Migrating From DCNM to NDFC

Prerequisites and Guidelines

Note If you are already running Nexus Dashboard with Fabric Controller service, skip this section and upgrade as described in Upgrading Existing ND Cluster to This Release instead.

Upgrading from DCNM 11.5(4) consists of the following workflow:

1. Ensure you complete the prerequisites and guidelines described in this section.
2. Back up your existing configuration using a migration tool specific to the target NDFC release.
3. Deploy a brand new Nexus Dashboard cluster with Fabric Controller (NDFC) service.

   Note that unlike in previous releases where you had to install the service and enable it after the cluster was already deployed, in this release you enable the service during initial cluster deployment due to the introduction of the unified installation.
4. Restore the configuration backup you created in step 1.

Note Before you proceed with the upgrade, validate each fabric's credentials.

For LAN fabrics, navigate to the **Web UI** > **Administration** > **Credentials Management** > **LAN Credentials** page, select each fabric, and choose **Validate** to validate credentials.

For SAN fabrics, navigate to the **Web UI** > **Administration** > **Credentials Management** > **SAN Credentials** page, select each fabric, and choose **Validate** to validate credentials.

Persona Compatibility

By using the appropriate Upgrade Tool, you can restore data that is backed up from DCNM Release 11.5(4) on a newly deployed Nexus Dashboard Fabric Controller for the personas as mentioned in the following table:

Backup from DCNM 11.5(4)	Persona Enabled in NDFC After Upgrade
DCNM 11.5(4) LAN Fabric Deployment on OVA/ISO/SE	Fabric Controller + Fabric Builder
DCNM 11.5(4) PMN Deployment on OVA/ISO/SE	Fabric Controller + IP Fabric for Media (IPFM)
DCNM 11.5(4) SAN Deployment on OVA/ISO/SE	SAN Controller
DCNM 11.5(4) SAN Deployment on Linux	SAN Controller
DCNM 11.5(4) SAN Deployment on Windows	SAN Controller

Feature Compatibility Post Upgrade

The following table lists caveats associated with features that are restored from DCNM 11.5(4) backup after upgrading.

Note SAN Insights and VMM Visualizer features are not enabled after restore; you can choose to enable them in the **Settings** > **Feature Management** page of the Nexus Dashboard Fabric Controller UI.

Feature in DCNM 11.5(4)	Upgrade Support
Nexus Dashboard Insights configured Refer to Cisco Nexus Dashboard User Guide for more information.	Supported
Container Orchestrator (K8s) Visualizer	Supported
VMM Visibility with vCenter	Supported
Nexus Dashboard Orchestrator configured	Not Supported
Preview features configured	Not supported
LAN switches in SAN installations	Not supported
Switches discovered over IPv6	Not supported
DCNM Tracker	Not supported
Fabric Backups	Not supported
Report Definitions and Reports	Not supported
Switch images and Image Management policies	Not supported
SAN CLI templates	Not carried over from 11.5(4)
Switch images/Image Management data	Not carried over from 11.5(4)
Slow drain data	Not carried over from 11.5(4)

Feature in DCNM 11.5(4)	Upgrade Support
Infoblox configuration	Not carried over from 11.5(4)
Endpoint Locator configuration	You must reconfigure Endpoint Locator (EPL) post upgrade. However, historical data is retained up to a maximum size of 500 MB.
Alarm Policy configuration	Not carried over from 11.5(4)
Performance Management data	CPU/Memory/Interface statistics up to 90 days is restored post upgrade.
Temperature data	Temperature data is not saved in the backup and as a result is not restored after the migration. You must re-enable temperature data collection after the migration.

Migrate Existing DCNM Configuration to NDFC

This section describes how to back up your existing DCNM 11.5(4) configuration, deploy a new Nexus Dashboard cluster, and restore the configuration to finish the migration.

Procedure

Step 1 Download the upgrade tool.

a) Navigate to the NDFC download page..

https://software.cisco.com/download/home/281722751/type/282088134/

b) In the **Latest Releases** list, choose the target release.

c) Download the upgrade tool appropriate for your deployment type.

DCNM 11.5(4) deployment type	Upgrade Tool File Name
ISO/OVA	`DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip`
Linux or Windows	`DCNM_To_NDFC_12_2_1_Upgrade_Tool_LIN_WIN.zip`

d) Copy the upgrade tool image to your existing DCNM 11.5(4) server using the **sysadmin** account.

Step 2 Extract the archive and validate the signature for Linux/Windows deployments.

Note
If you are using the ISO/OVA archive, skip to the next step.

a) Ensure that you have Python 3 installed.

```
$ python3 --version
Python 3.9.6
```

b) Extract the downloaded archive.

```
# unzip DCNM_To_NDFC_12_2_1_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_12_2_1_Upgrade_Tool_LIN_WIN.zip
 extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
 extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
  inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
  inflating: cisco_x509_verify_release.py3
```

c) Validate signature.

