Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(3a)

First Published: 2021-10-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

Installing the Cisco DCNM 1

System Requirements 1

Installing DCNM on Open Virtual Appliance 7

Downloading the Open Virtual Appliance File 7

Deploying the Open Virtual Appliance as an OVF Template 8

Installing the Cisco DCNM OVA in Standalone Mode 11

Installing the Cisco DCNM OVA in Native HA mode 16

Installing DCNM on ISO Virtual Appliance 23

Downloading the ISO Virtual Appliance File 24

Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal) 24

Installing the DCNM ISO Virtual Appliance on KVM 31

Installing the DCNM ISO Virtual Appliance on Windows Hyper-V 32

Creating Virtual Switches 32

Creating Virtual Machines 34

Installing DCNM ISO Virtual Appliance 38

Installing Cisco DCNM ISO in Standalone Mode 41

Installing the Cisco DCNM ISO in Native HA mode 46

Convert Standalone Setup to Native-HA Setup 53

Installing Cisco DCNM Compute Node 58

CHAPTER 2

Deployment Best Practices 63

Best Practices for Deploying Cisco DCNM and Computes 63

Guidelines to Use the Best Practices 64

Deployments for Redundancy in Cisco DCNM 64

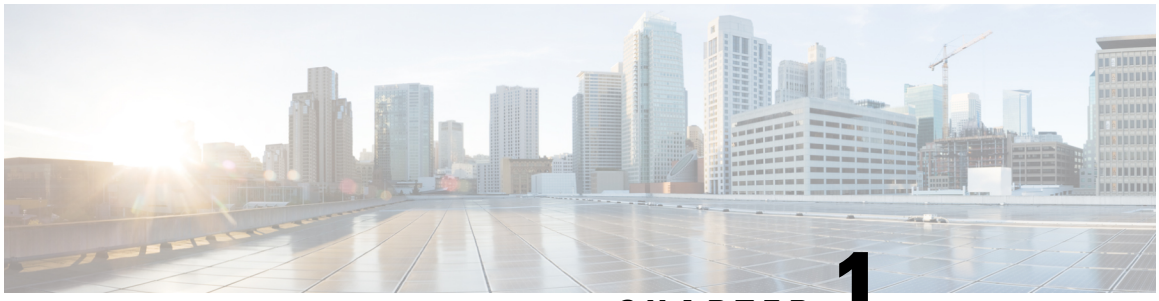
IP Address Configurations in Cisco DCNM 65
Scenario 1: All 3 Ethernet Interfaces are in Different Subnets 65
Scenario 2: eth2 Interface in Different Subnet 68
Physical Connectivity of Cisco DCNM and Compute Nodes 70

CHAPTER 3 **Disaster Recovery (Backup and Restore) 75**
Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup 75
Backup and Restore Cisco DCNM and Application Data on Native HA setup 76
Recovering Cisco DCNM Single HA Node 77
Recovering admin Account 79
HA Disaster Avoidance using SRM 80
Backup and Restore Cisco DCNM on a Cluster Setup 82

CHAPTER 4 **Managing Utility Services After DCNM Deployment 85**
Editing Network Properties Post DCNM Installation 85
Modifying eth0 IP Address of DCNM Compute Cluster 86
Modifying eth2 and eth1 IP Addresses of DCNM Compute Cluster 88
Nexus Dashboard Properties Modifications 90
Changing the DCNM Server Password on Standalone Setup 91
Changing the DCNM Server Password on Native HA Setup 92
Changing the DCNM Database Password on Standalone Setup 93
Changing the DCNM Database Password on Native HA Setup 93
Convert Standalone Setup to Native-HA Setup 94
Utility Services Details 98
Network Management 98
Orchestration 99
Device Power On Auto Provisioning 99
Managing Applications and Utility Services 99
Verifying the Application and Utility Services Status after Deployment 100
Stopping, Starting, and Resetting Utility Services 101
Updating the SFTP Server Address for IPv6 102

CHAPTER 5 **Installing Software Maintenance Update for log4j2 Vulnerability 103**
Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment 103

Installing SMU on Cisco DCNM 11.5(3a) Standalone Deployment 103
Installing SMU on Cisco DCNM 11.5(3a) Native HA Deployment 105
Installing SMU on Cisco DCNM 11.5(3a) Compute Nodes 108
Sample Output of Commands to address Log4j vulnerability 110
Scanning for Log4j2 Vulnerabilities 121
Validating of SMU Installation 130



CHAPTER 1

Installing the Cisco DCNM

Supported Latency

The supported latency for Cisco DCNM LAN Fabric deployment is defined below:

- Between Native HA Primary and Secondary appliances, latency is 50ms.
- Between DCNM Native HA Primary appliance to Switches, latency is 50ms.
- Between DCNM Computes latency is 50ms.

This chapter contains the following sections:

If you are installing Cisco DCNM on SE, install the DCNM ISO Virtual Appliance (.iso) installer.

- System Requirements, on page 1
- Installing DCNM on Open Virtual Appliance, on page 7
- Installing DCNM on ISO Virtual Appliance, on page 23
- Convert Standalone Setup to Native-HA Setup, on page 53
- Installing Cisco DCNM Compute Node, on page 58

System Requirements

This section describes the various system requirements for proper functioning of your Cisco DCNM Release 11.5(3a).

Note We recommend that you do not upgrade any underlying third-party software separately. All the necessary software components will be updated during the inline upgrade procedure. Upgrading the components outside of DCNM upgrade causes performance issues.

- Java Requirements, on page 2
- Server Requirements, on page 2
- Supported Latency
- Database Requirements, on page 2
- Hypervisors, on page 2

- Supported Hypervisors, on page 3
- Cisco DCNM LAN Fabric Deployment Without Network Insights (NI)
- VMware Snapshot Support for Cisco DCNM, on page 4
- Supported Web Browsers, on page 6
- Other Supported Software, on page 7

Note If you are deploying Network Insights applications on the Cisco DCNM Compute cluster, refer to the app-specific release notes for additional CPU or memory requirements for Computes.

Java Requirements

The Cisco DCNM server is distributed with JDK 11.0.8 into the following directory:

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM Release 11.5(3a), supports the Cisco DCNM server on these 64-bit operating systems:

- **LAN Fabric Deployments:**
  - Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.8
  - ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.8

Supported Latency

The supported latency for Cisco DCNM LAN Fabric deployment is defined below:

- Between Native HA Primary and Secondary appliances, latency is 50ms.
- Between DCNM Native HA Primary appliance to Switches, latency is 50ms.
- Between DCNM Computes latency is 50ms.

Database Requirements

Cisco DCNM Release 11.5(3a) supports the following databases:

- PostgreSQL 10.15 - For OVA/ISO deployments

Note The ISO and OVA installations support only the embedded PostgreSQL database.

Hypervisors

Cisco DCNM supports the ISO installation on a bare-metal server, no hypervisor, on the following server platforms:

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count [1] [2]
Cisco UCS C240M4	UCSC-C240-M4S	32G / 500G 16 vCPUs
Cisco UCS C240M4	UCSC-C240-M4L	32G / 500G 16 vCPUs
Cisco UCS C240 M5S	UCSC-C240-M5SX	32G / 500G 16 vCPUs
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G 16 vCPUs

1 Install the Cisco DCNM OVA Compute node with 16 vCPUs, 64G RAM, and 500GB hard disk.
2 If you are deploying Network Insights applications on the Cisco DCNM Compute cluster, refer to the app-specific Release Notes for additional CPU/memory requirements for the Computes.

Note Cisco DCNM can work on an alternative computing hardware with appropriate specifications, despite Cisco is only testing on Cisco UCS.

Supported Hypervisors

You can use the Cisco DCNM Server on the following hypervisors:

Hypervisor supported	Data Center Manager server application	Supported deployments
ESXi 7.0	vCenter 7.0	All
ESXi 6.7 P01	vCenter 6.7 P01	All
ESXi 6.5	vCenter 6.5	All
ESXi 6.0	vCenter 6.0	All
RedHat 7.6 KVM with QEMU version 1.5.3	Virtual Machine Manager (comes with RHEL 7.6)	LAN Fabric
Hyper-V on Windows Server 2019	Hyper-V Manager (comes with Windows Server 2019)	LAN Fabric This is supported with Native HA mode, and not in Cluster mode.

Server Resource (CPU/Memory) Requirements

Note If you install Cisco DCNM on a virtual machine, you must reserve resources equal to the server resource requirements to ensure a baseline with the physical machines.

Table 1: System Requirements for Cisco DCNM LAN Fabric Deployment

Deployment Type	Small (Lab or POC)	Large (Production)	Compute for 81-350 switches scale (without Network Insights)	Compute for up to 80 switches (with Network Insights)
OVA/ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 64 GB DISK: 500 GB	CPU: 32 vCPUs RAM: 64 GB DISK: 500 GB

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

Allocate sufficient disk space to the root partition to complete DCNM installation and for stable continuous operation of the DCNM applications. Refer to the applications' User guides for disk space requirements. You can mount another disk where the `/tmp` directory can be mounted during the installation or upgrade. You can also add additional disk space and the disk file system using **appmgr system scan-disks-and-extend-fs** command.

Cisco DCNM LAN Fabric Deployment Without Network Insights (NI)

Table 2: Upto 80 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	NA	—	—	—	—

Table 3: 81–350 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
DCNM on Applications Service Engine (SE)	ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	OVA/ISO	16 vCPUs	64G	500G HDD	3xNIC

VMware Snapshot Support for Cisco DCNM

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off. The following table shows snapshot support for your deployment.

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 P01	7.0
VMware vCenter Server	6.0	6.5	6.7	6.7 P01	7.0

Note You need VMware vCenter server to deploy Cisco DCNM OVA Installer. However, to install DCNM directly on VMware ESXi without vCenter, you can choose DCNM ISO deployment. Ensure that correct CPU, Memory, Disk, and NIC resources are allocated to that VM.

To take a snapshot on the VM, perform the following steps:

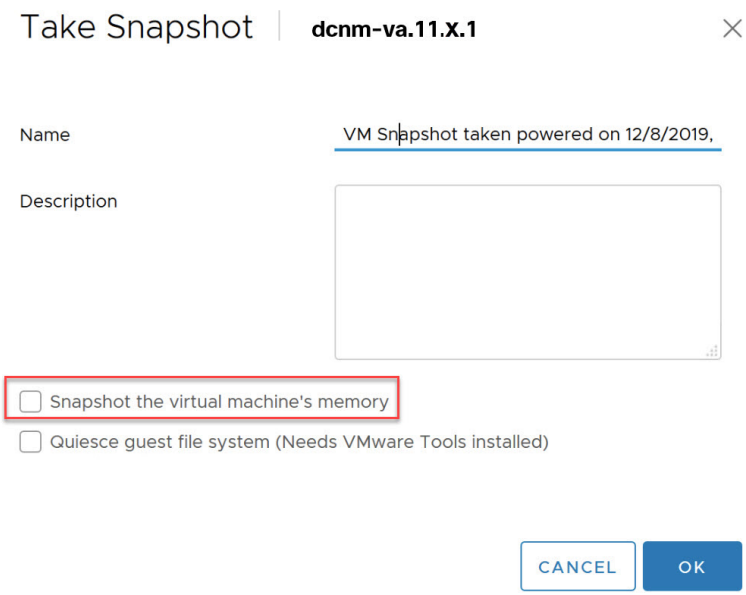
1. Right-click the virtual machine the inventory and select **Snapshots > Take Snapshot**.
2. In the **Take Snapshot** dialog box, enter a name and description for the snapshot.
3. Click **OK** to save the snapshot.

The following snapshots are available for VMs.

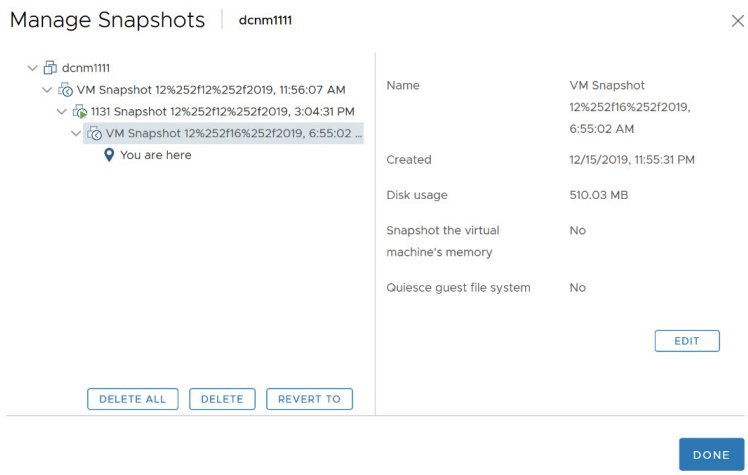
- When VM is powered off.
- When VM is powered on, and active.

Note Cisco DCNM supports snapshots when VM is either powered on or powered off. DCNM doesn't support snapshots when the Virtual Machine memory option is selected.

Ensure that **Snapshot the Virtual Machine's memory** check box must not be selected, as shown in the following figure. However, it is grayed out when the VM is powered off.



You can restore VM to the state in a Snapshot.



Right-click on the Virtual Machine and select **Manage Snapshot**. Select the snapshot to restore, and click **Done**.

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome version: 86.0.4240.198
- Mozilla Firefox version: 82.0.3 (64-bit)
- Microsoft Edge version: 86.0.622.63

Other Supported Software

The following table lists the other software that is supported by Cisco DCNM Release 11.5(1).

Table 4: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • ISE version 3.0 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client Encryption: HTTPS with TLS 1, 1.1 and 1.2 • TLS 1.3
OVA\ISO Installers	CentOS 7.8/Linux Kernel 3.10.x

Also, Cisco DCNM supports call-home events, fabric change events, and events that are forwarded by traps and email.

Installing DCNM on Open Virtual Appliance

This chapter contains the following sections:

Downloading the Open Virtual Appliance File

The first step to install the Open Virtual Appliance is to download the `dcnm.ova` file. Point to that `dcnm.ova` file on your computer when deploying the OVF template.

Note If you plan to use HA application functions, you must deploy the `dcnm.ova` file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/.

Step 2 Locate the DCNM Open Virtual Appliance Installer and click the **Download** icon.

Step 3 Save the `dcnm.ova` file to your directory that is easy to find when you start to deploy the OVF template.

Deploying the Open Virtual Appliance as an OVF Template

After you download the Open Virtual Appliance file, you must deploy the OVF template from the vSphere Client application or the vCenter Server.

Note Deploy two OVAs for the HA setup.

Procedure

Step 1 Open the vCenter Server application and connect to the vCenter Server with your vCenter user credentials.

Note ESXi host must be added to the vCenter Server application.

Depending on the version of the VMware vsphere web HTML5 interface may not work properly when deploying Huge or Compute OVA, as it does not allow users to specify extra disk size. Therefore, we recommend that you use Flex interface for deploying VMs.

If you're deploying OVF template using the ESXi 6.7, the installation fails if you use Internet Explorer browser with HTML5. Ensure that you one of the following options to successfully deploy OVF template with ESXi and 6.7:

- Mozilla Firefox browser, with HTML 5 support

  Use flex interface if HTML 5 is not supported
- Mozilla Firefox browser, with flex\flash support
- Google Chrome browser, with HTML 5 support

  Use flex interface if HTML 5 is not supported

Step 2 Navigate to **Home > Inventory > Hosts and Clusters** and choose the host on which the OVF template is deployed.

Step 3 On the correct Host, right-click and select **Deploy OVF Template**.

You can also choose **Actions > Deploy OVF Template.**

Deploy OVF Template Wizard opens.

Step 4 On the Select template screen, navigate to the location where you have downloaded the OVA image.

You can choose the OVA file by one of the following methods:

- Select the **URL** radio button. Enter the path of the location of the image file.
- Select **Local File** radio button. Click **Browse**. Navigate to the directory where the image is stored. Click **OK**.

Click **Next**.

Step 5 Verify the OVA template details and click **Next**.

Step 6 On the End User License Agreement screen, read the license agreement.

Click **Accept** and click **Next**.

Step 7 On the Select name and location screen, enter the following information:

- In the Name field, enter an appropriate name for the OVF.

  Note Ensure that the VM name is unique within the Inventory.

- In the Browse tab, select **Datacenter** as the deployment location under the appropriate ESXi host.

Click **Next**.

Step 8 On the Select configuration screen, select the configuration from the drop-down list.

- Choose **Small** (Lab or POC) to configure the virtual machine with 8 vCPUs, 24GB RAM.

  Choose Small for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time.

- Choose **Large** (Production) to configure the virtual machine with 16 vCPUs, 32GB RAM.

  We recommend that you use a Large deployment configuration when you are managing more than 50 devices to leverage better RAM, heap memory, and CPUs. For setups that could grow, choose Large.

- Choose **Compute** to configure the virtual machine with 16 vCPUs, 64GB RAM.

  You must have DCNM deployed in Compute mode to use applications in your deployment.

- Choose **Huge** to configure the virtual machine with 32 vCPUs, 128GB RAM.

  This configuration is recommended if you deploy DCNM for SAN Management and use SAN Insights feature.

- Choose **ComputeHuge** to configure the virtual machine with 32vCPUs and 128GB RAM with 2TB disk.

  This configuration is recommended if you use Cisco Network Insights applications.

Click **Next**.

Step 9 On **Select a resource** screen, select the host on which you want to deploy the OVA template.

Click **Next**.

Step 10 On **Select storage** screen, based on the Datastore and Available space choose the disk format and the destination storage for the virtual machine file.

a) Select the virtual disk format from the drop-down list.

The available disk formats are:

Note Choose one of the thick provision types if you have enough storage capacity as required by the virtual appliance and want to set a specific allocation of space for the virtual disks.

- **Thick Provision Lazy Zeroed**: The space that is required for the virtual disk is allocated when the virtual disk is created. The data that remains on the physical device is not erased when the virtual disk is created but is zeroed out on demand later on first write from the virtual disk.
- **Thin Provision**: The disk space available is less than 100 GB. The initial disk consumption is 3GB and increases as the size of the database increases with the number of devices being managed.

- **Thick Provision Eager Zeroed**: The space that is required for the virtual disk is allocated when the virtual disk is created. Unlike the Lazy Zeroed option, the data that remains on the physical device is erased when the virtual disk is created.

  Note With 500G, the DCNM installation will appear to be stuck with option Thick Provision Eager Zeroed. However, it takes longer time to complete.

b) Select the VM storage policy from the drop-down list.

   By default, no policy is selected.

c) Check the **Show datastores from Storage DRS clusters** to view the clusters' datastores.

d) Select the destination storage for the virtual machine, available in the datastore.

Click **Next**.

Step 11 On the Select Networks screen, map the networks that are used in the OVF template to networks in your inventory.

- **dcnm-mgmt network**

  This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. Associate this network with the portgroup that corresponds to the subnet that is associated with the DCNM Management network.

- **enhanced-fabric-mgmt**

  This network provides enhanced fabric management of Nexus switches. You must associate this network with the port group that corresponds to management network of leaf and spine switches.

- **enhanced-fabric-inband**

  This network provides in-band connection to the fabric. You must associate this network with port group that corresponds to a fabric in-band connection.

  Note If you do not configure enhanced-fabric-inband network, Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

From the Destination Network drop-down list, choose to associate the network mapping with the port group that corresponds to the subnet that is associated with the corresponding network.

If you are deploying more than one DCNM Open Virtual Appliance for HA functionality, you must meet the following criteria:

- Both OVAs must have their management access (eth0), enhanced fabric management (eth1) and inband management (eth2) interfaces in the same subnet.
- Each OVA must have their eth0-eth1 and eth2 interfaces in different subnets.
- Both OVAs must be deployed with the same administrative password. This is to ensure that both OVAs are duplicates of each other for application access.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

Click **Next**.

Step 12 On **Customize template** screen, enter the Management Properties information.

Enter the **IP Address** (for the outside management address for DCNM), **Subnet Mask**, and **Default Gateway**.

Note During Native HA installation and upgrade, ensure that you provide appropriate Management Properties for both Active and Standby appliances.

Ensure that add valid values for the **Management Network** properties. Properties with invalid values will not be assigned. The VM will not power on until you enter valid values.

From Release 11.3(1), for Huge and Compute configurations, you can add extra disk space on the VM. You can add from 32GB up to 1.5TB of disk space. In the **Extra Disk Size** field, enter the extra disk size that will be created on the VM.

Click **Next**.

Step 13 On **Ready to Complete** screen, review the deployment settings.

Click **Back** to go to the previous screens and modify the configuration.

Click **Finish** to deploy the OVF template.

You can see the deployment status in the Recent Tasks area on the vSphere Client.

Note If this deployment is a part of the upgrade process, do not Power on the VM. Edit and provide the MAC address and power on the VM.

Step 14 After the installation is complete, right click on the installed VM and select **Power > Power On**.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

You can see the status in the Recent Tasks area.

Step 15 Navigate to the Summary tab and click **Settings** icon and select **Launch Web Console**.

A message indicating that the DCNM appliance is configuring appears on the screen.

```
************************************************************
Please point your web browser to
https://<IP-address>:<port-number>
to complete the application
************************************************************
```

Copy and paste the URL to the browser to complete the installation, using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. For more information, see Installing the Cisco DCNM OVA in Standalone Mode, on page 11 or Installing the Cisco DCNM OVA in Native HA mode, on page 16.

Installing the Cisco DCNM OVA in Standalone Mode

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears.

To complete the installation of Cisco DCNM from the web installer, perform the following procedure.

Procedure

Step 1 On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

Step 2 On the **Cisco DCNM Installer** tab, select **Fresh Installation – Standalone** radio button.

Click **Next**.

Step 3 On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

Step 4 On the **Administration** tab, enter information about passwords.

- In the **Administrator Password** field, enter the password that is used to connect to the applications in the Cisco DCNM.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Administrator Password** field.

- In the **Database Password** field, enter the password for the PostgreSQL database.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Database Password** field.

  Note If **Database Password** field is left blank, it shall consider the Administrator password as the PostgreSQL password.

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

Select the **Show passwords in clear text** check box to view the password that you have entered.

Click **Next**.

Step 5 On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  You can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

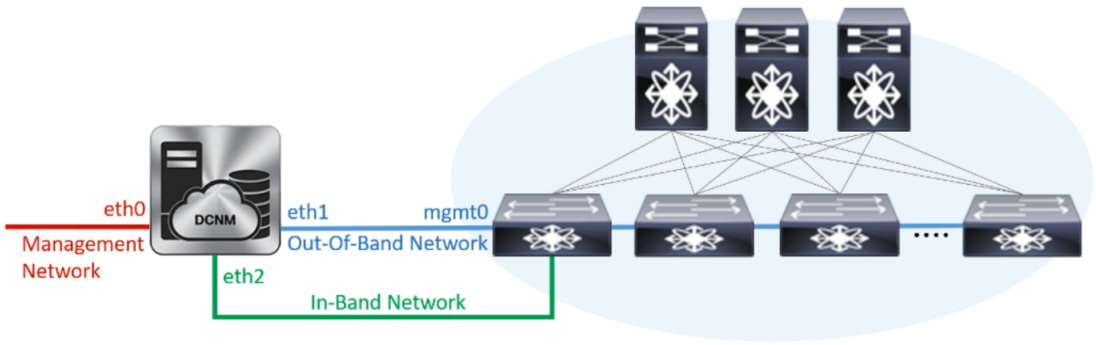
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

Step 6 On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 1: Cisco DCNM Management Network Interfaces



a) In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optional) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

b) In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

c) (Optional) In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

This field is mandatory if you have selected the Enable Cluster mode in Step Step 3, on page 12.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Click **Next**.

Step 7 On the **Applications** tab, configure the Device Connector and Internal Applications Services Network, and Cluster mode settings.

Note Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

a) (Optional) In the **Proxy Server** field, enter the IP address for the proxy server.

The proxy server must be of RFC1123-compliant name.

Note By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

b) In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

c) In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step Step 3, on page 12.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

- In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

  Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

- In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

  Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

Click **Next**.

Step 8 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

Note If you try to access the DCNM Web UI using the Management IP address while the installation is still in progress, an error message appears on the console.

```
************************************
*Preparing Appliance*

************************************
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Installing the Cisco DCNM OVA in Native HA mode

The native HA is supported on DCNM appliances with ISO or OVA installation only.

By default, an embedded PostgreSQL database engine with the Cisco DCNM. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following task to set up Native HA for DCNM.

Procedure

Step 1 Deploy two DCNM Virtual Appliances (either OVA or ISO).

For example, let us indicate them as **dcnm1** and **dcnm2**.

Step 2 Configure **dcnm1** as the Primary node. Paste the URL displayed on the Console tab of **dcnm1** and press **Enter** key.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the **Cisco DCNM Installer** tab, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Next**.

c) On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

- In the **Administrator Password** field, enter the password that is used to connect to the applications in the Cisco DCNM.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Administrator Password** field.

- In the **Database Password** field, enter the password for the PostgreSQL database.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Database Password** field.

  Note If the **Database Password** field is left blank, it shall consider the Administrator password as the PostgreSQL password.

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

Select the **Show passwords in clear text** check box to view the password that you have entered.

Click **Next**.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

  The value must be an IP or IPv6 address or RFC 1123 compliant name.

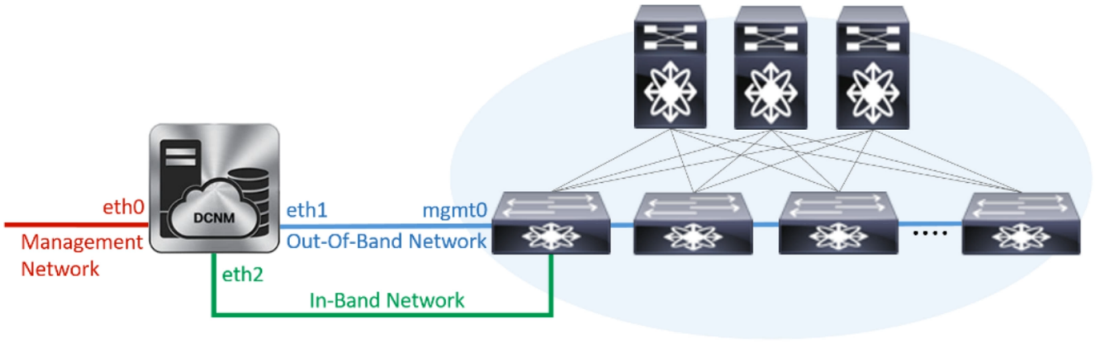
  From Release 11.3(1), you can configure more than one NTP server.

- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 2: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Out-of-band management provides a connection to the device management ports (Typically mgmt0).

   Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   This field is mandatory if you have selected the **Enable Cluster** mode..

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Click **Next**.

g) On the **Applications** tab, configure the Device Connector and Internal Applications Services Network.

Note Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

1. In the **Proxy Server** field, enter the IP address for the proxy server.

   The proxy server must be of RFC1123-compliant name.

   Note By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

   If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

2. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

   All the applications use the IP Address from this subnet. By default, the

   The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step 2.c, on page 16.

   Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

3. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

h) On the **HA Settings** tab, a confirmation message appears.

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

Click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A warning message appears stating that the setup is not complete until you install the Secondary node.

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on
this HA primary node.
However, the system will be ready to be used only after installation
of the secondary node has been completed.
Thank you.
```

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the **Install Mode** tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note All the passwords must be same as the passwords that you provided while configuring the Primary node.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

  The value must be an IP or IPv6 address or RFC 1123 compliant name.

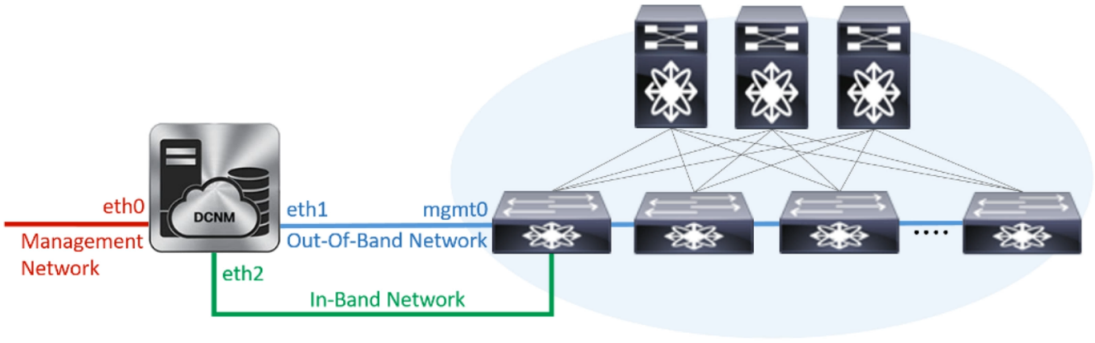
  From Release 11.3(1), you can configure more than one NTP server.

- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 3: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Ensure that the IP address belongs to the same Management Network configured on the Primary node.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

   Out-of-band management provides a connection to the device management ports (Typically mgmt0).

   Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

1. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.
2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.

- In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
- In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
- In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

  Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

  Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
- In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.
- In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

  Note This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.
- In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

  Note The configured IPv4 address must respond to the ICMP echo pings.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Installing DCNM on ISO Virtual Appliance

This chapter contains the following sections:

Note The screenshots in this section may change in your setup based on how you are booting the ISO; you will either see the blue (BIOS) screen or the black (UEFI) screen.

If you are installing Cisco DCNM on SE, install the DCNM ISO Virtual Appliance (.iso) installer.

Downloading the ISO Virtual Appliance File

The first step to installing the ISO Virtual Appliance is to download the `dcnm.iso` file. You must point to that dcnm.iso file on your computer when preparing the server for installing DCNM.

Note If you plan to use HA application functions, you must deploy the `dcnm.iso` file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/.

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Locate the DCNM ISO Virtual Appliance Installer and click the **Download** icon.

Step 4 Locate the DCNM VM templates at DCNM Virtual Appliance definition files for VMWare (.ovf) and KVM (domain XMLs) environment and click **Download**.

Step 5 Save the `dcnm.iso` file to your directory that will be easy to find when you being the installation.

What to do next

You can choose to install DCNM On KVM or Baremetal servers. Refer to Installing the DCNM ISO Virtual Appliance on KVM, on page 31 or Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal), on page 24 for more information.

Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal)

From Release 11.3(1), you can install Cisco DCNM ISO using an additional mode where the physical interfaces are bound together for a port channel or ethernet channel configured as a trunk with the management traffic, out-of-band traffic, and in-band traffic separated in different VLANs.

Ensure that the switch is configured correctly for bundled interface mode. The following shows a sample switch configuration for bundled interface mode:

```
vlan 100
vlan 101
vlan 102
interface port-channel1
  switchport
  switchport mode trunk
```

```
interface Ethernet101/1/1
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/2
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/3
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/4
  switchport mode trunk
  channel-group 1
  no shutdown
```

Perform the following tasks to install the DCNM ISO virtual appliance on UCS.

Procedure

Step 1 Launch Cisco Integrated Management Controller (CIMC).

Step 2 Click the **Launch KVM** button.

You can either launch Java-based KVM or HTML-based KVM.

Step 3 Click the URL displayed on the window to continue loading the KVM client application.

Step 4 On the Menu bar, click **Virtual Media > Activate Virtual Devices**.

Step 5 Click **Virtual Media** and choose one of the following mediums to browse and upload DCNM ISO images from the following:

- Map CD/DVD
- Map Removable Disk
- Map Floppy Disk

Navigate to the location where the ISO image is located and load the ISO image.

Step 6 Select **Power > Reset System (warm boot)** and Ok to continue and restart the UCS box.

Step 7 Press **F6** interrupt the reboot process when the server starts to select a boot device. The boot selection menu appears.

