Install Cisco Optical Network Controller Using VMware vSphere

Installation Requirements

The following list contains the pre-requisites of Cisco Optical Network Controller installation.

- Before installing Cisco Optical Network Controller, you must first login in to the VMware customer center and download VMware vCenter server version 7.0, as well as vSphere server and client with version 7.0. Cisco Optical Network Controller is deployed on rack or blade servers within vSphere.

Attention Upgrade to VMware vCenter Server 8.0 U2 if you are using VMware vCenter Server 8.0.2 or VMware vCenter Server 8.0.1.

- Install ESXi host version of 7.0 or higher on the servers to support creating Virtual Machines.
- You must have a DNS server. The DNS server can be an internal DNS server if the Cisco Optical Network Controller instance is not exposed to the internet.
- You must have an NTP server or NTP Pool for time synchronization. Configure the same NTP server or pool on Cisco Optical Network Controller and the PC or VM you use to access Cisco Optical Network Controller. Configure the ESXi host also with the same NTP configuration.
- Before the Cisco Optical Network Controller installation, three networks must be created.
  - **Control Plane Network**:

    The control plane network helps in the internal communication between the deployed VMs within a cluster. If you are setting up a standalone system, this can refer to any private network.

  - **VM Network or Northbound Network**:

The VM network is used for communication between the user and the cluster. It handles all the traffic to and from the VMs running on your ESXi hosts and this is your Public network through which the UI is hosted.

- **Eastbound Network**:

  The Eastbound Network helps in the internal communication between the deployed VMs within a cluster. If you are setting up a standalone system, this can refer to any private network.

- Accept the Self-Signed Certificate from the ESXi host.
  1. Access the ESXi host using your web browser.
  2. If you receive a security warning indicating that the connection is not private or that the certificate is not trusted, proceed by accepting the risk or bypassing the warning.

Note For more details on VMware vSphere, see *VMware vSphere*.

The minimum requirement for Cisco Optical Network Controller installation is given in the table below.

Table 1: Minimum Requirement

Sizing	CPU	Memory	Disk
XS	16 vCPU	64 GB	800 GB
S	32 vCPU	128 GB	1536 GB
M	48 vCPU	256 GB	1536 GB

Note Configure vCPU and memory according to the VM profile (XS=16vCPU+64GB, S=32vCPU+128GB) before you power on the VM in vCenter.

vCPU to Physical CPU Core Ratio: We support a vCPU to Physical CPU core ratio of 2:1 if hyperthreading is enabled and the hardware supports hyperthreading. Hyperthreading is enabled by default on Cisco UCS servers that support hyperthreading. In other cases, the vCPU to Physical CPU core ratio is 1:1.

The requirements based on type of deployment are given in the table below.

Table 2: Deployment Requirements

Deployment Type	Requirements
Standalone (SA)	**Control Plane Network:** Can be a private network for standalone setups. Requires 1 IP address. **Gateway:** Required. **DNS Server:** Should be an internal DNS if the node is not exposed to the internet; otherwise, an internet DNS can be used. **Northbound Network (VM Network):** Should be a public network. All communication between the Cisco Optical Network Controller and devices will flow through this network. Requires 1 public IP address. **Gateway:** Required. **DNS Server:**Required. Should be an internal DNS if the node is not exposed to the internet; otherwise, an internet DNS can be used. **Eastbound Network:** Can be a private network for standalone setups. Requires 1 private IP address. **Gateway:** Required. **DNS Server:**Required. Should be an internal DNS if the node is not exposed to the internet; otherwise, an internet DNS can be used.

To create the control plane and virtual management networks follow the steps listed below.

1. From the vSphere client, select the Datacenter where you want to add the ESXi host.
2. Right-click the server from the vCenter inventory and click **Add Networking**.
3. To create a private network for Control Plane and Eastbound Networks, follow the wizard for a Standard Switch addition for each network.
   a. In **Select connection type**, choose **Virtual Machine Port Group for a Standard Switch** and click **Next**.
   b. In **Select target device** , select **New Standard Switch (MTU 1500)** and click **Next**.
   c. In **Create a Standard Switch**, click **Next**, and confirm *There are no active physical network adapters for the switch.*
   d. In **Connection settings** choose a network label (Control Plane or Eastbound) and select VLAN ID as None(0) click **Next**.
   e. In **Ready to complete**, review your configuration and click **Finish**.

After adding the ESXi host, create the Control Plane, Northbound, and Eastbound Networks before deploying.

This table lists the default port assignments.

Table 3: Communications Matrix

Traffic Type	Port	Description
Inbound	TCP 22	SSH remote management
	TCP 8443	HTTPS for UI access

Traffic Type	Port	Description
Outbound	TCP 22	NETCONF to routers
	TCP 389	LDAP if using Active Directory
	TCP 636	LDAPS if using Active Directory
	Customer Specific	HTTP for access to an SDN controller
	User Specific	HTTPS for access to an SDN controller
	TCP 3082, 3083, 2361, 6251	TL1 to optical devices
Eastbound	TCP 10443	Supercluster join requests
	UDP 8472	VxLAN
syslog	User specific	TCP/UDP
Control Plane Ports (Internal network between cluster nodes, not exposed)	TCP 443	Kubernetes
	TCP 6443	Kubernetes
	TCP 10250	Kubernetes
	TCP 2379	etcd
	TCP 2380	etcd
	UDP 8472	VXLAN
	ICMP	Ping between nodes (optional)

SSH Key Generation

For accessing SSH, ed25519 key is required. The ed25519 key is different from the RSA key.

Use the following CLI to generate the ed25519 key.

```
ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/xyz/.ssh/id_ed25519):
./<file-name-of-your-key>.pem
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./<file-name-of-your-key>.pem
Your public key has been saved in ./<file-name-of-your-key>.pem.pub
The key fingerprint is:
SHA256:zGW6aGn8rxvEq82sA/97jOaHrl9rnoTaYi+TqU3MeRU xyz@abc
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|                 |
|          E      |
|       + + .     |
|        S .      |
|    .+ = =       |
|     o@o*+o      |
```

Install Cisco Optical Network Controller Using VMware vSphere

```
|      =XX++=o      |
|     .o*#/X=       |
+-----[SHA256]------+

#Once created you can cat the file with .pub extension for the public key. ( ex:
<file-name-of-your-key>.pem.pub )

cat <file-name-of-your-key>.pem.pub
#The above key has to be used in the deployment template ( SSH Public Key ) in the Deployment
 process
```

Install Cisco Optical Network Controller Using VMware vSphere

The Cisco Optical Network Controller is distributed as a single OVA file, which is a disk image deployed using vCenter on any ESXi host. This OVA includes several components, such as a file descriptor (OVF) and virtual disk files that contain a basic operating system and the Cisco Optical Network Controller installation files. It can be deployed on ESXi hosts supporting standalone (SA) or supercluster deployment models.

To deploy the OVA template, follow the steps given below.

Before you begin

Note During the OVF deployment, the deployment gets aborted if there is an internet disconnection.

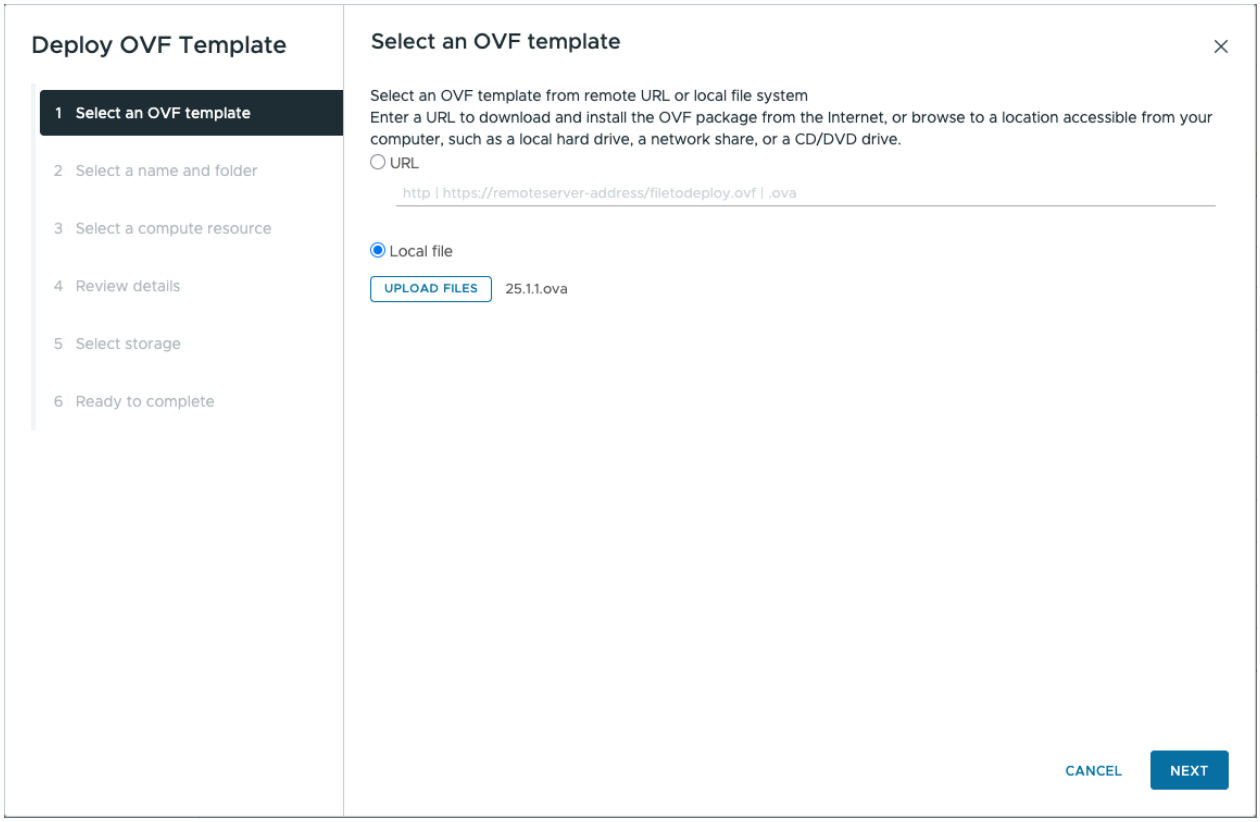
Procedure

Step 1 Right-click the ESXi host in the vSphere client screen and click **Deploy OVF Template**.

