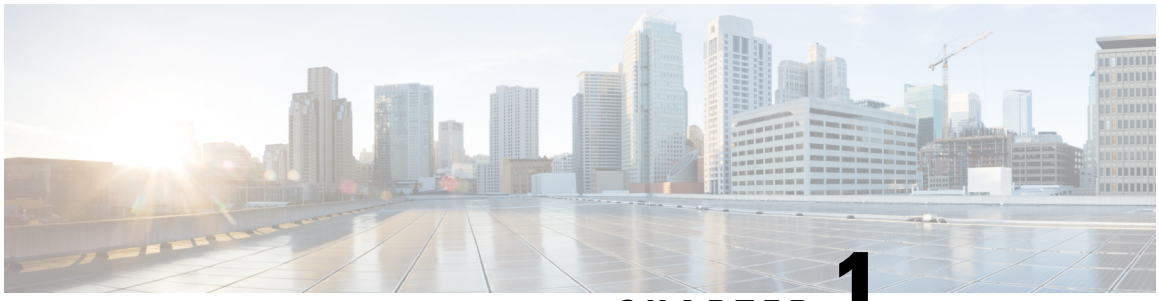
Cisco DCNM Release Notes, Release 11.3(1)

First Published: 2019-12-20

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, Classic LAN, 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. 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 11.3(1) manages SAN, LAN, and LAN Fabrics with VXLAN 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 VXLAN EVPN Fabrics Using Cisco DCNM 11.3(1):

- **Greenfield Deployments**: Applicable for provisioning new VXLAN EVPN fabrics
- **Brownfield Deployments**: Applicable for existing VXLAN EVPN fabrics:
  - Migrate CLI configured VXLAN EVPN fabrics to DCNM.
  - NFM migration to Cisco DCNM 11.3(1) using the `Easy_Fabric_11_1` fabric template is supported.
- **Upgrades**: Applicable for VXLAN EVPN fabrics created with previous DCNM versions:
  - Upgrade for VXLAN fabrics built with DCNM 11.1(1) to DCNM 11.3(1)
  - Upgrade for VXLAN fabrics built with DCNM 11.2(1) to DCNM 11.3(1)

Refer to the *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.3(1)*.

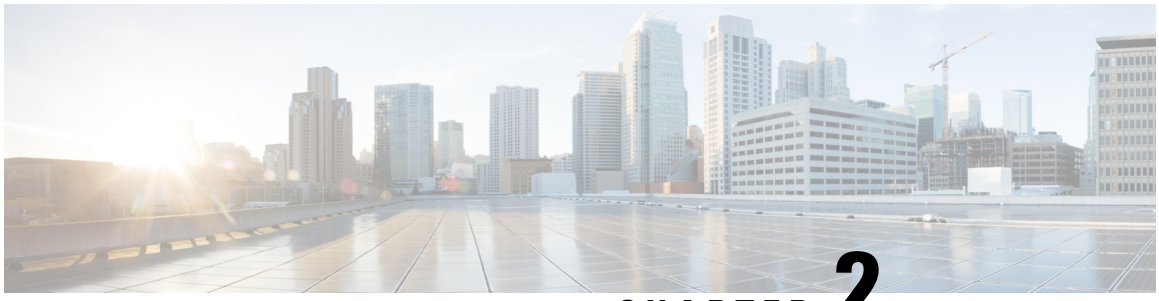
Note Cisco DCNM Classic LAN deployment can also be managed, monitored, automated, and controlled via the Cisco DCNM 11.3(1) LAN Fabric installation using **External Fabrics**. For more information, please refer to the External Fabrics in the *Cisco DCNM LAN Fabric Configuration Guide*.

This document provides the Release Notes for Cisco DCNM, Release 11.3(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
20 December 2019	Published Release Notes for Cisco DCNM Release 11.3(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 11.3(1).

Java Requirements

The Cisco DCNM Server is distributed with JRE 11.0.2 into the following directory:

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM, Release 11.3(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 7.6
  - ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.6
- **IP for Media, LAN Fabric, and Classic LAN Deployments:**

- Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.6
- ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.6

Cisco DCNM Release 11.3(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 Cisco DCNM Release 11.3(1) doesn't support the Oracle 12c pluggable database version installation.

- Oracle 12c RAC (nonpluggable installation)
- PostgreSQL 9.4.5

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.

From Release 11.2(1), 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]
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 16vCPUs, 64G RAM, and 500GB hard disk. Ensure that you do not install the Compute node on 32G RAM server.

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 as well, despite Cisco is only testing on Cisco UCS.

Supported Hypervisors

From Release 11.3(1), Cisco DCNM supports the running of the Cisco DCNM Server on the following hypervisors., for DCNM LAN Fabric and DCNM LAN Classic Deployments:

Hypervisor supported	Data Center Manager server application	Supported deployments
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	Virtual Machine Manager (comes with RHEL 7.6)	• LAN Fabric • Classic LAN
Hyper-V on Windows Server 2019	Hyper-V Manager (comes with Windows Server 2019)	• LAN Fabric[2] • Classic LAN

[2] 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.

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

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

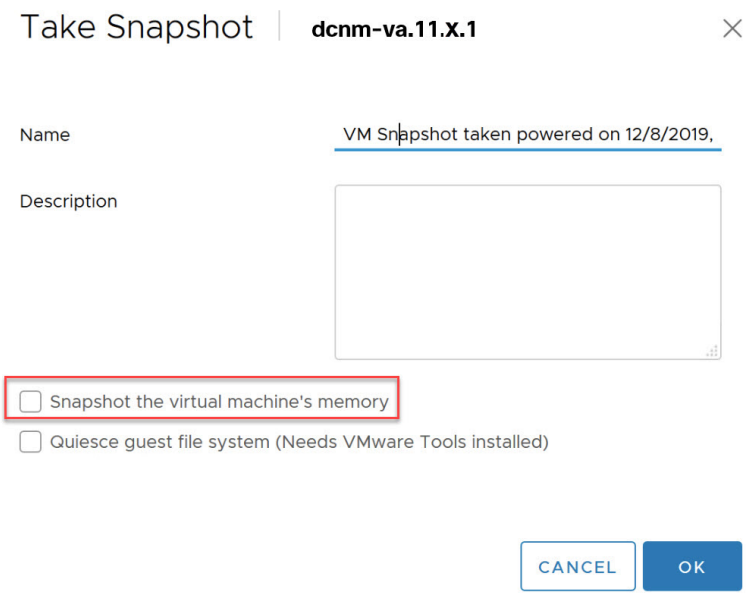
1. Right-click the virtual machine the inventory and select **Snapshots > Take Snapshot**.
2. In the Take Snapshot dialog box, enter a **Name** and description for the snapshot.
3. Click **OK** to save the snapshot.

