THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)
CONTENTS

Full Cisco Trademarks with Software License iii

CHAPTER 1

New and Revised Information 1

Chapter 1: New and Revised Information 1

CHAPTER 2

HX Storage Cluster Overview 5

Chapter 2: HX Storage Cluster Overview 5

CXSO HX Data Platform Overview 5

Storage Cluster Physical Components Overview 5

HX Data Platform Capacity Overview 7

Understanding Capacity Savings 8

Storage Capacity Event Messages 9

HX Data Platform High Availability Overview 10

Storage Cluster Status 10

Operational Status Values 10

Resiliency Status Values 11

HX Data Platform Cluster Tolerated Failures 11

Data Replication Factor Settings 13

Cluster Access Policy 13

Responses to Storage Cluster Node Failures 14

HX Data Platform ReadyClones Overview 18

HX Data Platform Native Snapshots Overview 18

CHAPTER 3

Logging in to HX Data Platform Interfaces 19

Chapter 3: Logging in to HX Data Platform Interfaces 19

HyperFlex Cluster Interfaces Overview 19
Secure Erase an Encrypted Disk 74
Remote Key Management 74
Configuring Remote Encryption Key 74
Generating Certificate Signing Requests 75
Configuring a Key Management Server Using CSRs (Certificate Signing Requests) 77
Generating Self-Signed Certificates 78
Configuring a key management server using SSCs (Self-Signed Certificates) 79
Start Over Encryption 80

CHAPTER 8
Managing Datastores 81
Managing Datastores 81
Adding Datastores 82
Editing Datastores 82
Mounting Datastores 83
Unmounting Datastores 83
Deleting Datastores 84
Recovering from Partially Unmounted Datastores 85

CHAPTER 9
Managing Disks 87
Managing Disks in the Cluster 87
Disk Requirements 87
Replacing Self Encrypted Drives (SEDs) 91
Replacing SSDs 93
Replacing NVMe SSDs 94
Replacing Housekeeping SSDs 95
Replacing or Adding Hard Disk Drives 96

CHAPTER 10
Managing Nodes 99
Managing Nodes 99
Identify Node Maintenance Methods 101
Searching by DNS Address or Host Name 103
Changing ESXi Host Root Password 104
Reinstalling Node Software 104
Changing Node Identification Form in vCenter Cluster from IP to FQDN 104
Replacing Node Components 106
Removing a Node 107
  Preparing to Remove a Node 108
  Removing a Node from an Online Storage Cluster 110
  Removing a Node from an Offline Storage Cluster 112
Replacing a Node 114

CHAPTER 11 Managing HX Controller VMs 119
Managing Storage Controller VMs 119
Powering On or Off Storage Controller VMs 119

CHAPTER 12 Managing ReadyClones 121
HX Data Platform ReadyClones Overview 121
Benefits of HX Data Platform ReadyClones 121
Supported Base VMs 122
ReadyClone Requirements 122
ReadyClone Best Practices 123
Creating ReadyClones Using HX Connect 123
Creating ReadyClones Using the HX Data Platform Plug-In 124
Prepare to Customize HX Data Platform ReadyClones 126
  Creating a Customization Specification for Linux in the vSphere Web Client 126
  Create a Customization Specification for Windows in the vSphere Web Client 126
Configuring ReadyClones Using Customized Specifications 127
Managing Virtual Machine Networking 127

CHAPTER 13 Managing Native Snapshots 129
HX Data Platform Native Snapshots Overview 129
Benefits of HX Data Platform Native Snapshots 129
Native Snapshot Considerations 131
Native Snapshot Best Practices 132
Understanding SENTINEL Snapshots 133
Native Snapshot Timezones 133
Creating Snapshots 134
Scheduling Snapshots Overview 135
Scheduling Snapshots  136
Setting the Frequency of Scheduled Snapshots  136
Deleting Snapshot Schedules  137
Reverting to a Snapshot  137
Deleting Snapshots  138

CHAPTER 14
Managing Virtual Machine Disaster Recovery  139
Data Protection Overview  139
   Replication and Recovery Considerations  140
   Data Protection Terms  141
Protecting Virtual Machines Overview  142
   Data Protection Workflow  143
   Configuring the Replication Network  144
      Editing the Replication Network  145
   Replication Pair Overview  146
      Creating a Replication Pair  146
      Editing a Replication Pair  148
      Deleting a Replication Pair  148
   Creating a Protection Group  149
      Editing Protection Groups  151
      Deleting Protection Groups  151
   Protecting Virtual Machines with an Existing Protection Group  152
   Protecting Virtual Machines with a New Protection Group  153
   Protecting Individual Virtual Machines  155
   Unprotecting Virtual Machines  156
VM Migration Overview  157
   Migrating Protected Virtual Machines  157
   Migrating Virtual Machines in Protection Groups  159
Data Protection Recovery Workflow  161
   Testing Virtual Machine Recovery  162
   Recovering Virtual Machines  164
      Recovering Virtual Machines in Protection Groups  166
Replication Maintenance Overview  169
   Pausing Replication  170
CHAPTER 15

Managing Users 173

Managing HyperFlex Users Overview 173
User Management Terms 174
Audit Logs for AAA Accounting 175
Creating HX Data Platform RBAC Users 175
Assigning Users Privileges 176
New and Changed Information

- New and Revised Information, on page 1

New and Revised Information

The following table provides an overview of the new features and changes made to this guide for this current release.

**Table 1: New Features in HX Release 2.6**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date Added</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>M5 disks with SED</td>
<td>Support for additional drives with SED.</td>
<td>12/18/2017</td>
<td>See Disk Requirements, on page 87</td>
</tr>
<tr>
<td>M5 disks</td>
<td>Support for additional drives.</td>
<td>09/26/2017</td>
<td>See Disk Requirements, on page 87</td>
</tr>
</tbody>
</table>

**Table 2: New Features in HX Release 2.5**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date Added</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Software support only for data at rest encryption.</td>
<td>07/24/2017</td>
<td>See Managing Encryption, on page 71</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Replication and recovery of data for protected virtual machines.</td>
<td>07/24/2017</td>
<td>See Managing Encryption, on page 71</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role based user access. Administrator and Read Only user permission roles.</td>
<td>07/24/2017</td>
<td>See Managing Users, on page 173</td>
</tr>
<tr>
<td>HX Connect</td>
<td>New HTML5 user interface including support for new features encryption and data protection.</td>
<td>07/24/2017</td>
<td>See Logging into HX Connect, on page 24</td>
</tr>
<tr>
<td>NMVe Disks</td>
<td>Support NMVe disks for cache in All Flash systems</td>
<td>07/24/2017</td>
<td>See Replacing NVMe SSDs, on page 94</td>
</tr>
</tbody>
</table>
### Table 3: New Features in HX Release 2.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date Added</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>SED</td>
<td>Hardware support only for data at rest encryption.</td>
<td>04/20/2017</td>
<td>Disk Requirements, on page 87</td>
</tr>
</tbody>
</table>

### Table 4: New Features in HX Release 2.0

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date Added</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Flash servers</td>
<td>Servers with SSD for persistent storage.</td>
<td>3/06/2017</td>
<td>See Managing Disks in the Cluster, on page 87</td>
</tr>
<tr>
<td>Post maintenance</td>
<td>Topic providing reference to UCS Manager documentation for networking VMs.</td>
<td>03/17/17</td>
<td>See Managing Virtual Machine Networking, on page 127</td>
</tr>
<tr>
<td>Reorganize chapters</td>
<td>Split Maintaining Storage Cluster into chapters for each managed component: cluster, hosts, controller VM, datastores, disks. Split Expanding the Cluster into chapters for ReadyClones and Snapshots.</td>
<td>3/06/17</td>
<td>See Contents.</td>
</tr>
</tbody>
</table>

### Table 5: New Features in HX Release 1.8

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date Added</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity events</td>
<td>Updated capacity event message descriptions</td>
<td>02/08/2017</td>
<td>See Cisco HyperFlex Systems Troubleshooting Guide</td>
</tr>
<tr>
<td>Added new topics</td>
<td>Guidelines for HX Data Platform Login Credentials</td>
<td>11/21/2016</td>
<td>See and Managing Datastores, on page 81</td>
</tr>
<tr>
<td></td>
<td>Powering On or Off Storage Controller VMs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovering from Partially Unmounted Datastores</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New guide name</td>
<td>The 1.7 Administration guide has been restructuring and renaming to the Management guide.</td>
<td>9/30/2016</td>
<td>See entire guide.</td>
</tr>
<tr>
<td>Node remove and replace</td>
<td>User can perform some cluster node remove and replace tasks without TAC assist.</td>
<td>9/30/2016</td>
<td>See Managing Nodes, on page 99.</td>
</tr>
<tr>
<td>Storage cluster status</td>
<td>Status now under Resiliency and Operational Status.</td>
<td>9/30/2016</td>
<td>See Storage Cluster Status, on page 10</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date Added</td>
<td>Where Documented</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Storage cluster events</td>
<td>Selected events are automatically acknowledged when resolution event occurs.</td>
<td>9/30/2016</td>
<td>See Cisco HyperFlex Systems Troubleshooting Guide</td>
</tr>
<tr>
<td>Snapshots and ReadyClones</td>
<td>Improved node failure tolerance.</td>
<td>9/30/2016</td>
<td>See HX Data Platform ReadyClones Overview, on page 18 and HX Data Platform Native Snapshots Overview, on page 18</td>
</tr>
<tr>
<td>Preparation for cluster maintenance</td>
<td>Documentation change, improved task description.</td>
<td>9/30/2016</td>
<td>See Storage Cluster Maintenance Operations Overview, on page 45</td>
</tr>
<tr>
<td>Generating support bundles</td>
<td>Documentation change, added task description.</td>
<td>9/30/2016</td>
<td>See Cisco HyperFlex Systems Troubleshooting Guide</td>
</tr>
</tbody>
</table>
Cisco HX Data Platform Overview

Cisco HyperFlex Data Platform (HX Data Platform) is a hyperconverged software appliance that transforms Cisco servers into a single pool of compute and storage resources. It eliminates the need for network storage and enables seamless interoperability between computing and storage in virtual environments. The Cisco HX Data Platform provides a highly fault-tolerant distributed storage system that preserves data integrity and optimizes performance for virtual machine (VM) storage workloads. In addition, native compression and deduplication, reduce storage space occupied by the VMs and VM workloads.

Cisco HX Data Platform has many integrated components. These include: Cisco Fabric Interconnects (FIs), Cisco UCS Manager, Cisco HX specific servers, and Cisco compute only servers; VMware vSphere, ESX servers, and vCenter; and the CiscoHX Data Platform Installer, controller VMs, HX Connect, vSphere HX Data Platform Plug-in, and stcli commands.

Cisco HX Data Platform is installed on a virtualized platform such as VMware vSphere. During installation, you specify the Cisco HyperFlex HX Cluster name, and the HX Data Platform creates a hyperconverged storage cluster on each of the nodes. As your storage needs increase and you add nodes in the HX cluster, the HX Data Platform balances the storage across the additional resources. Compute only nodes can be added to increase compute only resources to the storage cluster.

Storage Cluster Physical Components Overview

Cisco HX Data Platform storage clusters contain the following objects. These objects are monitored by the HX Data Platform for the storage cluster. They can be added and removed from the storage cluster.
• **Converged nodes.** Converged nodes are the physical hardware on which the VM runs. They provide computing and storage resources such as disk space, memory, processing, power, and network I/O.

When a converged node is added to the storage cluster, a storage controller VM is installed. The HX Data Platform services are handled through the storage controller VM. Converged nodes add storage resources to your storage cluster through their associated drives.

Adding converged nodes to your storage cluster is performed using the Expand Cluster feature of the HX Data Platform Installer. Removing converged nodes is a command line task.

• **Compute nodes.** Compute nodes add compute resource but not storage capacity to the storage cluster. They are used as means to add compute resources, including CPU and memory. They do not need to have any caching (SSD) or storage (HDD) drives. Compute nodes are optional to the storage cluster.

When a compute node is added to the storage cluster, an agent controller VM is installed. The HX Data Platform services are handled through the agent controller VM. Compute nodes do not add storage resources to your storage cluster.

Adding compute nodes to your storage cluster is performed using the Expand Cluster feature of the HX Data Platform Installer. Removing compute nodes is a command line task.

• **Drives.** There are two types of drives required for any node in the storage cluster: Solid State Drive (SSD) and Hard Disk Driver (HDD). HDD typically provide the physical storage units associated with converged nodes. SSD typically support management.

Adding HDD to existing converged nodes, also adds storage capacity to the storage cluster. When storage is added to any node in the storage cluster, an equal amount of storage must be added to every node in the storage cluster.

When disks are added or removed, the HX Data Platform rebalances the storage cluster to adjust for the change in storage resource.

Adding or removing disks on your converged nodes is not performed through the HX Data Platform. Prior to adding or removing disks, review the best practices. See the server hardware guides for specific instructions to add or remove disks in nodes.

• **Datastores.** Storage capacity and datastore capacity. This is the combined consumable physical storage available to the storage cluster through datastores, and managed by the HX Data Platform.

Datastore are logical containers used by the HX Data Platform to manage your storage use and storage resources.

Datastores are where the host places virtual disk files and other VM files. Datastores hide the specifics of physical storage devices and provide a uniform model for storing VM files.

Additional objects that can be monitored from a storage cluster point of view and are treated as field replaceable units (FRUs), include the following. See the server hardware guides for information about replacing these objects.

• Power Supply Units (PSUs)

• Network Interface Cards (NICs)
**HX Data Platform Capacity Overview**

In the HX Data Platform the concept of capacity is applied to both datastores and storage clusters. Values are measured in base-2 (GiB/TiB), but for simplicity and consistency are labeled as GB or TB.

- **Cleaner**—A process run on all the storage cluster datastores. After it completes, all the storage cluster datastores total capacity should be in a similar range to the total storage cluster capacity, excluding the metadata. Datastore capacity listed typically will not match the HX storage cluster capacity. See the *Cisco HX Data Platform Command Line Interface Reference* guide for information on the `cleaner` command.

- **Cluster capacity**—All the storage from all the disks on all the nodes in the storage cluster. This includes uncleaned data and the metadata overhead for each disk.

The total/used/free capacity of cluster is based on overall storage capacity and how much storage is used.

- **Condition**—When the HX Storage Cluster enters a space event state, the **Free Space Status** fields are displayed. The **Condition** field lists the space event state. The options are: **Warning**, **Critical**, and **Alert**.

- **Datastore capacity**—The amount of storage available for provisioning to datastores without over-provisioning. Generally, this is similar to the cleaned storage cluster capacity, but it is not an exact match. It does not include metadata or uncleaned data.

The provisioned/used/free capacity of each datastore is based on datastore (thin) provisioned capacity. Because the datastore is thin provisioned, the provisioned capacity (specified by the administrator when creating the datastore) can be well above the actual storage.

- **Free Capacity, storage cluster**—Same as available capacity. For the storage cluster, this is the difference between the amount available to the storage cluster and the amount used in the storage cluster.

- **Free capacity, datastore**—Same as available capacity. For all the storage cluster datastores, this is the difference between the amount provisioned to all the storage cluster datastores and the amount used on all the storage cluster datastores.

The amount used on the whole storage cluster is not included in this datastore calculation. Because datastores are frequently over provisioned, the free capacity can indicate a large availability on all the storage cluster datastores, while the storage cluster capacity can indicate a much lower availability.

- **Multiple users**—Can have different datastores with different provisioned capacities. At any point in time, users do not fully utilize their allocated datastore capacity. When allocating datastore capacity to multiple users, it is up to the administrator to ensure that each user’s provisioned capacity is honored at all time.

- **Over-provisioning**—Occurs when the amount of storage capacity allocated to all the datastores exceeds the amount available to the storage cluster.

It is a common practice to initially over-provision. It allows administrators to allocate the capacity now and backfill the actual storage later.

The value is the difference between the usable capacity and provisioned capacity.

It displays zero (0) value, unless more space has been allocated than the maximum physical amount possible.

Review the over provisioned capacity and ensure that your system does not reach an out-of-space condition.
• **Provisioned**—Amount of capacity allowed to be used by, allocated to, the storage cluster datastores.

The provisioned amount is not set aside for the sole use of the storage cluster datastores. Multiple datastores can be provisioned storage from the same storage capacity.

• **Space Needed**—When the HX Storage Cluster enters a space event state, the **Free Space Status** fields are displayed. **Space Needed** indicates the amount of storage that needs to be made available to clear the listed **Condition**.

• **Used**—Amount of storage capacity consumed by the listed storage cluster or datastore.

HX Data Platform internal meta-data uses 0.5% to 1% space. This might cause the HX Data Platform Plug-in or HX Connect to display a **Used Storage** value even if you have no data in your datastore.

Storage Used shows how much datastore space is occupied by virtual machine files, including configuration and log files, snapshots, and clones. When the virtual machine is running, the used storage space also includes swap files.

• **Usable Capacity**—Amount of storage in the storage cluster available for use to store data.

---

**Understanding Capacity Savings**

The Capacity portlet on the Summary tab displays the deduplication and compression savings provided by the storage cluster. For example, with 50% overall savings, a 6TB capacity storage cluster can actually store 9 TB of data.

The total storage capacity saved by the HX Data Platform system is a calculation of two elements:

- **Compression** - How much of the data is compressed.
- **Deduplication** - How much data is deduplicated. Deduplication is a method of reducing storage space by eliminating redundant data. It stores only one unique instance of the data.

Deduplication savings and compression savings are not simply added together. They are not independent operations. They are correlated using the following elements where essentially the amount of unique bytes used for storage is reduced through deduplication. Then the deduplicated storage consumption is compressed to make even more storage available to the storage cluster.

Deduplication and compression savings are particularly useful when working with VM clones.

If the savings is showing 0%, this indicates the storage cluster is new. The total ingested data to the storage cluster is insufficient to determine meaningful storage savings. Wait until sufficient data is written to the storage cluster.

**For example:**

1. **Initial values**

   Given a VM of 100 GB that is cloned 2 times.

   Total Unique Used Space (TUUS) = 100GB
   
   Total Addressable Space (TAS) = 100x2 = 200 GB

   Given, for this example:

   Total Unique Bytes (TUB) = 25 GB

2. **Deduplication savings**
Storage Capacity Event Messages

Cluster storage capacity includes all the storage from all the disks on all the nodes in the storage cluster. This available capacity is used to manage your data.

Error messages are issued if your data storage needs consume high amounts of available capacity, the performance and health of your storage cluster are affected. The error messages are displayed in vCenter Alarms panels, HX Connect, and HX Data Platform Plug-in Alarms and Events pages.

When the warning or critical errors appear:

Add additional drives or nodes to expand capacity. Additionally, consider deleting unused virtual machines and snapshots. Performance is impacted until storage capacity is reduced.

- **SpaceWarningEvent** – Issues an error. This is a first level warning.
  
  Cluster performance is affected.
  
  Reduce the amount of storage capacity used to below the warning threshold, of 70% total HX Storage Cluster capacity.

- **SpaceAlertEvent** – Issues and error. Space capacity usage remains at error level.
  
  This alert is issued after storage capacity has been reduced, but is still above the warning threshold.
  
  Cluster performance is affected.
  
  Continue to reduce the amount of storage capacity used, until it is below the warning threshold, of 80% total HX Storage Cluster capacity.

- **SpaceCriticalEvent** – Issues and error. This is a critical level warning.
  
  Cluster is in a read only state.
  
  Do not continue the storage cluster operations until you reduce the amount of storage capacity used to below this warning threshold, of 92% total HX Storage Cluster capacity.
• **SpaceRecoveredEvent** - This is informational. The cluster capacity has returned to normal range. Cluster storage space usage is back to normal.

**HX Data Platform High Availability Overview**

The HX Data Platform High Availability (HA) feature ensures that the storage cluster maintains at least two copies of all your data during normal operation with three or more fully functional nodes. If nodes or disks in the storage cluster fail, the cluster's ability to function is affected. If more than one node fails or one node and disk(s) on a different node fail, it is called a *simultaneous failure*.

The number of nodes in the storage cluster, combined with the Data Replication Factor and Access Policy settings, determine the state of the storage cluster that results from node failures.

---

**Note**

Before using the HX Data Platform HA feature, enable DRS and vMotion on the vSphere Web Client.

**Storage Cluster Status**

HX Data Platform storage cluster status information is available through HX Connect, the HX Data Platform Plug-in, and the storage controller VM `stcli` commands. Storage cluster status is described through resiliency and operational status values.

Storage cluster status is described through two reported status elements.

• **Operational Status** - Describes the ability of the storage cluster to perform the functions storage management and storage cluster management of the cluster. How well can the storage cluster perform operations.

• **Resiliency Status** - Describes the ability of the storage clusters to tolerate node failures within the storage cluster. How well can the storage cluster handle disruptions.

Two settings that work with each other affect when the storage cluster transitions into particular operational and resiliency status states.

• **Data Replication Factor** - Sets the number of redundant data replicas.

• **Cluster Access Policy** - Sets the level of data protection and data loss.

**Operational Status Values**

Cluster Operational Status indicates the operational status of the storage cluster and the ability for the applications to perform I/O.

The Operational Status options are:

• **Online** — Cluster is ready for IO.

• **Offline** — Cluster is not ready for IO.
• Out of space—Either the entire cluster is out of space or one or more disks are out of space. In both cases, the cluster cannot accept write transactions, but can continue to display static cluster information.

• Readonly—Cluster cannot accept write transactions, but can continue to display static cluster information.

• Unknown—This is a transitional state while the cluster is coming online.

Other transitional states might be displayed during cluster upgrades and cluster creation.

Color coding and icons are used to indicated various status states. Click icons to display additional information such as reason messages that explain what is contributing to the current state.

**Resiliency Status Values**

Resiliency status is the data resiliency health status and ability of the storage cluster to tolerate failures.

Resiliency Status options are:

- **Healthy**—The cluster is healthy with respect to data and availability.
- **Warning**—Either the data or the cluster availability is being adversely affected.
- **Unknown**—This is a transitional state while the cluster is coming online.

Color coding and icons are used to indicate various status states. Click an icon to display additional information, such as reason messages that explain what is contributing to the current state.

**HX Data Platform Cluster Tolerated Failures**

If nodes or disks in the storage cluster fail, the cluster's ability to function is affected. If more than one node fails or one node and disk(s) on a different node fail, it is called a *simultaneous failure*.

How the number of node failures affect the storage cluster is dependent upon:

- **Number of nodes in the cluster.** The response by the storage cluster is different for clusters with 3 to 4 nodes and 5 or greater nodes.

- **Data Replication Factor.** This is set during HX Data Platform installation and cannot be changed. The options are 2 or 3 redundant replicas of your data across the storage cluster.

  - **Attention** Data Replication Factor 3 is the recommended option.

- **Access Policy.** This can be changed from the default setting after the storage cluster is created. The options are strict, for protecting against data loss, or lenient, to support longer storage cluster availability.

**Cluster State with Number of Failed Nodes**

The tables below list how the storage cluster functionality changes with the listed number of simultaneous node failures.

**Cluster State in 5+ Node Cluster with Number of Failed Nodes**
Cluster State in 3 - 4 Node Clusters with Number of Failed Nodes

<table>
<thead>
<tr>
<th>Replication Factor</th>
<th>Access Policy</th>
<th>Number of Failed Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Read/Write</td>
</tr>
<tr>
<td>3</td>
<td>Lenient</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Strict</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Lenient</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Strict</td>
<td>--</td>
</tr>
</tbody>
</table>

Cluster State with Number of Nodes with Failed Disks

The table below lists how the storage cluster functionality changes with the number of nodes that have one or more failed disks. Note that the node itself has not failed but disk(s) within the node have failed. **For example:** 2 indicates that there are 2 nodes that each have at least one failed disk.

There are two possible types of disks on the servers: SSDs and HDDs. When we talk about multiple disk failures in the table below, it's referring to the disks used for storage capacity. **For example:** If a cache SSD fails on one node and a capacity SSD or HDD fails on another node the storage cluster remains highly available, even with an Access Policy strict setting.

The table below lists the worst case scenario with the listed number of failed disks. This applies to any storage cluster 3 or more nodes. **For example:** A 3 node cluster with Replication Factor 3, while self-healing is in progress, only shuts down if there is a total of 3 simultaneous disk failures on 3 separate nodes.

Note

HX storage clusters are capable of sustaining serial disk failures, (separate disk failures over time). The only requirement is that there is sufficient storage capacity available for support self-healing. The worst-case scenarios listed in this table only apply during the small window while HX is completing the automatic self-healing and rebalancing.

3+ Node Cluster with Number of Nodes with Failed Disks

<table>
<thead>
<tr>
<th>Replication Factor</th>
<th>Access Policy</th>
<th>Failed Disks on Number of Different Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Read/Write</td>
</tr>
<tr>
<td>3</td>
<td>Lenient</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Strict</td>
<td>1</td>
</tr>
</tbody>
</table>
Data Replication Factor Settings

Data Replication Factor Settings

<table>
<thead>
<tr>
<th>Replication Factor</th>
<th>Access Policy</th>
<th>Failed Disks on Number of Different Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Read/Write</td>
</tr>
<tr>
<td>2</td>
<td>Lenient</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Strict</td>
<td>--</td>
</tr>
</tbody>
</table>

Data Replication Factor cannot be changed after the storage cluster is configured.

Data Replication Factor is set when you configure the storage cluster. Data Replication Factor defines the number of redundant replicas of your data across the storage cluster. The options are 2 or 3 redundant replicas of your data.

- If you have hybrid servers (servers that contain both SSD and HDDs), then the default is 3.
- If you have all flash servers (servers that contain only SSDs), then you must explicitly select either 2 or 3 during HX Data Platform installation.

Choose a Data Replication Factor. The choices are:

- Data Replication Factor 3 — Keep three redundant replicas of the data. This consumes more storage resources, and ensures the maximum protection for your data in the event of node or disk failure.

  **Attention** Data Replication Factor 3 is the recommended option.

- Data Replication Factor 2 — Keep two redundant replicas of the data. This consumes fewer storage resources, but reduces your data protection in the event of node or disk failure.

Cluster Access Policy

The Cluster Access Policy works with the Data Replication Factor to set levels of data protection and data loss prevention. There are two Cluster Access Policy options. The default is lenient. It is not configurable during installation, but can be changed after installation and initial storage cluster configuration.

- **Strict** - Applies policies to protect against data loss.

  If nodes or disks in the storage cluster fail, the cluster's ability to function is affected. If more than one node fails or one node and disk(s) on a different node fail, it is called a simultaneous failure. The strict setting helps protect the data in event of simultaneous failures.

- **Lenient** - Applies policies to support longer storage cluster availability. This is the default.
Responses to Storage Cluster Node Failures

A storage cluster healing timeout is the length of time HX Connect or HX Data Platform Plug-in waits before automatically healing the storage cluster. If a disk fails, the healing timeout is 1 minute. If a node fails, the healing timeout is 2 hours. A node failure timeout takes priority if a disk and a node fail at the same time or if a disk fails after node failure, but before the healing is finished.

When the cluster resiliency status is Warning, the HX Data Platform system supports the following storage cluster failures and responses.

Optionally, click the associated Cluster Status/Operational Status or Resiliency Status/Resiliency Health in HX Connect and HX Data Platform Plug-in, to display reason messages that explain what is contributing to the current state.

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Number of Simultaneous Failures</th>
<th>Entity Failed</th>
<th>Maintenance Action to Take</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 nodes</td>
<td>1</td>
<td>One node.</td>
<td>The storage cluster does not automatically heal. Replace the failed node to restore storage cluster health.</td>
</tr>
</tbody>
</table>
### HX Storage Cluster Overview

#### Responses to Storage Cluster Node Failures

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Number of Simultaneous Failures</th>
<th>Entity Failed</th>
<th>Maintenance Action to Take</th>
</tr>
</thead>
</table>
| 3 nodes      | 2                                | Two or more disks on two nodes are blacklisted or failed. | 1. If one SSD fails, the storage cluster does not automatically heal.  
- Replace the faulty SSD and restore the system by rebalancing the cluster  
2. If one HDD fails or is removed, the disk is blacklisted immediately. The storage cluster automatically begins healing within a minute.  
3. If more than one HDD fails, the system might not automatically restore storage cluster health.  
- If the system is not restored, replace the faulty disks and restore the system by rebalancing the cluster |
| 4 nodes      | 1                                | One node.     | If the node does not recover in two hours, the storage cluster starts healing by rebalancing data on the remaining nodes.  
To recover the failed node immediately and fully restore the storage cluster:  
1. Check that the node is powered on and restart it if possible. You might need to replace the node.  
2. Rebalance the cluster |
### Responses to Storage Cluster Node Failures

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Number of Simultaneous Failures</th>
<th>Entity Failed</th>
<th>Maintenance Action to Take</th>
</tr>
</thead>
</table>
| 4 nodes      | 2                               | Two or more disks on two nodes. | If two SSDs fail, the storage cluster does not automatically heal.  
If the disk does not recover in one minute, the storage cluster starts healing by rebalancing data on the remaining nodes. |
| 5+ nodes     | 2                               | Up to two nodes. | If the node does not recover in two hours, the storage cluster starts healing by rebalancing data on the remaining nodes.  
To recover the failed node immediately and fully restore the storage cluster:  
1. Check that the node is powered on and restart it if possible.  
You might need to replace the node.  
2. Rebalance the cluster  
If the storage cluster shuts down, see Troubleshooting, Two Nodes Fail Simultaneously Causes the Storage Cluster to Shutdown section. |
| 5+ nodes     | 2                               | Two nodes with two or more disk failures on each node. | The system automatically triggers a rebalance after a minute to restore storage cluster health. |
### Responses to Storage Cluster Node Failures

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Number of Simultaneous Failures</th>
<th>Entity Failed</th>
<th>Maintenance Action to Take</th>
</tr>
</thead>
</table>
| 5+ nodes     | 2                               | One node and One or more disks on a different node     | If the disk does not recover in **one minute**, the storage cluster starts healing by rebalancing data on the remaining nodes. If the node does not recover in **two hours**, the storage cluster starts healing by rebalancing data on the remaining nodes. If a node in the storage cluster fails and a disk on a different node also fails, the storage cluster starts healing the failed disk (without touching the data on the failed node) in one minute. If the failed node does not come back up after two hours, the storage cluster starts healing the failed node as well. To recover the failed node immediately and fully restore the storage cluster:  
1. Check that the node is powered on and restart it if possible. You might need to replace the node.  
2. Rebalance the cluster. |

Review the table above and perform the action listed.
HX Data Platform ReadyClones Overview

HX Data Platform ReadyClones is a pioneer storage technology that enables you to rapidly create and customize multiple cloned VMs from a host VM. It is an expansion feature that is used for creating multiple copies of VMs that can then be used as standalone VMs.

A ReadyClone, similar to a standard clone, is a copy of an existing VM. The existing VM is called the host VM. When the cloning operation is complete, the ReadyClone is a separate guest VM.

Changes made to a ReadyClone do not affect the host VM. A ReadyClone's MAC address and UUID are different from those of the host VM.

Installing a guest operating system and applications can be time consuming. With ReadyClone, you can make many copies of a VM from a single installation and configuration process.

Clones are useful when you deploy many identical VMs to a group.

HX Data Platform Native Snapshots Overview

HX Data Platform Native Snapshots are a backup feature that saves versions (states) of working VMs. VMs can be reverted back to native snapshots.

Use the HX Data Platform plug-in to take native snapshots of your VMs. HX Data Platform native snapshot options include: create a native snapshot, revert to any native snapshot, and delete a native snapshot. Timing options include: Hourly, Daily, and Weekly, all in 15 minute increments.

A native snapshot is a reproduction of a VM that includes the state of the data on all VM disks and the VM power state (on, off, or suspended) at the time the native snapshot is taken. Take a native snapshot to save the current state of the VM, so that you have the option to revert to the saved state.

