Reconstruisez votre fabric Catalyst SD-WAN

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Prérequis avant la reconstruction du fabric
  - Options de déploiement
- Étapes communes à toutes les combinaisons
- Installer et activer des contrôleurs SD-WAN (gestionnaire, validateur, contrôleur)
  - Afficher un noeud Cisco Manager
  - Afficher le validateur
  - Activer un noeud de contrôleur (vSmart)
  - Configuration CLI de base sur tous les contrôleurs
- Combinaison 1 : vManage autonome + pas de DR
  - Étape 1: Vérifications préalables
  - Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
  - Étape 3: Sauvegarde/restauration Config-db
  - Étape 4: Réauthentification des contrôleurs et invalidation des anciens contrôleurs
  - Étape 5: Valider les chèques
- Combinaison 2 : vManage autonome + DR noeud unique
  - Étape 1: Vérifications préalables
  - Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
  - Étape 3: Sauvegarde/restauration Config-db
  - Étape 4: Configuration DR à noeud unique
  - Étape 5: Réauthentification des contrôleurs et invalidation des anciens contrôleurs
  - Étape 6: Valider les chèques
- Combinaison 3 : Cluster vManage + aucun DR
  - Étape 1: Vérifications préalables
  - Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
  - Étape 3: Créer un cluster vManage
  - Étape 4: Sauvegarde/restauration Config-db
  - Étape 5: Réauthentification des contrôleurs et invalidation des anciens contrôleurs
  - Étape 6: Valider les chèques
- Combinaison 4 : Cluster vManage + DR manuel/en veille froide
  - Étape 1: Vérifications préalables
  - Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
  - Étape 3: Créer un cluster vManage
  - Étape 4: Configuration du cluster DR en veille froide
  - Étape 5: Sauvegarde/restauration Config-db

Étape 6: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

Étape 7: Activation de la veille (et restauration)

Étape 8: Valider les chèques

Combinaison 5 : Cluster vManage + DR activé

Étape 1: Vérifications préalables

Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

Étape 3: Créer un cluster vManage

Étape 4: Sauvegarde/restauration Config-db

Étape 5: Activer la reprise après sinistre sur un cluster vManage

Étape 6: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

Valider les chèques

Introduction

Ce document décrit comment reconstruire un fabric Cisco SD-WAN, y compris la sauvegarde et la restauration des configurations de contrôleur pour divers déploiements.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco
- Cisco Software Central
- Téléchargez le logiciel Controllers depuis le site software.cisco.com

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Prérequis avant la reconstruction du fabric

- Un nouvel ensemble de system-ips, site-ids doit être configuré pour le nouveau fabric pour les contrôleurs

- S'assurer que les règles de pare-feu sont en place pour permettre la communication entre les contrôleurs et les périphériques
- Notez le nom d'utilisateur et le mot de passe neo4j(configuration-db) (ils doivent être identiques sur tous les noeuds vManage d'un cluster)
- Désactiver le saut de port sur tous les bords
- Augmenter les délais de redémarrage progressif à 7 jours
- Effacer les alarmes dans les outils tiers avant la migration
- Les données d'état historiques (alarmes, événements, état des périphériques, etc.) sont perdues, sauf si une configuration préalable est nécessaire pour exporter les statistiques vers un serveur externe tel que vAnalytics
- Si Cloud OnRamp est configuré, assurez-vous d'avoir accès au c8000v déployé dans le cloud avant de commencer cet exercice
- Si SDAVC est activé sur l'ancien fabric, assurez-vous qu'il est activé sur le nouveau fabric (pour le cluster, il doit être activé sur un seul noeud uniquement)
- La restauration Configuration-db est prise en charge uniquement sur la même version que le fabric d'origine
- Confirmez la personne utilisée pour les contrôleurs. Nous prenons en charge les personnages COMPUTE_DATA et DATA (détails sous chaque section)
- Pour l'autorité de certification d'entreprise, vous devez utiliser le certificat racine émis par l'autorité de certification d'entreprise, qui est utilisé dans la superposition existante, et le certificat est signé à l'aide du serveur de l'autorité de certification d'entreprise et installé pour tous les contrôleurs via l'interface utilisateur

Options de déploiement

Déploiement vManage

- Autonome (1 noeud)
- Cluster (3 noeuds ou 6 noeuds)

Options DR

- Pas de DR
- DR à noeud unique
- Cluster DR de secours (manuel / déclenché par l'administrateur)

Remarque : Pour plus de détails sur le type de reprise après sinistre, consultez ce lien

---

Combinaisons :

#	Configuration de vManage	Option DR
1	Autonome (1 noeud)	Pas de DR
2	Autonome (1 noeud)	DR à noeud unique
3	Cluster (3 noeuds ou 6 noeuds)	Pas de DR
4	Cluster (3 noeuds ou 6 noeuds)	Cluster DR de secours

Étapes communes à toutes les combinaisons

Ces étapes sont communes à toutes les combinaisons de déploiement. Elles couvrent le processus d'activation des instances de VM et d'application de la configuration CLI de base. Chaque section de combinaison indique le nombre d'instances à déployer et les étapes supplémentaires à effectuer.

Installer et activer des contrôleurs SD-WAN (gestionnaire, validateur, contrôleur)

Remarque : Cisco a renommé certains termes, qui sont donc interchangeables. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst Controller

---

Téléchargez les fichiers OVA pour les contrôleurs SD-WAN à partir de la page de téléchargement du logiciel Cisco ici :

- Choisissez vEDGE Cloud et téléchargez le vBond OVA pour la version logicielle requise.
- Choisissez le logiciel vManage et téléchargez le logiciel vManage OVA pour la version logicielle requise.
- Choisissez le logiciel vSmart et téléchargez la vSmart OVA pour la version logicielle requise.

Remarque : Sur les plates-formes ESXi/cloud, faites tourner les contrôleurs vSmart, vBond et vManage à l'aide du fichier OVA. Reportez-vous au document lié et assurez-vous que suffisamment de CPU, de mémoire vive et de disques sont alloués à tous les contrôleurs en fonction du type de déploiement SD-WAN. Accédez ici pour obtenir des

---

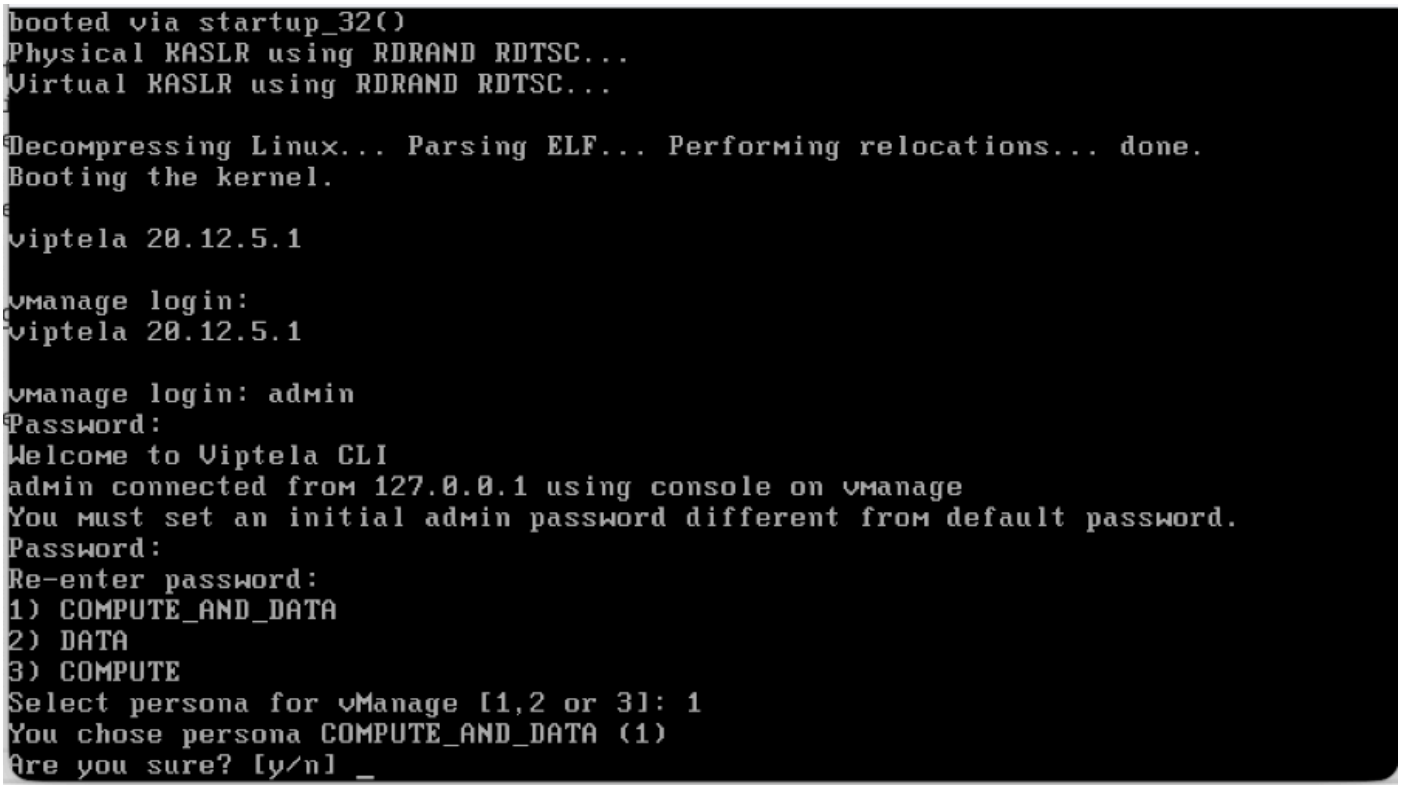
informations supplémentaires. Veillez à attribuer un disque secondaire au noeud vManage comme indiqué dans la colonne Taille de stockage* du guide de calcul lié.

Afficher un noeud Cisco Manager

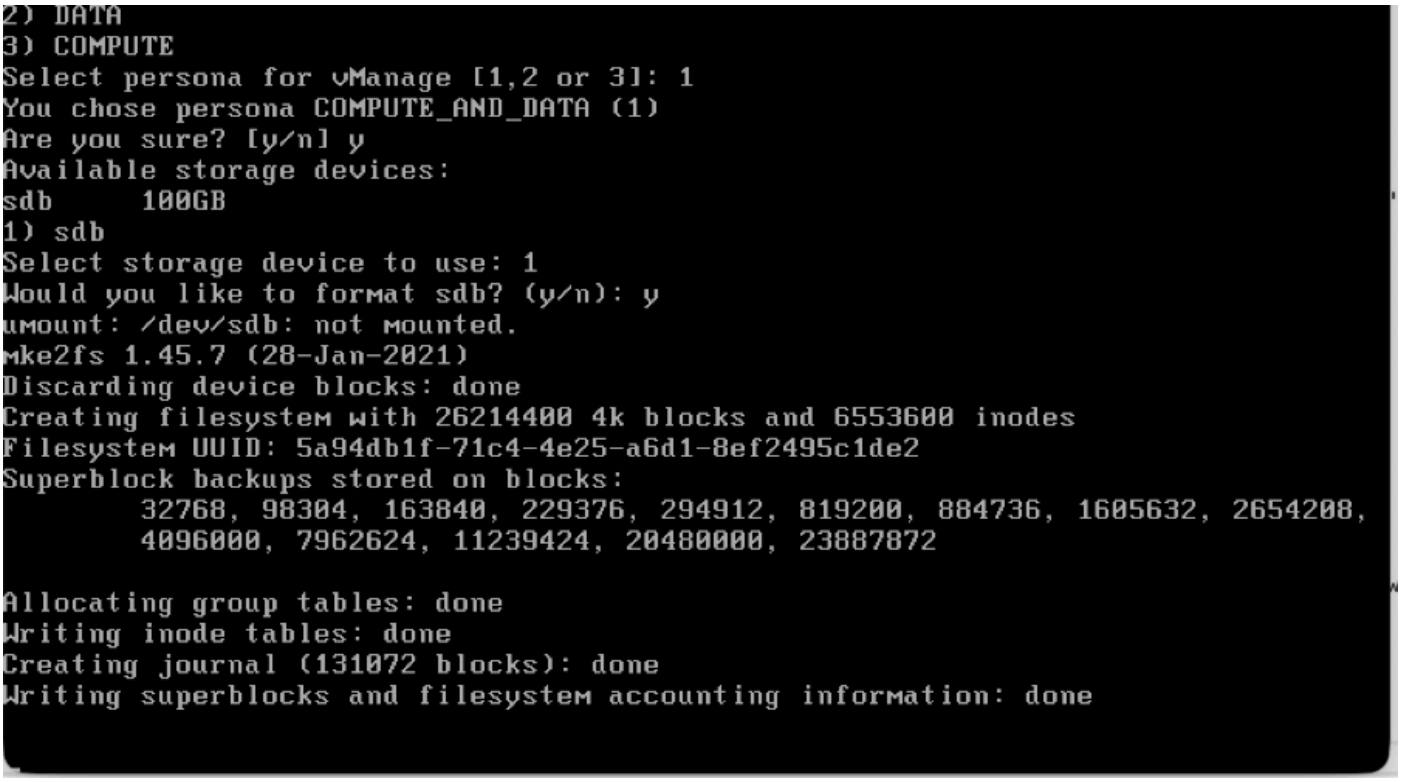
- Une fois que la machine virtuelle Cisco Manager ou vManage est déployée et que la console du gestionnaire est accessible, attendez la fin du démarrage. Une indication est qu'un système de messagerie est prêt et vous invite à saisir le nom d'utilisateur et le mot de passe.
- Entrez le nom d'utilisateur par défaut admin et le mot de passe admin. Publiez qu'il invite l'utilisateur à modifier le mot de passe, définissez le mot de passe nécessaire pour l'utilisateur admin selon votre choix.
- Il invite ensuite l'utilisateur à sélectionner le personnage. Il s'agit d'une étape critique si l'intention est d'avoir un cluster vManage. Veuillez choisir le personnage comme indiqué dans les scénarios suivants :

```
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
```

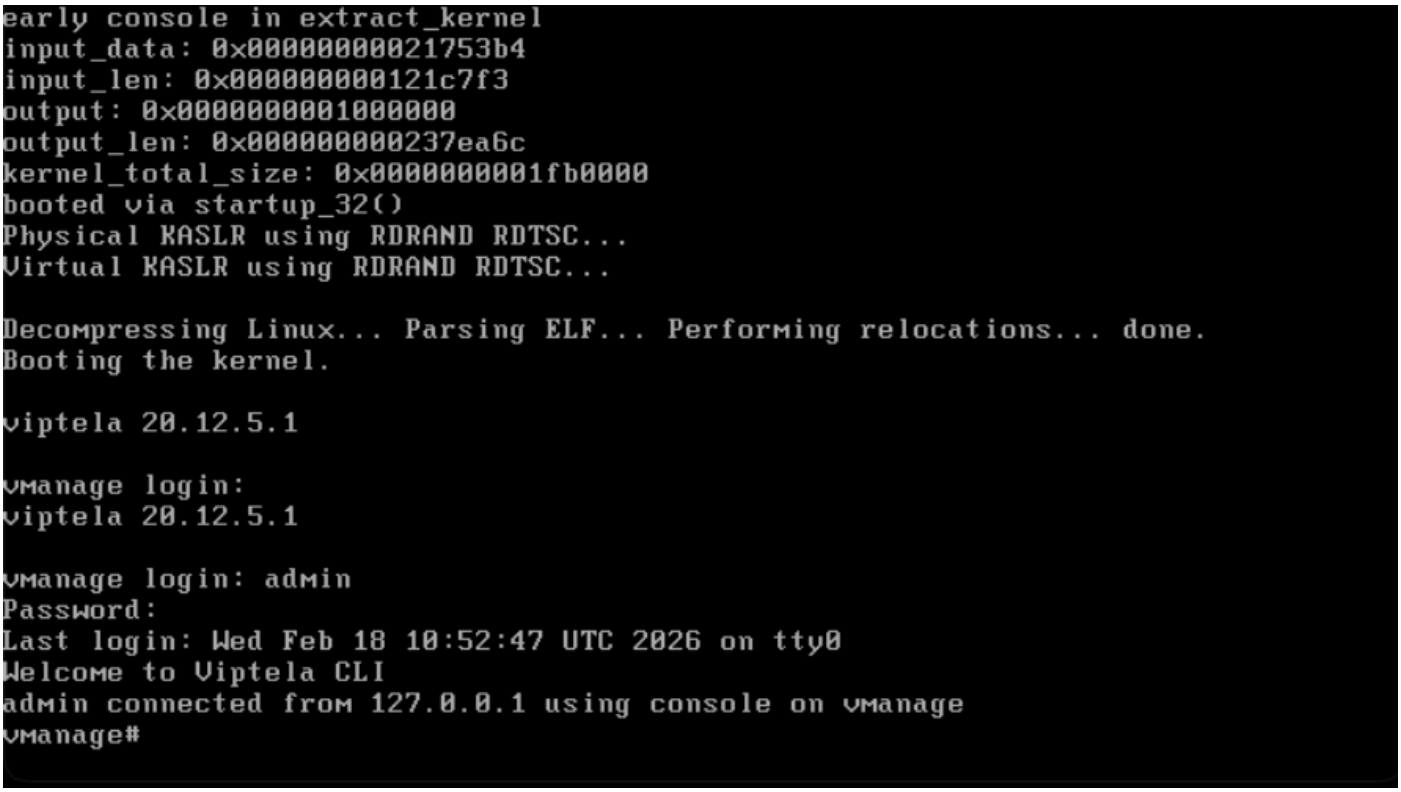
Exemple : Choisir 1 pour COMPUTE_AND_DATA



Choisissez le disque secondaire comme indiqué :

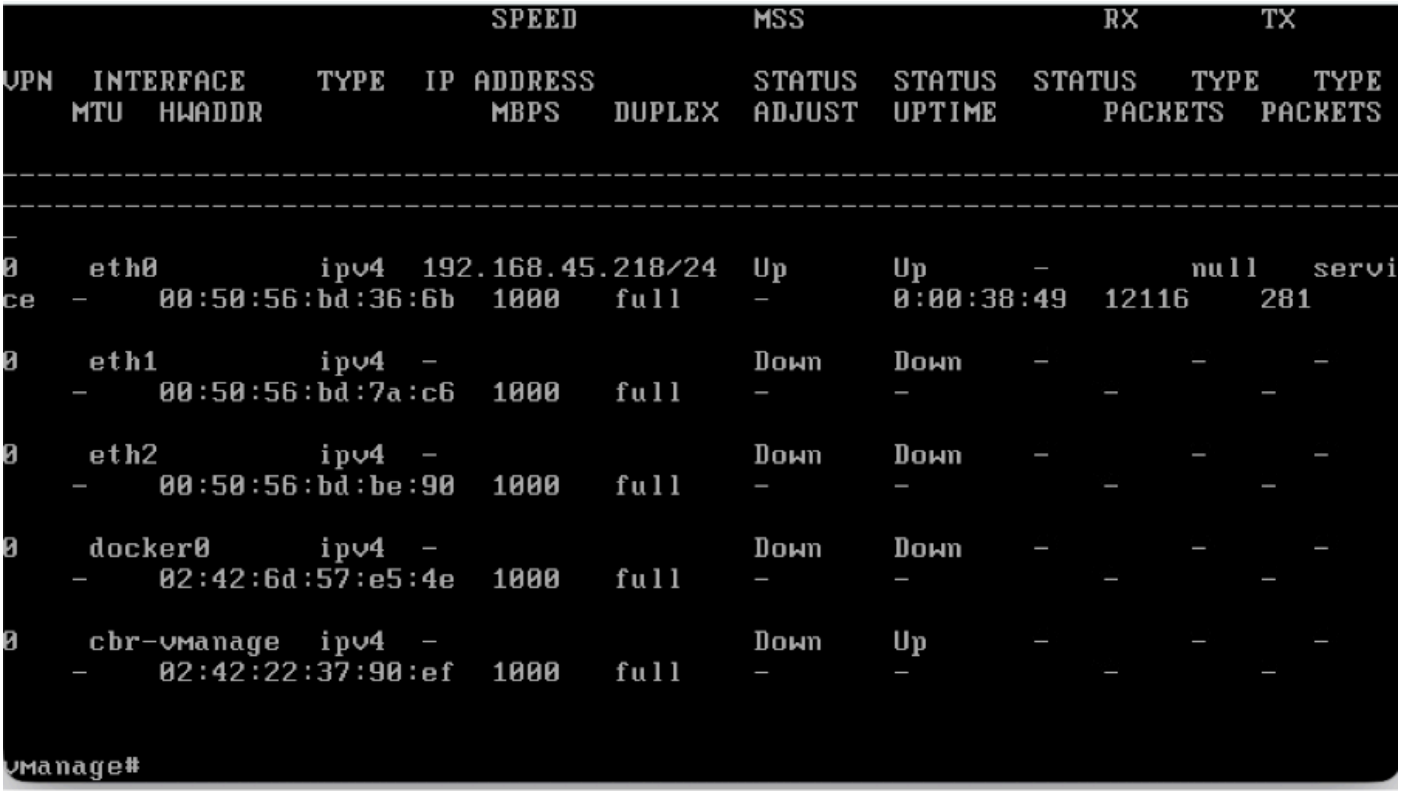


- Choisissez le disque secondaire et tapez Y pour confirmer.
- Cisco Manager se recharge. Une fois qu'il démarre, entrez le nom d'utilisateur et le mot de passe avec le nouveau mot de passe nouvellement configuré.



- Vous pouvez configurer l'interface de gestion VPN 512 pour activer l'accès de gestion hors bande au contrôleur.
- Utilisez la commande show interface | pour vérifier les VPN auxquels les interfaces sont actuellement mappées.
- configurez les interfaces en conséquence.

Exemple



```
                                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#
```

Remarque : Vous pouvez faire référence à la configuration du vManage existant et configurer le même schéma d'adresse IP ici.

Configurations d'interface de gestion (VPN 512)

- Si une interface doit être déplacée du VPN 0 vers le VPN 512, utilisez ces commandes, puis configurez l'adresse IP sur l'interface

```
Conf t
vpn 0
 no interface eth0
vpn 512
 interface eth0
  ip address <IP-address/mask>
  no shutdown
 !
 ip route 0.0.0.0/0 <default-gateway IP>
!
```

Afficher le validateur

- Sur l'hyperviseur, configurez l'ordinateur requis (processeur, mémoire vive et disque) pour le

noeud vBond et mettez-le sous tension.

- Une fois la console accessible, attendez que le vBond démarre complètement. Attendez le message System Ready.
- Le système vous demande ensuite le nom d'utilisateur et le mot de passe. Entrez les informations d'identification et de connexion utilisateur par défaut admin et admin. Ensuite, l'utilisateur est invité à modifier le mot de passe, définissez le mot de passe requis pour l'utilisateur admin selon votre choix.
- Vous pouvez configurer l'interface de gestion VPN 512 pour activer l'accès de gestion hors bande au contrôleur.
- Utilisez la commande show interface | pour vérifier les VPN auxquels les interfaces sont actuellement mappées.
- Configurez les interfaces en conséquence.

Exemple :

```
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#
```



Remarque : Vous pouvez faire référence à la configuration du vBond existant et configurer les mêmes configurations ici.

Configurations d'interface de gestion (VPN 512)

- Si une interface doit être déplacée du VPN 0 vers le VPN 512, utilisez ces commandes, puis

configurez l'adresse IP sur l'interface.

```
Conf t
vpn 0
 no interface eth0
vpn 512
 interface eth0
  ip address <IP-address/mask>
  no shutdown
 !
 ip route 0.0.0.0/0 <default-gateway IP>
!
commit
```

Activer un noeud de contrôleur (vSmart)

- Suivez les mêmes étapes que le validateur pour activer le noeud vSmart.
- Une fois l'adresse IP VPN 512 configurée sur tous les contrôleurs SD-WAN, vous pouvez y accéder à l'aide de SSH sur l'adresse IP VPN 512.

Configuration CLI de base sur tous les contrôleurs

Une fois que vous avez un accès SSH à tous les contrôleurs, configurez ces configurations CLI sur chaque contrôleur.

Configuration du système

```
config t
system
 host-name             <hostname>
 system-ip             <unique system-IP>
 site-id               <site-id>
 organization-name     <organization name>
 vbond <IP address/URL of vBond>
commit
```



Remarque : si nous utilisons une URL comme adresse vBond, assurez-vous de configurer les adresses IP du serveur DNS dans la configuration VPN 0 ou assurez-vous qu'elles peuvent être résolues.

Configuration de l'interface de transport (VPN 0)

Ces configurations sont nécessaires sur tous les contrôleurs pour activer l'interface de transport utilisée pour établir des connexions de contrôle avec les routeurs et le reste des contrôleurs.

```
config t
vpn 0
 dns <IP-address> primary
 dns <IP-address> secondary
 interface eth1
  ip address <IP-address/mask>
  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 <default-gateway IP>
commit
```



Remarque : vous pouvez faire référence aux configurations de votre contrôleur existant et si la configuration est présente, vous pouvez ajouter cette configuration aux nouveaux contrôleurs.

Configurez le protocole de contrôle en tant que TLS uniquement si les routeurs doivent établir des connexions de contrôle sécurisées avec les noeuds vManage à l'aide de TLS. Par défaut, tous les contrôleurs et les routeurs établissent une connexion de contrôle à l'aide de DTLS. Il s'agit d'une configuration facultative requise uniquement sur les noeuds vSmart et vManage, en fonction de vos besoins.

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

Combinaison 1 : vManage autonome + pas de DR

Instances nécessaires :

- 1 vManage (COMPUTE_AND_DATA)
- 1 ou plusieurs vBond
- 1 vSmart ou plus

Étapes:

1. Afficher toutes les instances à l'aide des étapes communes
2. Vérifications préalables
3. Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
4. Sauvegarde/restauration Config-db
5. Valider les chèques

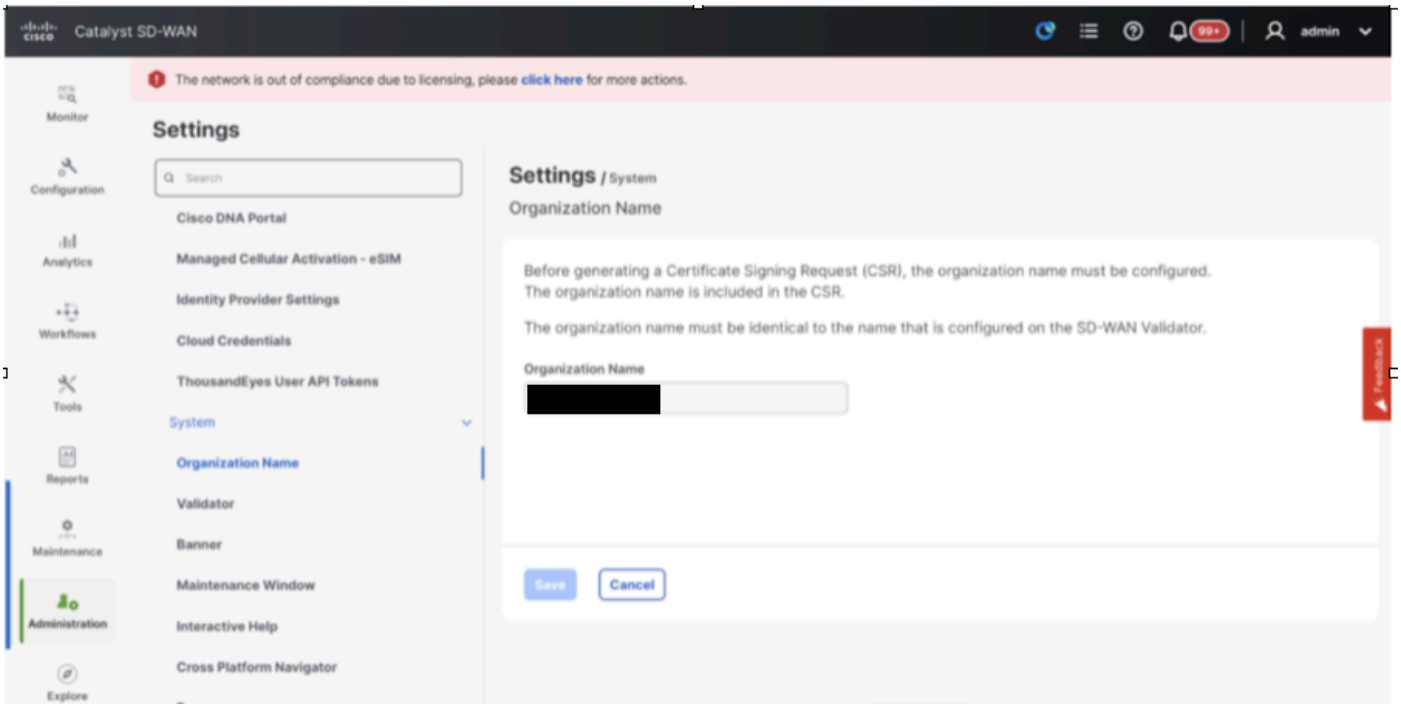
Étape 1: Vérifications préalables

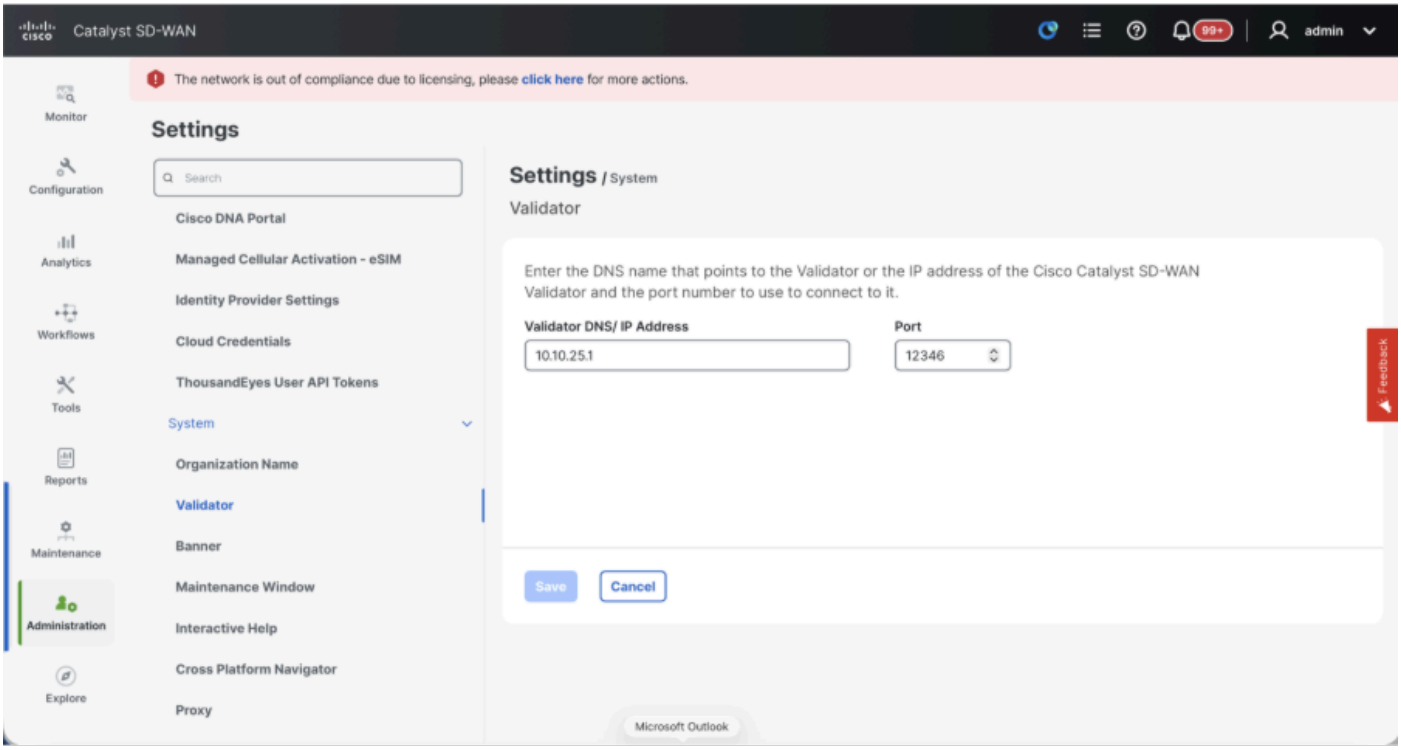
- Assurez-vous que le nombre d'instances Cisco SD-WAN Manager actives est identique au nombre d'instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles exécutent la même version logicielle.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles sont en mesure d'atteindre l'adresse IP de gestion de Cisco SD-WAN Validator.
- Assurez-vous que les certificats ont été installés sur les instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que les horloges sur tous les périphériques Cisco Catalyst SD-WAN, y compris les instances Cisco SD-WAN Manager nouvellement installées, sont synchronisées.
- Assurez-vous qu'un nouvel ensemble d'IP système et d'ID de site est configuré sur les instances de Cisco SD-WAN Manager nouvellement installées, avec la même configuration de base que le cluster actif.

Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

Mettre à jour les configurations sur l'interface utilisateur vManage

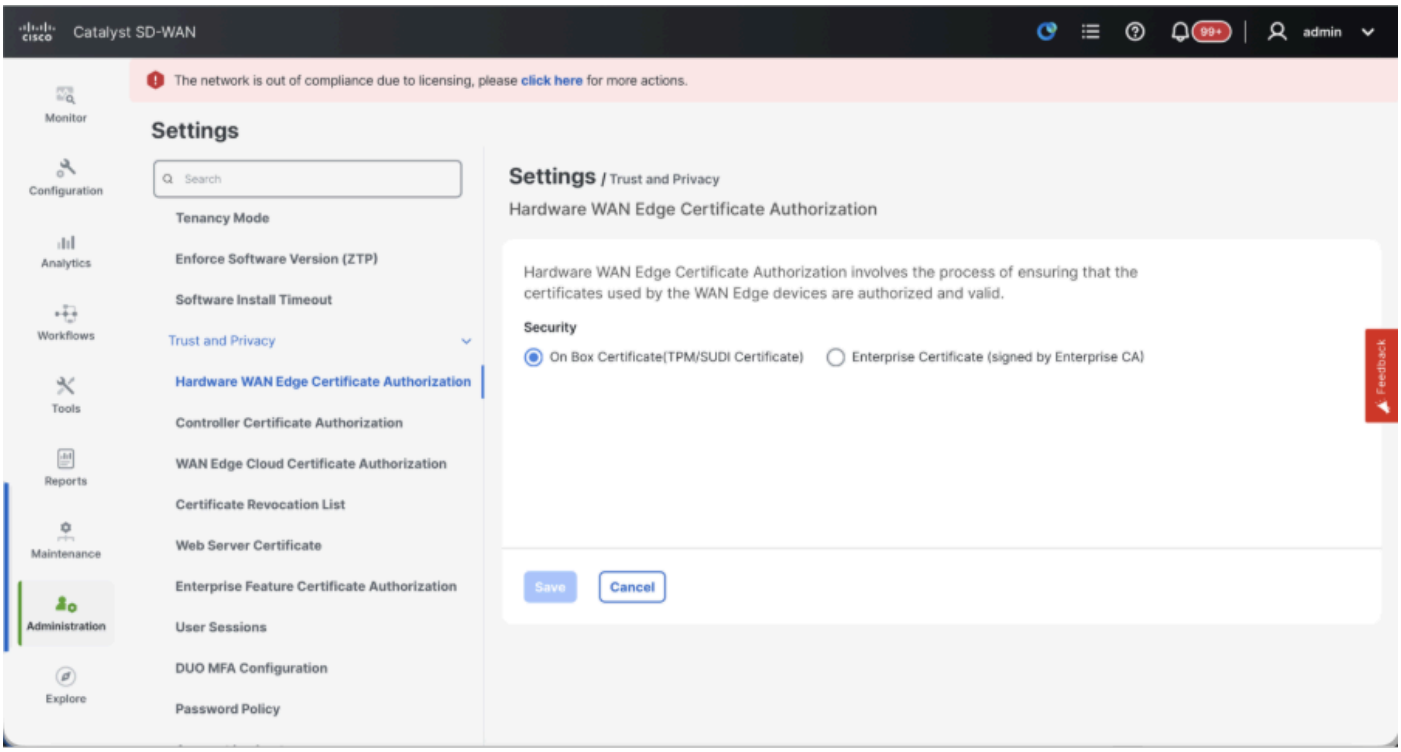
- Une fois les configurations de l'étape 1 ajoutées à l'interface de ligne de commande de tous les contrôleurs, nous pouvons accéder à l'interface utilisateur web de vManage, à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Administration > Settings et complétez ces étapes.
- Configurez le nom de l'organisation et l'adresse URL/IP du validateur/vBond. Configurez la même valeur que dans l'interface de ligne de commande du noeud vManage.
- Dans vManage 20.15/20.18, ces configurations sont disponibles dans la section Système.



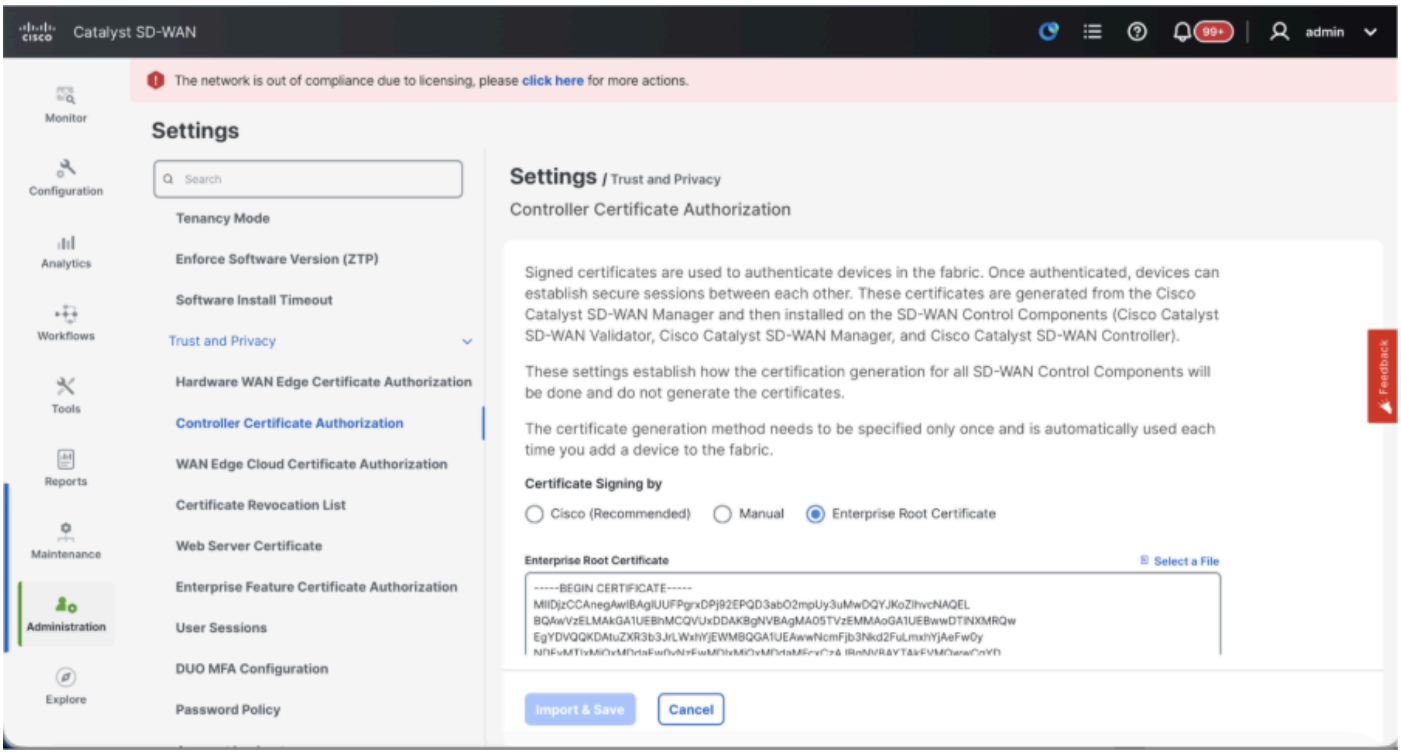


- Vérifiez les configurations de l'autorité de certification (CA), qui décide de l'autorité de certification utilisée pour signer les certificats. Nous pouvons voir 3 options ici :

1. Hardware WAN Edge Certificate Authorization : décide de l'autorité de certification pour les routeurs périphériques SD-WAN matériels.
    - Certificat On Box (certificat TPM/SUDI) : avec cette option, le certificat préinstallé sur le matériel du routeur est utilisé pour établir les connexions de contrôle (connexions TLS/DTLS)
    - Certificat d'entreprise (signé par l'autorité de certification d'entreprise) : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

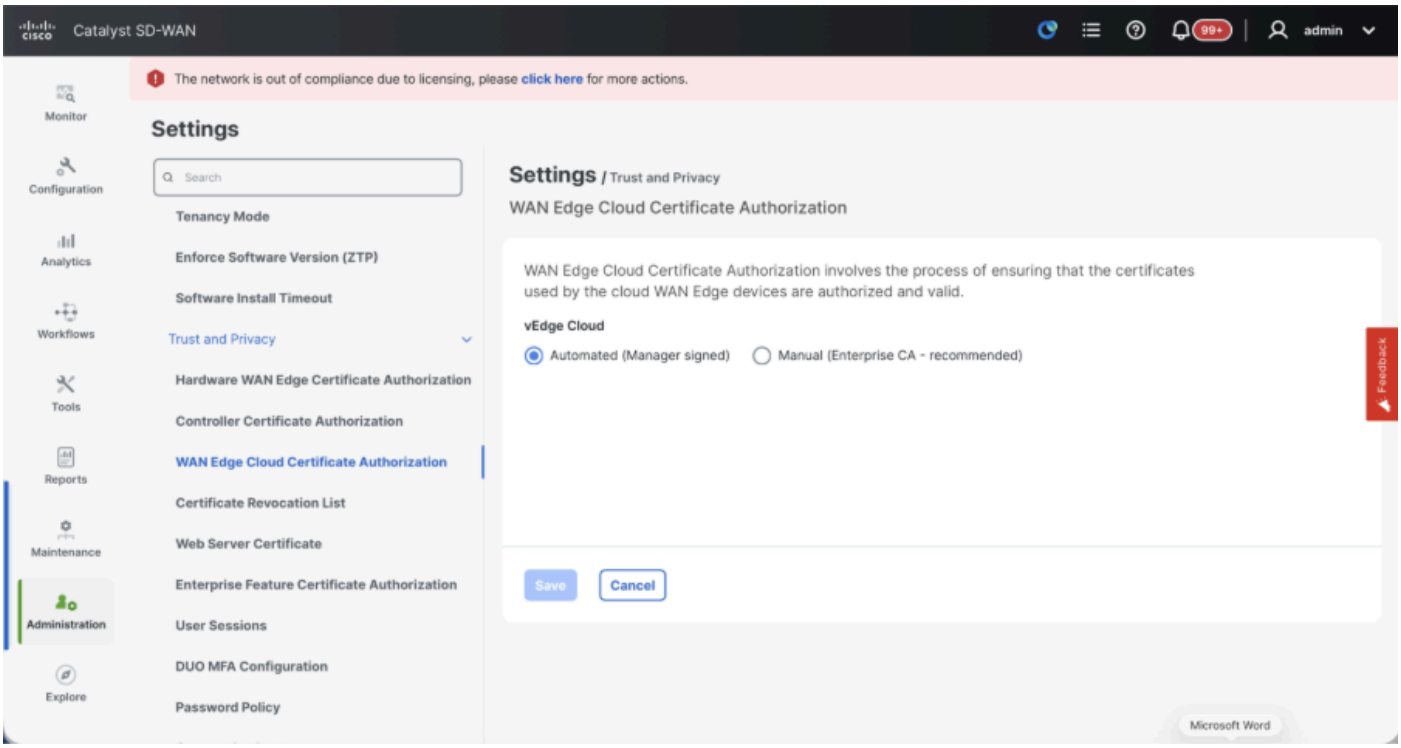


2. Autorisation de certificat de contrôleur - Décide de l'autorité de certification pour les contrôleurs SD-WAN.
    - Cisco (recommandé) : les contrôleurs utilisent les certificats signés par Cisco PKI. vManage contacte automatiquement le portail PNP à l'aide des informations d'identification de compte Smart configurées sur le vManage, obtient le certificat signé et est installé sur le contrôleur.
    - Manuel - Les contrôleurs utilisent les certificats signés par Cisco PKI. Signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
    - Certificat racine d'entreprise : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

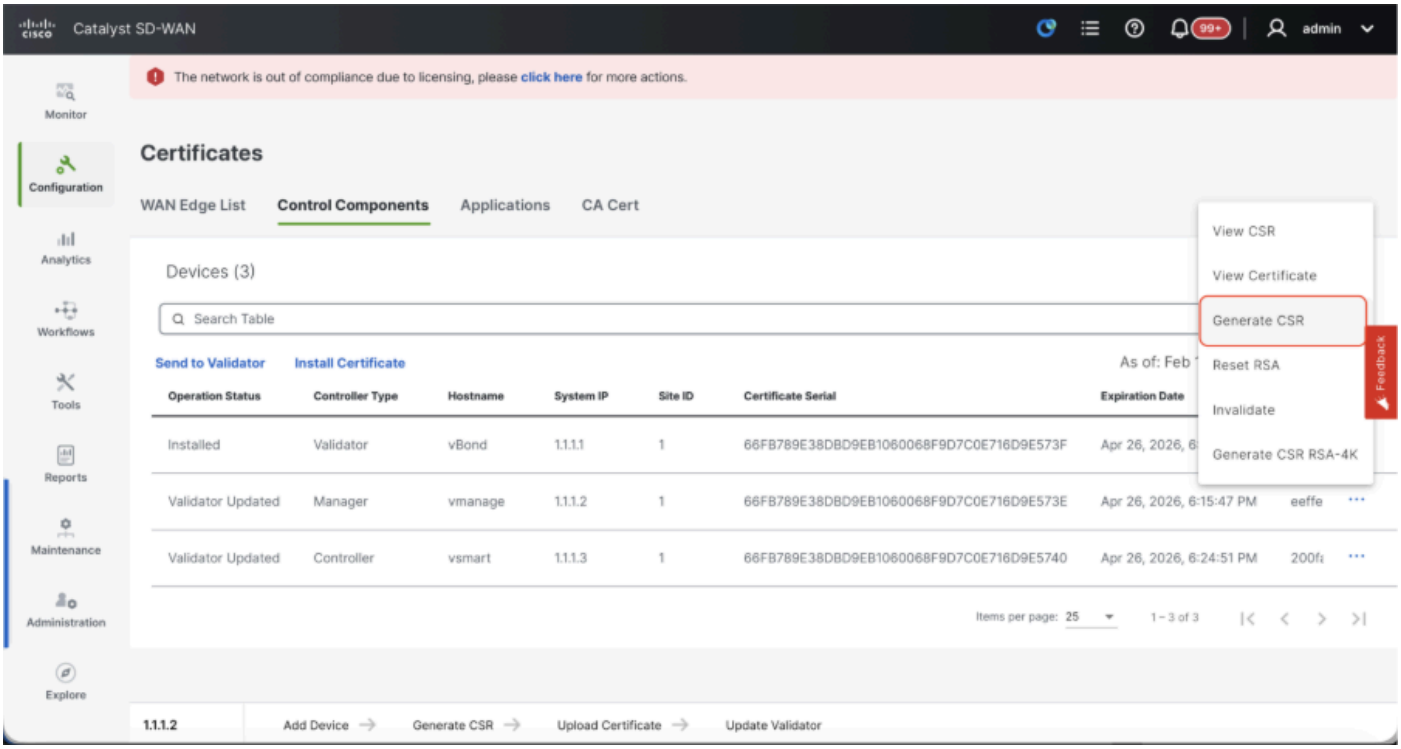


3. WAN Edge Cloud Authorization - Décide de l'autorité de certification pour les routeurs virtuels SD-WAN Edge (CSR1000v, C8000v, cloud vEdge)
    - Automatisé (vManage signed) : vManage signe automatiquement le CSR pour les routeurs de périphérie virtuels et installe le certificat sur le routeur.
    - Manuel (CA d'entreprise - recommandé) - Les routeurs virtuels utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

Dans ce cas, si nous utilisons notre propre autorité de certification, Enterprise certificate authority, sélectionnez Enterprise.



- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers
- Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par

vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.

Intégration de vBond/Validator et vSmart/Controller à vManage

Accédez à Configuration > Devices > Control Components dans le cas des noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

Intégration de vBond/Validator

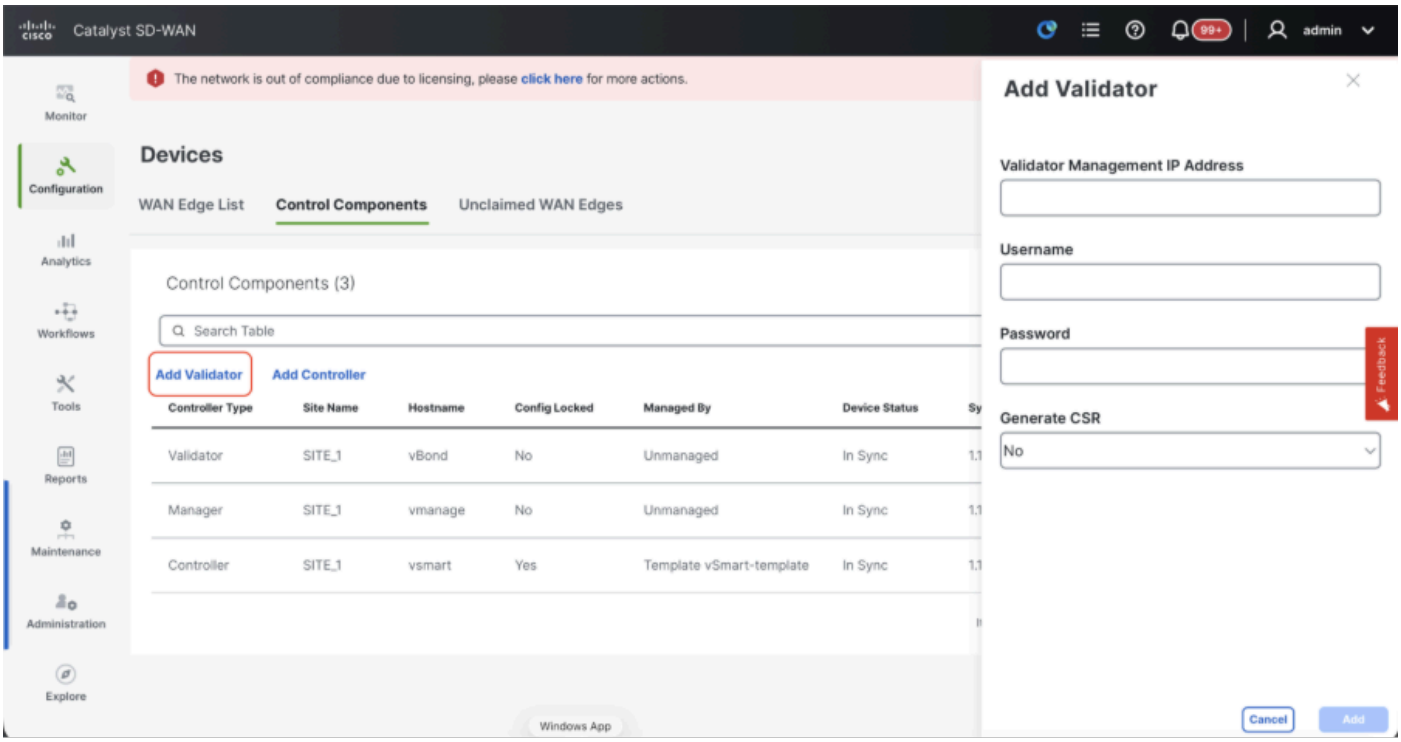
- Cliquez sur Add vBond dans le cas de 20.12 vManage ou sur Add Validator dans le cas de 20.15/20.18 vManage. Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vBond qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée de l'interface CLI de vManage vers vBond IP.
- Entrez les informations d'identification utilisateur de vBond.



Remarque : nous devons utiliser les identifiants d'administration de vBond ou une partie utilisateur du groupe netadmin. Vous pouvez le vérifier dans l'interface de ligne de commande du vBond. Sélectionnez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vBond.



Remarque : Si le vBond est derrière un périphérique NAT/pare-feu, vérifiez si l'adresse IP de l'interface VPN 0 de vBond est traduite en une adresse IP publique. Si l'adresse IP de l'interface VPN 0 n'est pas accessible depuis vManage, utilisez l'adresse IP publique de l'interface VPN 0 dans cette étape.



