Cisco HyperFlex Systems Installation Guide for Microsoft Hyper-V, Release 4.5

First Published: 2021-01-06

Last Modified: 2023-10-18

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Overview

Introduction

This guide provides instructions on how to install and configure *Cisco HyperFlex Systems on Microsoft Hyper-V*.

To install *Cisco HyperFlex Systems on VMware ESXi*, refer to the installation guides available at: https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-installation-guides-list.html

To install *Cisco HyperFlex Systems for Edge (Remote and branch offices)*, refer to the deployment guides available at: https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-installation-and-configuration-guides-list.html

Installation Workflow

The following illustration and table summarize the installation workflow:
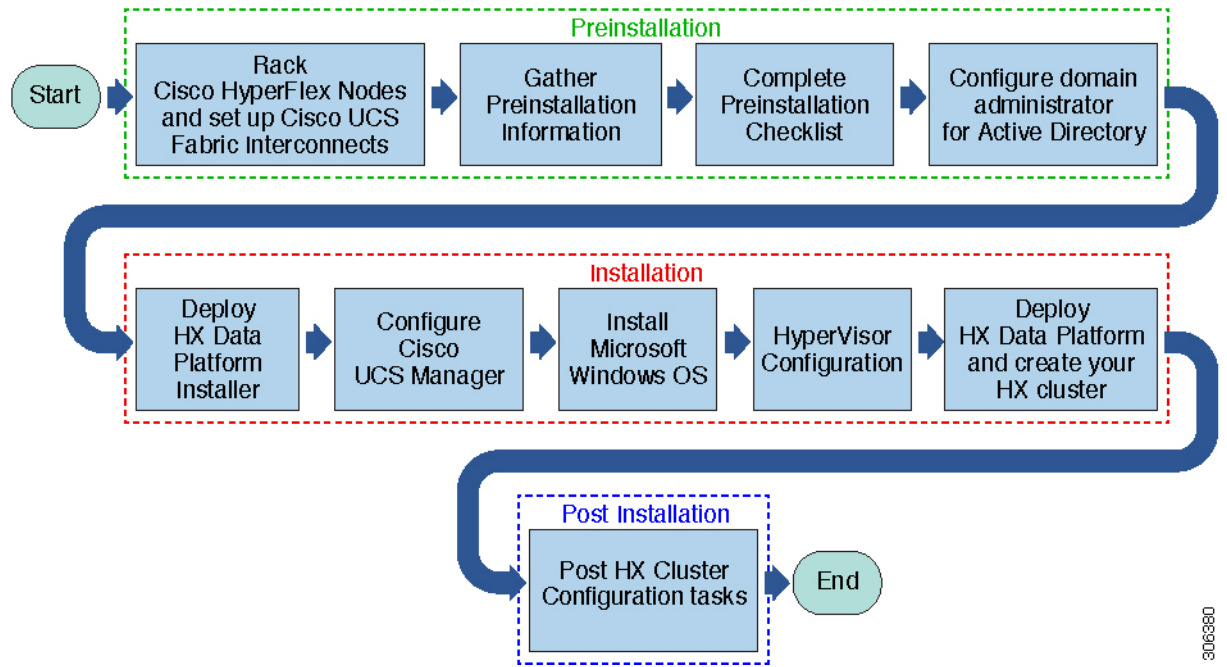
Task	Description	Reference
Preinstallation	Rack HyperFlex nodes, and set up Cisco UCS Fabric Interconnects (FIs).	See: Rack Cisco HyperFlex Nodes, on page 107
	Complete Preinstallation checklist.	Preinstallation Tasks Summary, on page 13
Installation	Deploy HX Data Platform Installer using Microsoft Hyper-V Manager	Deploying HX Data Platform Installer, on page 15
	Configure Cisco UCS Manager using HX Data Platform Installer.	Deploying a Hyper-V Cluster, on page 23
	Install Windows Server and Hyper V, Deploy HX Data Platform and create your initial cluster.	
	Install Windows Server and Hyper V, Deploy HX Data Platform and create your initial cluster.	
Post Installation	Post HX Cluster Configuration tasks.	Cluster Expansion—Converged Nodes, on page 63
		Create the First Datastore, on page 36

CHAPTER 2

Preinstallation Information

Preinstallation Information

To ease your installation, gather the following information that you would require during installation.

Global Information

Cisco UCS Manager Version		DNS Server 1	
NTP Server 1		DNS Server 2	
NTP Server 2		Domain Name (AD)	
Time Zone		SCVMM Host	
SMTP			

Fabric Interconnect Information

Component	IP Address	Hostname	Username	Password	Description
FI-VIP			admin		
FI-A			admin		
FI-B			admin		
IP-Ext-Mgmt: (range)					Must be same subnet as FI mgmt at must at least have 1 ip pr. HX Node
Subnet					For EXT mgmt and FI mgmt

Component	IP Address	Hostname	Username	Password	Description
Default Gateway					For EXT mgmt and FI mgmt
HX Installer					
HX Installer Subnet					
HX Installer Gateway					

HX Installer Information

MAC Pools Prefix (00:25:B5)	

Table 1: HX Nodes Hostnames: Node 1

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 2: HX Nodes Hostnames: Node 2

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 3: HX Nodes Hostnames: Node 3

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 4: HX Nodes Hostnames: Node 4

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 5: HX Nodes Hostnames: Node 5

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 6: HX Nodes Hostnames: Node 6

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 7: HX Nodes Hostnames: Node 7

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 8: HX Nodes Hostnames: Node 8

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 9: Microsoft Cluster Name

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 10: HX Connect UI

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

Table 11: HX File Cluster Name

Field Name	User Entry	Field Name	User Entry
Hostname:		Data Subnet Mask:	
Node Management IP:		Data Default Gateway:	
Management Subnet Mask:		(Optional) Live Migration IP:	
Management Default Gateway:		Live Migration:Subnet	
Node Data IP		Live Migration: Subnet	
HX Controller Data IP		Live Migration Default Gateway:	

VLAN Information

Usage	Name	Default VLAN ID	Chosen VLAN ID
Mgmt	hx-inband-mgmt	3091	
storage-data	hx-storage-data	3092	
Live Migration	hx-livemigrate	3093	
VM Network	vm-network	3094	

Hyper-V Information

HX Cluster Name	
Hyper-V Cluster Name	

Constrained Delegation

distinguished Name	
hxadmin password	

C H A P T E R 3

Preinstallation Checklist

System Requirements

Hardware Requirements

Requirement	Description
Cisco HX Data Platform Servers	Cisco HyperFlex M5 Converged nodes:[1] • All Flash—Cisco HyperFlex HXAF240c M5, HXAF220c M5 • Hybrid—Cisco HyperFlex HX240c M5, HX220c M5, HX240c-M5L
Cisco UCS Fabric Interconnects (FIs)	Cisco UCS Fabric Interconnects (FIs) 6200 and 6300 Starting with 4.0(1b), Cisco UCS Fabric Interconnects (FIs) 6400

[1] Hyper-V support is limited to M5 servers.

Software Requirements for Microsoft Hyper-V - 4.5(x) Releases

The software requirements include verification that you are using compatible versions of Cisco HyperFlex Systems (HX) components and Microsoft Hyper-V (Hyper-V) components.

HyperFlex Software versions

The HX components—Cisco HX Data Platform Installer, Cisco HX Data Platform, and Cisco UCS firmware—are installed on different servers. Verify that each component on each server used with and within the HX Storage Cluster are compatible. For detailed information on installation requirements and steps, see the *Cisco HyperFlex Systems Installation Guide on Microsoft Hyper-V*.

Table 12: Qualified Server Firmware for M5 Servers on Hyper-V

HyperFlex Release	M5 Qualified Server Firmware
4.5(2e)	4.1(3f)
4.5(2d)	4.1(3f)
4.5(2c)	4.1(3f)
4.5(2b)	4.1(3f)
4.5(2a)	4.1(3f)
4.5(1a)	4.1(3f)

Table 13: Supported Microsoft Software versions

Microsoft Component	Version
Windows Operating System (Windows OS)	Windows Server 2016 Datacenter Core & Desktop Experience. **Note** For Windows Server 2016 Datacenter Core and Desktop Experience, the Windows 2016 ISO image should be Update Build Revision (UBR) 1884 at a minimum. Windows Server 2019 Datacenter-Desktop Experience is supported starting from HXDP 4.0.1(a) onwards. **Note** For Windows Server 2019 Desktop Experience, the Windows 2019 ISO image should be Update Build Revision (UBR) 107 at a minimum. Windows Server 2019 Datacenter–Core is **not** supported currently. Also note that the following are currently not supported: OEM activated ISOs and Retail ISOs are **not** supported. Earlier versions of Windows Server such as Windows 2012r2 are **not** supported. Non-English versions of the ISO are **not** supported.
Active Directory	A Windows 2012 or later domain and forest functionality level.

Supported Microsoft License Editions

The Microsoft Windows Server version that is installed on one or more HyperFlex hosts must be licensed as per Microsoft licensing requirements listed on Microsoft Licensing.

Network Services

Network Service	Description
DNS	Microsoft Active Directory and Active Directory integrated DNS are required for the HX Platform and must be outside of the cluster. Standalone DNS server is not supported. Non-Windows DNS servers are not supported.
NTP	Ensure that the time is synchronized between the controller VMs and the hosts. For that purpose, use the Active Directory Time Synchronization Engine. **Attention** Ensure that you use the Active Directory domain name as the NTP server when prompted by HX Data Platform Installer. **Note** Do not nest all of your Active Directory servers in your HyperFlex cluster. Active Directory should reside outside of the HyperFlex cluster so that if the cluster were to encounter issues, you could still authenticate. **Note** If you are using Active Directory as an NTP server, please make sure that the NTP server is setup according to Microsoft best practices. For more information, see Windows Time Service Tools and Settings. Please note that if the NTP server is not set correctly, time sync may not work, and you may need to fix the time sync on the client-side. For more information, see Synchronizing ESXi/ESX time with a Microsoft Domain Controller.

Port Requirements

If your network is behind a firewall, in addition to the standard port requirements, Microsoft recommends ports for the Hyper-V Manager and Hyper-V cluster. Verify that the following firewall ports are open.

Port Number	Protocol	Direction	Usage
80	HTTP/TCP	Inbound	HX Data Platform Installer
443	HTTPS /TCP	Inbound	HX Data Platform Installer
2068	virtual keyboard/Video/ Mouse (vKVM) / TCP	Inbound	hx-ext-mgmt IP pool (one IP per HX node)
22	SSH/TCP	Inbound/Outbound	HX Data Platform Installer
110 (secure POP port is TCP; 995)	POP3/TCP	Inbound/Outbound	
143 (secure IMAP port is TCP; 993)	IMAP4/TCP	Inbound/Outbound	
25	SMTP/TCP	Outbound	Mail Server

Port Number	Protocol	Direction	Usage
53 (external lookups)	DNS/TCP/UDP	Outbound	DNS
123	NTP/UDP	Outbound	NTP
161	SNMP Poll	Inbound	SNMP
162	SNMP Trap	Outbound	SNMP
8089	TCP	Inbound	HX Data Platform Installer
445	SMB 2	Inbound	HX Controller VM
5986	HTTP/TCP	Inbound/Outbound	HX CLI, HX Connect

Note For additional information about ports, see Appendix A of the Cisco HX Data Platform Security Hardening Guide.

Guidelines and Limitations

For best experience with Microsoft Hyper-V installation, you must follow the specific guidelines listed below.

- Use UCSM 4.0.1i with Cisco HyperFlex System installations for Hyper-V, Release 4.5(x).

- Adding HyperFlex nodes to Microsoft System Center 2016 Virtual Machine Manager (Windows VMM 2016) evaluation version will cause errors. Refer to Microsoft help article for a resolution for this issue.

- The following features are NOT supported in the current release:

  - SED Drives

  - Native Replication

  - Cisco HyperFlex Edge

  - Stretched Clusters

  - Intersight-based deployment

  - LAZ and scale beyond 8 nodes

  - HX M4 or M6 Hardware

  - Shared VHDX / VHD Sets

  - Only use the Hyper-V ReadyClone PowerShell script on a cluster node that is not in a paused state.

Preinstallation Tasks Summary

Ensure the following is installed and configured prior to installing and deploying HyperFlex.

Task	Description
Rack HyperFlex nodes including Cisco UCS Fabric Interconnects set up	See Rack Cisco HyperFlex Nodes, on page 107
Verify Cisco UCS Manager version	Ensure that you are using Cisco UCS Manager version 4.1(2a) or later. Refer to the Release Notes for Cisco HX Data Platform for the latest supported releases.
Verify VLANs	Configure the upstream switches to accommodate non-native VLANs. Cisco HX Data Platform Installer sets the VLANs as non-native by default.
Add DNS Records	You must add DNS A and PTR records for your installation. See: Adding DNS Records, on page 13
Configure Domain Administrator for Active Directory	See: Enabling Constrained Delegation, on page 13

Adding DNS Records

Prior to the installation you must add DNS A and PTR records to avoid installation failures.

Device	Description
Hyper-V host	For each host, add an A and PTR record.
Controller node	Controller VM IP address for the A record. This is eth0 on the management IP network.
Windows Failover Cluster	Windows Failover Cluster Object.
HX Connect UI	Cluster management IP address.

Refer to DNS Records, on page 112 section in this guide for the records shown as PowerShell commands to run directly on your environment.

Enabling Constrained Delegation

The steps in this topic must be completed to enable constrained delegation.

Constrained delegation is used to join computers to the Active Directory. You provide constrained delegation information through the HX Data Platform Installer. Constrained delegation uses a service account that is created manually. For example: `hxadmin`. This service account is then used to log into Active Directory, join the computers, and perform authentication from the HyperFlex Storage Controller VM. The Active Directory computer accounts applied to every node in the HyperFlex cluster include:

- Hyper-V host

- HyperFlex Storage Controller VM

- Hyper-V host cluster namespace

- Server Message Block (SMB) Share namespace for the HyperFlex cluster

Step 1   Create an `hxadmin` domain user account as HX service account.

Step 2   Create an Organization Unit (OU) in Active Directory (AD), for example, HyperFlex.

a) Use the Active Directory Users and Computers management tool to create the OU. Select **View** > **Advanced Features** to enable advance features. Select the OU that you created. For example, **HyperFlex** > **Properties** > **Attribute Editor**.

b) Find the distinguished name attribute in the OU, and record the information as this will be required in the Constrained Delegation wizard of the HX Data Platform Installer wizard. The values will look like this: `OU=HyperFlex,DC=contoso,DC=com`.

Use the **Get-ADOrganizationalUnit** cmdlet to get an organizational unit (OU) object or to perform a search to get multiple OUs.

```
Get-ADOrganizationalUnit
[-AuthType <ADAuthType>]
[-Credential <PSCredential>]
-Filter <String>
[-Properties <String[]>]
[-ResultPageSize <Int32>]
[-ResultSetSize <Int32>]
[-SearchBase <String>]
[-SearchScope <ADSearchScope>]
[-Server <String>]
[<CommonParameters>]
```

Step 3   Use Active Directory Users and Computers management tool to grant full permissions for the `hxadmin` user for the newly created OU. Ensure that Advanced features are enabled. If not, go back to Step 2.

a) Select the OU that you created. For example, **HyperFlex** > **Properties** > **Security** > **Advanced**.

b) Click **Change Owner** and choose your `hxadmin` user.

c) Click **Add** in the **Advanced** view.

d) Select the principal and choose the hxadmin user. Then, choose **Full Control**, and click **OK**.

C H A P T E R 4

Installation

• Installation Tasks Summary, on page 15

Installation Tasks Summary

Microsoft Hyper-V Installation consists of the following steps:

Deploying HX Data Platform Installer

Deploy HX Data Platform Installer using **Microsoft Hyper-V Manager** to create a HX Data Platform Installer virtual machine.

Step 1	Locate and download the HX Data Platform Installer `.vhdx` zipped file (for example, `Cisco-HX-Data-Platform-Installer-v4.5.1a-33133-hyperv.vhdx.zip`) from the Cisco Software Downloads site.
Step 2	Extract the zipped folder to your local computer and copy the `.vhdx` file to the Hyper-V host where you want to host the HX Data Platform Installer. For example, `\\hyp-v-host01\....\HX-Installer\Cisco-HX-Data-Platform-Installer-v4.5.1a-33133-hyperv.vhdx`
Step 3	In **Hyper-V Manager**, navigate to one of the Hyper-V servers.
Step 4	Select the Hyper-V server, and right click and select **New** > **Create a virtual machine**. The Hyper-V Manager New Virtual Machine Wizard displays.
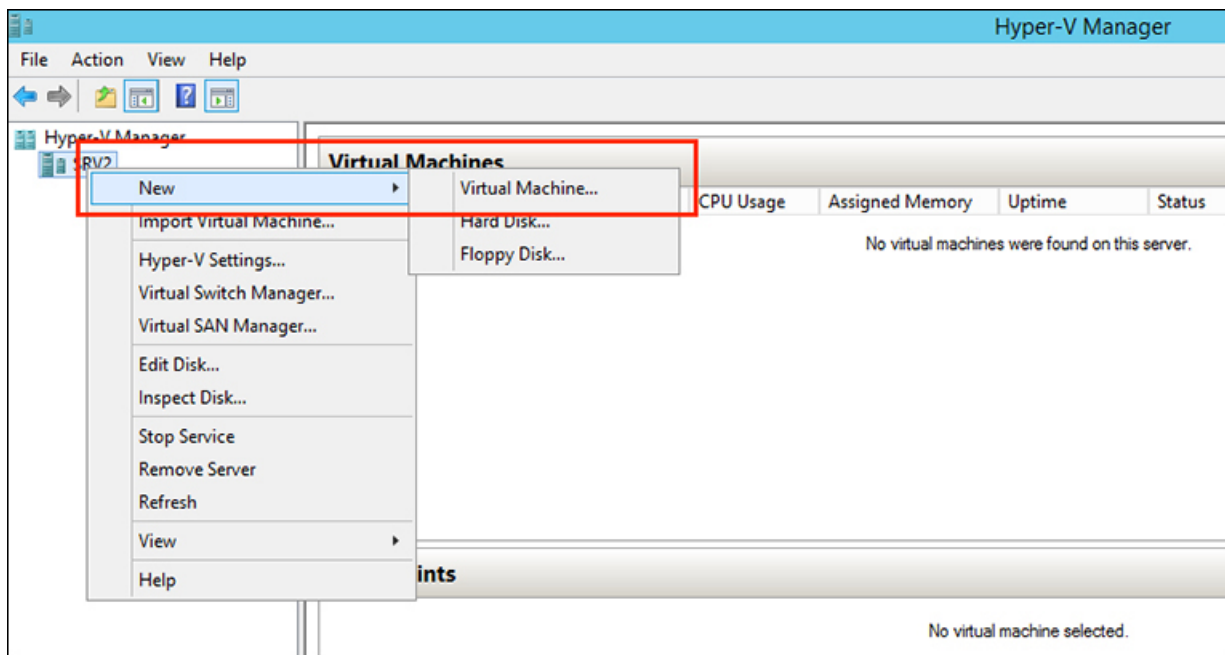
Step 5 In the **Before you Begin** page, click **Next**.
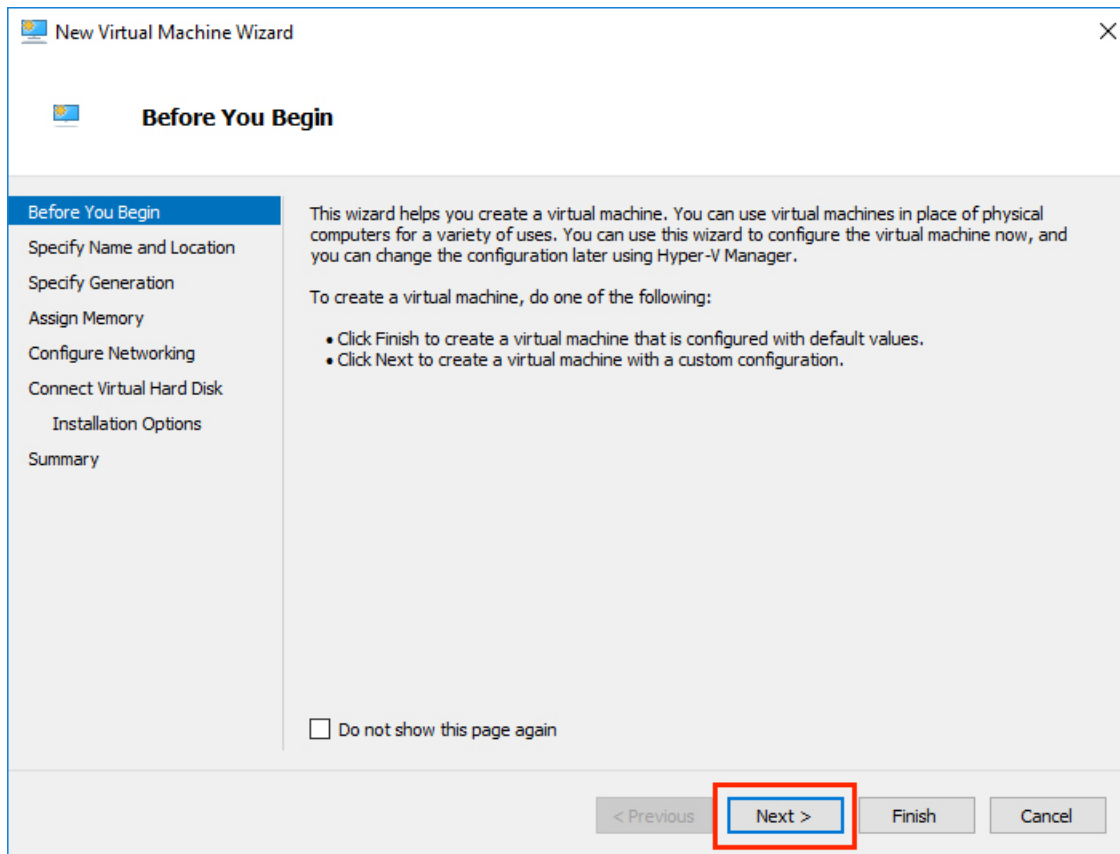
Step 6   In the **Specify Name and Location** page, enter a name and location for the virtual machine where the virtual machine configuration files will be stored. Click **Next**.

