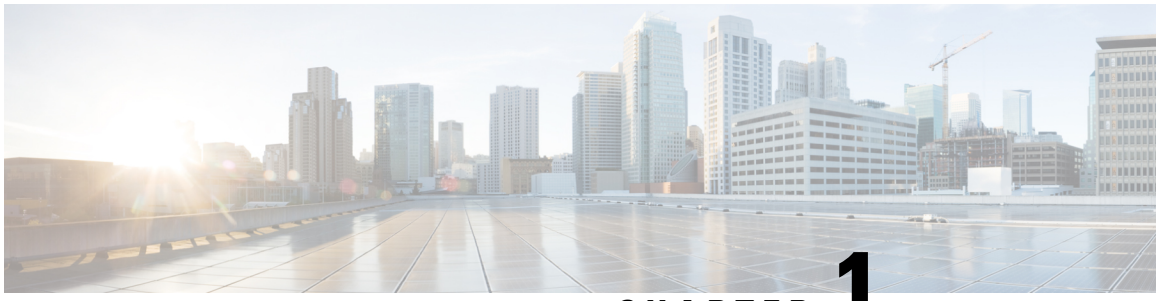
Cisco DCNM Release Notes, Release 11.5(3a)

First Published: 2021-10-30

Last Modified: 2021-10-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview

Overview

Cisco Data Center Network Manager (DCNM) is the comprehensive management solution for all NX-OS deployments spanning LAN Fabric, SAN, and IP Fabric for Media (IPFM) networks in data centers powered by Cisco. DCNM 11 automates Cisco MDS Switches and Cisco Nexus Family infrastructure, for data center management across Cisco Nexus 1000, 2000, 3000, 5000, 6000, 7000, and 9000 Series Switches in NX-OS mode. From Release 11.3(1), Cisco DCNM also supports non-Nexus devices, such as, IOS-XE, IOS-XR, and non-Cisco devices. DCNM 11 being a multi-fabric controller, it lets you manage many devices both legacy and new age fabric deployments simultaneously, while providing ready-to-use control, management, and automation capabilities for all these environments.

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

Note The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

DCNM Release 11.5(3a) supports LAN Fabric deployment only. For information about bugs fixed in this release, see Caveats, on page 17.

Note Cisco DCNM Release 11.5(3a) does not support fresh installation or upgrading DCNM Media Controller (IPFM) and SAN deployments.

Note You cannot upgrade to Release 11.5(3a). Only fresh installation is supported.

To download the Cisco DCNM software, go to Cisco DCNM Software Download, click **Download Software**.

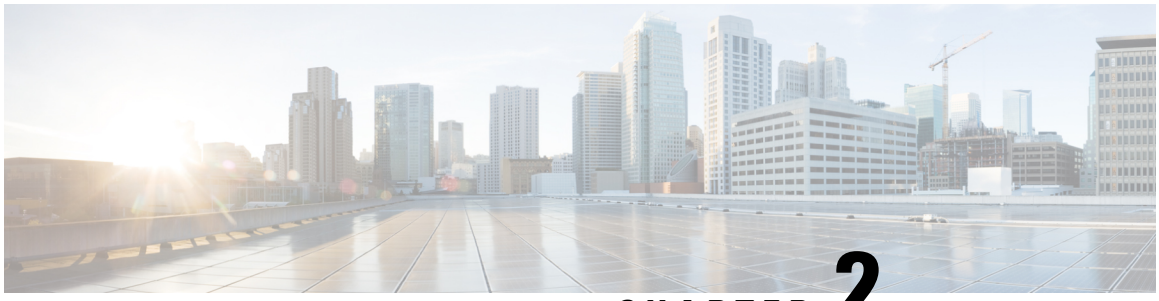
To install Cisco DCNM Release 11.5(3a) for LAN Fabric Deployment, refer to Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(3a).

This document provides the release notes for Cisco DCNM, Release 11.5(3a). Use this document with the documents that are listed in Related Documentation, on page 19.

The following table shows the change history for this document.

Table 1: Change History

Date	Description
31 October 2021	Published Release Notes for Cisco DCNM Release 11.5(3a)



CHAPTER 2

System Requirements

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

System Requirements

This section describes the various system requirements for proper functioning of your Cisco DCNM Release 11.5(3a).

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

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

Java Requirements

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

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM Release 11.5(3a), supports the Cisco DCNM server on these 64-bit operating systems:

- **LAN Fabric Deployments:**
  - Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.8
  - ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.8

Supported Latency

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

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

Database Requirements

Cisco DCNM Release 11.5(3a) supports the following databases:

- PostgreSQL 10.15 - For OVA/ISO deployments

Note The ISO and OVA installations support only the embedded PostgreSQL database.

Hypervisors

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

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

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count [1] [2]
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 OVA Compute node with 16 vCPUs, 64G RAM, and 500GB hard disk.
2 If you are deploying Network Insights applications on the Cisco DCNM Compute cluster, refer to the app-specific Release Notes for additional CPU/memory requirements for the Computes.

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

Supported Hypervisors

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

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

Server Resource (CPU/Memory) Requirements

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

Table 2: System Requirements for Cisco DCNM LAN Fabric Deployment

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

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

Allocate sufficient disk space to the root partition to complete DCNM installation and for stable continuous operation of the DCNM applications. Refer to the applications' User guides for disk space requirements. You can mount another disk where the `/tmp` directory can be mounted during the installation or upgrade. You can also add additional disk space and the disk file system using **appmgr system scan-disks-and-extend-fs** command.

Cisco DCNM LAN Fabric Deployment Without Network Insights (NI)

Table 3: Upto 80 Switches

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

Table 4: 81–350 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
DCNM on Applications Service Engine (SE)	ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	OVA/ISO	16 vCPUs	64G	500G HDD	3xNIC

VMware Snapshot Support for Cisco DCNM

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

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

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

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

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

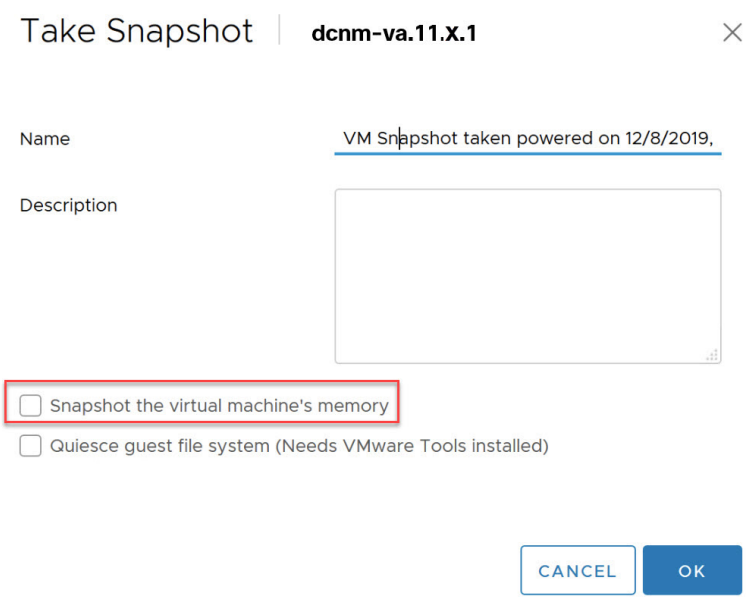
The following snapshots are available for VMs.

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

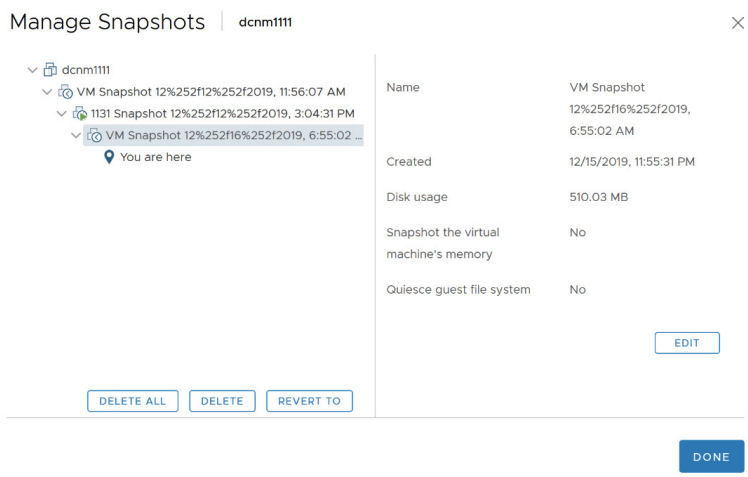
Note Cisco DCNM supports snapshots when VM is either powered on or powered off. DCNM doesn't support snapshots when the Virtual Machine memory option is selected.

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

System Requirements



You can restore VM to the state in a Snapshot.



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

Supported Web Browsers

Cisco DCNM supports the following web browsers:

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

Other Supported Software

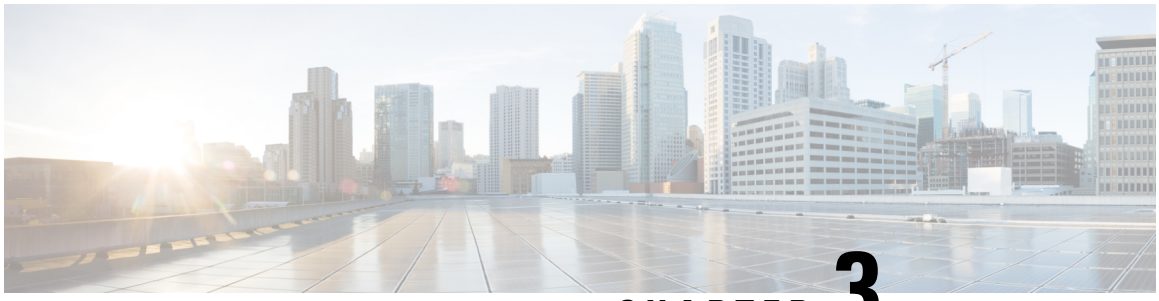
The following table lists the other software that is supported by Cisco DCNM Release 11.5(1).

Table 5: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • ISE version 3.0 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client Encryption: HTTPS with TLS 1, 1.1 and 1.2 • TLS 1.3
OVA\ISO Installers	CentOS 7.8/Linux Kernel 3.10.x

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

System Requirements



CHAPTER 3

Guidelines and Limitations

Guidelines and Limitations

- Ensure that you have installed Visual C++ Redistributable Packages for Visual Studio 2013 64 bit before installing or upgrading to Cisco DCNM Release 11.4(1).
- To check the status of the running Postgres database in Native HA setup, use **pg_ctl** command. Do not use the **systemctl** command.
- Do not begin the password with Hash (#) symbol. Cisco DCNM considers the password as an encrypted text if it begins with # symbol.
- Restoring DCNM with changes in IP addresses is not supported.
- **POAP Dynamic Breakout**—From Cisco NX-OS Release 7.0(3)I4(1), POAP dynamically breaks out ports to detect a DHCP server behind one of the broken-out ports. Previously, the DHCP server that is used for POAP was directly connected to a normal cable as the breakout cables were not supported. POAP determines which breakout map (for example, 10gx4, 50gx2, 25gx4, or 10gx2) brings up the link that is connected to the DHCP server. If breakout is not supported on any of the ports, POAP skips the dynamic breakout process. After the breakout loop completes, POAP proceeds with the DHCP discovery phase as normal.

  Cisco DCNM leverages the dynamic breakout to simplify the fabric setup by retaining successful breakout configuration. Since dynamic breakout requires the other side of the link to be active, there are circumstances where you must manually breakout interfaces, or may notice breakout in places which are not desired. In those situations, you must adjust the ports on the Interfaces page before performing Save and Deploy in the Fabric Builder.
- Before using the licensed features, install a Cisco DCNM license for each Nexus-managed or MDS-managed platform. For information about licensing, see the Cisco DCNM Licensing Guide, Release 11.x.
- Create a free-form configuration on all the white box switches that are managed by Cisco DCNM as shown below, and deploy them on all the switches before the final Save and Deploy operation.

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

  This is only applicable to the Cisco DCNM LAN Fabric mode.

- On Microsoft Windows 2016 Standard server, run the Cisco DCNM installation EXE file as an administrator. Cisco DCNM installation will not start on Microsoft Windows 2016 Standard server unless you set the EXE file as an administrator. To start the installation EXE file, you can right-click on the EXE file, and choose **Run as administrator**.
- When the Cisco Nexus 9000v Virtual Switches are cloned, they may use the same serial number. Since Cisco DCNM discovers them using the same serial number, the device discovery operation fails.
- You cannot access the Cisco DCNM Web UI, when the user system is configured with the same IP address range as that of internal subnet used by the Application Framework in DCNM. For more information, see *Cisco DCNM Troubleshooting Guide*.
- Though you can delete PMN hosts, we recommended that you use this option with extreme caution, understanding that manual effort is needed to bring the solution back in sync.
- Cisco DCNM in Media Controller Deployment Release 11.x does not support non-default VRFs for Cisco Nexus 9000 Release 9.3(x).
- Cisco DCNM does not support suspending or unsuspending of the VMs.
- If NIR was installed and stopped, it does not stop service containers running on DCNM compute nodes.

  If the NIR application is deleted from DCNM, a few service containers continue to run DCNM compute nodes and must be stopped manually using **afw service** commands.
- When NIR/NIA applications is enabled at higher scale, that is, with 250 switches and 10000 Hardware telemetry flows, DCNM Computes nodes must be connected on all eth0, eth1, and eth2 interfaces using a 10Gig link.
- For leaf-leaf ports in non-VPC cases, DCNM will always push the **shutdown** command. If you want to bring up the port, add the **no cdp enable** command to the interface freeform policy on one of the ports.

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

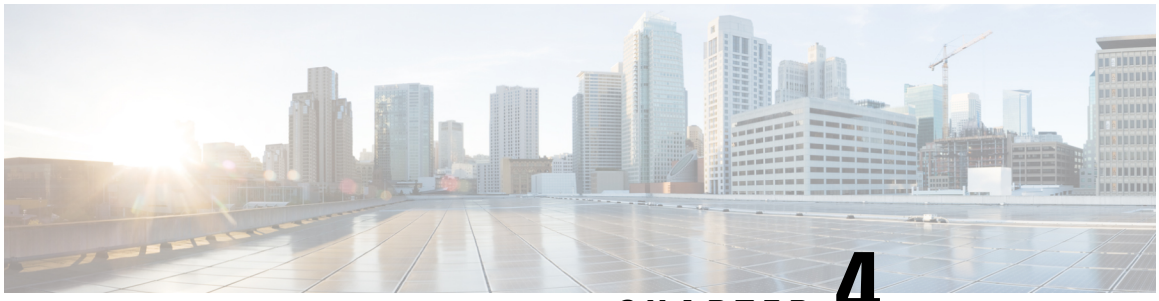
  To add route over the Inband Network in DCNM, on the Cisco DCNM Web UI, choose **Administration > Customzation > Network Preferences**. Enter the Routes to the ND Data Network over the In-band(eth2) inputs of the dashlet. For more information, see Network Preferences-Routes.
- From Release 11.4(1), Cisco DCNM does not support syncing fabric with switches in VTP server mode. For more information, refer to CSCvx86976.

- While upgrading from DCNM Release 11.5(1) to Release 11.5(4), if you try to retain when the CA-signed certificates, DCNM fails to launch. For more information, see CSCwb97942.
- In a DCNM managed by NDO, the MSD fabric backup is not restored completely. The MSD fabric is reverted to the time where the deployed networks created on NDO are not yet available. While the fabric shows as in sync in DCNM, there will be no configuration drift notifications in NDO.
- In Cisco DCNM SAN deployment, if the DCNM server streaming the SAN analytics is over-utilized, the Elasticsearch database service goes down. This results in performance issues. The Pipeline service may be consuming all the CPU and system resources on the Cisco DCNM server. To troubleshoot this, do the following task:
  1. Stop the Pipeline service.
  2. Reduce the streaming load from the MDS fabric.
  3. Start Elasticsearch service.
  4. Start the Pipeline service.
- From Cisco DCNM Release 11.5(2), VLAN range is extended. After patch update for LAN Fabric deployment, you can set VLAN range to 4094.
- In Cisco DCNM SAN deployment, when you enable or disable alarms on a Primary node, it will not be applied to all the nodes in the Federation. You must manually enable or disable alarms on all nodes on all servers in the Federation setup. You must restart the DCNM Server to apply the changes.
- In Cisco DCNM SAN deployment, when you modify the server properties on Cisco DCNM **Web UI > Administration > DCNM Server > Server Properties** on a Primary node, it will not be applied to all the nodes in the Federation. You must manually make the changes to the server properties on all nodes on all servers in the Federation setup. You must restart the DCNM Server to apply the changes.
- SAN Insights is best supported on Linux from Release 11.0(1), and on Cisco DCNM OVA/ISO deployments from Release 11.3(1).
- From Cisco DCNM Release 11.3(1), you cannot download the SAN Client package from the Software Downloads page. You must install Cisco DCNM, launch Web UI to download the SAN Client and Device Manager. For more information, *Cisco DCNM Installation and Upgrade Guide for SAN Deployment*.
- In Releases prior to 11.4, if you have installed a preview feature, perform the following before you upgrade to Release 11.4(1):
  - Remove the configuration from older release setup.
  - Reset the property to enable the preview feature. On the Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**. Reset the **enable preview feature** property.

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.
ifconfig ethx y.y.y.y/zz	Any change in the IP addresses of the DCNM nodes must be done with the **appmgr update network-properties** command. This includes changing the FQDN, adding static routes, adding/removing NTP servers etc.



CHAPTER 4

New Features and Enhancements

New Features and Enhancements

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

New Features and Enhancements in Cisco DCNM Release 11.5(3a)

These following sections include information about the new features, enhancements, and hardware support introduced in the Cisco DCNM Release 11.5(3a).

LAN Fabric Deployment Enhancements

The following features are new in Cisco DCNM Release 11.5(3a) for the LAN Fabric Deployment.

Inband POAP

DCNM Release 11.5(3a) allows you to enable Inband POAP for External Fabrics and LAN Classic fabrics. Inband POAP is supported with the DCNM internal packaged DHCP server or an external DHCP server. The Inband POAP selection is a per fabric knob. You can enable Out-of-band POAP on Easy Fabrics and simultaneously have Inband POAP enabled on other External/LAN Classic fabrics.

RMA for Pre-provisioned Switches (Serial Number Swap)

DCNM Release 11.5(3a) allows you to change serial numbers for pre-provisioned switches. You can build data center fabrics with dummy serial numbers including all underlay/overlay configurations. After the switch information is available, the serial number swap API is called to update the dummy serial numbers with actual serial numbers, so that the relevant configuration is pulled by the switches on boot-up for touchless provisioning.

While pre-provisioning devices, you can provide dummy values for the Serial number of the switch. After you configure the network successfully, DCNM Release 11.5(3a) provides a new API to swap the serial number with the correct serial number of the device. Launch APIs for DCNM using the following URL: https://%3Cdcnm-mgmt0-ip%3E/api-docs.

Navigate to **Control > Fabrics > swapSN** or launch REST API using the direct URL: https://%3Cdcnm-mgmt0-ip%3E/api-docs/#/Control%20-%20Fabrics/swapSN

Enter appropriate values in the **fabricName** and **oldSN** fields. Enter the correct Serial Number for the device in the **newSN** field. Click **Execute** to apply the changes.

Custom Template for eBGP p2p Peering

A new template **ebgp_dci_underlay** is introduced that allows easy provisioning of eBGP P2P peering configuration of the Inter-Site Network (ISN) across devices that connect two fabrics in different DCNM instances.

SVI Interface Enhancements

DCNM Release 11.5(3a) allows you to configure SVIs in the underlay for Easy Fabrics deployments.

Custom EVPN/MVPN Route Target Support

DCNM Release 11.5(3a) allows you to configure custom Route-Targets for Overlay VRFs in a VXLAN EVPN fabric. Per VRF knobs is provided to disable auto Route Target generation for EVPN address family and the ability to specify different EVPN/MVPN import and export Route Targets. This workflow is also integrated with the corresponding Nexus Dashboard Orchestrator workflow in Release 3.5(2) and later).

