

Install Cisco Optical Network Controller Using VMware vSphere

- Installation Requirements, on page 1
- SSH Key Generation, on page 4
- Install Cisco Optical Network Controller Using VMware vSphere, on page 5
- Service Pack Upgrade for Cisco Optical Network Controller, on page 19
- Revert to a Previous Version of Cisco Optical Network Controller, on page 22
- Install a Cisco Optical Network Controller service pack, on page 22

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.

  ESXi hosts use a self-signed certificate by default. Accepting the certificate allows you to continue with template customization, VM deployment, and login during the Cisco Optical Network Controller installation process.



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

The minimum hardware requirement for Cisco Optical Network Controller installation is given in this table.

Table 1: Minimum Hardware Requirements

Sizing	CPU	Memory	Solid State Drive (SSD)
Extra Small (XS)	16 vCPU	64 GB	2 TB
Small (S)	32 vCPU	128 GB	4 TB
Medium (M)	48 vCPU	256 GB	10 TB

Storage: SSDs to meet the disk write latency requirement of ≤ 100 ms.



Attention Cisco Optical Network Controller supports only SSDs for storage.



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 one 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 one 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 one 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-client: Enables client-facing communication with the etcd service. External clients, including the Kubernetes API server and *etcdctl*, connect to *etcd* using this port to read, write, and manage the key-value store data. Port 2379 typically requires client certificate authentication to ensure secure access.
	TCP 2380	etcd-server: Enables server-to-server (peer) communication within the etcd cluster. *etcd* instances use this port to communicate with each other, maintaining consensus through the Raft algorithm and replicating data across all cluster members.
	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.

Run the **ssh-keygen -t ed25519** command to generate the ed25519 key.

This example shows how to generate a ed25519 key.

```
root@conc-1:~# ssh-keygen -t ed25519
```