**Note**   As a best practice, store the VM together with the `.vhdx` file.
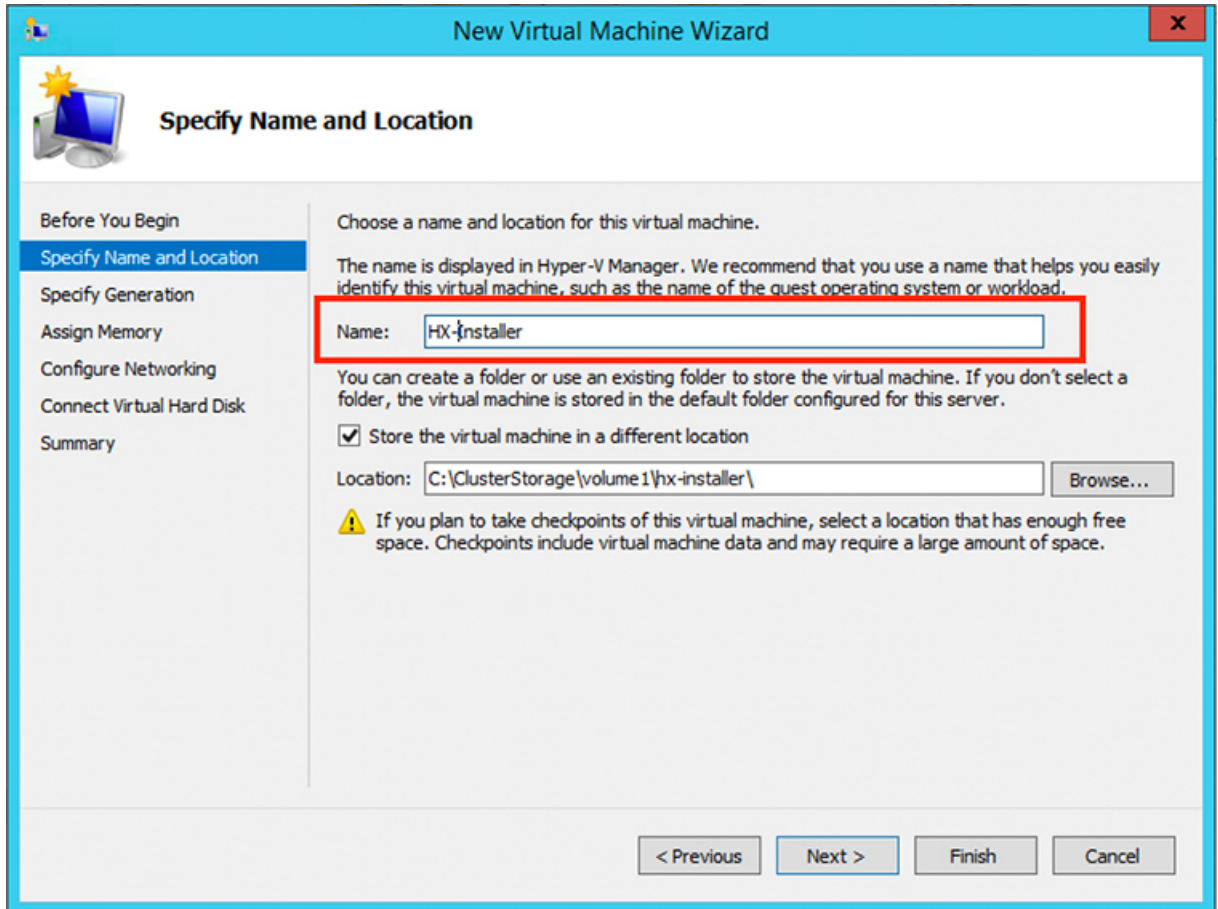
Step 7   In the **Specify Generation** page, select **Generation 1**. Click **Next**. If you select Generation 2, the VM may not boot.
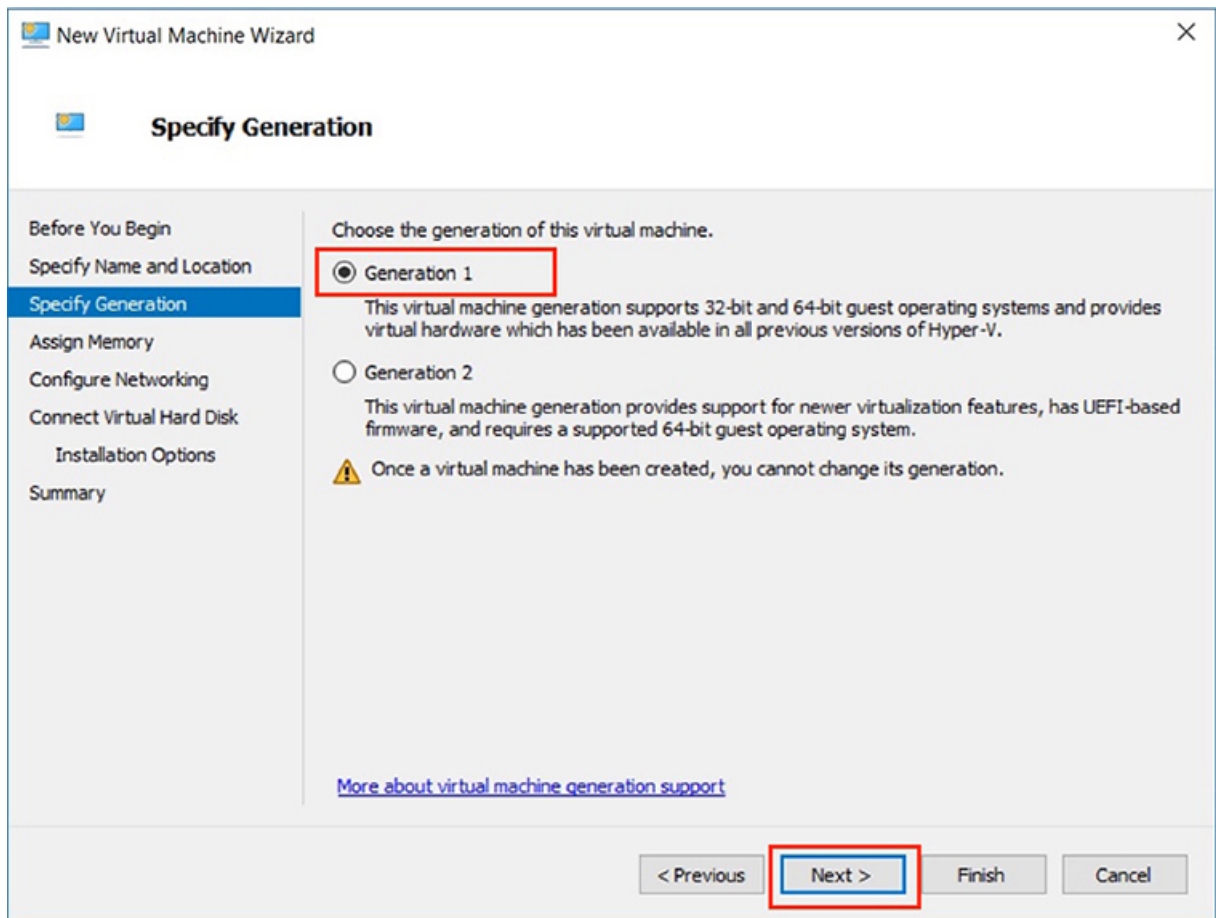
Step 8   In the **Assign Memory** page, set the start up memory value to `4096 MB`. Click **Next**.
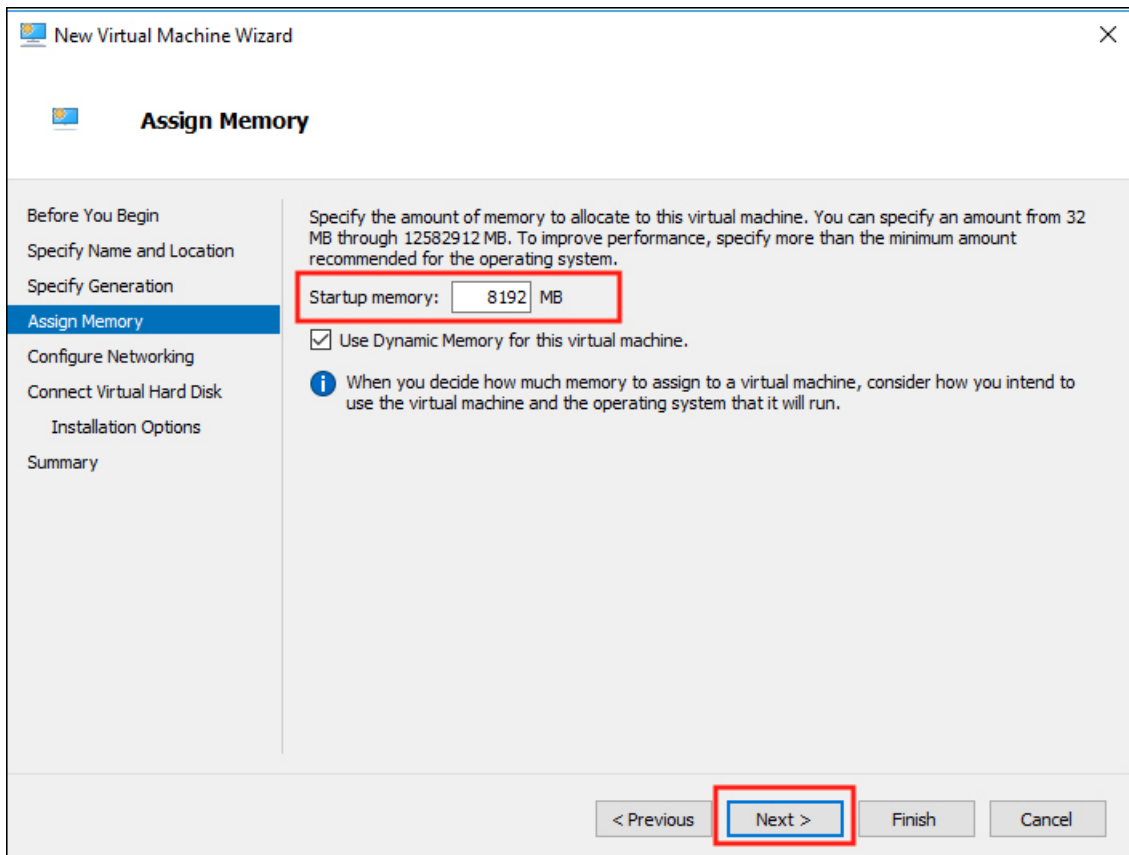
Step 9 In the **Configure Networking** page, select a network connection for the virtual machine to use from a list of existing virtual switches. Click **Next**.
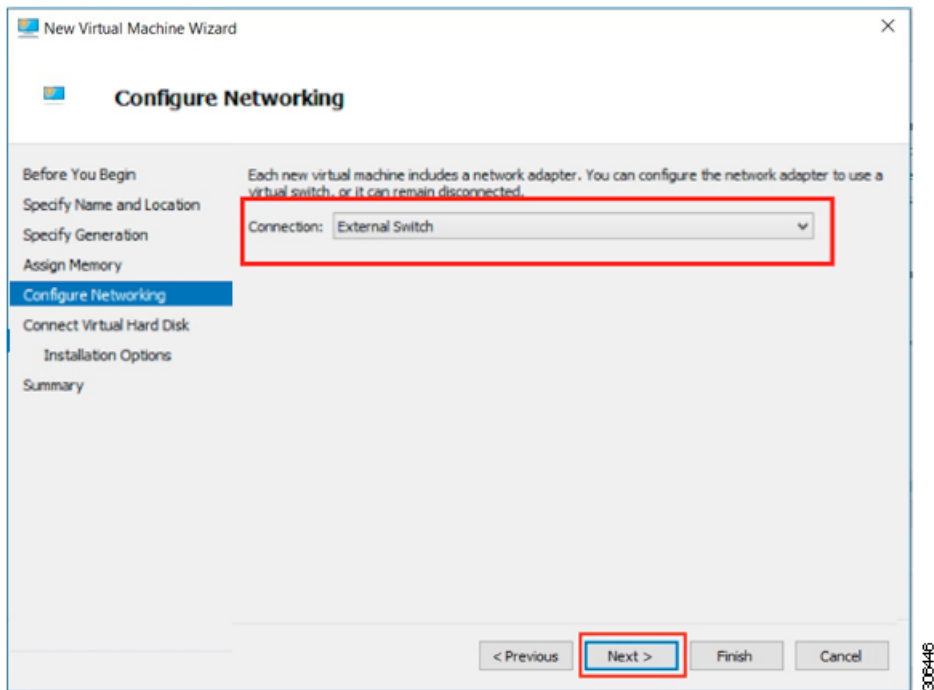
Step 10   In the **Connect Virtual Hard Disk** page, select **Use an existing virtual hard disk**, and browse to the folder on your Hyper-V host that contains the `.vhdx` file. Click **Next**.
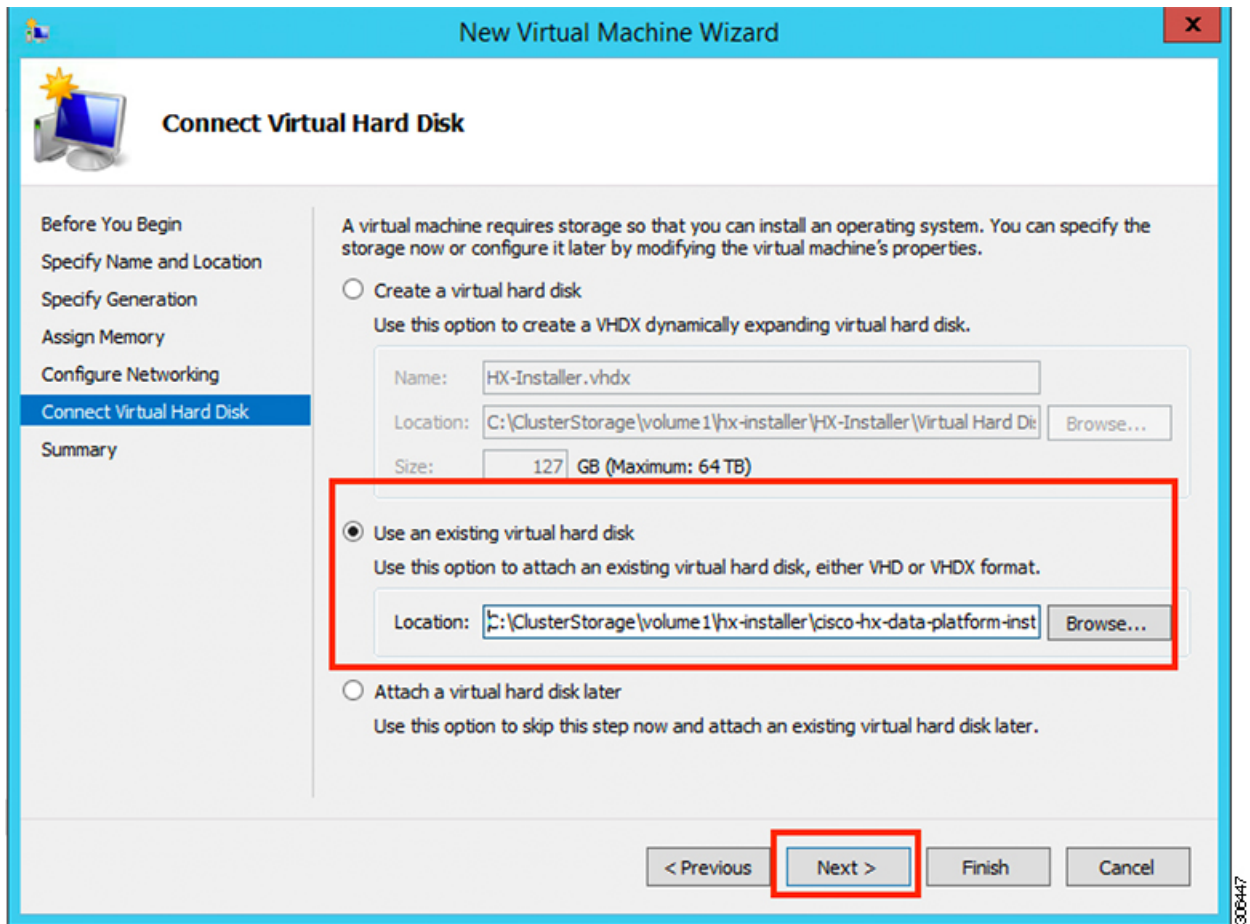
Step 11   In the **Summary** page, verify that the list of options displayed are correct. Click **Finish**.
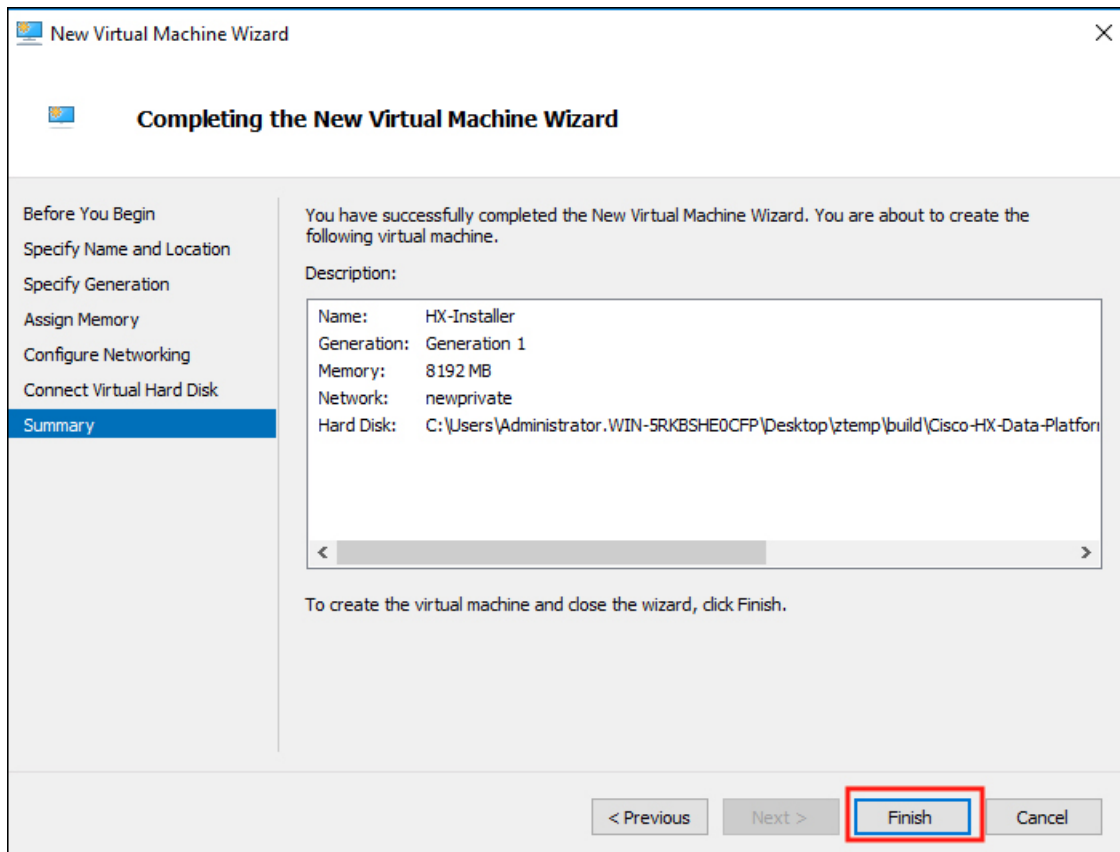
Step 12 After the VM is created, power it ON, and launch the GUI.

a) Right-click on the VM and choose **Connect**.

b) Choose **Action** > **Start (Ctrl+S)**.

c) When the VM is booted, make a note of the URL (IP address of the VM). You will need this information in the following steps in the installation.

d) Log in using the HX Installer default credentials **Cisco123**.

Configuring a Static IP Address on HX Data Platform Installer

During a default installation of the VM, the HX Installer will try and automatically obtain an IP address using DHCP. To ensure that you have the same IP address at every boot, you can assign a static IP address on the VM

Use the following commands to configure your network interface (/etc/network/interfaces) with a static IP address. Make sure you change the relevant settings to suit your network.

> ✎
>
> | **Note** | Network guidelines are:
> |
> | | • Should be able to connect to the Active Directory (AD).
> |
> | | • Use the network to stream OS media from Hyper-V Installer to Hyper-V host for Windows Install.

Step 1   Run the following command: **ifdown eth0**.

> | **Warning** | This step ensures that the interface is down before performing the static IP configuration. Failure to do so could lead to issues during the installation process that may require TAC support.

Step 2   Using your favorite editor, edit the `/etc/network/eth0.interface` file to match your environment. For example, add the following lines in the file:

```
auto eth0 # eth0 interface
iface eth0 inet static # configures static IP for the eth0 interface
metric 100
address XX.XX.XX.XX # Static IP address fr the installer VM
netmask 255.255.0.0 # netmask for the Static IP address
gateway XX.XX.X.X # gateway for the Static IP address
dns-nameservers XX.XX.X.XXX #DNS name servers used by the HX installer
dns-search <DNS_Search_Name>.local # DNS search domain name used by the installer
```

Step 3   Save the file so that the changes take effect.

Step 4   Run the following command: **ifup eth0**

Step 5   Reboot the installer VM.

Deploying a Hyper-V Cluster

After downloading and deploying Cisco HX Data Platform Installer, perform the following procedure to deploy your Hyper-V cluster. The following subtasks are also completed as part of this procedure.

- Cisco UCS Manager configuration

- Hyper-V installation

- Windows OS Installation

- Initial cluster creation

Before you begin

Prior to deploying your Hyper-V cluster, ensure that you have the **Windows 2016 Datacenter edition ISO** or the **Windows Server 2019 Datacenter-Desktop Experience ISO** available.

Step 1   Launch HX Data Platform Installer and log in.

Step 2   In the **Select a Workflow** screen, click **Cluster Creation with HyperFlex (FI)**, complete information for the UCS Manager, Domain Information and Hypervisor Credentials.

Field	Description	Example Value
UCS Manager Credentials		
UCS Manager Host Name	FQDN or the IP address for UCS Manager	eng.fi356.abc.com
UCS Manager User Name	The name for the administrator or a user with UCS Manager administrator privileges.	admin
Password	The password for UCS Manager.	Xyz$1234
Domain Information		
Domain Name	Active Directory domain name that the HyperFlex cluster.	contoso.com
HX Service Account	The HX service account that was created in the preinstallation phase. HX Service account should have full access to the organizational unit used for the cluster. **Note** Verify that the Active Directory policies allow HX service account to have effective permissions to "Write servicePrincipalName" on the computer object created for smb namespace.	hxadmin
Password	Password for the HX service account.	Cisco123
Constrained Delegation		
HX Service Account	Required for Constrained Delegation. The user must be a domain administrator.	sphxadmin
Password	Password for the HX Service Account	
Configure Constrained Delegation now (recommended) or Configure Constrained Delegation later	Select one of the checkboxes. Constrained Delegation is required for VM Live Migration.	

Use the following screenshot as a reference to complete the fields in this page.

The HX Data Platform Installer now connects to UCS Manager and fetches the lists the relevant servers for the HX cluster. The HX Data Platform Installer now validates UCS Firmware.

Click **Continue**.

Step 3 On the **Server Selection** page, view all the associated and unassociated servers under the **Associated** and **Unassociated** tabs respectively.

Under the **Unassociated** tab, you can choose to add any nodes to the existing cluster.

Under the **Associated** tab, you can choose to unassociate servers from the existing cluster.

Use the following screenshot as a reference to complete the fields in this page.

Click **Continue**.

Step 4   On the **UCSM Configuration** page, use the guidance below to complete the VLAN Configuration, Mac Pool, Cisco IMC access management (Out-of-band or in band) sub-sections.

a) **VLAN Configuration**—A minimum of 4 VLANs are required, and each VLAN needs to be on a different IP subnet and extended from the fabric interconnects to the connecting uplink switches. This will ensure that traffic can flow from the Primary Fabric Interconnect (Fabric A) to the Subordinate Fabric Interconnect (Fabric B).

Use the following table and illustration as reference for entering values in this screen.

Example VLAN Name	Example VLAN ID	Usage
hx-inband-mgmt	10	Hyper-V and HyperFlex VM Management.
hx-storage-data	20	HyperFlex Storage traffic
hx-livemigrate	30	Hyper-V Live Migration network
vm-network	100,101	VM guest network

VLAN Configuration

VLAN for Hypervisor and HyperFlex management

VLAN Name — hx-inband-mgmt   VLAN ID

VLAN for HyperFlex storage traffic

VLAN Name — hx-storage-data   VLAN ID

VLAN for VM Live Migration

VLAN Name — hx-livemigrate   VLAN ID

VLAN for VM Network

VLAN Name — vm-network   VLAN ID(s)

Note   The use of VLAN 1 may cause issues with disjoint layer 2.

The `vm-network` can be multiple VLANs added as a comma separated list.

b) **MAC Pool**— Use the following table and illustration to complete the remaining network configuration settings.

Field	Description	Example Value
MAC pool prefix	MAC address pool for the HX cluster, to be configured in UCS Manager by HX Installer. Ensure that the mac address pool is not used anywhere else in your layer 2 environment.	00:25:b5:xx
IP blocks	The range of IP addresses that are used for Out-Of-Band management of the HyperFlex nodes.	10.193.211.124-127
Subnet Mask	The subnet mask for the Out-Of-Band network.	255.255.0.0
Gateway	The gateway address for the Out-Of-Band network.	10.193.0.1
Cisco IMC access management	In-band or Out of band	Out of band

MAC Pool

MAC Pool Prefix

00:25:B5:F3

'hx-ext-mgmt' IP Pool for Cisco IMC

IP Blocks	Subnet Mask	Gateway
10.42.18.100-200	255.255.255.0	10.42.18.1

Cisco IMC access management (Out of band or Inband)

○ In band (recommended) ⓘ   ● Out of band ⓘ

Step 5   If you want to add external storage, use the guidance below:

a) Configure **iSCSI Storage** by completing the following fields:

Field	Description
Enable iSCSI Storage check box	Select to configure iSCSI storage.
VLAN A Name	Name of the VLAN associated with the iSCSI vNIC, on the primary Fabric Interconnect (FI-A).
VLAN A ID	ID of the VLAN associated with the iSCSI vNIC, on the primary Fabric Interconnect (FI-A).
VLAN B Name	Name of the VLAN associated with the iSCSI vNIC, on the subordinate Fabric Interconnect (FI-B).
VLAN B ID	ID of the VLAN associated with the iSCSI vNIC, on the subordinate Fabric Interconnect (FI-A).

b) Configure **FC Storage** by completing the following fields:

Field	Description
Enable FC Storage check box	Select to enable FC Storage.
WWxN Pool	A WWN pool that contains both WW node names and WW port names. For each Fabric Interconnect, a WWxN pool is created for WWPN and WWNN.
VSAN A Name	The name of the VSAN for the primary Fabric Interconnect (FI-A). Default—`hx-ext-storage-fc-a`.

Field	Description
VSAN A ID	The unique identifier assigned to the network for the primary Fabric Interconnect (FI-A).
	Caution Do not enter VSAN IDs that are currently used on the UCS or HyperFlex system. If you enter an existing VSAN ID in the installer which utilizes UCS zoning, zoning will be disabled in your existing environment for that VSAN ID.
VSAN B Name	The name of the VSAN for the subordinate Fabric Interconnect (FI-B).
	Default—`hx-ext-storage-fc-b`.
VSAN B ID	The unique identifier assigned to the network for the subordinate Fabric Interconnect (FI-B).
	Caution Do not enter VSAN IDs that are currently used on the UCS or HyperFlex system. If you enter an existing VSAN ID in the installer which utilizes UCS zoning, zoning will be disabled in your existing environment for that VSAN ID.

Step 6   On the **Hypervisor Configuration** page, complete the following fields.

Field	Description	Example Value
Bare metal configuration		
Install Hypervisor (Hyper-V)	By default, the Install Hypervisor (Hyper-V) checkbox is selected for Windows OS installation on a bare metal node. Click **Browse** to select and upload the ISO file. Alternatively, drag and drop the ISO file into the area.	
Select the operating system you want to install	The operating system to install can be one of the following: • Windows Server 2016 Datacenter (Desktop Experience) • Windows Server 2016 Datacenter (CORE)	
Configure common Hypervisor Settings		
Subnet Mask	Subnet mask for the hypervisor hosts management network	255.255.255.0
Gateway	Default gateway for the hypervisor hosts management network	10.101.251.1
DNS Servers	Comma separated list for the DNS Servers in the AD that the hypervisor hosts are going to be member of.	10.99.2.200,10.992.201
Hypervisor Settings		

Field	Description	Example Value
Static IP address	Management IP address for each host **Note** If you leave the checkbox **Make IP Addresses and Hostnames Sequential** as checked then the installer will automatically fill the rest of the servers sequential from the first.	10.101.251.41
Hostname	Hostname for each host	HX-Hypv-01

Click **Continue**.

Step 7   **HX Data Platform Deployment**

Field	Description	Example Value
Domain Information		
Domain Name	Active Directory Domain that the cluster will be a part of.	contoso.com
HX Service Account	The HX service account that was created in the preinstallation phase. **Important** Verify that the Active Directory policies allow HX service account to have effective permissions to "**Write servicePrincipalName**" on the computer object created for **smb** namespace.	hxadmin
Password	Password for the HX service account.	
Constrained Delegation		
HX Service Account and Password	Required for Constrained Delegation.	
Use HX Service Account	Uses the HX service account for Constrained Delegation. The user must be a domain administrator.	Click checkbox if HX service account is provided.
Configure Constrained Delegation now (recommended) or Configure Constrained Delegation later	Select one of the checkboxes. Constrained Delegation is required for VM Live Migration. To configure Constrained Delegation later, use the procedure described in Configuring a Static IP Address for Live Migration and VM Network, on page 37.	
Advanced Attributes (optional)		

Field	Description	Example Value
Domain Controller	FQDN for the Domain Controller that you want to use specifically for the installation.	dc.contoso.com
Organization Unit	The OU created during the preinstallation phase can be used here Then, the OU will be the home for the HX nodes in the Active Directory.	OU=HyperFlex, DC=contoso, DC=com
Hypervisor Credentials		
Hypervisor Local Administrator User Name	Local administrator username on the Hyper-V hosts	Default username/password: administrator/Cisco123 **Important** Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.

Click **Continue**.

Step 8 On the **IP Addresses** page, use the table below to complete the fields in this page.

Field	Description	Example Value
Cisco HX Cluster		
Cluster Name (SMB Access Point)	The cluster name to be used as the FQDN for the datastores.	HX-EAP-01
Replication Factor	Select the number of redundant data replicas across the HX storage cluster. Options are 2 or 3. This cannot be changed after the cluster is created. 3 is recommended for production workloads.	3 (Default Value)
Failover Cluster Name	The name used for the Windows Failover Cluster.	
Controller VM		
Create Admin Password		
Confirm Administrator Password		
System Services		
DNS Servers	Comma separated lists of DNS Servers.	10.99.2.200, 10.99.2.201

Field	Description	Example Value
NTP Servers	The controller VMs needs must be in sync with Windows Active Directory, therefore you must point to your AD domain controllers for time synchronization.	dc1.contoso.com, dc2.contoso.com
DNS Domain Name	The domain name for the Active Directory.	contoso.com
Timezone	The timezone that you want the HX controllers to report in.	
Auto Support		
Enable Connected Services	Auto Support to ship telemetry data of the HX cluster to Cisco Support.	
Send Service ticket to	Email address or alias to receive a copy of the ticket sent to Cisco.	*email_address*
Advance Networking		
Management VLAN tag	VLAN used for the Management Network. This must be the same as used earlier in the installation process for the management network.	
Data VLAN tag	VLAN used for the Management network. This must be the same as used earlier in the installation process for the data network.	
Advanced Configuration		
Enable Jumbo Frames on Data network	Sets the MTU size for the storage data network on the host vSwitches and vNICs, and each storage controller VM. The default value is 9000. Ensure that jumbo frames run on the links connected to the storage VMs.	
Disk Partitions	Removes all existing data and partitions from all nodes added to the storage cluster. You must backup any data that should be retained. Select this option to delete existing data and partitions. This is for manually prepared servers. Do not select this option for factory prepared systems. The disk partitions on factory prepared systems are properly configured.	
VDI	Configures for VDI only environments. To change the VDI settings after the storage cluster is created, shutdown or move the resources, make changes, and restart the cluster.	
Hypervisor Settings		

Field	Description	Example Value
Primary DNS suffix	Completed in earlier steps in the installation.	
Additional DNS suffixes	Complete this field if you need more suffices appended on your Hyper-V hosts.	

Refer to the illustration below as a sample entries for the various fields in this page.

Step 9 Click **Start** to begin the deployment. The **Progress** page displays the progress of the configuration tasks: Start, Deploy Validation, Deploy, Create Validation, Cluster Creation.
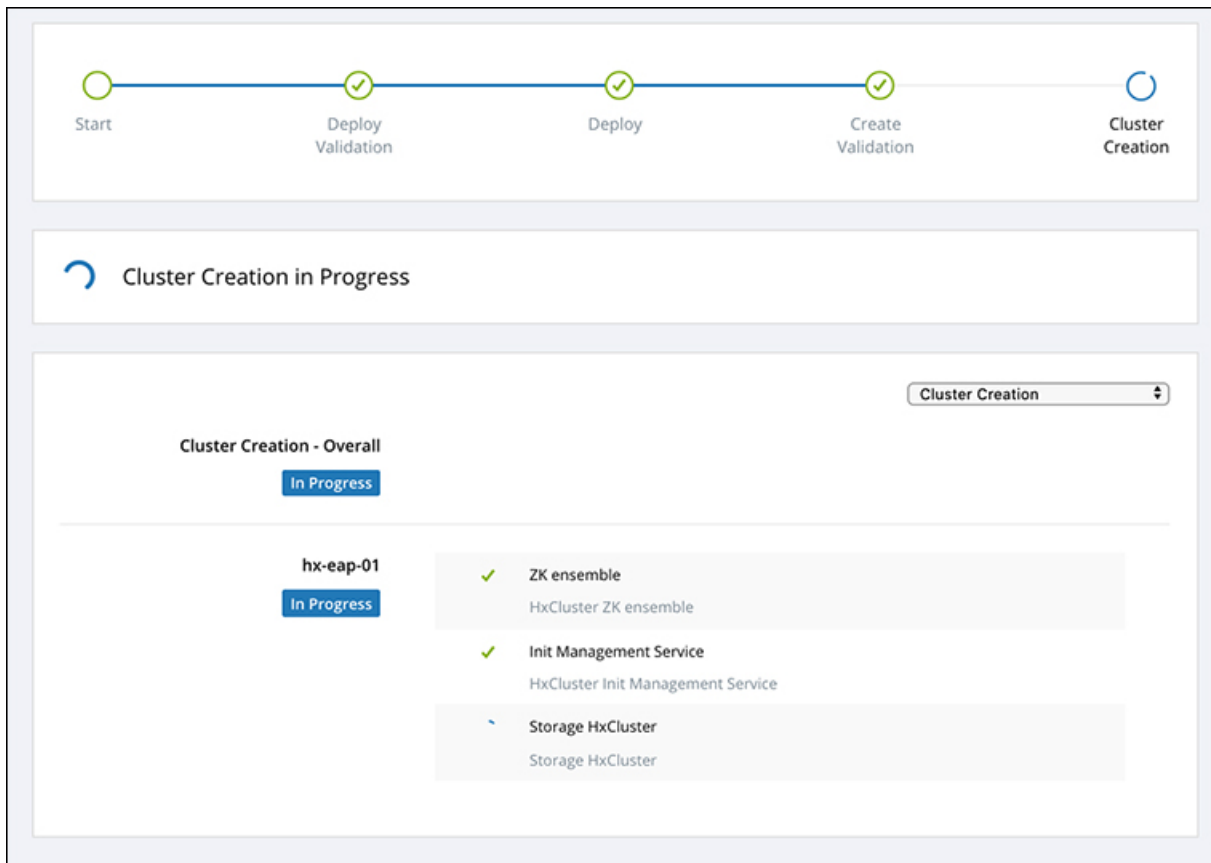
Best Practices

Common best practices for Cisco HyperFlex with Microsoft Hyper-V installations are listed below.

