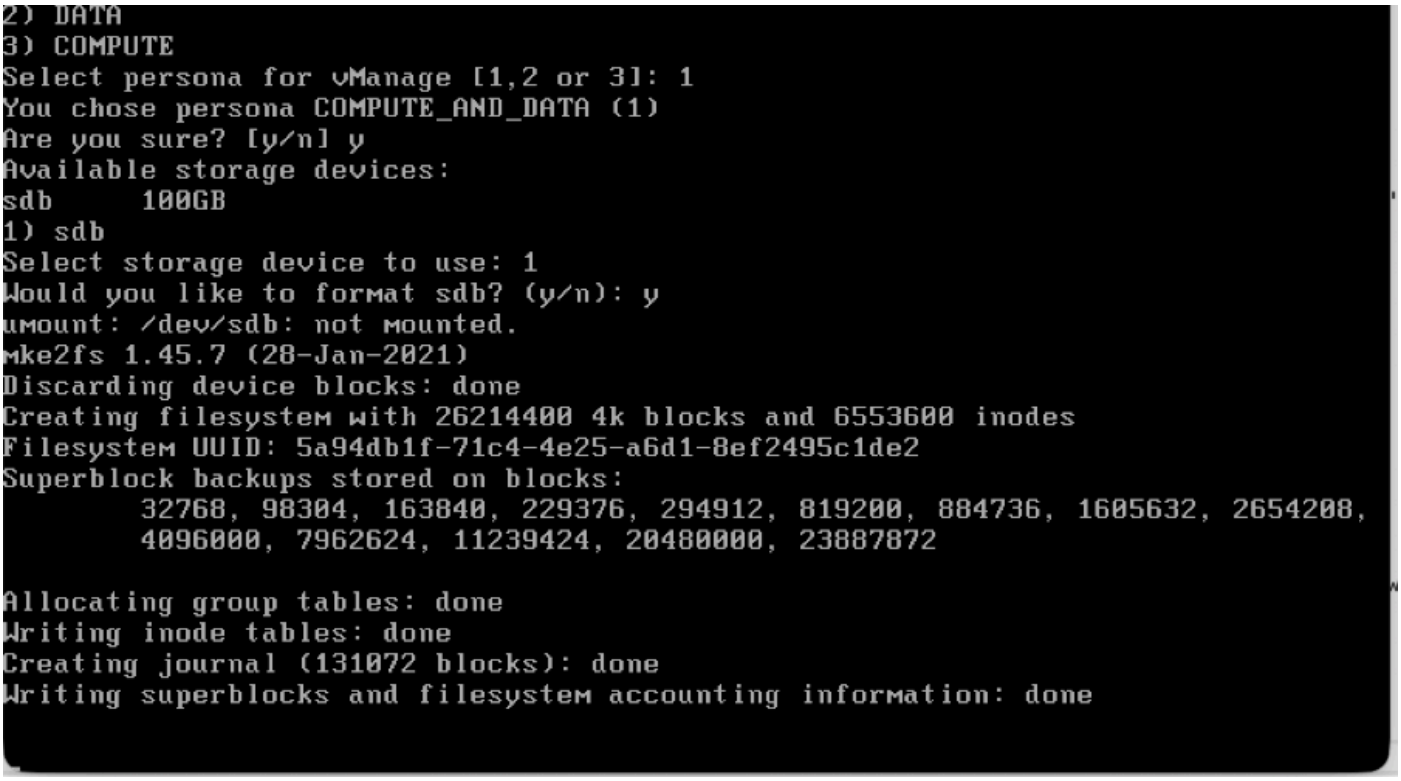
```
For a standalone vManage, choose the persona as COMPUTE_AND_DATA.
```

```
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
```

Ejemplo:Elija 1 para COMPUTE_AND_DATA

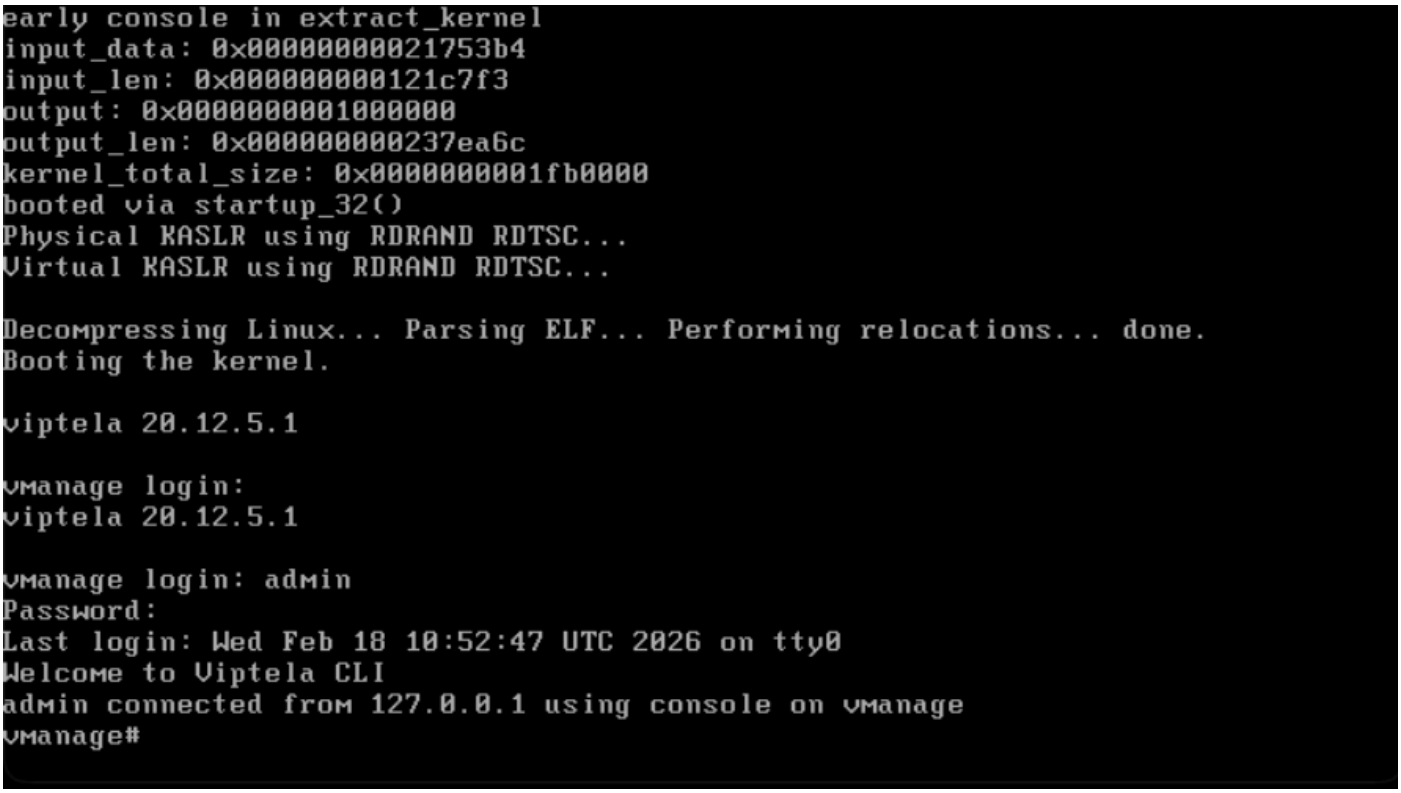


Elija el disco secundario como se muestra:



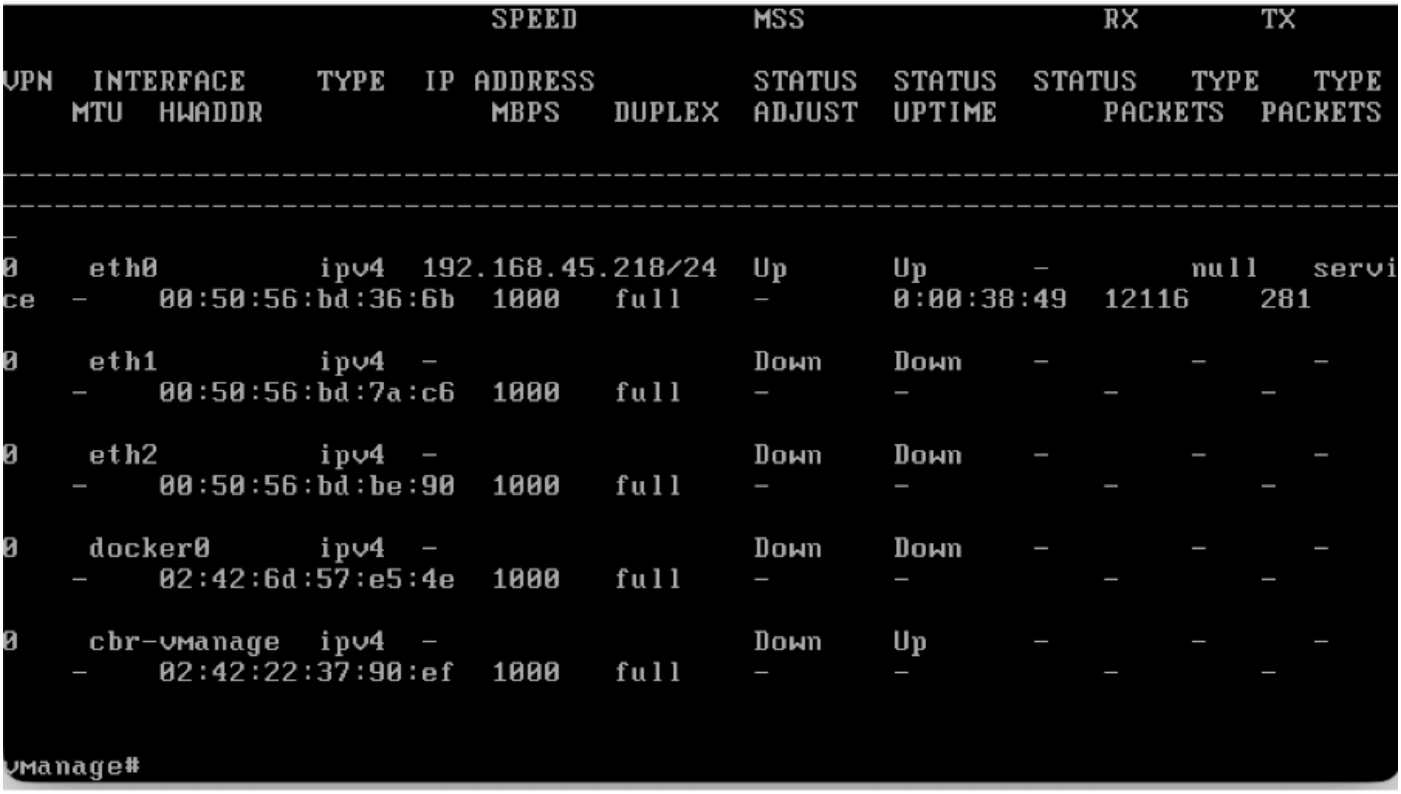
- Elija el disco secundario y escriba Y para confirmar.

- Cisco Manager se recarga. Una vez que arranque, introduzca el nombre de usuario y la contraseña con la nueva contraseña que se acaba de configurar.



- Puede configurar la interfaz de administración VPN 512 para habilitar el acceso de administración fuera de banda al controlador.
- Utilice el comando show interface | para comprobar las VPN a las que están asignadas actualmente las interfaces.
- configure las interfaces como corresponda.

Ejemplo:



```
                            SPEED          MSS                 RX       TX

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

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

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

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

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

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


vManage#
```

Nota: Puede consultar la configuración del vManage existente y configurar el mismo esquema de direcciones IP aquí.

Configuraciones de interfaz de gestión (VPN 512)

- Si es necesario mover una interfaz de VPN 0 a VPN 512, utilice estos comandos y luego configure la dirección IP en la interfaz

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




  no shutdown
 !
 ip route 0.0.0.0/0



!
```

Abra el Validador.

- En el hipervisor, configure el ordenador necesario (CPU, RAM y disco) para el nodo vBond y enciéndalo.
- Una vez que se pueda acceder a la consola, espere a que vBond se inicie por completo. Espere el mensaje System Ready (Sistema preparado).
- El sistema solicita el nombre de usuario y la contraseña. Introduzca las credenciales de usuario predeterminadas nombre de usuario como admin y la contraseña como admin. Después de esto, solicita al usuario que cambie la contraseña, establezca la contraseña necesaria para el usuario admin como prefiera.
- Puede configurar la interfaz de administración VPN 512 para habilitar el acceso de administración fuera de banda al controlador.
- Utilice el comando show interface | para comprobar las VPN a las que están asignadas actualmente las interfaces.
- Configure las interfaces como corresponda.

Ejemplo:

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

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

vbond-01#
```

Nota: Puede consultar la configuración del vBond existente y configurar las mismas configuraciones aquí.

Configuraciones de interfaz de gestión (VPN 512)

- Si es necesario mover una interfaz de VPN 0 a VPN 512, utilice estos comandos y luego configure la dirección IP en la interfaz.

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




  no shutdown
 !
 ip route 0.0.0.0/0




!
commit
```

Activar un nodo de controlador (vSmart)

- Realice los mismos pasos que el Validador para activar el nodo vSmart.
- Una vez configurada la dirección IP VPN 512 en todos los controladores SD-WAN, puede acceder a ellos mediante SSH en la dirección IP VPN 512.

Configuración CLI básica en todos los controladores

Una vez que tenga acceso SSH a todos los controladores, configure estas configuraciones CLI en cada controlador.

Configuración del sistema

```
config t
system
 host-name
```

```
 system-ip

 site-id

 organization-name

 vbond

commit
```

Nota: Si utilizamos URL como dirección vBond, asegúrese de configurar las direcciones IP del servidor DNS en la configuración VPN 0 o asegúrese de que se puedan resolver.

Configuración de la interfaz de transporte (VPN 0)

Estas configuraciones son necesarias en todos los controladores para habilitar la interfaz de transporte utilizada para establecer conexiones de control con los routers y el resto de los controladores.

```
config t
vpn 0
 dns

        primary
 dns
```

```
        secondary
 interface eth1
  ip address




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



commit
```

Nota: Puede consultar las configuraciones de su controlador existente y si la configuración está presente, puede agregar esta configuración a los nuevos controladores.

Configure el protocolo de control como TLS solo si hay un requisito para que los routers establezcan conexiones de control seguras con los nodos vManage mediante TLS. De forma predeterminada, todos los controladores y routers establecen conexiones de control mediante DTLS. Se trata de una configuración opcional que solo se requiere en los nodos vSmart y vManage, según sus necesidades.

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

Combinación 1: vManage independiente + sin DR

Instancias necesarias:

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

Pasos:

1. Abra todas las instancias mediante los pasos comunes
2. Comprobaciones previas
3. Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage
4. Copia de seguridad/restauración de Config-db
5. Registrar cheques

Paso 1: Comprobaciones previas

- Asegúrese de que el número de instancias de Cisco SD-WAN Manager activas sea idéntico al número de las instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager ejecuten la misma versión de software.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager puedan alcanzar la dirección IP de administración del Cisco SD-WAN Validator.
- Asegúrese de que los certificados se hayan instalado en las instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que los relojes de todos los dispositivos Cisco Catalyst SD-WAN, incluidas las nuevas instancias de Cisco SD-WAN Manager instaladas, estén sincronizados.
- Asegúrese de que se haya configurado un nuevo conjunto de IP del sistema e ID del sitio en las instancias de Cisco SD-WAN Manager recién instaladas, junto con la misma configuración básica que el clúster activo.

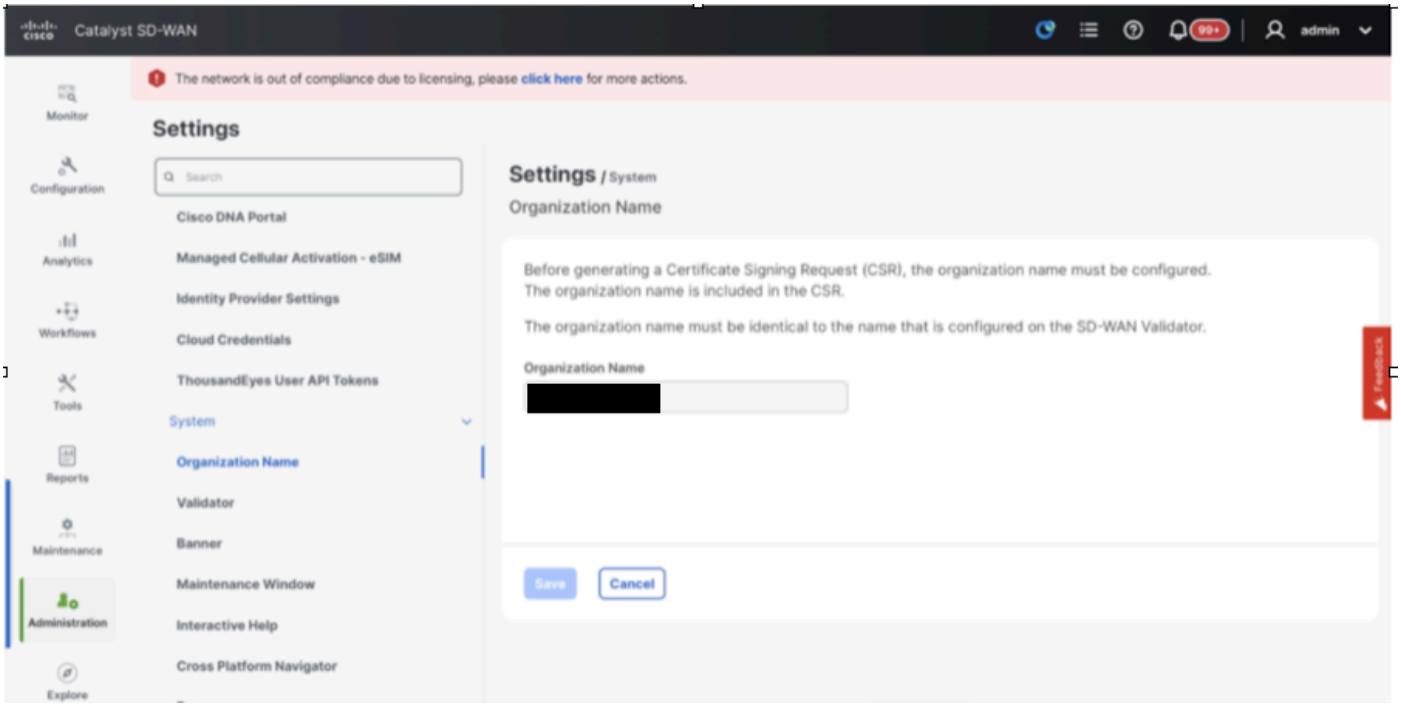
Paso 2: Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage

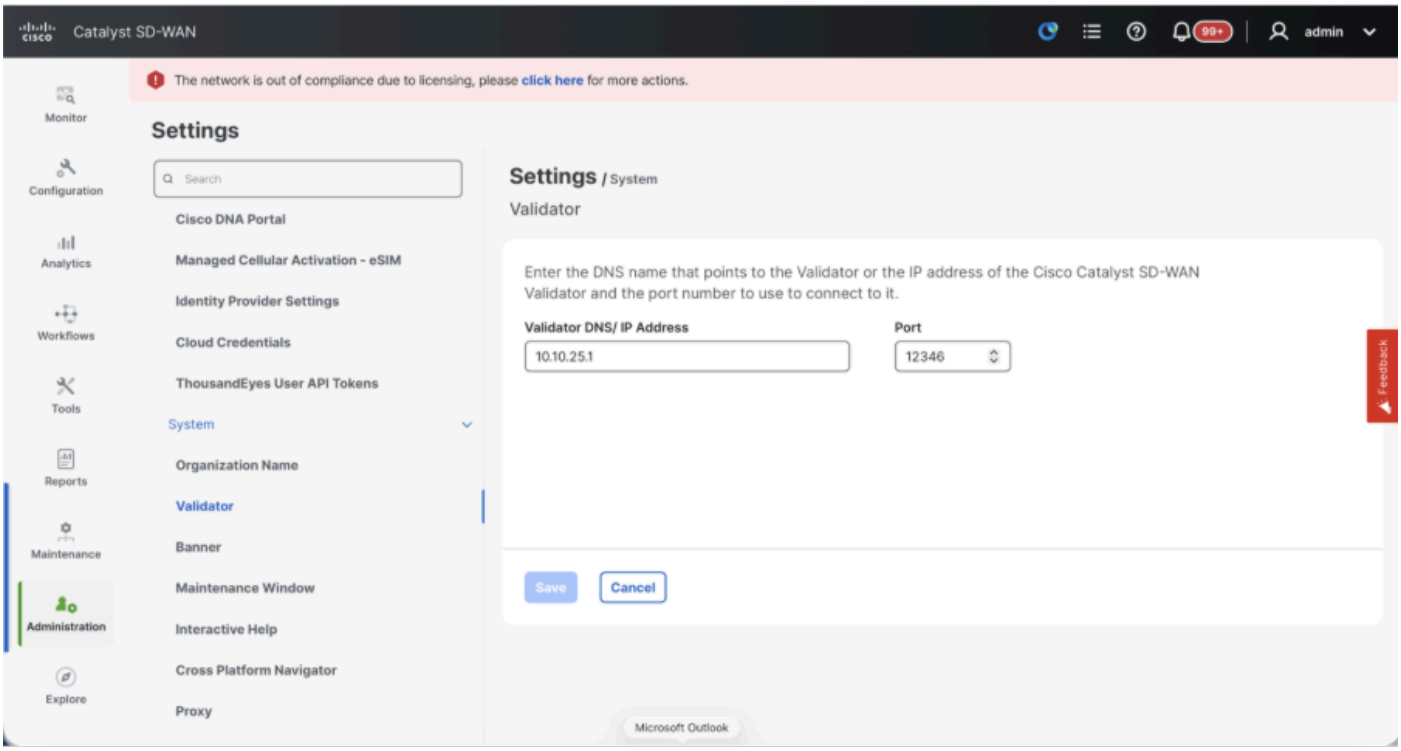
Actualizar las configuraciones en la interfaz de usuario de vManage

- Una vez agregadas las configuraciones del paso 1 en la CLI de todos los controladores, podemos acceder a la interfaz de usuario web de vManage mediante la dirección URL

https://<vmanage-ip> en el navegador. Utilice la dirección IP VPN 512 de los nodos vManage respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.

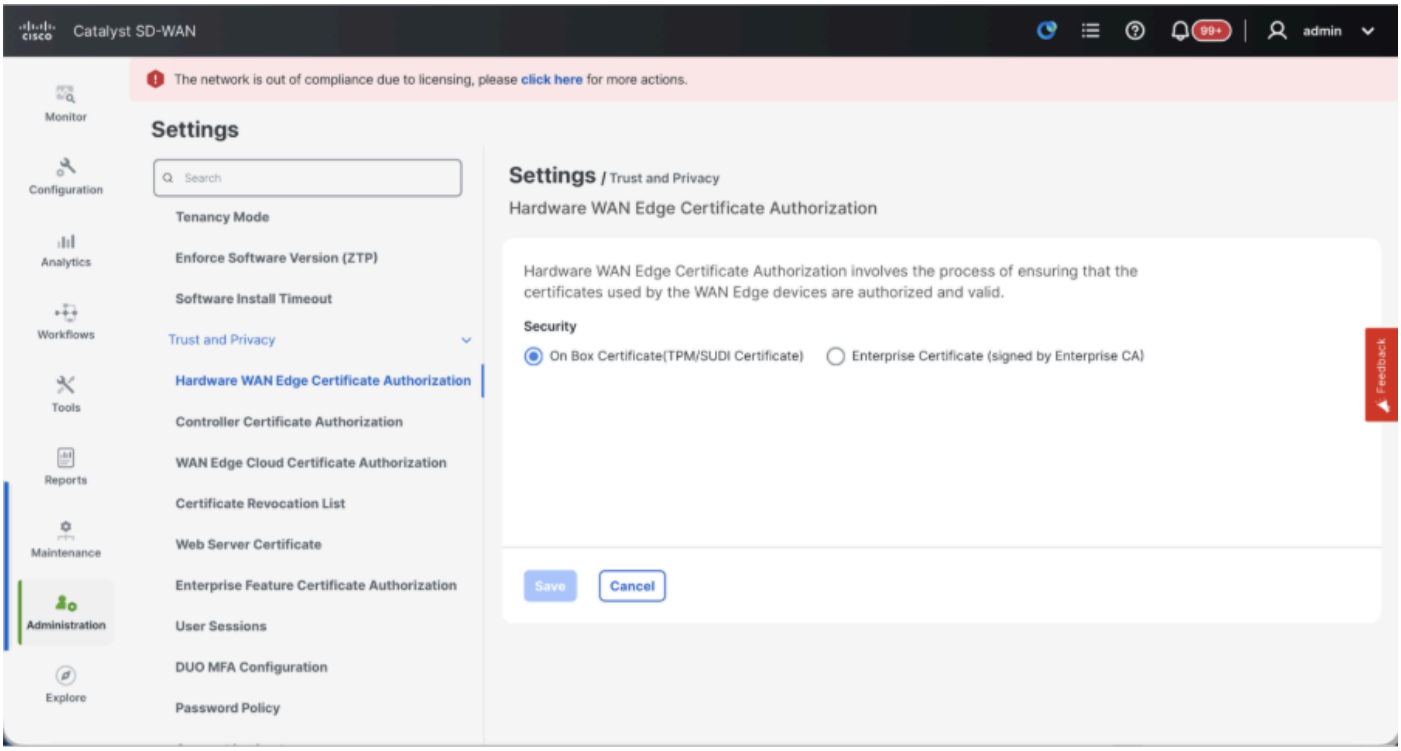
- Navegue hasta Administration > Settings y complete estos pasos.
- Configure el nombre de la organización y la dirección URL/IP del validador/vBond. Configure el mismo valor que en la CLI del nodo vManage.
- En vManage 20.15/20.18, estas configuraciones están disponibles en la sección Sistema.



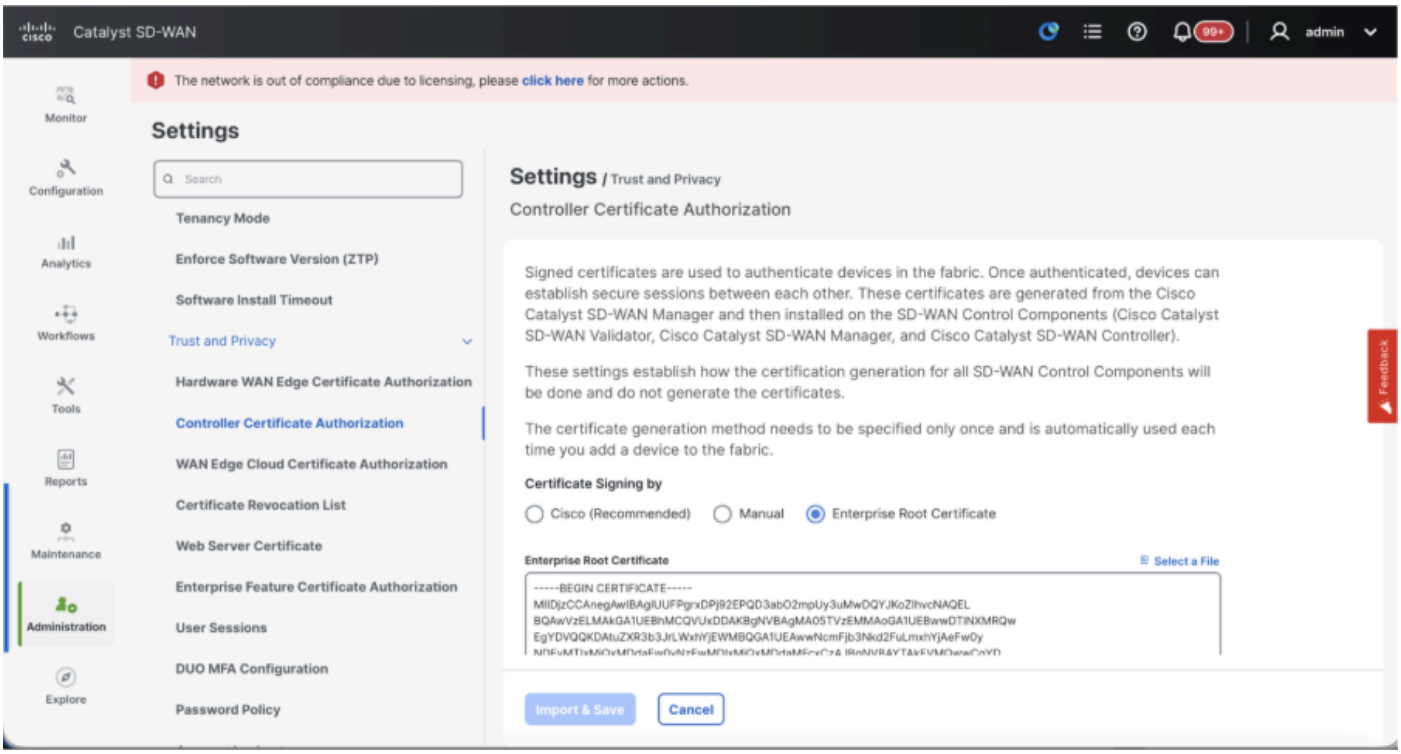


- Compruebe las configuraciones de la Autorización de certificados (CA), que decide la Autoridad de certificados utilizada para firmar los certificados. Podemos ver 3 opciones allí:

1. Autorización de certificado de extremo de WAN de hardware - Decide la CA para los routers periféricos SD-WAN de hardware.
    - Certificado en caja (certificado TPM/SUDI): con esta opción, el certificado preinstalado en el hardware del router se utiliza para establecer las conexiones de control (conexiones TLS/DTLS)
    - Certificado de empresa (firmado por la CA de empresa): con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

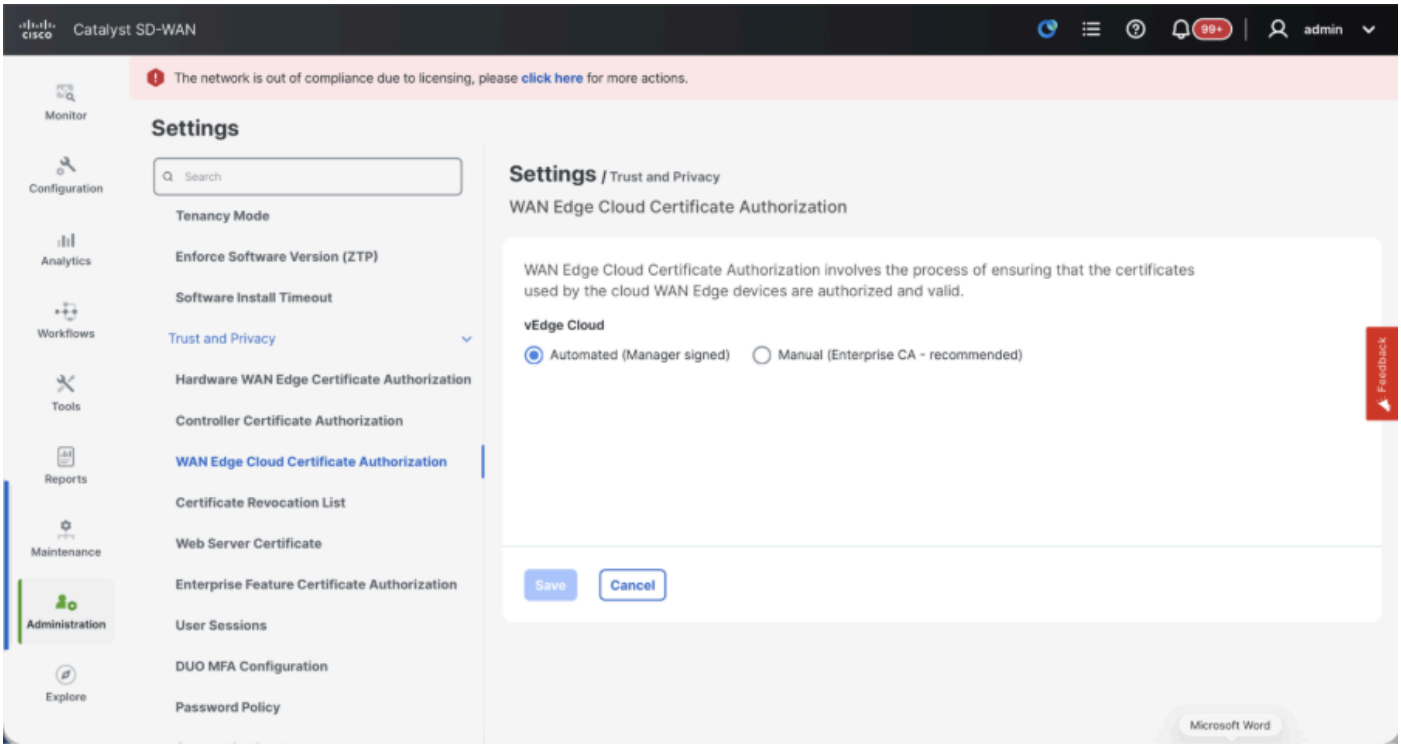


2. Autorización de certificado de controlador: decide la CA para los controladores SD-WAN.
    - Cisco (recomendado): los controladores utilizan los certificados firmados por Cisco PKI. vManage se pone en contacto automáticamente con el portal PNP mediante las credenciales de la cuenta inteligente configuradas en vManage y consigue que el certificado se firme y se instale en el controlador.
    - Manual: los controladores utilizan los certificados firmados por Cisco PKI. Firme manualmente el CSR mediante el portal Cisco PNP; para ello, acceda a la cuenta inteligente y la cuenta virtual de la superposición SD-WAN correspondiente.
    - Certificado raíz de empresa: con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

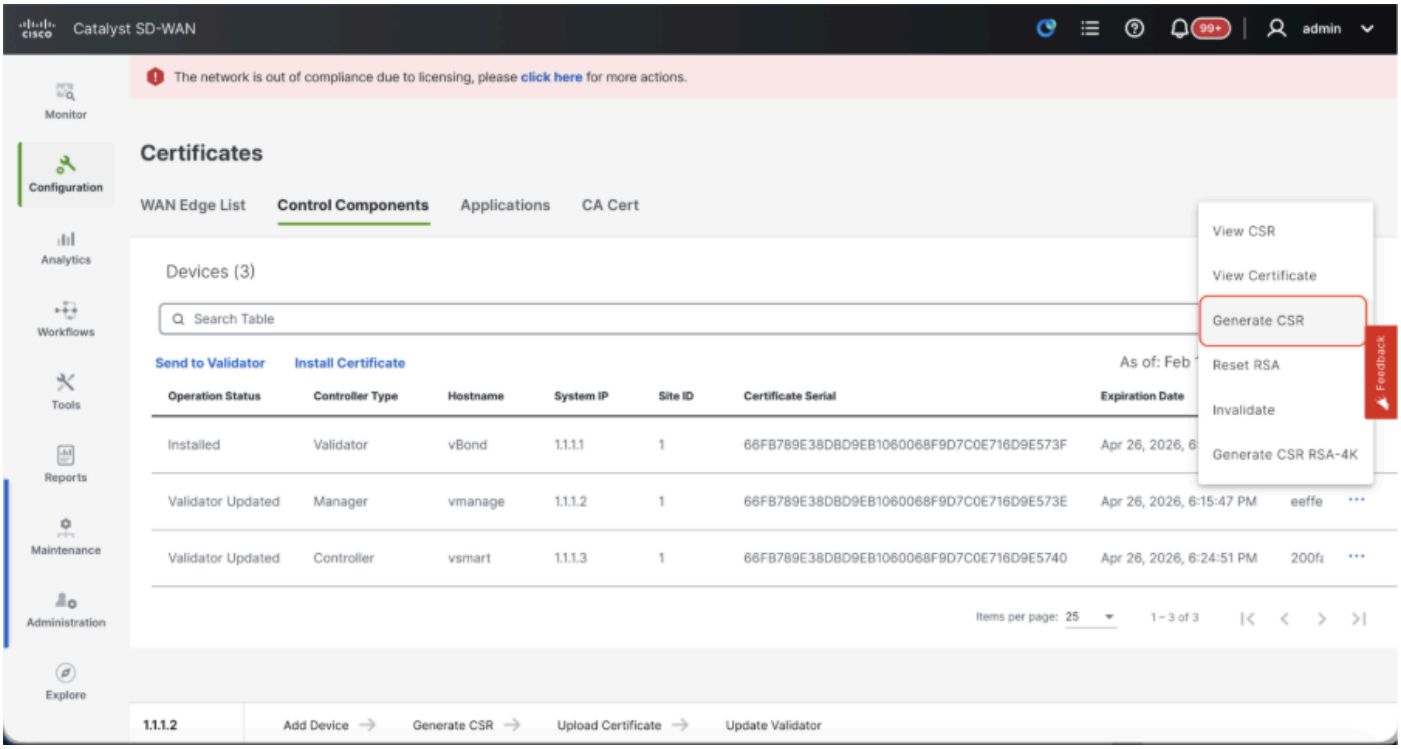


3. Autorización de certificado de nube de extremo de WAN: decide la CA para routers periféricos SD-WAN virtuales (CSR1000v, C8000v, nube vEdge)
    - Automatizado (vManage firmado): vManage firma automáticamente el CSR para los routers periféricos virtuales e instala el certificado en el router.
    - Manual (CA empresarial: recomendado): los routers virtuales utilizan certificados firmados por la autoridad de certificación empresarial de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

En este caso, si estamos utilizando nuestra propia CA, autoridad de certificación de empresa, elija Empresa.



- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers
- Haga clic en ... para Manager/vManage y haga clic en Generar CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.

Incorporación de vBond/Validator y vSmart/Controller a vManage

Vaya a Configuration > Devices > Control Components en caso de nodos vManage 20.15/20.18. En el caso de las versiones 20.9/20.12, Configuración > Dispositivos > Controladores

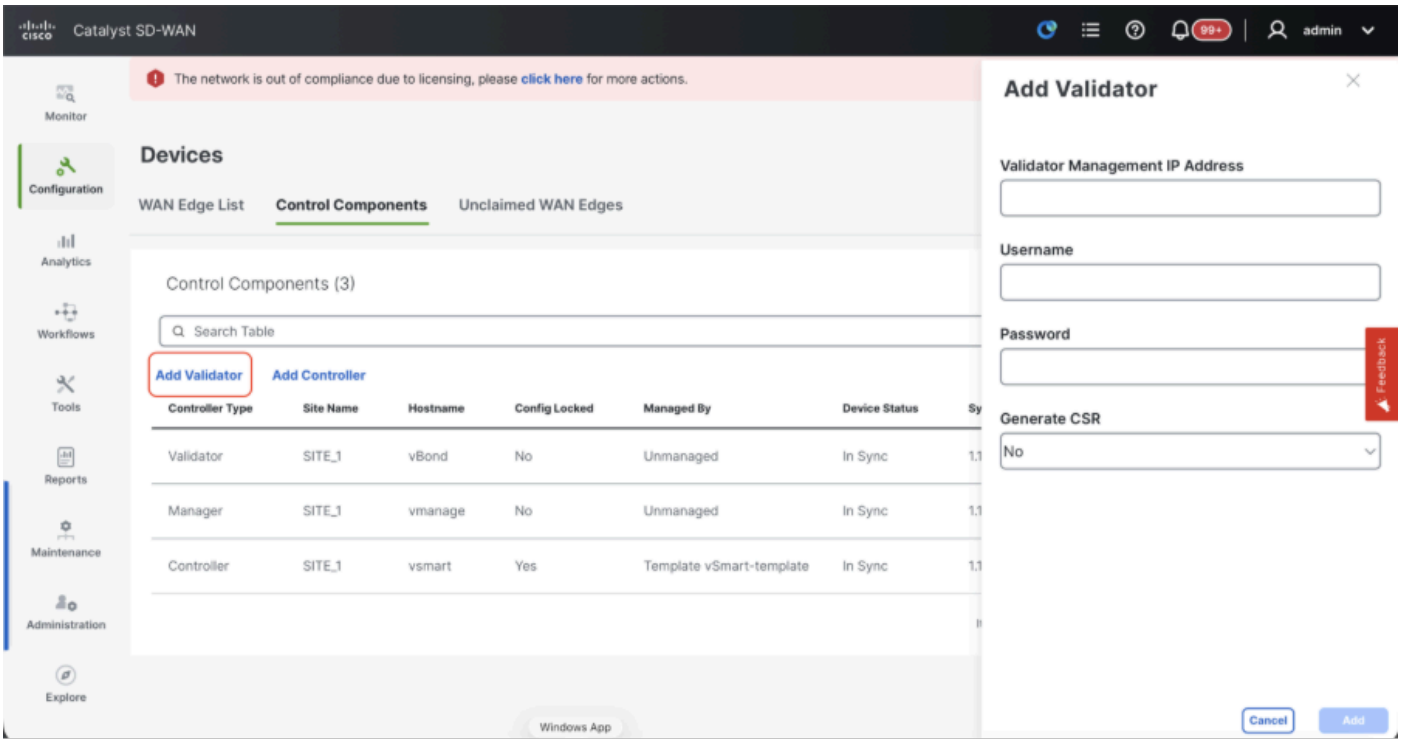
Incorporación de vBond/Validador

- Haga clic en AddvBonden caso de 20.12vManagerAgregar validadoren el caso de 20.15/20.18vManage. Se abre una ventana emergente, introduzca el IP de transporte VPN 0 de vBondque se puede alcanzar desde thevManage.
- Verifique la disponibilidad mediante ping si se permite desde la CLI de vManagetovBondIP.

- Introduzca las credenciales de usuario de vBond.

Nota: Necesitamos usar las credenciales de administración de vBono una parte de usuario denetadmingroup. Puede verificarlo en la CLI de thevBond. Elija Sí en el menú desplegable de "Generar CSR" si necesitamos instalar un nuevo certificado para vBond.

Nota: Si vBond está detrás de un dispositivo NAT/firewall, verifique si la IP de la interfaz VPN 0 de vBond se traduce a una IP pública. Si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la interfaz VPN 0 en este paso.

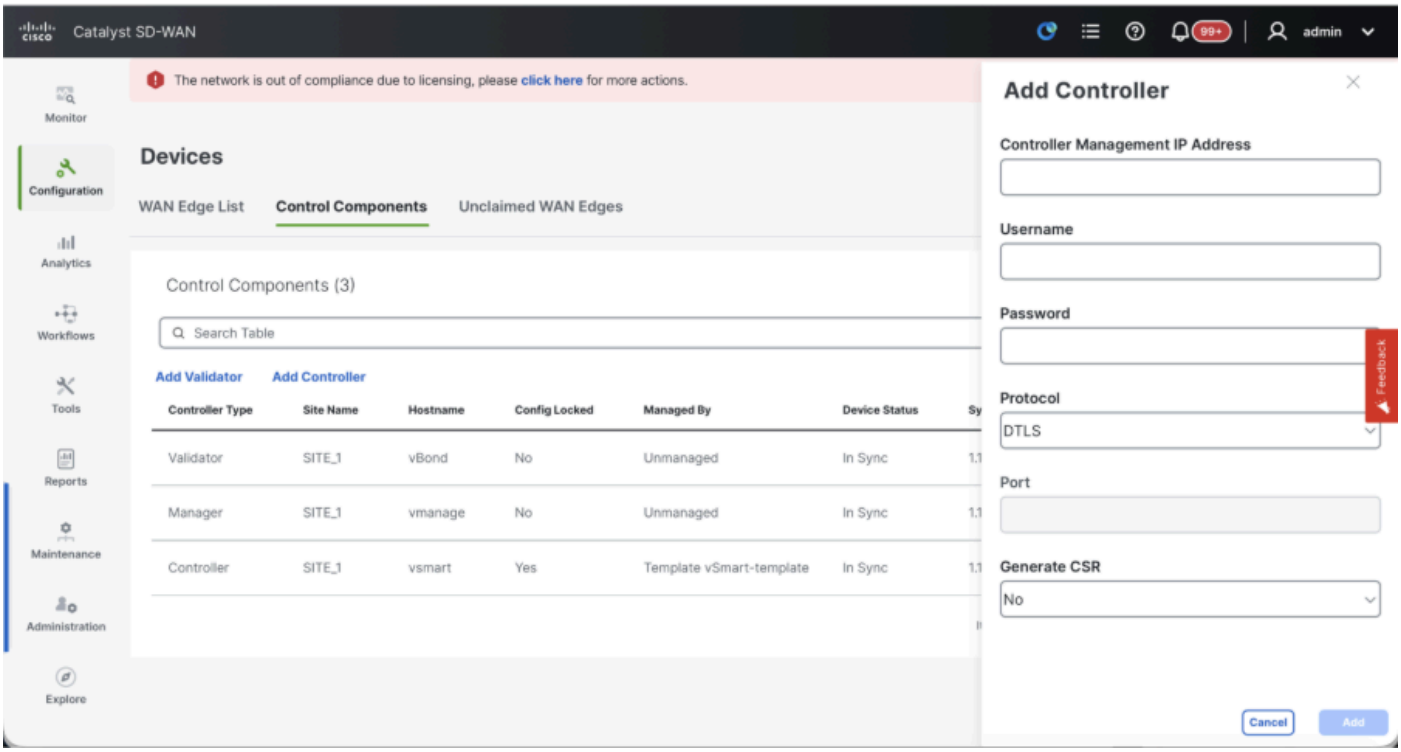


- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vBond.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vBonds, repita los mismos pasos.

Incorporación de vSmart/Controller

- Haga clic en Add vSmart en el caso de 20.12 vManage o Add Controller en el caso de 20.15/20.18 vManage.
- Se abre una ventana emergente, introduzca la IP de transporte VPN 0 de vSmart, a la que se puede acceder desde vManage.
- Compruebe la disponibilidad mediante ping si se permite desde la CLI de vManage a vSmart IP.
- Introduzca las credenciales de usuario de vSmart Note que necesitamos para utilizar las credenciales de administrador de vSmart o una parte de usuario del grupo netadmin.
- Puede comprobarlo en la CLI de vSmart.
- Establezca el protocolo en TLS, si pretendemos utilizar TLS para routers para establecer conexiones de control con vSmart. Esta configuración también debe configurarse en CLI de nodos vsmarts y vManage.
- Elija Sí en el menú desplegable "Generar CSR" si necesitamos instalar un nuevo certificado para vSmart.

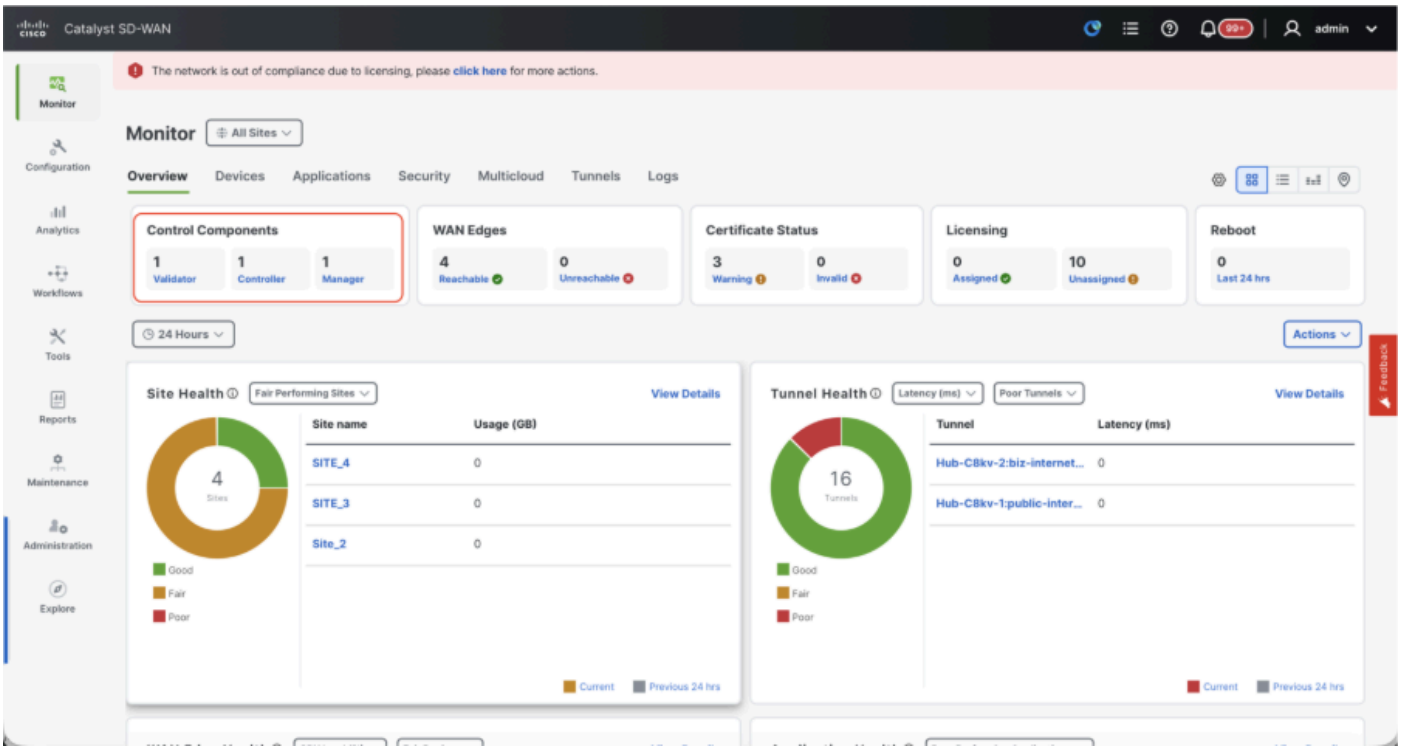
Nota: Si vSmart está detrás del dispositivo NAT/firewall, compruebe si la IP de la interfaz VPN 0 de vSmart se traduce a una IP pública y si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la IP de la interfaz VPN 0 en este paso.



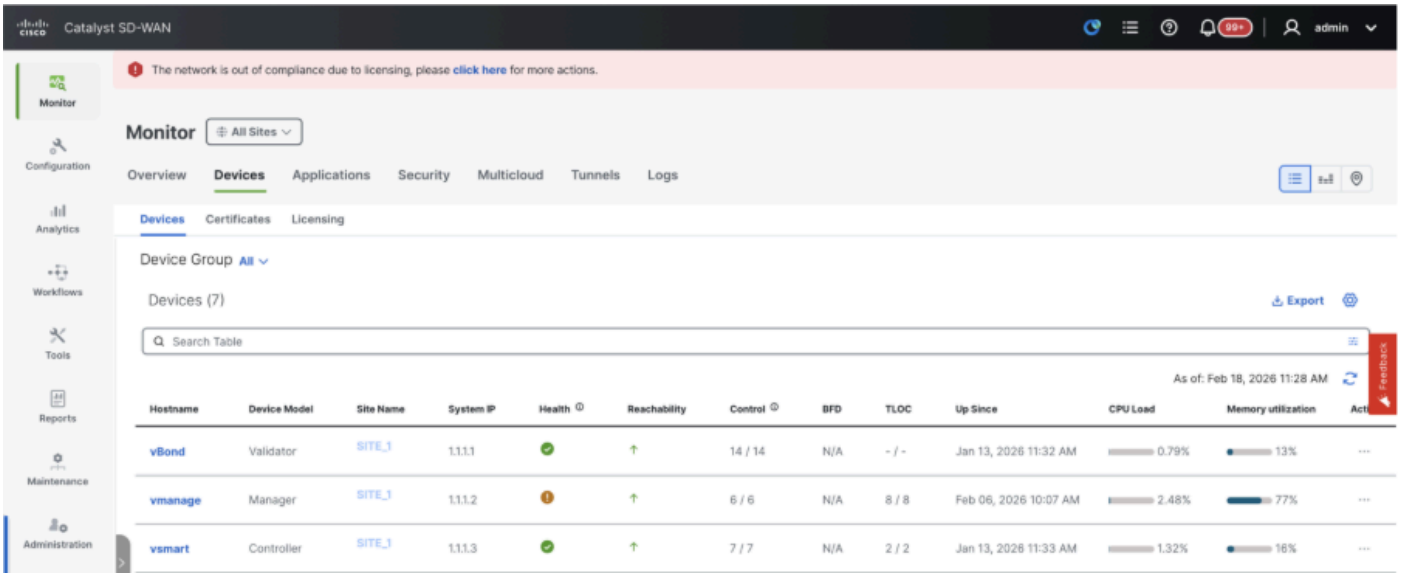
- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vSmart.
- Si selecciona Manual, firme manualmente el CSR mediante el portal PNP de Cisco accediendo a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN respectiva. Se aplica el mismo procedimiento si utilizamos Digicert y el certificado raíz de empresa.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- Si hay varios vsmarts, repita los mismos pasos.

Verificación

Una vez completados todos los pasos, verifique que todos los componentes de control sean accesibles en Monitor>Dashboard



- Haga clic en los componentes de control correspondientes y confirme que todos son accesibles.
- Navegue hasta Monitor > Devices y confirme que todos los componentes de control son accesibles.



Paso 3: Copia de seguridad/restauración de Config-db

Recopilar copia de seguridad de la base de datos de configuración de vManage y restaurar en otro nodo de vManage

Recopilar copia de seguridad de Configuration-DB:

- En el fabric SD-WAN que se utiliza actualmente, puede generar una copia de seguridad de la base de datos de configuración en las configuraciones de clúster vManage y vManage independientes.
- Para vManage independiente, vManage es el líder de la base de datos de configuración.

Confirme que configuration-db se esté ejecutando en el nodo vManage.

Puede verificar lo mismo mediante el comando request nms configuration-db status onvManageCLI. El resultado es como se muestra

```
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#
```

Utilice este comando para recopilar la copia de seguridad de la base de datos de configuración del nodo vManage del líder de la base de datos de configuración identificado.

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

El resultado esperado es el siguiente:

```
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#
```

- Tome nota de las credenciales de configuration-db si se ha actualizado.
- Si no conoce las credenciales de la base de datos de configuración, póngase en contacto con el TAC para recuperar las credenciales de la base de datos de configuración de los nodos de vManage existentes.

- Las credenciales de la base de datos de configuración predeterminada son username: neo4j y contraseña: contraseña

Restaurar copia de seguridad de Configuration-db en otro nodo de vManage

Copie la copia de seguridad de la base de datos de configuración en el directorio /home/admin/ de vManage mediante SCP.

Ejemplo de resultado del comando scp:

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

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

Para restaurar la copia de seguridad de la base de datos de configuración, primero debemos configurar las credenciales de la base de datos de configuración. Si sus credenciales de configuration-db son predeterminadas (neo4j/password), podemos saltarnos este paso.

Para configurar las credenciales de configuration-db, utilice el comando request nms configuration-db update-admin-user. Utilice el nombre de usuario y la contraseña que desee.

Tenga en cuenta que el servidor de aplicaciones de vManage se reinicia. Debido a lo cual, la interfaz de usuario de vManage se vuelve inaccesible durante un breve período de tiempo.