The following snapshots are available for VMs.

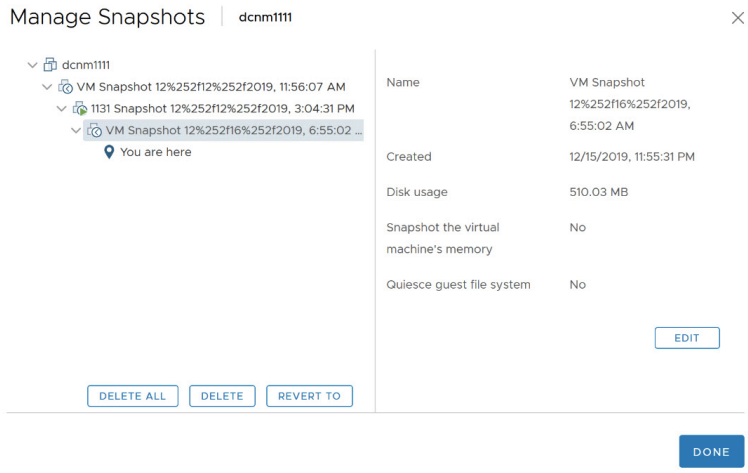
- When VM is powered off.
- When VM is powered on, and active.

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**.

Table 2: Snapshot Support for Classic LAN, LAN Fabric, Media Controller, and SAN OVA Deployments

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

Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Huge (Production)	Compute
SAN	Windows	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not Applicable	Not Applicable
	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
	• 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
IP for Media (IPFM)	• OVA • ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 32vCPUs RAM: 128 GB DISK: 500 GB	Not Applicable
LAN Fabric Classic LAN	• OVA • ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 32vCPUs RAM: 128 GB DISK: 500 GB	CPU: 16 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.

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.

You can add additional disk space to your DCNM set up. Logon to DCNM server using SSH. Extend 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.

Client 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.

Table 3: Client Hardware Requirements

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, you must 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, 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 79.0.3945.79
- Mozilla Firefox Version 71.0 (32/64 bit)
- Microsoft Internet Explorer Version 11.706 update version 11.0.120

Other Supported Software

The following table lists the other software that is supported by Cisco DCNM, Release 11.3(1).

Table 4: Other Supported Software

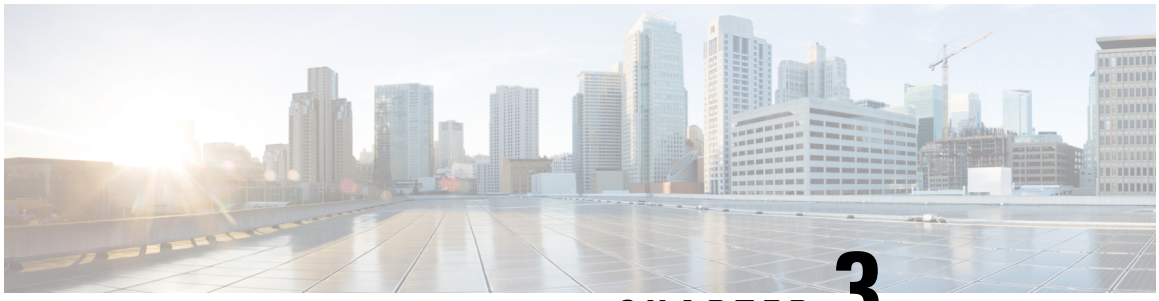
Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client and Cisco DCNM-SAN Server Encryption: HTTPS with TLS 1, 1.1 and 1.2 • TLS 1.3
OVA\ISO Installers	CentOS 7.6/Linux Kernel 3.10.x

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

Qualified Security Certifications

Security Certifications	Date run on DCNM 11.4(1)
Nessus	6/29/2020
Appscan	6/29/2020
Qualsys	6/29/2020

System Requirements



CHAPTER 3

Guidelines and Limitations

Guidelines and Limitations

This section lists guidelines and limitations that are related to the Cisco DCNM Release 11.3(1).

- The icons or fonts on Cisco DCNM GUI may not appear correctly on Microsoft Windows 10 browsers. This problem can occur if your Windows 10 is set to block untrusted fonts or some security or mitigation options. Microsoft's Internet Explorer Browser Support team has provided with the following steps to address this issue.

  Configure the *Allow Font Downloads* Internet Explorer Setting on the Internet Zone and Restricted Sites Zone (enabled by default). Perform the following steps:

  1. Search for **Group Policy Editor** in Control Panel.
  2. Choose **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Allow Font Downloads**.
  3. Double click and choose the **Enabled** radio button.
  4. Click **OK**.
  5. Choose **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Restricted Sites Zone > Allow Font Downloads**.
  6. Double click and choose the **Enabled** radio button.
  7. Click **OK**.
  8. Restart the computer so that the new setting takes effect.

- 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.

- 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 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.
- 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 continues to run DCNM compute nodes and must be stopped manually using **afw service** commands.
- 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.
- Two-factor authentication is not supported in DCNM.
- 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.

- 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 11.3(1), if you have installed a preview feature, perform the following before you upgrade to Release 11.3(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.

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. Use the equivalent **appmgr** commands for changing any IP addresses for eth0, eth1, or eth2 interfaces.

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 11.3(1) 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
...
```

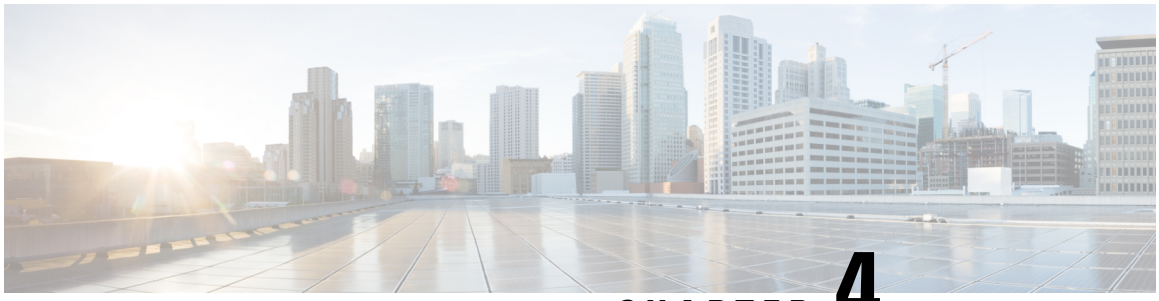
- **Example2**

  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 in Cisco DCNM, Release 11.3(1)

These following sections include information about the new features, enhancements, and hardware support introduced in the Cisco DCNM Release 11.3(1).

LAN Fabric Deployment Enhancements

The following features are new in Cisco DCNM Release 11.3(1) for the LAN Fabric Deployment.

Network Provisioning for Layer 4-Layer 7 Services

Automated provisioning and seamless integration of Layer 4-Layer 7 (L4-L7) services, or Elastic services, in a data center is required, due to the growing SLA and security requirements in a cloud environment. Service devices, such as, firewalls and load balancers are typically attached to service leafs with the goal of redirecting appropriate traffic to these nodes where traffic inspection policies can be applied. A simple workflow has been introduced for easy integration of L4-7 services into a VXLAN EVPN fabric. This includes steps for service node attachment, route peering, service policy configuration, and monitoring.

IPv6 Underlay aka VXLANv6

You can create a VXLAN EVPN fabric with IPv6 only underlay, using either IS-IS or OSPFv3 as the IGPs. This support has been added on N9k based NX-OS devices beginning with software version 9.3(1). In such a VXLANv6 fabric deployment, intra-fabric links, routing loopback, vPC peer link SVI, and NVE loopback interface for VTEPs are all configured only with IPv6 addresses. EVPN BGP neighbor peering is also established using IPv6 addressing. VXLANv6 does not support FEX attached to a VXLAN-enabled switch.

Support for POAPv6

Zero-touch Day-0 bring-up of devices is now supported with DCNM using only IPv6. The bootstrap functionality in DCNM has been extended to support either POAPv6. On a per fabric basis, either POAPv4 or POAPv6 can be selected. Coexistence of POAPv4 and POAPv6 across multiple fabrics is supported.

VXLAN EVPN to SR-MPLS and MPLS LDP Interconnection

The following handoff features are supported in DCNM:

- VXLAN to SR-MPLS
- VXLAN to MPLSLDP

These features are supported on the border devices, such as, border leaf, border spine, and border super-spine in VXLAN EVPN fabrics. The devices must be running Cisco NX-OS Release 9.3(1) or later. These DCI handoff approaches are the one box DCI solution where no extra Provider Edge (PE) device is needed on the external fabric.

Support for Non-Nexus devices

You can discover the following non-Nexus devices in an external fabric:

- IOS XE-based devices: Cisco CSR 1000v
- IOS XR-based devices: Cisco ASR 9000 Series Routers and Cisco NCS 5500 Series Routers
- Arista Devices

Hybrid Cloud Connectivity

DCNM 11.3(1) allows seamless integration of your existing Cisco Data Center to the public cloud, not only providing significant investment protection, but also acts as an incremental step for a customer's journey into the cloud. Cisco Multi-Cloud with DCNM version 11.3 supports Microsoft Azure as the first public cloud, with more to come. The integration is achieved employing the Cisco 1000V cloud services router using the same Multi-Site constructs and workflows that are used to extend DCI between multiple on-premise data centers managed by DCNM.

Endpoint Locator 2.0

From Cisco DCNM Release 11.3(1), information about the Endpoint Locator is displayed on a single landing page or dashboard. The dashboard displays a near real-time view (refreshed every 30 seconds) pertaining to all the active endpoints across all fabrics. The data that is displayed on this landing page depends on the scope that you select from the **SCOPE** drop-down list. The following enhancements are made to the Endpoint Locator (EPL) feature on DCNM:

- Support for monitoring and tracking of Dual-attached and Dual-Stack endpoints
- Capability to monitor and display MAC-only endpoints for Layer-2 VXLAN EVPN deployments.
- Multi-Fabric Support: Up to four fabrics are supported. This is supported only in clustered mode.
- Support for Multi-Site Deployments using Multi-Site Domains(MSD)
- EPL for VXLANv6 fabrics
- Supported scale: 100K unique endpoints

Super-Spine Support

Super Spines are supported within the VXLAN EVPN Easy Fabric (aka fabrics created with the Easy_Fabric_11_1 template). Super Spines are devices that allow multiple spine-leaf based VXLAN EVPN PODs to be interconnected in a seamless manner. The same IGP domain extends across the PODs all the way to the Super Spines. Border functionality can optionally be configured on the Super Spines. The following Super-Spine roles are supported in DCNM:

- Super-Spine
- Border Super-Spine
- Border Gateway Super-Spine

Autoprovisioning of ToR Switches

You can add Layer 2 Top-of-Rack (ToR) switches in an external fabric, and they can be connected to the Leaf switches in the Easy Fabric. Typically, the Leaf and ToR devices are connected with back-to-back vPC connection. By enabling an autoprovisioning knob in the Multi-Site Fabric template, appropriate VLAN and interface configuration can be auto-provisioned on the ToR switches, based on the overlay networks that are deployed on the attached leaf switches.

Deploying Networks in Routed Fabrics

From Cisco DCNM Release 11.3(1), you can use the existing Networks & VRFs workflow to create appropriate HSRP or VRRP-based network configuration in a spine-leaf based routed fabric. This is the typical deployment case for MSDs. A routed fabric is run in one VRF, which is the default VRF. Since the fabric is an IPv4 fabric, IPv6 address provisioning for the networks isn't supported. In a routed fabric, a layer-3 network can only be attached to one device or a pair of vPC devices, unless it's a Layer 2 only network.

DCNM Tracker

From Cisco DCNM Release 11.3(1), use the DCNM tracker feature to enable continuous configuration compliance(CC) checks. The DCNM Tracker is targeted for large-scale deployments or for users requiring prompt Out-of-band notifications. The core configuration compliance (CC) engine logic in DCNM is now packaged into a new form factor that can be installed directly on the switch. Installation of a DCNM tracker via the DCNM GUI, leads to the installation of a small utility that runs on the guest shell of the switch and monitors changes in intent, running configuration, and so on. The changes are then relayed back to the parent DCNM instance.

Strict Configuration Compliance

The Strict Configuration Compliance feature performs a strict check on the exact difference between the running configuration on the switch versus the associated intent. Any commands including any defaults generated in the running configuration by the switch, needs to be part of the intent; otherwise an OUT-OF-SYNC status will be reported. In that case, the pending configuration generates **no** commands for the configurations that are present on the switch but aren't present in the associated intent. You can enable the strict configuration compliance feature in the **Fabric Settings** of the easy fabric templates. This feature is disabled by default.

Note If Strict Configuration Compliance is enabled in a fabric, you can't deploy Network Insights for Resources on Cisco DCNM.

Preview Config

Starting from Cisco DCNM Release 11.3(1), you can right-click the switch in the **Fabric Builder** window and click **Preview Config** to view the pending configuration and the side-by-side comparison of the running and expected configuration aka intent.

BFD Underlay

From Cisco DCNM Release 11.3(1), BFD within a fabric is supported natively. The BFD feature is disabled by default in the Fabric Settings. If enabled, BFD can be enabled individually for the underlay protocols, BGP, PIM etc. across the entire fabric. Any custom required BFD configurations must be deployed via the per switch freeform or per interface freeform policies.

Layer 3 Port Channel Support

From Cisco DCNM Release 11.3(1) Layer 3-port channels are natively supported for external connectivity. This includes support for Layer-3 port-channel sub-interfaces. All configuration knobs related to Layer-3 port-channels are available in the default best practice template that is packaged with DCNM.

Symmetric VRF Lite Auto-Provisioning

From Cisco DCNM Release 11.3(1), VRF Lite configuration can be automatically provisioned in a symmetric manner between border devices and external routers connected via VRF Lite.

Operational Support for Easy Fabrics

This feature provides the operational status of a fabric in terms of active monitoring of BGP sessions, IS-IS/OSPF sessions, vPC peer-keep-alive sessions etc. and provides a logical link topology view for easy perusal. In the Fabric Builder, there's a tabular view that lists down this operational status on a per fabric basis.

Pre-ISSU and Post-ISSU Reports for LAN Fabric Deployments

While performing switch image upgrades using DCNM, you can now perform appropriate customized pre-upgrade and post-upgrade checks as part of the enhanced upgrade workflow. This leverages the novel flexible programmable report infrastructure introduced in DCNM 11.3(1). The infrastructure allows a user to generate pre-ISSU and post-ISSU reports when you install the Image Management and Upgrade workflow.

Package [SMU/RPM] in LAN Fabric Deployments

Image Management also helps you to install or uninstall the required packages and patches. All RPM packages and SMU patches of the selected fabric appear in the Package [SMU/ RPM] window. You can now install, uninstall, activate, or deactivate packages using SMU or RPM.

Image Management Policies in LAN Fabric Deployments

The image management policies have the information of intent of NX-OS images along with RPMs or SMUs. The policies can belong to a specific platform or to an umbrella of different types of platforms. An umbrella type policy can have policies for one or more platforms. Regardless of a switch's platform, you can associate an umbrella image management policy with a group of switches. Based on the policy applied on a switch, Cisco DCNM checks if the required NX-OS and RPMs or SMUs are present on the switch. If there is any mismatch between the policy and images on the switch, an appropriate fabric warning is generated.

DCNM on SE appliance

Beginning from Release 11.3(1), for the compute nodes on which NIR/NIA will be hosted, in addition to the OVA/ISO, you can now use the SE-CL-L3 appliance. With the SE, the ISO image is pre-installed in compute mode on the physical appliance. Refer to Application Services Engine Release Notes for Cisco DCNM for more information.

Media Controller Deployment Enhancements

The following features are new in Cisco DCNM Release 11.3(1) for Media Controller Deployment.

RTP Flow Monitor

Cisco DCNM allows you to monitor per flow RTP traffic and receive an alert in case of packet drops. Information about any loss in flow is streamed to the Cisco DCNM controller which then indicates the location in the network where the loss was detected. You can view the flow topology for the active flows.

Scope in Media Controller

The switch groups that you created in the **Administration > DCNM Server > Switch Groups** window are listed under the **SCOPE** drop-down list. Creating switch groups help you to manage switches because they are grouped logically. For example, you can create host or flow policies for switches in a specific switch group instead of creating it for all the switches. Similarly, you can view the flow topology for a specific switch group containing switches.

PMN Read-Only Update

Starting from Cisco DCNM Release 11.3(1), Host Policies, Flow Policies, and Global menu items are displayed in the Media Controller deployment in DCNM Read-only mode. DCNM retrieves information about the host policies, flow policies, and global configuration from each switch in the fabric and displays the retrieved information. The information that is displayed is specific to each switch.

PTP Monitoring Application

The Precision Time Protocol (PTP) is a time synchronization protocol for nodes that are distributed across a network. On a local area network, it achieves clock accuracy in the submicrosecond range, making it suitable for measurement and control systems. In DCNM, PTP Monitoring can be installed as an application.

Discovered Host Enhancement

Starting from Cisco DCNM Release 11.3(1), multiple entries of the same host are grouped as an expandable row

SAN Deployment Enhancements

The following features are new in Cisco DCNM Release 11.3(1) for SAN Deployment.

- From Release 11.3(1), Cisco DCNM allows SAN deployment using OVA/ISO installations. You can also migrate performance data from 10.4(x), 11.1(1), and 11.2(1) releases to the newly installed DCNM 11.3(1).
- From Release 11.3(1), Cisco DCNM SAN Client is shipped with self-signed certificate as trust certificate for the DCNM Server. If the DCNM server certificate is updated to use CA signed certificate, you must modify the trust certificate on the SAN Client.
- You can configure alarms for SAN switches.

SAN Insights Enhancements

- SAN Insights is not supported on Windows from Release 11.3(1).
- From Release 11.3(1), SAN Insights is supported with Cisco DCNM OVA/ISO deployments.
- Top 10 Host and Top 10 Storage analytics is displayed on the SAN Insights Dashboard. Each graph shows Top 10 details based on read/writes for IOPs, throughput, ECT.

  Also, you can also view the data for either Enclosure or WWN.
- Along with the current FC-SCSI endpoints, Cisco DCNM supports flows to the FC-NVMe endpoints also.
  - DCNM Nexus pipeline receives FC-NVMe flow data streaming from Cisco MDS9000 switches.

- Post processing is updated to calculate deviation and other metrics for FC-NVMe flows.
- San Insights Dashboard, Monitoring SAN Insights allow you to choose either FC-SCSI or FC-NMVe analysis.

- Deviation buckets can be configured, based on your requirements, by editing the **san.telemetry.deviation** parameters in the server properties file.

Common Enhancements applicable for all DCNM Install types

Software Maintenance Update to address Log4j2 vulnerability

Cisco DCNM Release 11.3(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.

DCNM Integration with ServiceNow

ServiceNow offers applications for IT Service Management (ITSM) and IT Operations Management (ITOM). There are four primary modules, namely, inventory discovery, incident management, event management, and change management workflows. Starting from Cisco DCNM Release 11.3(1), we provide Cisco DCNM integration with ServiceNow. This enables you to integrate end-user IT data with the ServiceNow platform. The integration provides a default set of ServiceNow custom tables that are populated with configuration data.

REST API Tool

All operations triggered via the DCNM Web UI like discovery, fabric management, monitoring, and so on, result in invocation of a series of HTTP calls to DCNM server to complete the respective task/operation. The REST API tool enables you to examine each of these API calls by viewing the structure of an API call. This tool also provides a corresponding CURL request that can aid in building quick prototypes for northbound integration to DCNM by calling the respective APIs. This tool compliments the Swagger-based REST API definitions that are exposed via the product URL, https://DCNM-IP/api-docs.

Login Image and MOTD

Now you can customize the background image and add a message to the Cisco DCNM Web UI login page. If you have many instances of DCNM, this allows you to identify the correct DCNM instance based on the background image and the message on the login screen.

Licensing Enhancements

