Recover Standalone vManage by Disaster Recovery

Contents

Introduction

This document describes the steps involved to restore vManage by utilization of a configuration-db backup.

Background Information

This document assumes that a configuration-db backup has been taken periodically and for some reason, the standalone vManage is irrecoverable and needs a software reset or a new install.

This document helps you to recover all the policies, templates, configurations, and Edge device certificates.

Backup Configuration-db

```
vManage_rcdn01# request nms configuration-db backup path 05_08_20_configdb
Starting backup of configuration-db
config-db backup logs are available in /var/log/nm/neo4j-backup.log file
Successfully saved database to /opt/data/backup/05_08_20_configdb.tar.gz
```

scp to an external server.

```
vManage_rcdn01# vshell
vManage_rcdn01:~$ scp /opt/data/backup/05_08_20_configdb.tar.gz user@10.2.3.1://home/ftpuser/ftp/amaugus
amaugust@10.2.3.1's password:
05_08_20_configdb.tar.gz                                          100%  484KB  76.6MB/s   00:
```

Recover vManage

Simulate a disaster by a reset of the vManage by the command:

```
vManage_rcdn01# request software reset
```

Now that you have a fresh vManage that looks like the one shown, it is advisable to adhere to the recovery process in the correct sequence before you restore the backup.
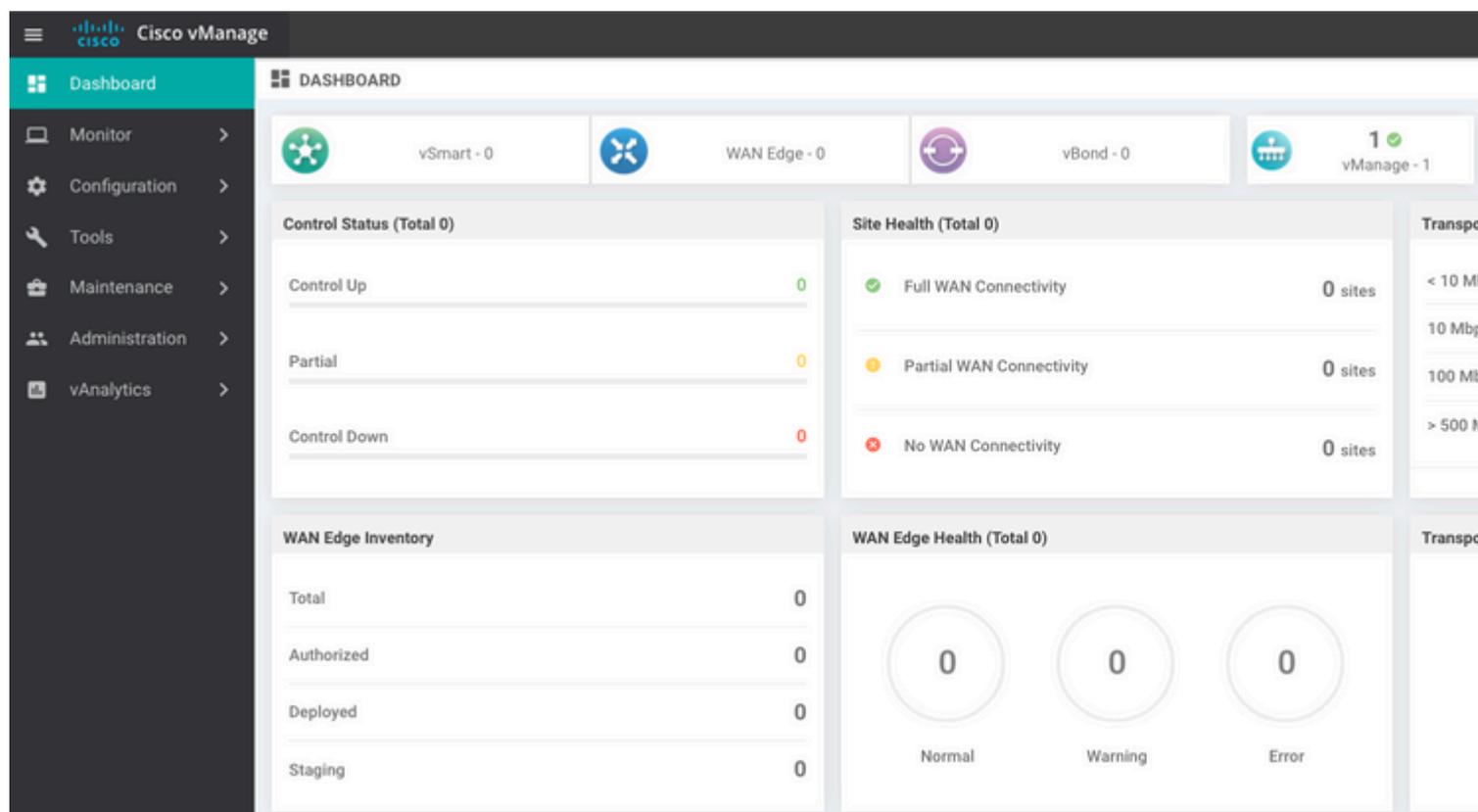
Step 1. Minimum Configuration on vManage

```
system
 host-name            vManage_rcdn01
 system-ip            xx.xx.xx.xx
 site-id              100
 organization-name    ****.cisco
 vbond vbond.list
 !
!
vpn 0
 host vbond.list ip 10.2.3.4 10.2.3.5
 interface eth0
  ip address 10.1.3.8/24
  tunnel-interface
  no shutdown
```

```
 !
 ip route 0.0.0.0/0 10.1.3.1
!
vpn 512
 interface eth1
  ip address 10.11.3.8/24
  no shutdown
 !
 ip route 0.0.0.0/0 10.1.3.1
!
```