```
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#
```

Publicación en la que podemos continuar con la restauración de la copia de seguridad de la base de datos de configuración:

Podemos utilizar el comando request nms configuration-db restore path /home/admin/< > para restaurar la base de datos de configuración en el nuevo vManage:

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

Una vez restaurada la base de datos de configuración, asegúrese de que se puede acceder a la interfaz de usuario de vManage. Espere unos 5 minutos e intente acceder a la interfaz de usuario.

Una vez que haya iniciado sesión correctamente en la interfaz de usuario, asegúrese de que la lista de routers periféricos, la plantilla, las políticas y el resto de las configuraciones que estaban presentes en la interfaz de usuario de vManage anterior o existente se reflejan en la nueva interfaz de usuario de vManage.

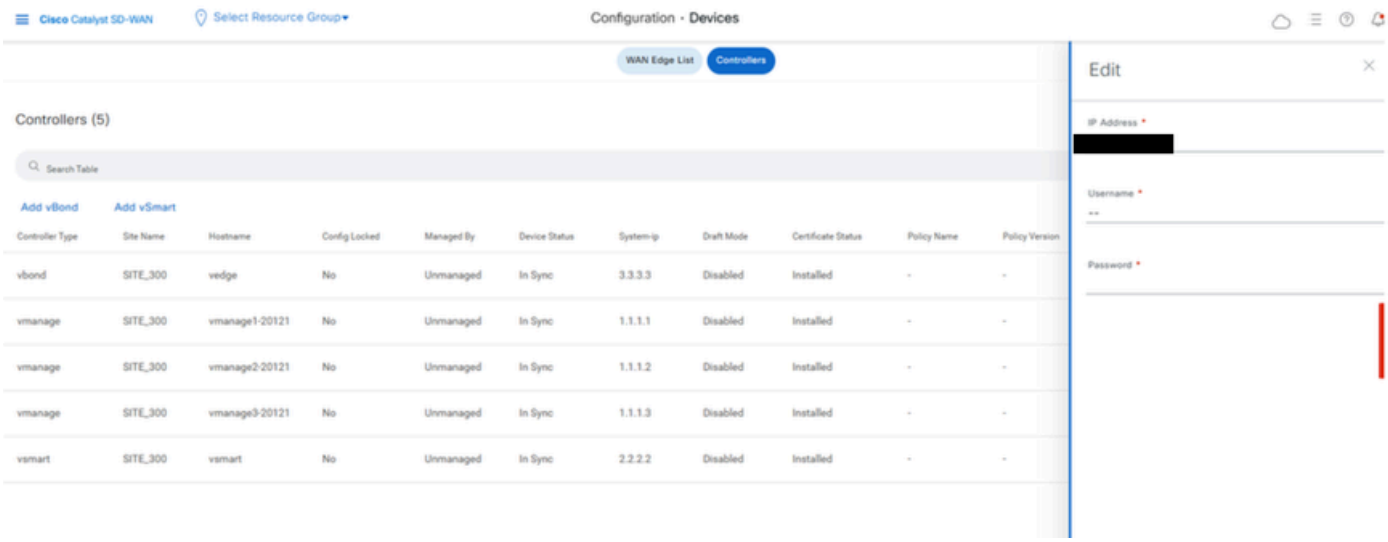
Paso 4: Reautenticación de controladores e invalidación de controladores antiguos

Una vez restaurada la base de datos de configuración, necesitamos volver a autenticar todos los nuevos controladores (vmanage/vsmart/vbond) en el fabric.

Nota: En la producción real, si la IP de interfaz utilizada para la reautenticación es la IP de interfaz de túnel, debe asegurarse de que se permite el servicio NETCONF en la interfaz de túnel de vManage, vSmart y vBond, así como en los firewalls a lo largo de la ruta. El puerto del firewall que se debe abrir es el puerto TCP 830 como regla bidireccional desde el clúster DR a todos los vBonds y vsmarts.

En vmanage UI, haga clic en Configuration > Devices > Controllers

- Haga clic en los tres puntos cerca de cada controlador y haga clic en Editar



- Reemplace la dirección ip (system-ip of the controller) por la dirección ip transport vpn 0 (tunnel interface). Introduzca el nombre de usuario y la contraseña y haga clic en Guardar
- Haga lo mismo con todos los nuevos controladores del fabric

Sincronizar la cadena de certificados raíz

Una vez que todos los controladores estén incorporados, complete este paso:

En cualquier servidor Cisco SD-WAN Manager del clúster recién activo, realice estas acciones:

Ingrese este comando para sincronizar el certificado raíz con todos los dispositivos Cisco Catalyst SD-WAN en el agrupamiento recientemente activo:

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

Ingrese este comando para sincronizar el UUID de Cisco SD-WAN Manager con el Validador de Cisco SD-WAN:

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

Una vez restaurado el fabric y activadas las sesiones de control y bfd para todos los bordes y controladores del fabric, debemos invalidar los controladores antiguos (vmanage/vsmart/vbond) de la interfaz de usuario

- En vmanage UI, haga clic en Configuration > Certificates > Controllers
- Haga clic en Controladores
- Haga clic en los tres puntos del lado derecho del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en invalidar
- Haga clic en enviar a vbond
- En vmanage UI, haga clic en Configuration > Devices > Controllers
- Haga clic en los tres puntos situados en el lado derecho del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en Eliminar

Paso 5: Registrar cheques

Nota: Continúe con la sección Post Checks (Comprobaciones posteriores) que se muestra aquí, que es común a todas las combinaciones de implementación.

Combinación 2: vManage independiente + DR de nodo único

Instancias necesarias:

- 1 vManage (principal, COMPUTE_AND_DATA)
- 1 vManage (DR en espera, COMPUTE_AND_DATA)
- 1 o más vBond
- 1 o más vSmart

Pasos:

1. Abra todas las instancias mediante los pasos comunes
2. Comprobaciones previas
3. Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage

4. Configuración DR de nodo único
5. Copia de seguridad/restauración de Config-db
6. Registrar cheques

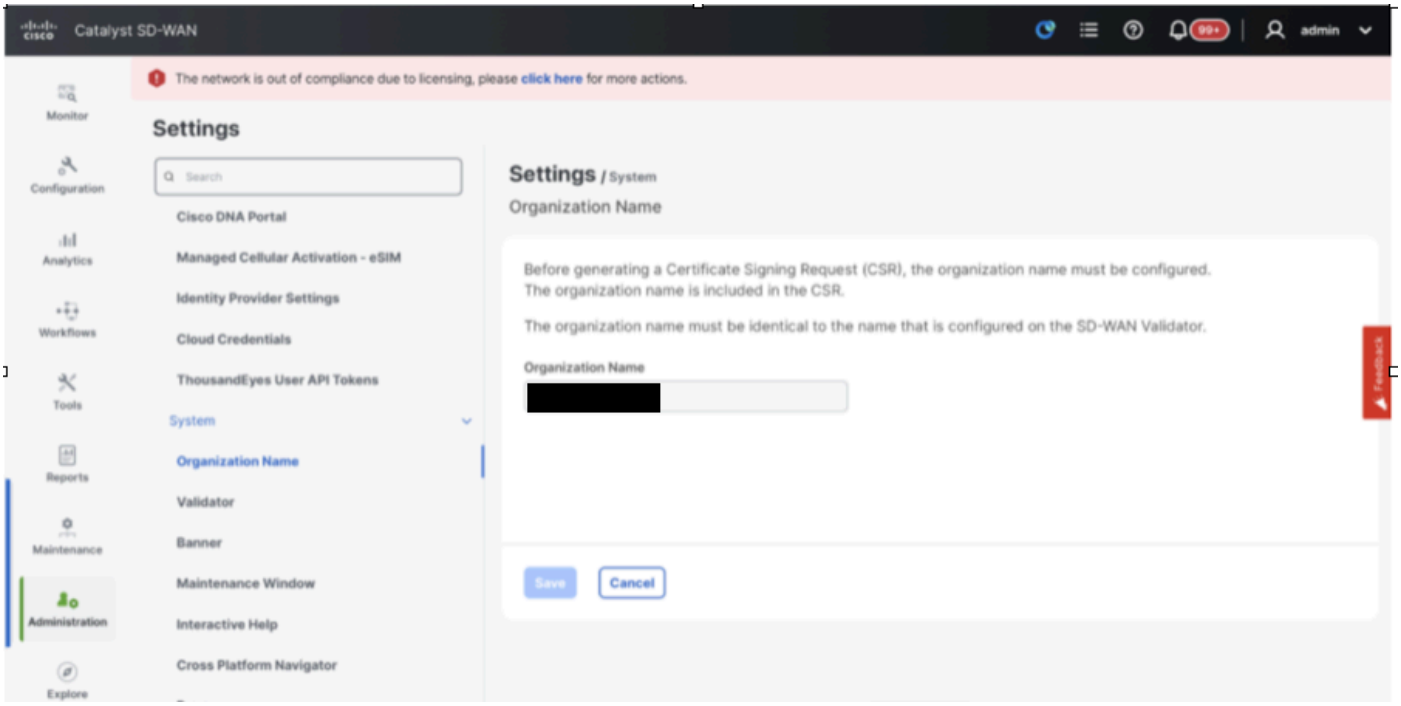
Paso 1: Comprobaciones previas

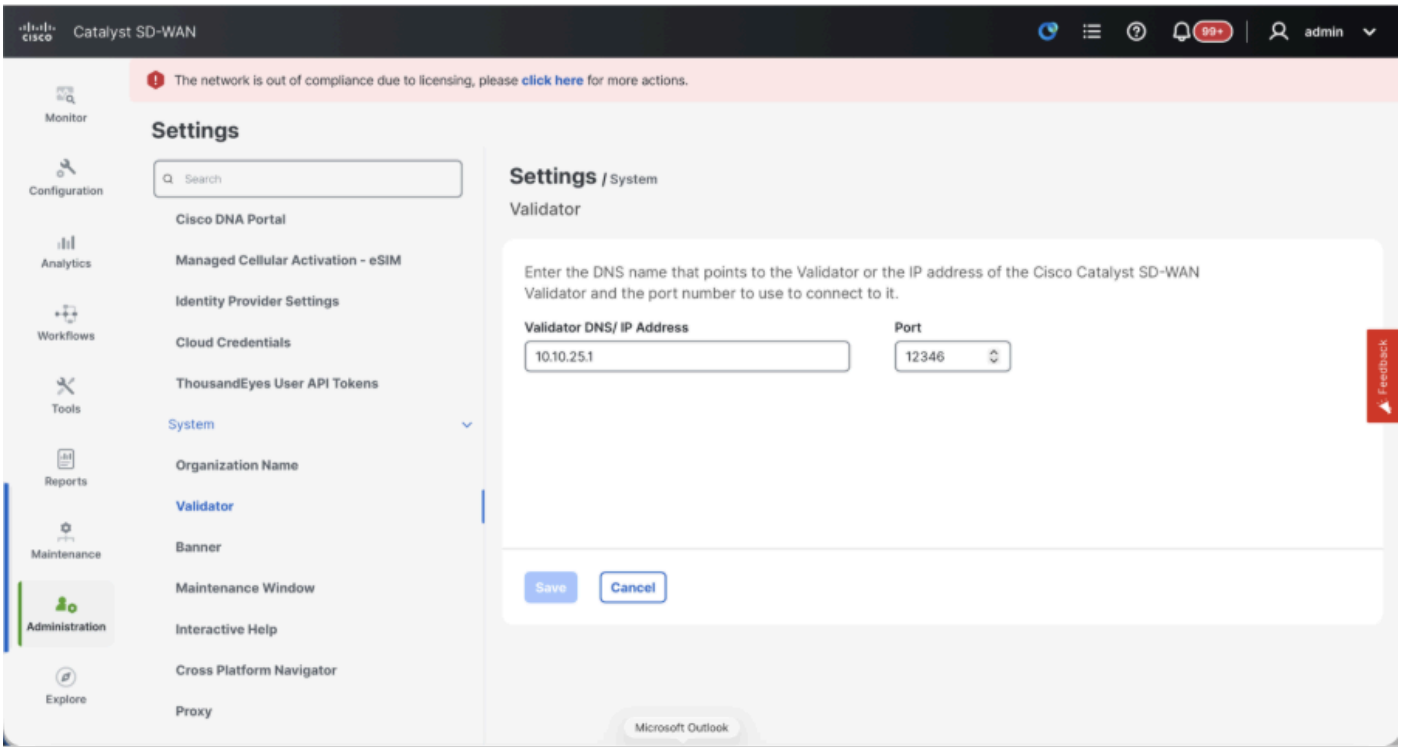
- Asegúrese de que el número de instancias activas de Cisco SD-WAN Manager sea idéntico al número de instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager ejecuten la misma versión de software.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager puedan alcanzar la dirección IP de administración del Cisco SD-WAN Validator.
- Asegúrese de que los certificados se hayan instalado en las instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que los relojes de todos los dispositivos Cisco Catalyst SD-WAN, incluidas las nuevas instancias de Cisco SD-WAN Manager instaladas, estén sincronizados.
- Asegúrese de que se haya configurado un nuevo conjunto de IP del sistema e ID del sitio en las instancias de Cisco SD-WAN Manager recién instaladas, junto con la misma configuración básica que el clúster activo.

Paso 2: Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage

Actualizar las configuraciones en la interfaz de usuario de vManage

- Una vez agregadas las configuraciones del paso 1 en la CLI de todos los controladores, podemos acceder a la interfaz de usuario web de vManage mediante la dirección URL https://<vmanage-ip> en el navegador. Utilice la dirección IP VPN 512 de los nodos vManage respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Navegue hasta Administration > Settings y complete estos pasos.
- Configure el nombre de la organización y la dirección URL/IP del validador/vBond. Configure el mismo valor que en la CLI del nodo vManage.
- En vManage 20.15/20.18, estas configuraciones están disponibles en la sección Sistema.

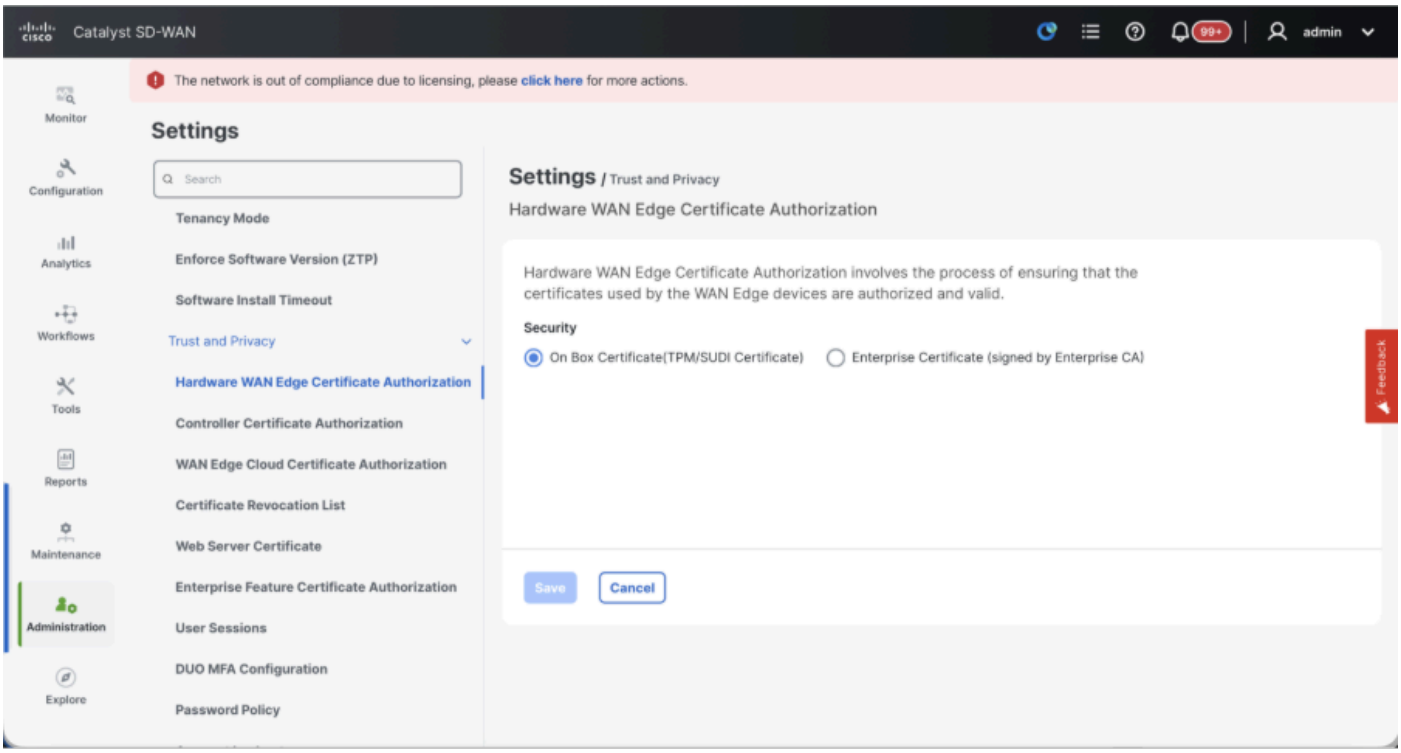




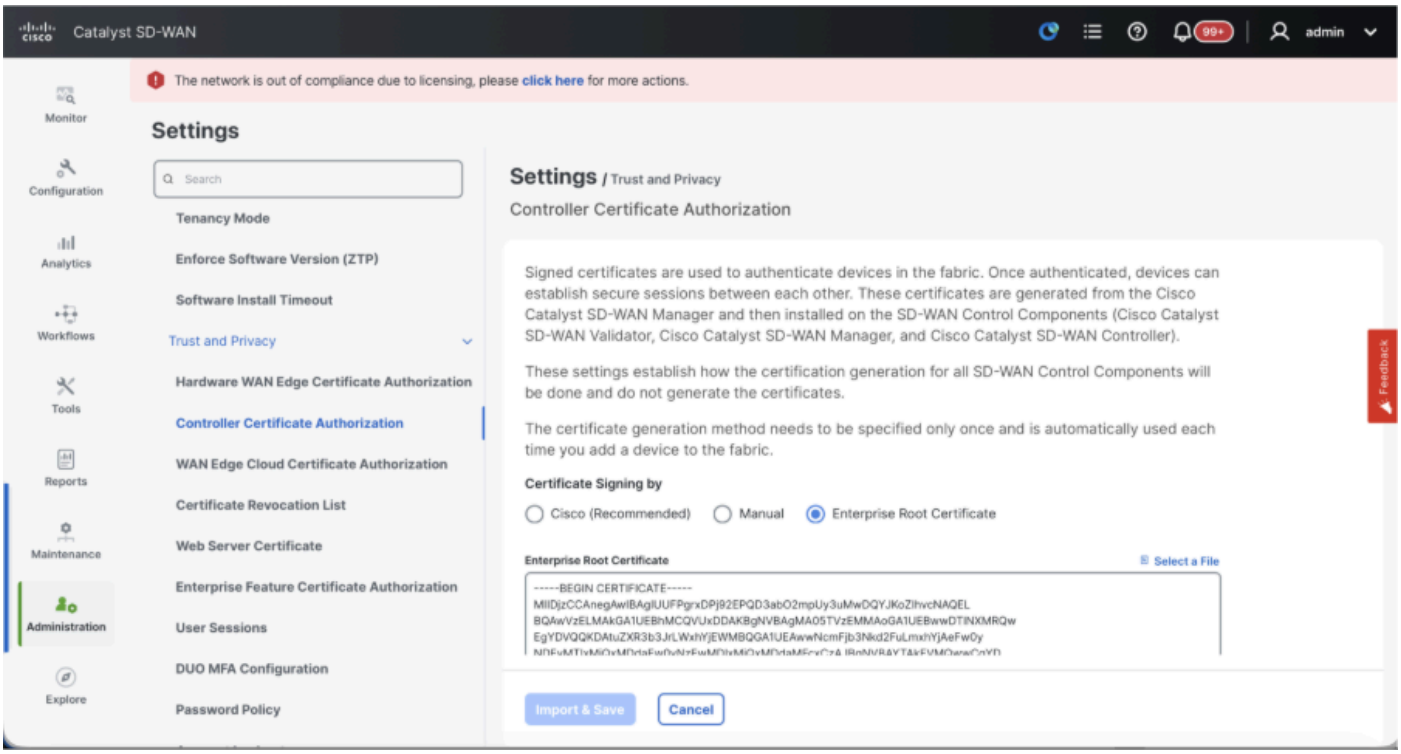
- Compruebe las configuraciones de la Autorización de certificados (CA), que decide la Autoridad de certificados utilizada para firmar los certificados. Podemos ver 3 opciones allí:

1. Autorización de certificado de extremo de WAN de hardware - Decide la CA para los routers periféricos SD-WAN de hardware.
    - Certificado en caja (certificado TPM/SUDI): con esta opción, el certificado preinstalado en el hardware del router se utiliza para establecer las conexiones de control (conexiones TLS/DTLS)
    - Certificado de empresa (firmado por la CA de empresa): con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe

actualizarse aquí.

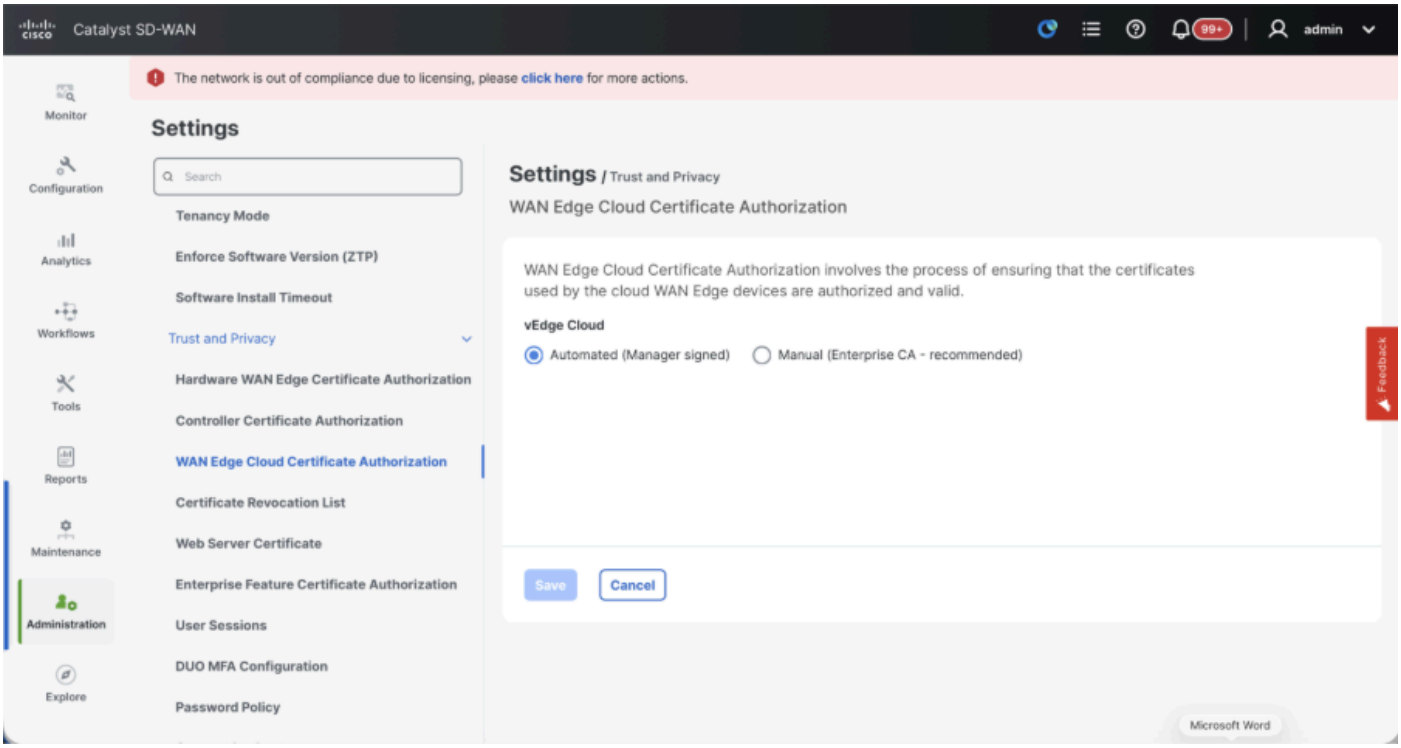


2. Autorización de certificado de controlador: decide la CA para los controladores SD-WAN.
    - Cisco (recomendado): los controladores utilizan los certificados firmados por Cisco PKI. vManage se pone en contacto automáticamente con el portal PNP mediante las credenciales de la cuenta inteligente configuradas en vManage y consigue que el certificado se firme y se instale en el controlador.
    - Manual: los controladores utilizan los certificados firmados por Cisco PKI. Firme manualmente el CSR mediante el portal Cisco PNP; para ello, acceda a la cuenta inteligente y la cuenta virtual de la superposición SD-WAN correspondiente.
    - Certificado raíz de empresa: con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

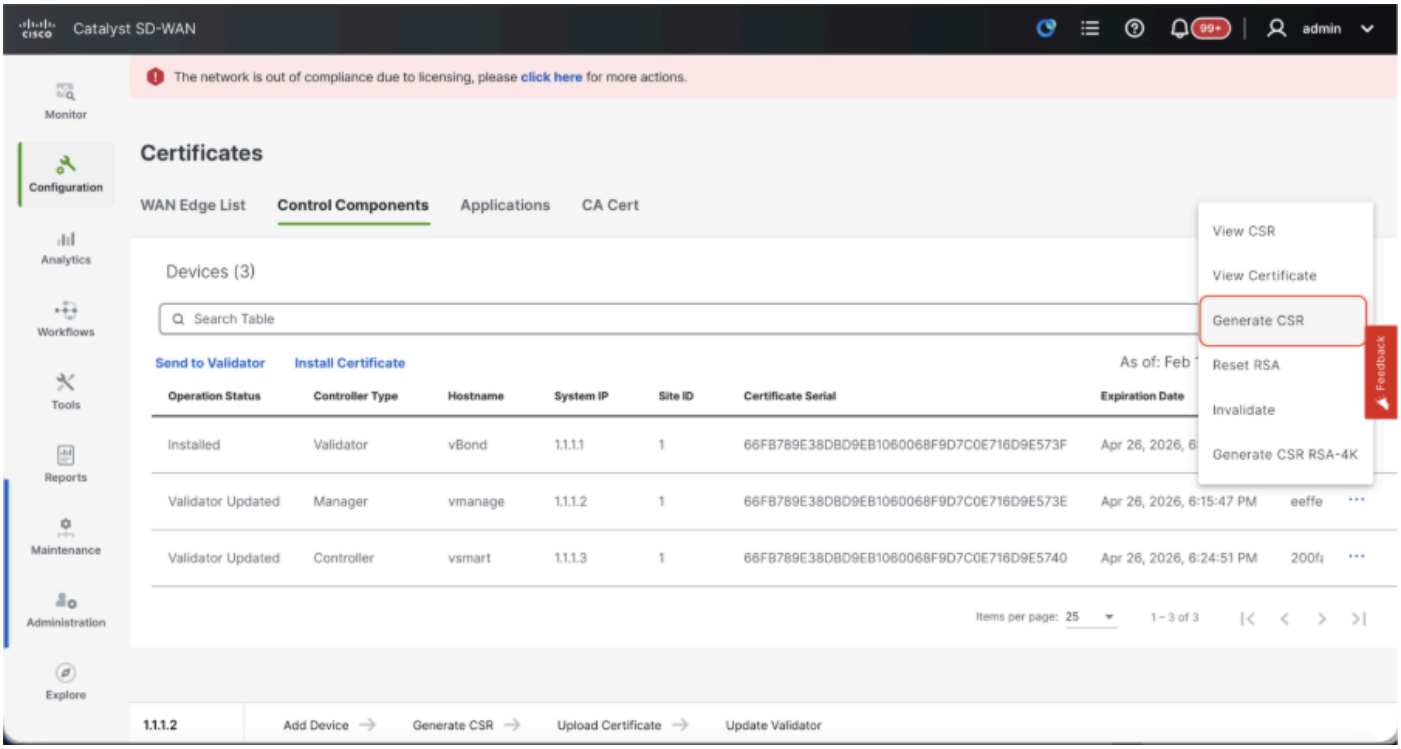


3. Autorización de certificado de nube de extremo de WAN: decide la CA para routers periféricos SD-WAN virtuales (CSR1000v, C8000v, nube vEdge)
    - Automatizado (vManage firmado): vManage firma automáticamente el CSR para los routers periféricos virtuales e instala el certificado en el router.
    - Manual (CA empresarial: recomendado): los routers virtuales utilizan certificados firmados por la autoridad de certificación empresarial de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

En este caso, si estamos utilizando nuestra propia CA, autoridad de certificación de empresa, elija Empresa.



- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers
- Haga clic en ... para Manager/vManage y haga clic en Generar CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.

Incorporación de vBond/Validator y vSmart/Controller a vManage

Vaya a Configuration > Devices > Control Components en caso de nodos vManage 20.15/20.18. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

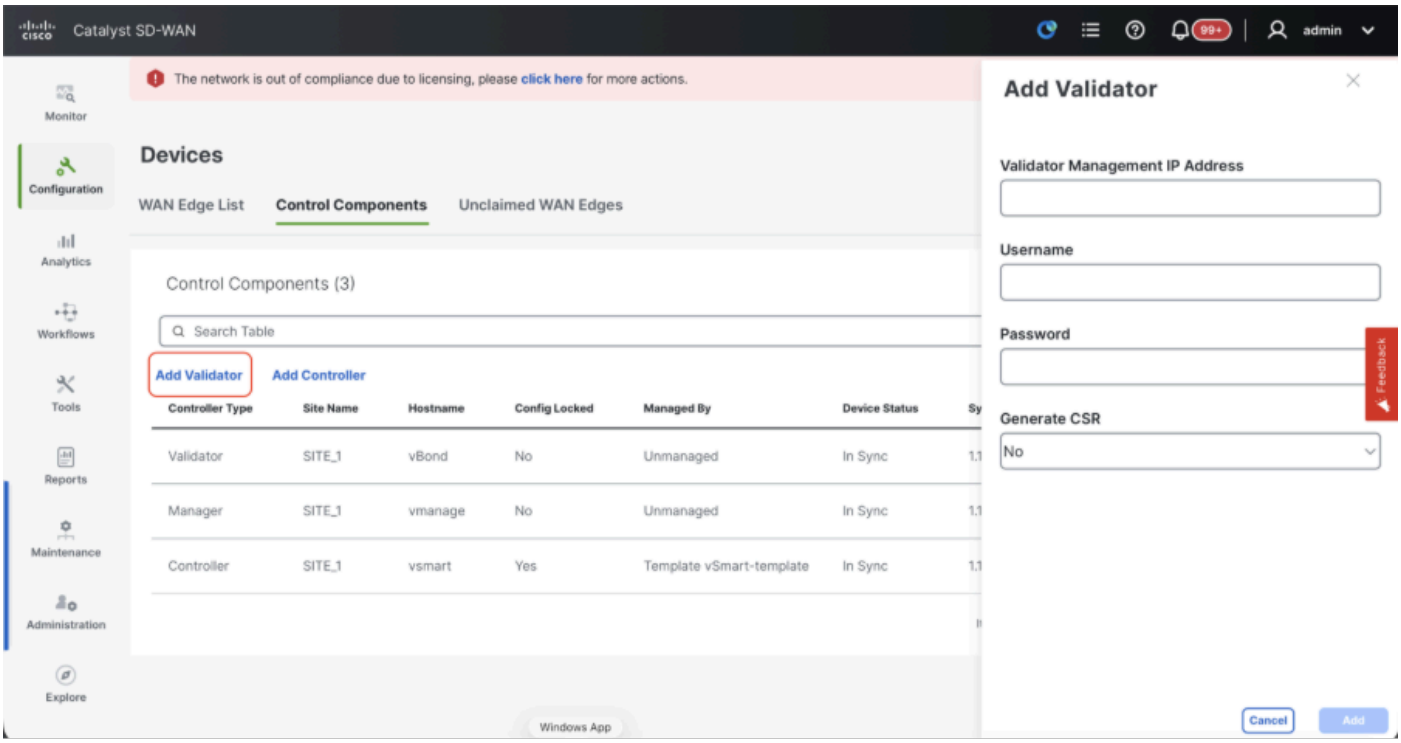
Incorporación de vBond/Validador

- Haga clic en AddvBonden caso de 20.12vManagerAgregar validadoren el caso de 20.15/20.18vManage. Se abre una ventana emergente, introduzca el IP de transporte VPN 0 de vBondque se puede alcanzar desde vManage.
- Verifique la disponibilidad mediante ping si se permite desde la CLI de vManagetovBondIP.

- Introduzca las credenciales de usuario de vBond.

Nota: Necesitamos usar las credenciales de administración de vBono una parte de usuario denetadmingroup. Puede verificarlo en la CLI de thevBond. Elija Sí en el menú desplegable de "Generar CSR" si necesitamos instalar un nuevo certificado para vBond

Nota: Si vBond está detrás de un dispositivo NAT/firewall, verifique si la IP de la interfaz VPN 0 de vBond se traduce a una IP pública. Si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la interfaz VPN 0 en este paso

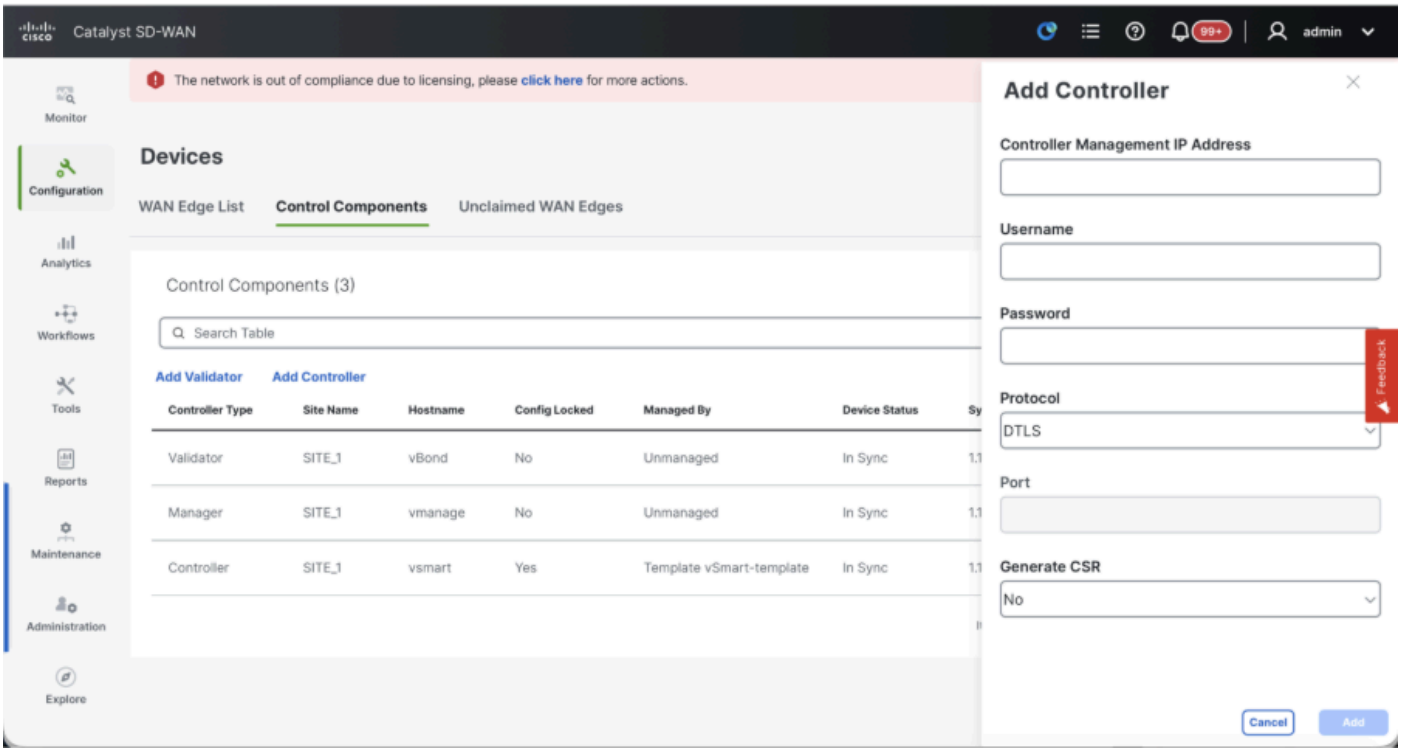


- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vBond.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vBonds, repita los mismos pasos.

Incorporación de vSmart/Controller

- Haga clic en Add vSmart en el caso de 20.12 vManage o Add Controller en el caso de 20.15/20.18 vManage.
- Se abre una ventana emergente, introduzca la IP de transporte VPN 0 de vSmart, a la que se puede acceder desde vManage.
- Compruebe la disponibilidad mediante ping si se permite desde la CLI de vManage a vSmart IP.
- Introduzca las credenciales de usuario de vSmart Note que necesitamos para utilizar las credenciales de administrador de vSmart o una parte de usuario del grupo netadmin.
- Puede comprobarlo en la CLI de vSmart.
- Establezca el protocolo en TLS, si pretendemos utilizar TLS para routers para establecer conexiones de control con vSmart. Esta configuración también debe configurarse en CLI de nodos vsmarts y vManage.
- Elija Sí en el menú desplegable "Generar CSR" si necesitamos instalar un nuevo certificado para vSmart.

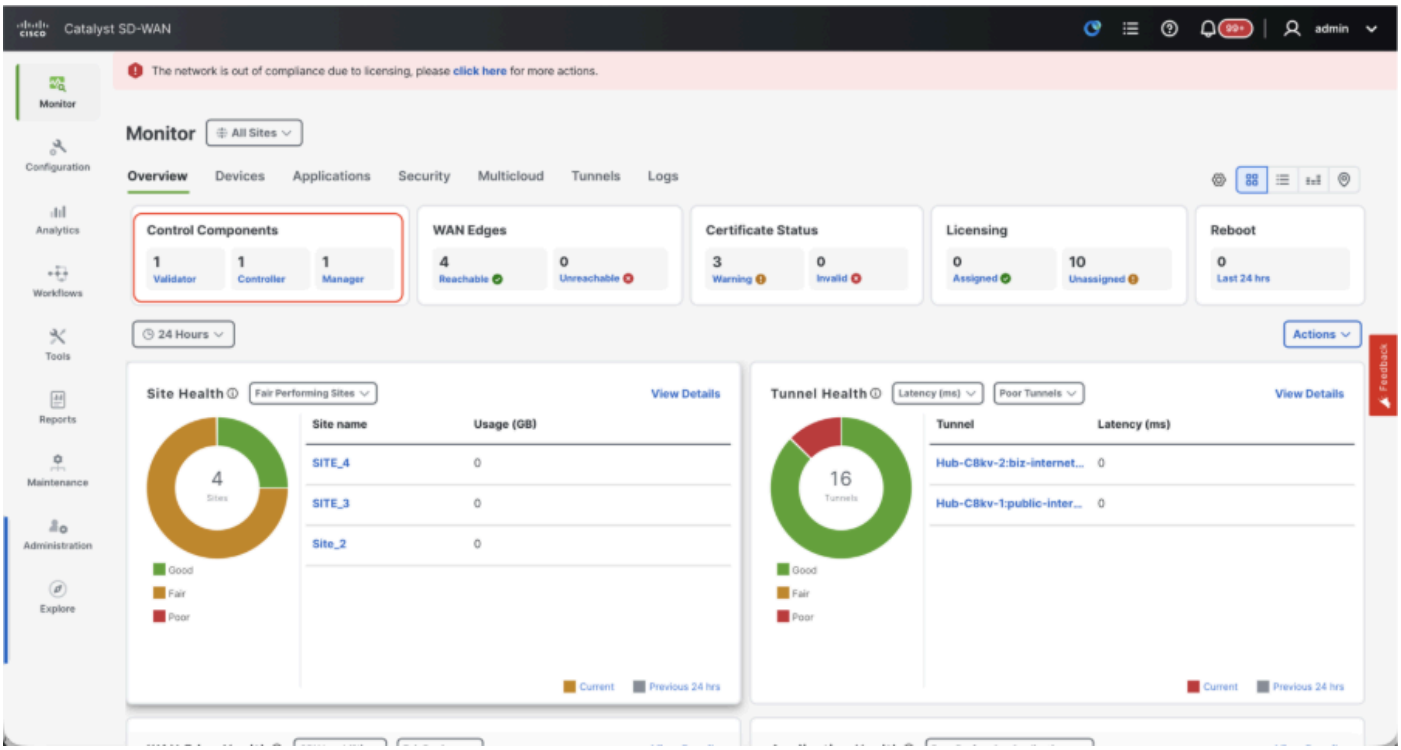
Nota: Si vSmart está detrás del dispositivo NAT/firewall, compruebe si la IP de la interfaz VPN 0 de vSmart se traduce a una IP pública y si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la IP de la interfaz VPN 0 en este paso.



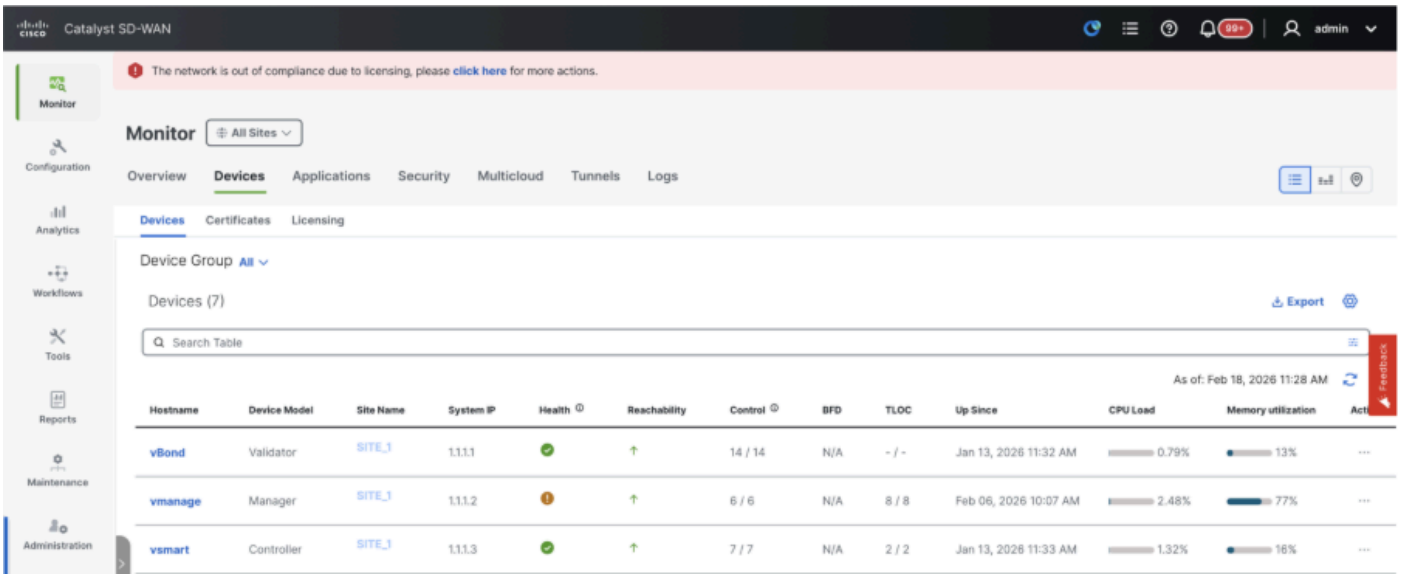
- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vSmart.
- Si selecciona Manual, firme manualmente el CSR mediante el portal PNP de Cisco accediendo a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN respectiva. Se aplica el mismo procedimiento si utilizamos Digicert y el certificado raíz de empresa.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- Si hay varios vsmarts, repita los mismos pasos.

Verificación

Una vez completados todos los pasos, verifique que todos los componentes de control sean accesibles en Monitor>Dashboard



- Haga clic en los componentes de control correspondientes y confirme que todos son accesibles.
- Navegue hasta Monitor > Devices y confirme que todos los componentes de control son accesibles.



Paso 3: Copia de seguridad/restauración de Config-db

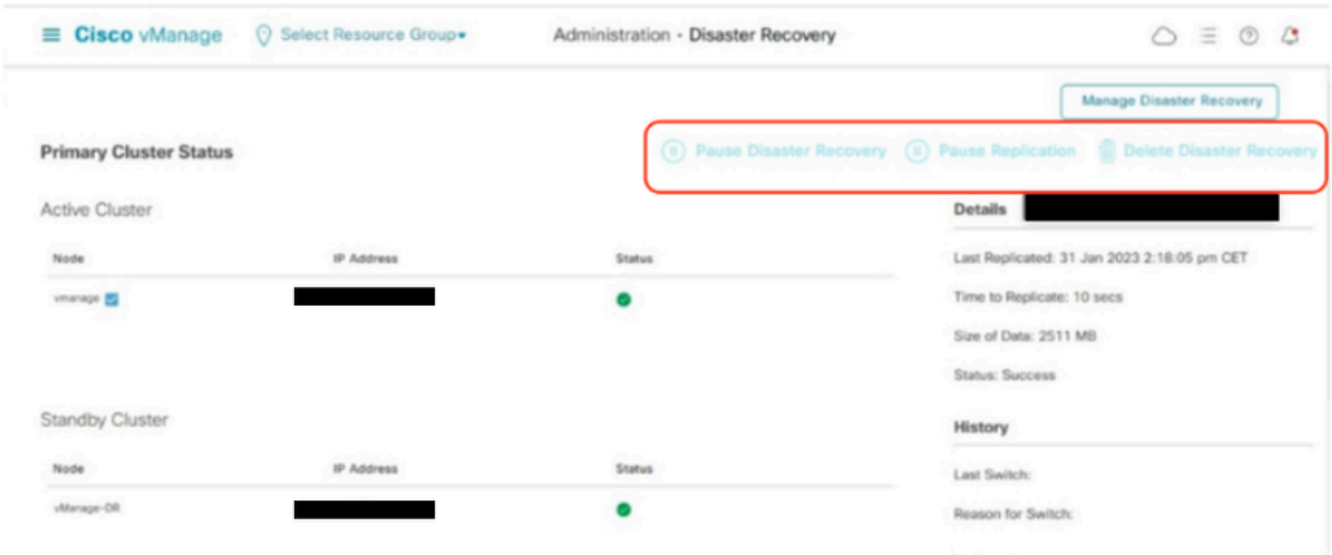
Recopilar copia de seguridad de la base de datos de configuración de vManage y restaurar en otro nodo de vManage

---

Nota: Mientras recopila la copia de seguridad de la base de datos de configuración del nodo de vManage existente que tiene habilitada la recuperación ante desastres, asegúrese de que se recopila después de pausar y eliminar la recuperación ante desastres de ese nodo.

Confirme que no hay replicación de recuperación ante desastres en curso. Vaya a Administration > Disaster Recovery y asegúrese de que el estado es Correcto y no está en un estado transitorio, como Importación pendiente, Exportación pendiente o Descarga pendiente. Si el estado no es correcto, póngase en contacto con Cisco TAC y asegúrese de que la replicación es correcta antes de proceder a pausar la recuperación ante desastres.

En primer lugar, detenga la recuperación ante desastres y asegúrese de que la tarea se ha completado. A continuación, elimine la recuperación ante desastres y confirme que la tarea se ha completado.



Póngase en contacto con el TAC de Cisco para asegurarse de que la recuperación ante desastres se ha limpiado correctamente.

Recopilar copia de seguridad de Configuration-DB:

- En el fabric SD-WAN que se utiliza actualmente, puede generar una copia de seguridad de la base de datos de configuración en las configuraciones de clúster vManage y vManage independientes.
- Para vManage independiente, vManage es el líder de la base de datos de configuración.

Confirme que configuration-db se esté ejecutando en el nodo vManage.

Puede verificar lo mismo mediante el comando request nms configuration-db statusonvManageCLI. El resultado es como se muestra

```
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#
```

Utilice este comando para recopilar la copia de seguridad de la base de datos de configuración del nodo vManage del líder de la base de datos de configuración identificado.

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

El resultado esperado es el siguiente:

```
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#
```

- Tome nota de las credenciales de configuration-db si se ha actualizado.
- Si no conoce las credenciales de la base de datos de configuración, póngase en contacto con el TAC para recuperar las credenciales de la base de datos de configuración de los nodos de vManage existentes.
- Las credenciales de la base de datos de configuración predeterminada son username: neo4j y contraseña: contraseña

Restaurar copia de seguridad de Configuration-db en otro nodo de vManage

Copie la copia de seguridad de la base de datos de configuración en el directorio /home/admin/ de vManage mediante SCP.

Ejemplo de resultado del comando scp:

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

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

Para restaurar la copia de seguridad de la base de datos de configuración, primero debemos configurar las credenciales de la base de datos de configuración. Si sus credenciales de configuration-db son predeterminadas (neo4j/password), podemos saltarnos este paso.

Para configurar las credenciales de configuration-db, utilice el comando request nms configuration-db update-admin-user.Use el nombre de usuario y la contraseña que desee.

Tenga en cuenta que el servidor de aplicaciones de vManage se reinicia. Debido a lo cual, la interfaz de usuario de vManage se vuelve inaccesible durante un breve período de tiempo.

