Prerequisites: Fabric Controller

Requirements for Fabric Controller

Overview

Nexus Dashboard Fabric Controller (NDFC) 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.

NDFC 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.

After you deploy Nexus Dashboard using a deployment mode that includes NDFC:

- **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.

Network Requirements

Note This section describes *additional* requirements and guidelines if you plan to enable the Fabric Controller service. Ensure that you have already satisfied the platform-level requirements described in the Prerequisites and guidelines for all enabled services section.

- Starting with Nexus Dashboard release 3.1.1, Cisco DC App Center connectivity has been removed from Nexus Dashboard because downloading the services separately is no longer required.

  To deploy Fabric Controller, download the unified installation image from the Software Download page; individual services' installation images are no longer available from the Cisco DC App Center.

- As mentioned in the previous section, all new Nexus Dashboard deployments must have the management network and data network in different subnets.

  Note Only SAN Controller persona can be deployed in Nexus Dashboard using the same subnets for the data and management networks.

- Interfaces on both Data and Management networks can be either Layer 2 or Layer 3 adjacent.

- Connectivity between the nodes is required on both networks with the following additional round trip time (RTT) requirements:

  Table 1: Fabric Controller RTT Requirements

Connectivity	Maximum RTT
To switches	200 ms*

  * POAP (PowerOn Auto Provisioning) is supported with a max RTT of 50 ms between Nexus Dashboard Fabric Controller and the switches.

- You must allocate the following number of persistent IP addresses depending on your use case.

  With LAN deployment type and **LAN Device Management Connectivity** set to `Management` (default):

  - 2 IPs in the **management network** for SNMP/Syslog and SCP services
  - If EPL is enabled, 1 additional IP in the data network for each fabric
  - If IP Fabric for Media is enabled, one of the following:
    - 1 additional IP in the **management network** for telemetry for single node ND
    - 3 additional IPs in the **management network** for telemetry in a 3 node ND cluster

  With LAN deployment type and **LAN Device Management Connectivity** set to `Data`:

  - 2 IPs in the **data network** for SNMP/Syslog and SCP services
  - If EPL is enabled, 1 additional IP in the data network for each fabric
  - If IP Fabric for Media is enabled, one of the following:

        - 1 additional IP in the **data network** for telemetry for single node ND
        - 3 additional IPs in the **data network** for telemetry for multi-node ND cluster

    - When operating in Layer 3 mode with LAN deployment type, **LAN Device Management Connectivity** must be set to `Data` and all persistent IPs must be part of a separate pool that must not overlap with the ND management or data subnets.

  When operating in Layer 2 mode with SAN Controller deployment type:

    - 1 IP for SSH
    - 1 IP for SNMP/Syslog
    - 1 IP per Nexus Dashboard cluster node for SAN Insights functionality

  For an overview of Persistent IP functionality, see Prerequisites and guidelines for all enabled services. Allocating persistent IP addresses can be done during the initial cluster deployment or after the cluster is deployed using the External Service Pools configuration in the UI.

- For cohosting NDFC and Nexus Dashboard Insights on the same Nexus Dashboard cluster, the Nexus Dashboard nodes must be Layer 2 adjacent.

- The network switch must support multiple concurrent SSH sessions, with the number of sessions being configurable based on the active feature set. Specific features such as discovery, image management, and preview and deploy (for managed switches) require seperate SSH sessions for each function. Hence, ensure that a switch allows a minimum of five configurable SSH sessions to enable effective device management.

Communication Ports for Fabric Controller

In addition to the ports required by the Nexus Dashboard cluster nodes (listed in a previous section), the following ports are required by the Fabric Controller service.

- 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)**
ICMP	ICMP	ICMP	In/Out	Switch discovery. **Note** Adding or discovering LAN devices uses ICMP echo packets as part of the discovery process. So if you have a firewall between the Nexus Dashboard cluster and your switches, it must allow ICMP messages through or the discovery process will fail.
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.
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.

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)
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. This applies to LAN deployments only. NX-API is an optional feature, used by limited set of NDFC functions, such as: • Endpoint locator (EPL), as described in **EPL Behavior with NX-API Configuration** • Layer 4 to Layer 7 services, as described in **Guidelines and Limitations for L4-L7 Services** You must enable the NX-API feature in the **Advanced** tab for the appropriate fabrics, such as the VXLAN, Enhanced Classic LAN, eBGP, and Campus fabrics.
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
NX-API	8443	TCP	In/Out	Used by Cisco MDS 9000 Series switches with NX-OS release 9.x and later for performance monitoring.

- The following ports apply to the External Service IPs, also known as persistent IPs, used by some of the NDFC services:

  Note that these External Service IPs may come from the Nexus Dashboard management subnet pool or the data subnet pool depending on the configured settings.

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.

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)
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.
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

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)
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
HTTP (PnP)	9666	TCP	In	Cisco Plug and Play (PnP) for Catalyst devices is accomplished via NDFC HTTP port 9666 and HTTPS port 9667. HTTP on port 9666 is used to send CA certificate bundle to devices to prime the device for HTTPS mode and actual PnP happens over HTTPS on port 9667 afterwards. PnP service, like POAP, runs on persistent IP that is associated with either the management or data subnet. Persistent IP subnet is controlled by the **LAN Device Management Connectivity** setting in the NDFC Server Settings. This applies to LAN deployments only.
HTTPS (PnP)	9667	TCP	In	
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.

- The following ports are required for NDFC SAN deployments on single-node clusters:

Table 4: Nexus Dashboard Fabric Controller Ports for SAN Deployments on Single-Node Clusters

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.
SMTP	25	TCP	Out	SMTP port is configurable through NDFC's Server Settings menu. This is an optional feature.

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)**
SNMP	161	TCP/UDP	Out	SNMP traffic from NDFC to devices.
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.
NX-API	8443	TCP	In/Out	Used by Cisco MDS 9000 Series switches with NX-OS release 9.x and later for performance monitoring.

- The following ports apply to the External Service IPs, also known as Persistent IPs, used by some of the NDFC services:

  Note that these External Service IPs may come from the Nexus Dashboard management subnet pool or the data subnet pool depending on the configured settings.

Table 5: Nexus Dashboard Fabric Controller Persistent IP Ports for SAN Deployments on Single-Node Clusters

Service	Port	Protocol	Direction `In`—towards the cluster `Out`—from the cluster towards the fabric or outside world	Connection
SCP	22	TCP	In	SCP is used by various features to transfer files between devices and the NDFC service. The NDFC SCP service functions for both downloads and uploads.
Syslog	514	UDP	In	When NDFC is configured as a Syslog server, syslogs from the devices are sent out towards 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.

Service	Port	Protocol	Direction In—towards the cluster Out—from the cluster towards the fabric or outside world	Connection
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.
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.