Catalyst SD-WANファブリックの再構築

内容

はじめに

このドキュメントでは、Cisco SD-WANファブリックを再構築する方法について説明します。これには、さまざまな導入用のコントローラ設定のバックアップと復元が含まれます。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- Cisco Software Central（登録ユーザ専用）
- software.cisco.comからのコントローラソフトウェアのダウンロード

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ファブリックを再構築する前の前提条件

- 新しいsystem-ips、site-idのセットは、コントローラの新しいファブリック用に設定する必要があります
- コントローラとエッジ間の通信を可能にするために、ファイアウォール規則が設定されていることを確認します。
- neo4j(configuration-db)のユーザ名とパスワードをメモします（クラスタ内のすべてのvManageノードで同じである必要があります）。
- すべてのエッジでポートホップを無効にする
- グレースフルリスタートのタイマーを7日に増やす
- 移行前に3rdpartyツールでアラームをクリアする
- 統計情報を外部サーバ(asvAnalyticsなど)にエクスポートするための事前設定がない限り、

履歴統計情報データ（アラーム、イベント、デバイス統計情報など）は失われます
- Cloud OnRampが設定されている場合は、この課題を開始する前に、クラウドに導入されているc8000vへの到達可能性を確認してください
- 古いファブリックでSDAVCを有効にしている場合は、新しいファブリックで有効にしてください（クラスタの場合は、1つのノードでのみ有効にする必要があります）
- 構成データベースの復元は、元のファブリックと同じバージョンでのみサポートされます
- コントローラに使用されているペルソナを確認します。COMPUTE_DATAおよびDATAペルソナをサポート（各セクションで詳細を説明）
- エンタープライズCAの場合は、エンタープライズCAによって発行されたルート証明書（既存のオーバーレイで使用）を使用する必要があります。証明書はエンタープライズCAサーバを使用して署名され、UIを介してすべてのコントローラにインストールされます

導入オプション

vManageの導入

- スタンドアロン（1ノード）
- クラスタ（3ノードまたは6ノード）

DRオプション

- DRなし
- シングルノードDR
- スタンバイDRクラスタ（手動/管理トリガー）

注：ディザスタリカバリのタイプの詳細については、次のリンクを参照してください。

組み合せ:

#	vManageの設定	DRオプション
1	スタンドアロン（1ノード）	DRなし
2	スタンドアロン（1ノード）	シングルノードDR
3	クラスタ（3ノードまたは6ノード）	DRなし
4	クラスタ（3ノードまたは6ノード）	スタンバイDRクラスタ

すべての組み合わせに適用できる共通の手順

これらの手順は、すべての導入の組み合わせに共通です。VMインスタンスを起動し、基本的なCLI設定を適用するプロセスについて説明します。各組み合わせセクションには、導入するインスタンスの数と完了すべき追加手順が記載されています。

SD-WANコントローラのインストールと起動（マネージャ、バリデータ、コントローラ）

注：シスコは特定の用語をブランド変更したため、これらの用語には互換性があります。Cisco vManage = Cisco Catalyst Manager、Cisco vBond = Cisco Catalyst Validator、Cisco vSmart = Cisco Catalystコントローラ

ここにあるシスコソフトウェアダウンロードページからSD-WANコントローラ用のOVAファイルをダウンロードします。

- vEDGE Cloudを選択し、必要なソフトウェアバージョンのvBond OVAをダウンロードします。
- vManageソフトウェアを選択し、必要なソフトウェアバージョンのvManage OVAをダウンロードします。
- vSmartソフトウェアを選択し、必要なソフトウェアバージョンのvSmart OVAをダウンロードします。

注:ESXi/クラウドプラットフォームで、OVAファイルを使用してvSmart、vBond、およびvManageコントローラをスピンアップします。リンクされたドキュメントを参照し、SD-WAN導入タイプに応じて、すべてのコントローラに十分なCPU、RAM、およびディスクが割り当てられていることを確認します。詳細については、ここを参照してください。リンクされたコンピューティングガイドのストレージサイズ*の列に記載されているように、vManageノードにセカンダリディスクを割り当ててください。

Cisco Managerノードの起動

- Cisco ManagerまたはvManage VMが導入され、マネージャのコンソールにアクセスできるようになったら、起動が完了するまで待ちます。その1つは、system is readyというメッセージが表示され、ユーザ名とパスワードの入力を求められることです。
- デフォルトのユーザクレデンシャルであるユーザ名をadminとして、パスワードをadminとして入力します。ユーザにパスワードの変更を求めるプロンプトが表示されたら、ユーザadminに必要なパスワードを任意に設定します。
- 次に、ユーザに対してペルソナを選択するよう求められます。vManageクラスタを使用する場合、これは重要な手順です。次のシナリオに従って、ペルソナを選択してください。

```
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
```

例：COMPUTE_AND_DATAに1を選択

```
booted via startup_32()
Physical KASLR using RDRAND RDTSC...
Virtual KASLR using RDRAND RDTSC...

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

viptela 20.12.5.1

vmanage login:
viptela 20.12.5.1

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

次に示すように、セカンダリディスクを選択します。

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

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

- セカンダリディスクを選択し、Yを入力して確定します。
- Cisco Managerがリロードします。起動したら、新しく設定した新しいパスワードでユーザ名とパスワードを入力します。

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

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

viptela 20.12.5.1

vmanage login:
viptela 20.12.5.1

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

- VPN 512 管理インターフェイスを設定して、コントローラへのアウトオブバンド管理アクセスを有効にできます。
- show interface | tabコマンドを使用して、インターフェイスが現在マップされているVPNを確認します。
- それに応じてインターフェイスを設定します。

例

```
                              SPEED          MSS                 RX       TX

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

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

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

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

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

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


vmanage#
```

注：ここでは、既存のvManageの設定を参照し、同じIPアドレス方式を設定できます。

管理インターフェイス(VPN 512)の設定

- インターフェイスをVPN 0からVPN 512に移動する必要がある場合は、次のコマンドを使用して、インターフェイスのIPアドレスを設定します

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




  no shutdown
 !
 ip route 0.0.0.0/0



!
```

バリデータの起動

- ハイパーバイザで、vBondノードに必要なコンピューティング（CPU、RAM、およびディスク）を設定し、電源をオンにします。
- コンソールにアクセスできるようになったら、vBondが完全に起動するまで待ちます。メッセージ「System Ready」が表示されるまで待ちます。
- 次に、ユーザ名とパスワードの入力を求められます。 デフォルトのユーザクレデンシャルであるユーザ名をadminとして、パスワードをadminとして入力します。 パスワードの変更を求めるプロンプトが表示されたら、ユーザadminに必要なパスワードを任意に設定します。
- VPN 512管理インターフェイスを設定して、コントローラへのアウトオブバンド管理アクセスを有効にすることができます。
- show interface | tabコマンドを使用して、インターフェイスが現在マップされているVPNを確認します。
- それに応じてインターフェイスを設定します。

例：

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

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

vbond-01#
```

注：既存のvBondの設定を参照し、同じ設定をここで設定できます。

管理インターフェイス(VPN 512)の設定

- インターフェイスをVPN 0からVPN 512に移動する必要がある場合は、次のコマンドを使用して、インターフェイスのIPアドレスを設定します。

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




  no shutdown
 !
 ip route 0.0.0.0/0



!
commit
```

コントローラ(vSmart)ノードの起動

- バリデータと同じ手順を実行して、vSmartノードを起動します。
- すべてのSD-WANコントローラでVPN 512 IPアドレスを設定すると、VPN 512 IPアドレスでSSHを使用してそれらにアクセスできます。

すべてのコントローラでの基本的なCLI設定

すべてのコントローラへのSSHアクセスが可能になったら、各コントローラでこれらのCLI設定を行います。

システム設定

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注:vBondアドレスとしてURLを使用している場合は、DNSサーバのIPアドレスをVPN 0設定で設定するか、解決できることを確認してください。

トランスポートインターフェイス(VPN 0)の設定

これらの設定は、ルータおよびその他のコントローラとの制御接続の確立に使用されるトランスポートインターフェイスを有効にするために、すべてのコントローラで必要です。

```
config t
vpn 0
 dns



        primary
 dns



         secondary
 interface eth1
  ip address



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



commit
```

注：既存のコントローラの設定を参照できます。設定が存在する場合は、この設定を新しいコントローラに追加できます。

ルータがTLSを使用してvManageノードとのセキュアな制御接続を確立する必要がある場合にのみ、制御プロトコルをTLSとして設定します。 デフォルトでは、すべてのコントローラとルータがDTLSを使用して制御接続を確立します。これは、要件に応じてvSmartおよびvManageノードでのみ必要なオプションの設定です。

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

組み合わせ1：スタンドアロンvManage + DRなし

必要なインスタンス

- 1 vManage(COMPUTE_AND_DATA)
- 1つ以上のvBond
- 1つ以上のvSmart

手順：

1. 共通ステップを使用してすべてのインスタンスを起動する
2. 事前チェック
3. vManage UI、証明書、およびオンボードコントローラの設定
4. Config-dbバックアップ/復元
5. 事後チェック

ステップ1：事前チェック

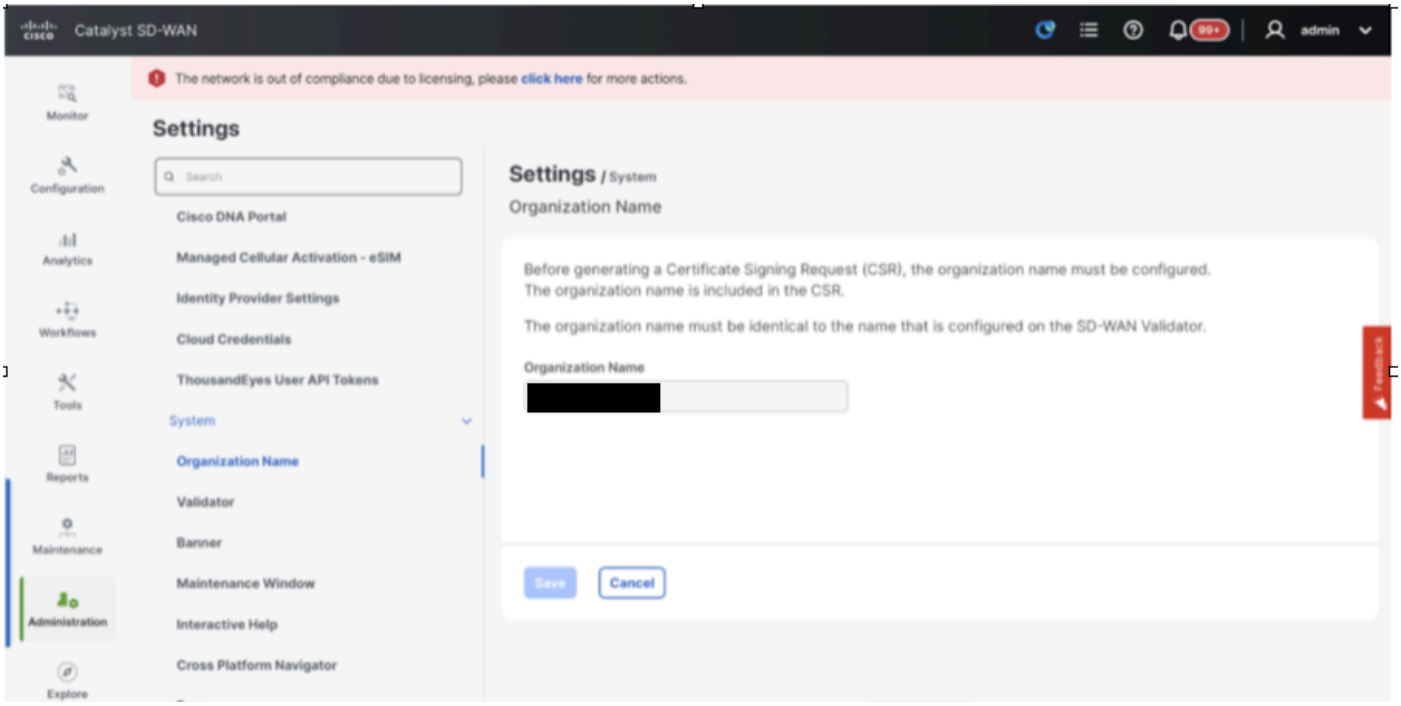
- アクティブなCisco SD-WAN Manager インスタンスの数が、新しくインストールしたCisco SD-WAN Manager インスタンスの数と同じであることを確認します。

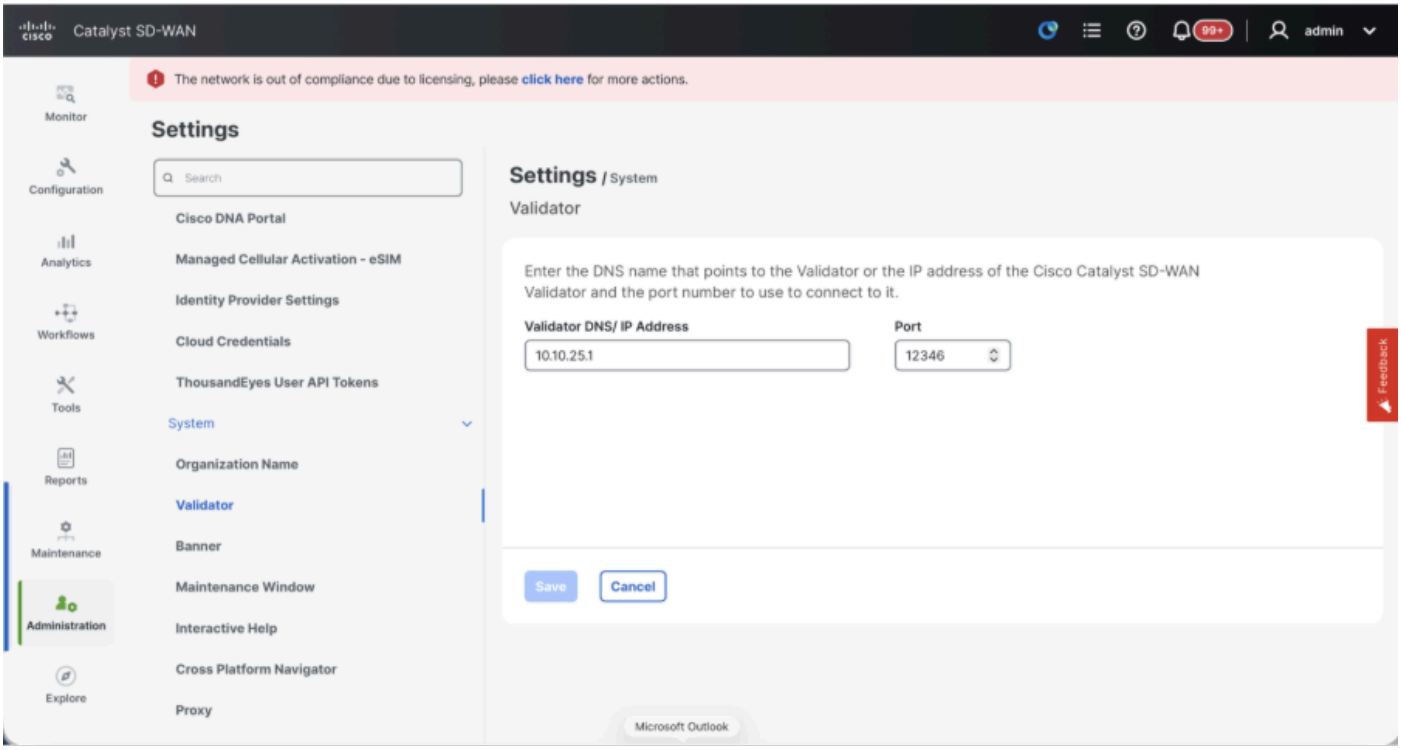
- アクティブなCisco SD-WAN Managerインスタンスと新しいCisco SD-WAN Managerインスタンスのソフトウェアバージョンがすべて同じであることを確認します。
- アクティブおよび新規のすべてのCisco SD-WAN Managerインスタンスが、Cisco SD-WAN Validatorの管理IPアドレスに到達できることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスに証明書がインストールされていることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスを含め、すべてのCisco Catalyst SD-WANデバイスのクロックが同期されていることを確認します。
- 新しくインストールされたCisco SD-WAN Managerインスタンスで、システムIPとサイトIDの新しいセットが、アクティブクラスタと同じ基本設定とともに設定されていることを確認します。

手順2:vManage UI、証明書、オンボードコントローラを設定します。

vManage UIでの設定の更新

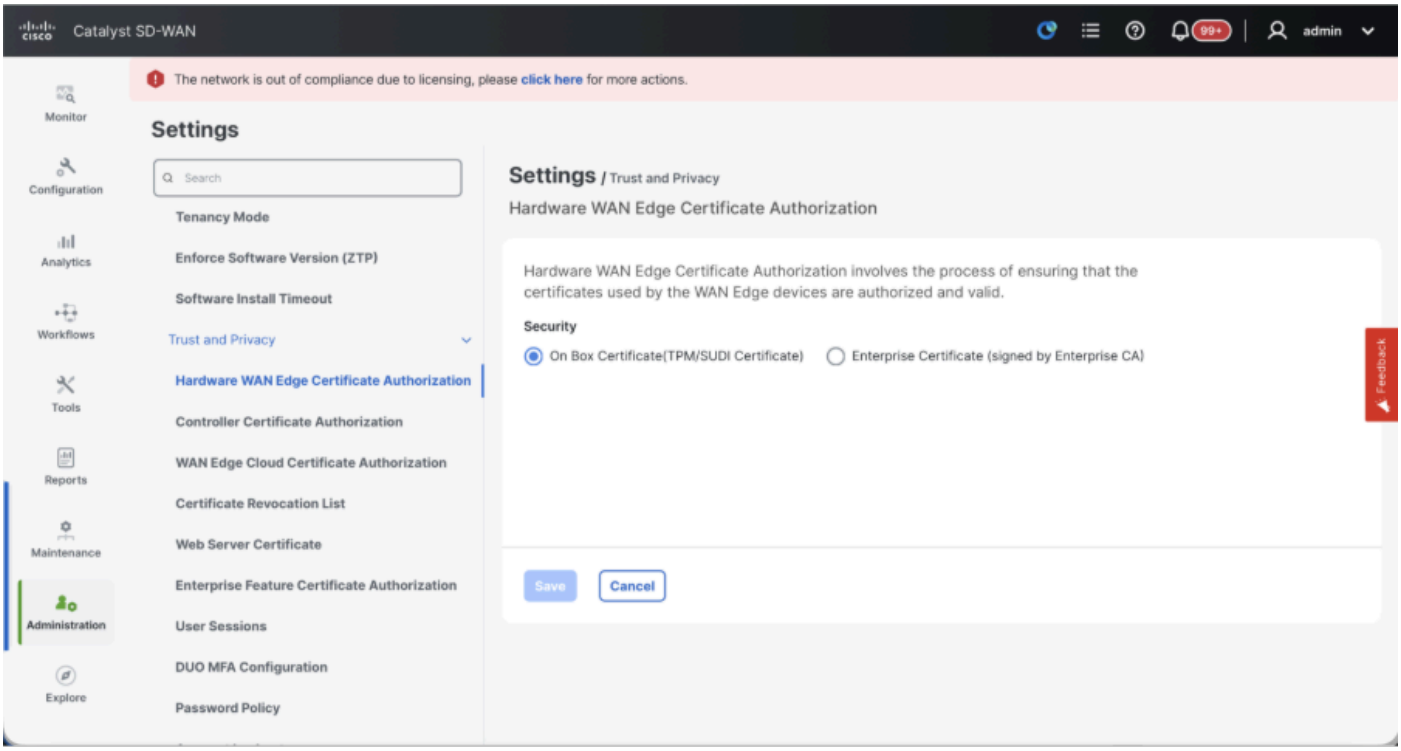
- ステップ1の設定がすべてのコントローラのCLIに追加されたら、ブラウザでURL https://<vmanage-ip>を使用して、vManageのWebUIにアクセスできます。各vManageノードのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- Administration > Settingsの順に移動し、次の手順を実行します。
- 組織名とValidator/vBond URL/IPアドレスを設定します。vManageノードのCLIと同じ値を設定します。
- vManage 20.15/20.18では、これらの設定はシステムのセクションで利用できます。



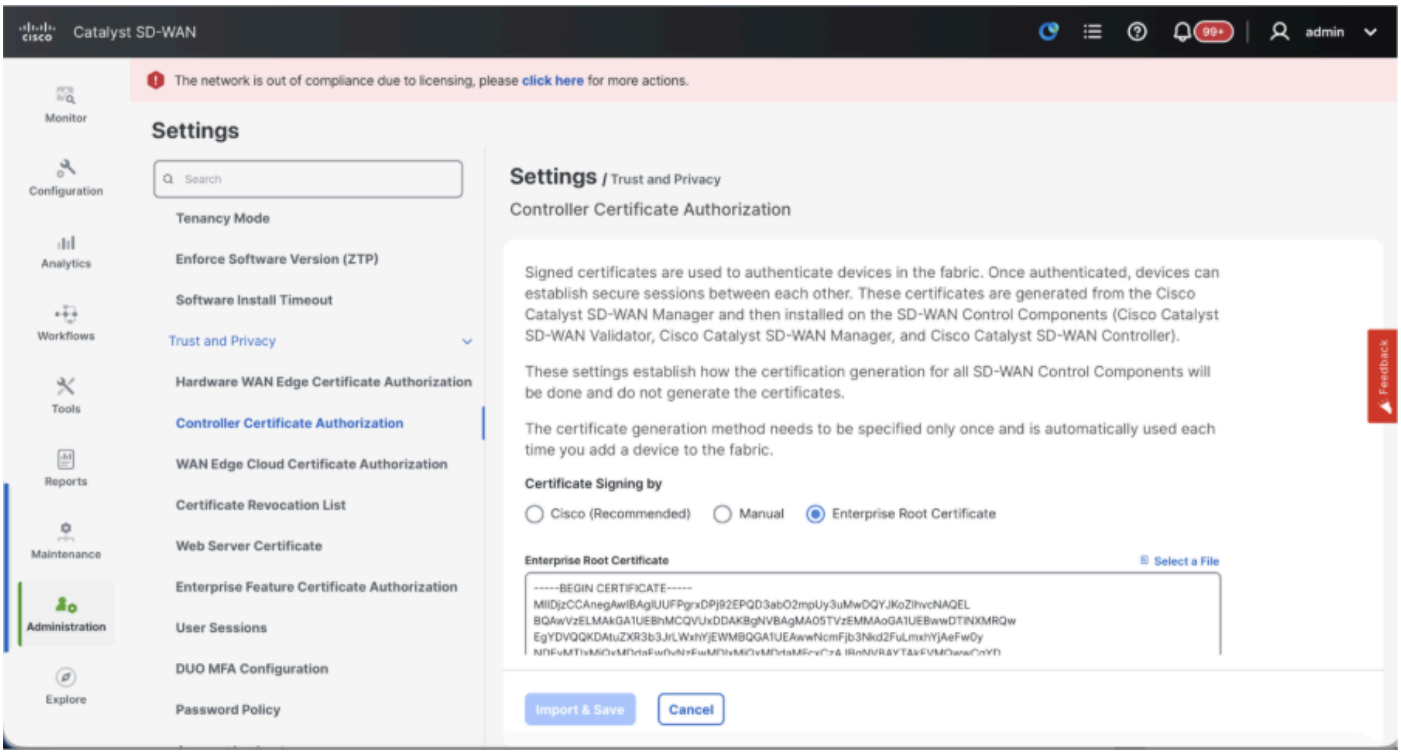


- 証明書の署名に使用する認証局(CA)を決定する証明書承認(CA)の設定を確認します。3つのオプションがあります。

1. ハードウェアWANエッジ証明書認証：ハードウェアSD-WANエッジルータのCAを決定します。
    - オンボックス証明書（TPM/SUDI証明書）– このオプションを使用すると、制御接続（TLS/DTLS接続）を確立するために、ルータハードウェアにプレインストールされている証明書が使用されます
    - エンタープライズ証明書（エンタープライズCAによって署名された）– このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

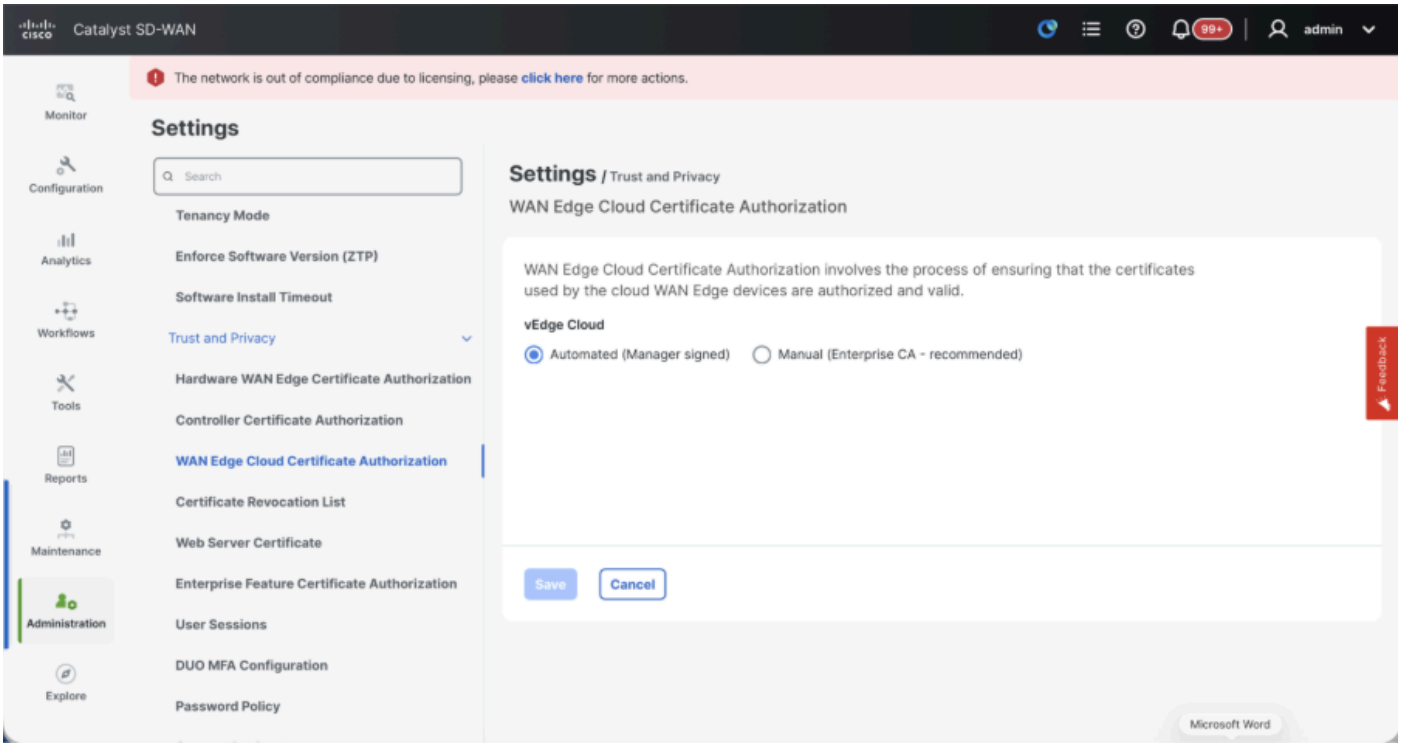


2. Controller Certificate Authorization（コントローラ証明書認証）:SD-WANコントローラのCAを決定します。
    - シスコ（推奨）– コントローラはCisco PKIによって署名された証明書を使用します。vManageは、vManageで設定されたスマートアカウント資格情報を使用してPNPポータルに自動的に接続し、証明書に署名してコントローラにインストールされます。
    - 手動：コントローラはCisco PKIによって署名された証明書を使用します。それぞれのSD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用して手動でCSRに署名します。
    - エンタープライズルート証明書：このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

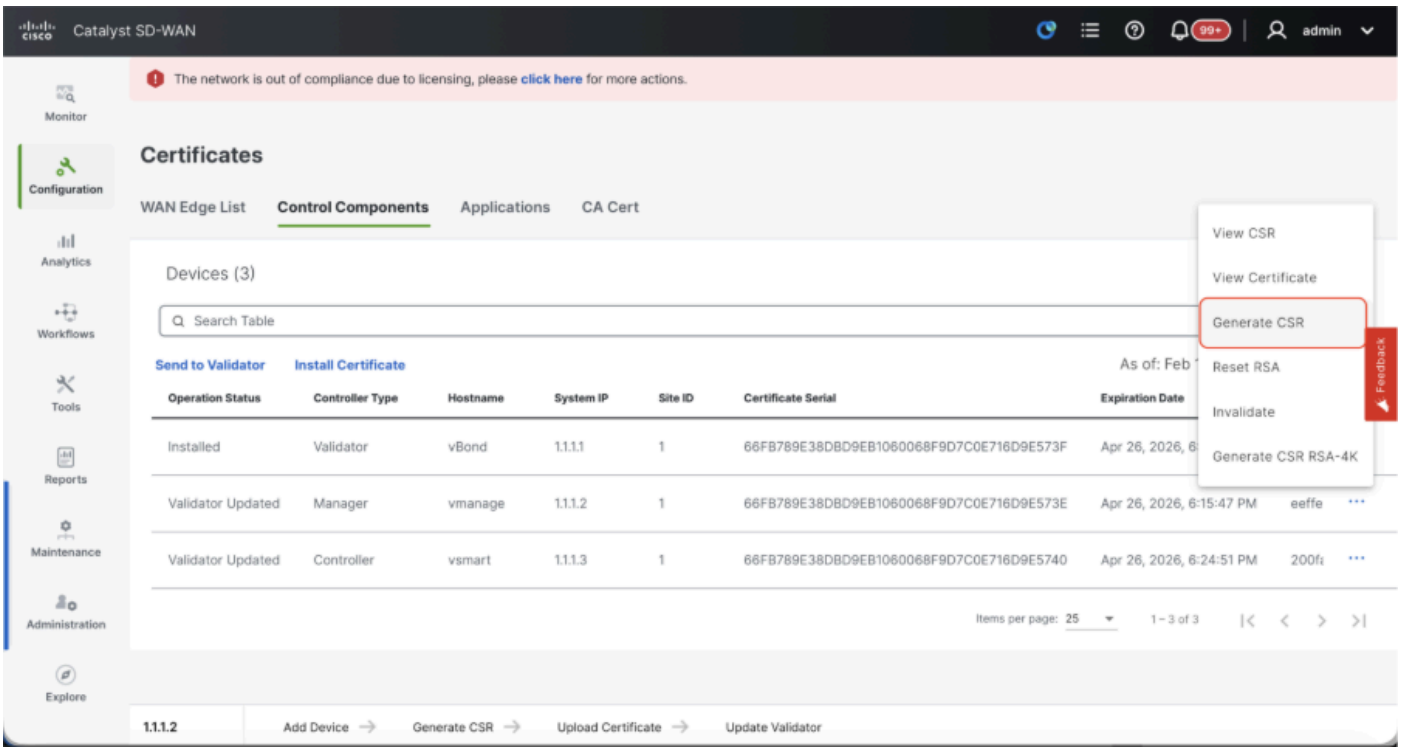


3. WANエッジクラウド証明書認証：仮想SD-WANエッジルータ（CSR1000v、C8000v、vEdgeクラウド）のCAを決定します。
    - 自動（vManage署名済み）:vManageは、仮想エッジルータのCSRに自動的に署名し、証明書をルータにインストールします。
    - 手動（エンタープライズCA – 推奨）– 仮想ルータは、組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

独自のCA（エンタープライズ認証局）を使用している場合は、Enterpriseを選択します。



- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers
- Manager/vManageの「。..」をクリックし、「CSRの生成」をクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。

vBond/ValidatorおよびvSmart/ControllerのvManageへのオンボーディング

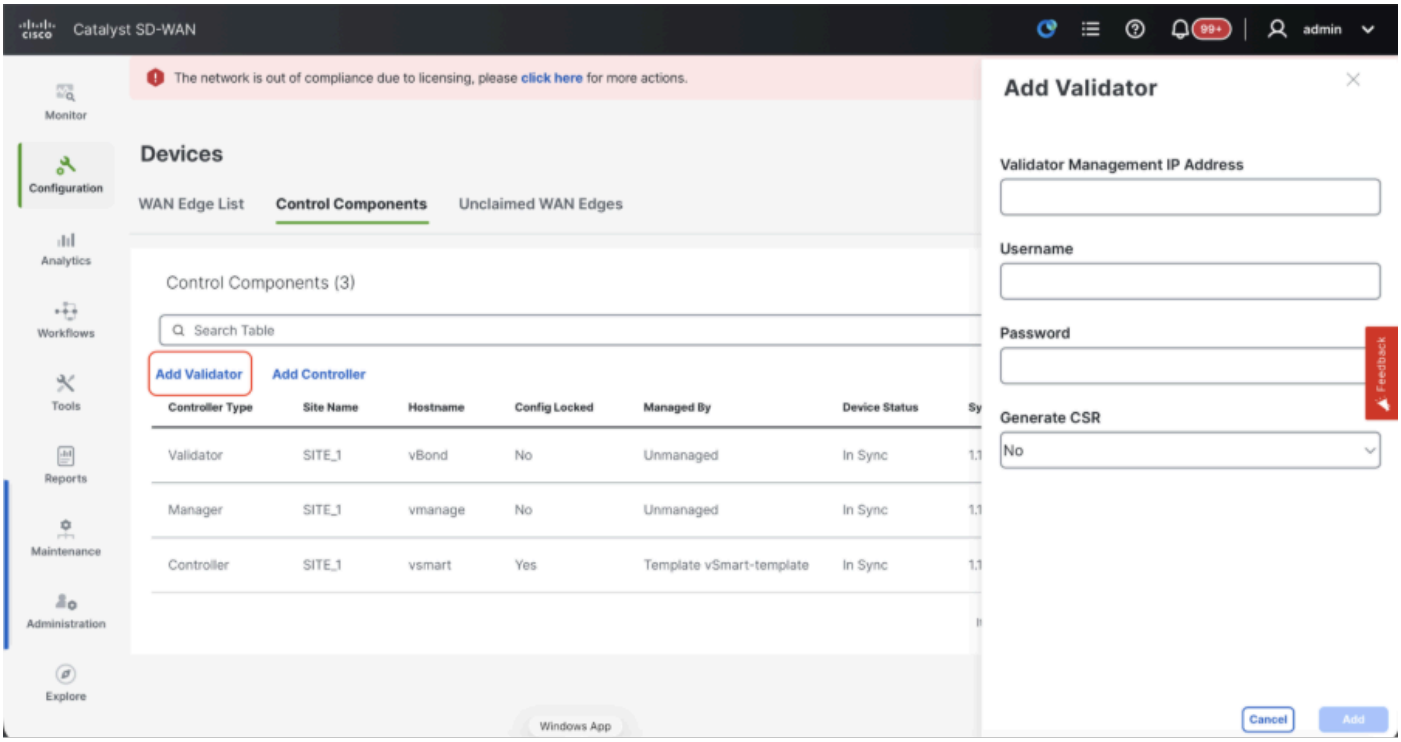
20.15/20.18 vManageノードの場合は、Configuration > Devices > Control Componentsの順に移動します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

オンボーディングvBond/バリデータ

- onAddvBondをクリックします20.12vManagerの場合バリデータの追加 20.15/20.18vManageの場合。ポップアップが表示されたら、 VPN 0は、vManageから到達可能なvBondのIPを転送します。
- vManagetovBondIPのCLIからpingを使用して（許可されている場合）到達可能性を確認します。
- vBondのユーザクレデンシャルを入力します。

注:NetAdminグループのユーザ部分であるvBondorの管理者クレデンシャルを使用する必要があります。これはthevBondのCLIで確認できます。vBondの新しい証明書をインストールする必要がある場合は、「CSRの生成」のドロップダウンでYesを選択します。

注:vBondがNATデバイス/ファイアウォールの背後にある場合は、vBond VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認してください。VPN 0インターフェイスIPにvManageから到達できない場合は、このステップでVPN 0インターフェイスのパブリックIPアドレスを使用します。

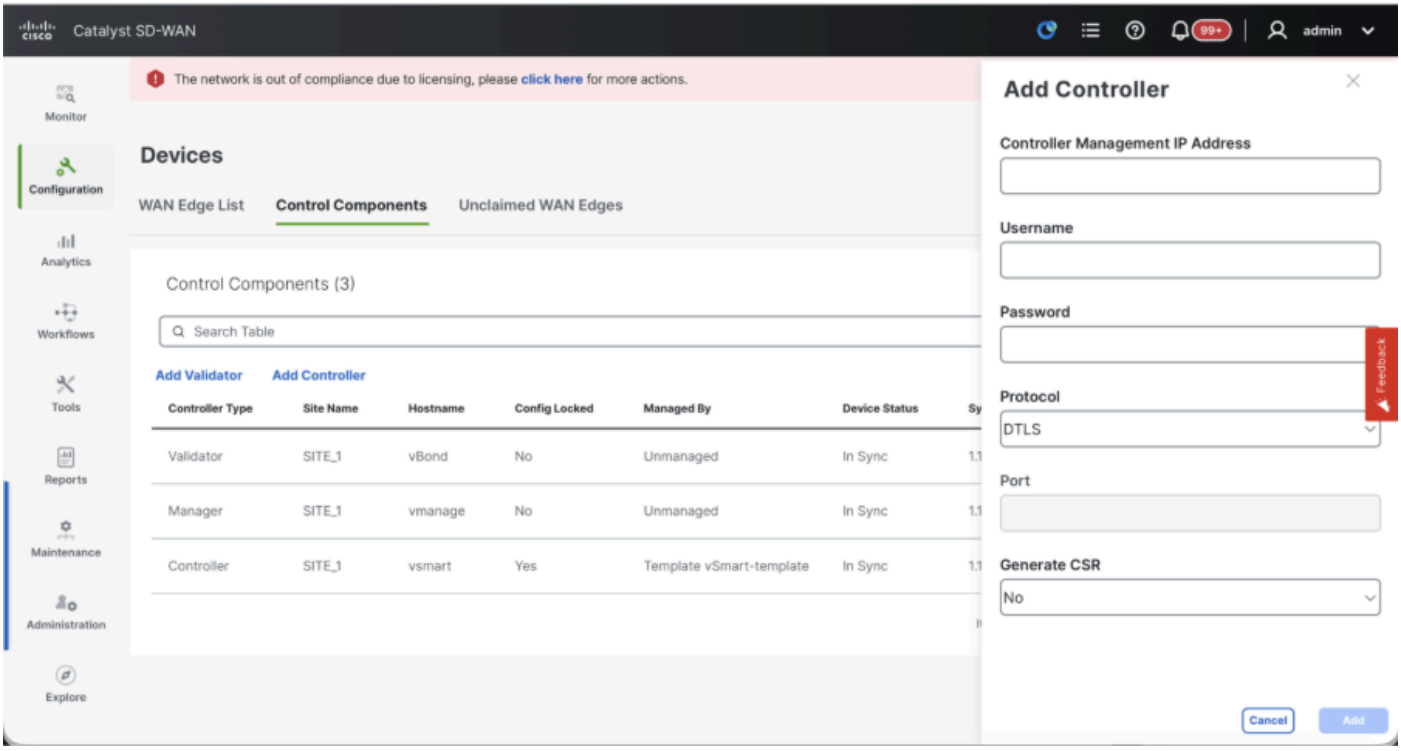


- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vBondに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvBondがある場合は、同じ手順を繰り返します。

vSmart/コントローラのオンボーディング

- 20.12 vManageの場合はAdd vSmartを、20.15/20.18 vManageの場合はAdd Controllerをクリックします。
- ポップアップが開いたら、vManageから到達可能なvSmartのVPN 0トランスポートIPを入力します。
- vManageのCLIからvSmart IPにpingを使用して（許可されている場合）到達可能性を確認します。
- vSmartの管理者クレデンシャルまたはnetadminグループのユーザ部分を使用する必要があるvSmart Noteのユーザクレデンシャルを入力します。
- これは、vSmartのCLIで確認できます。
- ルータにTLSを使用してvSmartとの制御接続を確立する場合は、プロトコルをTLSに設定します。 この構成は、vSmartsおよびvManageノードのCLIでも構成する必要があります。
- vSmartの新しい証明書をインストールする必要がある場合は、「Generate CSR」のドロップダウンで「Yes」を選択します。

注：vSmartがNATデバイス/ファイアウォールの背後にある場合は、vSmart VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認し、VPN 0インターフェイスIPがvManageから到達できない場合は、この手順でVPN 0インターフェイスIPのパブリックIPアドレスを使用します。

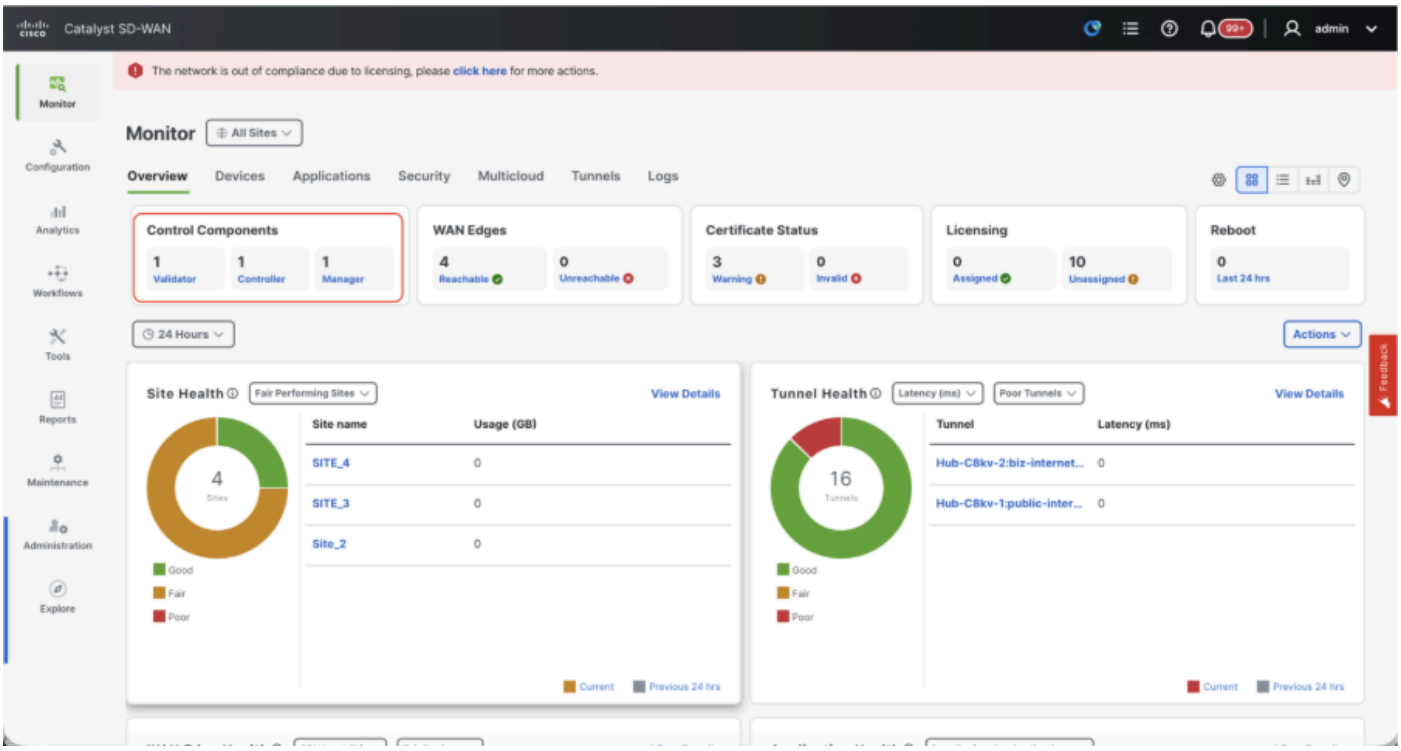


- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate

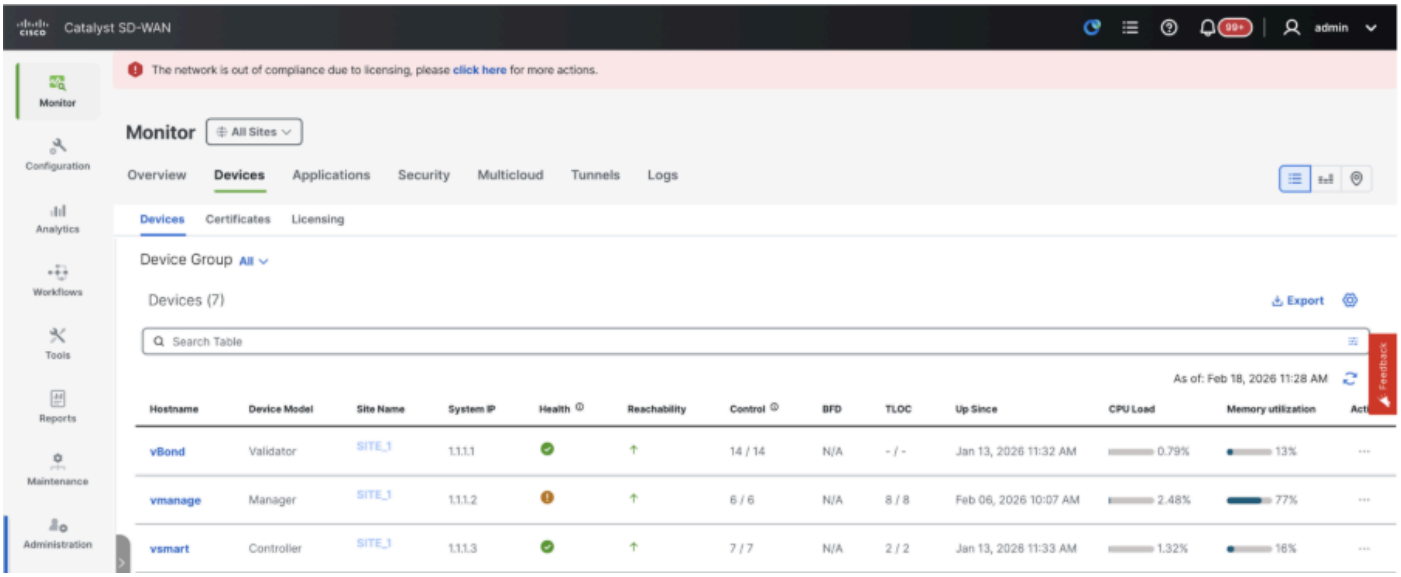
Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vSmartに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。 Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- 複数のvSmartsがある場合は、同じ手順を繰り返します。

検証

すべての手順が完了したら、Monitor>Dashboardですべての制御コンポーネントに到達できることを確認します



- それぞれの制御コンポーネントをクリックして、それらがすべて到達可能であることを確認します。
- Monitor > Devicesの順に移動し、すべての制御コンポーネントが到達可能であることを確認します。



ステップ3:Config-dbのバックアップ/復元

別のvManageノードでのvManage構成データベースのバックアップと復元の収集

Configuration-DBバックアップの収集：

- 現在使用されているSD-WANファブリックでは、スタンドアロンのvManageとvManageクラスタの両方のセットアップでconfiguration-dbバックアップを生成できます。
- スタンドアロンvManageの場合、そのvManage自体がconfiguration-dbのリーダーです。

configuration-dbがvManageノードで実行されていることを確認します。

同じことを確認するには、request nms configuration-db status onvManageCLIコマンドを使用します。出力は次のようになります

```
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#
```