```
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#
```

Publicación en la que podemos continuar con la restauración de la copia de seguridad de la base de datos de configuración:

Podemos utilizar el comando request nms configuration-db restore path /home/admin/< > para restaurar la base de datos de configuración en el nuevo vManage:

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

Una vez restaurada la base de datos de configuración, asegúrese de que se puede acceder a la interfaz de usuario de vManage. Espere unos 5 minutos e intente acceder a la interfaz de usuario.

Una vez que haya iniciado sesión correctamente en la interfaz de usuario, asegúrese de que la lista de routers periféricos, la plantilla, las políticas y el resto de las configuraciones que estaban presentes en la interfaz de usuario de vManage anterior o existente se reflejan en la nueva interfaz de usuario de vManage.

Paso 4: Configuración DR de nodo único

Consulte el paso 2: Comprobaciones previas en la combinación 2: vManage independiente + DR de nodo único y asegúrese de que hemos cumplido todos los requisitos antes de continuar con la activación de la recuperación ante desastres.

DR de nodo único

Prerequisites

- Asegúrese de que el nodo principal y el secundario estén accesibles mediante HTTPS en una VPN de transporte (VPN 0).
- Asegúrese de que el nodo principal y el nodo secundario de Cisco vManage ejecutan la misma versión de Cisco vManage.

Interfaz de clúster fuera de banda en VPN 0

1. Para cada instancia de vManage de un clúster, se requiere una tercera interfaz (enlace de clúster) además de las interfaces utilizadas para VPN 0 (transporte) y VPN 512 (gestión).
2. Esta interfaz se utiliza para la comunicación y la sincronización entre los servidores vManage del clúster.
3. Esta interfaz debe tener al menos 1 Gbps y una latencia de 4 ms o menos. Se recomienda una interfaz de 10 Gbps.
4. Ambos nodos de vManage deben poder comunicarse entre sí a través de esta interfaz: ya sea un segmento de capa 2 o a través del routing de capa 3.

- Asegúrese de que todos los servicios (application-server, configuration-db, messaging server, coordinator server y statistics-db) estén habilitados en ambos nodos de Cisco vManage.
- Distribuya todos los controladores, incluidos los Cisco vBond Orchestrators, entre los Data Centers principales y secundarios. Asegúrese de que los nodos de Cisco vManage que se distribuyen por estos Data Centers puedan acceder a estos controladores. Los controladores solo se conectan al nodo principal de Cisco vManage.
- Asegúrese de que no hay otras operaciones en proceso en el nodo activo (principal) y en el nodo de Cisco vManage en espera (secundario). Por ejemplo, asegúrese de que no haya servidores en proceso de actualización o que no haya plantillas en proceso de adjuntar plantillas a los dispositivos.

- Desactive el servidor proxy HTTP/HTTPS de Cisco vManage si está activado. Si no desactiva el servidor proxy, Cisco vManage intenta establecer la comunicación de recuperación ante desastres a través de la dirección IP del proxy, incluso si las direcciones IP del clúster fuera de banda de Cisco vManage son directamente accesibles. Puede volver a habilitar el servidor proxy HTTP/HTTPS de Cisco vManage una vez finalizado el registro de recuperación ante desastres.

- Antes de iniciar el proceso de registro de recuperación ante desastres, vaya a la ventana

Herramientas → Redescubrir red del nodo principal de Cisco vManage y vuelva a descubrir Cisco vBond Orchestrators.

Configuración

Configure las configuraciones CLI de todos los nodos de vManage que actúan como nodo de recuperación ante desastres

La configuración mínima para vManageantes del registro de recuperación ante desastres, como se muestra a continuación

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

Nota: Si utilizamos URL como dirección vBond, asegúrese de configurar las direcciones IP del servidor DNS en la configuración VPN 0 o asegúrese de que se puedan resolver.

Estas configuraciones son necesarias para habilitar la interfaz de transporte utilizada para establecer conexiones de control con los routers y el resto de los controladores

```
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
```

Configure también la interfaz de administración VPN 512para habilitar el acceso de administración

fuera de banda al controlador.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
commit
```

Configuración de la interfaz de servicio en DR vManage

Configure la interfaz de servicio en el nodo vManage. Esta interfaz se utiliza para la comunicación DR,

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Asegúrese de que la misma subred IP se utiliza para la interfaz de servicio en el vManage principal y el DR vManage

Actualizar las configuraciones en la interfaz de usuario de vManage

- Una vez agregadas las configuraciones en la CLI de todos los controladores, podemos

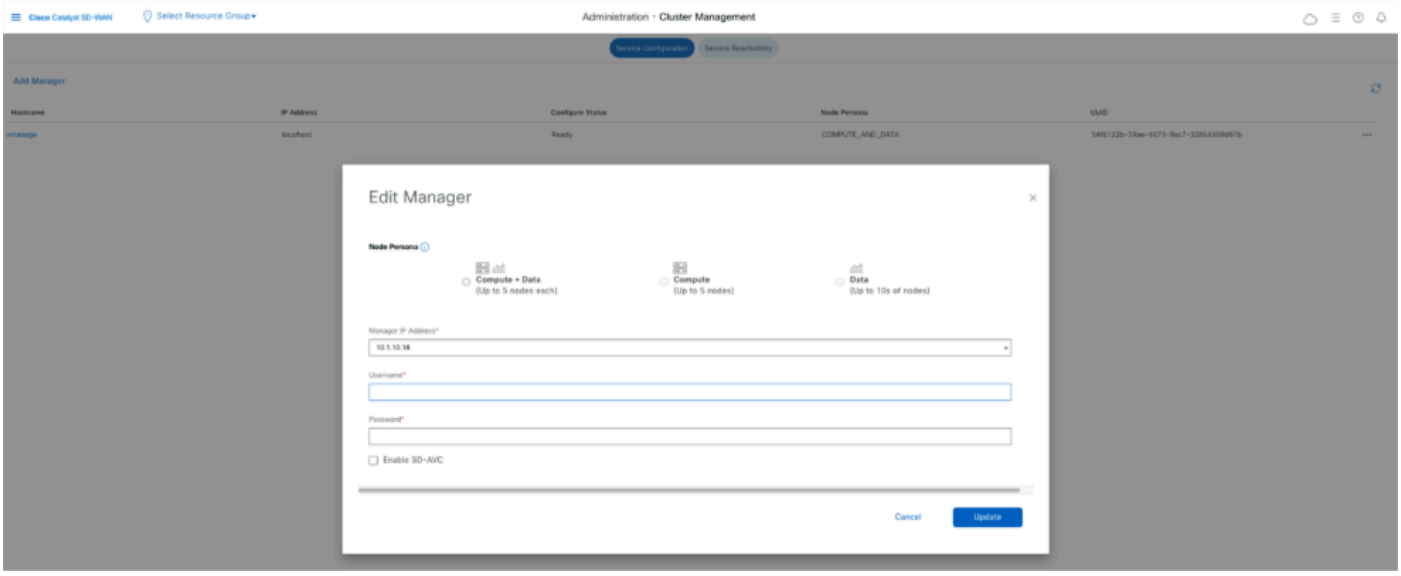
acceder a la interfaz de usuario web de vManage mediante la dirección URL https://<vmanage-ip> de su navegador. Utilice la dirección IP VPN 512 de los nodos vManage respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Navegue hasta Administration > Settings y complete estos pasos.
- Configure Organization name. Configure el mismo valor que en la CLI del nodo vManage.
- En vManage 20.15/20.18, estas configuraciones están disponibles en la sección Sistema.

Instalación del certificado en DR vManage

Continúe con los pasos dados en la sección Combinación 2: vManage independiente + DR de nodo único Paso 3: Configure la interfaz de usuario, los certificados y los controladores integrados de vManage para instalar el certificado en el vManage de recuperación ante desastres.

Adición de la configuración de recuperación ante desastres

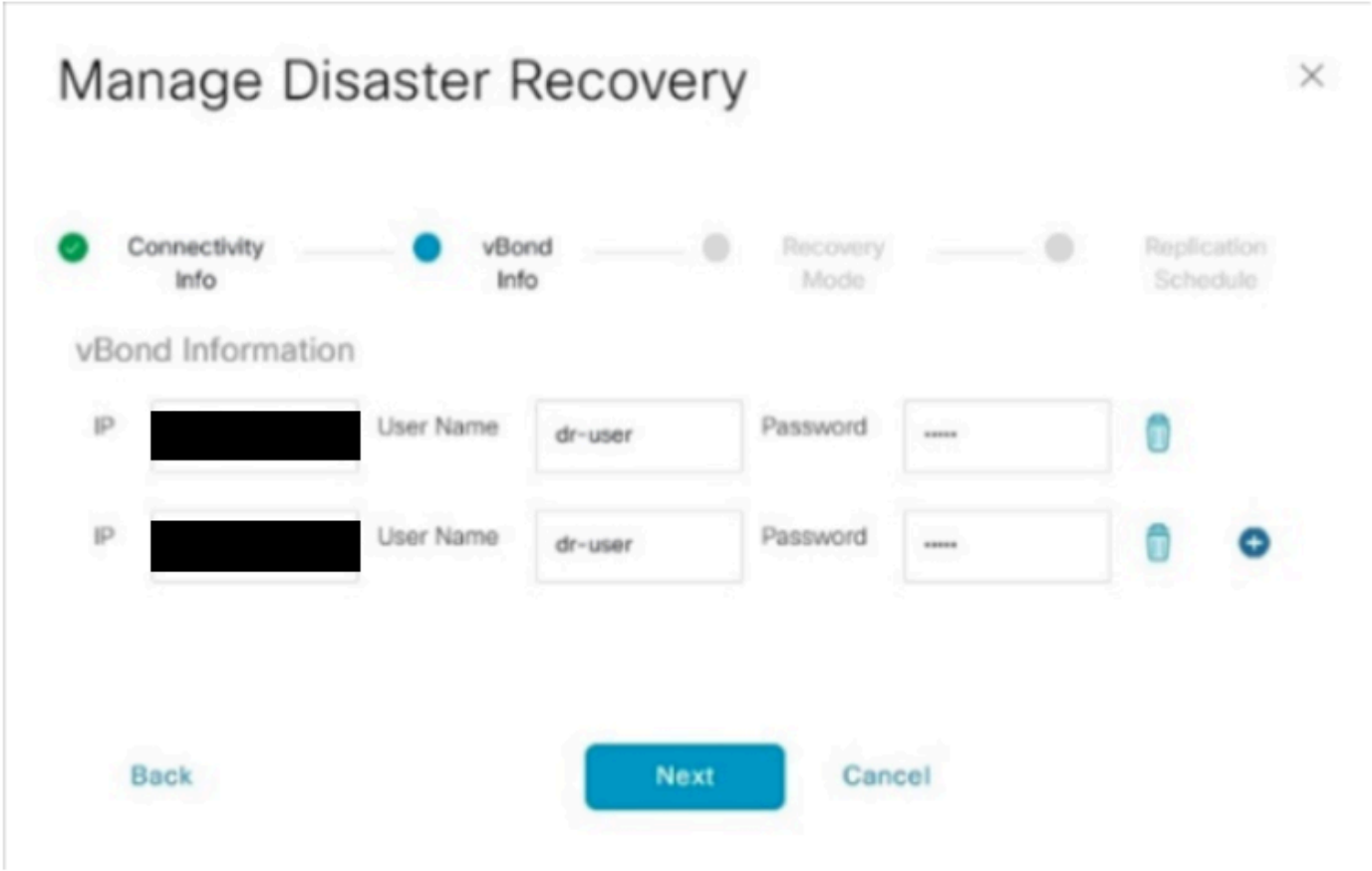
- Para ello, vaya a vManage principal.
- Vaya a Administration → Cluster Management e indique la dirección IP de la interfaz fuera de banda después de hacer clic en los tres puntos del lado derecho de la entrada de vManage e incluya el nombre de usuario y la contraseña. Se recomienda crear un usuario local independiente, por ejemplo dradmin, en vmanage principal y DR para esta configuración.



- VManage se reinicia después de este cambio.
- Una vez que aparezca el vManage principal, vaya a Administration → Disaster Recovery. Haga clic en "Administrar recuperación ante desastres".
- En la ventana emergente, rellene los detalles de vManage principal y secundaria.
- Las direcciones IP que se deben indicar son las direcciones IP de las interfaces de clúster fuera de banda (eth2).
- Las credenciales deben ser las de un usuario netadmin (dradmin) y no deben cambiarse una vez configurado el DR. Se puede utilizar una credencial de usuario local de vManage independiente para la recuperación ante desastres. Debemos asegurarnos de que el

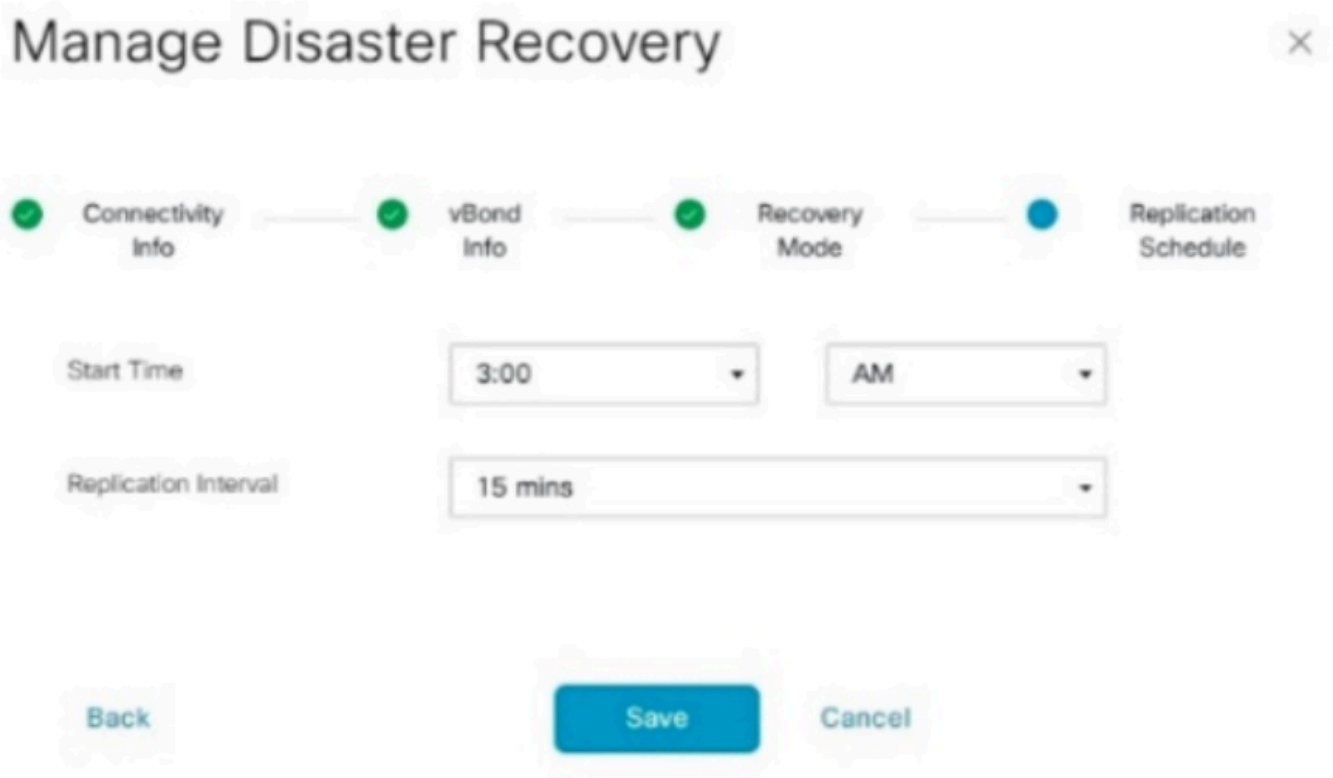
usuario local de vManage forma parte del grupo netadmin. Incluso las credenciales de administrador se pueden utilizar aquí.

- Una vez rellenado, haga clic en "Siguiente".
- Rellene los detalles de los controladores de vBond.
- Los controladores vBond deben ser accesibles en la dirección IP especificada a través de Netconf.
- Las credenciales deben ser las de un usuario netadmin (dradmin) y no deben cambiarse una vez configurado el DR.
- Para ello, se recomienda que vBond configure localmente este usuario dradmin o que utilice el usuario admin para agregar vBond.



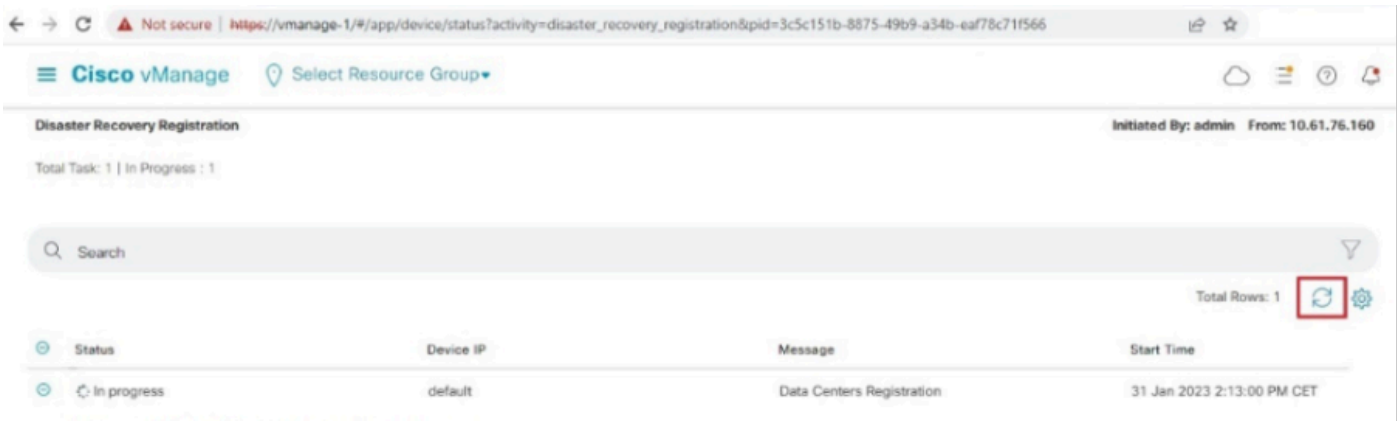
- Una vez rellenado, haga clic en "Siguiente".
- En el modo de recuperación, seleccione "Manual". Haga clic en "Siguiente".

En la programación de replicación, defina el valor de 'Intervalo de replicación'.Cada tiempo del intervalo de replicación, los datos se replican desde el principal vManage a vManage secundario El valor mínimo configurable es de 15 minutos.

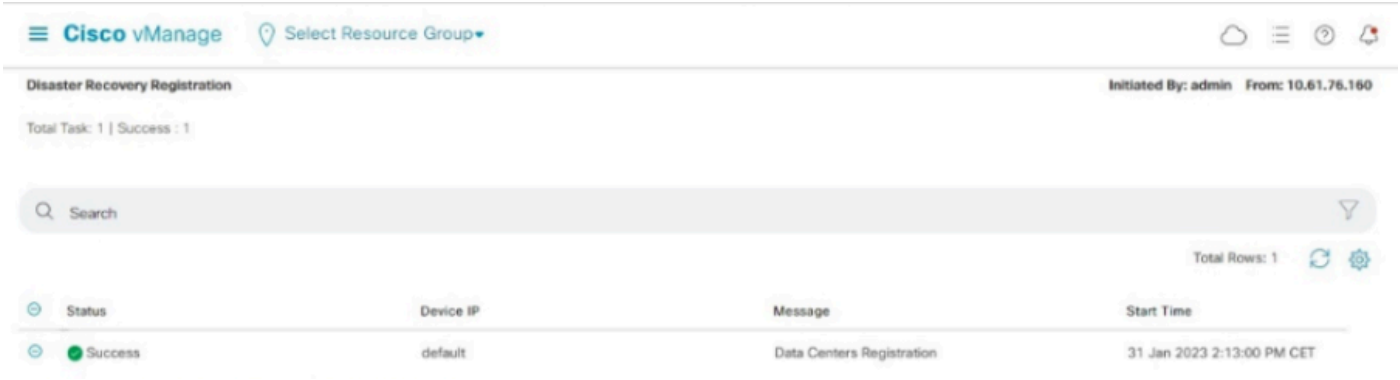


- Establezca el valor y haga clic en "Guardar".
- El registro de DR comienza ahora. Haga clic en el botón Actualizar para actualizar manualmente el estado y los registros de progreso. Este proceso puede tardar hasta 20-30

minutos.

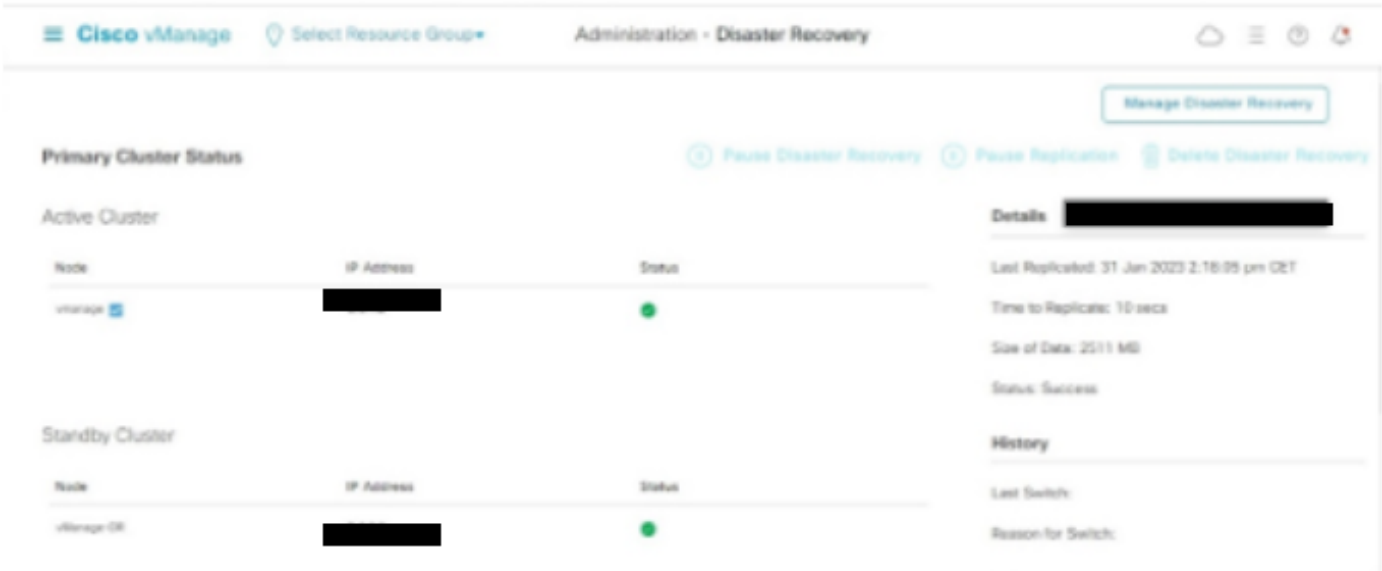


- Tenga en cuenta que la GUI de vManage se reinicia durante este proceso.
- Una vez finalizado, se debe ver el estado Correcto.



Verificación

Vaya aAdministración → Recuperación ante desastrespara ver el estado de Recuperación ante desastres y cuándo se replicaron los datos por última vez.



Paso 5: Reautenticación de controladores e invalidación de controladores antiguos

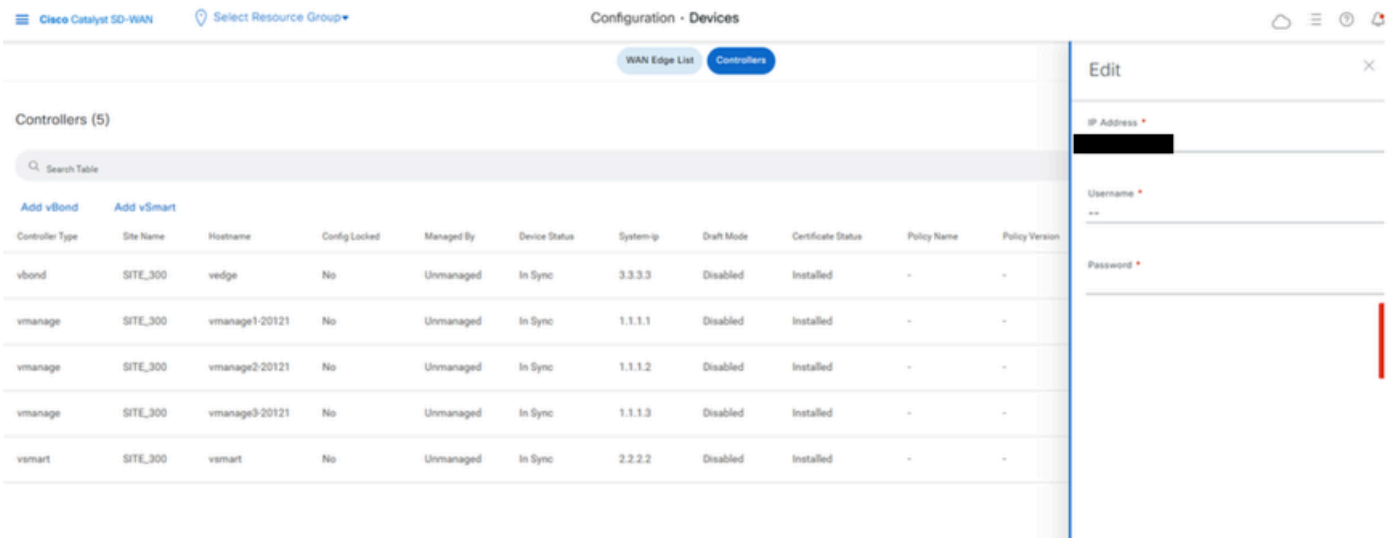
Una vez restaurada la base de datos de configuración, necesitamos volver a autenticar todos los nuevos controladores (vmanage/vsmart/vbond) en el fabric

---

Nota: En la producción real, si la IP de interfaz utilizada para la reautenticación es la IP de interfaz de túnel, debe asegurarse de que se permite el servicio NETCONF en la interfaz de túnel de vManage, vSmart y vBond, así como en los firewalls a lo largo de la ruta. El puerto del firewall que se debe abrir es el puerto TCP 830 como regla bidireccional desde el clúster DR a todos los vBonds y vsmarts .

En vmanage UI, haga clic en Configuration > Devices > Controllers

- Haga clic en los tres puntos cerca de cada controlador y haga clic en Editar



- Reemplace la dirección ip (system-ip of the controller) por la dirección ip transport vpn 0 (tunnel interface). Introduzca el nombre de usuario y la contraseña y haga clic en save (guardar)
- Haga lo mismo con todos los nuevos controladores del fabric

Sincronizar la cadena de certificados raíz

Una vez que todos los controladores estén incorporados, complete este paso:

En cualquier servidor Cisco SD-WAN Manager del clúster recién activo, realice estas acciones:

Ingrese este comando para sincronizar el certificado raíz con todos los dispositivos Cisco Catalyst SD-WAN en el agrupamiento recientemente activo:

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

Ingrese este comando para sincronizar el UUID de Cisco SD-WAN Manager con el Validador de

Cisco SD-WAN:

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

Una vez restaurado el fabric y activadas las sesiones de control y bfd para todos los bordes y controladores del fabric, debemos invalidar los controladores antiguos (vmanage/vsmart/vbond) de la interfaz de usuario

- En vmanage UI, haga clic en Configuration > Devices > Certificates .
- Haga clic en Controladores
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en invalidar
- Haga clic en enviar a vbond
- En vmanage UI, haga clic en Configuration > Devices > Controllers
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en Eliminar

Paso 6: Registrar cheques

Nota: Continúe con la sección Post Checks (Comprobaciones posteriores) que se muestra aquí, que es común a todas las combinaciones de implementación.

Combinación 3: Clúster vManage + Sin DR

Instancias necesarias:

- 3 vManage (clúster de 3 nodos, todos COMPUTE_AND_DATA) o 6 vManage (3 COMPUTE_AND_DATA + 3 DATA)
- 1 o más vBond
- 1 o más vSmart

Pasos:

1. Abra todas las instancias mediante los pasos comunes
2. Comprobaciones previas
3. Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage
4. Generar clúster de vManage
5. Copia de seguridad/restauración de Config-db
6. Registrar cheques

Paso 1: Comprobaciones previas

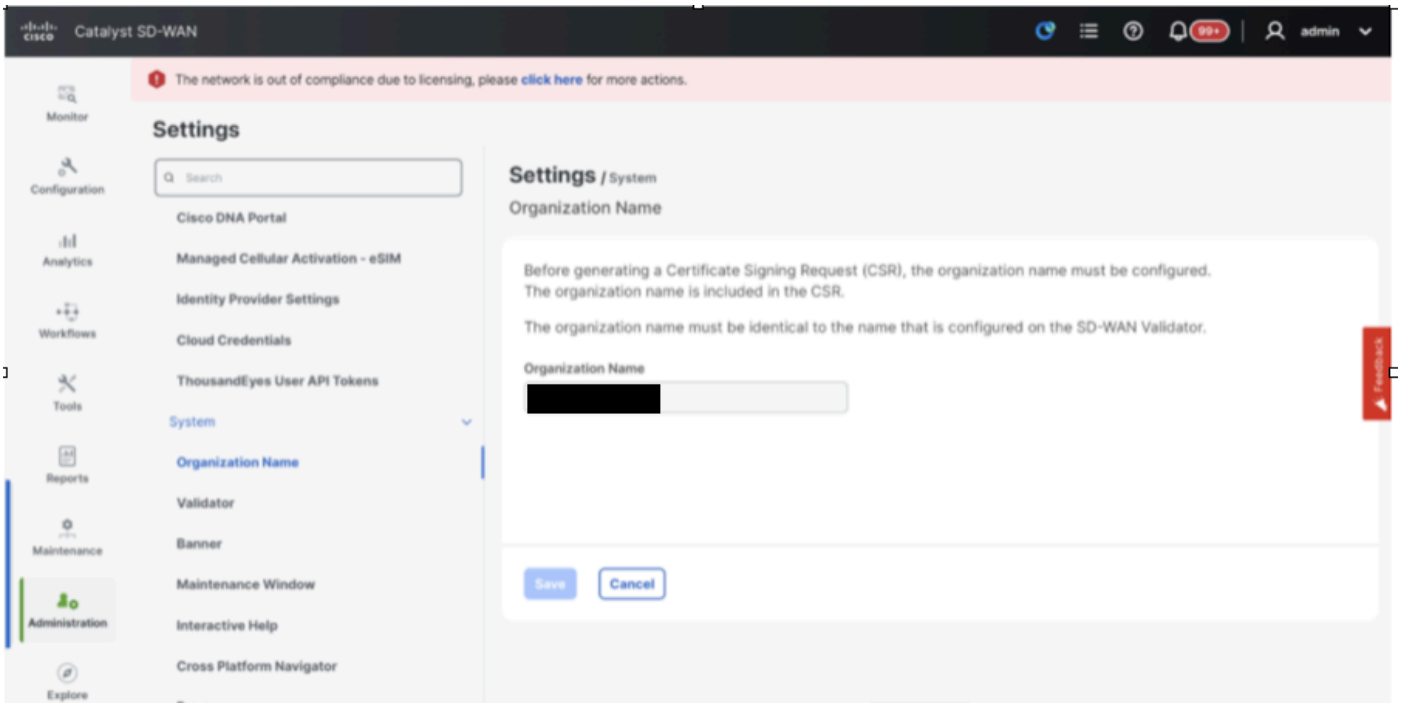
- Asegúrese de que el número de instancias activas de Cisco SD-WAN Manager sea idéntico al número de instancias de Cisco SD-WAN Manager recién instaladas.

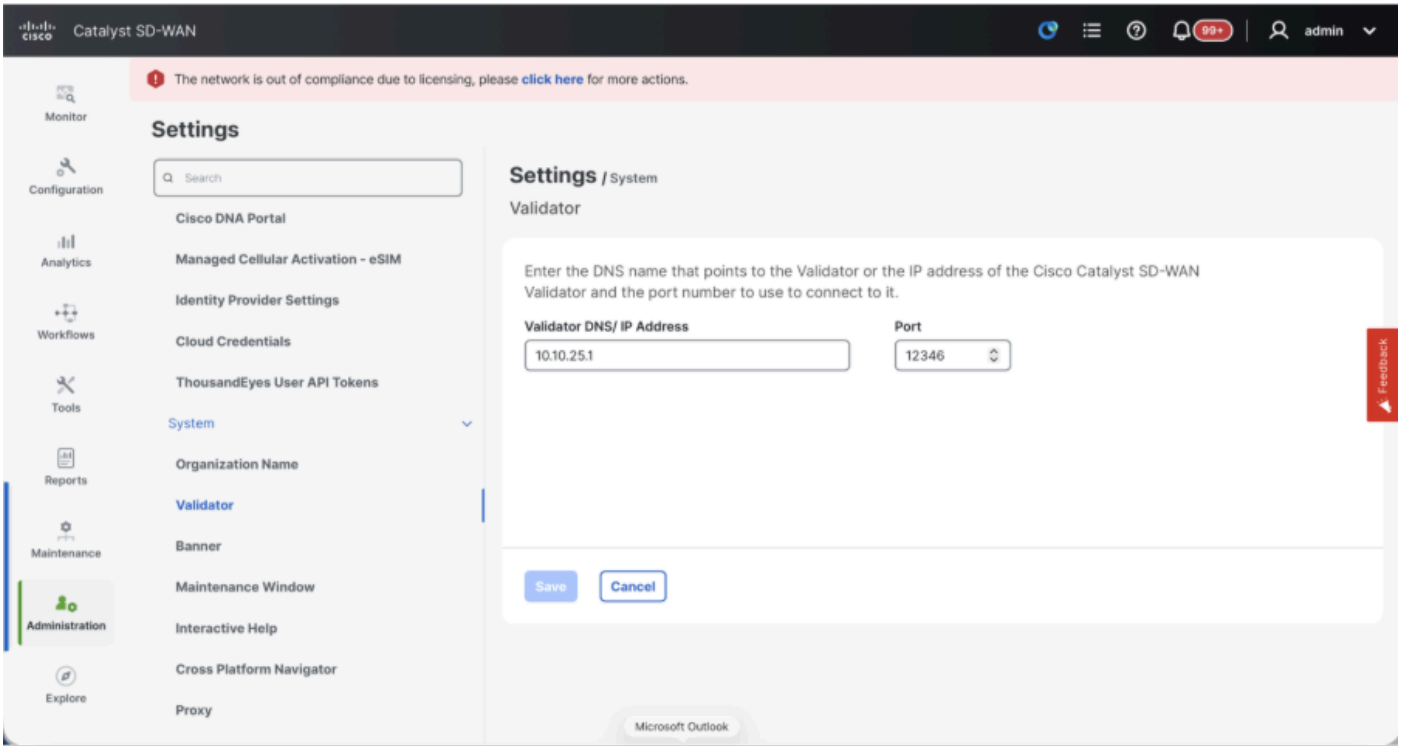
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager ejecuten la misma versión de software.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager puedan alcanzar la dirección IP de administración del Cisco SD-WAN Validator.
- Asegúrese de que los certificados se hayan instalado en las instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que los relojes de todos los dispositivos Cisco Catalyst SD-WAN, incluidas las nuevas instancias de Cisco SD-WAN Manager instaladas, estén sincronizados.
- Asegúrese de que se haya configurado un nuevo conjunto de IP del sistema e ID del sitio en las instancias de Cisco SD-WAN Manager recién instaladas, junto con la misma configuración básica que el clúster activo.

Paso 2: Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage

Actualizar las configuraciones en la interfaz de usuario de vManage

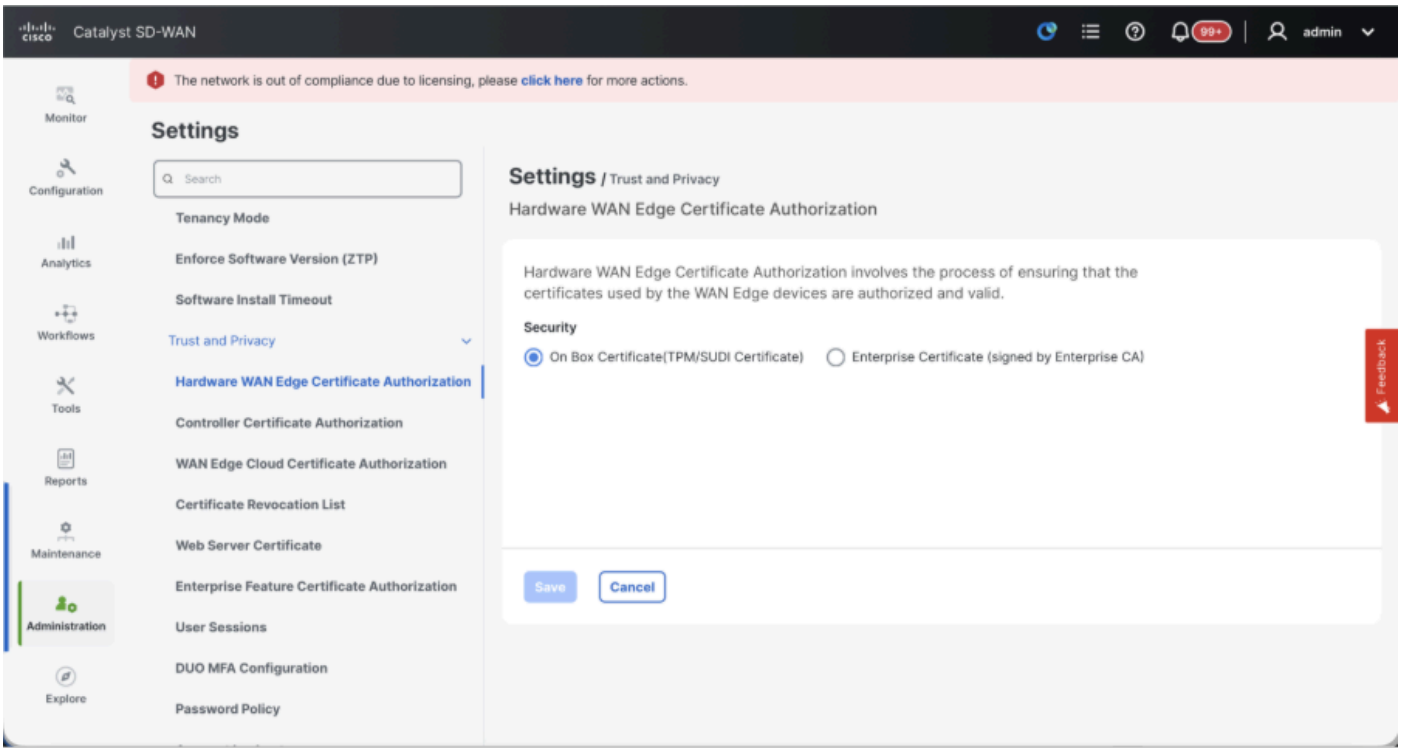
- Una vez agregadas las configuraciones del paso 1 en la CLI de todos los controladores, podemos acceder a la interfaz de usuario web de vManage mediante la dirección URL https://<vmanage-ip> en el navegador. Utilice la dirección IP VPN 512 de los nodos vManage respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Navegue hasta Administration > Settings y complete estos pasos.
- Configure el nombre de la organización y la dirección URL/IP del validador/vBond. Configure el mismo valor que en la CLI del nodo vManage.
- En vManage 20.15/20.18, estas configuraciones están disponibles en la sección Sistema.



