

Deploying in VMware ESX

- Prerequisites and Guidelines, on page 1
- Deploying Nexus Dashboard Using VMware vCenter, on page 4
- Deploying Nexus Dashboard Directly in VMware ESXi, on page 19

Prerequisites and Guidelines

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

• Ensure that the ESX form factor supports your scale and services requirements.

Scale and services support and co-hosting vary based on the cluster form factor and the specific services 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

This document describes how to initially deploy the base Cisco Nexus Dashboard cluster. If you want to expand an existing cluster with additional worker nodes, see the *Infrastructure Management* article instead, which is also available from the Cisco Nexus Dashboard UI.

Some services (such as Nexus Dashboard Fabric Controller) 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.

Standby nodes are not supported with this cluster form factor.

• Review and complete the general prerequisites described in Deployment Overview and Requirements.

Note that 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 worker 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*

- Review and complete any additional prerequisites described in the *Release Notes* for the services you plan to deploy.
- When deploying in VMware ESX, you can deploy two types of nodes:

- Data Node—node profile with higher system requirements designed for specific services that require the additional resources.
- App Node—node profile with a smaller resource footprint that can be used for most services.



Note

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

Ensure you have enough system resources:

Table	1: Den	lovment F	Requirements
Table	1. Dop	ioyiniciit i	icyuniciiciici

ta Node Requirements	App Node Requirements
• VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3	• VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3
• VMware vCenter 7.0.1, 7.0.2, 7.0.3 if deploying using vCenter	• VMware vCenter 7.0.1, 7.0.2, 7.0.3 if deploying using vCenter
• Each VM requires the following:	• Each VM requires the following:
• 32 vCPUs with physical reservation of at least 2.2GHz	 16 vCPUs with physical reservation of at least 2.2GHz
• 128GB of RAM with physical reservation	• 64GB of RAM with physical reservation
• 3TB SSD storage for the data volume and an additional 50GB for the system volume	 500GB HDD or SSD storage for the da volume and an additional 50GB for th system volume
Data nodes must be deployed on storage with the following minimum performance requirements:	Some services require App nodes to be deployed on faster SSD storage while other services support HDD. Check th Nexus Dashboard Capacity Planning to
• The SSD must be attached to the data store directly or in JBOD mode if using a RAID Host Bus Adapter	to ensure that you use the correct type storage.
(HBA)	Note Beginning with Nexus
• The SSDs must be optimized for	Dashboard release 3.0(1i) and Nexus Dashboard Insights
Mixed Use/Application (not Read-Optimized)	release $6.3(1)$, you can use the
• 4K Random Read IOPS: 93000	OVA-App node profile for the Insights service. However, you
	must change from the default
• 4K Random Write IOPS: 31000	500GB disk requirement to 1536GB when deploying node
• We recommend that each Nexus Dashboard	VMs which will be used for
node is deployed in a different ESXi server.	hosting Insights.
	• 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 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 vND 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.

Because Nexus Dashboard is a platform infrastructure, it is not possible to bring down all services.

In other words, if you want to take a snapshot of the virtual machine (such as for debugging purposes), the snapshot must have all Nexus Dashboard services running.

You can choose to deploy the nodes directly in ESXi or using vCenter.

If you want to deploy using vCenter, following the steps described in Deploying Nexus Dashboard Using VMware vCenter, on page 4.

If you want to deploy directly in ESXi, following the steps described in Deploying Nexus Dashboard Directly in VMware ESXi, on page 19.



Note

If you plan to deploy Nexus Dashboard Insights using the OVA-App node profile, you must deploy using vCenter.

Nexus Dashboard Insights requires a larger disk size than the default value for OVA-App node profiles. If you plan to deploy NDI using the OVA-App node profile, you must change the default disk size for OVA-App nodes from 500GB to 1.5TB during VM deployment. Disk size customization is supported when deploying through VMware vCenter only. For detailed Insights requirements, see the Nexus Dashboard Capacity Planning and the Nexus Dashboard Insights Deployment document.

Deploying 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 Deploying Nexus Dashboard Directly in VMware ESXi, on page 19 instead.

Before you begin

• Ensure that you meet the requirements and guidelines described in Prerequisites and Guidelines, on page 1.

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.

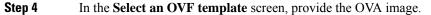
Depending on the version of your vSphere client, the location and order of configuration screens may differ slightly. The following steps provide deployment details using VMware vSphere Client 7.0.

Step 3 Start the new VM deployment.