このコマンドを使用して、特定されたconfiguration-dbリーダーのvManageノードからconfiguration-dbのバックアップを収集します。

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

予想される出力は次のとおりです。

```
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#
```

- configuration-dbクレデンシャルが更新されている場合は、それをメモします。
- configuration-dbクレデンシャルを知らない場合は、TACに問い合わせて、既存のvManageノードからconfiguration-dbクレデンシャルを取得してください。

- デフォルトのconfiguration-dbクレデンシャルは、ユーザ名：neo4jおよびパスワード：passwordです。

構成データベースのバックアップを別のvManageノードに復元

SCPを使用して、vManageの/home/admin/ディレクトリにconfiguration-dbバックアップをコピーします。

scpコマンドの出力例：

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

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

configuration-dbのバックアップを復元するには、まずconfiguration-dbのクレデンシャルを設定する必要があります。configuration-dbクレデンシャルがデフォルト(neo4j/password)の場合は、このステップを省略できます。

configuration-dbクレデンシャルを設定するには、request nms configuration-db update-admin-userコマンドを使用します。任意のユーザ名とパスワードを使用します。

vManageのアプリケーションサーバが再起動します。このため、vManage UIに短時間アクセスできなくなります。

```
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#
```

設定データベースのバックアップの復元に進むことができる投稿：

コマンドrequest nms configuration-db restore path /home/admin/< >を使用して、新しいvManageに設定データベースを復元できます。

```
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
```

configuration-dbが復元されたら、vManage UIにアクセスできることを確認します。5分ほど待ってから、UIへのアクセスを試みます。

UIに正常にログインしたら、エッジルータのリスト、テンプレート、ポリシー、および以前または既存のvManage UIに存在していた残りのすべての設定が、新しいvManage UIに反映されていることを確認します。

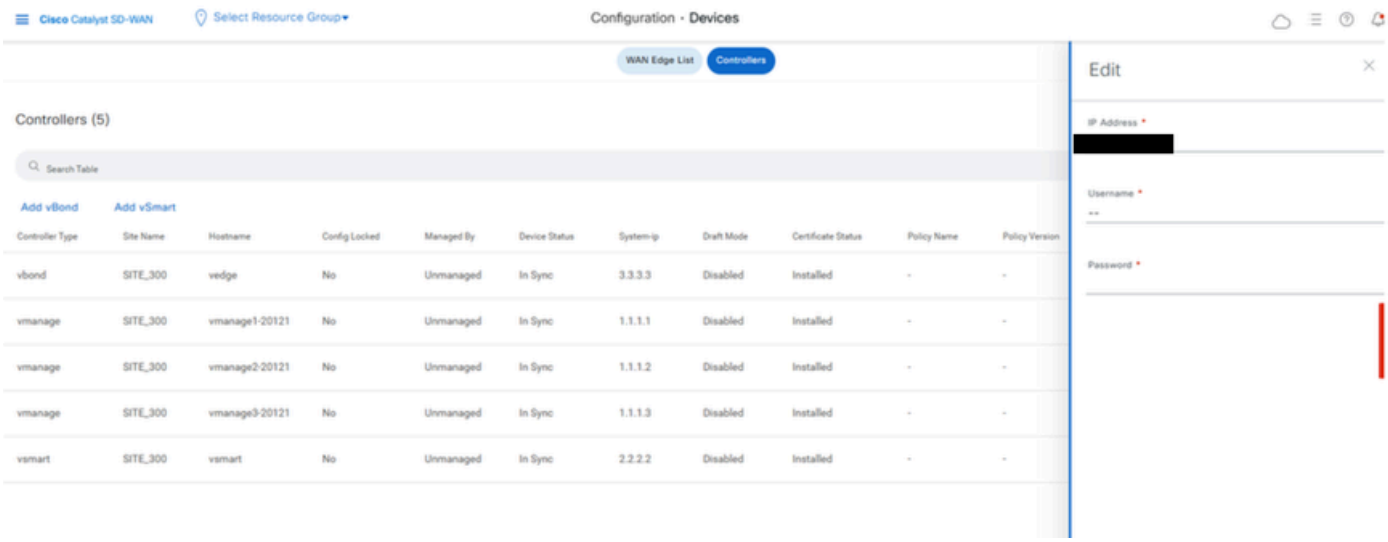
ステップ4：コントローラの再認証と古いコントローラの無効化

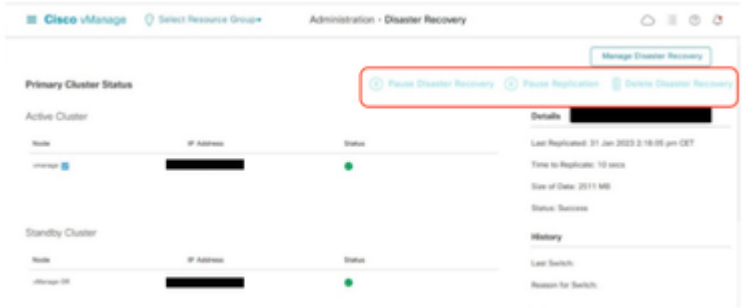
configuration-dbが復元されたら、ファブリック内のすべての新しいコントローラ(vmanage/vsmart/vbond)を再認証する必要があります。

注：実際の運用で、再認証に使用されるインターフェイスIPがトンネルインターフェイスIPである場合、vManage、vSmart、およびvBondのトンネルインターフェイスでNETCONFサービスが許可され、パスに沿ったファイアウォールでもNETCONFサービスが許可されるようにする必要があります。開くファイアウォールポートは、DRクラスタからすべてのvBondおよびvSmartsへの双方向ルールとしてTCPポート830です。

vmanage UIで、Configuration > Devices > Controllersの順にクリックします。

- 各コントローラの近くにある3つのドットをクリックし、[編集]をクリックします





- ip-address（コントローラのsystem-ip）をtransport vpn 0（トンネルインターフェイス）ipアドレスに置き換えます。ユーザ名とパスワードを入力し、保存をクリックします
- ファブリック内のすべての新しいコントローラに対して同じ操作を行います

Root-cert-chainの同期

すべてのコントローラがオンボーディングされたら、次の手順を実行します。

新しくアクティブになったクラスタ内の任意のCisco SD-WAN Managerサーバで、次の操作を実行します。

ルート証明書を、新しくアクティブになったクラスタ内のすべてのCisco Catalyst SD-WANデバイスと同期させるには、次のコマンドを入力します。

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

次のコマンドを入力して、Cisco SD-WAN Manager UUIDをCisco SD-WAN Validatorと同期させます。

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

ファブリックが復元され、ファブリック内のすべてのエッジとコントローラに対してコントロールセッションとbfdセッションが確立されたら、古いコントローラ(vmanage/vsmart/vbond)をUIから無効にする必要があります

- vmanage UIで、[設定] > [証明書] > [コントローラ]をクリックします。
- Controllersをクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の右側にある3つのドットをクリックします。[無効]をクリックします
- vbondに送信をクリックします。
- vmanage UIで、Configuration > Devices > Controllersの順にクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の右側にある3つのドットをクリックします。Deleteをクリックします

ステップ5:Postチェック

注：すべての導入の組み合わせに共通する、ここに示す導入後のチェックセクションを続行します。

組み合わせ2：スタンドアロンvManage +シングルノードDR

必要なインスタンス

- 1 vManage (プライマリ、COMPUTE_AND_DATA)
- 1 vManage (DRスタンバイ、COMPUTE_AND_DATA)
- 1つ以上のvBond
- 1つ以上のvSmart

手順：

1. 共通ステップを使用してすべてのインスタンスを起動する
2. 事前チェック
3. vManage UI、証明書、およびオンボードコントローラの設定
4. シングルノードDRの設定
5. Config-dbバックアップ/復元
6. 事後チェック

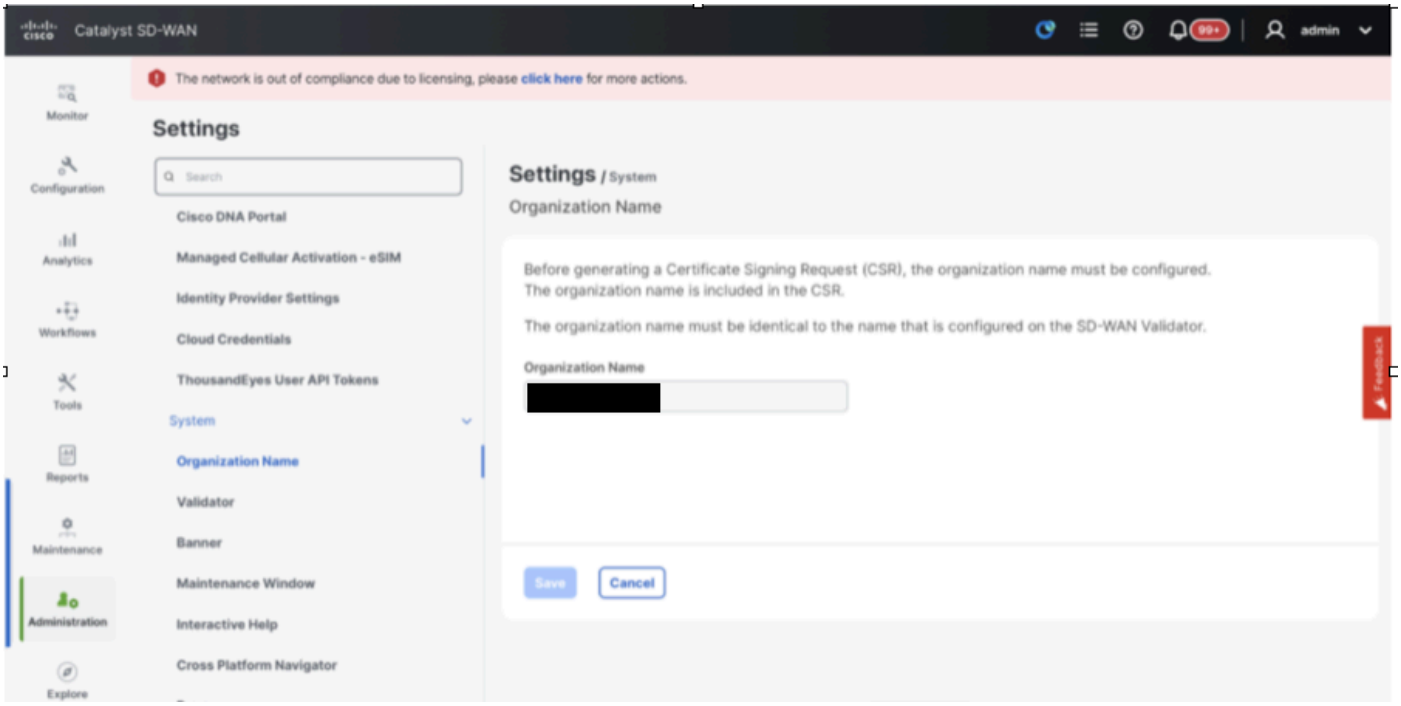
ステップ1：事前チェック

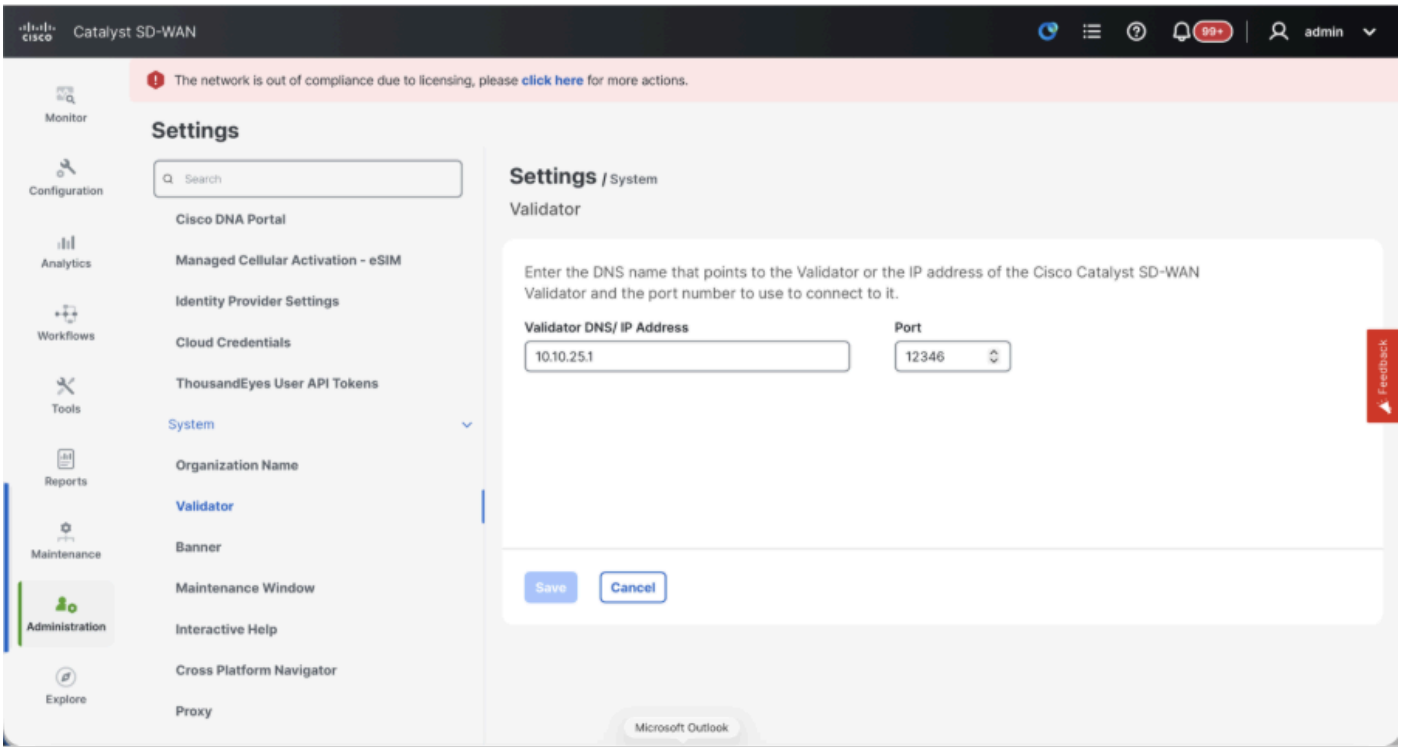
- アクティブなCisco SD-WAN Managerインスタンスの数が、新しくインストールしたCisco SD-WAN Managerインスタンスの数と同じであることを確認します。
- アクティブなCisco SD-WAN Managerインスタンスと新しいCisco SD-WAN Managerインスタンスのソフトウェアバージョンがすべて同じであることを確認します。
- アクティブおよび新規のすべてのCisco SD-WAN Managerインスタンスが、Cisco SD-WAN Validatorの管理IPアドレスに到達できることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスに証明書がインストールされていることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスを含め、すべてのCisco Catalyst SD-WANデバイスのクロックが同期されていることを確認します。
- 新しくインストールされたCisco SD-WAN Managerインスタンスで、システムIPとサイトIDの新しいセットが、アクティブクラスタと同じ基本設定とともに設定されていることを確認します。

手順2:vManage UI、証明書、オンボードコントローラを設定します。

vManage UIでの設定の更新

- ステップ1の設定がすべてのコントローラのCLIに追加されたら、ブラウザでURL https://<vmanage-ip>を使用して、vManageのWebUIにアクセスできます。各vManageノードのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- Administration > Settingsの順に移動し、次の手順を実行します。
- 組織名とValidator/vBond URL/IPアドレスを設定します。vManageノードのCLIと同じ値を設定します。
- vManage 20.15/20.18では、これらの設定はシステムのセクションで利用できます。

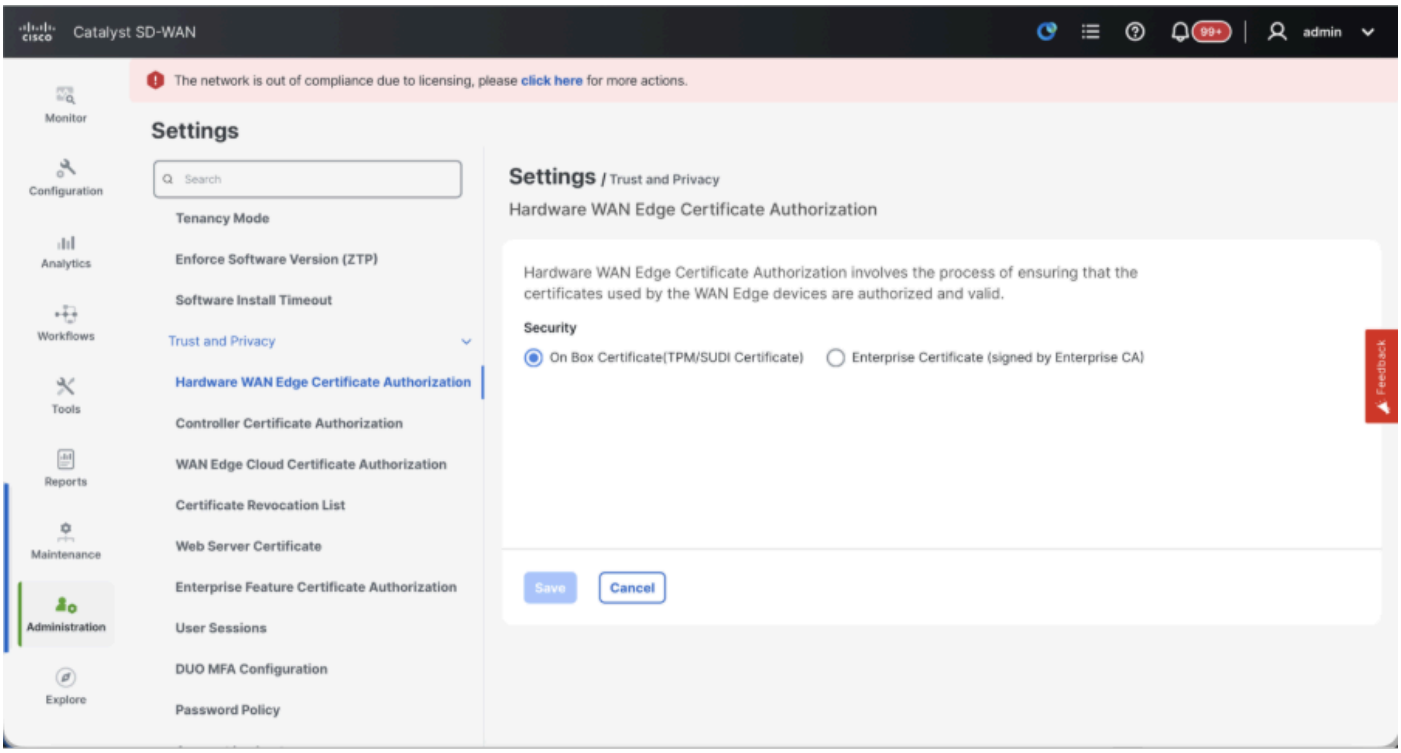




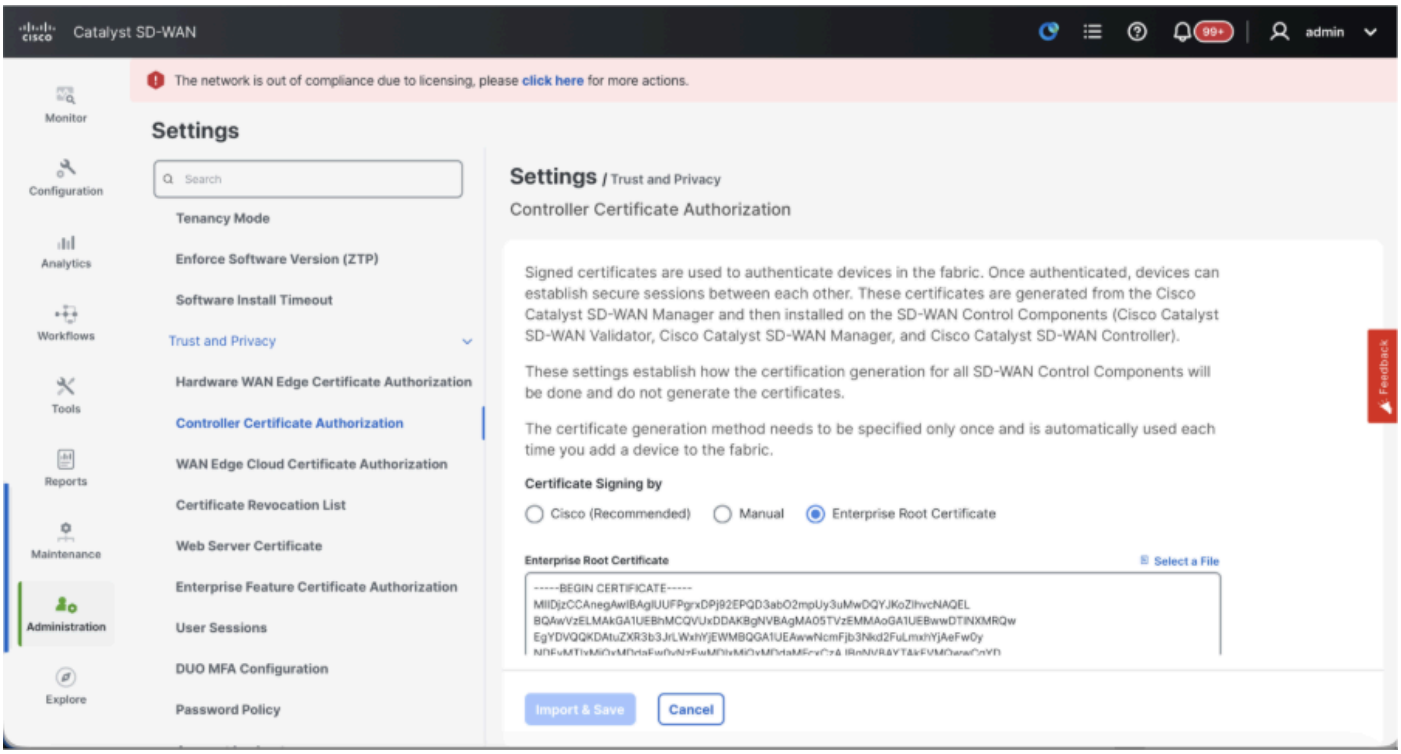
- 証明書の署名に使用する認証局(CA)を決定する証明書承認(CA)の設定を確認します。3つのオプションがあります。

1. ハードウェアWANエッジ証明書認証：ハードウェアSD-WANエッジルータのCAを決定します。
    - オンボックス証明書（TPM/SUDI証明書）– このオプションを使用すると、制御接続（TLS/DTLS接続）を確立するために、ルータハードウェアにプレインストールされている証明書が使用されます
    - エンタープライズ証明書（エンタープライズCAによって署名された）– このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明

書をここで更新する必要があります。

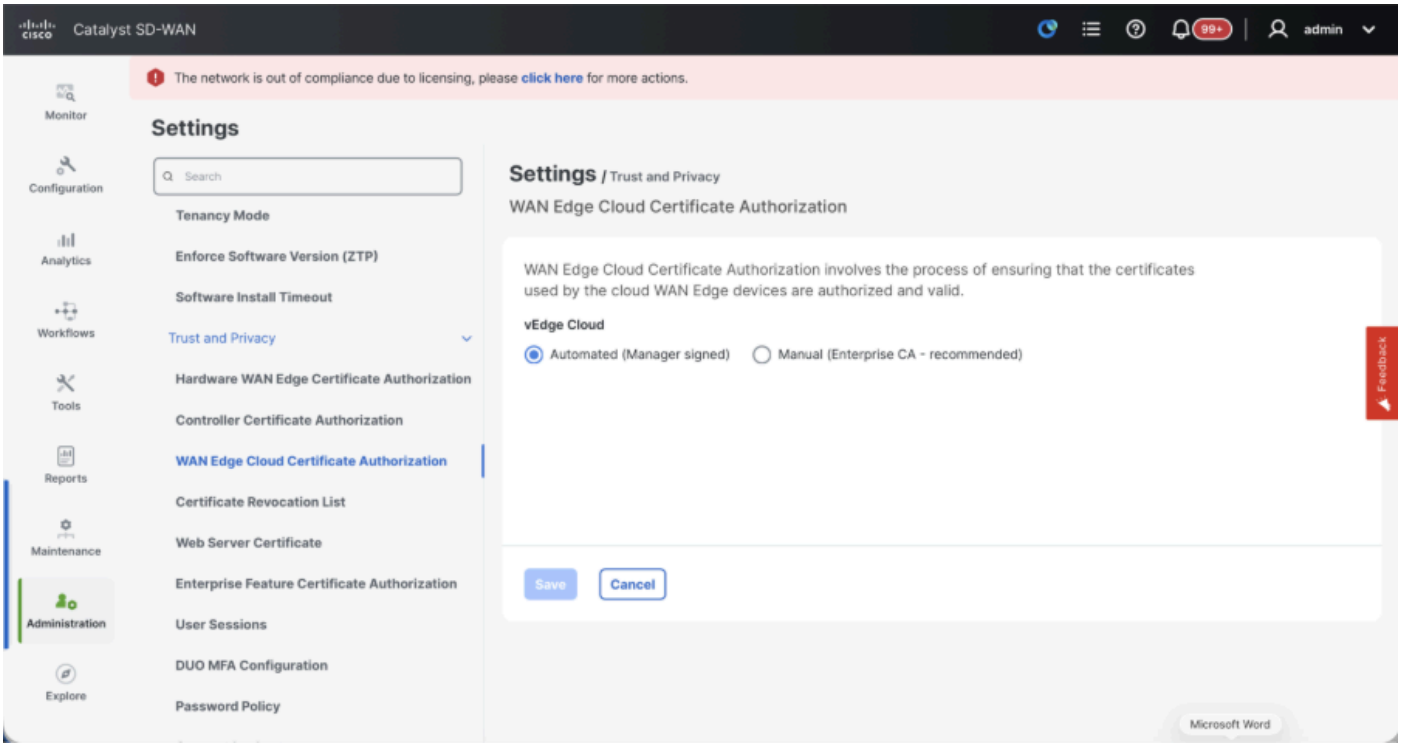


2. Controller Certificate Authorization（コントローラ証明書認証）:SD-WANコントローラのCAを決定します。
    - シスコ（推奨）– コントローラはCisco PKIによって署名された証明書を使用します。vManageは、vManageで設定されたスマートアカウント資格情報を使用してPNPポータルに自動的に接続し、証明書に署名してコントローラにインストールされます。
    - 手動：コントローラはCisco PKIによって署名された証明書を使用します。それぞれのSD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用して手動でCSRに署名します。
    - エンタープライズルート証明書：このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

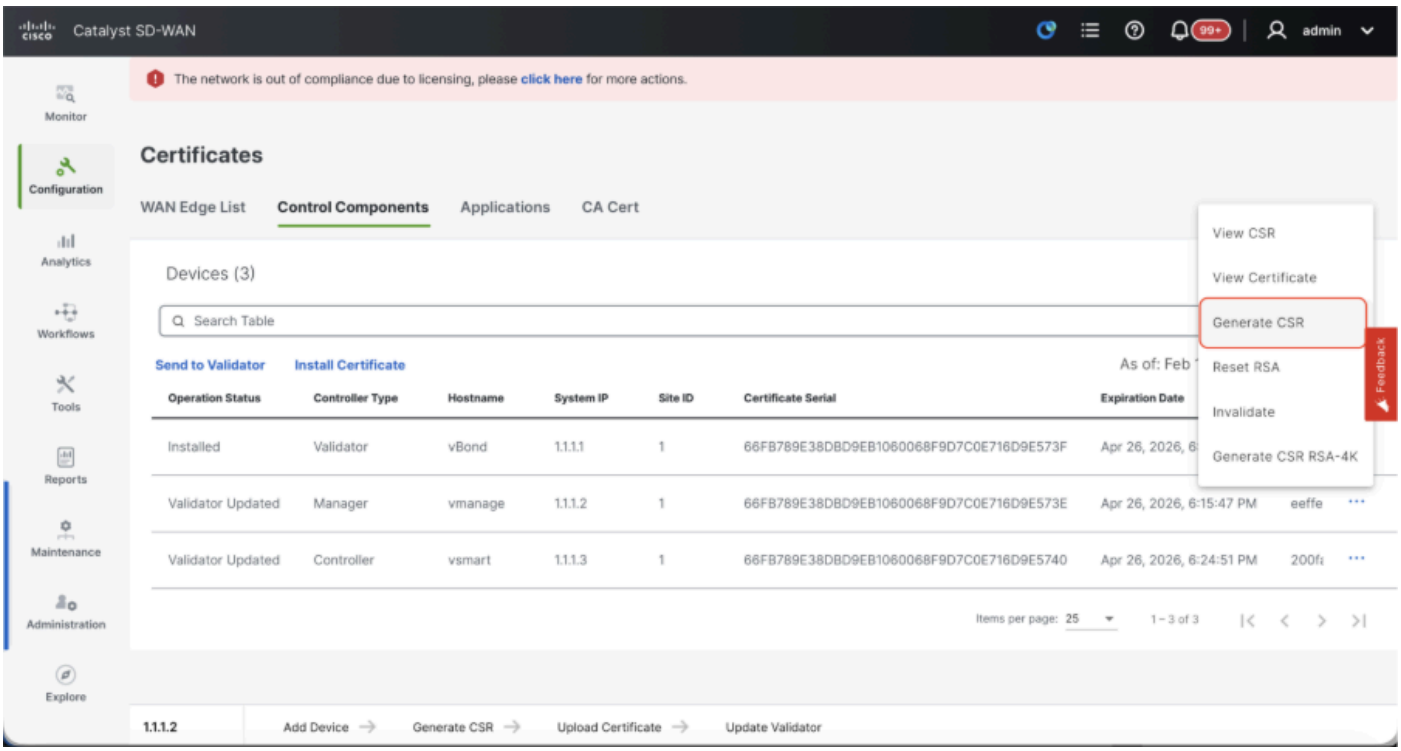


3. WANエッジクラウド証明書認証：仮想SD-WANエッジルータ（CSR1000v、C8000v、vEdgeクラウド）のCAを決定します。
    - 自動（vManage署名済み）:vManageは、仮想エッジルータのCSRに自動的に署名し、証明書をルータにインストールします。
    - 手動（エンタープライズCA – 推奨）– 仮想ルータは、組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

独自のCA（エンタープライズ認証局）を使用している場合は、Enterpriseを選択します。



- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers
- Manager/vManageの「。..」をクリックし、「CSRの生成」をクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。

vBond/ValidatorおよびvSmart/ControllerのvManageへのオンボーディング

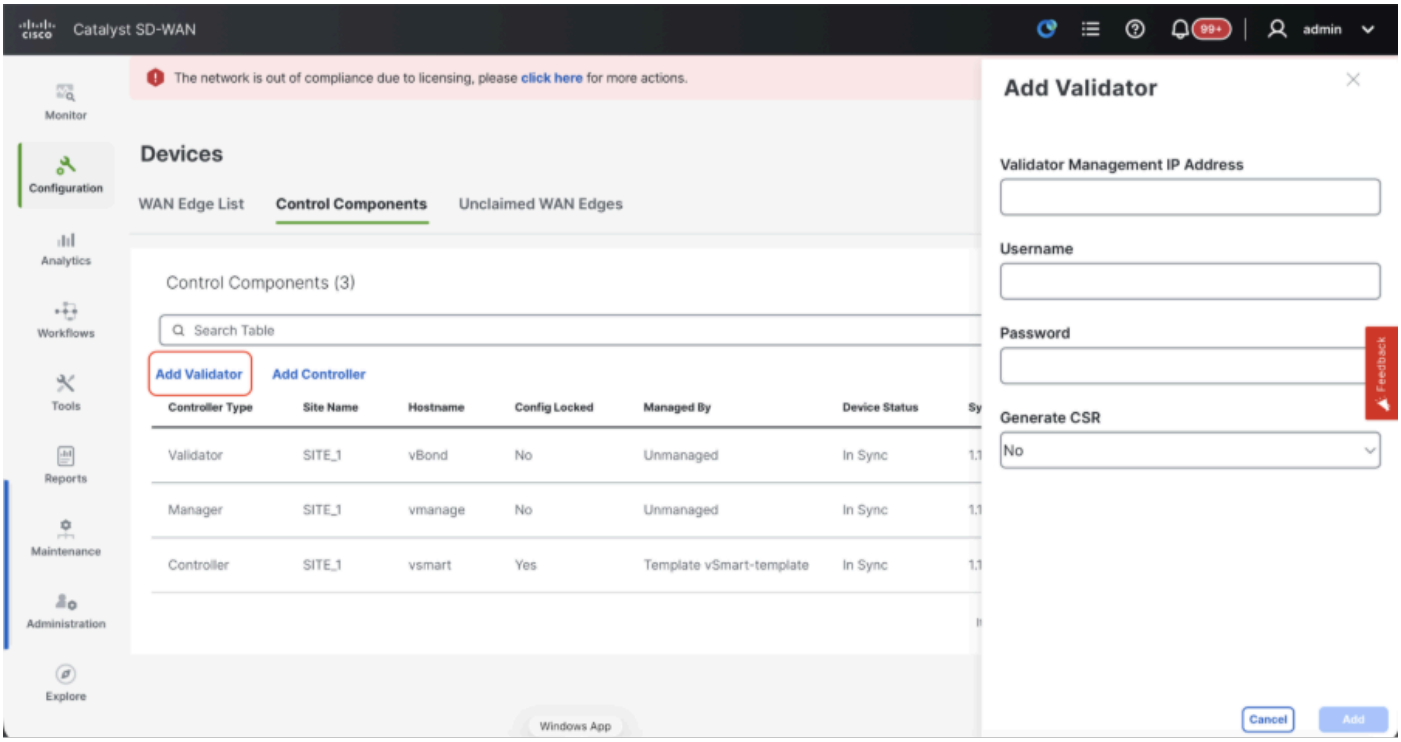
20.15/20.18 vManageノードの場合は、Configuration > Devices > Control Componentsの順に移動します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

オンボーディングvBond/バリデータ

- onAddvBondをクリックします20.12vManagerの場合バリデータの追加 20.15/20.18vManageの場合。ポップアップが表示されたら、 VPN 0は、vManageから到達可能なvBondのIPを転送します。
- vManagetovBondIPのCLIからpingを使用して（許可されている場合）到達可能性を確認します。
- vBondのユーザクレデンシャルを入力します。

注:NetAdminグループのユーザ部分であるvBondorの管理者クレデンシャルを使用する必要があります。これはthevBondのCLIで確認できます。vBondの新しい証明書をインストールする必要がある場合は、「CSRの生成」のドロップダウンでYesを選択します

注:vBondがNATデバイス/ファイアウォールの背後にある場合は、vBond VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認してください。VPN 0インターフェイスIPにvManageから到達できない場合は、このステップでVPN 0インターフェイスのパブリックIPアドレスを使用します

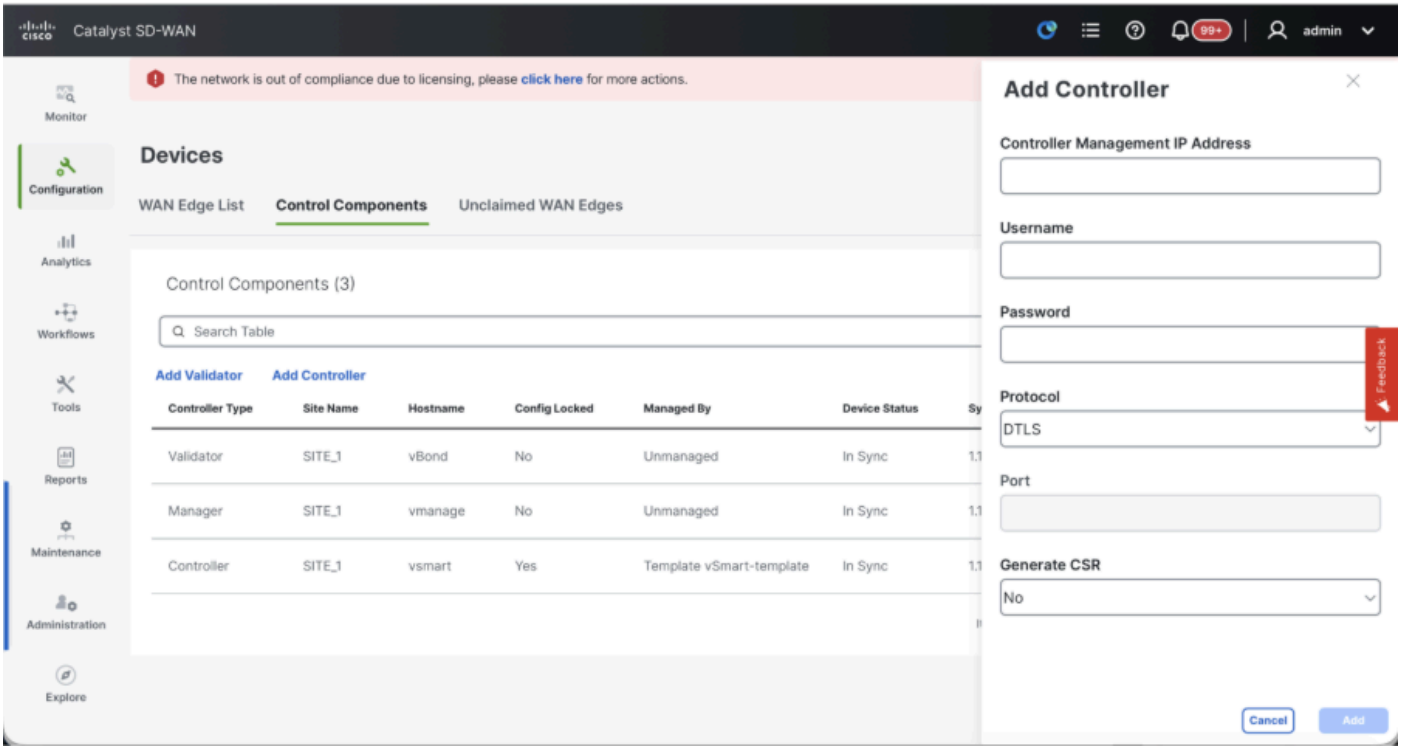


- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vBondに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvBondがある場合は、同じ手順を繰り返します。

vSmart/コントローラのオンボーディング

- 20.12 vManageの場合はAdd vSmartを、20.15/20.18 vManageの場合はAdd Controllerをクリックします。
- ポップアップが開いたら、vManageから到達可能なvSmartのVPN 0トランスポートIPを入力します。
- vManageのCLIからvSmart IPにpingを使用して（許可されている場合）到達可能性を確認します。
- vSmartの管理者クレデンシャルまたはnetadminグループのユーザ部分を使用する必要があるvSmart Noteのユーザクレデンシャルを入力します。
- これは、vSmartのCLIで確認できます。
- ルータにTLSを使用してvSmartとの制御接続を確立する場合は、プロトコルをTLSに設定します。 この構成は、vSmartsおよびvManageノードのCLIでも構成する必要があります。
- vSmartの新しい証明書をインストールする必要がある場合は、「Generate CSR」のドロップダウンで「Yes」を選択します。

注：vSmartがNATデバイス/ファイアウォールの背後にある場合は、vSmart VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認し、VPN 0インターフェイスIPがvManageから到達できない場合は、この手順でVPN 0インターフェイスIPのパブリックIPアドレスを使用します。



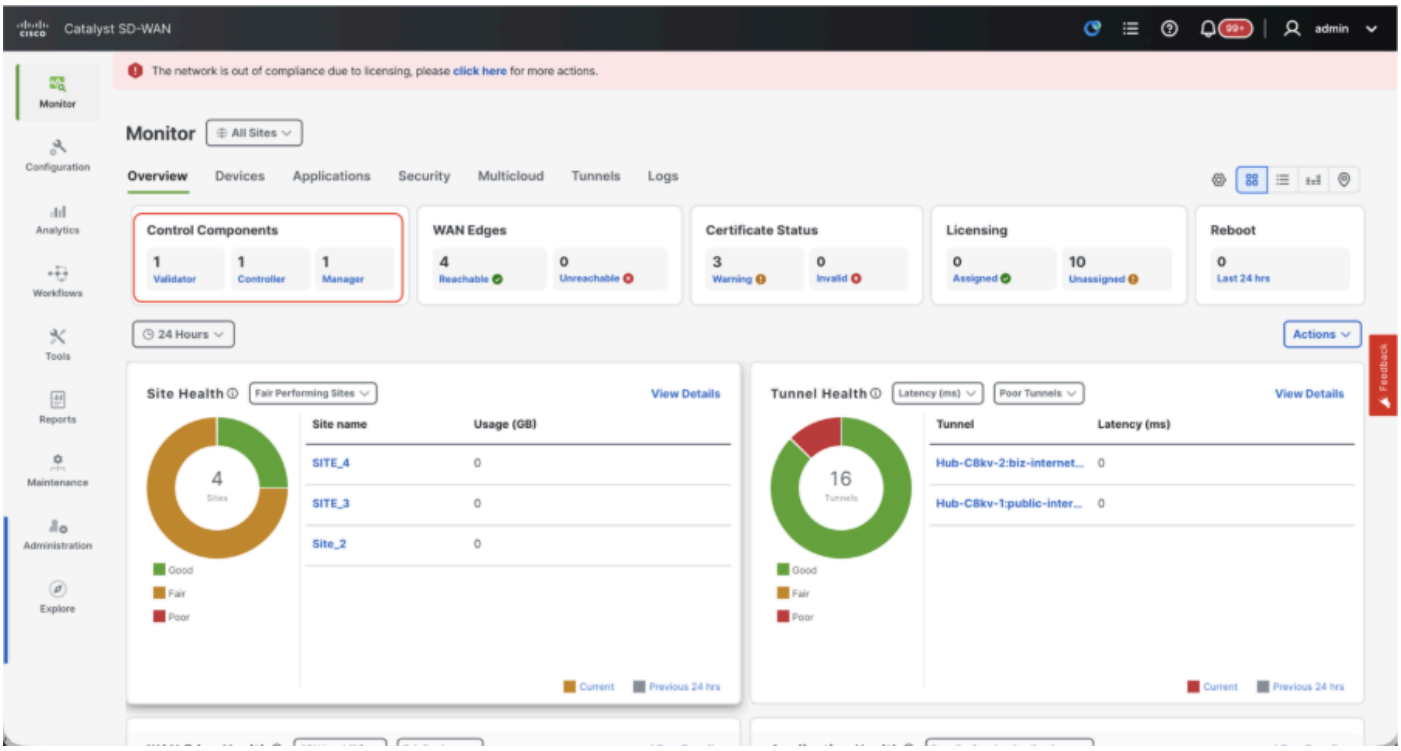
- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate

Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vSmartに自動的にインストールされます。

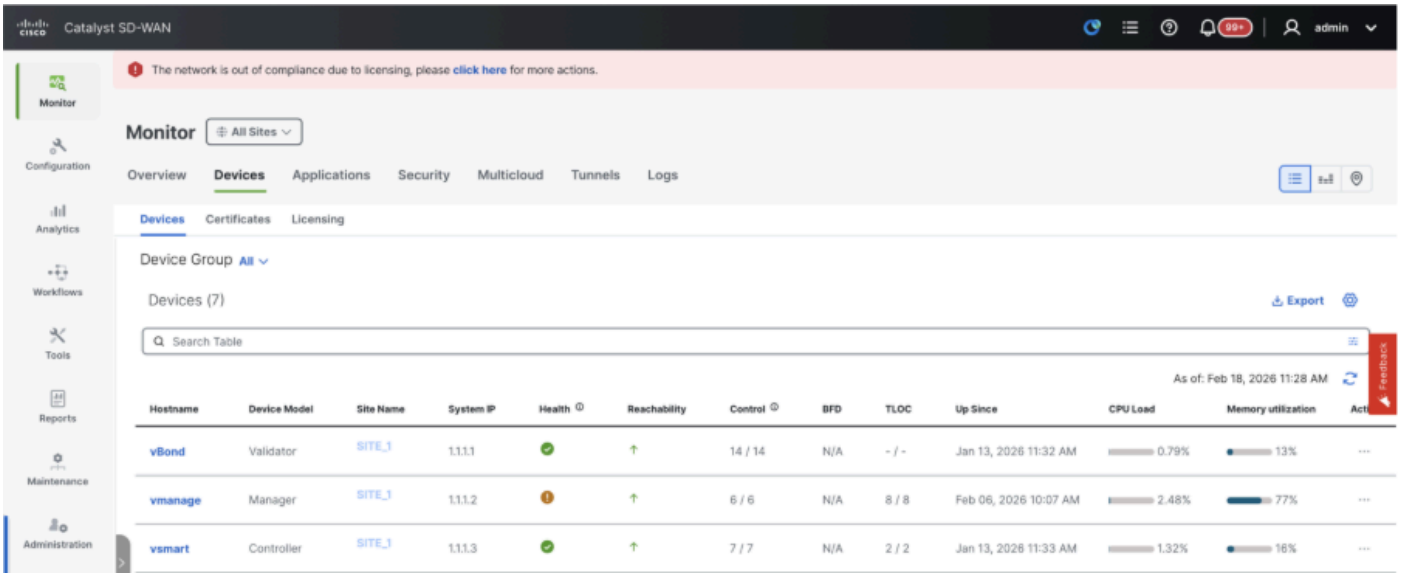
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。 Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- 複数のvSmartsがある場合は、同じ手順を繰り返します。

検証

すべての手順が完了したら、Monitor>Dashboardですべての制御コンポーネントに到達できることを確認します



- それぞれの制御コンポーネントをクリックして、それらがすべて到達可能であることを確認します。
- Monitor > Devicesの順に移動し、すべての制御コンポーネントが到達可能であることを確認します。



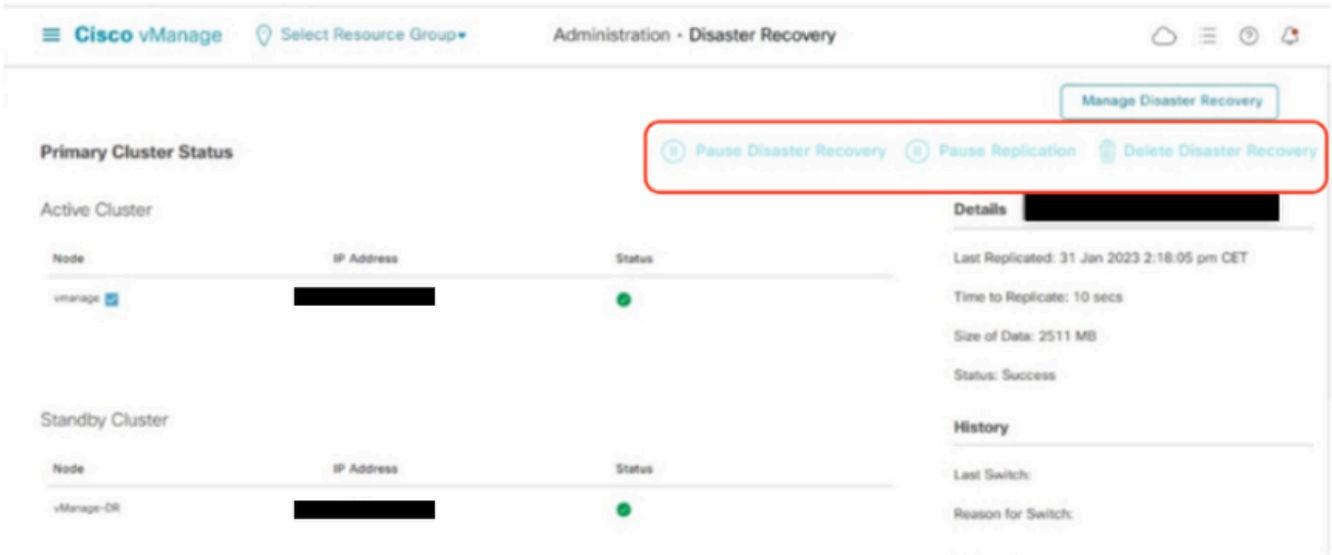
ステップ3:Config-dbのバックアップ/復元

別のvManageノードでのvManage構成データベースのバックアップと復元の収集

注：ディザスタリカバリが有効になっている既存のvManageノードから設定データベースのバックアップを収集する際には、そのノードのディザスタリカバリが一時停止して削除された後で、バックアップが収集されていることを確認してください。