You can take a native snapshot when a VM is powered on, powered off, or suspended. For additional information about VMware snapshots, see the VMware KB, Understanding virtual machine snapshots in VMware ESXi and ESX (1015180) at, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180
CHAPTER 3

Logging in to HX Data Platform Interfaces

• HyperFlex Cluster Interfaces Overview, on page 19
• Logging into HX Connect, on page 24
• Logging into the Controller VM (stcli) Command Line, on page 25
• Log in to Cisco HX Data Platform Installer, on page 27
• Accessing the HX Data Platform REST APIs, on page 28
• Accessing the Cisco HX Data Platform Plug-in, on page 28
• Contacting Cisco TAC, on page 30

HyperFlex Cluster Interfaces Overview

Each HyperFlex interface provides access to information about and a means to perform actions upon the HX Storage Cluster. The HX Storage Cluster interfaces include:

• HX Connect—Monitoring, performance charts, and tasks for upgrade, encryption, replication, datastores, nodes, disks, VM readyclones
• HX Data Platform Plug-in—Monitoring, performance charts, and tasks for datastores, hosts (nodes), and disks
• Storage Controller VM command line—Run HX Data Platform stcli commands
• HyperFlex Systems RESTful APIs—Enabling authentication, replication, encryption, monitoring, and management of HyperFlex Systems through an on-demand stateless protocol

Additional interfaces include:

• Cisco HX Data Platform Installer—Installing HX Data Platform, creating and expanding HX Storage Cluster
• Cisco UCS Manager—Tasks for networking, storage and storage access, and managing resources in the HX Storage Cluster
• VMware vSphere Web Client and vSphere Client—Managing all the VMware ESXi servers in the vCenter cluster.
• VMware ESXi—Managing the individual ESXi host, providing host command line
## Guidelines for HX Data Platform Login Credentials

stcli commands prompt for login credentials.

The storage controller VM password for the predefined users **admin** and **root** are specified during HX Data Platform installer. After installation you can change passwords through the stcli command line.

<table>
<thead>
<tr>
<th>Component</th>
<th>Permission Level</th>
<th>Username</th>
<th>Password</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Data Platform OVA</td>
<td>root</td>
<td>root</td>
<td>Cisco123</td>
<td></td>
</tr>
<tr>
<td>HX Data Platform Installer VM</td>
<td>root</td>
<td>root</td>
<td>Cisco123</td>
<td></td>
</tr>
<tr>
<td>HX Connect</td>
<td>administrator or read-only</td>
<td>User defined through vCenter.</td>
<td>User defined through vCenter.</td>
<td>Requires leading local/ for login: local/admin or local/root</td>
</tr>
<tr>
<td>HX Storage Controller VM</td>
<td>root</td>
<td>User defined during HX installation. User defined through vCenter. Predefined admin or root users.</td>
<td>As specified during HX installation. Strong password required.</td>
<td>Must match across all nodes in storage cluster. Use the stcli command when changing the password after installation.</td>
</tr>
<tr>
<td>vCenter</td>
<td>admin</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a> default. SSO enabled. As configured, MYDOMAIN\name or <a href="mailto:name@mydomain.com">name@mydomain.com</a></td>
<td>SSO enabled. As configured.</td>
<td>Ensure the vCenter credentials meet the vSphere 5.5 requirements if the ESX servers are at version 5.5. Read only users do not have access to HX Data Platform Plug-in.</td>
</tr>
<tr>
<td>ESX Server</td>
<td>root</td>
<td>SSO enabled. As configured.</td>
<td>SSO enabled. As configured.</td>
<td>Must match across all ESX servers in storage cluster.</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>root</td>
<td>root</td>
<td>As specified during HX installation.</td>
<td>Use vCenter or esxcli command when changing the password after HX installation.</td>
</tr>
<tr>
<td>UCS Manager</td>
<td>admin</td>
<td>As configured.</td>
<td>As configured.</td>
<td></td>
</tr>
<tr>
<td>FI</td>
<td>admin</td>
<td>As configured.</td>
<td>As configured.</td>
<td></td>
</tr>
</tbody>
</table>
HX Data Platform Names, Passwords, and Characters

Most printable and extended ASCII characters are acceptable for use in names and passwords. Certain characters are not allowed in HX Data Platform user names, passwords, virtual machine names, storage controller VM names, and datastore names. Folders and resource pools do not have character exceptions.

However, to simplify names and passwords, consider not using these special characters, as they are frequently assigned special purposes.

ampersand (&), apostrophe ('), asterisk (*), at sign (@), back slash (\), colon (:), comma (,), dollar sign ($), exclamation (!), forward slash (/), less than sign (<), more than sign (>), percent (%), pipe (|), pound (#), question mark (?), semi-colon (;)

When entering special characters, consider the shell being used. Different shells have different sensitive characters. If you have special characters in your names or passwords, place them in a single quote, 'speci@lword!'

HX Storage Cluster Name

HX cluster names cannot exceed 50 characters.

HX Storage Cluster Host Names

HX cluster host names cannot exceed 15 characters.

Virtual Machine and Datastore Names

Most characters used to create a virtual machine name, controller VM name, or datastore name are acceptable. Escaped characters are acceptable for virtual machine, controller VM names, or datastore names.

Maximum characters—Virtual machine names can have up to 15 characters.

Excluded characters—Do not use the following character in any user virtual machine name or datastore name for which you want to enable snapshots.

• accent grave (´)

Special characters—The following special characters are acceptable for user virtual machine or datastore names:

• ampersand (&), apostrophe ('), asterisk (*), at sign (@), back slash (\), circumflex (^), colon (:), comma (,), dollar sign ($), double quotation ("), equalsign (=), exclamation (!), forward slash (/), hyphen (-), left curly brace ({), left parentheses ((), left square bracket ([), less than sign (<), more than sign (>), percent (%), pipe (|), plus sign (+), pound (#), question mark (?), right curly brace (}), right parentheses ()), right square bracket (]), semi-colon (;), tilde (~), underscore (_)
• Must start with an alphabetic character.
• Must have: alphabetic characters (upper or lower case).
• Can have: numeric characters. Cannot be all numeric characters.
• Only special character allowed: underscore (_), dash (-), dot (.)

Controller VM Password Requirements

The following rules apply to controller VM root and admin user passwords.

Note

General rule about passwords: Do not include them in a command string. Allow the command to prompt for the password.

• Minimum Length: 10
• Minimum 1 Uppercase
• Minimum 1 Lowercase
• Minimum 1 Digit
• Minimum 1 Special Character
• A maximum of 3 retry to set the new password

To change a controller VM password, always use the stcli command. Do not use another change password command, such as a Unix password command.

1. Login to the management controller VM.
2. Run the stcli command.

    stcli security password set [-h] [--user USER] [--password PASSWORD]

    The change is propagated to all the controller VMs in the HX cluster.

UCS Manager and ESX Password Format and Character Requirements

The following is a summary of format and character requirements for UCS Manager and VMware ESXi passwords. See the Cisco UCS Manager and VMware ESXi documentation for additional information.

• Characters classes: lower case letters, upper case letters, numbers, special characters.
    Passwords are case sensitive.

• Character length: Minimum 6, maximum 80
    Minimum 6 characters required, if characters from all four character classes.
    Minimum 7 characters required, if characters from at least three character classes.
    Minimum 8 characters required, if characters from only one or two character classes.

• Start and end characters: An upper case letter at the beginning or a number at the end of the password do not count toward the total number of characters.
If password starts with uppercase letter, then 2 uppercase letters are required. If password ends with a digit, then 2 digits are required.

Examples that meet the requirements:

h#56Nu - 6 characters. 4 classes. No starting upper case letter. No ending number.
h5xj7Nu - 7 characters. 3 classes. No starting upper case letter. No ending number.
XhUwPeNu - 8 characters. 2 classes. No starting upper case letter. No ending number.
Xh#5*Nu - 6 characters counted. 4 characters classes. Starting upper case letter. No ending number.
h#5*Nu9 - 6 characters counted. 4 characters classes. No starting upper case letter. Ending number.

- **Consecutive characters**: Maximum 2. For example, hhh###555 is not acceptable.

Through vSphere SSO policy, this value is configurable.

- **Excluded characters**:

UCS Manager passwords cannot contain the escape (\) character.

ESX passwords cannot contain these characters.

  - Cannot be the username or the reverse of the username.
  - Cannot contain words found in the dictionary.
  - Cannot contain the characters escape (\), dollar sign ($), question mark (?), equal sign (=).

- **Dictionary words**:

  Do not use any words that can be found in the dictionary.

**vSphere 5.5 Password Exceptions**

Some characters, when processed by functions within vSphere are escaped. That is, the processing function applies an escape character prior to the special character before continuing to process the provided name.

Permitted special characters are specific to vSphere versions 5.5 or 6.0 and later. See VMware KB article, *Installing vCenter Single Sign-On 5.5 fails if the password for administrator@vsphere.local contains certain special character* (2060746), at https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2060746.

**Excluded characters**: Do not use the following characters with vSphere 5.5.

- Non-ASCII characters. Extended ASCII characters.
- Letters with accents. For example the accent grave, accent acute, circumflex, umlaut, tilde and cedilla (é, à, â, ã, ö, ü, ñ, ç, æ).
- vSphere 5.5 and SSO: ampersand (&), apostrophe (‘), back slash (\), circumflex (^), double quotation (“), exclamation (!), percent (%), semicolon (;), space ( )

VMware has vSphere SSO password policy setting options and upgrade considerations for user names. See VMware documentation for the topics: *How vCenter Single Sign-On Affects Upgrades* and *Edit the vCenter Single Sign-On Password Policy*.

- Location based exception: at the beginning of a name, do not use an at sign (@), parenthesis ( )
Logging into HX Connect

Cisco HyperFlex Connect provides an HTML5 based access to HX Storage Cluster monitoring, and replication, encryption, datastore, and virtual machine tasks.

About Sessions

Each login to HX Connect is a session. Sessions are the period of activity between time when you log into HX Connect and when you log out. Do not manually clear cookies in a browser during a session, because this also drops the session. Do not close the browser to close a session, though dropped, the session is still counted as an open session. Default session maximums include:

- 256 concurrent sessions per user
- 300 concurrent sessions across the HX Storage Cluster

Before you begin

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If you are a read-only user, you may not see all of the options described in the Help. To perform most actions in HX Connect, you must have administrative privileges.</td>
</tr>
<tr>
<td>• Ensure that the time on the vCenter and the controller VMs are in sync or near sync. If there is too large of a time skew between the vCenter time and the cluster time, AAA authentication will fail.</td>
</tr>
</tbody>
</table>

Step 1  
Locate the HX Storage Cluster management IP address.

Use fully qualified domain name (FQDN) for the management IP address, rather than individual Storage Controller VM.

Step 2  
Enter the HX Storage Cluster management IP address in a browser.

Step 3  
Enter the HX Storage Cluster login credentials.

• **RBAC users**—Cisco HyperFlex Connect supports role-based access control (RBAC) login for:
  - **Administrator**—Users with administrator role have read and modify operations permissions. These users can modify the HX Storage Cluster
  - **Read only**—Users with read only role have read (view) permissions. They cannot make any changes to the HX Storage Cluster.

These users are created through vCenter. vCenter user name format is <name>@domain.local. For example, administrator@vsphere.local.

• **HX pre-defined users**—To login using the HX Data Platform predefined users admin or root, enter a prefix local/. For example: local/root or local/admin.

Actions performed with the local/ login only affect the local cluster.

vCenter recognizes the session with HX Connect, therefore system messages that originate with vCenter might indicate the session user instead of local/root. For example, in Alarms, Acknowledged By might list com.springpath.sysmgmt.domain-c7.
Click the eye icon to view or hide the password field text. Sometimes this icon is obscured by other field elements. Click the eye icon area and the toggle function continues to work.

What to do next

- To refresh the HX Connect displayed content, click the refresh (circular) icon. If this does not refresh the page, the clear the cache and reload the browser.
- To logout of HX Connect, and properly close the session, select User menu (top right) > Logout.

Logging into the Controller VM (stcli) Command Line

All stcli command are divided into commands that read HX Cluster information and commands that modify the HX Cluster.

- Modify commands—Require administrator level permissions. Examples:
  -stcli cluster create
  -stcli datastore create
- Read commands—Permitted with administrator or read only level permissions. Examples:
  -stcli <cmd> -help
  -stcli cluster info
  -stcli datastore info

To execute HX Data Platform stcli commands, login to the HX Data Platform Storage Controller VM command line.

Important

Do not include passwords in command strings. Commands are frequently passed to the logs as plain text. Wait until the command prompts for the password. This applies to login commands as well as stcli commands.

Login to the HX Data Platform command line interface in the Storage Controller VM. Choose a method:

- From a browser
- From a command terminal
- From HX Connect Web CLI page

Only direct commands are supported through HX Connect.

- Direct commands—commands that complete in a single pass and do not require responses through the command line. Example direct command: stcli cluster info
- Indirect commands—multi-layered commands that require live response through the command line. Example interactive command: stcli cluster reregister
Step 1  Locate a controller VM DNS Name.
1. Select a VM > Summary > DNS Name.
2. From vSphere Web Client Home > VMs and Templates > vCenter server > datacenter > ESX Agents > VM.
3. Click through to the storage cluster list of controller VMs.

Step 2  From a browser, enter the DNS Name and /cli path.
   a) Enter the path.
      Example
      # cs002-stctlvm-a.eng.storvisor.com/cli
      Assumed username: admin, password: defined during HX Cluster creation.
   b) Enter the password at the prompt.

Step 3  From a command line terminal using ssh.
   Note  Do not include the password in an ssh login string. The login is passed to the logs as plain text.
   a) Enter the ssh command string.
      Examples
      • Pre-defined user for all controller VMs.
        # ssh admin@<ipaddress_controllervm>
      • RBAC user created through vCenter. vCenter user name format is: <name>@domain.local. For example,
        administrator@vsphere.local
        # ssh vc-<username>@<ipaddress_controllervm>
        # ssh vc-administrator@vsphere.local@<ipaddress_controllervm>
   b) Sometimes a certificate warning is displayed. Enter yes to ignore the warning and proceed.
      ------------------------------------------------------------------------
      !! ALERT !!
      This service is restricted to authorized users only.
      All activities on this system are logged. Unauthorized access will be reported.
      ------------------------------------------------------------------------
      HyperFlex StorageController 2.5(1a)# exit
      logout
      Connection to 10.198.3.22 closed.)$ssh root@10.198.3.24
      The authenticity of host '10.198.3.24 (10.198.3.24)' can't be established.
      Are you sure you want to continue connecting (yes/no)?
   c) Enter the password at the prompt.
      # ssh admin@10.198.3.22
      HyperFlex StorageController 2.5(1a)
      admin@10.198.3.22's password:

Step 4  From HX Connect Web CLI page. Login to HX Connect, select Web CLI.
Changing Storage Controller Password

To reset the HyperFlex storage controller password post installation, do the following.

**Step 1**
Login to a storage controller VM.

**Step 2**
Change the HyperFlex storage controller password.

```
# stcli security password set
```

This command applies the change to all the controller VMs in the storage cluster.

*Note*
Do not use the unix password command.

**Step 3**
Type in the new password.

**Step 4**
Press Enter.

Log in to Cisco HX Data Platform Installer

Next, you install the HX Data Platform software.

**Note**
Before launching the Cisco HX Data Platform installer, ensure that all the ESX servers that are in the vCenter cluster that you plan to include in the storage cluster are in maintenance mode.

**Step 1**
In a browser, enter the URL for the VM where HX Data Platform Installer was installed.

You must have this address from the earlier section on Deploying HX Data Platform Installer. For example, http://10.64.4.254

**Step 2**
Use the credentials:

username: `root` password: `Cisco123`

Read the EULA. Click **I accept the terms and conditions**.

Verify the product version listed in the lower right corner is correct. Click **Login**.

**Step 3**
This displays the HX Data Platform installer Workflow page. The page provides two options to navigate further.

- **Cluster Creation** - Click on this button to configure UCS Manager, ESXi, and deploy HX Data Platform software.

- **Cluster Expansion** - Displays the Expand Cluster page where you provide the data to add converged nodes and compute nodes to an existing storage cluster.
Select the **Cluster Creation** option to configure a new cluster and click **Continue**.

**Step 4**
This displays the next HX Data Platform installer Workflow page with the following options:

- **Run UCS Manager Configuration** - Click on this button to apply FI policies and profiles to HX nodes.
- **Run ESXi Configuration** - Click on this button to configure ESX servers. This to set the static IP address, hostname, and VLAN.
- **Deploy HX Software** - Enter the required configuration data manually to set up the storage clusters.

---

**Accessing the HX Data Platform REST APIs**

Cisco HyperFlex HX-Series Systems provide a fully-contained, virtual server platform that combines all three layers of compute, storage, and network with the powerful Cisco HX Data Platform software tool resulting in a single point of connectivity for simplified management. Cisco HyperFlex Systems are modular systems designed to scale out by adding HX nodes under a single UCS management domain. The hyperconverged system provides a unified pool of resources based on your workload needs.

Cisco HyperFlex Systems RESTful APIs with HTTP verbs integrate with other third-party management and monitoring tools that can be configured to make HTTP calls. It enables authentication, replication, encryption, monitoring, and management of a HyperFlex system through an on-demand stateless protocol. The APIs allow for external applications to interface directly with the Hyperflex management plane.

These resources are accessed through URI or Uniform Resource Identifier and operations are performed on these resources using http verbs such as POST (create), GET (read), PUT (update), DELETE (delete).

The REST APIs are documented using swagger which can also generate client libraries in various languages such as python, JAVA, SCALA, and Javascript. Using libraries thus generated, you can create programs and scripts to consume HyperFlex resources.

HyperFlex also provides a built-in REST API access tool, the REST explorer. Use this tool to access Hyperflex resources in real time and observe responses. The REST explorer also generates CURL commands that can be run from command line.

---

**Step 1**
Open a browser to the DevNet address, [https://developer.cisco.com/site/ucs-dev-center/docs/hyperflex/](https://developer.cisco.com/site/ucs-dev-center/docs/hyperflex/)

From developer.cisco.com, select **Technologies > Data Center > UCS Dev Center > Cisco HyperFlex Systems REST API Reference**.

**Step 2**
Click **Login** and enter credentials, if needed.

Use the same credentials to login to the Swagger UI.

---

**Accessing the Cisco HX Data Platform Plug-in**

Access the HX Data Platform plug-in through the vSphere Web Client.

• If you are using the Firefox browser, ensure you have the latest Adobe Flash Player installed.

• The HX Data Platform plug-in is not available through the vSphere Client for Windows, also known as the vSphere thick client. Event messages generated about activities in the HX Data Platform plug-in are included in the vSphere Client display. HX Data Platform plug-in tasks cannot be performed through the vSphere Client for Windows.

• If you have Read Only permissions, you cannot perform any configuration related tasks. You can only view status information.

**Step 1**
From the vSphere Web Client, click the Home icon (house) located at the top of the vCenter panel.

**Step 2**
Navigator Home page, select **vCenter Inventory Lists**.

**Step 3**
Scroll to the bottom of the vCenter Inventory List to access the HX Data Platform plug-in.

**Step 4**
Expand the Cisco HyperFlex Systems and click **Cisco HX Data Platform** to display the HX storage clusters available in the HX Data Platform plug-in.

Notice that the Cisco HXDP object lists the number of HX storage clusters.

From the **Objects** tab, you can:

• Edit the storage cluster name. Click the edit icon (pencil) or select **Rename Cluster** from the Actions menu.

• Display the storage cluster configuration. Click the summary icon (green paper) or select **Summary** from the Actions menu.

**Step 5**
Select an **HX storage cluster** from the list in the Navigator pane.

Under the Cisco HX Data Platform is a list of storage clusters. Select one storage cluster from this list.

**Step 6**
Click tabs in the center pane to access the HX Data Platform plug-in information and various actions.

<table>
<thead>
<tr>
<th>Tab Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started</td>
<td>Read introductory information and access basic actions.</td>
</tr>
<tr>
<td>Summary</td>
<td>Monitor basic status and configuration for HX Data Platform storage objects.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Monitor HX storage cluster, host, and datastore performance and events.</td>
</tr>
<tr>
<td>Manage</td>
<td>Monitor HX storage cluster details, create and manage datastores, copy and export information.</td>
</tr>
</tbody>
</table>
Contacting Cisco TAC

You can open a Cisco Technical Assistance Center (TAC) support case to reduce time addressing issues, and get efficient support directly with Cisco Prime Collaboration application.

For all customers, partners, resellers, and distributors with valid Cisco service contracts, Cisco Technical Support provides around-the-clock, award-winning technical support services. The Cisco Technical Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies:

http://www.cisco.com/techsupport

Using the TAC Support Case Manager online tool is the fastest way to open S3 and S4 support cases. (S3 and S4 support cases consist of minimal network impairment issues and product information requests.) After you describe your situation, the TAC Support Case Manager automatically provides recommended solutions. If your issue is not resolved by using the recommended resources, TAC Support Case Manager assigns your support case to a Cisco TAC engineer. You can access the TAC Support Case Manager from this location:

https://mycase.cloudapps.cisco.com/case

For S1 or S2 support cases or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 support cases consist of production network issues, such as a severe degradation or outage.) S1 and S2 support cases have Cisco TAC engineers assigned immediately to ensure your business operations continue to run smoothly.

To open a support case by telephone, use one of the following numbers:

• Asia-Pacific: +61 2 8446 7411
• Australia: 1 800 805 227
• EMEA: +32 2 704 5555
• USA: 1 800 553 2447

For a complete list of Cisco TAC contacts for Enterprise and Service Provider products, see http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Monitoring HX Storage Clusters

Monitoring HyperFlex Clusters

This chapter describes the monitoring content available through the HX Storage Cluster interfaces.

- HX Connect
- HX Data Platform Plug-in
- Storage Controller VM command line

View Performance Charts

The Monitor Performance tab displays the read and write performance of the storage cluster, hosts, and datastores.

- Performance charts display a pictorial representation of the storage cluster, host, and datastore performance.
- The system updates the performance charts every 20 seconds.
- Hover your mouse over individual data points to view peak performance information and time-stamp.
- Light blue indicates write operations and dark blue indicates read operations.
- Gaps in the performance charts indicate time periods when data was not available. Gaps do not necessarily indicate a drop in performance.

Storage Cluster Performance Chart

Step 1 From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Monitor > Performance.
On the left there are three options you can chose to Monitor: Storage Cluster, Hosts, and Datastores.

**Step 2**  Click **Storage Cluster** to view the storage cluster performance tab.

**Step 3**  Click **Hour, Day, Week, Month, Max, or Custom** option, to specify the time period in which you want to view storage cluster performance.

**Step 4**  Click **IOPS, Throughput, Latency, and Show** check boxes to display selected performance and objects.

---

### Hosts Performance Chart

**Step 1**  From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Monitor > Performance.**

On the left there are three options you can chose to Monitor: Storage Cluster, Hosts, and/or Datastores.

**Step 2**  Click **Hosts** to view the hosts performance tab.

**Step 3**  Click **Hour, Day, Week, Month, Max, or Custom** option, to specify the time period in which you want to view the host performance.

**Step 4**  Click **IOPS, Throughput, Latency, and Show** check boxes to display selected performance and objects.

**Step 5**  Click **host** to exclude or view individual hosts. Compute nodes do not have storage cluster performance values.

---

### Datastores Performance Chart

**Step 1**  From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Monitor > Performance.**

On the left there are three options you can chose to Monitor: Storage Cluster, Hosts, and Datastores.

**Step 2**  Click **Datastores** to view the datastores performance tab.

**Step 3**  Click **Hour, Day, Week, Month, Max, or Custom** option, to specify the time period in which you want to view the datastore performance.

**Step 4**  Click **IOPS, Throughput, Latency, and Show** check boxes to display selected performance and objects.

---

### Performance Portlet

The Performance portlet provides details about the HX Data Platform storage cluster performance. It displays the past one hour of performance data plotted in 20 second intervals. The Performance portlet charts show data for the entire storage cluster.

For details on storage cluster, datastore, and host-level performance reports, select the **Monitor** tab.

**Step 1**  From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary.**
Step 2
Scroll to the **Performance** portlet.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOPS</td>
<td>Input/Output Operations per Second.</td>
</tr>
<tr>
<td>Throughput</td>
<td>The rate of data transfer in the storage cluster. Measured in MBps.</td>
</tr>
<tr>
<td>Latency</td>
<td>Latency is a measure of how long it takes for a single I/O request to complete. It is the duration between issuing a request and receiving a response. Measured in msec.</td>
</tr>
<tr>
<td>Current</td>
<td>The most recent data point value for the chart.</td>
</tr>
<tr>
<td>Past Hour</td>
<td>A chart of the last hour of data points.</td>
</tr>
</tbody>
</table>

**Datastore Trends Portlet**

The Datastore Trends portlet is a chart of the IO performance of the selected datastore.

**Step 1**
From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage.**

**Step 2**
Select a **datastore** from the table list. The **Summary** tab updates to display the information for the selected datastore.

**Step 3**
Scrolls to view the **Trends** portlet.

The tab displays IOPS plotted every 20 minutes.

Hover your mouse over the peak values to obtain color-coded read IOPS and write IOPS.

**Customizing Performance Charts**

Modify the performance charts to display all or some of the listed options.

<table>
<thead>
<tr>
<th>Customize Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time period</strong></td>
<td>Choose from hour, days, week, month, all, or custom. See Specifying Performance Time Period section in this chapter.</td>
</tr>
<tr>
<td><strong>Cluster objects</strong></td>
<td>Choose from a list of storage clusters, hosts, or datastores.</td>
</tr>
<tr>
<td><strong>Chart type</strong></td>
<td>Choose from IOPS, Throughput, or Latency.</td>
</tr>
<tr>
<td><strong>Show objects</strong></td>
<td>Choose which listed object’s data to display. See Selecting Performance Charts section in this chapter.</td>
</tr>
</tbody>
</table>
Specify Performance Time Period

Step 1  From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Monitor > Performance

Step 2  Click one of the following tabs to specify the time period in which you want to view performance of the storage cluster, host, or datastore.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour</td>
<td>Displays performance in the past hour</td>
</tr>
<tr>
<td>Day</td>
<td>Displays performance in the past day</td>
</tr>
<tr>
<td>Week</td>
<td>Displays performance in the past week</td>
</tr>
<tr>
<td>Month</td>
<td>Displays performance in the past month</td>
</tr>
<tr>
<td>All</td>
<td>Displays the performance of the storage cluster since it was created</td>
</tr>
<tr>
<td>Custom</td>
<td>Select this tab and specify a custom range as described in Specifying Custom Range</td>
</tr>
</tbody>
</table>

Specify Custom Range

Step 1  From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Monitor > Performance

Step 2  Click the Custom tab to display the Custom Range dialog box.

Step 3  Choose a method, for the Custom Range dialog box:
   a) Click Last, type the number of minutes, hours, days, or months. Optionally, use the up or down arrow to increase or decrease the number.
   b) Click the drop-down list to specify the minutes, hours, days, weeks, or months.
   c) Click From, click the calendar icon, and select a date from which you want to start measuring the performance. Click the drop-down list to select a time.
   d) Click To, click the calendar icon, and select a date up to which you want to start measuring the performance. Click the drop-down list to select a time.

Step 4  Click Apply and then click OK to apply your configuration.

Selecting Performance Charts

You can select the performance charts to display for storage clusters, hosts, and datastores.
Select or deselect the check box corresponding to IOPS, Throughput, and Latency at the bottom of the tab to view specific information.

For example, to view only storage cluster IOPS performance:

a) From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Monitor > Performance.
b) Click either Storage Cluster, Hosts, or Datastores chart set. In a Hosts table, compute nodes do not display IOPS, Throughput, or Latency values, as they do not provide storage to the storage cluster.
c) Deselect chart options.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chart types</td>
<td>Click the check box to select which charts and table columns to view or hide. Options are:</td>
</tr>
<tr>
<td></td>
<td>• IOPS</td>
</tr>
<tr>
<td></td>
<td>• Throughput</td>
</tr>
<tr>
<td></td>
<td>• Latency</td>
</tr>
<tr>
<td>Show</td>
<td>For each storage cluster, hosts, and datastores, click the check boxes to select the specific object to include or exclude from the charts.</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Indicates the color representation in the chart for the read and write values of each object.</td>
</tr>
<tr>
<td>Storage Cluster</td>
<td>Names of the storage clusters in the charts.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Names of the hosts in the charts. This includes both converged nodes and compute nodes.</td>
</tr>
<tr>
<td>Datastores</td>
<td>Names of the datastores in the charts.</td>
</tr>
<tr>
<td>IOPS Read/Write</td>
<td>Latest data point for Input/Output Operations per Second.</td>
</tr>
<tr>
<td>Throughput Read/Write (Mbps)</td>
<td>Latest data point for the rate of data transfer in the storage cluster.Measured in Mbps.</td>
</tr>
<tr>
<td>Latency Read/Write (msec)</td>
<td>Latest data point for the Latency that is a measure of how long it takes for a single I/O request to complete. It is the duration between issuing a request and receiving a response. Measured in msec.</td>
</tr>
</tbody>
</table>
Using the HX Data Platform Plug-in Interface

There are several HX Data Platform plug-in features that apply across the interface. These are described in the following topics.

Cisco HX Data Platform Plug-in Integration with vSphere Web Client

The HX Data Platform plug-in is tightly integrated with the VMware vSphere vCenter interface to provide a seamless data management experience. You can use either the vSphere Web Client or the vSphere Client vSphere vCenter interface. Most of the task examples in this guide refer to the vSphere Web Client interface.

You access the HX Data Platform plug-in through the vSphere vCenter Inventory Lists. Select storage clusters to manage from the HX Data Platform plug-in. The HX Data Platform plug-in monitors and manages storage cluster specific objects such as datastores. vSphere monitors and manages objects in the storage cluster, such as ESX servers. Tasks overlap between the HX Data Platform plug-in and vSphere.

Links Between the Cisco HX Data Platform Plug-in and the vSphere Interface

In the vSphere Web Client, both the HX Data Platform plug-in and vCenter provide information on component and cluster status. Selected tabs and panels provide direct links between HX Data Platform plug-in and vCenter information and actions.

Note that following a link from either the HX Data Platform plug-in or vCenter does not mean there is a single-click link to return to your starting location.

Cisco HX Data Platform Plug-in Tabs Overview

The HX Data Platform plug-in monitoring information and managing functions are distributed among three tabs. The following is a list of all the HX Data Platform plug-in tabs and panels that display HX Data Platform storage cluster status and provide options for storage cluster administrative tasks.

Summary tab contains a Summary area and a Portlets area. The Summary tab portlets are: Capacity, Performance, and Status.

Monitor tab has two sub tabs:
- Performance tab - Displays Latency, Throughput, and IOPs performance charts for Storage Clusters, Hosts, and Datacenters.
- Events tab - Displays a list HX Data Platform events and a detail panel for a selected event.

Manage tab has two sub tabs:
- Cluster tab - Describes storage clusters, hosts, disks, PSUs, and NICs. This includes: List of clusters and hosts, detail panels for any selected cluster or host, and additional sub tabs: Hosts, Disks, PSUs, and NICs.
- Datastores tab - Describes information about hosts from the datastore point of view. This includes: List of datastores and additional sub tabs for any selected datastore. The datastore sub tabs include: a Summary tab that includes portlets: Details, Trends, and Top VMs by Disk Usage, and a Hosts tab.
Monitoring HyperFlex Clusters with HX Connect

The HX Connect user interface provides a view of the HX storage cluster status, components, and features, such as encryption and replication.