📃 vSphere Client (Q							
	<	🛛 172.23 Summary	3.136.87 ACT Monitor Configur		VMs	Resource Pools	Datastores	Networks 🔇
✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ☐ Datacenter ✓ ↓ ✓ ⑦ 22.2136.84 ✓ ↓ ⑦ 22.2136.85 ↓ ⑦ 22.2136.87 ↓ ⑦ 22.2136.87 ↓ ⑦ 172.23136.89 ↓ ⑦ 172.23136.89	me.Jocal 고,Actions - 172.23.136.87 슈킹: New Virtual Machine 양 Deploy OVF Template 양 New Resource Pool	0	Hypervisor: Model: Processor Type: Logical Processors: NICs: Virtual Machines: State: Uptime:	VMware ESXI, 7.0.3 UCSC-C220-MSSX Intel(R) Xeon(R) Gol 80 4 2 Connected 3 days		J @ 2.50GHz		
	Et New vApp	Hardware						\checkmark
\sim	Import VMs	Tags	~~~~	$\sim \sim$	\sim	~~~~	\sim	\sim

- a) Right-click the ESX host where you want to deploy the VM.
- b) Select **Deploy OVF Template...**

The Deploy OVF Template wizard appears.



Deploy OVF Template	Select an OVF template ×
1 Select an OVF template	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
2 Select a name and folder	
3 Select a compute resource	http://aci-artifactory-001.insieme.local:8040/artifactory/atom-bld/releases/nd/v3.0.0.213/nd-dk9.3.0.1a.ova
4 Review details	
5 Select storage	UPLOAD FILES No files selected.
6 Ready to complete	

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.

Deploy OVF Template	Select a name and folder × Specify a unique name and target location
1 Select an OVF template	Virtual machine name: a nd-ova-node1
2 Select a name and folder	Select a location for the virtual machine.
3 Select a compute resource	
4 Review details	
5 Select storage	
6 Ready to complete	
	CANCEL BAC NEXT

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.

Deploy OVF Template	Select a compute resource Select the destination compute resource for this operation	×
1 Select an OVF template	✓ Datacenter	
2 Select a name and folder	 > □ 172.23.136.84 > □ 172.23.136.86 □ 172.23.136.87 	
3 Select a compute resource	> 172.23.136.88	
4 Review details		
5 Select storage		
6 Ready to complete		
	Compatibility	
	Compatibility checks succeeded.	
	CANCEL BAD NEXT	

- 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.

Deploy OVF Template	Configuration Select a deployment configuration	×
1 Select an OVF template	© Арр	Description Use this deployment profile to
2 Select a name and folder	O Data	configure an App OVA with 16 vCPUs, 64 GB RAM, and 500 GB Disk.
3 Select a compute resource		
4 Review details		
5 Configuration		
6 Select storage		
7 Select networks		
8 Customize template		
9 Ready to complete		
	2 Items	
		CANCEL BAD NEXT

- 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, on page 1.
- b) Click Next to continue
- **Step 9** In the **Select storage** screen, provide the storage information.

Deploy OVF Template	Select sto	rage							×
1 Select an OVF template		rtual machi	nfiguration and dis ine (Requires Key I Thick Provisio		<u>~</u>	~	٦		
2 Select a name and folder 3 Select a compute resource	-		this virtual machine						
4 Review details	Name	٣	Storage T Compatibility	Capacity T	Provisioned T	Free	Type	Ŧ	Cluster
5 Configuration	 ○ 	tore1		989.75 GB 3.49 TB	613.47 GB 1.55 TB	376.28 GB 1.94 TB	VMFS 6 VMFS 6		
		tore3-s		3.49 TB 3.49 TB	1.46 GB 1.46 GB	3.49 TB 3.49 TB	VMFS 6 VMFS 6		
6 Select storage 7 Select networks									
8 Customize template									
9 Ready to complete									
									4 items
	Compatibility								
	✓ Compatibility	/ checks su	cceeded.						
						CANC	EL BA	d	NEXT

- a) From the Select virtual disk format drop-down, choose Thick Provisioning.
- b) Check the **Disable Storage DRS for this virtual machine** checkbox.

Nexus Dashboard does not support VMware DRS. We recommend that you check the **Disable Storage DRS for this virtual machine** option in case DRS is enabled at the ESXi cluster level.

c) Select the datastore for the virtual machine.

We recommend a unique datastore for each node.

- 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:

- fabric0 is used for the Nexus Dashboard cluster's Data Network
- mgmt0 is used for the Nexus Dashboard cluster's Management Network.

For more information about these networks, see Prerequisites and Guidelines in the "Deployment Overview and Requirements" chapter.

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

Deploy OVF Template	Customize template Customize the deployment properties of this softwar	e solution.			×
1 Select an OVF template	O All properties have valid values				×
2 Select a name and folder	✓ Resource Configuration	1 settings			
3 Select a compute resource	a 1. Data Disk Size (GB)	Data disk size (min 500) 500	GB, max 1536GB (1.5T)	B))	
4 Review details	✓ Node Configuration	3 settings			
5 Configuration	b 1. Password	Local "rescue-user" pas	sword		
		Password		0	
6 Select storage		Confirm Password		0	
7 Select networks					
8 Customize template	C 2. Management Network Address and subnet	Management network a 2222::32/120	ddress. Enter IP/subn	et Ex: 192.168.1.100/24	l or
9 Ready to complete		172.23.141.129/21			
	d 3. Management Gateway IP	Management network g or 2222::1	ateway IP address. Er	nter IP only Ex: 192.168	3.1.1
		172.23.136.1			
			CANCEL	BA e NEX	т

a) Provide the size for the node's data volume.