継続的な災害復旧レプリケーションがないことを確認します。Administration > Disaster Recoveryの順に移動し、 ステータスが「成功」であり、「インポート保留中」、「エクスポート保留中」、「ダウンロード保留中」などの一時的な状態ではないことを確認します。ステータスがsuccessではない場合、ディザスタリカバリを一時停止する前に、Cisco TACに連絡してレプリケーションが成功することを確認します。

まず、ディザスタリカバリを一時停止し、タスクが完了していることを確認します。次に、ディザスタリカバリを削除し、タスクが完了したことを確認します。



ディザスタリカバリが正常にクリーンアップされたことをCisco TACに確認します。

Configuration-DBバックアップの収集：

- 現在使用されているSD-WANファブリックでは、スタンドアロンのvManageとvManageクラスタの両方のセットアップでconfiguration-dbバックアップを生成できます。
- スタンドアロンvManageの場合、そのvManage自体がconfiguration-dbのリーダーです。

configuration-dbがvManageノードで実行されていることを確認します。

同じことを確認するには、commandrequest nms configuration-db statusonvManageCLIを使用します。出力は次のようになります

```
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#
```

このコマンドを使用して、特定されたconfiguration-dbリーダーのvManageノードからconfiguration-dbのバックアップを収集します。

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

予想される出力は次のとおりです。

```
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#
```

- configuration-dbクレデンシャルが更新されている場合は、それをメモします。
- configuration-dbクレデンシャルを知らない場合は、TACに問い合わせて、既存のvManageノードからconfiguration-dbクレデンシャルを取得してください。
- デフォルトのconfiguration-dbクレデンシャルは、ユーザ名：neo4jおよびパスワード：passwordです。

構成データベースのバックアップを別のvManageノードに復元

SCPを使用して、vManageの/home/admin/ディレクトリにconfiguration-dbバックアップをコピーします。

scpコマンドの出力例：

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

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

configuration-dbのバックアップを復元するには、まずconfiguration-dbのクレデンシャルを設定する必要があります。configuration-dbクレデンシャルがデフォルト(neo4j/password)の場合は、このステップを省略できます。

configuration-dbクレデンシャルを設定するには、コマンドrequest nms configuration-db update-admin-userを使用し、任意のユーザ名とパスワードを使用します。

vManageのアプリケーションサーバが再起動します。このため、vManage UIに短時間アクセスできなくなります。

```
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#
```

設定データベースのバックアップの復元に進むことができる投稿：

request nms configuration-db restore path /home/admin/< >コマンドを使用して、新しいvManageに設定データベースを復元できます。

```
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
```

configuration-dbが復元されたら、vManage UIにアクセスできることを確認します。5分ほど待ってから、UIへのアクセスを試みます。

UIに正常にログインしたら、エッジルータのリスト、テンプレート、ポリシー、および以前または既存のvManage UIに存在していた残りのすべての設定が、新しいvManage UIに反映されていることを確認します。

ステップ4：シングルノードDRの設定

「ステップ2:組み合わせ2：スタンドアロンvManage +シングルノードDR」の「ステップ2：事前チェック」を参照し、ディザスタリカバリを有効にする前に、すべての要件を満たしていることを確認します。

シングルノードDR

前提条件

- トランスポートVPN(VPN 0)上で、プライマリノードとセカンダリノードがHTTPSで到達可能であることを確認します。

- Cisco vManageプライマリノードとセカンダリノードで同じCisco vManageバージョンが実行されていることを確認します。

VPN 0のアウトオブバンドクラスタインターフェイス

1. クラスタ内のvManageインスタンスごとに、VPN 0（トランスポート）およびVPN 512（管理）に使用されるインターフェイスの他に、3番目のインターフェイス（クラスタリンク）が必要です。
2. このインターフェイスは、クラスタ内のvManageサーバ間の通信および同期に使用されます。
3. このインターフェイスは、1 Gbps以上で、遅延が4 ms以下である必要があります。10 Gbpsインターフェイスを推奨
4. 両方のvManageノードは、このインターフェイスを介して相互に到達できる必要があります。このインターフェイスがレイヤ2セグメントであるか、またはレイヤ3ルーティングを介しているかに関係ありません。

- すべてのサービス（application-server、configuration-db、messaging server、coordination server、およびstatistics-db）が両方のCisco vManageノードで有効になっていることを確認します。
- Cisco vBond Orchestratorを含むすべてのコントローラをプライマリおよびセカンダリデータセンターに分散させます。これらのコントローラが、これらのデータセンターに分散しているCisco vManageノードから到達可能であることを確認します。コントローラは、プライマリCisco vManageノードにのみ接続します。
- アクティブ（プライマリ）およびスタンバイ（セカンダリ）のCisco vManageノードで他の操作が実行されていないことを確認します。たとえば、アップグレード中のサーバや、デバイスへのテンプレートのアタッチ中のテンプレートがないことを確認します。

- Cisco vManage HTTP/HTTPSプロキシサーバが有効になっている場合は無効にします。プロキシサーバを無効にしないと、Cisco vManageは、Cisco vManageアウトオブバンドクラスタIPアドレスが直接到達可能な場合でも、プロキシIPアドレスを使用してディザスタリカバリ通信を確立しようとします。ディザスタリカバリの登録が完了したら、Cisco vManage HTTP/HTTPSプロキシサーバを再度有効にすることができます。

- 障害回復登録プロセスを開始する前に、プライマリCisco vManageノードのTools → Rediscover Networkウィンドウに移動し、Cisco vBond Orchestratorsを再検出します。

コンフィギュレーション

ディザスタリカバリノードとして機能するすべてのvManageノードのCLI設定を行います

Vmanageの最低限の設定ディザスタリカバリ登録前は、次のようになります。

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

注:vBondアドレスとしてURLを使用している場合は、DNSサーバのIPアドレスをVPN 0設定で設定するか、解決できることを確認してください。

これらの設定は、ルータおよびその他のコントローラとの制御接続の確立に使用されるトランスポートインターフェイスを有効にするために必要です

```
config t
vpn 0
 dns
```

```
        primary
 dns



         secondary
 interface eth1
  ip address



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



commit
```

また、コントローラへのアウトオブバンド管理アクセスを有効にするためにVPN 512managementインターフェイスも設定します。

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
```

```
 ip route 0.0.0.0/0




!
commit
```

DR vManageでのサービスインターフェイスの設定

vManageノードでサービスインターフェイスを設定します。このインターフェイスはDR通信に使用され、

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

プライマリvManageとDR vManageで、同じIPサブネットがサービスインターフェイスに使用されていることを確認します

vManage UIでの設定の更新

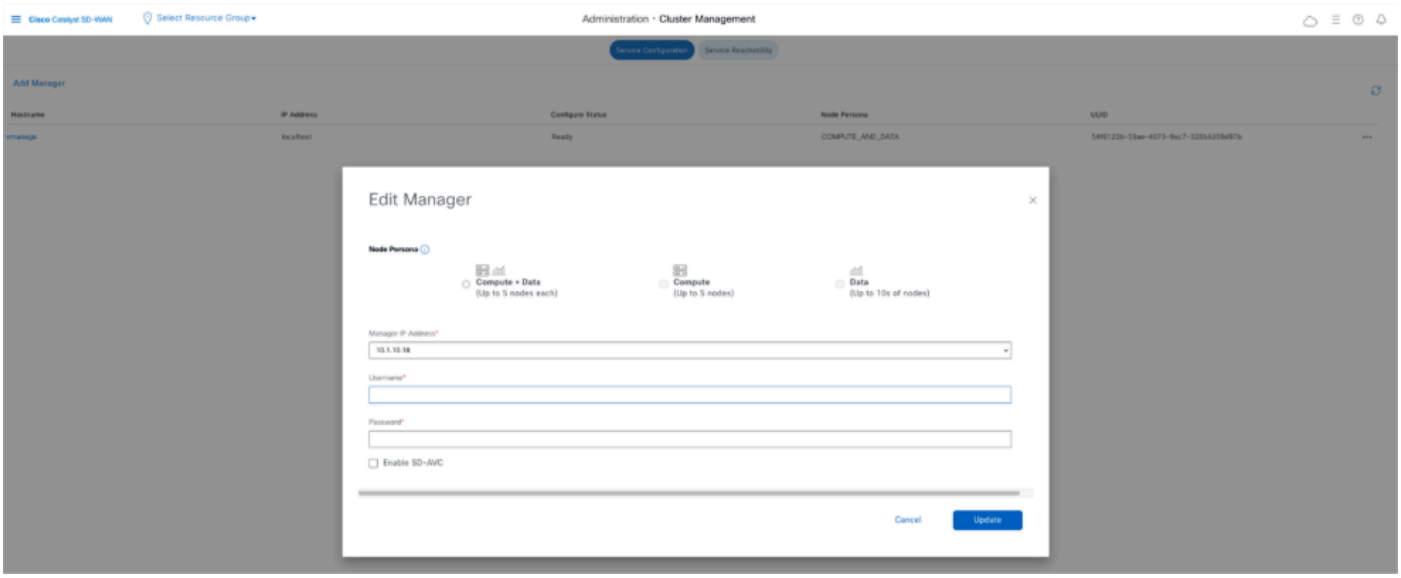
- すべてのコントローラのCLIに設定が追加されたら、ブラウザでURL https://<vmanage-ip>を使用して、vManageのWebUIにアクセスできます。各vManageノードのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- Administration > Settingsの順に移動し、次の手順を実行します。
- 組織名を設定します。 vManageノードのCLIと同じ値を設定します。
- vManage 20.15/20.18では、これらの設定はシステムのセクションで利用できます。

DR vManageへの証明書のインストール

組み合わせ2：スタンドアロンvManage +シングルノードDRの項で説明されている手順を実行します。手順3:vManage UI、証明書、およびオンボードコントローラを設定し、証明書をディザスタリカバリvManageにインストールします。

障害回復設定の追加

- そのためには、プライマリvManageに移動します。
- Administration→Cluster Managementの順に移動し、vManageエントリの右側にある3つのドット(...)をクリックして、ユーザ名とパスワードを入力してから、アウトオブバンドインターフェイスのIPアドレスを指定します。この設定では、プライマリとDRの両方のvmanageに対して個別のローカルユーザ（たとえばdradmin）を作成することを推奨します。



- この変更後、VManageがリブートします。
- プライマリvManageが起動したら、管理→ディザスタリカバリの順に移動します。Manage Disaster Recoveryをクリックします。
- ポップアップウィンドウで、プライマリとセカンダリの両方のvManageの詳細を入力します。
- 示されるIPアドレスは、アウトオブバンドクラスタインターフェイス(eth2)のIPアドレスです。
- クレデンシャルはnetadminユーザ(dradmin)のクレデンシャルである必要があり、DRが設定された後は変更できません。 ディザスタリカバリ用に別個のvManageローカルユーザクレデンシャルを使用できます。vManageローカルユーザがnetadminグループの一部であることを確認する必要があります。ここでは、管理者クレデンシャルも使用できます。

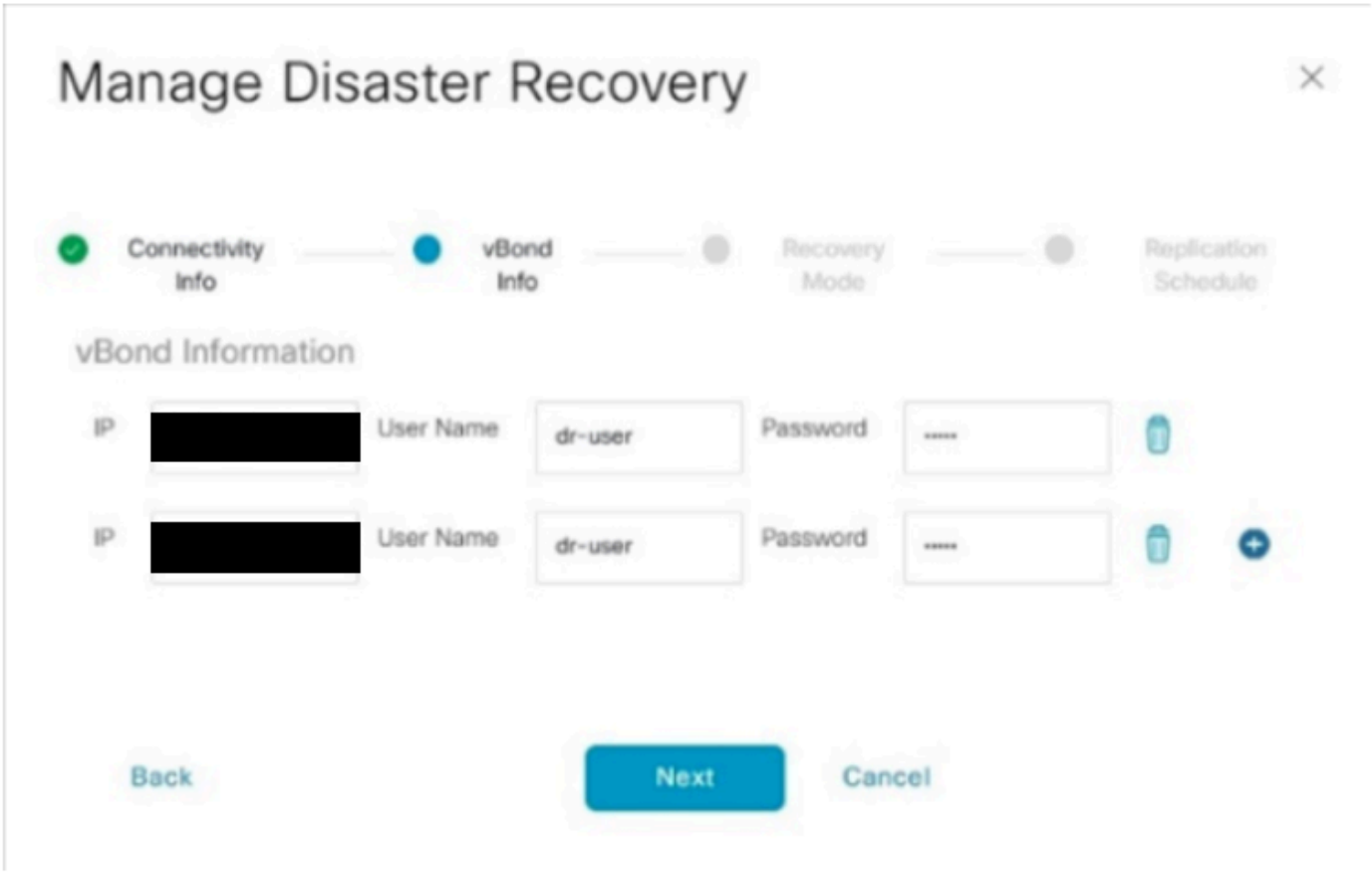
- 入力が完了したら、「Next」をクリックします。

- vBondコントローラの詳細を入力します。

- vBondコントローラは、指定されたIPアドレスでNetconfを介して到達可能である必要があります。

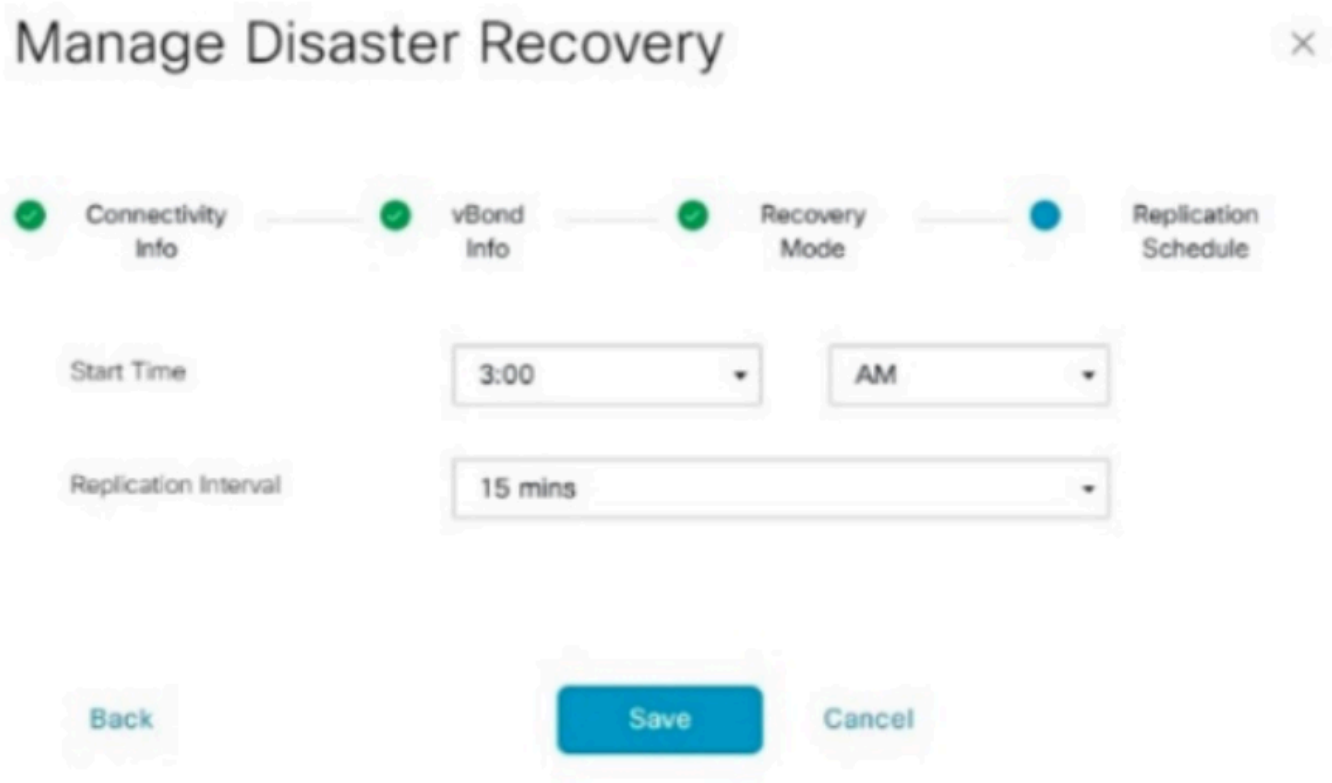
- クレデンシャルはnetadminユーザ(dradmin)のクレデンシャルである必要があり、DRが設定された後は変更できません。

- このためには、vBondでこのdradminユーザをローカルに設定しておくことを推奨します。または、adminユーザを使用してvBondを追加することもできます。

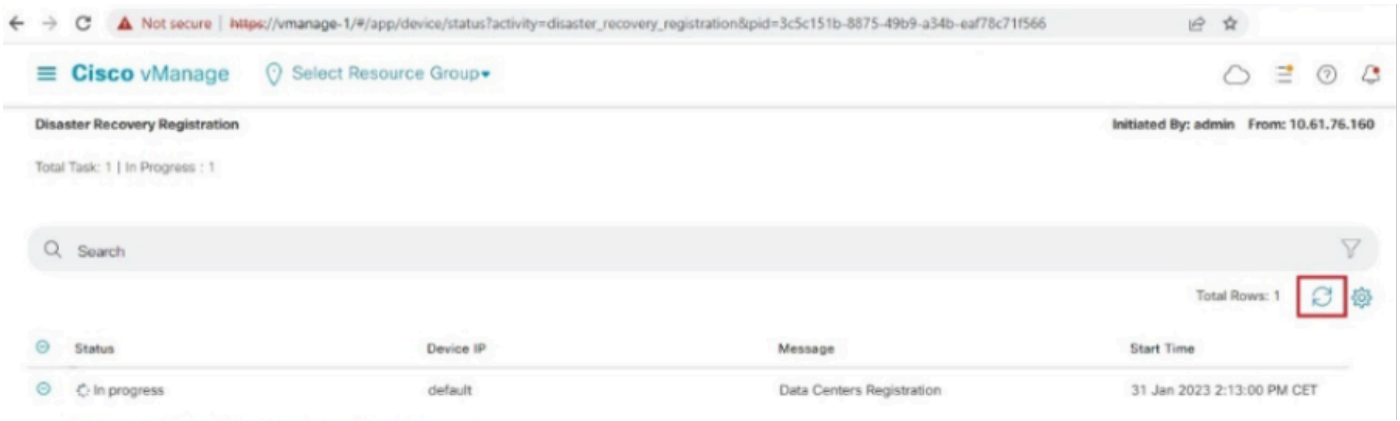


- 入力が完了したら、「Next」をクリックします。
- リカバリモードで、「手動」を選択します。 Nextをクリックします。

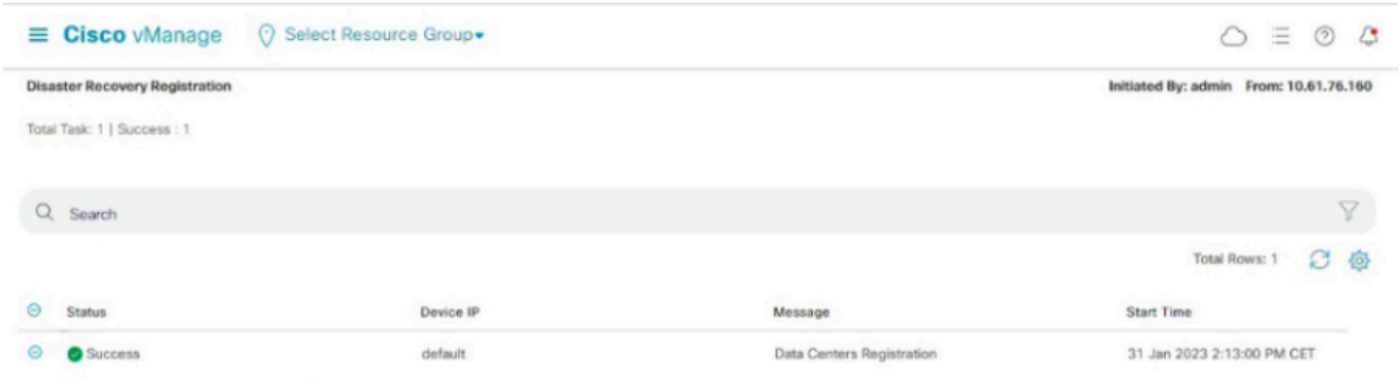
複製スケジュールで、「Replication Interval'.レプリケーション間隔ごとに、データはプライマリからレプリケートされます vManageからセカンダリvManage。設定可能な最小値は15分です。



- 値を設定し、「Save」をクリックします。
- DR登録が開始されます。[更新]ボタンをクリックして、状態と進行状況ログを手動で更新します。このプロセスには、最大で20 ~ 30分かかる場合があります。

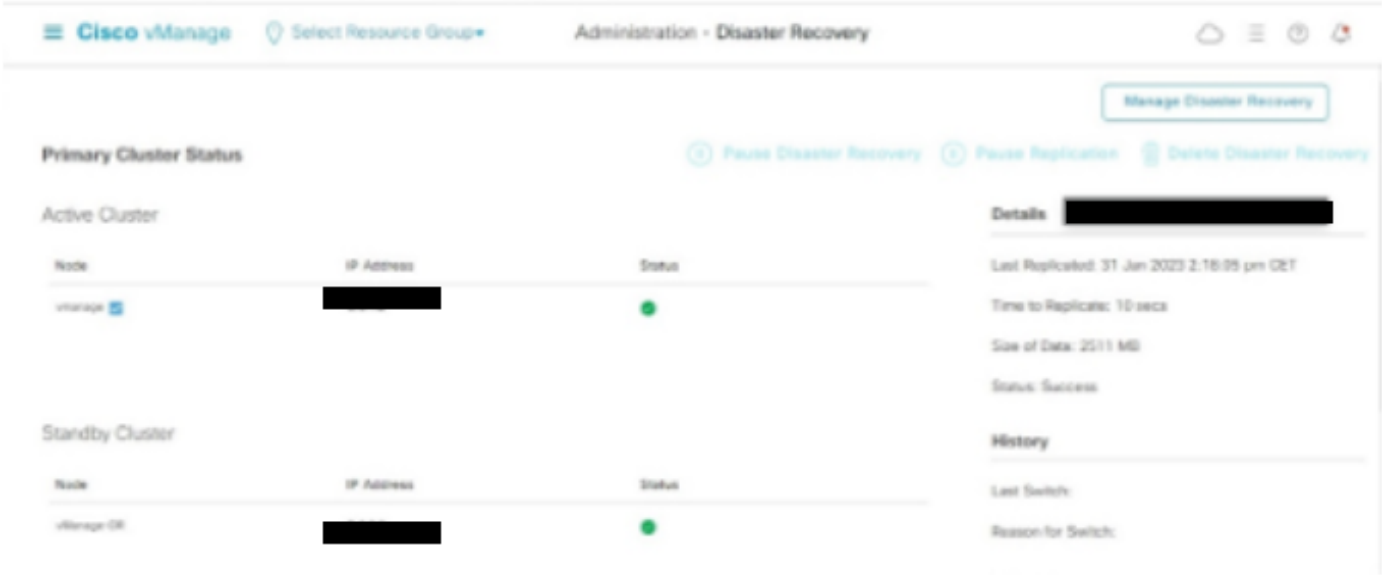


- このプロセス中にvManage GUIが再起動されることに注意してください。
- 完了すると、Successのステータスが表示されます。



確認

Administration → Disaster Recoveryの順に移動します。ディザスタリカバリのステータスと、データが最後に複製された日時を確認できます。



ステップ5：コントローラの再認証と古いコントローラの無効化

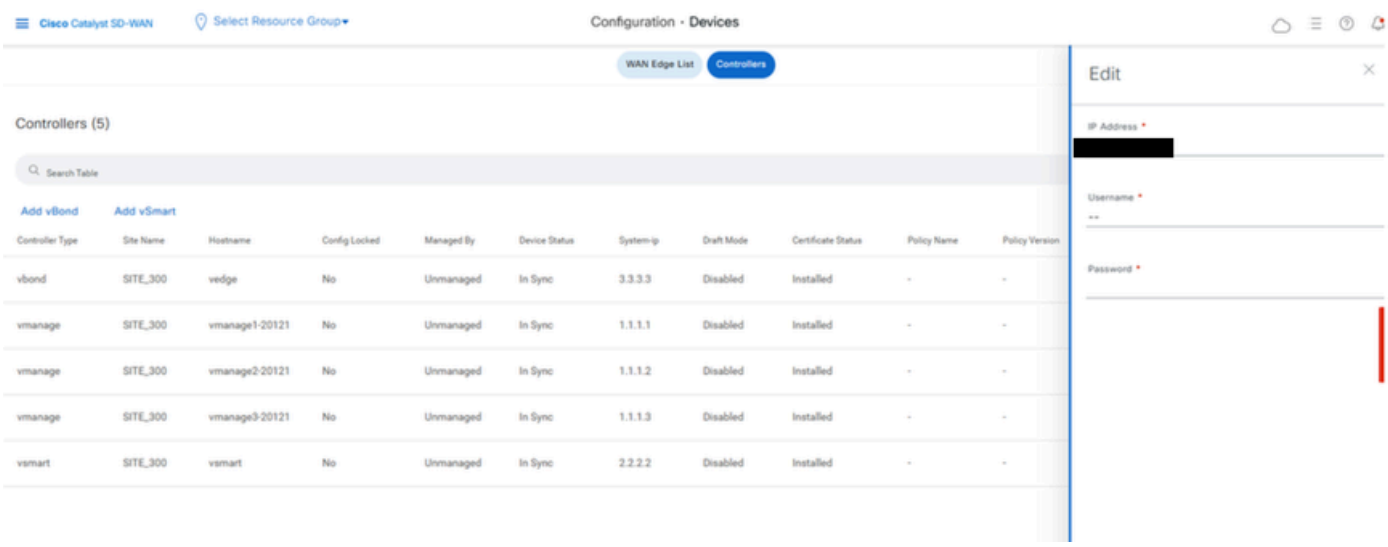
configuration-dbが復元されたら、ファブリック内のすべての新しいコントローラ(vmanage/vsmart/vbond)を再認証する必要があります

注：実際の運用で、再認証に使用されるインターフェイスIPがトンネルインターフェイスIPである場合、vManage、vSmart、およびvBondのトンネルインターフェイスでNETCONFサービスが許可され、パスに沿ったファイアウォールでもNETCONFサービスが許可されるようにする必要があります。開くファイアウォールポートは、DRクラスタからすべてのvBondおよびvSmartsへの双方向ルールとしてTCPポート830です（この例では、DRクラスタはIPアドレスがIPアドレスに一致します）。

---

vmanage UIで、Configuration > Devices > Controllersの順にクリックします。

- 各コントローラの近くにある3つのドットをクリックし、[編集]をクリックします



- ip-address（コントローラのsystem-ip）をtransport vpn 0（トンネルインターフェイス）ip addressに置き換えます。ユーザ名とパスワードを入力して、saveをクリックします
- ファブリック内のすべての新しいコントローラに対して同じ操作を行います

Root-cert-chainの同期

すべてのコントローラがオンボーディングされたら、次の手順を実行します。

新しくアクティブになったクラスタ内の任意のCisco SD-WAN Managerサーバで、次の操作を実行します。

ルート証明書を、新しくアクティブになったクラスタ内のすべてのCisco Catalyst SD-WANデバイスと同期させるには、次のコマンドを入力します。

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

次のコマンドを入力して、Cisco SD-WAN Manager UUIDをCisco SD-WAN Validatorと同期させます。

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

ファブリックが復元され、ファブリック内のすべてのエッジとコントローラに対してコントロールセッションとbfdセッションが確立されたら、古いコントローラ(vmanage/vsmart/vbond)をUIから無効にする必要があります

- vmanage UIで、Configuration > Devices > Certificatesの順にクリックします。
- Controllersをクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。[無効]をクリックします
- vbondに送信をクリックします。
- vmanage UIで、Configuration > Devices > Controllersの順にクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリ

ックします。Deleteをクリックします

ステップ6：事後チェック

注：すべての導入の組み合わせに共通する、ここに示す導入後のチェックセクションを続行します。

組み合わせ3:vManageクラスタ+ DRなし

必要なインスタンス

- 3つのvManage（3ノードクラスタ、すべてのCOMPUTE_AND_DATA）または6つのvManage（3つのCOMPUTE_AND_DATA + 3つのデータ）
- 1つ以上のvBond
- 1つ以上のvSmart

手順：

1. 共通ステップを使用してすべてのインスタンスを起動する
2. 事前チェック
3. vManage UI、証明書、およびオンボードコントローラの設定
4. vManageクラスタの構築
5. Config-dbバックアップ/復元
6. 事後チェック

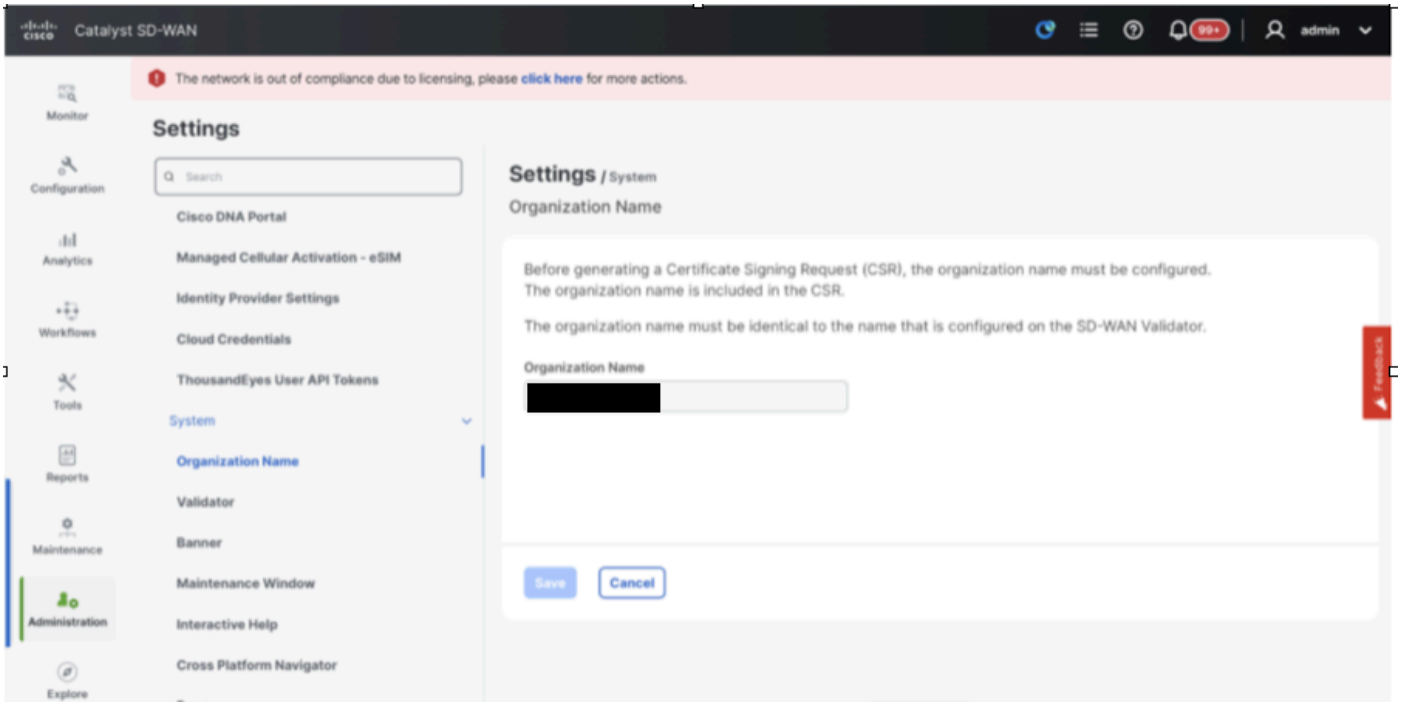
ステップ1：事前チェック

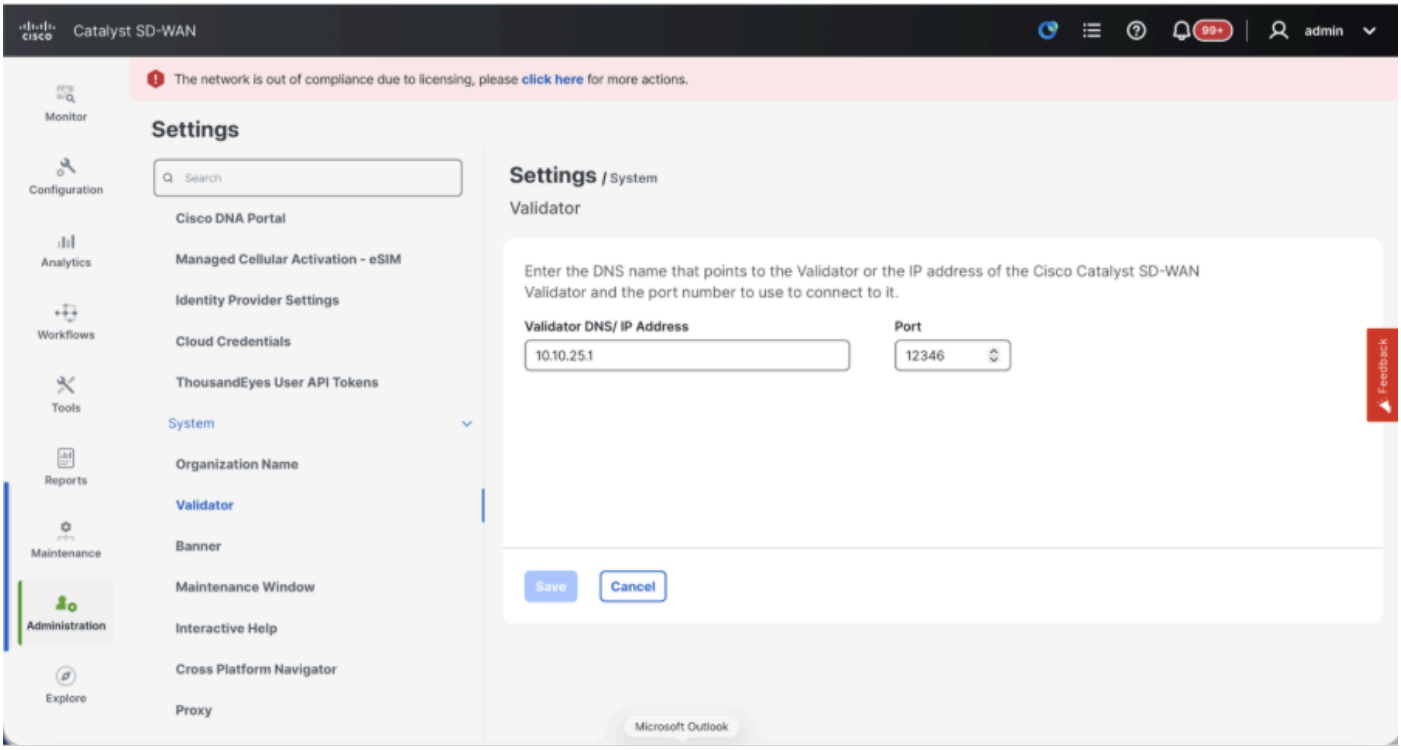
- アクティブなCisco SD-WAN Managerインスタンスの数が、新しくインストールしたCisco SD-WAN Managerインスタンスの数と同じであることを確認します。
- アクティブなCisco SD-WAN Managerインスタンスと新しいCisco SD-WAN Managerインスタンスのソフトウェアバージョンがすべて同じであることを確認します。
- アクティブおよび新規のすべてのCisco SD-WAN Managerインスタンスが、Cisco SD-WAN Validatorの管理IPアドレスに到達できることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスに証明書がインストールされていることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスを含め、すべてのCisco Catalyst SD-WANデバイスのクロックが同期されていることを確認します。
- 新しくインストールされたCisco SD-WAN Managerインスタンスで、システムIPとサイトIDの新しいセットが、アクティブクラスタと同じ基本設定とともに設定されていることを確認します。

手順2:vManage UI、証明書、オンボードコントローラを設定します。

vManage UIでの設定の更新

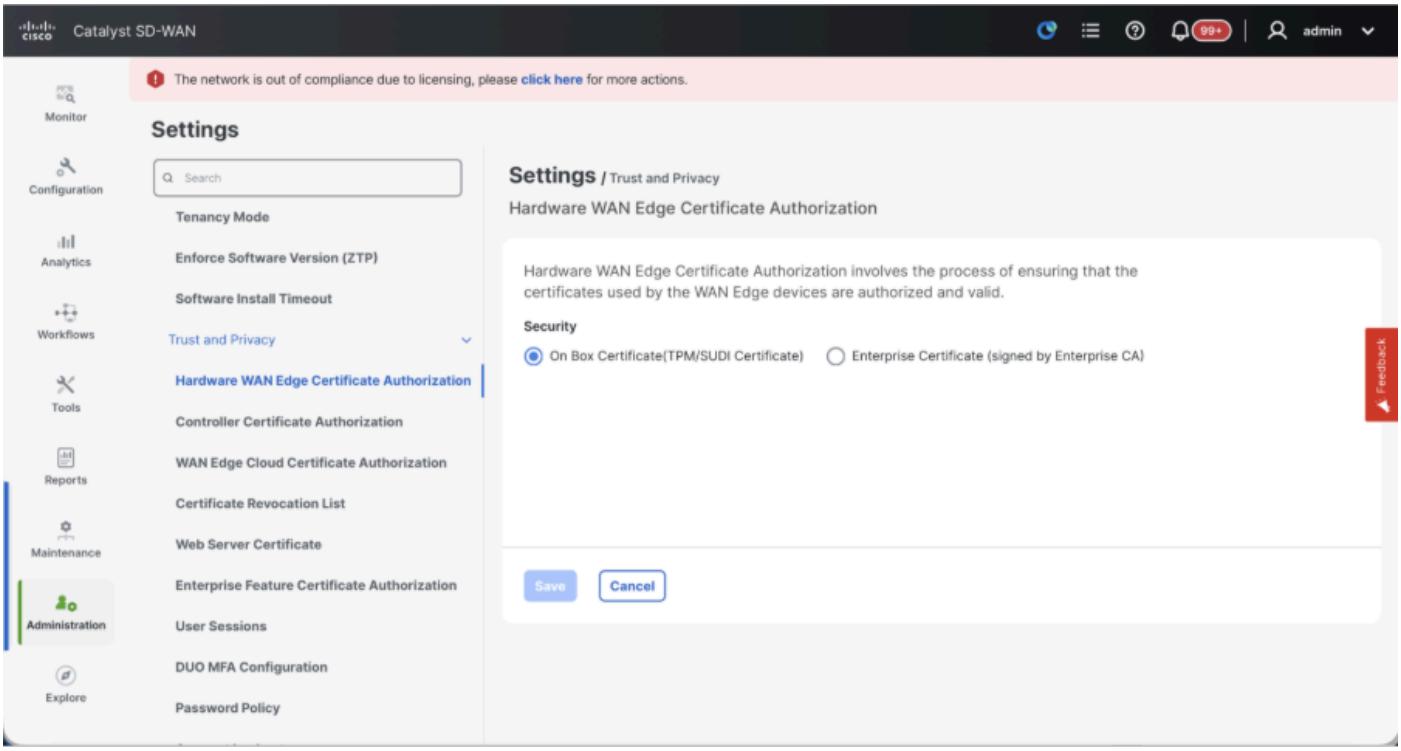
- ステップ1の設定がすべてのコントローラのCLIに追加されたら、ブラウザでURL https://<vmanage-ip>を使用して、vManageのWebUIにアクセスできます。各vManageノードのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- Administration > Settingsの順に移動し、次の手順を実行します。
- 組織名とValidator/vBond URL/IPアドレスを設定します。vManageノードのCLIと同じ値を設定します。
- vManage 20.15/20.18では、これらの設定はシステムのセクションで利用できます。



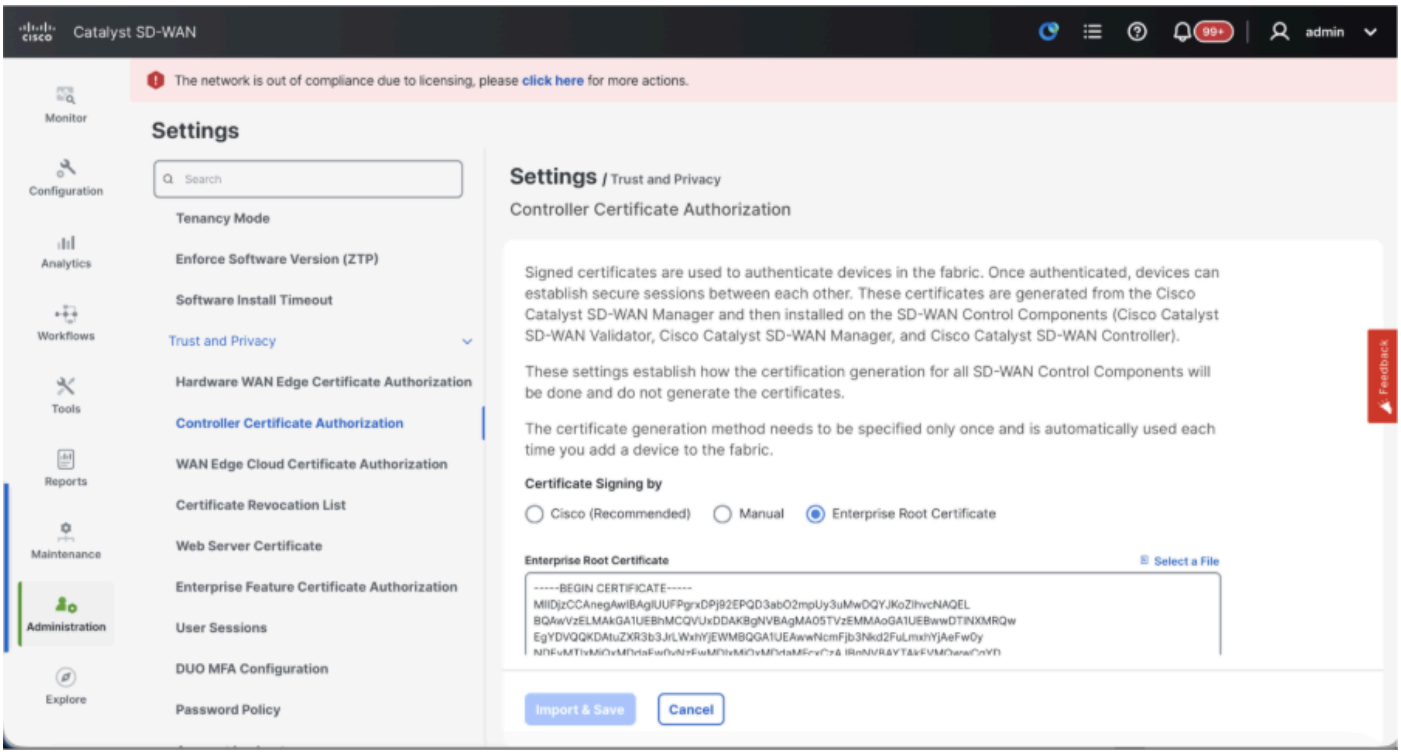


- 証明書の署名に使用する認証局(CA)を決定する証明書承認(CA)の設定を確認します。3つのオプションがあります。

1. ハードウェアWANエッジ証明書認証：ハードウェアSD-WANエッジルータのCAを決定します。
    - オンボックス証明書（TPM/SUDI証明書）– このオプションを使用すると、制御接続（TLS/DTLS接続）を確立するために、ルータハードウェアにプレインストールされている証明書が使用されます
    - エンタープライズ証明書（エンタープライズCAによって署名された）– このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

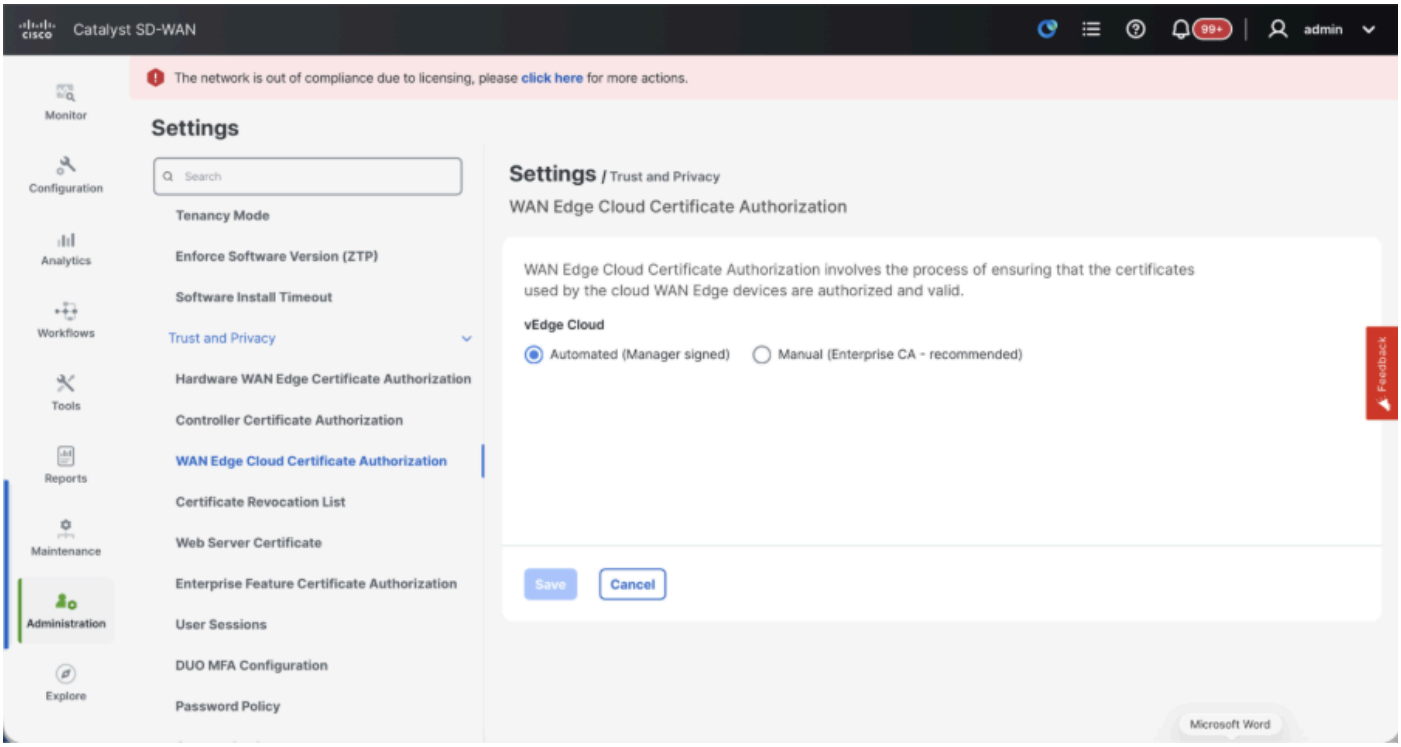


2. Controller Certificate Authorization（コントローラ証明書認証）:SD-WANコントローラのCAを決定します。
    - シスコ（推奨）– コントローラはCisco PKIによって署名された証明書を使用します。vManageは、vManageで設定されたスマートアカウント資格情報を使用してPNPポータルに自動的に接続し、証明書に署名してコントローラにインストールされます。
    - 手動：コントローラはCisco PKIによって署名された証明書を使用します。それぞれのSD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用して手動でCSRに署名します。
    - エンタープライズルート証明書：このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

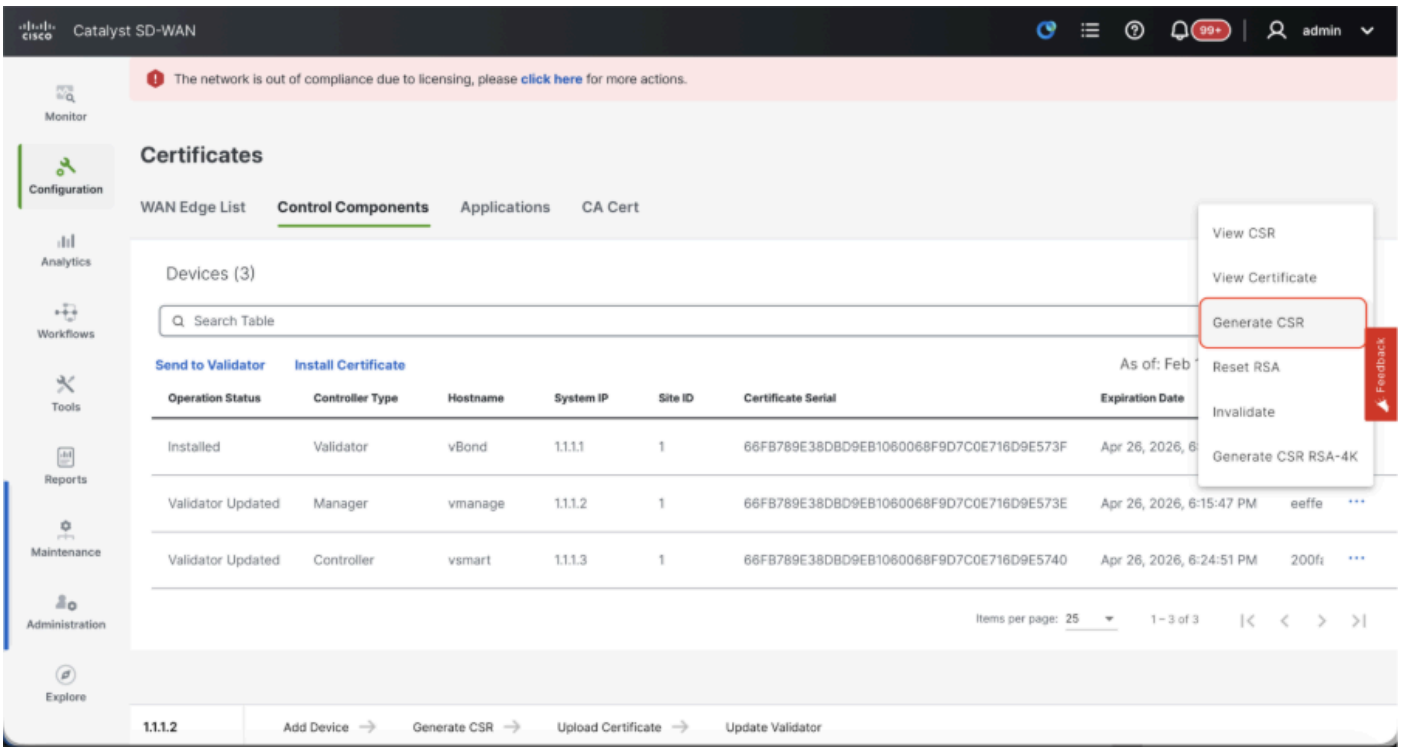


3. WANエッジクラウド証明書認証：仮想SD-WANエッジルータ（CSR1000v、C8000v、vEdgeクラウド）のCAを決定します。
    - 自動（vManage署名済み）:vManageは、仮想エッジルータのCSRに自動的に署名し、証明書をルータにインストールします。
    - 手動（エンタープライズCA – 推奨）– 仮想ルータは、組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

独自のCA（エンタープライズ認証局）を使用している場合は、Enterpriseを選択します。



- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers
- Manager/vManageの「。..」をクリックし、「CSRの生成」をクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。

vBond/ValidatorおよびvSmart/ControllerのvManageへのオンボーディング

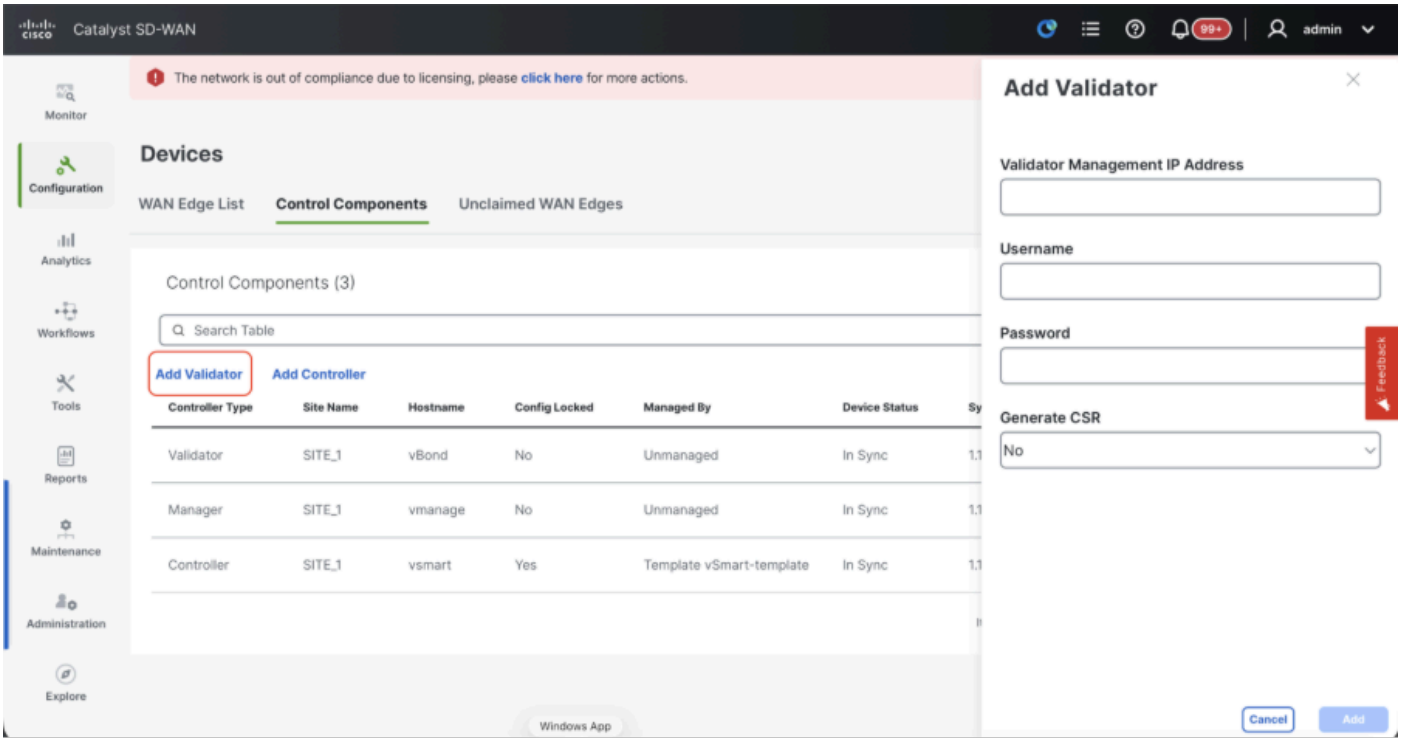
20.15/20.18 vManageノードの場合は、Configuration > Devices > Control Componentsの順に移動します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

オンボーディングvBond/バリデータ

- onAddvBondをクリックします20.12vManagerの場合バリデータの追加20.15/20.18vManageの場合。ポップアップが表示されたら、 VPN 0は、vManageから到達可能なvBondのIPを転送します。
- vManagetovBondIPのCLIからpingを使用して（許可されている場合）到達可能性を確認します。
- vBondのユーザクレデンシャルを入力します。

注:NetAdminグループのユーザ部分であるvBondorの管理者クレデンシャルを使用する必要があります。これはthevBondのCLIで確認できます。vBondの新しい証明書をインストールする必要がある場合は、「CSRの生成」のドロップダウンでYesを選択します

注:vBondがNATデバイス/ファイアウォールの背後にある場合は、vBond VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認してください。VPN 0インターフェイスIPにvManageから到達できない場合は、このステップでVPN 0インターフェイスのパブリックIPアドレスを使用します

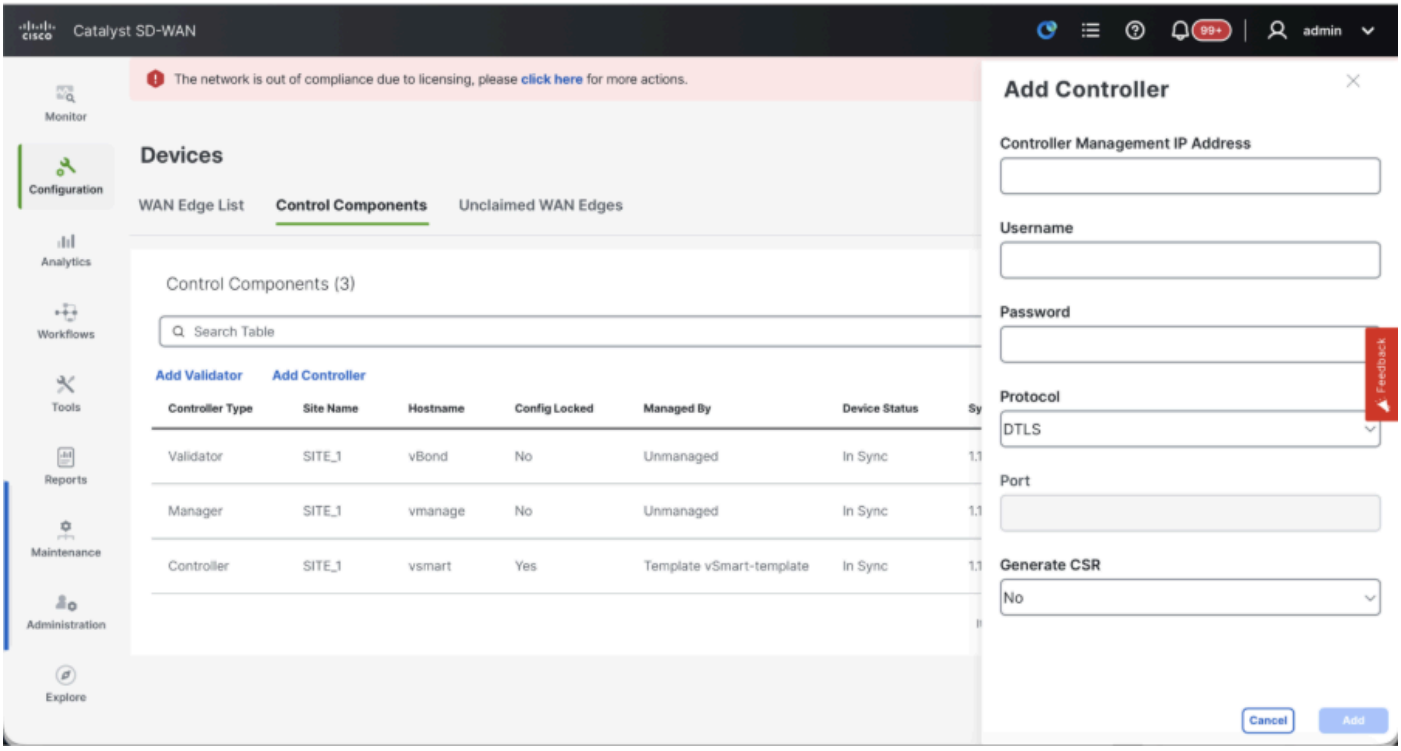


- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vBondに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvBondがある場合は、同じ手順を繰り返します。

vSmart/コントローラのオンボーディング

- 20.12 vManageの場合はAdd vSmartを、20.15/20.18 vManageの場合はAdd Controllerをクリックします。
- ポップアップが開いたら、vManageから到達可能なvSmartのVPN 0トランスポートIPを入力します。
- vManageのCLIからvSmart IPにpingを使用して（許可されている場合）到達可能性を確認します。
- vSmartの管理者クレデンシャルまたはnetadminグループのユーザ部分を使用する必要があるvSmart Noteのユーザクレデンシャルを入力します。
- これは、vSmartのCLIで確認できます。
- ルータにTLSを使用してvSmartとの制御接続を確立する場合は、プロトコルをTLSに設定します。 この構成は、vSmartsおよびvManageノードのCLIでも構成する必要があります。
- vSmartの新しい証明書をインストールする必要がある場合は、「Generate CSR」のドロップダウンで「Yes」を選択します。

注：vSmartがNATデバイス/ファイアウォールの背後にある場合は、vSmart VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認し、VPN 0インターフェイスIPがvManageから到達できない場合は、この手順でVPN 0インターフェイスIPのパブリックIPアドレスを使用します。



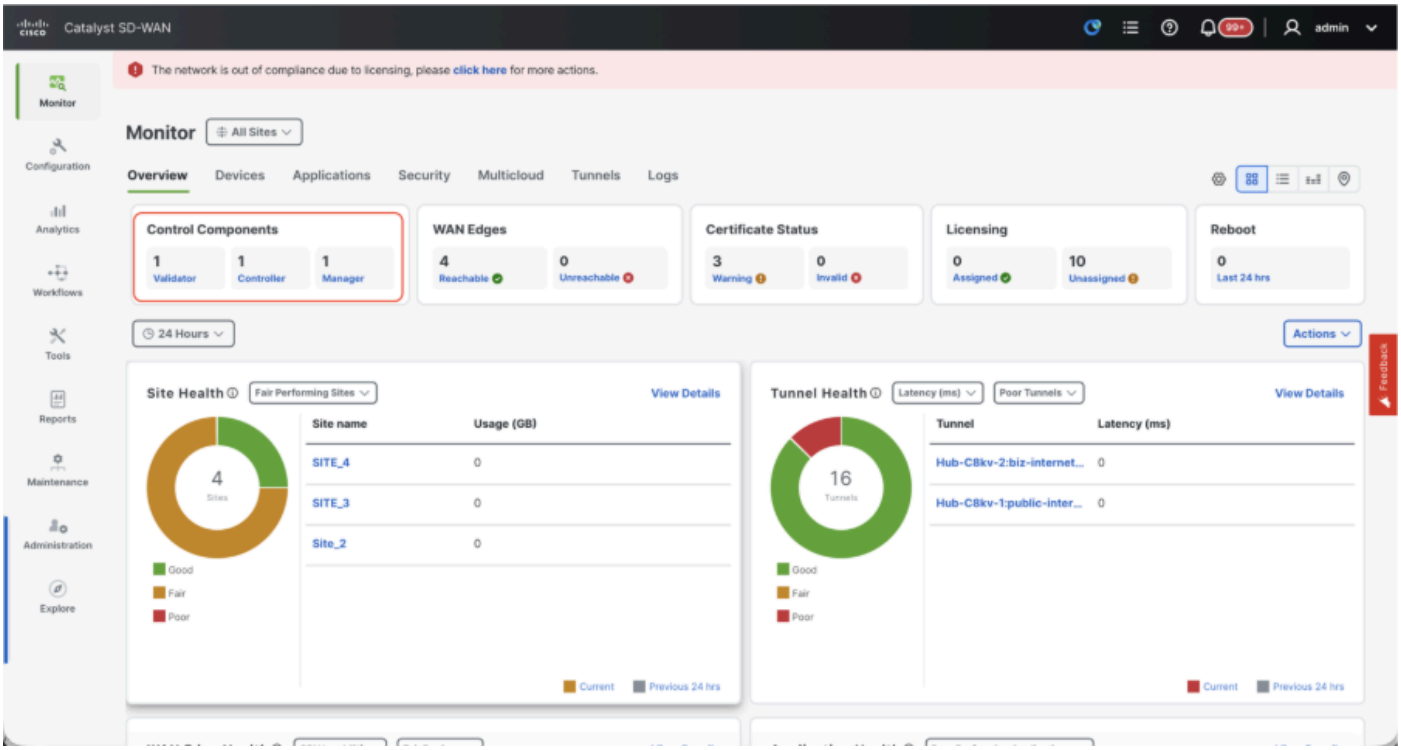
- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate

Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vSmartに自動的にインストールされます。

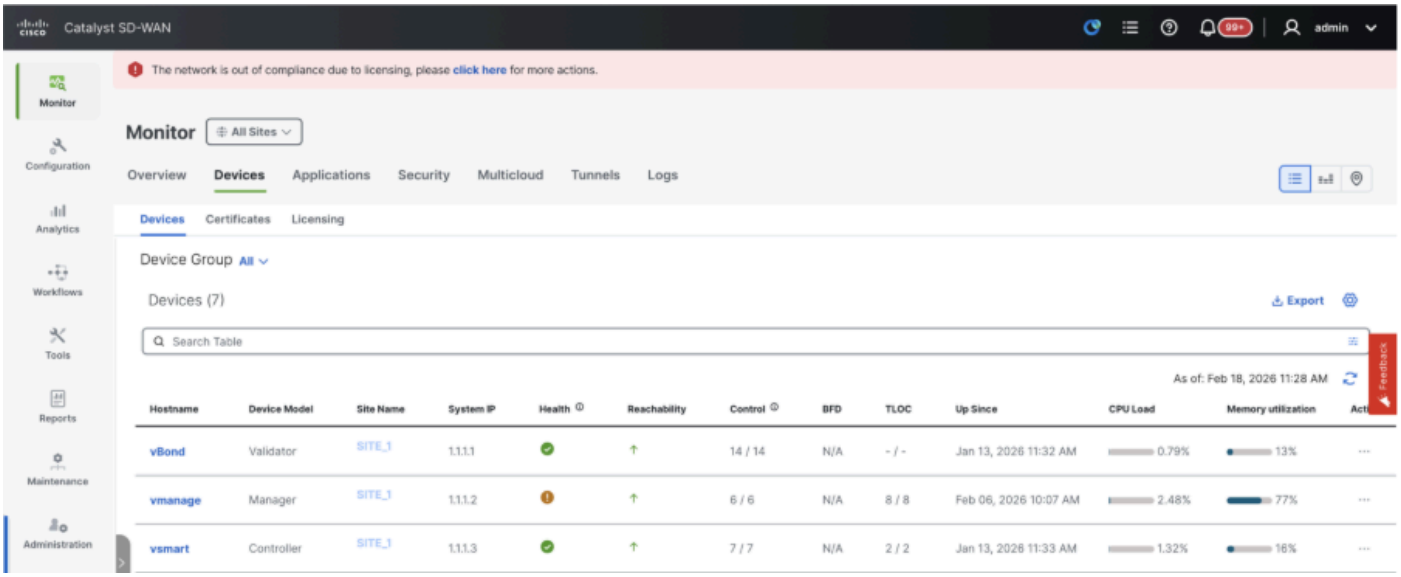
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvSmartsがある場合は、同じ手順を繰り返します。

検証

すべての手順が完了したら、Monitor>Dashboardですべての制御コンポーネントに到達できることを確認します



- それぞれの制御コンポーネントをクリックして、それらがすべて到達可能であることを確認します。
- Monitor > Devicesの順に移動し、すべての制御コンポーネントが到達可能であることを確認します。



ステップ3:vManageクラスタの構築

SD-WANオーバーレイでvManageクラスタを使用したオンボードSD-WANファブリック

注:vManageクラスタは、SD-WANファブリックにオンボーディングされたサイトの数に応じて、3つのvManageノードまたは6つのvManageノードで構成できます。既存のvManageクラスタを参照し、同じクラスタごとにノード数を選択します。

クラスタに含まれるすべてのvManageノードのCLI設定を構成します

すべてのvManageノードでシステム構成を構成する

- 残りのvManageノードを設定します。 3ノードクラスタの場合は、残りの2ノードを構成します。6ノードクラスタの場合は、5ノードを構成します。
- 次に示すように、システム設定を行います。