Step 2. Copy Backup Configuration and Root Certificate

<#root>

```
vManage_rcdn01:~$ scp am****@xx.xx.xx.xx://home/ftpuser/ftp/am****/05_08_20_configdb.tar.gz  .
am****@xx.xx.xx.xx's password:
05_08_20_configdb.tar.gz                                                  100%  484KB  76.6MB/s   00:0
```

Verify

```
vManage_rcdn01:~$ ls -lh
total 492K
-rw-r--r-- 1 admin admin  394 May  8 15:20 archive_id_rsa.pub
-rwxr-xr-x 1 admin admin 485K May  8 15:3905_08_20_configdb.tar.gz
```

Copy root certificate from other controller:

```
vManage_rcdn01:~$ scp admin@vbond://home/admin/root.crt .
viptela 18.4.4
admin@vbond's password:
root.crt                                                                  100% 1380     2.8MB/s   00:00
```

Step 3. Install Root Certificate

```
vManage_rcdn01# request root-cert-chain install /home/admin/root.crt
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/root.crt via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Step 4. Update Basic Information

Navigate to Administration > Settings and configure the basic information for vBond IP, Organization Name, and certificate.

Step 5. Install vManage Certificate

Use the root.crt that is installed in Step 2.

Cisco vManage

⚙ CONFIGURATION | CERTIFICATES

WAN Edge List   **Controllers**

➤ Send to vBond

No file chosen

	Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration Date
›	CSR Generated	vManage	vManage_rcdn01	1.11.11.11	100	No certificate installed	--

Install Certificate   ×

Certificate Text   📄 Select a file