The default values will be pre-populated based on the type of node you are deploying, with App node having a single 500GB disk and Data node having a single 3TB disk. In addition to the data volume, a second 50GB system volume will also be configured but cannot be customized.

Note If you want to specify a custom disk size for your node, you must do so during VM deployment. Resizing the disk after the node is brought up is not supported by Nexus Dashboard.

If you plan to deploy Nexus Dashboard Insights using the OVA-App node profile, you must change the data disk size from the default 500GB value to 1536GB. For additional information about cluster sizing, system resource requirements, and node profile support, see the Nexus Dashboard Capacity Planning and the Nexus Dashboard Insights Deployment document.

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 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'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 guest time with host 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 provided in a previous step and click **Login**

		<text><section-header></section-header></text>
--	--	--

Step 17Provide the Cluster Details.

In the Cluster Details screen of the Cluster Bringup wizard, provide the following information:

- -

Provide the necessary c Name and nd-duster. Enable IPv6 NTP Key Key ID	luster details to s	set up Nexus Dasht	ooard and bring up the u	er interface.	
Name + a nd-cluster- Enable IPv6					
a nd-cluster.					
Enable IPv6					
NTP Key Key ID					
	Auth Typ	be Trusted			
C Add NTP Key					
NTP Host* Ke	ey ID	Preferred			
171.68.38.65		false	/ 1		
Add NTP Server					
DNS Provider IP Address*					
171.70.168.183	/ 🗊				
e Add DNS Provider					
Proxy Server (j					
Authentication required	for provu				
	for proxy				
Yes No					
	resses beginning v	vith*			
 Add Ignore Host 					
DNS Search Domain*					
Add DNS Search Domain					
App Notwork + (i)					
Service Network* (i)					
Construction of the second					
2000::/108					
Service Network IPv6 🛈					
3000::/108					
Hide Advanced Settings 🥆					
	171.68.38.65 Add NTP Server DNS Provider IP Address* 171.70.168.183 Add DNS Provider Proxy Server ③ Authentication required Yes No Ignore proxy for host addl Add Ignore Host DNS Search Domain* Add Ignore Host DNS Search Domain* Add DNS Search Domain* App Network * ③ 100.80.0.0/16 App Network IPV6 ③ 2000:/108	171.68.38.65 C Add NTP Server DNS Provider IP Address* 171.70.168.183 ✓ Ø Add DNS Provider Proxy Server () ✓ f Authentication required for proxy g Yes No Ignore proxy for host addresses beginning w ● Add Ignore Host DNS Search Domain ● Add DNS Search Domain App Network * () 100.80.0.0/16 App Network IPv6 () 2000:/108 Service Network IPv6 () 3000://108 Hide Advanced Settings () 104.40	171.68.38.65 false DNS Provider IP Address* 171.70.168.183 171.70.168.183 ✓ 🗊 ④ Add DNS Provider Proxy Server () Proxy Server () ✓ ✓ ✓ Ø Ves No Ignore proxy for host addresses beginning with* ● Add Ignore Host DNS Search Domain* ● Add DNS Search Domain App Network * () 100.80.0.0/16 App Network IPv6 () 2000:/108 Service Network IPv6 () 3000:/108 Hide Advanced Settings ∧	171.68.38.65 false DNS Provider IP Address* 171.70.168.183 171.70.168.183 a Add DNS Provider Proxy Server (> a Add DNS Provider Proxy Server (> f Add IDNS Provider Proxy Server (> a Add DNS Provider Proxy Server (> f Add Ignore proxy for host addresses beginning with* a Add Ignore Host DNS Search Domain* a Add DNS Search Domain App Network * (>) 100.80.00/16 App Network IPv6 () 2000:/108 Service Network IPv6 () 3000:/108 Hide Advanced Settings ^	171.68.38.65 false DNS Provider IP Address* 171.70.168.183 IT.70.0168.183 Add DNS Provider Proxy Server () Add DNS Provider Proxy Server () Add INS Provider Proxy Server () Authentication required for proxy Yes No Ignore proxy for host addresses beginning with* Add INS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* Add DNS Search Domain* App Network IPv6 () 2000::/108 Service Network IPv6 () 3000::/108 Hide Advanced Settings ^

a) Provide the Cluster Name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

- b) (Optional) If you want to enable IPv6 functionality for the cluster, check the **Enable IPv6** checkbox.
- c) (Optional) If you want to enable NTP server authentication, click Add NTP Key.

In the additional fields, provide the following information:

• **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.
- Choose whether this key is **Trusted**. Untrusted keys cannot be used for NTP authentication.
- **Note** For the complete list of NTP authentication requirements and guidelines, see Prerequisites and Guidelines.

After you've entered the information, click the checkmark icon to save it.

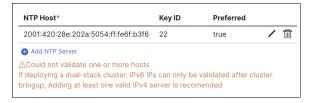
d) Click +Add NTP Host to add one or more NTP servers.

In the additional fields, provide the following information:

- NTP Host you must provide an IP address; fully qualified domain name (FQDN) are not supported.
- **Key ID** if you want to enable NTP authentication for this server, provide the key ID of the NTP key you defined in the previous step.
- Choose whether this NTP server is Preferred.

After you've entered the information, click the checkmark icon to save it.

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 provided 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 (you will provide it in the next step) and is unable to connect to an IPv6 address of the NTP server.

In this case, simply finish providing the other required information as described in the following steps and click **Next** to proceed to the next screen where you will provide IPv6 addresses for the nodes.

If you want to provide additional NTP servers, click +Add NTP Host again and repeat this substep.

e) Click +Add DNS Provider to add one or more DNS servers.

After you've entered the information, click the checkmark icon to save it.

f) Provide 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.

The proxy server must have the following URLs enabled:

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

If you want to skip proxy configuration, mouse over the information (i) icon next to the field, then click Skip.

- g) (Optional) If your proxy server required authentication, change **Authentication required for Proxy** to Yes and provide the login credentials.
- h) (Optional) Expand the Advanced Settings category and change the settings if required.

Under advanced settings, you can configure the following:

Provide one or more search domains by clicking +Add DNS Search Domain.

After you've entered the information, click the checkmark icon to save it.

• Provide custom App Network and Service Network.

The application overlay network defines the address space used by the application's services running in the Nexus Dashboard. The field is pre-populated with the default 172.17.0.1/16 value.

The services network is an internal network used by the Nexus Dashboard and its processes. The field is pre-populated with the default 100.80.0.0/16 value.

If you have checked the **Enable IPv6** option earlier, you can also define the IPv6 subnets for the App and Service networks.

Application and Services networks are described in the Prerequisites and Guidelines section earlier in this document.

- i) Click Next to continue.
 - **Note** If your node has only an IPv4 management address but you have checked **Enabled IPv6** and provided an IPv6 NTP server address, ensure that the NTP address is correct and click **Confirm** to proceed to the next screen where you will provide the nodes' IPv6 addresses.



Step 18 In the **Node Details** screen, update the current 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 provide the Data network information for the node before you can proceed with adding the other primary nodes and creating the cluster.

luster Bring	gup					
 Cluster Details Node Details 	Node Details Provide the necessary noc	e details to set up Nexus Dash	board and bring	up the user interface.		
3 Confirmation	Site		Fabric 0/1	Mgmt 0/	1	
	Site	Data Network	Fabric 0/1	Mgmt 0/	1 Management Network	MN
	Site		Fabric 0/1	Mgmt 0/	1	
	Serial Number	Name Management	Network	ſ	Data Network	
	D52C57566031	IPv4/mask: 172 IPv4 Gateway: IPv6/mask: - IPv6 Gateway:	172.23.136.1	1	Pv4/mask: Pv4 Gateway: Pv6/mask: - Pv6 Gateway: - /LAN: -	
	🚯 Add Node					

- a) Click the Edit button next to the first node.
- b) Provide the Name for the node.

The node's Serial Number and the Management Network information are automatically populated.

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

c) 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, 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 IPv4/IPv6 stack.

d) (Optional) If required, Enable BGP for the data network.

BGP configuration is required for the Persistent IPs feature used by some services, such as Nexus Dashboard Insights with NDFC fabrics. This feature is described in more detail in Prerequisites and Guidelines 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.

When you 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.
- e) Click **Update** 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.

ployment Details Management P Address * 0 r722.141.130 Uerrame * reacours our read Reased * readed *			
17223.141.30 Username: reconcurrer Personard: Personard: mormail: Nime: reformation: Statumbers: corred statumbers: corred Pr4 Address/Mask* 17223.136.1 IPv6 Address/Mask* 1723.136.1 IPv6 Address/Mask* 173.136.1 IPv6 Address/Mask* IPv6 Address/Mask IPv6 Address/Mask IPv6 Address/Mask	ment Details		
Wername * Wername * Wername * Password * Imme * merdad Serial Number * 0274E008000	agement IP Address * 🛈		
Password* Password* minum 0 hdidate 0	23.141.130		
Password* mercial Name • merciada Serial Number * our decleado our decleado pred Address/Mask * 1722.3.141.3021 PVA dadress/Mask * 1723.3.141.3021 PVA dadress/Mask * 1723.140.730.1 PVA dadress/Mask * 1723.140.701.1 PVA dadress/Mask * 1723.140.701.1 PVA dadress/Mask * 1723.140.701.1 PVA dadress/Mask * 1723.140.701.1	name *		
window Image: Imag	ue-user		
window Image: Imag	word *		
neral Name • nerded2 Serial Number • 027/4E0680400 Pv4 Address/Mask • 1722.3.141.130.21 Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * Pv6 Address/Mask * <p< td=""><td></td><td>Validate</td><td></td></p<>		Validate	
Name • ind-code2 Serial Number • 0274E0059C00 nagement Network ○ IPv4 Address/Mask • 172.23.141.130/21 IPv6 Address/Mask 172.23.136.1 IPv6 Gateway IPv6 Gateway. 172.31.136.1 IPv6 Address/Mask • 172.31.136.1 IPv6 Gateway. I72.31.136.1 IPv6 Gateway. I72.31.36.1 ITUE IPv6 Gateway. ITUE ITUE			
widdde2 erial Number* 1274E058B040	I		
adrodd yrial Number* 274EC0558C40 aggement Network () vd Address/Mask* 7223.141.13021 yd Address/Mask 723.138.1 v6 Address/Mask* 723.138.1 v8 Address/Mask* 723.138.1 v8 Address/Mask* 723.138.1 v8 Address/Mask* 723.138.1 v8 Address/Mask* 723.138.1 v4 Address/Mask v4 Address/Mask 723.138.1 v8 Address/Mask v8 Address/Mask v9 Address/Mask v9 Address/Mask v9 Address/Mask	e *		
Srial Number • 0274EC058C40 nagement Network () IPv4 Address/Mask • 17223.141.150/21 IPv4 Gateway • 17223.158.1 IPv6 Gateway • 1723.140.70/21 IPv6 Address/Mask • 1723.138.1 IPv6 Gateway • 1723.138.1 IPv6 Address/Mask • I723.138.1 IPv6 Gateway • I723.138.1 IPv6 Address/Mask • IPv6 Address/Mask •			
0274EC68BC40 aragement Network PV4 Address/Mask 172.23.146.130021 PV6 Address/Mask 172.23.136.1 PV6 Address/Mask 172.31.140.70/21 PV4 Address/Mask 172.31.136.1 PV6 Address/Mask 172.31.136.1 PV6 Address/Mask 172.31.136.1			
hagement Network Pv4 Address/Mask 172.23.136.1 Pv6 Gateway 172.31.36.1 Pv6 Address/Mask 172.31.36.1 Pv6 Address/Ma			
PV A Address/Mask 172.23.141.13021 Pv4 Gateway* 172.23.136.1 Pv6 Gateway Pv6 Gateway Image: Signal Sign			
172 23.141.13021 v4 Gateway • 172 23.136.1 v6 Gateway v12 Cateway • v	ement Network 🕠		
v4 Gateway * T2 23 138.1 v8 Address/Mask v8 Gateway	Address/Mask *		
172.23.136.1 v/6 Address/Mask • Ve Sateway • Ve Sateway	23.141.130/21		
172.23.138.1 IPV6 Address/Mask IPV6 Gateway I72.31.140.70/21 IPV6 Address/Mask I72.31.138.1 IPV6 Address/Mask IPV6 Address/Mask I72.31.138.1 IPV6 Address/Mask IVF6 Gateway	Gateway •		
Pv6 Gateway Image: Constraint of the constra			
Pv6 Gateway a Network ③ Pv4 Address/Mask * 172.31.340.70/21 Pv4 Gateway * 172.31.380.1 Pv6 Gateway Pv6 Gateway Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * Pv6 Gateway * <td>Address/Mask</td> <td></td> <td></td>	Address/Mask		
IPV4 Address/Mask* 172.31.40.70/21 IPV6 Address/Mask 172.31.30.1 IPV6 Address/Mask			
IPV4 Address/Mask* 172.31.40.70/21 IPV6 Address/Mask 172.31.30.1 IPV6 Address/Mask	Gateway		
IPv4 Address/Mask * 172.31.40.70/21 IPv4 Address/Mask 172.31.136.1 IPv6 Address/Mask IPv6 Gateway IV0 VLAN ()	outonay		
IPv4 Address/Mask * 172.31.40.70/21 IPv4 Address/Mask 172.31.136.1 IPv6 Address/Mask IPv6 Gateway IVVA Address/Mask			
172.31.140.70/21 IPV4 Gateway* 172.31.136.1 IPV6 Gateway VLAN O	etwork 🕕		
172.31.140.70/21 PV4 Gateway* 172.31.136.1 PV6 Address/Mask PV6 Gateway VLAN O	Address/Mask *		
172.31.136.1 Pv6 Address/Mask Pv6 Gateway VLAN O			
172.31.136.1 Pv6 Address/Mask Pv6 Gateway ILAN O	Gateway *		
Pv6 Address/Mask Pv6 Gateway VLAN O			
IPv6 Gateway			
	Gateway		
inable BGP	N (U)		
_	le BGP		

- 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.

