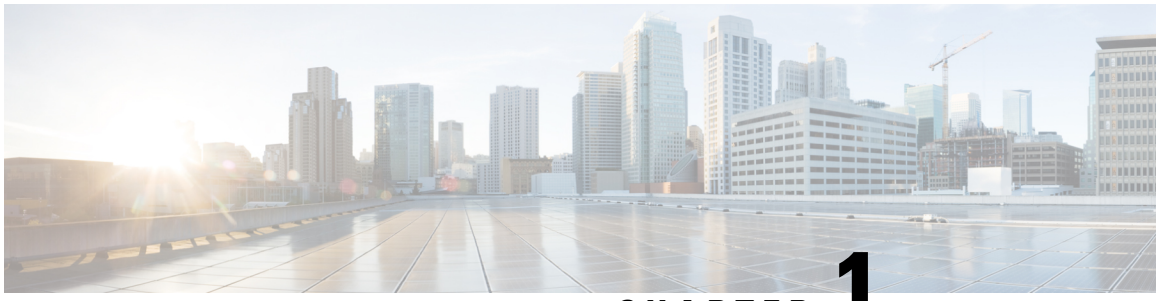
Cisco Nexus Dashboard Fabric Controller Installation and Upgrade Guide, Release 12.1.1e

First Published: 2022-06-07

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

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, FabricPath, and 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 with a focus on storage-specific features and analytics capabilities.

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 Orchestration 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 the 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 12.1.1e 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.

Note For any given instance of Nexus Dashboard, only one version of NDFC service will be active. On the active NDFC service, you can configure only one persona at any given instance.

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 in a cluster for deploying microservices. This has significant improvement in both latency and effective resource utilization.

Note For NDFC to run on top of the virtual Nexus Dashboard (vND) instance, you must enable promiscuous mode on port groups that are 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 Endpoint Locator (EPL) is enabled, you must specify External Service IP addresses in the Nexus Dashboard data interface subnet. You must also enable the promiscuous mode for the Nexus Dashboard data/fabric interface port-group. For NDFC SAN Controller, promiscuous mode must be enabled only on the Nexus Dashboard data interface associated 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 Deployment Guide.

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
03 June 2022	Release 12.1.1e became available.

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:

  - Fabric Discovery for lab/non-production environments (<= 25 switches)
  - Fabric Controller for lab/non-production environments (<= 25 switches)
  - Fabric Controller in IP Fabric for Media controller mode for production environments
  - SAN Controller for production environments (<= 80 switches)

Note Fabric Controller/Fabric Discovery deployment is for Lab purposes only. Do not deploy this in your production environment.

- 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

- NDFC on a 5-node virtual Nexus Dashboard (vND) Cluster (Active-Active HA mode)

  On 5-Node Nexus Dashboard, you can deploy NDFC with the following personas:

  - Fabric Discovery
  - Fabric Controller

- NDFC on a 3-node/4-node/5-node physical Nexus Dashboard (pND) Cluster (Active-Active HA mode)

  On a 4-node or 5-node Nexus Dashboard, you can deploy Nexus Dashboard Insights (NDI) along with NDFC with the following personas:

  - Nexus Dashboard Insights and NDFC in Fabric Discovery persona (NDFC-Monitored mode) – 4 pND nodes
  - Nexus Dashboard Insights and NDFC in Fabric Controller persona (NDFC-Managed mode) – 5 pND nodes

- NDFC on a Nexus Dashboard running on top of Red Hat Enterprise Linux (RHEL)

  From Release 12.1.1e, on a 1-node or 3-node Nexus Dashboard on the RHEL server, you can deploy NDFC with the following personas:

  - SAN Controller with or without SAN Insights

- NDFC on a virtual Nexus Dashboard (vND) with KVM hypervisor

  From Release 12.1.1e, on a virtual Nexus Dashboard with KVM hypervisor, you can deploy NDFC with the following personas:

Note You must create bridge interfaces on Linux before installing Nexus Dashboard on KVM with Centos7. Ensure that you use bridge interfaces and do not allow other interfaces during Nexus Dashboard installation.

  - Supports Fabric Controller, Fabric Discovery, and SAN Controller personas.

Refer to Nexus Dashboard Capacity Planning to determine the number of switches supported for each deployment.

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 functions normally in a one-node failure scenario. 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 be supported 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 the failure of two Master nodes or all NDFC services will be disrupted.

For virtual Nexus Dashboard (vND) OVA deployments on ESXi environments, it is imperative that promiscuous mode is enabled on the port groups that are 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.

Note that promiscuous mode settings are not required for the port group associated with the Data interface for Layer-3 adjacent network.

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

Cohosting of NDFC Managed mode with Nexus Dashboard Insights

From Release 12.1.1e, you can host NDFC Fabric Controller persona and Nexus Dashboard Insights on the same Nexus Dashboard Cluster in Managed mode to manage fabrics and Nexus Dashboard Insights to monitor the same fabrics. Note that NDFC in Fabric discovery mode, that is, monitored mode with NDI on the same

Nexus Dashboard cluster is supported with NDFC Release 12.0.2f. Cohosting requires 4 physical Nexus Dashboard nodes for a maximum scale of up to 50 switches. This functionality is also supported on NDFC Release 12.1.1e with the corresponding paired Nexus Dashboard Insights release.

Note Nexus Dashboard deployed on KVM doesn't support cohosting NDFC and Insights service on the same Nexus Dashboard cluster.

Note For cohosting NDFC and Insights on the same Nexus Dashboard cluster, the Nexus Dashboard nodes must be Layer 2 adjacent. Support for Layer 3 adjacency for cohosting deployments will be introduced in future releases.

The following table shows the compatible versions for Nexus Dashboard and services.

Services	Compatible Version
Nexus Dashboard	2.2.1h
Nexus Dashboard Insights	6.1.2
Nexus Dashboard Fabric Controller	12.1.1e

The following table shows the system requirements for Nexus Dashboard.

Specification	Supported Scale
Number of physical Nexus Dashboard nodes	5
Number of switches supported	50
Number of flows supported in Nexus Dashboard Insights	10000

Installation of NDFC and NDI on the same Nexus Dashboard

Cisco NDFC can be cohosted with Nexus Dashboard Insights on the same Nexus Dashboard.

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, on page 21 section.
- 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 Cisco 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, on page 26 section.

- 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.

Installing Nexus Dashboard

Install the required form factor of Cisco Nexus Dashboard. For instructions, refer to Cisco Nexus Dashboard Deployment Guide.

Installing NDFC

Refer to Installing Cisco Nexus Dashboard Fabric Controller, on page 25.

Configure NDFC sites on Nexus Dashboard. Refer to the *Adding Sites* section in the Cisco Nexus Dashboard Deployment Guide.

Installing NDI

On the same Nexus Dashboard set up, install the Nexus Dashboard Insights service. Refer to Cisco Nexus Dashboard Insights Deployment Guide, for more information.

Post Installation

After installing compatible versions of NDFC and NDI on the 5-node physical Nexus Dashboard, launch NDFC as Fabric (LAN) Controller. Create Fabric, discover and import switches on NDFC fabric. Nexus Dashboard automatically identifies the NDFC fabric and lists on the Sites page as entities.

Note You must provide the password for each of the sites in the Nexus Dashboard site manager.

Deployment Profile Simplification

Nexus Dashboard deployment profile simplification is intended to help streamline the onboarding of services against a given deployment scale and relieve the task of remembering the cross-connect of deployments.

Beginning with Cisco Nexus Dashboard Release 2.2.1h, resource profile selection has been reduced to several more intuitive parameters directly related to your deployment use case. These parameters, such as number of switches or flows describe the fabric size and use case intent, and allow the cluster to intelligently determine the resources needed for the service. The parameters are categorized as **Network Scale**.

NDFC selects an appropriate profile from among the predefined set of profiles to match the scale.

Note You must restart the services on the Nexus Dashboard after modifying the network scale parameters.

To view or modify the Network Scale parameters on Cisco Nexus Dashboard, perform the following steps:

1. Choose **Nexus Dashboard > Cluster Configuration > Network Scale**.
2. Click the edit icon to modify the network scale parameters.

3. In the **Number of Sites** field, provide the target number of sites for your deployment that this Nexus Dashboard cluster will manage.
4. In the **Number of Switches** field, provide the target number of switch nodes for your deployment.
5. In the **Flows per second** field, provide the target number of flows across sites for LAN/IPFM/SAN-Insights deployments or scale supported by NDFC/NDI cohosted setup.

