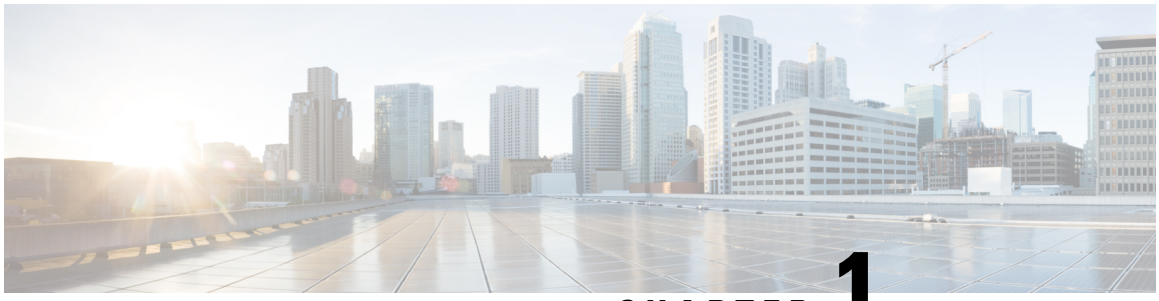
Cisco DCNM Release Notes, Release 11.2(1)

First Published: 2019-06-19

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 of Cisco DCNM

Cisco Data Center Network Manager (DCNM) is the comprehensive management solution for all NX-OS network deployments spanning LAN fabric, LAN Classic, SAN fabrics, and IP Fabric for Media (IPFM) networks in data centers powered by Cisco. Cisco DCNM 11 automates Cisco Nexus and Cisco MDS Family infrastructure for data center management across Cisco Nexus 1000, 2000, 3000, 5000, 6000, 7000, and 9000 Series Switches in NX-OS mode. Cisco DCNM 11 lets you manage large numbers 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 11.2(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 https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-data-center-network-manager/tsd-products-support-series-home.html and click **Download Software**.

Deployment of VXLAN EVPN Fabrics Using Cisco DCNM 11.2(1):

- **Greenfield Deployments**: Applicable for provisioning new VXLAN EVPN fabrics
- **Brownfield Deployments**: Applicable for existing VXLAN EVPN fabrics:
  - Migration of NFM fabrics to DCNM 11.3 using the `Easy_Fabric_11_1` fabric template is supported.

    Post DCNM upgrade, fabrics using the `NFM_Fabric` fabric template can be moved to the `Easy_Fabric_11_1` template.
  - Migrate CLI configured VXLAN EVPN fabrics to DCNM
- **Upgrades**: Applicable for VXLAN EVPN fabrics created with previous DCNM versions
  - Upgrade for VXLAN fabrics built with DCNM 11.0(1) to DCNM 11.2(1)
  - Upgrade for VXLAN fabrics built with DCNM 11.1(1) to DCNM 11.2(1)

Refer to the *Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.2(1)*.

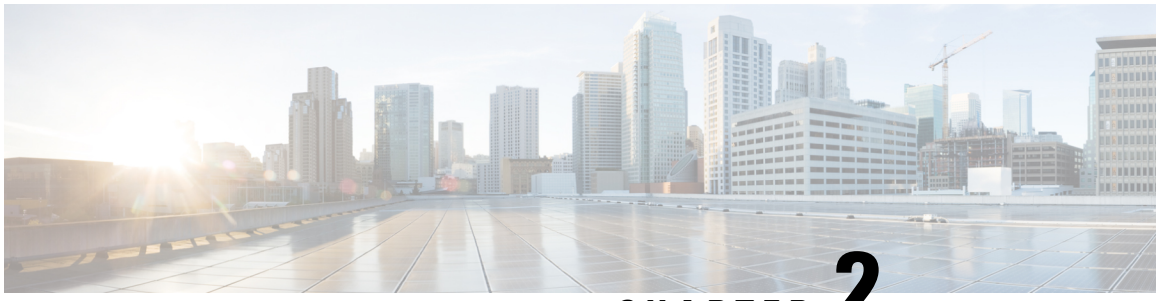
Note Cisco DCNM Classic LAN deployment can also be managed, monitored, automated, and controlled via the Cisco DCNM 11.2(1) LAN Fabric installation using **External Fabrics**. For more information, please refer to the External Fabrics in the *Cisco DCNM LAN Fabric Configuration Guide*.

This document provides the Release Notes for Cisco DCNM, Release 11.2(1). Use this document with the documents that are listed in the Related Documentation, on page 39.

The following table shows the change history for this document.

Table 1: Change History

Date	Description
20 June 2019	Published Release Notes for Cisco DCNM Release 11.2(1) - SAN deployment
06 June 2019	Published Release Notes for Cisco DCNM Release 11.2(1) - Classic LAN, LAN Fabric and IP Fabric for Media deployments



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 for Cisco DCNM

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 11.2(1).

Java Requirements

The Cisco DCNM Server is distributed with JRE 1.8.0_201 into the following directory:

```
DCNM_root_directory/java/jre1.8
```

Server Requirements

Cisco DCNM, Release 11.2(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, and 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 11.2(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 11.2(1) does not support the Oracle 12c pluggable database version installation.

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

Note The ISO/OVA installation only supports the embedded PostgreSQL database.

Note The Cisco DCNM database size is not limited. 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.

Cisco DCNM Release 11.2(1) 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-vCPU Cores with Cisco hardware RAID Controller [UCSC-MRAID12G-1GB/2 GB] for the RAID operation (small)
Cisco UCS C240M4	UCSC-C240-M4L	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count [1]
		[UCSC-MRAID12G- GB/2 GB] for the RAID operation (large)
Cisco UCS C240 M5S	UCSC-C240-M5SX	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for the RAID operation (small)
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for the RAID operation (small)

[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.

Note Cisco DCNM can work on an alternative computing hardware as well, despite Cisco is only testing on Cisco UCS.

Note Only Warm and Cold VMware snapshot is supported.

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

Supported Hypervisors

Cisco DCNM Release 11.2(1) supports the running of the Cisco DCNM Server on the following hypervisors, for DCNM LAN Fabric and DCNM LAN Classic Deployments:

Table 2: Cisco DCNM Redhat KVM Support for DCNM LAN Fabric and DCNM LAN Classic Deployments

Installation Mode	Hypervisor
DCNM LAN Fabric	Red Hat Enterprise Linux 7.6 with KVM
DCNM Classic LAN	Red Hat Enterprise Linux 7.4

Table 3: VMware Snapshot Support for DCNM LAN Fabric and DCNM LAN Classic Deployments

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 update 1

VMware vCenter Server	6.0	6.5	6.7	6.7 update 1

Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Compute
SAN	Windows, Linux (standalone or VM)	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs **Note** Standalone functioning of SAN Insights requires 28 vCPUs. RAM: 128 GB RAM(with SAN Insights) or 32 GB (without SAN Insights) DISK: 10 TB Disk (with SAN Insights) or 500 GB (without 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	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: 16 vCPUs RAM: 64 GB DISK: 500 GB

Note

- Cisco DCNM Small deployments does not support SAN Insights feature.
- You can use the SAN Insights feature on a medium-sized deployment with 2 TB disk space as well.
- Every Federation node must consists of 3 Large configuration nodes.
- From Cisco DCNM Release 11.2(1), you must 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 4: 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 74.0.3729.13
- Mozilla Firefox Version 66.0.4 (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 11.2(1).

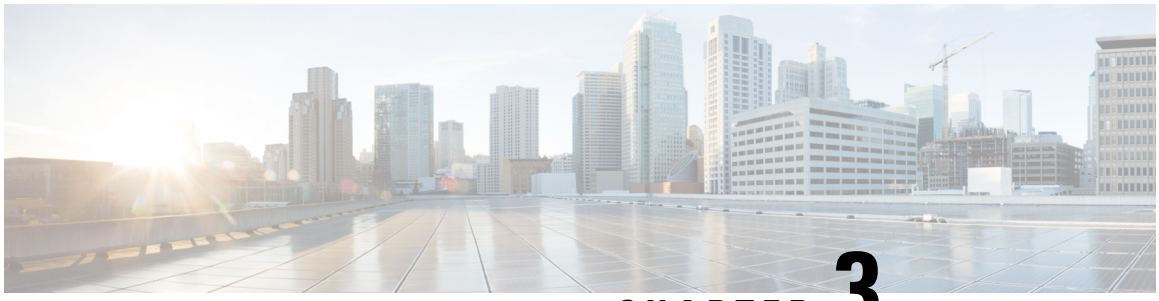
Table 5: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8. • 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
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.

Cisco DCNM Supported Scale Parameters

For more information about the Cisco DCNM Supported Scale Parameters, the see the Cisco DCNM Scalability Guide, Release 11.2(1).



CHAPTER 3

Guidelines and Limitations

Guidelines and Limitations

This section lists guidelines and limitations that are related to the Cisco DCNM Release 11.2(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 or MDS-managed platform. For information about licensing, see the Cisco DCNM Licensing Guide, Release 11.x.
- Depending on how a switch handles the **cdp enable** CLI command (enabled or disabled by default), Cisco DCNM shows this as config difference, although the Save and Deploy operation is performed to correct it. This depends on the default behavior of the switch image (that is, whether the **show running-config** shows the CLI or not). To address this issue, the respective policy template that is applied on the interfaces must be updated, so that the CLI is ignored during the configuration compliance check.
- Create a free-form configuration on all the white box switches that are managed by Cisco DCNM as shown below, and deploy them on all the switches before the final Save and Deploy operation.

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

  This is only applicable to the Cisco DCNM LAN Fabric mode.
- On Microsoft Windows 2016 Standard server, run the Cisco DCNM installation EXE file as an administrator. Cisco DCNM installation will not start on Microsoft Windows 2016 Standard server unless

you set the EXE file as an administrator. To start the installation EXE file, you can right-click on the EXE file, and choose **Run as administrator**.

- When the Cisco Nexus 9000v Virtual Switches are cloned, they may use the same serial number. Since Cisco DCNM discovers them using the same serial number, the device discovery operation fails.
- Addition of FEX or breakout of interfaces is not supported in External Fabrics.
- From Release 11.2(1), you can configure IPv6 address for Network Management for compute clusters. However, DCNM does not support IPv6 address for containers and must connect to DCNM using IPv4 address only.
- You cannot access the Cisco DCNM Web UI, when the user system is configured with the same IP address range as that of internal subnet used by the Application Framework in DCNM. For more information, see *Cisco DCNM Troubleshooting Guide*.
- The VXLAN OAM feature in Cisco DCNM is only supported on a single fabric or site.
- You cannot configure ICAM on the Cisco Nexus 9000 Series Switches Release 7.0(3)I7(6), and therefore, the telemetry will fail until the switch issue is resolved.
- Though you can delete PMN hosts, we recommended that you use this option with extreme caution, understanding that manual effort is needed to bring the solution back in sync.
- Cisco DCNM in Media Controller Deployment Release 11.x does not support non-default VRFs for Cisco Nexus 9000 Release 9.3(x).
- From Cisco DCNM Release 11.2(1), the Device Connector allows you to change the access mode via the Web UI at **Administration > DCNM Server > Device Connector > Settings > General**. The Cisco Intersight will not configure its device connector, and therefore, the Read-Only and Allow Control access mode in the Device Connector are not operational.
- Cisco DCNM does not support hot snapshots. While taking snapshots, we recommend that you power off the VM. Otherwise, ensure that you uncheck the **Snapshot the virtual machine's memory** option.
- Cisco DCNM does not support suspending or unsuspending of the VMs.
- Do not install NIR on standalone DCNM
- If NIR was installed and stopped, it does not stop service containers running on DCNM compute nodes.

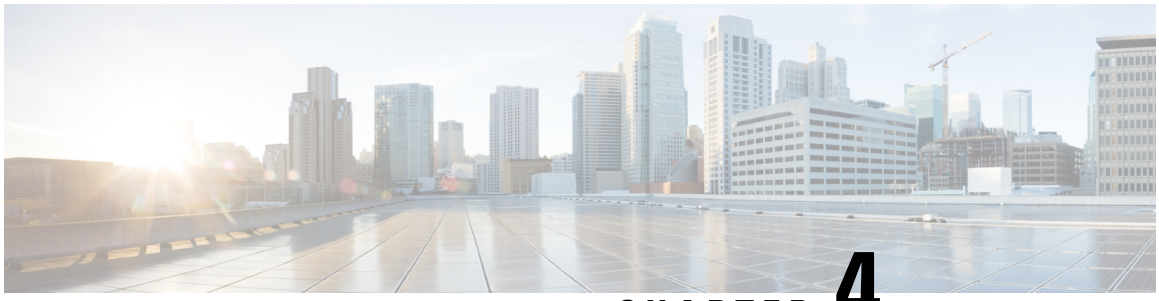
  If the NIR application is deleted from DCNM, a few service containers continues to run DCNM compute nodes and must be stopped manually using **afw service** commands.
- When DCNM Tracker is enabled, the NIR LAN Telemetry feature in Managed mode and the EPL feature with the **Configure my Fabric** option 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.
- 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 6: 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.



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 11.2(1)

This section includes information about the new features, enhancements, and hardware support for the Cisco DCNM Release 11.2(1).

vPC Fabric Peering

This feature is available on Cisco DCNM for LAN Fabric Deployment.

Cisco DCNM supports one click vPC pairing for traditional vPC deployments that employ a physical peer link and vPC fabric peering option. vPC fabric peering allows two switches in a VXLAN EVPN fabric to be configured as a vPC pair, without using a physical peer link. This feature is supported only with the NX-OS 9.2(3) release, on selected platforms. For supported Nexus Switches, see *Cisco Nexus 9000 Configuration Guide*.

Easy Fabric for eBGP Routed Fabrics with Optional EVPN Peering

This feature is available on Cisco DCNM for LAN Fabric Deployment.

A new fabric template **Easy_Fabric_eBGP** is available for support of spine-leaf based routed fabrics. In the fabric built with this template, eBGP is used as the routing protocol for the underlay connectivity between the spine-leaf network. This fabric supports the following 2 fabric types:

- The eBGP Routed Fabric provides IP connectivity and has no overlay support. The roles that are supported in this fabric are leaf, spine, and border. This is to support traditional MSDC network deployments.
- A VXLAN EVPN based fabric that employs eBGP for the underlay connectivity and eBGP EVPN for overlay peering. This fabric supports all the features of a traditional VXLAN EVPN based Easy fabric other than EVPN Multi-Site.

Brownfield Migration Enhancements

This feature is available on Cisco DCNM for LAN Fabric Deployment.

Cisco DCNM supports the following enhancements for the VXLAN EVPN based Brownfield migration:

- Switches with the Cisco NX-OS Release 7.0(3)I4(8b) and higher images.
- Tenant Routed Multicast (TRM) feature as the fabric overlay multicast protocol.
- Border Spine and Border Gateway Spine roles.
- BGP, OSPF, and ISIS authentication.
- Brownfield migration of VXLAN EVPN fabrics created via the bottom-up auto-configuration deployment method, into Easy fabrics managed via the fabric builder.

  After the migration, the Cisco DCNM can manage the fabric underlay and overlay networks.
- Bidirectional-PIM (bidir-PIM) feature is supported for the Brownfield migration. The **bidir** mode supports up to 2 rendezvous points (RP).
- During the brownfield migration, the overlay config-profiles are deployed to the switches, and the original configuration CLIs are removed if the switches in the brownfield migration have the following Cisco NX-OS images:
  - Cisco NX-OS Release 7.0(3)I7(6) or later
  - Cisco NX-OS Release 9.2(3) or later

Note If the switches do not meet these NX-OS release requirements, the brownfield migration behavior is same as the Cisco DCNM Release 11.1(1).

Compute Node for OVA and ISO Installation Modes

This feature is available on Cisco DCNM for LAN Fabric, and Classic LAN Deployments. This feature is not available for IPFM installations.

From Cisco DCNM Release 11.2(1), you can install a Cisco DCNM Compute node using an ISO or OVA of a regular Cisco DCNM image. It can be deployed directly on a bare metal using an ISO or a VM using the OVA. During the OVA/ISO installation, select **Compute** as the choice for installing of the compute node. The web installer works in a similar manner to complete the installation process. On a Compute node, you will not find DCNM processes or Postgres database; it runs a minimum set of services that are required to provision and monitor applications.

The specifications of the compute node must be minimum of 16 vCPUs, 64G RAM, 500G hard disk. To install a compute node, see *Cisco DCNM Installation Guide* for your deployment type.

App Center Based Application Delivery

This feature is available on Cisco DCNM for LAN Fabric, and Classic LAN Deployments.

Cisco DCNM allows you to download applications from the corresponding Cisco App Center. Applications such as Network Insights Resources (NIR) and Network Insights Advisor (NIA) are available for the Cisco

DCNM OVA/ISO install modes. For more information about the Network Insights Applications, see Cisco Network Insights for Data Center.

Note You must enable Compute Cluster before installing the applications. The applications that are installed via the Cisco App Center will not work if the compute cluster is configured after installing the applications.

For instructions about compute clusters, refer to the *Applications* chapter in the *Cisco DCNM Configuration Guides* for your Cisco DCNM Deployment type.

Save and Deploy Enhancements

This feature is available on Cisco DCNM for LAN Fabric Deployment.

The pending and side-by-side comparison tabs in the **Config Preview** window are enhanced. The side-by-side comparison tab shows the comparison between Running Configuration and Intent Configuration with leading space indentations, which signify the configuration hierarchy.

External DHCP Server for Bootstrap

This feature is available on Cisco DCNM for LAN Fabric Deployment.

In addition to the local DHCP server, Cisco DCNM provides support for an external DHCP server for bootstrap or automated day-0 bring-up of switches.

DHCP Multi-Subnet Scope

This feature is available on Cisco DCNM for LAN Fabric Deployment.

For bootstrap or automated day-0 bring-up of switches in a fabric, when using the local DHCP server, DCNM now supports multiple DHCP subnet scopes within a given fabric with the bootstrap option. This allows switches in different racks within a fabric to be in different layer-3 IP subnets. You can specify one subnet scope per line in a text box for DHCP Multi-Subnet Scope. You can add multi-subnets if the Local DHCP server is enabled.

Config Archive Enhancements

This feature is available on Cisco DCNM for Classic LAN Deployment.

From Cisco DCNM Release 11.2(1), while creating jobs on **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs > Add Job**, you can apply VRFs for all the selected devices simultaneously. You can either apply the Management VRF or Default VRF.

You can also modify the VRF type while modifying the Job.

IPv6 Support for Event and Alarm Forwarding Destination

This feature is available on Cisco DCNM for LAN Fabric Deployment and Cisco DCNM Classic LAN Deployment.

When you install Cisco DCNM, you can optionally provide an IPv6 address while configuring the management settings, which is for the eth0 interface. You can access the Cisco DCNM Web UI using the specified IPv6 address. You can also specify an IPv6 destination address for Event Forwarding and Alarm Forwarding.

CSR1kv Support

Note This is a preview only feature. We recommend that you use this feature only in Lab setups, and not in production environments.

This preview functionality allows cloud connectivity from a Cisco DCNM provisioned VXLAN EVPN fabric to the Microsoft Azure public cloud. Layer-3 connectivity is provided, so that workloads on-premise can seamlessly and securely communicated with workloads in the Azure cloud. The connectivity is provisioned via the Cisco Cloud Services Router 1000v Series that is managed by Cisco DCNM. VXLAN EVPN is employed for the control plane and VXLAN is employed for the data plane. Both the control plane and the data plane are established over an IPsec tunnel.

SAN Insights Enhancements

This feature is available on Cisco DCNM for SAN Deployment, only.

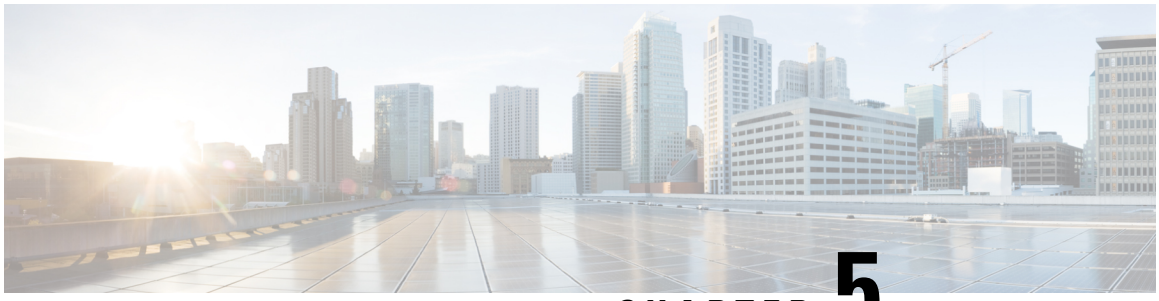
Cisco DCNM supports the following enhancements for SAN insights feature:

- Compact GBP transport for better I/O performance and improved San Insight scalability.
- From Cisco MDS NX-OS Release 8.4(1), SAN insights is supported on the following switches:
  - 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)

Support for New Cisco MDS Hardware

Cisco DCNM 11.2(1) supports the following new Cisco MDS hardware.

Product / Component	Part Number
Supervisor Module 4 for NextGen MDS Director Switch	DS-X97-SF4-K9
FabricModule for MDS 6-Slot Director Switch D9706	DS-X9706-FAB3
FabricModule for MDS 10-Slot Director Switch D9710	DS-X9710-FAB3



CHAPTER 5

Upgrading Cisco DCNM

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

Upgrading the Cisco DCNM

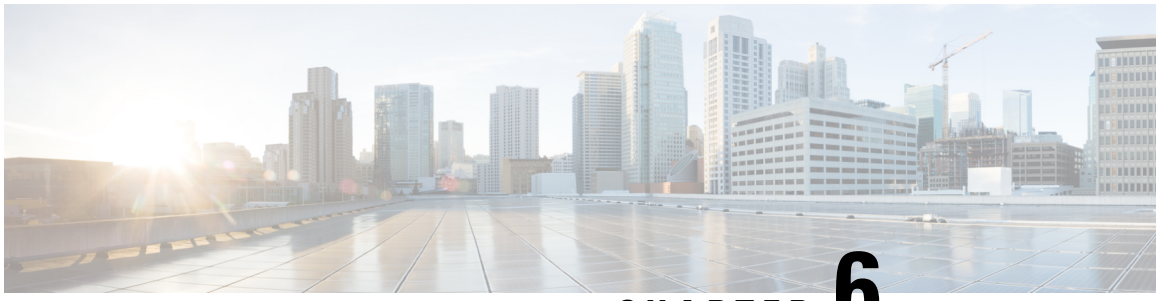
Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM 11.0(1), OVA, and ISO does not ship with SAN support.

You can upgrade to the Cisco DCNM Release 11.2(1) from DCNM Release 11.0(1) and 11.1(1) only. For instructions, refer to *Cisco DCNM Installation Guides*.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.2(1).

Table 7: Type of Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.2(1)
11.1(1)	Inline Upgrade
11.0(1)	Inline Upgrade
10.4(2)	**1.** Upgrade to 11.0(1) or 11.1(1) using the DCNMUpgradeTool. **2.** Inline Upgrade from 11.0(1) or 11.1(1) to 11.2(1)



CHAPTER 6

Supported Cisco Platforms and Software Versions

Compatibility Matrix for Cisco DCNM, Release 11.2(1)

The below table shows the Cisco DCNM Compatibility Matrix for Release 11.2(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 11.2(1)

Cisco MDS 9100	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	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(8h), 5.2(8c), 5.2(8d), 5.2(8e), 5.2(8f), 5, 2(8g)
Cisco MDS 9300	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	6.2(29), 6.2(27), 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	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	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)I2.2a, 7.0(3)I2.1, 7.0(3)I1.3, 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(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	8.4(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(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(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	9.2(4), 9.3(1), 9.2(3), 9.2(2)

Cisco Nexus 3500 Series	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 3100 Series	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	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 11.2(1)

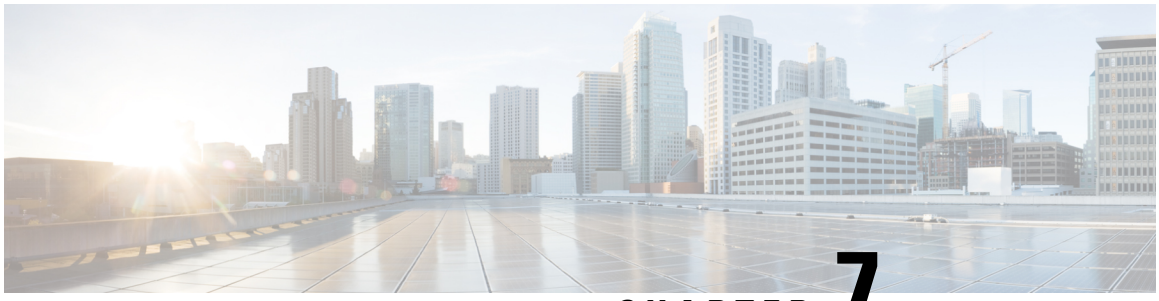
Installation Type	Switch Versions
LAN Classic	See Table 8: Compatibility Matrix for Cisco DCNM, Release 11.2(1).

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(2), 7.0(3)I7(6)* • External Fabric N3000/3100/3500 (External_Fabric_11_1): 7.0(3)I7(6)* • External Fabric N3600 (External_Fabric_11_1): 9.2(3) • External Fabric N5000/5600/6000 (External_Fabric_11_1): 7.3(5)N1(1)* • External Fabric N7000/7700 (External_Fabric_11_1): 7.3(3)D1(1)*, 8.2(3)* • External Fabric N9000 (External_Fabric_11_1): 9.2(3), 9.2(2), 7.0(3)I7(6)* • Migrating NFM-managed VXLAN fabric to DCNM (Easy_Fabric_11_1): 7.0(3)I7(6)* • Migrating Switch Command line configured VXLAN fabrics to DCNM (Easy_Fabric_11_1): 9.2(2), 7.0(3)I7(6)*, 7.0(3)I7(5a), 7.0(3)I4(9), 7.0(3)I4(8b)
IP Fabric for Media (IPFM)	9.3(2), 9.3(1), and 9.2(3)
SAN	See the SAN supported switches in Table 8: Compatibility Matrix for Cisco DCNM, Release 11.2(1).

*Indicates the recommended NX-OS version

Interoperability Matrix for Cisco Nexus and MDS 9000 Products

For Cisco DCNM Connect Support, see the Interoperability Matrix for Cisco Nexus and MDS 9000 Products.



CHAPTER 7

Supported Hardware

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

• Hardware Supported in Cisco DCNM, Release 11.2(1), on page 23

Hardware Supported in Cisco DCNM, Release 11.2(1)

In a LAN Fabric installation of Cisco DCNM 11.2(1), the Cisco Nexus 9000, and Nexus 3000 switches are supported for VXLAN EVPN fabric provisioning in Easy Fabrics. The specific Cisco Nexus 3000 models that are supported are:

- Cisco Nexus3636C-R
- Cisco Nexus36180YC-R

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 11.2(1).

Table 10: 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

Product/Component	Part Number
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 11: Cisco MDS 9000 Family

Product/Component	Part Number
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 9132U 1RU Switch 32x32G-FC	DS-C9132U

Table 12: 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 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	
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 13: Cisco Nexus 7000 Series Switches

Product/Component	Part Number
Supported Chassis	
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
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

Product/Component	Part Number
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
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 14: 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

Product/Component	Part Number
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 15: Cisco Nexus 5000 Series Switches

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

Product/Component	Part Number
16-port Universal GEM, Cisco Nexus 5500	N5K-M16UP
Version 2, Layer 3 daughter card	N55-D160L3-V2

Table 16: 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 17: Cisco Nexus 3000 Series Switches

Product/Component	Part Number
1RU 48 x SFP+/SFP28 and 6 x QSFP+/QSFP28	N3K-C34180YC
1RU 32 Port QSFP28 10/25/40/50/100 Gbps	N3K-C3132C-Z
Nexus 3548-XL Switch, 48 SFP+	N3K-C3548P-XL
Nexus 3264C-E switch with 64 QSFP28	N3K-C3264C-E
Cisco Nexus 3132Q Switch	N3K-C3132C-Z
Cisco Nexus 3132Q-V Switch	N3K-C3132Q-V
Nexus 34180YC programmable switch, 48 10/25G SFP, and 6 40/100G QSFP28 ports	N3K-C34180YC
Cisco Nexus 3464C Switch, 64 x QSFP+/QSFP28 ports and 2 x SFP+	N3K-C3464C
Cisco Nexus 3016 Switch	N3K-C3016Q-40GE
Cisco Nexus 3048 Switch	N3K-C3048TP-1GE
Cisco Nexus 3064-E Switch	N3K-C3064PQ-10GE
Cisco Nexus 3064-X Switch	N3K-C3064PQ-10GX
Cisco Nexus 3064-T Switch	N3K-C3064TQ-10GT
Nexus 31108PC-V, 48 SFP+ and 6 QSFP28 ports	N3K-C31108PC-V
Nexus 31108TC-V, 48 10GBase-T RJ-45, and 6 QSFP28 ports	N3K-C31108TC-V
Cisco Nexus 3132Q Switch	N3K-C3132Q-40GE
Nexus 3132 Chassis	N3K-C3132Q-40GX
Cisco Nexus 3172PQ Switch	N3K-C3172PQ-10GE
Cisco Nexus 3548 Switch	N3K-C3548P-10G

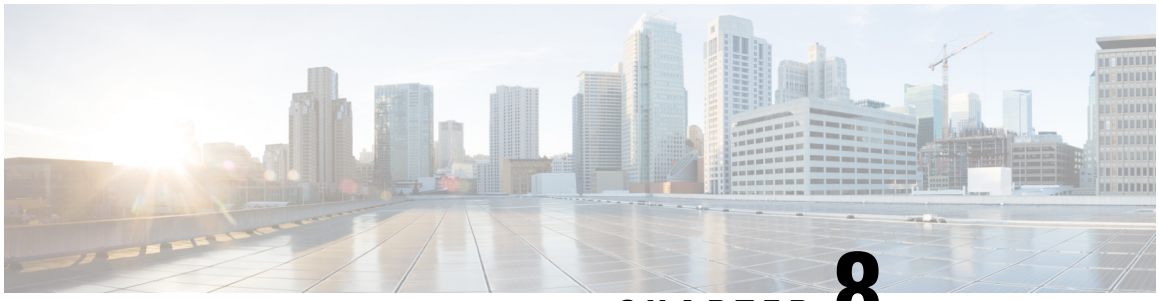
Product/Component	Part Number
Cisco Nexus 3636C-R Switch	N3K-C3636C-R

Table 18: Cisco Nexus 2000 Series Fabric Extenders

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

IBM Directors and switches supported in Cisco DCNM 11.2(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, perform the following task:

- 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 11.2(1).

Caveat ID Number	Description
CSCvk11305	LAN Fabric: Fail to change channel mode if po has > 1 member
CSCvk21156	Scale: Outlier detection gets stuck in loading the scatter plot. Needs multiple waits to load data.
CSCvm05536	LAN Fabric: BGP neighbors not detected on leaf switches after NXOS image upgrade
CSCvm62784	DCNM SAN Client gets timeout error when enabling FC-SP on ISLs between 2 9700s
CSCvm62784	Cisco DCNM SAN Client gets timeout error when enabling FC-SP on ISLs between two Cisco MDS 9700 series switches
CSCvn52673	LAN Fabric: After Brownfield migration, Refresh L2 / L3 migrated networks does not seem to work
CSCvn55041	LAN Fabric: BROWNFIELD Spine switches get out of migration mode with some diff after Save&Deploy
CSCvn58071	LAN Fabric: TRM Flooding occurs in fabric resulting from missing BGP peers between BorderSpine nodes
CSCvn64425	LAN Fabric: No diff if name-server is changed from default vrf to management vrf
CSCvn68148	when we delete and add Vcenter too qucik , VMM app is not running
CSCvn68243	LAN Fabric: vPC entry created with trunk_host policy should be deletable
CSCvn72577	LAN Fabric: Restore backup do not remove all freeform configs
CSCvn73214	No operational heat-map table visible after inline upgrade. (Aragon to Aragon MR S21)
CSCvn86194	Limit in UCS FI switch dashboard blades tab
CSCvn86194	Cisco DCNM Web Client does not show any blades in the switch dashboard blades tab if Cisco UCS has more than 16 blades.
CSCvn95975	LAN Fabric: Brownfield: Save and Deploy gets stuck when fabric has multiple of 10 devices
CSCvo64647	Cisco DCNM Arbitrary File Upload and Remote Code Execution Vulnerability

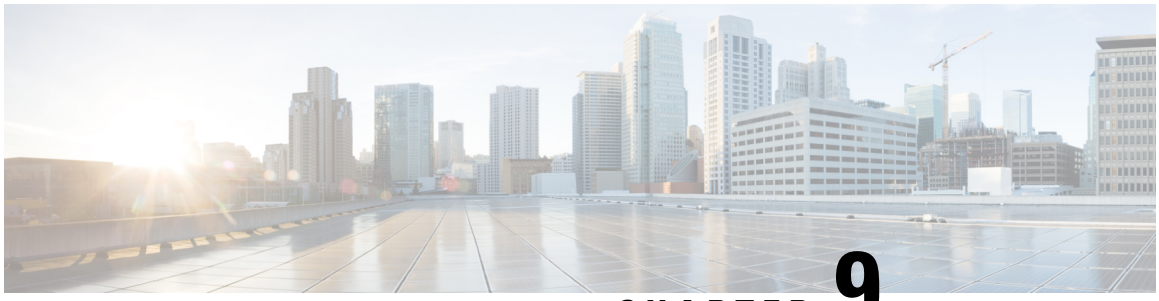
Open Caveats

The following table lists the Open bugs for Cisco DCNM, Release 11.2(1).

Caveat ID Number	Description
CSCvk03946	Auto-populated dot1q release does not happen if it is edited with used value and cancelled

Caveat ID Number	Description
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
CSCvm90923	SAN Insight: Display warning upon configuring different query types on switches in the same fabric
CSCvn24439	LAN Fabric: FEX GUI remains in topology & associated hif ports dangling in link page post deletion
CSCvn36807	LAN Fabric: Unable to import switch via bootstrap due to inadvertent assignment of ip address
CSCvn62682	DCNM SAN Client - Help content is empty on IE and Chrome browsers
CSCvn73161	when we click on the topology page, popup window appears 2 times
CSCvo62346	LAN Fabric: Error Configure or Unconfigure interface speed command
CSCvo77421	LAN Fabric: Special handling for Nxapi http port 80 upgrade from nxos.7.0.3.I7.5a -> 7.0.3.I7.6
CSCvo79169	Brownfield:Save&Deploy failed with error "Error reading the switch configurations"
CSCvo96834	ES-DB: stopping and starting telemetry with port-sampling enabled causes peak.
CSCvp07873	LAN Fabric: 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
CSCvp46574	Warning message is not thrown when feature nv overlay is pushed to N5600
CSCvp75809	LAN Fabric: Seen TCAM config missing after ascii replay while write-erase/reload on T2 N9504
CSCvp76165	VRF-Lite B2B IFC delete shows continuous diff for shut/no shut
CSCvp85964	Change of scope in tabular view and moving to topology view doesn't display vPC pairing on GUI
CSCvp88154	Monitor: Failures average value and Graph value are not similar - regression
CSCvp89323	Custom Graphing: With multiple graphs removing all filters on top graph removes all the graphs
CSCvp95679	Compute role not visible on bare-metal servers with 64BG memory
CSCvp96078	Watchtower:Service Utility page, Broker graph gets cleared
CSCvp97272	add DCNM term license for ACI device

Caveat ID Number	Description
CSCvp99625	LAN Fabric: Handling the case sensitive names after brownfield upgrade from DCNM11.1 to 11.2
CSCvq01047	DCNM/Network Insight Application reporting wrong TCAM utilization
CSCvq01063	Deletion of discovered VDC in external , Not updating the database entries - causes traceback
CSCvq01433	Post upgrade: Unable to edit network templates after L2-L3 network change
CSCvq02185	LAN Fabric: 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
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 11.2(1) Documentation Roadmap

Table 19: Cisco DCNM 11.2(1) Documentation

Document Title	Description
Cisco DCNM Release Notes, Release 11.2(1)	Provides information about the Cisco DCNM software release, open caveats, and workaround information.
Cisco DCNM Compatibility Matrix, Release 11.2(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 11.2(1)	Lists the supported scalability parameters for Cisco DCNM, Release 11.2(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 11.2(1) • Cisco DCNM Media Controller Configuration, Release 11.2(1) • Cisco DCNM Classic LAN Configuration, Release 11.2(1) • Cisco DCNM SAN Management Configuration Guide, Release 11.2(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 11.2(1) • Cisco DCNM Installation Guide for Media Controller Deployment, Release 11.2(1) • Cisco DCNM Installation Guide for LAN Fabric Management Deployment, Release 11.2(1) • Cisco DCNM Installation and Upgrade Guide for SAN Deployment, Release 11.2(1)
Cisco DCNM Licensing Guide, Release 11.2(1)	Describes the procedure used to generate, install, and assign a Cisco Data Center Network Manager (DCNM) license.
Software Upgrade Matrix for Cisco DCNM 11.2(1)	Lists the software upgrade paths that are supported for DCNM.
Cisco Data Center Network Manager Open Source Licensing, Release 11.2(1)	Provides information about the Cisco Data Center Network Manager Open Source Licensing, Release 11.2(1).
Cisco DCNM REST API Guide, Release 11.2(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	Lists all the videos created for Cisco DCNM 11.

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 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.