Step 2 In the **Select an OVF template** screen, select the **URL** radio button for specifying the URL to download and install the OVF package from the Internet or select the **Local file** radio button to upload the downloaded ova files from your local system and click **Next.**

Install Cisco Optical Network Controller Using VMware vSphere

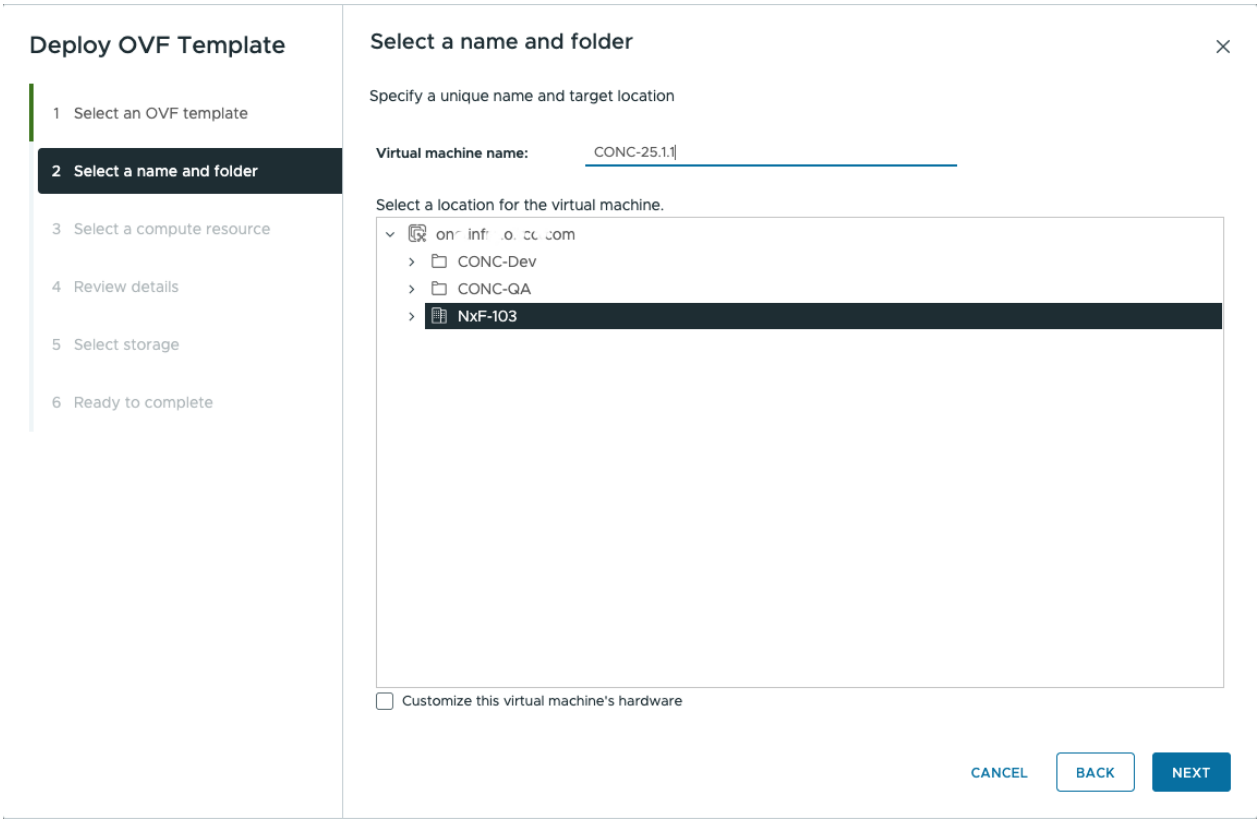
Figure 1: Select an OVF Template



Step 3 In the **Select a name and folder** screen, specify a unique name for the virtual machine Instance. From the list of options, select the location of the VM to be used and click **Next.**

Install Cisco Optical Network Controller Using VMware vSphere

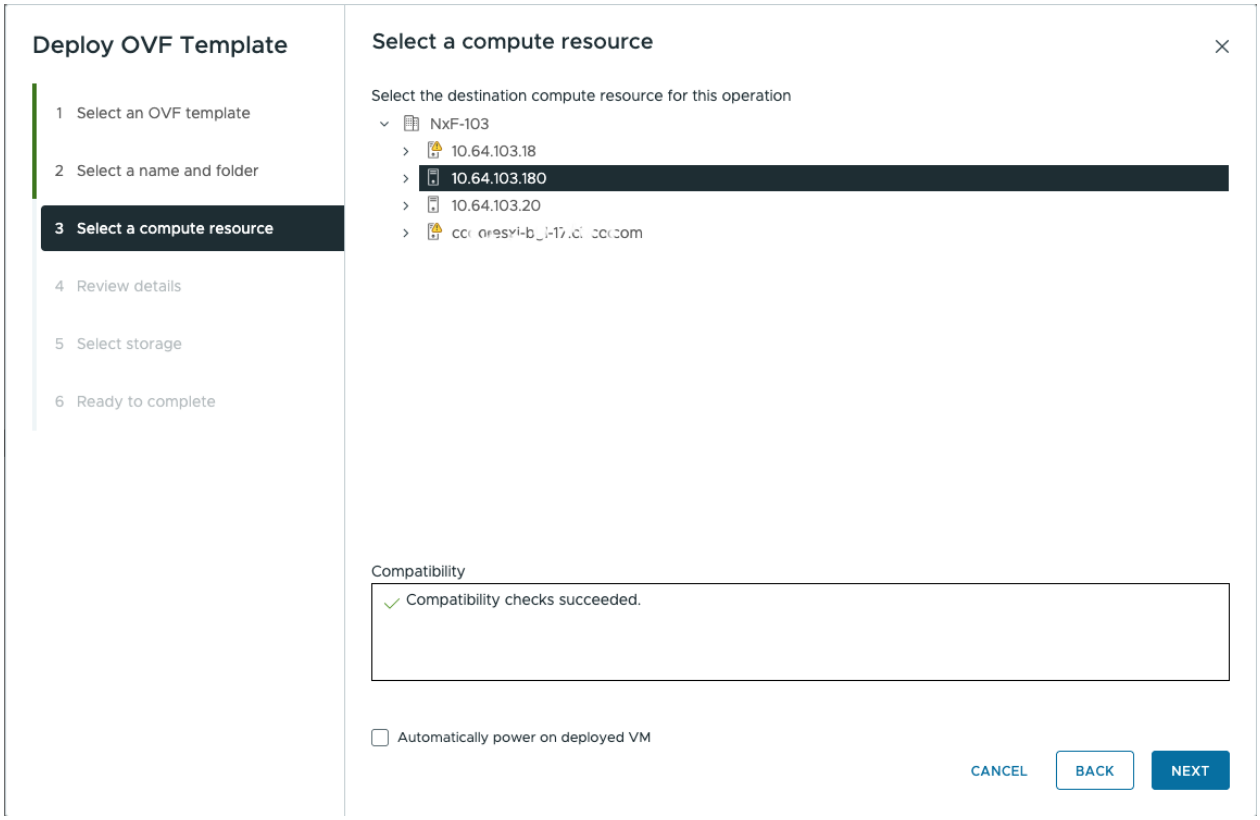
Figure 2: Select a name and folder



Step 4 In the **Select a compute resource** screen, select the destination compute resource on which you want to deploy the VM and click **Next.**

