Catalyst SD-WAN 패브릭 재구축

목차

소개

이 문서에서는 다양한 구축을 위한 컨트롤러 컨피그레이션 백업 및 복원을 포함하여 Cisco SD-WAN 패브릭을 재구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(소프트웨어 정의 WAN)
- Cisco Software Central
- software.cisco.com에서 컨트롤러 소프트웨어 다운로드

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

패브릭을 재구축하기 전의 사전 요구 사항

- 컨트롤러의 새 패브릭에 대해 새로운 system-ips, site-ids 집합을 구성해야 합니다.
- 컨트롤러와 에지 간의 통신을 지원하는 방화벽 규칙이 있는지 확인
- neo4j(configuration-db) 사용자 이름과 비밀번호를 확인합니다(클러스터의 모든 vManage 노드에서 동일해야 함).
- 모든 에지에서 포트 홉 비활성화
- Graceful Restart 타이머를 7일로 늘립니다
- 마이그레이션 전에 서드파티 툴에서 경보 지우기
- 통계를 외부 서버(예: vAnalytics)로 내보내기 위한 사전 설정이 없는 경우 기록 통계 데이터(경보, 이벤트, 디바이스 통계 등)가 손실됩니다
- Cloud OnRamp가 구성된 경우, 이 작업을 시작하기 전에 클라우드에 구축된 c8000v에 연결할 수 있는지 확인합니다

- 이전 패브릭에서 SDAVC를 활성화한 경우 새 패브릭이 활성화되었는지 확인합니다(클러스터의 경우 단일 노드에서만 활성화해야 함).
- Configuration-db 복원은 원래 패브릭과 동일한 버전에서만 지원됩니다
- 컨트롤러에 사용되는 페르소나를 확인합니다. COMPUTE_DATA 및 DATA 페르소나를 지원합니다(각 섹션에 자세히 설명).
- Enterprise CA의 경우 Enterprise CA에서 발급한 루트 인증서를 사용해야 합니다. 이 인증서는 기존 오버레이에서 사용되며, Enterprise CA 서버를 사용하여 서명되고 UI를 통해 모든 컨트롤러에 설치됩니다

구축 옵션

vManage 구축

- 독립형(1노드)
- 클러스터(3노드 또는 6노드)

DR 옵션

- DR 없음
- 단일 노드 DR
- 대기 DR 클러스터(수동/관리 트리거됨)

참고: 재해 복구 유형에 대한 자세한 내용은 이 링크를 참조하십시오.

조합:

#	vManage 설정	DR 옵션
1	독립형(1노드)	DR 없음
2	독립형(1노드)	단일 노드 DR
3	클러스터(3노드 또는 6노드)	DR 없음
4	클러스터(3노드 또는 6노드)	대기 DR 클러스터

모든 조합에 적용할 수 있는 공통 단계

이러한 단계는 모든 구축 조합에 공통적으로 적용됩니다. VM 인스턴스를 시작하고 기본 CLI 컨피그레이션을 적용하는 프로세스를 다룹니다. 각 조합 섹션에는 구축할 인스턴스 수와 완료할 추가 단계가 나와 있습니다.

SD-WAN 컨트롤러 설치 및 실행(관리자, 검증기, 컨트롤러)

참고: Cisco는 특정 용어를 변경했으므로 이 용어는 상호 교환 가능합니다. Cisco vManage = Cisco Catalyst Manager, Cisco vBond = Cisco Catalyst Validator, Cisco vSmart = Cisco Catalyst 컨트롤러

Cisco Software Download(Cisco 소프트웨어 다운로드) 페이지에서 SD-WAN 컨트롤러용 OVA 파일을 다운로드합니다.

- vEDGE Cloud(vEDGE 클라우드)를 선택하고 필요한 소프트웨어 버전에 대한 vBond OVA를 다운로드합니다.
- vManage software를 선택하고 필요한 소프트웨어 버전에 대한 vManage OVA를 다운로드합니다.
- vSmart 소프트웨어를 선택하고 필요한 소프트웨어 버전에 대한 vSmart OVA를 다운로드합니다.

참고: ESXi/클라우드 플랫폼에서 OVA 파일을 사용하여 vSmart, vBond 및 vManage 컨트롤러를 스핀업합니다. 연결된 문서를 참조하고 SD-WAN 구축 유형에 따라 모든 컨트롤러에 충분한 CPU, RAM 및 디스크가 할당되었는지 확인합니다. 추가 정보를 보려면 여기로 이동하십시오. 연결된 컴퓨팅 설명서의 Storage Size* 열에 설명된 대로 vManage 노드에 보조 디스크를 할당해야 합니다.

Cisco Manager 노드 표시

- Cisco Manager 또는 vManage VM이 구축되고 관리자 콘솔에 액세스할 수 있게 되면 부팅이 완료될 때까지 기다립니다. 한 가지 표시는 메시지 시스템이 준비되었고 사용자 이름과 비밀번호를 입력하라는 메시지가 표시된다는 것입니다.
- 기본 사용자 자격 증명 사용자 이름을 admin으로, 비밀번호를 admin으로 입력합니다. 사용자에게 비밀번호를 변경하라는 메시지가 표시되면 선택에 따라 사용자 관리에 필요한 비밀번호를 설정합니다.
- 그런 다음 사용자에게 페르소나를 선택하라는 프롬프트를 표시합니다. 이는 vManage 클러스터를 사용하려는 경우 매우 중요한 단계입니다. 다음 시나리오에 따라 페르소나를 선택하십시오.

```
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
```

예: COMPUTE_AND_DATA에 대해 1을 선택합니다.

```
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] _
```

다음과 같이 보조 디스크를 선택합니다.

```
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
```

- 보조 디스크를 선택하고 Y를 입력하여 확인합니다.
- Cisco Manager가 다시 로드됩니다. 부팅되면 새로 구성된 새 비밀번호와 함께 사용자 이름 및 비밀번호를 입력합니다.

```
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#
```

- 컨트롤러에 대한 대역 외 관리 액세스를 활성화하도록 VPN 512 관리 인터페이스를 구성할 수 있습니다.
- show interface 명령을 사용합니다 | 탭을 클릭하면 인터페이스가 현재 매핑된 VPN을 확인할 수 있습니다.
- 인터페이스를 적절하게 구성합니다.

예

```
                                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#
```

참고: 여기에서 기존 vManage의 컨피그레이션을 참조하고 동일한 IP 주소 체계를 구성할 수 있습니다.

관리 인터페이스(VPN 512) 구성

- 인터페이스를 VPN 0에서 VPN 512로 이동해야 하는 경우 이 명령을 사용한 다음 인터페이스에서 IP 주소를 구성합니다

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




  no shutdown
 !
 ip route 0.0.0.0/0



!
```

유효성 검사기를 불러옵니다.

- 하이퍼바이저에서 vBond 노드에 필요한 컴퓨팅(CPU, RAM 및 디스크)을 구성하고 전원을 켭니다.
- 콘솔에 액세스할 수 있게 되면 vBond가 완전히 부팅될 때까지 기다립니다. System Ready(시스템 준비) 메시지를 기다립니다.
- 그런 다음 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 기본 사용자 자격 증명 사용자 이름을 admin으로 입력하고 비밀번호를 admin으로 입력합니다. 비밀번호를 변경하라는 메시지가 표시되면 선택에 따라 사용자 admin에 필요한 비밀번호를 설정합니다.
- 컨트롤러에 대한 대역 외 관리 액세스를 활성화하도록 VPN 512 관리 인터페이스를 구성할 수 있습니다.
- show interface 명령을 사용합니다 | 탭을 클릭하면 인터페이스가 현재 매핑된 VPN을 확인할 수 있습니다.
- 그에 따라 인터페이스를 구성합니다.

예:

```
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#
```

참고: 기존 vBond에서 컨피그레이션을 참조하고 여기서 동일한 컨피그레이션을 구성할 수 있습니다.

관리 인터페이스(VPN 512) 구성

- 인터페이스를 VPN 0에서 VPN 512로 이동해야 하는 경우 이 명령을 사용한 다음 인터페이스에서 IP 주소를 구성합니다.

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




  no shutdown
 !
 ip route 0.0.0.0/0



!
```

```
commit
```

컨트롤러(vSmart) 노드 시작

- vSmart 노드를 불러오려면 검증기와 동일한 단계를 수행합니다.
- 모든 SD-WAN 컨트롤러에서 VPN 512 IP 주소가 구성되면 VPN 512 IP 주소에서 SSH를 사용하여 액세스할 수 있습니다.

모든 컨트롤러의 기본 CLI 컨피그레이션

모든 컨트롤러에 대한 SSH 액세스 권한을 갖게 되면 각 컨트롤러에서 이러한 CLI 컨피그레이션을 구성합니다.

시스템 컨피그레이션

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

참고: URL을 vBond 주소로 사용하는 경우 VPN 0 컨피그레이션에서 DNS 서버 IP 주소를 구성하거나 확인할 수 있는지 확인하십시오.

전송 인터페이스(VPN 0) 컨피그레이션

라우터 및 나머지 컨트롤러와의 제어 연결을 설정하는 데 사용되는 전송 인터페이스를 활성화하려면 모든 컨트롤러에서 이러한 컨피그레이션이 필요합니다.

```
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
```

참고: 기존 컨트롤러의 컨피그레이션을 참조할 수 있으며, 컨피그레이션이 있는 경우 이 컨피그레이션을 새 컨트롤러에 추가할 수 있습니다.

라우터가 TLS를 사용하여 vManage 노드와 보안 제어 연결을 설정해야 하는 경우에만 제어 프로토콜을 TLS로 구성합니다. 기본적으로 모든 컨트롤러와 라우터는 DTLS를 사용하여 제어 연결을 설정합니다. 이는 사용자의 요구 사항에 따라 vSmart 및 vManage 노드에서만 필요한 선택적 컨피그레이션입니다.

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

조합 1: 독립형 vManage + DR 없음

필요한 인스턴스:

- 1 vManage(COMPUTE_AND_DATA)
- vBond 1개 이상
- vSmart 1개 이상

단계:

1. 공통 단계를 사용하여 모든 인스턴스 가져오기
2. 사전 확인
3. vManage UI, 인증서 및 온보드 컨트롤러 구성
4. Config-db 백업/복원
5. 수표 게시

1단계: 사전 확인

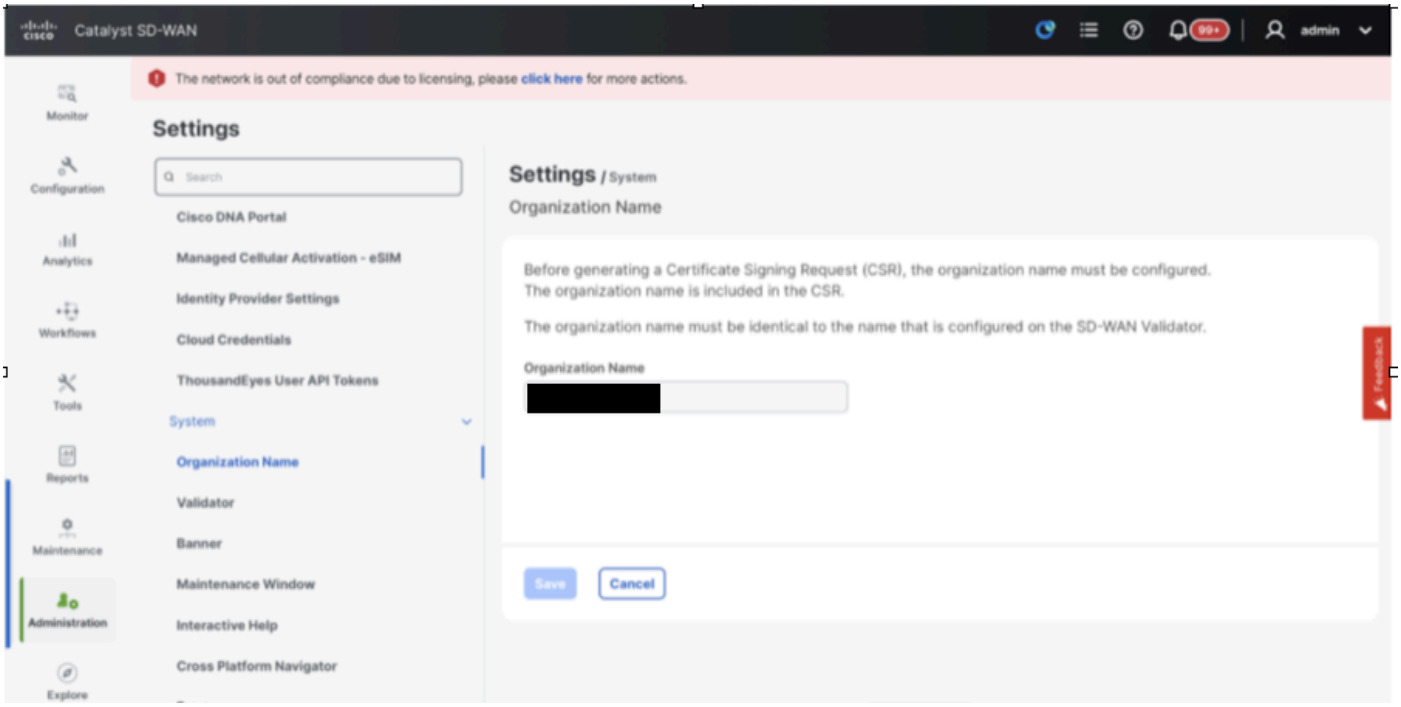
- 활성 Cisco SD-WAN Manager 인스턴스의 수가 새로 설치된 Cisco SD-WAN Manager 인스턴스의 수와 동일한지 확인합니다.

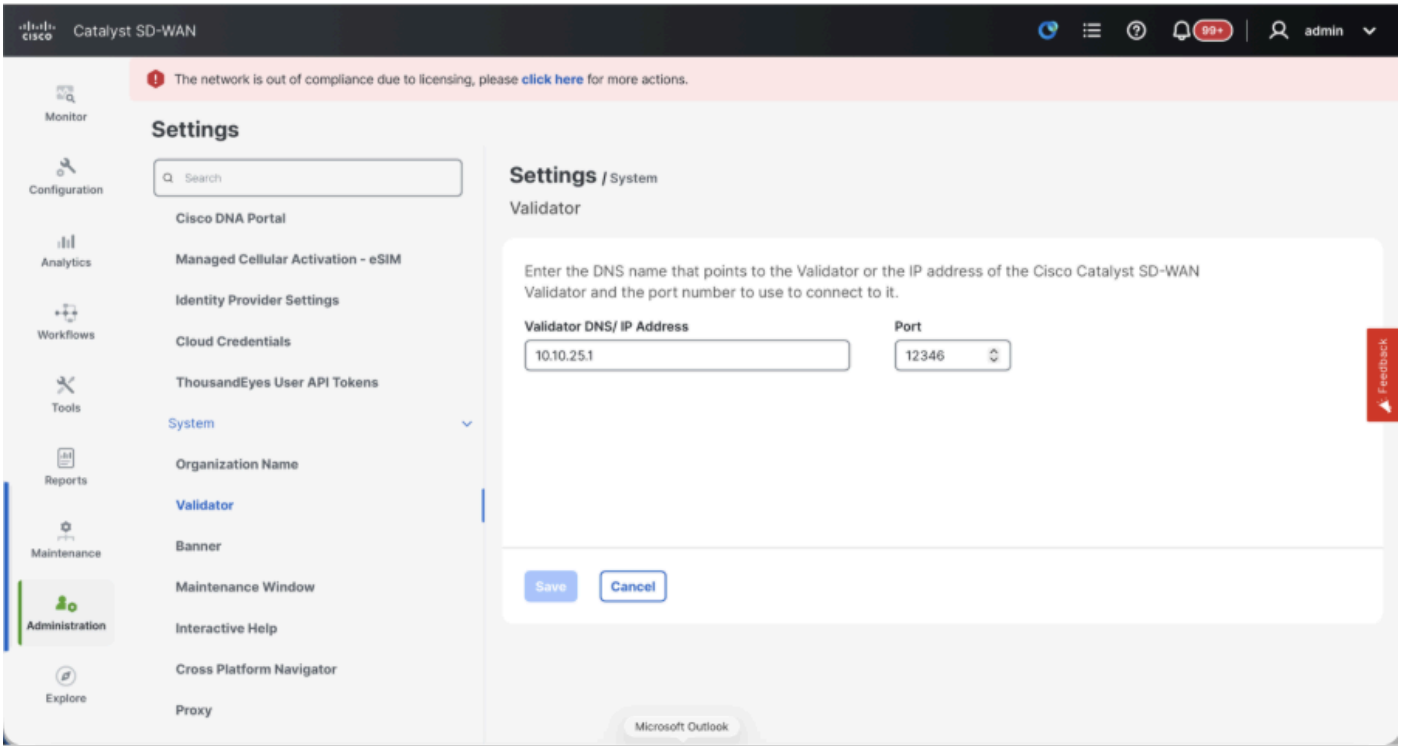
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 동일한 소프트웨어 버전을 실행하는지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 Cisco SD-WAN Validator의 관리 IP 주소에 연결할 수 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스에 인증서가 설치되어 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스를 포함하여 모든 Cisco Catalyst SD-WAN 디바이스의 시계가 동기화되었는지 확인합니다.
- 새 시스템 IP 및 사이트 ID 집합이 활성 클러스터와 동일한 기본 구성과 함께 새로 설치된 Cisco SD-WAN Manager 인스턴스에 구성되어 있는지 확인합니다.

2단계: vManage UI, 인증서 및 온보드 컨트롤러 구성

vManage UI에서 컨피그레이션 업데이트

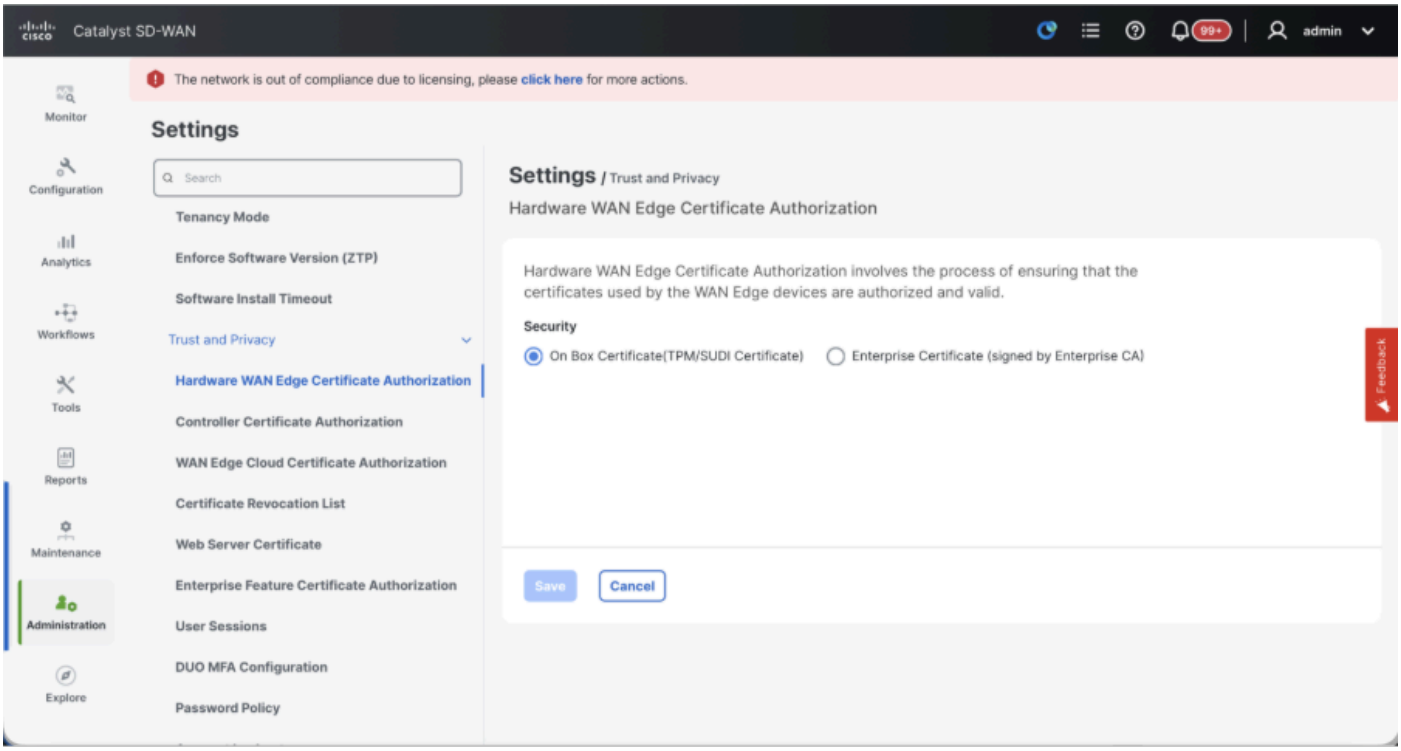
- 1단계의 컨피그레이션이 모든 컨트롤러의 CLI에 추가되면 브라우저의 URL https://<vmanage-ip>를 사용하여 vManage의 webUI에 액세스할 수 있습니다. 각 vManage 노드의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Administration(관리) > Settings(설정)로 이동하여 다음 단계를 완료합니다.
- 조직 이름 및 검증기/vBond URL/IP 주소를 구성합니다. vManage 노드의 CLI에서와 동일한 값을 구성합니다.
- vManage 20.15/20.18의 섹션 System에서 이러한 구성을 사용할 수 있습니다.



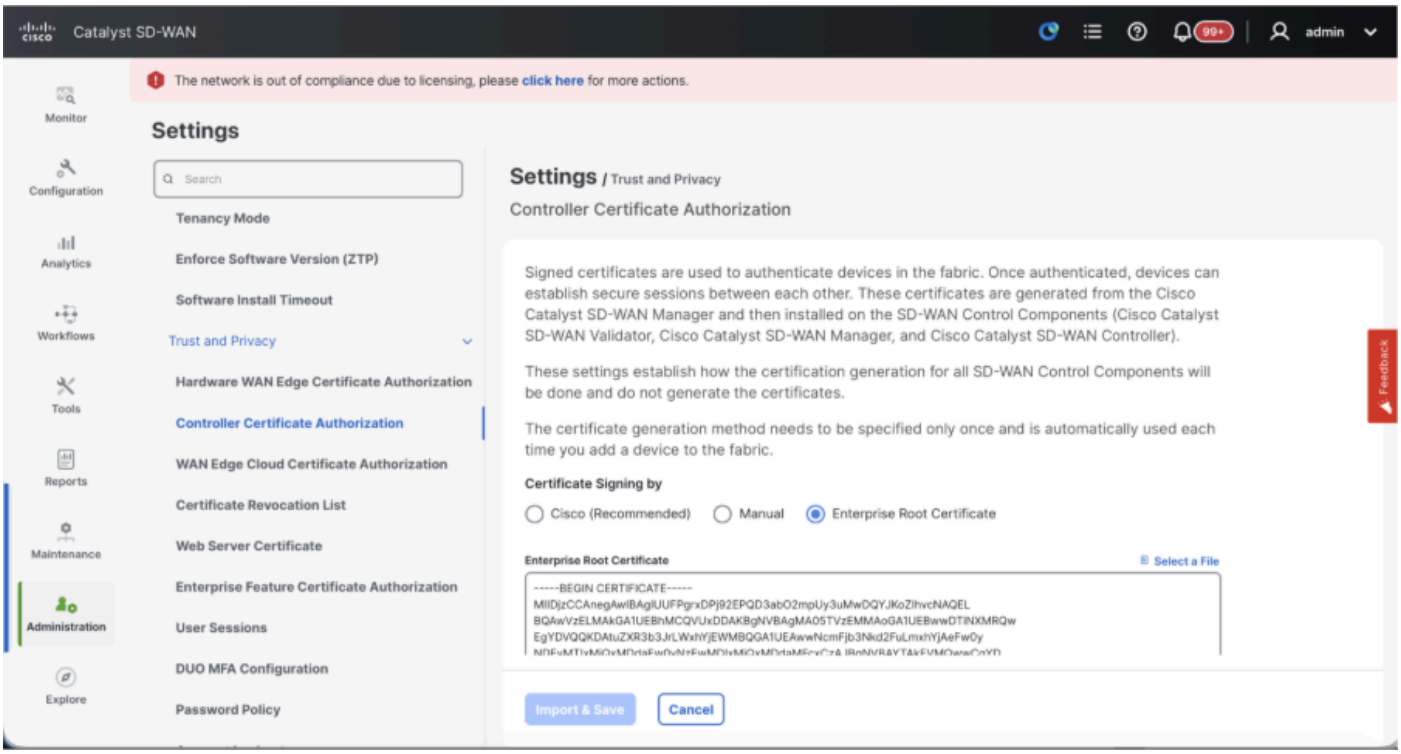


- 인증서 서명에 사용되는 인증 기관을 결정하는 CA(Certificate Authorization)의 컨피그레이션을 확인합니다. 3가지 옵션이 있습니다.

1. Hardware WAN Edge Certificate Authorization - 하드웨어 SD-WAN 에지 라우터의 CA를 결정합니다.
    - On Box Certificate(TPM/SUDI 인증서) - 이 옵션을 사용하면 라우터 하드웨어에 미리 설치된 인증서를 사용하여 제어 연결(TLS/DTLS 연결)을 설정합니다
    - 엔터프라이즈 인증서(Enterprise CA에서 서명) - 이 옵션을 사용하면 라우터가 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

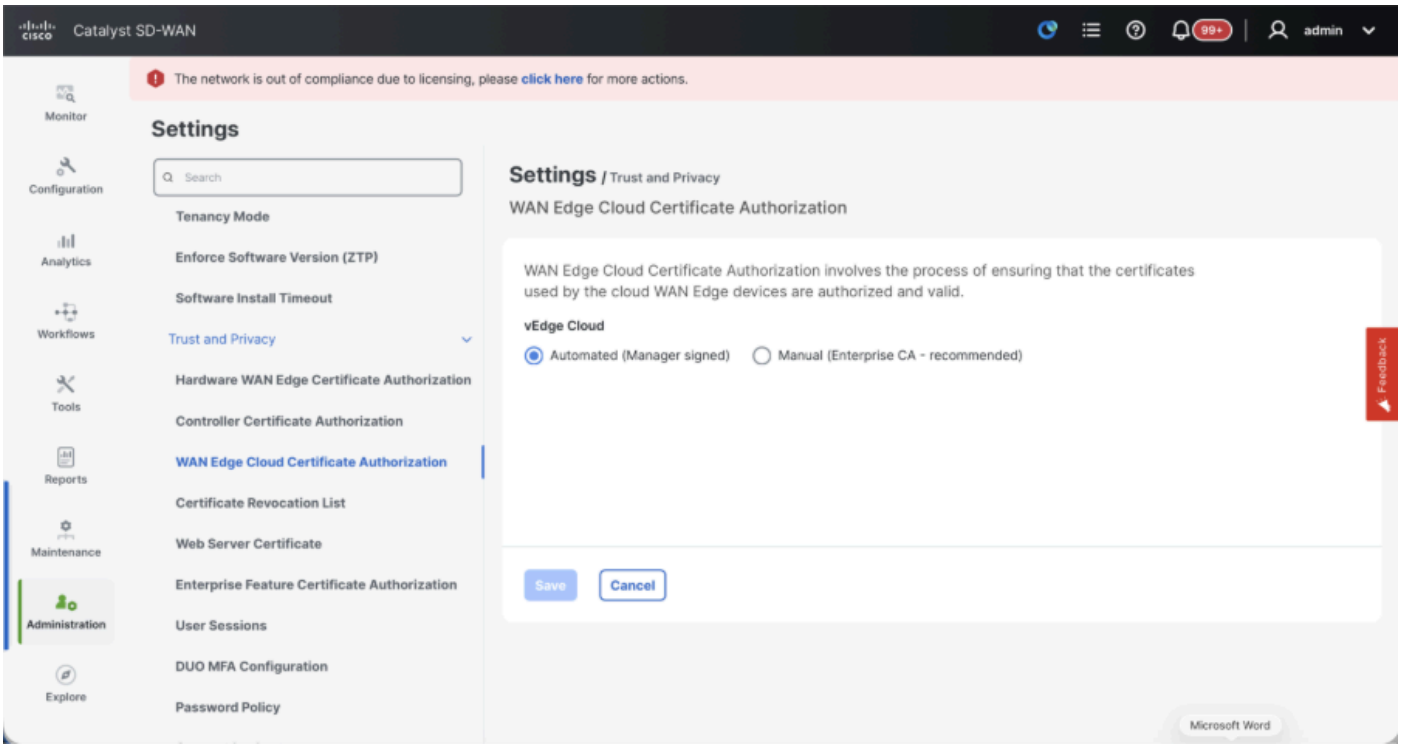


2. Controller Certificate Authorization(컨트롤러 인증서 권한 부여) - SD-WAN 컨트롤러에 대한 CA를 결정합니다.
    - Cisco(권장) - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. vManage는 vManage에 구성된 스마트 어카운트 자격 증명을 사용하여 PNP 포털에 자동으로 연결하고 서명된 인증서를 가져오며 컨트롤러에 설치됩니다.
    - 수동 - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. 각 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 수동으로 CSR에 서명합니다.
    - Enterprise Root Certificate(엔터프라이즈 루트 인증서) - 이 옵션을 사용하면 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

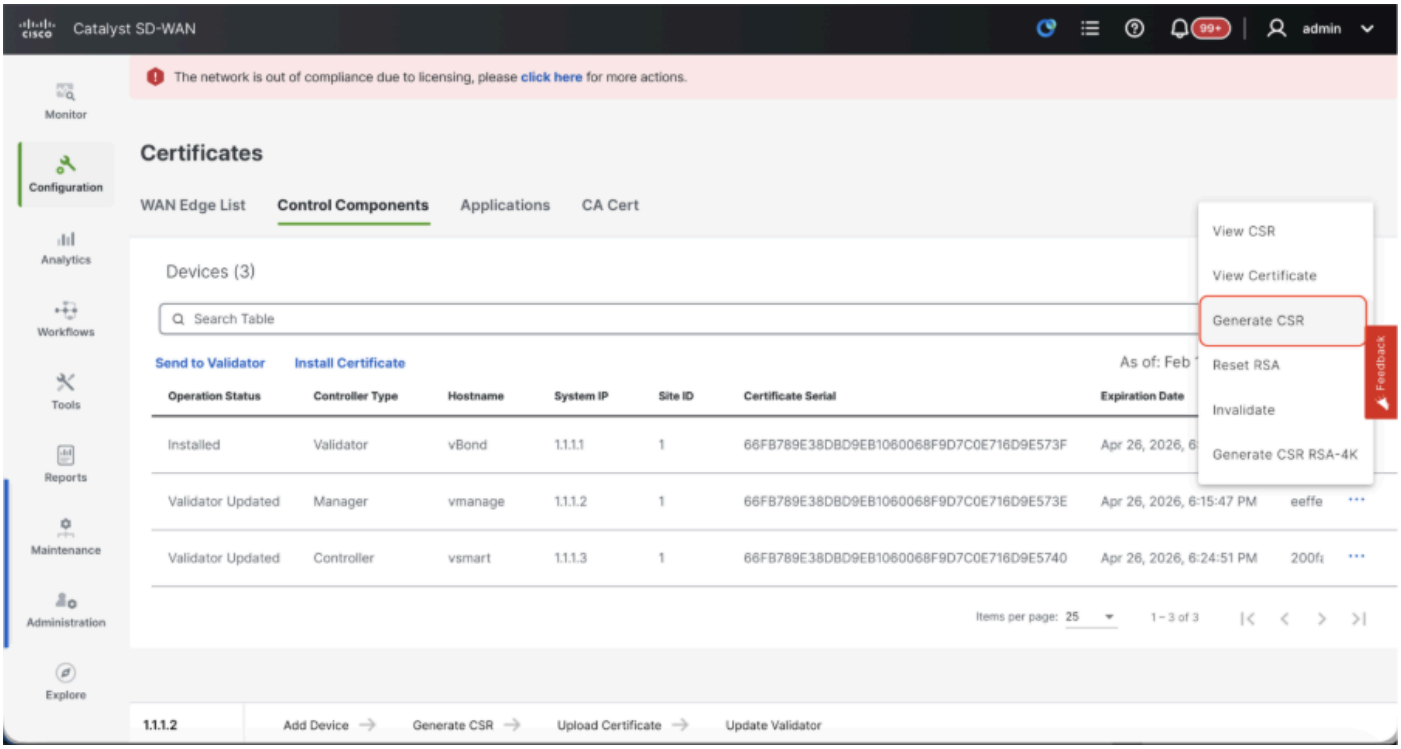


3. WAN Edge Cloud Certificate Authorization - 가상 SD-WAN Edge 라우터(CSR1000v, C8000v, vEdge 클라우드)에 대한 CA를 결정합니다.
    - 자동(vManage signed) - vManage는 가상 에지 라우터의 CSR에 자동으로 서명하고 라우터에 인증서를 설치합니다.
    - 수동(엔터프라이즈 CA - 권장) - 가상 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

자체 CA인 Enterprise Certificate Authority를 사용하는 경우 Enterprise를 선택합니다.



- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)
- Manager/vManage(관리자/vManage)에서 ...를 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.

- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

vManage에 vBond/Validator 및 vSmart/Controller 온보딩(Onboarding)

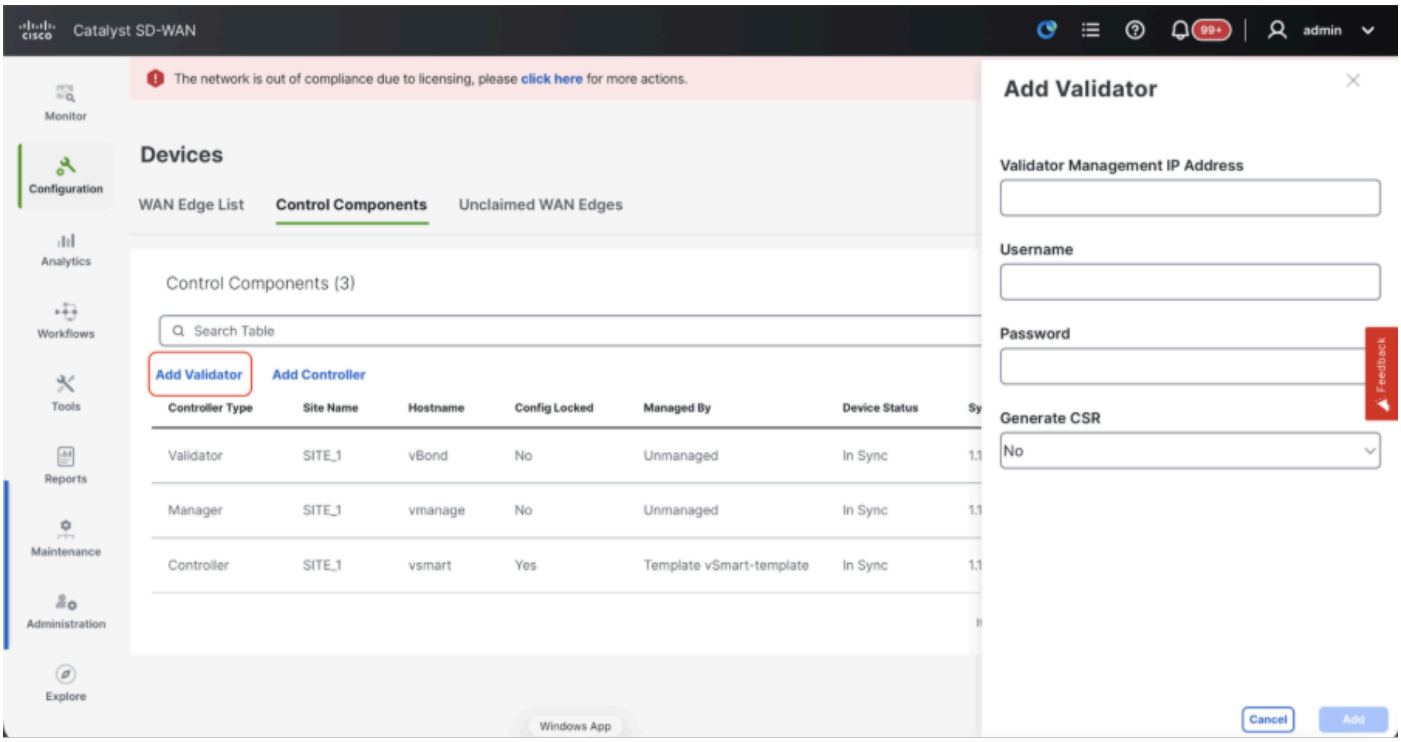
20.15/20.18 vManage 노드의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Control Components(제어 구성 요소)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

온보딩vBond/Validator

- Add(추가)VBond(vBond 추가)를 클릭합니다.제2012호의 경우유효성 검사기 추가 20.15/20.18 vManage입니다. 팝업이 열리면 vManage에서 연결할 수 있는 vBond의 VPN 0 전송 IP.
- vManagetovBondIP의 CLI에서 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.
- vBond의 사용자 자격 증명을 입력합니다.

참고: vBonor의 관리자 자격 증명 또는 netadmingroup의 사용자 부분이 필요합니다. vBond의 CLI에서 이를 확인할 수 있습니다. vBond에 대한 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다.

참고: vBond가 NAT 디바이스/방화벽 뒤에 있는 경우 vBond VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인합니다. vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스의 공용 IP 주소를 사용합니다.



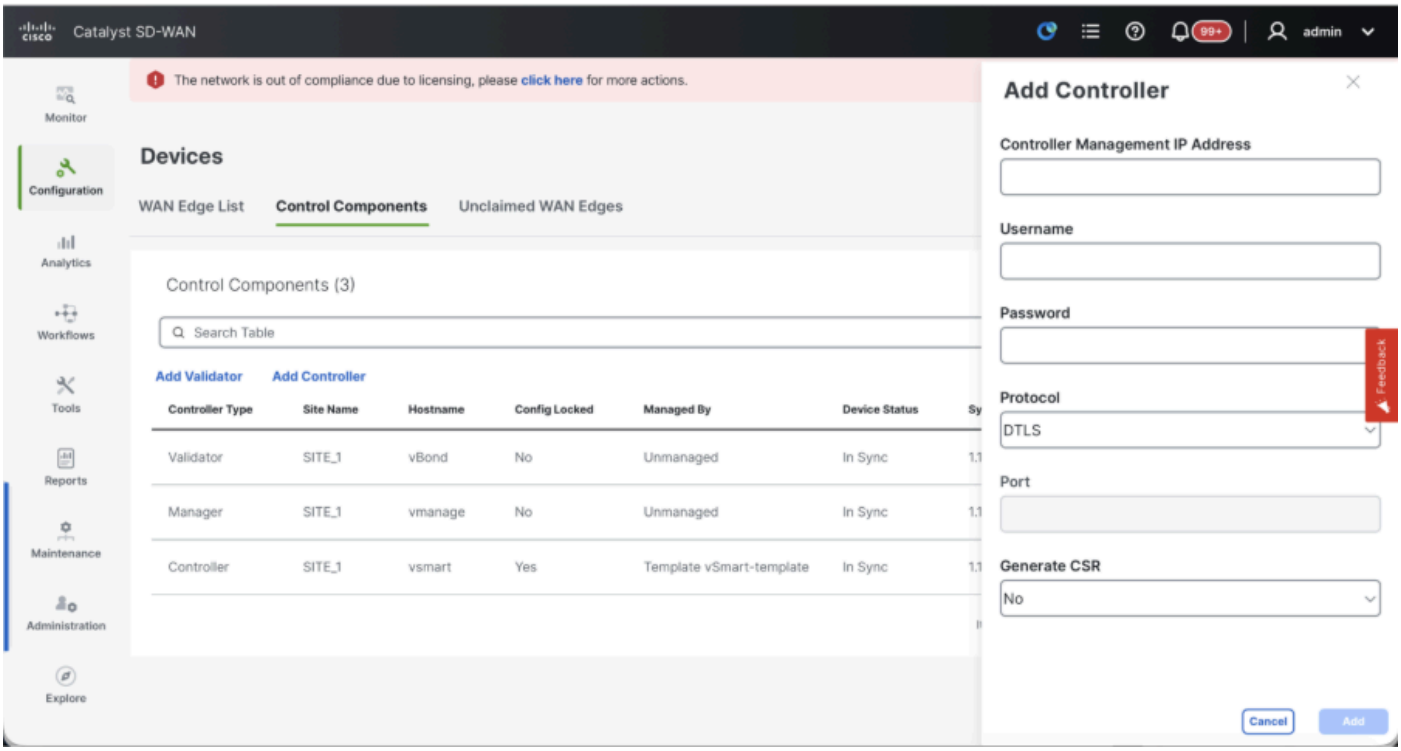
- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vBond에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vBond가 여러 개인 경우 동일한 단계를 반복합니다.

vSmart/컨트롤러 온보딩

- 20.12 vManage의 경우 vSmart 추가 또는 20.15/20.18 vManage의 경우 컨트롤러 추가를 클릭합니다.
- 팝업이 열리면 vManage에서 연결할 수 있는 vSmart의 VPN 0 전송 IP를 입력합니다.
- vManage의 CLI에서 vSmart IP로 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.
- vSmart의 사용자 자격 증명을 입력하십시오. vSmart의 관리자 자격 증명 또는 netadmin 그룹의 사용자 부분을 사용해야 합니다.
- vSmart의 CLI에서 이를 확인할 수 있습니다.
- 라우터에 TLS를 사용하여 vSmart와의 제어 연결을 설정하려면 프로토콜을 TLS로 설정합니다. vSmarts 및 vManage 노드의 CLI에서도 이 구성을 구성해야 합니다.
- vSmart용 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예

)를 선택합니다.

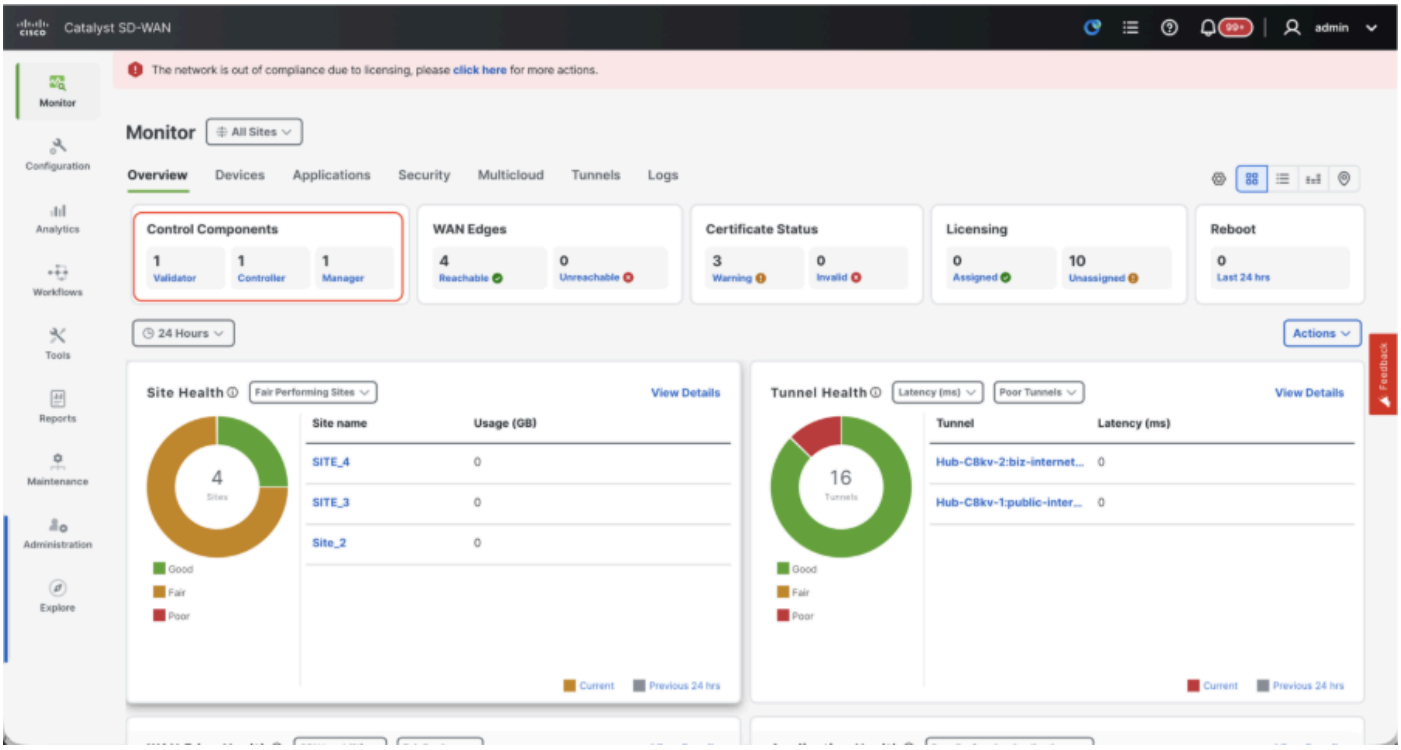
참고: vSmart가 NAT 장치/방화벽 뒤에 있는 경우 vSmart VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인하고, vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스 IP의 공용 IP 주소를 사용합니다.



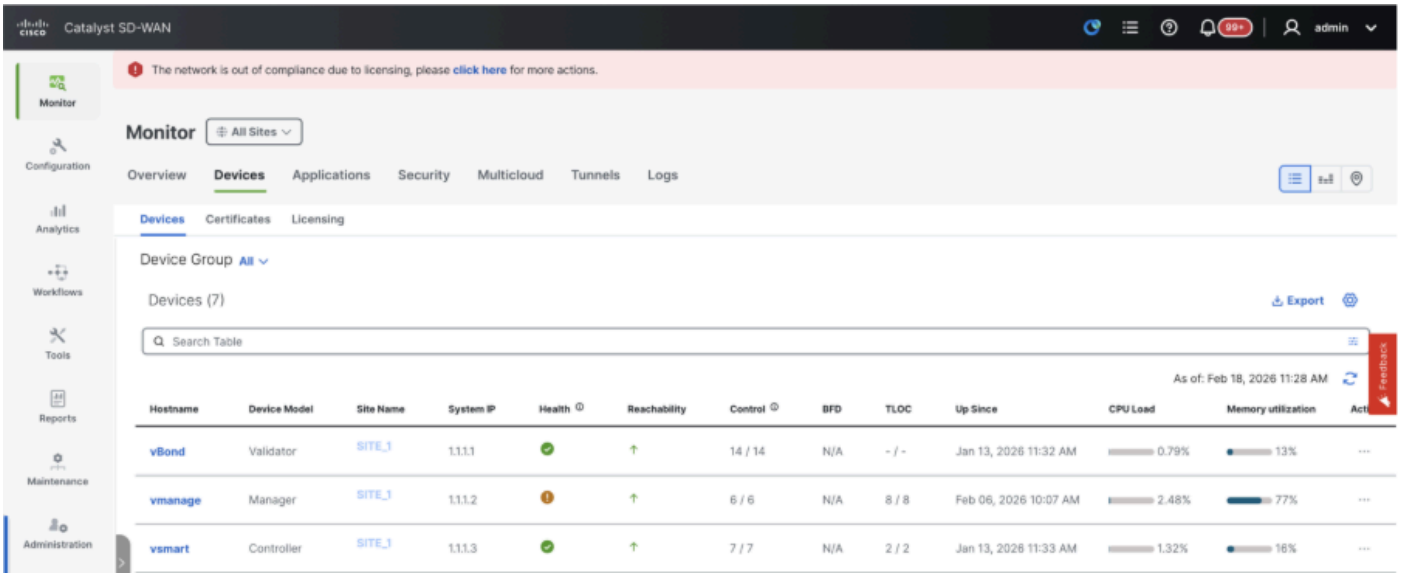
- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vSmart에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- vSmarts가 여러 개인 경우 동일한 단계를 반복합니다.

확인

모든 단계가 완료되면 Monitor>Dashboard에서 모든 제어 구성 요소에 연결할 수 있는지 확인합니다



- 각 Control(제어) 구성 요소를 클릭하고 모두 연결할 수 있는지 확인합니다.
- Monitor(모니터링) > Devices(디바이스)로 이동하여 모든 제어 구성 요소에 연결할 수 있는지 확인합니다.



3단계: Config-db 백업/복원

다른 vManage 노드에서 vManage configuration-db 백업 및 복원 수집

Configuration-DB 백업 수집:

- 현재 사용 중인 SD-WAN 패브릭에서는 독립형 vManage 및 vManage 클러스터 설정 모두에서 컨피그레이션 DB 백업을 생성할 수 있습니다.
- 독립형 vManage의 경우 해당 vManage 자체가 configuration-db 리더입니다.

vManage 노드에서 configuration-db가 실행 중인지 확인합니다.

명령 요청 nms configuration-db status onvManageCLI를 사용하여 동일한 항목을 확인할 수 있습니다. 출력은 다음과 같습니다

```
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#
```

식별된 configuration-db leader vManage 노드에서 configuration-db 백업을 수집하려면 이 명령을 사용합니다.