From Release 12.1.1e, NDFC deployment profiles use a different naming convention for these deployment profiles which is more in line with the scale numbers that each profile supports.

On the fresh install of Nexus Dashboard, the **Network Scale** is empty. We recommend that you define the number of sites, switches, and flows per second in the Network Scale. In such a scenario, the service selects a default profile based on the number of cluster nodes.

If the available cluster compute capacity is less than the desired **Network Scale**, Cisco NDFC installation displays an error. You must resolve the network scale values on Nexus Dashboard and proceed to install NDFC. Note that the recommendations specified in the error message provide useful suggestions about remedial action.

Nexus Dashboard assigns profile names for supported scale values with NDFC. For validated scale numbers, refer to Cisco NDFC Verified Scalability, Release 12.1.1e.

When you upgrade to NDFC 12.1.1e, the individual containers are restarted and the newly spawned 12.1.1e containers start with new resource requests and limit values.

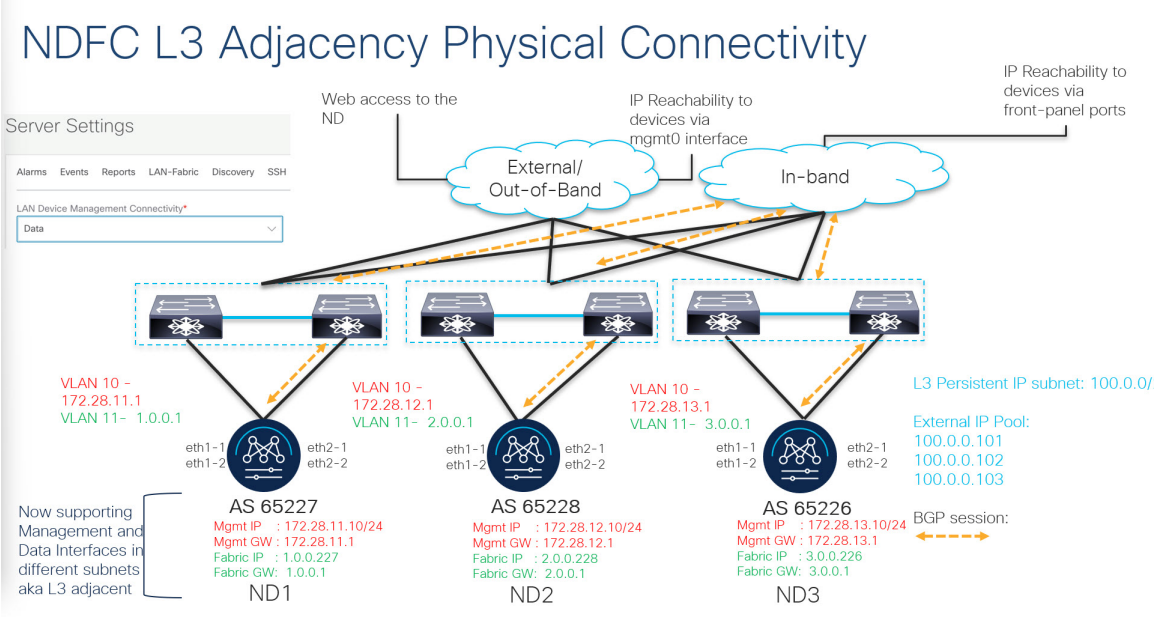
Layer 3 Reachability Between Cluster Nodes

From Release 12.1.1e, NDFC can be deployed as a service on Nexus Dashboard with Layer 3 adjacent nodes. A sample NDFC Layer 3 adjacent Physical Connectivity topology is as shown in the following image.

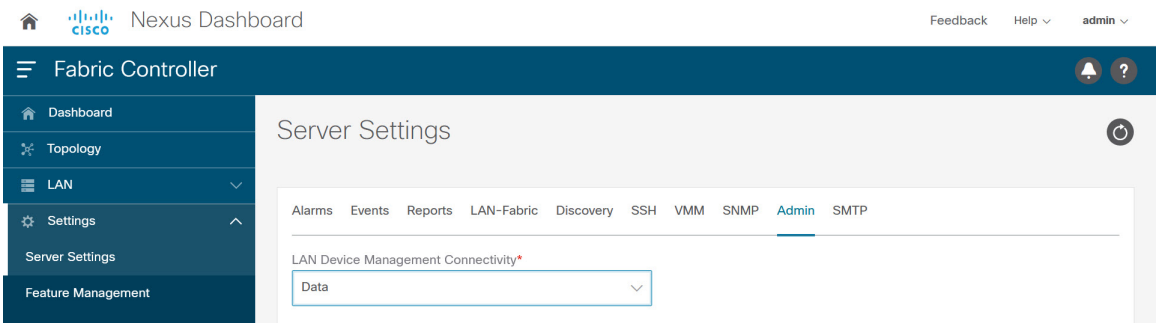
When using Layer 3 adjacency between the Nexus Dashboard nodes on which the NDFC service is running, the persistent IP addresses are advertised using the Nexus Dashboard Data or Fabric interface. The Layer 3 Persistent IP subnet pool must be unique and will be advertised to the fabric using BGP on Nexus Dashboard. Cisco NDFC pods, such as EPL/SNMP Trap/SCP that requires Persistent IPs, are advertised as /32 BGP entries with the next hop of Nexus Dashboard Data Interface. Also, the BGP session between the Nexus Dashboard node and the uplink switches must be configured using directly connected links.

For information about persistent IP addresses, see Persistent IP Requirements for NDFC.

To deploy Layer 3 cluster connectivity, Nexus Dashboard nodes use BGP local and remote autonomous system configuration, along with Data Network gateway of the node to establish eBGP sessions with neighboring routers over the Data interface. As Nexus Dashboard nodes use gateway IPs to establish sessions, during Nexus Dashboard cluster configuration, the neighboring BGP peers must be Layer 2 adjacent. Peers without Layer 2 adjacent connectivity are not supported. You must configure the BGP network correctly to ensure that the Nexus Dashboard routes are transmitted correctly.



Upgrade or modification from an existing Layer-2 adjacent Nexus Dashboard cluster to a Layer-3 adjacent cluster is not supported. When using Layer 3 adjacency, NDFC service is supported only when the switch connectivity is through the Nexus Dashboard Data interface. Choose NDFC **UI > Settings > Admin** tab. From the **LAN Device Management Connectivity** drop-down list, select **Data**.



Nexus Dashboard uses eBGP to publish up-to-date reachability of /32 routes for reaching NDFC features using external service IPs obtained from the Persistent IP subnet. If a node or network fails, the external IPs are not reachable until recovery is complete (if the network can recover itself). After the microservices on the failed node are brought up on one of the existing nodes on the cluster, the eBGP peering from that node will automatically advertise the corresponding /32 persistent IP reachability to the rest of the network, by that means, autorepairing the service disruption.

The following table provides information about different scenarios about Layer 3 adjacent cluster nodes connectivity.

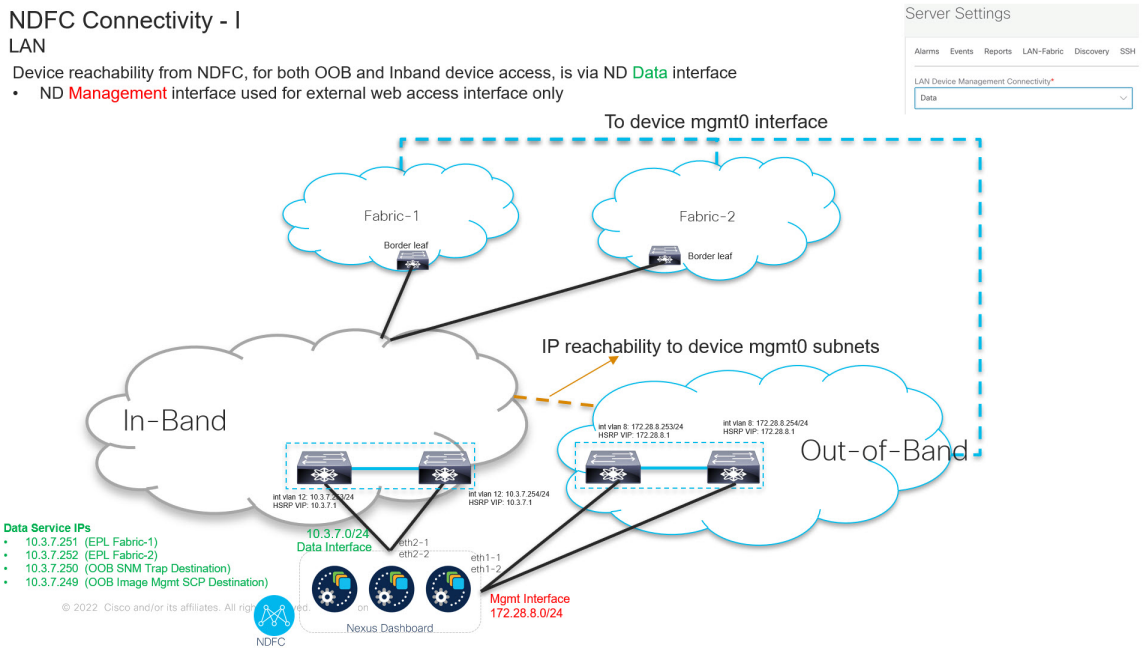
Network details	Support provided
Modify or upgrade from Layer 2 adjacency to Layer 3 adjacency	Not supported; the cluster must be redeployed if necessary.

