Cisco Nexus Dashboard Deployment and Upgrade Guide, Release 4.1.x

First Published: 2025-07-21

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

Trademarks ?

CHAPTER 1 New and Changed Information 1

New and changed information 1

PART I Preparing to Deploy Nexus Dashboard 3

CHAPTER 2 Deployment Overview and Requirements 5

Nexus Dashboard deployment overview 5

About supported node types and features 8

CHAPTER 3 Prerequisites and Guidelines 9

General prerequisites and guidelines 9

Prerequisites for the Nexus Dashboard data network and management network 13

Prerequisites for the Nexus Dashboard internal app and service networks 15

Prerequisites for LAN deployments 15

Network prerequisites for LAN deployments 15

Prerequisites for onboarding ACI fabrics in LAN deployments 16

Prerequisites for onboarding NX-OS, IOS XR, and IOS XE devices in LAN deployments 18

Communication ports for LAN deployments 19

Prerequisites for SAN deployments 30

Network prerequisites for SAN deployments 30

Communication ports for SAN deployments 30

Nexus Dashboard persistent IP addresses 39

BGP configuration and persistent IP addresses 45

Round trip time requirements 46

Fabric connectivity 46

PART II **Deploying the Cluster** 55

CHAPTER 4 **Pre-Installation Checklist** 57

Pre-installation checklist 57

CHAPTER 5 **Deploying as a Physical Appliance** 61

Prerequisites and guidelines for deploying Nexus Dashboard as a physical appliance 61

Configure a Cisco Integrated Management Controller IP address 62

Enable Serial over LAN in the Cisco Integrated Management Controller 63

Physical node cabling 63

Deploy Nexus Dashboard as a physical appliance 66

CHAPTER 6 **Deploying in VMware ESX** 75

Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX 75

Deploy Nexus Dashboard Using VMware vCenter 77

Deploy Nexus Dashboard Directly in VMware ESXi 91

CHAPTER 7 **Deploying in Linux KVM** 103

Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Linux KVM 103

Verify the I/O latency of a Linux KVM storage device 104

Understanding system resources 104

Deploy Nexus Dashboard in Linux KVM 105

CHAPTER 8 **Deploying a Virtual Nexus Dashboard (vND) in Amazon Web Services (AWS)** 117

About hosting a vND on the AWS public cloud 117

Prerequisites and guidelines for deploying the vNDs in Amazon Web Services 119

Prepare Amazon Web Services for the Nexus Dashboard cluster 120

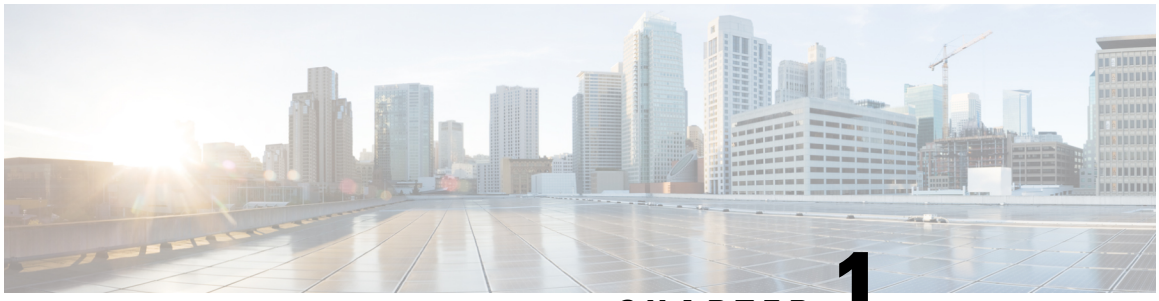
Deploy a virtual Nexus Dashboard (vND) in Amazon Web Services (AWS) 121

PART III **Upgrading or Migrating to This Release** 129

CHAPTER 9 **Upgrading an Existing Nexus Dashboard Cluster to This Release** 131

Prerequisites and guidelines for upgrading an existing Nexus Dashboard cluster 131
Supported upgrade paths 135
Upgrade Nexus Dashboard 137
Post-upgrade information and tasks 139
Troubleshooting upgrades 143

CHAPTER 10 Migrating From DCNM to ND 145
Prerequisites and guidelines for migrating from DCNM to ND 145
Migrate Existing DCNM Configuration to ND 147



CHAPTER 1

New and Changed Information

- New and changed information, on page 1

New and changed information

This table provides an overview of the significant changes to the organization and features in this guide from the release in which the guide was first published to the current release. The table does not provide an exhaustive list of all changes made to the guide.

Table 1: Latest updates

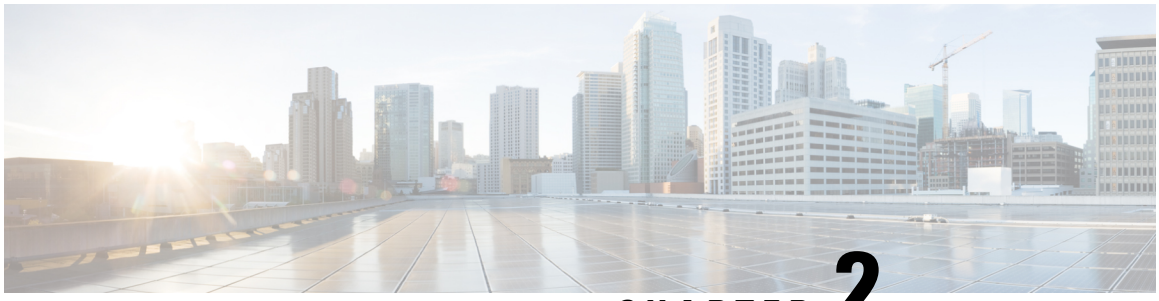
Release	New Feature or Update	Where Documented
4.1.1	First release of this document.	N/A

New and changed information

PART I

Preparing to Deploy Nexus Dashboard

- Deployment Overview and Requirements, on page 5
- Prerequisites and Guidelines, on page 9



CHAPTER 2

Deployment Overview and Requirements

- Nexus Dashboard deployment overview, on page 5

Nexus Dashboard deployment overview

Nexus Dashboard platform

Cisco Nexus Dashboard is a central management console for multiple data center fabrics that provides real-time analytics, visibility, assurance for network policies and operations, as well as policy orchestration for the data center fabrics, such as Cisco ACI and NX-OS.

Nexus Dashboard is the comprehensive management solution for ACI as well as NX-OS deployments spanning LAN fabric, SAN fabric, and IP Fabric for Media (IPFM) networks in data centers powered by Cisco. Nexus Dashboard also supports other devices, such as IOS-XE switches, IOS-XR routers, and non-Cisco devices. Being a multi-fabric controller, Nexus Dashboard manages multiple deployment models such as VXLAN EVPN, classic 3-tier LAN, FabricPath, and routed-based fabrics for LAN while providing ready-to-use control, management, monitoring, and automation capabilities for all these environments. In addition, Nexus Dashboard, when you select SAN installation, Cisco Nexus Dashboard automates Cisco MDS switches and Cisco Nexus-family infrastructure in NX-OS mode with a focus on storage-specific features and analytics capabilities.

Note This document describes how to deploy a Nexus Dashboard cluster initially and onboard the fabrics. After your cluster is up and running, see the Nexus Dashboard *configuration and operation articles* for day-to-day operation.

Unified Nexus Dashboard deployment

The Nexus Dashboard (ND) platform and related services were available in the following ways previously:

- Prior to ND release 3.1, Nexus Dashboard shipped with only the platform software and no services included. You would download, install, and enable the services separately (NDI, NDO, and/or NDFC) after the initial ND platform deployment.
- For ND releases 3.1 and 3.2, Nexus Dashboard packaged the ND platform software and the individual services' software in a unified packaging form; however, you still enabled the services separately. Management and Insights of the fabrics were still two independent pieces that were not unified.

In addition, there existed a concept of "deployment mode" in Nexus Dashboard releases 3.1 and 3.2, where you would statically enable specific services in Nexus Dashboard by selecting the deployment mode. However, changing the deployment mode was a disruptive exercise that would wipe out the entire service, including data and reinstalls. And finally, you could not run all the services in a single Nexus Dashboard cluster in Nexus Dashboard releases 3.1 and 3.2.

Now, beginning with ND release 4.1, the platform and the individual services have been unified into a single product. You no longer deploy and configure the services separately, and you do not have to activate invidual services or statically configure deployment modes. In addition, depending on the form factor, Nexus Dashboard allows you to consume any capabilities that were shipped as services in previous releases. The user experience is now unified, as there is no more concept of independent services; instead, all capabilities are now available from a single dashboard view.

Note Depending on the cluster format and the number of cluster nodes that you have deployed, certain features (such as controller, orchestrator, or telemetry) might not be available in the unified Nexus Dashboard product. Review the information in the Nexus Dashboard Capacity Planning tool to verify what features would be available for your cluster installation.

Hardware vs software stack

Nexus Dashboard is offered as a cluster of specialized Cisco UCS servers (Nexus Dashboard platform) with the software framework (Nexus Dashboard) pre-installed on it. The Cisco Nexus Dashboard software stack can be decoupled from the hardware and deployed in a number of virtual form factors. For the purposes of this document, we will use "Nexus Dashboard hardware" specifically to refer to the hardware and "Nexus Dashboard" to refer to the software stack and the GUI console.

This guide describes the initial deployment of the Nexus Dashboard software, which is common for physical and virtual form factors. If you are deploying a physical cluster, see *Nexus Dashboard Hardware Setup Guide* for the UCS servers' hardware overview, specification, and racking instructions.

Note Root access to the Nexus Dashboard software is restricted to Cisco TAC only. A special user `rescue-user` is created for all Nexus Dashboard deployments to enable a set of operations and troubleshooting commands. For additional information about the available `rescue-user` commands, see the "Troubleshooting" article in the Nexus Dashboard *documentation library*.

Available form factors

This release of Cisco Nexus Dashboard can be deployed using a number of different form factors. However, you must use the same form factor for all nodes, mixing nodes of different form factors within the same cluster is not supported. The physical form factor currently supports three different Cisco UCS servers (`SE-NODE-G2`, `ND-NODE-L4`, and `ND-NODE-G5S`). You can mix `SE-NODE-G2` and `ND-NODE-L4` servers in the same cluster, but you cannot mix a `ND-NODE-G5S` server in the same cluster as `SE-NODE-G2` and `ND-NODE-L4` servers.

- Physical appliance (`.iso`) – This form factor refers to the Cisco UCS physical appliance hardware with the Nexus Dashboard software stack pre-installed on it.

  The later sections in this document describe how to configure the software stack on the existing physical appliance hardware to deploy the cluster. Setting up the Nexus Dashboard hardware is described in *Nexus Dashboard Hardware Setup Guide* for the specific UCS model.

- Virtual Appliance – The virtual form factor allows you to deploy a Nexus Dashboard cluster using VMware ESX (`.ova`) or RHEL KVM (`.qcow2`).

  The virtual form factor supports the following two profiles:

  - Data node – This profile with higher system requirements is designed for higher scale and/or unified deployment.
  - App node – This profile with lower system requirements can be deployed as secondary nodes. Can also be deployed as primary nodes but does not support unified deployment.

  In addition, beginning with Nexus Dashboard release 4.1(1), support is available for running a virtual Nexus Dashboard (vND) on the AWS public cloud. See Deploying a Virtual Nexus Dashboard (vND) in Amazon Web Services (AWS), on page 117 for more information.

Note When planning your deployment, ensure to check the list of "Prerequisites and Guidelines" in one of the following sections of this document specific to the form factor you are deploying. A quick reference of the supported form factors, scale, and cluster sizing requirements are available in the Nexus Dashboard Cluster Sizing tool.

Scale and cluster sizing guidelines

A basic Nexus Dashboard deployment typically consists of 1 or 3 `primary` nodes, which are required for the cluster to come up. Depending on scale requirements, 3-node or larger clusters can be extended with up to 3 additional `secondary` nodes to support higher scale.

- For physical clusters, you can also add up to 2 `standby` nodes for easy cluster recovery in case of a primary node failure.
- For virtual clusters, up to 2 `standby` nodes are also supported, but only with a 3-node vND (app) profile for a Controller-only or Orchestration-only deployment.

Exact number of additional secondary nodes required for your specific use case is available from the Nexus Dashboard Cluster Sizing tool.

Scale and cluster sizing limitations

These limitations apply to scale and cluster sizing:

- Single-node deployments cannot be extended to a 3-node cluster after the initial deployment.

  If you deploy a single-node cluster and want to extend it to a 3-node cluster or add `secondary` nodes, you will need to back it up, deploy a new 3-node base cluster, and then restore the backup on this later. For more information, see *Backing Up and Restoring Your Nexus Dashboard*
- Single-node deployments do not support additional `secondary` or `standby` nodes.
- For 3-node clusters, at least two `primary` nodes are required for the cluster to remain operational.

  For more information, see *Deploying Highly Available Services with Cisco Nexus Dashboard*.

About supported node types and features

These node types have been available for releases prior to Nexus Dashboard release 4.1.1.

- `SE-NODE-G2` (UCS-C220-M5). The product ID of the 3-node cluster is `SE-CL-L3`.
- `ND-NODE-L4` (UCS-C225-M6). The product ID of the 3-node cluster is `ND-CLUSTER-L4`.

Beginning with Nexus Dashboard release 4.1.1, this node type is now also available.

- `ND-NODE-G5S` (UCS-C225-M8). The product ID of the 3-node cluster is `ND-CLUSTERG5S`.

In addition, in LAN deployments, these are the available features that you can leverage.

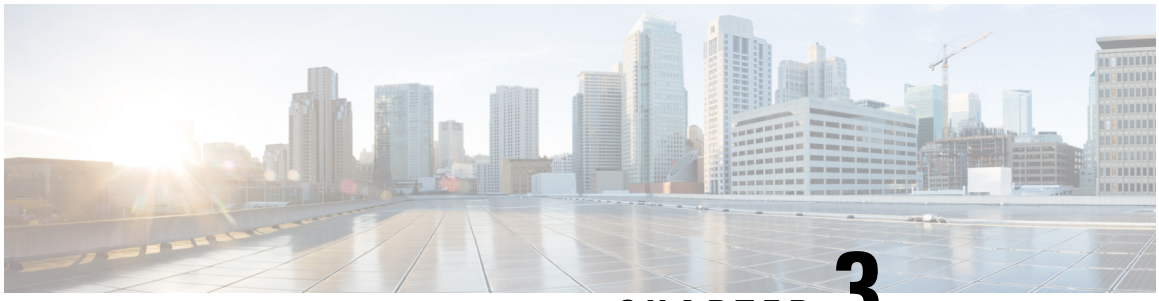
- **Controller**: Also referred to as Fabric Management. This feature is used to manage NX-OS and non-NX-OS switches (such as Catalyst, ASR, and so on). This includes creating any non-ACI fabric types, as well as performing software upgrades and creating new configurations on those fabrics.
- **Telemetry**: This feature provides telemetry functionality, similar to the functionality provided by Nexus Dashboard Insights in releases prior to Nexus Dashboard release 4.1.1. You can enable and use the **Telemetry** feature when you create or edit a fabric through **Manage** > **Fabrics**.
- **Orchestration**: You can use the **Orchestration** feature through Nexus Dashboard to connect multiple ACI fabrics together, and consolidate and deploy tenants, along with network and policy configurations, across multiple ACI fabrics. You can enable and use the **Orchestration** feature when you add an ACI through **Admin** > **System Settings** > **Multi-cluster connectivity** > **Connect Cluster**.

You can enable these features independently or, in some cases, as one of these combined feature sets.

- Controller and Telemetry
- Orchestration and Telemetry
- Controller, Telemetry, and Orchestration (not supported on an App node cluster or in a cluster with `SE-NODE-G2` nodes)

Guidelines and limitations

- For Nexus Dashboard release 4.1.1, you cannot mix the newer `ND-NODE-G5S` (UCS-C225-M8) nodes in a cluster with the older `SE-NODE-G2` (UCS-C220-M5) and `ND-NODE-L4` (UCS-C225-M6) nodes.
- A 6-node physical appliance cluster is primarily designed for extended scale NX-OS or ACI fabrics with the Telemetry feature enabled and is not recommended for non-Telemetry deployments.
- The virtual form factor does not support all features in many cluster sizes and types, as described in the *Cisco Nexus Dashboard Verified Scalability Guide*.



CHAPTER 3

Prerequisites and Guidelines

- General prerequisites and guidelines, on page 9
- Prerequisites for the Nexus Dashboard data network and management network, on page 13
- Prerequisites for the Nexus Dashboard internal app and service networks, on page 15
- Prerequisites for LAN deployments, on page 15
- Prerequisites for SAN deployments, on page 30
- Nexus Dashboard persistent IP addresses, on page 39
- Round trip time requirements, on page 46
- Fabric connectivity, on page 46

General prerequisites and guidelines

This section describes requirements and guidelines for the Nexus Dashboard cluster regardless of the deployment type.

General deployment guidelines and restrictions

- Deploying a 4-cluster node, where the cluster consists of:
  - 3 virtual nodes (data), and
  - 1 standby node

  is not a supported configuration. Redeploy this cluster without the standby node. If one of the nodes in the cluster fails, reinstall a new node and navigate to **Admin** > **System Status** > **Nodes**, then click **Actions** > **Re-Register** to add the reinstalled node back into the cluster.
- Deploying virtual Nexus Dashboard VMs on remote storage is unsupported and may lead to unexpected behavior.

Domain Name System (DNS) and Network Time Protocol (NTP)

The Nexus Dashboard nodes require valid DNS and NTP servers for all deployments and upgrades.

Lack of valid DNS connectivity (such as if using an unreachable or a placeholder IP address) can prevent the system from deploying or upgrading successfully, as well as impact regular services functionality.

Note Nexus Dashboard acts as both a DNS client and resolver. It uses an internal Core DNS server which acts as DNS resolver for internal services. It also acts as a DNS client to reach external hosts within the intranet or the Internet, hence it requires an external DNS server to be configured.

The following guidelines apply for DNS:

- For external DNS servers, both TCP and UDP traffic must be allowed. See Communication ports for LAN deployments, on page 19 and Communication ports for SAN deployments, on page 30 for more information.
- Nexus Dashboard does not support DNS servers with wildcard records.

Nexus Dashboard also supports NTP authentication using symmetrical keys. If you want to enable NTP authentication, you will need to provide the following information during cluster configuration:

- **NTP Key**–A cryptographic key that is used to authenticate the NTP traffic between the Nexus Dashboard and the NTP server(s). You will define the NTP servers in the following step, and multiple NTP servers can use the same NTP key.
- **Key ID**–Each NTP key must be assigned a unique key ID, which is used to identify the appropriate key to use when verifying the NTP packet.
- **Auth Type**–This release supports `MD5`, `SHA`, and `AES128CMAC` authentication types.

The following guidelines apply when enabling NTP authentication:

- We recommend that you do not use a Windows server as the NTP server.
- For symmetrical authentication, any key you want to use must be configured the same on both your NTP server and Nexus Dashboard.

  The ID, authentication type, and the key/passphrase itself must match and be trusted on both your NTP server and Nexus Dashboard.
- Multiple servers can use the same key.

  In this case the key must only be configured once on Nexus Dashboard, then assigned to multiple servers.
- Both Nexus Dashboard and the NTP servers can have multiple keys as long as key IDs are unique.
- This release supports SHA1, MD5, and AES128CMAC authentication/encoding types for NTP keys.

Note We recommend using AES128CMAC due to its higher security.

- When adding NTP keys in Nexus Dashboard, you must tag them as `trusted`; untrusted keys will fail authentication.

  This option allows you to easily disable a specific key in Nexus Dashboard if the key becomes compromised.
- You can choose to tag some NTP servers as `preferred` in Nexus Dashboard.

NTP clients can estimate the "quality" of an NTP server over time by taking into account RTT, time response variance, and other variables. Preferred servers will have higher priority when choosing a primary server.

- If you are using an NTP server running `ntpd`, we recommend version 4.2.8p12 at a minimum.
- The following restrictions apply to all NTP keys:
  - The maximum key length for SHA1 and MD5 keys is 40 characters, while the maximum length for AES128 keys is 32 characters.
  - Keys that are shorter than 20 characters can contain any ASCII character excluding '`#`' and spaces. Keys that are over 20 characters in length must be in hexadecimal format.
  - Keys IDs must be in the 1-65535 range.
  - If you configure keys for any one NTP server, you must also configure the keys for all other servers.
- 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 Nexus Dashboard cluster.
- These are the requirements for NTP delay, offset, and jitter:
  - Delay: < 100 ms
  - Offset: ±25 ms
  - Jitter: < 10 ms

Enabling and configuring NTP authentication is described as part of the deployment steps in the later sections.

IPv4 and IPv6 support

Nexus Dashboard supports pure IPv4, pure IPv6, or dual stack IPv4/IPv6 configurations for the cluster nodes and services.

When defining an IP address configuration, the following guidelines apply:

- All nodes and networks in the cluster must have a uniform IP configuration, either pure IPv4, pure IPv6, or dual stack IPv4/IPv6.
- If you deploy the cluster in pure IPv4 mode and want to switch to dual stack IPv4/IPv6 or pure IPv6, you must redeploy the cluster.
- For dual stack configurations:
  - The data, management, app, and service networks must be in dual stack mode.

    Mixed configurations, such as IPv4 data network and dual stack management network, are not supported.
  - For IPv6-based Nexus Dashboard deployments, the CIMCs of all physical servers must also have IPv6 addresses.
  - You can configure either IPv4 or IPv6 addresses for the nodes' management network during initial node bring up, but you must provide both types of IP addresses during the cluster bootstrap workflow.

Management IP addresses are used to log in to the nodes for the first time to initiate cluster bootstrap process.

- Kubernetes internal core services will start in IPv4 mode.
- DNS will serve and forward both IPv4 and IPv6 requests.
- VXLAN overlay for peer connectivity will use data network's IPv4 addresses.

  Both IPv4 and IPv6 packets are encapsulated within the VXLAN's IPv4 packets.
- The GUI will be accessible on both IPv4 and IPv6 management network addresses, provided both are configured.

- For pure IPv6 configurations:
  - Pure IPv6 mode is supported for physical and virtual form factors only.

    Clusters deployed through the vND deployment process on AWS public cloud do not support pure IPv6 or dual stack mode.
  - You must provide IPv6 management network addresses when initially configuring the nodes.

    After the nodes are up, these IP addresses are used to log in to the GUI and continue cluster bootstrap process.
  - You must provide IPv6 CIDRs for the internal app and service networks described above.
  - You must provide IPv6 addresses and gateways for the data and management networks described above.
  - All internal services will start in IPv6 mode.
  - VXLAN overlay for peer connectivity will use data network's IPv6 addresses.

    IPv6 packets are encapsulated within the VXLAN's IPv6 packets.
  - All internal services will use IPv6 addresses.
  - IPv6 addresses are required for physical servers' CIMCs.

Necessary URLs for certain connections

There are certain URLs that Nexus Dashboard must reach that are necessary for these connections:

- Cisco Intersight: Connecting your Nexus Dashboard cluster to Cisco Intersight has these benefits:
  - Automatic meta data updates that certain features can use to provide updated data
  - TAC log collection and uploads
- Connecting to Smart Licensing
- Pulling energy management stats from electricity maps

These are the URLs that Nexus Dashboard must reach for these connections and why:

URL	Protocol/Port/Service	Description
amazontrust.com	TCP/80(HTTP) TCP/443(HTTPS)	Used to securely connect to Cisco Intersight
connectdna.cisco.com	TCP/443(HTTPS)	Used to securely connect to Cisco Intersight and Smart Licensing
swapi.cisco.com	TCP/443(HTTPS)	Used to securely connect to Cisco Smart Licensing
svc.ucs-connect.com	TCP/443(HTTPS)	Used to securely connect to Cisco Intersight
svc-static1.ucs-connect.com	TCP/443(HTTPS)	Used to securely connect to Cisco Intersight
svc.eu-central-1.intersight.com	TCP/443(HTTPS)	Used to securely connect to Cisco Intersight (EMEA Region)
svc-static1.eu-central-1.intersight.com	TCP/443(HTTPS)	Used to securely connect to Cisco Intersight (EMEA Region)

Prerequisites for the Nexus Dashboard data network and management network

Nexus Dashboard is deployed as a cluster, connecting each node to two networks. When first configuring Nexus Dashboard, for each cluster node, you will need to provide two IP addresses for the two Nexus Dashboard interfaces:

- One connected to the data network, which is used for back-end, cluster, and Infra connectivity for optimal performance
- The other connected to the management network, which is used for seamless GUI and front-end operations

Table 2: External network purpose

Data network	Management network
• Nexus Dashboard node clustering • Service to service communication • Nexus Dashboard nodes to Cisco APIC and NX-OS controller capability communication • Telemetry traffic for switches and on-boarded fabrics	• Accessing Nexus Dashboard GUI • Accessing Nexus Dashboard CLI using SSH • DNS and NTP communication • Nexus Dashboard firmware upload • Intersight device connector • AAA traffic • Multi-cluster connectivity

The two networks have the following requirements:

- The management network and data network must be in different subnets.

Note Nexus Dashboard management interface (`bond1`) has internal iptables rules that rate-limit ICMP packets to an average of 6 packets per second with a burst limit of 5. Nexus Dashboard rate-limits ICMP packets on the data network port (`bond0`) to an average of 100 packets per second with a burst limit of 5. If you are using ICMP-based monitoring tools to track the health of the management network, you may observe intermittent packet drops if the polling frequency exceeds these limits. This is expected behavior designed to protect the management plane.

- Changing the data subnet requires re-deploying the cluster, so we recommend using a larger subnet (such as /27) than the bare minimum required by the nodes and features to account for any additional features that may require more IP addresses in the future.
- When setting up remote authentication, AAA server must not be in the same subnet as the data interface.
- For physical clusters, the management network must provide IP reachability to each node's CIMC using TCP ports 22 and 443 as the Nexus Dashboard cluster configuration uses each node's CIMC IP address to configure the node.
- The data network interface requires a minimum MTU of 1500 to be available for the Nexus Dashboard traffic.

  Higher MTU can be configured if desired on the switches to which the nodes are connected.

Note If external VLAN tag is configured for switch ports that are used for data network traffic, you must enable jumbo frames or configure custom MTU equal to or greater than 1504 bytes on the switch ports where the nodes are connected.

- If you are using telemetry, by default, the data network must provide IP reachability to the in-band network of each fabric and of the Cisco APIC for an ACI fabric (if you are using the orchestration functionality), as well as to these integrations.

Note You can also define routes in the route table of the Nexus Dashboard and use the management network instead to reach to any of the following services.

  - For DNS integration, to the DNS server.
  - For Panduit PDU integration, to the Panduit PDU server.
  - For External Kafka integration, to the External Kafka server (consumer).
  - For SysLog integration, to the SysLog server.
  - For Network-Attached Storage integration, to the Network-Attached Storage server.
  - For VMware vCenter integration, to the VMware vCenter.
  - For AppDynamics integration, to the AppDynamics controller.

  For more information, see *Working with Integrations in Your Nexus Dashboard*.

Note If all the integrations are in same subnet as the management network, then they will use the management network.

Prerequisites for the Nexus Dashboard internal app and service networks

Two additional internal networks are required for communication between the containers used by the Nexus Dashboard:

- App network--Used for applications internally within Nexus Dashboard. The app network must be a `/16` network for IPv4 or `/108` network for IPv6 and a default value is pre-populated during deployment.
- Service network--Used internally by the Nexus Dashboard. The service network must be a `/16` network for IPv4 or `/108` network for IPv6 and a default value is pre-populated during deployment.

If you are planning to deploy multiple Nexus Dashboard clusters, they can use the same application and service subnets.

Note Communications between containers deployed in different Nexus Dashboard nodes is VXLAN-encapsulated and uses the data interfaces IP addresses as source and destination. This means that the app network and service network addresses are never exposed outside the data network and any traffic on these subnets is routed internally and does not leave the cluster nodes.

For example, if you had another service (such as DNS) on the same subnet as the app or service network, you would not be able to access it from your Nexus Dashboard as the traffic on that subnet would never be routed outside the cluster. As such, when configuring these networks, ensure that they are unique and do not overlap with any existing networks or services external to the cluster, which you may need to access from the Nexus Dashboard cluster nodes.

For the same reason, we recommend not using `169.254.0.0/16` (the Kubernetes `br1` subnet) for the app or service subnets.

Prerequisites for LAN deployments

Network prerequisites for LAN deployments

These network prerequisites apply for LAN deployments:

- All new Nexus Dashboard deployments must have the management network and data network in different subnets.
- Interfaces on both data and management networks can be either Layer 2 or Layer 3 adjacent. For data network Layer 3 adjacency, you must configure BGP during the bootstrap process. Management network

interfaces do not support the BGP protocol. If different Nexus Dashboard nodes are deployed with management addresses in different subnets, those will simply be routed to one other.

- You must use persistent data IP addresses to bring up the cluster, so you must allocate a certain number of persistent IP addresses depending on your configuration.
  - If your cluster has 1 node, allocate 3 persistent IP addresses.
  - If your cluster has 3 or more nodes, allocate 5 persistent IP addresses.
  - If you configure dual stack IPv4 and IPv6, then add the same number of persistent IP addresses for IPv6 (in other words, 5 IPv4 and 5 IPv6 persistent IP addresses if you configure dual stack).

  For more information about persistent IP addresses, see Nexus Dashboard persistent IP addresses, on page 39. You must allocate the minimum required persistent IP addresses during the bootstrap process. You can allocate additional persistent IP addresses after the cluster is deployed using the External Service Pools configuration in the GUI.
- The pod profile policy is dynamically configured based on the number of nodes that you deploy.

Prerequisites for onboarding ACI fabrics in LAN deployments

These network prerequisites apply for onboarding ACI fabrics in LAN deployments:

- If you are planning to use orchestration to manage Cisco ACI fabrics, you can establish connectivity from either the data interface or the management interface to either the in-band or out-of-band (OOB) interface of each fabric's APIC cluster or both.

  If the fabric connectivity is from the Nexus Dashboard's management interface, you must configure specific static routes or ensure that the management interface is part of the same IP subnet of the APIC interfaces.

Additional prerequisites for using orchestration with ACI fabrics

If you plan to use orchestration with ACI fabrics, these prerequisites also apply:

- If you plan to use orchestration with ACI fabrics and remote leaf switches, these restrictions apply:
  - Remote leaf switches in one fabric cannot use another fabric's L3Out.
  - Stretching a bridge domain between one fabric (local leaf or remote leaf) and a remote leaf in another fabric is not supported.
- Orchestration is only supported on single-node Nexus Dashboard clusters (virtual-data profile or physical appliances) for non-production (lab) deployments. If you want to enable Orchestration on one of these form factors, it must be enabled using the built-in swagger API.
  1. From the Nexus Dashboard UI, click on the "?" icon and choose **Help Center**.
  2. In the **Help Center**, click on **API reference: Swagger (In-product)** .
  3. Within the API listing, click the **Infra** group from the left navigation.
  4. Locate the **System Settings** sub-menu and click the arrow to expand it, if necessary, then search for `/settings/general/actions/enableOrchestration`.

5. Expand the API and click **Try it Out**.

Orchestration services will now be enabled on your cluster.

Additional prerequisites for using telemetry with ACI fabrics

If you plan to use telemetry with ACI fabrics, these prerequisites also apply:

- Telemetry collection is supported with OOB networks of APIC and switches as long as they're running ACI version 6.1(2f) or later.
- You have configured NTP settings on Cisco APIC.

  For more information, see Configure NTP in ACI Fabric Solution.
- If you plan to use the following flow telemetry or traffic analytics functions, Telemetry Priority must be selected in the ACI fabric node control policy.

  In Cisco APIC, choose **Fabric** > **Fabric Policies** > **Policies** > **Monitoring** > **Fabric Node Controls** > **<*policy-name*>** > **Feature Selection** to select Telemetry Priority. Monitoring <*policy-name*> should be attached to **Fabric** > **Fabric Policies** > **Switches** > **Leaf/Spine Switches** > **Profiles** > .
- If you plan to use the flow telemetry functions, Precision Time Protocol (PTP) must be enabled on Cisco APIC so that telemetry can correlate flows from multiple switches accordingly

  In Cisco APIC, choose **System** > **System Settings** > **PTP and Latency Measurement** > **Admin State** to enable PTP.

  The quality of the time synchronization using PTP depends on the accuracy of the PTP Grandmaster (GM) clock which is the source of the clock, and the accuracy and the number of PTP devices such as ACI switches and IPN devices in between.

  Although a PTP GM device is generally equipped with a GNSS/GPS source to achieve the nanosecond accuracy which is the standard requirement of PTP, microsecond accuracy is sufficient for flow telemetry, hence a GNSS/GPS source is typically not required.

  For a single-pod ACI fabric, you can connect your PTP GM using leaf switches. Otherwise, one of the spine switches will be elected as a GM. For a multi-pod ACI fabric, you can connect your PTP GM using leaf switches or using IPN devices. Your IPN devices should be PTP boundary clocks or PTP transparent clocks so that ACI switch nodes can synchronize their clock across pods. To maintain the same degree of accuracy across pods, it is recommended to connect your PTP GM using IPN devices.

  See section "Precision Time Protocol" in the *Cisco APIC System Management Configuration Guide* for details about PTP connectivity options.
- You have configured in-band management as described in Cisco APIC and Static Management Access.
- If one or more DNS Domains are set under DNS Profiles, it is mandatory to set one DNS Domain as default.

  In Cisco APIC, choose **Fabric** > **Fabric Policies** > **Policies** > **Global** > **DNS Profile** > **default** > **DNS Domains** and set one as default.

  Failure to do so will result in the same switch appearing multiple times in the telemetry Flow map.
- Deploy ACI in-band network by configuring EPG using the following:
  - Tenant = `mgmt`

- VRF = `inb`
- BD = `inb`
- Node Management EPG = `default/<any_epg_name>`

- Nexus Dashboard's data-network IP address and ACI fabric's in-band IP address must be in different subnets.

Prerequisites for onboarding NX-OS, IOS XR, and IOS XE devices in LAN deployments

These network prerequisites apply for onboarding NX-OS, IOS XR, and IOS XE devices in LAN deployments:

- If you are planning to use orchestration to manage NX-OS fabrics, the data network must have in-band reachability for NX-OS fabrics.

Additional prerequisites for using telemetry with NX-OS fabrics or standalone NX-OS switches

If you plan to use telemetry with NX-OS fabrics or standalone NX-OS switches, these prerequisites also apply:

- The data network must have IP reachability to the fabrics' in-band or out-of-band IP addresses.

Note If you are using the Flow Telemetry feature, the data network must have IP reachability to the fabric's in-band IP addresses.

- To enable Flow Telemetry or Traffic Analytics, Precision Time Protocol (PTP) must be configured on all nodes you want to support with telemetry.

  In both managed and monitor fabric mode, you must ensure PTP is correctly configured on all nodes in the fabric. You can enable PTP in the fabric setup's **Advanced** tab by checking the **Enable Precision Time Protocol (PTP)** option.

  The PTP grandmaster clock should be provided by a device that is external to the network fabric.

Note N9k-C93180YC-FX3 switch in the fabric can be used as a PTP grandmaster.

  The quality of the time synchronization using PTP depends on the accuracy of the PTP Grandmaster (GM) clock which is the source of the clock, and the accuracy and the number of PTP devices along the network path. Although a PTP GM device is generally equipped with a GNSS/GPS source to achieve the nanosecond accuracy which is the standard requirement of PTP, microsecond accuracy is sufficient for flow telemetry, hence a GNSS/GPS source is typically not required.

  For details about manually configuring Precision Time Protocol on Nexus switches, see *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Communication ports for LAN deployments

Nexus Dashboard uses TLS or mTLS with encryption to protect data privacy and integrity while in transit.

This table lists the management network communication ports for LAN deployments, where in the **Direction** column:

- **In** means toward the cluster
- **Out** means from the cluster toward the fabric or outside world

Table 3: Management network communication ports for LAN deployments

Service	Port	Protocol	Direction (`In`/`Out`)	Connection
ICMP	ICMP	ICMP	In/Out	Other cluster nodes, CIMC, default gateway, 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. ICMP traffic on the management interface is rate-limited to an average of 6 packets/sec and a burst of 5. Monitoring systems should be configured with this limit in mind to avoid false-positive alerts regarding packet loss.
BGP	179	TCP	In/Out	For Endpoint Locator, per fabric where it is enabled, an EPL service is spawned with its own persistent IP address. This service is always associated with the Nexus Dashboard data interface. Nexus Dashboard 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.