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

예상 출력은 다음과 같습니다.

```
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#
```

- 컨피그레이션 DB 자격 증명이 업데이트된 경우 기록해 둡니다.
- configuration-db 자격 증명을 모르는 경우 TAC에 문의하여 기존 vManage 노드에서 configuration-db 자격 증명을 검색합니다.
- 기본 configuration-db 자격 증명은 사용자 이름입니다. neo4j 및 비밀번호: 암호

다른 vManage 노드에 Configuration-db 백업 복원

SCP를 사용하여 configuration-db 백업을 vManage의 /home/admin/ 디렉토리에 복사합니다.

샘플 scp 명령 출력:

```
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 백업을 복원하려면 먼저 configuration-db 자격 증명을 구성해야 합니다. configuration-db 자격 증명이 default(neo4j/password)인 경우 이 단계를 건너뛸 수 있습니다.

configuration-db 자격 증명을 구성하려면 nms configuration-db update-admin-user 명령을 사용합니다. 선택한 사용자 이름과 비밀번호를 사용합니다.

vManage의 애플리케이션 서버가 다시 시작됩니다. 따라서 vManage UI에 짧은 시간 동안 액세스할 수 없게 됩니다.

```
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#
```

구성 DB 백업을 복원하기 위해 진행할 수 있는 게시:

nms configuration-db 복원 경로 /home/admin/< > 명령을 사용하여 configuration-db를 새 vManage로 복원할 수 있습니다.

```
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-db가 복원되면 vManage UI에 액세스할 수 있는지 확인합니다. 약 5분 정도 기다린 후 UI에 액세스를 시도합니다.

UI에 성공적으로 로그인했으면 Edge 라우터 목록, 템플릿, 정책 및 이전 또는 기존 vManage UI에 존재했던 나머지 모든 컨피그레이션이 새 vManage UI에 반영되었는지 확인합니다.

4단계: 컨트롤러 재인증 및 이전 컨트롤러 무효화

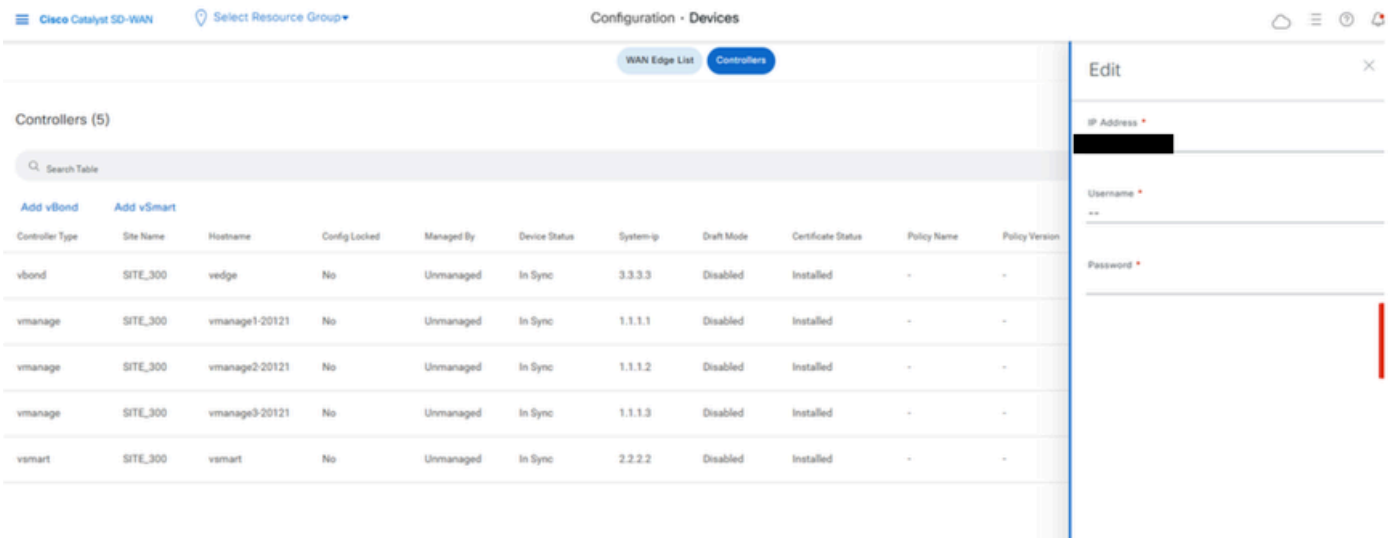
configuration-db가 복원되면 패브릭에서 모든 새 컨트롤러(vmanage/vsmart/vbond)를 다시 인증해야 합니다.

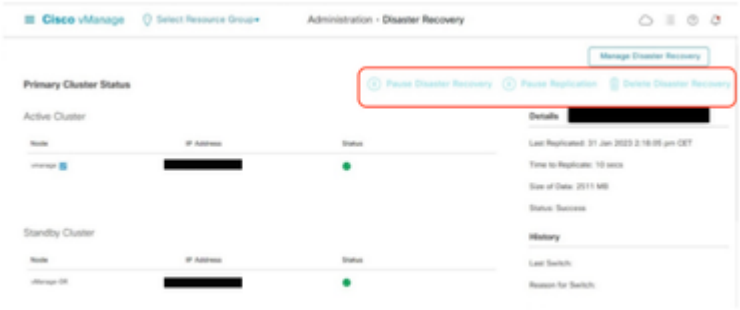
참고: 실제 프로덕션에서는 재인증에 사용되는 인터페이스 IP가 터널 인터페이스 IP인 경우 vManage, vSmart 및 vBond의 터널 인터페이스 및 경로에 따른 방화벽에서 NETCONF 서비스가 허용되는지 확인해야 합니다. 열 방화벽 포트는 DR 클러스터에서 모든 vBond 및 vSmarts로의 양방향 규칙인 TCP 포트 830입니다.

---

vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다

- 각 컨트롤러 근처의 점 3개를 클릭하고 Edit(수정)를 클릭합니다





- ip-address(컨트롤러의 system-ip)를 transport vpn 0(터널 인터페이스) ip 주소로 교체합니다. 사용자 이름 및 비밀번호를 입력하고 저장을 클릭합니다
- 패브릭에 있는 모든 새 컨트롤러에 대해 동일한 작업을 수행합니다.

루트 인증서 체인 동기화

모든 컨트롤러가 온보딩되면 다음 단계를 완료합니다.

새로 활성화된 클러스터의 Cisco SD-WAN Manager 서버에서 다음 작업을 수행합니다.

루트 인증서를 새로 활성화된 클러스터의 모든 Cisco Catalyst SD-WAN 디바이스와 동기화하려면 다음 명령을 입력합니다.

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

Cisco SD-WAN Manager UUID를 Cisco SD-WAN Validator와 동기화하려면 다음 명령을 입력합니다.

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

패브릭이 복원되고 패브릭의 모든 에지와 컨트롤러에 대해 제어 및 bfd 세션이 작동되면 UI에서 이전 컨트롤러(vmanage/vsmart/vbond)를 무효화해야 합니다

- vmanage UI에서 Configuration > Certificates > Controllers를 클릭합니다
- Controllers(컨트롤러) 클릭
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond)의 오른쪽에 있는 점 3개를 클릭합니다. Invalidate를 클릭합니다.
- Send to Bond를 클릭합니다.
- vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond)의 오른쪽에 있는 3개의 주소를 클릭합니다. 삭제를 클릭합니다.

5단계: 수표 게시

참고: 여기에 표시된 모든 구축 조합에 공통적으로 적용되는 Post Checks(사후 검사) 섹션을 계속 진행합니다.

조합 2: 독립형 vManage + 단일 노드 DR

필요한 인스턴스:

- 1 vManage(기본, COMPUTE_AND_DATA)
- 1 vManage(DR 대기, COMPUTE_AND_DATA)
- vBond 1개 이상
- vSmart 1개 이상

단계:

1. 공통 단계를 사용하여 모든 인스턴스 가져오기
2. 사전 확인
3. vManage UI, 인증서 및 온보드 컨트롤러 구성
4. 단일 노드 DR 설정
5. Config-db 백업/복원
6. 수표 게시

1단계: 사전 확인

- 활성 Cisco SD-WAN Managerinstances의 수가 새로 설치된 Cisco SD-WAN Managerinstances의 수와 동일한지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 동일한 소프트웨어 버전을 실행하는지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 Cisco SD-WAN Validator의 관리 IP 주소에 연결할 수 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스에 인증서가 설치되어 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스를 포함하여 모든 Cisco Catalyst SD-WAN 디바이스의 시계가 동기화되었는지 확인합니다.
- 새 시스템 IP 및 사이트 ID 집합이 활성 클러스터와 동일한 기본 구성과 함께 새로 설치된 Cisco SD-WAN Manager 인스턴스에 구성되어 있는지 확인합니다.

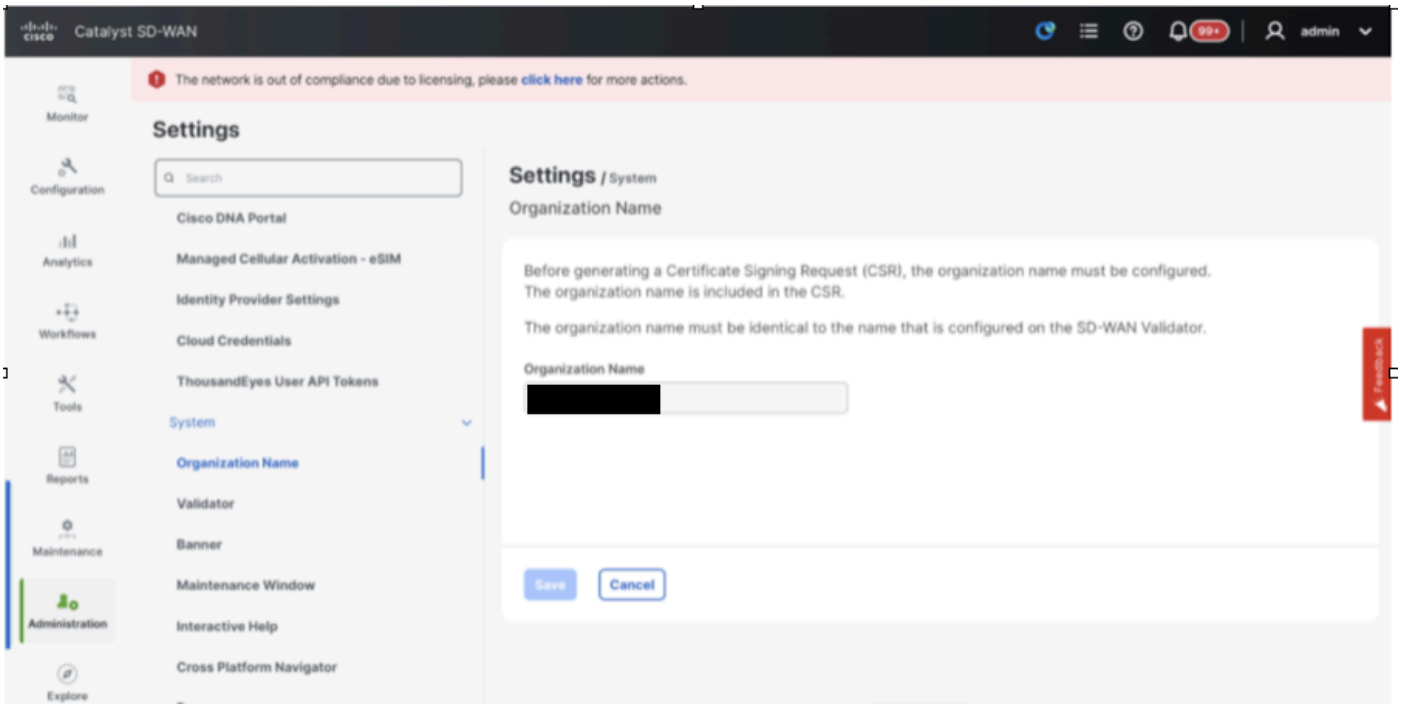
2단계: vManage UI, 인증서 및 온보드 컨트롤러 구성

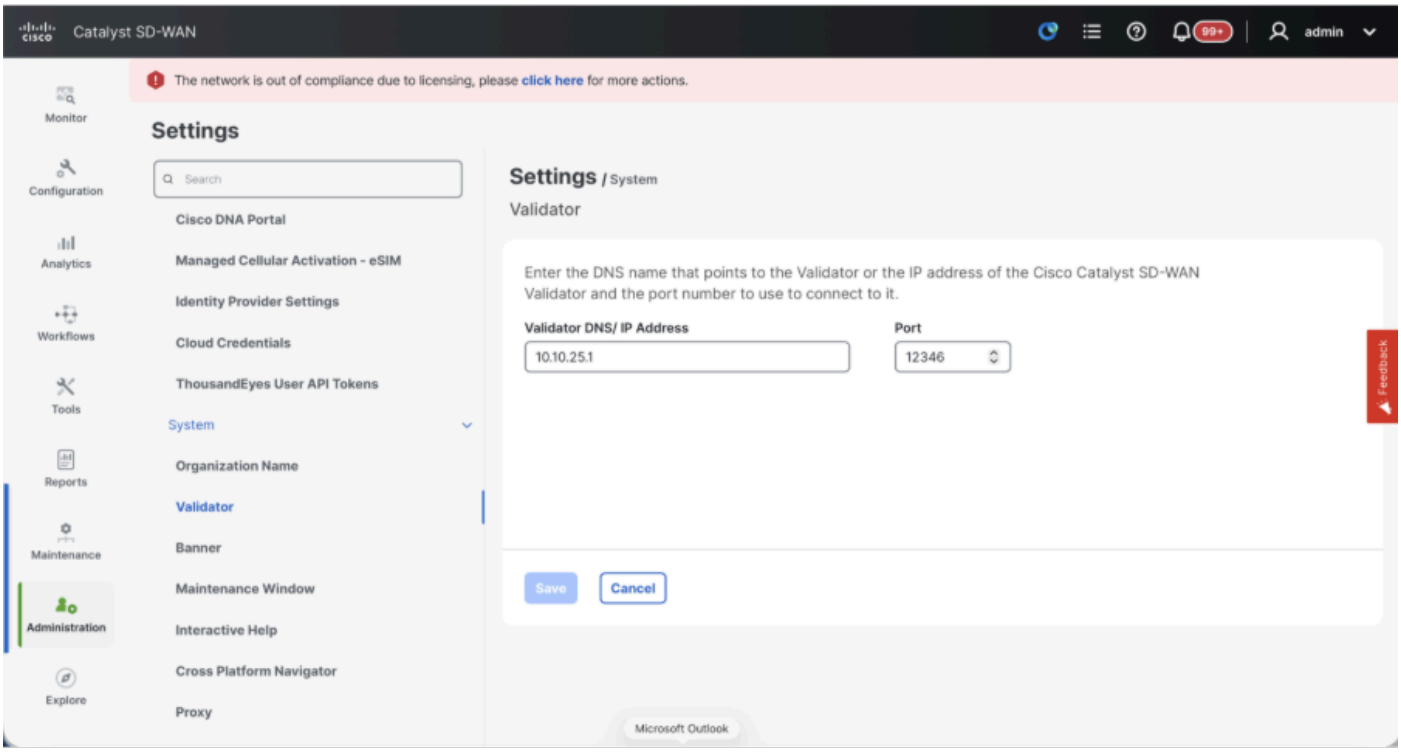
vManage UI에서 컨피그레이션 업데이트

- 1단계의 컨피그레이션이 모든 컨트롤러의 CLI에 추가되면 브라우저의 URL https://<vmanage-ip>를 사용하여 vManage의 webUI에 액세스할 수 있습니다. 각 vManage 노드의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Administration(관리) > Settings(설정)로 이동하여 다음 단계를 완료합니다.
- 조직 이름 및 검증기/vBond URL/IP 주소를 구성합니다. vManage 노드의 CLI에서와 동일한

값을 구성합니다.

- vManage 20.15/20.18의 섹션 System에서 이러한 구성을 사용할 수 있습니다.

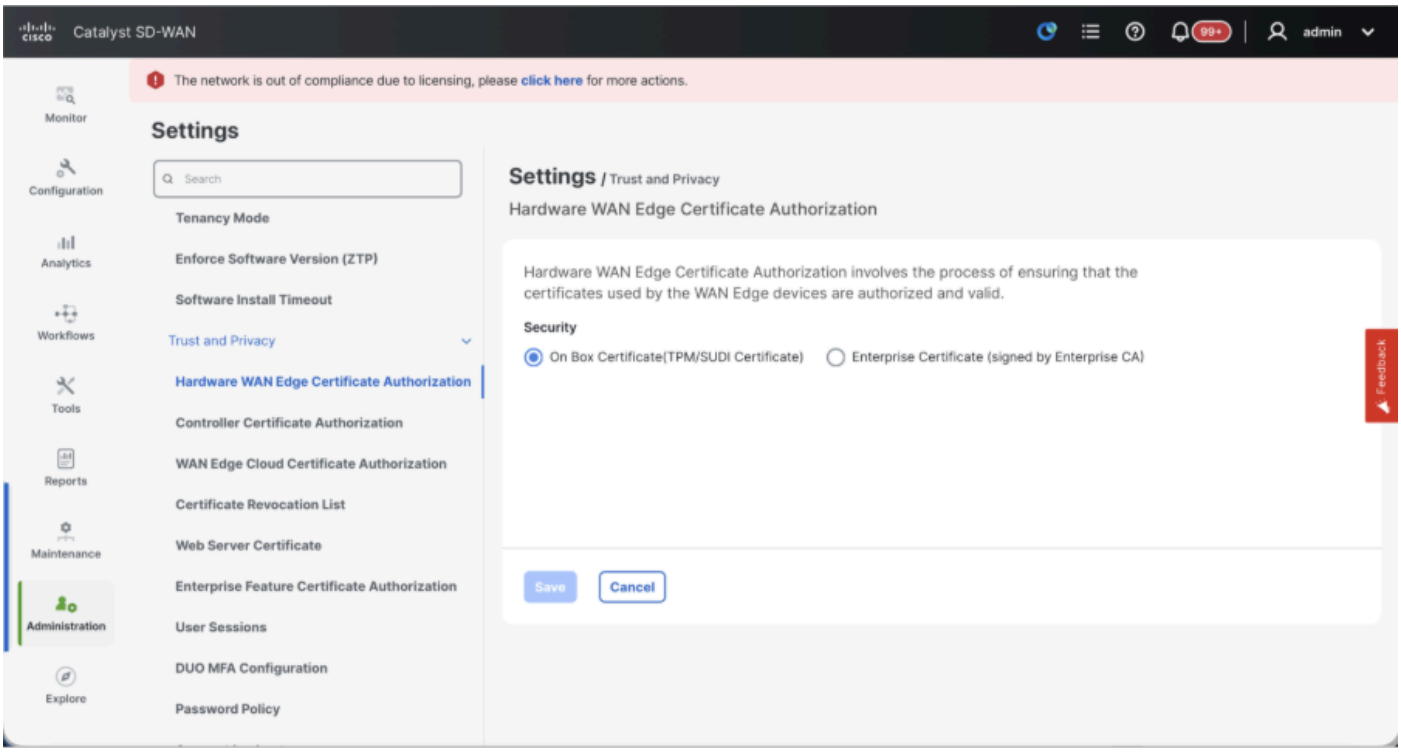




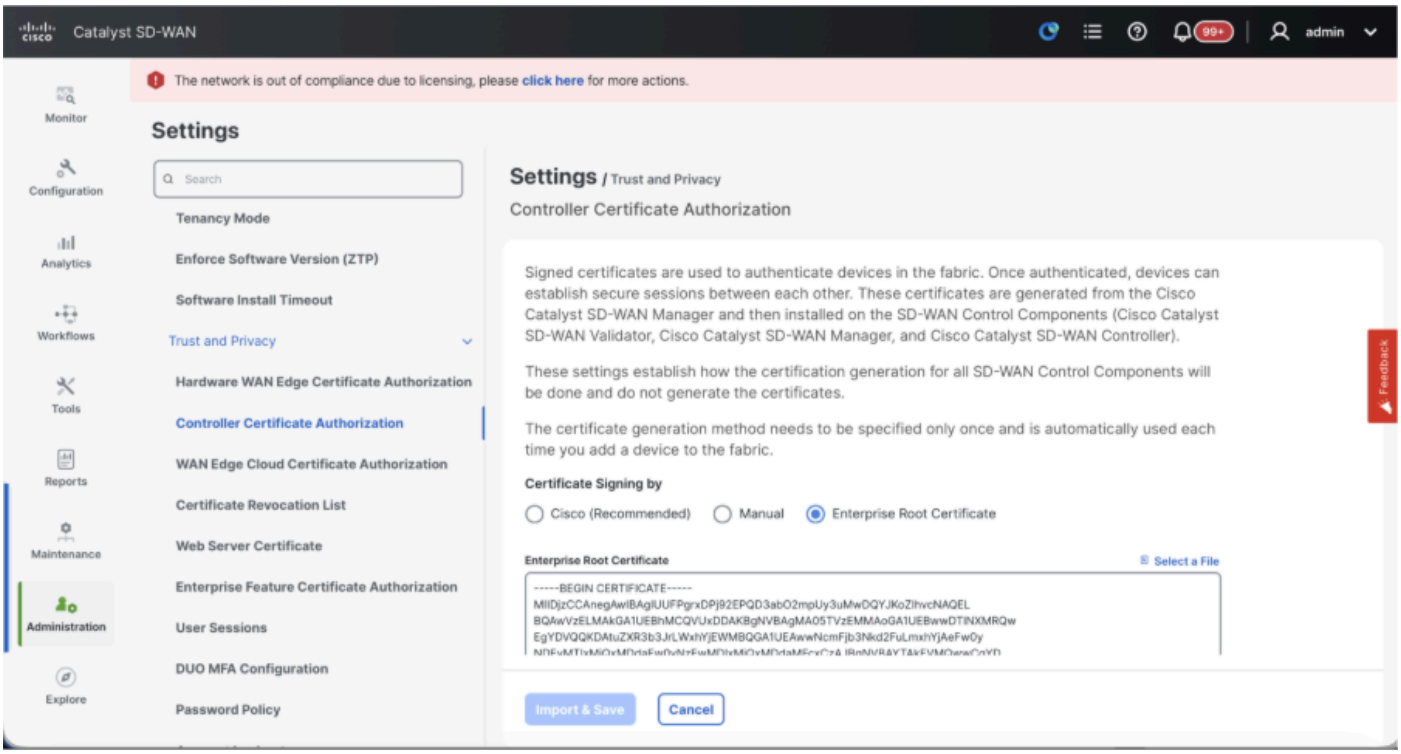
- 인증서 서명에 사용되는 인증 기관을 결정하는 CA(Certificate Authorization)의 컨피그레이션을 확인합니다. 3가지 옵션이 있습니다.

1. Hardware WAN Edge Certificate Authorization - 하드웨어 SD-WAN 에지 라우터의 CA를 결정합니다.
    - On Box Certificate(TPM/SUDI 인증서) - 이 옵션을 사용하면 라우터 하드웨어에 미리 설치된 인증서를 사용하여 제어 연결(TLS/DTLS 연결)을 설정합니다
    - 엔터프라이즈 인증서(Enterprise CA에서 서명) - 이 옵션을 사용하면 라우터가 조직의

엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

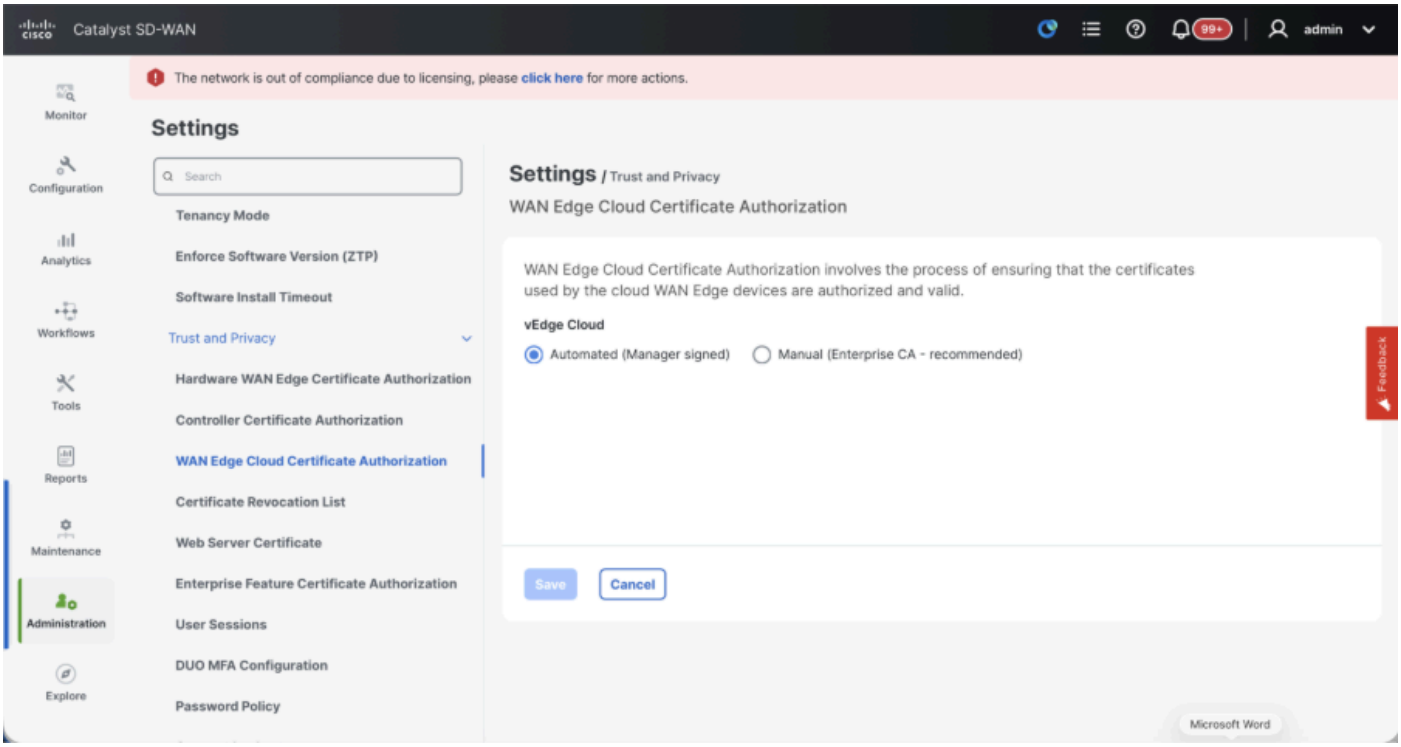


2. Controller Certificate Authorization(컨트롤러 인증서 권한 부여) - SD-WAN 컨트롤러에 대한 CA를 결정합니다.
    - Cisco(권장) - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. vManage는 vManage에 구성된 스마트 어카운트 자격 증명을 사용하여 PNP 포털에 자동으로 연결하고 서명된 인증서를 가져오며 컨트롤러에 설치됩니다.
    - 수동 - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. 각 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 수동으로 CSR에 서명합니다.
    - Enterprise Root Certificate(엔터프라이즈 루트 인증서) - 이 옵션을 사용하면 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

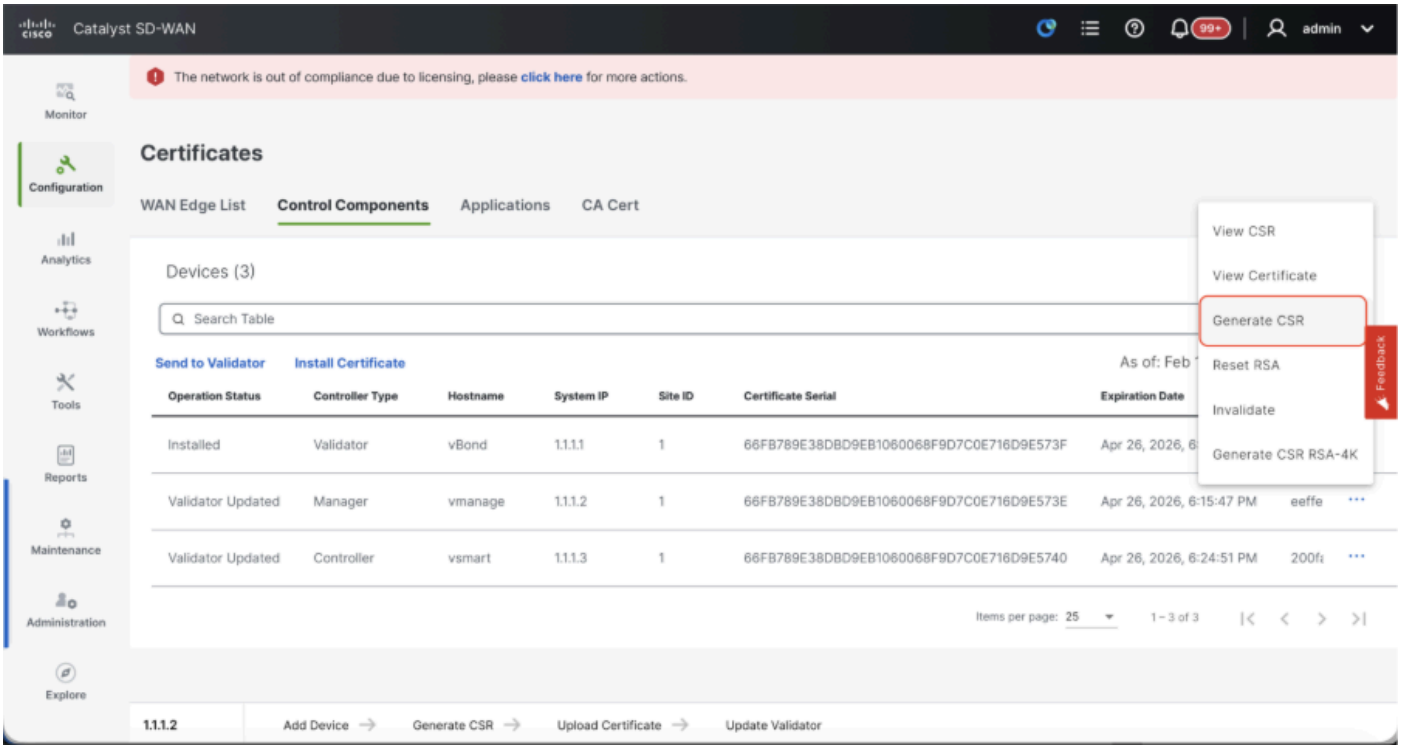


3. WAN Edge Cloud Certificate Authorization - 가상 SD-WAN Edge 라우터(CSR1000v, C8000v, vEdge 클라우드)에 대한 CA를 결정합니다.
    - 자동(vManage signed) - vManage는 가상 에지 라우터의 CSR에 자동으로 서명하고 라우터에 인증서를 설치합니다.
    - 수동(엔터프라이즈 CA - 권장) - 가상 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

자체 CA인 Enterprise Certificate Authority를 사용하는 경우 Enterprise를 선택합니다.



- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)
- Manager/vManage(관리자/vManage)에서 ...를 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

vManage에 vBond/Validator 및 vSmart/Controller 온보딩(Onboarding)

20.15/20.18 vManage 노드의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Control Components(제어 구성 요소)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

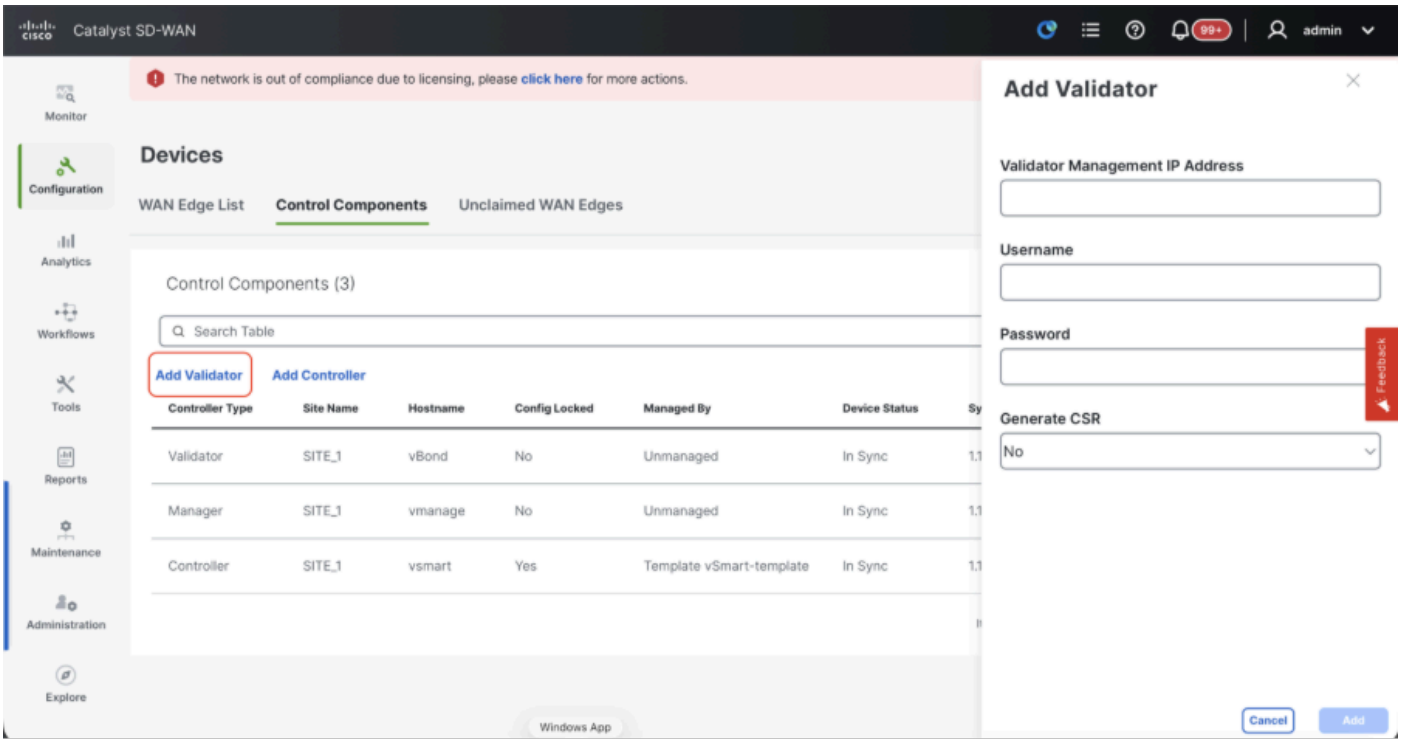
온보딩vBond/Validator

- Add(추가)VBond(vBond 추가)를 클릭합니다.제2012호의 경우유효성 검사기 추가 20.15/20.18 vManage입니다. 팝업이 열리면 vManage에서 연결할 수 있는 vBond의 VPN 0 전송 IP.
- vManagetovBondIP의 CLI에서 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.

- vBond의 사용자 자격 증명을 입력합니다.

참고: vBonor의 관리자 자격 증명 또는 netadmingroup의 사용자 부분이 필요합니다. vBond의 CLI에서 이를 확인할 수 있습니다. vBond에 대한 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다

참고: vBond가 NAT 디바이스/방화벽 뒤에 있는 경우 vBond VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인합니다. vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스의 공용 IP 주소를 사용합니다



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vBond에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vBond가 여러 개인 경우 동일한 단계를 반복합니다.

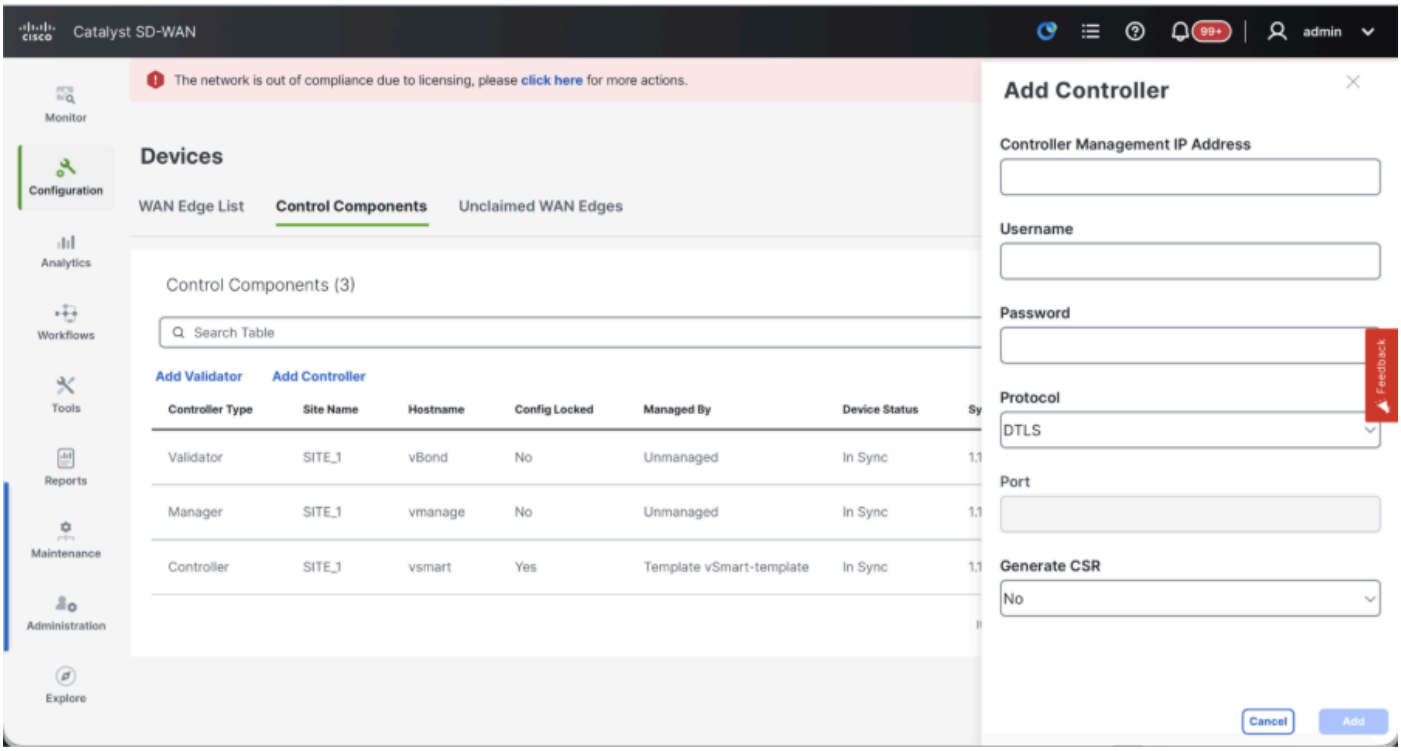
vSmart/컨트롤러 온보딩

- 20.12 vManage의 경우 vSmart 추가 또는 20.15/20.18 vManage의 경우 컨트롤러 추가를 클

릭합니다.

- 팝업이 열리면 vManage에서 연결할 수 있는 vSmart의 VPN 0 전송 IP를 입력합니다.
- vManage의 CLI에서 vSmart IP로 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.
- vSmart의 사용자 자격 증명을 입력하십시오. vSmart의 관리자 자격 증명 또는 netadmin 그룹의 사용자 부분을 사용해야 합니다.
- vSmart의 CLI에서 이를 확인할 수 있습니다.
- 라우터에 TLS를 사용하여 vSmart와의 제어 연결을 설정하려면 프로토콜을 TLS로 설정합니다. vSmarts 및 vManage 노드의 CLI에서도 이 구성을 구성해야 합니다.
- vSmart용 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다.

참고: vSmart가 NAT 장치/방화벽 뒤에 있는 경우 vSmart VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인하고, vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스 IP의 공용 IP 주소를 사용합니다.



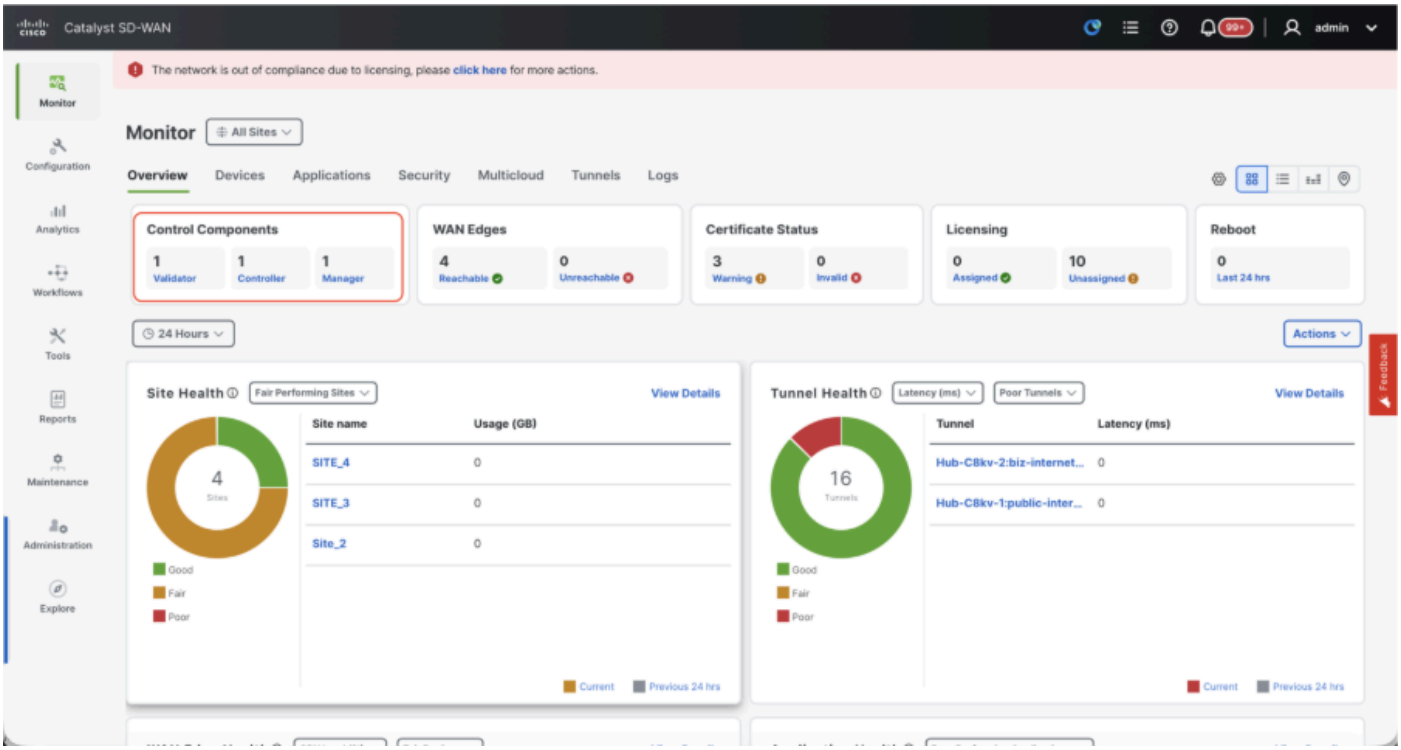
- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vSmart에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. Digicert 및 Enterprise

Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

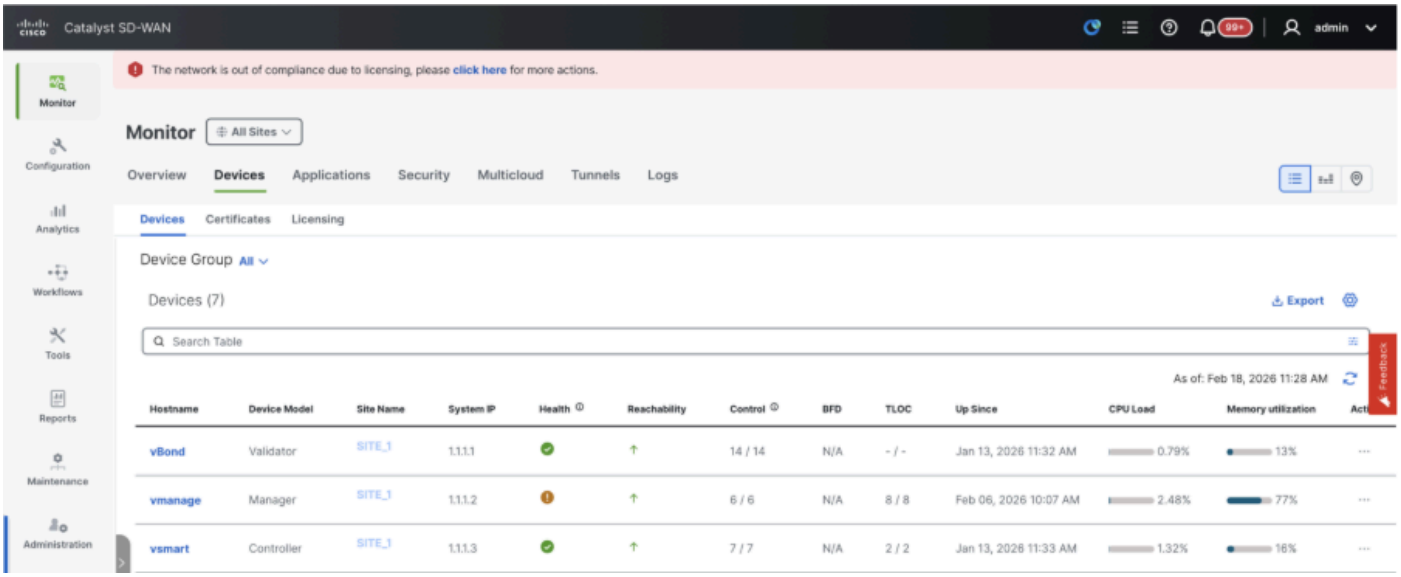
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- vSmarts가 여러 개인 경우 동일한 단계를 반복합니다.

확인

모든 단계가 완료되면 Monitor>Dashboard에서 모든 제어 구성 요소에 연결할 수 있는지 확인합니다



- 각 Control(제어) 구성 요소를 클릭하고 모두 연결할 수 있는지 확인합니다.
- Monitor(모니터링) > Devices(디바이스)로 이동하여 모든 제어 구성 요소에 연결할 수 있는지 확인합니다.



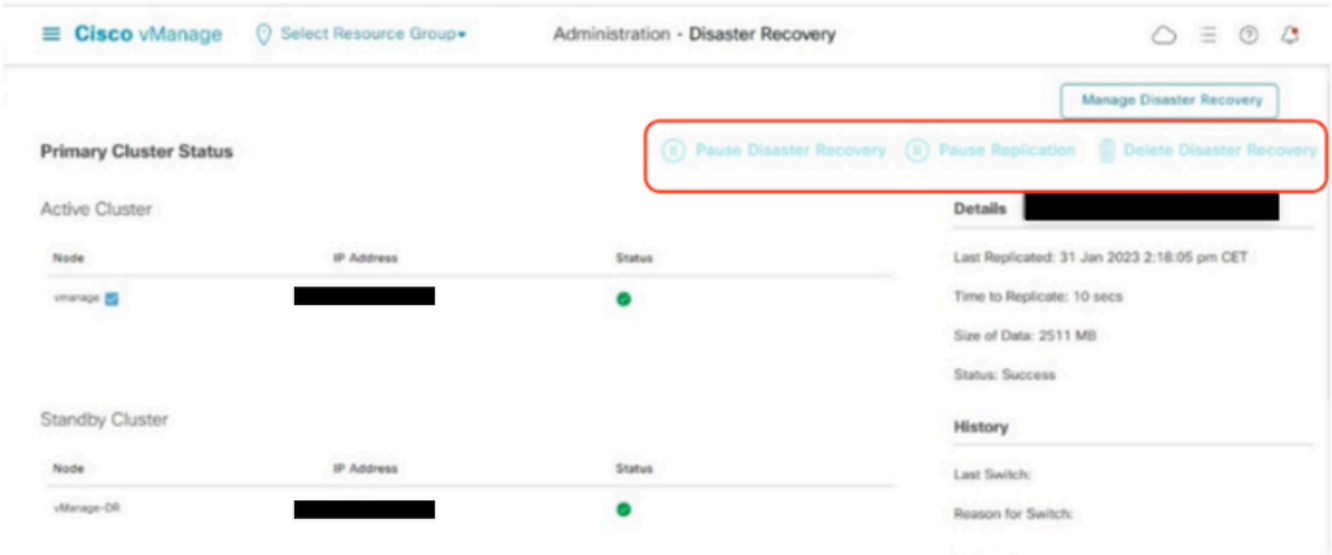
3단계: Config-db 백업/복원

다른 vManage 노드에서 vManage configuration-db 백업 및 복원 수집

참고: 재해 복구가 활성화된 기존 vManage 노드에서 컨피그레이션 데이터베이스 백업을 수집하는 동안 해당 노드의 재해 복구가 일시 중지되고 삭제된 후에 수집되어야 합니다.

진행 중인 재해 복구 복제가 없는지 확인합니다. Administration(관리) > Disaster Recovery(재해 복구) 및 상태가 Success(성공)이고 Import Pending(가져오기 보류 중), Export Pending(내보내기 보류 중) 또는 Download Pending(다운로드 보류 중)과 같은 일시적인 상태가 아닌지 확인합니다. 상태가 성공적이지 않으면 Cisco TAC에 문의하여 복제가 성공적인지 확인한 후 재해 복구를 일시 중지합니다.