```
-----BEGIN CERTIFICATE-----
MIIEQjCCAyqgAwIBAgIITwjqFHbasy8wDQYJKoZIhvcNAQELBQAwbDELMAkGA1UE
BhMCVVMxCzAJBgNVBAgTAlRYMQ0wCwYDVQQHEwRSQ0ROMRcwFQYDVQQKEw5hbWF1
Z3VzdC5jaXNjbnjbzEXMBUGA1UECxMOYW1hdWd1c3QuY2IzY28xDzANBgNVBAMTBlJv
b3RDQTAeFw0yMDA1MDgxNjE0MDBaFw0yMzA1MDgxNjE0MDBaMIHNMQswCQYDVQQG
EwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuJEpvc2UxFzAV
BgNVBAsTDmFtYXVndXN0LmNpc2NvMRQwEgYDVQQKEwt2SVB0ZWxhIEluY2FzFDMEEG
A1UEAxM6dm1hbmFnZS05MjMwMjMMwMmU3Ny1jMDVjLTQ2MmEtYTcxNy01ZjAxM2IzMWQ1
MmYtMC52aXB0ZWxhLmNvbTEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEB2aXB0ZWxh
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKeHM8FHcKmhqX0E
tlZnLicP5bGjZTTBiihm+kXwWyqnupv/JTdSy4AEx28gamKt/+d7dNg9iPrfAsBc
5rVoP6kyeT2MGXOFdostMNVy8asUnCJhtiRsrEn6mnd5YOHSNz6jPS/Wx2IAnIZB
Z/W46TM7kyqDl1tus4R1vj3H7ASkeAHucVZ4NmPoAJSn1Uzx8plPBIoG2bwmErJP
17zpn8WBVhqT2r0z0Az3Jb246lPd7d8smBXcBKif51FY+nXepDhrQz3XZUcToqm/
```

[Install] [Cancel]

Cisco vManage

📋 TASK VIEW

Install Certificate

Total Task: 1 | Success : 1

	Status	Message	Device Type	Device IP
⌄	✔ Success	Successfully synced vEdge list on vManage-9...	vManage	92302e77-c05c-462a-a71