Service	Port	Protocol	Direction (In/Out)	Connection
DHCP	67	UDP	In	If the local DHCP server is configured for bootstrap or POAP purposes. **Note** When using Nexus Dashboard as a local DHCP server for POAP purposes, all Nexus Dashboard primary node IP addresses must be configured as DHCP relays. Whether the Nexus Dashboard nodes' management IP addresses are bound to the DHCP server is determined by the LAN Device Management Connectivity in the server settings.
DHCP	68	UDP	Out	
DNS	53	TCP/UDP	Out	DNS server
Flow Telemetry	5640-5671	UDP	In	In-band of switches Used to receive flow telemetry from fabrics
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 using software telemetry to a persistent IP address associated with a Nexus Dashboard GRPC receiver service pod.
HTTP	80	TCP	Out	Internet/proxy
HTTP (PnP)	9666	TCP	In	Cisco Plug and Play (PnP) for Catalyst devices is accomplished using Nexus Dashboard 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, as with POAP, runs on a persistent IP address that is associated with either the management or data subnet. The persistent IP subnet is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

Service	Port	Protocol	Direction (In /Out)	Connection
HTTP (POAP)	80	TCP	In	Only used for device zero-touch provisioning using POAP, where devices can send (limited jailed write-only access to Nexus Dashboard) basic inventory information to Nexus Dashboard to start secure POAP communication. Nexus Dashboard Bootstrap or POAP can be configured for TFTP or HTTP/HTTPS. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
HTTPS	443	TCP	In/Out	UI, other clusters (for multi-cluster connectivity), fabrics, Internet/proxy
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 Nexus Dashboard functions.
HTTPS (PnP)	9667	TCP	In	Cisco Plug and Play (PnP) for Catalyst devices is accomplished using Nexus Dashboard 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, as with POAP, runs on a persistent IP address that is associated with either the management or data subnet. The persistent IP subnet is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

Service	Port	Protocol	Direction (In/Out)	Connection
HTTPS (POAP)	443	TCP	In	Secure POAP is accomplished using the Nexus Dashboard HTTPS Server on port 443. The HTTPS server is bound to the SCP-POAP service and uses the same persistent IP address assigned to that pod. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
Infra-Service	30012 30021 30500-30600	TCP/UDP	In/Out	Other cluster nodes
KMS	9880	TCP	In/Out	Other cluster nodes and ACI fabrics
LDAP	389 636	TCP	Out	LDAP server
NTP	123	UDP	Out	NTP server
NX-API	8443	TCP	In/Out	Used by Cisco MDS 9000 Series switches with NX-OS release 9.x and later for performance monitoring.
Radius	1812	TCP	Out	Radius server
SCP	22	TCP	In/Out	SCP is used by various features to transfer files between devices and Nexus Dashboard, such as for archiving backup files to remote server. The Nexus Dashboard 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 Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

Service	Port	Protocol	Direction (In /Out)	Connection
SCP/Show Techcollection	22	TCP	Out	Transport tech-support file from persistent IP address of Nexus Dashboard POAP-SCP pod to a separate ND cluster running telemetry. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings
SMTP	25	TCP	Out	You can configure the SMTP port on the **Admin** > **Server Settings** > **General** page. This is an optional feature.
SNMP	161	TCP/UDP	Out	SNMP traffic from Nexus Dashboard to devices.
SNMP Trap	2162	UDP	In	SNMP traps from devices to Nexus Dashboard are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings,
SSH	22	TCP	In/Out	CLI and CIMC of the cluster nodes
TAC Assist	8884	TCP	In/Out	Other cluster nodes Used for TAC Assist, which is a service to collect **show tech** from switches and upload the information to Intersight. This port is used to exchange **show tech** data across cluster nodes.
TACACS	49	TCP	Out	TACACS server

Service	Port	Protocol	Direction (In/Out)	Connection
TFTP (POAP)	69	TCP	In	Only used for device zero-touch provisioning using POAP, where devices can send (limited jailed write-only access to Nexus Dashboard) basic inventory information to Nexus Dashboard to start secure POAP communication. Nexus Dashboard bootstrap or POAP can be configured for TFTP or HTTP/HTTPS. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

This table lists the data network communication ports for LAN deployments, where in the **Direction** column:

- **In** means toward the cluster
- **Out** means from the cluster toward the fabric or outside world

Table 4: Data network communication ports for LAN deployments

Service	Port	Protocol	Direction (In/Out)	Connection
BGP	179	TCP	In/Out	For Endpoint Locator, per fabric where it is enabled, an EPL service is spawned with its own persistent IP address. This service is always associated with the Nexus Dashboard data interface. Nexus Dashboard 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.

Service	Port	Protocol	Direction (In /Out)	Connection
DHCP	67	UDP	In	If the Nexus Dashboard local DHCP server is configured for bootstrap or POAP purposes. **Note** When using Nexus Dashboard as a local DHCP server for POAP purposes, all Nexus Dashboard primary node IP addresses must be configured as DHCP relays. Whether the Nexus Dashboard nodes' data IP addresses are bound to the DHCP server is determined by the LAN Device Management Connectivity in the server settings.
DHCP	68	UDP	Out	
DNS	53	TCP/UDP	In/Out	Other cluster nodes and DNS server
Flow Telemetry	5640-5671	UDP	In	In-band of switches Used to receive flow telemetry from fabrics
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 using software telemetry to a persistent IP address associated with a Nexus Dashboard GRPC receiver service pod.
HTTP (PnP)	9666	TCP	In	Cisco Plug and Play (PnP) for Catalyst devices is accomplished using Nexus Dashboard 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, as with POAP, runs on a persistent IP address that is associated with either the management or data subnet. The persistent IP subnet is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

Service	Port	Protocol	Direction (In/Out)	Connection
HTTP (POAP)	80	TCP	In	Only used for device zero-touch provisioning using POAP, where devices can send (limited jailed write-only access to Nexus Dashboard) basic inventory information to Nexus Dashboard to start secure POAP communication. Nexus Dashboard Bootstrap or POAP can be configured for TFTP or HTTP/HTTPS. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
HTTPS	443	TCP	Out	In-band of switches and APIC and NX-OS fabrics
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 Nexus Dashboard functions.
HTTPS (PnP)	9667	TCP	In	Cisco Plug and Play (PnP) for Catalyst devices is accomplished using Nexus Dashboard 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, as with POAP, runs on a persistent IP address that is associated with either the management or data subnet. The persistent IP subnet is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

Service	Port	Protocol	Direction (In /Out)	Connection
HTTPS (POAP)	443	TCP	In	Secure POAP is accomplished using the Nexus Dashboard HTTPS Server on port 443. The HTTPS server is bound to the SCP-POAP service and uses the same persistent IP address assigned to that pod. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
HTTPS (vCenter, Kubernetes, OpenStack, Discovery)	443	TCP	Out	Nexus Dashboard 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
ICMP	ICMP	ICMP	In/Out	Other cluster nodes, default gateway
Infra-Service	3379 3380 8989 9090 9969 9979 9989 15223 30002-30006 30009-30010 30012 30014-30015 30018-30019 30025 30027	TCP	In/Out	Other cluster nodes
Infra-Service	30016 30017	TCP/UDP	In/Out	Other cluster nodes

Service	Port	Protocol	Direction (In/Out)	Connection
Infra-Service	30019	UDP	In/Out	Other cluster nodes
Infra-Service	30500-30600	TCP/UDP	In/Out	Other cluster nodes
Kafka	30001	TCP	In/Out	In-band IP of switches and APIC/Controller
KMS	9989	TCP	In/Out	Other cluster nodes and ACI fabrics
NFSv3	111	TCP/UDP	In/Out	Remote NFS server
NFSv3	608	UDP	In/Out	Remote NFS server
NFSv3	2049	TCP	In/Out	Remote NFS server
NX-API	8443	TCP	In/Out	Used by Cisco MDS 9000 Series switches with NX-OS release 9.x and later for performance monitoring.
SCP	22	TCP	In/Out	SCP is used by various features to transfer files between devices and Nexus Dashboard, such as for archiving backup files to remote server.. The Nexus Dashboard 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 Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
SCP	22	TCP	Out	Transport tech-support file from persistent IP address of Nexus Dashboard POAP-SCP pod to a separate ND cluster running telemetry. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings
SMTP	25	TCP	Out	You can configure the SMTP port on the **Admin** > **Server Settings** > **General** page. This is an optional feature.

Service	Port	Protocol	Direction (In /Out)	Connection
SNMP	161	TCP/UDP	Out	SNMP traffic from Nexus Dashboard to devices.
SNMP Trap	2162	UDP	In	SNMP traps from devices to Nexus Dashboard are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings,
SSH	22	TCP	Out	UI, in-band of switches, and APIC
SSH	1022	TCP/UDP	In/Out	Other cluster nodes
SW Telemetry	5695 30000 57500 30570	TCP	In/Out	Other cluster nodes Used to collect various telemetry information from fabrics Port 57500 is needed between switches and Nexus Dashboard for telemetry and NX-OS based switches
TFTP (POAP)	69	TCP	In	Only used for device zero-touch provisioning using POAP, where devices can send (limited jailed write-only access to Nexus Dashboard) basic inventory information to Nexus Dashboard to start secure POAP communication. Nexus Dashboard bootstrap or POAP can be configured for TFTP or HTTP/HTTPS. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
VXLAN	4789	UDP	In/Out	Other cluster nodes

Prerequisites for SAN deployments

Network prerequisites for SAN deployments

These network prerequisites apply for SAN deployments:

- In SAN deployments, management and data networks can use the same subnet.
- Persistent IP addresses are supported on the data network only with Layer 2 adjacent and Layer 3 adjacent with BGP configured. However, if you configure the management and data networks to use the same subnet, then you cannot use Layer 3 adjacency because you must configure BGP during the bootstrap process for the data network Layer 3 adjacency, but the management network doesn't support Layer 3 adjacency with BGP configured.

  In this situation, you can:

  - Use Layer 2 adjacency instead if you want to configure the management and data networks to use the same subnet, or
  - Use different subnets for the management and data networks, where you can configure Layer 2 adjacency on the management network and Layer 3 adjacency with BGP configured on the data network

- You must allocate some number of persistent IP addresses depending on your configuration. For more information about persistent IP addresses, see Nexus Dashboard persistent IP addresses, on page 39.

Communication ports for SAN deployments

Nexus Dashboard uses TLS or mTLS with encryption to protect data privacy and integrity while in transit.

This table lists the management network communication ports for SAN deployments.

Table 5: Management network communication ports for SAN deployments

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
DNS	53	TCP/UDP	Out	DNS server
GRPC (Telemetry)	33000	TCP	In	SAN Telemetry Server which receives SAN data (such as storage, hosts, flows, and so on) over GRPC transport tied to Nexus Dashboard persistent IP address.

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
HTTP	80	TCP	Out	Internet/proxy
HTTPS	443	TCP	In/Out	UI, other clusters (for multi-cluster connectivity), fabrics, Internet/proxy
HTTPS (vCenter, Kubernetes, OpenStack, Discovery)	443	TCP	Out	Nexus Dashboard 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
ICMP	ICMP	ICMP	In/Out	Other cluster nodes, CIMC, default gateway
Infra-Service	30012 30021 30500-30600	TCP/UDP	In/Out	Other cluster nodes
KMS	9880	TCP	In/Out	Other cluster nodes and ACI fabrics
LDAP	389 636	TCP	Out	LDAP server
NTP	123	UDP	Out	NTP server
NX-API	8443	TCP	In/Out	Used by Cisco MDS 9000 Series switches with NX-OS release 9.x and later for performance monitoring.
Radius	1812	TCP	Out	Radius server

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
SCP	22	TCP	In/Out	SCP is used by various features to transfer files between devices and Nexus Dashboard, such as for archiving backup files to remote server.. The Nexus Dashboard 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 Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
SCP	22	TCP	Out	Transport tech-support file from persistent IP address of Nexus Dashboard POAP-SCP pod to a separate ND cluster running telemetry. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings
SMTP	25	TCP	Out	You can configure the SMTP port on the **Admin** > **Server Settings** > **General** page. This is an optional feature.
SNMP	161	TCP/UDP	Out	SNMP traffic from Nexus Dashboard to devices.

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
SNMP Trap	2162	UDP	In	SNMP traps from devices to Nexus Dashboard are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings,
SSH	22	TCP	In/Out	CLI and CIMC of the cluster nodes
Syslog	514	UDP	In	When Nexus Dashboard is configured as a Syslog server, Syslogs from the devices are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
TACACS	49	TCP	Out	TACACS server

This table lists the data network communication ports for SAN deployments.

Table 6: Data network communication ports for SAN deployments

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
DNS	53	TCP/UDP	In/Out	Other cluster nodes and DNS server
GRPC (Telemetry)	33000	TCP	In	SAN Telemetry Server which receives SAN data (such as storage, hosts, flows, and so on) over GRPC transport tied to Nexus Dashboard persistent IP address.
HTTPS	443	TCP	Out	In-band of switches and APIC and NX-OS fabrics
HTTPS (vCenter, Kubernetes, OpenStack, Discovery)	443	TCP	Out	Nexus Dashboard 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
ICMP	ICMP	ICMP	In/Out	Other cluster nodes, default gateway

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
Infra-Service	3379 3380 8989 9090 9969 9979 9989 15223 30002-30006 30009-30010 30012 30014-30015 30018-30019 30025 30027	TCP	In/Out	Other cluster nodes
Infra-Service	30016 30017	TCP/UDP	In/Out	Other cluster nodes
Infra-Service	30019	UDP	In/Out	Other cluster nodes
Infra-Service	30500-30600	TCP/UDP	In/Out	Other cluster nodes
KMS	9880	TCP	In/Out	Other cluster nodes and ACI fabrics
NFSv3	111	TCP/UDP	In/Out	Remote NFS server
NFSv3	608	UDP	In/Out	Remote NFS server
NFSv3	2049	TCP	In/Out	Remote NFS server
NX-API	8443	TCP	In/Out	Used by Cisco MDS 9000 Series switches with NX-OS release 9.x and later for performance monitoring.

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
SCP	22	TCP	In/Out	SCP is used by various features to transfer files between devices and Nexus Dashboard, such as for archiving backup files to remote server.. The Nexus Dashboard 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 Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
SCP	22	TCP	Out	Transport tech-support file from persistent IP address of Nexus Dashboard POAP-SCP pod to a separate ND cluster running telemetry. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings
SMTP	25	TCP	Out	You can configure the SMTP port on the **Admin** > **Server Settings** > **General** page. This is an optional feature.
SNMP	161	TCP/UDP	Out	SNMP traffic from Nexus Dashboard to devices.

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection
SNMP Trap	2162	UDP	In	SNMP traps from devices to Nexus Dashboard are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings,
SSH	22	TCP	Out	In-band of switches and APIC
SSH	1022	TCP/UDP	In/Out	Other cluster nodes
Syslog	514	UDP	In	When Nexus Dashboard is configured as a Syslog server, Syslogs from the devices are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
VXLAN	4789	UDP	In/Out	Other cluster nodes

This table lists the ports that the Nexus Dashboard SAN deployments on single-node clusters require.

Table 7: Nexus Dashboard ports for SAN deployments on single-node clusters

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
GRPC (Telemetry)	33000	TCP	In	SAN Telemetry Server which receives SAN data (such as storage, hosts, flows, and so on) over GRPC transport tied to Nexus Dashboard persistent IP address.
HTTPS (vCenter, Kubernetes, OpenStack, Discovery)	443	TCP	Out	Nexus Dashboard 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.
SCP	22	TCP	In/Out	SCP is used by various features to transfer files between devices and Nexus Dashboard, such as for archiving backup files to remote server.. The Nexus Dashboard 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 Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.
SCP	22	TCP	Out	Transport tech-support file from persistent IP address of Nexus Dashboard POAP-SCP pod to a separate ND cluster running telemetry. The SCP-POAP service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings

Service	Port	Protocol	Direction `In`—toward the cluster `Out`—from the cluster toward the fabric or outside world	Connection (Applies to both LAN and SAN deployments, unless stated otherwise)
SMTP	25	TCP	Out	You can configure the SMTP port on the **Admin** > **Server Settings** > **General** page. This is an optional feature.
SNMP	161	TCP/UDP	Out	SNMP traffic from Nexus Dashboard to devices.
SNMP Trap	2162	UDP	In	SNMP traps from devices to Nexus Dashboard are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings,
SSH	22	TCP	Out	SSH is a basic mechanism for accessing devices.
Syslog	514	UDP	In	When Nexus Dashboard is configured as a Syslog server, Syslogs from the devices are sent out toward the persistent IP address associated with the SNMP-Trap/Syslog service pod. The SNMP-Trap-Syslog service in Nexus Dashboard has a persistent IP address that is associated with either the management or data subnet. This is controlled by the **LAN Device Management Connectivity** setting in the Nexus Dashboard server settings.

Nexus Dashboard persistent IP addresses

Persistent IP addresses, also known as external service IP addresses, are IP addresses that are used for various controller and telemetry functions within the Nexus Dashboard cluster. The word “persistent” is used because while the service may move between different Nexus Dashboard nodes in the event of a node or pod failure, the IP address for the service being referred by the switches in the fabric is preserved. This ensures that no

configuration updates to the switches are needed in case of a Nexus Dashboard-related failure event. Persistent IP addresses can be programmed in both the management and data subnets depending on the features deployed.

You can view the configured persistent IP addresses on your Nexus Dashboard by navigating to:

Admin > **System Settings** > **General**

Locate the **External Pools** tile and click **View all** at the bottom left area of the **External Pools** tile to view the configured persistent IP addresses on your Nexus Dashboard.

Persistent IP address updates in release 4.x

This section provides information on the changes in Nexus Dashboard release 4.x for the persistent IP addresses. It also explains how to make certain updates in the number of persistent IP addresses before proceeding to upgrade to Nexus Dashboard release 4.x.

- Reduction of number of IP addresses needed

  Starting with release 4.1.1, some services that needed exclusive IP addresses in previous Nexus Dashboard releases were merged with others. For example, on a per Nexus Dashboard node basis, software telemetry, flow telemetry and IPFM telemetry collectors on the data network have been merged in such a way that one IP address per collector service is sufficient to serve all three functions.

- LAN Device Connectivity

  You can set the type of LAN device connectivity (Data or Management) under **Admin** > **System Settings** > **Fabric management** > **Advanced settings** > **Admin** > **LAN Device Management Connectivity**.

  Prior to release 4.1.1, the default setting for LAN Device connectivity was Management. Beginning with release 4.1.1, this default has been changed to Data. However, when upgrading from Nexus Dashboard release 3.2.x to 4.x, any user-configured setting for LAN device connectivity is preserved.

- Layer-3 Persistent IP Support for Telemetry

  Starting with Nexus Dashboard release 4.1.1, telemetry-collector-X persistent IPs are supported in layer-3 adjacent Nexus Dashboard clusters. See below for Layer 3 BGP deployment details.

The number of persistent IP addresses and how they are mapped to services has changed in Nexus Dashboard release 4.x. The following services consume persistent IP addresses on Nexus Dashboard:

LAN deployments:

- Telemetry collector-x: There is a requirement for 1 persistent IP address for a 1-node cluster, or 3 persistent IP addresses for a 3-node or larger cluster, on the data network.
- SNMP trap and syslog receiver: 1 persistent IP address on the data network if the LAN device connectivity type is set to Data or 1 persistent IP address on the management network if the LAN device connectivity type is set to Management.
- Switch bootstrap service (POAP/PnP): 1 persistent IP address on the data network if the LAN device connectivity type is set to Data or 1 persistent IP address on the management network if the LAN device connectivity type is set to Management.
- (Optional) Endpoint Locator (EPL): 1 persistent IP address on the data network for each fabric where EPL is enabled. The EPL feature can be enabled for up to 4 fabrics in a given Nexus Dashboard cluster.
- (Optional) IPFM (IP Fabric for Media) telemetry collector-x: If LAN device connectivity is set to Data, then no additional persistent IPs are required. However if LAN device connectivity type is set to

Management, there is a requirement for 1 persistent IP address for a 1-node cluster, or 3 persistent IP addresses for a 3-node or larger cluster, on the management network.

SAN deployments:

- SNMP trap and syslog receiver: 1 persistent IP address on the data network.
- Switch bootstrap service: 1 persistent IP address on the data network.
- (Optional) SAN Insights receiver-x: There is a requirement for 1 persistent IP address for a 1-node cluster, or 3 persistent IP addresses for a 3-node or larger cluster, on the data network.

For an IPv4-only Nexus Dashboard cluster deployment, each service listed above will consume 1 persistent IPv4 address. For an IPv6-only Nexus Dashboard cluster deployment, each service will consume 1 persistent IPv6 address. For a dual-stack Nexus Dashboard cluster deployment, each service needing a persistent IP will consume an IPv4 address and an IPv6 address.

Fresh installation or upgrade

The total number of persistent IP addresses that you will need won't necessarily change based on whether you are performing a fresh installation or an upgrade. In addition, for a fresh installation of Nexus Dashboard (greenfield deployment), you must configure persistent IP addresses only on the data network. You can change the LAN device connectivity type from Data to Management after the cluster installation is complete.

As mentioned earlier, there is a change in the default setting in Nexus Dashboard 4.x compared to previous Nexus Dashboard releases. In Nexus Dashboard 4.x, the default LAN Device Management Connectivity is set to Data, while in earlier releases it was set to Management. As part of the effort towards delivering the unified Nexus Dashboard, the goal is to make the recommended best practice deployment as easy as possible. The reachability from Nexus Dashboard to and from switches is recommended to be over the Nexus Dashboard data interface. The Nexus Dashboard management interface should primarily be used for UI/API access and reachability for AAA, DNS, Proxy, NTP, Intersight, and so on. Finally, note that the connectivity setting set by the user is preserved when doing an inline upgrade from Nexus Dashboard release 3.2.x to Nexus Dashboard release 4.x.

Additional considerations to keep in mind

Along with the factors listed above, there are several additional considerations that you should keep in mind regarding persistent IP addresses:

- Nexus Dashboard deployment mode:
  - Layer 2: Here the Nexus Dashboard nodes within the cluster are layer-2 adjacent. This means that all Nexus Dashboard nodes share the same management and data subnet respectively. Persistent IP addresses need to be on the same network as the data network or management network.
  - Layer 3 BGP: In this mode, the Nexus Dashboard nodes within the cluster are layer-3 adjacent. In other words, unique management and data subnets are associated with each Nexus Dashboard node in the cluster. There needs to be IP reachability between the nodes to form the cluster. Persistent IP addresses cannot be from a subnet that belongs to any of the Nexus Dashboard nodes' Data or Management interface subnets. In this case, LAN Device Management Connectivity must be set to Data and cannot be changed.

Updates to mapping

The mapping for persistent IP addresses has been updated to show correct service names.

Older	Newer
cisco-nir-collectorpersistent1-service	Telemetry collector-1
cisco-nir-collectorpersistent2-service	Telemetry collector-2
cisco-nir-collectorpersistent3-service	Telemetry collector-3
cisco-ndfc-dcnm-poap-data-http-ssh	Switch Bootstrap server
cisco-ndfc-dcnm-poap-mgmt-http-ssh	Switch Bootstrap server
cisco-ndfc-dcnm-syslog-trap-data	SNMP trap and syslog receiver
cisco-ndfc-dcnm-syslog-trap-mgmt	SNMP trap and syslog receiver
cisco-ndfc-pmn-telemetry-mgmt-worker-0	IPFM telemetry collector-1
cisco-ndfc-pmn-telemetry-mgmt-worker-1	IPFM telemetry collector-2
cisco-ndfc-pmn-telemetry-mgmt-worker-2	IPFM telemetry collector-3
cisco-ndfc-dcnm-san-insight-receiver-1	SAN Insights receiver-1
cisco-ndfc-dcnm-san-insight-receiver-2	SAN Insights receiver-2
cisco-ndfc-dcnm-san-insight-receiver-3	SAN Insights receiver-3

Determining the total number of persistent IP addresses that you will need

All the factors listed above come into play when you are trying to determine the total number of persistent IP addresses that you will need and which network they come from. Make sure you review you final Nexus Dashboard deployment configuration to verify that you have enough persistent IP addresses in the proper subnet range for your deployment, and that you have additional persistent IP addresses if necessary, depending on the type of LAN device connectivity that you set and for services that you might enable, such as Endpoint Locator (EPL).

Following is an example scenario that demonstrates how persistent IP addresses are used:

Fresh installation:

First, at cluster bringup, you will need a certain number of persistent IP addresses on the data network, based on the cluster size, as mentioned earlier:

- **1-node cluster, with physical or virtual nodes**: Minimum of **3** persistent IP addresses needed on the data network
- **3-node or larger cluster, with physical or virtual nodes**: Minimum of **5** persistent IP addresses needed on the data network

Note These values are valid for either IPv4 or IPv6, but double the number for dual-stack IPv4 and IPv6. For example, for a 3-node or larger cluster, a minimum of 10 persistent IP addresses would be needed on the data network for dual-stack IPv4 and IPv6 (5 IPv4 and 5 IPv6 persistent IP addresses).

After bootstrapping, you may need to add additional persistent IP addresses as needed, depending on these scenarios:

- If you leave the LAN device connectivity type set to **Data**, you won't need any additional persistent IP addresses unless you enable the Endpoint Locator (EPL) feature, which requires 1 additional persistent IP address on the data network per fabric where EPL is enabled.
- If you change the LAN device connectivity type from **Data** to **Management**:
  - You will need 2 additional persistent IP addresses on the management network for Syslog/SNMP trap and switch bootstrap functionality.
  - (Optional) If you want to enable Endpoint Locator (EPL), you will need 1 persistent IP address on the data network per fabric where EPL is enabled.
  - (Optional) If you want IP Fabric for Media (IPFM) fabrics, you will need 1 persistent IP address for a 1-node cluster, or 3 persistent IP addresses for a 3-node or larger cluster, on the management network.

Table 8: Persistent IP requirements: Fresh installation of 4.x

Number of ND nodes	LAN Device Connectivity	Mandatory persistent IP addresses	Optional persistent IP addresses	Other common persistent IP addresses
1	Data [1]	3 in data network	N/A	1 in data network per fabric where EPL is enabled
	Management	2 in management network 1 in data network	1 in management network for IPFM fabrics	
3 or more	Data [1]	5 in data network	N/A	
	Management	2 in management network 3 in data network	3 in management network for IPFM fabrics	

[1] Indicates default option set during ND bootstrap process

Upgrade:

Now assume that you want to upgrade from Nexus Dashboard 3.2.x to 4.x. The number of persistent IP addresses that you will need in Nexus Dashboard 4.x will vary, depending on the services that you were running and how they were configured on Nexus Dashboard 3.2.x, and the size of your cluster in Nexus Dashboard 4.x. Note that the LAN Device Management Connectivity that you set in the Nexus Dashboard 3.2.x release is preserved as-is when performing an inline upgrade to the Nexus Dashboard 4.x release.

- If you had only **NDFC** running in your Nexus Dashboard 3.2.x system, and
  - If you had **Data** set as the type of LAN device connectivity in Nexus Dashboard 3.2.x, and
    - You have a 1-node cluster that you want to upgrade to Nexus Dashboard 4.x, then you'll need 3 persistent IP addresses on the data network.
    - You have a 3-node or larger cluster that you want to upgrade to Nexus Dashboard 4.x, then you'll need 5 persistent IP addresses on the data network.

- If you had **Management** set as the type of LAN device connectivity in Nexus Dashboard 3.2.x, and
  - You have a 1-node cluster that you want to upgrade to in Nexus Dashboard 4.x, then you would already have either 2 or 3 persistent IP addresses (additional IP is required if IPFM/PTP feature was enabled) in the management network. In addition, you will need 1 persistent IP address in the data network, otherwise the upgrade to 4.x will fail during the pre-upgrade validation step.
  - You have a 3-node or larger cluster that you want to upgrade to in Nexus Dashboard 4.x, then you would already have either 2 or 5 persistent IP addresses (3 additional IPs are required if IPFM/PTP feature was enabled) in the management network. You will need to configure 3 persistent IP addresses in the data network; only then will the upgrade to 4.x proceed.

- If you had only **NDI** running in your Nexus Dashboard 3.2.x system, and
  - You have a 1-node cluster that you want to upgrade to Nexus Dashboard 4.x, then you would already have configured 4 persistent IP addresses in the data network. After the upgrade to 4.x, only 3 persistent IP addresses will be in use. The remaining can be reclaimed.
  - You have a 3-node or larger cluster that you want to upgrade to Nexus Dashboard 4.x, then you would already have configured 8 persistent IP addresses in the data network and 2 additional data IPs for support of standalone NX-OS deployments. After the upgrade to 4.x, only 5 of these data IP addresses will be in use. The remaining can be reclaimed.

- If you had only **NDO** running in your Nexus Dashboard 3.2.x system, then you did not have any persistent IP addresses in your Nexus Dashboard 3.2.x system. When you upgrade to Nexus Dashboard 4.x, if you have a 3-node cluster that you want to upgrade to Nexus Dashboard 4.x, then you'll need 5 persistent IP addresses on the data network before the upgrade can proceed.
- If you had an **NDO** and **NDI** deployment mode in your Nexus Dashboard 3.2.x system, and you have a 3-node or larger cluster that you want to upgrade to Nexus Dashboard 4.x, then you would already have configured 8 persistent IP addresses in the data network. After the upgrade to 4.x, only 5 of these data persistent IP addresses will be in use. The remaining persistent IP addresses can be reclaimed.
- If you had only **NDFC** and **NDI** deployment mode in your Nexus Dashboard 3.2.x system, and you have a 3-node or larger physical ND cluster that you want to upgrade to Nexus Dashboard 4.x, then there were two options based on the LAN Device Management Connectivity setting:
  - If you had **Management** set as the type of LAN device connectivity in Nexus Dashboard 3.2.x, you would already have configured 8 persistent IP addresses in the data network for NDI and 2 persistent IP addresses in the management network for NDFC. After the upgrade to 4.x, the 2 persistent IP addresses in the management subnet will be used along with only 3 of the data persistent IP addresses. The remaining persistent IP addresses can be reclaimed.
  - If you had **Data** set as the type of LAN device connectivity in Nexus Dashboard 3.2.x, you would already have configured 8 persistent IP addresses in the data network for NDI and 2 additional data persistent IP addresses for NDFC. After the upgrade to 4.x, only 5 of these data persistent IP addresses will be in use. The remaining persistent IP addresses can be reclaimed.

Table 9: Persistent IP requirements: Upgrade from 3.2.x to 4.x

ND 3.2.x deployment mode	Number of ND nodes	LAN Device Connectivity	ND 3.2.x persistent IP address requirement	ND 4.x persistent IP address requirement
NDFC	1	Data	2 in data network, plus 1 in data network if IPFM/PTP is enabled	3 in data network
		Management	2 in management network, plus 1 in management network if IPFM/PTP is enabled	2 in management network, plus 1 in management network for IPFM fabrics 1 in data network
NDFC	3 or more	Data	2 in data network, plus 3 in data network if IPFM/PTP is enabled	5 in data network
		Management	2 in management network, plus 3 in management network if IPFM/PTP is enabled	2 in management network, plus 3 in management network for IPFM fabrics 3 in data network
NDFC + NDI	3 physical	Data	10 in data network	5 in data network
		Management	2 in management network 8 in data network	2 in management network, plus 3 in management network for IPFM fabrics 3 in data network
NDI	1	N/A	3 in data network	3 in data network
NDI	3 or more	N/A	10 in data network	5 in data network
NDO	3	N/A	None	5 in data network
NDO + NDI	3 or more	N/A	8 in data network	5 in data network

Note EPL persistent IP address requirements remain the same in release 4.x as they were in release 3.2.x.

BGP configuration and persistent IP addresses

Some prior releases of Nexus Dashboard allowed you to configure one or more persistent IP addresses that require retaining the same IP addresses even in case they are relocated to a different Nexus Dashboard node. However, in those releases, the persistent IP addresses had to be part of the management and data subnets and the feature could be enabled only if all nodes in the cluster were part of the same Layer 3 network. Here, the services used Layer 2 mechanisms such as gratuitous ARP or neighbor discovery to advertise the persistent IP addresses within its Layer 3 network.

While that is still supported, this release also allows you to configure the persistent IP addresses feature even if you deploy the cluster nodes in different Layer 3 networks. In this case, the persistent IP addresses are

advertised out of each node's data links using BGP, which we refer to as "Layer 3 mode". The IP addresses must also be part of a subnet that is not overlapping with any of the nodes' management or data subnets. If the persistent IP addresses are outside the data and management networks, this feature will operate in Layer 3 mode by default; if the IP addresses are part of those networks, the feature will operate in Layer 2 mode. BGP can be enabled during cluster deployment or from the Nexus Dashboard GUI after the cluster is up and running.

If you plan to enable BGP and use the persistent IP address functionality, you must:

- Ensure that the peer routers exchange the advertised persistent IP addresses between the nodes' Layer 3 networks.
- For data network Layer 3 adjacency, you must configure BGP during the bootstrap process. BGP does not support management network Layer 3 adjacency.
- Ensure that the persistent IP addresses you allocate do not overlap with any of the nodes' management or data subnets.

Round trip time requirements

Connectivity between the nodes is required on both networks with additional round trip time (RTT) requirements, as listed in this table.

Table 10: Cluster round trip time requirements

Connectivity	Maximum RTT
Between nodes within the same Nexus Dashboard cluster	50 ms
Between nodes in one cluster and nodes in a different cluster if the clusters are connected using multi-cluster connectivity For more information about multi-cluster connectivity, see *Cisco Nexus Dashboard Infrastructure Management*.	500 ms
Between external DNS servers and the Nexus Dashboard cluster	5 seconds
To fabric switches	150 ms

Fabric connectivity

These sections describe how to connect your Nexus Dashboard cluster nodes to the management and data networks and how to connect the cluster to your fabrics. For more information on configuring the fabric to enable the in-band telemetry functions, see the following documents:

- *Getting Your Cisco ACI Fabrics Ready for Cisco Nexus Dashboard Insights*
- *Deploying Nexus Fabrics with Telemetry on Cisco Nexus Dashboard*

For on-premises APIC or NX-OS fabrics, you can connect the Nexus Dashboard cluster in one of these ways:

- The Nexus Dashboard cluster connected to the fabric using a Layer 3 network.
- The Nexus Dashboard nodes connected to the leaf switches as typical hosts.

Connecting using an external Layer 3 network

We recommend connecting the Nexus Dashboard cluster to the fabrics using an external Layer 3 network as it does not tie the cluster to any one fabric and the same communication paths can be establish to all fabrics. Specific connectivity depends on the type of applications deployed in the Nexus Dashboard:

- If you are using orchestration to manage Cisco ACI fabrics, you can establish connectivity from either the data interface or the management interface to either the in-band or out-of-band (OOB) interface of each fabric's APIC or both.

  If the fabric connectivity is from the Nexus Dashboard's management interface, you must configure specific static routes or ensure that the management interface is part of the same IP subnet of the APIC interfaces.

- If you are using telemetry, you must establish connectivity from the data interface to the in-band network of each fabric and of the APIC.

If you plan to connect the cluster across a Layer 3 network, keep the following in mind:

- For ACI fabrics, you must configure an L3Out and the external EPG for Cisco Nexus Dashboard data network connectivity in the management tenant.

  Configuring external connectivity in an ACI fabric is described in the Cisco APIC Layer 3 Networking Configuration Guide.

- If you specify a VLAN ID for your data interface during setup of the cluster, the host port must be configured as `trunk` allowing that VLAN.

  However, in most common deployments, you can leave the VLAN ID empty and configure the host port in `access` mode.

The following two figures show two distinct network connectivity scenarios when connecting the Nexus Dashboard cluster to the fabrics using a Layer 3 network, where the first figure shows a mix of ACI and NX-OS fabrics, and the second figure shows only ACI fabrics.