Key monitoring pages include information about the local HX storage cluster:

- **Dashboard**—Overall HX storage cluster status.
- **Alarms, Events, Activity**—See the Cisco HyperFlex Systems Troubleshooting Guide for details.
- **Performance**—Charts for IOPS, throughput, latency, and replication network bandwidth.
- **System Information**—System overview, plus status and tasks for nodes and disks.

See the Cisco HyperFlex Systems Troubleshooting Guide for generating support bundles, Storage Cluster Maintenance Operations Overview, on page 45 for entering and exiting maintenance mode, and Setting a Beacon, on page 47 to set a node or disk beacon.

- **Datastores**—Status and tasks related to datastores.
- **Virtual Machines**—Status and tasks related to protecting virtual machines.

Additional HX Connect pages provide management access:

- **Encryption**—For data at rest disk and node encryption tasks.
- **Replication**—For disaster recovery VM protection tasks.

The **Upgrade** page provides access to HX Data Platform and Cisco UCS Manager firmware upgrade tasks.

**Dashboard Page**

If you are a read-only user, you may not see all of the options available in the Help. To perform most actions in HX Connect, you must have administrative privileges.

Displays a status summary of your HX storage cluster. This is the first page that you see when you log in to Cisco HyperFlex Connect.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational Status</strong> section</td>
<td>Provides the functional status of the HX storage cluster and application performance.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Information</strong> (ℹ️) to access the HX storage cluster name and status data.</td>
</tr>
<tr>
<td><strong>Resiliency Health</strong> section</td>
<td>Provides the data health status and ability of the HX storage cluster to tolerate failures.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Information</strong> (ℹ️) to access the resiliency status, and replication and failure data.</td>
</tr>
</tbody>
</table>
### Essential Information

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capacity</strong></td>
<td>Displays a breakdown of the total storage versus how much storage is used or free. Also displays the storage optimization, compression-savings, and deduplication percentages based on the data stored in the cluster.</td>
</tr>
<tr>
<td><strong>Nodes</strong></td>
<td>Displays the number of nodes in the HX storage cluster, and the division of converged versus compute nodes. Hovering over a node icon displays that node's name, IP address, node type, and an interactive display of disks with access to capacity, usage, serial number, and disk type data.</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Displays an HX storage cluster performance snapshot for a configurable amount of time, showing IOPS, throughput, and latency data. For full details, see <a href="#">Performance Page</a>.</td>
</tr>
<tr>
<td><strong>Cluster Time</strong></td>
<td>System date and time for the cluster.</td>
</tr>
</tbody>
</table>

### Table Header Common Fields

Several tables in HX Connect provide one or more of the following three fields that affect the content displayed in the table.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Refresh</strong></td>
<td>The table automatically refreshes for dynamic updates to the HX Cluster. The timestamp indicates the last time the table was refreshed. Click the circular icon to refresh the content now.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>Display in the table only list items that match the entered filter text. The items listed in the current page of the table below are automatically filtered. Nested tables are not filtered. Type in the selection text in the Filter field. To empty the Filter field, click the x. To export content from other pages in the table, scroll to the bottom, click through the page numbers, and apply the filter.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Save out a copy of the current page of table data. The table content is downloaded to the local machine in the selected file type. If the listed items are filtered, the filtered subset list is exported. Click the down arrow to select an export file type. The file type options are: csv, xls, and doc. To export content from other pages in the table, scroll to the bottom, click through the page numbers, and apply the export.</td>
</tr>
</tbody>
</table>
**Activity Page**

Displays a list of recent activity on the HX storage cluster that was gathered from vSphere to monitor the progress of ReadyClone and VM-power operations.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Expand All / Collapse All button</strong></td>
<td>Toggles the view of the Activity list to display top-level task information or task details. You can also expand and collapse individual tasks.</td>
</tr>
</tbody>
</table>
| **Activity list** | Displays a list of recent tasks including the following details:  
  - ID  
  - Description  
  - VM power on/off/suspend status  
  - Task status:  
    - In Progress  
    - Success  
    - Failed  
  
  For failed VM-power operations, the **Existing State** and **Required State** fields are also included.  
  - Date and time stamp  
  - Progress bar  
  
  An expanded Activity list shows the task's step name and status. Click the circular icon to refresh the content now and fetch recent activity. The refresh rate is five minutes. |

**System Information Overview Page**

Displays HX storage cluster system-related information, including node and disk data, and provides access to HX maintenance mode.

**HX Storage Cluster Configuration Data**

Displays the basic configuration information for this HX storage cluster.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX storage cluster field</td>
<td>Name of this storage cluster.</td>
</tr>
</tbody>
</table>
## Essential Information

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
</table>
| HX storage cluster status field | Provides functional status of the HX storage cluster. Applicable for Stretched Cluster only—Provides the functional status of Site A, Site B, and the Witness site. Provides the IP address of the Witness site.  
  - **Online**—Cluster is ready.  
  - **Offline**—Cluster is not ready.  
  - **Read Only**—Cluster is out of space.  
  - **Unknown**—Transitional state while the cluster is coming online. |
| vCenter link | Secure URL to the VMware vSphere associated with this HX storage cluster. Click the link to remotely access the vSphere Web Client. |
| Hypervisor field | Hypervisor version installed on this HX storage cluster. |
| HXDP Version field | Installer package version installed on this HX storage cluster. |
| Data Replication Factor field | Number of the redundant data replicas stored on this HX storage cluster. |
| Uptime field | Length of time this HX storage cluster has been online. |
| Total Capacity field | Overall storage size of this cluster. |
| Available Capacity field | Amount of free storage in this cluster. |
| DNS Server(s) | IP address for the DNS server(s) for this HX storage cluster. |
| NTP Server(s) | IP address for the NTP server(s) for this HX storage cluster. |

### Node Data

Displays data about individual nodes in this HX storage cluster. To see this information in tabular format, go to the **Nodes** page.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node field</td>
<td>Name of a node on this cluster.</td>
</tr>
<tr>
<td>Model field</td>
<td>Physical hardware model number of this node.</td>
</tr>
<tr>
<td>Disks field</td>
<td>Number of caching versus persistent disks in this node.</td>
</tr>
<tr>
<td>Node status field</td>
<td></td>
</tr>
</tbody>
</table>
  - **Online**  
  - **Offline**  
  - **In Maintenance**  
  - **Healthy**  
  - **Warning** |
<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>HXDP Version field</td>
<td>Installer package version installed on this node.</td>
</tr>
<tr>
<td>Type field</td>
<td>• Hyper Converged</td>
</tr>
<tr>
<td></td>
<td>• Compute</td>
</tr>
<tr>
<td>Hypervisor Status field</td>
<td>• Online</td>
</tr>
<tr>
<td></td>
<td>• Offline</td>
</tr>
<tr>
<td></td>
<td>• In Maintenance</td>
</tr>
<tr>
<td></td>
<td>• In Progress</td>
</tr>
<tr>
<td>Hypervisor Address field</td>
<td>IP address for the management network to this HX storage cluster.</td>
</tr>
</tbody>
</table>

For nodes with disks, an interactive display of disks is included with the following pop-up data:

**Table 6: Caching Disks**

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot Number</td>
<td>Location of the drive.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Physical serial number of this disk.</td>
</tr>
<tr>
<td>Disk State</td>
<td>• Ready</td>
</tr>
<tr>
<td>Capacity</td>
<td>Total disk size.</td>
</tr>
<tr>
<td>Locator LED</td>
<td>Activates a physical light on the host to help locate a disk; options are On and Off.</td>
</tr>
</tbody>
</table>

**Table 7: Persistent Disks**

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot Number</td>
<td>Location of the drive.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Physical serial number of this disk.</td>
</tr>
<tr>
<td>Disk State</td>
<td>• Ready</td>
</tr>
<tr>
<td></td>
<td>• Blacklisted</td>
</tr>
<tr>
<td></td>
<td>• To Be Removed</td>
</tr>
<tr>
<td>Used / Total Capacity</td>
<td>Amount of the disk used versus the total disk size.</td>
</tr>
<tr>
<td>Storage Usage</td>
<td>Percentage of disk storage used.</td>
</tr>
<tr>
<td>Locator LED</td>
<td>Activates a physical light on the host to help locate a disk; options are On and Off.</td>
</tr>
</tbody>
</table>
Nodes Page

Displays data about all of the nodes in this HX storage cluster in an 8-column table. Each column can be used to sort the data.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter HX Maintenance Mode button</td>
<td>Select a node to access this button. Opens the Confirm HX Maintenance Mode dialog box.</td>
</tr>
<tr>
<td>Exit HX Maintenance Mode button</td>
<td>Select a node to access this button. After you complete any maintenance tasks, you must manually exit HX maintenance mode.</td>
</tr>
<tr>
<td>Node column</td>
<td>Name of a node in this HX storage cluster.</td>
</tr>
<tr>
<td>Hypervisor Address column</td>
<td>IP address for the management network to this HX storage cluster.</td>
</tr>
</tbody>
</table>
| Hypervisor Status column    | • Online  
                                 • Offline  
                                 • In Maintenance  
                                 • In Progress |
| Controller Address column   | IP address for the HX storage controller VM.                                           |
| Controller Status column    | • Online  
                                 • Offline  
                                 • In Maintenance |
| Model column                | Physical hardware model number of this node.                                          |
| Version column              | HyperFlex Data Platform installer package version installed on this node.             |
| Disks column                | Number of disks in the node. Click the number to open the Disks page filtered by the selected node name. |

Disks Page

Displays data about all of the disks in this HX storage cluster in a 7-column table. Each column can be used to sort the data.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node column</td>
<td>Name of the node where the disk resides.</td>
</tr>
<tr>
<td>Slot column</td>
<td>Location of the SED drive. This identifies the drive for maintenance procedures.</td>
</tr>
<tr>
<td>UI Element</td>
<td>Essential Information</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Capacity column</strong></td>
<td>Total disk size.</td>
</tr>
<tr>
<td><strong>Status column</strong></td>
<td></td>
</tr>
</tbody>
</table>

- **Available**—Initial state for a newly added, data-at-rest capable disk. Also, a transitional state when disks move into one of the other states.  
- **Blacklisted**—State when a disk is not being consumed by the cluster due to either a software error or an IO error. This could be a transitional state while the cluster attempts to repair the disk, if the disk is still available, before the state transitions to **Repairing**.  
- **Claimed**—State when a disk is recognized and in use.  
- **Ignored**—State when a disk is not being consumed by the cluster; for example, the HX controller VM system disk, a disk with other data (valid file system partitions), or a disk where the IO is failing.  
- **Ok To Remove**—State when an SED disk was securely erased using the Secure Erase option and can safely be removed.  
  
  **Note** For Cisco HX Data Platform 2.5, a disk in the **Ok to Remove** state is no longer consumed by the cluster.  
- **Repairing**—State when a blacklisted disk is currently being repaired.  
- **To Be Removed**—State when a disk is scheduled for RMA.  

| **Encrypted column** |  

- **Enabled**—Encryption is configured for this data-at-rest-capable disk.  
- **Disabled**—Encryption is not configured for this data-at-rest-capable disk. This occurs when a new disk is present, but the Key has not yet been applied.  
- **Locked**  
- **Unknown**  

The following states can be ignored:  

- **Invalid**  
- **Normal**  
- **Removed**—State when an SED disk is removed after using the Secure Erase option.  
- **Time out**  
- **Unknown**
<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type column</strong></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Rotational—Hybrid drive</td>
</tr>
<tr>
<td></td>
<td>• Solid State—SSD drive</td>
</tr>
<tr>
<td><strong>Usage column</strong></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Cache</td>
</tr>
<tr>
<td></td>
<td>• Persistent</td>
</tr>
<tr>
<td><strong>Turn On Locator LED and Turn Off Locator LED radio buttons</strong></td>
<td>Select a disk to access the radio buttons.</td>
</tr>
<tr>
<td></td>
<td>Activates or deactivates a physical light, or beacon, on the host to help locate the disk.</td>
</tr>
<tr>
<td><strong>(Optional) Secure erase button</strong></td>
<td>This button in visible only if your HX storage cluster is encrypted using local-key encryption.</td>
</tr>
<tr>
<td></td>
<td>Select a disk to access the button.</td>
</tr>
<tr>
<td></td>
<td>Enter the encryption key in use on the cluster, click Secure erase, and then click Yes, erase this disk to securely erase the local encryption key.</td>
</tr>
</tbody>
</table>
Preparing for HX Storage Cluster Maintenance

- Storage Cluster Maintenance Operations Overview, on page 45
- Serial vs. Parallel Operations, on page 47
- Checking Cluster Status, on page 47
- Setting a Beacon, on page 47
- Verify vMotion Configuration for HX Cluster, on page 48
- Maintenance Modes for Storage Cluster Nodes, on page 49
- Entering Cisco HyperFlex Maintenance Mode, on page 50
- Exiting Cisco HyperFlex Maintenance Mode, on page 51
- Creating a Backup Operation, on page 52
- Shut Down and Power Off the HX Storage Cluster, on page 56
- Power On and Start Up the HX Storage Cluster, on page 58
- Configure PCI Passthrough After Changing vNIC or vHBAs, on page 60

Storage Cluster Maintenance Operations Overview

Maintaining the HX Data Platform storage cluster tasks affect both hardware and software components of the storage cluster. Storage cluster maintenance operations include adding or removing nodes and disks, and network maintenance.

Some steps in maintenance tasks are performed from the storage controller VM of a node in the storage cluster. Some commands issued on a storage controller VM affect all the nodes in the storage cluster.

Note

Three node storage clusters. Contact Technical Assistance Center (TAC) for any task that requires removing or shutting down a node in a three node cluster. With any 3 node storage cluster, if one node fails or is removed, the cluster remains in an unhealthy state until a third node is added and joins the storage cluster.

Upgrading from vSphere 5.5 to 6.0. Before you upgrade either your ESX server or your vCenter server from 5.5 to 6.0, contact Technical Assistance Center (TAC).

Adding nodes. Nodes are added to the storage cluster through the Expand Cluster feature of the HX Data Platform Installer. All new nodes must meet the same system requirements as when you installed the HX Data Platform and created the initial storage cluster. See the Cisco HX Data Platform Getting Started Guide for a complete list of requirements and steps for using the Expand Cluster feature.
Online vs Offline Maintenance

Depending upon the task, the storage cluster might need to be either online or offline. Typically maintenance tasks require that all nodes in the storage cluster are online.

When storage cluster maintenance is performed in an offline mode, this means the Cisco HX Data Platform is offline, however the storage controller VMs are up and Cisco HX Data Platform management is viewable through the `stcli` command line, HX Connect, and HX Data Platform Plug-in. The vSphere Web Client can report on the storage I/O layer. The `stcli cluster info` command returns that the overall storage cluster status is offline.

Pre-Maintenance Tasks

Before you perform maintenance on the storage cluster, ensure the following.

- Identify the maintenance task to be performed.
  See

- All maintenance operations such as remove/replace resources are done during maintenance windows when the load on the system is low.

- The storage cluster is healthy and operational before the maintenance tasks.

- Identify disks using the HX Connect or HX Data Platform Plug-in Beacon options.
  The HX Beacon option is not available for housekeeping 120GB SSDs. Physically check the server for the location of the housekeeping SSD.

- Check the list of maintenance tasks that cannot be performed in parallel. Some tasks can only be performed serially to each other.

- Ensure that SSH is enabled on all the ESX hosts.

- Put the ESX host into HX maintenance mode prior to performing a maintenance task on the host. The HX maintenance mode performs additional storage cluster specific steps compared to the vSphere provided ESX maintenance mode.

Post Maintenance Tasks

After the maintenance task is completed, the nodes need to exit Maintenance Mode and the storage cluster needs to be restarted. In addition, some changes to the HX storage cluster require additional post maintenance tasks. For example, if you change the vNICS or vHBAs, the PCI Passthrough needs to be reconfigured.

Ensure the following:

- The ESX host is exited from HX maintenance mode after performing maintenance tasks on the host.

- The storage cluster is healthy and operational after any remove or replace tasks are completed.

- If vNICS or vHBAs have been added, removed, or replace on any ESX host in the HX storage cluster, reconfigure the PCI Passthrough.
Serial vs. Parallel Operations

Certain operations cannot be performed simultaneously. Ensure that you perform the following operations serially (not in parallel).

- Upgrade a storage cluster or a node.
- Create, re-create, or configure a storage cluster.
- Add or remove a node.
- Any node maintenance that requires a node be shutdown. This includes adding or removing disks or network interface cards (NICs).
- Start or shut down a storage cluster.
- Re-register a storage cluster with vCenter.

Checking Cluster Status

Step 1 Login to any controller VM in the storage cluster. Run the listed commands from the controller VM command line.

Step 2 Verify the storage cluster is healthy.

```bash
# stcli cluster info
```

Example response that indicates the storage cluster is online and healthy:

```
locale: English (United States)
state: online
upgradeState: ok
healthState: healthy
state: online
state: online
```

Step 3 Verify the number of node failures.

```bash
# stcli cluster storage-summary
```

Example response:

```
# of node failures tolerable to be > 0
```

Setting a Beacon

Beaconing is a method of turning on an LED to assist in locating and identifying a node (host) and a disk. Nodes have the beacon LED in the front near the power button and in the back. Disks have the beacon LED on the front face.

You set a node beacon through Cisco UCS Manager. You set a disk beacon through the HX Data Platform Plug-in or HX Connect user interface.
Step 1  
Turn on and off a node beacon using UCS Manager.  
   a) From the UCS Manager left panel, select Equipment > Servers > server.  
   b) From the UCS Manager central panel, select General > Turn on Locator LED.  
   c) After you locate the server, turn off the locator LED.  
      From the UCS Manager central panel, select General > Turn off Locator LED.

Step 2  
Turn on and off a disk beacon using the HX Data Platform Plug-in.  
   a) From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage.  
   b) From Manage, select Cluster > cluster > host > Disks > disk.  
   c) Locate the physical location of the object and turn on the beacon.  
      From Actions drop-down list, select Beacon ON.  
   d) After you locate the disk, turn off the beacon.  
      From Actions drop-down list, select Beacon OFF.

Step 3  
Turn on and off a disk beacon using HX Connect.  
   a) Log in to HX Connect.  
   b) Select System Information > Disks.  
   c) Select a node, and then click Turn On Locator LED or Turn Off Locator LED.  
      The beacon LED for all the disks on the selected node are toggled, except Housekeeping SSDs and cache NVMe SSDs.  
      Housekeeping SSDs or cache NVMe SSDs do not have functioning LED beacons.

Verify vMotion Configuration for HX Cluster

Before you perform maintenance operations on the HX cluster, verify all nodes in the HX cluster are configured for vMotion. Confirm the following from your vSphere Web Client:

1. Verify that the vMotion port group is configured with vmnic6 and vmnic7 in an active/standby configuration across all of the ESXi hosts in the cluster.

2. Verify that a port group is configured for vMotion, and that the naming convention is EXACTLY the same across all ESXi hosts in the cluster.

   **Note**  
The name is case-sensitive.

3. Verify that you have assigned a static IP to each vMotion port group, and that the static IPs for each vMotion port group are in the same subnet.

4. Verify that the vMotion port group has the vMotion option checked in the properties, and that no other port groups (such as management) have this option checked, on each ESXi host in the cluster.
5. Verify in the settings that the vMotion port group is set to 9000 MTU, (if you are using jumbo frames), and the VLAN ID matches the network configuration for the vMotion subnet.

6. Verify you can ping from the vMotion port group on one ESXi host to the vMotion IP on the other host.
   
   ```
   Type `vmkping -I vmk2 -d -s 8972 <vMotion IP address of neighboring server>`
   ```

---

**Maintenance Modes for Storage Cluster Nodes**

Maintenance mode is applied to nodes in a cluster. It prepares the node for assorted maintenance tasks by migrating all VMs to other nodes before you decommission or shut the node down.

There are two types of maintenance modes.

- Cisco HX maintenance mode
- VMware ESX maintenance mode

**Cisco HX Maintenance Mode**

Cisco HX maintenance mode performs HX Data Platform specific functions in addition to the ESX maintenance mode. Be sure to select Cisco HX maintenance mode and not ESX maintenance mode for maintenance tasks performed on storage cluster nodes after initial storage cluster creation.

This mode is the preferred maintenance mode for performing selected tasks on individual nodes in the cluster. Including:

- Shutting down an individual host for maintenance, such as disk replacement.
- Upgrading selected software on a host, such as ESX Server version.

**Cisco HX Maintenance Mode Considerations**

- Ensure that SSH is enabled in ESX on all the nodes in the storage cluster prior to using HX Maintenance Mode.
- When HX Maintenance Mode is entered to enable performing tasks on an ESX host, be sure to exit HX Maintenance Mode after the tasks on the ESX host are completed.
- Cisco HX Maintenance Mode is applied to nodes in a healthy cluster only. If the cluster is unhealthy, for example too many nodes are down, or you are shutting down the cluster, use ESX Maintenance Mode.
- See *Entering Cisco HyperFlex Maintenance Mode* and *Exiting Cisco HyperFlex Maintenance Mode* for steps.

**VMware ESX Maintenance Mode**

This mode is used when you are installing HX Data Platform or applying cluster wide changes.

To enter or exit vSphere maintenance mode:

- Through the vCenter GUI, select the **host**, then from the right-click menu select **maintenance mode**.
- Through the ESX command line, use the `esx maintenance mode` command.
Entering Cisco HyperFlex Maintenance Mode

Note
If you have replication configured, put replication in pause mode prior to performing upgrade or expansion or cluster maintenance. After the upgrade or expansion or cluster maintenance is completed, resume replication. Perform the pause and resume on any cluster that has replication configured to or from this local cluster.

If the HX Storage Cluster is offline, use the VMware Maintenance Mode.

Using the HX Connect User Interface

Note
Only supported on release 2.5(1a)/2.5(1b) and later releases.

1. Log in to HX Connect: https://<cluster management ip>.
2. In the menu, click System Information.
3. Click Nodes, and then click the row of the node you want to put in to maintenance mode.
4. Click Enter HX Maintenance Mode.
5. In the Confirm HX Maintenance Mode dialog box, click Enter HX Maintenance Mode.

Note
After you complete any maintenance tasks, you must manually exit HX maintenance mode.

Using the vSphere Web Client
1. Log in to the vSphere web client.
2. Go to Home > Hosts and Clusters.
3. Expand the Datacenter that contains the HX Cluster.
4. Expand the HX Cluster and select the node.
5. Right-click the node and select Cisco HX Maintenance Mode > Enter HX Maintenance Mode.

Using the Command-Line Interface
1. Log in to the storage controller cluster command line as a user with root privileges.
2. Move the node into HX Maintenance Mode.
   1. Identify the node ID and IP address.
      
      # stcli node list --summary
   2. Enter the node into HX Maintenance Mode.
Preparing for HX Storage Cluster Maintenance

```bash
# stcli node maintenanceMode (--id ID | --ip IP Address) --mode enter

(see also stcli node maintenanceMode --help)
```

3. Log in to the ESXi command line of this node as a user with root privileges.

4. Verify that the node has entered HX Maintenance Mode.

   ```bash
   # esxcli system maintenanceMode get
   
   You can monitor the progress of the Enter Maintenance Mode task in vSphere Web Client, under the Monitor > Tasks tab.
   
   If the operation fails, an error message displays. Try to fix the underlying problem and attempt to enter maintenance mode again. If you are unable to resolve the problem, please contact Cisco TAC.
   
### Exiting Cisco HyperFlex Maintenance Mode

**Note**

If you have replication configured, put replication in pause mode prior to performing upgrade or expansion or cluster maintenance. After the upgrade or expansion or cluster maintenance is completed, resume replication. Perform the pause and resume on any cluster that has replication configured to or from this local cluster.

**Using the HX Connect User Interface**

**Note**

Only supported on release 2.5(1a)/2.5(1b) and later releases.

1. Log in to HX Connect: `https://<cluster management ip>`.
2. In the menu, click System Information.
3. Click Nodes, and then click the row of the node you want to remove from maintenance mode.
4. Click Exit HX Maintenance Mode.

**Using the vSphere Web Client**

1. Log in to the vSphere web client.
2. Go to Home > Hosts and Clusters.
3. Expand the Datacenter that contains the HX Cluster.
4. Expand the HX Cluster and select the node.
5. Right-click the node and select Cisco HX Maintenance Mode > Exit HX Maintenance Mode.

**Using the Command-Line Interface**

1. Log in to the storage controller cluster command line as a user with root privileges.
2. Exit the node out of HX Maintenance Mode.
   1. Identify the node ID and IP address.
      
      # stcli node list --summary
   2. Exit the node out of HX Maintenance Mode.
      
      # stcli node maintenanceMode (--id ID | --ip IP Address) --mode exit
      (see also stcli node maintenanceMode --help)

3. Log into the ESXi command line of this node as a user with root privileges.
4. Verify that the node has exited HX Maintenance Mode.
   
   # esxcli system maintenanceMode get

You can monitor the progress of the Exit Maintenance Mode task in vSphere Web Client, under the Monitor > Tasks tab.

If the operation fails, an error message displays. Try to fix the underlying problem and attempt to exit maintenance mode again. If you are unable to resolve the problem, please contact Cisco TAC.

### Creating a Backup Operation

Before you shutdown your HX storage cluster, backup the configuration. Perform both the Full-State and All Configuration type backups with the Preserve Identities attribute.

**Before you begin**

1. Login to UCS Manager.
2. Obtain the backup server IPv4 or IPv6 address and authentication credentials.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click Admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the All node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, click the General tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Actions area, click Backup Configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Backup Configuration dialog box, click Create Backup Operation.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Create Backup Operation dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State field</td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Cisco UCS Manager runs the backup operation as soon as you click OK.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Cisco UCS Manager does not run the backup operation when you click OK. If you select this option, all fields in the dialog box remain visible. However, you must manually run the backup from the Backup Configuration dialog box.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Type field</strong></td>
<td>The information saved in the backup configuration file. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full state</strong>—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All configuration</strong>—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users.</td>
</tr>
<tr>
<td></td>
<td>• <strong>System configuration</strong>—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Logical configuration</strong>—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Preserve Identities check box | This checkbox remains selected for All Configuration and System Configuration type of backup operation, and provides the following functionality:  
  - **All Configuration**—The backup file preserves all identities derived from pools, including vHBAs, WWPNs, WWNN, vNICs, MACs and UUIDs. Also, the identities for Chassis, FEX, Rack Servers, and user labels for Chassis, FEX, Rack Servers, IOMs and Blade Servers are preserved.  
    - **Note** If this check box is not selected the identities will be reassigned and user labels will be lost after a restore.  
  - **System Configuration**—The backup file preserves identities for Chassis, FEX, Rack Servers, and user labels for Chassis, FEX, Rack Servers, IOMs and Blade Servers.  
    - **Note** If this check box is not selected the identities will be reassigned and user labels will be lost after a restore.  
  If this checkbox is selected for Logical Configuration type of backup operation, the backup file preserves all identities derived from pools, including vHBAs, WWPNs, WWNN, vNICs, MACs and UUIDs.  
    - **Note** If this check box is not selected the identities will be reassigned and user labels will be lost after a restore. |
| Location of the Backup File field | Where the backup file should be saved. This can be one of the following:  
  - **Remote File System**—The backup XML file is saved to a remote server. Cisco UCS Manager GUI displays the fields described below that allow you to specify the protocol, host, filename, username, and password for the remote system.  
  - **Local File System**—The backup XML file is saved locally.  
    HTML-based Cisco UCS Manager GUI displays the Filename field. Enter a name for the backup file in `<filename>.xml` format. The file is downloaded and saved to a location depending on your browser settings. |
### Protocol field

The protocol to use when communicating with the remote server. This can be one of the following:

- **FTP**
- **TFTP**
- **SCP**
- **SFTP**
- **USB A**—The USB drive inserted into fabric interconnect A. 
  This option is only available for certain system configurations.
- **USB B**—The USB drive inserted into fabric interconnect B. 
  This option is only available for certain system configurations.

### Hostname field

The hostname, IPv4 or IPv6 address of the location where the backup file is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.

**Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.

### Remote File field

The full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.

### User field

The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or USB.

### Password field

The password for the remote server username. This field does not apply if the protocol is TFTP or USB.

Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the backup operation immediately.

---

**Step 7**

Click OK.

**Step 8**

If Cisco UCS Manager displays a confirmation dialog box, click OK.

If you set the Admin State field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the Backup Operations table in the Backup Configuration dialog box.

**Step 9**

(Optional) To view the progress of the backup operation, do the following:

a) If the operation does not display in the Properties area, click the operation in the Backup Operations table.

b) In the Properties area, click the down arrows on the FSM Details bar.
The **FSM Details** area expands and displays the operation status.

**Step 10** Click **OK** to close the **Backup Configuration** dialog box.

The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

---

**Shut Down and Power Off the HX Storage Cluster**

Some storage cluster maintenance tasks require that the storage cluster be shutdown. This is different than the storage cluster being in an offline state. It is also separate from shutting down a node in the storage cluster. Powering down the storage cluster affects all the physical components of the cluster.

- **A powered off cluster** has all the physical components of the storage cluster removed from electrical power.

  Very rarely would a storage cluster need to have all the components powered off. No regular maintenance or upgrade processes require that the entire storage cluster be completely powered off.

- **A shutdown cluster** has all storage cluster processes, including the working VMs, powered down. This does not include powering down the nodes in the cluster or shutting down the vCenter or FI cluster.

- **An offline cluster** is one of the storage cluster operational states. A storage cluster can be offline if there is an unknown or specific error, or if the storage cluster has been shutdown.

**Before you begin**

- The storage cluster must be in a healthy state.

- Perform both the Full-State and All Configuration type backups with the Preserve Identities attribute. See *Creating a Backup Operation, on page 52.*

**Step 1** To shutdown the HX storage cluster, perform the following two steps.

**Step 2** Gracefully shutdown all workload VMs on all the HX datastores.

Alternatively, use vMotion to migrate the workload VMs to another cluster.

**Note** Do not shutdown or move the storage controller VMs (stCtlVMs).

**Step 3** Gracefully shutdown the HX storage cluster.

a) From any controller VM command line, run the command and wait for the shell prompt to return.

   ```bash
   # stcli cluster shutdown
   ```

b) Run the cluster information command. Confirm the storage cluster is offline.

   ```bash
   # stcli cluster info
   ```

   In the command response text, check the cluster subsection and verify the **healthstate** is **offline**.

This HX cluster shutdown procedure does not shutdown the ESXi hosts.
If the maintenance or upgrade task does not require the physical components be powered off, exit these steps and proceed to What to do next:

Step 4  **To power off the HX storage cluster**, complete Step 2 and Step 3, then complete the rest of the following steps.

Step 5  On each storage cluster ESX host, shutdown the controller VM (stCtlVM).

Choose a method:

**Using vCenter VM Power Off**

a) From vCenter client, locate the controller VM on each ESX host.
b) Right-click the controller VM and select **Power > Power Off**.

This method performs a graceful guest VM shutdown.

**Using vCenter ESX Agent Manager**

a) From vCenter client, open the ESX Agent Manager console.
b) Locate the controller VM on each ESX host, and select **Power > Power Off**.

This method performs a graceful shutdown of agent VMs. The controller VM is an agent VM.

**Using vCenter ESX Maintenance Mode**

a) From vCenter client, locate each ESX host.
b) Right-click the ESX host and select **Maintenance Mode > Enter Maintenance Mode**.

This method performs a hard shutdown on every VM in the ESX host, including the controller VM.

Step 6  Shutdown each storage cluster ESX host.

a) From the vCenter client, locate the host.
b) Right-click the host and select **Power > Shut Down**.

Step 7  Power off the FIs, if this is needed for your maintenance task.

Cisco UCS FIs are designed for continuous operation. In a production environment, there is no need to shut down or reboot Fabric Interconnects. Therefore, there is no power button on UCS Fabric Interconnects.

**To power off Cisco UCS Fabric Interconnect**, pull the power cable manually. Alternatively, if you have the FI power cables connected to a smart PDUs, use the provided remote control to turn off the power from the electrical outlet.

a) Verify all the storage cluster servers on the FI do not have a green power LED.
b) Power off the secondary FI.
c) Power off the primary FI.

The HX storage cluster is now safely powered off.

**What to do next**

1. Complete the task that required the storage cluster shutdown or power off. For example, an offline upgrade, physically moving the storage cluster, or performing maintenance on nodes.
   - For upgrade tasks, see the *Cisco HyperFlex Systems Upgrade Guide*.
   - For hardware replacement tasks, see the server hardware guides.
Sometimes these tasks require that the host is shutdown. Follow the steps in the server hardware guides for migrating VMs, entering HX Maintenance Mode, and powering down the servers, as directed.

**Note**

Most hardware maintenance tasks do not require the HX cluster is shutdown.

2. To restart the HX storage cluster, proceed to Power On and Start Up the HX Storage Cluster, on page 58.

---

### Power On and Start Up the HX Storage Cluster

The steps here are for use in restarting the HX storage cluster after a graceful shutdown and power off. Typically, this is performed after maintenance tasks are completed on the storage cluster.

**Before you begin**

Complete the steps in Shut Down and Power Off the HX Storage Cluster, on page 56.

---

**Step 1**

Plug in to power up the FIs.

a) Power on the primary FI. Wait until you can gain access to UCS Manager.

b) Power on the secondary FI. Verify it is online in UCS Manager.

In some rare cases, you might need to reboot the Fabric Interconnects.

1. Log in to each Fabric Interconnect using SSH.

2. Issue the commands:

   ```
   FI# connect local-mgmt
   FI# reboot
   ```

**Step 2**

Connect all the ESX hosts to the FIs.

a) Power on each node in the storage cluster, if it does not power on automatically.

   The node should automatically power on and boot into ESX. If any node does not, then connect to the UCS Manager and power up the servers (nodes) from UCS Manager.

b) Verify each ESX host is up and associated with its respective service profile in UCS Manager.

**Step 3**

Verify all the ESXi hosts are network reachable.

Ping all the management addresses.

**Step 4**

Power on all the controller VMs (stCtlVM).

Choose a method:

Using vSphere Client.

a) From the vSphere Client, view a storage controller host.

b) Right-click the stCtlVM and select Power > Power On.

c) Repeat for each host.
Using ESXi host command line.

a) Login to a host.
b) Identify the VMID of the stCtlVM.
   
   ```
   # vim-cmd vmsvc/getallvms
   ```
c) Using the VMID power on the controller VM.
   
   ```
   # vim-cmd vmsvc/power.on VMID
   ```
d) Repeat for each host.

**Step 5**
Wait for all the controller VMs to boot and become network reachable. Then verify.

Ping the management addresses of each of the controller VMs.

**Step 6**
Verify the storage cluster is ready to be restarted.

a) SSH to any controller VM, run the command:

   ```
   # stcli about
   ```
b) If the command returns full storage cluster information, including build number, the storage cluster is ready to be started. Proceed to restarting the storage cluster.
c) If the command does not return full storage cluster information, wait until all the services have started on the host.

**Step 7**
Optionally, exit each node from maintenance mode.

This is automatically completed by the **stcli cluster start** command.

**Step 8**
Restart the storage cluster.

From the command line of any controller VM, run the command.