```
config t
system
 host-name



 system-ip



 site-id
```

```
 organization-name


 vbond


commit
```

注:vBondアドレスとしてURLを使用している場合は、DNSサーバのIPアドレスをVPN 0設定で設定するか、解決できることを確認してください。

すべてのvManageノードでトランスポートインターフェイスを設定する

これらの設定は、ルータおよびその他のコントローラとの制御接続の確立に使用されるトランスポートインターフェイスを有効にするために必要です。

```
config t
vpn 0
 dns


        primary
 dns


         secondary
 interface eth1
  ip address


  tunnel-interface
   allow-service all
```

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



commit
```

すべてのvManageノードで管理インターフェイスを設定します。

また、コントローラへのアウトオブバンド管理アクセスを有効にするためにVPN 512managementインターフェイスも設定します。

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

オプションの構成：

- 既存のコントローラの設定を参照できます。ここにリストされている設定が存在する場合は、新しいコントローラにこの設定を追加できます。
- ルータがTLSを使用してvManageノードとのセキュアな制御接続を確立する必要がある場合にのみ、制御プロトコルをTLSとして設定します。デフォルトでは、すべてのコントローラとルータがDTLSを使用して制御接続を確立します。これは、要件に応じてvSmartおよびvManageノードでのみ必要なオプションの設定です。

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

すべてのvManageノードでサービスインターフェイスを設定する

すでにオンボーディングされているvManage-1を含むすべてのvManagenodesでサービスインターフェイスを設定します。このインターフェイスは、クラスタ通信に使用されます。つまり、クラスタ内のvManagerノード間の通信です。

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

同じIPサブネットがvManageclusterのすべてのノードでサービスインターフェイスに使用されていることを確認します。

クラスタクレデンシャルの設定

vManagenodesと同じ管理者クレデンシャルを使用して、vManageclusterを設定できます。または、netadmingroupの一部である新しいユーザクレデンシャルを設定できます。新しいユーザクレデンシャルを設定する設定は次のとおりです

```
conf t
system
```

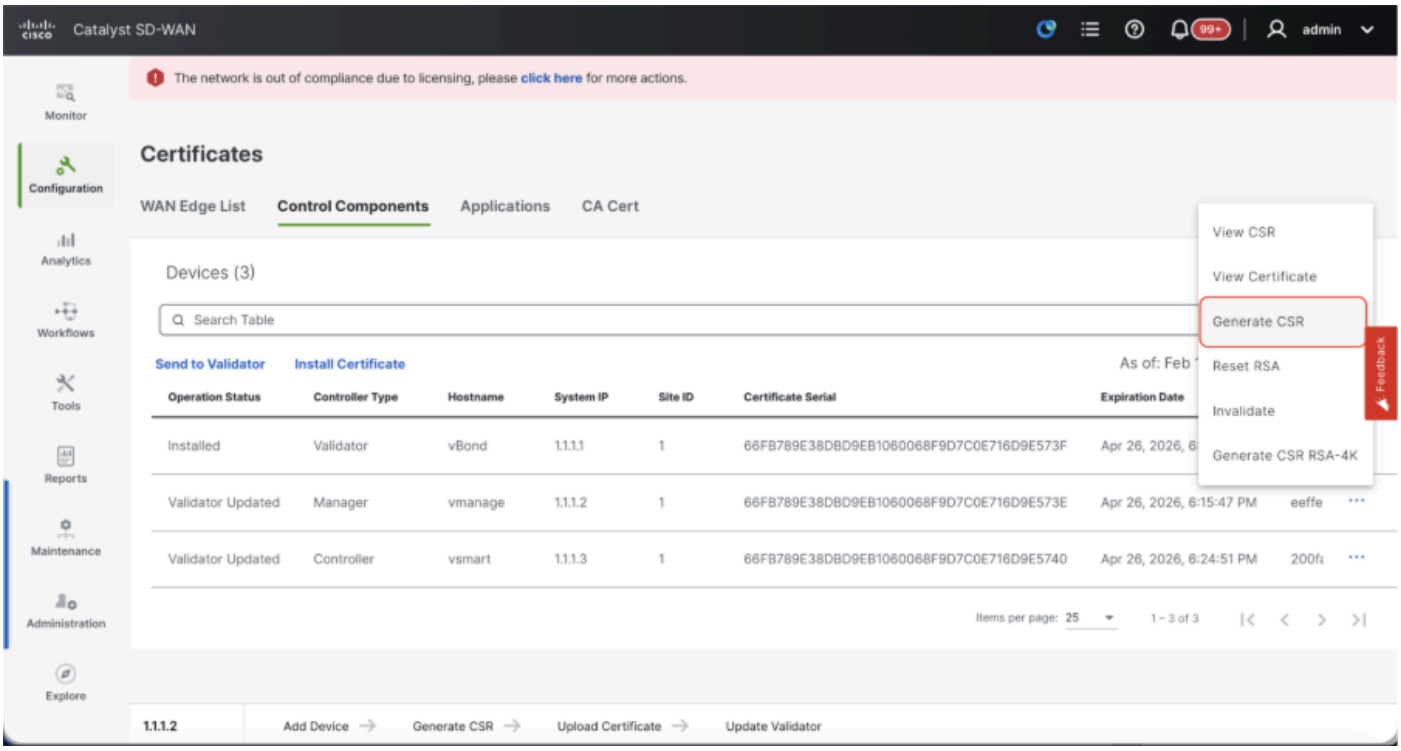
```
 aaa
  user



   password



   group    netadmin
commit
```

クラスタの一部であるすべてのvManagenodesで同じユーザクレデンシャルを設定してください。管理者クレデンシャルを使用する場合は、すべてのvManagenodesで同じユーザ名/パスワードを使用する必要があります。

すべてのvManageノードにデバイス証明書をインストール

- ブラウザでURL https://<vmanage-ip>を使用して、すべてのvManagenodesのvManageUIにログインします。それぞれのvManagenodesのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

  Manager/vManageで…をクリックし、Generate CSRをクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。

- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。 Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。

- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。

- クラスタに含まれるすべてのvManageノードに対してこの手順を実行します。

vManageクラスタの構築の準備

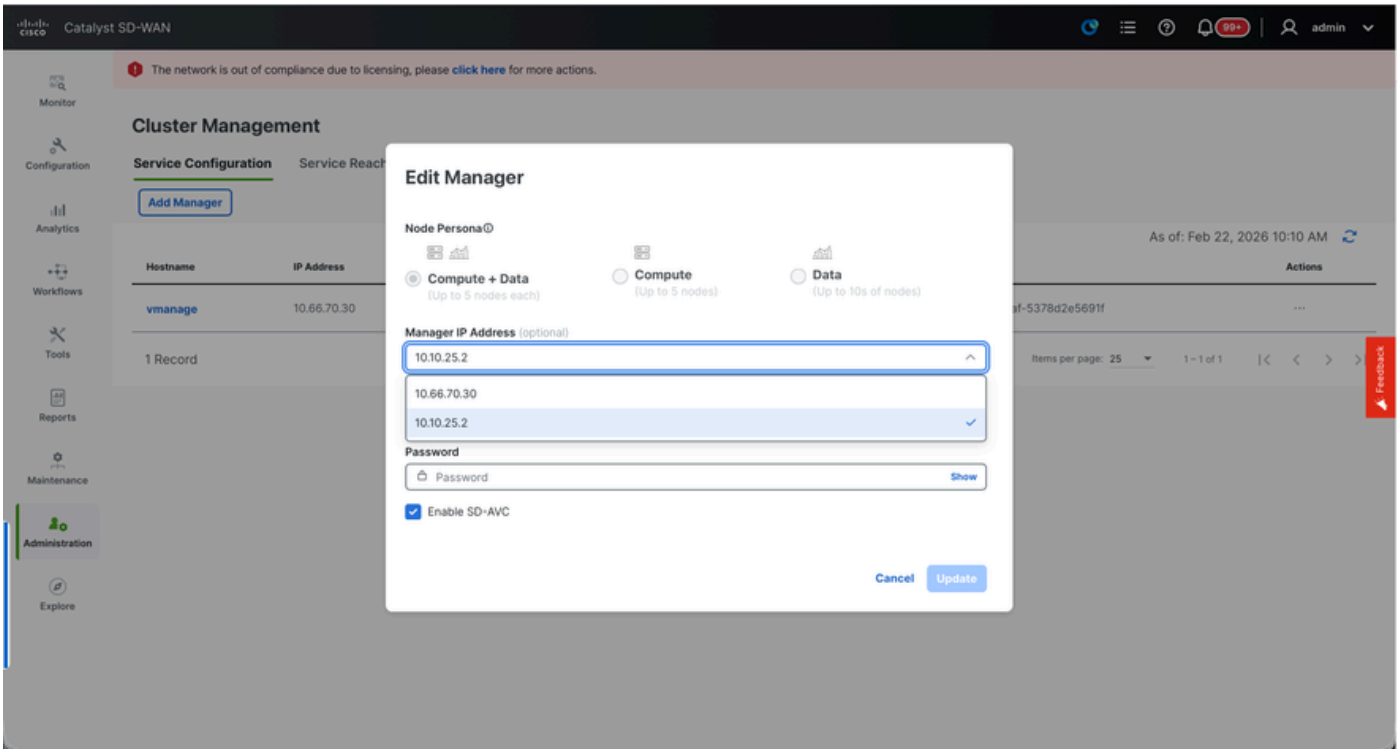
  - vManage-1のWebUIで、[管理] > [クラスタ管理] に移動し、[vManage-1のアクション]の下の[...]をクリックし、[編集]を選択します。
  - ノードのペルソナは、VMのスピンアップ時に選択したペルソナに基づいて自動的に選択されます。

注:3ノードクラスタの場合、3つのvManageノードはすべて、ペルソナとしてcompute+dataを使用して起動されます。

- 6ノードクラスタの場合、3つのvManageノードはpersonaとしてcompute+dataを使用して

起動され、3つのvManageノードはpersonaとしてdataを使用して起動されます。

- Manager IP addressのドロップダウンから、vManageのservice interface IPを選択します。

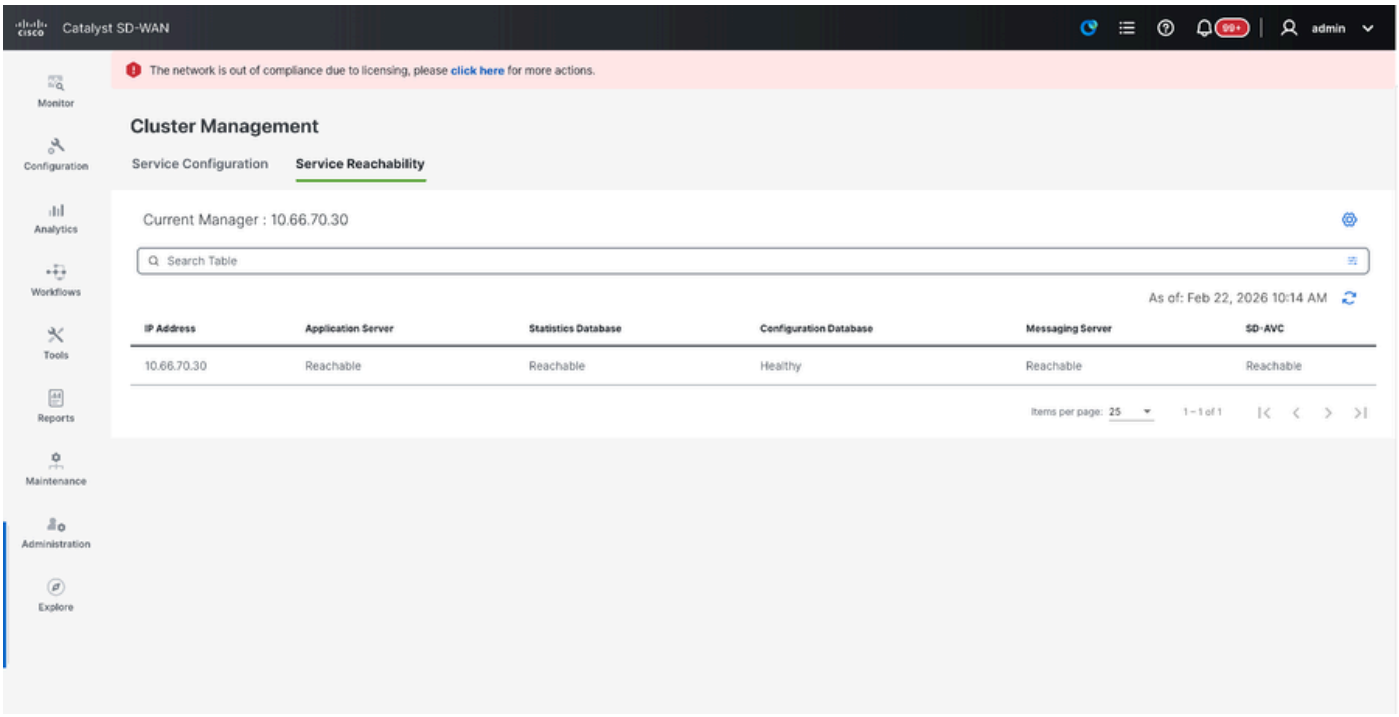


- vManageクラスタ（クラスタクレデンシャルと呼ばれます）を有効にするために使用するユーザ名とパスワードを入力します。
- 前述のように、すべてのvManageノードで同じクレデンシャルを設定し、すべてのノードをクラスタに追加する際に同じクレデンシャルを使用する必要があります。

注:SDAVCを有効にするには、既存のクラスタでこの設定を参照してください。必要な場合にのみチェックし、クラスタの1つのvManageノードでのみ必要な場合はチェックする必要があります。

Updateをクリックします。

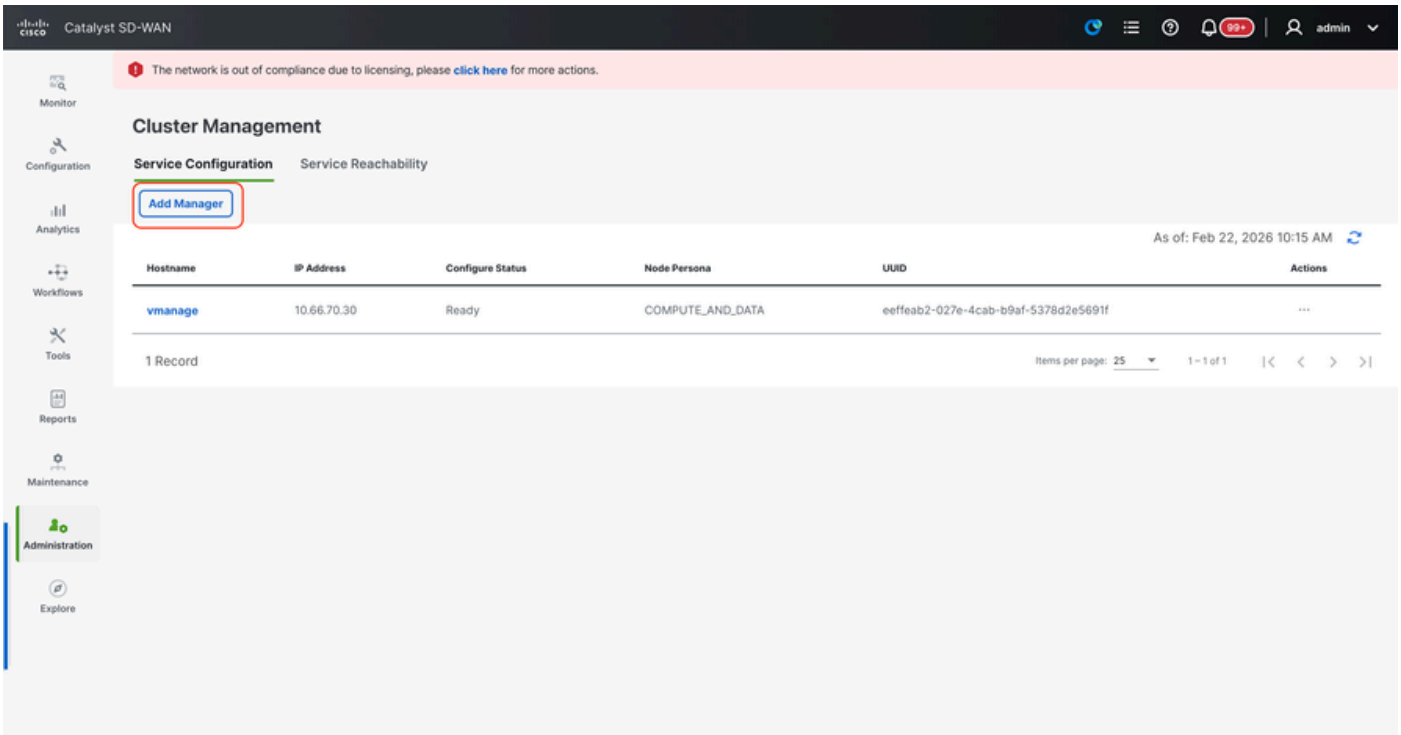
- この後、vManage NMSサービスがバックグラウンドで再起動し、UIは約5 ~ 10分間使用できません。この間、vManageのCLIアクセスが可能になります。
- vManage-1 UIにアクセスしたら、Administration > Cluster Managementに移動し、vManageのサービスインターフェイスIPがIP addressの下に反映されていることを確認します。設定ステータスはReadyで、ノードのペルソナが正しく反映されています。
- 同じページのService reachabilityセクションに切り替え、すべてのサービスが到達可能であることを確認します。

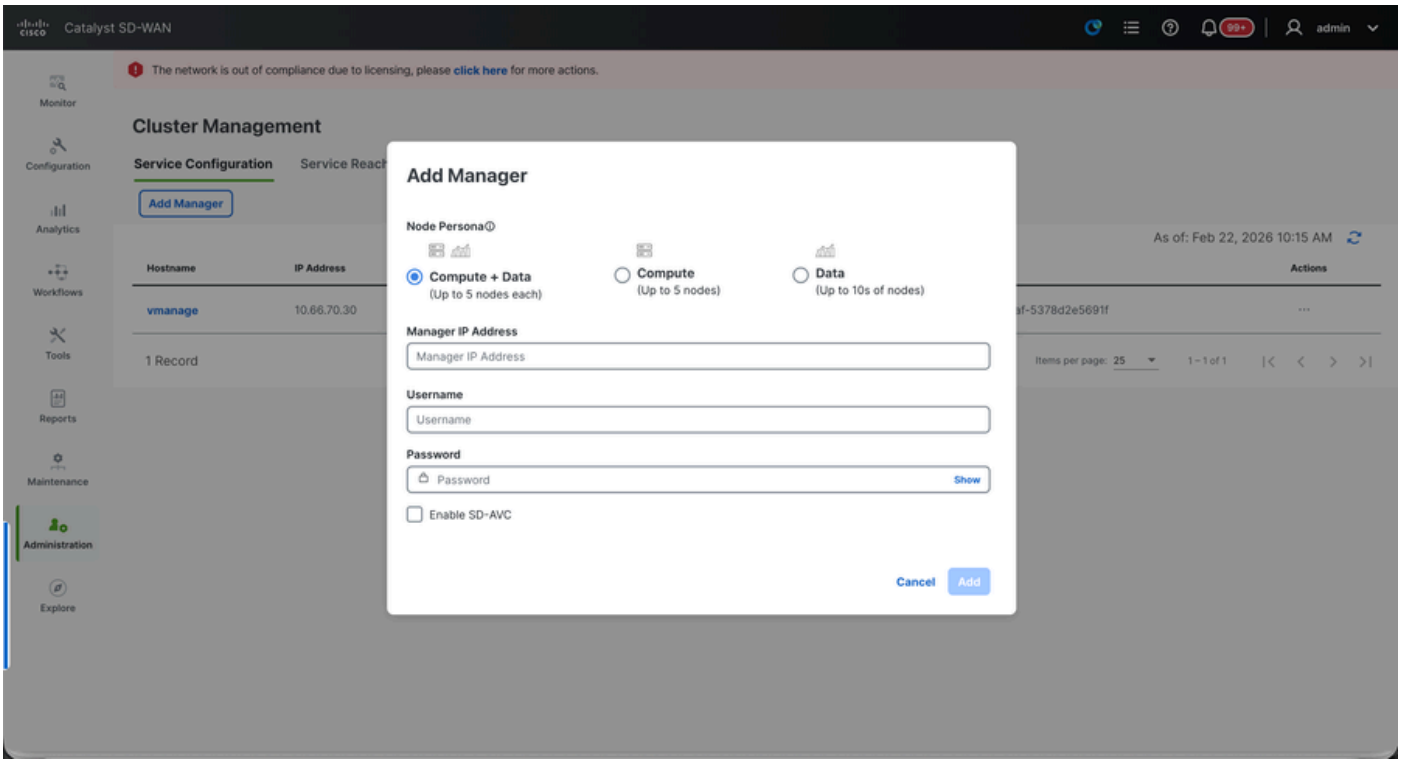


- まだ到達できないサービスがある場合は、お待ちください。通常は20 ~ 30分ほどかかります。

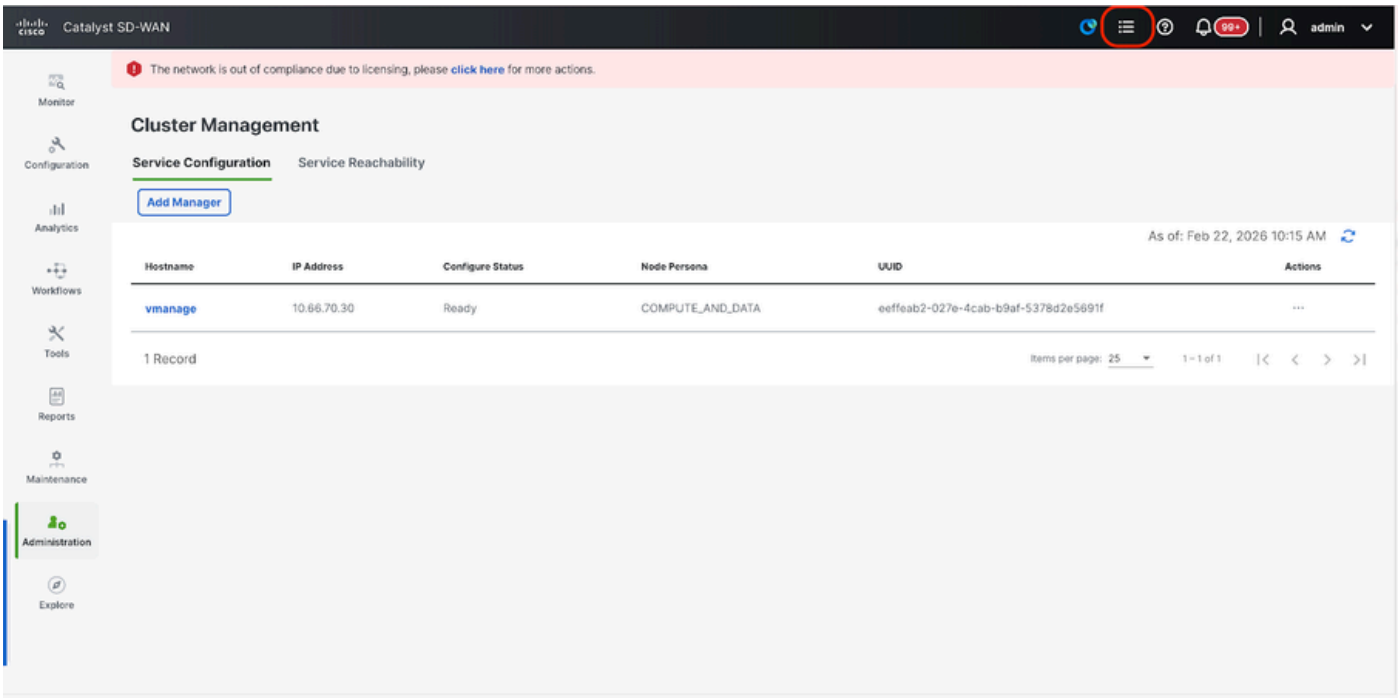
vManageクラスタの構築

- vManage-1のwebUIで、「Service Configuration,
- Add Managerをクリックすると、ポップアップウィンドウが表示されます。