From Release 11.3(1), Cisco DCNM Evaluation license validity is extended from 30 days to 60 days. That implies, the evaluation license expires after 60 days. However, Cisco DCNM allows you to use all the licensed features. Switches remain in honor mode until the switch is licensed again or the user manually removes the license.

In addition, the new UI enhancement for bulk license installation, allows you to upload multiple license files at once. It parses the license files, extract serial numbers, and tag them to the respective switches. The appropriate licenses are then applied to the respective switches.

New Hardware Supported

- N9K FC/FCoE switch-mode support for N9K-93180YC-FX

User Access

From Release 11.3(1), Cisco DCNM offers the user access based on your network security requirements. The following user roles are used to access DCNM via SSH or console that is introduced with Release 11.3(1).

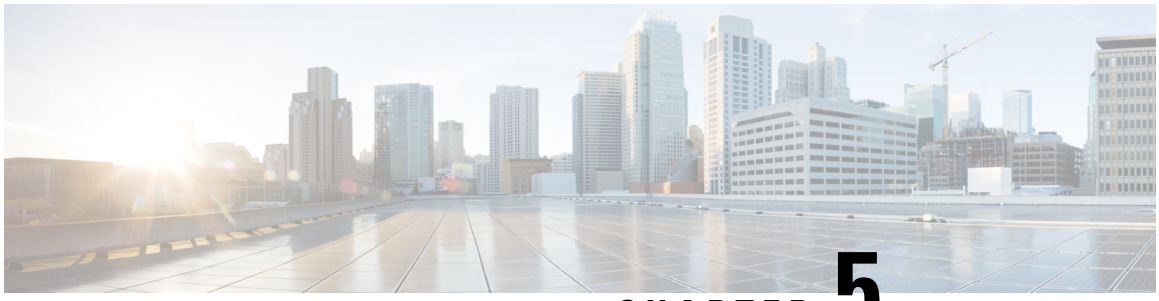
- sysadmin
- SSH access by user root

The DCNM GUI root user is no longer created. Alternatively, use the Admin user role to log on to the DCNM Web UI.

Note During Inline upgrade, you must provide a new password for the **sysadmin** user.

Videos: Cisco DCNM Release 11.3(1)

For videos created for features in Release 11.3(1), see Cisco Data Center Network Manager, Release 11.3(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. However, there is not upgrade path for SAN OVA\ISO.

From Release 11.3(1), Cisco DCNM OVA and ISO is supported for SAN functionality.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.3(1).

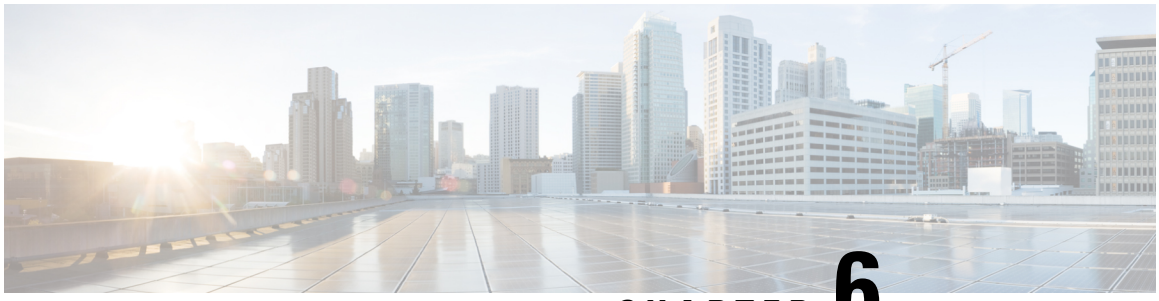
Table 6: Type of Upgrade for Classic LAN, LAN Fabric, and IP for Media (IPFM) deployments

Current Release Number	Upgrade type to upgrade to Release 11.3(1)
11.2(1)	Inline Upgrade
11.1(1)	Inline Upgrade
11.0(1)	11.0(1) → 11.1(1) → 11.3(1) **1.** Upgrade to 11.1(1) using Inline Upgrade **2.** Upgrade from 11.1(1) to 11.3(1) using Inline Upgrade
10.4(2) [3]	10.4(2) → 11.1(1) → 11.3(1) **1.** Upgrade to 11.1(1) using the DCNMUpgradeTool **2.** Upgrade from 11.1(1) to 11.3(1) using Inline Upgrade

[3] (This upgrade path is not supported for Cisco DCNM Media Controller deployments)

Table 7: Type of Upgrade for Cisco DCNM SAN deployments

Current Release Number	Upgrade type to upgrade to Release 11.3(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 **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(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 **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(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 **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).



CHAPTER 6

Supported Cisco Platforms and Software Versions

Compatibility Matrix for Cisco DCNM, Release 11.3(1)

The below table shows the Cisco DCNM Compatibility Matrix for Release 11.3(1).

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

Table 8: Compatibility Matrix for Cisco DCNM, Release 11.3(1)

Cisco MDS 9100	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), 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 9300	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(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 9000v	9.3(2), 9.2(4), 9.3(1), 9.2(3), 9.2(1), 7.0(3)I7(3), 7.0(3)I7(2), 7.0(3)I7(1), 7.0(3)I6(2)
Cisco Nexus 9000 Series	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)
Cisco Nexus 7000 Series	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(12), 6.2(10), 6.2(8), 6.2(6a), 6.2(6), 6.2(2a), 6.2(2), 6.1, 6.0, 5.2, 5.1, 5.0, 4.2, 4.1, 4.0
Cisco Nexus 7700 Series	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(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(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)
Cisco Nexus 4000 Series	4.1(2)
Cisco Nexus 3600 Series	9.3(3), 9.3(2), 9.2(4), 9.3(1), 9.2(3), 9.2(2)

Cisco Nexus 3500 Series	7.0(3)I7(8), 9.3(3), 7.0(3)I7(7), 7.0(3)I7(6), 9.3(2), 9.2(4), 9.3(1), 9.2(3), 9.2(2), 9.2(1), 7.0(3)I7(5), 7.0(3)I7(1), 7.0(3)I2(4), 7.0(3)I2(5), 7.0(3)I4(5), 7.0(3)I4(6), 7.0(3)I4(7), 7.0(3)I4(8), 7.0(3)I5(2), 7.0(3)I5(1), 7.0(3)I4(4), 7.0(3)I4(3), 7.0(3)I4(2), 7.0(3)I4(1), 7.0(3)i3(2), 7.0(3)I3(1), 7.0(3)I2.3, 7.0(3)l2.2a,7.0(3)l2.1, 6.0(2)U3(2), 6.0(2)A8(9), 6.0(2)A3(1), 6.0(2)A1(1d), 5.0(3)A1(2a)
Cisco Nexus 3400 Series	9.2(2v), 9.2(2t)
Cisco Nexus 3100 Series	7.0(3)I7(8), 9.3(3), 7.0(3)I7(7), 9.2(4), 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)I4(8), 7.0(3)I4(7), 7.0(3)I7(3), 7.0(3)I7(2), 7.0(3)I7(1), 7.0(3)I6(2), 7.0(3)I6(1), 7.0(3)I2(4), 7.0(3)I2(5), 7.0(3)I4(5), 7.0(3)I4(6), 7.0(3)I4(7), 7.0(3)I4(8), 7.0(3)I5(2), 7.0(3)I5(1), 7.0(3)I4(4), 7.0(3)I4(3), 7.0(3)I4(2), 7.0(3)I4(1), 7.0(3)I3(1), 7.0(3)I2.3, 7.0(3)l2.2a, 7.0(3)l2.1, 6.0(2)U3(2), 6.0(2)U3(1), 6.0(2)U2(1), 6.0(2)U2(1)
Cisco Nexus 3000 Series	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)I4(8), 7.0(3)I4(7), 7.0(3)I7(3), 7.0(3)I7(2), 7.0(3)I7(1), 7.0(3)I6(2), 7.0(3)I6(1), 7.0(3)I2(4), 7.0(3)I2(5), 7.0(3)I4(5), 7.0(3)I4(6), 7.0(3)I4(7), 7.0(3)I4(8), 7.0(3)I5(2), 7.0(3)I5(1), 7.0(3)I4(4), 7.0(3)I4(3), 7.0(3)I4(2), 7.0(3)I3(2), 7.0(3)I3(1), 7.0(3)I2.3, 7.0(3)l2.2a, 7.0(3)l2.1, 6.0(2)U3(2), 6.0(2)U3(1), 6.0(2)U2(3), 6.0(2)U2(1), 6.0(2)U1(3), 6.0(2)A1(1b), 6.0(2)A1(1a), 6.0(2)A1(1), 6.0(2)U1(2), 6.0(2)U1(1), 5.0(3)U5(1i), 5.0(3)U4(1), 5.0(3)A1(2a), 5.0(3)U5(1e), 5.0(3)U4, 5.0(3)U3, 5.0(3)U2, 5.0(3)U1
