# Upgrading Cisco DCNM

This chapter provides information about upgrading Cisco DCNM, and contains the following section:



## Upgrading Cisco DCNM

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(3).

**Note** Cisco DCNM Release 11.5(3) does not support IP Fabric for Media (IPFM) and SAN Deployments.

| Deployment Type | Current Release Number | Upgrade type to upgrade to Release 11.5(3) |
|---|---|---|
| LAN Fabric | 11.5(2) | Inline Upgrade |
| | 11.5(1) | Inline Upgrade |

## Upgrading ISO or OVA through Inline Upgrade

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

When you install Cisco DCNM, a self-signed certificate is installed, by default. However, after upgrading to the latest Cisco DCNM Release, you must restore the certificates.

**Note** Restoring certificates is a disruptive mechanism; it requires you to stop and restart applications. Restore the certificates only when the upgraded system is stable, that is, you must be able to login to Cisco DCNM Web UI.

To restore certificates after upgrade, see Restoring the certificates after an upgrade.

This section contains the procedure to upgrade the DCNM using the Inline Upgrade method.

**Note** For Classic LAN Deployment upgrade, the deployment is automatically converted to LAN Fabric deployment mode when you upgrade to DCNM Release .

# Inline Upgrade for DCNM Virtual Appliance in Standalone Mode

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

Perform the following task to upgrade the DCNM virtual appliance in standalone mode.

### Before you begin

If the Cisco DCNM setup is in clustered mode, ensure that you stop the Network Insights - Resources (NIR) 2.x application. On the Cisco DCNM Web UI, choose **Applications > Catalog**. On the NIR app, click **Stop** icon to stop the application. Click **Delete** to remove the application from the Catalog.

### Procedure

**Step 1** Log on to the Cisco DCNM appliance console.

**Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements logon to DCNM via Console/SSH.

- For OVA Installation: On the OVF template deployed for the host, right click and select **Settings > Launch Web Console**.
- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

**Caution** Do not perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

OR

Run the following command to create a screen session.

```
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 2** Take a backup of the application data using the **appmgr backup** command.

```
dcnm# appmgr backup
```

Copy the backup file to a safe location outside the DCNM server.

**Step 3** Log on to the `/root/` directory, by using the **su** command.

```
dcnm# su
Enter password: <<enter-password>>
[root@dcnm]#
```

**Note** Ensure that you have access to the `/root/` folder before you mount the ISO to the directory.

**Step 4** Create folder that is named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm]# mkdir /mnt/iso
```

**Step 5** Navigate to **/mnt/iso/packaged-files/scripts/** and run the **./inline-upgrade.sh** script.

```
[root@dcnm]# cd /mnt/iso/packaged-files/scripts/
dcnm# ./inline-upgrade.sh
Do you want to continue and perform the inline upgrade to ? [y/n]: y
```

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.2(1) only.

**Step 6** Provide the new sysadmin user password at the prompt:

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.2(1) only.

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

**Step 7** Ensure that the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm]# appmgr status all
```

**Step 8** To verify that you have successfully installed the Cisco DCNM Release , use the **appmgr show version** command.

```
[root@dcnm]# appmgr show version

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

**Step 9** Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm]# exit
```

**Step 10** Unmount the  file from the DCNM setup.

**Note** You must terminate the screen session before unmounting the **.iso** file.

```
[root@dcnm]# umount /mnt/iso
```

### What to do next

Log on to the DCNM Web UI with appropriate credentials.

**Note** In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(3), 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.

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

The old PM data is retained in Elasticsearch. Elasticsearch shows as reindex required on Cisco DCNM **Web UI > Dashboard > Health** and **Administration > DCNM Server > Server Status**.

If you choose to conserve the Performance Manager data when you upgrade to Release , we recommend that you contact Cisco TAC for further assistance.

If you choose to conserve the Performance Manager data, we recommend that you contact Cisco TAC for further assistance.

To gracefully onboard Cisco DCNM Release 11.2(1), Release 11.3(1), or Release 11.4(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.5(1), see Post DCNM 11.5(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.

# Inline Upgrade for DCNM Virtual Appliance in Native HA Mode

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

Perform the following task to upgrade the DCNM virtual appliance in Native HA mode.

### Before you begin

- Ensure that both the Cisco DCNM Active and Standby peers are up and running.
- Before upgrading Cisco DCNM in Clustered mode, stop the Network Insights - Resources (NIR) 2.x application. On the Cisco DCNM Web UI, choose **Applications > Catalog**. On the NIR app, click Stop icon to stop the application. Click Delete to remove the application from the Catalog.

**Note** Inline upgrade of Cisco DCNM in Clustered mode is supported from Release 11.2(1). Release 11.1(1) doesn't support inline upgrade for DCNM in clustered mode.

- 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
```

### Procedure

**Step 1** Unzip the file and upload the file to the `/root/` folder in both Active and Standby node of the DCNM setup that you want to upgrade.

**Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

**Step 2** Log on to the Cisco DCNM appliance console.

**Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements logon to DCNM via Console/SSH.

- For OVA Installation: On the OVF template that is deployed for the host, right click and select **Settings > Launch Web Console**.
- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

**Caution** Do not perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

OR

Run the following command to create a screen session.

```
dcnm1# screen
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 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
```

Copy the backup file to a safe location outside the DCNM server.