Figure 1: Connecting using Layer 3 network, With a mix of ACI and NX-OS fabrics

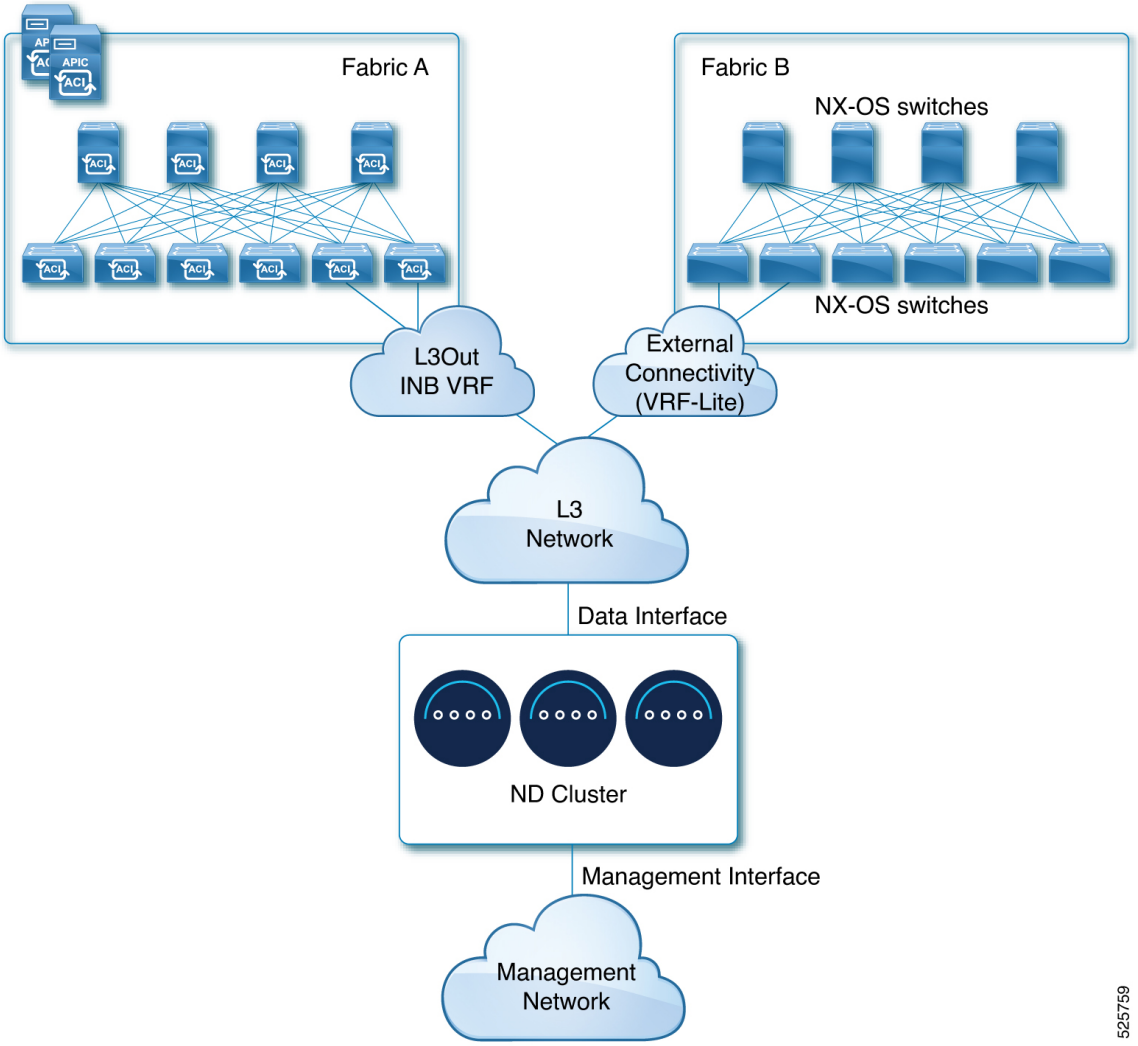
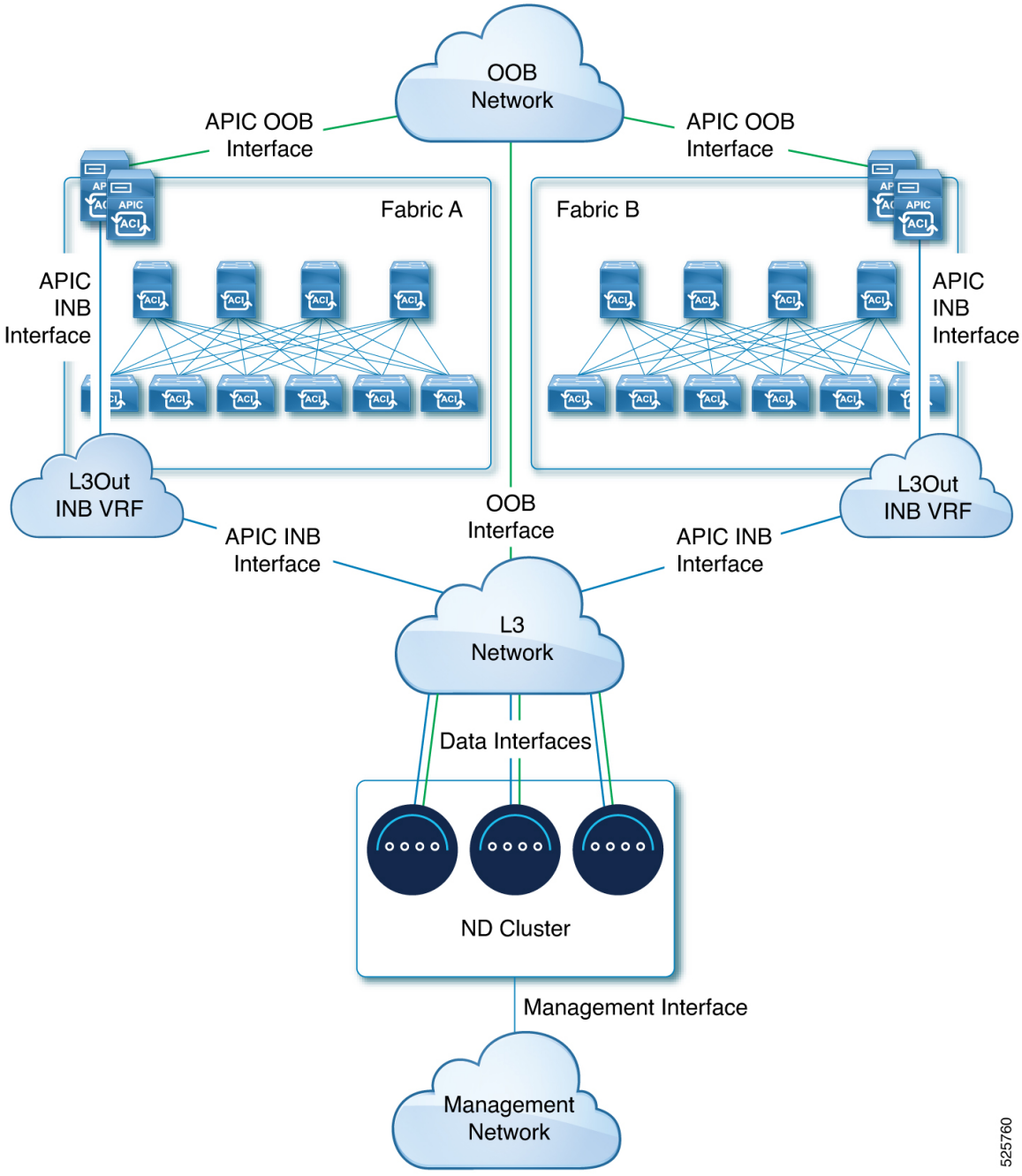


Figure 2: Connecting using Layer 3 network, with ACI fabrics only



Connecting nodes directly to leaf switches

You can also connect the Nexus Dashboard cluster directly to one of the fabrics. This provides easy connectivity between the cluster and in-band management of the fabric, but ties the cluster to the specific fabric and requires reachability to other fabrics to be established through external connectivity. This also makes the cluster dependent on the specific fabric so issues within the fabric may impact Nexus Dashboard connectivity. Like in the previous example, connectivity depends on the type of applications deployed in the Nexus Dashboard:

- If you are using orchestration to manage Cisco ACI fabrics, you can establish connectivity from either the data interface or the management interface to either the in-band or out-of-band (OOB) interface of each fabric's APIC or both.

  If the fabric connectivity is from the Nexus Dashboard's management interface, you must configure specific static routes or ensure that the management interface is part of the same IP subnet of the APIC interfaces.

- If you are using telemetry, you can establish connectivity from the data interface to the in-band or out-of-band (OOB) interface of each fabric. However, you must add the route if you establish connectivity from the data interface to the out-of-band interface.

  For ACI fabrics, the data interface IP subnet connects to an EPG/ or bridge domain in the fabric and must have a contract established to the local in-band EPG in the management tenant. We recommend deploying the Nexus Dashboard in the management tenant and in-band VRF. Connectivity to other fabrics is established using an L3Out.

If you plan to connect the cluster directly to the leaf switches, keep the following in mind:

- If deploying in VMware ESX or Linux KVM, the host must be connected to the fabric using trunk port.
- If you specify a VLAN ID for your data network during setup of the cluster, the Nexus Dashboard interface and the port on the connected network device must be configured as `trunk`.

  However, in most cases we recommend not assigning a VLAN to the data network, in which case you must configure the ports in `access` mode.

- For configurations on the APIC side, following are recommended configurations:
  - We recommend configuring the bridge domain, subnet, and endpoint group (EPG) for Cisco Nexus Dashboard connectivity in management tenant.

    Because the Nexus Dashboard requires connectivity to the in-band EPG in the in-band VRF, creating the EPG in the management tenant means no route leaking is required.

  - You must create a contract between the fabric's in-band management EPG and Cisco Nexus Dashboard EPG.
  - If several fabrics are monitored with apps on the Nexus Dashboard cluster, L3Out with default route or specific route to other ACI fabric in-band EPG must be provisioned and a contract must be established between the cluster EPG and the L3Out's external EPG.

The following figures show two distinct network connectivity scenarios when connecting the Nexus Dashboard cluster directly to the fabrics' leaf switches. The primary purpose of each depends on the type of application you may be running in your Nexus Dashboard.

The following graphics show these types of connections:

- Connecting directly to ACI fabric
- Connecting directly to NX-OS fabric
- Connecting directly to ACI and NX-OS fabrics

Figure 3: Connecting Directly to ACI Fabric

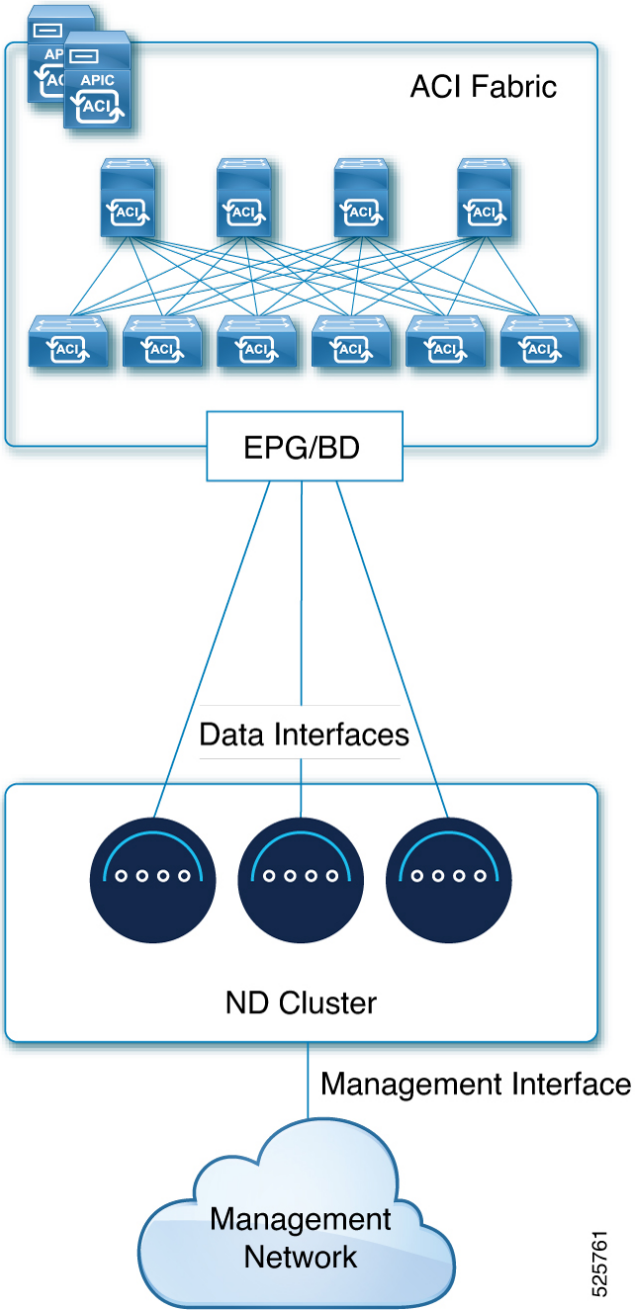


Figure 4: Connecting Directly to NX-OS Fabric

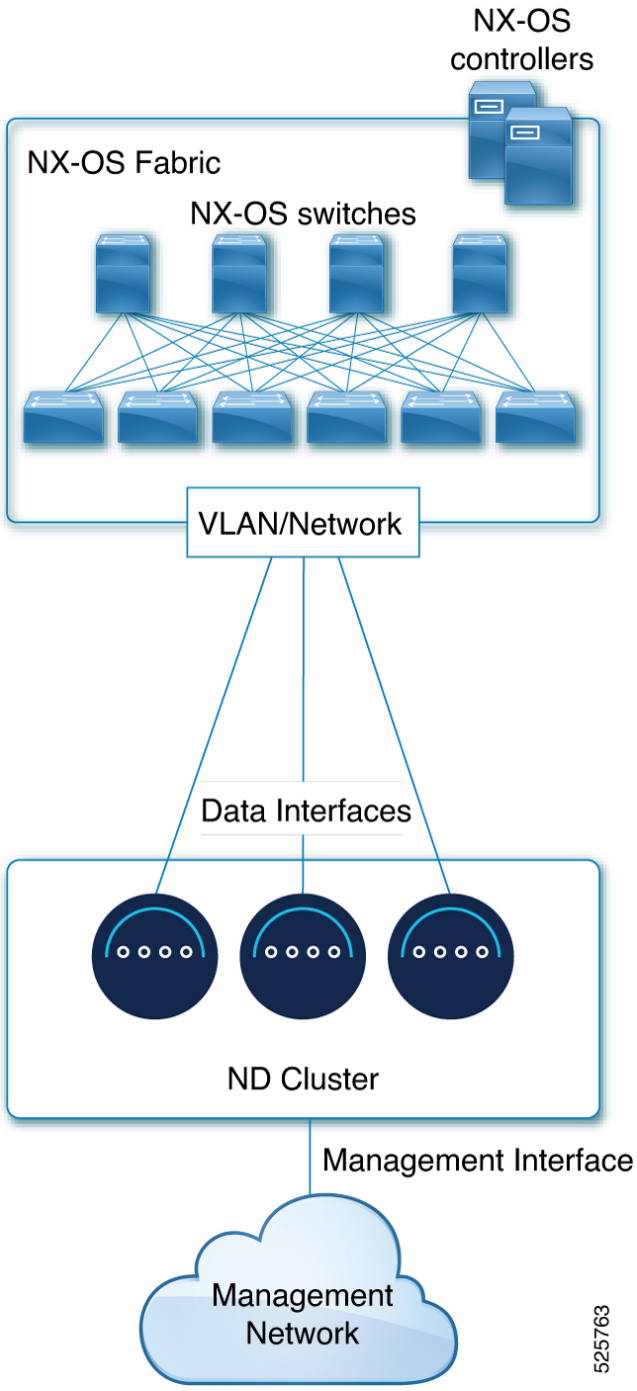
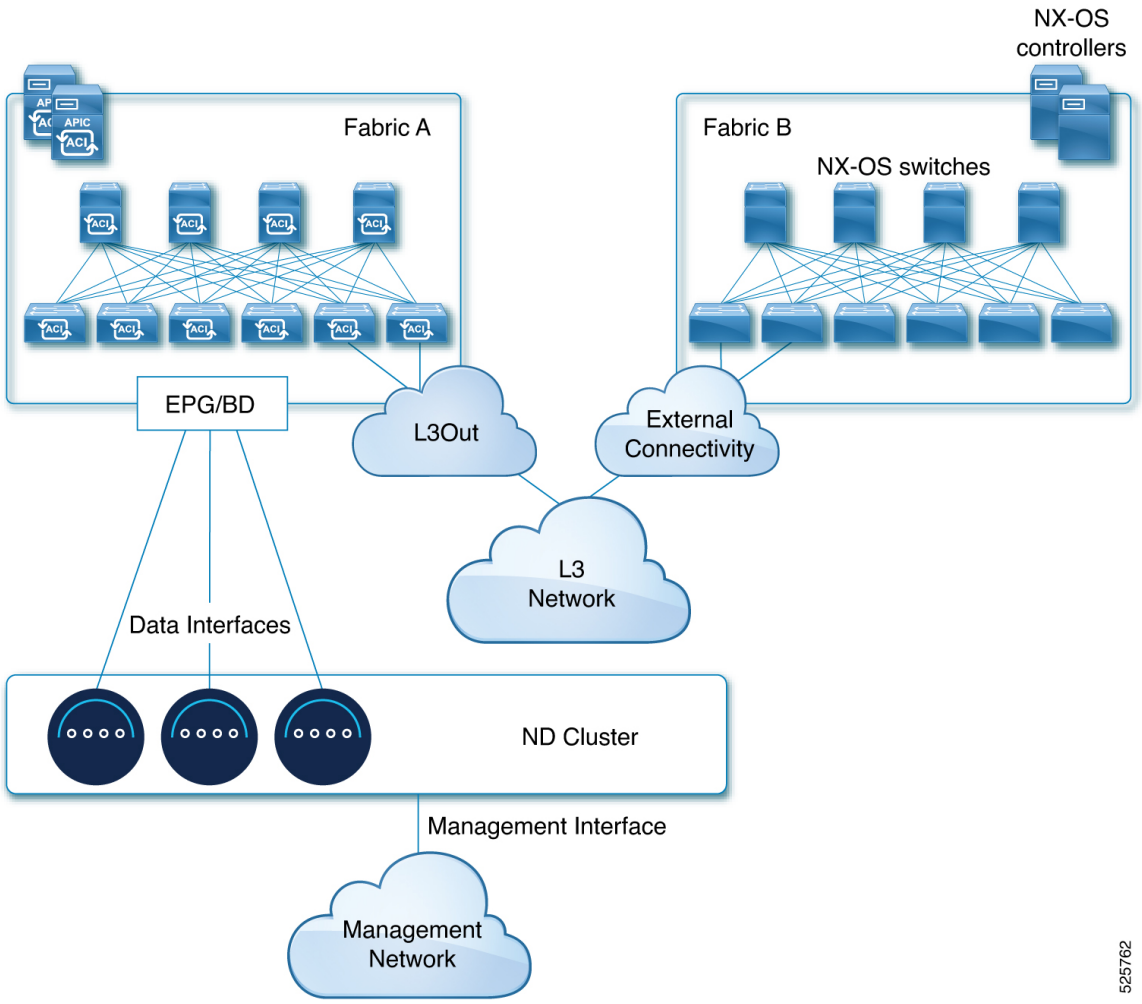


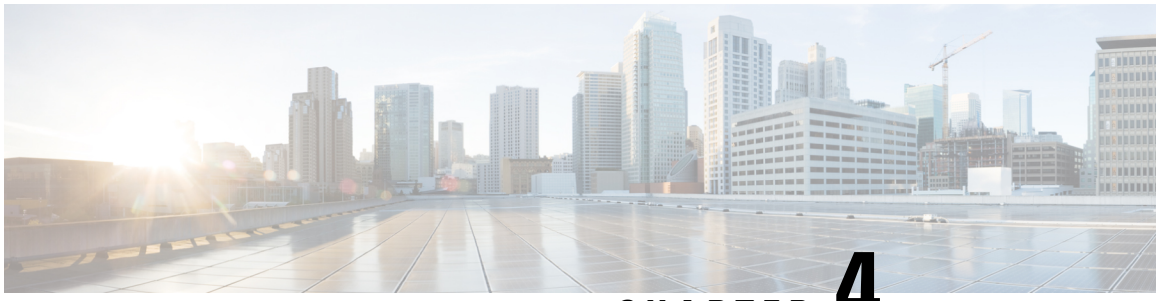
Figure 5: Connecting Directly to ACI and NX-OS Fabrics



PART II

Deploying the Cluster

- Pre-Installation Checklist, on page 57
- Deploying as a Physical Appliance, on page 61
- Deploying in VMware ESX, on page 75
- Deploying in Linux KVM, on page 103
- Deploying a Virtual Nexus Dashboard (vND) in Amazon Web Services (AWS), on page 117



CHAPTER 4

Pre-Installation Checklist

- Pre-installation checklist, on page 57

Pre-installation checklist

Before you proceed with deploying your Nexus Dashboard cluster, prepare this information for easy reference during the process.

Table 11: Cluster details

Parameters	Example	Your entry
Cluster **Name**	`ND-Prod-CL01`	
Nexus Dashboard Implementation Type (LAN/SAN)	`LAN`	
DNS Provider(s)	`8.8.8.8`	
DNS Search Domain	`cisco.com`	
NTP Provider(s)	`1.1.1.1`	
(Optional) **NTP Authentication Key**	`123456789`	
(Optional) **NTP Authentication ID**	`100`	
(Optional) **NTP Authentication Type**	`MD5`	
Proxy Server	`192.168.50.1`	
(Optional) **Proxy Server Ignore Hosts**	`10.0.0.1`	
(Optional) **Proxy Username**	`Proxy-user`	

Parameters	Example	Your entry
(Optional) **Proxy Password**	`P@ssword!123`	
App Network	`172.17.0.1/16 (default)`[1]	
Services Network	`100.80.0.0/16 (default)`[2]	
(Optional) **App Network IPv6**	`2001:db8:abcd:0012::0/64`	
(Optional) **Services Network IPv6**	`2001:db8:efgh:0012::0/64`	

[2] These are the default values and we do not recommend that you change them. If you want to change the values, see the appropriate chapter in the "Deploying the Cluster" part.

Note You can define all nodes during the initial cluster deployment, including the `secondary` and `standby` nodes. For simplicity, the following tables assume a 3-node base cluster, but if you are deploying a larger cluster, you must also have the details for all additional nodes.

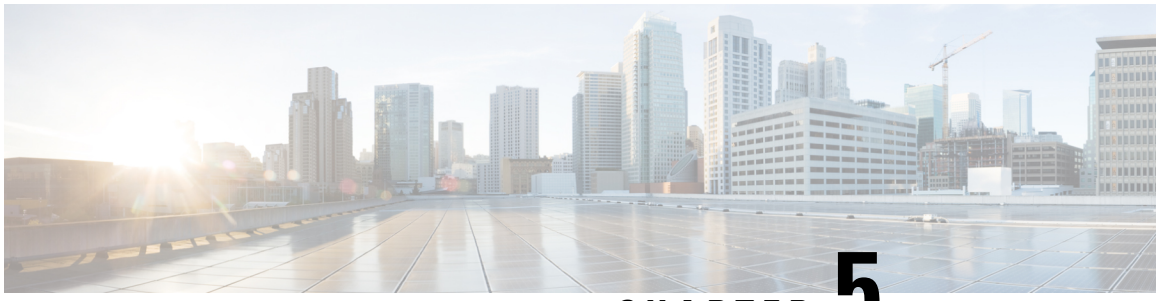
Table 12: Node details

Parameters	Example	Your entry
For physical nodes, **CIMC** address and login information of the first node	`10.196.220.84/24` Username: `admin` Password: `Cisco1234`	
For physical nodes, **CIMC** address and login information of the second node	`10.196.220.85/24` Username: `admin` Password: `Cisco1234!`	
For physical nodes, **CIMC** address and login information of the third node	`10.196.220.86/24` Username: `admin` Password: `Cisco1234!`	
Password used for each node's `rescue-user` and the initial GUI password. We recommend configuring the same password for all nodes in the cluster.	`Welcome2Cisco!`	
Management IP of the first node	`192.168.11.172/24`	
Management Gateway of the first node.	`192.168.11.1`	
Data Network IP of the first node	`192.168.8.172/24`	

Parameters	Example	Your entry
Data Network Gateway of the first node	`192.168.8.1`	
(Optional) **Data Network VLAN** of the first node (only enter a VLAN if the upstream switchport configuration is “trunk” and the VLAN is added to the trunk allowed list)	`101`	
(Optional) If you enable BGP, **ASN** of the first node	`63331`	
(Optional) If you enable BGP and use pure IPv6 deployment, **Router ID** for the first node in the form of an IPv4 address	`1.1.1.1`	
(Optional) If you enable BGP, IP addresses of the first node's **BGP Peer**s	`200.11.11.2`	
(Optional) If you enable BGP, ASNs of the first node's **BGP Peer**s	`55555`	
Management IP of the second node	`192.168.9.173/24`	
Management Gateway of the second node.	`192.168.9.1`	
Data Network IP of the second node	`192.168.6.173/24`	
Data Network Gateway of the second node	`192.168.6.1`	
(Optional) **Data Network VLAN** of the second node	`101`	
(Optional) If you enable BGP, **ASN** of the second node	`63331`	
(Optional) If you enable BGP and use pure IPv6 deployment, **Router ID** for the second node in the form of an IPv4 address	`2.2.2.2`	
(Optional) If you enable BGP, IP addresses of the second node's **BGP Peer**s	`200.12.12.2`	

Parameters	Example	Your entry
Cluster Connectivity (L2/BGP)s	`L2`	
(Optional) If you enable BGP, ASNs of the second node's **BGP Peer**s	`55555`	
Management IP of the third node	`192.168.9.174/24`	
Management Gateway of the third node.	`192.168.9.1`	
Data Network IP of the third node	`192.168.6.174/24`	
Data Network Gateway of the third node	`192.168.6.1`	
(Optional) **Data Network VLAN** of the third node	`101`	
(Optional) If you enable BGP, **ASN** of the third node	`63331`	
(Optional) If you enable BGP and use pure IPv6 deployment, **Router ID** in the form of an IPv4 address	`3.3.3.3`	
(Optional) If you enable BGP, IP addresses of the third node's **BGP Peer**s	`200.13.13.2`	
(Optional) If you enable BGP, ASNs of the third node's **BGP Peer**s	`55555`	

You will also need to program persistent IP addresses during the cluster bringup. For more information, see Nexus Dashboard persistent IP addresses, on page 39.



CHAPTER 5

Deploying as a Physical Appliance

- Prerequisites and guidelines for deploying Nexus Dashboard as a physical appliance, on page 61
- Physical node cabling, on page 63
- Deploy Nexus Dashboard as a physical appliance, on page 66

Prerequisites and guidelines for deploying Nexus Dashboard as a physical appliance

Before you proceed with deploying the Nexus Dashboard cluster, you must:

- Review and complete the prerequisites described in Prerequisites and Guidelines, on page 9.
- Review the *Cisco Nexus Dashboard Release Notes* for any information that can affect your deployment. See the Cisco Nexus Dashboard documentation landing page.
- Ensure you are using the following hardware and the servers are racked and connected as described in *Cisco Nexus Dashboard Hardware Setup Guide* specific to the model of server you have.

  The physical appliance form factor is supported only on these versions of the original Cisco Nexus Dashboard platform hardware:

  - `SE-NODE-G2` (UCS-C220-M5). The product ID of the 3-node cluster chassis is `SE-CL-L3`.
  - `ND-NODE-L4` (UCS-C225-M6). The product ID of the 3-node cluster chassis is `ND-CLUSTER-L4`.
  - `ND-NODE-G5S` (UCS-C225-M8). The product ID of the 3-node cluster chassis is `ND-CLUSTERG5S`.

Note This hardware only supports Cisco Nexus Dashboard software. If any other operating system is installed, the node can no longer be used as a Cisco Nexus Dashboard node.

- Ensure that you are running a supported version of Cisco Integrated Management Controller (CIMC).

  The minimum that is supported and recommended versions of CIMC are listed in the "Compatibility" section of the *Release Notes* for your Cisco Nexus Dashboard release.
- Ensure that you have configured an IP address for the server's CIMC.

See Configure a Cisco Integrated Management Controller IP address, on page 62.

- Ensure that Serial over LAN (SoL) is enabled in CIMC.

  See Enable Serial over LAN in the Cisco Integrated Management Controller, on page 63.

  You might have a misconfiguration of SoL if the bootstrap fails at the `bootstrap peer nodes` point with this error:

  ```
  Waiting for firstboot prompt on NodeX
  ```

- Ensure that all nodes are running the same release version image.
- If your Cisco Nexus Dashboard hardware came with a different release image than the one you want to deploy, we recommend deploying the cluster with the existing image first and then upgrading it to the needed release.

  For example, if the hardware you received came with the release 3.2.1 image pre-installed, but you want to deploy release 4.1.1 instead, we recommend:

  1. First, bring up the release 3.2.1 cluster, as described in the deployment guide for that release.
  2. Then upgrade to release 4.1.1, as described in Upgrading an Existing Nexus Dashboard Cluster to This Release, on page 131.

Note For brand new deployments, you can also choose to simply re-image the nodes with the latest version of the Cisco Nexus Dashboard (for example, if the hardware came with an image which does not support a direct upgrade to this release through the GUI workflow) before returning to this document for deploying the cluster. This process is described in the "Re-Imaging Nodes" section of the *Troubleshooting* article for this release.

- You must have at least a 1-node cluster. Extra secondary nodes can be added for horizontal scaling if required. For the maximum number of `secondary` and `standby` nodes in a single cluster, see the *Release Notes* for your release.

Configure a Cisco Integrated Management Controller IP address

Follow these steps to configure a Cisco Integrated Management Controller (CIMC) IP address.

Procedure

Step 1 Power on the server.

After the hardware diagnostic is complete, you will be prompted with different options controlled by the function (Fn) keys.

Step 2 Press the **F8** key to enter the **Cisco IMC configuration Utility**.

Step 3 Follow these substeps.

a) Set **NIC mode** to `Dedicated`.

b) Choose between the **IPv4** and **IPv6** IP modes.

You can choose to enable or disable DHCP. If you disable DHCP, provide the static IP address, subnet, and gateway information.

c) Ensure that **NIC Redundancy** is set to `None`..

d) Press **F1** for more options such as hostname, DNS, default user passwords, port properties, and reset port profiles.

Step 4 Press **F10** to save the configuration and then restart the server.

Enable Serial over LAN in the Cisco Integrated Management Controller

Serial over LAN (SoL) is required for the `connect host` command, which you use to connect to a physical appliance node to provide basic configuration information. To use the SoL, you must first enable it on your Cisco Integrated Management Controller (CIMC).

Follow these steps to enable Serial over LAN in the Cisco Integrated Management Controller.

Procedure

Step 1 SSH into the node using the CIMC IP address and enter the sign-in credentials.

Step 2 Run these commands:

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol *#
Server /sol # show

C220-WZP23150D4C# scope sol
C220-WZP23150D4C /sol # show

Enabled Baud Rate(bps)  Com Port SOL SSH Port
------- --------------- -------- -------------
yes     115200          com0     2400
```

Step 3 In the command output, verify that `com0` is the com port for SoL.

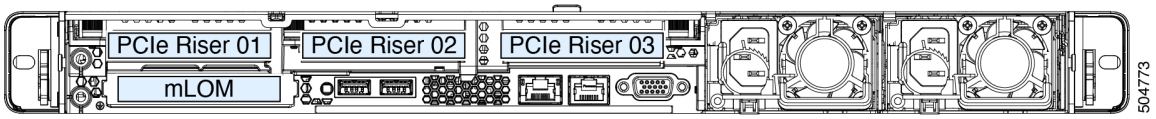
This enables the system to monitor the console using the `connect host` command from the CIMC CLI, which is necessary for the cluster bringup.

Physical node cabling

Physical nodes can be deployed in these physical servers:

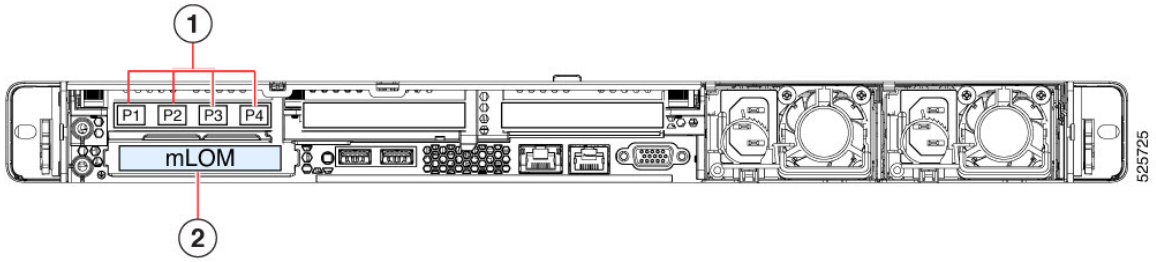
- `SE-NODE-G2` (UCS-C220-M5) and `ND-NODE-L4` (UCS-C225-M6) physical servers:

Figure 6: mLOM and PCIe riser 01 card used for node connectivity: SE-NODE-G2 (UCS-C220-M5) and ND-NODE-L4 (UCS-C225-M6)



- ND-NODE-G5S (UCS-C225-M8) physical server, where you will make these connections.

Figure 7: mLOM and PCIe riser 01 card used for node connectivity: ND-NODE-G5S (UCS-C225-M8)



1	**Data connections**: Ports are numbered 1, 2, 3, and 4, from left-to-right in the UCSC-P-V5Q50G-D (Cisco UCS VIC 15425 Quad Port 10/25/50G CNA) PCIE card installed in the PCIe Riser 01 location. See the "Data network connections" information below for the supported port channel configurations.
2	**Management connections**: Through the two MGMT ports in the Modular LAN-on-motherboard (mLOM).

Note The OCP card included on the ND-NODE-G5S servers supports a 1Gb copper connection for management only. All other network connections for Nexus Dashboard need to leverage the four port VIC card (callout 1 in the figure above). This VIC card supports 10/25/50Gbps, and the recommended SFP+ cable is the SFP-10G-AOC3M, but Cisco also offers 5-meter and 7-meter options as well. The VIC card requires a minimum of two connections per server for data network connectivity. These VIC connections can leverage any supported SFP, but Cisco recommends this connection for seamless deployments of Nexus Dashboard.

The physical nodes can be deployed with these guidelines:

- All servers come with a Modular LAN on Motherboard (mLOM) card, which you use to connect to the Nexus Dashboard management network.
- The SE-NODE-G2 server includes a 4-port VIC1455 card in the "PCIe-Riser-01" slot (shown in the above diagram), which you use for Nexus Dashboard data network connectivity
- The ND-NODE-L4 server includes either a 2x10GbE NIC (APIC-P-ID10GC), or 2x25/10GbE SFP28 NIC (APIC-P-I8D25GF), or the VIC1455 card in the "PCIe-Riser-01" slot (shown in the above diagram), which you use for Nexus Dashboard data network connectivity.
- The ND-NODE-G5S includes a UCSC-P-V5Q50G-D (Cisco UCS VIC 15425 Quad Port 10/25/50G CNA) PCIE card in the "PCIe-Riser-01" slot (shown in the above diagram), which you use for Nexus Dashboard data network connectivity.

When connecting the node to your management and data networks:

- The interfaces are configured as Linux bonds, one for the data interfaces (bond0) and one for the management interfaces (bond1), running in active-standby mode.
- **Management network connections**:
  - You must use the `mgmt0` and `mgmt1` on the mLOM card.
  - All ports must have the same speed, either 1G or 10G.
- **Data network connections**:
  - On the `SE-NODE-G2` server, you must use the VIC1455 card.
  - On the `ND-NODE-L4` server, you can use the 2x10GbE NIC (`APIC-P-ID10GC`), or 2x25/10GbE SFP28 NIC (`APIC-P-I8D25GF`), or the VIC1455 card.

Note If you connect using the 25G Intel NIC, you must disable the FEC setting on the switch port to match the setting on the NIC:

```
(config-if)# fec off
# show interface ethernet 1/34
Ethernet1/34 is up
admin state is up, Dedicated Interface
  [...]
  FEC mode is off
```

  - On the `ND-NODE-G5S` server, you must use optical connections through the necessary port channel combinations in the UCSC-P-V5Q50G-D (Cisco UCS VIC 15425 Quad Port 10/25/50G CNA) PCIE card.

Note For 25/50 GB speed connections, you will need one of the following pairs of Forward Error Correction (FEC) configurations:

On the Nexus 9000	CIMC port
FEC AUTO	cl74
FC-FEC	cl74
FEC OFF	FEC OFF

  - All interfaces must be connected to individual host-facing switch ports; fabric extenders (FEX), port channel (PC), and virtual port channel (vPC) are not supported.
  - All ports must have the same speed, either 10G, 25G, or 50G.
  - `fabric0` and `fabric1` in Nexus Dashboard corresponds to these ports:
    - `SE-NODE-G2` and `ND-NODE-L4` servers: Port-1 corresponds to `fabric0` and Port-2 corresponds to `fabric1`.

- `ND-NODE-G5S` server: `fabric0` and `fabric1` in the `ND-NODE-G5S` server corresponds to these ports:
  - Port-1 and Port-2 correspond to `fabric0`
  - Port-3 and Port-4 correspond to `fabric1`

  You can therefore have these port channel combinations:
  - Port-1 (`fabric0`), Port-3 (`fabric1`)
  - Port-2 (`fabric0`), Port-4 (`fabric1`)
  - Port-1 (`fabric0`), Port-4 (`fabric1`)
  - Port-2 (`fabric0`), Port-3 (`fabric1`)

You can use both `fabric0` and `fabric1` for data network connectivity as Active-Standby.

Note When using a 4-port card, the order of ports depends on the model of the server you are using:

- On the `SE-NODE-G2` server, the order from left to right is Port-1, Port-2, Port-3, Port-4.
- On the `ND-NODE-L4` server, the order from left to right is Port-4, Port-3, Port-2, Port-1. If you configure a port channel, Port-1 and Port-2 are fabric0 and Port-3 and Port-4 are fabric1.

Caution If you connect the two cables for the data network connections using different port channel combinations from those listed above, there will be MAC move notifications on the upstream switch and the ports will flap.

- If you connect the nodes to Cisco Catalyst switches, packets are tagged on those Catalyst switches with `vlan0` if no VLAN is specified. In this case, you must add `switchport voice vlan dot1p` command to the switch interfaces where the nodes are connected to ensure reachability over the data network.

Deploy Nexus Dashboard as a physical appliance

When you first receive the Nexus Dashboard physical hardware, it comes preloaded with the software image. Follow these steps to deploy Nexus Dashboard as a physical appliance.

Before you begin

Complete the requirements and guidelines described in Prerequisites and guidelines for deploying Nexus Dashboard as a physical appliance, on page 61.

Procedure

Step 1 Configure the first node's basic information.

You must configure only a single ("first") node as described in this step. Other nodes will be configured during the GUI-based cluster deployment process described in the following steps and will accept settings from the first `primary` node. The other two `primary` nodes do not require any additional configuration besides ensuring that their CIMC IP addresses are reachable from the first `primary` node and login credentials are set, as well as network connectivity between the nodes is established on the data network.

a) SSH into the node using CIMC management IP and use the `connect host` command to connect to the node's console.