After network connectivity is validated, you can provide the other required information for the node.

c) Provide the Name for the node.

The node's **Serial Number** and the **Management Network** information are automatically populated during the management network information validation in the previous step.

d) 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, 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 IPv4/IPv6 stack.

e) (Optional) If required, Enable BGP for the data network.

BGP configuration is required for the Persistent IPs feature used by some services, such as Nexus Dashboard Insights with NDFC fabrics. This feature is described in more detail in Prerequisites and Guidelines 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.

When you 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 2.2.2.2

- BGP Peer Details, which includes the peer's IPv4 or IPv6 address and peer's ASN.
- f) Click **Add** to save the changes.
- **Step 20** Repeat the previous step to add the 3rd node.

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

Step 21 In the **Node Details** page, click **Next** to continue.

After you have provided the management and data network information for all nodes, you can proceed to the final **Confirmation** screen.

Cluster Details	Node Details	rv node details to	set up Nexus Dashl	board and bring up the	user interface		
2 Node Details	Site			Fabric 0/1	Mgmt 0/1		
3 Confirmation	Site	L2/L3	Data Network	Fabric 0/1	Mgmt 0/1	Management Netwo	ork MN
	Site	_		Fabric 0/1	Mgmt 0/1		
	Serial Number	Name	Managemen	t Network	Data Network		
	D52C57566031	nd-node1			IPv4/mask: 172.3 IPv4 Gateway: 17 IPv6/mask: - IPv6 Gateway: - VLAN: -		/ 1
	0274EC65BC40	nd-node2			IPv4/mask: 172.3 IPv4 Gateway: 17 IPv6/mask: - IPv6 Gateway: - VLAN: -		/ 1
	B244B532BA5D	nd-node3			IPv4/mask: 172.3 IPv4 Gateway: 17 IPv6/mask: - IPv6 Gateway: - VLAN: -		/ 1

Step 22 In the **Confirmation** screen, review and verify the configuration information and click **Configure** to create 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 23 Verify that the cluster is healthy.

It may take up to 30 minutes for the cluster to form and all the services to start.

After all three nodes are ready, you can log in to any one node via SSH as the rescue-user using the password you provided during node deployment and run the following command to verify cluster health:

a) Verify that the cluster is up and running.

You can check the current status of cluster deployment by logging in to any of the nodes and running the acs health command.

While the cluster is converging, you may see the following outputs:

```
$ 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

b) Log in to the Nexus Dashboard GUI.

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 of the Nexus Dashboard cluster.

Step 24 Configure the **Network Scale** parameters for your cluster.

This is described in the **Infrastructure Management** > **Cluster Configuration** section of the *Cisco Nexus Dashboard User Guide*, which is also available directly from your Nexus Dashboard's Help Center.

Deploying 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 Deploying Nexus Dashboard Directly in VMware ESXi, on page 19 instead.

Before you begin

• Ensure that you meet the requirements and guidelines described in Prerequisites and Guidelines, on page 1.

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.
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. Th following steps provide deployment details using VMware ESXi 7.0.

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

☆ Navigator	insbudoc	-esx2.insieme.local
Manage	🗄 Host	h vCenter 🎁 Create/Register VM 🖑 🖥 Shut down 🦓 Reboot C Refresh 🏟 Actions
Monitor	R Manage with vCenter Serve	er nsbudoc-esx2.insieme.local
🛱 Virtual Machi	S Disconnect from vCenter S	
Stora	Create/Register VM	tate: Normal (connected to vCenter Server at 172.31.141.49) ptime: 4.13 days
Networking vSwitch0	C Shut down	
	C Reboot	
	Services	>
	_	Cisco Systems Inc
	enter maintenance mode	UCSC-C220-M5SX
	Lockdown mode	40 CPUs x Intel(R) Xeon(R) Gold 6248 CPU @ 2.50GHz
	覺 Permissions	255.66 GB
	Generate support bundle	0 B used, 0 B capacity
	F- Get SSH for Chrome	

Step 4

Select creation type Select OVF and VMDK files	Select creation type How would you like to create a Virtual Machine?	
 3 Select OV and Vib/Cilles 3 Select storage 4 License agreements 5 Deployment options 6 Additional settings 7 Ready to complete 	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	This option guides you through the process of creating a virtual machine from an OVF and VMDK flies.

- **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.

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

Nexus Dashboard networks are described in Deployment Overview and Requirements.

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

Node profiles are described in Prerequisites and Guidelines, on page 1.

- 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 keyhole...
[ OK ] Started keyhole.
[ OK ] Started logrotate.
[ OK ] Started logrotate.
```

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 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.