```
# stcli cluster start
```

Depending upon the maintenance or upgrade task performed while the HX cluster was shutdown, the nodes might be exited from HX maintenance mode or ESX maintenance mode. Ignore any error messages about an unknown host exception.

**Step 9**
Wait until the storage cluster is online and returns to a healthy state.

a) From any controller VM, run the command.

   ```
   # stcli cluster info
   ```

b) In the command response text, check the cluster subsection and verify the healthstate is online.

This could take up to 30 minutes, it could take less time depending upon the last known state.

**Step 10**
Through vCenter, verify that ESX remounted the datastores.

Once the cluster is available, the datastores are automatically mounted and available.

If ESX does not recognize the datastores, from the ESX command line, run the command.

```
# esxcfg-nas -r
```

**Step 11**
When the storage cluster is healthy and the datastores are remounted, power on the workload VMs.

Alternatively, use vMotion to migrate the workload VMs back to the storage cluster.
Configure PCI Passthrough After Changing vNIC or vHBAs

Description
After vNIC or vHBA are manually added to an HX service profile or service profile template, the PCI devices are re-enumerated and the VMware directpath I/O configuration is lost. When the service profile is changed, the host hardware is updated and the PCI passthrough must be reconfigured. Perform the following steps on each ESX host with a modified service profile.

Perform the following steps on the storage controller VM of the modified ESX host:

Action: Update the vSphere Service Profile on the ESX Host

Step 1
Put the ESX host into HX Maintenance mode.

Step 2
Make or confirm the changes, such as adding hardware, in the Service Profile.

Step 3
Reboot the ESX host.
This host loses the direct path configuration.

Step 4
Login to vCenter and select the DirectPath I/O Configuration page.
From vCenter Client: Select the ESX host > Configuration tab > Hardware pane > Advanced Settings > Edit.
From vCenter Web Client: From the vCenter Inventory, select Resources > Hosts > ESX host > Manage > Settings > Hardware > PCI Devices > Edit.

Step 5
Select the LSI card for passthrough.

a) From the DirectPath I/O Configuration page, select Configure Passthrough.
b) From the Mark devices for passthrough list, select the LSI card for the passthrough.
c) Click OK.

Step 6
Reboot the ESX host.

Step 7
Re-map the PCI device to the HX storage controller VM (StCtlVM), by editing the storage controller VM settings.

a) Locate and remove the unknown PCI Device.

   From vCenter Client: Right-click the HX storage controller VM, select Edit Settings > PCI device 0 > Remove > OK.

   From vCenter Web Client: Right-click the HX storage controller VM, select Edit Settings > Remove PCI device 0 > OK.

b) Locate and re-add the LSI Logic PCI device.

   From vCenter Client: Right-click the HX storage controller VM, select Edit Settings > Add > PCI Device > LSI Logic PCI device > OK.

   From vCenter Web Client: Right-click the HX storage controller VM, select Edit Settings > PCI Device > Add > LSI Logic PCI device > OK.

Step 8
Remove the ESX host from HX Maintenance mode.
When the host is active again, the HX storage controller VM properly boots and rejoins the storage cluster.
Managing HX Storage Clusters

- Changing the Cluster Access Policy Level, on page 61
- Rebalancing the Cluster, on page 61
- Handling Out of Space Errors, on page 63
- Planning to Move a Storage Cluster Between vCenters, on page 64
- Renaming Clusters, on page 69

### Changing the Cluster Access Policy Level

**Step 1**
The storage cluster must be in a healthy state prior to changing the Cluster Access Policy to strict.

**Step 2**
From the command line of a storage controller VM in the storage cluster, type:

```
# stcli cluster get-cluster-access-policy
# stcli cluster set-cluster-access-policy --name {strict,lenient}
```

### Rebalancing the Cluster

The storage cluster is rebalanced on a regular schedule. It is used to realign the distribution of stored data across changes in available storage and to restore storage cluster health. If you add or remove a node in the storage cluster, you can manually initiate a storage cluster rebalance using the `stcli rebalance` command.

**Note**
Rebalancing might take some time depending on the disk capacity used on the failed node or disk.

**Step 1**
Start rebalancing the storage cluster.

a) Login to a controller VM in the storage cluster.

b) From the controller VM command line, run the command:

```
# stcli rebalance start --force
```
Step 2  Verify rebalancing status from the storage controller VM.
   a) Enter the following on the command line:
      
      ```
      # stcli rebalance status
      rebalanceStatus: rebalanceState: cluster_rebalance_ongoing
      percentComplete: 10
      rebalanceEnabled: True
      ```
   
   b) Reenter the command to monitor progress:
      
      ```
      # stcli rebalance status
      rebalanceStatus: percentComplete: 0
      rebalanceState: cluster_rebalance_not_running
      rebalanceEnabled: True
      ```
   
   c) Reenter the command line to confirm the process completes:
      
      ```
      # stcli rebalance status
      rebalanceStatus: rebalanceState: cluster_rebalance_not_running
      rebalanceEnabled: True
      ```
   
   This sample indicates that rebalance is enabled, and ready to perform a rebalance, but is not currently rebalancing the storage cluster.

Checking Cluster Rebalance and Self Healing Status

The storage cluster is rebalanced on a regular schedule and when the amount of available storage in the cluster changes. A rebalance is also triggered when there is a change in the amount of available storage. This is an automatic self-healing function.

You can check rebalance status through the HX Data Platform plug-in or through the storage controller VM command line.
The rebalanceState: cluster_rebalance_not_running
rebalanceEnabled: True

The Recent Tasks tab in the HX Data Platform plug-in displays a status message.

## Handling Out of Space Errors

If your system displays an Out of Space error, you can either add a node to increase free capacity or delete existing unused VMs to release space.

When there is an Out of Space condition, the VMs are unresponsive.

---

**Note**

Do not delete storage controller VMs. Storage controller VM names have the prefix `stCtlVM`.

---

### Step 1

To add a node, use the Expand Cluster feature of the HX Data Platform Installer.

### Step 2

To delete unused VMs, complete the following:

a) Determine which guest VMs you can delete. You can consider factors such as disk space used by the VM or naming conventions.

b) Go to `vCenter > Virtual Machines` to display the virtual machines in the inventory.

c) Double-click a VM that you want to delete.

    d) Select the *Summary > Answer Questions* to display a dialog box.

    e) Click the *Cancel* radio button and click *OK*.

    f) Power off the VM.

    g) Delete the VM.

### Step 3

After the Out of Space condition is cleared, complete the following:

a) Go to `vCenter > Virtual Machines` to display the VM in the inventory.

b) Double-click a VM that you want to use.

    c) Select the *Summary > Answer Questions* to display a dialog box.

    d) Click the *Retry* radio button and click *OK*.

---

## Checking Cleaner Schedule

The `stcli cleaner` command typically runs in the background continuously. The `cleaner` goes into sleep mode when it is not needed and wakes when policy defined conditions are met. For example, if your storage cluster is experiencing ENOSPC condition, the cleaner automatically runs at High Priority.

Do not expand the cluster while the `cleaner` is running. Check the cleaner schedule or adjust the schedule, as needed.

### Step 1

Login to any controller VM in the storage cluster. Run the listed commands from the controller VM command line.
Planning to Move a Storage Cluster Between vCenters

When you rename the vCenter datacenter or vCenter cluster, you must re-register the HX storage cluster.

Moving a storage cluster from one vCenter cluster to another requires the listed steps. See the following topics for detailed information.

1. Meet the prerequisites to this task. See Moving the Storage Cluster from a Current vCenter Server to a New VCenter Server, on page 64.

2. Delete the cluster from the old vCenter, create a new cluster on the new vCenter. Use the same cluster name. See Moving the Storage Cluster from a Current vCenter Server to a New VCenter Server, on page 64.

3. Unregister HX Data Platform using the vCenter Extension Manager. See Unregistering a Storage Cluster from a vCenter Cluster, on page 65.

4. Use the `stcli cluster reregister` command to associate the HX Storage Cluster with a new vCenter. See Registering a Storage Cluster with a New vCenter Cluster, on page 68.

Moving the Storage Cluster from a Current vCenter Server to a New VCenter Server

Before you begin

- If your HX Cluster is running HX Data Platform version older than 1.8(1c), upgrade before attempting to reregister to a new vCenter.
- Perform this task during a maintenance window.
- Ensure the cluster is healthy and upgrade state is OK and Healthy. You can view the state using the `stcli` command from the controller VM command line.

```bash
# stcli cluster info
```

Check response for:

```
upgradeState: ok
healthState: healthy
```

- Ensure vCenter must be up and running.
• Snapshot schedules are not moved with the storage cluster when you move the storage cluster between vCenter clusters.

Step 1
From the current vCenter, delete the cluster.
This is the vCenter cluster specified when the HX storage cluster was created.

Step 2
On the new vCenter, create a new cluster using the same cluster name.

Step 3
Add ESX hosts to new vCenter in the newly created cluster.

What to do next
Proceed to Unregistering a Storage Cluster from a vCenter Cluster, on page 65.

Unregistering a Storage Cluster from a vCenter Cluster

This step is optional and not required. It is recommended to leave the HX Data Platform Plug-in registration alone in the old vCenter.

Before you begin
As part of the task to move a storage cluster from one vCenter server to another vCenter server, complete the steps in Moving the Storage Cluster from a Current vCenter Server to a New vCenter Server, on page 64.

Note
• If multiple HX clusters are registered to the same vCenter, do not attempt this procedure until all HX clusters have been fully migrated to different vCenter. Running this procedure is disruptive to any existing HX clusters registered to the vCenter.

Step 1
Complete the steps in Unregistering and Removing EAM Extensions, on page 66.
This is the step that removes (unregisters) the HX cluster from the old vCenter server.
Also, if there are more ESX agencies than the number of HX clusters installed on the given vSphere server, it is likely there are stale EAM configurations that need cleanup.

Step 2
Complete the steps in Removing HX Data Platform Files from the vSphere Client, on page 67.

Step 3
Complete the steps in Verifying HX Cluster is Unregistered from vCenter, on page 68.

What to do next
Proceed to Registering a Storage Cluster with a New vCenter Cluster, on page 68.
Unregistering and Removing EAM Extensions

If you have partially installed or uninstalled HX Data Platform, or unregistered a HX cluster where there are more agencies than the number of HX clusters installed on the given vSphere, sometimes a stale ESX Agent Manager (EAM) for the HX Data Platform extension remains. Remove stale extensions using the Managed Object Browser (MOB) extension manager.

**Before you begin**
- Download the vSphere ESX Agent Manager SDK, if you have not already done so.
- If multiple HX clusters are registered to the same vCenter, do not attempt this procedure until all HX clusters have been fully migrated to a different vCenter. Running this procedure is disruptive to any existing HX clusters registered to the vCenter.
- Remove the datacenter from your vSphere cluster.

**Step 1** Identify the HX cluster UUID.

Every agency has a field `cluster_domain_id` which refers to the underlying vSphere extension. This extension ID uses a Managed Object ID (moid).

If you have multiple HyperFlex clusters, ensure that you select the correct cluster ID to unregister.

From a storage controller VM command line, run the command:

```bash
# stcli cluster info | grep vCenterClusterId:
vCenterClusterId: domain-c26
```

**Step 2** To unregister the storage cluster extension: Login to the vCenter server MOB extension manager

First unregister the HyperFlex cluster.

a) In a browser, enter the path and command.

```
https://vcenter_server/mob/?moid=ExtensionManager
```

`vcenter_server` is the IP address of the vCenter where the storage cluster is currently registered.

b) Enter administrator login credentials.

**Step 3** Locate the HX storage cluster extensions with the cluster IDs. Scroll through the Properties > extensionList to locate the storage cluster extensions:

```
com.springpath.sysmgmt.cluster_domain_id and com.springpath.sysmgmt.uuid.cluster_domain_id.
```

Copy each of these strings into your clipboard. Exclude the double quotes (" ) on either end of string, if there are any.

**Step 4** Unregister each storage cluster extension.

a) From the Methods table click UnregisterExtension.

b) In the UnregisterExtension popup, enter an extension key value, `com.springpath.sysmgmt.cluster_domain_id`.

For example: `com.springpath.sysmgmt.domain-26`

c) Click Invoke Method.

**Step 5** To remove stale EAM extensions: Login to the vCenter server MOB ESX agencies extension manager.

Second remove stale EAM extensions that were associated with the HyperFlex cluster.
a) In a browser, enter the path and command.

https://vcenter_server/eam/mob/

vcenter_server is the IP address of the vCenter where the storage cluster is currently registered.

b) Enter administrator login credentials.

Step 6 Locate the stale HX storage cluster ESX agency extensions with the cluster IDs.

a) Scroll through the Properties > agency > Value.

b) Click an agency value.

c) In the Agency window, check the Properties > solutionID > Value extension. Verify has the correct cluster_domain_id.

For example: com.springpath.sysgmt.domain-26

Step 7 Remove stale ESX agency extensions.

a) From the Agency window, Methods table select a method.

   Stale ESX agencies can be removed using either the destroyAgency or uninstall.

b) In the method popup, click Invoke Method.

Step 8 Refresh the ExtensionManager tab and verify that the extensionList entry does not include com.springpath.sysgmt.cluster_domain_id extensions.

Step 9 Restart the vSphere Client services.

The HX Data Platform extensions are removed when the vSphere Client services are restarted. Restarting the vSphere client service temporarily disables access to vCenter through the browser.

For additional information, see the VMware KB, Stopping, starting, or restarting VMware vCenter Server Appliance 6.0 services (2109887).

---

Removing HX Data Platform Files from the vSphere Client

This task is a step in unregistering a HX Storage Cluster from vCenter.

Remove the HX Data Platform files from the vSphere Client. Select a method.

Linux vCenter

a) Login to the Linux vCenter server using ssh as a root user.

b) Change to the folder containing the HX Data Platform Plug-in folder.

   For vCenter 6.0
   
   # cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/

   For vCenter 5.5

   # cd /var/lib/just/vmware/vsphere-client/vc-packages/vsphere-client-serenity/

c) Remove the HX Data Platform Plug-in folder and files.

   # rm -rf com.springpath*

d) Restart the vSphere Client.
Verifying HX Cluster is Unregistered from vCenter

This task is a step in unregistering a HX Storage Cluster from vCenter. Verify the HX cluster is no longer on the old vCenter.

**Before you begin**

Complete the steps in:

- Unregistering and Removing EAM Extensions, on page 66
- Removing HX Data Platform Files from the vSphere Client, on page 67

---

### Step 1
Logout out of the old vCenter.

### Step 2
Login in again to the old vCenter and verify the HX Data Platform Plug-in has been removed.

---

**Registering a Storage Cluster with a New vCenter Cluster**

**Before you begin**

As part of the task to move a storage cluster from one vCenter server to another vCenter server, complete the steps in Unregistering a Storage Cluster from a vCenter Cluster, on page 65.

---

### Step 1
Login to a controller VM.

### Step 2
Run the stcli cluster reregister command.

```
```
Apply additional listed options as needed.

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vcenter-cluster</td>
<td>Required.</td>
<td>Name of the new vCenter cluster.</td>
</tr>
<tr>
<td>NEWVCENTERCLUSTER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--vcenter-datacenter</td>
<td>Required.</td>
<td>Name of the new vCenter datacenter.</td>
</tr>
<tr>
<td>NEWDATACENTER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--vcenter-password</td>
<td>Optional.</td>
<td>Password of the new vCenter administrator.</td>
</tr>
<tr>
<td>NEWVCENTERPASSWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--vcenter-sso-url</td>
<td>Optional.</td>
<td>URL of the new vCenter SSO server. This is inferred</td>
</tr>
<tr>
<td>NEWVCENTERSSOURL</td>
<td></td>
<td>from --vcenter-url, if not specified.</td>
</tr>
<tr>
<td>--vcenter-url</td>
<td>Required.</td>
<td>URL of the new vCenter, &lt;&lt;vcentername&gt;&gt;. Where</td>
</tr>
<tr>
<td>NEWVCENTERURL</td>
<td></td>
<td>&lt;&lt;vcentername&gt;&gt; can be FQDN or IP.</td>
</tr>
<tr>
<td>--vcenter-user</td>
<td>Required.</td>
<td>User name of the new vCenter administrator.</td>
</tr>
<tr>
<td>NEWVCENTERUSER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example response:**

Reregister StorFS cluster with a new vCenter ...
Enter NEW vCenter Administrator password:
Waiting for Cluster creation to finish ...

If, after your storage cluster is re-registered, your compute only nodes fail to register with EAM, or are not present in the EAM client, and not under the resource pool, then contact TAC to complete the compute node reregister.

**Step 3**

If you have compute nodes on your cluster, after completing the reregister, re-add the compute nodes.

