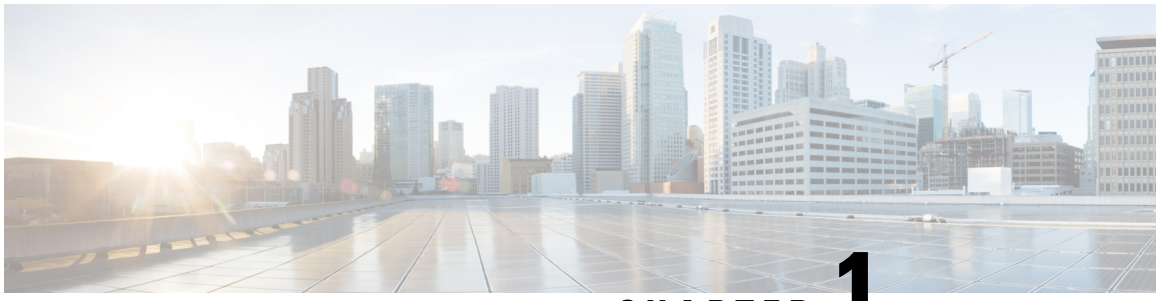
Cisco DCNM Release Notes, Release 11.5(1)

First Published: 2020-12-23

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 non-Cisco devices. DCNM 11 being a multi-fabric controller, it lets you manage many devices both legacy and new age fabric deployments simultaneously, while providing ready-to-use control, management, and automation capabilities for all these environments.

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 11.5(1) manages various kinds of SAN deployments, LAN deployments (including VXLAN EVPN, Routed Fabrics, FabricPath, 3-tier classic deployments, and so on), and IP for Media deployments 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 LAN Fabrics Using Cisco DCNM 11.5(1):

- **Greenfield Deployments**: Applicable for provisioning new VXLAN EVPN fabrics, eBGP based Routed fabrics, and traditional three-tier Access-Aggregation networks
- **Brownfield Deployments**: Applicable for existing VXLAN EVPN fabrics and other legacy environments:
  - 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.
  - Import all existing 3-tier Access-Aggregation, FabricPath, MSDC etc., networks into the DCNM using either the **External_11_1** or **LAN_Classic** fabric templates.
- **Upgrades**: Applicable for all LAN Fabric deployments created with previous DCNM versions:
  - Upgrade for fabrics built with DCNM 11.4(1) to DCNM 11.5(1)
  - Upgrade for fabrics built with DCNM 11.3(1) to DCNM 11.5(1)

- Upgrade for fabrics built with DCNM 11.2(1) to DCNM 11.5(1)

Refer to the *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(1)*.

The Classic LAN Installation mode is deprecated in Release 11.4(1), and isn't available in new installations. Existing DCNM Classic LAN installations are automatically migrated to the DCNM 11.5(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 11.5(1)* .

Note After upgrading the Classic LAN Deployment to Cisco DCNM Release 11.5(1), you can manage, monitor, automate, and control the Classic LAN deployment via the Cisco DCNM 11.5(1) LAN Fabric installation.

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*.

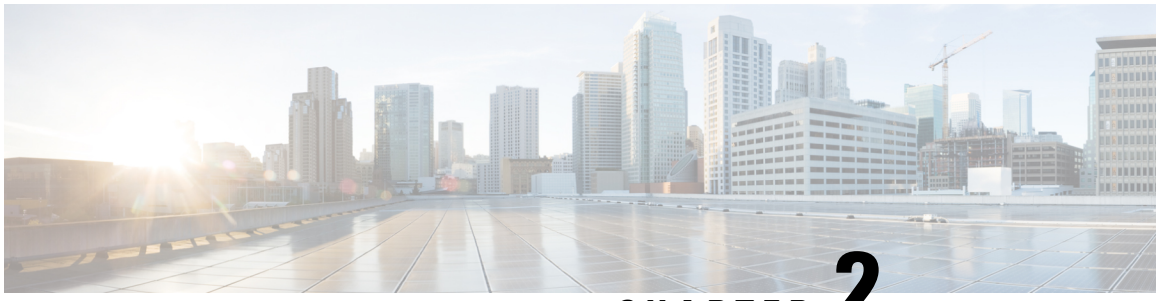
Cisco DCNM LAN Fabric deployment with Compute nodes allows you to install Network Insights applications via the Cisco DCNM Web UI. Refer to *Cisco DCNM LAN Fabric Configuration Guide*

This document provides the Release Notes for Cisco DCNM, Release 11.5(1). Use this document with the documents that are listed in the Related Documentation, on page 51.

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
22 December 2020	Published Release Notes for Cisco DCNM Release 11.5(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

This section describes the various system requirements for proper functioning of your Cisco DCNM Release 11.5(1).

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

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

Java Requirements

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

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM Release 11.5(1), supports the Cisco DCNM server on these 64-bit operating systems:

- **SAN Deployments:**
  - Microsoft Windows 2016
  - Microsoft Windows 2012 R2 update 2919355
  - Red Hat Enterprise Linux Release 7.8, 8.1, and 8.2
  - 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

Supported Latency

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

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

Database Requirements

Cisco DCNM Release 11.5(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 Oracle 12c pluggable database version installation is not supported.

- Oracle 12c RAC (nonpluggable installation)
- PostgreSQL 10.15 - For OVA/ISO deployments
- PostgreSQL 10.15 - For Linux/OVA/ISO deployments
- PostgreSQL 10.15 - 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 and OVA installations support only the embedded PostgreSQL database.

