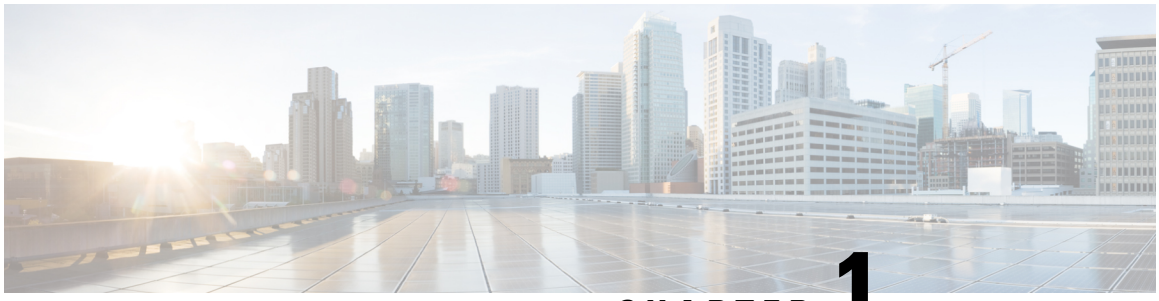
Cisco DCNM Release Notes, Release 11.4(1)

First Published: 2020-07-02

Last Modified: 2021-12-22

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



CHAPTER 1

Overview

Overview

Cisco Data Center Network Manager (DCNM) is the comprehensive management solution for all NX-OS deployments spanning LAN Fabric, SAN, and IP Fabric for Media (IPFM) networks in data centers powered by Cisco. DCNM 11 automates Cisco MDS Switches and Cisco Nexus Family infrastructure, for data center management across Cisco Nexus 1000, 2000, 3000, 5000, 6000, 7000, and 9000 Series Switches in NX-OS mode. From Release 11.3(1), Cisco DCNM also supports non-Nexus devices, such as, IOS-XE, IOS-XR, and Arista devices. DCNM 11 lets you manage a large number of devices while providing ready-to-use control, management, and automation capabilities, plus Virtual Extensible LAN (VXLAN) control and automation for Cisco Nexus LAN fabrics.

For more information, see https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-data-center-network-manager/index.html.

Cisco DCNM Release 11.4(1) manages various kinds of SAN deployments, and LAN deployments (including VXLAN EVPN, Routed Fabrics, FabricPath, 3-tier classic deployments, and so on) in the Cisco NX-OS driven data center environment. To download the Cisco DCNM software, go to Cisco DCNM Software Download, click **Download Software**.

Deployment of Fabrics Using Cisco DCNM 11.4(1):

- **Greenfield Deployments**: Applicable for provisioning new VXLAN EVPN fabrics, and eBGP based Routed fabrics
- **Brownfield Deployments**: Applicable for existing VXLAN EVPN fabrics:
  - Migrate CLI configured VXLAN EVPN fabrics to DCNM using the Easy_Fabric_11_1 fabric template.
  - NFM migration to Cisco DCNM using the `Easy_Fabric_11_1` fabric template.
- **Upgrades**: Applicable for all LAN Fabric deployments created with previous DCNM versions:
  - Upgrade for fabrics built with DCNM 11.3(1) to DCNM 11.4(1)
  - Upgrade for fabrics built with DCNM 11.2(1) to DCNM 11.4(1)
  - Upgrade for fabrics built with DCNM 11.1(1) to DCNM 11.4(1)

Refer to the *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.4(1)*.

Note After upgrading the Classic LAN Deployment to Cisco DCNM Release 11.4(1), you can manage, monitor, automate, and control the Classic LAN deployment via the Cisco DCNM 11.4(1) LAN Fabric installation.

The Classic LAN Installation mode is obsolete in Release 11.4(1), and isn't available in new installations. Existing Classic LAN installations are automatically migrated to the DCNM 11.4(1) LAN Fabric installation mode as a part of the inline upgrade process. For more information, refer to the Upgrading the Cisco DCNM Classic LAN Deployment in the *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.4(1)* .

The existing switches in a switch group and the top-level container switch groups are converted to LAN Fabrics using the **LAN_Classic** and **Fabric_Group** templates respectively. Switches are placed in Migration mode after upgrade. In order to get the switches out of this mode, choose the appropriate LAN_Classic fabric and click **Save & Deploy**. For more information, refer to the External Fabrics in the *Cisco DCNM LAN Fabric Configuration Guide*.

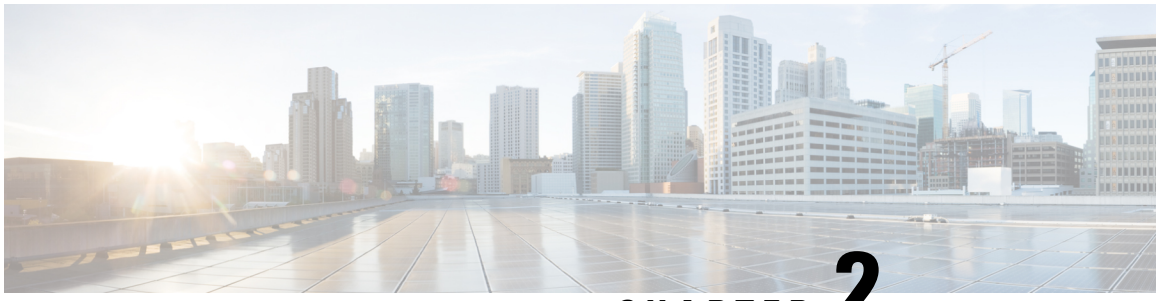
Cisco DCNM LAN Fabric deployment with Compute nodes allows you to install Network Insights applications via the Cisco DCNM Web UI. Refer to *Cisco DCNM Configuration Guide LAN Fabric Deployment.*

This document provides the Release Notes for Cisco DCNM, Release 11.4(1). Use this document with the documents that are listed in the Related Documentation, on page 49.

The following table shows the change history for this document.

Table 1: Change History

Date	Description
22 December 2021	Added Software Maintenance Update for log4j2 Vulnerability
26 July 2020	Added Software Maintenance Update to use NIR 2.2.2 with Cisco DCNM 11.4(1) LAN Fabric deployment.
02 July 2020	Published Release Notes for Cisco DCNM Release 11.4(1)



CHAPTER 2

System Requirements

This chapter lists the tested and supported hardware and software specifications for Cisco Data Center Network Management (DCNM) server and client architecture. The application is in English locales only. This chapter contains the following section:

System Requirements

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 will cause performance issues.

This section describes the various system requirements for proper functioning of your Cisco DCNM, Release 11.4(1).

Note 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.

Java Requirements

The Cisco DCNM Server is distributed with JRE 11.0.6 into the following directory:

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM, Release 11.4(1), supports the Cisco DCNM Server on these 64-bit operating systems:

- **SAN Deployments:**
  - Microsoft Windows 2016
  - Microsoft Windows 2012 R2
  - Red Hat Enterprise Linux Release 7.3, 7.4, 7.6, and 7.7

- Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.8
- ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.8

- **IP for Media, and 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

Database Requirements

Cisco DCNM Release 11.4(1) supports the following databases:

- Oracle11g Express (XE), Standard, and Enterprise Editions, and Oracle 11g Real Application Clusters (RAC)
- Oracle 12c Enterprise Edition (Conventional)—(Nonpluggable installation)

Note From Cisco DCNM Release 11.3(1), Oracle 12c pluggable database version installation is not supported.

- Oracle 12c RAC (nonpluggable installation)
- PostgreSQL 9.6.16 - For OVA/ISO deployments
- PostgreSQL 9.6.16 - For Linux/OVA/ISO deployments
- PostgreSQL 9.6.18 - For Windows deployments

Note The database size increases according to the number of nodes and ports that the DCNM manages, with Performance Manager Collections enabled. You cannot restrict the database size. If you choose an Oracle database, we recommend that you use Oracle SE or Enterprise edition, instead of Oracle XE due to table space limitations.

Note You are responsible for all the support that is associated with the Oracle databases, including maintenance, troubleshooting, and recovery. We recommend that you take regular backup of the database; either daily or weekly, to ensure that all the data is preserved.

Note The ISO/OVA installation only supports 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 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

From Release 11.4(1), Cisco DCNM supports the running of the Cisco DCNM Server on the following hypervisors:

Hypervisor supported	Data Center Manager server application	Supported deployments
ESXi 7.0	vCenter 7.0 **Note** VMM visualization on vCenter 7.0 is not supported with Cisco DCNM 11.4(1).	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.

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	For DCNM[3]

[3] Virtual Machine Manager import for compute visibility with vCenter 7.0 is not supported

Note vCenter server is mandatory to deploy the Cisco DCNM OVA Installer.

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

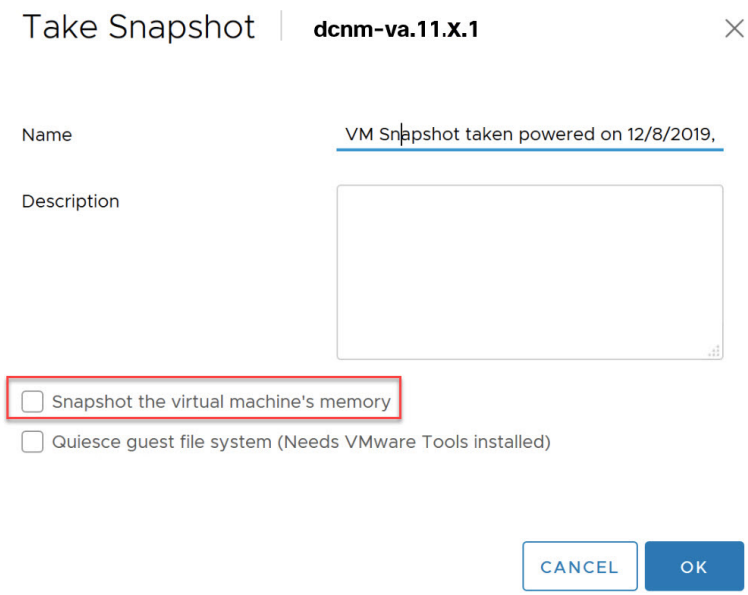
1. Right-click the virtual machine the inventory and select **Snapshots** > **Take Snapshot**.
2. In the Take Snapshot dialog box, enter a **Name** and description for the snapshot.
3. Click **OK** to save the snapshot.

The following snapshots are available for VMs.

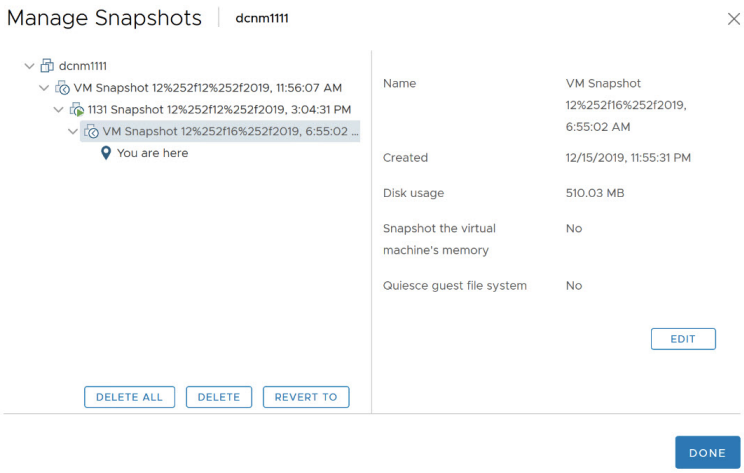
- When VM is powered off.
- When VM is powered on, and active.

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.

Note that the 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**.

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.

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Huge (Production)	Compute	ComputeHuge
SAN	Windows	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not Applicable	Not Applicable	Not Applicable
SAN	Linux (standalone or VM)	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB Disk: 500 GB	With SAN Insights: • CPU: 32 vCPUs • RAM: 128 GB • DISK: 2 TB	Not Applicable	Not Applicable
SAN	• OVA standalone • ISO standalone	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 32vCPUs RAM: 128 GB DISK: 2 TB (with SAN Insights)	Not Applicable	Not Applicable
IP for Media (IPFM)	• OVA • ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not Applicable	Not Applicable	Not Applicable
LAN Fabric	• OVA • ISO • Hyper-V on Windows	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not Applicable	CPU: 16 vCPUs RAM: 64 GB DISK: 500 GB	CPU: 32vCPUs RAM: 128GB DISK: 2TB for Network Insights Applications

Note For Huge and Compute deployments, you can add extra disk. The size of the disk can range from a minimum of 32GB to a maximum of 1.5TB.

Ensure that there is enough disk space to the root partition or mount another disk where the `/tmp` directory can be mounted during the installation or upgrade.

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.