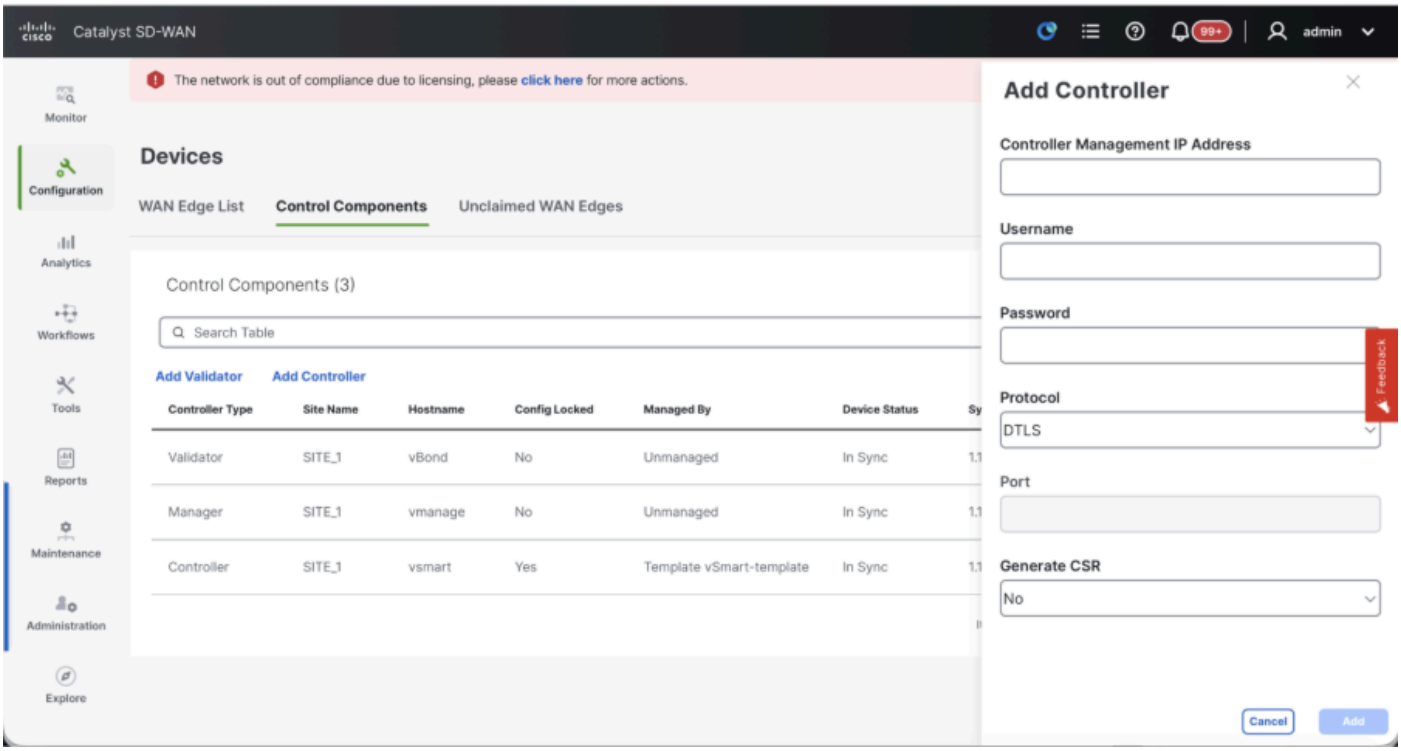
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vBond.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il existe plusieurs vBonds, répétez les mêmes étapes.

Intégration de vSmart/Controller

- Cliquez sur Add vSmart dans le cas de vManage 20.12 ou sur Add Controller dans le cas de vManage 20.15/20.18.
- Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vSmart qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée depuis l'interface CLI de vManage vers vSmart IP.
- Entrez les informations d'identification de l'utilisateur de vSmart. Notez que nous devons utiliser les informations d'identification d'administration de vSmart ou d'une partie utilisateur du groupe netadmin.

- Vous pouvez le vérifier dans l'interface de ligne de commande du vSmart.
- Définissez le protocole sur TLS, si nous avons l'intention d'utiliser TLS pour les routeurs afin d'établir des connexions de contrôle avec vSmart. Cette configuration doit également être configurée sur l'interface de ligne de commande des noeuds vSmarts et vManage.
- Choisissez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vSmart.

Remarque : si le vSmart est derrière le périphérique/pare-feu NAT, vérifiez si l'adresse IP de l'interface VPN 0 vSmart est traduite en une adresse IP publique, et si l'adresse IP de l'interface VPN 0 n'est pas accessible à partir de vManage, utilisez l'adresse IP publique de l'adresse IP de l'interface VPN 0 dans cette étape.



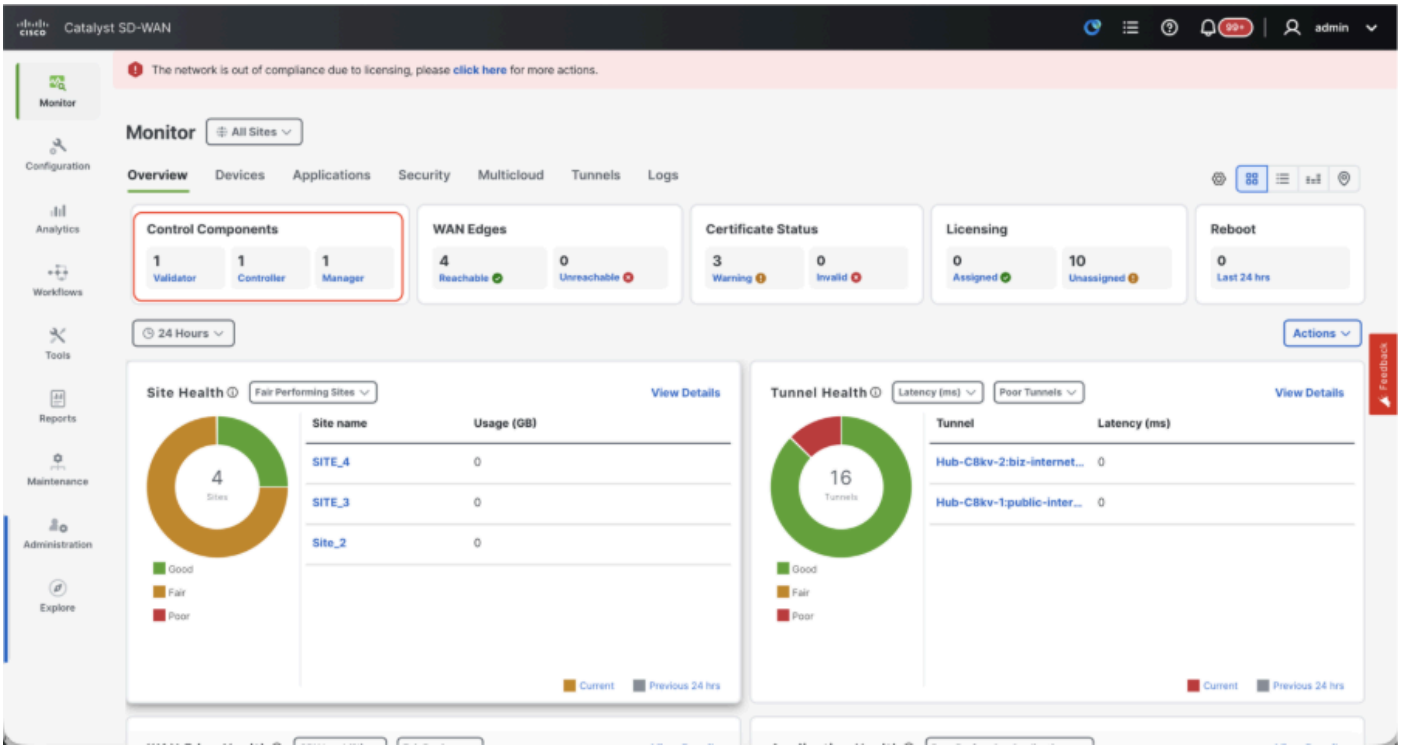
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vSmart.
- Si vous choisissez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en naviguant jusqu'au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. La même procédure s'applique si nous utilisons Digicert et le certificat

racine d'entreprise.

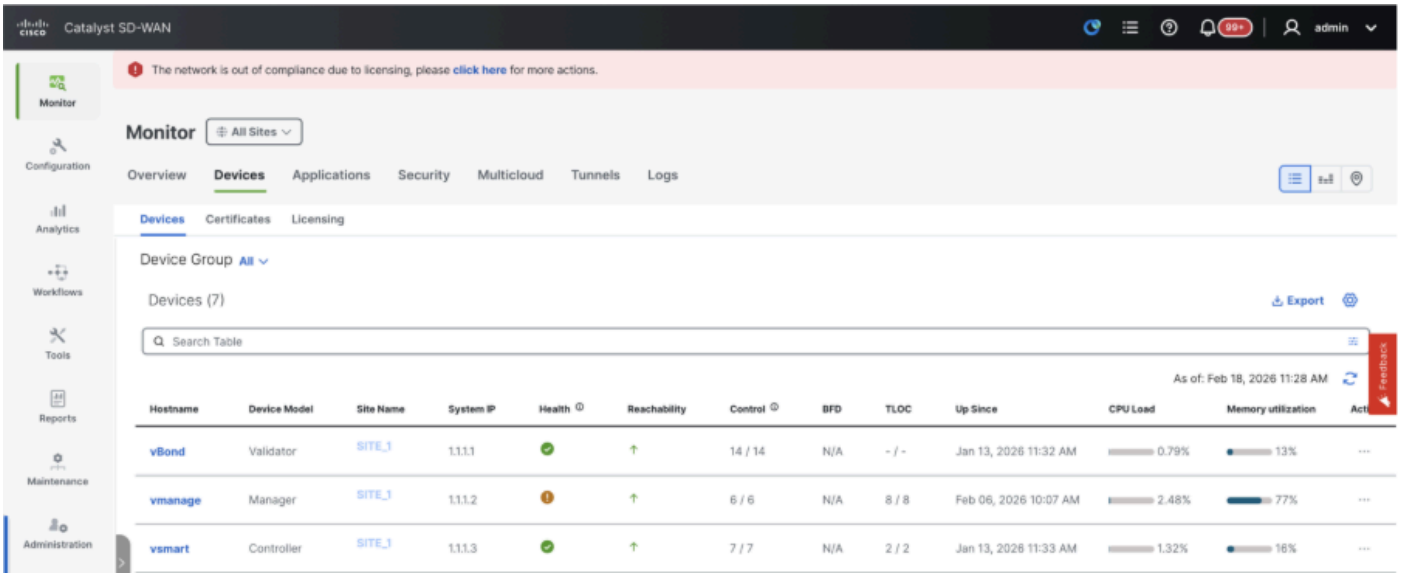
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- S'il y a plusieurs vSmarts, répétez les mêmes étapes.

Vérification

Une fois toutes les étapes terminées, vérifiez que tous les composants de contrôle sont accessibles dans Monitor > Dashboard



- Cliquez sur les composants de contrôle respectifs et vérifiez qu'ils sont tous accessibles.
- Accédez à Monitor > Devices et vérifiez que tous les composants de contrôle sont accessibles.



Étape 3: Sauvegarde/restauration Config-db

Collecter la sauvegarde et la restauration de la base de données de configuration vManage sur un autre noeud vManage

Collecter la sauvegarde Configuration-DB :

- Dans le fabric SD-WAN actuellement utilisé, vous pouvez générer une sauvegarde de la base de données de configuration sur les configurations de cluster vManage et vManage autonomes.
- Pour vManage autonome, ce vManage est lui-même le leader de la base de données de configuration.

Vérifiez que la base de données de configuration est en cours d'exécution sur le noeud vManage.

Vous pouvez vérifier la même chose à l'aide de la commande request nms configuration-db status sur l'interface de ligne de commande vManage. Le résultat est le suivant

```
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#
```

Utilisez cette commande pour collecter la sauvegarde configuration-db à partir du noeud vManage de tête de base de données de configuration identifié.

```
request nms configuration-db backup path /opt/data/backup/<filename>
```

Le résultat attendu est le suivant :

```
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#
```

- Notez les informations d'identification de configuration-db si elles ont été mises à jour.
- Si vous ne connaissez pas les informations d'identification de la base de données de configuration, contactez le TAC pour récupérer les informations d'identification de la base de données de configuration à partir des noeuds vManage existants.

- Les informations d'identification configuration-db par défaut sont username : neo4j et password : mot de passe

Restaurer la sauvegarde Configuration-db vers un autre noeud vManage

Copiez la sauvegarde configuration-db dans le répertoire /home/admin/ de vManage à l'aide de SCP.

Exemple de sortie de commande 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
```

Pour restaurer la sauvegarde configuration-db, nous devons d'abord configurer les informations d'identification configuration-db. Si vos identifiants configuration-db sont default(neo4j/password), nous pouvons ignorer cette étape.

Pour configurer les informations d'identification configuration-db, utilisez la commande request nms configuration-db update-admin-user. Utilisez le nom d'utilisateur et le mot de passe de votre choix.

Veuillez noter que le serveur d'applications de vManage est redémarré. En raison de laquelle l'interface utilisateur vManage devient inaccessible pendant une courte période.

```
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#
```

Publication que nous pouvons poursuivre pour restaurer la sauvegarde configuration-db :

Nous pouvons utiliser la commande request nms configuration-db restore path /home/admin/< > pour restaurer la base de données de configuration dans le nouveau 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
```

Une fois la base de données de configuration restaurée, assurez-vous que l'interface utilisateur vManage est accessible. Attendez environ 5 minutes, puis essayez d'accéder à l'interface utilisateur.

Une fois connecté à l'interface utilisateur avec succès, assurez-vous que la liste des routeurs Edge, le modèle, les stratégies et toutes les autres configurations qui étaient présentes sur votre interface utilisateur vManage précédente ou existante sont reflétés sur la nouvelle interface utilisateur vManage.

Mise en garde : La base de données de configuration restaurée contient toujours le ou les gestionnaires SD-WAN à partir desquels la sauvegarde a été effectuée. Elles sont répertoriées en tant qu'entrées Manager dans Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) mais ne sont pas membres de Administration > Cluster Management. Jusqu'à leur suppression à l'étape 4 :

- chaque rapport Send to Validator signale Failed to find Vmanage Cluster node for uuid <uuid> for them, et
- chaque installation de certificat de contrôleur à partir de l'interface utilisateur échoue et est restaurée.

N'effectuez aucune opération de certificat de contrôleur ou d'envoi au validateur sur ce vManage avant la fin de l'étape 4. Si l'installation d'un certificat échoue, n'installez pas le même certificat à partir de l'interface de ligne de commande ; Contactez le centre d'assistance technique Cisco TAC.

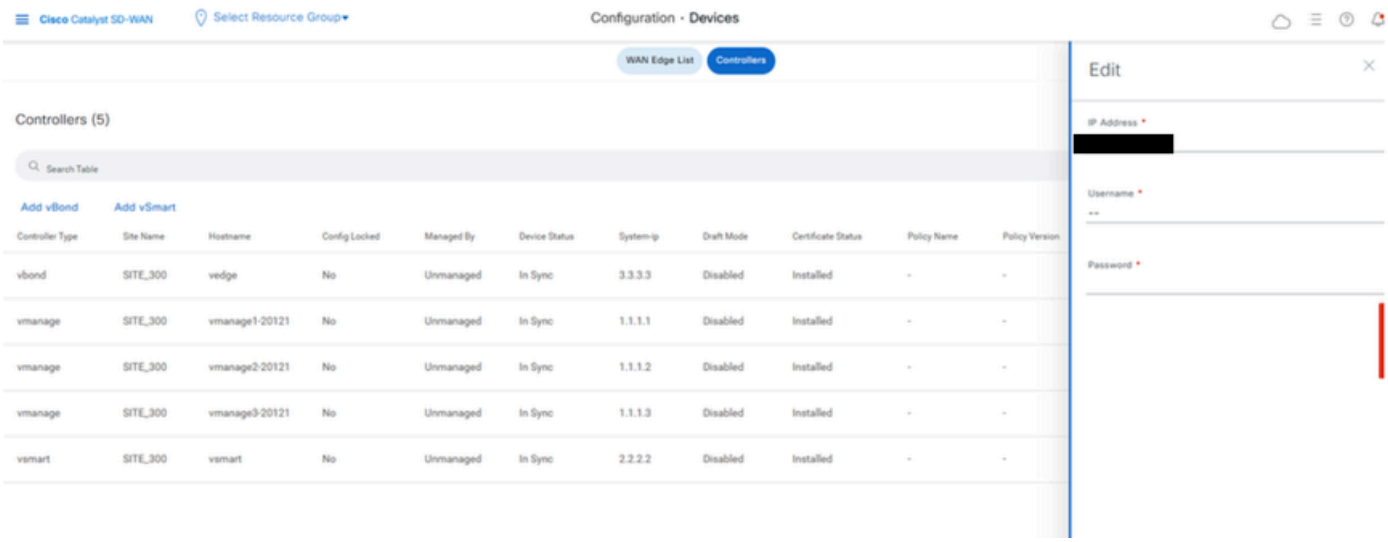
Étape 4: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

Une fois la base de données de configuration restaurée, nous devons réauthentifier tous les nouveaux contrôleurs (vmanage/vsmart/vbond) dans le fabric.

Remarque : en production réelle, si l'interface IP utilisée pour la ré-authentification est l'interface IP du tunnel, vous devez vous assurer que le service NETCONF est autorisé sur l'interface du tunnel de vManage, vSmart et vBond, ainsi que sur les pare-feu le long du chemin. Le port de pare-feu à ouvrir est le port TCP 830 en tant que règle bidirectionnelle du cluster DR vers tous les vBonds et vSmarts.

Sur l'interface utilisateur vmanage, cliquez sur Configuration > Devices > Controllers

- Cliquez sur les trois points situés près de chaque contrôleur, puis cliquez sur Edit





- Remplacez l'adresse IP (ip système du contrôleur) par l'adresse IP du VPN de transport 0 (interface de tunnel). Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur Enregistrer
- Procédez de la même manière pour tous les nouveaux contrôleurs du fabric

Synchroniser la chaîne de certificats racine

Une fois tous les contrôleurs intégrés, procédez comme suit :

Sur tout serveur Cisco SD-WAN Manager du cluster nouvellement actif, effectuez les actions suivantes :

Entrez cette commande pour synchroniser le certificat racine avec tous les périphériques Cisco Catalyst SD-WAN dans le nouveau cluster actif :

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

Entrez cette commande pour synchroniser l'UUID du gestionnaire Cisco SD-WAN avec le validateur Cisco SD-WAN :

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

Supprimer les entrées précédentes du gestionnaire SD-WAN

Effectuez cette opération juste après la synchronisation root-cert-chain et avant toute opération de certificat de contrôleur ou Envoyer au validateur.

1. Ouvrez Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) et Administration > Cluster Management. Chaque entrée vManage qui n'est pas cette entrée vManage est une entrée SD-WAN Manager précédente et doit être supprimée.
2. Avant toute action Envoyer au validateur ou Invalider, recherchez un enregistrement de numéro de série en conflit. Accédez à https://<vmanage-url>/dataservice/certificate/vsmart/list. Aucune entrée ne peut avoir un ancien numéro de série dont le numéro de série est égal à son propre numéro de série. Cette vérification est en lecture seule. Si une telle entrée existe, arrêtez-vous et contactez le TAC Cisco : any Send to Validator or Invalidate envoie la liste des contrôleurs et ce contrôleur perdrait ses connexions de contrôle.
3. Accédez à Monitor > Tasks et ouvrez la dernière tâche Push vSmart List. Examiner uniquement les résultats des tâches existantes ; ne cliquez pas ici sur Envoyer au validateur. Si aucune tâche récente n'est répertoriée, attendez la diffusion de la liste en début d'heure suivante. Chaque entrée précédente du gestionnaire SD-WAN doit indiquer Failed to find Vmanage Cluster node for uuid <uuid>. Si un uuid vManage a été envoyé avec succès, il s'agit d'un uuid vManage actif : ne l'invalidez pas.
4. Cliquez sur les trois points à droite de la première entrée précédente du gestionnaire SD-WAN, puis cliquez sur Invalidate. Attendez la fin de la tâche. Le résultat attendu est Success with warning, avec cet exercice :

```
Invalidating Root Certificate Autority of vManage-<uuid>
Sending serial number of vManage-<uuid> as invalid to all controllers
Failed to push serial list to vManage-<uuid> - retry in 30 seconds; Failed to find Vmanage Cluster node
Updated serial list will be sent to vManage-<uuid> when it is reachable
Clearing certificate on vManage-<uuid>
Successfully invalidated vManage-<uuid>
```

L'entrée affiche désormais No certificate installed. Le numéro de série précédent du gestionnaire SD-WAN et l'autorité de certification racine sont supprimés des validateurs.

5. Cliquez sur les trois points de la même entrée, puis cliquez à nouveau sur Invalider. Il se termine immédiatement, sans tâche, et l'entrée est supprimée.
6. Répétez les étapes 4 et 5 pour chaque entrée précédente du gestionnaire SD-WAN.
7. Cliquez sur Envoyer au validateur. Le résultat attendu est Success pour chaque destinataire dans quelques secondes, avec no Failed to find Vmanage Cluster node.

Invalider les anciens contrôleurs

Une fois que le fabric est restauré et que les sessions de contrôle et BFD sont actives pour tous les bords et contrôleurs du fabric, invalidez les anciennes entrées vBond/Validator et vSmart/Controller de l'interface utilisateur :

- Sur l'interface utilisateur de vManage, accédez à Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificats > Contrôleurs).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Invalidate.
- Cliquez sur Send to Validator (Send to vBond in 20.9/20.12). Il doit indiquer le succès de chaque destinataire.
- Accédez à Configuration > Devices > Control Components (20.9/20.12 : Configuration > Devices > Controllers).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Delete.

Étape 5: Valider les chèques



Remarque : Poursuivez avec la section Post Checks présentée ici, qui est commune à toutes les combinaisons de déploiement.

Combinaison 2 : vManage autonome + DR noeud unique

Instances nécessaires :

- 1 vManage (principal, COMPUTE_AND_DATA)
- 1 vManage (DR en veille, COMPUTE_AND_DATA)
- 1 ou plusieurs vBond

- 1 vSmart ou plus

Étapes:

1. Afficher toutes les instances à l'aide des étapes communes
2. Vérifications préalables
3. Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
4. Configuration DR à noeud unique
5. Sauvegarde/restauration Config-db
6. Valider les chèques

Étape 1: Vérifications préalables

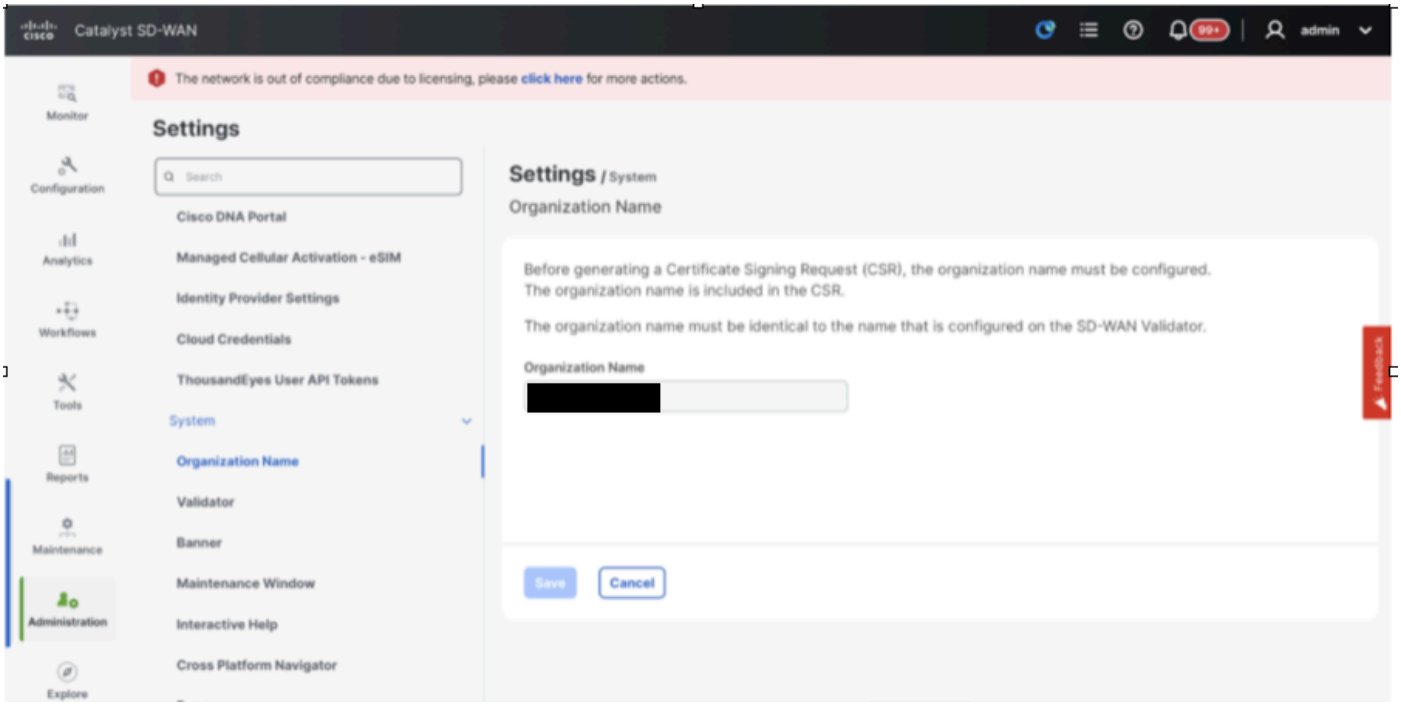
- Assurez-vous que le nombre d'instances Cisco SD-WAN Manager actives est identique au nombre d'instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles exécutent la même version logicielle.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles sont en mesure d'atteindre l'adresse IP de gestion de Cisco SD-WAN Validator.
- Assurez-vous que les certificats ont été installés sur les instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que les horloges sur tous les périphériques Cisco Catalyst SD-WAN, y compris les instances Cisco SD-WAN Manager nouvellement installées, sont synchronisées.
- Assurez-vous qu'un nouvel ensemble d'IP système et d'ID de site est configuré sur les instances de Cisco SD-WAN Manager nouvellement installées, avec la même configuration de base que le cluster actif.

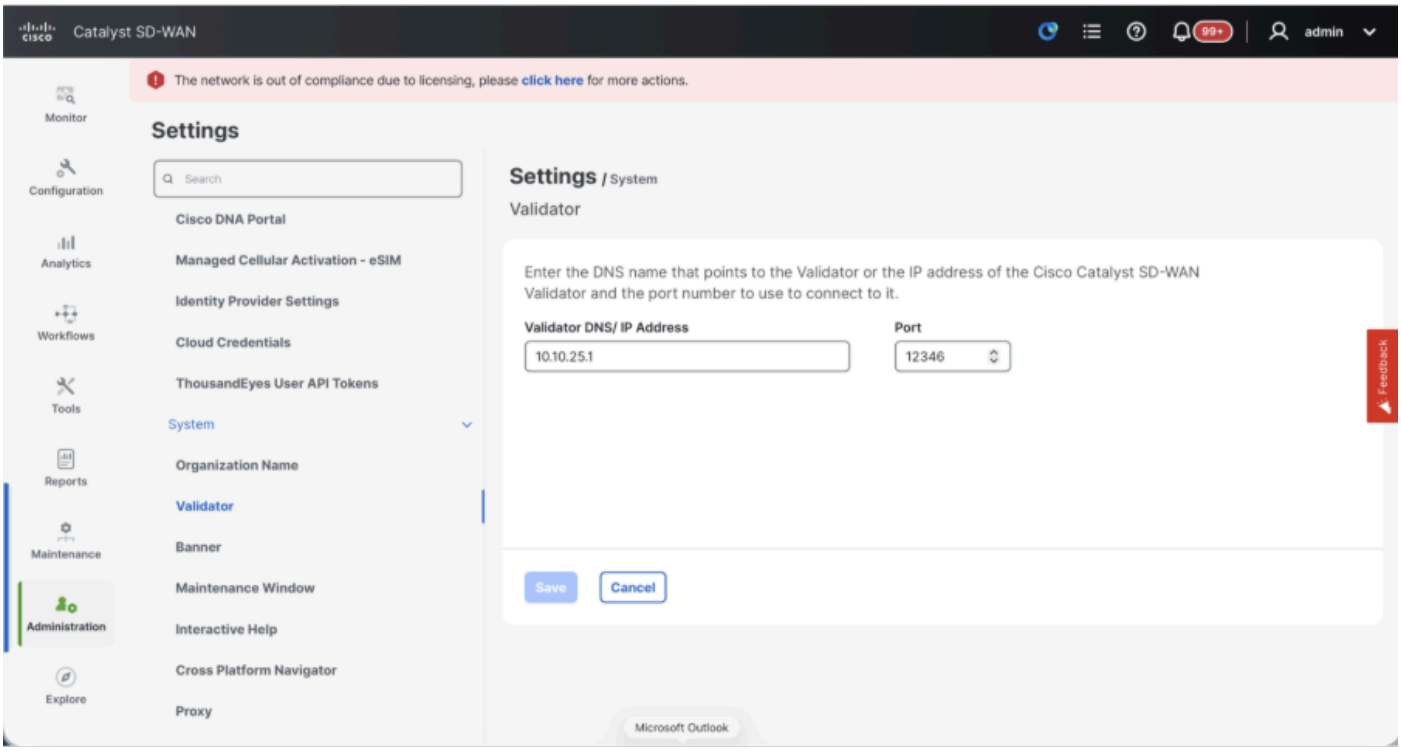
Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

Mettre à jour les configurations sur l'interface utilisateur vManage

- Une fois les configurations de l'étape 1 ajoutées à l'interface de ligne de commande de tous les contrôleurs, nous pouvons accéder à l'interface utilisateur web de vManage, à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.

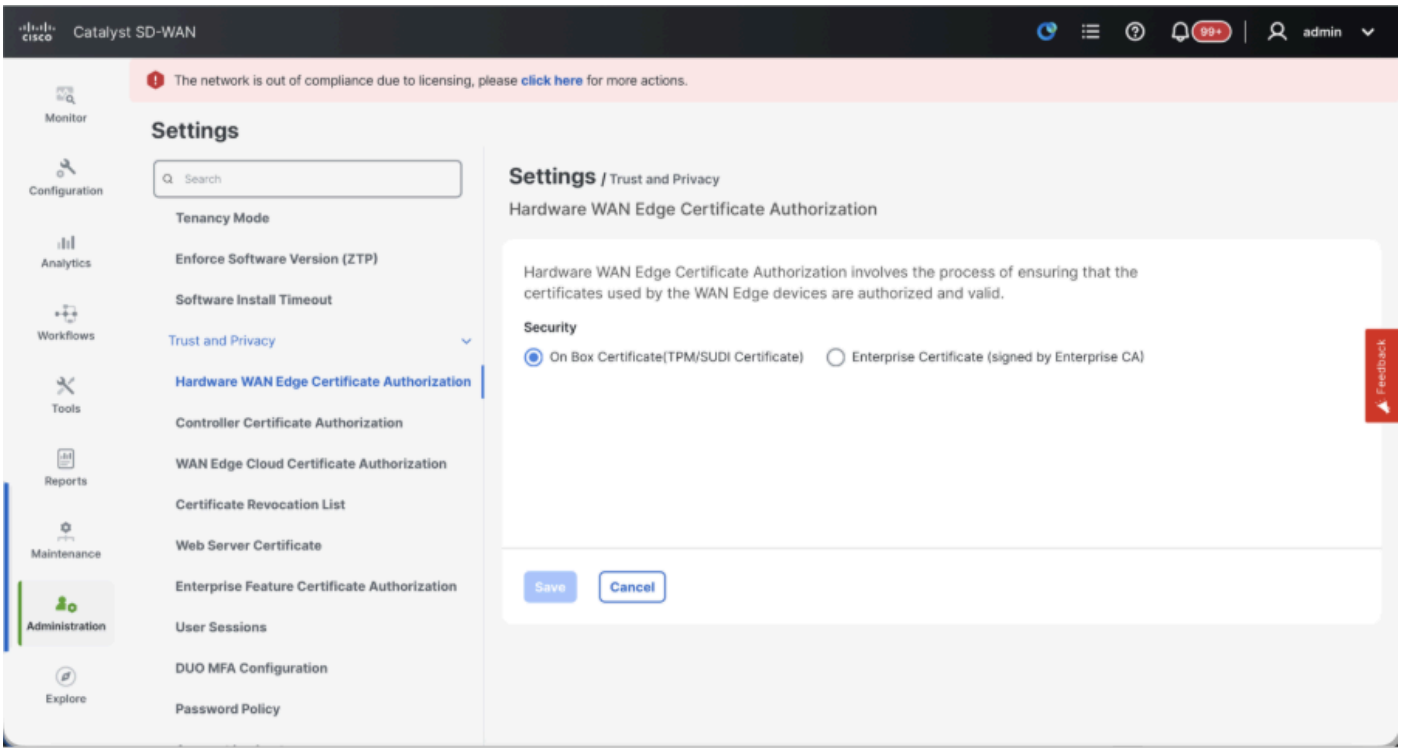
- Accédez à Administration > Settings et complétez ces étapes.
- Configurez le nom de l'organisation et l'adresse URL/IP du validateur/vBond. Configurez la même valeur que dans l'interface de ligne de commande du noeud vManage.
- Dans vManage 20.15/20.18, ces configurations sont disponibles dans la section Système.



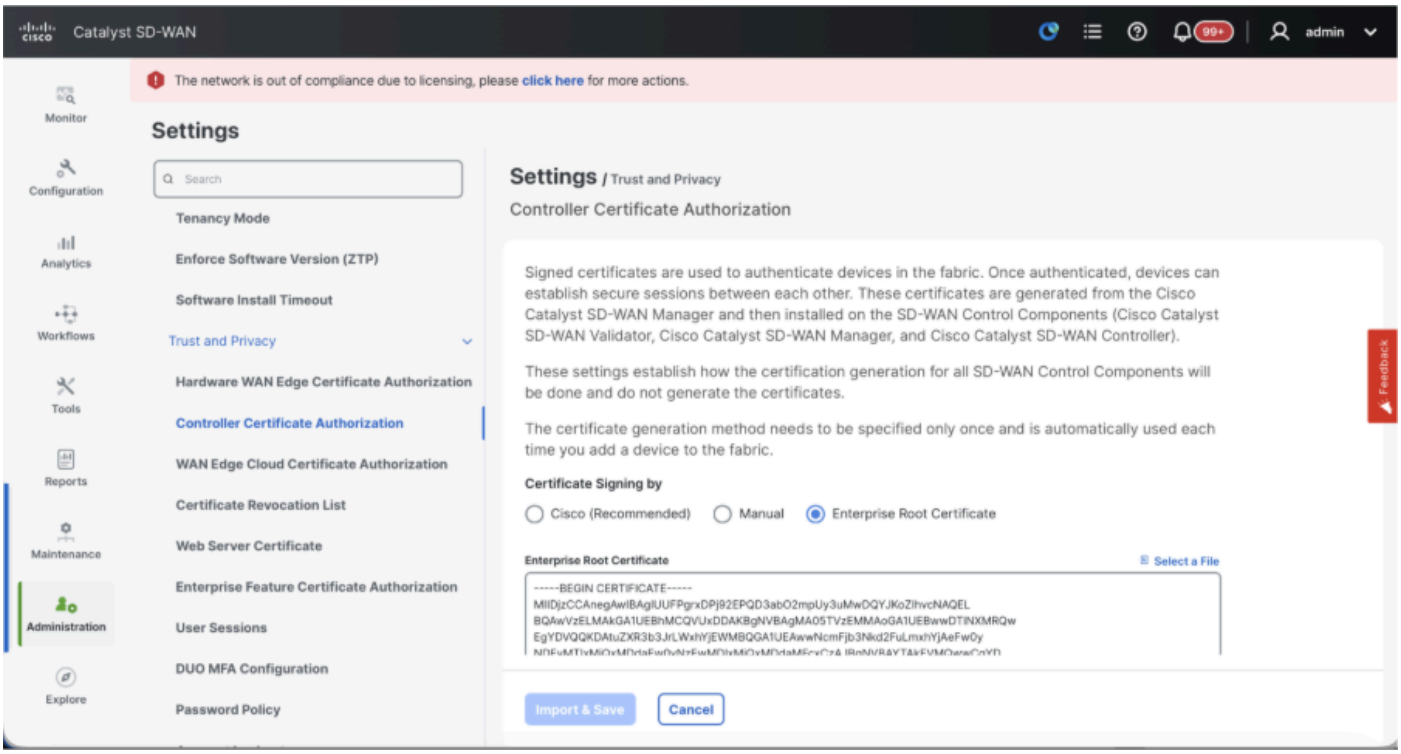


- Vérifiez les configurations de l'autorité de certification (CA), qui décide de l'autorité de certification utilisée pour signer les certificats. Nous pouvons voir 3 options ici :

1. Hardware WAN Edge Certificate Authorization : décide de l'autorité de certification pour les routeurs périphériques SD-WAN matériels.
    - Certificat On Box (certificat TPM/SUDI) : avec cette option, le certificat préinstallé sur le matériel du routeur est utilisé pour établir les connexions de contrôle (connexions TLS/DTLS)
    - Certificat d'entreprise (signé par l'autorité de certification d'entreprise) : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

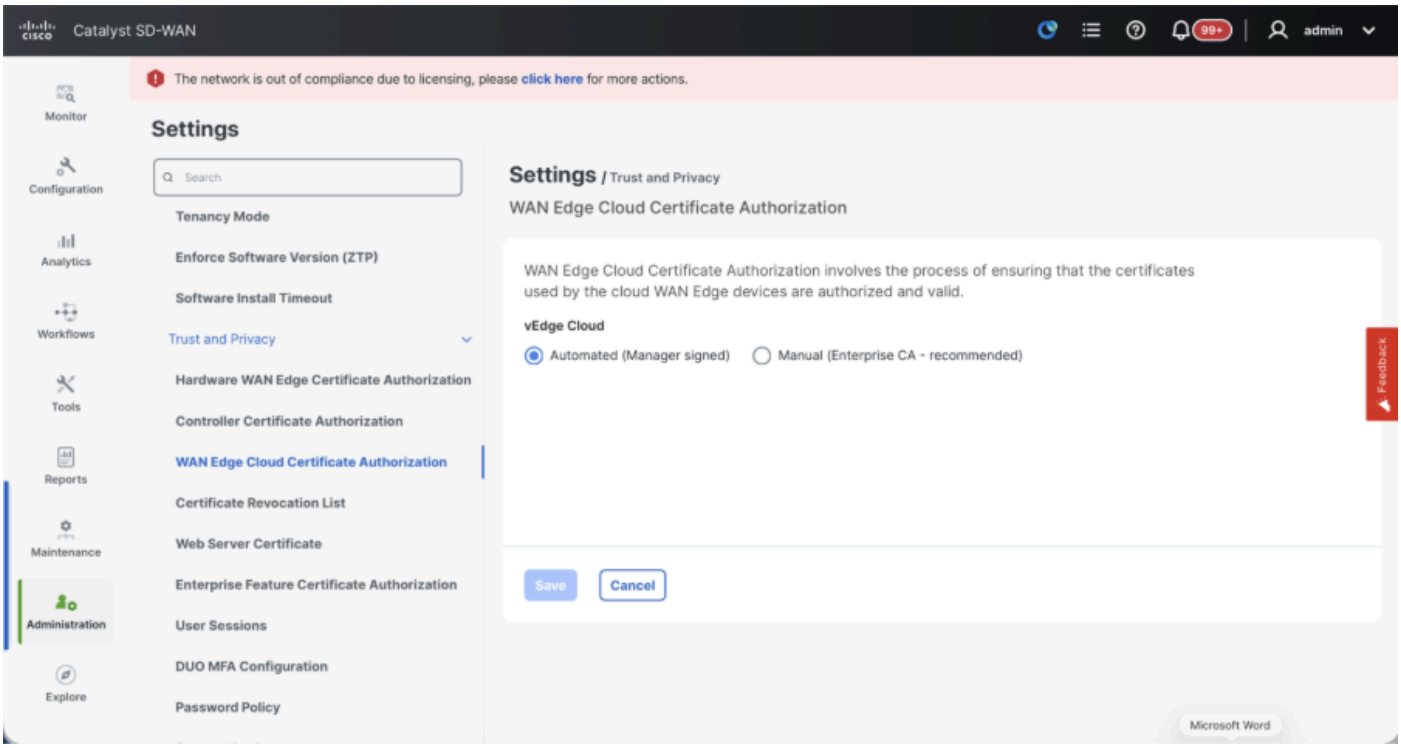


2. Autorisation de certificat de contrôleur - Décide de l'autorité de certification pour les contrôleurs SD-WAN.
    - Cisco (recommandé) : les contrôleurs utilisent les certificats signés par Cisco PKI. vManage contacte automatiquement le portail PNP à l'aide des informations d'identification de compte Smart configurées sur le vManage, obtient le certificat signé et est installé sur le contrôleur.
    - Manuel - Les contrôleurs utilisent les certificats signés par Cisco PKI. Signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
    - Certificat racine d'entreprise : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

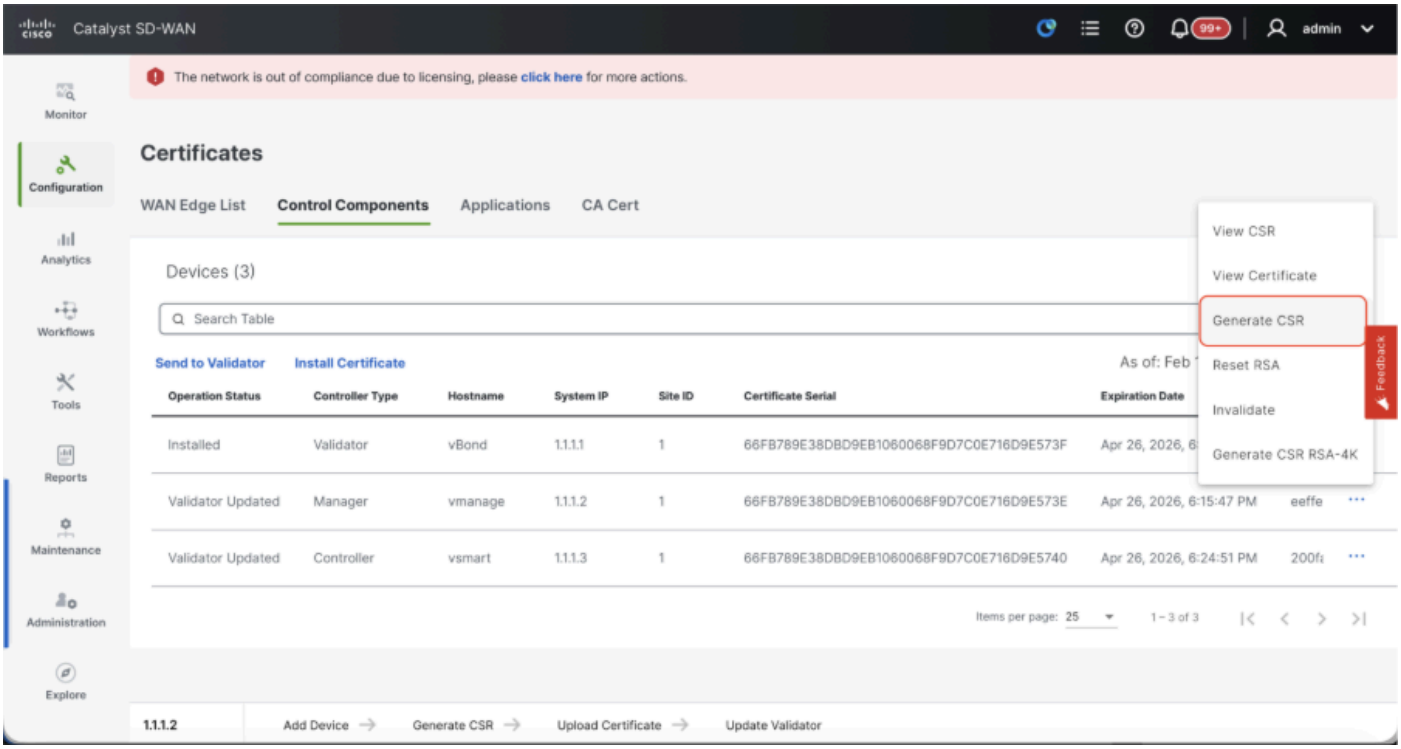


3. WAN Edge Cloud Authorization - Décide de l'autorité de certification pour les routeurs virtuels SD-WAN Edge (CSR1000v, C8000v, cloud vEdge)
    - Automatisé (vManage signed) : vManage signe automatiquement le CSR pour les routeurs de périphérie virtuels et installe le certificat sur le routeur.
    - Manuel (CA d'entreprise - recommandé) - Les routeurs virtuels utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

Dans ce cas, si nous utilisons notre propre autorité de certification, Enterprise certificate authority, sélectionnez Enterprise.



- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers
- Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par

vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.

Intégration de vBond/Validator et vSmart/Controller à vManage

Accédez à Configuration > Devices > Control Components dans le cas des noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

Intégration de vBond/Validator

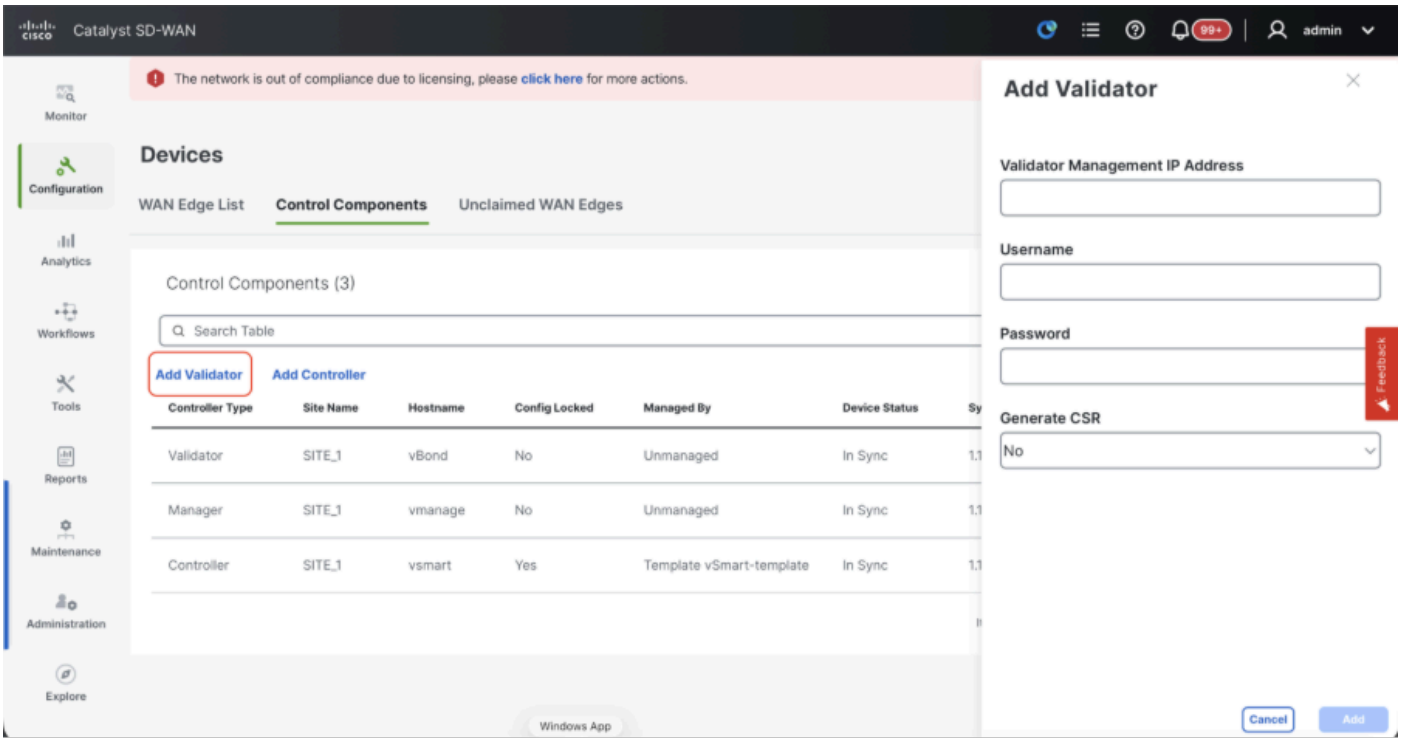
- Cliquez sur Add vBond dans le cas de 20.12 vManage ou sur Add Validator dans le cas de 20.15/20.18 vManage. Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vBond qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée de l'interface CLI de vManage vers vBond IP.
- Entrez les informations d'identification utilisateur de vBond.



Remarque : nous devons utiliser les identifiants d'administration de vBond ou une partie utilisateur du groupe netadmin. Vous pouvez le vérifier dans l'interface de ligne de commande du vBond. Sélectionnez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vBond



Remarque : Si le vBond est derrière un périphérique NAT/pare-feu, vérifiez si l'adresse IP de l'interface VPN 0 de vBond est traduite en une adresse IP publique. Si l'adresse IP de l'interface VPN 0 n'est pas accessible depuis vManage, utilisez l'adresse IP publique de l'interface VPN 0 dans cette étape



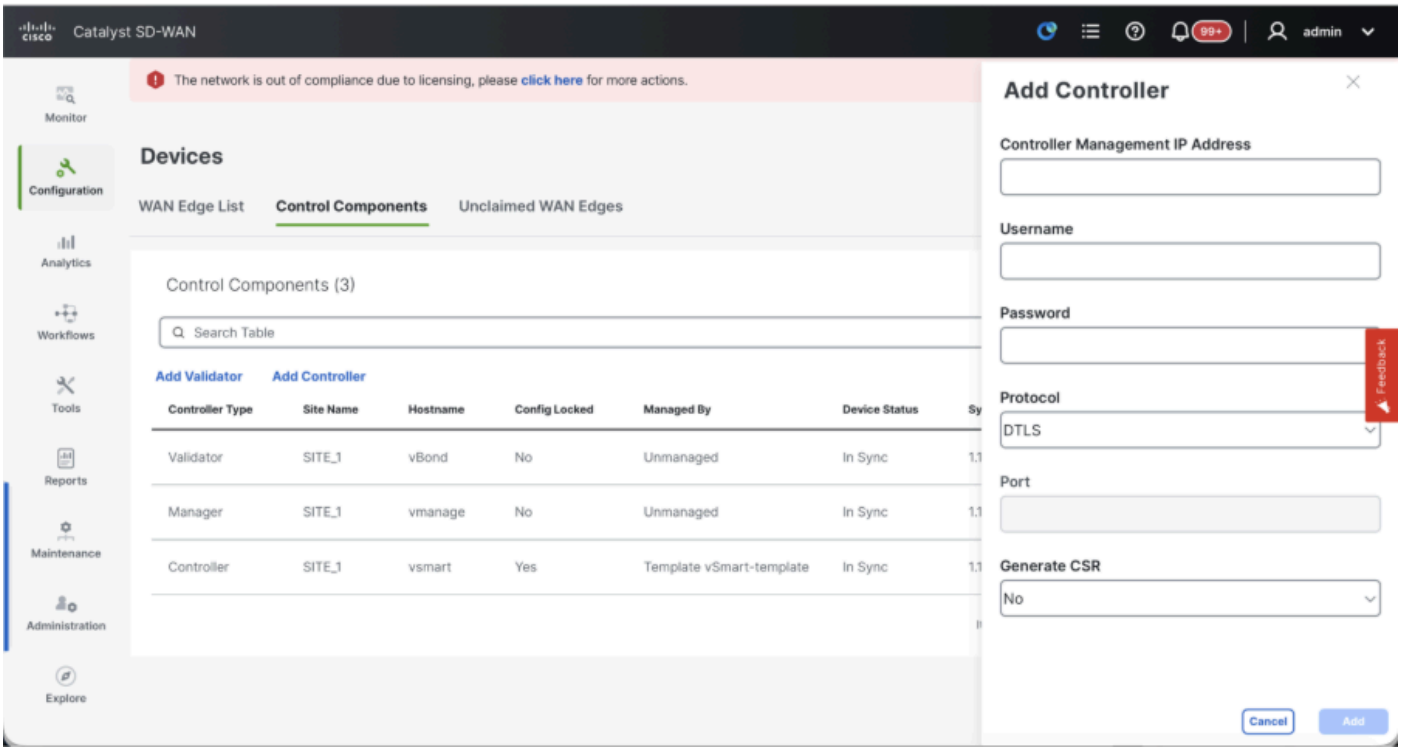
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vBond.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il existe plusieurs vBonds, répétez les mêmes étapes.

Intégration de vSmart/Controller

- Cliquez sur Add vSmart dans le cas de vManage 20.12 ou sur Add Controller dans le cas de vManage 20.15/20.18.
- Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vSmart qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée depuis l'interface CLI de vManage vers vSmart IP.
- Entrez les informations d'identification de l'utilisateur de vSmart. Notez que nous devons utiliser les informations d'identification d'administration de vSmart ou d'une partie utilisateur du groupe netadmin.

- Vous pouvez le vérifier dans l'interface de ligne de commande du vSmart.
- Définissez le protocole sur TLS, si nous avons l'intention d'utiliser TLS pour les routeurs afin d'établir des connexions de contrôle avec vSmart. Cette configuration doit également être configurée sur l'interface de ligne de commande des noeuds vSmarts et vManage.
- Choisissez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vSmart.

Remarque : si le vSmart est derrière le périphérique/pare-feu NAT, vérifiez si l'adresse IP de l'interface VPN 0 vSmart est traduite en une adresse IP publique, et si l'adresse IP de l'interface VPN 0 n'est pas accessible à partir de vManage, utilisez l'adresse IP publique de l'adresse IP de l'interface VPN 0 dans cette étape.