**Step 4** Log on to the **/root/** directory by using the **su** command.

```
dcnm1# su
Enter password: <<enter-password>>
[root@dcnm1]#
```

```
dcnm2# su
Enter password: <<enter-password>>
[root@dcnm2]#
```

**Note** Ensure that you have access to the /root/ folder before you mount the ISO to the directory.

**Step 5** On the Active node, perform the inline upgrade.

a) Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm1]# mkdir /mnt/iso
```

b) Mount the DCNM ISO file on the Active node in the `/mnt/iso` folder.

c) Navigate to **/mnt/iso/packaged-files/scripts/** location and run the **./inline-upgrade.sh** script.

```
[root@dcnm1]# cd /mnt/iso/packaged-files/scripts/
dcnm1# ./inline-upgrade.sh
```

**Note** If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press **y** to continue.

d) Provide the new sysadmin user password at the prompt:

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

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 upgrade Standby node.

f) Verify the role of the Active node, by using **appmgr show ha-role** command. Current role must show as Active.

```
[root@dcnm1]# appmgr show ha-role

Native HA enabled.
Deployed role: Active
Current role: Active
```

**Warning** We recommend that you do not continue to upgrade the Standby node, unless the Active node Current role is Active.

**Step 6** On the Standby node, perform the inline upgrade.

a) Create folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm2]# mkdir /mnt/iso
```

b) Mount the DCNM ISO file on the Standby node in the `/mnt/iso` folder.

c) Navigate to **/mnt/iso/packaged-files/scripts/** location and run the **./inline-upgrade.sh** script.

```
[root@dcnm2]# cd /mnt/iso/packaged-files/scripts/
dcnm2# ./inline-upgrade.sh --standby
```

**Note** If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press y and continue.

d) Provide the new sysadmin user password at the prompt:

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

After the upgrade is complete, the appliance reboots. Verify the role of the appliance, using the following command:

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

**Step 7** Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm1]# exit
[root@dcnm2]# exit
```

**Step 8** Unmount the  file in both Active and Standby node of the DCNM setup.

**Note** You must terminate the screen session before unmounting the **.iso** file.

```
[root@dcnm1]# umount /mnt/iso
[root@dcnm2]# umount /mnt/iso
```

### What to do next

Log on to the DCNM Web UI with appropriate credentials.

**Note** In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(3), 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.

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

The old PM data is retained in Elasticsearch. Elasticsearch shows as reindex required on Cisco DCNM **Web UI > Dashboard > Health** and **Administration > DCNM Server > Server Status**.

If you choose to conserve the Performance Manager data, we recommend that you contact Cisco TAC for further assistance.

Verify the role of both the appliances using the **appmgr show ha-role**

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

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

Verify the status of all applications using the **appmgr status all** command.

To gracefully onboard Cisco DCNM Release 11.2(1), Release 11.3(1), or Release 11.4(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.5(1), see Post DCNM 11.5(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.

# Inline Upgrade for DCNM Compute Nodes

You can upgrade the DCNM compute nodes from using the inline upgrade. Inline upgrade allows you to upgrade the compute node by imposing the new DCNM version to the existing compute node.

**Note** You can upgrade the Compute nodes on Cisco Application Services Engine for Cisco DCNM Release 11.3(1) to using the inline upgrade procedure. For more information, refer to https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html.

Perform the following task to upgrade the DCNM compute node in both Standalone and Native HA modes.

### Before you begin

Cisco DCNM Servers in either Standalone node or Native HA mode must be upgraded to Release , before upgrading the DCNM compute nodes.

### Procedure

**Step 1** Log on to the Cisco DCNM Compute console.

**Caution** Don’t perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

**Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements logon to DCNM via Console/SSH.

OR

Run the following command to create a screen session on the compute node.

```
dcnm-compute# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window isn’t visible or if you get disconnected.

**Step 2** Create folder that is named **iso** using the **mkdir /mnt/iso** command, on all the computes.

```
dcnm-compute# mkdir /mnt/iso
```

**Step 3** Mount the DCNM ISO file on the compute node in the `/mnt/iso` folder.

Mount the ISO on all the compute nodes.

**Step 4** Navigate to **/mnt/iso/packaged-files/scripts** and run the **./inline-upgrade.sh** script.

**Note** If some services are still running, a prompt to stop the services appears. When prompted, press **y** to continue.

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

**Step 5** Provide the new sysadmin user password at the prompt:

```
Enter the password for the new sysadmin user:<<sysadmin_password>>
Enter it again for verification:<<sysadmin_password>>
```

After the upgrade is complete, the compute node reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

**Step 6** Verify that you have successfully upgraded to Cisco DCNM Release , using the **appmgr show version** command.

```
dcnm-compute# appmgr show version

Cisco Data Center Network Manager
Version:
Install mode: Compute
```

**Step 7** Terminate the **screen** session, by using the **exit** command on all compute nodes.

```
dcnm-compute# exit
```

**Step 8** Unmount the  file from all compute nodes of the DCNM setup.

**Note** You must terminate the screen session on all compute nodes before unmounting the **.iso** file.

```
dcnm-compute# umount /mnt/iso
```

### What to do next

You must upgrade all the three compute nodes in the cluster.

After the Upgrade process is complete, each compute node will reboot and join the cluster automatically. On the Cisco DCNM Web UI, choose **Applications > Compute** to verify if the compute node appears as **Joined**.

To gracefully onboard Cisco DCNM Release 11.2(1), Release 11.3(1), or Release 11.4(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.5(1), see Post DCNM 11.5(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.