Network details	Support provided
Modify or upgrade from Layer 3 adjacency to Layer 2 adjacency	Not supported; the cluster must be redeployed if necessary.
NDFC to Switch connectivity over the management interface	Supported (The traffic initiated by the switch to NDFC is routed via the Data Interface)
NDFC to Switch connectivity over Data interface	Supported
Nexus Dashboard BGP traffic over the management interface	Not supported
Cisco Nexus Dashboard BGP traffic over Data interface	Supported
Nexus Dashboard BGP peer L2-Adjacent	Supported
Nexus Dashboard BGP peer L3-Adjacent	Not supported

See Cisco Nexus Dashboard User Guide for more information.

Appendix

The following images show different NDFC connectivity

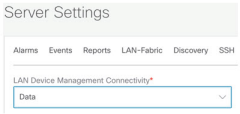


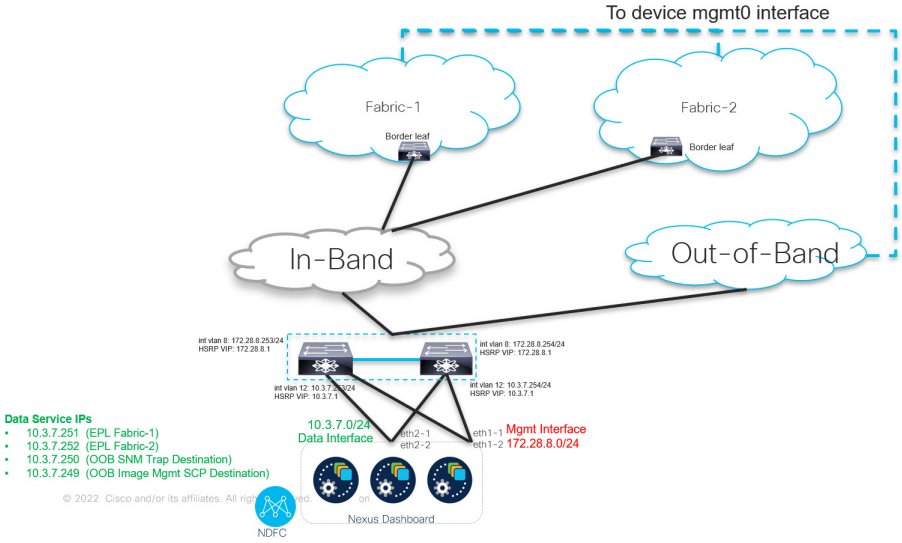
NDFC Connectivity - II

LAN

Device reachability from NDFC, for both OOB and Inband device access, is via ND Data interface

- ND Management interface used for external web access interface only



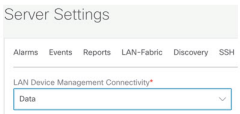


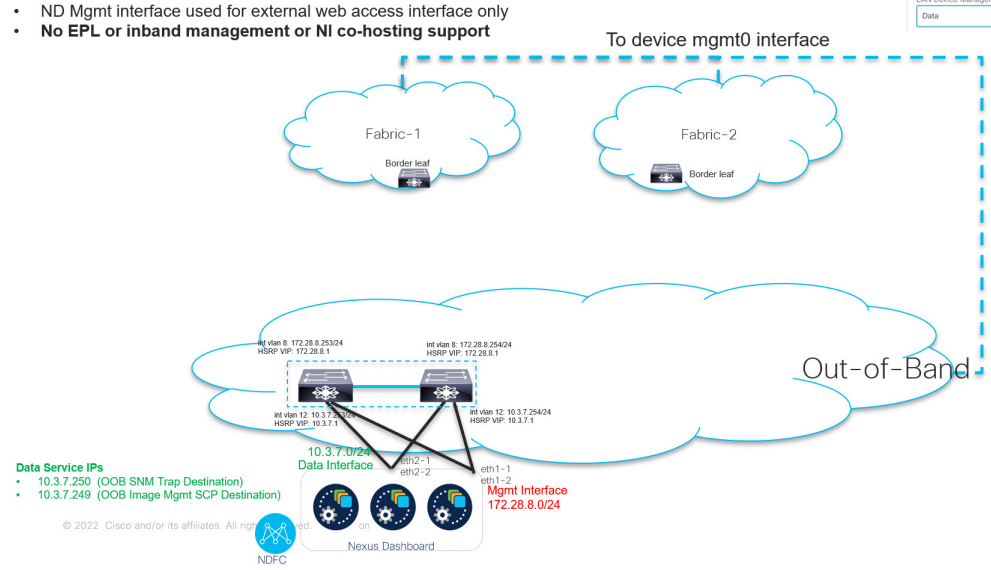
NDFC Connectivity - III

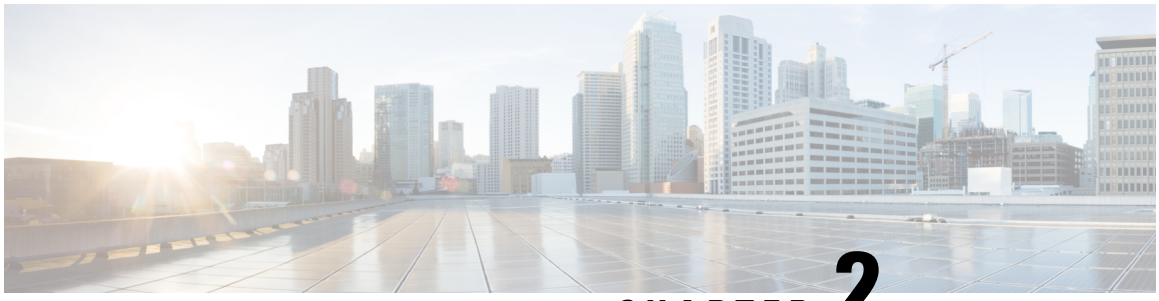
LAN

Device reachability from NDFC for OOB device access is via ND Data interface

- ND Mgmt interface used for external web access interface only
- **No EPL or inband management or NI co-hosting support**







CHAPTER 2

System Requirements

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 12.1.1e.

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 2.2.1h or higher. If you try to upload NDFC 12.1.1e on a Nexus Dashboard version earlier than 2.2.1h, 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

The following table provides information about Server Resource (CPU/Memory) Requirements to run NDFC on top of Nexus Dashboard. Refer to Nexus Dashboard Capacity Planning to determine the number of switches supported for each deployment.

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

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

Deployment Type	Node Type	CPUs	Memory	Storage (Throughput: 40-50MB/s)
SAN Controller	Virtual Node (vND) – app OVA (without SAN Insights)	16vCPUs with physical reservation	64GB with physical reservation	550GB SSD
	Data Node (vND) – Data OVA (with SAN Insights)	32vCPUs with physical reservation	128GB with physical reservation	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
	Virtual Node (vND) Virtual Node (Default Profile on Linux RHEL)	16vCPUs	64 GB	550GB SSD 500GB HDD **Note** SSD+HDD = 550GB
	Virtual Node (vND) Virtual Node (Large Profile on Linux RHEL)	32vCPUs	128 GB	3TB

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. Different nodes that belong to the same Nexus Dashboard cluster can either be Layer-2 adjacent or Layer-3 adjacent. Refer to Layer 3 Reachability Between Cluster Nodes, on page 7 for more information.

Connectivity between the Nexus Dashboard nodes is required on both networks with the round trip time (RTT) not exceeding 50ms. Other applications 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. Refer to Cisco Nexus Dashboard Deployment Guide for more information.

