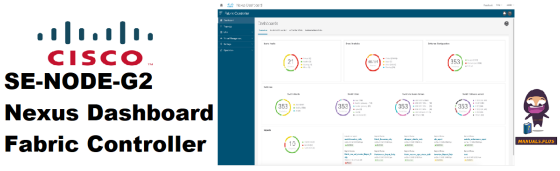
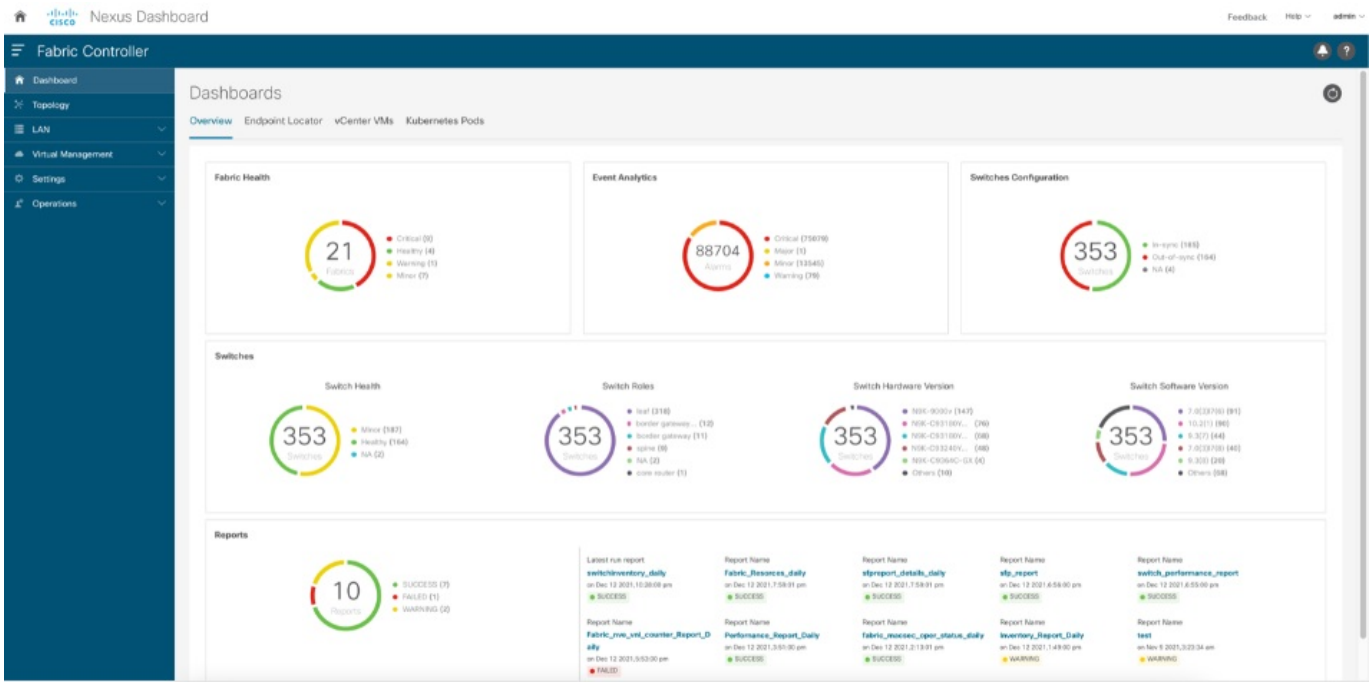


CISCO SE-NODE-G2 Nexus Dashboard Fabric Controller User Guide

Contents

CISCO SE-NODE-G2 Nexus Dashboard Fabric Controller



Product Information

Specifications

- Product Name: Cisco Nexus Dashboard Fabric Controller
- Release Version: 12.2.2
- Maximum ToR Switches: 32
- Node Types: SE-NODE-G2, ND-NODE-L4

Product Information

The Cisco Nexus Dashboard Fabric Controller, Release 12.2.2, allows for connecting a maximum of 32 ToR switches or 16 vPC-ToR pairs per leaf-vPC pair. It provides verified scalability values for various deployment types and system resources required to run NDFC on top of Nexus Dashboard.

Server Resource Requirements:

NDFC can be deployed on different form factors with varying CPU, memory, and storage requirements. The following are the specifications for different node types:

- **Physical Node (pND) – SE-NODE-G2:** 16 vCPUs, 64 GB Memory, 2 x 10-core 2.2GHz Intel Xeon Silver CPU
- **Physical Node (pND) – ND-NODE-L4:** 2.8GHz AMD CPU, 256 GB Memory
- **SAN Controller:** 16 vCPUs, 64 GB Memory, 128GB node (with SAN Insights)

Scale Limits for Fabric Discovery:

Deployment Type	Verified Limit
1-Node vND (app node)	100 switches
3-Node vND (app node)	200 switches
5-Node vND (app node)	1000 switches
1-Node pND	100 switches
3-Node pND	1000 switches

Product Usage Instructions

Connecting ToR Switches:

- To connect ToR switches, ensure that each leaf-vPC pair supports a maximum of 32 ToR switches or 16 vPC-ToR pairs.

Running NDFC on Nexus Dashboard:

- Refer to the Nexus Dashboard Capacity Planning guide to determine the appropriate server resource requirements based on the deployment type and node type.

Fabric Discovery Scale Limits:

- When deploying Fabric Discovery personas on Nexus Dashboard, ensure that you stay within the verified limits specified for each deployment type to avoid scalability issues.

FAQ

- **Q:** Can I exceed the verified scale limits for Fabric Discovery?
  - **A:** Exceeding the verified limits may lead to performance issues and is not recommended. Stick to the specified limits for optimal operation.
- **Q:** How many ToR switches can be connected per leaf-vPC pair?
  - **A:** You can connect a maximum of 32 ToR switches or 16 vPC-ToR pairs per leaf-vPC pair.

Overview

Note: Cisco Data Center Network Manager (DCNM) is renamed as Cisco Nexus Dashboard Fabric Controller (NDFC) from Release 12.0.1a.

Cisco Nexus Dashboard Fabric Controller 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. Cisco Nexus Dashboard Fabric Controller also supports other devices, such as IOS-XE switches, IOS-XR routers, and non-Cisco devices. Being a multi-fabric controller, Cisco Nexus Dashboard Fabric Controller manages multiple deployment models like VXLAN EVPN, Classic 3-Tier, Routed based fabrics for LAN while providing ready-to-use control, management, monitoring, and automation capabilities for all these environments. In addition, Cisco NDFC when enabled as a SAN Controller, automates Cisco MDS Switches and Cisco Nexus Family infrastructure in NX-OS mode.

Nexus Dashboard Fabric Controller primarily focuses on Control and Management for three primary market segments:

- LAN networking including VXLAN, Multi-site, Classic Ethernet, and External Fabrics supporting Cisco Nexus switches running standalone NX-OS, with additional support for IOS-XR, IOS-XE and adjacent Host, Compute, Virtual Machine, and Container Management systems.
- SAN networking for Cisco MDS and Cisco Nexus switches running standalone NX-OS, including support for integration with storage arrays and additionally Host, Compute, Virtual Machine, and Container Management systems.
- Media Control for Multicast Video production networks running Cisco Nexus switches operated as standalone NX-OS, with additional integrations for 3rd party media control systems.