- vManage - 2ノードがスピンアップした際に行ったペルソナ設定に基づいて、ノードのペルソナを選択します。
- Manager IP addressの下に、service interface IP of vManage-2を入力します
- ユーザ名とパスワードを入力します。これは、ステップ6で使用したクレデンシャルと同じです。
- SDAVCを有効にする：vManage-1ですでに有効にしているので、オフのままにします。
- [Add] をクリックします。
- この後、vManage NMSサービスがvManage 1および2ノードのバックグラウンドで再起動します。vManage 1および2では、UIは数分（約5 ~ 10分）使用できません。
- この間、vManage 1および2のCLIアクセスが使用できます。
- vManage-1 UIにアクセスできたら、Administration > Cluster Managementに移動し、両方のvManageのサービスインターフェイスIPがIPアドレスの下に反映されていることを確認します。Configure StatusはReady、ノードペルソナは正しく反映されています。
- 同じページのサービス到達可能性セクションに切り替え、両方のvManageノードですべてのサービスに到達できることを確認します。
- まだ到達できないサービスがある場合は、お待ちください。通常は5 ~ 10分ほどかかります。
- クラスタ追加プロセスのステータスは、vManage UIの右上隅にあるタスクリストで確認できます。



- [アクティブなタスクの一覧]を検索し、タスクがまだ[アクティブなタスクの一覧]に表示されている場合は、タスクがまだ完了していないことを示します。
- タスクをクリックすると、同じタスクの進捗状況を確認できます。 タスクが[アクティブなタスクの一覧]に表示されていない場合は、[完了]に切り替えて、タスクが正常に完了することを確認します。
- これらのポイントが検証された後にのみ、次の手順に進みます。

クラスタに次のノードを追加する前に、次の点を考慮する必要があります。

これまでにクラスタに追加したvManageノードのすべてのUIで、次の点を確認してください。

- vManage UIのMonitor > Overviewに移動し、vManageノードの数が正しく反映されていること、およびクラスタに追加されたノードの数に応じて到達可能と表示されていることを確認します。

- Administration > Cluster Managementの順に移動し、IP addressの下に両方のvManageのサービスインターフェイスIPが反映されていること、Configure StatusがReadyであること、ノードペルソナが正しく反映されていることを確認します。
- 同じページのサービス到達可能性セクションに切り替え、両方のvManageノードですべてのサービスに到達できることを確認します。

- クラスタにノードが追加されるたびに、クラスタ内のすべてのノードのNMSサービスが再起動されるため、これらのノードのUIがしばらくの間到達不能になります。
- クラスタ内のノードの数によっては、UIがバックアップされ、すべてのサービスが到達可能になるまでに時間がかかる場合があります。
- vManage UIの右上隅にあるTask-list availableでタスクをモニタできます。
- クラスタに追加された各ノードのvManage UIで、すべてのルータ、テンプレート、およびポリシー（vManage-1で使用可能な場合）を確認する必要があります。
- これらの構成がvManage-1にない場合は、vManage-1に追加されたvBondおよびvSmartsと、Organization-name、vBond、Certificate AuthorizationのAdministration > Settings構成が、

クラスタに追加された残りのvManageノードに反映されている必要があります。
- 残りのvManageノードに対して同じ手順を繰り返します。

すべてのコントローラがオンボーディングされたら、次の手順を実行します。

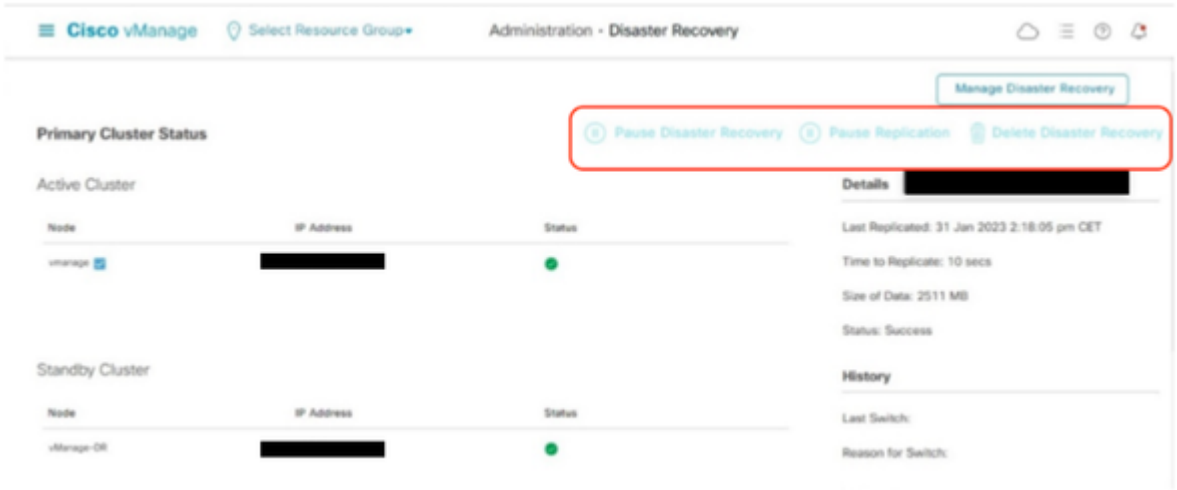
ステップ4:Config-dbのバックアップ/復元

別のvManageノードでのvManage構成データベースのバックアップと復元の収集

注：ディザスタリカバリが有効になっている既存のvManageクラスタから設定データベースバックアップを収集する際には、そのノードのディザスタリカバリが一時停止して削除された後に、バックアップが収集されていることを確認してください。

継続的な災害復旧レプリケーションがないことを確認します。Administration > Disaster Recoveryの順に移動し、 ステータスが「成功」であり、「インポート保留中」、「エクスポート保留中」、「ダウンロード保留中」などの一時的な状態ではないことを確認します。ステータスがsuccessではない場合、ディザスタリカバリを一時停止する前に、Cisco TACに連絡してレプリケーションが成功することを確認します。

まず、ディザスタリカバリを一時停止し、タスクが完了していることを確認します。次に、ディザスタリカバリを削除し、タスクが完了したことを確認します。



ディザスタリカバリが正常にクリーンアップされたことをCisco TACに確認します。

Configuration-DBバックアップの収集：

- 現在使用されているSD-WANファブリックでは、vManageクラスタからconfiguration-dbバックアップを生成できます。
- configuration-dbバックアップは、configuration-dbのリーダーであるvManageクラスタの1つのノードでのみ生成する必要があることに注意してください。

- スタンドアロンvManageの場合、そのvManage自体がconfiguration-dbのリーダーです。

- vManageクラスタで、コマンドrequest nms configuration-db diagnosticsを使用して、configuration-dbリーダーノードを特定します。このコマンドは、3ノードvManageクラスタのすべてのノードで実行できます。
- 6ノードクラスタでは、リーダーノードを識別するためにconfiguration-dbが有効になっているvManageノードで必ずこのコマンドを実行します。 Administration > Cluster Managementの順に移動し、同じことを確認します。
- スクリーンショットに示すように、ペルソナCOMPUTE_AND_DATAで設定されたノードではconfiguration-dbが実行されています。

vManageCLIでコマンドrequestnmsconfiguration-dbstatusを使用して同じ内容を確認できます。出力は次のようになります

```
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#
```

- コマンドを実行すると、これらのノードに対してnms configuration-db diagnosticsを要求します。出力は次のようになります。
- 「IsLeader」の強調表示されたフィールドを探します。 1に設定されている場合、ノードがリーダーノードであることを示し、そこからconfiguration-dbバックアップを収集できます。

```
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     .
```

このコマンドを使用して、特定されたconfiguration-dbリーダーのvManageノードから configuration-dbのバックアップを収集します。

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

予想される出力は次のとおりです。

```
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#
```

- configuration-dbクレデンシャルが更新されている場合は、それをメモします。
- configuration-dbクレデンシャルを知らない場合は、TACに問い合わせて、既存のvManageノードからconfiguration-dbクレデンシャルを取得してください。
- デフォルトのconfiguration-dbクレデンシャルは、ユーザ名：neo4jおよびパスワード：passwordです。

構成データベースのバックアップを別のvManageノードに復元

SCPを使用して、vManageの/home/admin/ディレクトリにconfiguration-dbバックアップをコピーします。

scpコマンドの出力例：

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

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

configuration-dbのバックアップを復元するには、まずconfiguration-dbのクレデンシャルを設定する必要があります。configuration-dbクレデンシャルがデフォルト(neo4j/password)の場合は、このステップを省略できます。

configuration-dbクレデンシャルを設定するには、コマンドrequest nms configuration-db update-admin-userを使用し、任意のユーザ名とパスワードを使用します。

vManageのアプリケーションサーバが再起動します。このため、vManage UIに短時間アクセスできなくなります。

```
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#
```

設定データベースのバックアップの復元に進むことができる投稿：

request nms configuration-db restore path /home/admin/< >コマンドを使用して、新しいvManageに設定データベースを復元できます。

```
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
```

configuration-dbが復元されたら、vManage UIにアクセスできることを確認します。5分ほど待ってから、UIへのアクセスを試みます。

UIに正常にログインしたら、エッジルータのリスト、テンプレート、ポリシー、および以前または既存のvManage UIに存在していた残りのすべての設定が、新しいvManage UIに反映されていることを確認します。

ステップ5：コントローラの再認証と古いコントローラの無効化

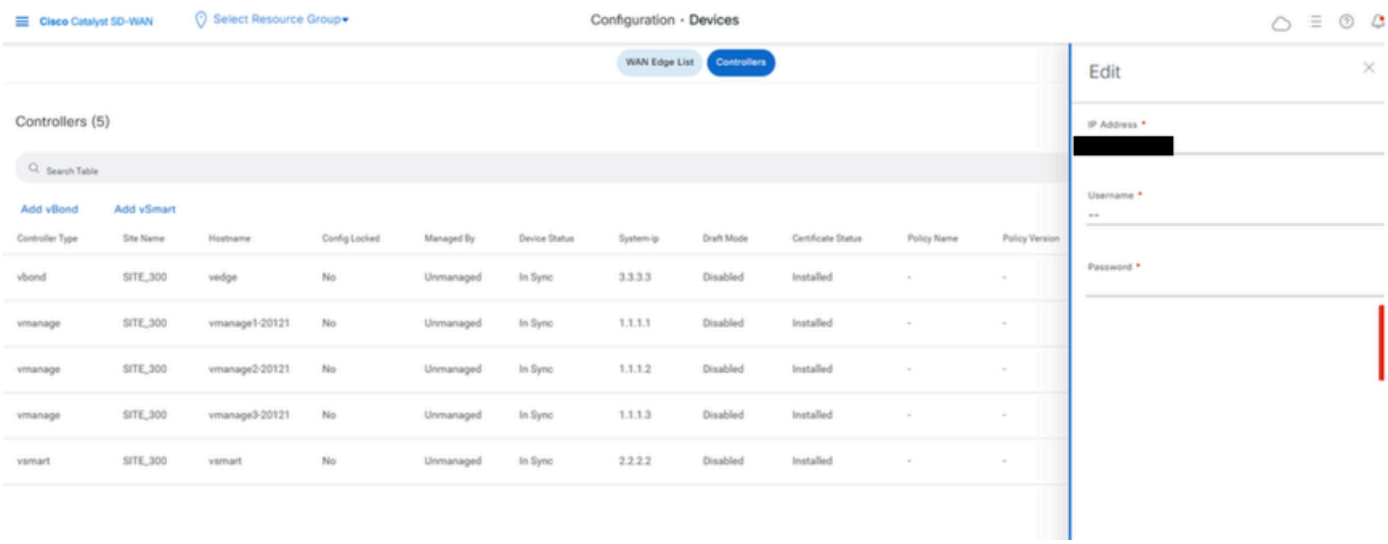
configuration-dbが復元されたら、ファブリック内のすべての新しいコントローラ(vmanage/vsmart/vbond)を再認証する必要があります

注：実際の運用で、再認証に使用されるインターフェイスIPがトンネルインターフェイスIPである場合、vManage、vSmart、およびvBondのトンネルインターフェイスでNETCONFサービスが許可され、パスに沿ったファイアウォールでもNETCONFサービスが許可されるようにする必要があります。開くファイアウォールポートは、DRクラスタ

からすべてのvBondおよびvSmartsへの双方向ルールとしてTCPポート830です（この例では、DRクラスタはIPアドレスがIPアドレスに一致します）。

vmanage UIで、Configuration > Devices > Controllersの順にクリックします。

- 各コントローラの近くにある3つのドットをクリックし、[編集]をクリックします



- ip-address（コントローラのsystem-ip）をtransport vpn 0（トンネルインターフェイス）ip addressに置き換えます。ユーザ名とパスワードを入力して、saveをクリックします
- ファブリック内のすべての新しいコントローラに対して同じ操作を行います

Root-cert-chainの同期

すべてのコントローラがオンボーディングされたら、次の手順を実行します。

新しくアクティブになったクラスタ内の任意のCisco SD-WAN Managerサーバで、次の操作を実行します。

ルート証明書を、新しくアクティブになったクラスタ内のすべてのCisco Catalyst SD-WANデバイスと同期させるには、次のコマンドを入力します。

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

次のコマンドを入力して、Cisco SD-WAN Manager UUIDをCisco SD-WAN Validatorと同期させます。

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

ファブリックが復元され、ファブリック内のすべてのエッジとコントローラに対してコントロールセッションとbfdセッションが確立されたら、古いコントローラ(vmanage/vsmart/vbond)をUIから無効にする必要があります

- vmanage UIで、Configuration > Devices > Certificatesの順にクリックします。

- Controllersをクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。[無効]をクリックします
- vbondに送信をクリックします。
- vmanage UIで、Configuration > Devices > Controllersの順にクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。[Delete] をクリックします。

ステップ6：事後チェック

注：すべての導入の組み合わせに共通する、ここに示す導入後のチェックセクションを続行します。

組み合わせ4:vManageクラスタ+手動/コールドスタンバイDR

手動/コールドスタンバイDRとは バックアップSD-WAN ManagerサーバまたはSD-WAN Managerクラスタは、コールドスタンバイ状態でシャットダウンされたままになります。

アクティブなデータベースの定期的なバックアップが取られ、プライマリのSD-WAN ManagerまたはSD-WAN Managerクラスタがダウンした場合は、スタンバイのSD-WAN ManagerまたはSD-WAN Managerクラスタが手動で起動され、バックアップデータベースがその上に復元されます。

必要なインスタンス

- 3または6 vManage（プライマリクラスタ）
- 3または6 vManage（DRスタンバイクラスタ）
- 1つ以上のvBond（プライマリデータセンターとDRデータセンターに分散）
- 1つ以上のvSmart（プライマリデータセンターとDRデータセンターに分散）

手順：

1. 共通ステップを使用してすべてのインスタンスを起動する
2. 事前チェック
3. vManage UI、証明書、およびオンボードコントローラの設定
4. vManageクラスタの構築
5. コールドスタンバイDRクラスタセットアップ
6. Config-dbバックアップ/復元
7. 事後チェック

ステップ1：事前チェック

- アクティブなCisco SD-WAN Managerインスタンスの数が、新しくインストールしたCisco SD-WAN Managerインスタンスの数と同じであることを確認します。

- アクティブなCisco SD-WAN Managerインスタンスと新しいCisco SD-WAN Managerイン

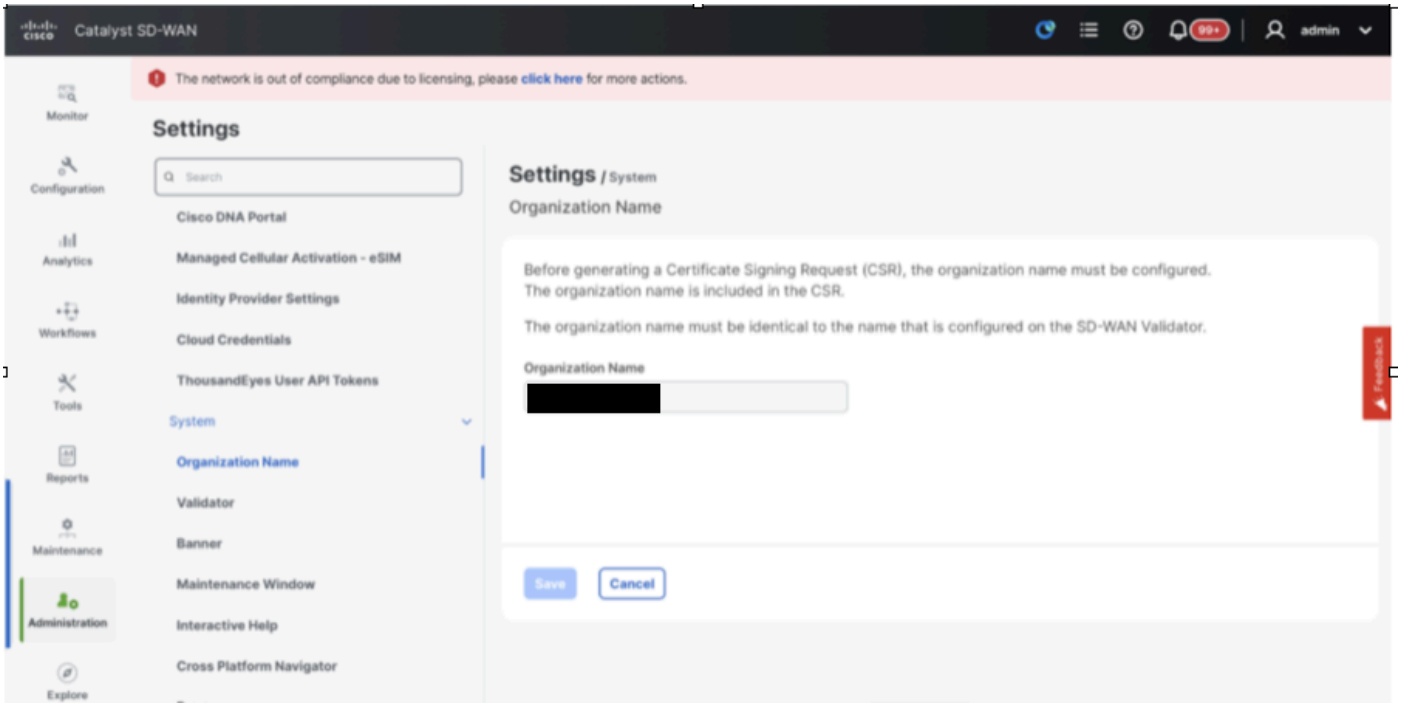
スタンスのソフトウェアバージョンがすべて同じであることを確認します。

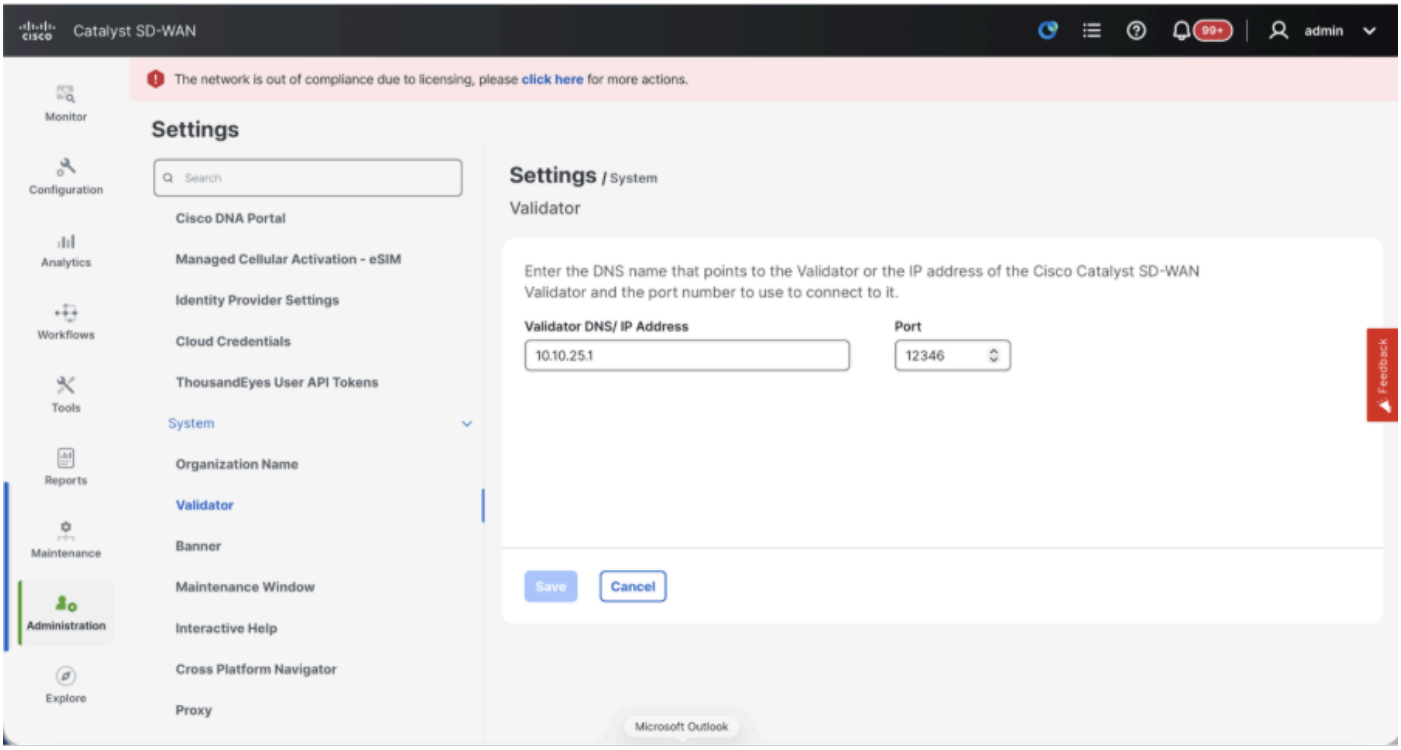
- アクティブおよび新規のすべてのCisco SD-WAN Managerインスタンスが、Cisco SD-WAN Validatorの管理IPアドレスに到達できることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスに証明書がインストールされていることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスを含め、すべてのCisco Catalyst SD-WANデバイスのクロックが同期されていることを確認します。
- 新しくインストールされたCisco SD-WAN Managerインスタンスで、システムIPとサイトIDの新しいセットが、アクティブクラスタと同じ基本設定とともに設定されていることを確認します。

手順2:vManage UI、証明書、オンボードコントローラを設定します。

vManage UIでの設定の更新

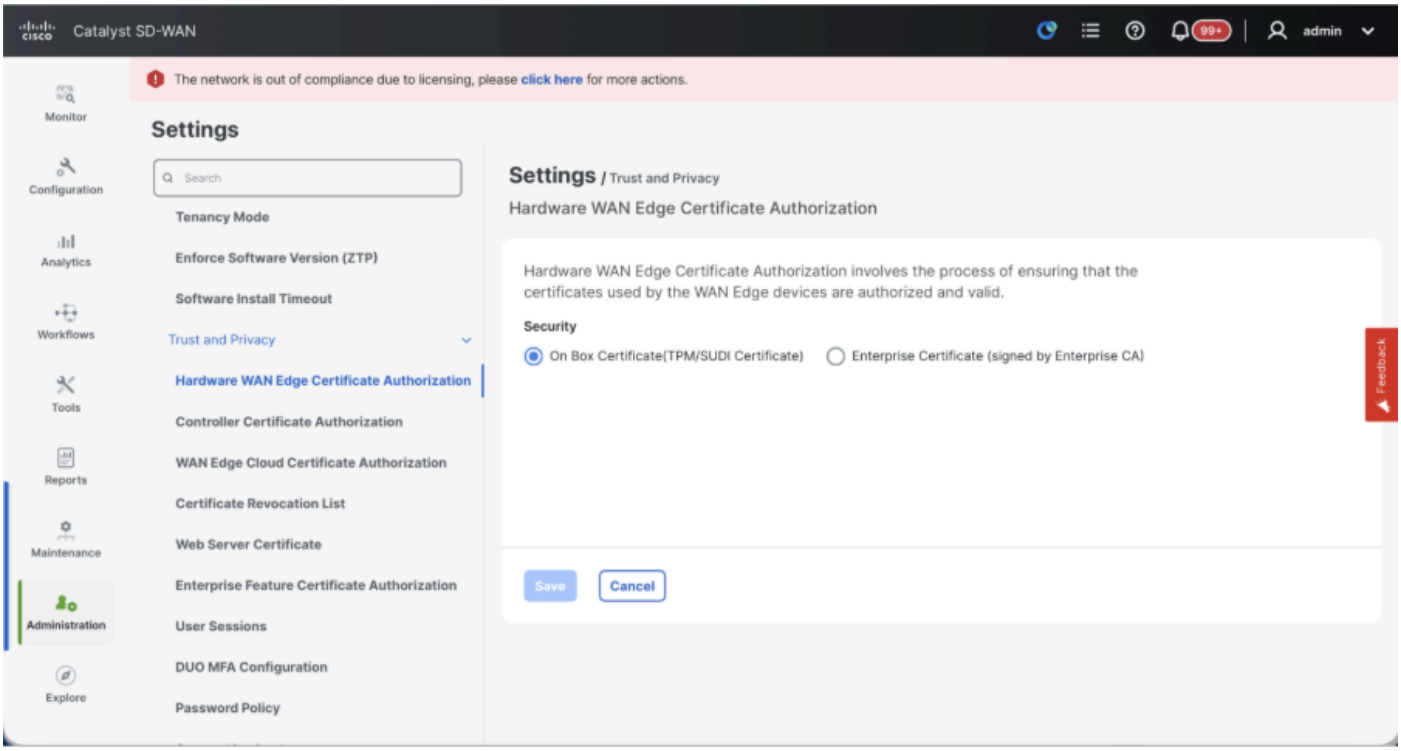
- ステップ1の設定がすべてのコントローラのCLIに追加されたら、ブラウザでURL https://<vmanage-ip>を使用して、vManageのWebUIにアクセスできます。各vManageノードのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- Administration > Settingsの順に移動し、次の手順を実行します。
- 組織名とValidator/vBond URL/IPアドレスを設定します。vManageノードのCLIと同じ値を設定します。
- vManage 20.15/20.18では、これらの設定はシステムのセクションで利用できます。



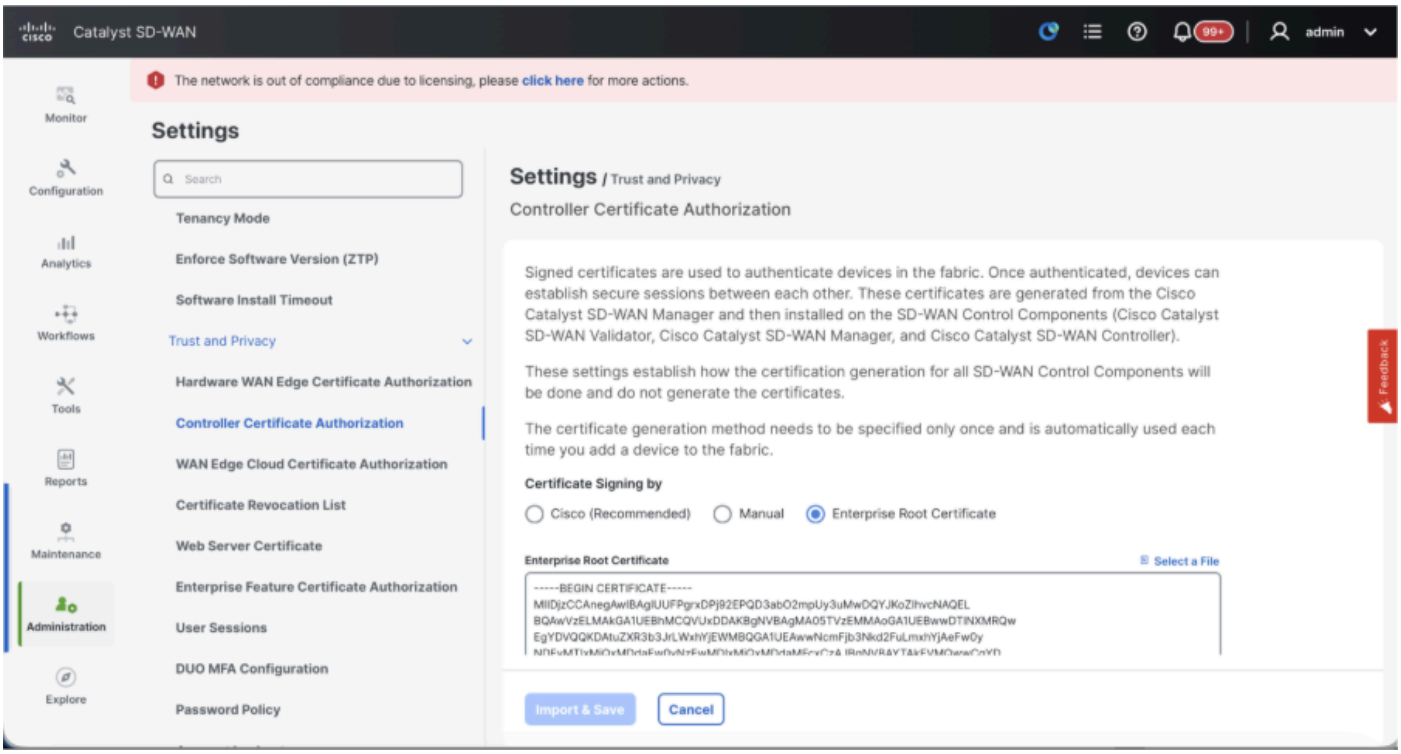


- 証明書の署名に使用する認証局(CA)を決定する証明書承認(CA)の設定を確認します。3つのオプションがあります。

1. ハードウェアWANエッジ証明書認証：ハードウェアSD-WANエッジルータのCAを決定します。
    - オンボックス証明書（TPM/SUDI証明書）– このオプションを使用すると、制御接続（TLS/DTLS接続）を確立するために、ルータハードウェアにプレインストールされている証明書が使用されます
    - エンタープライズ証明書（エンタープライズCAによって署名された）– このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

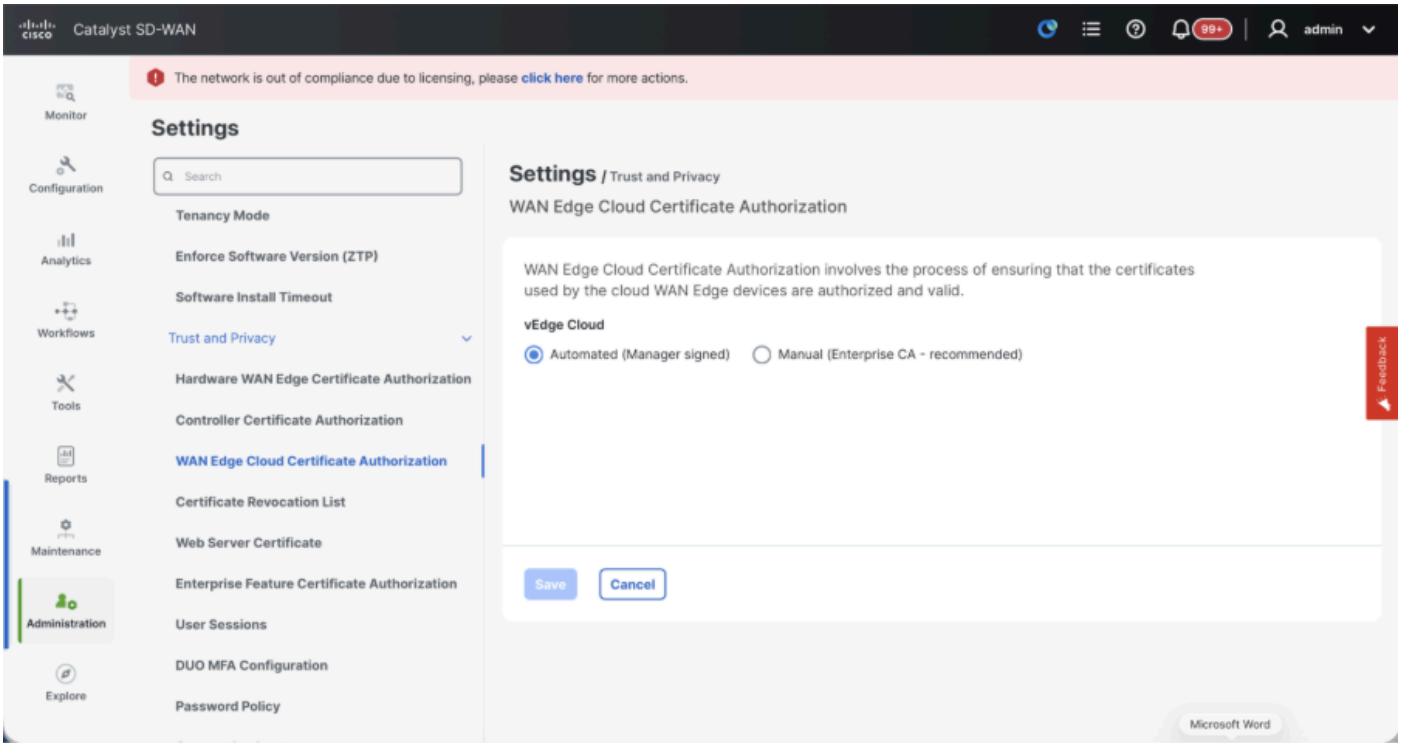


2. Controller Certificate Authorization（コントローラ証明書認証）:SD-WANコントローラのCAを決定します。
    - シスコ（推奨）– コントローラはCisco PKIによって署名された証明書を使用します。vManageは、vManageで設定されたスマートアカウント資格情報を使用してPNPポータルに自動的に接続し、証明書に署名してコントローラにインストールされます。
    - 手動：コントローラはCisco PKIによって署名された証明書を使用します。それぞれのSD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用して手動でCSRに署名します。
    - エンタープライズルート証明書：このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

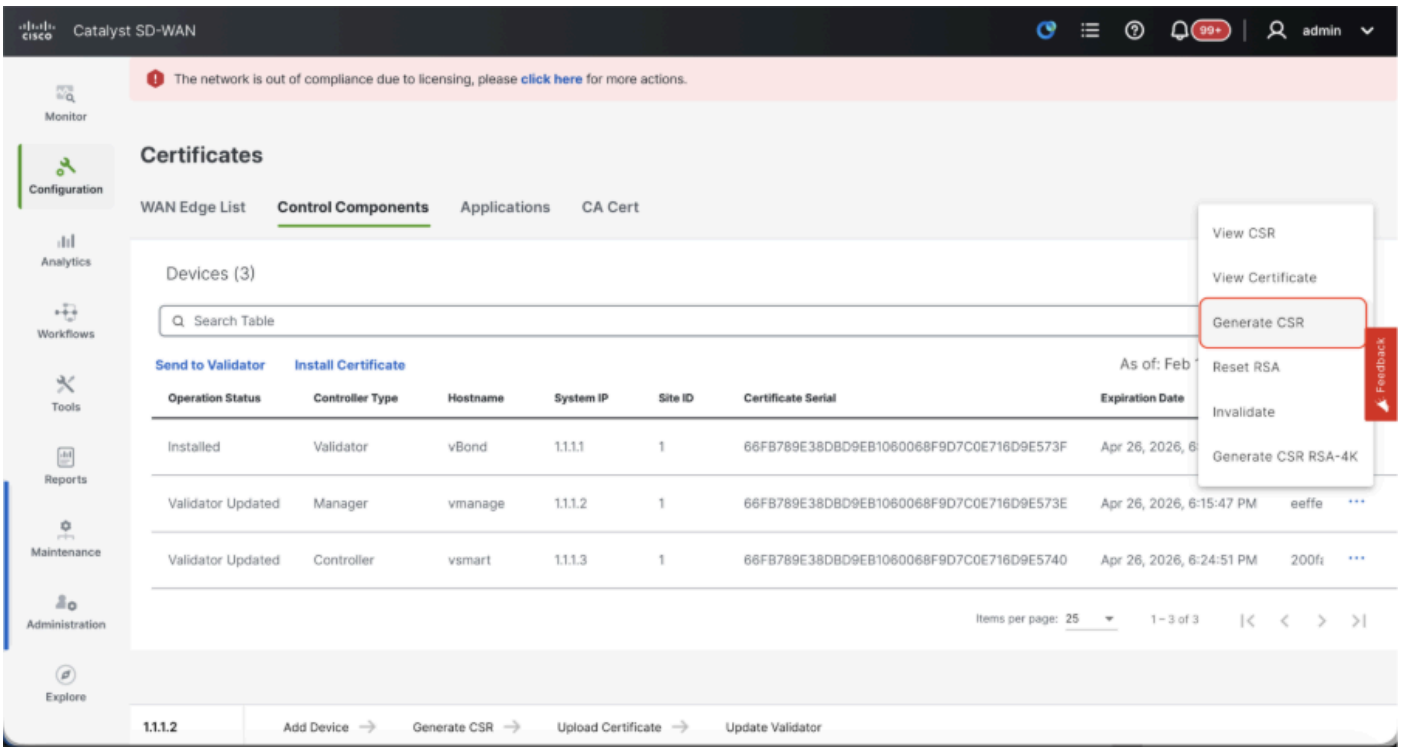


3. WANエッジクラウド証明書認証：仮想SD-WANエッジルータ（CSR1000v、C8000v、vEdgeクラウド）のCAを決定します。
    - 自動（vManage署名済み）:vManageは、仮想エッジルータのCSRに自動的に署名し、証明書をルータにインストールします。
    - 手動（エンタープライズCA – 推奨）– 仮想ルータは、組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

独自のCA（エンタープライズ認証局）を使用している場合は、Enterpriseを選択します。



- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers
- Manager/vManageの「。..」をクリックし、「CSRの生成」をクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。

vBond/ValidatorおよびvSmart/ControllerのvManageへのオンボーディング

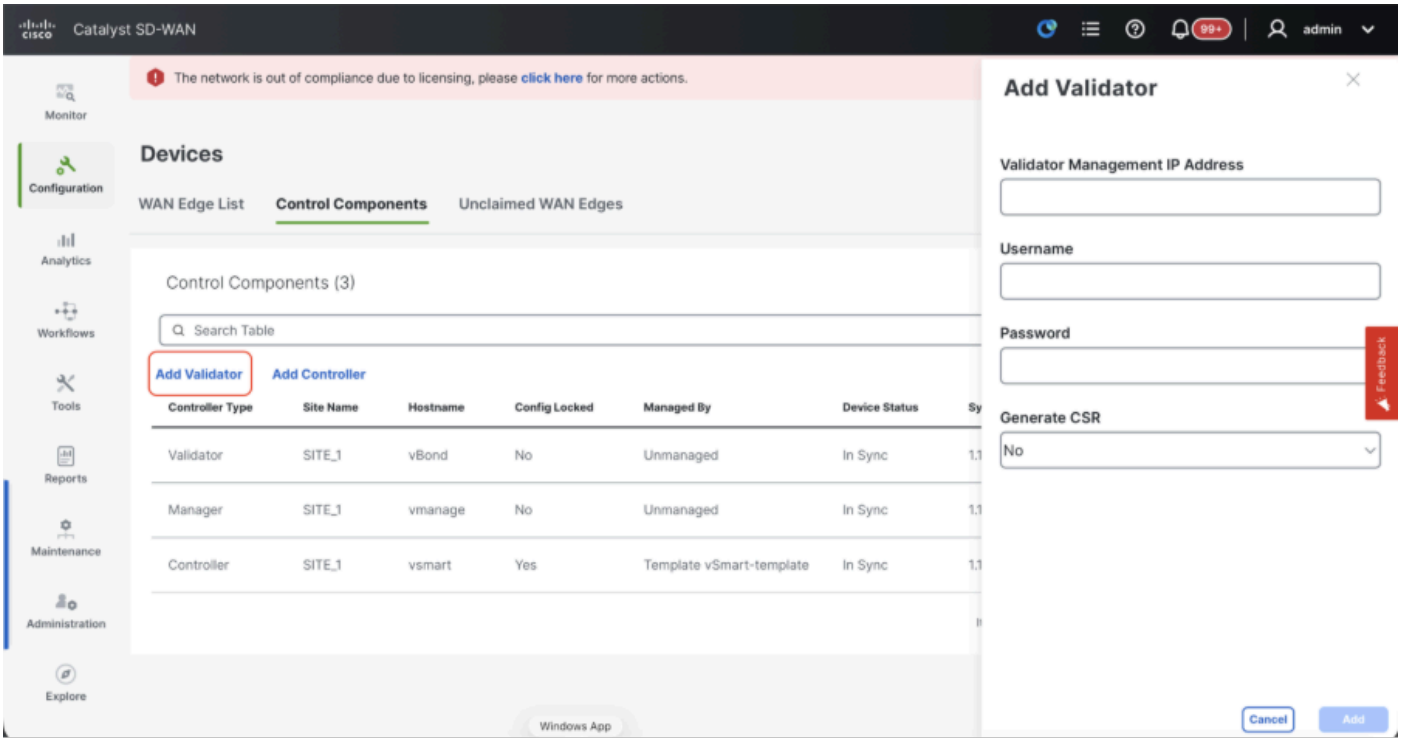
20.15/20.18 vManageノードの場合は、Configuration > Devices > Control Componentsの順に移動します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

オンボーディングvBond/バリデータ

- onAddvBondをクリックします20.12vManagerの場合バリデータの追加20.15/20.18vManageの場合。ポップアップが表示されたら、 VPN 0は、vManageから到達可能なvBondのIPを転送します。
- vManagetovBondIPのCLIからpingを使用して（許可されている場合）到達可能性を確認します。
- vBondのユーザクレデンシャルを入力します。

注:NetAdminグループのユーザ部分であるvBondorの管理者クレデンシャルを使用する必要があります。これはthevBondのCLIで確認できます。vBondの新しい証明書をインストールする必要がある場合は、「CSRの生成」のドロップダウンでYesを選択します

注:vBondがNATデバイス/ファイアウォールの背後にある場合は、vBond VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認してください。VPN 0インターフェイスIPにvManageから到達できない場合は、このステップでVPN 0インターフェイスのパブリックIPアドレスを使用します

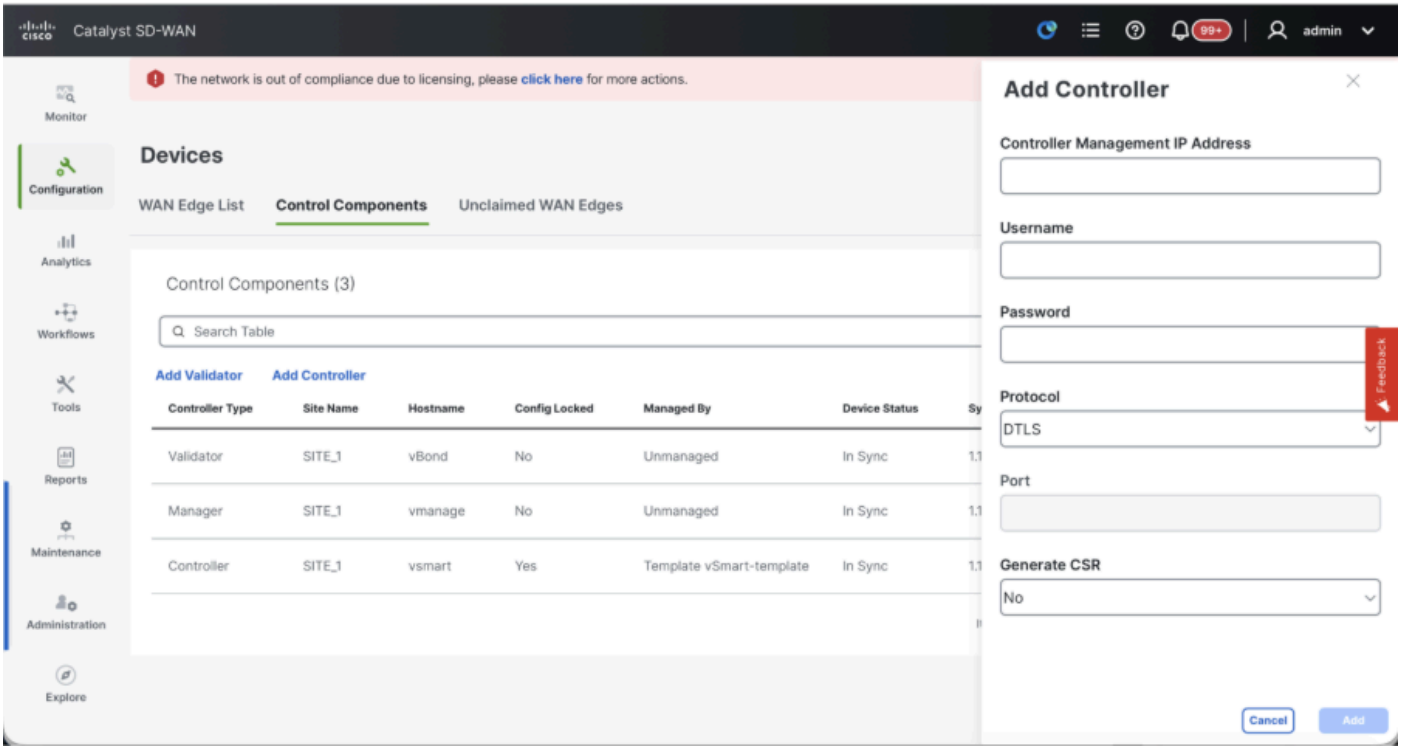


- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vBondに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvBondがある場合は、同じ手順を繰り返します。

vSmart/コントローラのオンボーディング：

- 20.12 vManageの場合はAdd vSmartを、20.15/20.18 vManageの場合はAdd Controllerをクリックします。
- ポップアップが開いたら、vManageから到達可能なvSmartのVPN 0トランスポートIPを入力します。
- vManageのCLIからvSmart IPにpingを使用して（許可されている場合）到達可能性を確認します。
- vSmartの管理者クレデンシャルまたはnetadminグループのユーザ部分を使用する必要があるvSmart Noteのユーザクレデンシャルを入力します。
- これは、vSmartのCLIで確認できます。
- ルータにTLSを使用してvSmartとの制御接続を確立する場合は、プロトコルをTLSに設定します。 この構成は、vSmartsおよびvManageノードのCLIでも構成する必要があります。
- vSmartの新しい証明書をインストールする必要がある場合は、「Generate CSR」のドロップダウンで「Yes」を選択します。

注：vSmartがNATデバイス/ファイアウォールの背後にある場合は、vSmart VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認し、VPN 0インターフェイスIPがvManageから到達できない場合は、この手順でVPN 0インターフェイスIPのパブリックIPアドレスを使用します。