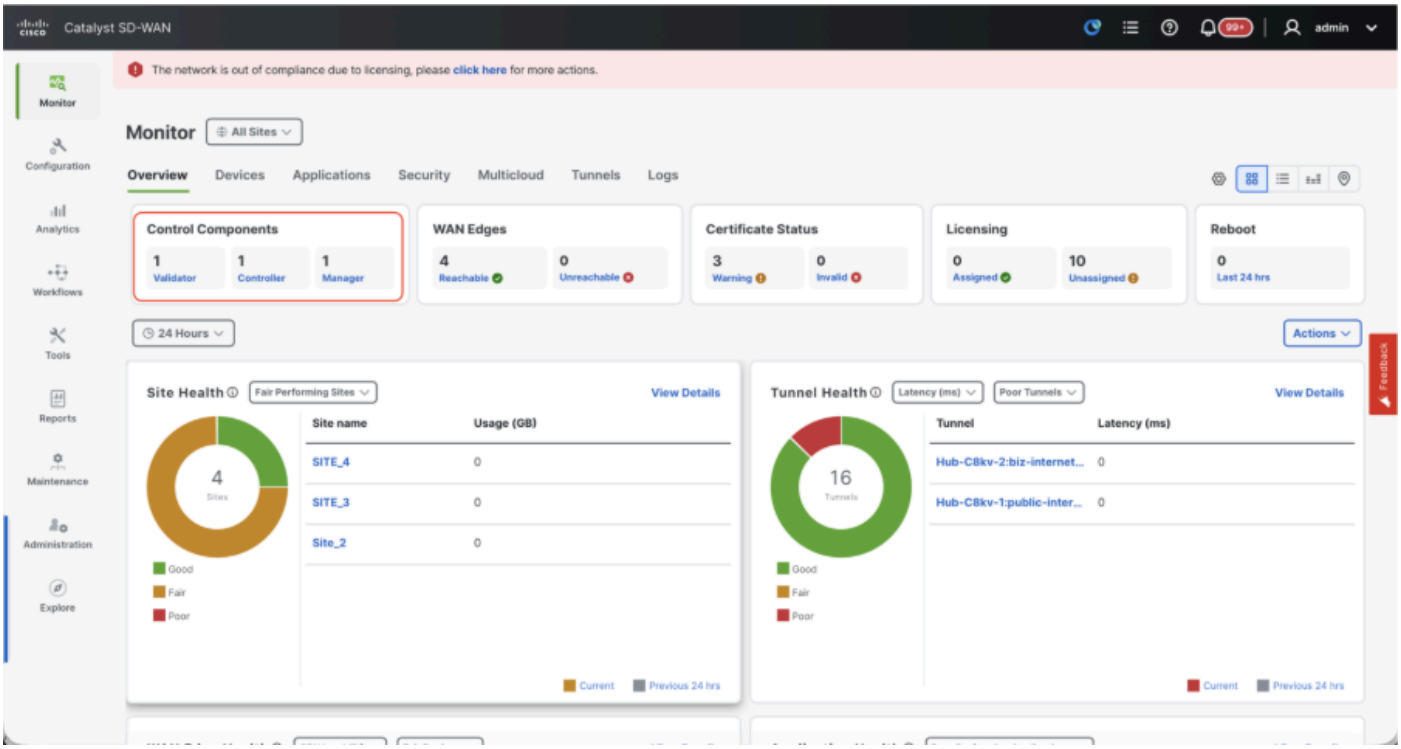
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vSmart.
- Si vous choisissez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en naviguant jusqu'au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. La même procédure s'applique si nous utilisons Digicert et le certificat

racine d'entreprise.

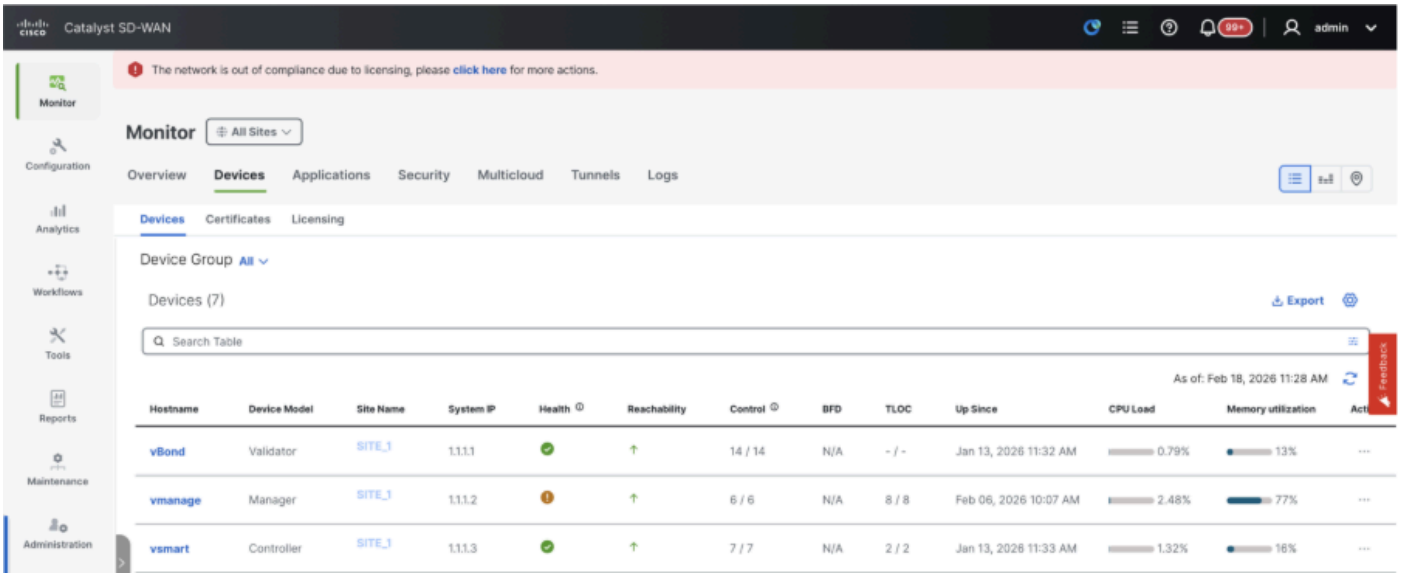
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- S'il y a plusieurs vSmarts, répétez les mêmes étapes.

Vérification

Une fois toutes les étapes terminées, vérifiez que tous les composants de contrôle sont accessibles dans Monitor > Dashboard



- Cliquez sur les composants de contrôle respectifs et vérifiez qu'ils sont tous accessibles.
- Accédez à Monitor > Devices et vérifiez que tous les composants de contrôle sont accessibles.



Étape 3: Sauvegarde/restauration Config-db

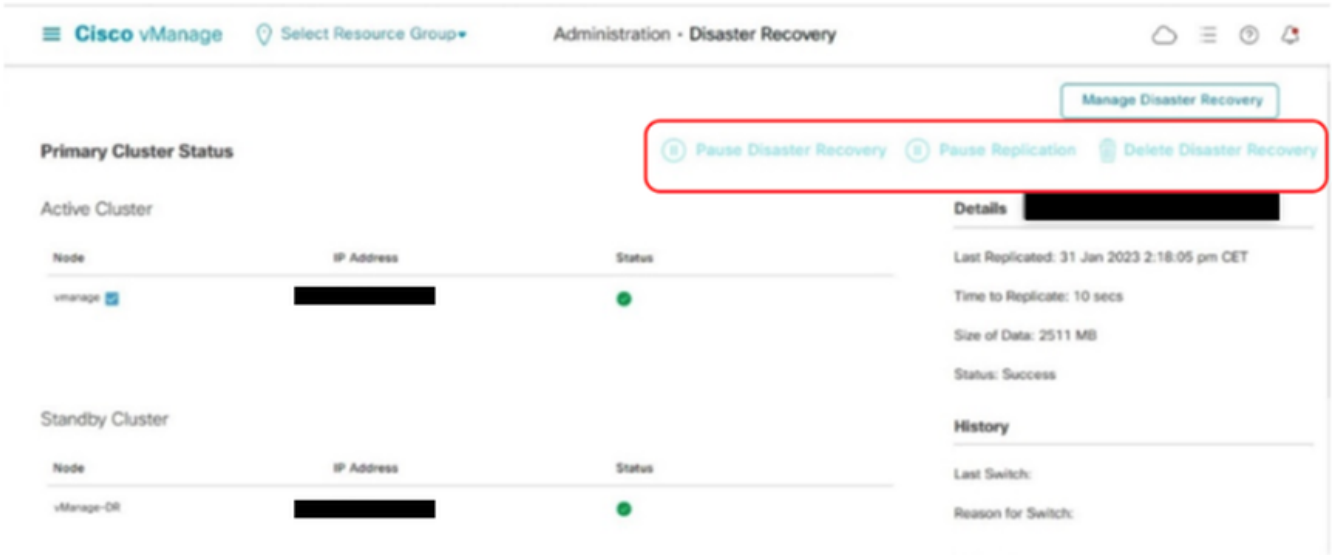
Collecter la sauvegarde et la restauration de la base de données de configuration vManage sur un autre noeud vManage

---

Remarque : Lors de la collecte de la sauvegarde de la base de données de configuration à partir du noeud vManage existant sur lequel la récupération après sinistre est activée, assurez-vous qu'elle est collectée après la suspension et la suppression de la récupération après sinistre sur ce noeud.

Vérifiez qu'aucune réplication de reprise après sinistre n'est en cours. Accédez à Administration > Disaster Recovery et assurez-vous que l'état est Réussite et qu'il n'est pas dans un état transitoire tel que Importation en attente, Exportation en attente ou Téléchargement en attente. Si l'état n'est pas réussi, contactez le TAC Cisco et assurez-vous que la réplication est réussie avant de procéder à la pause de la reprise après sinistre.

Tout d'abord, suspendez la reprise après sinistre et assurez-vous que la tâche est terminée. Supprimez la reprise après sinistre et confirmez que la tâche est terminée.



Contactez le TAC Cisco pour vous assurer que la reprise après sinistre est correctement nettoyée.

Collecter la sauvegarde Configuration-DB :

- Dans le fabric SD-WAN actuellement utilisé, vous pouvez générer une sauvegarde de la base de données de configuration sur les configurations de cluster vManage et vManage autonomes.
- Pour vManage autonome, ce vManage est lui-même le leader de la base de données de configuration.

Vérifiez que la base de données de configuration est en cours d'exécution sur le noeud vManage.

Vous pouvez vérifier la même chose à l'aide de la commande request nms configuration-db status sur l'interface de ligne de commande vManage. Le résultat est le suivant

```
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#
```

Utilisez cette commande pour collecter la sauvegarde configuration-db à partir du noeud vManage de tête de base de données de configuration identifié.

```
request nms configuration-db backup path /opt/data/backup/<filename>
```

Le résultat attendu est le suivant :

```
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#
```

- Notez les informations d'identification de configuration-db si elles ont été mises à jour.
- Si vous ne connaissez pas les informations d'identification de la base de données de configuration, contactez le TAC pour récupérer les informations d'identification de la base de données de configuration à partir des noeuds vManage existants.
- Les informations d'identification configuration-db par défaut sont username : neo4j et password : mot de passe

Restaurer la sauvegarde Configuration-db vers un autre noeud vManage

Copiez la sauvegarde configuration-db dans le répertoire /home/admin/ de vManage à l'aide de SCP.

Exemple de sortie de commande 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
```

Pour restaurer la sauvegarde configuration-db, nous devons d'abord configurer les informations d'identification configuration-db. Si vos identifiants configuration-db sont default(neo4j/password), nous pouvons ignorer cette étape.

Pour configurer les informations d'identification configuration-db, utilisez la commande request nms configuration-db update-admin-user. Utilisez le nom d'utilisateur et le mot de passe de votre choix.

Veuillez noter que le serveur d'applications de vManage est redémarré. En raison de laquelle l'interface utilisateur vManage devient inaccessible pendant une courte période.

```
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#
```

Publication que nous pouvons poursuivre pour restaurer la sauvegarde configuration-db :

Nous pouvons utiliser la commande request nms configuration-db restore path /home/admin/< > pour restaurer la base de données de configuration dans le nouveau 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
```

Une fois la base de données de configuration restaurée, assurez-vous que l'interface utilisateur vManage est accessible. Attendez environ 5 minutes, puis essayez d'accéder à l'interface utilisateur.

Une fois connecté à l'interface utilisateur avec succès, assurez-vous que la liste des routeurs Edge, le modèle, les stratégies et toutes les autres configurations qui étaient présentes sur votre interface utilisateur vManage précédente ou existante sont reflétés sur la nouvelle interface utilisateur vManage.



Mise en garde : La base de données de configuration restaurée contient toujours le ou les gestionnaires SD-WAN à partir desquels la sauvegarde a été effectuée. Elles sont répertoriées en tant qu'entrées Manager dans Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) mais ne sont pas membres de Administration > Cluster Management. Jusqu'à leur suppression à l'étape 5 :

- chaque rapport Send to Validator signale Failed to find Vmanage Cluster node for uuid <uuid> for them, et
- chaque installation de certificat de contrôleur à partir de l'interface utilisateur échoue et est restaurée.

N'effectuez aucune opération de certificat de contrôleur ou d'envoi au validateur sur ce vManage avant la fin de l'étape 5. Si l'installation d'un certificat échoue, n'installez pas le même certificat à partir de l'interface de ligne de commande ; Contactez le centre d’assistance technique Cisco TAC.

Étape 4: Configuration DR à noeud unique

Reportez-vous à l’étape 2: Prévérifications dans la combinaison 2 : vManage autonome + DR noeud unique et assurez-vous que nous avons rempli toutes les conditions requises avant de procéder à l'activation de la récupération après sinistre.

DR à noeud unique

Conditions préalables

- Assurez-vous que le noeud principal et le noeud secondaire sont accessibles par HTTPS sur un VPN de transport (VPN 0).

- Assurez-vous que le noeud principal et le noeud secondaire Cisco vManage exécutent la

même version de Cisco vManage.

Interface de cluster hors bande dans VPN 0

1. Pour chaque instance vManage d'un cluster, une troisième interface (liaison de cluster) est requise en plus des interfaces utilisées pour VPN 0 (transport) et VPN 512 (gestion).
2. Cette interface est utilisée pour la communication et la synchronisation entre les serveurs vManage du cluster.
3. Cette interface doit être d'au moins 1 Gbit/s et avoir une latence de 4 ms ou moins. Une interface 10 Gbit/s est recommandée.
4. Les deux noeuds vManage doivent être en mesure de se joindre via cette interface : qu'il s'agisse d'un segment de couche 2 ou du routage de couche 3.

- Assurez-vous que tous les services (application-server, configuration-db, messaging server, coordination server et statistics-db) sont activés sur les deux noeuds Cisco vManage.
- Distribuez tous les contrôleurs, y compris les orchestrateurs Cisco vBond, dans les data centers principal et secondaire. Assurez-vous que ces contrôleurs sont accessibles par les noeuds Cisco vManage distribués dans ces data centers. Les contrôleurs se connectent uniquement au noeud Cisco vManage principal.
- Assurez-vous qu'aucune autre opération n'est en cours dans le noeud Cisco vManage actif (principal) et en veille (secondaire). Par exemple, assurez-vous qu'aucun serveur n'est en cours de mise à niveau ou qu'aucun modèle n'est en cours d'association à des périphériques.

- Désactivez le serveur proxy HTTP/HTTPS Cisco vManage s'il est activé. Si vous ne désactivez pas le serveur proxy, Cisco vManage tente d'établir une communication de reprise après sinistre via l'adresse IP proxy, même si les adresses IP de cluster hors bande Cisco vManage sont directement accessibles. Vous pouvez réactiver le serveur proxy HTTP/HTTPS Cisco vManage une fois l'enregistrement de la reprise après sinistre terminé.

- Avant de commencer le processus d'enregistrement de reprise après sinistre, accédez à la fenêtre Outils → Redécouvrir le réseau sur le noeud principal Cisco vManage et retrouvez les orchestrateurs Cisco vBond.

Configuration

Configurez les configurations CLI de tous les noeuds vManage qui agissent en tant que noeuds de reprise après sinistre

La configuration minimale pour vManage avant l'enregistrement de la reprise après sinistre est comme indiqué

```
config t
system
 host-name             <hostname>
 system-ip             <unique system-ip>
 site-id               <site-id>
 organization-name     <organization name>
 vbond <IP address/URL of vBond>
commit
```



Remarque : si nous utilisons une URL comme adresse vBond, assurez-vous de configurer les adresses IP du serveur DNS dans la configuration VPN 0 ou assurez-vous qu'elles peuvent être résolues.

Ces configurations sont nécessaires pour activer l'interface de transport utilisée pour établir des connexions de contrôle avec les routeurs et le reste des contrôleurs

```
config t
vpn 0
 dns <IP-address> primary
 dns <IP-address> secondary
 interface eth1
  ip address <IP-address/mask>
  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 <default-gateway IP>
commit
```

Configurez également l'interface de gestion du VPN 512 pour activer l'accès de gestion hors bande au contrôleur.

```
Conf t
```

```
vpn 512
 interface eth0
  ip address <IP-address/mask>
  no shutdown
 !
 ip route 0.0.0.0/0 <default-gateway IP>
!
commit
```

Configurer l'interface de service sur le routeur désigné vManage

Configurez l'interface de service sur le noeud vManage. Cette interface est utilisée pour la communication DR,

```
conf t
 interface eth2
  ip address <IP-address/mask>
  no shutdown
commit
```

Assurez-vous que le même sous-réseau IP est utilisé pour l'interface de service sur le vManage principal et le DR vManage

Mettre à jour les configurations sur l'interface utilisateur vManage

- Une fois les configurations ajoutées à l'interface de ligne de commande de tous les contrôleurs, nous pouvons accéder à l'interface utilisateur web de vManage, en utilisant l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Administration > Settings et complétez ces étapes.
- Configurez le nom de l'organisation. Configurez la même valeur que dans l'interface de ligne de commande du noeud vManage.
- Dans vManage 20.15/20.18, ces configurations sont disponibles dans la section Système.

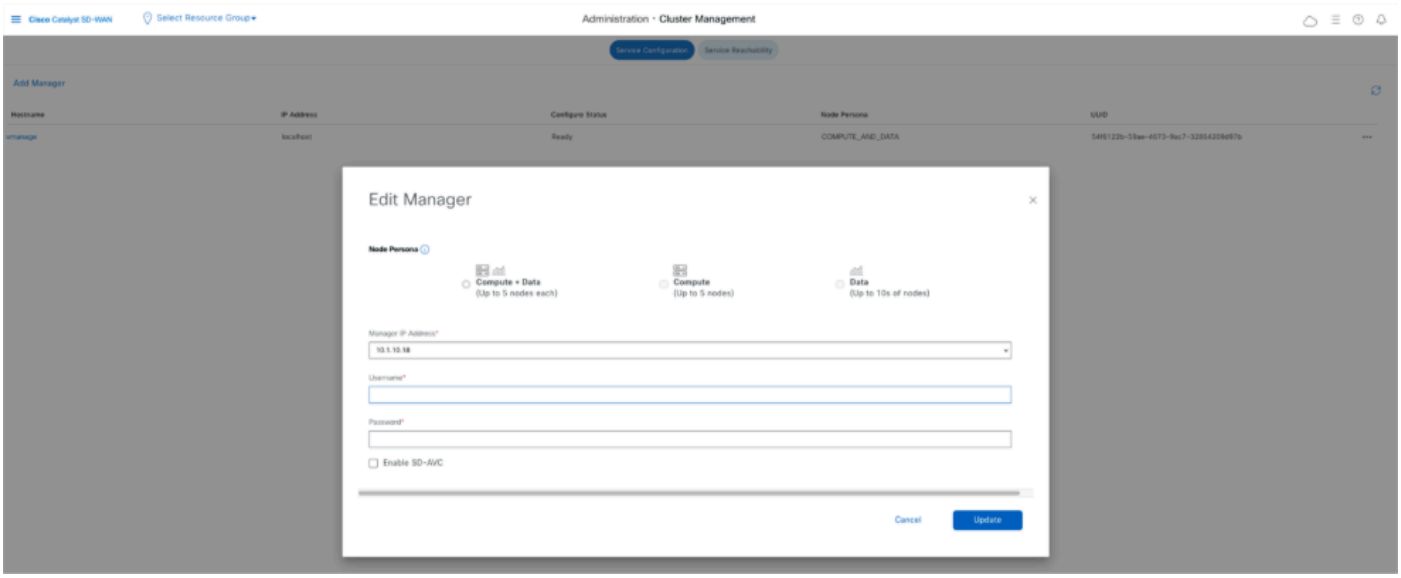
Installation du certificat sur DR vManage

Suivez les étapes décrites à la section Combinaison 2 : vManage autonome + DR noeud unique Étape 2 : Configurez l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

pour installer le certificat sur le vManage Reprise après sinistre.

Ajout de la configuration de reprise après sinistre

- Pour cela, accédez au vManage principal.
- Accédez à Administration → Cluster Management et indiquez l'adresse IP de l'interface hors bande après avoir cliqué sur les trois points à droite de l'entrée vManage et incluez le nom d'utilisateur et le mot de passe. Il est recommandé de créer un utilisateur local distinct, par exemple dradmin, à la fois sur le serveur principal et sur le routeur désigné vmanage pour cette configuration.



- VManage redémarre après cette modification.
- Une fois que le vManage principal est activé, accédez à Administration → Disaster Recovery. Cliquez sur « Gérer la reprise après sinistre ».
- Dans la fenêtre contextuelle, renseignez les détails de vManage principal et secondaire.
- Les adresses IP à indiquer sont les adresses IP des interfaces de cluster hors bande (eth2).
- Les informations d'identification doivent être celles d'un utilisateur netadmin (dradmin) et ne doivent pas être modifiées une fois le DR configuré. Une information d'identification d'utilisateur local vManage distincte pour la récupération après sinistre peut être utilisée. Nous devons nous assurer que l'utilisateur local vManage fait partie du groupe netadmin. Même les identifiants d'administrateur peuvent être utilisés ici.

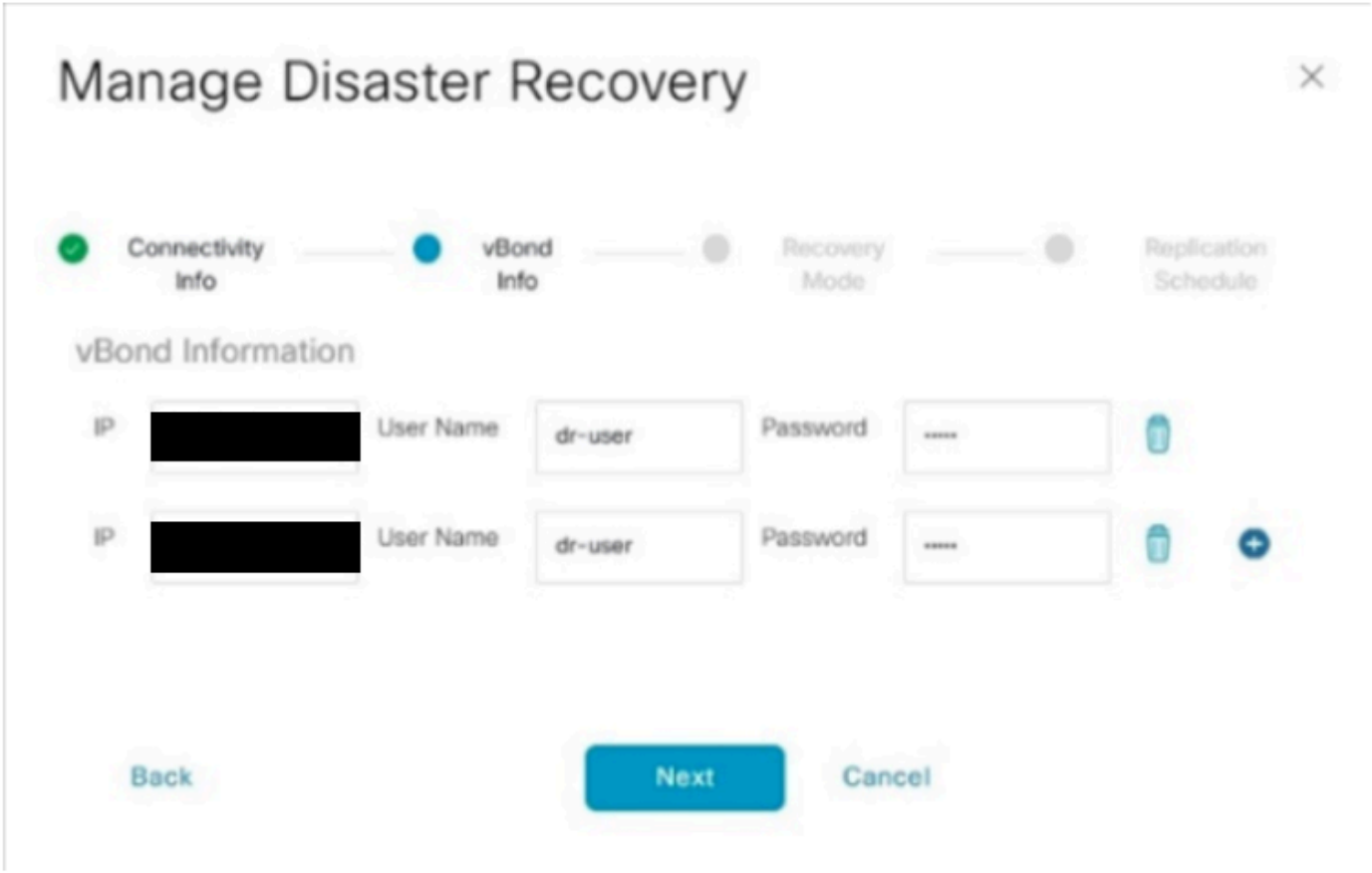
- Une fois rempli, cliquez sur « Suivant ».

- Renseignez les détails des contrôleurs vBond.

- Les contrôleurs vBond doivent être accessibles dans l'adresse IP spécifiée via Netconf.

- Les informations d'identification doivent être celles d'un utilisateur netadmin (dradmin) et ne doivent pas être modifiées une fois le DR configuré.

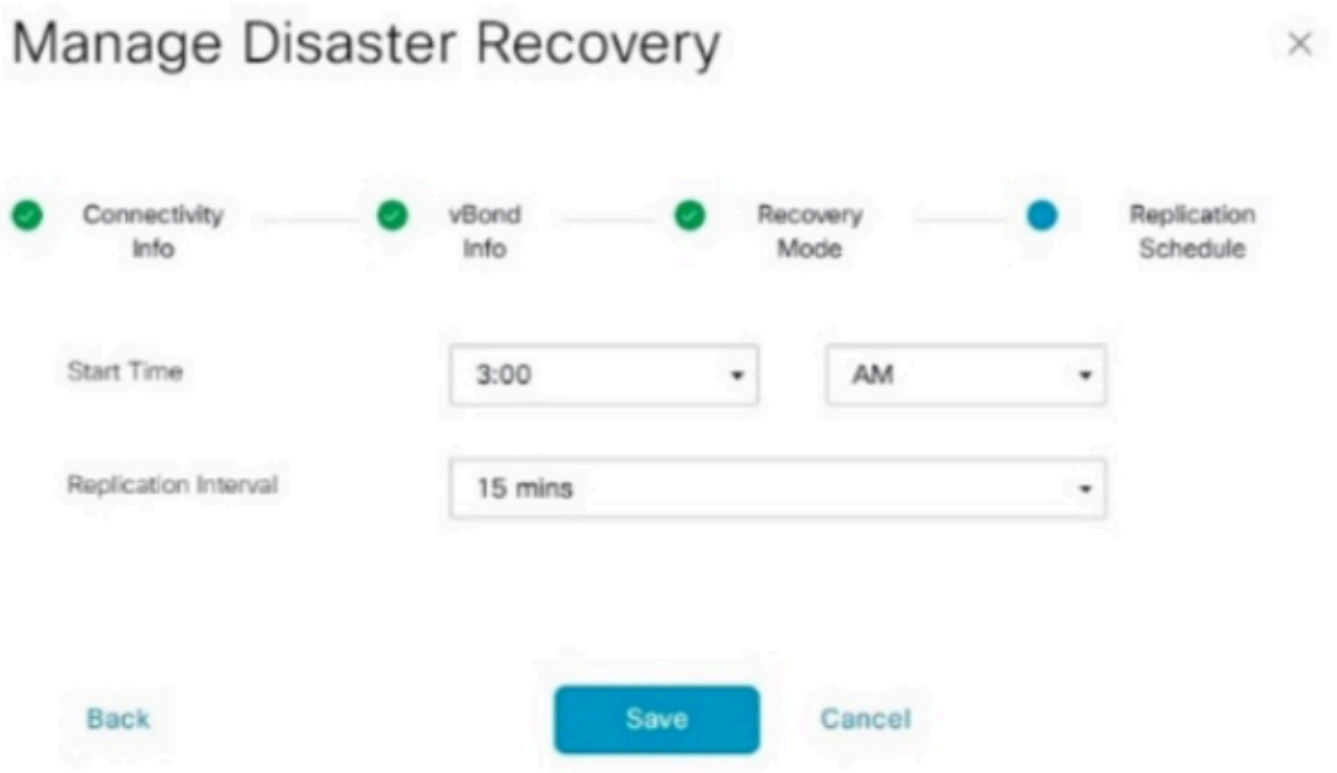
- Pour cela, il est recommandé que vBond ait cet utilisateur dradmin configuré localement ou vous pouvez utiliser l'utilisateur admin pour ajouter le vBond.



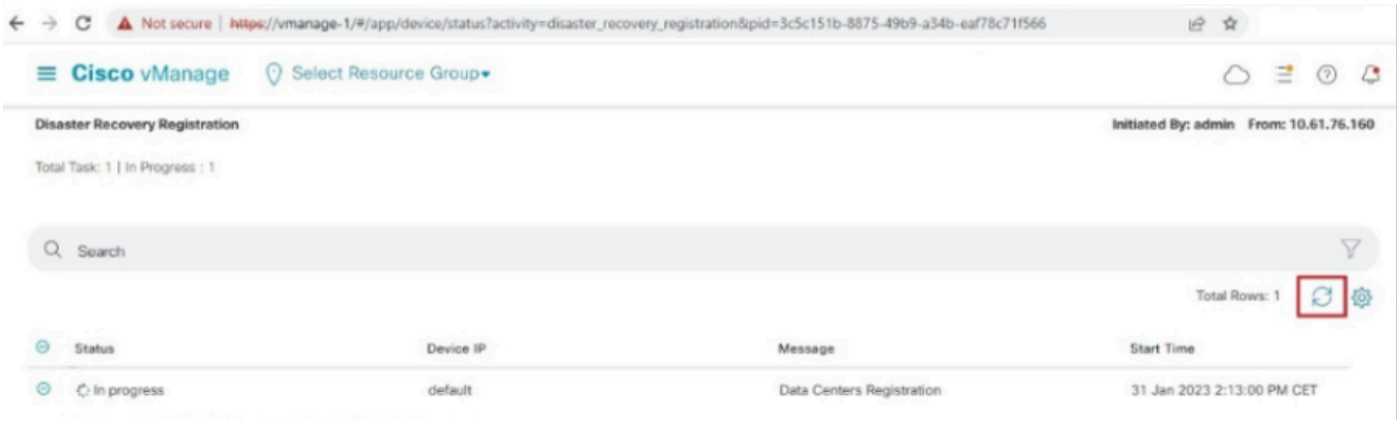
- Une fois rempli, cliquez sur « Suivant ».
- Dans le mode de récupération, choisissez « Manual ». Cliquez sur « Next ».



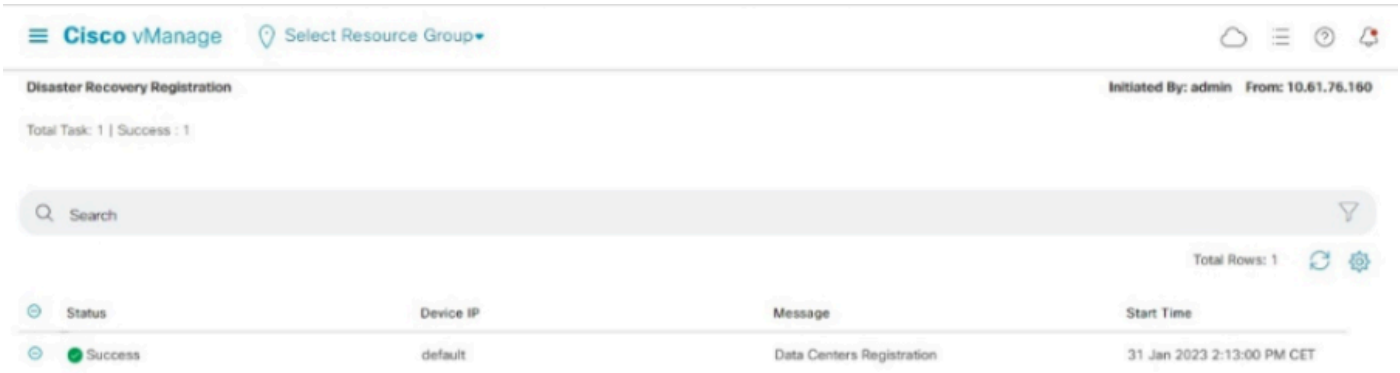
Dans la planification de réplication, définissez l'« Intervalle de réplication ». À chaque intervalle de réplication, les données sont répliquées de vManage principal vers vManage secondaire. La valeur minimale configurable est de 15 minutes.



- Définissez la valeur et cliquez sur « Enregistrer ».
- L'enregistrement du DR commence maintenant. Cliquez sur le bouton Actualiser pour actualiser manuellement l'état et les journaux de progression. Ce processus peut prendre de 20 à 30 minutes.

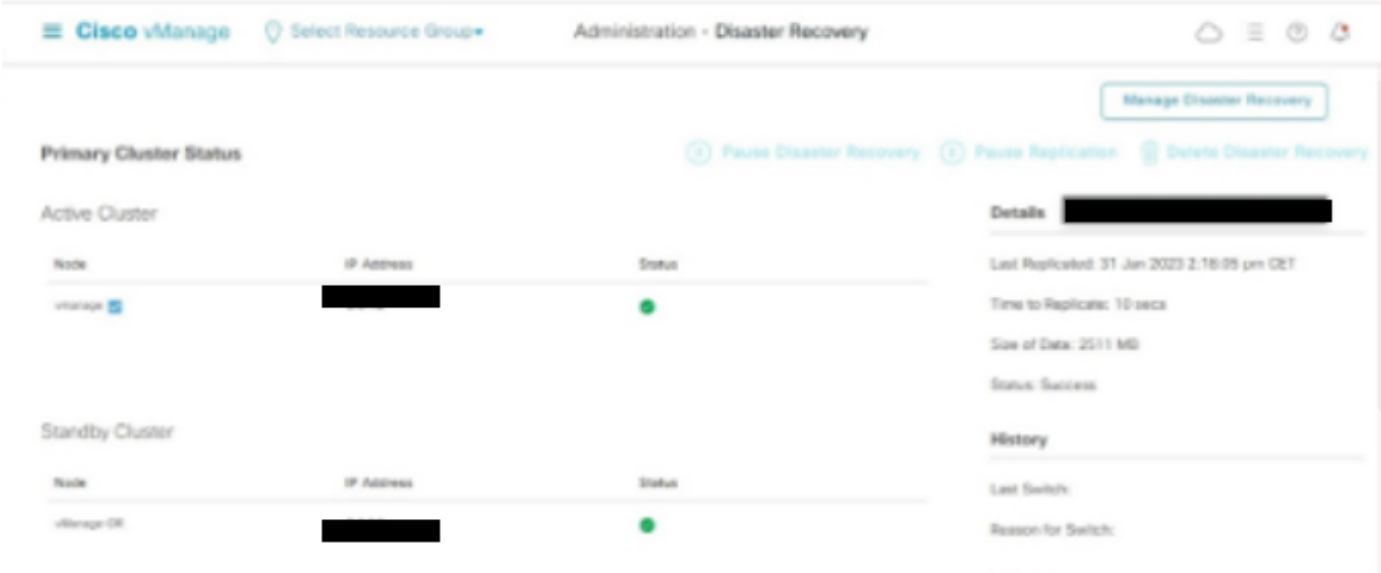


- Notez que l'interface graphique utilisateur vManage est redémarrée au cours de ce processus.
- Une fois terminé, l'état Succès doit être affiché.



Vérifier

Accédez à Administration → Disaster Recovery pour voir l'état de la reprise après sinistre et quand les données ont été répliquées la dernière fois.



Étape 5: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

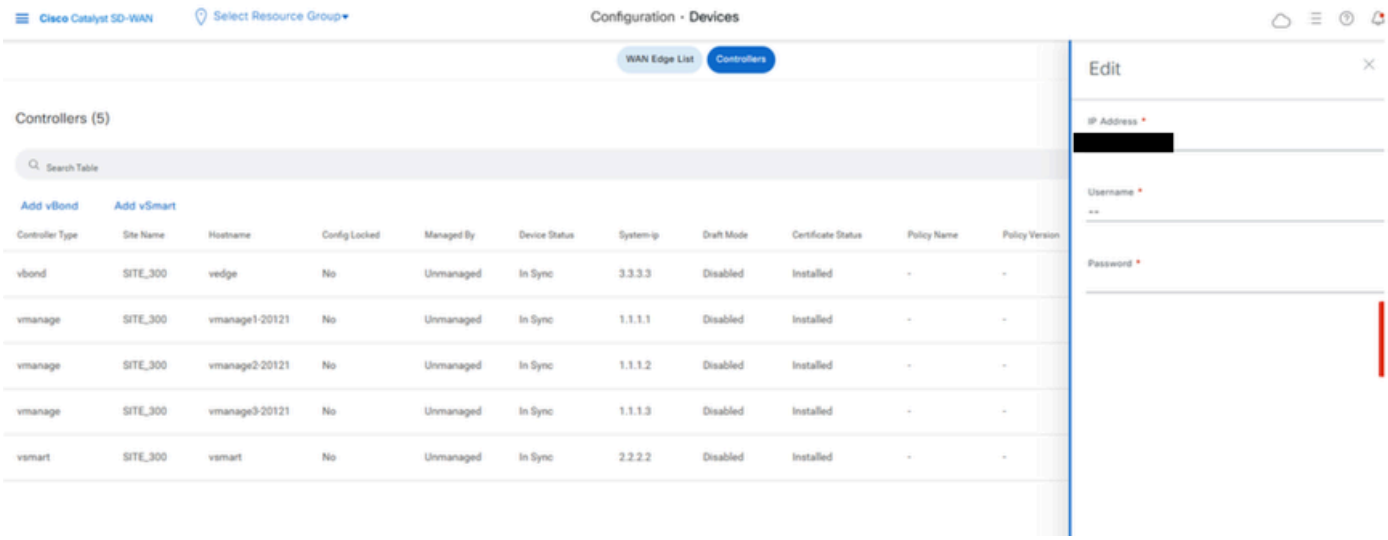
Une fois la base de données de configuration restaurée, nous devons réauthentifier tous les nouveaux contrôleurs (vmanage/vsmart/vbond) dans le fabric

---

Remarque : en production réelle, si l'interface IP utilisée pour la ré-authentification est l'interface IP du tunnel, vous devez vous assurer que le service NETCONF est autorisé sur l'interface du tunnel de vManage, vSmart et vBond, ainsi que sur les pare-feu le long du chemin. Le port de pare-feu à ouvrir est le port TCP 830 en tant que règle bidirectionnelle du cluster DR vers tous les vBonds et vSmarts .

Sur l'interface utilisateur vmanage, cliquez sur Configuration > Devices > Controllers

- Cliquez sur les trois points situés près de chaque contrôleur, puis cliquez sur Edit



- Remplacez l'adresse IP (ip système du contrôleur) par l'adresse IP du vpn de transport 0 (interface de tunnel). Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur save (enregistrer)
- Procédez de la même manière pour tous les nouveaux contrôleurs du fabric

Synchroniser la chaîne de certificats racine

Une fois tous les contrôleurs intégrés, procédez comme suit :

Sur tout serveur Cisco SD-WAN Manager du cluster nouvellement actif, effectuez les actions suivantes :

Entrez cette commande pour synchroniser le certificat racine avec tous les périphériques Cisco Catalyst SD-WAN dans le nouveau cluster actif :

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

Entrez cette commande pour synchroniser l'UUID du gestionnaire Cisco SD-WAN avec le validateur Cisco SD-WAN :

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

Supprimer les entrées précédentes du gestionnaire SD-WAN

Effectuez cette opération juste après la synchronisation root-cert-chain et avant toute opération de certificat de contrôleur ou Envoyer au validateur.

1. Ouvrez Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) et Administration > Cluster Management. Chaque entrée vManage qui n'est pas cette entrée vManage est une entrée SD-WAN Manager précédente et doit être supprimée. N'invalidez pas le vManage Reprise après sinistre affiché dans Administration > Reprise après sinistre. Seules les entrées vManage de la source de la sauvegarde configuration-db sont supprimées ici.
2. Avant toute action Envoyer au validateur ou Invalider, recherchez un enregistrement de numéro de série en conflit. Accédez à https://<vmanage-url>/dataservice/certificate/vsmart/list. Aucune entrée ne peut avoir un ancien numéro de série dont le numéro de série est égal à son propre numéro de série. Cette vérification est en lecture seule. Si une telle entrée existe, arrêtez-vous et contactez le TAC Cisco : any Send to Validator or Invalidate envoie la liste des contrôleurs et ce contrôleur perdrait ses connexions de contrôle.
3. Accédez à Monitor > Tasks et ouvrez la dernière tâche Push vSmart List. Examiner uniquement les résultats des tâches existantes ; ne cliquez pas ici sur Envoyer au validateur. Si aucune tâche récente n'est répertoriée, attendez la diffusion de la liste en début d'heure suivante. Chaque entrée précédente du gestionnaire SD-WAN doit indiquer Failed to find Vmanage Cluster node for uuid <uuid>. Si un uuid vManage a été envoyé avec succès, il s'agit d'un uuid vManage actif : ne l'invalidez pas.
4. Cliquez sur les trois points à droite de la première entrée précédente du gestionnaire SD-WAN, puis cliquez sur Invalidate. Attendez la fin de la tâche. Le résultat attendu est Success with warning, avec cet exercice :

```
Invalidating Root Certificate Autority of vManage-<uuid>
Sending serial number of vManage-<uuid> as invalid to all controllers
Failed to push serial list to vManage-<uuid> - retry in 30 seconds; Failed to find Vmanage Cluster node
Updated serial list will be sent to vManage-<uuid> when it is reachable
Clearing certificate on vManage-<uuid>
Successfully invalidated vManage-<uuid>
```

L'entrée affiche désormais No certificate installed. Le numéro de série précédent du gestionnaire SD-WAN et l'autorité de certification racine sont supprimés des validateurs.

5. Cliquez sur les trois points de la même entrée, puis cliquez à nouveau sur Invalider. Il se termine immédiatement, sans tâche, et l'entrée est supprimée.
6. Répétez les étapes 4 et 5 pour chaque entrée précédente du gestionnaire SD-WAN.
7. Cliquez sur Envoyer au validateur. Le résultat attendu est Success pour chaque destinataire dans quelques secondes, avec no Failed to find Vmanage Cluster node.

Invalider les anciens contrôleurs

Une fois que le fabric est restauré et que les sessions de contrôle et BFD sont actives pour tous les bords et contrôleurs du fabric, invalidez les anciennes entrées vBond/Validator et

vSmart/Controller de l'interface utilisateur :

- Sur l'interface utilisateur de vManage, accédez à Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificats > Contrôleurs).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Invalidate.
- Cliquez sur Send to Validator (Send to vBond in 20.9/20.12). Il doit indiquer le succès de chaque destinataire.
- Accédez à Configuration > Devices > Control Components (20.9/20.12 : Configuration > Devices > Controllers).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Delete.

Étape 6: Valider les chèques



Remarque : Poursuivez avec la section Post Checks présentée ici, qui est commune à toutes les combinaisons de déploiement.

Combinaison 3 : Cluster vManage + aucun DR

Instances nécessaires :

- 3 vManage (cluster à 3 noeuds, tous COMPUTE_AND_DATA) ou 6 vManage (3 COMPUTE_AND_DATA + 3 DATA)
- 1 ou plusieurs vBond
- 1 vSmart ou plus

Étapes:

1. Afficher toutes les instances à l'aide des étapes communes
2. Vérifications préalables
3. Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
4. Créer un cluster vManage
5. Sauvegarde/restauration Config-db
6. Valider les chèques

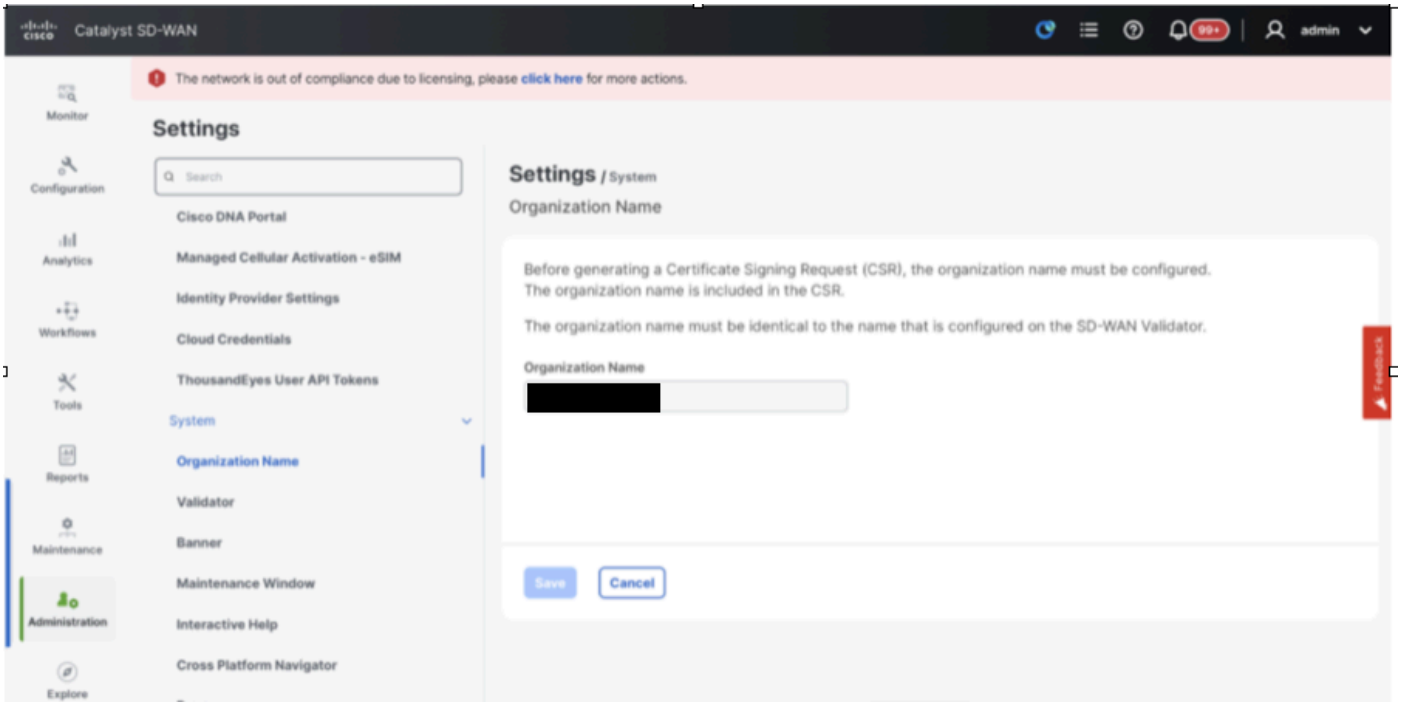
Étape 1: Vérifications préalables

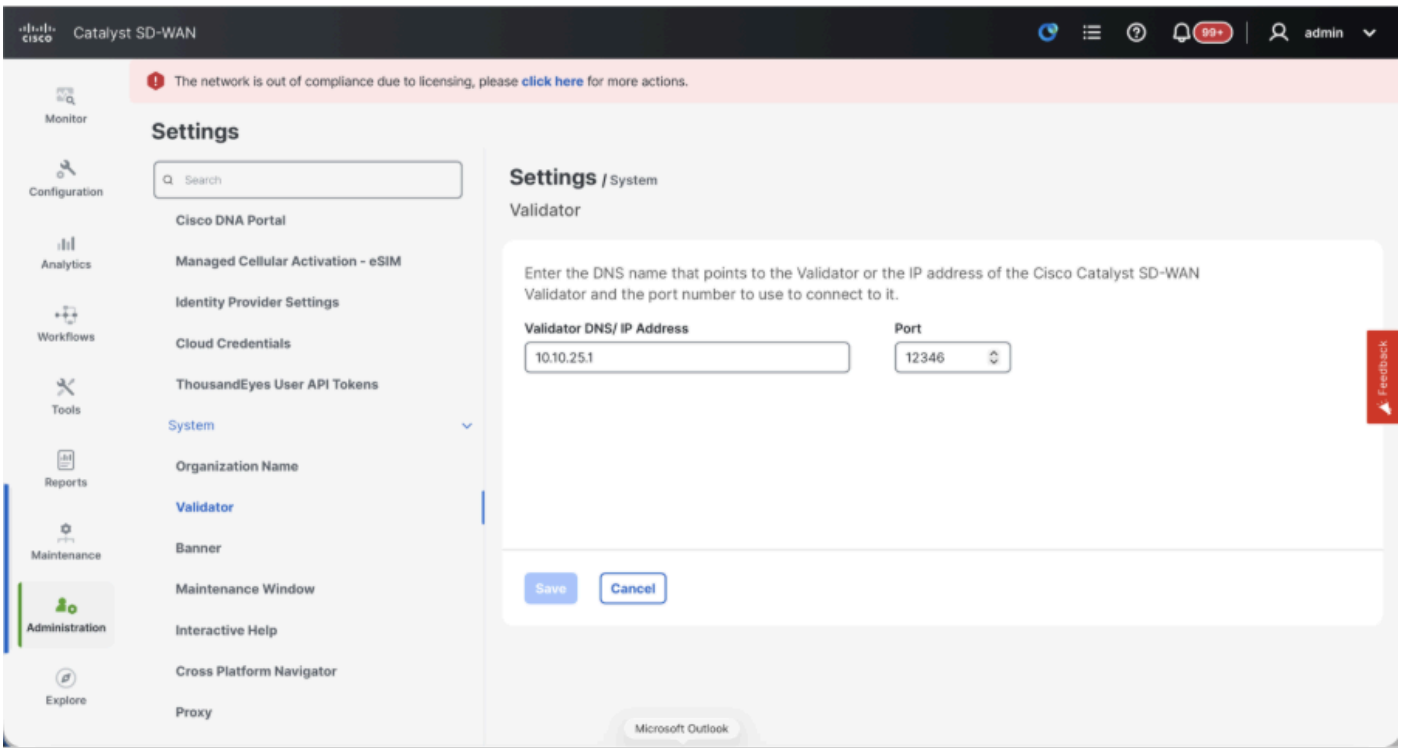
- Assurez-vous que le nombre d'instances Cisco SD-WAN Manager actives est identique au nombre d'instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles exécutent la même version logicielle.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles sont en mesure d'atteindre l'adresse IP de gestion de Cisco SD-WAN Validator.
- Assurez-vous que les certificats ont été installés sur les instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que les horloges sur tous les périphériques Cisco Catalyst SD-WAN, y compris les instances Cisco SD-WAN Manager nouvellement installées, sont synchronisées.
- Assurez-vous qu'un nouvel ensemble d'IP système et d'ID de site est configuré sur les instances de Cisco SD-WAN Manager nouvellement installées, avec la même configuration de base que le cluster actif.

Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

Mettre à jour les configurations sur l'interface utilisateur vManage

- Une fois les configurations de l'étape 1 ajoutées à l'interface de ligne de commande de tous les contrôleurs, nous pouvons accéder à l'interface utilisateur web de vManage, à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Administration > Settings et complétez ces étapes.
- Configurez le nom de l'organisation et l'adresse URL/IP du validateur/vBond. Configurez la même valeur que dans l'interface de ligne de commande du noeud vManage.
- Dans vManage 20.15/20.18, ces configurations sont disponibles dans la section Système.