```
C220-WZP23150D4C# connect host
CISCO Serial Over LAN:
Press Ctrl+x to Exit the session
```

After connecting to the host, press **Enter** to continue.

b) After you see the Nexus Dashboard setup utility prompt, press **Enter**.

```
Starting Nexus Dashboard setup utility
Welcome to Nexus Dashboard 4.1.1
Press Enter to manually bootstrap your first master node...
```

c) Enter and confirm the `admin` password

This password will be used for the `rescue-user` CLI login as well as the initial GUI password.

```
Admin Password:
Reenter Admin Password:
```

d) Enter the management network information.

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

Note
If you want to configure pure IPv6 mode, enter the IPv6 in the above example instead.

e) Review and confirm the entered information.

You will be asked if you want to change the entered information. If all the fields are correct, enter the capital letter `N` to proceed. If you want to change any of the entered information, enter `y` to re-start the basic configuration script.

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24

Re-enter config? (y/N): N
```

Step 2 Wait for the process to complete.

After you enter and confirm management network information of the first node, the initial setup configures the networking and brings up the UI, which you will use to add two and configure other nodes and complete the cluster deployment.

```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.
```

```
System UI online, please login to https://192.168.9.172 to continue.
```

Step 3 Open your browser and navigate to `https://<node-mgmt-ip>` to open the GUI.

The rest of the configuration workflow takes place from one of the node's GUI. You can choose any one of the nodes you deployed to begin the bootstrap process and you do not need to log in to or configure the other two nodes directly.

Enter the password you entered in a previous step and click **Login**

Step 4 Enter the requested information in the **Basic Information** page of the **Cluster Bringup** wizard.

a) For **Cluster Name**, enter a name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

b) For **Select the Nexus Dashboard Implementation type**, choose either **LAN** or **SAN** then click **Next**.

Step 5 Enter the requested information in the **Configuration** page of the **Cluster Bringup** wizard.

a) (Optional) If you want to enable IPv6 functionality for the cluster, put a check in the **Enable IPv6** checkbox.

b) Click **+Add DNS provider** to add one or more DNS servers, enter the DNS provider IP address, then click the checkmark icon.

c) (Optional) Click **+Add DNS search domain** to add a search domain, enter the DNS search domain IP address, then click the checkmark icon.

d) (Optional) If you want to enable NTP server authentication, put a check in the **NTP Authentication** checkbox.

e) If you enabled NTP authentication, click **+ Add Key**, enter the required information, and click the checkmark icon to save the information.

- **Key**–Enter the NTP authentication key, which is a cryptographic key that is used to authenticate the NTP traffic between the Nexus Dashboard and the NTP servers. You will define the NTP servers in the following step, and multiple NTP servers can use the same NTP authentication key.
- **ID**–Enter a key ID for the NTP host. Each NTP key must be assigned a unique key ID, which is used to identify the appropriate key to use when verifying the NTP packet.
- **Authentication Type**–Choose authentication type for the NTP key.
- Put a check in the **Trusted** checkbox if you want this key to be trusted. Untrusted keys cannot be used for NTP authentication.

For the complete list of NTP authentication requirements and guidelines, see General prerequisites and guidelines, on page 9.

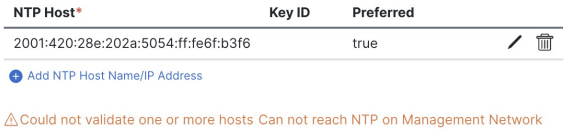
If you want to enter additional NTP keys, click **+ Add Key** again and enter the information.

f) If you enabled NTP authentication, click **+Add NTP Host Name/IP Address**, enter the required information, and click the checkmark icon to save the information.

- **NTP Host**–Enter an IP address; fully qualified domain names (FQDN) are not supported.
- **Key ID**–Enter the key ID of the NTP key you defined in the previous substep.

  If NTP authentication is disabled, this field is grayed out.
- Put a check in the **Preferred** checkbox if you want this host to be preferred.

Note
If the node into which you are logged in is configured with only an IPv4 address, but you have checked **Enable IPv6** in a previous step and entered an IPv6 address for an NTP server, you will get the following validation error:



This is because the node does not have an IPv6 address yet and is unable to connect to an IPv6 address of the NTP server. You will enter IPv6 address in the next step. In this case, enter the other required information as described in the following steps and click **Next** to proceed to the next page where you will enter IPv6 addresses for the nodes.

If you want to enter additional NTP servers, click **+Add NTP Host Name/IP Address** again and enter the information.

g) For **Proxy Server**, enter the URL or IP address of a proxy server.

For clusters that do not have direct connectivity to Cisco cloud, we recommend configuring a proxy server to establish the connectivity. This allows you to mitigate risk from exposure to non-conformant hardware and software in your fabrics.

You can click **+Add Ignore Host** to enter one or more destination IP addresses for which traffic will skip using the proxy.

The proxy server must have these URLs enabled:

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

If you do not want to configure a proxy, click **Skip Proxy** then click **Confirm**.

h) (Optional) If your proxy server requires authentication, put a check in the **Authentication required for Proxy** checkbox and enter the login credentials.

i) (Optional) Expand the **Advanced Settings** category and change the settings if required.

Under advanced settings, you can configure these settings:

- **App Network**–The address space used by the application's services running in the Nexus Dashboard. Enter the IP address and netmask.
- **Service Network**–An internal network used by Nexus Dashboard and its processes. Enter the IP address and netmask.
- **App Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the app network.
- **Service Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the service network.

For more information about the application and service networks, see General prerequisites and guidelines, on page 9.

j) Click **Next**.

Step 6 In the **Node Details** page, update the first node's information.

You have defined the Management network and IP address for the node into which you are currently logged in during the initial node configuration in earlier steps, but you must also enter the Data network information for the node before you can proceed with adding the other `primary` nodes and creating the cluster.

a) For **Cluster Connectivity**, if your cluster is deployed in L3 HA mode, choose **BGP**. Otherwise, choose **L2**.

BGP configuration is required for the persistent IP addresses feature used by telemetry. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed. All remaining nodes need to configure BGP if it is configured. You must enable BGP now if the data network of nodes have different subnets.

b) Click the **Edit** button next to the first node.

The node's **Serial Number**, **Management Network** information, and **Type** are automatically populated, but you must enter the other information.

c) For **Name**, enter a name for the node.

The node's **Name** will be set as its hostname, so it must follow the RFC-1123 requirements.

Note
If you need to change the name but the **Name** field is not editable, run the CIMC validation again to fix this issue.

d) For **Type**, choose **Primary**.

The first nodes of the cluster must be set to **Primary**. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, enter the node's data network information.

Enter the data network IP address, netmask, and gateway. Optionally, you can also enter the VLAN ID for the network. Leave the VLAN ID field blank if your configuration does not require VLAN. If you chose **BGP** for **Cluster Connectivity**, enter the ASN.

If you enabled IPv6 functionality in a previous page, you must also enter the IPv6 address, netmask, and gateway.

Note
If you want to enter IPv6 information, you must do so during the cluster bootstrap process. To change the IP address configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) If you chose **BGP** for **Cluster Connectivity**, then in the **BGP peer details** area, enter the peer's IPv4 address and ASN.

You can click **+ Add IPv4 BGP peer** to add addition peers.

If you enabled IPv6 functionality in a previous page, you must also enter the peer's IPv6 address and ASN.

g) Click **Save** to save the changes.

Step 7 If you are deploying a multi-node cluster, in the **Node Details** page, click **Add Node** to add the second node to the cluster.

a) In the **Deployment Details** area, enter the **CIMC IP Address**, **Username**, and **Password** for the second node.

Note

For **Username** for the second node, enter the admin user ID.

b) Click **Validate** to verify connectivity to the node.

The node's serial number is automatically populated after CIMC connectivity is validated.

c) For **Name**, enter the name for the node.

The node's name will be set as its hostname, so it must follow the RFC-1123 requirements.

d) For **Type**, choose `Primary`.

The first 3 nodes of the cluster must be set to `Primary`. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Management Network** area, enter the node's management network information.

You must enter the management network IP address, netmask, and gateway.

If you enabled IPv6 functionality in a previous page, you must also enter the IPv6 address, netmask, and gateway.

Note
All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) In the **Data Network** area, enter the node's data network information.

Enter the data network IP address, netmask, and gateway. Optionally, you can also enter the VLAN ID for the network. Leave the VLAN ID field blank if your configuration does not require VLAN. If you chose **BGP** for **Cluster Connectivity**, enter the ASN.

If you enabled IPv6 functionality in a previous page, you must also enter the IPv6 address, netmask, and gateway.

Note
If you want to enter IPv6 information, you must do so during the cluster bootstrap process. To change the IP address configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4 and IPv6.

g) If you chose **BGP** for **Cluster Connectivity**, then in the **BGP peer details** area, enter the peer's IPv4 address and ASN.

You can click **+ Add IPv4 BGP peer** to add addition peers.

If you enabled IPv6 functionality in a previous page, you must also enter the peer's IPv6 address and ASN.

h) Click **Save** to save the changes.

i) Repeat this step for the final (third) primary node of the cluster.

Step 8 (Optional) Repeat the previous step to enter information about any additional secondary or standby nodes.

Note
To support higher scale, you must provide a sufficient number of secondary nodes during deployment. Refer to the Nexus Dashboard Cluster Sizing tool for exact number of additional secondary nodes required for your specific use case.

You can choose to add the standby nodes now or at a later time after the cluster is deployed.

Step 9 In the **Node Details** page, verify the information that you entered, then click **Next**.

Step 10 In the **Persistent IPs** page, if you want to add more persistent IP addresses, click **+ Add Data Service IP Address**, enter the IP address, and click the checkmark icon. Repeat this step as many times as desired, then click **Next**.

You must configure the minimum number of required persistent IP addresses during the bootstrap process. This step enables you to add more persistent IP addresses if desired.

Step 11 In the **Summary** page, review and verify the configuration information, click **Save**, and click **Continue** to confirm the correct deployment mode and proceed with building the cluster.

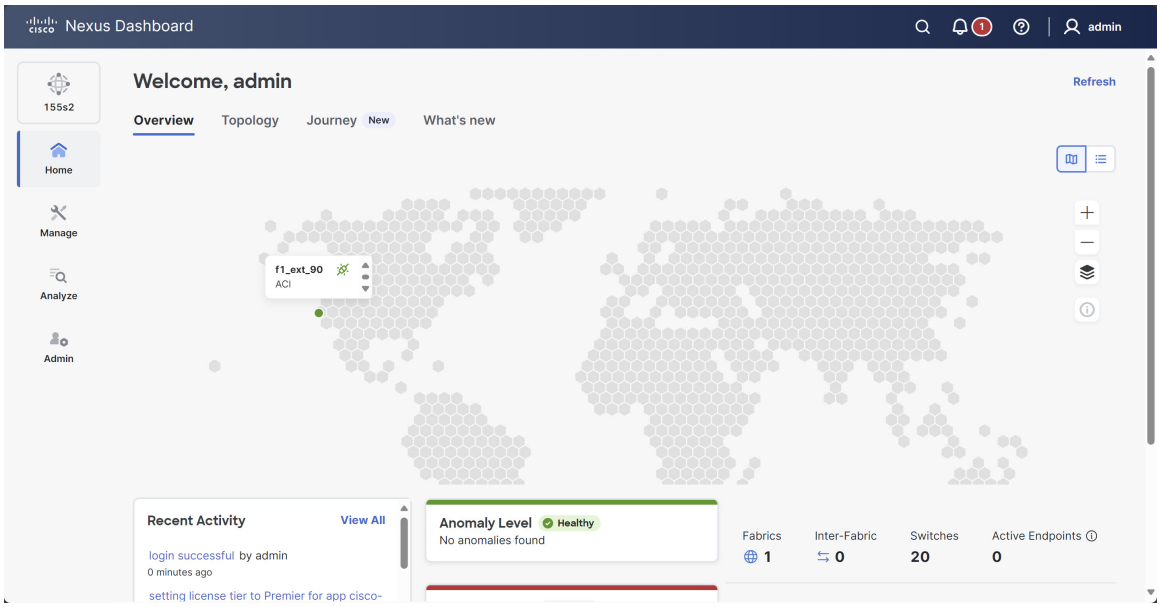
During the node bootstrap and cluster bring-up, the overall progress as well as each node's individual progress will be displayed in the UI. If you do not see the bootstrap progress advance, manually refresh the page in your browser to update the status.

It may take up to 60 minutes or more for the cluster to form, depending on the number of nodes in the cluster, and all the features to start. When cluster configuration is complete, the page will reload to the Nexus Dashboard GUI.

Step 12 Verify that the cluster is healthy.

After the cluster becomes available, you can access it by browsing to any one of your nodes' management IP addresses. The default password for the `admin` user is the same as the `rescue-user` password you chose for the first node. During this time, the UI will display a banner at the top stating "Service Installation is in progress, Nexus Dashboard configuration tasks are currently disabled".

After all the cluster is deployed and all services are started, you can look at the **Anomaly Level** on the **Home** > **Overview** page to ensure the cluster is healthy:



Alternatively, you can log in to any one node using SSH as the `rescue-user` using the password you entered during node deployment and using the `acs health` command to see the status:

- While the cluster is converging, you may see the following output:

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- When the cluster is up and running, the following output will be displayed:

```
$ acs health
All components are healthy
```

Note
In some situations, you might power cycle a node (power it off and then back on) and find it stuck in this stage:

```
deploy base system services
```

This is due to an issue with `etcd` on the node after a reboot of the physical Nexus Dashboard cluster.

To resolve the issue, enter the `acs reboot clean` command on the affected node.

Step 13 (Optional) Connect your Cisco Nexus Dashboard cluster to Cisco Intersight for added visibility and benefits. Refer to *Working with Cisco Intersight* for detailed steps.

Step 14 After you have deployed Nexus Dashboard, see the collections page for this release for configuration information.

What to do next

The next task is to create the fabrics and fabric groups. See the *Creating Fabrics and Fabric Groups* article for this release on the Cisco Nexus Dashboard collections page.

CHAPTER 6

Deploying in VMware ESX

- Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX, on page 75
- Deploy Nexus Dashboard Using VMware vCenter, on page 77
- Deploy Nexus Dashboard Directly in VMware ESXi, on page 91

Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX

Before you proceed with deploying the Nexus Dashboard cluster in VMware ESX, you must:

- Ensure that the ESX form factor supports your scale requirements.

  Scale support and co-hosting vary based on the cluster form factor you plan to deploy. You can use the Nexus Dashboard Capacity Planning tool to verify that the virtual form factor satisfies your deployment requirements.

Note Some deployments may require only a single ESX virtual node for one or more specific use cases. In that case, the capacity planning tool will indicate the requirement and you can simply skip the additional node deployment step in the following sections.

- Review and complete the general prerequisites described in Prerequisites and Guidelines, on page 9.

  This document describes how to initially deploy the base Nexus Dashboard cluster. If you want to expand an existing cluster with additional nodes (such as `secondary` or `standby`), see the "Infrastructure Management" chapter of the *Cisco Nexus Dashboard User Guide* instead, which is available from the Nexus Dashboard UI or online at *Cisco Nexus Dashboard User Guide*

- Ensure that the CPU family used for the Nexus Dashboard VMs supports AVX instruction set.
- The disk must have I/O latency of 20ms or less.
- Choose the type of node to deploy:
  - Data node—Node profile with higher system requirements designed for specific Nexus Dashboard features that require the additional resources.

- App node—Node profile with a smaller resource footprint that can be used for most Nexus Dashboard features.

Note Some larger scale deployments may require additional secondary nodes. If you plan to add secondary nodes to your Nexus Dashboard cluster, you can deploy all nodes (the initial 3-node cluster and the additional secondary nodes) using the OVA-App profile. Detailed scale information is available in the *Cisco Nexus Dashboard Verified Scalability Guide* for your release.

Ensure you have enough system resources:

Table 13: Deployment requirements

Data node requirements	App node requirements

• VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3, 8.0, 8.0.2, 8.0.3
• VMware vCenter 7.0.1, 7.0.2, 7.0.3, 8.0, 8.0.2, 8.0.3 if deploying using VMware vCenter
• Each node/VM requires the following:
  • 32 vCPUs with physical CPU reservation of at least 35,200 MHz
  • 128GB of RAM with physical reservation
  • 3TB SSD storage for the data volume and an additional 50GB for the system volume
  `Data` nodes must be deployed on storage with the following minimum performance requirements:
  • The SSD must be attached to the data store directly or in JBOD mode if using a RAID Host Bus Adapter (HBA)
  • The SSDs must be optimized for `Mixed Use/Application` (not `Read-Optimized`)
  • 4K Random Read IOPS: `93000`
  • 4K Random Write IOPS: `31000`
• We recommend that each Nexus Dashboard node is deployed in a different ESXi server.
	• VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3, 8.0, 8.0.2, 8.0.3
	• VMware vCenter 7.0.1, 7.0.2, 7.0.3, 8.0, 8.0.2, 8.0.3 if deploying using VMware vCenter
	• Each node/VM requires the following:
	  • 16 vCPUs with physical CPU reservation of at least 17,600 MHz
	  • 64GB of RAM with physical reservation
	  • 500GB HDD or SSD storage for the data volume and an additional 50GB for the system volume
	  Some features require `App` nodes to be deployed on faster SSD storage while other features support HDD. Check the Nexus Dashboard Capacity Planning tool to ensure that you use the correct type of storage.
	• We recommend that each Nexus Dashboard node is deployed in a different ESXi server.

- If you plan to configure VLAN ID for the cluster nodes' data interfaces, you must enable VLAN 4095 on the data interface port group in VMware vCenter for Virtual Guest VLAN Tagging (VGT) mode. If you specify a VLAN ID for Nexus Dashboard data interfaces, the packets must carry a Dot1q tag with that VLAN ID. When you set an explicit VLAN tag in a port group in the vSwitch and attach it to a Nexus Dashboard VM's VNIC, the vSwitch removes the Dot1q tag from the packet coming from the uplink before it sends the packet to that VNIC. Because the virtual Nexus Dashboard node expects the Dot1q tag, you must enable VLAN 4095 on the data interface port group to allow all VLANs.
- After each node's VM is deployed, ensure that the VMware Tools' periodic time synchronization is disabled as described in the deployment procedure in the next section.
- VMware vMotion is not supported for Nexus Dashboard cluster nodes.
- VMware Distributed Resource Scheduler (DRS) is not supported for Nexus Dashboard cluster nodes.

  If you have DRS enabled at the ESXi cluster level, you must explicitly disable it for the Nexus Dashboard VMs during deployment as described in the following section.
- Deploying using the content library is not supported.
- VMware snapshots are supported with virtual Nexus Dashboard VMs under the following conditions:
  - Snapshots must be taken while the VMs are powered off. Taking snapshots while the VMs are powered on is not supported.
  - Snapshots must be taken for all VMs that are part of the same cluster together.
  - When rolling back to a previous snapshot, all VMs that belong to the same cluster must be rolled back at the same time.
- Cisco does not support the use of nested virtualization environments. Deploying Nexus Dashboard on a virtual machine that is itself running on a virtualized hypervisor (for example, KVM on ESXi) is not a supported configuration and may result in performance degradation or system instability.
- You can choose to deploy the nodes directly in ESXi or using VMware vCenter.

  If you want to deploy using VMware vCenter, following the steps described in Deploy Nexus Dashboard Using VMware vCenter, on page 77.

  If you want to deploy directly in ESXi, following the steps described in Deploy Nexus Dashboard Directly in VMware ESXi, on page 91.

Deploy Nexus Dashboard Using VMware vCenter

This section describes how to deploy Cisco Nexus Dashboard cluster using VMware vCenter. If you prefer to deploy directly in ESXi, follow the steps described in Deploy Nexus Dashboard Directly in VMware ESXi, on page 91 instead.

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX, on page 75.

Procedure

Step 1 Obtain the Cisco Nexus Dashboard OVA image.

a) Browse to the Software Download page.

https://software.cisco.com/download/home/286327743/type/286328258/

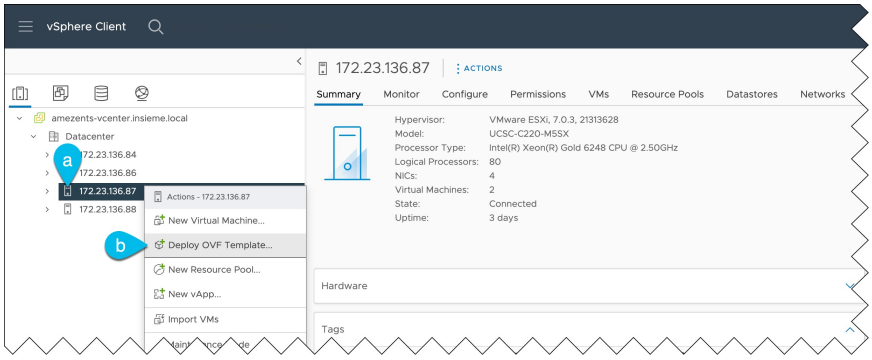
b) Choose the Nexus Dashboard release version you want to download.

c) Click the **Download** icon next to the Nexus Dashboard OVA image (`nd-dk9.<version>.ova`).

Step 2 Log in to your VMware vCenter.

Depending on the version of your vSphere client, the location and order of configuration screens may differ slightly. The following steps provide deployment details using VMware vSphere Client 7.0.

Step 3 Start the new VM deployment.

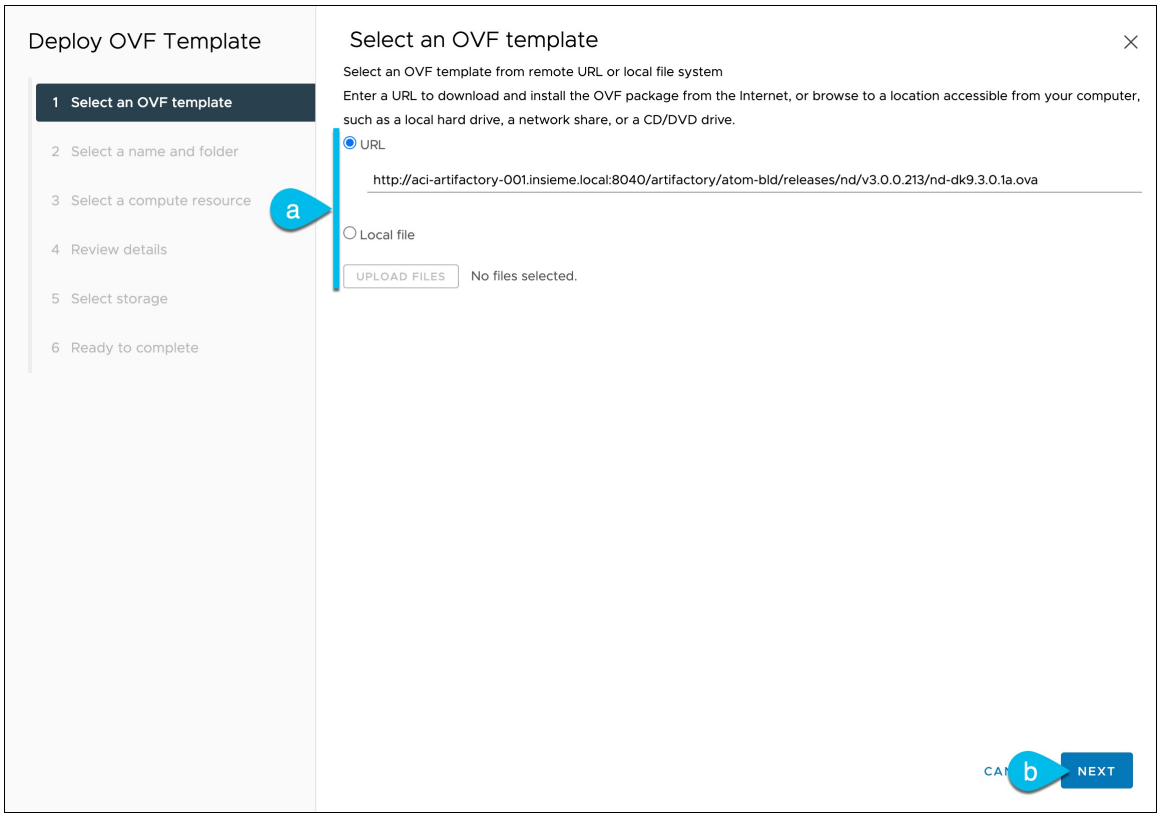


a) Right-click the ESX host where you want to deploy the VM.

b) Select **Deploy OVF Template...**

The **Deploy OVF Template** wizard appears.

Step 4 In the **Select an OVF template** screen, provide the OVA image.



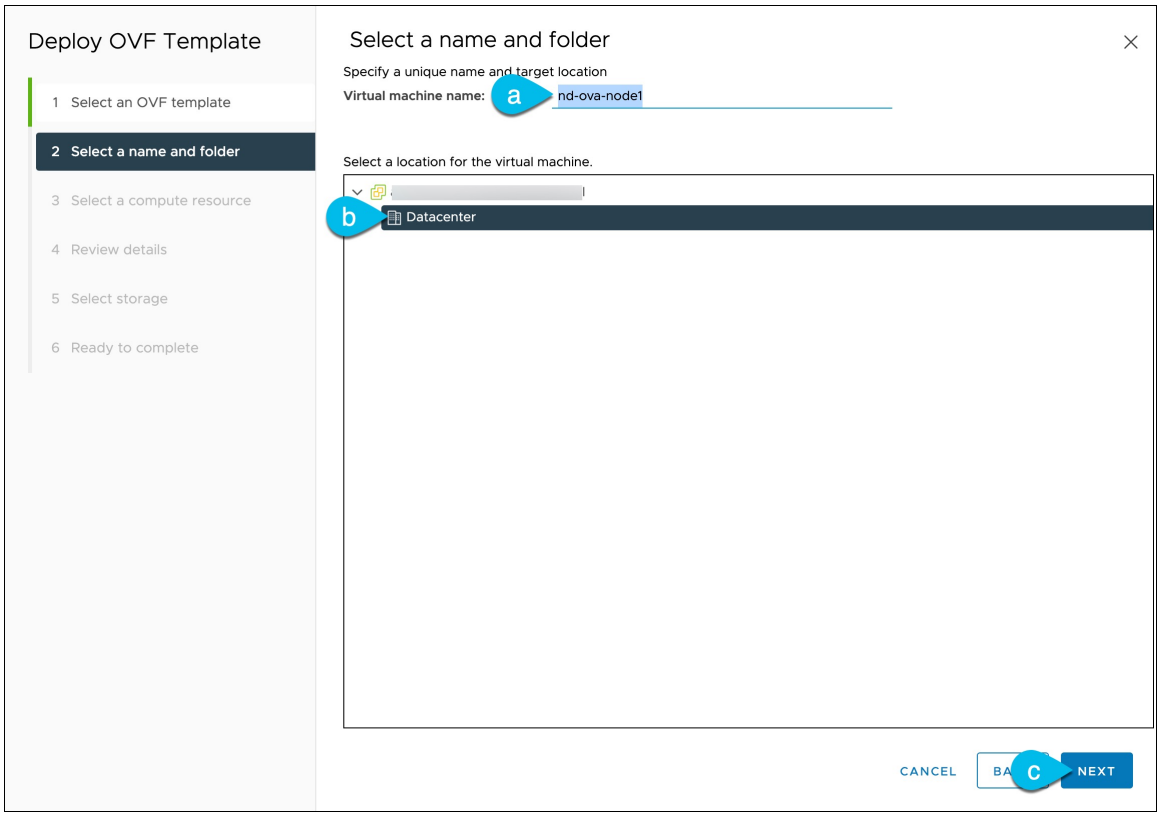
a) Provide the location of the image.

If you hosted the image on a web server in your environment, select **URL** and provide the URL to the image as shown in the above screenshot.

If your image is local, select **Local file** and click **Choose Files** to select the OVA file you downloaded.

b) Click **Next** to continue.

Step 5 In the **Select a name and folder** screen, provide a name and location for the VM.



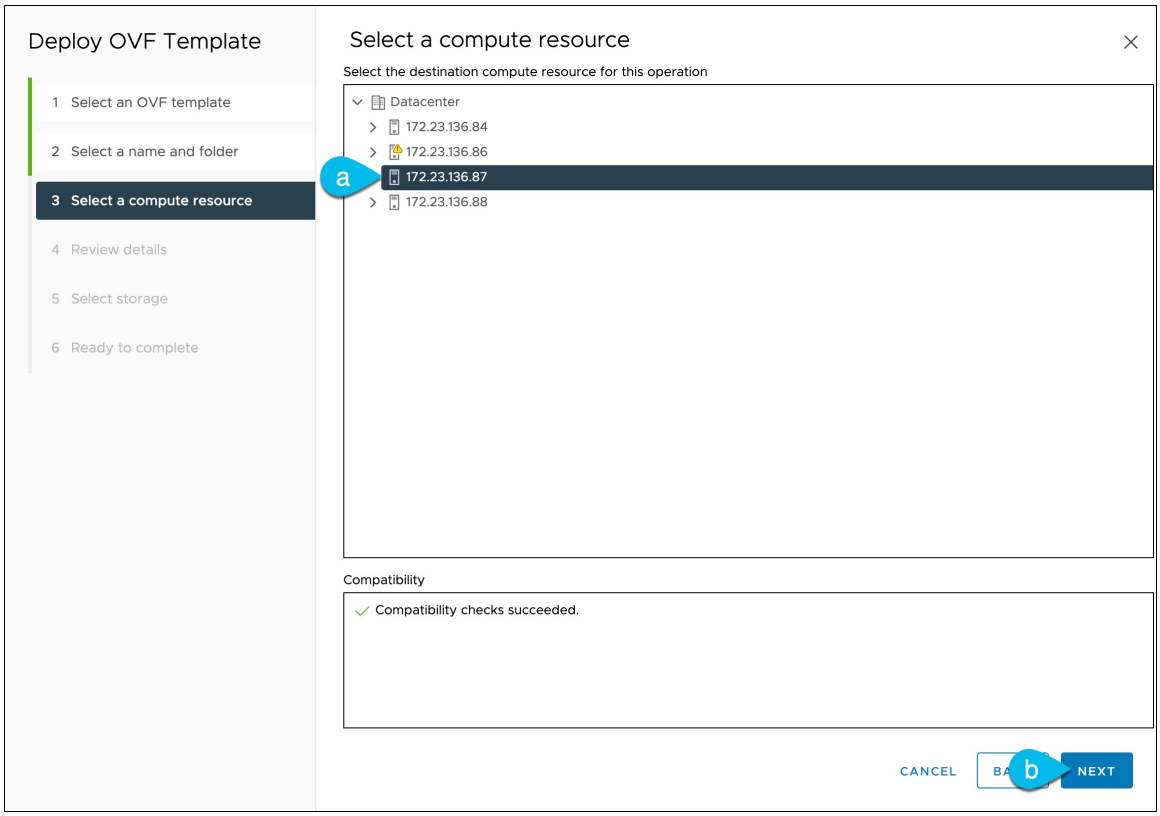
a) Provide the name for the virtual machine.

   For example, `nd-ova-node1`.

b) Select the location for the virtual machine.

c) Click **Next** to continue

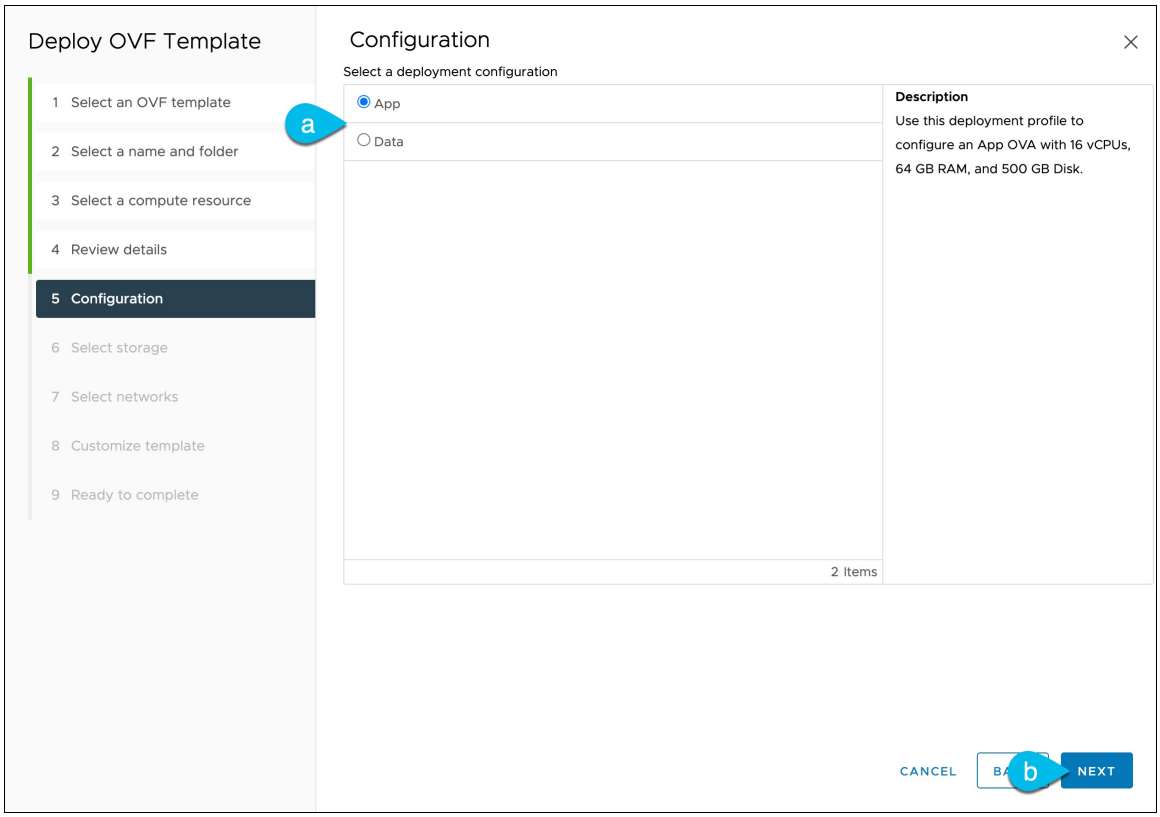
Step 6 In the **Select a compute resource** screen, select the ESX host.



a) Select the vCenter data center and the ESX host for the virtual machine.
b) Click **Next** to continue

Step 7 In the **Review details** screen, click **Next** to continue.

Step 8 In the **Configuration** screen, select the node profile you want to deploy.

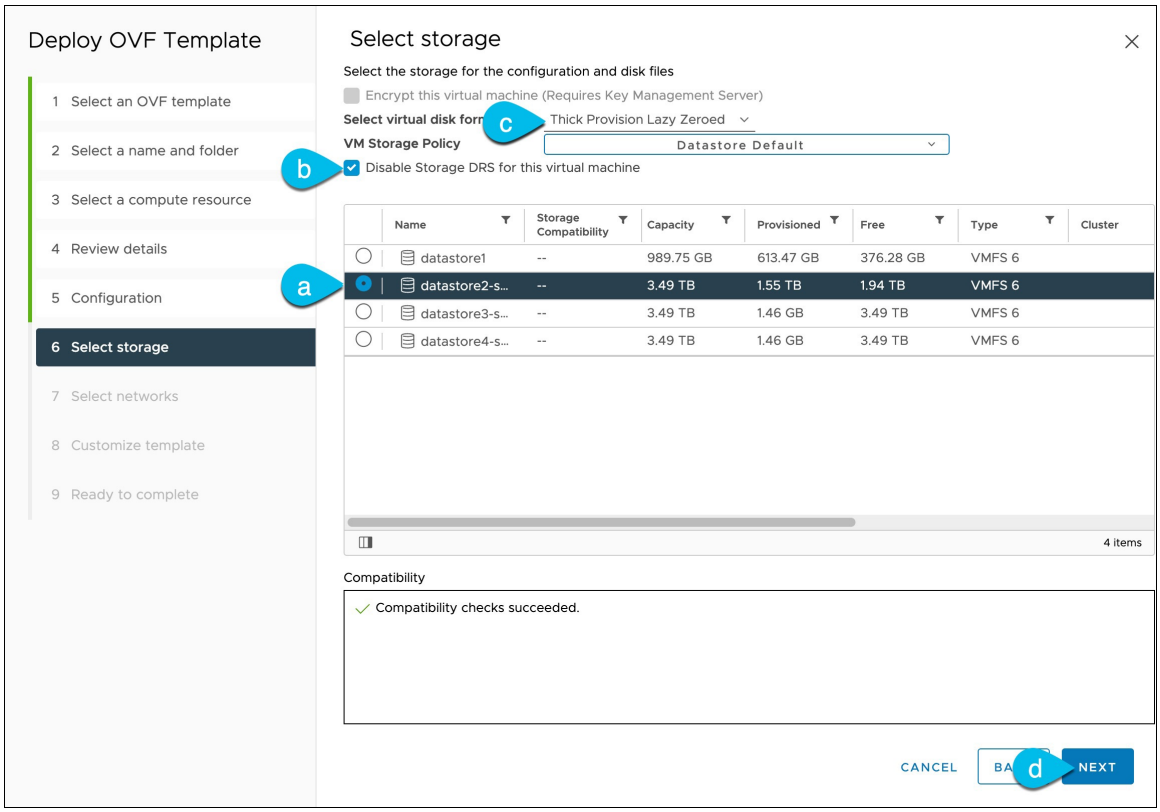


a) Select either `App` or `Data` node profile based on your use case requirements.

For more information about the node profiles, see Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX, on page 75.

b) Click **Next** to continue

Step 9 In the **Select storage** screen, provide the storage information.



a) Select the datastore for the virtual machine.

We recommend a unique datastore for each node.

b) Check the **Disable Storage DRS for this virtual machine** checkbox.

Nexus Dashboard does not support VMware DRS.

c) From the **Select virtual disk format** drop-down, choose `Thick Provisioning Lazy Zeroed`.

d) Click **Next** to continue

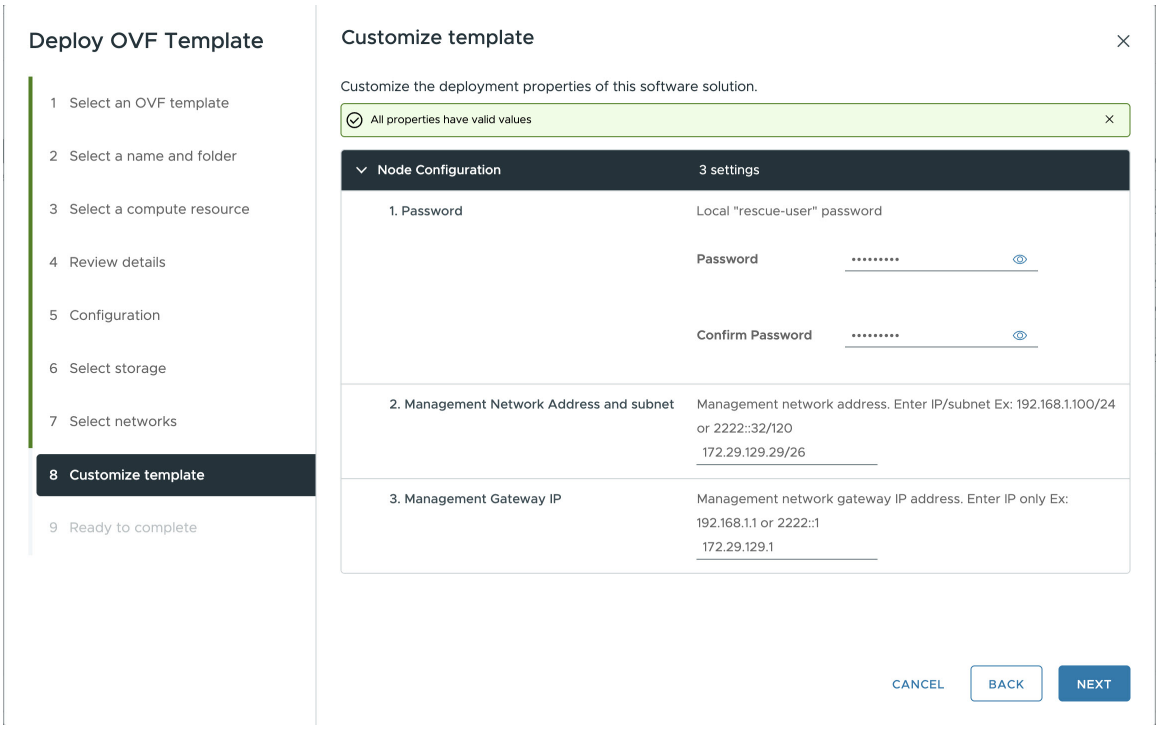
Step 10 In the **Select networks** screen, choose the VM network for the Nexus Dashboard's Management and Data networks and click **Next** to continue.

There are two networks required by the Nexus Dashboard cluster, both of which that have ports configured for high availability:

- **Data network**: The bonded ports **fabric0/fabric1** are used for the Nexus Dashboard cluster's data network.
- **Management network**: The bonded ports **mgmt0/mgmt1** are used for the Nexus Dashboard cluster's management network.

For more information about these networks, see General prerequisites and guidelines, on page 9 in the "Deployment Overview and Requirements" chapter.

Step 11 In the **Customize template** screen, provide the required information.



a) Choose the APP/Data type.
b) Provide and confirm the **Password**.

   This password is used for the `rescue-user` account on each node.

   Note
   You must provide the same password for all nodes or the cluster creation will fail.

c) Provide the **Management Network** IP address and netmask.
d) Provide the **Management Network** IP gateway.
e) Click **Next** to continue.

Step 12 In the **Ready to complete** screen, verify that all information is accurate and click **Finish** to begin deploying the first node.

Step 13 Repeat previous steps to deploy the additional nodes.

Note
If you are deploying a single-node cluster, you can skip this step.

For multi-node clusters, you must deploy two additional `Primary` nodes and as many `Secondary` nodes as required by your specific use case. The total number of required nodes is available in the Nexus Dashboard Capacity Planning tool.

You do not need to wait for the first node's VM deployment to complete, you can begin deploying the other two nodes simultaneously. The steps to deploy the second and third nodes are identical to the first node's.

Step 14 Wait for the VM(s) to finish deploying.

Step 15 Ensure that the VMware Tools periodic time synchronization is disabled, then start the VMs.

To disable time synchronization:

a) Right-click the node's VM and select **Edit Settings**.

b) In the **Edit Settings** window, select the **VM Options** tab.
c) Expand the **`VMware Tools`** category and uncheck the **`Synchronize time periodically`** option.

Step 16 Open your browser and navigate to `https://<node-mgmt-ip>` to open the GUI.

The rest of the configuration workflow takes place from one of the node's GUI. You can choose any one of the nodes you deployed to begin the bootstrap process and you do not need to log in to or configure the other two nodes directly.

Enter the password you entered in a previous step and click **Login**

Step 17 Enter the requested information in the **Basic Information** page of the **Cluster Bringup** wizard.

a) For **Cluster Name**, enter a name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

b) For **Select the Nexus Dashboard Implementation type**, choose either **LAN** or **SAN** then click **Next**.

Step 18 Enter the requested information in the **Configuration** page of the **Cluster Bringup** wizard.

a) (Optional) If you want to enable IPv6 functionality for the cluster, put a check in the **Enable IPv6** checkbox.
b) Click **+Add DNS provider** to add one or more DNS servers, enter the DNS provider IP address, then click the checkmark icon.
c) (Optional) Click **+Add DNS search domain** to add a search domain, enter the DNS search domain IP address, then click the checkmark icon.
d) (Optional) If you want to enable NTP server authentication, put a check in the **NTP Authentication** checkbox.
e) If you enabled NTP authentication, click **+ Add Key**, enter the required information, and click the checkmark icon to save the information.

- **Key**–Enter the NTP authentication key, which is a cryptographic key that is used to authenticate the NTP traffic between the Nexus Dashboard and the NTP servers. You will define the NTP servers in the following step, and multiple NTP servers can use the same NTP authentication key.
- **ID**–Enter a key ID for the NTP host. Each NTP key must be assigned a unique key ID, which is used to identify the appropriate key to use when verifying the NTP packet.
- **Authentication Type**–Choose authentication type for the NTP key.
- Put a check in the **Trusted** checkbox if you want this key to be trusted. Untrusted keys cannot be used for NTP authentication.

For the complete list of NTP authentication requirements and guidelines, see General prerequisites and guidelines, on page 9.

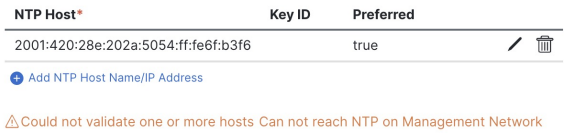
If you want to enter additional NTP keys, click **+ Add Key** again and enter the information.

f) If you enabled NTP authentication, click **+Add NTP Host Name/IP Address**, enter the required information, and click the checkmark icon to save the information.

- **NTP Host**–Enter an IP address; fully qualified domain names (FQDN) are not supported.
- **Key ID**–Enter the key ID of the NTP key you defined in the previous substep.

  If NTP authentication is disabled, this field is grayed out.
- Put a check in the **Preferred** checkbox if you want this host to be preferred.

Note
If the node into which you are logged in is configured with only an IPv4 address, but you have checked **Enable IPv6** in a previous step and entered an IPv6 address for an NTP server, you will get the following validation error:



This is because the node does not have an IPv6 address yet and is unable to connect to an IPv6 address of the NTP server. You will enter IPv6 address in the next step. In this case, enter the other required information as described in the following steps and click **Next** to proceed to the next page where you will enter IPv6 addresses for the nodes.

If you want to enter additional NTP servers, click **+Add NTP Host Name/IP Address** again and enter the information.

g) For **Proxy Server**, enter the URL or IP address of a proxy server.

For clusters that do not have direct connectivity to Cisco cloud, we recommend configuring a proxy server to establish the connectivity. This allows you to mitigate risk from exposure to non-conformant hardware and software in your fabrics.

You can click **+Add Ignore Host** to enter one or more destination IP addresses for which traffic will skip using the proxy.

The proxy server must have these URLs enabled:

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

If you do not want to configure a proxy, click **Skip Proxy** then click **Confirm**.

h) (Optional) If your proxy server requires authentication, put a check in the **Authentication required for Proxy** checkbox and enter the login credentials.

i) (Optional) Expand the **Advanced Settings** category and change the settings if required.

Under advanced settings, you can configure these settings:

- **App Network**–The address space used by the application's services running in the Nexus Dashboard. Enter the IP address and netmask.
- **Service Network**–An internal network used by Nexus Dashboard and its processes. Enter the IP address and netmask.
- **App Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the app network.
- **Service Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the service network.

For more information about the application and service networks, see General prerequisites and guidelines, on page 9.

j) Click **Next**.

Step 19 In the **Node Details** page, update the first node's information.

You have defined the Management network and IP address for the node into which you are currently logged in during the initial node configuration in earlier steps, but you must also enter the Data network information for the node before you can proceed with adding the other `primary` nodes and creating the cluster.

a) For **Cluster Connectivity**, if your cluster is deployed in L3 HA mode, choose **BGP**. Otherwise, choose **L2**.

BGP configuration is required for the persistent IP addresses feature used by telemetry. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed. All remaining nodes need to configure BGP if it is configured. You must enable BGP now if the data network of nodes have different subnets.

b) Click the **Edit** button next to the first node.

The node's **Serial Number**, **Management Network** information, and **Type** are automatically populated, but you must enter the other information.

c) For **Name**, enter a name for the node.

The node's **Name** will be set as its hostname, so it must follow the RFC-1123 requirements.

Note
If you need to change the name but the **Name** field is not editable, run the CIMC validation again to fix this issue.

d) For **Type**, choose **Primary**.

The first nodes of the cluster must be set to **Primary**. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, enter the node's data network information.

Enter the data network IP address, netmask, and gateway. Optionally, you can also enter the VLAN ID for the network. Leave the VLAN ID field blank if your configuration does not require VLAN. If you chose **BGP** for **Cluster Connectivity**, enter the ASN.

If you enabled IPv6 functionality in a previous page, you must also enter the IPv6 address, netmask, and gateway.

Note
If you want to enter IPv6 information, you must do so during the cluster bootstrap process. To change the IP address configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) If you chose **BGP** for **Cluster Connectivity**, then in the **BGP peer details** area, enter the peer's IPv4 address and ASN.

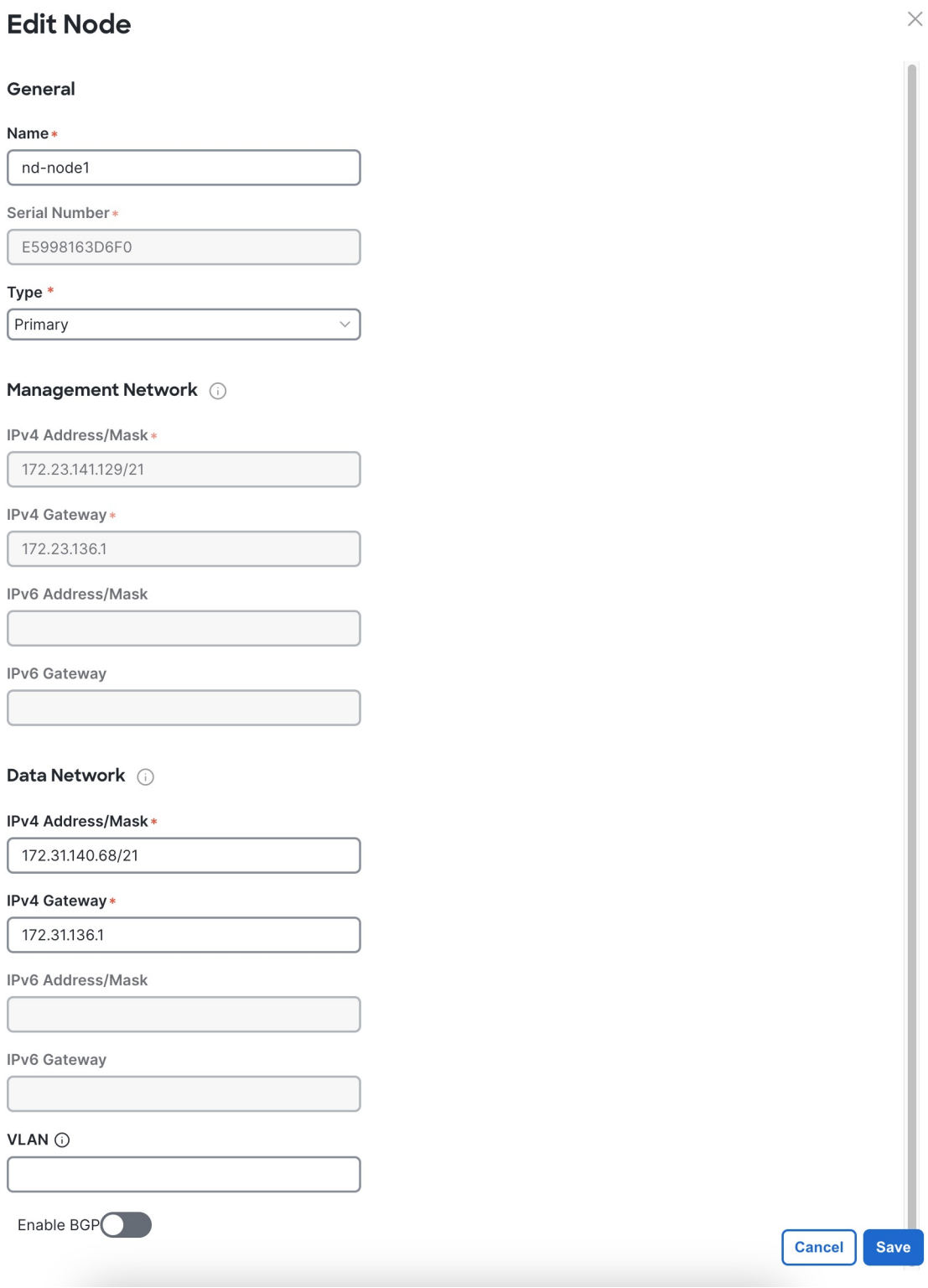
You can click **+ Add IPv4 BGP peer** to add addition peers.

If you enabled IPv6 functionality in a previous page, you must also enter the peer's IPv6 address and ASN.

g) Click **Save** to save the changes.

Step 20 In the **Node Details** screen, click **Add Node** to add the second node to the cluster.

If you are deploying a single-node cluster, skip this step.



a) In the **Deployment Details** area, provide the **Management IP Address** and **Password** for the second node

You defined the management network information and the password during the initial node configuration steps.

b) Click **Validate** to verify connectivity to the node.

The node's **Serial Number** and the **Management Network** information are automatically populated after connectivity is validated.

c) Provide the **Name** for the node.

d) From the **Type** dropdown, select `Primary`.

The first 3 nodes of the cluster must be set to `Primary`. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, provide the node's **Data Network** information.

You must provide the data network IP address, netmask, and gateway. Optionally, you can also provide the VLAN ID for the network. For most deployments, you can leave the VLAN ID field blank.

If you had enabled IPv6 functionality in a previous screen, you must also provide the IPv6 address, netmask, and gateway.

Note
If you want to provide IPv6 information, you must do it during cluster bootstrap process. To change IP configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) (Optional) If your cluster is deployed in L3 HA mode, **Enable BGP** for the data network.

BGP configuration is required for the persistent IP addresses feature. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed.

If you choose to enable BGP, you must also provide the following information:

- **ASN** (BGP Autonomous System Number) of this node.

  You can configure the same ASN for all nodes or a different ASN per node.

- For pure IPv6, the **Router ID** of this node.

  The router ID must be an IPv4 address, for example `1.1.1.1`

- **BGP Peer Details**, which includes the peer's IPv4 or IPv6 address and peer's ASN.

g) Click **Save** to save the changes.

h) Repeat this step for the final (third) primary node of the cluster.

Step 21 (Optional) Repeat the previous step to enter information about any additional secondary or standby nodes.

Note
To support higher scale, you must provide a sufficient number of secondary nodes during deployment. Refer to the Nexus Dashboard Cluster Sizing tool for exact number of additional secondary nodes required for your specific use case.

You can choose to add the standby nodes now or at a later time after the cluster is deployed.

Step 22 In the **Node Details** page, verify the information that you entered, then click **Next**.

Step 23 In the **Persistent IPs** page, if you want to add more persistent IP addresses, click **+ Add Data Service IP Address**, enter the IP address, and click the checkmark icon. Repeat this step as many times as desired, then click **Next**.

You must configure the minimum number of required persistent IP addresses during the bootstrap process. This step enables you to add more persistent IP addresses if desired.

Step 24 In the **Summary** page, review and verify the configuration information, click **Save**, and click **Continue** to confirm the correct deployment mode and proceed with building the cluster.

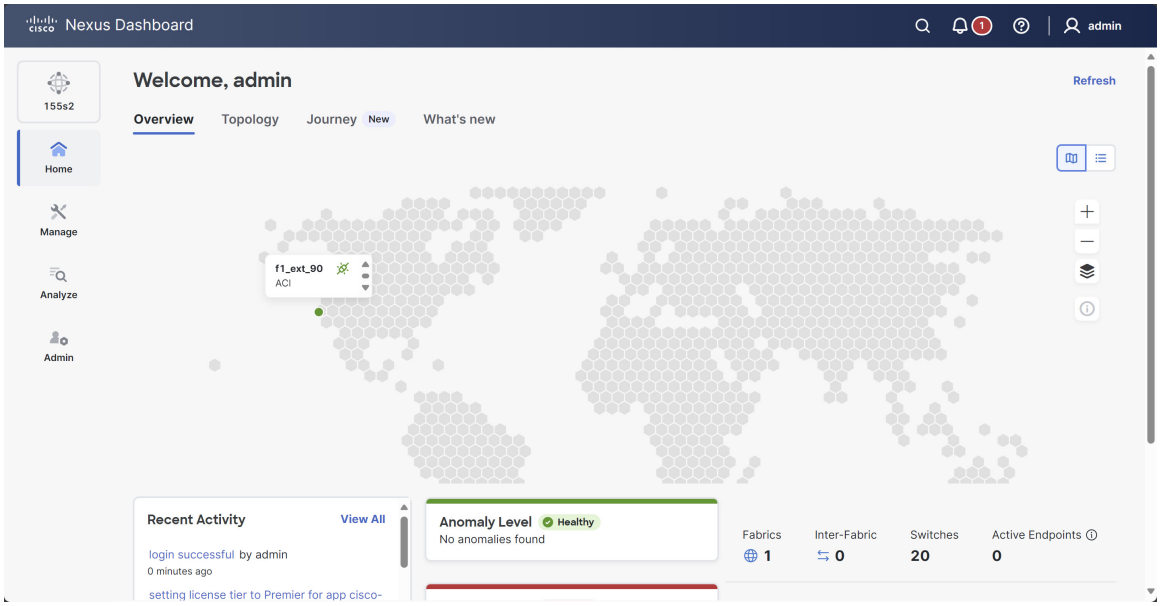
During the node bootstrap and cluster bring-up, the overall progress as well as each node's individual progress will be displayed in the UI. If you do not see the bootstrap progress advance, manually refresh the page in your browser to update the status.

It may take up to 60 minutes or more for the cluster to form, depending on the number of nodes in the cluster, and all the features to start. When cluster configuration is complete, the page will reload to the Nexus Dashboard GUI.

Step 25 Verify that the cluster is healthy.

After the cluster becomes available, you can access it by browsing to any one of your nodes' management IP addresses. The default password for the `admin` user is the same as the `rescue-user` password you chose for the first node. During this time, the UI will display a banner at the top stating "Service Installation is in progress, Nexus Dashboard configuration tasks are currently disabled".

After all the cluster is deployed and all services are started, you can look at the **Anomaly Level** on the **Home** > **Overview** page to ensure the cluster is healthy:



Alternatively, you can log in to any one node using SSH as the `rescue-user` using the password you entered during node deployment and using the `acs health` command to see the status:

- While the cluster is converging, you may see the following output:

```
$ acs health
k8s install is in-progress
```

```
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- When the cluster is up and running, the following output will be displayed:

```
$ acs health
All components are healthy
```

Note
In some situations, you might power cycle a node (power it off and then back on) and find it stuck in this stage:

```
deploy base system services
```

This is due to an issue with `etcd` on the node after a reboot of the physical Nexus Dashboard cluster.

To resolve the issue, enter the `acs reboot clean` command on the affected node.

Step 26 (Optional) Connect your Cisco Nexus Dashboard cluster to Cisco Intersight for added visibility and benefits. Refer to *Working with Cisco Intersight* for detailed steps.

Step 27 After you have deployed Nexus Dashboard, see the collections page for this release for configuration information.

What to do next

The next task is to create the fabrics and fabric groups. See the *Creating Fabrics and Fabric Groups* article for this release on the Cisco Nexus Dashboard collections page.

Deploy Nexus Dashboard Directly in VMware ESXi

This section describes how to deploy Cisco Nexus Dashboard cluster directly in VMware ESXi. If you prefer to deploy using vCenter, follow the steps described in Deploy Nexus Dashboard Directly in VMware ESXi, on page 91 instead.

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX, on page 75.

Procedure

Step 1 Obtain the Cisco Nexus Dashboard OVA image.

a) Browse to the Software Download page.

https://software.cisco.com/download/home/286327743/type/286328258/

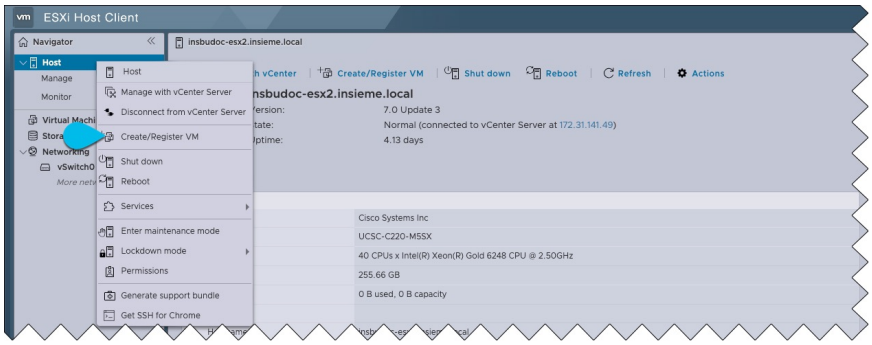
b) Choose the Nexus Dashboard release version you want to download.

c) Click the **Download** icon next to the Nexus Dashboard OVA image (`nd-dk9.<version>.ova`).

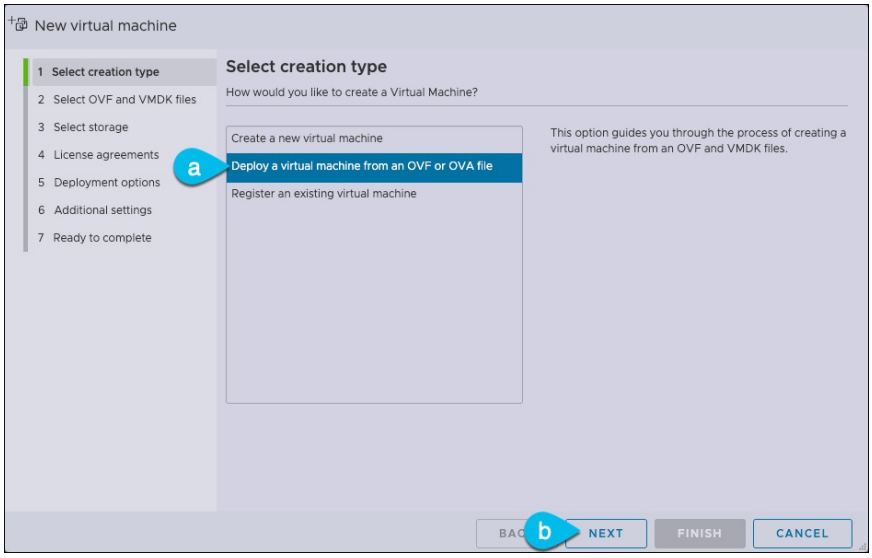
Step 2 Log in to your VMware ESXi.

Depending on the version of your ESXi server, the location and order of configuration screens may differ slightly. The following steps provide deployment details using VMware ESXi 7.0.

Step 3 Right-click the host and select **Create/Register VM**.



Step 4 In the **Select creation type** screen, choose `Deploy a virtual machine from an OVF or OVA file`, then click **Next**.



Step 5 In the **Select OVF and VMDK files** screen, provide the virtual machine name (for example, `nd-ova-node1`) and the OVA image you downloaded in the first step, then click **Next**.

Step 6 In the **Select storage** screen, choose the datastore for the VM, then click **Next**.

Step 7 In the **Select OVF and VMDK files** screen, provide the virtual machine name (for example, `nd-node1`) and the OVA image you downloaded in the first step, then click **Next**.

Step 8 Specify the **Deployment options**.

In the **Deployment options** screen, provide the following:

- From the **Network mappings** dropdowns, choose the networks for the Nexus Dashboard management (`mgmt0`) and data (`fabric0`) interfaces.

  Nexus Dashboard networks are described in General prerequisites and guidelines, on page 9.

- From the **Deployment type** dropdown, choose the node profile (`App` or `Data`).

  Node profiles are described in Prerequisites and guidelines for deploying the Nexus Dashboard cluster in VMware ESX, on page 75.

- For **Disk provisioning** type, choose `Thick`.
- Disable the **Power on automatically** option.

Step 9 In the **Ready to complete** screen, verify that all information is accurate and click **Finish** to begin deploying the first node.

Step 10 Repeat previous steps to deploy the second and third nodes.

Note
If you are deploying a single-node cluster, you can skip this step.

You do not need to wait for the first node deployment to complete, you can begin deploying the other two nodes simultaneously.

Step 11 Wait for the VM(s) to finish deploying.

Step 12 Ensure that the VMware Tools periodic time synchronization is disabled, then start the VMs.

To disable time synchronization:

a) Right-click the node's VM and select **Edit Settings**.
b) In the **Edit Settings** window, select the **VM Options** tab.
c) Expand the **`VMware Tools`** category and uncheck the **`Synchronize guest time with host`** option.

Step 13 Open one of the node's console and configure the node's basic information.

a) Begin initial setup.

You will be prompted to run the first-time setup utility:

```
[ OK ] Started atomix-boot-setup.
       Starting Initial cloud-init job (pre-networking)...
       Starting logrotate...
       Starting logwatch...
       Starting keyhole...
[ OK ] Started keyhole.
[ OK ] Started logrotate.
[ OK ] Started logwatch.

Press any key to run first-boot setup on this console...
```

b) Enter and confirm the `admin` password

This password will be used for the `rescue-user` SSH login as well as the initial GUI password.

Note
You must provide the same password for all nodes or the cluster creation will fail.

```
Admin Password:
Reenter Admin Password:
```

c) Enter the management network information.

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

d) For the first node only, designate it as the "Cluster Leader".

You will log into the cluster leader node to finish configuration and complete cluster creation.

```
Is this the cluster leader?: y
```

e) Review and confirm the entered information.

You will be asked if you want to change the entered information. If all the fields are correct, choose `n` to proceed. If you want to change any of the entered information, enter `y` to re-start the basic configuration script.

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: no

Re-enter config? (y/N): n
```

Step 14 Repeat previous steps to deploy the additional nodes.

If you are deploying a single-node cluster, you can skip this step.

For multi-node clusters, you must deploy two additional `Primary` nodes and as many `Secondary` nodes as required by your specific use case. The total number of required nodes is available in the Nexus Dashboard Capacity Planning tool.

You do not need to wait for the first node configuration to complete, you can begin configuring the other two nodes simultaneously.

Note
You must provide the same password for all nodes or the cluster creation will fail.

The steps to deploy additional nodes are identical with the only exception being that you must indicate that they are not the **Cluster Leader**.

Step 15 Open your browser and navigate to `https://<node-mgmt-ip>` to open the GUI.

The rest of the configuration workflow takes place from one of the node's GUI. You can choose any one of the nodes you deployed to begin the bootstrap process and you do not need to log in to or configure the other two nodes directly.

Enter the password you entered in a previous step and click **Login**

Step 16 Enter the requested information in the **Basic Information** page of the **Cluster Bringup** wizard.

a) For **Cluster Name**, enter a name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

b) For **Select the Nexus Dashboard Implementation type**, choose either **LAN** or **SAN** then click **Next**.

Step 17 Enter the requested information in the **Configuration** page of the **Cluster Bringup** wizard.

a) (Optional) If you want to enable IPv6 functionality for the cluster, put a check in the **Enable IPv6** checkbox.
b) Click **+Add DNS provider** to add one or more DNS servers, enter the DNS provider IP address, then click the checkmark icon.
c) (Optional) Click **+Add DNS search domain** to add a search domain, enter the DNS search domain IP address, then click the checkmark icon.
d) (Optional) If you want to enable NTP server authentication, put a check in the **NTP Authentication** checkbox.
e) If you enabled NTP authentication, click **+ Add Key**, enter the required information, and click the checkmark icon to save the information.

- **Key**–Enter the NTP authentication key, which is a cryptographic key that is used to authenticate the NTP traffic between the Nexus Dashboard and the NTP servers. You will define the NTP servers in the following step, and multiple NTP servers can use the same NTP authentication key.

- **ID**–Enter a key ID for the NTP host. Each NTP key must be assigned a unique key ID, which is used to identify the appropriate key to use when verifying the NTP packet.
- **Authentication Type**–Choose authentication type for the NTP key.
- Put a check in the **Trusted** checkbox if you want this key to be trusted. Untrusted keys cannot be used for NTP authentication.

For the complete list of NTP authentication requirements and guidelines, see General prerequisites and guidelines, on page 9.

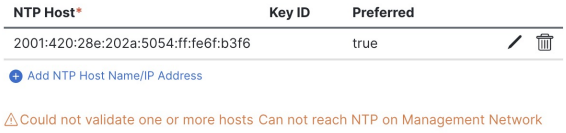
If you want to enter additional NTP keys, click **+ Add Key** again and enter the information.

f) If you enabled NTP authentication, click **+Add NTP Host Name/IP Address**, enter the required information, and click the checkmark icon to save the information.

- **NTP Host**–Enter an IP address; fully qualified domain names (FQDN) are not supported.
- **Key ID**–Enter the key ID of the NTP key you defined in the previous substep.

  If NTP authentication is disabled, this field is grayed out.
- Put a check in the **Preferred** checkbox if you want this host to be preferred.

Note
If the node into which you are logged in is configured with only an IPv4 address, but you have checked **Enable IPv6** in a previous step and entered an IPv6 address for an NTP server, you will get the following validation error:



This is because the node does not have an IPv6 address yet and is unable to connect to an IPv6 address of the NTP server. You will enter IPv6 address in the next step. In this case, enter the other required information as described in the following steps and click **Next** to proceed to the next page where you will enter IPv6 addresses for the nodes.

If you want to enter additional NTP servers, click **+Add NTP Host Name/IP Address** again and enter the information.

g) For **Proxy Server**, enter the URL or IP address of a proxy server.

For clusters that do not have direct connectivity to Cisco cloud, we recommend configuring a proxy server to establish the connectivity. This allows you to mitigate risk from exposure to non-conformant hardware and software in your fabrics.

You can click **+Add Ignore Host** to enter one or more destination IP addresses for which traffic will skip using the proxy.

The proxy server must have these URLs enabled:

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

If you do not want to configure a proxy, click **Skip Proxy** then click **Confirm**.

h) (Optional) If your proxy server requires authentication, put a check in the **Authentication required for Proxy** checkbox and enter the login credentials.

i) (Optional) Expand the **Advanced Settings** category and change the settings if required.

Under advanced settings, you can configure these settings:

- **App Network**–The address space used by the application's services running in the Nexus Dashboard. Enter the IP address and netmask.
- **Service Network**–An internal network used by Nexus Dashboard and its processes. Enter the IP address and netmask.
- **App Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the app network.
- **Service Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the service network.

For more information about the application and service networks, see General prerequisites and guidelines, on page 9.

j) Click **Next**.

Step 18 In the **Node Details** page, update the first node's information.

You have defined the Management network and IP address for the node into which you are currently logged in during the initial node configuration in earlier steps, but you must also enter the Data network information for the node before you can proceed with adding the other `primary` nodes and creating the cluster.

a) For **Cluster Connectivity**, if your cluster is deployed in L3 HA mode, choose **BGP**. Otherwise, choose **L2**.

BGP configuration is required for the persistent IP addresses feature used by telemetry. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed. All remaining nodes need to configure BGP if it is configured. You must enable BGP now if the data network of nodes have different subnets.

b) Click the **Edit** button next to the first node.

The node's **Serial Number**, **Management Network** information, and **Type** are automatically populated, but you must enter the other information.

c) For **Name**, enter a name for the node.

The node's **Name** will be set as its hostname, so it must follow the RFC-1123 requirements.

Note
If you need to change the name but the **Name** field is not editable, run the CIMC validation again to fix this issue.

d) For **Type**, choose **Primary**.

The first nodes of the cluster must be set to **Primary**. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, enter the node's data network information.

Enter the data network IP address, netmask, and gateway. Optionally, you can also enter the VLAN ID for the network. Leave the VLAN ID field blank if your configuration does not require VLAN. If you chose **BGP** for **Cluster Connectivity**, enter the ASN.

If you enabled IPv6 functionality in a previous page, you must also enter the IPv6 address, netmask, and gateway.

Note
If you want to enter IPv6 information, you must do so during the cluster bootstrap process. To change the IP address configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) If you chose **BGP** for **Cluster Connectivity**, then in the **BGP peer details** area, enter the peer's IPv4 address and ASN.