Previously, DCNM was an application server running on a VM deployed via OVA or ISO, a physical appliance deployed via ISO, or software installed on a qualified Windows or Linux machine. Cisco Nexus Dashboard Fabric Controller, Release 12 is available as an application running exclusively on top of the Cisco Nexus Dashboard Virtual or Physical Appliance. Virtual Nexus Dashboard deployment with OVA is also referred to as virtual Nexus Dashboard (vND) deployment, while deployment of Nexus Dashboard on physical appliance (Service Engine) is known as physical Nexus Dashboard (pND) deployment. To deploy Nexus Dashboard based on your requirement, refer to **Cisco Nexus Dashboard Deployment Guide**.

Beginning with Release 12, Cisco Nexus Dashboard Fabric Controller has a single installation mode. Post installation, it supports selection from multiple personas at run-time. After the Nexus Dashboard Fabric Controller Release 12.0.2f is installed, you can choose from one of the following personas:

- Fabric Discovery—Discover, Monitor, and Visualize LAN Deployments.
- Fabric Controller—LAN Controller for Classic Ethernet (vPC), Routed, VXLAN, and IP Fabric for Media Deployments.
- SAN Controller—SAN Controller for MDS and Nexus switches. Enhanced SAN Analytics with streaming telemetry.

All features/services are modularized, broken into smaller microservices, and the required microservices are orchestrated based on the feature set or feature selections. Therefore, if any feature or microservice is down, only that microservice is restarted and recovered, resulting in minimal disruption. In contrast to the previous DCNM Active-Standby HA model, Cisco NDFC introduces Active-Active HA deployment model utilizing all three nodes for deploying microservices. This has significant improvement in both latency and effective resource utilization.

Note

For NDFC to run on top of virtual Nexus Dashboard (vND) instance, you must enable promiscuous mode on port groups associated with Nexus Dashboard interfaces where External Service IP addresses are specified. vND comprises of Nexus Dashboard management interface and data interface. By default, for LAN deployments, 2 external service IP addresses are required for the Nexus Dashboard management interface subnet. Therefore, you must enable promiscuous mode for the associated port-group. If inband management or EPL is enabled, you must specify External Service IP addresses in the Nexus Dashboard data interface subnet. The promiscuous mode also needs to be enabled for the Nexus Dashboard data/fabric interface port-group. For NDFC SAN Controller, promiscuous mode only needs to be enabled on the Nexus Dashboard data interface associated port-group. For more information, refer to **Cisco Nexus Dashboard Fabric Controller Deployment Guide**.

Note

The documentation set for this product strives to use bias-free language. For 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.

For more information, see **Cisco Nexus Dashboard Fabric Controller (Formerly DCNM)**.

Change History

The following table shows the change history for this document.

Table 1: Change History

Date	Description
17 December 2021	Published Release Notes for Cisco Nexus Dashboard Fabric Controller Release 12.0.2f.
30 September 2021	Published Release Notes for Cisco Nexus Dashboard Fabric Controller Release 12.0.1a.

Deployment Options

The following deployment options are available for Cisco Nexus Dashboard Fabric Controller:

- NDFC on Single node (non-HA Cluster)
  On Single node Nexus Dashboard, you can deploy NDFC with the following personas:
  - SAN Controller with SAN Insights
  - Fabric Controller for IP Fabric for Media (IPFM) deployments
  - Fabric Controller for lab/non-production environments (<= 25 switches)
- NDFC on a 3-node Cluster (Active-Active HA mode)
  On 3-Node Nexus Dashboard, you can deploy NDFC with the following personas:
  - Fabric Discovery
  - Fabric Controller
  - SAN Controller with or without SAN Insights
    - **Note:** For NDFC deployments, the Nexus Dashboard node should have a different subnet on the management interface and the data/fabric interface. In addition, in a 3-node Nexus Dashboard cluster, all Nexus Dashboard nodes should be layer-2 adjacent. In other words, the 3 Nexus Dashboard nodes must all belong to the same management and data networks respectively.
    - In summary, Nexus Dashboard Fabric Controller is not supported on Nexus Dashboard nodes that are deployed with management and data networks using overlapping subnets.
- NDFC on a 5-node vND Cluster (Active-Active HA mode)
  From Release 12.0.2f, on 5-Node Nexus Dashboard, you can deploy NDFC with the following personas:
  - Fabric Discovery

- Fabric Controller

In the 3-node and 5-node deployment, there are 3 Nexus Dashboard master nodes. In the 5-node deployment, the additional 2 nodes serve as worker nodes. The 3-node or 5-node cluster deployment is an active-active solution, that is, all nodes are utilized to run micro-services of Nexus Dashboard Fabric Controller. When a node fails, microservices running on the node, are moved to the other nodes. Nexus Dashboard Fabric Controller will perform normally under one node failure scenarios. However, it is expected that there will be a brief disruption to services that must be migrated on node failure. After the migration of services is complete, the supported scale will continue to function albeit at degraded performance. To restore optimal NDFC performance, a system running with one failed node is not the desired situation and must be rectified at the earliest. A 3-node or 5-node cluster cannot tolerate failure of two nodes and all NDFC services will be disrupted.

Note Nexus Dashboard cluster federation is not supported with Nexus Dashboard Fabric Controller.

For virtual Nexus Dashboard OVA deployments on ESXi environments, it is imperative that promiscuous mode is enabled on the port groups associated with Nexus Dashboard management and Nexus Dashboard data/fabric interfaces. Otherwise, some of the functionality such as SNMP trap, Image management, Endpoint Locator, SAN Insights and so on will not work.

Deployment Profiles

While enabling Cisco Cisco Nexus Dashboard Fabric Automation, based on the persona, you can choose a deployment profile. When deploying the application, the Nexus Dashboard indicates the deployment profile that is chosen for the cluster form factor. This generally does not need to be overridden, unless explicitly stated below:

To choose an appropriate profile, refer to the following recommendations.

virtual-demo

- This deployment profile must be selected for the application running on a virtual Nexus Dashboard cluster deployed using the app OVA.

Note

- SAN Insights is supported with this deployment profile in single or 3 master cluster node

Supported deployment personas include:

- Fabric Discovery in a single node cluster
- Fabric Controller deployment in single node cluster
- Fabric Controller with IPFM in a single node cluster
- SAN Controller deployment with SAN Insights in a single node cluster

Note

- virtual-demo profile is purely for demo purposes and not intended to be used for production environments.

virtual-app

This deployment profile must be selected for the application running on a virtual Nexus Dashboard cluster deployed using the app OVA. By default, this profile is selected when the application is enabled on a app node virtual Nexus Dashboard.
Supported deployment personas include:

- Fabric Controller in 3-node or 5-node cluster
- Fabric Controller with IPFM in single or 3-node cluster
- SAN Controller in single or 3-node cluster

Note SAN Insights is not supported with this deployment profile.

virtual-data

This deployment profile must be selected for the application running on a virtual Nexus Dashboard cluster deployed using the data OVA. This profile should be used for the SAN Controller persona with SAN Insights.
By default, this profile will be selected when the application is enabled on a data node virtual Nexus Dashboard.
Supported deployment personas include:

- SAN Controller in single or 3 node cluster

Note SAN Insights is supported with this deployment profile in single or 3 master cluster node

physical

This deployment profile must be selected for the application running on a physical Nexus Dashboard cluster. By default, this profile will be selected when the application is enabled on a physical Nexus Dashboard.
Supported deployment personas include:

- Fabric Controller in 3 node cluster
- Fabric Controller with IPFM in single or 3 node cluster
- SAN Controller in single or 3 node cluster

Note SAN Insights is supported with this deployment profile.