Management Interface	Data Interface	Persistent IPs

Layer 2 adjacent	Layer 2 adjacent	One of the following for LAN:
		• If using default LAN Device Management Connectivity (set to Management):
		  • 2 IPs in management network for SNMP/Syslog and SCP services
		  • Plus one IP per fabric for EPL (if enabled) in data network
		  • Plus one IP for Telemetry receiver in management network if IP Fabric for Media is enabled
		• If LAN Device Management Connectivity is set to Data:
		  • 2 IPs in data network for SNMP/Syslog and SCP services
		  • Plus one IP per fabric for EPL (if enabled) in data network
		  • Plus one IP for Telemetry receiver in data network if IP Fabric for Media is enabled
		For SAN:
		• 2 IPs in data network for SNMP/Syslog and SCP services
		• Plus one IP per Nexus Dashboard node in data network if SAN Insights receivers is enabled

Layer 3 adjacent	Layer 3 adjacent	For LAN: • LAN Device Management Connectivity on NDFC must be set to Data • 2 IPs for SNMP/Syslog and SCP/POAP services • Plus one IP per fabric for EPL These IPs must be part of a subnet that is different from Nexus Dashboard management and Nexus Dashboard data subnets associated with any of Nexus Dashboard nodes. These IPs must belong to the Layer-3 External Persistent Service Pool. **Note** SAN Controller and IP Fabric for Media modes are not supported in this deployment.

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 that are associated with the Nexus Dashboard Management and/or Data vNICs where IP stickiness is required. In addition to enabling promiscuous mode, you must also enable "Mac Address change" and "Forged transmits". The Persistent IP addresses are given to the pods (for example, SNMP Trap or Syslog receiver, Endpoint Locator instance per Fabric, SAN Insights receiver, and so on). 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 that matches the Source-MAC that is associated with that vNIC. If 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, enable the required settings on the VMware side to allow this traffic to flow seamlessly in and out of the vND node.

When vND nodes are deployed with the new Layer-3 HA feature, you need not enable Promiscuous mode on the vND vNIC interfaces. Promiscuous mode is required only for vND deployments when the vNDs are layer-2 adjacent from each other.

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

Nexus Dashboard Fabric Controller Ports

In addition to the ports required by the Nexus Dashboard (ND) cluster nodes, the following ports are required by the Nexus Dashboard Fabric Controller (NDFC) service.

Note The following ports apply to the Nexus Dashboard management network and/or data network interfaces depending on which interface provides IP reachability from the NDFC service to the switches.

Table 3: Nexus Dashboard Fabric Controller Ports

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
SSH	22	TCP	Out	SSH is a basic mechanism for accessing devices.
SCP	22	TCP	Out	SCP clients archiving NDFC backup files to remote server.

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
SMTP	25	TCP	Out	SMTP port is configurable through NDFC's **Server Settings** menu. This is an optional feature.
DHCP	67	UDP	In	If NDFC local DHCP server is configured for Bootstrap/POAP purposes. This applies to LAN deployments only. **Note** When using NDFC as a local DHCP server for POAP purposes, all ND master node IPs must be configured as DHCP relays. Whether the ND nodes' management or data IPs are bound to the DHCP server is determined by the LAN Device Management Connectivity in the NDFC Server Settings.
DHCP	68	UDP	Out	
SNMP	161	TCP/UDP	Out	SNMP traffic from NDFC to devices.
HTTPS/HTTP (NX-API)	443/80	TCP	Out	NX-API HTTPS/HTTP client connects to device NX-API server on port 443/80, which is also configurable. NX-API is an optional feature, used by limited set of NDFC functions. This applies to LAN deployments only.
HTTPS (vCenter, Kubernetes, OpenStack, Discovery)	443	TCP	Out	NDFC provides an integrated host and physical network topology view by correlating the information obtained from registered VMM domains, such as VMware vCenter or OpenStack, as well as container orchestrators, such as Kubernetes. This is an optional feature

Note The following ports apply to the External Service IPs, also known as persistent IPs, used by some of the NDFC services. These External Service IPs may come from certain subnet pools, depending on the type of deployment:

- For LAN deployments, these External Service IPs may come from the Nexus Dashboard management subnet pool or the data subnet pool, depending on the configured settings.
- For SAN deployments, these External Service IPs come from the Nexus Dashboard data subnet pool.

Table 4: Nexus Dashboard Fabric Controller Persistent IP Ports

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
SCP	22	TCP	In	SCP is used by various features to transfer files between devices and the NDFC service. The NDFC SCP service serves as the SCP server for both downloads and uploads. SCP is also used by the POAP client on the devices to download POAP-related files. The SCP-POAP service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings.
TFTP (POAP)	69	TCP	In	Only used for device zero-touch provisioning via POAP, where devices can send (limited jailed write-only access to NDFC) basic inventory information to NDFC to start secure POAP communication. NDFC Bootstrap or POAP can be configured for TFTP or HTTP/HTTPS. The SCP-POAP service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings. This applies to LAN deployments only.

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
HTTP (POAP)	80	TCP	In	Only used for device zero-touch provisioning via POAP, where devices can send (limited jailed write-only access to NDFC) basic inventory information to NDFC to start secure POAP communication. NDFC Bootstrap or POAP can be configured for TFTP or HTTP/HTTPS. The SCP-POAP service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings. This applies to LAN deployments only.
BGP	179	TCP	In/Out	For Endpoint Locator, per fabric where it is enabled, an EPL service is spawned with its own persistent IP. This service is always associated with the Nexus Dashboard data interface. NDFC EPL service peers with the appropriate BGP entity (typically BGP Route-Reflectors) on the fabric to get BGP updates needed to track endpoint information. This feature is only applicable for VXLAN BGP EVPN fabric deployments. This applies to LAN deployments only.
HTTPS (POAP)	443	TCP	In	Secure POAP is accomplished via the NDFC HTTPS Server on port 443. The HTTPS server is bound to the SCP-POAP service and uses the same persistent IP assigned to that pod. The SCP-POAP service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings. This applies to LAN deployments only.

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
Syslog	514	UDP	In	When NDFC is configured as a Syslog server, Syslogs from the devices are sent out toward the persistent IP associated with the SNMP-Trap/Syslog service pod The SNMP-Trap-Syslog service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings
SCP	2022	TCP	Out	Transport tech-support file from persistent IP of NDFC POAP-SCP pod to a separate ND cluster running Nexus Dashboard Insights. The SCP-POAP service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings
SNMP Trap	2162	UDP	In	SNMP traps from devices to NDFC are sent out toward the persistent IP associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in NDFC has a persistent IP that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings
GRPC (Telemetry)	33000	TCP	In	SAN Insights Telemetry Server which receives SAN data (such as storage, hosts, flows, and so on) over GRPC transport tied to NDFC Persistent IP. This is enabled on SAN deployments only.

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
GRPC (Telemetry)	50051	TCP	In	Information related to multicast flows for IP Fabric for Media deployments as well as PTP for general LAN deployments is streamed out via software telemetry to a persistent IP associated with a NDFC GRPC receiver service pod. This is enabled on LAN and Media deployments only.

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.

Supported Web Browsers

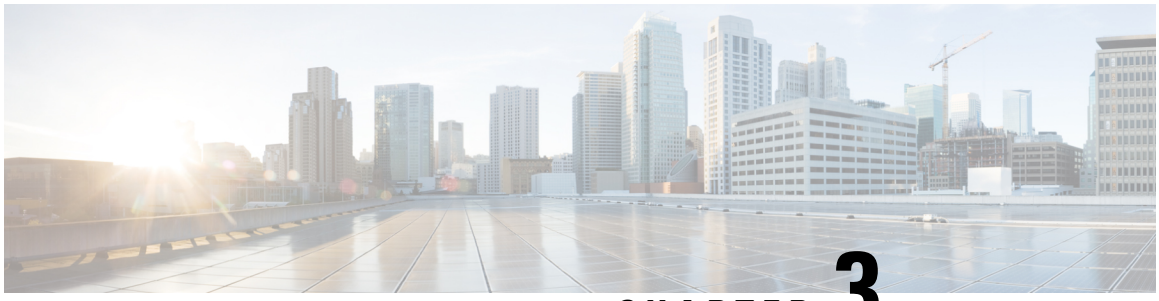
Cisco Nexus Dashboard Fabric Controller is supported on the following web browsers:

- Google Chrome version 101.0.4951.64
- Microsoft Edge version 101.0.1210.47 (64-bit)
- Mozilla Firefox version 100.0.1 (64-bit)

Other Supported Software

The following table lists the other software that is supported by Cisco Nexus Dashboard Fabric Controller Release 12.1.1e.