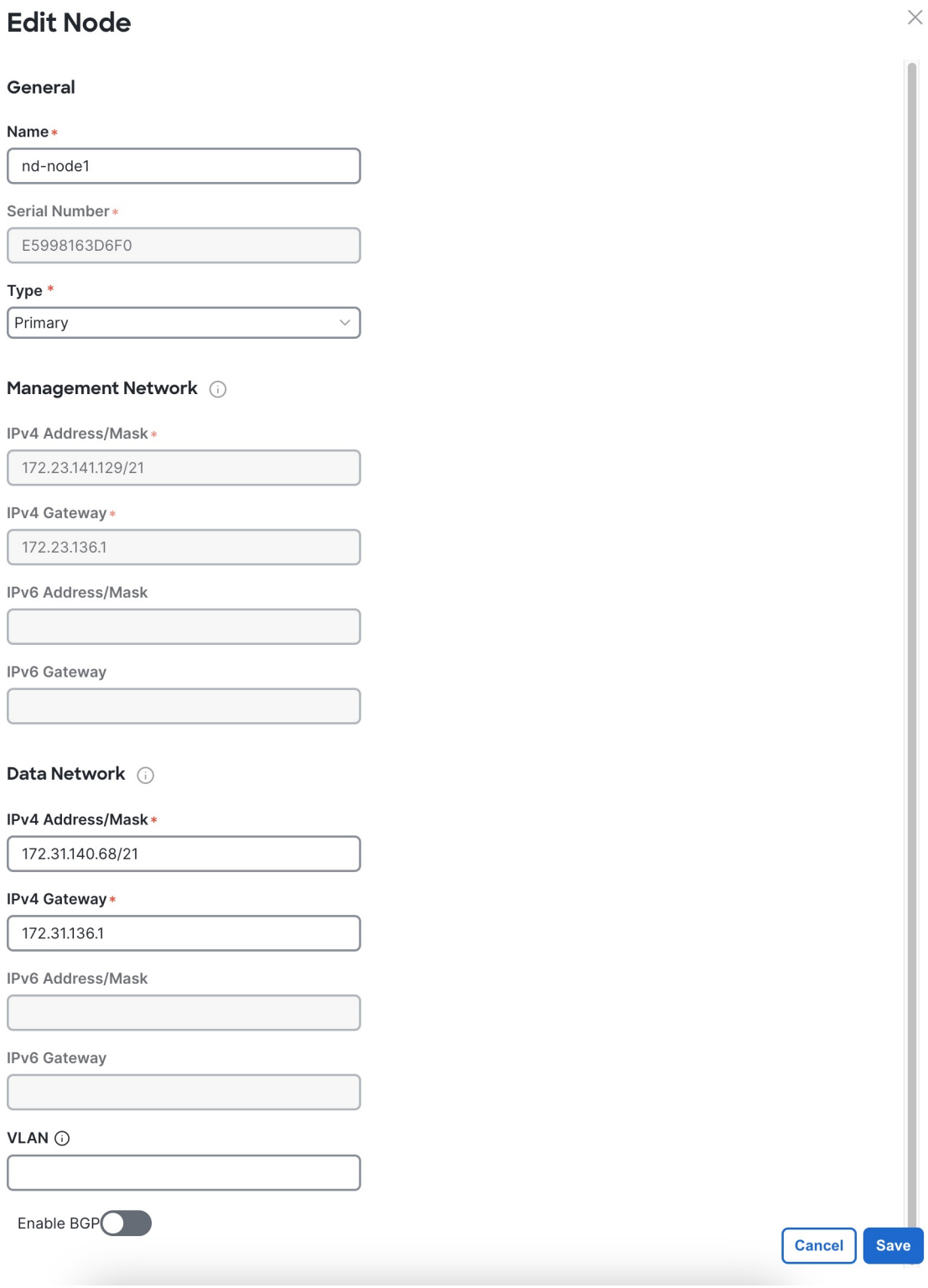
You can click **+ Add IPv4 BGP peer** to add addition peers.

If you enabled IPv6 functionality in a previous page, you must also enter the peer's IPv6 address and ASN.

g) Click **Save** to save the changes.

Step 19 In the **Node Details** screen, click **Add Node** to add the second node to the cluster.

If you are deploying a single-node cluster, skip this step.



a) In the **Deployment Details** area, provide the **Management IP Address** and **Password** for the second node

You defined the management network information and the password during the initial node configuration steps.

b) Click **Validate** to verify connectivity to the node.

The node's **Serial Number** and the **Management Network** information are automatically populated after connectivity is validated.

c) Provide the **Name** for the node.

d) From the **Type** dropdown, select `Primary`.

The first 3 nodes of the cluster must be set to `Primary`. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, provide the node's **Data Network** information.

You must provide the data network IP address, netmask, and gateway. Optionally, you can also provide the VLAN ID for the network. For most deployments, you can leave the VLAN ID field blank.

If you had enabled IPv6 functionality in a previous screen, you must also provide the IPv6 address, netmask, and gateway.

Note
If you want to provide IPv6 information, you must do it during cluster bootstrap process. To change IP configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) (Optional) If your cluster is deployed in L3 HA mode, **Enable BGP** for the data network.

BGP configuration is required for the persistent IP addresses feature. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed.

If you choose to enable BGP, you must also provide the following information:

- **ASN** (BGP Autonomous System Number) of this node.

  You can configure the same ASN for all nodes or a different ASN per node.

- For pure IPv6, the **Router ID** of this node.

  The router ID must be an IPv4 address, for example `1.1.1.1`

- **BGP Peer Details**, which includes the peer's IPv4 or IPv6 address and peer's ASN.

g) Click **Save** to save the changes.

h) Repeat this step for the final (third) primary node of the cluster.

Step 20 (Optional) Repeat the previous step to enter information about any additional secondary or standby nodes.

Note
To support higher scale, you must provide a sufficient number of secondary nodes during deployment. Refer to the Nexus Dashboard Cluster Sizing tool for exact number of additional secondary nodes required for your specific use case.

You can choose to add the standby nodes now or at a later time after the cluster is deployed.

Step 21 In the **Node Details** page, verify the information that you entered, then click **Next**.

Step 22 In the **Persistent IPs** page, if you want to add more persistent IP addresses, click **+ Add Data Service IP Address**, enter the IP address, and click the checkmark icon. Repeat this step as many times as desired, then click **Next**.

You must configure the minimum number of required persistent IP addresses during the bootstrap process. This step enables you to add more persistent IP addresses if desired.

Step 23 In the **Summary** page, review and verify the configuration information, click **Save**, and click **Continue** to confirm the correct deployment mode and proceed with building the cluster.

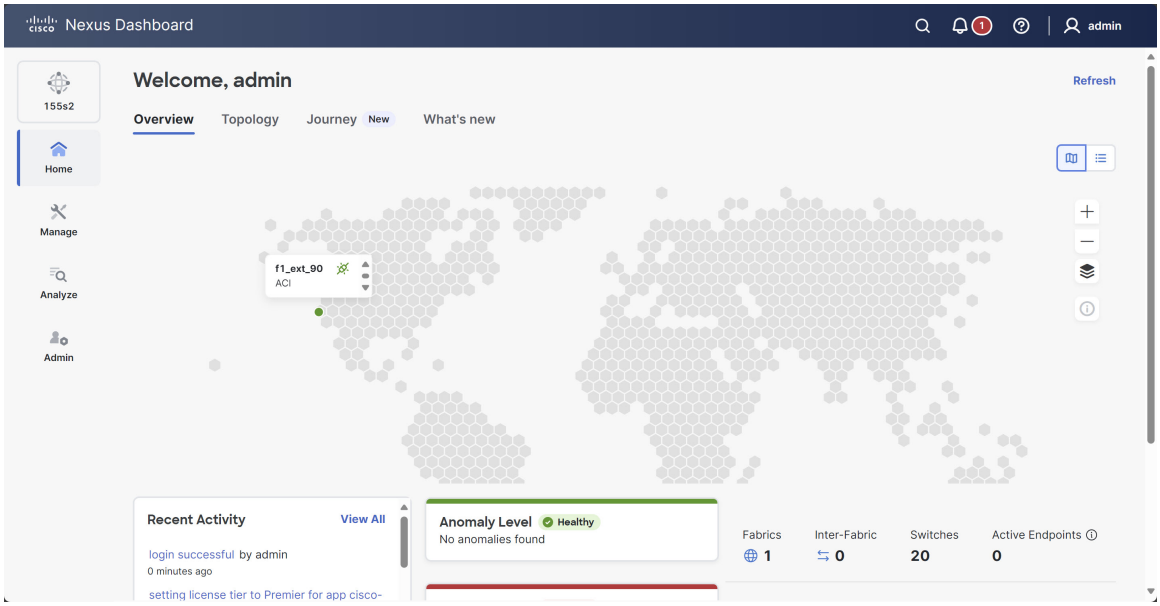
During the node bootstrap and cluster bring-up, the overall progress as well as each node's individual progress will be displayed in the UI. If you do not see the bootstrap progress advance, manually refresh the page in your browser to update the status.

It may take up to 60 minutes or more for the cluster to form, depending on the number of nodes in the cluster, and all the features to start. When cluster configuration is complete, the page will reload to the Nexus Dashboard GUI.

Step 24 Verify that the cluster is healthy.

After the cluster becomes available, you can access it by browsing to any one of your nodes' management IP addresses. The default password for the `admin` user is the same as the `rescue-user` password you chose for the first node. During this time, the UI will display a banner at the top stating "Service Installation is in progress, Nexus Dashboard configuration tasks are currently disabled".

After all the cluster is deployed and all services are started, you can look at the **Anomaly Level** on the **Home** > **Overview** page to ensure the cluster is healthy:



Alternatively, you can log in to any one node using SSH as the `rescue-user` using the password you entered during node deployment and using the `acs health` command to see the status:

- While the cluster is converging, you may see the following output:

```
$ acs health
k8s install is in-progress

$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

- When the cluster is up and running, the following output will be displayed:

```
$ acs health
All components are healthy
```

Note
In some situations, you might power cycle a node (power it off and then back on) and find it stuck in this stage:

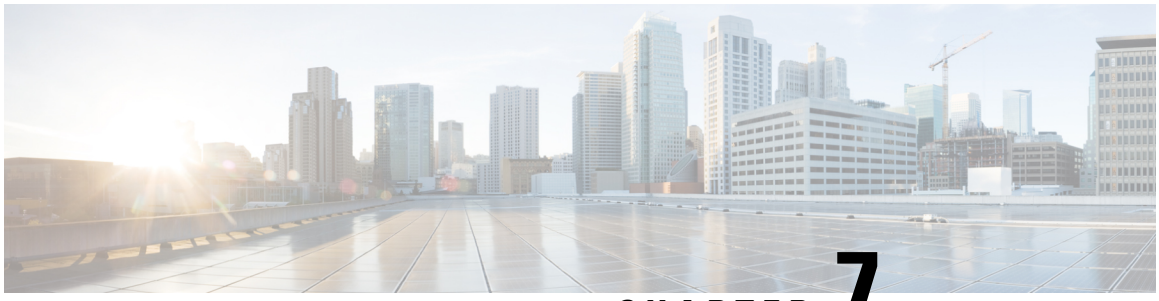
```
deploy base system services
```

This is due to an issue with `etcd` on the node after a reboot of the physical Nexus Dashboard cluster.

To resolve the issue, enter the `acs reboot clean` command on the affected node.

Step 25 (Optional) Connect your Cisco Nexus Dashboard cluster to Cisco Intersight for added visibility and benefits. Refer to *Working with Cisco Intersight* for detailed steps.

Step 26 After you have deployed Nexus Dashboard, see the collections page for this release for configuration information.



CHAPTER 7

Deploying in Linux KVM

- Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Linux KVM, on page 103
- Deploy Nexus Dashboard in Linux KVM, on page 105

Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Linux KVM

Before you proceed with deploying the Nexus Dashboard cluster in a Linux KVM, the KVM must meet these prerequisites and you must follow these guidelines:

- The KVM form factor must support your scale requirements.

  Scale support and co-hosting vary based on the cluster form factor. You can use the Nexus Dashboard Capacity Planning tool to verify that the virtual form factor satisfies your deployment requirements.

- Review and complete the general prerequisites described in Prerequisites and Guidelines, on page 9.
- The CPU family used for the Nexus Dashboard VMs must support the AVX instruction set.
- The KVM must have enough system resources, and each node requires a dedicated disk partition. See Understanding system resources, on page 104 for more information.
- The disk must have I/O latency of 20ms or less.

  See Verify the I/O latency of a Linux KVM storage device, on page 104

- Cisco does not support the use of nested virtualization environments. Deploying Nexus Dashboard on a virtual machine that is itself running on a virtualized hypervisor (for example, KVM on ESXi) is not a supported configuration and may result in performance degradation or system instability.
- KVM deployments are supported for NX-OS and ACI fabrics, as well as for SAN deployments.
- You must deploy in Red Hat Enterprise Linux 8.8, 8.10, or 9.4.
- In order for Nexus Dashboard to be up and running on OS reboot scenarios, you must add the UUIDs in the `fstab conf` files of your RHEL host operating system, which is the only way to preserve the Nexus Dashboard upon a reboot of the RHEL operating system.
- You must also configure the following required network bridges at the host level for Nexus Dashboard deployments:

- Management Network Bridge (mgmt-bridge): The external network to manage Nexus Dashboard.
- Data Network Bridge (data-bridge): The internal network used to form clustering within Nexus Dashboard.

- We recommend that each Nexus Dashboard node is deployed in a different KVM hypervisor.

Verify the I/O latency of a Linux KVM storage device

When you deploy a Nexus Dashboard cluster in a Linux KVM, the storage device of the KVM must have a latency under 20ms.

Follow these steps to verify the I/O latency of a Linux KVM storage device.

Procedure

Step 1 Create a test directory.

For example, create a directory named `test-data`.

Step 2 Run the Flexible I/O tester (FIO).

```
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data --size=22m --bs=2300 --name=mytest
```

Step 3 After you use the command, confirm that the `99.00th=[value]` in the `fsync/fdatasync/sync_file_range` section is under 20ms.

Understanding system resources

When deploying a Nexus Dashboard cluster in Linux KVM, the KVM must have enough system resources. There are multiple form factors supported with a virtual Nexus Dashboard KVM, and the amount of system resources needed for each node differs based on the form factor.

Table 14: Per node resource requirements

Form factor	Number or vCPUs	RAM size	Disk size
1-node KVM (app)	16	64 GB	550 GB
1-node KVM (data)	32	128 GB	3 TB
3-node KVM (app)	16	64 GB	550 GB
3-node KVM (data)	32	128 GB	3 TB

You will need to know the information above for your form factor when you go through the procedures in Deploy Nexus Dashboard in Linux KVM, on page 105.

Deploy Nexus Dashboard in Linux KVM

This section describes how to deploy Cisco Nexus Dashboard cluster in Linux KVM.

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Linux KVM, on page 103.

Procedure

Step 1 Download the Cisco Nexus Dashboard image.

a) Browse to the Software Download page.

https://software.cisco.com/download/home/286327743/type/286328258

b) Click **Nexus Dashboard Software**.

c) From the left sidebar, choose the Nexus Dashboard version you want to download.

d) Download the Cisco Nexus Dashboard image for Linux KVM (`nd-dk9.<version>.qcow2`).

Step 2 Copy the image to the Linux KVM servers where you will host the nodes.

You can use `scp` to copy the image, for example:

```
# scp nd-dk9.<version>.qcow2 root@<kvm-host-ip>:/home/nd-base
```

The following steps assume you copied the image into the `/home/nd-base` directory.

Step 3 Make the following configurations on each KVM host:

a) Edit `/etc/libvirt/qemu.conf` and make sure the user and group is correctly configured based on the ownership of the storage that you plan to use for the Nexus Dashboard deployment.

This is only required if you plan to use disk storage paths that are different from the default `libvirtd`.

b) Edit `/etc/libvirt/libvirt.conf` and uncomment `uri_default`.

c) Restart the `libvirtd` service after updating the configuration using the `systemctl restart libvirtd` command from root.

Step 4 Log in to your KVM host as the `root` user and perform the following steps to create the required disk images on each node.

As mentioned in Understanding system resources, on page 104, you will need a total of 550 GB or 3 TB of SSD storage to create two disk images:

- Boot disk based on QCOW2 image that you downloaded
- Data disk

a) Verify that you have a directory with enough space to store the VM disks (for example, `/home/nd-node1`) or mount the storage disk (raw disk or LVM) to directory `/opt/cisco/nd`.

b) Create the following script as `/root/create_vm.sh` under the root directory.

Note

If you manually type this information, verify that there are no empty spaces present after any of these lines.

Create the script based on the information provided in Understanding system resources, on page 104 for your form factor:

- For 1-node or 3-node KVM (**app**) form factors:

```
#!/bin/bash -ex

# Configuration
# Name of Nexus Dashboard Virtual machine
name=nd1

# Path of Nexus Dashboard QCOW2 image.
nd_qcow2=/home/nd-base/nd-dk9.4.1.1g.qcow2

# Disk Path to storage Boot and Data Disks.
data_disk=/opt/cisco/nd/data

# Management Network Bridge
mgmt_bridge=mgmt-bridge

# Data Network bridge
data_bridge=data-bridge

# Data Disk Size
data_size=500G

# CPU Cores
cpus=16

# Memory in units of MB.
memory=65536

# actual script
rm -rf $data_disk/boot.img
/usr/bin/qemu-img convert -f qcow2 -O raw $nd_qcow2 $data_disk/boot.img
rm -rf $data_disk/disk.img
/usr/bin/qemu-img create -f raw $data_disk/disk.img $data_size
virt-install \
--import \
--name $name \
--memory $memory \
--vcpus $cpus \
--os-type generic \
--osinfo detect=on,require=off \
--check path_in_use=off \
--disk path=${data_disk}/boot.img,format=raw,bus=virtio \
--disk path=${data_disk}/disk.img,format=raw,bus=virtio \
--network bridge=$mgmt_bridge,model=virtio \
--network bridge=$data_bridge,model=virtio \
--console pty,target_type=serial \
--noautoconsole \
--autostart
```

- For 1-node or 3-node KVM (**data**) form factors:

```
#!/bin/bash -ex

# Configuration
# Name of Nexus Dashboard Virtual machine
name=nd1

# Path of Nexus Dashboard QCOW2 image.
```

```
nd_qcow2=/home/nd-base/nd-dk9.4.1.1g.qcow2

# Disk Path to storage Boot and Data Disks.
data_disk=/opt/cisco/nd/data

# Management Network Bridge
mgmt_bridge=mgmt-bridge

# Data Network bridge
data_bridge=data-bridge

# Data Disk Size
data_size=3072G

# CPU Cores
cpus=32

# Memory in units of MB.
memory=131072

# actual script
rm -rf $data_disk/boot.img
/usr/bin/qemu-img convert -f qcow2 -O raw $nd_qcow2 $data_disk/boot.img
rm -rf $data_disk/disk.img
/usr/bin/qemu-img create -f raw $data_disk/disk.img $data_size
virt-install \
--import \
--name $name \
--memory $memory \
--vcpus $cpus \
--os-type generic \
--osinfo detect=on,require=off \
--check path_in_use=off \
--disk path=${data_disk}/boot.img,format=raw,bus=virtio \
--disk path=${data_disk}/disk.img,format=raw,bus=virtio \
--network bridge=$mgmt_bridge,model=virtio \
--network bridge=$data_bridge,model=virtio \
--console pty,target_type=serial \
--noautoconsole \
--autostart
```

Step 5 Make the `create_vm.sh` script executable and run it using these commands.

```
# chmod +x /root/create_vm.sh
# /root/create_vm.sh
```

Step 6 Repeat previous steps to deploy the second and third nodes, then start all VMs.

Note
If you are deploying a single-node cluster, you can skip this step.

Step 7 Open one of the node's console and configure the node's basic information.

a) Press any key to begin initial setup.

You will be prompted to run the first-time setup utility:

```
[ OK ] Started atomix-boot-setup.
       Starting Initial cloud-init job (pre-networking)...
       Starting logrotate...
       Starting logwatch...
       Starting keyhole...
[ OK ] Started keyhole.
```

```
[ OK ] Started logrotate.
[ OK ] Started logwatch.

Press any key to run first-boot setup on this console...
```

b) Enter and confirm the `admin` password

This password will be used for the `rescue-user` SSH login as well as the initial GUI password.

Note
You must provide the same password for all nodes or the cluster creation will fail.

```
Admin Password:
Reenter Admin Password:
```

c) Enter the management network information.

```
Management Network:
  IP Address/Mask: 192.168.9.172/24
  Gateway: 192.168.9.1
```

d) For the first node only, designate it as the "Cluster Leader".

You will log into the cluster leader node to finish configuration and complete cluster creation.

```
Is this the cluster leader?: y
```

e) Review and confirm the entered information.

You will be asked if you want to change the entered information. If all the fields are correct, choose `n` to proceed. If you want to change any of the entered information, enter `y` to re-start the basic configuration script.

```
Please review the config
Management network:
  Gateway: 192.168.9.1
  IP Address/Mask: 192.168.9.172/24
Cluster leader: yes

Re-enter config? (y/N): n
```

Step 8 Repeat previous step to configure the initial information for the second and third nodes.

You do not need to wait for the first node configuration to complete, you can begin configuring the other two nodes simultaneously.

Note
You must provide the same password for all nodes or the cluster creation will fail.

The steps to deploy the second and third nodes are identical with the only exception being that you must indicate that they are not the **Cluster Leader**.

Step 9 Wait for the initial bootstrap process to complete on all nodes.

After you provide and confirm management network information, the initial setup on the first node (`Cluster Leader`) configures the networking and brings up the UI, which you will use to add two other nodes and complete the cluster deployment.

```
Please wait for system to boot: [#########################] 100%
System up, please wait for UI to be online.

System UI online, please login to https://192.168.9.172 to continue.
```

Step 10 Open your browser and navigate to `https://<node-mgmt-ip>` to open the GUI.

The rest of the configuration workflow takes place from one of the node's GUI. You can choose any one of the nodes you deployed to begin the bootstrap process and you do not need to log in to or configure the other two nodes directly.

Enter the password you entered in a previous step and click **Login**

Step 11 Enter the requested information in the **Basic Information** page of the **Cluster Bringup** wizard.

a) For **Cluster Name**, enter a name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

b) For **Select the Nexus Dashboard Implementation type**, choose either **LAN** or **SAN** then click **Next**.

Step 12 Enter the requested information in the **Configuration** page of the **Cluster Bringup** wizard.

a) (Optional) If you want to enable IPv6 functionality for the cluster, put a check in the **Enable IPv6** checkbox.

b) Click **+Add DNS provider** to add one or more DNS servers, enter the DNS provider IP address, then click the checkmark icon.

c) (Optional) Click **+Add DNS search domain** to add a search domain, enter the DNS search domain IP address, then click the checkmark icon.

d) (Optional) If you want to enable NTP server authentication, put a check in the **NTP Authentication** checkbox.

e) If you enabled NTP authentication, click **+ Add Key**, enter the required information, and click the checkmark icon to save the information.

- **Key**–Enter the NTP authentication key, which is a cryptographic key that is used to authenticate the NTP traffic between the Nexus Dashboard and the NTP servers. You will define the NTP servers in the following step, and multiple NTP servers can use the same NTP authentication key.
- **ID**–Enter a key ID for the NTP host. Each NTP key must be assigned a unique key ID, which is used to identify the appropriate key to use when verifying the NTP packet.
- **Authentication Type**–Choose authentication type for the NTP key.
- Put a check in the **Trusted** checkbox if you want this key to be trusted. Untrusted keys cannot be used for NTP authentication.

For the complete list of NTP authentication requirements and guidelines, see General prerequisites and guidelines, on page 9.

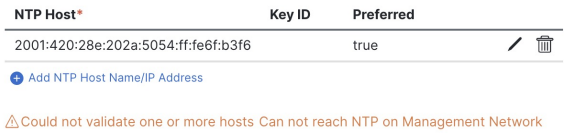
If you want to enter additional NTP keys, click **+ Add Key** again and enter the information.

f) If you enabled NTP authentication, click **+Add NTP Host Name/IP Address**, enter the required information, and click the checkmark icon to save the information.

- **NTP Host**–Enter an IP address; fully qualified domain names (FQDN) are not supported.
- **Key ID**–Enter the key ID of the NTP key you defined in the previous substep.

  If NTP authentication is disabled, this field is grayed out.
- Put a check in the **Preferred** checkbox if you want this host to be preferred.

Note
If the node into which you are logged in is configured with only an IPv4 address, but you have checked **Enable IPv6** in a previous step and entered an IPv6 address for an NTP server, you will get the following validation error:



This is because the node does not have an IPv6 address yet and is unable to connect to an IPv6 address of the NTP server. You will enter IPv6 address in the next step. In this case, enter the other required information as described in the following steps and click **Next** to proceed to the next page where you will enter IPv6 addresses for the nodes.

If you want to enter additional NTP servers, click **+Add NTP Host Name/IP Address** again and enter the information.

g) For **Proxy Server**, enter the URL or IP address of a proxy server.

For clusters that do not have direct connectivity to Cisco cloud, we recommend configuring a proxy server to establish the connectivity. This allows you to mitigate risk from exposure to non-conformant hardware and software in your fabrics.

You can click **+Add Ignore Host** to enter one or more destination IP addresses for which traffic will skip using the proxy.

The proxy server must have these URLs enabled:

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

If you do not want to configure a proxy, click **Skip Proxy** then click **Confirm**.

h) (Optional) If your proxy server requires authentication, put a check in the **Authentication required for Proxy** checkbox and enter the login credentials.

i) (Optional) Expand the **Advanced Settings** category and change the settings if required.

Under advanced settings, you can configure these settings:

- **App Network**–The address space used by the application's services running in the Nexus Dashboard. Enter the IP address and netmask.
- **Service Network**–An internal network used by Nexus Dashboard and its processes. Enter the IP address and netmask.
- **App Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the app network.
- **Service Network IPv6**–If you put a check in the **Enable IPv6** checkbox earlier, enter the IPv6 subnet for the service network.

For more information about the application and service networks, see General prerequisites and guidelines, on page 9.

j) Click **Next**.

Step 13 In the **Node Details** page, update the first node's information.

You have defined the Management network and IP address for the node into which you are currently logged in during the initial node configuration in earlier steps, but you must also enter the Data network information for the node before you can proceed with adding the other `primary` nodes and creating the cluster.

a) For **Cluster Connectivity**, if your cluster is deployed in L3 HA mode, choose **BGP**. Otherwise, choose **L2**.

BGP configuration is required for the persistent IP addresses feature used by telemetry. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed. All remaining nodes need to configure BGP if it is configured. You must enable BGP now if the data network of nodes have different subnets.

b) Click the **Edit** button next to the first node.

The node's **Serial Number**, **Management Network** information, and **Type** are automatically populated, but you must enter the other information.

c) For **Name**, enter a name for the node.

The node's **Name** will be set as its hostname, so it must follow the RFC-1123 requirements.

Note
If you need to change the name but the **Name** field is not editable, run the CIMC validation again to fix this issue.

d) For **Type**, choose **Primary**.

The first nodes of the cluster must be set to **Primary**. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, enter the node's data network information.

Enter the data network IP address, netmask, and gateway. Optionally, you can also enter the VLAN ID for the network. Leave the VLAN ID field blank if your configuration does not require VLAN. If you chose **BGP** for **Cluster Connectivity**, enter the ASN.

If you enabled IPv6 functionality in a previous page, you must also enter the IPv6 address, netmask, and gateway.

Note
If you want to enter IPv6 information, you must do so during the cluster bootstrap process. To change the IP address configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) If you chose **BGP** for **Cluster Connectivity**, then in the **BGP peer details** area, enter the peer's IPv4 address and ASN.

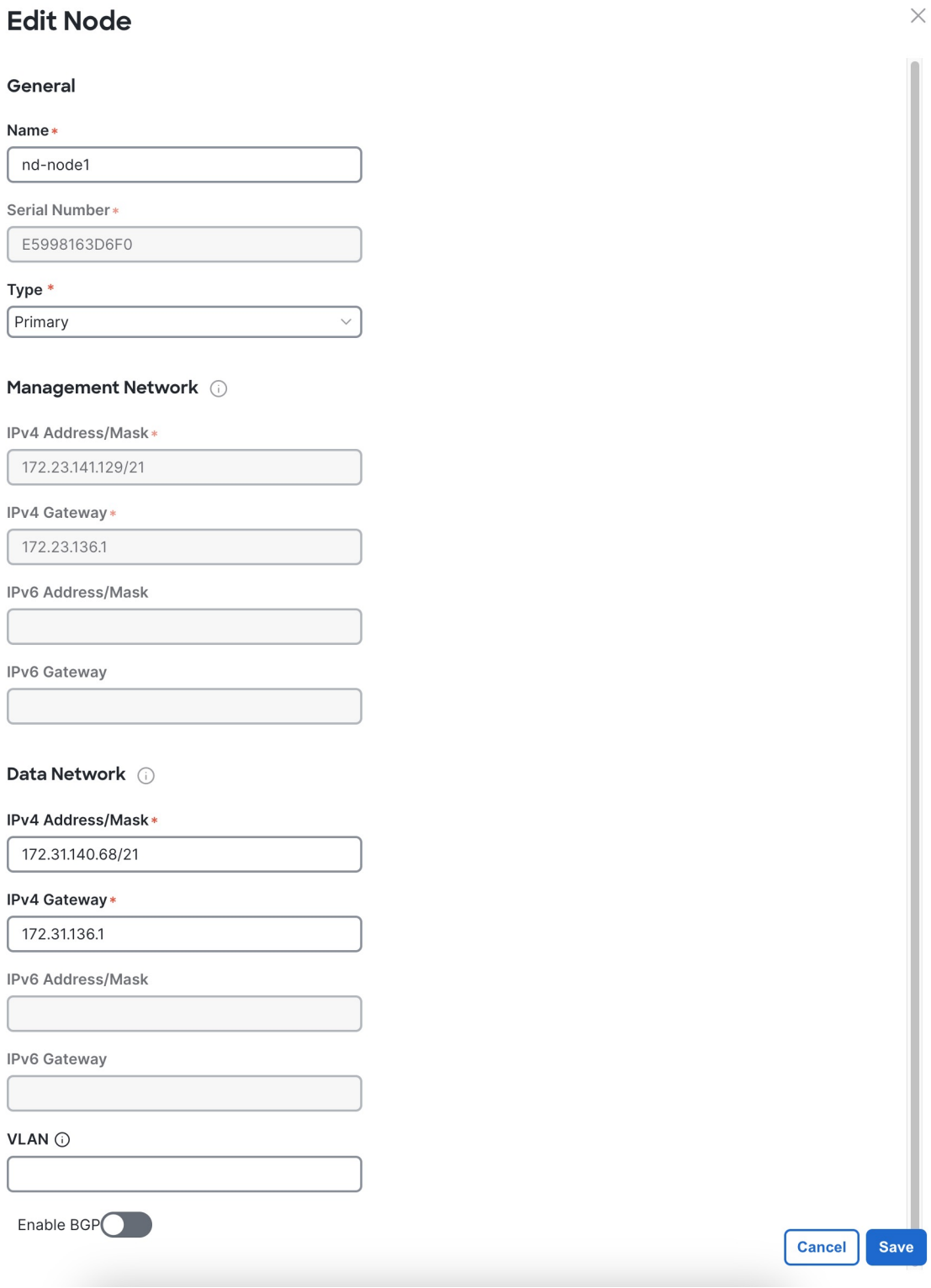
You can click **+ Add IPv4 BGP peer** to add addition peers.

If you enabled IPv6 functionality in a previous page, you must also enter the peer's IPv6 address and ASN.

g) Click **Save** to save the changes.

Step 14 In the **Node Details** screen, click **Add Node** to add the second node to the cluster.

If you are deploying a single-node cluster, skip this step.



a) In the **Deployment Details** area, provide the **Management IP Address** and **Password** for the second node

You defined the management network information and the password during the initial node configuration steps.

b) Click **Validate** to verify connectivity to the node.

The node's **Serial Number** and the **Management Network** information are automatically populated after connectivity is validated.

c) Provide the **Name** for the node.

d) From the **Type** dropdown, select `Primary`.

The first 3 nodes of the cluster must be set to `Primary`. You will add the secondary nodes in a later step if required for higher scale.

e) In the **Data Network** area, provide the node's **Data Network** information.

You must provide the data network IP address, netmask, and gateway. Optionally, you can also provide the VLAN ID for the network. For most deployments, you can leave the VLAN ID field blank.

If you had enabled IPv6 functionality in a previous screen, you must also provide the IPv6 address, netmask, and gateway.

Note
If you want to provide IPv6 information, you must do it during cluster bootstrap process. To change IP configuration later, you would need to redeploy the cluster.

All nodes in the cluster must be configured with either only IPv4, only IPv6, or dual stack IPv4/IPv6.

f) (Optional) If your cluster is deployed in L3 HA mode, **Enable BGP** for the data network.

BGP configuration is required for the persistent IP addresses feature. This feature is described in more detail in BGP configuration and persistent IP addresses, on page 45 and the "Persistent IP Addresses" sections of the *Cisco Nexus Dashboard User Guide*.

Note
You can enable BGP at this time or in the Nexus Dashboard GUI after the cluster is deployed.

If you choose to enable BGP, you must also provide the following information:

- **ASN** (BGP Autonomous System Number) of this node.

  You can configure the same ASN for all nodes or a different ASN per node.

- For pure IPv6, the **Router ID** of this node.

  The router ID must be an IPv4 address, for example `1.1.1.1`

- **BGP Peer Details**, which includes the peer's IPv4 or IPv6 address and peer's ASN.

g) Click **Save** to save the changes.

h) Repeat this step for the final (third) primary node of the cluster.

Step 15 In the **Node Details** page, verify the information that you entered, then click **Next**.

Step 16 Choose the **Deployment Mode** for the cluster.

a) Click **Add Persistent Service IPs/Pools** to provide the required persistent IP addresses.

For more information about persistent IP addresses, see the Nexus Dashboard persistent IP addresses, on page 39 section.

b) Click **Next** to proceed.

Step 17 In the **Summary** screen, review and verify the configuration information and click **Save** to build the cluster.

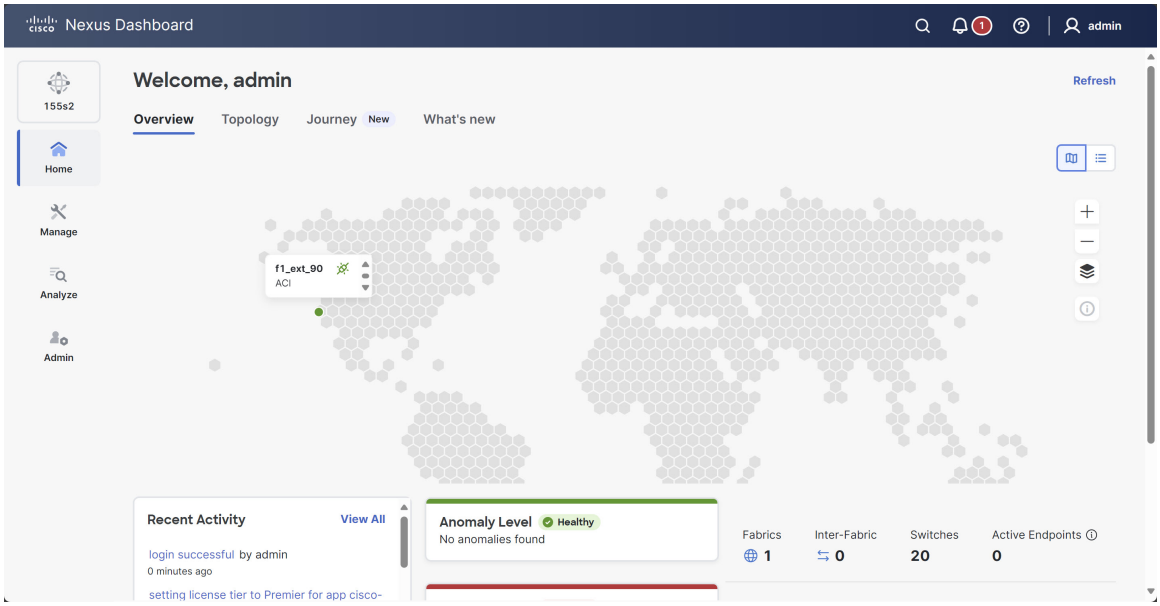
During the node bootstrap and cluster bring-up, the overall progress as well as each node's individual progress will be displayed in the UI. If you do not see the bootstrap progress advance, manually refresh the page in your browser to update the status.

It may take up to 30 minutes for the cluster to form and all the services to start. When cluster configuration is complete, the page will reload to the Nexus Dashboard GUI.

Step 18 Verify that the cluster is healthy.

After the cluster becomes available, you can access it by browsing to any one of your nodes' management IP addresses. The default password for the `admin` user is the same as the `rescue-user` password you chose for the first node. During this time, the UI will display a banner at the top stating "Service Installation is in progress, Nexus Dashboard configuration tasks are currently disabled".

After all the cluster is deployed and all services are started, you can look at the **Anomaly Level** on the **Home** > **Overview** page to ensure the cluster is healthy:



Alternatively, you can log in to any one node using SSH as the `rescue-user` using the password you entered during node deployment and using the `acs health` command to see the status:

- While the cluster is converging, you may see the following output:

```
$ acs health
k8s install is in-progress

$ acs health
k8s services not in desired state - [...]