Note

- From Release 11.3(1), Cisco DCNM Windows deployments does not support the SAN Insights feature.
- Cisco SAN Insights feature is only supported with the Huge deployment.
- You can use the SAN Insights feature on a medium-sized deployment with 2 TB disk space.
- Every federation deployment consists of three large configuration nodes.
- From Cisco DCNM Release 11.2(1), synchronize the Federation nodes from the Primary node only.

Cisco DCNM LAN Fabric Deployment Without Network Insights (NI)

Note For information about various system requirements for proper functioning of Cisco DCNM LAN Fabric deployment, see System Requirements.

Refer to *Network Insights User guide* for sizing information for Cisco DCNM LAN Deployment with Network Insights (NI).

To see the verified scale limits for Cisco DCNM 11.4(1) for managing LAN Fabric deployments, see Verified Scale Limits for Cisco DCNM LAN Fabric Deployment.

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
Computes	OVA/ISO	16 vCPUs	64G	500G HDD	3xNIC

Client Hardware Requirements

Cisco DCNM SAN desktop client and Cisco Device Manager support Microsoft Windows 10, Microsoft Windows 2012, Microsoft Windows 2016, and Red Hat Linux. The following table lists the minimum hardware requirements for these client systems.

Hardware	Minimum Requirements
RAM (free)	6 GB or more
CPU speed	3 GHz or faster
Disk space (free)	20 GB

Some Cisco DCNM features require a license. Before using the licensed features, you must install a Cisco DCNM license for each Nexus-managed or MDS-managed platform. For information about Licensing in DCNM, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_x/licensing/cisco_dcnm_licensing_guide_11_x.html.

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome Version 83.0.4103.97
- Mozilla Firefox Version 77.0.1 (64-bit)
- Microsoft Edge Version 83.0.478.45

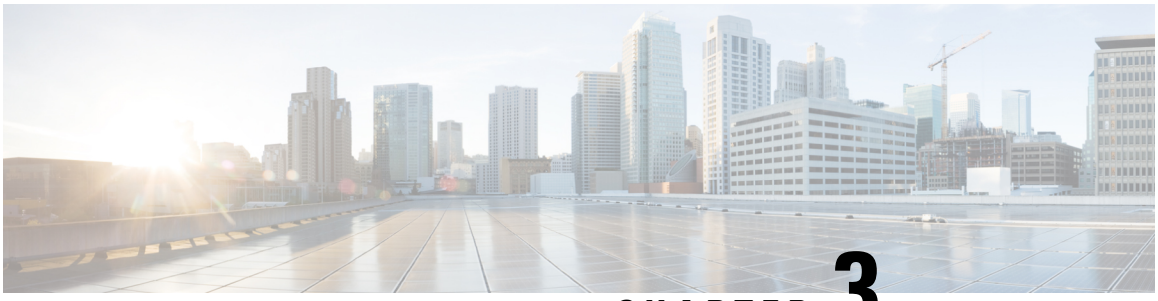
Other Supported Software

The following table lists the other software that is supported by Cisco DCNM, Release 11.4(1).

Table 4: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client and Cisco DCNM-SAN Server 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.



CHAPTER 3

Guidelines and Limitations

Guidelines and Limitations

- You must apply patch for any changes that happen on switch side (Nexus 3000 and/or Nexus 9000), to enable Cisco DCNM to support those features. To apply that patch to your Cisco DCNM Native HA setup, follow the steps below:

  1. Stop the services on the Active node using the **/etc/init.d/FMServer** stop command.
  2. Run **patch.sh** on the Active node.
  3. Run **patch.sh** on Standby node.

  Note Services are not stopped on Standby node.

  4. Start services on the Active node using the **/etc/init.d/FMServer start** command.
  5. Stop the services on Active node using the **/etc/init.d/FMServer stop** command and roll back the patch.
  6. Roll back the patch on the Standby node.
  7. Start services on the Active node using **/etc/init.d/FMServer start** command.

- Ensure that you've installed Visual C++ Redistributable Packages for Visual Studio 2013 64 bit before installing or upgrading to Cisco DCNM Release 11.4(1).
- To check the status of the running Postgres database in Native HA setup, use **pg_ctl** command. Do not use the **systemctl** command.
- Do not begin the password with Hash (#) symbol. Cisco DCNM considers the password as an encrypted text if it begins with # symbol.
- **POAP Dynamic Breakout**—From Cisco NX-OS Release 7.0(3)I4(1), POAP dynamically breaks out ports to detect a DHCP server behind one of the broken-out ports. Previously, the DHCP server that is

used for POAP was directly connected to a normal cable as the breakout cables were not supported. POAP determines which breakout map (for example, 10gx4, 50gx2, 25gx4, or 10gx2) brings up the link that is connected to the DHCP server. If breakout is not supported on any of the ports, POAP skips the dynamic breakout process. After the breakout loop completes, POAP proceeds with the DHCP discovery phase as normal.

Cisco DCNM leverages the dynamic breakout to simplify the fabric setup by retaining successful breakout configuration. Since dynamic breakout requires the other side of the link to be active, there are circumstances where you must manually breakout interfaces, or may notice breakout in places which are not desired. In those situations, you must adjust the ports on the Interfaces page before performing Save and Deploy in the Fabric Builder.

- Before using the licensed features, install a Cisco DCNM license for each Nexus-managed or MDS-managed platform. For information about licensing, see the Cisco DCNM Licensing Guide, Release 11.x.
- Depending on how a switch handles the **cdp enable** CLI command (enabled or disabled by default), Cisco DCNM shows this as config difference, although the Save and Deploy operation is performed to correct it. This depends on the default behavior of the switch image (that is, whether the **show running-config** shows the CLI or not). To address this issue, the respective policy template that is applied on the interfaces must be updated, so that the CLI is ignored during the configuration compliance check.
- Create a free-form configuration on all the white box switches that are managed by Cisco DCNM as shown below, and deploy them on all the switches before the final Save and Deploy operation.

```
line console
speed 115200
stopbits 2
```

  This is only applicable to the Cisco DCNM LAN Fabric mode.
- On Microsoft Windows 2016 Standard server, run the Cisco DCNM installation EXE file as an administrator. Cisco DCNM installation will not start on Microsoft Windows 2016 Standard server unless you set the EXE file as an administrator. To start the installation EXE file, you can right-click on the EXE file, and choose **Run as administrator**.
- When the Cisco Nexus 9000v Virtual Switches are cloned, they may use the same serial number. Since Cisco DCNM discovers them using the same serial number, the device discovery operation fails.
- Addition of FEX or breakout of interfaces is not supported in External Fabrics.
- From Release 11.2(1), you can configure IPv6 address for Network Management for compute clusters. However, DCNM does not support IPv6 address for containers and must connect to DCNM using IPv4 address only.
- You cannot access the Cisco DCNM Web UI, when the user system is configured with the same IP address range as that of internal subnet used by the Application Framework in DCNM. For more information, see *Cisco DCNM Troubleshooting Guide*.
- The VXLAN OAM feature in Cisco DCNM is only supported on a single fabric or site.
- You cannot configure ICAM on the Cisco Nexus 9000 Series Switches Release 7.0(3)I7(6), and therefore, the telemetry will fail until the switch issue is resolved.
- Though you can delete PMN hosts, we recommended that you use this option with extreme caution, understanding that manual effort is needed to bring the solution back in sync.

- Cisco DCNM in Media Controller Deployment Release 11.x does not support non-default VRFs for Cisco Nexus 9000 Release 9.3(x).
- From Cisco DCNM Release 11.2(1), the Device Connector allows you to change the access mode via the Web UI at **Administration > DCNM Server > Device Connector > Settings > General**. The Cisco Intersight will not configure its device connector, and therefore, the Read-Only and Allow Control access mode in the Device Connector are not operational.
- Cisco DCNM does not support hot snapshots. While taking snapshots, we recommend that you power off the VM. Otherwise, ensure that you uncheck the **Snapshot the virtual machine's memory** option.
- Cisco DCNM does not support suspending or unsuspending of the VMs.
- Do not install NIR on standalone DCNM
- If NIR was installed and stopped, it does not stop service containers running on DCNM compute nodes.

  If the NIR application is deleted from DCNM, a few service containers continue to run DCNM compute nodes and must be stopped manually using **afw service** commands.
- 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.
- When DCNM Tracker is enabled, the NIR LAN Telemetry feature in Managed mode and the EPL feature with the **Configure my Fabric** option selected, will not work. As a workaround, disable the DCNM tracker on the switches that are configured during the EPL or NIR LAN Telemetry configuration. For EPL, disable the DCNM tracker on the Spines/Route Reflectors (both RR1 and RR2). For NIR LAN Telemetry, disable the DCNM tracker on all the switches selected for telemetry configuration.
- The DCNM installer creates a `_deviceImage-0.iso` in the DCNM VM folder and mounts the ISO permanently to the VM. If this ISO is removed or the CD/DVD is disconnected, the VM will not boot. The VM will enter Emergency Mode and prompt you with the message:Give root password for maintenance. If the VM is down, CD/DVD drive can be disconnected. However, after you power it up again, the VM will enter Emergency Mode and provide a prompt.
- For leaf-leaf ports in non-VPC cases, DCNM will always push the **shutdown** command. If you want to bring up the port, add the **no cdp enable** command to the interface freeform policy on one of the ports.

  For leaf-leaf or border-border connected ports in non-VPC cases, DCNM will always push the **shutdown** command to avoid the potential of loops in a VXLAN EVPN fabric. To bring up the port, add **no cdp enable** command to the interface freeform policy on one of the ports. Consequently, the link will however not be discovered and consequently not show up in the topology but the interfaces will still be up.
- Two-factor authentication is not supported in DCNM.
- After the eth0 IP address (for standalone deployment) or the vip0 IP address (for Native HA deployment) is modified using the **appmgr update network-properties** command, on the **Web UI > Administration > MultiSite Manager** does not display the correct IP address for AMQP.
- When a Nexus Dashboard server is adding a Site from DCNM 11.5(1), it must reach the DCNM server over the Data Network. DCNM Data Network connectivity is defined to be over eth2 interface of the DCNM server; also known as Inband Connectivity interface in DCNM. When the eth2 connectivity of the DCNM with the Data Network Connectivity of the Nexus Dashboard is spanning multiple subnets, that is, when they are Layer3 Route connected, you must add routes in DCNM before adding the Site on ND.

To add route over the Inband Network in DCNM, on the Cisco DCNM Web UI, choose **Administration > Customzation > Network Preferences**. Enter the Routes to the ND Data Network over the In-band(eth2) inputs of the dashlet. For more information, see Network Preferences-Routes.

- From Release 11.4(1), Cisco DCNM does not support syncing fabric with switches in VTP server mode. For more information, refer to CSCvx86976.
- In Cisco DCNM SAN deployment, if the DCNM server streaming the SAN analytics is over-utilized, the Elasticsearch database service goes down. This results in performance issues. The Pipeline service may be consuming all the CPU and system resources on the Cisco DCNM server. To troubleshoot this, do the following task:
  1. Stop the Pipeline service.
  2. Reduce the streaming load from the MDS fabric.
  3. Start Elasticsearch service.
  4. Start the Pipeline service.
- From Cisco DCNM Release 11.5(2), VLAN range is extended. After patch update for LAN Fabric deployment, you can set VLAN range to 4094.
- In Cisco DCNM SAN deployment, when you enable or disable alarms on a Primary node, it will not be applied to all the nodes in the Federation. You must manually enable or disable alarms on all nodes on all servers in the Federation setup. You must restart the DCNM Server to apply the changes.
- In Cisco DCNM SAN deployment, when you add or delete alarm policies on a Primary node, it will not be applied to all the nodes in the Federation. You must restart all the DCNM servers to apply this change on all servers in the Federation setup.
- In Cisco DCNM SAN deployment, when you modify the server properties on Cisco DCNM **Web UI > Administration > DCNM Server > Server Properties** on a Primary node, it will not be applied to all the nodes in the Federation. You must manually make the changes to the server properties on all nodes on all servers in the Federation setup. You must restart the DCNM Server to apply the changes.
- SAN Insights is not recommended on Windows Deployments, and is no longer supported from Release 11.3(1).
- SAN Insights is best supported on Linux from Release 11.0(1), and on Cisco DCNM OVA/ISO deployments from Release 11.3(1).
- From Cisco DCNM Release 11.3(1), you cannot download the SAN Client package from the Software Downloads page. You must install Cisco DCNM, launch Web UI to download the SAN Client and Device Manager. For more information, *Cisco DCNM Installation and Upgrade Guide for SAN Deployment*.
- In Releases prior to 11.4, if you have installed a preview feature, perform the following before you upgrade to Release 11.4(1):
  - Remove the configuration from older release setup.
  - Reset the property to enable the preview feature. On the Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**. Reset the **enable preview feature** property.
- We recommend that you do not upgrade any underlying third-party software separately. All the necessary software components will be DCNM upgrade will cause performance issues.