먼저 재해 복구를 일시 중지하고 작업이 완료되었는지 확인합니다. 그런 다음 재해 복구를 삭제하고 작업이 완료되었는지 확인합니다.



Cisco TAC에 문의하여 재해 복구가 성공적으로 정리되었는지 확인합니다.

Configuration-DB 백업 수집:

- 현재 사용 중인 SD-WAN 패브릭에서는 독립형 vManage 및 vManage 클러스터 설정 모두에서 컨피그레이션 DB 백업을 생성할 수 있습니다.
- 독립형 vManage의 경우 해당 vManage 자체가 configuration-db 리더입니다.

vManage 노드에서 configuration-db가 실행 중인지 확인합니다.

commandrequest nms configuration-db statusonvManageCLI를 사용하여 이를 확인할 수 있습니다. 출력은 다음과 같습니다

```
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#
```

식별된 configuration-db leader vManage 노드에서 configuration-db 백업을 수집하려면 이 명령을 사용합니다.

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

예상 출력은 다음과 같습니다.

```
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#
```

- 컨피그레이션 DB 자격 증명이 업데이트된 경우 기록해 둡니다.
- configuration-db 자격 증명을 모르는 경우 TAC에 문의하여 기존 vManage 노드에서 configuration-db 자격 증명을 검색합니다.
- 기본 configuration-db 자격 증명은 사용자 이름입니다. neo4j 및 비밀번호: 암호

다른 vManage 노드에 Configuration-db 백업 복원

SCP를 사용하여 configuration-db 백업을 vManage의 /home/admin/ 디렉토리에 복사합니다.

샘플 scp 명령 출력:

```
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 백업을 복원하려면 먼저 configuration-db 자격 증명을 구성해야 합니다. configuration-db 자격 증명이 default(neo4j/password)인 경우 이 단계를 건너뛸 수 있습니다.

configuration-db 자격 증명을 구성하려면 nms configuration-db update-admin-user 명령을 사용합니다.선택한 사용자 이름과 비밀번호를 사용합니다.

vManage의 애플리케이션 서버가 다시 시작됩니다. 따라서 vManage UI에 짧은 시간 동안 액세스할 수 없게 됩니다.

```
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#
```

구성 DB 백업을 복원하기 위해 진행할 수 있는 게시:

nms configuration-db 복원 경로 /home/admin/< > 명령을 사용하여 configuration-db를 새 vManage로 복원할 수 있습니다.

```
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-db가 복원되면 vManage UI에 액세스할 수 있는지 확인합니다. 약 5분 정도 기다린 후 UI에 액세스를 시도합니다.

UI에 성공적으로 로그인했으면 Edge 라우터 목록, 템플릿, 정책 및 이전 또는 기존 vManage UI에 존재했던 나머지 모든 컨피그레이션이 새 vManage UI에 반영되었는지 확인합니다.

4단계: 단일 노드 DR 설정

2단계를 참조하십시오: 조합 2의 사전 검사: 독립형 vManage + 단일 노드 DR을 사용하고 재해 복구를 활성화하기 전에 모든 요구 사항을 완료했는지 확인합니다.

단일 노드 DR

사전 요구 사항

- 전송 VPN(VPN 0)에서 HTTPS를 통해 기본 및 보조 노드에 연결할 수 있는지 확인합니다.
- Cisco vManage 기본 노드 및 보조 노드에서 동일한 Cisco vManage 버전을 실행하고 있는지 확인합니다.

VPN 0의 대역 외 클러스터 인터페이스

1. 클러스터 내의 각 vManage 인스턴스에는 VPN 0(전송) 및 VPN 512(관리)에 사용되는 인터페이스 외에 세 번째 인터페이스(클러스터 링크)가 필요합니다.
2. 이 인터페이스는 클러스터 내에서 vManage 서버 간의 통신 및 동기화에 사용됩니다.
3. 이 인터페이스는 1Gbps 이상이어야 하며 지연 시간은 4ms 이하여야 합니다. 10Gbps 인터페이스를 사용하는 것이 좋습니다.
4. 두 vManage 노드는 다음 인터페이스를 통해 서로 연결할 수 있어야 합니다. 레이어 2 세그먼트 또는 레이어 3 라우팅을 통해 제공되어야 합니다.

- 모든 서비스(application-server, configuration-db, messaging server, coordination server 및 statistics-db)가 두 Cisco vManage 노드에서 모두 활성화되었는지 확인합니다.
- Cisco vBond Orchestrator를 비롯한 모든 컨트롤러를 기본 및 보조 데이터 센터 전체에 배포합니다. 이러한 데이터 센터에 분산된 Cisco vManage 노드에서 이러한 컨트롤러에 연결할 수 있는지 확인합니다. 컨트롤러는 기본 Cisco vManage 노드에만 연결됩니다.
- 활성(기본) 및 대기(보조) Cisco vManage 노드에서 다른 작업이 진행 중이 아닌지 확인합니다. 예를 들어, 업그레이드 중인 서버가 없는지 또는 디바이스에 템플릿을 연결하는 중인 템플릿이 없는지 확인합니다.

- 활성화된 경우 Cisco vManage HTTP/HTTPS 프록시 서버를 비활성화합니다. 프록시 서버를 비활성화하지 않으면 Cisco vManage는 Cisco vManage 대역외 클러스터 IP 주소에 직접 연결할 수 있는 경우에도 프록시 IP 주소를 통해 재해 복구 통신을 설정하려고 시도합니다. 재해 복구 등록이 완료된 후 Cisco vManage HTTP/HTTPS 프록시 서버를 다시 활성화할 수 있습니다.

- 재해 복구 등록 프로세스를 시작하기 전에 기본 Cisco vManage 노드의 Tools → Rediscover Network 창으로 이동하여 Cisco vBond Orchestrator를 다시 검색합니다.

설정

재해 복구 노드로 작동하는 모든 vManage 노드의 CLI 컨피그레이션을 구성합니다

vManage의 최소 구성은재해 복구 등록 전의 상태는 다음과 같습니다

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

참고: URL을 vBond 주소로 사용하는 경우 VPN 0 컨피그레이션에서 DNS 서버 IP 주소를 구성하거나 확인할 수 있는지 확인하십시오.

이러한 컨피그레이션은 라우터 및 나머지 컨트롤러와의 제어 연결을 설정하는 데 사용되는 전송 인터페이스를 활성화하는 데 필요합니다

```
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
```

컨트롤러에 대한 대역 외 관리 액세스를 활성화하도록 VPN 512 관리 인터페이스도 구성합니다.

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

```
  no shutdown
 !
 ip route 0.0.0.0/0




!
commit
```

DR vManage에서 서비스 인터페이스 구성

vManage 노드에서 서비스 인터페이스를 구성합니다. 이 인터페이스는 DR 통신에 사용됩니다.

```
conf t
 interface eth2
  ip address



  no shutdown
commit
```

기본 vManage 및 DR vManage의 서비스 인터페이스에 동일한 IP 서브넷이 사용되는지 확인합니다

vManage UI에서 컨피그레이션 업데이트

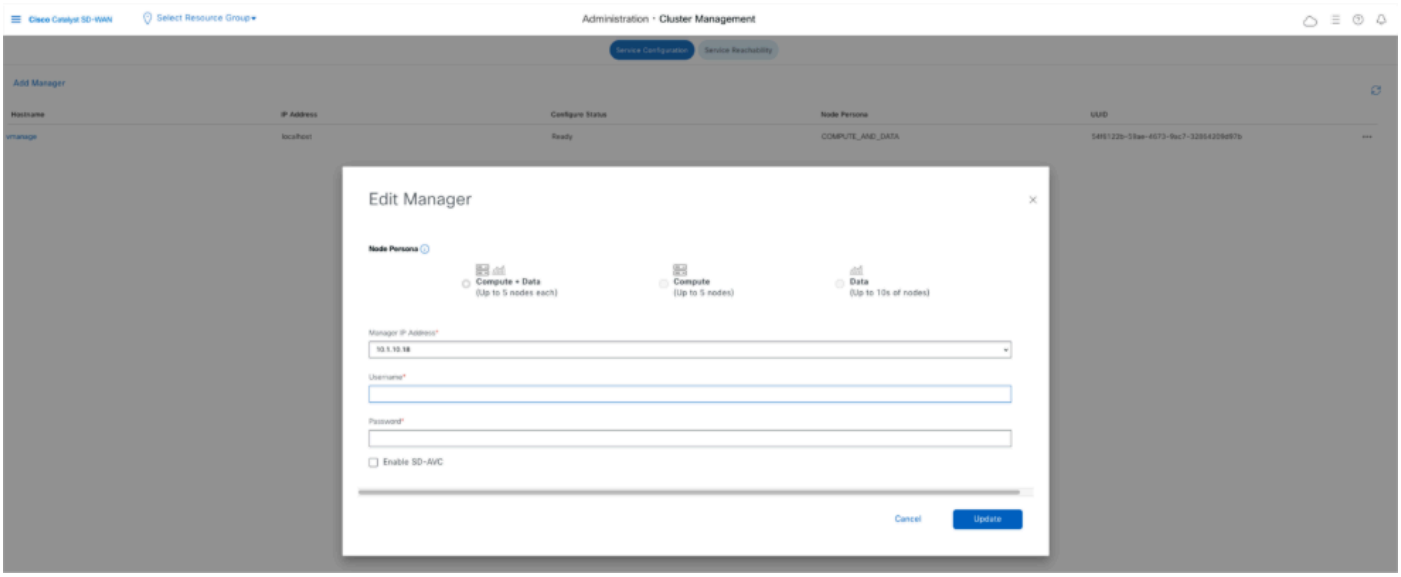
- 모든 컨트롤러의 CLI에 컨피그레이션이 추가되면 브라우저의 URL https://<vmanage-ip>를 사용하여 vManage의 webUI에 액세스할 수 있습니다. 각 vManage 노드의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Administration(관리) > Settings(설정)로 이동하여 다음 단계를 완료합니다.
- 조직 이름을 구성합니다. vManage 노드의 CLI에서와 동일한 값을 구성합니다.
- vManage 20.15/20.18의 섹션 System에서 이러한 구성을 사용할 수 있습니다.

DR vManage에 인증서 설치

섹션 조합 2에 제시된 단계를 진행합니다. 독립형 vManage + 단일 노드 DR 3단계: 재해 복구 vManage에 인증서를 설치하기 위해 vManage UI, 인증서 및 온보드 컨트롤러를 구성합니다.

재해 복구 구성 추가

- 이를 위해 기본 vManage로 이동합니다.
- Administration(관리) → Cluster Management(클러스터 관리)로 이동하고 vManage 항목의 오른쪽에 있는 세 개의 점을 클릭한 후 사용자 이름과 비밀번호를 포함하여 대역 외 인터페이스의 IP 주소를 지정합니다. 이 컨피그레이션의 경우 기본 및 DR vmanage 둘 다에 별도의 로컬 사용자(예: dradmin)를 생성하는 것이 좋습니다.



- 이 변경 후 VManage가 재부팅됩니다.
- Primary vManage(기본 vManage)가 나타나면 Administration(관리) → Disaster Recovery(재해 복구)로 이동합니다. 'Manage Disaster Recovery'를 클릭합니다.
- 팝업 창에서 기본 및 보조 vManage의 세부사항을 모두 입력합니다.
- 표시할 IP 주소는 대역 외 클러스터 인터페이스(eth2) IP 주소입니다.
- 자격 증명은 netadmin 사용자(dradmin)의 자격 증명이어야 하며 DR이 구성된 후에는 변경할 수 없습니다. 재해 복구용 별도의 vManage 로컬 사용자 자격 증명을 사용할 수 있습니다. vManage 로컬 사용자가 netadmin 그룹의 일부인지 확인해야 합니다. 관리자 자격 증명도 여기에서 사용할 수 있습니다.

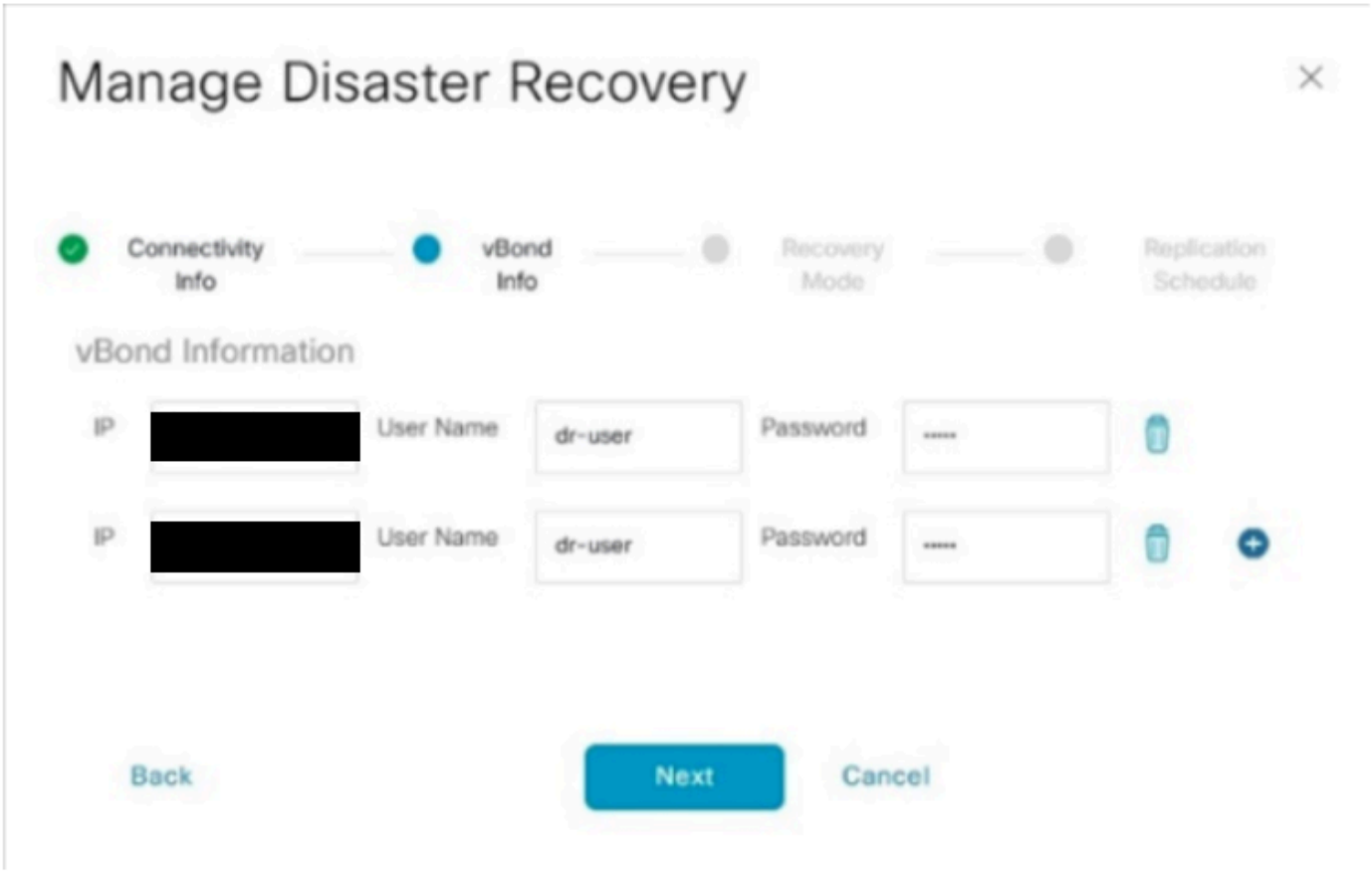
- 입력을 마쳤으면 'Next(다음)'를 클릭합니다.

- vBond 컨트롤러의 세부사항을 입력합니다.

- vBond 컨트롤러는 지정된 IP 주소에서 Netconf를 통해 연결할 수 있어야 합니다.

- 자격 증명은 netadmin 사용자(dradmin)의 자격 증명이어야 하며 DR이 구성된 후에는 변경할 수 없습니다.

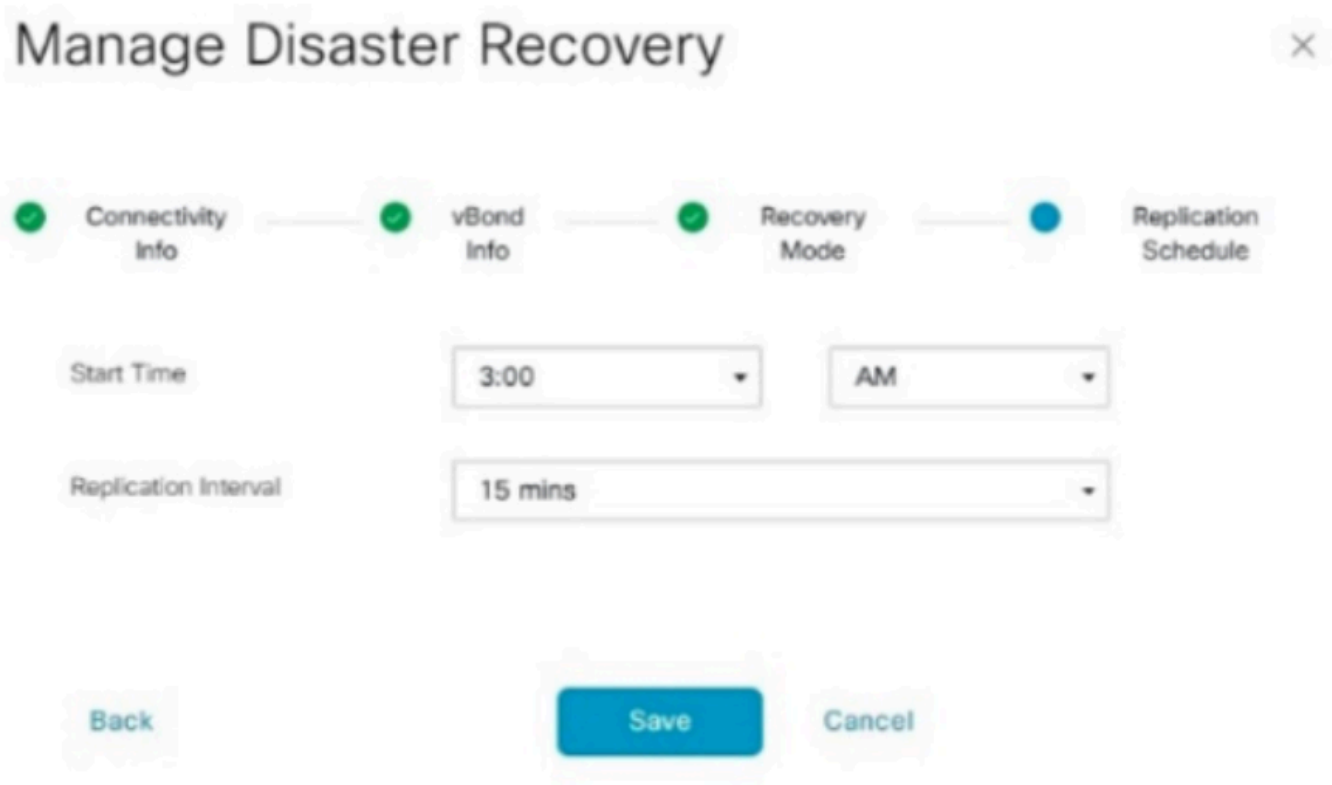
- 이를 위해서는 vBond에서 이 dradmin 사용자를 로컬로 구성하거나 admin 사용자를 사용하여 vBond를 추가할 수 있습니다.



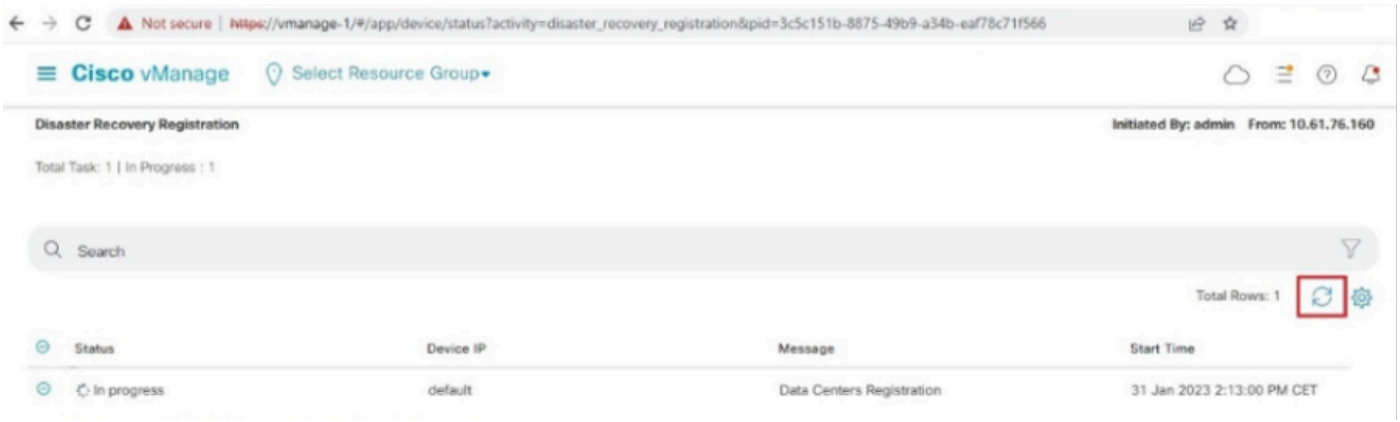
- 입력을 마쳤으면 'Next(다음)'를 클릭합니다.
- 복구 모드에서 '수동'을 선택하고 '다음'을 클릭합니다.

Replication Schedule(복제 일정)에서 'Replication Interval(복제 간격)'을 설정합니다'.복제 간격 시간마다 데이터는 운영 시스템에서 복제됩니다. vManagto 보조 vManage. 최소 구성 가능 값은 15분

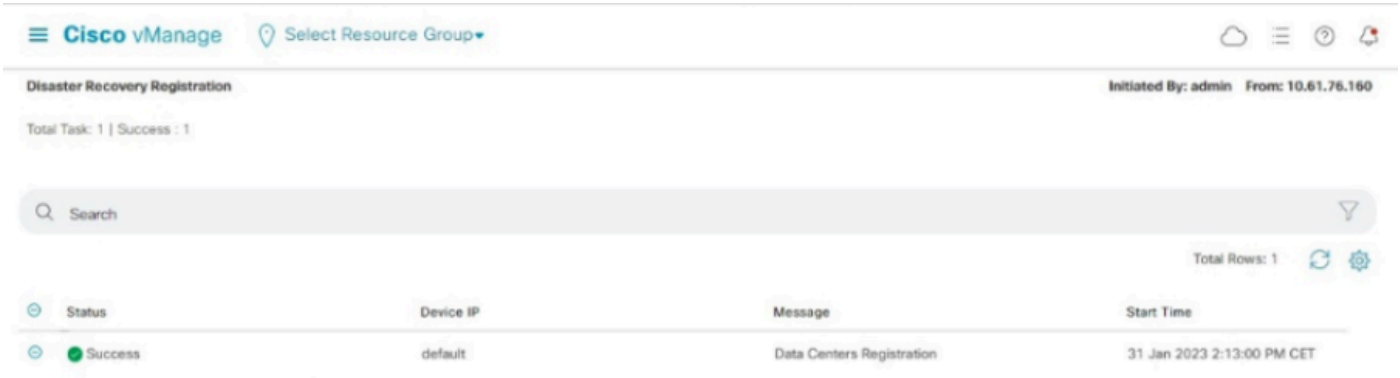
입니다.



- 값을 설정하고 'Save'를 클릭합니다.
- 이제 DR 등록이 시작됩니다. 상태 및 진행 로그를 수동으로 새로 고치려면 새로 고침 버튼을 클릭합니다. 이 프로세스는 최대 20-30분이 소요될 수 있습니다.

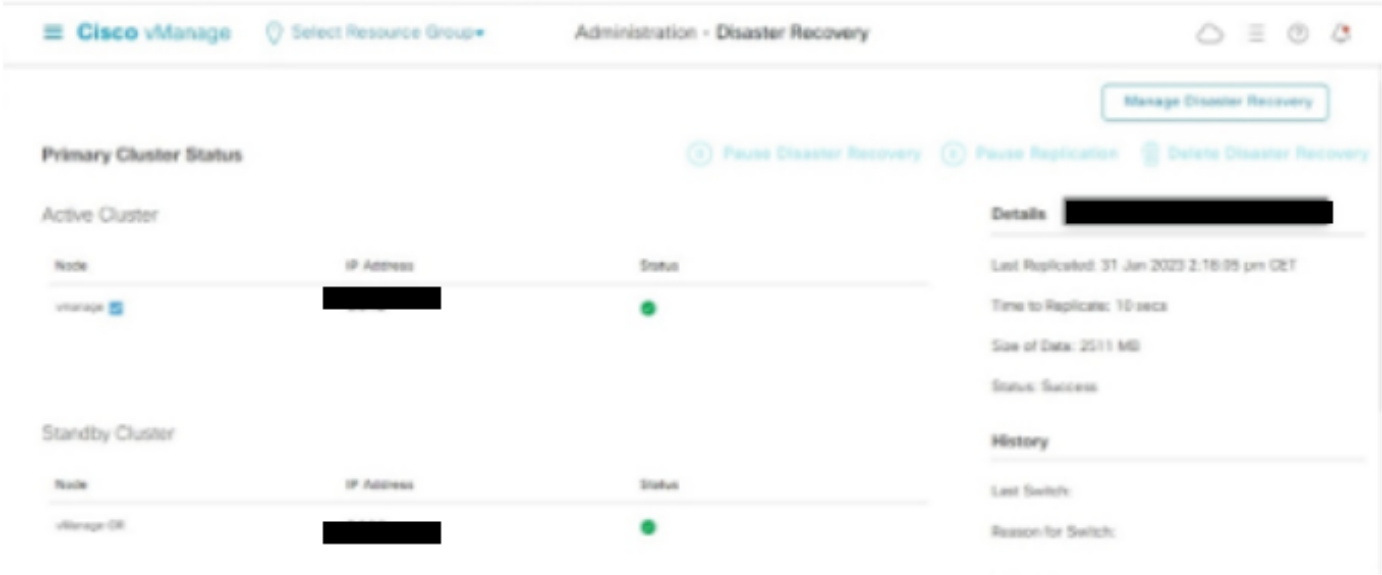


- 이 프로세스 중에 vManage GUI가 다시 시작됩니다.
- 작업을 마치면 성공 상태가 표시되어야 합니다.



다음을 확인합니다.

Administration(관리) → Disaster Recovery(재해 복구)로 이동합니다.재해 복구 상태 및 마지막으로 데이터가 복제된 시간을 확인합니다.



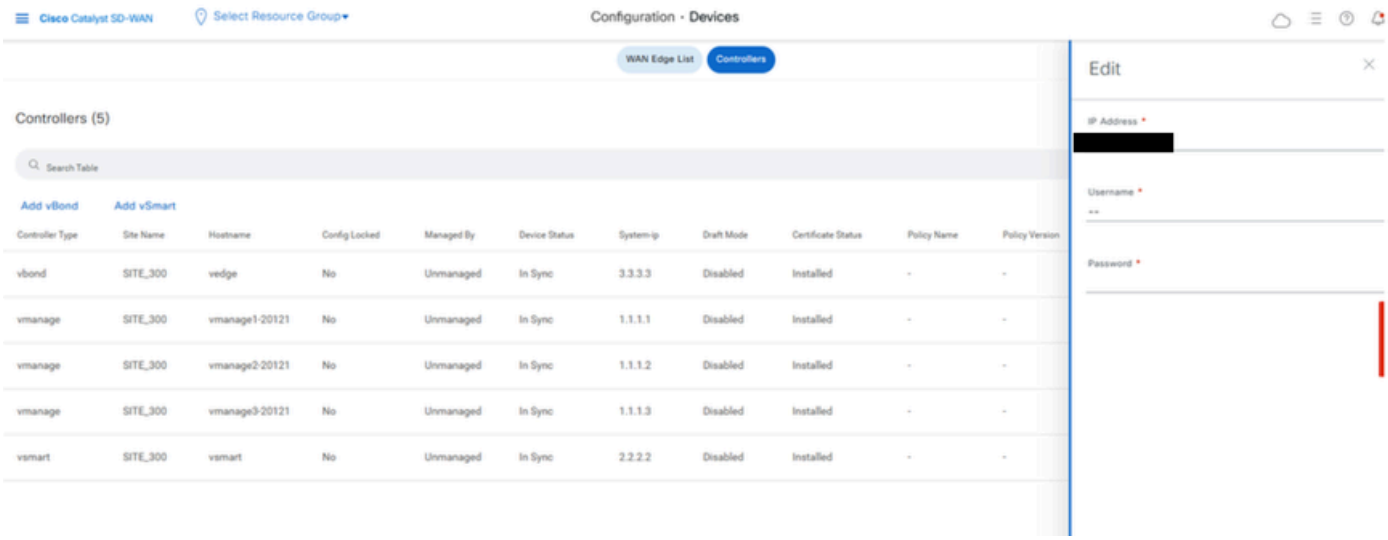
5단계: 컨트롤러 재인증 및 이전 컨트롤러 무효화

configuration-db가 복원되면 패브릭에서 모든 새 컨트롤러(vmanage/vsmart/vbond)를 재인증해야 합니다

참고: 실제 프로덕션에서는 재인증에 사용되는 인터페이스 IP가 터널 인터페이스 IP인 경우 vManage, vSmart 및 vBond의 터널 인터페이스 및 경로에 따른 방화벽에서 NETCONF 서비스가 허용되는지 확인해야 합니다. 열 방화벽 포트는 DR 클러스터에서 모든 vBonds 및 vSmarts로의 양방향 규칙인 TCP 포트 830입니다.

vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다

- 각 컨트롤러 근처의 점 3개를 클릭하고 Edit(수정)를 클릭합니다



- ip-address(컨트롤러의 system-ip)를 transport vpn 0(tunnel interface) ip 주소로 바꿉니다. 사용자 이름과 암호를 입력하고 save(저장)를 클릭합니다
- 패브릭에 있는 모든 새 컨트롤러에 대해 동일한 작업을 수행합니다.

루트 인증서 체인 동기화

모든 컨트롤러가 온보딩되면 다음 단계를 완료합니다.

새로 활성화된 클러스터의 Cisco SD-WAN Manager 서버에서 다음 작업을 수행합니다.

루트 인증서를 새로 활성화된 클러스터의 모든 Cisco Catalyst SD-WAN 디바이스와 동기화하려면 다음 명령을 입력합니다.

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

Cisco SD-WAN Manager UUID를 Cisco SD-WAN Validator와 동기화하려면 다음 명령을 입력합니다.

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

패브릭이 복원되고 패브릭의 모든 에지와 컨트롤러에 대해 제어 및 bfd 세션이 작동되면 UI에서 이전 컨트롤러(vmanage/vsmart/vbond)를 무효화해야 합니다

- vmanage UI에서 Configuration > Devices > Certificates를 클릭합니다
- Controllers(컨트롤러) 클릭
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. Invalidate를 클릭합니다.
- Send to Bond를 클릭합니다.
- vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. 삭제를 클릭합니다.

6단계: 수표 게시

참고: 여기에 표시된 모든 구축 조합에 공통적으로 적용되는 Post Checks(사후 검사) 섹션을 계속 진행합니다.

조합 3: vManage 클러스터 + DR 없음

필요한 인스턴스:

- 3 vManage(3노드 클러스터, 모든 COMPUTE_AND_DATA) 또는 6 vManage(3 COMPUTE_AND_DATA + 3 DATA)
- vBond 1개 이상
- vSmart 1개 이상

단계:

1. 공통 단계를 사용하여 모든 인스턴스 가져오기
2. 사전 확인
3. vManage UI, 인증서 및 온보드 컨트롤러 구성
4. vManage 클러스터 구축
5. Config-db 백업/복원
6. 수표 게시

1단계: 사전 확인

- 활성 Cisco SD-WAN Managerinstances의 수가 새로 설치된 Cisco SD-WAN Managerinstances의 수와 동일한지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 동일한 소프트웨어 버전을 실행하는지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 Cisco SD-WAN Validator의 관리 IP 주소에 연결할 수 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스에 인증서가 설치되어 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스를 포함하여 모든 Cisco Catalyst SD-WAN 디바이스의 시계가 동기화되었는지 확인합니다.
- 새 시스템 IP 및 사이트 ID 집합이 활성 클러스터와 동일한 기본 구성과 함께 새로 설치된 Cisco SD-WAN Manager 인스턴스에 구성되어 있는지 확인합니다.

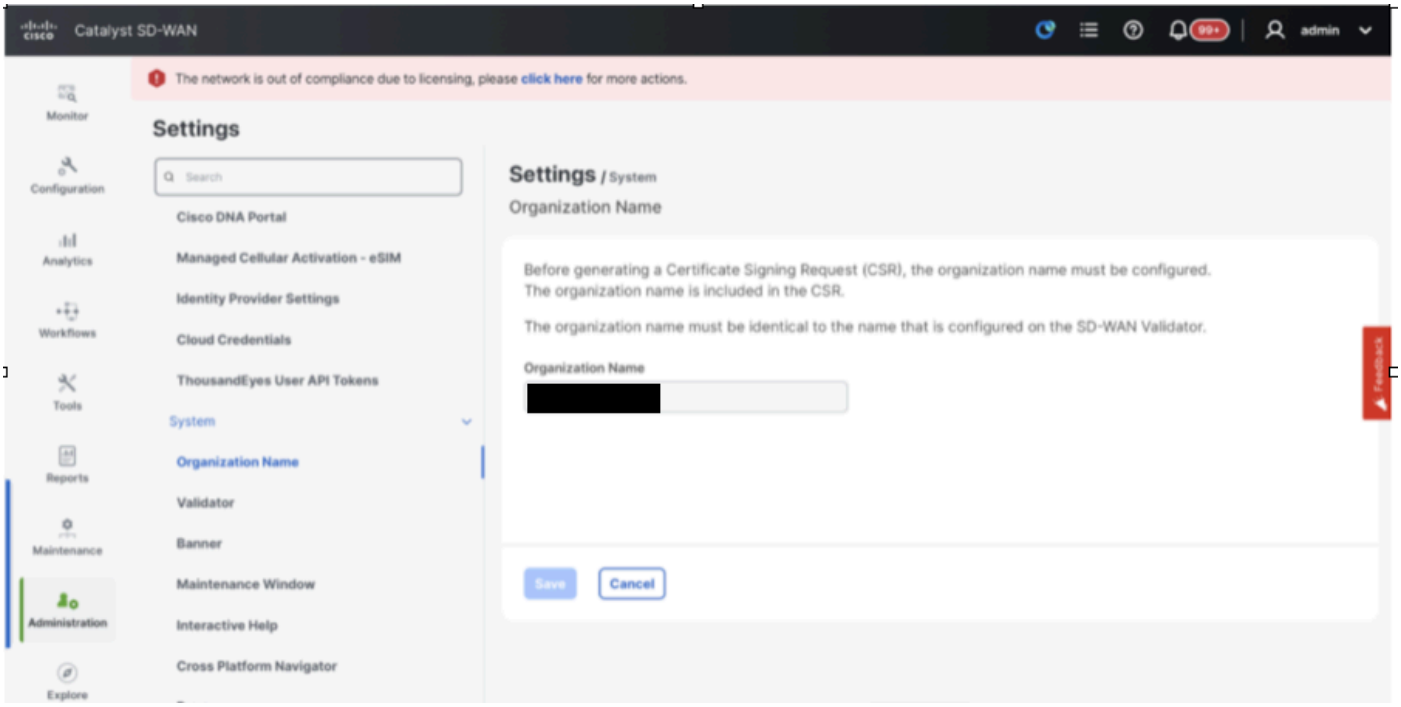
2단계: vManage UI, 인증서 및 온보드 컨트롤러 구성

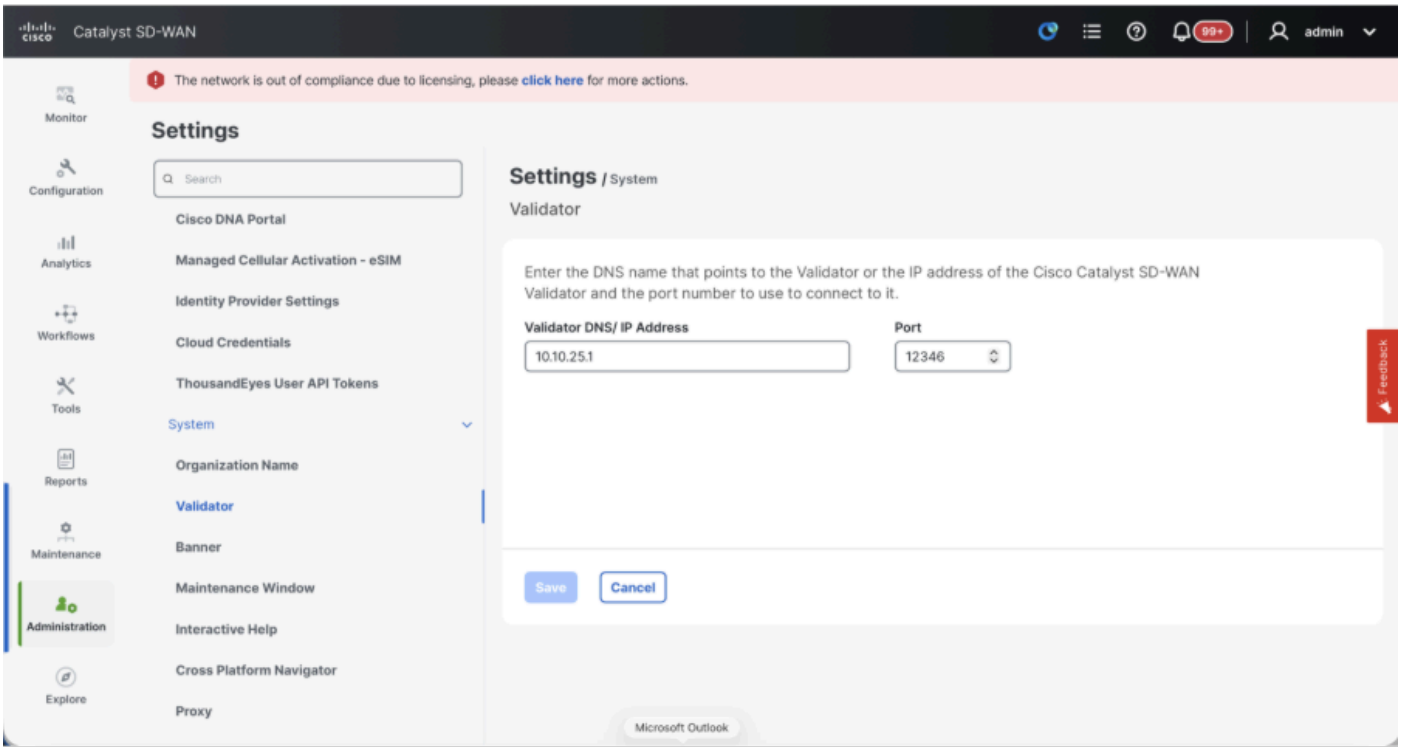
vManage UI에서 컨피그레이션 업데이트

- 1단계의 컨피그레이션이 모든 컨트롤러의 CLI에 추가되면 브라우저의 URL

https://<vmanage-ip>를 사용하여 vManage의 webUI에 액세스할 수 있습니다. 각 vManage 노드의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.

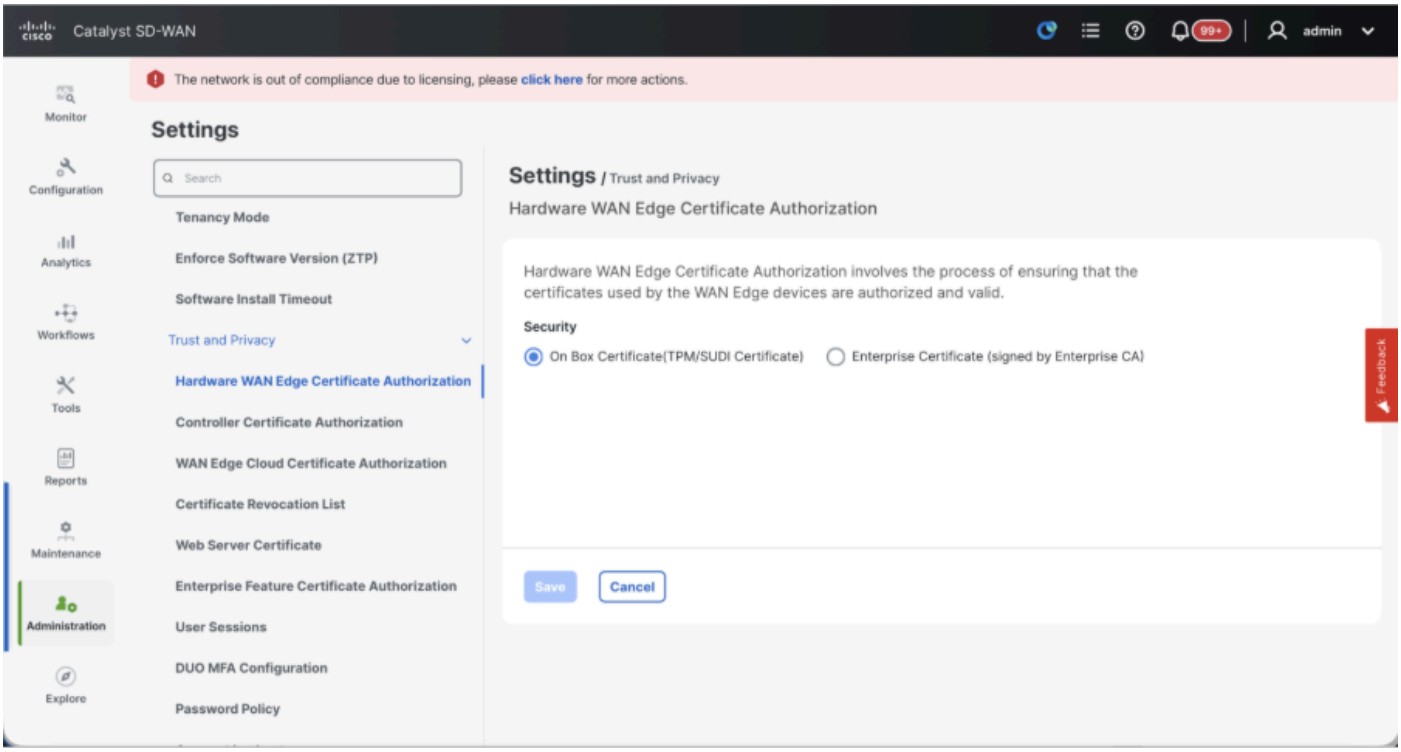
- Administration(관리) > Settings(설정)로 이동하여 다음 단계를 완료합니다.
- 조직 이름 및 검증기/vBond URL/IP 주소를 구성합니다. vManage 노드의 CLI에서와 동일한 값을 구성합니다.
- vManage 20.15/20.18의 섹션 System에서 이러한 구성을 사용할 수 있습니다.



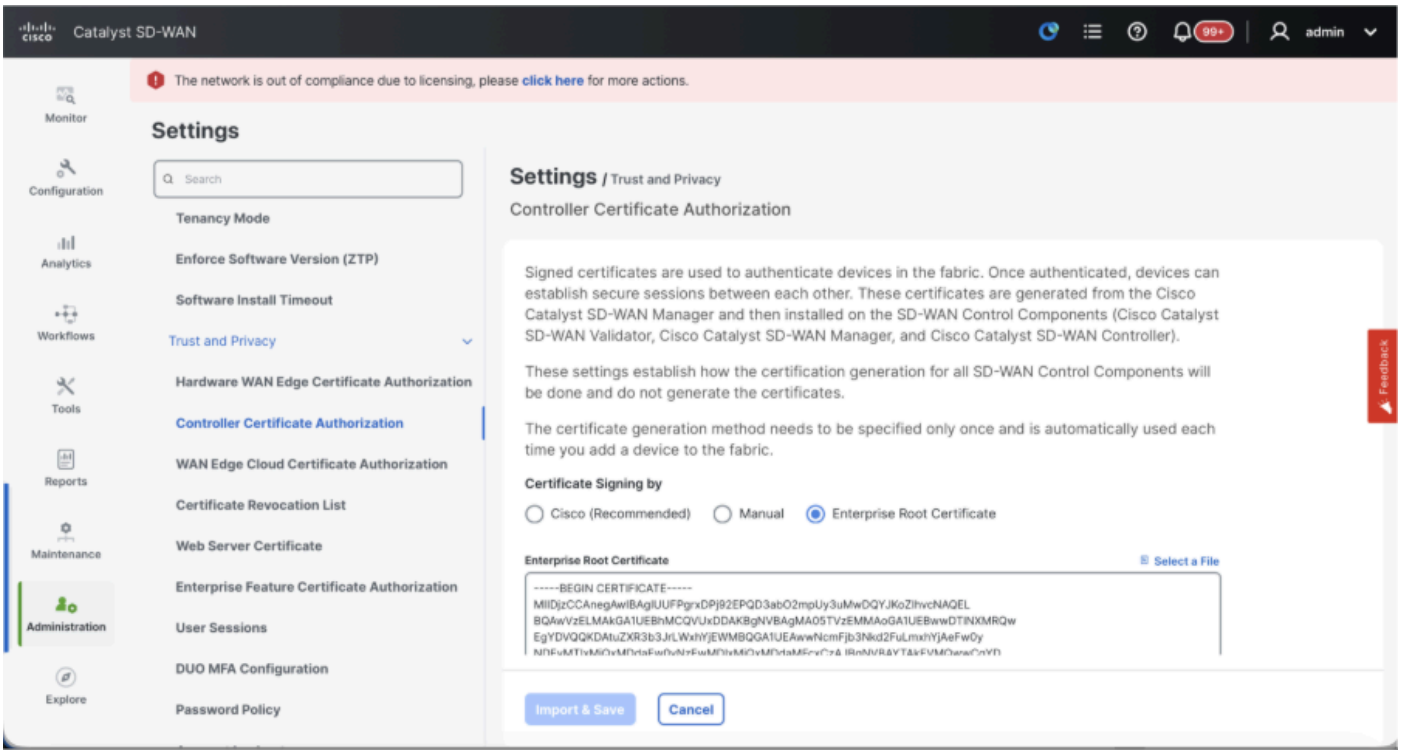


- 인증서 서명에 사용되는 인증 기관을 결정하는 CA(Certificate Authorization)의 컨피그레이션을 확인합니다. 3가지 옵션이 있습니다.