```bash
# stcli node add --node-ips <computeNodeIP> --controller-root-password <ctlvm-pwd> --esx-username <esx-user> --esx-password <esx-pwd>
```

**Step 4**

Re-enter your snapshot schedules.

Snapshot schedules are not moved with the storage cluster when you move the storage cluster between vCenter clusters.

---

## Renaming Clusters

After you create a HX Data Platform storage cluster, you can rename it without disrupting any processes.

### Note

These steps apply to renaming the HX Cluster, not the vCenter cluster.

**Step 1**

From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster** to rename.
Renaming Clusters

Step 2: Open the Rename Cluster dialog box. Either right-click on the storage cluster or click the Actions drop-down list at the top of the tab.

Step 3: Select Rename Cluster.

Step 4: Enter a new name for the storage cluster in the text field.

HX cluster names cannot exceed 50 characters.

Step 5: Click OK to apply the new name.
Managing Encryption

- Self-Encrypting Drives Overview, on page 71
- Verify if the HyperFlex Cluster Is Encryption Capable, on page 72
- Configuring Local Encryption Key, on page 72
- Modifying Local Encryption Key, on page 73
- Disabling Local Encryption Key, on page 73
- Secure Erase an Encrypted Disk, on page 74
- Remote Key Management, on page 74
- Configuring Remote Encryption Key, on page 74
- Generating Certificate Signing Requests, on page 75
- Configuring a Key Management Server Using CSRs (Certificate Signing Requests), on page 77
- Generating Self-Signed Certificates, on page 78
- Configuring a key management server using SSCs (Self-Signed Certificates), on page 79
- Start Over Encryption, on page 80

Self-Encrypting Drives Overview

Self-Encrypting Drives (SEDs) have special hardware that encrypts incoming data and decrypts outgoing data in real-time. The data on the disk is always stored in encrypted form. A media encryption key controls this encryption and decryption. This key is never stored in the processor or memory.

A security key, also known as Key-Encryption Key or an authentication passphrase, is used to encrypt the media encryption key. To enable SED, you must provide a security key. No key is required to fetch the data, if the disk is not locked.

Cisco HyperFlex Systems enables you to configure security keys locally or remotely. When you configure the key locally, you must remember the key. In case you forget the key, it cannot be retrieved, and the data is lost if the drive power cycles. You can configure the key remotely by using a key management server (also known as KMIP server). This method addresses the issues related to safe-keeping and retrieval of the keys in the local management.

The encryption and decryption for SEDs is done through the hardware. Thus, it does not affect the overall system performance. SEDs reduce the disk retirement and redeployment costs through instantaneous cryptographic erasure. Cryptographic erasure is done by changing the media encryption key. When the media encryption key of a disk is changed, the data on the disk cannot be decrypted, and is immediately rendered unusable.
Verify if the HyperFlex Cluster Is Encryption Capable

Verify Using the HX Data Platform Plug-in
1. From the HX Data Platform Plug-in log in to vSphere Web Client.
2. Select Cisco HX Data Platform > hx_cluster > Summary.
3. If the HyperFlex cluster has SED drives and is encryption capable, Data At Rest Encryption-Capable is listed at the top of the Summary tab.

Verify Using the HX Connect User Interface
1. From the HX Connect UI, select Encryption.
2. If the HX HyperFlex cluster has SED drives and is encryption capable, Data At Rest Encryption-Available is listed on the Encryption page.

Configuring Local Encryption Key

Step 1 On the Cisco HyperFlex Connect Navigation Pane, choose Encryption.
Step 2 On the Encryption Page, click Configure encryption.
Step 3 Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS Manager host name field</td>
<td>Cisco UCS Manager cluster host name. Enter an IP address or FQDN.</td>
</tr>
<tr>
<td></td>
<td>&lt;eng-fi12.eng.storvisor.com&gt;</td>
</tr>
<tr>
<td>User name field</td>
<td>&lt;admin&gt; username</td>
</tr>
<tr>
<td>Password field</td>
<td>&lt;root&gt; password</td>
</tr>
</tbody>
</table>

Click Next.

Step 4 To secure the HyperFlex cluster using an encryption key generated and stored locally, select Local Key.
Click Next.

Step 5 Enter the encryption key (passphrase) for this cluster.

Note Enter exactly 32 alphanumeric characters.

Step 6 Click Enable Encryption.
Modifying Local Encryption Key

**Step 1**  
On the Cisco HyperFlex Connect Navigation Pane, choose **Encryption**.

**Step 2**  
On the Encryption Page, click **Re-key**.

**Step 3**  
Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS Manager host name field</td>
<td>For example, 10.193.211.120.</td>
</tr>
<tr>
<td>User name field</td>
<td>&lt;admin&gt; username.</td>
</tr>
<tr>
<td>Password field</td>
<td>&lt;root&gt; password.</td>
</tr>
</tbody>
</table>

Click Next.

**Step 4**  
Enter the **Existing Encryption Key** and the **New Encryption Key** for the cluster.

**Note**  
Enter exactly 32 alphanumeric characters.

**Step 5**  
Click **Re-key**.

Disabling Local Encryption Key

**Step 1**  
On the Cisco HyperFlex Connect Navigation Pane, choose **Encryption**.

**Step 2**  
On the Encryption Page, from the **Edit configuration** drop-down menu, choose **Disable encryption**.

**Step 3**  
Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS Manager host name field</td>
<td>Cisco UCS Manager cluster host name.</td>
</tr>
<tr>
<td></td>
<td>Enter an IP address or FQDN.</td>
</tr>
<tr>
<td></td>
<td>&lt;eng-fi12.eng.storvisor.com&gt;</td>
</tr>
<tr>
<td>User name field</td>
<td>&lt;admin&gt; username</td>
</tr>
<tr>
<td>Password field</td>
<td>&lt;root&gt; password</td>
</tr>
</tbody>
</table>

Click Next.

**Step 4**  
To disable the encryption key on the cluster, enter the **encryption key** in use for the cluster.

**Step 5**  
Click **Disable encryption**.
Secure Erase an Encrypted Disk

Step 1  On the Cisco HyperFlex Connect Navigation Pane, choose System Information.
Step 2  From the Disks tab, select the disk from which you want to securely erase the local key.
Step 3  Click the Secure erase button.
Step 4  To securely erase the encrypted disk on the cluster, enter the encryption key in use on the cluster.
Step 5  Click Secure erase.
Step 6  In the Erase this disk? dialog box, click Yes, erase this disk to securely erase the encrypted disk.

Remote Key Management

The generic steps for remote KMIP certificate handling are as follows:

- If you are self-signing, specify local certificate authority in the configuration and get a root certificate.
- If you are using a trusted third-party CA, then specify that in the configuration and use their root certificate.
- Enter the root certificate in the HX encryption field that asks for the cluster key.
- Create an SSL server certificate and generate a Certificate Signing Request (CSR).
- Sign the CSR with whatever root certificate you are using.
- Update the KMIP server settings to use the client certificate.
- With the SSL certs and root CAs available, proceed with the KMIP service configuration specific to the vendor you have chosen.

SafeNet Key Management

For details on managing encryption keys using a SafeNet key management server, see the HyperFlex Encryption and SafeNet Key Management TechNote and the SafeNet Admin Guide.

Vormetric Key Management

For details on managing encryption keys using a vormetric key management server, see the Vormetric support portal documentation downloads section.

Configuring Remote Encryption Key

Step 1  On the Cisco HyperFlex Connect navigation Pane, choose Encryption.
Step 2
On the Encryption Page, click **Configure encryption**.

Step 3
Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS Manager host name field</td>
<td>Cisco UCS Manager cluster host name.</td>
</tr>
<tr>
<td></td>
<td>Enter an IP address or FQDN.</td>
</tr>
<tr>
<td></td>
<td>&lt;eng-fi12.eng.storvisor.com&gt;</td>
</tr>
<tr>
<td>User name field</td>
<td>&lt;admin&gt; username</td>
</tr>
<tr>
<td>Password field</td>
<td>&lt;root&gt; password</td>
</tr>
</tbody>
</table>

Click Next.

Step 4
To secure the HyperFlex cluster using a remote security key generated by the key management (KMIP) server, select **Key Management Server**.

You can configure a server with Self-Encrypting Drives in the cluster to use one of the following certificates.

- **Use certificate authority signed certificates**—Generate Certificate Signing Requests (CSRs) signed by an external certificate authority.
- **Use self-signed certificates**—Generate self-signed certificates.

Click Next.

Step 5

---

**What to do next**

You can generate certificate signing requests or self-signed certificates.

---

## Generating Certificate Signing Requests

Step 1
On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

Step 2
On the Encryption Page, click **Configure encryption**.

Step 3
Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS Manager host name field</td>
<td>Cisco UCS Manager cluster host name.</td>
</tr>
<tr>
<td></td>
<td>Enter an IP address or FQDN.</td>
</tr>
<tr>
<td></td>
<td>&lt;eng-fi12.eng.storvisor.com&gt;</td>
</tr>
<tr>
<td>User name field</td>
<td>&lt;admin&gt; username</td>
</tr>
<tr>
<td>Password field</td>
<td>&lt;root&gt; password</td>
</tr>
</tbody>
</table>
Click Next.

**Step 4** Select **Key Management Server > Use certificate authority signed certificates.**

Click Next.

**Step 5** To generate the remote encryption key for configuring the key management (KMIP) server, complete the following details.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address field</td>
<td>&lt;admin&gt; email address.</td>
</tr>
<tr>
<td>Organization name field</td>
<td>The organization requesting the certificate.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 32 characters.</td>
</tr>
<tr>
<td>Organization unit name field</td>
<td>The organizational unit.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 64 characters.</td>
</tr>
<tr>
<td>Locality field</td>
<td>The city or town in which the company requesting the certificate is headquartered.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 32 characters.</td>
</tr>
<tr>
<td>State field</td>
<td>The state or province in which the company requesting the certificate is headquartered.</td>
</tr>
<tr>
<td></td>
<td>Enter up to 32 characters.</td>
</tr>
<tr>
<td>Country field</td>
<td>The country in which the company resides.</td>
</tr>
<tr>
<td></td>
<td>Enter two alphabetic characters in uppercase.</td>
</tr>
<tr>
<td>Valid for (days) field</td>
<td>The validity period of the certificate.</td>
</tr>
</tbody>
</table>

**Step 6** To generate Certificate Signing Requests (CSRs) for all the HyperFlex nodes and download them, click **Generate certificates.**

**Step 7** Download the certificates to get them signed by a certificate authority. Click **Close.**

---

**What to do next**

1. Upload the signed certificates.
2. Configure KMIP server (key management server).
Configuring a Key Management Server Using CSRs (Certificate Signing Requests)

**Before you begin**
Ensure that you have downloaded the generated CSRs on your local machine, signed it by a certificate authority and uploaded through the Cisco HX Data Platform UI for configuring the KMIP (key management) server.

---

**Step 1**
On the Cisco HyperFlex Connect navigation Pane, choose *Encryption*.

**Step 2**
On the Encryption Page, click *Continue configuration*.

**Step 3**
From the *Continue configuration* drop-down list, select *Manage certificates* to upload the CSRs.

**Step 4**
Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UCS Manager host name</strong> field</td>
<td>Cisco UCS Manager cluster host name.</td>
</tr>
<tr>
<td></td>
<td>Enter an IP address or FQDN.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;eng-fi12.eng.storvisor.com&gt;</code></td>
</tr>
<tr>
<td><strong>User name</strong> field</td>
<td><code>&lt;admin&gt;</code> username</td>
</tr>
<tr>
<td><strong>Password</strong> field</td>
<td><code>&lt;root&gt;</code> password</td>
</tr>
</tbody>
</table>

Click *Next*.

**Step 5**
Select *Upload certificate authority signed certificates*. Click *Next*.

**Step 6**
Upload the CA signed certificate under *Upload new certificate*. Click *Upload*.

**Step 7**
From the *Continue configuration* drop-down list select *Configure key management server* to configure the KMIP server.

**Step 8**
Enter Cisco UCS Manager credentials to set up a primary key management server (KMIP) server and optionally a secondary KMIP server.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary key management server</strong> field</td>
<td>Enter the primary Key Management Server IP address.</td>
</tr>
<tr>
<td><em>(Optional) Secondary key management server</em>* field</td>
<td>If you have a secondary key management server set up for redundancy, enter the details here.</td>
</tr>
<tr>
<td><strong>Port number</strong> field</td>
<td>Enter the port number you wish to use for the key management servers.</td>
</tr>
<tr>
<td><strong>Public key</strong> field</td>
<td>Enter the public root certificate of the certificate authority that you generated during KMIP server configuration.</td>
</tr>
</tbody>
</table>
Step 9  
Click **Save** to encrypt the cluster with remotely managed keys.

---

Example

### Generating Self-Signed Certificates

**Step 1**  
On the Cisco HyperFlex Connect navigation Pane, choose **Encryption**.

**Step 2**  
On the Encryption Page, click **Configure encryption**.

**Step 3**  
Enter the following Cisco UCS Manager credentials.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UCS Manager host name</strong></td>
<td>Cisco UCS Manager cluster host name.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>&lt;admin&gt; username</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>&lt;root&gt; password</td>
</tr>
</tbody>
</table>

Click **Next**.

**Step 4**  
Select **Key Management Server > Use self-signed certificates**.

Click **Next**.

**Step 5**  
To generate the remote encryption key for configuring the key management (KMIP) server, complete the following details.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email address</strong></td>
<td>&lt;admin&gt; email address.</td>
</tr>
<tr>
<td><strong>Organization name</strong></td>
<td>The organization requesting the certificate. Enter up to 32 characters.</td>
</tr>
<tr>
<td><strong>Organization unit name</strong></td>
<td>The organizational unit. Enter up to 64 characters.</td>
</tr>
<tr>
<td><strong>Locality</strong></td>
<td>The city or town in which the company requesting the certificate is headquartered. Enter up to 32 characters.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The state or province in which the company requesting the certificate is headquartered. Enter up to 32 characters.</td>
</tr>
</tbody>
</table>
### Configuring a key management server using SSCs (Self-Signed Certificates)

#### What to do next
1. Upload the signed certificates.
2. Configure KMIP server (key management server).

#### Configuring a key management server using SSCs (Self-Signed Certificates)

**Before you begin**
Ensure that you have downloaded the generated SSCs on your local machine to configure the KMIP (key management) server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On the Cisco HyperFlex Connect navigation Pane, choose <strong>Encryption</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>On the Encryption Page, click <strong>Edit configuration</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>From the <strong>Edit configuration</strong> drop-down list, select <strong>Manage certificates</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Enter the following Cisco UCS Manager credentials, to set up a primary key management (KMIP) server and optionally a secondary KMIP server.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the primary and secondary key management (KMIP) server credentials.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UCS Manager host name</strong> field</td>
<td>Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <em>&lt;eng-fi12.eng.storvisor.com&gt;</em></td>
</tr>
<tr>
<td><strong>User name</strong> field</td>
<td><em>&lt;admin&gt;</em> username</td>
</tr>
<tr>
<td><strong>Password</strong> field</td>
<td><em>&lt;root&gt;</em> password</td>
</tr>
</tbody>
</table>

Click **Next**.
**Step 6**
Click **Save** to encrypt the cluster with remotely managed keys.

---

**Start Over Encryption**

Enter Cisco UCS Manager credentials to restart configuring the key management server or local key, for securely encrypting the HyperFlex cluster.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UCS Manager host name</strong> field</td>
<td>Cisco UCS Manager cluster host name.</td>
</tr>
<tr>
<td></td>
<td>Enter an IP address or FQDN.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;eng-fi12.eng.storvisor.com&gt;</code></td>
</tr>
<tr>
<td><strong>User name</strong> field</td>
<td><code>&lt;admin&gt;</code> username</td>
</tr>
<tr>
<td><strong>Password</strong> field</td>
<td><code>&lt;root&gt;</code> password</td>
</tr>
</tbody>
</table>
Managing Datastores

Datastores are logical containers used by the HX Data Platform to manage your storage use and storage resources. Datastores are where the host places virtual disk files and other VM files. Datastores hide the specifics of physical storage devices and provide a uniform model for storing VM files.

You can add, refresh the list, edit name and size, delete, mount, and unmount datastores from either the HX Connect or HX Data Platform Plug-in UIs.

Step 1  Choose an interface.
- From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage > Datastores**.
- From HX Connect, select **Datastores**.

Step 2  Create a new or select an existing datastore, to view options.
- Create a new datastore
- Refresh the datastore list
- Edit the datastore name and size
- Delete the datastore
- Mount the datastore on the host
- Unmount the datastore from the host
Adding Datastores

Datastores are logical containers, similar to file systems, that hide specifics of physical storage and provide a uniform model for storing VM files. You can also use datastores to store ISO images and VM templates.

Step 1
Choose an interface.

- From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage > Datastores.
- From HX Connect, select Datastores.

Step 2
Select the create datastore.

Step 3
Enter a name for the datastore. vSphere Web Client enforces a 42 character limit for the datastore name. Assign each datastore a unique name.

Step 4
Specify the datastore size. Choose GB or TB from the drop-down list.

Step 5
Specify the data block size. From HX Connect, choose 8K or 4K. Default is 8K. In the HX Data Platform Plug-in, the default is assumed. For VDI workloads, default is 4K.

Step 6
Click OK to accept your changes or Cancel to cancel all changes.

Step 7
Verify the datastore. Click the Refresh icon if needed to display your new datastore.

From HX Data Platform Plug-in, Click the Manage > Datastores > Hosts tab to see the mount status of the new datastore.

If you check the datastore through the vSphere Client application, host > Configuration > Datastores, the Drive Type is listed as Unknown. This is expected vSphere behavior, to list NFS datastores as Unknown.

Editing Datastores

A HX Data Platform datastore can be modified using the edit (pencil) option. Edit options are:

- Change the datastore name.

  Do not rename datastores with controller VMs.

- Change the datastore storage allocation. That is, the size of the datastore.

Step 1
Choose an interface.

- From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage > Datastores.
- From HX Connect, select Datastores.

Step 2
Select a datastore.
Step 3 Unmount the datastore.

If you are only resizing the datastore, you do not need to unmount the datastore. Skip this step.

Step 4 Click the Edit (pencil icon) datastore.

Step 5 Change the datastore name and/or size, as needed. Click OK.

Step 6 Remount the datastore, if you previously unmounted it.

---

**Mounting Datastores**

**Prepare to mount a datastore.**

- No VM, template, snapshot, or CD/DVD image resides on the datastore. This is the most common error while unmounting.
- Storage I/O Control is disabled for the datastore.
- The datastore is not used for vSphere HA heartbeat.
- The datastore is not used to host RDM metadata files. RDM is not supported.
- The datastore is not used as a scratch location.

**Mount a datastore.**

---

**Step 1** Choose an interface.

- From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage > Datastores.
- From HX Connect, select Datastores.

**Step 2** Select a datastore.

**Step 3** Click the Mount.

**Step 4** Confirm to mount the datastore, click OK.

---

**Unmounting Datastores**

**Prepare to unmount a datastore.**

- No VM, template, snapshot, or CD/DVD image resides on the datastore. This is the most common error while unmounting.
- Storage I/O Control is disabled for the datastore.
- The datastore is not used for vSphere HA heartbeat.
- The datastore is not used to host RDM metadata files. RDM is not supported.
The datastore is not used as a scratch location.

**Unmount a datastore.**

---

### Step 1
Choose an interface.

- From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage > Datastores.
- From HX Connect, select Datastores.

### Step 2
Select a datastore.

### Step 3
Click the Unmount.

### Step 4
Confirm to unmount the datastore, click OK.

### Step 5
If needed, recover from partial unmounts.
- Go through the above checklist and unmount or delete through one of the UIs or CLI again.
- Use the UI or CLI to re-mount the datastore.

---

## Deleting Datastores

Prepare to delete the datastores.

- Power off all VMs.
- Close all open shells on the datastore mount point.
- Disable HA on the datastore.
- Close all applications that use the datastore.

Delete datastores.

---

### Step 1
Choose an interface.

- From the vSphere Web Client Navigator, select vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Manage > Datastores.
- From HX Connect, select Datastores.

### Step 2
Select a datastore.

### Step 3
Click the Delete.

### Step 4
Confirm to delete the datastore, click OK.
Recovering from Partially Unmounted Datastores

When mounting, unmounting, or deleting datastores, sometime a datastore can become partially unmounted. If this occurs, complete the following, as needed.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Depending upon the task you are attempting, complete the items in Prepare to mount a datastore, Prepare to unmount a datastore, or Prepare to delete the datastores.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Retry to mount, unmount, or delete the datastore through the HX Connect or HX Data Platform Plug-in UI or CLI again.</td>
</tr>
<tr>
<td>Step 3</td>
<td>If the datastore is not in the desired mount, unmount, or deleted state, complete the following.</td>
</tr>
<tr>
<td>a)</td>
<td>Ensure VMs are not running on the datastore.</td>
</tr>
<tr>
<td>b)</td>
<td>From ESX host, check to see if the HX Data Platform datastore is being used by VMware service, storageRM.</td>
</tr>
<tr>
<td></td>
<td># ls -lta /vmfs/volumes/stfs-ds1/</td>
</tr>
<tr>
<td></td>
<td>Sample response</td>
</tr>
<tr>
<td></td>
<td>-rwxr-xr-x 1 root root 16511 Jan 20 20:05 .iormstats.sf</td>
</tr>
<tr>
<td></td>
<td>drwxr-xr-x 1 root root 1125 Jan 20 20:06 .iorm.sf</td>
</tr>
<tr>
<td>c)</td>
<td>Check the storageRM status.</td>
</tr>
<tr>
<td></td>
<td># /etc/init.d/storageRM status</td>
</tr>
<tr>
<td></td>
<td>Sample response</td>
</tr>
<tr>
<td></td>
<td>storageRM is running</td>
</tr>
<tr>
<td>d)</td>
<td>Stop the storageRM service.</td>
</tr>
<tr>
<td></td>
<td># /etc/init.d/storageRM stop</td>
</tr>
<tr>
<td></td>
<td>Sample response</td>
</tr>
<tr>
<td></td>
<td>watchdog-storageRM: Terminating watchdog process with PID 34096</td>
</tr>
<tr>
<td></td>
<td>storageRM stopped</td>
</tr>
<tr>
<td>e)</td>
<td>Try to mount, unmount, or delete the datastore again.</td>
</tr>
<tr>
<td>f)</td>
<td>This is one possible solution, if this doesn't resolve the issue, contact Technical Assistance Center (TAC).</td>
</tr>
</tbody>
</table>
Recovering from Partially Unmounted Datastores
Managing Disks

Managing Disks in the Cluster

Disks, SSDs or HDDs, might fail. If this occurs, you need to remove the failed disk and replace it. Follow the server hardware instructions for removing and replacing the disks in the host. The HX Data Platform identifies the SSD or HDD and incorporates it into the storage cluster.

To increase the datastore capacity of a storage cluster add the same size and type SSDs or HDDs to each converged node in the storage cluster. For hybrid servers, add hard disk drives (HDDs). For all flash servers, add SSDs.

Note

When performing a hot-plug pull and replace on multiple drives, pause for a few moments (30 seconds) between each action. Pull and replace a drive, pause, pull and replace the next drive.

Sometimes, when a disk is removed it continues to be listed in cluster summary information. To refresh this, restart the HX cluster.

Disk Requirements

The disk requirements vary between converged nodes and compute-only nodes. To increase the available CPU and memory capacity, you can expand the existing cluster with compute-only nodes as needed. These compute-only nodes provide no increase to storage performance or storage capacity.

Alternatively, adding converged nodes increase storage performance and storage capacity alongside CPU and memory resources.
Servers with only Solid-State Disks (SSDs) are All-Flash servers. Servers with both SSDs and Hard Disk Drives (HDDs) are hybrid servers.

The following applies to all the disks in a HyperFlex cluster:

- All the disks in the storage cluster must have the same amount of storage capacity. All the nodes in the storage cluster must have the same number of disks.
- All SSDs must support TRIM and have TRIM enabled.
- All HDDs can be either SATA or SAS type. All SAS disks in the storage cluster must be in a pass-through mode.
- Disk partitions must be removed from SSDs and HDDs. Disks with partitions are ignored and not added to your HX storage cluster.
- Optionally, you can remove or backup existing data on disks. All existing data on a provided disk is overwritten.

**Note**

New factory servers are shipped with appropriate disk partition settings. Do not remove disk partitions from new factory servers.

- Only the disks ordered directly from Cisco are supported.
- On servers with Self Encrypting Drives (SED), both the cache and persistent storage (capacity) drives must be SED capable. These servers support Data at Rest Encryption (DARE).

**Converged Nodes**

In addition to the disks listed in the table below, all M4 converged nodes have 2 x 64-GB SD FlexFlash cards in a mirrored configuration with ESX installed. All M5 converged nodes have M.2 SATA SSD with ESXi installed.

**Note**

Do not mix storage disks type or storage size on a server or across the storage cluster. Mixing storage disk types is not supported.

- When replacing cache or persistent disks, always use the same type and size as the original disk.
- Do not mix any of the persistent drives. Use all HDD or SSD and the same size drives in a server.
- Do not mix hybrid and All-Flash cache drive types. Use the hybrid cache device on hybrid servers and All-Flash cache devices on All-Flash servers.
- Do not mix encrypted and non-encrypted drive types. Use SED hybrid or SED All-Flash drives. On SED servers, both the cache and persistent drives must be SED type.
- All nodes must use same size and quantity of SSDs. Do not mix SSD types.

The following tables list the compatible drives for each HX server type. Drives are located in the front slots of the server, unless otherwise indicated. Multiple drives listed are options. Use one drive size for capacity per server. Minimum and maximum number of drives are listed for each component.
### HX240 M5 Servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housekeeping SSD</td>
<td>1</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
</tr>
<tr>
<td>Cache SSD</td>
<td>1</td>
<td>1.6 TB SSD</td>
<td>1.6 TB SSD</td>
<td>1.6 TB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td>Persistent</td>
<td>6-23</td>
<td>1.2 TB HDD</td>
<td>960 GB SSD</td>
<td>1.2 TB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.8 TB HDD</td>
<td>3.8 TB SSD</td>
<td></td>
<td>960 GB SSD</td>
</tr>
</tbody>
</table>

### HX240 M4 Servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housekeeping SSD</td>
<td>1</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
</tr>
<tr>
<td>Cache SSD</td>
<td>1</td>
<td>1.6 TB SSD</td>
<td>1.6 TB SSD</td>
<td>1.6 TB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td>Persistent</td>
<td>6-23</td>
<td>1.2 TB HDD</td>
<td>960 GB SSD</td>
<td>1.2 TB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.8 TB HDD</td>
<td>3.8 TB SSD</td>
<td></td>
<td>960 GB SSD</td>
</tr>
</tbody>
</table>

### HX220 M5 Servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housekeeping SSD</td>
<td>1</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
</tr>
<tr>
<td>Cache SSD</td>
<td>1</td>
<td>480 GB SSD</td>
<td>1.6 TB SSD</td>
<td>800 GB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td>Persistent</td>
<td>6-8</td>
<td>1.2 TB HDD</td>
<td>960 GB SSD</td>
<td>1.2 TB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.8 TB HDD</td>
<td>3.8 TB SSD</td>
<td></td>
<td>960 GB SSD</td>
</tr>
</tbody>
</table>

### HX 220 M4 Servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housekeeping SSD</td>
<td>1</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td></td>
<td>240 GB SSD</td>
</tr>
</tbody>
</table>
### Disk Requirements

The following table lists the supported compute-only node configurations for compute-only functions. Storage on compute-only nodes is not included in the cache or capacity of storage clusters.

#### Note

When adding compute nodes to your HyperFlex cluster, the compute-only service profile template automatically configures it for booting from an SD card. If you are using another form of boot media, update the local disk configuration policy. See the Cisco UCS Manager Server Management Guide for server-related policies.

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent</td>
<td>6</td>
<td>1.2 TB HDD</td>
<td>960 GB SSD</td>
<td>1.2 TB HDD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.8 TB HDD</td>
<td>3.8 TB SSD</td>
<td></td>
<td>960 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>800 GB SSD</td>
<td></td>
<td></td>
<td>3.8 TB SSD</td>
</tr>
</tbody>
</table>

### HX220 M5 Servers for Edge Clusters

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housekeeping SSD</td>
<td>1</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
<td>240 GB SSD</td>
</tr>
<tr>
<td>Cache SSD</td>
<td>1</td>
<td>480 GB SSD</td>
<td>1.6 TB NVMe</td>
<td>800 GB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td>Persistent</td>
<td>3-8</td>
<td>1.2 TB HDD</td>
<td>960 GB SSD</td>
<td>1.2 TB HDD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.8 TB SSD</td>
<td></td>
<td>960 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.8 TB SSD</td>
</tr>
</tbody>
</table>

### HX 220 M4 Servers for Edge Clusters

<table>
<thead>
<tr>
<th>Component</th>
<th>Qty</th>
<th>Hybrid</th>
<th>All Flash</th>
<th>Hybrid SED</th>
<th>All Flash SED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Housekeeping SSD</td>
<td>1</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
<td>120 GB SSD</td>
</tr>
<tr>
<td>Cache SSD</td>
<td>1</td>
<td>480 GB SSD</td>
<td>400 GB SSD</td>
<td>800 GB SSD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td>Persistent</td>
<td>3-6</td>
<td>1.2 TB HDD</td>
<td>960 GB SSD</td>
<td>1.2 TB HDD</td>
<td>800 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.8 TB SSD</td>
<td></td>
<td>960 GB SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.8 TB SSD</td>
</tr>
</tbody>
</table>
Supported Compute-Only Node Servers | Supported Methods for Booting ESXi
---|---
- Cisco B200 M3/M4/M5
- B260 M4
- B420 M4
- B460 M4
- C240 M3/M4/M5
- C220 M3/M4/M5
- C460 M4
- C480 M5
- B480 M5

Choose any method.

**Important**

- Ensure that only one form of boot media is exposed to the server for ESXi installation.
- Post install, you may add in additional local or remote disks.
- USB boot is not supported for HX Compute-only nodes.

- SD Cards in a mirrored configuration with ESXi installed.
- Local drive HDD or SSD.
- SAN boot.
- M.2 SATA SSD Drive.

---

**Replacing Self Encrypted Drives (SEDs)**

Cisco HyperFlex Systems offers Data-At-Rest protection through Self-Encrypting Drives (SEDs) and Enterprise Key Management Support.

- Servers that are data at rest capable refer to servers with self encrypting drives.
- All servers in an encrypted HX Clusters must be data at rest capable.
- Encryption is configured on a HX Cluster, after the cluster is created, using HX Connect.
- Servers with self encrypting drives can be either solid state drive (SSD) or hybrid.

---

**Important**

Before you begin

To ensure the encrypted data remains secure, the data on the drive must be **securely erased** prior to removing the SED.

**Before you begin**

Determine if the encryption is applied to the HX Cluster.

- **Encryption not configured**—No encryption related prerequisite steps are required to remove or replace the SED. See Replacing SSDs, on page 93 or Replacing or Adding Hard Disk Drives, on page 96 and the hardware guide for your server.

- **Encryption is configured**—Ensure the following:
  1. If you are replacing the SED, obtain a Return to Manufacturer Authorization (RMA). Contact TAC.
  2. If you are using a local key for encryption, locate the key. You will be prompted to provide it.
  3. To prevent data loss, ensure the data on the disk is not the last primary copy of the data.
If needed, add disks to the servers on the cluster. Initiate or wait until a rebalance completes.

4. Complete the steps below before removing any SED.

**Step 1**
Ensure the HX Cluster is healthy.
If the cluster is not healthy, contact TAC to remove or replace an SED.

**Step 2**
Login to HX Connect.

**Step 3**
Select **System Information** > **Disks** page.

**Step 4**
Identify and verify the disk to remove.
1. Use the Turn On Locator LED button.
2. Physically view the disks on the server.
3. Use the Turn Off Locator LED button.

**Step 5**
Select the corresponding **Slot** row for the disk to be removed.

**Step 6**
Click **Secure erase**. This button is available only after a disk is selected.

**Step 7**
If you are using a local encryption key, enter the **Encryption Key** in the field and click **Secure erase**.
If you are using a remote encryption server, no action is needed.

**Step 8**
Confirm deleting the data on this disk, click **Yes, erase this disk**.
**Warning**  This deletes all your data from the disk.

**Step 9**
Wait until the **Status** for the selected **Disk Slot** changes to **Ok To Remove**, then physically remove the disk as directed.

---

**What to do next**

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not reuse a removed drive in a different server in this, or any other, HX Cluster. If you need to reuse the removed drive, contact TAC.</td>
</tr>
</tbody>
</table>

1. After securely erasing the data on the SED, proceed to the disk replacing tasks appropriate to the disk type: SSD or hybrid.

   Check the **Type** column for the disk type.

   - **Solid State** (SSDs)—See **Replacing SSDs**, on page 93 and the hardware guide for your server.

   - **Rotational** (hybrid drives)—See **Replacing or Adding Hard Disk Drives**, on page 96 and the hardware guide for your server.

2. Check the status of removed and replaced SEDs.

   When the SED is removed:
   - **Status**—Remains **Ok To Remove**.
• **Encryption**—Changes from **Enabled** to **Unknown**.

When the SED is replaced, the new SED is automatically consumed by the HX Cluster. If encryption is not applied, the disk is listed the same as any other consumable disk. If encryption is applied, the security key is applied to the new disk.

• **Status**—Transitions from **Ignored** > **Claimed** > **Available**.

• **Encryption**—Transitions from **Disabled** > **Enabled** after the encryption key is applied.

---

**Replacing SSDs**

The procedures for replacing an SSD vary depending upon the type of SSD. Identify the failed SSD and perform the associated steps.

---

**Note**

Mixing storage disks type or size on a server or across the storage cluster is not supported.

- Use all HDD, or all 3.8 TB SSD, or all 960 GB SSD
- Use the hybrid cache device on hybrid servers and all flash cache devices on all flash servers.
- When replacing cache or persistent disks, always use the same type and size as the original disk.

---

**Step 1**

Identify the failed SSD.

- For cache or persistent SSDs, perform a disk beacon check. See *Setting a Beacon*, on page 47.
  
  Only cache and persistent SSDs respond to the beacon request. NVMe cache SSDs and housekeeping SSDs do not respond to beacon requests.
  
  - For cache NVMe SSDs, perform a physical check. These drives are in Drive Bay 1 of the HX servers.
  
  - For housekeeping SSDs on HXAF240c or HX240c servers, perform a physical check at the back of the server.
  
  - For housekeeping SSDs on HXAF220c or HX220c servers, perform a physical check at Drive Bay 2 of the server.

---

**Step 2**

If the failed SSD is a **housekeeping SSD**, proceed based on the type of server.

- For HXAF220c or HX220c servers, proceed to Step 3.
  
- For HXAF240c or HX240c servers, contact Technical Assistance Center (TAC).

---

**Step 3**

If a failed SSD is a **cache or persistent SSD**, proceed based on the type of disk.

- For NVMe SSDs, see *Replacing NVMe SSDs*, on page 94.
  
- For all other SSDs, follow the instructions for removing and replacing a failed SSD in the host, per the server hardware guide.

After the cache or persistent drive is replaced, the HX Data Platform identifies the SDD and updates the storage cluster.
When disks are added to a node, the disks are immediately available for HX consumption.

**Step 4** To enable the Cisco UCS Manager to include new disks in the UCS Manager Server Inventory Storage tab, re-acknowledge the server node. This applies to cache and persistent disks.

**Step 5** If you replaced an SSD, and see a message *Disk successfully scheduled for repair*, it means that the disk is present, but is still not functioning properly. Check that the disk has been added correctly per the server hardware guide procedures.

---

**Replacing NVMe SSDs**

The procedures for replacing an SSD vary depending upon the type of SSD. This topic describes the steps for replacing NVMe cache SSDs.

**Note**

Mixing storage disks type or size on a server or across the storage cluster is not supported.

When replacing NVMe disks, always use the same type and size as the original disk.

---

**Before you begin**

Ensure the following conditions are met when using NVMe SSDs in HX Cluster servers.

- NVMe SSDs are supported in HX240 and HX220 All-Flash servers.
- Replacing NVMe SSDs with an HGST SN200 disk requires HX Data Platform version 2.5.1a or later.
- NVMe SSDs are only allowed in slot 1 of the server. Other server slots do not detect NVMe SSDs.
- NVMe SSDs are only used for cache.
  - Using them for persistent storage is not supported.
  - Using them as the housekeeping drive is not supported.
  - Using them for hybrid servers is not supported.

---

**Step 1** Confirm the failed disk is an NVMe cache SSD.

Perform a physical check. These drives are in Drive Bay 1 of the HX servers. NVMe cache SSDs and housekeeping SSDs do not respond to beacon requests.

If the failed SSD is not an NVMe SSD, see Replacing SSDs, on page 93.

**Step 2** Put ESXi host into HX Maintenance Mode.

a) Login to HX Connect.

b) Select System Information > Nodes > node > Enter HX Maintenance Mode.

**Step 3** Follow the instructions for removing and replacing a failed SSD in the host, per the server hardware guide.

**Note** When you remove an HGST NVMe disk, the controller VM will fail until you reinsert a disk of the same type into the same slot or reboot the host.
After the cache or persistent drive is replaced, the HX Data Platform identifies the SDD and updates the storage cluster. When disks are added to a node, the disks are immediately available for HX consumption.

**Step 4**
Reboot the ESXi host. This enables ESXi to discover the NVMe SSD.

**Step 5**
Exit ESXi host from HX Maintenance Mode.

**Step 6**
To enable the Cisco UCS Manager to include new disks in the **UCS Manager Server Inventory Storage** tab, re-acknowledge the server node. This applies to cache and persistent disks.

**Step 7**
If you replaced an SSD, and see a message *Disk successfully scheduled for repair*, it means that the disk is present, but is still not functioning properly. Check that the disk has been added correctly per the server hardware guide procedures.

---

**Replacing Housekeeping SSDs**

*Note* This procedure applies to HXAF220c or HX220c servers only. To replace the housekeeping SSD on an HXAF240c or HX240c, contact Cisco TAC.

Identify the failed housekeeping SSD and perform the associated steps.

**Step 1**
Identify the failed housekeeping SSD.

Physically check the SSD drives, as housekeeping drives are not listed through a beacon check.

**Step 2**
Remove the SSD and replace with a new SSD of the same kind and size. Follow the steps in the server hardware guide. The server hardware guide describes the physical steps required to replace the SSD.

*Note* Before performing the hardware steps, enter the node into Cisco HX Maintenance Mode. After performing the hardware steps, exit the node from Cisco HX Maintenance Mode.

**Step 3**
Using **SSH**, login into the storage controller VM of the affected node and run the following command.

```
# /usr/share/springpath/storfs-appliance/config-bootdev.sh -r -y
```

This command consumes the new disk, adding it into the storage cluster.

**Sample response**

Creating partition of size 65536 MB for /var/stv ...
Creating ext4 filesystem on /dev/sdg1 ...
Creating partition of size 24576 MB for /var/zookeeper ...
Creating ext4 filesystem on /dev/sdg2 ...
Model: ATA INTEL SSDSC2BB12 (scli)
Disk /dev/sdg: 120034MB
Sector size (logical/physical): 512B/4096B
Partition Table: gpt ...
discovered. Rebooting in 60 seconds

**Step 4**
Wait for the storage controller VM to automatically reboot.

**Step 5**
When the storage controller VM completes its reboot, verify that partitions are created on the newly added SSD. Run the command.
Replacing or Adding Hard Disk Drives

Note

Mixing storage disks type or size on a server or across the storage cluster is not supported.

- Use all HDD, or all 3.8 TB SSD, or all 960 GB SSD
- Use the hybrid cache device on hybrid servers and all flash cache devices on all flash servers.
- When replacing cache or persistent disks, always use the same type and size as the original disk.

Step 1
Refer to the hardware guide for your server and follow the directions for adding or replacing disks.

Step 2
Add HDDs of the same size to each node in the storage cluster.

Step 3
Add the HDDs to each node within a reasonable amount of time.
The storage starts being consumed by storage cluster immediately.

The vCenter Event log displays messages reflecting the changes to the nodes.

**Note**  When disks are added to a node, the disks are immediately available for HX consumption although they will not be seen in the UCSM server node inventory. This includes cache and persistent disks. To include the disks in the UCS Manager Server Inventory Storage tab, re-acknowledge the server node.
Managing Nodes

Nodes are initially added to a storage cluster using the Create Cluster feature of the HX Data Platform Installer. Nodes are added to an existing storage cluster using the Expand Cluster feature of the HX Data Platform Installer. When nodes are added or removed from the storage cluster, the HX Data Platform adjusts the storage cluster status accordingly.

- Tasks for node maintenance with a failed nodes.
  - The ESXi or HX software needs to be reinstalled.
  - A node component needs to be replaced.
  - The node needs to be replaced.
  - The node needs to be removed.

- Tasks for node maintenance with a non-failed nodes.
  - Putting the node into maintenance mode.
  - Changing the ESX password.
Note Though there are subtle differences, the terms server, host, and node are used interchangeably throughout the HyperFlex documentation. Generally a server is a physical unit that runs software dedicated to a specific purpose. A node is a server within a larger group, typically a software cluster or a rack of servers. Cisco hardware documentation tends to use the term node. A host is a server that is running the virtualization and/or HyperFlex storage software, as it is 'host' to virtual machines. VMware documentation tends to use the term host.

Step 1 Monitor the nodes in the cluster.

HX storage cluster, node, and node component status is monitored and reported to HX Connect, HX Data Platform Plug-in, vCenter UI, and assorted logs as Operational status (online, offline) and Resiliency (healthy, warning) status values.

Note Functional state distinctions contribute to, but are separate from, the storage cluster operational and resiliency status reported in the HX Connect and HX Data Platform Plug-in views. For each Data Replication Factor (2 or 3), Cluster Access Policy (lenient or strict), and given number of nodes in the storage cluster, the storage cluster shifts between Read and Write, Read Only, or Shutdown state, depending on the number of failed nodes or failed disks in nodes.

Step 2 Analyze the node failure and determine the action to take.

This frequently requires monitoring the node state through HX Connect, HX Data Platform Plug-in, vCenter, or ESXi; checking the server beacons; collecting and analyzing logs; and working with TAC.

Step 3 Complete the identified tasks.

- Reinstall or upgrade software.
  
  For steps to reinstall ESXi or the HX Data Platform see TAC. For steps to upgrade software, see the Cisco HyperFlex Systems Upgrade Guide.

- Repair a component in the node.
  
  Node components, such as solid state drives (SSD), hard disk drives (HDD), power supply units (PSU), and network interface cards (NIC) components are not configurable through HX Connect or HX Data Platform Plug-in, but the HX Data Platform monitors them and adjusts the storage cluster status when any of these items are disrupted, added, removed, or replaced.
  
  The steps to add or remove disks, depends upon the type of disk. Field replaceable units (FRUs), such as PSUs and NICs are replaced following steps described in the server hardware guides.

- Replace a node in the cluster.
  
  Replacing a node in a storage cluster typically requires TAC assistance. Provided the requirements are met, nodes can be replaced without TAC assistance while the storage cluster is online (5+ node clusters only) or offline (4+ node clusters). To replace a node in a 3 node cluster always requires TAC assistance.

- Remove a node from the cluster.
Note: Removing the node must not reduce the number of available nodes below the minimum 3 nodes, as this makes the storage cluster unhealthy. To remove a node in a 3 node cluster always requires TAC assistance. You can remove a maximum of 2 nodes from an offline cluster.

Identify Node Maintenance Methods

When performing maintenance tasks on nodes, some of these tasks are performed while the storage cluster is offline, others can be performed while the cluster is online and only require that the node is in HX maintenance mode, and other require TAC assistance.

- **Online tasks** - require that the storage cluster is healthy before the task begins.
- **Offline tasks** - require that the storage cluster will be shutdown.
  If 2 or more nodes are down, then the storage cluster is automatically offline.
- **TAC assisted tasks** - typically require steps that are performed by the TAC representative.

Note: Replacing a node in a 3 node cluster **always** requires TAC assistance.

The following tables lists the methods available to perform the associated node maintenance task.

**Repair Node Software**

ESX and HX Data Platform software is install on every node in the storage cluster. If it is determined after node failure analysis that either software item needs to be re-installed, contact TAC. For steps to upgrade software, see the *Cisco HyperFlex Systems Upgrade Guide*.

**Repair Node Hardware**

A reparable item on node fails. This includes FRUs and disks. Some node components require TAC assistance. Replacing a node’s mother board, for example, requires TAC assistance.

<table>
<thead>
<tr>
<th>No. Nodes in Cluster</th>
<th>No. Failed Nodes in Cluster</th>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1 or more</td>
<td>TAC assisted only node repair.</td>
<td>Node does not need to be removed to perform repair. Includes replacing disks on node.</td>
</tr>
<tr>
<td>4-8</td>
<td>1</td>
<td>Online or Offline node repair.</td>
<td>Node does not need to be removed to perform repair. Includes replacing disks on node.</td>
</tr>
</tbody>
</table>

**Remove Node**

A non-reparable item on node fails. Disks on the removed node are not reused in the storage cluster.
### Identify Node Maintenance Methods

<table>
<thead>
<tr>
<th>No. Nodes in Cluster</th>
<th>No. Failed Nodes in Cluster</th>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>Offline node remove.</td>
<td>A 4 node cluster with 2 nodes down, requires TAC assistance.</td>
</tr>
<tr>
<td>5 or more</td>
<td>1</td>
<td>Online or Offline node remove.</td>
<td></td>
</tr>
<tr>
<td>5 or more</td>
<td>2</td>
<td>Offline 2 node remove.</td>
<td>A 5 node cluster with 3 nodes down, requires TAC assistance.</td>
</tr>
</tbody>
</table>

**Replace Node and Discard Storage**

A non-reparable item on node fails. Disks on the removed node are not reused in the storage cluster.

<table>
<thead>
<tr>
<th>No. Nodes in Cluster</th>
<th>No. Failed Nodes in Cluster</th>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>TAC assisted only node replace.</td>
<td>TAC assisted node replacement required to return cluster to minimum 3 nodes. A 3 node cluster with 1 node down, requires TAC assistance.</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Offline replace node.</td>
<td>Use Expand cluster to add new nodes. All other nodes must be up and running. A 4 node cluster with 2 nodes down, requires TAC assistance.</td>
</tr>
<tr>
<td>5 or more</td>
<td>1</td>
<td>Online or offline replace node.</td>
<td>Use Expand cluster to add new nodes. All other nodes must be up and running.</td>
</tr>
<tr>
<td>5 or more</td>
<td>2</td>
<td>Offline replace 1 or 2 nodes.</td>
<td>Use Expand cluster to add new nodes. All other nodes must be up and running. Replacing up to 2 nodes is supported. Replacing 3 or more nodes requires TAC assistance.</td>
</tr>
</tbody>
</table>

**Replace Node and Reuse Storage**

A non-reparable item on node fails. Disks on the removed node are reused in the storage cluster.
### Searching by DNS Address or Host Name

Sometimes for troubleshooting purposes it is useful to be able to search by the DNS server address or DNS server host name. This is an optional task.

#### Step 1: Assign DNS search addresses

a) Login to the HX Data Platform Installer virtual machine. Use either `ssh` or the vSphere console interface.