- Do not perform updates to your Windows system out of band with regards to Cisco HyperFlex.

- If you are using Group Policy settings to configure the behavior of Windows Update (WU), ensure that they do not override the default settings configured by Cisco HyperFlex. Do not configure policies that specify downloading updates automatically and installing them on a schedule.

Note   By default, Cisco HyperFlex disables automatic updates. The AU Options value is set to **2**: Notify of download and installation. For more information about Windows update settings, see Manage additional Windows Update settings.

Post Installation

- Post Installation Tasks Summary, on page 35

Post Installation Tasks Summary

After successful cluster configuration, perform the following additional post installation tasks to ensure that the cluster is ready to serve VMs.

Task	Reference
Create the First Datastore	Create the First Datastore, on page 36
Assign a static IP address for Live Migration and VM Network	Configuring a Static IP Address for Live Migration and VM Network, on page 37
(Optional) Constrained Delegation	(Optional) Post Installation Constrained Delegation, on page 38
Configure Local Default Paths	Configure Local Default Paths, on page 39
Configure File Share Witness	Configuring a File Share Witness, on page 40
Checking the Windows Version on the Hyper-V Host	Checking the Windows Version on the Hyper-V Host, on page 46
Validate Failover Cluster Manager	Validate Failover Cluster Manager, on page 46
Testing Upstream Failover	Testing Upstream Failover for Storage Data Network
Deploying VMs on a Hyper-V cluster	Deploying VMs on a Hyper-V cluster, on page 48
Configuring HyperFlex Share to SCVMM	Configuring HyperFlex Share to SCVMM, on page 55
Re-enabling Windows Defender	Re-enabling Windows Defender, on page 57
VM Migration between standalone Hyper-V and HX Hyper-V hosts.	VM Migration between Hosts, on page 57

Create the First Datastore

Before you begin using the cluster, you must create a datastore. The datastore can be created in HX Connect UI.
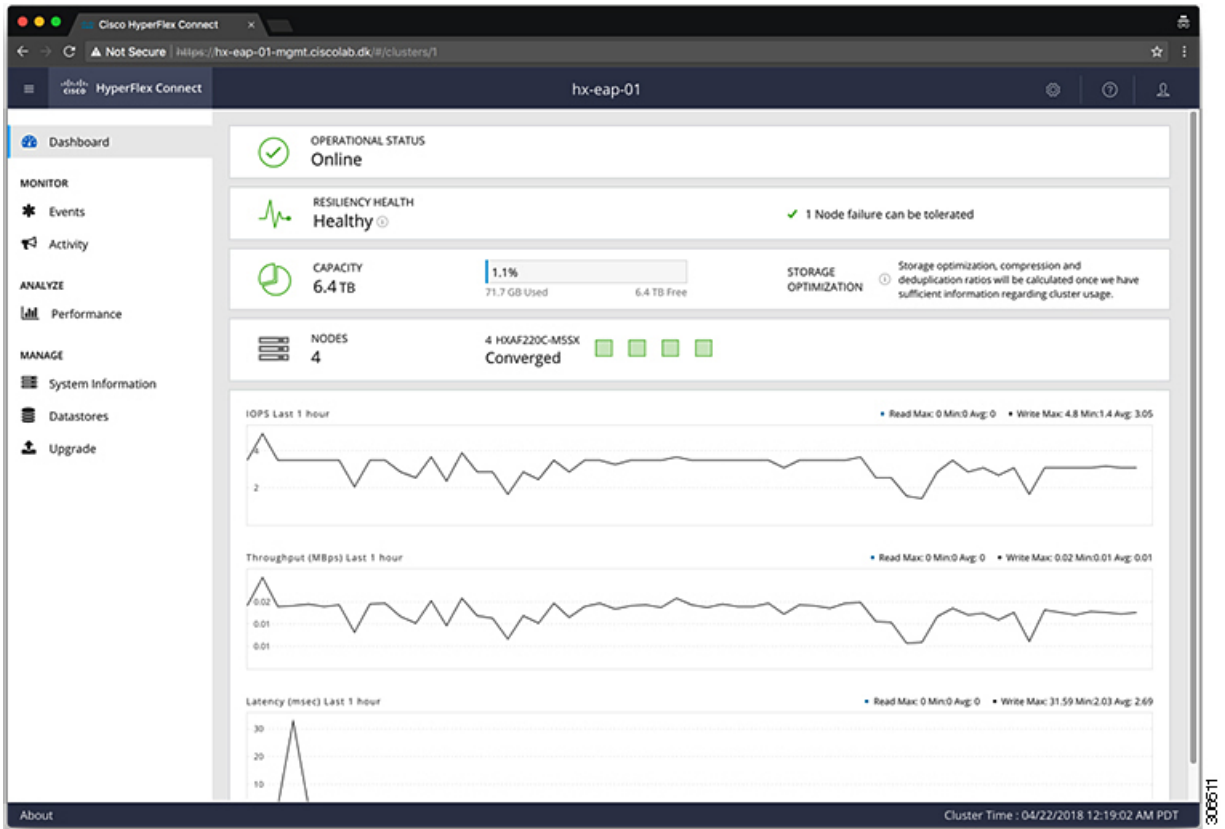
Step 1 Launch HX Connect UI from a browser of your choice from *https://Cluster_IP/* or *https://FQDN*.
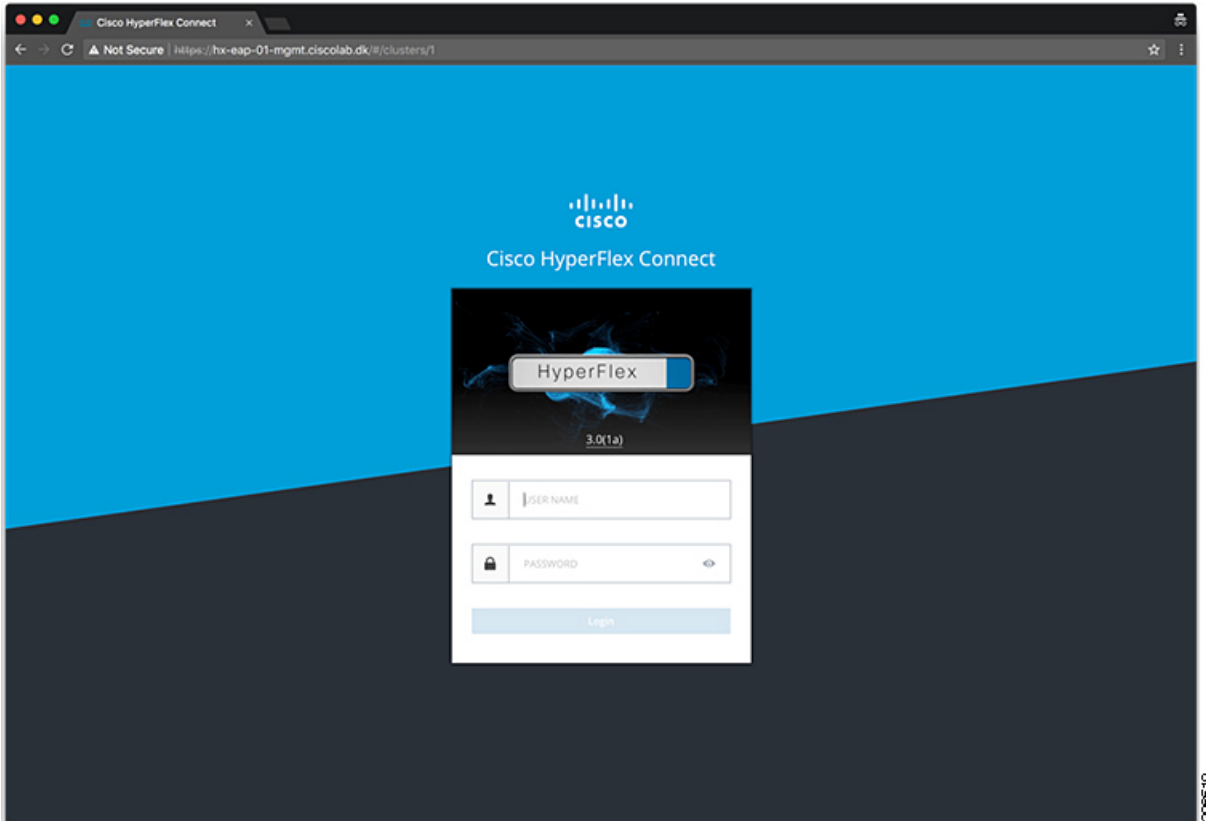
Step 2 Log in with the following credentials:

- **Username—hxadmin**

- **Password**—Use the password set during cluster installation.

Step 3 In the Navigation pane, select **Datastores**.

Step 4   In the Work pane, click **Create Datastore**.

Step 5   In the **Create Datastore** dialog box, complete the following fields:

Field	Description
Datastore Name	Enter a name for the datastore. Cisco recommends that you use all lower case characters for the datastore name.
Size	Select the size for the datastore.
Block Size	Select the block size for the datastore.

Note   Cisco recommends 8K block size and as few datastores as possible to ensure the best performance.

Configuring a Static IP Address for Live Migration and VM Network

Log into each Hyper-V node and execute the following commands in Power Shell to assign a static IP address for Live Migration and VM Network.

| #	Command	Purpose

1	`New-NetIPAddress -ifAlias`
	`"vSwitch-hx-livemigration" -IPAddress`
	`192.168.73.21 -PrefixLength 24`
		Assigns a static IP address to the Live Migration network.

2	`New-NetIPAddress -ifAlias`
	`"vswitch-hx-vm-network" -IPAddress`
	`192.168.74.21 -PrefixLength 24`
		Assigns a static IP address to the VM network.

(Optional) Post Installation Constrained Delegation

⚠️

Attention   This step must be performed only if Constrained Delegation was not configured during initial installation. It is recommended that you perform this procedure using the HX Installer and not as part of post-installation.

Constrained Delegation gives granular control over impersonation. When the remote management requests are made to the Hyper-V hosts, it needs to make those requests to the storage on behalf of the caller. This is allowed if that host is trusted for delegation for the CIFS service principal of HX Storage.

Constrained Delegation requires that the option for the security setting **User Account Control: Behavior of the elevation prompt for Administrators in Admin Approval Mode** is set to **Elevate without Prompting**. This will prevent the global AD policy from overriding policy on HX OU.

Perform the following procedure *on each Hyper-V host in the HX Cluster* to configure using **Windows Active Directory Users and Computers**.

Step 1   Click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.

Step 2   Expand domain, and then expand the Computers folder.

Step 3   In the right pane, right-click on the computer name (for example, HX-Properties), and then click **Properties**.

Step 4   Click on the **Delegation** tab.

Step 5   Select **Trust this computer for delegation to specified services only**.

Step 6   Ensure that **Use any authentication protocol** is selected.

Step 7   Click **Add**. In the **Add Services** dialog box, click **Users or Computers**, and then browse or type the name of the Service Type (such as CIFS). Click OK. The following illustration can be used as an example.
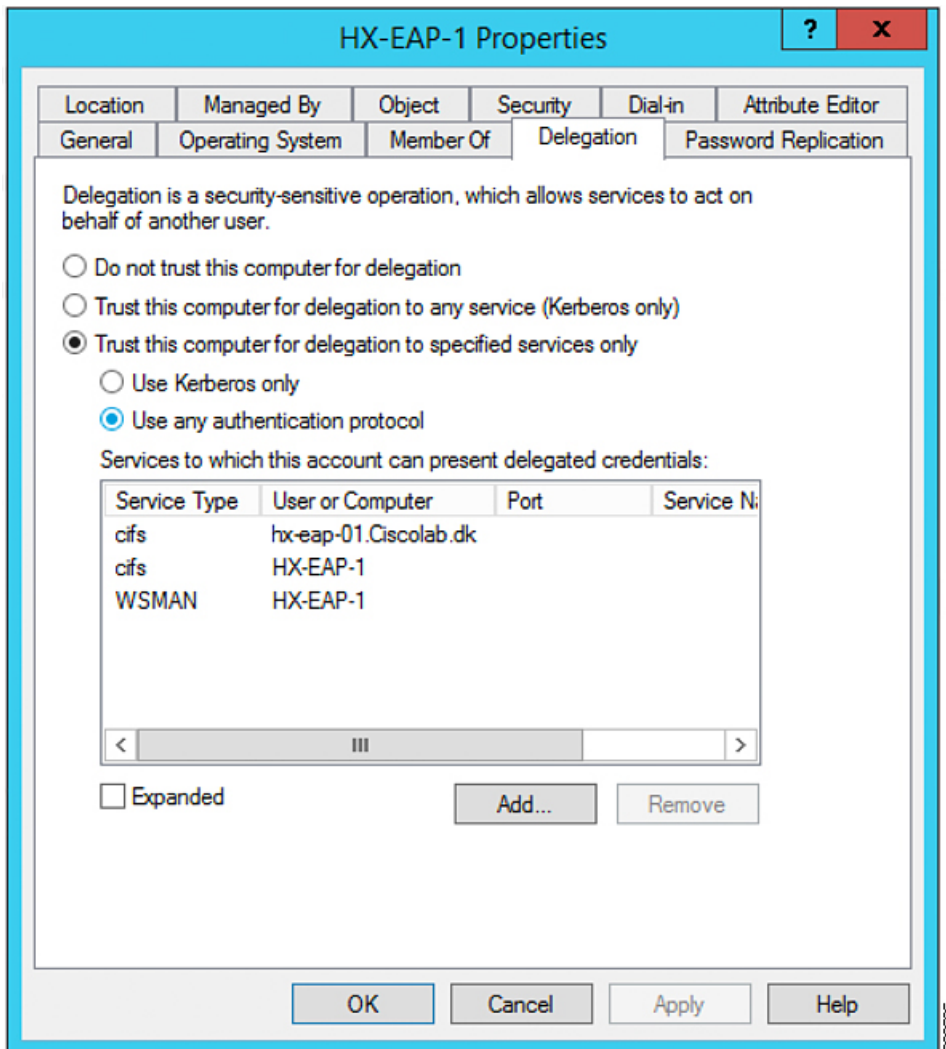
Step 8 Repeat these steps for all nodes.

Configure Local Default Paths

Configure the default local path for the VMs to ensure that they will be on the HX cluster datastore.

Run the following commands in PowerShell:

```
$Creds = Get-Credential -Message "User Credentials" -UserName <<current logon username>>
$hosts = ("hostname1","hostname2","hostname3","hostname4")
Invoke-Command -ComputerName $hosts -Credential $Creds -ScriptBlock {Set-VMHost
-VirtualHardDiskPath
"\\HX-EAP-01.ciscolab.dk\DS1_8K" -VirtualMachinePath "\\HX-EAP-01.ciscolab.dk\DS1_8K"}
```

✎

Note   The username should either be a Domain admin account or the HX service account. The local Administrator on the Hyper-V host will not work.

✎

Note   Remember to change the variables to suit your environment.

Configuring a File Share Witness

As a Microsoft best practice, ensure that you configure a Quorum witness datastore. Use the following procedure to configure a File Share Witness using **Failover Cluster Manager** (FCM). A File Share Witness ensures high availability of the failover cluster when nodes on the network fail. Specifically, a File Share Witness is needed to maintain a failover cluster quorum, which is designed to prevent split-brain scenarios that may happen when a partition in the network and subsets of nodes cannot communicate with each other. For more information, see "Understanding cluster and pool quorum".

✎

Note   In an HX cluster, the storage is designed to be highly available and no host should lose access to the storage. In the event that one host does stop writing to the datastore, Microsoft's storage resiliency behavior kicks in. The host repeatedly retries to establish a connection with the storage for 30 mins by default. During this time, the user VMs may be paused. If it cannot connect after 30 mins, the VM moves to a 'stopped' state.

The following procedure describes how to configure a File Share Witness for Microsoft Windows 2016. If you are deploying Microsoft Windows 2019, do not use HyperFlex Share or any other file share as a witness. Microsoft has identified a defect in Windows 2019, which will be resolved in a subsequent patch release. Until such time, you must configure the Microsoft Windows 2019 Failover cluster without any witness.

✎

Note   • If you are using Microsoft Windows 2019 and planning to use any file share (including HX share) as a file share witness, you must install the https://support.microsoft.com/en-us/help/4497934 patch before configuring.

    • If you do not want to use file share as a quorum witness, then you can use other quorum methods described by Microsoft Windows 2019.

Before you begin

Microsoft released a security patch on November 12, 2019 that applies to Windows 2019. If you are running Windows 2019, upgrade your Hyper-V hosts with the patch at the path level, before using the following procedure to configure a file share witness. For more information, see the Microsoft article "November 12, 2019—KB4523205 (OS Build 17763.864)".
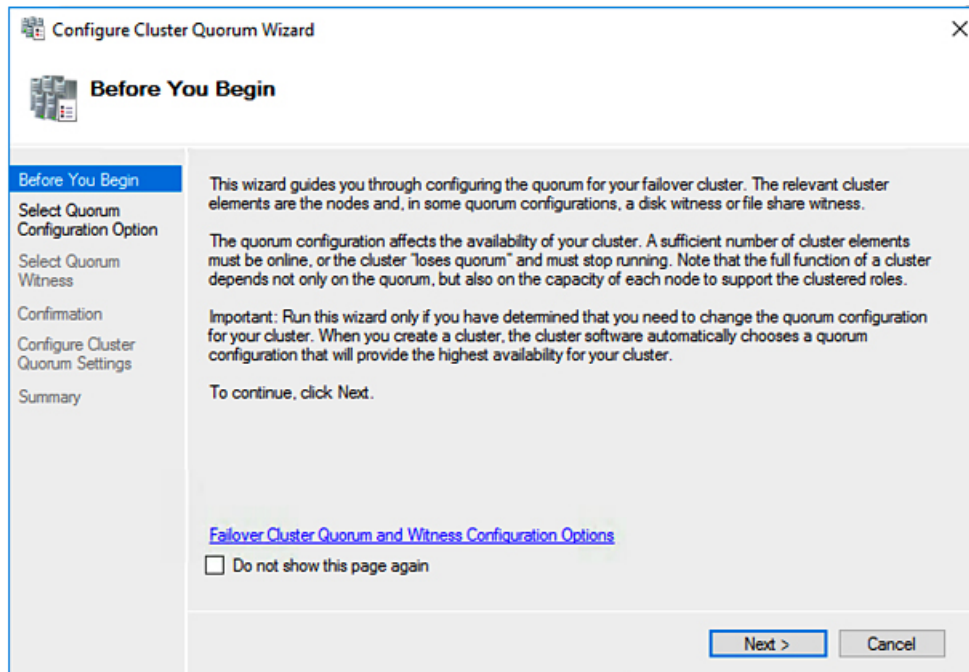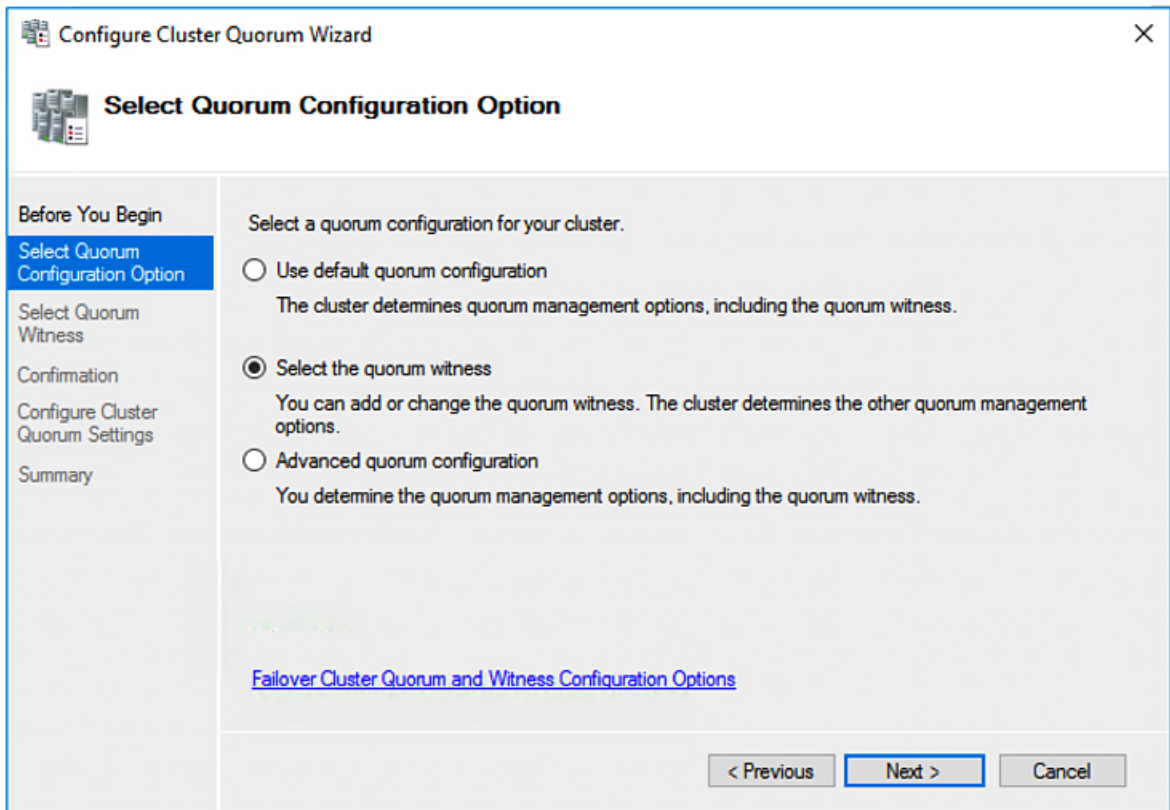
Step 1   Launch FCM.

Step 2   In the navigation pane, select your cluster. Then, in the **Actions** pane, select **More Actions** > **Configure Cluster Quorum Settings...**.
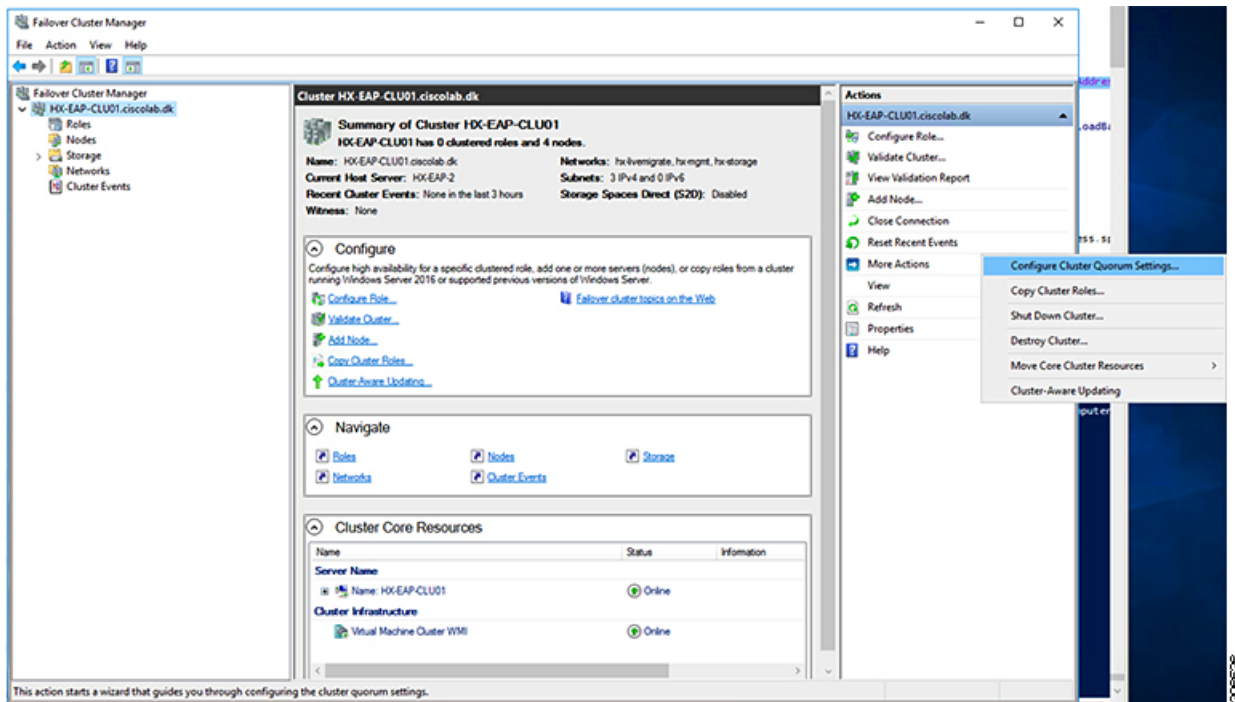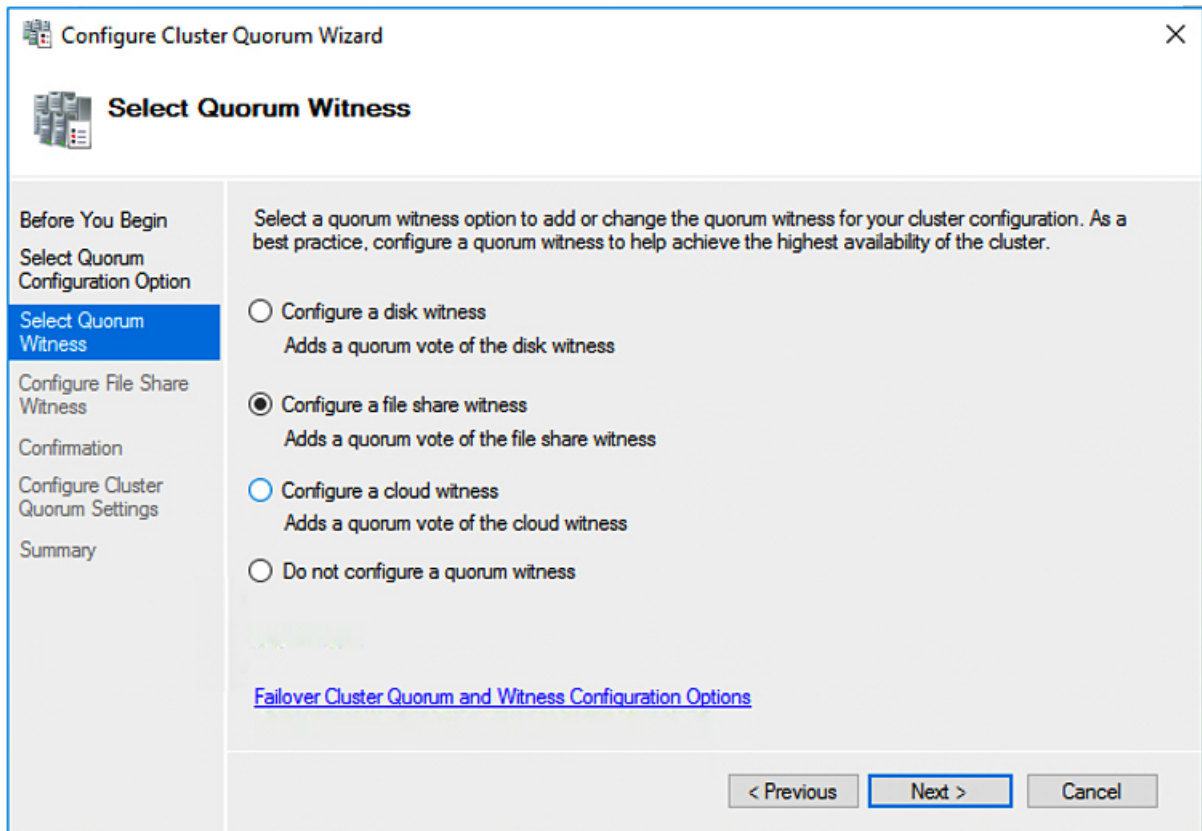