1. Hardware WAN Edge Certificate Authorization - 하드웨어 SD-WAN 에지 라우터의 CA를 결정합니다.
    - On Box Certificate(TPM/SUDI 인증서) - 이 옵션을 사용하면 라우터 하드웨어에 미리 설치된 인증서를 사용하여 제어 연결(TLS/DTLS 연결)을 설정합니다
    - 엔터프라이즈 인증서(Enterprise CA에서 서명) - 이 옵션을 사용하면 라우터가 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

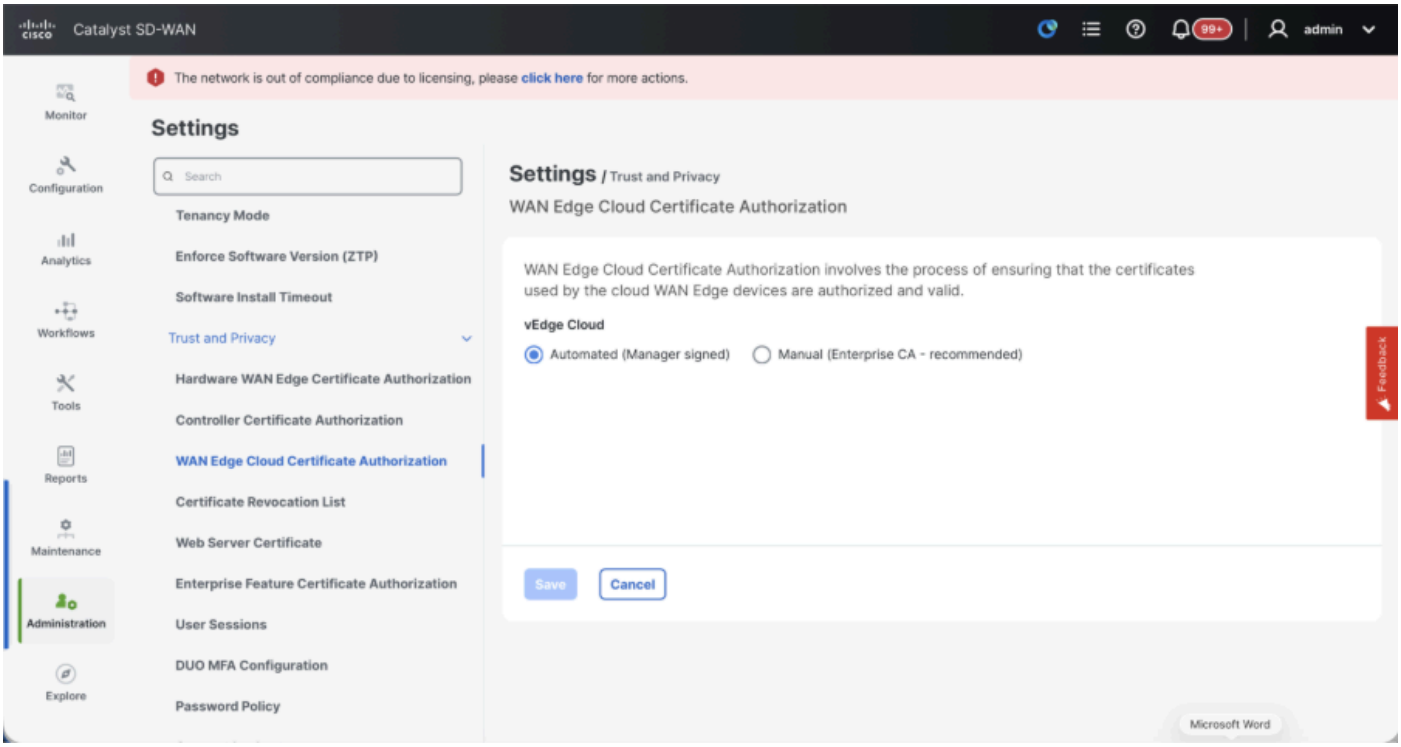


2. Controller Certificate Authorization(컨트롤러 인증서 권한 부여) - SD-WAN 컨트롤러에 대한 CA를 결정합니다.
    - Cisco(권장) - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. vManage는 vManage에 구성된 스마트 어카운트 자격 증명을 사용하여 PNP 포털에 자동으로 연결하고 서명된 인증서를 가져오며 컨트롤러에 설치됩니다.
    - 수동 - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. 각 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 수동으로 CSR에 서명합니다.
    - Enterprise Root Certificate(엔터프라이즈 루트 인증서) - 이 옵션을 사용하면 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

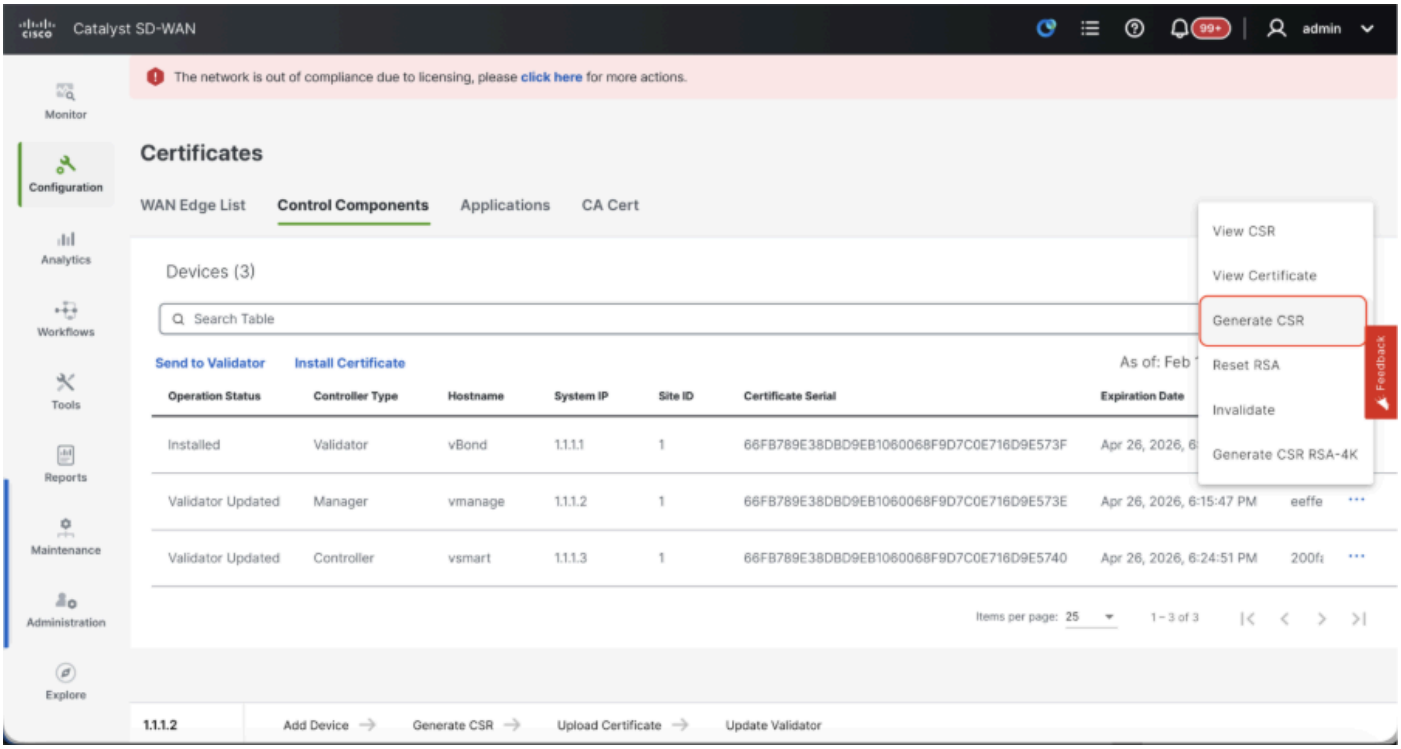


3. WAN Edge Cloud Certificate Authorization - 가상 SD-WAN Edge 라우터(CSR1000v, C8000v, vEdge 클라우드)에 대한 CA를 결정합니다.
    - 자동(vManage signed) - vManage는 가상 에지 라우터의 CSR에 자동으로 서명하고 라우터에 인증서를 설치합니다.
    - 수동(엔터프라이즈 CA - 권장) - 가상 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

자체 CA인 Enterprise Certificate Authority를 사용하는 경우 Enterprise를 선택합니다.



- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)
- Manager/vManage(관리자/vManage)에서 ...를 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

vManage에 vBond/Validator 및 vSmart/Controller 온보딩(Onboarding)

20.15/20.18 vManage 노드의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Control Components(제어 구성 요소)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

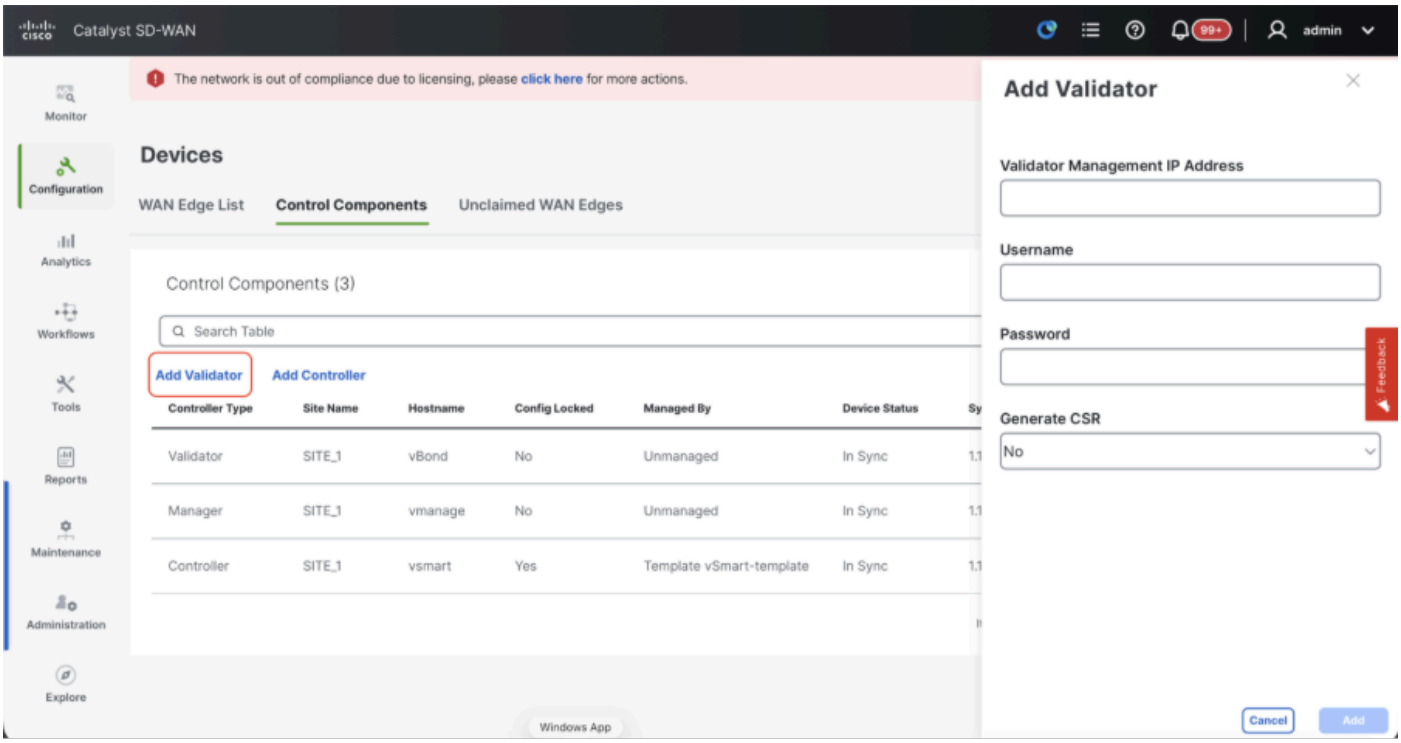
온보딩vBond/Validator

- Add(추가)VBond(vBond 추가)를 클릭합니다.제2012호의 경우유효성 검사기 추가 20.15/20.18 vManage입니다. 팝업이 열리면 vManage에서 연결할 수 있는 vBond의 VPN 0 전송 IP.
- vManagetovBondIP의 CLI에서 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.

- vBond의 사용자 자격 증명을 입력합니다.

참고: vBonor의 관리자 자격 증명 또는 netadmingroup의 사용자 부분이 필요합니다. vBond의 CLI에서 이를 확인할 수 있습니다. vBond에 대한 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다

참고: vBond가 NAT 디바이스/방화벽 뒤에 있는 경우 vBond VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인합니다. vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스의 공용 IP 주소를 사용합니다



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vBond에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vBond가 여러 개인 경우 동일한 단계를 반복합니다.

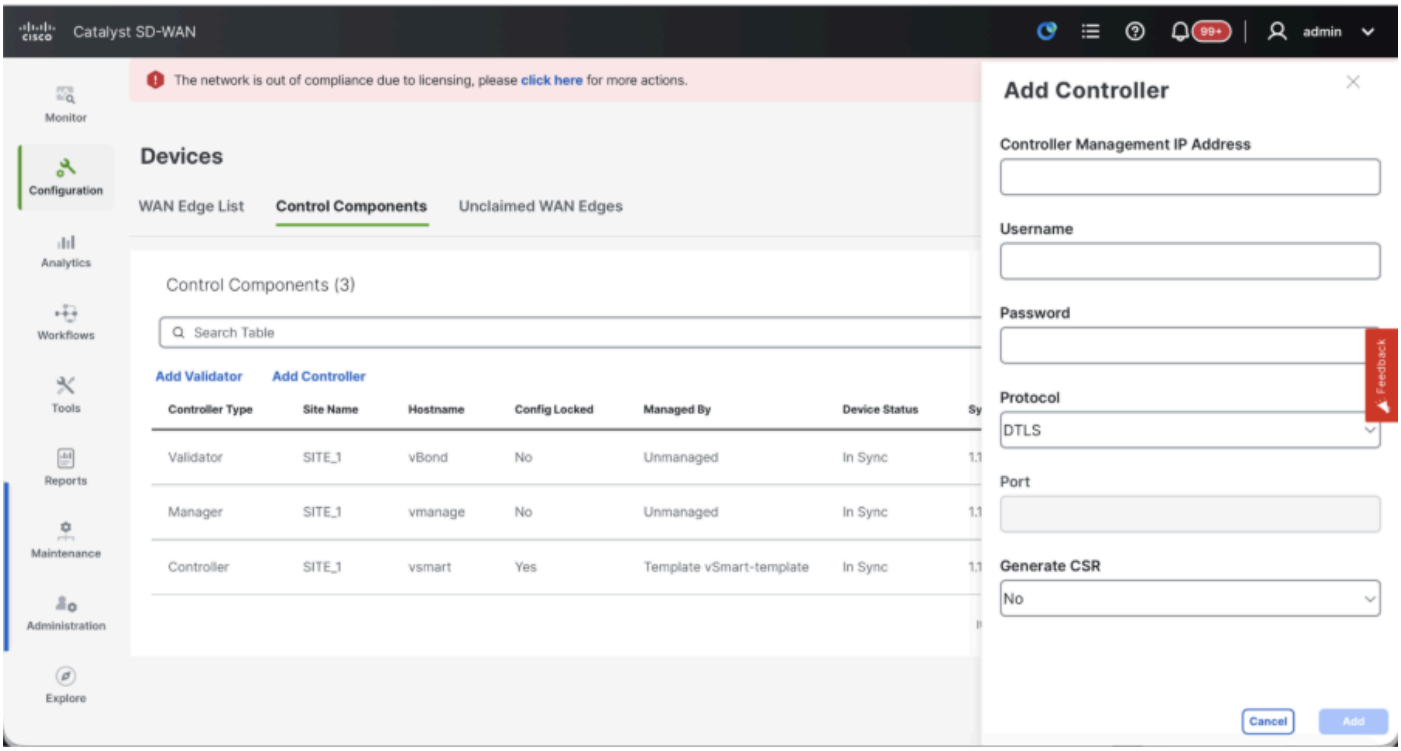
vSmart/컨트롤러 온보딩

- 20.12 vManage의 경우 vSmart 추가 또는 20.15/20.18 vManage의 경우 컨트롤러 추가를 클

릭합니다.

- 팝업이 열리면 vManage에서 연결할 수 있는 vSmart의 VPN 0 전송 IP를 입력합니다.
- vManage의 CLI에서 vSmart IP로 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.
- vSmart의 사용자 자격 증명을 입력하십시오. vSmart의 관리자 자격 증명 또는 netadmin 그룹의 사용자 부분을 사용해야 합니다.
- vSmart의 CLI에서 이를 확인할 수 있습니다.
- 라우터에 TLS를 사용하여 vSmart와의 제어 연결을 설정하려면 프로토콜을 TLS로 설정합니다. vSmarts 및 vManage 노드의 CLI에서도 이 구성을 구성해야 합니다.
- vSmart용 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다.

참고: vSmart가 NAT 장치/방화벽 뒤에 있는 경우 vSmart VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인하고, vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스 IP의 공용 IP 주소를 사용합니다.

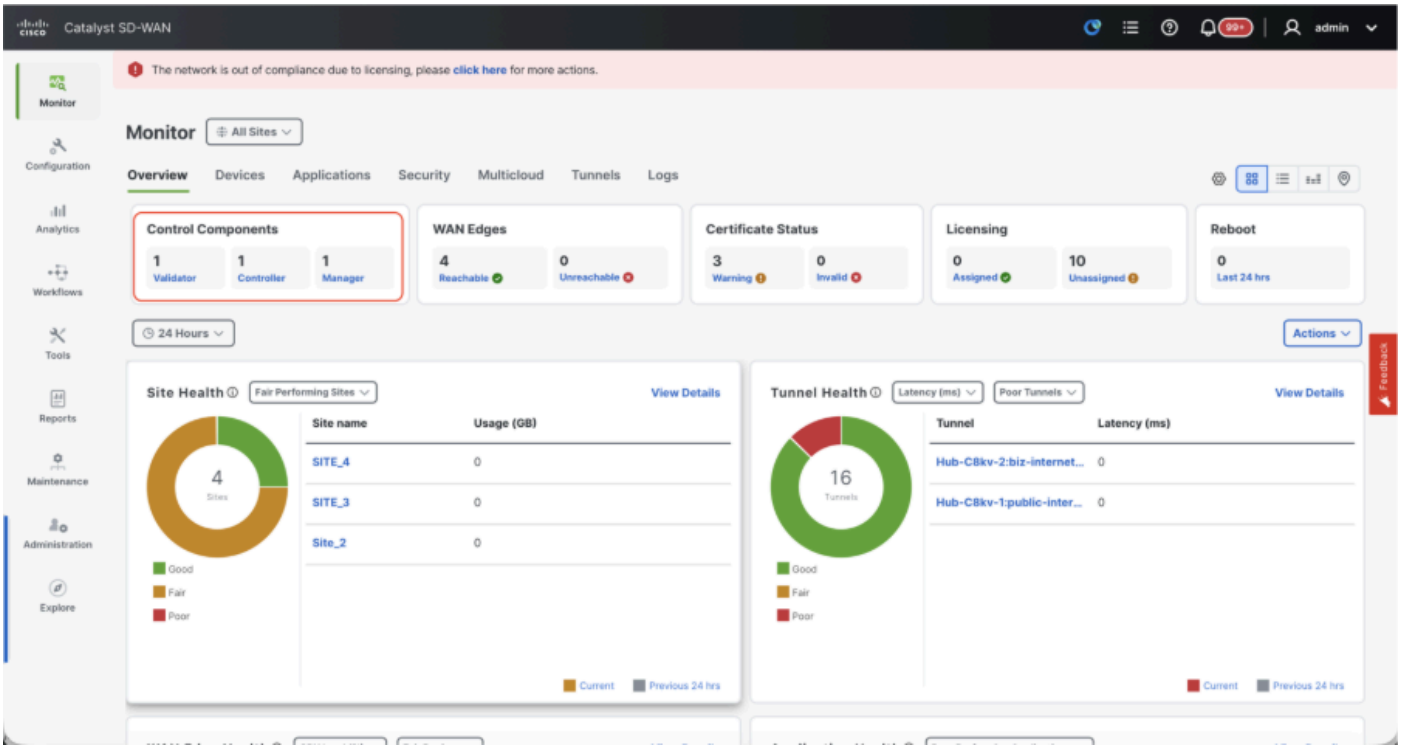


- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vSmart에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다.

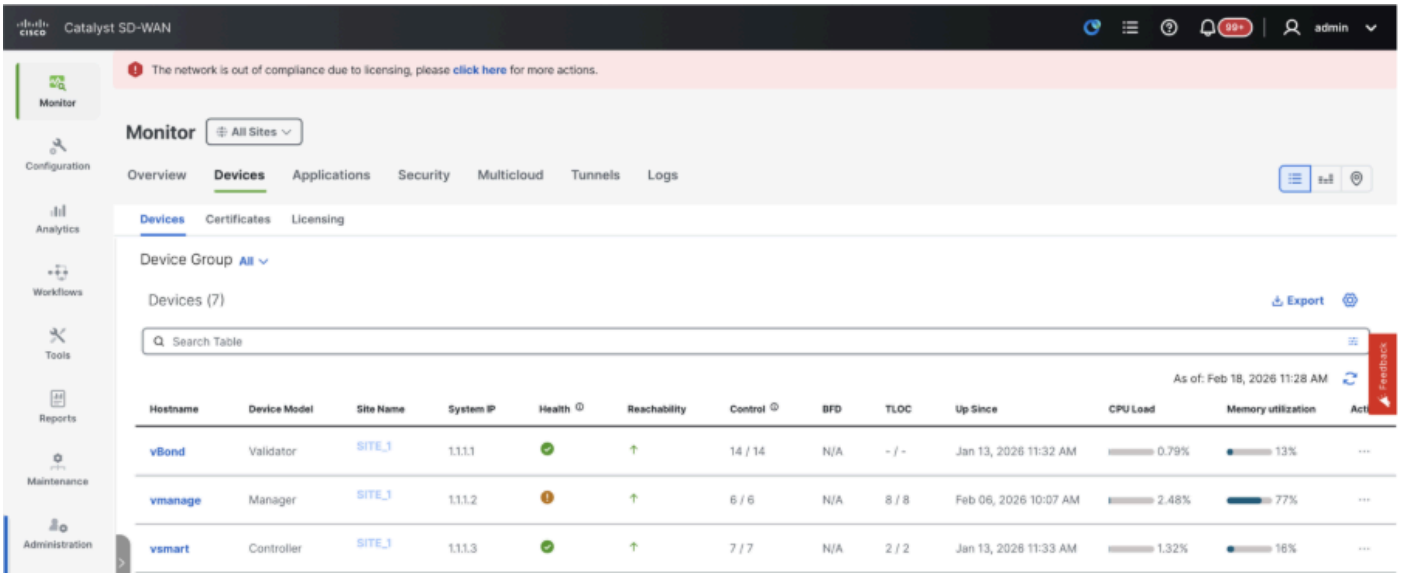
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vSmarts가 여러 개인 경우 동일한 단계를 반복합니다.

확인

모든 단계가 완료되면 Monitor>Dashboard에서 모든 제어 구성 요소에 연결할 수 있는지 확인합니다



- 각 Control(제어) 구성 요소를 클릭하고 모두 연결할 수 있는지 확인합니다.
- Monitor(모니터링) > Devices(디바이스)로 이동하여 모든 제어 구성 요소에 연결할 수 있는지 확인합니다.



3단계: vManage 클러스터 구축

SD-WAN 오버레이에 vManage 클러스터를 포함하는 온보드 SD-WAN 패브릭

참고: SD-WAN 패브릭에 온보딩된 사이트의 수에 따라 vManage 클러스터를 3개의 vManage 노드 또는 6개의 vManage 노드로 구성할 수 있습니다. 기존 vManage 클러스터를 참조하고 동일한 노드 수를 선택하십시오.

클러스터의 일부인 모든 vManage 노드의 CLI 컨피그레이션을 구성합니다

모든 vManage 노드에서 시스템 구성

- vManage 노드의 나머지를 구성합니다. 3노드 클러스터의 경우 나머지 2개 노드를 구성해야 하고 6노드 클러스터의 경우 5개 노드를 구성해야 합니다.
- 다음과 같이 시스템 컨피그레이션을 구성합니다.

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

참고: URL을 vBond 주소로 사용하는 경우 VPN 0 컨피그레이션에서 DNS 서버 IP 주소를 구성하거나 확인할 수 있는지 확인하십시오.

모든 vManage 노드에서 전송 인터페이스 구성

이러한 컨피그레이션은 라우터 및 나머지 컨트롤러와의 제어 연결을 설정하는 데 사용되는 전송 인터페이스를 활성화하는 데 필요합니다.

```
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
```

모든 vManage 노드에서 관리 인터페이스 구성

컨트롤러에 대한 대역 외 관리 액세스를 활성화하도록 VPN 512 관리 인터페이스도 구성합니다.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

선택적 구성:

- 기존 컨트롤러의 컨피그레이션을 참조할 수 있으며 여기에 나열된 컨피그레이션이 있는 경우 이 컨피그레이션을 새 컨트롤러에 추가할 수 있습니다.
- 라우터가 TLS를 사용하여 vManage 노드와 보안 제어 연결을 설정해야 하는 경우에만 제어 프로토콜을 TLS로 구성합니다. 기본적으로 모든 컨트롤러와 라우터는 DTLS를 사용하여 제어 연결을 설정합니다. 이는 사용자의 요구 사항에 따라 vSmart 및 vManage 노드에서만 필요한 선택적 컨피그레이션입니다.

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

모든 vManage 노드에서 서비스 인터페이스 구성

이미 온보딩된 vManage-1을 포함하여 모든 vManagenodes에서 서비스 인터페이스를 구성합니다. 이 인터페이스는 클러스터 통신에 사용됩니다. 즉, 클러스터에서 vManagenodes 간의 통신을 의미합니다.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

vManagecluster의 모든 노드에서 서비스 인터페이스에 동일한 IP 서브넷이 사용되는지 확인합니다.

클러스터 자격 증명 구성

vManagenodes의 동일한 관리자 자격 증명을 사용하여 vManagecluster를 구성할 수 있습니다. 그렇지 않으면 netadmingroup의 일부인 새 사용자 자격 증명을 구성할 수 있습니다. 새 사용자 자격 증명을 구성하기 위한 컨피그레이션은 다음과 같습니다

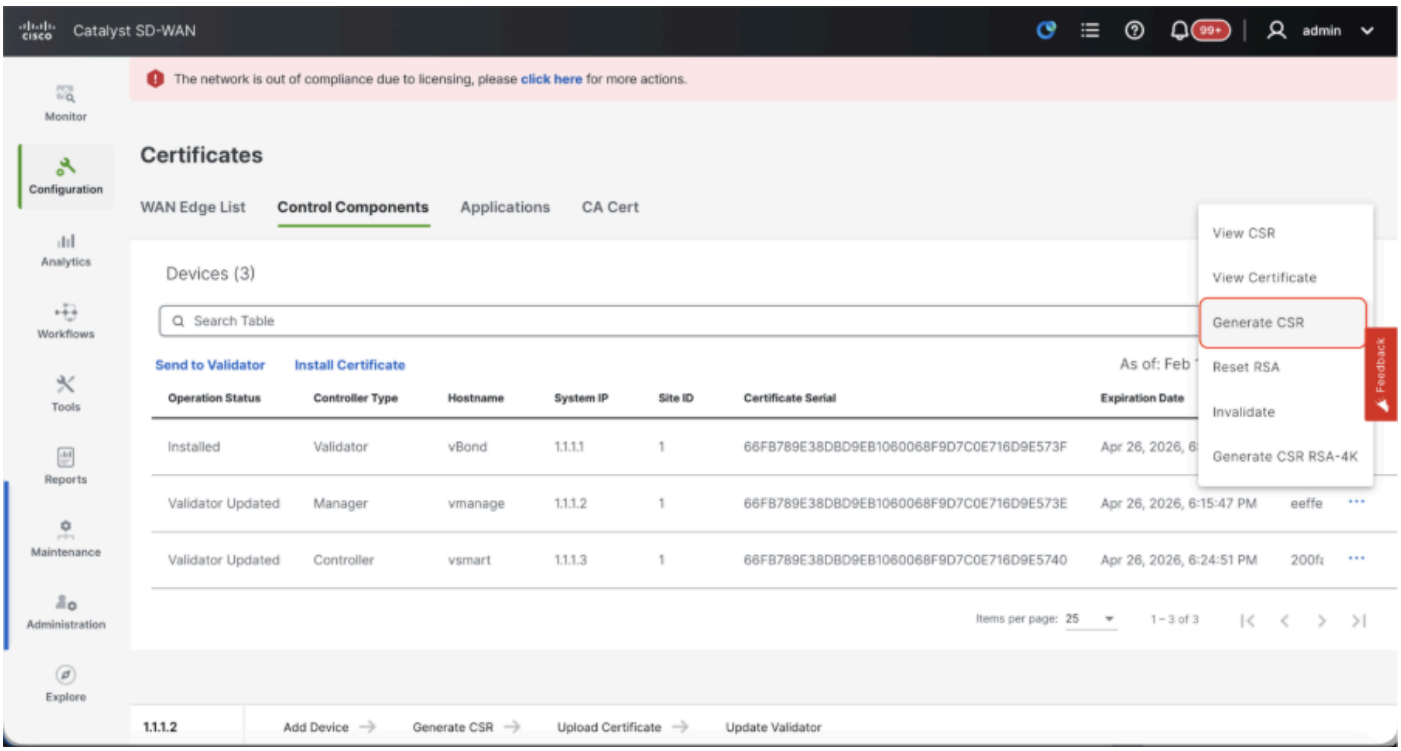
```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

클러스터의 일부인 모든 vManagenodessi에서 동일한 사용자 자격 증명을 구성해야 합니다.관리자 자격 증명을 사용하려면 모든 vManagenodes에서 동일한 사용자 이름/비밀번호여야 합니다.

모든 vManage 노드에 디바이스 인증서 설치

- 브라우저의 URL https://<vmanage-ip>를 사용하여 모든 vManagenodes의 vManageUI에 로그인합니다. 각 vManagenodes의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

  Manager/vManage(관리자/vManage)에서 ...을 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



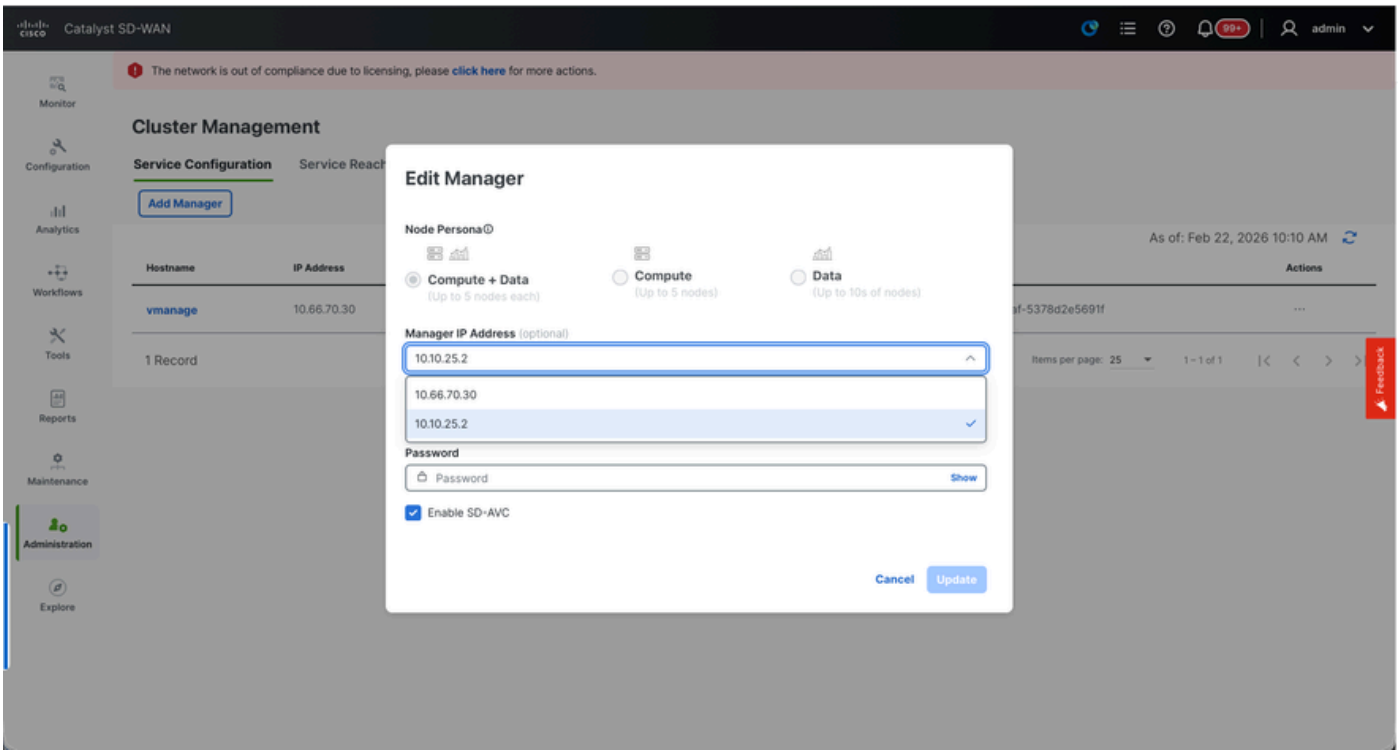
- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- 클러스터의 일부인 모든 vManage 노드에서 이 단계를 완료합니다.

vManage 클러스터 구축 준비

- vManage-1의 webUI에서 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고 vManage-1에 대한 Actions(작업) 아래에서 ...를 클릭한 후 Edit(수정)를 선택합니다.
- 노드 페르소나는 VM이 스핀업되는 동안 선택한 페르소나에 따라 자동으로 선택됩니다.

참고: 3노드 클러스터의 경우 3개의 vManage 노드 모두 컴퓨팅+데이터가 페르소나로 표시됩니다.

- 6노드 클러스터의 경우 3개의 vManage 노드가 compute+data를 페르소나로, 3개의 vManage 노드가 data를 페르소나로 가져옵니다.
- 관리자 IP 주소의 드롭다운에서 vManage의 서비스 인터페이스 IP를 선택해야 합니다.

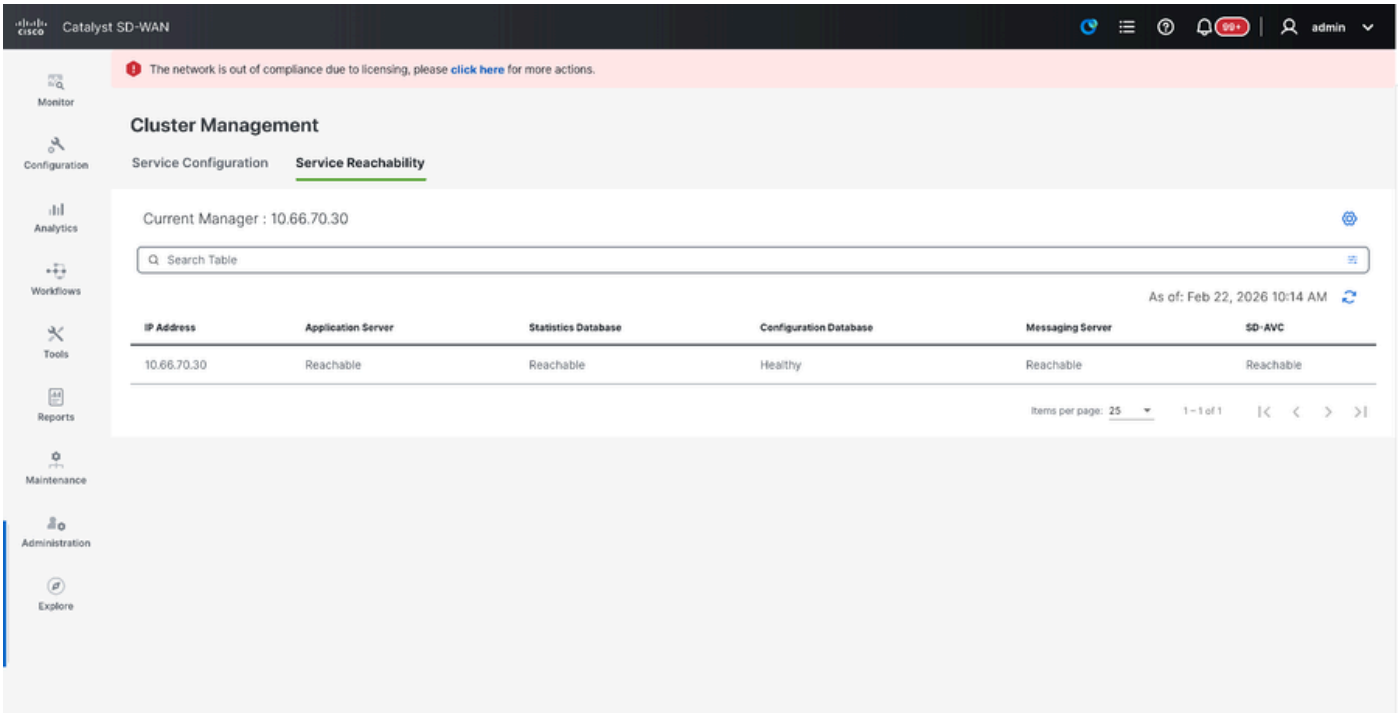


- vManage 클러스터를 활성화하는 데 사용할 사용자 이름 및 비밀번호를 입력합니다. 이를 클러스터 자격 증명이라고 합니다.
- 앞에서 언급한 것처럼 모든 vManage 노드에서 동일한 자격 증명을 구성해야 하며 모든 노드를 클러스터에 추가하는 동안 사용해야 합니다.

참고: SDAVC 활성화 - SDAVC가 필요하고 클러스터의 vManage 노드 하나에서만 필요한 경우에만 이 컨피그레이션을 기존 클러스터에서 참조하십시오.

Update(업데이트)를 클릭합니다.

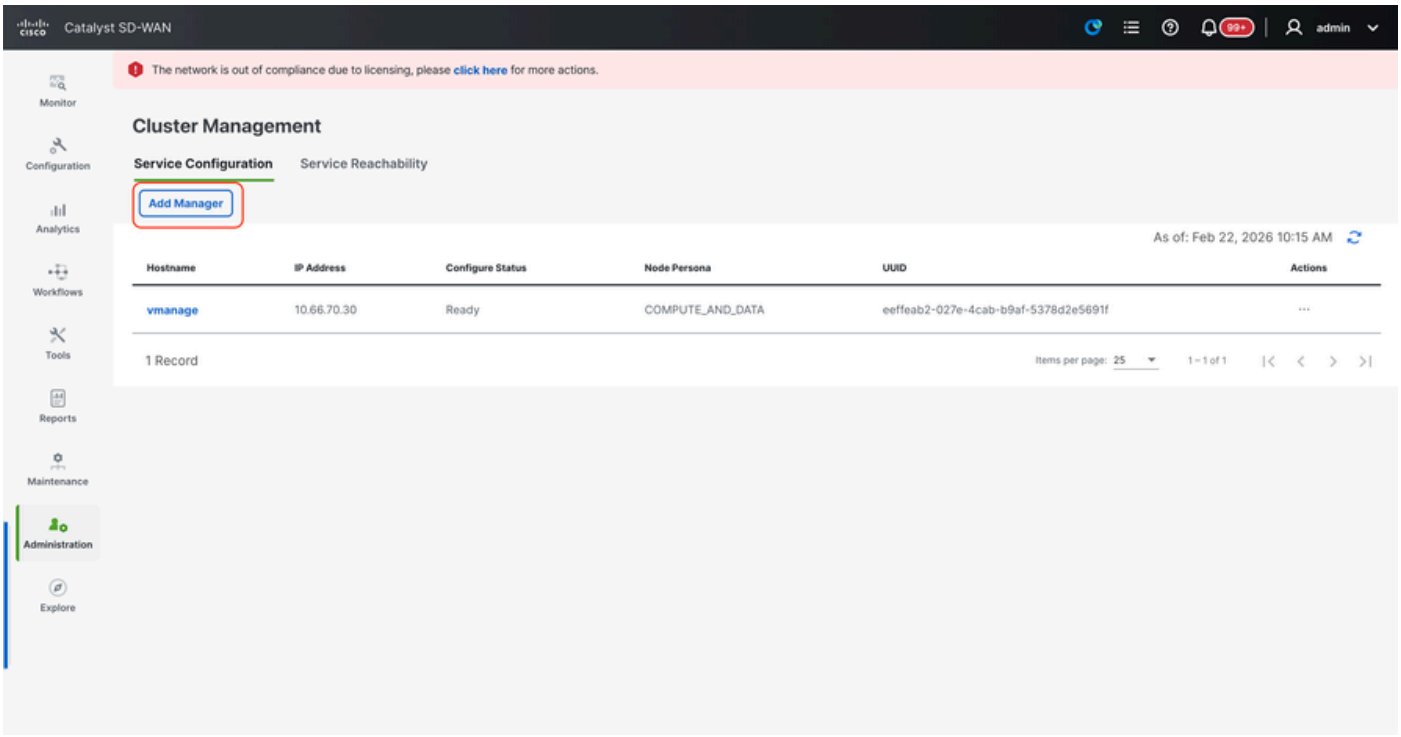
- 이 게시물을 올리면 백그라운드에서 vManage NMS 서비스가 다시 시작되고 5~10분 정도의 몇 분 동안 UI를 사용할 수 없습니다. 이 기간 동안 vManage의 CLI 액세스를 사용할 수 있습니다.
- vManage-1 UI에 액세스할 수 있게 되면 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고 IP 주소 아래에 vManage의 서비스 인터페이스 IP가 반영되었는지 확인합니다.Configure Status(상태 구성)가 Ready(준비)이고 노드 페르소나가 올바르게 반영됩니다.
- 같은 페이지의 서비스 연결 가능 섹션으로 전환하고 모든 서비스에 연결할 수 있는지 확인합니다.

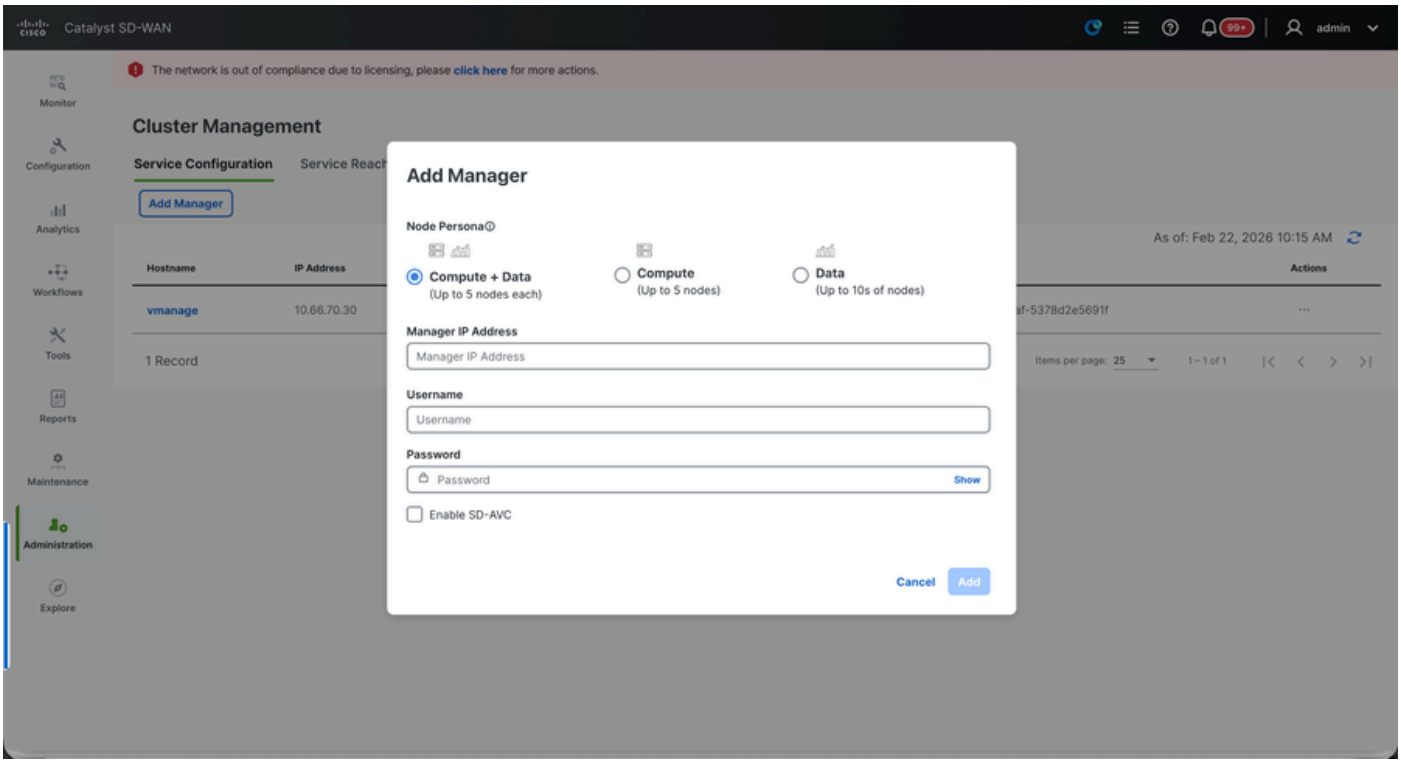


- 아직 연결되지 않은 서비스가 있는 경우 잠시 기다려 주십시오. 보통 20분에서 30분 정도 걸립니다.

vManage 클러스터 구축

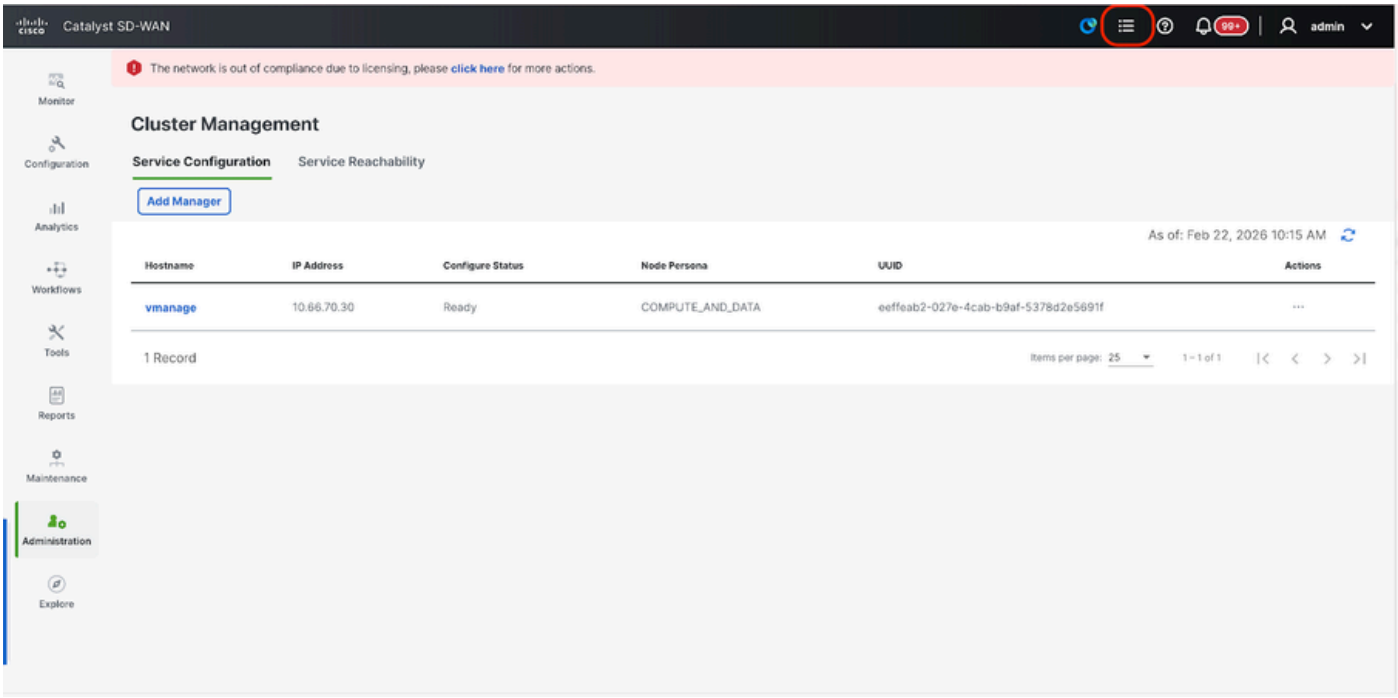
- vManage-1의 webUI에서 Service Configuration(서비스 컨피그레이션) 섹션의 Administration(관리) > Cluster Management(클러스터 관리)로 이동합니다.
- Add Manager(관리자 추가)를 클릭하면 팝업 창이 나타납니다.





- vManage - 2 노드를 스핀업하는 동안 수행한 페르소나 컨피그레이션에 따라 노드 페르소나를 선택합니다.
- 관리자 IP 주소 아래 vManage-2의 서비스 인터페이스 IP를 입력합니다
- 사용자 이름과 비밀번호를 입력합니다. 이는 6단계에서 사용한 것과 동일한 자격 증명입니다 .
- Enable SDAVC(SDAVC 활성화) - vManage-1에서 SDAVC를 이미 활성화했으므로 선택하지 않은 상태로 둡니다.
- Add(추가)를 클릭합니다.
- 이를 게시하면 vManage NMS 서비스가 백그라운드에서 vManage 1 및 2 노드에 대해 다시

시작됩니다. vManage 1 및 2의 경우 약 5~10분 동안 UI를 사용할 수 없습니다.
- 이 기간 동안 vManage 1 및 2의 CLI 액세스를 사용할 수 있습니다.
- vManage-1 UI에 액세스할 수 있게 되면 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고, vManage의 서비스 인터페이스 IP가 모두 IP 주소에 반영되었는지 확인하고, Configure Status(구성 상태)가 Ready(준비)이고 노드 페르소나가 올바르게 반영되었는지 확인합니다.
- 같은 페이지의 서비스 연결 가능 섹션으로 전환하고 모든 서비스가 두 vManage 노드 모두에 연결할 수 있는지 확인합니다.
- 아직 연결되지 않은 서비스가 있는 경우 잠시 기다려 주십시오. 보통 5분에서 10분 정도 걸립니다.
- vManage UI의 오른쪽 상단 모서리에 있는 Task-list(작업 목록)에서 클러스터 추가 프로세스의 상태를 확인할 수 있습니다.



- Active(활성) 작업 목록을 조회할 수 있으며, 작업이 Active(활성) 작업 목록 아래에 여전히 나열되어 있으면 작업이 아직 완료되지 않았음을 나타냅니다.
- 작업을 클릭하여 진행 상태를 확인할 수 있습니다. 작업이 활성 작업 목록에 나열되지 않으면 완료로 전환하고 작업이 성공적으로 완료되었는지 확인하십시오.
- 이러한 점이 검증된 후에만 다음 단계로 진행합니다.

클러스터에 다음 노드를 추가하기 전에 이러한 점을 고려해야 합니다.

지금까지 클러스터에 추가된 vManage 노드의 모든 UI에서 다음 사항을 확인하십시오.

- Monitor(모니터) > Overview of vManage UI(vManage UI 개요)로 이동하여 vManage 노드 수가 올바르게 반영되고 클러스터에 추가된 노드 수에 따라 연결 가능한 것으로 표시되는지 확인합니다.

- Administration(관리) > Cluster Management(클러스터 관리)로 이동하여 IP 주소 아래에 vManage의 서비스 인터페이스 IP가 모두 반영되고, Configure Status(구성 상태)가 Ready(준비)이고 노드 페르소나가 올바르게 반영되었는지 확인합니다.

- 같은 페이지의 서비스 연결 가능 섹션으로 전환하고 모든 서비스가 두 vManage 노드 모두에 연결할 수 있는지 확인합니다.

- 노드가 클러스터에 추가될 때마다 클러스터에 있는 모든 노드의 NMS 서비스가 다시 시작되므로 해당 노드의 UI에 한동안 연결할 수 없게 됩니다.
- 클러스터의 노드 수에 따라 UI를 백업하고 모든 서비스에 연결하는 데 더 오랜 시간이 걸릴 수 있습니다.
- vManage UI의 오른쪽 상단 모서리에 있는 Task-list(작업 목록)에서 작업을 모니터링할 수 있습니다.
- 클러스터에 추가된 각 노드의 vManage UI에서 vManage-1에서 사용 가능한 모든 라우터, 템플릿 및 정책을 확인해야 합니다.
- 이러한 컨피그레이션이 vManage-1에 없는 경우 vManage-1에 추가된 vBonds 및 vSmarts와 Administration(관리) > Settings(설정) 컨피그레이션에서 Organization-name(조직 이름), vBond, Certificate Authorization(인증서 권한 부여)이 클러스터에 추가된 나머지 vManage 노드에 반영되어야 합니다.
- 나머지 vManage 노드에 대해서도 동일한 단계를 반복합니다.

모든 컨트롤러가 온보딩되면 다음 단계를 완료합니다.

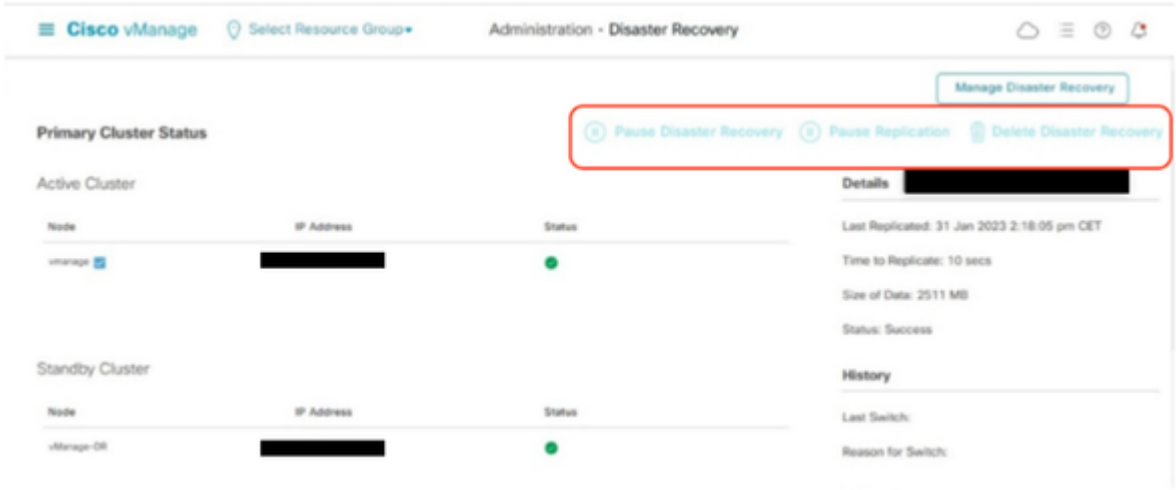
4단계: Config-db 백업/복원

다른 vManage 노드에서 vManage configuration-db 백업 및 복원 수집

참고: 재해 복구가 활성화된 기존 vManage 클러스터에서 컨피그레이션 데이터베이스 백업을 수집하는 동안 해당 노드의 재해 복구가 일시 중지되고 삭제된 후에 수집되어야 합니다.

진행 중인 재해 복구 복제가 없는지 확인합니다. Administration(관리) > Disaster Recovery(재해 복구) 및 상태가 Success(성공)이고 Import Pending(가져오기 보류 중), Export Pending(내보내기 보류 중) 또는 Download Pending(다운로드 보류 중)과 같은 일시적인 상태가 아닌지 확인합니다. 상태가 성공적이지 않으면 Cisco TAC에 문의하여 복제가 성공적인지 확인한 후 재해 복구를 일시 중지합니다.

먼저 재해 복구를 일시 중지하고 작업이 완료되었는지 확인합니다. 그런 다음 재해 복구를 삭제하고 작업이 완료되었는지 확인합니다.



Cisco TAC에 문의하여 재해 복구가 성공적으로 정리되었는지 확인합니다.

Configuration-DB 백업 수집:

- 현재 사용 중인 SD-WAN 패브릭에서는 vManage 클러스터에서 configuration-db 백업을 생성할 수 있습니다.
- configuration-db 백업은 configuration-db 리더인 vManage 클러스터의 한 노드에서만 생성해야 합니다.

- 독립형 vManage의 경우 해당 vManage 자체가 configuration-db 리더입니다.
- vManage 클러스터에서 request nms configuration-db diagnostics 명령을 사용하여 configuration-db 리더 노드를 식별합니다.3노드 vManage 클러스터의 모든 노드에서 이 명령을 실행할 수 있습니다.
- 6노드 클러스터에서 컨피그레이션 DB가 활성화되어 리더 노드를 식별하는 vManage 노드에서 이 명령을 실행해야 합니다. Administration(관리) > Cluster Management(클러스터 관리)로 이동하여 다음을 확인합니다.
- 스크린샷에서 볼 수 있듯이, COMPUTE_AND_DATA 페르소나로 구성된 노드는 컨피그레이션 DB가 실행 중입니다.

vManageCLI에서 requestnmsconfiguration-dbstatus 명령을 사용하여 동일한 사항을 확인할 수 있습니다. 출력은 다음과 같습니다

```
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#
```

- 명령을 실행하면이러한 노드에서 nms configuration-db 진단을 요청하면 다음과 같이 출력됩니다.
- "IsLeader"에 대해 강조 표시된 필드를 찾습니다. 1로 설정된 경우 노드가 리더 노드임을 나타

내며, 여기서 configuration-db 백업을 수집할 수 있습니다.