Inside the ZIP archive, you will find the upgrade tool as well as the signature file. Use the following commands to validate the upgrade tool:

```
# ls -l
total 4624
-rw-rw-r-- 1 root root    1422 Aug 11  2023 ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
-rwxr-xr-x 1 root root   16788 Feb 26 15:57 cisco_x509_verify_release.py3
-rw-r--r-- 1 root root 2344694 Feb 27 07:51 DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
-rwxr-xr-x 1 root root 2359065 Feb  2 09:19 DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
-rw-rw-r-- 1 root root     256 Feb 26 16:54 DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature

# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v dgst
 -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

d) Once the validation script signature is verified, extract the script itself.

```
# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
   creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat
   creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbackup.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
```

Step 3 Extract the archive and validate the signature for ISO/OVA deployments.

Note
If you are using the Linux/Windows archive, skip to the next step.

a) Extract the downloaded archive.

```
# unzip DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
Archive:  DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
```

```
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

b) Validate signature.

Inside the ZIP archive, you will find the upgrade tool as well as the signature file. Use the following commands to validate the upgrade tool:

```
$ ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_OVA_ISO -s DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature -v dgst -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_OVA_ISO using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

Step 4 Back up existing configuration.

The backup tool collects last 90 days Performance Management data.

a) Log in to your DCNM Release 11.5(4) appliance console.
b) Create a screen session.

The following command creates a session which allows you to execute additional commands:

```
dcnm# screen
```

Note that the commands continue to run even when the window is not visible or if you get disconnected.

c) Gain super user (`root`) access.

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

d) For OVA and ISO, enable execution permissions for the upgrade tool.

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
```

e) Run the upgrade tool you downloaded in the previous step.

- For Windows:

```
G:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:

Initializing, please wait...

********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 is possible, this tool will create files to be used for performing
 the upgrade.

Thank you!
```

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

This tool will backup config data. Exporting Operational data like Performance(PM) might take
 some time.

Do you want to export operational data also? [y/N]: y
********************************************************************************


Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.


Please enter the encryption key:
Enter it again for verification:
….
2024-02-26 17:57:32,247 [main] INFO  DCNMBackup - Creating final tar.gz file....
2024-02-26 17:57:32,649 [main] INFO  DCNMBackup - Final tar.gz elapsed time: 402 in ms
2024-02-26 17:57:32,650 [main] INFO  DCNMBackup - Backup done.
2024-02-26 17:57:32,657 [main] INFO  DCNMBackup - Log file: backup.log
2024-02-26 17:57:32,658 [main] INFO  DCNMBackup - Backup file:
backup11_win57_20240226-172247.tar.gz
```

- For Linux:

```
# ./DCNMBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:

Initializing, please wait...

********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 is possible, this tool will create files to be used for performing
 the upgrade.

Thank you!

********************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM) might take
 some time.

Do you want to export operational data also? [y/N]: y
********************************************************************************


Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.


Please enter the encryption key:
Enter it again for verification:
2024-02-27 07:53:46,562 [main] INFO  DCNMBackup - Inside init() method
2024-02-27 07:53:46,564 [main] INFO  DCNMBackup - Loading properties....
2024-02-27 07:53:46,649 [main] INFO  DCNMBackup - Inside checkLANSwitches...
2024-02-27 07:53:46,732 [main] INFO  fms.db - set database url
as:jdbc:postgresql://localhost:5432/dcmdb
2024-02-27 07:53:46,887 [main] INFO  DCNMBackup - LAN Switch count: 0
2024-02-27 07:53:46,889 [main] INFO  DCNMBackup - Inside exportDBTables...
```

```
2024-02-27 07:53:46,892 [main] INFO  DCNMBackup - Exporting ---------> statistics
2024-02-27 07:53:46,903 [main] INFO  DCNMBackup - Exporting ---------> sequence
2024-02-27 07:53:46,964 [main] INFO  DCNMBackup - Exporting ---------> clustersequence
2024-02-27 07:53:46,965 [main] INFO  DCNMBackup - Exporting ---------> logicsvr_fabric
……..
2024-02-27 07:53:49,147 [main] INFO  DCNMBackup - Creating final tar.gz file....
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Final tar.gz elapsed time: 35 in ms
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Backup done.
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Log file: backup.log
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Backup file:
backup11_onefiveseven.cisco.com_20240227-72149.tar.gz
```

- For OVA:

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.

This tool will analyze this system and determine whether you can move to
NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 is possible, this tool will create files
to be used for performing the upgrade.

NOTE:
Only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to NDFC 12.2.1

Thank you!

********************************************************************************

Continue? [y/n]: y

Collect operational data (e.g. PM, EPL)? [y/n]: y

Does this DCNM 11.5(4) have DCNM Tracker feature enabled on any switch on any fabric? [y/n]:
 n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:

Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!


Collecting AFW app info
Decrypting stored credentials
Adjusting DB tables
Creating backup file
```

```
Done.
Backup file: backup11_host108_20240227-153940.tar.gz
```

Step 5 Deploy a brand new Nexus Dashboard cluster as described in one of the earlier chapters in this document.