Install Cisco Optical Network Controller Using VMware vSphere

```
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      |
|     =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.

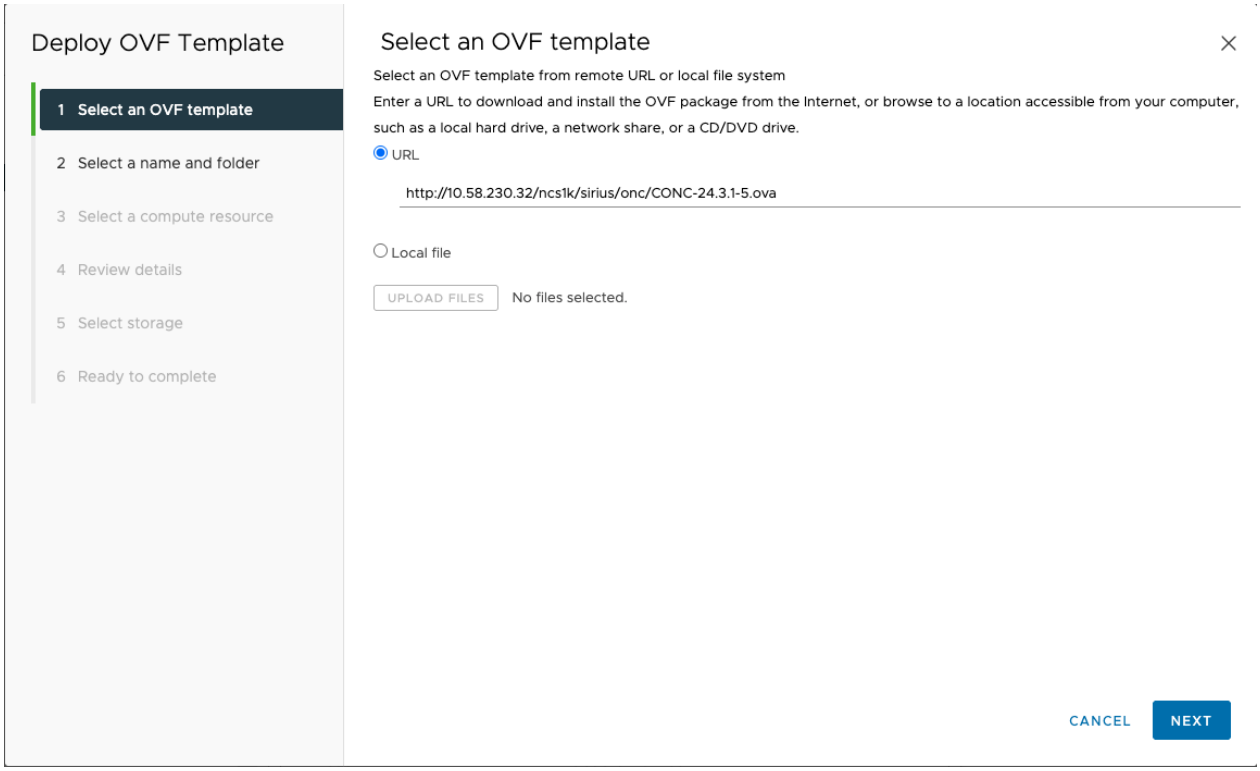
Procedure

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

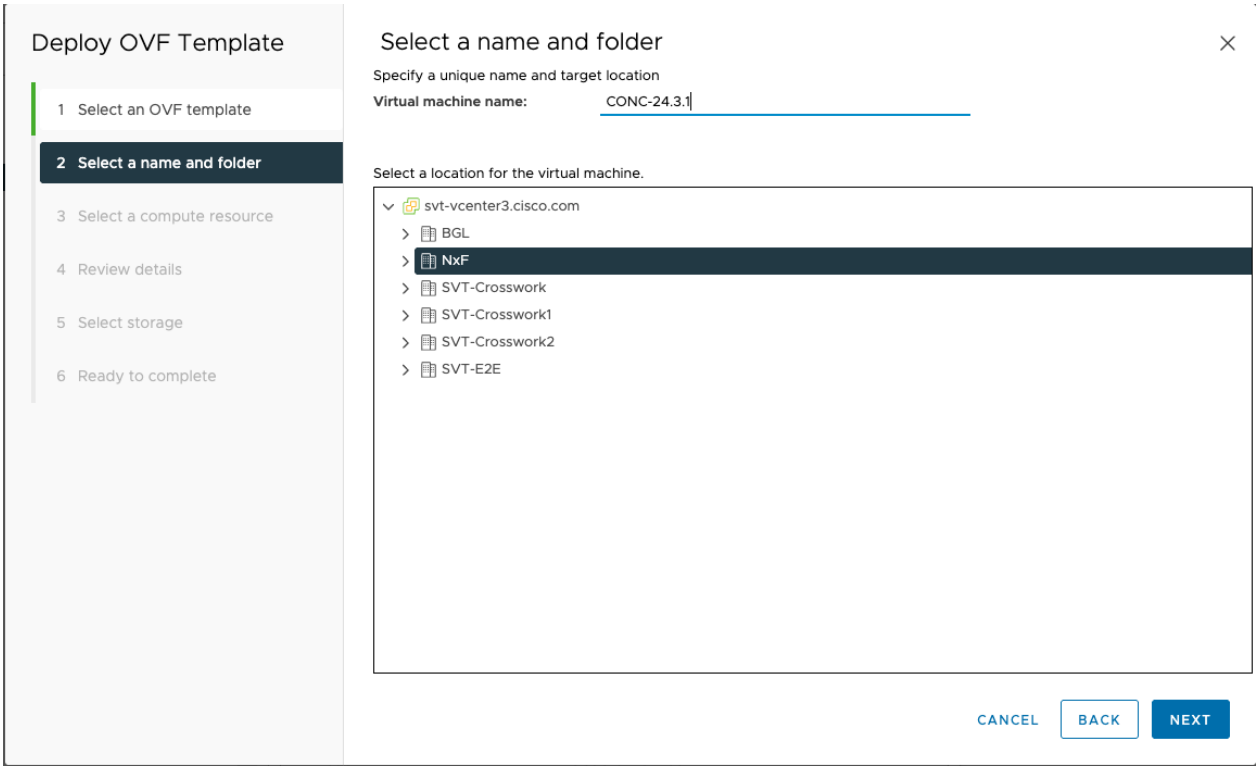
Figure 1: Select an OVF Template



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.**

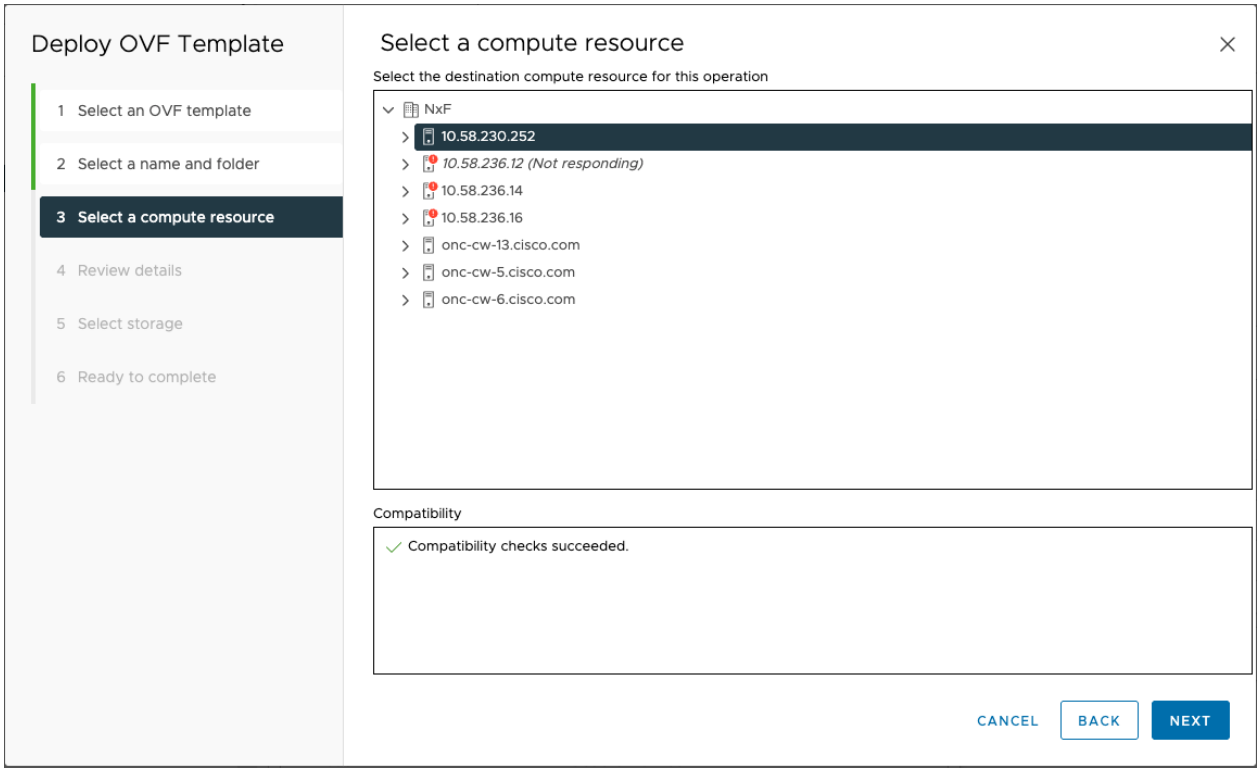
Install Cisco Optical Network Controller Using VMware vSphere

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.**

Figure 3: Select a Compute Resource

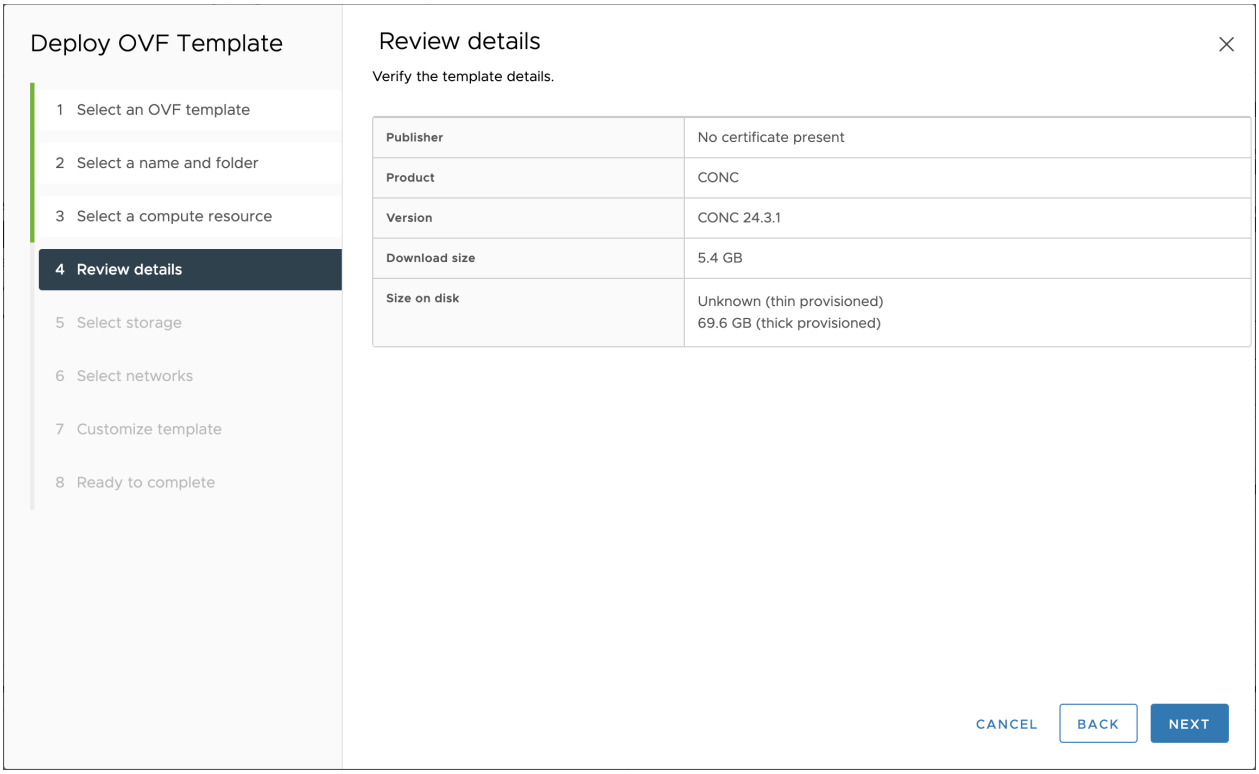


Note
While selecting the compute resource the compatibility check proceeds till it completes successfully.

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



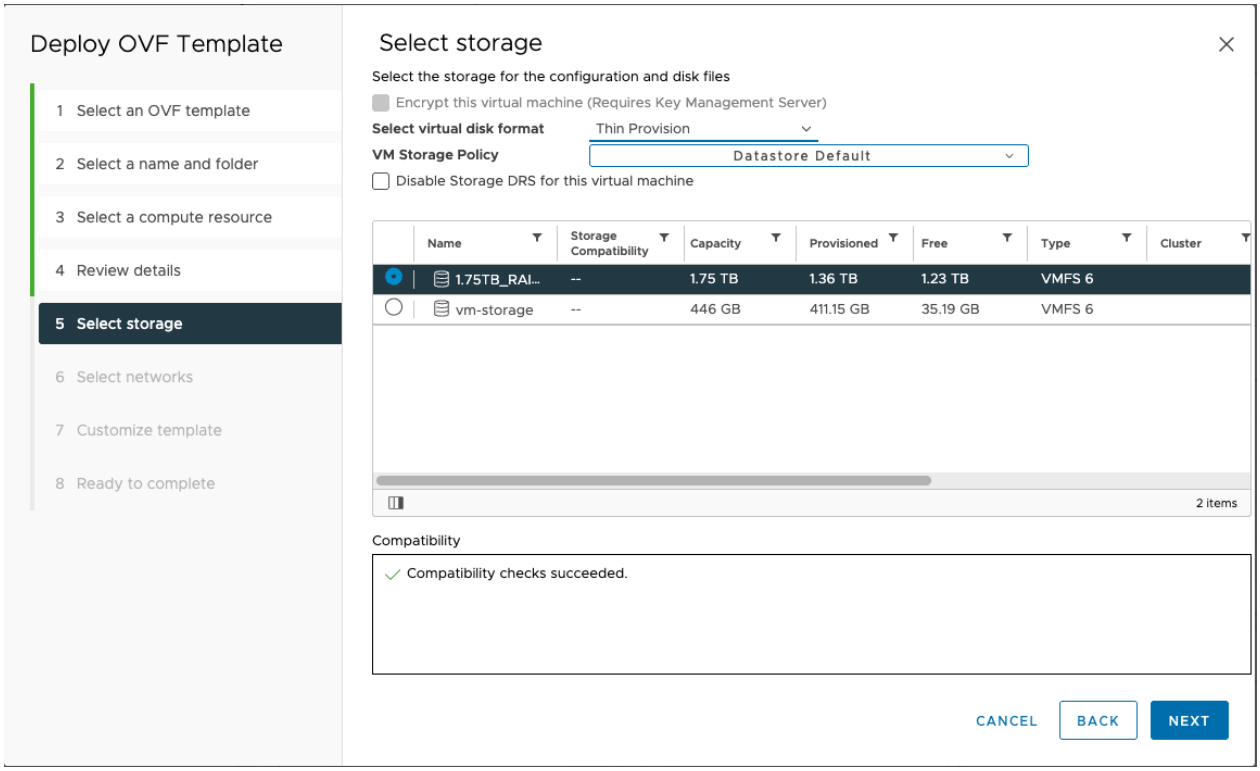
Step 6 In the *Select storage* screen, select the virtual disk format based on provision type requirement.

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

a) Set *VM Storage Policy* as *Datastore Default*
b) Click **Next**.
c) Select the **virtual disk format** as *Thin Provision* to allocate space as storage is required or *Thick Provision* to allocate the entire space.

Install Cisco Optical Network Controller Using VMware vSphere

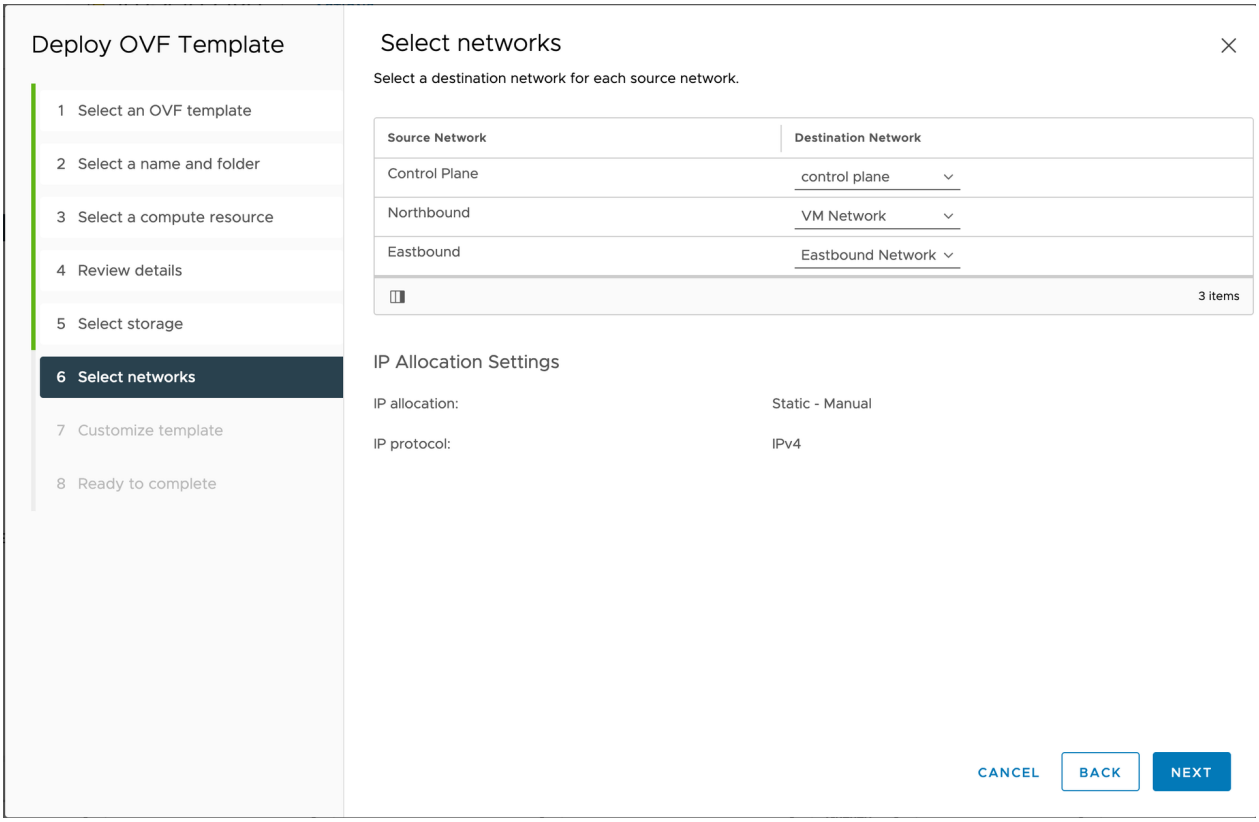
Figure 5: Select Storage



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

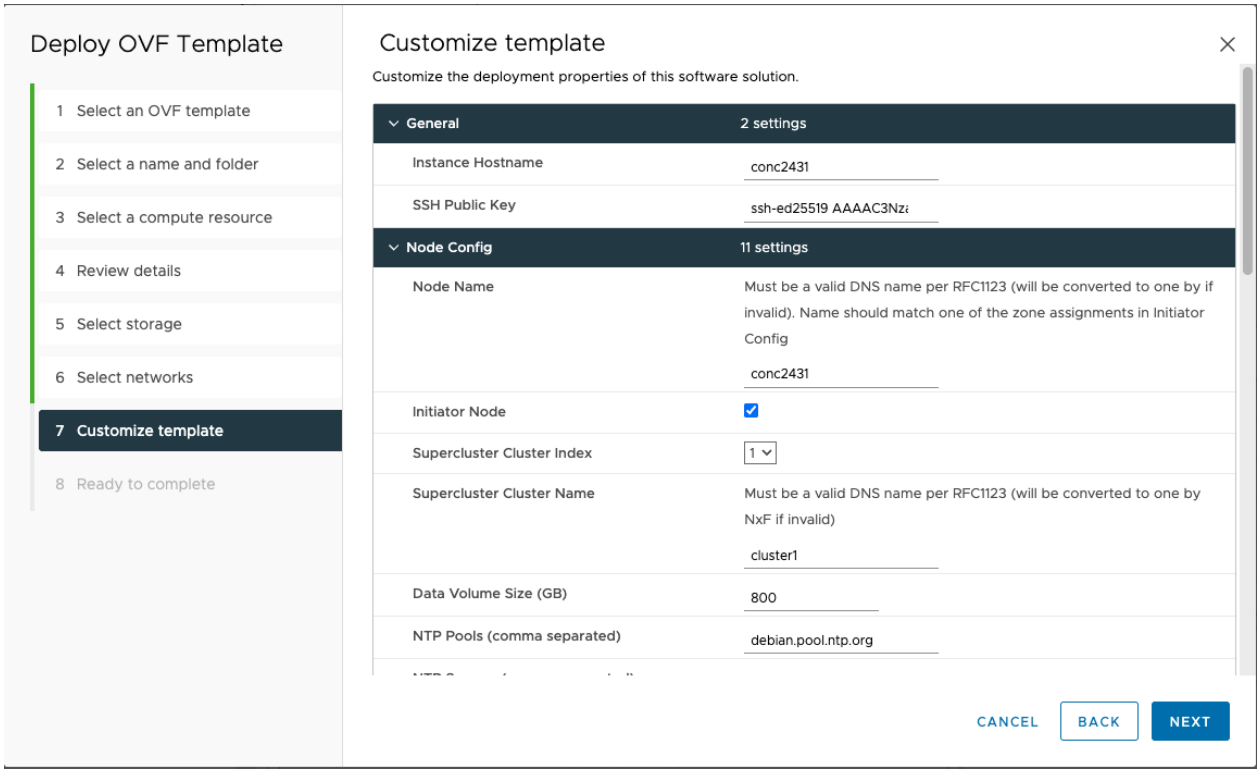
Figure 6: Select Networks

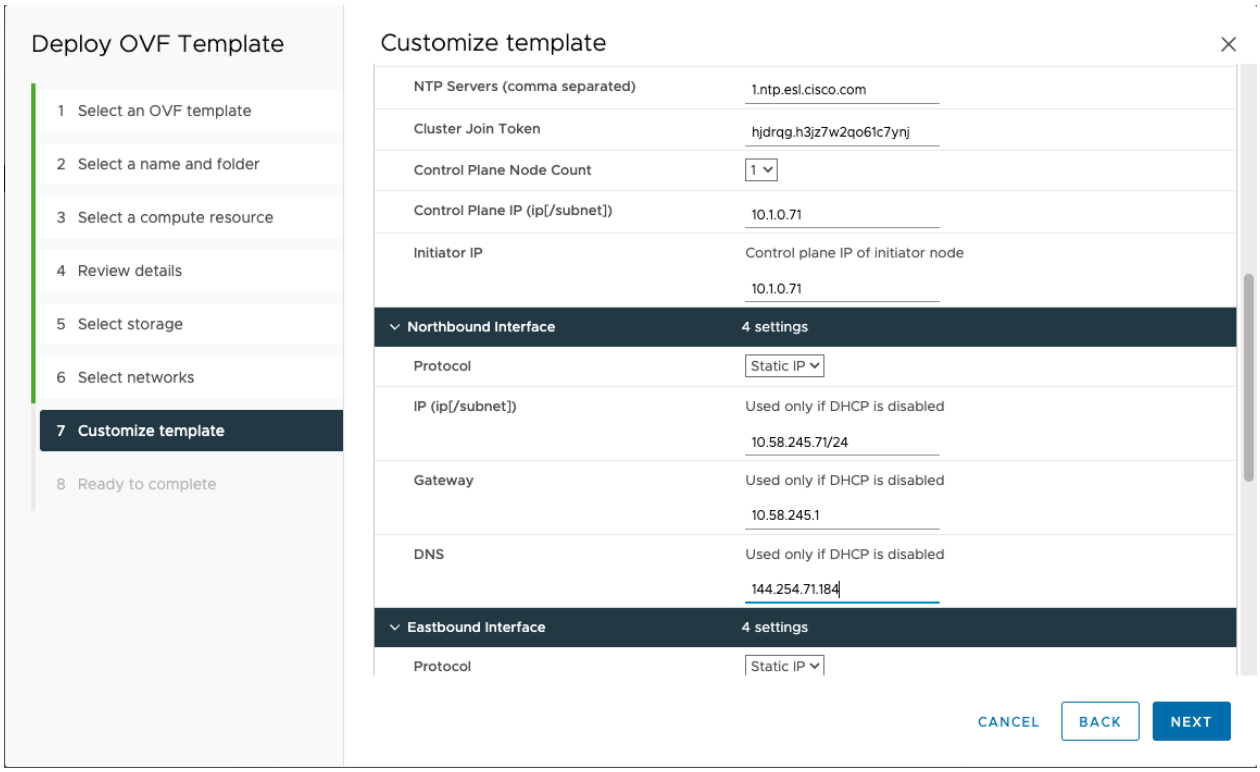


Step 8 In the **Customize template** screen, set the values using the #unique_3 unique_3_Connect_42_CustomizeTemplate table as a guideline for deployment.

Install Cisco Optical Network Controller Using VMware vSphere

Figure 7: Customize Template





Install Cisco Optical Network Controller Using VMware vSphere

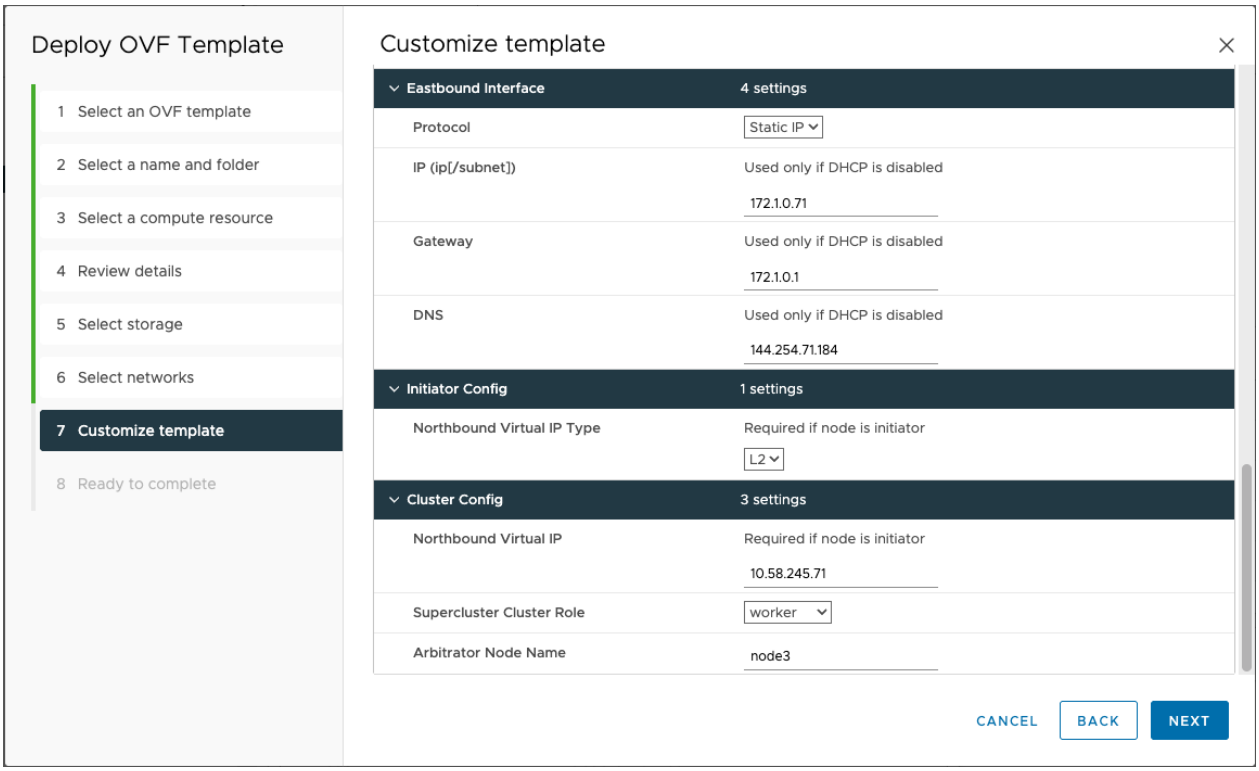


Table 4: Customize Template

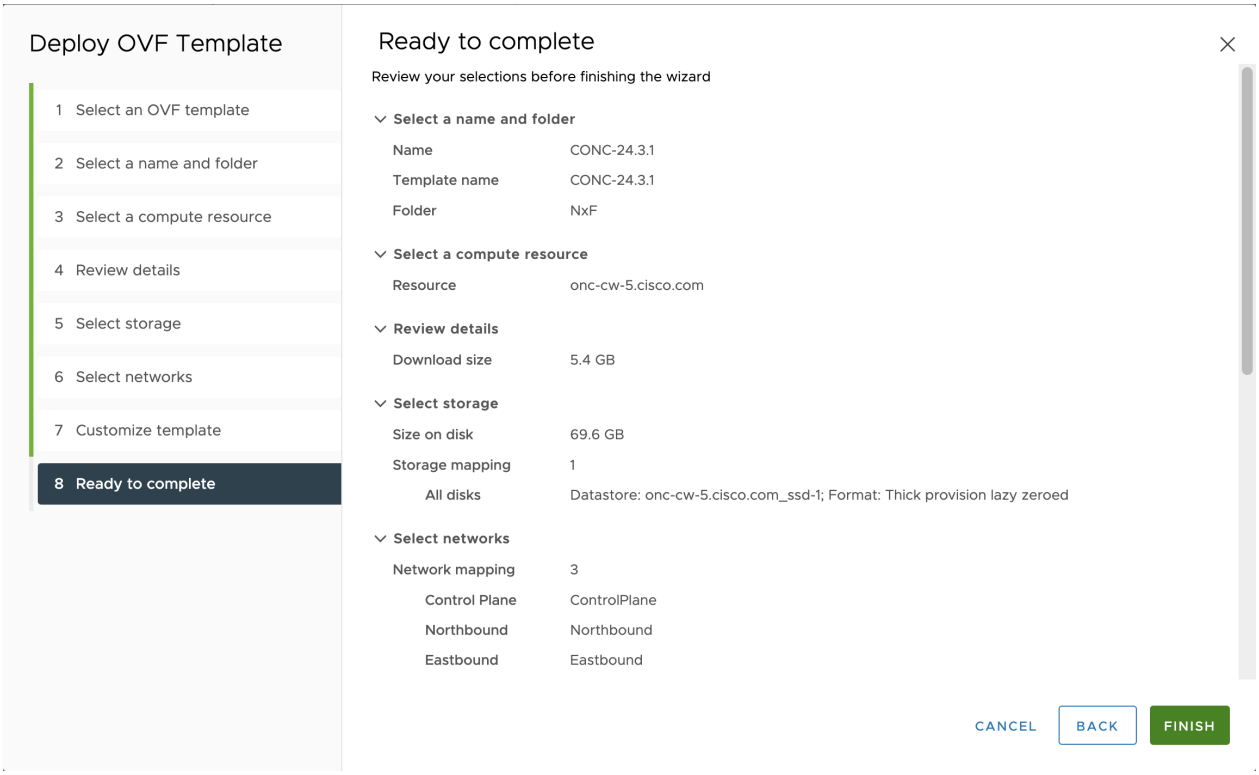
Key	Values
Instance Hostname	*<instance-name>*
SSH Public Key	*<ssh-public-key>*. Used for SSH access that allows you to connect to the instances securely without the need to manage credentials for multiple instances. SSH public key must be a ed25519 key.