```
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     .
```

식별된 configuration-db leader vManage 노드에서 configuration-db 백업을 수집하려면 이 명령을 사용합니다.

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

예상 출력은 다음과 같습니다.

```
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#
```

- 컨피그레이션 DB 자격 증명이 업데이트된 경우 기록해 둡니다.
- configuration-db 자격 증명을 모르는 경우 TAC에 문의하여 기존 vManage 노드에서 configuration-db 자격 증명을 검색합니다.
- 기본 configuration-db 자격 증명은 사용자 이름입니다. neo4j 및 비밀번호: 암호

다른 vManage 노드에 Configuration-db 백업 복원

SCP를 사용하여 configuration-db 백업을 vManage의 /home/admin/ 디렉토리에 복사합니다.

샘플 scp 명령 출력:

```
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 백업을 복원하려면 먼저 configuration-db 자격 증명을 구성해야 합니다. configuration-db 자격 증명이 default(neo4j/password)인 경우 이 단계를 건너뛸 수 있습니다.

configuration-db 자격 증명을 구성하려면 nms configuration-db update-admin-user 명령을 사용합니다.선택한 사용자 이름과 비밀번호를 사용합니다.

vManage의 애플리케이션 서버가 다시 시작됩니다. 따라서 vManage UI에 짧은 시간 동안 액세스할 수 없게 됩니다.

```
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#
```

구성 DB 백업을 복원하기 위해 진행할 수 있는 게시:

nms configuration-db 복원 경로 /home/admin/< > 명령을 사용하여 configuration-db를 새 vManage로 복원할 수 있습니다.

```
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-db가 복원되면 vManage UI에 액세스할 수 있는지 확인합니다. 약 5분 정도 기다린 후 UI에 액세스를 시도합니다.

UI에 성공적으로 로그인했으면 Edge 라우터 목록, 템플릿, 정책 및 이전 또는 기존 vManage UI에 존재했던 나머지 모든 컨피그레이션이 새 vManage UI에 반영되었는지 확인합니다.

5단계: 컨트롤러 재인증 및 이전 컨트롤러 무효화

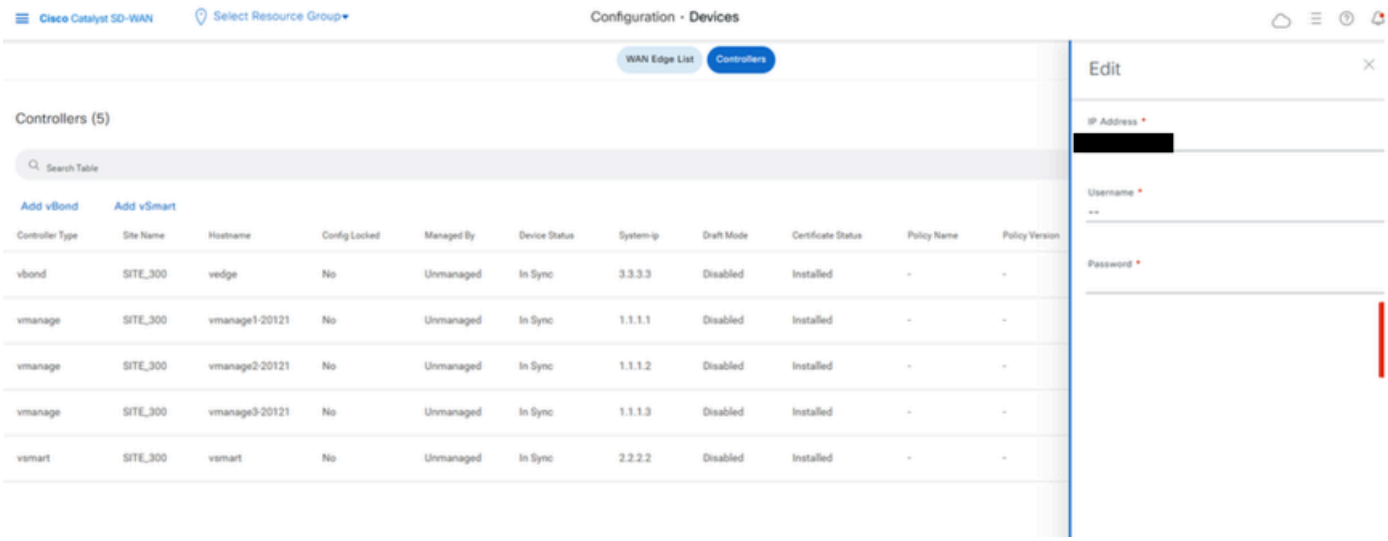
configuration-db가 복원되면 패브릭에서 모든 새 컨트롤러(vmanage/vsmart/vbond)를 재인증해야 합니다

참고: 실제 프로덕션에서는 재인증에 사용되는 인터페이스 IP가 터널 인터페이스 IP인 경우 vManage, vSmart 및 vBond의 터널 인터페이스 및 경로에 따른 방화벽에서 NETCONF 서비스가 허용되는지 확인해야 합니다. 열 방화벽 포트는 DR 클러스터에서 모든 vBonds 및 vSmarts로의 양방향 규칙인 TCP 포트 830입니다.

---

vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다

- 각 컨트롤러 근처의 점 3개를 클릭하고 Edit(수정)를 클릭합니다



- ip-address(컨트롤러의 system-ip)를 transport vpn 0(tunnel interface) ip 주소로 바꿉니다. 사용자 이름과 암호를 입력하고 save(저장)를 클릭합니다
- 패브릭에 있는 모든 새 컨트롤러에 대해 동일한 작업을 수행합니다.

루트 인증서 체인 동기화

모든 컨트롤러가 온보딩되면 다음 단계를 완료합니다.

새로 활성화된 클러스터의 Cisco SD-WAN Manager 서버에서 다음 작업을 수행합니다.

루트 인증서를 새로 활성화된 클러스터의 모든 Cisco Catalyst SD-WAN 디바이스와 동기화하려면 다음 명령을 입력합니다.

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

Cisco SD-WAN Manager UUID를 Cisco SD-WAN Validator와 동기화하려면 다음 명령을 입력합니다.

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

패브릭이 복원되고 패브릭의 모든 에지와 컨트롤러에 대해 제어 및 bfd 세션이 작동되면 UI에서 이전 컨트롤러(vmanage/vsmart/vbond)를 무효화해야 합니다

- vmanage UI에서 Configuration > Devices > Certificates를 클릭합니다
- Controllers(컨트롤러) 클릭
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. Invalidate를 클릭합니다.
- Send to Bond를 클릭합니다.
- vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. 삭제를 클릭합니다.

6단계: 수표 게시

참고: 여기에 표시된 모든 구축 조합에 공통적으로 적용되는 Post Checks(사후 검사) 섹션을 계속 진행합니다.

조합 4: vManage 클러스터 + 수동/콜드 스탠바이 DR

수동/콜드 스탠바이 DR이란? 백업 SD-WAN 관리자 서버 또는 SD-WAN 관리자 클러스터는 콜드 스탠바이 상태로 종료됩니다.

활성 데이터베이스의 정기적인 백업이 수행되며 기본 SD-WAN 관리자 또는 SD-WAN 관리자 클러스터가 다운되면 대기 SD-WAN 관리자 또는 SD-WAN 관리자 클러스터가 수동으로 시작되고 백업 데이터베이스가 복원됩니다.

필요한 인스턴스:

- 3 또는 6 vManage(기본 클러스터)
- 3 또는 6 vManage(DR 대기 클러스터)
- 1개 이상의 vBond(기본 및 DR 데이터 센터에 분산)
- 1개 이상의 vSmart(기본 및 DR 데이터 센터에 분산)

단계:

1. 공통 단계를 사용하여 모든 인스턴스 가져오기
2. 사전 확인
3. vManage UI, 인증서 및 온보드 컨트롤러 구성
4. vManage 클러스터 구축

5. 콜드 스탠바이 DR 클러스터 설정
6. Config-db 백업/복원
7. 수표 게시

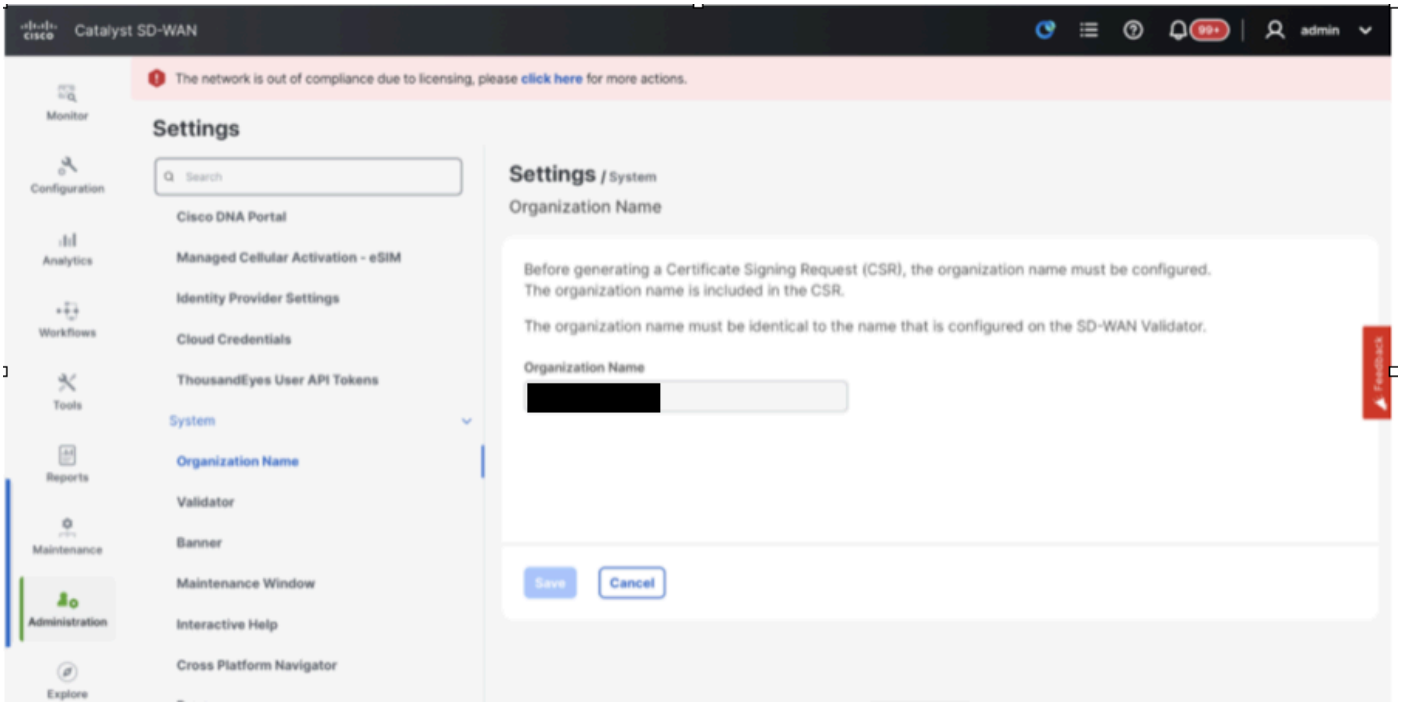
1단계: 사전 확인

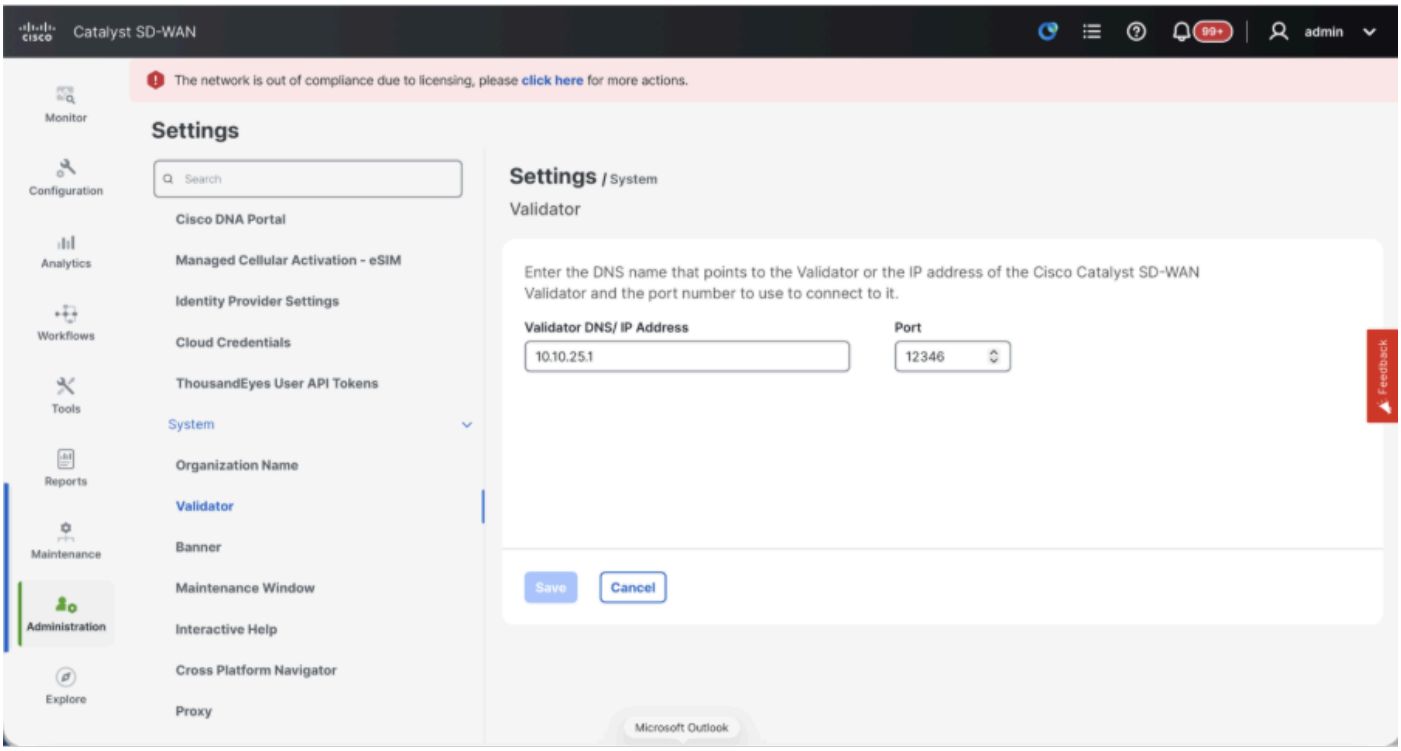
- 활성 Cisco SD-WAN Manager 인스턴스의 수가 새로 설치된 Cisco SD-WAN Manager 인스턴스의 수와 동일한지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 동일한 소프트웨어 버전을 실행하는지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 Cisco SD-WAN Validator의 관리 IP 주소에 연결할 수 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스에 인증서가 설치되어 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스를 포함하여 모든 Cisco Catalyst SD-WAN 디바이스의 시계가 동기화되었는지 확인합니다.
- 새 시스템 IP 및 사이트 ID 집합이 활성 클러스터와 동일한 기본 구성과 함께 새로 설치된 Cisco SD-WAN Manager 인스턴스에 구성되어 있는지 확인합니다.

2단계: vManage UI, 인증서 및 온보드 컨트롤러 구성

vManage UI에서 컨피그레이션 업데이트

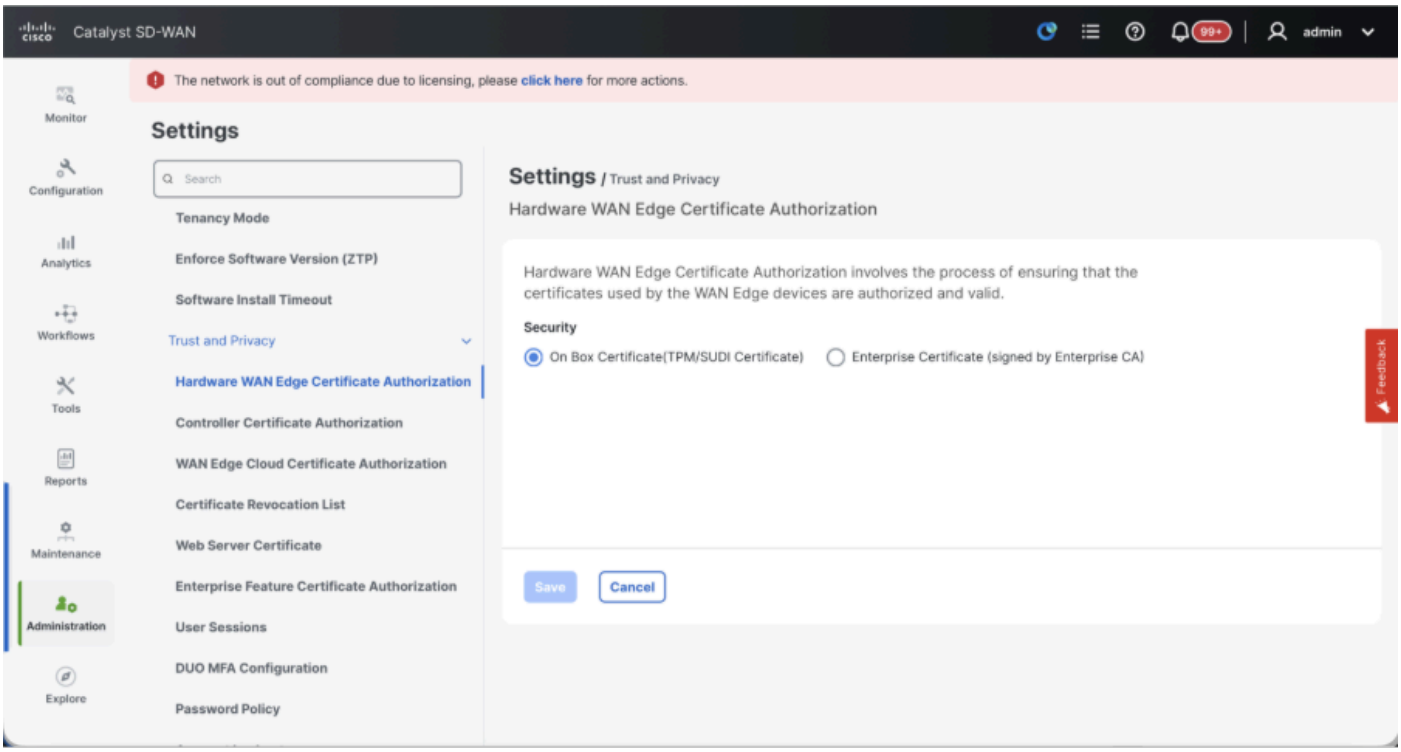
- 1단계의 컨피그레이션이 모든 컨트롤러의 CLI에 추가되면 브라우저의 URL https://<vmanage-ip>를 사용하여 vManage의 webUI에 액세스할 수 있습니다. 각 vManage 노드의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Administration(관리) > Settings(설정)로 이동하여 다음 단계를 완료합니다.
- 조직 이름 및 검증기/vBond URL/IP 주소를 구성합니다. vManage 노드의 CLI에서와 동일한 값을 구성합니다.
- vManage 20.15/20.18의 섹션 System에서 이러한 구성을 사용할 수 있습니다.



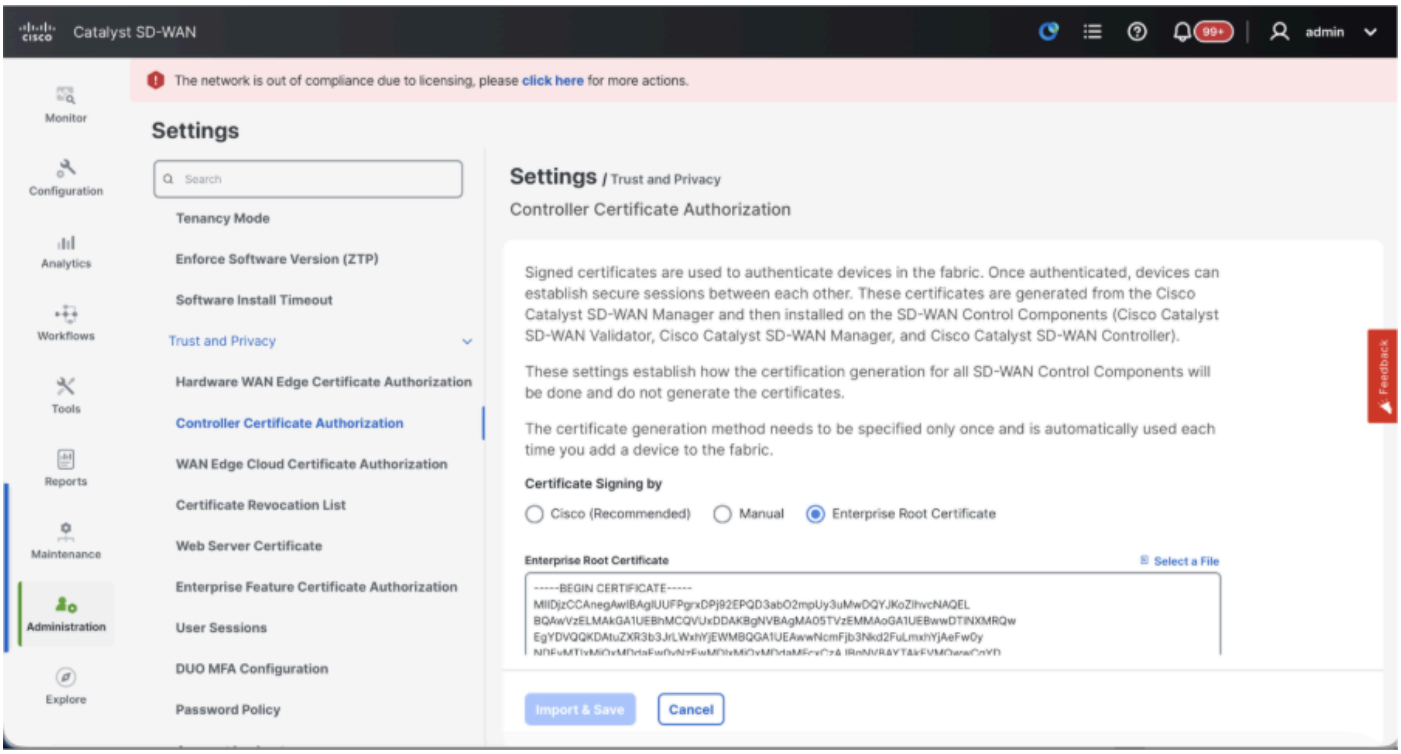


- 인증서 서명에 사용되는 인증 기관을 결정하는 CA(Certificate Authorization)의 컨피그레이션을 확인합니다. 3가지 옵션이 있습니다.

1. Hardware WAN Edge Certificate Authorization - 하드웨어 SD-WAN 에지 라우터의 CA를 결정합니다.
    - On Box Certificate(TPM/SUDI 인증서) - 이 옵션을 사용하면 라우터 하드웨어에 미리 설치된 인증서를 사용하여 제어 연결(TLS/DTLS 연결)을 설정합니다
    - 엔터프라이즈 인증서(Enterprise CA에서 서명) - 이 옵션을 사용하면 라우터가 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

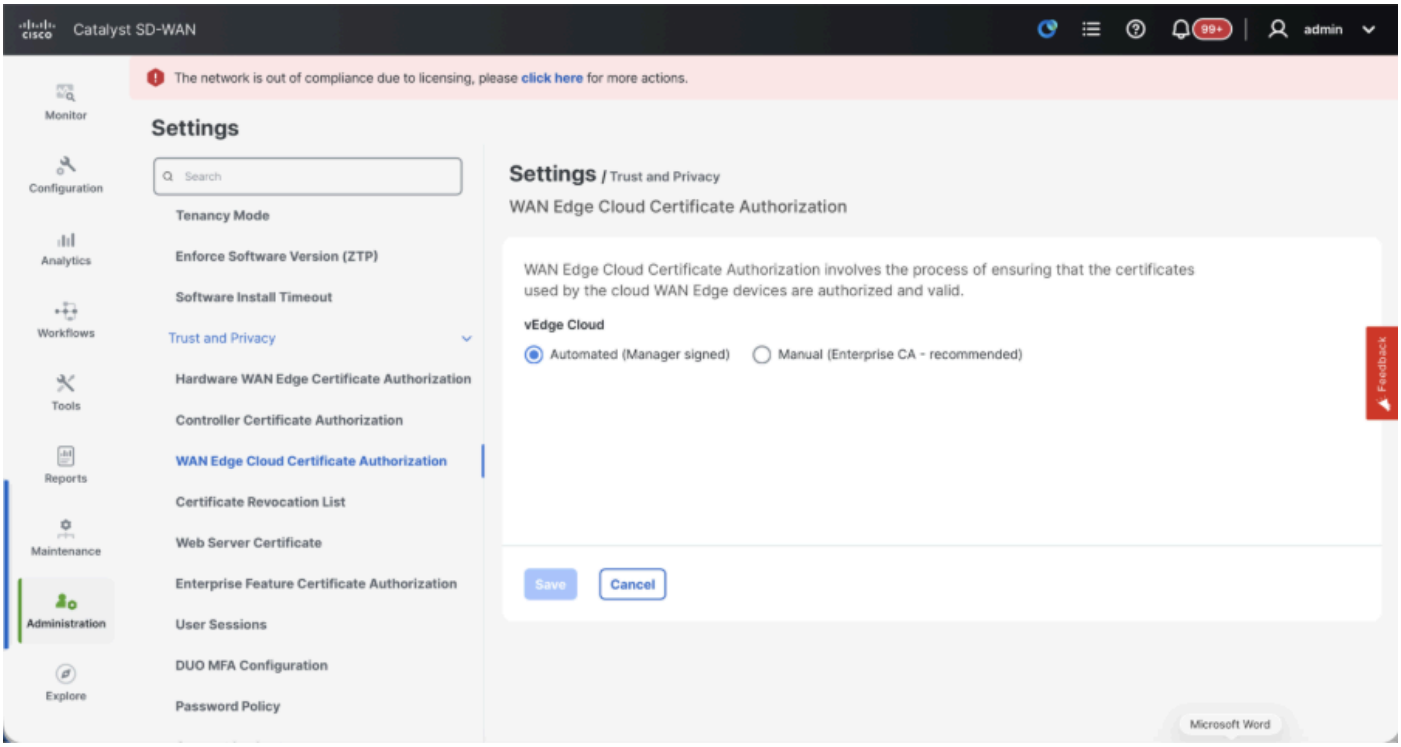


2. Controller Certificate Authorization(컨트롤러 인증서 권한 부여) - SD-WAN 컨트롤러에 대한 CA를 결정합니다.
    - Cisco(권장) - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. vManage는 vManage에 구성된 스마트 어카운트 자격 증명을 사용하여 PNP 포털에 자동으로 연결하고 서명된 인증서를 가져오며 컨트롤러에 설치됩니다.
    - 수동 - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. 각 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 수동으로 CSR에 서명합니다.
    - Enterprise Root Certificate(엔터프라이즈 루트 인증서) - 이 옵션을 사용하면 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

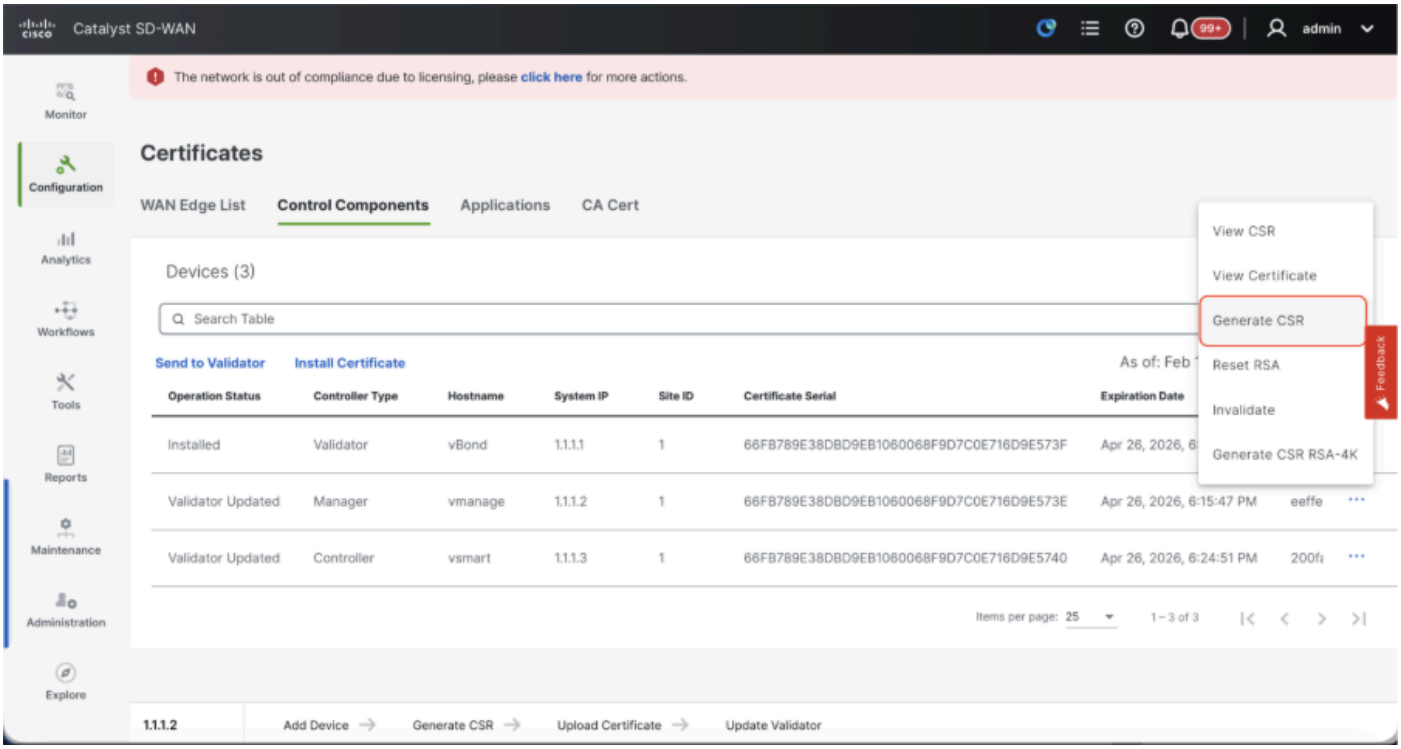


3. WAN Edge Cloud Certificate Authorization - 가상 SD-WAN Edge 라우터(CSR1000v, C8000v, vEdge 클라우드)에 대한 CA를 결정합니다.
    - 자동(vManage signed) - vManage는 가상 에지 라우터의 CSR에 자동으로 서명하고 라우터에 인증서를 설치합니다.
    - 수동(엔터프라이즈 CA - 권장) - 가상 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

자체 CA인 Enterprise Certificate Authority를 사용하는 경우 Enterprise를 선택합니다.



- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)
- Manager/vManage(관리자/vManage)에서 ...를 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

vManage에 vBond/Validator 및 vSmart/Controller 온보딩(Onboarding)

20.15/20.18 vManage 노드의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Control Components(제어 구성 요소)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

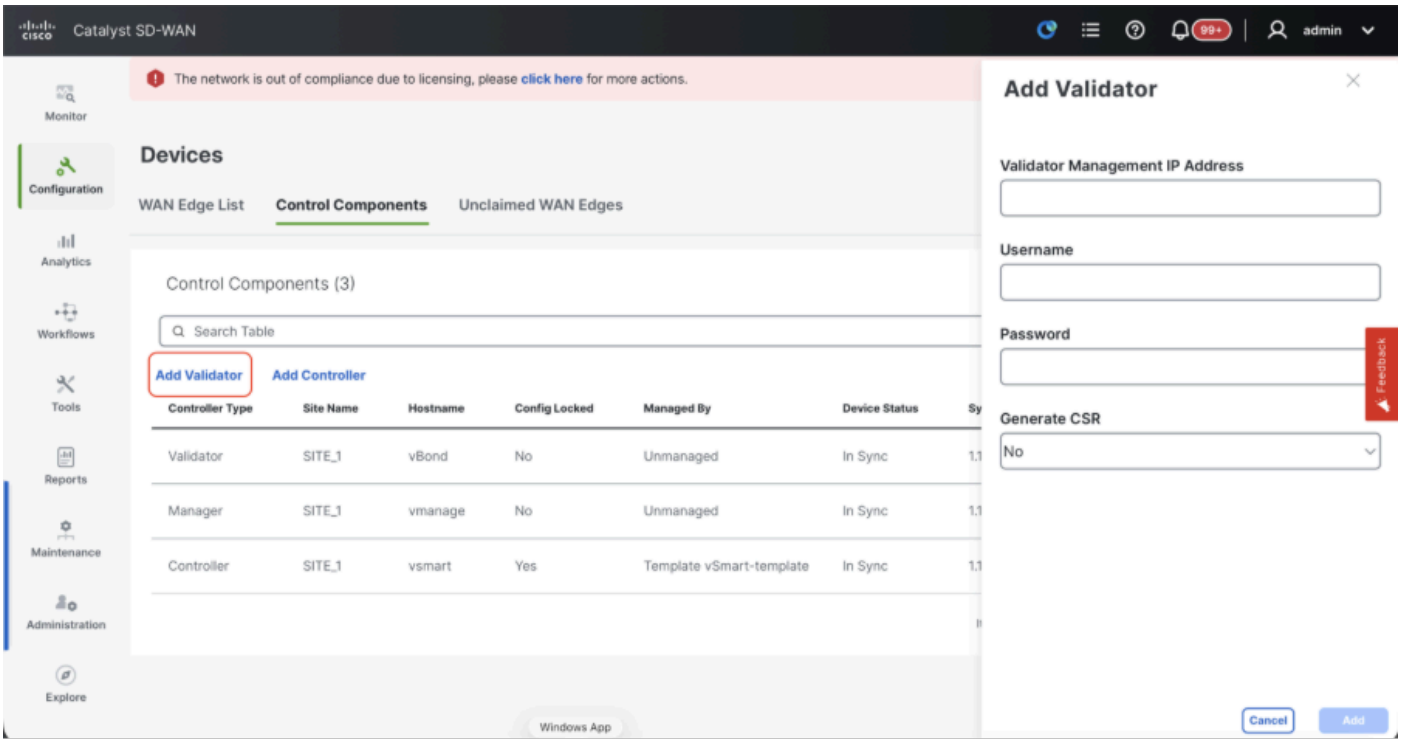
온보딩vBond/Validator

- Add(추가)VBond(vBond 추가)를 클릭합니다.제2012호의 경우유효성 검사기 추가 20.15/20.18 vManage입니다. 팝업이 열리면 vManage에서 연결할 수 있는 vBond의 VPN 0 전송 IP.
- vManagetovBondIP의 CLI에서 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.

- vBond의 사용자 자격 증명을 입력합니다.

참고: vBonor의 관리자 자격 증명 또는 netadmingroup의 사용자 부분이 필요합니다. vBond의 CLI에서 이를 확인할 수 있습니다. vBond에 대한 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다

참고: vBond가 NAT 디바이스/방화벽 뒤에 있는 경우 vBond VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인합니다. vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스의 공용 IP 주소를 사용합니다



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vBond에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vBond가 여러 개인 경우 동일한 단계를 반복합니다.

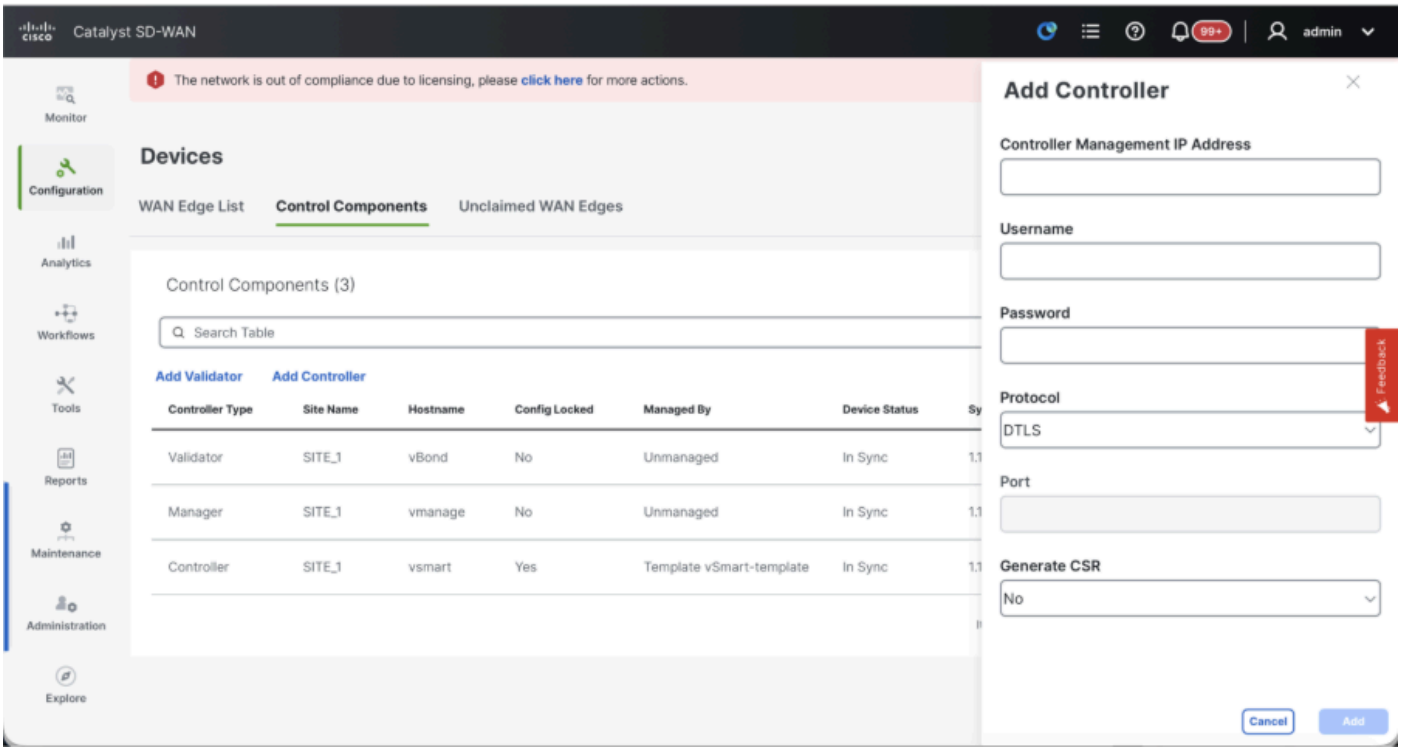
vSmart/Controller 온보딩:

- 20.12 vManage의 경우 vSmart 추가 또는 20.15/20.18 vManage의 경우 컨트롤러 추가를 클

릭합니다.

- 팝업이 열리면 vManage에서 연결할 수 있는 vSmart의 VPN 0 전송 IP를 입력합니다.
- vManage의 CLI에서 vSmart IP로 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.
- vSmart의 사용자 자격 증명을 입력하십시오. vSmart의 관리자 자격 증명 또는 netadmin 그룹의 사용자 부분을 사용해야 합니다.
- vSmart의 CLI에서 이를 확인할 수 있습니다.
- 라우터에 TLS를 사용하여 vSmart와의 제어 연결을 설정하려면 프로토콜을 TLS로 설정합니다. vSmarts 및 vManage 노드의 CLI에서도 이 구성을 구성해야 합니다.
- vSmart용 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다.

참고: vSmart가 NAT 장치/방화벽 뒤에 있는 경우 vSmart VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인하고, vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스 IP의 공용 IP 주소를 사용합니다.

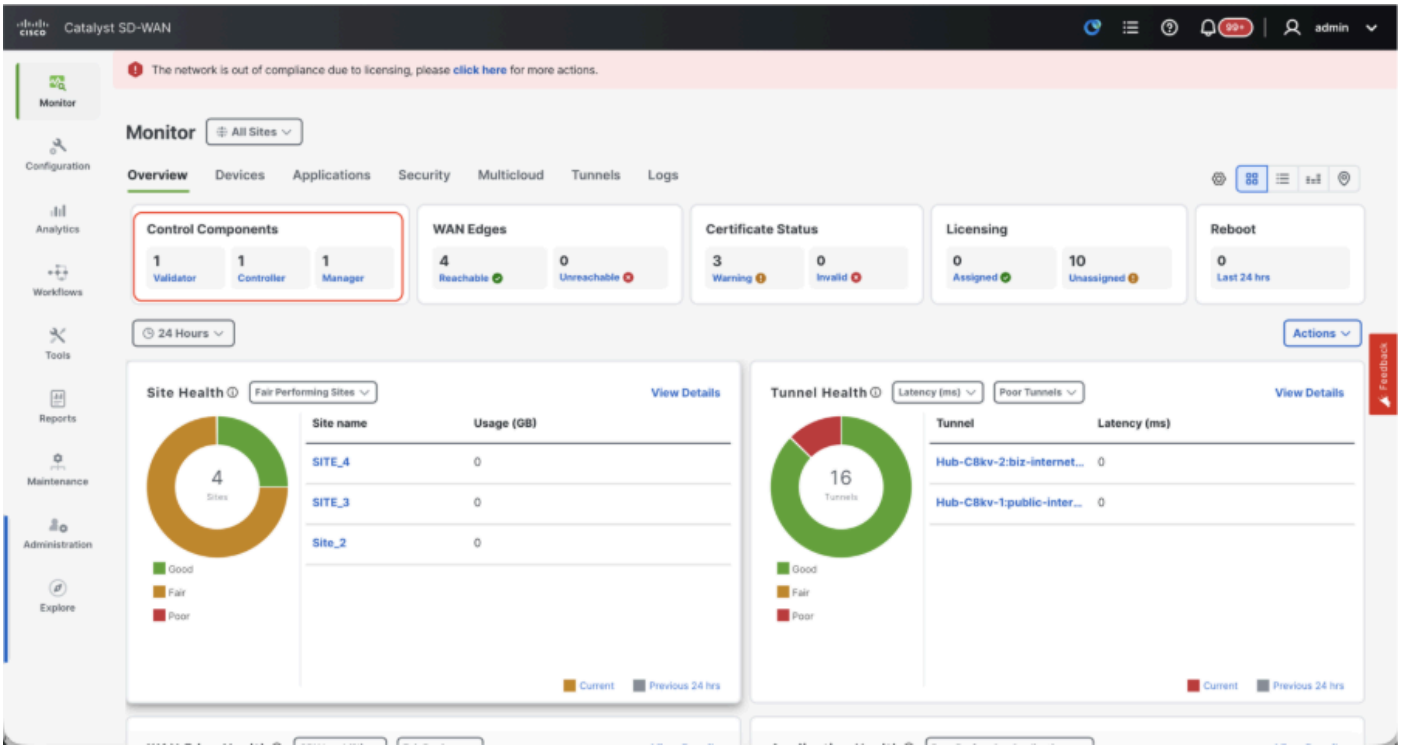


- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vSmart에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다.

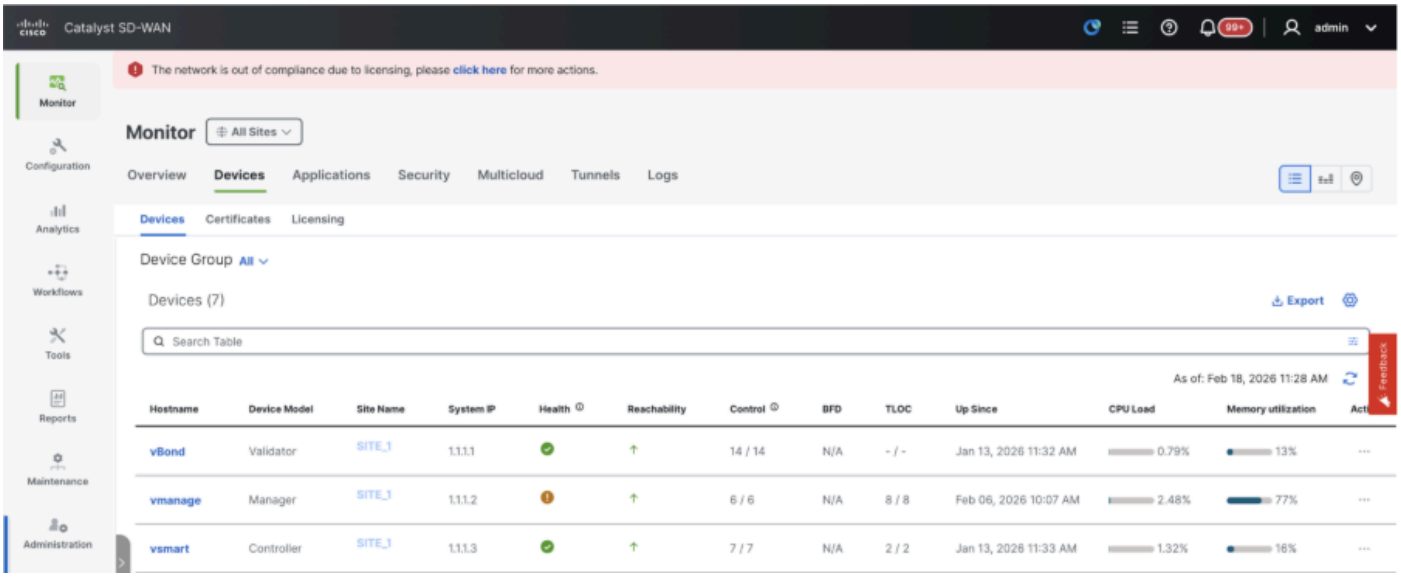
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vSmarts가 여러 개인 경우 동일한 단계를 반복합니다.

확인

모든 단계가 완료되면 Monitor>Dashboard에서 모든 제어 구성 요소에 연결할 수 있는지 확인합니다



- 각 Control(제어) 구성 요소를 클릭하고 모두 연결할 수 있는지 확인합니다.
- Monitor(모니터링) > Devices(디바이스)로 이동하여 모든 제어 구성 요소에 연결할 수 있는지 확인합니다.



3단계: vManage 클러스터 구축

SD-WAN 오버레이에 vManage 클러스터를 포함하는 온보드 SD-WAN 패브릭

참고: SD-WAN 패브릭에 온보딩된 사이트의 수에 따라 vManage 클러스터를 3개의 vManage 노드 또는 6개의 vManage 노드로 구성할 수 있습니다

단일 vManage 노드를 사용하여 모든 SD-WAN 컨트롤러 온보딩

"SD-WAN 오버레이에 단일 노드 vManage를 사용하여 SD-WAN 컨트롤러 온보드"에서 공유하는 단계를 진행하여 먼저 하나의 vManage 노드를 사용하여 SD-WAN 패브릭을 시작하고 필요한 모든 Validator(vBond) 및 컨트롤러(vSmart)를 온보딩합니다.

클러스터의 일부인 모든 vManage 노드의 CLI 컨피그레이션을 구성합니다

- vManage 노드의 나머지를 구성합니다. 3노드 클러스터의 경우 나머지 2개 노드를 구성해야 하고 6노드 클러스터의 경우 5개 노드를 구성해야 합니다.
- 다음과 같이 시스템 컨피그레이션을 구성합니다.

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

참고: URL을 vBond 주소로 사용하는 경우 VPN 0 컨피그레이션에서 DNS 서버 IP 주소를 구성하거나 확인할 수 있는지 확인하십시오.

이러한 컨피그레이션은 라우터 및 나머지 컨트롤러와의 제어 연결을 설정하는 데 사용되는 전송 인터페이스를 활성화하는 데 필요합니다.