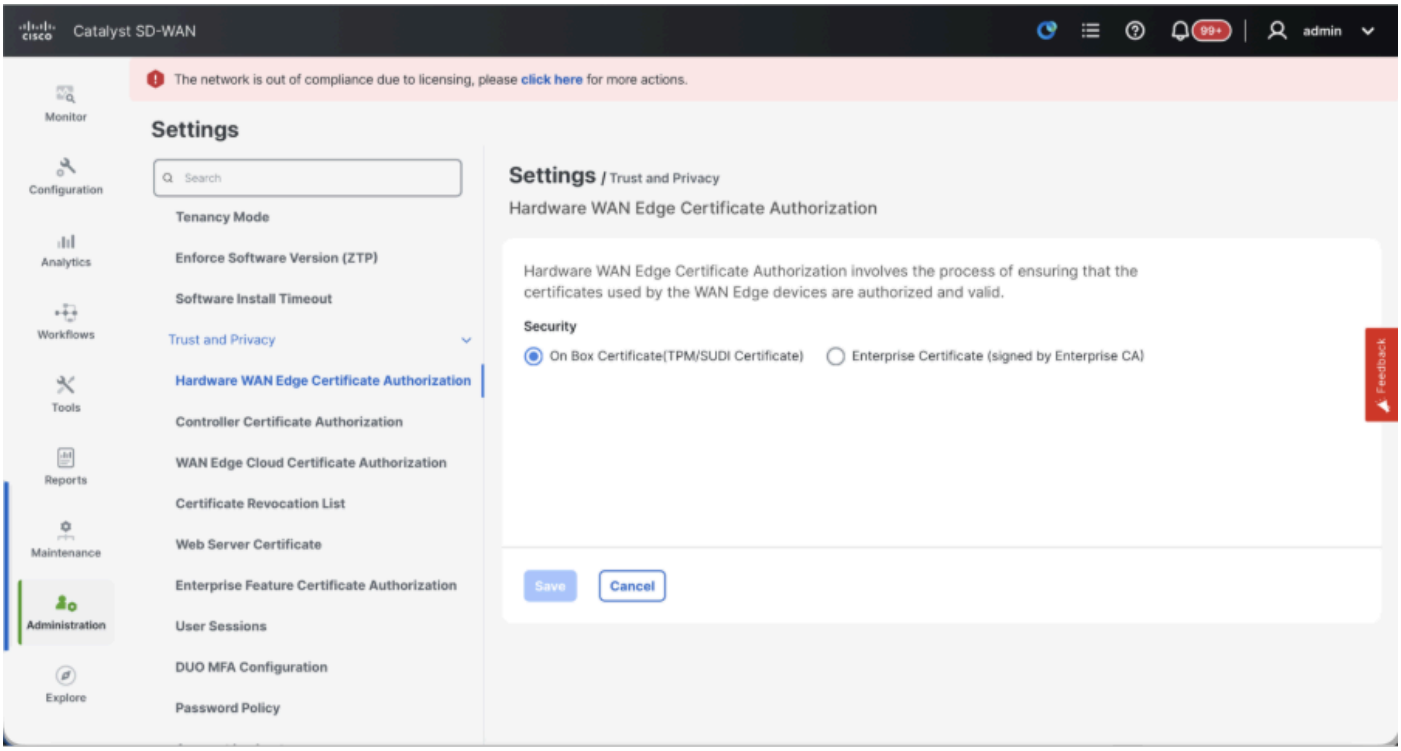




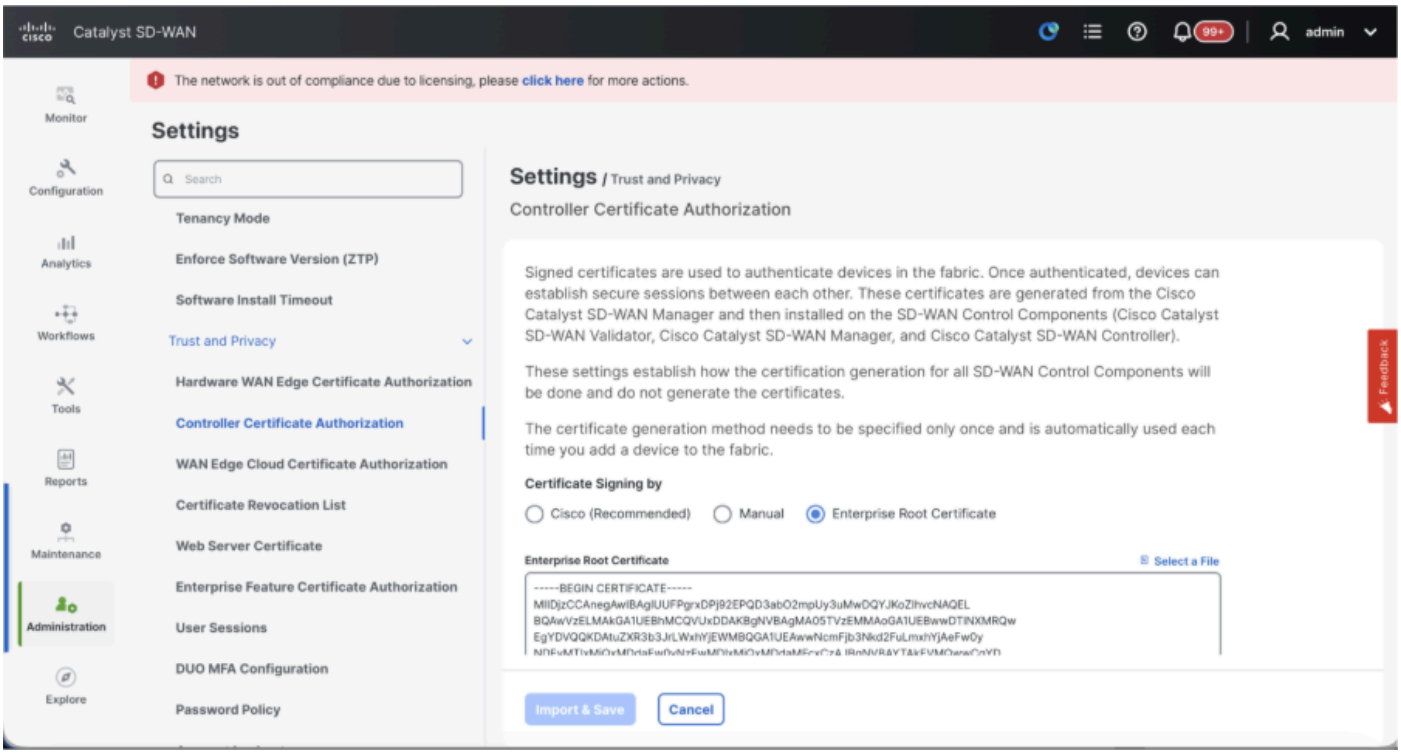
- Vérifiez les configurations de l'autorité de certification (CA), qui décide de l'autorité de certification utilisée pour signer les certificats. Nous pouvons voir 3 options ici :

1. Hardware WAN Edge Certificate Authorization : décide de l'autorité de certification pour les routeurs périphériques SD-WAN matériels.
    - Certificat On Box (certificat TPM/SUDI) : avec cette option, le certificat préinstallé sur le matériel du routeur est utilisé pour établir les connexions de contrôle (connexions TLS/DTLS)

- Certificat d'entreprise (signé par l'autorité de certification d'entreprise) : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

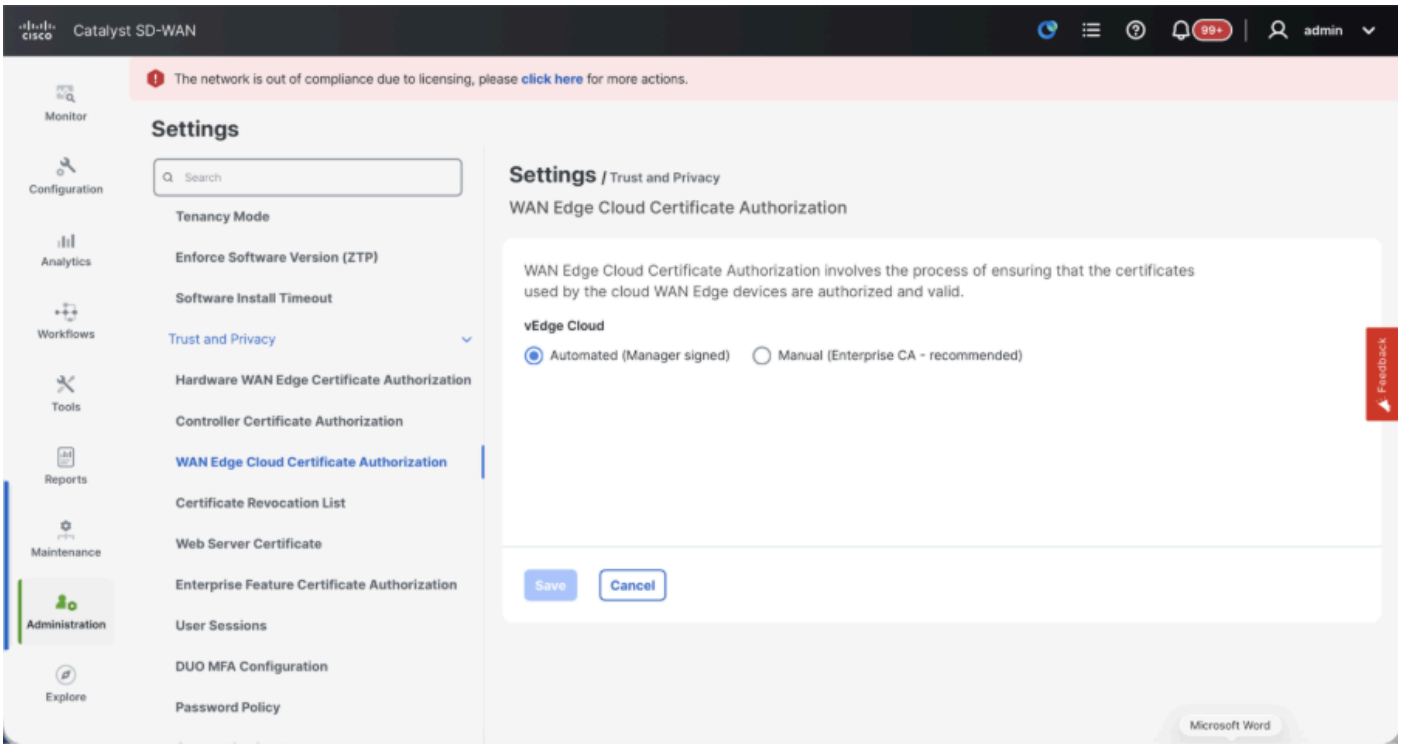


2. Autorisation de certificat de contrôleur - Décide de l'autorité de certification pour les contrôleurs SD-WAN.
    - Cisco (recommandé) : les contrôleurs utilisent les certificats signés par Cisco PKI. vManage contacte automatiquement le portail PNP à l'aide des informations d'identification de compte Smart configurées sur le vManage, obtient le certificat signé et est installé sur le contrôleur.
    - Manuel - Les contrôleurs utilisent les certificats signés par Cisco PKI. Signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
    - Certificat racine d'entreprise : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

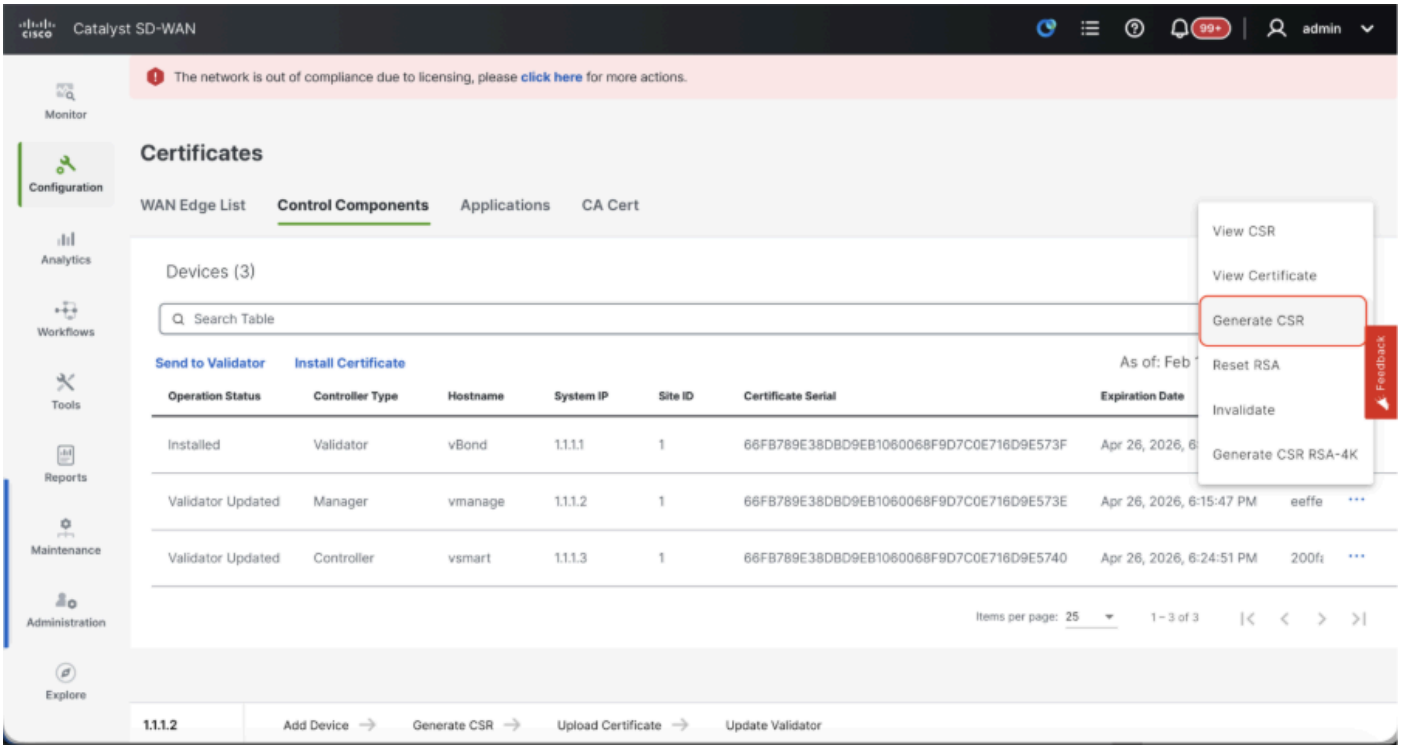


3. WAN Edge Cloud Authorization - Décide de l'autorité de certification pour les routeurs virtuels SD-WAN Edge (CSR1000v, C8000v, cloud vEdge)
    - Automatisé (vManage signed) : vManage signe automatiquement le CSR pour les routeurs de périphérie virtuels et installe le certificat sur le routeur.
    - Manuel (CA d'entreprise - recommandé) - Les routeurs virtuels utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

Dans ce cas, si nous utilisons notre propre autorité de certification, Enterprise certificate authority, sélectionnez Enterprise.



- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers
- Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par

vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.

Intégration de vBond/Validator et vSmart/Controller à vManage

Accédez à Configuration > Devices > Control Components dans le cas des noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

Intégration de vBond/Validator

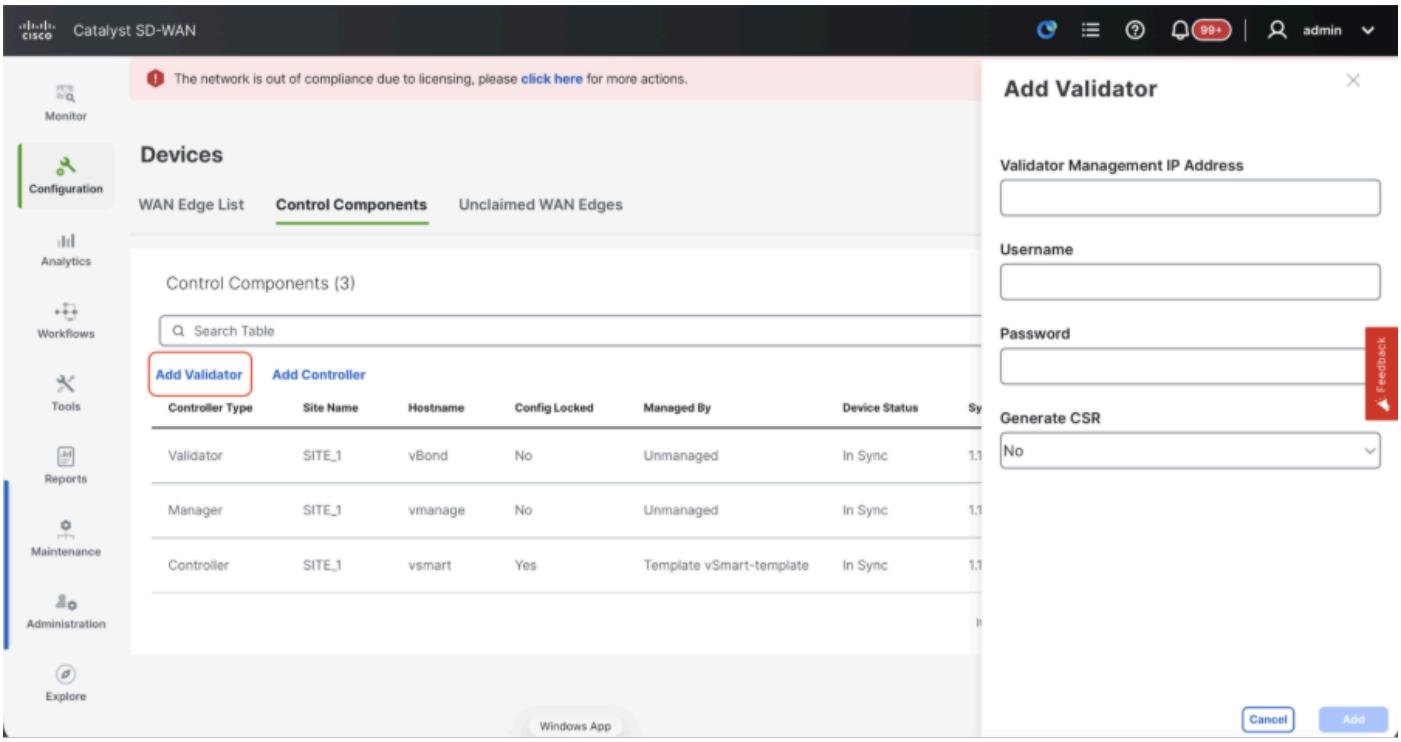
- Cliquez sur Add vBond dans le cas de 20.12 vManage ou sur Add Validator dans le cas de 20.15/20.18 vManage. Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vBond qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée de l'interface CLI de vManage vers vBond IP.
- Entrez les informations d'identification utilisateur de vBond.



Remarque : nous devons utiliser les identifiants d'administration de vBond ou une partie utilisateur du groupe netadmin. Vous pouvez le vérifier dans l'interface de ligne de commande du vBond. Sélectionnez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vBond



Remarque : Si le vBond est derrière un périphérique NAT/pare-feu, vérifiez si l'adresse IP de l'interface VPN 0 de vBond est traduite en une adresse IP publique. Si l'adresse IP de l'interface VPN 0 n'est pas accessible depuis vManage, utilisez l'adresse IP publique de l'interface VPN 0 dans cette étape



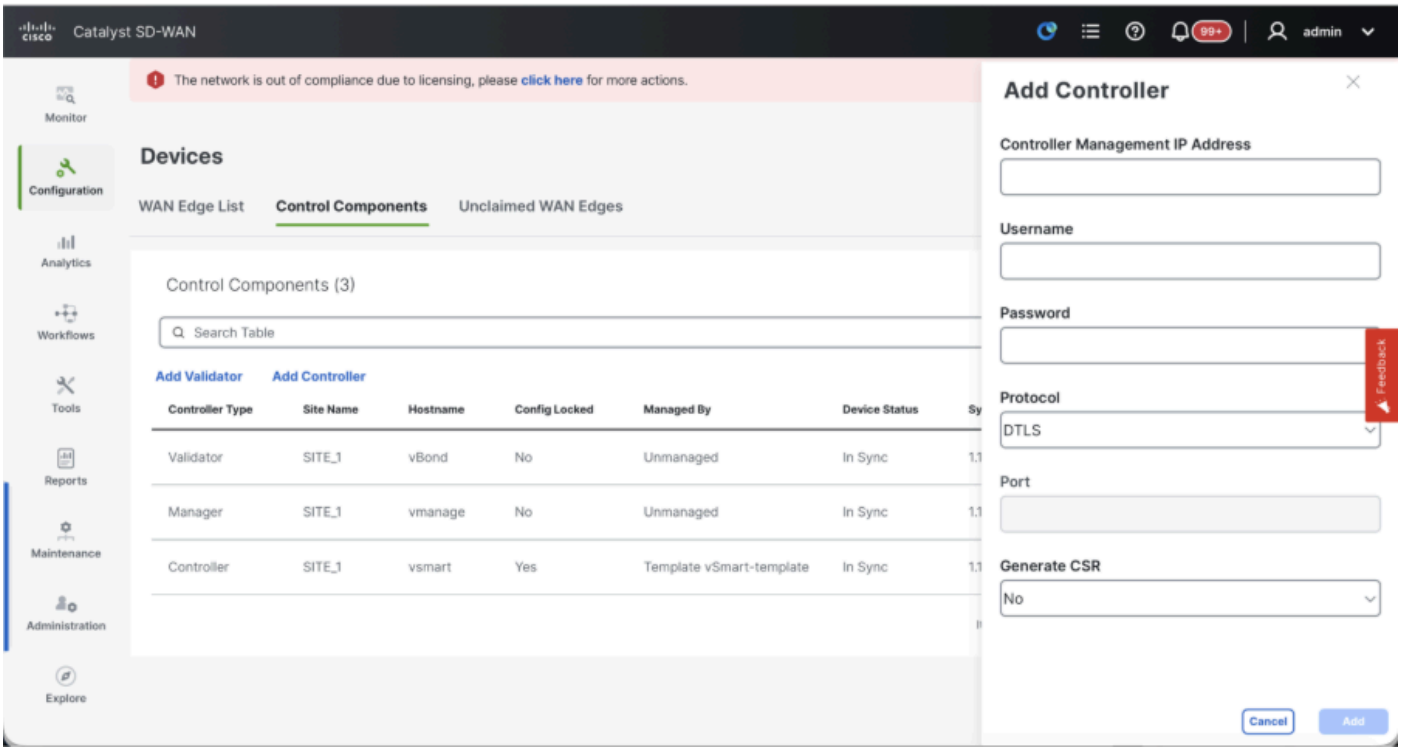
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vBond.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il existe plusieurs vBonds, répétez les mêmes étapes.

Intégration de vSmart/Controller

- Cliquez sur Add vSmart dans le cas de vManage 20.12 ou sur Add Controller dans le cas de vManage 20.15/20.18.
- Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vSmart qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée depuis l'interface CLI de vManage vers vSmart IP.
- Entrez les informations d'identification de l'utilisateur de vSmart. Notez que nous devons utiliser les informations d'identification d'administration de vSmart ou d'une partie utilisateur du groupe netadmin.

- Vous pouvez le vérifier dans l'interface de ligne de commande du vSmart.
- Définissez le protocole sur TLS, si nous avons l'intention d'utiliser TLS pour les routeurs afin d'établir des connexions de contrôle avec vSmart. Cette configuration doit également être configurée sur l'interface de ligne de commande des noeuds vSmarts et vManage.
- Choisissez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vSmart.

Remarque : si le vSmart est derrière le périphérique/pare-feu NAT, vérifiez si l'adresse IP de l'interface VPN 0 vSmart est traduite en une adresse IP publique, et si l'adresse IP de l'interface VPN 0 n'est pas accessible à partir de vManage, utilisez l'adresse IP publique de l'adresse IP de l'interface VPN 0 dans cette étape.

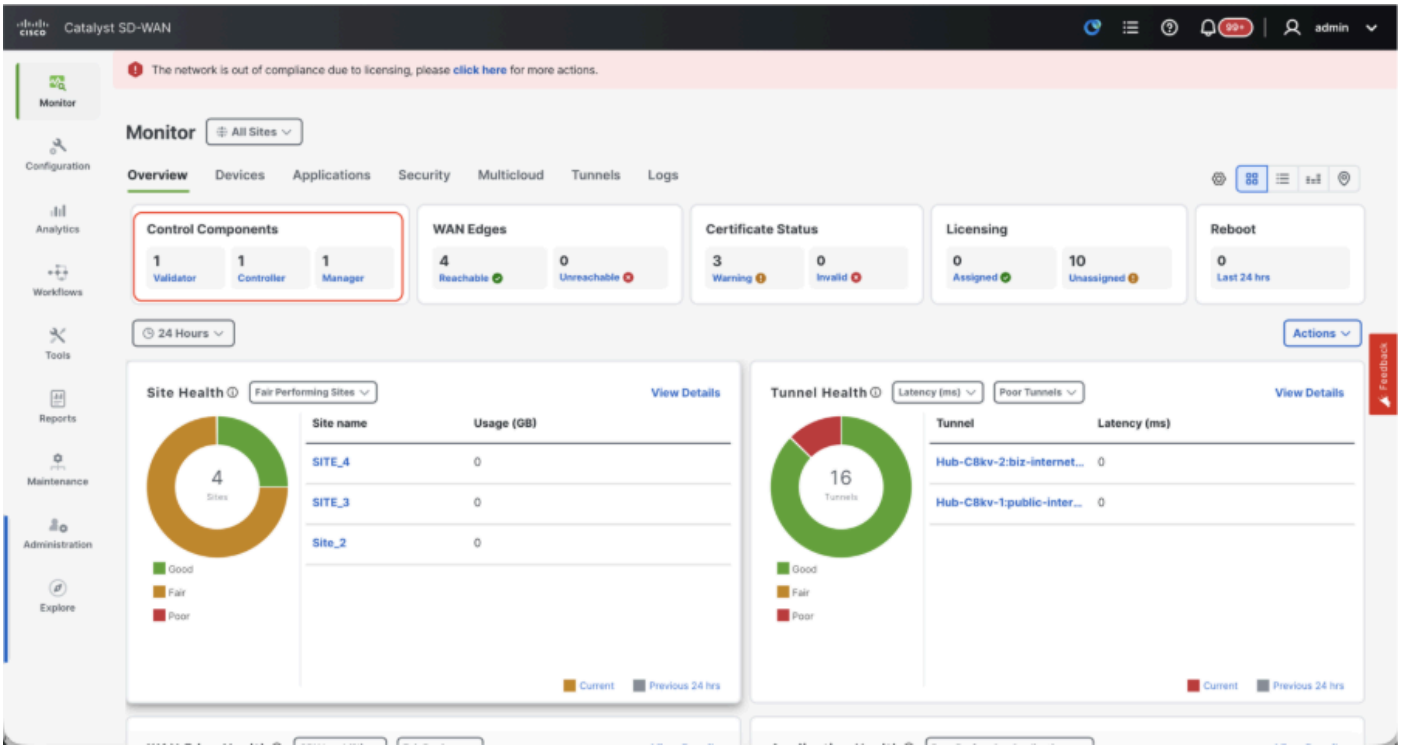


- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vSmart.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.

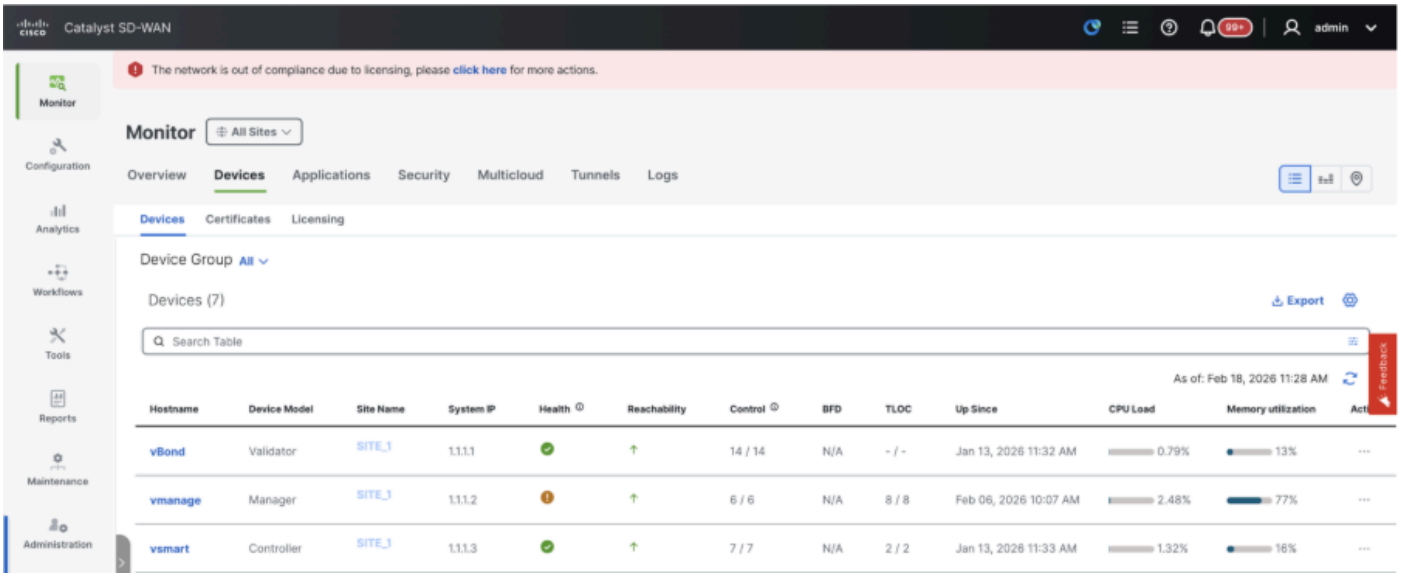
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il y a plusieurs vSmarts, répétez les mêmes étapes.

Vérification

Une fois toutes les étapes terminées, vérifiez que tous les composants de contrôle sont accessibles dans Monitor > Dashboard



- Cliquez sur les composants de contrôle respectifs et vérifiez qu'ils sont tous accessibles.
- Accédez à Monitor > Devices et vérifiez que tous les composants de contrôle sont accessibles.



Étape 3: Créer un cluster vManage

Structure SD-WAN intégrée avec un cluster vManage dans la superposition SD-WAN

Remarque : le cluster vManage peut être configuré avec 3 noeuds vManage ou 6 noeuds vManage en fonction du nombre de sites intégrés au fabric SD-WAN. Veuillez vous reporter à votre cluster vManage existant et choisir le nombre de noeuds correspondant.

Configurez les configurations CLI de tous les noeuds vManage qui font partie du cluster

Configurer la configuration système sur tous les noeuds vManage

- Configurez le reste des noeuds vManage. Dans le cas d'un cluster de 3 noeuds, vous avez 2 noeuds restants à configurer, dans le cas d'un cluster de 6 noeuds, vous avez 5 noeuds à configurer.
- Configurez les configurations système comme indiqué :

```
config t
system
 host-name             <hostname>
 system-ip             <unique system-ip>
 site-id               <site-id>
 organization-name     <organization name>
```

```
 vbond <IP address/URL of vBond>
commit
```



Remarque : si nous utilisons une URL comme adresse vBond, assurez-vous de configurer les adresses IP du serveur DNS dans la configuration VPN 0 ou assurez-vous qu'elles peuvent être résolues.

Configurer l'interface de transport sur tous les noeuds vManage

Ces configurations sont nécessaires pour activer l'interface de transport utilisée pour établir des connexions de contrôle avec les routeurs et le reste des contrôleurs.

```
config t
vpn 0
 dns <IP-address> primary
 dns <IP-address> secondary
 interface eth1
  ip address <IP-address/mask>
  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 <default-gateway IP>
commit
```

Configurer l'interface de gestion sur tous les noeuds vManage

Configurez également l'interface de gestion du VPN 512 pour activer l'accès de gestion hors bande au contrôleur.

```
Conf t
vpn 512
 interface eth0
  ip address <IP-address/mask>
```

```
  no shutdown
 !
 ip route 0.0.0.0/0 <default-gateway IP>
!
Commit
```

Configuration facultative :

- Vous pouvez vous référer aux configurations de votre contrôleur existant et si la configuration listée ici est présente, vous pouvez ajouter cette configuration aux nouveaux contrôleurs.
- Configurez le protocole de contrôle comme TLS uniquement si les routeurs doivent établir des connexions de contrôle sécurisées avec les noeuds vManage à l'aide de TLS. Par défaut, tous les contrôleurs et routeurs établissent une connexion de contrôle à l'aide de DTLS. Il s'agit d'une configuration facultative requise uniquement sur les noeuds vSmart et vManage, en fonction de vos besoins.

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

Configurer l'interface de service sur tous les noeuds vManage

Configurez l'interface de service sur tous les noeuds vManage, y compris vManage-1 qui a déjà été intégré. Cette interface est utilisée pour la communication de cluster, ce qui signifie la communication entre les noeuds vManage dans le cluster.

```
conf t
 interface eth2
  ip address <IP-address/mask>
  no shutdown
commit
```

Assurez-vous que le même sous-réseau IP est utilisé pour l'interface de service sur tous les noeuds du cluster vManage.

Configurer les identifiants de cluster

Nous pouvons utiliser les mêmes informations d'identification d'administration des noeuds vManage pour configurer le cluster vManage. Sinon, nous pouvons configurer une nouvelle information d'identification d'utilisateur qui fait partie du groupe netadmin. Les configurations permettant de configurer de nouvelles informations d'identification utilisateur sont les suivantes :

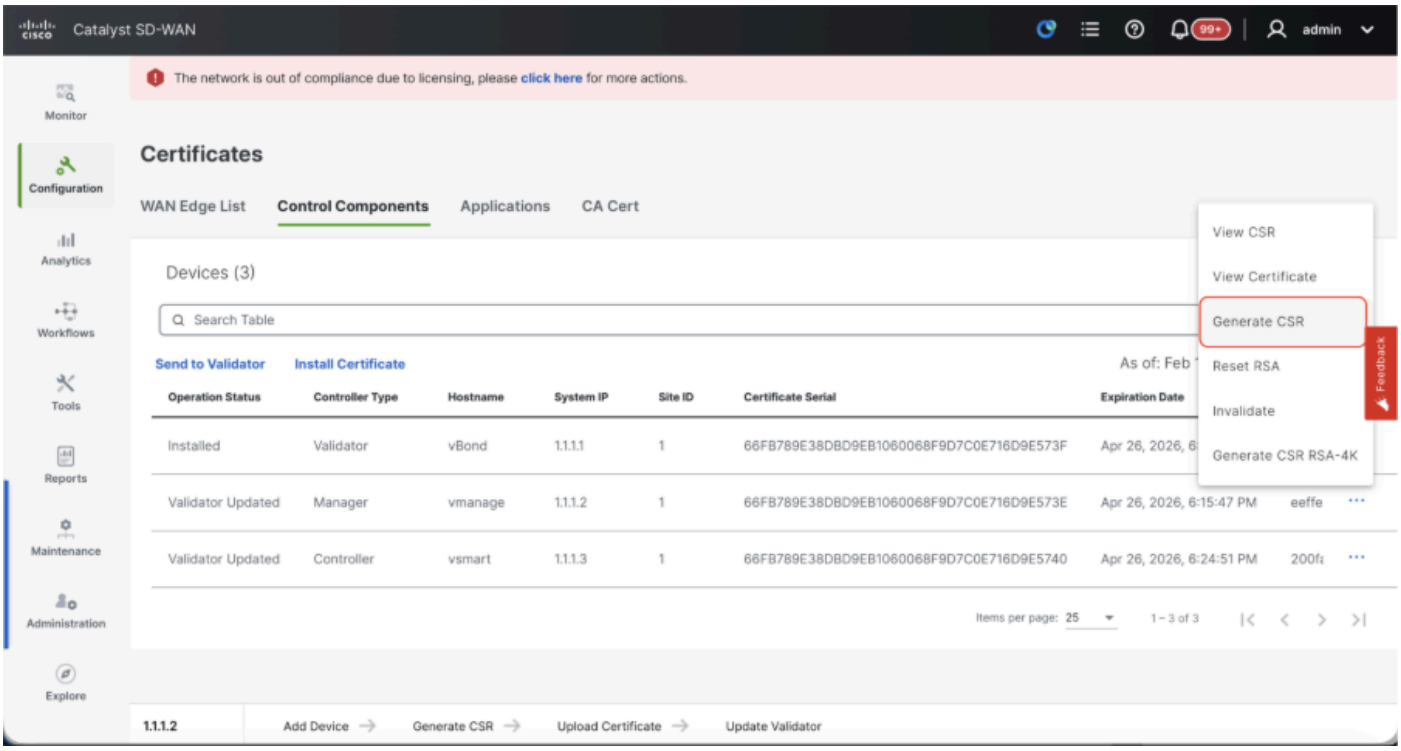
```
conf t
system
 aaa
  user <username>
   password <password>
   group    netadmin
commit
```

Assurez-vous de configurer les mêmes informations d'identification d'utilisateur sur tous les noeuds vManage qui font partie du cluster. Si nous décidons d'utiliser les informations d'identification d'administrateur, il doit s'agir du même nom d'utilisateur/mot de passe sur tous les noeuds vManage.

Installer le certificat de périphérique sur tous les noeuds vManage

- Connectez-vous à l'interface utilisateur vManage de tous les noeuds vManage à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

  Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.
- Si vous choisissez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en naviguant jusqu'au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- Effectuez cette étape sur tous les noeuds vManage qui font partie du cluster.

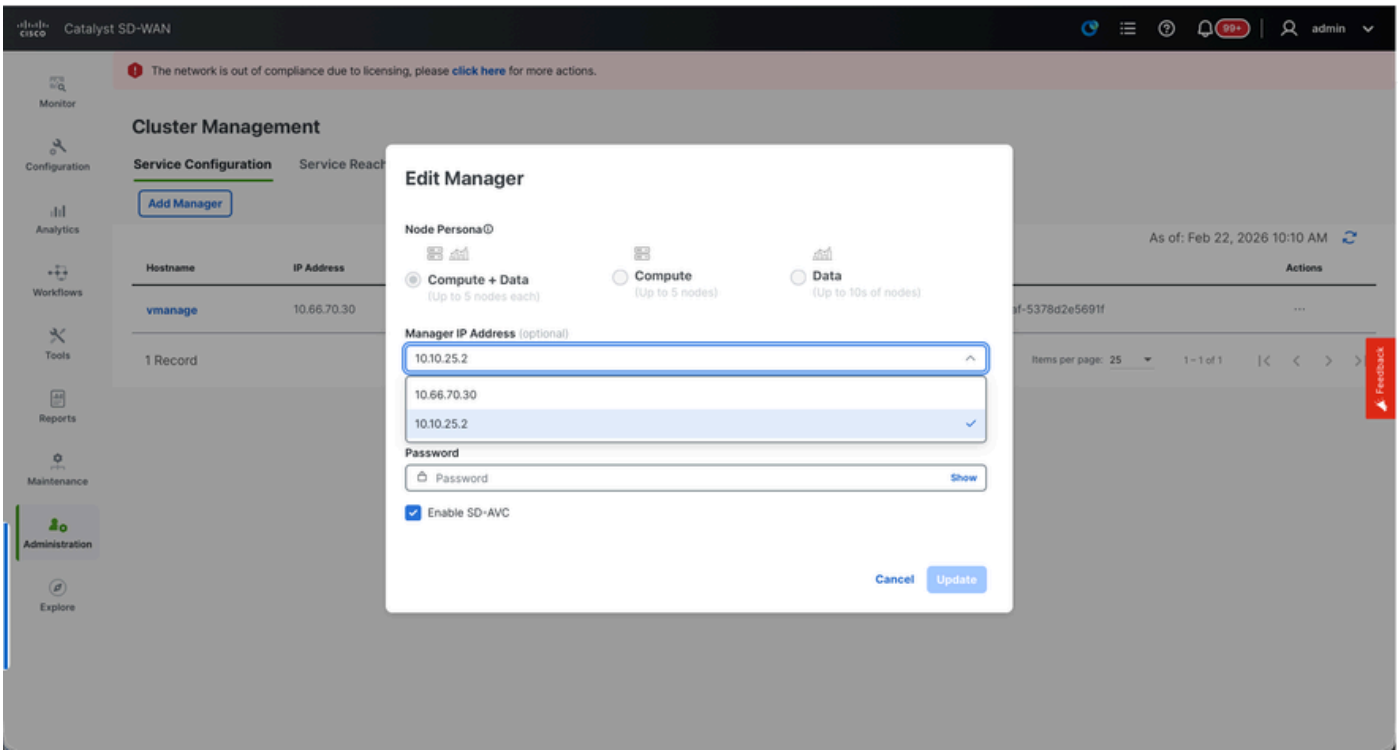
Préparation de la création du cluster vManage

- Dans l'interface utilisateur web de vManage-1, accédez à Administration > Cluster Management, cliquez sur ... sous Actions pour vManage-1, choisissez Edit.
- Le personnage du noeud est choisi automatiquement en fonction du personnage que nous avons choisi lors de la mise sous tension de la VM.

Remarque : Dans le cas d'un cluster à 3 noeuds, les 3 noeuds vManage sont présentés

avec compute+data comme personnage.

- Pour un cluster à 6 noeuds, 3 noeuds vManage sont activés avec calcul+données comme personnage et 3 noeuds vManage avec données comme personnage.
- Dans la liste déroulante de l'adresse IP du gestionnaire, assurez-vous de choisir l'adresse IP de l'interface de service du vManage.



- Entrez le nom d'utilisateur et le mot de passe que vous souhaitez utiliser pour activer le cluster vManage, appelé informations d'identification du cluster.
- Comme mentionné précédemment, les mêmes informations d'identification doivent être configurées sur tous les noeuds vManage et doivent être utilisées lors de l'ajout de tous les noeuds au cluster.

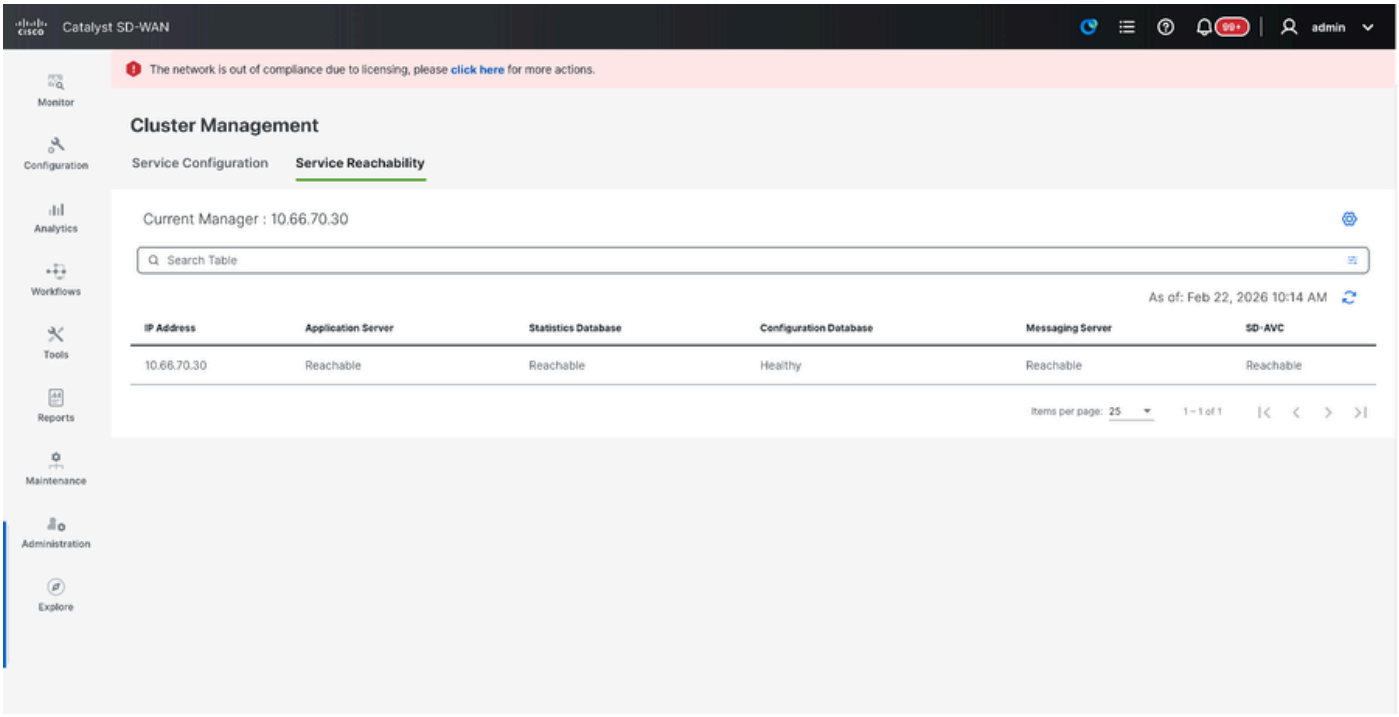
Remarque : Reportez-vous à cette configuration dans votre cluster existant pour activer SDAVC. Vous devez la vérifier uniquement si elle est requise et si elle n'est nécessaire que sur un noeud vManage du cluster.

Cliquez sur Update.

- Publiez ceci, les services vManage NMS redémarrent en arrière-plan et l'interface utilisateur n'est pas disponible pendant quelques minutes d'environ 5 à 10 minutes. Pendant ce temps,

l'accès CLI de vManage est disponible.

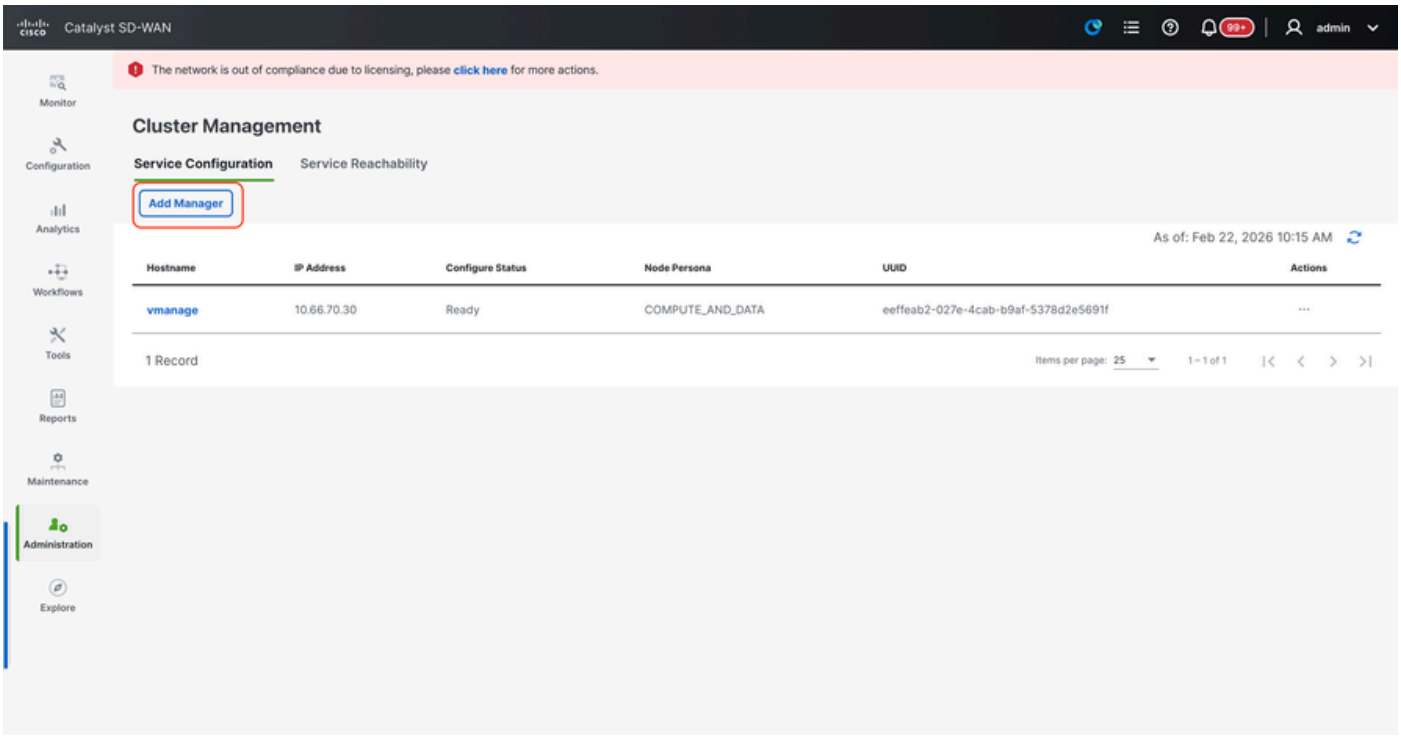
- Une fois que l'interface utilisateur de vManage-1 est accessible, accédez à Administration > Cluster Management, assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et que la personnalité du noeud est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles.

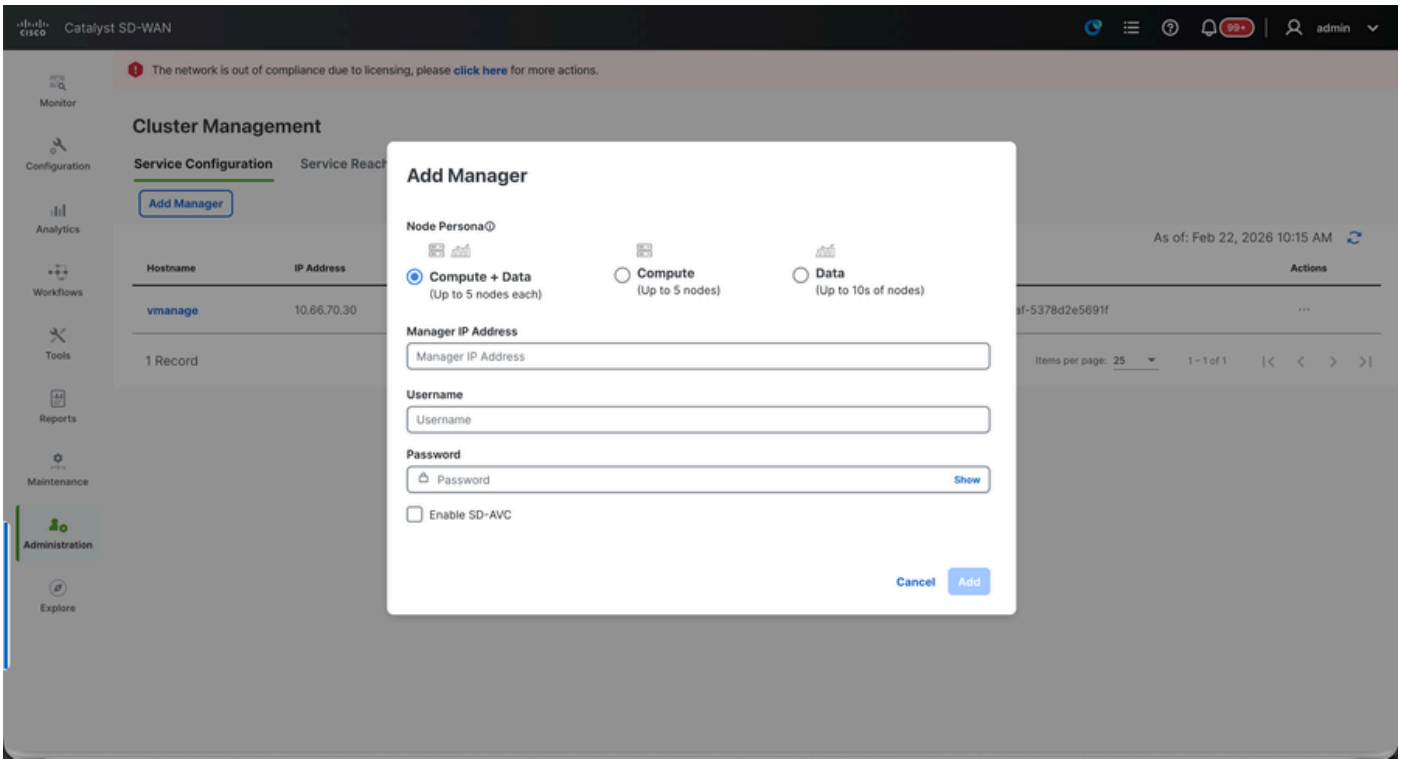


- Si l'un des services n'est pas encore accessible, veuillez patienter. Cela prend généralement entre 20 et 30 minutes.

Créer le cluster vManage

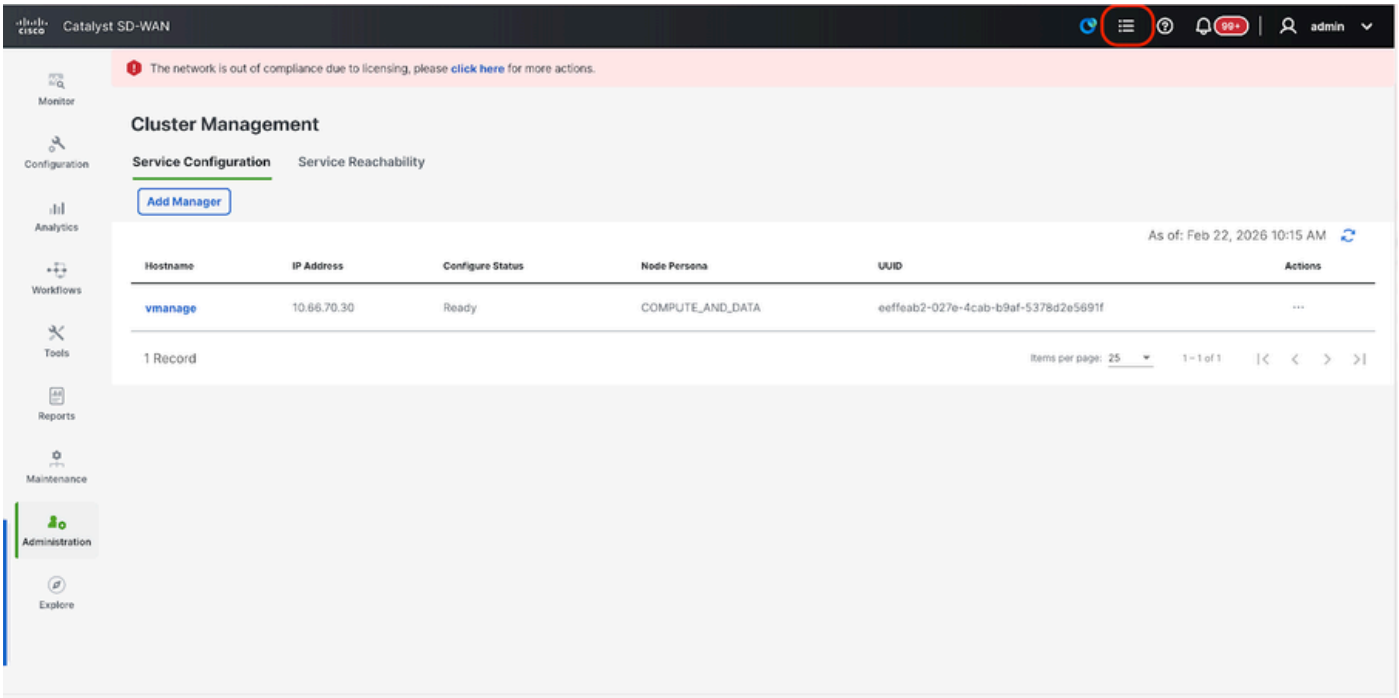
- Sur l'interface utilisateur web de vManage-1, accédez à Administration > Cluster Management, dans la section Configuration du service,
- Cliquez sur Add Manager, une fenêtre contextuelle s'affiche :





- Choisissez le personnage de noeud en fonction des configurations de personnage effectuées pendant que le noeud vManage - 2 a été lancé.
- Entrez l'adresse IP de l'interface de service de vManage-2 sous l'adresse IP du gestionnaire
- Saisissez le nom d'utilisateur et le mot de passe, qui sont les mêmes informations d'identification que celles utilisées à l'étape 6.
- Enable SDAVC (Activer SDAVC) : cette case n'est pas cochée, car elle est déjà activée sur vManage-1
- Cliquez sur Ajouter.