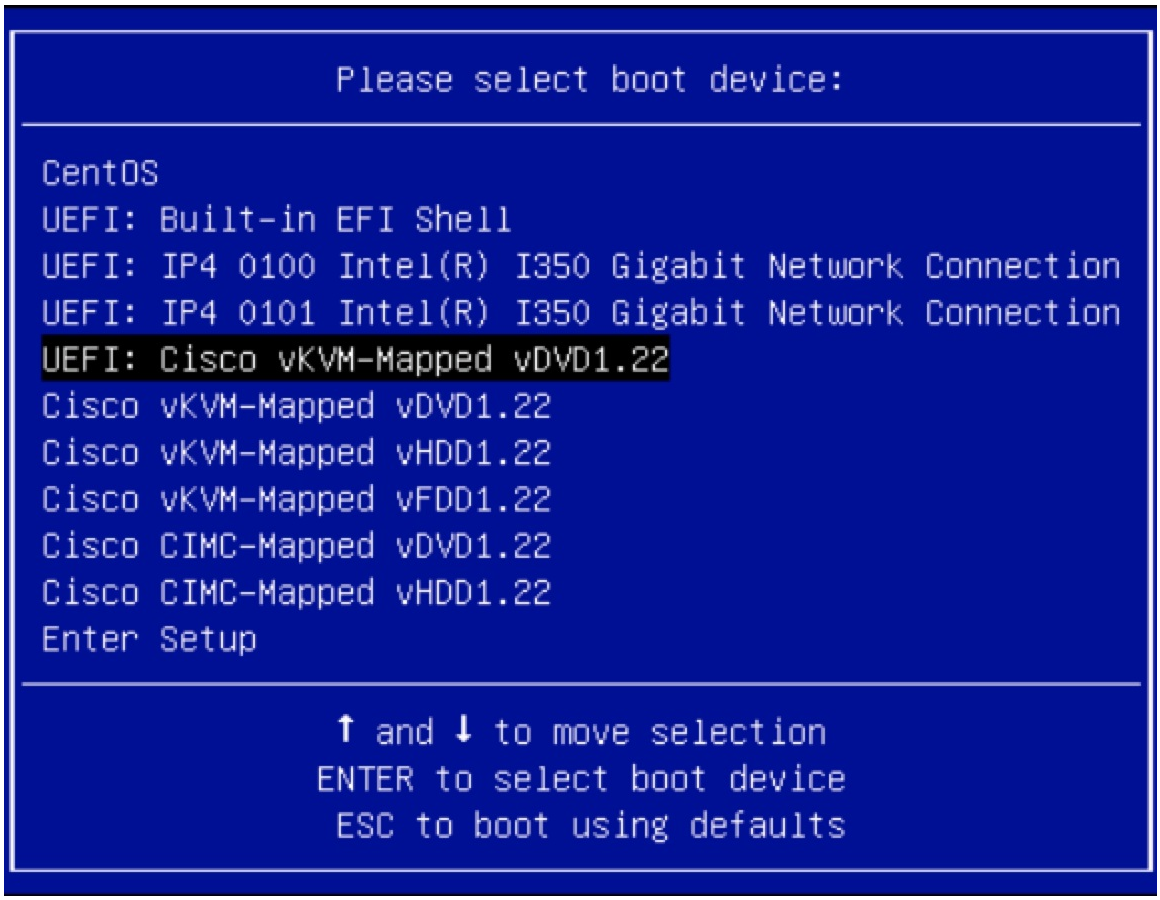
For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/31/UCS_SCU/booting.html#wp1078073

Step 8 Use the arrow keys to select Cisco Virtual CD/DVD and press **Enter**. The server boots with the DCNM ISO image from the mapped location.

Note The following image highlights UEFI installation. However, you can also choose **Cisco vKVM-Mapped vDVD1.22** for BIOS installation. ISO can be booted in both modes, BIOS, and UEFI.

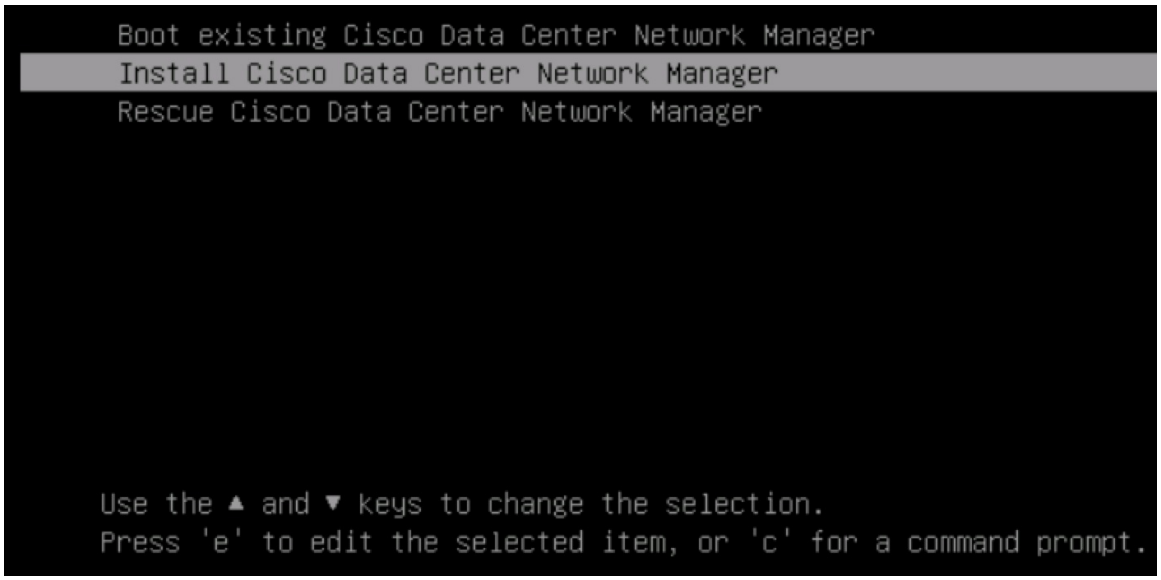
UEFI is mandatory for a system with minimum of 2TB disks.



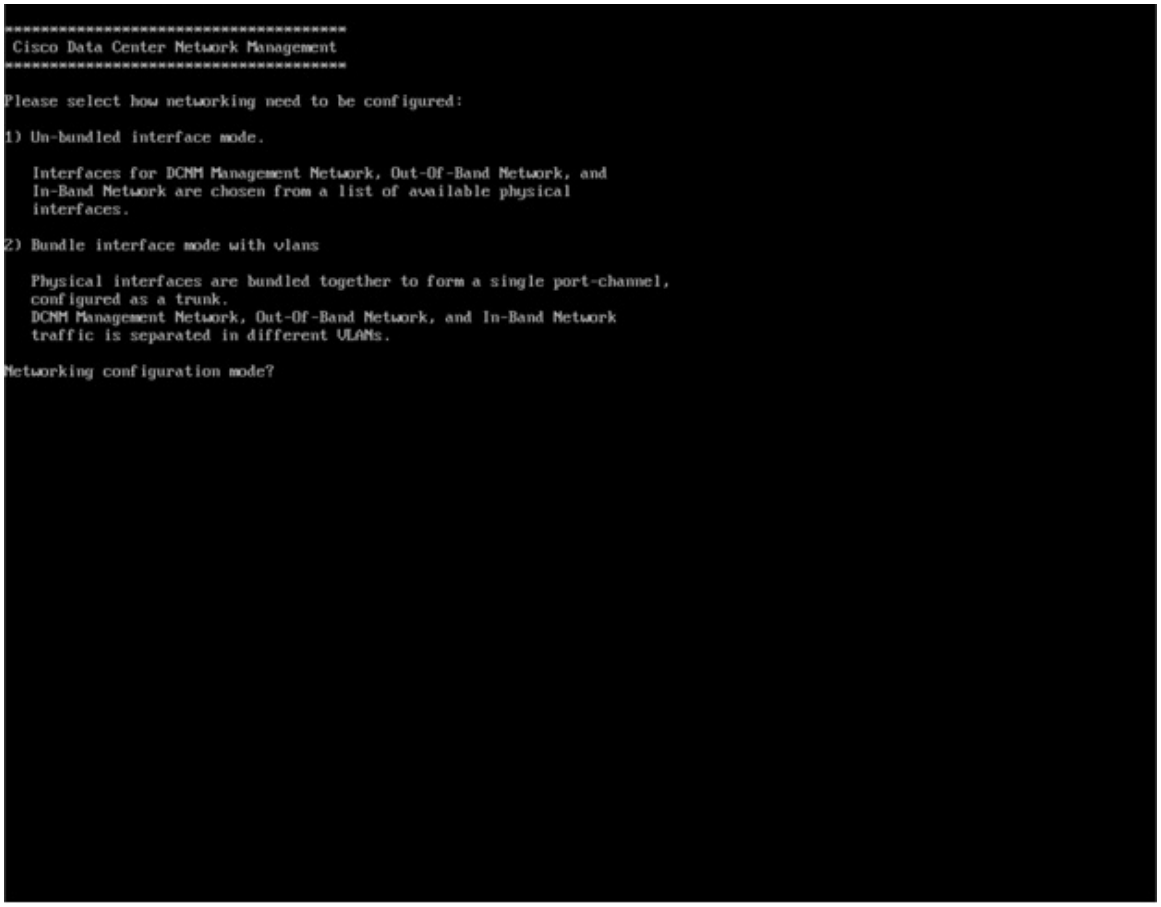
For Cisco UCS with the disk size of 2TB or higher and with 4K sector size drivers, the UEFI boot option is required. For more information, see UEFI Boot Mode.

Step 9 Select **Install Cisco Data Center Network Manager** using the up or down arrow keys. Press **Enter**.

The option shown in the following image appears when the ISO image is booted with UEFI.



Step 10 On the Cisco Management Network Management screen, select the mode to configure the network.

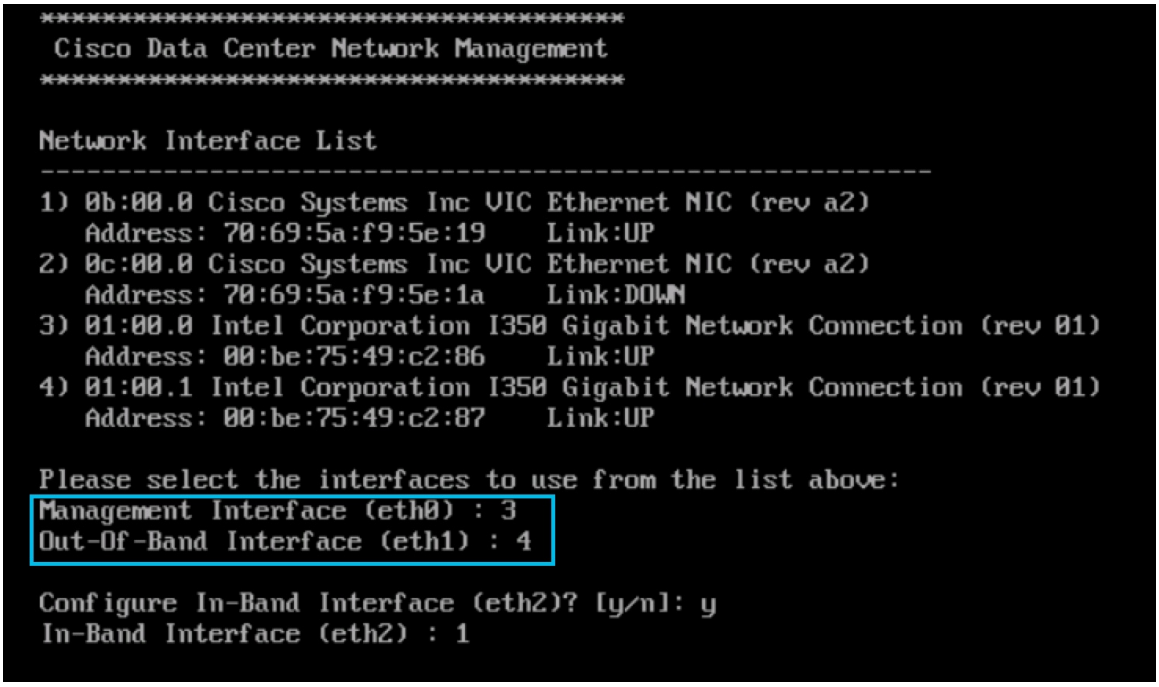


Enter 1 to configure the Cisco DCNM network interfaces from the available physical interfaces.

Enter 2 to configure the Cisco DCNM network interfaces from the available physical interfaces that are bundled together to form a single port-channel, configured as a trunk.

Step 11 If you entered 1, to install Cisco DCNM ISO in un-bundled interface mode, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the Management Interface (eth0) and Out-of-Band interface (eth1) from the Network Interface List. You can also configure the in-band interface (eth2) if necessary.



Note If you do not configure In-Band interface, Endpoint Locator and Telemetry features are not operational.

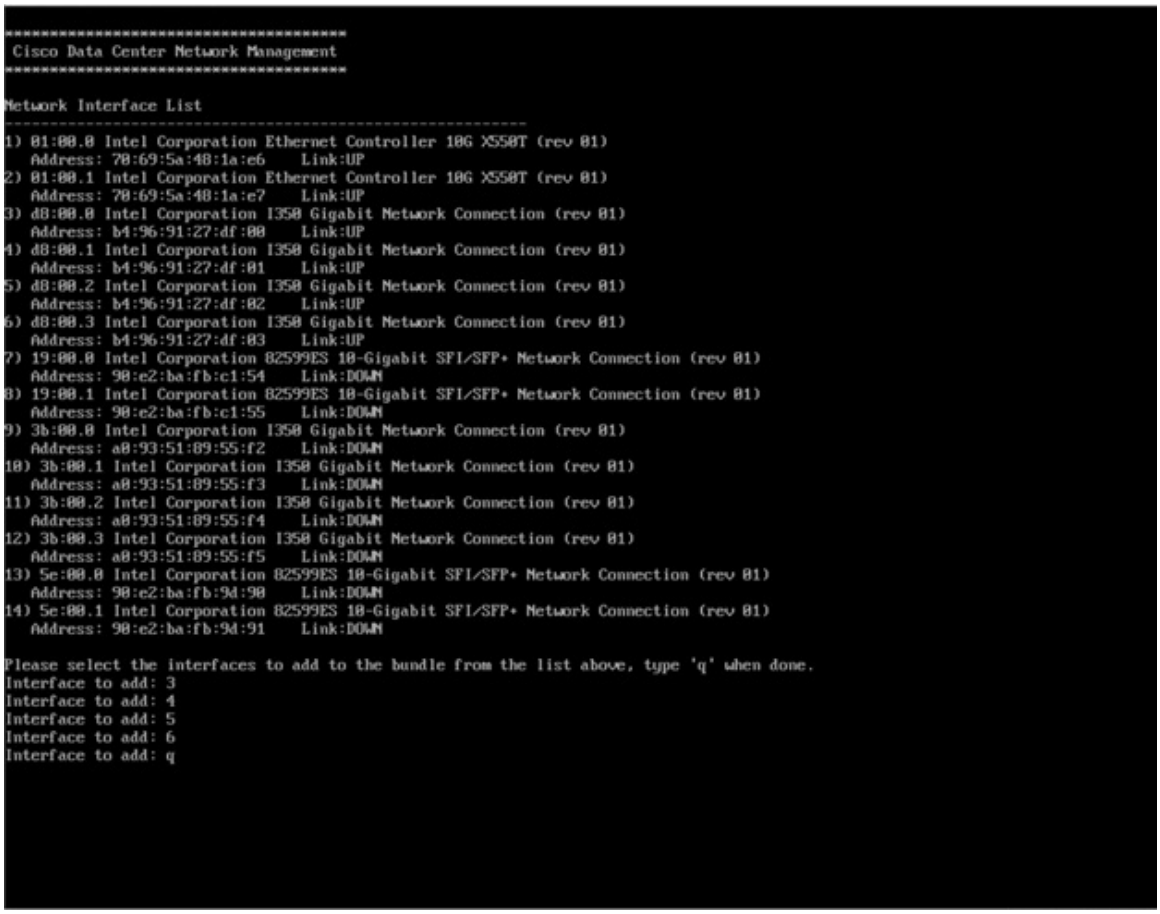
However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Step 12 If you entered 2, to install Cisco DCNM ISO in bundled interface mode, perform the following tasks:

a) Select interface from the list to form a bundle.

Note A minimum of one physical interface must be a part of the bundle.

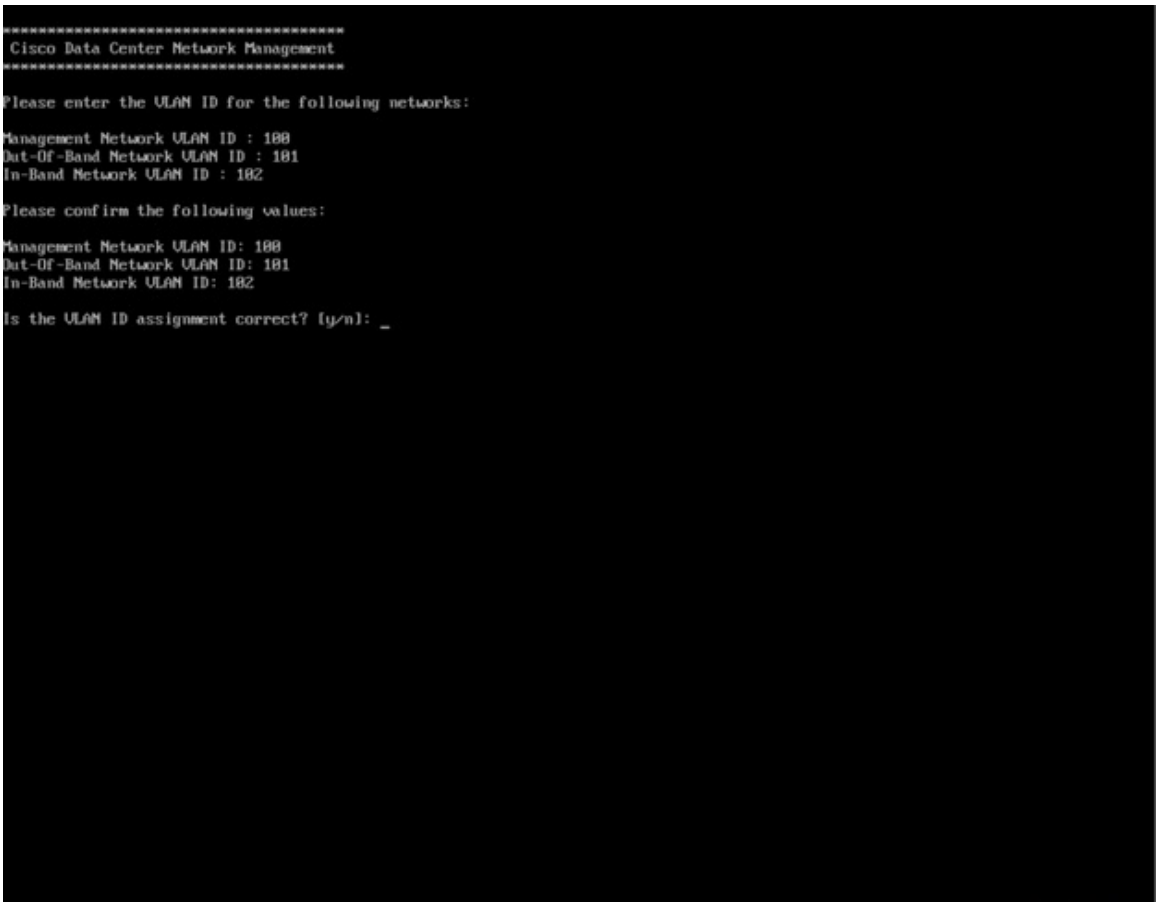
Enter **q** after you enter all the interface that must be added to the bundle.



b) Enter the VLAN IDs to be used for Management Network, Out-Of-Band Network and In-band Network Select interface from the list to form a bundle.

Verify and confirm if the correct VLAN IDs are assigned.

Note The VLAN IDs for Management Network and Out-Of-Band Network can be the same when Management Network and Out-Of-Band Network use the same subnet (that is, when eth0/eth1 are in the same subnet)



Step 13 Review the selected interfaces. Press **y** to confirm and continue with the installation.

Step 14 Configure the Management Network for Cisco DCNM. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
************************************************************
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
************************************************************
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to *Installing Cisco DCNM ISO in Standalone Mode* or *Installing Cisco DCNM ISO in Native HA Mode* sections for more information.

Installing the DCNM ISO Virtual Appliance on KVM

Perform the following tasks to install the ISO virtual appliance on KVM.

Procedure

Step 1 Unzip and extract and locate the **dcnm-kvm-vm.xml** file.

Step 2 Upload this file on the RHEL server that is running KVM to the same location as the ISO.

Step 3 Connect to the RHEL server running KVM via SCP File transfer terminal.

Step 4 Upload the and **dcnm-kvm-vm.xml** to the RHEL server.

Step 5 Close the file transfer session.

Step 6 Connect to the RHEL server running KVM via SSH terminal.

Step 7 Navigate to the location where both the ISO and domain XMLs is downloaded.

Step 8 Create the VM (or Domains, as they are known in the KVM terminology) using the **virsh** command.

need info on dcnm-kvm-vm-huge.xml

```
sudo virsh define [{dcnm-kvm-vm-huge.xml|dcnm-kvm-vm-compute.xml|
dcnm-kvm-vm-large.xml|dcnm-kvm-vm-small.xml}]
```

Step 9 Enable a VNC server and open the required firewall ports.

Step 10 Close the SSH session.

Step 11 Connect to the RHEL server running KVM via a VNC terminal.

Step 12 Navigate to **Applications > System Tools > Virtual Machine Manager (VMM)**.

A VM is created in the Virtual Machine Manager.

Step 13 From Virtual Machine Manager, edit the VM by selecting the VM in the listing. Click **Edit > Virtual Machine Details > Show virtual hardware details**.

Step 14 In the Virtual Hardware Details, navigate to **Add Hardware > Storage**.

Step 15 Create a hard disk with Device type withe the following specifications:

- device type: IDE disk
- cache-mode: default
- storage format: raw

We recommend that you use storage size of 500GB.

Step 16 Select IDE CDROM on the edit window of the Virtual Machine and click **Connect**.

Step 17 Navigate to dcnm-va.iso and click **OK**.

Step 18 Select both the NICs and assign appropriate networks that are created.

Step 19 Power on the Virtual Machine.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

The operating system is installed.

Step 20 On the Cisco Management Network Management screen, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the Management Interface (eth0) and Out-of-Band interface (eth1) from the Network Interface List. You can also configure in-band interface (eth2) if necessary.

Note If you do not configure in-band interface (eth2), Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Step 21 Press **y** to confirm and continue with the installation.

Step 22 Configure the Management Network. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
*************************************************************
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*************************************************************
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to *Installing Cisco DCNM ISO in Standalone Mode* or *Installing Cisco DCNM ISO in Native HA Mode* sections for more information.

Installing the DCNM ISO Virtual Appliance on Windows Hyper-V

Hyper-V Manager provides management access to your virtualization platform. You can install DCNM ISO virtual appliance using Hyper-V manager.

Launch the Windows Server Manager using appropriate credentials. To launch the Hyper-V Manager, from the Menu bar, choose **Tools > Hyper-V Manager**.

Note DCNM ISO Virtual Appliance on Windows Hyper-V doesn't support Clustered mode.

To install Cisco DCNM ISO Virtual Appliance on Windows Hyper-V, perform the following tasks:

Creating Virtual Switches

Cisco DCNM requires three virtual switches for network interfaces:

- dcnm-mgmt network (eth0) interface
- enhanced-fabric-mgmt (eth1) interface

- enhanced-fabric-inband (eth2) interface

To create Virtual Switches on the Hyper-V Manager, perform the following steps:

Procedure

Step 1 On the Action pane, click **Virtual Switch Manager**.

The Virtual Switch Manager for the Windows Hyper-V window appears.

Step 2 On the left pane, under Virtual Switches, click **New virtual network switch** to create a virtual switch.

Step 3 Create the virtual switch for DCNM Management network.

a) Select **External** and click **Create Virtual Switch**.
b) In the Name field, enter the enter an appropriate name for the **eth0** interface.

Note Ensure that the virtual switch name is unique within the Inventory.

c) From the External network drop-down list, select the appropriate physical interface available on the server.
d) Click **Apply**.

Step 4 Create the virtual switch for Enhanced Fabric Management interface.

a) Select **External** and click **Create Virtual Switch**.
b) In the Name field, enter the enter an appropriate name for the **eth1** interface.

Note Ensure that the virtual switch name is unique within the Inventory.

c) From the External network drop-down list, select the appropriate physical interface available on the server.
d) Click **Apply**.

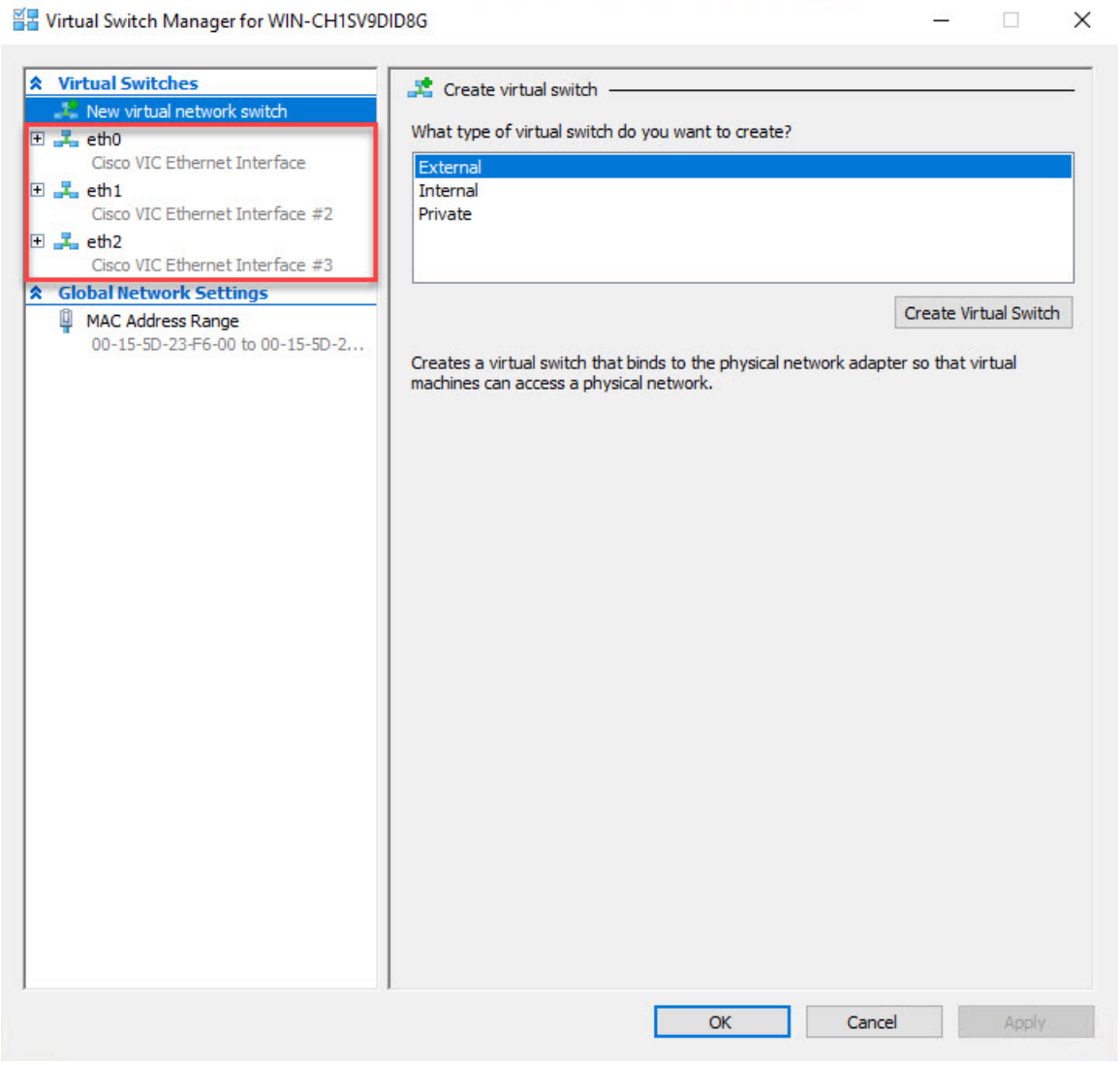
Step 5 Create the virtual switch for Enhanced Fabric Inband interface.

a) Select **External** and click **Create Virtual Switch**.
b) In the Name field, enter the enter an appropriate name for the **eth2** interface.

Note Ensure that the virtual switch name is unique within the Inventory.

c) From the External network drop-down list, select the appropriate physical interface available on the server.
d) Click **Apply**.

All the interfaces appear under the Virtual Switches in the left pane, as shown in the following figure.



What to do next

Create the Virtual Machines to mount the ISO. Refer to Creating Virtual Machines, on page 34 for more information.

Creating Virtual Machines

To create virtual machines for either Standalone, or Primary and Secondary nodes for Native HA setup, perform the following procedure:

Before you begin

If you're installing Cisco DCNM in Native HA Mode, you must create two virtual machines; one for Primary node, and one for Secondary node.

Procedure

Step 1 In the Actions pane, from the New drop-down list, select **Virtual Machine**.

The New Virtual Machine Wizard appears.

Step 2 In the Before You Begin screen, click **Next**.

Step 3 In the Specify Name and Location screen, enter the name for the Active DCNM node.

Click **Next**.

Step 4 In the Specify Generation screen, select **Generation 2**.

This virtual machine supports new virtualization features, has UEFI-based firmware, and requires 64-bit operating system.

Click **Next**.

Step 5 In the Assign Memory screen, in the **Startup memory** field, enter **32768** MB to configure the virtual machine with 32GB memory.

Step 6 In the Configuration Networking screen, from the **Connection** drop-down list, select the interface for this VM. Select **eth0** (Management Network interface).

Click **Next**.

Step 7 In the Connect Virtual Hard Disk screen, create a virtual hard disk.

a) Select **Create a virtual hard disk**.

b) Enter appropriate **Name**, **Location**, and **Size** of the hard disk.

Note The default name for the virtual hard disk is derived from the virtual machine name that you provided in the Specify Name and Location screen.

The size of the hard disk must be minimum of 500GB.

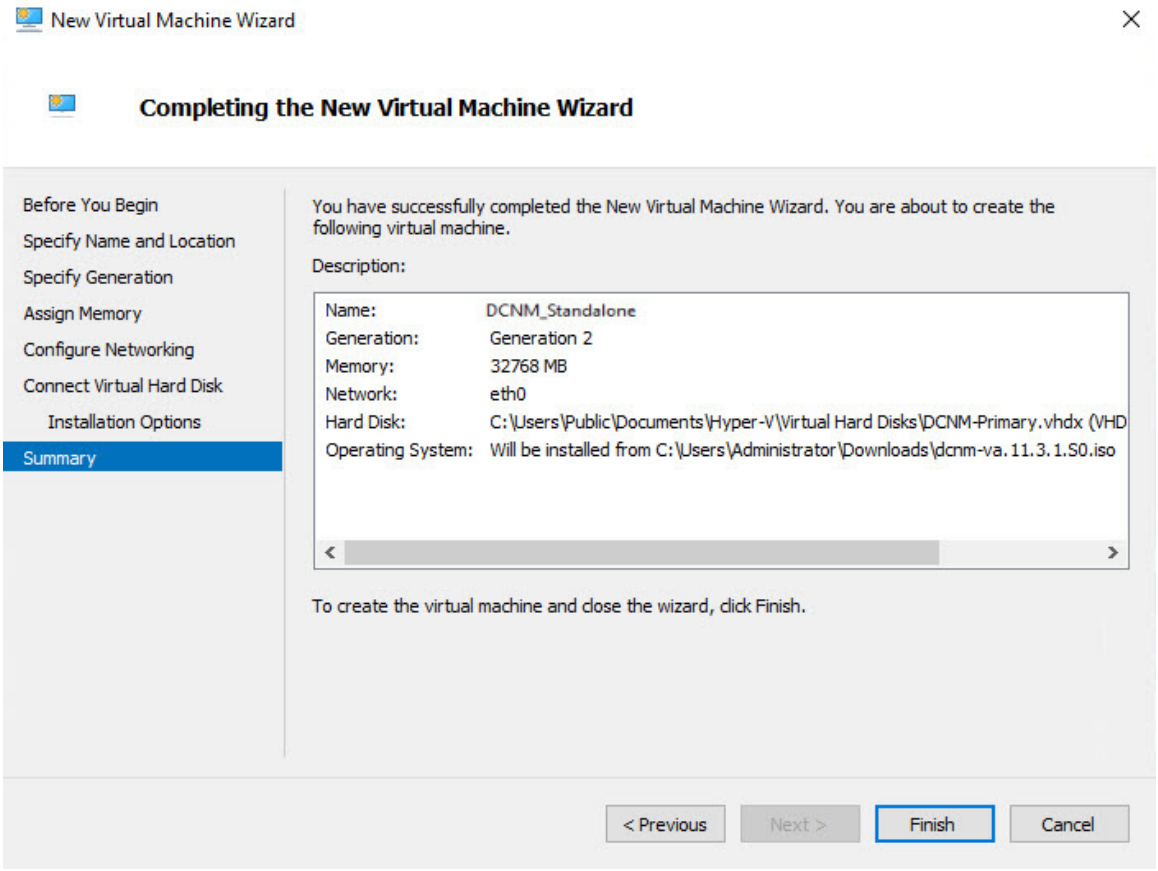
Click **Next**.

Step 8 In the Installation Options screen, select **Install as operating system from a bootable image file**.

In the Image file (.iso) field, click **Browse**. Navigate to the directory and select the DCNM ISO image.

Click **Next**.

Step 9 In the Summary screen, review the configuration details.



Click **Finish** to create the DCNM Active node.

The newly created virtual machine appears in the Virtual Machines block on the Hyper-V Manager.

Step 10 Right click on the virtual machine and select **Settings**.

The Settings screen for DCNM node appears.

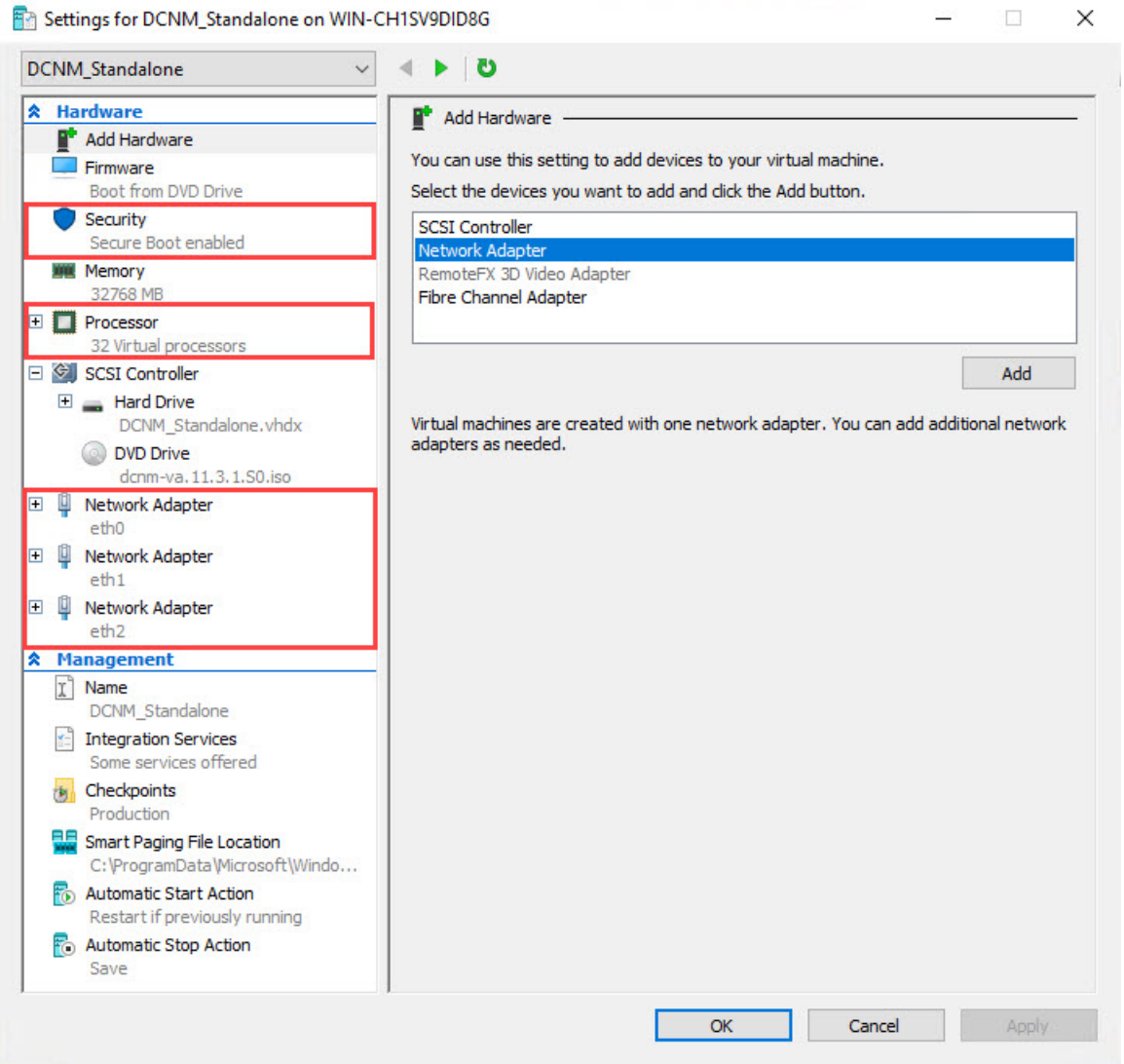
Step 11 On the left pane, in the Hardware block, click **Add Hardware**.

Step 12 In the main pane, select **Network Adapter** and click **Add**.

Step 13 In the Network Adapter screen, create network adapter for the virtual switch.

- From the **Virtual Switch** drop-down list, select the **eth1** virtual switch. Click **Apply**.
- From the **Virtual Switch** drop-down list, select the **eth2** virtual switch. Click **Apply**.

All the three Network Adapters are displayed in the left pane, under the **Hardware** section.



Step 14 In the left pane, select **Security**.

In the main pane, from the template drop-down list, select **Microsoft UEFI Certificate Authority**.

Note This template is a mandatory if you've selected the Generation 2 hyper-V virtual machines.

Click **Apply**.

Step 15 In the Settings screen, click **Processor**.

In the main pane, in the **Number of virtual processors** field, enter **32**, to choose 32vCPUs. Click **Apply**.

Click **OK** to confirm the settings for the DCNM node.

What to do next

Install the Cisco DCNM ISO on the Windows Hyper-V. Refer to Installing DCNM ISO Virtual Appliance, on page 38 for more information.

Installing DCNM ISO Virtual Appliance

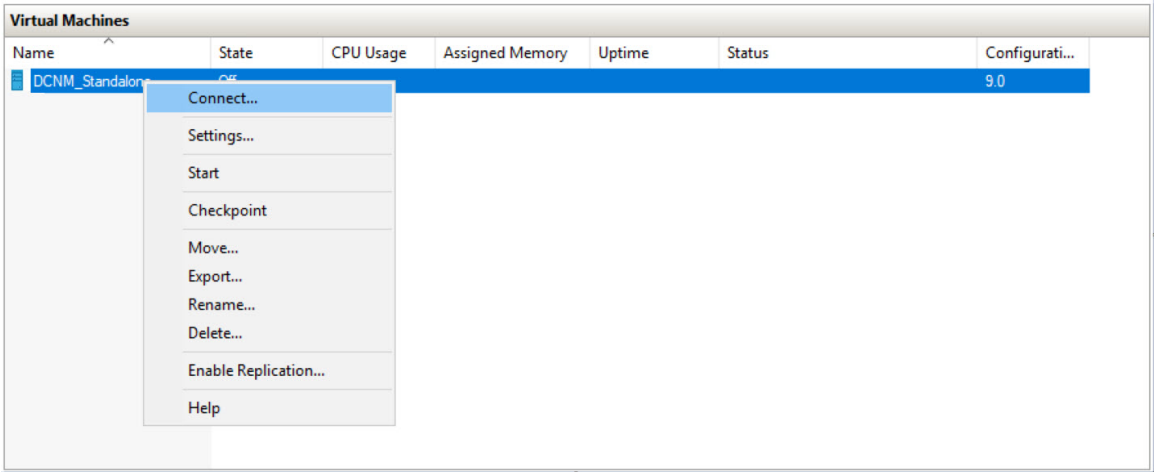
To configure the DCNM ISO virtual appliance for either Standalone, or Primary and Secondary nodes for Native HA setup, perform the following procedure:

Before you begin

Ensure that the Virtual Machine is configured correctly with proper security settings.

Procedure

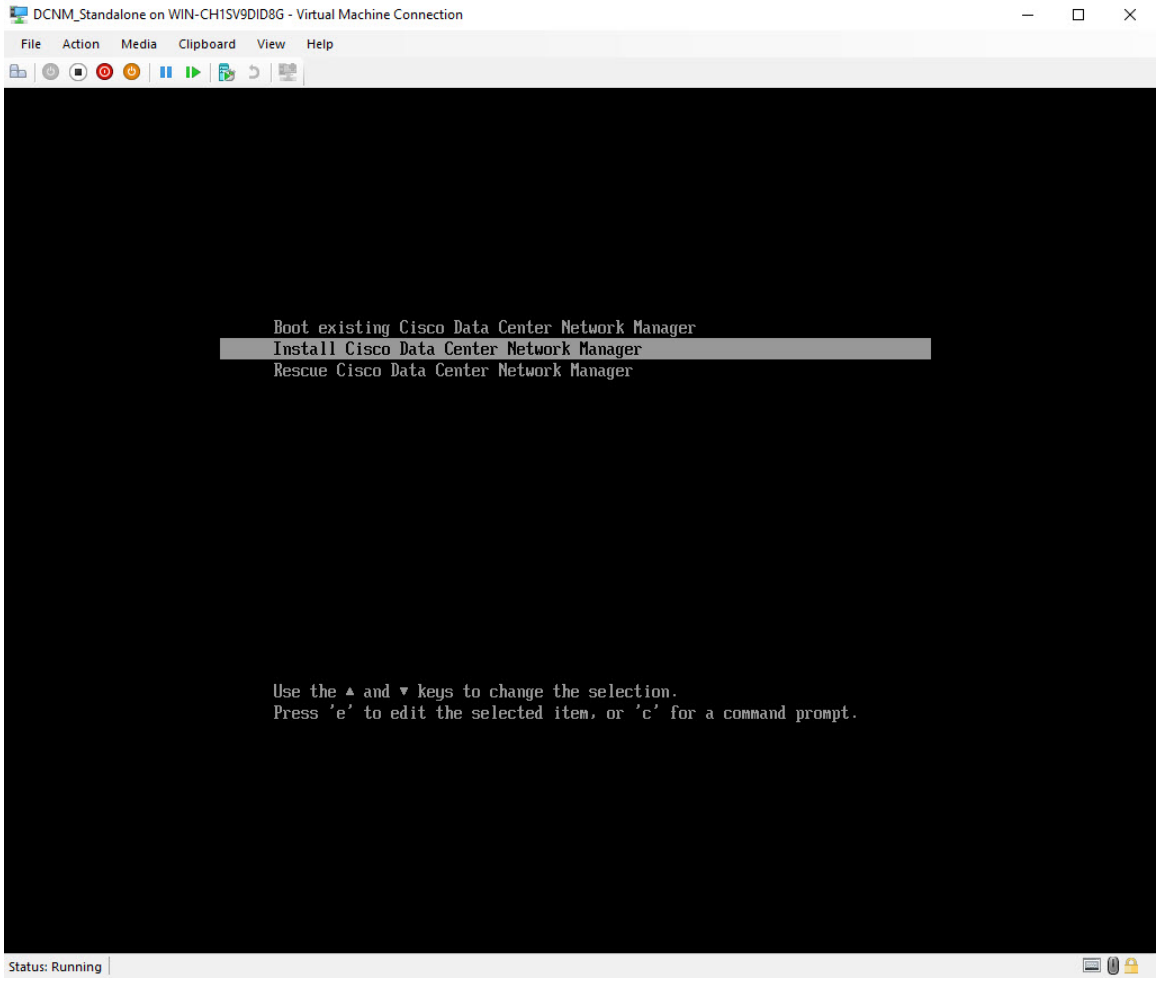
Step 1 From the Virtual Machines block, right click n the Active node and select **Connect**.



Step 2 In the Virtual Machine Connection screen, from the Menu bar, select **Media > DVD Drive** to verify the image selected.

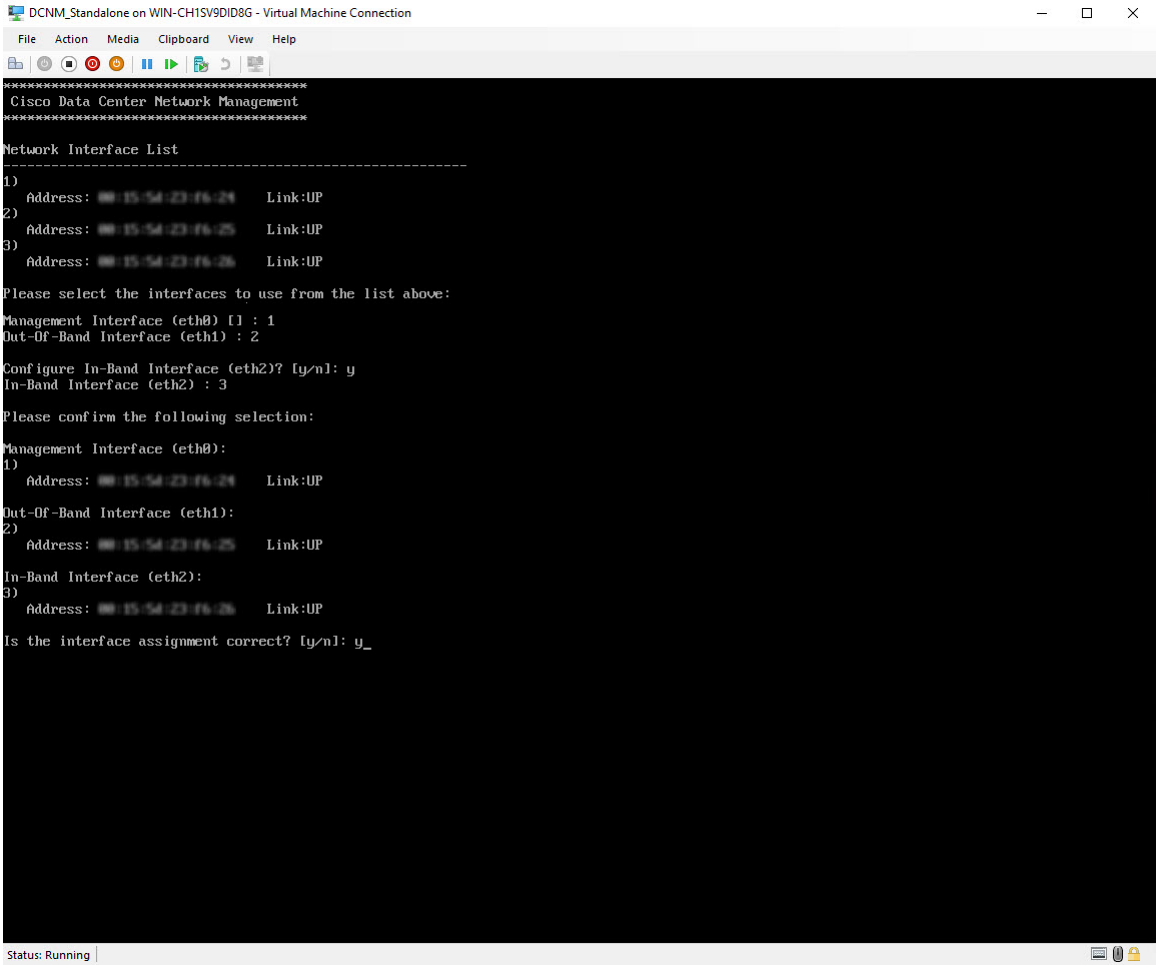
Click **Start**. The DCNM Server boots.

Step 3 Select **Install Cisco Data Center Network Manager** using the up or down arrow keys. Press **Enter** to install the Cisco DCNM Active node.



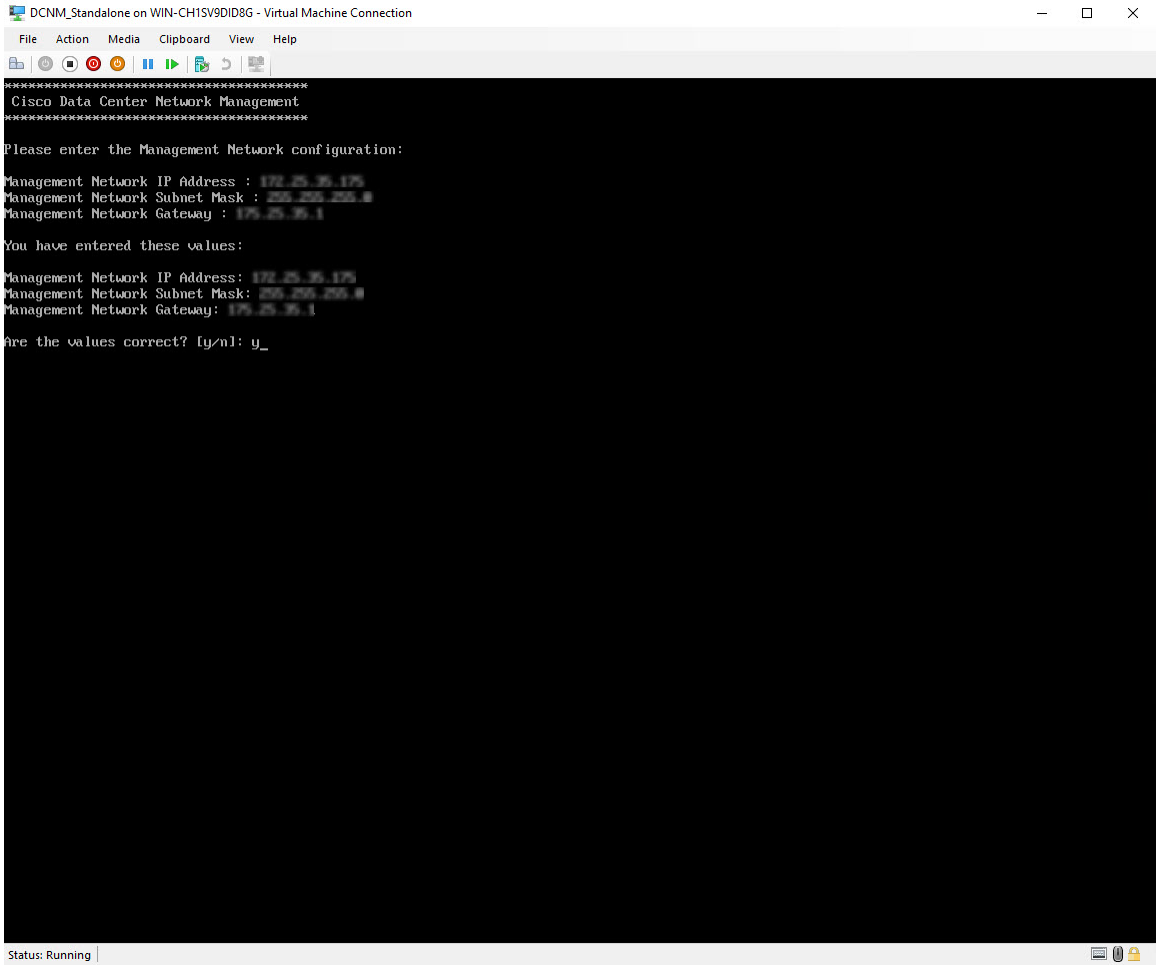
Step 4 On the Cisco Management Network Management screen, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the **Management Interface (eth0)** and **Out-of-Band interface (eth1)** from the Network Interface List. You can also configure the **In-band interface (eth2)** if necessary.



Review the selected interfaces. Press **y** to confirm and continue with the installation.

Step 5 Configure the Management Network for Cisco DCNM. Enter the **IP address**, **Subnet Mask**, and **Gateway**. Verify the values and press **y** to continue with the installation.



After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
************************************************************
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
************************************************************
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. For more information, see Installing Cisco DCNM ISO in Standalone Mode, on page 41 or Installing the Cisco DCNM ISO in Native HA mode, on page 46.

Installing Cisco DCNM ISO in Standalone Mode

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears.

To complete the installation of Cisco DCNM from the web installer, perform the following procedure.

Procedure

Step 1 On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

Step 2 On the **Cisco DCNM Installer** tab, select **Fresh Installation – Standalone** radio button.

Click **Next**.

Step 3 On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

Step 4 On the **Administration** tab, enter information about passwords.

- In the **Administrator Password** field, enter the password that is used to connect to the applications in the Cisco DCNM.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Administrator Password** field.

- In the **Database Password** field, enter the password for the PostgreSQL database.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Database Password** field.

  Note If **Database Password** field is left blank, it shall consider the Administrator password as the PostgreSQL password.

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

Select the **Show passwords in clear text** check box to view the password that you have entered.

Click **Next**.

Step 5 On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  You can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

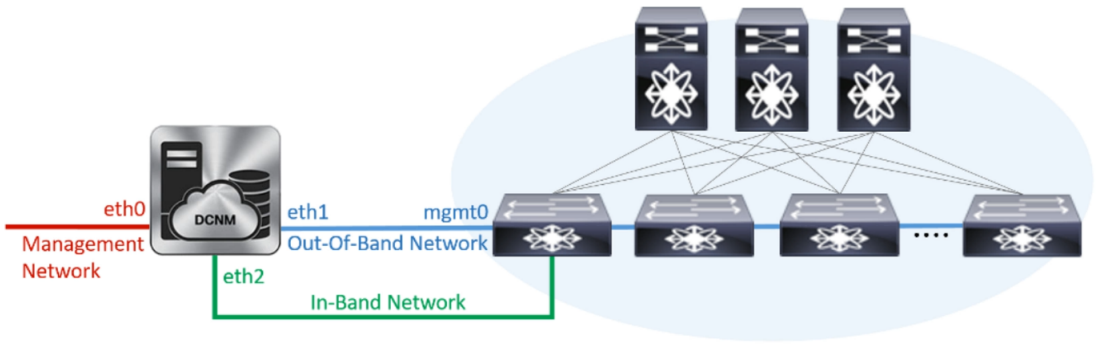
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

Step 6 On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 4: Cisco DCNM Management Network Interfaces



a) In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optional) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

b) In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

c) (Optional) In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

This field is mandatory if you have selected the Enable Cluster mode in Step Step 3, on page 42.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Click **Next**.

Step 7 On the **Applications** tab, configure the Device Connector and Internal Applications Services Network, and Cluster mode settings.

Note Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

a) (Optional) In the **Proxy Server** field, enter the IP address for the proxy server.

The proxy server must be of RFC1123-compliant name.

Note By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

b) In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

c) In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step Step 3, on page 42.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

- In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

  Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

- In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

  Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

Click **Next**.

Step 8 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

Note If you try to access the DCNM Web UI using the Management IP address while the installation is still in progress, an error message appears on the console.

```
************************************
*Preparing Appliance*

************************************
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Installing the Cisco DCNM ISO in Native HA mode

The native HA is supported on DCNM appliances with ISO or OVA installation only.

By default, an embedded PostgreSQL database engine with the Cisco DCNM. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following task to set up Native HA for DCNM.

Procedure

Step 1 Deploy two DCNM Virtual Appliances (either OVA or ISO).

For example, let us indicate them as **dcnm1** and **dcnm2**.

Step 2 Configure **dcnm1** as the Primary node. Paste the URL displayed on the Console tab of **dcnm1** and press **Enter** key.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the **Cisco DCNM Installer** tab, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Next**.

c) On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

- In the **Administrator Password** field, enter the password that is used to connect to the applications in the Cisco DCNM.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Administrator Password** field.

- In the **Database Password** field, enter the password for the PostgreSQL database.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

  Enter the password again in the **Repeat Database Password** field.

  Note If the **Database Password** field is left blank, it shall consider the Administrator password as the PostgreSQL password.

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

Select the **Show passwords in clear text** check box to view the password that you have entered.

Click **Next**.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

  The value must be an IP or IPv6 address or RFC 1123 compliant name.

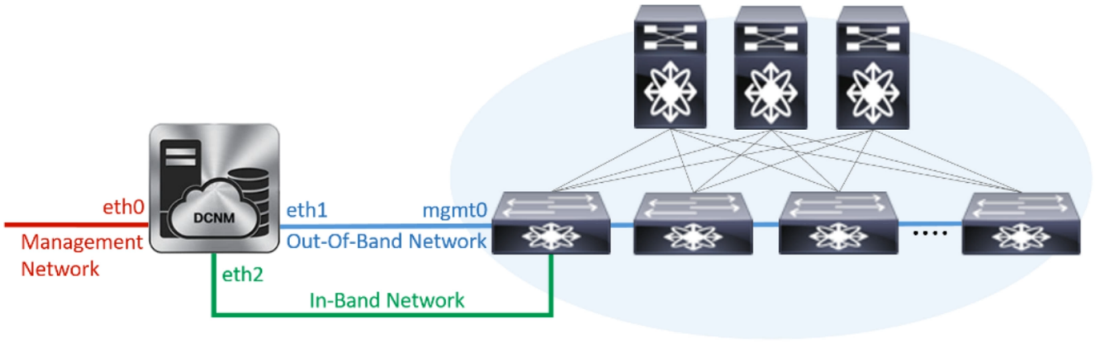
  From Release 11.3(1), you can configure more than one NTP server.

- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 5: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Out-of-band management provides a connection to the device management ports (Typically mgmt0).

   Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   This field is mandatory if you have selected the **Enable Cluster** mode..

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Click **Next**.

g) On the **Applications** tab, configure the Device Connector and Internal Applications Services Network.

Note Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

1. In the **Proxy Server** field, enter the IP address for the proxy server.

   The proxy server must be of RFC1123-compliant name.

   Note By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

   If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

2. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

   All the applications use the IP Address from this subnet. By default, the

   The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step 2.c, on page 46.

   Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

3. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

h) On the **HA Settings** tab, a confirmation message appears.

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

Click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A warning message appears stating that the setup is not complete until you install the Secondary node.

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on
this HA primary node.
However, the system will be ready to be used only after installation
of the secondary node has been completed.
Thank you.
```

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the **Install Mode** tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note All the passwords must be same as the passwords that you provided while configuring the Primary node.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you’re using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

  The value must be an IP or IPv6 address or RFC 1123 compliant name.

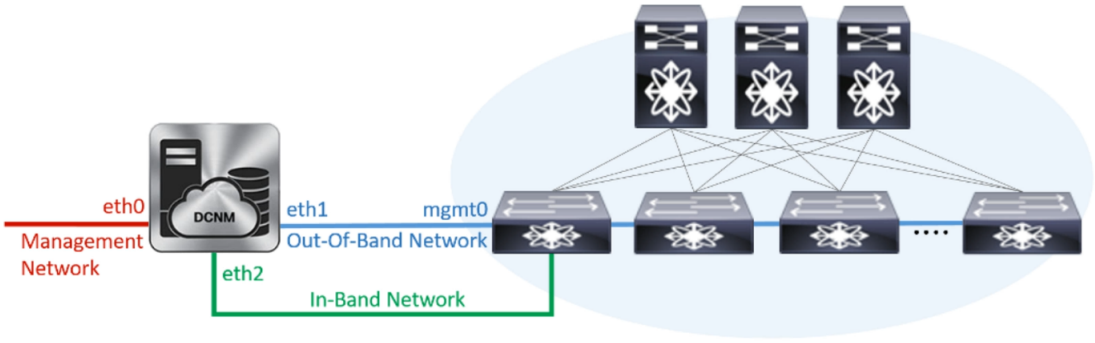
  From Release 11.3(1), you can configure more than one NTP server.

- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 6: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Ensure that the IP address belongs to the same Management Network configured on the Primary node.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

   Out-of-band management provides a connection to the device management ports (Typically mgmt0).

   Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

1. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.
2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.

- In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
- In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
- In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

  Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

  Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
- In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.
- In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

  Note This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.
- In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

  Note The configured IPv4 address must respond to the ICMP echo pings.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Convert Standalone Setup to Native-HA Setup

To convert an existing Cisco DCNM Standalone setup to a Native HA setup, perform the following steps:

Before you begin

Ensure that the Standalone setup is active and operational, by using the **appmgr show version** command.

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version:
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

Procedure

Step 1 On the Standalone setup, launch SSH and enable **root** user access by using the **appmgr root-access permit** command:

```
dcnm# appmgr root-access permit
```

Step 2 Deploy a new DCNM as secondary node. Choose **Fresh installation - HA Secondary**

For example, let us indicate the existing setup as **dcnm1** and the new DCNM as secondary node as **dcnm2**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the **Install Mode** tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note All the passwords must be same as the passwords that you provided while configuring the Primary node.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.

- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

  The value must be an IP or IPv6 address or RFC 1123 compliant name.

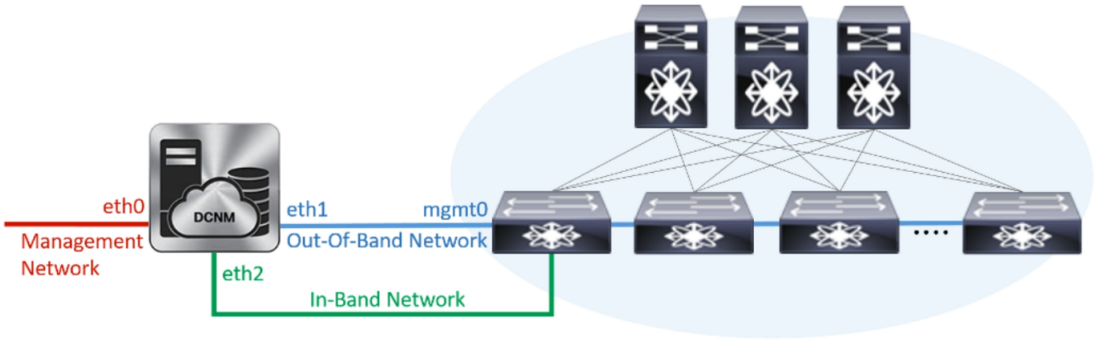
  From Release 11.3(1), you can configure more than one NTP server.

- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 7: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Ensure that the IP address belongs to the same Management Network configured on the Primary node.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

   Out-of-band management provides a connection to the device management ports (Typically mgmt0).

   Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

1. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.
2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.

- In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
- In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
- In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

  Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

  Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
- In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.

- In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

  Note This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.

- In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

  Note The configured IPv4 address must respond to the ICMP echo pings.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

  You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Verify the HA role by using the appmgr show ha-role command.

On the Active node (old standalone node):

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node (newly deployed node):

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Installing Cisco DCNM Compute Node

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears. You can install compute nodes on both Cisco DCNM OVA and ISO deployments.

Note Compute nodes allows users to scale DCNM, as application load can be shared across all the compute nodes, instead of the usual 1 or 2 (if you have HA) nodes.

Note If **Enable Clustered Mode** was selected during DCNM installation, applications such as, Configuration Compliance, EPL, NIA, and NIR won't work until you install the compute nodes.

When NIR/NIA applications is enabled at higher scale, that is, with 250 switches and 10000 Hardware telemetry flows, DCNM Computes nodes must be connected on all eth0, eth1, and eth2 interfaces using a 10Gig link.

To complete the installation of Cisco DCNM Compute Node from the web installer, perform the following procedure.

Before you begin

Ensure that you have 16 vCPUs, 64GB RAM, and 500GB hard disc to install compute nodes.

By default, the **ComputeHuge** configuration has 32vCPUs and 128GB RAM with 2TB disk. This configuration is recommended if you use Cisco Network Insights applications.

Procedure

Step 1 On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Step 2 On the Cisco DCNM Installer screen, select the **Fresh Installation – Standalone** radio button.

Click **Continue**.

Step 3 On the **Install Mode** tab, choose **Compute** to deploy this DCNM instance as a compute node.

Note **Compute** option appears in the drop-down list only if you have chosen **Compute** or **ComputeHuge** while configuring the OVF template or ISO hypervisors.

Click **Next**.

Step 4 On the **Administration** tab, enter information about passwords.

- In the **Administrator Password** field, enter the password that is used to connect to the applications in the Cisco DCNM.

  All special characters, except **%$^=;.*\'" <SPACE>** is allowed in the password.

Enter the password again in the **Repeat Administrator Password** field.

Select the **Show passwords in clear text** check box to view the password that you have entered.

Click **Next**.

Step 5 On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

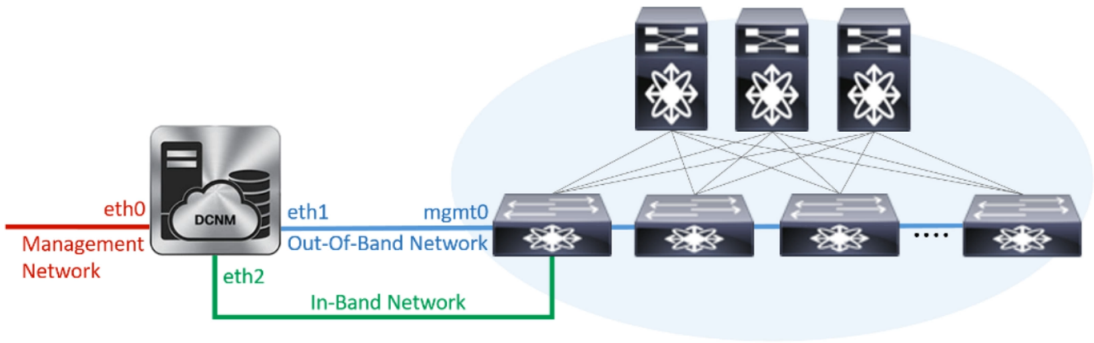
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

Step 6 On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 8: Cisco DCNM Management Network Interfaces



a) In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

b) In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

c) In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 85.

Click **Next**.

Step 7 In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

Click **Next**.

Step 8 On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

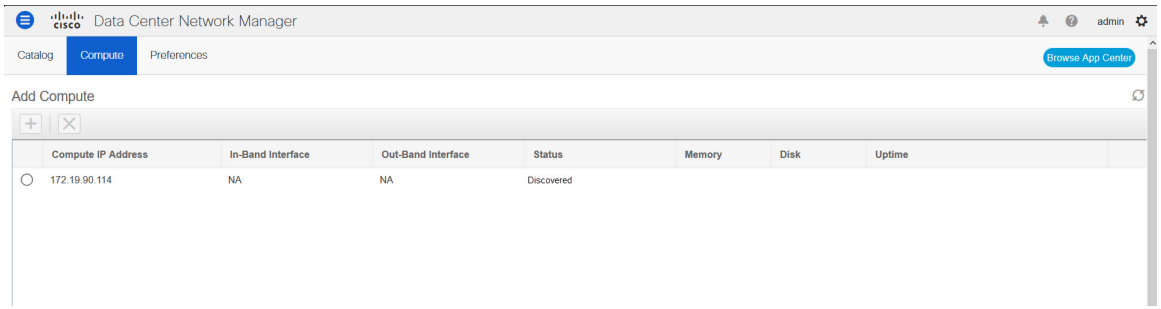
A success message appears with the URL to access DCNM Compute Node.

```
************************************************************
Your Cisco DCNM Compute Node has been installed.
Click on the following link to go to DCNM GUI's Application page:
DCNM GUI's Applications
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

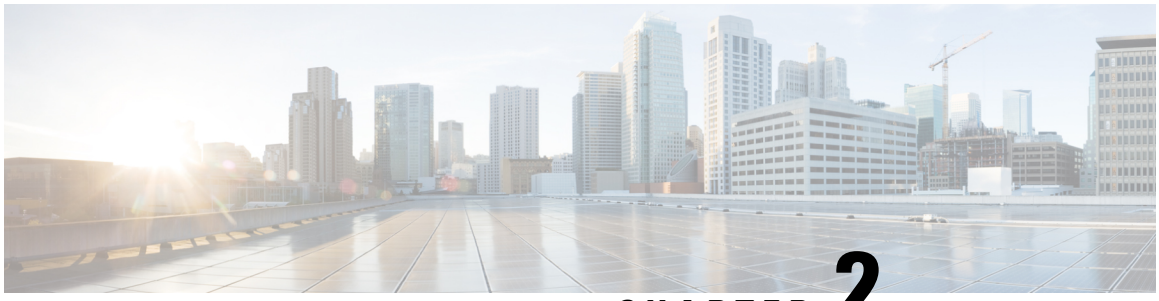
What to do next

Log on to the DCNM Web UI with appropriate credentials.

The **Applications** tab displays all the services running on the DCNM deployment that you have installed. Click **Compute** tab to view the new Compute in Discovered state on the Cisco DCNM Web UI.



When a compute node goes through a unscheduled powercycle and restarts, the Elasticsearch container will not start. It is possible that some filesystems are corrupted. To resolve this issue. reboot the Compute node in safe mode by using **fsck -y** command.



CHAPTER 2

Deployment Best Practices

- Best Practices for Deploying Cisco DCNM and Computes, on page 63

Best Practices for Deploying Cisco DCNM and Computes

This chapter describes the document best practices to deploy Cisco DCNM OVA and ISO in clustered and unclustered modes. The following sections explain the recommended design for configurations of IP addresses and relevant IP pools during the Cisco DCNM installation.

The Cisco DCNM OVA or the ISO installation consists of 3 network interfaces:

- dcnm-mgmt network (eth0) interface

  This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM.

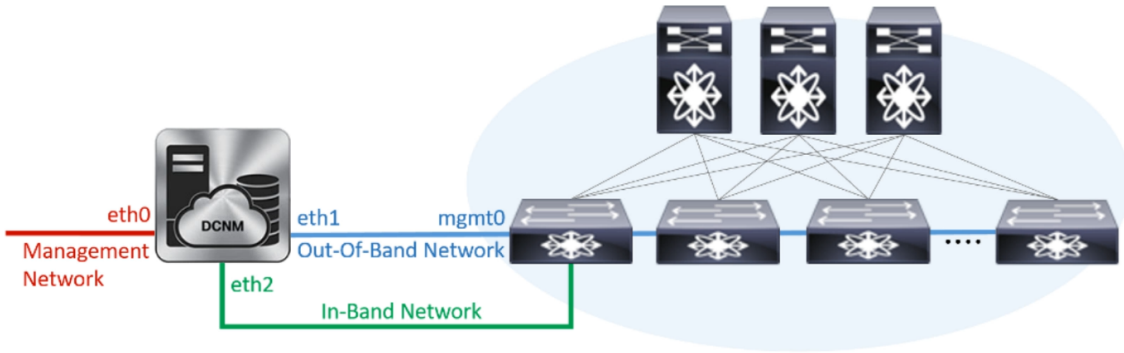
- enhanced-fabric-mgmt (eth1) interface

  This network provides enhanced fabric management of Cisco Nexus switches through the out-of-band or mgmt0 interface.

- enhanced-fabric-inband (eth2) interface

  This network provides in-band connection to the fabric through the front-panel ports. This network interface is used for applications such as Endpoint Locator (EPL) and Network Insights Resources (NIR).

The following figure shows the network diagram for the Cisco DCNM management interfaces.



Guidelines to Use the Best Practices

The following are the guidelines to remember while you use the best practices for deploying DCNM and Computes.

- The IP addresses specified in this document are sample addresses. Ensure that your setup reflects the IP addresses used in the production network.
- Ensure that the eth2 interface subnet is different from the subnet that is associated with the eth0 interface and the eth1 interface.
- As eth0 and eth1 interfaces are both on the same subnet, the DHCP returns the same IP address, two responses but same for both queries.
- Cisco DCNM Native HA consists of two Cisco DCNM appliances, that run as Active and Standby applications. The embedded databases of both Active and Standby appliances are synchronized in real time. The eth0, eth1, and eth2 interfaces of the Cisco DCNM and Compute nodes, in a clustered mode, must be Layer-2 adjacent.
- For information about Cluster Mode in your Cisco DCNM Deployment, refer to Applications chapter in the *Cisco DCNM Configuration Guide* for your deployment type.

Deployments for Redundancy in Cisco DCNM

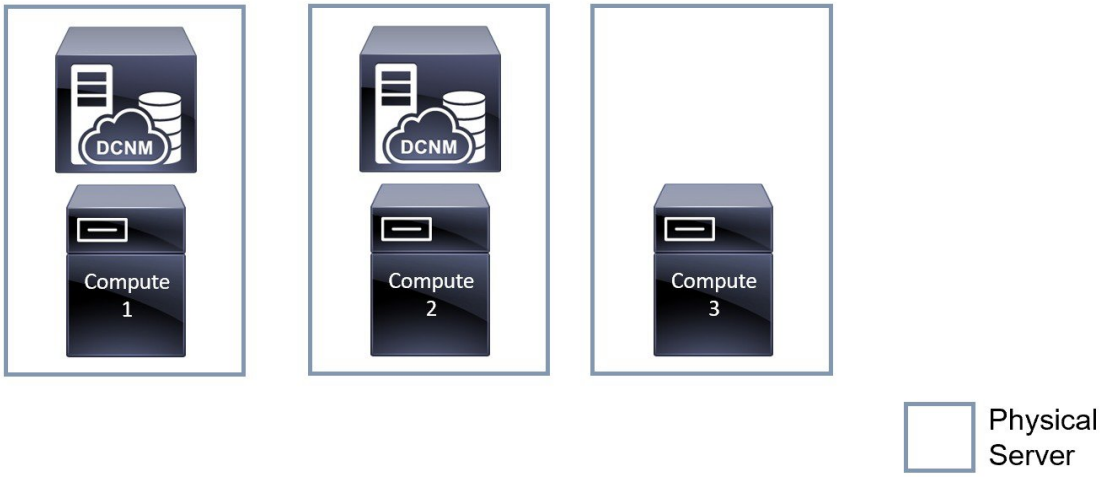
This section describes the recommended deployments for redundancy of DCNM operations. As a general assumption, the DCNM and the compute nodes are installed as Virtual Machines. During Cisco DCNM ISO installation on Virtual Appliance on UCS (Bare Metal), all DCNMs and computes have their own individual servers.

Deployment 1: Minimum Redundancy Configuration

The recommended configuration for minimum redundancy in a Cisco DCNM Cluster mode installation is as follows:

- DCNM Active Node and Compute Node 1 in Server 1
- DCNM Standby Node and Compute Node 2 in Server 2
- Compute Node 3 in Server 3
- Compute VMs deployed on an exclusive disk
- No oversubscription of memory or CPU of the physical servers

Figure 9: Cisco DCNM Cluster Mode: Physical Server to VM Mapping

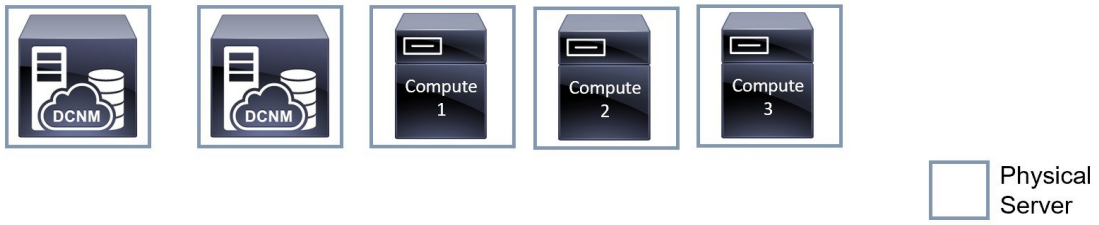


Deployment 2: Maximum Redundancy Configuration

The recommended configuration for maximum redundancy in a DCNM Cluster mode installation is as follows:

- DCNM Active Node(Active) in Server 1
- DCNM Standby Node in Server 2
- Compute Node 1 in Server 3
- Compute Node 2 in Server 4
- Compute Node 3 in Server 5

Figure 10: Cisco DCNM Cluster Mode: Physical Server to VM Mapping



IP Address Configurations in Cisco DCNM

This section describes the best practices and recommended deployments for IP address configurations of all interfaces of the Cisco DCNM and Compute nodes.

Scenario 1: All 3 Ethernet Interfaces are in Different Subnets

In this scenario, consider all three Ethernet interfaces of DCNM on different subnets.

For example:

- eth0 – 172.28.8.0/24
- eth1 – 10.0.8.0/24
- eth2 – 192.168.8.0/24

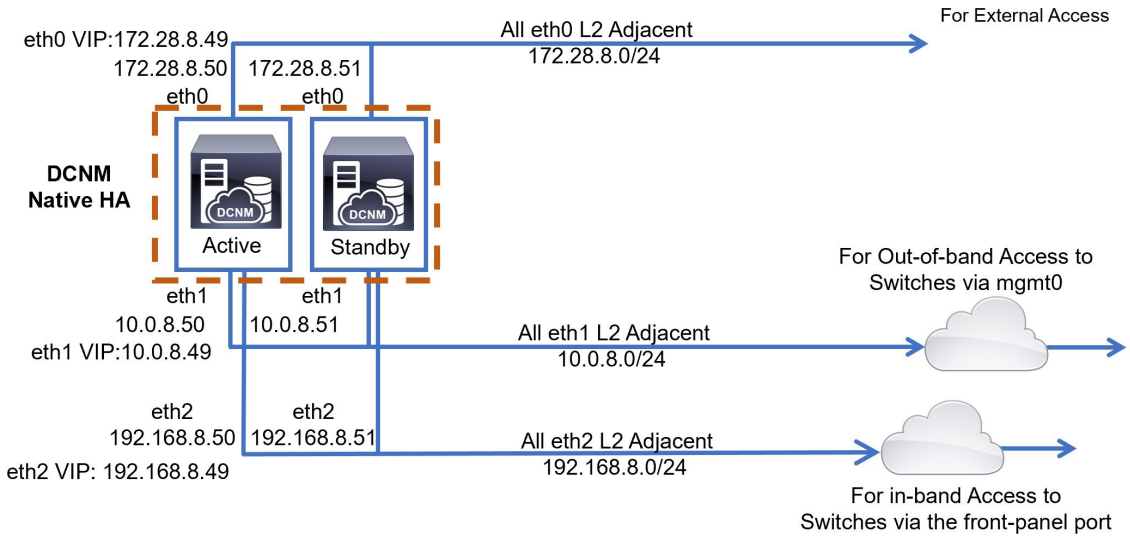
The possible deployments are as follows:

- Cisco DCNM Unclustered mode, on page 66
- Cisco DCNM Clustered Mode, on page 67

Cisco DCNM Unclustered mode

Figure 11: Cisco DCNM Standalone Deployment without Compute Cluster

Figure 12: Cisco DCNM HA Deployment without Compute Cluster



Cisco DCNM Clustered Mode

Figure 13: Cisco DCNM Standalone Deployment with Compute Cluster

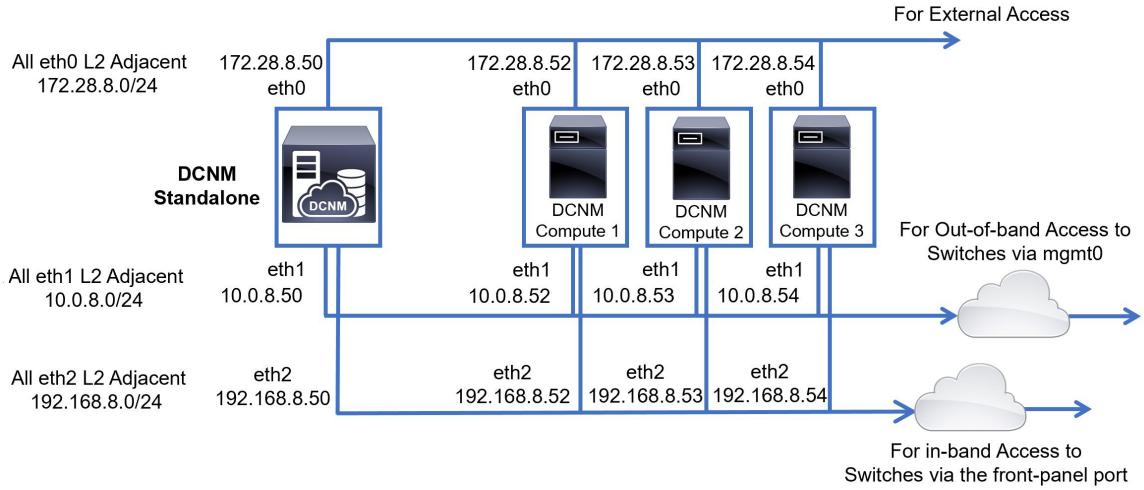
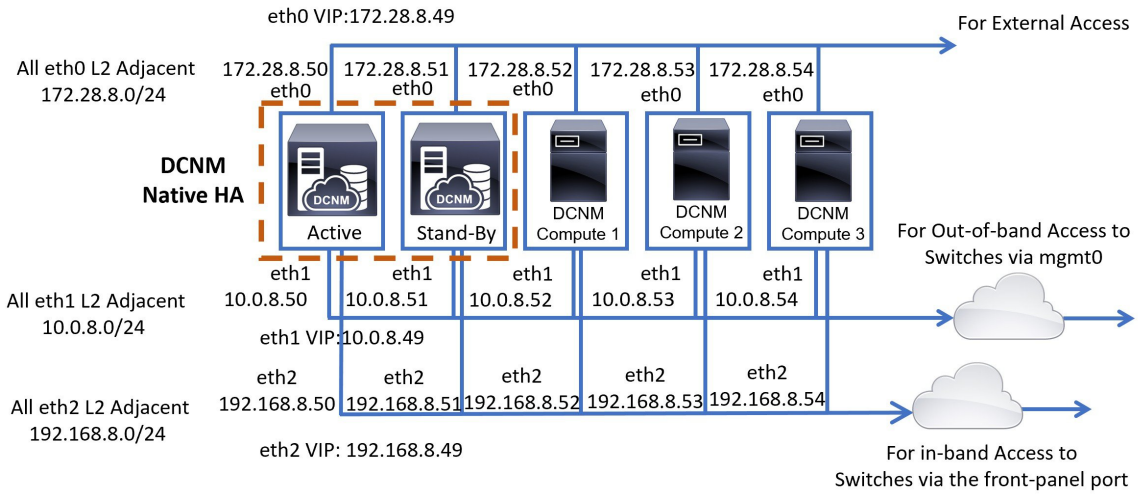


Figure 14: Cisco DCNM HA Deployment with Compute Cluster



Scenario 2: eth2 Interface in Different Subnet

In this scenario, consider that the eth0 and eth1 interfaces are in the same subnet, and eth2 interfaces of DCNMs and Computes are in a different subnet.

For example:

- eth0 – 172.28.8.0/24
- eth1 – 172.28.8.0/24
- eth2 – 192.168.8.0/24

The possible deployments are as follows:

- Cisco DCNM Unclustered Mode, on page 69
- Cisco DCNM Clustered Mode, on page 70

Cisco DCNM Unclustered Mode

Figure 15: Cisco DCNM Standalone deployment (No HA) without Compute Cluster

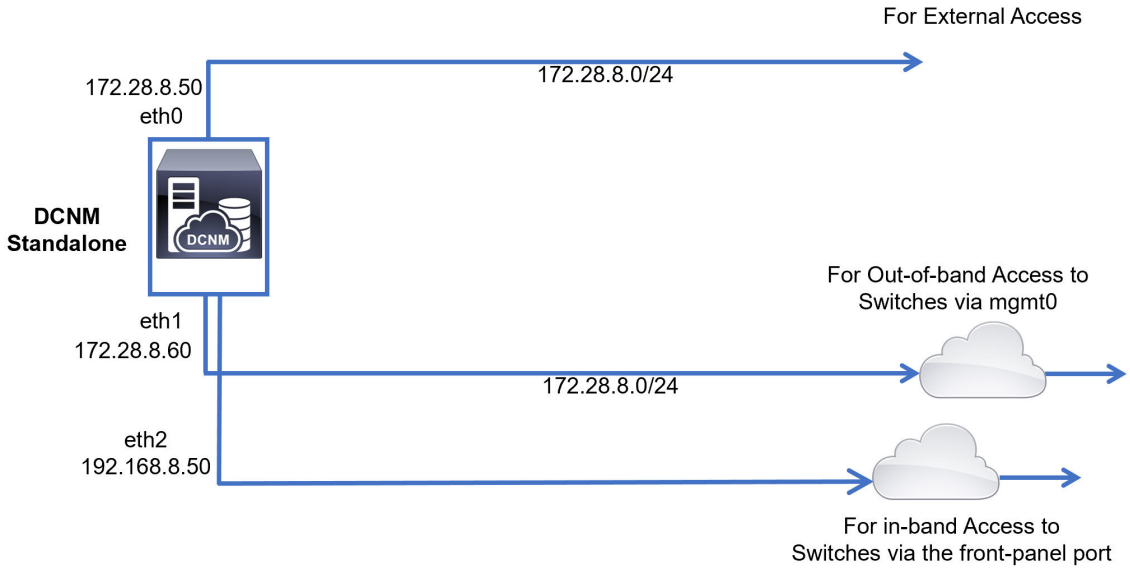
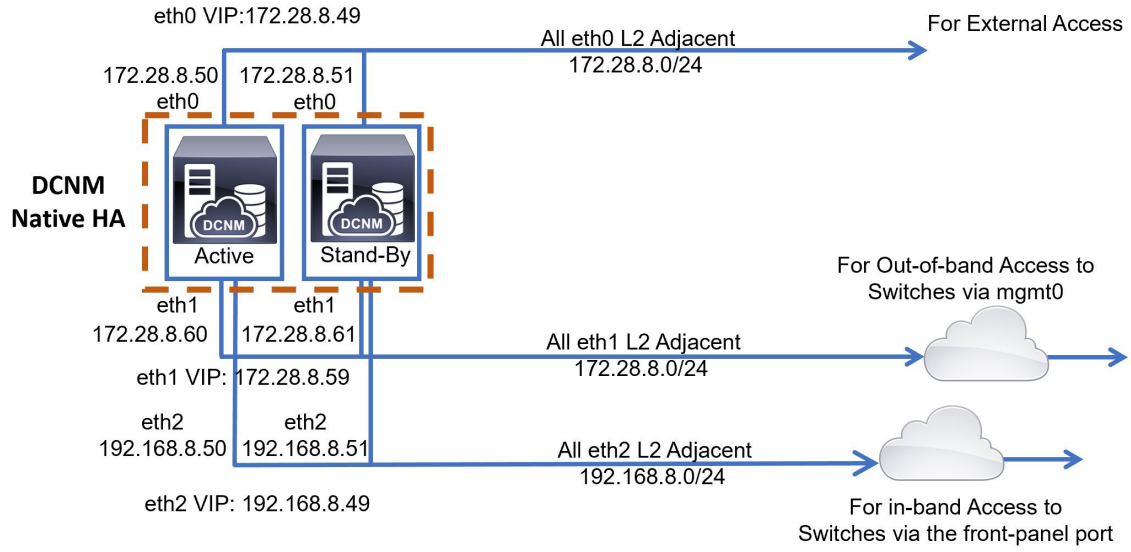


Figure 16: Cisco DCNM Native HA deployment without Compute Cluster



Cisco DCNM Clustered Mode

Figure 17: Cisco DCNM Standalone Deployment with Compute Cluster

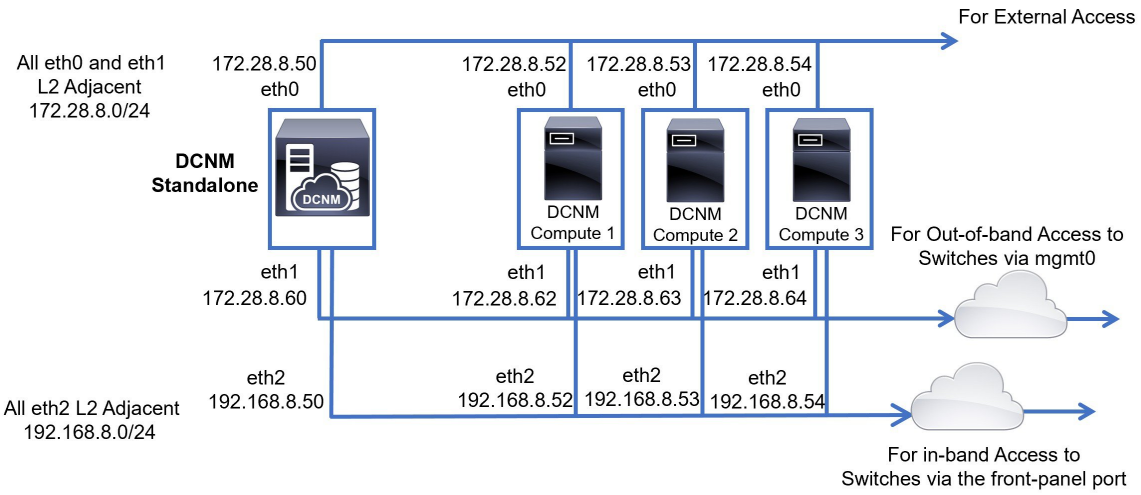
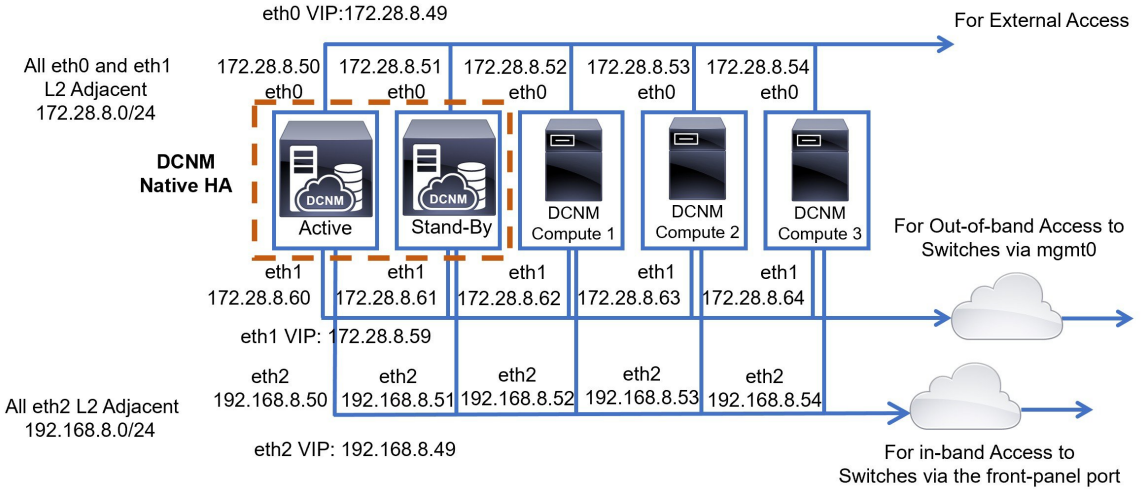


Figure 18: Cisco DCNM Native HA Deployment with Compute Cluster



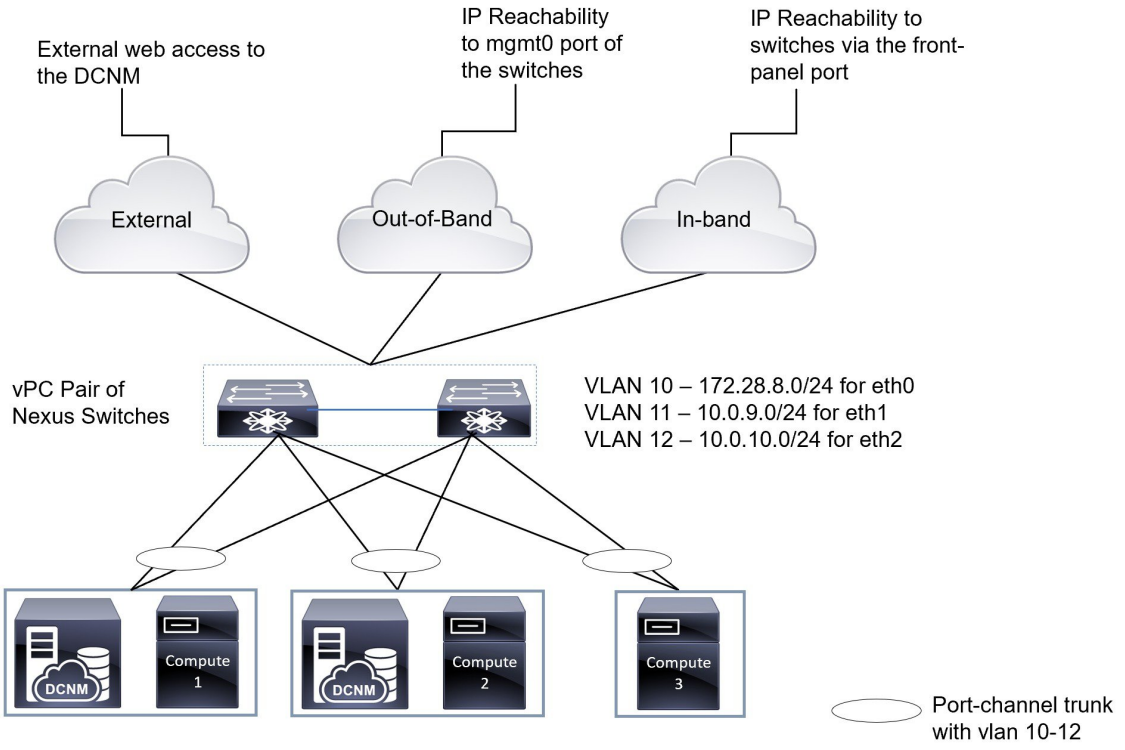
Physical Connectivity of Cisco DCNM and Compute Nodes

This section describes the physical connectivity of the Cisco DCNM and Compute nodes in both Virtual Machines and Bare Metal installations.

Virtual Machines

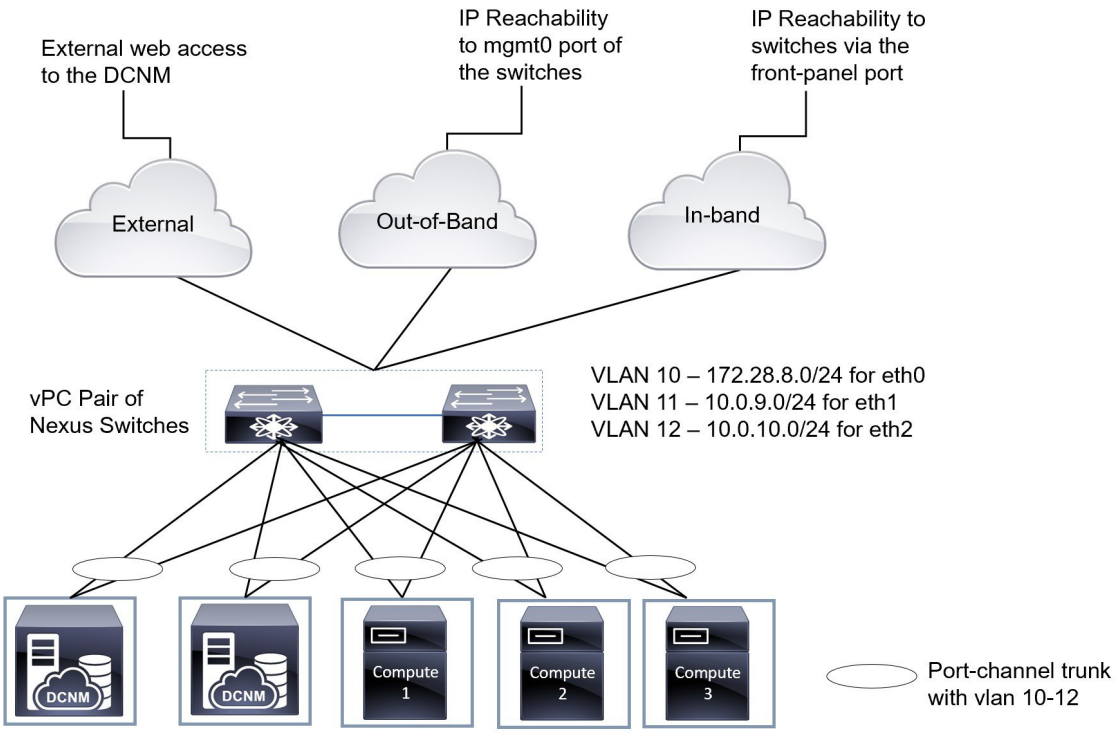
The following image shows the physical connectivity of DCNM and compute nodes supported in a 3 server redundancy configuration. The physical servers must be connected to a vPC pair of switches via port-channels. This provides adequate fault-tolerance, if a single link fails or a single switch fails. The vPC pair of switches is considered as the infra vPC pair that provides management connectivity to the physical servers.

Figure 19: Cisco DCNM VM Physical Connectivity with 3 servers



The following image shows the physical connectivity of Cisco DCNM and Compute nodes supported in an VM installation in a 5 server redundancy configuration.

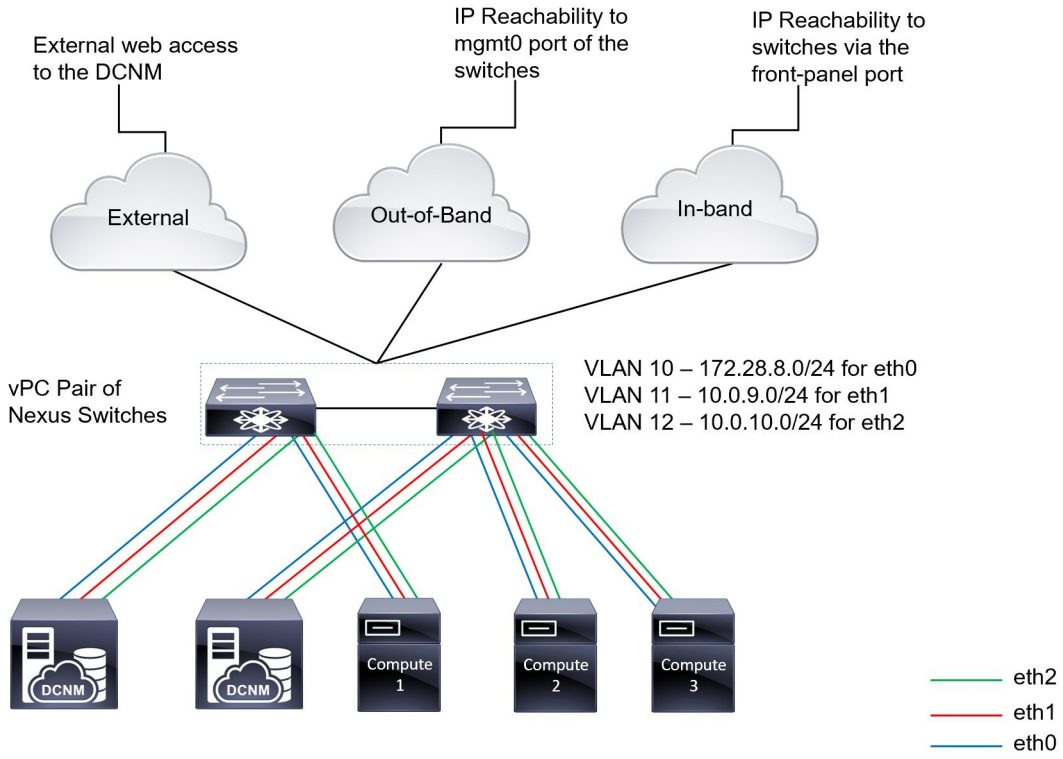
Figure 20: Cisco DCNM VM Physical Connectivity with 5 servers

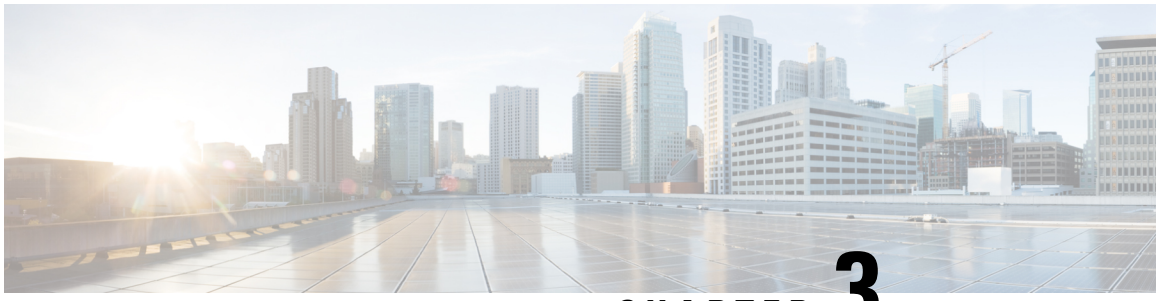


Bare Metal Installation

For installing Cisco DCNM on Bare Metal, 5 servers are required. The following image shows the physical connectivity of Cisco DCNM and Compute nodes. Note that, there are 3 physical interfaces on each server that map to the eth0, eth1, and eth2 interfaces, respectively. If the physical server consists of a managed network adapter such as the Cisco UCS VIC 1455 Virtual Interface Card, you can have a port-channel connectivity from the servers to the switches, similar to the Virtual Machines.

Figure 21: Cisco DCNM and Compute Bare Metal Physical Connectivity





CHAPTER 3

Disaster Recovery (Backup and Restore)

This chapter contains the following sections:

- Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup, on page 75
- Backup and Restore Cisco DCNM and Application Data on Native HA setup, on page 76
- Recovering Cisco DCNM Single HA Node, on page 77
- Recovering admin Account, on page 79
- HA Disaster Avoidance using SRM, on page 80
- Backup and Restore Cisco DCNM on a Cluster Setup, on page 82

Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to , the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

Perform the following task to take a backup of Cisco DCNM and Application data.

Procedure

Step 1 Logon to the Cisco DCNM appliance using SSH.

Step 2 Take a backup of the application data using the **appmgr backup** command.