Install Cisco Optical Network Controller Using VMware vSphere

Figure 3: Select a Compute Resource

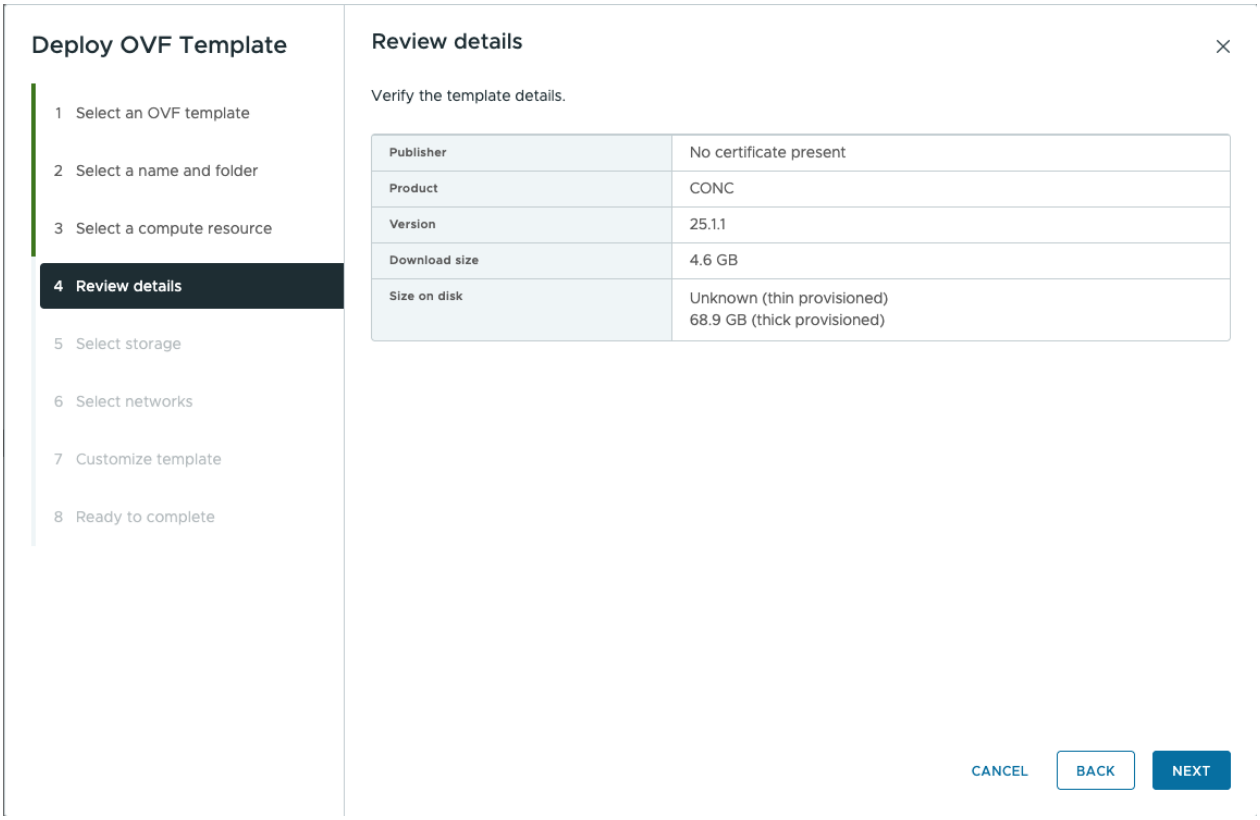


Note
While selecting the compute resource the compatibility check proceeds till it completes successfully.

Step 5 In the **Review details** screen, verify the template details and click **Next**.

Install Cisco Optical Network Controller Using VMware vSphere

Figure 4: Review Details

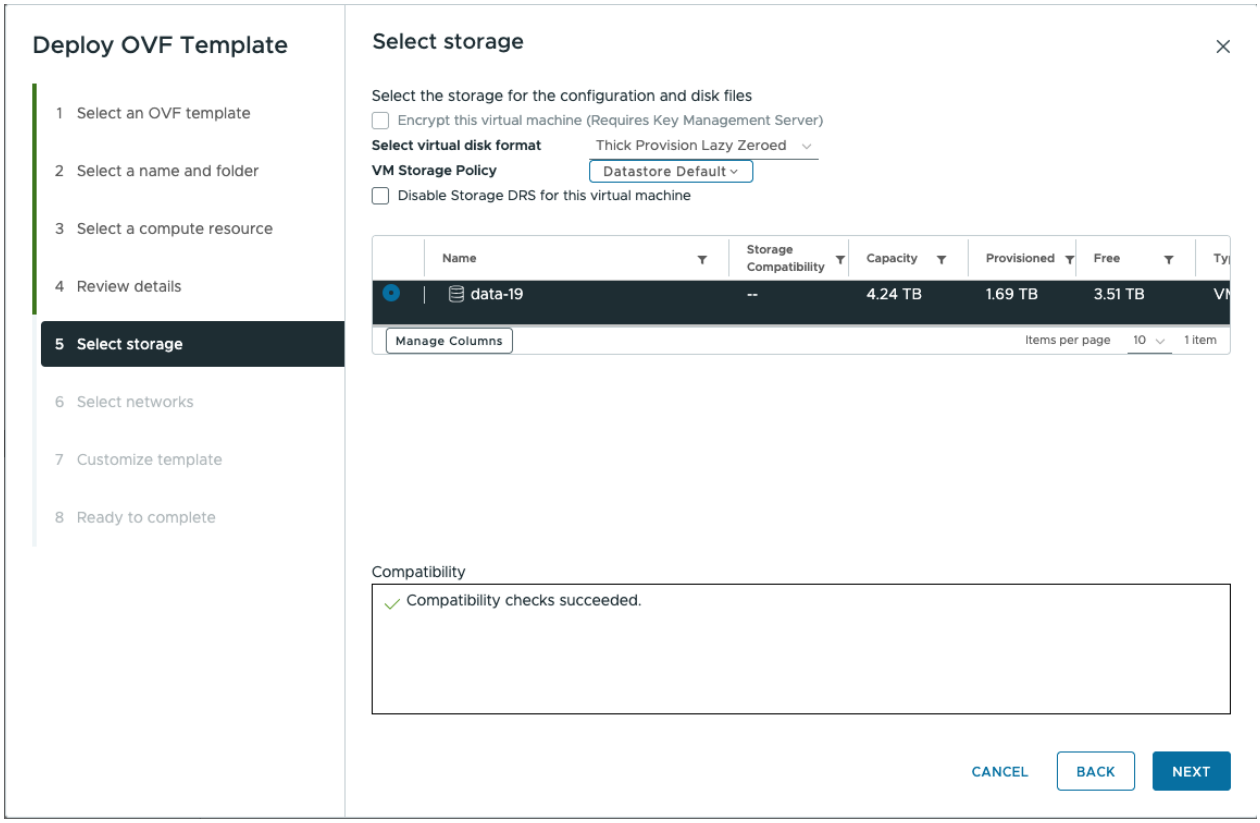


Step 6 In the Select storage screen, select the virtual disk format based on provision type requirement. **VM Storage Policy** is set as *Datastore Default* and click **Next**. Select the **virtual disk format** as *Thin Provision*.

You must select "Thin provision" as the virtual disk format.

Install Cisco Optical Network Controller Using VMware vSphere

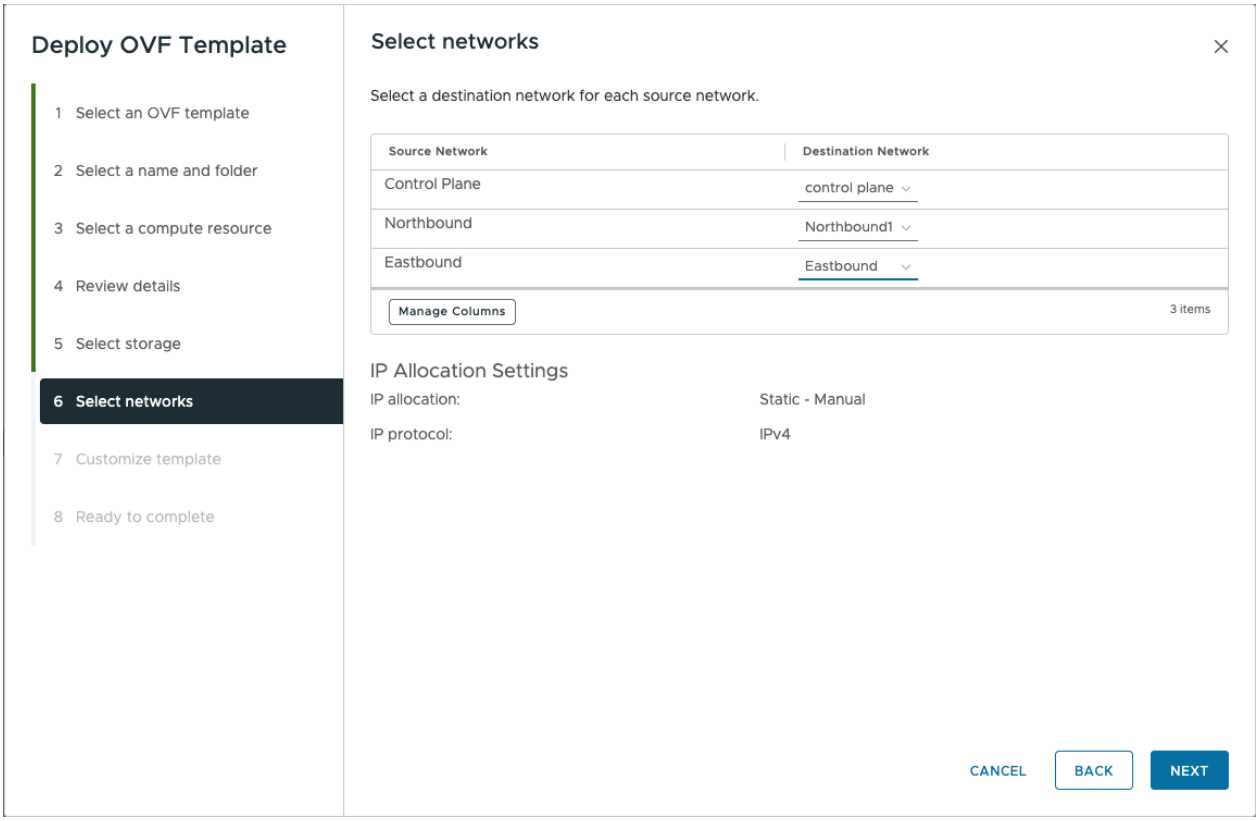
Figure 5: Select Storage



Step 7 In the **Select networks** screen, select the control and management networks as **Control Plane, Eastbound,** and **Northbound** from the networks created earlier and **click Next**.