- Dans ce message, les services vManage NMS redémarrent en arrière-plan pour les noeuds vManage 1 et 2. L'interface utilisateur n'est pas disponible pendant quelques minutes, de l'ordre de 5 à 10 minutes pour vManage 1 et 2.
- Pendant ce temps, l'accès CLI de vManage 1 et 2 est disponible.
- Une fois que l'interface utilisateur de vManage-1 est accessible, accédez à Administration > Cluster Management, assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et node persona est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles pour les deux noeuds vManage.
- Si l'un des services n'est pas encore accessible, veuillez patienter. Cela prend généralement entre 5 et 10 minutes.
- Vous pouvez vérifier l'état du processus d'ajout de cluster dans la liste des tâches disponible dans l'angle supérieur droit de l'interface utilisateur vManage.



- Vous pouvez rechercher la liste des tâches actives et si la tâche est toujours répertoriée sous Liste des tâches actives, cela indique que la tâche n'est pas encore terminée.
- Vous pouvez cliquer sur la tâche pour vérifier sa progression. Si la tâche n'est pas répertoriée dans la liste des tâches actives, passez à Terminée et vérifiez qu'elle est terminée avec succès.
- Une fois ces points validés, passez à l'étape suivante.

Ces points doivent être pris en compte avant d'ajouter le noeud suivant au cluster :

Vérifiez ces points sur toutes les interfaces utilisateur des noeuds vManage qui ont été ajoutés au cluster jusqu'à présent :

- Accédez à Monitor > Overview of vManage UI et assurez-vous que le nombre de noeuds vManage sont reflétés correctement et sont visibles accessibles en fonction du nombre de noeuds ajoutés au cluster.

- Accédez à Administration > Cluster Management et assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et node persona est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles pour les deux noeuds vManage.

- Chaque fois qu'un noeud est ajouté au cluster, les services NMS de tous les noeuds du cluster sont redémarrés, ce qui rend l'interface utilisateur de tous ces noeuds inaccessible pendant un certain temps.
- Selon le nombre de noeuds dans le cluster, la restauration de l'interface utilisateur et l'accessibilité de tous les services peuvent prendre plus de temps.
- Vous pouvez surveiller la tâche sous Liste des tâches disponible dans le coin supérieur droit de l'interface utilisateur vManage.
- Sur l'interface utilisateur vManage de chaque noeud ajouté au cluster, nous devons voir tous les routeurs, modèles et stratégies s'ils étaient disponibles dans vManage-1.
- Si ces configurations n'étaient pas présentes sur vManage-1, les vBonds et vSmarts qui ont été ajoutés à vManage-1 ainsi que les configurations Administration > Settings pour Organization-name, vBond, Certificate Authorization doivent être reflétées sur le reste des noeuds vManage ajoutés au cluster.
- Répétez les mêmes étapes pour le reste des noeuds vManage.

Une fois tous les contrôleurs intégrés, procédez comme suit :

Étape 4: Sauvegarde/restauration Config-db

Collecter la sauvegarde et la restauration de la base de données de configuration vManage sur un autre noeud vManage

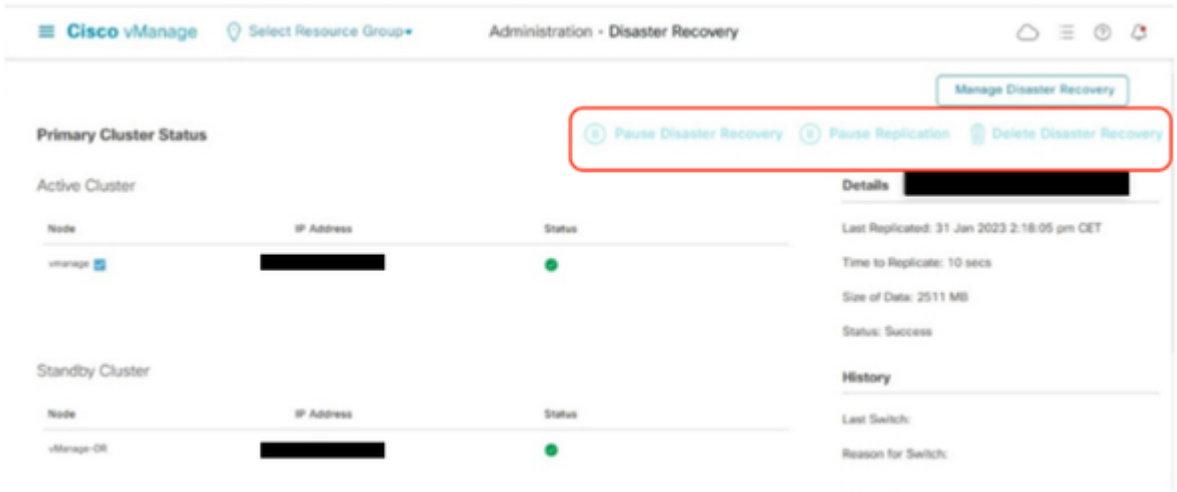
---

Remarque : Lors de la collecte de la sauvegarde de la base de données de configuration à partir du cluster vManage existant pour lequel la récupération après sinistre est activée, assurez-vous qu'elle est collectée après la suspension et la suppression de la récupération après sinistre sur ce noeud.

Vérifiez qu'aucune réplication de reprise après sinistre n'est en cours. Accédez à Administration > Disaster Recovery et assurez-vous que l'état est Réussite et qu'il n'est pas dans un état transitoire tel que Importation en attente, Exportation en attente ou Téléchargement en attente. Si

l'état n'est pas réussi, contactez le TAC Cisco et assurez-vous que la réplication est réussie avant de procéder à la pause de la reprise après sinistre.

Tout d'abord, suspendez la reprise après sinistre et assurez-vous que la tâche est terminée. Supprimez la reprise après sinistre et confirmez que la tâche est terminée.



Contactez le TAC Cisco pour vous assurer que la reprise après sinistre est correctement nettoyée.

Collecter la sauvegarde Configuration-DB :

- Dans le fabric SD-WAN actuellement utilisé, vous pouvez générer une sauvegarde de la base de données de configuration à partir du cluster vManage.
- Veuillez noter que nous devons générer une sauvegarde de la base de données de configuration uniquement sur un noeud du cluster vManage qui est le leader de la base de données de configuration.

- Pour vManage autonome, ce vManage est lui-même le leader de la base de données de configuration.
- Dans le cluster vManage, identifiez le noeud de tête configuration-db à l'aide de la commande request nms configuration-db diagnostics. Vous pouvez exécuter cette commande sur tous les noeuds du cluster vManage à 3 noeuds.
- Dans un cluster de 6 noeuds, assurez-vous d'exécuter cette commande sur les noeuds vManage où configuration-db est activé pour identifier le noeud de tête. Accédez à Administration > Gestion du cluster pour vérifier la même chose :
- Comme nous le voyons dans la capture d'écran, les noeuds configurés avec persona COMPUTE_AND_DATA ont configuration-db en cours d'exécution.

Vous pouvez vérifier la même chose à l'aide de la commande request nms configuration-db status sur l'interface de ligne de commande vManage. Le résultat est le suivant

```
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#
```

- Une fois que vous exécutez la commande request nms configuration-db diagnostics sur ces noeuds, le résultat est comme indiqué :
- Recherchez le champ mis en surbrillance pour « IsLeader ». S'il est défini sur 1, il indique que le noeud est le noeud leader et nous pouvons collecter la sauvegarde configuration-db à partir de celui-ci.

```
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     .
```

Utilisez cette commande pour collecter la sauvegarde configuration-db à partir du noeud vManage de tête de base de données de configuration identifié.

```
request nms configuration-db backup path /opt/data/backup/<filename>
```

Le résultat attendu est le suivant :

```
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#
```

- Notez les informations d'identification de configuration-db si elles ont été mises à jour.

- Si vous ne connaissez pas les informations d'identification de la base de données de configuration, contactez le TAC pour récupérer les informations d'identification de la base de données de configuration à partir des noeuds vManage existants.

- Les informations d'identification configuration-db par défaut sont username : neo4j et password : mot de passe

Restaurer la sauvegarde Configuration-db vers un autre noeud vManage

Copiez la sauvegarde configuration-db dans le répertoire /home/admin/ de vManage à l'aide de SCP.

Exemple de sortie de commande 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
```

Pour restaurer la sauvegarde configuration-db, nous devons d'abord configurer les informations d'identification configuration-db. Si vos identifiants configuration-db sont default(neo4j/password), nous pouvons ignorer cette étape.

Pour configurer les informations d'identification configuration-db, utilisez la commande request nms configuration-db update-admin-user. Utilisez le nom d'utilisateur et le mot de passe de votre choix.

Veuillez noter que le serveur d'applications de vManage est redémarré. En raison de laquelle l'interface utilisateur vManage devient inaccessible pendant une courte période.

```
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#
```

Publication que nous pouvons poursuivre pour restaurer la sauvegarde configuration-db :

Nous pouvons utiliser la commande request nms configuration-db restore path /home/admin/< > pour restaurer la base de données de configuration dans le nouveau 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
```

Une fois la base de données de configuration restaurée, assurez-vous que l'interface utilisateur vManage est accessible. Attendez environ 5 minutes, puis essayez d'accéder à l'interface utilisateur.

Une fois connecté à l'interface utilisateur avec succès, assurez-vous que la liste des routeurs Edge, le modèle, les stratégies et toutes les autres configurations qui étaient présentes sur votre interface utilisateur vManage précédente ou existante sont reflétés sur la nouvelle interface utilisateur vManage.



Mise en garde : La base de données de configuration restaurée contient toujours le ou les

---

gestionnaires SD-WAN à partir desquels la sauvegarde a été effectuée. Elles sont répertoriées en tant qu'entrées Manager dans Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) mais ne sont pas membres de Administration > Cluster Management. Jusqu'à leur suppression à l'étape 5 :

- chaque rapport Send to Validator signale Failed to find Vmanage Cluster node for uuid <uuid> for them, et
- chaque installation de certificat de contrôleur à partir de l'interface utilisateur échoue et est restaurée.

N'effectuez aucune opération de certificat de contrôleur ou d'envoi au validateur sur ce vManage avant la fin de l'étape 5. Si l'installation d'un certificat échoue, n'installez pas le même certificat à partir de l'interface de ligne de commande ; Contactez le centre d'assistance technique Cisco TAC.

Étape 5: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

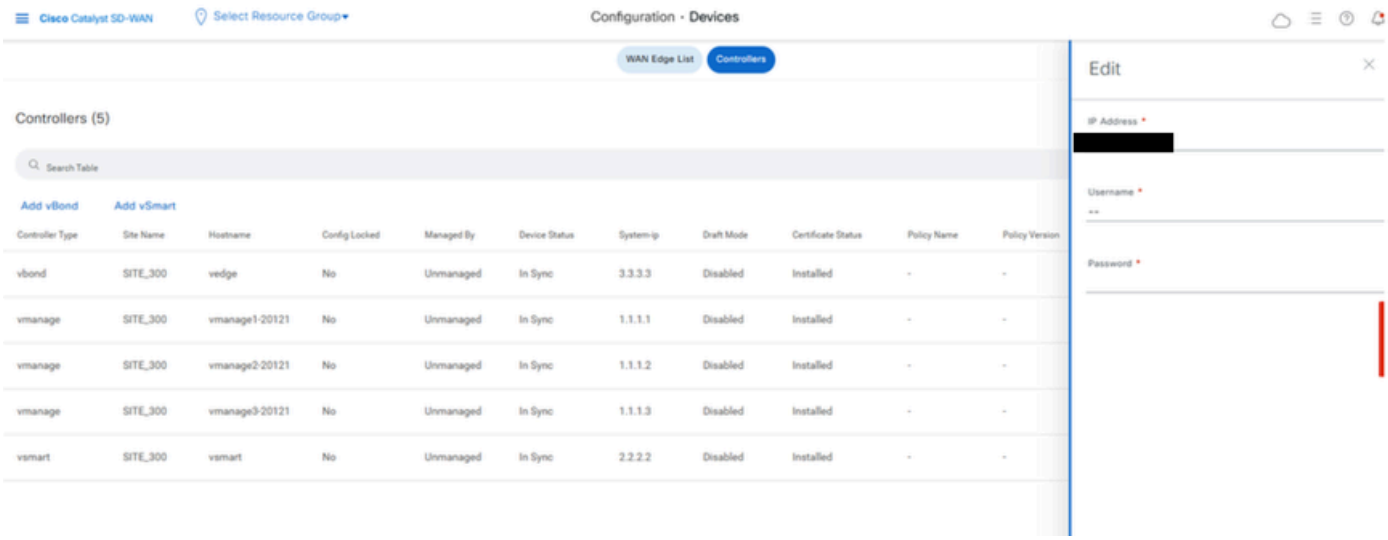
Une fois la base de données de configuration restaurée, nous devons réauthentifier tous les nouveaux contrôleurs (vmanage/vsmart/vbond) dans le fabric



Remarque : en production réelle, si l'interface IP utilisée pour la ré-authentification est l'interface IP du tunnel, vous devez vous assurer que le service NETCONF est autorisé sur l'interface du tunnel de vManage, vSmart et vBond, ainsi que sur les pare-feu le long du chemin. Le port de pare-feu à ouvrir est le port TCP 830 en tant que règle bidirectionnelle du cluster DR vers tous les vBonds et vSmarts .

Sur l'interface utilisateur vmanage, cliquez sur Configuration > Devices > Controllers

- Cliquez sur les trois points situés près de chaque contrôleur, puis cliquez sur Edit



- Remplacez l'adresse IP (ip système du contrôleur) par l'adresse IP du vpn de transport 0 (interface de tunnel). Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur save (enregistrer)
- Procédez de la même manière pour tous les nouveaux contrôleurs du fabric

Synchroniser la chaîne de certificats racine

Une fois tous les contrôleurs intégrés, procédez comme suit :

Sur tout serveur Cisco SD-WAN Manager du cluster nouvellement actif, effectuez les actions suivantes :

Entrez cette commande pour synchroniser le certificat racine avec tous les périphériques Cisco Catalyst SD-WAN dans le nouveau cluster actif :

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

Entrez cette commande pour synchroniser l'UUID du gestionnaire Cisco SD-WAN avec le validateur Cisco SD-WAN :

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

Supprimer les entrées précédentes du gestionnaire SD-WAN

Effectuez cette opération juste après la synchronisation root-cert-chain et avant toute opération de certificat de contrôleur ou Envoyer au validateur.

1. Ouvrez Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) et Administration > Cluster Management. Chaque entrée vManage qui n'est pas répertoriée dans Administration > Cluster Management est une entrée précédente de SD-WAN Manager et doit être supprimée.
2. Avant toute action Envoyer au validateur ou Invalider, recherchez un enregistrement de numéro de série en conflit. Accédez à https://<vmanage-url>/dataservice/certificate/vsmart/list. Aucune entrée ne peut avoir un ancien numéro de série dont le numéro de série est égal à son propre numéro de série. Cette vérification est en lecture seule. Si une telle entrée existe, arrêtez-vous et contactez le TAC Cisco : any Send to Validator or Invalidate envoie la liste des contrôleurs et ce contrôleur perdrait ses connexions de contrôle.
3. Accédez à Monitor > Tasks et ouvrez la dernière tâche Push vSmart List. Examiner uniquement les résultats des tâches existantes ; ne cliquez pas ici sur Envoyer au validateur. Si aucune tâche récente n'est répertoriée, attendez la diffusion de la liste en début d'heure suivante. Chaque entrée précédente du gestionnaire SD-WAN doit indiquer Failed to find Vmanage Cluster node for uuid <uuid>. Si un uuid vManage a été envoyé avec succès, il est membre actif de ce cluster : ne l'invalidez pas.
4. Cliquez sur les trois points à droite de la première entrée précédente du gestionnaire SD-WAN, puis cliquez sur Invalidate. Attendez la fin de la tâche. Le résultat attendu est Success with warning, avec cet exercice :

```
Invalidating Root Certificate Autority of vManage-<uuid>
Sending serial number of vManage-<uuid> as invalid to all controllers
Failed to push serial list to vManage-<uuid> - retry in 30 seconds; Failed to find Vmanage Cluster node
Updated serial list will be sent to vManage-<uuid> when it is reachable
Clearing certificate on vManage-<uuid>
Successfully invalidated vManage-<uuid>
```

L'entrée affiche désormais No certificate installed. Le numéro de série précédent du gestionnaire SD-WAN et l'autorité de certification racine sont supprimés des validateurs.

5. Cliquez sur les trois points de la même entrée, puis cliquez à nouveau sur Invalider. Il se termine immédiatement, sans tâche, et l'entrée est supprimée.
6. Répétez les étapes 4 et 5 pour chaque entrée précédente du gestionnaire SD-WAN.
7. Cliquez sur Envoyer au validateur. Le résultat attendu est Success pour chaque destinataire dans quelques secondes, avec no Failed to find Vmanage Cluster node.

Invalider les anciens contrôleurs

Une fois que le fabric est restauré et que les sessions de contrôle et BFD sont actives pour tous les bords et contrôleurs du fabric, invalidez les anciennes entrées vBond/Validator et vSmart/Controller de l'interface utilisateur :

- Sur l'interface utilisateur de vManage, accédez à Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificats > Contrôleurs).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Invalidate.
- Cliquez sur Send to Validator (Send to vBond in 20.9/20.12). Il doit indiquer le succès de chaque destinataire.
- Accédez à Configuration > Devices > Control Components (20.9/20.12 : Configuration > Devices > Controllers).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Delete.

Étape 6: Valider les chèques



Remarque : Poursuivez avec la section Post Checks présentée ici, qui est commune à toutes les combinaisons de déploiement.

Combinaison 4 : Cluster vManage + DR manuel/en veille froide

Qu’est-ce que le DR manuel/en veille froide ? Le serveur de sauvegarde du gestionnaire SD-WAN ou le cluster du gestionnaire SD-WAN est maintenu en veille froide.

Il peut également être maintenu sous tension avec son interface de transport VPN 0 arrêtée. Dans les deux cas, le module de secours doit rester isolé du fabric jusqu'à son activation et le module vManage/cluster actif doit être isolé avant l'activation de l'interface de transport du module de secours.

Des sauvegardes régulières de la base de données active sont effectuées. Si le cluster principal du gestionnaire SD-WAN ou du gestionnaire SD-WAN tombe en panne, le cluster du gestionnaire SD-WAN ou du gestionnaire SD-WAN de secours est activé manuellement et la base de données de sauvegarde est restaurée.

Instances nécessaires :

- 3 ou 6 vManage (cluster principal)
- 3 ou 6 vManage (cluster de secours DR)
- 1 ou plusieurs vBond (répartis entre les data centers principaux et DR)
- 1 vSmart ou plus (distribué dans les data centers principaux et DR)

Étapes:

1. Afficher toutes les instances à l'aide des étapes communes
2. Vérifications préalables
3. Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
4. Créer un cluster vManage
5. Configuration du cluster DR en veille froide
6. Sauvegarde/restauration Config-db
7. Réauthentification des contrôleurs et invalidation des anciens contrôleurs
8. Activation de la veille (et restauration)
9. Valider les chèques

Étape 1: Vérifications préalables

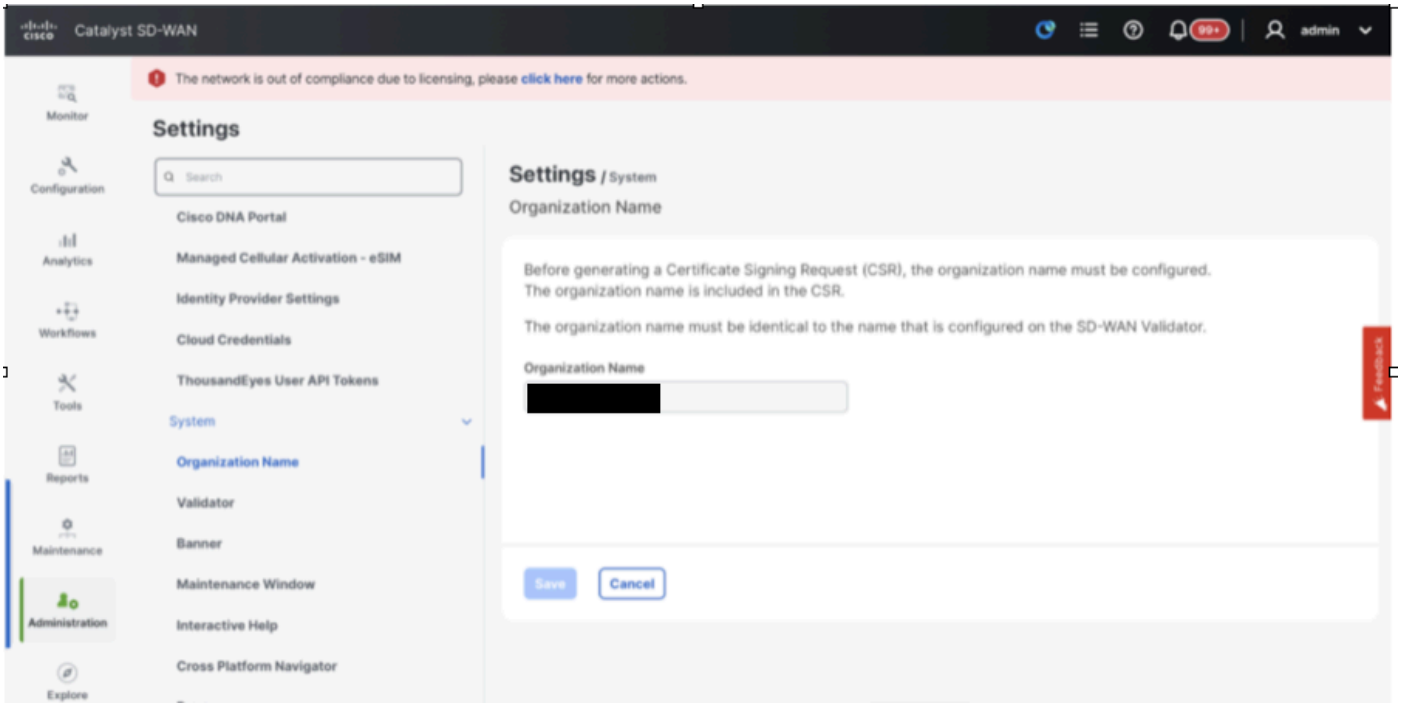
- Assurez-vous que le nombre d'instances Cisco SD-WAN Manager actives est identique au nombre d'instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles exécutent la même version logicielle.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles sont en mesure d'atteindre l'adresse IP de gestion de Cisco SD-WAN Validator.
- Assurez-vous que les certificats ont été installés sur les instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que les horloges sur tous les périphériques Cisco Catalyst SD-WAN, y compris les instances Cisco SD-WAN Manager nouvellement installées, sont synchronisées.
- Assurez-vous qu'un nouvel ensemble d'IP système et d'ID de site est configuré sur les instances de Cisco SD-WAN Manager nouvellement installées, avec la même configuration de base que le cluster actif.

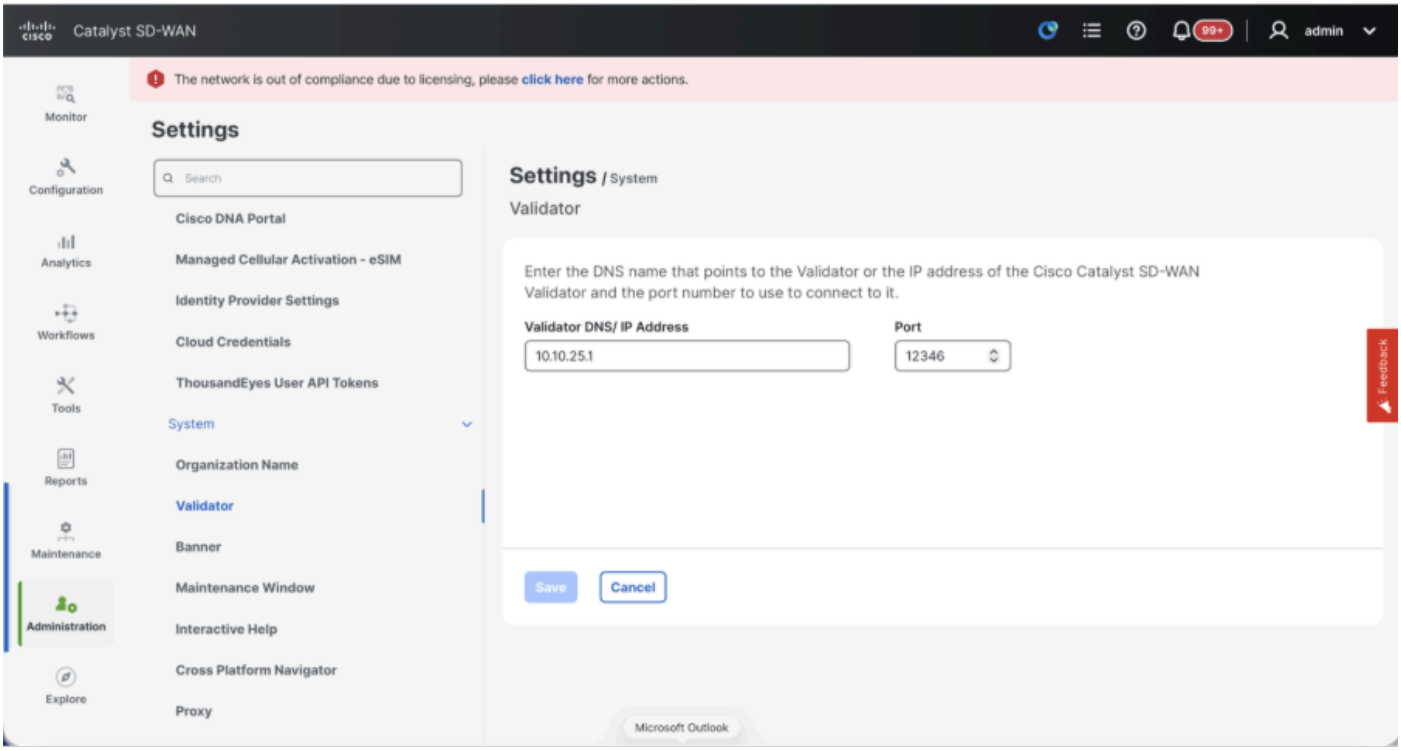
Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

Mettre à jour les configurations sur l'interface utilisateur vManage

- Une fois les configurations de l'étape 1 ajoutées à l'interface de ligne de commande de tous les contrôleurs, nous pouvons accéder à l'interface utilisateur web de vManage, à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Administration > Settings et complétez ces étapes.
- Configurez le nom de l'organisation et l'adresse URL/IP du validateur/vBond. Configurez la

même valeur que dans l'interface de ligne de commande du noeud vManage.
- Dans vManage 20.15/20.18, ces configurations sont disponibles dans la section Système.

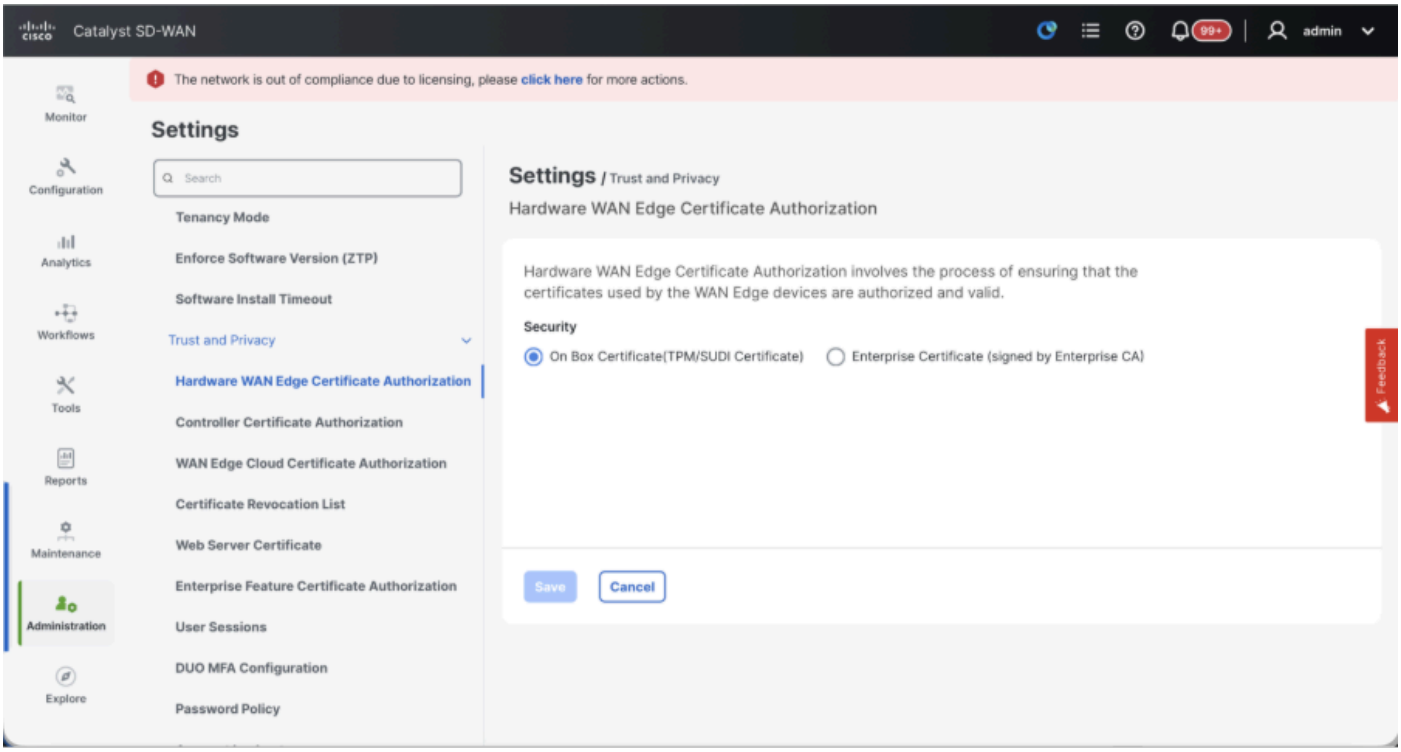




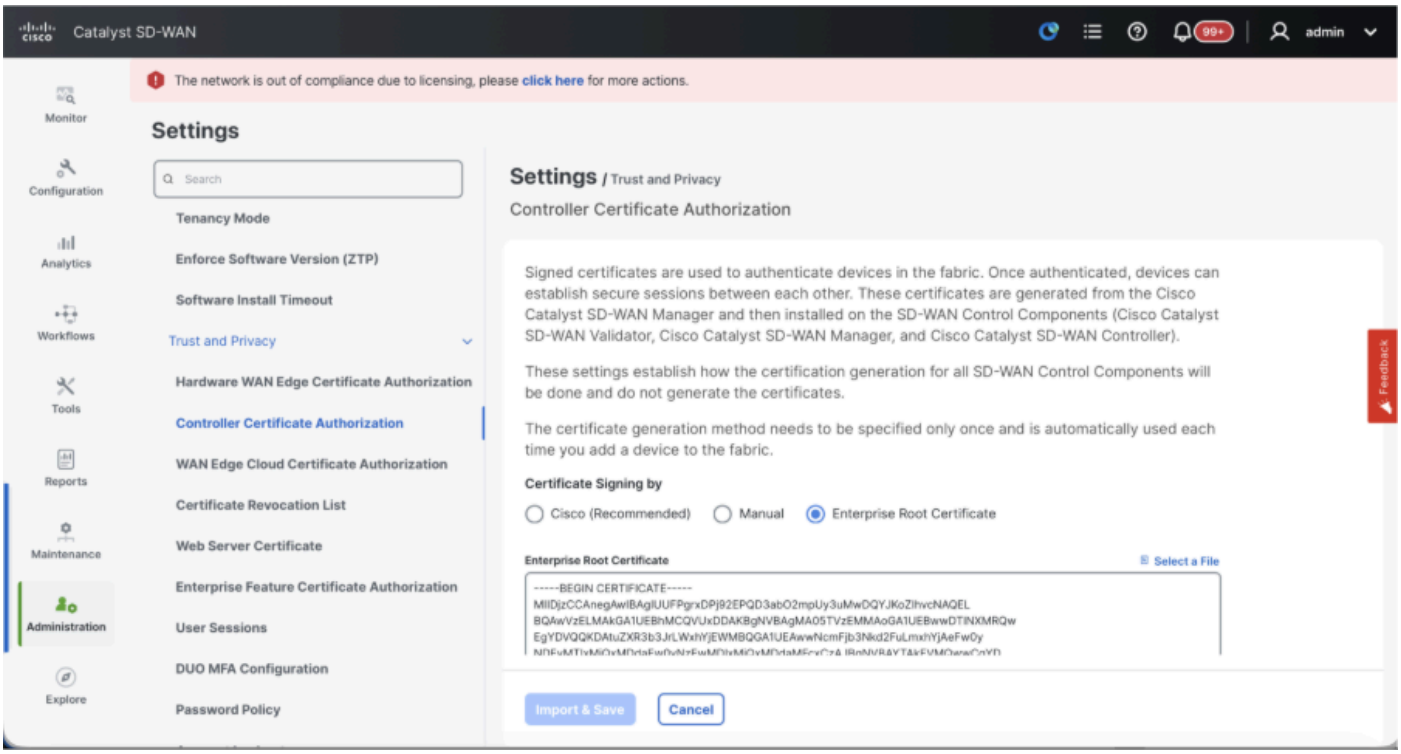
- Vérifiez les configurations de l'autorité de certification (CA), qui décide de l'autorité de certification utilisée pour signer les certificats. Nous pouvons voir 3 options ici :

1. Hardware WAN Edge Certificate Authorization : décide de l'autorité de certification pour les routeurs périphériques SD-WAN matériels.

- Certificat On Box (certificat TPM/SUDI) : avec cette option, le certificat préinstallé sur le matériel du routeur est utilisé pour établir les connexions de contrôle (connexions TLS/DTLS)
- Certificat d'entreprise (signé par l'autorité de certification d'entreprise) : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

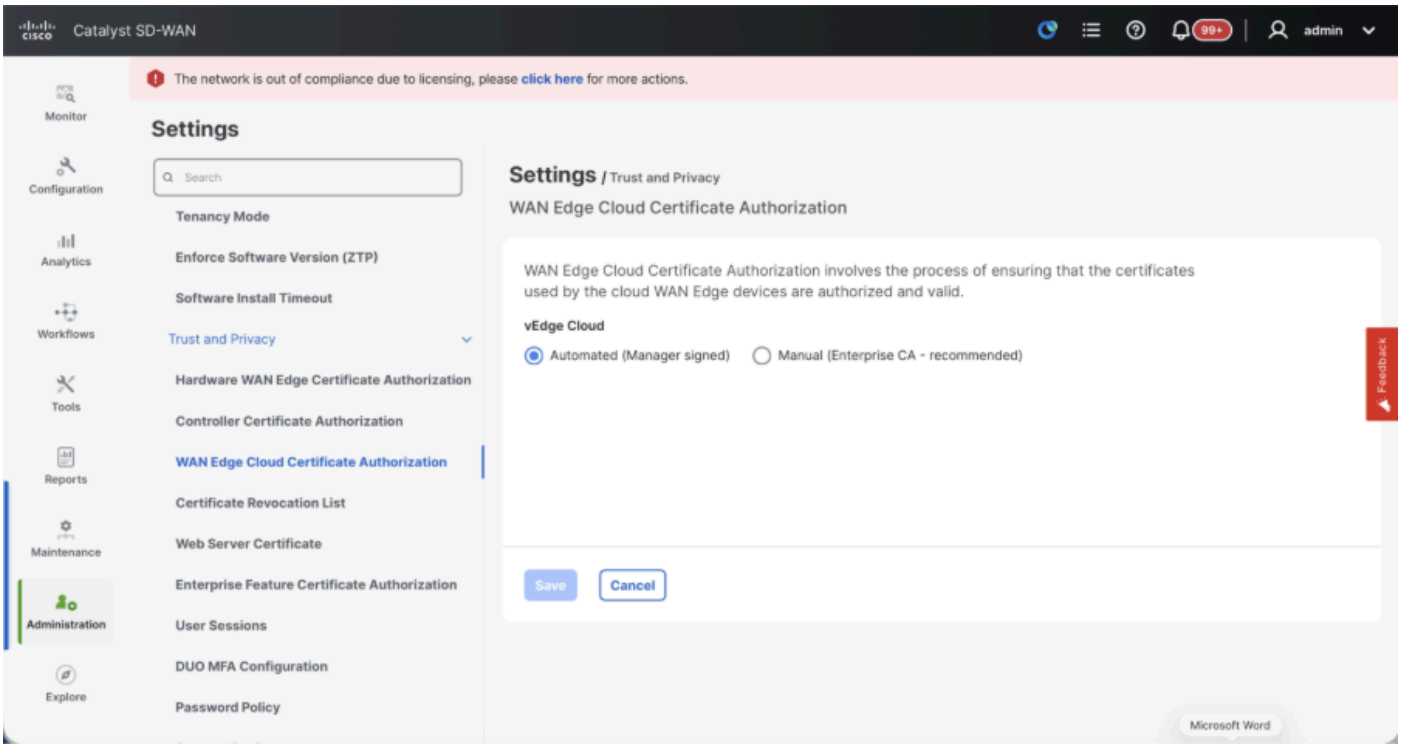


2. Autorisation de certificat de contrôleur - Décide de l'autorité de certification pour les contrôleurs SD-WAN.
    - Cisco (recommandé) : les contrôleurs utilisent les certificats signés par Cisco PKI. vManage contacte automatiquement le portail PNP à l'aide des informations d'identification de compte Smart configurées sur le vManage, obtient le certificat signé et est installé sur le contrôleur.
    - Manuel - Les contrôleurs utilisent les certificats signés par Cisco PKI. Signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
    - Certificat racine d'entreprise : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

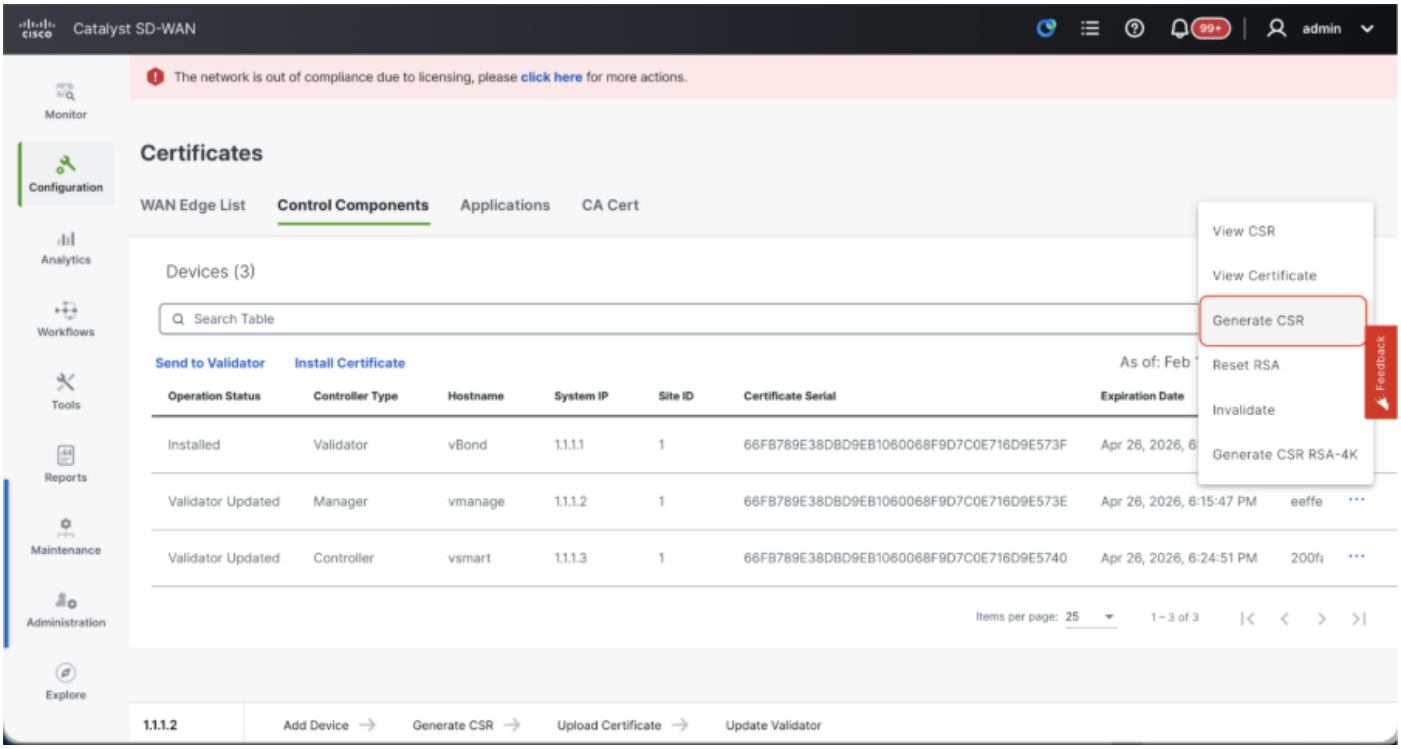


3. WAN Edge Cloud Authorization - Décide de l'autorité de certification pour les routeurs virtuels SD-WAN Edge (CSR1000v, C8000v, cloud vEdge)
    - Automatisé (vManage signed) : vManage signe automatiquement le CSR pour les routeurs de périphérie virtuels et installe le certificat sur le routeur.
    - Manuel (CA d'entreprise - recommandé) - Les routeurs virtuels utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

Dans ce cas, si nous utilisons notre propre autorité de certification, Enterprise certificate authority, sélectionnez Enterprise.



- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers
- Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de

l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.

- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.

Intégration de vBond/Validator et vSmart/Controller à vManage

Accédez à Configuration > Devices > Control Components dans le cas des noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

Intégration de vBond/Validator

- Cliquez sur Add vBond dans le cas de 20.12 vManage ou sur Add Validator dans le cas de 20.15/20.18 vManage. Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vBond qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée de l'interface CLI de vManage vers vBond IP.
- Entrez les informations d'identification utilisateur de vBond.



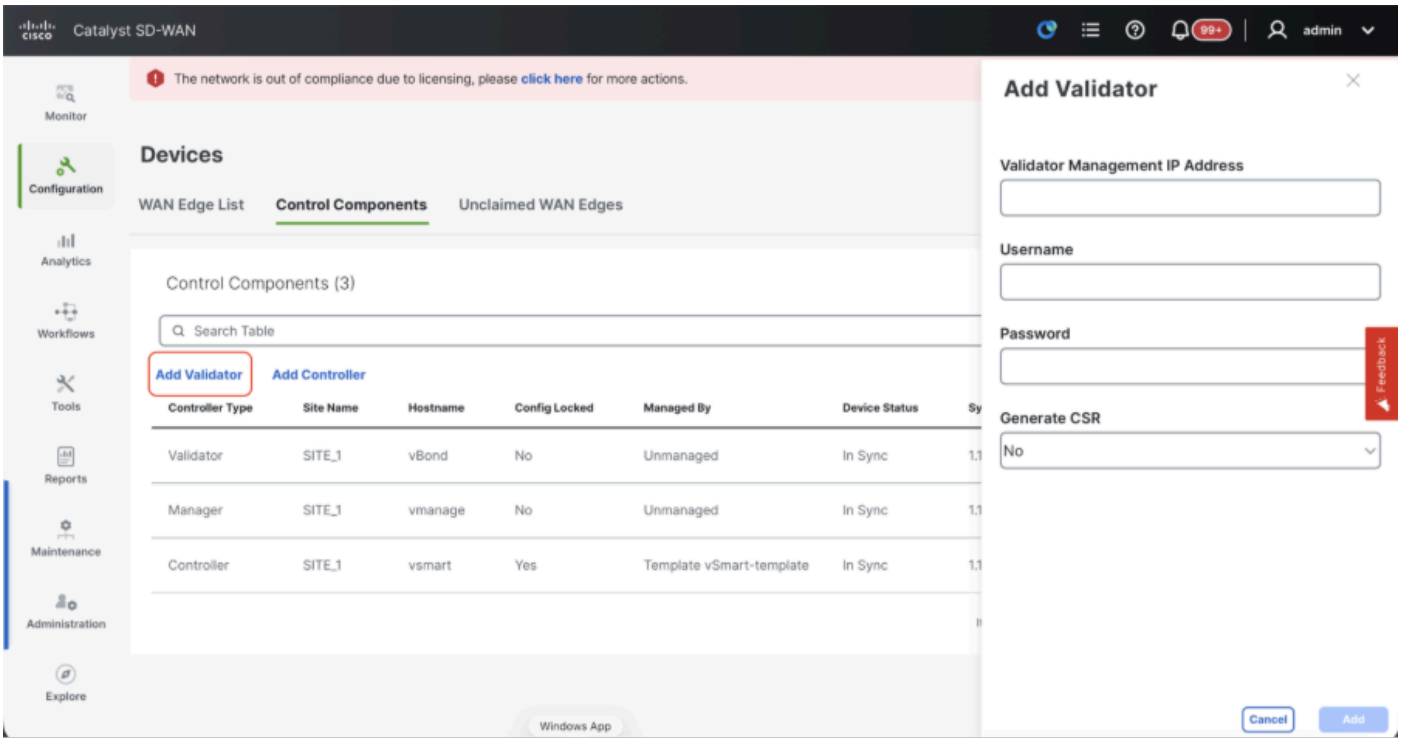
Remarque : nous devons utiliser les identifiants d'administration de vBond ou une partie utilisateur du groupe netadmin. Vous pouvez le vérifier dans l'interface de ligne de commande du vBond. Sélectionnez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vBond

---



Remarque : Si le vBond est derrière un périphérique NAT/pare-feu, vérifiez si l'adresse IP de l'interface VPN 0 de vBond est traduite en une adresse IP publique. Si l'adresse IP de l'interface VPN 0 n'est pas accessible depuis vManage, utilisez l'adresse IP publique de l'interface VPN 0 dans cette étape

---



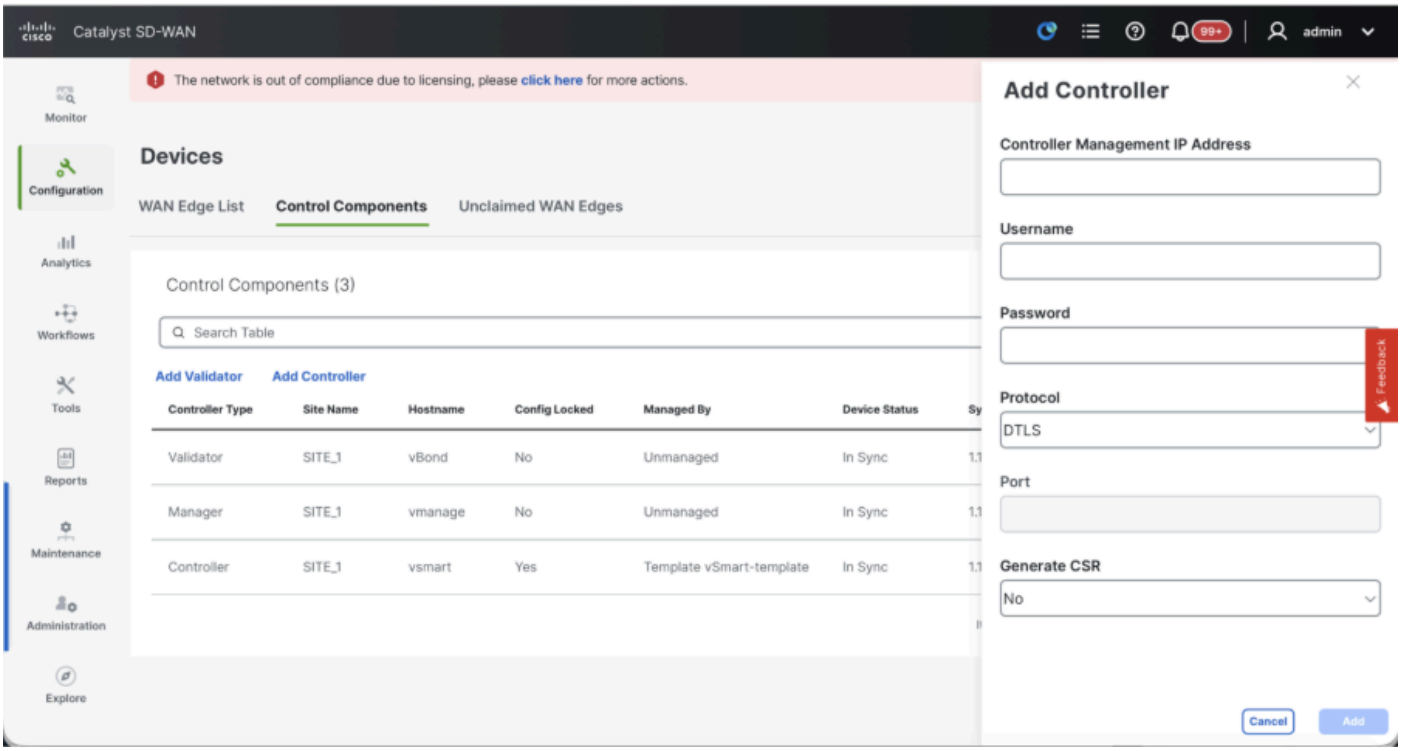
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vBond.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il existe plusieurs vBonds, répétez les mêmes étapes.

Intégration de vSmart/Controller :

- Cliquez sur Add vSmart dans le cas de vManage 20.12 ou sur Add Controller dans le cas de vManage 20.15/20.18.
- Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vSmart qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée depuis l'interface CLI de vManage vers vSmart IP.
- Entrez les informations d'identification de l'utilisateur de vSmart. Notez que nous devons utiliser les informations d'identification d'administration de vSmart ou d'une partie utilisateur du groupe netadmin.

- Vous pouvez le vérifier dans l'interface de ligne de commande du vSmart.
- Définissez le protocole sur TLS, si nous avons l'intention d'utiliser TLS pour les routeurs afin d'établir des connexions de contrôle avec vSmart. Cette configuration doit également être configurée sur l'interface de ligne de commande des noeuds vSmarts et vManage.
- Choisissez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vSmart.

Remarque : si le vSmart est derrière le périphérique/pare-feu NAT, vérifiez si l'adresse IP de l'interface VPN 0 vSmart est traduite en une adresse IP publique, et si l'adresse IP de l'interface VPN 0 n'est pas accessible à partir de vManage, utilisez l'adresse IP publique de l'adresse IP de l'interface VPN 0 dans cette étape.

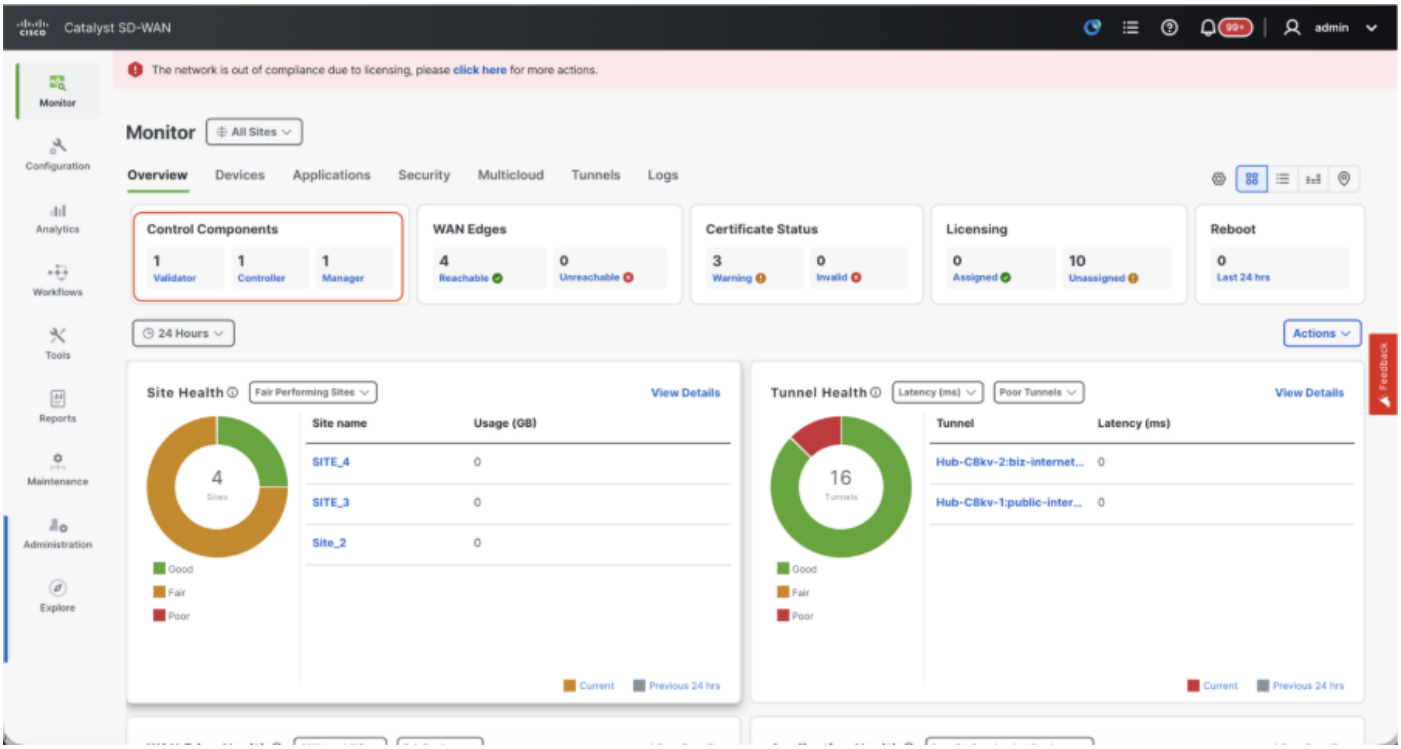


- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vSmart.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.