```
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
```

컨트롤러에 대한 대역 외 관리 액세스를 활성화하도록 VPN 512 관리 인터페이스도 구성합니다.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

선택적 구성:

- 기존 컨트롤러의 컨피그레이션을 참조할 수 있으며 여기에 나열된 컨피그레이션이 있는 경우 이 컨피그레이션을 새 컨트롤러에 추가할 수 있습니다.
- 라우터가 TLS를 사용하여 vManage 노드와 보안 제어 연결을 설정해야 하는 경우에만 제어 프로토콜을 TLS로 구성합니다. 기본적으로 모든 컨트롤러와 라우터는 DTLS를 사용하여 제어 연결을 설정합니다. 이는 사용자의 요구 사항에 따라 vSmart 및 vManage 노드에서만 필요한 선택적 컨피그레이션입니다.

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

모든 vManage 노드에서 서비스 인터페이스 구성

이미 온보딩된 vManage-1을 포함하여 모든 vManagenodes에서 서비스 인터페이스를 구성합니다. 이 인터페이스는 클러스터 통신에 사용됩니다. 즉, 클러스터에서 vManagenodes 간의 통신을 의미합니다.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

vManagecluster의 모든 노드에서 서비스 인터페이스에 동일한 IP 서브넷이 사용되는지 확인합니다.

클러스터 자격 증명 구성

vManagenodes의 동일한 관리자 자격 증명을 사용하여 vManagecluster를 구성할 수 있습니다. 그렇지 않으면 netadmingroup의 일부인 새 사용자 자격 증명을 구성할 수 있습니다. 새 사용자 자격 증명을 구성하기 위한 컨피그레이션은 다음과 같습니다

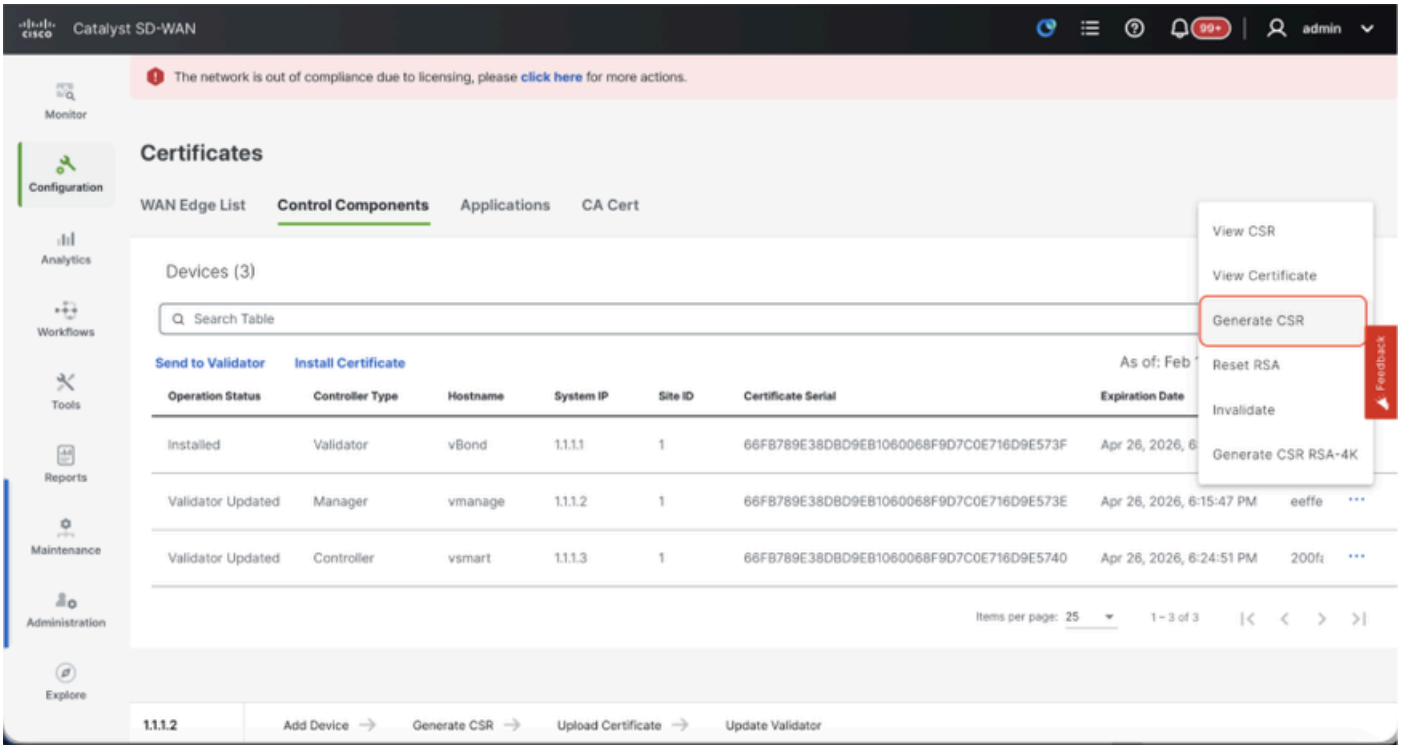
```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

클러스터에 속하는 모든 vManagenodesisc에서 동일한 사용자 자격 증명을 구성해야 합니다.관리자 자격 증명을 사용하려면 모든 vManagenodes에서 동일한 사용자 이름/비밀번호여야 합니다.

모든 vManage 노드에 디바이스 인증서 설치

- 브라우저의 URL https://<vmanage-ip>를 사용하여 모든 vManagenodes의 vManageUI에 로그인합니다. 각 vManagenodes의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

  Manager/vManage(관리자/vManage)에서 ...을 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다.
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

- 클러스터의 일부인 모든 vManage 노드에서 이 단계를 완료합니다.

vManage 클러스터 구축 준비

  - vManage-1의 webUI에서 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고 vManage-1에 대한 Actions(작업) 아래에서 ...를 클릭한 후 Edit(수정)를 선택합니다.
  - 노드 페르소나는 VM이 스핀업되는 동안 선택한 페르소나에 따라 자동으로 선택됩니다.

참고: 3노드 클러스터의 경우 3개의 vManage 노드 모두 컴퓨팅+데이터가 페르소나로 표시됩니다.

- 6노드 클러스터의 경우 3개의 vManage 노드가 compute+data를 페르소나로, 3개의 vManage 노드가 data를 페르소나로 가져옵니다.
- 관리자 IP 주소의 드롭다운에서 vManage의 서비스 인터페이스 IP를 선택해야 합니다.
- vManage 클러스터를 활성화하는 데 사용할 사용자 이름 및 비밀번호를 입력합니다. 이를 클러스터 자격 증명이라고 합니다.
- 앞에서 언급한 것처럼 모든 vManage 노드에서 동일한 자격 증명을 구성해야 하며 모든 노드를 클러스터에 추가하는 동안 사용해야 합니다.

선택적 구성:

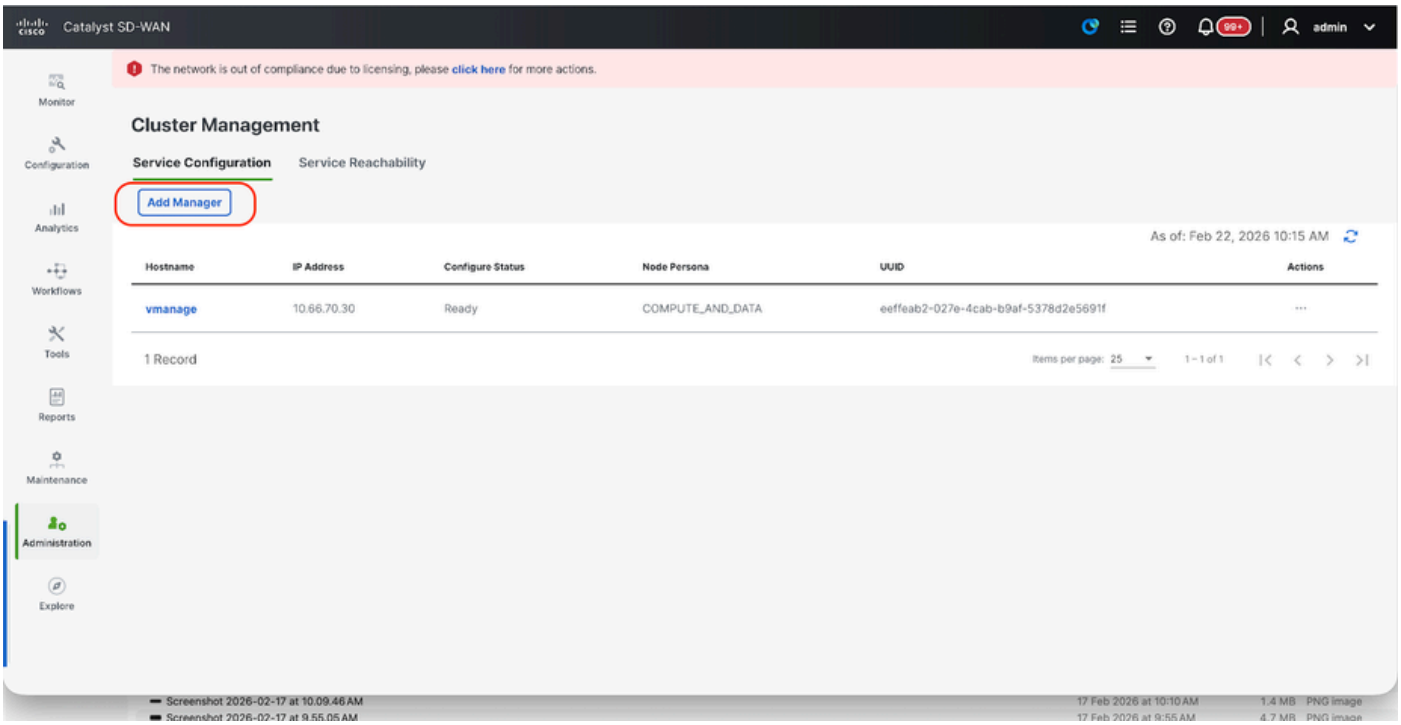
SDAVC를 활성화하려면 기존 클러스터의 이 컨피그레이션을 참조하시기 바랍니다. SDAVC가 필요하고 클러스터의 한 vManage 노드에서만 필요한 경우에만 이 컨피그레이션을 확인해야 합니다.

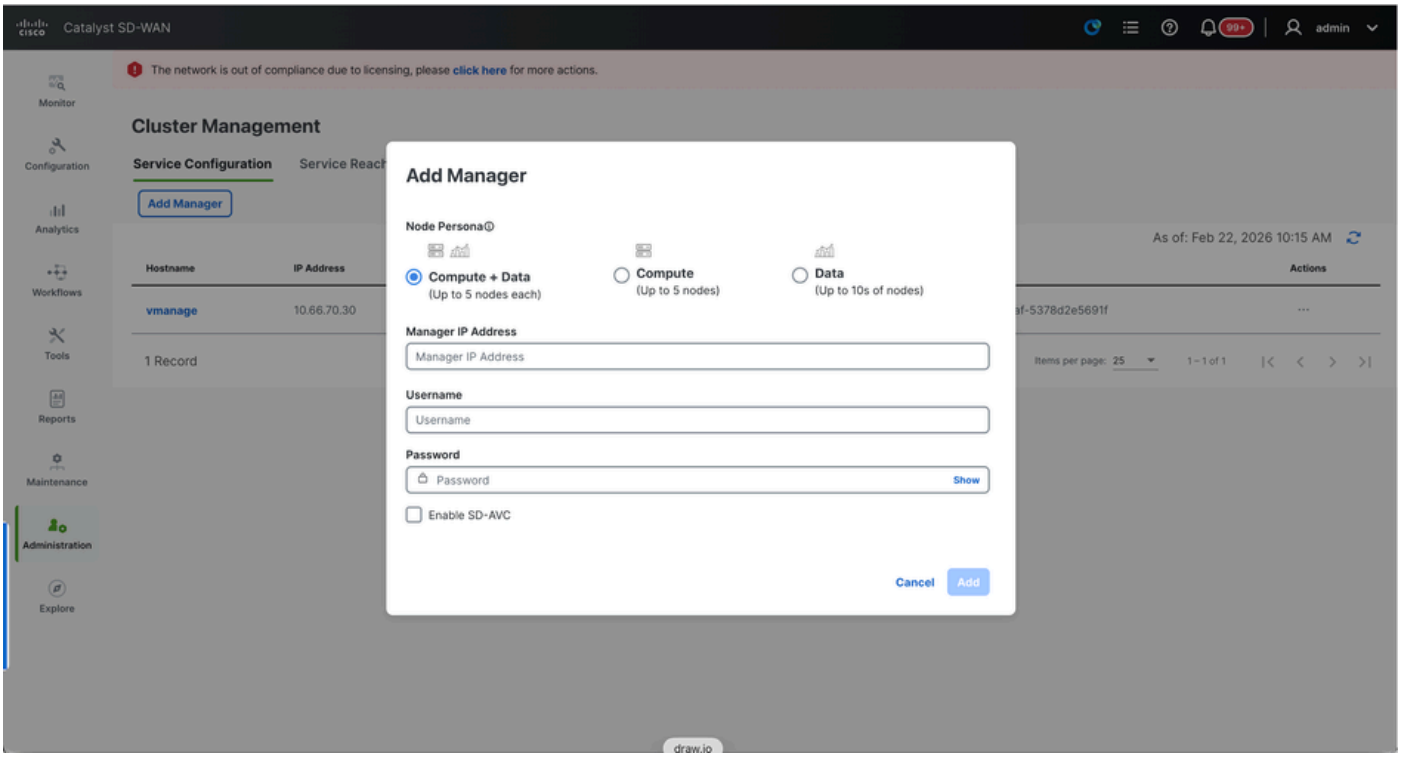
Update(업데이트)를 클릭합니다.

- 이 게시물을 올리면 백그라운드에서 vManage NMS 서비스가 다시 시작되고 5~10분 정도의 몇 분 동안 UI를 사용할 수 없습니다. 이 기간 동안 vManage의 CLI 액세스를 사용할 수 있습니다.
- vManage-1 UI에 액세스할 수 있게 되면 Administration(관리) > Cluster Management(클러스터 관리)로 이동하며, vManage의 서비스 인터페이스 IP가 IP 주소 아래에 반영되는지 확인합니다.Configure Status(상태 구성)가 Ready(준비)이고 노드 페르소나가 올바르게 반영됩니다. 같은 페이지의 서비스 연결 가능 섹션으로 전환하고 모든 서비스에 연결할 수 있는지 확인합니다.
- 아직 연결되지 않은 서비스가 있는 경우 잠시 기다려 주십시오. 보통 20분에서 30분 정도 걸립니다.

vManage 클러스터 구축

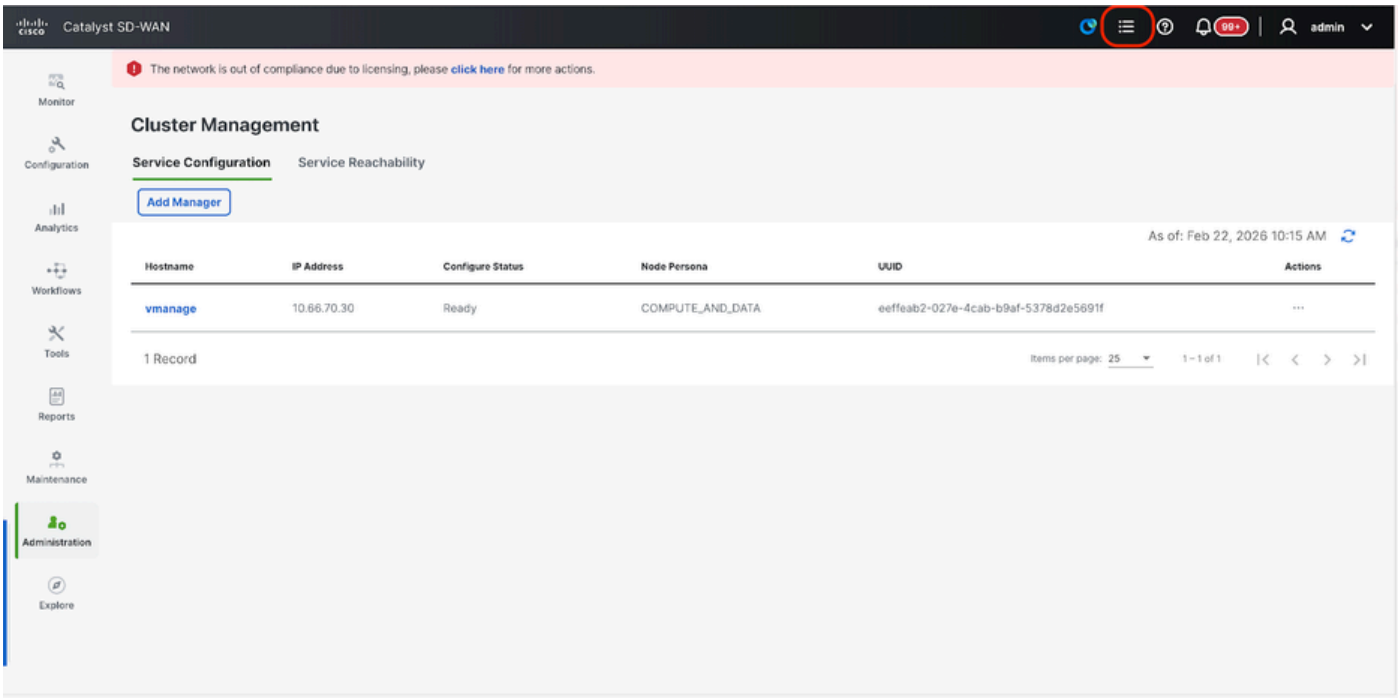
- vManage-1의 webUI에서 Service Configuration(서비스 컨피그레이션) 섹션의 Administration(관리) > Cluster Management(클러스터 관리)로 이동합니다.
- Add Manager(관리자 추가)를 클릭하면 팝업 창이 나타납니다.





- vManage - 2 노드를 스핀업하는 동안 수행한 페르소나 컨피그레이션에 따라 노드 페르소나를 선택합니다.
- 관리자 IP 주소 아래 vManage-2의 서비스 인터페이스 IP를 입력합니다
- 사용자 이름과 비밀번호를 입력합니다. 이는 6단계에서 사용한 것과 동일한 자격 증명입니다 .
- Enable SDAVC(SDAVC 활성화) - vManage-1에서 SDAVC를 이미 활성화했으므로 선택하지 않은 상태로 둡니다.
- Add(추가)를 클릭합니다.
- 이를 게시하면 vManage NMS 서비스가 백그라운드에서 vManage 1 및 2 노드에 대해 다시 시작됩니다. vManage 1 및 2의 경우 약 5~10분 동안 UI를 사용할 수 없습니다.

- 이 기간 동안 vManage 1 및 2의 CLI 액세스를 사용할 수 있습니다.
- vManage-1 UI에 액세스할 수 있게 되면 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고, vManage의 서비스 인터페이스 IP가 모두 IP 주소에 반영되었는지 확인하고, Configure Status(구성 상태)가 Ready(준비)이고 노드 페르소나가 올바르게 반영되었는지 확인합니다.
- 동일한 페이지의 서비스 연결 가능 섹션으로 전환하고 vManage 노드 모두에 대해 모든 서비스에 연결할 수 있는지 확인합니다.
- 아직 연결되지 않은 서비스가 있는 경우 잠시 기다려 주십시오. 보통 5분에서 10분 정도 걸립니다.
- vManage UI의 오른쪽 상단 모서리에 있는 Task-list(작업 목록)에서 클러스터 추가 프로세스의 상태를 확인할 수 있습니다.



- Active(활성) 작업 목록을 조회할 수 있으며, 작업이 Active(활성) 작업 목록 아래에 여전히 나열되어 있으면 작업이 아직 완료되지 않았음을 나타냅니다.
- 작업을 클릭하여 진행 상태를 확인할 수 있습니다. 작업이 활성 작업 목록에 나열되지 않으면 완료로 전환하고 작업이 성공적으로 완료되었는지 확인하십시오.
- 이러한 점이 검증된 후에만 다음 단계로 진행합니다.

클러스터에 다음 노드를 추가하기 전에 이러한 점을 고려해야 합니다.

지금까지 클러스터에 추가된 vManage 노드의 모든 UI에서 다음 사항을 확인하십시오.

- Monitor(모니터) > Overview of vManage UI(vManage UI 개요)로 이동하여 vManage 노드 수가 올바르게 반영되고 클러스터에 추가된 노드 수에 따라 연결 가능한 것으로 표시되는지 확인합니다.

- Administration(관리) > Cluster Management(클러스터 관리)로 이동하여 IP 주소 아래에 vManage의 서비스 인터페이스 IP가 모두 반영되고, Configure Status(구성 상태)가 Ready(준비)이고 노드 페르소나가 올바르게 반영되었는지 확인합니다.
- 같은 페이지의 서비스 연결 가능 섹션으로 전환하고 모든 서비스가 두 vManage 노드 모두에

연결할 수 있는지 확인합니다.

- 노드가 클러스터에 추가될 때마다 클러스터에 있는 모든 노드의 NMS 서비스가 다시 시작되므로 해당 노드의 UI에 한동안 연결할 수 없게 됩니다.
- 클러스터의 노드 수에 따라 UI를 백업하고 모든 서비스에 연결하는 데 더 오랜 시간이 걸릴 수 있습니다.
- vManage UI의 오른쪽 상단 모서리에 있는 Task-list(작업 목록)에서 작업을 모니터링할 수 있습니다.
- 클러스터에 추가된 각 노드의 vManage UI에서 vManage-1에서 사용 가능한 모든 라우터, 템플릿 및 정책을 확인해야 합니다.
- 이러한 컨피그레이션이 vManage-1에 없는 경우 vManage-1에 추가된 vBonds 및 vSmarts와 Administration(관리) > Settings(설정) 컨피그레이션에서 Organization-name(조직 이름), vBond, Certificate Authorization(인증서 권한 부여)이 클러스터에 추가된 나머지 vManage 노드에 반영되어야 합니다.
- 나머지 vManage 노드에 대해서도 동일한 단계를 반복합니다.

4단계: 콜드 스탠바이 DR 클러스터 설정

콜드 스탠바이 DR 클러스터 설정

4단계에 설명된 단계를 사용하여 vManage 클러스터를 하나 이상 시작할 수 있습니다. vManage 클러스터 구축 6단계에 설명된 단계를 완료하는 게시물: Config-db Backup/Restore - 대기 클러스터에서 config-db 백업을 복원합니다.

5단계: Config-db 백업/복원

다른 vManage 노드에서 vManage configuration-db 백업 및 복원 수집

Configuration-DB 백업 수집:

- 현재 사용 중인 SD-WAN 패브릭에서는 vManage 클러스터에서 configuration-db 백업을 생성할 수 있습니다.
- configuration-db 백업은 configuration-db 리더인 vManage 클러스터의 한 노드에서만 생성해야 합니다.

- 독립형 vManage의 경우 해당 vManage 자체가 configuration-db 리더입니다.
- vManage 클러스터에서 request nms configuration-db diagnostics 명령을 사용하여 configuration-db 리더 노드를 식별합니다.3노드 vManage 클러스터의 모든 노드에서 이 명령을 실행할 수 있습니다.
- 6노드 클러스터에서 컨피그레이션 DB가 활성화되어 리더 노드를 식별하는 vManage 노드에서 이 명령을 실행해야 합니다. Administration(관리) > Cluster Management(클러스터 관리)로 이동하여 다음을 확인합니다.
- 스크린샷에서 볼 수 있듯이, COMPUTE_AND_DATA 페르소나로 구성된 노드는 컨피그레이션 DB가 실행 중입니다.

vManageCLI에서 requestnmsconfiguration-dbstatus 명령을 사용하여 동일한 사항을 확인할 수 있습니다. 출력은 다음과 같습니다

```
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#
```

- 명령을 실행하면이러한 노드에서 nms configuration-db 진단을 요청하면 다음과 같이 출력됩니다.
- "IsLeader"에 대해 강조 표시된 필드를 찾습니다. 1로 설정된 경우 노드가 리더 노드임을 나타내며, 여기서 configuration-db 백업을 수집할 수 있습니다.

```
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     .
```

식별된 configuration-db leader vManage 노드에서 configuration-db 백업을 수집하려면 이 명령을 사용합니다.

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

예상 출력은 다음과 같습니다.

```
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#
```

- 컨피그레이션 DB 자격 증명이 업데이트된 경우 기록해 둡니다.
- configuration-db 자격 증명을 모르는 경우 TAC에 문의하여 기존 vManage 노드에서 configuration-db 자격 증명을 검색합니다.
- 기본 configuration-db 자격 증명은 사용자 이름입니다. neo4j 및 비밀번호: 암호

다른 vManage 노드에 Configuration-db 백업 복원

SCP를 사용하여 configuration-db 백업을 vManage의 /home/admin/ 디렉토리에 복사합니다.

샘플 scp 명령 출력:

```
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 백업을 복원하려면 먼저 configuration-db 자격 증명을 구성해야 합니다. configuration-db 자격 증명이 default(neo4j/password)인 경우 이 단계를 건너뛸 수 있습니다.

configuration-db 자격 증명을 구성하려면 nms configuration-db update-admin-user 명령을 사용합니다.선택한 사용자 이름과 비밀번호를 사용합니다.

vManage의 애플리케이션 서버가 다시 시작됩니다. 따라서 vManage UI에 짧은 시간 동안 액세스할 수 없게 됩니다.

```
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#
```

구성 DB 백업을 복원하기 위해 진행할 수 있는 게시:

nms configuration-db 복원 경로 /home/admin/< > 명령을 사용하여 configuration-db를 새 vManage로 복원할 수 있습니다.

```
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-db가 복원되면 vManage UI에 액세스할 수 있는지 확인합니다. 약 5분 정도 기다린 후 UI에 액세스를 시도합니다.

UI에 성공적으로 로그인했으면 Edge 라우터 목록, 템플릿, 정책 및 이전 또는 기존 vManage UI에 존재했던 나머지 모든 컨피그레이션이 새 vManage UI에 반영되었는지 확인합니다.

6단계: 컨트롤러 재인증 및 이전 컨트롤러 무효화

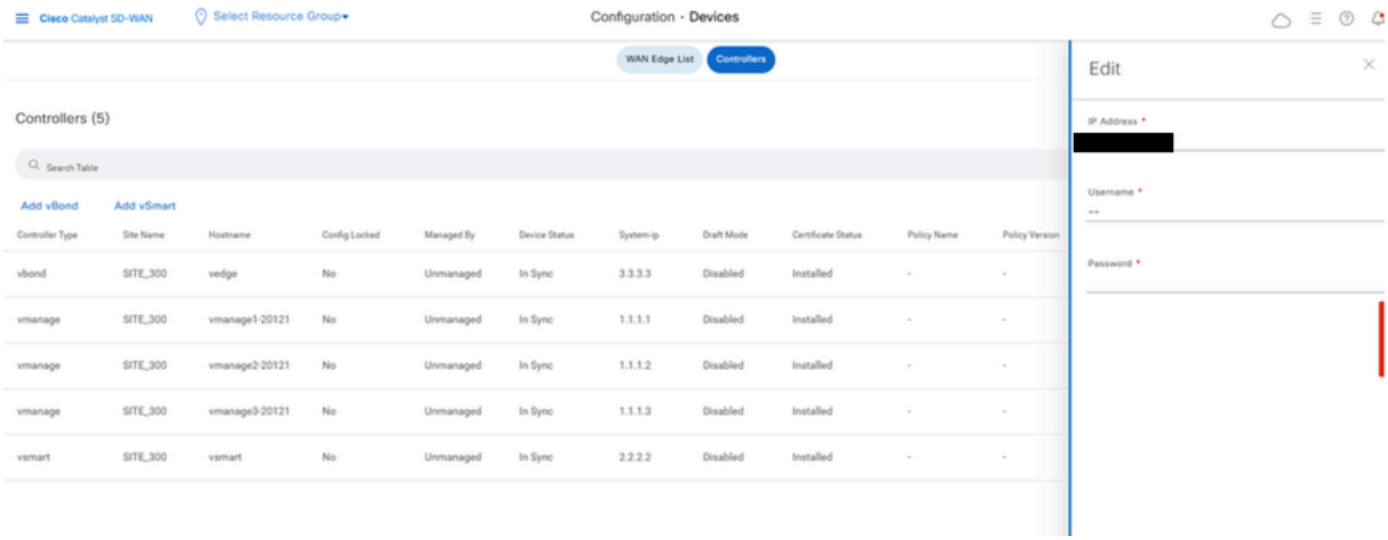
configuration-db가 복원되면 패브릭에서 모든 새 컨트롤러(vmanage/vsmart/vbond)를 재인증해야 합니다

참고: 실제 프로덕션에서는 재인증에 사용되는 인터페이스 IP가 터널 인터페이스 IP인 경우 vManage, vSmart 및 vBond의 터널 인터페이스 및 경로에 따른 방화벽에서 NETCONF 서비스가 허용되는지 확인해야 합니다. 열 방화벽 포트는 DR 클러스터에서 모든 vBonds 및 vSmarts로의 양방향 규칙인 TCP 포트 830입니다.

---

vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다

- 각 컨트롤러 근처의 점 3개를 클릭하고 Edit(수정)를 클릭합니다



- ip-address(컨트롤러의 system-ip)를 transport vpn 0(tunnel interface) ip 주소로 바꿉니다. 사용자 이름과 암호를 입력하고 save(저장)를 클릭합니다
- 패브릭에 있는 모든 새 컨트롤러에 대해 동일한 작업을 수행합니다.

루트 인증서 체인 동기화

모든 컨트롤러가 온보딩되면 다음 단계를 완료합니다.

새로 활성화된 클러스터의 Cisco SD-WAN Manager 서버에서 다음 작업을 수행합니다.

루트 인증서를 새로 활성화된 클러스터의 모든 Cisco Catalyst SD-WAN 디바이스와 동기화하려면 다음 명령을 입력합니다.

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

Cisco SD-WAN Manager UUID를 Cisco SD-WAN Validator와 동기화하려면 다음 명령을 입력합니다.

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

패브릭이 복원되고 패브릭의 모든 에지와 컨트롤러에 대해 제어 및 bfd 세션이 작동되면 UI에서 이전 컨트롤러(vmanage/vsmart/vbond)를 무효화해야 합니다

- vmanage UI에서 Configuration > Devices > Certificates를 클릭합니다
- Controllers(컨트롤러) 클릭
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. Invalidate를 클릭합니다.
- Send to Bond를 클릭합니다.
- vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. 삭제를 클릭합니다.

7단계: 수표 게시

참고: 여기에 표시된 모든 구축 조합에 공통적으로 적용되는 Post Checks(사후 검사) 섹션을 계속 진행합니다.

조합 5: vManage 클러스터 + DR 사용

필요한 인스턴스:

- 3 또는 6 vManage(기본 클러스터)
- 3 또는 6 vManage(DR 대기 클러스터)
- 1개 이상의 vBond(기본 및 DR 데이터 센터에 분산)
- 1개 이상의 vSmart(기본 및 DR 데이터 센터에 분산)

단계:

1. 공통 단계를 사용하여 모든 인스턴스 가져오기
2. 사전 확인
3. vManage UI, 인증서 및 온보드 컨트롤러 구성
4. vManage 클러스터 구축
5. 콜드 스탠바이 DR 클러스터 설정
6. Config-db 백업/복원
7. 수표 게시

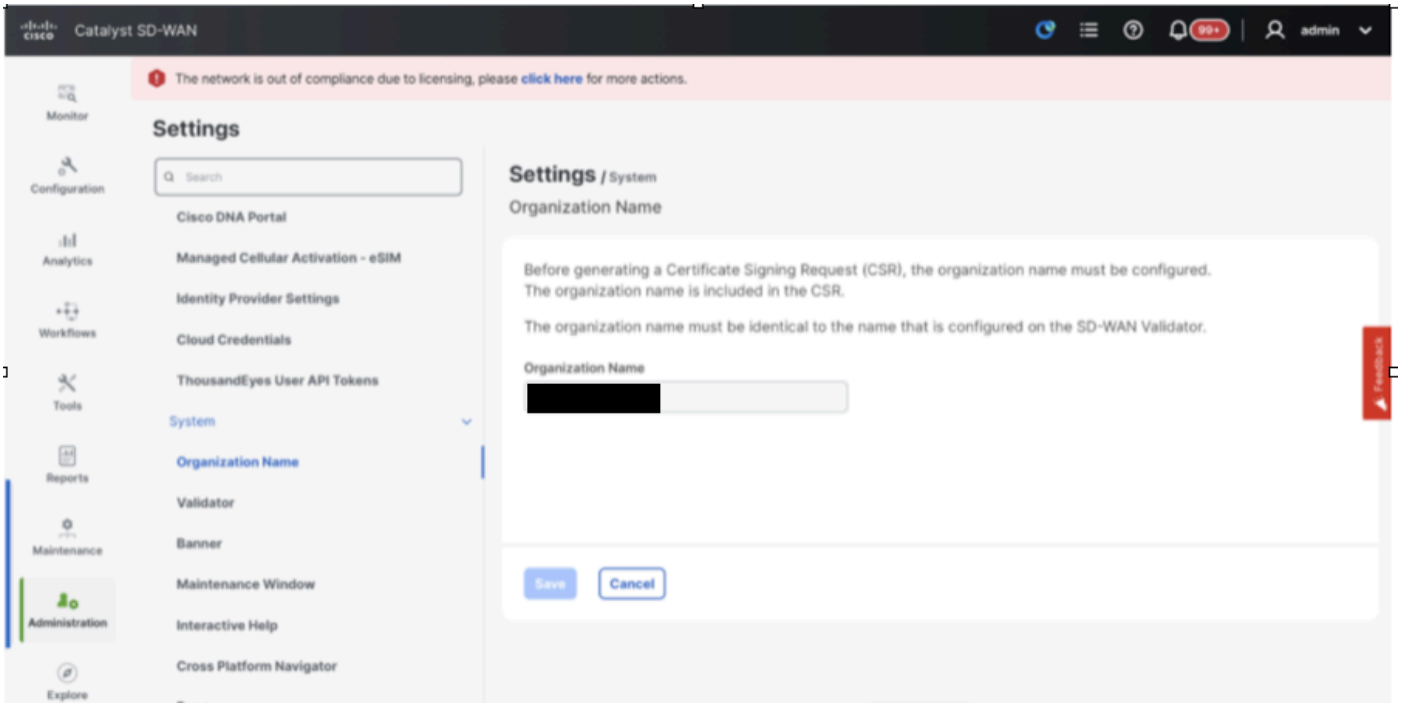
1단계: 사전 확인

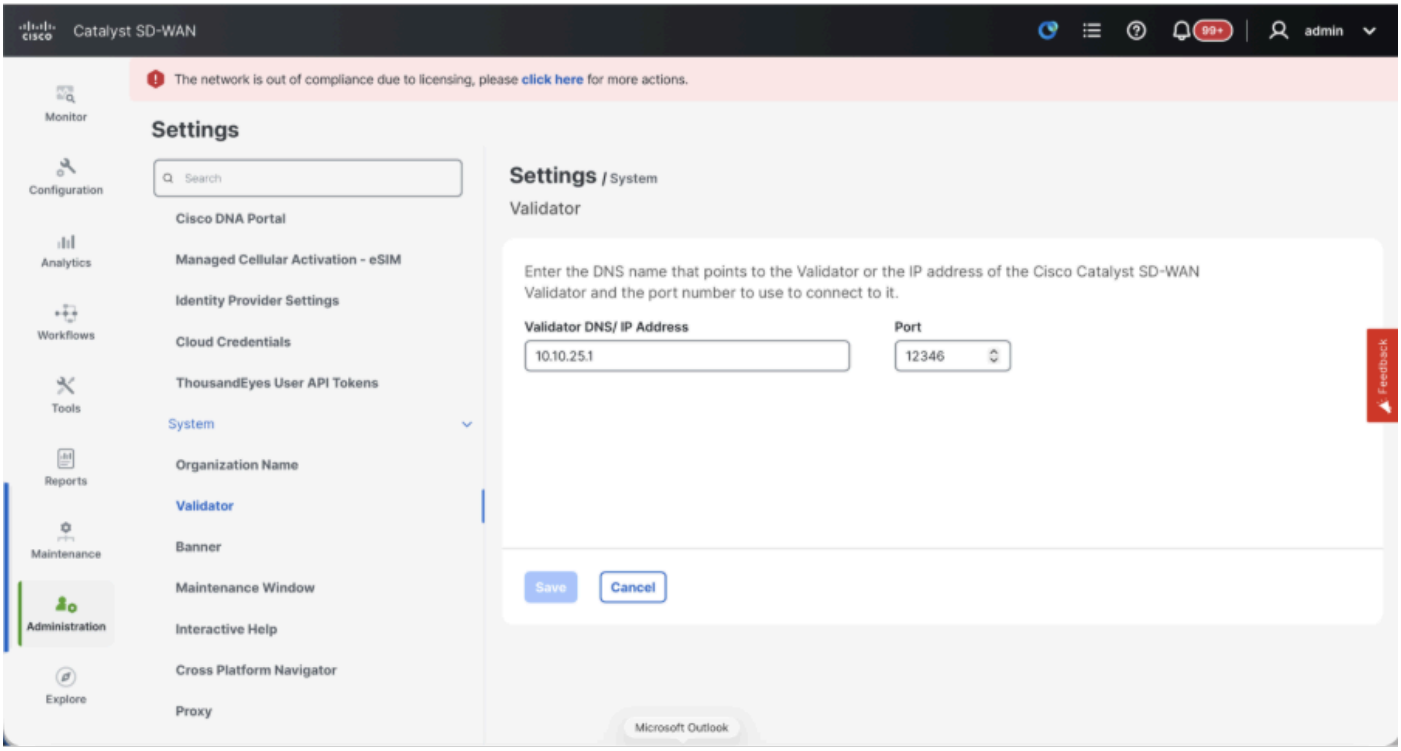
- 활성 Cisco SD-WAN Manager 인스턴스의 수가 새로 설치된 Cisco SD-WAN Manager 인스턴스의 수와 동일한지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 동일한 소프트웨어 버전을 실행하는지 확인합니다.
- 모든 활성 및 새로운 Cisco SD-WAN Manager 인스턴스가 Cisco SD-WAN Validator의 관리 IP 주소에 연결할 수 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스에 인증서가 설치되어 있는지 확인합니다.
- 새로 설치된 Cisco SD-WAN Manager 인스턴스를 포함하여 모든 Cisco Catalyst SD-WAN 디바이스의 시계가 동기화되었는지 확인합니다.
- 새 시스템 IP 및 사이트 ID 집합이 활성 클러스터와 동일한 기본 구성과 함께 새로 설치된 Cisco SD-WAN Manager 인스턴스에 구성되어 있는지 확인합니다.

2단계: vManage UI, 인증서 및 온보드 컨트롤러 구성

vManage UI에서 컨피그레이션 업데이트

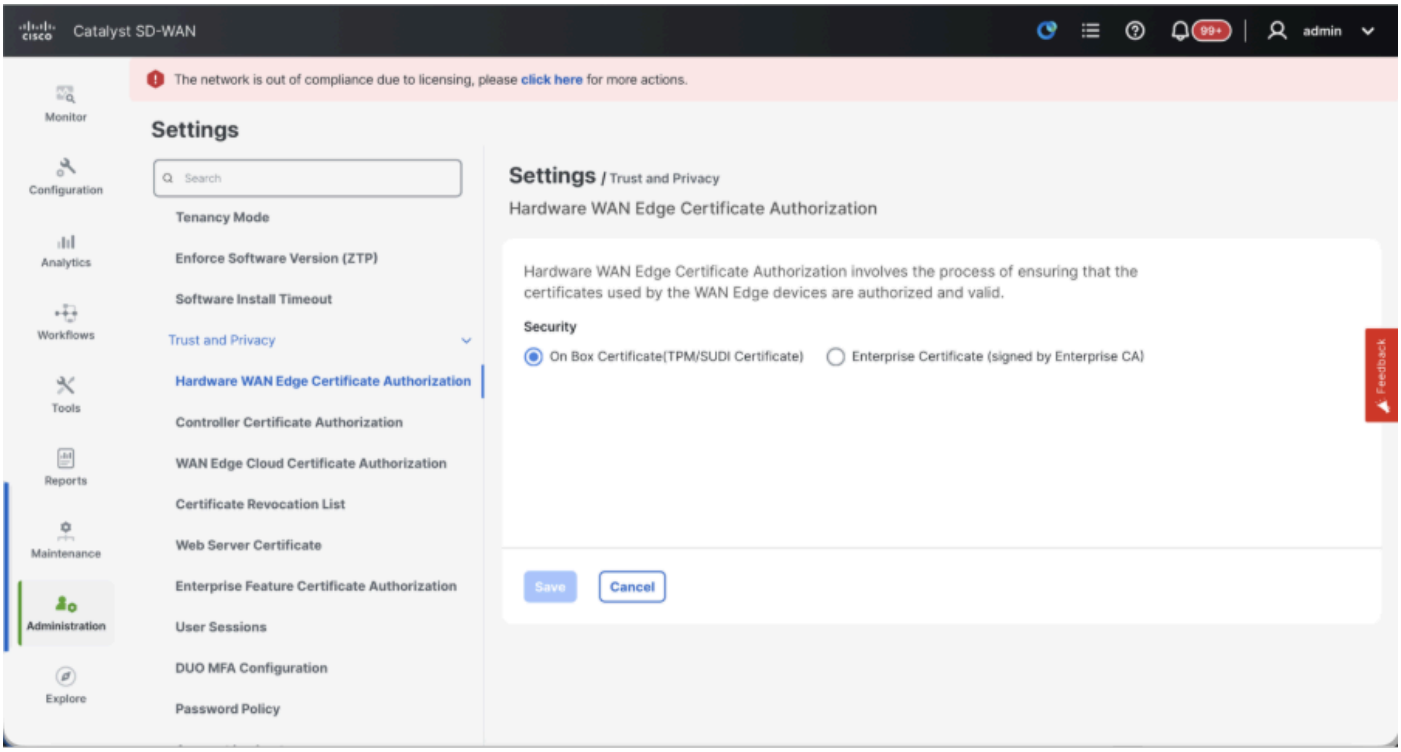
- 1단계의 컨피그레이션이 모든 컨트롤러의 CLI에 추가되면 브라우저의 URL https://<vmanage-ip>를 사용하여 vManage의 webUI에 액세스할 수 있습니다. 각 vManage 노드의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Administration(관리) > Settings(설정)로 이동하여 다음 단계를 완료합니다.
- 조직 이름 및 검증기/vBond URL/IP 주소를 구성합니다. vManage 노드의 CLI에서와 동일한 값을 구성합니다.
- vManage 20.15/20.18의 섹션 System에서 이러한 구성을 사용할 수 있습니다.



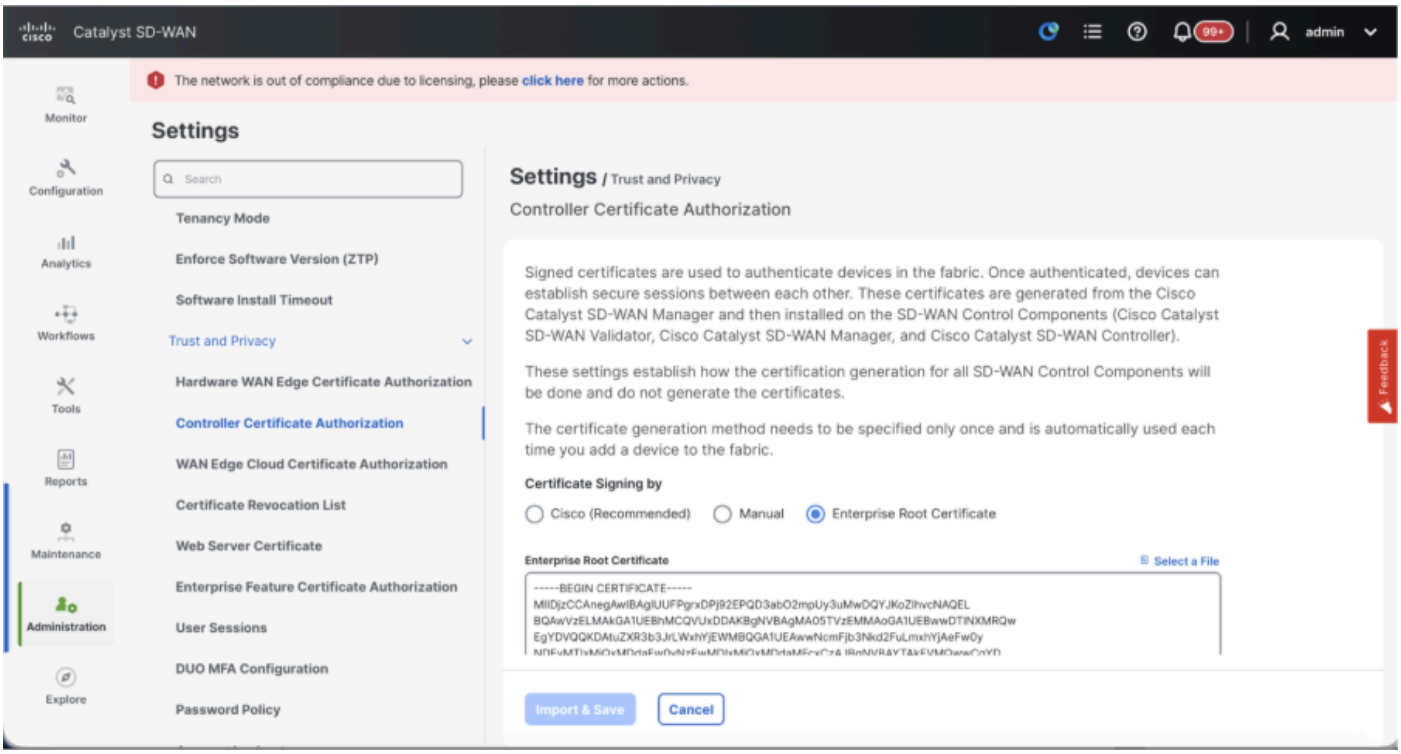


- 인증서 서명에 사용되는 인증 기관을 결정하는 CA(Certificate Authorization)의 컨피그레이션을 확인합니다. 3가지 옵션이 있습니다.