Install Cisco Optical Network Controller Using VMware vSphere

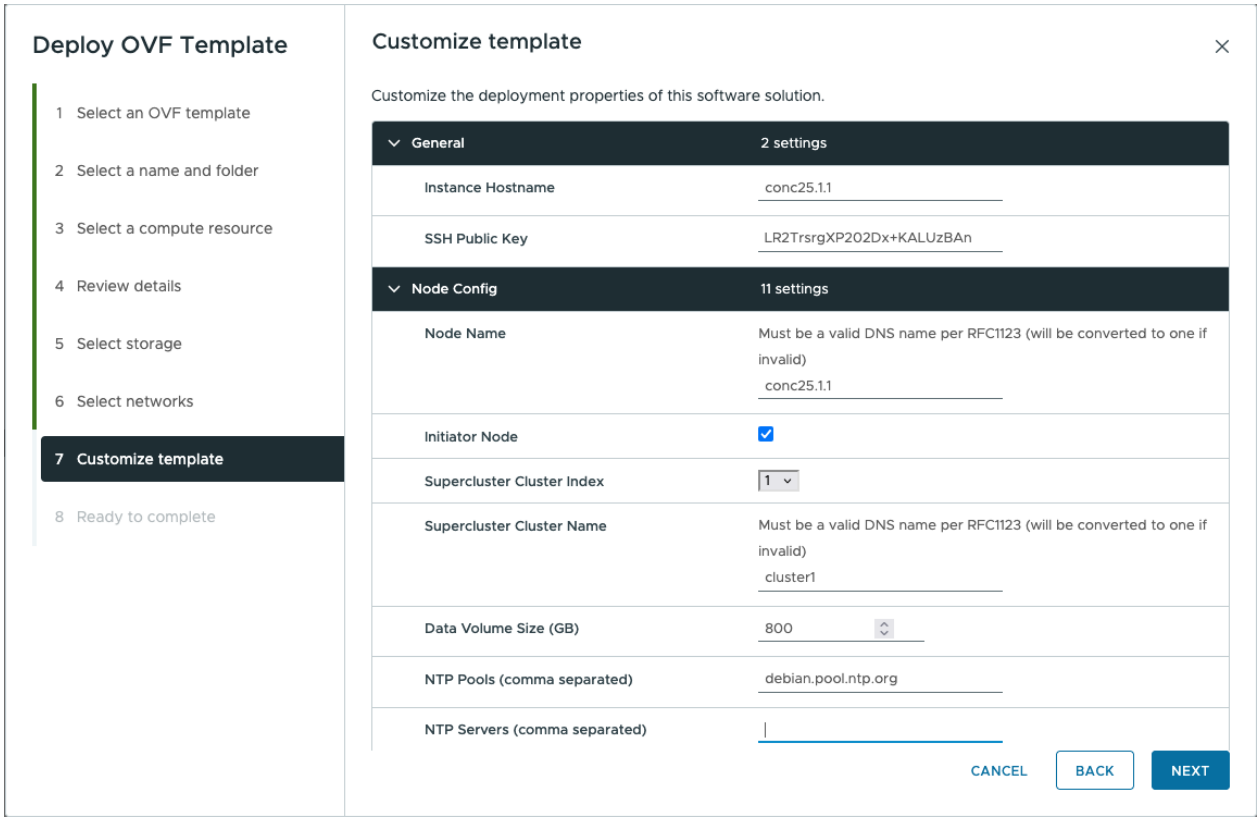
Figure 6: Select Networks



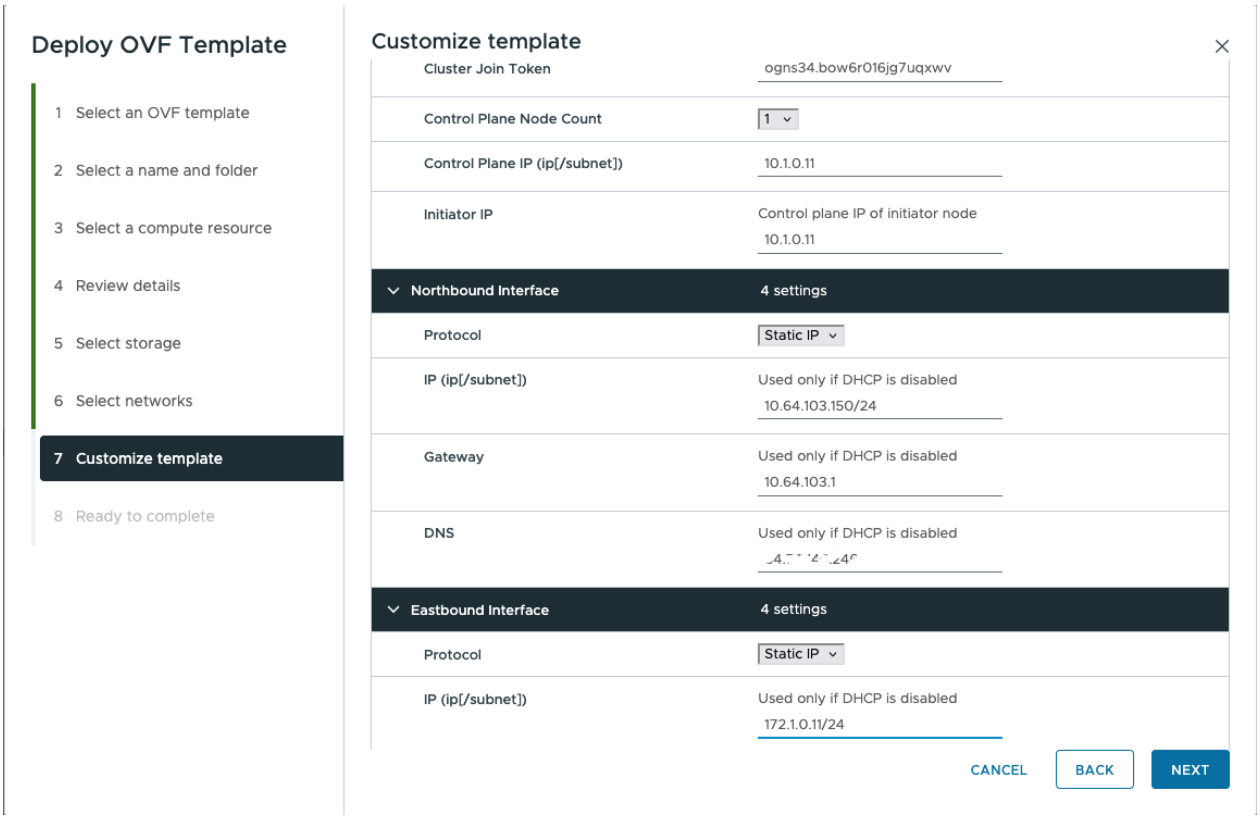
Step 8 In the **Customize template** screen, set the values using the following table as a guideline for deployment.