Hypervisors

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

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

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

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

Supported Hypervisors

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

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

Server Resource (CPU/Memory) Requirements

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

Table 2: System Requirements for Cisco DCNM SAN Deployment

Deployment Type	Small (Lab or POC)	Large (Production)	Huge (Production with SAN Insights)
Windows	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not supported
Linux (RHEL)	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 32 vCPUs RAM: 128 GB DISK: 2 TB
OVA/ISO Standalone	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 32 vCPUs RAM: 128 GB DISK: 2 TB

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

Table 3: System Requirements for Cisco DCNM IPFM Deployment

Deployment Type	Small (Lab or POC)	Large (Production)
OVA/ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB

Table 4: System Requirements for Cisco DCNM LAN Fabric Deployment

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

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.

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

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.
- 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 11.5(1) for managing LAN Fabric deployments, see *Verified Scale Limits for Cisco DCNM*.

Table 5: Upto 80 Switches

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

Table 6: 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

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

Some Cisco DCNM features require a license. Before using the licensed features, 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.

VMware Snapshot Support for Cisco DCNM

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

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

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

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

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

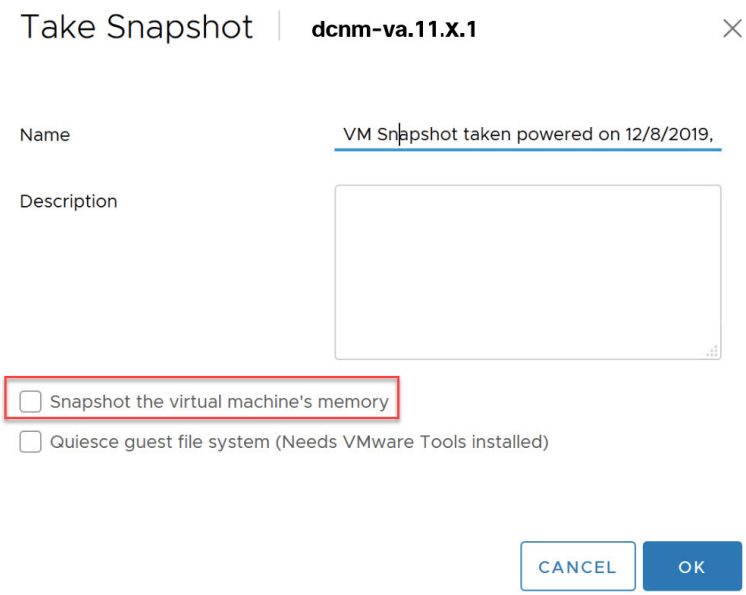
The following snapshots are available for VMs.

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

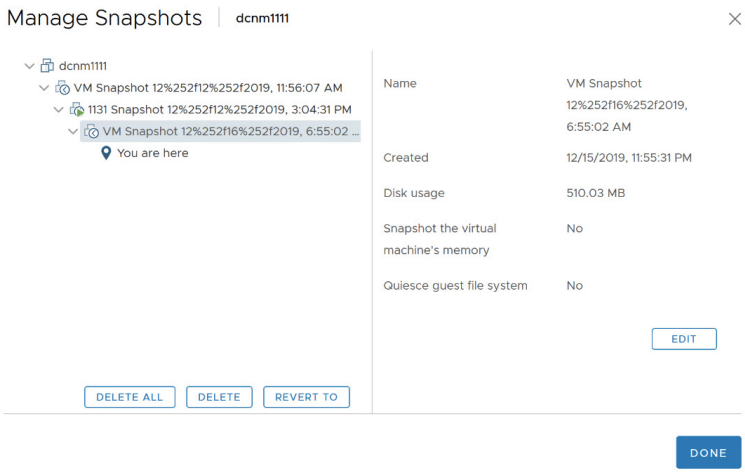
Note Cisco DCNM supports snapshots when VM is either powered on or powered off. DCNM doesn’t support snapshots when the Virtual Machine memory option is selected.

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

System Requirements



You can restore VM to the state in a Snapshot.



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

Supported Web Browsers

Cisco DCNM supports the following web browsers:

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

Other Supported Software

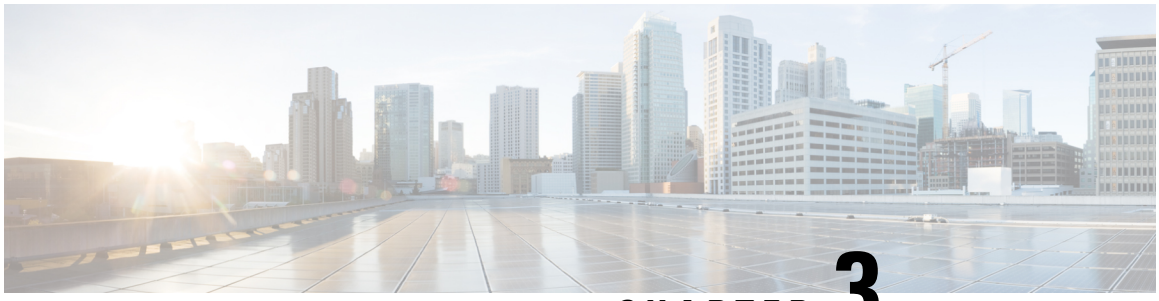
The following table lists the other software that is supported by Cisco DCNM Release 11.5(1).

Table 7: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • ISE version 3.0 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client 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.

System Requirements



CHAPTER 3

Guidelines and Limitations

Guidelines and Limitations

- Ensure that you have 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.
- Restoring DCNM with changes in IP addresses is not supported.
- **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.
- 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.
- 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*.
- 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).
- Cisco DCNM does not support suspending or unsuspending of the VMs.
- 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.
- 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.

- While upgrading from DCNM Release 11.5(1) to Release 11.5(4), if you try to retain when the CA-signed certificates, DCNM fails to launch. For more information, see CSCwb97942.
- In a DCNM managed by NDO, the MSD fabric backup is not restored completely. The MSD fabric is reverted to the time where the deployed networks created on NDO are not yet available. While the fabric shows as in sync in DCNM, there will be no configuration drift notifications in NDO.
- 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 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 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.
- When large number entities (>20K) are collected in PM collections the performance data on **Web UI > Monitor > ISL/NPV Links** may not load completely, as large performance monitor data causes the database query to timeout. To load **Monitor > ISL/NPV Links** entries completely, elasticsearch heap allocation must be increased from 8GB to 12GB or more. You could also increase the RAM configuration for the VM.

Note Scripts are located at the relative folder location where Cisco DCNM is installed.

1. Stop the ElasticSearch by using the following command:

   service elasticsearch stop

2. Edit the jvm options using the following command:

   vi <install-folder>/dcm/elasticsearch/config/jvm.options.

3. Update **-Xms16g** and **-Xmx16g** and save and close the file.

4. Start the ElasticSearch by using the following command:

   service elasticsearch start

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 8: 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 11.5(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
...
```

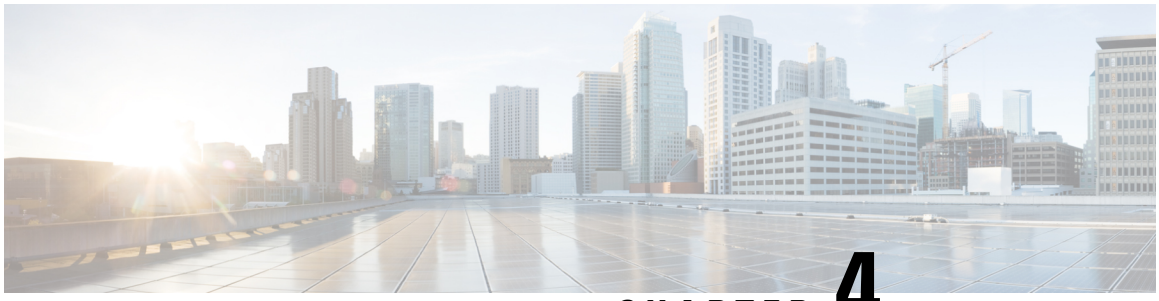
- **Example2**

  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 11.5(1)

These following sections include information about the new features, enhancements, and hardware support introduced in the Cisco DCNM Release 11.5(1).

LAN Fabric Deployment Enhancements

The following features are new in Cisco DCNM Release 11.5(1) for the LAN Fabric Deployment.

Cisco MSO-DCNM Integration

Cisco Multi-Site Orchestrator (MSO) and DCNM integration enables you to perform Layer-2 or Layer-3 extension of overlay Networks or VRFs between multiple VXLAN-EVPN fabrics that are managed by different DCNM controllers. This compliments the Multi-Site Domain (MSD) functionality already present in DCNM that supports VXLAN EVPN Multi-Site capability between multiple fabrics that are part of a single DCNM controller.

You can onboard all of your DCNM fabrics into the Nexus Dashboard (ND) by providing login credentials for the DCNM controllers that manage them all in a single, centralized location. Once onboarded, the ND

makes these fabrics automatically available to MSO as individual sites. The appropriate sites can be converted from unmanaged to managed in the MSO, followed by setting up of the baseline infrastructure connectivity between the sites for VXLAN EVPN Multi-Site underlay/overlay EVPN peering. Subsequently, overlay networks/vrfs can then be provisioned and managed from the MSO for all the managed sites thereby offering a single point of management/provisioning.

Overall, Cisco DCNM and MSO integration enable you to manage VXLAN EVPN-based NX-OS fabrics as well as the fabrics that are already part of a DCNM Multi-Site domain (MSD), establish connectivity across fabrics, configure overlay Layer-2/Layer-3 stretch within and between sites, and scale out existing DCNM deployments.

For more information refer to Cisco Multi-Site Orchestrator Release Notes, Release 3.2(1).

Cisco Nexus Dashboard and DCNM

Cisco Nexus Dashboard (ND) provides a common platform for deploying Cisco Data Center applications. Nexus Dashboard supports the Cisco Day-2 Operations apps, which provide real-time analytics, visibility, and assurance for policy and infrastructure, and the Cisco Multi-Site Orchestrator (MSO) application, which provides a single pane of glass view into managing multiple Cisco DCNM fabrics. ND supports onboarding of Cisco DCNM and APIC sites. Site onboarding entails providing the DCNM hostname or IP address followed by the admin level access credentials. Using this information, ND pulls all the existing fabrics from that DCNM and allows the user to onboard one or more fabrics onto the ND. Each (DCNM, fabric) combination maps to a unique ND Site. All onboarded sites on the ND are made available to all applications that run on top of ND such as MSO.

When ND nodes are deployed for MSO/DCNM environments, the ND computes in a given ND cluster must all be layer-2 adjacent. In other words, the management interface of all nodes must be in one IP subnet and the data interface in a different IP subnet.

For more information, refer to Cisco Nexus Dashboard Release Notes, Release 2.0.1.

Easy Overlay Network Provisioning Using Interface Groups

DCNM now supports configuration provisioning of N overlay networks to M interfaces with a single click. One can select multiple host-facing interfaces and associate them with an Interface Group (IG). Specifically, you can create an interface group for physical Ethernet interfaces, Layer-2 port-channels, or vPCs. You can then associate multiple overlay networks with this IG that in turn automatically attaches those overlay networks to all the interfaces that are part of the IG. Subsequently, any membership change of interfaces to IGs or networks to IGs results in automatic percolation of the appropriate overlay network attachment/detachment state automatically to the respective interfaces. IGs have fabric local scope.

Enhanced RBAC

From Cisco DCNM Release 11.5(1), two new RBAC roles **device-upg-admin** and **access-admin** roles are introduced. A user with role device-upg-admin will only be allowed to perform device upgrade/downgrade, RPM/SMU installation, and EPLD upgrade. The user won't be able to perform any other write operations on the DCNM or the switches. A user with role access-admin will only be able to make configuration changes to host or server-facing ports typically tied to the Interface Manager workflows. They won't be able to make any changes to the underlay or within the fabric builder.

Sync up Out-of-Band Switch Interface Configurations with DCNM

You can now sync-up interface configurations from the switches back up to the DCNM so that the intent in DCNM is appropriately updated. This feature is supported for Easy Fabrics, and External or LAN_Classic fabrics. The interface sync up knob can be enabled on a per switch basis. vPC pairs are detected and the corresponding vPC domain configuration is automatically learned. You can use the **host_port_resync** policy for this purpose.

CloudSec Operational View

You can use the **CloudSec Operational View** tab in DCNM to check the operational status of the CloudSec sessions if CloudSec is enabled on the MSD fabric.

Support for MACsec in Easy Fabric and eBGP Fabric

MACsec is supported in the Easy Fabric and eBGP Fabric on intra-fabric links. You need to enable MACsec on the fabric and on each required intra-fabric link to configure MACsec. There is also an operational view enabled for MACsec.

Inband Management in External Fabrics and LAN Classic Fabrics

From Release 11.5(1), Cisco DCNM allows you to import or discover switches with inband connectivity for External and LAN Classic fabrics. To enable this functionality, select Inband Mgmt check box on Fabric Settings. When this knob is enabled, the fabric supports switch discovery/import over the DCNM inband interface (eth2), in addition to the switches that can be discovered or onboarded via their mgmt0 interfaces. Note that inband POAP is not supported.

Single-switch Configuration Restore

You can restore configuration for a Cisco Nexus switch in external and LAN classic fabrics from the Cisco DCNM Web UI. The information you restore at switch-level is extracted from the fabric-level backups. The switch-level restoration does not restore fabric-level intents and other configurations applied using the fabric settings. Only switch-level intents are restored.

EPLD Golden Upgrade

From Cisco DCNM Release 11.5(1), DCNM supports EPLD golden upgrade as well. When you perform the EPLD upgrade, you have an option to choose the golden or primary region of the Nexus 9000 Series switches. You can view the EPLD golden upgrade notifications in the Events window. From the homepage of the Cisco DCNM Web UI, choose **Monitor > Switch > Events**.

L4-7 Services Enhancements

The following enhancements are introduced in DCNM Release 11.5(1):

- You can specify an arbitrary network, that has not been defined in the top-down configuration, as a source or destination network in the service policy. This helps in streamlining policy enforcement for north-south traffic.
- Layer 4-Layer 7 Service pushes static routes on all VTEPs, including service leaf switches, where the VRF being referenced in the static route is attached. This expedites service node failover with static routes.
- The one-arm Virtual Network Function is supported.
- Layer 4-Layer 7 Service REST APIs are accessible via DCNM packaged REST API Swagger documentation.
- Bulk attachment, detachment, preview, and deployment of route peering and service policies is supported and they are limited up to 10 route peerings or 10 service policies only.
- Audit History feature displays the logs for changes made to service nodes, route peering, and service policies.

Support for Simplified CLI Configuration for Brownfield Deployment

The Brownfield import in DCNM supports the simplified NX-OS VXLAN EVPN configuration CLIs.

OpenStack Workload Visibility

OpenStack plugin application is provided by DCNM that helps you to monitor OpenStack Clusters. You can get visibility with respect to the physical network connectivity and virtualized workloads, and debug VM networking-specific issues within the context of the data center.

This is a preview feature in Cisco DCNM Release 11.5(1). We recommend that you do not deploy this feature in production environments.