Step 3   The **Configure Cluster Quorum** wizard is launched. Click **Next**.
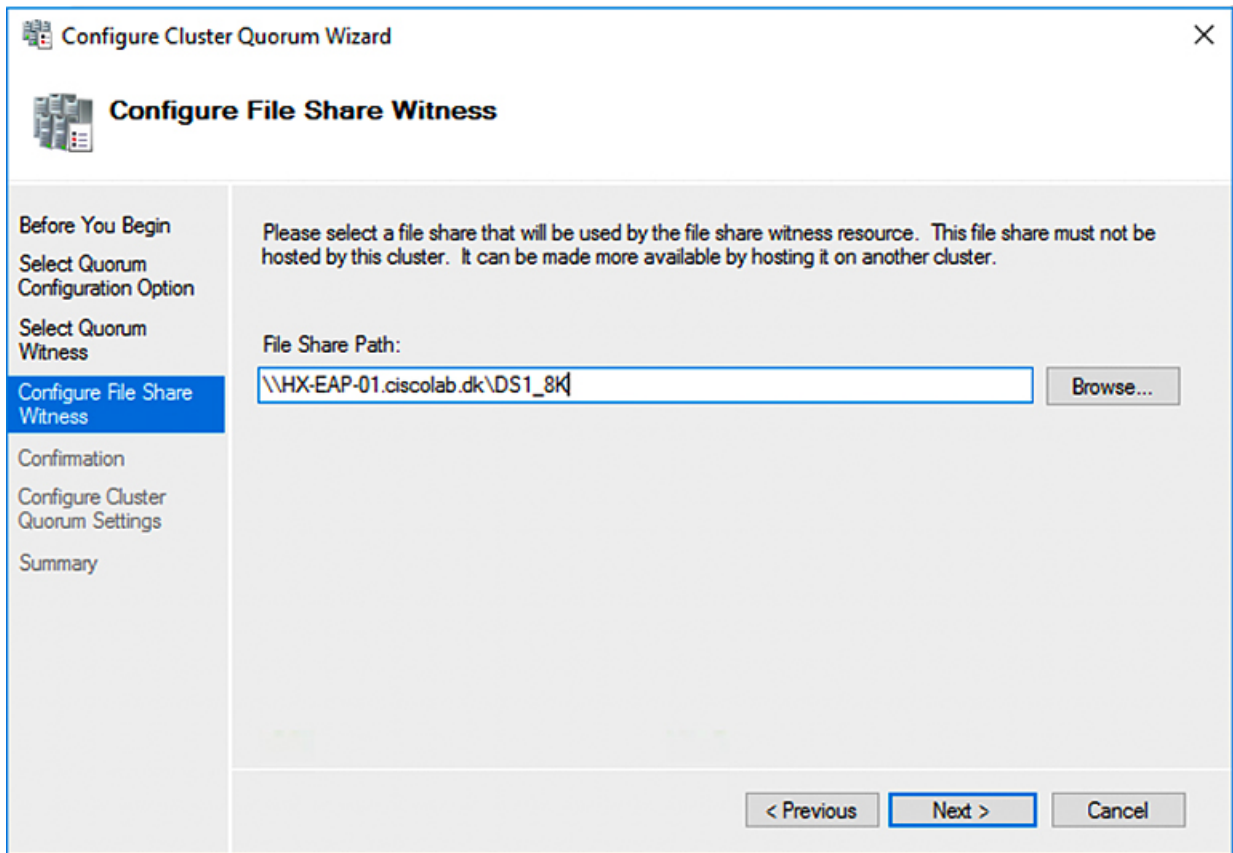

Step 4   In the **Select Quorum Configuration Option** screen, choose **Select the quorum witness**. Click **Next**.
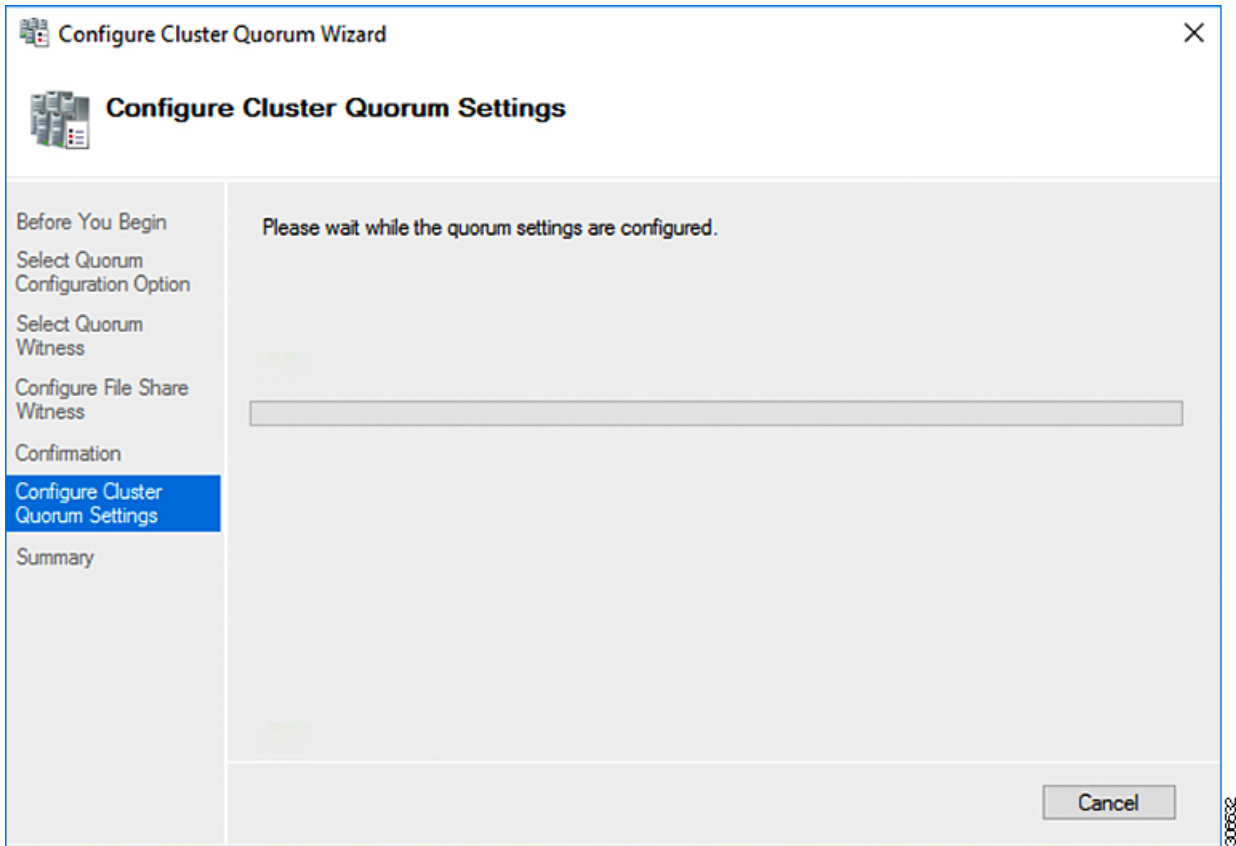
Step 5   In the **Select Quorum Witness** screen, choose **Configure a file share witness**. Click **Next**.

Step 6   In the **Configure File Share Witness** screen, specify the path to the File Share. Click **Next**.

Step 7 In the **Confirmation** screen, click **Next**.

Step 8 In the **Summary** screen, click **Finish** to close the wizard.

Step 9 Alternatively, you can configure a file share witness using Windows PowerShell.

a) Open a Windows PowerShell console as an administrator.

b) Type **Set-ClusterQuorum -FileShareWitness <File Share Witness Path>**

c) You should now see the File Share Witness configured for your cluster. When you navigate to your File Share Witness share you will see a folder created for your cluster.
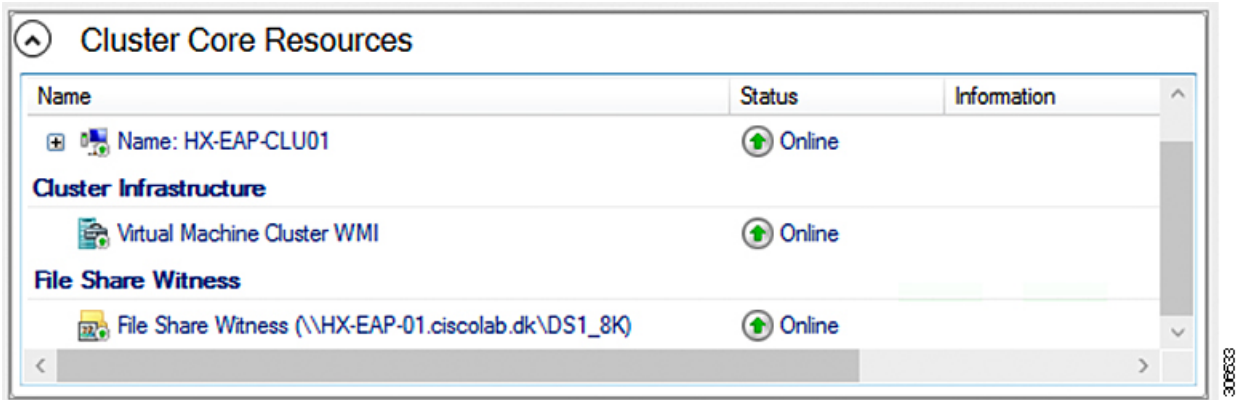
Checking the Windows Version on the Hyper-V Host

Follow the steps below to check the version of Windows installed.

Step 1   Log into the Hyper-V server as an administrator or HX Service Administrator account.

Step 2   In Powershell, run the following command:

C:\Users\adminhyperflex> Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion'

Step 3   Verify the installed Windows version in the result of the command output.

Following is a sample output if you have installed Windows Server 2016.

```
ProductName : Windows Server 2016 Datacenter
ReleaseId : 1607
SoftwareType : System
UBR : 447
```

Following is a sample output if you have installed Windows Server 2019.

```
ProductName : Windows Server 2019 Datacenter
ReleaseId : 1809
SoftwareType : System
UBR : 107
```

Step 4   In addition, verify the following:

- For Windows Server 2016 Datacenter Core and Desktop Experience, the Windows 2016 ISO image should be Update Build Revision (UBR) 1884 at a minimum. If not, upgrade the HyperV servers to the latest update. Refer to the *Microsoft Knowledge Base article: KB4467691*.

- If you are using a standalone Hyper-V manager outside HX nodes, then the Hyper-V management server should have a version UBR number greater than 1884. You must upgrade the Hyper-V management server if the version is 1884 or earlier.

- For Windows Server 2019 Desktop Experience, the Windows 2019 ISO image should be Update Build Revision (UBR) 107 at a minimum.
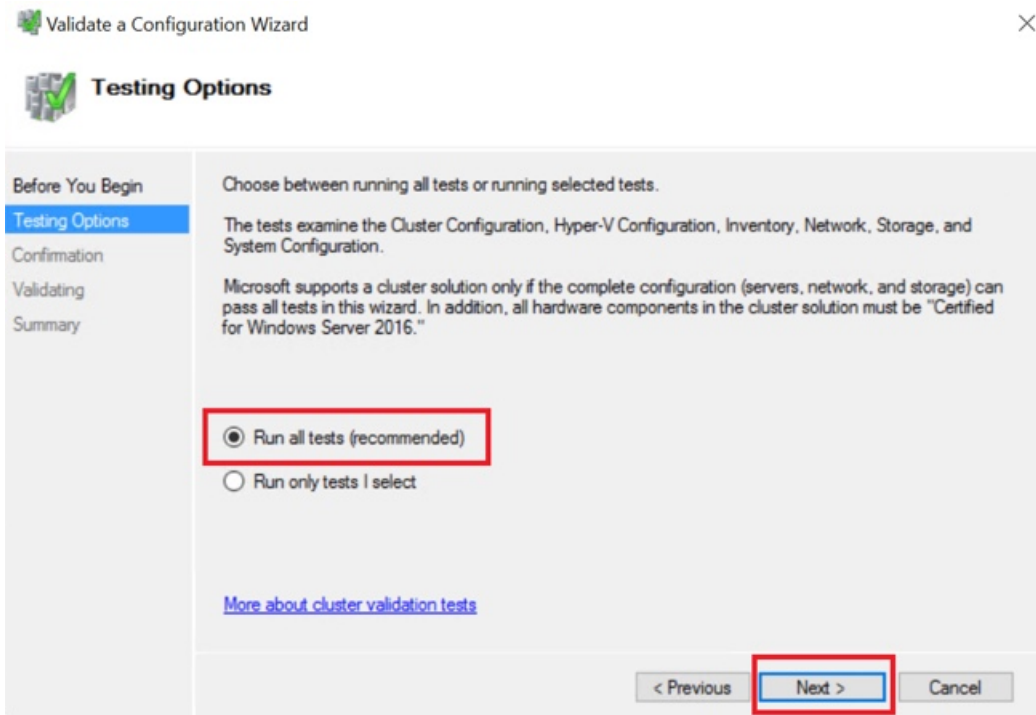
Validate Failover Cluster Manager

Step 1   Open the Failover Cluster Manager and click **Validate Cluster** and then click **Next**.
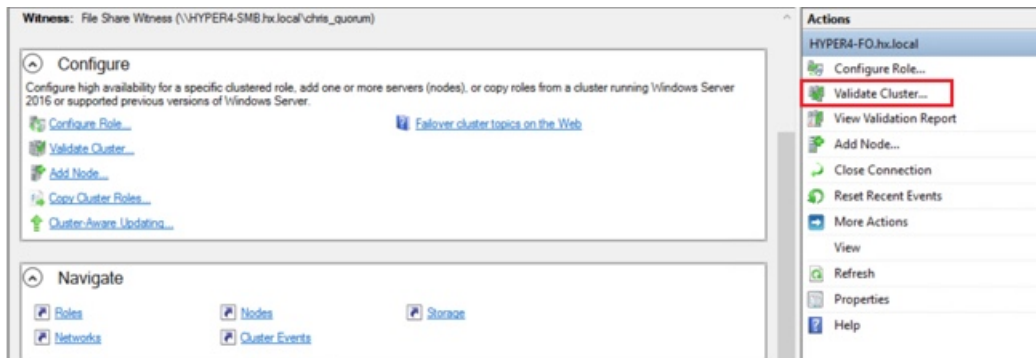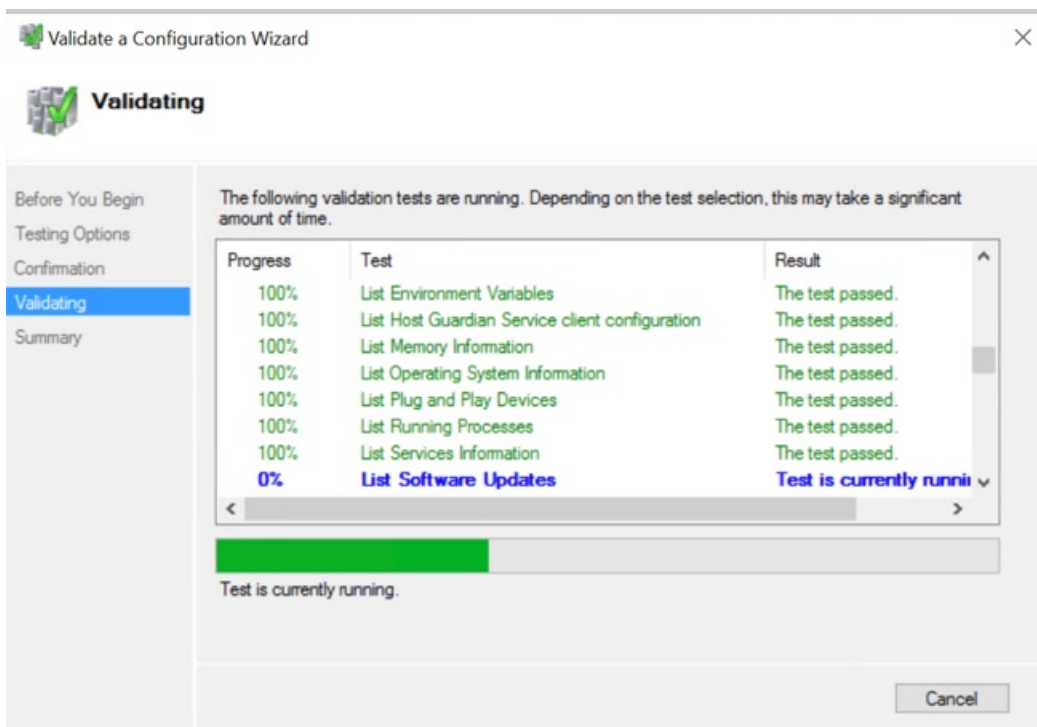
Step 2   Select **Run all tests (recommended)** and then click **Next**.

After clicking **Next**, the validation procedure starts running.

Step 3   Verify that there are no validation failures. If there are any validation failures, click **View Report** and address any results that show **Failed**.

Deploying VMs on a Hyper-V cluster

Deploying VMs on a Hyper-V cluster is a multi-step process as described below:

- **Install Remote Server Administration Tools (RSAT) on the management station/host**—You must install administrator tools such as Hyper-V Manager and Failover Cluster Manager as features Server Manager. For more information see, Install RSAT tools on the Management Station or Host, on page 48.

- **Manage VMs**—Connecting to all the Hyper-V nodes in the HX cluster and creating new VMs can be accomplished using either Hyper-V Manager or Failover Cluster Manager. For more information see, Creating VMs using Hyper-V Manager, on page 53.

Install RSAT tools on the Management Station or Host

To install RSAT, complete the following steps:

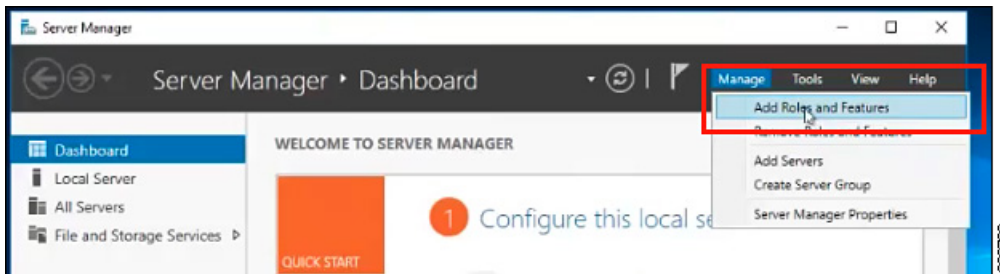**Before you begin**

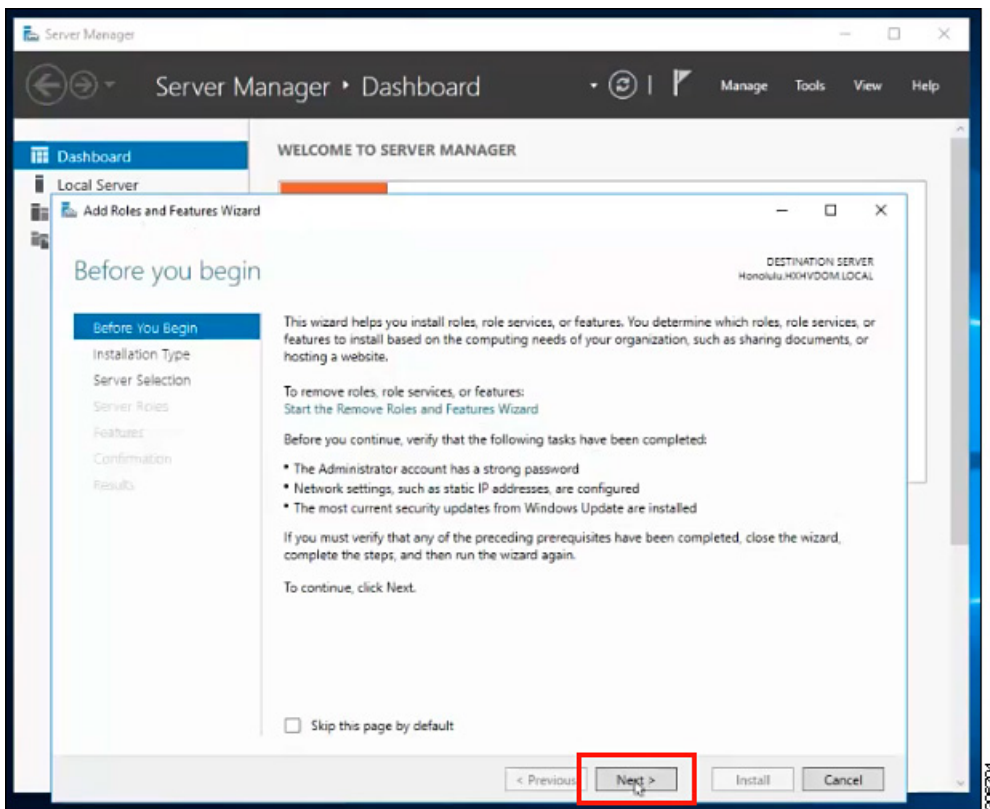RSAT tool installation requires the following:

- A server from which you can install, manage, monitor the VMs on the Hyper-V HX cluster.

- Administrator tools such as Hyper-V Manager, FCM, PowerShell, SCVMM.

Step 1 In Server Manager, click **Manage** and then select **Add Roles and Features**. The **Add Roles and Features** wizard appears.
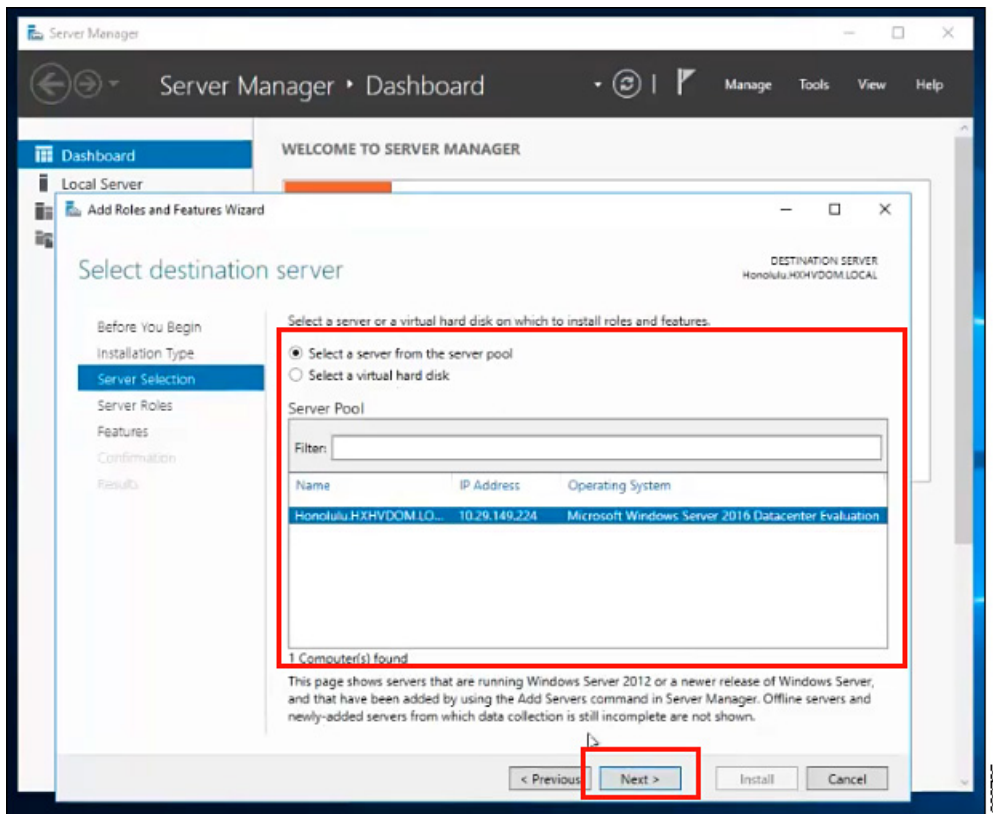

**Step 2** In the **Before you begin** page, click **Next**.

Step 3 In the **Select installation type** page, select **Role-based or feature-based installation**. Click **Next**.

Step 4 In the **Server Selection** page, select your server from the list. This server belongs to the same domain as the HX cluster. Click **Next**.

Step 5   In the **Select Roles** page, click **Next**.

Step 6   In the **Features** page, select **Remote Server Administration Tools** > **Feature Administration Tools** > **Failover Clustering Tools**, and **Role Administration Tools** > **Hyper-V Management Tools** > **Failover Clustering Tools**. Click **Next**.
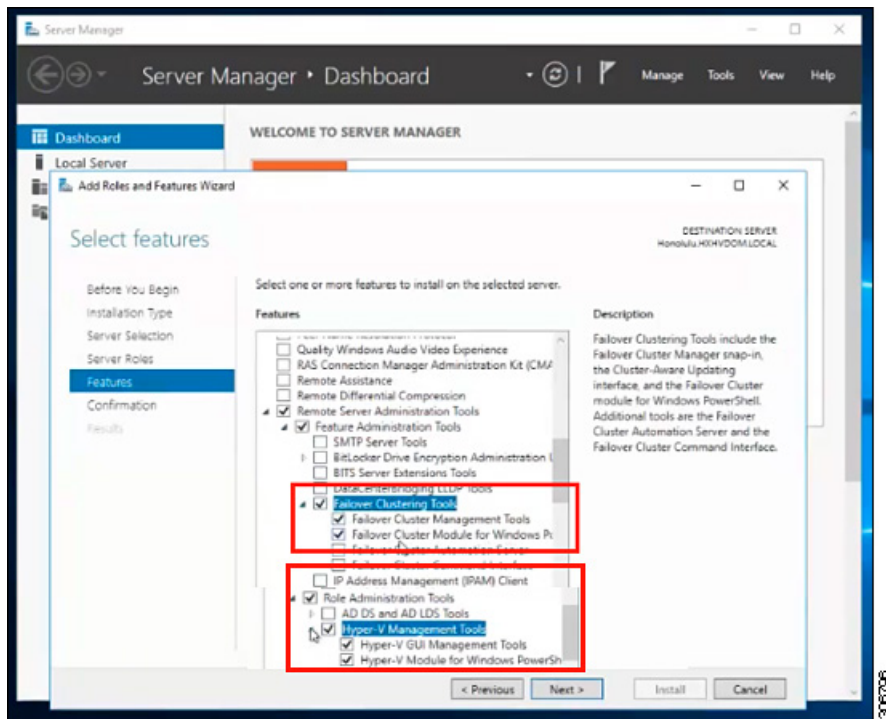
Step 7 In the **Confirmation** page, click **Install**. Leave the **Restart the destination server if required** checkbox unchecked.

Step 8 The **Installation Progress** page displays installation progress. When installation completes, click **Close** to exit the wizard.
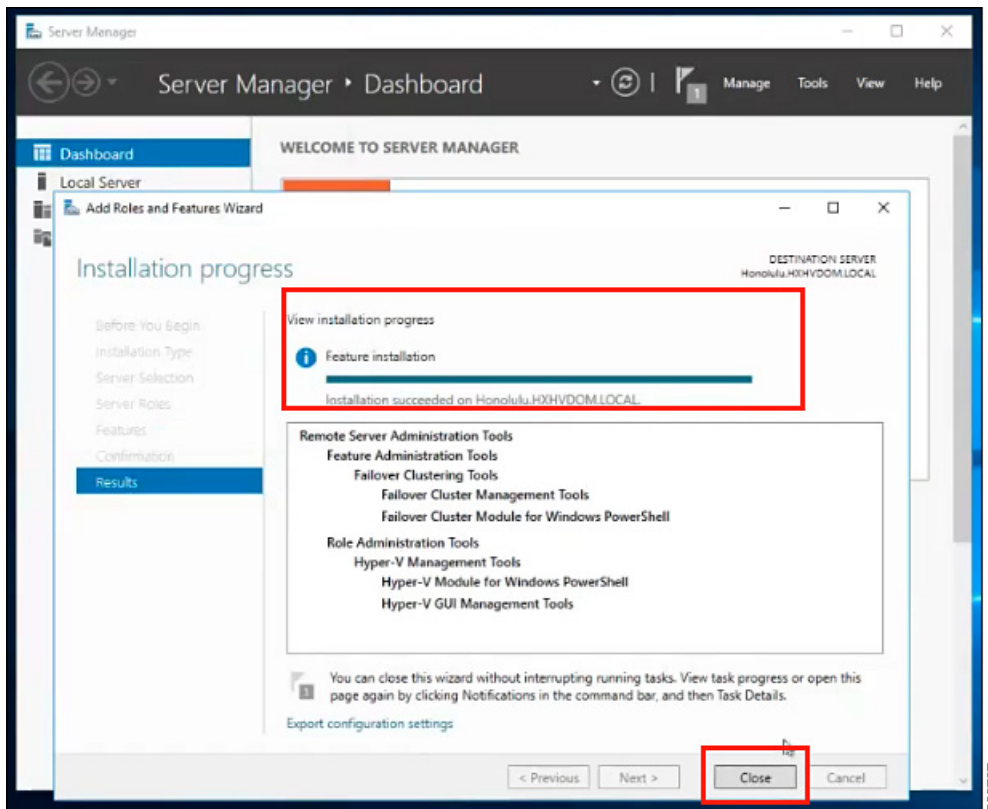
Managing VMs using Hyper-V Manager

Connecting to Hyper-V Nodes

Complete the following steps to connect to all the Hyper-V nodes in the Hyper-V HX Cluster.