```
[8-May-2020 16:15:06 UTC] Install Certificate, on device 92302e77-c05c-462a-a717-5f013b31d52f, started by user "admin" from IP address "169.
[8-May-2020 16:15:06 UTC] Pushing serial list to vManage-92302e77-c05c-462a-a717-5f013b31d52f (vManage_rcdn01)
[8-May-2020 16:15:06 UTC] Started processing serial list file on vManage-92302e77-c05c-462a-a717-5f013b31d52f (vManage_rcdn01)
[8-May-2020 16:15:07 UTC] Completed processing serial list file on vManage-92302e77-c05c-462a-a717-5f013b31d52f (vManage_rcdn01)
[8-May-2020 16:15:07 UTC] Done - Push vSmart List for vManage-92302e77-c05c-462a-a717-5f013b31d52f (vManage_rcdn01)
[8-May-2020 16:15:07 UTC] Pushed serial list to vManage-92302e77-c05c-462a-a717-5f013b31d52f (vManage_rcdn01)
[8-May-2020 16:15:07 UTC] Updated controllers with new certificate serial number of vManage-92302e77-c05c-462a-a717-5f013b31d52f
```
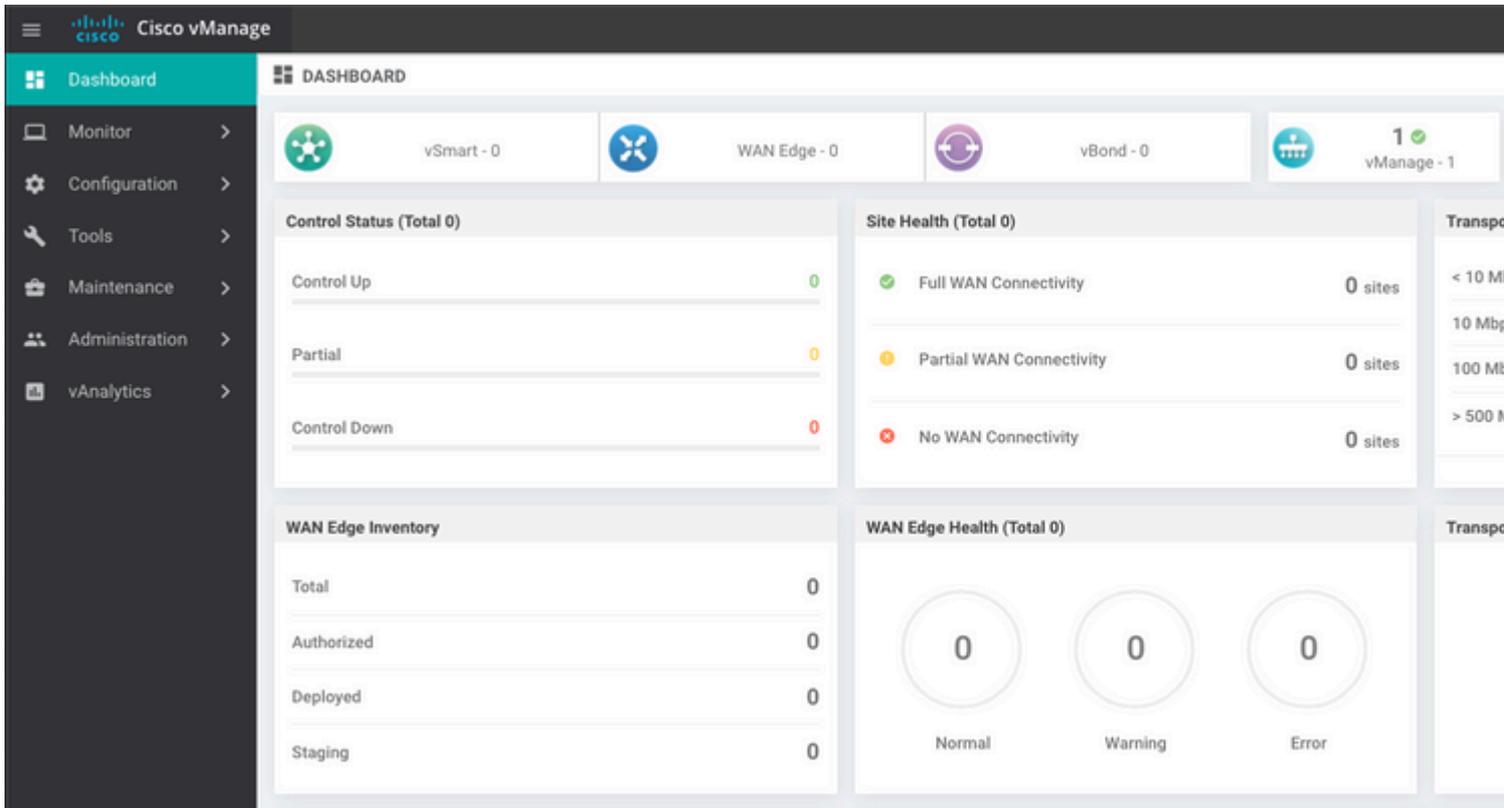
Step 6. Restore The Database

<#root>

vManage_rcdn01# request nms configuration-db restore path /home/admin/05_08_20_configdb.tar.gz

```
Configuration database is running in a standalone mode
0 [main] INFO com.viptela.vmanage.server.deployment.cluster.ClusterConfigurationFileHandler  - Trying to
4 [main] INFO com.viptela.vmanage.server.deployment.cluster.ClusterConfigurationFileHandler  - Working o
Successfully saved cluster configuration for localhost
Starting DB backup from: localhost
Creating directory: local
cmd to backup db: sh /usr/bin/vconfd_script_nms_neo4jwrapper.sh backup localhost /opt/data/backup/local
Finished DB backup from: localhost
Stopping NMS application server on localhost
Stopping NMS configuration database on localhost
Reseting NMS configuration database on localhost
Restoring from DB backup: /opt/data/backup/staging/graph.db-backup
cmd to restore db: sh /usr/bin/vconfd_script_nms_neo4jwrapper.sh  restore /opt/data/backup/staging/graph
Successfully restored DB backup: /opt/data/backup/staging/graph.db-backup
Starting NMS configuration database on localhost
Waiting for 10s before starting other instances...
Polling neo4j at: localhost
NMS configuration database on localhost has started.
Updating DB with the saved cluster configuration data
Successfully reinserted cluster meta information
Starting NMS application-server on localhost
Waiting for 120s for the instance to start...
Removed old database directory: /opt/data/backup/local/graph.db-backup
Successfully restored database
```

This step takes more time and it depends on the backup.

You can verify the process by tailing the logs on vShell.