PTP Monitoring Application

The Precision Time Protocol (PTP) is a time synchronization protocol for nodes that are distributed across the network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. In DCNM, PTP Monitoring can be installed as an application. This PTP monitoring application, which can be previously installed in Media Controller deployment can now be installed in LAN Fabric deployment as a preview feature. We recommend that you do not deploy this feature in production environments.

Ability to update network parameters

Cisco DCNM allows you to modify few network parameters from the Web UI. Modifying these overwrite the previously configured parameters. Choose Cisco DCNM **Web UI > Admin > DCNM Server > Customization > Network Preferences** to modify the DNS, NTP, and addition or removal of static routes over the out-of-band (eth1) and inband (eth2) interfaces.

DCNM Backup

You can trigger scheduled DCNM backups from the Cisco DCNM Web UI. Based on the schedule that has been set up, at the appropriate time, the appropriate DCNM backup will be triggered. This is supported on both Cisco DCNM Standalone and Native HA deployments. The history and status of the triggered backups is available on the GUI. Backups can be scheduled for local as well as remote destinations. The maximum number of backups you can save is 10.

Media Controller Deployment Enhancements

The following features are new in Cisco DCNM Release 11.5(1) for Media Controller Deployment.

Support for Multicast NAT

Multicast NAT translation of UDP stream is supported on the DCNM IPFM mode. You can apply NAT for the incoming traffic (ingress), or on the egress link or interface. The scope of ingress NAT is entire switch, whereas egress NAT is for a specific interface. The same switch can have both ingress and egress NAT. However, it can’t be on the same flow for a given switch.

Unicast Bandwidth Management Per Port

You can configure an interface to allot a dedicated percentage of bandwidth to unicast traffic. The remaining percentage is automatically reserved for multicast traffic.

SAN Deployment Enhancements

The following features are new in Cisco DCNM Release 11.5(1) for SAN Deployment.

DCNM Web UI start page

When you launch Cisco DCNM SAN and SAN OVA/ISO deployment, the **Summary Dashboard** is displayed. The intent of the Summary dashboard is to enable network and storage administrators to focus on particular areas of concern around the health and performance of data center switching.

Device alias zoning for offline nodes

You can add offline members to device alias zone for SAN and IVR zoning.

Renaming Host and Storage enclosures

You can rename individual members or all members in the enclosures at a single instance. Choose **Dashboard** on Cisco DCNM Web UI, to rename Storage and Host Enclosures.

FICON Dashlets

Three new dashlets, namely, Top FICON Host Ports, Top FICON Control Unit Ports, and Top FCIP ISL are introduced in Release 11.5(1).

SAN Insights Enhancements

- For SAN OVA/ISO deployments
  - DCNM on VM supports 40K ITLs/ITNs.
  - DCNM on Cisco Nexus Dashboard supports 60K ITLs/ITNs.
- For SAN Linux deployment, DCNM supports 20K ITLs/ITNs.

Common Enhancements applicable for all DCNM Install types

Software Maintenance Update to address Log4j2 vulnerability

Cisco DCNM Release 11.5(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.

Set up authentication via TACACS+ server

From Release 11.5(1), Cisco DCNM provides an appmgr command to set up authentication via TACACS+ server for all ssh access as well. Note that DCNM GUI has always supported remote authentication via TACACS+, LDAP, and RADIUS. Once the appmgr related configuration has been set up, any ssh access to the DCNM first will be redirected to the configured TACACS+ server to determine if access is allowed. In case of success, access is granted. When the TACACS+ servers are not reachable, the system reverts to local authentication.

Running DCNM behind a Firewall -- IPv6 Support

Along with IPv4 firewalls, DCNM now supports IPv6 firewalls.

Licensing Enhancements

- From Release 11.5(1), DCNM license trial period is extended to 120 days. However, the trial period remains 60 days for inline upgrades.
- If the switch already has a smart license, DCNM recognizes this during discovery and allows you to assign switch smart license.
- For DCNM LAN Fabric deployments, before you assign switch smart license to a switch, you must configure switches using the fabric builder freeform with the appropriate smart licensing enablement CLIs.

- In the DCNM SAN Client, you can assign honor license to unlicensed fabrics also.

For a more detailed overview on Cisco Licensing, go to https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html.

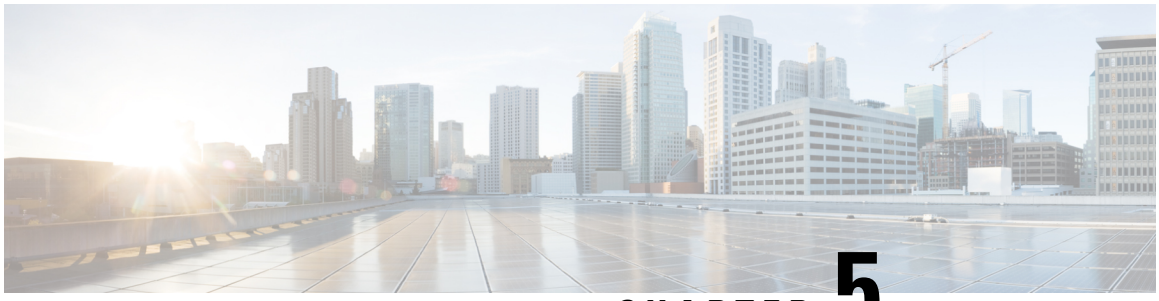
New Hardware Supported

The following new hardware is supported from Cisco DCNM Release 11.5(1).

- Fabric Module for Cisco Nexus 9504 chassis—N9K-C9504-FM-G
- Fan tray for Cisco Nexus 9508 chassis—N9K-C9508-FAN2
- Cisco Nexus 9504 chassis—N9K-C9504-FAN2
- Fabric Module for Cisco Nexus 9508 chassis—N9K-C9508-FM-G
- Cisco Nexus 9500 16p 400G QSFP-DD cloud-scale line card—N9K-X9716D-GX
- Cisco Nexus 9336C-FX2-E, 1RU, fixed-port switch—N9K-C9336C-FX2-E
- Cisco MDS 9220i Intelligent Fabric switch chassis, 12X32G FC+6IPS—DS-C9220I-K9

Videos: Cisco DCNM Release 11.5(1)

For videos created for features in Release 11.5(1), see Cisco Data Center Network Manager, Release 11.5(1).



CHAPTER 5

Upgrading Cisco DCNM

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

Upgrading to Cisco DCNM Release 11.5(1)

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 11.5(1).

Table 9: Type of Upgrade for LAN Fabric deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	Inline Upgrade
11.3(1)	Inline Upgrade
11.2(1)	Inline Upgrade
11.1(1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → represents an Inline Upgrade

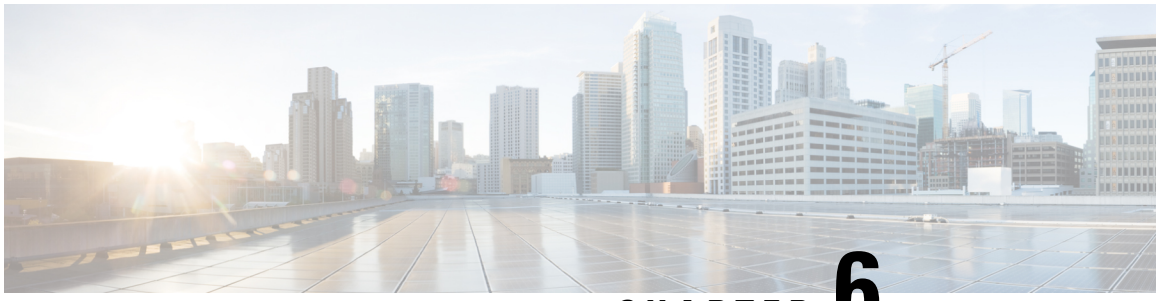
Table 10: Type of Upgrade for IP for Media (IPFM) deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	Inline Upgrade
11.3(1)	Inline Upgrade
11.2(1)	Inline Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.1(1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → represents an Inline Upgrade

Table 11: Type of Upgrade for Cisco DCNM SAN deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO—Inline Upgrade
11.3(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO—Inline Upgrade
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 11.5(1)
11.1(1)	To Windows— 11.1(1) → 11.4(1) → 11.5(1) To Linux— 11.1(1) → 11.4(1) → 11.5(1) 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 11.5(1)



CHAPTER 6

Supported Cisco Platforms and Software Versions

Compatibility Matrix for Cisco DCNM, Release 11.5(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 11.5(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	10.1(1) 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7) 7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9)	9.3(6) 7.0(3)I7(9)
	Newly provisioned VXLAN fabrics N3600	10.1(1) 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7)	9.3(6)
	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	10.1(1) 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7) 7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9)	7.0(3)I7(9)
	Brownfield deployment for N3600	10.1(1) 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7)	9.3(6)
	External/LAN Classic Fabric N3000/3100/3500	10.1(1) 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7) 7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9)	9.3(6)
	External/LAN Classic Fabric N3600	10.1(1) 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7)	9.3(6)
	External/LAN Classic Fabric N5000/5600/6000	7.3(9)N1(1), 7.3(8)N1(1), 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(8)N1(1)
	External/LAN Classic Fabric N7000/7700	8.4(4), 8.4(3), 8.4(2), 8.4(1), 8.3(2), 8.2(6), 8.2(5), 8.2(4) 7.3(7)D1(1), 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(9), 9.3(6)

Installation Type	Fabric Type	Supported Releases	Recommended Releases
		10.1(1) 9.2(4), 9.2(3), 9.3(1), 9.3(2), 9.3(3), 9.3(4), 9.3(5), 9.3(6), 9.3(7) 7.0(3)I7(6), 7.0(3)I7(7), 7.0(3)I7(8), 7.0(3)I7(9)	
	External Fabric for Non-Nexus Devices	Compatibility Matrix for Supported Non-Nexus Devices and Versions, on page 32	
IP for Media (IPFM)	—	10.1(1), 10.1(2), 10.2(1)F 9.3(5), 9.3(6), 9.3(7), 9.3(8)	
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(2c), 8.5(1), 8.4(2b), 8.4(2a), 8.4(2), 8.4.(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 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(33), 6.2(31), 6.2(29), 6.2(27), 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(8g), 5.2(8f), 5.2(8e), 5.2(8d), 5.2(8c)
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(33), 6.2(31), 6.2(29), 6.2(27), 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(2c), 8.5(1), 8.4(2b), 8.4(2a), 8.4(2), 8.1(1b), 8.4.(1a), 8.4(1), 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(33), 6.2(31), 6.2(29), 6.2(27), 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 9220i	8.5(1)

Switches	Supported Switch Releases
Cisco MDS 9300	8.4(2c), 8.5(1), 8.4(2b), 8.1(1b), 8.4(2a), 8.4(2), 8.4(1a), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1a), 8.1(1), 8.4(1), 7.3(1)DY(1), 7.3(1)D1(1), 7.3(0)DY(1), 7.3(0)D1(1) 6.2(33), 6.2(31), 6.2(29), 6.2(29), 6.2(27), 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(33), 6.2(31), 6.2(29), 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(2c), 8.5(1), 8.4(2b), 8.1(1b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 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(33), 6.2(31), 6.2(29), 6.2(27), 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	10.1(1) 9.3(7), 9.3(6), 9.3(5), 9.3(4), 9.3(3), 9.3(2), 9.2(4), 9.3(1), 9.2(3), 9.2(2), 9.2(1) 7.0(3)I7(9), 7.0(3)I7(8), 7.0(3)I7(7), 7.0(3)I4(9), 7.0(3)I7(6), 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)