Step 1 Open the **Server Manager** dashboard and click **Tools**. Then, click **Hyper-V Manager**. The **Hyper-V Manager** console appears.

Step 2 In the left pane, select **Hyper-V Manager** and click **Connect to Server...**.

Step 3 In the **Select Computer** dialog box, select **Another computer** and type in the name of the Hyper-V node (for example, HXHV1) that belongs to the Hyper-V cluster. Click **OK**.

Step 4 Repeat all of the above steps for each node in the Hyper-V HX cluster.

> **Note**   For a fresh installation, the storage controller virtual machine (StCtlVM) in the only virtual machine that appears in **Virtual Machines** pane in the **Hyper-V Manager** console. Virtual machines appear in the list under this pane as they are added in each node. For more information on how to create VMs using Hyper-V Manager, see: Creating VMs using Hyper-V Manager, on page 53

Creating VMs using Hyper-V Manager

Complete the following steps to create VMs using Hyper-V Manager.

Step 1   Open **Hyper-V Manager**.

Step 2   Select the Hyper-V server, and right click and select **New** > **Create a virtual machine**. The **Hyper-V Manager New Virtual Machine** wizard displays.

Step 3   In the **Before you Begin** page, click **Next**.

Step 4   In the **Specify Name and Location** page, enter a name for the virtual machine configuration file. The location for the virtual machine click **Next**.

Step 5   In the **Specify Generation** page, choose either **Generation 1** or **Generation 2**.

Step 6   In the **Assign Memory** page, set the start memory value 2048 MB. Click **Next**.

Step 7   In the **Configure Networking** page, select a network connection for the virtual machine to use from a list of existing virtual switches.

Step 8   In the **Connect Virtual Hard Disk** page, select **Create a Virtual Hard Disk** page, and enter the name, location and size for the virtual hard disk. Click **Next**.

Step 9   In the **Installation Options**, you can leave the default option **Install an operating system later** selected. Click **Next**.

Step 10   In the Summary page, verify that the list of options displayed are correct. Click **Finish**.

Step 11   In Hyper-V Manager, right-click the virtual machine and click **Connect**.

Step 12   In the **Virtual Machine Connection** window, select **Action** > **Start**.

Managing VMs using Failover Cluster Manager

Creating VMs using Failover Cluster Manager

Complete the following steps to connect to the Windows Failover cluster (installed along with the Hyper-V HX cluster) and create new VMs using Failover Cluster Manager.

Step 1   In the **Failover Cluster Manager** console, under the **Actions** pane, click **Connect to Server...**

Step 2   In the **Select Cluster** dialog box, click **Browse** to navigate to the Hyper-V HX cluster. Click **OK**.

Step 3   In the left pane, click **Roles** > **Virtual Machines...** > **New Virtual Machines...**.

Step 4   In the **New Virtual Machine** dialog box, search and select the Hyper-V node where you wish to create new VMs. Click **OK**. The **New Virtual Machine** wizard appears.

Step 5   In the **Before You Begin** page, click **Next**.

Step 6   In the **Specify Name and Location** page, choose a name for the VM, and specify the location or drive where the VM will be stored. Click **Next**.

Step 7   In the **Specify Generation** page, select the generation of virtual machine you want to use (Generation 1 or Generation 2) and click **Next**.

Step 8   In the **Assign Memory** page, enter the amount of memory that you want for the VM. Click **Next**.

Step 9   In the **Connect Virtual Hard Disk** page, enter the name, location and hard drive size. Click **Next**.

Step 10   In the **Installation Options** page, select the install location for the OS. Click **Next**.

Step 11   In the **Summary** page, review the options selected and click **Finish**.

Step 12   Right-click on the newly created VM, and click **Connect...**. In the **Virtual Machine Connection** window, click **Start**.

Note   By default, the Failover Cluster Manager will assign a default name for the 4 networks created. It is recommended to rename these network names.

What to do next

To enable redirection of datastore access requests from outside the HX cluster boundary through the management path, add the following entry to the hosts file on the (remote) machine running Hyper-V manager, Failover Cluster Manager, or SCVMM Console. For example, edit `C:\Windows\System32\drivers\etc\hosts` and add:

```
cluster_mgmt_ip \\smb_namespace_name\datastore_name

10.10.10.100 \\hxcluster.company.com\ds1
```

Opening Data Path Access to the SCVMM Host

To open data path access to the SCVMM host, complete the following steps:

Before you begin

Beginning with Cisco HX Release 4.5 the `FixScvmmAccess.py` script must be invoked with python3.

Note   `FixScvmmAccess.py` requires root access.

Step 1   Launch a secure shell login session to the cluster management IP address.

Step 2   Determine the ensemble members in the cluster by reviewing the following information:

```
root@ucs900scvm:~# cat /etc/springpath/storfs.cfg | grep crmZKEnsemble
crmZKEnsemble=10.107.48.14:2181,10.107.48.15:2181,10.107.48.16:2181
root@ucs900scvm:~#
```

Step 3   From the current SSH login session, launch an SSH session to any of the IP addresses displayed for the **crmZKEnsemble** parameter.

Step 4   Run the following script without any additional parameters:

```
python3 /opt/springpath/storfs-hyperv/FixScvmmAccess.py
```

The script prompts you to enter the SCVMM IP address.

Step 5   Add the SCVMM IP address and exit the SSH session.

Configuring HyperFlex Share to SCVMM

Before you begin

Edit the `/etc/hosts` file on the host running the VMM admin console to resolve the **smb** access point to the cluster management IP address of HyperFlex cluster. This IP address is typically used to launch Cisco HX Connect.

```
The complete path is : C:\Windows\System32\drivers\etc
Open the "hosts" file in the above directory in Notepad or any other text editor and add
the following entry in the bottom :

<CMIP>  <smb_share_namespace>

CMIP will be the Cluster Management IP which is usually used to open HX connect UI.

For example,
10.10.10.1    hxhvsmb.example.com
```

> **Note**   For SCVMM Run As account, it is recommended to use **hxadmin** (or any other Domain Admin account which has **FULL** permissions) for the corresponding HyperFlex Organization Unit (OU) in the Active Directory (AD).

Step 1   Add the cluster to **System Center - Virtual Machine Manager (VMM)**.

Step 2   In the VMM console, go to **Fabric** > **Servers** > **All Hosts**.

Step 3   Right-click on the cluster and select **Properties**.
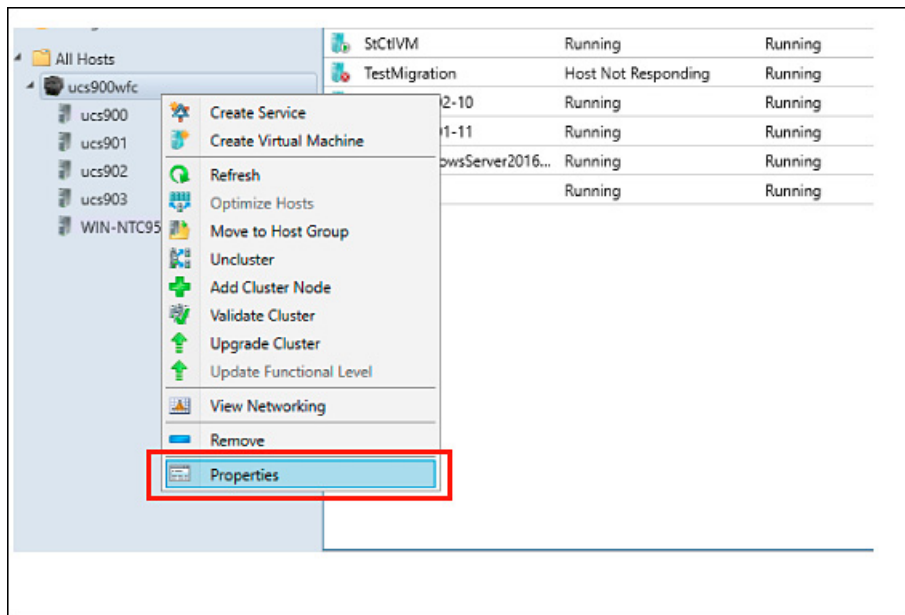
Step 4   In the **Properties** window, right-click **File Share Storage** > **Add File Storage**.
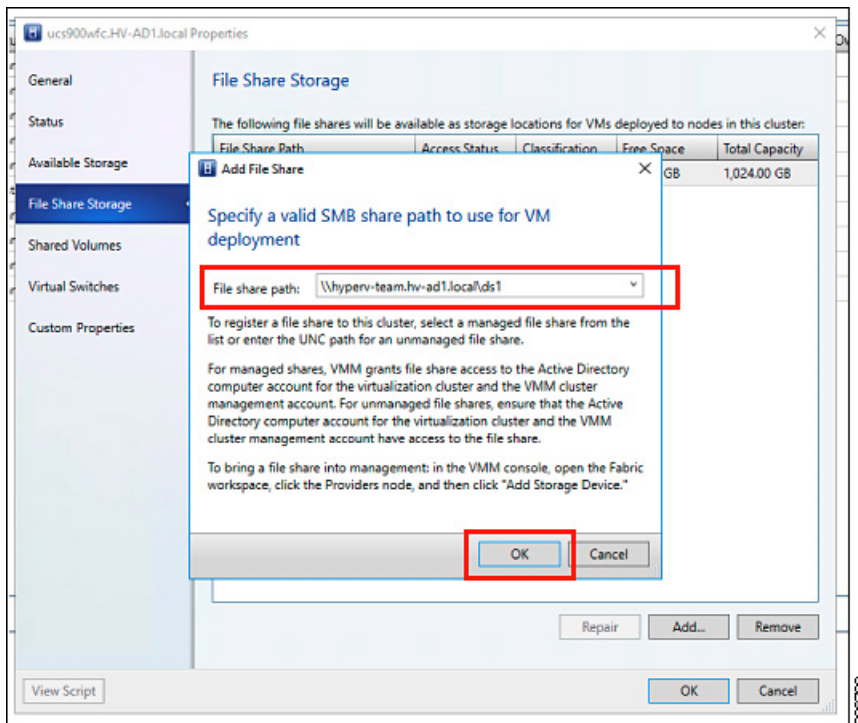
Step 5 When mapping completes, the share is added as shown in the screenshot below.
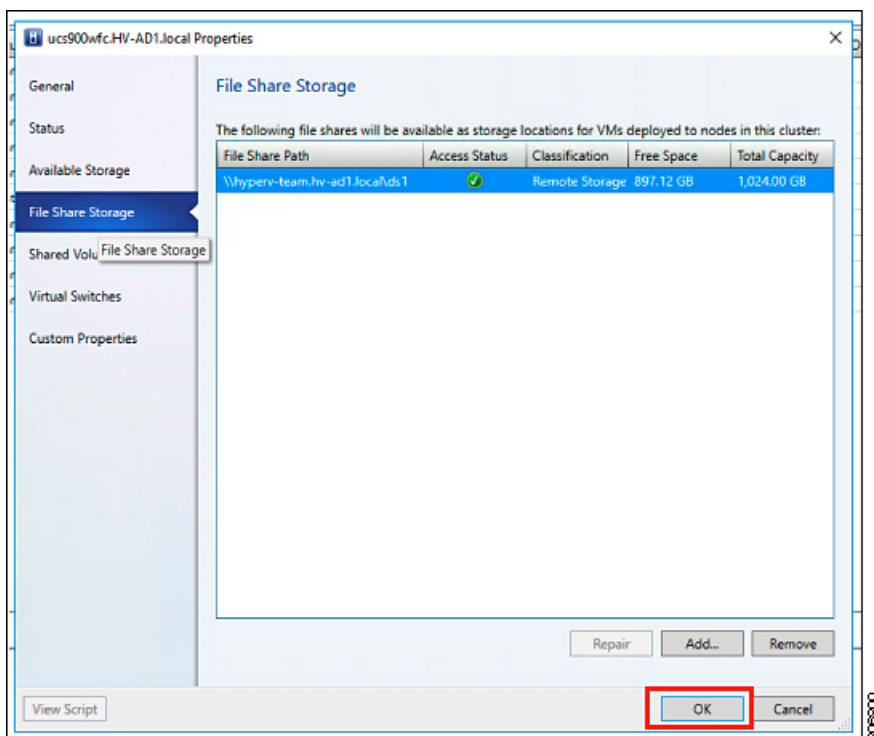
Step 6 Click **OK** and exit VMM. The HyperFlex Share is now mapped and VMs can be created on this share using SCVMM.

Re-enabling Windows Defender

Run the following commands to re-enable Windows Defender.

Install Defender from PowerShell

```
Install-WindowsFeature -Name Windows-Defender
```

(Optional) Install Defender GUI from PowerShell

```
Install-WindowsFeature -Name Windows-Defender-GUI
```

VM Migration between Hosts

Before you begin

Follow the steps below to perform VM migration between a standalone host and an HX Hyper-V host. Prior to performing this procedure, make sure that your environment meets the following prerequisites:

- The source and destination computers either belong to the same Active Directory domain or belong to domains that trust each other.

- In Failover Cluster Manager, configure Live Migration settings on both the source and destination Hyper-V hosts.

Step 1   Open **Hyper-V Manager**.

Step 2   In the navigation pane, select, **HXHVINFRA2**.

Step 3   In the **Action** pane, click **Hyper-V Settings** > **Live Migrations**.

Step 4   In the **Live Migrations** pane, check **Enable incoming and outgoing live migrations**.

Step 5   Under **Incoming live migrations**, select **Use the IP addresses for live migration**. Click **Add**, and then click **OK**. This opens the Move Wizard.

Step 6   Use the wizard pages to choose the type of move, destination server, and options.

Step 7   On the **Summary** page, review your choices and then click **Finish**.

Testing Upstream Failover for Storage Data Network

Configure upstream (top-of-rack (ToR)) so storage data network jumbo frames communicate between FI-A and FI-B.

Note   In some cases 1500 based frames are used because you are not able to configure ToR for jumbo frames as the cluster was previously configured to use 1500 sized frames. The ping test enables you to test basic 1500 frame connectivity across the ToR.
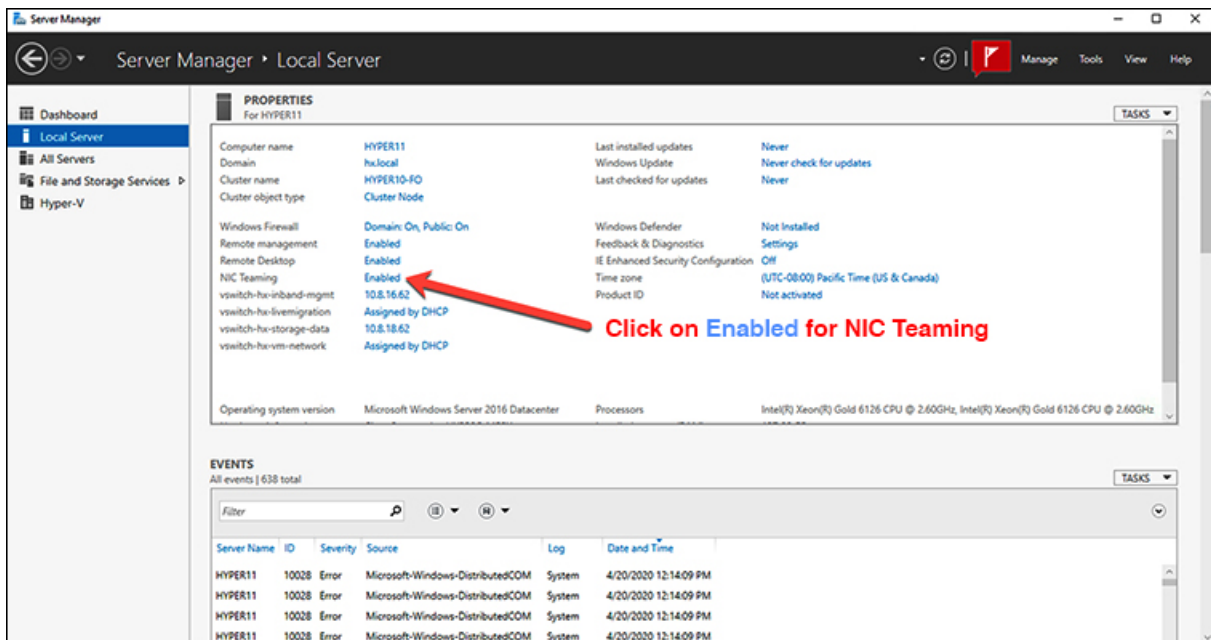
Step 1   Log into a single Hyper-V Host as HX Service account.

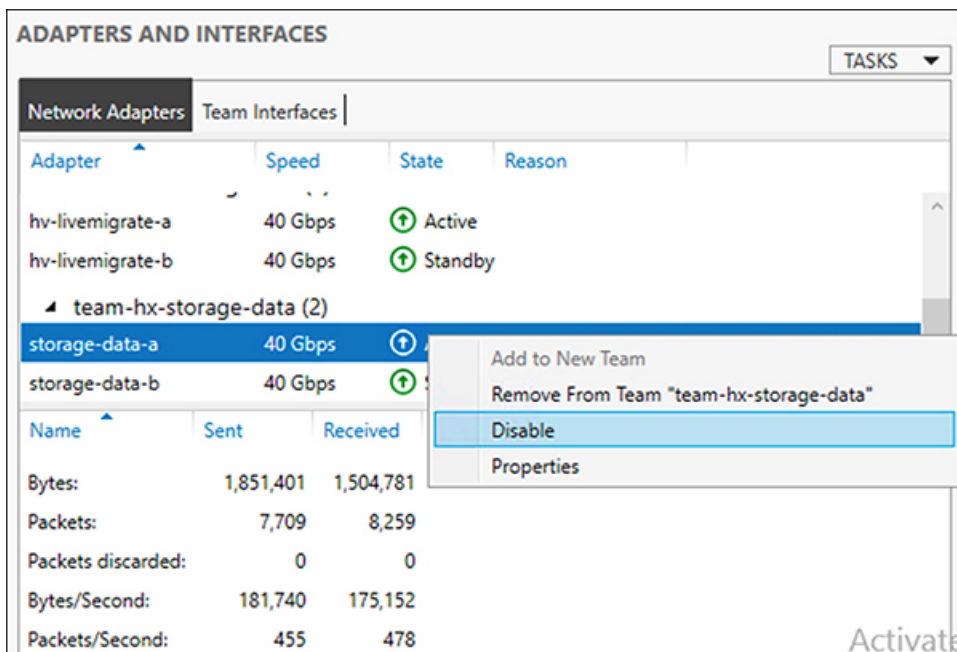**Step 2**   Open **Server Manager** > **Local Server**.
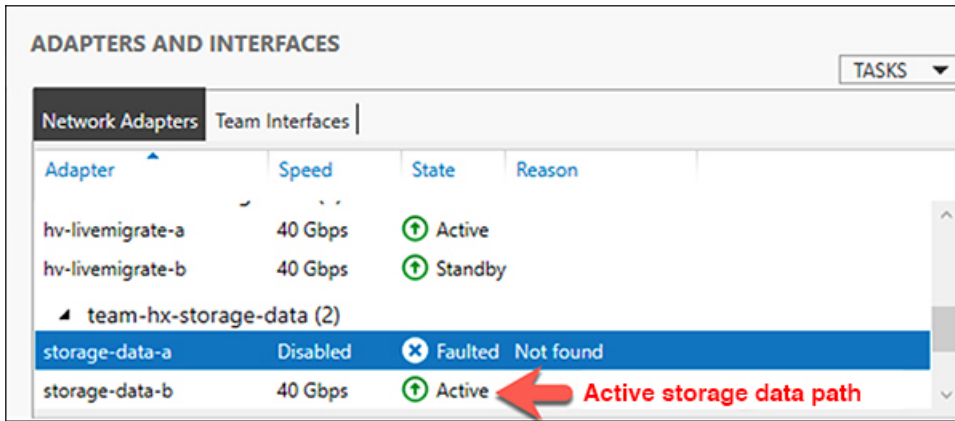
Step 3   Click on **Enabled** for NIC Teaming.

Step 4   Right mouse click on storage-data-a and select **Disable**.
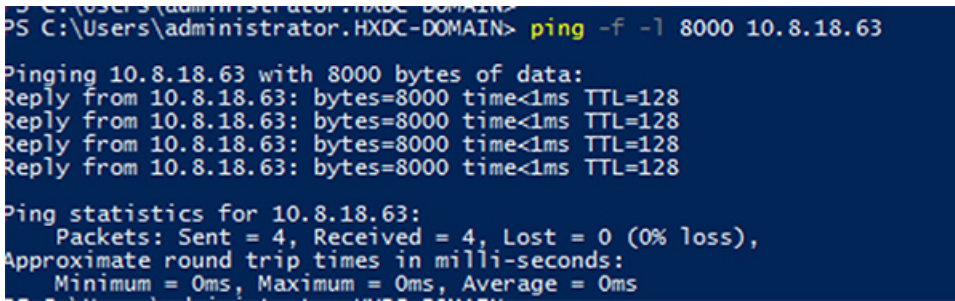

This forces the storage-data-b interface on FI-B to become the active path for data.
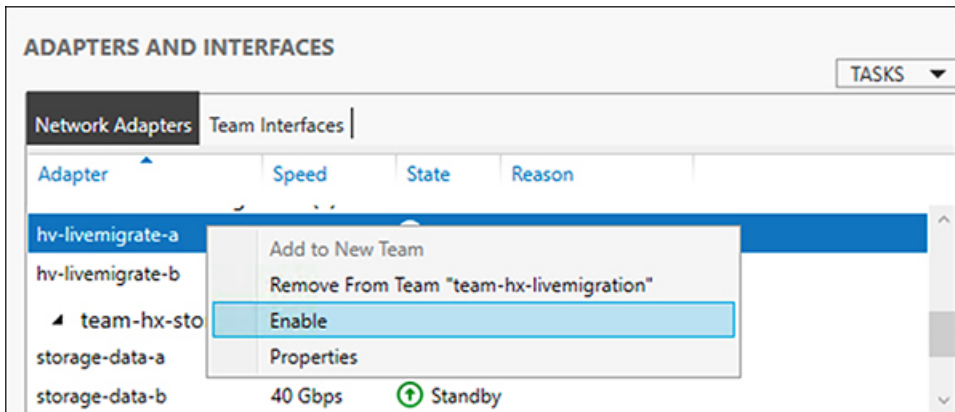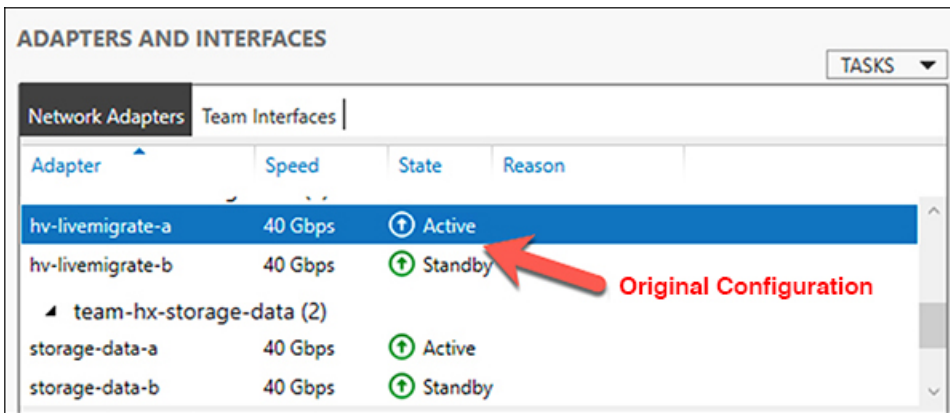
Step 5   Test jumbo pings from local powershell window to remote host storage data ip addresses. For example:

```
# ping -f -l 8000 <data_ip_address_of_other_hosts>
```


Step 6   Reset the storage-data-a team interface to Active by right mouse-clicking and selecting **Enable**.

Adding VLANs after Installation

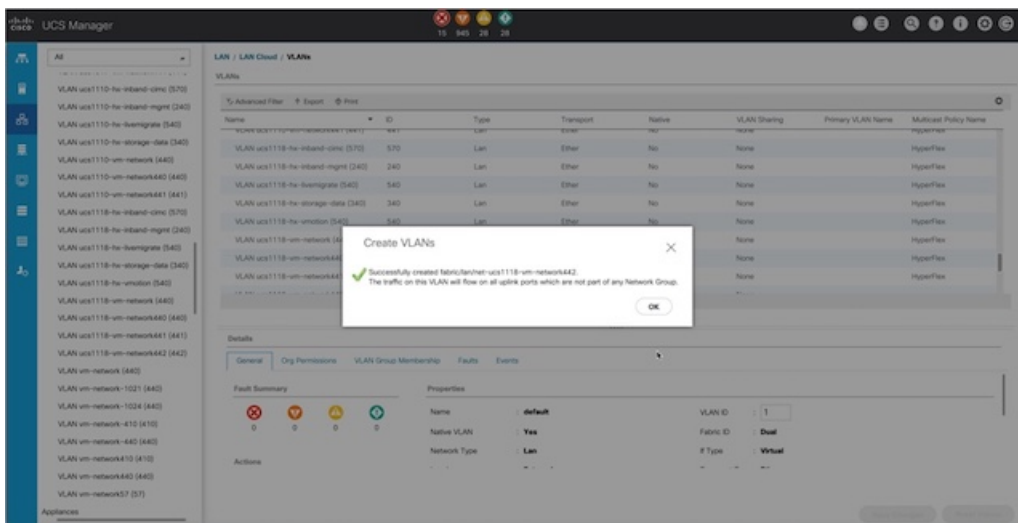To add a VLAN to your cluster after installation is complete, perform the following:
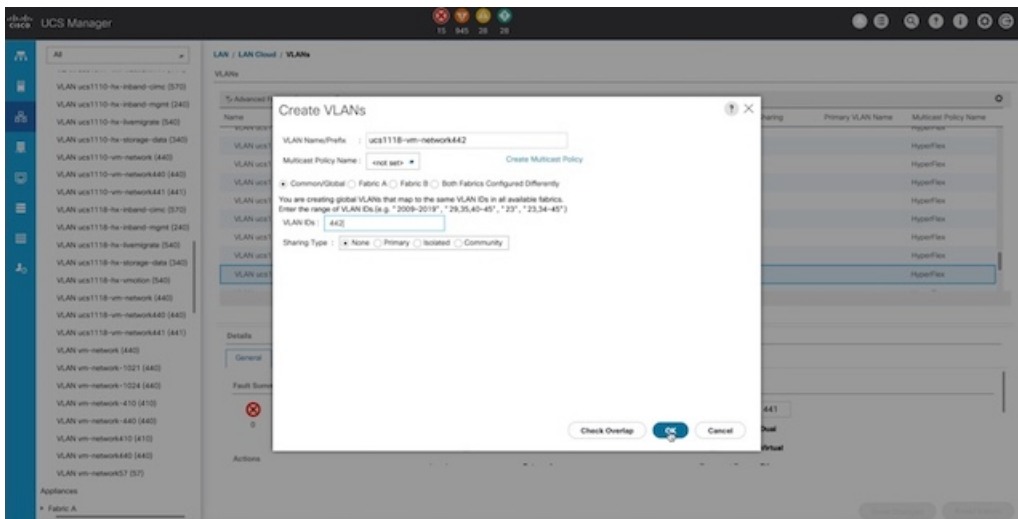
Step 1   In Cisco UCS Manager, navigate to **LAN** > **LAN Cloud** > **VLANs**:
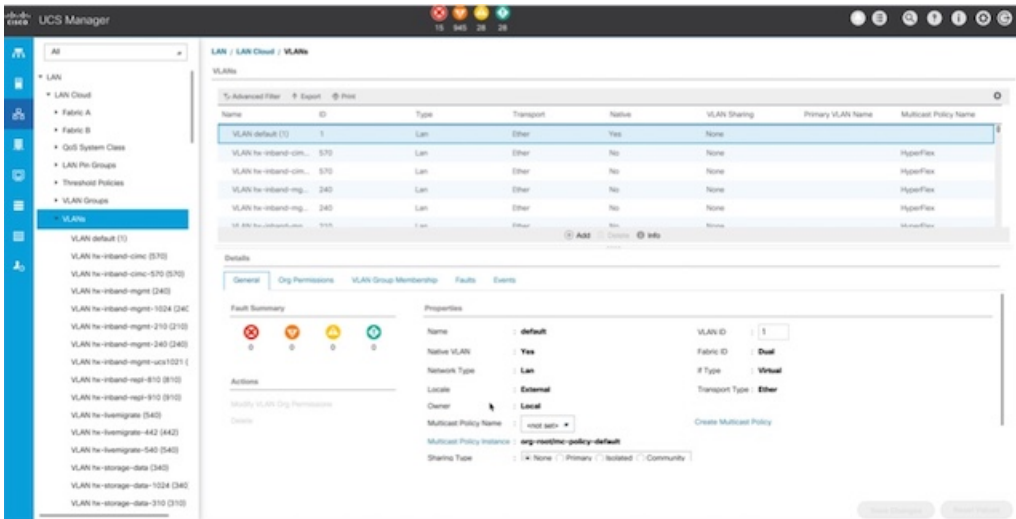
Step 2   To add a new VLAN, click on the **Add** sign at the bottom of the VLAN table:
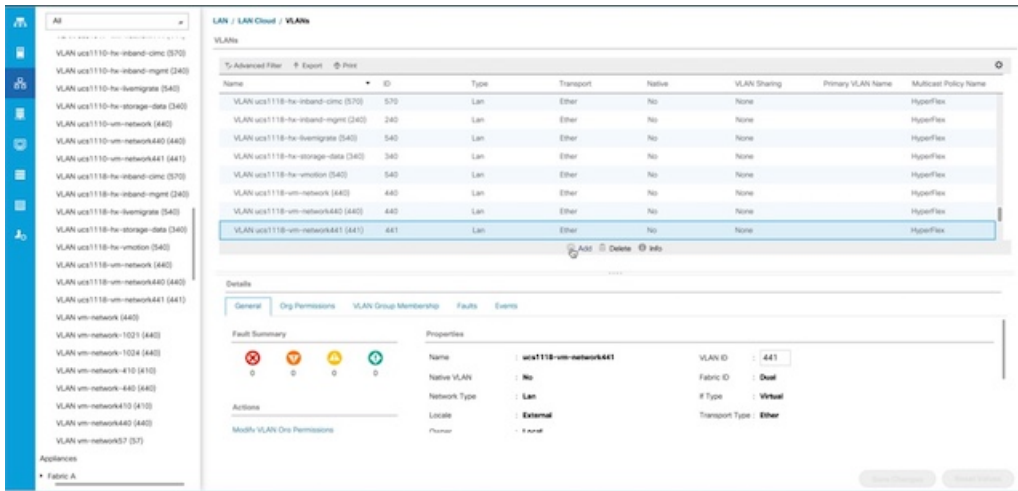
Step 3   Enter the **VLAN Name/Prefix** and **VLAN IDs**:

Step 4   Tag the new VLAN on the required Hyper-V VMs.

| Note | • There is no additional Hyper-V networking configuration needed. |

CHAPTER 6

Cluster Expansion—Converged Nodes

• Cluster Expansion—Converged Nodes, on page 63

Cluster Expansion—Converged Nodes

Before you begin

• Converged nodes can be added after cluster creation.

• This procedure includes Windows Operating System installation.

• Prior to cluster expansion, ensure that the Windows ISO file is available.

• For Hyper-V clusters running on releases earlier than 3.5(2a), cluster expansion is supported for **converged nodes** only.

Step 1 Launch the **Cisco HX Data Platform Installer**.

Step 2 In the login page, enter the following credentials:

Username: `root`

Password (Default): `Cisco123`

Note Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.

Step 3 Check the **I accept the terms and conditions** checkbox, and click **Login**.

Step 4 On the **Select a Workflow** page, select **Cluster Expansion**.

Step 5 On the **Cluster** page, complete the following fields and click **Continue**.

Field	Description
Cluster Management Hostname	The hostname for the existing cluster.
User Name	Administrator username for the existing cluster.
Password	Password for the administrator user of the HX cluster.

Step 6   On the **Credentials** page, complete the following fields and click **Continue**.

Field	Description
UCS Manager Credentials	
UCS Manager Hostname	Cisco UCS Manager FQDN or IP address
UCS Manager User Name	Administrator user or a user with Cisco UCS Manager administrator privileges.
Password	The password for UCS Manager.
Domain Information	
HX Service Account	The HX Service account associated with the existing cluster.
Password	The password for the HX Service account.
Constrained Delegation	
Configure Constrained Delegation now(recommended) or Configure Constrained Delegation later	Select one of the checkboxes. Constrained Delegation is required for VM Live Migration. To configure Constrained Delegation later, use the procedure described in Configuring a Static IP Address for Live Migration and VM Network.
HX Service Account Password	Required for Constrained Delegation.
Use HX Service Account	Click the checkbox if HX service account is provided. If checked, the HX service account will be used for Constrained Delegation. The user must be a domain administrator.
Username	Enter a domain level username.
Password	Enter a domain level password.
Hypervisor Credentials	
Local Administrator Account	Local administrator username for the Hyper-V hosts.
Password	Password for the local administrator account.

Step 7   On the **Node Selection** page, view all the associated and unassociated servers under the **Associated** and **Unassociated** tabs respectively.

Under the **Unassociated** tab, you can choose to add any nodes to the existing cluster.

Under the **Associated** tab, you can choose to unassociate servers from the existing cluster.

Step 8   On the **UCSM Configuration** page, view or modify the auto-populated details for the VLAN configuration and MAC Pool information for the existing cluster. Then, click **Continue**.

Step 9   On the **Hypervisor Configuration** page, complete the following fields:

Field	Description
Install Hypervisor (Hyper-V)	By default, this checkbox is selected.
	Leave the checkbox selected to enable OS installation and network configuration. Click **Browse** to select and upload the ISO file. Alternatively, drag and drop the ISO file into the area.
	From **Select the Operating System you wish to install** choose one of the following
	• Windows Server 2016 Datacenter (Desktop Experience)
	• Windows Server 2016 Datacenter (Core)
	• Windows Server 2019 Datacenter (Desktop Experience)

Click **Continue**.

Step 10 On the **Node Configuration** page, click **Add Converged Server** to add the servers to your existing cluster.

Step 11 Click **Start** to begin the expansion. The **Progress** page displays the progress of the configuration tasks

Step 12 Perform the following post installation steps:

Cluster Expansion—Compute-only Nodes

Overview

You can add converged or compute-only nodes to expand a Hyper-V cluster. Below is the list of supported converged and compute-only nodes in Hyper-V clusters.

- **Converged Nodes**—HX220c M5, HX240c M5, HX220c AF M5, HX240c AF M5

- **Compute-only Nodes**—B200 M5, B200 M4 Blade Servers, and C220 M5 C-Series Rack Servers

The following procedure describes adding **compute-only** nodes to expand a Hyper-V cluster. This expansion workflow includes Windows OS installation and is not performed as part of cluster creation using HX Installer. To expand Hyper-V clusters with converged nodes, refer to Cluster Expansion—Converged Nodes, on page 63.

Pre-expansion Checklist

To add **compute-only** nodes to expand your Hyper-V cluster, complete the following pre-expansion checklist that summarizes key requirements, considerations and tasks.

Note The following check-list applies to Cisco HX Release 4.5(x) and later.

Requirement/Task	Description		
Supported Versions and Platforms	**HX Data Platform**	3.5(2a) and later	
		Important	If your cluster is running on releases earlier than 3.5(2a), ensure that you upgrade your existing cluster to 3.5(2a) at the minimum.
	Compute-only Nodes and Storage Options	**Attention**	UCS B200 M5 blade servers with M.2 SATA drives.
			HW RAID M.2 (UCS-M2-HWRAID and HX-M2-HWRAID) is not supported on Compute-only nodes.
			UCS B200 M4 blade servers with local SAS or Fibre Channel SANs.
	Windows ISO	Customer provided Windows 2016 Datacenter edition ISO.	
Maximum Compute to Converged ratio	1:1		
Maximum Cluster Size	A single cluster can have a maximum of 32 nodes.		
Network Speed	Mixing network speeds between compute-only nodes and HyperFlex converged nodes is not recommended. For example, if the existing network connectivity of the converged nodes is 40 GbE, then the compute-only nodes should also be connected at 40 Gb speeds.		
Determine Boot Disk Connection	Based on your topology, and the type of compute-only nodes that you want to add, choose one of the following expansion scenarios: • Cluster Expansion for UCS M5 blade servers with M.2 SATA drives, or UCS M4 blade servers with Local SAS drives **Note** HW RAID M.2 (UCS-M2-HWRAID and HX-M2-HWRAID) is not supported on Compute-only nodes. • Cluster Expansion for UCS M4 blade servers with Fibre Channel		

Requirement/Task	Description
Boot Disk Capacity	Ensure that you have only ONE boot disk of size **greater than 240GB** during Windows OS installation. After cluster expansion is complete, you may choose additional disks.

Stage HyperFlex Driver Image	The **Windows ISO** and **HyperFlex Driver image** files must be placed on a shared location (such as HX Installer) that is reachable from Cisco UCS Manager and the out-of-band subnet. Use the following steps to download and host the HyperFlex Driver Image and Windows ISO in a shared location within the installer VM
	
	Note Windows is configured to boot to UEFI mode starting Cisco HX Release 4.5 and later.
	
	Note These steps apply to both **Windows Server 2016** and **Windows Server 2019**.
	
	1. Copy the HyperFlex Driver Image. For example, run the following command:
	
	    rsync -avzP /opt/springpath/packages/latest.img /var/www/localhost/images/install.img
	
	2. Mount the HyperFlex Driver Image. For example, run the following command:
	
	    mkdir -p /mnt/install-img && mount -o loop,rw /var/www/localhost/images/install.img /mnt/install-img
	
	3. Copy the answer file specific files for your Windows Server Version and run the following command:
	
	    Windows Server 2016
	
	    cp /opt/springpath/packages/FactoryUnattendXML/WindowsServer2016/Autounattend.xml.uefi /mnt/install-img/Autounattend.xml
	
	    Windows Server 2019
	
	    cp /opt/springpath/packages/FactoryUnattendXML/WindowsServer2019/Autounattend.xml.uefi /mnt/install-img/Autounattend.xml
	
	4. Unmount the HyperFlex Driver Image. For example, run the following command:
	
	    umount /mnt/install-img
	
	Note You cannot install Windows Server 2019 or 2016 on SD cards.
	
	Note The DiskID referenced in autounattend.xml should correctly point to the local disk on the compute node where the OS is installed.

Requirement/Task	Description
Multipathing with Fibre Channel SAN	Do NOT use multipathing with Fibre Channel SANs.
Fabric Interconnect Support	Compute-only node expansion is supported only when the compute node are on the same Fabric Interconnects.

Cluster Expansion - M5 Blade Servers (M.2 SATA) or M4 Blade Servers (Local SAS Drives)

Procedure Overview

The Hyper-V cluster expansion procedure for adding **UCS M5 Blade Servers (M.2 SATA) Or M4 Blade Servers (Local SAS Drives)** consists of the following sequence of tasks:

Cisco UCS Manager Configuration

The following procedure describes configuring Cisco UCS Manager using HX Installer.

Step 1 Log into the HX Data Platform Installer using the following steps:

a) In a browser, enter the URL for the VM where HX Data Platform Installer was installed.

b) Use the credentials: `username:` root, `password:` Cisco123

Important Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.
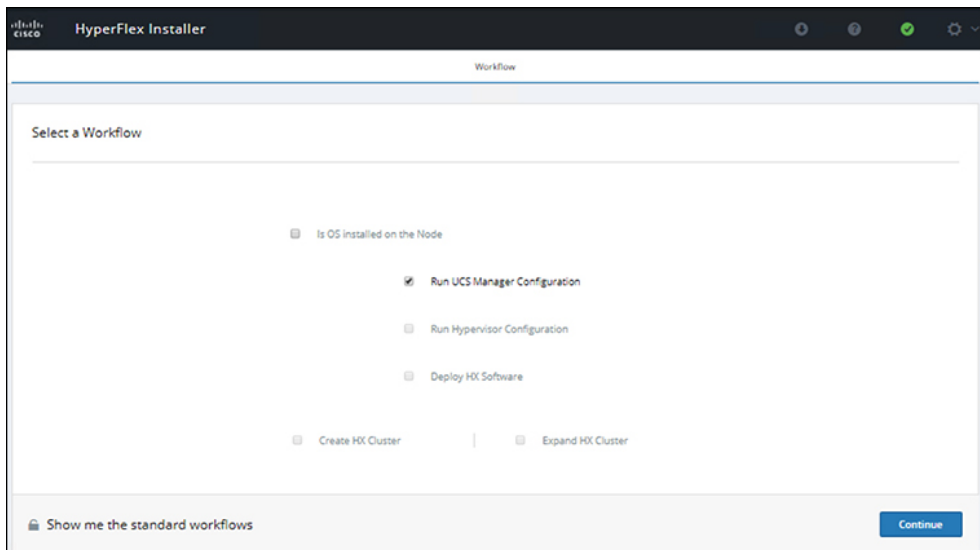
c) Read the EULA. Click **I accept the terms and conditions**. Click **Login**.

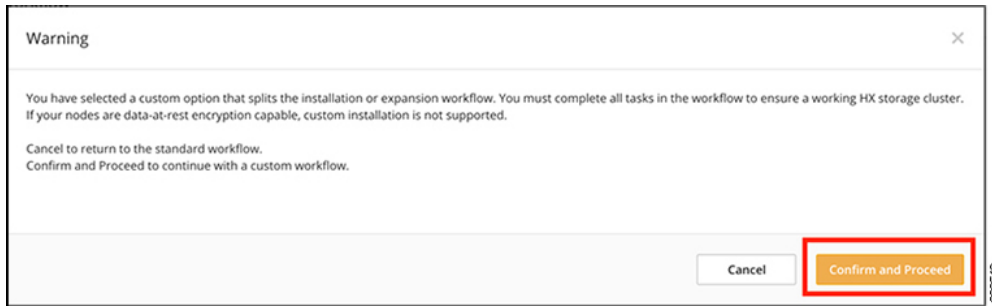**Step 2** In the **Select a Workflow** page, select **Expand Cluster** > **Compute Node**.
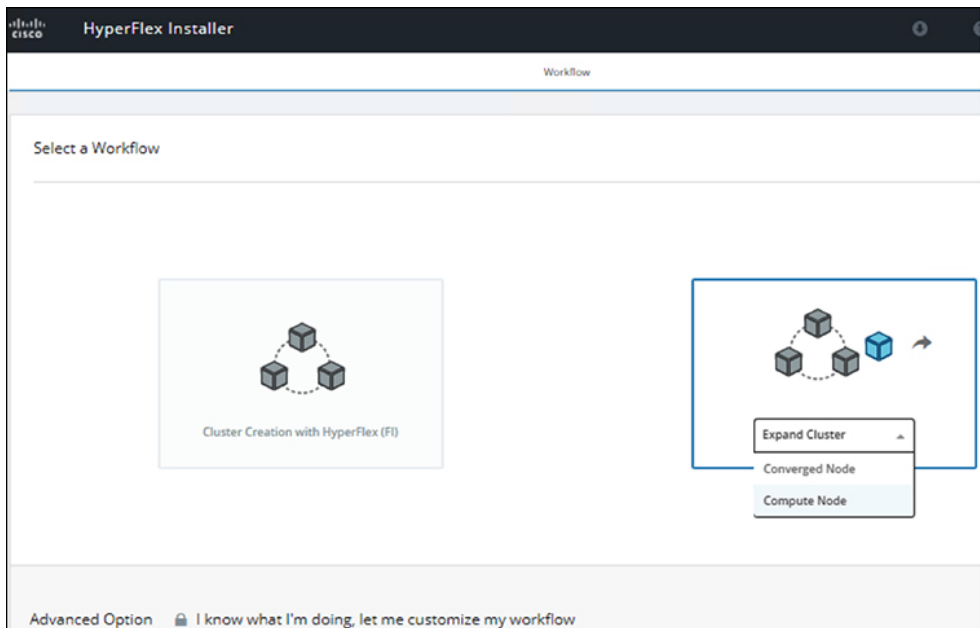
Step 3 In the next screen, click **Run UCS Manager Configuration** and then **Continue**.

**Caution** Do not choose any other workflow option at this point.

Step 4 Click **Confirm** in the pop-up that displays.

Step 5   In the **Credentials** page, complete the following fields for UCS Manager.

Field	Description
UCS Manager Host Name	FQDN or the VIP address of the UCS Manager.
UCS Manager User Name and Password	Administrator user and password or a user with UCS Manager administrative privileges.

Use the following illustration as a reference for entering values in this page.
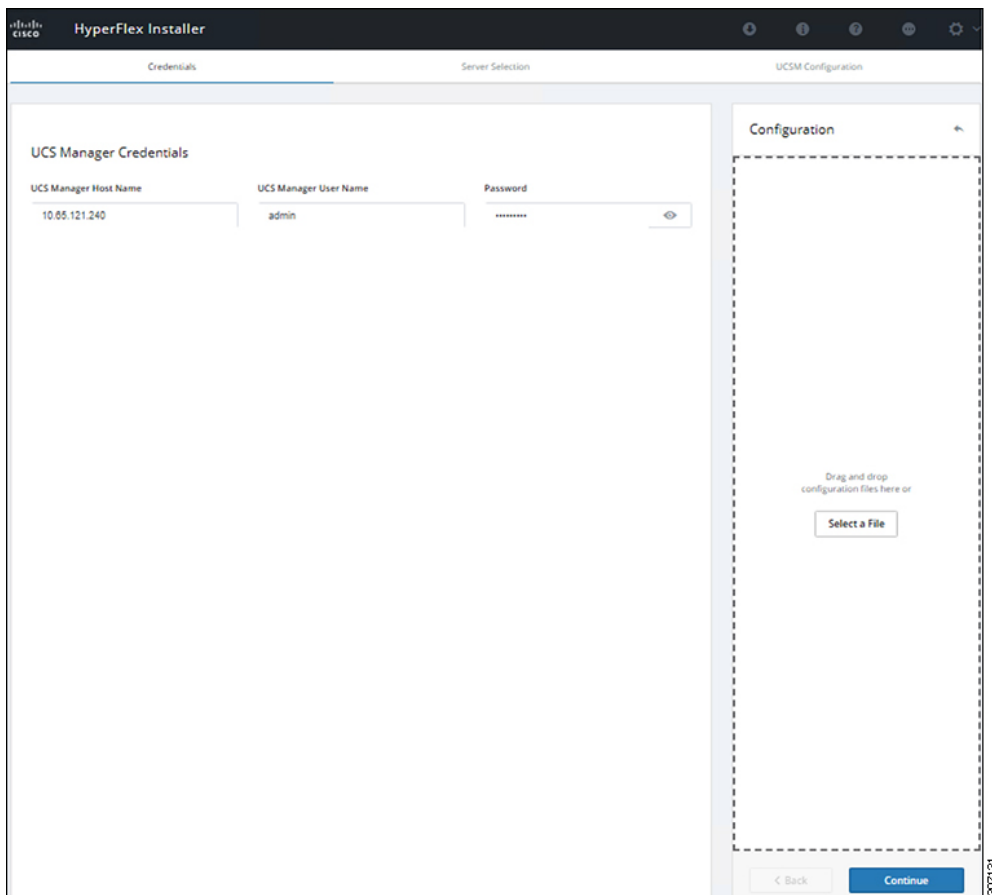
Click **Continue** to proceed. The installer will now try to connect to the UCS Manager and query for available servers. The configuration pane will be populated as the installer progresses. After the query finishes a screen with the available servers is displayed.

Step 6   In the **Server Selection** page, choose all the servers that you want to install in the cluster and click **Continue**.
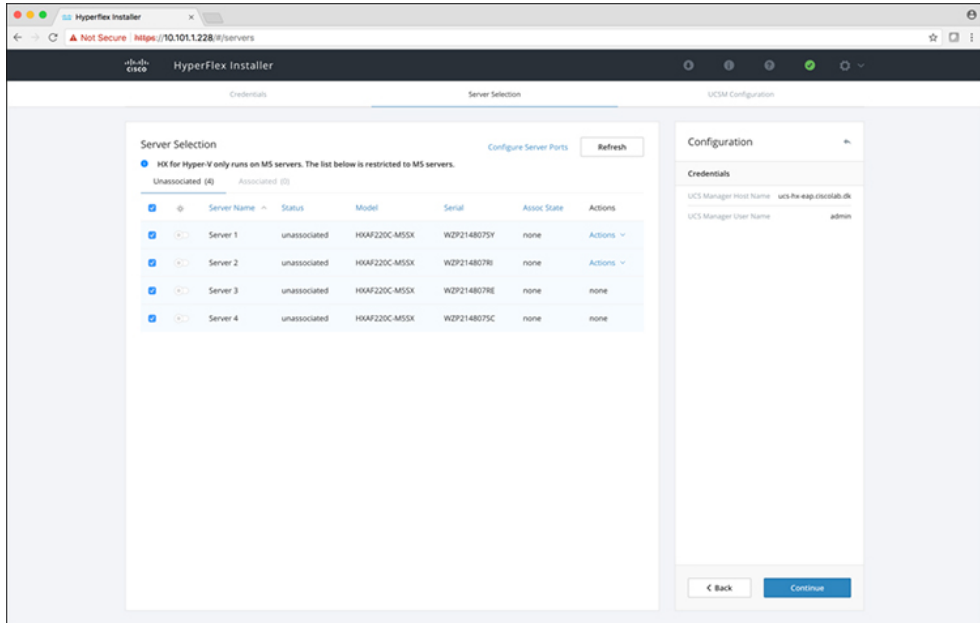
Step 7   In the **UCSM Configuration** page, complete the following fields for **VLAN Configuration**.

HyperFlex needs to have at least 4 VLANs to function, each needs to be on different IP subnets and extended from the fabric interconnects to the connecting uplink switches, to ensure that traffic can flow from the Primary Fabric Interconnect (Fabric A) to the Subordinate Fabric Interconnect (Fabric B).

Name	Usage	ID
hx-inband-mgmt	Hyper-V and HyperFlex VM mgmt.	10
hx-storage-data	HyperFlex storage traffic	20
hx-livemigrate	Hyper-V Live Migration network	30
vm-network	VM guest network	100,101

Use the following illustration as a reference for entering values in this page.

VLAN Configuration

VLAN for Hypervisor and HyperFlex management

| VLAN Name | VLAN ID |
| hx-inband-mgmt | |

VLAN for HyperFlex storage traffic

| VLAN Name | VLAN ID |
| hx-storage-data | |

VLAN for VM Live Migration

| VLAN Name | VLAN ID |
| hx-livemigrate | |

VLAN for VM Network

| VLAN Name | VLAN ID(s) |
| vm-network | |

Note
- Do not use VLAN 1 as it is not best practice and can cause issues with disjoint layer 2.
- vm-network can be multiple VLANs added as a comma separated list.

Caution Renaming the 4 core networks is not supported.

Step 8 Enter the remaining network configuration for MAC Pool, 'hx' IP Pool for Cisco IMC, Cisco IMC access management (Out of band or in band)

Field	Description	Value
MAC Pool		
MAC pool prefix	MAC address pool for the HX cluster, to be configured in UCSM by the installer. Ensure that the mac address pool isn't used anywhere else in your layer 2 environment.	00:25:b5:*xx*
'hx' IP Pool for Cisco IMC		
IP Blocks	The range of IP addresses that are used for Out-Of-Band management of the HyperFlex nodes.	10.193.211.124-.127
Subnet Mask	The subnet mask for the Out-Of-Band network	255.255.0.0
Gateway	The gateway address for the Out-Of-Band network	10.193.0.1
Cisco IMC access management (Out of band or In band)		
In band (recommended) Out of Band	Select the option that was used for converged-nodes cluster creation.	

Note
- The Out-Of-Band network needs to be on the same subnet as UCS Manager.
- You can add multiple blocks of addresses as a comma separated line.

MAC Pool

MAC Pool Prefix

00:25:B5:

'hx-ext-mgmt' IP Pool for Out-of-band CIMC

| IP Blocks | Subnet Mask | Gateway |
| ex: 10.193.211.124-127,10.193.211.158-1(| ex: 255.255.0.0 | ex: 10.193.0.1 |

Important   If you choose to expand your Hyper-V cluster using **M4 blade servers with FC SAN** boot option, you must enable FC Storage. Complete the fields for FC Storage.

Table 14: (Optional) Applicable for M4 blade servers with FC SAN

| Field	Description	Example Value
FC Storage	Checkbox that indicates if FX Storage should be enabled.	Check to enable FC Storage
WWxN Pool	A WWN pool that contains both WW node names and WW port names. For each fabric interconnect, a WWxN pool is created for WWPN and WWNN.	20:00:25:B5:C2
VSAN A Name	The name of the VSAN for the primary fabric interconnect (FI-A). By default, this is set to hx-ext-storage-fc-a.	hx-ext-storage-fc-a
VSAN A ID	The unique identifier assigned to the network for the primary fabric interconnect (FI-A).	70
VSAN B Name	The name of the VSAN for the subordinate fabric interconnect (FI-B). By default, this is set to hx-ext-storage-fc-b.	hx-ext-storage-fc-b
VSAN B ID	The unique identifier assigned to the network for the subordinate fabric interconnect (FI-B).	70

Step 9   **Advanced Section**

Field	Description	Example Value
UCS Firmware Server Version	Choose the appropriate UCS Server Firmware version.	3.2(3a)
HyperFlex Cluster Name	This user defined name will be used as part of the service profile naming In UCSM for easier identification.	

Field	Description	Example Value
Org Name	The org. name is used for isolating the HX environment from the rest of the UCS platform to ensure consistency.	HX-Cluster1

Step 10   When you click **Start**, the installer validates your input and then begins configuring UCS Manager.

Step 11   When the HX Data Platform Installer is finished, then you are ready to proceed to next step.
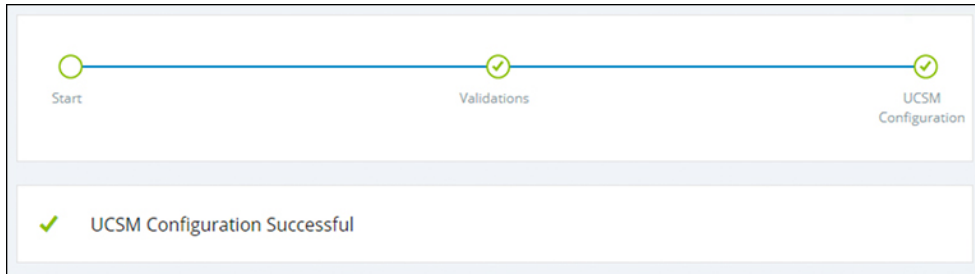
Microsoft OS Installation

For Microsoft OS installation, you will need to first configure a vMedia policy in Cisco UCS Manager to map the following two image files:

- Customer provided **Windows 2016 Datacenter edition ISO** or **Windows Server 2019 Datacenter-Desktop Experience ISO**, and

- Cisco provided **Cisco HyperFlex Driver image**.

✏️

Note   Ensure network connectivity exists between the fileshare and all server management IP addresses.

Step 1   **Launch Cisco UCS Manager**:

a)   In your web browser, type the **Cisco UCS Manager** IP address.

b)   Click **Launch UCS Manager**.

c)   In the login screen, enter the with the username as **admin** and the password set in the beginning of the installation. Click **Log in**.

Step 2   **Create a vMedia policy for the Windows OS and Cisco driver images:**

a)   In the Navigation pane, click **Servers**.

b)   Expand **Servers** > **Policies** > **root** > **Sub-Organizations** > *hx-cluster_name* > **vMedia Policies**

c)   Right-click **vMedia Policies** and select **Create vMedia Policy HyperFlex**.

d) In the **Create vMedia Policy** dialog box, complete the following fields:

Field Name	Description
Name	The name of the vMedia policy. For example, *HX-vMedia*.
	This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description	A description of the policy. We recommend including information about where and when the policy should be used. Maximum 115 characters.
Retry on Mount Failure	Designates if the vMedia will continue mounting when a mount failure occurs. This can be:
	• **Yes**
	• **No**
	Note The default setting is **Yes**. When **Yes** is selected the remote server will continue to try to mount the vMedia mount process until it is successful, or you disable this option. If you select No, a warning message will appear indicating retry on mount failure will not work in case of mount failure.

Refer to the following screenshot as an example:

e) On the icon bar under the **vMedia Mounts** pane, click + **Add**. In the **Create vMedia Mount** dialog box, complete the following fields:

Field Name	Description	Example Value
Name	Name for the mount point.	Windows-ISO
Description	Can be used for more information.	Windows Server 2016 image or Windows Server 2019 image
Device Type	Type of image that you want to mount. This can be: • **CDD**—Scriptable vMedia CD. • **HDD**—Scriptable vMedia HDD.	CDD
Protocol	The protocol used for accessing the share where the ISO files are located.	HTTP
Hostname/IP Address	IP address or FQDN of the server hosting the images.	10.101.1.92
Image Name Variable	This value is not used in HyperFlex installation.	None

Field Name	Description	Example Value
Remote File	The filename of the ISO file that you want to mount.	
Remote Path	The path on the remote server to where the file resides	
Username	If you use CIFS or NFS a username might be necessary	
Password	If you use CIFS or NFS a password might be necessary	

Refer to the screenshot below as an example:

f) Click **OK**. When you click **OK**, you will now be returned to the **vMedia Policies** screen, and you should see the information that you just submitted.

g) Repeat **Steps 2e and 2f**, however, change the type to **HDD** and the remote file name to the **Cisco HyperFlex driver image**.

h) At the end of this step, the two vMedia mounts will be listed in the Create vMedia Policy screen as shown in the following screenshot:

Step 3 **Associate the vMedia Policy to a Service Profile**:

a) In the Navigation pane, select **Servers** > **Service Profile Templates** > **root** > **Sub-Organizations** > *hx-cluster_name* > **Service Template** *compute-nodes, or compute-nodes-m5*

b) Click the **vMedia Policy** tab. Then, click **Modify vMedia Policy**

c) Choose the **vMedia Policy** that you created earlier from the drop-down selection, and click **OK** twice.

d) Under the **General** tab, verify that the vMedia policy is added to the Service Profile.

Step 4 **Modify Boot Policy and set the boot order to have CIMC CD/DVD to the list:**

a) In the Navigation pane, click the **Servers** tab.

b) Expand **Servers** > **Policies** > **root** > > **Boot Policies** > *hx-compute, or hx-compute-m5*
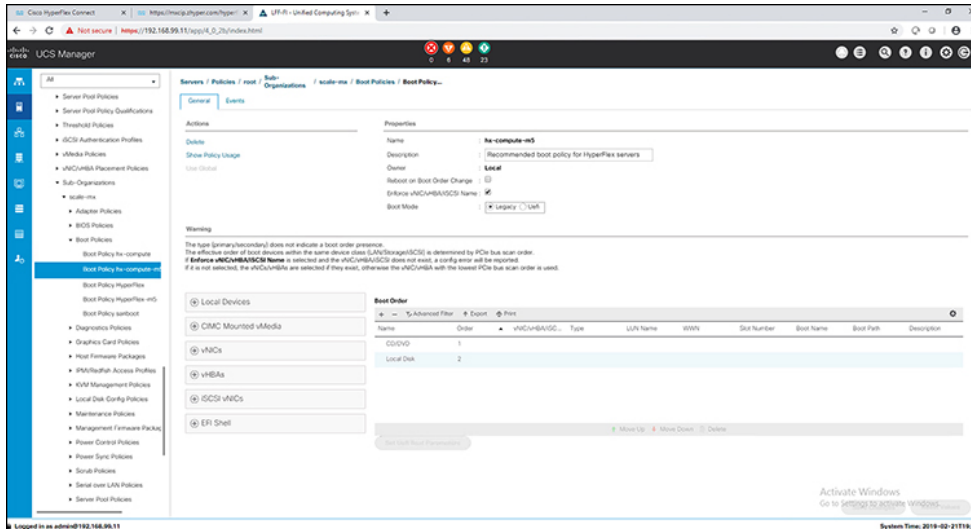
c) In the **Boot Order** configuration pane, click **CIMC Mounted CD/DVD** . Then, click **Add CIMC Mounted CD/DVD** to add this to the boot order. Move it to the top of the boot order using the **Move up** button.
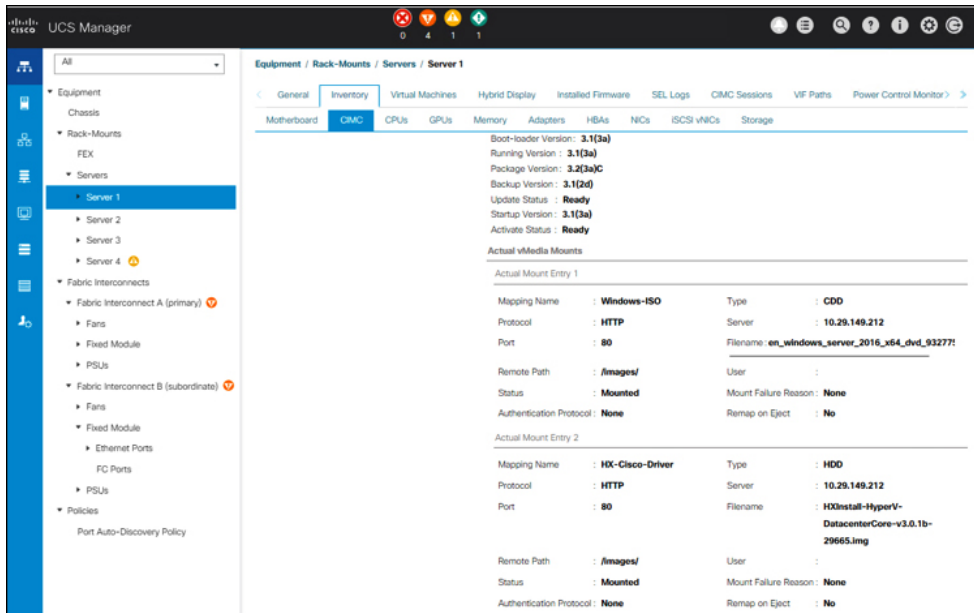
> **Important** As shown in the screenshot below, the **CIMC Mounted CD/DVD** option must be highest in the boot order preceding the other options, **Embedded Local Disk** and **CD/DVD**.
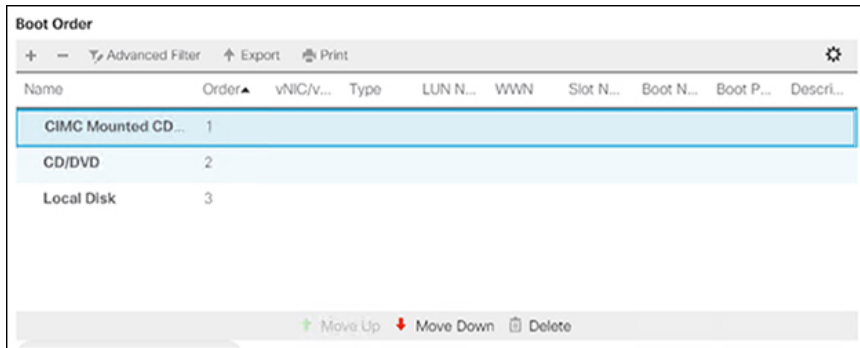
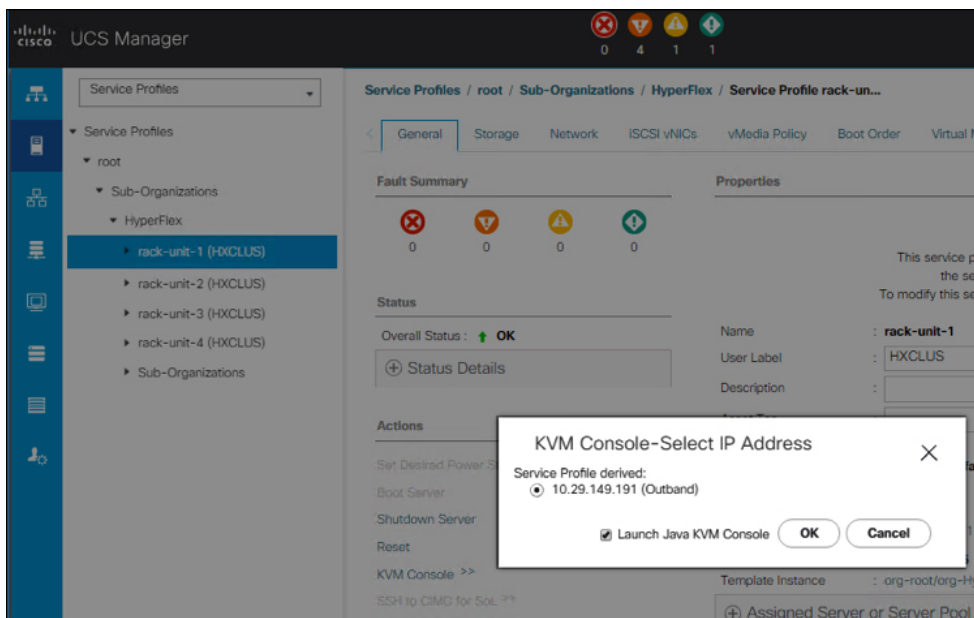d) Click **Save Changes**, and click **OK** in the **Success** dialog box. The modified boot policy is saved.

Step 5 **Verify successful vMedia mounting:**

a) On the **Equipment** tab, select one of the servers.

b) Click **Inventory** > **CIMC**, scroll down and ensure for mount entry #1(OS image) and mount entry #2 (Cisco HyperFlex driver image) you see status as **Mounted** and there are no failures.

c) In the menu bar, click **Servers** and choose the first HyperFlex service profile.

d) Click the **General tab** and choose **Actions** > **KVM Console>>**.

Note   The KVM console will try to open in a new browser. Be aware of any pop-up blockers. Allow the pop-ups and re-open the KVM

e) Reboot the host, launch the KVM Console, and power on the server to monitor the progress of the Windows installation. You should see the **Loading Files** screen appear. Windows should install automatically without user intervention.

Note   The option to install Windows automatically without user intervention is applicable for fresh or first-time installations only. For reinstallations, or if the node already contains a Windows partition, you will need to respond to the prompt to "Press any key to boot from CD/DVD".

You should see a blue screen and within a few moments you should see the **Setup is starting** message. The host will reboot a few times. If automated installation does not begin, double-check that both images are mounted to the server.

f) The installation is complete when you get a clear command prompt at `c:\users\administrator>`. This is applicable for both Windows Core and Desktop Experience installations. It may take several minutes for the Driver Image to be copied and installed.

Note   Ignore the prompt with the **The system cannot find the file specified** message.

Important   Ensure that you have completed **Steps e and f,** on ALL servers that will be part of the HX cluster.

Note   If Microsoft Windows OS is already installed on the node, you must click **any** key to continue when the node boots back up so that the fresh OS installation can happen.

            If you haven't clicked **any** key to continue, and an existing node with a previous OS installed is used to expand, then the new installation is skipped causing further expansion to fail.

g) Log into each server and verify the following:

Run the powershell command: `Get-ScheduledTask -TaskName HXInstallbootstraplauncherTask`. Verify that the HX Install Bootstrap Launcher task is running. Sample output as follows:

```
TaskPath                            TaskName                          State
--------                            --------                          -----
\                                   HXInstallbootstraplauncherTask    Running
```

Validate that the log line "Done with HX PostSysPrepSetup" exists in `C:\ProgramData\Cisco\HyperFlex\Install\Log\PostSysprepSetup.log`.

Run powershell command: `Get-Command Get-VMSwitch`. Verify that the command runs successfully (no exception). Sample output as follows:

```
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Get-VMSwitch                                       2.0.0.0    Hyper-V
```

Step 6   **Reset the vMedia policy back to the default HyperFlex policy:**

a) Update the vMedia policy for compute nodes. Go to **Servers** > **Service Profile Templates** > **root** > **Sub-Organizations** > *hx-cluster_name* > **Service Template** *compute-nodes, or compute-nodes-m5*. Then, click on **Modify vMedia Policy**.

b) Under the vMedia Policy drop-down selection, choose "HyperFlex" policy.

Step 7   **Restore the boot order to the one before installation:**

a) In the Navigation pane, click the **Servers** tab.

b) Expand **Servers** > **Policies** > **root** > > **Boot Policies** > *hx-compute, or hx-compute-m5*

c) In the **Boot Order** configuration pane, use the **Move Down** button to move **CIMC Mounted CD/DVD** option to the bottom of the list.

Step 8   **Change the local Administrator password to match the password on the existing cluster.**

a) Log into the newly-installed compute node.

b) Open a command prompt.

c) Run the following command: `net user Administrator <password>`.

Step 9   **Update the password for HXInstallbootstraplauncherTask and verify that it is Running:**

a) Stop the scheduled task "HXInstallbootstraplauncherTask" if it is running.

            For example:

```
Get-ScheduledTask -TaskName "HXInstallbootstraplauncherTask" | Stop-ScheduledTask
```

b) Update task credentials.

For example:

```
Get-ScheduledTask -TaskName "HXInstallbootstraplauncherTask" | Set-ScheduledTask -User
"Administrator" -Password <password>
```

c) Start the scheduled task and verify that it is Running.

For example:

```
Get-ScheduledTask -TaskName "HXInstallbootstraplauncherTask" | Start-ScheduledTask
```

```
Get-ScheduledTask -TaskName "HXInstallbootstraplauncherTask"
```

Hypervisor Configuration, HXDP Software Installation and Cluster Expansion

After the installation of Windows OS is completed, perform the following steps to configure the hypervisor, install the HX Data Platform Software and expand the cluster.

Step 1   **Re-open** the HX Data Platform Installer and log in.

Step 2   You might need to "start over" because the previous workflow was finished. Click on the gear icon in the top right corner and select **Start Over**.

Step 3   In the **Select a Workflow** page, select **Expand Cluster** > **Compute Node**.
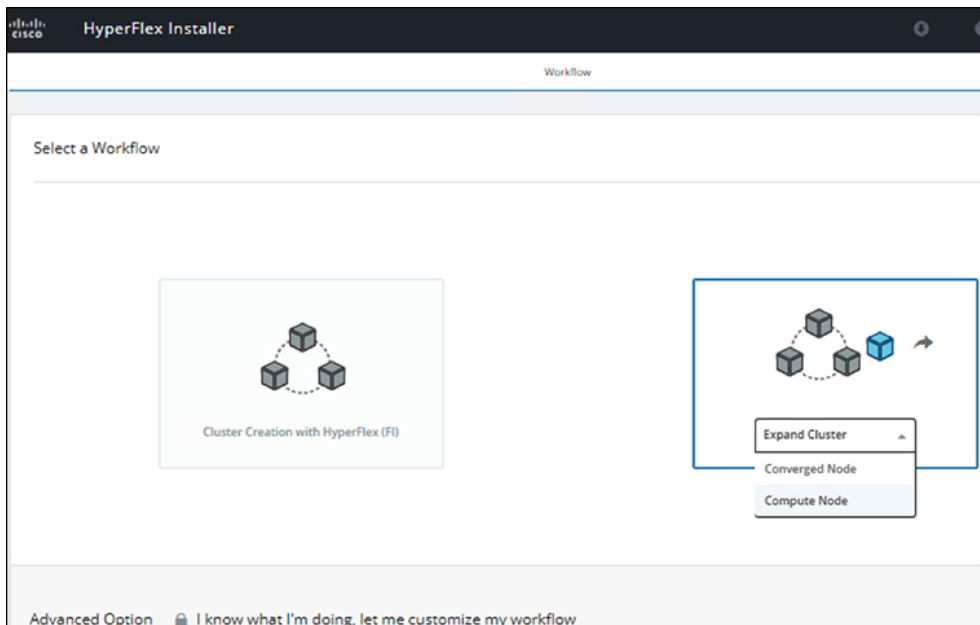
Step 4   In the **Select a Workflow** page, select **Expand HX Cluster**. Leave the **Is OS installed on the Node**, **Run Hypervisor Configuration** and **Deploy HX Software** checkboxes selected.

Select a Workflow

☑ Is OS installed on the Node

☐ Run UCS Manager Configuration

☑ Run Hypervisor Configuration

☑ Deploy HX Software

☐ Create HX Cluster | ☑ Expand HX Cluster

🔒 Show me the standard workflows   Continue

Step 5   In the **Warning** dialog box, click **Confirm and Proceed**.

Warning   ✕

You have selected a custom option that splits the installation or expansion workflow. You must complete all tasks in the workflow to ensure a working HX storage cluster.
If your nodes are data-at-rest encryption capable, custom installation is not supported.

Cancel to return to the standard workflow.
Confirm and Proceed to continue with a custom workflow.

Cancel   Confirm and Proceed

Step 6   In the **Cluster** page, complete the following fields:

Field	Description	Example Value
HX Cluster Management IP	The management IP address for the HX cluster	10.104.252.135
Cluster Admin User	Administrator username	admin
Password	Administrator password	
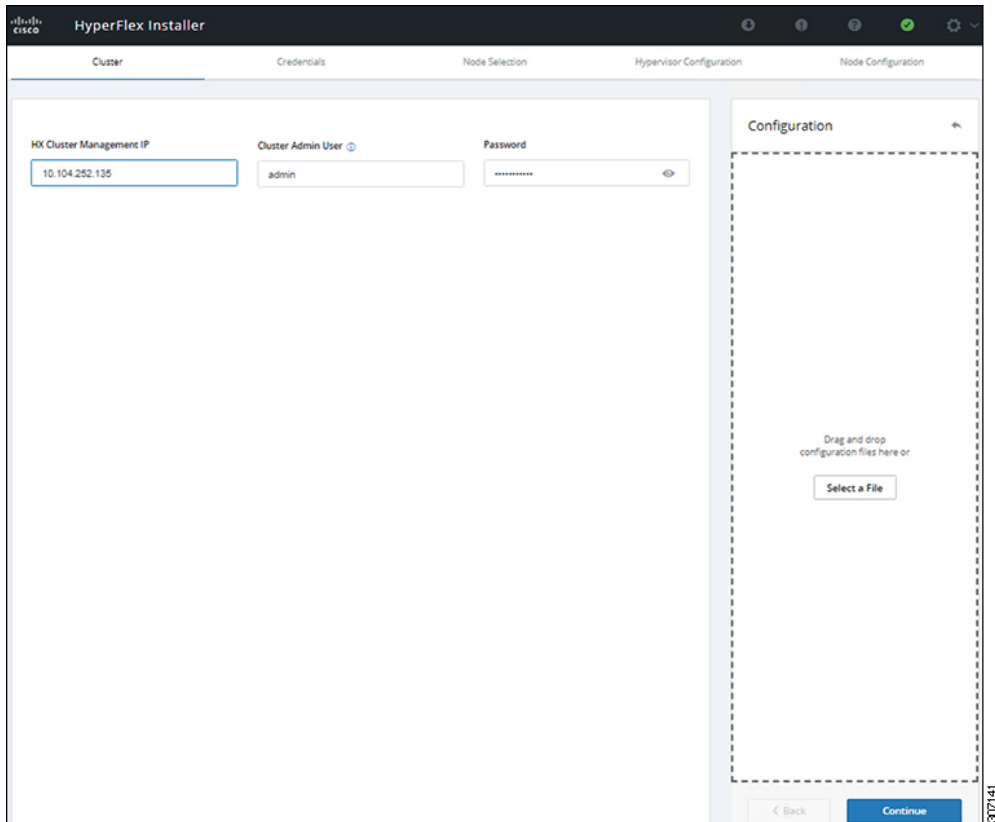
Step 7   In the **Credentials** page, complete the following fields:

Table 15: UCS Manager Credentials

Field		
UCS Manager Host Name	FQDN or the VIP address of UCSM.	
UCS Manager User Name	Admin user or a user with UCSM admin rights.	
Password	Password for the UCS Manager User Name.	

Table 16: Domain Information

Field		
HX Service Account	The HX service account that was created in the preinstallation phase.	hxadmin
Password	Password for the HX service account.	
Configure Constrained Delegation now (recommended) Constrained Delegation later	Select one of the checkboxes. Constrained Delegation is required for VM Live Migration.	

Use the following illustration as a reference for entering values in this screen.

Step 8 In the **Node Selection** page, choose all the servers that you want to install in the cluster and click **Continue.**

Step 9 In the **Hypervisor Configuration** page, complete the following fields for **VLAN Configuration**, **Hypervisor Settings**, and **Hypervisor Credentials**.

VLAN Configuration—HyperFlex needs to have at least 4 VLANs, each needs to be on different IP subnets and extended from the fabric interconnects to the connecting uplink switches, to ensure that traffic can flow from the Primary Fabric Interconnect (Fabric A) to the Subordinate Fabric Interconnect (Fabric B).

Use the following illustration as a reference for entering values in this screen.

Hypervisor Settings—If you leave the checkbox Make IP Addresses and Hostnames Sequential as checked then the installer will automatically fill the rest of the servers sequential from the first.

Hypervisor Credentials— Enter the Local administrator username on the Hyper-V hosts. Click **Continue**.

Step 10   In the **Node Configuration** page, complete the fields for **Hypervisor Settings** and **IP Addresses**.

Field	Description	Example Value
Subnet Mask	Subnet mask for the hypervisor hosts management network	255.255.255.0
Gateway	Default gateway for the hypervisor hosts management network	10.101.251.1
DNS Servers	Comma separated list for the DNS Servers in the AD that the hypervisor hosts are going to be member.	10.101.251.1

Use the following illustration as reference for entering values in this screen.

Click **Start** to begin the Hypervisor Configuration. The installation now continues and configures the Hypervisor hosts.

Step 11   In the **Warning** dialog box, click **Confirm and Proceed**.
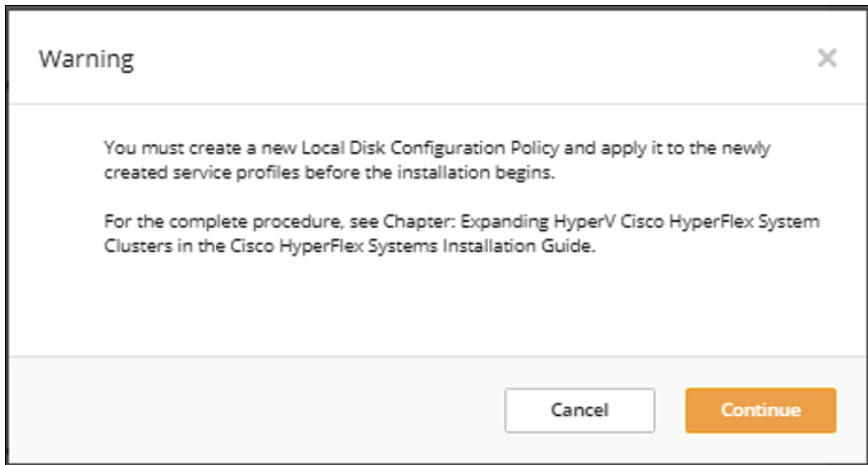
Step 12 The **Progress** screen displays the status of the hypervisor configuration and cluster expansion.
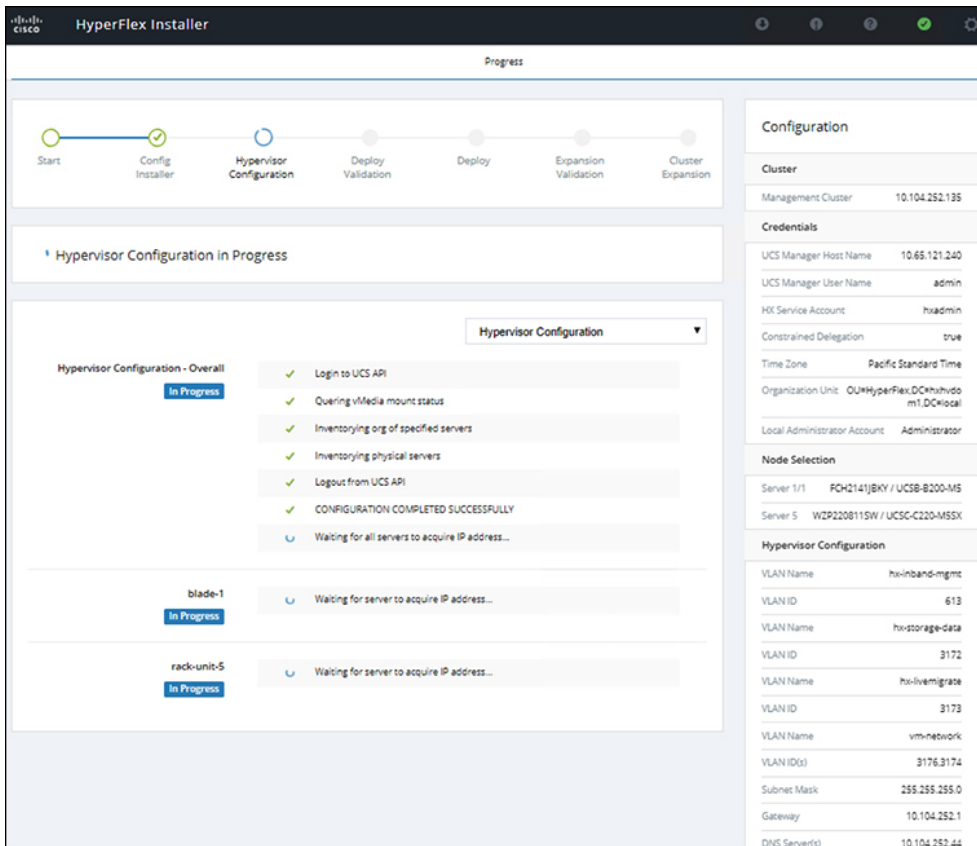
Step 13 When the process finishes successfully, the **Summary** page displays the completion status.

To log into HX Connect, click **Launch HX Connect**. The HX Connect **Dashboard** page displays cluster health, operational status and information for the newly added compute-only nodes in the cluster.

Cluster Expansion - M4 Blade Servers (Fibre Chanel SAN)

Overview

The Hyper-V cluster expansion procedure for **UCS B200 M4 blade servers with Fibre Channel** storage boot option consists of the following sequence of tasks:

5. Perform the following post installation steps:

Microsoft Windows OS Installation

This procedure is when you wish to expand your Hyper-V cluster by adding **UCS B200 M4 Blade servers (compute-only nodes)** and enable **Fibre Channel SAN** boot option.

Step 1 Launch UCS Manager and log in.

Step 2 **Perform the following steps to clone a Service Profile template:**

   a) In the Navigation pane, click **Servers**.

   b) Expand the node for the organization where you want to clone and select **Create a Clone**

   c) In the **Create Clone from Service Profile** dialog box, enter a name you to use for the new profile in the **Clone Name** field (Example: `hx-compute`. Click **OK**.

Step 3 **Perform the following steps to enable FC Zoning:**

   a) In the Navigation pane, go to **SAN** > **VSAN**.

   b) Ensure that the **Enabled** radio-button is selected under **FC Zoning**.

Step 4 Unbind your blade server from the current Service Profile template, and bind it to the newly created template in Step 2.

Step 5 Perform the following steps to mount the `HyperFlex Driver Image` file and modify the `autounattend.xml` file:

   a) Connect to your HX Installer VM and navigate to the shared folder that contains the Windows ISO and HyperFlex Driver Image files.

   b) Run the following commands to mount the HyperFlex image:

```
mkdir /mnt/hx-img
mount /var/www/localhost/images/latest.img /mnt/hx-img
```
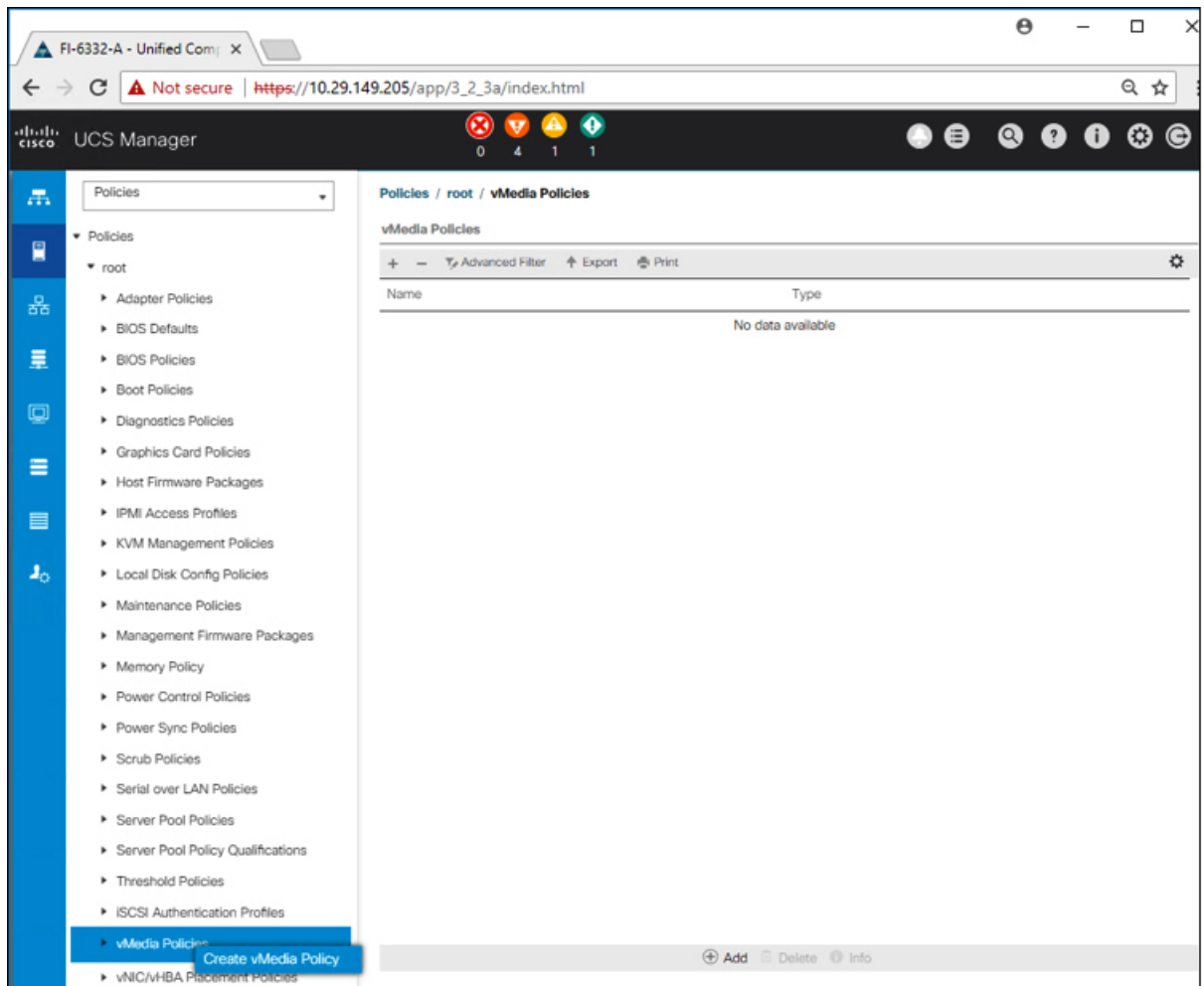
    c) Open the `autounattend.xml` file, search for DiskID and change the value from 0 to the value in Windows PE (WinPE).