$ acs health
k8s: Etcd cluster is not ready
```

- When the cluster is up and running, the following output will be displayed:

```
$ acs health
All components are healthy
```

Note
In some situations, you might power cycle a node (power it off and then back on) and find it stuck in this stage:

```
deploy base system services
```

This is due to an issue with `etcd` on the node after a reboot of the physical Nexus Dashboard cluster.

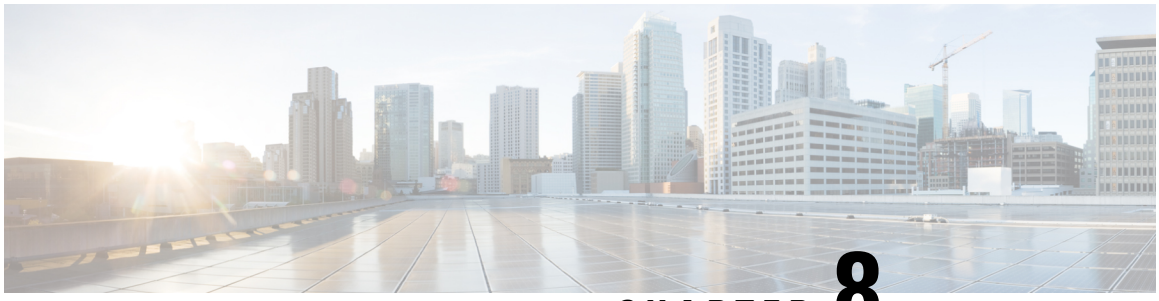
To resolve the issue, enter the `acs reboot clean` command on the affected node.

Step 19 (Optional) Connect your Cisco Nexus Dashboard cluster to Cisco Intersight for added visibility and benefits. Refer to *Working with Cisco Intersight* for detailed steps.

Step 20 After you have deployed Nexus Dashboard, see the collections page for this release for configuration information.

What to do next

The next task is to create the fabrics and fabric groups. See the *Creating Fabrics and Fabric Groups* article for this release on the Cisco Nexus Dashboard collections page.



CHAPTER 8

Deploying a Virtual Nexus Dashboard (vND) in Amazon Web Services (AWS)

- About hosting a vND on the AWS public cloud, on page 117
- Prerequisites and guidelines for deploying the vNDs in Amazon Web Services, on page 119
- Prepare Amazon Web Services for the Nexus Dashboard cluster, on page 120
- Deploy a virtual Nexus Dashboard (vND) in Amazon Web Services (AWS), on page 121

About hosting a vND on the AWS public cloud

This feature allows you to run a virtual Nexus Dashboard (vND) on the AWS public cloud. The components to this solution are:

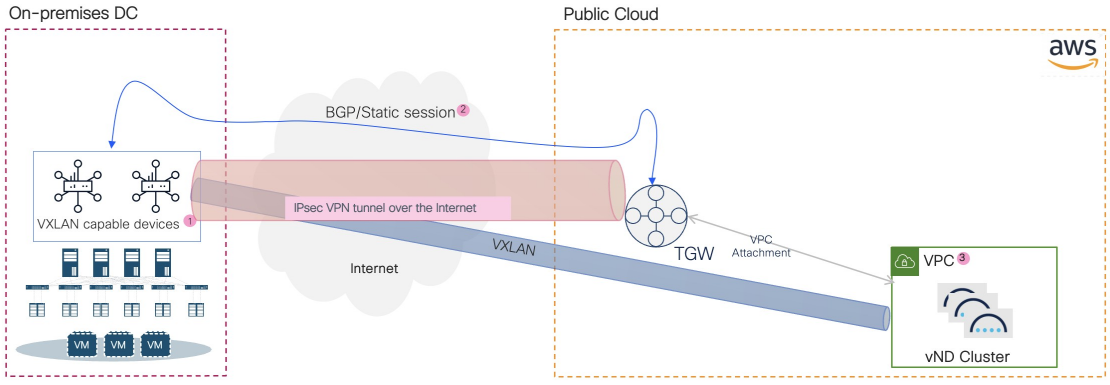
- Virtual Nexus Dashboard
- Nexus 9000 switch
- Two Catalyst 8000 series routers, or another type of device (such as the Nexus 9000 switch) that allows the Nexus Dashboard to terminate the VXLAN tunnel from the vND to the on-premises data center for persistent IP address (PIP) traffic
- AWS public cloud account

Understanding how vNDs are deployed on AWS public cloud

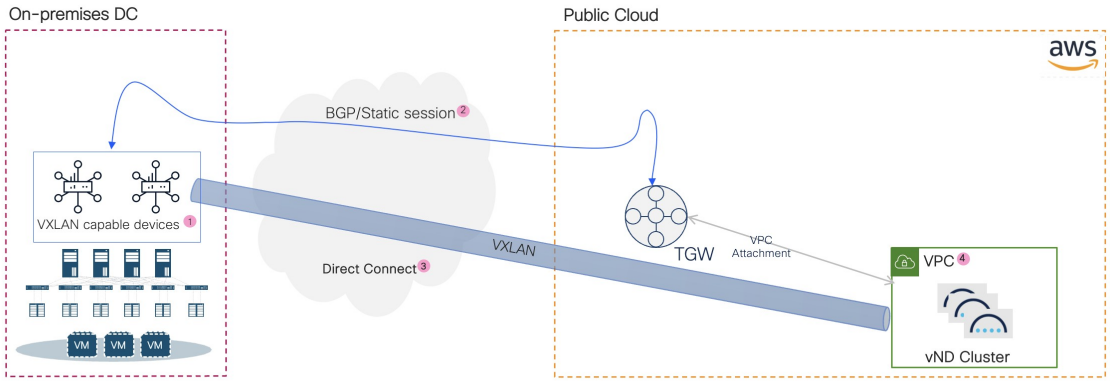
When you deploy the vNDs on the AWS public cloud, you do not have to do any manual bootstrapping; instead, the Nexus Dashboard bootstrapping performs the bootstrapping automatically for you. Once you go through the vND deployment process on AWS public cloud, a highly-available three-node cluster is created automatically for you across three availability zones (AZs) in a Virtual Private Cloud (VPC). In the Nexus Dashboard GUI, navigate to **Admin** > **System Status** > **Overview**, then view the information on the three-node cluster in the **Cluster nodes** area.

Example topology

These figures show example topologies:



1 On-premises device with VXLAN support for example, Catalyst 8000 series router, Nexus 9000
2 BGP / static session for ND data IP reachability
3 VPC in AWS terminology stands for virtual private cloud and is an equivalent of VRF



1 On-premises device with VXLAN support for example, Catalyst 8000 series router, Nexus 9000
2 BGP / static session for ND data IP reachability
3 Direct connect takes the role of a private transport for carrying data
4 VPC in AWS terminology stands for virtual private cloud and is an equivalent of VRF

Where:

- The connectivity between your on-premises data center and the AWS public cloud is achieved using either direct connect (recommended for production deployments) or an IPSec tunnel (for PoC or lab as additional overhead) between the two.
- The two on-premises routers could be one of the following:
  - If you are using direct connect, you can use two physical switches, such as the Nexus 9000 switches.
  - If you are using an IPSec tunnel, you can use a network appliance from the Cisco 8000 family, with VXLAN support because you will be terminating a VXLAN tunnel in this case.
- A transit gateway is used to create transit gateway attachments to connect to the VPC (the app VPC) that hosts the Nexus Dashboard nodes, as well as another transit gateway attachment, a VPN attachment or router, that is terminated on the transit gateway.

Note The Catalyst 8000V (C8000V) was launched as an evolution of the Cisco Cloud Services Router (CSR) 1000V. Throughout this documentation, C8000V will be used as an example of the VXLAN capable edge device. For more information, see *Release Notes for Cisco Catalyst 8000V Edge Software*.

Prerequisites and guidelines for deploying the vNDs in Amazon Web Services

Before you proceed with deploying the virtual Nexus Dashboards (vNDs) in Amazon Web Services (AWS):

Note The vND type that is supported for AWS is vND data only with 32vCPU, 128G RAM, 3TB SSD (GP3) and 10G of network throughput.

- This feature is supported on 3-node virtual clusters (data) on AWS with Nexus Dashboard as a single product (IPv4 only).
- Only NX-OS fabrics are supported with this feature, and only with these enabled features:
  - Controller
  - Telemetry, with these restrictions:
    - Only out-of-band
    - Traffic analytics, but no flow telemetry

  The Orchestration feature is not supported with this feature.
- This feature is supported on LAN fabrics only. It is not supported on IP Fabric for Media (IPFM) or SAN fabrics.

Note An AI fabric is considered a LAN fabric. Deploying this type of fabric in a vND in AWS is not restricted from a solution perspective. The basic AI fabric requirement is to not exceed latency between devices and the vND over 50ms.

- Secondary/worker nodes are not supported with this feature. Only three primary and one standby nodes are supported.
- Scale per cluster: 100 switches on a single three-node vND cluster
- You cannot change the IP address or the VNI assigned to the tunnel endpoints after you have deployed the vNDs in AWS.
- Before you can deploy your Nexus Dashboard vNDs, it is best to have your on-premises site ready, with the Catalyst 8000 series routers or a pair of Nexus 9000 switches already deployed, which allows you to provide the necessary BDI and TEP IP addresses during the Nexus Dashboard vND deployment. If

necessary, you can deploy the on-premises network appliances after you have deployed your Nexus Dashboard vNDs, but then you will have to ensure that you configure the on-premises devices with the same information that you provided during the Nexus Dashboard vND deployment. If you fail to provide the same configuration information in both places, you might have to re-install the Nexus Dashboard vNDs again.

- Verify that your on-premises VXLAN capable device is configured properly:
  - Dataplane: Ingress Replication
  - Control Plane: Flood and Learn
- Ensure that the AWS form factor supports your scale and services requirements.

  Scale and services support and co-hosting vary based on the cluster form factor. You can use the Nexus Dashboard Capacity Planning tool to verify that the cloud form factor satisfies your deployment requirements.
- Review and complete the general prerequisites described in the General prerequisites and guidelines, on page 9.
- Review and complete any additional prerequisites described in the *Release Notes* for the services you plan to deploy.
- Have appropriate access privileges for your AWS account.

  You must be able to launch multiple instances of Elastic Compute Cloud (`m5.8xlarge`) to host the Nexus Dashboard cluster.
- Ensure that the CPU family used for the Nexus Dashboard VMs supports AVX instruction set.
- Perform the Prepare Amazon Web Services for the Nexus Dashboard cluster, on page 120 procedure.

Prepare Amazon Web Services for the Nexus Dashboard cluster

Before you deploy the Nexus Dashboard vNDs in Amazon Web Services (AWS), follow these prerequisites to prepare AWS for your deployment:

- Familiarize yourself with AWS and how it works.
- (Optional) Establish a connection between AWS and your on-premises data center (ideally, a direct connection).
- Identify the region that you will use for the deployment of the Nexus Dashboard nodes.
- Have an existing VPC, or create a new VPC, that you will use for this deployment.
- Enable external access.

  This is necessary for mapping Elastic IP addresses to the vND management interfaces and for accessing the GUI and SSH externally. You may or may not need to create and attach an Internet Gateway to the VPC to enable external access, depending on the connection method that you choose:
  - **Option 1**: Connecting the management interface using the Ethernet Interface Processor (EIP), in which case you will need the Internet Gateway.
  - **Option 2**: Use a private IP address, in which case you will not need the Internet Gateway.

- Update the security group to allow access from your public IP address or range for required services, such as:
  - HTTPS (TCP port 443): For accessing the Nexus Dashboard GUI
  - SSH (TCP port 22): For secure remote login to the vND nodes

  This is necessary so that you can access the GUI and SSH into the Nexus Dashboard nodes.
- Create 6 subnets:
  - One set of subnets for management for each node (3) - minimum /28
  - One set of subnets for data for each node (3) - minimum /28

  Subnets for management and data for a specific node must be in the same availability zone.
- Ensure that you have enough AWS Elastic IP addresses available for the vND deployment.

  This installation requires 3 AWS Elastic IP addresses, 1 for each node, where each AWS Elastic IP address is used to access the management services, such as accessing the vND UI or SSH.
- Because the management subnets IP addresses will be mapped with AWS Elastic IP addresses as part of the deployment, those management subnets will need external access. Data subnets need to have reachability to the on-premises devices and on-premises Catalyst 8000 series routers (or other devices, such as Nexus 9000 switches) used for the termination of the VXLAN tunnel (used by persistent pods) from the vNDs.
- One /28 (such as 100.100.100.0/28) subnet that is not owned by AWS and comes from the on-premises data center (but is not already being used) that will be used by the PIP (persistent IP addresses), where 100.100.100.1 and 100.100.100.2 of that subnet must be the BDI IP addresses on the on-premises data center devices (Catalyst 8000 or Nexus 9000 switches) and the rest of the IP addresses are used by vND persistent pods (trap, telemetry collectors, and so on).
- On-premises devices should be able to reach these persistent IP addresses and Nexus Dashboard data IP addresses, and vice versa, for proper functioning.
- Create a security group with all the necessary IP addresses and ports so that the vND nodes can communicate with each other and form the cluster, and communicate externally and with the on-premises devices.
- Configure one EC2 key pair for deployment.

Note Complete this configuration as part of the prerequisites, even though EC2 key pair is not currently used and user/password is the only supported option at this time.

Deploy a virtual Nexus Dashboard (vND) in Amazon Web Services (AWS)

This section describes how to deploy a virtual Nexus Dashboard (vND) in Amazon Web Services (AWS).

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and guidelines for deploying the vNDs in Amazon Web Services, on page 119.

Procedure

Step 1 Subscribe to Cisco Nexus Dashboard product in AWS Marketplace.

a) Log into your AWS account and navigate to the AWS Management Console.

The Management Console is available at https://console.aws.amazon.com/.

b) Navigate to **Services** > **AWS Marketplace Subscriptions**.
c) Click **Manage subscriptions**.
d) Click **Discover products**.
e) Search for **Cisco Nexus Dashboard - Cloud** and click the result.
f) Click the **View Purchase** options and scroll down to click **Subscribe**.
g) In the product page, click **View subscription**.
h) In the **Manage subscriptions** page, locate the line for **Cisco Nexus Dashboard - Cloud**, then click **Launch** in that line.

Step 2 Select software options and region.

a) In the **Configure this software** page for **Cisco Nexus Dashboard - Cloud**, make the following choices:

- **Fulfillment option**: Leave the default **Nexus Dashboard - Cloud Deployment** choice as-is.
- **Software version**: Choose the latest 4.1.1 option available from the dropdown list.
- **Region**: Choose the appropriate region where the template will be deployed.

  This must be the same region where you created your VPC.

b) Click **Continue to Launch**.
c) In the **Launch this software** page for **Cisco Nexus Dashboard - Cloud**, locate the **Choose Action** field and choose **Launch CloudFormation** from the dropdown list, then click **Launch**.

The **Create stack** page appears.

Step 3 Complete the stack configuration.

a) Leave the options in the **Create stack** page as-is.

Note
Do not make changes in the provided template. Only by using the smart default template configuration can you ensure a successful cluster formation.

- **Prerequisite - Prepare template**: Leave `Choose an existing template` option as-is.
- **Specify Template**: Leave `Amazon S3 URL` option as-is.
- **Amazon S3 URL**: Leave pre-configured URL entry as-is.

b) Click **Next** to continue.

The **Specify stack details** page appears.

Step 4 Specify the stack details.

a) Provide the **Stack name**.

b) Review the information provided in the **Parameters** area and make changes, if necessary.

For the most part, you can leave the pre-populated fields as-is based on the configurations that are part of this vND CFT.

- In the **Nexus Dashboard Cluster Name** field, enter the cluster name for the Nexus Dashboard cluster.
- In the **Fabric Deployment Mode** field, the default **LAN** option is the only supported option for the Nexus Dashboard 4.1.1 release.
- In the **VPC identifier** field, enter the VPC identifier.

  The application VPC is automatically entered in this field. If you want to change the VPC in this field, choose another VPC under **VPC dashboard** > **Virtual private cloud** > **Your VPCs**.
- In the **Security Group Identifier** field, enter the security group identifier.

  This is a pre-created security group that must allow ingress access for ports 22 and 443.
- In the **Instance Type** field, specify the EC2 instance type for the node instances.
- In the **AMI Identifier** field, specify the AWS AMI for the Nexus Dashboard.
- In the **Password** field, enter the admin password for the Nexus Dashboard node.

  The admin password for the Nexus Dashboard node must contain at least 1 letter, number, and special character (@$!%*#?&) and must be between 8 and 64 characters in length.
- (Optional) In the **Key Pair Name** field, specify the name of an existing SSH key pair to enable SSH access to the Nexus Dashboard.

c) Enter the necessary information in the **DNS Configuration** area.

- In the **Primary DNS Server IP** field, enter the primary DNS server IP address.
- In the **Secondary DNS Server IP** field, enter the secondary DNS server IP address.
- In the **Search Domain Name** field, enter the search domain name.

d) (Optional) Enter the necessary information in the **Proxy Configuration** area.

- In the **Proxy Type** field, specify the proxy type (for example, HTTP or HTTPS).
- In the **Proxy URL** field, specify the full proxy URL, including the protocol and port (for example, `http://proxy.example.com:8080`).
- In the **Proxy Username** field, specify the proxy username, if authentication is required.
- In the **Proxy Password** field, specify the proxy password, if authentication is required.
- In the **Proxy Ignore Hosts IP** field, specify the proxy ignore hosts IP addresses.

  Only one entry is allowed in this field (for example, 192.168.10.101).

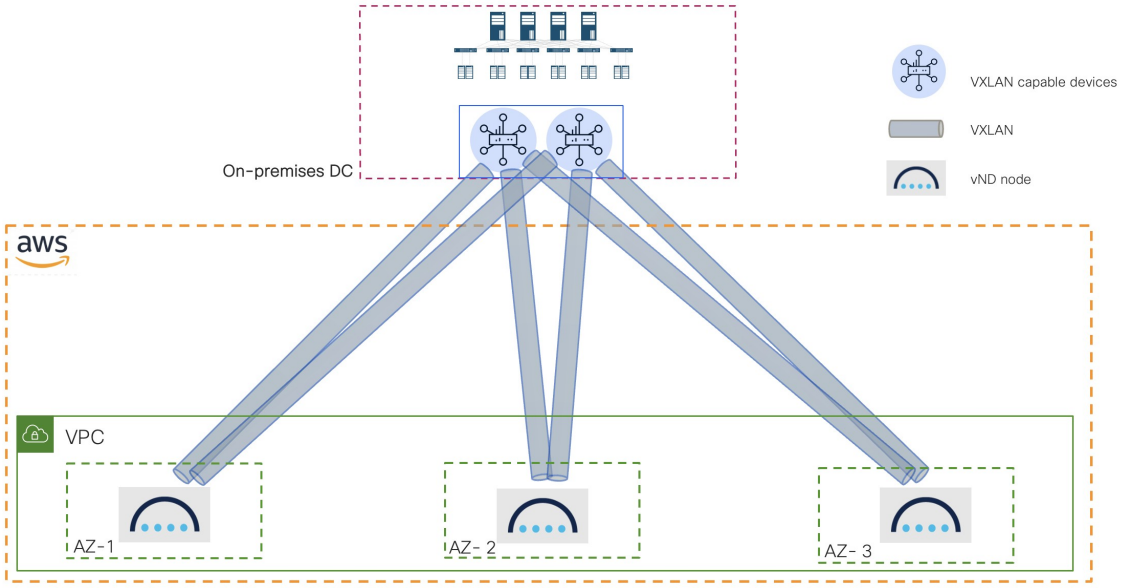
e) Enter the necessary information in the **NTP Configuration** area.

- In the **NTP Server Host** field, specify the NTP server host.
- In the **NTP Server Key Identifier** field, specify the NTP server key identifier.
- In the **NTP Server Preferred** field, choose `true` if the server is preferred.
- In the **NTP Key Identifier** field, specify the identifier for the NTP key.
- In the **NTP Key** field, specify the key for the NTP key.
- In the **NTP Key Authentication Type** field, specify the authentication type for the NTP key (for example, MDS or SHA1).
- In the **NTP Key Trusted** field, specify `true` or `false` for whether the NTP key is trusted.

f) Enter the necessary information in the **Cisco VXLAN Capable Device** area.

- In the **Device VXLAN Identifier (VNI)** field, enter a VNI value to be used for the VXLAN tunnel between the Cisco VXLAN capable device (if you are using an IPSec tunnel) or Nexus 9000 switches (if you are using direct connect) and the Nexus Dashboard nodes.

  A single VNI value will be used for all the VXLAN tunnels between the Cisco VXLAN capable devices and the Nexus Dashboard nodes (the vNDs), as shown in this figure.



- In the **Device 1 Bridge Domain IP** and **Device 2 Bridge Domain IP** fields, enter the bridge domain IP addresses for both of the Cisco VXLAN capable devices.

  The bridge domain IP addresses for the devices should come from the subnet that you provide in the **Private IP Subnet for Nexus Dashboard Pods** field. For example, if you enter `100.100.100.0/28` in the **Private IP Subnet for Nexus Dashboard Pods** field, you might enter `100.100.100.1` and `100.100.100.2` as the bridge domain IP addresses for the devices.

- In the **Device 1 Tunnel Endpoint IP** and **Device 2 Tunnel Endpoint IP** fields, enter the tunnel endpoint IP addresses (the data IP addresses) for both of the Cisco VXLAN capable devices.
- In the **Private IP Subnet for Nexus Dashboard Pods** field, enter the private IP subnet to be used by the Nexus Dashboard pods.

The IP subnet size must be a /28, such as `100.100.100.0/28`.

Note
This procedures in this section do not deploy any Cisco VXLAN capable devices; they only ensure Nexus Dashboard has all the variables required to build connections with the edge devices.

g) In the **Nexus Dashboard Node 1 Configuration**, **Nexus Dashboard Node 2 Configuration**, and **Nexus Dashboard Node 3 Configuration** areas, enter the necessary information for each of the vND nodes in the cluster:

- **ND Node *x* Hostname**: Enter the hostname for each Nexus Dashboard node.
- **ND Node *x* Management Subnet**: Enter the first management subnet each Nexus Dashboard node.
- **ND Node *x* Static Management IP**: Enter a static management IP address from the management subnet that you entered above for each Nexus Dashboard node.

  Verify that the IP address that you enter in this field is not being used already.
- **ND Node *x* Management Subnet Netmask**: Enter the first management subnet netmask for each Nexus Dashboard node in the CIDR format (16-28).
- **ND Node *x* Management Subnet Gateway**: Enter the first management default gateway on the management subnet that you entered above for each Nexus Dashboard node.

  This is typically the first address on the subnet.
- **ND Node *x* Data Subnet**: Enter the first data subnet each Nexus Dashboard node.
- **ND Node *x* Static Data IP**: Enter a static data IP address from the management subnet that you entered above for each Nexus Dashboard node.

  Verify that the IP address that you enter in this field is not being used already.
- **ND Node *x* Data Subnet Netmask**: Enter the first data subnet netmask for each Nexus Dashboard node in the CIDR format (16-28).
- **ND Node *x* Data Subnet Gateway**: Enter the first data default gateway on the management subnet that you entered above for each Nexus Dashboard node.

  This is typically the first address on the subnet.

h) In the **Kubernetes Network Configuration (Optional)** area, enter the configuration information, if necessary:

- In the **Kubernetes Service Network** field, specify the network address for the Kubernetes service network.

  The CIDR range is fixed to /16.
- In the **Kubernetes App Network** field, specify the network address for the Kubernetes app network.

  The CIDR range is fixed to /16.

i) Click **Next** to continue.

Step 5 In the **Configure stack options** page, review and modify the information provided in this page, if necessary.

a) Under **Stack failure options**, we recommend that you change the choice under **Behavior on provisioning failure** to **Preserve successfully provisioned resources**.

b) Click **Next** when you have finished reviewing or modifying the information in the **Configure stack options** page.

Step 6 In the **Review and create** page, verify the template configuration information, then click **Submit**.

Step 7 Wait for the deployment to complete, then start the VMs.

You can view the status of the instance deployment in the **CloudFormation** > **Stacks** page, for example `CREATE_IN_PROGRESS`. You can click the refresh button in the top right corner of the page to update the status.

When the status for your stack changes to `CREATE_COMPLETE`, you can proceed to the next step.

Step 8 In your stack under **CloudFormation** > **Stacks**, click the **Outputs** tab to view the public IP addresses for the three vNDs in the cluster.

Note
The CloudFormation template takes care of the connectivity within the cluster. Nodes should automatically form a cluster, if all the variables are filled in correctly.

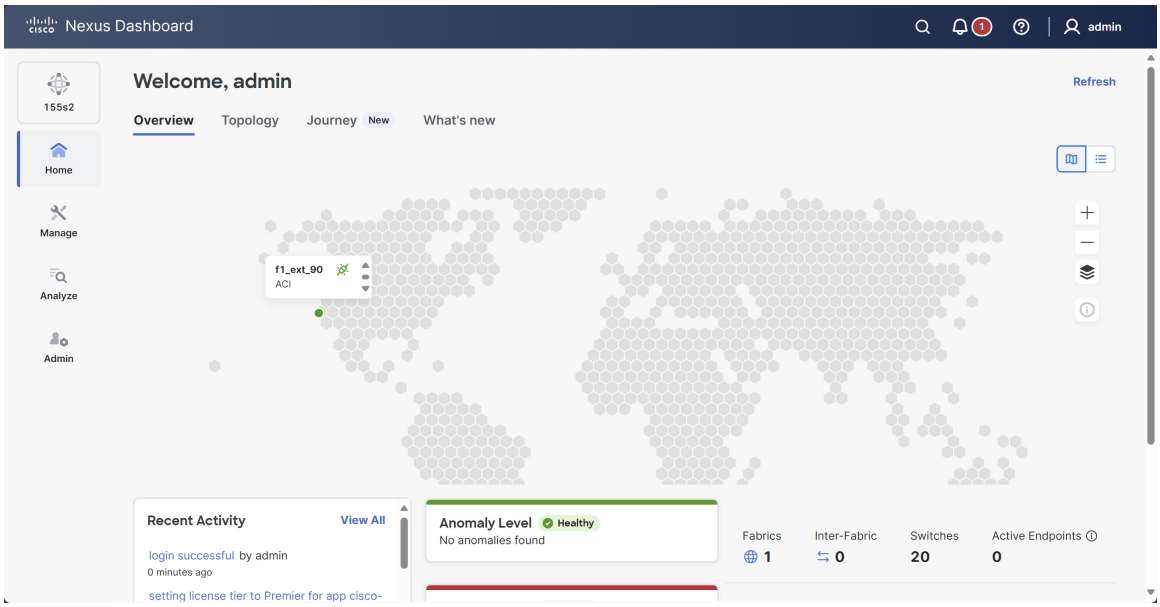
Step 9 Log into the Nexus Dashboard GUI using one of the public IP addresses listed in the previous step.

Note
You might have to wait for around 40 minutes after you have started the VMs before you can log into the Nexus Dashboard GUI using one of the public IP addresses.

Step 10 Verify that the cluster is healthy.

After the cluster becomes available, you can access it by browsing to any one of your nodes' management IP addresses. The default password for the `admin` user is the same as the `rescue-user` password you chose for the first node. During this time, the UI will display a banner at the top stating "Service Installation is in progress, Nexus Dashboard configuration tasks are currently disabled".

After all the cluster is deployed and all services are started, you can look at the **Anomaly Level** on the **Home** > **Overview** page to ensure the cluster is healthy:



Alternatively, you can log in to any one node using SSH as the `rescue-user` using the password you entered during node deployment and using the `acs health` command to see the status:

- While the cluster is converging, you may see the following output:

```
$ acs health
k8s install is in-progress

$ acs health
k8s services not in desired state - [...]

$ acs health
k8s: Etcd cluster is not ready
```

- When the cluster is up and running, the following output will be displayed:

```
$ acs health
All components are healthy
```

Note
In some situations, you might power cycle a node (power it off and then back on) and find it stuck in this stage:

```
deploy base system services
```

This is due to an issue with `etcd` on the node after a reboot of the physical Nexus Dashboard cluster.

To resolve the issue, enter the `acs reboot clean` command on the affected node.

Step 11 (Optional) Connect your Cisco Nexus Dashboard cluster to Cisco Intersight for added visibility and benefits. Refer to *Working with Cisco Intersight* for detailed steps.

Step 12 After you have deployed Nexus Dashboard, see the collections page for this release for configuration information.

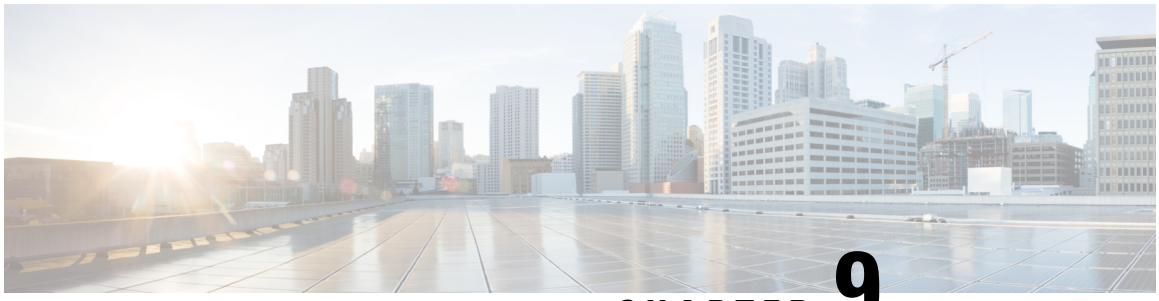
What to do next

The next task is to create the fabrics and fabric groups. See the *Creating Fabrics and Fabric Groups* article for this release on the Cisco Nexus Dashboard collections page.

PART III

Upgrading or Migrating to This Release

- Upgrading an Existing Nexus Dashboard Cluster to This Release, on page 131
- Migrating From DCNM to ND, on page 145



CHAPTER 9

Upgrading an Existing Nexus Dashboard Cluster to This Release

- Prerequisites and guidelines for upgrading an existing Nexus Dashboard cluster, on page 131
- Supported upgrade paths, on page 135
- Upgrade Nexus Dashboard, on page 137
- Post-upgrade information and tasks, on page 139
- Troubleshooting upgrades, on page 143

Prerequisites and guidelines for upgrading an existing Nexus Dashboard cluster

Before you upgrade your existing Nexus Dashboard cluster:

- Ensure that you have read the target release's *Release Notes* for any changes in behavior, guidelines, and issues that may affect your upgrade.
- Before upgrading to Nexus Dashboard release 4.1.1:
  - Make sure your NTP and DNS services are configured. At least one NTP and DNS are required for the system to upgrade successfully.
  - Verify that the management network and data network are in different subnets. The upgrade will fail if the management network and data network are not in different subnets.
  - We highly recommend that you use the Nexus Dashboard Preupgrade Validation script before performing any Nexus Dashboard upgrades. The Nexus Dashboard Preupgrade Validation script is a Python script that performs various checks for known issues that have been identified to affect the success of a Nexus Dashboard upgrade. The script is continuously updated and maintained in an effort to mitigate any new upgrade-related issues that are detected in the field.

    For detailed information about the script functionality and how to use it in your environment, visit https://github.com/datacenter/Nexus-Dashboard.
- Verify that the `acs health` is healthy.
  1. Access the Nexus Dashboard using `ssh -l rescue-user {management-ip-of-nd}`.
  2. Issue the `acs health` command.

The output from the `acs health` command should show that all components are healthy:

```
rescue-user@node1:~$ acs health
======
Status
======
All components are healthy
```

- Ensure that you perform a backup of your Nexus Dashboard cluster before upgrading and you store the backup file in a safe place. To perform a backup, refer to *Unified Backup and Restore for Nexus Dashboard and Services*. Note that you will not be able to restore this backup directly to a Nexus Dashboard cluster running the 4.1.1 release.
- An upgrade will not proceed if the most recent backup had a failure. Make sure you have a successful backup before proceeding with the upgrade. If you are unable to perform a successful backup and cannot upgrade, contact Cisco Technical Assistance Center (TAC) for support.
- Upgrading an NDFC vND cluster (single-node or multi-node) with an app-large profile (1.5TB disk) is not supported. Restore the Nexus Dashboard cluster from a backup onto a regular app node (16 vCPUs/64GB RAM/500GB disk) or data node (32 vCPUs/128GB RAM/3TB disk) and upgrade the cluster again.
- If you have either NDI or NDFC, with NDI performing telemetry for remotely-created NDFC clusters, or if you have multi-cluster connectivity with multiple ND clusters, all the clusters must be upgraded to Nexus Dashboard 4.1.1. Having a mix of Nexus Dashboard release 3.2x and 4.1.1 clusters using multi-cluster connectivity is not supported.
- If you are upgrading a physical Nexus Dashboard cluster, ensure that the nodes have the minimum supported CIMC version for the target Nexus Dashboard release.

  Supported CIMC versions are listed in the *Nexus Dashboard Release Notes* for the target release.

  The CIMC upgrade is described in detail in the "Troubleshooting" article in the Nexus Dashboard *documentation library*.
- If you are upgrading a virtual Nexus Dashboard cluster, Nexus Dashboard will enforce a check of the HDD latency to verify that it is <30ms. If the HDD has a higher latency, the upgrade will fail.
- If you are upgrading a virtual Nexus Dashboard cluster deployed in VMware ESX, ensure that the ESX version is still supported by the target release.

  This release supports VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3, 8.0, 8.0.2, 8.0.3.

Note If you need to upgrade the ESX server, you must do that before upgrading your Nexus Dashboard. ESX upgrades are outside the scope of this document, but in short:

1. Upgrade one of the ESX hosts as you typically would with your existing Nexus Dashboard node VM running.
2. After the host is upgraded, ensure that the Nexus Dashboard cluster is still operational and healthy.
3. Repeat the upgrade on the other ESX hosts one at a time.
4. After all ESX hosts are upgraded and the existing Nexus Dashboard cluster is healthy, proceed with upgrading your Nexus Dashboard to the target release as described in this document.

- Ensure that your current Nexus Dashboard cluster is healthy.

  You can check the system status on the **Overview** page of the Nexus Dashboard's **Admin Console** or by logging in to one of the nodes as `rescue-user` and ensuring that the `acs health` command returns `All components are healthy`.

- Nexus Dashboard does not support platform downgrades.

  If you want to downgrade to an earlier release, you will need to deploy a new cluster.

- If you have a user who only has the `Dashboard User` (app-user) user role in Nexus Dashboard release 3.2.1, after the upgrade to Nexus Dashboard release 4.1.1, delete the user with the `Dashboard User` user role or use the `Observer` role instead for that user in Nexus Dashboard release 4.1.1.

- The number of persistent IP addresses and how they are mapped out has changed from previous releases to Nexus Dashboard release 4.1.1. See Nexus Dashboard persistent IP addresses, on page 39 to understand the number of persistent IP addresses that were needed in previous releases, and how you will have to make certain updates in the number of persistent IP addresses that you will need before you can upgrade to Nexus Dashboard release 4.1.1.

- If you have a Nexus Dashboard (ND) in any persona with any services, specifically Nexus Dashboard Fabric Controller (NDFC) and Nexus Dashboard Insights (NDI), and you have upgraded from previous releases (such as ND 2.2.x and below) to ND 3.2.x, be aware of the following important information regarding Elasticsearch (ES) indices size:

  If the cluster was deployed on ND 2.2.x or earlier and was upgraded since then, the upgrade from ND 3.2.x to ND 4.1.1 may be indexing the time series database. The process will prompt you to contact Cisco Technical Assistance Center (TAC) if the sizes exceed the sizes of the ability to reindex on this cluster. If the process fails to reindex, you can use the `acs recover` command that's provided in the UI to proceed with the upgrade after the failure.

- If you had multi-cluster connectivity configured and you had NDFC and NDI co-located in your Nexus Dashboard release 3.2.x system, where:
  - NDFC was running on one cluster, and
  - NDI was running on another cluster

Then we mandate that you disconnect the clusters and delete the federation before you begin the upgrade process to Nexus Dashboard release 4.1.1. See the sections "Disconnecting Clusters" and "Deleting the Federation" in the *Nexus Dashboard Infrastructure Management* for those procedures. After you have completed the upgrade, you will re-enable multi-cluster connectivity as part of the post-upgrade tasks.

- If you have Nexus Dashboard Orchestrator as part of your pre-ND release 4.1.1 cluster with different data subnets, before upgrading to Nexus Dashboard release 4.1.1, you must make the following configurations:
  - Add BGP configurations on all the nodes
  - Add persistent IP addresses

  The validation of the image during the upgrade will fail if you do not have these items configured before upgrading.

Auto reconcile configuration drifts on upgrade

When upgrading to ND release 4.1.1 from any pre-4.2.(1) NDO release, you must perform a multi-step upgrade:

1. First upgrade the pre-4.2(1) NDO release to ND 3.0.1i, then to ND release 3.2.x, as described in the "Supported Upgrade Paths" section in *Cisco Nexus Dashboard and Services Deployment and Upgrade Guide, Release 3.2.x*.
2. Then upgrade from ND release 3.2.x to ND release 4.1.1, as described in this chapter.

When upgrading a pre-4.2(1) NDO release to ND release 3.2.x, you may observe some configuration drifts in application templates. These drifts occur because NDO release 4.2(1) and later support managing new application template object properties that were not managed in earlier versions. For a list of new properties managed by NDO 4.2(1), refer to the Nexus Dashboard Orchestrator 4.2(1) release notes.

ND release 4.1.1 supports automatic reconciliation of configuration drifts as part of the upgrade process. Nexus Dashboard will check whether the templates are in sync with the fabrics and, if necessary, will import fabric values into Nexus Dashboard to automatically resolve the drifts.

When following the multi-step upgrade path from a pre-4.2(1) NDO version, we recommend that you ignore any drifts detected in ND release 3.2.x and continue the upgrade to ND release 4.1.1.

Any drifts remaining after upgrading to ND release 4.1.1 will need to be resolved manually. For example, a drift that cannot be auto-resolved occurs when a configured object is part of a stretched template across multiple fabrics, and the template-level property has different values configured on different fabrics.

(Optional) Convert a 6-node pND cluster to a 3-node pND cluster

If you want to convert a 6-node pND cluster to a 3-node pND as part of the upgrade process (for example, if you have a 6-node pND **controller** deployment in Nexus Dashboard release 3.2.2, which isn't supported in Nexus Dashboard release 4.1.1), use these procedures to make this conversion in Nexus Dashboard release 3.2.2, before upgrading to Nexus Dashboard release 4.1.1.

Note that a 6-node pND **telemetry**-only deployment is supported in Nexus Dashboard release 4.1.1 so this optional procedure is not needed in this case.

1. Perform a backup of the 6-node pND cluster in Nexus Dashboard release 3.2.x.

   See *Unified Backup and Restore for Nexus Dashboard and Services* for more information.
2. Ensure that the primary nodes and the cluster are healthy, then delete the secondary nodes one by one.

a. In your Nexus Dashboard running on release 3.2.x, navigate to **Manage** > **Nodes**.

b. Select the secondary node that you want to delete.

c. From the **Actions** menu, choose **Delete** to delete the node.

d. Navigate to **Overview** > **Platform View** and wait until the cluster health status shows **GREEN** after each secondary node deletion.

Note Kafka may take up to 30 minutes to stabilize after deleting a node.

e. Once you see the cluster health status as **GREEN** after you deleted a secondary node, proceed to delete the next secondary node.

   Continue the process of deleting each secondary node one-by-one, waiting for the cluster status to turn **GREEN** before proceeding to the deletion of the next secondary node.

3. When you have deleted all the secondary nodes, verify that the cluster is healthy, then perform a new backup in Nexus Dashboard release 3.2.x.

   See *Unified Backup and Restore for Nexus Dashboard and Services* for more information.

4. Upgrade the cluster from Nexus Dashboard release 3.2.x to release 4.1.1 using the procedures in this chapter.

Supported upgrade paths

As described in Nexus Dashboard deployment overview, on page 5, in earlier releases, Nexus Dashboard shipped with only the platform software and no services included, which you would then download, install, and enable separately after the initial platform deployment. In addition, Nexus Dashboard release 3.1(1) introduced a tighter coupling between the Nexus Dashboard and individual services with only a single version of each service compatible with each version of the platform. As a result, as long as you were on the minimum required version of the Nexus Dashboard software, you could upgrade both the platform and all currently enabled services directly to Nexus Dashboard release 3.1x and 3.2x.

Now, the platform and the individual services have been unified into a single product, which means that you no longer deploy, configure, or upgrade the services separately.

The following table provides a few example scenarios for specific deployment combinations:

Table 15:

Current Nexus Dashboard Release	Compatible Services (depending on form factor and cluster size, you may have one or more of these services currently enabled)	Upgrade Workflow
3.2(2)	Fabric Controller: 12.2(3) Orchestrator: 4.4(2) Insights: 6.5(2)	Upgrade directly to release 4.1(1) as described in the following section. All services are unified under a single Nexus Dashboard product in release 4.1(1).
3.2(1)	Fabric Controller: 12.2(2) Orchestrator: 4.4(1) Insights: 6.5(1)	Upgrade directly to release 4.1(1) as described in the following section. All services are unified under a single Nexus Dashboard product in release 4.1(1).
3.1(1)	Fabric Controller: 12.2(1) Orchestrator: 4.3(x) Insights: 6.4(1)	1. Upgrade the Nexus Dashboard platform to release 3.2(x) as described in *Nexus Dashboard Deployment Guide, Release 3.2.x* All services will be automatically upgraded along with the platform. 2. Upgrade from release 3.2(x) to release 4.1(1) . All services are unified under a single Nexus Dashboard product in release 4.1(1).
3.0(1)	Fabric Controller: 12.1(3) Orchestrator: 4.2(x) Insights: 6.3(1)	1. Upgrade the Nexus Dashboard platform to release 3.2(x) as described in *Nexus Dashboard Deployment Guide, Release 3.2.x* All services will be automatically upgraded along with the platform. 2. Upgrade from release 3.2(x) to release 4.1(1) . All services are unified under a single Nexus Dashboard product in release 4.1(1).
2.3(2) and earlier	Fabric Controller: 12.1(2) or earlier Orchestrator: 4.1(x) or earlier Insights: 6.2(x) or earlier	1. Upgrade the Nexus Dashboard platform to release 3.1(1) as described in *Nexus Dashboard Deployment Guide, Release 3.1.x* All services will be automatically upgraded along with the platform. 2. Upgrade from release 3.1(1) to release 3.2(x) as described in *Nexus Dashboard Deployment Guide, Release 3.2.x*. All services will be automatically upgraded along with the platform. 3. Upgrade from release 3.2(x) to release 4.1(1) . All services are unified under a single Nexus Dashboard product in release 4.1(1).

Upgrade Nexus Dashboard

This section describes how to upgrade an existing Nexus Dashboard cluster.

As described in Supported upgrade paths, on page 135, you must be on Nexus Dashboard release 3.2(x) to upgrade directly to Nexus Dashboard release 4.1(1). Note these important points on these releases:

- **Nexus Dashboard release 3.2(x)**: As described in Nexus Dashboard deployment overview, on page 5, for these Nexus Dashboard releases, Nexus Dashboard was available as one product, and individual services (such as Nexus Dashboard Insights, Orchestrator, and Fabric Controller) were available as individual products, separate from Nexus Dashboard.
- **Nexus Dashboard release 4.1(1)**: This is the first Nexus Dashboard release where Nexus Dashboard and the individual services listed above are packaged together as a single, unified product.

This means that your upgrade process will go through these phases:

1. You will begin the upgrade process in Nexus Dashboard release 3.2(x), where Nexus Dashboard and the individual services are separate products.
2. You will then upgrade to Nexus Dashboard 4.1(1), where you will end the upgrade process with Nexus Dashboard and the individual services packaged together as a single, unified product.

Before you begin

Ensure that you have completed the prerequisites described in Prerequisites and guidelines for upgrading an existing Nexus Dashboard cluster, on page 131

Procedure

Step 1 In your Nexus Dashboard release 3.2(x) system, download the Nexus Dashboard 4.1(1) image.

a) Browse to the Software Download page.

https://software.cisco.com/download/home/286327743/type/286328258

b) Choose the Nexus Dashboard 4.1(1) release to download.

c) Download the Nexus Dashboard image for the 4.1(1) release.

Note

- The upgrade process is the same for all Nexus Dashboard form factors and uses the Nexus Dashboard ISO image (`nd-dk9.<version>.iso`). In other words, even if you used the virtual form factors (such as the ESX `.ova`) or a cloud provider's marketplace for initial cluster deployment, you must still use the `.iso` image for upgrades.
- If the image fails to download completely, verify the network connectivity between the Nexus Dashboard and the image server. Check the proxy configuration under **Admin** > **System Settings** > **General** > **Proxy configuration**.

d) (Optional) Host the image on a web server in your environment.

Note

We recommend hosting the image on a server in your environment. When you upload the image to your Nexus Dashboard cluster, you will have an option to provide a direct URL to the image, which can significantly speed up the process.

Step 2 Log in to your current Nexus Dashboard's **Admin Console** as an `Administrator` user.

Step 3 Delete any older, non-active upgrade images from your cluster.

If this is the first time you're upgrading your cluster, you can skip this step.

a) Navigate to **Manage** > **Software Management**.
b) Click the trash icon on an upgrade image's tile to delete any older, non-active upgrade **Images**.
c) Repeat this step for all older, non-active upgrade images.

Step 4 Upload the new image to the cluster.

a) Navigate to **Manage** > **Software Management**.
b) Click **Add Image**.
c) In the **Add Software Image** window, select whether the image is **Remote** on a web server or **Local** on your machine.

In both cases, the image will be a file ending with `.iso`.

- **Remote**: Provide the **URL** to the image you downloaded in the first step.
- **Local**: Click **Choose file** and navigate to the local folder where you downloaded the image.

d) Click **Add** to add the image.

Nexus Dashboard then downloads the upgrade image and starts processing the image, and goes through a number of preparation and validation stages to ensure successful upgrade. This may take several minutes to complete.

Note
See Troubleshooting upgrades, on page 143 for more information on the validation checks that occur during this point of the upgrade and how to deal with upgrade issues that might arise.

e) After the validation is complete, then the **Install** button appears in the card in the **Software Management** page. Click **Install** to install the software and go through the upgrade process.

The installation progress window is displayed. You can navigate away from this screen while the update is in progress.

This step may take up to 60 minutes or more, depending on the number of nodes in the cluster, during which the nodes will reboot and the GUI will not be accessible. Nexus Dashboard goes through several stages:

- Install Release Firmware
- Disable Services
- Shutdown Infrastructure services
- Update Platform Services
- Enable Infrastructure Services
- Enable Services

You can click on the **Details** link to see the progress and the various stages of the upgrade.

Note

If you see any issues during the upgrade process, such as a possible indexing issue, refer to Prerequisites and guidelines for upgrading an existing Nexus Dashboard cluster, on page 131 for more information and possible workarounds.

After the process above is complete, you should be upgraded to Nexus Dashboard 4.1(1), where Nexus Dashboard and the individual services are packaged together as a single, unified product.

Note
Depending on the cluster format and the number of cluster nodes that you have deployed, certain features (such as controller, orchestrator, or telemetry) might not be available. Review the information in the Nexus Dashboard Capacity Planning tool to verify what features would be available for your cluster installation.

Step 5 After the node upgrade tasks are completed, verify that the nodes are healthy and you can log into the UI.

Once the upgrade process completes, you can view the Nexus Dashboard UI as you typically would.

You can check the **Overview** page for overall system health and the **Admin** > **System Software** page to see the current `Running` version.

What to do next

Go to Post-upgrade information and tasks, on page 139 to perform the necessary post-upgrade tasks.

Post-upgrade information and tasks

This section provides information about changes and tasks that you must complete after upgrading from Nexus Dashboard release 3.2.x to Nexus Dashboard 4.1.1.

- Perform multi-cluster connectivity post-upgrade tasks, on page 139
- Re-upload switch firmware images, on page 140
- Address Anomalies issues, on page 140
- Set device credentials, on page 140
- Migrate older cluster types to new 3 node virtual cluster (data) cluster type, on page 141
- Redeploy the telemetry configuration, on page 141
- Review changes in SNMP server users, on page 143
- View historical Performance Manager (PM) data, on page 143

Perform multi-cluster connectivity post-upgrade tasks

If you had any of these configurations in pre-4.1.1. Nexus Dashboard:

- If you had Nexus Dashboard Insights onboarding remotely-created NDFC fabrics
- If you were using One Manage to manage and monitor multiple NDFC or NDI clusters
- If you had multi-cluster fabric groups.with multiple NDFC clusters

If these clusters were already connected in the previous release using multi-cluster connectivity, then, on the primary cluster, you will have to re-register all the clusters that you upgraded to Nexus Dashboard release 4.1.1.

In addition, if you had NDI and NDO integrations in the previous release, this is not supported in Nexus Dashboard release 4.1.1, and in order to leverage the NDO integration, you will have to federate NDI and NDO clusters in Nexus Dashboard release 4.1.1.

If you had multi-cluster connectivity configured in your Nexus Dashboard release 3.2.x system, after you have completed the upgrade, you will need to re-enable multi-cluster connectivity. This task is applicable only when you have NX-OS fabrics in a co-location environment. See *Connecting Clusters* for more information.

Re-upload switch firmware images

Switch firmware images that were uploaded to Nexus Dashboard in release 3.2.x will not be carried over when you upgrade to Nexus Dashboard 4.1.1. After upgrading to Nexus Dashboard 4.1.1, re-upload those switch firmware images:

1. Navigate to **Manage** > **Fabric Software** > **NX-OS/IOS-XE** > **Images**.
2. From the **Actions** drop-down list, select **Upload** and re-upload the necessary switch firmware images.

See Managing Your Fabric Software for more information.

Address Anomalies issues

After you have completed the upgrade, check the **Anomalies** area for any issues and check for requests to complete the **Recalculate and Deploy** in some NX-OS fabrics..

Set device credentials

If you had co-hosted NX-OS fabrics configured in the Nexus Dashboard release 3.2.x system, follow these procedures to make sure the appropriate device credentials are configured after you've upgraded to Nexus Dashboard release 4.1.1.

1. In your upgraded Nexus Dashboard 4.1.1 system, navigate to **Manage** > **Device Credentials**.
2. Review the information displayed in the **Device Credentials** area.

   You should see **Not Set** displayed in red text in the **Device Credentials** area.
3. In the **Device Credentials** area, click **Set**.
4. In the **Set Default Credentials** page, enter the necessary information.
   - Username, Password, and Confirm password: Enter the necessary username and password information.
   - Robot: Choose the **Robot** checkbox to set the robot credentials, if necessary.

   Then click **Save**.

   You are returned to the **Set Default Credentials** page, and the text **Default Set** is now displayed in blue.

Migrate older cluster types to new 3 node virtual cluster (data) cluster type

The pre-4.1.1 cluster type `App node with 1.5TB disk` is not supported in Nexus Dashboard release 4.1.1; after upgrading to Nexus Dashboard release 4.1.1, it will show up as `SE-VIRTUAL-APP-LARGE`.

In addition, these pre-4.1.1 cluster types are not supported as greenfield deployments in Nexus Dashboard release 4.1.1 but are supported when upgrading to release 4.1.1:

- 3-node virtual cluster (app node with 1.5TB storage)
- 5-node virtual cluster (app 500G or 1.5TB storage)

If you want to migrate from those older cluster types to the new cluster type `3 node virtual cluster (data)`, you can migrate to the new cluster type using these procedures:

1. Upgrade to Nexus Dashboard release 4.1.1, keeping the older cluster type as-is, using the procedures provided in this chapter.
2. After you have upgraded to Nexus Dashboard release 4.1.1, perform a backup of your older cluster type.

   See *Backing Up and Restoring Your Nexus Dashboard* for more information.

   - You can use either a **Config-only** or **Full** backup option when backing up the older cluster type.
   - Verify that you have successfully retrieved the backup from the older cluster before proceeding.
3. Shut down the cluster with the older cluster type.
4. Perform a greenfield deployment of the new cluster type `3 node virtual cluster (data).`
   - Reuse the name of the older cluster for the new cluster.
   - You can deploy a virtual data cluster or a physical cluster.
   - You can reuse the IP addresses from the older cluster type, or you can use new IP addresses in the new cluster and restore with a check in the **Ignore External Service IP Configuration** check box, as described in *Backing Up and Restoring Your Nexus Dashboard*.
5. Restore the backup of the older `3 node virtual cluster (app)` or `5 node virtual cluster (app)` to the newer `3 node virtual cluster (data).`

   See *Backing Up and Restoring Your Nexus Dashboard* for more information.

Redeploy the telemetry configuration

After upgrading to Nexus Dashboard release 4.1.1, the persistent IP addresses for handling software telemetry streaming from the NX-OS fabrics would have changed. To resume telemetry operations after the upgrade to Nexus Dashboard 4.1.1, you must redeploy the telemetry configuration.

1. Navigate to the **System Status** page.

   Admin > **System Status**
2. Click **Telemetry**, then click the **Fabrics** tab in the **Telemetry status** area.
3. Review the information displayed in the **Fabrics** table.

For NX-OS fabrics, you will notice that one or more fabrics listed in the **Fabrics** table will show a status of **Pending updates** in the **Telemetry config status** column, even though those same fabrics had a status of **OK** prior to the upgrade.

In this state, telemetry streaming will not be functional, and the status of individual features (such as software telemetry, flow collection, and switch status) are not valid and should be ignored.

Note Some fabrics in the **Fabrics** table might show a status of **OK** in the **Telemetry config status** column, while other fabrics might show a status of **Pending updates**. If you were to click the **Switches** tab in the **Telemetry status** area, you might see switches with incorrect green **OK** or **Success** status entries in the telemetry columns, even though those switches are associated with the fabrics that show a status of **Pending updates** in the **Fabrics** table. This is incorrect status information displayed at the switch level for those fabrics and should be ignored.

4. With the **Fabrics** tab selected in the **Telemetry status** area, click **Redeploy telemetry**.

   Click **Confirm** in the confirmation page.

   After you click **Confirm**, the status of the individual features will change to **Enable in Progress**, and the cumulative **Telemetry Config Status** will update to **In Progress**.

5. After you click **Confirm**, you are returned to the **Fabrics** tab in the **Telemetry** page under **System Status**. Click **Refresh** in the upper right corner of the page.

   The telemetry status might be shown incorrectly immediately after you click **Confirm** in the confirmation page, but will show the correct telemetry status after you click **Refresh**.

6. Review the information displayed in the **Fabrics** table again.

   After clicking **Refresh**, you should see that the status change in these areas:

   - The status of the individual features will change to **Enable in Progress**, and
   - The status for the fabric in the **Telemetry config status** column will change from **Pending updates** to **In Progress**. After several minutes, the status for the fabric will change to **OK** in the **Telemetry config status** column, either automatically or after you click **Refresh** again.

After the operation completes, the individual feature statuses will be:

- `Enabled` if the configuration push is successful for all switches,
- `Enable Fail` if it fails for any switch, or
- `Enable Pending` if change control mode is enabled. In that case, apply the change control ticket explicitly through **Manage** > **Change control**. See *Using Change Control and Rollback in Your Nexus Dashboard* for more information.

The cumulative **Telemetry Configuration Status** will then display as:

- `OK` if the configuration is successful for all switches,
- `Not OK` if it fails or is pending in change control mode for all switches, or
- `Partial OK` if it succeeds for some switches and fails or is pending in change control mode for others.

Review changes in SNMP server users

In releases prior to Nexus Dashboard release 4.1.1, SNMP server users that were configured on managed NX-OS switches without passwords as part of the intent, such as the example shown below:

```
snmp-server user Demo_CMDv5 vdc-operator
snmp-server user DemoOps_admin vdc-operator
snmp-server user DemoOps_admin network-admin
```

were not shown in the diffs during **Recalculate and Deploy** operations. These often went unnoticed, especially in environments where the switches relied on remote authentication methods such as TACACS+.

Once you upgrade to Nexus Dashboard release 4.1.1, these differences are now correctly detected and displayed in the GUI as expected diffs. After the upgrade to release 4.1.1, you must now either:

- Push these configurations to bring the switches into sync, or
- Remove these SNMP user entries from the intent if they are no longer needed.

View historical Performance Manager (PM) data

After you upgrade Nexus Dashboard from release 3.2.x to release 4.1.1, if you enable Telemetry on the fabrics, the historical Performance Manager (PM) data will not be displayed. Instead, the system will start collecting PM data fresh from that point forward.

To view the historical PM data, disable Telemetry on the affected fabrics. The older PM data will now re-appear.

Troubleshooting upgrades

After all the nodes restart during new image activation stage described in the previous section, you may log in to the GUI to check the status of the upgrade workflows. Initially, you can see the bootstrap process similar to the initial cluster deployment and once the nodes come up, you can see additional information about service activation in the GUI's **Overview** page.

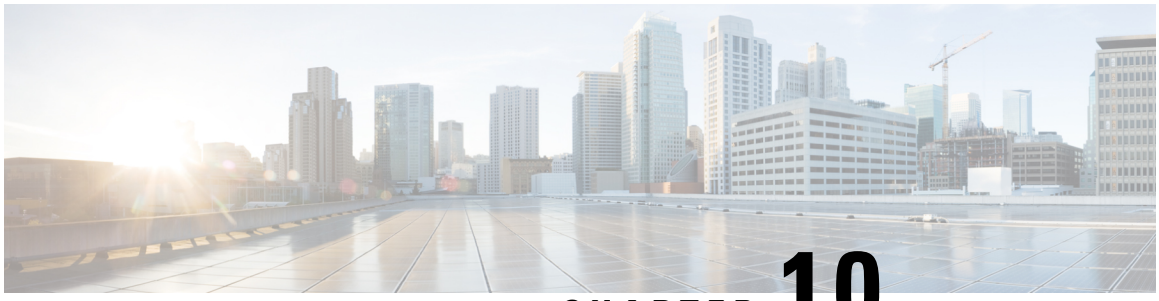
In case the upgrade fails for any reason, the GUI will display the error and additional workaround steps. For example, you might then see an error message, along with the remedy, similar to this:

```
Failed to activate

Upgrade failed while shutting down the cluster: Operation Timedout, last status: Operation
 Timedout


Please login to one of the primary nodes as 'rescue-user' and follow the steps provided by
 the upgrade recovery
helper by invoking following command: 'acs upgrade recover Cluster Shutdown'. If the issue
 persists, please contact Cisco TAC for assistance.
```

If an issue persists, click **Admin** to access Tech support. See *Working with Cisco Tech Support* for more information.



CHAPTER 10

Migrating From DCNM to ND

- Prerequisites and guidelines for migrating from DCNM to ND, on page 145
- Migrate Existing DCNM Configuration to ND, on page 147

Prerequisites and guidelines for migrating from DCNM to ND

Upgrading from DCNM 11.5(4) consists of the following workflow:

1. Ensure you complete the prerequisites and guidelines described in this section.
2. Back up your existing configuration using a migration tool specific to the target ND release.
3. Deploy a brand new Nexus Dashboard cluster.
4. Restore the configuration backup you created in step 1.

Note Before you proceed with the upgrade:

- Validate each fabric's credentials.
  - For LAN fabrics, navigate to the **Web UI** > **Administration** > **Credentials Management** > **LAN Credentials** page, select each fabric, and choose **Validate** to validate credentials.
  - For SAN fabrics, navigate to the **Web UI** > **Administration** > **Credentials Management** > **SAN Credentials** page, select each fabric, and choose **Validate** to validate credentials.
- If you are running an app on your DCNM, such as the Thousand Eyes integration app, disable that app before proceeding with these migration procedures.

Fabric Type Compatibility

By using the appropriate Upgrade Tool, you can restore data that is backed up from DCNM Release 11.5(4) on a newly deployed Nexus Dashboard for the fabric type as mentioned in the following table.

Note SAN fabrics are mainly unchanged in Nexus Dashboard release 4.1.1.

Pre-4.1.1 fabrics		4.1.1 fabric types
Fabric technologies	**Fabric types**	
LAN		
VXLAN EVPN	Data Center VXLAN EVPN	Data Center VXLAN EVPN - iBGP
eBGP VXLAN EVPN	BGP fabric	Data Center VXLAN EVPN - eBGP
VXLAN EVPN	Campus VXLAN EVPN	Campus VXLAN EVPN
eBGP Routed	BGP fabric	BGP fabric
Classic LAN	Enhanced Classic LAN	Enhanced Classic LAN
Classic LAN	Classic LAN	Legacy Classic LAN
Custom	External connectivity network	External and inter-fabric connectivity network
Custom	Custom network	External and inter-fabric connectivity network
Custom	Multi-site external network	External and inter-fabric connectivity network
LAN Monitor	LAN Monitor	External and inter-fabric connectivity network
VXLAN EVPN	VXLAN EVPN Multi-Site	VXLAN (fabric group)
Multi-Fabric Domain	Fabric Group	Classic (fabric group)
IPFM		
IPFM	IPFM	IPFM
IPFM	IPFM Classic	IPFM classic
Generic Multicast	IPFM Classic	IPFM classic
Multi-Fabric Domain	Fabric Group	IPFM (fabric group)

Feature Compatibility Post Upgrade

The following table lists caveats associated with features that are restored from DCNM 11.5(4) backup after upgrading.

Feature in DCNM 11.5(4)	Upgrade Support
Nexus Dashboard Insights configured	Carried over from 11.5(4)
Container Orchestrator (K8s) Visualizer	Carried over from 11.5(4)

Feature in DCNM 11.5(4)	Upgrade Support
VMM Visibility with vCenter	Carried over from 11.5(4)
Nexus Dashboard Orchestrator configured	Not carried over from 11.5(4)
Preview features configured	Not carried over from 11.5(4)
LAN switches in SAN installations	Not carried over from 11.5(4)
IPAM Integration	Not carried over from 11.5(4)
Custom topologies	Not carried over from 11.5(4); must be recreated and saved
DCNM Tracker	Not carried over from 11.5(4)
Fabric Backups	Not carried over from 11.5(4)
Report Definitions and Reports	Not carried over from 11.5(4)
Switch images and Image Management policies	Not carried over from 11.5(4)
SAN CLI templates	Not carried over from 11.5(4)
Switch images/Image Management data	Not carried over from 11.5(4)
Slow drain data	Not carried over from 11.5(4)
Infoblox configuration	Not carried over from 11.5(4)
Endpoint Locator configuration	You must reconfigure Endpoint Locator (EPL) post upgrade. However, historical data is retained up to a maximum size of 500 MB.
Alarm Policy configuration	Not carried over from 11.5(4)
Performance Management data	CPU/Memory/Interface statistics up to 90 days is restored post upgrade. Must be re-enabled on fabrics.
Temperature data	Temperature data is not saved in the backup and as a result is not restored after the migration. You must re-enable temperature data collection after the migration.

Migrate Existing DCNM Configuration to ND

This section describes how to back up your existing DCNM 11.5(4) configuration, deploy a new Nexus Dashboard cluster, and restore the configuration to finish the migration.

Procedure

Step 1 Download the upgrade tool.

a) Navigate to the Nexus Dashboard download page.

https://software.cisco.com/download/home/286327743/type/286328258/

b) In the **Latest Releases** list, choose the target release.

c) Download the upgrade tool appropriate for your deployment type.

DCNM 11.5(4) deployment type	Upgrade Tool File Name
ISO/OVA	`DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip`
Linux or Windows	`DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip`

d) Copy the upgrade tool image to your existing DCNM 11.5(4) server using the **sysadmin** account.

Step 2 Extract the archive and validate the signature for Linux/Windows deployments.

Note
If you are using the ISO/OVA archive, skip to the next step.

a) Ensure that you have Python 3 installed.

```
$ python3 --version
Python 3.9.6
```

b) Extract the downloaded archive.

```
# unzip DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_4.1.1_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

c) Validate signature.

Inside the ZIP archive, you will find the upgrade tool as well as the signature file. Use the following commands to validate the upgrade tool:

```
# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v dgst
 -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

d) Once the validation script signature is verified, extract the script itself.

```
# 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/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
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/bcprov-jdk15on-1.68.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/jnm.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbackup.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
```

Step 3 Extract the archive and validate the signature for ISO/OVA deployments.

Note
If you are using the Linux/Windows archive, skip to the next step.

a) Extract the downloaded archive.

```
# unzip DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip
Archive: DCNM_To_NDFC_4.1.1_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1.signature
inflating: cisco_x509_verify_release.py3
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

b) Validate signature.

Inside the ZIP archive, you will find the upgrade tool as well as the signature file. Use the following commands to validate the upgrade tool:

```
# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1 -s DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature -v dgst
-sha512
Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_OVA_ISO using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

Step 4 Back up existing configuration.

a) Log in to your DCNM Release 11.5(4) appliance console.

b) Create a screen session.

The following command creates a session which allows you to execute additional commands:

```
dcnm# screen
```

Note that the commands continue to run even when the window is not visible or if you get disconnected.

c) Gain super user (`root`) access.

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

d) For OVA and ISO, enable execution permissions for the upgrade tool.

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
```

e) Run the upgrade tool you downloaded in the previous step.

- For example, for release 4.1.1 for Windows:

```
C:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:
Initializing, please wait...
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard 4.1.1
 or not.
If upgrade to Nexus Dashboard 4.1.1 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 it again for verification:
…..
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection [id: 0][route:
{s}->https://127.0.0.1:9200] can be kept alive indefinitely
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.DefaultManagedHttpClientConnection - http-outgoing-0: set socket
timeout to 0
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection released: [id:
0][route: {s}->https://127.0.0.1:9200][total kept alive: 1; route allocated: 1 of 20; total
allocated: 1 of 20]
2024-07-25 22:35:34,969 [main] INFO DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 145
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ###### Total time to export Daily data: 7
seconds.
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ###### Total time to export PM data: 36
seconds.
2024-07-25 22:35:35,169 [main] INFO DCNMBackup - Creating data file...
2024-07-25 22:35:38,083 [main] INFO DCNMBackup - Creating metadata file...
2024-07-25 22:35:38,085 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-25 22:35:38,267 [main] INFO DCNMBackup - Done
```

- For example, for release 4.1.1 for Linux:

```
# ./DCNMBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:
Initializing, please wait...
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard 4.1.1
 or not.
If upgrade to Nexus Dashboard 4.1.1 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 it again for verification:
……
2024-07-26 04:04:46,540 [main] INFO DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 92
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ###### Total time to export Daily data: 3
seconds.
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ###### Total time to export PM data: 11
seconds.
2024-07-26 04:04:46,958 [main] INFO DCNMBackup - Creating data file...
2024-07-26 04:04:47,456 [main] INFO DCNMBackup - Creating metadata file...
2024-07-26 04:04:47,467 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-26 04:04:47,478 [main] INFO DCNMBackup - Done.
```

- For example, for release 4.1.1 for OVA:

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO_4.1.1
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for OVA/ISO.
This tool will analyze this system and determine whether you can move to
Nexus Dashboard 4.1.1 or not.
If upgrade to Nexus Dashboard 4.1.1 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 Nexus Dashboard 4.1.1
Thank you!

********************************************************************************
Continue? [y/n]: y
Collect operational data (e.g. PM, EPL)? [y/n]: y
Does this DCNM 11.5(4) 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 it again for verification:
……
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
Adjusting DB tables
Creating dcnm backup file
Creating final backup file
Done.
Backup file: backup11_sandcnm_20240726-113054.tar.gz
```

Step 5 Deploy a brand new Nexus Dashboard cluster as described in one of the earlier chapters in this document.

Ensure that you complete all guidelines and prerequisites for the Nexus Dashboard platform and the specific form factor listed in the deployment chapters above.

Note

- You must provide the required number of Persistent IP addresses in the Nexus Dashboard GUI before proceeding with restoring your DCNM configuration..
- If your existing configuration used smart licensing with direct connectivity to Cisco Smart Software Management (CSSM), you must ensure that your new Nexus Dashboard has the routes required to reach the CSSM website.

  Ensure that subnets for IP addresses on `smartreceiver.cisco.com` are added to the route table in the Nexus Dashboard's **Admin** > **System Settings** > **General** > **Routes** page for the Nexus Dashboard management network.

  You can `nslookup` on `smartreceiver.cisco.com` to find the most recent subnet, for example:

```
$ nslookup smartreceiver.cisco.com
Server:         24.233.18.143
Address:        24.233.18.143#53

Name:   smartreceiver.cisco.com
Address: 146.112.59.81
Name:   smartreceiver.cisco.com
Address: 2a04:e4c7:fffe::f
```

  You can use either and IPv4 address or an IPv6 address, based on your Nexus Dashboard deployment.

  In addition, because Nexus Dashboard is considered a new product instance, you must re-establish trust. If you took the backup with an expired Trust Token, you must manually run the Smart Licensing Configuration wizard and enter a valid token after the upgrade.

Step 6 Restore the configuration backup in the new cluster.

For more information, see *Backing Up and Restoring Your Nexus Dashboard*.

a) Navigate to the unified backup and restore page in the Admin Console GUI: **Admin** > **Backup and Restore**.

Backups that are already configured are listed in the **Backups** page.

b) Click **Restore** in the upper right corner of the main **Backup and Restore** page to access the **Restore** slider page.

The **Restore** slide page appears.

c) In the **Source** field, determine where the backup is that you want to restore, if applicable.

- **Upload Configuration Backup Table**: The Backup File area appears, where you can either drag and drop a local backup file to restore or you can navigate to the local area on your system to select a backup file to restore.
- **Remote Location**:

  1. In the **Remote Location** field, select an already-configured remote location from the list, if available, or click **Create Remote Location**.

If you click **Create Remote Location**, follow the procedures provided in "Create a remote storage location" in *Backing Up and Restoring Your Nexus Dashboard*, then return here. Even though you should have configured a remote location as part of the remote backup process, you might also have to configure a remote location as part of the restore process if you're in a different cluster from the one where you configured the remote backup. In this case, you would be configuring the remote location again at this point so that the system can find the remote backup that you configured in the other cluster.

2. In the **Remote Path** field, enter the remote path where the remote backup resides.

d) In the **Encryption Key** field, enter the encryption key that you used when you backed up the file.
e) In the Validation area, on the row with your backup, click **Validate and Upload**.
f) When the Progress bar shows 100% for the validation, the **Next** button becomes active. Click **Next**.
g) When upgrading from DCNM to ND/NDFC, ND/NDFC always ignores the **Ignore External IP** setting and will always try to use existing IPs from the backup, if possible; otherwise, it uses new IPs.

The following table provides more information on how the system handles IP addresses.

Deployment Type in Release 11.5(4)	In 11.5(4), trap IP address is collected from	LAN Device Management Connectivity	Trap IP address after upgrade	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.
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 **Manage > Fabrics**, double click on the fabric to view **Fabric Overview**. From the **Actions** drop-down list, select **Recalculate and Deploy**. 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.

Deployment Type in Release 11.5(4)	In 11.5(4), trap IP address is collected from	LAN Device Management Connectivity	Trap IP address after upgrade	Result
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 **Manage > Fabrics**, double click on the fabric to view **Fabric Overview**. From the **Actions** drop-down list, select **Recalculate and Deploy**. Click **Deploy Config**.
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.

h) Click **Restore**.

A warning window appears to verify that you want to begin the restore process. Note that you will not be able to access any Nexus Dashboard functionality while the restore process runs, which could take several minutes.

i) Click **Restore** in the warning window to proceed with the restore process.

Another window appears, showing the progress of the restore process. Click the arrow next to the entry in the **Type** column to get more details of the restore process.

j) If the restore process is successful, you will see 100% as the Progress, and the **View History** button becomes active.

Click **View History** to navigate to the **History** area in the **Backup and Restore** window, with the restore process displayed and **Success** shown in the **Status** column.

Note

After you have restored a configuration that was backed up using the new ND unified backup and restore feature, the state of the fabrics shown at the ND level might be out of sync with the true state of the fabrics. To bring the fabrics status back in sync, in the **Fabric Overview** page, click **Actions** at the top of the page and select **Recalculate and Deploy**.

Step 7 Complete the post-upgrade tasks.

a) If you have a SAN deployment in ND release 4.1.1:

After restoring the data from backup, all the server-smart licenses are **OutofCompliance**.

You can migrate to Smart Licensing using Policy from the **Admin** > **Licensing** > **Smart** page in the UI and establish trust with CCSM using SLP.

b) If you have a LAN deployment in ND release 4.1.1:

Certain features might not carried over when you upgrade from DCNM 11.5(4). See Feature Compatibility Post Upgrade, on page 146 for more information.