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, 1.2, and 1.3



CHAPTER 3

Prerequisites

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

Prerequisites

This section provides detailed information about the prerequisites that you must complete before launching Cisco Nexus Dashboard Fabric Controller.

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.

Note The Fabric Controller service cannot recover from a two `master` node failure of the Nexus Dashboard cluster where it is deployed. As a result, we recommend that you maintain at least one `standby` node in your Nexus Dashboard cluster and create regular backups of your NDFC configuration, as described in the **Operations** > **Backup and Restore** chapter of the *Cisco NDFC-Fabric Controller Configuration Guide* for your release.

If you run into a situation where two `master` nodes of your Nexus Dashboard cluster fail, you can follow the instructions described in the **Troubleshooting** > **Replacing Two Master Nodes with Standby Nodes** section of the *Cisco Nexus Dashboard User Guide* for your release to recover the cluster and NDFC configuration.

NDFC Release	Minimum Nexus Dashboard Release
Release 12.1.1e	Cisco Nexus Dashboard, Release 2.2.1h or later

The following Nexus Dashboard form factors are supported with NDFC deployments:

- Cisco Nexus Dashboard physical appliance (.iso)
- VMware ESX (.ova)
  - ESXi 6.7

- ESXi 7.0

- Linux KVM (.qcow2)
  - CentOS 7.9

- Existing Red Hat Enterprise Linux (SAN Controller persona only)
  - RedHat Enterprise Linux (RHEL) 8.4

Sizing of the Cluster

Refer to your release-specific Verified Scalability Guide for NDFC for information about the number of Nexus Dashboard cluster nodes required for the desired scale.

Nexus Dashboard supports co-hosting 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.

Network Connectivity

- **LAN Device Management Connectivity** – Fabric discovery and Fabric controller features can manage Devices over both Management Network and Data Network of ND Cluster Appliances.
- When using Management network, add the routes to all subnets of the devices that NDFC needs to manage or monitor in the Management Network.
- When using Data Network, add the route towards a DHCP relay server in the Data Network.
- SAN controller persona requires all the devices to be reachable via the Data network of Nexus Dashboard cluster nodes.

Persistent IP address

- Persistent IPs are needed by NDFC for multiple use cases.
- If Nexus Dashboard cluster is deployed over a Layer 3 separation of network, configure BGP on all ND nodes.
- All Persistent IPs must be configured such that they are not part of any of the Nexus Dashboard nodes' subnets. This is supported only when LAN Device Management connectivity is Data. This is not supported with a cluster that co-hosts Nexus Dashboard Insights with NDFC.
- If Nexus Dashboard cluster is deployed with all nodes in the same subnet, persistent IPs can be configured to be from the same subnet.

  In this case, persistent IPs must belong to the network chosen based on LAN Device Management connectivity setting in the NDFC Server Settings.

  For more information, see Persistent IP Requirements for NDFC.
- Fabric Discovery – 2 IPs based on LAN Device Management Connectivity.
- Fabric Controller – 2 based on LAN Device Management connectivity and 1 for each EPL fabric instance

- Fabric Controller with IPFM – 2 based on LAN Device Management connectivity
  - 1 IP for ingest of software Telemetry for a single node IPFM deployment
  - 3 IPs for ingest of software Telemetry for a three node IPFM deployment
- SAN Controller:
  - SAN Controller 3 Node Cluster – 2 IPs for Data Network + 3 IPs for SAN Insights
  - SAN Controller 1 Node Cluster – 2 IPs for Data Network + 1 IP for SAN Insights

POAP related requirements

- Devices must support POAP.
- Device must have no start up configuration or **boot poap enable** command must be configured to bypass the start up configuration and enter the POAP mode.
- DHCP server with scope defined.
- The script server that stores POAP script and devices' configuration files must be accessible.
- Software and Image Repository server must be used to store software images for the devices.

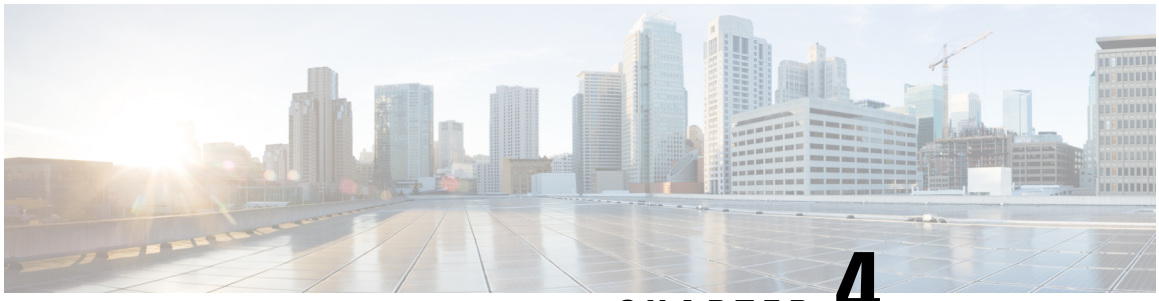
Network Time Protocol (NTP)

Nexus Dashboard nodes must be in synchronization with the NTP Server; however, there can be latency of up to 1 second between the Nexus Dashboard nodes. If the latency is greater than or equal to 1 second between the Nexus Dashboard nodes, this may result in unreliable operations on the NDFC cluster.

Restoring configurations

If this system is to be restored from the previously taken backup, you must upload a backup file that was taken from the same version.

Prerequisites



CHAPTER 4

Installing Cisco Nexus Dashboard Fabric Controller

This chapter contains the following sections:

Installing Nexus Dashboard Fabric Controller Service Using App Store

To install Cisco Nexus Dashboard Fabric Controller Release 12.1.1e 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, on page 21.
- If you choose to deploy NDFC on Nexus Dashboard on KVM, you must create bridge interfaces on Linux before installing Nexus Dashboard on KVM with Centos7. Ensure that you use bridge interfaces and do not allow other interfaces during Nexus Dashboard installation.
- 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.

  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, on page 26.
- 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 12.1.1e 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 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 6 Click on **Open** to launch Cisco Nexus Dashboard Fabric Controller Web UI.

Note 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.

The **Nexus Dashboard Fabric Controller Web UI** opens in a new browser. The **Feature Management** window appears.

Note If External Service Pool IP addresses are not configured, an error message appears. Go to **Nexus Dashboard Web 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.

Three cards namely **Fabric Discovery**, **Fabric Controller**, and **SAN Controller** is displayed.

Step 7 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 8 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**.

Installing Nexus Dashboard Fabric Controller Service Manually

To manually upload and install Cisco Nexus Dashboard Fabric Controller Release 12.1.1e 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, on page 21.
- If you choose to deploy NDFC on Nexus Dashboard on KVM, you must create bridge interfaces on Linux before installing Nexus Dashboard on KVM with Centos7. Ensure that you use bridge interfaces and do not allow other interfaces during Nexus Dashboard installation.
- 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 12.1.1e 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 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 10 Click on **Open** to launch Cisco Nexus Dashboard Fabric Controller Web UI.

Note 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.

The **Nexus Dashboard Fabric Controller Web UI** opens in a new browser. The **Feature Management** window appears.

Note If External Service Pool IP addresses are not configured, an error message appears. Go to **Nexus Dashboard Web 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.

Three cards namely **Fabric Discovery**, **Fabric Controller**, and **SAN Controller** is displayed.

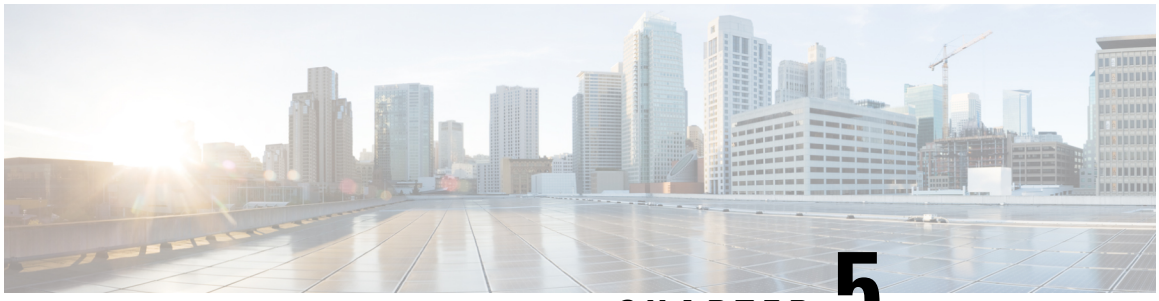
Step 11 Based on the requirement, select the deployment.

