Post Installation

- Post Installation Tasks Summary, on page 1

Post Installation Tasks Summary

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the First Datastore</td>
<td>Create the First Datastore, on page 1</td>
</tr>
<tr>
<td>Assign a static IP address for Live Migration and VM Network</td>
<td>Configuring a Static IP Address for Live Migration and VM Network, on page 3</td>
</tr>
<tr>
<td>(Optional) Constrained Delegation</td>
<td>(Optional) Post Installation Constrained Delegation, on page 4</td>
</tr>
<tr>
<td>Configure Local Default Paths</td>
<td>Configure Local Default Paths, on page 5</td>
</tr>
<tr>
<td>Configure File Share Witness</td>
<td>Configuring a File Share Witness, on page 6</td>
</tr>
<tr>
<td>Checking the Windows Version on the Hyper-V Host</td>
<td>Checking the Windows Version on the Hyper-V Host, on page 11</td>
</tr>
<tr>
<td>Deploying VMs on a Hyper-V cluster</td>
<td>Deploying VMs on a Hyper-V cluster, on page 11</td>
</tr>
<tr>
<td>Configuring HyperFlex Share to SCVMM</td>
<td>Configuring HyperFlex Share to SCVMM, on page 17</td>
</tr>
<tr>
<td>Re-enabling Windows Defender</td>
<td>Re-enabling Windows Defender, on page 19</td>
</tr>
</tbody>
</table>

Create the First Datastore

Before you begin using the cluster, you must create a datastore. The datastore can be created in HX Connect UI.
Procedure

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore Name</td>
<td>Enter a name for the datastore. Cisco recommends that you use all lower case characters for the datastore name.</td>
</tr>
<tr>
<td>Size</td>
<td>Select the size for the datastore.</td>
</tr>
<tr>
<td>Block Size</td>
<td>Select the block size for the datastore.</td>
</tr>
</tbody>
</table>

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 in to each Hyper-V node and execute the following commands in Power Shell to assign a static IP address for Live Migration and VM Network.
(Optional) Post Installation Constrained Delegation

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.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click Start, click Administrative Tools, and then click Active Directory Users and Computers.</td>
</tr>
<tr>
<td>2</td>
<td>Expand domain, and then expand the Computers folder.</td>
</tr>
<tr>
<td>3</td>
<td>In the right pane, right-click on the computer name (for example, HX-Properties), and then click Properties.</td>
</tr>
<tr>
<td>4</td>
<td>Click on the Delegation tab.</td>
</tr>
<tr>
<td>5</td>
<td>Select Trust this computer for delegation to specified services only.</td>
</tr>
<tr>
<td>6</td>
<td>Ensure that Use any authentication protocol is selected.</td>
</tr>
<tr>
<td>7</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

```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
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).

**Procedure**

**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.

**Procedure**

**Step 1**
Login to 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

**Step 4**
In addition, verify the following:

- The UBR # should be greater than 1884. If not, upgrade the HyperV servers to the latest update. Refer to the *Microsoft Knowledge Base article: KB4467691*.
- The Hyper-V management server should have a version UBR # greater than 1884. You must upgrade the Hyper-V management server if the version is 1884 or lower.

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 11.

- **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 16, or *Creating VMs using Failover Cluster Manager*, on page 16

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.

Procedure

**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**.

**Post Installation**

Install RSAT tools on the Management Station or Host
**Step 5**  
In the Select Roles page, click Next.

**Step 6**  
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.

Procedure

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 16
Creating VMs using Hyper-V Manager

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

Procedure

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.

Procedure

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**.

---

**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.

**Procedure**

**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
```
Re-enabling Windows Defender