```
<#root>

vManage_rcdn01:~$

tail -fq /var/log/nms/vmanage-server.log /var/log/nms/neo4j-out.log
```

Step 7. Check Services

```
vManage_rcdn01# request nms all status
```

Step 8. Reauthenticate Controllers

Currently, you can observe that all policies, templates, and configurations have been loaded onto vManage, but all controllers are down.
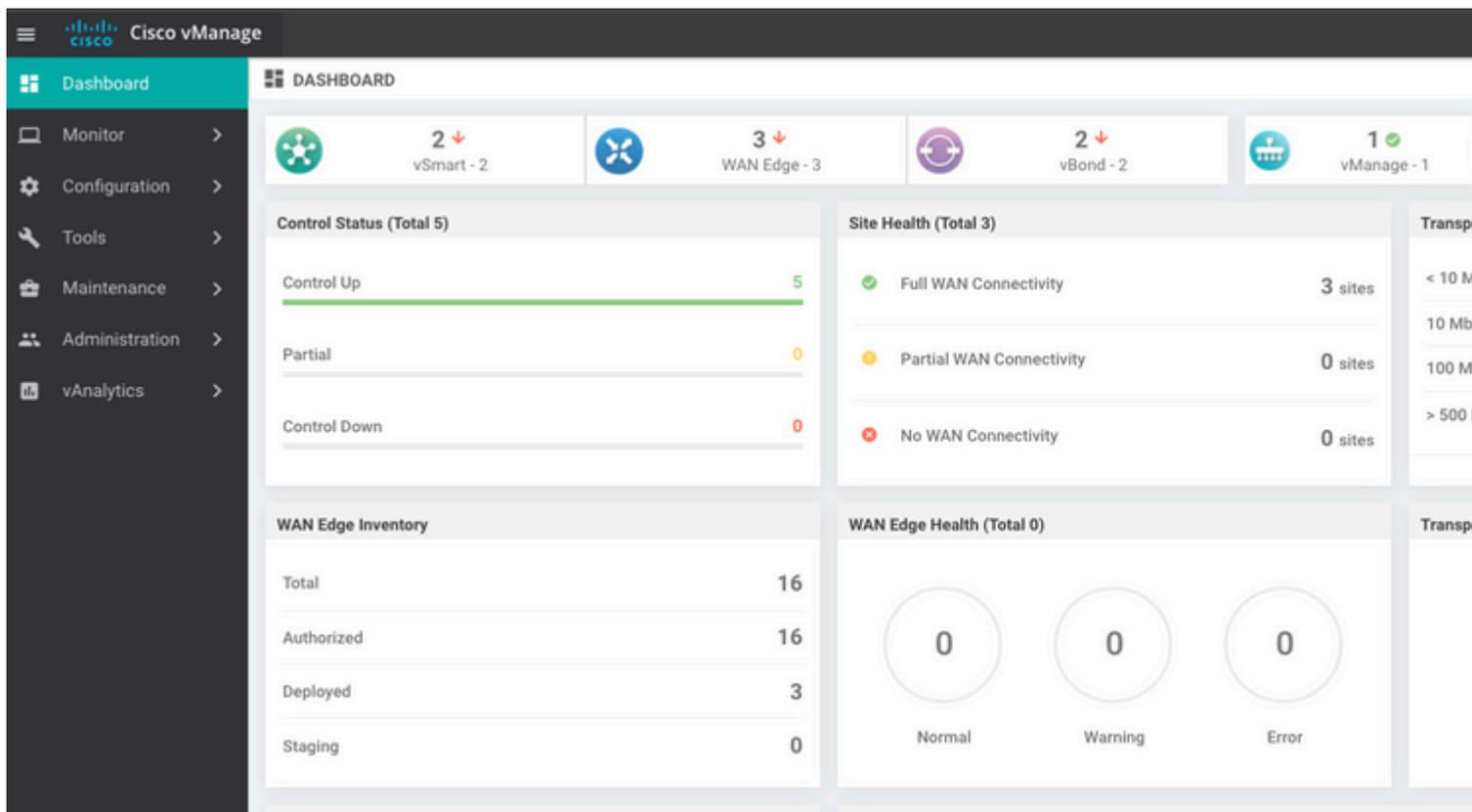
You need to re-authenticate all the controllers.

Navigate to Configuration > Devices. Edit each controller and fill in the management IP address (management IP can be found in the local configuration) username and password.
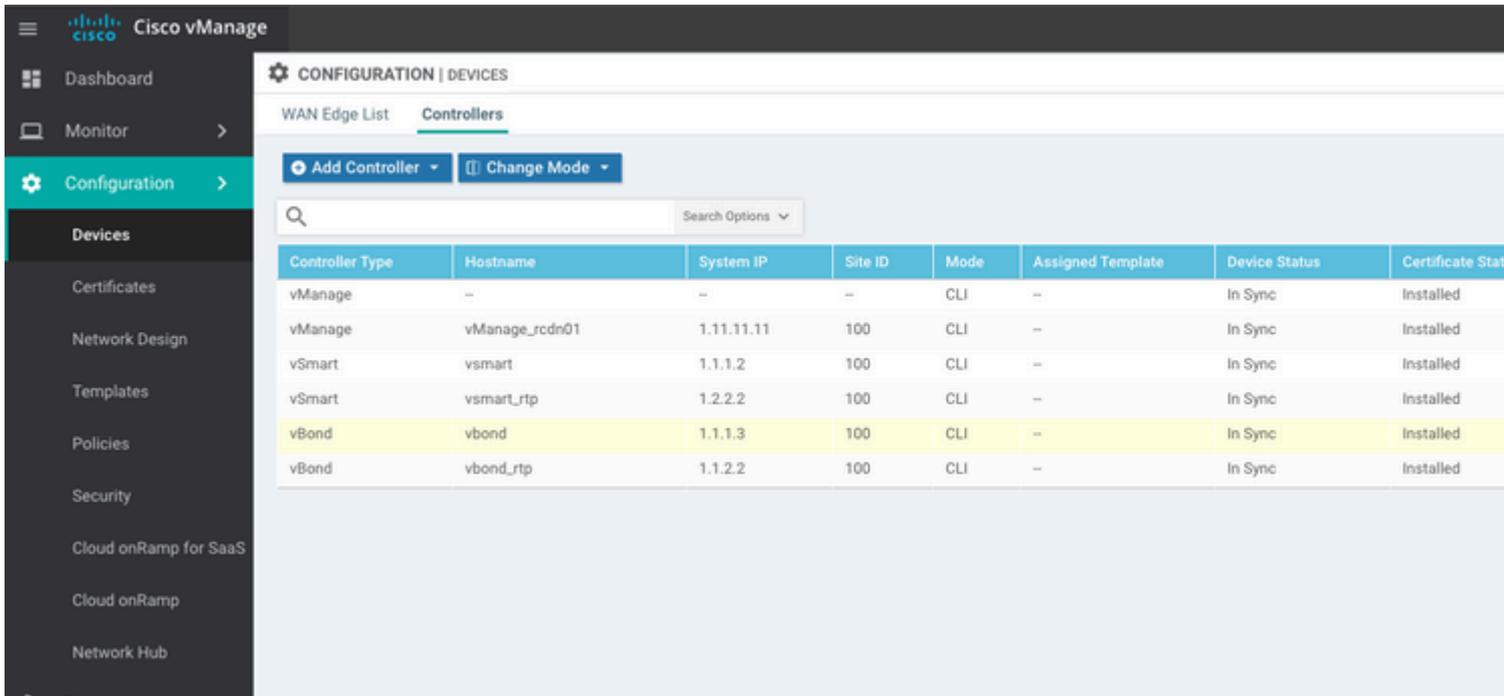
Step 9. Send Updates to Controllers
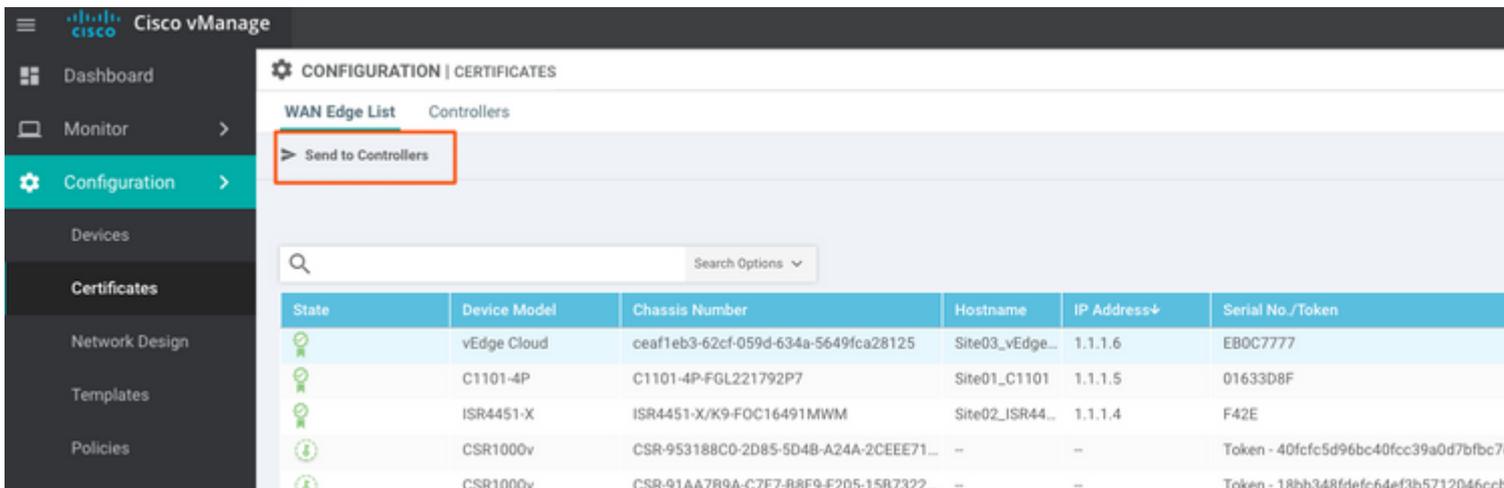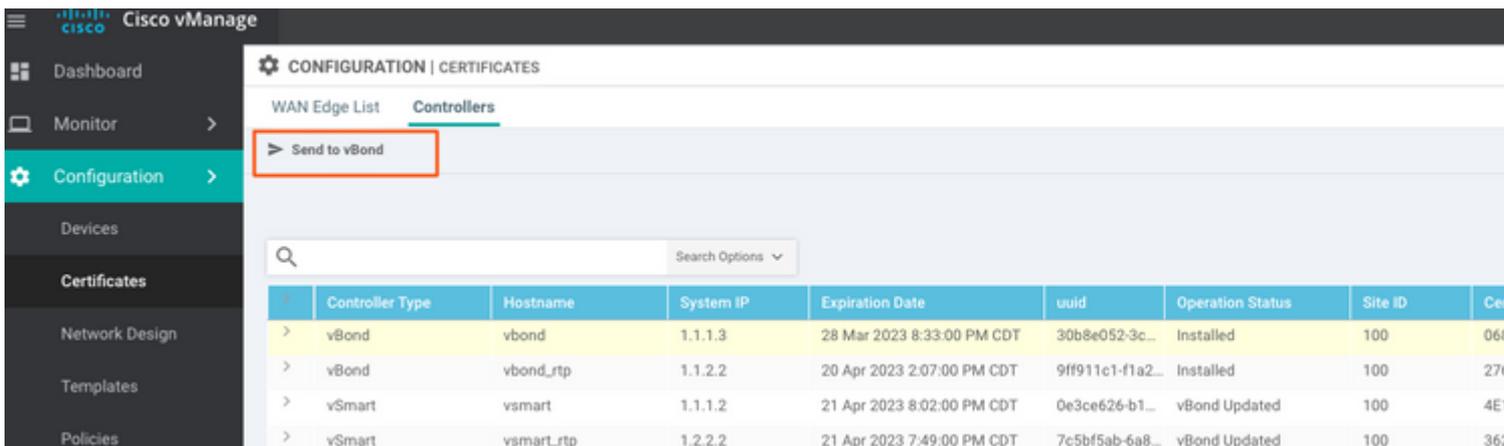