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 12 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**.



CHAPTER 5

Upgrading Cisco Nexus Dashboard Fabric Controller

This chapter provides information about upgrading Cisco Nexus Dashboard Fabric Controller, and contains the following sections:

Upgrade Paths to Release 12.1.1e

The following table summarizes the type of upgrade that you must follow to upgrade to Release 12.1.1e.

Go to Software Download to download the Upgrade Tool scripts.

Current Release Number	Deployment Type	Compatible Nexus Dashboard Version in Current Release	Upgrade type when upgrade to Release 12.1.1e
12.0.2f	All	2.1.2d	1. Backup on **Web UI** > **Operations** > **Backup & Restore** 2. Disable **Nexus Dashboard Fabric Controller** service on **Nexus Dashboard** 3. Upgrade **Nexus Dashboard** version to 2.2.1h 4. Enable **Nexus Dashboard Fabric Controller** service on **Nexus Dashboard** 5. Upgrade **NDFC** application to 12.1.1e
12.0.1a	All	2.1.1e	1. Backup on **Web UI** > **Operations** > **Backup & Restore** 2. Disable **Nexus Dashboard Fabric Controller** service on **Nexus Dashboard** 3. Upgrade Nexus Dashboard version to 2.2.1h 4. Enable **Nexus Dashboard Fabric Controller** service on **Nexus Dashboard** 5. Upgrade **NDFC** application to 12.1.1e.
11.5(4)	All	Not Applicable	Not Supported
11.5(3)	LAN Fabric Deployment **Note** Media Controller and all SAN deployments are not supported in Release 11.5(3).	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**

Current Release Number	Deployment Type	Compatible Nexus Dashboard Version in Current Release	Upgrade type when upgrade to Release 12.1.1e
11.5(2)	SAN Deployment on Windows and Linux	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**
	SAN Deployment on OVA/ISO/SE	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**
	LAN Fabric Deployment on OVA/ISO/SE	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**

Current Release Number	Deployment Type	Compatible Nexus Dashboard Version in Current Release	Upgrade type when upgrade to Release 12.1.1e
11.5(1)	SAN Deployment on Windows and Linux	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**
	SAN Deployment on OVA/ISO/SE	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**
	LAN Fabric Deployment on OVA/ISO/SE	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **Web UI** > **Operations** > **Backup & Restore**
	Media Controller Deployment on OVA/ISO	Not Applicable	1. Backup using **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** 2. Install **Nexus Dashboard** version 2.2.1h 3. Install **NDFC** Release 12.1.1e 4. Restore on **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] [3]	Persona Enabled in NDFC 12.1.1e 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), 11.5(2) or 11.5(3).
2 Upgrade to NDFC 12 from DCNM 11.5(3) is supported for LAN Fabric Deployments only. DCNM Release 11.5(3) does not support Media Controller and SAN deployments.
3 Upgrade from 11.5(4) is not supported.

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 12.1.1e.

Note 11.5(x) includes Releases 11.5(1), 11.5(2), and 11.5(3) only. Upgrade from 11.5(4) to 12.1.1e is not supported.

Feature in DCNM 11.5(x)	Upgrade Support
Nexus Dashboard Insights configured Refer to Cisco Nexus Dashboard 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
Fabric Backups	Not supported
Report Definitions and Reports	Not supported
Switch images and Image Management policies	Not supported
SAN CLI templates	Not carried over from 11.5(x) to 12.1.1e

Feature in DCNM 11.5(x)	Upgrade Support
Switch images/Image Management data	Not carried over from 11.5(x) to 12.1.1e
Slow drain data	Not carried over from 11.5(x) to 12.1.1e
Infoblox configuration	Not carried over from 11.5(x) to 12.1.1e
Endpoint Locator configuration	You must reconfigure Endpoint Locator (EPL) post upgrade to Release 12.1.1e. However, historical data is retained up to a maximum size of 500 MB.
Alarm Policy configuration	Not carried over from 11.5(x) to 12.1.1e
Performance Management data	CPU/Memory/Interface statistics up to 90 days is restored post upgrade.

Note SAN Insights and VMM Visualizer features are not enabled after restore. You must choose check boxes on **Settings** > **Feature Management** and click **Save** to enable these features after restore.

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 12.1.1e.

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

Stop Performance Management collection before running backup script for large scaled DCNM. To stop the Performance Management collection, perform the following steps:

- Navigate to **Administration** > **DCNM Server** > **Server Status**.
- Click on **Stop Service** of **Performance Collector** and wait a few seconds.
- Click on the **refresh** icon on the top right to check the status. Make sure it shows **Stopped**.

The backup tool collects last 90 days Performance Management data.

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 DCNM **Web 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.

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.

Ensure that you have enabled execution permissions to the Upgrade tool. Use **chmod +x .** to enable executable permissions.

For OVA/ISO-

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

For Windows/Linux-

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_LIN_WIN
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 12.1.1e or not.

Note The backup that is generated by using this tool can be used to restore data on NDFC 12.1.1e only.

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 12.1.1e or
not.
If upgrade to NDFC 12.1.1e 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 12.1.1e
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 12.1.1e or not.

If upgrade to NDFC 12.1.1e 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 12.1.1e

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 12.1.1e
or not.

If upgrade to NDFC 12.1.1e 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 NDFC Release 12.0.x to NDFC Release 12.1.1e

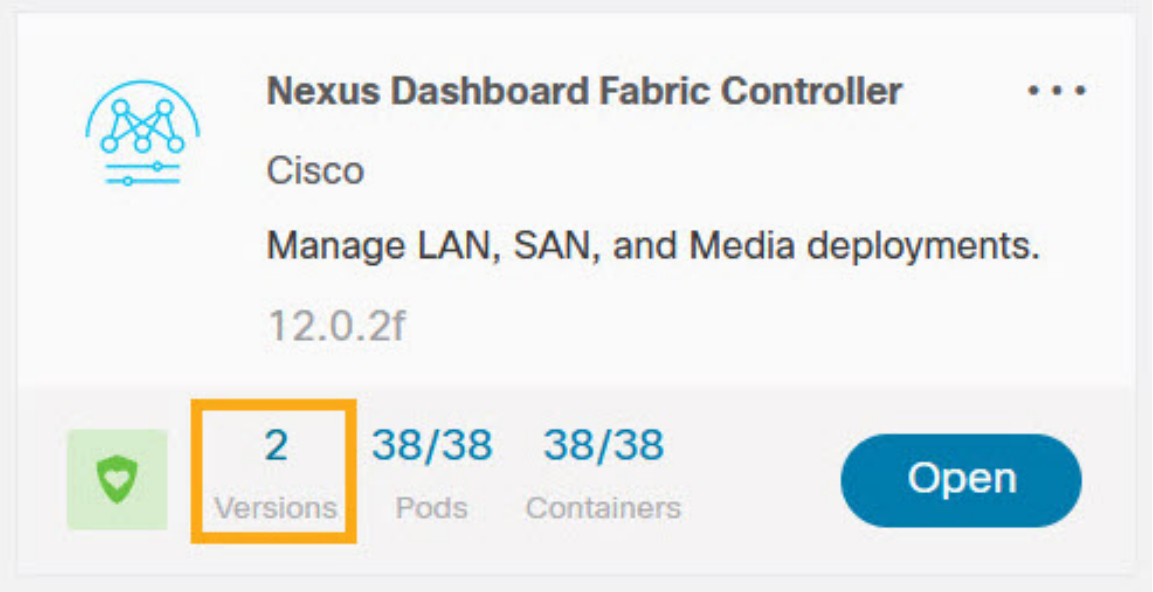
To upgrade to Cisco NDFC Release 12.1.1e from NDFC Release 12.0.1a or 12.0.2f, perform the following steps:

Before you begin

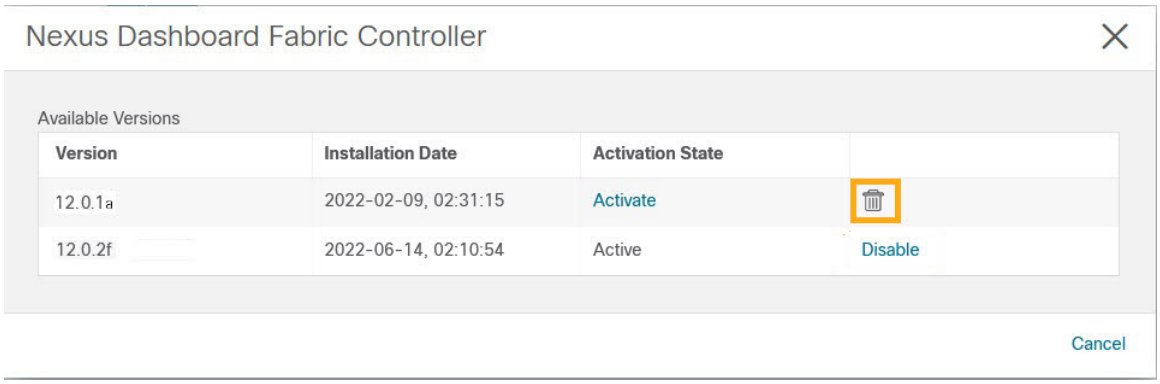
Note Release 12.0.x includes 12.0.1a and 12.0.2f releases.