Ensure that you complete all guidelines and prerequisites for the Nexus Dashboard platform, the Fabric Controller service, and the specific form factor listed in the deployment chapters above.

Note

- You must provide the required number of Persistent IP addresses in the Nexus Dashboard Fabric Controller UI before proceeding with restoring your DCNM configuration..
- If your existing configuration used smart licensing with direct connectivity to Cisco Smart Software Management (CSSM), you must ensure that your new Nexus Dashboard has the routes required to reach the CSSM website.

  Ensure that subnets for IP addresses on `smartreceiver.cisco.com` are added to the route table in the Nexus Dashboard's **Admin** > **System Settings** > **Routes** page for the Nexus Dashboard management network.

  You can ping `smartreceiver.cisco.com` to find the most recent subnet, for example:

  ```
  $ ping smartreceiver.cisco.com
  PING smartreceiver.cisco.com (146.112.59.81): 56 data bytes
  64 bytes from 146.112.59.81: icmp_seq=0 ttl=52 time=48.661 ms
  64 bytes from 146.112.59.81: icmp_seq=1 ttl=52 time=44.730 ms
  64 bytes from 146.112.59.81: icmp_seq=2 ttl=52 time=48.188 ms
  ```

  In addition, because NDFC is considered a new product instance, you must re-establish trust. If you took the backup with an expired Trust Token, you must manually run the Smart Licensing Configuration wizard and enter a valid token after the upgrade.

Step 6 Restore the configuration backup in the new cluster.

a) Log in to your Nexus Dashboard using an admin account.
b) From the dropdown menu at the top, choose **Fabric Controller**.
c) From the left navigation menu, choose **Admin** > **Backup and Restore**.
d) In the main pane, click **Restore**.
e) In the **Restore Now** window, provide the details.
   - Choose **Config Only** or **Full** based on the backup that you created in the previous step.
   - Choose the **Source** where the backup file is located, then upload the file or provide the remote server location and path.
   - Enter the **Encryption Key** you provided during configuration backup.
   - Ensure that the **Ignore External Service IP Configuration** option is unchecked.
f) Click **Next**, verify the information, and proceed to **Restore** the configuration.

   The UI is locked while the restore is in progress; the time required to restore depends on the data in the backup file.

   Once the restore process is completed, click the `x` icon in the **Restore Now** pop-up window to close it.

   After successful restoration, click **Reload the page** or refresh the browser page to complete restore and begin using you Nexus Dashboard Fabric Controller.

Step 7 Complete the post-upgrade tasks.

a) If you are using the SAN Controller persona:

After restoring the data from backup, all the server-smart licenses are **OutofCompliance**.

You can migrate to Smart Licensing using Policy from the **Operations** > **License Management** > **Smart** page in the UI and establish trust with CCSM using SLP.

b) If you are using the Fabric Controller persona:

The following features are not carried over when you upgrade from DCNM 11.5(4):

- Endpoint Locator must be reconfigured
- IPAM Integration must be reconfigured
- Alarm Policies must be reconfigured
- Custom topologies must be recreated and saved
- PM collection must be re-enabled on fabrics
- Temperature data collection must be re-enabled to start collecting data
- Switch images must be uploaded

Deployment Type in Release 11.5(4)	In 11.5(4), trap IP address is collected from	LAN Device Management Connectivity	Trap IP address after upgrade	Result
LAN Fabric Media Controller	`eth1` (or `vip1` for HA systems)	Management	Belongs to Management subnet	Honored There is no configuration difference. No further action required.
LAN Fabric Media Controller	`eth0` (or `vip0` for HA systems)	Management	Does not belong to Management subnet	Ignored, another IP from the Management pool will be used as trap IP. Configuration difference is created. On the **Web UI > LAN > Fabrics > Fabrics**, double click on the Fabric to view **Fabric Overview**. From **Fabrics Actions** drop-down list, select **Recalculate Config**. Click **Deploy Config**.

Deployment Type in Release 11.5(4)	In 11.5(4), trap IP address is collected from	LAN Device Management Connectivity	Trap IP address after upgrade	Result
LAN Fabric Media Controller	`eth0` (or `vip0` for HA systems)	Data	Belongs to Data subnet	Honored There is no configuration difference. No further action required.
LAN Fabric Media Controller	`eth0` (or `vip0` for HA systems)	Data	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP. Configuration difference is created. On the **Web UI** > **LAN** > **Fabrics** > **Fabrics**, double click on the Fabric to view **Fabric Overview**. From **Fabrics Actions** drop-down list, select **Recalculate Config**. Click **Deploy Config**.
SAN Management	OVA/ISO – • `trap.registaddress` (if set) • eth0 (if `trap.registaddress` is not set) Windows/Linux – • `trap.registaddress` (if set) • Interface based on event-manager algorithm (if `trap.registaddress` is not set	Not applicable	Belongs to Data subnet	Honored There is no configuration difference. No further action required.
		Not applicable	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP.