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 1: 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 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 2: 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 3: 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