System Requirements

This chapter lists the tested and supported hardware and software specifications for Cisco Nexus Dashboard Fabric Controller architecture. The application is in English locales only.
The following sections describes the various system requirements for the proper functioning of your Cisco Nexus Dashboard Fabric Controller, Release 12.0.2f.

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 Nexus Dashboard Fabric Controller upgrade causes functionality issues.

Cisco Nexus Dashboard Version Compatibility

Cisco Nexus Dashboard Fabric Controller (NDFC) requires Nexus Dashboard version 2.1(2d) or higher. If you try to upload NDFC 12.0.2f on a Nexus Dashboard version earlier than 2.1(2d), you will not be allowed to upload the application. To download the correct version of Nexus Dashboard, visit **Software Download – Nexus Dashboard**.

Nexus Dashboard Server Resource (CPU/Memory) Requirements

Table 2: Server Resource (CPU/Memory) Requirements to run NDFC on top of ND

Deployment Type	Node Type	CPUs	Memory	Storage (Throughput: 40-50MB/s)
Fabric Discovery	Virtual Node (vND) – app OVA	16vCPUs	64GB	550GB SSD
	Physical Node (pND) (PID: SE-NODE-G2)	2x 10-core 2.2G Intel Xeon Silver CPU	256 GB of RAM	4x 2.4TB HDDs 400GB SSD 1.2TB NVME drive
Fabric Controller	Virtual Node (vND) – app OVA	16vCPUs	64GB	550GB SSD
	Physical Node (pND) (PID: SE-NODE-G2)	2x 10-core 2.2G Intel Xeon Silver CPU	256 GB of RAM	4x 2.4TB HDDs 400GB SSD 1.2TB NVME drive
SAN Controller	Virtual Node (vND) – app OVA (without SAN Insights)	16vCPUs	64GB	550GB SSD
	Data Node (vND) – Data OVA (with SAN Insights)	32vCPUs	128GB	3TB SSD
	Physical Node (pND) (PID: SE-NODE-G2)	2x 10-core 2.2G Intel Xeon Silver CPU	256 GB of RAM	4x 2.4TB HDDs 400GB SSD 1.2TB NVME drive

Nexus Dashboard Networks

When first-configuring Nexus Dashboard, on every node, you must provide two IP addresses for the two Nexus Dashboard interfaces—one connected to the Data Network and the other to the Management Network. The data network is typically used for the nodes' clustering and north-south connectivity to the physical network. The management network typically connects to the Cisco Nexus Dashboard Web UI, CLI, or API.

For enabling the Nexus Dashboard Fabric Controller, the Management and Data Interfaces on a Nexus Dashboard node must be in different subnets. The interfaces between different nodes that belong to the same Nexus Dashboard cluster, must be within the same Layer-2 Network and Layer-3 subnet. Connectivity between the Nexus Dashboard nodes is required on both networks with the round trip time (RTT) not exceeding 50ms. Other application running on the same Nexus Dashboard cluster may have lower RTT requirements and you must always use the lowest RTT requirement when deploying multiple applications in the same Nexus Dashboard cluster. We recommend consulting the **Cisco Nexus Dashboard Deployment Guide** for more information.

Table 3: Network Requirements for NDFC on Nexus Dashboard

Management Interface	**Data Interface**	**Persistent IPs**	**Support for Data and Management in the same subnet**
Layer 2 adjacent	Layer 2 adjacent	One of the following for LAN: • 2 IPs in management network if using the default LAN Device Management Connectivity setting • 2 IPs in data network if setting LAN Device Management Connectivity to Data Plus one IP per fabric for EPL in data network Plus one IP for Telemetry receiver in data or management network if IP Fabric for Media is enabled. For SAN: • 2 IPs in data network Plus one IP pernode in data network for SAN Insights receiver if enabled.	Not supported

Virtual Nexus Dashboard (vND) Prerequisites

For virtual Nexus Dashboard deployments, each vND node has 2 interfaces or vNICs. The Data vNIC maps to bond0 (also known as bond0br) interface and Management vNIC maps to bond1 (also known as bond1br) interface. The requirement is to enable/accept promiscuous mode on the port groups associated with the Nexus Dashboard Management and/or Data vNICs where IP stickiness is required. The Persistent IP addresses are

given to the pods (e.g., SNMP Trap/Syslog receiver, Endpoint Locator instance per Fabric, SAN Insights receiver, etc.). Every POD in Kubernetes can have multiple virtual interfaces.

Specifically for IP stickiness, an extra virtual interface is associated with the POD that is allocated an appropriate free IP from the external service IP pool. The vNIC has its own unique MAC address that is different from the MAC addresses associated with the vND virtual vNICs. Moreover, all North-to-South communication to and from these PODs go out of the same bond interface. By default, the VMware ESXi systems check if the traffic flows out of a particular VM vNIC matches the Source-MAC associated with that vNIC. In the case of NDFC pods with an external service IP, the traffic flows are sourced with the Persistent IP addresses of the given PODs that map to the individual POD MAC associated with the virtual POD interface. Therefore, we need to enable the required settings on the VMware side to allow this traffic to flow seamless in and out of the vND node.

For more information, refer to **Cisco Nexus Dashboard Deployment Guide**.

Supported Latency

As Cisco Nexus Dashboard Fabric Controller is deployed atop Cisco Nexus Dashboard, the latency factor is dependent on Cisco Nexus Dashboard. Refer to **Cisco Nexus Dashboard Deployment Guide** for information about latency.

SupportedWeb Browsers

Cisco Nexus Dashboard Fabric Controller is supported on the following web browsers:

- Google Chrome version 96.0.4664.93
- Microsoft Edge version 96.0.1054.43 (64-bit)
- Mozilla Firefox version 94.0.2 (64-bit)

Other Supported Software

The following table lists the other software that is supported by Cisco Nexus Dashboard Fabric Controller Release 12.0.2f.

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: HTTPS with TLS 1, 1.1 and 1.2 • TLS 1.3

Prerequisites

This chapter provides release-specific prerequisites information for your deployment of Cisco Nexus Dashboard Fabric Controller.

Prerequisites

Before you install the Cisco Nexus Dashboard Fabric Controller on Cisco Nexus Dashboard, you must need to meet the following prerequisites:

Nexus Dashboard

You must have Cisco Nexus Dashboard cluster deployed and its fabric connectivity configured, as described in **Cisco Nexus Dashboard Deployment Guide** before proceeding with any additional requirements and the Nexus Dashboard Fabric Controller service installation described here.

Nexus Dashboard Fabric Controller Release	Minimum Nexus Dashboard Release
Release 12.0.2f	Cisco Nexus Dashboard, Release 2.1.2d or later **Note** Cisco Nexus Dashboard cluster in Linux KVM does not support Nexus Dashboard Fabric Controller Release 12.0.2f.

Nexus Dashboard Networks

When first-configuring Nexus Dashboard, on every node, you must provide two IP addresses for the two Nexus Dashboard interfaces—one connected to the Data Network and the other to the Management Network. The data network is typically used for the nodes' clustering and north-south connectivity to the physical network. The management network typically connects to the Cisco Nexus Dashboard Web UI, CLI, or API.

For enabling the Nexus Dashboard Fabric Controller, the Management and Data Interfaces on a Nexus Dashboard node must be in different subnets. The interfaces between different nodes that belong to the same Nexus Dashboard cluster, must be within the same Layer-2 Network and Layer-3 subnet. Connectivity between the Nexus Dashboard nodes is required on both networks with the round trip time (RTT) not exceeding 50ms. Other application running on the same Nexus Dashboard cluster may have lower RTT requirements and you must always use the lowest RTT requirement when deploying multiple applications in the same Nexus Dashboard cluster. We recommend consulting the **Cisco Nexus Dashboard Deployment Guide** for more information.