```
dcnm# appmgr backup
```

From Release 11.4(1), Cisco DCNM allows you to configure a cron job that allows saves the backup to a remote scp server. Use **appmgr backup schedule** command to configure a scheduled backup.

```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:[<dir>]]
```

Copy the backup file to a safe location and shut down the DCNM Appliance.

Step 3 Right click on the installed VM and select **Power** > **Power Off**.

Step 4 Deploy the new DCNM appliance.

Step 5 After the VM is powered on, click on **Console** tab.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

Step 6 On the DCNM Web Installer UI, click **Get Started**.

Step 7 On the Cisco DCNM Installer screen, select radio button.

Select the backup file that was generated in Step 2, on page 75.

Continue to deploy the DCNM.

Step 8 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

Step 9 After the data is restored, check the status using the **appmgr status all** command.

Backup and Restore Cisco DCNM and Application Data on Native HA setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to , the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

Perform the following task to take perform backup and restore of data in a Native HA setup.

Before you begin

Ensure that the Active node is operating and functional.

Procedure

Step 1 Check if the Active node is operational. Otherwise, trigger a failover.

Step 2 Logon to the Cisco DCNM appliance using SSH.

Step 3 Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.

```
dcnm1# appmgr backup
dcnm2 appmgr backup
```

From Release 11.4(1), Cisco DCNM allows you to configure a cron job that allows saves the backup to a remote scp server. Use **appmgr backup schedule** command to configure a scheduled backup.

```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:[<dir>]]
```

Copy the backup file of both active and standby appliances to a safe location and shut down the DCNM Appliance.

Step 4 Right click on the installed VM and select **Power > Power Off**.

Step 5 Deploy the new DCNM appliance in Native HA mode.

Step 6 For both the Active and Standby appliances, after the VM is powered on, click on **Console** tab.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

Step 7 On the DCNM Web Installer UI, click **Get Started**.

Step 8 On the Cisco DCNM Installer screen, select radio button.

Select the backup file that was generated in Step Step 3, on page 77.

The values for parameters are read from the backup file, and auto-populated. Modify the values, if required.

Continue to deploy the DCNM.

Step 9 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

Step 10 After the data is restored, check the status using the **appmgr status all** command.

Recovering Cisco DCNM Single HA Node

This section details the scenarios and provides instructions to recover Cisco DCNM Single HA node.

The following table details all the recovery procedures when one or both the nodes fail in a Cisco DCNM Native HA set up.

Failure type	Node/Database to recover	Primary backup available	Secondary backup available	Recovery procedure
Primary node is lost. Secondary node is now Primary (due to fail over).	Primary Node	—	—	1. Convert Secondary node to Primary node. 2. Configure new Secondary node.
Primary and Secondary server database is lost. Secondary node is now Primary (due to fail over)	Primary database	—	—	The Active Secondary node will restart and sync to the Standby Primary node.
Active Secondary node is lost. Primary node is now active due to fail over.	Secondary node	—	No	Configure new Secondary node.
Active Secondary node is lost. Primary node is not active due to fail over.	Secondary node	—	Yes	Configure new Secondary node, using the Web Installer. Choose **Fresh installation with backup file for restore**. Select **Restore secondary DCNM node only** in HA settings screen.
Secondary standby node is lost.	Secondary node	—	No	Configure new Secondary node.
Secondary standby node lost	Secondary node	—	Yes	Configure new Secondary node, using the Web Installer. Choose **Fresh installation with backup file for restore**. Select **Restore secondary DCNM node only** in HA settings screen.
Primary node is active. Secondary standby database lost.	Secondary database	—	—	Primary node will restart to sync with Secondary node.

Converting Secondary node to Primary node

To convert the secondary node to Primary node, perform the following steps:

1. Log on to the DCNM server via SSH on the Secondary node.
2. Stop all the applications on the Secondary node by using the **appmgr stop all** command.
3. Navigate to the `/root/packaged-files/properties/ha-setup.properties` file.
4. Set the node ID to 1 to configure the secondary node as the primary node.

```
NODE_ID 1
```

After you change the node ID for the secondary node to 1, reboot the server. The old Secondary will restart as the new Primary Node. Consider the lost Primary as lost secondary node, and configure the new secondary node.

Configuring Secondary node

To configure the secondary node, perform the following steps:

1. Install a standalone Cisco DCNM. Use the same configuration settings as the lost secondary node.

Note If the Primary node was lost, and the old secondary node was converted to primary node, configure the new standalone node with the lost primary configuration.

2. Log on to the new DCNM standalone server via SSH, and stop all applications, using the **appmgr stop all** command.
3. Provide access to the `/root` directory on the new node, using the **appmgr root-access permit**.
4. Log on to the primary node via SSH, and stop all applications, using the **appmgr stop all** command.
5. Provide access to the `/root` directory on the Primary node, using the **appmgr root-access permit**.
6. On the Primary node, edit the `/root/.DO_NOT_DELETE` file. Set the **NATIVE_HA_STATUS** parameter to **NOT_TRIGGERED** on the primary node.
7. Configure the Primary node as Active, using the **appmgr setup native-ha active** command.
8. Configure the Secondary node as Standby, using the **appmgr setup native-ha standby** command.

Recovering admin Account

If you have the network-admin user/password credentials, you can login and recover the password for other users from the Cisco DCNM Web UI. See Step 5, on page 80.

To recover the Cisco DCNM Web UI user or password, perform the following steps:

Before you begin

Ensure that you have privileges to change the password.

Procedure

Step 1 Launch SSH and login to the DCNM server as a **/root** user.

```
[root@dcnm]#
```

Step 2 Navigate to `/usr/local/cisco/dcm/fm/bin` folder.

```
[root@dcnm]# cd /usr/local/cisco/dcm/fm/bin
[root@dcnm bin]#
```

Step 3 Execute **addUser.sh** script to create a new network-admin user. Provide a new username, password and the database password.

```
[root@dcnm bin]# ./addUser.sh <user> <password> <dbpassword>
```

The following message is generated and a new user is created.

```
----------------------- OUTPUT ----------------------------
----insertUser--------
----username----------john123
----role--------------network-admin
----insertUser--------done...
    Added user : john123 successful!
----------------------- END -----------------------------
```

Step 4 Login to the Cisco DCNM Web UI with new user to Cisco DCNM Web UI.

Step 5 Choose **Administration > Management Users > Local**.

The new user is displayed in the list.

Step 6 Select the user to recover the password, and click **Edit** icon.

Step 7 On the Edit User window, modify the **Role** and **Password** for the user.

You can also set the password to expire in 180 days.

Step 8 Click **Apply** to save your changes.

HA Disaster Avoidance using SRM

Cisco DCNM Release 11.5(1) can be successfully deployed on the VM Site Recovery Manager (SRM). SRM is a disaster recovery software that provides automated orchestration of failover and fail-back to minimize downtime.

Note This document provides a high-level work flow. Fro detailed information, refer to https://docs.vmware.com/en/Site-Recovery-Manager/index.html.

To setup the DCNM and migrate to SRM, perform the following task:

1. Configure a management server (ESXi 6.7) running vCenter, SRM, VM replicator manager running on Site 1.
2. Similarly, configure a management server (ESXi 6.7) running vCenter, SRM, VM replicator manager running on Site 2.

   VRM helps replicate VMs from one site to another.

Note All VMs must be deployed together in the same site. When migrating DCNM VMs (planned recovery or disaster recovery), all DCNM VMs must be migrated to the recovery site.

3. Replicate Site1 to Site2 to sync.
4. Migrate Site1 and Site2 to the Site Recovery Manager.
5. Deploy the VMs on the Recovery Site.

Compatibility:

- ESXi 6.7
- SRM 8.3

To configure the SRM for DCNM HA disaster recovery, perform the following task:

1. Launch the SRM.
2. Pair Site1 and Site2. After the replication is complete, both the Sites are synchronized.
3. Click View Details.

   The Summary page opens.
4. On the Summary tab,
   a. Click Network Mappings and map the networks used by the VM on both Site1 and Site2.
   b. Click Folder Mappings. Map all the folders used by vCenter for the VMs.
   c. Click Resource Mappings. Map the resources on each component in Site1 to components in Site2. Choose Yes under Reverse Mapping.
   d. Click on Placeholder Datastores. Map hosts/clusters to the correct datastores. For example, the VMs in the Host/Cluster will be replicated to the mapped Datastore.

Note Ensure that VMs are replicated to the correct datastores. Recovery plan fails, otherwise.

5. On the Replications tab
   a. Replicate VMs from a source site to a target site with vSphere Replication.
   b. Click Outgoing in the left pane. All the data synchronized with site2 are displayed.
   c. If you're on Site1 and everything replication on Site2, this tab will be empty.
   d. Click Incoming in the left pane. Status of all the VMs synchronizing with Site2 are displayed.
   e. Configure a Recovery Point Objective (RPO) value during replication configuration, to determine the maximum data loss that you can tolerate.
   f. Click New to configure Replication Latency to configure the Recovery Point Objective. Click on the arrow before the VM to view configuration data for the VM.
6. On the Protection Groups tab:

   Configure one or more protection groups in a recovery plan. A recovery plan specifies how Site Recovery Manager recovers the virtual machines in the protection groups that it contains.
7. On the Recovery Plans tab,

   After you configure Site Recovery Manager at the protected and recovery sites, you can create, test, and run a recovery plan.
   a. When you create or modify a recovery plan, test it before you try to use it for planned migration or for disaster recovery.

b. You can run a recovery plan under planned circumstances to migrate virtual machines from the protected site to the recovery site. If the protected site suffers an unforeseen event that might result in data loss, you can also run a recovery plan under unplanned circumstances.

c. You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

d. Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

e. You can choose one of the recovery type:

- **Planned migration** – replicates recent changes to the recovery site and cancel recovery if errors are encountered. Do not perform and resource intense operations during planned migration.
- **Disaster recovery** – attempts to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. It continues the recovery even if errors are encountered.

f. Click on … after Run and click Reprotect to protect the VMs or click Cancel to stop the recovery plan.

After Site Recovery Manager performs a recovery, the virtual machines start up on the recovery site. By running reprotect when the protected site comes back online, you reverse the direction of replication to protect the recovered virtual machines on the recovery site back to the original protected site.

Backup and Restore Cisco DCNM on a Cluster Setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Perform the following task to take perform backup and restore of data in a Cisco DCNM Cluster setup.

Before you begin

Check and ensure that the Active and Standby servers are operational, using the appmgr show ha-role command.

Example:

On the Active node:

```
dcnm-active# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node:

```
dcnm2-standby# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Procedure

Step 1 Log on to the Cisco DCNM appliance using SSH.

Step 2 Take a backup of the application data using the **appmgr backup** command on both Active, Standby appliances, and on all Compute nodes.

```
dcnm-active# appmgr backup
dcnm-standby# appmgr backup
dcnm-compute1# appmgr backup
dcnm-compute2# appmgr backup
dcnm-compute3# appmgr backup
```

Copy the backup files of all nodes to a safe location and shut down the DCNM Appliance.

Step 3 Right click on the installed VM and select **Power > Power Off**.

Step 4 Install two Cisco DCNM Release 11.5(3a) appliances.

Note Ensure that the Hostnames match the earlier Active and Standby appliances.

For instructions, see Installing the Cisco DCNM.

Step 5 Install three Cisco DCNM Compute nodes.

Note Ensure that the Hostnames match the earlier Compute nodes.

For instructions, see Installing Cisco DCNM Compute Node.

Step 6 Provide access to the `/root` directory on all nodes using the following command.

```
dcnm# appmgr root-access permit
```

Step 7 Stop telemetry on Active and Standby nodes using the following command:

```
dcnm-active# systemctl stop pmn-telemetry
dcnm-standby# systemctl stop pmn-telemetry
```

Step 8 Set the environment variable to allow restore process using CLI and restore the node with the same hostname as respective Active and Standby backup files, using the following command:

Note Ensure that you perform the restore in the same order—Active, Standby, Compute1, Compute2, and Compute3.

```
dcnm-active# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm1-backup-file>
dcnm-standby# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm2-backup-file>
dcnm-compute1# APPMGR_ALLOW_RESTORE=1 appmgr restore <compute1-backup-file>
dcnm-compute2# APPMGR_ALLOW_RESTORE=1 appmgr restore <compute2-backup-file>
dcnm-compute3# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm2-backup-file>
```

Step 9 After the data is restored, check the status using the **appmgr status all** command.

What to do next

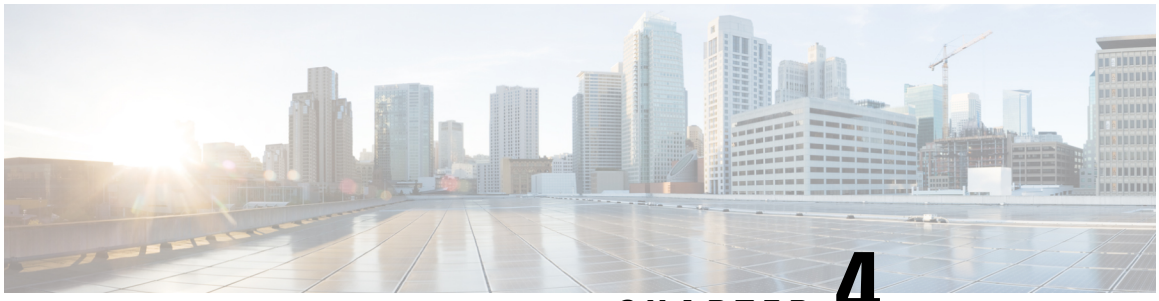
Log on to the DCNM Web UI with appropriate credentials.

The Applications tab displays all the services running on the DCNM deployment that you have installed. Click Compute tab to view the new Compute in Discovered state on the Cisco DCNM Web UI.

To add the compute nodes to a cluster, see Adding Computes to a Cluster Node in your deployment-specific *Cisco DCNM Configuration Guide* for more information.

Note If you didn't enable clustered mode while installing DCNM, use the **appmgr afw config-cluster** command to enable the compute cluster. For instructions, refer to Enabling the Compute Cluster in the Cisco DCNM LAN Fabric Configuration Guide.

When a compute node goes through an unscheduled powercycle and restarts, the Elasticsearch container won't start. It's possible that some filesystems are corrupted. To resolve this issue, reboot the Compute node in safe mode by using **fsck -y** command.



CHAPTER 4

Managing Utility Services After DCNM Deployment

This chapter describes how to verify and manage all of the utility services that provide DC3 (Programmable Fabric) central point of management functions after the DCNM is deployed.

Table 5: Cisco DCNM Utility Services

Category	Application	Username	Password	Protocol Implemented
Network Management	Data Center Network Manager	admin	User choice [3]	Network Management

[3] User choice refers to the administration password entered by the user during the deployment.

This chapter contains the following sections:

- Editing Network Properties Post DCNM Installation, on page 85
- Convert Standalone Setup to Native-HA Setup, on page 94
- Utility Services Details, on page 98
- Managing Applications and Utility Services , on page 99
- Updating the SFTP Server Address for IPv6, on page 102

Editing Network Properties Post DCNM Installation

The Cisco DCNM OVA or the ISO installation consists of 3 network interfaces:

- dcnm-mgmt network (eth0) interface

  This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. Associate this network with the port group that corresponds to the subnet that is associated with the DCNM Management network.

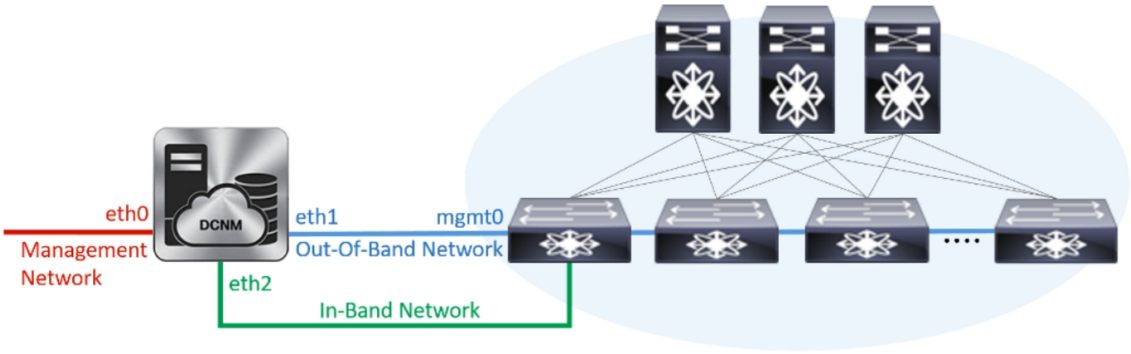
- enhanced-fabric-mgmt (eth1) interface

  This network provides enhanced fabric management of Nexus switches. Associate this network with the port group that corresponds to management network of leaf and spine switches.

- enhanced-fabric-inband (eth2) interface

This network provides in-band connection to fabric. Associate this network with the port group that corresponds to a fabric in-band connection.

The following figure shows the network diagram for the Cisco DCNM Management interfaces.



During Cisco DCNM installation for your deployment type, you can configure these interfaces. However, from Cisco DCNM Release 11.2(1), you can edit and modify the network settings post installation.

Note We recommend that you use **appmgr** commands to update network properties. Do not restart network interfaces manually.

You can modify the parameters as explained in the following sections:

Modifying eth0 IP Address of DCNM Compute Cluster

Note Execute the following commands on the DCNM Appliance console to avoid a premature session timeout.

Ensure that you execute the commands in the same order as mentioned in the following steps.

Note When DCNM is onboarded to Cisco Multi-Site orchestrator, if you change the In-band network properties, you must re-register the site on Nexus Dashboard. For Native HA appliance, wait until the HA nodes establish connectivity before you re-register the sites on Nexus Dashboard. For instructions, refer to Editing Sites section in , Cisco Nexus Dashboard User Guide.

You must re-register site for fabrics in each DCNM instance. Save the settings.

If you've multiple DCNM instances on Cisco Multi-Site Orchestrator, you must deploy the infra to update the names of the fabric with the IP addresses of the remote fabric. For instructions, see Deploying Infra Configuration.

To change the eth2 and eth IP Addresses, perform the following steps:

1. On Standby DCNM Node:

appmgr stop all

2. On Active DCNM Node:

   appmgr stop all

3. On Active DCNM Node:

   appmgr update network-properties session start

   appmgr update network-properties set ipv4 eth0 <*ipv4 address*> <*netmask*> <*gateway*>

   appmgr update network-properties set ipv4 peer0 <*ipv4-address*>

   appmgr update network-properties set ipv4 vip0 <*ipv4-address*>

   appmgr update network-properties session apply

4. On Standby DCNM Node:

   appmgr update network-properties session start

   appmgr update network-properties set ipv4 eth0 <*ipv4 address*> <*netmask*> <*gateway*>

   appmgr update network-properties set ipv4 peer0 <*ipv4-address*>

   appmgr update network-properties set ipv4 vip0 <*ipv4-address*>

   appmgr update network-properties session apply

5. On Active DCNM Node:

   appmgr update ssh-peer-trust

   appmgr start all

6. On Standby DCNM Node:

   appmgr update ssh-peer-trust

   appmgr start all

7. On all Compute Nodes:

Note Execute the commands on Compute 1, and then on Compute Node 2 and later on Compute 3.

   appmgr stop all

   appmgr update network-properties session start

   appmgr update network-properties set ipv4 eth0 <*ipv4 address*> <*netmask*> <*gateway*>

   appmgr update network-properties session apply

   appmgr afw dcnm-ip <*new-vip0-of-dcnm-server*>

   appmgr start all

8. Ensure that the Active and Standby DCNM Nodes are in a HA pair.

   - On Active DCNM Node:

     appmgr show ha-role

- On Standby DCNM Node:

  appmgr show ha-role

9. On the Compute Node:

   afw compute list --brief

Note This command list all three old computes in **Offline** state. If you have also modified the DNS names for all of the nodes, the Compute Nodes are in **Discovered** state.

   afw apps list --brief

   docker service ls

Moving the Nodes to a new location

You can move all the nodes to the new location and wire them up. By using the Console, run the following on the DCNM nodes:

appmgr show ha-role

Access the DCNM **Web UI > Applications > Compute**. All three computes are in **Offline** state.

Adding Compute Nodes back to the Cluster

On the Cisco DCNM Web UI, you can add the new Compute nodes. Choose **DCNM Web UI > Applications > Compute** and perform the following steps:

Note Execute the commands on Compute 1, and then on Compute Node 2 and later on Compute 3.

1. Delete one old Compute in Offline state.
2. Refresh the table to see new IP to show up in Discovered state.
3. Add the Discovered compute corresponding to the deleted one into the cluster on the Cisco DCNM Web UI.
4. Repeat the process one at a time for each Compute Node.

After executing for all three Compute Nodes, all the computes are in **Joined** state and the cluster is functional.

Modifying eth2 and eth1 IP Addresses of DCNM Compute Cluster

Note Execute the following commands on the DCNM Appliance console to avoid a premature session timeout.

Ensure that you execute the commands in the same order as mentioned in the following steps.

To change the eth2 and eth1 IP Addresses, perform the following steps:

1. On Standby DCNM Node:

   appmgr stop all

2. On Active DCNM Node:

   appmgr stop all

3. On Active DCNM Node:

   appmgr update network-properties session start

   appmgr update network-properties set ipv4 eth2 *<ipv4 address> <netmask> <gateway>*

   appmgr update network-properties set ipv4 peer2 *<ipv4-address>*

   appmgr update network-properties set ipv4 vip2 *<ipv4-address>*

   appmgr update network-properties set ipv4 eth1 *<ipv4 address> <netmask> <gateway>*

   appmgr update network-properties set ipv4 peer1 *<ipv4-address>*

   appmgr update network-properties set ipv4 vip1 *<ipv4-address>*

   appmgr update network-properties session apply

4. On Standby DCNM Node:

   appmgr update network-properties session start

   appmgr update network-properties set ipv4 eth2 *<ipv4 address> <netmask> <gateway>*

   appmgr update network-properties set ipv4 peer2 *<ipv4-address>*

   appmgr update network-properties set ipv4 vip2 *<ipv4-address>*

   appmgr update network-properties set ipv4 eth1 *<ipv4 address> <netmask> <gateway>*

   appmgr update network-properties set ipv4 peer1 *<ipv4-address>*

   appmgr update network-properties set ipv4 vip1 *<ipv4-address>*

   appmgr update network-properties session apply

5. On Active DCNM Node:

   appmgr start all

6. On Standby DCNM Node:

   appmgr start all

7. On all Compute Nodes:

Note Execute the commands on Compute 1, and then on Compute Node 2 and later on Compute 3.

   appmgr stop all

   appmgr update network-properties session start

   appmgr update network-properties set ipv4 eth2 *<ipv4 address> <netmask> <gateway>*

   appmgr update network-properties set ipv4 eth1 *<ipv4 address> <netmask> <gateway>*

appmgr update network-properties session apply

appmgr start all

Note Ensure that the DCNM Web UI is operational, and **Applications > Catalog** displays the catalog list and the compute list.

8. On the Active DCNM Node:

   afw apps stop --app NIALite_Cisco_afw

   sleep 300 (wait for 5 mins)

   appmgr afw config-pool --ibpool <*inband-subnet/mask*>

9. On the Standby DCNM Node:

   appmgr afw config-pool --ibpool <*inband-subnet/mask*>

Note Ensure that the DCNM Web UI is operational, and **Applications > Catalog** displays the catalog list and the compute list.

10. On Active DCNM Node:

    afw apps stop --app NIALite_Cisco_afw

    sleep 300 (wait for 5 mins)

    appmgr afw config-pool --oobpool <*OutOfBand-subnet/mask*>

11. On Standby DCNM Node:

    appmgr afw config-pool --oobpool <*OutOfBand-subnet/mask*>

To validate the network properties:

- **ip address show eth1**
- **ip address show eth2**

To verify **docker** information:

1. **docker info**
2. **docker node ls**
3. **docker service ls**

Nexus Dashboard Properties Modifications

When DCNM is onboarded to Nexus Dashboard via Cisco Multi-Site Orchestrator, DCNM stores Nexus Dashboard information such as cluster name, serial number and data IP address of the nodes. If any of these parameters is modified when migrating a cluster on Nexus Dashboard, Release 11.5(3a) provides a set of APIs that you can call to update information about the new cluster.

If Nexus Dashboard node list is provided in the API data, it removes all existing nodes and adds the newly provided nodes. If Nexus Dashboard node list is not provided in the API, it uses the existing ND node data to modify the cluster name.

Payload

curl --insecure -X PUT -H "Dcnm-Token: $token" -H 'Content-Type: application/json' https://$ip/rest/nexusdashboard/replace-cluster/ND-GR-DCNM --data '

```
{
    "clusterName":"ND-G-RESEARCH",
    "nodes":
    [
        {
            "serialNumber":"WZP23470JUS",
            "ipAddress":"8.1.168.172",
            "role":"Master"
        },
        {
            "serialNumber":"WZP23470JZF",
            "ipAddress":"8.1.168.173",
            "role":"Master"
        },
        {
            "serialNumber":"WZP23470JY2",
            "ipAddress":"8.1.168.174",
            "role":"Master"
        }
    ]
}
```

Changing the DCNM Server Password on Standalone Setup

The password to access Cisco DCNM Web UI is configured while installing the Cisco DCNM for your deployment type. However, you can modify this password post installation also, if required.

To change the password post installation, perform the following steps:

Procedure

Step 1 Stop the applications using the **appmgr stop all** command.

Wait until all the applications stop running.

Step 2 Change the password for the management interface by using the **appmgr change_pwd ssh {root|poap|sysadmin}**[*password* command.

Ensure that the new password adheres to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password: <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Step 3 Start the application using the **appmgr start all** command.

Example

```
dcnm# appmgr stop all

dcnm# appmgr change_pwd ssh root <<new-password>>
dcnm# appmgr change_pwd ssh poap <<new-password>>
dcnm# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm# appmgr start all
```

Changing the DCNM Server Password on Native HA Setup

The password to access Cisco DCNM Web UI is configured while installing the Cisco DCNM for your deployment type. However, you can modify this password post installation also, if required.

To change the password post installation, perform the following steps:

Procedure

Step 1 Stop all the applications on the Standby appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 2 Stop all the applications on the Active appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 3 Change the password for the management interface by using the **appmgr change_pwd ssh {root|poap|sysadmin}**[*password*] command. on both Active and Standby nodes.

Note You provide the same password for both the nodes at the prompt.

Ensure that the new password adheres to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password: <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Step 4 Start the applications on the Active appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Step 5 Start the applications on the Standby appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Example

Let us consider Active and standby as dcnm1 and dcnm2, respectively.