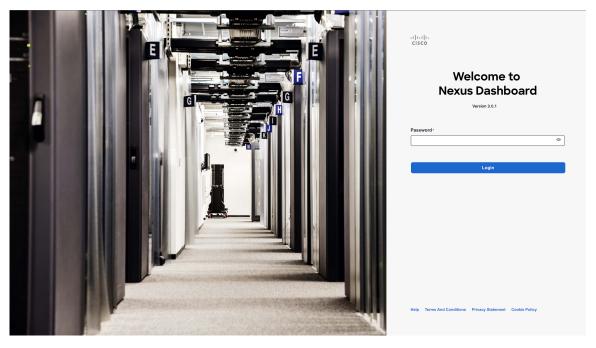
Note You must provide the same password for all nodes or the cluster creation will fail.

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 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 provided in a previous step and click Login



Step 16 Provide the Cluster Details.

In the Cluster Details screen of the Cluster Bringup wizard, provide the following information:

Cluster Bring	up
 Cluster Details Node Details Confirmation 	Cluster Details Provide the necessary cluster details to set up Nexus Dashboard and bring up the user interface. Name: Ind-duster: Ind-duster: Imd-duster: Imd-duster: I
h	Authentication required for proxy Yes No Ignore proxy for host addresses beginning with* Add Ignore Host DNS Search Domain* Add DNS Search Domain App Network * Intervice Network * Intervice
$\overline{\langle}$	Cancel

a) Provide the Cluster Name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

- b) (Optional) If you want to enable IPv6 functionality for the cluster, check the Enable IPv6 checkbox.
- c) (Optional) If you want to enable NTP server authentication, click Add NTP Key.

In the additional fields, provide the following information:

• **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.
- Choose whether this key is **Trusted**. Untrusted keys cannot be used for NTP authentication.

Note For the complete list of NTP authentication requirements and guidelines, see Prerequisites and Guidelines.

After you've entered the information, click the checkmark icon to save it.

d) Click +Add NTP Host to add one or more NTP servers.

In the additional fields, provide the following information:

- NTP Host you must provide an IP address; fully qualified domain name (FQDN) are not supported.
- **Key ID** if you want to enable NTP authentication for this server, provide the key ID of the NTP key you defined in the previous step.
- Choose whether this NTP server is Preferred.

After you've entered the information, click the checkmark icon to save it.

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 provided an IPv6 address for an NTP server, you will get the following validation error:

NTP Host*	Key ID	Preferred		
2001:420:28e:202a:5054:ff:fe6f:b3f6	22	true	/	1
Add NTP Server Could not validate one or more hosts If deploying a dual-stack cluster, IPv6 IP bringup, Adding at least one valid IPv4 s			uster	

This is because the node does not have an IPv6 address yet (you will provide it in the next step) and is unable to connect to an IPv6 address of the NTP server.

In this case, simply finish providing the other required information as described in the following steps and click **Next** to proceed to the next screen where you will provide IPv6 addresses for the nodes.

If you want to provide additional NTP servers, click +Add NTP Host again and repeat this substep.

e) Click +Add DNS Provider to add one or more DNS servers.

After you've entered the information, click the checkmark icon to save it.

f) Provide 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.

The proxy server must have the following URLs enabled:

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

If you want to skip proxy configuration, mouse over the information (i) icon next to the field, then click Skip.

- g) (Optional) If your proxy server required authentication, change **Authentication required for Proxy** to Yes and provide the login credentials.
- h) (Optional) Expand the Advanced Settings category and change the settings if required.

Under advanced settings, you can configure the following:

• Provide one or more search domains by clicking +Add DNS Search Domain.

After you've entered the information, click the checkmark icon to save it.

• Provide custom App Network and Service Network.

The application overlay network defines the address space used by the application's services running in the Nexus Dashboard. The field is pre-populated with the default 172.17.0.1/16 value.

The services network is an internal network used by the Nexus Dashboard and its processes. The field is pre-populated with the default 100.80.0.0/16 value.

If you have checked the **Enable IPv6** option earlier, you can also define the IPv6 subnets for the App and Service networks.

Application and Services networks are described in the Prerequisites and Guidelines section earlier in this document.

- i) Click Next to continue.
 - **Note** If your node has only an IPv4 management address but you have checked **Enabled IPv6** and provided an IPv6 NTP server address, ensure that the NTP address is correct and click **Confirm** to proceed to the next screen where you will provide the nodes' IPv6 addresses.



Step 17 In the **Node Details** screen, update the current 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 provide the Data network information for the node before you can proceed with adding the other primary nodes and creating the cluster.