Table 4: Network Requirements for NDFC on Nexus Dashboard

Management Interface	Data Interface	Persistent IPs	Support for Data and Management in the same subnet
Layer 2 adjacent	Layer 2 adjacent	One of the following for LAN: • 2 IPs in management network if using the default LAN Device Management Connectivity setting • 2 IPs in data network if setting LAN Device Management Connectivity to Data Plus one IP per fabric for EPL in data network Plus one IP for Telemetry receiver in data or management network if IP Fabric for Media is enabled. For SAN: • 2 IPs in data network Plus one IP pernode in data network for SAN Insights receiver if enabled.	Not supported

Virtual Nexus Dashboard (vND) Prerequisites

For virtual Nexus Dashboard deployments, each vND node has 2 interfaces or vNICs. The Data vNIC maps to bond0 (also known as bond0br) interface and Management vNIC maps to bond1 (also known as bond1br) interface. The requirement is to enable/accept promiscuous mode on the port groups associated with the Nexus Dashboard Management and/or Data vNICs where IP stickiness is required.

The Persistent IP addresses are given to the pods (e.g., SNMP Trap/Syslog receiver, Endpoint Locator instance per Fabric, SAN Insights receiver, etc.). Every POD in Kubernetes can have multiple virtual interfaces. Specifically for IP stickiness, an extra virtual interface is associated with the POD that is allocated an appropriate free IP from the external service IP pool. The vNIC has its own unique MAC address that is different from the MAC addresses associated with the vND virtual vNICs. Moreover, all North-to-South communication to and from these PODs go out of the same bond interface. By default, the VMware ESXi systems check if the traffic flows out of a particular VM vNIC matches the Source-MAC associated with that vNIC. In the case of NDFC pods with an external service IP, the traffic flows are sourced with the Persistent IP addresses of the given PODs that map to the individual POD

MAC associated with the virtual POD interface. Therefore, we need to enable the required settings on the VMware side to allow this traffic to flow seamless in and out of the vND node.

For more information, refer to **Cisco Nexus Dashboard Deployment Guide**.

Nexus Dashboard Cluster Sizing

Nexus Dashboard supports cohosting of services. Depending on the type and number of services you choose to run, you may be required to deploy extra worker nodes in your cluster. For cluster sizing information and recommended number of nodes based on specific use cases, see the **Cisco Nexus Dashboard Capacity Planning** tool.

If you plan to host other applications in addition to the Nexus Dashboard Fabric Controller, ensure that you deploy and configure additional Nexus Dashboard nodes based on the cluster sizing tool recommendation, as described in the **Cisco Nexus Dashboard User Guide**, which is also available directly from the Nexus Dashboard Web UI.

Network Time Protocol (NTP)

- Nexus Dashboard Fabric Controller uses NTP for clock synchronization, so you must have an NTP server configured in your environment.
- Clocks on all nodes must be synchronized within the same second. Any delta between two nodes that exceeds more than 1 second could affect database consistency mechanism between the nodes.

Installing Cisco Nexus Dashboard Fabric Controller

Installing Nexus Dashboard Fabric Controller Service Using App Store

To install Cisco Nexus Dashboard Fabric Controller Release 12.0.2f in an existing Cisco Nexus Dashboard cluster, perform the following steps:

Before you begin

- Ensure that you've installed the required form factor of Cisco Nexus Dashboard. For instructions, refer to **Cisco Nexus Dashboard Deployment Guide**.
- Ensure that you meet the requirements and guidelines described in Prerequisites.
- The Cisco DC App Center must be reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration. Nexus Dashboard proxy configuration is described in the **Cisco Nexus Dashboard User Guide**.

Nexus Dashboard User Guide.

- If you are unable to establish the connection to the DC App Center, skip this section and follow the steps described in Installing Nexus Dashboard Fabric Controller Service Manually.
- Ensure that the services are allocated with IP pool addresses on the Cisco Nexus Dashboard. For more information, refer to Cluster Configuration section in **Cisco Nexus Dashboard User Guide**.

Procedure

- **Step 1** Launch the Cisco Nexus Dashboard Web UI using appropriate credentials.
- **Step 2** Click on Admin Console > Services menu in the left navigation pane to open the Services Catalog window.
- **Step 3** On the App Store tab, identify the Nexus Dashboard Fabric Controller Release 12.0.2f card and click Install.
- **Step 4** On the License Agreement screen, read the CISCO APP CENTER AGREEMENT and click on Agree and Download.
    - Wait for the application to be downloaded to the Nexus Dashboard and deployed.
    - It may take up to 30 minutes for the application to replicate to all nodes and all services to fully deploy. Nexus Dashboard Fabric Controller application appears in the Services Catalog. The status is shown as Initializing.
- **Step 5** After the Nexus Dashboard Fabric Controller application is initialized, click Enable on the Nexus Dashboard Fabric Controller application card.
    - The Enable Cisco Nexus Dashboard Fabric Controller window appears.
- **Step 6** Click on the Deployment Profile field to view the different profiles.
    - Deployment profile contains the resources profile required for Cisco Nexus Dashboard Fabric Controller. For more information, refer to Deployment Profiles, on page 4.
- **Step 7** Click Enable.
    - After the services are enabled, the button on the Nexus Dashboard Fabric Controller card shows Open.
    - Wait until all the pods and containers are up and running.
- **Step 8** Click on Open to launch Cisco Nexus Dashboard Fabric Controller Web UI.
    - The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you used for the Nexus Dashboard.
    - **Note** The Nexus Dashboard Fabric ControllerWeb UI opens in a new browser. The Feature Management window appears.
    - If External Service Pool IP addresses are not configured, an error message appears. Go to Nexus DashboardWeb UI > Infrastructure > Cluster Configuration. Configure the Management Service and Data Service IP addresses in the External Service Pools section. For more information, refer to Cluster Configuration section in **Cisco Nexus Dashboard User Guide**.
    - **Note** Three cards namely Fabric Discovery, Fabric Controller, and SAN Controller is displayed.
- **Step 9** Based on the requirement, select the deployment.
    - From the list of Features, select features that you need to enable on the Nexus Dashboard Fabric Controller deployment.
    - **Note** The list of features displayed is based on the Deployment selected on the card.
- **Step 10** Click Apply to deploy Nexus Dashboard Fabric Controllerwith the selected features.
    - After the installation is complete, the deployment card and all the features status show as Started.

InstallingNexusDashboardFabricControllerServiceManually

To manually upload and install Cisco Nexus Dashboard Fabric Controller Release 12.0.2f in an existing Cisco Nexus Dashboard cluster, perform the following steps:

Before you begin

- Ensure that you've installed the required form factor of Cisco Nexus Dashboard. For instructions, refer to **Cisco Nexus Dashboard Deployment Guide**.
- Ensure that you meet the requirements and guidelines described in Prerequisites.
- Ensure that the services are allocated with IP pool addresses on the Cisco Nexus Dashboard. For more information, refer to Cluster Configuration section in **Cisco Nexus Dashboard User Guide**.

Procedure

- **Step 1** Go to the following site: **https://dcappcenter.cisco.com**. Cisco DC App Center page opens.
  - In the All apps section, all the applications supported on Cisco Nexus Dashboard.
- **Step 2** Locate the Cisco Nexus Dashboard Fabric Controller Release 12.0.2f application and click the Download icon.
- **Step 3** On the License Agreement screen, read the CISCO APP CENTER AGREEMENT and click on Agree and Download.
  - Save the Nexus Dashboard Fabric Controller application to your directory that is easy to find when you must import/upload to Nexus Dashboard.
- **Step 4** Launch the Cisco Nexus Dashboard using appropriate credentials.
- **Step 5** Choose Admin Console > Services > Installed Services to view the services installed on the Cisco Nexus Dashboard.
- **Step 6** From the Actions drop-down list, choose Upload Service.
- **Step 7** Choose the Location toggle button and select either Remote or Local.
  You can choose to either upload the service from a remote or local directory.
  - If you select Remote, in the URL field, provide an absolute path to the directory where the Nexus Dashboard Fabric Controller application is saved.
  - If you select Local, click Browse and navigate to the location where the Nexus Dashboard Fabric Controller application is saved. Select the application and click Open.
- **Step 8** Click Upload.
  - Nexus Dashboard Fabric Controller application appears in the Services Catalog. The status is shown as Initializing.
  - Wait for the application to be downloaded to the Nexus Dashboard and deployed.
  - It may take up to 30 minutes for the application to replicate to all nodes and all services to fully deploy.
  - Nexus Dashboard Fabric Controller application appears in the Services Catalog. The status is shown as Initializing.
- **Step 9** After the Nexus Dashboard Fabric Controller application is initialized, click Enable on the Nexus Dashboard Fabric Controller application card.
  - The Enable Cisco Nexus Dashboard Fabric Controller window appears.
- **Step 10** Click on the Deployment Profile field to view the different profiles.
  - Deployment profile contains the resources profile required for Cisco Nexus Dashboard Fabric Controller. For more information, refer to Deployment Profiles, on page 4.
- **Step 11** Click Enable.
  - After the services are enabled, the button on the Nexus Dashboard Fabric Controller card shows Open.
  - Wait until all the pods and containers are up and running.
- **Step 12** Click on Open to launch Cisco Nexus Dashboard Fabric Controller Web UI.
  - The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you

used for the Nexus Dashboard.

- **Note** The Nexus Dashboard Fabric ControllerWeb UI opens in a new browser. The Feature Management window appears.
  - If External Service Pool IP addresses are not configured, an error message appears. Go to Nexus DashboardWeb UI > Infrastructure > Cluster Configuration. Configure the Management Service and Data Service IP addresses in the External Service Pools section. For more information, refer to Cluster Configuration section in **Cisco Nexus Dashboard User Guide**.
  - **Note** Three cards namely Fabric Discovery, Fabric Controller, and SAN Controller is displayed.
- **Step 13** Based on the requirement, select the deployment.
  - From the list of Features, select features that you need to enable on the Nexus Dashboard Fabric Controller deployment.
  - **Note** The list of features displayed is based on the Deployment selected on the card.
- **Step 14** Click Apply to deploy Nexus Dashboard Fabric Controller with the selected features.
  - After the installation is complete, the deployment card and all the features status show as Started.

Upgrading Cisco Nexus Dashboard Fabric Controller

Upgrade Paths to Release 12.0.2f

The following table summarizes the type of upgrade that you must follow to upgrade to Release 12.0.2f.
Go to **Software Download** to download the Upgrade Tool scripts.

Current Release Number	**Deployment Type**	**Upgrade type when upgrade to Release 12.0.2f**
12.0.1a	All	**1.** Upgrade Nexus Dashboard version 2.1.1e to version 2.1.2d **2.** Upgrade NDFC application to 12.0.2f.
11.5(3)	LAN Fabric Deployment	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
	Note Media Controller and all SAN deployments are not supported in Release 11.5(3).	

11.5(2)	SAN Deployment on Windows and Linux	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
	SAN Deployment on OVA/ISO/SE	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
	LAN Fabric Deployment on OVA/ISO/SE	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
11.5(1)	SAN Deployment on Windows and Linux	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
	SAN Deployment on OVA/ISO/SE	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
	LAN Fabric Deployment on OVA/ISO/SE	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**
	Media Controller Deployment on OVA/ISO	**1.** Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** **2.** Restore on Nexus Dashboard Fabric Controller **Web UI > Operations > Backup & Restore**

Persona Compatibility for Upgrade

By using the appropriate Upgrade Tool, you can restore data that is backed up from DCNM Release 11.5(1) or 11.5(2) or 11.5(3) on a newly deployed Cisco Nexus Dashboard Fabric Controller for the personas as mentioned in the following table:

Backup from DCNM 11.5(x)[1] [2]	**Persona Enabled in NDFC 12.0.2f after Upgrade**
DCNM 11.5(x) LAN Fabric Deployment on OVA/ISO/SE	Fabric Controller + Fabric Builder
DCNM 11.5(x) PMN Deployment on OVA/ISO/SE	Fabric Controller + IP Fabric for Media (IPFM)
DCNM 11.5(x) SAN Deployment on OVA/ISO/SE	SAN Controller
DCNM 11.5(x) SAN Deployment on Linux	SAN Controller
DCNM 11.5(x) SAN Deployment on Windows	SAN Controller

1 All references to 11.5(x) are for 11.5(1) or 11.5(2). Upgrade to NDFC 12 from DCNM 11.5(3) is supported for LAN Fabric Deployments only.
2 DCNM Release 11.5(3) does not support Media Controller and SAN deployments.

Feature Compatibility Post Upgrade

The following table lists caveats associated with features that are restored from DCNM 11.5(x) backup after upgrade to NDFC, Release 12.0.2f.

Feature in DCNM 11.5(x)	Upgrade Support
Nexus Dashboard Insights configured Refer to Nexus Dashboard Insights User Guide for more information.	Supported
Container Orchestrator (K8s) Visualizer	Supported
VMM Visibility with vCenter	Supported
Nexus Dashboard Orchestrator configured	Not Supported
Preview features configured	Not supported
LAN switches in SAN installations	Not supported
Switches discovered over IPv6	Not supported
DCNM Tracker	Not supported
SAN CLI templates	Not carried over from 11.5(x) to 12.0.2f
Switch images/Image Management data	Not carried over from 11.5(x) to 12.0.2f
Slow drain data	Not carried over from 11.5(x) to 12.0.2f
Infoblox configuration	Not carried over from 11.5(x) to 12.0.2f
Endpoint Locator configuration	You must reconfigure Endpoint Locator (EPL) post upgrade to Release 12.0.2f. However, historical data is retained up to a m aximum size of 500 MB.
Alarm Policy configuration	Not carried over from 11.5(x) to 12.0.2f
Performance Management data	CPU/Memory/Interface statistics up to 90 days is restored post upgrade.

Downloading the Nexus Dashboard Fabric Controller Upgrade Tool

To download Upgrade tool to upgrade from Cisco DCNM to Nexus Dashboard Fabric Controller, perform the following steps:

Before you begin

- Identify the deployment type of Cisco DCNM Release 11.5(x) setup.

Procedure

- **Step 1** Go to the following site: **http://software.cisco.com/download/**.
  - A list of the latest release software for Cisco Nexus Dashboard Fabric Controller available for download is displayed.
- **Step 2** In the Latest Releases list, choose Release 12.0.2f.
- **Step 3** Based on your Cisco DCNM 11.5(x) deployment type, locate the DCNM_To_NDFC_Upgrade_Tool and click the Download icon.
  - The following table displays the DCNM 11.5(x) deployment type, and the corresponding Nexus Dashboard Fabric Controller upgrade tool that you must download.
  - **Table 5:** DCNM 11.5(x) Deployment type and Upgrade Tool Compatibility Matrix

DCNM 11.5(x) deployment type	UpgradeTool Name
ISO/OVA	DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
Linux	DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Windows	DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip

- **Step 4** Save the appropriate Upgrade Tool to the 11.5(x) server using sysadmin credentials.

Backup Using the Upgrade Tool

To run the DCNM_To_NDFC_Upgrade_Tool to take a backup of all the applications and data on DCNM 11.5, perform the following steps:

Before you begin

- On Cisco DCNM Release 11.5(1), ensure that you validate each fabric before proceeding to take backup.
  - Choose Cisco DCNMWeb UI > Administration > Credentials Management > SAN Credentials.
  - Select each fabric and click Validate to validate credentials before taking backup.
- Ensure that you've copied the appropriate Upgrade Tool to the server of your DCNM 11.5(x) setup.
- Ensure that you have enabled execution permissions to the Upgrade tool. Use chmod +x . to enable executable permissions.
  - [root@dcnm]# chmod +x ./DCNM12UpgradeToolOVAISO

Procedure

- **Step 1** Log on to the Cisco DCNM Release 11.5(x) appliance console.
- **Step 2** Run the following command to create a screen session.
  - dcnm# screen

    This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.
- **Step 3** Log on to the /root/ directory, by using the su command.
  - dcnm# su

- Enter password: <<enter-password>>
- [root@dcnm]#

- **Step 4** Execute the upgrade tool, by using the ./DCNM_To_NDFC_Upgrade_Tool command.

  For OVA/ISO-

```
[root@dcnm]# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO /* for OVA/ISO
```

  For Windows/Linux-

```
root@dcnm]# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
[root@dcnm-rhel]# cd DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
[root@dcnm-rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ls
DCNMBackup.bat  DCNMBackup.sh  jar
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.sh        /* Enter this command
 for Linux appliance */
OR
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.bat       /* Enter this command
 for Windows appliance */
```

  - The upgrade tool analysis the DCNM appliance data, and determines whether you can upgrade to Cisco Nexus Dashboard Fabric Controller Release 12.0.2f or not.
  - **Note** The backup that is generated by using this tool can be used to restore data, after upgrade.

- **Step 5** At the prompt to continue with backup, press y.

```
********************************************************************************
Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.
This tool will analyze this system and determine whether you can move to NDFC 12.0.2f or
not.
If upgrade to NDFC 12.0.2f is possible, this tool will create files to be used for performing
 the upgrade.
NOTE: only backup files created by this tool can be used for upgrading, older backup files
 created with 'appmgr backup'
CAN NOT be used for upgrading to NDFC 12.0.2f
Thank you!
********************************************************************************

Continue? [y/n]: y

Collect operational data (e.g. PM, EPL)? [y/n]: y

Does this DCNM 11.5(1) have DCNM Tracker feature enabled on any switch on any fabric? [y/n]:
 n
```

- **Step 6** Enter the encryption key to the backup file.
  - **Note:** You must provide this encryption key when you're restoring the backup file. Ensure that you save the encryption key in a safe location. If you loose the encryption key, you cannot restore the backup.

```
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring the backup file generated by
this tool.

Please enter the encryption key:      /* enter the encryption key for the backup file */
Enter it again for verification:      /* re-enter the encryption key for the backup file
*/

...
...
Creating backup file
Done.
Backup file: backup11_dcnm-172-23-87-224_20210928-093355.tar.gz       /* backup file name*/
[root@dcnm]#
```

  - The encrypted backup file is created.

- **Step 7** Copy the backup file to a safe location and shut down the application 11.5(x) DCNM appliance.

Example

Example for taking backup using the DCNM backup Tool

- Taking backup on DCNM 11.5(x) OVA/ISO appliance

```
[root@dcnm]# chmod +x DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
[root@dcnm]# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.

This tool will analyze this system and determine whether you can move to
NDFC 12.0.2f or not.

If upgrade to NDFC 12.0.2f is possible, this tool will create files
to be used for performing the upgrade.

NOTE:
only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to NDFC 12.0.2f

Thank you!
********************************************************************************

Continue? [y/n]: y

Collect operational data (e.g. PM, EPL)? [y/n]: y

Does this DCNM 11.5(1) have DCNM Tracker feature enabled on any switch on any fabric?
[y/n]: n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:      /* enter the encryption key for the backup file
*/
Enter it again for verification:      /* re-enter the encryption key for the backup
file */

Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!
Collecting AFW app info
Decrypting stored credentials
Creating backup file
Done.
Backup file: backup11_dcnm-172-23-87-224_20210913-012857.tar.gz        /* backup file
name*/
[root@dcnm]#
```

- Taking backup on DCNM 11.5(x) Windows/Linux appliance

```
[root@dcnm]# chmod +x DCNM_To_NDFC_Upgrade_Tool_LIN_WIN
[root@dcnm]# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
    creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
    creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/DCNMBackup.java
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar

   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
   inflating:
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat

[root@dcnm-rhel]# cd DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
[root@dcnm-rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ls
DCNMBackup.bat  DCNMBackup.sh  jar
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.sh        /* Enter this
command for Linux appliance */
OR
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.bat        /* Enter this
command for Windows appliance */

Enter DCNM root directory [/usr/local/cisco/dcm]:

Initializing, please wait...

Note: ./jar/DCNMBackup.java uses unchecked or unsafe operations.
Note: Recompile with -Xlint:unchecked for details.
********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.0.2f
or not.

If upgrade to NDFC 12.0.2f is possible, this tool will create files to be used for
performing the upgrade.

Thank you!

********************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM) might
 take some time.

Do you want to export operational data also? [y/N]: y
********************************************************************************

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring the backup file generated
by this tool.
```

```
Please enter the encryption key:       /* enter the encryption key for the backup file
 */
Enter it again for verification:       /* re-enter the encryption key for the backup
file */
2021-09-13 14:36:31 INFO  DCNMBackup:223 - Inside init() method
2021-09-13 14:36:31 INFO  DCNMBackup:245 - Loading properties....
2021-09-13 14:36:31 INFO  DCNMBackup:301 - Inside checkLANSwitches...
2021-09-13 14:36:32 INFO  DCNMBackup:315 - LAN Switch count: 0
2021-09-13 14:36:32 INFO  DCNMBackup:342 - Inside exportDBTables...
2021-09-13 14:36:32 INFO  DCNMBackup:358 - Exporting ---------> statistics
2021-09-13 14:36:32 INFO  DCNMBackup:358 - Exporting ---------> sequence
...
...
...
2021-09-13 14:49:48 INFO  DCNMBackup:1760 - ###### Total time to export Hourly data:
42 seconds.


2021-09-13 14:49:48 INFO  DCNMBackup:1767 - Exporting SanPort Daily entries.
2021-09-13 14:49:48 INFO  DCNMBackup:1768 - Total number of ports: 455
2021-09-13 14:49:48 INFO  DCNMBackup:1769 - This might take a while, please wait...
2021-09-13 14:50:23 INFO  DCNMBackup:1791 - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 13751
2021-09-13 14:50:23 INFO  DCNMBackup:1795 - ###### Total time to export Daily data: 34
 seconds.


2021-09-13 14:50:23 INFO  DCNMBackup:1535 - ###### Total time to export PM data: 81
seconds.
2021-09-13 14:50:23 INFO  DCNMBackup:879 - Creating final tar.gz file....
2021-09-13 14:50:30 INFO  DCNMBackup:892 - Final tar.gz elapsed time: 7049 in ms
2021-09-13 14:50:30 INFO  DCNMBackup:893 - Backup done.
2021-09-13 14:50:30 INFO  DCNMBackup:894 - Log file: backup.log
2021-09-13 14:50:30 INFO  DCNMBackup:895 - Backup file:
backup11_rhel77-160_20210913-149215.tar.gz        /* backup file name*/
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]#
```