```
dcnm1# appmgr stop all
dcnm2# appmgr stop all

dcnm1# appmgr change_pwd ssh root <<new-password>>
dcnm1# appmgr change_pwd ssh poap <<new-password>>
dcnm1# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm2# appmgr change_pwd ssh root <<new-password>>
dcnm2# appmgr change_pwd ssh poap <<new-password>>
dcnm2# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm1# appmgr start all
dcnm2# appmgr start all
```

Changing the DCNM Database Password on Standalone Setup

To change the Postgres database password on Cisco DCNM Standalone setup, perform the following steps:

Procedure

Step 1 Stop all the applications using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 2 Change the Postgres password by using the **appmgr change_pwd db** command.

Provide the new password at the prompt.

Step 3 Start the application using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Example

```
dcnm# appmgr stop all
dcnm# appmgr change_pwd db <<new-password>>
dcnm# appmgr start all
```

Changing the DCNM Database Password on Native HA Setup

To change the Postgres database password on Cisco DCNM Native HA setup, perform the following steps:

Procedure

Step 1 Stop all the applications on the Standby appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 2 Stop all the applications on the Active appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 3 Change the Postgres password by using the **appmgr change_pwd db** command on both Active and Standby nodes.

Ensure that you provide the same password at the prompt.

Step 4 Start the applications on the Active appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Step 5 Start the applications on the Standby appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Example

Let us consider Active and standby as **dcnm1** and **dcnm2**, respectively.

```
dcnm1# appmgr stop all
dcnm2# appmgr stop all

dcnm1# appmgr change_pwd db <<new-password>>
dcnm2# appmgr change_pwd db <<new-password>>

dcnm1# appmgr start all
dcnm2# appmgr start all
```

Convert Standalone Setup to Native-HA Setup

To convert an existing Cisco DCNM Standalone setup to a Native HA setup, perform the following steps:

Before you begin

Ensure that the Standalone setup is active and operational, by using the **appmgr show version** command.

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version:
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

Procedure

Step 1 On the Standalone setup, launch SSH and enable **root** user access by using the **appmgr root-access permit** command:

```
dcnm# appmgr root-access permit
```

Step 2 Deploy a new DCNM as secondary node. Choose **Fresh installation - HA Secondary**

For example, let us indicate the existing setup as **dcnm1** and the new DCNM as secondary node as **dcnm2**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the **Install Mode** tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note All the passwords must be same as the passwords that you provided while configuring the Primary node.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

  The value must be an IP or IPv6 address or RFC 1123 compliant name.

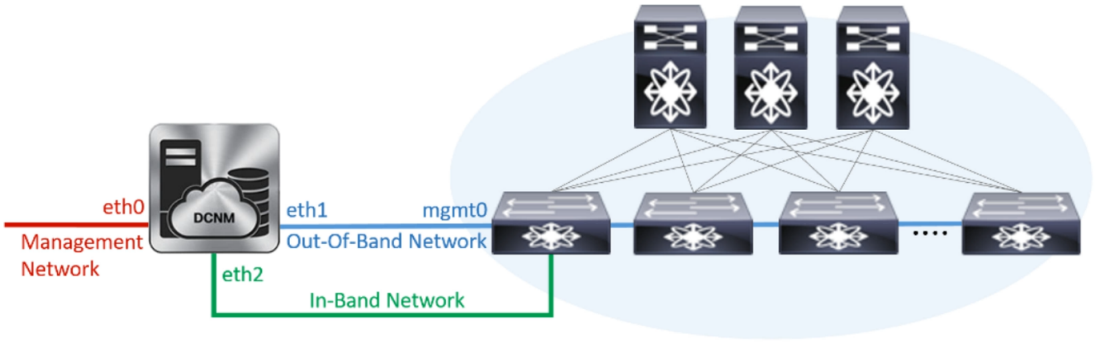
  From Release 11.3(1), you can configure more than one NTP server.

- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 22: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Ensure that the IP address belongs to the same Management Network configured on the Primary node.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

   Out-of-band management provides a connection to the device management ports (Typically mgmt0).

   Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

1. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.
2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.

- In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
- In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
- In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

  Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

  Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
- In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.
- In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

  Note This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.
- In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

  Note The configured IPv4 address must respond to the ICMP echo pings.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Verify the HA role by using the appmgr show ha-role command.

On the Active node (old standalone node):

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node (newly deployed node):

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Utility Services Details

This section describes the details of all the utility services within the functions they provide in Cisco DCNM. The functions are as follows:

Network Management

The data center network management function is provided by the Cisco Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser: `http://<<hostname/IP address>>`.

Note For more information about Cisco DCNM, see http://cisco.com/go/dcnm.

Orchestration

RabbitMQ

Rabbit MQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP). The RabbitMQ message broker sends events from the vCloud Director/vShield Manager to the Python script for parsing. You can configure this protocol by using certain CLI commands from the Secure Shell (SSH) console of the firmware.

Note You need to stop and restart AMQP on both DCNM's server in HA within 30 seconds, otherwise AMQP may not start. For more information about RabbitMQ, go to https://www.rabbitmq.com/documentation.html.

After upgrade, enable RabbitMQ management service stop the service and start the services using the following commands:

```
dcnm# appmgr stop amqp
dcnm# appmgr start amqp
```

If AMQP is not running. the memory space must be exhausted that is indicated in the file `/var/log/rabbitmq/erl_crash.dump`.

Device Power On Auto Provisioning

Power On Auto Provisioning (POAP) occurs when a switch boots without any startup configuration. It is accomplished by two components that were installed:

- DHCP Server

  The DHCP server parcels out IP addresses to switches in the fabric and points to the location of the POAP database, which provides the Python script and associates the devices with images and configurations.

  During the Cisco DCNM installation, you define the IP Address for the inside fabric management address or OOB management network and the subnets associated with the Cisco Programmable Fabric management.

- Repositories

  The TFTP server hosts boot scripts that are used for POAP.

  The SCP server downloads the database files, configuration files, and the software images.

Managing Applications and Utility Services

You can manage the applications and utility services for Cisco Programmable Fabric in the Cisco DCNM through commands in an SSH terminal.

Enter the **appmgr** command from the SSH terminal by using the following credentials:

- Username: **root**
- Password: **Administrative password provided during deployment**

Note For your reference, context sensitive help is available for the **appmgr** command. Use the **appmgr** command to display help.

Use the **appmgr tech_support** command to produce a dump of the log files. You can then provide this information to the TAC team for troubleshooting and analysis of your setup.

Note This section does not describe commands for Network Services using Cisco Prime Network Services Controller.

This section includes the following:

Verifying the Application and Utility Services Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of various applications and utility services that were deployed in the file. You can use the **appmgr status** command in an SSH session to perform this procedure.

Note Context-sensitive help is available for the **appmgr status** command. Use the **appmgr status ?** command to display help.

Procedure

Step 1 Open up an SSH session:

a) Enter the **ssh root DCNM network IP address** command.

b) Enter the administrative password to login.

Step 2 Check the status by using the following command:

appmgr status all

Example:

```
DCNM Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1891 root 20 02635m 815m  15m S  0.0 21.3    1:32.09  java

LDAP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1470 ldap      20   0  692m  12m 4508 S  0.0  0.3   0:00.02 slapd

AMQP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
```

```
1504 root      20   0 52068  772  268 S  0.0  0.0   0:00.00 rabbitmq

TFTP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1493 root      20   0 22088 1012  780 S  0.0  0.0   0:00.00 xinetd

DHCP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1668 dhcpd 20   0 46356 3724 408 S  0.0  0.0   0:05.23 dhcp
```

Stopping, Starting, and Resetting Utility Services

Use the following CLI commands for stopping, starting, and resetting utility services:

- To stop an application, use the **appmgr stop** command.

  ```
  dcnm# appmgr stop dhcp
  Shutting down dhcpd:     [  OK  ]
  ```

- To start an application, use the **appmgr start** command.

  ```
  dcnm# appmgr start amqp
  Starting vsftpd for amqp:     [  OK  ]
  ```

- To restart an application use the **appmgr restart** command.

  ```
  # appmgr restart tftp
  Restarting TFTP...
  Stopping xinetd:     [  OK  ]
  Starting xinetd:     [  OK  ]
  ```

Note From Cisco DCNM Release 7.1.x, when you stop an application by using the **appmgr stop** *app_name* command, the application will not start during successive reboots.

For example, if DHCP is stopped by using the **appmgr stop dhcp** command, and the OS is rebooted, the DHCP application will still be down after the OS is up and running.

To start again, use the command **appmgr start dhcp**. The DHCP application will be started after reboots also. This is to ensure that when an environment uses an application that is not packaged as part of the virtual appliance (like CPNR instead of DHCP), the application locally packaged with the virtual appliance will not interfere with its function after any OS reboots.

Note When a DCNM appliance (ISO/OVA) is deployed, the Cisco SMIS component will not get started by default. However, this component can be managed using the appmgr CLI: **appmgr start/stop dcnm-smis**

appmgr start/stop dcnm will start or stop only the DCNM web component.

Updating the SFTP Server Address for IPv6

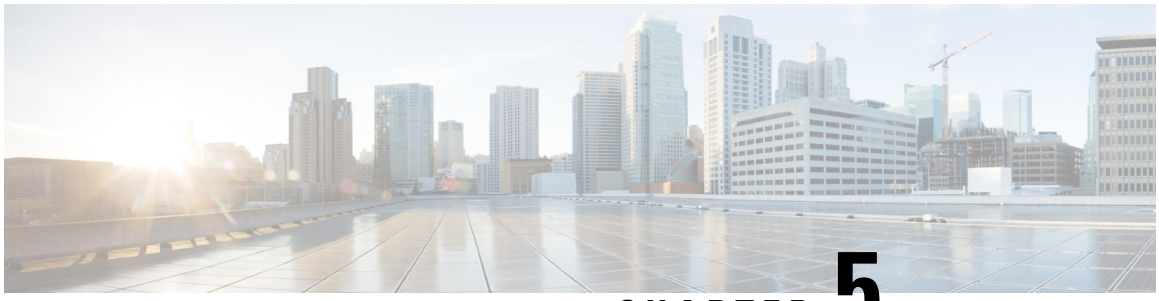
After deploying the DCNM OVA/ISO successfully with EFM IPv4 and IPv6, by default the SFTP address is pointed to IPv4 only. You need to change the IPv6 address manually in the following two places:

- In the DCNM Web Client, choose **Administration > Server Properties** and then update the below fields to IPv6 and click the **Apply Changes** button.

```
#_____________________________________________________________________
# GENERAL>xFTP CREDENTIAL
#
# xFTP server's ip address for copying switch files:
server.FileServerAddress
```

- Log in to the DCNM through ssh and update the SFTP address with IPv6 manually in the server.properties file (/usr/local/cisco/dcm/fm/conf/server.properties).

```
# xFTP server's ip address for copying switch files:
server.FileServerAddress=2001:420:5446:2006::224:19
```



CHAPTER 5

Installing Software Maintenance Update for log4j2 Vulnerability

- Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment, on page 103

Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment

Cisco DCNM provides a Software Maintenance Update (SMU) to address the **CVE-2021-45046 and CVE-2021-44228** issue in Release 11.5(3a).

This section contains the following topics:

Installing SMU on Cisco DCNM 11.5(3a) Standalone Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO in Standalone deployment mode, perform the following steps:

Before you begin

- Take a backup of the application data using the **appmgr backup** command on the DCNM appliance.

  ```
  dcnm# appmgr backup
  ```

  Copy the backup file to a safe location outside the DCNM server.

- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.

- Ensure that you plan for a maintenance window to install SMU.

- Ensure that Cisco DCNM 11.5(3a) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(3a) appliance

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

b) Locate **DCNM 11.5.3a Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

c) Save the **dcnm-va-patch.11.5.3a-p1.iso.zip** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **dcnm-va-patch.11.5.3a-p1.iso.zip** file and upload the file to the `/root/` folder in the DCNM node.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm# su
Enter the root password:
[root@dcnm]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm1]# mkdir -p /mnt/iso
```

Step 6 Mount the DCNM 11.5(3a) SMU file in the `/mnt/iso` folder.

```
[root@dcnm]# mount -o loop dcnm-va-patch.11.5.3a-p1.iso /mnt/iso
```

Step 7 Navigate to **/scripts/** directory.

```
[root@dcnm]# cd /mnt/iso/packaged-files/scripts/
```

Step 8 Run the **./inline-upgrade.sh** script.

```
[root@dcnm]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

Step 9 Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm]# appmgr status all
```

Step 10 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm]# exit
```

Step 11 Unmount the **dcnm-va-patch.11.5.3a-p1.iso** file from the DCNM setup.

Note You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm]# umount /mnt/iso
```

Installing SMU on Cisco DCNM 11.5(3a) Native HA Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO in Native HA deployment mode, perform the following steps:

Before you begin

- Check and ensure that the Active and Standby servers are operational, using the **appmgr show ha-role** command.

  Example:

  On the Active node:

  ```
  dcnm1# appmgr show ha-role
  Native HA enabled.
  Deployed role: Active
  Current role: Active
  ```

  On the Standby node:

  ```
  dcnm2# appmgr show ha-role
  Native HA enabled.
  Deployed role: Standby
  Current role: Standby
  ```

- Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.

  ```
  dcnm1# appmgr backup
  ```

  ```
  dcnm2# appmgr backup
  ```

  Copy the backup file to a safe location outside the DCNM server.

- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.

- Ensure that you plan for a maintenance window to install SMU.

- Ensure that both the Cisco DCNM 11.5(3a) Active and Standby peers are up and running.

To apply this software maintenance update on Cisco DCNM Virtual Appliance in Native HA Mode, apply this update on the Active and Standby appliance. Wait until the role of the Active appliance is Active again. Apply the update on the Standby appliance, later.

For Native HA cluster deployments, install the SMU on Active and Standby appliances, before installing SMU on the compute nodes.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(3a) appliance.

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

b) Locate **DCNM 11.5.3a Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

c) Save the **dcnm-va-patch.11.5.3a-p1.iso.zip** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **dcnm-va-patch.11.5.3a-p1.iso.zip** file and upload the file to the `/root/` folder in both Active and Standby node of the DCNM setup.

Note For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm1# su
Enter the root password:
[root@dcnm1]#
```

```
dcnm2# su
Enter the root password:
[root@dcnm2]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm1]# screen
```

```
[root@dcnm2]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 On the Active node, install the SMU.

a) Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm1]# mkdir -p /mnt/iso
```

b) Mount the DCNM 11.5(3a) SMU file on the Active node in the `/mnt/iso` folder.

```
[root@dcnm1]# mount -o loop dcnm-va-patch.11.5.3a-p1.iso /mnt/iso
```

c) Navigate to **/scripts/** directory.

```
[root@dcnm1]# cd /mnt/iso/packaged-files/scripts/
```

d) Run the **./inline-upgrade.sh** script.

```
[root@dcnm1]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

e) Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm1]# appmgr status all
```

Note Ensure that all the services are up and running on the Cisco DCNM Active node before proceeding to apply SMU on the Standby node.

Step 6 On the Standby node, install the SMU.

a) Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm2]# mkdir -p /mnt/iso
```

b) Mount the DCNM 11.5(3a) SMU file on the Standby node in the `/mnt/iso` folder.

```
[root@dcnm2]# mount -o loop dcnm-va-patch.11.5.3a.iso /mnt/iso
```

c) Navigate to **/scripts/** directory.

```
[root@dcnm2]# cd /mnt/iso/packaged-files/scripts/
```

d) Run the **./inline-upgrade.sh** script.

```
[root@dcnm2]# ./inline-upgrade.sh --standby
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

e) Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm2]# appmgr status all
```

Step 7 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm1]# exit
```

```
[root@dcnm2]# exit
```

Step 8 Unmount the **dcnm-va-patch.11.5.3a-p1.iso** file in both Active and Standby node of the DCNM setup.

Note You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm1]# umount /mnt/iso
```

```
[root@dcnm2]# umount /mnt/iso
```

Installing SMU on Cisco DCNM 11.5(3a) Compute Nodes

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on compute nodes in Cisco DCNM clustered setup, perform the following steps:

Before you begin

- You must install the SMU on Cisco DCNM Servers in Native HA mode, before upgrading the DCNM compute nodes.
- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.
- Ensure that you plan for a maintenance window to install SMU.
- Ensure that Cisco DCNM 11.5(3a) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(3a) appliance.

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

b) Locate **DCNM 11.5.3a Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

c) Save the **`dcnm-va-patch.11.5.3a-p1.iso.zip`** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **`dcnm-va-patch.11.5.3a-p1.iso.zip`** file and upload the file to the `/root/` folder in all three compute nodes of the DCNM setup.

For example, let us indicate the three Compute Nodes as Compute1, Compute2, and Compute3.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm-compute1# su
Enter the root password:
[root@dcnm-compute1]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm-compute1]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 On Compute1 node, install the SMU.

a) Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm-compute1]# mkdir -p /mnt/iso
```

b) Mount the DCNM 11.5(3a) SMU file on Compute1 node in the `/mnt/iso` folder.

```
[root@dcnm-compute1]# mount -o loop dcnm-va-patch.11.5.3a-p1.iso /mnt/iso
```

c) Navigate to **/scripts/** directory.

```
[root@dcnm-compute1]# cd /mnt/iso/packaged-files/scripts/
```

d) Run the **./inline-upgrade.sh** script.

```
[root@dcnm-compute1]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

If some services are still running, a prompt to stop the services appears. When prompted, press **y** to continue.

e) Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm-compute1]# appmgr status all
```

Note Ensure that all the services are up and running on the **dcnm-compute1** node.

f) Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm-compute1]# exit
```

g) Unmount the **dcnm-va-patch.11.5.3a-p1.iso** file from the Compute1.

Note You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm]# umount /mnt/iso
```

Step 6 Install the SMU on the other two Compute nodes also.

Follow the instructions as explained in Step Step 5, on page 109.

What to do next

After the installation is complete, each compute node joins the cluster automatically. On the Web UI, choose **Applications > Compute** to verify if the compute node appears as **Joined**.

Note If you try to install the SMU again, an error message appears stating that the patch is already applied on the Cisco DCNM/Compute.

Sample Output of Commands to address Log4j vulnerability

The following is a sample output while installing the SMU on Cisco DCNM Release 11.5(3a).

- Sample Output to Install SMU in DCNM Standalone Deployment, on page 110
- Sample output to install SMU in DCNM Native HA Deployment, on page 115
- Sample Output to Install SMU in DCNM Compute Nodes, on page 121

Sample Output to Install SMU in DCNM Standalone Deployment

```
[root@dcnm]# ./inline-upgrade.sh
### Sat Jan 15 15:09:55 PST 2022 ### CMD: ./inline-upgrade.sh

============================================================
============ Inline Upgrade to DCNM 11.5(3a)-p1 =============
============================================================

Upgrading from version: 11.5(3a)
Upgrading from install option: LAN Fabric
System type: Standalone
Compute only: No

Do you want to continue and perform the inline upgrade to 11.5(3a)-p1? [y/n]: ==== Sat Jan
 15 15:10:00 PST 2022 - Task disableAppsOnStandby started ====
==== Sat Jan 15 15:10:00 PST 2022 - Task disableAppsOnStandby finished ====
==== Sat Jan 15 15:10:00 PST 2022 - Task checkAfwStatus started ====
==== Sat Jan 15 15:10:00 PST 2022 - Task checkAfwStatus finished ====
==== Sat Jan 15 15:10:00 PST 2022 - Task updateAfwApps started ====
==== Sat Jan 15 15:10:00 PST 2022 - Updating AFW applications ====
Pausing Services that need to be patched
Deleted Containers:
72f9b30d7f6730c2548b3369e6cd2c8c200f314c7bce50a0267f17269ade73df
6966bf8cb5622a506807e7b3002ee57b22f29c4bbb2e973f83ffdd5313b648b3
a0fac1df5fa347af5123bfab16c107328a0ddc9e0e4998974fb66c6a735e789e
e7c6daad5c14d13cde68459f921bd3adffd0ef27cc54f0feb3592748df9169d7
f6924dd3a9da2d2f64f0be9d9e64ab9557aa182ae99862d5da42ef7f35ce0ddf
a939bd37779e36c5d2239e62ab761dbbefecfce9aa129b09eec2a301453b3848
10e8781b3e7603fec9c7b8ee083398f2ef8287fb9e02b06dc78b28f061f21db5
6506df9196bad4e3a454fe2de84ac6a204022a8441ba47219c03b75ebf8b8526
69479853dd371a613dd461a3464e4a1f7ca1b60d0cf9e2db62eabbe6d8aab06e

Total reclaimed space: 4.441MB
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Sat, 15 Jan 2022 23:10:00 GMT
Content-Length : 99
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Content-Type : text/plain; charset=utf-8
Date : Sat, 15 Jan 2022 23:10:20 GMT
Content-Length : 96
```

```
{
  "ResponseType": 0,
  "Response": "Application is Paused for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Content-Type : text/plain; charset=utf-8
Date : Sat, 15 Jan 2022 23:10:41 GMT
Content-Length : 91
{
  "ResponseType": 0,
  "Response": "Application is Paused for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Sat, 15 Jan 2022 23:11:01 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticservice_Cisco_afw. Check for status"
}
Now Removing Images from Runtime
Untagged: 127.0.0.1:5001/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5001/dcnmelastic@sha256:fa6d0f283eaa5e349637733e9cdd122cde8ea417c71dc4ad75f6e7d6bb5275c2
Untagged: 127.0.0.1:5000/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5000/dcnmelastic@sha256:fa6d0f283eaa5e349637733e9cdd122cde8ea417c71dc4ad75f6e7d6bb5275c2
Untagged: dcnmelastic:6.8.3_11.5.2
Deleted: sha256:db0af4dad6d9897181f3e81c776ca71e9fa240a120a62b1a54b9bc0675a26fbd
Deleted: sha256:e5e3ef624580c19ec6700c34d2ef44ca4f8c0d0b15b6eac526c1dbc8c8770fc3
Deleted: sha256:218bd8d63dc8108eff590be2d8611709eb1f502419b4d9579d791c26acbbf886
Deleted: sha256:6012192615fef866c9794b39c3edee86b031297ab9d9da898c5c138c12ef8d9e
Deleted: sha256:788999021c20856febb15522fee91992551a2813f55b2c061ddab2a897eeefa2
Deleted: sha256:2807d6e48bd7e95e0f12eb85bad701b46f7b06f65cde330695a0a57d9bda997f
Deleted: sha256:8ca7df1686fe965a316575f1ba71819dbedb3517c74f6f376c17b594ec469fa4
Deleted: sha256:98a4fbf550f7758f0432e61eaed22e0ab529c62255c3e6366713788b4c876dc7
Deleted: sha256:7b84ae7a055765f029ffb3dcec87f78575e0f9930200ad17d634ffeaafa9fc55
Deleted: sha256:544fc6ed244eef6449d95305179600648f339c0adbcbcbf93cc4f9e402122c53
Deleted: sha256:6810a2c88653fe864294296c70a5a657caa0f638689ff58f13493acc532f5c77
Untagged: 127.0.0.1:5001/elasticservice:1.3
Untagged:
127.0.0.1:5001/elasticservice@sha256:fb77f4863b1536c3e659f55cdf94768946fe46076d456eddec83e948f6f61e1c
Untagged: 127.0.0.1:5000/elasticservice:1.3
Untagged:
127.0.0.1:5000/elasticservice@sha256:fb77f4863b1536c3e659f55cdf94768946fe46076d456eddec83e948f6f61e1c
Untagged: elasticservice:1.3
Deleted: sha256:e445f43b46bfe4b369869b81a24c9eb6d3f8ee5e72f673932b391224d6e84293
Deleted: sha256:c974f7f5941212aa9b669067e1bd9cf0d6545d4878eef521184b403638cb3dd5
Deleted: sha256:acb7dd716a843bc8f1341f1c56bac254da7f9dcf97dfddcc79d0a94a2c4fe73d
Deleted: sha256:0fcb60a4db2f4faab4258776cb67466c8ebc71d28a7bf69efcf87f04717aaba4
Deleted: sha256:b1c67c757c196ebdc7a18d3b4992a8c5c4f31f143122aab8b50c62981aa0db3d
Untagged: 127.0.0.1:5001/watchtower:2.1
Untagged:
127.0.0.1:5001/watchtower@sha256:43af6c1738a85ff103225ede6127afae10378b8d77854ae2e1d02109d5515cd7
Untagged: 127.0.0.1:5000/watchtower:2.1
Untagged:
127.0.0.1:5000/watchtower@sha256:43af6c1738a85ff103225ede6127afae10378b8d77854ae2e1d02109d5515cd7
Untagged: watchtower:2.1
```

```
Deleted: sha256:9d159636c92c091d6d51ee9b1c283bb2d75585e90494d54cc4674a4f002a8106
Deleted: sha256:aca239829b0c0fa3a64d34f65b94aac5b2f3b6cc4da01a0c1160892af1192326
Deleted: sha256:1a44b78736dae701a0e3376c6e19ae0d17423cbf1584b7d771e4a4056cfc6cc9
Deleted: sha256:a1529e1623caaf7445365798f0b5577019ddc7a2ac7196cdae36794e7af927a1
Untagged: 127.0.0.1:5001/eplui:2.2
Untagged:
127.0.0.1:5001/eplui@sha256:40cce94a59583545142c82fff6a67c54c94a35bc2f9b0ce577e291a192c2f860
Untagged: 127.0.0.1:5000/eplui:2.2
Untagged:
127.0.0.1:5000/eplui@sha256:40cce94a59583545142c82fff6a67c54c94a35bc2f9b0ce577e291a192c2f860
Untagged: eplui:2.2
Deleted: sha256:19ae3e3113a3f612a330f8740b0b64b3a3e150b71e344ffabf2c3db88a6b5a21
Deleted: sha256:4627c5b7d2ae88d6ed7677054bc2da749ac67883f2bab53211913411479e62d9
Deleted: sha256:5b3a9450cb30987c193253556242fe33ed6567dfdad7381579c1a53cb3172df4
Deleted: sha256:9dda6b3ab9689d6018d9516200a06589140726e6a19afe447ebb0c144a198559
Checking and starting a writable registry
Error response from daemon: no such image: AfwAppRegistry: invalid reference format:
repository name must be lowercase
0112e20217274f37caddaf572759d8d7180e5f1c8c81e4ff9be97b2d01fa5925
Achieved Pause state for all services, Now Patching services
Loading Images into the writable registry
Loaded image: elasticservice:1.3
Loaded image: eplui:2.2
Loaded image: dcnmelastic:6.8.3_11.5.2
The push refers to a repository [127.0.0.1:5000/dcnmelastic]
3a2afa29fade: Preparing
f6b47e978cbe: Preparing
84f76e17ea24: Preparing
ce16df607324: Preparing
2582f2f60fcb: Preparing
edaa115e0391: Preparing
4192589bd87d: Preparing
edaa115e0391: Waiting
7904c9b104c6: Preparing
2455ddff124b: Preparing
d3071a656898: Preparing
0bcab5b3cf37: Preparing
7904c9b104c6: Waiting
2455ddff124b: Waiting
4192589bd87d: Waiting
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
9785ac5771f5: Waiting
5d50c3ca45af: Waiting
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
ce16df607324: Pushed
3a2afa29fade: Pushed
2582f2f60fcb: Pushed
84f76e17ea24: Pushed
f6b47e978cbe: Pushed
d3071a656898: Layer already exists
0bcab5b3cf37: Layer already exists
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
fbb373121c59: Layer already exists
7b9f72883f99: Layer already exists
edaa115e0391: Pushed
5fb2dee77c93: Layer already exists
```

```
bc2717dd2942: Layer already exists
7904c9b104c6: Pushed
4192589bd87d: Pushed
2455ddff124b: Pushed
6.8.3_11.5.2: digest: sha256:e561c11835c635141a07665d45af3f2a30ebccc9d6e756ea6eb98b5c766e4f7a
 size: 3882
The push refers to a repository [127.0.0.1:5000/elasticservice]
6ccfea03ca23: Preparing
162d8286ed1b: Preparing
4a51e2c0d99c: Preparing
53e47eb6c77d: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
9785ac5771f5: Waiting
bc2717dd2942: Waiting
5fb2dee77c93: Waiting
7b9f72883f99: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
fbb373121c59: Layer already exists
7b9f72883f99: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
162d8286ed1b: Pushed
53e47eb6c77d: Pushed
6ccfea03ca23: Pushed
4a51e2c0d99c: Pushed
1.3: digest: sha256:103fe8019fbe93993b9e30d1ed97edaf82081219131fdbb58e688a5526923606 size:
 2422
Error response from daemon: No such image: watchtower:2.1
The push refers to a repository [127.0.0.1:5000/watchtower]
An image does not exist locally with the tag: 127.0.0.1:5000/watchtower
The push refers to a repository [127.0.0.1:5000/eplui]
a10dac8af164: Preparing
6a2ffc7d6528: Preparing
00ead5d1b2ac: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
fbb373121c59: Waiting
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
fbb373121c59: Layer already exists
7b9f72883f99: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
00ead5d1b2ac: Pushed
a10dac8af164: Pushed
6a2ffc7d6528: Pushed
2.2: digest: sha256:f675abc97f7d231c4f00268002ca98520b166da4b4af05290cb65500900585a5 size:
 2214
AfwAppRegistry
Loaded images, now unpausing services
pauseAfwApp: calling PUT with  {unpause}
```

```
HTTP/1.1 200 OK
Date : Sat, 15 Jan 2022 23:12:57 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Sat, 15 Jan 2022 23:13:18 GMT
Content-Length : 97
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Sat, 15 Jan 2022 23:13:39 GMT
Content-Length : 92
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Sat, 15 Jan 2022 23:14:00 GMT
Content-Length : 101
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticservice_Cisco_afw. Check for status"
}
Nothing to Patch in NI Base image is not installed here
==== Sat Jan 15 15:14:20 PST 2022 - Task updateAfwApps finished ====
==== Sat Jan 15 15:14:20 PST 2022 - Task disableHaPingFeature started ====
==== Sat Jan 15 15:14:20 PST 2022 - Task disableHaPingFeature finished ====
==== Sat Jan 15 15:14:20 PST 2022 - Task stopDcnmServer started ====
==== Sat Jan 15 15:14:21 PST 2022 - Trying to upgrade your DCNM, so stopping the dcnm to
proceed... ====
Stopping FMServer (via systemctl):  [  OK  ]
==== Sat Jan 15 15:14:57 PST 2022 - Task stopDcnmServer finished ====
==== Sat Jan 15 15:14:57 PST 2022 - Task updatePackagedFiles started ====
==== Sat Jan 15 15:14:57 PST 2022 - Updating packaged-files ====
==== Sat Jan 15 15:14:57 PST 2022 - Task updatePackagedFiles finished ====
==== Sat Jan 15 15:14:57 PST 2022 - Task updateFmServer started ====
==== Sat Jan 15 15:14:57 PST 2022 - Updating FMServer ====
==== Sat Jan 15 15:14:57 PST 2022 - Backing up dcm.ear ====
==== Sat Jan 15 15:14:58 PST 2022 - Applying patch... ====
==== Sat Jan 15 15:14:59 PST 2022 - Task updateFmServer finished ====
==== Sat Jan 15 15:14:59 PST 2022 - Task updatePatchList started ====
==== Sat Jan 15 15:14:59 PST 2022 - Task updatePatchList finished ====
==== Sat Jan 15 15:14:59 PST 2022 - Task startDcnmServer started ====
Started AFW Server Processes
Started AFW Agent Processes
Started DCNM
Check the status using 'appmgr status dcnm'
==== Sat Jan 15 15:15:49 PST 2022 - Task startDcnmServer finished ====
```

```
==== Sat Jan 15 15:15:49 PST 2022 - Task enableHaPingFeature started ====
==== Sat Jan 15 15:15:49 PST 2022 - Task enableHaPingFeature finished ====
==== Sat Jan 15 15:15:49 PST 2022 - Task completeUpgrade started ====

********************************************************************************
Inline upgrade is complete.
********************************************************************************

==== Sat Jan 15 15:15:49 PST 2022 - Task completeUpgrade finished ====
```

Sample output to install SMU in DCNM Native HA Deployment

Installing DCNM SMU for Release 11.5(3a) on Active Node