1. Hardware WAN Edge Certificate Authorization - 하드웨어 SD-WAN 에지 라우터의 CA를 결정합니다.
    - On Box Certificate(TPM/SUDI 인증서) - 이 옵션을 사용하면 라우터 하드웨어에 미리 설치된 인증서를 사용하여 제어 연결(TLS/DTLS 연결)을 설정합니다
    - 엔터프라이즈 인증서(Enterprise CA에서 서명) - 이 옵션을 사용하면 라우터가 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

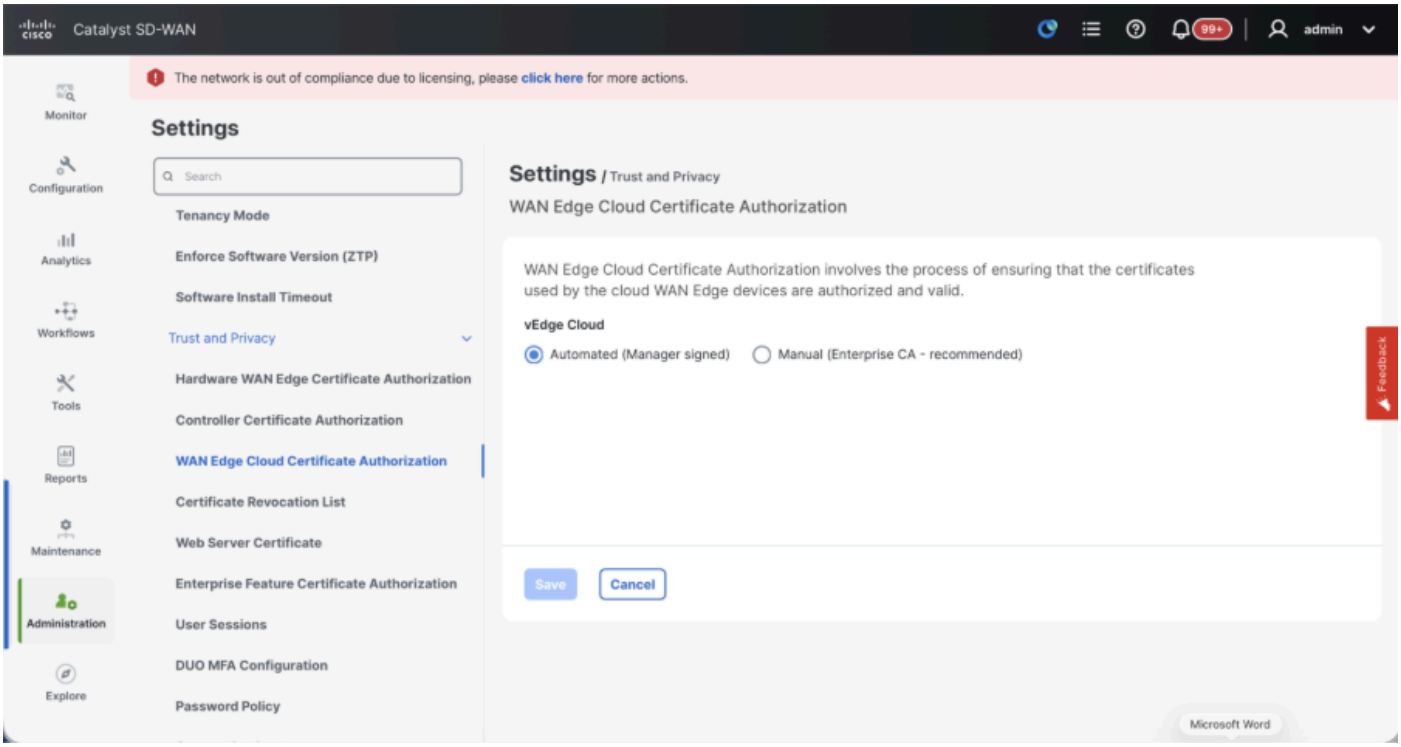


2. Controller Certificate Authorization(컨트롤러 인증서 권한 부여) - SD-WAN 컨트롤러에 대한 CA를 결정합니다.
    - Cisco(권장) - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. vManage는 vManage에 구성된 스마트 어카운트 자격 증명을 사용하여 PNP 포털에 자동으로 연결하고 서명된 인증서를 가져오며 컨트롤러에 설치됩니다.
    - 수동 - 컨트롤러는 Cisco PKI에서 서명한 인증서를 사용합니다. 각 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 수동으로 CSR에 서명합니다.
    - Enterprise Root Certificate(엔터프라이즈 루트 인증서) - 이 옵션을 사용하면 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

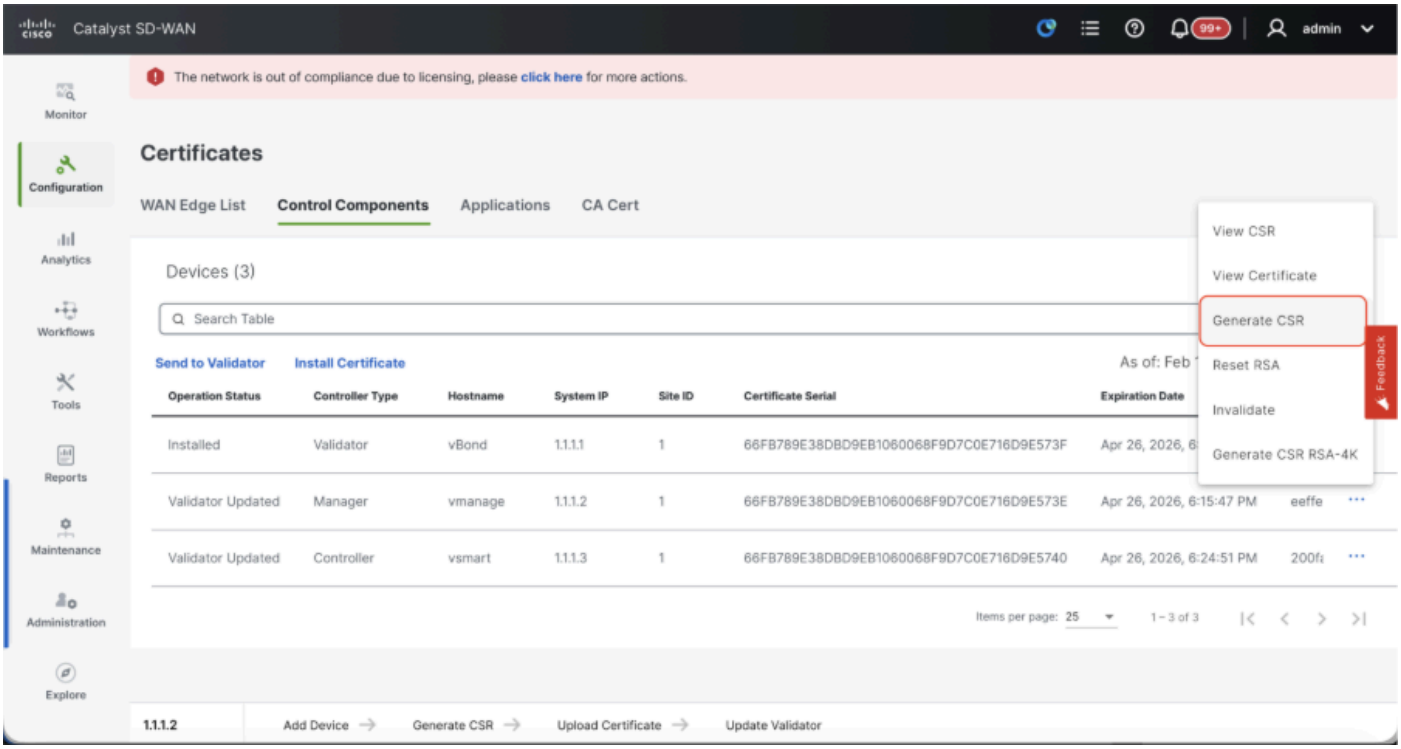


3. WAN Edge Cloud Certificate Authorization - 가상 SD-WAN Edge 라우터(CSR1000v, C8000v, vEdge 클라우드)에 대한 CA를 결정합니다.
    - 자동(vManage signed) - vManage는 가상 에지 라우터의 CSR에 자동으로 서명하고 라우터에 인증서를 설치합니다.
    - 수동(엔터프라이즈 CA - 권장) - 가상 라우터는 조직의 엔터프라이즈 인증 기관에서 서명한 인증서를 사용합니다. 이 옵션을 선택하는 동안 엔터프라이즈 CA의 루트 인증서를 여기서 업데이트해야 합니다.

자체 CA인 Enterprise Certificate Authority를 사용하는 경우 Enterprise를 선택합니다.



- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)
- Manager/vManage(관리자/vManage)에서 ...를 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

vManage에 vBond/Validator 및 vSmart/Controller 온보딩(Onboarding)

20.15/20.18 vManage 노드의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Control Components(제어 구성 요소)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

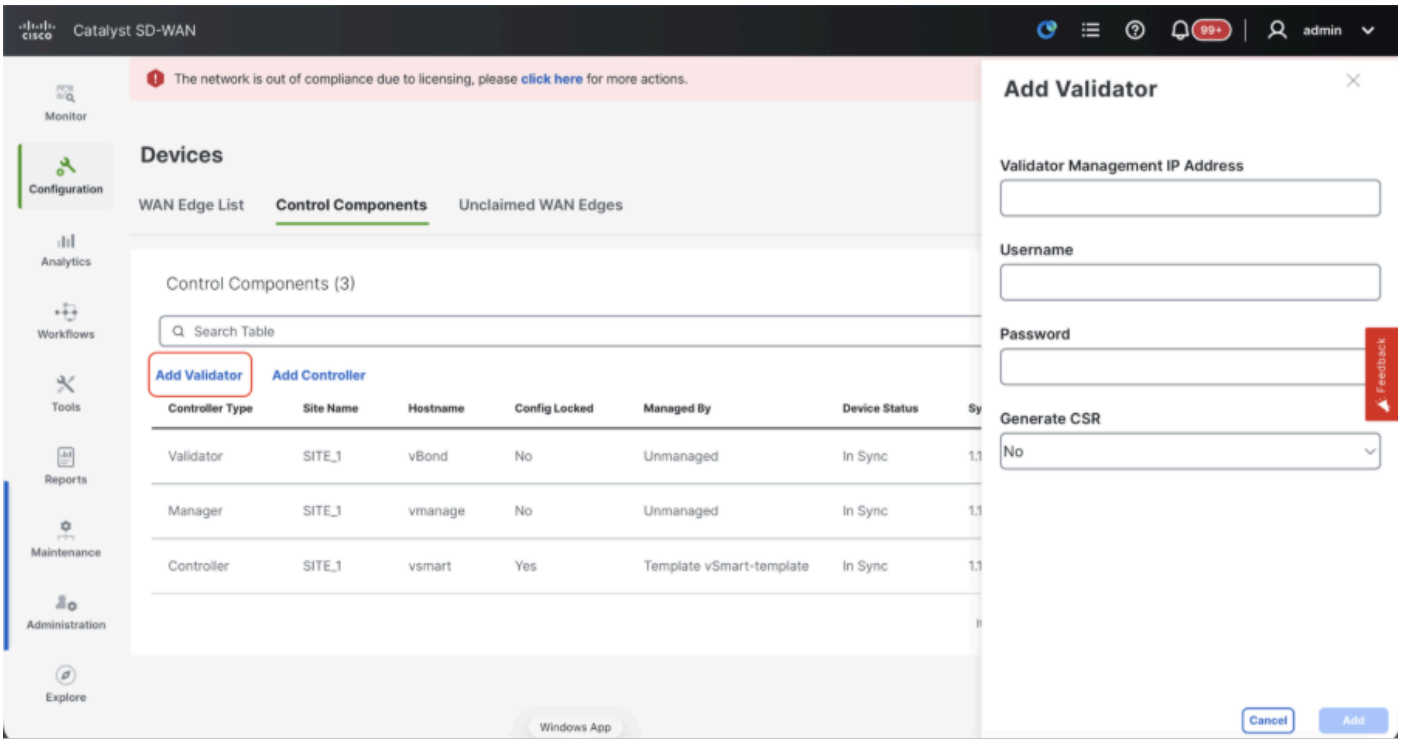
온보딩vBond/Validator

- Add(추가)VBond(vBond 추가)를 클릭합니다.제2012호의 경우유효성 검사기 추가 20.15/20.18 vManage입니다. 팝업이 열리면 vManage에서 연결할 수 있는 vBond의 VPN 0 전송 IP.
- vManagetovBondIP의 CLI에서 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.

- vBond의 사용자 자격 증명을 입력합니다.

참고: vBonor의 관리자 자격 증명 또는 netadmingroup의 사용자 부분이 필요합니다. vBond의 CLI에서 이를 확인할 수 있습니다. vBond에 대한 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다

참고: vBond가 NAT 디바이스/방화벽 뒤에 있는 경우 vBond VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인합니다. vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스의 공용 IP 주소를 사용합니다



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vBond에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다. PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다. Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vBond가 여러 개인 경우 동일한 단계를 반복합니다.

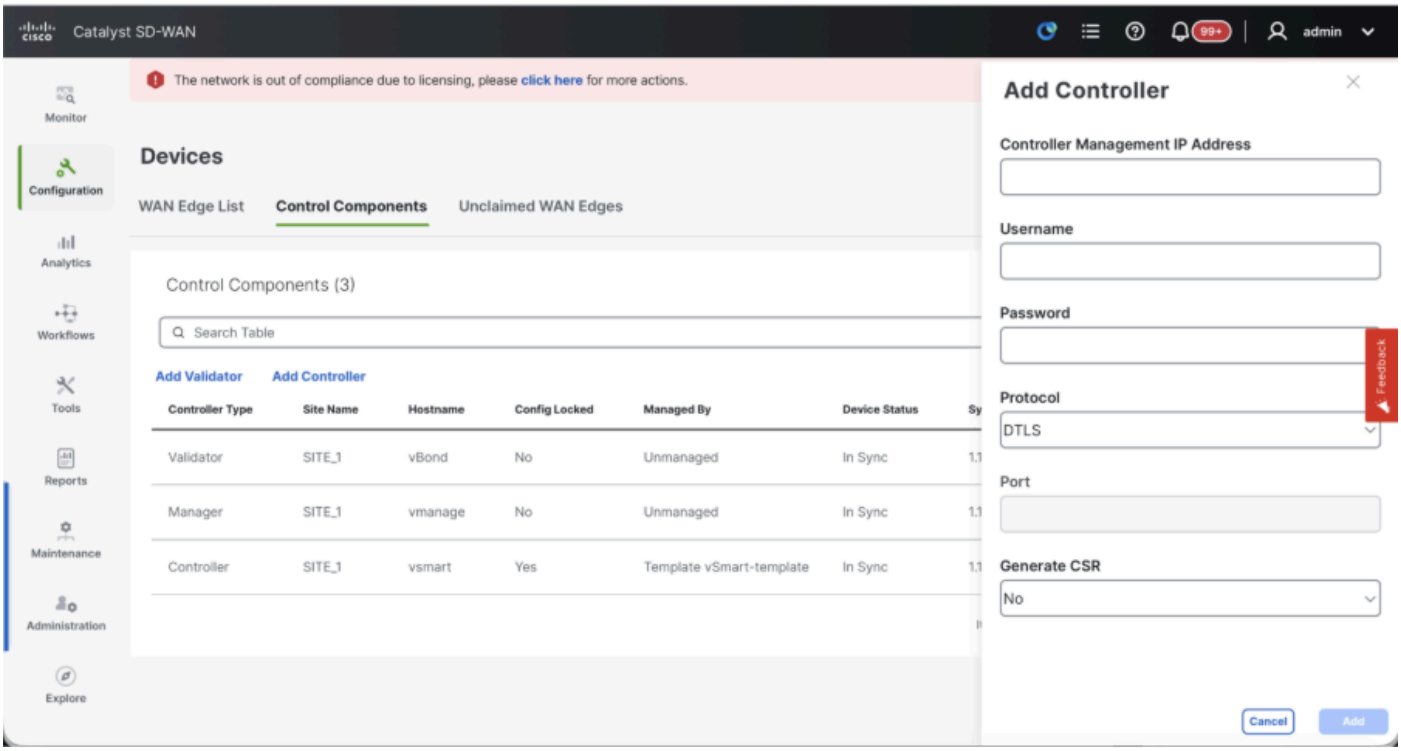
vSmart/Controller 온보딩:

- 20.12 vManage의 경우 vSmart 추가 또는 20.15/20.18 vManage의 경우 컨트롤러 추가를 클

릭합니다.

- 팝업이 열리면 vManage에서 연결할 수 있는 vSmart의 VPN 0 전송 IP를 입력합니다.
- vManage의 CLI에서 vSmart IP로 허용되는 경우 ping을 사용하여 연결 가능성을 확인합니다.
- vSmart의 사용자 자격 증명을 입력하십시오. vSmart의 관리자 자격 증명 또는 netadmin 그룹의 사용자 부분을 사용해야 합니다.
- vSmart의 CLI에서 이를 확인할 수 있습니다.
- 라우터에 TLS를 사용하여 vSmart와의 제어 연결을 설정하려면 프로토콜을 TLS로 설정합니다. vSmarts 및 vManage 노드의 CLI에서도 이 구성을 구성해야 합니다.
- vSmart용 새 인증서를 설치해야 하는 경우 "Generate CSR(CSR 생성)" 드롭다운에서 Yes(예)를 선택합니다.

참고: vSmart가 NAT 장치/방화벽 뒤에 있는 경우 vSmart VPN 0 인터페이스 IP가 공용 IP로 변환되었는지 확인하고, vManage에서 VPN 0 인터페이스 IP에 연결할 수 없는 경우 이 단계에서 VPN 0 인터페이스 IP의 공용 IP 주소를 사용합니다.

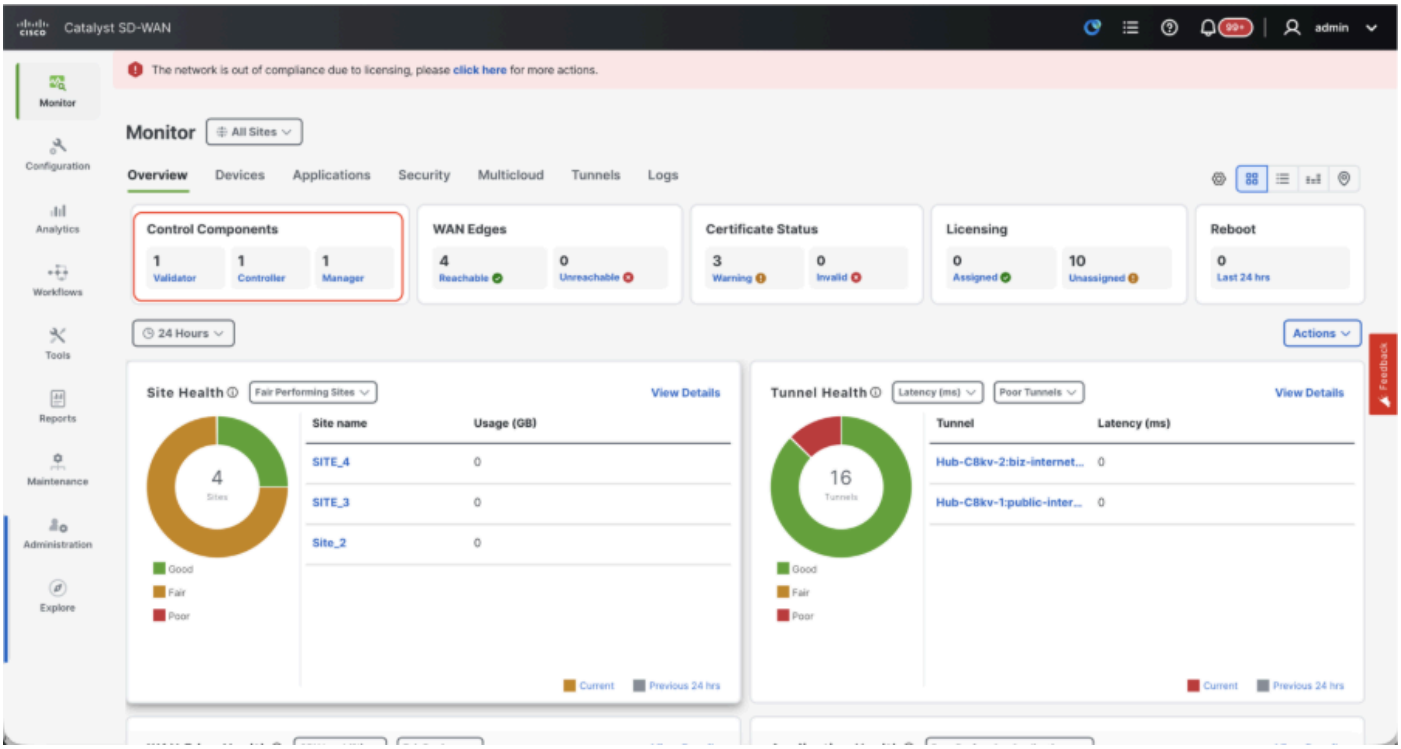


- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vSmart에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다.

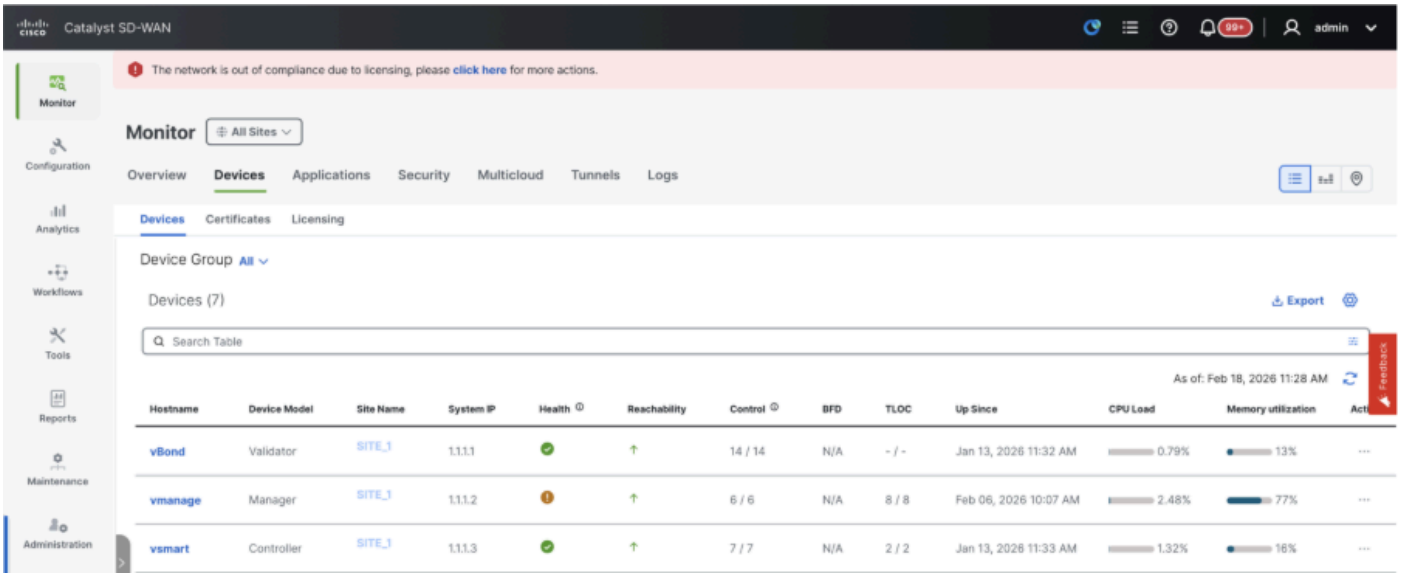
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.
- vSmarts가 여러 개인 경우 동일한 단계를 반복합니다.

확인

모든 단계가 완료되면 Monitor>Dashboard에서 모든 제어 구성 요소에 연결할 수 있는지 확인합니다



- 각 Control(제어) 구성 요소를 클릭하고 모두 연결할 수 있는지 확인합니다.
- Monitor(모니터링) > Devices(디바이스)로 이동하여 모든 제어 구성 요소에 연결할 수 있는지 확인합니다.



3단계: vManage 클러스터 구축

SD-WAN 오버레이에 vManage 클러스터를 포함하는 온보드 SD-WAN 패브릭

참고: SD-WAN 패브릭에 온보딩된 사이트의 수에 따라 vManage 클러스터를 3개의 vManage 노드 또는 6개의 vManage 노드로 구성할 수 있습니다

단일 vManage 노드를 사용하여 모든 SD-WAN 컨트롤러 온보딩

"SD-WAN 오버레이에 단일 노드 vManage를 사용하여 SD-WAN 컨트롤러 온보드"에서 공유하는 단계를 진행하여 먼저 하나의 vManage 노드를 사용하여 SD-WAN 패브릭을 시작하고 필요한 모든 Validator(vBond) 및 컨트롤러(vSmart)를 온보딩합니다.

클러스터의 일부인 모든 vManage 노드의 CLI 컨피그레이션을 구성합니다

- vManage 노드의 나머지를 구성합니다. 3노드 클러스터의 경우 나머지 2개 노드를 구성해야 하고 6노드 클러스터의 경우 5개 노드를 구성해야 합니다.
- 다음과 같이 시스템 컨피그레이션을 구성합니다.

```
config t
system
 host-name



 system-ip



 site-id



 organization-name



 vbond



commit
```

참고: URL을 vBond 주소로 사용하는 경우 VPN 0 컨피그레이션에서 DNS 서버 IP 주소를 구성하거나 확인할 수 있는지 확인하십시오.

이러한 컨피그레이션은 라우터 및 나머지 컨트롤러와의 제어 연결을 설정하는 데 사용되는 전송 인터페이스를 활성화하는 데 필요합니다.

```
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
```

컨트롤러에 대한 대역 외 관리 액세스를 활성화하도록 VPN 512 관리 인터페이스도 구성합니다.

```
Conf t
vpn 512
 interface eth0
  ip address




  no shutdown
 !
 ip route 0.0.0.0/0




!
Commit
```

선택적 구성:

- 기존 컨트롤러의 컨피그레이션을 참조할 수 있으며 여기에 나열된 컨피그레이션이 있는 경우 이 컨피그레이션을 새 컨트롤러에 추가할 수 있습니다.
- 라우터가 TLS를 사용하여 vManage 노드와 보안 제어 연결을 설정해야 하는 경우에만 제어 프로토콜을 TLS로 구성합니다. 기본적으로 모든 컨트롤러와 라우터는 DTLS를 사용하여 제어 연결을 설정합니다. 이는 사용자의 요구 사항에 따라 vSmart 및 vManage 노드에서만 필요한 선택적 컨피그레이션입니다.

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

모든 vManage 노드에서 서비스 인터페이스 구성

이미 온보딩된 vManage-1을 포함하여 모든 vManagenodes에서 서비스 인터페이스를 구성합니다. 이 인터페이스는 클러스터 통신에 사용됩니다. 즉, 클러스터에서 vManagenodes 간의 통신을 의미합니다.

```
conf t
 interface eth2
  ip address




  no shutdown
commit
```

vManagecluster의 모든 노드에서 서비스 인터페이스에 동일한 IP 서브넷이 사용되는지 확인합니다.

클러스터 자격 증명 구성

vManagenodes의 동일한 관리자 자격 증명을 사용하여 vManagecluster를 구성할 수 있습니다. 그렇지 않으면 netadmingroup의 일부인 새 사용자 자격 증명을 구성할 수 있습니다. 새 사용자 자격 증명을 구성하기 위한 컨피그레이션은 다음과 같습니다

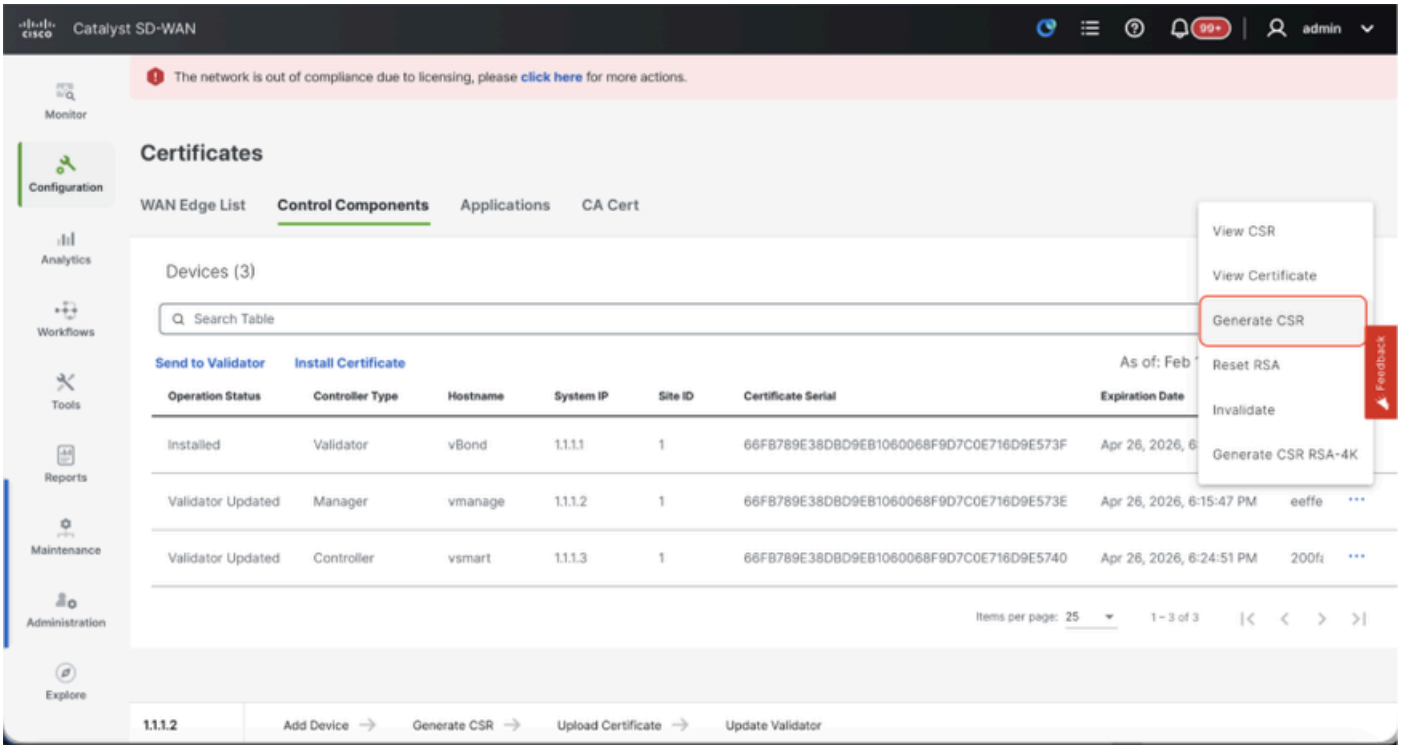
```
conf t
system
 aaa
  user




   password




   group    netadmin
commit
```

클러스터에 속하는 모든 vManagenodesisc에서 동일한 사용자 자격 증명을 구성해야 합니다.관리자 자격 증명을 사용하려면 모든 vManagenodes에서 동일한 사용자 이름/비밀번호여야 합니다.

모든 vManage 노드에 디바이스 인증서 설치

- 브라우저의 URL https://<vmanage-ip>를 사용하여 모든 vManagenodes의 vManageUI에 로그인합니다. 각 vManagenodes의 VPN 512 IP 주소를 사용합니다. 관리자 사용자 이름 및 비밀번호로 로그인할 수 있습니다.
- Configuration(컨피그레이션) > Certificates(인증서) > Control Components(제어 구성 요소)(20.15/20.18 vManage 노드의 경우)로 이동합니다. 20.9/20.12 버전의 경우 Configuration(컨피그레이션) > Devices(디바이스) > Controllers(컨트롤러)

  Manager/vManage(관리자/vManage)에서 ...을 클릭하고 Generate CSR(CSR 생성)을 클릭합니다.



- CSR이 생성되면 CSR을 다운로드하고 컨트롤러에 대해 선택한 인증 기관에 따라 CSR에 서명을 받을 수 있습니다. Administration > Settings > Controller Certificate Authorization에서 이 컨피그레이션을 확인할 수 있습니다. Cisco(권장)를 선택한 경우 vManage에서 CSR을 PNP 포털에 자동으로 업로드하고 인증서가 서명되면 vManage에 자동으로 설치됩니다.
- Manual(수동)을 선택한 경우 해당 SD-WAN 오버레이의 Smart Account 및 Virtual Account로 이동하여 Cisco PNP 포털을 사용하여 CSR에 수동으로 서명합니다.
- PNP 포털에서 인증서를 사용할 수 있게 되면 vManage의 동일한 섹션에서 install certificate(인증서 설치)를 클릭하고 인증서를 업로드한 다음 인증서를 설치합니다.
- Digicert 및 Enterprise Root Certificate를 사용하는 경우에도 동일한 절차를 적용할 수 있습니다.

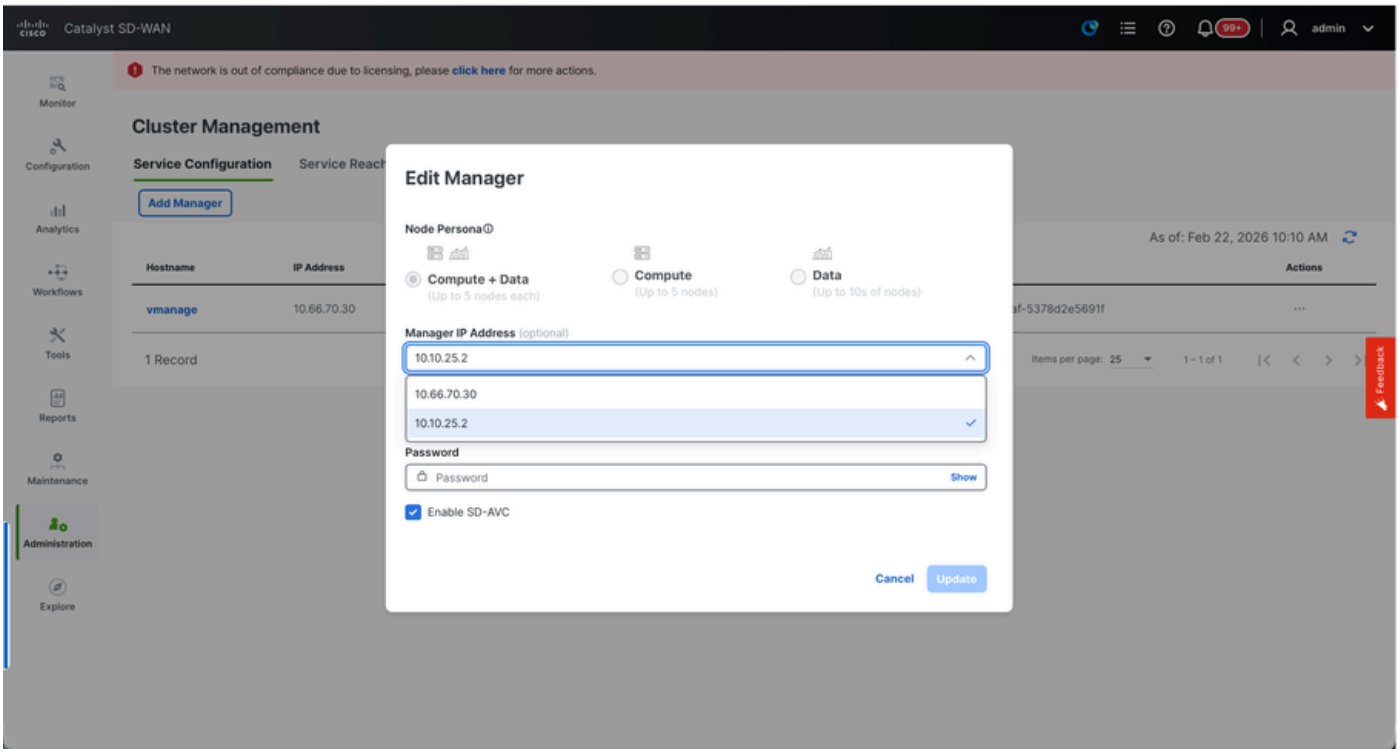
- 클러스터의 일부인 모든 vManage 노드에서 이 단계를 완료합니다.

vManage 클러스터 구축 준비

- vManage-1의 webUI에서 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고 vManage-1에 대한 Actions(작업) 아래에서 ...를 클릭한 후 Edit(수정)를 선택합니다.
- 노드 페르소나는 VM이 스핀업되는 동안 선택한 페르소나에 따라 자동으로 선택됩니다.

참고: 3노드 클러스터의 경우 3개의 vManage 노드 모두 컴퓨팅+데이터가 페르소나로 표시됩니다. 6노드 클러스터의 경우 3개의 vManage 노드가 compute+data를 페르소나로, 3개의 vManage 노드가 data를 페르소나로 가져옵니다.

- 관리자 IP 주소의 드롭다운에서 vManage의 서비스 인터페이스 IP를 선택해야 합니다.



- vManage 클러스터를 활성화하는 데 사용할 사용자 이름 및 비밀번호를 입력합니다. 이를 클러스터 자격 증명이라고 합니다.
- 앞에서 언급한 것처럼 모든 vManage 노드에서 동일한 자격 증명을 구성해야 하며 모든 노드를 클러스터에 추가하는 동안 사용해야 합니다.

선택적 구성:

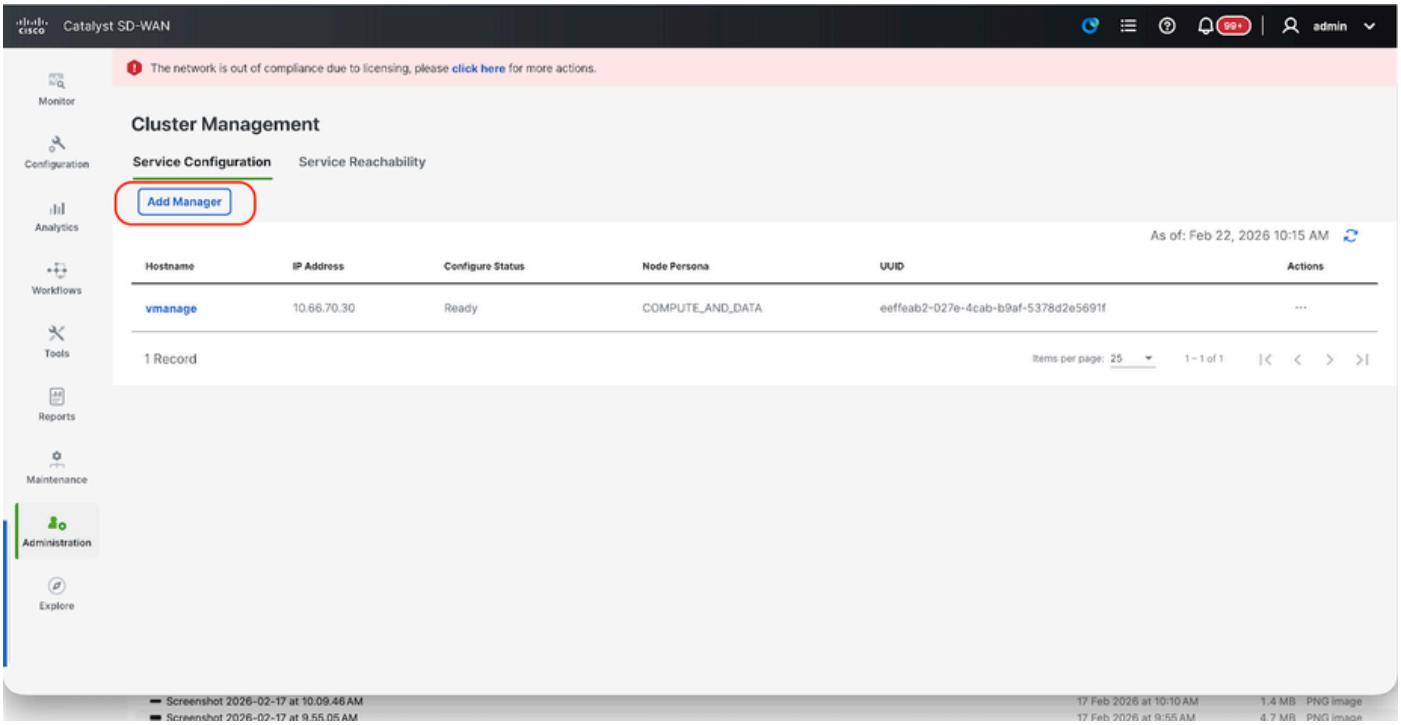
SDAVC를 활성화하려면 기존 클러스터의 이 컨피그레이션을 참조하시기 바랍니다. SDAVC가 필요하고 클러스터의 한 vManage 노드에서만 필요한 경우에만 이 컨피그레이션을 확인해야 합니다.

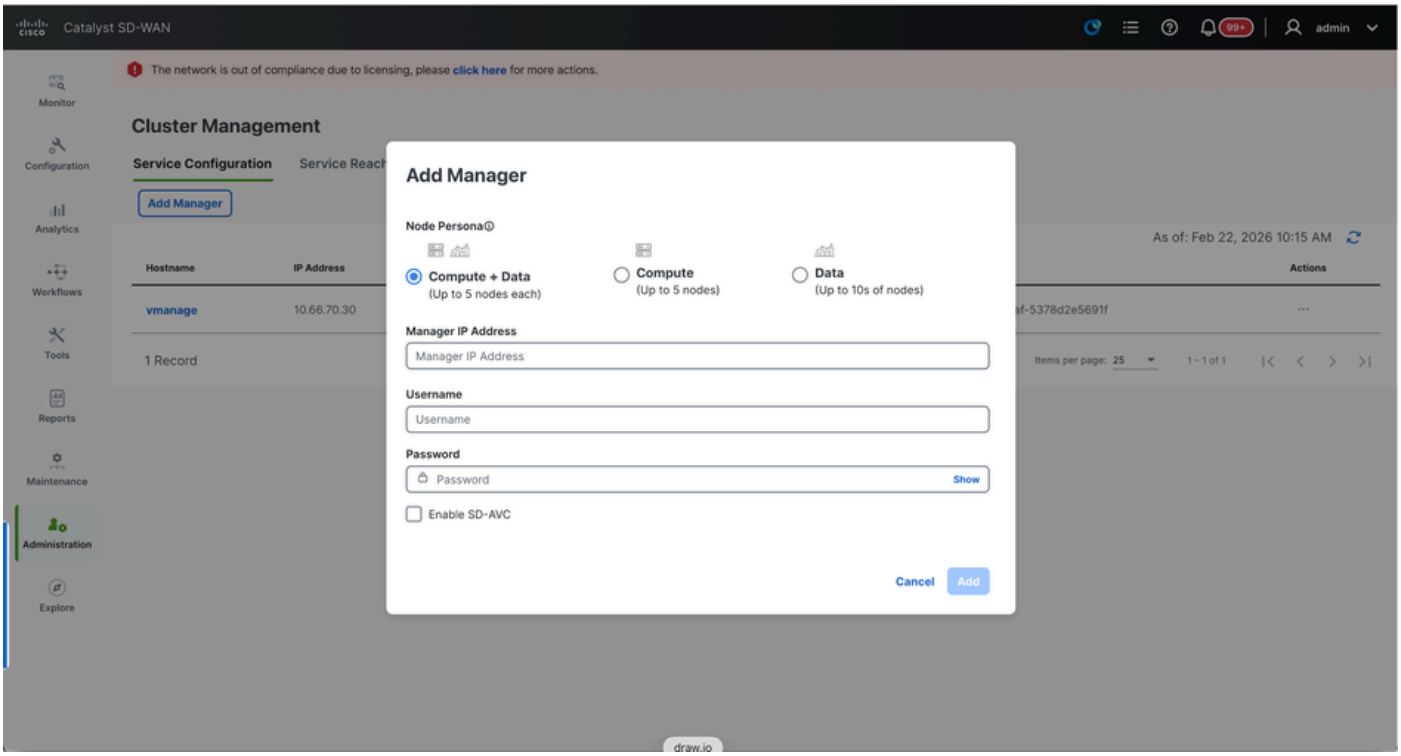
Update(업데이트)를 클릭합니다.

- 이 게시물을 올리면 백그라운드에서 vManage NMS 서비스가 다시 시작되고 5~10분 정도의 몇 분 동안 UI를 사용할 수 없습니다. 이 기간 동안 vManage의 CLI 액세스를 사용할 수 있습니다.
- vManage-1 UI에 액세스할 수 있게 되면 Administration(관리) > Cluster Management(클러스터 관리)로 이동하며, vManage의 서비스 인터페이스 IP가 IP 주소 아래에 반영되는지 확인합니다.Configure Status(상태 구성)가 Ready(준비)이고 노드 페르소나가 올바르게 반영됩니다. 같은 페이지에서 서비스 연결 가능 섹션으로 전환하고 모든 서비스에 연결할 수 있는지 확인합니다.
- 아직 연결되지 않은 서비스가 있는 경우 잠시 기다려 주십시오. 보통 20분에서 30분 정도 걸립니다.

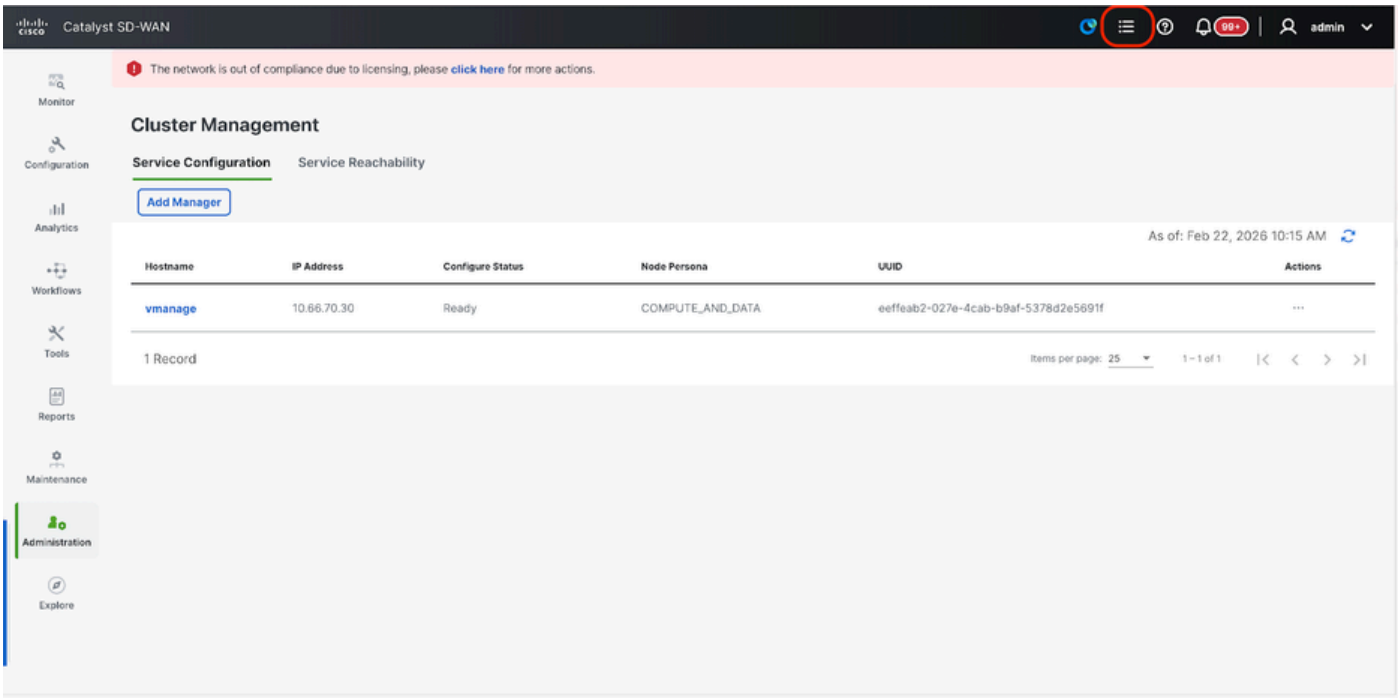
vManage 클러스터 구축

- vManage-1의 webUI에서 Service Configuration(서비스 컨피그레이션) 섹션의 Administration(관리) > Cluster Management(클러스터 관리)로 이동합니다.
- Add Manager(관리자 추가)를 클릭하면 팝업 창이 나타납니다.