Now, you see all the devices can be managed by vManage.

Screenshot 1 — Dashboard

Dashboard
- Monitor >
- Configuration >
- Tools >
- Maintenance >
- Administration >
- vAnalytics >

DASHBOARD

2 ↑ vSmart - 2		3 ↑ WAN Edge - 3		2 ↑ vBond - 2		1 ⊘ vManage - 1	

Control Status (Total 4)

Control Up	4
Partial	0
Control Down	0

Site Health (Total 2)

⊘	Full WAN Connectivity	2 sites
!	Partial WAN Connectivity	0 sites
⊗	No WAN Connectivity	0 sites

Transp...
- < 10 M
- 10 MB
- 100 M
- > 500

WAN Edge Inventory

Total	15
Authorized	15
Deployed	3
Staging	0

WAN Edge Health (Total 2)

2	0	0
Normal	Warning	Error

Transp...
- 100 %
- 50 %
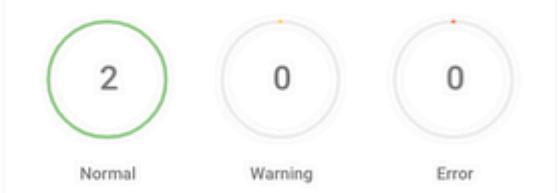
Top Applications

No data to display

Application-Aware Routing

	Tunnel Endpoints	Avg. Latency (ms)	Av...