Install Cisco Optical Network Controller Using VMware vSphere

Figure 7: Customize Template



Install Cisco Optical Network Controller Using VMware vSphere



Install Cisco Optical Network Controller Using VMware vSphere

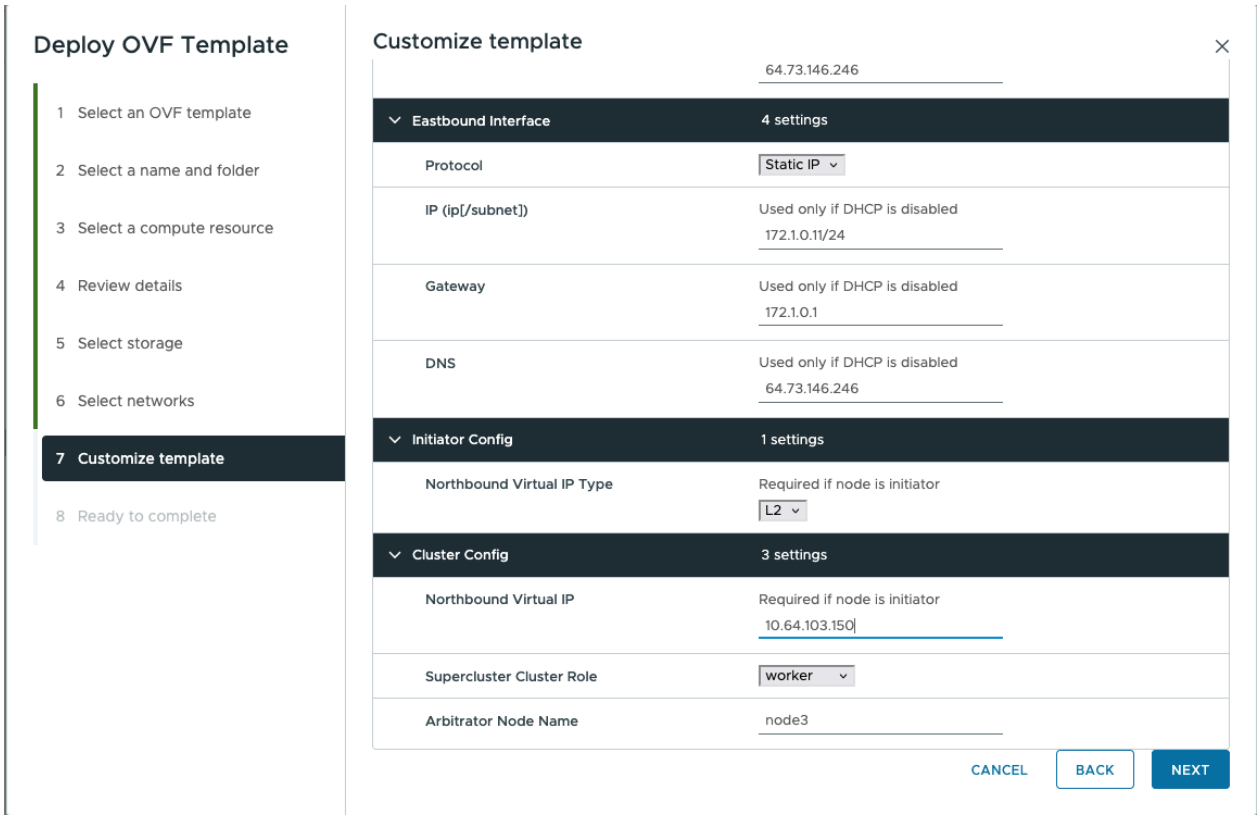


Table 4: Customize Template

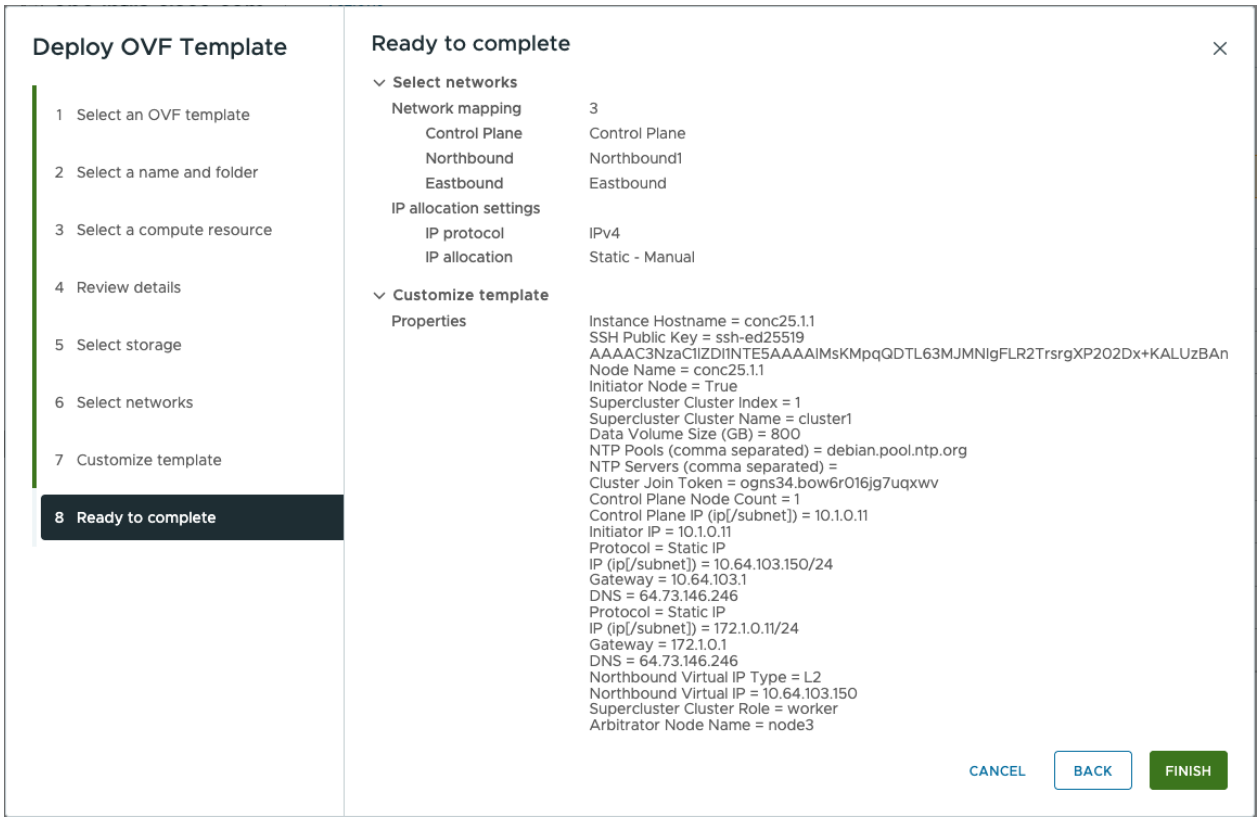
Key	Values
General	
Instance Hostname	*<instance-name>* Must be a valid DNS name per RFC1123.1.2.4. • Contain at most 63 characters. • Contain only lowercase alphanumeric characters or '-' • Start with an alphanumeric character. • End with an alphanumeric character.
SSH Public Key	*<ssh-public-key>*. Used for SSH access that allows you to connect to the instances securely without the need to manage credentials for multiple instances. SSH public key must be a ed25519 key. See SSH Key Generation, on page 4.
Node Config	
Node Name	Use the same name as *Instance Hostname*
Initiator Node	Select the check box

Key	Values
Supercluster Cluster Index	1 If you want to add your Cisco Optical Network Controller instance to a geo-redundant SuperCluster in the future, use different Super Cluster Index values for each instance.
Supercluster Cluster Name	cluster1 Must be a valid DNS name per RFC1123 If you want to add your Cisco Optical Network Controller instance to a geo-redundant SuperCluster in the future, use unique Super Cluster Names for each instance.
Data Volume Size (GB)	Configure data volume according to the VM profile.
NTP Pools (comma separated)	(Optional) A comma-separated list of the NTP pools. For example, debian.pool.ntp.org
NTP Servers (comma separated)	(Optional) A comma-separated list of the NTP servers.
Cluster Join Token	Autogenerated value. Leave as is.
Control Plane Node Count	1
Control Plane IP (ip[/subnet])	<Private IP for the Instance> Control Plane Network
Initiator IP	<Same IP as Control Plane> Control Plane Network
Northbound Interface	
Protocol	Static IP
IP (ip[/subnet]) - if not using DHCP	<Public IP for the Instance> Northbound Network
Gateway - if not using DHCP	<Gateway IP for the Instance> Northbound Network
DNS	DNS Server IP
Eastbound Interface	
Protocol	Static IP
IP (ip[/subnet]) - if not using DHCP	< IP for the Instance> Eastbound Network
Gateway - if not using DHCP	<Gateway IP for the Network> Eastbound Network
DNS	DNS Server IP
Initiator Config	
Northbound Virtual IP Type	L3
Cluster Config	
Northbound Virtual IP	Same as Northbound IP
Supercluster Cluster Role	*worker*

Key	Values
Arbitrator Node Name	a unique node name **Note** If you have other instances of Cisco Optical Network Controller, ensure that the node name is unique across instances.

Step 9 In **Review the details** screen, review all your selections and click **Finish**. To check or change any properties from the review screen anytime, before clicking Finish **click BACK** to go back to the previous screen **Customize template** to add your changes.

Figure 8: Ready to Complete



Step 10 After the VM is created, power-on the VM and try connecting to the VM using the pem key which was generated earlier, see *SSH Key Generation* above. For this, use the private key that is generated along with the public key during customizing the public key options.

Attention
Upon activation of the virtual machine (VM), it is designed not to respond to ping requests. However, you can log in using SSH if the installation has been completed successfully.

Step 11 Log in to the VM using the private key.

Note:

- After the nodes are deployed, the deployment of OVA progress can be checked in the Tasks console of vSphere Client. After Successful deployment Cisco Optical Network Controller takes around 30 minutes to boot.
- By default, the user ID is admin, and only the password needs to be set. This username is to login to the web UI only. For ssh, the username is `nxf`.

Step 12 **SSH to the node** and execute the following CLI command.

```
ssh -i [ed25519 Private key] nxf@<northbound-vip>
Enter passphrase for key '<file-name-of-your-key>.pem':
```

Note
Private key is created as part of the key generation with just the **.pem** extension, and it must be set with the least permission level before using it.