- You can choose to discard the old performance manager (PM) data and continue to upgrade to DCNM Release 11.4(1). For instructions about how to drop performance manager data, see *Dropping Performance Manager Data* in the *Cisco DCNM Installation and Upgrade guide* for your deployment. If you choose to retain the old PM data while you upgrade to Release 11.4(1), we recommend that you contact Cisco TAC for further assistance.

Certain commands must not be executed on Cisco DCNM, as they may harm the functionality of various components on the network. The following table shows the commands and specifies the reason why they must not be executed.

Table 5: List of Commands that must not be executed on Cisco DCNM

Command	Reason
systemctl restart network	This is a common Linux command that the network administrators use when editing the interface properties. The command has shown to render the DCNM useless when converting to the cluster mode.
ifconfig ethx y.y.y.y/zz	Any change in the IP addresses of the DCNM nodes must be done with the **appmgr update network-properties** command. This includes changing the FQDN, adding static routes, adding/removing NTP servers etc.

Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard

A few Cisco Application Services Engine (SE) nodes that was factory pre-installed with DCNM 11.4(1) or earlier may have a corrupted TPM partition. This causes the installation of Cisco Nexus Dashboard software to fail. You must check the TPM Partition before upgrading from Cisco DCNM-SE to Cisco Nexus Dashboard.

Note TPM is not a requirement for DCNM 11.x releases. Therefore, this issue does not affect existing DCNM 11.x functionality of the device, even if the device is affected by this issue. No further action is required until you decide to upgrade to Cisco Nexus Dashboard.

To identify if your Cisco DCNM-SE is affected by this issue, perform the following steps:

Step 1 SSH to Cisco Application Services Engine using **sysadmin** user.

Step 2 Run the following command to view the list of models and their vendors.

lsblk-S

```
[root@dcnm-se-active sysadmin]$ lsblk -S
NAME    HCTL       TYPE     VENDOR   MODEL             REV TRAN
...
sdc     0:2:2:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sdd     0:2:3:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sde     0:2:4:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sdf     7:0:0:0    disk     UNIGEN   PQT8000           1100 usb  /*identiifying device from UNIGEN
```

```
Vendor*/
sdg     8:0:0:0     disk      UNIGEN    PHF16H0CM1-ETG     PMAP usb
sdl     1:0:0:0     disk      ATA       Micron_5100_MTFD   H072 sata
...
```

Applications Services Engine from **UNIGEN** vendor is detected with device name **sdf**.

Step 3 Run the following command to view the partitions in the disk.

lsblk -s or **lsblk**

- **Example1**

  The following example shows functioning TPM disk with two partitions sdf1 and sdf2. This can be installed with Cisco Nexus Dashboard software with no issues.

```
[root@dcnm-se-active sysadmin]$ lsblk
NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
...
sdc                     8:32   0   2.2T  0 disk
sdd                     8:48   0   2.2T  0 disk
sde                     8:64   0   371.6G  0 disk
sdf                     8:80   1   7.7G  0 disk  /*functioning TPM with partition*/
 |--sdf1                  8:81   1    60M  0 part
 |--sdf2                  8:82   1   3.7G  0 part
nvme0n1               259:0    0   1.5T  0 disk
 |--nvme0n1p1           259:1    0   1.5T  0 part
   |--flashvg-flashvol 253:3    0   1.5T  0 lvm  /var/afw/vols/data/flash
...
```

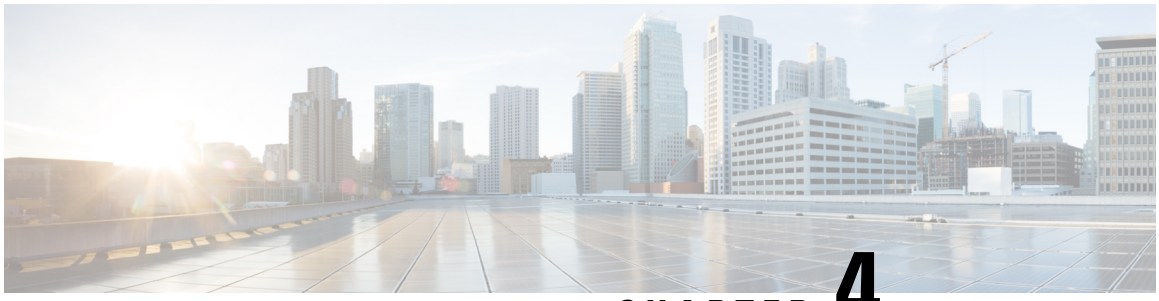
- **Example2**

  The following example shows defective or corrupted TPM disk with no partitions defined on device **sdf**. This unit cannot be used to install Cisco Nexus Dashboard software, and must be replaced.

```
[root@dcnm-se-active sysadmin]$ lsblk
NAME                  MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
...
sdc                     8:32   0   2.2T  0 disk
sdd                     8:48   0   2.2T  0 disk
sde                     8:64   0   371.6G  0 disk
sdf                     8:80   1   16G  0 disk  /*corrupted TPM without partition*/
nvme0n1               259:0    0   1.5T  0 disk
 |--nvme0n1p1           259:1    0   1.5T  0 part
   |--flashvg-flashvol 253:3    0   1.5T  0 lvm  /var/afw/vols/data/flash
...
```

Step 4 If your device has a TPM disk with no partitions, contact Cisco Technical Assistance Center (TAC) to initiate RMA and replace the device.

No further action is required if your TPM has partitions.



CHAPTER 4

New Features and Enhancements

New Features and Enhancements

Cisco Data Center Network Manager (DCNM) includes the new features, enhancements, and hardware support that are described in the following section:

New Features and Enhancements in Cisco DCNM, Release 11.4(1)

These following sections include information about the new features, enhancements, and hardware support introduced in the Cisco DCNM Release 11.4(1).

LAN Fabric Deployment Enhancements

The following features are new in Cisco DCNM Release 11.4(1) for the LAN Fabric Deployment.

Software Maintenance Update to use Network Insights for Resources (NIR) Application

To use NIR 2.2.2+ application with DCNM 11.4(1), you must install a maintenance update. Refer to Installing Software Maintenance Update in *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.4(1)* for instructions about how to install the maintenance update.

For more information about Network Insights for Resources, refer to the NIR 2.2.2 Release Notes.

Applications Services Engine

Beginning with Release 11.4(1), along with Computes, you can install Cisco DCNM in Standalone and Native HA mode on Cisco Applications Services Engine. For more information, see Application Services Engine Release Notes for Cisco DCNM.

Support for ASR1K and Cat9K

You can add Cisco IOS XE devices, like ASR1K and Cat9K, to your external fabric in Cisco DCNM. You can use them as edge and core routers. You can also create VRF-Lite external connectivity to them from the border devices that are part of VXLAN EVPN or Routed fabrics.

Enhanced Role-based Access Control

You can see the following role-based access control (RBAC) changes:

- Enhanced Read-only access to the Cisco DCNM Web UI and APIs for the **network-operator** user role
- A new user role called **network-stager**
- Freeze deployment for a particular fabric or all fabrics in DCNM as a user with the **network-admin** role

Note Actions that cannot be performed by a **network-stager** or a **network-operator** role will be grayed out on the DCNM Web UI and appropriately blocked on the corresponding REST APIs.

EPLD Support

Cisco DCNM supports EPLD upgrade for Cisco Nexus 9000 Series Switches and Cisco Nexus 3000 Series Switches. You can upload EPLD images like other images and upgrade them as well.

Multi-Site Domain (MSD) Backup and Restore

You can take a backup of MSD fabrics. When you initiate a backup from the MSD fabric, the backup and restore process is applicable for the member fabrics also.

Golden Backup

You can mark certain fabrics backups as golden in Cisco DCNM. Golden backups of fabrics cannot be deleted. Cisco DCNM archives up to 10 golden backups on a per fabric basis.

IPAM Integration Using Infoblox

You can use the IPAM Integrator application to view the dynamic and static IP allocation in an IPAM server such as Infoblox for the relevant overlay networks defined in DCNM. This application requires read-only access to the IPAM. Currently, this feature is supported for VXLAN EVPN fabrics including MSDs for overlay IPv4 networks for which DHCPv4 has been enabled. You can also choose to sync up records on-demand between the DCNM and Infoblox.

Preprovisioning an Ethernet Interfaces

You can preprovision Ethernet interfaces in the **Interface** window. This preprovisioning feature is supported in Easy, eBGP, and External fabrics. You can add the Ethernet interfaces to only preprovisioned devices before they are discovered in DCNM.

Support for CloudSec in Multi-Site Deployment

CloudSec feature allows secured data center interconnect in a VXLAN EVPN Multi-Site deployment by supporting source-to-destination packet encryption between border gateway devices in different fabrics. Cisco DCNM Release 11.4(1) provides an option to enable CloudSec in an MSD fabric.

The CloudSec feature is supported on Cisco Nexus 9000 Series FX2 platform starting with Cisco NX-OS Release 9.3(5) or later.

Migrating LAN Classic to LAN Fabric

From Cisco DCNM Release 11.4(1), the LAN Classic installation for DCNM is no longer supported. If you're planning to upgrade your LAN Classic deployment to DCNM Release 11.4(1), the only available upgrade option is to the DCNM Release 11.4(1) LAN Fabric deployment, and it's done automatically during the DCNM inline upgrade process.

In the LAN Fabric deployment, there are two fabric templates, namely, **LAN_Classic** and **Fabric_Group**, that you can use to manage your switches in a similar way as it was done in the DCNM Classic LAN, but with an enhanced feature-set.

BGP Peer Template Support

Until Cisco DCNM Release 11.3(1), in VXLAN EVPN Easy Fabric deployments, the same iBGP peer template for iBGP definition was used for the leafs, borders, and BGP RRs. From DCNM Release 11.4(1), the following fields can be used to specify different configurations:

- **iBGP Peer-Template Config** – Specifies the configuration used for BGP RRs on spines.
- **Leaf/Border/Border Gateway iBGP Peer-Template Config** – Specifies the config used for leaf, border, or border gateway. If this field is empty, the peer template defined in **iBGP Peer-Template Config** is used on all BGP enabled devices (RRs, leafs, border, or border gateways).

Viewing Policy Change History

In the DCNM Fabric Builder, you can click the **History** button to view per switch deployment and policy change history.

The newly introduced **Policy Change History** tab provides granular accounting on a per policy basis for each configurable entity in the fabric. This includes information of which users made what changes to what policies capturing all add, update, or delete operations including before and after configuration state comparison.

VMM Workload Automation

VMM workload automation is about the automation of network configuration in Cisco's Nexus switches for workloads spawned in a VMware environment. Note that this is a preview feature in the Cisco DCNM Release 11.4(1). This is an independent daemon that is not packaged with the DCNM. It needs to be downloaded and separately installed either on the DCNM or another Linux system if the pre-requisites are met. In a nutshell, the daemon listens to events from VMware vCenter and appropriate triggers overlay configuration on the corresponding switches below which the workloads are attached.

This feature allows the following functionalities:

- Discover the network objects in the VMware vCenter.
- Discover the connectivity between the servers (vswitches/DVSes) and the Nexus switches imported into DCNM.
- Use DCNM APIs to trigger creation and attachment of the appropriate overlay network configuration on the appropriate switches.

Configuration Compliance (CC) Side-by-side Comparison Enhancements

In prior DCNM 11.x releases, configurations such as boot string, rommon configuration, and other default configurations are ignored during strict CC checks. For such cases, the internal configuration compliance engine ensures that these config changes are not called out as diffs. These diffs are also not displayed in the

Pending Config window. But, the Side-by-side diff utility compares the diff in the two text files and does not leverage the internal logic used in the diff computation. As a result, the diff in default configurations is highlighted in red in the **Side-by-side Comparison** window. Starting from Cisco DCNM Release 11.4(1), such diffs are not highlighted in the **Side-by-side Comparison** window. The auto-generated default configuration that is highlighted in the **Running config** window is not visible in the **Expected config**window.

Programmable Reports

The Programmable Report application enables generation of rich contextual reports using Python scripts. The reports can collect information either directly from the devices or from the DCNM itself. Example reports include Resource tracking in fabrics, top-N top talkers based on VXLAN VNI counters in a fabric etc. Report jobs are run to generate reports. Each report job can generate multiple reports. You can schedule the report to be executed on a per device level or at a fabric level. These reports are then analyzed to obtain detailed information about the devices.