- Ensure that NDFC Release 12.0.x is up and operational before you begin this procedure.
- Cisco NDFC 12.1.1e is compatible with Nexus Dashboard Release 2.2.1h or later. Upgrade the Nexus Dashboard to Release 2.2.1h. For instructions, refer to Upgrading Nexus Dashboard.
- You cannot have multiple versions of NDFC service on Nexus Dashboard. Retain the current operational version, and delete the other NDFC versions on Nexus Dashboard before proceeding to upgrade.

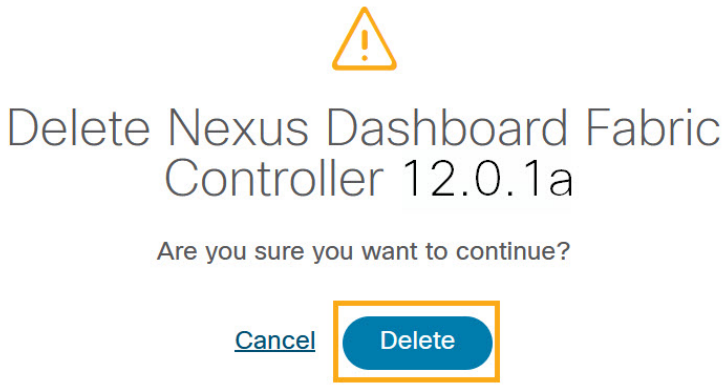
  To check the number of NDFC versions, choose **Nexus Dashboard > Services > Installed Services**. The number of versions is displayed on the NDFC service under **Versions**.



Click on ellipsis (…) icon and choose **Available Versions**. NDFC versions are displayed. Note that if there is one version, **Available Versions** option is not seen in the drop-down list.



Click delete icon to remove the NDFC service. Click **Delete** on the confirmation message.



- If you've enabled preview features in 12.0.x, you must disable those features.
  - On the Web UI, choose **Settings > Feature Management**. Ensure that you the uncheck the BETA features.
  - For Fabric Controller, on the Web UI, choose **Settings > Server Settings > LAN Fabric** tab. Ensure that the **Enable Preview Features** check box is unchecked.

Procedure

Step 1 Take a backup of NDFC data on **Web UI > Operations > Backup & Restore**.

Ensure that NDFC Release 12.0.x is up and operational when you take the backup. Save the backup file in a secured directory. See *Backup & Restore chapter* in the *Cisco NDFC Configuration Guide* for more information.

Note Ensure that there is only one version on NDFC enabled on Nexus Dashboard.

Step 2 On the **Nexus Dashboard Fabric Controller** card, click on ellipsis (**…**) icon. From the drop-down list, select **Disable**.

Caution Upgrade fails if the NDFC 12.0.x service is not disabled before upgrading the Nexus Dashboard.

Step 3 Upgrade the Nexus Dashboard to Release 2.2.1h.

For instructions, see Upgrading Nexus Dashboard.

Note Do not perform any operations on Nexus Dashboard or on any other services while the Nexus Dashboard upgrade is in progress.

Step 4 After the upgrade is completed, launch **Nexus Dashboard**.

Step 5 On the **Nexus Dashboard Fabric Controller Version: 12.0.x** card, click on ellipsis (**…**) icon. From the drop-down list, select **Enable**.

Note Ensure that you enable NDFC service only after the Nexus Dashboard upgrade process is completed.

Wait until all the pods and containers are up and running.

Step 6 Install NDFC Release 12.1.1e service on the Nexus Dashboard.

To install NDFC 12.1.1e from **Cisco App Store**, perform the following steps:

a) On the **Nexus Dashboard > Services > App Store** tab, locate **Nexus Dashboard Fabric Controller** service.

Click **Update**.

b) On the **License Agreement** screen, click **Agree and Download** to begin download.

NDFC 12.1.1e service is downloaded and installed on Nexus Dashboard.

c) After the **Nexus Dashboard Fabric Controller** service card shows **Installed**, click on **Installed Services** tab.

d) On NDFC card, click on the ellipsis (**…**) icon and choose **Disable**.

Click **Disable** on the confirmation screen to disable the previous version.

The **Nexus Dashboard Fabric Controller** service card now displays the version as 12.1.1e.

To install NDFC from **Nexus Dashboard > Services > Actions > Upload Service**, perform the following steps:

a) On the **Nexus Dashboard > Services** tab, from the **Actions** drop-down list, choose **Upload Service**.

b) Go to Cisco DC App Center to view and download NDFC service.

On the Cisco DC App Center, identify the Nexus Dashboard Fabric Controller card with **Version:** 12.1.1e.

c) Click on the download icon to download NDFC service.

d) Click **Agree and download** to accept the **License Agreement**.

Save the `Cisco-ndfc-12.1.1e.nap` file to a local or remote directory.

e) 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 NDFC application is saved.
- If you select **Local**, click **Browse** and navigate to the location where the NDFC application is saved. Select the application and click **Open**.

f) Click **Upload**.

Another 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.

After installation, Nexus Dashboard Fabric Controller service appears in the **Services Catalog**. Note that Versions displays as 2 on the Nexus Dashboard Fabric Controller card.

Step 7 On the **Nexus Dashboard Fabric Controller** card, click on ellipsis (…) icon.

From the drop-down list, choose **Available Versions**.

Step 8 Click **Activate** on Nexus Dashboard Fabric Controller 12.1.1e version to initiate upgrade activation.

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 9 Click **Open** to launch Cisco Nexus Dashboard Fabric Controller Release 12.1.1e Web UI.

Note The single sign-on (SSO) feature allows you to log in to the application using the same credentials that you used for Nexus Dashboard.

Upgrading from Cisco DCNM Release 11.5(x) to Cisco NDFC Release 12.1.1e

To upgrade to Cisco Nexus Dashboard Fabric Controller Release 12.1.1e 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.

- Both Nexus Dashboard Release 2.2.1h is supported. To upgrade with Nexus Dashboard Release 2.2.1e, ensure that you **Disable** NDFC before upgrading Nexus Dashboard.

  Refer to Upgrading Nexus Dashboard for instructions to upgrade Nexus Dashboard.

- 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, on page 26.
  - Installing Nexus Dashboard Fabric Controller Service Using App Store, on page 25

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.

Note Select **Config only** or **Full** based on the backup that was created on DCNM Release 11.5(x).

- Choose **Config only** to restore only configuration data.

  You can choose either **Config only** or **Full** backup files.

- Choose **Full** to restore all previous version data to this application.

  You must choose **Full** backup files.

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.
  a. Open the directory where you've saved the backup file.
  b. Drag and drop the backup file to the **Restore now** window

     or

     Click **Browse**. Navigate to the directory where you've saved the backup file. Select the backup file and click **Open**.
  c. Enter the **Encryption Key** to the backup file.

- Choose **Import from SCP server** or **Import from SFTP server**if the backup file is stored in a remote directory.
  a. In the **Server** field, provide the server IP Address.
  b. In the **File Path** field, provide the relative file path to the backup file.
  c. In the **Username** and **Password** fields, enter appropriate details.
  d. In the **Encryption Key** field, enter the Encryption Key to the backup file.

Step 6 (Optional) Check the **Ignore External Service IP Configuration** check box.

If the Ignore External Service IP Configuration check box is selected, then the external service IP configuration is ignored. This selection allows you to take a backup on a system and restore it on a different system, with different management and/or data subnets.

This option does not have any impact during an upgrade from Cisco DCNM 11.5(x) to Cisco NDFC.

Step 7 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.

Note 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.

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.

Feature Management

After restoring the backup, based on the type of deployment, Nexus Dashboard Fabric Controller Release 12.1.1e is deployed with one of the following personalities:

- Fabric Controller
- SAN Controller

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**.