Step 13 After you SSH into the node, use the sedo system status command to check the status of all the pods.

```
sedo system status
┌──────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ System Status (Wed, 16 Apr 2025 10:16:55 UTC)
          │
├─────────┬──────────────────────────────┬─────────────────┬─────────┬──────────────────────┬──────────┤
│ OWNER   │ NAME                         │ NODE            │ STATUS  │ RESTARTS             │
STARTED      │
├─────────┼──────────────────────────────┼─────────────────┼─────────┼──────────────────────┼──────────┤
│ onc     │ monitoring                   │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-alarm-service            │ vc39-es33-sa-169 │ Running │ 0                    │
11 hours ago │
│ onc     │ onc-apps-ui-service          │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-circuit-service          │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-collector-service        │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-config-service           │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-devicemanager-service    │ vc39-es33-sa-169 │ Running │ 0                    │
12 hours ago │
│ onc     │ onc-inventory-service        │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-nbi-service              │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-netconfcollector-service │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-osapi-gw-service         │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-pce-service              │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-pm-service               │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-pmcollector-service      │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-topology-service         │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ onc     │ onc-torch-service            │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ system  │ authenticator                │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
│ system  │ controller                   │ vc39-es33-sa-169 │ Running │ 0                    │
17 hours ago │
```

```
| system | flannel                     | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
| system | ingress-proxy               | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
| system | kafka                       | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
| system | loki                        | vc39-es33-sa-169 | Running | 1 (Latest 17 hours ago)  |
17 hours ago |
| system | metrics                     | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
| system | minio                       | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
| system | postgres                    | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
| system | promtail-grp7c              | vc39-es33-sa-169 | Running | 0                        |
17 hours ago |
```

Note

- The different pods along with their statuses including active and standby modes are all displayed in the different terminal sessions for each pod.
- All the services with owner *onc* must display the status as *Running.*

Step 14 You can check the current version using the **sedo version** command.

```
 sedo version
```

```
Installer: 25.1.1
```

NODE NAME	OS VERSION	KERNEL VERSION
vc39-es33-sa-169	NxFOS 3.2-555 (93358ad257a6cf1e3da439144e3d2e8343b53008)	6.1.0-31-amd64

IMAGE NAME	VERSION	NODES
docker.io/library/alpine	3.20.3	vc39-es33-sa-169
docker.io/rancher/local-path-provisioner	v0.0.30	vc39-es33-sa-169
quay.io/coreos/etcd	v3.5.15	vc39-es33-sa-169
registry.k8s.io/pause	3.10	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmservice	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector-service	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicemanager-service	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory-service	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/monitoring	25.1.1-2	vc39-es33-sa-169
registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-service	25.1.1-2	vc39-es33-sa-169

Install Cisco Optical Network Controller Using VMware vSphere

```
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service      | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/osapi-gw-service         | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pce_service              | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service               | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pmcollector-service      | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service         | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/torch                    | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/authenticator                            | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/bgp                                      | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/controller                               | 3.2-533      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/firewalld                                | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/flannel                                  | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/ingress-proxy                            | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/iptables                                 | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/kafka                                    | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/kubernetes                               | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/loki                                     | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/metrics-exporter                         | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/minio                                    | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/service-proxy                            | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/syslog-forwarder                         | 3.2-503      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/timescale                                | 3.2-515      |
vc39-es33-sa-169 |
└────────────────────────────────────────────────────────────────────────────┴──────────────┴──────────────┘
```

```
sedo version
┌──────────────────────────────────────────────────────────────────────────────────────────────┐
│ Installer: 25.1.1                                                                            │
├──────────────────┬──────────────────────────────────────────────────────────┬────────────────┤
│ NODE NAME        │ OS VERSION                                               │ KERNEL VERSION │
├──────────────────┼──────────────────────────────────────────────────────────┼────────────────┤
│ vc39-es33-sa-169 │ NxFOS 3.2-555 (93358ad257a6cf1e3da439144e3d2e8343b53008) │ 6.1.0-31-amd64 │
└──────────────────┴──────────────────────────────────────────────────────────┴────────────────┘

┌──────────────────────────────────────────────────────────────────┬──────────────┬──────────────┐
│ IMAGE NAME                                                       | VERSION      | NODES
          |
├──────────────────────────────────────────────────────────────────┼──────────────┼──────────────┤
| docker.io/library/alpine                                         | 3.20.3       |
vc39-es33-sa-169 |
| docker.io/rancher/local-path-provisioner                         | v0.0.30      |
vc39-es33-sa-169 |
| dockerhub.cisco.com/cisco-onc-docker/dev/ciscotestautomation/pyats | 23.7.1-beta5 |
```

```
vc39-es33-sa-169 |
| quay.io/coreos/etcd                                                    | v3.5.15      |
vc39-es33-sa-169 |
| registry.k8s.io/pause                                                  | 3.10         |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmservice         | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service      | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector-service    | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service       | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicemanager-service | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory-service    | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/monitoring           | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-service          | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service  | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/osapi-gw-service     | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pce_service          | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service           | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pmcollector-service  | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service     | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/torch                | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/authenticator                        | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/bgp                                  | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/controller                           | 3.2-533      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/firewalld                            | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/flannel                              | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/ingress-proxy                        | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/iptables                             | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/kafka                                | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/kubernetes                           | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/loki                                 | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/metrics-exporter                     | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/minio                                | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/service-proxy                        | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/syslog-forwarder                     | 3.2-503      |
```

```
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/timescale                                  | 3.2-515      |
vc39-es33-sa-169 |
└──────────────────────────────────────────────────────────────────────────────┴──────────────┘
```

Step 15 SSH to the node and set the initial UI password for the admin user.

```
sedo security user set admin --password
```

Note
The password policy for the system includes both configurable settings and non-configurable hard requirements to ensure security.

Password Requirements

- The password must contain at least:
  - 1 uppercase letter
  - 1 lowercase letter
  - 1 number
  - 1 special character
- Must have a minimum length of 8 characters

Configurable Requirements

You can change the password policy settings using the sedo security password-policy set command. Specify the desired parameters to adjust the configuration:

```
sedo security password-policy set --expiration-days <number> --reuse-limit <number>
--min-complexity-score <number>
```

Step 16 To check the default admin user ID, use the command sedo security user list. To change the default password, use the command sedo security user admin set --password on the CLI console of the VM or through the web UI.

Step 17 Use a web browser to access *https://<virtual ip>:8443/* to access the Cisco Optical Network Controller Web UI. Use the admin id and the password you set to log in to Cisco Optical Network Controller.

Note
Access the web UI only after all the `onc` services are running. Use the **sedo system status** to verify that all services are running.

Upgrade a Standalone Deployment of Cisco Optical Network Controller to a new version

The following sections provide instructions for upgrading a standalone deployment of Cisco Optical Network Controller from Release 24.3.1 to 25.1.x and configuring the necessary networks to ensure seamless communication between nodes in a geo-redundant supercluster.

Cisco Optical Network Controller supports upgrades to 25.1.1 from previous releases except 24.3.2. This table lists the upgrade paths you must follow.

Table 5: Upgrade paths

Current version	Upgrade Path to 25.1.1
24.3.2	Unsupported
24.3.1	24.3.1 > 25.1.1

Restriction

- Cisco Optical Network Controller does not support downgrading to an older release. To go back to an older version, take a database backup using the SWIMU application and install the older version using the ova file for the release. After installation, restore the database.
- You can only revert to a previous version if you have created a copy of the target Cisco Optical Network Controller database before upgrading Cisco Optical Network Controller, as described in Backup and Restore Database.

Cisco Optical Network Controller does not support upgrades from 24.3.2 to 25.1.1.

Before you begin

- **Backup Creation:** Ensure that a full system backup is created using the command `sedo backup create full` and exported for recovery if needed.

  Example:

```
root@conc-1:~# sedo backup  create full
Creating backup, this may take a while...
Done creating backup


root@conc-1:~# sedo backup  list
┌──────────────────────┬──────────────────────────────────┬──────┬──────────┬──────────┐
│ NAME                 │ TIME                             │ SIZE                       │
                       │ TYPE │ HOSTNAME   │ POSTGRES VERSION │
├──────────────────────┼──────────────────────────────────┼──────┼──────────┼──────────┤
│ base_0000000E000000010000009E │ 2025-03-11 04:11:47.733980894 +0000 UTC │ 87 MB (838
 MB Uncompressed) │ full │ postgres-0 │ 150008           │
└──────────────────────┴──────────────────────────────────┴──────┴──────────┴──────────┘


root@conc-1:~# cd /data
root@conc-1:/data# sedo backup download base_0000000E000000010000009E
Downloading Backup       ...  [.....<#>..............] [63.03MB in 9.200973s]
Finished downloading backup to "/data/nxf-backup-3.2-1741666307.tar.gz"

root@conc-1:/data# scp /data/nxf-backup-3.0-1736872559.tar.gz <remote location>
```

- **Network Configuration**: Before the Cisco Optical Network Controller upgrade, three networks must be created.
  - **Control Plane Network:** The control plane network helps in the internal communication between the deployed VMs within a cluster.

- **VM Network or Northbound Network:** The VM network is used for communication between the user and the cluster. It handles all the traffic to and from the VMs running on your ESXi hosts. This network is your public network through which the UI is hosted. Cisco Optical Network Controller uses this network to connect to Cisco Optical Site Manager devices using Netconf/gRPC.
- **Eastbound Network**: The Eastbound Network helps in the internal communication between the deployed VMs within a cluster. If you are setting up a standalone system, this can refer to any private network.