〜	Site02_ISR4451:default-Site03_vEdge_Cloud...	50.5	0.0
〜	Site01_C1101:default-Site02_ISR4451:default	32.167	0.0
〜	Site02_ISR4451:default-Site01_C1101:default	32	0
〜	Site01_C1101:default-Site03_vEdge_Cloud:d...	25.917	0

Screenshot 2 — Configuration | Templates

- Dashboard
- Monitor >
- **Configuration** >
  - Devices
  - Certificates
  - Network Design
  - **Templates**
  - Policies
  - Security
  - Cloud onRamp for SaaS
  - Cloud onRamp
  - Network Hub

CONFIGURATION | TEMPLATES

Device | Feature

⊕ Add Template

Template Type: Non-Default ▼   🔍   Search Options ▼

Name	Description	Type	Device Model	Device Templates	Devices Attached
vEdge_VPN_0	Default Transport VPN tem...	WAN Edge VPN	C1111-4PLTEEA | C1117-4P...	0	0
Default_AAA	Default AAA template settin...	AAA	C1111-4PLTEEA | C1117-4P...	1	1
cEdge_VPN_0	Default Transport VPN tem...	WAN Edge VPN	C1111-4PLTEEA | C1117-4P...	1	1
vEdge_VPN_512_Interface	VPN 512 interface config	WAN Edge Interface	C1111-4PLTEEA | C1117-4P...	0	0
vEdge_VPN_0_Interface	VPN 0 interface config	WAN Edge Interface	C1111-4PLTEEA | C1117-4P...	0	0
Default_Banner	Banner for amaugust.cisco	Banner	ISR4451-X | C1101-4P | vEd...	1	1
vEdge_VPN_512	VPN 512 add default route	WAN Edge VPN	C1111-4PLTEEA | C1117-4P...	0	0
cEdge_VPN_0_Interface	VPN 0 interface config	WAN Edge Interface	C1111-4PLTEEA | C1117-4P...	1	1
cEdge_VPN_512	VPN 512 add default route	WAN Edge VPN	C1111-4PLTEEA | C1117-4P...	1	1
cEdge_VPN_512_Interface	VPN 512 interface config	WAN Edge Interface	C1111-4PLTEEA | C1117-4P...	1	1