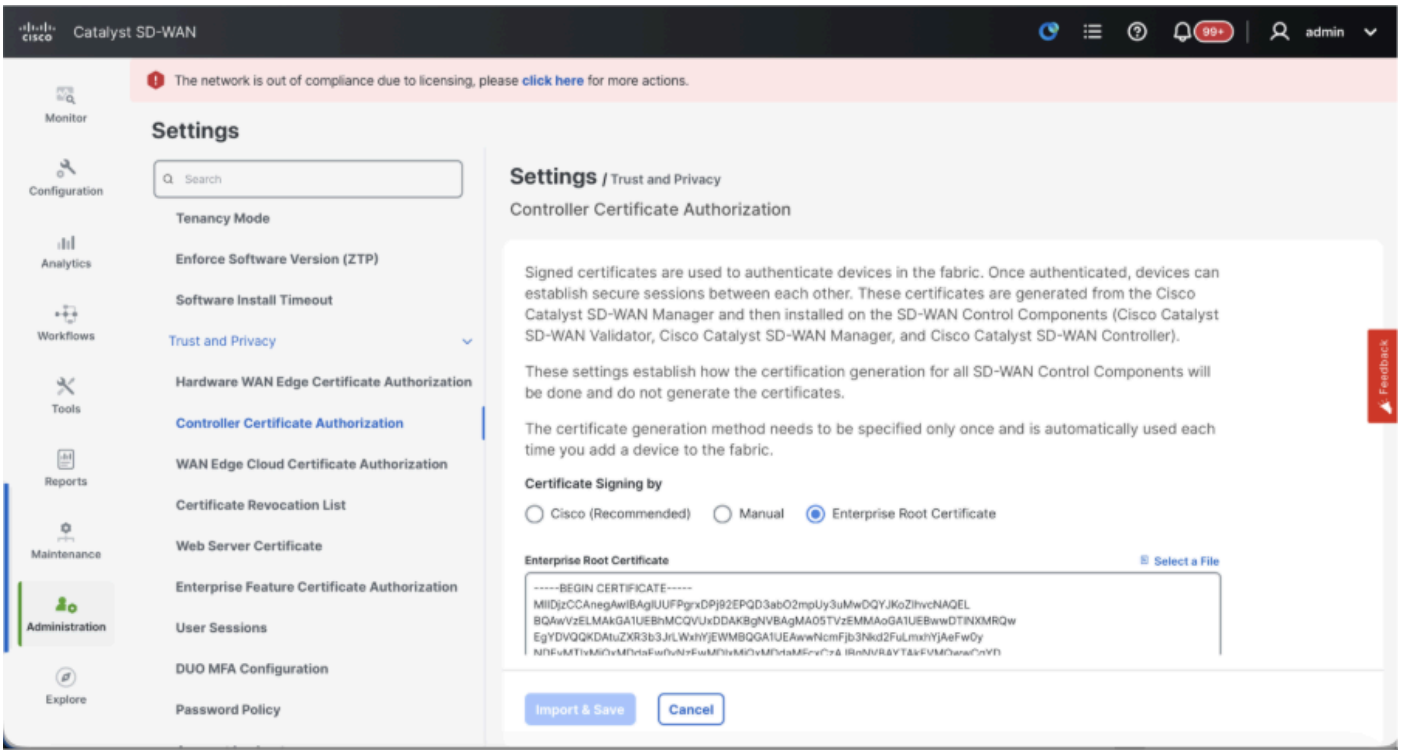


- Compruebe las configuraciones de la Autorización de certificados (CA), que decide la Autoridad de certificados utilizada para firmar los certificados. Podemos ver 3 opciones allí:

1. Autorización de certificado de extremo de WAN de hardware - Decide la CA para los routers periféricos SD-WAN de hardware.
    - Certificado en caja (certificado TPM/SUDI): con esta opción, el certificado preinstalado en el hardware del router se utiliza para establecer las conexiones de control (conexiones TLS/DTLS)
    - Certificado de empresa (firmado por la CA de empresa): con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

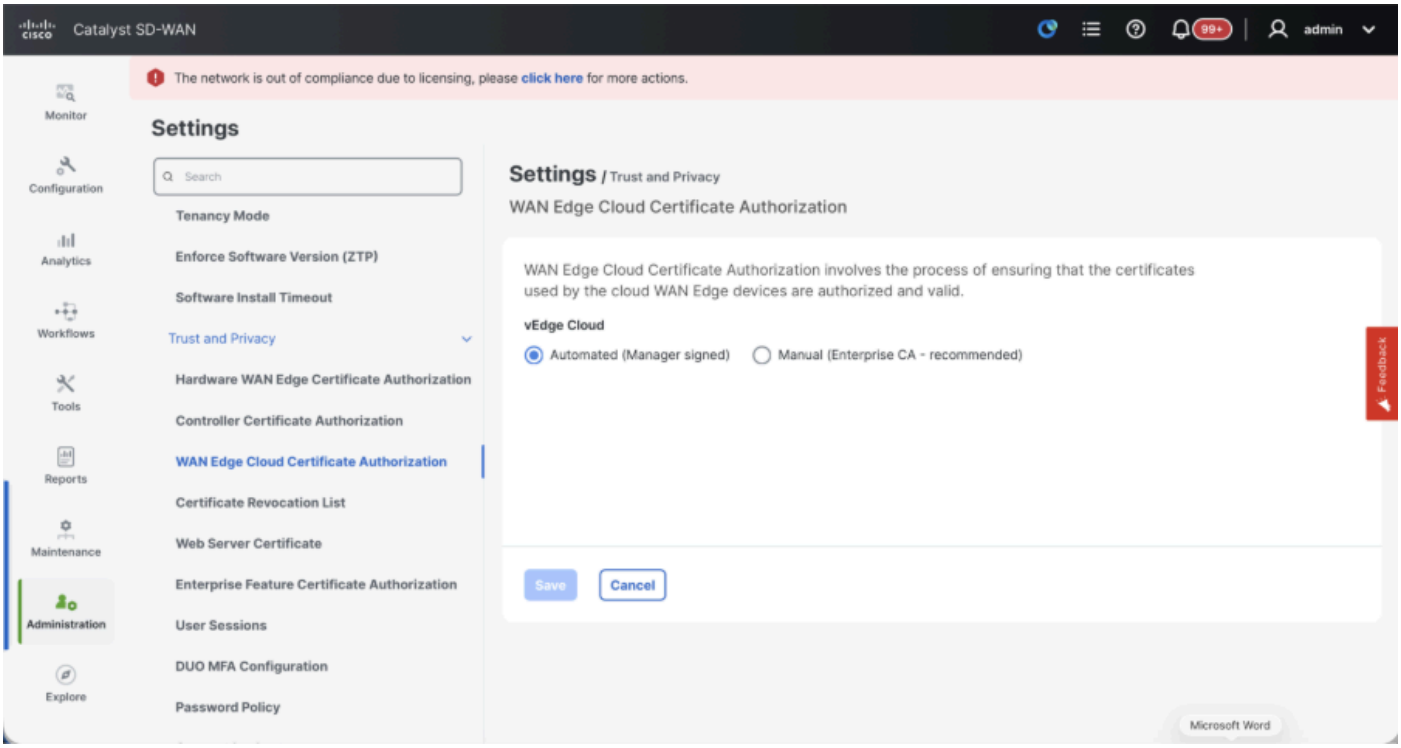


2. Autorización de certificado de controlador: decide la CA para los controladores SD-WAN.
    - Cisco (recomendado): los controladores utilizan los certificados firmados por Cisco PKI. vManage se pone en contacto automáticamente con el portal PNP mediante las credenciales de la cuenta inteligente configuradas en vManage y consigue que el certificado se firme y se instale en el controlador.
    - Manual: los controladores utilizan los certificados firmados por Cisco PKI. Firme manualmente el CSR mediante el portal Cisco PNP; para ello, acceda a la cuenta inteligente y la cuenta virtual de la superposición SD-WAN correspondiente.
    - Certificado raíz de empresa: con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

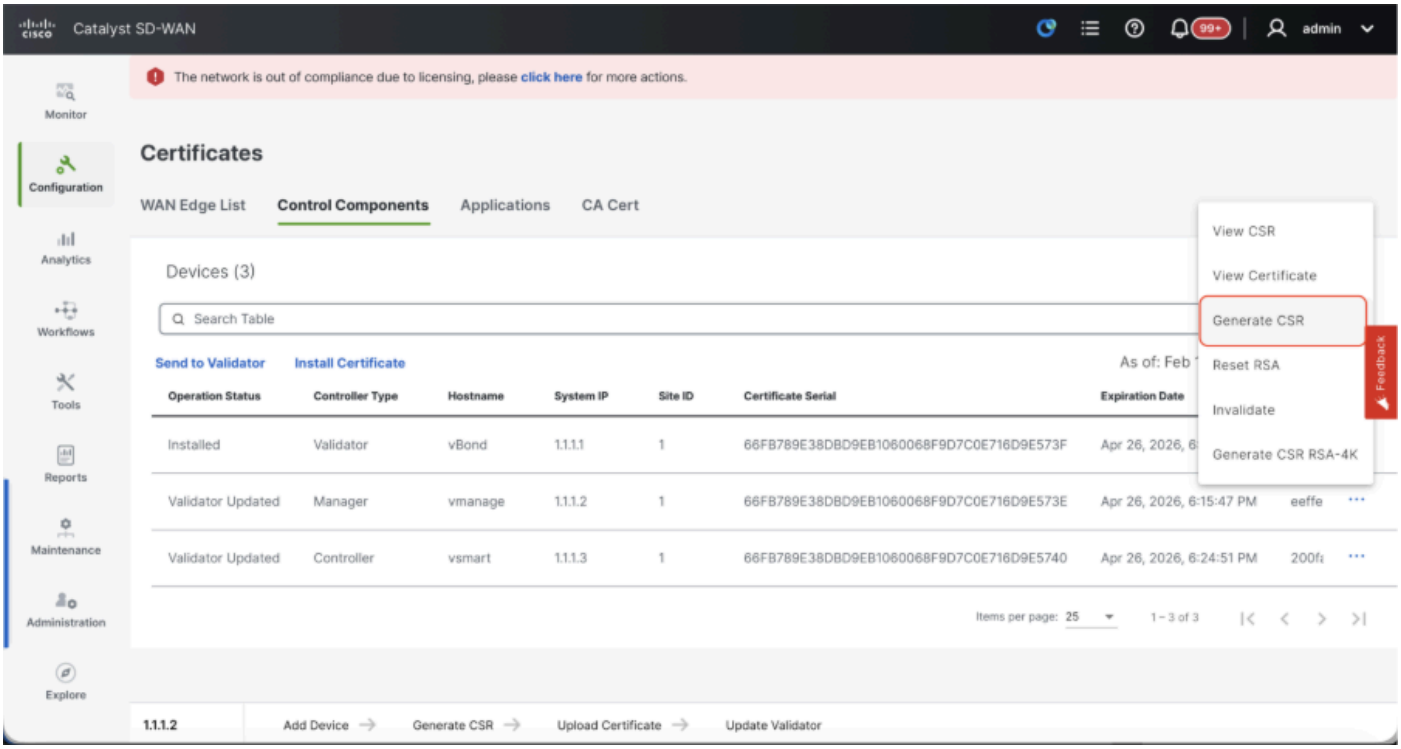


3. Autorización de certificado de nube de extremo de WAN: decide la CA para routers periféricos SD-WAN virtuales (CSR1000v, C8000v, nube vEdge)
    - Automatizado (vManage firmado): vManage firma automáticamente el CSR para los routers periféricos virtuales e instala el certificado en el router.
    - Manual (CA empresarial: recomendado): los routers virtuales utilizan certificados firmados por la autoridad de certificación empresarial de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

En este caso, si estamos utilizando nuestra propia CA, autoridad de certificación de empresa, elija Empresa.



- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers
- Haga clic en ... para Manager/vManage y haga clic en Generar CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.

Incorporación de vBond/Validator y vSmart/Controller a vManage

Vaya a Configuration > Devices > Control Components en caso de nodos vManage 20.15/20.18. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

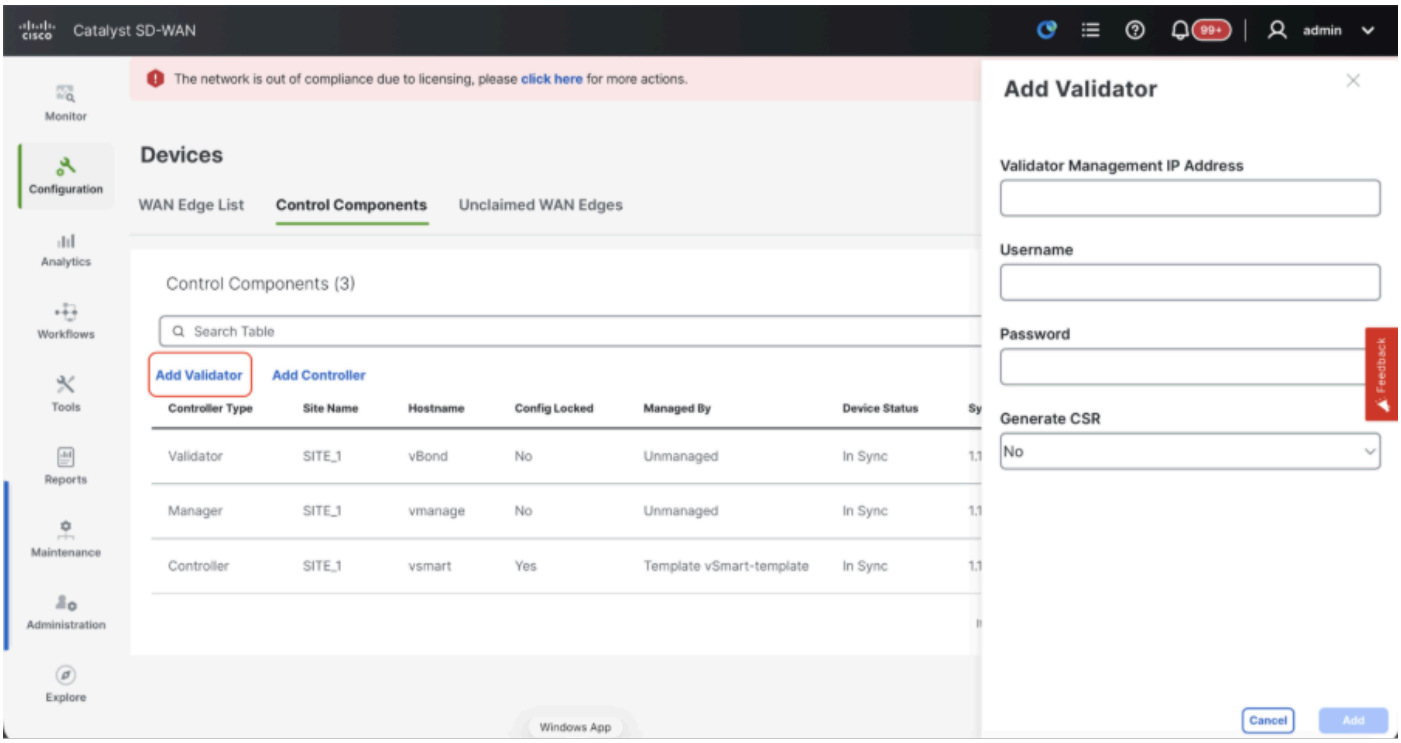
Incorporación de vBond/Validador

- Haga clic en AddvBonden caso de 20.12vManagerAgregar validadoren el caso de 20.15/20.18vManage. Se abre una ventana emergente, introduzca el IP de transporte VPN 0 de vBondque se puede alcanzar desde vManage.
- Verifique la disponibilidad mediante ping si se permite desde la CLI de vManagetovBondIP.

- Introduzca las credenciales de usuario de vBond.

Nota: Necesitamos usar las credenciales de administración de vBono una parte de usuario denetadmingroup. Puede verificarlo en la CLI de thevBond. Elija Sí en el menú desplegable de "Generar CSR" si necesitamos instalar un nuevo certificado para vBond

Nota: Si vBond está detrás de un dispositivo NAT/firewall, verifique si la IP de la interfaz VPN 0 de vBond se traduce a una IP pública. Si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la interfaz VPN 0 en este paso

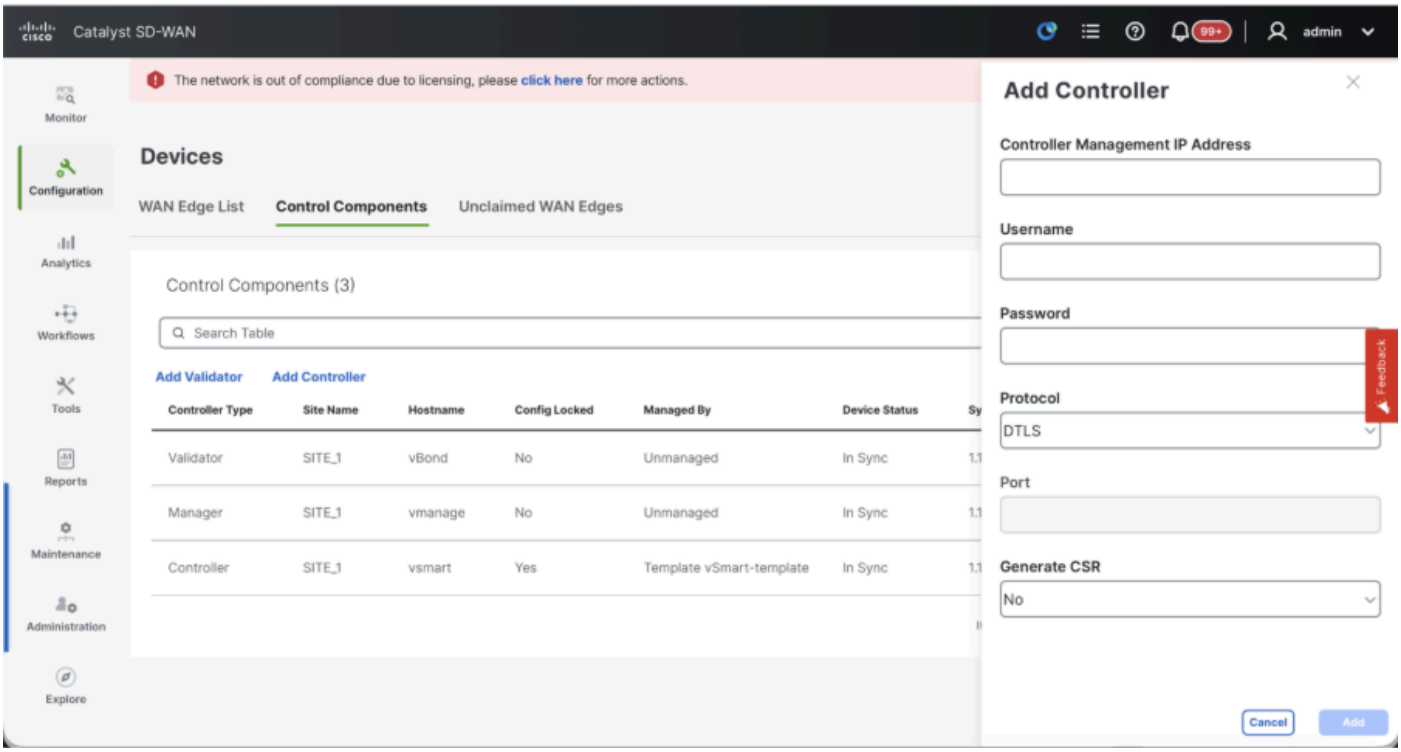


- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vBond.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vBonds, repita los mismos pasos.

Incorporación de vSmart/Controller

- Haga clic en Add vSmart en el caso de 20.12 vManage o Add Controller en el caso de 20.15/20.18 vManage.
- Se abre una ventana emergente, introduzca la IP de transporte VPN 0 de vSmart, a la que se puede acceder desde vManage.
- Compruebe la disponibilidad mediante ping si se permite desde la CLI de vManage a vSmart IP.
- Introduzca las credenciales de usuario de vSmart Note que necesitamos para utilizar las credenciales de administrador de vSmart o una parte de usuario del grupo netadmin.
- Puede comprobarlo en la CLI de vSmart.
- Establezca el protocolo en TLS, si pretendemos utilizar TLS para routers para establecer conexiones de control con vSmart. Esta configuración también debe configurarse en CLI de nodos vsmarts y vManage.
- Elija Sí en el menú desplegable "Generar CSR" si necesitamos instalar un nuevo certificado para vSmart.

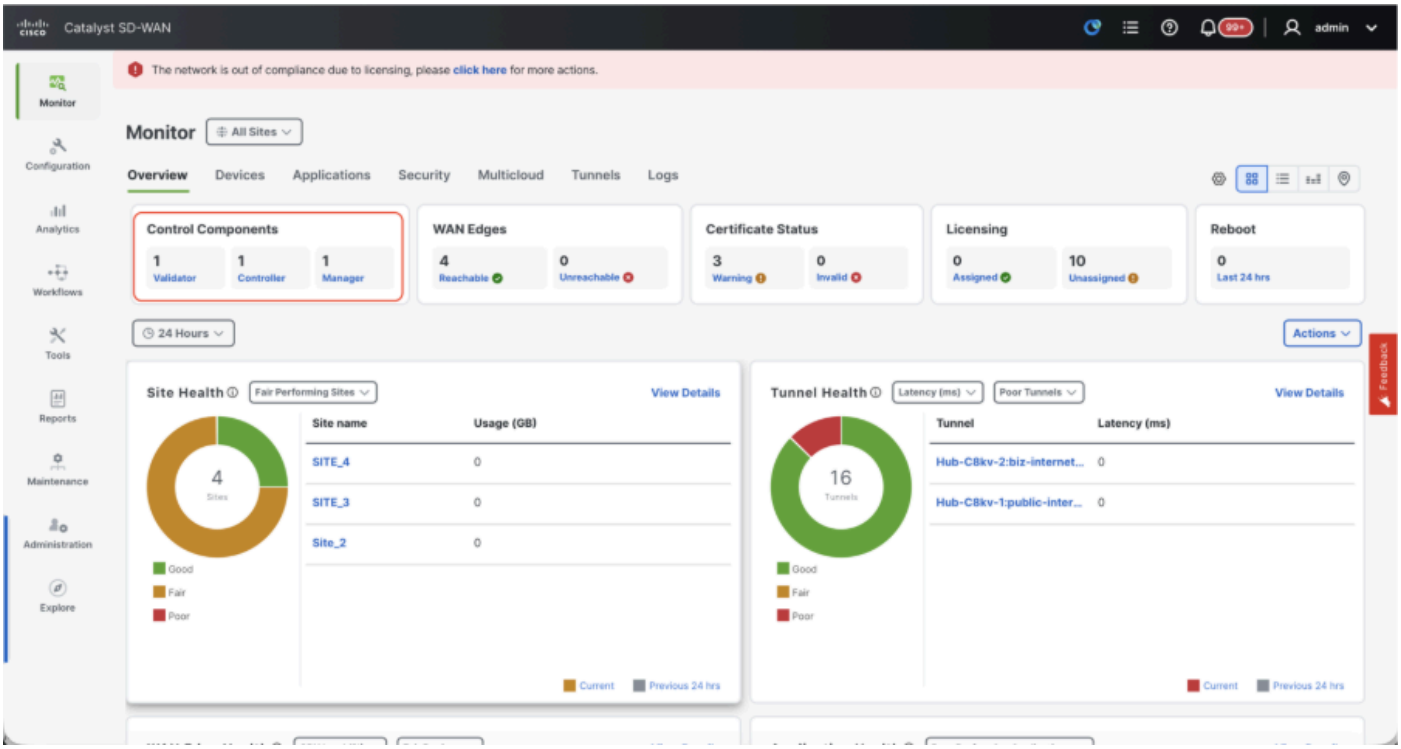
Nota: Si vSmart está detrás del dispositivo NAT/firewall, compruebe si la IP de la interfaz VPN 0 de vSmart se traduce a una IP pública y si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la IP de la interfaz VPN 0 en este paso.



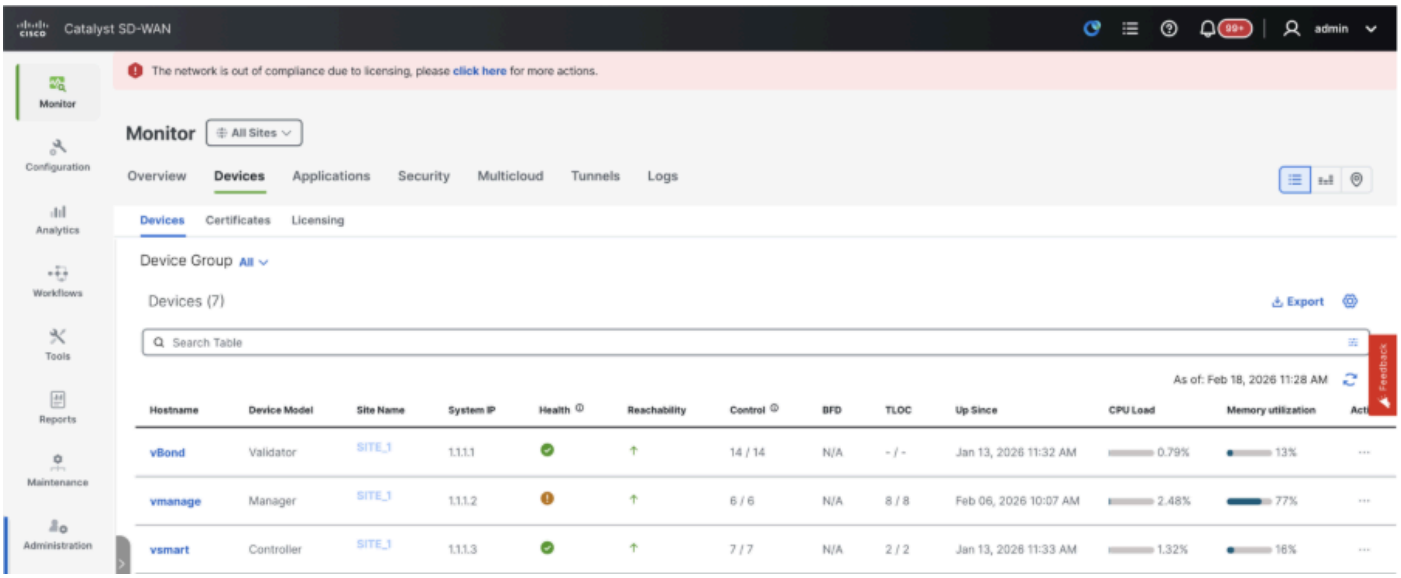
- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vSmart.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vsmarts, repita los mismos pasos.

Verificación

Una vez completados todos los pasos, verifique que todos los componentes de control sean accesibles en Monitor>Dashboard



- Haga clic en los componentes de control correspondientes y confirme que todos son accesibles.
- Navegue hasta Monitor > Devices y confirme que todos los componentes de control son accesibles.



Paso 3: Generar clúster de vManage

Fabric SD-WAN integrado con un clúster vManage en la superposición SD-WAN

Nota: vManage Cluster se puede configurar con 3 nodos vManage o 6 nodos vManage en función del número de sitios incorporados al fabric SD-WAN. Consulte el clúster de vManage existente y elija el número de nodos de la misma forma.

Configure las configuraciones CLI de todos los nodos de vManage que forman parte del clúster

Configurar la configuración del sistema en todos los nodos de vManage

- Configure el resto de los nodos de vManage. En el caso de un clúster de 3 nodos, tiene 2 nodos restantes que configurar; en el caso de un clúster de 6 nodos, tiene 5 nodos que configurar.
- Configure las configuraciones del sistema como se muestra:

```
config t
system
 host-name



 system-ip



 site-id
```

```
 organization-name


 vbond


commit
```

Nota: Si utilizamos URL como dirección vBond, asegúrese de configurar las direcciones IP del servidor DNS en la configuración VPN 0 o asegúrese de que se puedan resolver.

Configuración de la interfaz de transporte en todos los nodos de vManage

Estas configuraciones son necesarias para habilitar la interfaz de transporte utilizada para establecer conexiones de control con los routers y el resto de los controladores.

```
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
```

Configuración de la interfaz de gestión en todos los nodos de vManage

Configure también la interfaz de administración VPN 512para habilitar el acceso de administración fuera de banda al controlador.

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

Configuración opcional:

- Puede consultar las configuraciones de su controlador existente y, si la configuración que se muestra aquí está presente, puede agregar esta configuración a los nuevos controladores.
- Configure el protocolo de control como TLS solo si hay un requisito para que los routers establezcan conexiones de control seguras con los nodos vManage mediante TLS. De forma predeterminada, todos los controladores y routers establecen una conexión de control mediante DTLS. Se trata de una configuración opcional que solo se requiere en los nodos vSmart y vManage, según sus necesidades.

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

Configurar la interfaz de servicio en todos los nodos de vManage

Configure la interfaz de servicio en todos los thevManagenodes, incluido vManage-1, que ya se ha incorporado. Esta interfaz se utiliza para la comunicación del clúster, lo que significa comunicación entre losnodos de administración del clúster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Asegúrese de que se utiliza la misma subred IP para la interfaz de servicio en todos los nodos delclúster de administración.

Configurar credenciales de clúster

Podemos utilizar las mismas credenciales de administrador de thevManagenodes para configurar thevManagecluster. De lo contrario, podemos configurar una nueva credencial de usuario que forma parte denetadmingroup. Las configuraciones para configurar las nuevas credenciales de usuario son las siguientes

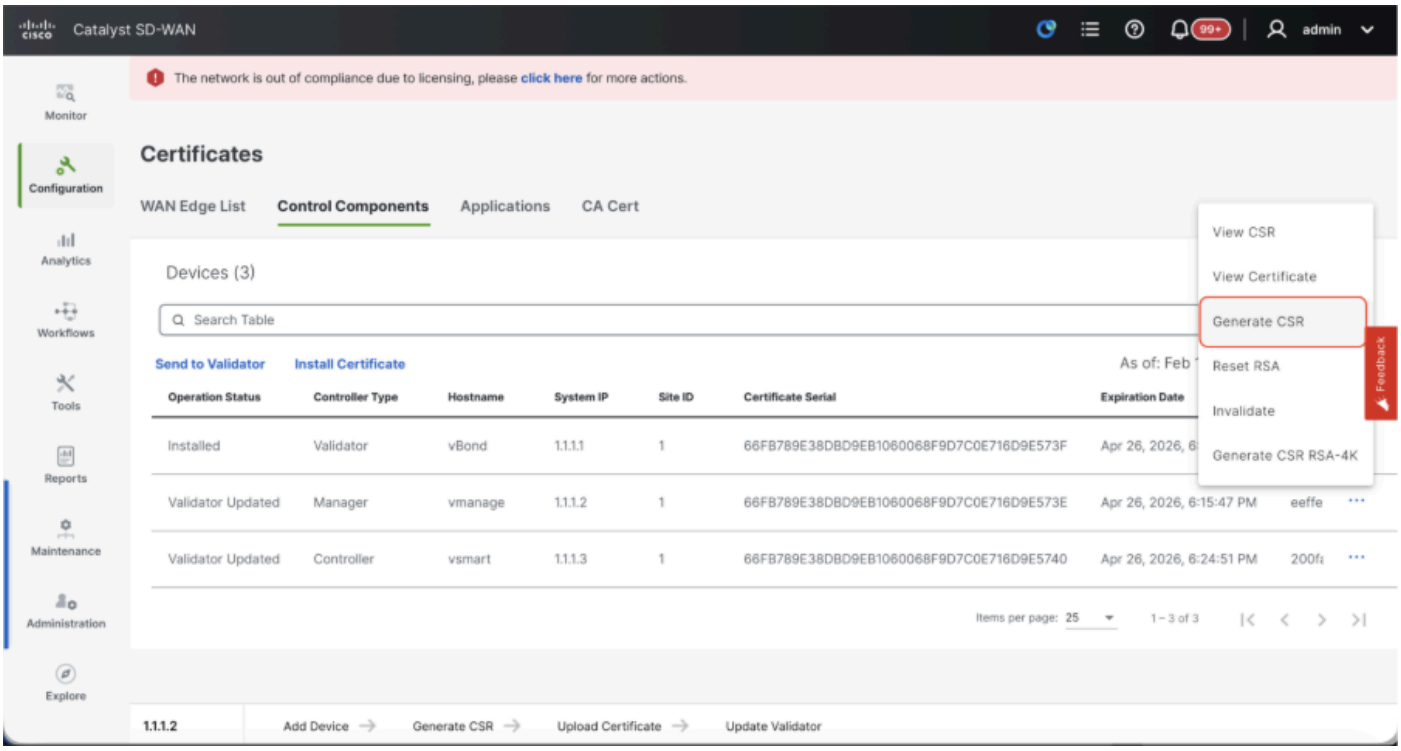
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

Asegúrese de configurar las mismas credenciales de usuario en todos los vManagenodesque forman parte del clúster.Si decidimos utilizar credenciales de administrador, debe ser el mismo nombre de usuario/contraseña en todos los vManagenodes.

Instalar el certificado de dispositivo en todos los nodos de vManage

- Inicie sesión en tovManageUI de todos los thevManagenodes mediante la dirección URL https://<vmanage-ip>en su navegador. Utilice la dirección IP VPN 512 de los vManagenodes respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

  Haga clic en ... para Manager/vManage y haga clic en Generate CSR.



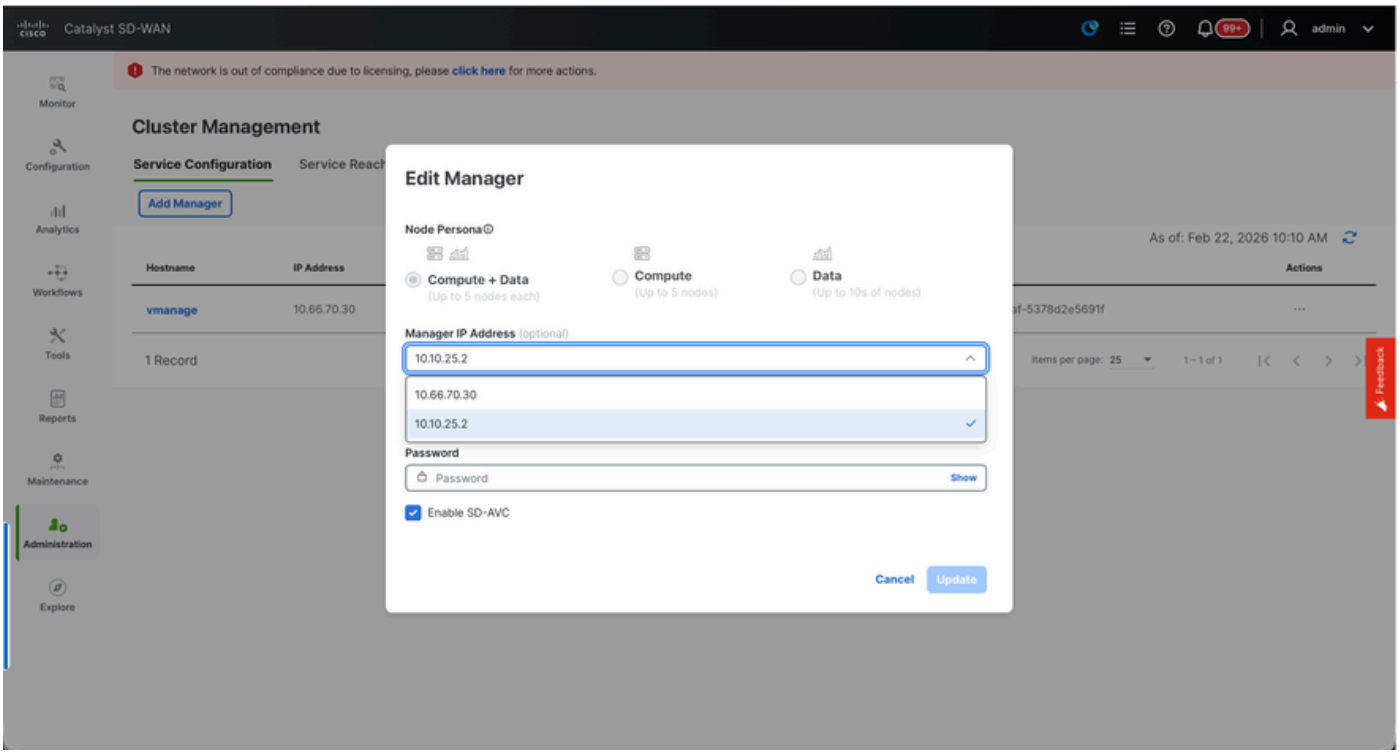
- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si selecciona Manual, firme manualmente el CSR mediante el portal PNP de Cisco accediendo a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN respectiva. Se aplica el mismo procedimiento si utilizamos Digicert y el certificado raíz de empresa.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- Complete este paso en todos los nodos de vManage que forman parte del clúster.

Preparación para crear el clúster de vManage

- En la interfaz de usuario web de vManage-1, vaya a Administration > Cluster Management, haga clic en ... en Actions for vManage-1, elija Edit.
- El personaje del nodo se elige automáticamente en función del personaje que elegimos mientras se giraba la máquina virtual.

Nota: Para un clúster de 3 nodos, los 3 nodos de vManage se activan con compute+data como persona.

- Para un clúster de 6 nodos, 3 nodos de vManage se activan con compute+data como persona y 3 nodos de vManage se activan con datos como persona.
- En el menú desplegable Dirección IP del administrador, asegúrese de elegir la dirección IP de la interfaz de servicio de vManage.

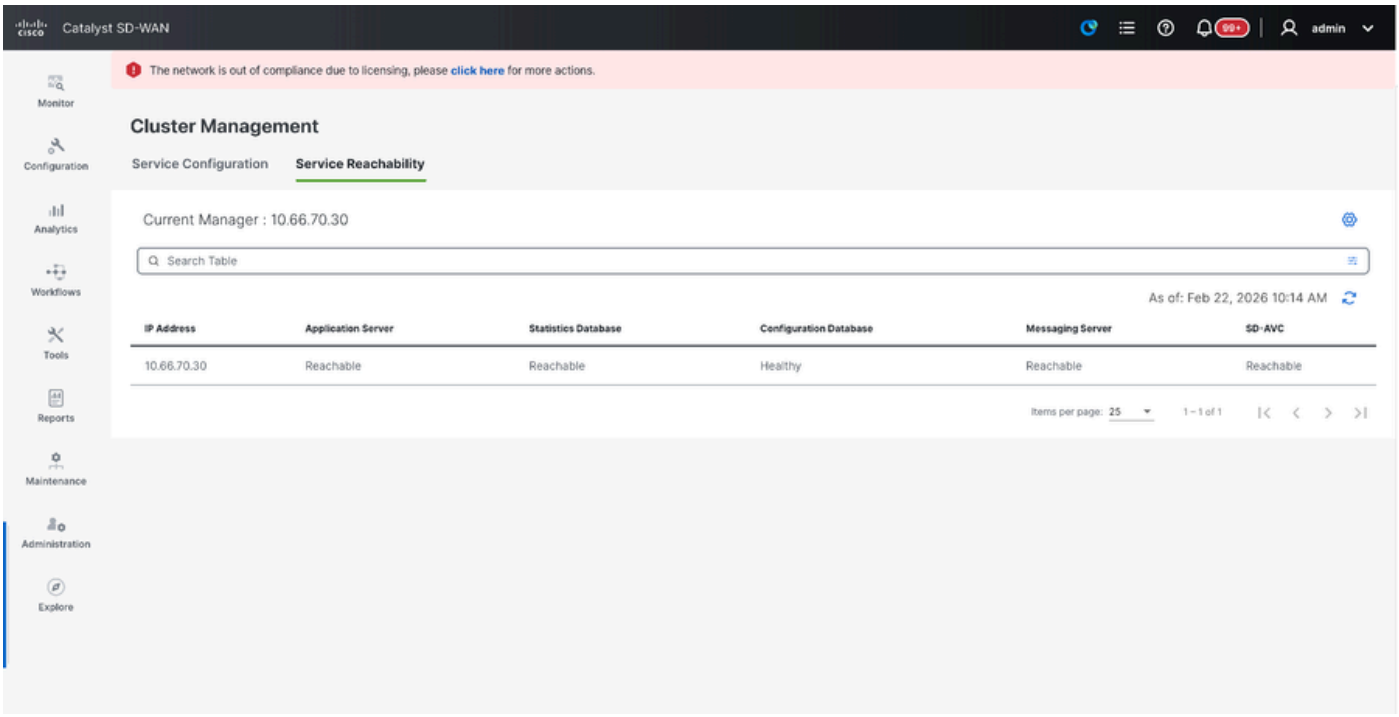


- Introduzca el nombre de usuario y la contraseña que desee utilizar para activar el clúster de vManage, que se conoce como credenciales del clúster.
- Como se ha mencionado anteriormente, se deben configurar las mismas credenciales en todos los nodos de vManage y se deben utilizar al agregar todos los nodos al clúster.

Nota: Haga referencia a esta configuración en su clúster existente para habilitar SDAVC: solo debe comprobarse si es necesario y sólo es necesario en un nodo vManage del clúster.

Haga clic en Actualizar.

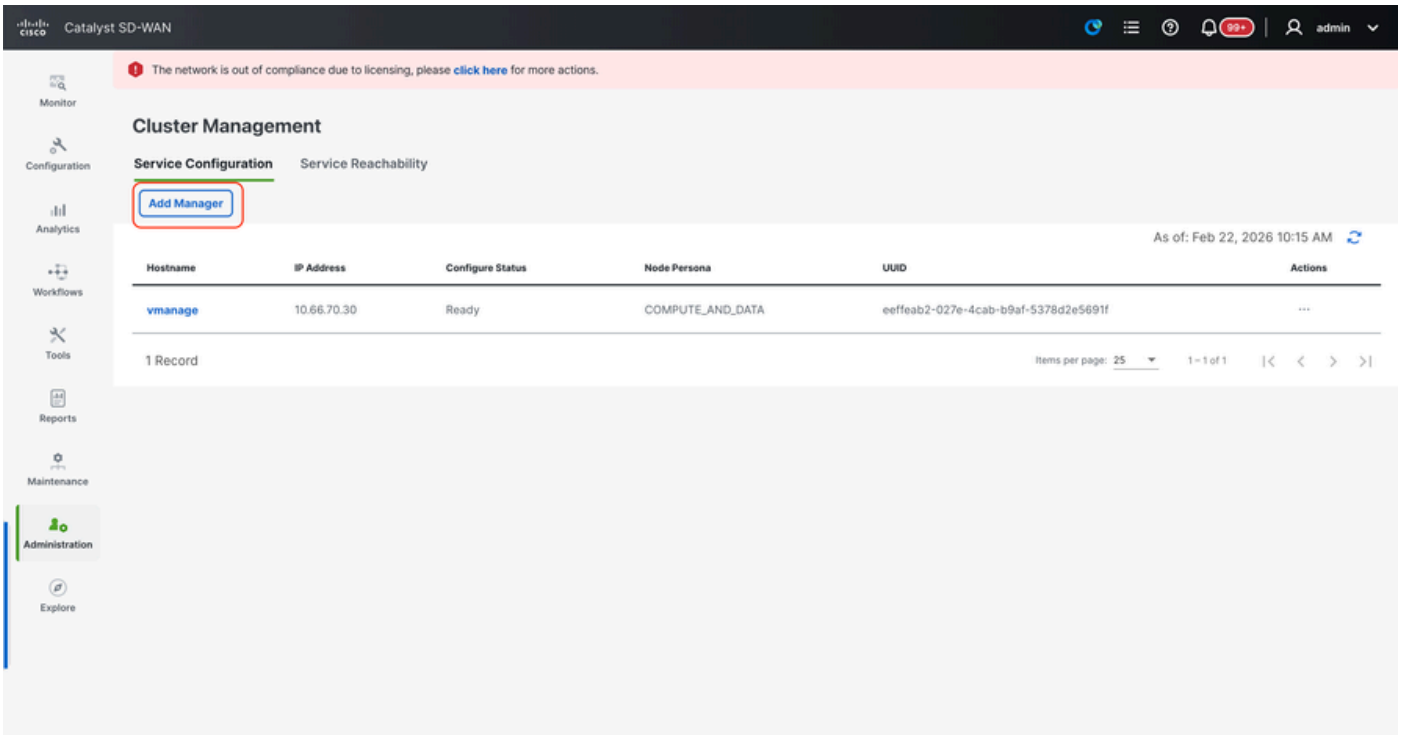
- Al publicar esto, los servicios de vManage NMS se reinician en segundo plano y la interfaz de usuario no está disponible durante unos minutos de entre 5 y 10 minutos. Durante este tiempo, está disponible el acceso CLI de vManage.
- Una vez que se pueda acceder a la interfaz de usuario de vManage-1, vaya a Administration > Cluster Management (Administración > Administración de clústeres) y asegúrese de que la IP de la interfaz de servicio de vManage se refleja en IP address (Dirección IP).El estado de configuración es Preparado y el personaje del nodo se refleja correctamente.
- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios están disponibles.

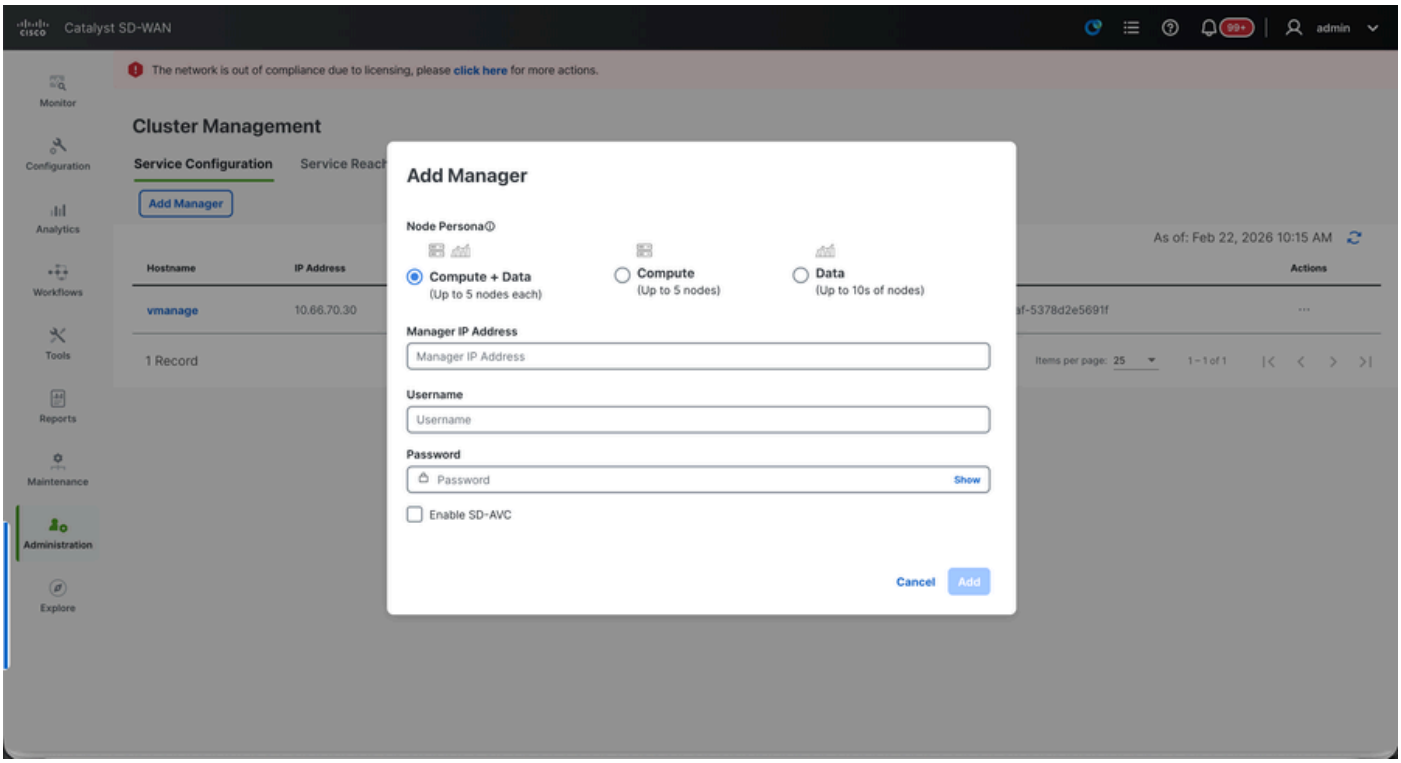


- Si vemos que alguno de los servicios aún no está disponible, espere. Por lo general, toma alrededor de 20 a 30 minutos.

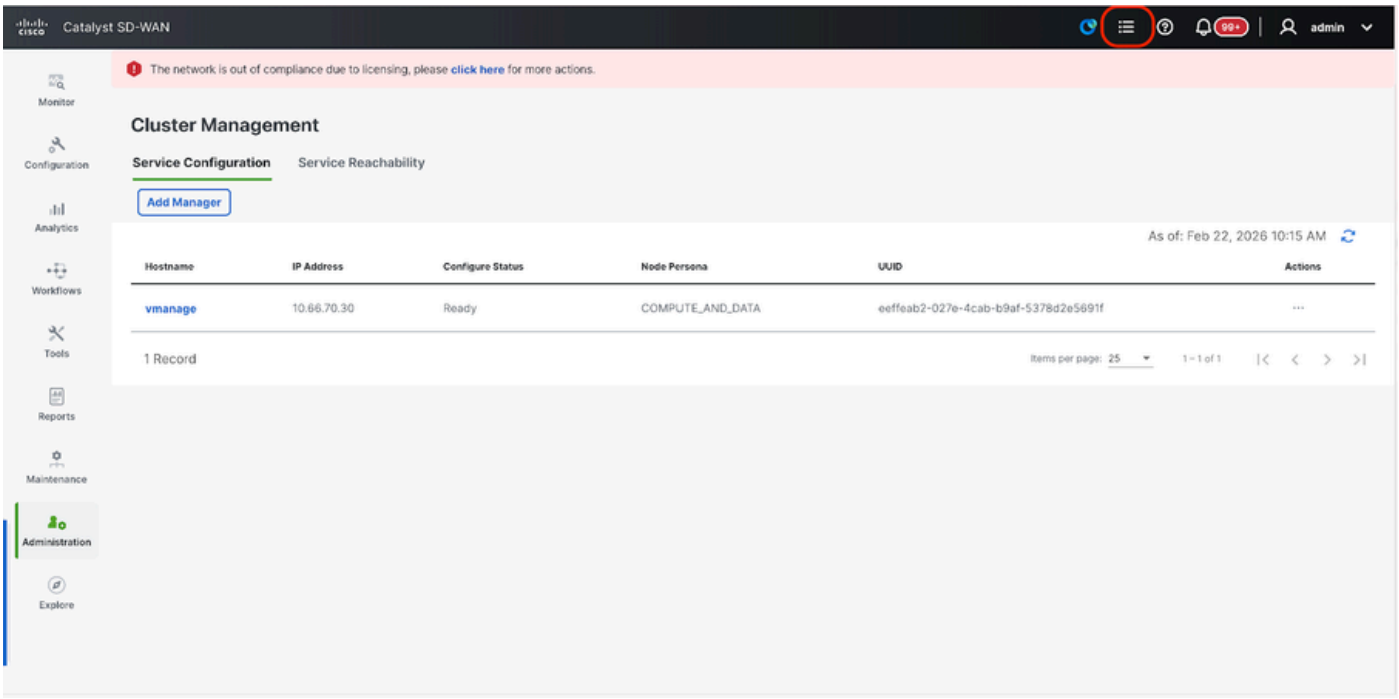
Creación del clúster de vManage

- En la interfaz de usuario web de vManage-1, vaya a Administration > Cluster Management, en la sección Service Configuration,
- Haga clic en Add Manager, aparecerá una ventana emergente:





- Elija el Node persona en función de las configuraciones de persona realizadas mientras se giraba el nodo vManage - 2.
- Introduzca la IP de la interfaz de servicio de vManage-2 en Dirección IP del jefe
- Introduzca el nombre de usuario y la contraseña, que son las mismas credenciales que utilizamos en el paso 6.
- Habilitar SDAVC: no se debe marcar porque ya lo habríamos activado en vManage-1
- Haga clic en Agregar.
- Al publicar esto, los servicios de vManage NMS se reinician en segundo plano para los nodos de vManage 1 y 2. La interfaz de usuario no está disponible durante unos minutos de 5 a 10 minutos aproximadamente para vManage 1 y 2.
- Durante este tiempo, está disponible el acceso CLI de vManage 1 y 2.
- Una vez que se pueda acceder a la interfaz de usuario de vManage-1, vaya a Administration > Cluster Management, asegúrese de que la IP de la interfaz de servicio de vManage se refleja en IP address, Configure Status is Ready y node persona se refleja correctamente.
- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios son accesibles para ambos nodos de vManage.
- Si vemos que alguno de los servicios aún no está disponible, espere. Por lo general, toma alrededor de 5 a 10 minutos.
- Puede comprobar el estado del proceso de adición de clústeres en la lista de tareas disponible en la esquina superior derecha de la interfaz de usuario de vManage.