- **VMware Setup:** Ensure that the vCenter has the required networks configured and attached correctly. Verify that physical adapters are correctly mapped for Northbound and Eastbound networks.
- **Access and Permissions:** Ensure you have the necessary permissions to execute commands and modify network settings on the nodes.

Procedure

Step 1 Log in to the standalone node CLI using the private key.

Example:

```
ssh -i <private-key_file> nxf@<node_ip>
```

Step 2 Download or copy the 25.1.1 system pack `system-pack-file.tar.gz` to the NxF system running 24.3.1 and place it in the `/tmp` directory using `curl` or `scp`.

Example:

```
scp user@remote_server:/path/to/system-pack-file.tar.gz /tmp/
```

```
curl -o /tmp/system-pack-file.tar.gz http://example.com/path/to/system-pack-file.tar.gz
```

Step 3 Upgrade the SA VM from 24.3.1 to 25.1.1 using the sedo system upgrade commands:

Example:

```
sedo system upgrade upload /tmp/system-pack-file.tar.gz
sedo system upgrade apply
reboot
```

The system reboots and upgrades. The system takes approximately 30 minutes to complete this.

Step 4 After the system reboots, verify the NxF version and system status. Use the `sedo version` and `sedo system status` commands.

Example:

```
sedo version
```

```
┌──────────────────────────────────────────────────────────────────────────────────────────┐
│ Installer: 25.1.1                                                                        │
├──────────────────┬──────────────────────────────────────────────────────────┬────────────┤
│ NODE NAME        │ OS VERSION                                               │ KERNEL VERSION │
├──────────────────┼──────────────────────────────────────────────────────────┼────────────┤
│ vc39-es33-sa-169 │ NxFOS 3.2-555 (93358ad257a6cf1e3da439144e3d2e8343b53008) │ 6.1.0-31-amd64 │
└──────────────────┴──────────────────────────────────────────────────────────┴────────────┘
```

```
┌──────────────────────────────────────────────────────────────┬──────────┬──────────┐
│ IMAGE NAME                                                   │ VERSION  │ NODES    │
│          │                                                   │          │          │
├──────────┼──────────────────────────────────────────────────┼──────────┼──────────┤
│ docker.io/library/alpine                                     │ 3.20.3   │          │
```

```
vc39-es33-sa-169 |
| docker.io/rancher/local-path-provisioner                                  | v0.0.30      |
vc39-es33-sa-169 |
| quay.io/coreos/etcd                                                       | v3.5.15      |
vc39-es33-sa-169 |
| registry.k8s.io/pause                                                     | 3.10         |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmservice            | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service         | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector-service       | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service          | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicemanager-service   | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory-service       | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/monitoring              | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-service             | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service     | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/osapi-gw-service        | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pce_service             | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service              | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pmcollector-service     | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service        | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/torch                   | 25.1.1-2     |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/authenticator                           | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/bgp                                     | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/controller                              | 3.2-533      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/firewalld                               | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/flannel                                 | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/ingress-proxy                           | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/iptables                                | 3.2-508      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/kafka                                   | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/kubernetes                              | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/loki                                    | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/metrics-exporter                        | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/minio                                   | 3.2-505      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/service-proxy                           | 3.2-508      |
```

```
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/syslog-forwarder                          | 3.2-503      |
vc39-es33-sa-169 |
| registry.sedona.ciscolabs.com/nxf/timescale                                 | 3.2-515      |
vc39-es33-sa-169 |
└──────────────────────────────────────────────────────────────────────────────┴──────────────┴──────────────┘
```

```
sedo system status
┌──────────────────────────────────────────────────────────────────────────────────────────────────────────┐
| System Status (Wed, 16 Apr 2025 10:16:55 UTC)
          |
├─────────┬──────────────────────────┬─────────────────┬─────────┬──────────────────────────┬──────────────┤
| OWNER   | NAME                     | NODE            | STATUS  | RESTARTS                 |
STARTED      |
├─────────┼──────────────────────────┼─────────────────┼─────────┼──────────────────────────┼──────────────┤
| onc     | monitoring               | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-alarm-service        | vc39-es33-sa-169 | Running | 0                        | 11
 hours ago |
| onc     | onc-apps-ui-service      | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-circuit-service      | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-collector-service    | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-config-service       | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-devicemanager-service | vc39-es33-sa-169 | Running | 0                        | 12
 hours ago |
| onc     | onc-inventory-service    | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-nbi-service          | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-netconfcollector-service | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-osapi-gw-service     | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-pce-service          | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-pm-service           | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-pmcollector-service  | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-topology-service     | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| onc     | onc-torch-service        | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | authenticator            | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | controller               | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | flannel                  | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | ingress-proxy            | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | kafka                    | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | loki                     | vc39-es33-sa-169 | Running | 1 (Latest 17 hours ago)  | 17
 hours ago |
| system  | metrics                  | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | minio                    | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
| system  | postgres                 | vc39-es33-sa-169 | Running | 0                        | 17
 hours ago |
```

```
| system | promtail-grp7c              | vc39-es33-sa-169 | Running | 0                      | 17
 hours ago |
└────────┴─────────────────────────────┴──────────────────┴─────────┴────────────────────────┴──────────┘
```

Step 5 Verify onboarded sites and services by accessing the Cisco Optical Network Controller UI.

Example:

Use a web browser to access *https://<virtual ip>:8443/* to access the Cisco Optical Network Controller Web UI.

Update time zone configuration in a standalone deployment

From Cisco Optical Network Controller Release 25.1.2, you can update the timezone configuration. Previously, only the UTC timezone was supported. Now you can configure Cisco Optical Network Controller in your preferred timezone.

For standalone deployments, you must use the command to update the timezone in the CLI for each VM and then restart the VM according to the steps in this procedure to ensure a seamless change into the new timezone configuration.

Limitations

- Alarms and logs are saved in UTC in the database, which minimizes impact during time zone transitions, although during the transition period, for example, during a switchover, you might briefly see alarms with different time zone stamps in the UI before the system converges to the final setting.
- Do not make timezone changes frequently as they might cause inconsistencies and require reboots of VMs/services.
- When cross-launching from Cisco Optical Network Controller, the time zone offset will remain the same, but the IANA time zone name displayed in the cross-launched application might differ from the one configured in Cisco Optical Network Controller. This discrepancy occurs because the same timezone offset can have multiple IANA timezone names.
- TAPI data and notifications continue to use UTC +0000.
- SNMP traps use epoch time without any time zone offset calculated on the epoch.
- Developer logs and techdump data uses UTC.

Before you begin

You must perform these pre-checks on each VM before changing the timezone.

- Make sure all the pods are running by running the kubectl get pods -A | grep onc command.

  This example shows a sample output where all pods are running. Verify status of every pod is `Running`.

```
root@vm1-cluster1-node1:~# kubectl get pods -A | grep onc

onc                  monitoring-0                                 2/2     Running
 0              21m

onc                  onc-alarm-service-0                          2/2     Running
 3 (51m ago)    3h6m
```

```
onc                  onc-apps-ui-service-6f95dfbc7c-60w87ne           2/2     Running
 3 (51m ago)    3h6m

onc                  onc-circuit-service-0                            2/2     Running
 3 (51m ago)    3h6m

onc                  onc-collector-service-0                          2/2     Running
 3 (51m ago)    3h6m

onc                  onc-config-service-0                             2/2     Running
 3 (51m ago)    3h6m

onc                  onc-devicemanager-service-0                      2/2     Running
 3 (51m ago)    3h6m

onc                  onc-inventory-service-0                          2/2     Running
 3 (51m ago)    3h6m

onc                  onc-nbi-service-0                                2/2     Running
 3 (51m ago)    3h6m

onc                  onc-netconfcollector-service-85bd7c89bf-qc8pf    2/2     Running
 0              21m

onc                  onc-osapi-gw-service-0                           2/2     Running
 3 (51m ago)    3h6m

onc                  onc-pce-service-0                                2/2     Running
 3 (51m ago)    3h6m

onc                  onc-pm-service-0                                 2/2     Running
 3 (51m ago)    136m

onc                  onc-pmcollector-service-86dbcbc87b-9cnhc         2/2     Running
 0              21m

onc                  onc-topology-service-0                           2/2     Running
 3 (51m ago)    3h6m

onc                  onc-torch-service-0                              2/2     Running
 3 (51m ago)    3h6m
```

Procedure

Step 1 SSH into the VM and run this command.

sudo timedatectl set-timezone *timezone-name*

Example:

In the following example, we set the timezone to JST.

```
root@vm1-cluster1-node1:~# sudo timedatectl set-timezone Asia/Tokyo

root@vm1-cluster1-node1:~# timedatectl

               Local time: Mon 2025-06-09 15:01:26 JST

           Universal time: Mon 2025-06-09 06:01:26 UTC
```

```
                  RTC time: Mon 2025-06-09 06:01:26

                 Time zone: Japan (JST, +0900)

System clock synchronized: yes

              NTP service: active

          RTC in local TZ: no
```

A few valid timezones are:

```
Asia/Kolkata
Asia/Dubai
Europe/Amsterdam
Africa/Bujumbura
```

Step 2 Reboot the node using the **sudo reboot** command.