```bash
# vi /etc/resolvconf/resolv.conf.d/base
```

c) Confirm the change.

```bash
# resolvconf -u
# cat /etc/resolv.conf
```

d) Confirm the DNS server can be queried from either the IP address or the host name.

```bash
# nslookup ip_address
# nslookup newhostname
```

#### Step 2: Assign a DNS host name.

a) Login to the HX Data Platform Installer virtual machine. Use either `ssh` or the vSphere console interface.

b) Open the hosts file for editing.

```bash
# vi /etc/hosts
```

c) Add the following line and save the file.

```bash
ip_address ubuntu newhostname
```

For each host `ip_address`, enter the host `newhostname`.

a) Add the `newhostname` to `hostname`.

```bash
# hostname newhostname
```
Changing ESXi Host Root Password

To change the default ESXi root password post installation, do the following.

Note
If you have forgotten the ESXi root password, for password recovery please contact Cisco TAC.

Step 1
Log into the ESXi host service control using SSH.

Step 2
Acquire root privileges.

su -

Step 3
Enter the current root password.

Step 4
Change the root password.

passwd root

Step 5
Enter the new password, and press Enter. Enter the password a second time for confirmation.

Note
If the password entered the second time does not match, you must start over.

Reinstalling Node Software

To re-install software on a node that is a member of an existing storage cluster, contact TAC. This task must be performed with TAC assistance.

Step 1
Reinstall ESX following the directions from TAC.

Ensure the server meets the required hardware and configuration listed in Host ESX Server Setting Requirements. HX configuration settings are applied during the HX Data Platform process.

Step 2
Reinstall HX Data Platform, following the directions from TAC.

The HX Data Platform must always be re-installed after ESX is re-installed.

Changing Node Identification Form in vCenter Cluster from IP to FQDN

This task describes how to change how vCenter identifies the nodes in the cluster, from IP address to Fully Qualified Domain Name (FQDN).
Step 1 Schedule a maintenance window to perform this task.

Step 2 Ensure the storage cluster is healthy.

Check the storage cluster status through either HX Connect, HX Data Platform Plug-in, or from the `stcli cluster info` command on the storage controller VM.

Step 3 Look up the FQDN for each ESXi host in the storage cluster.
   a) From the ESXi host command line.
      ```
      # cat /etc/hosts
      
      In this example, the FQDN is `sjs-hx-3-esxi-01.sjs.local`.
      # Do not remove the following line, or various programs
      # that require network functionality will fail.
      127.0.0.1 localhost.localdomain localhost
      ::1 localhost.localdomain localhost
      172.16.67.157 sjs-hx-3-esxi-01.sjs.local sjs-hx-3-esxi-01
      
      b) Repeat for each ESXi host in the storage cluster.
      
      Step 4 Verify the FQDNs for each ESXi host are resolvable from vCenter, each other ESXi host, and the controller VMs.
   a) From the vCenter command line.
      ```
      # nslookup <fqdn_esx_host1>
      # nslookup <fqdn_esx_host2>
      # nslookup <fqdn_esx_host3>
      ... 
      b) Repeat for each ESXi host from an ESXi host.
      c) Repeat for each ESXi host from each controller VM.

Step 5 If the FQDN name is not resolvable, then verify the DNS configuration on each ESXi host and each controller VM.
   a) Check that the controller VMs have the correct IP address for the DNS server.
      From a controller VM command line.
      ```
      # stcli services dns show
      10.192.0.31
      
      a) Check the ESXi hosts have the same DNS configuration as the controller VMs.
      From vCenter, select each ESXi host then `Configuration > DNS Servers`.

Step 6 Locate and note the Datacenter Name and the Cluster Name.

From vCenter client or web client, scroll through to see the Datacenter Name and Cluster Name. Write them down. They will be used in a later step.

Step 7 Delete the `cluster` from vCenter.

From vCenter, select `datacenter` > `cluster`. Right-click the `cluster` and select `Delete`.

**Note** Do not delete the `datacenter`.

Step 8 Recreate the `cluster` in vCenter.
   a) From vCenter, right-click the `datacenter`. Select `New Cluster`. 
b) Enter the exact same name for the Cluster Name as the cluster you deleted. This is the name you wrote down from Step 6.

**Step 9**
Add ESXi hosts (nodes) to the cluster using the FQDN name. Perform these steps for all ESXi hosts.

a) From vCenter, right-click the datacenter > cluster. Select Add Host.
b) Select an ESXi host using their FQDN.
c) Repeat for each ESXi host in the cluster.

**Step 10**
Reregister the cluster with vCenter.

```bash
# stcli cluster reregister
--vcenter-datacenter <datacenter_name>
--vcenter-cluster <hx_cluster_name>
--vcenter-url <vCenter_IP>
--vcenter-user <vCenter_username>
--vcenter-password <vCenter_Password>
```

The SSO URL is not required for HX version 1.8.1c or later. See Registering a Storage Cluster with a New vCenter Cluster, on page 68 for additional information on reregistering a cluster.

---

**Replacing Node Components**

Selected components on a node can be replaced. Some components can be replaced while the node is up and running. Replacing some components requires that the node be placed into a maintenance mode and shutdown. Refer to the hardware installation guide for your specific server for a complete list of field replaceable units (FRUs). Some components cannot be replaced or can only be replaced with TAC assistance. The following is a general list of components than can be replaced in a node.

---

**Note**
When disks are removed, the disk UUIDs continue to be listed, even when not physically present. To reuse disks on another node in the same cluster see TAC for assistance.

- Components that do not require the node be shutdown. These are hot-swappable.
  - HDD data drives. Front bays
    See this guide for the storage cluster tasks and the hardware installation guides for the hardware focused tasks. Both sets of tasks are required to replace this component.
  - SSD cache driver. Front bay 1
    See this guide for the storage cluster tasks and the hardware installation guides for the hardware focused tasks. Both sets of tasks are required to replace this component.
  - Fan Modules
    See the hardware installation guides to replace this component.
  - Power Supplies
    See the hardware installation guides to replace this component.

- Components that do required the node be put into maintenance mode and shutdown.
For all of the following components, see the hardware installation guides.

- **Housekeeping SSD**
  
  See TAC for the storage cluster tasks and the hardware installation guides for the hardware focused tasks. Both sets of tasks are required to replace this component.

- **RTC Battery on motherboard**

  **Note**  The motherboard itself is not a replaceable component. Contact TAC for assistance.

- **DIMMS**
- **CPUs and Heatsinks**
- **Internal SD Card**
- **Internal USB Port**
- **Modular HBA Riser (HX 220c servers)**
- **Modular HBA Card**
- **PCIe Riser Assembly**
- **PCIe Card**
- **Trusted Platform Module**
- **mLOM Card**
- **RAID Controller**
- **Virtual Interface Card (VIC)**
- **Graphic Processing Unit (GPU)**

### Removing a Node

Depending upon the node maintenance task, removing a node can be while the storage cluster is online or offline. Ensure you have completed the preparation steps before removing a node.

**Note**  It is highly recommended that you work with TAC when removing a converged node in a storage cluster. Do not reuse the removed converged node or its disks in the original or another cluster.

The affecting context is based on the number of converged nodes. The number of compute nodes does not affect the replacing a node workflow.
Preparing to Remove a Node

Before you remove a node from a storage cluster, whether the cluster is online or offline, complete the following steps.

### Table 8: Removing a Node Workflows

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Nodes Removed</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 node cluster</td>
<td>1 or more</td>
<td>Workflow requires TAC assistance.</td>
</tr>
<tr>
<td>4 node cluster</td>
<td>1</td>
<td>1. Cluster is healthy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Affected node in Cisco HX Maintenance mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Shutdown the cluster (take cluster offline).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli cluster shutdown</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Remove the node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli node remove</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Restart the cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli cluster start</code> command.</td>
</tr>
<tr>
<td>5 node cluster</td>
<td>2 or more</td>
<td>Workflow requires TAC assistance.</td>
</tr>
<tr>
<td>5 node cluster</td>
<td>1</td>
<td>1. Cluster is healthy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Affected node in Cisco HX Maintenance mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Cluster remains online.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Remove the node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli node remove</code> command.</td>
</tr>
<tr>
<td>5 node cluster</td>
<td>2</td>
<td>1. Cluster is healthy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Affected node in Cisco HX Maintenance mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Shutdown the cluster (take cluster offline).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli cluster shutdown</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Remove the nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli node remove</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify both nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Restart the cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli cluster start</code> command.</td>
</tr>
<tr>
<td>5 node cluster</td>
<td>3 or more</td>
<td>Workflow requires TAC assistance.</td>
</tr>
</tbody>
</table>
For all 3 node clusters, see TAC to assist with preparing, removing, and replacing a node.

---

**Step 1**

Ensure the cluster is healthy.

```
# stcli cluster info
```

Example response that indicates the storage cluster is online and healthy:

```
locale: English (United States)
state: online
upgradeState: ok
healthState: healthy
state: online
state: online
```

**Step 2**

Ensure that SSH is enabled in ESX on all the nodes in the storage cluster.

**Step 3**

Ensure that the Distributed Resource Scheduler (DRS) is enabled.

DRS migrates only powered-on VMs. If your network has powered-off VMs, you must manually migrate them to a node in the storage cluster that will not be removed.

**Note** If DRS is not available then manually move the Virtual Machines from the node.

**Step 4**

Rebalance the storage cluster.

This ensures that all datastores associated with the node will be removed.

The rebalance command is used to realign the distribution of stored data across changes in available storage and to restore storage cluster health. If you add or remove a node in the storage cluster, you can manually initiate a storage cluster rebalance using the `stcli rebalance` command.

**Note** Rebalancing might take some time depending on the disk capacity used on the failed node or disk.

a) Login to a controller VM in the storage cluster.
b) From the controller VM command line, run the command:

```
# stcli rebalance start --force
```

**Step 5**

Put the node to be removed into Cisco HX Maintenance mode. Choose a method: vSphere GUI or controller VM command line (CLI).

**GUI**

a) From vSphere web client, select **Home > Hosts and Clusters > Hosts > host**.
b) Right-click each host, scroll down the list, and select **Cisco HX Maintenance Mode > Enter HX Maintenance Mode**.

The vSphere Maintenance Mode option is at the top of the host right-click menu. Be sure to scroll to the bottom of the list to select Cisco HX Maintenance Mode.

**CLI**

a) On the ESX host, log in to a controller VM as a user with root privileges.
b) Identify the node.
# stcli node info

stNodes:

----------------------------------------
type: node
id: 689324b2-b30c-c440-a08e-5b37c7e0eefe
name: 192.168.92.144

----------------------------------------
type: node
id: 9314ac70-77aa-4345-8f35-7854f71a0d0c
name: 192.168.92.142

----------------------------------------
type: node
id: 9e6ba2e3-4bb6-214c-8723-019fa483a308
name: 192.168.92.141

----------------------------------------
type: node
id: 575ace48-1513-0b4f-bfe1-e6abd5ff6895
name: 192.168.92.143

Under stNodes section the id is listed for each node in the cluster.

c) Move the ESX host into Maintenance mode.

# stcli node maintenanceMode (--id ID | --ip NAME) --mode enter

(see also stcli node maintenanceMode --help)

Step 6  Open a command shell and login to the storage controller VM. For example, using `ssh`.

# ssh root@controller_vm_ip

At the prompt, enter password, Cisco123.

What to do next

Proceed to Removing a Node. Choose the Online or Offline method per the condition of your storage cluster and the desired results listed in Managing Nodes.

Removing a Node from an Online Storage Cluster

Use the `stcli node remove` to clean up a deployment or remove a node from a storage cluster. Removing a converged node or compute node follow the same procedure.

Removing a node from a storage cluster while the cluster remains online has a slightly different requirements from removing a node while the cluster is offline.

Note

It is highly recommended that you work with TAC when removing a converged node in a storage cluster.

The affecting context is based on the number of converged nodes. The number of compute nodes does not affect the replacing a node workflow.
### Removing a Node from an Online Storage Cluster

<table>
<thead>
<tr>
<th>Number of nodes in cluster</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 node cluster</td>
<td>See TAC to remove and replace the node.</td>
</tr>
<tr>
<td>4 node cluster</td>
<td>Cluster must be offline. See Removing a Node from an Offline Storage Cluster, on page 112.</td>
</tr>
<tr>
<td>5 node cluster, removing 2 nodes</td>
<td>Cluster must be offline. See Removing a Node from an Offline Storage Cluster, on page 112.</td>
</tr>
<tr>
<td>5 node cluster, removing 1 node from a healthy cluster</td>
<td>Cluster can be online. Continue with the steps listed here.</td>
</tr>
</tbody>
</table>

**Note:** Do not remove the controller VM or other HX Data Platform components before you complete the steps in this task.

---

#### Step 1
Complete the steps in Preparing for Maintenance Operations and Preparing to Remove a Node. This includes:

- **a)** Ensure the cluster is healthy.
  - For 3 node clusters see TAC, as any node failure in a 3 node cluster means the cluster is not healthy.

- **b)** Ensure DRS is enabled or manually move the VMs from the node.

- **c)** Rebalance the storage cluster.

- **d)** Put the node being removed into HX maintenance mode.

- **e)** Login to the controller VM of a node that is not being removed.

#### Step 2
Rebalance the storage cluster.

- **a)** Run the rebalance command.
  
  ```
  # stcli rebalance start -f
  ```

- **b)** Wait and confirm that rebalance has completed.

#### Step 3
Remove the desired node using the `stcli node remove` command.

```
stcli node remove [-h] [--id-1 ID1 | --ip-1 NAME1] [--id-2 ID2 | --ip-2 NAME2] [-f]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--id-1 ID1</td>
<td>One of set required.</td>
<td>A unique ID number for the storage cluster node. The ID is listed in the <code>stcli cluster info</code> command under the <code>stNode id</code> field.</td>
</tr>
<tr>
<td>--ip-1 NAME1</td>
<td>One of set required.</td>
<td>IP address of storage cluster node. The IP is listed in the <code>stcli cluster info</code> command under the <code>stNode name</code> field.</td>
</tr>
<tr>
<td>--id-2 ID2</td>
<td>Optional.</td>
<td>A unique ID number for the storage cluster node. The ID is listed in the <code>stcli cluster info</code> command under the <code>stNode id</code> field.</td>
</tr>
</tbody>
</table>
**Removing a Node from an Offline Storage Cluster**

Use the `stcli node remove` to clean up a deployment or remove a node from a storage cluster. Removing a converged node or compute node follow the same procedure.

---

**Note**

It is highly recommended that you work with TAC when removing a converged node in a storage cluster.

---

### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ip-2 NAME2</td>
<td>Optional.</td>
<td>IP address of storage cluster node. The IP is listed in the <code>stcli cluster info</code> command under the <code>stNode</code> field name. The <code>--ip</code> option is currently not supported.</td>
</tr>
<tr>
<td>-f, --force</td>
<td>Optional.</td>
<td>Forcibly remove storage cluster nodes.</td>
</tr>
</tbody>
</table>

For example

```
# stcli node remove --name-1 esx.SVHOST144A.complab
```

**Response**

`Successfully removed node: EntityRef(type=3, id='', name='esx.SVHOST144A.complab')`

This command unmounts all data stores, removes from the cluster ensemble, resets the EAM for this node, stops all services (stores, cluster management IP), and removes all firewall rules.

This command does not:

- Remove the node from vCenter. The node remains in vCenter.
- Remove the installed HX Data Platform elements, such as the controller VM.

After the `stcli node remove` command completes successfully, the system rebalances the storage cluster until the storage cluster state is Healthy. Do not perform any failure tests during this time. The storage cluster remains healthy.

Because the node is no longer in the storage cluster, you do not need to exit HX maintenance mode.

**Note** If you want to reuse a removed node in another storage cluster, contact Technical Assistance Center (TAC). Additional steps are required to prepare the node for another storage cluster.

---

**Step 4**

Confirm the node is removed from the storage cluster.

a) Check the storage cluster information.

```
# stcli cluster info
```

b) Check the `ActiveNodes` entry in the response to verify the cluster has one less node.

**Step 5**

Confirm all the node-associated datastores are removed.

**Note** If any node-associated datastores are listed, then manually unmount and delete those datastores.
The affecting context is based on the number of converged nodes. The number of compute nodes does not affect the replacing a node workflow.

<table>
<thead>
<tr>
<th>Number of nodes in cluster</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 node cluster</td>
<td>See TAC to remove and replace the node.</td>
</tr>
<tr>
<td>4 node cluster</td>
<td>Cluster must be offline.</td>
</tr>
<tr>
<td>5 node cluster, removing 2 nodes</td>
<td>Cluster must be offline.</td>
</tr>
<tr>
<td>5 node cluster, removing 1 node from a healthy cluster</td>
<td>Cluster can be online. See Removing a Node from an Online Storage Cluster, on page 110.</td>
</tr>
</tbody>
</table>

Note
Do not remove the controller VM or other HX Data Platform components before you complete the steps in this task.
You can remove a maximum of 2 nodes from an offline cluster.

---

**Step 1**
Complete the steps in Preparing for Maintenance Operations and Preparing to Remove a Node. This includes:

a) Ensure the cluster is healthy.
   For 3 node clusters see TAC, as any node failure in a 3 node cluster means the cluster is not healthy.

b) Ensure DRS is enabled or manually move the VMs from the node.

c) Rebalance the storage cluster.

d) Put the node being removed into HX maintenance mode.

e) Login to the controller VM of a node that is not being removed.

**Step 2**
Prepare to shutdown, then shutdown the storage cluster.
This step is need only for either of the following conditions:

- The cluster is less than 5 nodes.
- Removing 2 nodes from a 5 node cluster.

a) Gracefully shutdown all resident VMs on all the HX datastores.
   Optionally, vMotion the VMs.

b) Gracefully shutdown all VMs on non-HX datastores on HX storage cluster nodes, and unmount.

c) From any controller VM command line, issue the `stcli cluster shutdown` command.

   ```sh
   # stcli cluster shutdown
   ```

**Step 3**
Remove the desired node using the `stcli node remove` command.
For example, you can specify the node to be removed by either IP address or domain name.

```sh
# stcli node remove --ip-1 10.10.2.4 --ip-2 10.10.2.6
```
or
# stcli node remove --name-1 esx.SVHOST144A.complab --name-2 esx.SVHOST144B.complab.lab

**Note** Enter the second IP address if you are removing a second node from a 5+ node storage cluster.

**Response**

Successfully removed node: EntityRef(type=3, id='', name='10.10.2.4' name='10.10.2.6')

This command unmounts all datastores, removes from the cluster ensemble, resets the EAM for this node, stops all services (stores, cluster management IP), and removes all firewall rules.

This command does not:

- Remove the node from vCenter. The node remains in vCenter.
- Remove the installed HX Data Platform elements, such as the controller VM.

After the `stcli node remove` command completes successfully, the system rebalances the storage cluster until the storage cluster state is Healthy. Do not perform any failure tests during this time. The storage cluster health remains Average. Because the node is no longer in the storage cluster, you do not need to exit HX maintenance mode.

**Note** If you want to reuse a removed node in another storage cluster, contact Technical Assistance Center (TAC). Additional steps are required to prepare the node for another storage cluster.

---

**Step 4** Confirm the node is removed from the storage cluster.

a) Check the storage cluster information.

```
# stcli cluster info
```

b) Check the `ActiveNodes` entry in the response to verify the cluster has one less node.

**Step 5** Confirm all the node-associated datastores are removed.

**Note** If any node-associated datastores are listed, then manually unmount and delete those datastores.

**Step 6** Restart the cluster.

```
# stcli cluster start
```

---

## Replacing a Node

Replacing a node uses Expand Cluster to add the replacement node after removing the failed node. Replacing a node can be performed while the HX storage cluster is online or offline, provided the requirements are met. Replacing a converged node in a storage cluster typically requires TAC assistance.

**Note** It is highly recommended that you work with TAC when replacing a node in a storage cluster.

**Conditions that require TAC assistance to replace a converged node.**

- 3 node cluster
All 3 node clusters require TAC assistance to replace a node. Replace the node during cluster maintenance.

- **4 node cluster**
  - Storage cluster is unhealthy.
  - Storage cluster will become unhealthy if a node is removed.
  - 2 or more nodes have failed.
  - Disks on the replaced node will be reused.

  When a node is added to a storage cluster, the HX Data Platform associates each disk UUID with the node UUID. This is a fixed relationship for the life of the storage cluster. Disks cannot be reassigned to nodes with different UUIDs. TAC will work with you to assign the old node's UUID to the new node to ensure the disk UUID to node UUID association.

  - Storage cluster to remain online while replacing a node.

- **5 node cluster**
  - Storage cluster is unhealthy.
  - Storage cluster will become unhealthy if a node is removed.
  - 3 or more nodes have failed.
  - Disks on the replaced node will be reused.

  When a node is added to a storage cluster, the HX Data Platform associates each disk UUID with the node UUID. This is a fixed relationship for the life of the storage cluster. Disks cannot be reassigned to nodes with different UUIDs. TAC will work with you to assign the old node's UUID to the new node to ensure the disk UUID to node UUID association.

  - Storage cluster to remain online while replacing 2 nodes.
  - Storage cluster to remain online and the cluster was initially 3 or 4 nodes.

  If your storage cluster was initially configured with either 3 or 4 nodes, adding nodes to make a total of 5 keeps your cluster as a 3+2 or 4+1 cluster. To keep the cluster online while replacing a node requires TAC assistance.

**Replace a Node Workflows**

The affecting context is based on the number of converged nodes. The number of compute nodes does not affect the replacing a node workflow.

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Nodes Replaced</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 node cluster</td>
<td>1 or more</td>
<td>Workflow requires TAC assistance.</td>
</tr>
</tbody>
</table>
### Replacing a Node

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Nodes Replaced</th>
<th>Workflow</th>
</tr>
</thead>
</table>
| 4 node cluster | 1              | 1. Cluster is healthy.  
2. Affected node in Cisco HX Maintenance mode.  
3. Shutdown the cluster (take cluster offline).  
   Use the `stcli cluster shutdown` command.  
4. Remove the node.  
   Use the `stcli node remove` command.  
5. Restart the cluster.  
   Use the `stcli cluster start` command.  
6. Wait until cluster is online and healthy.  
7. Use **HX Installer > Expand Cluster** to add replacement node.  
**Note** Do not reuse the removed node or its disks in this or another cluster. |
| 4 node cluster | 2 or more       | Workflow requires TAC assistance. |
| 5 node cluster | 1              | 1. Cluster is healthy.  
2. Affected node in Cisco HX Maintenance mode.  
3. Cluster remains online.  
4. Remove the node.  
   Use the `stcli node remove` command.  
5. Restart the cluster.  
   Use the `stcli cluster start` command.  
6. Wait until cluster is online and healthy.  
7. Use **HX Installer > Expand Cluster** to add replacement node.  
**Note** Do not reuse the removed node or its disks in this or another cluster. |
### Replacing a Node and discarding the failed node's disks.

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Nodes Replaced</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 node cluster</td>
<td>2</td>
<td>1. Cluster is healthy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Affected node in Cisco HX Maintenance mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Shutdown the cluster (take cluster offline).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli cluster shutdown</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Remove the nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli node remove</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify both nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Restart the cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>stcli cluster start</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Wait until cluster is online and healthy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Use <strong>HX Installer &gt; Expand Cluster</strong> to add replacement node</td>
</tr>
</tbody>
</table>

**Note**  
Do not reuse the removed node or its disks in this or another cluster.

If replacing more than 2 nodes:

<table>
<thead>
<tr>
<th>Cluster Size</th>
<th>Nodes Replaced</th>
<th>Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 node cluster</td>
<td>3 or more</td>
<td>Workflow requires TAC assistance.</td>
</tr>
</tbody>
</table>

---

**Step 1**  
Remove the old node. Follow the steps in the appropriate topic:

- **Removing a Node from an Online Storage Cluster**
  
  Use this method only if the HX cluster was initially configured with at least 5 nodes and currently still has at least 5 nodes.

- **Removing a Node from an Offline Storage Cluster**
  
  Use this method for all other non-TAC assisted node removal.

**Note**  
Even though you remove a node and its associated disks, the HX Data Platform remembers the disk UUIDs. When logs and reports are generated, messages indicate that the disks exist but cannot be found. Ignore these messages.

**Step 2**  
Add the new node using the Expand option in the HX Data Platform Installer. See the *Cisco HyperFlex Systems Getting Started Guide*. 

---
Managing HX Controller VMs

- Managing Storage Controller VMs, on page 119
- Powering On or Off Storage Controller VMs, on page 119

Managing Storage Controller VMs

Storage controller VMs provide critical functionality for the Cisco HX Distributed Data Platform. A storage controller VM is installed on every converged node in the storage cluster. The storage controller VMs provide a command line interface for running `stcli` commands on the storage cluster.

Powering On or Off Storage Controller VMs

You can power on or off VMs through the vSphere Web Client or through the ESX command line. This also applies to storage controller VMs, though generally the storage cluster operations handle powering on or off the storage controller VMs.

Step 1 Using the vSphere Web Client to power on or off a VM.
   a) Login to the vSphere Web Client.
   b) Locate the VM.
      - From the Navigator select, **vCenter Inventory Lists > Virtual Machines > vm**.
      - Storage controller VMs, have the prefix, `stCtlVM`.
   c) From the right-click or Actions menu select, **Power > Power On** or **Power > Power Off**.

Step 2 Using the ESX command line to power on or off a VM.
   a) Login to the command line for the ESX host for a VM.
   b) Locate the VM `vmid`.
      - This is specific to the ESX host. Run the command.

```
# vim-cmd vmsvc/getallvms
```

Sample response

```
Vmid Name File Guest OS Version Annotation
1 stCtlVM=<vm_number> [SpringpathDS=<vm_number>] stCtlVM=<vm_number>/stCtlVM=<vm_number>.vmx
```
Storage controller VMs, have the prefix, stCtlVM.

c) To power on a VM. Run the command specifying the VM to power on.

   # vim-cmd vmsvc/power.on 1

d) To power off a VM. Run the command specifying the VM to power off.

   # vim-cmd vmsvc/power.off 1
Managing ReadyClones

• HX Data Platform ReadyClones Overview, on page 121
• Benefits of HX Data Platform ReadyClones, on page 121
• Supported Base VMs, on page 122
• ReadyClone Requirements, on page 122
• ReadyClone Best Practices, on page 123
• Creating ReadyClones Using HX Connect, on page 123
• Creating ReadyClones Using the HX Data Platform Plug-In, on page 124
• Prepare to Customize HX Data Platform ReadyClones, on page 126
• Configuring ReadyClones Using Customized Specifications, on page 127
• Managing Virtual Machine Networking, on page 127

HX Data Platform ReadyClones Overview

HX Data Platform ReadyClones is a pioneer storage technology that enables you to rapidly create and customize multiple cloned VMs from a host VM. Is an expansion feature that is used for creating multiple copies of VMs that can then be used as standalone VMs.

A ReadyClone, similar to a standard clone, is a copy of an existing VM. The existing VM is called the host VM. When the cloning operation is complete, the ReadyClone is a separate guest VM.

Changes made to a ReadyClone do not affect the host VM. A ReadyClone's MAC address and UUID are different from those of the host VM.

Installing a guest operating system and applications can be time consuming. With ReadyClone, you can make many copies of a VM from a single installation and configuration process.

Clones are useful when you deploy many identical VMs to a group.

Benefits of HX Data Platform ReadyClones

HX Data Platform ReadyClones provide the following benefits:

• Create multiple clones of a VM at a time - Simply right-click a VM and create multiple clones of the VM using the ReadyClones feature.
• **Rapid cloning** - HX Data Platform ReadyClones are extremely fast and efficient than legacy cloning operations because they support VMware vSphere® Storage APIs – Array Integration (VAAI) data offloads. VAAI also called hardware acceleration or hardware offload APIs, are a set of APIs to enable communication between VMware vSphere ESXi hosts and storage devices. Use HX Data Platform ReadyClones to clone VMs in seconds instead of minutes.

• **Batch customization of guest VMs** - Use the HX Data Platform Customization Specification to instantly configure parameters such as IP address, host name, VM name for multiple guest VMs cloned from a host VM.