Node Name	node1 Must be a valid DNS name per RFC1123.1.2.4 • Contain at most 63 characters. • Contain only lowercase alphanumeric characters or '-'.3 • Start with an alphanumeric character. • End with an alphanumeric character. • Node Name should be the same as instance name.
Initiator Node	Select the Checkbox
Supercluster Cluster Index	1 If you want to add your Cisco Optical Network Controller instance to a GeoHA 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 GeoHA SuperCluster in the future, use unique Super Cluster Names for each instance.
Data Volume Size (GB)	Configure data volume according to the VM profile. 800 GB and 1.5 TB for XS and S profiles respectively.
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	Can be left with the default value
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
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
Protocol	Static IP
IP (ip[/subnet]) - if not using DHCP	< IP for the Instance> Eastbound Network Can be a private IP **Warning** Do not include subnet when you enter this IP address.
Gateway - if not using DHCP	<Gateway IP for the Network> Eastbound Network
DNS	DNS Server IP
Northbound Virtual IP Type	L2
Northbound Virtual IP	Same as Northbound IP
Supercluster Cluster Role	worker
Arbitrator Node Name	node3

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.

Install Cisco Optical Network Controller Using VMware vSphere

Figure 8: Ready to Complete



Step 10 After creating the VM, power it on and verify that the IP addresses appear in vSphere.

Step 11 Connect to the VM using the pem key generated earlier.

Attention

- For more details on pem key, see *SSH Key Generation*.
- Use the private key that is generated along with the public key during customizing the public key options.
- 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 12 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, use the username `admin` to log in to the Web UI. Only the password must be configured. To access the device through SSH, use the username `nxf`.

Step 13 Set read permissions on the *.pem* file.