- Puede buscar una lista de tareas activas y, si la tarea sigue apareciendo en Lista de tareas activas, indica que la tarea no se ha completado todavía.
- Puede hacer clic en la tarea para comprobar el progreso de la misma. Si la tarea no aparece en Lista de tareas activas, cambie a Completada y asegúrese de que la tarea se ha completado correctamente.
- Solo después de validar estos puntos, continúe con el siguiente paso.

Estos puntos deben tenerse en cuenta antes de agregar el siguiente nodo al clúster:

Verifique estos puntos en todas las UI de los nodos vManage que se han agregado al clúster hasta el momento:

- Vaya a Monitor > Overview of vManage UI y asegúrese de que el número de nodos de vManage se reflejen correctamente y se vean accesibles en función del número de nodos agregados al clúster.

- Navegue hasta Administration > Cluster Management y asegúrese de que la IP de la interfaz de servicio de vManage se refleje bajo IP address, Configure Status is Ready y node persona se refleje correctamente.
- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios son accesibles para ambos nodos de vManage.

- Cada vez que se agrega un nodo al clúster, se reinician los servicios NMS de todos los nodos del clúster, por lo que la interfaz de usuario de todos esos nodos queda inaccesible durante algún tiempo.
- Dependiendo del número de nodos del clúster, puede ser necesario más tiempo para que se realice una copia de seguridad de la interfaz de usuario y todos los servicios sean accesibles.
- Puede supervisar la tarea en Lista de tareas disponible en la esquina superior derecha de la interfaz de usuario de vManage.

- En la interfaz de usuario de vManage de cada nodo agregado al clúster, necesitamos ver todos los routers, plantillas y políticas si estuvieran disponibles en vManage-1.
- Si esas configuraciones no estaban presentes en vManage-1, los vBonds y vSmarts que se agregaron a vManage-1 y también las configuraciones de Administration > Settings para Organization-name, vBond, Certificate Authorization deben reflejarse en el resto de los nodos vManage agregados al clúster.
- Repita los mismos pasos para el resto de los nodos de vManage.

Una vez que todos los controladores estén incorporados, complete este paso:

Paso 4: Copia de seguridad/restauración de Config-db

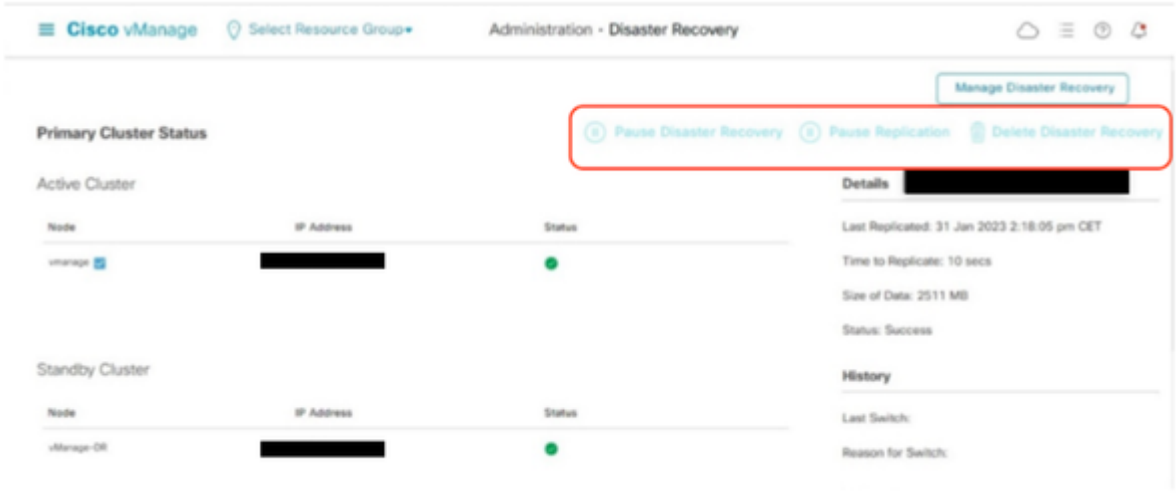
Recopilar copia de seguridad de la base de datos de configuración de vManage y restaurar en otro nodo de vManage

---

Nota: Mientras recopila la copia de seguridad de la base de datos de configuración del clúster de vManage existente que tiene habilitada la recuperación ante desastres, asegúrese de que se recopila después de pausar y eliminar la recuperación ante desastres de ese nodo.

Confirme que no hay replicación de recuperación ante desastres en curso. Vaya a Administration > Disaster Recovery y asegúrese de que el estado es Correcto y no está en un estado transitorio, como Importación pendiente, Exportación pendiente o Descarga pendiente. Si el estado no es correcto, póngase en contacto con Cisco TAC y asegúrese de que la replicación es correcta antes de proceder a pausar la recuperación ante desastres.

En primer lugar, detenga la recuperación ante desastres y asegúrese de que la tarea se ha completado. A continuación, elimine la recuperación ante desastres y confirme que la tarea se ha completado.



Póngase en contacto con el TAC de Cisco para asegurarse de que la recuperación ante desastres se ha limpiado correctamente.

Recopilar copia de seguridad de Configuration-DB:

- En el fabric SD-WAN que se está utilizando actualmente, puede generar una copia de seguridad de la base de datos de configuración desde el clúster de vManage.
- Tenga en cuenta que solo debemos generar una copia de seguridad de la base de datos de configuración en un nodo del clúster de vManage que es el líder de la base de datos de configuración.

- Para vManage independiente, vManage es el líder de la base de datos de configuración.
- En el clúster vManage, identifique el nodo líder configuration-db mediante el comando request nms configuration-db diagnostics.Puede ejecutar este comando en todos los nodos del clúster vManage de 3 nodos.
- En un clúster de 6 nodos, asegúrese de ejecutar este comando en los nodos vManage donde configuration-db está habilitado para identificar el nodo líder. Navegue hasta Administración > Administración de clústeres para verificar lo mismo:
- Como vemos en la captura de pantalla, los nodos configurados con persona COMPUTE_AND_DATA tienen configuration-db en ejecución.

Puede verificar lo mismo mediante el comando requestnmsconfiguration-dbstatus en vManageCLI. El resultado es como se muestra

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

- Una vez ejecutado el comandorequest nms configuration-db diagnostics en estos nodos, el resultado es el siguiente:
- Busque el campo resaltado para "IsLeader". Si se establece en 1, indica que el nodo es el nodo líder y podemos recopilar una copia de seguridad de la base de datos de configuración de él.

```
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     .
```

Utilice este comando para recopilar la copia de seguridad de la base de datos de configuración del nodo vManage del líder de la base de datos de configuración identificado.

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

El resultado esperado es el siguiente:

```
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#
```

- Tome nota de las credenciales de configuration-db si se ha actualizado.
- Si no conoce las credenciales de la base de datos de configuración, póngase en contacto con el TAC para recuperar las credenciales de la base de datos de configuración de los nodos de vManage existentes.

- Las credenciales de la base de datos de configuración predeterminada son username: neo4j y contraseña: contraseña

Restaurar copia de seguridad de Configuration-db en otro nodo de vManage

Copie la copia de seguridad de la base de datos de configuración en el directorio /home/admin/ de vManage mediante SCP.

Ejemplo de resultado del comando scp:

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

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

Para restaurar la copia de seguridad de la base de datos de configuración, primero debemos configurar las credenciales de la base de datos de configuración. Si sus credenciales de configuration-db son predeterminadas (neo4j/password), podemos saltarnos este paso.

Para configurar las credenciales de configuration-db, utilice el comando request nms configuration-db update-admin-user.Use el nombre de usuario y la contraseña que desee.

Tenga en cuenta que el servidor de aplicaciones de vManage se reinicia. Debido a lo cual, la interfaz de usuario de vManage se vuelve inaccesible durante un breve período de tiempo.

```
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#
```

Publicación en la que podemos continuar con la restauración de la copia de seguridad de la base de datos de configuración:

Podemos utilizar el comando request nms configuration-db restore path /home/admin/< > para restaurar la base de datos de configuración en el nuevo vManage:

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

Una vez restaurada la base de datos de configuración, asegúrese de que se puede acceder a la interfaz de usuario de vManage. Espere unos 5 minutos e intente acceder a la interfaz de usuario.

Una vez que haya iniciado sesión correctamente en la interfaz de usuario, asegúrese de que la

lista de routers periféricos, la plantilla, las políticas y el resto de las configuraciones que estaban presentes en la interfaz de usuario de vManage anterior o existente se reflejan en la nueva interfaz de usuario de vManage.

Paso 5: Reautenticación de controladores e invalidación de controladores antiguos

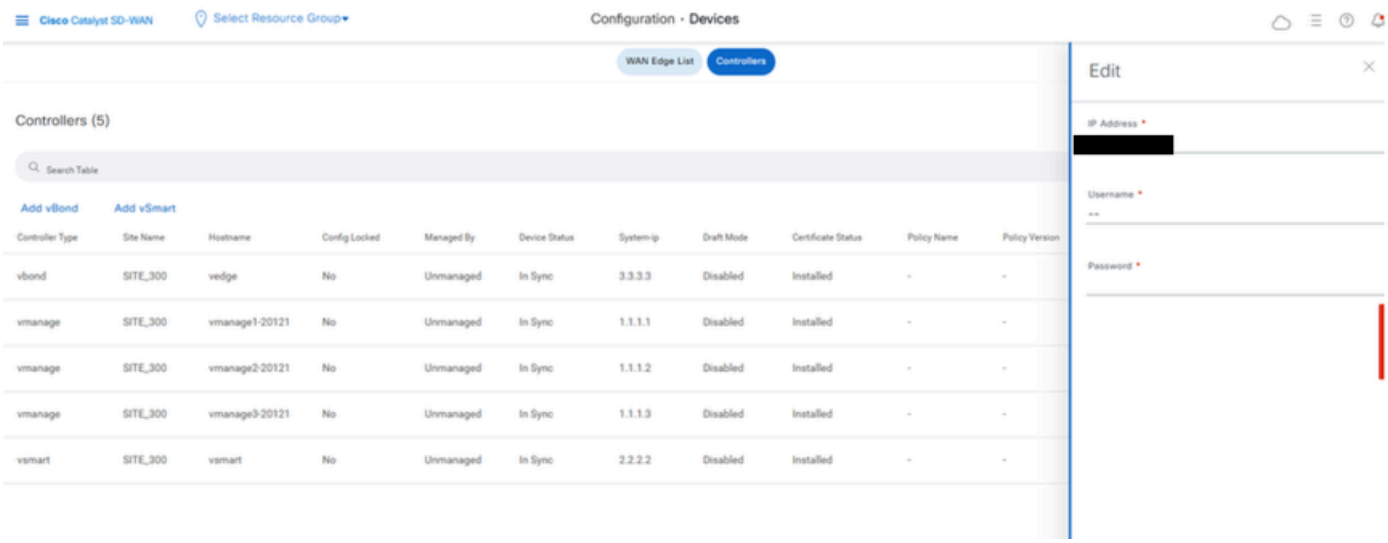
Una vez restaurada la base de datos de configuración, necesitamos volver a autenticar todos los nuevos controladores (vmanage/vsmart/vbond) en el fabric

---

Nota: En la producción real, si la IP de interfaz utilizada para la reautenticación es la IP de interfaz de túnel, debe asegurarse de que se permite el servicio NETCONF en la interfaz de túnel de vManage, vSmart y vBond, así como en los firewalls a lo largo de la ruta. El puerto del firewall que se debe abrir es el puerto TCP 830 como regla bidireccional desde el clúster DR a todos los vBonds y vsmarts .

En vmanage UI, haga clic en Configuration > Devices > Controllers

- Haga clic en los tres puntos cerca de cada controlador y haga clic en Editar



- Reemplace la dirección ip (system-ip of the controller) por la dirección ip transport vpn 0 (tunnel interface). Introduzca el nombre de usuario y la contraseña y haga clic en save (guardar)
- Haga lo mismo con todos los nuevos controladores del fabric

Sincronizar la cadena de certificados raíz

Una vez que todos los controladores estén incorporados, complete este paso:

En cualquier servidor Cisco SD-WAN Manager del clúster recién activo, realice estas acciones:

Ingrese este comando para sincronizar el certificado raíz con todos los dispositivos Cisco Catalyst SD-WAN en el agrupamiento recientemente activo:

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

Ingrese este comando para sincronizar el UUID de Cisco SD-WAN Manager con el Validador de Cisco SD-WAN:

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

Una vez restaurado el fabric y activadas las sesiones de control y bfd para todos los bordes y controladores del fabric, debemos invalidar los controladores antiguos (vmanage/vsmart/vbond) de la interfaz de usuario

- En vmanage UI, haga clic en Configuration > Devices > Certificates .
- Haga clic en Controladores
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en invalidar
- Haga clic en enviar a vbond
- En vmanage UI, haga clic en Configuration > Devices > Controllers
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en Eliminar.

Paso 6: Registrar cheques

Nota: Continúe con la sección Post Checks (Comprobaciones posteriores) que se muestra aquí, que es común a todas las combinaciones de implementación.

Combinación 4: vManage Cluster + DR en espera manual/en frío

¿Qué es Manual/Cold Standby DR ? El servidor de respaldo SD-WAN Manager o el clúster de SD-WAN Manager se mantiene apagado en el estado de espera en frío.

Se realizan copias de seguridad periódicas de la base de datos activa y, si el clúster del administrador de SD-WAN o el administrador de SD-WAN principal deja de funcionar, el clúster del administrador de SD-WAN o el administrador de SD-WAN en espera se activa manualmente y la base de datos de copia de seguridad se restaura en él.

Instancias necesarias:

- 3 o 6 vManage (clúster principal)
- 3 o 6 vManage (clúster de DR en espera)
- 1 o más vBond (distribuidos entre Data Centers primarios y de DR)
- 1 o más vSmart (distribuido entre Data Centers primarios y de recuperación ante desastres)

Pasos:

1. Abra todas las instancias mediante los pasos comunes
2. Comprobaciones previas

3. Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage
4. Generar clúster de vManage
5. Configuración del clúster de DR en espera en frío
6. Copia de seguridad/restauración de Config-db
7. Registrar cheques

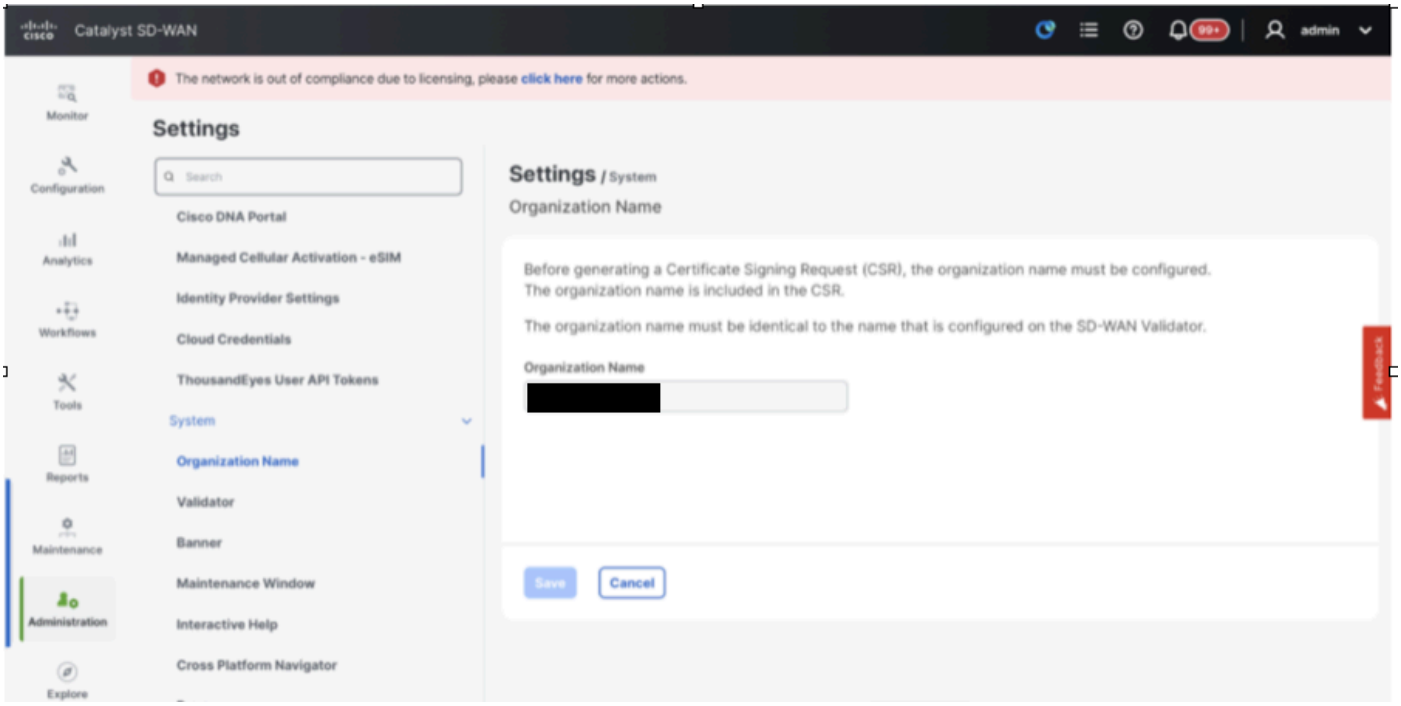
Paso 1: Comprobaciones previas

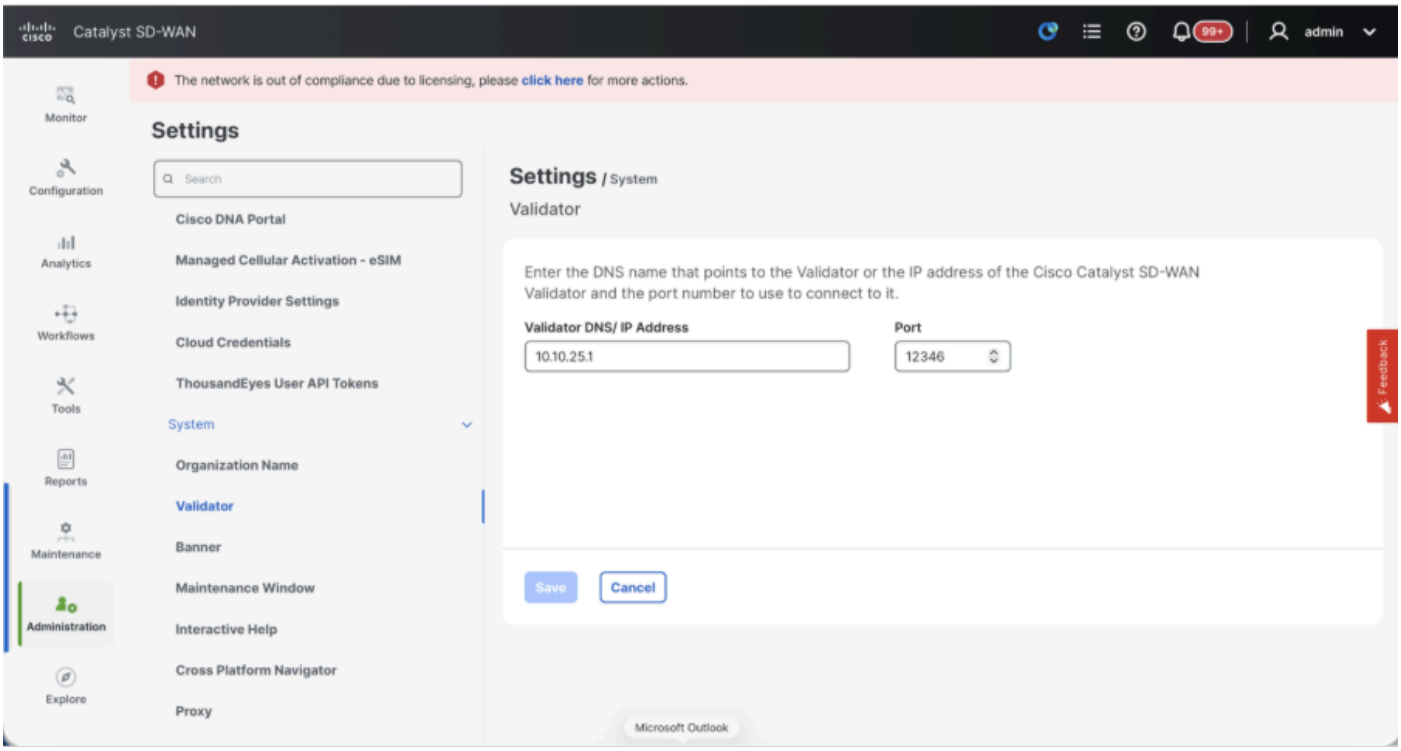
- Asegúrese de que el número de instancias de Cisco SD-WAN Manager activas sea idéntico al número de instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager ejecuten la misma versión de software.
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager puedan alcanzar la dirección IP de administración del Cisco SD-WAN Validator.
- Asegúrese de que los certificados se hayan instalado en las instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que los relojes de todos los dispositivos Cisco Catalyst SD-WAN, incluidas las nuevas instancias de Cisco SD-WAN Manager instaladas, estén sincronizados.
- Asegúrese de que se haya configurado un nuevo conjunto de IP del sistema e ID del sitio en las instancias de Cisco SD-WAN Manager recién instaladas, junto con la misma configuración básica que el clúster activo.

Paso 2: Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage

Actualizar las configuraciones en la interfaz de usuario de vManage

- Una vez agregadas las configuraciones del paso 1 en la CLI de todos los controladores, podemos acceder a la interfaz de usuario web de vManage mediante la dirección URL https://<vmanage-ip> en el navegador. Utilice la dirección IP VPN 512 de los nodos vManage respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Navegue hasta Administration > Settings y complete estos pasos.
- Configure el nombre de la organización y la dirección URL/IP del validador/vBond. Configure el mismo valor que en la CLI del nodo vManage.
- En vManage 20.15/20.18, estas configuraciones están disponibles en la sección Sistema.

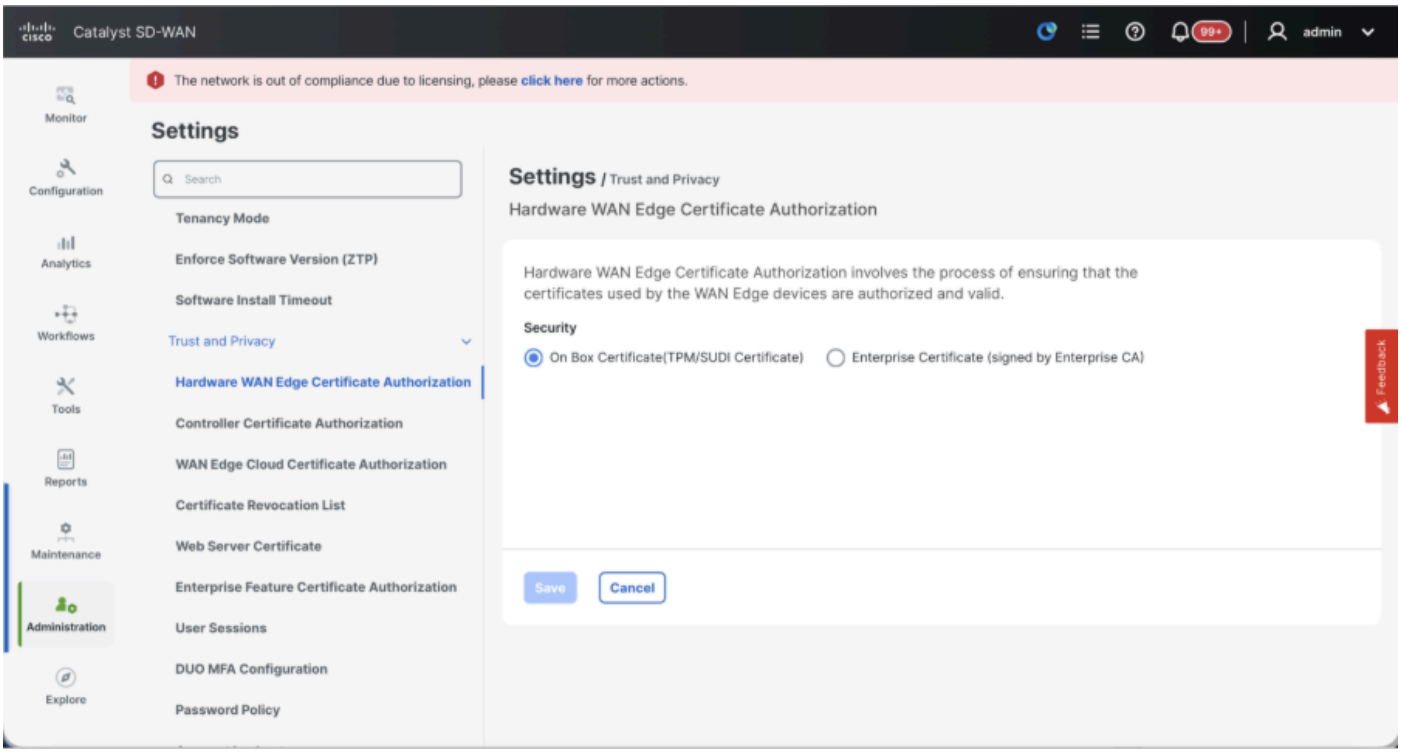




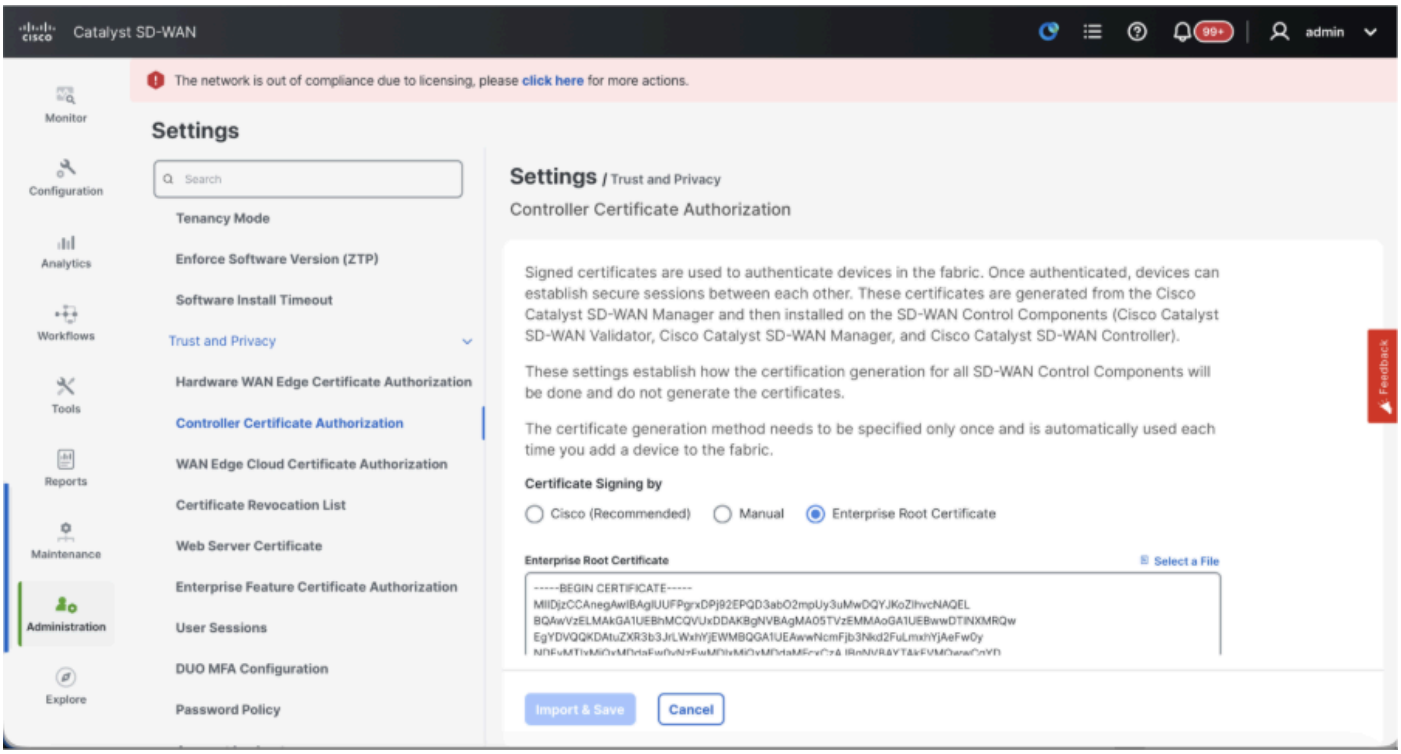
- Compruebe las configuraciones de la Autorización de certificados (CA), que decide la Autoridad de certificados utilizada para firmar los certificados. Podemos ver 3 opciones allí:

1. Autorización de certificado de extremo de WAN de hardware - Decide la CA para los routers periféricos SD-WAN de hardware.
    - Certificado en caja (certificado TPM/SUDI): con esta opción, el certificado preinstalado en el hardware del router se utiliza para establecer las conexiones de control (conexiones TLS/DTLS)
    - Certificado de empresa (firmado por la CA de empresa): con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe

actualizarse aquí.

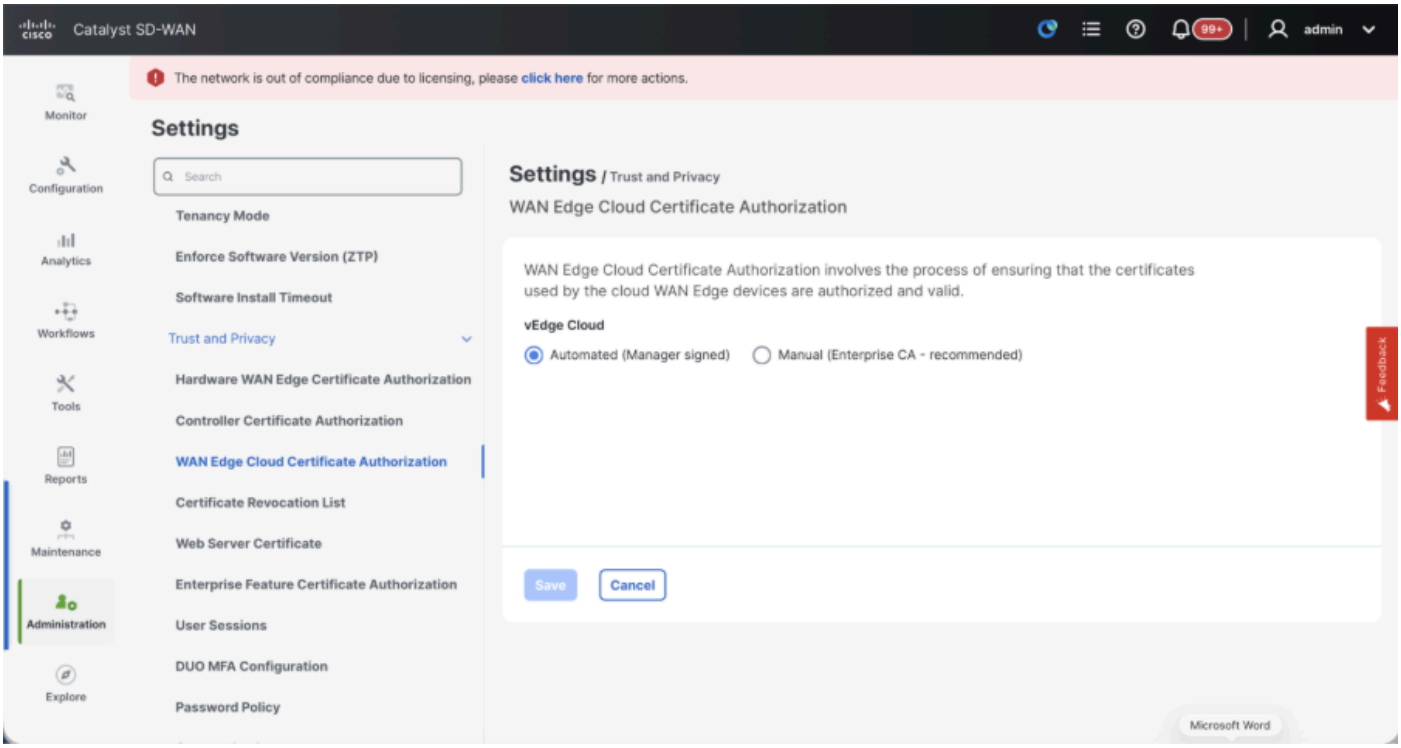


2. Autorización de certificado de controlador: decide la CA para los controladores SD-WAN.
    - Cisco (recomendado): los controladores utilizan los certificados firmados por Cisco PKI. vManage se pone en contacto automáticamente con el portal PNP mediante las credenciales de la cuenta inteligente configuradas en vManage y consigue que el certificado se firme y se instale en el controlador.
    - Manual: los controladores utilizan los certificados firmados por Cisco PKI. Firme manualmente el CSR mediante el portal Cisco PNP; para ello, acceda a la cuenta inteligente y la cuenta virtual de la superposición SD-WAN correspondiente.
    - Certificado raíz de empresa: con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

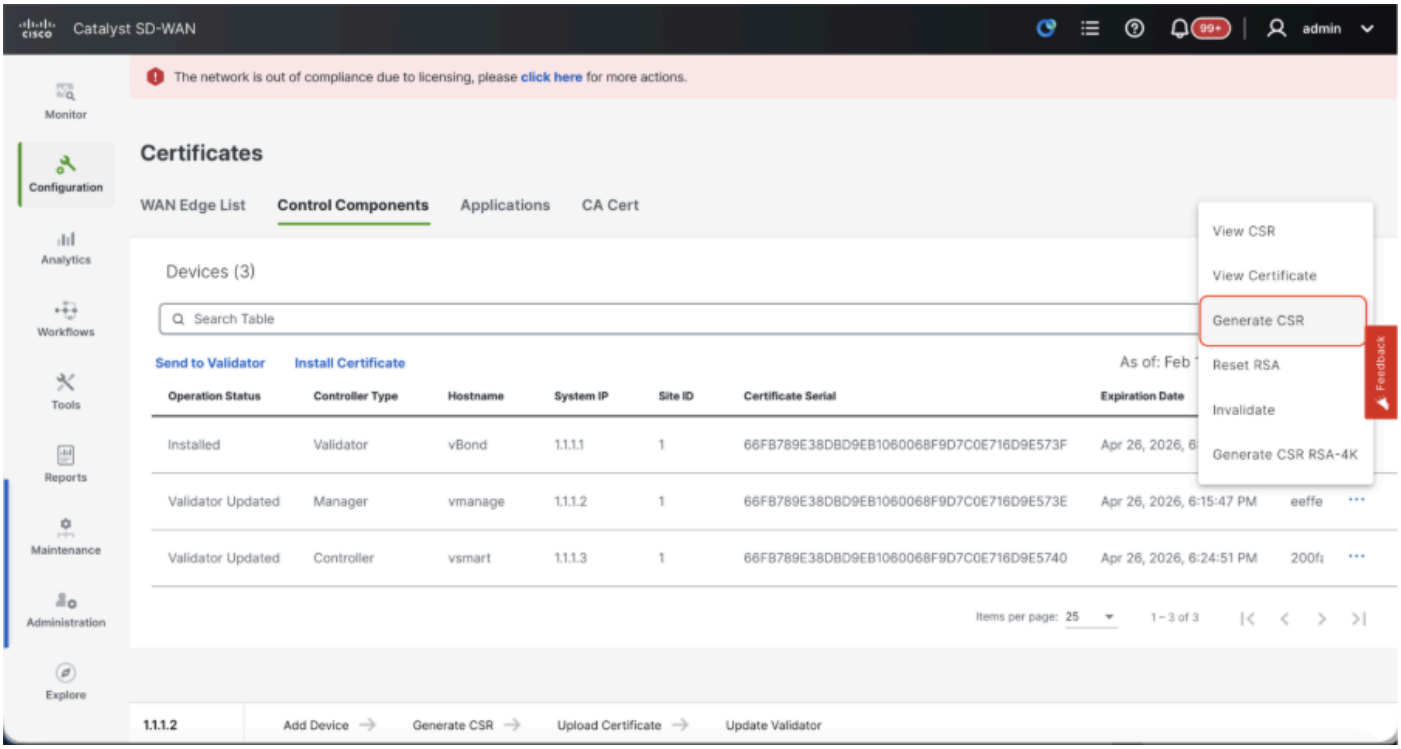


3. Autorización de certificado de nube de extremo de WAN: decide la CA para routers periféricos SD-WAN virtuales (CSR1000v, C8000v, nube vEdge)
    - Automatizado (vManage firmado): vManage firma automáticamente el CSR para los routers periféricos virtuales e instala el certificado en el router.
    - Manual (CA empresarial: recomendado): los routers virtuales utilizan certificados firmados por la autoridad de certificación empresarial de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

En este caso, si estamos utilizando nuestra propia CA, autoridad de certificación de empresa, elija Empresa.



- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers
- Haga clic en ... para Manager/vManage y haga clic en Generar CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.

Incorporación de vBond/Validator y vSmart/Controller a vManage

Vaya a Configuration > Devices > Control Components en caso de nodos vManage 20.15/20.18. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

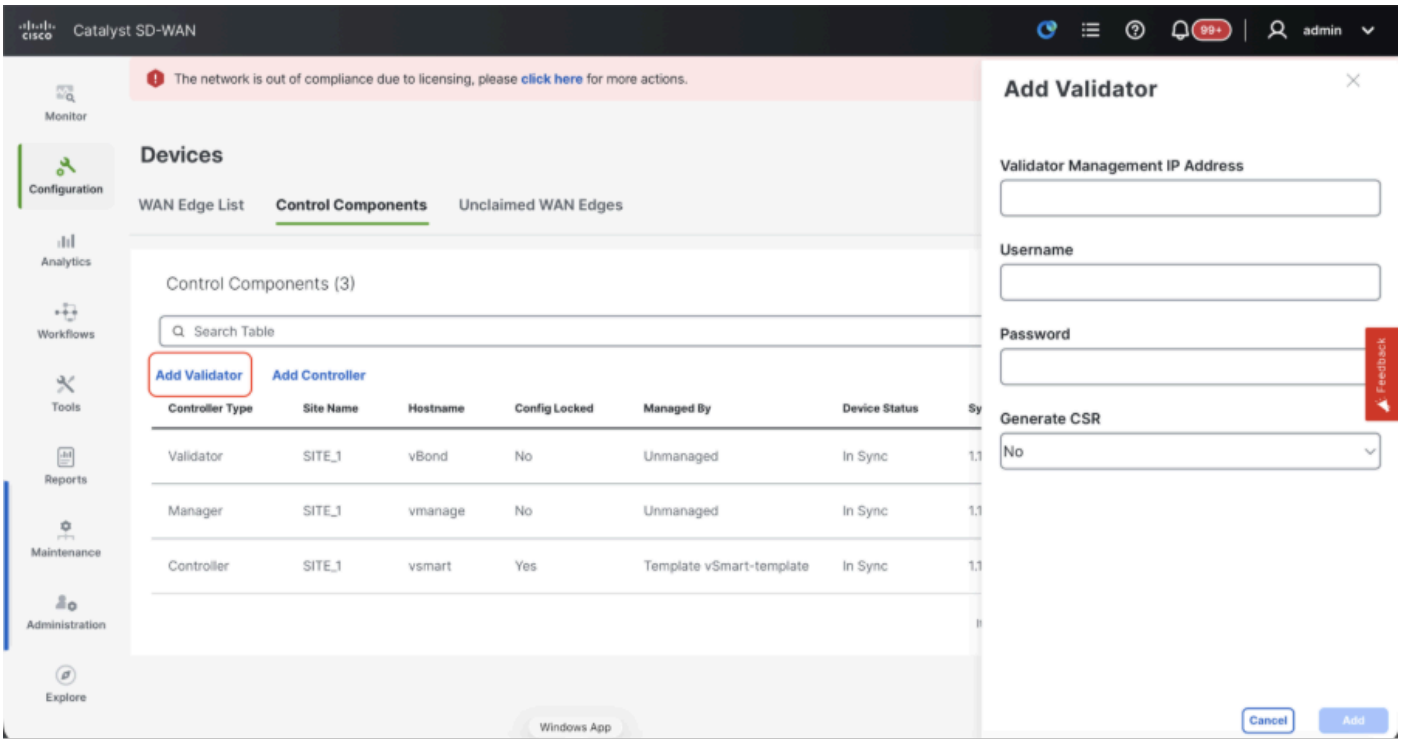
Incorporación de vBond/Validador

- Haga clic en AddvBonden caso de 20.12vManagerAgregar validadoren el caso de 20.15/20.18vManage. Se abre una ventana emergente, introduzca el IP de transporte VPN 0 de vBondque se puede alcanzar desde vManage.
- Verifique la disponibilidad mediante ping si se permite desde la CLI de vManagetovBondIP.

- Introduzca las credenciales de usuario de vBond.

Nota: Necesitamos usar las credenciales de administración de vBono una parte de usuario denetadmingroup. Puede verificarlo en la CLI de thevBond. Elija Sí en el menú desplegable de "Generar CSR" si necesitamos instalar un nuevo certificado para vBond

Nota: Si vBond está detrás de un dispositivo NAT/firewall, verifique si la IP de la interfaz VPN 0 de vBond se traduce a una IP pública. Si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la interfaz VPN 0 en este paso

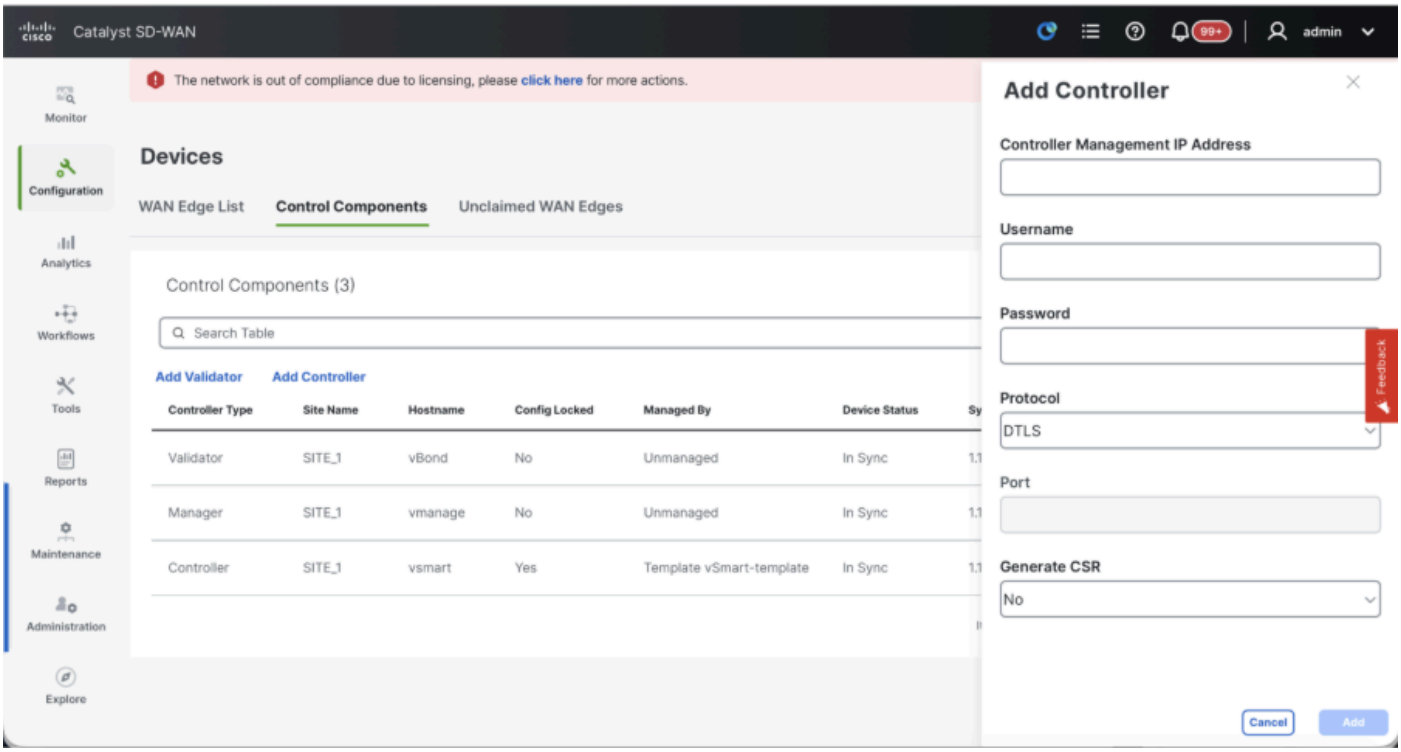


- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vBond.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vBonds, repita los mismos pasos.

Incorporación de vSmart/Controller:

- Haga clic en Add vSmart en el caso de 20.12 vManage o Add Controller en el caso de 20.15/20.18 vManage.
- Se abre una ventana emergente, introduzca la IP de transporte VPN 0 de vSmart, a la que se puede acceder desde vManage.
- Compruebe la disponibilidad mediante ping si se permite desde la CLI de vManage a vSmart IP.
- Introduzca las credenciales de usuario de vSmart Note que necesitamos para utilizar las credenciales de administrador de vSmart o una parte de usuario del grupo netadmin.
- Puede comprobarlo en la CLI de vSmart.
- Establezca el protocolo en TLS, si pretendemos utilizar TLS para routers para establecer conexiones de control con vSmart. Esta configuración también debe configurarse en CLI de nodos vsmarts y vManage.
- Elija Sí en el menú desplegable "Generar CSR" si necesitamos instalar un nuevo certificado para vSmart.