Step 6   Perform the following steps to configure a SAN boot policy:

    a) Select the newly created Service Profile Template from Step 2 and go to the **Boot Order** tab. Click **Modify Boot Policy**. In the **Modify Boot Policy** page, click **Create Boot Policy**.

    b) Expand vHBAs, select **Add SAN Boot**, and in the name field, type the name of the vHBA(Example: hx-ext-fc-a).

    c) Select **Primary** and click **OK**.

    d) In the **Add SAN Boot Target**, leave the **Boot Target LUN** set to **0**. In the **Boot Target WWPN** field, type the WWPN from your storage array. Verify **Type** is set to **Primary** and click **OK**.

Step 7   **Create a vMedia policy for the Windows OS and Cisco driver images:**

    a) In the Navigation pane, click **Servers**.

    b) Expand **Servers** > **Policies** > **root** > **Sub-Organizations** > *hx-cluster_name* > **vMedia Policies**

    c) Right-click **vMedia Policies** and select **Create vMedia Policy HyperFlex**.

    d) In the **Create vMedia Policy** dialog box, complete the following fields:

Field Name	Description
Name	The name of the vMedia policy. For example, *HX-vMedia*. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description	A description of the policy. We recommend including information about where and when the policy should be used. Maximum 115 characters.
Retry on Mount Failure	Designates if the vMedia will continue mounting when a mount failure occurs. This can be: • **Yes** • **No** **Note** The default setting is **Yes**. When **Yes** is selected the remote server will continue to try to mount the vMedia mount process until it is successful or you disable this option. If you select No, a warning message will appear indicating retry on mount failure will not work in case of mount failure.

Refer to the following screenshot as an example:

e) On the icon bar under the **vMedia Mounts** pane, click + **Add**. In the **Create vMedia Mount** dialog box, complete the following fields:

Field Name	Description	Example Value
Name	Name for the mount point.	Windows-ISO
Description	Can be used for more information.	Windows Server 2016 image
Device Type	Type of image that you want to mount. This can be: • **CDD**—Scriptable vMedia CD. • **HDD**—Scriptable vMedia HDD.	CDD
Protocol	The protocol used for accessing the share where the ISO files are located.	HTTP
Hostname/IP Address	IP address or FQDN of the server hosting the images.	10.101.1.92
Image Name Variable	This value is not used in HyperFlex installation.	None
Remote File	The filename of the ISO file that you want to mount.	
Remote Path	The path on the remote server to where the file resides	
Username	If you use CIFS or NFS a username might be necessary	
Password	If you use CIFS or NFS a password might be necessary	

Refer to the screenshot below as an example:

f) Click **OK**. When you click **OK**, you will now be returned to the **vMedia Policies** screen, and you should see the information that you just submitted.

g) Repeat **Steps 2e and 2f**, however, change the type to **HDD** and the remote file name to the **Cisco HyperFlex driver image**.

h) At the end of this step, the two vMedia mounts will be listed in the Create vMedia Policy screen as shown in the following screenshot:

Step 8   **Associate the vMedia Policy to a Service Profile**:

a)   In the Navigation pane, select **Servers** > **Service Profile Templates** > **root** > **Sub-Organizations** > *hx-cluster_name* > **Service Template** *compute-nodes, or compute-nodes-m5*

b) Click the **vMedia Policy** tab. Then, click **Modify vMedia Policy**

c) Choose the **vMedia Policy** that you created earlier from the drop-down selection, and click **OK** twice.

d) Under the **General** tab, verify that the vMedia policy is added to the Service Profile.

Step 9   **Modify Boot Policy and set the boot order to have CIMC CD/DVD to the list:**

a) In the Navigation pane, click the **Servers** tab.

b) Expand **Servers** > **Policies** > **root** > > **Boot Policies** > *hx-compute, or hx-compute-m5*
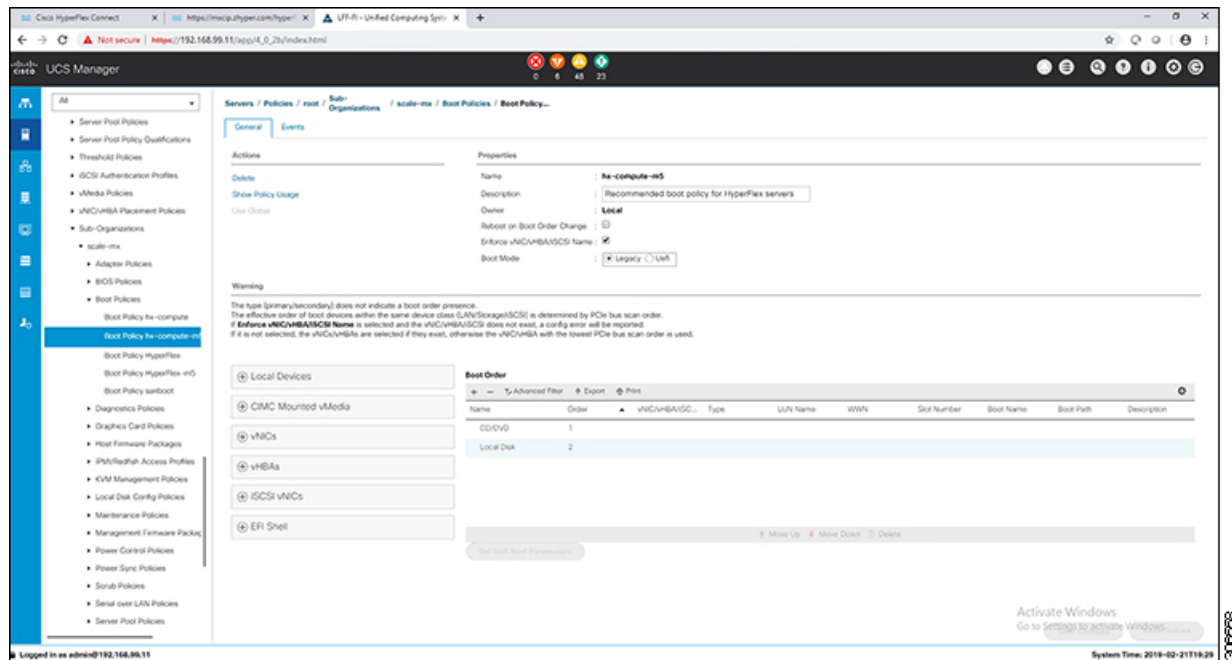
c) **(For M5 Servers only)** In the **Boot Order** configuration pane, click **CIMC Mounted CD/DVD** . Then, click **Add CIMC Mounted CD/DVD** to add this to the boot order. Move it to the top of the boot order using the **Move up** button.

> **Important**   The **CIMC Mounted CD/DVD** option must be highest in the boot order preceding the other options, **Embedded Local Disk** and **CD/DVD**.

(For M4 Servers with Local SAS Drivers) In the **Boot Order** configuration pane, click **vHBAs**. Then, click **Add SAN Boot** to add this to the boot order.

d) Click **Save Changes**, and click **OK** in the **Success** dialog box. The modified boot policy is saved.

Step 10   **Verify successful vMedia mounting:**

a) On the **Equipment** tab, select one of the servers.

b) Click **Inventory** > **CIMC**, scroll down and ensure for mount entry #1(OS image) and mount entry #2 (Cisco HyperFlex driver image) you see status as **Mounted** and there are no failures.

c) In the menu bar, click **Servers** and choose the first HyperFlex service profile.

d) Click the **General tab** and choose **Actions** > **KVM Console>>**.

Note   The KVM console will try to open in a new browser. Be aware of any pop-up blockers. Allow the pop-ups and re-open the KVM

e) Reboot the host, launch the KVM Console, and power on the server to monitor the progress of the Windows installation. You should see the **Loading Files** screen appear. Windows should install automatically without user intervention. You should see a blue screen and within a few moments you should see the **Setup is starting** message. If automated installation does not begin, double-check that both images are mounted to the server.

f) Once Windows installation completes, a command prompt will show up. Wait for the installation to complete. The host will then reboot a few times. The installation is complete when you get a clear command prompt at `c:\users\administrator>`. It may take several minutes and reboot operations for the Driver Image to be copied and installed.

Note   Ignore the prompt with the **The system cannot find the file specified** message.

Important   Ensure that you have completed **Steps e and f,** on ALL servers that will be part of the HX cluster.

g) Log into each server, enter the command `C>Users>Administrator>Get-ScheduledTask` and verify that the HX Install Bootstrap Launcher task is running.

Step 11   **Remove the vMedia policy from the service profile:**

a) To un-map the vMedia policy from the service profile, go to **Servers** > **Service Profile Templates** > **root** > **Sub-Organizations** > *hx-cluster_name* > **Service Template** *compute-nodes, or compute-nodes-m5*. Then, click on **Modify vMedia Policy**.

b) Under the vMedia Policy drop-down selection, deselect the vMedia policy (*HX-vMedia*) previously used to map the two images.

Step 12   **Restore the boot order to the one before installation:**

a) In the Navigation pane, click the **Servers** tab.

b) Expand **Servers** > **Policies** > **root** > > **Boot Policies** > *hx-compute, or hx-compute-m5*

c) In the **Boot Order** configuration pane, use the **Move Down** button to move **CIMC Mounted CD/DVD** option to the bottom of the list.

Refer to the screenshot below for the boot order after it is restored in this step:
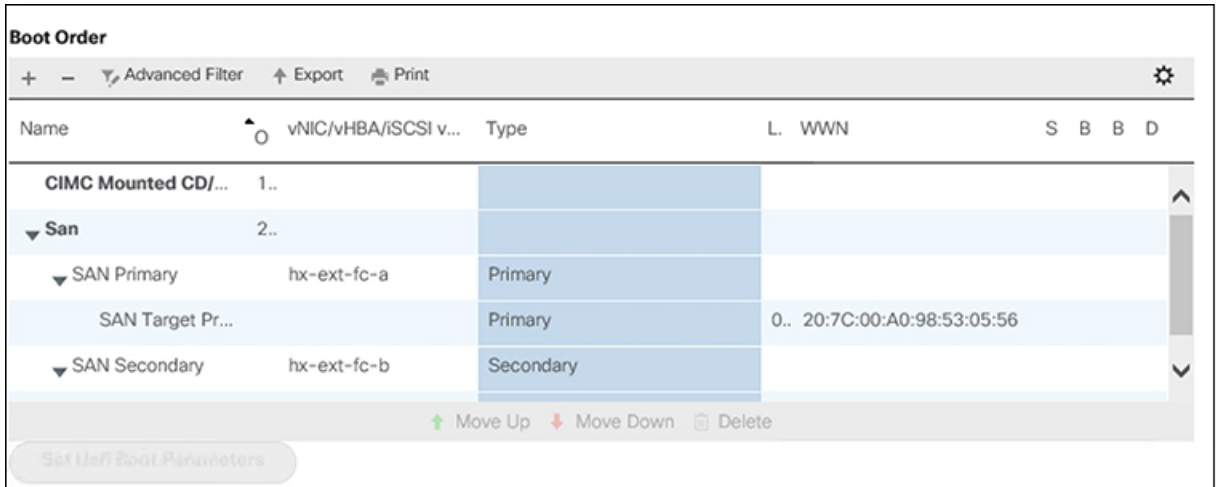
What to do next

At the end of this procedure, Windows OS is successfully installed. Then, continue to "Hypervisor Configuration, HXDP Software Installation and Cluster Expansion" to complete the remaining steps in the cluster expansion workflow.

Troubleshooting Information

• Troubleshooting, on page 105

Troubleshooting

This section contains troubleshooting information for issues seen during Hyper-V deployment.

Symptom or Scenario	Workaround or Recommendation
Cisco HX Release 4.5(x) installations with UCSM 4.1.2a and 4.1.2b are not supported.	Use UCSM 4.0.4i with a new Cisco HyperFlex System installation for Hyper-V, Release 4.5.
During cluster expansion deployment, one node fails with the following error message: `failed in Task:'Enable And Run Scheduled Tasks' with Error` The "retry deploy" did not work and the same node fails again. The Windows error logs also indicate that: "`You don't have administrator privileges on the server`", even though this node actually has the privileges.	Reboot the failed node or log out and log back in.
File Witness Share is not configured.	Create a File Witness Share and configure it as a Witness Share in Failover Cluster Manager (FCM). It is recommended that you not use the Witness Share created for anything else.
Waiting for Storage Controller VM (SCVM) times out.	• Set the VLAN ID manually and retry, or, • Delete the controller VM and retry.
HX Installer fails to join computers to the domain due to incorrect Active Directory credentials to HX Installer.	Restart the HX Installer in the "Deploying HX Data Platform Installer and Cluster Configuration" phase in installation, and provide the correct credentials.

Symptom or Scenario	Workaround or Recommendation
Unreliable per node statistics displayed for a node in the duration when any of controller VMs are down in the cluster.	Use Windows side counters during the time when any of the controller VMs are down.
The FQDN address for HX Connect may be inaccessible after successful cluster installation.	The default Internet Explorer security setting on Windows 2008 prevents HX Connect accessibility with the FQDN name. As a workaround, try one of the following: • Modify the Internet Explorer setting. • Use an IP address. • Use other supported browsers such as Chrome or Firefox.
For compute-only nodes, performance charts are unavailable in the HX Connect Dashboard page.	This is a l only node.
Windows installation failed with the following error: `Could not detect system partition.` In addition, `setupact.log` shows that the setup could not detect any available disk as a valid boot device.	1. Switch the boot policy to Embedded Disk (Any). 2. For the Service Profile or Service Profile Template use a boot policy that mirrors `hx-nodes-m5` than `compute-nodes-m5`.
Migration failed due to incompatible processors.	A cluster may not have a combination of different CPU types.

CHAPTER 9

Appendix

Rack Cisco HyperFlex Nodes

For details on the HyperFlex cluster and node limits, see **Cisco HX Data Platform Storage Cluster Specifications** in the latest version of the Release Notes for Cisco HX Data Platform.

For details on the installation of Cisco HyperFlex nodes, refer to respective links from the following table:

Type of Node To Be Installed	Reference
Converged Nodes	
HyperFlex HX220c M5 Nodes	Cisco HyperFlex HX220c M5 Node Installation Guides
HyperFlex HX240c M5 Nodes	Cisco HyperFlex HX240c M5 Node Installation Guides

Note Hyper-V is only supported on M5 servers.

Setting Up the Fabric Interconnects

Configure a redundant pair of fabric interconnects for high availability. Connect the two fabric interconnects directly using Ethernet cables between the L1 and L2 high availability ports. Connect Port L1 on fabric interconnect A to port L1 on fabric interconnect B, and Port L2 on fabric interconnect A to port L2 on fabric interconnect B. This allows both the fabric interconnects to continuously monitor the status of each other.

Verify and obtain the following information before connecting the fabric interconnects.

Item	Description
Verify the physical connections of the fabric interconnects.	• Console port for the first fabric interconnect must be physically connected to a computer or console server. • Management Ethernet port (mgmt0) must be connected to an external hub, switch, or router. • L1 ports on both the fabric interconnects must be directly connected to each other. • L2 ports on both the fabric interconnects must be directly connected to each other.
Verify console port parameters on the computer terminal.	• 9600 baud • 8 data bits • No parity • 1 stop bit
Obtain information for initial setup.	Collect the following information for initial setup: • System name • Password for admin account • Three static IP addresses • Subnet mask for three static IP addresses • Default gateway IP address • DNS server IP address • Domain name for the system

Both fabric interconnects must go through the same setup process. Set up the primary fabric interconnect and enable for cluster configuration. When you use the same process to set up the secondary fabric interconnect, it detects the first fabric interconnect as a peer.

Configure the Primary Fabric Interconnect Using GUI

You can either follow the procedure below for configuring the primary fabric interconnect or watch Cisco UCS Manager Initial Setup part 1.

⚠️

Attention   IPv4 addressing is required for HyperFlex.

Step 1   Power up the fabric interconnect.
You will see the power on self-test messages as the fabric interconnect boosts.

Step 2   If the system obtains a lease, go to step 6, otherwise, continue to the next step.

Step 3   Connect to the console port.

Step 4   At the installation method prompt, enter `gui`.

Step 5   If the system cannot access a DHCP server, you are prompted to enter the following information:

- IPv4 address for the management port on the fabric interconnect.

- IPv4 subnet mask for the management port on the fabric interconnect.

- IPv4 address for the default gateway assigned to the fabric interconnect.

Step 6   Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 7   On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 8   On the **Express Setup** page, select **Initial Setup** and click **Submit**.

Step 9   In the **Cluster and Fabric Setup** area:

a) Click the **Enable Clustering** option.

b) For the **Fabric Setup** option, select **Fabric A**.

c) In the **Cluster IP Address** field, enter the IPv4 address that Cisco UCS Manager will use.

Step 10   In the **System Setup** area, complete the following fields:

Field	Description
System Name field	The name assigned to the Cisco UCS domain.
	In a standalone configuration, the system adds "-A" to the system name. In a cluster configuration, the system adds "-A" to the fabric interconnect assigned to fabric A, and "-B" to the fabric interconnect assigned to fabric B.
Admin Password field	The password used for the Admin account on the fabric interconnect.
	Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
Confirm Admin Password field	The password used for the Admin account on the fabric interconnect.
Mgmt IP Address field	The static IPv4 address for the management port on the fabric interconnect.
Mgmt IP Netmask field or **Mgmt IP Prefix** field	The IPv4 subnet mask prefix for the management port on the fabric interconnect.
	Note The system prompts for a **Mgmt IP Netmask** or a **Mgmt IP Prefix** based on what address type you entered in the **Mgmt IP Address** field.
Default Gateway field	The IPv4 address for the default gateway assigned to the management port on the fabric interconnect.
	Note The system prompts for a **Default Gateway** address type based on what type you entered in the **Mgmt IP Address** field.

Field	Description
DNS Server IP field	The IPv4 address for the DNS Server assigned to the fabric interconnect.
Domain Name field	The name of the domain in which the fabric interconnect resides.

Step 11   Click **Submit**.
A page displays the results of your setup operation.

Configure the Subordinate Fabric Interconnect Using GUI

You can either follow the procedure below for configuring the subordinate fabric interconnect or watch Cisco UCS Manager Initial Setup part 2.

Step 1   Power up the fabric interconnect.
You will see the power-up self-test message as the fabric interconnect boots.

Step 2   It the system obtains a lease, go to step 6, otherwise, continue to the next step.

Step 3   Connect to the console port.

Step 4   At the installation method prompt, enter `gui`.

Step 5   If the system cannot access a DHCP server, you are prompted to enter the following information:

- IPv4 address for the management port on the fabric interconnect

- IPv4 subnet mask for the management port on the fabric interconnect

- IPv4 address for the default gateway assigned to the fabric interconnect

Step 6   Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 7   On the Cisco UCS Manager GUI launch page, select **Express Setup**.

Step 8   On the **Express Setup** page, select **Initial Setup** and click **Submit**.

The fabric interconnect should detect the configuration information for the first fabric interconnect.

Step 9   In the **Cluster and Fabric Setup** Area:
a)   Select the **Enable Clustering** option.
b)   For the **Fabric Setup** option, make sure **Fabric B** is selected.

Step 10   In the **System Setup** Area, enter the password for the Admin account into the **Admin Password of Master** field.
The **Manager Initial Setup** Area is displayed.

Step 11   In the **Manager Initial Setup** Area, complete the following:

Field	Description
Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address field	Enter an IPv4 address for the Mgmt0 interface on the local fabric interconnect.

Step 12   Click **Submit**.

A page displays the results of your setup operation.

# How to upload the iso and img file to the installer VM using WinSCP

You may choose to use the Installer VM as host for the ISO and IMG files to install Hyper-V. To accomplish that you need to upload the Windows ISO and the Cisco HyperFlex driver image to the installer.

For the purpose of this guide we will use WinSCP, you can use whatever SCP client you have available.

Step 1 Download a SCP client for Windows. It could be WinSCP (https://winscp.net/eng/download.php) and install it on your workstation.

Step 2 Connect to your installer VM from WinSCP. Username **root** and password **Cisco123**

Important Systems ship with a default password of Cisco123 that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.
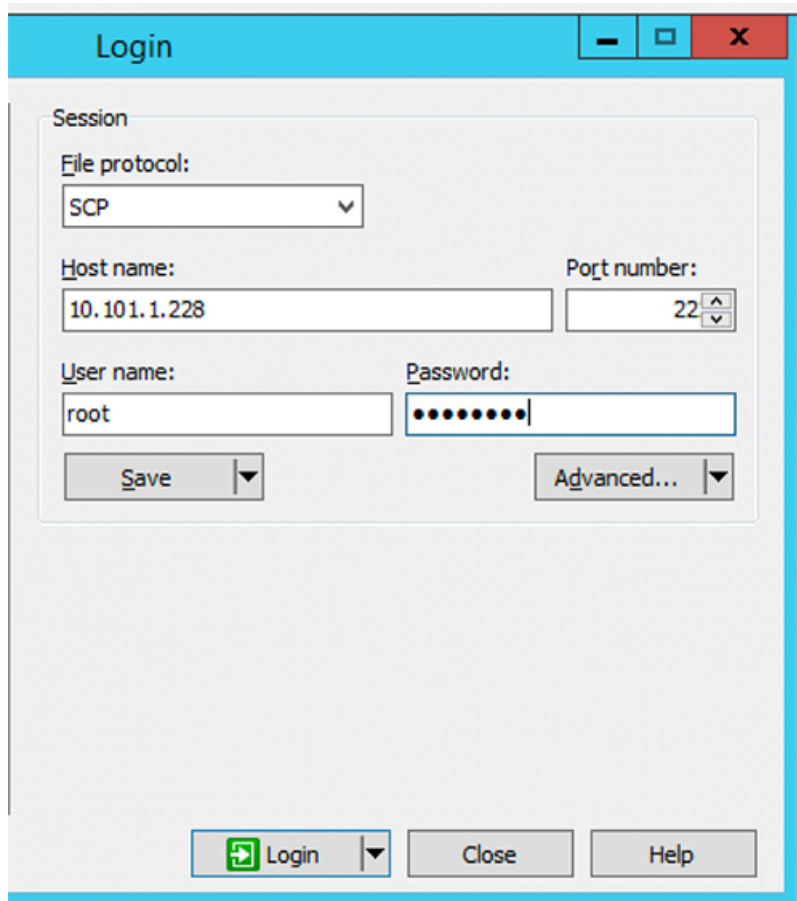
Step 3   Accept the key and add to the cache.
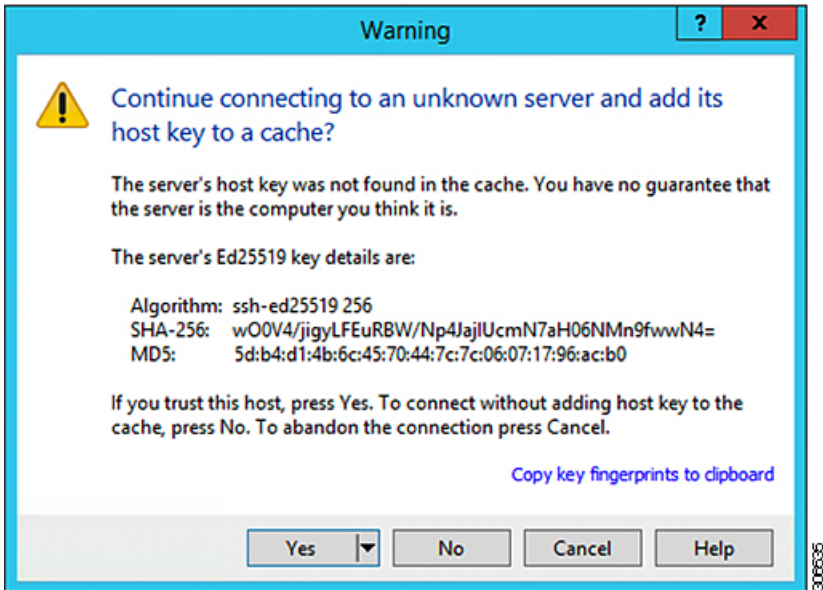
Step 4   Once connected browse to the folder **/var/www/localhost/images/** on the installer. Browse to where to local files are located on your machine.

Step 5   Transfer the files. File names can be copied if you access the URL in a browser: *http://<controller_IP>/images/*
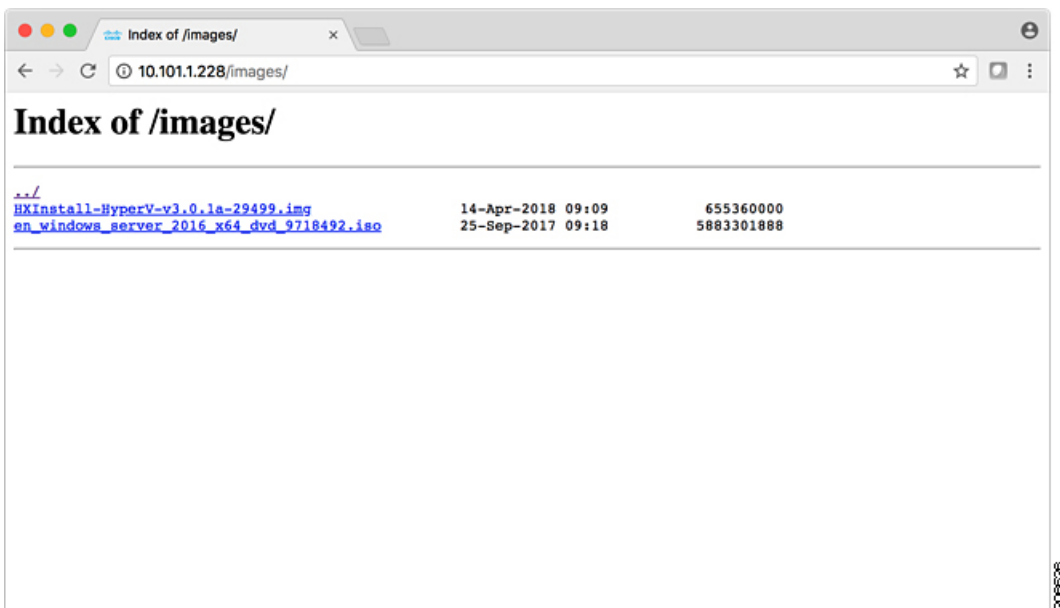
DNS Records

Refer to the list below for the DNS records that must be added to your environment.

Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "-CNTL" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "-CNTL" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "-CNTL" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername
Add-DnsServerResourceRecordA -Name "-CNTL" -ZoneName "Ciscolab.dk" -AllowUpdateAny -IPv4Address "" -TimeToLive 01:00:00 -CreatePtr -computername

Updating HX Service Account Username and Password

A new password must be updated within an HX Cluster if the password expired or was changed voluntarily. Perform the following step to update the Cisco HX Service Account Password.

Note The access to VMs and datastores will still continue to work without the new password. However, the cluster will experience some issues with the Alert, Systems Status, Support Bundle and Datastore Access reporting.

Before you begin

Ensure that the Cisco HX Service Account User Name is in the following format:

```
username@domain.com
```

Step 1   Run the `resethypervcred -u` command from one of the Storage Controller node within the cluster.

Example:

The following is an example of the command with sample output:

```
root@cvmhv1:~# resethypervcred -u
Enter service admin name:<hx-service-account>@domain.com
Enter service admin passwd:
Enter local admin name:administrator
Enter local admin passwd:
Hyperv creds updated successfully
```

Log into each controller vm as the root user and run **restart hxHyperVSvcMgr**.

After you have completed the reset and service restarts, then log into **HX Connect** as the HX Service Account User to verify your login works and HX Connect is displaying the cluster information.

Step 2   To change the HX Service Account username, run the `resethypervcred -u` command.

Example:

```
root@cvmhv1:~# resethypervcred -u
Enter service admin name:hxadmin@domain.com
Enter service admin passwd:
Enter local admin name:administrator
Enter local admin passwd:
Hyperv creds updated successfully
```