```
root@conc-1:~#chmod 400 <file-name-of-your-key>.pem
```

Step 14 **SSH to the node** and execute the following CLI command.

```
root@conc-1:~# 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 15 After you SSH into the node, use the sedo system status command to check the status of all the pods.

```
root@conc-1:~# sedo system status
```

System Status (Fri, 20 Sep 2024 08:21:27 UTC)

OWNER	NAME	NODE	STATUS	RESTARTS	STARTED
onc	monitoring	node1	Running	0	3 hours ago
onc	onc-alarm-service	node1	Running	0	3 hours ago
onc	onc-apps-ui-service	node1	Running	0	3 hours ago
onc	onc-circuit-service	node1	Running	0	3 hours ago
onc	onc-collector-service	node1	Running	0	3 hours ago
onc	onc-config-service	node1	Running	0	3 hours ago
onc	onc-devicemanager-service	node1	Running	0	3 hours ago
onc	onc-inventory-service	node1	Running	0	3 hours ago
onc	onc-nbi-service	node1	Running	0	3 hours ago
onc	onc-netconfcollector-service	node1	Running	0	3 hours ago
onc	onc-osapi-gw-service	node1	Running	0	3 hours ago
onc	onc-pce-service	node1	Running	0	3 hours ago
onc	onc-pm-service	node1	Running	0	3 hours ago
onc	onc-pmcollector-service	node1	Running	0	3 hours ago
onc	onc-topology-service	node1	Running	0	3 hours ago
onc	onc-torch-service	node1	Running	0	3 hours ago
system	authenticator	node1	Running	0	12 hours ago
system	controller	node1	Running	0	12 hours ago
system	flannel	node1	Running	0	12 hours ago
system	ingress-proxy	node1	Running	0	12 hours ago
system	kafka	node1	Running	0	12 hours ago
system	loki	node1	Running	0	12 hours ago
system	metrics	node1	Running	0	12 hours ago
system	minio	node1	Running	0	12 hours ago
system	postgres	node1	Running	0	12 hours ago
system	promtail-cltmk	node1	Running	0	12 hours ago
system	vip-add	node1	Running	0	12 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 16 (Optional) Change the password policy settings using the **sedo security password-policy set** command.

```
root@conc-1:~# sedo security password-policy set --expiration-days <number> --reuse-limit <number>
 --min-complexity-score <number>
```

Table 5: Password policy parameters

Parameter	Description
expiration-days	Default password expiration used when creating new users, in days. Default: 180 days

Parameter	Description
min-complexity-score	Minimum password complexity score required. Default: 3
reuse-limit	Number of historical passwords retained and blocked from reuse when changing a password. Default: 12

Step 17 You can check the current version using the **sedo version** command.

```
root@conc-1:~# 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 |
└──────────────────────────────────────────────────────────────────────────┴──────────────┘
```

Step 18 SSH to the node and set the initial UI password for the admin user.

```
root@conc-1:~# 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:

```
root@conc-1:~# sedo security password-policy set --expiration-days <number> --reuse-limit <number>
 --min-complexity-score <number>
```

Step 19 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 20 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.

Service Pack Upgrade for Cisco Optical Network Controller

You can install service pack upgrades when Cisco releases upgrades to get additional functionality or bug fixes. This topic describes how to install a Service Pack Upgrade.

Before you begin

Download the Service Pack from the Cisco Software Download page. The service pack file is in .tar.gz format.

You must have an instance of the Cisco Optical Network Controller.

Procedure

Step 1 SSH into the Cisco Optical Network Controller instance.

Example:

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

Step 2 Copy the downloaded service pack file into the `/data` folder. You can use scp to copy the file into the Cisco Optical Network Controller instance from your local machine.

Note
You can download the SHA-256 checksum from the Cisco Software Download page and compare the checksum with the service pack file to verify the integrity of the file. Use the following command to get the checksum of the downloaded file.