Step 3 Verify the node is up and running using these commands.

- **kubectl get pods -A | grep onc**

Verify the timezone in one of the pods using these commands. See the offset after the time.

```
root@vm1-cluster1-node1:~# kubectl exec -ti onc-torch-service-0 -n onc -- bash

onc-torch-service-0:/$ date -R

Mon, 09 Jun 2025 15:22:42 +0900
```

Timezone configuration has been updated and Cisco Optical Network Controller webUI now displays time in the newly configured timezone.

The following screenshots show the difference between the behaviour in 25.1.1 and 25.1.2. Note that the timestamps are displayed differently with the timezone name and offset included in the timestamp in Release 25.1.2.

Figure 9: PM History in Release 25.1.2

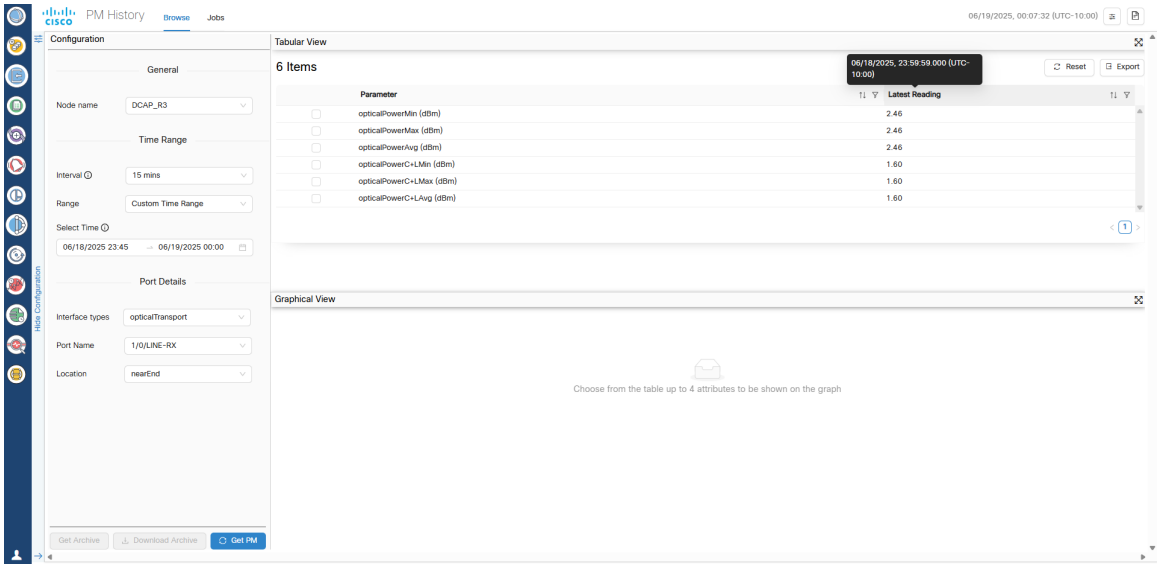


Figure 10: PM History in Release 25.1.1

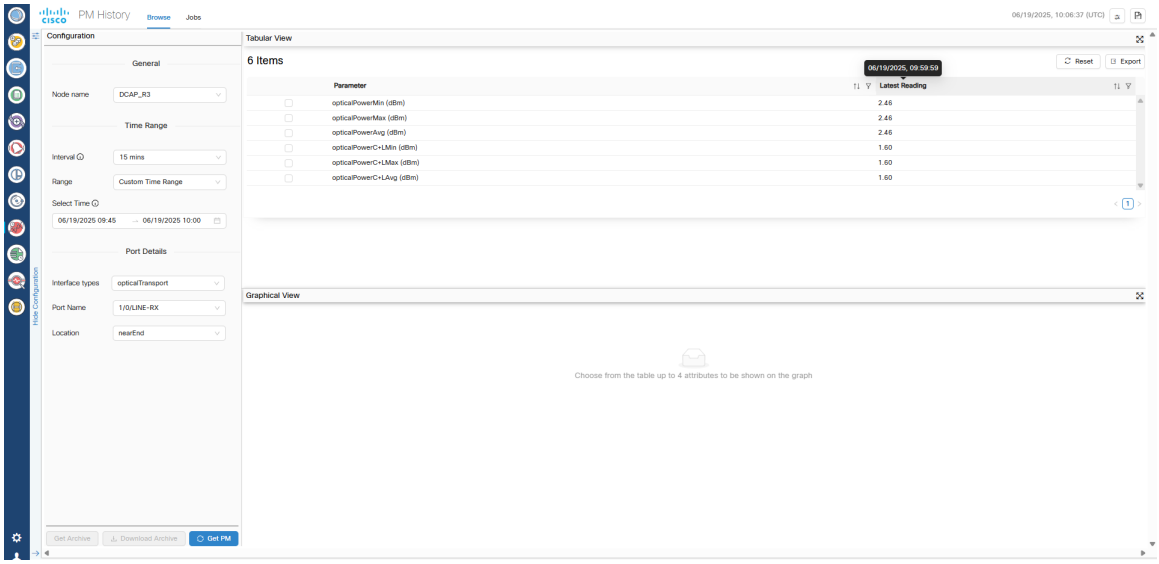


Figure 11: Nodes in Release 25.1.2

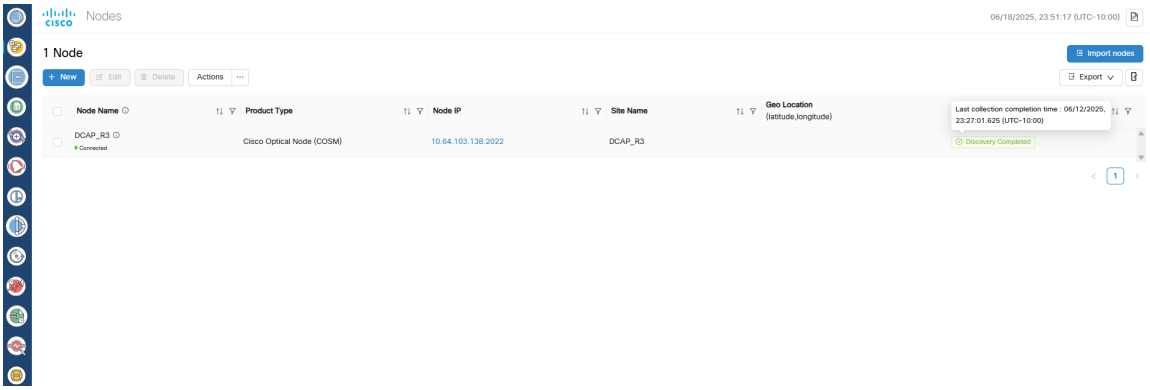
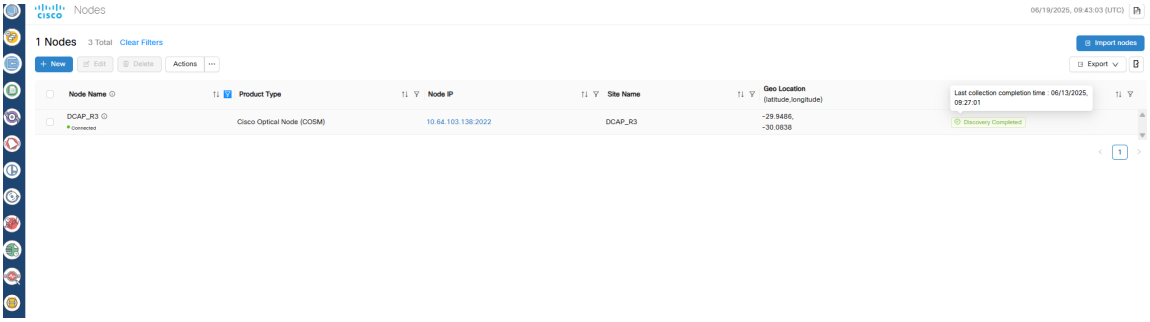


Figure 12: Nodes in Release 25.1.1



Revert to a Previous Version of Cisco Optical Network Controller

This section describes how to revert to the previous version of Cisco Optical Network Controller after you have installed Cisco Optical Network Controller, for both geo-redundant and standalone deployments. This is a manual process—Automatic rollback is not supported. You cannot perform a revert from within Cisco Optical Network Controller.

Restriction

- Cisco Optical Network Controller does not support downgrading to an older release. To go back to an older version, take a database backup using the SWIMU application and install the older version using the ova file for the release. After installation, restore the database.
- You can only revert to a previous version if you have created a copy of the target Cisco Optical Network Controller database before upgrading Cisco Optical Network Controller, as described in Backup and Restore Database.

Procedure

Step 1 For standalone deployments:

a) Reinstall the previous version of Cisco Optical Network Controller—The version from which you did the backup. See Install Cisco Optical Network Controller Using VMware vSphere, on page 1.
b) Follow the procedure to perform database restore from a backup. See Backup and Restore Database.

Step 2 For geo-redundant deployments:

a) Reinstall the previous version of Cisco Optical Network Controller—The version from which you did the backup. See Install and Deploy Geo Redundant Cisco Optical Network Controller.
b) Follow the procedure to perform database restore from a backup. See Backup and Restore Database.