Cisco Nexus 1010 Series	4.2(1)SP1(6.1), 4.2(1)SP1(5.1a) , 4.2(1)SP1(4a)
Cisco Nexus 1000v Series	5.2(1)SV3(1.4), 4.2(1)SV2(2.3), 4.2(1)SV2(2.2), 4.2(1)SV2(2.1), 4.2(1)SV2(1.1), 4.2(1)SV1(4), 5.2(1)SM1(5.1)
UCS Infrastructure and UCS Manager Software	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 Each Installation Type

Table 9: Supported Switch Versions for Cisco DCNM 11.3(1)

Installation Type	Switch Versions
Classic LAN	See Table 8: Compatibility Matrix for Cisco DCNM, Release 11.3(1).

Installation Type	Switch Versions
LAN Fabric	• Newly provisioned VXLAN fabrics using DCNM (Easy_Fabric_11_1, Easy_Fabric_eBGP and MSD_Fabric_11_1): 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 7.0(3)I7(7)*****, 7.0(3)I7(6), 7.0(3)I7(8) • External Fabric N3000/3100/3500 (External_Fabric_11_1): 7.0(3)I7(8), 7.0(3)I7(7)***** • External Fabric N3600 (External_Fabric_11_1): 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3) • External Fabric N5000/5600/6000 (External_Fabric_11_1): 7.3(6)N1(1), 7.3(5)N1(1)***** • External Fabric N7000/7700 (External_Fabric_11_1): 8.2(5),7.3(5)D1(1),7.3(3)D1(1)*****, 8.2(3)***** • External Fabric N9000 (External_Fabric_11_1): 9.2(3), 9.2(4), 9.3(1), 9.3(2), 9.3(3), 7.0(3)I7(8), 7.0(3)I7(7)*****, 7.0(3)I7(6) • Migrating NFM-managed VXLAN fabric to DCNM (Easy_Fabric_11_1): 7.0(3)I7(8), 7.0(3)I7(7)*****, 7.0(3)I7(6) • Migrating Switch CLI configured VXLAN fabrics to DCNM (Easy_Fabric_11_1): 9.3(3), 9.3(2), 9.2(4), 7.0(3)I7(8), 7.0(3)I7(7)*****, 7.0(3)I7(6), 7.0(3)I4(9)
IP Fabric for Media (IPFM)	9.3(3),9.3(2), and 9.3(1)
SAN	See the SAN supported switches in Table 8: Compatibility Matrix for Cisco DCNM, Release 11.3(1), on page 27.

*****Indicates the recommended NX-OS version

Compatibility Matrix for Cisco DCNM and Applications

Table 10: Supported Application Versions for Cisco DCNM 11.3(1)

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

Compatibility Matrix for Cisco Non-Nexus Switches and Third Party Switches

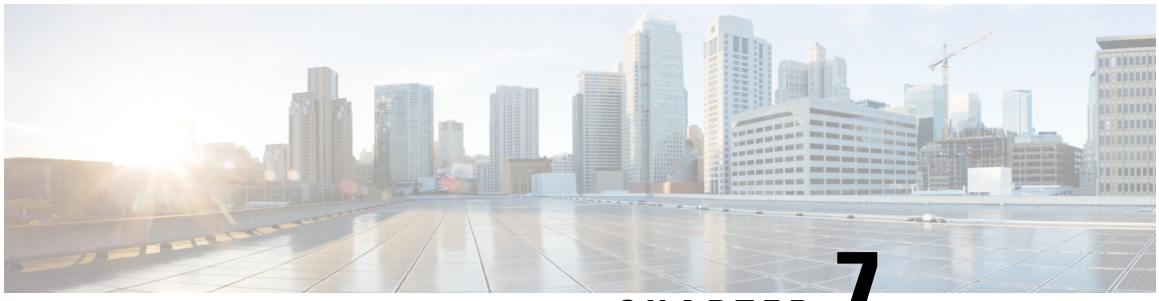
Table 11: Supported Cisco Non-Nexus Switches and Third Party Switches supported with Cisco DCNM 11.3(1)

Cisco Non-Nexus Switches/Third Party Switches	Versions
Cisco CSR1000v	IOS XE Gibraltar 16.10.x

Cisco Non-Nexus Switches/Third Party Switches	Versions
Cisco NCS 5500	IOS XR 6.5(3)
Cisco ASR-9904	IOS XR 6.3.1
Cisco ASR-9006	IOS XR 5.3.0
Arista DCX-7050SX-72Q	EOS 4.21.4f
Arista DCS-7504N	EOS 4.21.4f

Table 12: Supported ServiceNow versions with Cisco DCNM

Cisco DCNM Release Version	Supported ServiceNow Version
Release 11.3(1)	1.0



CHAPTER 7

Supported Hardware

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

Hardware Supported in Cisco DCNM, Release 11.3(1)

In a LAN Fabric installation of Cisco DCNM 11.3(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 11.3(1).

Table 13: 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

Table 14: Cisco MDS 9000 Family

Product/Component	Part Number
Cisco MDS 9710 Crossbar Fabric-3 Switching Module	DS-X9710-FAB3
Cisco MDS 9700 Series Supervisor-4 Module ()	DS-X97-SF4-K9
MDS 9700 Series Supervisor-4/FAb3 6 slot 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

Table 15: 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
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 10/25G SFP28 + 6 40/100G QSFP28	N9K-C93180YC-FX
1RU TOR, fixed module for Nexus 9300 Series 6 40G/100G QSFP28 + 48 10G BASE-T	N9K-C93108TC-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

Product/Component	Part Number
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
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	

Product/Component	Part Number
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
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

Product/Component	Part Number
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

Table 16: 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
Supported Supervisor	
Cisco Nexus 7000 Supervisor 1 Module	N7K-SUP1
Cisco Nexus 7000 Supervisor 2 Module	N7K-SUP2

Product/Component	Part Number
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
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

Product/Component	Part Number
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

Table 17: 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

Table 18: 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=

Product/Component	Part Number
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

Table 19: 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

Table 20: 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

Product/Component	Part Number
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

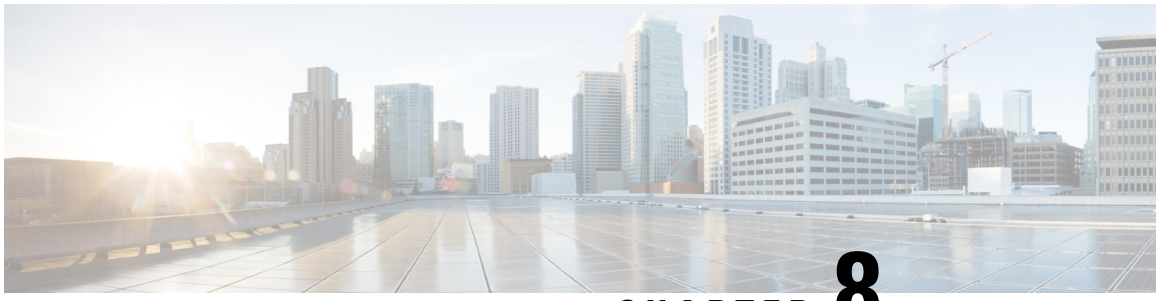
Table 21: Cisco Nexus 2000 Series Fabric Extenders

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

Product/Component	Part Number
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 11.3(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 11.3(1).

Caveat ID Number	Description
CSCvk03946	LAN Fabric: auto-populated dot1q release doesnt happen if its edited with used value and cancelled
CSCvk19306	LAN Fabric: FEX will show up in fabric builder topology even if cleaned up
CSCvk22938	SAN Insight ES-DB Spike in IOPS at Midnight