```
openssl sha256 <service-pack-file>.tar.gz
```

Step 3 Run the `sedo service install` command to install the service pack.

Example:

```
sedo service install <service-pack-file>.tar.gz
```

Wait for the installation to complete.

Step 4 Run the `sedo service list-installed` command to verify the service pack version.

Example:

This sample output shows the 24.3.1-5-SP-1 as the installed service pack.

```
sedo service list-installed
```

INSTALLED BY	APPLY TIME	SERVICE PACK VERSION	PLATFORM VERSION	FILE NAME
sedo	2024-11-13T17:00:31Z	CONC-24.3.1-5	3.0-23+a71ee7572eee85ecad82d2841045d4a5b90425cd	/config/service-packs/000_CONC-24.3.1-5.tar.gz
sedo	2024-11-13T17:20:17Z	**CONC-24.3.1-5-SP-1**	3.0-23+a71ee7572eee85ecad82d2841045d4a5b90425cd	CONC-24.3.1-SP-1.tar.gz

Step 5 Run the `sedo version` command to verify the image version.

Example:

This sample output shows the 24.3.1-5-SP-1 as the installed service pack.

```
sedo version
```

Installer: CONC 24.3.1

NODE NAME	OS VERSION	KERNEL VERSION
vc39-es20-sa-86	NxFOS 3.0-408 (f2beddad9abeb84896cc13efcd9a87c48ccb5d0c)	6.1.0-23-amd64

IMAGE NAME	VERSION	NODES
docker.io/library/alpine	3.20.0	vc39-es20-sa-86
docker.io/rancher/local-path-provisioner	v0.0.27	vc39-es20-sa-86
quay.io/coreos/etcd	v3.5.12	vc39-es20-sa-86
registry.k8s.io/coredns/coredns	v1.11.1	vc39-es20-sa-86
registry.k8s.io/kube-apiserver	v1.30.2	vc39-es20-sa-86
registry.k8s.io/kube-controller-manager	v1.30.2	vc39-es20-sa-86
registry.k8s.io/kube-proxy	v1.30.2	vc39-es20-sa-86
registry.k8s.io/kube-scheduler	v1.30.2	vc39-es20-sa-86
registry.k8s.io/pause	3.9	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmservice	24.3.1-5	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service	24.3.1-5	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service	24.3.1-5-SP-1	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector-service	24.3.1-5	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service	24.3.1-5-SP-1	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service	24.3.1-5	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicemanager-service	24.3.1-5	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory-service	24.3.1-5	vc39-es20-sa-86
registry.nxf-system.svc:8443/cisco-onc-docker/dev/monitoring	release2431_latest	vc39-es20-sa-86

```
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-service              | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service | 24.3.1-5-SP-1     |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service      | 24.3.1-5-SP-1     |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service      | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/osapi-gw-service         | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pce_service              | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service               | 24.3.1-5-SP-1     |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service               | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pmcollector-service      | 24.3.1-5-SP-1     |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pmcollector-service      | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service         | 24.3.1-5-SP-1     |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service         | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/torch                    | 24.3.1-5          |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/authenticator                            | 3.0-348           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/bgp                                      | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/controller                               | 3.0-384           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/firewalld                                | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/flannel                                  | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/ingress-proxy                            | 3.0-370           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/iptables                                 | 3.0-370           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/kafka                                    | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/loki                                     | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/metrics-exporter                         | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/minio                                    | 3.0-365           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/service-proxy                            | 3.0-370           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/syslog-forwarder                         | 3.0-340           |
vc39-es20-sa-86 |
| registry.sedona.ciscolabs.com/nxf/timescale                                | 3.0-359           |
vc39-es20-sa-86 |
└────────────────────────────────────────────────────────────────────────────┴───────────────────┴──────────────┘
```

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 direct downgrades to older releases.
- To revert to a previous version, you must first create a database backup using the SWIMU application before upgrading. Then, install the desired older version using its OVA file, and finally, restore the database.
- Refer to the Backup and Restore Database documentation for detailed instructions.

Procedure

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.

Install a Cisco Optical Network Controller service pack

Install a service pack to update your Cisco Optical Network Controller with bug fixes and enhancements. Transfer the Service Pack file, install the service pack, and verify that the new image is active.

Apply service packs to keep the controller up to date. In GeoHA deployments, install the service pack only on the active node.

Before you begin

Download the *.tar.gz* file for your service pack from the Cisco Software Download page.

Follow these steps to install a Cisco Optical Network Controller Service Pack:

Procedure

Step 1 Use the **scp** command to copy the file to the */data* directory on the active node.

Example:

```
scp 25.1.2-MSMU-2.tar.gz -i <pem_file> nxf@<CONC_HOST_IP>:/data
```

Note

- You can download the SHA-256 checksum from the Cisco Software Download page and compare the checksum with the service pack file to verify the integrity of the file. Use the following command to get the checksum of the downloaded file.

  ```
  openssl sha256 <service-pack-file>.tar.gz
  ```

- Avoid copying it to other directories, such as */home/nxf*, as these locations may have restricted disk space, potentially leading to deployment failures or related issues.

Step 2 Use the **sedo supercluster status** command to identify the active Cisco Optical Network Controller instance.

Look for the rows labeled **Cluster Name** and **Current Active**.

Example:

This sample output shows the **Cluster Name** and **Current Active** as the active Cisco Optical Network Controller instance in bold.

```
concgha2-clb-vm1:~# sedo supercluster status
```

Supercluster Status	
Cluster ID	INVetOV3DZKTSR5kmTFrE1PmDj954yyoBO6F4GbjlM8
Cluster Name	**cluster2**
Cluster Role	worker
Peers	cluster1 (worker, ej60l6x1PZtRdmAj9sEd07Vk201duytRUaPttJnXwk8) cluster3 (arbitrator, lSK7K7xavBTjaNDou6mTVGKR15bRZeOPRmC6fwgX8)
Mode	Running
Current Active	**cluster2**
Previous Active	cluster1
Standby Clusters	cluster1
Last Switchover	2025-11-13 14:32:40.801 +0000 UTC
Last Failover	2025-11-14 10:22:02.158 +0000 UTC
Last Seen	controller-0.cluster2: 2025-11-20 10:28:26.17 +0000 UTC controller-0.cluster3: 2025-11-20 10:28:26.17 +0000 UTC controller-0.cluster1: 2025-11-20 10:28:26.165 +0000 UTC
Last Peer Error	
Server Error	
DB Replication	streaming
DB Lag	0 bytes

Step 3 Use the **sedo service install** command to install the Service Pack on the active node.

Example:

```
root@superman-c1-n1:/data# sedo service install 25.1.2-MSMU-2.tar.gz
Importing images...
```

The Cisco Optical Network Controller service is restarted with the new image. Images are automatically synced to the standby node, and services restart on standby.

Step 4 Use the **sedo system status -w** command to verify that all services are running.

In a GeoHA setup, verify the system status on both the active and standby virtual machines.

Example:

This sample output shows all the services as *Running* under the **STATUS** column.