The REPORT template type is used to support the Programmable Reports feature. This template has two template subtypes- UPGRADE and GENERIC. A python SDK is provided to simplify report generation. This SDK is bundled with the DCNM and provides APIs to generate reports.

Layer 4-Layer 7 Services Support for Multi-Site Domain (MSD) Fabrics

The following enhancements are supported from Cisco DCNM Release 11.4(1):

- The service node can now be attached to a vPC border gateway or a vPC leaf or standalone leaf in a member fabric that is part of the MSD..
- RBAC support - the Layer 4-Layer 7 Service supports Role-Based Access Control (RBAC) along with fabric access mode.
- Service node backup and restore
- Fabric Backup and Restore
- Refreshing the Service Policy and Route Peering List
- Attaching a Service Policy or a Route Peering - To attach a specific service policy or route peering to a switch, select the check box next to the required service policy or route peering and click **Attach**.
- Detaching a Service Policy or a Route Peering - To detach a specific service policy or route peering from a switch, select the check box next to the required service policy or route peering and click **Detach**.
- Deployment history - To view deployment history of the switches and networks that are involved in the selected service policy or route peering, click **History** in the **Service Nodes** window.

Adding Authentication Parameters to Outbound Emails

Some SMTP servers may require addition of authentication parameters to emails that are sent from DCNM to the SMTP servers. Starting from Cisco DCNM Release 11.4(1), you can add authentication parameters to the emails that are sent by DCNM to any SMTP server that requires authentication.

Endpoint Locator Enhancements

The following enhancements are supported from Cisco DCNM Release 11.4(1):

- Click the **i** icon in the **Control > Endpoint Locator > Configure** window to view a template of the configuration that is pushed to the switches while enabling EPL. This configuration can be copied and pushed to RR/Spine devices to enable EPL on external fabrics.

- The name of the network is also displayed in the **Network** drop-down list in the **Monitor > Endpoint Locator > Explore** window. The Network name is obtained from the overlay networks defined in the Networks/VRFs listing.
- Search can be initiated by using the **VM Name** in the **Monitor > Endpoint Locator > Explore** window. The VM information retrieved from VMware vCenter is correlated with the endpoint information in the EPL database to provide a correlated view.
- To display a list of the most recent notifications, click the **Notifications** icon in the **Monitor > Endpoint Locator > Explore** window.
- An alarm is generated if there are any endpoint-related anomalies.

Endpoint Locator and Health Monitor Alarms

Starting from Cisco DCNM Release 11.4(1), alarms are registered and created under the **External** alarm category by the Endpoint Locator (EPL) and Health Monitor applications.

400G Tier Added to Physical Capacity Table

Starting from Cisco DCNM Release 11.4(1), the 400G tier has also been added to the **Physical Capacity** table under the **Capacity** tab. However, the **Physical Capacity** table under the **Capacity** tab will only show information about the physical ports that are present on the switch. For example, if the switch does not have a 400G physical port, the 400G tier is not displayed in the **Physical Capacity** table.

Discovery Support in DCNM Tracker

Typically, with DCNM 11.x, for all imported switches, by default, the discovery engine retrieves relevant inventory, interface, license, feature, module, connectivity etc. information, every 5 minutes. Starting from Cisco DCNM Release 11.4(1), the DCNM tracker has been enhanced to act as a pre-checker for the periodic discovery by comparing and checking the state or configuration outputs and updating the discovery engine if any state or configuration of interest to the discovery engine has changed on the switch. If nothing has changed on the switch, the tracker informs the discovery engine, which then optimizes and skips that periodic discovery cycle for the switch. So, the tracker acts as a discovery helper in this case. In large-scale deployments, the total discovery time is faster when the tracker is installed as unnecessarily polling of discovery-related information on the switch is not performed when there is no change in switch configuration. By default, this feature is turned on when the DCNM tracker is installed.

NX-API Certificate Management for Switches

Cisco NX-OS switches require an SSL certificate to function in NX-API HTTPS mode. SSL certificates are generated by users and signed by their Certificate Authority (CA). You can install the certificates manually using CLI commands on the switch console. From Release 11.4(1), Cisco DCNM provides an easy workflow to upload NX-API certificates to the DCNM, that in turn can be easily installed on the appropriate switches that are managed by DCNM.

Note This feature is supported on switches running on NXOS version 9.2(3) or higher.

Kubernetes Compute Visualization

From Release 11.4(1), Cisco DCNM allows you to import a Kubernetes (K8s) Container Orchestrator in the DCNM. Using standard K8s APIs, DCNM provides a correlated compute and network view of container workloads that are running on compute nodes that are attached to switches imported into the DCNM. The K8s clusters themselves may be running on either bare-metal servers or on virtual machines running in ESXi environments managed by VMware vCenter.

Media Controller Deployment Enhancements

The following features are new in Cisco DCNM Release 11.4(1) for Media Controller Deployment.

Generic Multicast Monitoring

In addition to IP Fabric Non-Blocking Multicast (NBM), IP Fabric Media mode now provides visibility into Generic Multicast traffic. The feature provides end to end flow path visibility, topology, and statistics.

You can use the Generic Multicast feature for monitoring purposes. This feature is applicable for switches with the Cisco NX-OS Release 9.3(5) and later.

Generic Multicast is available with the Media Controller deployment mode. After DCNM installation, you need to decide whether to run DCNM in IP Fabric for Media (IPFM) mode or Generic Multicast mode. You can enable the Generic Multicast mode by using the **pmn.generic-multicast.enabled** server property.

Flow Priority

You can now control priority of migrating flows in case of node or link failures by controlling flow priority through Flow Policy Management.

In the **Add Flow Policy** or **Edit Flow Policy** windows, from the **Flow Priority** drop-down list, you can choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.

Any Source Multicast (ASM) Enhancements

You can decide whether to stream sender traffic to spine or not. You can choose to conserve uplink bandwidth at the cost of slight increase in overall flow setup time.

You can check the **Reserve Bandwidth to Receiver Only** check box to push the ASM traffic to spine only if there is a receiver. This feature is applicable for switches with the Cisco NX-OS Release 9.3(5) and later.

You can use the **Deploy** button to deploy only unicast bandwidth configuration or reserve bandwidth configuration.

Real-time Fault and Threshold Notifications

Real-time fault and threshold crossing notifications are available via AMQP. You can create a dedicated queue to get the real-time events. An event is generated when an **interface used bandwidth** reaches to - 60%, 75%, or 90%. A clear event is generated when the usage falls below the 5% threshold.

Copying Switch Running Configuration to Start-up Configuration

Whenever there is any deployment to the switch via DCNM, the switch running configuration is automatically saved to the start-up configuration. In other words, DCNM invokes the **copy r s** command on a switch immediately after a deployment to make sure that the configuration is preserved between the switch reloads. An event with the category ‘CopyRS’ is logged in **Media Controller > Events** when the **copy r s** command is invoked as well as when it’s completed either successfully or with an error.

SAN Deployment Enhancements

The following features are new in Cisco DCNM Release 11.4(1) for SAN Deployment.

Viewing FICON Ports

You can view the Port WWN details by choosing **Settings > Columns** and choose the **Port WWN** option from the drop-down list.

You can print, export the data, or customize the columns you want to view.

Zone Migration Tool

You can migrate pWWN-based SAN zones from a Brocade switch to a Cisco MDS switch. This involves the following steps:

1. Generate the Brocade configuration files.
2. Convert the files using the zone migration tool to make them compatible with Cisco MDS switches.
3. Apply the generated zoning output to Cisco MDS switches.

This feature supports migration of Brocade's fabric switches running Brocade Fabric OS v7.x.x or later in this release.

Removal of LAN Items in Topology

In the DCNM Release 11.4(1) SAN deployment modes, the LAN items have been removed from the Topology window.

The following search options are available for the DEFAULT_LAN scope:

- Quick Search
- VLAN

The following search options are available for the DEFAULT_SAN scope:

- Quick Search
- VLAN
- VSAN ID/Name

Shutdown Interfaces

Click the **No Shutdown** or **Shutdown** toolbar button to enable or disable switch interfaces. After you click a button, a dialog box pops up asking for a confirmation. Click **Yes** to proceed or **No** to cancel the operation.

SAN Insights Enhancements

- The **SAN Insights Flows** dashlet displays donuts depicting flow summary for IT Pairs and ITL Flows when the SCSI protocol is selected from the protocol drop-down list. The **SAN Insights Flows** dashlet displays donuts depicting flow summary for IT Pairs and ITN Flows when the NVMe protocol is selected from the protocol drop-down list. You can display data for Read Completion Time or Write Completion Time by selecting the required option from the dropdown list.
- Top 10 Hosts and the Top 10 Storage charts on the Dashboard now display enclosures/WWPNs/Device Alias in the selected Protocol/Fabric/Switch scope.
- The Flow Summary and the Enclosure Summary donuts are refreshed every 15 minutes.
- From Release 11.4(1), Cisco DCNM allows user to view data for more than two weeks time frame (up to a default maximum of 90 days). You can choose the date using the date picker and view the historical data starting from the selected date at hourly granularity.
- From Release 11.4(1), you can filter ECT Analysis by **Device Alias**, also.
- Starting 11.4 release, the deviation of the ECT less than the baseline is considered as negative deviation. The Web UI screens are expected to display negative values for the computed deviation percentage.
- If ECT is below 10% from Baseline, the color Green implies normal range.

- In Release 11.4(1), the Custom Graphing metrics is enhanced to include the Write IO Failures, Read IO Failures, Write IO Aborts and Read IO Aborts to the drop-down metrics list.
- From Release 11.4(1), the San Insight Pipeline Collector and the SAN Insight Post Processing applications can only be paused and resumed from Cisco DCNM **Web UI > Applications > Catalog**.

Common Enhancements applicable for all DCNM Install types

Software Maintenance Update to address Log4j2 vulnerability

Cisco DCNM Release 11.4(1) provides Software Maintenance Update (SMU) 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, therefore it is not addressed here.

For more information, refer to ***Installing Software Maintenance Update for log4j2 Vulnerability*** chapter in Cisco DCNM Installation Guide for your deployment type.

Tetration Agent with DCNM Validation

You can install tetration agent on Cisco DCNM and compute nodes for OVA and ISO installations. After you install the agent, the server nodes will point to the titration cluster and start streaming data to it.

Server Status

From Cisco DCNM Release 11.4(1), you can see the status of the following services as well:

- NTPD server
- DHCP server
- SNMP traps
- Docker Registry
- Syslog Receiver

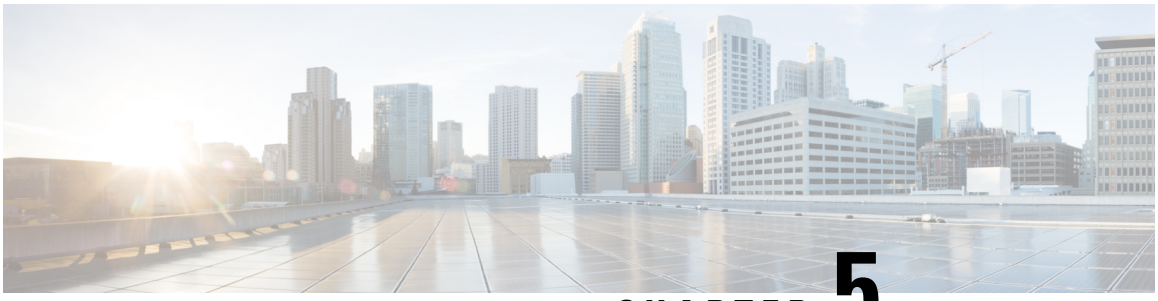
New Hardware Supported

The following new hardware is supported from Cisco DCNM Release 11.4(1).

- N9K FC/FCoE switch mode support
- N9K FC/FCOE NPV support for N9K-C93360YC-FX2
- N9K-C93180YC-FX3S
- N9K-C93108TC-FX3P

Videos: Cisco DCNM Release 11.4(1)

For videos created for features in Release 11.4(1), see Cisco Data Center Network Manager, Release 11.4(1).



CHAPTER 5

Upgrading Cisco DCNM

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

Upgrading Cisco DCNM

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM Release 11.3(1), you can install Cisco DCNM for SAN Deployment on both OVA and ISO virtual appliances.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.4(1).