Upgrading from Cisco DCNM 11.5(x) to Cisco NDFC Release 12.0.2d

To upgrade to Cisco Nexus Dashboard Fabric Controller Release 12.0.2d from DCNM Release 11.5(x), perform the following steps:

- context here

Before you begin

- Ensure that you've access to the Backup file created from 11.5(x) appliance.
- If you do not have the encryption key, you cannot restore from the backup file.
- Ensure that you've installed the required form factor of Cisco Nexus Dashboard. For instructions, refer to **Cisco Nexus Dashboard Deployment Guide**.
- Ensure that you've installed a fresh installation of Cisco Nexus Dashboard Fabric Controller. For instructions to install Cisco Nexus Dashboard Fabric Controller, refer to:
  - Installing Nexus Dashboard Fabric Controller Service Manually,.
  - Installing Nexus Dashboard Fabric Controller Service Using App Store

Procedure

- **Step 1** On Nexus Dashboard > Services, identify Cisco Nexus Dashboard Fabric Controller card and click Open.
    - On the Nexus Dashboard Fabric Controller Web UI, Feature Management screen is displayed.
    - Note that none of the personas are selected on the freshly installed Nexus Dashboard Fabric Controller.
- **Step 2** Click Restore.
    - The Operations > Backup & Restore window opens.
- **Step 3** Click Restore.
    - The Restore now window appears.
- **Step 4** Under Type, select your desired format to restore.
    - Choose Config only to restore only configuration data.
    - Choose Full to restore all previous version data to this application.
- **Step 5** Choose the appropriate destination where you have stored the backup file.
    - Choose Upload File if the file is stored in a local directory.
        - Open the directory where you've saved the backup file.
        - Drag and drop the backup file to the Restore now window

          Click Browse. Navigate to the directory where you've saved the backup file. Select the backup file and click Open.
        - Enter the Encryption Key to the backup file.
    - Choose Import from SCP if the backup file is stored in a remote directory.
        - In the SCP Server field, provide the SCP server IP Address.
        - In the File Path field, provide the relative file path to the backup file.
        - In the Username and Password fields, enter appropriate details.
        - In the Encryption Key field, enter the Encryption Key to the backup file.
- **Step 6** Click Restore.
    - A progress bar appears showing the completed percentage and the description of the operation. The Web UI is locked while the upgrade is in progress. After the restore is complete, the backup file appears in the table on Backup & Restore screen. The time required to restore depends on the data in the backup file.
    - An error appears if you've not allocated with IP pool addresses on the Cisco Nexus Dashboard. For more information, refer to Cluster Configuration section in **Cisco Nexus Dashboard User Guide**.

      Note After successful restoration, a notification banner appears as below:
        - Reload the page to see latest changes.
        - Click Reload the page, or refresh the browser page to complete restore and begin using you Cisco Nexus Dashboard Fabric Controller Web UI.

Upgrading from Cisco NDFC Release 12.0.1a to NDFC Release 12.0.2d

To upgrade to Cisco Nexus Dashboard Fabric Controller Release 12.0.2d from NDFC Release 12.0.1a, perform the following steps:

- context here

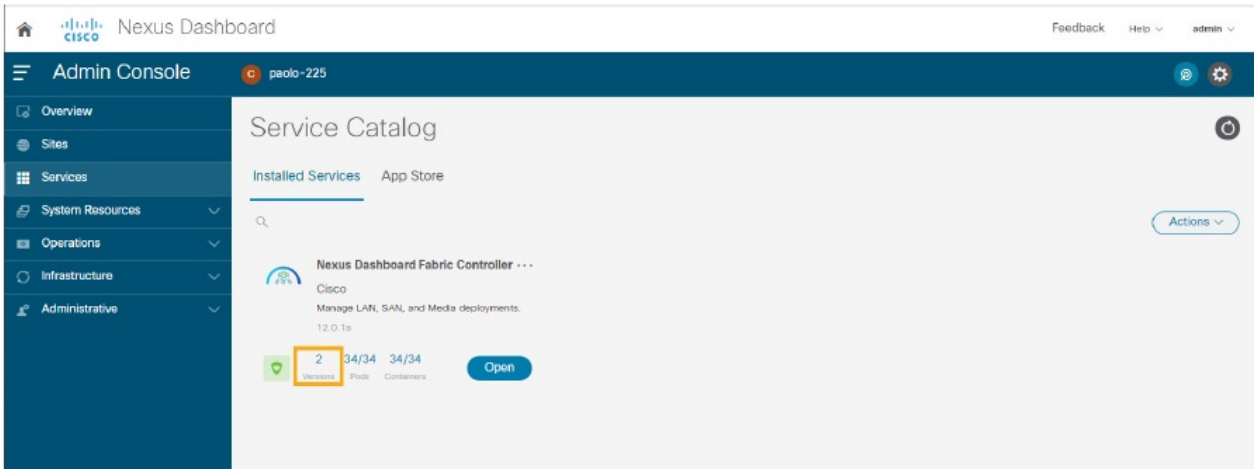
Before you begin

- Cisco NDFC 12.0.2d is compatible with Nexus Dashboard Release 2.1.2c or later. Upgrade the Nexus Dashboard to Release 2.1.2c. For instructions, refer to **Upgrading Nexus Dashboard**.

Note You cannot install or upgrade to NDFC Release 12.0.2d without Nexus Dashboard Release 2.1.2c or later.

Procedure

- **Step 1** Ensure that the Nexus Dashboard Release 2.2.2c or later is installed.
  - On Nexus Dashboard > Services, you must see Nexus Dashboard Fabric Controller Release 12.0.1a.
- **Step 2** From the Actions drop-down list, choose Upload Service.
- **Step 3** Choose the Location toggle button and select either Remote or Local.
  You can choose to either upload the service from a remote or local directory.
  - If you select Remote, in the URL field, provide an absolute path to the directory where the Nexus Dashboard Fabric Controller application is saved.
  - If you select Local, click Browse and navigate to the location where the Nexus Dashboard Fabric Controller application is saved. Select the application and click Open.
- **Step 4** Click Upload.
  - A second Nexus Dashboard Fabric Controller application appears in the Services Catalog. The progress bar indicates the upload status.
  - Wait for the application to be downloaded to the Nexus Dashboard and deployed.
  - It may take up to 30 minutes for the application to replicate to all nodes and all services to fully deploy.
  - Nexus Dashboard Fabric Controller application appears in the Services Catalog. Note that Versions displays as 2 on the Nexus Dashboard Fabric Controller card.



- **Step 5** On the Nexus Dashboard Fabric Controller card, click on ellipsis (…) icon. From the drop-down list, select Available Versions.
  - The Available Versions table displays both 12.0.1a and 12.0.2d.
- **Step 6** Click Activate in the 12.0.2d version row to activate NDFC Release 12.0.2d.
  - The Activate Nexus Dashboard Fabric Controller window appears.
- **Step 7** Verify if all the configurations displayed are correct. Click Activate.
  - After the services are enabled, the button on the Nexus Dashboard Fabric Controller card shows Open.
  - Wait until all the pods and containers are up and running.
- **Step 8** Click on Open to launch Cisco Nexus Dashboard Fabric Controller Web UI.
  - The single sign-on (SSO) feature allows you to log in to the application using the same credentials as you used for the Nexus Dashboard.