```
[root@dcnm-se-active scripts]# ./inline-upgrade.sh

============================================================
============ Inline Upgrade to DCNM 11.5(3a)-p1 =============
============================================================

Upgrading from version: 11.5(3a)
Upgrading from install option: LAN Fabric
System type: HA
Compute only: No

Do you want to continue and perform the inline upgrade to 11.5(3a)-p1? [y/n]: y

Enter the Compute Root Password:

==== Fri Jan 28 09:51:56 PST 2022 - Task disableAppsOnStandby started ====

Stopping HA apps on Standby node
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

==== Fri Jan 28 09:52:33 PST 2022 - Task disableAppsOnStandby finished ====
==== Fri Jan 28 09:52:33 PST 2022 - Task checkAfwStatus started ====
==== Fri Jan 28 09:52:33 PST 2022 - Task checkAfwStatus finished ====
==== Fri Jan 28 09:52:33 PST 2022 - Task updateAfwApps started ====
==== Fri Jan 28 09:52:33 PST 2022 - Updating AFW applications ====
Pausing Services that need to be patched
Total reclaimed space: 0B
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 17:52:33 GMT
Content-Length : 99
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 17:52:53 GMT
Content-Length : 96
Content-Type : text/plain; charset=utf-8
{
```

```
  "ResponseType": 0,
  "Response": "Application is Paused for elasticsix_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Content-Length : 100
Content-Type : text/plain; charset=utf-8
Date : Fri, 28 Jan 2022 17:53:13 GMT
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticsixhwtm_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 17:53:33 GMT
Content-Length : 96
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 17:53:53 GMT
Content-Length : 91
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for eplui_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 17:54:13 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticservice_Cisco_afw. Check for status"
}

Now Removing Images from Runtime
Error: No such image: dcnmelastic:6.8.3_11.5.2
Error: No such image: elasticservice:1.3
Error: No such image: watchtower:2.1
Error: No such image: eplui:2.2
Checking and starting a writable registry
Error response from daemon: no such image: AfwAppRegistry: invalid reference format:
repository name must be lowercase
6ee467fb9421965e7b0efbdcdc87907486556f580a4a5c1e3e9f224c9c856698
Achieved Pause state for all services, Now Patching services
Loading Images into the writable registry

Now Removing Images from Runtime
Untagged: 127.0.0.1:5000/dcnmelastic:6.8.3_11.5.2
```

```
Untagged:
127.0.0.1:5000/dcnmelastic@sha256:4d94e2ebf829438578580189993505 49f618abc24733bbeac62eee0a8f39d3be
Untagged: dcnmelastic:6.8.3_11.5.2
Deleted: sha256:5cde8ea0b573929652d18db8ab922f0a745edd338423b0651d4b0c552097bc3f
Deleted: sha256:3539fb8f8355b8a1d48e05a1f5fca33d2c9bdc8558934ee5bc7caee927643d22
Deleted: sha256:708fdb1eceb5e9a6992ec0a1a26f027c233943f56e6adfd67f847046867633c9
Deleted: sha256:384cf552d13562a15e3bf387b1f433cb127058e1c576e5ef49cb27a72167645f
Deleted: sha256:d3ff4218ebaf62496a4ac5eaf3dd3e40063f59f1020b00dfe37db4b746b786fe
Deleted: sha256:b09223f19bb25f888c3d8fcb385f00643d8facab2f5f3fec3f93199e2799ed9f
Deleted: sha256:c713847c0545c150b20206dfbc573edeefb95175396055f98252057f9583eff7
Deleted: sha256:246ca06f181f79c596924fe24425be72e89af5cbad4f3c19a8e393ba15a627da
Deleted: sha256:0c1fbb6b49eaf1eedf86b97230038901d03b1ad19b7624030131f76925760343
Deleted: sha256:19d91bd1a0bc84617afce83c8c6eb963761b4fd63cb9f9954810b85e476e381c
Deleted: sha256:544fc6ed244eef6449d95305179600648f339c0adbcbcbf93cc4f9e402122c53
Deleted: sha256:6810a2c88653fe864294296c70a5a657caa0f638689ff58f13493acc532f5c77
Untagged: 127.0.0.1:5000/elasticservice:1.3
Untagged:
127.0.0.1:5000/elasticservice@sha256:c19b3f5647fce6077e90abb3204e3b0a98eb04eff63d9a55a03cfd6fec635906
Untagged: elasticservice:1.3
Deleted: sha256:fbed7e0b93c4bf4357e4dde7d5995f7fd92f5fae83b32155610b9fe47aa49def
Deleted: sha256:eab90edde889eba59ed2712ff1ac9d0eea15ca06a511365083bb8dffd6f42814
Deleted: sha256:a38ebbc8e72b40db53253c823d1523d7291d7860668e63aac44885642d949247
Deleted: sha256:e77607ca6a7517afedcb25360ab2d41f57431c64df038ae26d26f01362f97fa8
Deleted: sha256:934e36f89e20b1c31601826a82bec5641fcb8429d742d07b3c0bd7abda026089
Untagged: 127.0.0.1:5000/watchtower:2.1
Untagged:
127.0.0.1:5000/watchtower@sha256:da4524d8f6054c8330152e20ec189f7ba7240c33583e967bd42b6e14540a1141
Untagged: watchtower:2.1
Deleted: sha256:a262b887747edb92f8f862b35cc70952a24a2f342f7cdd9bbe9e30bb09f4e5b3
Deleted: sha256:726e666b14833ba115aca2a3a158b6fd542362da85e660b8e49b172133c07f94
Deleted: sha256:8dfbde2e4eea973045fdfe0b850999cd5b8fe01fb9a89eb02251627cbade2b51
Deleted: sha256:7e2e285f77a8d0f30fa0503f4390a2e98d4d337601aef56b146ffc0b33f24a98
Untagged: 127.0.0.1:5000/eplui:2.2
Untagged:
127.0.0.1:5000/eplui@sha256:57e64a4146d8a82ee08b5f90e66abe37402358962fd9c6b0811deb593ee3b945
Untagged: eplui:2.2
Deleted: sha256:86c201584d06801bc46d871eebcfa255c8269fe9867fbb8986b01f17b4bf5c2e
Deleted: sha256:2070e2517a0136381264fa00668e6183712e06cca383a4543f3cd68669909771
Deleted: sha256:e2d5d3d393cac7ac6075822ae7f7680606fff7e9218c41ba7b607c06fdf10660
Deleted: sha256:0ba6706db1684cfb545f54ad2f7c972c96463ed48a19713885aceda6d3affe7b
Deleted: sha256:d72413f24ba6bdf70934e16489d44fc59919eba8ffbca6a3a012e2e066a25ad7
Deleted: sha256:482c552eb8917bf9da4725929271deb7df363e15294d4971fe82a93e1a371bac
Deleted: sha256:abbba6a4018d6689322f90e9ed42175b33b9d584a57e997ac132e76fa07f325d
Deleted: sha256:bdbfd81f5117cb1faa7033648bae43b2a4b149d73a80ced772219bf43368d0eb
Deleted: sha256:298466b2f385429721f9fa293edd7af3d008a0feef3be80b8c259ab8509278de
Checking and starting a writable registry
Error response from daemon: no such image: AfwAppRegistry: invalid reference format:
repository name must be lowercase
61809911fa8c87f2edda0d0d8a871909c42a010bd68975120c1c8014d8e5b963
Achieved Pause state for all services, Now Patching services
Loading Images into the writable registry
338da879175a: Preparing
46917051dd7f: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
fbb373121c59: Waiting
7b9f72883f99: Waiting
bc2717dd2942: Waiting
5fb2dee77c93: Waiting
9785ac5771f5: Layer already exists
```

```
46917051dd7f: Layer already exists
338da879175a: Layer already exists
d1b055091140: Layer already exists
5d50c3ca45af: Layer already exists
5fb2dee77c93: Layer already exists
7b9f72883f99: Layer already exists
fbb373121c59: Layer already exists
bc2717dd2942: Layer already exists
2.1: digest: sha256:da4524d8f6054c8330152e20ec189f7ba7240c33583e967bd42b6e14540a1141 size:
 2214
The push refers to a repository [127.0.0.1:5000/eplui]
00904eb93bbc: Preparing
ca5ea9680890: Preparing
681596314eb0: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
fbb373121c59: Waiting
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
681596314eb0: Layer already exists
5d50c3ca45af: Layer already exists
ca5ea9680890: Layer already exists
00904eb93bbc: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
5fb2dee77c93: Layer already exists
fbb373121c59: Layer already exists
bc2717dd2942: Layer already exists
2.2: digest: sha256:57e64a4146d8a82ee08b5f90e66abe37402358962fd9c6b0811deb593ee3b945 size:
 2214
AfwAppRegistry
Loaded images, now unpausing services
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 18:21:34 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 18:21:55 GMT
Content-Length : 97
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticsix_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Content-Type : text/plain; charset=utf-8
Date : Fri, 28 Jan 2022 18:22:16 GMT
Content-Length : 101
{
  "ResponseType": 0,
```

```
  "Response": "Application is Running for elasticsixhwtm_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 18:22:37 GMT
Content-Length : 97
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 28 Jan 2022 18:22:58 GMT
Content-Length : 92
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Content-Length : 101
Content-Type : text/plain; charset=utf-8
Date : Fri, 28 Jan 2022 18:23:19 GMT
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticservice_Cisco_afw. Check for status"
}
Nothing to Patch in NI Base image is not installed here
==== Fri Jan 28 10:23:39 PST 2022 - Task updateAfwApps finished ====
==== Fri Jan 28 10:23:39 PST 2022 - Task disableHaPingFeature started ====
==== Fri Jan 28 10:23:39 PST 2022 - Task disableHaPingFeature finished ====
==== Fri Jan 28 10:23:39 PST 2022 - Task stopDcnmServer started ====
==== Fri Jan 28 10:23:39 PST 2022 - Trying to upgrade your DCNM in Native HA setup, so
stopping the ha-apps to proceed... ====
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

==== Fri Jan 28 10:25:01 PST 2022 - Task stopDcnmServer finished ====
==== Fri Jan 28 10:25:01 PST 2022 - Task updatePackagedFiles started ====
==== Fri Jan 28 10:25:01 PST 2022 - Updating packaged-files ====
==== Fri Jan 28 10:25:01 PST 2022 - Task updatePackagedFiles finished ====
==== Fri Jan 28 10:25:01 PST 2022 - Task updateFmServer started ====
==== Fri Jan 28 10:25:01 PST 2022 - Updating FMServer ====
==== Fri Jan 28 10:25:01 PST 2022 - Backing up dcm.ear ====
==== Fri Jan 28 10:25:01 PST 2022 - Applying patch... ====
==== Fri Jan 28 10:25:01 PST 2022 - Task updateFmServer finished ====
==== Fri Jan 28 10:25:01 PST 2022 - Task updatePatchList started ====
==== Fri Jan 28 10:25:01 PST 2022 - Task updatePatchList finished ====
==== Fri Jan 28 10:25:01 PST 2022 - Task startDcnmServer started ====
updating the Navigation file
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.
```

```
==== Fri Jan 28 10:25:03 PST 2022 - Task startDcnmServer finished ====
==== Fri Jan 28 10:25:03 PST 2022 - Task enableHaPingFeature started ====
==== Fri Jan 28 10:25:03 PST 2022 - Task enableHaPingFeature finished ====
==== Fri Jan 28 10:25:03 PST 2022 - Task completeUpgrade started ====

********************************************************************************
Inline upgrade of this Active DCNM node is complete.
Please wait until this node is Active again
before upgrading the Standby node.
********************************************************************************

==== Fri Jan 28 10:25:03 PST 2022 - Task completeUpgrade finished ====
```

Installing DCNM SMU for Release 11.5(3a) on Standby Node

```
[root@dcnm-standby scripts]# ./inline-upgrade.sh --standby

============================================================
============ Inline Upgrade to DCNM 11.5(3a)-p1 =============
============================================================

Upgrading from version: 11.5(3a)
Upgrading from install option: LAN Fabric
System type: HA
Compute only: No

Do you want to continue and perform the inline upgrade to 11.5(3a)-p1? [y/n]: y
==== Fri Jan 28 10:04:05 PST 2022 - Task disableAppsOnStandby started ====
==== Fri Jan 28 10:04:05 PST 2022 - Task disableAppsOnStandby finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task checkAfwStatus started ====
==== Fri Jan 28 10:04:05 PST 2022 - Task checkAfwStatus finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updateAfwApps started ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updateAfwApps finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task disableHaPingFeature started ====
==== Fri Jan 28 10:04:05 PST 2022 - Task disableHaPingFeature finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task stopDcnmServer started ====
==== Fri Jan 28 10:04:05 PST 2022 - Task stopDcnmServer finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updatePackagedFiles started ====
==== Fri Jan 28 10:04:05 PST 2022 - Updating packaged-files ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updatePackagedFiles finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updateFmServer started ====
==== Fri Jan 28 10:04:05 PST 2022 - Updating FMServer ====
==== Fri Jan 28 10:04:05 PST 2022 - Backing up dcm.ear ====
==== Fri Jan 28 10:04:05 PST 2022 - Applying patch... ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updateFmServer finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updatePatchList started ====
==== Fri Jan 28 10:04:05 PST 2022 - Task updatePatchList finished ====
==== Fri Jan 28 10:04:05 PST 2022 - Task startDcnmServer started ====
updating the Navigation file
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.

==== Fri Jan 28 10:04:07 PST 2022 - Task startDcnmServer finished ====
==== Fri Jan 28 10:04:07 PST 2022 - Task enableHaPingFeature started ====
==== Fri Jan 28 10:04:07 PST 2022 - Task enableHaPingFeature finished ====
==== Fri Jan 28 10:04:07 PST 2022 - Task completeUpgrade started ====

********************************************************************************
Inline upgrade of the HA DCNM system is complete.
********************************************************************************
```

```
==== Fri Jan 28 10:04:07 PST 2022 - Task completeUpgrade finished ====
```

Sample Output to Install SMU in DCNM Compute Nodes

```
[root@dcnm-c1 scripts]# ./inline-upgrade.sh

================================================================
============ Inline Upgrade to DCNM 11.5(3a)-p1 =============
================================================================

Upgrading from version: 11.5(3a)
Upgrading from install option: N/A
System type: Standalone
Compute only: Yes

*************************************************************************
ALERT: AFTER THE UPGRADE MAKE SURE COMPUTE NODE IS BACK IN JOINED STATE.
       USE DCNM "APPLICATIONS->COMPUTE" GUI TO CHECK STATUS
*************************************************************************

Do you want to continue and perform the inline upgrade to 11.5(3a)-p1? [y/n]: y
==== Fri Jan 28 10:05:40 PST 2022 - Task updatePackagedFiles started ====
==== Fri Jan 28 10:05:40 PST 2022 - Updating packaged-files ====
==== Fri Jan 28 10:05:40 PST 2022 - Task updatePackagedFiles finished ====
==== Fri Jan 28 10:05:40 PST 2022 - Task updatePatchList started ====
==== Fri Jan 28 10:05:40 PST 2022 - Task updatePatchList finished ====
==== Fri Jan 28 10:05:40 PST 2022 - Task completeUpgrade started ====

*******************************************************************************
Inline updgrade of this compute is complete
*******************************************************************************

==== Fri Jan 28 10:05:40 PST 2022 - Task completeUpgrade finished ====

[root@dcnm-c1 scripts]#
```

Scanning for Log4j2 Vulnerabilities

Download a scanner (such as logpresso) from https://github.com/logpresso/CVE-2021-44228-Scanner.

Warning Use this utility only to scan for vulnerabilities. DO NOT use it to fix anything in the system.

Caution After installing the SMU, ensure that the DCNM Web UI is up and running. Also, ensure that all the processes are up and running, by using the **appmgr status all** command. Ensure that the **Applications > Compute** shows all nodes in **Joined** state.

Before running the scan again, clear the old docker images that are no longer used, by using the following command:

If **docker ps -a** shows many containers in Exited state, then first run the following:

```
docker container prune
WARNING! This will remove all stopped containers.
Are you sure you want to continue? [y/N] y
Deleted Containers:
```

```
33d2a44706663870d062b7ee8b4aba18ea94ea6fdc285b6ba1d133334f226d73
9fba3140120f7fbc41993a97d0bc6bec254ffed638da1445e3a91fb04614cba6
67d4cd575d1febdec54fe161d716334908eb18d1a9a5d053a8f21ed1e3089d8c
4b8f2463cf899341fd5a028078a3d6b98790807db1ba6f6ece13a5a0a7783749
5b066b6eb334986d0cb0442249218d8582936439f8c8b3a3c81426ab81beaac3
14b965917498dcaaaa3e586d0d65e702d884c3cef7e425e60215a192cbff9945
359ab2ca568d10c42e406fec6a6f7499637936080b0ca109e307c51ca9431532
a18a752de7208d3802989f9209893140cac404cf33dcdf5cb362ebbddbde4e04
519e0e7654ecff8601f868c2a55fd1507a9ce52d137c33c79067fe3d7f834048
03e0c0ccaa35e2b4d07c6afae90c758f3db5ea639528afcc550a26e9c1ef1b43
Total reclaimed space: 155.4MB
```

If there are no containers in Exited state, then you can directly run the **docker image prune** to clean up the old images, as follows:

```
docker image prune -a
WARNING! This will remove all images without at least one container associated to them.
Are you sure you want to continue? [y/N] y
Deleted Images:
untagged: baseactivedata:2.0.28
deleted: sha256:e6df05057635c16ab9719158f58ccb63bece4c9ef83241ecbfd363dba8612a61
deleted: sha256:f610703a2c6abf3cf71cc31fd7804d79a91fcd01906bf80c452b02fe0b528733
deleted: sha256:6db60bb9b58b76fedcc80bc4f48293c8b41d16fd03a66ac45c4be048ab4874c0
deleted: sha256:79716a587dfb9cd8d2cd85bc011ae85f18d6969fb4aa01e2a2adf3d4c513bc25
deleted: sha256:336fdce93308d8b14b0e953da06f575217de3658111c7dd9ca6b11c53b4c6e26
deleted: sha256:52b83194fbf1ff2891e286b7bc99b9d8f4c4c5806c72648c3ab741938251349b
deleted: sha256:e5406c9c341937f94eb8c0e01cfa1fd398cb2a04102ba9e051ea006c0f965a65
deleted: sha256:f8603be917dec8a46150a2c2c1c33125d2d46432a4987efb3af68eb6aa5c318b
deleted: sha256:c40b0a54b89e6acdd0f4b78d213b86154aba78449f51de8ecd79920b609d3be2
untagged: 127.0.0.1:5000/elasticservice:1.3
untagged:
127.0.0.1:5000/elasticservice@sha256:103fe8019fbe93993b9e30d1ed97edaf82081219131fdbb58e688a5526923606
untagged: 127.0.0.1:5001/elasticservice:1.3
untagged:
127.0.0.1:5001/elasticservice@sha256:103fe8019fbe93993b9e30d1ed97edaf82081219131fdbb58e688a5526923606
untagged: basejobscheduler:2.0.28
deleted: sha256:47e7aabab17281ee79f538f6feca10483075e618f572efe5d4bed34c9b119b6a
deleted: sha256:2edd5e253617887e219136f7fa1d5a6207f811771b869db2a5e532824a8d32a3
deleted: sha256:b7e9d708cf0ebd4cc7dea111b05d27eb55bdde10d1a7c6c803eea38ea49b1896
deleted: sha256:7264dca82d7646598c781cbba14de9d71ed35bab0ed65f5ababc1054afb701ce
deleted: sha256:c855489cd9458fa2b8accf3a10ef88caf7b90bd87dc21d8cd9f28795f091bd84
deleted: sha256:944eafe4332049ac3cb8d619a021b95fae9863a7ad546b5efd684ee694aa2b15
deleted: sha256:7245aded621dbb4bb544362f140aa76136fb0195329d9b80d16589bf46b1f13e
deleted: sha256:aa45ff2fc948610111fc98d5d985873ec6ca5dcccdb5dc957afd51c3a561e8ab
deleted: sha256:951d71bbc1d3e1f0178b6f7db7b464e3d5a2bddf30bdde5e2d829ddb5f562ca2
untagged: 127.0.0.1:5000/openstackviz:1.0.1
untagged:
127.0.0.1:5000/openstackviz@sha256:7eb849e43bc805b7779429c418401f6f6853584f2b970afeb7ac7600b6ede721
untagged: openstackviz:1.0.1
deleted: sha256:4140d07362070c1dc7d2a68de7417428a7522863452cbf257016f6beff13749e
deleted: sha256:fcef14fe2b3ccae0309a1b07c09dc51d1086b6da3467da40ce073e2e294d7372
deleted: sha256:5f160d09f243bc6ceccb4f8c90d5aadb46675d834f2ee8bfa1324b6724afb1a3
deleted: sha256:ac67f453d123f8fe51b9b6c72defb524581321e2d89227edcc326dfd0b7c14ef
deleted: sha256:8dc33bc40b40998d64a9525375d46f5c4df7c0640e280acf0cd2dbc18e796293
deleted: sha256:d9c344fc33ac9f02868b2e5af0955f1213911e9b1b1c70e33a0678c81c1ab1eb
deleted: sha256:b6c21210ed41cebef89cb1f543ac082c1edf4da52994e15847ffabc53973b964
deleted: sha256:7c98faecdae6aaf04b82571f009add8df4dfffb094e2737ec184b01690c385e8
deleted: sha256:0b2f06b83ed6612d837fd3de042f7c9f3f62d4df87aeac1e8ffab9da760053a8
deleted: sha256:243c4f2457310f6c25335147459390e1b2a6cd76ffbd3baff209563cd52b8a57
deleted: sha256:f372fe340c288ca18e584dc74e651d5afb5a38dc94a194d6605898e20bcc0a84
deleted: sha256:21cbb8a027cc40ce9f9a5169fe6d4bc39cfb4cfce4c9602de9eb206b30f123d6
deleted: sha256:531f1b1c4325c94f90ab230cc322d43ee7d6123e9c2e37eb1917986184b5f8d8
deleted: sha256:e38494bdd3b84de75a9703364e528ff4301e06741dee54010ed505daebcd026a
deleted: sha256:d5dc39e0022ed33a4c45d0f327c21705d508da8cde1821cbffb716a82f1df786
deleted: sha256:93d0c20d5d1280a11b16b4a8cc521409048f8202796c4f29d3ed5e488a6200f5
```

```
untagged: 127.0.0.1:5000/stalker:1.7
untagged:
127.0.0.1:5000/stalker@sha256:c63be04ca5d10c24a91795376512291221663 67cbf2bdb9c1fd992b75b719ef1
untagged: 127.0.0.1:5001/stalker:1.7
untagged:
127.0.0.1:5001/stalker@sha256:c63be04ca5d10c24a91795376512291221663 67cbf2bdb9c1fd992b75b719ef1
untagged: 127.0.0.1:5000/kibana:2.1
untagged:
127.0.0.1:5000/kibana@sha256:a338b26c498192ed0220ea4db3c24e2ed6014695d44d56bab48e746f176c6d3a
untagged: kibana:2.1
deleted: sha256:af601a8851b7d6879721e4615700f1c506c98d104e0293c5e54328e4c05629f6
deleted: sha256:841d0e0be230989edfdefb7a96da1781fc718f9b51762ba68664a84a09ee12bf
deleted: sha256:49b6d15a32a43629d07f868e0b163fc6192853e9fd2c05249ea22920670c8cf3
deleted: sha256:80547b9f48b6b7247ea5f7cc24e55f7518f57cfc9089f58ab49cb25d1c61cc65
deleted: sha256:d7b3cc7abfd65e7d9115d7aeb06738ff111f8eb1ca58220c17f0384b05f3acef
deleted: sha256:6823c797c41b8f99166454d1cab11a552d8cf002e317f17cffc6dc8bddb53494
deleted: sha256:974c90d761a210f76a78164043a9a339159cfa654612174766289d1523dd8d4f
deleted: sha256:0f6b7a3a37464b66e0c489660321372949c842a2863ee516236888cf428d3a8b
deleted: sha256:97a3fafd0a7a20a6062b577ea48e8bc8fdd08ae2d890a8260438d4bc805204b4
deleted: sha256:e49d4182e39ee4be36241a1aacf388554b037a6ada41994ce84d89ef00e48e50
deleted: sha256:b94a74b32e662681e38fa7f9844981ecb8f9a67da3ddf741784062dfc4a7c8ce
untagged: 127.0.0.1:5000/dss:1.2
untagged:
127.0.0.1:5000/dss@sha256:b5bfe155acbcc8539b16c28ef632ae29cb7381661298cd5a3291d4afb605eb9d
untagged: 127.0.0.1:5001/dss:1.2
untagged:
127.0.0.1:5001/dss@sha256:b5bfe155acbcc8539b16c28ef632ae29cb7381661298cd5a3291d4afb605eb9d
untagged: 127.0.0.1:5000/preport:1.2
untagged:
127.0.0.1:5000/preport@sha256:1caddaadded881bff4b0ce3fcf14c6cf1494f9ff21103dd69df7707cb4edeb06
untagged: 127.0.0.1:5001/preport:1.2
untagged:
127.0.0.1:5001/preport@sha256:1caddaadded881bff4b0ce3fcf14c6cf1494f9ff21103dd69df7707cb4edeb06
untagged: baseeventaggregator:2.0.28
deleted: sha256:c6fe086baa00e9a29a8d2066a91b6d53b378283680e4dfff620f81efb852ef82
deleted: sha256:98ea7fc02636eef04b3ef131a5fdb38a00e5a774406d5f8610738a97c0f6d483
deleted: sha256:f5e83bafd81a70f1259ee96ae72c274fe805e275be2cb53ddded77e869c3d51c
deleted: sha256:ed23f7c322b49d753c92fb25a68ee96939313fc32274dab7d958d0d8c776f513
deleted: sha256:8e5decda24d17642ffb7ab9f8baad0dcc8844e605c7b3b9aef4fc02d0289759b
deleted: sha256:7a0e193cf7d94fa498634c3d356bcceac3d4da1a89e9a318b304e6cbb0f3aea5
deleted: sha256:534f1fdf09e105bead265e61d18194fabc9c3875f6f703fd4b3f0dcb5f5ea205
deleted: sha256:1687e16fee06a5436cf5499a9d847c2efb613fae39cf30bf331bc3eb559ed7b6
deleted: sha256:7726639a6adf96cc733a3d4c0694c24e5d4f07c0eadb9e6569d0fdb3f2e0cda4
untagged: 127.0.0.1:5000/dcnmzookeeper:3.4.12_11.5.1
untagged:
127.0.0.1:5000/dcnmzookeeper@sha256:483975e729967b2ddc5307bd2bdd8ab7efef4b397b683ea48ccd68c7961f7980
untagged: dcnmzookeeper:3.4.12_11.5.1
deleted: sha256:deb0ce6e8ff8cd1a009e460905ca4210bf101a8356f9fadff4cf12d5646c5265
deleted: sha256:c89669797e2063bf2631cea538806673ec9a2a58598d630e604e9eb6bf5a6131
deleted: sha256:b3d6f433df4550881bb20faa703e2ef4ce991ed6c59b385c1eeec9e90c63e537
deleted: sha256:d2e817d7e05fce2a1ac2666928bfec7d0d5812ce58e183dd060aaba8cacde75c
deleted: sha256:4e501478b08dc84587283abe9cec77244740c2c1ebc0aa0c4327cbef71ef75ae
deleted: sha256:d3c75966ff2ad5c217fbc8a54095d69bd04b5151784434ef61dc79e8365a048d
untagged: basestatscollect:2.0.28
deleted: sha256:41a150807a24cf5bd8ea36e88a9a140a03b083f188af509d4f17f642117e7800
deleted: sha256:dfe7d666b380e06b1a4670f3d1039733f7c97fb30d789becbd05d20bcaf04de4
deleted: sha256:b7aff3ad627ba3c0e12dc55c6fbd5e129964c48e51b314d21d40d8c820d6bb27
deleted: sha256:12be919d1ed2901af148371a269cef130be58c79b276cf3d733719eb66f78dfa
deleted: sha256:787e1787134c2055cd9d55e0b089d87527a629e1ba76c8dcbb564bc0b2e2bba0
deleted: sha256:0de08e047bf81484befb84f4634c7a4165e99b564d80f99eca7a36b406da16b8
deleted: sha256:4c7d3cbd8331d0b836e2dddbddbe730c5f7a41eb4d96ac595f2824bdddf38996
untagged: 127.0.0.1:5000/dcnmkafka:2.12_2.4.1_11.5.2
untagged:
127.0.0.1:5000/dcnmkafka@sha256:24898be28fea46c95e0e36cbcc9139505b353fb00ec4688dcfb91eb55768917a
```

```
untagged: dcnmkafka:2.12_2.4.1_11.5.2
deleted: sha256:0ae815ac85352d14699a6dfeb8b058c4b2f98ce8c3c5426cc570745b2b41d321
deleted: sha256:3888566966da85fe37642b071bf802dcf3d7162083c76e63fda9aa9ed88e2936
deleted: sha256:47677cac6b8b40ab21d9e77bb5e93c0a82bf60044c2910a2395ece2a4fdd3eee
deleted: sha256:21e9055be91a06a68d590e03746ded7b585a79823ea5c99acc4c18a94a201fa4
deleted: sha256:5a8f7f5f4a837b291f1c70a3346d8fa5e1e1ce6a491bc07f930abce6ca4e0323
deleted: sha256:2f8d256de1bd2b257fe9a30008996a22d6b535252d97acadf99d6205e439d1dd
deleted: sha256:8f86bbb07258e5b2fe9f7841623168fa72545a017f60e7d9efa8de596d3f5060
deleted: sha256:bb4a5c6c6b72f32c81244a4b7a1516b5eca2477a1c69d7ac781768e6405f2e13
deleted: sha256:421b779723ac33ace8f2f26cc71fcee09ce3072dcbabb4d252c3e2a31ba070e1
deleted: sha256:6529d679e0a301fde0739bb8d402bad208a89ce4f0a86d4d7e71c336ef42c149
deleted: sha256:c646553c96017807ddaa91929374d8c17ee048d09d91416ab4474fd5d3522b05
deleted: sha256:f6dd2339f342b8c608605efc889e9a7fc212d7cc6082c04619b7e6b59e629200
untagged: 127.0.0.1:5000/dcnmdebugplugin:2.3
untagged:
127.0.0.1:5000/dcnmdebugplugin@sha256:e6f39e1f554f24fd86a3c37eff9a4407b5ce8e395682796cede1a601bb1e55aa
untagged: dcnmdebugplugin:2.3
deleted: sha256:4bdb9ad4af4a4e0299d57d564cadc5394decc39d6ace02450c53b17bab822c0c
deleted: sha256:76231ffcb8745d0a13dd59d6dc7a7ad323e81d22c7f1333e097f75c28bd65c44
deleted: sha256:5f770c43536ab9b0fdb122694d44c40730b63ebc62f13c09753e7db813f5c450
deleted: sha256:5ed0e801907a66fa0ad75b81c2d779396e596948b1a27430b4de8e6767c355c4
deleted: sha256:5463572ac3c387aee8e7591cfe248481cebd36b7bcb945fba90640896bfd51f7
deleted: sha256:04d9b5e002436f67c4c2386f21259f2558943bdf037bfd0c43d2cbe325a300c2
deleted: sha256:2b745f3a7cc97ba7364d8a9b6dccdd333754976490dd56bddc4bba46ae99f60f
deleted: sha256:1532664ec0fe90ce53af7fddf7429d1f90ff21c57fde53cade705179843aa048
untagged: 127.0.0.1:5000/dcnminfoblox:1.2
untagged:
127.0.0.1:5000/dcnminfoblox@sha256:1435c84615fbce1f0fddb2248b7fc458c0bc638913b828de8b5744c1ec96a7ab
untagged: dcnminfoblox:1.2
deleted: sha256:0b4201158dec237cdfc00b0bf87e28937634c73272a153b04c31ffb63b7e9756
deleted: sha256:1d6d3ce3131051bf91cdbb3096ec787461d013f6c363b3aa74b1803f6d9c83b7
deleted: sha256:a4d7c1c1241f78d48412a62308e3b0466c4c1fd5352ea03641b27aa061f5b729
untagged: 127.0.0.1:5000/epl:2.2
untagged:
127.0.0.1:5000/epl@sha256:291add3aee8196378678b925d9d6cced75dc3eb0693df8e01b1db679ec5477ca
untagged: epl:2.2
deleted: sha256:c7ecf09737d11b846896980faff17f00c9ceaf27c3bf27b315a1dd41fd22fe95
deleted: sha256:99cd413c2859a0a0d412389b55442375fb9c273572385c3543187a75163977cf
deleted: sha256:80806d29100d98866b9d65066aa2b00b9c3668355a81a879ab398f7f8f907e61
deleted: sha256:9bc0ff42bf8b34ead128fd4ede58ffb012d28bdcea0f2c42143b0ef7e42337cf
deleted: sha256:ae846bd9c4721ccddf25de117d6d178017c9169211fe2ca224d4ed793228435d
deleted: sha256:e3e5ad8b246eea2de4d86a61a72f36d1b4f0654384d0812c0c48d97fd0578329
deleted: sha256:b28004cbbb822a37c348ce9e96e0caa4347a7e4312be506b0b23d5f0a4898056
deleted: sha256:4ca0ad5f0e35e1db57ff696e578799ffd1e3e7df4e5cbaa7642864dee36a80a5
deleted: sha256:6e805b02a129df11d05ab881d2bd3112ec5ac3fde0d4baff474ea436a45022e2
deleted: sha256:db2d5b490782f132c0f2a8f6b1d8f7a26a1255beb7a9fa09b3050faa231a3fc6
deleted: sha256:e23e9693f114bf44020393394f477e18cfd0cdae74b28febae7b4e34d32dfe9e
deleted: sha256:c1fdf4d0502df0c3c16e23a4f0f7dce37ebc32891dc64fb5abb45227cdefd85a
deleted: sha256:5657c7196ae8853b1df6ebcd4ca9146cd95591d879eacf31664d42a9b05c900a
deleted: sha256:8afaf16caf3eff491e9e07c5e2422644c9a0e3b4560c58b085bdec210e44626e
untagged: basecore:2.0.28
deleted: sha256:3f0c067bc0fb00477a87f80ab39dc8c47d1751f118cf89c853b7490354ea5b91
deleted: sha256:7fba6eecfc4f029baf1c239293d08c7547792184e998f562472c952536759827
deleted: sha256:cc9d960c75bced209d1f887619972faf91312f04d17cfb00818a3665251b73ca
deleted: sha256:65f78f9ec238f6b46fac15428d78996f0024bc3d277119dd329912df4976fcfc
deleted: sha256:1462eb8d1b842b5cfe4a6390adbdd89d8568cd5be9dc5ed81c347e7af0f6a4f2
untagged: 127.0.0.1:5000/dcnmvault:1.2
untagged:
127.0.0.1:5000/dcnmvault@sha256:99439d62230ef05cd0ba4a6587230c6608b25c39e903a6b2ceb6644e4fca0e9a
untagged: 127.0.0.1:5001/dcnmvault:1.2
untagged:
127.0.0.1:5001/dcnmvault@sha256:99439d62230ef05cd0ba4a6587230c6608b25c39e903a6b2ceb6644e4fca0e9a
untagged: 127.0.0.1:5000/vmmplugin:4.2
untagged:
```