Cisco Nexus 7000 Series	8.4(4), 8.2(6), 8.2(5), 8.4(1), 8.2(4), 8.4(3), 8.4(2), 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(7)D1(1), 7.3(6)D1(1), 7.3(5)D1(1), 7.3(4)D1(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)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(24), 6.2(22), 6.2(24a), 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)

Switches	Supported Switch Releases
Cisco Nexus 7700 Series	8.4(4), 8.2(6), 8.4(3), 8.4(2), 8.2(5), 8.4(1), 8.2(4), 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(7)D1(1), 7.3(6)D1(1), 7.3(5)D1(1), 7.3(4)D1(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(24a), 6.2(24), 6.2(22), 6.2(24a), 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(10)N1(1), 7.3(9)N1(1), 7.3(8)N1(1), 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(10)N1(1), 7.3(9)N1(1), 7.3(8)N1(1), 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

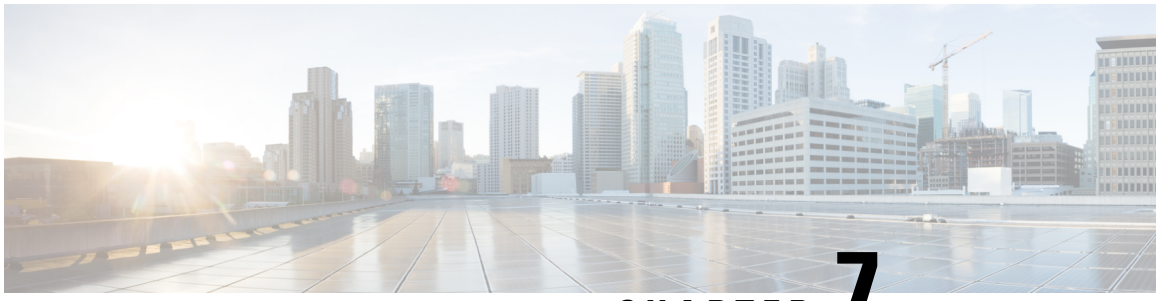
Applications	Supported Versions
Day2 Applications	Refer to Cisco Data Center Networking Applications Compatibility Matrix.
Cisco Multi-Site Orchestrator (MSO)	Release Notes

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 16.12.4a
Cisco NCS 5500	IOS XR 6.5(3)
Arista DCS-7280SR2A	EOS 4.24.2F
Arista DCS-7504N	EOS 4.24.2F



CHAPTER 7

Supported Hardware

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

Hardware Supported in Cisco DCNM, Release 11.5(1)

In a LAN Fabric installation of Cisco DCNM 11.5(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 11.5(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 9220i Intelligent Fabric switch chassis, 12X32G FC+6IPS	DS-C9220I-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

Product/Component	Part Number
Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module	DS-X9112
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

Product/Component	Part Number
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

Product/Component	Part Number
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
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

Product/Component	Part Number
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
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 1-rack unit (RU), switch with following fixed ports: • 48 100M/1/10/25-Gigabit Ethernet SFP28 ports (ports 1-48). • 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54) • One management port (one 10/100/1000BASE-T port) • One console port (RS-232) • 1 USB port	N9K-C93180YC-FX3
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

Product/Component	Part Number
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
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	

Product/Component	Part Number
Fabric Module for Nexus 9504 with 100G support, NX-OS, and ACI spine	N9K-C9504-FM-E
Fabric Module for Nexus 9504 chassis	N9K-C9504-FM-G
Fan tray for Nexus 9504 chassis	N9K-C9504-FAN2
Fabric Module for Nexus 9504 with 100G support, NX-OS only	N9K-C9504-FM-S
Fan tray for Nexus 9508 chassis	N9K-C9508-FAN2
Fabric Module for Nexus 9508 chassis 100G support, NX-OS, and ACI spine	N9K-C9508-FM-E
Fabric Module for Nexus 9508 chassis	N9K-C9508-FM-G
Fabric Module for Nexus 9508 chassis 100G support, NX-OS only	N9K-C9508-FM-S
Cisco Nexus 9500 16p 400G QSFP-DD cloud-scale line card	N9K-X9716D-GX

Cisco Nexus 7000 Series Switches

Product/Component	Part Number
Supported Chassis	
Cisco Nexus 7702 chassis	N77-C7702
Cisco Nexus 7004 chassis	N7K-C7004
Cisco Nexus 7706 chassis	N77-C7706-FAB2
Cisco Nexus 7009 chassis	N7K-C7009
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

Product/Component	Part Number
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
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

Product/Component	Part Number
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
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

Product/Component	Part Number
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
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
1RU 48 x SFP+/SFP28 and 6 x QSFP+/QSFP28	N3K-C34180YC
Cisco Nexus 34200YC-SM Switch with top-of-rack, Layer 2 and 3 switching	N3K-C34200YC-SM
1RU 32 Port QSFP28 10/25/40/50/100 Gbps	N3K-C3132C-Z
Nexus 3548-XL Switch, 48 SFP+	N3K-C3548P-XL

Product/Component	Part Number
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

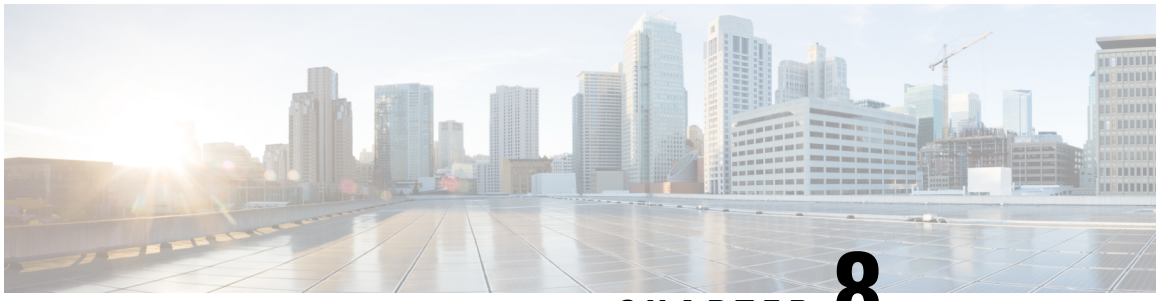
Cisco Nexus 2000 Series Fabric Extenders

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

Product/Component	Part Number
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 11.5(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 11.5(1).

Caveat ID Number	Description
CSCvr28767	On attaching multiple networks to same interface, the interface diff gets aggregated to single N/W
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
CSCvu49958	inherited config not removed from member after PO removed
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

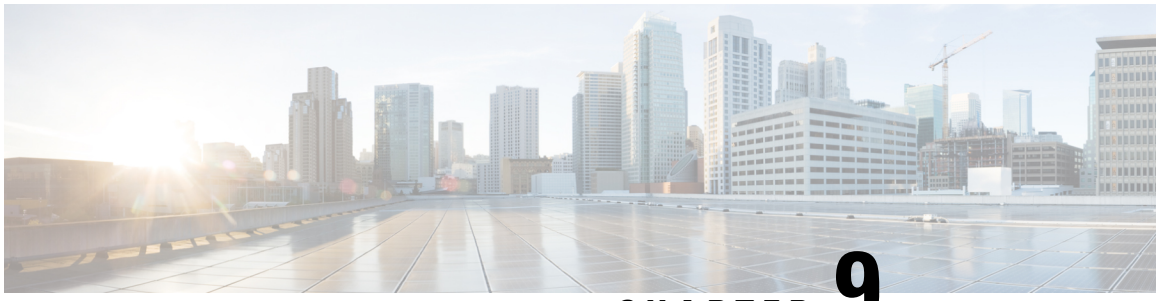
Open Caveats

The following table lists the Open bugs for Cisco DCNM, Release 11.5(1).

Caveat ID Number	Description