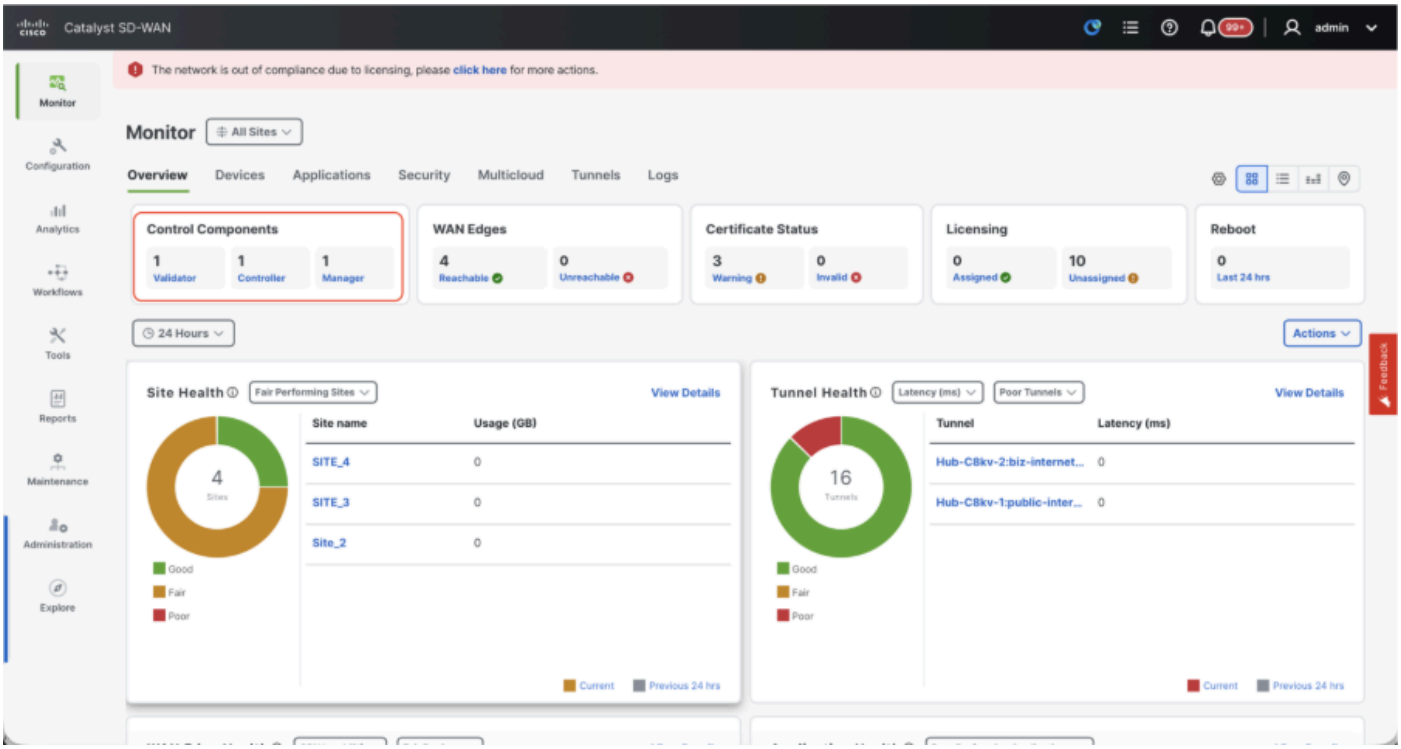
Nota: Si vSmart está detrás del dispositivo NAT/firewall, compruebe si la IP de la interfaz VPN 0 de vSmart se traduce a una IP pública y si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la IP de la interfaz VPN 0 en este paso.



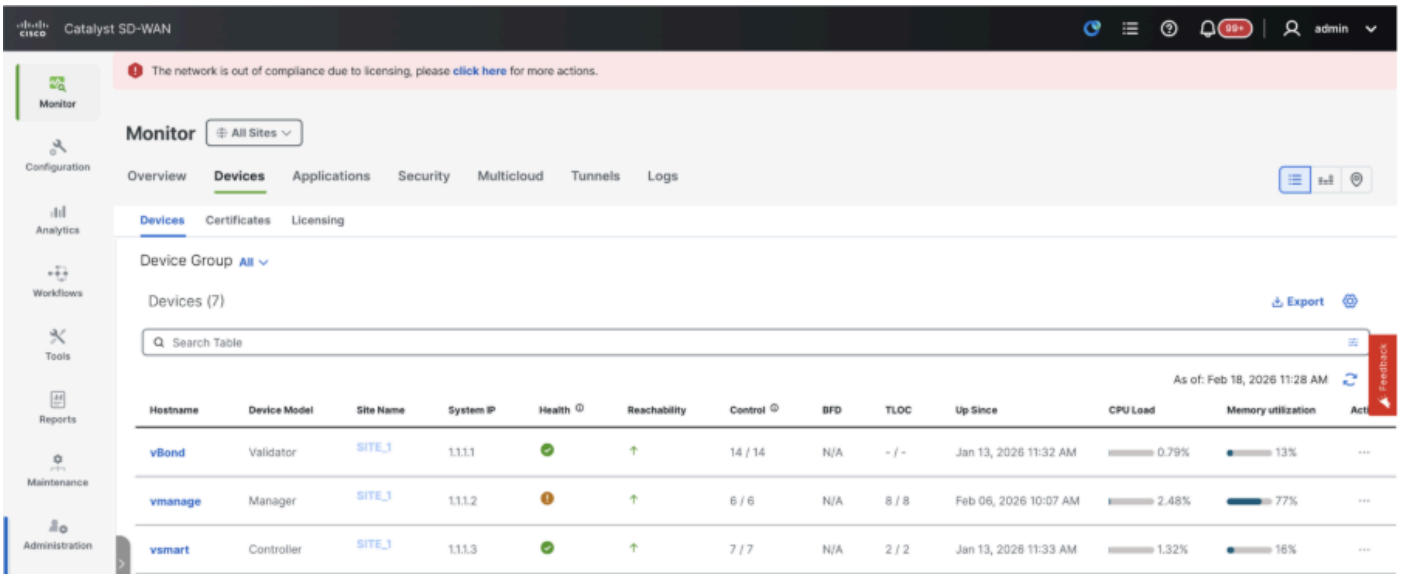
- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vSmart.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vsmarts, repita los mismos pasos.

Verificación

Una vez completados todos los pasos, verifique que todos los componentes de control sean accesibles en Monitor>Dashboard



- Haga clic en los componentes de control correspondientes y confirme que todos son accesibles.
- Navegue hasta Monitor > Devices y confirme que todos los componentes de control son accesibles.



Paso 3: Generar clúster de vManage

Fabric SD-WAN integrado con un clúster vManage en la superposición SD-WAN

Nota: vManage Cluster se puede configurar con 3 nodos vManage o 6 nodos vManage en función del número de sitios incorporados al fabric SD-WAN

Incorpore todos los controladores SD-WAN con un solo nodo vManage

Continúe con los pasos compartidos en "Controladores SD-WAN integrados con vManage de un solo nodo en la superposición SD-WAN" para activar primero el fabric SD-WAN con un nodo vManage e integrar todos los validadores (vBond) y controladores (vSmart) necesarios.

Configure las configuraciones CLI de todos los nodos de vManage que forman parte del clúster

- Configure el resto de los nodos de vManage. En el caso de un clúster de 3 nodos, tiene 2 nodos restantes que configurar; en el caso de un clúster de 6 nodos, tiene 5 nodos que configurar.
- Configure las configuraciones del sistema como se muestra:

```
config t
system
 host-name



 system-ip
```

```
 site-id


 organization-name


 vbond


commit
```

Nota: Si utilizamos URL como dirección vBond, asegúrese de configurar las direcciones IP del servidor DNS en la configuración VPN 0 o asegúrese de que se puedan resolver.

Estas configuraciones son necesarias para habilitar la interfaz de transporte utilizada para establecer conexiones de control con los routers y el resto de los controladores.

```
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
```

Configure también la interfaz de administración VPN 512para habilitar el acceso de administración fuera de banda al controlador.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

Configuración opcional:

- Puede consultar las configuraciones de su controlador existente y, si la configuración que se muestra aquí está presente, puede agregar esta configuración a los nuevos controladores.
- Configure el protocolo de control como TLS solo si hay un requisito para que los routers establezcan conexiones de control seguras con los nodos vManage mediante TLS. De forma predeterminada, todos los controladores y routers establecen una conexión de control mediante DTLS. Se trata de una configuración opcional que solo se requiere en los nodos vSmart y vManage, según sus necesidades.

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

Configurar la interfaz de servicio en todos los nodos de vManage

Configure la interfaz de servicio en todos los thevManagenodes, incluido vManage-1, que ya se ha incorporado. Esta interfaz se utiliza para la comunicación del clúster, lo que significa comunicación entre losnodos de administración del clúster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Asegúrese de que se utiliza la misma subred IP para la interfaz de servicio en todos los nodos delclúster de administración.

Configurar credenciales de clúster

Podemos utilizar las mismas credenciales de administrador de thevManagenodes para configurar thevManagecluster. De lo contrario, podemos configurar una nueva credencial de usuario que forma parte denetadmingroup. Las configuraciones para configurar las nuevas credenciales de usuario son las siguientes

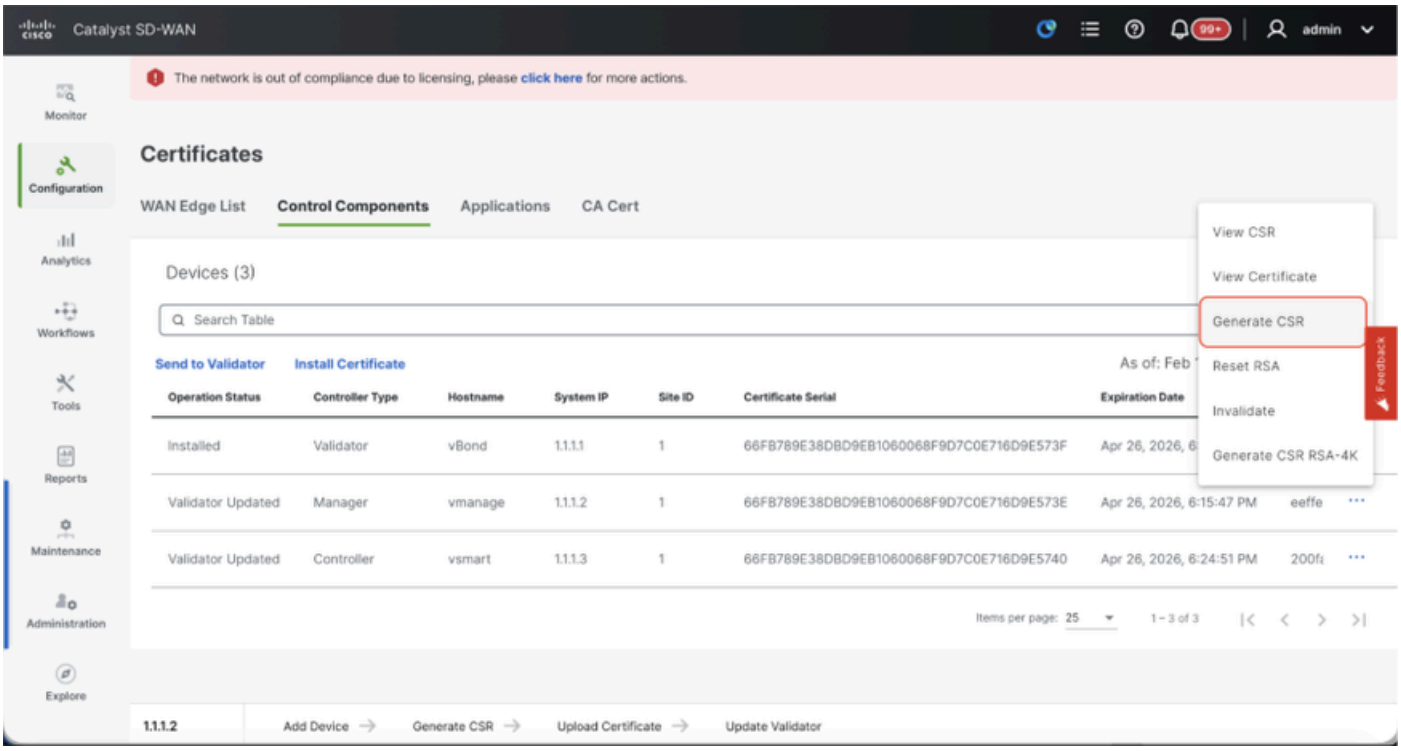
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

Asegúrese de configurar las mismas credenciales de usuario en todos los thevManagenodesque forman parte del clúster.Si decidimos utilizar credenciales de administrador, debe ser el mismo nombre de usuario/contraseña en todos los thevManagenodes.

Instalar el certificado de dispositivo en todos los nodos de vManage

- Inicie sesión en tovManageUI de todos los thevManagenodes mediante la dirección URL https://<vmanage-ip>en su navegador. Utilice la dirección IP VPN 512 de los vManagenodes respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

  Haga clic en ... para Manager/vManage y haga clic en Generate CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Complete este paso en todos los nodos de vManage que forman parte del clúster.

Preparación para crear el clúster de vManage

- En la interfaz de usuario web de vManage-1, vaya a Administration > Cluster Management, haga clic en ... en Actions for vManage-1, elija Edit.
- El personaje del nodo se elige automáticamente en función del personaje que elegimos mientras se giraba la máquina virtual.

Nota: Para un clúster de 3 nodos, los 3 nodos de vManage se activan con compute+data como persona.

- Para un clúster de 6 nodos, 3 nodos de vManage se activan con compute+data como persona y 3 nodos de vManage se activan con datos como persona.
- En el menú desplegable Dirección IP del administrador, asegúrese de elegir la dirección IP de la interfaz de servicio de vManage.
- Introduzca el nombre de usuario y la contraseña que desee utilizar para activar el clúster de vManage, que se conoce como credenciales del clúster.
- Como se ha mencionado anteriormente, se deben configurar las mismas credenciales en todos los nodos de vManage y se deben utilizar al agregar todos los nodos al clúster.

Configuración opcional:

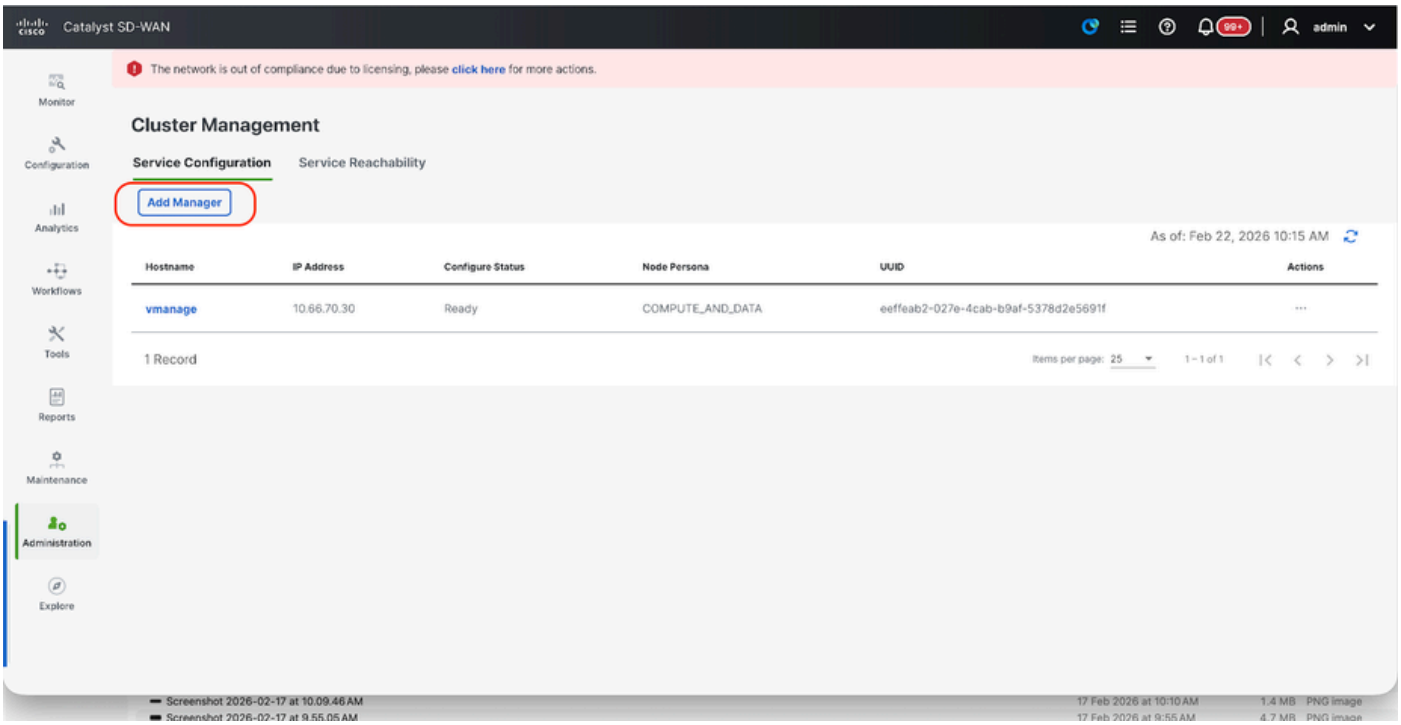
Consulte esta configuración en el clúster existente para Habilitar SDAVC: sólo debe comprobarse si es necesario y sólo es necesario en un nodo vManage del clúster.

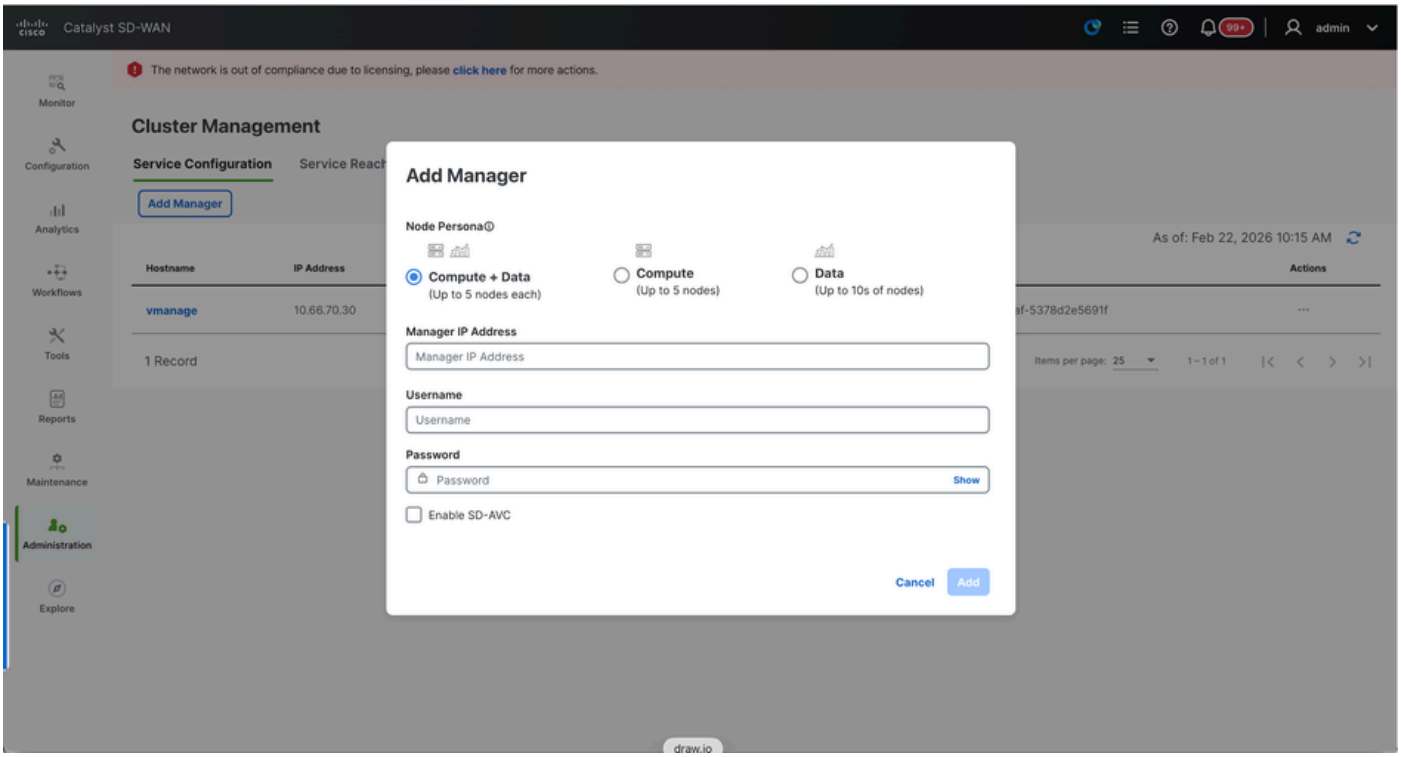
Haga clic en Actualizar.

- Al publicar esto, los servicios de vManage NMS se reinician en segundo plano y la interfaz de usuario no está disponible durante unos minutos de entre 5 y 10 minutos. Durante este tiempo, está disponible el acceso CLI de vManage.
- Una vez que se pueda acceder a la interfaz de usuario de vManage-1, vaya a Administration > Cluster Management, asegúrese de que la IP de la interfaz de servicio de vManage se refleja en IP address,El estado de configuración es Preparado y el personaje del nodo se refleja correctamente. Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios están disponibles.
- Si vemos que alguno de los servicios aún no está disponible, espere. Por lo general, toma alrededor de 20 a 30 minutos.

Creación del clúster de vManage

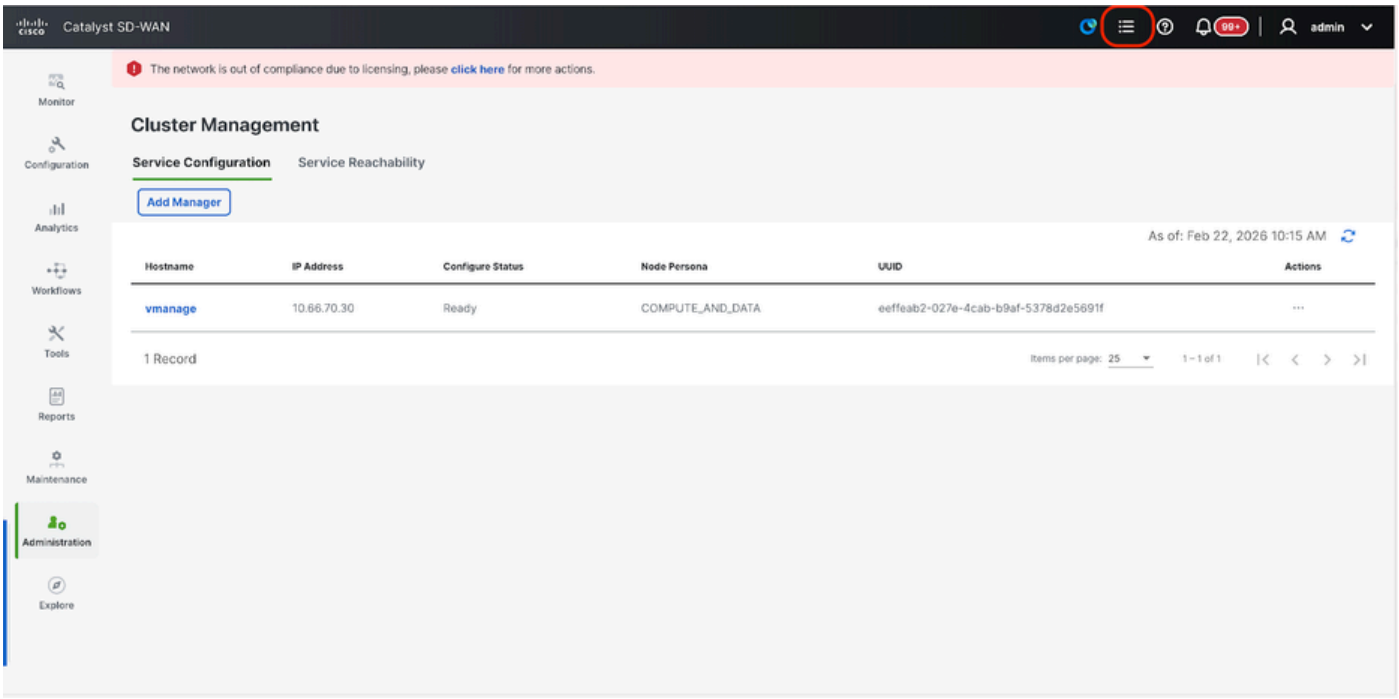
- En la interfaz de usuario web de vManage-1, vaya a Administration > Cluster Management, en la sección Service Configuration,
- Haga clic en Add Manager, aparecerá una ventana emergente:





- Elija el Node persona en función de las configuraciones de persona realizadas mientras se giraba el nodo vManage - 2.
- Introduzca la IP de la interfaz de servicio de vManage-2 en Dirección IP del jefe
- Introduzca el nombre de usuario y la contraseña, que son las mismas credenciales que utilizamos en el paso 6.
- Habilitar SDAVC: no se debe marcar porque ya lo habríamos activado en vManage-1
- Haga clic en Agregar.
- Al publicar esto, los servicios de vManage NMS se reinician en segundo plano para los nodos de vManage 1 y 2. La interfaz de usuario no está disponible durante unos minutos de 5 a 10 minutos aproximadamente para vManage 1 y 2.

- Durante este tiempo, está disponible el acceso CLI de vManage 1 y 2.
- Una vez que se pueda acceder a la interfaz de usuario de vManage-1, vaya a Administration > Cluster Management, asegúrese de que la IP de la interfaz de servicio de vManage se refleja en IP address, Configure Status is Ready y node persona se refleja correctamente.
- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios están disponibles para ambos nodos de vManage.
- Si vemos que alguno de los servicios aún no está disponible, espere. Por lo general, toma alrededor de 5 a 10 minutos.
- Puede comprobar el estado del proceso de adición de clústeres en la lista de tareas disponible en la esquina superior derecha de la interfaz de usuario de vManage.



- Puede buscar una lista de tareas activas y, si la tarea sigue apareciendo en Lista de tareas activas, indica que la tarea no se ha completado todavía.
- Puede hacer clic en la tarea para comprobar el progreso de la misma. Si la tarea no aparece en Lista de tareas activas, cambie a Completada y asegúrese de que la tarea se ha completado correctamente.
- Solo después de validar estos puntos, continúe con el siguiente paso.

Estos puntos deben tenerse en cuenta antes de agregar el siguiente nodo al clúster:

Verifique estos puntos en todas las UI de los nodos vManage que se han agregado al clúster hasta el momento:

- Vaya a Monitor > Overview of vManage UI y asegúrese de que el número de nodos de vManage se reflejen correctamente y se vean accesibles en función del número de nodos agregados al clúster.

- Navegue hasta Administration > Cluster Management y asegúrese de que la IP de la interfaz de servicio de vManage se refleje bajo IP address, Configure Status is Ready y node persona se refleje correctamente.

- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios son accesibles para ambos nodos de vManage.

- Cada vez que se agrega un nodo al clúster, se reinician los servicios NMS de todos los nodos del clúster, por lo que la interfaz de usuario de todos esos nodos queda inaccesible durante algún tiempo.
- Dependiendo del número de nodos del clúster, puede ser necesario más tiempo para que se realice una copia de seguridad de la interfaz de usuario y todos los servicios sean accesibles.
- Puede supervisar la tarea en Lista de tareas disponible en la esquina superior derecha de la interfaz de usuario de vManage.
- En la interfaz de usuario de vManage de cada nodo agregado al clúster, necesitamos ver todos los routers, plantillas y políticas si estuvieran disponibles en vManage-1.
- Si esas configuraciones no estaban presentes en vManage-1, los vBonds y vSmarts que se agregaron a vManage-1 y también las configuraciones de Administration > Settings para Organization-name, vBond, Certificate Authorization deben reflejarse en el resto de los nodos vManage agregados al clúster.
- Repita los mismos pasos para el resto de los nodos de vManage.

Paso 4: Configuración del clúster de DR en espera en frío

Configuración del clúster de DR en espera en frío

Puede activar un clúster más de vManage siguiendo los pasos descritos en el Paso 4: Generar clúster de vManage. Publicación que completa los pasos descritos en el paso 6: Copia de seguridad/Restauración de Config-db para restaurar la copia de seguridad de config-db en el clúster en espera.

Paso 5: Copia de seguridad/restauración de Config-db

Recopilar copia de seguridad de la base de datos de configuración de vManage y restaurar en otro nodo de vManage

Recopilar copia de seguridad de Configuration-DB:

- En el fabric SD-WAN que se está utilizando actualmente, puede generar una copia de seguridad de la base de datos de configuración desde el clúster de vManage.
- Tenga en cuenta que solo debemos generar una copia de seguridad de la base de datos de configuración en un nodo del clúster de vManage que es el líder de la base de datos de configuración.

- Para vManage independiente, vManage es el líder de la base de datos de configuración.
- En el clúster vManage, identifique el nodo líder configuration-db mediante el comando request nms configuration-db diagnostics.Puede ejecutar este comando en todos los nodos del clúster vManage de 3 nodos.
- En un clúster de 6 nodos, asegúrese de ejecutar este comando en los nodos vManage

donde configuration-db está habilitado para identificar el nodo líder. Navegue hasta Administración > Administración de clústeres para verificar lo mismo:

- Como vemos en la captura de pantalla, los nodos configurados con persona COMPUTE_AND_DATA tienen configuration-db en ejecución.

Puede verificar lo mismo mediante el comando requestnmsconfiguration-dbstatus en vManageCLI. El resultado es como se muestra

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

- Una vez ejecutado el comandorequest nms configuration-db diagnostics en estos nodos, el resultado es el siguiente:
- Busque el campo resaltado para "IsLeader". Si se establece en 1, indica que el nodo es el nodo líder y podemos recopilar una copia de seguridad de la base de datos de configuración de él.

```
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     .
```

Utilice este comando para recopilar la copia de seguridad de la base de datos de configuración del nodo vManage del líder de la base de datos de configuración identificado.

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

El resultado esperado es el siguiente:

```
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#
```

- Tome nota de las credenciales de configuration-db si se ha actualizado.
- Si no conoce las credenciales de la base de datos de configuración, póngase en contacto con el TAC para recuperar las credenciales de la base de datos de configuración de los nodos de vManage existentes.
- Las credenciales de la base de datos de configuración predeterminada son username: neo4j y contraseña: contraseña

Restaurar copia de seguridad de Configuration-db en otro nodo de vManage

Copie la copia de seguridad de la base de datos de configuración en el directorio /home/admin/ de vManage mediante SCP.

Ejemplo de resultado del comando scp:

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

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

Para restaurar la copia de seguridad de la base de datos de configuración, primero debemos configurar las credenciales de la base de datos de configuración. Si sus credenciales de configuration-db son predeterminadas (neo4j/password), podemos saltarnos este paso.

Para configurar las credenciales de configuration-db, utilice el comando request nms configuration-db update-admin-user.Use el nombre de usuario y la contraseña que desee.

Tenga en cuenta que el servidor de aplicaciones de vManage se reinicia. Debido a lo cual, la interfaz de usuario de vManage se vuelve inaccesible durante un breve período de tiempo.

```
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#
```

Publicación en la que podemos continuar con la restauración de la copia de seguridad de la base de datos de configuración:

Podemos utilizar el comando request nms configuration-db restore path /home/admin/< > para restaurar la base de datos de configuración en el nuevo vManage:

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

Una vez restaurada la base de datos de configuración, asegúrese de que se puede acceder a la interfaz de usuario de vManage. Espere unos 5 minutos e intente acceder a la interfaz de usuario.

Una vez que haya iniciado sesión correctamente en la interfaz de usuario, asegúrese de que la lista de routers periféricos, la plantilla, las políticas y el resto de las configuraciones que estaban presentes en la interfaz de usuario de vManage anterior o existente se reflejan en la nueva interfaz de usuario de vManage.

Paso 6: Reautenticación de controladores e invalidación de controladores antiguos

Una vez restaurada la base de datos de configuración, necesitamos volver a autenticar todos los nuevos controladores (vmanage/vsmart/vbond) en el fabric

---

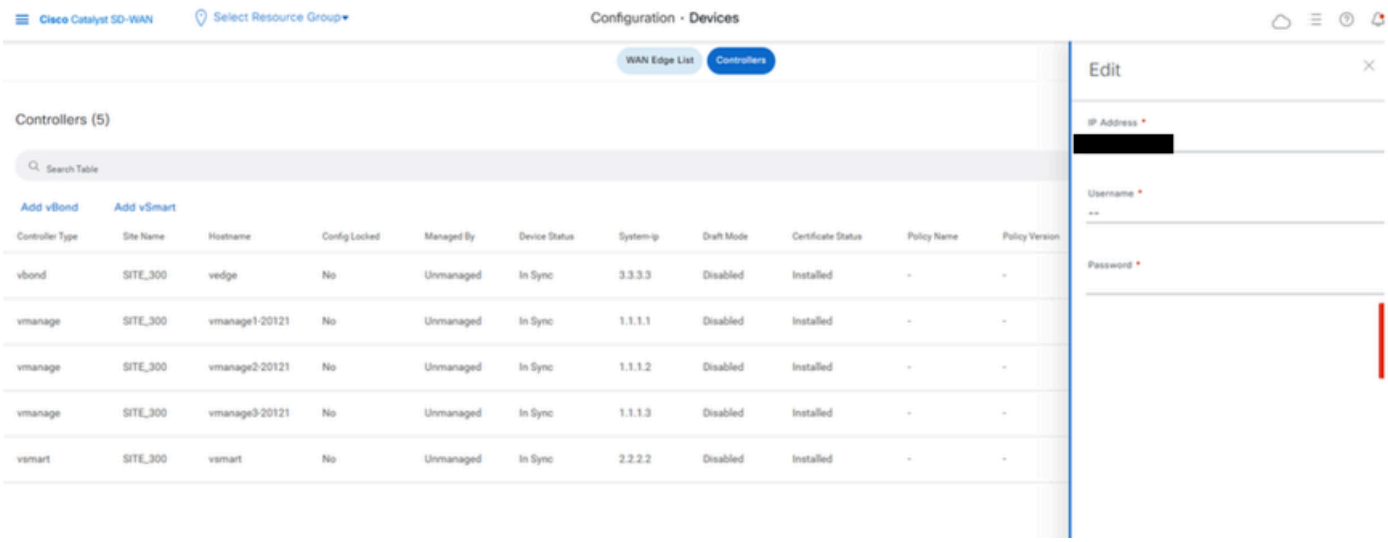
Nota: En la producción real, si la IP de interfaz utilizada para la reautenticación es la IP de interfaz de túnel, debe asegurarse de que se permite el servicio NETCONF en la interfaz

---

de túnel de vManage, vSmart y vBond, así como en los firewalls a lo largo de la ruta. El puerto del firewall que se debe abrir es el puerto TCP 830 como regla bidireccional desde el clúster DR a todos los vBonds y vsmarts .

En vmanage UI, haga clic en Configuration > Devices > Controllers

- Haga clic en los tres puntos cerca de cada controlador y haga clic en Editar



- Reemplace la dirección ip (system-ip of the controller) por la dirección ip transport vpn 0 (tunnel interface). Introduzca el nombre de usuario y la contraseña y haga clic en save (guardar)
- Haga lo mismo con todos los nuevos controladores del fabric

Sincronizar la cadena de certificados raíz

Una vez que todos los controladores estén incorporados, complete este paso:

En cualquier servidor Cisco SD-WAN Manager del clúster recién activo, realice estas acciones:

Ingrese este comando para sincronizar el certificado raíz con todos los dispositivos Cisco Catalyst SD-WAN en el agrupamiento recientemente activo:

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

Ingrese este comando para sincronizar el UUID de Cisco SD-WAN Manager con el Validador de Cisco SD-WAN:

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

Una vez restaurado el fabric y activadas las sesiones de control y bfd para todos los bordes y controladores del fabric, debemos invalidar los controladores antiguos (vmanage/vsmart/vbond) de la interfaz de usuario

- En vmanage UI, haga clic en Configuration > Devices > Certificates .
- Haga clic en Controladores
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en invalidar
- Haga clic en enviar a vbond
- En vmanage UI, haga clic en Configuration > Devices > Controllers
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en Eliminar

Paso 7: Registrar cheques

Nota: Continúe con la sección Post Checks (Comprobaciones posteriores) que se muestra aquí, que es común a todas las combinaciones de implementación.

Combinación 5: Clúster vManage + DR habilitado

Instancias necesarias:

- 3 o 6 vManage (clúster principal)
- 3 o 6 vManage (clúster de DR en espera)
- 1 o más vBond (distribuidos entre Data Centers primarios y de DR)
- 1 o más vSmart (distribuido entre Data Centers primarios y de recuperación ante desastres)

Pasos:

1. Abra todas las instancias mediante los pasos comunes
2. Comprobaciones previas
3. Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage
4. Generar clúster de vManage
5. Configuración del clúster de DR en espera en frío
6. Copia de seguridad/restauración de Config-db
7. Registrar cheques

Paso 1: Comprobaciones previas

- Asegúrese de que el número de instancias de Cisco SD-WAN Manager activas sea idéntico al número de instancias de Cisco SD-WAN Manager recién instaladas.

- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager ejecuten la misma versión de software.

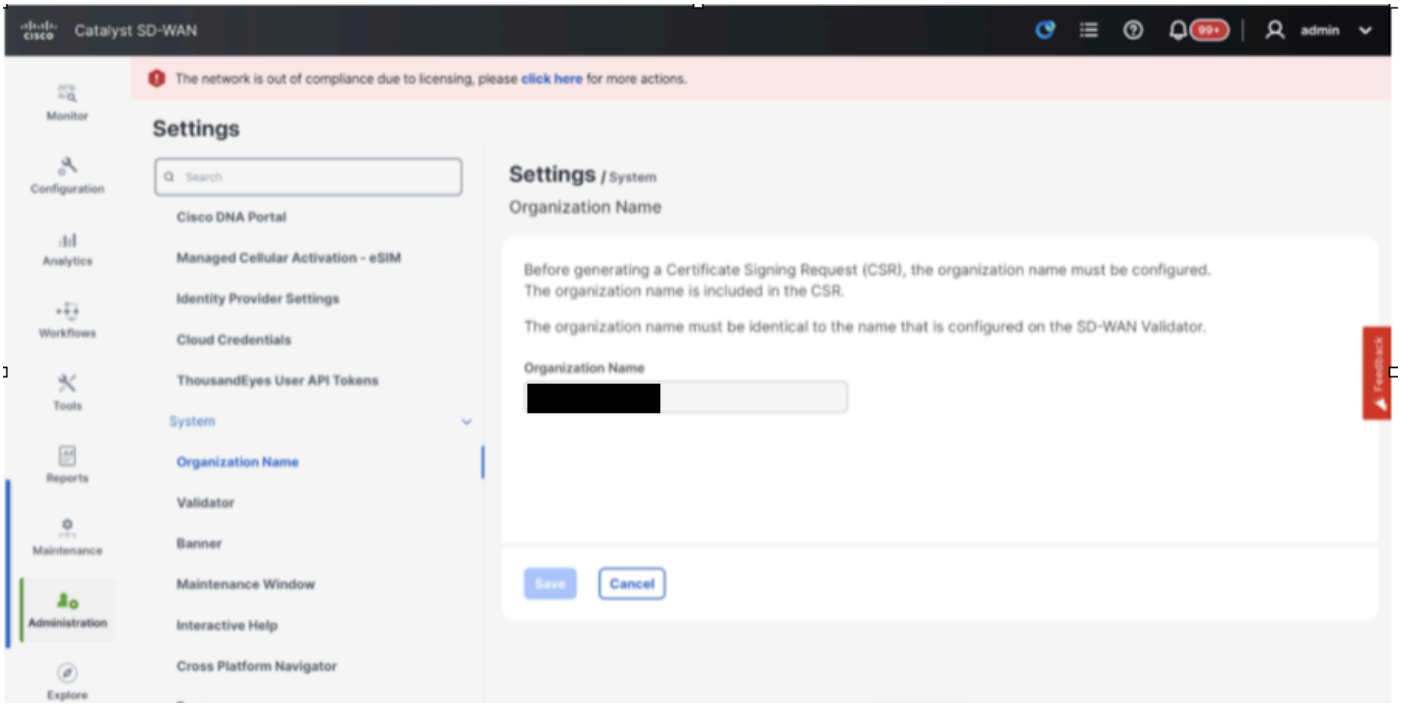
- Asegúrese de que todas las instancias activas y nuevas de Cisco SD-WAN Manager puedan alcanzar la dirección IP de administración del Cisco SD-WAN Validator.

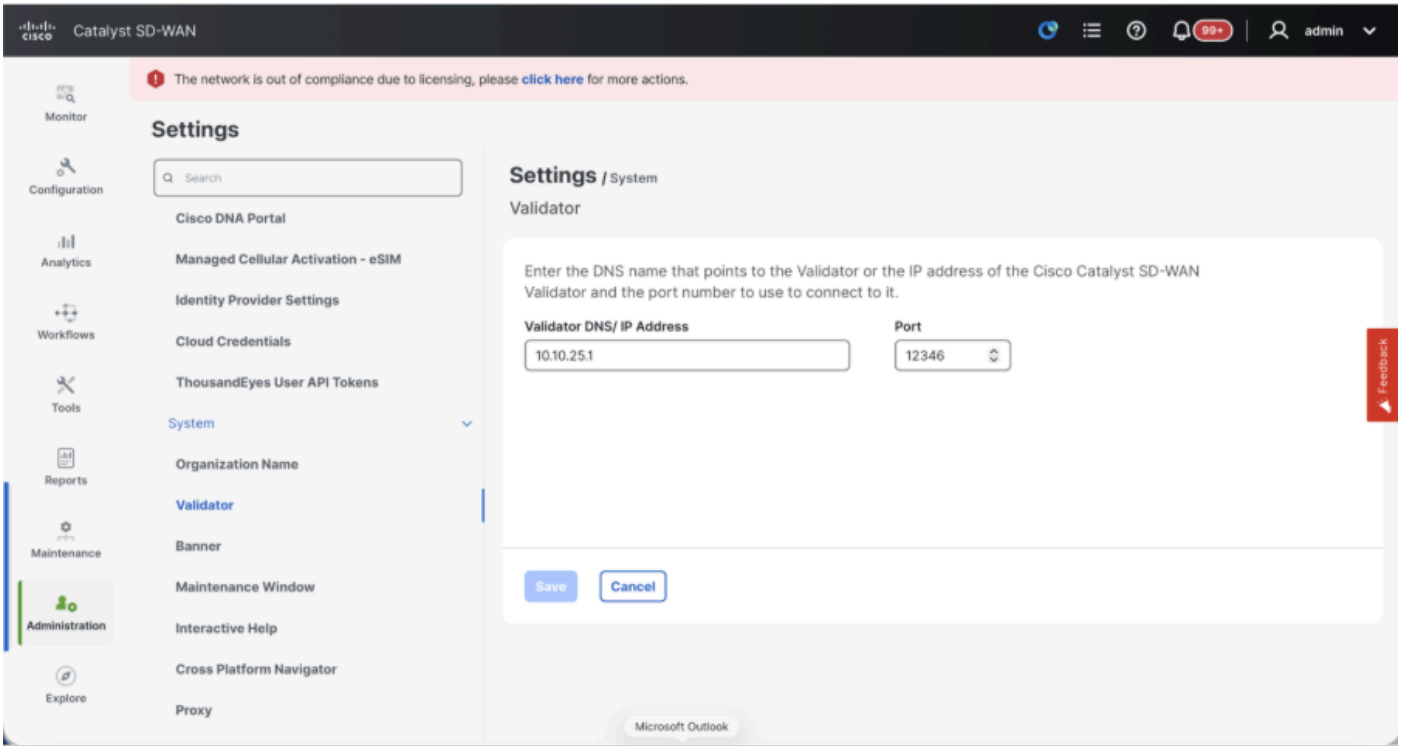
- Asegúrese de que los certificados se hayan instalado en las instancias de Cisco SD-WAN Manager recién instaladas.
- Asegúrese de que los relojes de todos los dispositivos Cisco Catalyst SD-WAN, incluidas las nuevas instancias de Cisco SD-WAN Manager instaladas, estén sincronizados.
- Asegúrese de que se haya configurado un nuevo conjunto de IP del sistema e ID del sitio en las instancias de Cisco SD-WAN Manager recién instaladas, junto con la misma configuración básica que el clúster activo.

Paso 2: Configuración de la interfaz de usuario, los certificados y los controladores integrados de vManage

Actualizar las configuraciones en la interfaz de usuario de vManage

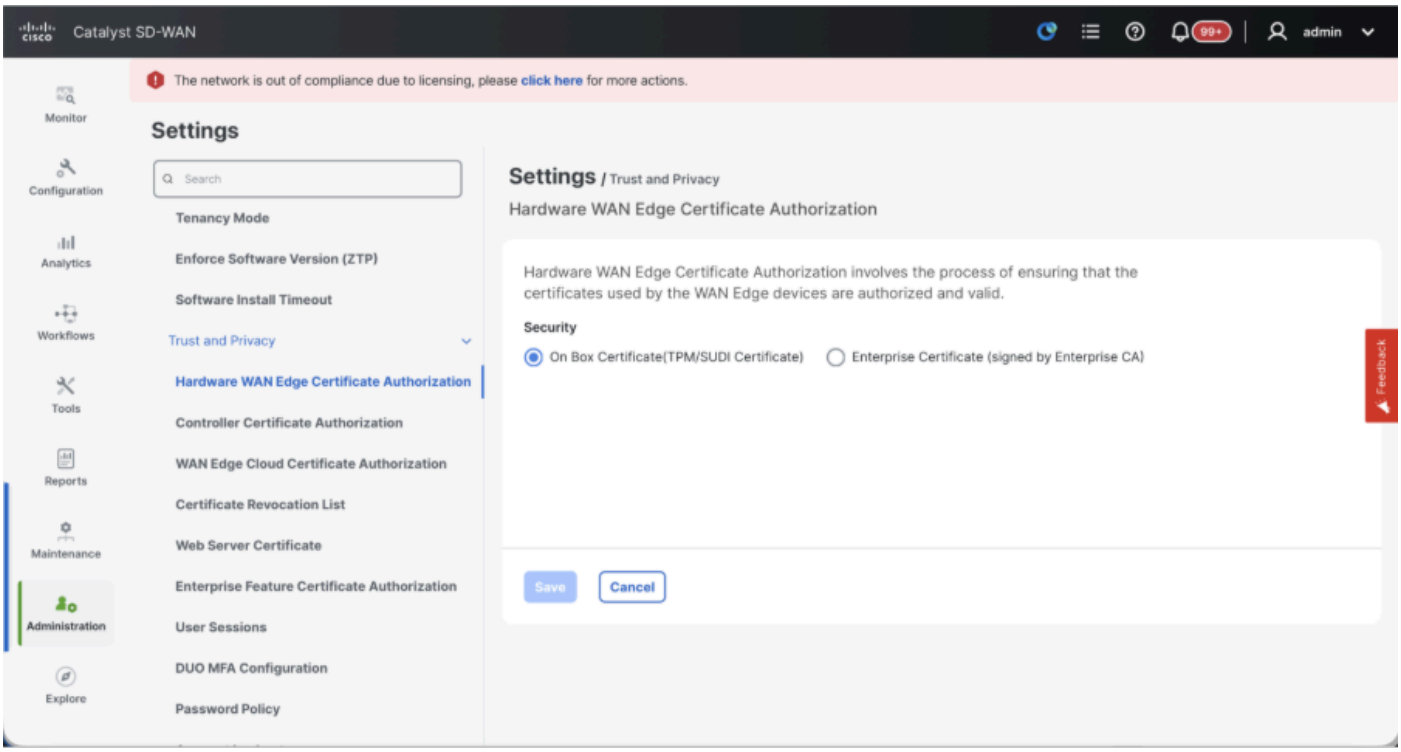
- Una vez agregadas las configuraciones del paso 1 en la CLI de todos los controladores, podemos acceder a la interfaz de usuario web de vManage mediante la dirección URL https://<vmanage-ip> en el navegador. Utilice la dirección IP VPN 512 de los nodos vManage respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Navegue hasta Administration > Settings y complete estos pasos.
- Configure el nombre de la organización y la dirección URL/IP del validador/vBond. Configure el mismo valor que en la CLI del nodo vManage.
- En vManage 20.15/20.18, estas configuraciones están disponibles en la sección Sistema.