```
127.0.0.1:5000/vmmplugin@sha256:45ccc8f40027683a0489f933e51dac9d8e49b8cf40229e6864b2cccb218bda70
untagged: 127.0.0.1:5001/vmmplugin:4.2
untagged:
127.0.0.1:5001/vmmplugin@sha256:45ccc8f40027683a0489f933e51dac9d8e49b8cf40229e6864b2cccb218bda70
untagged: 127.0.0.1:5000/kcvplugin:1.2
untagged:
127.0.0.1:5000/kcvplugin@sha256:01dd37ea97edf4cfa5c5cfbffc47a3e045d8426b349eed19119dc9438797ea33
untagged: 127.0.0.1:5001/kcvplugin:1.2
untagged:
127.0.0.1:5001/kcvplugin@sha256:01dd37ea97edf4cfa5c5cfbffc47a3e045d8426b349eed19119dc9438797ea33
untagged: 127.0.0.1:5000/afwapiproxy:2.3.3
untagged:
127.0.0.1:5000/afwapiproxy@sha256:6ab1a3168d5f7b56b42ddc4735d7c8d9f225ce85e74867e3d1c070348862652f
untagged: 127.0.0.1:5001/afwapiproxy:2.3.3
untagged:
127.0.0.1:5001/afwapiproxy@sha256:6ab1a3168d5f7b56b42ddc4735d7c8d9f225ce85e74867e3d1c070348862652f
untagged: 127.0.0.1:5000/afwceti:1.4
untagged:
127.0.0.1:5000/afwceti@sha256:c7318c33093fdcb1c48aac93193ca86e4ab71db786fcfe9684fc4464f1cb13bd
untagged: 127.0.0.1:5001/afwceti:1.4
untagged:
127.0.0.1:5001/afwceti@sha256:c7318c33093fdcb1c48aac93193ca86e4ab71db786fcfe9684fc4464f1cb13bd
untagged: 127.0.0.1:5000/registry:2
untagged:
127.0.0.1:5000/registry@sha256:35bd3eadeb0e1f30d51063350ca5fc64972c8f9704cf9f64826fed057e83583f
untagged: 127.0.0.1:5001/registry:2
untagged:
127.0.0.1:5001/registry@sha256:35bd3eadeb0e1f30d51063350ca5fc64972c8f9704cf9f64826fed057e83583f
untagged: basearchiver:2.0.28
deleted: sha256:4ad62898be47c0cf38faf3e53e3a9ef9596036ed0f696abefef6a24dc07bf612
deleted: sha256:6197fd46cf469f88763f9cdd851dd299b3b8fe89a328f7d2d9b91b27ad005d9a
deleted: sha256:92b58f47fd3f07efefb4a37d6300cf4d9d50654c14d0156ad13028f3b9b713b0
deleted: sha256:deb230646f11981f805717e621a3cdbe7c79720941ea28d61c5cb5d2a3967e0b
deleted: sha256:23a1953b554d4459772dea3c7e6e17f95387ab6cbeda2cd431f8c5966d68f691
deleted: sha256:0d9acfa2c30b14c781b68ef56229ec705cf94a5a14dba7dc5cbf4032620c0bac
deleted: sha256:9ef0eeac23f3bb8b2fad196d7cb9c0b2c1930f830598e1cb18b916720d5158a3
deleted: sha256:6a58fb9905a349d036cda0600afbadeb581d999f50ec8e73e25b549866f80e81
deleted: sha256:d00483f1d7312f9b8a64f2fb17ec0603791d788b9236b0b40db7151a33a0af22
deleted: sha256:505f68af87ccd3e247dc14f96ad2cf5a6e9d18d2df78f92b120112598b4d01a5
deleted: sha256:2969a31b51f2a3138c6abac3b11ec127801970f0f6423b38b0e7c53d7a31a565
deleted: sha256:043db469e6c39d0808e69b931daee9f4e2b728c48cd12f2d7e6349a06d8a1585
untagged: baseborglet:2.0.28
deleted: sha256:26513cfcfd9c54e85fc8323db5651469c92bc32c7d809e48a2ab3b47a6e38cca
deleted: sha256:f98e31c97379a97e1bceb77e1392a7c39d0b77495346847086c1b59bce0e52c4
deleted: sha256:947def0e80eb81b52fb9d9d298a39eb1ef11f9de96166c6799868156c7b25321
deleted: sha256:d338942b2f26507a62f11188ad44f0fe0719f8eb724200df591fcf21e4416d62
deleted: sha256:a7467582fa09b1cfa70ab62d82927ba4594b93d0079c9d7497173b0e181b7c27
deleted: sha256:8fadf727f4c3332b5cd5c74c8b77dd5c67367490982538806eea697f7a489229
deleted: sha256:55c0c3ccf50bd8bbcaa5fd81aed551168a6b85c892147aa6e59580db9720dc08
deleted: sha256:419f7434f109250c5aa01574cc044447d752c7e3d974a4301febe5e85f71ba9f
untagged: saninsightpost:1.1
deleted: sha256:9118a7d2897650c6f2aac4af6411031d652688614498c156b455fe99a9463acf
deleted: sha256:59b8900e92bba1e080dcdc1c9804948d9a42eaaae88245936a5e9e9e16765248
deleted: sha256:4a70922d869b247a040d9e07488ceed344d6be6e724c356dd8d78f57e7088df3
untagged: 127.0.0.1:5000/nialite:1.0.4
untagged:
127.0.0.1:5000/nialite@sha256:623853ddfa844d88af0df8de6694cdcab593f854bcb937b652b422ca451fe568
untagged: 127.0.0.1:5001/nialite:1.0.4
untagged:
127.0.0.1:5001/nialite@sha256:623853ddfa844d88af0df8de6694cdcab593f854bcb937b652b422ca451fe568
untagged: 127.0.0.1:5000/ptp:1.2
untagged:
127.0.0.1:5000/ptp@sha256:35f99c8cd6b01fdf5d76fa9ae58126cc20653a3786245c3175711196065e8e0d
untagged: ptp:1.2
```

```
deleted: sha256:ce6ae138209c27b7a0d12daa94889933013be5a9f6bed2753206e44d09acfe97
deleted: sha256:07f9f6746bbf83c8a664cae260526ea4fc1968f751cfa62f17b677a29b9cce2a
deleted: sha256:173f53e67abaff757399c035c6853345e270b8de5b941c144d07b9536d7b62ab
deleted: sha256:c931f5ffb6365398b1ff03376fa9658aeb44d464e19d41a70d21724e0d850599
untagged: baseborgcore:2.0.28
deleted: sha256:6c627d04e8a7bda379b1bc80f015fb6843d6efa417aada1ae72c021b2ebefdaa
deleted: sha256:a654391e5858531676e9e4abaf8bae87312484467cdf8b918596e1a8922cb3ce
deleted: sha256:832064fbf9f156a8ccd37645dd54710ccdec360584c966711525498f1d9e97d5
deleted: sha256:f9d249b96a8ac9a335e5169da42d13e16a483779723bc142aa49b7c2c4763249
deleted: sha256:99a8f4fbba9b89e4062e90a7eed1c91885bef8df1843d8bd85441700bdda25cd
deleted: sha256:3ba223bbf41c85b50e2b274bccf74615fa2e90b8f775629423cb507525accb1e
deleted: sha256:5c91d22e76637d81ff652909cf8a3b1f01c9fb224d8511adfb674a2d62412e51
untagged: basedeviceprofile:2.0.28
deleted: sha256:2e0acba3eb04f6d2258a508334c4deee56d44e0f9f92990aa2ffe3d060d3ea01
deleted: sha256:a70eb20943813378945aef8c051a40c6f6643bb9f0cffc725e8a8bb5430e72b5
deleted: sha256:f0303890a9edddd3d1f7005b7ce766305e0d4599fc69cd19f732ccf8d124f5d5
deleted: sha256:f44438937f3f1831805a6d2ac0bf3b411727296d4bf9ad7cc8500b9d50ab67f0
deleted: sha256:6cf60a47f5b81d321999862f26c79c69e885ebafbc83d554c8042a0030aae82b
deleted: sha256:02e8684acc0028d77895d32deaba9b43832bee56a0c89744e857b862d645db60
deleted: sha256:0fe8616e89a9fa6727fb2b300b71b0d10e8b85b07dc0a063cd2967591c736b6f
deleted: sha256:b24f81ad0084a7e4a1abe74bfe23552792e6b9c51f45f5e986bf4e7ba331a7d8
deleted: sha256:413010fb70603e562cd32c3af2f2b14f7c273babdabc94ffd129ffaa33aa4566
deleted: sha256:6502ad18354253870c8f84a45382946d3402d7cc81ffcb19193ed852265e1cbc
deleted: sha256:ea0905da00dee6bd89d2a26ad75c2c05a80b6acbf2c39e28b4832b0aec5b4d83
deleted: sha256:bd818ca41d1a0ca679988ff6a672b68bf7528b0d5067ce8e2492b855283d7562
deleted: sha256:1f6336d099cb070086c5c1d2a8e42333014de8cdc2f7a7caca8a667bd391983d
untagged: baseconfigmanager:2.0.28
deleted: sha256:c30873f860682ddf8b42727ebcadd2a6c6c2224180f621ecd64361c5b996302d
deleted: sha256:bc902bae8293d2bfa2184fba847e2fb7ac05873c81551366f2099ccd564247e2
deleted: sha256:1592fc08c6f9683e95f0207a0499528e992a74c25a6f7b7164866eee59feb705
deleted: sha256:ae13906ef73c64317c9ec5953184e3301c8c22467c651758a7c89443eea33a46
deleted: sha256:eddf2ce0e4e4f30a44fc03435e9bea8fe2953fbaf24fc75ecca1ffe5dc9f47c8
deleted: sha256:988d4946fceab00c767eb40482e3aee729d84773d27f06a648d1d1b01007defe
deleted: sha256:736bac0e693c0af30aa052e1c3863cdf96efd8a1083037a5085e3cc1e3a4bfd4
deleted: sha256:230592135c8f973b4d1994d888512d8abb539b6057fae2be30b1052e21effc2e
deleted: sha256:f5db8aefd47d36dbec169ccdaabe632034a49e9bc093b72fdf1dd6910bed89c8
deleted: sha256:c64a618650d4c37596c05de66140504f124a469e951964954a1004d32cae6789
deleted: sha256:3f004fdffc817806f77c49cc042e94fc174684831f75c23687c5b1141cca060c
untagged: basebootstrap:2.0.28
deleted: sha256:db26e192958d43f87c7da3a26996c0e6ff2e1373b9af9a07d76681ebefea8367
deleted: sha256:fa308ce807c665ae265145374a882ea64ef8e92dfa18aa7b274ac917d3824df6
deleted: sha256:cdbb403caebe9fa381e5de58f3e459fc4fb30c6475424aaef4618ea69d56a828
deleted: sha256:40cb00d5093b0821bae5abe0edc6b387cee17e93a616b4203bc77eaee3e63de4
deleted: sha256:750ed74d6c7367fe39ef908178ea63448de89c3c10249e99a0504b7280a89418
deleted: sha256:741e829bf4d575edcce9585a84de15cc66c3622f9d898497d5c442abc25338c0
deleted: sha256:a6c1e151b345001750759ff4042771f1e784f876c42f8f895a56f085257dd57b
deleted: sha256:d2aae74624eaa4416a1d861b733e6c2b7e643e5fa24ebcf7f5e2b6a1287b662e
deleted: sha256:e6917d5a8b9f6d8206c641407120502d06956e13d237a8e4803fe82d9263ce2f
deleted: sha256:9034b5ff36d35feb7914ae97d57dd8af3a840e0ba809328d9b3379acc5631d18
deleted: sha256:e6166d282b8204db9cecc6b0dfa8cff8464300e28f08c593f23e5b62501a65c
untagged: 127.0.0.1:5000/dcnmelastic:6.8.3_11.5.2
untagged:
127.0.0.1:5000/dcnmelastic@sha256:e561c11835c635141a07665d45af3f2a30ebccc9d6e756ea6eb98b5c766e4f7a
untagged: 127.0.0.1:5001/dcnmelastic:6.8.3_11.5.2
untagged:
127.0.0.1:5001/dcnmelastic@sha256:e561c11835c635141a07665d45af3f2a30ebccc9d6e756ea6eb98b5c766e4f7a
untagged: 127.0.0.1:5000/compliance:5.0.2
untagged:
127.0.0.1:5000/compliance@sha256:b9d028fcbc708cc997bfb7d6701889d43f4877772bede2777bca87f765ec4d25
untagged: 127.0.0.1:5001/compliance:5.0.2
untagged:
127.0.0.1:5001/compliance@sha256:b9d028fcbc708cc997bfb7d6701889d43f4877772bede2777bca87f765ec4d25
untagged: 127.0.0.1:5000/eplui:2.2
untagged:
```

```
127.0.0.1:5000/eplui@sha256:f675abc97f7d231c4f00268002ca98520b166da4b4af05290cb65500900585a5
untagged: 127.0.0.1:5001/eplui:2.2
untagged:
127.0.0.1:5001/eplui@sha256:f675abc97f7d231c4f00268002ca98520b166da4b4af05290cb65500900585a5

Total reclaimed space: 2.21GB
```

After that, the log4j scanner tool can be run. A sample post patch run output is depicted below:

CLI snap of a sample result - CVE-2021-44228 Vulnerability Scanner 2.7.2 (2022-01-15)

```
[root@dcnm]# ./log4j2-scan /
Logpresso CVE-2021-44228 Vulnerability Scanner 2.7.2 (2022-01-11)
Scanning directory: / (without /dev, /dev/shm, /run, /sys/fs/cgroup, /proc/sys/fs/binfmt_misc,

/var/lib/docker/containers/fcb139bf718c1ea432eb59a0b1ab1bc1393e4223e56cfb7c17f900621ab666f1/shm,

/var/lib/docker/containers/d49d1ba94ee10a36ee05f1fe6db14a8961dd327116ad80fbbcfdc49fc64849f2/shm,

/var/lib/docker/containers/d49d1ba94ee10a36ee05f1fe6db14a8961dd327116ad80fbbcfdc49fc64849f2/secrets,

/var/lib/docker/containers/2e09a0d7e4ac04db9b3d4645429a7b7d9bd6600c3cae0a29f33f5ec74f734c9b/shm,

/var/lib/docker/containers/2e09a0d7e4ac04db9b3d4645429a7b7d9bd6600c3cae0a29f33f5ec74f734c9b/secrets,

/var/lib/docker/containers/30fa64dd97fe50a4e7300763b72a1c3963d61f69c6dac7f765b54ba66e02026a/shm,

/var/lib/docker/containers/30fa64dd97fe50a4e7300763b72a1c3963d61f69c6dac7f765b54ba66e02026a/secrets,

/var/lib/docker/containers/bd3c36ce282bce8fed65a984cc4ce72cddb13ab34ad6d99c06e79dbbe209f291/shm,

/var/lib/docker/containers/bd3c36ce282bce8fed65a984cc4ce72cddb13ab34ad6d99c06e79dbbe209f291/secrets,

/var/lib/docker/containers/4403a31bef7fe9c4ad9c6fd8b252284ce33ed975e69ebb2ddb99dc1dcf1537fc/shm,

/var/lib/docker/containers/4403a31bef7fe9c4ad9c6fd8b252284ce33ed975e69ebb2ddb99dc1dcf1537fc/secrets,

/var/lib/docker/containers/637ab772ed0960c8c74c5e163ef3052a6703d3d92373b11ce1e75a515e26af38/shm,

/var/lib/docker/containers/f8a04a8159d1fde7d214fcf33d9e87c1091d944df0d6ef9f0b9a23c48871ff78/shm,

/var/lib/docker/containers/637ab772ed0960c8c74c5e163ef3052a6703d3d92373b11ce1e75a515e26af38/secrets,

/var/lib/docker/containers/f8a04a8159d1fde7d214fcf33d9e87c1091d944df0d6ef9f0b9a23c48871ff78/secrets,

/var/lib/docker/containers/89ceda6e8934683c889c4e7be0a736cdf6290ab8feba3ab4476b29f3cf02e763/shm,

/var/lib/docker/containers/89ceda6e8934683c889c4e7be0a736cdf6290ab8feba3ab4476b29f3cf02e763/secrets,

/var/lib/docker/containers/6e874d498653784662fc9bf677fc154dbf43dcdd967220d9f20224b9f2c21e5a/shm,

/var/lib/docker/containers/b730b7aa02d0f15c4372b40ae5b970a1f95c18b9c2e9e5b771adf82d80883d9c/shm,

/var/lib/docker/containers/6e874d498653784662fc9bf677fc154dbf43dcdd967220d9f20224b9f2c21e5a/secrets,

/var/lib/docker/containers/2af1d590e322f0756f707ab011b3aba8f0101f25d59c5263fe8502d1b18466fd/shm,

/var/lib/docker/containers/2af1d590e322f0756f707ab011b3aba8f0101f25d59c5263fe8502d1b18466fd/secrets,

/var/lib/docker/containers/d60c21eade5f0b9d9c384e3e9d1ed71a0a3ff3256cd67d7b070f9da4d1f207a3/shm,

/var/lib/docker/containers/d60c21eade5f0b9d9c384e3e9d1ed71a0a3ff3256cd67d7b070f9da4d1f207a3/secrets,

/var/lib/docker/containers/33cb0313acac974be15732d0ffbfbf612364f3b1e56be1b8423b98b20c2b4512/shm,
```

```
/var/lib/docker/containers/0fe9e377b0d506e32e2298909ef2316b8897ce86ff9758a4ca1f0f709eefbbc1/shm,

/var/lib/docker/containers/eb7f46e96ab062949bc80bcd5b082102120a93ce276291178b3a01cbdb0176a6/shm,

/var/lib/docker/containers/33cb0313acac974be15732d0ffbfbf612364f3b1e56be1b8423b98b20c2b4512/secrets,

/var/lib/docker/containers/0fe9e377b0d506e32e2298909ef2316b8897ce86ff9758a4ca1f0f709eefbbc1/secrets,

/var/lib/docker/containers/eb7f46e96ab062949bc80bcd5b082102120a93ce276291178b3a01cbdb0176a6/secrets,

/var/lib/docker/containers/575ac722dc3e59fa648b34061f8c0092e22ac9212e646e5eab67d6e39079d142/shm,

/var/lib/docker/containers/575ac722dc3e59fa648b34061f8c0092e22ac9212e646e5eab67d6e39079d142/secrets,

/run/user/1002,
/var/lib/docker/containers/5ea1110b69dd55b7143d0249d16e6995cda4f12f959fad551c88663bf35d1336/shm,

/var/lib/docker/containers/5ea1110b69dd55b7143d0249d16e6995cda4f12f959fad551c88663bf35d1336/secrets,

/var/lib/docker/containers/28d5f24e3d3bf1cd04f26de37637e787f96f4a6cea22b2590248044174434450/shm,

/var/lib/docker/containers/28d5f24e3d3bf1cd04f26de37637e787f96f4a6cea22b2590248044174434450/secrets,

/var/lib/docker/containers/a45b32b86fcc04dfa2c39276734ebb2f08533ba3649eff8cc4068f2b92a4de43/shm,

/var/lib/docker/containers/a45b32b86fcc04dfa2c39276734ebb2f08533ba3649eff8cc4068f2b92a4de43/secrets,

/var/lib/docker/containers/d73dcad858b6bc652aee0fb1f4098bea670146f46cd0be234d4ba442aeab9642/shm,

/var/lib/docker/containers/d73dcad858b6bc652aee0fb1f4098bea670146f46cd0be234d4ba442aeab9642/secrets)
Running scan (11s): scanned 4052 directories, 22291 files, last visit:
/var/lib/docker/overlay2/53f552585d46efec39e40e4109f10b09428ac99c92a97ea923b98d24b7d7ac3/merged/usr/lib/jvm-exports/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
Running scan (55s): scanned 4108 directories, 23291 files, last visit:
/var/lib/docker/overlay2/53f552585d46efec39e40e4109f10b09428ac99c92a97ea923b98d24b7d7ac3/merged/usr/lib64/python2.7/idlelib/idle_test
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-core-2.16.0.jar,
 log4j 2.16.0
Scan error:
'/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-1.2-api-2.11.1.jar
 (No such device or address)' on file:
/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-1.2-api-2.11.1.jar
Scan error:
'/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-core-2.11.1.jar
 (No such device or address)' on file:
/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-core-2.11.1.jar
Scan error:
'/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-api-2.11.1.jar
 (No such device or address)' on file:
/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/lib/log4j-api-2.11.1.jar
Scan error:
'/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/bin/elasticsearch-sql-cli-6.8.3.jar
 (No such device or address)' on file:
/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/bin/elasticsearch-sql-cli-6.8.3.jar
Scan error:
'/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/modules/x-pack-security/log4j-slf4j-impl-2.11.1.jar
 (No such device or address)' on file:
/var/lib/docker/overlay2/dba8d3fa55736a29219034b6488a5ec97ea334054442cf83e550d6268452f339/diff/usr/share/elasticsearch/modules/x-pack-security/log4j-slf4j-impl-2.11.1.jar
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/857fbaa740b735483808ccfded8cb3a1731075739e657a636e4761e28dbc1654/diff/elastic_service/dcnm-elastic-service.jar
 (BOOT-INF/lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (65s): scanned 18734 directories, 128581 files, last visit:
/var/lib/docker/overlay2/d3c3355795268b6a6e2763e5756f3c47ba0aed083fa961d5981749f8f/diff/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64/jre/lib/ext
Running scan (108s): scanned 18937 directories, 129581 files, last visit:
/var/lib/docker/overlay2/58f1ff142b4c310ebf2d28bb722a6a3059b49b8620b615d061083/merged/var/lib/yum/yumdb/l/2e6f727e835464bb62f3e1ddadb982a5a0l-libverto-0.2.5-4.el7-x86_64
```

```
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/927f72952c7e12cdc44faee53427550 6fdbe833a8e1286a96f608d0e1f9a8934/diff/usr/share/elasticsearch/lib/log4j-core-2.11.1.jar,
 log4j 2.11.1
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/927f72952c7e12cdc44faee53427550 6fdbe833a8e1286a96f608d0e1f9a8934/diff/usr/share/elasticsearch/bin/elasticsearch-sql-cli-6.8.3.jar,
 log4j 2.11.1
Running scan (119s): scanned 22623 directories, 161616 files, last visit:
/var/lib/docker/overlay2/f4bcd24a9b01ac86004e36db483fda312481950ec320eb32756f79c6a27072825/merged/usr/share/elasticsearch/lib/tools/security-cli
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/f4bcd24a9b01ac86004e36db483fda312481950ec320eb32756f79c6a27072825/merged/usr/share/elasticsearch/lib/log4j-core-2.16.0.jar,
 log4j 2.16.0
Running scan (130s): scanned 23130 directories, 166506 files, last visit:
/var/lib/docker/overlay2/f4bcd24a9b01ac86004e36db483fda312481950ec320eb32756f79c6a2707 2825/merged/usr/lib/jvm-exports/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
Running scan (171s): scanned 23186 directories, 167506 files, last visit:
/var/lib/docker/overlay2/f4bcd24a9b01ac86004e36db483fda312481950ec320eb32756f79c6a27072825/merged/usr/lib64/python2.7/idlelib/idle_test
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/1f18922f000af35c9036db32719387a65626bc5f3da317de3010303fdbab0fbe/diff/opt/epl/dcmmepl-2.0-SNAPSHOT.jar
 (BOOT-INF/lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (182s): scanned 32250 directories, 245503 files, last visit:
/var/lib/docker/overlay2/ab25775602355 6b2c6ebfb9cd3782c3006f472eddb22017a1322264507c31107/merged/usr/lib/jvm-exports/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
Running scan (223s): scanned 32306 directories, 246503 files, last visit:
/var/lib/docker/overlay2/ab25775602355 6b2c6ebfb9cd3782c3006f472eddb22017a1322264507c31107/merged/usr/lib64/python2.7/idlelib/idle_test
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/ab25775602355 6b2c6ebfb9cd3782c3006f472eddb22017a1322264507c31107/merged/elastic_service/dcnm-elastic-service.jar
 (BOOT-INF/lib/log4j-core-2.16.0.jar), log4j 2.16.0
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/4687e6cf265a07ef206c9dfca92c55578ac94edf413e0adec643120aeb71295c/diff/opt/watchtower/dcnmwatchtower-1.0-SNAPSHOT.jar
 (BOOT-INF/lib/log4j-core-2.16.0.jar), log4j 2.16.0
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/cc5fb692a64e8fa5b74fa69ce8ac471c68318cd242db01d8ed9c0a44b17c31d9/merged/opt/epl/dcmmepl-2.0-SNAPSHOT.jar
 (BOOT-INF/lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (235s): scanned 35581 directories, 271953 files, last visit:
/var/lib/docker/overlay2/cc5fb692a64e8fa5b74fa69ce8ac471c68318cd242db01d8ed9c0a44b17c31d9/merged/usr/lib/jvm-exports/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
Running scan (279s): scanned 35637 directories, 272953 files, last visit:
/var/lib/docker/overlay2/cc5fb692a64e8fa5b74fa69ce8ac471c68318cd242db01d8ed9c0a44b17c31d9/merged/usr/lib64/python2.7/idlelib/idle_test
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/var/lib/docker/overlay2/4f67155e6d233ed8b9c91aa10f03da263624074f29e24db551191dde04a25704/merged/opt/watchtower/dcnmwatchtower-1.0-SNAPSHOT.jar
 (BOOT-INF/lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (290s): scanned 39690 directories, 305761 files, last visit:
/var/lib/docker/overlay2/4f67155e6d233ed8b9c91aa10f03da263624074f29e24db551191dde04a25704/merged/usr/lib/jvm-exports/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64
Running scan (330s): scanned 39746 directories, 306761 files, last visit:
/var/lib/docker/overlay2/4f67155e6d233ed8b9c91aa10f03da263624074f29e24db551191dde04a25704/merged/usr/lib64/python2.7/idlelib/idle_test
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments/dcm.ear
(lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (348s): scanned 51678 directories, 393956 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments
Running scan (359s): scanned 53391 directories, 418216 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment250b67505c5649e8/jviews-framework-all.jar-8e25e8e572048aaf
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment250b6750 5c5649e8/log4j-core-2.16.0.jar-ad088e168bc326dd/log4j-core-2.16.0.jar,
 log4j 2.16.0
Running scan (369s): scanned 53997 directories, 420135 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment250b67505c5649e8/xmlbeans-2.3.0.jar-587720b9202c5028
Running scan (392s): scanned 55099 directories, 421135 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/modules/system/layers/base/org/wildfly/extension/rts/main
Running scan (403s): scanned 57805 directories, 436350 files, last visit:
/usr/local/cisco/dcm/smis/server/java/jre1.8_152/lib/oblique-fonts
Running scan (417s): scanned 57920 directories, 437350 files, last visit:
/usr/local/cisco/dcm/fm/help/vxlanhelp/css
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/root/packaged-files/pmn/pmn-telemetry.jar, log4j 2.16.0
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.5.3a-p1.backup/dcm.ear
 (lib/log4j-core-2.8.2.jar), log4j 2.8.2
```

```
Running scan (438s): scanned 58763 directories, 445252 files, last visit:
/root/patch-11.5.3a-p1.backup

Scanned 59475 directories and 447565 files
Found 14 vulnerable files
Found 0 potentially vulnerable files
Found 0 mitigated files
Completed in 438.27 seconds
```

Note Installing SMU on Cisco DCNM addresses CVE-2021-44228 and CVE-2021-45046. As CVE-2021-45105 is lower severity, and refers to an issue with a configuration which is not used in Cisco DCNM with the default shipping configuration. Therefore, CVE-2021-45105 is not addressed in this SMU installation.

The backup contains original unaltered files which are still vulnerable. They are not used, but are retained as a reference. If you choose to delete, no functionality will be impacted. There are few files which are inside of container filesystem layers. These files record the changes to the container filesystems and are not a concern until they do not appear in the “merged” container files. These files are not available to processes at run-time. There are no vulnerable files in the merged resultant container filesystems.

Note After DCNM HA failover, the log4j2 scan may show some vulnerabilities. This is due to the old docker image package bundle in the Standby server, which is not available for use at run-time for any process. If the CVE reports are still seen, execute the **docker image prune -a** command. This results in clearing the stale entries on the Standby node. After clearing stale entries, there will be no issues during further DCNM HA failovers. If the scan report still shows some CVE errors, we recommend that you contact Cisco TAC.

Validating of SMU Installation

To validate that the patch has been successfully applied on Cisco DCNM appliances and Compute nodes, check the contents of the file located at **`/root/packaged-files/properties/dcnm-version.txt`**. If the patch is successfully applied, an extra line is included in the dcnm-version.txt as shown below:

PATCH_LIST=X

where,

X is the number of patches installed on your Cisco DCNM appliance.