CSCvm90923	SAN Insight: Display warning upon configuring different query types on switches in the same fabric
CSCvu61857	pod Name search and Host name search results do not go away on clearing search field
CSCvu81292	Interface page is not reflecting the port channel id , when edited the PO
CSCvv55810	SL: No Licenses are listed in Device Manager of N9k SAN Switch (Admin > Licenses)

Caveat ID Number	Description
CSCvv90161	When containers is checked and page is refreshed, default view is Hierarchical
CSCvw48818	De-associate interfaces with an IG from Interface Manager page click on preview showing interface
CSCvw65832	Support to upload, install 32 bit and 64bit NXOS image of the same version on image upload screen
CSCvw65904	ES Access error after upgrading RHEL Federation set-up form 11.3.1 to 11.5(0.377)
CSCvw73415	Configure: switchTable variable context is lost in wizard
CSCvw73467	Need a dcnm flow to support seamless downgrade to NXOS 936
CSCvw75538	Tracker cannot be installed on switches running 10.1(1)
CSCvw77940	ISSU : After successful upg job status shows in progress
CSCvw78719	DCNM upgrade AMQP server communication failure AMQP User Name or Password is not specified
CSCvw78884	Quick attach of networks in routed fabric throws traceback error
CSCvw80161	DCNM Sanity: Tracker Status on IPV6 Address Switches
CSCvw82589	Upg:Monitor > ISL page blank & hogging CPU , ES heap and not loading the data
CSCvw83178	After inline upgrade from 11.3 to S16 , primary is not coming up
CSCvw83380	IPAM: Failure to load IP-Allocation records after upgrade from DCNM 11.4 to 11.5
CSCvw83599	"For traps to work for inband devices, DCNM needs to push some additional commands using template"
CSCvw83412	when more than 20VM's are added to a vSwitch, vm's get cropped and container namespaces are dangling
CSCvw84262	DCNM Windows Upgrade(11.0.1>11.1.1>11.3.1>11.5.1) - PIPELINE Service should not be shown
CSCvw84520	"upgrading from 11.0.1 > 11.1.1 > 11.2.1/11.3.1 > 11.5.1, ES 2.3 index handling"
CSCvw84929	Certificates are not refreshed after the DCNM is changed from unclustered mode to clustered mode.
CSCvw85005	DCNM Upgrade: IPV6 POAP failure after upgrade from 11.4(1) to 11.5(1.S26) as dhcp6.conf overwritten
CSCvw85354	Errors are not reported during PTP configurations
CSCvw85533	DCNM Sanity: Scheduled Backup does not show in GUI after Upgrade
CSCvw86499	AMQP Server is down After Backup/restore on 11.5

Caveat ID Number	Description
CSCvw86528	MSD/Easy Fabric backup restore after upgrade from 11.4 to 11.5(S27)
CSCvw86814	After Brownfield Import of Networks to MSO and deployment , Moved to pending state on DCNM
CSCvw86849	Update on MSO vrf/nets global parameters is not reflected on the MSD level but on the fabric level
CSCvw87205	Quick detach of network when not attached on switch puts it in pending state without pending configs
CSCvw87293	Loopback update on MSO is not reflected on the MSD level but on the fabric level
CSCvw87461	Template save for network failed on MSD level when created a netwok on MSO with specific parameters
CSCvw87601	Configure:Got null value for time when we refresh the page after the parse error
CSCvx49721	Event forwarder Rule fails for Traps
CSCvx78714	Archive FTP credentials failing for some SAN switches with different confirmation prompt message
CSCvx10880	HW PortMode Policy Create UI failed with "Invalid PORT_MODE with XSS vulnerable content"



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 11.5(1) Documentation Roadmap

Table 12: Cisco DCNM 11.5(1) Documentation

Document Title	Description
Cisco DCNM Release Notes, Release 11.5(1)	Provides information about the Cisco DCNM software release, open caveats, and workaround information.
Cisco DCNM Compatibility Matrix, Release 11.5(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 11.5(1)	Lists the supported scalability parameters for Cisco DCNM, Release 11.5(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 11.5(1) • Cisco DCNM Media Controller Configuration, Release 11.5(1) • Cisco DCNM SAN Management Configuration Guide, Release 11.5(1) • Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide, Release 11.5(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 11.5(1) • Cisco DCNM Installation Guide for LAN Fabric Management Deployment, Release 11.5(1) • Cisco DCNM Installation and Upgrade Guide for SAN Deployment, Release 11.5(1)
Cisco DCNM Licensing Guide, Release 11.x	Describes the procedure used to generate, install, and assign a Cisco Data Center Network Manager (DCNM) license.
Software Upgrade Matrix for Cisco DCNM 11.5(1)	Lists the software upgrade paths that are supported for DCNM.
Cisco Data Center Network Manager Open Source Licensing, Release 11.5(1)	Provides information about the Cisco Data Center Network Manager Open Source Licensing, Release 11.5(1).
Cisco DCNM REST API Guide, Release 11.5(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 11.5(1)	Lists all the videos created for Cisco DCNM 11.5(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.