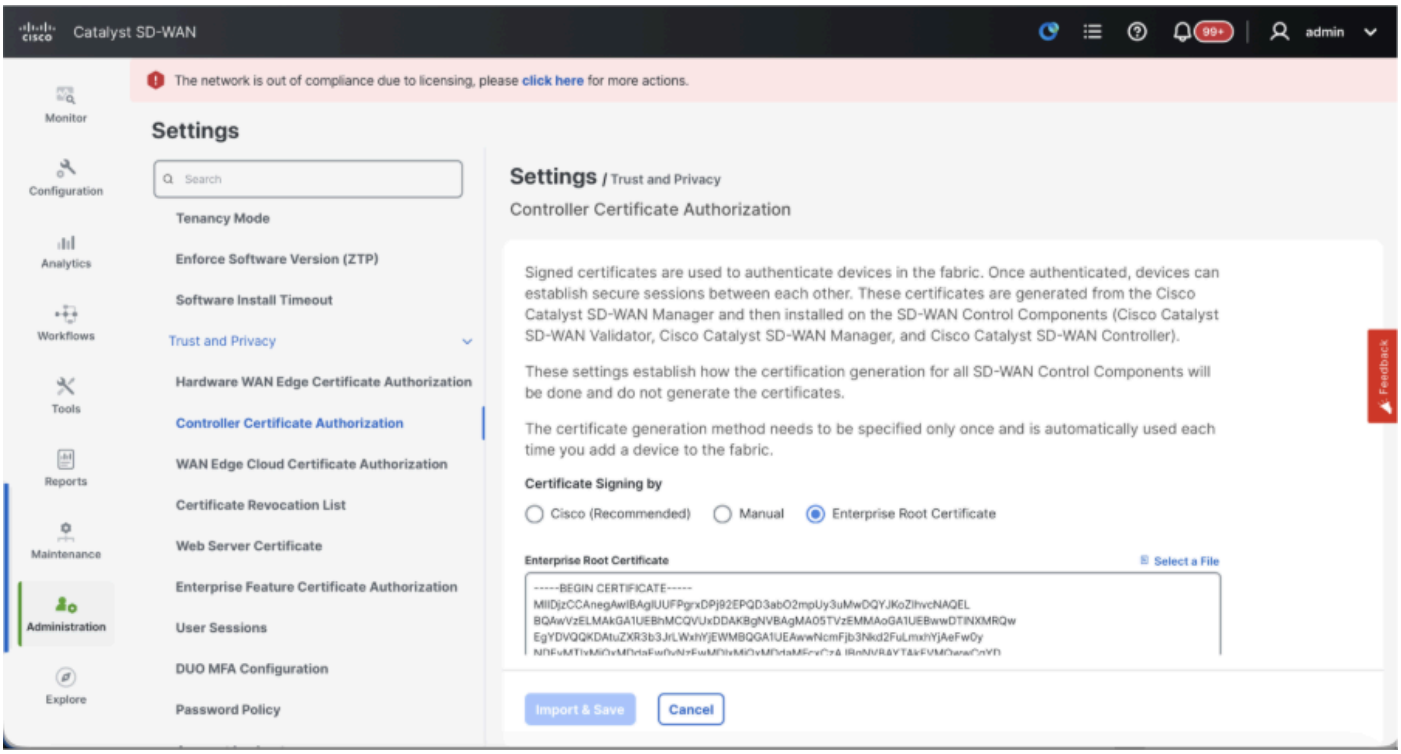


- Compruebe las configuraciones de la Autorización de certificados (CA), que decide la Autoridad de certificados utilizada para firmar los certificados. Podemos ver 3 opciones allí:

1. Autorización de certificado de extremo de WAN de hardware - Decide la CA para los routers periféricos SD-WAN de hardware.
    - Certificado en caja (certificado TPM/SUDI): con esta opción, el certificado preinstalado en el hardware del router se utiliza para establecer las conexiones de control (conexiones TLS/DTLS)
    - Certificado de empresa (firmado por la CA de empresa): con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

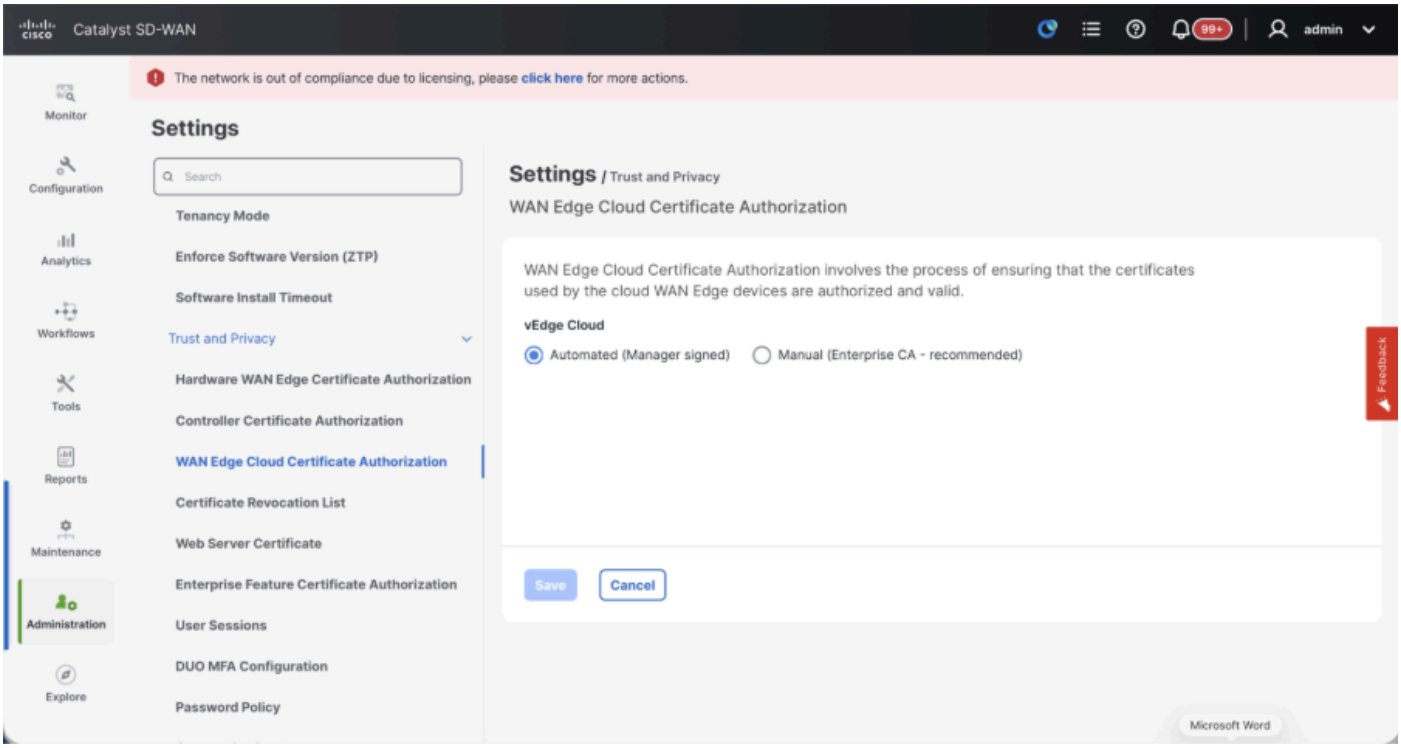


2. Autorización de certificado de controlador: decide la CA para los controladores SD-WAN.
    - Cisco (recomendado): los controladores utilizan los certificados firmados por Cisco PKI. vManage se pone en contacto automáticamente con el portal PNP mediante las credenciales de la cuenta inteligente configuradas en vManage y consigue que el certificado se firme y se instale en el controlador.
    - Manual: los controladores utilizan los certificados firmados por Cisco PKI. Firme manualmente el CSR mediante el portal Cisco PNP; para ello, acceda a la cuenta inteligente y la cuenta virtual de la superposición SD-WAN correspondiente.
    - Certificado raíz de empresa: con esta opción, los routers utilizan certificados firmados por la autoridad de certificación de empresa de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

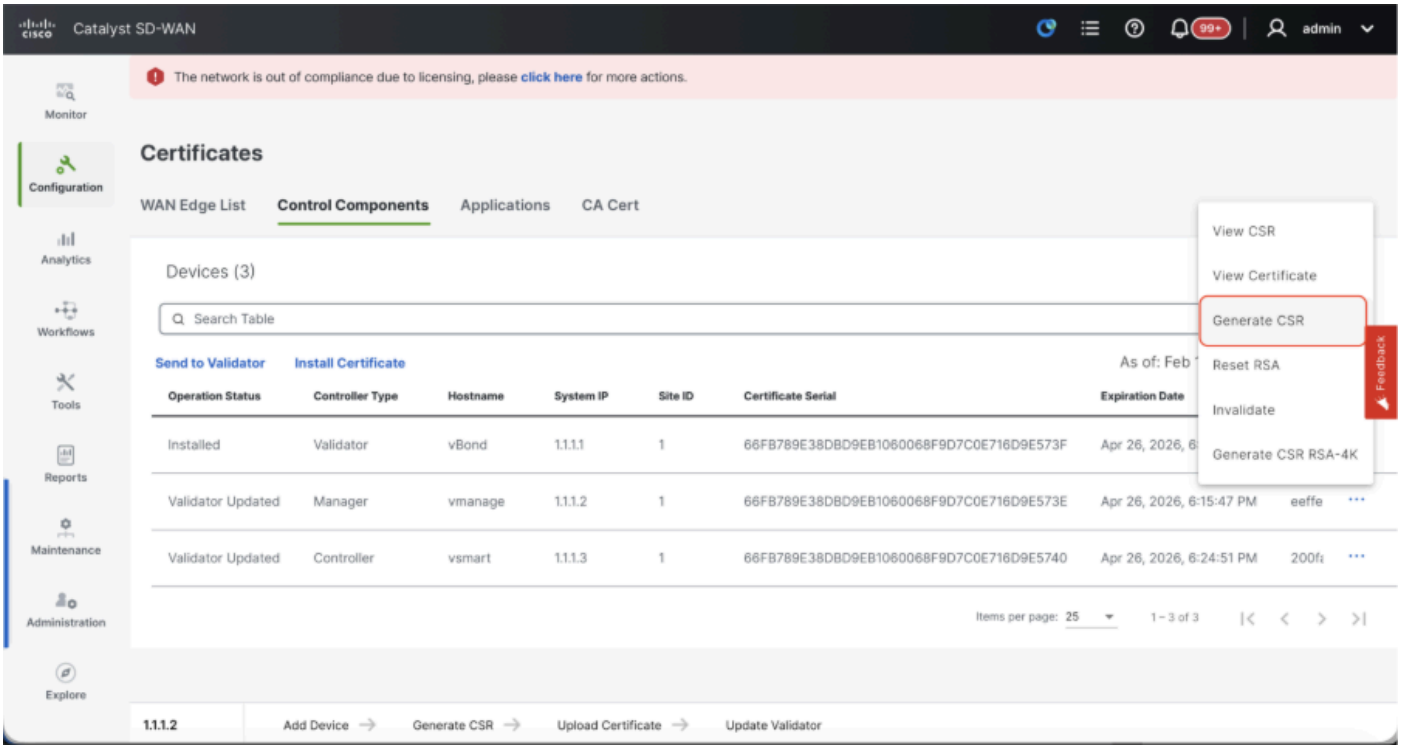


3. Autorización de certificado de nube de extremo de WAN: decide la CA para routers periféricos SD-WAN virtuales (CSR1000v, C8000v, nube vEdge)
    - Automatizado (vManage firmado): vManage firma automáticamente el CSR para los routers periféricos virtuales e instala el certificado en el router.
    - Manual (CA empresarial: recomendado): los routers virtuales utilizan certificados firmados por la autoridad de certificación empresarial de su organización. Al elegir esta opción, el certificado raíz de la CA empresarial debe actualizarse aquí.

En este caso, si estamos utilizando nuestra propia CA, autoridad de certificación de empresa, elija Empresa.



- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers
- Haga clic en ... para Manager/vManage y haga clic en Generar CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.

Incorporación de vBond/Validator y vSmart/Controller a vManage

Vaya a Configuration > Devices > Control Components en caso de nodos vManage 20.15/20.18. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

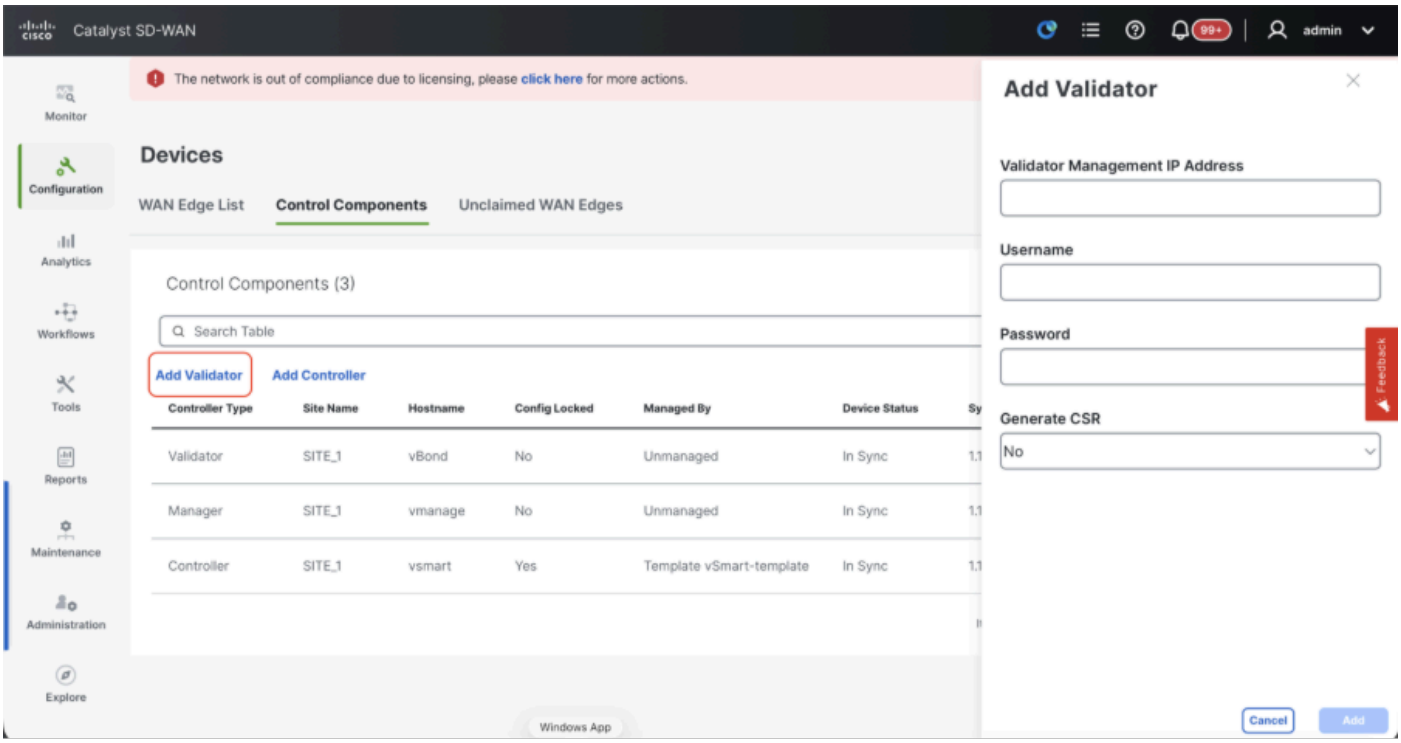
Incorporación de vBond/Validador

- Haga clic en AddvBonden caso de 20.12vManagerAgregar validadoren el caso de 20.15/20.18vManage. Se abre una ventana emergente, introduzca el IP de transporte VPN 0 de vBondque se puede alcanzar desde vManage.
- Verifique la disponibilidad mediante ping si se permite desde la CLI de vManagetovBondIP.

- Introduzca las credenciales de usuario de vBond.

Nota: Necesitamos usar las credenciales de administración de vBono una parte de usuario denetadmingroup. Puede verificarlo en la CLI de thevBond. Elija Sí en el menú desplegable de "Generar CSR" si necesitamos instalar un nuevo certificado para vBond

Nota: Si vBond está detrás de un dispositivo NAT/firewall, verifique si la IP de la interfaz VPN 0 de vBond se traduce a una IP pública. Si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la interfaz VPN 0 en este paso

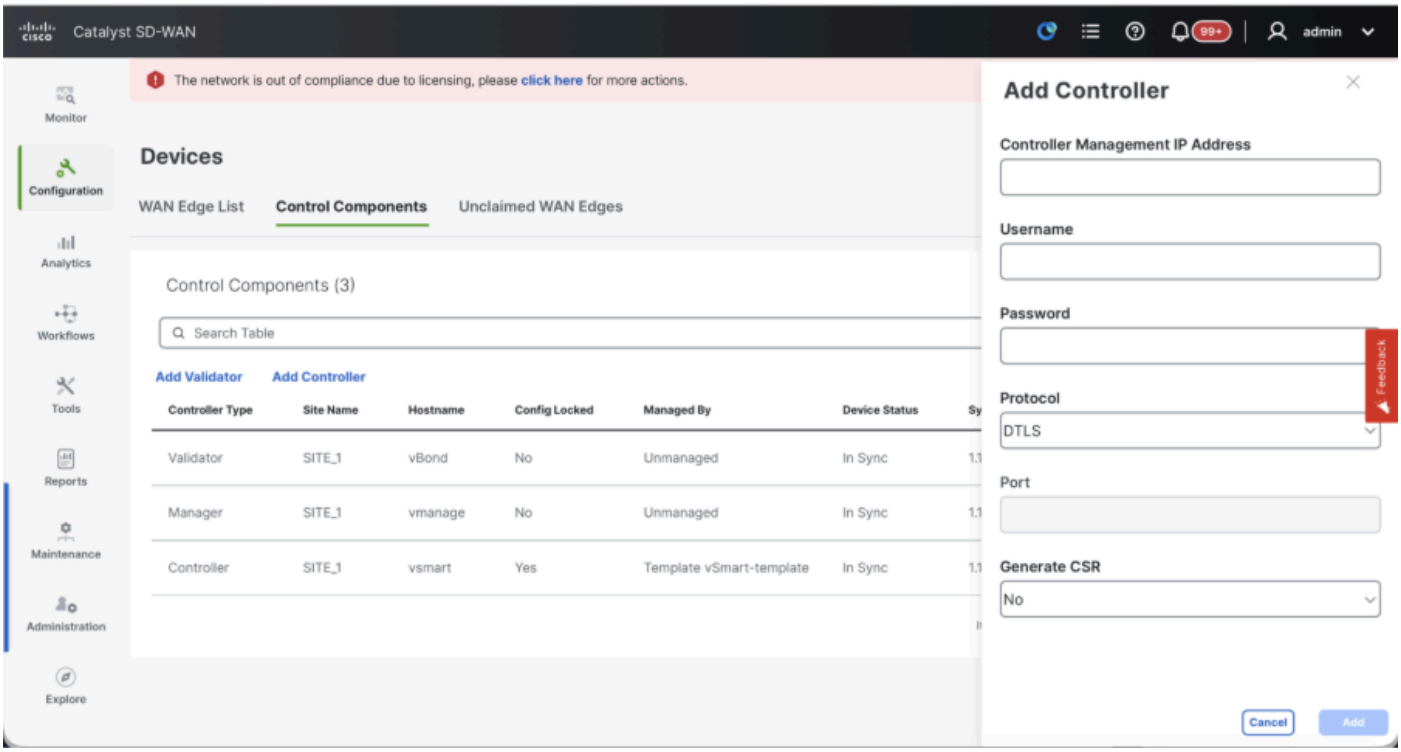


- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vBond.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente. Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo. El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vBonds, repita los mismos pasos.

Incorporación de vSmart/Controller:

- Haga clic en Add vSmart en el caso de 20.12 vManage o Add Controller en el caso de 20.15/20.18 vManage.
- Se abre una ventana emergente, introduzca la IP de transporte VPN 0 de vSmart, a la que se puede acceder desde vManage.
- Compruebe la disponibilidad mediante ping si se permite desde la CLI de vManage a vSmart IP.
- Introduzca las credenciales de usuario de vSmart Note que necesitamos para utilizar las credenciales de administrador de vSmart o una parte de usuario del grupo netadmin.
- Puede comprobarlo en la CLI de vSmart.
- Establezca el protocolo en TLS, si pretendemos utilizar TLS para routers para establecer conexiones de control con vSmart. Esta configuración también debe configurarse en CLI de nodos vsmarts y vManage.
- Elija Sí en el menú desplegable "Generar CSR" si necesitamos instalar un nuevo certificado para vSmart.

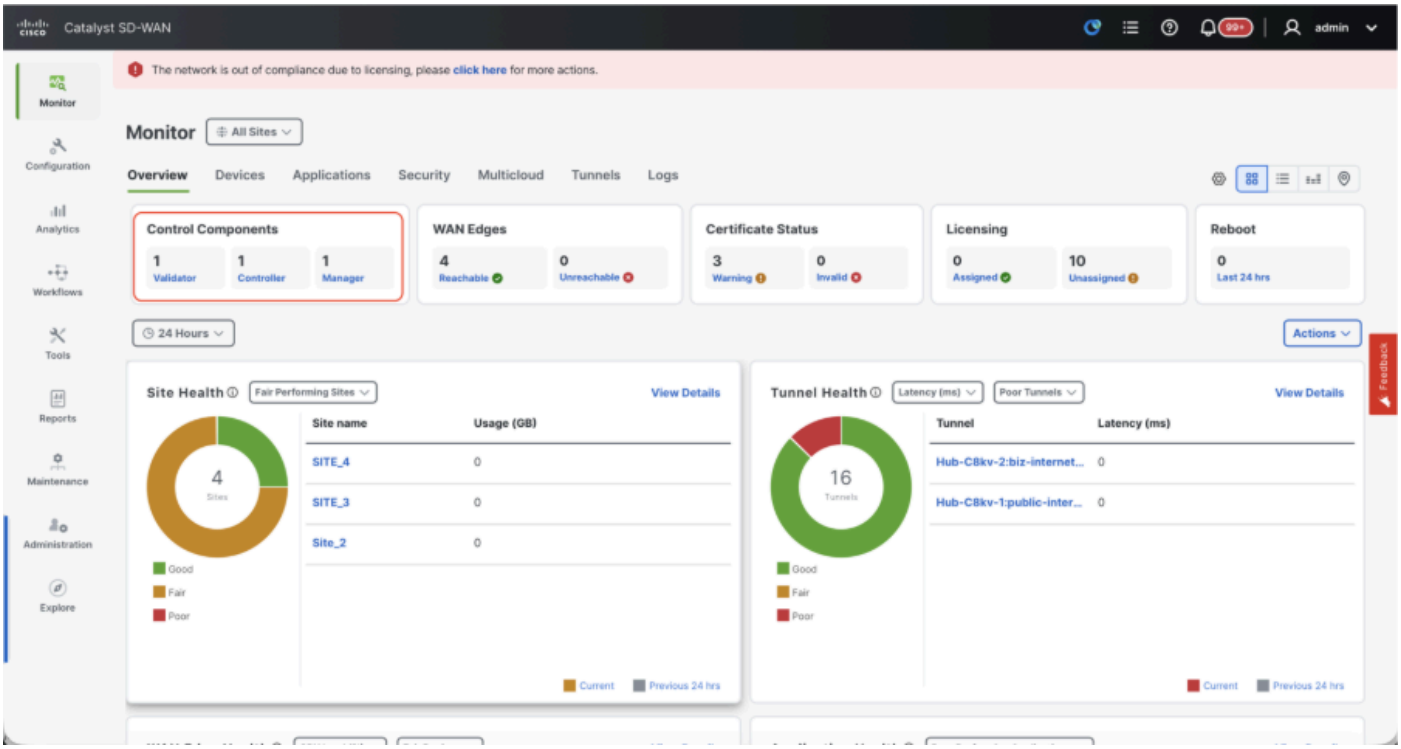
Nota: Si vSmart está detrás del dispositivo NAT/firewall, compruebe si la IP de la interfaz VPN 0 de vSmart se traduce a una IP pública y si la IP de la interfaz VPN 0 no es accesible desde vManage, utilice la dirección IP pública de la IP de la interfaz VPN 0 en este paso.



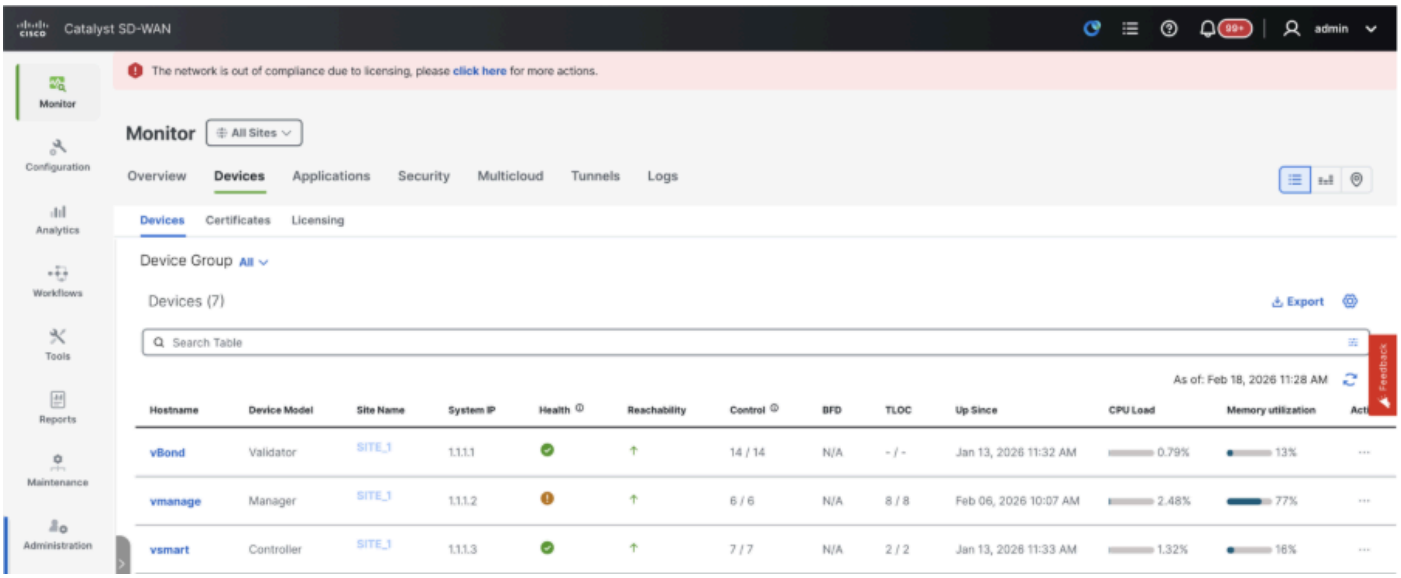
- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vSmart.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Si hay varios vsmarts, repita los mismos pasos.

Verificación

Una vez completados todos los pasos, verifique que todos los componentes de control sean accesibles en Monitor>Dashboard



- Haga clic en los componentes de control correspondientes y confirme que todos son accesibles.
- Navegue hasta Monitor > Devices y confirme que todos los componentes de control son accesibles.



Paso 3: Generar clúster de vManage

Fabric SD-WAN integrado con un clúster vManage en la superposición SD-WAN

Nota: vManage Cluster se puede configurar con 3 nodos vManage o 6 nodos vManage en función del número de sitios incorporados al fabric SD-WAN

Incorpore todos los controladores SD-WAN con un solo nodo vManage

Continúe con los pasos compartidos en "Controladores SD-WAN integrados con vManage de un solo nodo en la superposición SD-WAN" para activar primero el fabric SD-WAN con un nodo vManage e integrar todos los validadores (vBond) y controladores (vSmart) necesarios.

Configure las configuraciones CLI de todos los nodos de vManage que forman parte del clúster

- Configure el resto de los nodos de vManage. En el caso de un clúster de 3 nodos, tiene 2 nodos restantes que configurar; en el caso de un clúster de 6 nodos, tiene 5 nodos que configurar.
- Configure las configuraciones del sistema como se muestra:

```
config t
system
 host-name



 system-ip
```

```
 site-id


 organization-name


 vbond


commit
```

Nota: Si utilizamos URL como dirección vBond, asegúrese de configurar las direcciones IP del servidor DNS en la configuración VPN 0 o asegúrese de que se puedan resolver.

Estas configuraciones son necesarias para habilitar la interfaz de transporte utilizada para establecer conexiones de control con los routers y el resto de los controladores.

```
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
```

Configure también la interfaz de administración VPN 512para habilitar el acceso de administración fuera de banda al controlador.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

Configuración opcional:

- Puede consultar las configuraciones de su controlador existente y, si la configuración que se muestra aquí está presente, puede agregar esta configuración a los nuevos controladores.
- Configure el protocolo de control como TLS solo si hay un requisito para que los routers establezcan conexiones de control seguras con los nodos vManage mediante TLS. De forma predeterminada, todos los controladores y routers establecen una conexión de control mediante DTLS. Se trata de una configuración opcional que solo se requiere en los nodos vSmart y vManage, según sus necesidades.

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

Configurar la interfaz de servicio en todos los nodos de vManage

Configure la interfaz de servicio en todos los thevManagenodes, incluido vManage-1, que ya se ha incorporado. Esta interfaz se utiliza para la comunicación del clúster, lo que significa comunicación entre losnodos de administración del clúster.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

Asegúrese de que se utiliza la misma subred IP para la interfaz de servicio en todos los nodos delclúster de administración.

Configurar credenciales de clúster

Podemos utilizar las mismas credenciales de administrador de thevManagenodes para configurar thevManagecluster. De lo contrario, podemos configurar una nueva credencial de usuario que forma parte denetadmingroup. Las configuraciones para configurar las nuevas credenciales de usuario son las siguientes

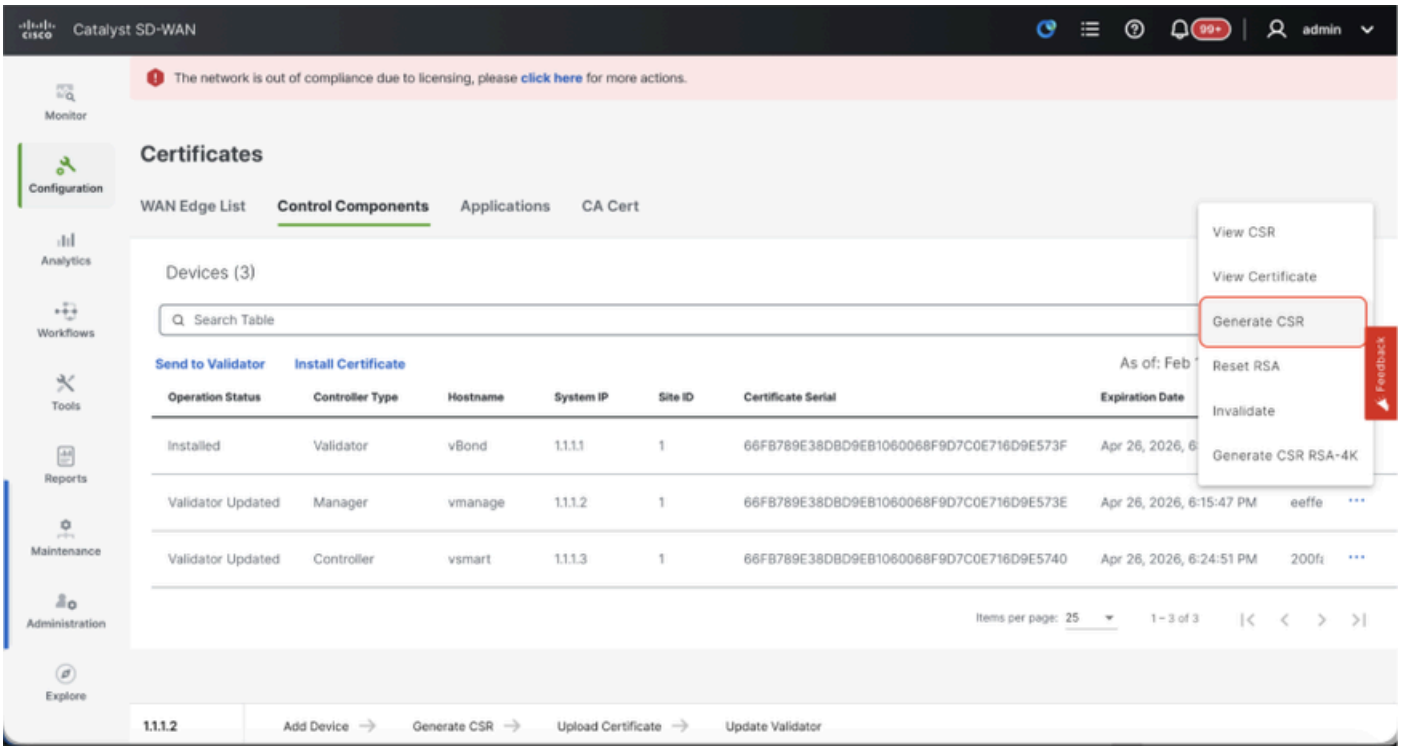
```
conf t
system
 aaa
  user



   password



   group    netadmin
commit
```

Asegúrese de configurar las mismas credenciales de usuario en todos los thevManagenodesque forman parte del clúster.Si decidimos utilizar credenciales de administrador, debe ser el mismo nombre de usuario/contraseña en todos los thevManagenodes.

Instalar el certificado de dispositivo en todos los nodos de vManage

- Inicie sesión en tovManageUI de todos los thevManagenodes mediante la dirección URL https://<vmanage-ip>en su navegador. Utilice la dirección IP VPN 512 de los vManagenodes respectivos. Puede iniciar sesión con el nombre de usuario y la contraseña del administrador.
- Vaya a Configuration > Certificates > Control Components en el caso de los nodos 20.15/20.18 vManage. En el caso de las versiones 20.9/20.12, Configuration > Devices > Controllers

  Haga clic en ... para Manager/vManage y haga clic en Generate CSR.



- Una vez generada la CSR, puede descargar la CSR y firmarla en función de la autoridad de certificados elegida para los controladores. Puede verificar esta configuración en Administration > Settings > Controller Certificate Authorization. Si se elige Cisco (recomendado), vManage carga automáticamente el CSR en el portal PNP y, una vez firmado el certificado, se instala automáticamente en vManage.
- Si elige Manual, firme manualmente el CSR mediante el portal PNP de Cisco. Para ello, vaya a la cuenta inteligente y a la cuenta virtual de la superposición SD-WAN correspondiente.
- Una vez que el certificado esté disponible en el portal PNP, haga clic en Instalar certificado en la misma sección de vManage y cargue el certificado e instálelo.
- El mismo procedimiento es aplicable si estamos utilizando Digicert y Enterprise Root Certificate.
- Complete este paso en todos los nodos de vManage que forman parte del clúster.

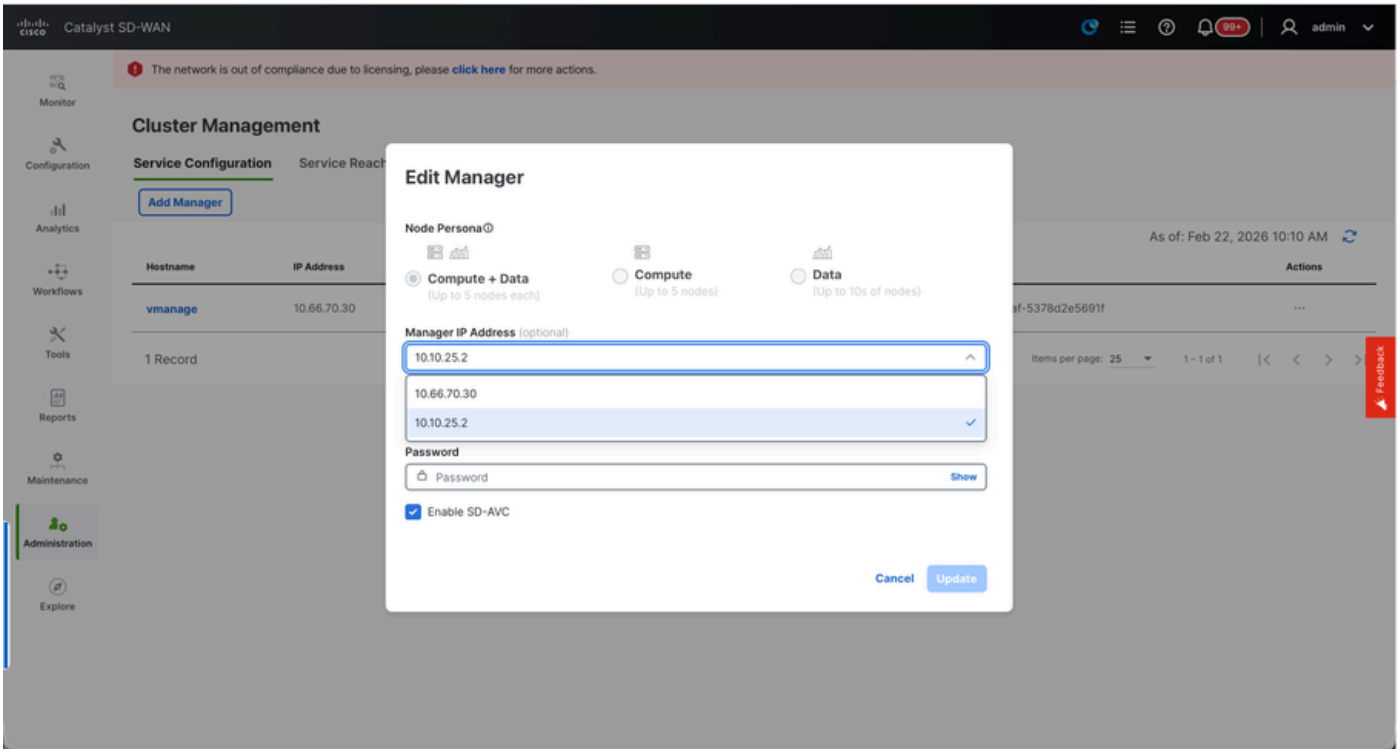
Preparación para crear el clúster de vManage

- En la interfaz de usuario web de vManage-1, vaya a Administration > Cluster Management, haga clic en ... en Actions for vManage-1, elija Edit.
- El personaje del nodo se elige automáticamente en función del personaje que elegimos mientras se giraba la máquina virtual.

Nota: Para un clúster de 3 nodos, los 3 nodos de vManage se activan con compute+data como persona. Para un clúster de 6 nodos, 3 nodos de vManage se activan con

compute+data como persona y 3 nodos de vManage se activan con datos como persona.

- En el menú desplegable Dirección IP del administrador, asegúrese de elegir la dirección IP de la interfaz de servicio de vManage.



- Introduzca el nombre de usuario y la contraseña que desee utilizar para activar el clúster de vManage, que se conoce como credenciales del clúster.
- Como se ha mencionado anteriormente, se deben configurar las mismas credenciales en todos los nodos de vManage y se deben utilizar al agregar todos los nodos al clúster.

Configuración opcional:

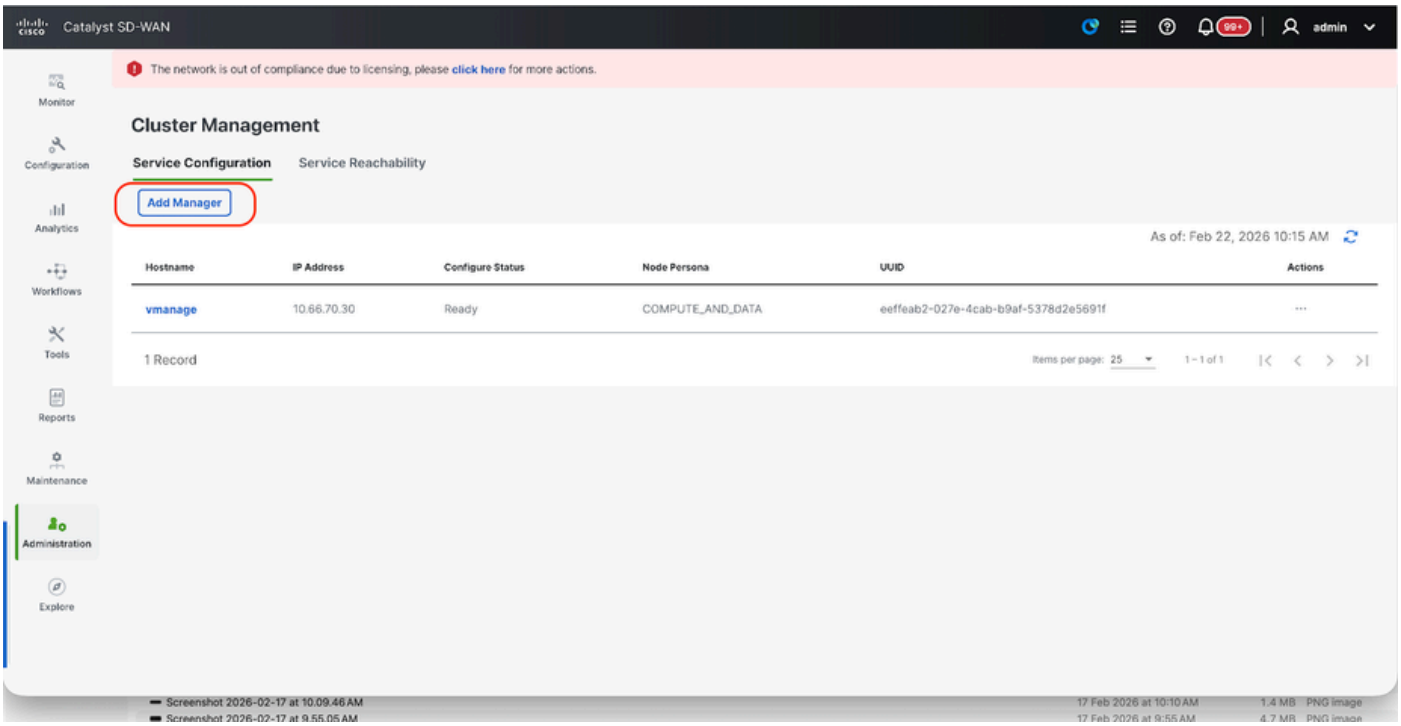
Consulte esta configuración en el clúster existente para Habilitar SDAVC: sólo debe comprobarse si es necesario y sólo es necesario en un nodo vManage del clúster.

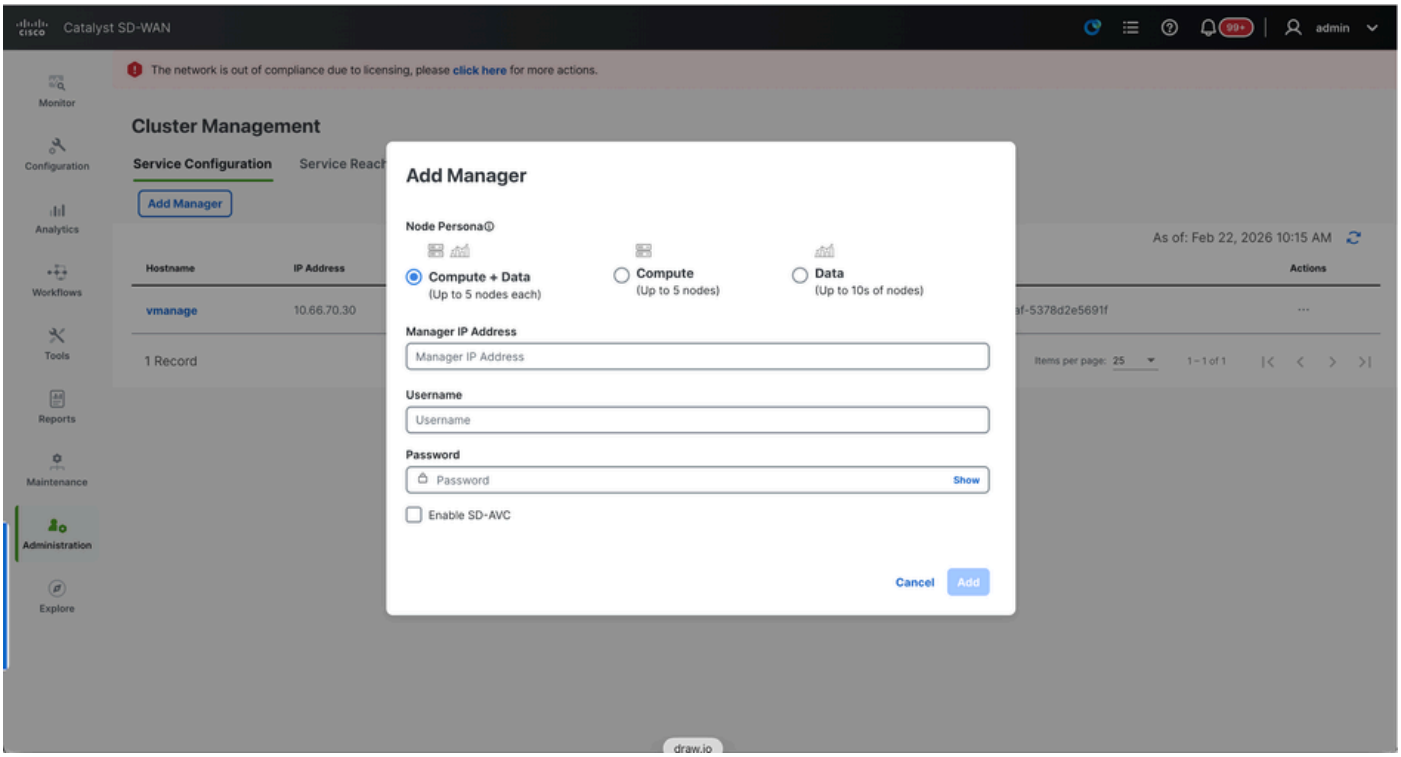
Haga clic en Actualizar.

- Al publicar esto, los servicios de vManage NMS se reinician en segundo plano y la interfaz de usuario no está disponible durante unos minutos de entre 5 y 10 minutos. Durante este tiempo, está disponible el acceso CLI de vManage.
- Una vez que se pueda acceder a la interfaz de usuario de vManage-1, vaya a Administration > Cluster Management, asegúrese de que la IP de la interfaz de servicio de vManage se refleja en IP address,El estado de configuración es Preparado y el personaje del nodo se refleja correctamente. Cambie a la sección de disponibilidad del servicio en la misma página y asegúrese de que todos los servicios estén disponibles.
- Si vemos que alguno de los servicios aún no está disponible, espere. Por lo general, toma alrededor de 20 a 30 minutos.

Creación del clúster de vManage

- En la interfaz de usuario web de vManage-1, vaya a Administration > Cluster Management, en la sección Service Configuration,
- Haga clic en Add Manager, aparecerá una ventana emergente:

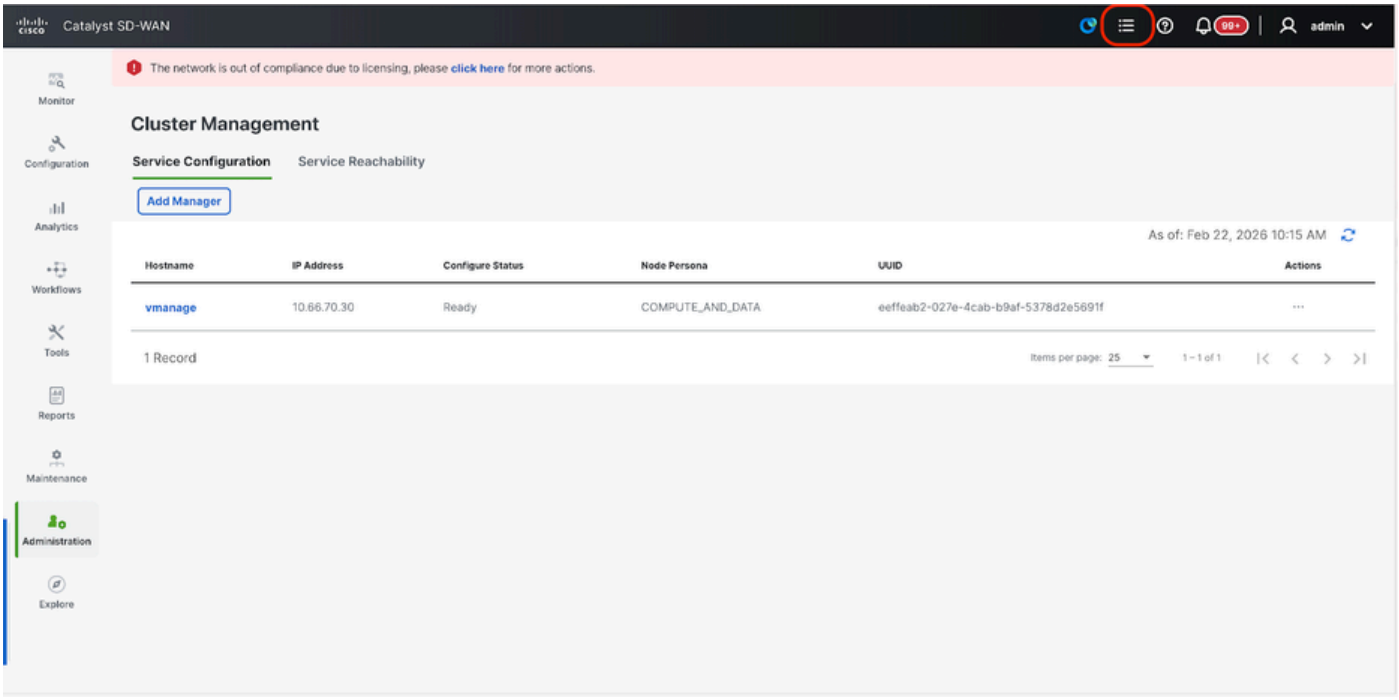




- Elija el Node persona en función de las configuraciones de persona realizadas mientras se giraba el nodo vManage - 2.
- Introduzca la IP de la interfaz de servicio de vManage-2 en Dirección IP del jefe
- Introduzca el nombre de usuario y la contraseña, que son las mismas credenciales que

utilizamos en el paso 6.