• **Automation of several steps to a one-click process** - The HX Data Platform ReadyClones feature automates the task to create each guest VM.

• **VDI deployment support** - ReadyClones are supported for desktop VMs on VDI deployments which are using VMware native technology.

• **Datastore access** - ReadyClone work on partially mounted/accessible datastores as long as the VM being cloned is on an accessible mountpoint.

### Supported Base VMs

HX Data Platform supports:

- Base VMs stored on a HX Data Platform datastore
- Base VMs with HX Data Platform Snapshots
- Maximum 2048 ReadyClones from one base VM
- Maximum 256 ReadyClones created in one batch at a time.

HX Data Platform does not support:

- Powered on base VMs with Win2008 and Win2012 server guest
- Powered on base VMs with > 30 snapshots
- Powered on base VMs with Redo log snapshots

### ReadyClone Requirements

- VMs must be within the HX Data Platform storage cluster. Non-HX Data Platform VMs are not supported.
- VMs must reside on a HX Data Platform datastore, VM folder, and resource pool.
  
  ReadyClones fail for any VM that is not on a HX Data Platform datastore. This applies to ReadyClones on a VM level, VM folder level, or resource pool level.

- VMs can have only native snapshots. ReadyClones cannot be created from VMs with snapshots that have redo logs, (non-native snapshots).

- SSH must be enabled in ESX on all the nodes in the storage cluster.

- Use only the single vNIC customization template for ReadyClones.
ReadyClone Best Practices

- Use the customization specification as a profile or a template.
- Ensure that properties that apply to the entire batch are in the customization specification.
- Obtain user-defined parameters from the HX Data Platform ReadyClone batch cloning work flow.
- Use patterns to derive per-clone identity settings such as the VM guest name.
- Ensure that the network administrator assigns static IP addresses for guest names and verify these addresses before cloning.
- You can create a batch of 1 through 256 at a given time. The HX Data Platform plug-in enables you to verify this.
- Do not create multiple batches of clones simultaneously on the same VM (when it is powered on or powered off) because it causes failures or displays incorrect information on the master task updates in the HX Data Platform plug-in.

Creating ReadyClones Using HX Connect

Use HX Data Platform ReadyClones feature to populate your cluster by creating multiple clones of a VM, each with different static IP addresses.

**Step 1**
Login to HX Connect as an administrator.

**Step 2**
From Virtual Machines page, select a virtual machine, then click ReadyClones.

**Step 3**
Complete the ReadyClone dialog fields.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of clones field</td>
<td>Enter the number of ReadyClones that you want to create. You can create a batch of 1 through 256 clones at a given time.</td>
</tr>
</tbody>
</table>
| Customization Specification field | Optional field.  
Click the drop-down list and select a Customization Specification for the clone from the drop-down list (which includes the customization specifications available in vCenter).  
The system filters the customization specifications for the selected host virtual machine. For example, if the selected host virtual machine uses Windows OS for guest virtual machines, the drop-down list displays Windows OS customization specifications. |
| Resource Pool field      | Optional field.  
If you have resource pools defined in your HX Storage Cluster, you can select one to store the ReadyClones of the selected virtual machine. |
<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name Prefix field</td>
<td>Enter a prefix for the guest virtual machine name. This prefix is added to the name of each ReadyClone created.</td>
</tr>
<tr>
<td>Starting clone number field</td>
<td>Enter a clone number for the starting clone. Each ReadyClone must have a unique name, numbering is used to ensure a unique element in the name.</td>
</tr>
<tr>
<td>Increment clone numbers by</td>
<td>Enter a value using which the clone number in the guest virtual machine name must be increased, or leave the default value 1 as is. The system appends a number to the names of the virtual machine ReadyClones (such as clone1, clone2, and clone3). By default, the number starts from 1. You can change this value to any number.</td>
</tr>
<tr>
<td>Use same name for Guest Name checkbox</td>
<td>Select this check box to use the vCenter VM inventory name as the guest host virtual machine name. If you uncheck this box, a text box is enabled. Enter the name you want to use for the guest host virtual machine name.</td>
</tr>
<tr>
<td>Preview field</td>
<td>After required fields are completed, HX Data Platform lists the proposed ReadyClones names. As you change the content in the required fields, the Clone Name and Guest Name fields update.</td>
</tr>
<tr>
<td>Power on VMs after cloning checkbox</td>
<td>Select this check box to turn the guest virtual machines on after the cloning process completes.</td>
</tr>
</tbody>
</table>

**Step 4**

Click **Clone**.

HX Data Platform creates the number of ReadyClones with the naming and location specified.

---

**Creating ReadyClones Using the HX Data Platform Plug-In**

If you use the VMware cloning operation, you can create only a single clone from a VM. This operation is manual and slower than batch processing multiple clones from a VM. For example, to create 20 clones of a VM, you must manually perform the clone operation over and over again.

---

**Note**

Use HX Data Platform ReadyClones to create multiple clones of a VM in one click!

For example, you can create ten different clones with different static IP addresses from a Windows VM.

---

**Step 1**

From the vSphere Web Client Navigator, select **vCenter Inventory Lists > Virtual Machines**. This displays the list of VMs in vCenter.

**Step 2**

Select a storage cluster VM and open the **Actions** menu. Either right-click the VM or click the Actions menu in the VM information portlet.
If needed, view the list of clusters and associated VMs to verify the VM is a storage cluster VM.

**Step 3**
Select **Cisco HX Data Platform > ReadyClones** to display the ReadyClones dialog box.

**Step 4**
Specify the following information in the ReadyClones dialog box:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of clones</td>
<td>Type the number of clones that you want to create. You can create a batch of 1 through 256 clones at a given time.</td>
</tr>
<tr>
<td>Customization Specification</td>
<td>Click the drop-down list and select a Customization Specification for the clone from the drop-down list (which includes the customization specifications available in vCenter). The system filters the customization specifications for the selected host VM. For example, if the selected host VM uses Windows OS for guest VMs, the drop-down list displays Windows OS customization specifications.</td>
</tr>
<tr>
<td>VM name prefix</td>
<td>Type a prefix for the guest VM name.</td>
</tr>
<tr>
<td>Starting clone number</td>
<td>Type a clone number for the starting clone.</td>
</tr>
<tr>
<td>Use same name for ‘Guest Name’</td>
<td>Select this check box to use the vCenter VM inventory name as the guest host VM name. If you uncheck this box, a text box is displayed. Enter the name you want to use for the guest host VM name. The system displays the guest VM names in the Guest Name column in the dialog box. There is a similar option in the Customization Specification itself. This HX Data Platform ReadyClone batch customization process overrides the option that you specify in the Customization Specification option.</td>
</tr>
<tr>
<td>Increment clone number by</td>
<td>Type a value using which the clone number in the guest VM name must be increased, or leave the default value 1 as is. The system appends a number to the names of the VM clones (such as clone1, clone2, and clone3). By default, the number starts from 1. You can change this value to any number.</td>
</tr>
<tr>
<td>Power on VMs after cloning</td>
<td>Select this check box to turn the guest VMs on after the cloning process completes.</td>
</tr>
</tbody>
</table>

**Step 5**
Click **OK** to apply your configuration changes.

The vSphere Web Client Recent Tasks tab displays the status of the ReadyClones task. The system displays:

- Top-level progress with the initiator as the logged in vCenter user.
- Implementation work flows with the initiator as the logged in vCenter user and a HX Data Platform extension.
As part of the ReadyClone workflow a temporary snapshot is listed in vCenter and HXConnect. This is listed as an extra powered off VM transiently, only while the ReadyClones are being created.

Prepare to Customize HX Data Platform ReadyClones

- Create a customization specification per the VMware documentation.
  - Apply the customization settings described in the following topics specific to either Linux or Windows VMs.
  - Obtain the IP addresses from the administrator. For example, ten IP addresses 10.64.1.0 through 10.64.1.9.
  - Gather information specific to your network such as the subnet mask for these IP addresses.
  - Ensure that the base VM is valid (not disconnected, undergoing snapshots, or vMotion).
  - Ensure that Guest Tools is installed on the base VM. Update it if necessary.
  - Go to the VM Summary tab and verify that Guest Tools is working.

Creating a Customization Specification for Linux in the vSphere Web Client

Use the vSphere Web Client Guest Customization wizard to save guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.

Complete the wizard with the following considerations.

- You can use the HX Data Platform ReadyClones feature to overwrite the guest name that you specify in when you create the customization specification.
- HX Data Platform ReadyClones enable you to use patterns in the VM name or guest name.
- HX Data Platform supports only one NIC.
- Editing the NIC of a Customized Linux VM
  - You can use a fake IP address because the HX Data Platform ReadyClone customization process overwrites this address.
  - HX Data Platform ReadyClones resolve VM guest names to static IP addresses and sets them for the cloned VMs.

The customization specification you created is listed in the Customization Specification Manager. You can use it to customize virtual machine guest operating systems.

Create a Customization Specification for Windows in the vSphere Web Client

Use the vSphere Web Client Guest Customization wizard to save Windows guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.
The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine boots the first time after customization.

Complete the wizard with the following considerations.

• The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.
• HX Data Platform supports only one NIC.
• Editing the NIC of a Customized Windows VM

You can use a fake IP address because the HX Data Platform ReadyClone customization process overwrites it.

The customization specification you created is listed in the Customization Specification Manager. You can use it to customize virtual machine guest operating systems.

### Configuring ReadyClones Using Customized Specifications

Use a customized specification to ensure IP addresses are applied correctly to the new VMs if you use static IP addresses.

For example, if you create a Windows server VM clone and you use DHCP, the guest VMs are automatically assigned new IP addresses. But, if you use static IP addresses, the IP address is not automatically replicated in the guest VM. To resolve this, configure HX Data Platform ReadyClones using a Customization Specification.

**Step 1**
Obtain the valid DNS names and ensure that they resolve to valid IP addresses.

For example, to provision a batch of 100 Windows VMs where the guest name is userwinvm1 to userwinvm100, check that userwinvm1 through userwinvm100 are valid IP addresses.

**Step 2**
Install Guest VM tools on the source VM.

**Step 3**
Clone the source VM using the ReadyClones feature. The cloned guest VMs obtain the identity of the source VM.

**Step 4**
Use the Customization Specification to change the identity of all cloned VMs. You can configure parameters such as IP address, host name, and VM name.

### Managing Virtual Machine Networking

After you have made changes to your storage cluster, you can ensure that the networking for the virtual machines on the nodes in the clusters is configured correctly. See the UCS Manager documentation for complete virtual machine networking information.
Step 1  Verify the VLANs are configured correctly.


Step 2  Verify the vNICs are configured correctly.


Step 3  Verify the Virtual Port Groups are configured correctly.

Managing Native Snapshots

- HX Data Platform Native Snapshots Overview, on page 129
- Benefits of HX Data Platform Native Snapshots, on page 129
- Native Snapshot Considerations, on page 131
- Native Snapshot Best Practices, on page 132
- Understanding SENTINEL Snapshots, on page 133
- Native Snapshot Timezones, on page 133
- Creating Snapshots, on page 134
- Scheduling Snapshots, on page 135
- Scheduling Snapshots, on page 136
- Setting the Frequency of Scheduled Snapshots, on page 136
- Deleting Snapshot Schedules, on page 137
- Reverting to a Snapshot, on page 137
- Deleting Snapshots, on page 138

HX Data Platform Native Snapshots Overview

HX Data Platform Native Snapshots are a backup feature that saves versions (states) of working VMs. VMs can be reverted back to native snapshots.

Use the HX Data Platform plug-in to take native snapshots of your VMs. HX Data Platform native snapshot options include: create a native snapshot, revert to any native snapshot, and delete a native snapshot. Timing options include: Hourly, Daily, and Weekly, all in 15 minute increments.

A native snapshot is a reproduction of a VM that includes the state of the data on all VM disks and the VM power state (on, off, or suspended) at the time the native snapshot is taken. Take a native snapshot to save the current state of the VM, so that you have the option to revert to the saved state.

You can take a native snapshot when a VM is powered on, powered off, or suspended. For additional information about VMware snapshots, see the VMware KB, Understanding virtual machine snapshots in VMware ESXi and ESX (1015180) at, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

Benefits of HX Data Platform Native Snapshots

HX Data Platform native snapshots use native technology. Native snapshots provide the following benefits:
• **Reverting registered VMs** - If a VM is registered, whether powered-on or powered-off, native snapshots, same as VM snapshots, can be used to revert to an earlier point in time at which the snapshot was created.

• **High performance** - The HX Data Platform native snapshot process is fast because it does not incur I/O overhead.

• **VM I/O independent** - The HX Data Platform native snapshot creation time is independent of the I/O on the VM.

• **VM performance** - HX Data Platform native snapshots do not degrade VM performance.

• **Crash-consistent. HX Data Platform native snapshots are crash-consistent by default** - I/O crash consistency is defined as maintaining the correct order of write operations to enable an application to restart properly from a crash.

• **Application-consistent** - You can select the `quiesce` option of the `stcli vm snapshot` command through the HX Data Platform CLI to enable HX Data Platform native snapshots to be application-consistent. The applications in the guest VM run transparently exactly like they do in the host VM. For details, see the Cisco HX Data Platform Command Line Interface Reference CLI Reference.

Quiescing a file system is a process of bringing the on-disk data of a physical or virtual computer into a state suitable for backups. This process might include operations such as flushing dirty buffers from the operating system's in-memory cache to disk, or other higher-level application-specific tasks.

If your system displays quiesce errors, see the following VMware KB article *Troubleshooting Volume Shadow Copy (VSS) quiesce related issues (1007696)*, at:

http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=1007696

• **Scheduled snapshots tolerant to node failures** - Scheduled snapshots are tolerant to administrative operations that require a node shutdown, such as HX maintenance mode and HX online upgrade.

Scheduled Snapshots are tolerant to failures in other HX clusters in multi-cluster environments.

• **Unified interface** - You can manage native snapshots created through the HX Data Platform plug-in using VMware snapshot manager™.

• **Individual or grouped** - You can take native snapshots on a VM level, VM folder level, or resource pool level.

• **Granular progress and error reporting** - These monitoring tasks performed at Task level for Resource Pool, Folder and VM level snapshot.

• **Instantaneous snapshot delete** - Deletion of a snapshot and consolidation is always instantaneous.

• **Parallel batch snapshots** - Support for up to 255 VMs in a Resource Pool or Folder for parallel batched snapshots.

• **VDI deployment support** - HX scheduled snapshots are supported for desktop VMs on VDI deployments which are using VMware native technology.

• **Recoverable VM** - The VM is always recoverable when there are snapshot failures.

• **Datastore access** - Snapshots work on partially mounted/accessible datastores as long as the VM being snapshotted is on an accessible mountpoint.
Native Snapshot Considerations

Snapshots parameters

- **Native snapshots** - After you create the first native snapshot using the HX Data Platform plug-in, if you create more snapshots in the vSphere Web Client, these are considered to be native as well. However, if you create the first snapshot using the vSphere Web Client and not the HX Data Platform plug-in, then the vSphere Web Client snapshots are considered to be non-native.

- **Maximum number of stored snapshots** - Currently VMware has a limitation of 31 snapshots per VM. This maximum total includes VMware created snapshots, HX Data Platform SENTINEL snapshot, and HX Data Platform native snapshots.

  For details, see VMware KB, *Committing snapshots in vSphere when more than 32 levels of snapshots are present fails with the error: Too many levels of redo logs (1004545)*, at: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004545

- **Scheduled snapshots** - Do not have overlapping snapshots scheduled on VMs and their resource pools.

VMs

- **Deleted VMs** - The life cycle of native snapshots, similar to VM snapshots, is tied to the virtual machine. If the VM is deleted, accidentally or intentionally, all associated snapshots are also deleted. Snapshots do not provide a mechanism to recover from a deleted VM. Use a backup solution to protect against VM deletion.

- **HX Data Platform storage controller VMs** - You cannot schedule snapshots for storage controller VMs.

- **Non-HX Data Platform VMs** - Snapshots fail for any VM that is not on a HX Data Platform datastore. This applies to snapshots on a VM level, VM folder level, or resource pool level. To make a snapshot, the VM must reside on a HX Data Platform datastore in a HX Data Platform storage cluster.

- **Suspended VMs** - Creating the first native snapshot, the SENTINEL snapshot, from VMs in suspended state is not supported.

vCenter

- **Ready storage cluster** - To allow a native snapshot: The storage cluster must be healthy, including sufficient space and online. The datastores must be accessible. The VMs must be valid and not in a transient state, such as vMotioning.

- **vMotion** - vMotion is supported on VMs with native snapshots.

  **Storage vMotion** - Storage vMotion is not supported on VMs with native snapshots. If the VM needs to be moved to a different datastore, delete the snapshots before running storage vMotion.

Naming

- **Duplicate names** - Do not have VMs or Resource Pools with duplicate names within the HX Data Platform vCenter or snapshots fail. This includes parents and children within nested resource pools and resource pools within different vCenter clusters.

- **Characters in names** - Do not use the special characters, dot (.), dollar sign ($), or accent grave (’) in any guest/user VM name for which you want to enable snapshots.
Disks and datastores

- **VM datastores** - Ensure that all the VM (VMDK) disks are on the same datastore prior to creating native snapshots. This applies to HX Snapshot now and HX Scheduled Snapshots.

- **Thick disks** - If the source disk is thick, then the snapshot of the VM's disk will also be thick. Increase the datastore size to accommodate the snapshot.

- **Virtual disk types** - VMware supports a variety of virtual disk backing types. The most common is the FlatVer2 format. Native snapshots are supported for this format.

  There are other virtual disk formats like Raw Device Mapping (RDM), SeSparse, VmfsSparse (Redlog format). VMs containing virtual disks of these formats are not supported for native snapshots.

Login access

- **SSH** - Ensure that SSH is enabled in ESX on all the nodes in the storage cluster.

Limitations

<table>
<thead>
<tr>
<th>Object</th>
<th>Maximum Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshots</td>
<td>30 per storage cluster</td>
</tr>
<tr>
<td></td>
<td>VMware limit is 31. One snapshot is consumed by SENTINEL.</td>
</tr>
<tr>
<td>Datastores</td>
<td>8 per storage cluster</td>
</tr>
<tr>
<td>VMs</td>
<td>1024 per host</td>
</tr>
<tr>
<td>Powered on VMs</td>
<td>100 per host</td>
</tr>
<tr>
<td>vDisks per VM</td>
<td>60 per VM</td>
</tr>
</tbody>
</table>

**Native Snapshot Best Practices**

**Important**

Always use the HX Data Platform Snapshot feature to create your first snapshot of a VM. This ensures that all subsequent snapshots are in native format.

- Do not use the VMware Snapshot feature to create your first snapshot.

  VMware snapshots use redo log technology that result in degraded performance of the original VM. This performance degrades further with each additional snapshot.

  Native format snapshots do not impact VM performance after the initial native snapshot is created.

  If you have any redo log snapshots, on the ESXi hosts where the redo log snapshots reside, edit the
  /etc/vmware/config file and set snapshot.asyncConsolidate="TRUE".

- Add all the VMDKs to the VM prior to creating the first snapshot.

  When VMDKs are added to the VM, additional SENTINEL snapshots are taken. Each additional SENTINEL consumes a space for additional snapshots.
For example, if you have an existing VM and you add 2 new VMDKs, at the next scheduled snapshot, 1 new SENTINEL is created. Check the snapshot schedule retention number to be sure you have sufficient snapshot slots available; one for the new SENTINEL, one for the snapshot.

• When creating large numbers of snapshots consider the following:
  • Schedule the snapshots at a time when you expect data traffic might be low.
  • Use multiple resource pools or VM folders to group VMs rather than a single resource pool or VM folder. Then stagger the snapshot schedule by group.
    For example resourcePool1, schedule snapshots at :00, resourcePool2, schedule snapshots at :15, resourcePool3, schedule snapshots at :30.

• If you have your vCenter running on a VM in the storage cluster, do not take a native snapshot of the vCenter VM. This is related to VMware KB, VMware VirtualCenter Server service fails due to a quiesced snapshot operation on the vCenter Server database virtual machine (2003674), at https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003674

Understanding SENTINEL Snapshots

When you create the first snapshot of a VM, through either Snapshot Now or a Scheduled Snapshot, the HX Data Platform plug-in creates a base snapshot called a SENTINEL snapshot. The SENTINEL snapshot ensures follow-on snapshots are all native snapshots.

SENTINEL snapshots prevent reverted VMs from having VMware redo log-based virtual disks. Redo log-based virtual disks occur when an original snapshot is deleted and the VM is reverted to the second oldest snapshot.

SENTINEL snapshots are in addition to the revertible native snapshot. The SENTINEL snapshot consumes one snapshot of the total 31 available per VMware limitation.

Using SENTINEL snapshots
  • Do not delete the SENTINEL snapshot.
  • Do not revert your VM to the SENTINEL snapshot.

Native Snapshot Timezones

There are three objects that display and affect the timestamp and schedule of snapshots:
  • vSphere and vCenter use UTC time.
  • vSphere Web client uses the browser timezone.
  • HX Data Platform plug-in, storage cluster, and storage controller VM use the same timezone. This is enforced across the storage cluster. The timezone used by these is configurable. The default is UTC.

The storage controller VM time is used to set the schedule. The vSphere UTC time is used to create the snapshots. The logs and timestamps vary depending upon the method used to view them.
When a schedule is created, the scheduled times are converted to UTC. When you view the schedule through the HX Data Platform plug-in, it displays the controller VM time. When you view a completed snapshot in the vCenter events log, it displays the UTC time.

Because it is possible to have different timezones applying to each object, the event messages and schedules that display in the HX Data Platform plug-in and the vCenter logs might not appear in sync. However, this is only an artifact of the timezones assigned to each display option. When converted to the same timezone, they translate to the same time. For example: 5:30pm PST, 8:30PM EST, 1:30AM UTC are all the same time.

To have vSphere Scheduled Task tab display the same time for a Scheduled Snapshot that you create in the HX Data Platform plug-in, set the storage controller VM to UTC.

To have Scheduled Snapshots run based on local time zone settings, set that timezone for the storage cluster. By default, the storage controller VM uses the UTC time zone set during HX Data Platform installation.

vSphere scheduled tasks lists. If the vSphere and the storage controller VM are not using the same timezone, the vSphere Scheduled tasks tab might display a different time than the scheduled in the HX Data Platform Schedule Snapshot dialog.

vSphere task completed lists. When you configure an hourly snapshot, the snapshot schedule runs between a specific start time and end time. The vSphere Task Window might display a status that a scheduled snapshot was completed outside the hourly end time. This message indicates that vSphere confirmed that the sequence of snapshots are complete.

At the designated hour, vSphere checks if a snapshot should be created and if it is outside the end time, vSphere confirms that a snapshot is not needed, and posts a status message that says the larger task (of taking a series of hourly snapshots) is complete.

Identify and set the timezone used by the storage controller VM

1. From the storage controller VM command line, view the set timezone.
   
   `stcli services timezone show`

2. Change the storage cluster timezone.
   
   `stcli services timezone set --timezone timezone_code`

   See a timezone reference for timezone codes, such as
   

Creating Snapshots

Before you begin

If you have any redo log snapshots for VMs in the HX storage cluster, edit the ESXi host configuration where the redo log snapshots reside. If this step is not completed, VMs might be stunned during snapshot consolidation.

Redo log snapshots are snapshots that are created through the VMWare Snapshot feature and not through the HX Data Platform Snapshot feature.

1. Login to the ESXi host command line

2. Locate and open for editing the file, `/etc/vmware/config`

3. Set the `snapshot.asyncConsolidate` parameter to `TRUE`.
Step 1
From the vSphere Web Client Navigator, select the VM level, VM folder level, or resource pool level. For example, vCenter Inventory Lists > Virtual Machines to display the list of VMs in vCenter.

Step 2
Select a storage cluster VM and open the Actions menu. Either right-click the VM or click the Actions menu in the VM information portlet.

Note
Ensure there are no non-HX Data Platform datastores on the storage cluster resource pool or the snapshot will fail.

Step 3
Select Cisco HX Data Platform > Snapshot Now to display the Snapshot dialog box.

Step 4
Type a name for the snapshot in the snapshot dialog box.

Step 5
Type a description of the snapshot.

Step 6
Click OK to accept your configuration.

The Recent Tasks tab displays the status message:
Create virtual machine native snapshot.

The first snapshot

Scheduling Snapshots Overview

You apply snapshot schedules to storage cluster objects: VMs or resource pools.

Note
If you re-register the vCenter cluster, your HX Data Platform snapshot schedule is lost. If this happens, reconfigure your snapshot schedule.

You can schedule a snapshot to adjust your backup requirements. For example, you can retain more frequent snapshots of critical data. If there is a disaster, you can restore recent snapshots or create a custom real-time snapshot. For less critical data, you do not need to create frequent snapshots or retain backup copies.

Snapshot scheduling enables you to control the costs of using backup. For each VM in your storage cluster, you can schedule hourly, daily, or weekly snapshots. The maximum frequency for any specific VM is once per hour. Hourly setting is in 15 minute increments.

For example, snapshots are taken each day, given the following settings.

VM 1 hourly snapshots to run at hour:15 minutes, between 10 PM and 1 AM.
VM 2 hourly snapshots to run at hour:30 minutes, between 8 PM and 12 AM.
VM 3 and 4 hourly snapshots to run at hour:45, between 6 AM and 8 AM.
VM 5 daily snapshot to run at 6:00 AM

Each day these snapshots are taken.

6:00 AM — VM 5
6:45 AM — VM 3, VM 4
7:45 AM — VM 3, VM 4
8:30 PM — VM2
9:30 PM — VM2
10:15 PM — VM1
10:30 PM — VM2
11:15 PM — VM1
11:30 PM — VM2
12:15 AM — VM1

Notice that the last snapshot is before the ending hour:00.

To schedule a snapshot every hour over 24 hours, set the start time, then set the end time one hour before. For example, hour:15, start 4 PM, end 3 PM. This takes a snapshot at 4:14 PM, 5:15 PM, ... 12:15 AM, 1:15 AM ... 2:15 PM, 3:15 PM. Then restarts the 24 hour cycle. Note: The maximum number of snapshots per VM is 32. So, you could only take an hourly snapshot up to 32 hours.

The schedule snapshot displays the set time for the snapshot based on the current time zone setting for the storage controller VM. So, if a snapshot was set at 7 pm PST and the storage controller VM time zone is changed to EST. The next time you open the scheduler window, it automatically updates to 10 pm EST.

### Scheduling Snapshots

**Step 1**
From the vSphere Web Client Navigator Home page, select the VM or resource pool list.

For example, **vCenter Inventory Lists > Virtual Machines** to display the list of VMs in vCenter.

**Step 2**
Select a storage cluster VM or resource pool and open the **Actions** menu.

Either right-click the object or click the Actions menu.

**Step 3**
From the Actions menu, select **Cisco HX Data Platform > Schedule Snapshot** to display the Schedule Snapshot dialog box.

**Step 4**
Select the snapshot frequency.

Click the boxes for hourly, daily, and/or weekly frequency and set the starting days, times, and duration.

**Step 5**
Set the number of snapshots to retain.

When the maximum number is reached, older snapshots are removed as newer snapshots are created.

**Step 6**
Unselect existing scheduled items, as needed.

If a previous schedule existed, unselecting items deletes those items from the future schedule.

**Step 7**
Click **OK** to accept the schedule and close the dialog.

### Setting the Frequency of Scheduled Snapshots

Create a snapshot every hour at specific times, daily at a specific time, or weekly on selected days and times.
Before you begin

Open the **Schedule Snapshot** dialog box for a VM or resource pool.

### Managing Native Snapshots

**Step 1**
From the Schedule Snapshot dialog box, select the **Enable Hourly Snapshot**, **Enable Daily Snapshot**, or **Enable Weekly Snapshot** check box.

**Step 2**
Click the **Start** at drop-down list to select a start time. Select hour, minutes in 15 minute increments, and AM or PM.

**Step 3**
For an hourly snapshot schedule, click the **Until** drop-down list to select an end time. Select hour, minutes in 15 minute increments, and AM or PM. Set the minute to the same value as the Start at time.

The HX Data Platform plug-in creates a snapshot of the VM every hour between the start and end times.

**Step 4**
Select the corresponding check box to specify **Days** of the week on which you want to take the snapshots.

**Step 5**
Under **Retention**, either type a number or use the arrow button to specify the maximum number of copies to retain for each schedule.

### Deleting Snapshot Schedules

**Step 1**
From the vSphere Web Client Navigator Home page, select the VM or resource pool list. For example, **vCenter Inventory Lists > Virtual Machines** to display the list of VMs in vCenter.

**Step 2**
Select a storage cluster VM or resource pool and open the **Actions** menu. Either right-click the object or click the Actions menu.

**Step 3**
From the Actions menu, select **Cisco HX Data Platform > Schedule Snapshot** to display the Schedule Snapshot dialog box.

**Step 4**
Unclick the scheduled options you no longer want.

**Step 5**
Click **OK** to accept the changes, this includes deleting previously configured schedules, and exit the dialog.

**Step 6**
Confirm the schedule is deleted.

Select a storage cluster VM or resource pool. Click the vCenter tabs, **Manage > Scheduled Tasks**. The previous snapshot schedule should not be listed.

### Reverting to a Snapshot

Reverting a snapshot is returning a VM to a state stored in a snapshot. Reverting to a snapshot is performed on one VM at a time. This is not performed at the resource pool or VM folder level. Reverting snapshots is performed through the vCenter Snapshot Manager and not through the HX Data Platform plug-in.

**Before you begin**

Snapshots of the VM must exist.
Step 1  From the vSphere Web Client Navigator Home page, select the VM level, VM folder level, or resource pool level. For example, **vCenter Inventory Lists > Virtual Machines** to display the list of VMs in vCenter.

Step 2  Select a storage cluster VM and open the **Actions** menu. Either right-click the VM or click the Actions menu in the VM information portlet.

Step 3  Select **Snapshots > Manage Snapshots** to open the vSphere Snapshot Manager.

Step 4  Select a snapshot to revert to from the hierarchy of snapshots for the selected VM.

Step 5  Click **Revert to > Yes > Close**.

The reverted VM is included in the list of VMs and powered off. In selected cases, a VM reverted from a VM snapshot is already powered on.

Step 6  Select the reverted VM and power it on.

---

### Deleting Snapshots

Deleting snapshots is managed through the vSphere interface and not through the HX Data Platform plug-in.

Step 1  From the vSphere Web Client Navigator, select **VMs and Templates > vcenter_server > Snapshots > datacenter > vm**.

Step 2  Right-click the **vm** and select **Snapshots > Manage Snapshots**.

Step 3  Select a snapshot and click **Delete**.

**Note**  Delete the SENTINEL snapshot by using **Delete All** option only. Do not delete the SENTINEL snapshot individually.
Managing Virtual Machine Disaster Recovery

Data Protection Overview

The HX Data Platform disaster recovery feature allows you to protect virtual machines from a disaster by setting up replication of running VMs between a pair of network connected clusters. Protected virtual machines running on one cluster replicate to the other cluster in the pair, and vice versa. The two paired clusters typically are located at a distance from each other, with each cluster serving as the disaster recovery site for virtual machines running on the other cluster.

Once protection has been set up on a VM, HX Data Platform periodically takes a replication snapshot of the running VM on the local cluster and replicates (copies) the snapshot to the paired remote cluster. In the event of a disaster at the local cluster, the most recently replicated snapshot of each protected VM is used by the user to recover and run the VM at the remote cluster. Each cluster that serves as a disaster recovery site for another cluster, must be sized with adequate spare resources so that upon a disaster, it can run the newly recovered virtual machines in addition to its normal workload.

Each virtual machine can be individually protected by assigning it protection attributes, chief among which is the replication interval (schedule). The shorter the replication interval, the fresher the replicated snapshot data is likely to be, when it is time to recover the VM after a disaster. Replication intervals can range between 15 minutes and 24 hours.