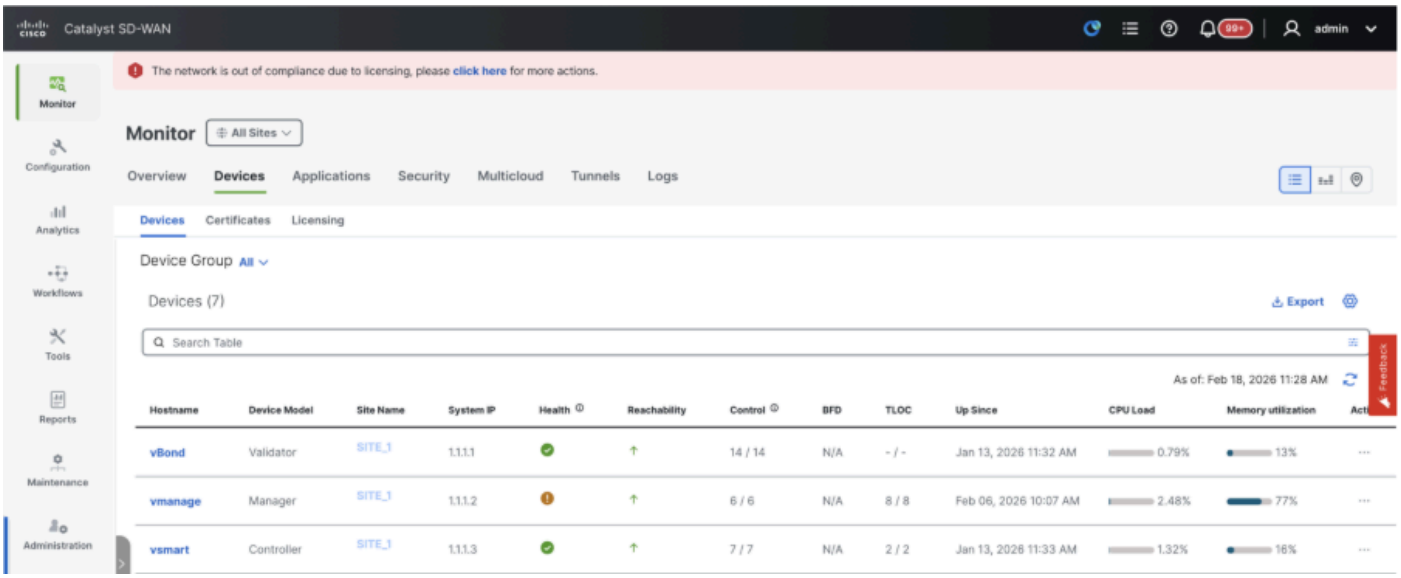
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il y a plusieurs vSmarts, répétez les mêmes étapes.

Vérification

Une fois toutes les étapes terminées, vérifiez que tous les composants de contrôle sont accessibles dans Monitor > Dashboard



- Cliquez sur les composants de contrôle respectifs et vérifiez qu'ils sont tous accessibles.
- Accédez à Monitor > Devices et vérifiez que tous les composants de contrôle sont accessibles.



Étape 3: Créer un cluster vManage

Structure SD-WAN intégrée avec un cluster vManage dans la superposition SD-WAN

Remarque : le cluster vManage peut être configuré avec 3 noeuds vManage ou 6 noeuds vManage en fonction du nombre de sites intégrés au fabric SD-WAN

Intégrer tous les contrôleurs SD-WAN avec un seul noeud vManage

Suivez les étapes décrites dans la section « Contrôleurs SD-WAN intégrés avec un seul noeud vManage dans la superposition SD-WAN » pour commencer par activer le fabric SD-WAN avec un noeud vManage et intégrer tous les validateurs (vBond) et contrôleurs (vSmart) requis.

Configurez les configurations CLI de tous les noeuds vManage qui font partie du cluster

- Configurez le reste des noeuds vManage. Dans le cas d'un cluster de 3 noeuds, vous avez 2 noeuds restants à configurer, dans le cas d'un cluster de 6 noeuds, vous avez 5 noeuds à

configurer.

- Configurez les configurations système comme indiqué :

```
config t
system
 host-name             <hostname>
 system-ip             <unique system-ip>
 site-id               <site-id>
 organization-name     <organization name>
 vbond <IP address/URL of vBond>
commit
```



Remarque : si nous utilisons une URL comme adresse vBond, assurez-vous de configurer les adresses IP du serveur DNS dans la configuration VPN 0 ou assurez-vous qu'elles peuvent être résolues.

Ces configurations sont nécessaires pour activer l'interface de transport utilisée pour établir des connexions de contrôle avec les routeurs et le reste des contrôleurs.

```
config t
vpn 0
 dns <IP-address> primary
 dns <IP-address> secondary
 interface eth1
  ip address <IP-address/mask>
  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 <default-gateway IP>
commit
```

Configurez également l'interface de gestion du VPN 512 pour activer l'accès de gestion hors bande au contrôleur.

```
Conf t
```

```
vpn 512
 interface eth0
  ip address <IP-address/mask>
  no shutdown
 !
 ip route 0.0.0.0/0 <default-gateway IP>
!
Commit
```

Configuration facultative :

- Vous pouvez vous référer aux configurations de votre contrôleur existant et si la configuration listée ici est présente, vous pouvez ajouter cette configuration aux nouveaux contrôleurs.
- Configurez le protocole de contrôle comme TLS uniquement si les routeurs doivent établir des connexions de contrôle sécurisées avec les noeuds vManage à l'aide de TLS. Par défaut, tous les contrôleurs et routeurs établissent une connexion de contrôle à l'aide de DTLS. Il s'agit d'une configuration facultative requise uniquement sur les noeuds vSmart et vManage, en fonction de vos besoins.

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

Configurer l'interface de service sur tous les noeuds vManage

Configurez l'interface de service sur tous les noeuds vManage, y compris vManage-1 qui a déjà été intégré. Cette interface est utilisée pour la communication de cluster, ce qui signifie la communication entre les noeuds vManage dans le cluster.

```
conf t
 interface eth2
  ip address <IP-address/mask>
  no shutdown
commit
```

Assurez-vous que le même sous-réseau IP est utilisé pour l'interface de service sur tous les noeuds du cluster vManage.

Configurer les identifiants de cluster

Nous pouvons utiliser les mêmes informations d'identification d'administration des noeuds vManage pour configurer le cluster vManage. Sinon, nous pouvons configurer une nouvelle information d'identification d'utilisateur qui fait partie du groupe netadmin. Les configurations permettant de configurer de nouvelles informations d'identification utilisateur sont les suivantes :

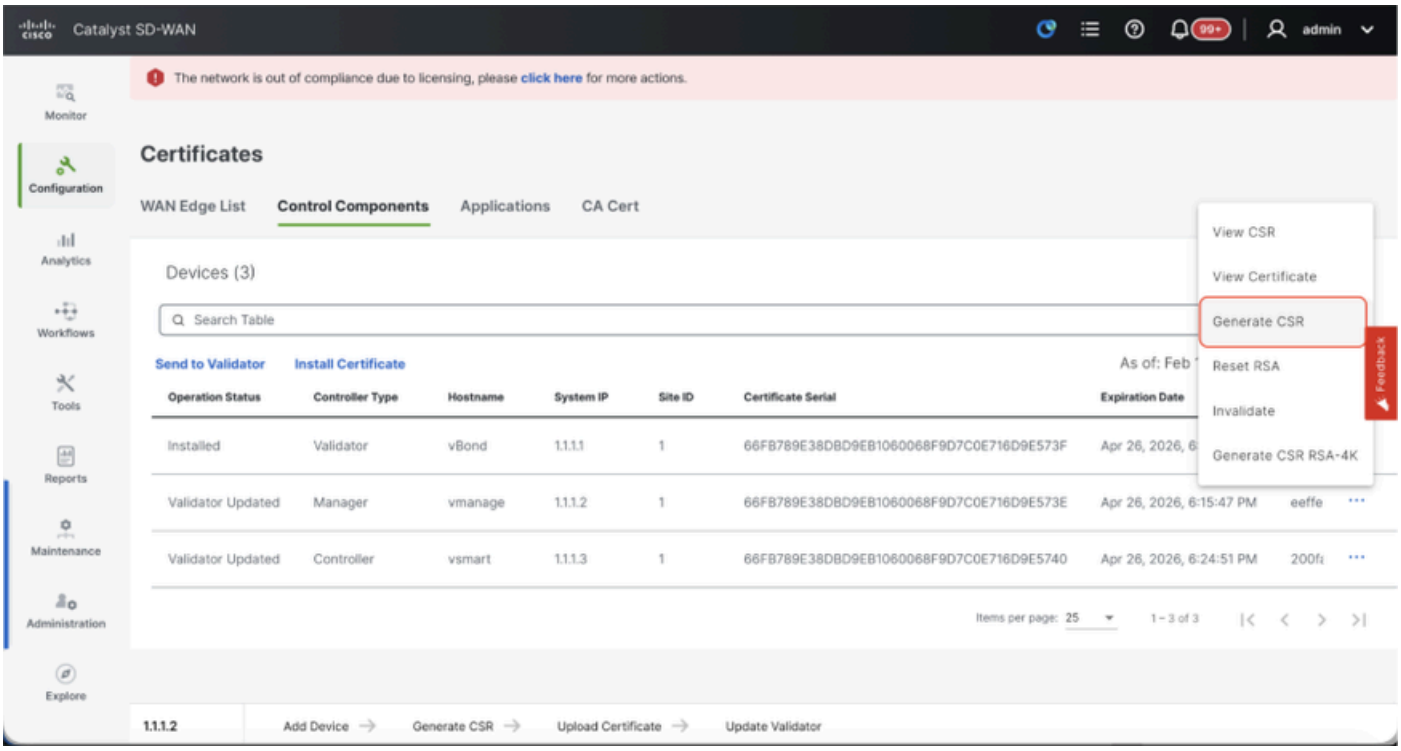
```
conf t
system
 aaa
  user <username>
   password <password>
   group    netadmin
commit
```

Assurez-vous de configurer les mêmes informations d'identification d'utilisateur sur tous les noeuds vManage qui font partie du cluster. Si nous décidons d'utiliser les informations d'identification d'administrateur, il doit s'agir du même nom d'utilisateur/mot de passe sur tous les noeuds vManage.

Installer le certificat de périphérique sur tous les noeuds vManage

- Connectez-vous à l'interface utilisateur vManage de tous les noeuds vManage à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

  Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- Effectuez cette étape sur tous les noeuds vManage qui font partie du cluster.

Préparation de la création du cluster vManage

- Dans l'interface utilisateur web de vManage-1, accédez à Administration > Cluster Management, cliquez sur ... sous Actions pour vManage-1, choisissez Edit.
- Le personnage du noeud est choisi automatiquement en fonction du personnage que nous avons choisi lors de la mise sous tension de la VM.

Remarque : Dans le cas d'un cluster à 3 noeuds, les 3 noeuds vManage sont présentés avec compute+data comme personnage.

- Pour un cluster à 6 noeuds, 3 noeuds vManage sont activés avec calcul+données comme personnage et 3 noeuds vManage avec données comme personnage.
- Dans la liste déroulante de l'adresse IP du gestionnaire, assurez-vous de choisir l'adresse IP de l'interface de service du vManage.
- Entrez le nom d'utilisateur et le mot de passe que vous souhaitez utiliser pour activer le cluster vManage, appelé informations d'identification du cluster.
- Comme mentionné précédemment, les mêmes informations d'identification doivent être configurées sur tous les noeuds vManage et doivent être utilisées lors de l'ajout de tous les noeuds au cluster.

Configuration facultative :

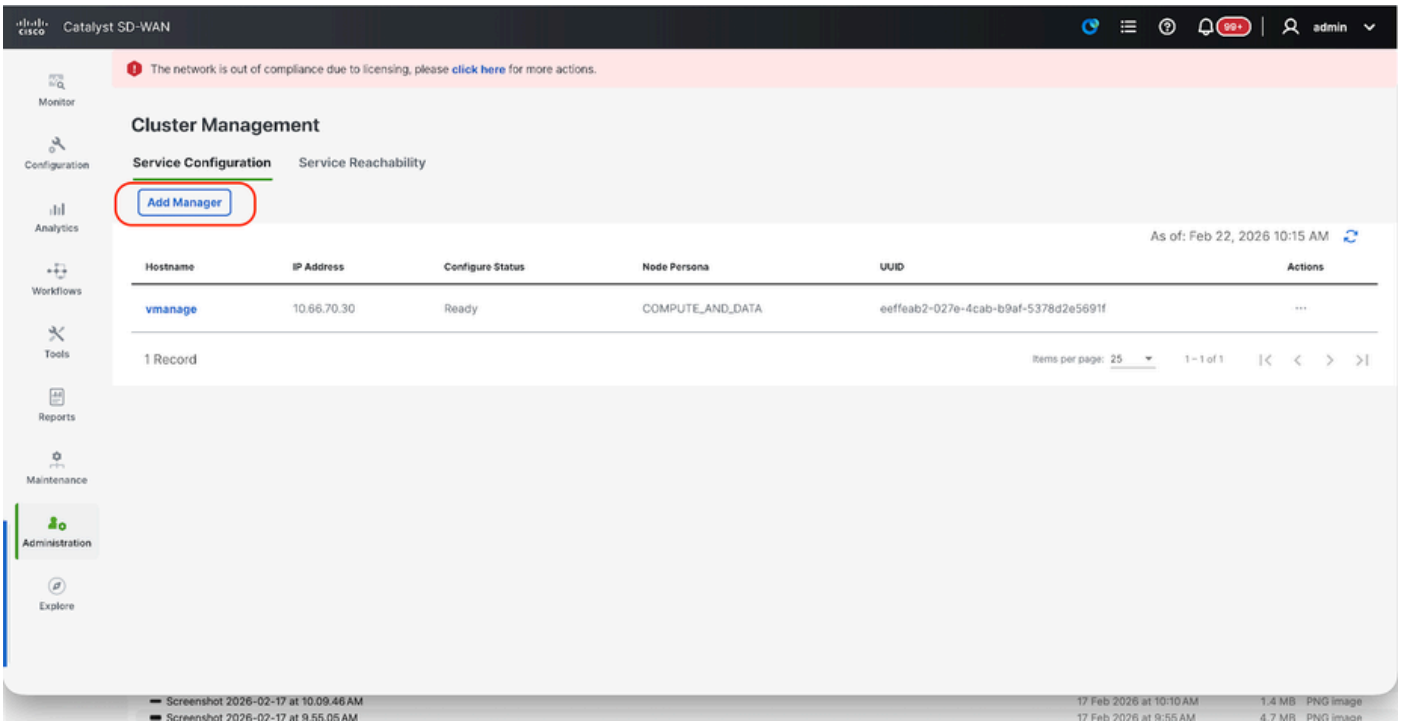
Reportez-vous à cette configuration dans votre cluster existant pour Activer SDAVC - Nécessaire d'être coché seulement si elle est requise et n'est nécessaire que sur un noeud vManage du cluster.

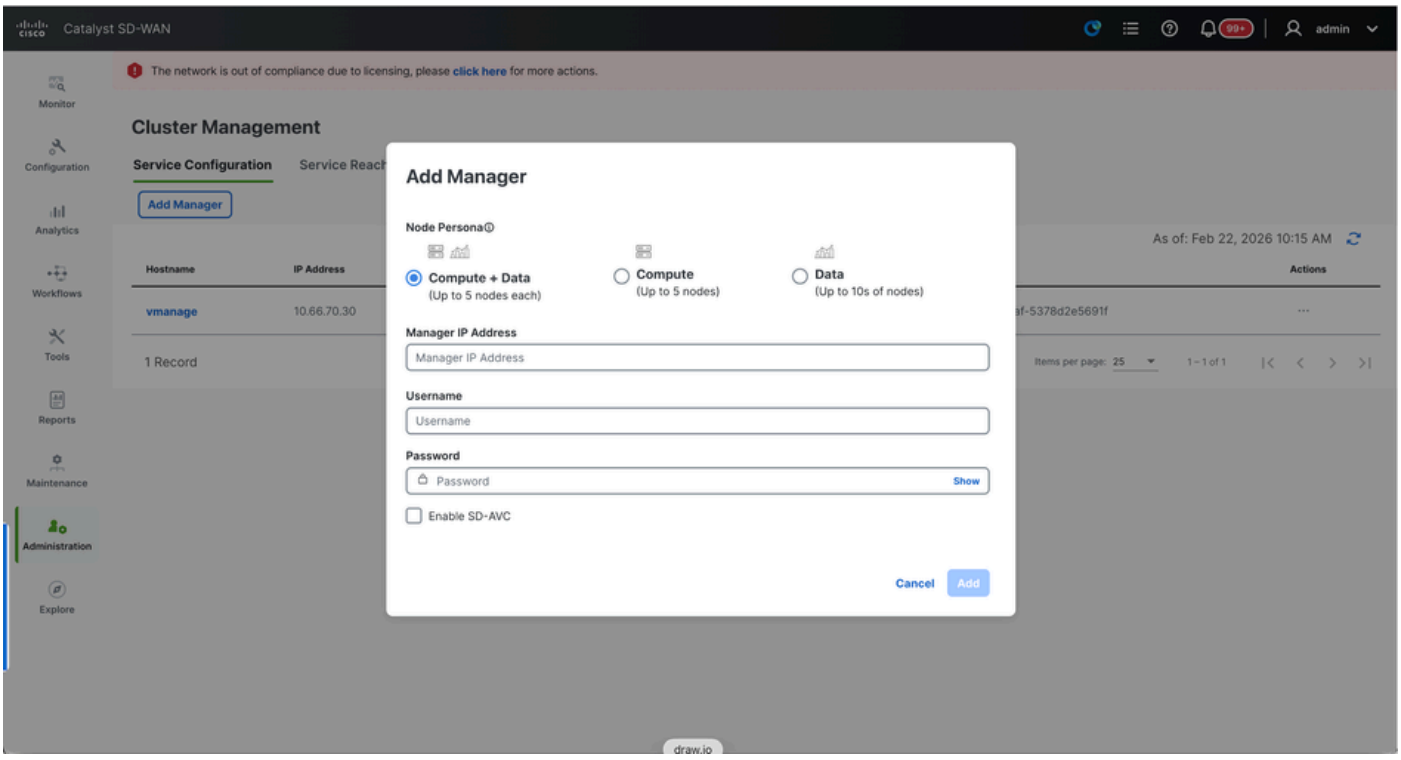
Cliquez sur Update.

- Publiez ceci, les services vManage NMS redémarrent en arrière-plan et l'interface utilisateur n'est pas disponible pendant quelques minutes d'environ 5 à 10 minutes. Pendant ce temps, l'accès CLI de vManage est disponible.
- Une fois que l'interface utilisateur de vManage-1 est accessible, accédez à Administration > Cluster Management, assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et que la personnalité du noeud est reflétée correctement. Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles.
- Si l'un des services n'est pas encore accessible, veuillez patienter. Cela prend généralement entre 20 et 30 minutes.

Créer le cluster vManage

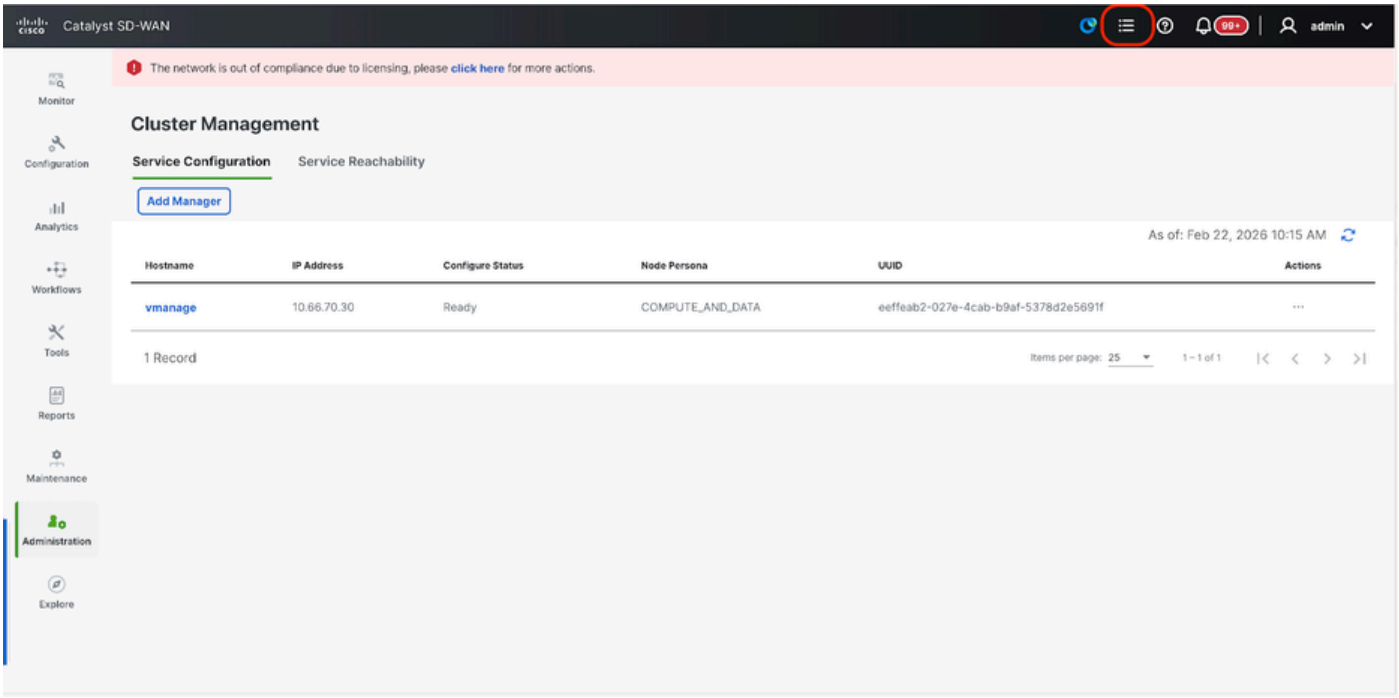
- Sur l'interface utilisateur web de vManage-1, accédez à Administration > Cluster Management, dans la section Configuration du service,
- Cliquez sur Add Manager, une fenêtre contextuelle s'affiche :





- Choisissez le personnage de noeud en fonction des configurations de personnage effectuées pendant que le noeud vManage - 2 a été lancé.
- Entrez l'adresse IP de l'interface de service de vManage-2 sous l'adresse IP du gestionnaire
- Saisissez le nom d'utilisateur et le mot de passe, qui sont les mêmes informations d'identification que celles utilisées à l'étape 6.
- Enable SDAVC (Activer SDAVC) : cette case n'est pas cochée, car elle est déjà activée sur vManage-1
- Cliquez sur Ajouter.

- Dans ce message, les services vManage NMS redémarrent en arrière-plan pour les noeuds vManage 1 et 2. L'interface utilisateur n'est pas disponible pendant quelques minutes, de l'ordre de 5 à 10 minutes pour vManage 1 et 2.
- Pendant ce temps, l'accès CLI de vManage 1 et 2 est disponible.
- Une fois que l'interface utilisateur de vManage-1 est accessible, accédez à Administration > Cluster Management, assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et node persona est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles pour les deux noeuds vManage.
- Si l'un des services n'est pas encore accessible, veuillez patienter. Cela prend généralement entre 5 et 10 minutes.
- Vous pouvez vérifier l'état du processus d'ajout de cluster dans la liste des tâches disponible dans l'angle supérieur droit de l'interface utilisateur vManage.



- Vous pouvez rechercher la liste des tâches actives et si la tâche est toujours répertoriée sous Liste des tâches actives, cela indique que la tâche n'est pas encore terminée.
- Vous pouvez cliquer sur la tâche pour vérifier sa progression. Si la tâche n'est pas répertoriée dans la liste des tâches actives, passez à Terminée et vérifiez qu'elle est terminée avec succès.
- Une fois ces points validés, passez à l'étape suivante.

Ces points doivent être pris en compte avant d'ajouter le noeud suivant au cluster :

Vérifiez ces points sur toutes les interfaces utilisateur des noeuds vManage qui ont été ajoutés au cluster jusqu'à présent :

- Accédez à Monitor > Overview of vManage UI et assurez-vous que le nombre de noeuds vManage sont reflétés correctement et sont visibles accessibles en fonction du nombre de noeuds ajoutés au cluster.

- Accédez à Administration > Cluster Management et assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et node persona est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles pour les deux noeuds vManage.

- Chaque fois qu'un noeud est ajouté au cluster, les services NMS de tous les noeuds du cluster sont redémarrés, ce qui rend l'interface utilisateur de tous ces noeuds inaccessible pendant un certain temps.
- Selon le nombre de noeuds dans le cluster, la restauration de l'interface utilisateur et l'accessibilité de tous les services peuvent prendre plus de temps.
- Vous pouvez surveiller la tâche sous Liste des tâches disponible dans le coin supérieur droit de l'interface utilisateur vManage.
- Sur l'interface utilisateur vManage de chaque noeud ajouté au cluster, nous devons voir tous les routeurs, modèles et stratégies s'ils étaient disponibles dans vManage-1.
- Si ces configurations n'étaient pas présentes sur vManage-1, les vBonds et vSmarts qui ont été ajoutés à vManage-1 ainsi que les configurations Administration > Settings pour Organization-name, vBond, Certificate Authorization doivent être reflétées sur le reste des noeuds vManage ajoutés au cluster.
- Répétez les mêmes étapes pour le reste des noeuds vManage.

Étape 4: Configuration du cluster DR en veille froide

Configuration du cluster DR en veille froide

Vous pouvez activer un cluster vManage supplémentaire en suivant les étapes décrites à l'étape 3 : Créer un cluster vManage. Publiez les messages qui suivent les étapes décrites à l'étape 5 : Config-db Backup/Restore pour restaurer la sauvegarde config-db dans le cluster de secours.

Étape 5: Sauvegarde/restauration Config-db

Collecter la sauvegarde et la restauration de la base de données de configuration vManage sur un autre noeud vManage

Collecter la sauvegarde Configuration-DB :

- Dans le fabric SD-WAN actuellement utilisé, vous pouvez générer une sauvegarde de la base de données de configuration à partir du cluster vManage.
- Veuillez noter que nous devons générer une sauvegarde de la base de données de configuration uniquement sur un noeud du cluster vManage qui est le leader de la base de données de configuration.

- Pour vManage autonome, ce vManage est lui-même le leader de la base de données de configuration.
- Dans le cluster vManage, identifiez le noeud de tête configuration-db à l'aide de la commande request nms configuration-db diagnostics. Vous pouvez exécuter cette commande sur tous les noeuds du cluster vManage à 3 noeuds.
- Dans un cluster de 6 noeuds, assurez-vous d'exécuter cette commande sur les noeuds vManage où configuration-db est activé pour identifier le noeud de tête. Accédez à Administration > Gestion du cluster pour vérifier la même chose :
- Comme nous le voyons dans la capture d'écran, les noeuds configurés avec persona COMPUTE_AND_DATA ont configuration-db en cours d'exécution.

Vous pouvez vérifier la même chose à l'aide de la commande request nms configuration-db status sur l'interface de ligne de commande vManage. Le résultat est le suivant

```
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#
```

- Une fois que vous exécutez la commande request nms configuration-db diagnostics sur ces noeuds, le résultat est comme indiqué :
- Recherchez le champ mis en surbrillance pour « IsLeader ». S'il est défini sur 1, il indique que le noeud est le noeud leader et nous pouvons collecter la sauvegarde configuration-db à partir de celui-ci.

```
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     .
```

Utilisez cette commande pour collecter la sauvegarde configuration-db à partir du noeud vManage de tête de base de données de configuration identifié.

```
request nms configuration-db backup path /opt/data/backup/<filename>
```

Le résultat attendu est le suivant :

```
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#
```

- Notez les informations d'identification de configuration-db si elles ont été mises à jour.
- Si vous ne connaissez pas les informations d'identification de la base de données de configuration, contactez le TAC pour récupérer les informations d'identification de la base de données de configuration à partir des noeuds vManage existants.
- Les informations d'identification configuration-db par défaut sont username : neo4j et password : mot de passe

  Restaurer la sauvegarde Configuration-db vers un autre noeud vManage

  Copiez la sauvegarde configuration-db dans le répertoire /home/admin/ de vManage à l'aide de SCP.

  Exemple de sortie de commande 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
  ```

  Pour restaurer la sauvegarde configuration-db, nous devons d'abord configurer les informations d'identification configuration-db. Si vos identifiants configuration-db sont default(neo4j/password), nous pouvons ignorer cette étape.

  Pour configurer les informations d'identification configuration-db, utilisez la commande request nms configuration-db update-admin-user. Utilisez le nom d'utilisateur et le mot de passe de votre choix.

  Veuillez noter que le serveur d'applications de vManage est redémarré. En raison de

laquelle l'interface utilisateur vManage devient inaccessible pendant une courte période.

```
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#
```

Publication que nous pouvons poursuivre pour restaurer la sauvegarde configuration-db :

Nous pouvons utiliser la commande request nms configuration-db restore path /home/admin/< > pour restaurer la base de données de configuration dans le nouveau 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
```

Une fois la base de données de configuration restaurée, assurez-vous que l'interface utilisateur vManage est accessible. Attendez environ 5 minutes, puis essayez d'accéder à l'interface utilisateur.

Une fois connecté à l'interface utilisateur avec succès, assurez-vous que la liste des routeurs Edge, le modèle, les stratégies et toutes les autres configurations qui étaient présentes sur votre interface utilisateur vManage précédente ou existante sont reflétés sur la nouvelle interface utilisateur vManage.

Mise en garde : La base de données de configuration restaurée contient toujours le ou les gestionnaires SD-WAN à partir desquels la sauvegarde a été effectuée. Elles sont répertoriées en tant qu'entrées Manager dans Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) mais ne sont pas membres de Administration > Cluster Management. Jusqu'à leur suppression à l'étape 6 :

- chaque rapport Send to Validator signale Failed to find Vmanage Cluster node for uuid <uuid> for them, et
- chaque installation de certificat de contrôleur à partir de l'interface utilisateur échoue et est restaurée.

N'effectuez aucune opération de certificat de contrôleur ou d'envoi au validateur sur ce vManage avant la fin de l'étape 6. Si l'installation d'un certificat échoue, n'installez pas le même certificat à partir de l'interface de ligne de commande ; Contactez le centre d'assistance technique Cisco TAC.

Étape 6: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

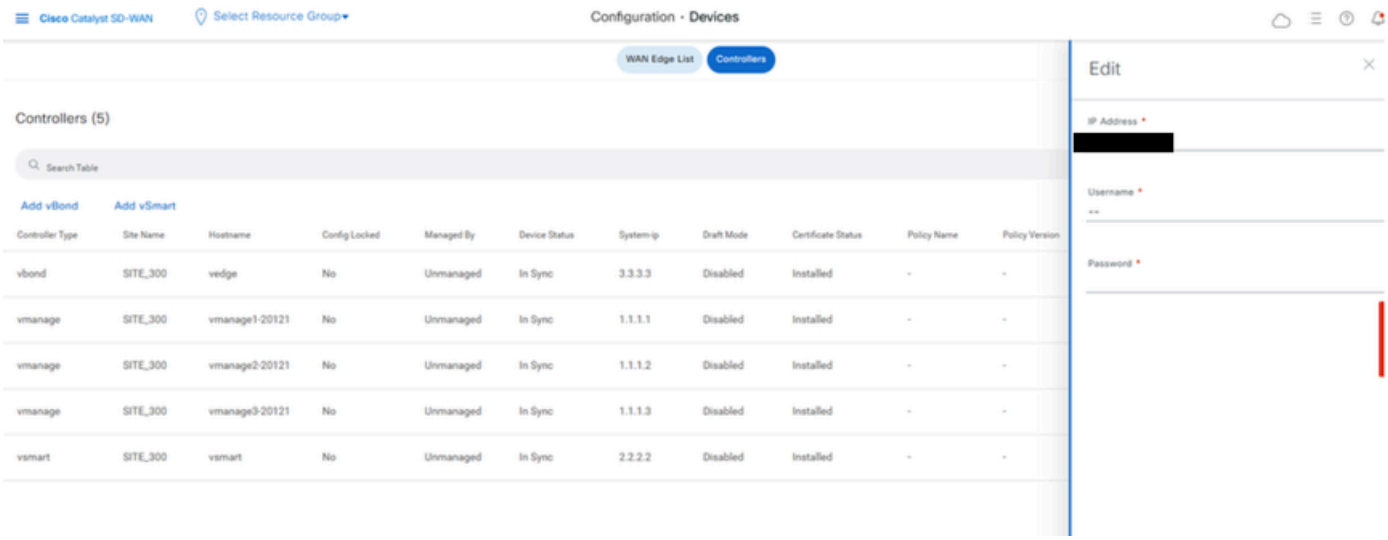
Une fois la base de données de configuration restaurée, nous devons réauthentifier tous les nouveaux contrôleurs (vmanage/vsmart/vbond) dans le fabric

---

Remarque : en production réelle, si l'interface IP utilisée pour la ré-authentification est l'interface IP du tunnel, vous devez vous assurer que le service NETCONF est autorisé sur l'interface du tunnel de vManage, vSmart et vBond, ainsi que sur les pare-feu le long du chemin. Le port de pare-feu à ouvrir est le port TCP 830 en tant que règle bidirectionnelle du cluster DR vers tous les vBonds et vSmarts .

Sur l'interface utilisateur vmanage, cliquez sur Configuration > Devices > Controllers

- Cliquez sur les trois points situés près de chaque contrôleur, puis cliquez sur Edit



- Remplacez l'adresse IP (ip système du contrôleur) par l'adresse IP du vpn de transport 0 (interface de tunnel). Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur save (enregistrer)
- Procédez de la même manière pour tous les nouveaux contrôleurs du fabric

Synchroniser la chaîne de certificats racine

Une fois tous les contrôleurs intégrés, procédez comme suit :

Sur tout serveur Cisco SD-WAN Manager du cluster nouvellement actif, effectuez les actions suivantes :

Entrez cette commande pour synchroniser le certificat racine avec tous les périphériques Cisco Catalyst SD-WAN dans le nouveau cluster actif :

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

Entrez cette commande pour synchroniser l'UUID du gestionnaire Cisco SD-WAN avec le validateur Cisco SD-WAN :

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

Supprimer les entrées précédentes du gestionnaire SD-WAN

Effectuez cette opération juste après la synchronisation root-cert-chain et avant toute opération de certificat de contrôleur ou Envoyer au validateur.

1. Ouvrez Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) et Administration > Cluster Management. Chaque entrée vManage qui n'est pas répertoriée dans Administration > Cluster Management est une entrée précédente de SD-WAN Manager et doit être supprimée.
2. Avant toute action Envoyer au validateur ou Invalider, recherchez un enregistrement de numéro de série en conflit. Accédez à https://<vmanage-url>/dataservice/certificate/vsmart/list. Aucune entrée ne peut avoir un ancien numéro de série dont le numéro de série est égal à son propre numéro de série. Cette vérification est en lecture seule. Si une telle entrée existe, arrêtez-vous et contactez le TAC Cisco : any Send to Validator or Invalidate envoie la liste des contrôleurs et ce contrôleur perdrait ses connexions de contrôle.
3. Accédez à Monitor > Tasks et ouvrez la dernière tâche Push vSmart List. Examiner uniquement les résultats des tâches existantes ; ne cliquez pas ici sur Envoyer au validateur. Si aucune tâche récente n'est répertoriée, attendez la diffusion de la liste en début d'heure suivante. Chaque entrée précédente du gestionnaire SD-WAN doit indiquer Failed to find Vmanage Cluster node for uuid <uuid>. Si un uuid vManage a été envoyé avec succès, il est membre actif de ce cluster : ne l'invalidez pas.
4. Cliquez sur les trois points à droite de la première entrée précédente du gestionnaire SD-WAN, puis cliquez sur Invalidate. Attendez la fin de la tâche. Le résultat attendu est Success with warning, avec cet exercice :

```
Invalidating Root Certificate Autority of vManage-<uuid>
Sending serial number of vManage-<uuid> as invalid to all controllers
Failed to push serial list to vManage-<uuid> - retry in 30 seconds; Failed to find Vmanage Cluster node
Updated serial list will be sent to vManage-<uuid> when it is reachable
Clearing certificate on vManage-<uuid>
Successfully invalidated vManage-<uuid>
```

L'entrée affiche désormais No certificate installed. Le numéro de série précédent du gestionnaire SD-WAN et l'autorité de certification racine sont supprimés des validateurs.

5. Cliquez sur les trois points de la même entrée, puis cliquez à nouveau sur Invalider. Il se termine immédiatement, sans tâche, et l'entrée est supprimée.
6. Répétez les étapes 4 et 5 pour chaque entrée précédente du gestionnaire SD-WAN.
7. Cliquez sur Envoyer au validateur. Le résultat attendu est Success pour chaque destinataire dans quelques secondes, avec no Failed to find Vmanage Cluster node.

Invalider les anciens contrôleurs

Une fois que le fabric est restauré et que les sessions de contrôle et BFD sont actives pour tous les bords et contrôleurs du fabric, invalidez les anciennes entrées vBond/Validator et vSmart/Controller de l'interface utilisateur :

- Sur l'interface utilisateur de vManage, accédez à Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificats > Contrôleurs).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Invalidate.
- Cliquez sur Send to Validator (Send to vBond in 20.9/20.12). Il doit indiquer le succès de chaque destinataire.
- Accédez à Configuration > Devices > Control Components (20.9/20.12 : Configuration > Devices > Controllers).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Delete.

Étape 7: Activation de la veille (et restauration)

Effectuez cette étape chaque fois que la veille devient active, et à nouveau dans la direction opposée lors du re-basculement.

1. Effectuez une sauvegarde de la base de données de configuration sur le cluster/vManage actif, copiez-la en veille et restaurez-la comme décrit à l'étape 5 : request nms configuration-db restore path /home/admin/<fichier>.tar.gz. Patientez jusqu'à la restauration de la base de données.
2. Isolez le cluster/vManage précédemment actif (arrêtez son interface de transport VPN 0 ou mettez-le hors tension).
3. Activez l'interface de transport VPN 0 sur le routeur de secours.
4. Cochez show control connections et show control connections-history sur le mode veille. Si les validateurs le rejettent avec CRTREJSER, son numéro de série n'est plus sur les validateurs (attendu après que les entrées précédentes du gestionnaire SD-WAN ont été supprimées de l'autre côté). Pour le réadmettre :
    - Sur le standby, accédez à Configuration > Devices > Control Components, cliquez sur les trois points sur chaque vBond/vSmart et cliquez sur Edit. Entrez l'adresse IP, le nom d'utilisateur et le mot de passe du VPN 0 de transport et cliquez sur Save. Les conditions requises pour le port 830 NETCONF / TCP à l'étape 6 s'appliquent.
    - Avant de cliquer sur Envoyer au validateur, recherchez un enregistrement de numéro de série en conflit. Accédez à https://<vmanage-url>/dataservice/certificate/vsmart/list sur le routeur de secours. Aucune entrée ne peut avoir un ancien numéro de série dont le numéro de série est égal à son propre numéro de série. Cette vérification est en lecture seule. Si une telle entrée existe, arrêtez-vous et contactez le centre d'assistance technique Cisco.
    - Cliquez sur Envoyer au validateur. Les validateurs et ce rapport vManage Success, ainsi que les formulaires de secours contrôlent les connexions en une minute environ. La transmission vers le vManage précédemment actif échoue avec Échec de la recherche du noeud de cluster Vmanage pour uuid <uuid>; c'est prévu.
5. Supprimez les entrées vManage précédemment actives avant toute opération de certificat de contrôleur :
    - Dans Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers), chaque entrée vManage non répertoriée dans

Administration > Cluster Management est une entrée SD-WAN Manager précédente.
- Vérifiez que chaque noeud de cluster Vmanage pour uuid <uuid> a échoué dans la tâche Envoyer au validateur. Si un uuid vManage a été envoyé avec succès, il est membre actif de ce cluster : ne l'invalidez pas.
- Sur chaque entrée précédente du gestionnaire SD-WAN, cliquez sur les trois points et cliquez sur Invalidate, puis attendez Success with warning. Cliquez à nouveau sur Invalidate ; l'entrée est supprimée.
- Cliquez sur Envoyer au validateur. Le résultat attendu est Success pour chaque destinataire dans quelques secondes.

6. Continuez avec les chèques postaux.

Étape 8: Valider les chèques

Remarque : Poursuivez avec la section Post Checks présentée ici, qui est commune à toutes les combinaisons de déploiement.

Combinaison 5 : Cluster vManage + DR activé

Instances nécessaires :

- 3 ou 6 vManage (cluster principal)
- 3 ou 6 vManage (cluster de secours DR)
- 1 ou plusieurs vBond (répartis entre les data centers principaux et DR)
- 1 vSmart ou plus (distribué dans les data centers principaux et DR)

Étapes:

1. Afficher toutes les instances à l'aide des étapes communes
2. Vérifications préalables
3. Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage
4. Créer un cluster vManage
5. Configuration du cluster DR en veille froide
6. Sauvegarde/restauration Config-db
7. Valider les chèques

Étape 1: Vérifications préalables

- Assurez-vous que le nombre d'instances Cisco SD-WAN Manager actives est identique au

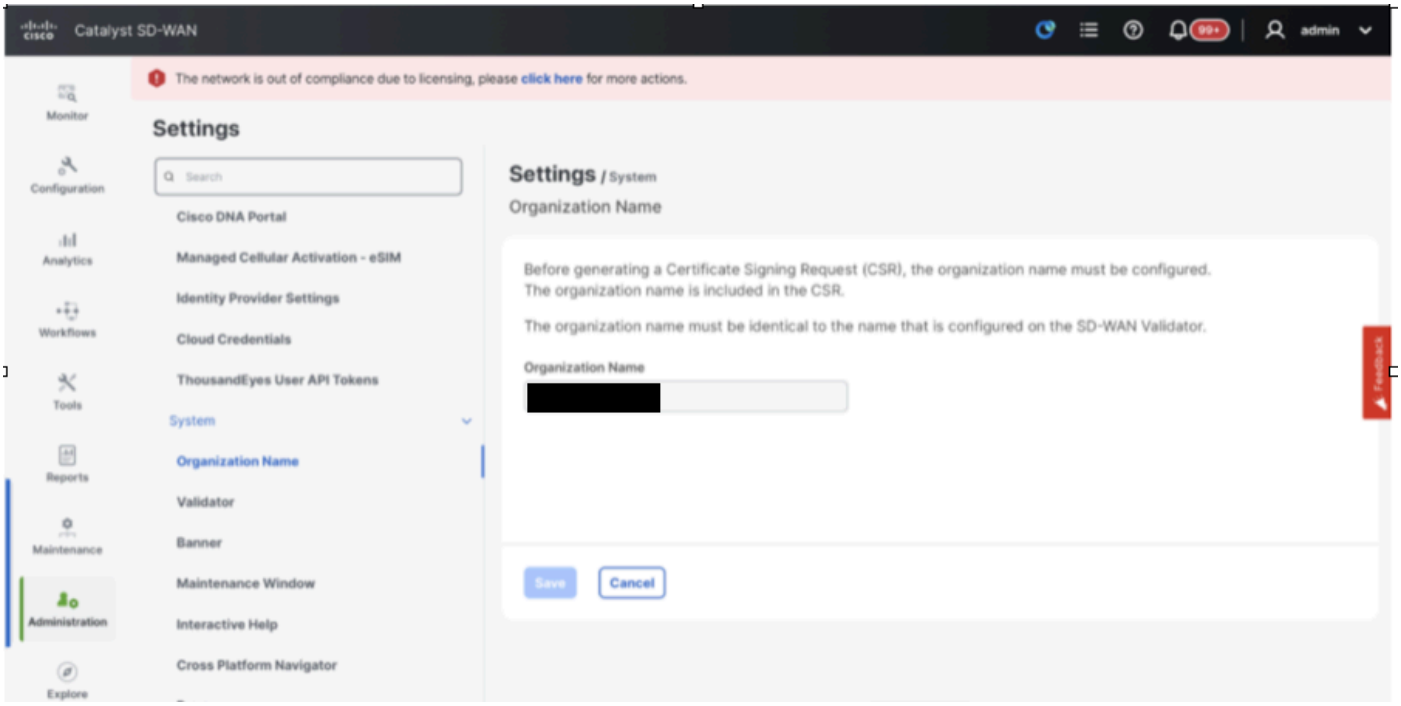
nombre d'instances Cisco SD-WAN Manager nouvellement installées.

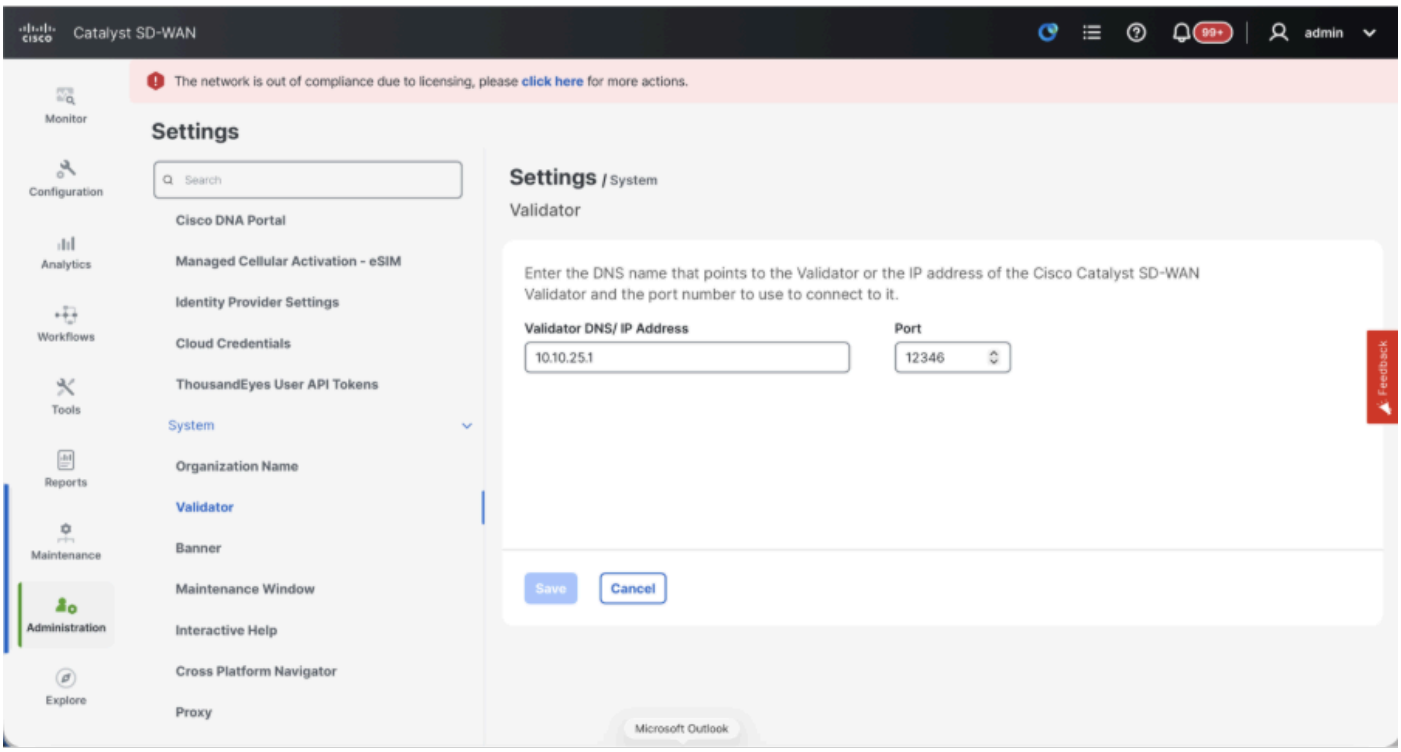
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles exécutent la même version logicielle.
- Assurez-vous que toutes les instances Cisco SD-WAN Manager actives et nouvelles sont en mesure d'atteindre l'adresse IP de gestion de Cisco SD-WAN Validator.
- Assurez-vous que les certificats ont été installés sur les instances Cisco SD-WAN Manager nouvellement installées.
- Assurez-vous que les horloges sur tous les périphériques Cisco Catalyst SD-WAN, y compris les instances Cisco SD-WAN Manager nouvellement installées, sont synchronisées.
- Assurez-vous qu'un nouvel ensemble d'IP système et d'ID de site est configuré sur les instances de Cisco SD-WAN Manager nouvellement installées, avec la même configuration de base que le cluster actif.

Étape 2: Configurer l'interface utilisateur, les certificats et les contrôleurs embarqués vManage

Mettre à jour les configurations sur l'interface utilisateur vManage

- Une fois les configurations de l'étape 1 ajoutées à l'interface de ligne de commande de tous les contrôleurs, nous pouvons accéder à l'interface utilisateur web de vManage, à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Administration > Settings et complétez ces étapes.
- Configurez le nom de l'organisation et l'adresse URL/IP du validateur/vBond. Configurez la même valeur que dans l'interface de ligne de commande du noeud vManage.
- Dans vManage 20.15/20.18, ces configurations sont disponibles dans la section Système.