VRF Lite Support with SVI Interfaces

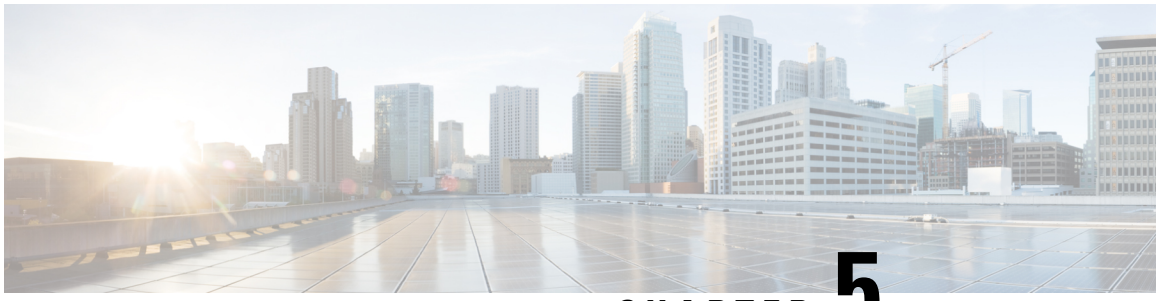
DCNM Release 11.5(3a) allows you to configure VRF Lite for Layer-3 connectivity out of the border devices over eBGP using SVIs. This is supported for both VXLAN EVPN and External fabrics.

Modifying DCNM In-Band (eth2) Interface IP Address

From Release 11.5(3a), you can modify DCNM In-Band IP address on DCNM server and re-register the sites on Nexus Dashboard when onboarded to Cisco Multi-Site Orchestrator.

Nexus Dashboard IP address change

When DCNM is onboarded to Nexus Dashboard via Cisco Multi-Site Orchestrator, DCNM stores Nexus Dashboard information such as cluster name, serial number, and data IP address of the nodes. If these parameters are modified while migrating a cluster on Nexus Dashboard, DCNM Release 11.5(3a) provides a set of APIs that you can call to update information about the new cluster.



CHAPTER 5

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:

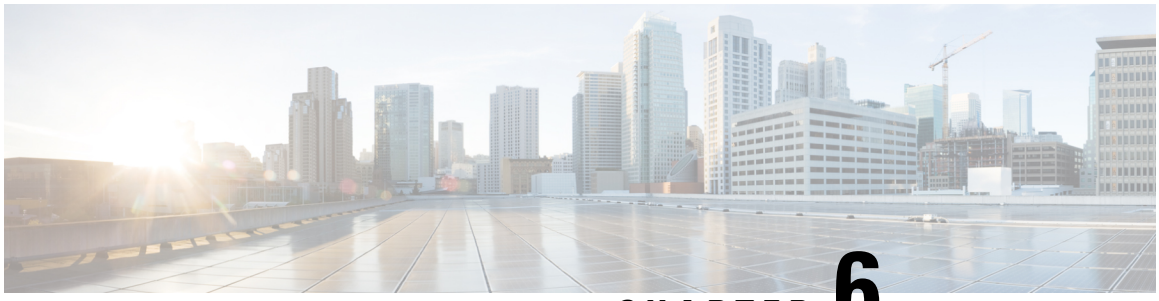
Open Caveats

The following table lists the Open bugs for Cisco DCNM, Release 11.5(3a).

Caveat ID Number	Description
CSCvz92179	GR-RMA-11.5.3a.9: Dup dir's for old dummy Serial numbers created after change to new serial number
CSCvz92193	GR-RMA-11.5.3a.9: GUI has Close button active but is greyed out for POAP screen
CSCvz89391	hyphen/~ in SN causes issues in some ifmgr calls for pre-provisioning

Resolved Caveats

There are no resolved caveats associated with this release.



CHAPTER 6

Related Documentation

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

Navigating the Cisco DCNM Documentation

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

Cisco DCNM 11.5(3a) Documentation Roadmap

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.

Table 7: Cisco DCNM 11.5(3a) Documentation

Document Title	Description
Cisco DCNM Release Notes, Release 11.5(3)a	Provides information about the Cisco DCNM software release, open caveats, and workaround information.
Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(3a)	Provides information about how to plan your requirements and install the Cisco Data Center Network Manager.
Cisco DCNM LAN Fabric Configuration Guide, Release 11.5(1)	Provides conceptual and procedural information about all the features supported with this deployment.

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.