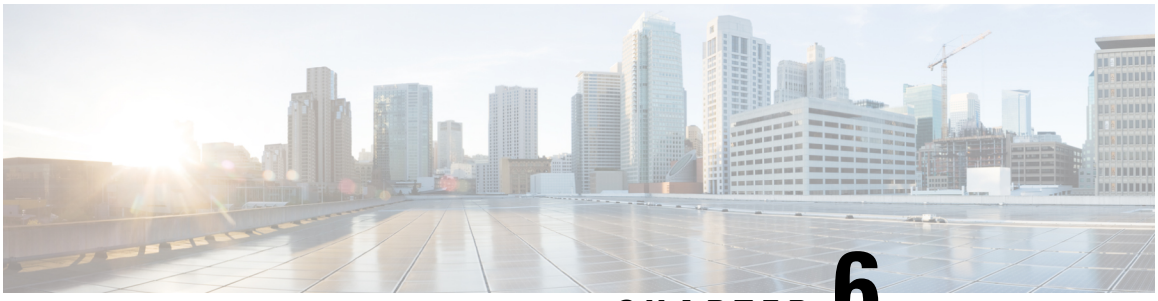
Table 6: Type of Upgrade for LAN Fabric, and IP for Media (IPFM) deployments

Current Release Number	Upgrade type to upgrade to Release 11.4(1)
11.3(1)	Inline Upgrade
11.2(1)	Inline Upgrade
11.1(1)	Inline Upgrade
11.0(1)	11.0(1) → 11.2(1) → 11.4(1) 11.0(1) → 11.1(1) → 11.4(1) → represents an Inline Upgrade

Table 7: Type of Upgrade for Cisco DCNM SAN deployments

Current Release Number	Upgrade type to upgrade to Release 11.4(1)
11.3(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO—Inline Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.4(1)
11.2(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— **1.** Fresh 11.3(1) SAN Only Installation. **2.** Migrate Performance Manager Collections to 11.3(1) **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1). **3.** Inline upgrade to 11.4(1)
11.1(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— **1.** Fresh 11.3(1) SAN Only Installation. **2.** Migrate Performance Manager Collections to 11.3(1). **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1). **3.** Inline upgrade to 11.4(1)
10.4(2) OVA 10.4(1) OVA	To 11.3(1) OVA\ISO— **1.** Fresh 11.3(1) SAN Only Installation. **2.** Migrate Performance Manager Collections to 11.3(1). **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1). **3.** Inline upgrade to 11.4(1)



CHAPTER 6

Supported Cisco Platforms and Software Versions

Compatibility Matrix for Cisco DCNM, Release 11.4(1)

Note Cisco DCNM Compatibility Matrix Tool provides an intuitive/interactive tool to find the NXOS version compatible with the DCNM release version.

The following sections provide information regarding the Compatibility of Cisco DCNM Release 11.4(1) with various switches, applications, and other devices.

Compatibility Matrix for Each Installation Type

Installation Type	Fabric Type	Supported Releases	Recommended Releases
LAN Fabric	Newly provisioned VXLAN fabrics N9000, N9000v	7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9), 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	7.0(3)I7(8), 9.3(4)
	Newly provisioned VXLAN fabrics N3600	9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	9.3(4)
	Migrating NFM-managed VXLAN fabric to DCNM	7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9)	7.0(3)I7(6)
	Brownfield deployment for N9000	7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9), 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	7.0(3)I7(8)
	Brownfield deployment for N3600	9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	9.3(4)
	External/LAN Classic Fabric N3000/3100/3500	7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9), 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	9.3(4)
	External/LAN Classic Fabric N3600	9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	9.3(4)
	External/LAN Classic Fabric N5000/5600/6000	7.3(7)N1(1b), 7.3(7)N1(1a), 7.3(7)N1(1), 7.3(6)N1(1), 7.3(5)N1(1)	7.3(7)N1(1b)
	External/LAN Classic Fabric N7000/7700	8.2(6), 8.4(2), 8.4(1), 8.3(2), 8.2(5), 8.2(4), 7.3(6)D1(1),7.3(5)D1(1)	7.3(5)D1(1), 8.2(5)
	External/LAN Classic Fabric N9000, N9000v	7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9), 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5)	7.0(3)I7(8), 9.3(4)
	External Fabric for Non-Nexus Devices	Compatibility Matrix for Supported Non-Nexus Devices and Versions, on page 31	
IP for Media (IPFM)	—	9.3(6), 9.3(5), 9.3(4), 9.3(3), 9.3(2), 9.3(1)	
SAN	—	Compatibility Matrix for Cisco DCNM SAN Deployment, on page 29	

Compatibility Matrix for Cisco DCNM SAN Deployment

Switches	Supported Switch Releases
Cisco MDS 9100	8.4(2a), 8.4(2), 8.4.(1a), 6.2(29), 8.4(1), 6.2(27), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1a), 7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1), 6.2(25), 6.2(23), 6.2.(21), 6.2(19), 6.2(17), 6.2(15), 6.2(13b), 6.2(13a), 6.2(13), 6.2(11c), 6.2(11b), 6.2(11), 6.2(9c), 6.2(9b), 6.2(9a), 6.2(9), 6.2(7), 6.2(5a), 6.2(5), 6.2(3), 6.2(1), 5.2(8i), 5.2(8h), 5.2(8c), 5.2(8d), 5.2(8e), 5.2(8f), 5.2(8g)
Cisco MDS 9200	7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1), 6.2(25), 6.2(23), 6.2.(21), 6.2(19), 6.2(17), 6.2(15), 6.2(13b), 6.2(13a), 6.2(13), 6.2(11c), 6.2(11b), 6.2(11), 6.2(9c), 6.2(9b), 6.2(9a), 6.2(9), 6.2(7), 6.2(5a), 6.2(5), 6.2(3), 6.2(1), 5.2(8h), 5.2(8c), 5.2(8d), 5.2(8e), 5.2(8f), 5, 2(8g)
Cisco MDS 9250i	8.4(2a), 8.4(2), 8.4.(1a), 6.2(29), 8.4(1), 6.2(27), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1a), 7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1), 6.2(25), 6.2(23), 6.2.(21), 6.2(19), 6.2(17), 6.2(15), 6.2(13b), 6.2(13a), 6.2(13), 6.2(11c), 6.2(11b), 6.2(11), 6.2(9c), 6.2(9b), 6.2(9a), 6.2(9), 6.2(7), 6.2(5a), 6.2(5)
Cisco MDS 9300	8.4(2a), 8.4(2), 8.4(1a), 6.2(29), 8.4(1), 6.2(27), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1a), 8.1(1), 7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1), 6.2(25), 6.2(23), 6.2.(21), 6.2(19), 6.2(17), 6.2(15), 6.2(13b), 6.2(13a), 6.2(13)
Cisco MDS 9500	7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1), 6.2(25), 6.2(23), 6.2.(21), 6.2(19), 6.2(17), 6.2(15), 6.2(13b), 6.2(13a), 6.2(13), 6.2(11c), 6.2(11b), 6.2(11), 6.2(9c), 6.2(9b), 6.2(9a), 6.2(9), 6.2(7), 6.2(5a), 6.2(5), 6.2(3), 6.2(1), 5.2(8h), 5.2(8c), 5.2(8d), 5.2(8e), 5.2(8f), 5, 2(8g)
Cisco MDS 9700	8.4(2a), 8.4(2), 8.4(1a), 6.2(29), 8.4(1), 6.2(27), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1a), 8.1(1), 7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1), 6.2(25), 6.2(23), 6.2.(21), 6.2(19), 6.2(17), 6.2(15), 6.2(13b), 6.2(13a), 6.2(13), 6.2(11c), 6.2(11b), 6.2(11), 6.2(9c), 6.2(9b), 6.2(9a), 6.2(9), 6.2(7), 6.2(5a), 6.2(5), 6.2(3), 6.2(1)
Cisco Nexus 9000 Series	9.3(5), 9.3(4), 7.0(3)I7(8), 9.3(3), 7.0(3)I7(7), 9.3(2), 9.2(4), 9.3(1), 9.2(3), 7.0(3)I4(9), 7.0(3)I7(6), 9.2(2), 9.2(1), 7.0(3)I7(5), 7.0(3)I7(4), 7.0(3)I7(3), 7.0(3)I7(2), 7.0(3)I7(1), 7.0(3)I4(8), 7.0(3)I4(7), 7.0(3)I4(6), 7.0(3)I4(5), 7.0(3)I4(4), 7.0(3)I4(3), 7.0(3)I4(2), 7.0(3)I4(1), 7.0(3)F3(2), 7.0(3)F3(1), 7.0(3)F1(2), 7.0(3)I6(2), 7.0(3)I6(1), 7.0(3)F2(1), 7.0(3)F1(1), 7.0(3)I2(4), 7.0(3)I2(5), 7.0(3)I5(2), 7.0(3)I5(1), 7.0(3)I3(2), 7.0(3)I3(1), 7.0(3)I2.3, 7.0.3.I2.2c, 7.0(3)l2.2a, 7.0(3)l2.1, 7.0(3)l1.3, 7.0(3)I1.2, 6.2(9), 6.1(2)I3.4, 6.1(2)I3.2, 6.1(2)I3(1), 6.1(2)I2(1), 6.1(2)I1(2), 6.1(2)I1(1)

Switches	Supported Switch Releases
Cisco Nexus 7000 Series	8.2(6), 8.4(2), 7.3(6)D1(1), 6.2(24a), 6.2(24), 8.2(5), 7.3(5)D1(1), 8.4(1), 8.2(4), 7.3(4)D1(1), 6.2(22), 8.3(2), 8.3(1), 8.2(3), 8.2(2), 8.2(1), 8.1(2), 8.1(1), 8.0(1), 7.3(3) D1(1), 7.3(2)D1(3), 7.3(2)D1(2), 7.3(2)D1(1), 7.3(1)D1(1), 7.3(0)DX(1), 7.3(0)D1(1), 7.2(2)D1(4), 7.2(2)D1(2), 7.2(2)D1(1), 7.2(1)D1(1), 7.2(0)D1(2), 7.2(0)D1(1) , 6.2(20), 6.2(18), 6.2(16), 6.2(14), 6.2(10), 6.2(8), 6.2(6a), 6.2(6), 6.2(2a), 6.2(2)
Cisco Nexus 7700 Series	8.2(6), 8.4(2), 7.3(6)D1(1), 6.2(24a), 6.2(24), 6.2(24), 8.2(5), 7.3(5)D1(1), 8.4(1), 8.2(4), 7.3(4)D1(1), 6.2(22), 8.3(2), 8.3(1), 8.2(3), 8.2(2), 8.2(1), 8.1(2), 8.1(1), 8.0(1), 7.3(3) D1(1), 7.3(2)D1(3), 7.3(2)D1(2), 7.3(2)D1(1), 7.3(1)D1(1), 7.3(0)DX(1), 7.3(0)D1(1), 7.2(2)D1(4), 7.2(2)D1(2), 7.2(2)D1(1), 7.2(1)D1(1), 7.2(0)D1(2), 7.2(0)D1(1) , 6.2(20), 6.2(18), 6.2(16), 6.2(14), 6.2(10), 6.2(8), 6.2(6a), 6.2(6), 6.2(2a), 6.2.2
Cisco Nexus 6000/5600 Series	7.3(7)N1(1b), 7.3(7)N1(1a), 7.3(7)N1(1), 7.3(6)N1(1), 7.3(5)N1(1), 7.1(5)N1(1b), 7.3(4)N1(1), 7.3(3)N1(1), 7.3(2)N1(1e), 7.3(2)N1(1), 7.3(1)N1(1), 7.3(0)N1(1), 7.2(1)N1(1), 7.1(5)N1(1), 7.2(0)N1(1), 7.1(5)N1(1), 7.1(4)N1(1), 7.1(3)N1(2), 7.1(3)N1(1), 7.1(2)N1(1), 7.1(1)N1(1), 7.1(0)N1(1), 7.0(8)N1(1), 7.0(7)N1(1), 7.0(6)N1(1), 7.0(5)N1(1), 7.0(4)N1(1), 7.0(3)N1(1), 7.0(2)N1(1), 7.0(1)N1(1), 6.0(2)N2(7), 6.0(2)N2(2), 6.0(2)N2(1), 6.0(2)N1(2)
Cisco Nexus 5000 Series	7.3(7)N1(1b), 7.3(7)N1(1a), 7.3(7)N1(1), 7.3(6)N1(1), 7.3(5)N1(1), 7.1(5)N1(1b), 7.3(4)N1(1), 7.3(3)N1(1), 7.3(2)N1(1e), 7.3(2)N1(1), 7.3(1)N1(1), 7.3(0)N1(1), 7.2(1)N1(1), 7.2(0)N1(1), 7.1(5)N1(1), 7.1(4)N1(1), 7.1(3)N1(2), 7.1(3)N1(1), 7.1(2)N1(1), 7.1(1)N1(1), 7.1(0)N1(1), 7.0(8)N1(1), 7.0(7)N1(1), 7.0(6)N1(1), 7.0(5)N1(1), 7.0(4)N1(1), 7.0(3)N1(1), 7.0(2)N1(1), 7.0(1)N1(1), 6.0(2)N2(7), 6.0(2), 5.2(1)N1(9a), 5.2(1)N1(9), 5.2(1), 5.1(3), 5.0(3), 5.0(2), 4.2(1), 4.1(3)
UCS Infrastructure and UCS Manager Software	4.0.4g, 4.1.1a, 3.2.3n, 4.0.4, 4.0.1, 3.2(3k), 2.2.5a

Note The Cisco NX-OS version of the Cisco Nexus 2000 Series Fabric Extenders will be same as the NX-OS version of the supported Nexus switch (that is, Cisco Nexus 5000, Cisco Nexus 7000 or Cisco Nexus 9000).