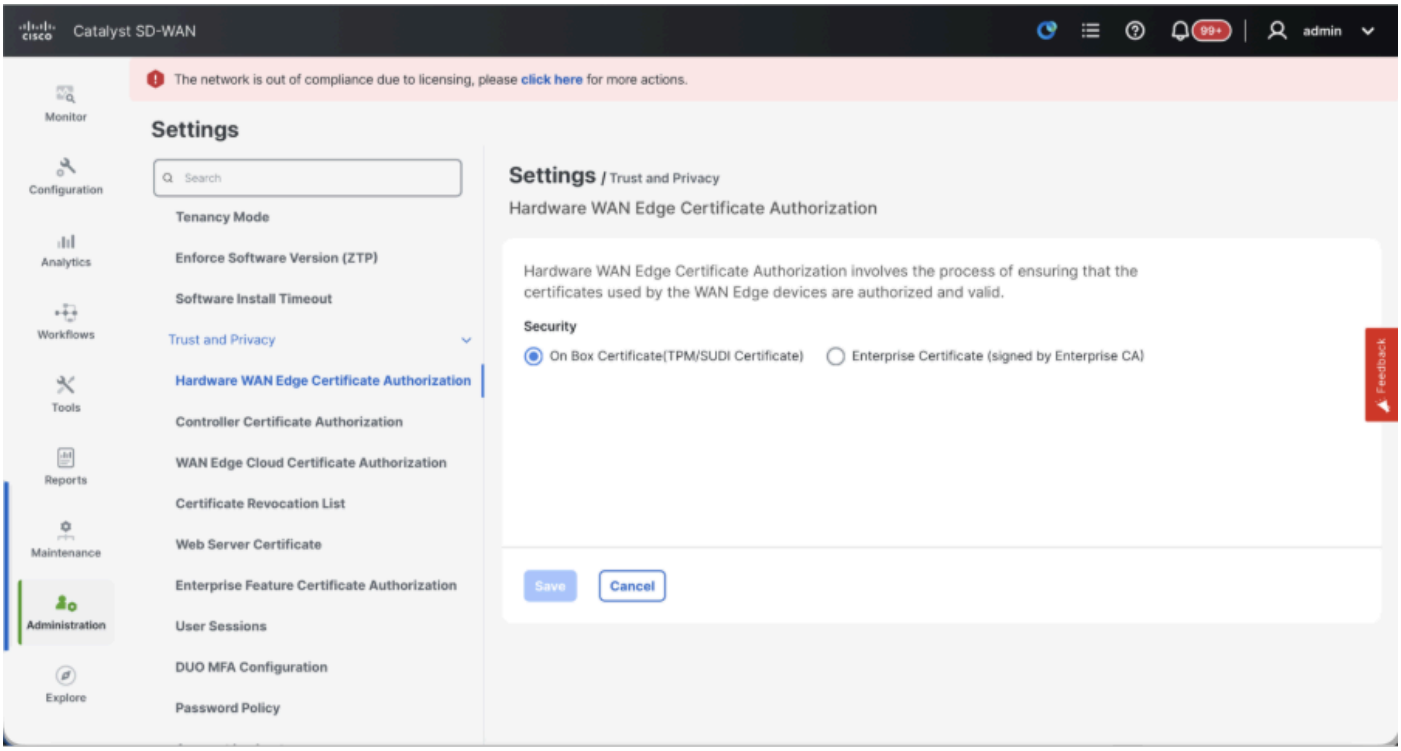




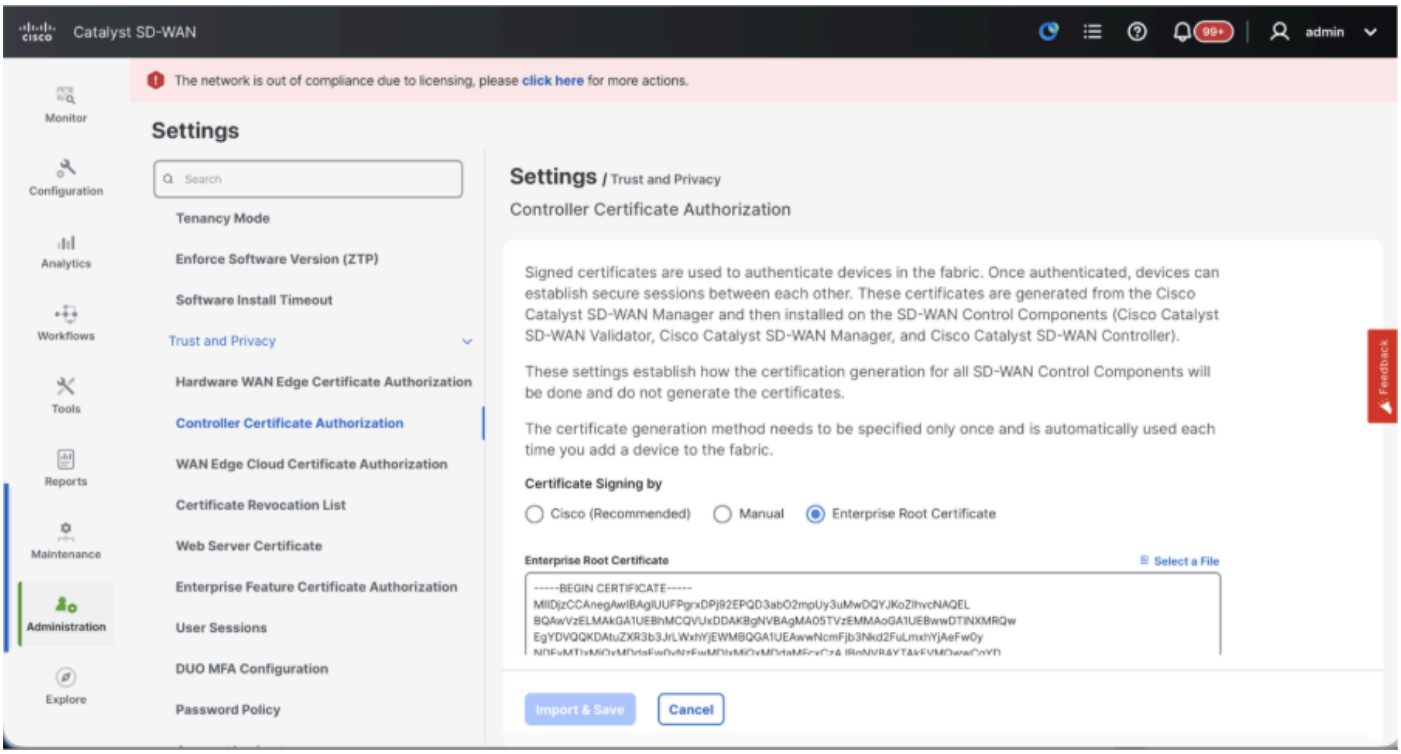
- Vérifiez les configurations de l'autorité de certification (CA), qui décide de l'autorité de certification utilisée pour signer les certificats. Nous pouvons voir 3 options ici :

1. Hardware WAN Edge Certificate Authorization : décide de l'autorité de certification pour les routeurs périphériques SD-WAN matériels.
    - Certificat On Box (certificat TPM/SUDI) : avec cette option, le certificat préinstallé sur le matériel du routeur est utilisé pour établir les connexions de contrôle (connexions TLS/DTLS)

- Certificat d'entreprise (signé par l'autorité de certification d'entreprise) : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

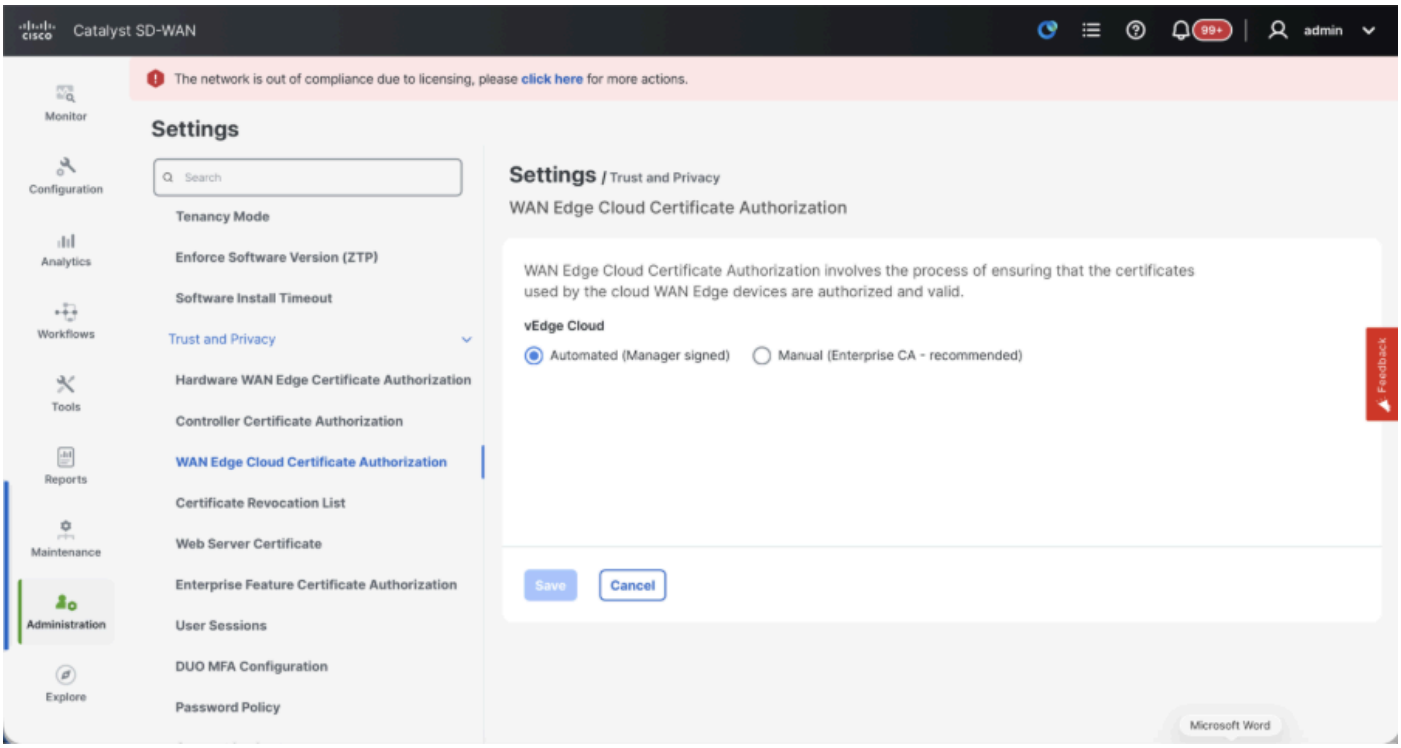


2. Autorisation de certificat de contrôleur - Décide de l'autorité de certification pour les contrôleurs SD-WAN.
    - Cisco (recommandé) : les contrôleurs utilisent les certificats signés par Cisco PKI. vManage contacte automatiquement le portail PNP à l'aide des informations d'identification de compte Smart configurées sur le vManage, obtient le certificat signé et est installé sur le contrôleur.
    - Manuel - Les contrôleurs utilisent les certificats signés par Cisco PKI. Signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
    - Certificat racine d'entreprise : avec cette option, les routeurs utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

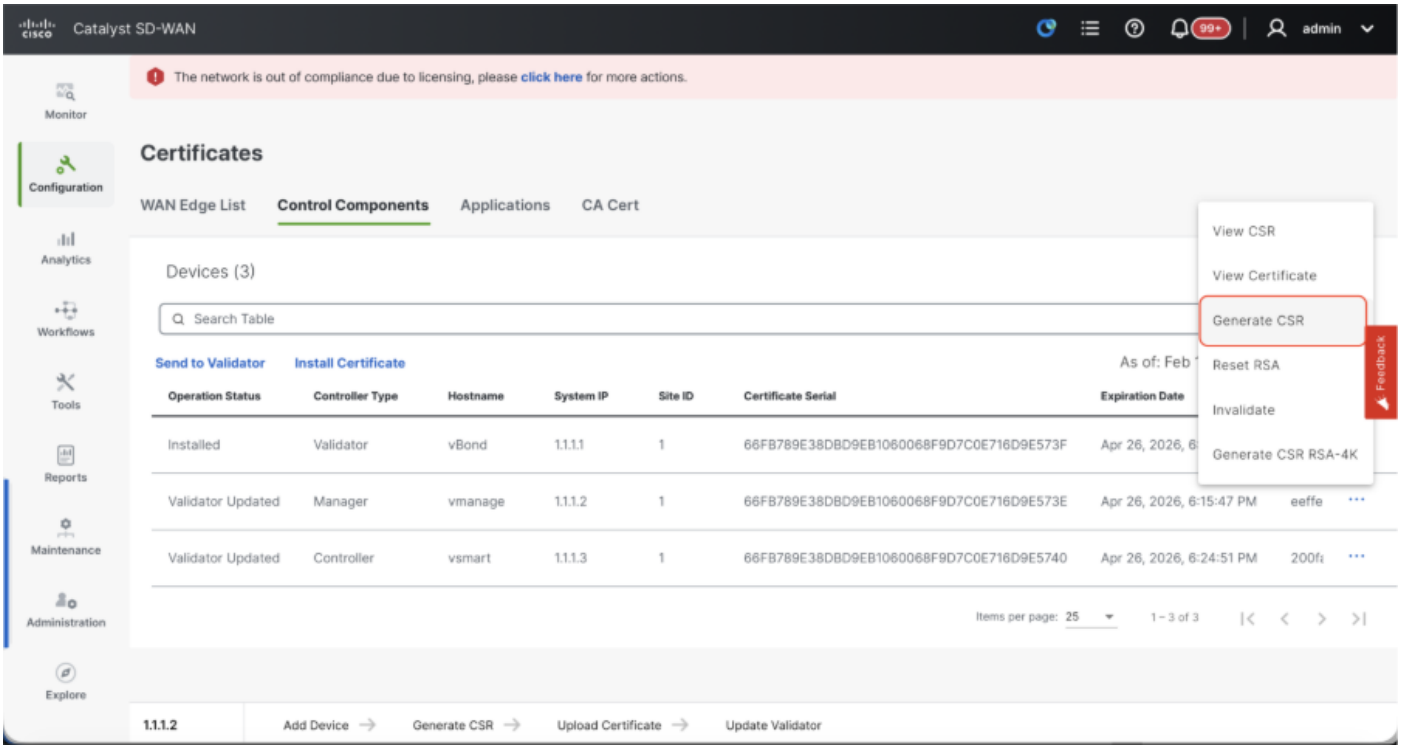


3. WAN Edge Cloud Authorization - Décide de l'autorité de certification pour les routeurs virtuels SD-WAN Edge (CSR1000v, C8000v, cloud vEdge)
    - Automatisé (vManage signed) : vManage signe automatiquement le CSR pour les routeurs de périphérie virtuels et installe le certificat sur le routeur.
    - Manuel (CA d'entreprise - recommandé) - Les routeurs virtuels utilisent des certificats signés par l'autorité de certification d'entreprise de votre organisation. Lorsque vous choisissez cette option, le certificat racine de l'autorité de certification d'entreprise doit être mis à jour ici.

Dans ce cas, si nous utilisons notre propre autorité de certification, Enterprise certificate authority, sélectionnez Enterprise.



- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers
- Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de

l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.

- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.

Intégration de vBond/Validator et vSmart/Controller à vManage

Accédez à Configuration > Devices > Control Components dans le cas des noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

Intégration de vBond/Validator

- Cliquez sur Add vBond dans le cas de 20.12 vManage ou sur Add Validator dans le cas de 20.15/20.18 vManage. Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vBond qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée de l'interface CLI de vManage vers vBond IP.
- Entrez les informations d'identification utilisateur de vBond.



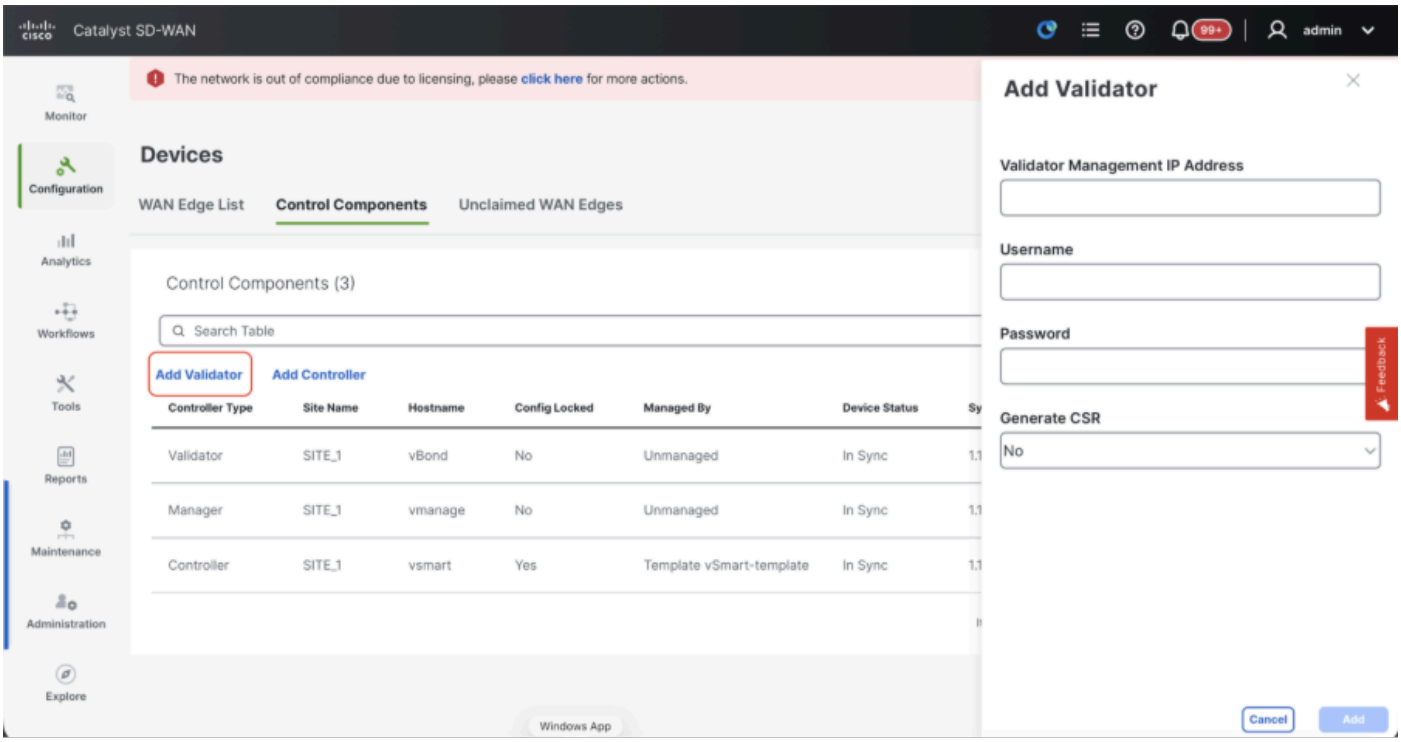
Remarque : nous devons utiliser les identifiants d'administration de vBond ou une partie utilisateur du groupe netadmin. Vous pouvez le vérifier dans l'interface de ligne de commande du vBond. Sélectionnez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vBond

---



Remarque : Si le vBond est derrière un périphérique NAT/pare-feu, vérifiez si l'adresse IP de l'interface VPN 0 de vBond est traduite en une adresse IP publique. Si l'adresse IP de l'interface VPN 0 n'est pas accessible depuis vManage, utilisez l'adresse IP publique de l'interface VPN 0 dans cette étape

---



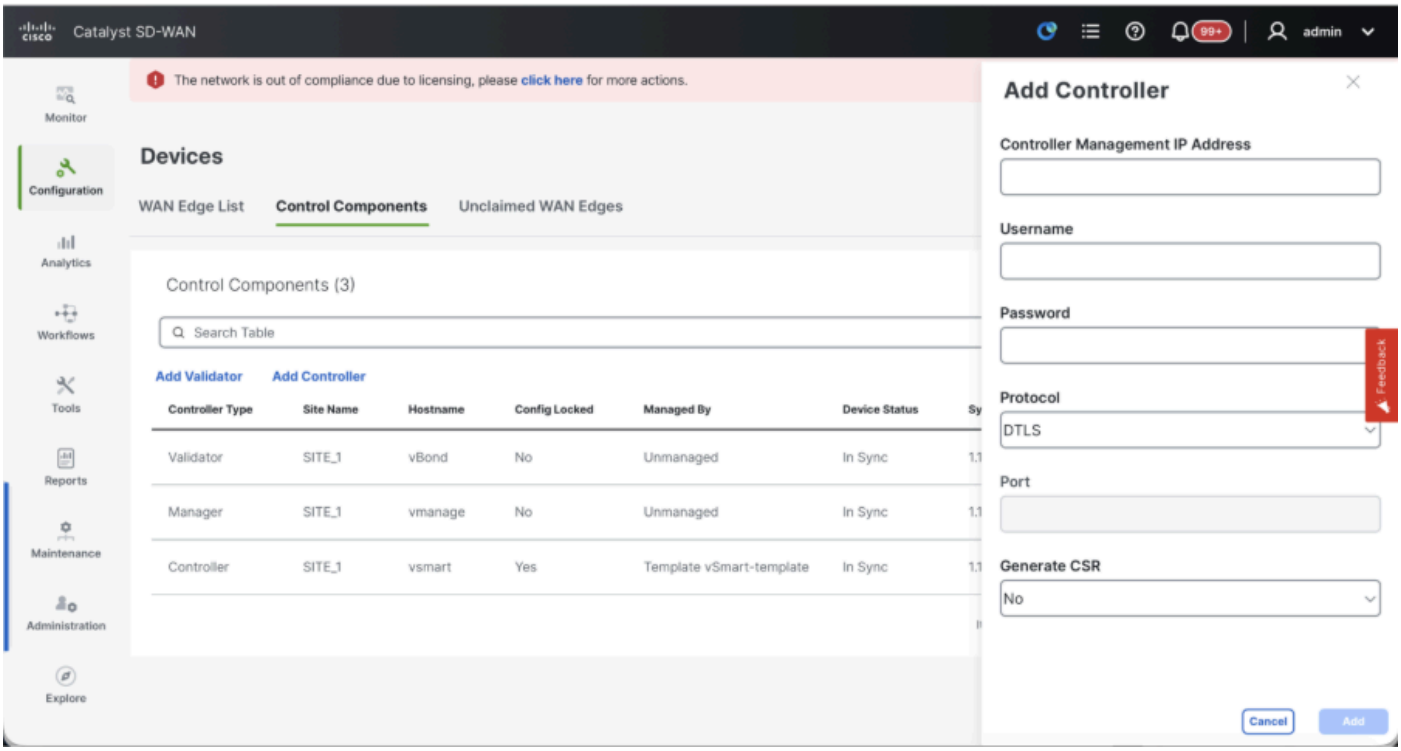
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vBond.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante. Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le. La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il existe plusieurs vBonds, répétez les mêmes étapes.

Intégration de vSmart/Controller :

- Cliquez sur Add vSmart dans le cas de vManage 20.12 ou sur Add Controller dans le cas de vManage 20.15/20.18.
- Une fenêtre contextuelle s'ouvre, entrez l'IP de transport VPN 0 de vSmart qui est accessible à partir de vManage.
- Vérifiez l'accessibilité à l'aide de la commande ping si elle est autorisée depuis l'interface CLI de vManage vers vSmart IP.
- Entrez les informations d'identification de l'utilisateur de vSmart. Notez que nous devons utiliser les informations d'identification d'administration de vSmart ou d'une partie utilisateur du groupe netadmin.

- Vous pouvez le vérifier dans l'interface de ligne de commande du vSmart.
- Définissez le protocole sur TLS, si nous avons l'intention d'utiliser TLS pour les routeurs afin d'établir des connexions de contrôle avec vSmart. Cette configuration doit également être configurée sur l'interface de ligne de commande des noeuds vSmarts et vManage.
- Choisissez Oui dans la liste déroulante de « Générer CSR » si nous devons installer un nouveau certificat pour vSmart.

Remarque : si le vSmart est derrière le périphérique/pare-feu NAT, vérifiez si l'adresse IP de l'interface VPN 0 vSmart est traduite en une adresse IP publique, et si l'adresse IP de l'interface VPN 0 n'est pas accessible à partir de vManage, utilisez l'adresse IP publique de l'adresse IP de l'interface VPN 0 dans cette étape.

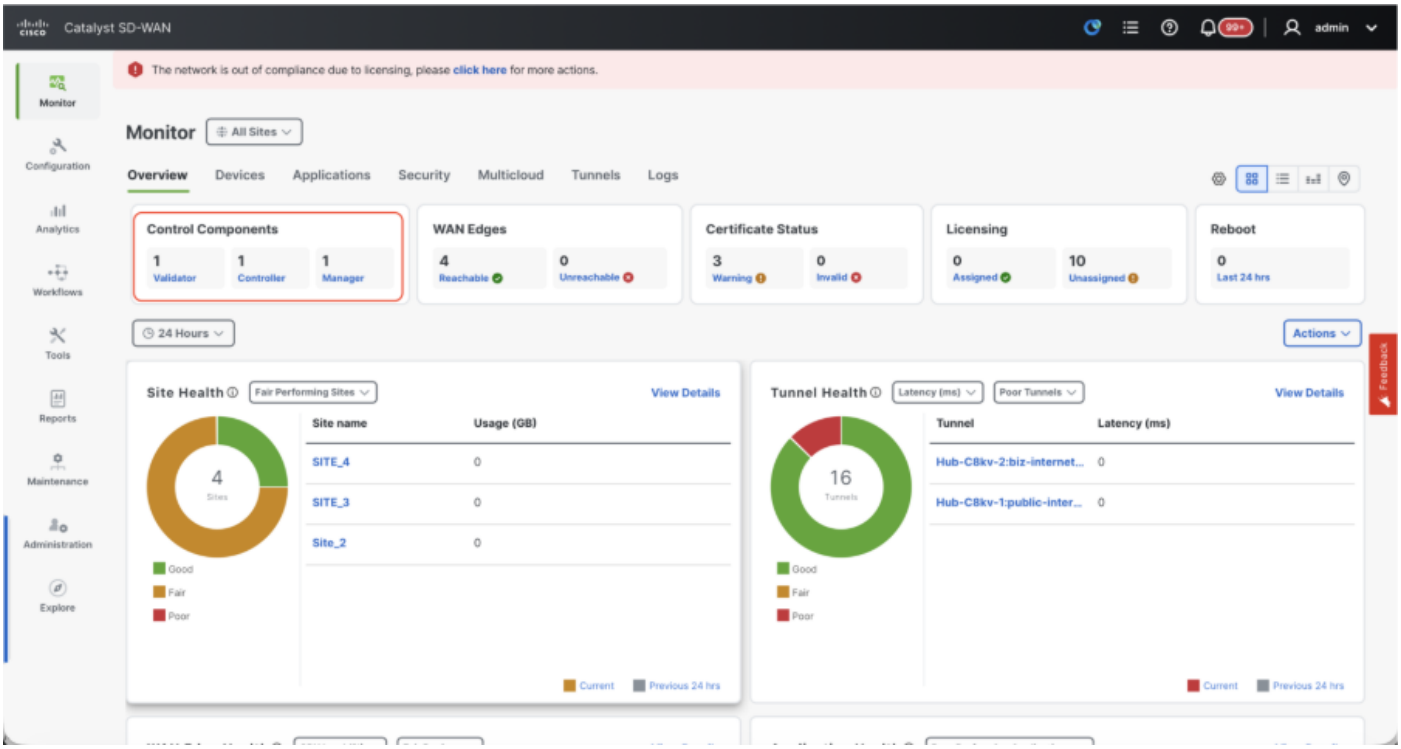


- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est automatiquement installé sur le vSmart.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.

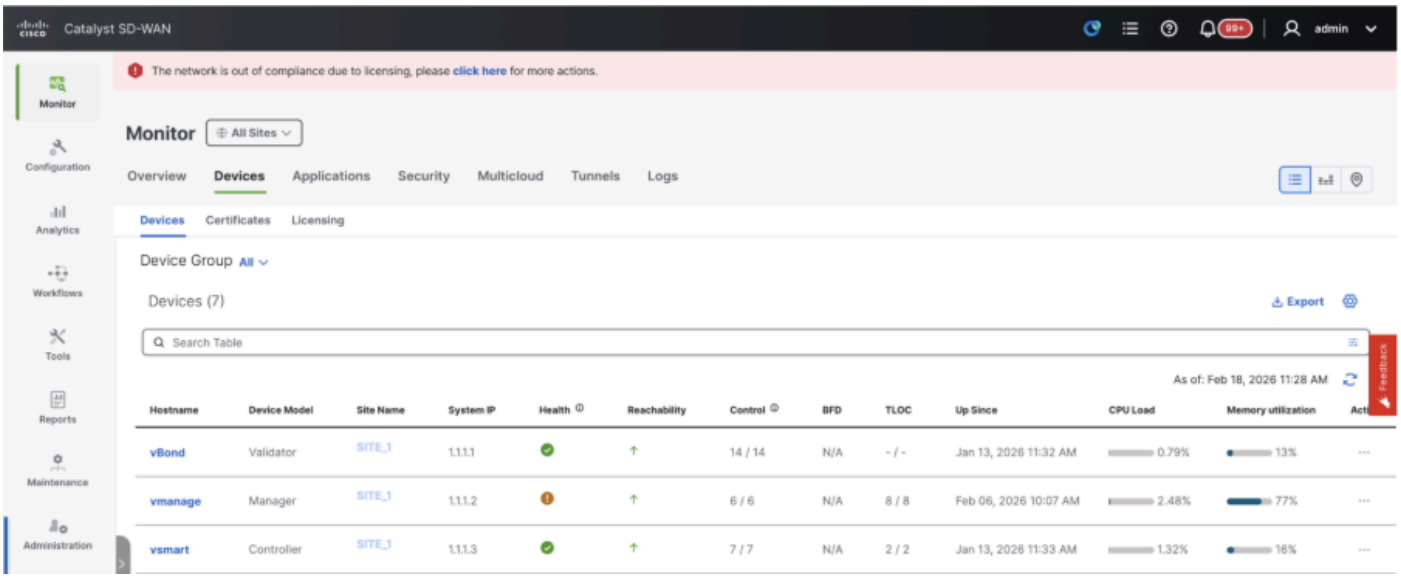
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- S'il y a plusieurs vSmarts, répétez les mêmes étapes.

Vérification

Une fois toutes les étapes terminées, vérifiez que tous les composants de contrôle sont accessibles dans Monitor > Dashboard



- Cliquez sur les composants de contrôle respectifs et vérifiez qu'ils sont tous accessibles.
- Accédez à Monitor > Devices et vérifiez que tous les composants de contrôle sont accessibles.



Étape 3: Créer un cluster vManage

Structure SD-WAN intégrée avec un cluster vManage dans la superposition SD-WAN

Remarque : le cluster vManage peut être configuré avec 3 noeuds vManage ou 6 noeuds vManage en fonction du nombre de sites intégrés au fabric SD-WAN

Intégrer tous les contrôleurs SD-WAN avec un seul noeud vManage

Suivez les étapes décrites dans la section « Contrôleurs SD-WAN intégrés avec un seul noeud vManage dans la superposition SD-WAN » pour commencer par activer le fabric SD-WAN avec un noeud vManage et intégrer tous les validateurs (vBond) et contrôleurs (vSmart) requis.

Configurez les configurations CLI de tous les noeuds vManage qui font partie du cluster

- Configurez le reste des noeuds vManage. Dans le cas d'un cluster de 3 noeuds, vous avez 2 noeuds restants à configurer, dans le cas d'un cluster de 6 noeuds, vous avez 5 noeuds à

configurer.

- Configurez les configurations système comme indiqué :

```
config t
system
 host-name             <hostname>
 system-ip             <unique system-ip>
 site-id               <site-id>
 organization-name     <organization name>
 vbond <IP address/URL of vBond>
commit
```



Remarque : si nous utilisons une URL comme adresse vBond, assurez-vous de configurer les adresses IP du serveur DNS dans la configuration VPN 0 ou assurez-vous qu'elles peuvent être résolues.

Ces configurations sont nécessaires pour activer l'interface de transport utilisée pour établir des connexions de contrôle avec les routeurs et le reste des contrôleurs.

```
config t
vpn 0
 dns <IP-address> primary
 dns <IP-address> secondary
 interface eth1
  ip address <IP-address/mask>
  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 <default-gateway IP>
commit
```

Configurez également l'interface de gestion du VPN 512 pour activer l'accès de gestion hors bande au contrôleur.

```
Conf t
```

```
vpn 512
 interface eth0
  ip address <IP-address/mask>
  no shutdown
 !
 ip route 0.0.0.0/0 <default-gateway IP>
!
Commit
```

Configuration facultative :

- Vous pouvez vous référer aux configurations de votre contrôleur existant et si la configuration listée ici est présente, vous pouvez ajouter cette configuration aux nouveaux contrôleurs.
- Configurez le protocole de contrôle comme TLS uniquement si les routeurs doivent établir des connexions de contrôle sécurisées avec les noeuds vManage à l'aide de TLS. Par défaut, tous les contrôleurs et routeurs établissent une connexion de contrôle à l'aide de DTLS. Il s'agit d'une configuration facultative requise uniquement sur les noeuds vSmart et vManage, en fonction de vos besoins.

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

Configurer l'interface de service sur tous les noeuds vManage

Configurez l'interface de service sur tous les noeuds vManage, y compris vManage-1 qui a déjà été intégré. Cette interface est utilisée pour la communication de cluster, ce qui signifie la communication entre les noeuds vManage dans le cluster.

```
conf t
 interface eth2
  ip address <IP-address/mask>
  no shutdown
commit
```

Assurez-vous que le même sous-réseau IP est utilisé pour l'interface de service sur tous les noeuds du cluster vManage.

Configurer les identifiants de cluster

Nous pouvons utiliser les mêmes informations d'identification d'administration des noeuds vManage pour configurer le cluster vManage. Sinon, nous pouvons configurer une nouvelle information d'identification d'utilisateur qui fait partie du groupe netadmin. Les configurations permettant de configurer de nouvelles informations d'identification utilisateur sont les suivantes :

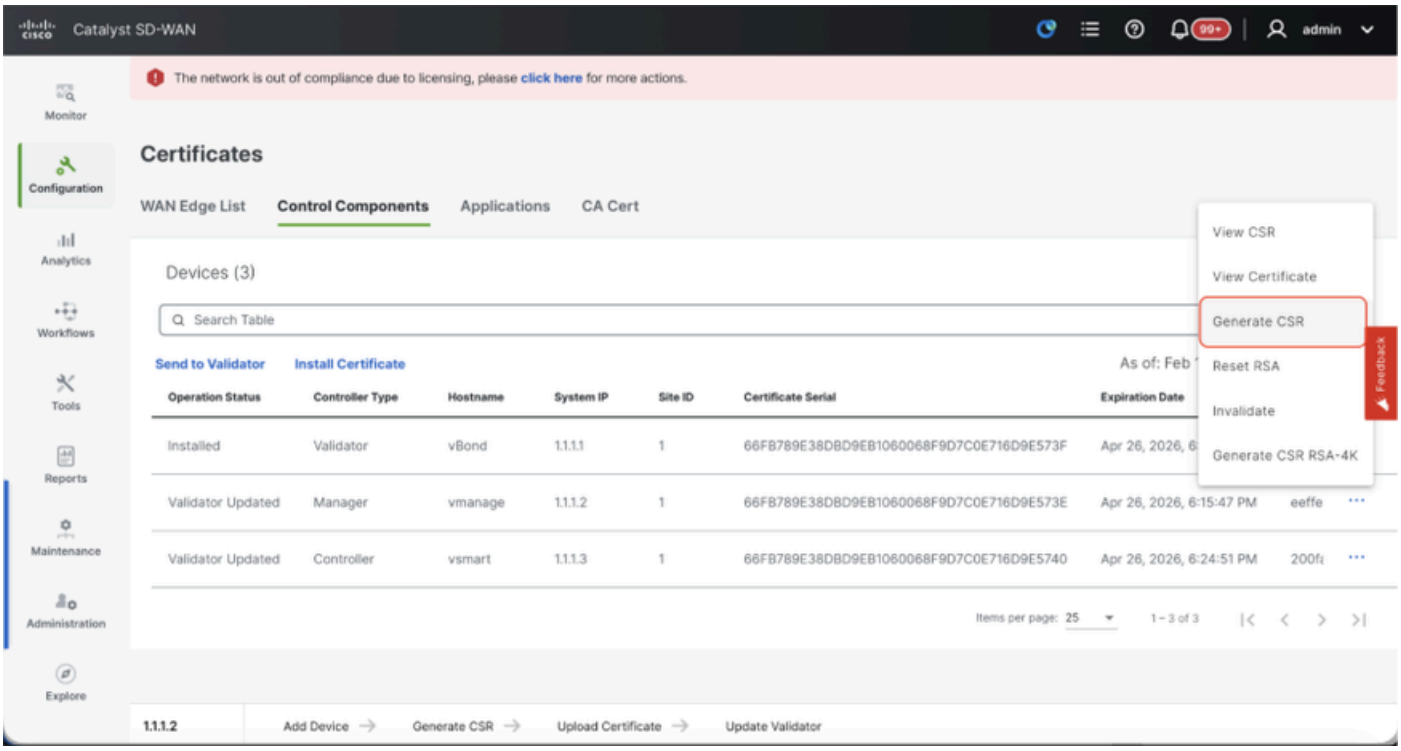
```
conf t
system
 aaa
  user <username>
   password <password>
   group    netadmin
commit
```

Assurez-vous de configurer les mêmes informations d'identification d'utilisateur sur tous les noeuds vManage qui font partie du cluster. Si nous décidons d'utiliser les informations d'identification d'administrateur, il doit s'agir du même nom d'utilisateur/mot de passe sur tous les noeuds vManage.

Installer le certificat de périphérique sur tous les noeuds vManage

- Connectez-vous à l'interface utilisateur vManage de tous les noeuds vManage à l'aide de l'URL https://<vmanage-ip> dans votre navigateur. Utilisez l'adresse IP VPN 512 des noeuds vManage respectifs. Vous pouvez vous connecter avec le nom d'utilisateur et le mot de passe admin.
- Accédez à Configuration > Certificates > Control Components en cas de noeuds vManage 20.15/20.18. Dans le cas des versions 20.9/20.12, Configuration > Devices > Controllers

  Cliquez sur ... pour Manager/vManage et cliquez sur Generate CSR.



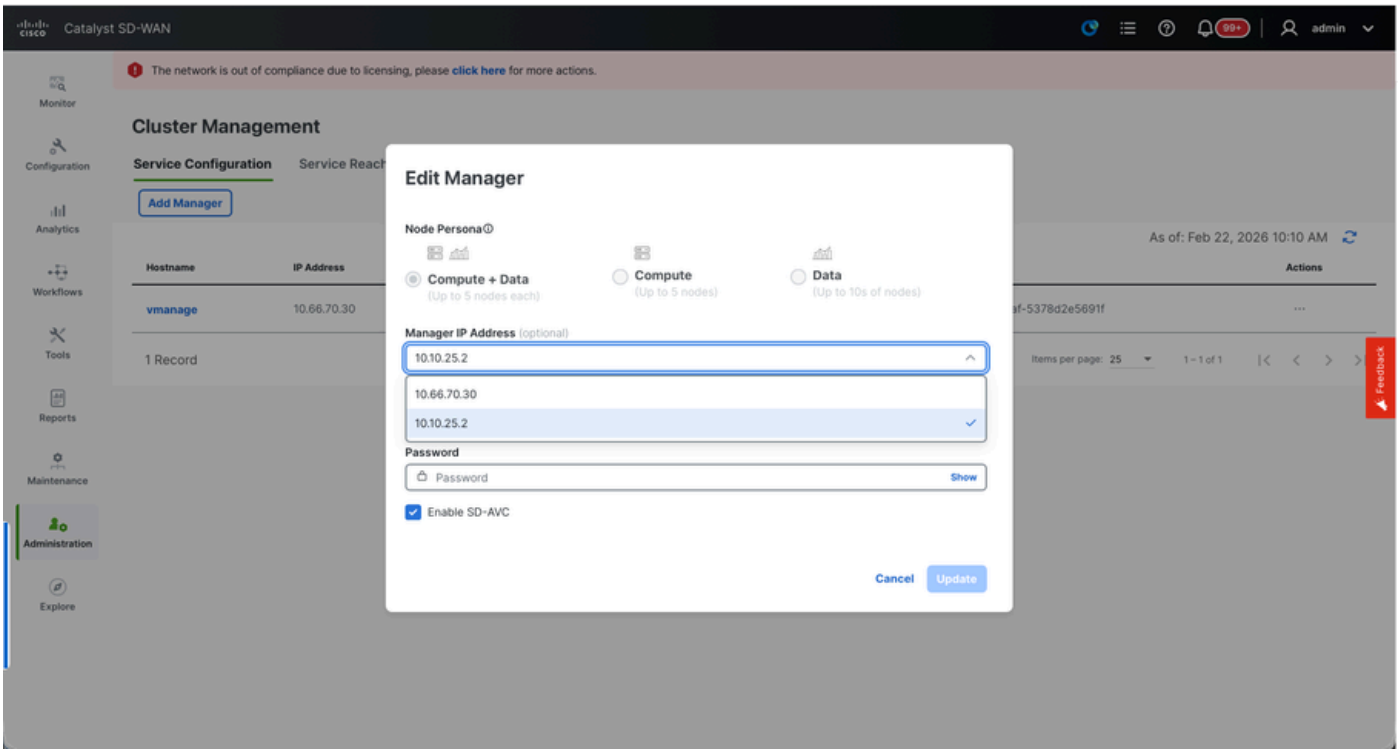
- Une fois le CSR généré, vous pouvez télécharger le CSR et le faire signer en fonction de l'autorité de certification choisie pour les contrôleurs. Vous pouvez vérifier cette configuration dans Administration > Settings > Controller Certificate Authorization. Si vous choisissez Cisco (recommandé), le CSR est automatiquement téléchargé sur le portail PNP par vManage et une fois le certificat signé, il est installé automatiquement sur le vManage.
- Si vous sélectionnez Manual (Manuel), signez manuellement le CSR à l'aide du portail Cisco PNP en accédant au compte Smart et au compte virtuel de la superposition SD-WAN correspondante.
- Une fois le certificat disponible sur le portail PNP, cliquez sur Installer le certificat dans la même section de vManage, téléchargez le certificat et installez-le.
- La même procédure s'applique si nous utilisons Digicert et le certificat racine d'entreprise.
- Effectuez cette étape sur tous les noeuds vManage qui font partie du cluster.

Préparation de la création du cluster vManage

- Dans l'interface utilisateur web de vManage-1, accédez à Administration > Cluster Management, cliquez sur ... sous Actions pour vManage-1, choisissez Edit.
- Le personnage du noeud est choisi automatiquement en fonction du personnage que nous avons choisi lors de la mise sous tension de la VM.

Remarque : Dans le cas d'un cluster à 3 noeuds, les 3 noeuds vManage sont présentés avec compute+data comme personnage. Dans le cas d'un cluster à 6 noeuds, 3 noeuds vManage sont activés avec compute+data en tant que personnage et 3 noeuds vManage avec des données en tant que personnage.

- Dans la liste déroulante de l'adresse IP du gestionnaire, assurez-vous de choisir l'adresse IP de l'interface de service du vManage.



- Entrez le nom d'utilisateur et le mot de passe que vous souhaitez utiliser pour activer le cluster vManage, appelé informations d'identification du cluster.
- Comme mentionné précédemment, les mêmes informations d'identification doivent être configurées sur tous les noeuds vManage et doivent être utilisées lors de l'ajout de tous les noeuds au cluster.

Configuration facultative :

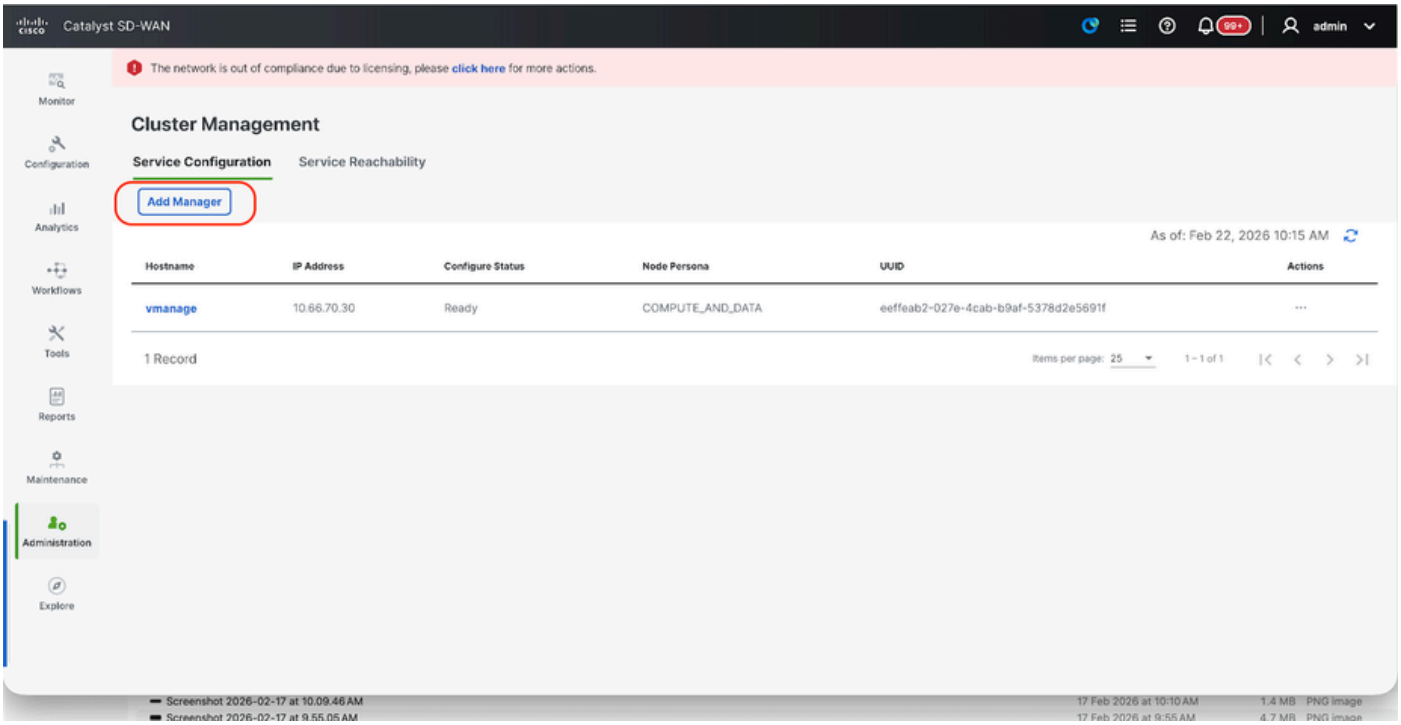
Reportez-vous à cette configuration dans votre cluster existant pour Activer SDAVC - Nécessaire d'être coché seulement si elle est requise et n'est nécessaire que sur un noeud vManage du cluster.

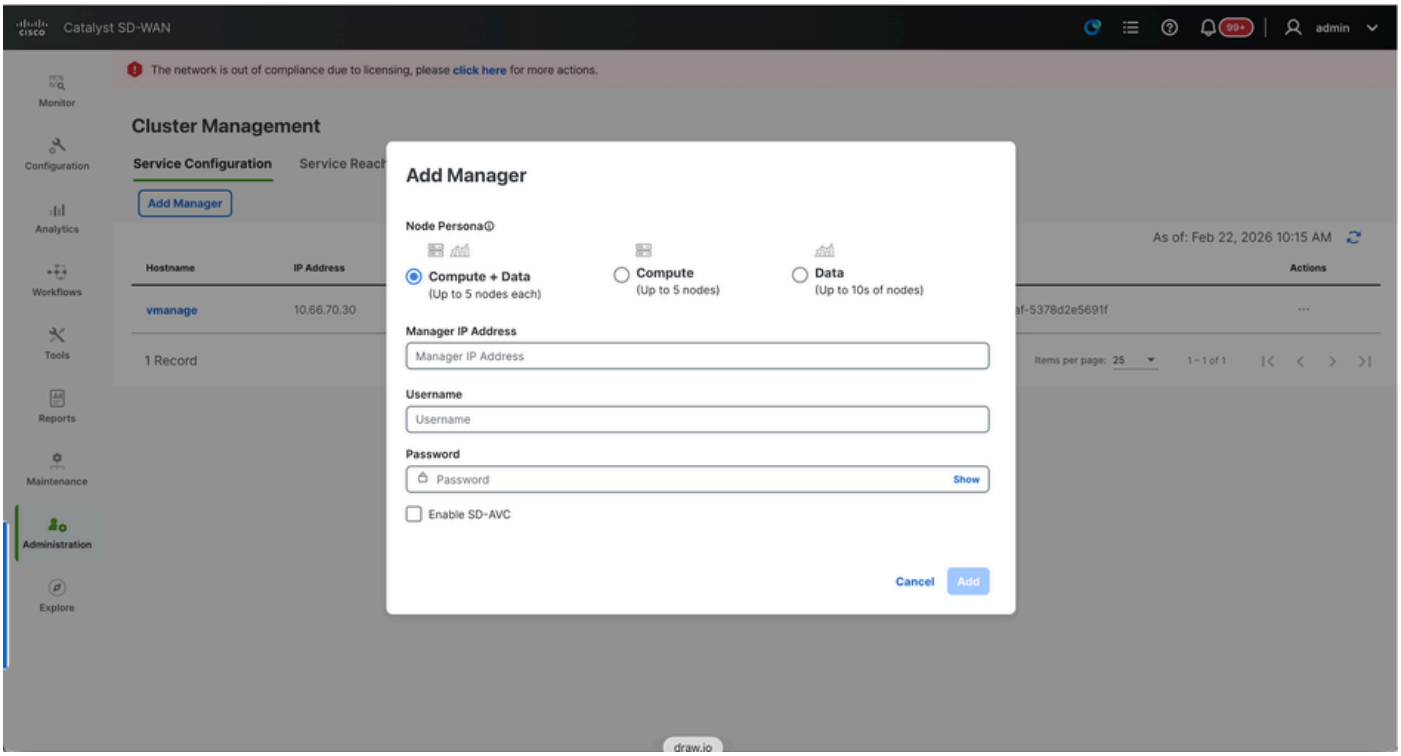
Cliquez sur Update.

- Publiez ceci, les services vManage NMS redémarrent en arrière-plan et l'interface utilisateur n'est pas disponible pendant quelques minutes d'environ 5 à 10 minutes. Pendant ce temps, l'accès CLI de vManage est disponible.
- Une fois que l'interface utilisateur de vManage-1 est accessible, accédez à Administration > Cluster Management, assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et que la personnalité du noeud est reflétée correctement. Passez à la section Accessibilité des services dans la même page et assurez-vous que tous les services sont accessibles.
- Si l'un des services n'est pas encore accessible, veuillez patienter. Cela prend généralement entre 20 et 30 minutes.

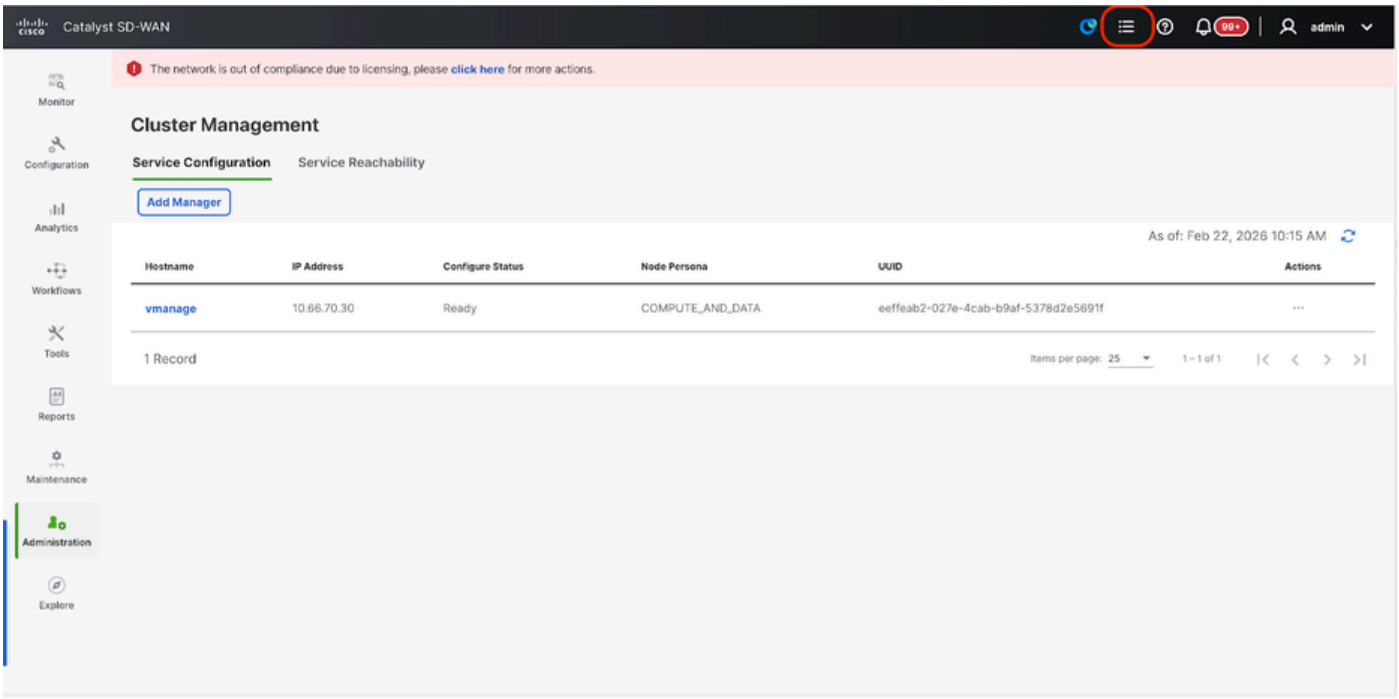
Créer le cluster vManage

- Sur l'interface utilisateur web de vManage-1, accédez à Administration > Cluster Management, dans la section Configuration du service,
- Cliquez sur Add Manager, une fenêtre contextuelle s'affiche :





- Choisissez le personnage de noeud en fonction des configurations de personnage effectuées pendant que le noeud vManage - 2 a été lancé.
- Entrez l'adresse IP de l'interface de service de vManage-2 sous l'adresse IP du gestionnaire
- Saisissez le nom d'utilisateur et le mot de passe, qui sont les mêmes informations d'identification que celles utilisées à l'étape 6.
- Enable SDAVC (Activer SDAVC) : cette case n'est pas cochée, car elle est déjà activée sur vManage-1
- Cliquez sur Ajouter.
- Dans ce message, les services vManage NMS redémarrent en arrière-plan pour les noeuds vManage 1 et 2. L'interface utilisateur n'est pas disponible pendant quelques minutes, de l'ordre de 5 à 10 minutes pour vManage 1 et 2.
- Pendant ce temps, l'accès CLI de vManage 1 et 2 est disponible.
- Une fois que l'interface utilisateur de vManage-1 est accessible, accédez à Administration > Cluster Management, assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et node persona est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles pour les deux noeuds vManage.
- Si l'un des services n'est pas encore accessible, veuillez patienter. Cela prend généralement entre 5 et 10 minutes.
- Vous pouvez vérifier l'état du processus d'ajout de cluster dans la liste des tâches disponible dans l'angle supérieur droit de l'interface utilisateur vManage.



- Vous pouvez rechercher la liste des tâches actives et si la tâche est toujours répertoriée sous Liste des tâches actives, cela indique que la tâche n'est pas encore terminée.
- Vous pouvez cliquer sur la tâche pour vérifier sa progression. Si la tâche n'est pas répertoriée dans la liste des tâches actives, passez à Terminée et vérifiez qu'elle est terminée avec succès.
- Une fois ces points validés, passez à l'étape suivante.

Ces points doivent être pris en compte avant d'ajouter le noeud suivant au cluster :

Vérifiez ces points sur toutes les interfaces utilisateur des noeuds vManage qui ont été ajoutés au cluster jusqu'à présent :

- Accédez à Monitor > Overview of vManage UI et assurez-vous que le nombre de noeuds vManage sont reflétés correctement et sont visibles accessibles en fonction du nombre de noeuds ajoutés au cluster.

- Accédez à Administration > Cluster Management et assurez-vous que l'adresse IP de l'interface de service de vManage est reflétée sous IP address, Configure Status is Ready et node persona est reflétée correctement.
- Passez à la section Accessibilité des services de la même page et assurez-vous que tous les services sont accessibles pour les deux noeuds vManage.