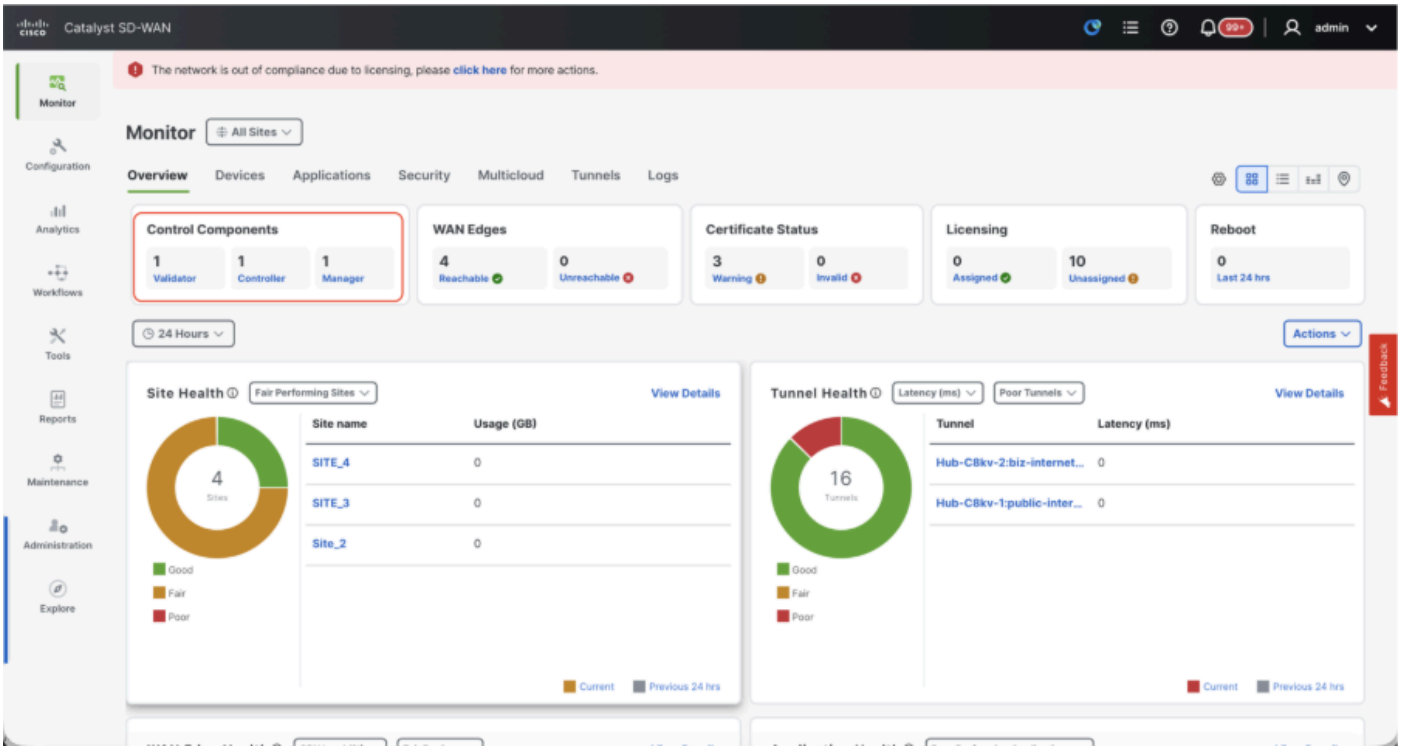
- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate

Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vSmartに自動的にインストールされます。

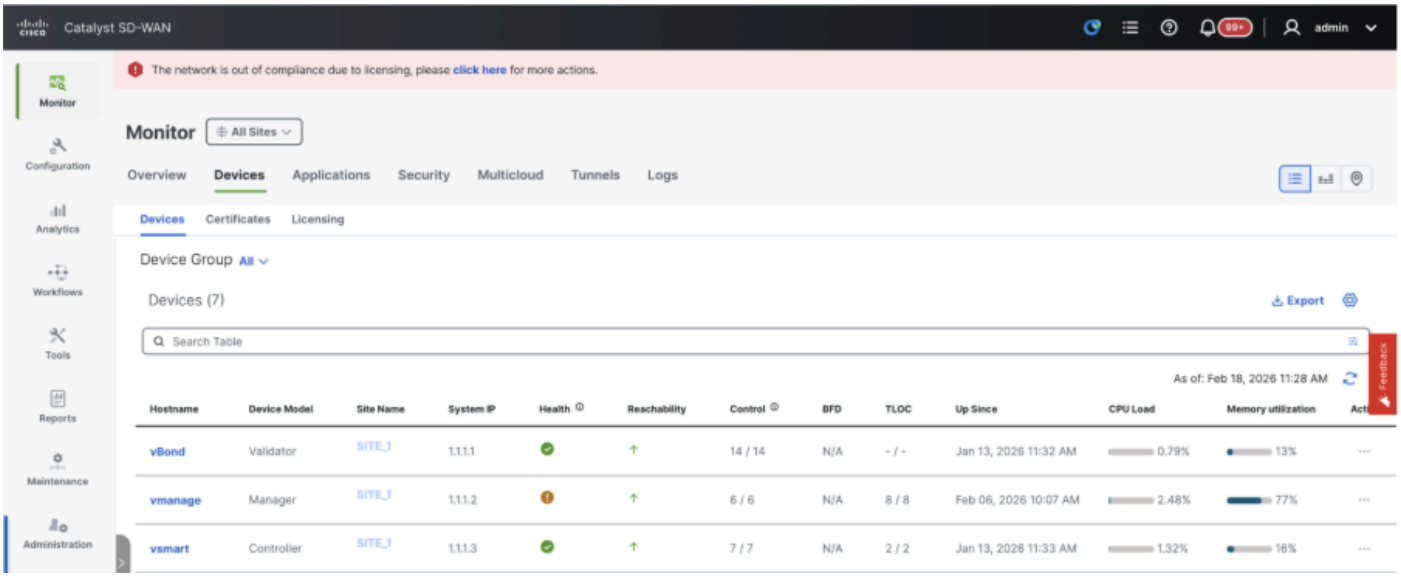
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvSmartsがある場合は、同じ手順を繰り返します。

検証

すべての手順が完了したら、Monitor>Dashboardですべての制御コンポーネントに到達できることを確認します



- それぞれの制御コンポーネントをクリックして、それらがすべて到達可能であることを確認します。
- Monitor > Devicesの順に移動し、すべての制御コンポーネントが到達可能であることを確認します。



ステップ3:vManageクラスタの構築

SD-WANオーバーレイでvManageクラスタを使用したオンボードSD-WANファブリック

注:vManageクラスタは、SD-WANファブリックにオンボーディングされたサイトの数に応じて、3つのvManageノードまたは6つのvManageノードで構成できます

1つのvManageノードですべてのSD-WANコントローラをオンボード

「SD-WANオーバーレイでの単一ノードvManageによるSD-WANコントローラのオンボード」で共有されている手順に進み、まず1つのvManageノードでSD-WANファブリックを起動し、必要なすべてのバリデータ(vBond)とコントローラ(vSmart)をオンボードします。

クラスタに含まれるすべてのvManageノードのCLI設定を構成します

- 残りのvManageノードを設定します。 3ノードクラスタの場合は、残りの2ノードを構成します。6ノードクラスタの場合は、5ノードを構成します。
- 次に示すように、システム設定を行います。

```
config t
system
 host-name



 system-ip
```

```
 site-id


 organization-name


 vbond


commit
```

注:vBondアドレスとしてURLを使用している場合は、DNSサーバのIPアドレスをVPN 0設定で設定するか、解決できることを確認してください。

これらの設定は、ルータおよびその他のコントローラとの制御接続の確立に使用されるトランスポートインターフェイスを有効にするために必要です。

```
config t
vpn 0
 dns


        primary
 dns


         secondary
 interface eth1
  ip address


  tunnel-interface
```

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



commit
```

また、コントローラへのアウトオブバンド管理アクセスを有効にするためにVPN 512managementインターフェイスも設定します。

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

オプションの構成：

- 既存のコントローラの設定を参照できます。ここにリストされている設定が存在する場合は、新しいコントローラにこの設定を追加できます。
- ルータがTLSを使用してvManageノードとのセキュアな制御接続を確立する必要がある場合にのみ、制御プロトコルをTLSとして設定します。デフォルトでは、すべてのコントローラとルータがDTLSを使用して制御接続を確立します。これは、要件に応じてvSmartおよびvManageノードでのみ必要なオプションの設定です。

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

すべてのvManageノードでサービスインターフェイスを設定する

すでにオンボーディングされているvManage-1を含むすべてのvManagenodesでサービスインターフェイスを設定します。このインターフェイスは、クラスタ通信に使用されます。つまり、クラスタ内のvManagerノード間の通信です。

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

同じIPサブネットがvManageclusterのすべてのノードでサービスインターフェイスに使用されていることを確認します。

クラスタクレデンシャルの設定

vManagenodesと同じ管理者クレデンシャルを使用して、vManageclusterを設定できます。または、netadmingroupの一部である新しいユーザクレデンシャルを設定できます。新しいユーザクレデンシャルを設定する設定は次のとおりです

```
conf t
system
 aaa
  user
```

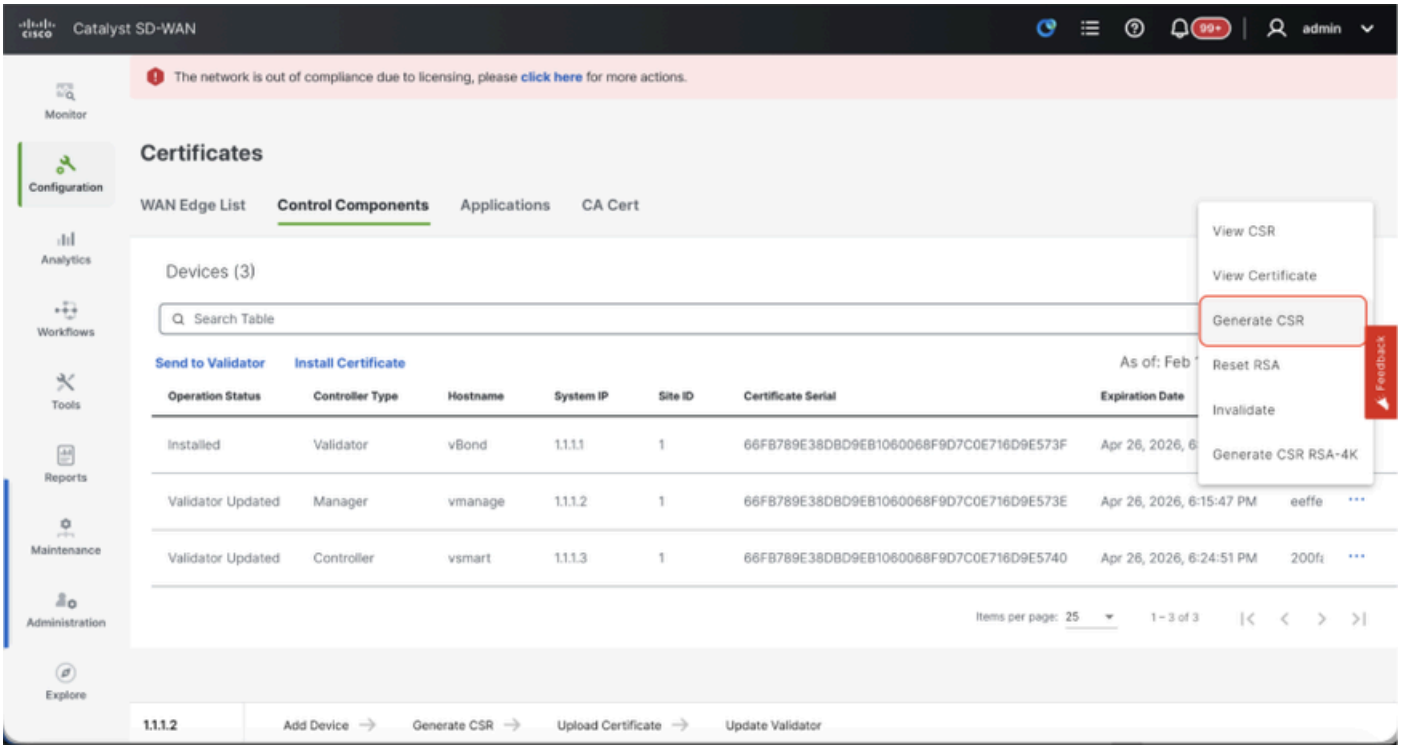
```
   password



   group    netadmin
commit
```

クラスタの一部であるvManagenodes全体で同じユーザクレデンシャルを設定することを確認します。管理者クレデンシャルを使用する場合は、すべてのvManagenodesで同じユーザ名/パスワードを使用する必要があります。

すべてのvManageノードにデバイス証明書をインストール

- ブラウザでURL https://<vmanage-ip>を使用して、すべてのvManagenodesのvManageUIにログインします。それぞれのvManagenodesのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

  Manager/vManageで…をクリックし、Generate CSRをクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- クラスタに含まれるすべてのvManageノードに対してこの手順を実行します。

vManageクラスタの構築の準備

- vManage-1のWebUIで、[管理] > [クラスタ管理] に移動し、[vManage-1のアクション]の下の[...]をクリックし、[編集]を選択します。
- ノードのペルソナは、VMのスピンアップ時に選択したペルソナに基づいて自動的に選択されます。

注:3ノードクラスタの場合、3つのvManageノードはすべて、ペルソナとしてcompute+dataを使用して起動されます。

- 6ノードクラスタの場合、3つのvManageノードはpersonaとしてcompute+dataを使用して起動され、3つのvManageノードはpersonaとしてdataを使用して起動されます。
- Manager IP addressのドロップダウンから、vManageのservice interface IPを選択します。
- vManageクラスタ（クラスタクレデンシャルと呼ばれます）を有効にするために使用するユーザ名とパスワードを入力します。
- 前述のように、すべてのvManageノードで同じクレデンシャルを設定し、すべてのノードをクラスタに追加する際に同じクレデンシャルを使用する必要があります。

オプションの構成：

SDAVCを有効にするには、既存のクラスタでこの設定を参照してください。この設定は、必要な場合、およびクラスタの1つのvManageノードでのみ必要な場合にのみ確認してください。

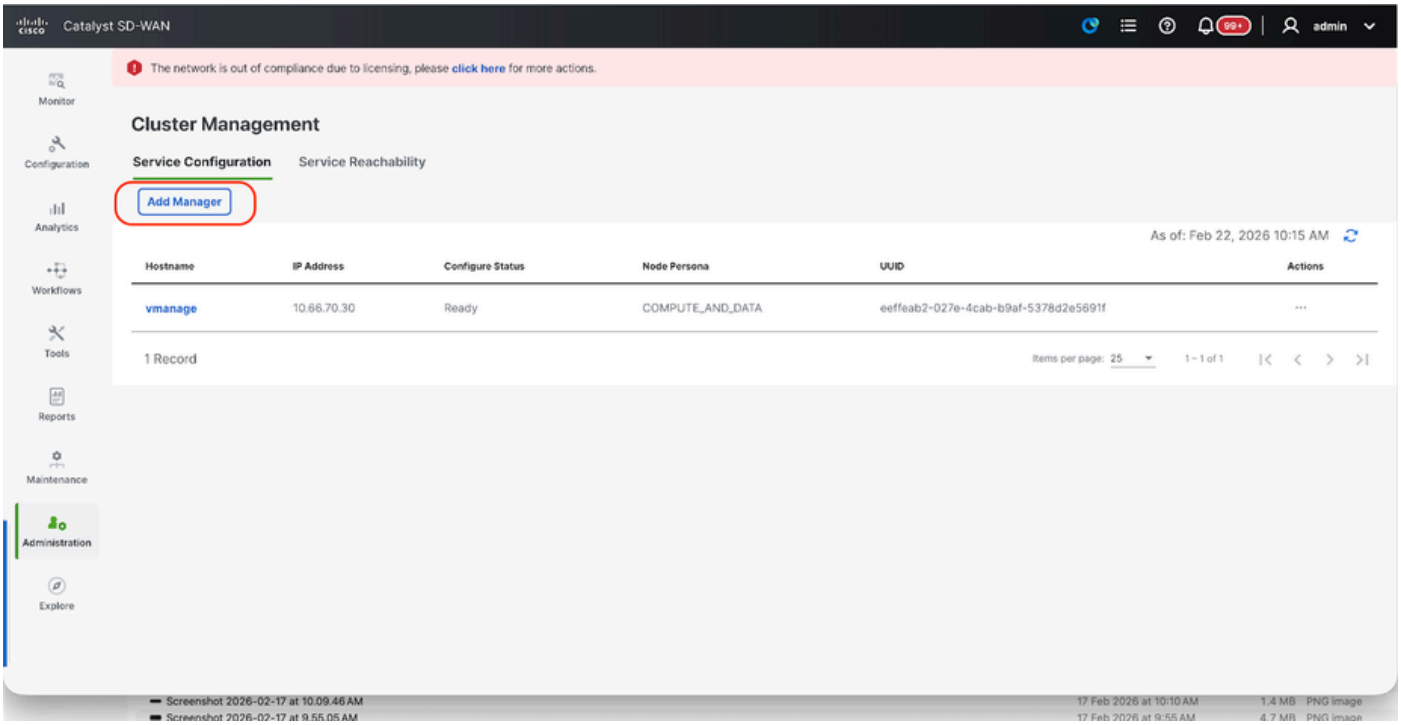
Updateをクリックします。

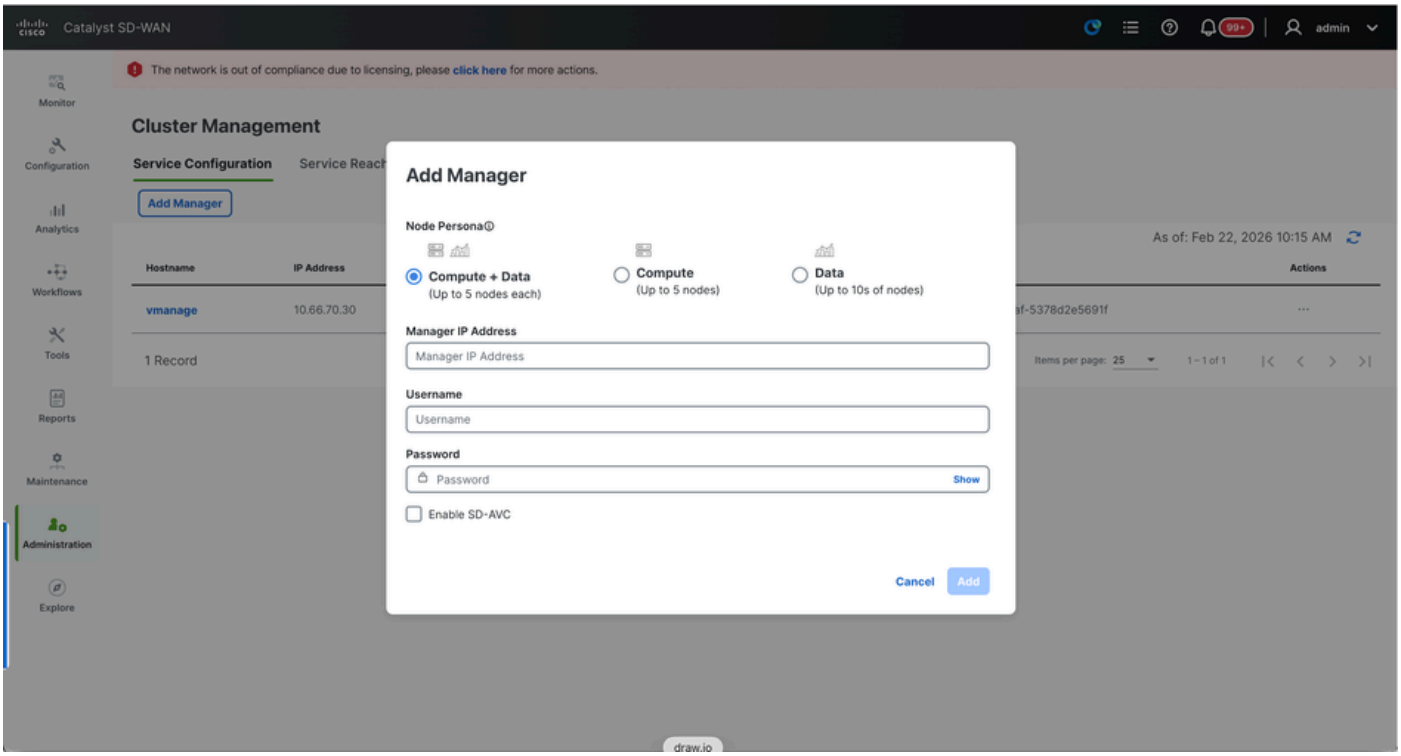
- この後、vManage NMSサービスがバックグラウンドで再起動し、UIは約5 ~ 10分間使用できません。この間、vManageのCLIアクセスが可能になります。
- vManage-1 UIにアクセスしたら、Administration > Cluster Managementに移動し、vManageのサービスインターフェイスIPがIP addressの下に反映されていることを確認しま

す。設定ステータスはReadyで、ノードのペルソナが正しく反映されています。同じページのService reachabilityセクションに切り替え、すべてのサービスが到達可能であることを確認します。
- まだ到達できないサービスがある場合は、お待ちください。通常は20 ~ 30分ほどかかります。

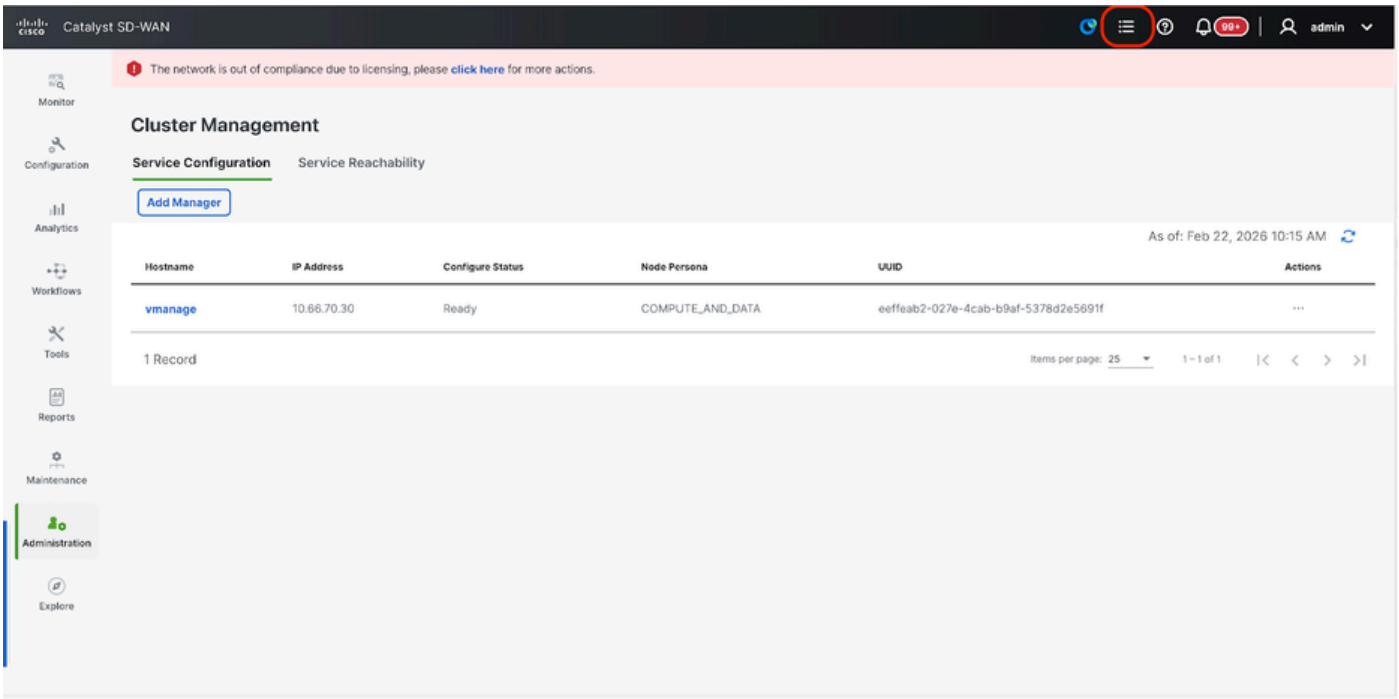
vManageクラスタの構築

- vManage-1のwebUIで、「Service Configuration,
- Add Managerをクリックすると、ポップアップウィンドウが表示されます。





- vManage - 2ノードがスピンアップした際に行ったペルソナ設定に基づいて、ノードのペルソナを選択します。
- Manager IP addressの下に、service interface IP of vManage-2を入力します
- ユーザ名とパスワードを入力します。これは、ステップ6で使用したクレデンシャルと同じです。
- SDAVCを有効にする：vManage-1ですでに有効にしているので、オフのままにします。
- [Add] をクリックします。
- この後、vManage NMSサービスがvManage 1および2ノードのバックグラウンドで再起動します。vManage 1および2では、UIは数分（約5 ~ 10分）使用できません。
- この間、vManage 1および2のCLIアクセスが使用できます。
- vManage-1 UIにアクセスできたら、Administration > Cluster Managementに移動し、両方のvManageのサービスインターフェイスIPがIPアドレスの下に反映されていることを確認します。Configure StatusはReady、ノードペルソナは正しく反映されています。
- 同じページのサービス到達可能性セクションに切り替え、両方のvManageノードですべてのサービスが到達可能であることを確認します。
- まだ到達できないサービスがある場合は、お待ちください。通常は5 ~ 10分ほどかかります。
- クラスタ追加プロセスのステータスは、vManage UIの右上隅にあるタスクリストで確認できます。



- [アクティブなタスクの一覧]を検索し、タスクがまだ[アクティブなタスクの一覧]に表示されている場合は、タスクがまだ完了していないことを示します。
- タスクをクリックすると、同じタスクの進捗状況を確認できます。 タスクが[アクティブなタスクの一覧]に表示されていない場合は、[完了]に切り替えて、タスクが正常に完了することを確認します。
- これらのポイントが検証された後にのみ、次の手順に進みます。

クラスタに次のノードを追加する前に、次の点を考慮する必要があります。

これまでにクラスタに追加したvManageノードのすべてのUIで、次の点を確認してください。

- vManage UIのMonitor > Overviewに移動し、vManageノードの数が正しく反映されていること、およびクラスタに追加されたノードの数に応じて到達可能と表示されていることを確認します。

- Administration > Cluster Managementの順に移動し、IP addressの下に両方のvManageのサービスインターフェイスIPが反映されていること、Configure StatusがReadyであること、ノードペルソナが正しく反映されていることを確認します。
- 同じページのサービス到達可能性セクションに切り替え、両方のvManageノードですべてのサービスに到達できることを確認します。

- クラスタにノードが追加されるたびに、クラスタ内のすべてのノードのNMSサービスが再起動されるため、これらのノードのUIがしばらくの間到達不能になります。
- クラスタ内のノードの数によっては、UIがバックアップされ、すべてのサービスが到達可能になるまでに時間がかかる場合があります。
- vManage UIの右上隅にあるTask-list availableでタスクをモニタできます。
- クラスタに追加された各ノードのvManage UIで、すべてのルータ、テンプレート、およびポリシー（vManage-1で使用可能な場合）を確認する必要があります。
- これらの構成がvManage-1にない場合は、vManage-1に追加されたvBondおよびvSmartsと、Organization-name、vBond、Certificate AuthorizationのAdministration > Settings構成が、クラスタに追加された残りのvManageノードに反映されている必要があります。
- 残りのvManageノードに対して同じ手順を繰り返します。

ステップ4：コールドスタンバイDRクラスタのセットアップ

コールドスタンバイDRクラスタセットアップ

「ステップ4:vManageクラスタの構築」で説明する手順を使用して、もう1つのvManageクラスタを起動できます。その後、「ステップ6:config-dbバックアップ/復元」で説明されている手順を実行して、スタンバイクラスタのconfig-dbバックアップを復元します。

ステップ5:Config-dbのバックアップ/復元

別のvManageノードでのvManage構成データベースのバックアップと復元の収集

Configuration-DBバックアップの収集：

- 現在使用されているSD-WANファブリックでは、vManageクラスタからconfiguration-dbバックアップを生成できます。
- configuration-dbバックアップは、configuration-dbのリーダーであるvManageクラスタの1つのノードでのみ生成する必要があることに注意してください。

- スタンドアロンvManageの場合、そのvManage自体がconfiguration-dbのリーダーです。
- vManageクラスタで、コマンドrequest nms configuration-db diagnosticsを使用して、configuration-dbリーダーノードを特定します。このコマンドは、3ノードvManageクラスタのすべてのノードで実行できます。
- 6ノードクラスタでは、リーダーノードを識別するためにconfiguration-dbが有効になっているvManageノードで必ずこのコマンドを実行します。 Administration > Cluster

Managementの順に移動し、同じことを確認します。
- スクリーンショットに示すように、ペルソナCOMPUTE_AND_DATAで設定されたノードではconfiguration-dbが実行されています。

vManageCLIでコマンドrequestnmsconfiguration-dbstatusを使用して同じ内容を確認できます。出力は次のようになります

```
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#
```

- コマンドを実行すると、これらのノードに対してnms configuration-db diagnosticsを要求します。出力は次のようになります。
- 「IsLeader」の強調表示されたフィールドを探します。 1に設定されている場合、ノードがリーダーノードであることを示し、そこからconfiguration-dbバックアップを収集できます。

```
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     .
```

このコマンドを使用して、特定されたconfiguration-dbリーダーのvManageノードから configuration-dbのバックアップを収集します。

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

予想される出力は次のとおりです。

```
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#
```

- configuration-dbクレデンシャルが更新されている場合は、それをメモします。
- configuration-dbクレデンシャルを知らない場合は、TACに問い合わせて、既存のvManageノードからconfiguration-dbクレデンシャルを取得してください。
- デフォルトのconfiguration-dbクレデンシャルは、ユーザ名：neo4jおよびパスワード：passwordです。

構成データベースのバックアップを別のvManageノードに復元

SCPを使用して、vManageの/home/admin/ディレクトリにconfiguration-dbバックアップをコピーします。

scpコマンドの出力例：

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

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

configuration-dbのバックアップを復元するには、まずconfiguration-dbのクレデンシャルを設定する必要があります。configuration-dbクレデンシャルがデフォルト(neo4j/password)の場合は、このステップを省略できます。

configuration-dbクレデンシャルを設定するには、コマンドrequest nms configuration-db update-admin-userを使用し、任意のユーザ名とパスワードを使用します。

vManageのアプリケーションサーバが再起動します。このため、vManage UIに短時間アクセスできなくなります。

```
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#
```

設定データベースのバックアップの復元に進むことができる投稿：

request nms configuration-db restore path /home/admin/< >コマンドを使用して、新しいvManageに設定データベースを復元できます。