- Habilitar SDAVC: no se debe marcar porque ya lo habríamos activado en vManage-1
- Haga clic en Agregar.
- Al publicar esto, los servicios de vManage NMS se reinician en segundo plano para los nodos de vManage 1 y 2. La interfaz de usuario no está disponible durante unos minutos de 5 a 10 minutos aproximadamente para vManage 1 y 2.
- Durante este tiempo, está disponible el acceso CLI de vManage 1 y 2.
- Una vez que se pueda acceder a la interfaz de usuario de vManage-1, vaya a Administration > Cluster Management, asegúrese de que la IP de la interfaz de servicio de vManage se refleja en IP address, Configure Status is Ready y node persona se refleja correctamente.
- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios están disponibles para ambos nodos de vManage.
- Si vemos que alguno de los servicios aún no está disponible, espere. Por lo general, toma alrededor de 5 a 10 minutos.
- Puede comprobar el estado del proceso de adición de clústeres en la lista de tareas disponible en la esquina superior derecha de la interfaz de usuario de vManage.



- Puede buscar una lista de tareas activas y, si la tarea sigue apareciendo en Lista de tareas activas, indica que la tarea no se ha completado todavía.
- Puede hacer clic en la tarea para comprobar el progreso de la misma. Si la tarea no aparece en Lista de tareas activas, cambie a Completada y asegúrese de que la tarea se ha completado correctamente.
- Solo después de validar estos puntos, continúe con el siguiente paso.

Estos puntos deben tenerse en cuenta antes de agregar el siguiente nodo al clúster:

Verifique estos puntos en todas las UI de los nodos vManage que se han agregado al clúster hasta el momento:

- Vaya a Monitor > Overview of vManage UI y asegúrese de que el número de nodos de

vManage se reflejen correctamente y se vean accesibles en función del número de nodos agregados al clúster.

- Navegue hasta Administration > Cluster Management y asegúrese de que la IP de la interfaz de servicio de vManage se refleje bajo IP address, Configure Status is Ready y node persona se refleje correctamente.
- Cambie a la sección Disponibilidad del servicio en la misma página y asegúrese de que todos los servicios son accesibles para ambos nodos de vManage.

- Cada vez que se agrega un nodo al clúster, se reinician los servicios NMS de todos los nodos del clúster, por lo que la interfaz de usuario de todos esos nodos queda inaccesible durante algún tiempo.
- Dependiendo del número de nodos del clúster, puede ser necesario más tiempo para que se realice una copia de seguridad de la interfaz de usuario y todos los servicios sean accesibles.
- Puede supervisar la tarea en Lista de tareas disponible en la esquina superior derecha de la interfaz de usuario de vManage.
- En la interfaz de usuario de vManage de cada nodo agregado al clúster, necesitamos ver todos los routers, plantillas y políticas si estuvieran disponibles en vManage-1.
- Si esas configuraciones no estaban presentes en vManage-1, los vBonds y vSmarts que se agregaron a vManage-1 y también las configuraciones de Administration > Settings para Organization-name, vBond, Certificate Authorization deben reflejarse en el resto de los nodos vManage agregados al clúster.
- Repita los mismos pasos para el resto de los nodos de vManage.

Paso 4: Copia de seguridad/restauración de Config-db

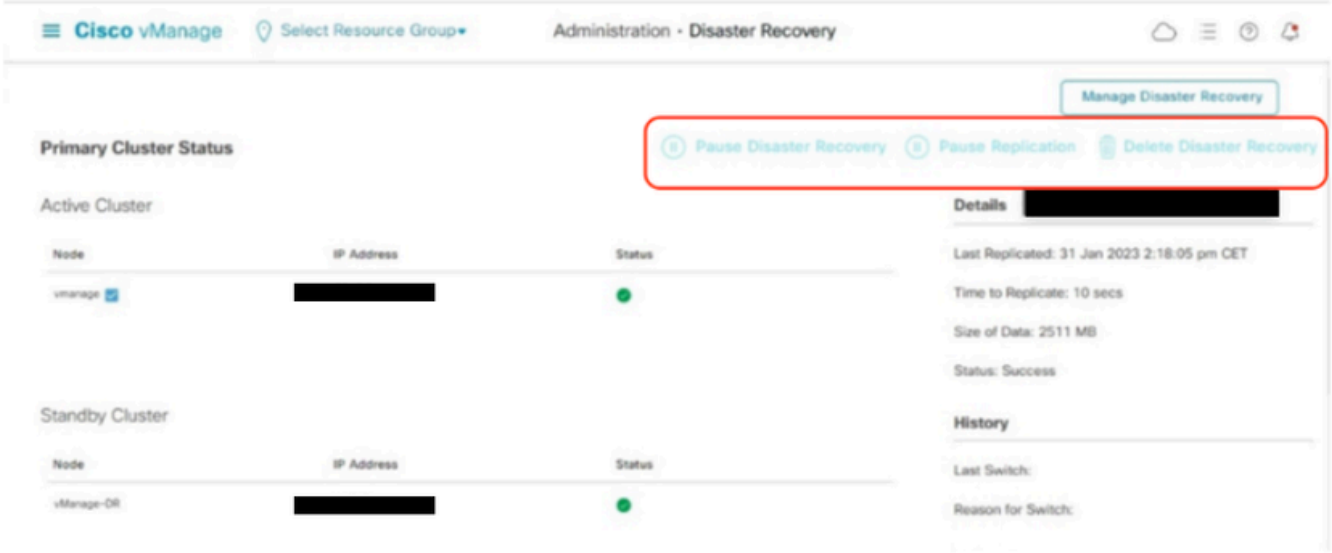
Recopilar copia de seguridad de la base de datos de configuración de vManage y restaurar en otro nodo de vManage

---

Nota: Mientras recopila la copia de seguridad de la base de datos de configuración del clúster de vManage existente que tiene habilitada la recuperación ante desastres, asegúrese de que se recopila después de pausar y eliminar la recuperación ante desastres de ese nodo.

Confirme que no hay replicación de recuperación ante desastres en curso. Vaya a Administration > Disaster Recovery y asegúrese de que el estado es Correcto y no está en un estado transitorio, como Importación pendiente, Exportación pendiente o Descarga pendiente. Si el estado no es correcto, póngase en contacto con Cisco TAC y asegúrese de que la replicación es correcta antes de proceder a pausar la recuperación ante desastres.

En primer lugar, detenga la recuperación ante desastres y asegúrese de que la tarea se ha completado. A continuación, elimine la recuperación ante desastres y confirme que la tarea se ha completado.



Póngase en contacto con el TAC de Cisco para asegurarse de que la recuperación ante desastres se ha limpiado correctamente.

Recopilar copia de seguridad de Configuration-DB:

- En el fabric SD-WAN que se está utilizando actualmente, puede generar una copia de seguridad de la base de datos de configuración desde el clúster de vManage.
- Tenga en cuenta que solo debemos generar una copia de seguridad de la base de datos de configuración en un nodo del clúster de vManage que es el líder de la base de datos de configuración.

- Para vManage independiente, vManage es el líder de la base de datos de configuración.
- En el clúster vManage, identifique el nodo líder configuration-db mediante el comando request nms configuration-db diagnostics.Puede ejecutar este comando en todos los nodos del clúster vManage de 3 nodos.
- En un clúster de 6 nodos, asegúrese de ejecutar este comando en los nodos vManage donde configuration-db está habilitado para identificar el nodo líder. Navegue hasta Administración > Administración de clústeres para verificar lo mismo:
- Como vemos en la captura de pantalla, los nodos configurados con persona COMPUTE_AND_DATA tienen configuration-db en ejecución.

Puede verificar lo mismo mediante el comando requestnmsconfiguration-dbstatus en vManageCLI. El resultado es como se muestra

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

- Una vez ejecutado el comandorequest nms configuration-db diagnostics en estos nodos, el resultado es el siguiente:
- Busque el campo resaltado para "IsLeader". Si se establece en 1, indica que el nodo es el nodo líder y podemos recopilar una copia de seguridad de la base de datos de configuración de él.

```
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     .
```

Utilice este comando para recopilar la copia de seguridad de la base de datos de configuración del nodo vManage del líder de la base de datos de configuración identificado.

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

El resultado esperado es el siguiente:

```
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#
```

- Tome nota de las credenciales de configuration-db si se ha actualizado.
- Si no conoce las credenciales de la base de datos de configuración, póngase en contacto con el TAC para recuperar las credenciales de la base de datos de configuración de los nodos de vManage existentes.
- Las credenciales de la base de datos de configuración predeterminada son username: neo4j y contraseña: contraseña

Restaurar copia de seguridad de Configuration-db en otro nodo de vManage

Copie la copia de seguridad de la base de datos de configuración en el directorio /home/admin/ de vManage mediante SCP.

Ejemplo de resultado del comando scp:

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

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

Para restaurar la copia de seguridad de la base de datos de configuración, primero debemos configurar las credenciales de la base de datos de configuración. Si sus credenciales de configuration-db son predeterminadas (neo4j/password), podemos saltarnos este paso.

Para configurar las credenciales de configuration-db, utilice el comando request nms configuration-db update-admin-user.Use el nombre de usuario y la contraseña que desee.

Tenga en cuenta que el servidor de aplicaciones de vManage se reinicia. Debido a lo cual, la interfaz de usuario de vManage se vuelve inaccesible durante un breve período de tiempo.

```
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#
```

Publicación en la que podemos continuar con la restauración de la copia de seguridad de la base de datos de configuración:

Podemos utilizar el comando request nms configuration-db restore path /home/admin/< > para restaurar la base de datos de configuración en el nuevo vManage:

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

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

Una vez restaurada la base de datos de configuración, asegúrese de que se puede acceder a la interfaz de usuario de vManage. Espere unos 5 minutos e intente acceder a la interfaz de usuario.

Una vez que haya iniciado sesión correctamente en la interfaz de usuario, asegúrese de que la lista de routers periféricos, la plantilla, las políticas y el resto de las configuraciones que estaban presentes en la interfaz de usuario de vManage anterior o existente se reflejan en la nueva interfaz de usuario de vManage.

Paso 5: Habilitar la recuperación ante desastres en un clúster de vManage

Comprobaciones previas importantes

Se deben configurar y poner en funcionamiento dos clústeres independientes de 3 nodos de vManage para continuar con la recuperación ante desastres. En el clúster activo debe tener validadores y controladores incorporados. En caso de que tenga un validador y controladores en el sitio DR, también deben estar incorporados en el clúster activo y no en el clúster DR vManage.

Cisco recomienda que, antes de registrar la recuperación ante desastres, se cumplan estos requisitos:

- Asegúrese de que el nodo principal y el secundario estén accesibles mediante HTTPS en una VPN de transporte (VPN 0).
- Asegúrese de que Cisco vSmart Controllers y Cisco vBond Orchestrators de la configuración secundaria estén conectados a la configuración principal.
- Asegúrese de que el nodo principal y el nodo secundario de Cisco vManage ejecutan la misma versión de Cisco vManage.
- Interfaz de clúster fuera de banda (interfaz de servicio) en VPN 0.
- Para cada instancia de vManage de un clúster, se requiere una tercera interfaz (enlace de clúster) además de las interfaces utilizadas para VPN 0 (transporte) y VPN 512 (gestión).
- Esta interfaz se utiliza para la comunicación y la sincronización entre los servidores vManage del clúster.

- Esta interfaz debe tener al menos 1 Gbps y una latencia de 4 ms o menos. Se recomienda una interfaz de 10 Gbps.
- Ambos nodos de vManage deben poder comunicarse entre sí a través de esta interfaz: ya sea un segmento de capa 2 o a través del routing de capa 3.
- En cada vManage, esta interfaz se debe configurar en la GUI como una interfaz de clúster (Administration > Cluster Management: indique su propia dirección IP, usuario y contraseña de la interfaz de clúster fuera de banda).
- Para permitir que los nodos de Cisco vManage se comuniquen entre sí en los Data Centers, habilite los puertos TCP 8443 y 830 en los firewalls de los Data Centers.
- Asegúrese de que todos los servicios (application-server, configuration-db, messaging server, coordinator server y statistics-db) estén habilitados en ambos nodos de Cisco vManage.
- Distribuya todos los controladores, incluidos los Cisco vBond Orchestrators, entre los Data Centers principales y secundarios. Asegúrese de que los nodos de Cisco vManage que se distribuyen por estos Data Centers puedan acceder a estos controladores. Los controladores solo se conectan al nodo principal de Cisco vManage.
- Asegúrese de que no hay otras operaciones en proceso en el nodo activo (principal) y en el nodo de Cisco vManage en espera (secundario). Por ejemplo, asegúrese de que ningún servidor esté en proceso de actualizar o adjuntar plantillas a los dispositivos.
- Desactive el servidor proxy HTTP/HTTPS de Cisco vManage si está activado. Consulte Servidor proxy HTTP/HTTPS para Cisco vManage Communication con servidores externos. Si no desactiva el servidor proxy, Cisco vManage intenta establecer la comunicación de recuperación ante desastres a través de la dirección IP del proxy, incluso si las direcciones IP del clúster fuera de banda de Cisco vManage son directamente accesibles. Puede volver a habilitar el servidor proxy HTTP/HTTPS de Cisco vManage una vez finalizado el registro de recuperación ante desastres.
- Antes de iniciar el proceso de registro de recuperación ante desastres, vaya a la ventana Tools > Rediscover Network en el nodo principal de Cisco vManage y vuelva a descubrir Cisco vBond Orchestrators.

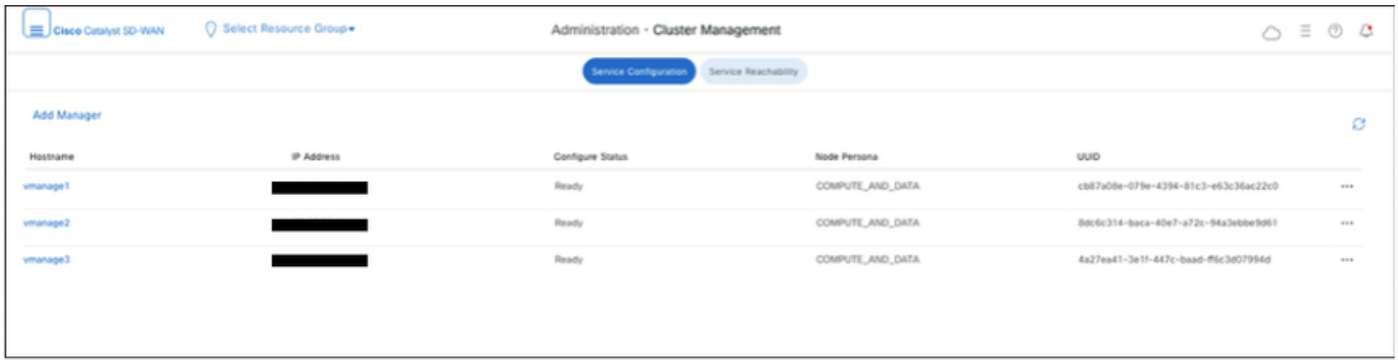
Configuraciones

Para obtener más información sobre vManage Disaster Recovery, consulte este enlace.

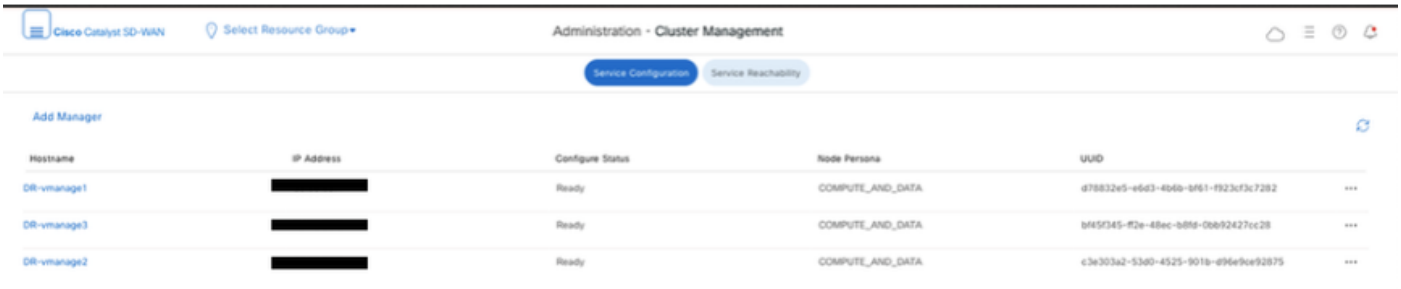
Ya se han creado los dos clústeres de 3 nodos independientes, suponiendo que cada administrador de SD-WAN tiene una configuración mínima y que se ha completado la parte de certificación.

Vaya a Administration > Cluster Management en ambos clústeres y verifique que todos los nodos estén en estado Ready.

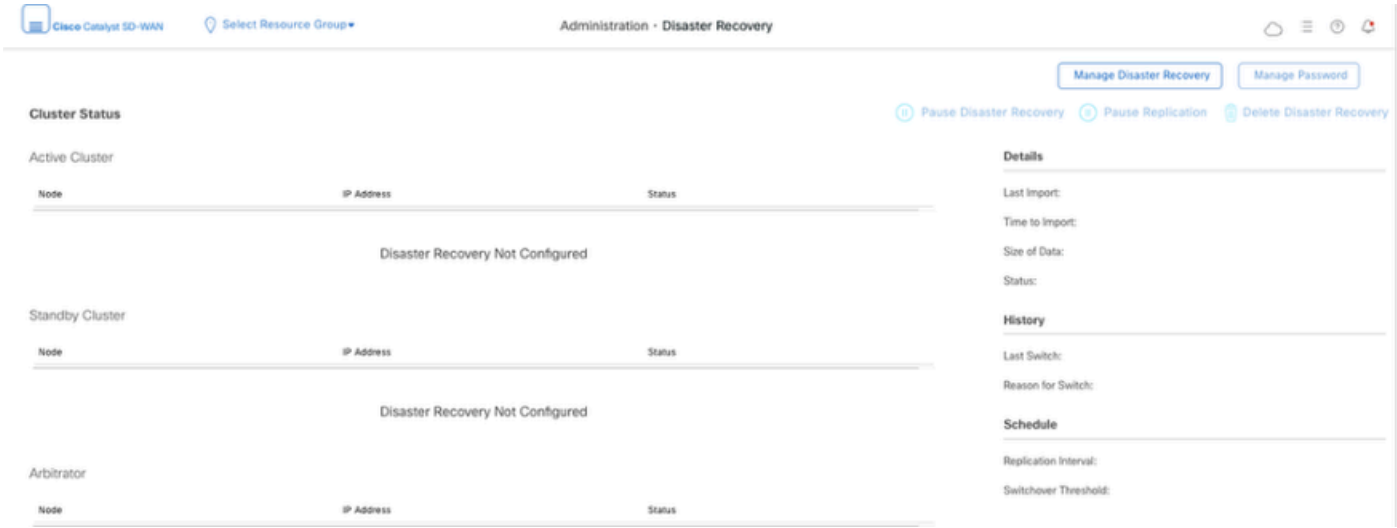
vManage de DC



DR vmanage



Vaya a Administration>Disaster Recovery of Primary vManage Cluster. Haga clic en Administrar recuperación ante desastres.

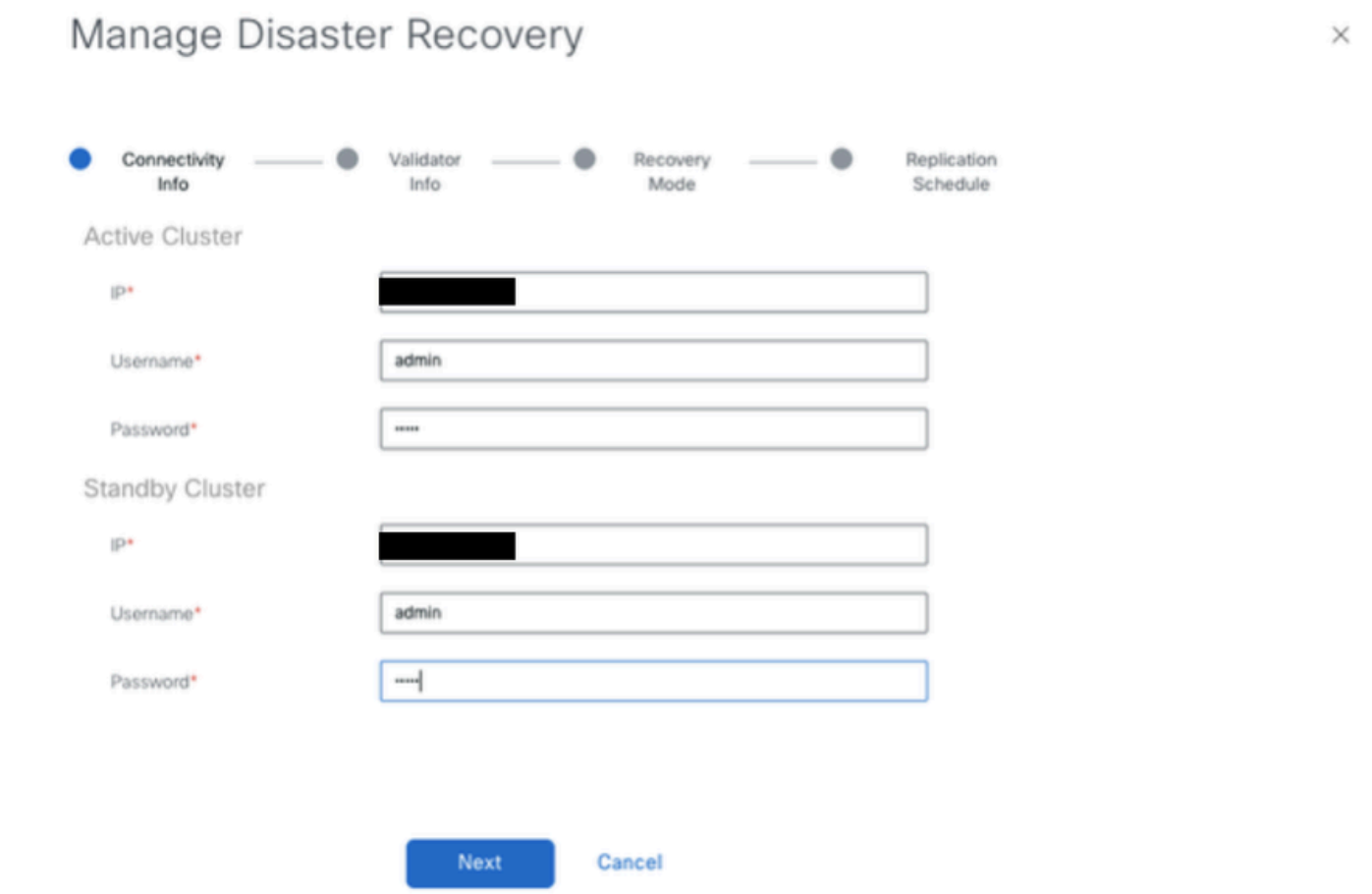


En la ventana emergente, rellene los detalles de vManage principal y secundaria.

Las direcciones IP que se deben indicar son las direcciones IP de las interfaces de clúster fuera de banda. Utilice preferiblemente la dirección IP de la interfaz de servicio VPN 0 de vManage-1 en cada clúster.

Las credenciales deben ser las de un usuario netadmin y no se deben cambiar una vez configurado el DR, a menos que se elimine. Se puede utilizar una credencial de usuario local de

vManage independiente para la recuperación ante desastres. Debemos asegurarnos de que el usuario local de vManage forma parte del grupo netadmin. Incluso las credenciales de administrador se pueden utilizar aquí.



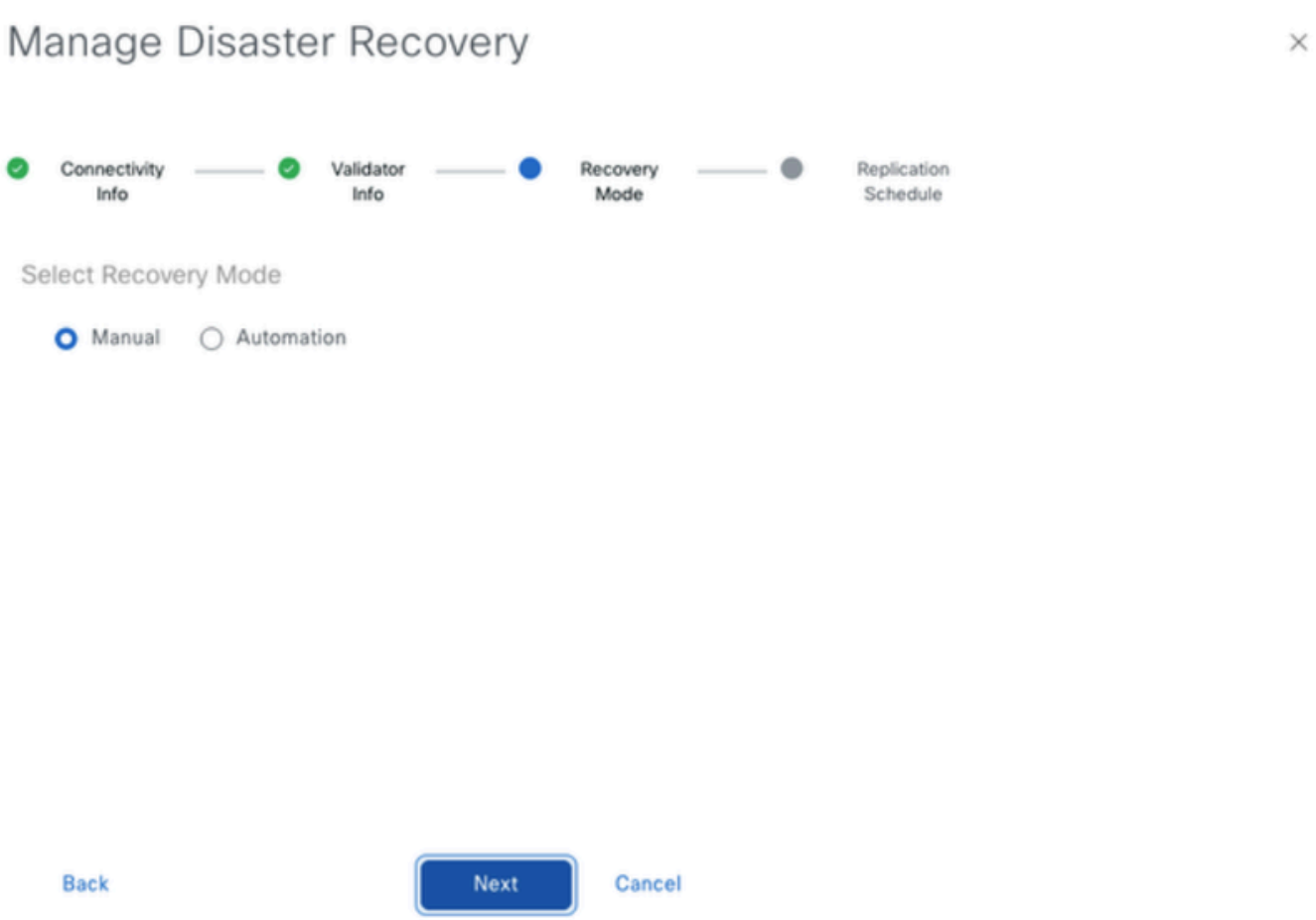
Una vez rellenado, haga clic en Next.

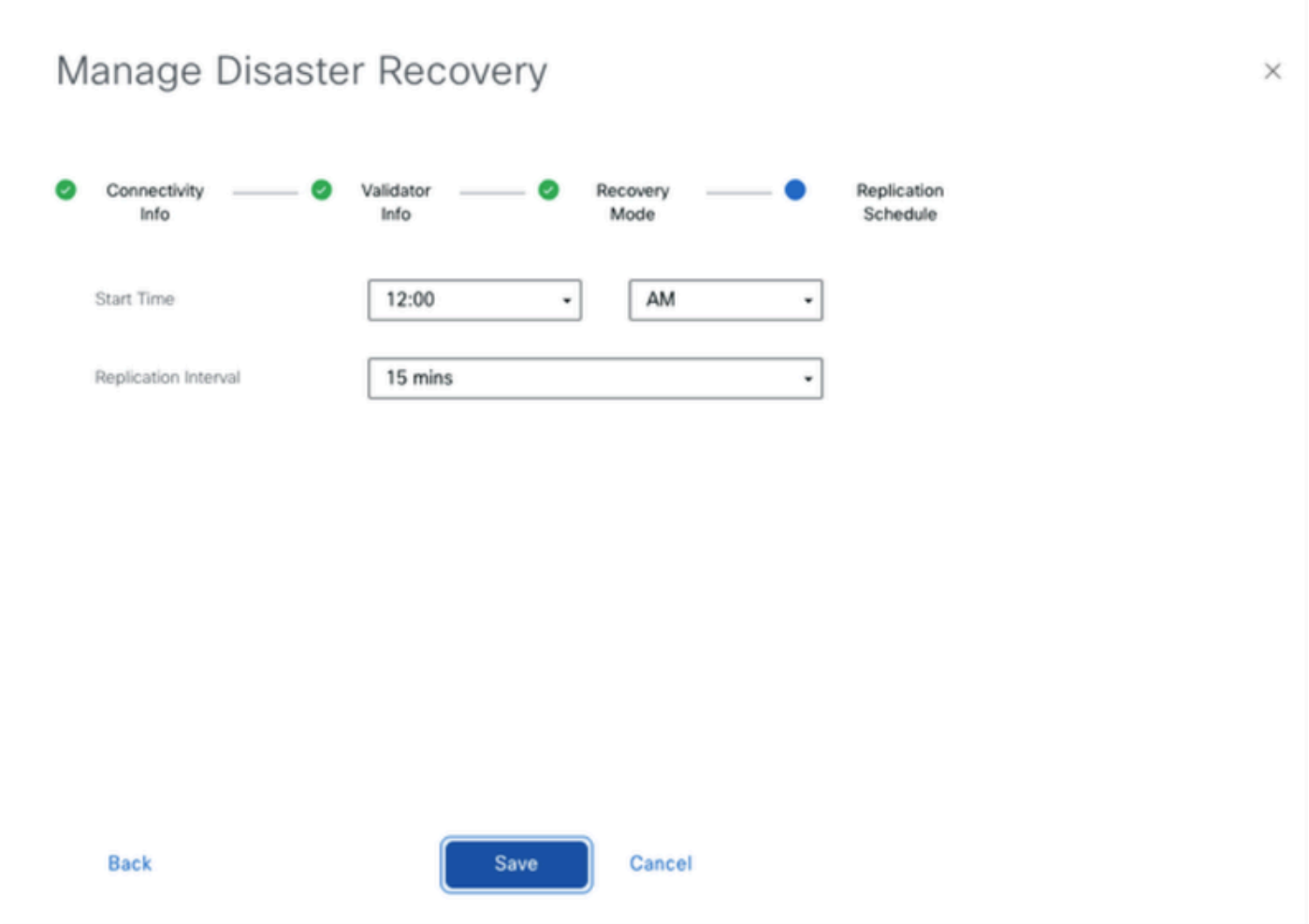
- Rellene los detalles de los controladores de vBond.

Los controladores vBond deben ser accesibles en la dirección IP especificada a través de Netconf.

Una vez rellenado, haga clic en Next.

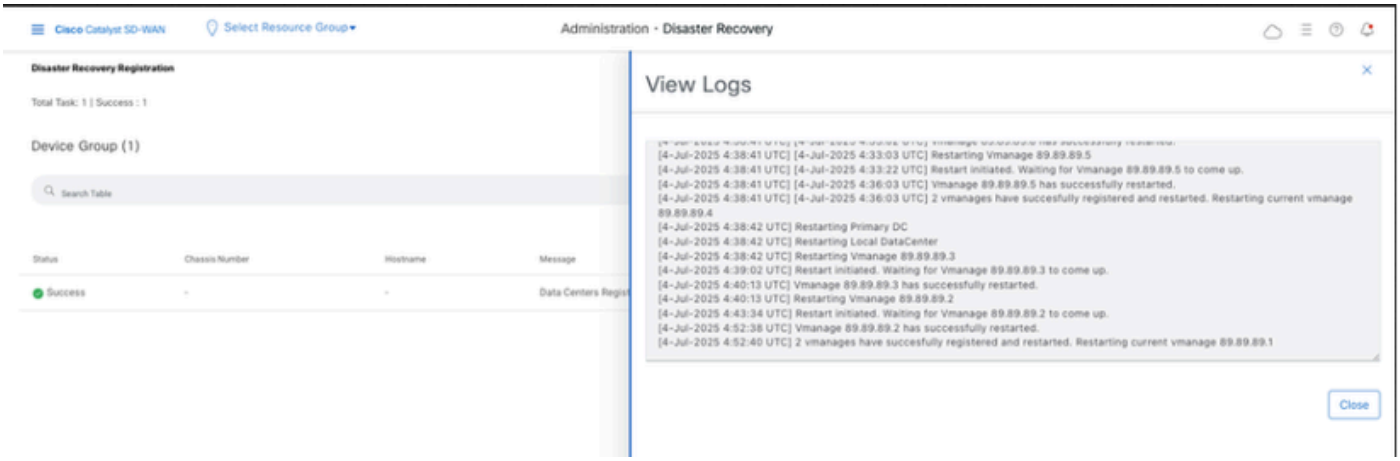
- En el modo de recuperación, seleccione Manual. El modo de automatización está obsoleto. Haga clic en Next (Siguiente).


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



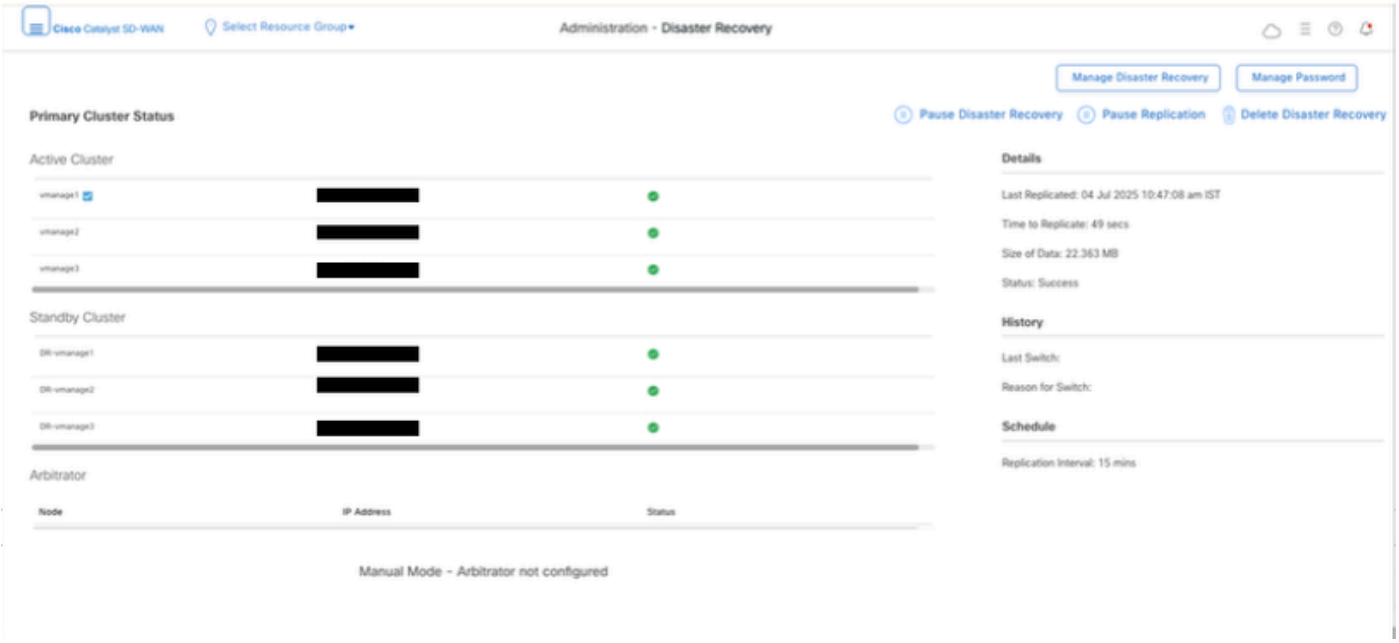
Establezca el valor y haga clic en Guardar.

- El registro de DR comienza ahora. Haga clic en el botón Actualizar para actualizar manualmente el estado y los registros de progreso. Este proceso puede tardar hasta 20-30 minutos.



Verificación

Navegue hasta Administración>Recuperación ante desastres para ver el estado de Recuperación ante desastres y cuándo se replicaron los datos por última vez.



Nota: La replicación puede tardar varias horas en función del tamaño de la base de datos. Además, puede requerir algunos ciclos para lograr una replicación correcta.

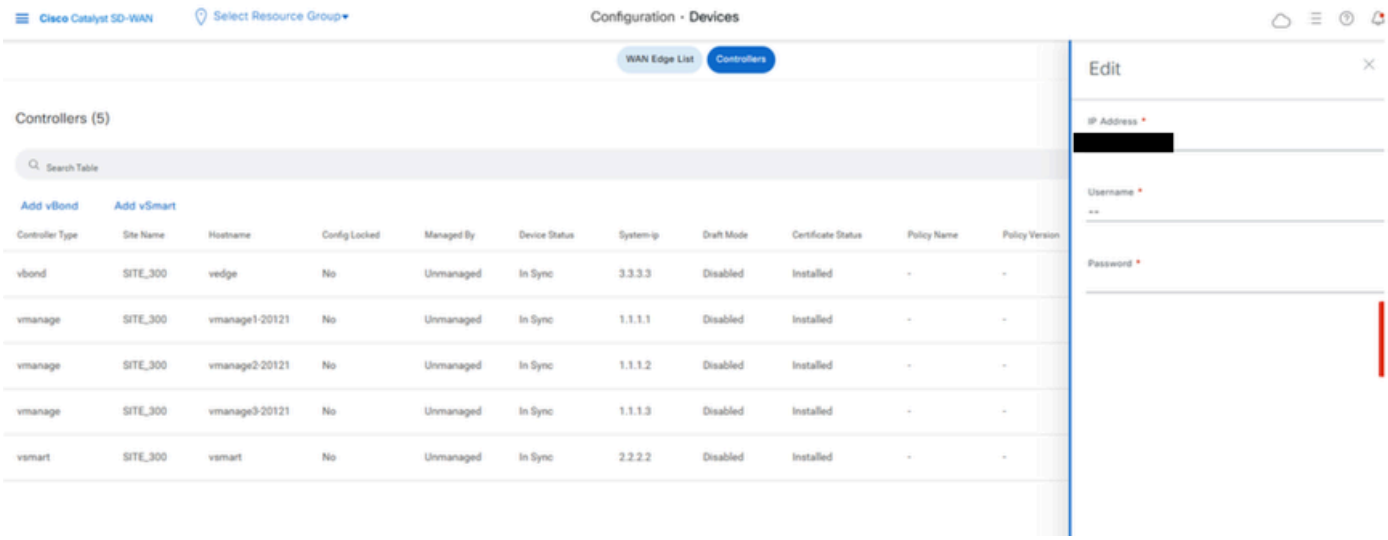
Paso 6: Reautenticación de controladores e invalidación de controladores antiguos

Una vez restaurada la base de datos de configuración, necesitamos volver a autenticar todos los nuevos controladores (vmanage/vsmart/vbond) en el fabric

Nota: En la producción real, si la IP de interfaz utilizada para la reautenticación es la IP de interfaz de túnel, debe asegurarse de que se permite el servicio NETCONF en la interfaz de túnel de vManage, vSmart y vBond, así como en los firewalls a lo largo de la ruta. El puerto del firewall que se debe abrir es el puerto TCP 830 como regla bidireccional desde el clúster DR a todos los vBonds y vsmarts .

En vmanage UI, haga clic en Configuration > Devices > Controllers

- Haga clic en los tres puntos cerca de cada controlador y haga clic en Editar



- Reemplace la dirección ip (system-ip of the controller) por la dirección ip transport vpn 0 (tunnel interface). Introduzca el nombre de usuario y la contraseña y haga clic en save (guardar)
- Haga lo mismo con todos los nuevos controladores del fabric

Sincronizar la cadena de certificados raíz

Una vez que todos los controladores estén incorporados, complete este paso:

En cualquier servidor Cisco SD-WAN Manager del clúster recién activo, realice estas acciones:

Ingrese este comando para sincronizar el certificado raíz con todos los dispositivos Cisco Catalyst SD-WAN en el agrupamiento recientemente activo:

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

Ingrese este comando para sincronizar el UUID de Cisco SD-WAN Manager con el Validador de Cisco SD-WAN:

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

Una vez restaurado el fabric y activadas las sesiones de control y bfd para todos los bordes y controladores del fabric, debemos invalidar los controladores antiguos (vmanage/vsmart/vbond) de la interfaz de usuario

- En vmanage UI, haga clic en Configuration > Devices > Certificates .
- Haga clic en Controladores
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en invalidar
- Haga clic en enviar a vbond
- En vmanage UI, haga clic en Configuration > Devices > Controllers
- Haga clic en los tres puntos cerca del controlador (vmanage/vsmart/vbond) del fabric antiguo. Haga clic en Eliminar

Registrar cheques

Estas comprobaciones posteriores se aplican a todas las combinaciones de implementación.

Reactive los routers periféricos de nube:

- Si C8000v forma parte de la superposición y vmanaged está firmado, debe volver a autenticarse, es decir:

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

        token
```

- Confirme que las conexiones de control y las sesiones BFD estén activas
- Confirmar que el tráfico de aplicaciones fluye de extremo a extremo
- Si se hicieron cambios en el salto de puerto antes de reconstruir el fabric en los bordes, se deben revertir

- Verifique que los elementos aparezcan como se espera:
    - Plantillas
    - Políticas
    - Página Dispositivo (ambas fichas)WAN vEdge ListControllers

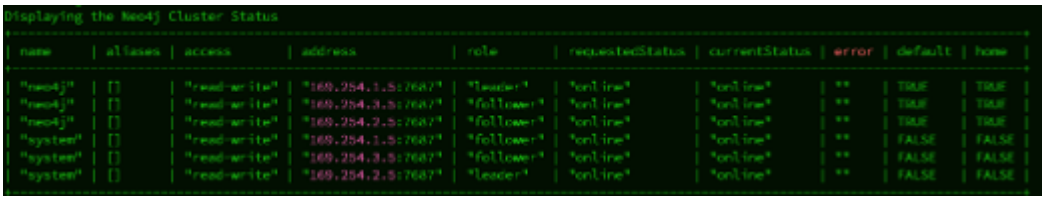
  vManage post checks

- Aplicable a nodos vManage:

  Comprobaciones de Configuration-DB(Neo4j):

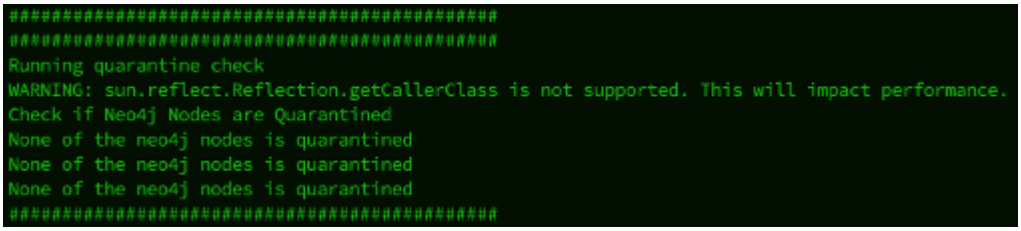
  Ejecute el comando "request nms configuration-db diagnostics" en todos los nodos de vManage:

  1. Compruebe el estado del nodo online y del liderazgo:(no disponible para todas las versiones)



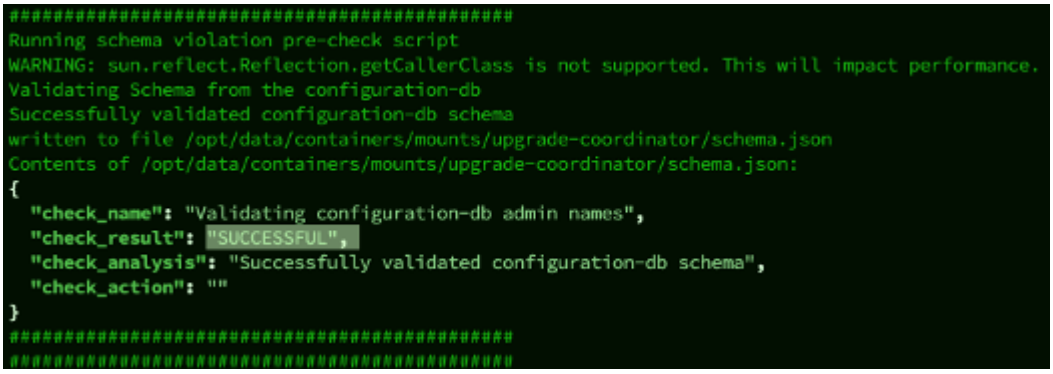
"Neo4j" debe mostrar 3 nodos en línea y 1 líder y 2 seguidores. "system" también debe mostrar 3 nodos en línea y 1 líder y 2 seguidores; sin embargo, como este no es el Db predeterminado, el indicador predeterminado es false. Si hay menos de 3 entradas en cada neo4j y el sistema significa que el nodo se ha caído del clúster. Póngase en contacto con el TAC de Cisco para solucionar el mismo problema.

2. Compruebe si algún nodo está en "cuarentena".

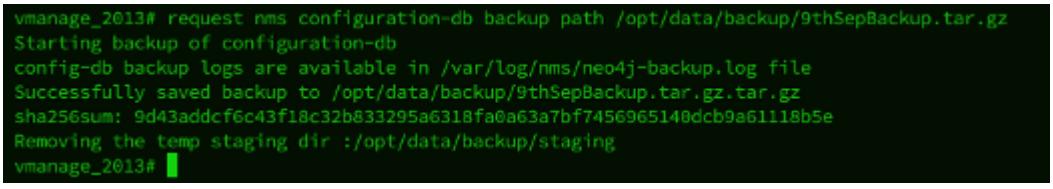


Ninguno de los nodos debe estar en cuarentena.

3. La validación del esquema debe ser "correcta".



4. Recopile una copia de seguridad de configuration-db usando el comando "request nms configuration-db diagnostics" y asegúrese de que sea exitosa.



Si se observan incoherencias o errores, póngase en contacto con el TAC de Cisco para obtener información sobre la solución de problemas.

Alternativamente, podemos ejecutar estas llamadas API para confirmar el estado del nodo vmanage para un clúster (para todos los nodos COMPUTE+DATA) - funciona sólo en la versión 20.12 y posteriores

```
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
```

Asegúrese de que en un clúster sólo haya un líder tanto para neo4j como para el sistema y que descanse como seguidores. Asegúrese de que todos los nodos estén en línea. Si tiene un clúster de 3 nodos (los tres son COMPUTE+DATA), debe haber un solo líder tanto para neo4j como para el sistema. Cualquier desviación, debe comunicarse con TAC

5. Verifique /var/log/kern.log para ver si hay errores de disco, memoria o E/S. Esto debe comprobarse en todos los nodos de vManage.

6. Verifique el paso cuando forme un clúster nuevo para vmanage que no tenga CC entre cada nodo
Realice ssh como vmanage-admin desde el nodo 1 a otros nodos cluster ip y viceversa, para verificar si se intercambia la clave pública y si funciona la contraseña menos ssh [Se requiere token de consentimiento para mostrar estos pasos]

```
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:
```

En caso de que el resultado pida introducir la contraseña, póngase en contacto con el TAC

Comprobaciones de Controller Post:

Aplicable a todos los controladores SD-WAN (vBond, vManage, vSmart):

Ejecute los comandos en todos los controladores de la superposición y confirme que el UUID de vManage y los números de serie vistos sean válidos para el fabric actual:

Comandos de vBond:

show orchestrator valid-vsmarts

show orchestrator valid-vmanage-id

Comandos vManage/vSmart:

show control valid-vsmarts

show control valid-vmanage-id

Tenga en cuenta que el resultado de show control valid-vsmarts incluye los números de serie de los nodos vsmarts y vManage.

Compárelo con los que se ven en la interfaz de usuario de vManage. Vaya a la sección Configuración > Certificados > Controladores.

Si se observan entradas adicionales para el UUID/número de serie que actualmente no están incorporadas al fabric, debemos eliminarlas. Puede ponerse en contacto con el TAC de Cisco para el mismo fin.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).