Note There are caveats associated with features enabled on DCNM 11.5(x) with respect to upgrade to NDFC, Release 12.1.1e. For more information, see Feature Compatibility Post Upgrade, on page 33 .

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

From/To	Fabric Discovery	Fabric Controller	SAN Controller
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 12.1.1e.

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 12.1.1e:

- 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 12.1.1e, trap IP address belongs to	Result
LAN Fabric Media Controller	eth1 (or vip1 for HA systems)	Management	Belongs to Management subnet	Honored There is no configuration difference. No further action required.

Deployment Type in Release 11.5(x)	In 11.5(x), trap IP address is collected from	LAN Device Management Connectivity	In 12.1.1e, trap IP address belongs to	Result
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. 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**.
LAN Fabric Media Controller	eth0 (or vip0 for HA systems)	Data	Belongs to Data subnet	Honored There is no configuration difference. No further action required.
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. 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**.

Deployment Type in Release 11.5(x)	In 11.5(x), trap IP address is collected from	LAN Device Management Connectivity	In 12.1.1e, trap IP address belongs to	Result
SAN Management	OVA/ISO – • trap.registaddress (if set) • eth0 (if trap.registaddress is not set) Windows/Linux – • trap.registaddress (if set) • Interface based on event-manager algorithm (if trap.registaddress is not set	Not applicable	Belongs to Data subnet	Honored There is no configuration difference. No further action required.
		Not applicable	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP.

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 12.1.1e[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.

Default Templates available with Cisco NDFC

The following table provides the details of default templates available with Cisco Nexus Dashboard Fabric Controller.

Note A change in the template is defined as changes to the template variables and body contents. Changes to comment strings are ignored.

Category (Fabric/Link/Interface)	Template Name	Is changed from Cisco NDFC Release 12.0.1a to 12.1.1e		Is changed from Cisco NDFC Release 12.0.2f to 12.1.1e	
		Yes/No	Change Description	Yes/No	Change Description
Fabric	Easy_Fabric	Yes	New features/bug fix	Yes	New features/bug fix
	Easy_Fabric_eBGP	Yes	New features/bug fix	Yes	New features/bug fix
	Easy_Fabric_IOS_XE	Yes	New features/bug fix	Yes	New features/bug fix
	Easy_Fabric_IPFM	Yes	New features/bug fix	Yes	New features/bug fix
	LAN_Classic	Yes	New features/bug fix	Yes	New features/bug fix
	Fabric_Group	No	No Change	No	No Change
	IPFM_Classic	Yes	New features/bug fix	Yes	New features/bug fix
	LAN_Monitor	Yes	New features/bug fix	No	No Change
	External_Fabric	Yes	New features/bug fix	Yes	New features/bug fix
	MSD_Fabric	Yes	New features/bug fix	Yes	New features/bug fix

Category (Fabric/Link/Interface)	Template Name	Is changed from Cisco NDFC Release 12.0.1a to 12.1.1e		Is changed from Cisco NDFC Release 12.0.2f to 12.1.1e	
		Yes/No	Change Description	Yes/No	Change Description
Interface	int_access_host	Yes	New features/bug fix	Yes	New features/bug fix
	int_dot1q_tunnel_host	Yes	New features/bug fix	Yes	New features/bug fix
	int_freeform	No	No change	No	No change
	int_l3_port_channel	Yes	New features/bug fix	Yes	New features/bug fix
	int_loopback	No	No change	No	No change
	int_mgmt	Yes	New features/bug fix	Yes	New features/bug fix
	int_monitor_ethernet	Yes	New features/bug fix	Yes	New features/bug fix
	int_monitor_port_channel	No	No change	No	No change
	int_monitor_subif	No	No change	No	No change
	int_monitor_vpc	Not applicable	Not applicable	No	No Change
	int_mpls_loopback	No	No change	No	No change
	int_multisite_loopback	No	No change	No	No change
	int_nve	No	No change	No	No change
	int_port_channel_aa_fex	Yes	New features/bug fix	Yes	New features/bug fix
	int_port_channel_access_host	Yes	New features/bug fix	No	No change
	int_port_channel_dot1q_tunnel_host	Yes	New features/bug fix	No	No change
	int_port_channel_fex	Yes	New features/bug fix	Yes	New features/bug fix
	int_port_channel_pvlan_host	Yes	New features/bug fix	No	No change
	int_port_channel_trunk_host	Yes	New features/bug fix	No	No change

Category (Fabric/Link/Interface)	Template Name	Is changed from Cisco NDFC Release 12.0.1a to 12.1.1e		Is changed from Cisco NDFC Release 12.0.2f to 12.1.1e	
		Yes/No	Change Description	Yes/No	Change Description
	int_pvlan_host	Yes	New features/bug fix	No	No change
	int_routed_host	Yes	New features/bug fix	No	No change
	int_subif	Yes	New features/bug fix	No	No change
	int_vlan	Yes	New features/bug fix	No	No change
	int_vlan_admin_state	No	No change	No	No change
	int_trunk_host	Yes	New features/bug fix	No	No change
	int_vpc_access_host	Yes	New features/bug fix	No	No change
	int_vpc_dot1q_tunnel	Yes	New features/bug fix	No	No change
	int_vpc_peer_keepalive_ll_1	No	No Change	No	No Change
	int_vpc_peer_link_po	Yes	New features/bug fix	No	No change
	int_vpc_pvlan_host	Yes	New features/bug fix	No	No change
	int_vpc_trunk_host	Yes	New features/bug fix	No	No change
	int_ipfm_access_host	Yes	New features/bug fix	No	No change
	int_ipfm_l3_port	Yes	New features/bug fix	No	No change
	int_ipfm_portchannel_access_host	Yes	New features/bug fix	No	No change
	int_ipfm_portchannel_trunk_host	Yes	New features/bug fix	No	No change
	int_ipfm_trunk_host	Yes	New features/bug fix	No	No change

Category (Fabric/Link/Interface)	Template Name	Is changed from Cisco NDFC Release 12.0.1a to 12.1.1e		Is changed from Cisco NDFC Release 12.0.2f to 12.1.1e	
		Yes/No	Change Description	Yes/No	Change Description
	int_ipfm_vlan	No	No change	No	No change
Link	int_intra_fabric_ipv6_link_local	Yes	New features/bug fix	Yes	New features/bug fix
	int_intra_fabric_num_link	Yes	New features/bug fix	Yes	New features/bug fix
	int_intra_fabric_unnum_link	Yes	New features/bug fix	Yes	New features/bug fix
	int_intra_vpc_peer_keep_alive_link	No	No Change	No	No Change
	int_pre_provision_intra_fabric_link	No	No Change	No	No Change
	int_ipfm_intra_fabric_num_link	Yes	New features/bug fix	Yes	New features/bug fix
	int_mpls_xe_intra_fabric_num_link	No	No Change	No	No Change
	ext_fabric_setup	Yes	New features/bug fix	No	No Change
	ext_multisite_underlay_setup	No	No Change	No	No Change
	ext_multisite_underlay_setup	Yes	New features/bug fix	No	No Change
	ext_multisite_ipn_underlay_setup	No	No Change	No	No Change
	csr_link_template	No	No Change	No	No Change
	ext_routed_fabric	Yes	New features/bug fix	Yes	New features/bug fix
	ext_multisite_underlay_setup	Yes	New features/bug fix	No	No Change
	ext_vxlan_mpls_overlay_setup	Yes	New features/bug fix	No	No Change
	ext_vxlan_mpls_underlay_setup	No	No Change	No	No Change

Category (Fabric/Link/Interface)	Template Name	Is changed from Cisco NDFC Release 12.0.1a to 12.1.1e		Is changed from Cisco NDFC Release 12.0.2f to 12.1.1e	
		Yes/No	Change Description	Yes/No	Change Description
Profile	Default_Network_Extension_Universal	Yes	New features/bug fix	No	No Change
	Default_Network_Universal	Yes	New features/bug fix	No	No Change
	Default_VRF_Extension_Universal	Yes	New features/bug fix	Yes	New features/bug fix
	Default_VRF_Universal	Yes	New features/bug fix	Yes	New features/bug fix
	Service_Network_Universal	Yes	New features/bug fix	Yes	New features/bug fix
	IOS_XE_Network	Yes	New features/bug fix	Yes	New features/bug fix
	IOS_XE_VRF	Yes	New features/bug fix	Yes	New features/bug fix
	Routed_Network_Universal	Yes	New features/bug fix	Yes	New features/bug fix