- Chaque fois qu'un noeud est ajouté au cluster, les services NMS de tous les noeuds du cluster sont redémarrés, ce qui rend l'interface utilisateur de tous ces noeuds inaccessible pendant un certain temps.
- Selon le nombre de noeuds dans le cluster, la restauration de l'interface utilisateur et

l'accessibilité de tous les services peuvent prendre plus de temps.
- Vous pouvez surveiller la tâche sous Liste des tâches disponible dans le coin supérieur droit de l'interface utilisateur vManage.
- Sur l'interface utilisateur vManage de chaque noeud ajouté au cluster, nous devons voir tous les routeurs, modèles et stratégies s'ils étaient disponibles dans vManage-1.
- Si ces configurations n'étaient pas présentes sur vManage-1, les vBonds et vSmarts qui ont été ajoutés à vManage-1 ainsi que les configurations Administration > Settings pour Organization-name, vBond, Certificate Authorization doivent être reflétées sur le reste des noeuds vManage ajoutés au cluster.
- Répétez les mêmes étapes pour le reste des noeuds vManage.

Étape 4: Sauvegarde/restauration Config-db

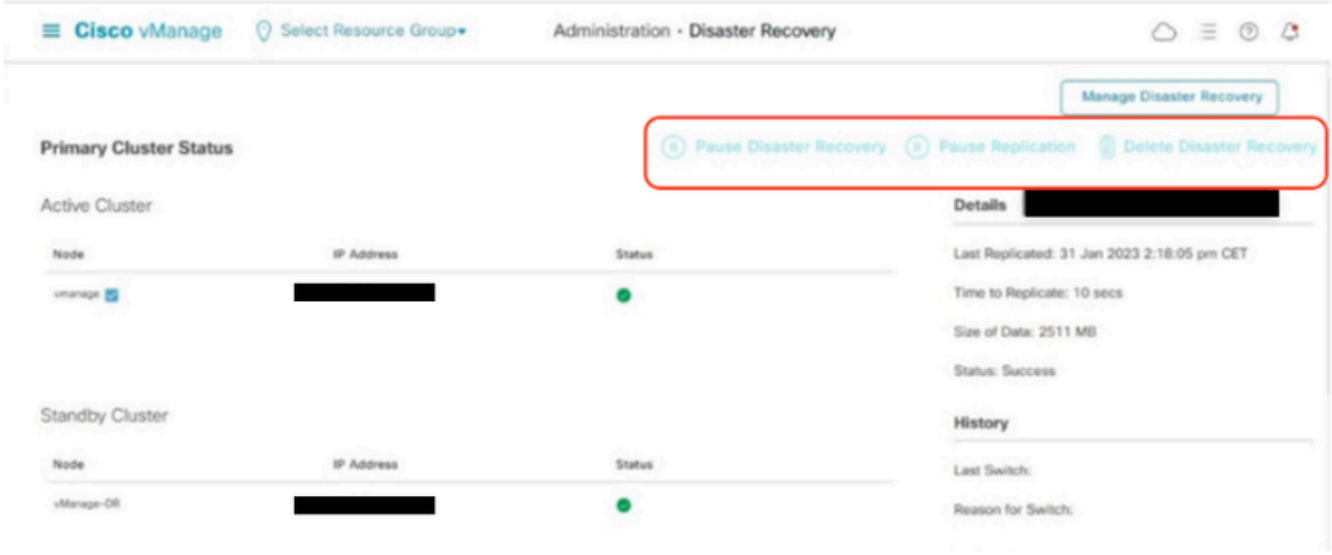
Collecter la sauvegarde et la restauration de la base de données de configuration vManage sur un autre noeud vManage

---

Remarque : Lors de la collecte de la sauvegarde de la base de données de configuration à partir du cluster vManage existant pour lequel la récupération après sinistre est activée, assurez-vous qu'elle est collectée après la suspension et la suppression de la récupération après sinistre sur ce noeud.

Vérifiez qu'aucune réplication de reprise après sinistre n'est en cours. Accédez à Administration > Disaster Recovery et assurez-vous que l'état est Réussite et qu'il n'est pas dans un état transitoire tel que Importation en attente, Exportation en attente ou Téléchargement en attente. Si l'état n'est pas réussi, contactez le TAC Cisco et assurez-vous que la réplication est réussie avant de procéder à la pause de la reprise après sinistre.

Tout d'abord, suspendez la reprise après sinistre et assurez-vous que la tâche est terminée. Supprimez la reprise après sinistre et confirmez que la tâche est terminée.



Contactez le TAC Cisco pour vous assurer que la reprise après sinistre est correctement nettoyée.

Collecter la sauvegarde Configuration-DB :

- Dans le fabric SD-WAN actuellement utilisé, vous pouvez générer une sauvegarde de la base de données de configuration à partir du cluster vManage.
- Veuillez noter que nous devons générer une sauvegarde de la base de données de configuration uniquement sur un noeud du cluster vManage qui est le leader de la base de données de configuration.

- Pour vManage autonome, ce vManage est lui-même le leader de la base de données de configuration.
- Dans le cluster vManage, identifiez le noeud de tête configuration-db à l'aide de la commande request nms configuration-db diagnostics. Vous pouvez exécuter cette commande sur tous les noeuds du cluster vManage à 3 noeuds.
- Dans un cluster de 6 noeuds, assurez-vous d'exécuter cette commande sur les noeuds vManage où configuration-db est activé pour identifier le noeud de tête. Accédez à Administration > Gestion du cluster pour vérifier la même chose :
- Comme nous le voyons dans la capture d'écran, les noeuds configurés avec persona COMPUTE_AND_DATA ont configuration-db en cours d'exécution.

Vous pouvez vérifier la même chose à l'aide de la commande request nms configuration-db status sur l'interface de ligne de commande vManage. Le résultat est le suivant

```
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#
```

- Une fois que vous exécutez la commande request nms configuration-db diagnostics sur ces noeuds, le résultat est comme indiqué :
- Recherchez le champ mis en surbrillance pour « IsLeader ». S'il est défini sur 1, il indique que le noeud est le noeud leader et nous pouvons collecter la sauvegarde configuration-db à partir de celui-ci.

```
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     .
```

Utilisez cette commande pour collecter la sauvegarde configuration-db à partir du noeud vManage de tête de base de données de configuration identifié.

```
request nms configuration-db backup path /opt/data/backup/<filename>
```

Le résultat attendu est le suivant :

```
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#
```

- Notez les informations d'identification de configuration-db si elles ont été mises à jour.
- Si vous ne connaissez pas les informations d'identification de la base de données de configuration, contactez le TAC pour récupérer les informations d'identification de la base de données de configuration à partir des noeuds vManage existants.

- Les informations d'identification configuration-db par défaut sont username : neo4j et

password : mot de passe

Restaurer la sauvegarde Configuration-db vers un autre noeud vManage

Copiez la sauvegarde configuration-db dans le répertoire /home/admin/ de vManage à l'aide de SCP.

Exemple de sortie de commande 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
```

Pour restaurer la sauvegarde configuration-db, nous devons d'abord configurer les informations d'identification configuration-db. Si vos identifiants configuration-db sont default(neo4j/password), nous pouvons ignorer cette étape.

Pour configurer les informations d'identification configuration-db, utilisez la commande request nms configuration-db update-admin-user. Utilisez le nom d'utilisateur et le mot de passe de votre choix.

Veuillez noter que le serveur d'applications de vManage est redémarré. En raison de laquelle l'interface utilisateur vManage devient inaccessible pendant une courte période.

```
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#
```

Publication que nous pouvons poursuivre pour restaurer la sauvegarde configuration-db :

Nous pouvons utiliser la commande request nms configuration-db restore path /home/admin/< > pour restaurer la base de données de configuration dans le nouveau 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
```

Une fois la base de données de configuration restaurée, assurez-vous que l'interface utilisateur vManage est accessible. Attendez environ 5 minutes, puis essayez d'accéder à l'interface utilisateur.

Une fois connecté à l'interface utilisateur avec succès, assurez-vous que la liste des routeurs Edge, le modèle, les stratégies et toutes les autres configurations qui étaient présentes sur votre interface utilisateur vManage précédente ou existante sont reflétés sur la nouvelle interface utilisateur vManage.



Mise en garde : La base de données de configuration restaurée contient toujours le ou les gestionnaires SD-WAN à partir desquels la sauvegarde a été effectuée. Elles sont répertoriées en tant qu'entrées Manager dans Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) mais ne sont pas membres de Administration > Cluster Management. Jusqu'à leur suppression à l'étape 6 :

- chaque rapport Send to Validator signale Failed to find Vmanage Cluster node for uuid <uuid> for them, et
- chaque installation de certificat de contrôleur à partir de l'interface utilisateur échoue et est restaurée.

N'effectuez aucune opération de certificat de contrôleur ou d'envoi au validateur sur ce vManage avant la fin de l'étape 6. Si l'installation d'un certificat échoue, n'installez pas le même certificat à partir de l'interface de ligne de commande ; Contactez le centre d'assistance technique Cisco TAC.

Étape 5: Activer la reprise après sinistre sur un cluster vManage

Précontrôles importants

Deux clusters à 3 noeuds vManage distincts doivent être configurés et opérationnels pour poursuivre la reprise après sinistre. Sur le cluster actif, vous devez avoir des validateurs et des contrôleurs intégrés. Si vous avez des validateurs et des contrôleurs sur le site DR, ils doivent également être intégrés sur le cluster actif et non sur le cluster vManage DR.

Cisco recommande de respecter les conditions suivantes avant d'enregistrer une reprise après sinistre :

- Assurez-vous que le noeud principal et le noeud secondaire sont accessibles par HTTPS sur un VPN de transport (VPN 0).
- Assurez-vous que les contrôleurs Cisco vSmart et les orchestrateurs Cisco vBond de la configuration secondaire sont connectés à la configuration principale.
- Assurez-vous que le noeud principal et le noeud secondaire Cisco vManage exécutent la même version de Cisco vManage.
- Interface de cluster hors bande (interface de service) dans VPN 0.
- Pour chaque instance vManage d'un cluster, une troisième interface (liaison de cluster) est requise en plus des interfaces utilisées pour VPN 0 (transport) et VPN 512 (gestion).
- Cette interface est utilisée pour la communication et la synchronisation entre les serveurs vManage du cluster.

- Cette interface doit être d'au moins 1 Gbit/s et avoir une latence de 4 ms ou moins. Une interface 10 Gbit/s est recommandée.

- Les deux noeuds vManage doivent être en mesure de se joindre via cette interface : qu'il s'agisse d'un segment de couche 2 ou du routage de couche 3.

- Dans chaque vManage, cette interface doit être configurée dans l'interface utilisateur graphique en tant qu'interface de cluster (Administration > Cluster Management - indiquez votre propre adresse IP, votre utilisateur et votre mot de passe d'interface de cluster hors bande).

- Afin de permettre aux noeuds Cisco vManage de communiquer entre eux à travers les data centers, activez les ports TCP 8443 et 830 sur les pare-feu de votre data center.

- Assurez-vous que tous les services (application-server, configuration-db, messaging server, coordination server et statistics-db) sont activés sur les deux noeuds Cisco vManage.

- Distribuez tous les contrôleurs, y compris les orchestrateurs Cisco vBond, dans les data centers principal et secondaire. Assurez-vous que ces contrôleurs sont accessibles par les noeuds Cisco vManage distribués dans ces data centers. Les contrôleurs se connectent uniquement au noeud Cisco vManage principal.

- Assurez-vous qu'aucune autre opération n'est en cours dans le noeud Cisco vManage actif (principal) et en veille (secondaire). Par exemple, assurez-vous qu'aucun serveur n'est en cours de mise à niveau ou d'association de modèles à des périphériques.

- Désactivez le serveur proxy HTTP/HTTPS Cisco vManage s'il est activé. Voir Serveur proxy HTTP/HTTPS pour Cisco vManage Communication with External Servers. Si vous ne désactivez pas le serveur proxy, Cisco vManage tente d'établir une communication de reprise après sinistre via l'adresse IP proxy, même si les adresses IP de cluster hors bande Cisco vManage sont directement accessibles. Vous pouvez réactiver le serveur proxy HTTP/HTTPS Cisco vManage une fois l'enregistrement de la reprise après sinistre terminé.

- Avant de commencer le processus d'enregistrement de reprise après sinistre, accédez à la fenêtre Outils > Redécouvrir le réseau sur le noeud principal Cisco vManage et retrouvez les orchestrateurs Cisco vBond.

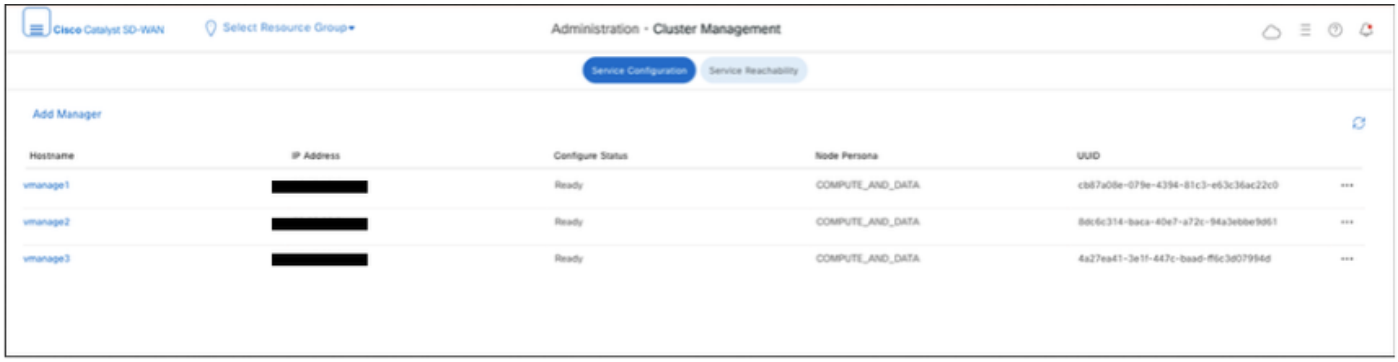
Configurations

Pour plus d'informations sur vManage Disaster Recovery, consultez ce lien.

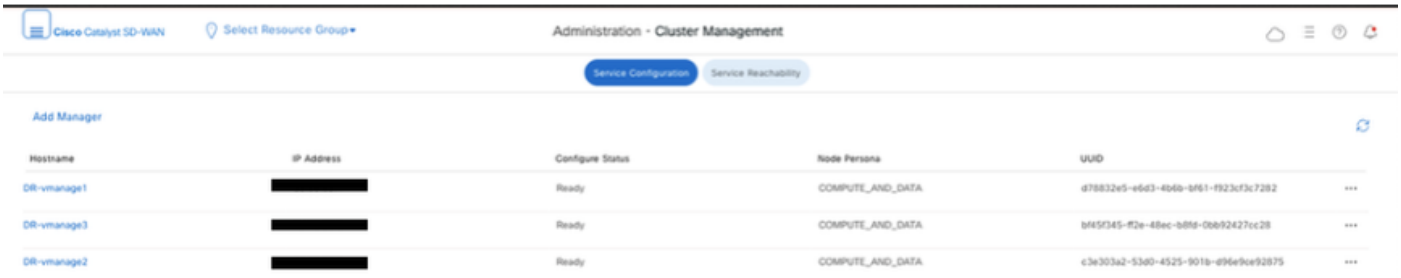
Les deux clusters à 3 noeuds distincts sont déjà créés, à condition que chaque gestionnaire SD-WAN dispose d'une configuration minimale et que la partie certification soit terminée.

Accédez à Administration > Cluster Management sur les deux clusters et vérifiez que tous les noeuds sont à l'état Prêt.

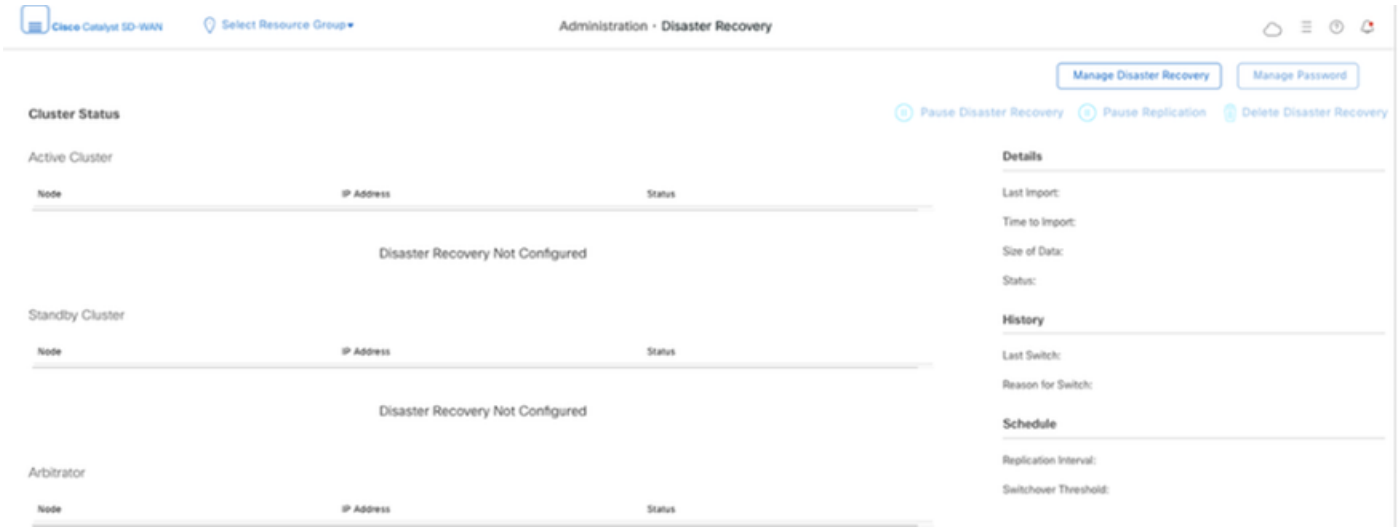
DC vManage



DR vmanage



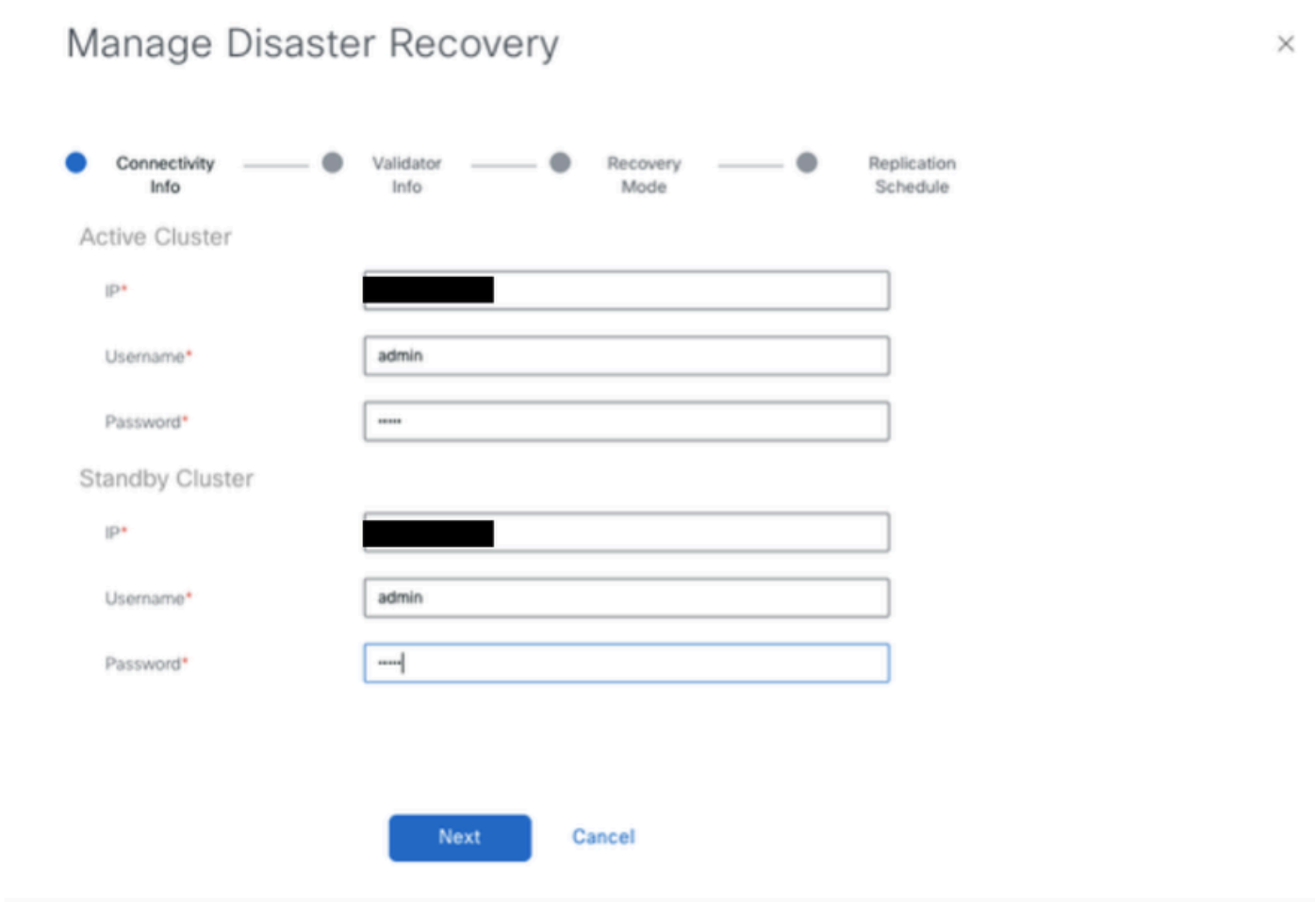
Accédez à Administration>Reprise après sinistre du cluster vManage principal. Cliquez sur Gérer la reprise après sinistre.



Dans la fenêtre contextuelle, renseignez les détails de vManage principal et secondaire.

Les adresses IP à indiquer sont les adresses IP des interfaces de cluster hors bande. Utilisez de préférence l'adresse IP de l'interface de service VPN 0 de vManage-1 dans chaque cluster.

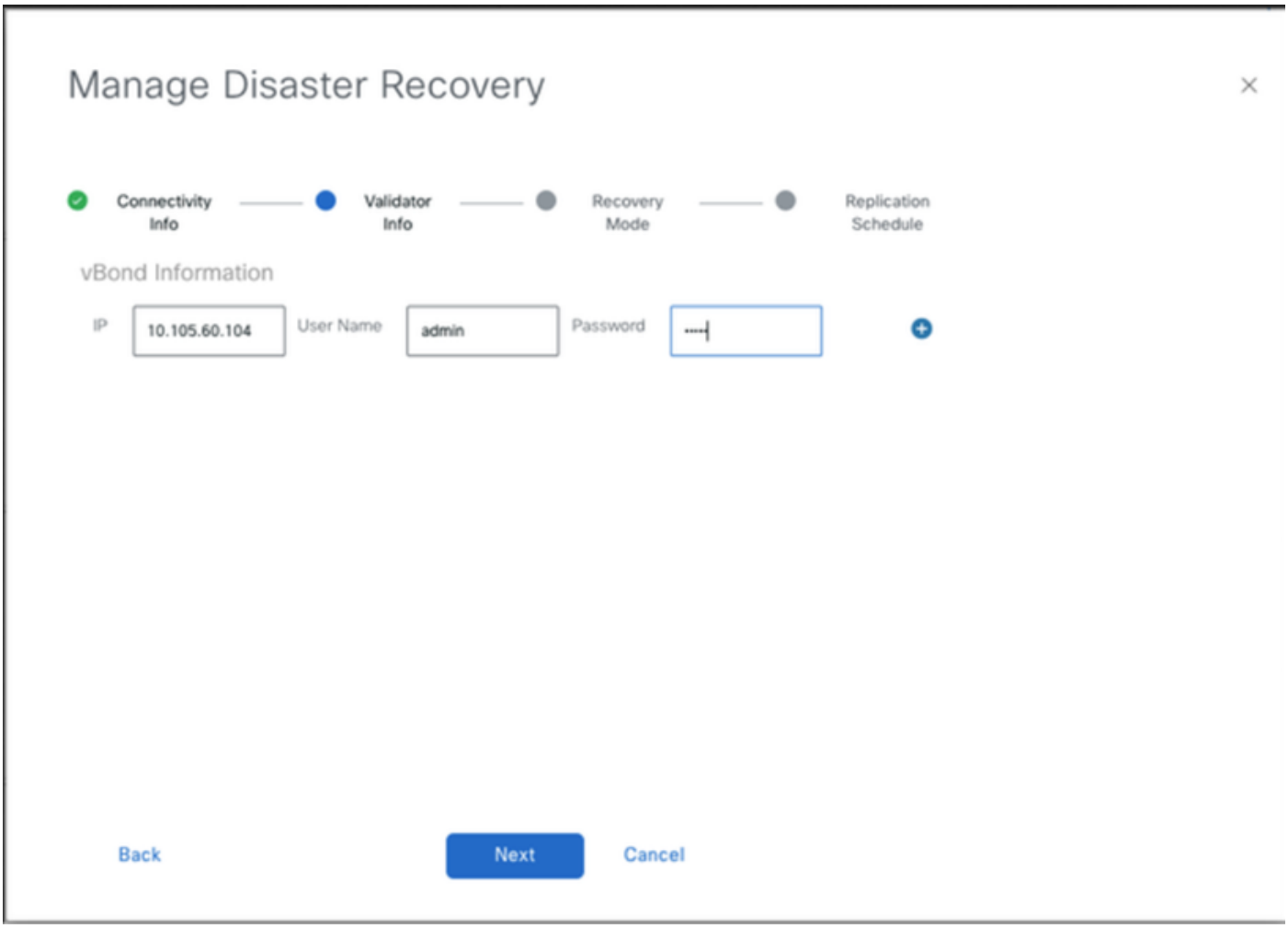
Les informations d'identification doivent être celles d'un utilisateur netadmin et ne doivent pas être modifiées une fois le DR configuré, sauf si celui-ci est supprimé. Vous pouvez utiliser des informations d'identification d'utilisateur local vManage distinctes pour la reprise après sinistre. Nous devons nous assurer que l'utilisateur local vManage fait partie du groupe netadmin. Même les identifiants d'administrateur peuvent être utilisés ici.



Une fois rempli, cliquez sur Next.

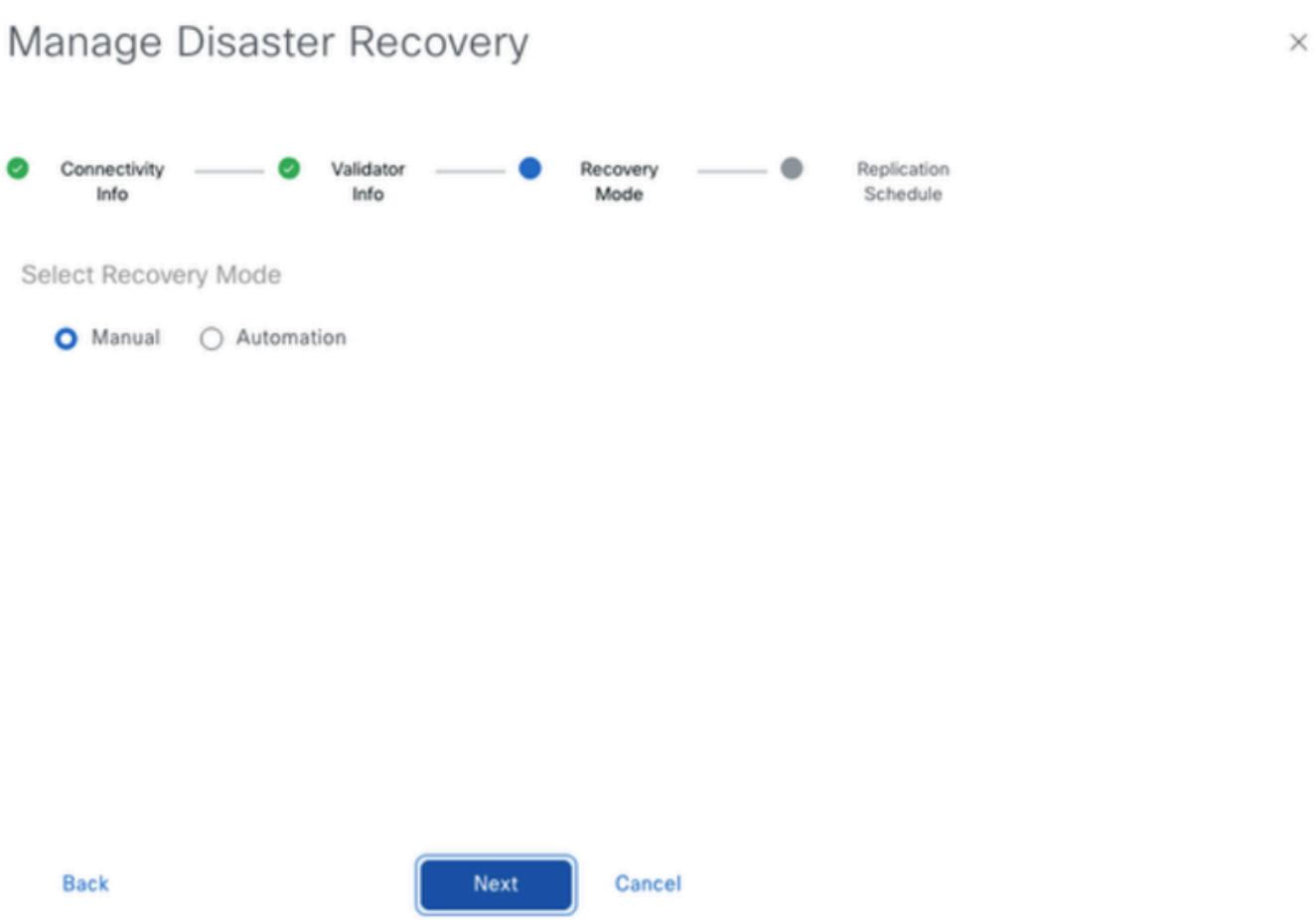
- Renseignez les détails des contrôleurs vBond.

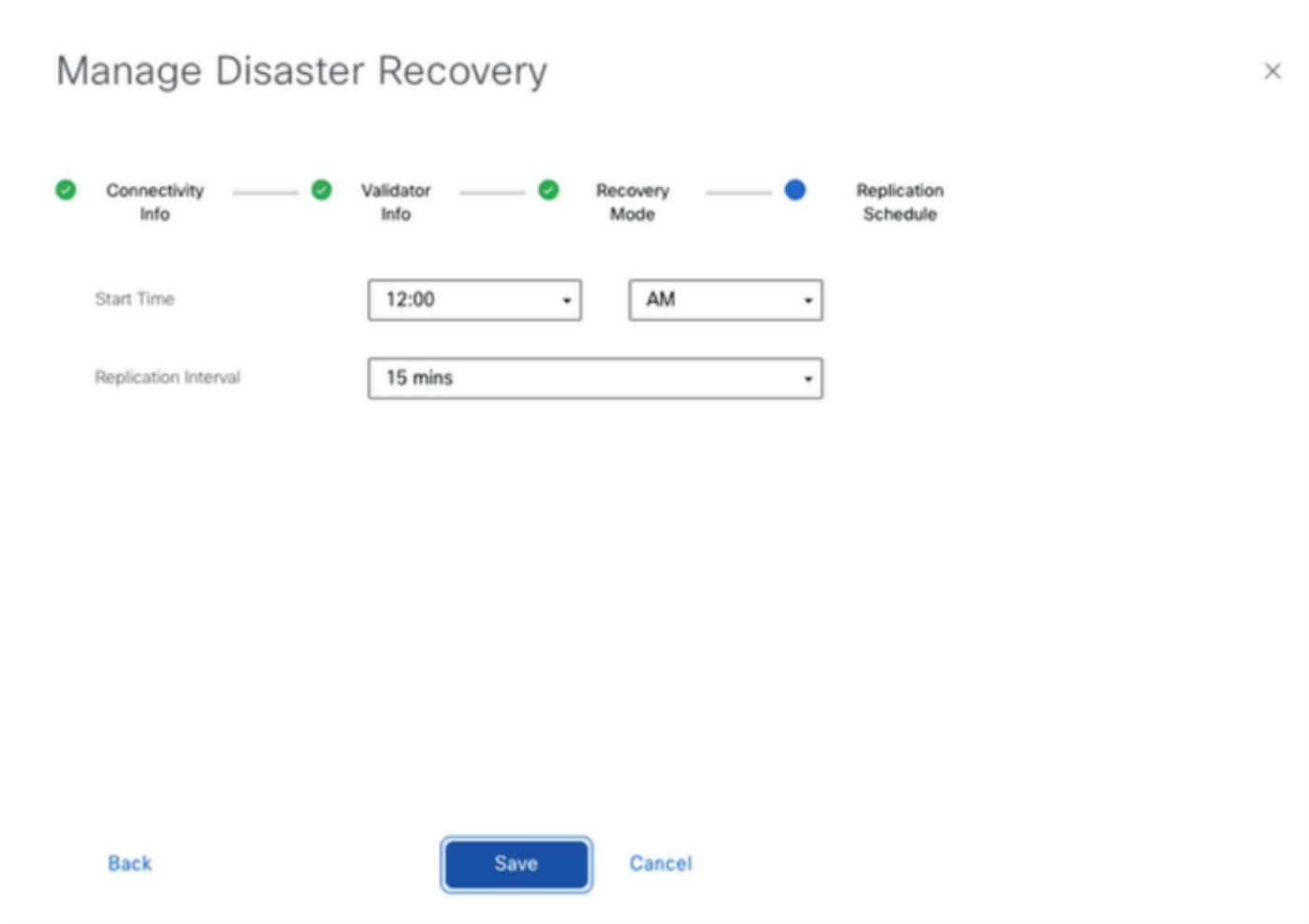
Les contrôleurs vBond doivent être accessibles dans l'adresse IP spécifiée via Netconf.



Une fois rempli, cliquez sur Next.

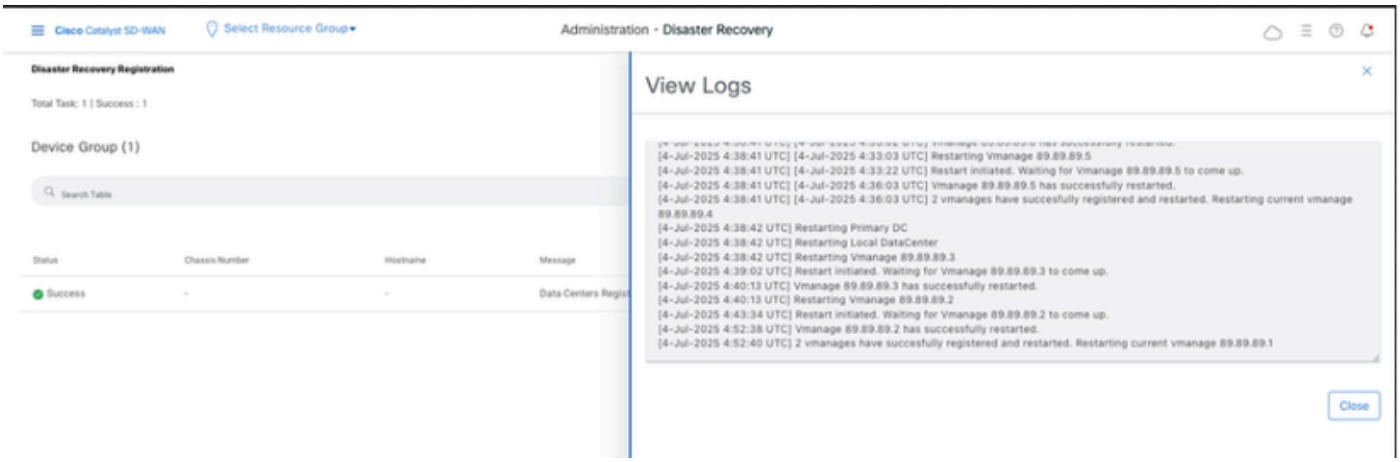
- Dans le champ Recovery Mode, sélectionnez Manual. Le mode Automation est déconseillé. Cliquez sur Suivant.


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



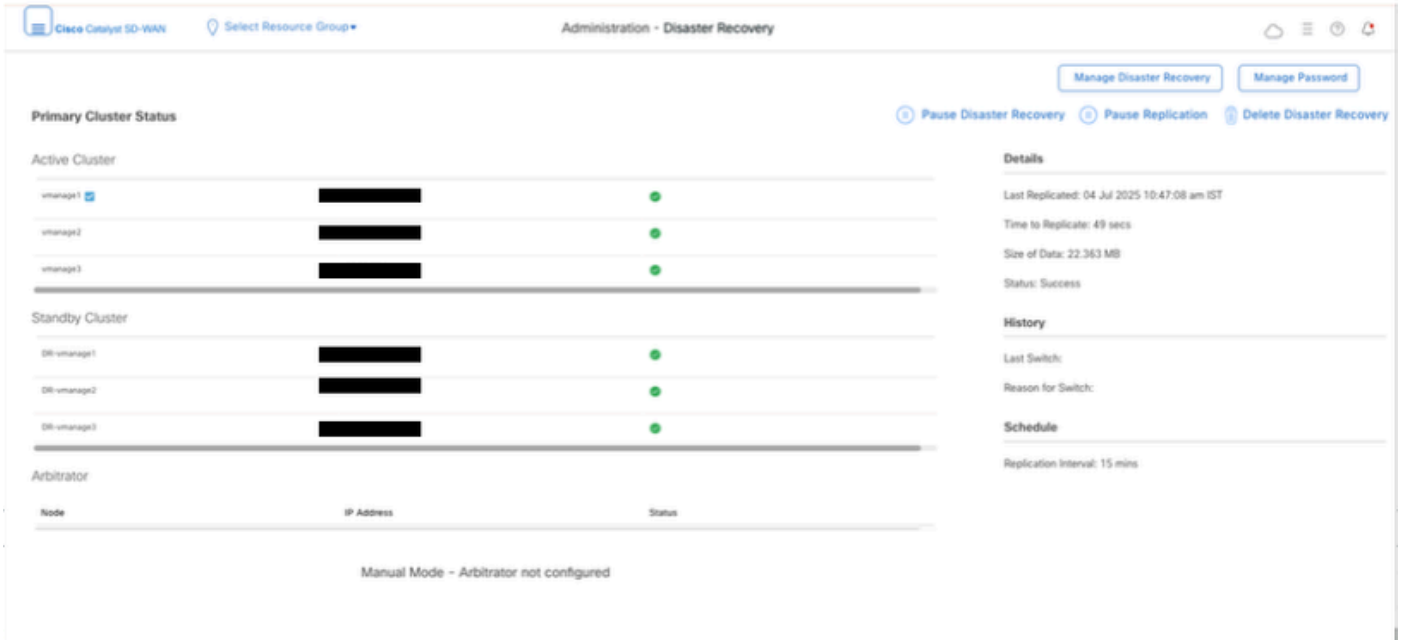
Définissez la valeur et cliquez sur Save.

- L'enregistrement du DR commence maintenant. Cliquez sur le bouton Actualiser pour actualiser manuellement l'état et les journaux de progression. Ce processus peut prendre de 20 à 30 minutes.



Vérification

Accédez à Administration>Disaster Recovery afin de voir l'état de la reprise après sinistre et quand les données ont été répliquées la dernière fois.



Remarque : La réplication peut prendre plusieurs heures en fonction de la taille de la base de données. En outre, quelques cycles peuvent être nécessaires pour réussir la réplication.

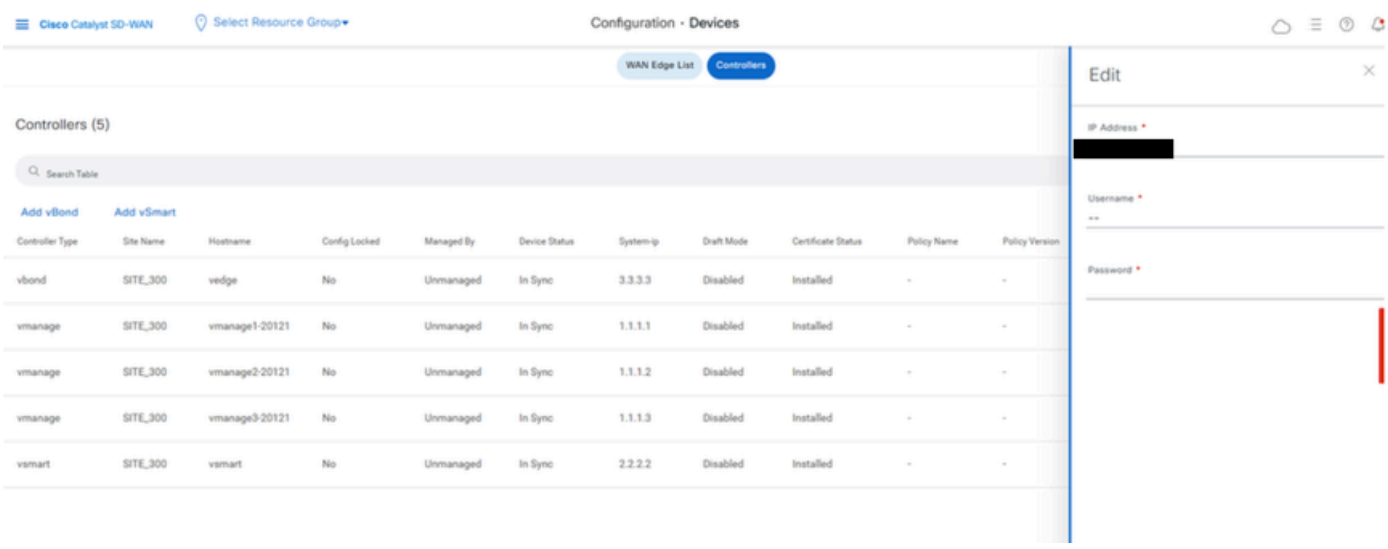
Étape 6: Réauthentification des contrôleurs et invalidation des anciens contrôleurs

Une fois la base de données de configuration restaurée, nous devons réauthentifier tous les nouveaux contrôleurs (vmanage/vsmart/vbond) dans le fabric

Remarque : en production réelle, si l'interface IP utilisée pour la ré-authentification est l'interface IP du tunnel, vous devez vous assurer que le service NETCONF est autorisé sur l'interface du tunnel de vManage, vSmart et vBond, ainsi que sur les pare-feu le long du chemin. Le port de pare-feu à ouvrir est le port TCP 830 en tant que règle bidirectionnelle du cluster DR vers tous les vBonds et vSmarts .

Sur l'interface utilisateur vmanage, cliquez sur Configuration > Devices > Controllers

- Cliquez sur les trois points situés près de chaque contrôleur, puis cliquez sur Edit



- Remplacez l'adresse IP (ip système du contrôleur) par l'adresse IP du vpn de transport 0

(interface de tunnel). Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur save (enregistrer)
- Procédez de la même manière pour tous les nouveaux contrôleurs du fabric

Synchroniser la chaîne de certificats racine

Une fois tous les contrôleurs intégrés, procédez comme suit :

Sur tout serveur Cisco SD-WAN Manager du cluster nouvellement actif, effectuez les actions suivantes :

Entrez cette commande pour synchroniser le certificat racine avec tous les périphériques Cisco Catalyst SD-WAN dans le nouveau cluster actif :

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

Entrez cette commande pour synchroniser l'UUID du gestionnaire Cisco SD-WAN avec le validateur Cisco SD-WAN :

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

Supprimer les entrées précédentes du gestionnaire SD-WAN

Effectuez cette opération juste après la synchronisation root-cert-chain et avant toute opération de certificat de contrôleur ou Envoyer au validateur.

1. Ouvrez Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificates > Controllers) et Administration > Cluster Management. Chaque entrée vManage qui n'est pas répertoriée dans Administration > Cluster Management est une entrée précédente de SD-WAN Manager et doit être supprimée. N'invalidez pas les noeuds vManage du cluster de reprise après sinistre (secondaire) indiqués dans Administration > Disaster Recovery. Seules les entrées vManage de la source de la sauvegarde configuration-db sont supprimées ici.
2. Avant toute action Envoyer au validateur ou Invalider, recherchez un enregistrement de numéro de série en conflit. Accédez à https://<vmanage-url>/dataservice/certificate/vsmart/list. Aucune entrée ne peut avoir un ancien numéro de série dont le numéro de série est égal à son propre numéro de série. Cette vérification est en lecture seule. Si une telle entrée existe, arrêtez-vous et contactez le TAC Cisco : any Send to Validator or Invalidate envoie la liste des contrôleurs et ce contrôleur perdrait ses connexions de contrôle.

3. Accédez à Monitor > Tasks et ouvrez la dernière tâche Push vSmart List. Examiner uniquement les résultats des tâches existantes ; ne cliquez pas ici sur Envoyer au validateur. Si aucune tâche récente n'est répertoriée, attendez la diffusion de la liste en début d'heure suivante. Chaque entrée précédente du gestionnaire SD-WAN doit indiquer Failed to find Vmanage Cluster node for uuid <uuid>. Si un uuid vManage a été envoyé avec succès, il est membre actif de ce cluster : ne l'invalidez pas.
4. Cliquez sur les trois points à droite de la première entrée précédente du gestionnaire SD-WAN, puis cliquez sur Invalidate. Attendez la fin de la tâche. Le résultat attendu est Success with warning, avec cet exercice :

```
Invalidating Root Certificate Autority of vManage-<uuid>
Sending serial number of vManage-<uuid> as invalid to all controllers
Failed to push serial list to vManage-<uuid> - retry in 30 seconds; Failed to find Vmanage Cluster node
Updated serial list will be sent to vManage-<uuid> when it is reachable
Clearing certificate on vManage-<uuid>
Successfully invalidated vManage-<uuid>
```

L'entrée affiche désormais No certificate installed. Le numéro de série précédent du gestionnaire SD-WAN et l'autorité de certification racine sont supprimés des validateurs.

5. Cliquez sur les trois points de la même entrée, puis cliquez à nouveau sur Invalider. Il se termine immédiatement, sans tâche, et l'entrée est supprimée.
6. Répétez les étapes 4 et 5 pour chaque entrée précédente du gestionnaire SD-WAN.
7. Cliquez sur Envoyer au validateur. Le résultat attendu est Success pour chaque destinataire dans quelques secondes, avec no Failed to find Vmanage Cluster node.

Invalider les anciens contrôleurs

Une fois que le fabric est restauré et que les sessions de contrôle et BFD sont actives pour tous les bords et contrôleurs du fabric, invalidez les anciennes entrées vBond/Validator et vSmart/Controller de l'interface utilisateur :

- Sur l'interface utilisateur de vManage, accédez à Configuration > Certificates > Control Components (20.9/20.12 : Configuration > Certificats > Contrôleurs).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Invalidate.
- Cliquez sur Send to Validator (Send to vBond in 20.9/20.12). Il doit indiquer le succès de chaque destinataire.
- Accédez à Configuration > Devices > Control Components (20.9/20.12 : Configuration > Devices > Controllers).
- Cliquez sur les trois points sur le côté droit de l'ancien vBond/vSmart et cliquez sur Delete.

Valider les chèques

Ces contrôles postérieurs s'appliquent à toutes les combinaisons de déploiement.

Réactiver les routeurs de périphérie du cloud :

- Si C8000v fait partie de la superposition et est géré et signé, ils doivent être authentifiés à nouveau, c'est-à-dire :

```
request platform software sdwan vedge_cloud activate chassis-number <chassis-number >  token <token numb
```

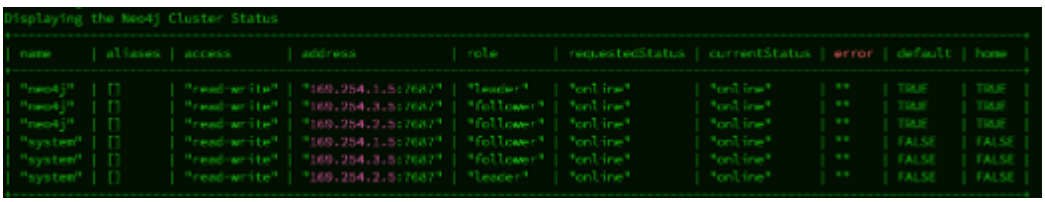
- Vérifiez que les connexions de contrôle et les sessions BFD sont actives
- Vérifiez que le trafic des applications circule de bout en bout
- Si des modifications ont été apportées au saut de port avant la reconstruction du fabric sur les arêtes, elles doivent être annulées
- Vérifiez que les éléments apparaissent comme prévu :
    - Modèles
    - Politiques
    - Page Device (les deux onglets) WAN vEdge List and Controllers

  vManage post-vérifications
- Applicable aux noeuds vManage :

  Contrôles de configuration-DB(Neo4j) :

  Exécutez la commande « request nms configuration-db diagnostics » sur tous les noeuds vManage :

  1. Vérifier le statut du noeud en ligne et du leadership : (non disponible pour toutes les versions)



«Neo4j» doit montrer 3 noeuds en ligne et 1 leader et 2 suiveurs. «system» doit également afficher 3 noeuds en ligne et 1 point de repère et 2 suiveurs, mais comme ce n'est pas le Db par défaut, l'indicateur par défaut est false. S'il y a moins de 3 entrées dans chaque neo4j et que le système signifie que le noeud est tombé de la grappe. Veuillez contacter le TAC Cisco pour le dépanner.

2. Vérifiez si un noeud est en « quarantaine ».

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

Aucun des noeuds ne doit être en état de quarantaine.

3. La validation du schéma doit être réussie.

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

4. Collectez une sauvegarde configuration-db à l'aide de la commande « request nms configuration-db diagnostics » et assurez-vous qu'elle est correcte.

```
vmanage_2013# request nms configuration-db backup path /opt/data/backup/9thSepBackup.tar.gz
Starting backup of configuration-db
config-db backup logs are available in /var/log/nms/neo4j-backup.log file
Successfully saved backup to /opt/data/backup/9thSepBackup.tar.gz.tar.gz
sha256sum: 9d43addcf6c43f18c32b833295a6318fa0a63a7bf7456965140dcb9a61118b5e
Removing the temp staging dir :/opt/data/backup/staging
vmanage_2013#
```

En cas d'incohérence ou d'erreur, contactez le centre d'assistance technique Cisco pour obtenir des informations de dépannage.

Vous pouvez également exécuter ces appels d'API pour confirmer l'état du noeud vmanage pour un cluster (pour tous les noeuds COMPUTE+DATA) - fonctionne uniquement sur les versions

20.12 et ultérieures

```
go to vshell of the vmanage node ( to be done on all vmanages)
============================================================
curl -u <config-db username>:<config-db password>  -H "Content-Type: application/json"   -d '{"statemen

curl -u <config-db username>:<config-db password>  -H "Content-Type: application/json"   -d '{"statemen
```

Assurez-vous que dans un cluster n'a qu'un seul leader pour neo4j et le système et restez en tant que suiveurs .Assurez-vous que tous les noeuds sont en ligne .Si vous avez un cluster de 3 noeuds (les trois sont CALCULER+DONNÉES), il doit y avoir un seul leader pour neo4j et le système .Toute déviation, vous devez contacter le TAC

5. Recherchez les erreurs de disque, de mémoire et d'E/S dans /var/log/kern.log. Cela doit être vérifié sur tous les noeuds vManage.

6. Vérifiez l'étape lorsque vous formez un nouveau cluster pour vmanage qui n'ont pas de CC entre chaque noeud
Exécutez ssh en tant que vmanage-admin du noeud 1 vers les autres noeuds cluster ip et vice versa, pour vérifier si la clé publique est échangée et si le mot de passe moins ssh fonctionne [le jeton de consentement est requis pour les étapes indiquées ici]

```
DR-vManage-1:~# ssh -i /etc/viptela/.ssh/id_dsa -p 830 vmanage-admin@<ClusterIP>
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:
```

Si le résultat vous demande d'entrer le mot de passe, contactez le TAC

Vérifications post-contrôleur :

Applicable à tous les contrôleurs SD-WAN (vBond, vManage, vSmart) :

Exécutez les commandes sur tous les contrôleurs de la superposition et vérifiez que l'UUID vManage et les numéros de série affichés sont valides pour le fabric actuel :

Commandes vBond :

show orchestrator valid-vsmarts

show orchestrator valid-vmanage-id

Commandes vManage/vSmart :

show control valid-vsmarts

show control valid-vmanage-id

Notez que le résultat de la commande show control valid-vsmarts inclut les numéros de série des noeuds vSmarts et vManage.

Comparez-le à ceux de l'interface utilisateur vManage. Accédez à la section Configuration > Certificates > Controllers.

Confirmez également :

- Configuration > Certificates > Control Components répertorie, parmi les entrées vManage, uniquement les noeuds vManage dans Administration > Cluster Management. Toute autre entrée vManage est une entrée SD-WAN Manager précédente reportée par la restauration configuration-db et doit être supprimée comme décrit dans l'étape Réauthentification des contrôleurs et invalidation des anciens contrôleurs de votre combinaison.
- https://<vmanage-url>/dataservice/certificate/vsmart/list n'a pas d'entrée dont l'ancien numéro de série SerialNumber est égal à son numéro de série. S'il y en a un, contactez le centre d'assistance technique Cisco avant de cliquer sur Envoyer au validateur.
- Envoyer au validateur se termine en quelques secondes avec Succès pour chaque destinataire et aucun noeud Cluster Vmanage introuvable.
- Après la diffusion suivante de la liste en début d'heure, la tâche Push vSmart List dans Monitor > Tasks affiche Succès pour chaque destinataire.

Si d'autres entrées sont visibles pour l'UUID/le numéro de série qui ne sont pas actuellement intégrés au fabric, contactez le TAC Cisco.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.