Cluster Bringup Node Details Cluster Details Provide the necessary node details to set up Nexus Dashboard and bring up the user interface. Node Details Site Fabric 0/1 Mgmt 0/1 3 Confirmation Site Data Network Mgmt 0/1 Management Network Fabric 0/1 Mgmt 0/1 Fabric 0/1 Site Data Network Serial Number Name Management Network IPv4/mask: 172.23.141.129/21 D52C57566031 IPv4/mask IPv4 Gateway: 172.23.136.1 IPv6/mask: -IPv4 Gateway IPv6/mask: IPv6 Gateway: -IPv6 Gateway: VLAN: Add Node

- a) Click the Edit button next to the first node.
- b) Provide the Name for the node.

The node's Serial Number and the Management Network information are automatically populated.

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

c) 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, 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 IPv4/IPv6 stack.

d) (Optional) If required, Enable BGP for the data network.

BGP configuration is required for the Persistent IPs feature used by some services, such as Nexus Dashboard Insights with NDFC fabrics. This feature is described in more detail in Prerequisites and Guidelines 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.

When you 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.
- e) Click **Update** to save the changes.

Step 18 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.

9			
D	eployment Details		
	Management IP Address * 🛈		
	172.23.141.130		
	Username *		
	rescue-user		
	Password *		
		Validate	
G	eneral		
	Name *		
	nd-node2		
	Serial Number •		
	0274EC65BC40		
N	lanagement Network 🕠		
	IPv4 Address/Mask *		
	172.23.141.130/21		
	IPv4 Gateway *		
	172.23.136.1		
	IPv6 Address/Mask		
	IPv6 Gateway		
D	ata Network 🕕		
	IPv4 Address/Mask ∗		
	172.31.140.70/21		
	IPv4 Gateway *		
	172.31.136.1		
d	IPv6 Address/Mask		
	IPv6 Gateway		
	VLAN ①		
e	Enable BGP		

- 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.

After network connectivity is validated, you can provide the other required information for the node.

c) Provide the Name for the node.

The node's **Serial Number** and the **Management Network** information are automatically populated during the management network information validation in the previous step.

d) 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, 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 IPv4/IPv6 stack.

e) (Optional) If required, Enable BGP for the data network.

BGP configuration is required for the Persistent IPs feature used by some services, such as Nexus Dashboard Insights with NDFC fabrics. This feature is described in more detail in Prerequisites and Guidelines 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.

When you 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 2.2.2.2

- BGP Peer Details, which includes the peer's IPv4 or IPv6 address and peer's ASN.
- f) Click **Add** to save the changes.
- **Step 19** Repeat the previous step to add the 3rd node.

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

Step 20 In the **Node Details** page, click **Next** to continue.

After you have provided the management and data network information for all nodes, you can proceed to the final **Confirmation** screen.

L

2 Node Details	Site		set up Nexus Dash	Fabric 0/1	Mgmt 0/1			
	Site	L2/L3	Data Network	Fabric 0/1	Mgmt 0/1	Managemen	Network	MN
	Site			Fabric 0/1	Mgmt 0/1			
	Serial Number	Name	Managemen	it Network	Data Network			
	D52C57566031	nd-node1			IPv4/mask: 172. IPv4 Gateway: ' IPv6/mask: - IPv6 Gateway: · VLAN: -	72.31.136.1	/	1
	0274EC65BC40	nd-node2			IPv4/mask: 172. IPv4 Gateway: ' IPv6/mask: - IPv6 Gateway: - VLAN: -	72.31.136.1	/	Î
	B244B532BA5D	nd-node3			IPv4/mask: 172. IPv4 Gateway: ' IPv6/mask: - IPv6 Gateway: - VLAN: -	72.31.136.1	/	Î

Step 21 In the **Confirmation** screen, review and verify the configuration information and click **Configure** to create 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 22 Note

Step 23 Verify that the cluster is healthy.

It may take up to 30 minutes for the cluster to form and all the services to start.

After all three nodes are ready, you can log in to any one node via SSH as the rescue-user using the password you provided during node deployment and run the following command to verify cluster health:

a) Verify that the cluster is up and running.

You can check the current status of cluster deployment by logging in to any of the nodes and running the acs health command.

While the cluster is converging, you may see the following outputs:

\$ 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

b) Log in to the Nexus Dashboard GUI.

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 of the Nexus Dashboard cluster.

Note There may be an issue during the bootstrap process on 3-node vND (ESX) clusters which can cause the 'acs health' command to show the following error: 'k8s: services not in desired state - aaamgr, cisco-intersightdc, eventmonitoring, infra-kafka, kafka, mongodb, sm, statscollect'

Contact Cisco TAC and open a case referring to open Bug ID CSCwf65557 requesting root access to run the workaround command on each node.

Step 24 Configure the **Network Scale** parameters for your cluster.

This is described in the **Infrastructure Management** > **Cluster Configuration** section of the *Cisco Nexus Dashboard User Guide*, which is also available directly from your Nexus Dashboard's Help Center.