- vManage - 2 노드를 스핀업하는 동안 수행한 페르소나 컨피그레이션에 따라 노드 페르소나를 선택합니다.
- 관리자 IP 주소 아래 vManage-2의 서비스 인터페이스 IP를 입력합니다
- 사용자 이름과 비밀번호를 입력합니다. 이는 6단계에서 사용한 것과 동일한 자격 증명입니다 .
- Enable SDAVC(SDAVC 활성화) - vManage-1에서 SDAVC를 이미 활성화했으므로 선택하지 않은 상태로 둡니다.
- Add(추가)를 클릭합니다.
- 이를 게시하면 vManage NMS 서비스가 백그라운드에서 vManage 1 및 2 노드에 대해 다시 시작됩니다. vManage 1 및 2의 경우 약 5~10분 동안 UI를 사용할 수 없습니다.
- 이 기간 동안 vManage 1 및 2의 CLI 액세스를 사용할 수 있습니다.
- vManage-1 UI에 액세스할 수 있게 되면 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고, vManage의 서비스 인터페이스 IP가 모두 IP 주소에 반영되었는지 확인하고, Configure Status(구성 상태)가 Ready(준비)이고 노드 페르소나가 올바르게 반영되었는지 확인합니다.
- 동일한 페이지의 서비스 연결 가능 섹션으로 전환하고 vManage 노드 모두에 대해 모든 서비스에 연결할 수 있는지 확인합니다.
- 아직 연결되지 않은 서비스가 있는 경우 잠시 기다려 주십시오. 보통 5분에서 10분 정도 걸립니다.
- vManage UI의 오른쪽 상단 모서리에 있는 Task-list(작업 목록)에서 클러스터 추가 프로세스의 상태를 확인할 수 있습니다.



- Active(활성) 작업 목록을 조회할 수 있으며, 작업이 Active(활성) 작업 목록 아래에 여전히 나열되어 있으면 작업이 아직 완료되지 않았음을 나타냅니다.
- 작업을 클릭하여 진행 상태를 확인할 수 있습니다. 작업이 활성 작업 목록에 나열되지 않으면 완료로 전환하고 작업이 성공적으로 완료되었는지 확인하십시오.
- 이러한 점이 검증된 후에만 다음 단계로 진행합니다.

클러스터에 다음 노드를 추가하기 전에 이러한 점을 고려해야 합니다.

지금까지 클러스터에 추가된 vManage 노드의 모든 UI에서 다음 사항을 확인하십시오.

- Monitor(모니터) > Overview of vManage UI(vManage UI 개요)로 이동하여 vManage 노드 수가 올바르게 반영되고 클러스터에 추가된 노드 수에 따라 연결 가능한 것으로 표시되는지 확인합니다.

- Administration(관리) > Cluster Management(클러스터 관리)로 이동하여 IP 주소 아래에 vManage의 서비스 인터페이스 IP가 모두 반영되고, Configure Status(구성 상태)가 Ready(준비)이고 노드 페르소나가 올바르게 반영되었는지 확인합니다.
- 같은 페이지의 서비스 연결 가능 섹션으로 전환하고 모든 서비스가 두 vManage 노드 모두에 연결할 수 있는지 확인합니다.

- 노드가 클러스터에 추가될 때마다 클러스터에 있는 모든 노드의 NMS 서비스가 다시 시작되므로 해당 노드의 UI에 한동안 연결할 수 없게 됩니다.
- 클러스터의 노드 수에 따라 UI를 백업하고 모든 서비스에 연결하는 데 더 오랜 시간이 걸릴 수 있습니다.
- vManage UI의 오른쪽 상단 모서리에 있는 Task-list(작업 목록)에서 작업을 모니터링할 수 있습니다.
- 클러스터에 추가된 각 노드의 vManage UI에서 vManage-1에서 사용 가능한 모든 라우터, 템플릿 및 정책을 확인해야 합니다.
- 이러한 컨피그레이션이 vManage-1에 없는 경우 vManage-1에 추가된 vBonds 및 vSmarts와 Administration(관리) > Settings(설정) 컨피그레이션에서 Organization-name(조직 이름),

vBond, Certificate Authorization(인증서 권한 부여)이 클러스터에 추가된 나머지 vManage 노드에 반영되어야 합니다.
- 나머지 vManage 노드에 대해서도 동일한 단계를 반복합니다.

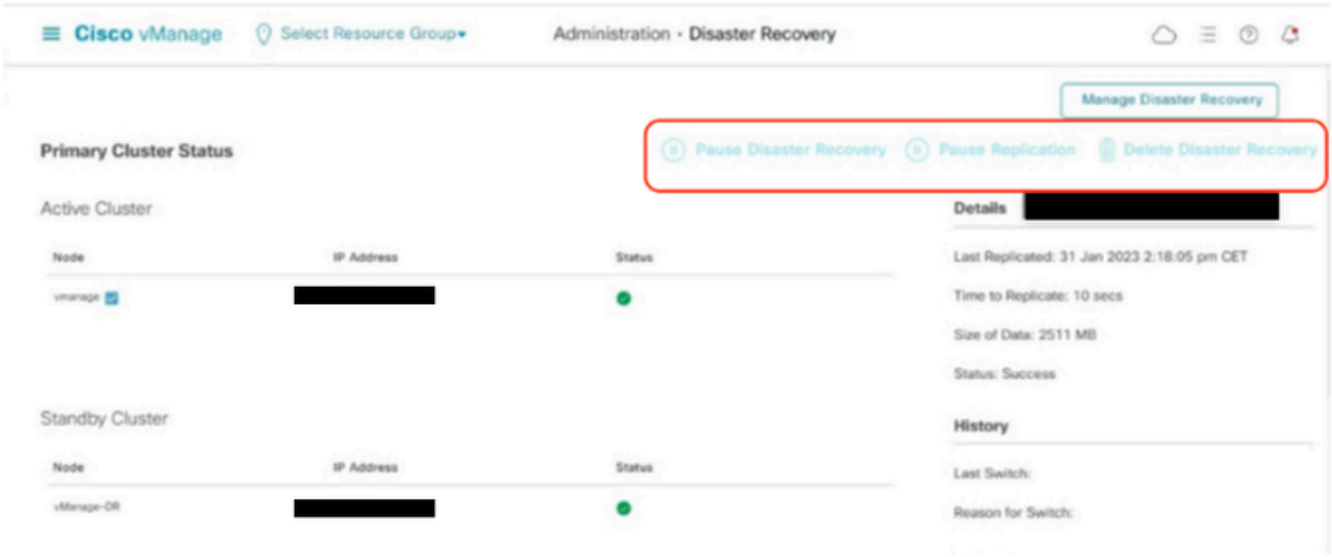
4단계: Config-db 백업/복원

다른 vManage 노드에서 vManage configuration-db 백업 및 복원 수집

참고: 재해 복구가 활성화된 기존 vManage 클러스터에서 컨피그레이션 데이터베이스 백업을 수집하는 동안 해당 노드의 재해 복구가 일시 중지되고 삭제된 후에 수집되어야 합니다.

진행 중인 재해 복구 복제가 없는지 확인합니다. Administration(관리) > Disaster Recovery(재해 복구) 및 상태가 Success(성공)이고 Import Pending(가져오기 보류 중), Export Pending(내보내기 보류 중) 또는 Download Pending(다운로드 보류 중)과 같은 일시적인 상태가 아닌지 확인합니다. 상태가 성공적이지 않으면 Cisco TAC에 문의하여 복제가 성공적인지 확인한 후 재해 복구를 일시 중지합니다.

먼저 재해 복구를 일시 중지하고 작업이 완료되었는지 확인합니다. 그런 다음 재해 복구를 삭제하고 작업이 완료되었는지 확인합니다.



Cisco TAC에 문의하여 재해 복구가 성공적으로 정리되었는지 확인합니다.

Configuration-DB 백업 수집:

- 현재 사용 중인 SD-WAN 패브릭에서는 vManage 클러스터에서 configuration-db 백업을 생성할 수 있습니다.
- configuration-db 백업은 configuration-db 리더인 vManage 클러스터의 한 노드에서만 생성해야 합니다.

- 독립형 vManage의 경우 해당 vManage 자체가 configuration-db 리더입니다.

- vManage 클러스터에서 request nms configuration-db diagnostics 명령을 사용하여 configuration-db 리더 노드를 식별합니다.3노드 vManage 클러스터의 모든 노드에서 이 명령을 실행할 수 있습니다.
- 6노드 클러스터에서 컨피그레이션 DB가 활성화되어 리더 노드를 식별하는 vManage 노드에서 이 명령을 실행해야 합니다. Administration(관리) > Cluster Management(클러스터 관리)로 이동하여 다음을 확인합니다.
- 스크린샷에서 볼 수 있듯이, COMPUTE_AND_DATA 페르소나로 구성된 노드는 컨피그레이션 DB가 실행 중입니다.

vManageCLI에서 requestnmsconfiguration-dbstatus 명령을 사용하여 동일한 사항을 확인할 수 있습니다. 출력은 다음과 같습니다

```
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#
```

- 명령을 실행하면이러한 노드에서 nms configuration-db 진단을 요청하면 다음과 같이 출력됩니다.
- "IsLeader"에 대해 강조 표시된 필드를 찾습니다. 1로 설정된 경우 노드가 리더 노드임을 나타내며, 여기서 configuration-db 백업을 수집할 수 있습니다.

```
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     .
```

식별된 configuration-db leader vManage 노드에서 configuration-db 백업을 수집하려면 이 명령을 사용합니다.

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

예상 출력은 다음과 같습니다.

```
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#
```

- 컨피그레이션 DB 자격 증명이 업데이트된 경우 기록해 둡니다.
- configuration-db 자격 증명을 모르는 경우 TAC에 문의하여 기존 vManage 노드에서 configuration-db 자격 증명을 검색합니다.

- 기본 configuration-db 자격 증명은 사용자 이름입니다. neo4j 및 비밀번호: 암호

다른 vManage 노드에 Configuration-db 백업 복원

SCP를 사용하여 configuration-db 백업을 vManage의 /home/admin/ 디렉토리에 복사합니다.

샘플 scp 명령 출력:

```
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 백업을 복원하려면 먼저 configuration-db 자격 증명을 구성해야 합니다. configuration-db 자격 증명이 default(neo4j/password)인 경우 이 단계를 건너뛸 수 있습니다.

configuration-db 자격 증명을 구성하려면 nms configuration-db update-admin-user 명령을 사용합니다.선택한 사용자 이름과 비밀번호를 사용합니다.

vManage의 애플리케이션 서버가 다시 시작됩니다. 따라서 vManage UI에 짧은 시간 동안 액세스할 수 없게 됩니다.

```
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#
```

구성 DB 백업을 복원하기 위해 진행할 수 있는 게시:

nms configuration-db 복원 경로 /home/admin/< > 명령을 사용하여 configuration-db를 새 vManage로 복원할 수 있습니다.

```
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-db가 복원되면 vManage UI에 액세스할 수 있는지 확인합니다. 약 5분 정도 기다린 후 UI에 액세스를 시도합니다.

UI에 성공적으로 로그인했으면 Edge 라우터 목록, 템플릿, 정책 및 이전 또는 기존 vManage UI에 존재했던 나머지 모든 컨피그레이션이 새 vManage UI에 반영되었는지 확인합니다.

5단계: vManage 클러스터에서 재해 복구 사용

중요 사전 점검

재해 복구를 진행하려면 두 개의 별도의 vManage 3노드 클러스터를 구성하고 작동해야 합니다. 활성 클러스터에는 검증자 및 컨트롤러가 온보딩되어야 합니다. DR 사이트에 검증기와 컨트롤러가 있는 경우, DR vManage 클러스터가 아니라 활성 클러스터에서도 온보딩해야 합니다.

Cisco에서는 재해 복구를 등록하기 전에 다음 요구 사항을 충족해야 한다고 권장합니다.

- 전송 VPN(VPN 0)에서 HTTPS를 통해 기본 및 보조 노드에 연결할 수 있는지 확인합니다.
- 보조 설정의 Cisco vSmart Controller 및 Cisco vBond Orchestrator가 기본 설정에 연결되어 있는지 확인합니다.
- Cisco vManage 기본 노드 및 보조 노드에서 동일한 Cisco vManage 버전을 실행하고 있는지 확인합니다.

- VPN 0의 OOB(Out of Band) 클러스터 인터페이스(서비스 인터페이스)
- 클러스터 내의 각 vManage 인스턴스에는 VPN 0(전송) 및 VPN 512(관리)에 사용되는 인터페이스 외에 세 번째 인터페이스(클러스터 링크)가 필요합니다.
- 이 인터페이스는 클러스터 내에서 vManage 서버 간의 통신 및 동기화에 사용됩니다.
- 이 인터페이스는 1Gbps 이상이어야 하며 지연 시간은 4ms 이하여야 합니다. 10Gbps 인터페이스를 사용하는 것이 좋습니다.
- 두 vManage 노드는 다음 인터페이스를 통해 서로 연결할 수 있어야 합니다. 레이어 2 세그먼트 또는 레이어 3 라우팅을 통해 제공되어야 합니다.
- 각 vManage에서 이 인터페이스는 GUI에서 클러스터 인터페이스로 구성되어야 합니다(Administration(관리) > Cluster Management(클러스터 관리) - 자체 OOB(Out-of-Band) 클러스터 인터페이스 IP 주소, 사용자 및 비밀번호를 나타냄).
- Cisco vManage 노드가 데이터 센터 전체에서 서로 통신할 수 있도록 하려면 데이터 센터 방화벽에서 TCP 포트 8443 및 830을 활성화합니다.
- 모든 서비스(application-server, configuration-db, messaging server, coordination server 및 statistics-db)가 두 Cisco vManage 노드에서 모두 활성화되었는지 확인합니다.
- Cisco vBond Orchestrator를 비롯한 모든 컨트롤러를 기본 및 보조 데이터 센터 전체에 배포합니다. 이러한 데이터 센터에 분산된 Cisco vManage 노드에서 이러한 컨트롤러에 연결할 수 있는지 확인합니다. 컨트롤러는 기본 Cisco vManage 노드에만 연결됩니다.
- 활성(기본) 및 대기(보조) Cisco vManage 노드에서 다른 작업이 진행 중이 아닌지 확인합니다. 예를 들어, 어떤 서버도 디바이스에 템플릿을 업그레이드하거나 연결하는 중이지 않는지 확인합니다.
- 활성화된 경우 Cisco vManage HTTP/HTTPS 프록시 서버를 비활성화합니다. 외부 서버와의 Cisco vManage 통신에 대해서는 HTTP/HTTPS 프록시 서버를 참조하십시오. 프록시 서버를 비활성화하지 않으면 Cisco vManage는 Cisco vManage 대역외 클러스터 IP 주소에 직접 연결할 수 있는 경우에도 프록시 IP 주소를 통해 재해 복구 통신을 설정하려고 시도합니다. 재해 복구 등록이 완료된 후 Cisco vManage HTTP/HTTPS 프록시 서버를 다시 활성화할 수 있습니다.
- 재해 복구 등록 프로세스를 시작하기 전에 기본 Cisco vManage 노드에서 Tools > Rediscover Network 창으로 이동하여 Cisco vBond Orchestrator를 다시 검색합니다.

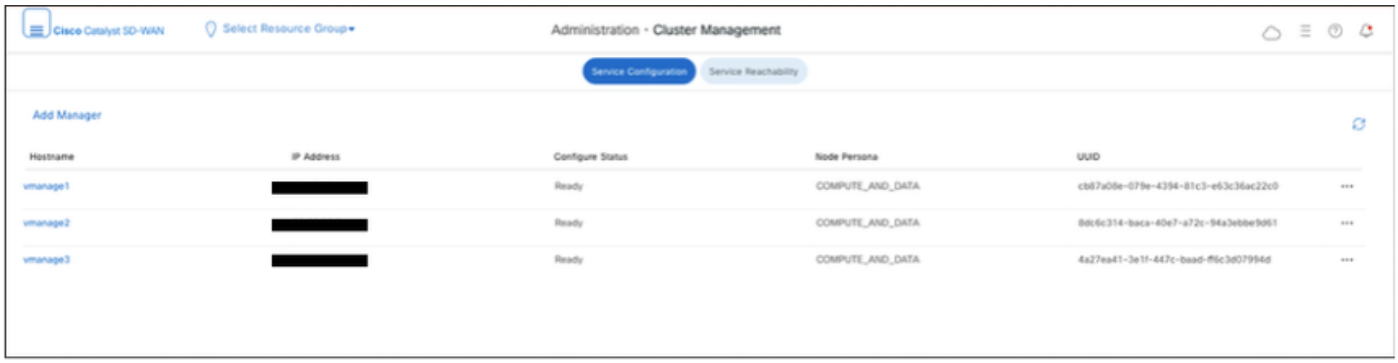
설정

vManage 재해 복구에 대한 자세한 내용은 이 링크를 참조하십시오.

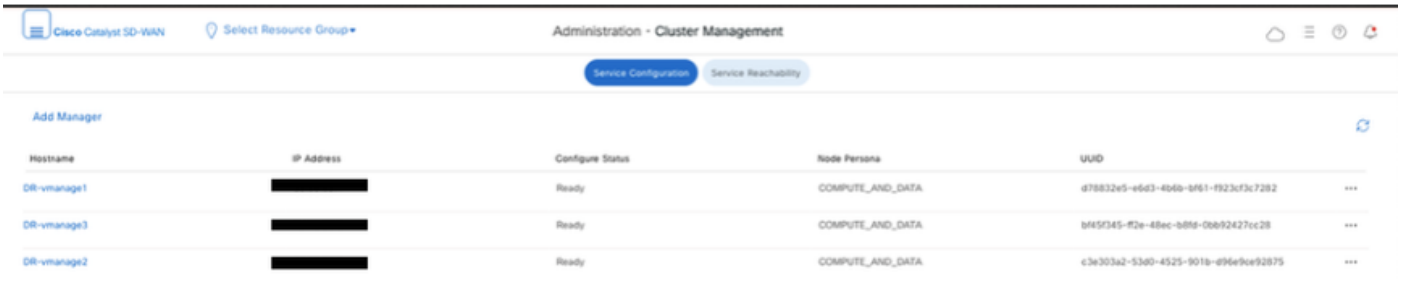
각 SD-WAN 관리자에 최소 컨피그레이션이 있고 인증 부분이 완료되었다고 가정할 때 두 개의 개별 3-노드 클러스터가 이미 생성됩니다.

두 클러스터에서 Administration(관리) > Cluster Management(클러스터 관리)로 이동하고 모든 노드가 준비 상태인지 확인합니다.

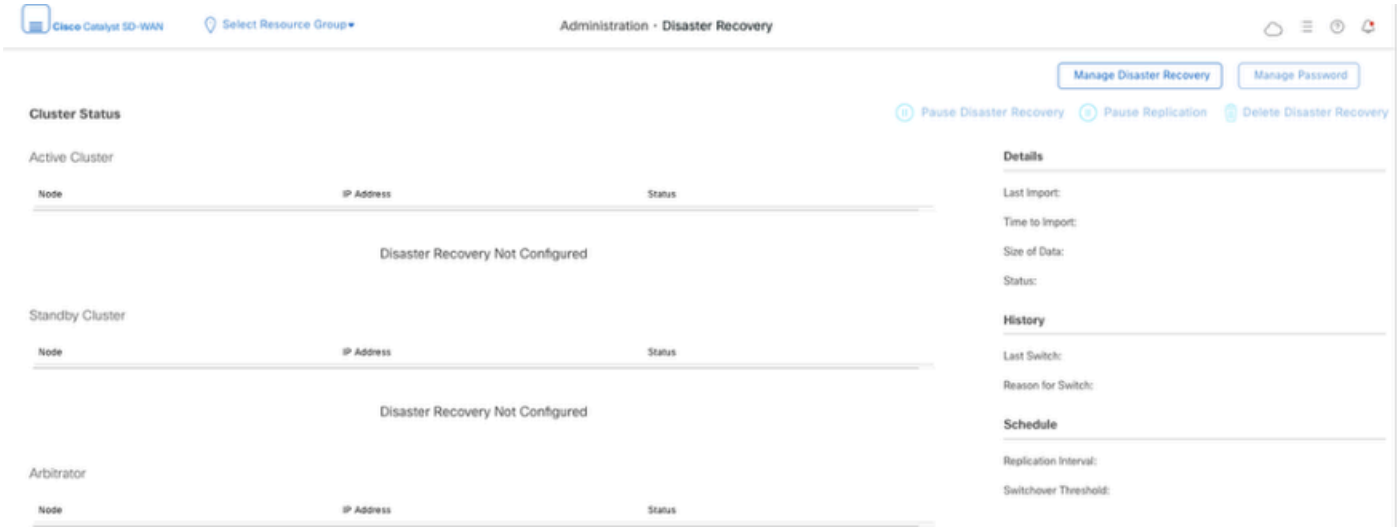
DC vManage



DR vmanage



Administration(관리) >Disaster Recovery of Primary vManage Cluster(기본 vManage 클러스터의 재해 복구)로 이동합니다. Manage Disaster Recovery를 클릭합니다.

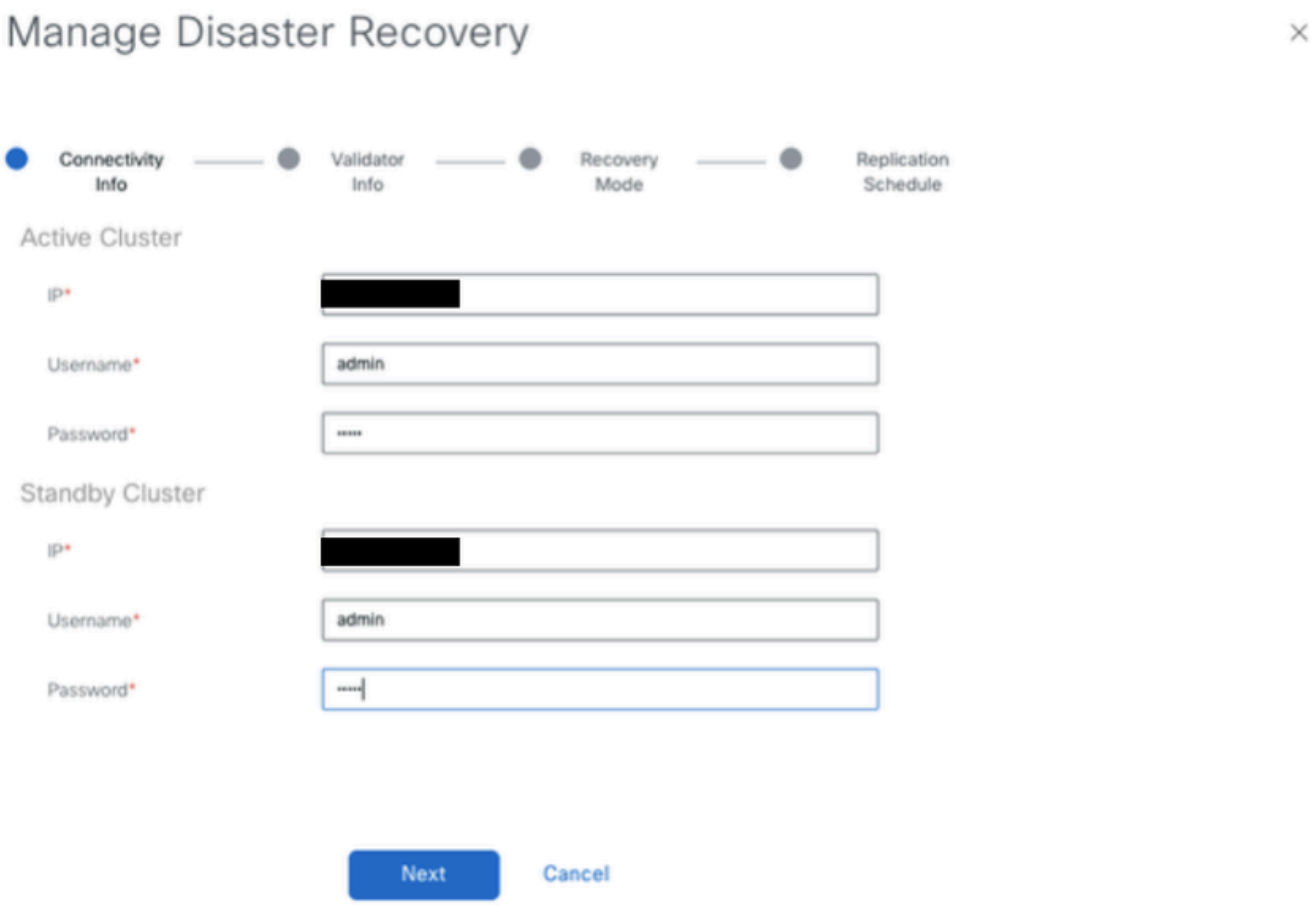


팝업 창에서 기본 및 보조 vManage의 세부사항을 모두 입력합니다.

표시할 IP 주소는 OOB(Out of Band) 클러스터 인터페이스 IP 주소입니다. 각 클러스터에서 vManage-1의 VPN 0 서비스 인터페이스의 IP 주소를 사용하는 것이 좋습니다.

자격 증명은 netadmin 사용자의 자격 증명이어야 하며 DR이 구성된 후에는 삭제되지 않는 한 변경할 수 없습니다. 재해 복구를 위한 별도의 vManage 로컬 사용자 자격 증명을 사용할 수 있습니다. vManage 로컬 사용자가 netadmin 그룹의 일부인지 확인해야 합니다. 관리자 자격 증명도 여기에서

사용할 수 있습니다.



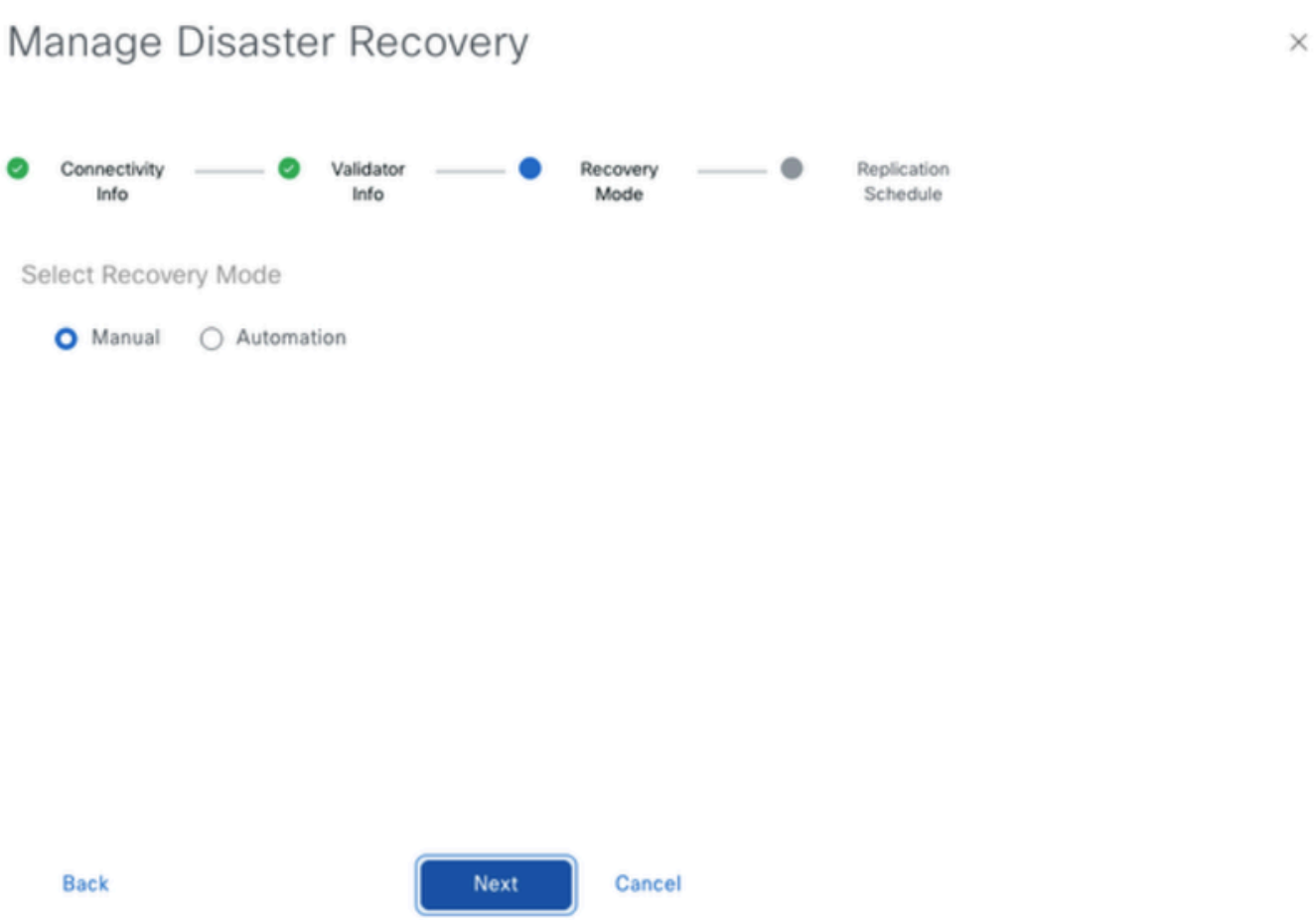
입력을 마쳤으면 다음을 클릭합니다.

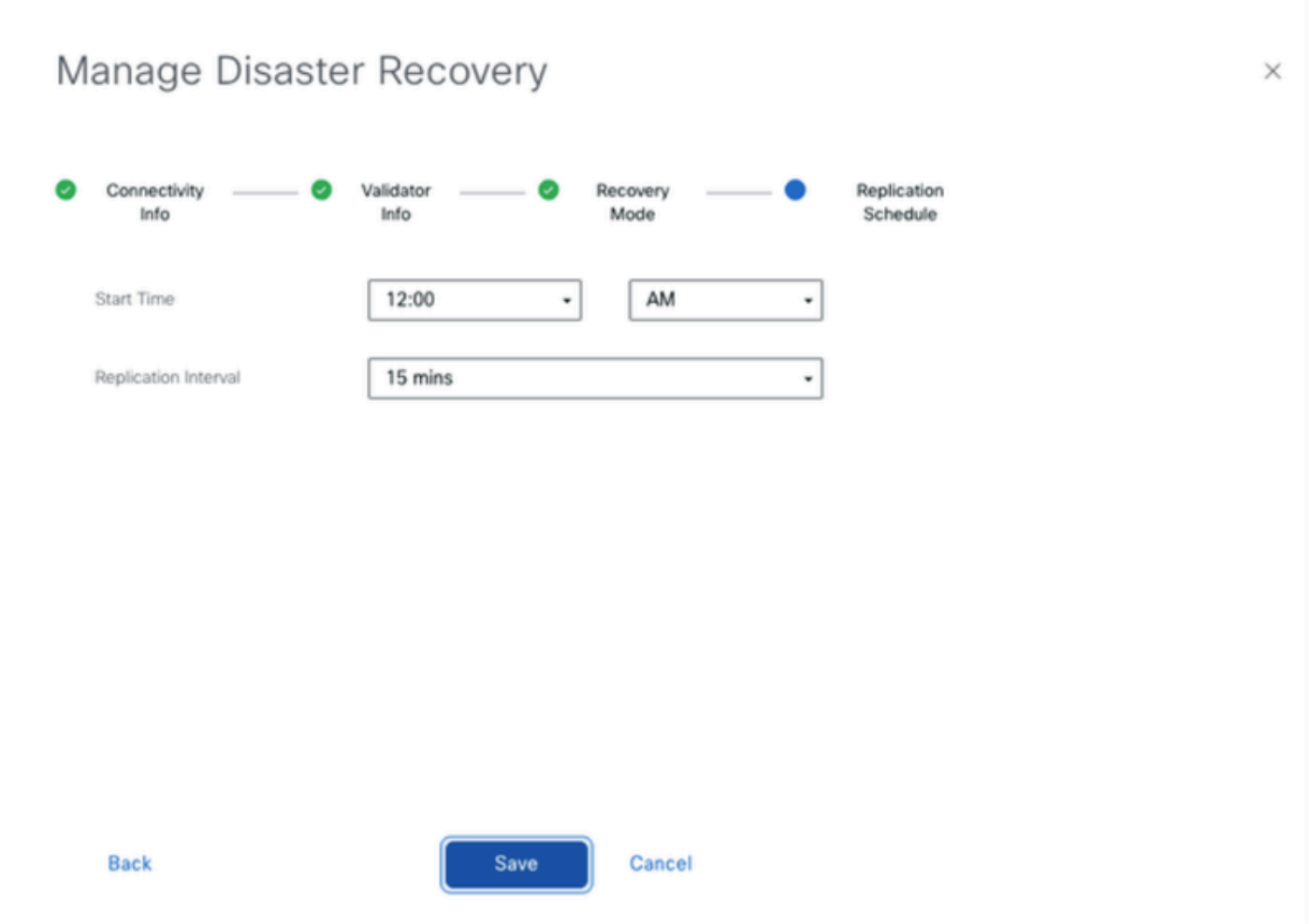
- vBond 컨트롤러의 세부사항을 입력합니다.

vBond 컨트롤러는 지정된 IP 주소에서 Netconf를 통해 연결할 수 있어야 합니다.

입력을 마쳤으면 다음을 클릭합니다.

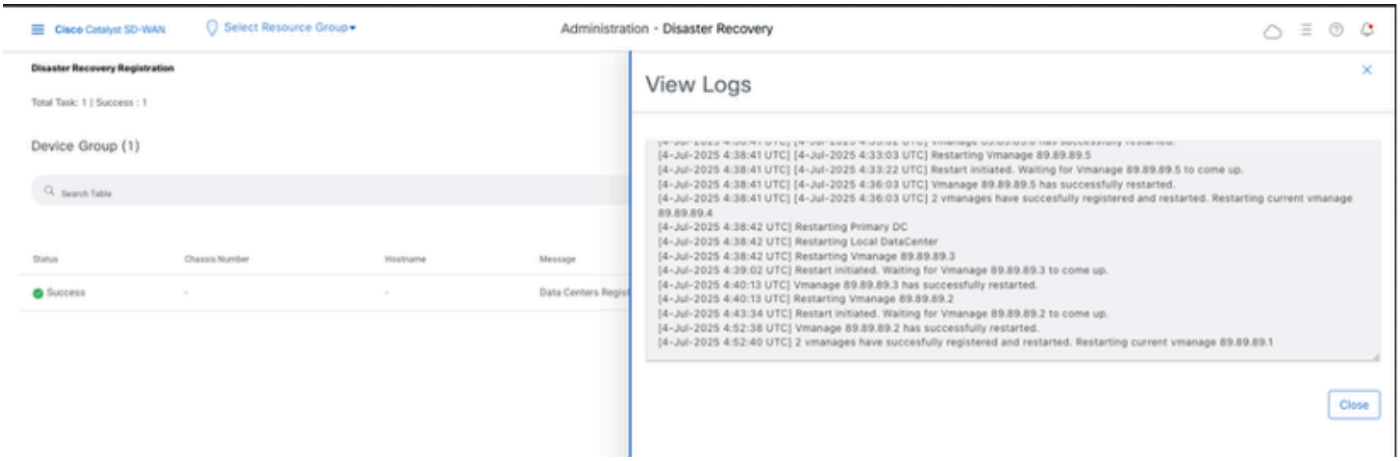
- Recovery Mode(복구 모드)에서 Manual(수동)을 선택합니다. 자동화 모드는 사용되지 않습니다. Next(다음)를 클릭합니다.


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



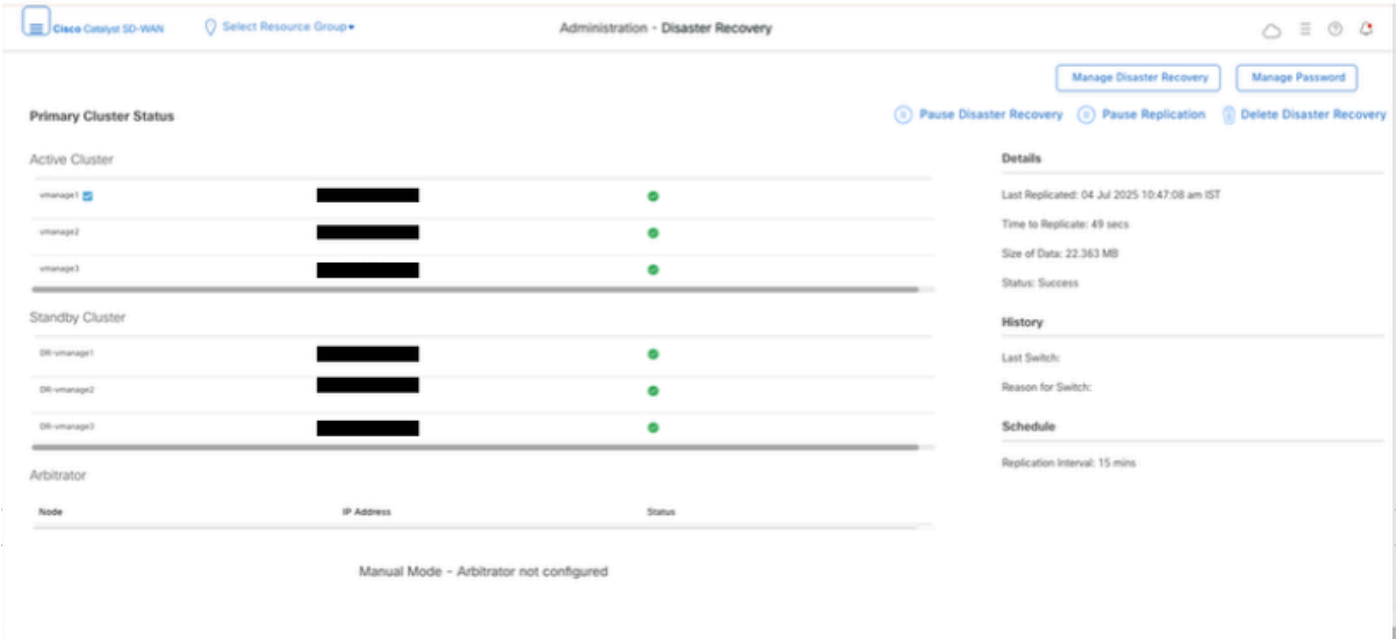
값을 설정하고 저장을 클릭합니다.

- 이제 DR 등록이 시작됩니다. 상태 및 진행 로그를 수동으로 새로 고치려면 새로 고침 버튼을 클릭합니다. 이 프로세스는 최대 20-30분이 소요될 수 있습니다.



확인

Administration(관리)>Disaster Recovery(재해 복구)로 이동하여 재해 복구 상태 및 마지막으로 데이터가 복제된 시기를 확인합니다.



참고: 복제는 데이터베이스 크기에 따라 몇 시간이 걸릴 수 있습니다. 또한 성공적인 복제를 위해서는 몇 번의 사이클이 필요할 수 있습니다.

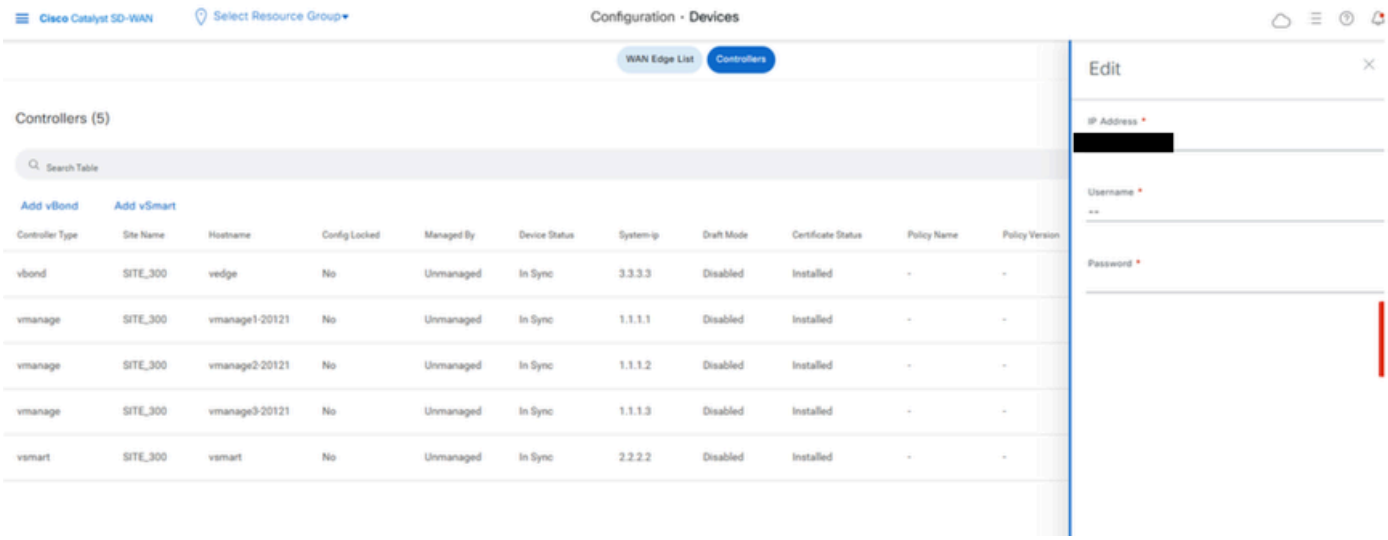
6단계: 컨트롤러 재인증 및 이전 컨트롤러 무효화

configuration-db가 복원되면 패브릭에서 모든 새 컨트롤러(vmanage/vsmart/vbond)를 재인증해야 합니다

참고: 실제 프로덕션에서는 재인증에 사용되는 인터페이스 IP가 터널 인터페이스 IP인 경우 vManage, vSmart 및 vBond의 터널 인터페이스 및 경로에 따른 방화벽에서 NETCONF 서비스가 허용되는지 확인해야 합니다. 열 방화벽 포트는 DR 클러스터에서 모든 vBonds 및 vSmarts로의 양방향 규칙인 TCP 포트 830입니다.

vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다

- 각 컨트롤러 근처의 점 3개를 클릭하고 Edit(수정)를 클릭합니다



- ip-address(컨트롤러의 system-ip)를 transport vpn 0(tunnel interface) ip 주소로 바꿉니다. 사용자 이름과 암호를 입력하고 save(저장)를 클릭합니다
- 패브릭에 있는 모든 새 컨트롤러에 대해 동일한 작업을 수행합니다.

루트 인증서 체인 동기화

모든 컨트롤러가 온보딩되면 다음 단계를 완료합니다.

새로 활성화된 클러스터의 Cisco SD-WAN Manager 서버에서 다음 작업을 수행합니다.

루트 인증서를 새로 활성화된 클러스터의 모든 Cisco Catalyst SD-WAN 디바이스와 동기화하려면 다음 명령을 입력합니다.

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

Cisco SD-WAN Manager UUID를 Cisco SD-WAN Validator와 동기화하려면 다음 명령을 입력합니다.

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

패브릭이 복원되고 패브릭의 모든 에지와 컨트롤러에 대해 제어 및 bfd 세션이 작동되면 UI에서 이전 컨트롤러(vmanage/vsmart/vbond)를 무효화해야 합니다

- vmanage UI에서 Configuration > Devices > Certificates를 클릭합니다
- Controllers(컨트롤러) 클릭
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. Invalidate를 클릭합니다.
- Send to Bond를 클릭합니다.
- vmanage UI에서 Configuration > Devices > Controllers를 클릭합니다
- 기존 패브릭에서 컨트롤러(vmanage/vsmart/vbond) 근처의 점 3개를 클릭합니다. 삭제를 클릭합니다.

수표 게시

이러한 사후 검사는 모든 구축 조합에 적용됩니다.

클라우드 에지 라우터 재활성화:

- C8000v가 오버레이의 일부이고 관리되는 서명인 경우, 다시 인증해야 합니다. 즉,

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

        token
```

- 제어 연결 및 BFD 세션이 작동 중인지 확인합니다.
- 애플리케이션 트래픽이 엔드 투 엔드로 이동하고 있는지 확인
- 에지에서 패브릭을 재구축하기 전에 포트 홉을 변경한 경우 반드시 되돌리십시오

- 항목이 예상대로 표시되는지 확인합니다.
    - 템플릿
    - 정책
    - 디바이스 페이지(두 탭 모두)WAN vEdge ListControllers

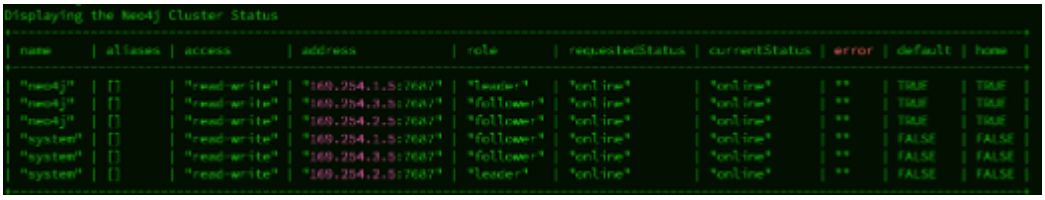
  vManage 사후 검사

- vManage 노드에 적용 가능:

  Configuration-DB(Neo4j) 검사:

  모든 vManage 노드에서 "request nms configuration-db diagnostics" 명령을 실행합니다.

  1. Node online 및 Leadership 상태 확인: (일부 버전에서는 사용할 수 없음)



"Neo4j"는 온라인으로 3개의 노드와 1개의 리더 및 2개의 팔로워를 표시해야 합니다. "system"은 또한 3개의 노드를 온라인으로 표시하고 1개의 지시자와 2개의 팔로워를 표시해야 합

니다. 그러나 기본 Db가 아니므로 기본 플래그는 false입니다. 각 neo4j에 3개 미만의 항목이 있고 시스템은 노드가 클러스터에서 떨어진 것을 의미합니다. 동일한 문제를 해결하려면 Cisco TAC에 문의하십시오.

2. 노드가 "quarantine"인지 확인합니다.

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

노드가 격리 상태에 있어서는 안 됩니다.

3. 스키마 유효성 검사는 "성공"해야 합니다.

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

4. "nms configuration-db 진단 요청" 명령을 사용하여 configuration-db 백업을 수집하고 성공했는지 확인합니다.

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

불일치나 오류가 발견되면 Cisco TAC에 문의하여 문제를 해결하십시오.

또는 이러한 API 호출을 실행하여 클러스터에 대한 vmanage 노드 상태(모든 COMPUTE+DATA 노드에 대해)를 확인할 수 있습니다. 이 작업은 버전 20.12 이상에서만 작동합니다

```
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
```

클러스터에 neo4j와 system 모두에 대해 하나의 지시자만 있고 나머지는 추종자로 유지되는지 확인합니다. 모든 노드가 온라인 상태인지 확인합니다. 노드가 3개인 경우(모두 COMPUTE+DATA) neo4j와 system 모두에 대해 하나의 지시자만 있어야 합니다. 편차가 있으면 TAC에 문의해야 합니다.

5. 디스크, 메모리, IO 오류에 대해서는 /var/log/kern.log을 참조하십시오. 모든 vManage 노드에서 이를 확인해야 합니다.

6. 각 노드 사이에 CC가 없는 vmanage에 대한 새 클러스터를 구성할 때 단계를 확인합니다
노드 1에서 다른 노드 클러스터 ip로 vmanage-admin으로 ssh를 수행하고 그 반대로 공개 키가 교환되고 비밀번호에서 ssh가 덜 작동하는지 확인합니다. [다음 단계에 동의함 토큰이 필요함]

```
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:
```

출력에서 비밀번호를 입력하도록 요청하는 경우 TAC에 문의하십시오.

컨트롤러 게시물 확인:

모든 SD-WAN 컨트롤러에 적용 가능(vBond, vManage, vSmart):

오버레이의 모든 컨트롤러에서 명령을 실행하고 vManage UUID 및 일련 번호가 현재 패브릭에 대해 유효한지 확인합니다.

vBond 명령:

show orchestrator valid-vsmarts

show orchestrator valid-vmanage-id

vManage/vSmart 명령:

show control valid-vsmarts

show control valid-vmanage-id

show control valid-vsmarts의 출력에는 vSmarts 및 vManage 노드의 일련 번호가 모두 포함됩니다.

vManage UI에 표시된 것과 비교합니다. Configuration(컨피그레이션) > Certificates(인증서) > Controllers(컨트롤러) 섹션으로 이동합니다.

현재 패브릭에 온보딩되지 않은 UUID/일련 번호에 대한 추가 항목이 있으면 해당 항목을 삭제해야 합니다. Cisco TAC에 문의할 수도 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.