Compatibility Matrix for Cisco DCNM and Applications

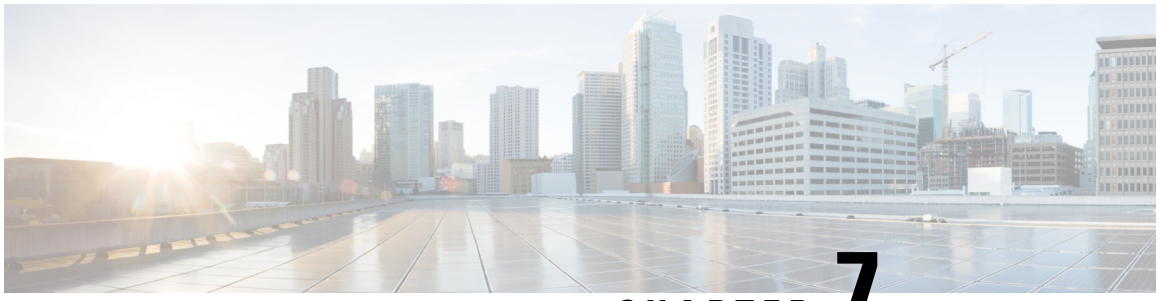
Applications	Supported Versions
Day2 Applications	Refer to Cisco Data Center Networking Applications Compatibility Matrix.

Applications	Supported Versions
ServiceNow Integration	• 1.0 • 1.1 Refer to the deployment-specific Cisco DCNM Configuration guide.

Compatibility Matrix for Supported Non-Nexus Devices and Versions

Note The following table is applicable to External Fabrics in Cisco DCNM LAN Fabric Deployment.

Non-Nexus Devices	Supported Versions
Cisco ASR 1001-X	IOS XE 16.06.04
Cisco ASR 1002-HX	IOS XE 16.06.04
Cisco ASR-9006	IOS XR 6.2(1)
Cisco Catalyst 9300-24T	IOS XE 17.01.01
Cisco Catalyst 9300-48U	IOS XE 17.01.01
Cisco CSR 1000v	IOS XE 16.10
Cisco NCS 5500	IOS XR 6.5(3)
Arista DCS-7280SR2A	EOS 4.24.0F
Arista DCS-7504N	EOS 4.24.0F



CHAPTER 7

Supported Hardware

This chapter contains information about the products and components supported in Cisco DCNM.

Hardware Supported in Cisco DCNM, Release 11.4(1)

In a LAN Fabric installation of Cisco DCNM 11.4(1), the Cisco Nexus 9000, and Nexus 3000 switches are supported for VXLAN EVPN fabric provisioning in Easy Fabrics.

Note In External fabrics in the DCNM LAN Fabric installation and in the DCNM LAN Classic installation, all Nexus switches are supported.

The following tables list the products and components that are supported in the Cisco DCNM, Release 11.4(1).

UCS Fabric Interconnect Integration

Product/Component	Part Number
Cisco UCS Unified Computing System 6454 1RU In-Chassis FI with 36x10G/25G + 4x 1G/10G/25G + 6x40G/100G + 8 UP Ports	UCS-FI-6454-U
Cisco UCS Unified Computing System 6332 1RU In-Chassis FI with 16UP + 24x40G Fixed Ports	UCS-FI-6332-16UP
Cisco UCS Unified Computing System 6332 1RU In-Chassis FI with 32x40G Fixed Ports	UCS-FI-6332
Cisco UCS Unified Computing System 6324 In-Chassis FI with 4UP, 1x40G Exp Port	UCS-FI-M-6324
Cisco UCS Unified Computing System 6296UP 96-Unified Port Fabric Interconnect	UCS-FI-6296UP
Cisco UCS Unified Computing System 6248UP 48-Unified Port Fabric Interconnect	UCS-FI-6248UP

Cisco MDS 9000 Family

Product/Component	Part Number
Cisco MDS 9718 Supervisor-1E Modules	DS-X97-SF1-K9
Cisco MDS 9710 Crossbar Fabric-3 Switching Module	DS-X9710-FAB3
Cisco MDS 9700 Series Supervisor-4 Module	DS-X97-SF4-K9
MDS 9706 Crossbar Switching Fabric-3 Module	DS-X9706-FAB3
Cisco MDS 9396T 32 Gbps 96-Port Fibre Channel Switch	DS-C9396T-K9
Cisco MDS 9148T 32 Gbps 48-Port Fibre Channel Switch	DS-C9148T-K9
Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module	DS-X9648-1536K9
Cisco MDS 9250i Multilayer Fabric Switch	DS-9250I-K9
Cisco MDS 9124 24-Port Multilayer Fabric Switch	DS-C9124-K9
Cisco MDS 9134 34-Port Multilayer Fabric Switch	DS-C9134-K9
Cisco MDS 9148 48-Port Multilayer Fabric Switch	DS-C9148-K9
Cisco MDS 9148 48-Port Multilayer Fabric Switch	DS-C9148S-K9
Cisco MDS 9216i Multilayer Fabric Switch	DS-C9216i-K9
Cisco MDS 9222i Multilayer Fabric Switch	DS-C9222i-K9
Cisco MDS 9506 Multilayer Director	DS-C9506
Cisco MDS 9509 Multilayer Director	DS-C9509
Cisco MDS 9513 Multilayer Director	DS-C9513
Cisco MDS 9706 Multilayer Director	DS-C9706
Cisco MDS 9710 Multilayer Director	DS-C9710
Cisco MDS 9718 Multilayer Director	DS-C9718
Cisco MDS 9000 32-Port 2-Gbps Fibre Channel Switching Module	DS-X9032
Cisco MDS 9000 32-Port Storage Services Module	DS-X9032-SSM
Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module	DS-X9112
Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module	DS-X9112
Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module	DS-X9112

Product/Component	Part Number
Cisco MDS 9000 24-port 4-Gbps Fibre Channel Switching Module	DS-X9124
Cisco MDS 9000 48-port 4-Gbps Fibre Channel Switching Module	DS-X9148
Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module	DS-X9224-96K9
Cisco MDS 9000 32-port 8-Gbps Advanced Fibre Channel Switching Module	DS-X9232-256K9
Cisco MDS 9000 48-port 8-Gbps Advanced Fibre Channel Switching Module	DS-X9248-256K9
Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module	DS-X9248-48K9
Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module	DS-X9248-96K9
Cisco MDS 9000 Family 14-Port Fibre Channel and 2-port Gigabit Ethernet Module	DS-X9302-14K9
Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)	DS-X9304-18K9
Cisco MDS 9000 4-port 1-Gbps IP Storage Module	DS-X9304-SMIP
Cisco MDS 9000 8-port 1-Gbps IP Storage Module	DS-X9308-SMIP
Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16)	DS-X9316-SSNK9
Cisco MDS 9000 Family 24/10 SAN Extension Module	DS-X9334-K9
Cisco MDS 9000 48-port 16-Gbps Fibre Channel Switching Module with SFP LC connectors	DS-X9448-768K9
Cisco MDS 9500 Series Supervisor-1 Module	DS-X9530-SF1-K9
Cisco MDS 9500 Series Supervisor-2 Module	DS-X9530-SF2-K9
Cisco MDS 9500 Series Supervisor-2A Module	DS-X9530-SF2A-K9
Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module	DS-X9704
Cisco MDS 9000 8-port 10-Gbps Fibre Channel over Ethernet (FCoE) Module	DS-X9708-K9
Cisco MDS 48-Port 10-Gigabit Fibre Channel over Ethernet (FCoE) Module with SFP LC connectors	DS-X9848-480K9
Cisco MDS 9132T 32-Gbps 32-Port Fibre Channel Switch	DS-C9132T-K9

Cisco Nexus 9000 Series Switches

Product/Component	Part Number
Cisco Nexus 9000 Series Switches	
32P 40/100G QSFP28, 2P 1/10G SFP	N9K-C9332C
1RU 48x1/10GT + 6x40G/100G Ethernet Ports	N9K-C93180TC-FX
Cisco Nexus 7700 F4 40G Line card	Cisco Nexus 7700 F4 40G Line card
Cisco Nexus 9336C-FX2, 1RU, fixed-port switch	N9K-C9336C-FX2
Cisco Nexus 9000 Fixed with 48p 1/10G/25G SFP and 12p 40G/100G QSFP28	N9K-C93240YC-FX2
32-port 100Gigabit EthernetQuad Small Form-Factor Pluggable 28 (QSFP28) line card	N9K-X9732C-FX
48-port 1 and 10GBASE-T plus 4-port 40/100Gigabit Ethernet QSFP 28 line card	N9K-X9788TC-FX
48-port 1 and 10GBASE-T plus 4-port 40/100Gigabit Ethernet QSFP 28 line card (BMA)	N9K-X9788TC2-FX
FabricModule for Nexus 9516 chassis 100G support (100G/flow), NX-OS and ACI Spine	N9K-C9516-FM-E2
FabricModule for Nexus 9504 R-Series LC, NX-OS only	N9K-C9504-FM-R
Fretta 48p 1/10/25G + 4p 100G Line card	N9K-X96160YC-R
100-Gigabit N9K-C9508-FM-E2 Fabric Module	N9K-C9508-FM-E2
48P 1/10/25G + 6x100G QSFP28 1RU	N3K-C36180YC-R
36 40/100G Ethernet module for Nexus 9500 Series	N9K-X9736C-FX
64x100G QSFP28 + 2x10GSFP 1RU	N9K-C9364C
36x100G Ethernet module for Nexus 9000 Series	N9K-X9636C-RX
1RU TOR, fixed module 48 100/1000Mbps + 4 25G SFP28 + 2 100G QSFP28	N9K-C9348GC-FXP
1RU TOR, fixed module 48 100/1000Mbps + 4 25G SFP28 + 2 100G QSFP28 (BMA)	N9K-C9348GC2-FXP
1RU TOR, fixed module 48 10/25G SFP28 + 6 40/100G QSFP28	N9K-C93180YC-FX

Product/Component	Part Number
1RU TOR, fixed module 48 10/25G SFP28 + 6 40/100G QSFP28 (BMA)	N9K-C93180YC2-FX
1RU TOR, fixed module for Nexus 9300 Series 6 40G/100G QSFP28 + 48 10G BASE-T	N9K-C93108TC-FX
1RU TOR, fixed module for Nexus 9300 Series 6 40G/100G QSFP28 + 48 10G BASE-T (BMA)	N9K-C93108TC2-FX
Broadwell CPU-based Supervisor module for Nexus 9400 Series	N9K-SUPA-PLUS
Broadwell CPU-based Supervisor module for Nexus 9400 Series	N9K-SUPB-PLUS
Nexus 9K Fixed with 48p 10G BASE-T and 6p 40G/100G QSFP28	N9K-C93108TC-EX
N9K-C92300YC-Fixed Module	N9K-C92300YC
48-port 1/10/25 Gigabit Ethernet SFP+ and 4-port 40/100 Gigabit Ethernet QSFP Line Card	N9K-X97160YC-EX
Nexus N9K-C9232C Series fixed module with 32x40G/100G	N9K-C9232C
Nexus 9K Fixed with 48p 1/10G/25G SFP+ and 6p 40G/100G QSFP28	N9K-C93180YC-EX
Cisco Nexus 9000 Series 40GE Modules	
N9K 32p 40G Ethernet Module	N9K-X9432PQ
36p 40G Ethernet Module	N9K-X9636PQ
Cisco Nexus 9000 Series 10GE Fiber and Copper Modules	
8-port 100-Gigabit CFP2 I/O module	N9K-X9408PC-CFP2
100 Gigabit Ethernet uplink ports	N9K-M4PC-CFP2
Cisco Nexus 9500 Line Card support	N9K-X9564PX
N9K 48x1/10G-T 4x40G Ethernet Module	N9K-X9464PX
Cisco Nexus 9500 Line Card support	N9K-X9564TX
N9K 48x1/10G SFP+ 4x40G Ethernet Module	N9K-X9464TX
Cisco Nexus 9000 Series GEM Module	
N9K 40G Ethernet Expansion Module	N9K-M12PQ
N9K 40G Ethernet Expansion Module	N9K-M6PQ