```
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
```

configuration-dbが復元されたら、vManage UIにアクセスできることを確認します。5分ほど待ってから、UIへのアクセスを試みます。

UIに正常にログインしたら、エッジルータのリスト、テンプレート、ポリシー、および以前または既存のvManage UIに存在していた残りのすべての設定が、新しいvManage UIに反映されていることを確認します。

ステップ6：コントローラの再認証と古いコントローラの無効化

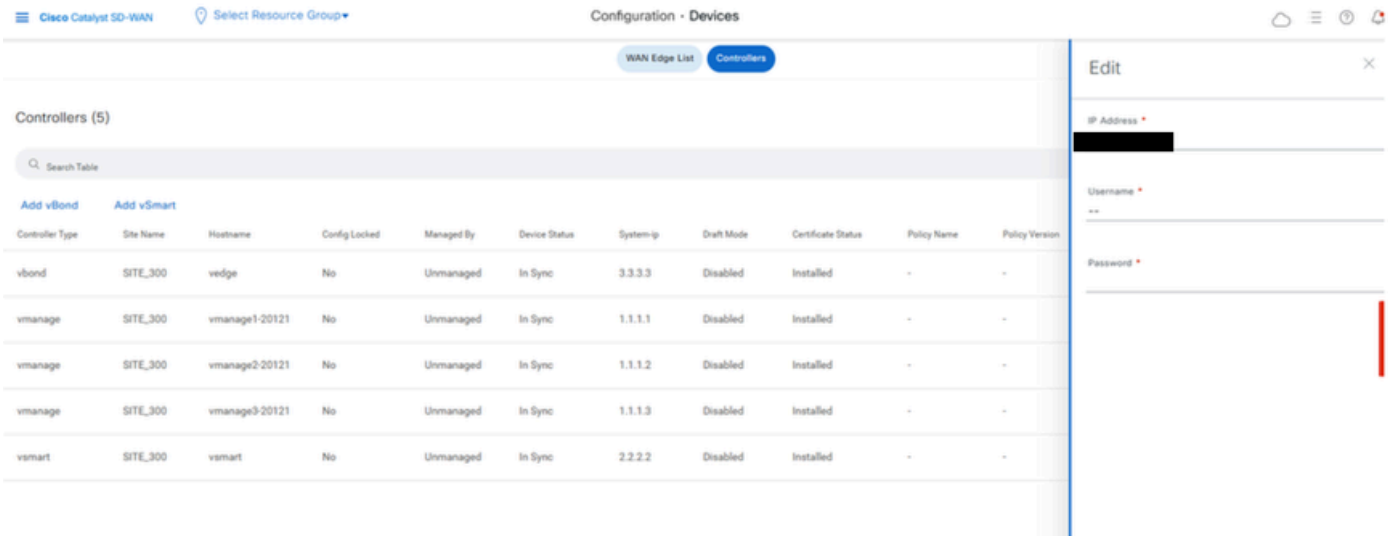
configuration-dbが復元されたら、ファブリック内のすべての新しいコントローラ(vmanage/vsmart/vbond)を再認証する必要があります

注：実際の運用で、再認証に使用されるインターフェイスIPがトンネルインターフェイスIPである場合、vManage、vSmart、およびvBondのトンネルインターフェイスでNETCONFサービスが許可され、パスに沿ったファイアウォールでもNETCONFサービスが許可されるようにする必要があります。開くファイアウォールポートは、DRクラスタからすべてのvBondおよびvSmartsへの双方向ルールとしてTCPポート830です（この例では、DRクラスタはIPアドレスがIPアドレスに一致します）。

---

vmanage UIで、Configuration > Devices > Controllersの順にクリックします。

- 各コントローラの近くにある3つのドットをクリックし、[編集]をクリックします



- ip-address（コントローラのsystem-ip）をtransport vpn 0（トンネルインターフェイス）ip addressに置き換えます。ユーザ名とパスワードを入力して、saveをクリックします
- ファブリック内のすべての新しいコントローラに対して同じ操作を行います

Root-cert-chainの同期

すべてのコントローラがオンボーディングされたら、次の手順を実行します。

新しくアクティブになったクラスタ内の任意のCisco SD-WAN Managerサーバで、次の操作を実行します。

ルート証明書を、新しくアクティブになったクラスタ内のすべてのCisco Catalyst SD-WANデバイスと同期させるには、次のコマンドを入力します。

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

次のコマンドを入力して、Cisco SD-WAN Manager UUIDをCisco SD-WAN Validatorと同期させます。

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

ファブリックが復元され、ファブリック内のすべてのエッジとコントローラに対してコントロールセッションとbfdセッションが確立されたら、古いコントローラ(vmanage/vsmart/vbond)をUIから無効にする必要があります

- vmanage UIで、Configuration > Devices > Certificatesの順にクリックします。
- Controllersをクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。[無効]をクリックします
- vbondに送信をクリックします。
- vmanage UIで、Configuration > Devices > Controllersの順にクリックします。

- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。Deleteをクリックします

ステップ7:Postチェック

注：すべての導入の組み合わせに共通する、ここに示す導入後のチェックセクションを続行します。

組み合わせ5:vManageクラスタ+ DR有効

必要なインスタンス

- 3または6 vManage（プライマリクラスタ）
- 3または6 vManage（DRスタンバイクラスタ）
- 1つ以上のvBond（プライマリデータセンターとDRデータセンターに分散）
- 1つ以上のvSmart（プライマリデータセンターとDRデータセンターに分散）

手順：

1. 共通ステップを使用してすべてのインスタンスを起動する
2. 事前チェック
3. vManage UI、証明書、およびオンボードコントローラの設定
4. vManageクラスタの構築
5. コールドスタンバイDRクラスタセットアップ
6. Config-dbバックアップ/復元
7. 事後チェック

ステップ1：事前チェック

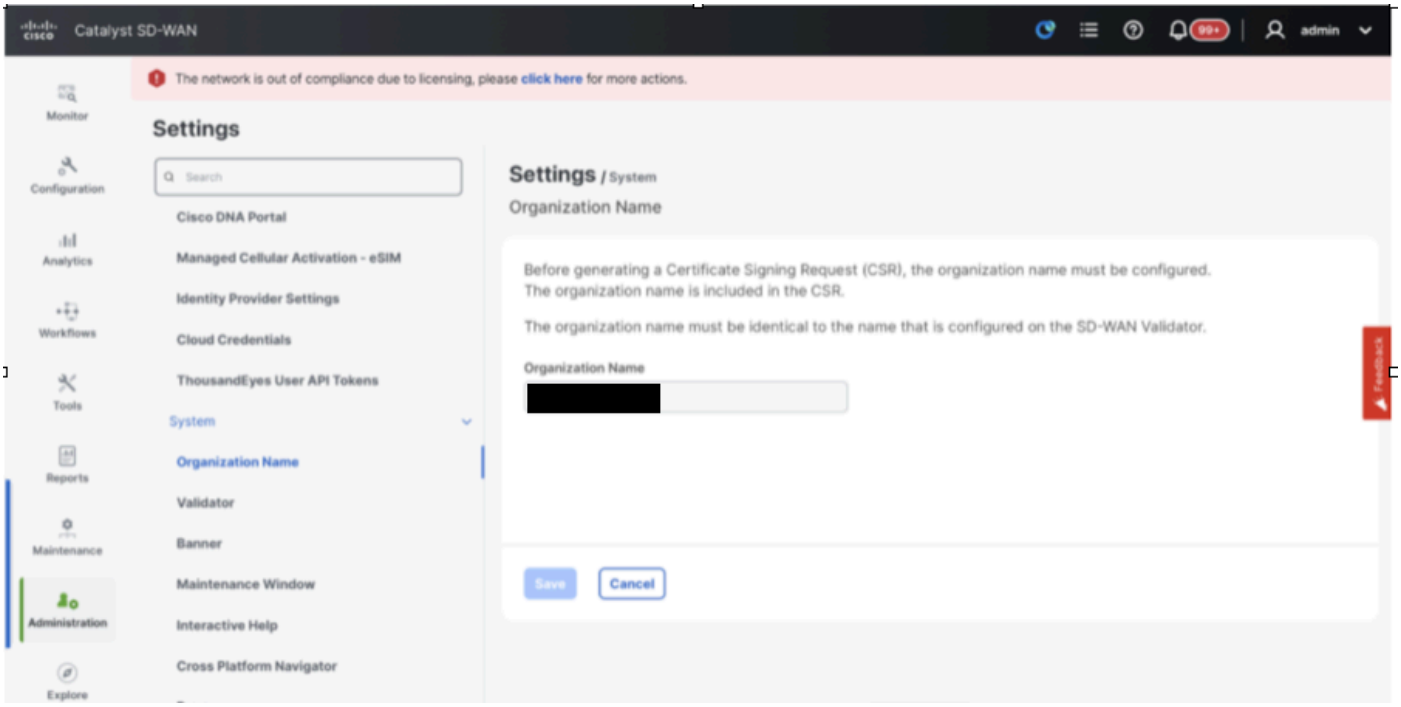
- アクティブなCisco SD-WAN Managerインスタンスの数が、新しくインストールしたCisco SD-WAN Managerインスタンスの数と同じであることを確認します。
- アクティブなCisco SD-WAN Managerインスタンスと新しいCisco SD-WAN Managerインスタンスのソフトウェアバージョンがすべて同じであることを確認します。
- アクティブおよび新規のすべてのCisco SD-WAN Managerインスタンスが、Cisco SD-WAN Validatorの管理IPアドレスに到達できることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスに証明書がインストールされていることを確認します。
- 新しくインストールしたCisco SD-WAN Managerインスタンスを含め、すべてのCisco Catalyst SD-WANデバイスのクロックが同期されていることを確認します。
- 新しくインストールされたCisco SD-WAN Managerインスタンスで、システムIPとサイト

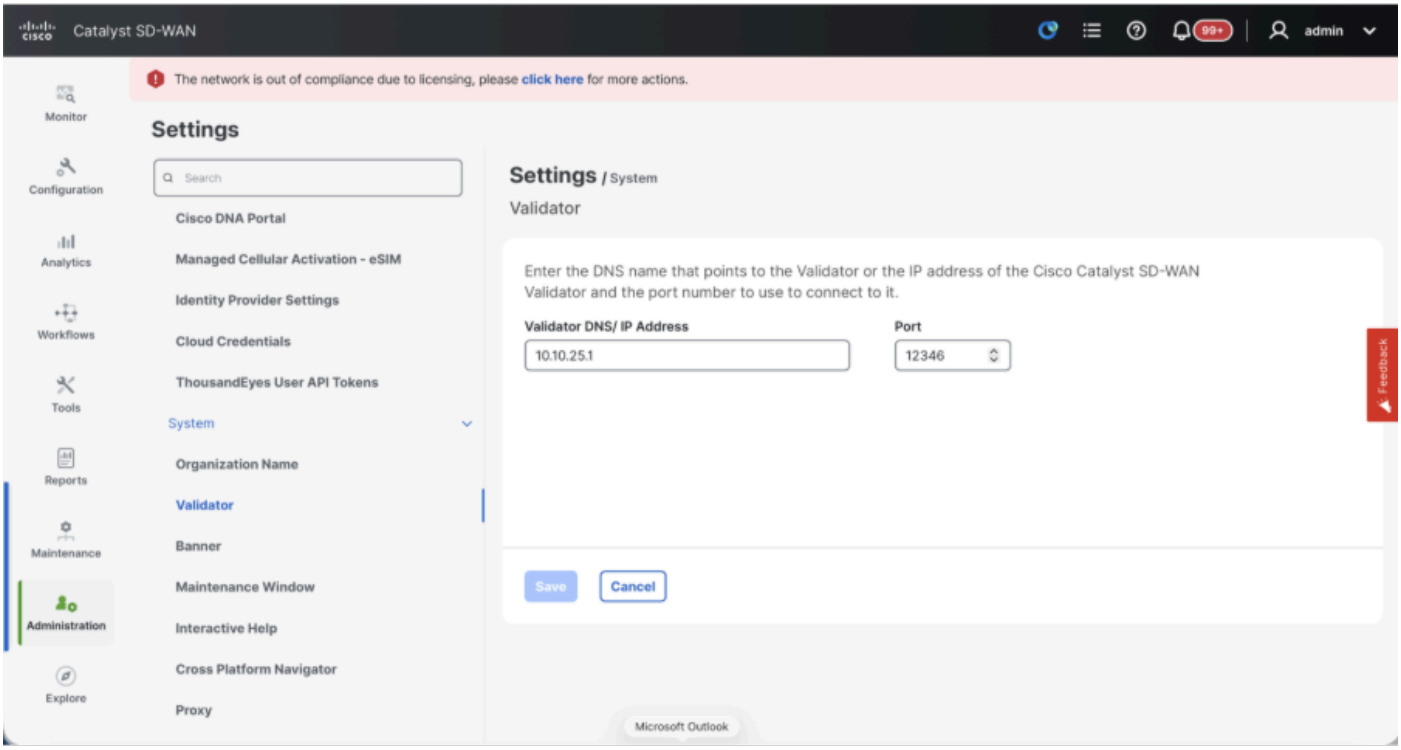
IDの新しいセットが、アクティブクラスタと同じ基本設定とともに設定されていることを確認します。

手順2:vManage UI、証明書、オンボードコントローラを設定します。

vManage UIでの設定の更新

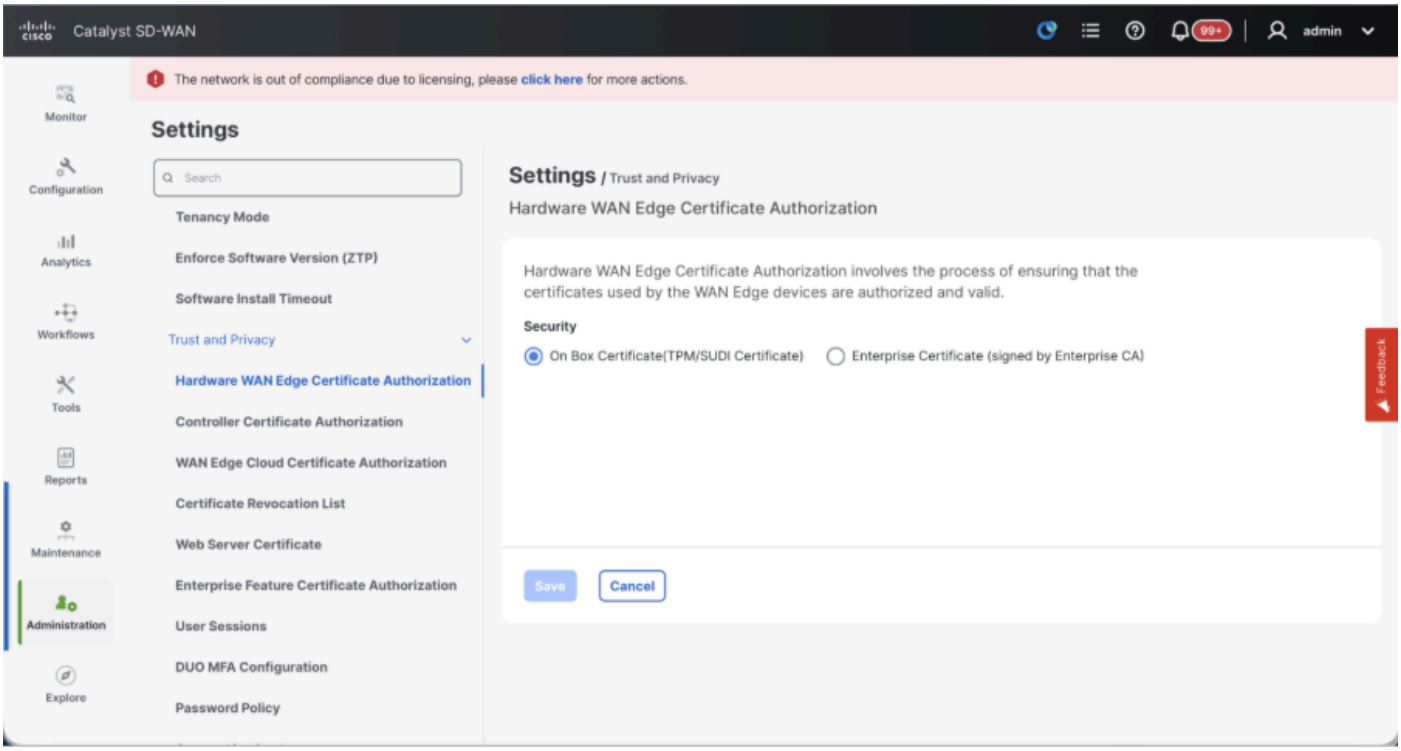
- ステップ1の設定がすべてのコントローラのCLIに追加されたら、ブラウザでURL https://<vmanage-ip>を使用して、vManageのWebUIにアクセスできます。各vManageノードのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- Administration > Settingsの順に移動し、次の手順を実行します。
- 組織名とValidator/vBond URL/IPアドレスを設定します。vManageノードのCLIと同じ値を設定します。
- vManage 20.15/20.18では、これらの設定はシステムのセクションで利用できます。



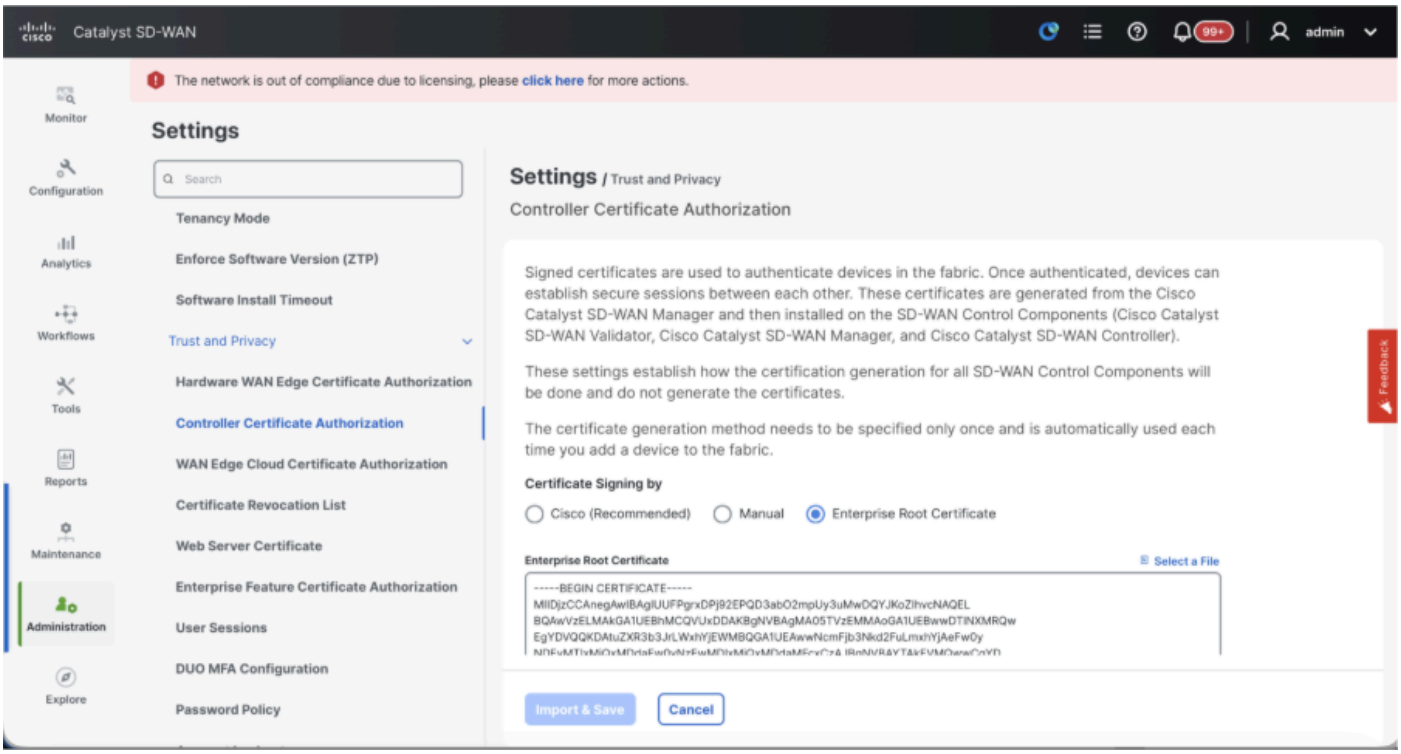


- 証明書の署名に使用する認証局(CA)を決定する証明書承認(CA)の設定を確認します。3つのオプションがあります。

1. ハードウェアWANエッジ証明書認証：ハードウェアSD-WANエッジルータのCAを決定します。
    - オンボックス証明書（TPM/SUDI証明書）– このオプションを使用すると、制御接続（TLS/DTLS接続）を確立するために、ルータハードウェアにプレインストールされている証明書が使用されます
    - エンタープライズ証明書（エンタープライズCAによって署名された）– このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

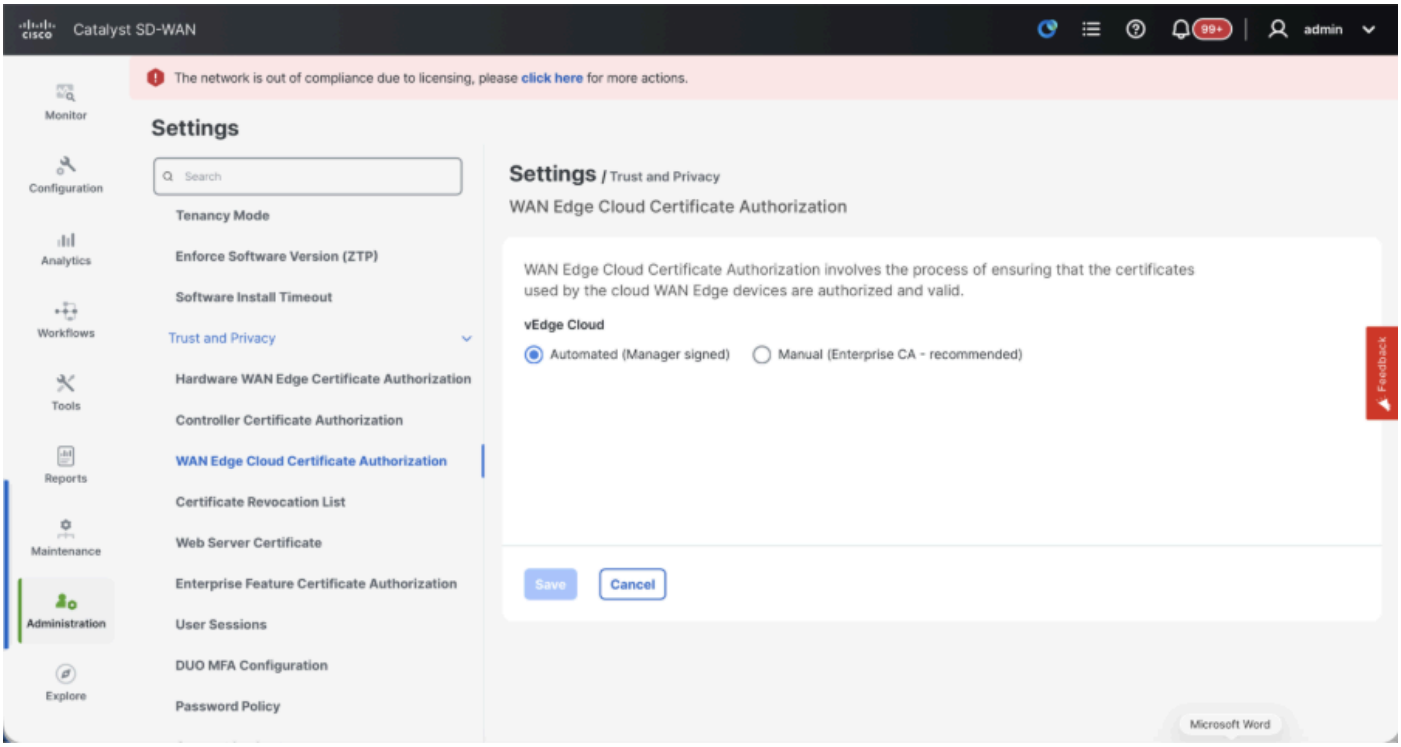


2. Controller Certificate Authorization（コントローラ証明書認証）:SD-WANコントローラのCAを決定します。
    - シスコ（推奨）– コントローラはCisco PKIによって署名された証明書を使用します。vManageは、vManageで設定されたスマートアカウント資格情報を使用してPNPポータルに自動的に接続し、証明書に署名してコントローラにインストールされます。
    - 手動：コントローラはCisco PKIによって署名された証明書を使用します。それぞれのSD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用して手動でCSRに署名します。
    - エンタープライズルート証明書：このオプションを使用すると、ルータは組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

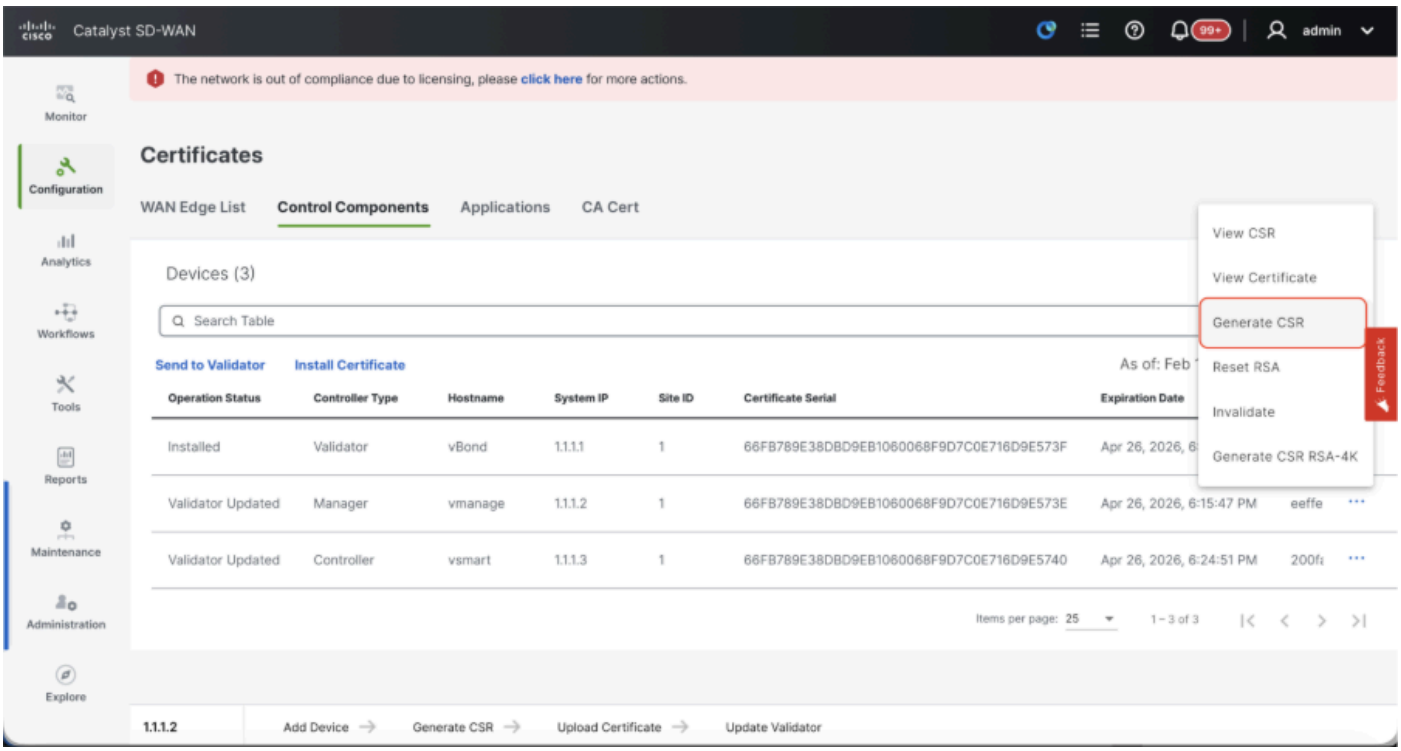


3. WANエッジクラウド証明書認証：仮想SD-WANエッジルータ（CSR1000v、C8000v、vEdgeクラウド）のCAを決定します。
    - 自動（vManage署名済み）:vManageは、仮想エッジルータのCSRに自動的に署名し、証明書をルータにインストールします。
    - 手動（エンタープライズCA – 推奨）– 仮想ルータは、組織のエンタープライズ認証局によって署名された証明書を使用します。このオプションを選択する際には、エンタープライズCAのルート証明書をここで更新する必要があります。

独自のCA（エンタープライズ認証局）を使用している場合は、Enterpriseを選択します。



- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers
- Manager/vManageの「。..」をクリックし、「CSRの生成」をクリックします。



- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。

vBond/ValidatorおよびvSmart/ControllerのvManageへのオンボーディング

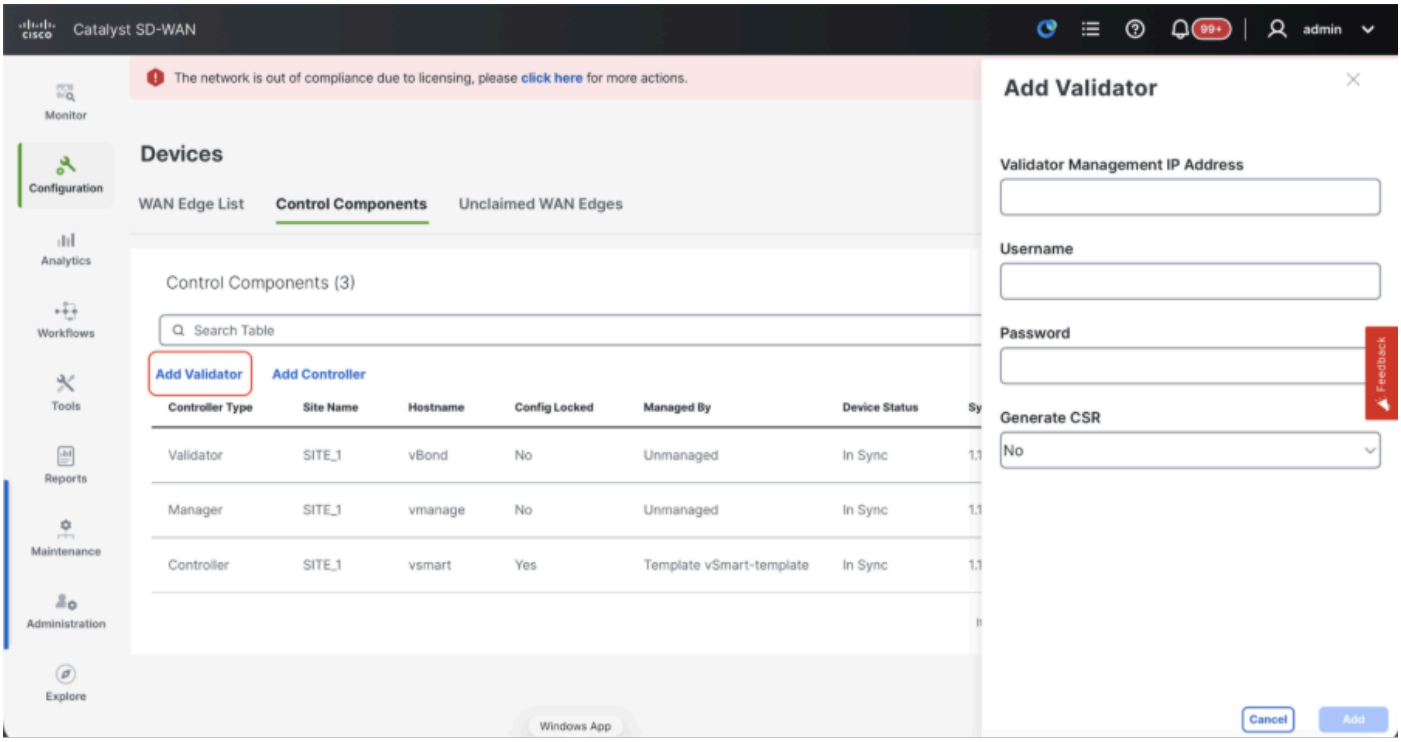
20.15/20.18 vManageノードの場合は、Configuration > Devices > Control Componentsの順に移動します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

オンボーディングvBond/バリデータ

- onAddvBondをクリックします20.12vManagerの場合バリデータの追加20.15/20.18vManageの場合。ポップアップが表示されたら、 VPN 0は、vManageから到達可能なvBondのIPを転送します。
- vManagetovBondIPのCLIからpingを使用して（許可されている場合）到達可能性を確認します。
- vBondのユーザクレデンシャルを入力します。

注:NetAdminグループのユーザ部分であるvBondorの管理者クレデンシャルを使用する必要があります。これはthevBondのCLIで確認できます。vBondの新しい証明書をインストールする必要がある場合は、「CSRの生成」のドロップダウンでYesを選択します

注:vBondがNATデバイス/ファイアウォールの背後にある場合は、vBond VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認してください。VPN 0インターフェイスIPにvManageから到達できない場合は、このステップでVPN 0インターフェイスのパブリックIPアドレスを使用します

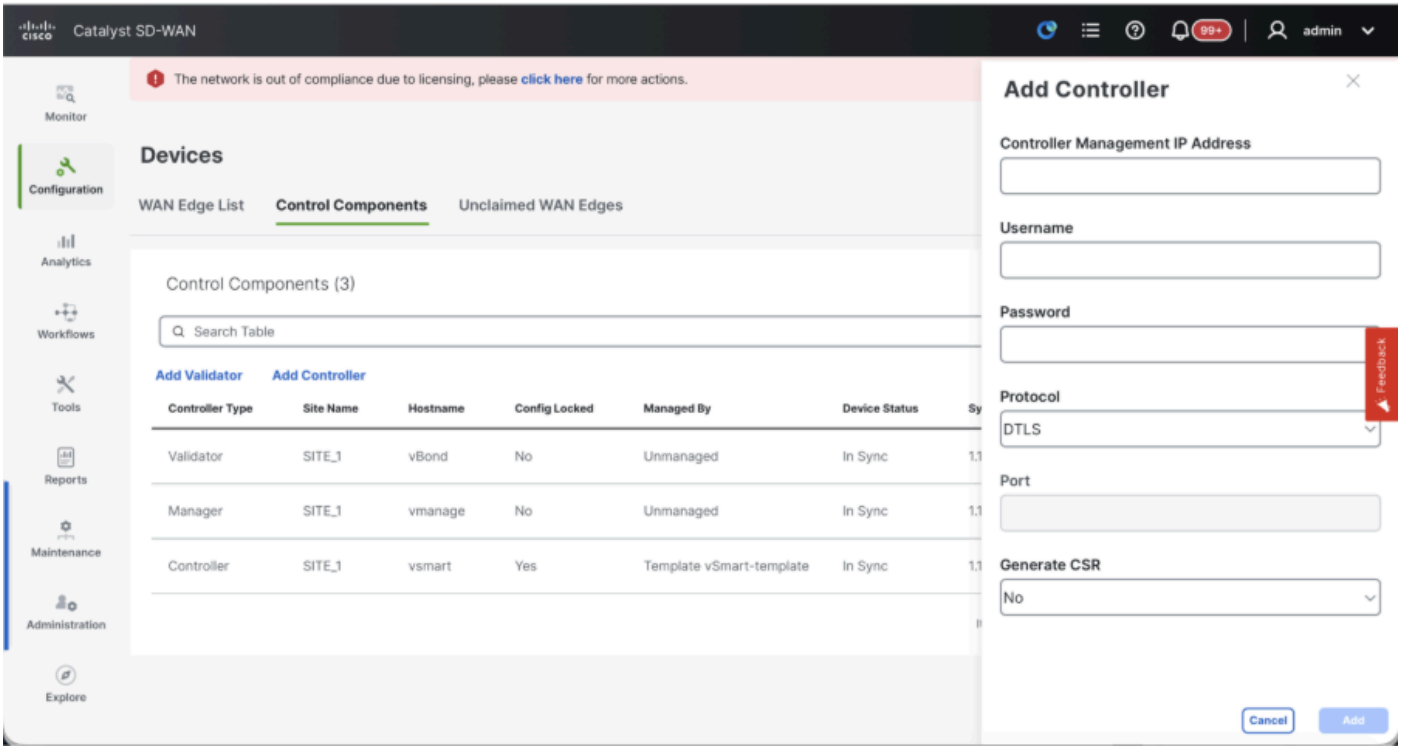


- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vBondに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvBondがある場合は、同じ手順を繰り返します。

vSmart/コントローラのオンボーディング：

- 20.12 vManageの場合はAdd vSmartを、20.15/20.18 vManageの場合はAdd Controllerをクリックします。
- ポップアップが開いたら、vManageから到達可能なvSmartのVPN 0トランスポートIPを入力します。
- vManageのCLIからvSmart IPにpingを使用して（許可されている場合）到達可能性を確認します。
- vSmartの管理者クレデンシャルまたはnetadminグループのユーザ部分を使用する必要があるvSmart Noteのユーザクレデンシャルを入力します。
- これは、vSmartのCLIで確認できます。
- ルータにTLSを使用してvSmartとの制御接続を確立する場合は、プロトコルをTLSに設定します。 この構成は、vSmartsおよびvManageノードのCLIでも構成する必要があります。
- vSmartの新しい証明書をインストールする必要がある場合は、「Generate CSR」のドロップダウンで「Yes」を選択します。

注：vSmartがNATデバイス/ファイアウォールの背後にある場合は、vSmart VPN 0インターフェイスIPがパブリックIPに変換されているかどうかを確認し、VPN 0インターフェイスIPがvManageから到達できない場合は、この手順でVPN 0インターフェイスIPのパブリックIPアドレスを使用します。



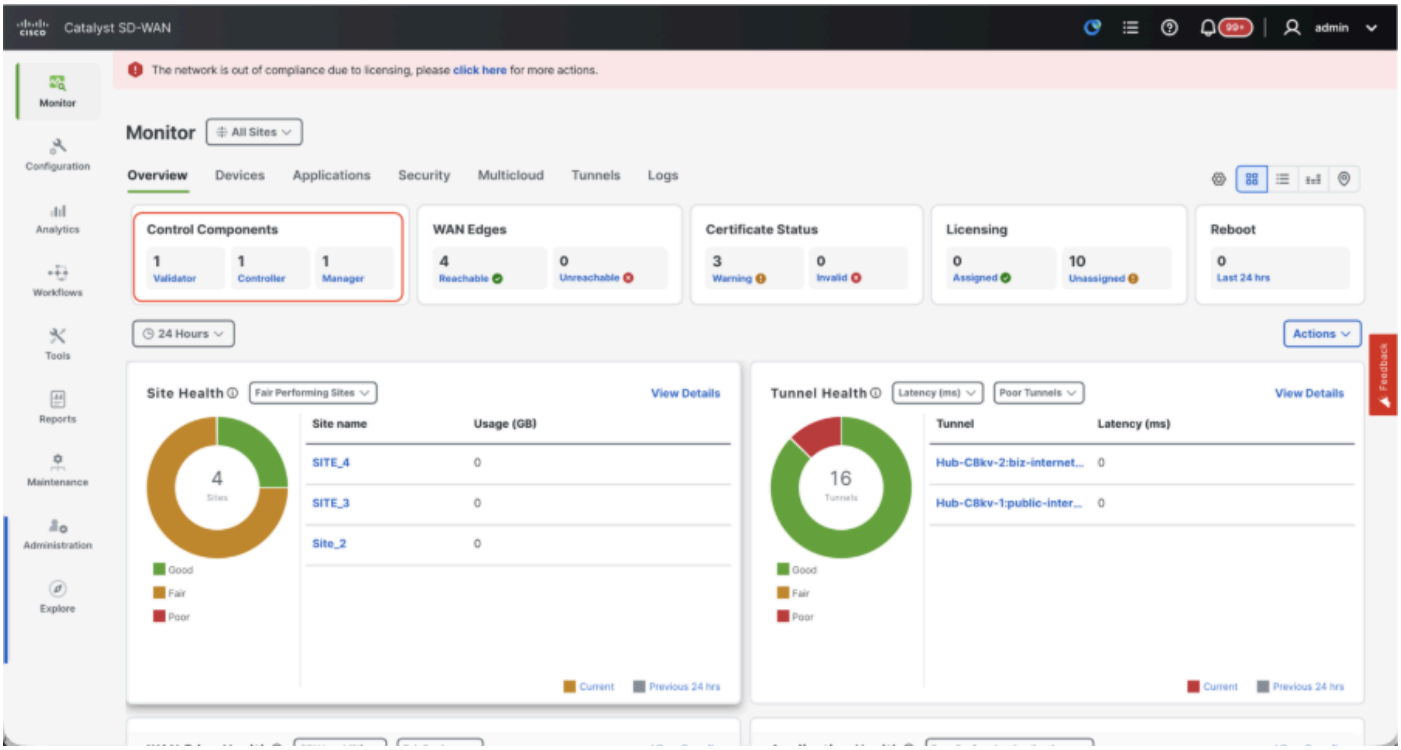
- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate

Authorizationで確認できます。シスコ（推奨）を選択すると、vManageによってCSRがPNPポータルに自動的にアップロードされ、証明書が署名されると、vSmartに自動的にインストールされます。

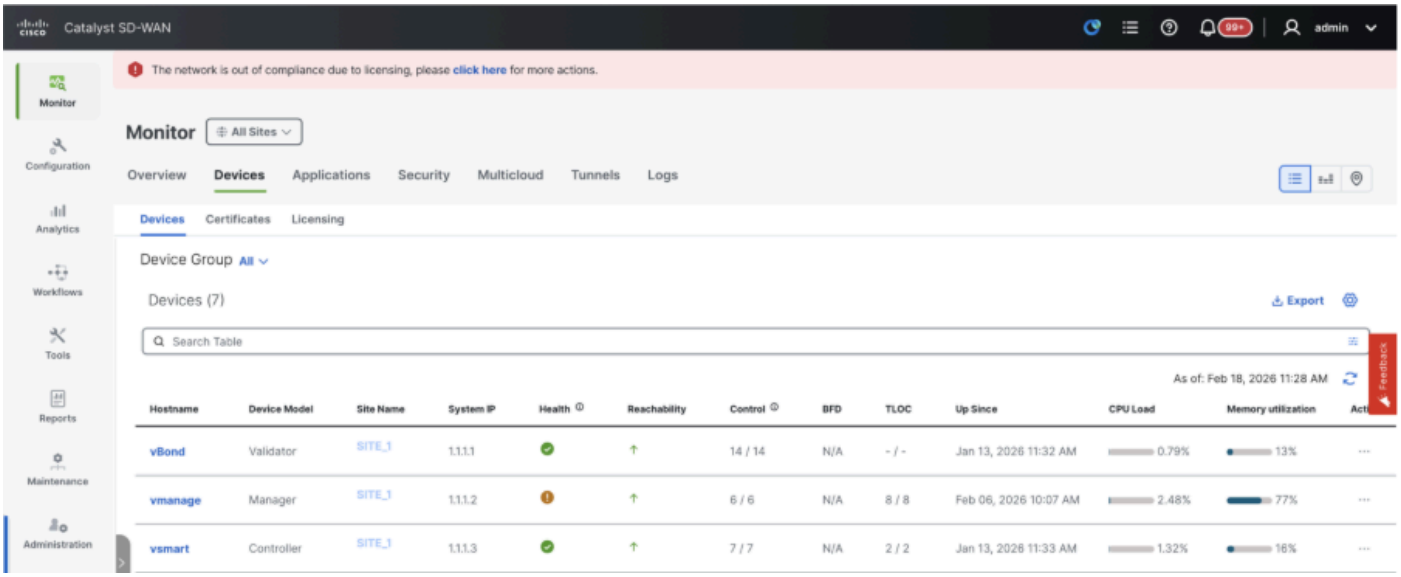
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- 複数のvSmartsがある場合は、同じ手順を繰り返します。

検証

すべての手順が完了したら、Monitor>Dashboardですべての制御コンポーネントに到達できることを確認します



- それぞれの制御コンポーネントをクリックして、それらがすべて到達可能であることを確認します。
- Monitor > Devicesの順に移動し、すべての制御コンポーネントが到達可能であることを確認します。



ステップ3:vManageクラスタの構築

SD-WANオーバーレイでvManageクラスタを使用したオンボードSD-WANファブリック

注:vManageクラスタは、SD-WANファブリックにオンボーディングされたサイトの数に応じて、3つのvManageノードまたは6つのvManageノードで構成できます

1つのvManageノードですべてのSD-WANコントローラをオンボード

「SD-WANオーバーレイでの単一ノードvManageによるSD-WANコントローラのオンボード」で共有されている手順に進み、まず1つのvManageノードでSD-WANファブリックを起動し、必要なすべてのバリデータ(vBond)とコントローラ(vSmart)をオンボードします。

クラスタに含まれるすべてのvManageノードのCLI設定を構成します

- 残りのvManageノードを設定します。 3ノードクラスタの場合は、残りの2ノードを構成します。6ノードクラスタの場合は、5ノードを構成します。
- 次に示すように、システム設定を行います。

```
config t
system
 host-name



 system-ip
```

```
 site-id


 organization-name


 vbond


commit
```

注:vBondアドレスとしてURLを使用している場合は、DNSサーバのIPアドレスをVPN 0設定で設定するか、解決できることを確認してください。

これらの設定は、ルータおよびその他のコントローラとの制御接続の確立に使用されるトランスポートインターフェイスを有効にするために必要です。

```
config t
vpn 0
 dns


        primary
 dns


         secondary
 interface eth1
  ip address


  tunnel-interface
```

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



commit
```

また、コントローラへのアウトオブバンド管理アクセスを有効にするためにVPN 512managementインターフェイスも設定します。

```
Conf t
vpn 512
 interface eth0
  ip address



  no shutdown
 !
 ip route 0.0.0.0/0



!
Commit
```

オプションの構成：

- 既存のコントローラの設定を参照できます。ここにリストされている設定が存在する場合は、新しいコントローラにこの設定を追加できます。
- ルータがTLSを使用してvManageノードとのセキュアな制御接続を確立する必要がある場合にのみ、制御プロトコルをTLSとして設定します。デフォルトでは、すべてのコントローラとルータがDTLSを使用して制御接続を確立します。これは、要件に応じてvSmartおよびvManageノードでのみ必要なオプションの設定です。

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

すべてのvManageノードでサービスインターフェイスを設定する

すでにオンボーディングされているvManage-1を含むすべてのvManagenodesでサービスインターフェイスを設定します。このインターフェイスは、クラスタ通信に使用されます。つまり、クラスタ内のvManagerノード間の通信です。

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

同じIPサブネットがvManageclusterのすべてのノードでサービスインターフェイスに使用されていることを確認します。

クラスタクレデンシャルの設定

vManagenodesと同じ管理者クレデンシャルを使用して、vManageclusterを設定できます。または、netadmingroupの一部である新しいユーザクレデンシャルを設定できます。新しいユーザクレデンシャルを設定する設定は次のとおりです

```
conf t
system
 aaa
  user
```

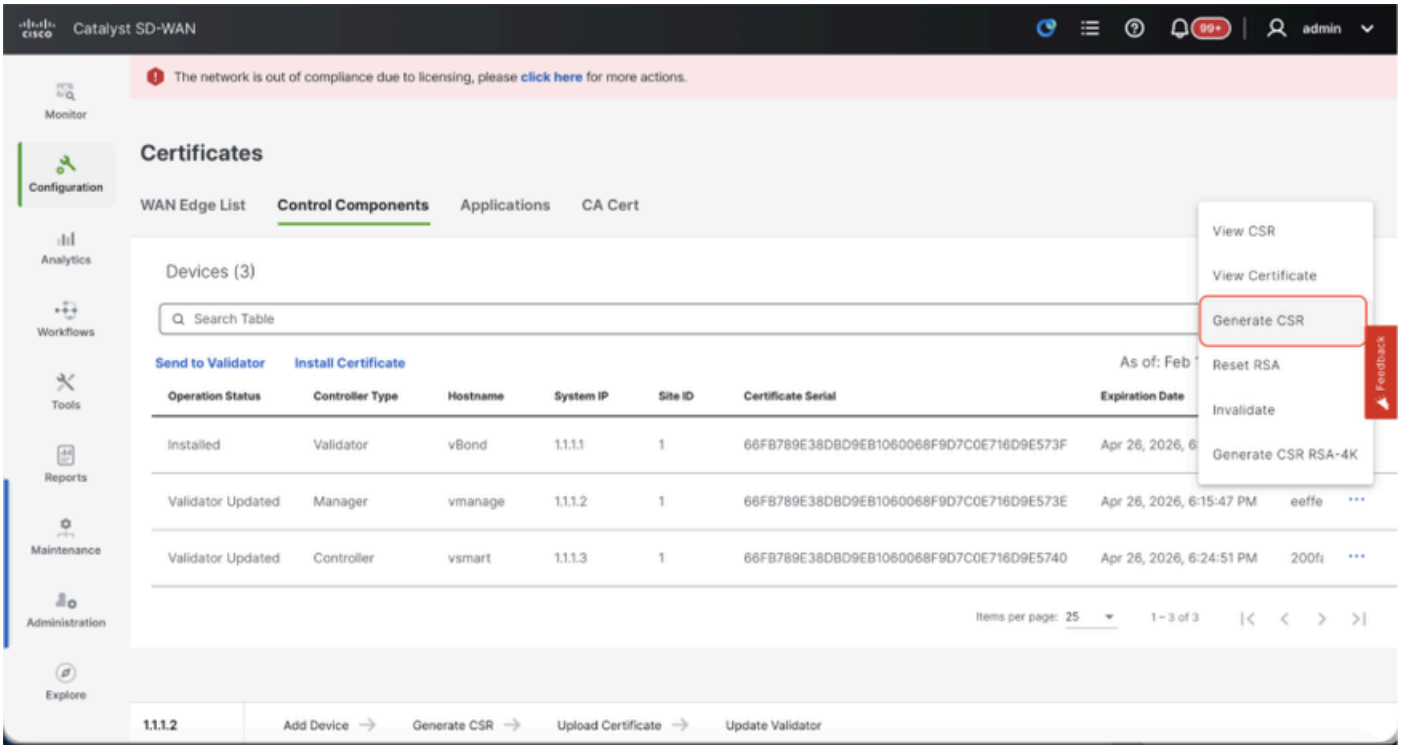
```
   password



   group    netadmin
commit
```

クラスタの一部であるvManagenodes全体で同じユーザクレデンシャルを設定することを確認します。管理者クレデンシャルを使用する場合は、すべてのvManagenodesで同じユーザ名/パスワードを使用する必要があります。

すべてのvManageノードにデバイス証明書をインストール

- ブラウザでURL https://<vmanage-ip>を使用して、すべてのvManagenodesのvManageUIにログインします。それぞれのvManagenodesのVPN 512 IPアドレスを使用します。adminユーザ名とパスワードを使用してログインできます。
- 20.15/20.18 vManageノードの場合は、Configuration > Certificates > Control Componentsの順に選択します。20.9/20.12バージョンの場合、Configuration > Devices > Controllers

  Manager/vManageで…をクリックし、Generate CSRをクリックします。



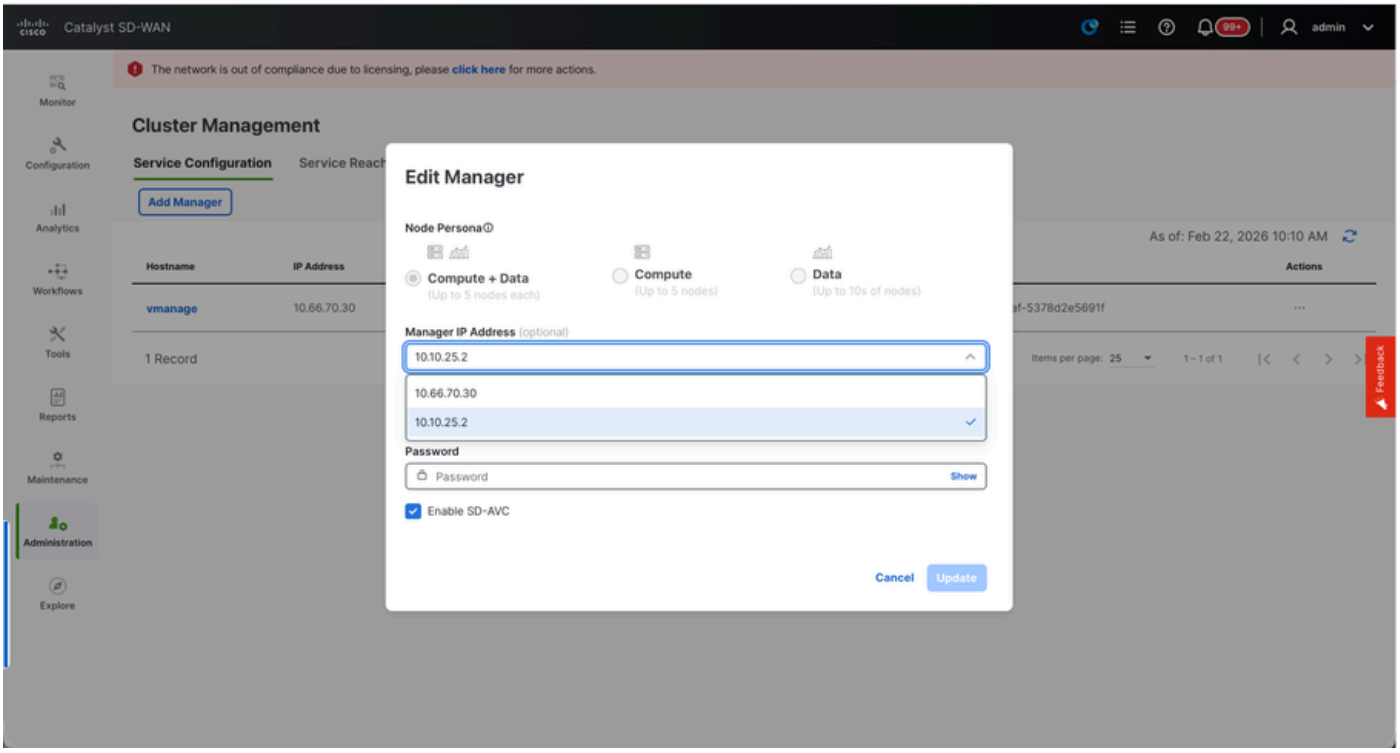
- CSRが生成されると、コントローラ用に選択された認証局に基づいて、CSRをダウンロードして署名を取得できます。この設定は、Administration > Settings > Controller Certificate Authorizationで確認できます。シスコ（推奨）を選択すると、CSRはvManageによってPNPポータルに自動的にアップロードされ、証明書が署名されると、vManageに自動的にインストールされます。
- Manualを選択した場合は、各SD-WANオーバーレイのスマートアカウントと仮想アカウントに移動し、Cisco PNPポータルを使用してCSRに手動で署名します。
- PNPポータルから証明書が利用できるようになったら、vManageの同じセクションでinstall certificateをクリックし、証明書をアップロードしてインストールします。
- Digicertおよびエンタープライズルート証明書を使用している場合も、同じ手順が適用されます。
- クラスタに含まれるすべてのvManageノードに対してこの手順を実行します。

vManageクラスタの構築の準備

- vManage-1のWebUIで、[管理] > [クラスタ管理] に移動し、[vManage-1のアクション]の下の[...]をクリックし、[編集]を選択します。
- ノードのペルソナは、VMのスピンアップ時に選択したペルソナに基づいて自動的に選択されます。

注:3ノードクラスタの場合、3つのvManageノードはすべて、ペルソナとしてcompute+dataを使用して起動されます。6ノードクラスタの場合、3つのvManageノードはpersonaとしてcompute+dataを使用して起動され、3つのvManageノードはpersonaとしてdataを使用して起動されます。

- Manager IP addressのドロップダウンから、vManageのservice interface IPを選択します。



- vManageクラスタ（クラスタクレデンシャルと呼ばれます）を有効にするために使用するユーザ名とパスワードを入力します。
- 前述のように、すべてのvManageノードで同じクレデンシャルを設定し、すべてのノードをクラスタに追加する際に同じクレデンシャルを使用する必要があります。

オプションの構成：

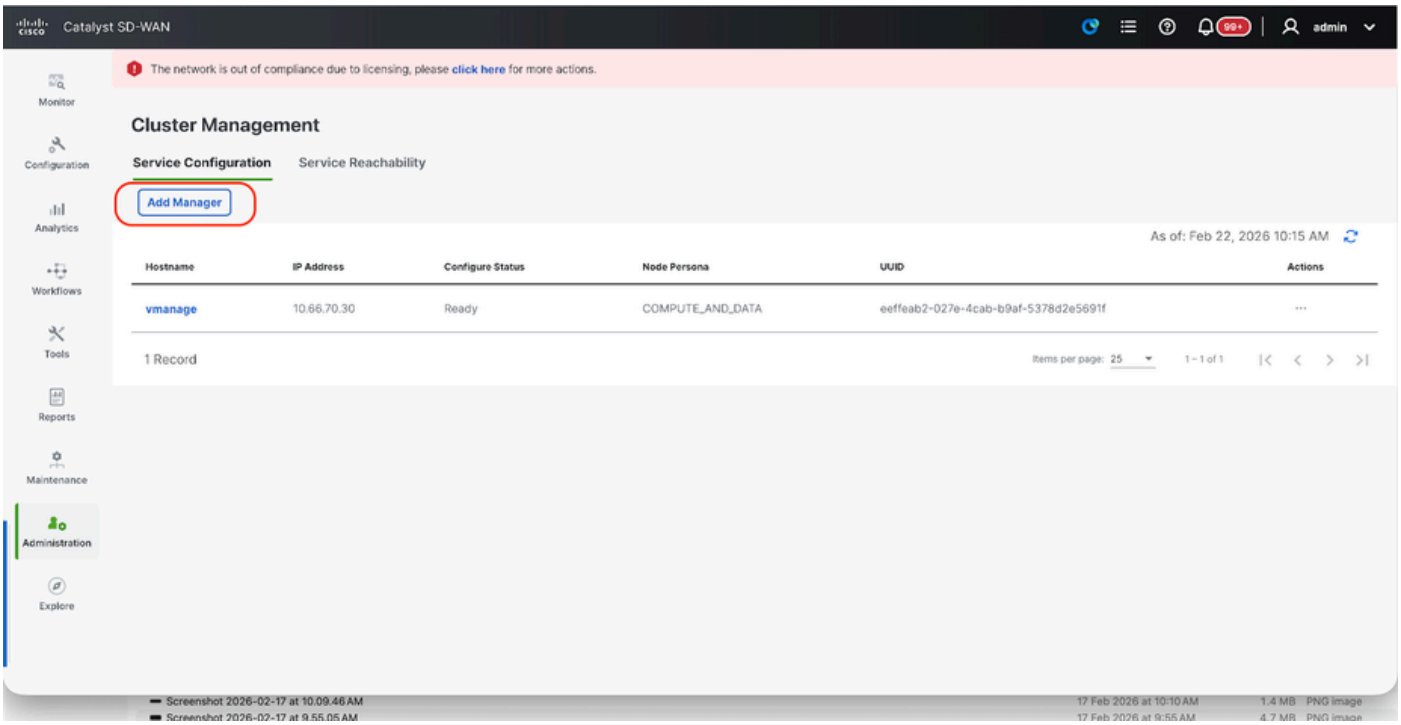
SDAVCを有効にするには、既存のクラスタでこの設定を参照してください。この設定は、必要な場合、およびクラスタの1つのvManageノードでのみ必要な場合にのみ確認してください。

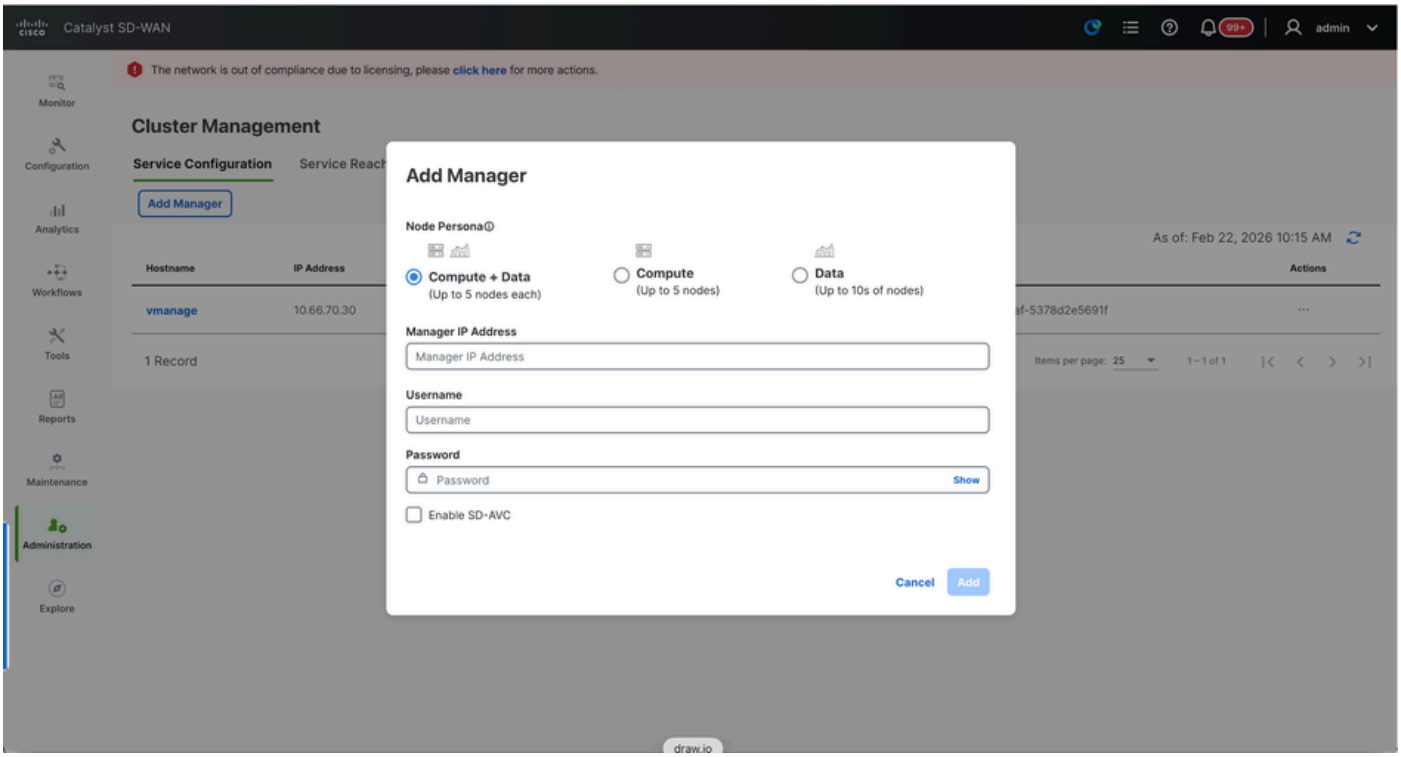
Updateをクリックします。

- この後、vManage NMSサービスがバックグラウンドで再起動し、UIは約5 ~ 10分間使用できません。この間、vManageのCLIアクセスが可能になります。
- vManage-1 UIにアクセスしたら、Administration > Cluster Managementに移動し、vManageのサービスインターフェイスIPがIP addressの下に反映されていることを確認します。設定ステータスはReadyで、ノードのペルソナが正しく反映されています。同じページのサービス到達可能性セクションに切り替え、すべてのサービスが到達可能であることを確認します。
- まだ到達できないサービスがある場合は、お待ちください。通常は20 ~ 30分ほどかかります。

vManageクラスタの構築

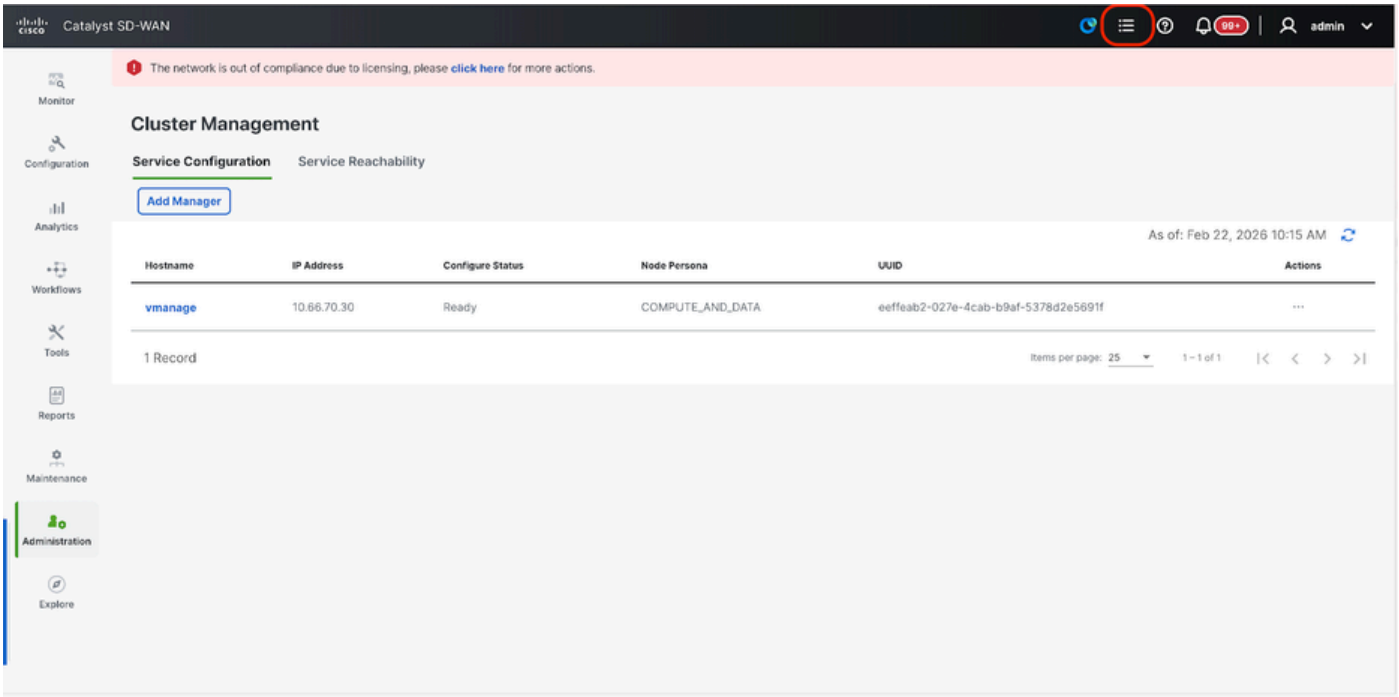
- vManage-1のwebUIで、「Service Configuration,
- Add Managerをクリックすると、ポップアップウィンドウが表示されます。