CSCvn62682	DCNM SAN Client - Help content is empty on IE and Chrome browsers
CSCvn74546	EPL: Download of operational heatmap endpoints not working with Mozilla browser
CSCvo62346	Error Configure or Unconfigure interface speed command
CSCvo77421	Special handling for Nxapi http port 80 upgrade from nxos.7.0.3.I7.5a -> 7.0.3.I7.6
CSCvp07873	Caveats when adding device via bootstrap with AAA authentication
CSCvp31098	ECT Analysis with specific search criteria and last goto 'trend identifier' back lose user selection
CSCvp43643	"Outlier detection" page n back to ECT Analysis w specific search criteria loses user selection
CSCvp75809	Seen TCAM config missing after ascii replay while write-erase/reload on T2 N9504
CSCvp85964	Change of scope in tabular view and moving to topology view doesn't display vPC pairing on GUI
CSCvp89323	Custom Graphing: With multiple graphs removing all filters on top graph removes all the graphs
CSCvp95425	VRF profile refresh fails when per vrf freeform configs are overlapping with profile configs
CSCvp95679	Compute role not vislble on bare-metal servers with 64BG memory
CSCvp96078	Watchtower:Service Utility page, Broker graph gets cleared
CSCvp99625	Handling the case sensitive names after brownfield upgrade from DCNM11.1 to 11.2
CSCvq01433	Post upgrade: Unable to edit network templates after L2-L3 network change
CSCvq02185	Undeploy migrated network status shows OOS on Network page and FB topology page for the network
CSCvq03395	Real time job failing for default vrf for group level jobs
CSCvq08970	Unable to modify the repeat interval for created archive jobs
CSCvq21119	Swap followed by submit when using Host to Host option with VXLAN OAM causes page to hang
CSCvq61767	\" is getting replaced by " and \ is getting removed during template save

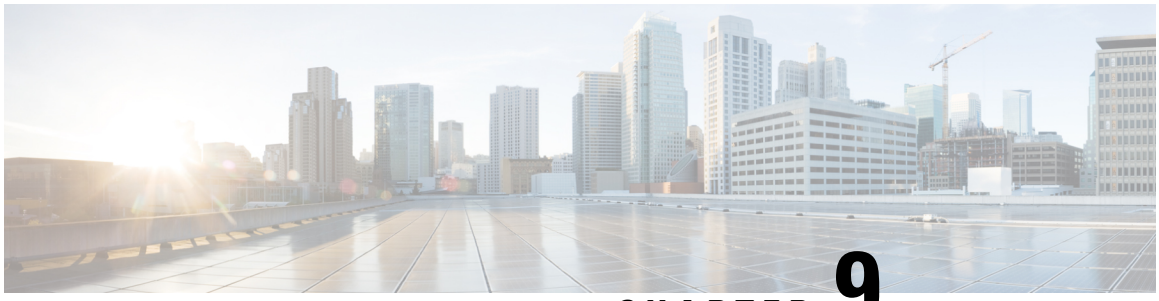
Caveat ID Number	Description
CSCvs20230	L1 page counts are wrong
CSCvs31542	After vpc link shut, dual attached counts does not move to single attached.
CSCvs31657	Removing a fabric with endpoints and re adding it with no endpoints show endpoints for 10min
CSCvs45655	CC diffs for cli system routing template-vxlan-scale on switch upg 7.0(3).I4(8b) -> 7.0.3.I7(6)
CSCvs45727	PBR stats not shown on DCNM L4-L7 service GUI with switch image nxos 9.2.2

Open Caveats

The following table lists the Open bugs for Cisco DCNM, Release 11.3(1).

Caveat ID Number	Description
CSCvm90923	SAN Insight: Display warning upon configuring different query types on switches in the same fabric
CSCvn36807	LAN Fabric: Unable to import switch via bootstrap due to inadvertent assignment of ip address
CSCvr27504	After removing of the port channel member from L3-port channel its not reflected in the GUI
CSCvr28767	On attaching multiple networks to same interface, the interface diff gets aggregated to single N/W
CSCvs19617	Pending config API giving 0 line diff in case of freeform restore
CSCvs26334	Undeploy of TRM-enabled VRFs fails post-brownfield migration
CSCvs26355	[FSV-sim] FHR discovery fails, sim connection failure
CSCvs28595	Mcast v4/v6 multipath config gets negated after first deploy
CSCvs31710	Incomplete deployment of service network vlan
CSCvs31986	In EPL application data downloads are not in 'csv' format.
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

Caveat ID Number	Description
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.
CSCvv35543	DCNM post-install IP address change - leaving AMQP server address unchanged



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 11.3(1) Documentation Roadmap

Table 22: Cisco DCNM 11.3(1) Documentation

Document Title	Description
Cisco DCNM Release Notes, Release 11.3(1)	Provides information about the Cisco DCNM software release, open caveats, and workaround information.
Cisco DCNM Compatibility Matrix, Release 11.3(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 11.3(1)	Lists the supported scalability parameters for Cisco DCNM, Release 11.3(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 11.3(1) • Cisco DCNM Media Controller Configuration, Release 11.3(1) • Cisco DCNM Classic LAN Configuration, Release 11.3(1) • Cisco DCNM SAN Management Configuration Guide, Release 11.3(1) • Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide, Release 11.3(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 Classic LAN Deployment, Release 11.3(1) • Cisco DCNM Installation Guide for Media Controller Deployment, Release 11.3(1) • Cisco DCNM Installation Guide for LAN Fabric Management Deployment, Release 11.3(1) • Cisco DCNM Installation and Upgrade Guide for SAN Deployment, Release 11.3(1)
Cisco DCNM Licensing Guide, Release 11.3(1)	Describes the procedure used to generate, install, and assign a Cisco Data Center Network Manager (DCNM) license.
Software Upgrade Matrix for Cisco DCNM 11.3(1)	Lists the software upgrade paths that are supported for DCNM.
Cisco Data Center Network Manager Open Source Licensing, Release 11.3(1)	Provides information about the Cisco Data Center Network Manager Open Source Licensing, Release 11.3(1).
Cisco DCNM REST API Guide, Release 11.3(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).

Document Title	Description
Videos: Cisco Data Center Network Manager, Release 11.3(1)	Lists all the videos created for Cisco DCNM 11.3(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.