Product/Component	Part Number
Cisco Nexus 9200 Switches	
Nexus 92160YC-X with High performance 1RU box, 48 1/10/25-Gb host ports	N9K-C92160YC-X
Nexus 9272Q with High-performance, 72-port/40-Gb fixed switching 2RU box, 5.76 Tbps of bandwidth	N9K-C9272Q
Nexus 9200 with 56p 40G QSFP+ and 8p 100G QSFP28	N9K-C92304QC
Nexus 9200 with 36p 40G 100G QSFP28	N9K-C9236C
Nexus 9200 with 48p 1/10G/25G SFP+ and 6p 40G QSFP or 4p 100G QSFP28	N9K-C92160YC-X
Nexus 9200 with 72p 40G QSFP+	N9K-C9272Q
Cisco Nexus 9300 Fixed Switches	
Nexus 9300 with 48p 10G BASE-T and 6p 40G/100G QSFP28, MACsec capable	N9K-C93108TC-FX3P
Nexus 9300 with 48p 1/10G/25G SFP and 6p 40G/100G QSFP28, MACsec, and Unified Ports capable	N9K-C93180YC-FX3S
Nexus 9K Fixed with 96p 1/10G/25G SFP and 12p 40G/100G QSFP28	N9K-C93360YC-FX2
96p 100M/1/10GBASE-T and 12p 40G/100G QSFP28	N9K-C93216TC-FX2
Nexus 9200 with 48p 100M/1G Base-T ports and 4p 1/10/25G SPF28 and 2p 40/100G QSFP28	N9K-C92348GC-X
Nexus 9316D Spine and Leaf switch with 28p 100/40G QSFP28 and 8p 400/100G QSFP-DD	N9K-C93600CD-GX
Cisco Nexus 9364C ACI Spine Switch with 64p 40/100G QSFP28, 2p 1/10G SFP	N9K-C9364C-GX
Nexus 9316D Spine switch with 16p 400/100G QSFP-DD	N9K-C9316D-GX
Nexus 9300 with 24p 40/50G QSFP+ and 6p 40G/100G QSFP28	N9K-C93180LC-EX
9372-PXE - 48 1/10-Gbps (SFP+) ports and 6 Quad SFP+ (QSFP+) uplink port, 1RU box	N9K-C9372PX-E
Cisco Nexus 9396PX Switch	N9K-C9396PX
Cisco Nexus 9396TX Switch	N9K-C9396TX
Cisco Nexus 9372PX Switch	N9K-C9372TX
Cisco Nexus 9372PX Switch	N9K-C9372TX

Product/Component	Part Number
Cisco Nexus 9372TX Switch	N9K-C9372TX
Cisco Nexus 9372TX Switch	N9K-C9372PX
Cisco Nexus 9332PQ Switch	N9K-C9332PQ
Cisco Nexus 93128TX Switch	N9K-C93128TX
Nexus 9300 with 48p 1/10G-T and 6p 40G QSFP+	N9K-C9372TX-E
Cisco Nexus 9500 Modular Chassis	
New fabric module for the Cisco Nexus 9516 Switch chassis	N9K-C9516-FM-E
40/100G Ethernet Module for Nexus 9500 Series chassis	N9K-X9736C-EX
Cisco Nexus 9504 Switch	N9K-C9504
Cisco Nexus 9508 Switch	N9K-C9508
Cisco Nexus 9516 Switch	N9K-C9516
Nexus 9500 linecard, 32p 100G QSFP aggregation linecard	N9K-X9732C-EX
Nexus 9500 linecard, 32p 100G QSFP28 aggregation linecard (Linerate >250 Bytes)	N9K-X9432C-S
Cisco Nexus 9500 Fabric Modules	
Fabric Module for Nexus 9504 with 100G support, NX-OS, and ACI spine	N9K-C9504-FM-E
Fabric Module for Nexus 9504 with 100G support, NX-OS only	N9K-C9504-FM-S
Fabric Module for Nexus 9508 chassis 100G support, NX-OS, and ACI spine	N9K-C9508-FM-E
Fabric Module for Nexus 9508 chassis 100G support, NX-OS only	N9K-C9508-FM-S

Cisco Nexus 7000 Series Switches

Product/Component	Part Number
Supported Chassis	
CiscoNexus7702 chassis	N77-C7702
Cisco Nexus 7004 chassis	N7K-C7004
Cisco Nexus 7706 chassis	N77-C7706-FAB2
Cisco Nexus 7009 chassis	N7K-C7009

Product/Component	Part Number
Cisco Nexus 7010 chassis	N7K-C7010
Cisco Nexus 7018 chassis	N7K-C7018
Cisco Nexus 7710 chassis	N7K-C7710
Cisco Nexus 7718 chassis	N7K-C7718
Fabric module, Cisco Nexus 7009 chassis	N7K-C7009-FAB-2
Fabric module, Cisco Nexus 7010 chassis	N7K-C7010-FAB-1
Fabric module, Cisco Nexus 7010 chassis	N7K-C7010-FAB-2
Fabric module, Cisco Nexus 7018 chassis	N7K-C7018-FAB-1
Fabric module, Cisco Nexus 7018 chassis	N7K-C7018-FAB-2
Fabric module, Cisco Nexus 7710 chassis	N77-C7710-FAB-1
Fabric module, Cisco Nexus 7710 chassis	N77-C7710-FAB-2
Fabric module, Cisco Nexus 7718 chassis	N77-C7718-FAB-2
Supported Supervisor	
Cisco Nexus 7000 Supervisor 1 Module	N7K-SUP1
Cisco Nexus 7000 Supervisor 2 Module	N7K-SUP2
Cisco Nexus 7000 Supervisor 2 Enhanced Module	N7K-SUP2E
Cisco Nexus 7700 Supervisor 2 Enhanced Module	N77-SUP2E
Cisco Nexus 7700 Supervisor 3	N77-SUP3E
Supported F Line Cards	
Cisco Nexus 7700 Fabric module 3	N77-C7706-FAB-3, N77-C7710-FAB-3
LC, N77, FANGIO CB100, 30PT, 40GE, zQFSP+	N77-F430CQ-36
32-port 1/10 Gigabit Ethernet SFP+ I/O Module	N7K-F132XP-15
48-port 1/10 Gigabit Ethernet SFP+ I/O Module (F2 Series)	N7K-F248XP-25
48-port 1/10 Gigabit Ethernet SFP+ I/O Module (Enhanced F2 Series)	N7K-F248XP-25E
48-port 1/10 GBase-T RJ45 Module (Enhanced F2-Series)	N7K-F248XT-25E
Cisco Nexus 7700 Enhanced 48-port 1/10 Gigabit Ethernet SFP+ I/O Module (F2 Series)	N77-F248XP-23E
Cisco Nexus 7000 1 F3 100G	N7K-F306CK-25
Cisco Nexus 7000 F3-Series 6-Port 100G Ethernet Module	N7K-F306CK-25

Product/Component	Part Number
Cisco Nexus 7000 F3-Series 12-Port 40G Ethernet Module	N7K-F312FQ-25
Cisco Nexus 7700 F3-Series 24-Port 40G Ethernet Module	N77-F324FQ-25
Cisco Nexus 7700 F3-Series 48-Port Fiber 1 and 10G Ethernet Module	N77-F348XP-23
Nexus 7000 F3-Series 48-Port Fiber 1 and 10G Ethernet Module	N7K-F348XP-25
Supported M Line Cards	
8-port 10-Gigabit Ethernet Module with XL Option (requires X2)	N7K-M108X2-12L
32-port 10-Gigabit Ethernet SFP+ I/O Module	N7K-M132XP-12
32-port 10-Gigabit Ethernet SFP+ I/O Module with XL Option	N7K-M132XP-12L
48-port 10/100/1000 Ethernet I/O Module	N7K-M148GT-11
48-port 1-Gigabit Ethernet SFP I/O Module	N7K-M148GS-11
48-port 1-Gigabit Ethernet Module with XL Option	N7K-M148GS-11L
2-port 100 Gigabit Ethernet I/O Module with XL Option	N7K-M202CF-22L
6-port 40 Gigabit Ethernet I/O Module with XL Option	N7K-M206FQ-23L
24-port 10 Gigabit Ethernet I/O Module with XL Option	N7K-M224XP-23L
Network Analysis Module NAM-NX1	N7K-SM-NAM-K9

Cisco Nexus 6000 Series Switches

Product/Component	Part Number
N6004X/5696 chassis **Note** This has been rebranded as Cisco Nexus 5000 Series Switches Chassis	N5K-C5696Q
Cisco Nexus 6001-64T Switch	N6K-C6001-64T
Cisco Nexus 6001-64P Switch	N6K-C6001-64P
Cisco Nexus 6004 EF Switch	N6K-C6004
Cisco Nexus 6004 module 12Q 40-Gigabit Ethernet Linecard Expansion Module/FCoE, spare	N6004X-M12Q
Cisco Nexus 6004 M20UP LEM	N6004X-M20UP

Product/Component	Part Number
Cisco Nexus 6004P-96Q Switch	N6K-6004-96Q

Cisco Nexus 5000 Series Switches

Product/Component	Part Number
Cisco Nexus 5648Q Switch is a 2RU switch, 24 fixed 40-Gbps QSFP+ ports, and 24 additional 40-Gbps QSFP+ ports	N5K-C5648Q
Cisco Nexus 5624Q Switch 1RU, -12 fixed 40-Gbps QSFP+ ports and 12 X 40-Gbps QSFP+ ports expansion module	N5K-C5624Q
20 port UP LEM	N5696-M20UP
12 port 40G LEM	N5696-M12Q
4 port 100G LEM	N5696-M4C
N5000 1000 Series Module 6-port 10GE	N5K-M1600(=)
N5000 1000 Series Module 4x10GE 4xFC 4/2/1G	N5K-M1404=
N5000 1000 Series Module 8-port 4/2/1G	N5K-M1008=
N5000 1000 Series Module 6-port 8/4/2G	N5K-M1060=
Cisco Nexus 56128P Switch	N5K-C56128P
Cisco Nexus 5010 chassis	N5K-C5010P-BF
Cisco Nexus 5020 chassis	N5K-C5020P-BF N5K-C5020P-BF-XL
Cisco Nexus 5548P Switch	N5K-C5548P-FA
Cisco Nexus 5548UP Switch	N5K-C5548UP-FA
Cisco Nexus 5672UP Switch	N5K-C5672UP
Cisco Nexus 5596T Switch	N5K-C5596T-FA
Cisco Nexus 5596UP Switch	N5K-C5596UP-FA
Cisco Nexus 0296-UPT chassis and GEM N55-M12T support	N5K-C5596T-FA-SUP
16-port Universal GEM, Cisco Nexus 5500	N5K-M16UP
Version 2, Layer 3 daughter card	N55-D160L3-V2

Cisco Nexus 4000 Series Switches

Product/Component	Part Number
Cisco Nexus 4001I Switch Module	N4K-4001I-XPX

Product/Component	Part Number
Cisco Nexus 4005I Switch Module	N4K-4005I-XPX

Cisco Nexus 3000 Series Switches

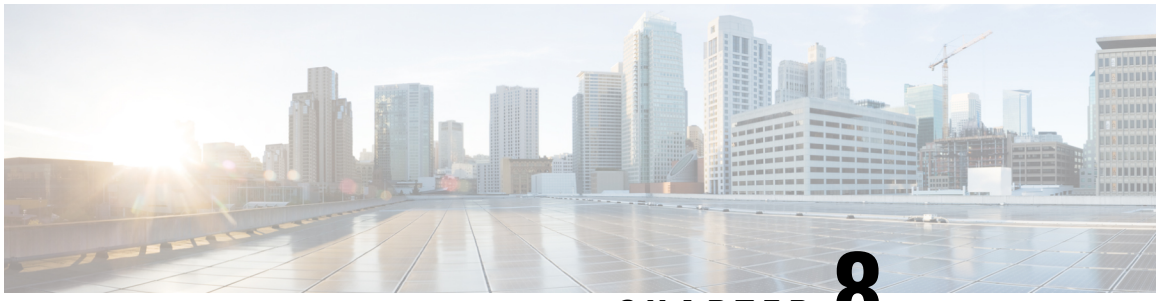
Product/Component	Part Number
Quad Small Form-Factor Pluggable – Double Density (QSFP-DD) switch with 32 ports	N3K-C3432D-S
Nexus 3408-S switch with 32 ports of QSFP-DD	N3K-C3408-S
Cisco Nexus 34200YC-SM Switch with top-of-rack, Layer 2 and 3 switching	N3K-C34200YC-SM
1RU 48 x SFP+/SFP28 and 6 x QSFP+/QSFP28	N3K-C34180YC
1RU 32 Port QSFP28 10/25/40/50/100 Gbps	N3K-C3132C-Z
Nexus 3548-XL Switch, 48 SFP+	N3K-C3548P-XL
Nexus 3264C-E switch with 64 QSFP28	N3K-C3264C-E
Cisco Nexus 3132Q Switch	N3K-C3132C-Z
Cisco Nexus 3132Q-V Switch	N3K-C3132Q-V
Nexus 34180YC programmable switch, 48 10/25G SFP, and 6 40/100G QSFP28 ports	N3K-C34180YC
Cisco Nexus 3464C Switch, 64 x QSFP+/QSFP28 ports and 2 x SFP+	N3K-C3464C
Cisco Nexus 3016 Switch	N3K-C3016Q-40GE
Cisco Nexus 3048 Switch	N3K-C3048TP-1GE
Cisco Nexus 3064-E Switch	N3K-C3064PQ-10GE
Cisco Nexus 3064-X Switch	N3K-C3064PQ-10GX
Cisco Nexus 3064-T Switch	N3K-C3064TQ-10GT
Nexus 31108PC-V, 48 SFP+ and 6 QSFP28 ports	N3K-C31108PC-V
Nexus 31108TC-V, 48 10GBase-T RJ-45, and 6 QSFP28 ports	N3K-C31108TC-V
Cisco Nexus 3132Q Switch	N3K-C3132Q-40GE
Nexus 3132 Chassis	N3K-C3132Q-40GX
Cisco Nexus 3172PQ Switch	N3K-C3172PQ-10GE
Cisco Nexus 3548 Switch	N3K-C3548P-10GX
Cisco Nexus 3636C-R Switch	N3K-C3636C-R