- vManage - 2ノードがスピンアップした際に行ったペルソナ設定に基づいて、ノードのペルソナを選択します。
- Manager IP addressの下に、service interface IP of vManage-2を入力します
- ユーザ名とパスワードを入力します。これは、ステップ6で使用したクレデンシャルと同じです。
- SDAVCを有効にする：vManage-1ですでに有効にしているので、オフのままにします。
- [Add] をクリックします。
- この後、vManage NMSサービスがvManage 1および2ノードのバックグラウンドで再起動します。vManage 1および2では、UIは数分（約5 ～ 10分）使用できません。
- この間、vManage 1および2のCLIアクセスが使用できます。

- vManage-1 UIにアクセスできたら、Administration > Cluster Managementに移動し、両方のvManageのサービスインターフェイスIPがIPアドレスの下に反映されていることを確認します。Configure StatusはReady、ノードペルソナは正しく反映されています。
- 同じページのサービス到達可能性セクションに切り替え、両方のvManageノードですべてのサービスが到達可能であることを確認します。
- まだ到達できないサービスがある場合は、お待ちください。通常は5 ~ 10分ほどかかります。
- クラスタ追加プロセスのステータスは、vManage UIの右上隅にあるタスクリストで確認できます。



- [アクティブなタスクの一覧]を検索し、タスクがまだ[アクティブなタスクの一覧]に表示されている場合は、タスクがまだ完了していないことを示します。
- タスクをクリックすると、同じタスクの進捗状況を確認できます。 タスクが[アクティブなタスクの一覧]に表示されていない場合は、[完了]に切り替えて、タスクが正常に完了することを確認します。
- これらのポイントが検証された後にのみ、次の手順に進みます。

クラスタに次のノードを追加する前に、次の点を考慮する必要があります。

これまでにクラスタに追加したvManageノードのすべてのUIで、次の点を確認してください。

- vManage UIのMonitor > Overviewに移動し、vManageノードの数が正しく反映されていること、およびクラスタに追加されたノードの数に応じて到達可能と表示されていることを確認します。

- Administration > Cluster Managementの順に移動し、IP addressの下に両方のvManageのサービスインターフェイスIPが反映されていること、Configure StatusがReadyであること、ノードペルソナが正しく反映されていることを確認します。
- 同じページのサービス到達可能性セクションに切り替え、両方のvManageノードですべてのサービスに到達できることを確認します。

- クラスタにノードが追加されるたびに、クラスタ内のすべてのノードのNMSサービスが再起動されるため、これらのノードのUIがしばらくの間到達不能になります。
- クラスタ内のノードの数によっては、UIがバックアップされ、すべてのサービスが到達可能になるまでに時間がかかる場合があります。
- vManage UIの右上隅にあるTask-list availableでタスクをモニタできます。
- クラスタに追加された各ノードのvManage UIで、すべてのルータ、テンプレート、およびポリシー（vManage-1で使用可能な場合）を確認する必要があります。
- これらの構成がvManage-1にない場合は、vManage-1に追加されたvBondおよびvSmartsと、Organization-name、vBond、Certificate AuthorizationのAdministration > Settings構成が、クラスタに追加された残りのvManageノードに反映されている必要があります。
- 残りのvManageノードに対して同じ手順を繰り返します。

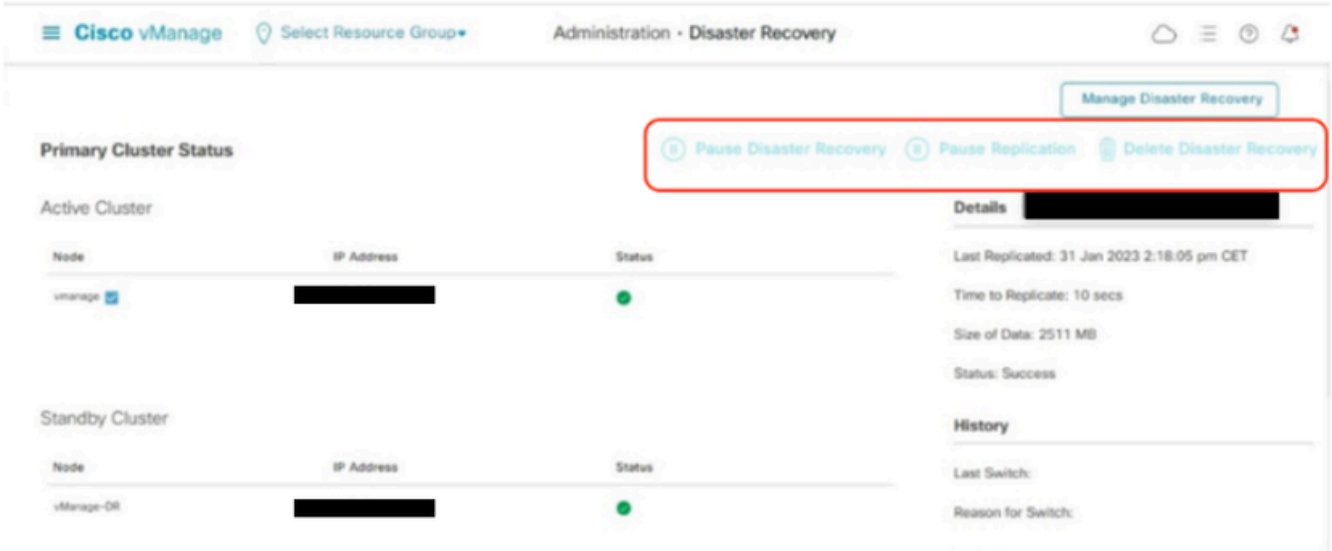
ステップ4:Config-dbのバックアップ/復元

別のvManageノードでのvManage構成データベースのバックアップと復元の収集

注：ディザスタリカバリが有効になっている既存のvManageクラスタから設定データベースバックアップを収集する際には、そのノードのディザスタリカバリが一時停止して削除された後に、バックアップが収集されていることを確認してください。

継続的な災害復旧レプリケーションがないことを確認します。Administration > Disaster Recoveryの順に移動し、 ステータスが「成功」であり、「インポート保留中」、「エクスポート保留中」、「ダウンロード保留中」などの一時的な状態ではないことを確認します。ステータスがsuccessではない場合、ディザスタリカバリを一時停止する前に、Cisco TACに連絡してレプリケーションが成功することを確認します。

まず、ディザスタリカバリを一時停止し、タスクが完了していることを確認します。次に、ディザスタリカバリを削除し、タスクが完了したことを確認します。



ディザスタリカバリが正常にクリーンアップされたことをCisco TACに確認します。

Configuration-DBバックアップの収集：

- 現在使用されているSD-WANファブリックでは、vManageクラスタからconfiguration-dbバックアップを生成できます。
- configuration-dbバックアップは、configuration-dbのリーダーであるvManageクラスタの1つのノードでのみ生成する必要があることに注意してください。

- スタンドアロンvManageの場合、そのvManage自体がconfiguration-dbのリーダーです。
- vManageクラスタで、コマンドrequest nms configuration-db diagnosticsを使用して、configuration-dbリーダーノードを特定します。このコマンドは、3ノードvManageクラスタのすべてのノードで実行できます。
- 6ノードクラスタでは、リーダーノードを識別するためにconfiguration-dbが有効になっているvManageノードで必ずこのコマンドを実行します。 Administration > Cluster Managementの順に移動し、同じことを確認します。
- スクリーンショットに示すように、ペルソナCOMPUTE_AND_DATAで設定されたノードではconfiguration-dbが実行されています。

vManageCLIでコマンドrequestnmsconfiguration-dbstatusを使用して同じ内容を確認できます。出力は次のようになります

```
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#
```

- コマンドを実行すると、これらのノードに対してnms configuration-db diagnosticsを要求します。出力は次のようになります。
- 「IsLeader」の強調表示されたフィールドを探します。 1に設定されている場合、ノードがリーダーノードであることを示し、そこからconfiguration-dbバックアップを収集できます。

```
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     .
```

このコマンドを使用して、特定されたconfiguration-dbリーダーのvManageノードから configuration-dbのバックアップを収集します。

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

予想される出力は次のとおりです。

```
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#
```

- configuration-dbクレデンシャルが更新されている場合は、それをメモします。
- configuration-dbクレデンシャルを知らない場合は、TACに問い合わせて、既存のvManageノードからconfiguration-dbクレデンシャルを取得してください。
- デフォルトのconfiguration-dbクレデンシャルは、ユーザ名：neo4jおよびパスワード：passwordです。

構成データベースのバックアップを別のvManageノードに復元

SCPを使用して、vManageの/home/admin/ディレクトリにconfiguration-dbバックアップをコピーします。

scpコマンドの出力例：

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

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

configuration-dbのバックアップを復元するには、まずconfiguration-dbのクレデンシャルを設定する必要があります。configuration-dbクレデンシャルがデフォルト(neo4j/password)の場合は、このステップを省略できます。

configuration-dbクレデンシャルを設定するには、コマンドrequest nms configuration-db update-admin-userを使用し、任意のユーザ名とパスワードを使用します。

vManageのアプリケーションサーバが再起動します。このため、vManage UIに短時間アクセスできなくなります。

```
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#
```

設定データベースのバックアップの復元に進むことができる投稿：

request nms configuration-db restore path /home/admin/< >コマンドを使用して、新しいvManageに設定データベースを復元できます。

```
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
```

configuration-dbが復元されたら、vManage UIにアクセスできることを確認します。5分ほど待ってから、UIへのアクセスを試みます。

UIに正常にログインしたら、エッジルータのリスト、テンプレート、ポリシー、および以前または既存のvManage UIに存在していた残りのすべての設定が、新しいvManage UIに反映されていることを確認します。

ステップ5:vManageクラスタでディザスタリカバリを有効にする

重要な事前確認

ディザスタリカバリを進めるには、2つの別個のvManage 3ノードクラスタを設定し、動作させる必要があります。アクティブクラスタでは、バリデータとコントローラがオンボーディングされている必要があります。DRサイトにバリデータとコントローラがある場合は、DR vManageクラスタではなく、アクティブクラスタにもオンボーディングする必要があります。

シスコでは、ディザスタリカバリを登録する前に、次の要件を満たしていることを推奨しています。

- トランスポートVPN(VPN 0)上で、プライマリノードとセカンダリノードがHTTPSで到達可能であることを確認します。
- セカンダリ設定のCisco vSmart ControllerおよびCisco vBond Orchestratorsがプライマリ設定に接続されていることを確認します。
- Cisco vManageプライマリノードとセカンダリノードで同じCisco vManageバージョンが実行されていることを確認します。
- VPN 0のアウトオブバンドクラスタインターフェイス（サービスインターフェイス）。
- クラスタ内のvManageインスタンスごとに、VPN 0（トランスポート）およびVPN 512（管理）に使用されるインターフェイスの他に、3番目のインターフェイス（クラスタリンク）が必要です。
- このインターフェイスは、クラスタ内のvManageサーバ間の通信および同期に使用されます。
- このインターフェイスは、1 Gbps以上で、遅延が4 ms以下である必要があります。10 Gbpsインターフェイスを推奨
- 両方のvManageノードは、このインターフェイスを介して相互に到達できる必要があります。このインターフェイスがレイヤ2セグメントであるか、またはレイヤ3ルーティングを介しているかに関係ありません。
- 各vManageで、このインターフェイスをクラスタインターフェイス(GUI)として設定する必要があります(Administration > Cluster Management：独自のアウトオブバンドクラスタインターフェイス(OOB)のIPアドレス、ユーザ、およびパスワードを示します)。
- Cisco vManageノードがデータセンター間で相互に通信できるようにするには、データセンターファイアウォールでTCPポート8443および830を有効にします。
- すべてのサービス（application-server、configuration-db、messaging server、coordination server、およびstatistics-db）が両方のCisco vManageノードで有効になっていることを確認します。
- Cisco vBond Orchestratorを含むすべてのコントローラをプライマリおよびセカンダリデー

タセンターに分散させます。これらのコントローラが、これらのデータセンターに分散しているCisco vManageノードから到達可能であることを確認します。コントローラは、プライマリCisco vManageノードにのみ接続します。

- アクティブ（プライマリ）およびスタンバイ（セカンダリ）のCisco vManageノードで他の操作が実行中でないことを確認します。たとえば、サーバがアップグレード中でないか、またはテンプレートをデバイスに添付していないことを確認します。
- Cisco vManage HTTP/HTTPSプロキシサーバが有効になっている場合は無効にします。「Cisco vManageと外部サーバとの通信に使用するHTTP/HTTPSプロキシサーバ」を参照してください。プロキシサーバを無効にしないと、Cisco vManageは、Cisco vManageアウトオブバンドクラスタIPアドレスが直接到達可能な場合でも、プロキシIPアドレスを使用してディザスタリカバリ通信を確立しようとします。ディザスタリカバリの登録が完了したら、Cisco vManage HTTP/HTTPSプロキシサーバを再度有効にすることができます。
- 障害回復登録プロセスを開始する前に、プライマリCisco vManageノードでTools > Rediscover Networkウィンドウに移動し、Cisco vBond Orchestratorsを再検出します。

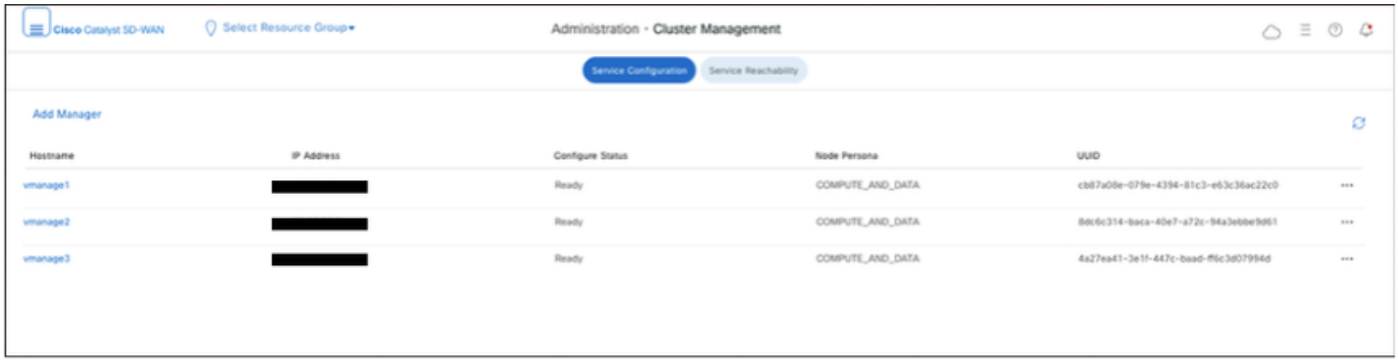
コンフィギュレーション

vManageディザスタリカバリの詳細については、このリンクを参照してください。

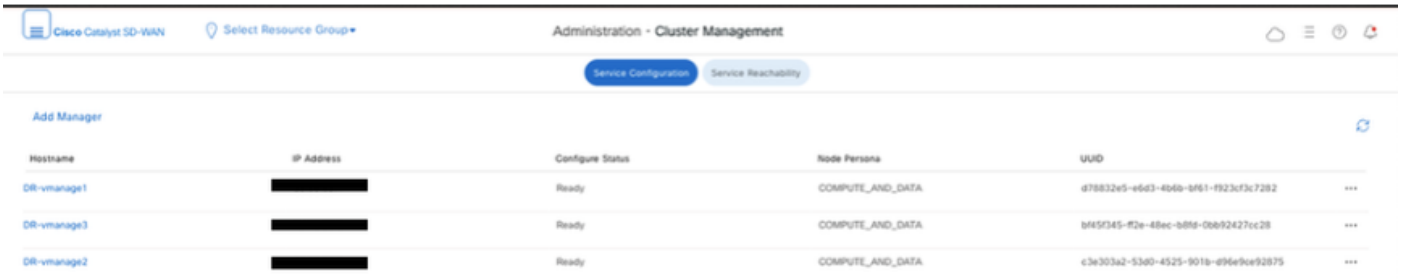
各SD-WANマネージャの設定が最小限で、認証部分が完了していることを前提として、2つの個別の3ノードクラスタがすでに作成されています。

両方のクラスタでAdministration > Cluster Managementの順に移動し、すべてのノードがready状態であることを確認します。

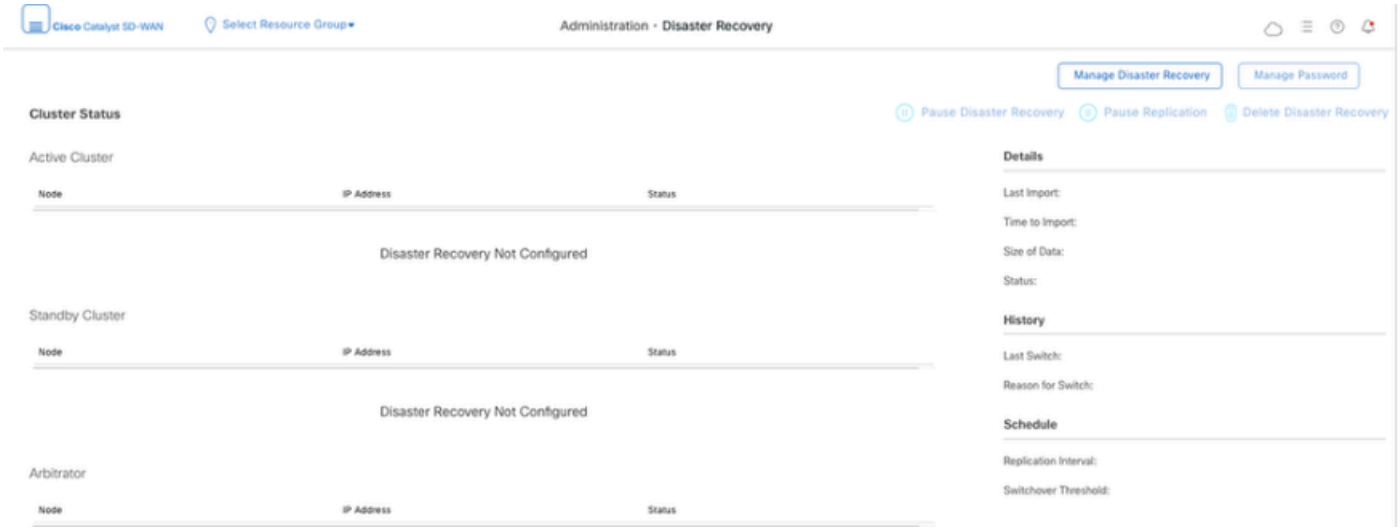
DC vManage



DR vmanage



Administration >Disaster Recovery of Primary vManage Clusterの順に選択します。Manage Disaster Recoveryをクリックします。



ポップアップウィンドウで、プライマリとセカンダリの両方のvManageの詳細を入力します。

示されるIPアドレスは、アウトオブバンドクラスタインターフェイスのIPアドレスです。 各クラスタで、vManage-1のVPN 0サービスインターフェイスのIPアドレスを使用することが望ましい。

クレデンシャルはnetadminユーザのクレデンシャルである必要があり、DRが設定された後は、削除されない限り、クレデンシャルを変更しないでください。 ディザスタリカバリ用に別個のvManageローカルユーザクレデンシャルを使用できます。vManageローカルユーザがnetadminグループの一部であることを確認する必要があります。ここでは、管理者クレデンシャルも使用できます。

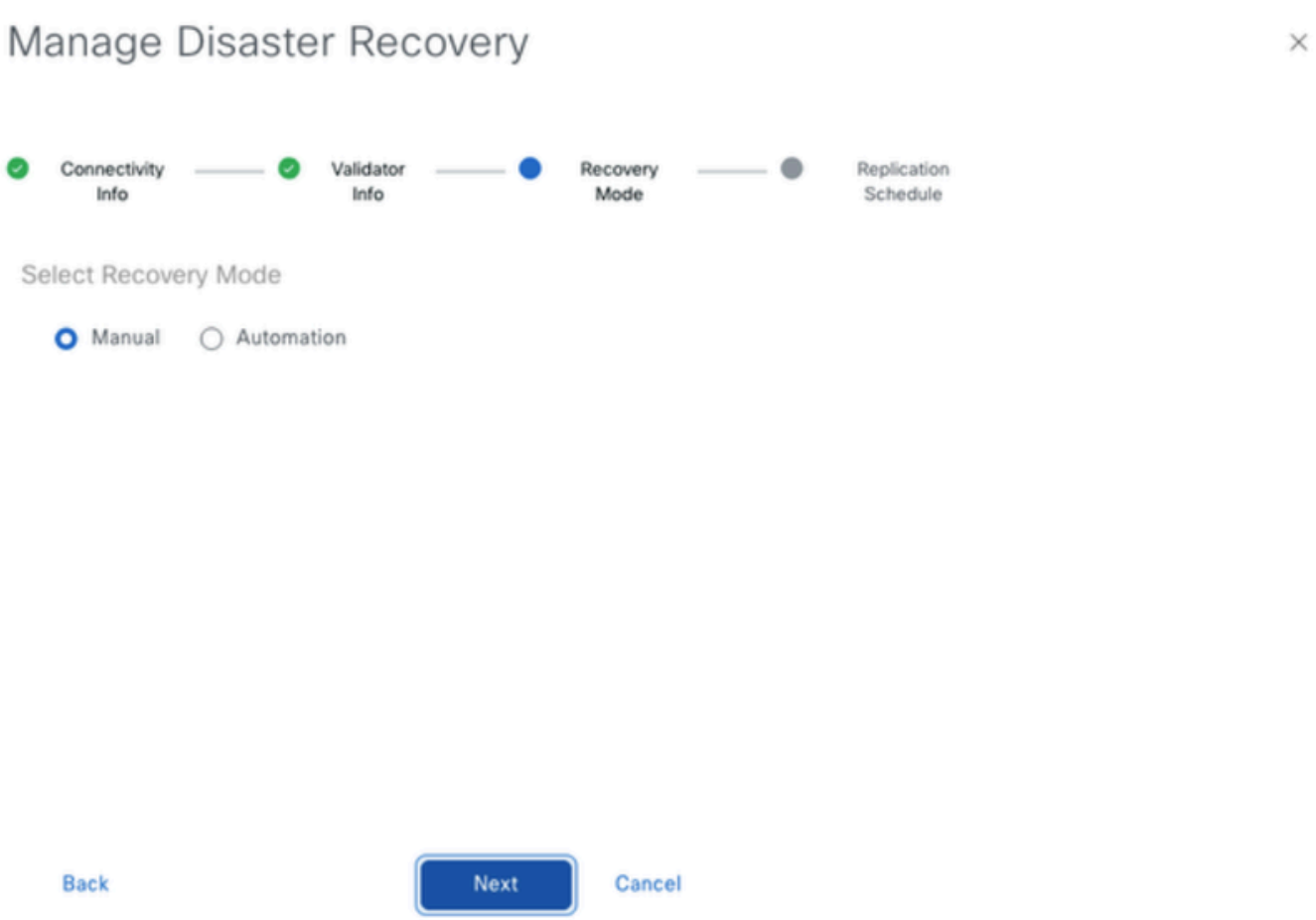
入力が完了したら、Nextをクリックします。

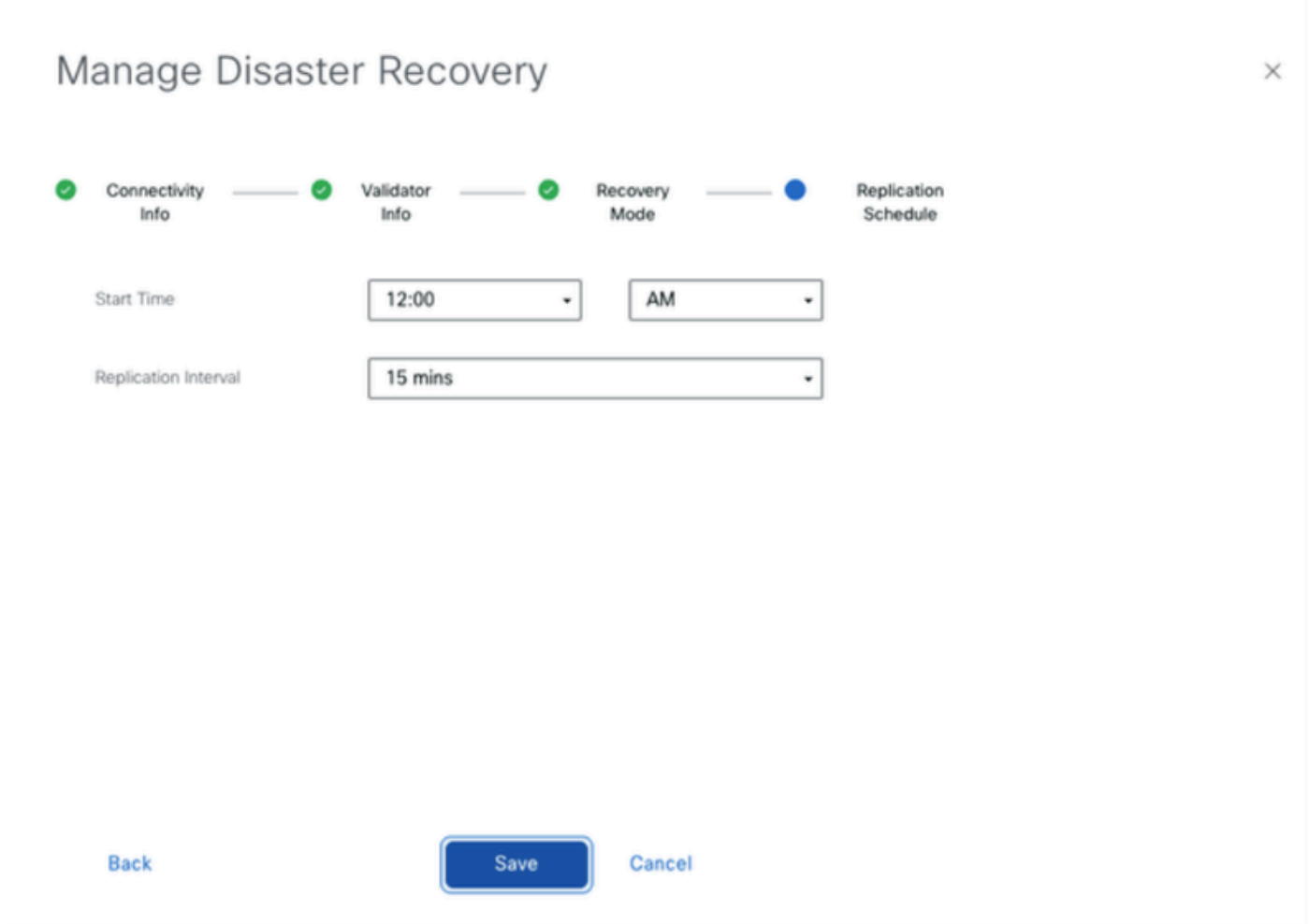
- vBondコントローラの詳細を入力します。

vBondコントローラは、指定されたIPアドレスでNetconfを介して到達可能である必要があります。

入力が完了したら、Nextをクリックします。

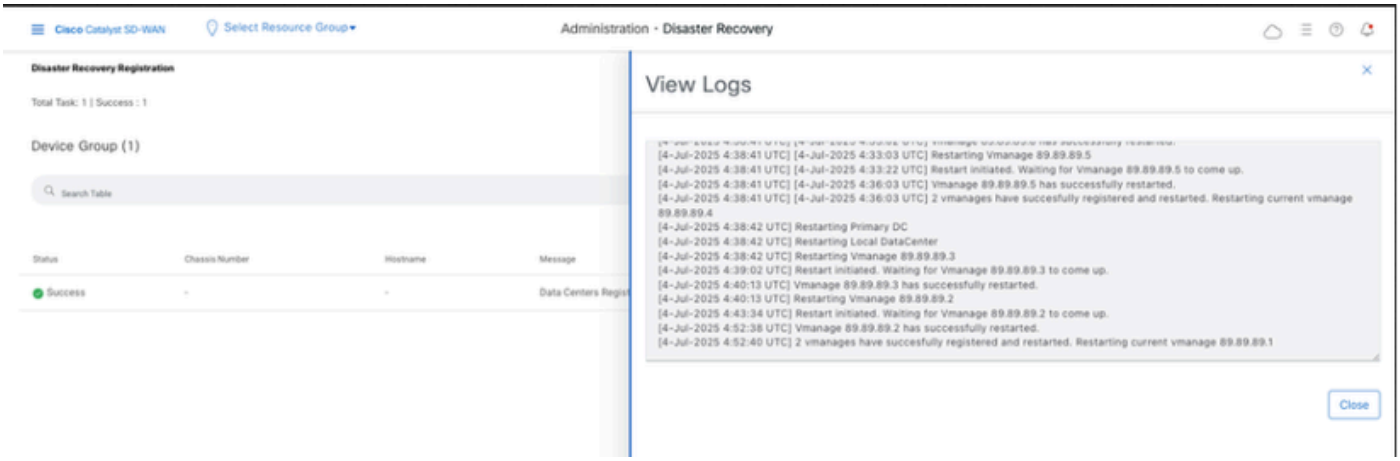
- Recovery ModeでManualを選択します。自動化モードは廃止されました。[Next] をクリックします。


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



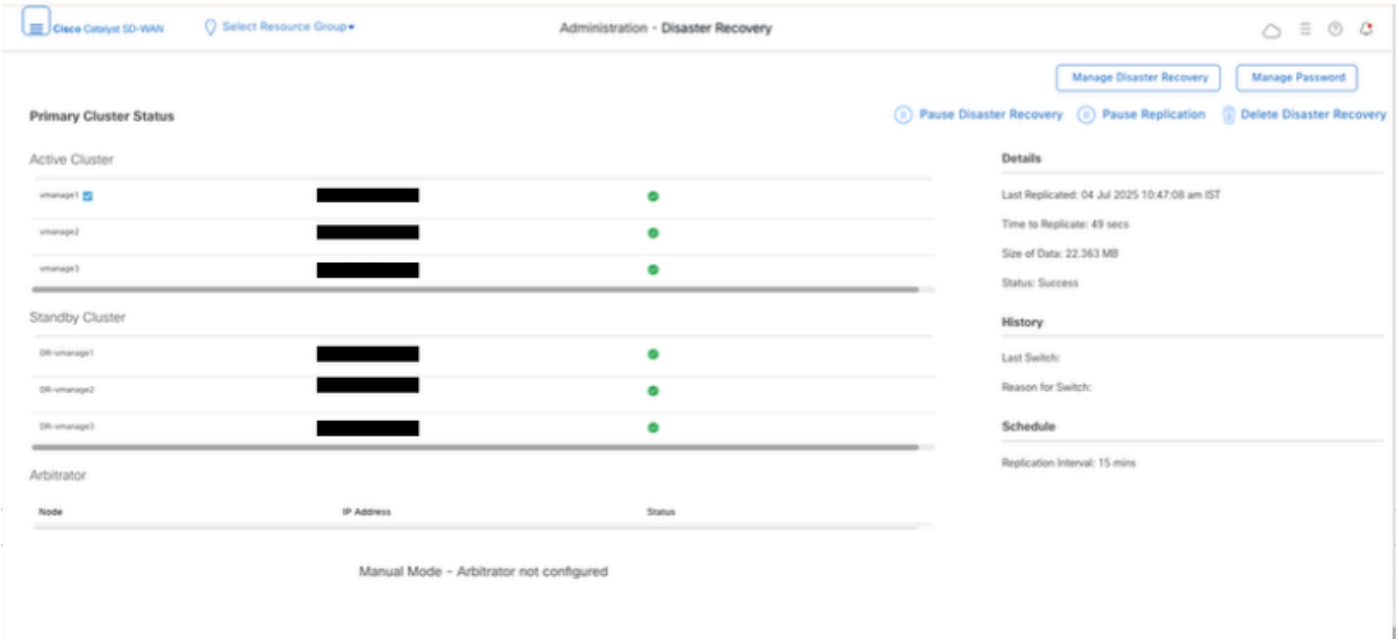
値を設定して、Saveをクリックします。

- DR登録が開始されます。[更新]ボタンをクリックして、状態と進行状況ログを手動で更新します。このプロセスには、最大で20 ~ 30分かかる場合があります。



検証

Administration > Disaster Recoveryの順に移動し、ディザスタリカバリのステータスと、データが最後にいつ複製されたかを確認します。



注：レプリケーションは、データベースのサイズによっては数時間かかる場合があります。また、レプリケーションを正常に実行するには、数回のサイクルが必要になる場合があります。

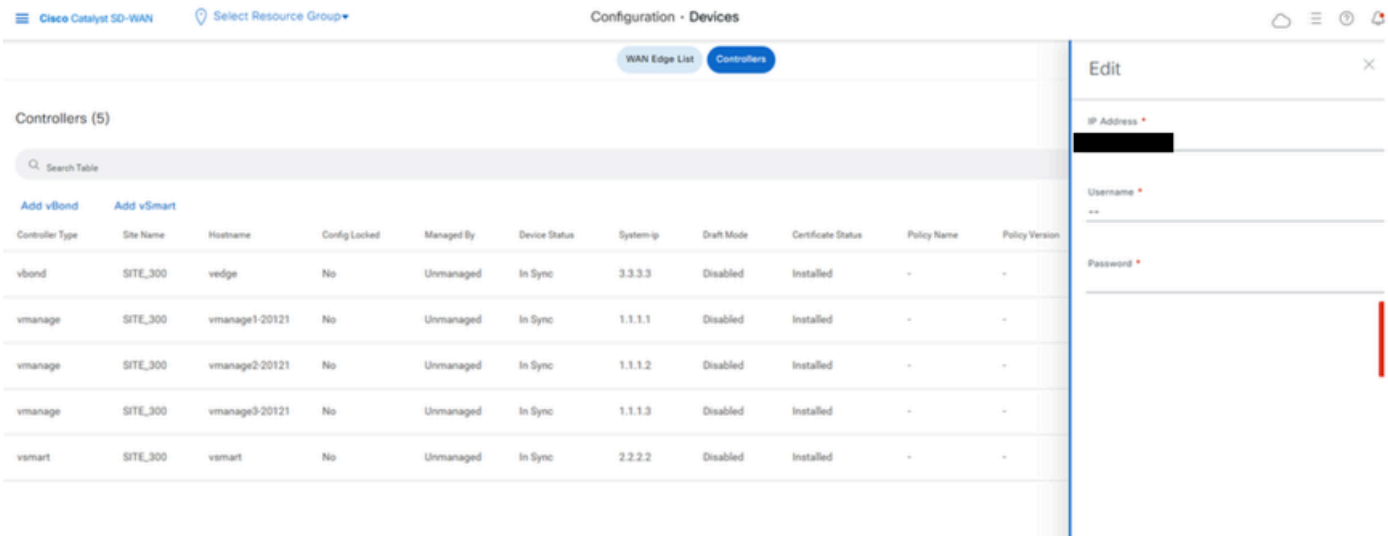
ステップ6：コントローラの再認証と古いコントローラの無効化

configuration-dbが復元されたら、ファブリック内のすべての新しいコントローラ(vmanage/vsmart/vbond)を再認証する必要があります

注：実際の運用で、再認証に使用されるインターフェイスIPがトンネルインターフェイスIPである場合、vManage、vSmart、およびvBondのトンネルインターフェイスでNETCONFサービスが許可され、パスに沿ったファイアウォールでもNETCONFサービスが許可されるようにする必要があります。開くファイアウォールポートは、DRクラスタからすべてのvBondおよびvSmartsへの双方向ルールとしてTCPポート830です（この例では、DRクラスタはIPアドレスがIPアドレスに一致します）。

vmanage UIで、Configuration > Devices > Controllersの順にクリックします。

- 各コントローラの近くにある3つのドットをクリックし、[編集]をクリックします



- ip-address（コントローラのsystem-ip）をtransport vpn 0（トンネルインターフェイス）ip addressに置き換えます。ユーザ名とパスワードを入力して、saveをクリックします
- ファブリック内のすべての新しいコントローラに対して同じ操作を行います

Root-cert-chainの同期

すべてのコントローラがオンボーディングされたら、次の手順を実行します。

新しくアクティブになったクラスタ内の任意のCisco SD-WAN Managerサーバで、次の操作を実行します。

ルート証明書を、新しくアクティブになったクラスタ内のすべてのCisco Catalyst SD-WANデバイスと同期させるには、次のコマンドを入力します。

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

次のコマンドを入力して、Cisco SD-WAN Manager UUIDをCisco SD-WAN Validatorと同期させます。

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

ファブリックが復元され、ファブリック内のすべてのエッジとコントローラに対してコントロールセッションとbfdセッションが確立されたら、古いコントローラ(vmanage/vsmart/vbond)をUIから無効にする必要があります

- vmanage UIで、Configuration > Devices > Certificatesの順にクリックします。
- Controllersをクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。[無効]をクリックします
- vbondに送信をクリックします。
- vmanage UIで、Configuration > Devices > Controllersの順にクリックします。
- 古いファブリックのコントローラ(vmanage/vsmart/vbond)の近くにある3つのドットをクリックします。Deleteをクリックします

事後チェック

これらの投稿チェックは、すべての展開の組み合わせに適用されます。

クラウドエッジルータを再アクティブ化します。

- C8000vがオーバーレイの一部であり、vmanaged signedである場合は、再認証が必要です。次のようになります。

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

        token
```

- コントロール接続とBFDセッションが確立していることを確認します。
- アプリケーショントラフィックがエンドツーエンドで流れていることを確認する
- エッジでファブリックを再構築する前にポートホップに変更を加えた場合は、変更を元に戻す必要があります

- 項目が期待どおりに表示されることを確認します。
    - テンプレート
    - ポリシー
    - デバイスページ（両方のタブ）WAN vEdge ListandControllers

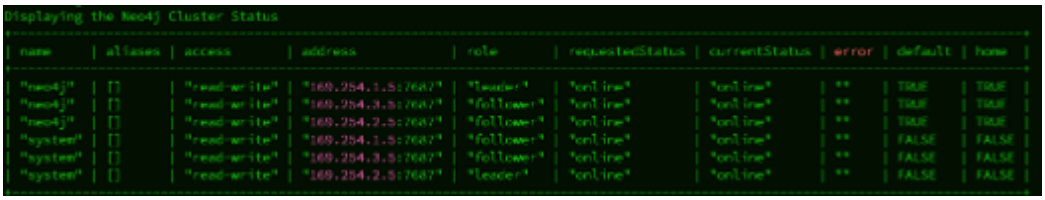
  vManageポストチェック

- vManageノードに適用可能：

  Configuration-DB(Neo4j)チェック：

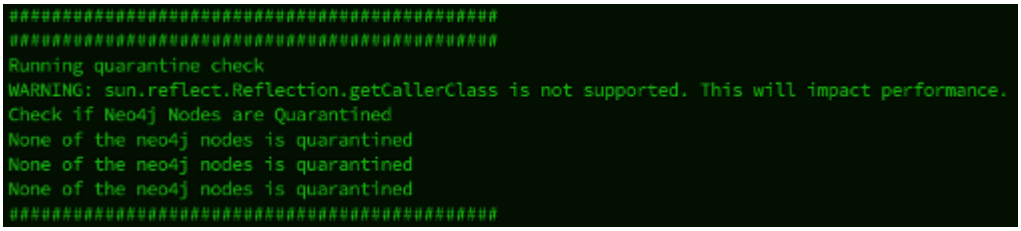
  すべてのvManageノードでコマンド「request nms configuration-db diagnostics」を実行します。

  1. ノードのオンラインおよびリーダーシップステータスを確認します（すべてのバージョンで使用できるわけではありません）。



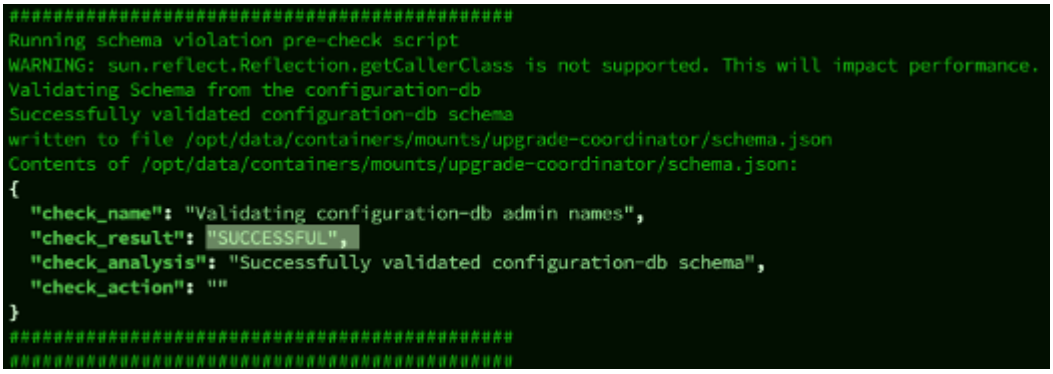
「Neo4j」は、オンラインで3つのノード、リーダー1人とフォロワー2人を表示する必要があります。「system」は、オンラインで3つのノード、リーダーが1つ、フォロワーが2つ表示されている必要がありますが、これはデフォルトのDbではないため、デフォルトのフラグはfalseです。各neo4jに3つ未満のエントリがあり、systemはノードがクラスタから脱落したことを意味します。Cisco TACに問い合わせて、同じ問題のトラブルシューティングを行ってください。

2. いずれかのノードが「検疫」であるかどうかを確認します。

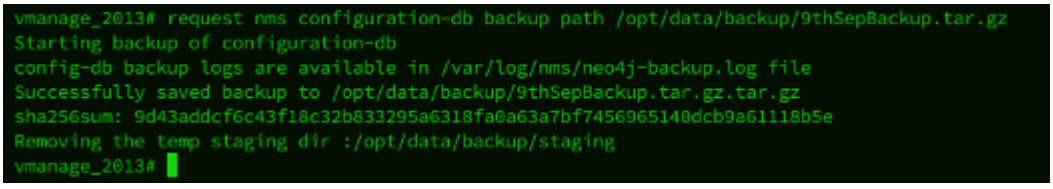


いずれのノードも検疫状態であってはなりません。

3. スキーマの検証は「成功」である必要があります。



4. 「request nms configuration-db diagnostics」コマンドを使用してconfiguration-dbのバックアップを収集し、バックアップが正常に行われたことを確認します。



不整合やエラーが見つかった場合は、Cisco TACに問い合わせてトラブルシューティングを依頼してください。

または、これらのAPI呼び出しを実行して、クラスタのvmanageノードのステータスを確認できます（すべてのCOMPUTE+DATAノードの場合）。バージョン20.12以降でのみ動作します。

```
go to vshell of the vmanage node ( to be done on all vmanages)
================================================================
curl -u



       :



          -H "Content-Type: application/json"   -d '{"statements":[{"statement":"call dbms.cluster.over



         :7474/db/neo4j/tx/commit | jq -r

curl -u



          :



             -H "Content-Type: application/json"   -d '{"statements":[{"statement":"show databases"}]}'



            :7474/db/neo4j/tx/commit | jq -r
```

クラスタ内でneo4jとシステムの両方にリーダーが1つしかないことを確認し、その他のノードはフォロワーになるようにします。すべてのノードがオンラインになっていることを確認します。ノードクラスタが3つある場合（3つすべてがCOMPUTE+DATAです）、neo4jとシステムの両方にリーダーが1つしかないことを確認します。相違点がある場合は、TACに問い合わせてください

5. /var/log/kern.logで、Disk、Mem、IOのエラーを確認します。これは、すべてのvManageノードでチェックする必要があります。

6. 各ノード間にCCがないvmanageの新しいクラスタを形成する場合は、この手順を確認しますノード1から他のノードのクラスタIPへのvmanage-adminとしてsshを実行し、その逆も実行して、公開キーが交換され、パスワードなしのsshが機能しているかどうかを確認します[この手順では、同意トークンが必要です]

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



The authenticity of host '[192.168.50.5]:830 ([192.168.50.5]:830)' can't be established.
ECDSA key fingerprint is SHA256:rSpscoYCVC+yifUMHVTlxtjqmyrZSFg93msFdoSUieQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.50.5]:830' (ECDSA) to the list of known hosts.
viptela 20.9.3.0.31

Password:
```

出力でパスワードの入力が求められる場合は、TACに連絡してください。

コントローラのPostチェック：

すべてのSD-WANコントローラ(vBond、vManage、vSmart)に適用可能：

オーバーレイ内のすべてのコントローラでコマンドを実行し、表示されたvManage UUIDとシリアル番号が現在のファブリックに対して有効であることを確認します。

vBondコマンド：

show orchestrator valid-vsmarts（任意）

show orchestrator valid-vmanage-id

vManage/vSmartコマンド：

show control valid-vsmarts（隠しコマンド）

show control valid-vmanage-id

show control valid-vsmartsの出力には、vSmartsノードとvManageノードの両方のシリアル番号が含まれることに注意してください。

vManage UIで表示される内容と比較します。Configuration > Certificates > Controllersの順に選択します。

現在ファブリックにオンボードされていないUUIDまたはシリアル番号に対するエントリが追加されている場合は、それらを削除する必要があります。Cisco TACにも同様に問い合わせることができます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。