    - **Note** The Nexus Dashboard Fabric ControllerWeb UI opens in a new browser. The Feature Management window appears.
    - If External Service Pool IP addresses are not configured, an error message appears. Go to Nexus DashboardWeb UI > Infrastructure > Cluster Configuration. Configure the Management Service and Data Service IP addresses in the External Service Pools section. For more information, refer to Cluster Configuration section in **Cisco Nexus Dashboard User Guide**.
    - **Note** Three cards namely Fabric Discovery, Fabric Controller, and SAN Controller is displayed.
- **Step 9** Based on the requirement, select the deployment.
    - From the list of Features, select features that you need to enable on the Nexus Dashboard Fabric Controller deployment.
    - **Note** The list of features displayed is based on the Deployment selected on the card.
- **Step 10** Click Apply to deploy Nexus Dashboard Fabric Controllerwith the selected features.
    - After the installation is complete, the deployment card and all the features status show as Started.

Feature Management

After restoring the backup, based on the type of deployment, Nexus Dashboard Fabric Controller Release 12.0.2f is deployed with one of the following personalities:

- Fabric Controller
- SAN Controller

Note

- The status on the Feature Management changes to Starting. Additionally, you can select the features that you want to enable. Check the Feature check box and click Save & Continue.
- There are caveats associated with features enabled on DCNM 11.5(x) with respect to upgrade to NDFC, Release 12.0.2f. For more information, see Feature Compatibility Post Upgrade.

Changing across Feature-Set

Nexus Dashboard Fabric Controller 12 allows you to switch from one feature set to another. Choose Settings > Feature Management. Select the desired feature set and applications in the table below. Click Save & Continue. Refresh the browser to begin using Cisco Nexus Dashboard Fabric Controller with the new feature set and applications.

There are a few features/applications supported with specific deployments. When you change the feature set, some of these features are not supported in the new deployment. The following table provides details about the pre-requisites and criteria based on which you can change the feature set.

Table 6: Supported Switching between deployments

From/To	Fabric Discovery	Fabric Controller	SAN Controller
Fabric Discovery	–	Only monitor mode fabric is supported in Fabric Discovery deployment. When you change the feature set, the fabric can be used in the Fabric Controller deployment.	Not supported
Fabric Controller	You must delete the existing fabrics before changing the fabric set.	If you're changing from Easy Fabric to IPFM fabric application, you must delete the exiting fabrics.	Not supported
SAN Controller	Not supported	Not supported	–

Post Upgrade Tasks

The following sections describe the tasks that must be performed post upgrading to Cisco NDFC, Release 12.0.2f.

Post Upgrade tasks for SAN Controller

After restoring the data from backup, all the server-smart licenses are OutofCompliance. To migrate to Smart Licensing using Policy, launch Nexus Dashboard Fabric Controller. On the Web UI, choose Operations > License Management > Smart tab. Establish trust with CCSM using SLP. For instructions, refer to License Management chapter in Cisco Nexus Dashboard Fabric Controller Configuration Guides.

Post Upgrade tasks for Fabric Controller

The following features are not carried over when you upgrade from DCNM 11.5(x) to Cisco NDFC 12.0.2f:

- Endpoint Locator must be reconfigured
- IPAM Integration must be reconfigured
- Alarm Policies must be reconfigured
- Custom topologies must be recreated and saved
- PM collection must be re-enabled on fabrics
- Switch images must be uploaded

Managing Trap IP on Nexus Dashboard and Nexus Dashboard Fabric Controller

Deployment Type in Release 11.5(x)	In 11.5(x), trap IP address is collected from	LAN Device Management Connectivity	In 12.0.2f, trap IP address belongs to	Result
LAN Fabric Media Controller	eth1 (or vip1 for HA systems)	Management	Belongs to Management subnet	Honored[3]
LAN Fabric Media Controller	eth0 (or vip0 for HA systems)	Management	Does not belong to Management subnet	Ignored, another IP from the Management pool will be used as trap IP
LAN Fabric Media Controller	eth0 (or vip0 for HA systems)	Data	Belongs to Data subnet	Honored
LAN Fabric Media Controller	eth0 (or vip0 for HA systems)	Data	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP
SAN Management	OVA/ISO – • trap.registaddress (if set) • eth0 (if trap.Regis address is not set)	Not applicable	Belongs to Data subnet	Honored
		Not applicable	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP
	Windows/Linux –			
	• trap.registaddress (if set)			
	• Interface based on event-manager algorithm (if trap.Regis address is not set			

3 There is no configuration difference. No further action required.

***** Honored – There is no configuration difference. No further action required.

****** Ignored – Configuration difference is created. On the Web UI > LAN > Fabrics > Fabrics, double click on the Fabric to view Fabric Overview. From Fabrics Actions drop-down list, select Recalculate Config.
Click Deploy Config.

Changes to Templates for Fabric, Interfaces, and Links

The following fabrics, interface and link template names are changed in Nexus Dashboard Fabric Controller

Release 12.0.2f, where the _11_1 string is removed.

- **Fabric Templates:**
  - Easy_Fabric.template
  - External_Fabric.template
  - MSD_Fabric.template
- **Interface Policy Template:**
  - int_access_host.template
  - int_dot1q_tunnel_host.template
  - int_routed_host.template
  - int_trunk_host.template
  - int_intra_fabric_num_link.template
  - int_intra_fabric_unnum_link.template
  - int_intra_vpc_peer_keep_alive_link.template
  - int_loopback.template
  - int_mgmt.template
  - int_monitor_ethernet.template
  - int_monitor_port_channel.template
  - int_nve.template
  - int_port_channel_aa_fex.template
  - int_port_channel_fex.template
  - int_port_channel_access_host.template
  - int_port_channel_dot1q_tunnel_host.template
  - int_port_channel_trunk_host.template
  - int_subif.template
  - int_vpc_access_host.template
  - int_vpc_dot1q_tunnel.template
  - int_vpc_trunk_host.template
  - int_vpc_peer_link_po.template

Link IFC Templates:

- ext_fabric_setup.template
- ext_multisite_underlay_setup.template

Configuration Compliance changes

The Configuration Compliance (CC) related files are also changed as follows:

- Configuration Compliance is now INTERNAL NDFC templates.
- Path n file system for DCNM 11.5 (x)
  - /usr/local/cisco/dcm/dcnm/model-config

Table 7: DCNM 11.5 to NDFC Template Name Mapping

Template name in DCNM 11.5(x)	Template name in NDFC 12.0.2f[4]
compliance_case_insensitive_clis	compliance_case_insensitive_clis
ipv6_clis	compliance_ipv6_clis
strict_cc_exclude_clis	compliance_strict_cc_exclude_clis

4 Refer to Cisco NDFC Fabric Controller Configuration Guide for more information.

More Information

Contact

Americas Headquarters

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

Documents / Resources

	CISCO SE-NODE-G2 Nexus Dashboard Fabric Controller [pdf] User Guide SE-NODE-G2, SE-NODE-G2 Nexus Dashboard Fabric Controller, Nexus Dashboard Fabric Controller, Dashboard Fabric Controller, Fabric Controller, Controller

References

- User Manual