Cisco Nexus 2000 Series Fabric Extenders

Product/Component	Part Number
Nexus 2348 Chassis	N2K-C2348TQ-10GE
Cisco Nexus 2348UPQ 10GE 48 x 1/10 Gigabit Ethernet and unified port host interfaces (SFP+) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces	N2K-C2348UPQ
Cisco Nexus 2148 1 GE Fabric Extender	N2K-C2148T-1GE
Cisco Nexus 2224TP Fabric Extender	N2K-C2224TP-1GE
Cisco Nexus 2232TM 10GE Fabric Extender	N2K-C2232TM-10GE
Cisco Nexus 2232TM 10GE Fabric Extender	N2K-C2232TM-E-10GE
Cisco Nexus 2232PP 10 GE Fabric Extender	N2K-C2232PP-10GE
Cisco Nexus 2248TP 1 GE Fabric Extender	N2K-C2248TP-1GE
Cisco Nexus 2248TP E GE Fabric Extender	N2K-C2248TP-E GE
Cisco Nexus 2248PQ Fabric Extender	N2K-C2248PQ-10GE
Cisco Nexus B22 Fabric Extender for HP	N2K-B22HP-P
Cisco Nexus B22 Fabric Extender for Fujitsu	N2K-B22FTS-P
Cisco Nexus B22 Fabric Extender for Dell	N2K-B22DELL-P
Cisco Nexus 2348TQ-E 10GE Fabric Extender	N2K-C2348TQ-E++

IBM Directors and switches supported in Cisco DCNM 11.4(1)

- IBM SAN192C-6 8978-E04 (4 Module) SAN Director
- IBM SAN384C-6 8978-E08 (8 Module) SAN Director
- IBM SAN768C-6 8978-E16 (16 Module) SAN Director
- IBM SAN50C-R 8977-R50 50-Port SAN Extension Switch
- IBM SAN32C-6 8977-T32 32X32G FC SAN Switch
- IBM SAN48C-6 8977-T48 48X32G FC SAN Switch
- IBM SAN96C-6 8977-T96 96X32G FC SAN Switch



CHAPTER 8

Caveats

Caveats

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, click the **Caveat ID/Bug ID** number in the table. The corresponding **Bug Search Tool** window is displayed with details of the Caveat ID/Bug ID.

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data, such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password at:

   https://tools.cisco.com/bugsearch/

2. In the **Bug Search** window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

This chapter lists the Open and Resolved Caveats in Cisco DCNM, and contains the following section:

Resolved Caveats

The following table lists the Resolved bugs for Cisco DCNM, Release 11.4(1).

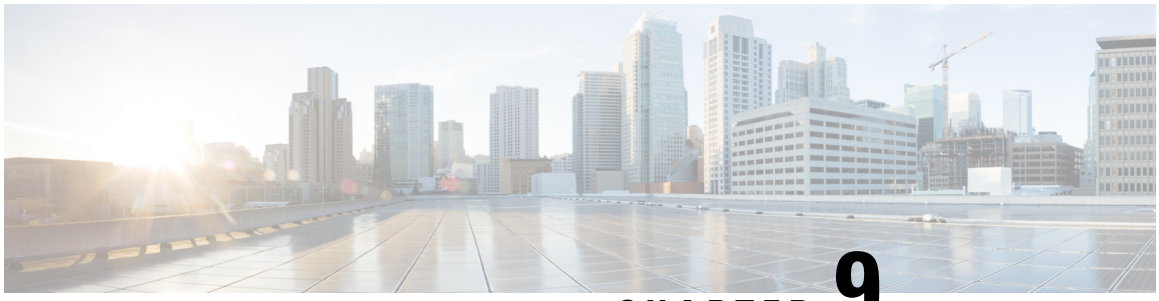
Caveat ID Number	Description
CSCvr27504	After removing of the port channel member from L3-port channel its not reflected in the GUI
CSCvs19617	Pending config API giving 0 line diff in case of freeform restore
CSCvs26355	[FSV-sim] FHR discovery fails, sim connection failure
CSCvs28595	Mcast v4/v6 multipath config gets negated after first deploy
CSCvs32334	Error seen while attaching a policy which was imported using csv
CSCvs33668	Health-monitor: Duplicate alerts showing
CSCvs45584	DCNM-Install:DCNM install should validate the oracle DB during the install.
CSCvs47591	EPL: Dual Attached and Dual Stacked Level 2 charts data issue
CSCvs47864	Cluster mode inline upgrade from 11.2 to 11.3(0.556) stuck at rabbitmq restart
CSCvs47883	Profile refresh of the VRF- edit of dot1q and IP are not reflected on the other side of fabric
CSCvs49653	EPL and Telemetry enable/disable fails when DCNM tracker is enabled
CSCvs52351	Subinterface mtu ordering issue seen after Backup Restore
CSCvt42395	DCNM 11.3.1 and earlier version extremely slow with Chrome version 80 and above.
CSCvu42893	EPL: EPL dashboard is empty when NXAPI calls are dropped by ISE due to missing Remote IP

Open Caveats

The following table lists the Open bugs for Cisco DCNM, Release 11.4(1).

Caveat ID Number	Description
CSCvm90923	SAN Insight: Display warning upon configuring different query types on switches in the same fabric
CSCvr28767	On attaching multiple networks to same interface, the interface diff gets aggregated to single N/W
CSCvt39784	Multi-line banners not shown correctly in side by side diff when Tracker is installed.
CSCvu23101	N/w Name modifications not reflected on N/w deployment page
CSCvu42611	Unassigned ES shards results in ES status as RED
CSCvu44795	config push failed but reported as success in deployment history
CSCvu47104	st fex qos policy deployed only at one peer causes vpc type 2 inconsistency

Caveat ID Number	Description
CSCvu49958	inherited config not removed from member after PO removed
CSCvu54422	"Few licenses are assigned with Eval license, When we assign license through Smart license proxy "
CSCvu61857	pod Name search and Host name search results do not go away on clearing search field
CSCvu67744	EPL: the data downloaded from the snapshot generation has VRF and network interchanged
CSCvu68076	KCV: On resync, one of the cluster data is not visualized
CSCvu73694	Attach/detach of service-policy fails to generate intent in some occassions
CSCvu81364	Failed to load logs error in Administration ---> Logs on click on log files
CSCvu81878	L2 DA/DS dashlet in Data Center scope is missing endpoint data for certain duration
CSCvu81964	NXOS Images uploaded are not put in var lib dcnm images folder
CSCvu82874	EPL: NHV not created after upgrade when DCNM is upgraded during a particular span of time
CSCvu83118	PMN: Exception while trying to add switch in default POD while pushing global config
CSCvu83159	Infoblox: Multiple Manual poll is causing delay/duplicate entries
CSCvu84291	send-lifetime/accept-lifetime commands in key chain configuration dont work for 'local' timezone
CSCvu84565	Not able to create Sub-interface on L3-Po with the API /rest/interface
CSCvu84786	Unable to authenticate from IPAM Integrator app after DCNM restart
CSCvv35543	DCNM post-install IP address change - leaving AMQP server address unchanged
CSCvw83412	when more than 20VM's are added to a vSwitch, vm's get cropped and container namespaces are dangling



CHAPTER 9

Related Documentation

This chapter provides information about the documentation available for Cisco Data Center Network Manager (DCNM) and the platforms that Cisco DCNM manages, and includes the following sections:

Navigating the Cisco DCNM Documentation

This document describes and provides links to the user documentation available for Cisco Data Center Network Manager (DCNM). To find a document online, use one of the links in this section.

Cisco DCNM 11.4(1) Documentation Roadmap

Table 8: Cisco DCNM 11.4(1) Documentation

Document Title	Description
Cisco DCNM Release Notes, Release 11.4(1)	Provides information about the Cisco DCNM software release, open caveats, and workaround information.
Cisco DCNM Compatibility Matrix, Release 11.4(1)	Lists the Cisco Nexus and the Cisco MDS platforms and their software releases that are compatible with Cisco DCNM.
Cisco DCNM Scalability Guide, Release 11.4(1)	Lists the supported scalability parameters for Cisco DCNM, Release 11.4(1).

Document Title	Description
Cisco DCNM Configuration Guides	These configuration guides provide conceptual and procedural information on the Cisco DCNM Web GUI. • Cisco DCNM LAN Fabric Configuration Guide, Release 11.4(1) • Cisco DCNM Media Controller Configuration, Release 11.4(1) • Cisco DCNM SAN Management Configuration Guide, Release 11.4(1) • Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide, Release 11.4(1)
Cisco DCNM Installation Guides	These documents guide you to plan your requirements and deployment of the Cisco Data Center Network Manager. • Cisco DCNM Installation Guide for Media Controller Deployment, Release 11.4(1) • Cisco DCNM Installation Guide for LAN Fabric Management Deployment, Release 11.4(1) • Cisco DCNM Installation and Upgrade Guide for SAN Deployment, Release 11.4(1)
Cisco DCNM Licensing Guide, Release 11.4(1)	Describes the procedure used to generate, install, and assign a Cisco Data Center Network Manager (DCNM) license.
Software Upgrade Matrix for Cisco DCNM 11.4(1)	Lists the software upgrade paths that are supported for DCNM.
Cisco Data Center Network Manager Open Source Licensing, Release 11.4(1)	Provides information about the Cisco Data Center Network Manager Open Source Licensing, Release 11.4(1).
Cisco DCNM REST API Guide, Release 11.4(1)	Cisco DCNM provides REST APIs that allow third parties to test and develop application software. The REST API documentation is packaged with Cisco DCNM, and can be accessed through any browser.
Cisco Data Center Network Manager Troubleshooting Guide, Release 11.x	Describes some common issues you might experience while using Cisco DCNM, and provides solutions.
Cisco DCNM SMI-S and Web Services Programming Guide for SAN, Release 11.x	Provides an industry standard application programming interface (API) using the Storage Management Initiative Specification (SMI-S).
Videos: Cisco Data Center Network Manager, Release 11.4(1)	Lists all the videos created for Cisco DCNM 11.4(1).

Platform-Specific Documents

The documentation set for platform-specific documents that Cisco DCNM manages includes the following:

Cisco Nexus 2000 Series Fabric Extender Documentation

https://www.cisco.com/c/en/us/products/switches/nexus-2000-series-fabric-extenders/index.html

Cisco Nexus 3000 Series Switch Documentation

https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/series.html

Cisco Nexus 4000 Series Switch Documentation

https://www.cisco.com/c/en/us/support/switches/nexus-4000-series-switches/series.html

Cisco Nexus 5000 Series Switch Documentation

https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/series.html

Cisco Nexus 6000 Series Switch Documentation

https://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/series.html

Cisco Nexus 7000 Series Switch Documentation

https://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/series.html

Cisco Nexus 9000 Series Switch Documentation

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/series.html

Day-2 Operation Applications Documentation

- Cisco Network Insights for Data Center
- Cisco Network Insights Base (Cisco NIB)

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to:

dcnm-docfeedback@cisco.com.

We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.