```
concgha2-clb-vm1:~# sedo system status -w
```

System Status (Thu, 20 Nov 2025 09:55:35 UTC)

```
|
┌──────┬──────────────────────────────┬──────────────┬─────────┬──────────────────────┬──────────────┐
| OWNER | NAME                         | NODE         | STATUS  | RESTARTS             | STARTED
    |
├──────┼──────────────────────────────┼──────────────┼─────────┼──────────────────────┼──────────────┤
| onc   | monitoring                   | concgha2-clb-vm1 | Running | 0                    | 5 days
 ago  |
| onc   | onc-alarm-service            | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-apps-ui-service          | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-circuit-service          | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-collector-service        | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-config-service           | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-devicemanager-service    | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-inventory-service        | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-nbi-service              | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-netconfcollector-service | concgha2-clb-vm1 | Running | 0                    | 5 days
 ago  |
| onc   | onc-osapi-gw-service         | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-pce-service              | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-pm-service               | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-pmcollector-service      | concgha2-clb-vm1 | Running | 0                    | 5 days
 ago  |
| onc   | onc-topology-service         | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| onc   | onc-torch-service            | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| system | authenticator               | concgha2-clb-vm1 | Running | 0                    | 5 days
 ago  |
| system | bgp                         | concgha2-clb-vm1 | Running | 0                    | 5 days
 ago  |
| system | controller                  | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 2
weeks ago |
| system | flannel                     | concgha2-clb-vm1 | Running | 1 (Latest 5 days ago) | 2
weeks ago |
| system | ingress-proxy               | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 1 week
 ago  |
| system | kafka                       | concgha2-clb-vm1 | Running | 1 (Latest 5 days ago) | 2
weeks ago |
| system | loki                        | concgha2-clb-vm1 | Running | 4 (Latest 5 days ago) | 2
weeks ago |
| system | metrics                     | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 2
weeks ago |
| system | minio                       | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 2
weeks ago |
| system | postgres                    | concgha2-clb-vm1 | Running | 3 (Latest 5 days ago) | 2
weeks ago |
| system | promtail-vff8n              | concgha2-clb-vm1 | Running | 1 (Latest 5 days ago) | 2
weeks ago |
└──────┴──────────────────────────────┴──────────────┴─────────┴──────────────────────┴──────────────┘
```

Step 5 Use the **sedo version** command to verify the Service Pack image is installed on both active and standby nodes.

Example:

This sample output shows the *25.1.2-13-MSMU-2-5* as the installed service pack.

```
concgha2-clb-vm1:~# sedo version
┌──────────────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ Installer: 25.1.2
       │
├──────────────────┬──────────────────────────────────────────────────────────────────┬────────────────────────┤
│ NODE NAME        │ OS VERSION                                                       │ KERNEL VERSION
       │
├──────────────────┼──────────────────────────────────────────────────────────────────┼────────────────────────┤
│ concgha2-clb-vm1 │ NxFOS 3.2-580 (00d31aecf87d877b8638ea4d295189852b4164e9) │
6.1.0-35-cisco-cloud-amd64 │
└──────────────────┴──────────────────────────────────────────────────────────────────┴────────────────────────┘

┌──────────────────────────────────────────────────────────────────────────────┬──────────────────┬──────────────┐
│ IMAGE NAME                                                                   │ VERSION          │
 NODES            │
├──────────────────────────────────────────────────────────────────────────────┼──────────────────┼──────────────┤
│ docker.io/library/alpine                                                     │ 3.20.3           │
 concgha2-clb-vm1 │
│ docker.io/rancher/local-path-provisioner                                     │ v0.0.30          │
 concgha2-clb-vm1 │
│ quay.io/coreos/etcd                                                          │ v3.5.15          │
 concgha2-clb-vm1 │
│ registry.k8s.io/pause                                                        │ 3.10             │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmservice               │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/alarmservice               │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service            │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/circuit-service            │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector-service          │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/collector-service          │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service             │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/config-service             │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicemanager-service      │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/devicemanager-service      │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory-service          │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/inventory-service          │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/monitoring                 │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-service                │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/nbi-service                │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service   │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/netconfcollector-service   │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service        │ 25.1.2-13-MSMU-2-5 │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/onc-apps-ui-service        │ 25.1.2-13        │
 concgha2-clb-vm1 │
│ registry.nxf-system.svc:8443/cisco-onc-docker/dev/osapi-gw-service           │ 25.1.2-13-MSMU-2-5 │
```

```
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/osapi-gw-service         | 25.1.2-13          |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pce_service              | 25.1.2-13-MSMU-2-5 |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pce_service              | 25.1.2-13          |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service               | 25.1.2-13-MSMU-2-5 |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pm-service               | 25.1.2-13          |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/pmcollector-service      | 25.1.2-13          |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service         | 25.1.2-13          |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/topology-service         | 25.1.2-13-MSMU-2-5 |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/torch                    | 25.1.2-13          |
concgha2-clb-vm1 |
| registry.nxf-system.svc:8443/cisco-onc-docker/dev/torch                    | 25.1.2-13-MSMU-2-5 |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/authenticator                            | 3.2-509            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/bgp                                      | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/controller                               | 3.2-542            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/firewalld                                | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/flannel                                  | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/ingress-proxy                            | 3.2-510            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/iptables                                 | 3.2-510            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/kafka                                    | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/kubernetes                               | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/loki                                     | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/metrics-exporter                         | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/minio                                    | 3.2-507            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/service-proxy                            | 3.2-510            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/syslog-forwarder                         | 3.2-503            |
concgha2-clb-vm1 |
| registry.sedona.ciscolabs.com/nxf/timescale                                | 3.2-516            |
concgha2-clb-vm1 |
└----------------------------------------------------------------------------┴--------------------┴--------------------┘
```

All Cisco Optical Network Controller services display the installer service pack number in the **Version** column. For example *25.1.2-13*.

The Cisco Optical Network Controller Service Pack is installed, and all services are running the updated version.

What to do next

After installation, monitor the system logs. Verify that all services are operational.