A new per-cluster grouping construct, called a Protection Group, groups protected VMs and assigns them the same protection attributes. A VM can be protected simply by adding it to a protection group for which attributes have already been defined.

Setting up replication requires two existing clusters running HX Data Platform version 2.5 or higher. Both clusters must be on the same HX Data Platform version. This setup can be completed online.

First, each cluster is set up for replication networking. This involves, using HX Connect to provide a set of IP addresses to be used by local cluster nodes to replicate to the remote cluster. As part of the process, HX Connect creates VLANs through UCS Manager, for dedicated replication network use.
Next, the two clusters, and their corresponding existing relevant datastores must be explicitly paired. The pairing setup can be completed using HX Connect from one of the two clusters. This requires administrative credentials of the other cluster.

Finally, virtual machines can be protected (or have their existing protection attributes modified) by using HX Connect at the cluster where they are currently active.

HX Connect can be used to monitor status of both incoming and outgoing replications at a cluster.

After a disaster, a protected VM can be recovered and run at the cluster that serves as the disaster recovery site for that VM, using the stcli command line tool invoked on any node within the cluster.

**Replication and Recovery Considerations**

The following is a list of considerations when configuring virtual machine replication and performing disaster recovery of virtual machines.

- **Administrator**—All replication and recovery tasks, except monitoring, can only be performed by users with administrator privileges on the local cluster. For tasks involving a remote cluster, both the local and remote users provided must have administrator privileges and be configured with vCenter SSO on their respective clusters.

- **Storage Space**—Ensure you have sufficient space on the remote cluster to support your replication schedule. The protected virtual machines are replicated (copied) to the remote cluster at every scheduled interval. Though storage capacity methods are applied, (deduplication, compression), each replicated virtual machine does consume some storage space.

Not having sufficient storage space on the remote cluster can cause the remote cluster to reach capacity usage maximums. If you see Out of Space errors, see [Handling Out of Space Errors](#), on page 63. Pause all replication schedules until you have appropriately adjusted the space available on the HX Cluster. Always ensure your cluster capacity consumption is below the space utilization warning threshold.

- **Unsupported Clusters**—Replication protection is between two HX Clusters.
  - Replication between, to, or from Edge clusters is not supported.

- **Rebooting Nodes**—Do not reboot any nodes in the HX Cluster during any restore, replication, or recovery operation.

- **Thin Provision**—Protected virtual machines are recovered with thin provisioned disks irrespective of how disks were specified in the originally protected virtual machine.

- **Protection Group Limitations**—
  - The maximum number of VMs allowed in a protection group is 32.
  - Do not add VMs with ISOs or floppies to protection groups.

- **Non-HX Datastores**—If you have protected a VM that includes storage on a non-HX datastore, attempts to periodically replicate this VM fail. Either unprotected this VM, or remove its non-HX storage.

Similarly, Do not move protected VMs from HX datastores to non-HX datastores. If a VM is moved to a non-HX datastore through storage vMotion, unprotect the VM, then reapply the protection.

- **Hierarchy of Recovered Virtual Machines**—
  - Recovery of virtual machines replication keeps the hierarchy as is.
• Test recovery consolidates the replication virtual machines consolidates the replication hierarchy into a common cloned base disk. The data is all in the cloned common disk. However, since it is testing as a clone with a new vm-uuid, the test recovery starts a new replication virtual machine hierarchy.

• **Snapshot Memory Option**—Do not include the snapshot memory option when configuring virtual machines for data protection replication or recovery.

A memory snapshot includes the memory and power state of the VM. This type of snapshot takes longer to complete. See VMware vSphere best practices documentation for additional information.

• **Snapshot Types**—HX Data Platform uses several forms of snapshot technology. Each snapshot satisfies a specific use case and has specific traits. They are not interchangeable.
  - A ReadyClone—similar to a standard clone, is a copy of an existing VM. The existing VM is called the host VM. When the cloning operation is complete, the ReadyClone is a separate guest VM.
  - A Native Snapshots—a backup feature that saves versions (states) of working VMs. VMs can be reverted back to native snapshots.
  - A Replication Snapshot—created as part of the VM replication protection. At the scheduled time, a replication snapshot is taken of a running VM. This snapshot is then replicated (copied) to the remote cluster.
  - A Recovery Test Snapshot—a temporary snapshot used to verify that the recovery system is working.
  - A Recovered VM—the restored VM, created by restoring a most recent replication snapshot from the recovery cluster.

**Data Protection Terms**

**Failover**—Part of the manual VM recovery process in the event of a disaster on the source cluster. Failover, in this context, is converting a replication snapshot on the target cluster into a working VM.

**Interval**—Part of the replication schedule configuration. This is how often the protected VMs replication snapshot is taken and copied to the target cluster.

**Local cluster**—One of a VM replication cluster pair. The cluster you are currently logged into through HX Connect. From the local cluster, you configure replication protection for locally resident VMs. The VMs are then replicated to the paired remote cluster.

**Migration**—A routine system maintenance and management task where a recent replication snapshot copy of the VM becomes the working VM. The replication pair of source and target cluster does not change.

**Primary cluster**—An alternative name for the source cluster in VM disaster recovery.

**Protected virtual machine**—A VM that has replication configured. Protected VMs:
  - Reside on a datastore in the local cluster of a replication pair.
  - Have a replication schedule configured either individually or through a protection group.

**Protection group**—A means to apply the same replication configuration on a group of VMs.

**Recovery process**—Manual process to recover protected VMs in the event the source cluster fails or a disaster occurs.
Recovery test—A maintenance task that ensures the recovery process would be successful in the event of a disaster.

Remote cluster—One of a VM replication cluster pair. The remote cluster receives the replication snapshots from the local cluster's protected VMs.

Replication pair—Two clusters that together provide a remote cluster location for storing replication snapshots of local cluster VMs.

Clusters in a replication pair can be both a remote or local cluster. Both clusters in a replication pair can have resident VMs. Each cluster is local to its resident VMs. Each cluster is remote to the VMs that reside on the paired local cluster.

Replication snapshot—Part of the replication protection mechanism. A type of snapshot taken of the protected VM. Copied from the local cluster to the remote cluster.

Secondary cluster—An alternative name for the target cluster in VM disaster recovery.

Source cluster—One of a VM recovery cluster pair. The source cluster is where the protected VMs reside.

Target cluster—One of a VM recovery cluster pair. The target cluster receives the replication snapshots from the source cluster's VMs. The target cluster is used to recover the VMs in the event of a disaster on the source cluster.

Protecting Virtual Machines Overview

A virtual machine can be protected by specifying its protection attributes.

- A replication interval, which also can be thought of as frequency of replication
- A start time (within the next 24 hours), which specifies the first time replication is attempted for that virtual machine
- Whether the replication snapshot should be taken with the virtual machine quiesced, or not.

Protection groups can be created and assigned protection attributes. Virtual machines can be added to a protection group and, through the grouping, all be assigned the same protection attributes.

For example, say you have three classes of protection: gold, silver, and bronze. Set up a protection group for each class, with replication intervals such as 15 minutes for gold, 4 hours for silver, and 24 hours for bronze. Most of your VMs could be protected by merely adding them to one of the three already created protection groups.

To protect virtual machines, select a method.

Note

When you select multiple virtual machines you must add them to a protection group.

- Independently—Select one virtual machine and configure. You set the replication schedule and the VMware quiesce option for the specific virtual machine. Changes to the replication settings only affect the independently protected virtual machine. The virtual machine in not included in a protection group.

- Existing protection group—Select one or more virtual machines and them to an existing protection group. The schedule and VMware quiesce option settings are applied to all the virtual machines in the
protection group. When the protection group settings are changed, the changes are applied to all the virtual machines in the protection group.

• **New protection group**—Select two or more virtual machines and choose to create a new protection group. Define the protection group name, schedule, and VMware quiesce option settings. These settings are applied to all the virtual machines in the protection group. When the protection group settings are changed, the changes are applied to all the virtual machines in the protection group.

### Data Protection Workflow

Replication is the process of protecting VMs and their data. This requires:

- Configuring two clusters. Configure each to support the replication network activity and pair them to each other.
- Assigning VMs replication schedule to set the frequency (interval) for creating replication snapshots on the source cluster and copying them to the target cluster. This is set on individual VMs and VMs in protection groups.

#### Replication workflow

1. HX Data Platform installed and two clusters created.
2. Create at least one datastore, on each cluster.
3. Login to HX Connect.
4. Configure cluster replication network. Configure this on each cluster. The replication network information is unique to each cluster.
   
   Specify the subnet, gateway, range of IP addresses, bandwidth limit for dedicated use by the replication network. HX Data Platform configures a VLAN through UCS Manager for both clusters through UCS Manager.
5. Create a replication pair, connecting the two clusters.
   This is performed from one cluster.
6. Optionally, create protection groups.
   - Set the schedule. Each protection group has one schedule.
   - Create multiple protection groups if you want to have a variety of replication intervals (schedules) for different virtual machines. A virtual machine can only belong to one protection group.
7. Select virtual machines to protect, as either:
   
   Individual virtual machines
   
   Virtual machines assigned to protection groups
8. Set protection
   1. Select one or more virtual machines. Click Protect.
   2. From the Protect Virtual Machine wizard, options are:
      
      - Protect a single virtual machine through an existing protection group.
• Protect a single virtual machine independently.
  Set the schedule.
• Protect multiple virtual machines through an existing protection group.
• Protect multiple virtual machines through an new protection group.
  Create new protection group and set schedule.

Configuring the Replication Network

Before a replication pair can be configured, the replication network has to be configured on both the local and remote cluster. Complete the configuration on the local cluster, then login to the remote cluster and complete the configuration there.

**Step 1**
Login to HX Connect as administrator for this cluster's management network.

**Step 2**
Select **Replication** > **Configure**.

You can only configure the replication network once. Once configured, you can edit the available IP addresses and the networking bandwidth.

**Step 3**
Enter the network information.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
</table>
| Select an existing VLAN radio button | Select this check box to add an existing VLAN.  
  If you manually configured a VLAN for use by the replication network through Cisco UCS Manager, the VLAN name is automatically populated with a default VLAN name.  
  Otherwise, enter a VLAN ID or a VLAN name. |
| Create a new VLAN radio button  | Select this check box to create a new VLAN.                                                                                                                                                                      |
| VLAN ID field                  | Click the up or down arrows to select a number for the VLAN ID or type a number in the field.  
  Enter the VLAN ID configured through Cisco UCS Manager for use by the replication network. This is separate from the HX Data Platform Management traffic network and Data traffic network.  
  **Important** Be sure to use a different VLAN ID number for each HX Storage Cluster in the replication pair.  
  Replication is between two HX Storage Clusters. Each HX Storage Cluster requires a VLAN dedicated to the replication network.  
  For example, 1.  
  When a value is added, the default VLAN Name is updated to include the additional identifier. The VLAN ID value does not affect a manually entered VLAN name. |
Step 4  
Click **Configure**.

HX Data Platform verifies the remote network, logs in and obtains a VLAN from UCS Manager, assigns an IP address to each node in the local cluster.

---

**What to do next**

Be sure to configure the replication network on both HX Storage Clusters for the replication pair.

**Editing the Replication Network**

When you expand a HX Cluster that has replication configured, ensure that you have sufficient IP addresses available for the replication network. The replication network requires dedicated IP addresses, one for every node in the cluster plus one more. So, in a 3 node cluster, 4 IP addresses are required. If you are adding one more node to the cluster, 5 IP addresses are minimum. Edit the replication network to add IP addresses.

Removing a node releases the assigned IP address.

---

**Step 1**
Login to HX Connect as administrator for this cluster's management network.

**Step 2**
Select **Replication > Edit** button.

After the replication network is created, you can edit the range of IPs to use and set the outbound bandwidth value for replication traffic. The replication network subnet, gateway, and VLAN ID are displayed for reference only and cannot be edited.

**Step 3**
Update the fields as required and click **Save Changes**.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name field</td>
<td>This field is automatically populated with a default VLAN name when the <strong>Create a new VLAN</strong> check box is selected. The VLAN ID is concatenated to the name.</td>
</tr>
<tr>
<td>UCS Manager host IP or FQDN field</td>
<td>Enter Cisco UCS Manager FQDN or IP address. For example, 10.193.211.120.</td>
</tr>
<tr>
<td>Username field</td>
<td>Enter administrative username for Cisco UCS Manager.</td>
</tr>
<tr>
<td>Password field</td>
<td>Enter administrative password for Cisco UCS Manager.</td>
</tr>
<tr>
<td>VLAN ID field</td>
<td>The VLAN ID configured for this replication network. This value cannot be edited.</td>
</tr>
<tr>
<td>Subnet field</td>
<td>The subnet configured for the replication network in network prefix notation. This value cannot be edited.</td>
</tr>
<tr>
<td>Gateway field</td>
<td>The gateway configured for the replication network. This is value cannot be edited.</td>
</tr>
</tbody>
</table>
### Replication Pair Overview

Creating a replication cluster pair is a pre-requisite for setting up VMs for replication. The replication network and at least one datastore must be configured prior to creating the replication pair.

By pairing cluster 1 with cluster 2, you are specifying that all VMs on cluster 1 that are explicitly set up for replication, can replicate to cluster 2, and that all VMs on cluster 2 that are explicitly set up for replication, can replicate to cluster 2.

By pairing a datastore A on cluster 1 with a datastore B on cluster 2, you are specifying that for any VM on cluster 1 that is set up for replication, if it has files in datastore A, those files will be replicated to datastore B on cluster 2. Similarly, for any VM on cluster 2 that is set up for replication, if it has files in datastore B, those files will be replicated to datastore a on cluster 1.

Pairing is strictly 1-to-1. A cluster can be paired with no more than one other cluster. A datastore on a paired cluster, can be paired with no more than one datastore on the other cluster.

### Creating a Replication Pair

The replication pair defines the two halves of the protection network. The HX Storage Cluster you are logged into is the local cluster, the first half of the pair. Through this dialog, you identify another HX Storage Cluster, the second half of the pair, the remote cluster. To ensure the storage component, map the replication pair to datastores on each HX Storage Cluster.

Repeat these steps on the remote cluster, too.
Before you begin

- Configure the replication network on each cluster.
- Create at least one datastore on each cluster.
- Ensure both local and remote HX Storage Clusters are using Single Sign-on (SSO).
- Specify users that have administrative privileges.
- Login to HX Connect as a user with administrator privileges.

Step 1
From HX Connect, select **Replication > Create Replication Pair**.

Step 2
Enter a **Name** for the replication pair and click **Next**.

Enter a name for the replication pairing between two HX Storage Clusters. This name is set for both the local and remote cluster. The name cannot be changed.

Step 3
Enter the **Remote Connection** identification and click **Pair**.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP or FQDN field</td>
<td>Enter the IP address or fully qualified domain name (FQDN) for the management network on the remote HX Storage Cluster. For example: 10.10.10.10.</td>
</tr>
<tr>
<td>User Name and Password fields</td>
<td>Enter vCenter single sign-on or cluster specific credentials for the remote HX Storage Cluster. The user entered must have administrator privileges.</td>
</tr>
</tbody>
</table>

HX Data Platform verifies the remote HX Storage Cluster and assigns the replication pair name.

**Note** Virtual machines to be protected must reside on one of the datastores in the replication pair.

Step 4
Set the **Datastore Mapping** from both clusters and click **Next**.

**Note** The virtual machines to be protected must on the datastores you select. Moving virtual machines from the configured datastores for the replication pair, also removes protection from the virtual machines.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Datastore column</td>
<td>List of the configured datastores on this cluster, the local HX Storage Cluster. Map one local datastore to one remote datastore.</td>
</tr>
<tr>
<td>Remote Datastore column</td>
<td>Pair the datastores between the HX Storage Clusters. From the desired Local Datastore row, select a datastore from the Remote Datastore pull-down menu. This selects both the remote and local datastores in a single action.</td>
</tr>
</tbody>
</table>

Step 5
Review the Summary information and click **Map Datastores**.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore field</td>
<td>The selected datastore on this local HX Storage Cluster.</td>
</tr>
</tbody>
</table>
**Editing a Replication Pair**

Editing a replication pair is changing the datastores for the replication pair.

---

**Note**

Changing the datastores used in a replication pair removes protection from all virtual machines on both the local and remote clusters.

---

**Step 1**

Login to HX Connect as an administrator.

**Step 2**

Select Replication > Replication Pairs > Edit.

**Step 3**

Select the local or remote datastore and click Finish.

---

### UI Element | Essential Information
--- | ---
**Target Datastore** field | The datastore on the remote HX Storage Cluster where the replication snapshot is copied to.

---

### UI Element | Essential Information
--- | ---
**Local Datastore** column | List of the configured datastores on this cluster, the local HX Storage Cluster. Map one local datastore to one remote datastore.

**Remote Datastore** column | Pair the datastores between the HX Storage Clusters.

1. To change the local datastore selection, remove the mapping to the current local datastore.

   From the pull-down menu in the Remote Datastore column, select **Do not map this datastore**.

2. From the desired Local Datastore row, select a datastore from the Remote Datastore pull-down menu. This selects both the remote and local datastores in a single action.

---

### Deleting a Replication Pair

Delete a replication pair on the local and remote clusters.

Select Replication > Replication Pairs > Delete.

**Before you begin**

On both the local and remote clusters, remove dependencies from the replication pair.

From this local HX Storage Cluster, perform the following. Then login to the remote HX Storage Cluster and perform the following.
• Unprotect all virtual machines. Remove individual protection. Remove virtual machines from protection groups.
• Remove protection groups.

### Step 1
Login to HX Connect as an administrator.

### Step 2
Unmap the datastores in the replication pair.

   a) Select Replication > Replication Pairs > Edit.
   b) From the Edit Replication Pair dialog box, select Do not map this datastore from the Remote Datastore menu.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Datastore</strong> column</td>
<td>List of the configured datastores on this cluster, the local HX Storage Cluster. Map one local datastore to one remote datastore.</td>
</tr>
<tr>
<td><strong>Remote Datastore</strong> column</td>
<td>Pair the datastores between the HX Storage Clusters.</td>
</tr>
</tbody>
</table>

1. To change the local datastore selection, remove the mapping to the current local datastore.
   
   From the pull-down menu in the Remote Datastore column, select Do not map this datastore.

2. From the desired Local Datastore row, select a datastore from the Remote Datastore pull-down menu. This selects both the remote and local datastores in a single action.

   c) Ensure all the possible remote datastores are set to Do not map this datastore.
   d) Click Finish.

### Step 3
Select Replication > Replication Pairs > Delete.

### Step 4
Enter administrator credentials for the remote cluster and click Delete.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong> field</td>
<td>Enter the administrator user name for the remote HX Storage Cluster.</td>
</tr>
<tr>
<td><strong>Password</strong> field</td>
<td>Enter the administrator password for the remote HX Storage Cluster.</td>
</tr>
</tbody>
</table>

### Creating a Protection Group
Create protection groups on a local cluster. Protection groups can only be manage through, and provide protection to, the cluster where they are created. If protection groups have protected virtual machines that replicate to the local cluster, these protection groups are listed in HX Connect. However, you can only manage a protection group from its local cluster, the cluster where it is created.

**Before you begin**
Replication network and replication pair must be configured.
Step 1  Login to HX Connect as an administrator.

Step 2  Select Replication $>$ Protection Groups $>$ Create Protection Group.

Step 3  Enter the information in the dialog fields.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Group Name field</td>
<td>Enter a name for the new protection group for this local cluster. Protection groups are unique to each cluster. The name is referenced on the remote cluster, but not editable on the remote cluster. You can create multiple protection groups on the cluster.</td>
</tr>
<tr>
<td>Protect virtual machines in this group every field</td>
<td>Select how often the virtual machines are to be replicated to the paired cluster. Default is every 1 hour. The pull-down menu options are: 5 minutes, 15 minutes, 30 minutes, 1 hour, 90 minutes, 2 hours, 4 hours, 8 hours, 12 hours, 24 hours</td>
</tr>
<tr>
<td>Start protecting the virtual machines immediately radio button</td>
<td>Select this radio button if you want the first replication to start immediately after you add the first virtual machine to this protection group.</td>
</tr>
</tbody>
</table>
| Start protecting the virtual machines at radio button | Select this radio button if you want to set a specific time for the first replication to start. Before you start replication ensure:  
  • At least one virtual machine is added to the protection group.  
  • The scheduled start time is reached. To specify the protection start time:  
    1. Check the Start protecting the virtual machines at radio button.  
    2. Click in the time field and select an hour and minute. Then click out of the field.  
  
  Cluster time zone and Current time on cluster are references to help you to choose the appropriate replication start time. Start time is based on the local cluster clock. For example:  
  10 hours, 3 minutes from now with Current time on cluster, 1:56:15PM, means that the first replication occurs at 11:59:00PM.  
  The hours, minutes from now states when the first replication will occur. This is updated when you change the time field setting.  
  
Use VMware Tools to quiesce the virtual machine check box | To have HX Data Platform quiesce the virtual machines before taking the replication snapshot, click this check box.  
  
This only applies to virtual machines with VMware Tools installed. |

Step 4  Click Create Protection Group.

HX Data Platform adds the new group to the Protection Groups tab. This protection group is available to protect virtual machines on this cluster.
Step 5  
Click the **Replication** > **Protection Groups** to view or edit the new protection group.

Notice that the number of VMs is zero, (0). You must add virtual machines to this new protection group to apply the replication schedule set in this protection group.

---

**Editing Protection Groups**

Change the replication interval (schedule) for the virtual machines in the protection group.

---

### Step 1
Login to HX Connect as an administrator.

### Step 2
Select **Replication** > **Protection Groups** > **Edit Schedule**.

### Step 3
Edit the information in the dialog fields.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect virtual machines in this group every</strong> field</td>
<td>Select from the pull-down list how often the virtual machines are to be replicated to the paired cluster. The options are: 15 minutes, 30 minutes, 1 hour, 90 minutes, 2 hours, 4 hours, 8 hours, 12 hours, 24 hours</td>
</tr>
<tr>
<td><strong>Use VMware Tools to quiesce the virtual machine</strong> check box</td>
<td>To have HX Data Platform quiesce the virtual machines before taking the replication snapshot, click this checkbox. This only applies to virtual machines with VMware Tools installed.</td>
</tr>
</tbody>
</table>

### Step 4
Click **Save Changes**.

HX Data Platform updates the interval and start time for the protection group. See the **Protection Groups** tab to view the new interval frequency.

---

**Deleting Protection Groups**

**Before you begin**

Remove all virtual machines from the protection group.

### Step 1
Unprotect all virtual machines in the protection group.

a) From the HX Connect select **Replication** > **Protected Virtual Machines**

b) Select all the virtual machines in the protection group.

c) Click **Unprotect**. Click **Unprotect** in the verification pop-up.

### Step 2
Select **Replication** > **Protection Groups** > **protection_group_name**

### Step 3
Click **Delete**. Click **Delete** in the verification pop-up.
Protecting Virtual Machines with an Existing Protection Group

This task describes how to protect multiple virtual machines using an existing protection group.

Using an Existing protection group—Select one or more virtual machines and them to an existing protection group. The schedule and VMware quiesce option settings are applied to all the virtual machines in the protection group. When the protection group settings are changed, the changes are applied to all the virtual machines in the protection group.

Before you begin
Replication network and replication pair configured.
Create protection group prior to adding the virtual machines.

---

### Step 1
Login to HX Connect with administrator privileges and select Virtual Machines.
This lists the virtual machines on the local cluster.

### Step 2
Select two or more unprotected virtual machine from the list.
Click in the virtual machine row to select it. As you click a virtual machine row, the corresponding virtual machine checkbox is selected.

### Step 3
Click Protect.
The Protect Virtual Machines wizard, Protection Group page is displayed.

### Step 4
Click the radio button, Add to an existing protection group

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the protection parameters table</td>
<td>Verify the selected virtual machine Name. Use the Storage Provisioned and Storage Used to check you have sufficient resources available on the remote HX Storage Cluster.</td>
</tr>
<tr>
<td>Add to an existing protection group radio button</td>
<td>Select an existing protection group from the pull-down list. The interval and schedule settings of the protection group are applied to this virtual machine.</td>
</tr>
<tr>
<td>Create a new protection group radio button</td>
<td>Enter a name for the new protection group for this local cluster. Protection groups are unique to each cluster. The name is referenced on the remote cluster, but not editable on the remote cluster. You can create multiple protection groups on the cluster.</td>
</tr>
</tbody>
</table>

### Step 5
Select a protection group from the pull-down list and click Next
Be sure the protection group you choose has the schedule interval desired.
The Protect Virtual Machines wizard, Summary page is displayed.

### Step 6
Confirm the information in the Summary page and click Add to Protection Group.
Protecting Virtual Machines with a New Protection Group

This task describes how to protect multiple virtual machines by creating a new protection group.

Using a New protection group—Select two or more virtual machines and choose to create a new protection group. Define the protection group name, schedule, and VMware quiesce option settings. These settings are applied to all the virtual machines in the protection group. When the protection group settings are changed, the changes are applied to all the virtual machines in the protection group.

Before you begin
Replication network and replication pair configured.

Step 1
Login to HX Connect with administrator privileges and select Virtual Machines. This lists the virtual machines on the local cluster.

Step 2
Select two or more unprotected virtual machine from the list.
Click in the virtual machine row to select it. As you click a virtual machine row, the corresponding virtual machine checkbox is selected.

Step 3
Click Protect.
The Protect Virtual Machines wizard, Protection Group page is displayed.

Step 4
Click the radio button, Create a new protection group, add a name for the protection group, and click Next.
The Protection Schedule Wizard Page wizard page is displayed.

Step 5
Complete the schedule and VMware quiesce option, as needed, and click Next.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect virtual machines in this group every</td>
<td>Select how often the virtual machines are to be replicated to the paired cluster. Default is every 1 hour. The pull-down menu options are:</td>
</tr>
<tr>
<td>field</td>
<td>Select this radio button if you want the first replication to start immediately after you add the first virtual machine to this protection group.</td>
</tr>
<tr>
<td>Start protecting the virtual machines immediately radio button</td>
<td></td>
</tr>
</tbody>
</table>

HX Data Platform adds the virtual machines to replication protection. View the Replication or Virtual Machines pages to confirm. Notice on the Replication page the Protection Group is listed.
Start protecting the virtual machines at radio button

Select this radio button if you want to set a specific time for the first replication to start. To start replication requires:

- At least one virtual machine is added to the protection group.
- The scheduled start time is reached.

To specify the protection start time:

1. Check the Start protecting the virtual machines at radio button.
2. Click in the time field and select an hour and minute. Then click out of the field.

The hours, minutes from now states when the first replication will occur. This is updated when you change the time field setting.

Cluster time zone and Current time on cluster are references to help you to choose the appropriate replication start time. Start time is based on the local cluster clock. For example:

10 hours, 3 minutes from now with Current time on cluster, 1:56:15PM, means that the first replication occurs at 11:59:00PM.

Use VMware Tools to quiesce the virtual machine check box

To have HX Data Platform quiesce the virtual machines before taking the replication snapshot, click this checkbox. This only applies to virtual machines with VMware Tools installed.

The Protect Virtual Machines wizard, Summary page is displayed.

Step 6

Confirm the information in the Summary page and click Add to Protection Group.

Review the summary content to confirm the settings to apply to the selected virtual machines.

- Name of the protection group
- Number of virtual machine to protect
- Names of virtual machines
- Storage provisioned for each virtual machine
- Storage used (consumed) by each virtual machine

HX Data Platform adds the virtual machines to replication protection. View the Replication or Virtual Machines pages to confirm. Notice on the Replication page the Protection Group is listed.
Protecting Individual Virtual Machines

This task describes how to protect a virtual machine.

- **Independently**—Select one virtual machine and configure. You set the replication schedule and the VMware quiesce option for the specific virtual machine. Changes to the replication settings only affect the independently protected virtual machine. The virtual machine is not included in a protection group.

- **Existing protection group**—Select one or more virtual machines and them to an existing protection group. The schedule and VMware quiesce option settings are applied to all the virtual machines in the protection group. When the protection group settings are changed, the changes are applied to all the virtual machines in the protection group.

**Before you begin**

Replication network and replication pair configured.

**Step 1**

Login to HX Connect with administrator privileges and select **Virtual Machines**. This lists the virtual machines on the local cluster.

**Step 2**

Select one unprotected virtual machine from the list. Click in the virtual machine row to select it. Click in the virtual machine row to select it. As you click a virtual machine row, the corresponding virtual machine checkbox is selected.

**Step 3**

Click **Protect**. The **Protect Virtual Machine** dialog box is displayed.

**Step 4**

Complete the fields as needed.

<table>
<thead>
<tr>
<th>UI Element</th>
<th>Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add to an existing protection group</strong> radio button</td>
<td>Select an existing protection group from the pull-down list. The interval and schedule settings of the protection group are applied to this virtual machine. No additional configuration is required, click <strong>Protect Virtual Machine</strong>.</td>
</tr>
<tr>
<td><strong>Protect this virtual machine independently</strong> radio button</td>
<td>Enables the interval, schedule options, and VMware Tools option for defining protection for this virtual machine.</td>
</tr>
<tr>
<td><strong>Protect this virtual machine every</strong> field</td>
<td>Select from the pull-down list how often the virtual machines are to be replicated to the paired cluster. The options are: 15 minutes, 30 minutes, 1 hour, 90 minutes, 2 hours, 4 hours, 8 hours, 12 hours, 24 hours</td>
</tr>
<tr>
<td><strong>Start protecting the virtual machines immediately</strong> radio button</td>
<td>Select this radio button if you want the first replication to start immediately after you add the first virtual machine to this protection group.</td>
</tr>
</tbody>
</table>
UI Element | Essential Information
--- | ---
Start protecting the virtual machines at radio button | Select this radio button if you want to set a specific time for the first replication to start. To start replication requires:
- At least one virtual machine is added to the protection group.
- The scheduled start time is reached.
To specify the protection start time:
1. Check the Start protecting the virtual machines at radio button.
2. Click in the time field and select an hour and minute. Then click out of the field.
   The hours, minutes from now states when the first replication will occur. This is updated when you change the time field setting.

Cluster time zone and Current time on cluster are references to help you to choose the appropriate replication start time. Start time is based on the local cluster clock. For example:
10 hours, 3 minutes from now with Current time on cluster, 1:56:15PM, means that the first replication occurs at 11:59:00PM.

VMware Tools to quiesce the virtual machine check box | To have HX Data Platform quiesce the virtual machines before taking the replication snapshot, click this checkbox.
This only applies to virtual machines with VMware Tools installed.

Step 5  
Click Protect Virtual Machine.

The virtual machine status is updated in the Virtual Machine page and the Replication page. Notice on the Replication page no Protection Group is listed.
Replication is now enabled on this virtual machine.

### Unprotecting Virtual Machines

When you want to remove a protection group, you must unprotect the virtual machines in that protection group.

**Note**  
You do not need to unprotect virtual machines to pause replication for cluster activities. See Pausing Replication, on page 170.

**Step 1**  
Login to HX Connect as an administrator.

**Step 2**  
Select Virtual Machines.

This lists the virtual machines on the local cluster.
Step 3  
Select a protected virtual machine from the list. Click in the virtual machine row.
You can unprotect one virtual machine at a time.

Step 4  
Click Unprotect and click to confirm.
The state changes for the virtual machine from protected to unprotected.

---

**VM Migration Overview**

Migration is a form of failover that can be used at anytime, for routine system maintenance and management.

Migration features:
- Removes the ownership of VMs from the source cluster and adds ownership to the target cluster.
- Retains the pairing between the source and target clusters.

**Note**
Migration is not a disaster recovery task.

Migration process:
1. On the target cluster, use a recent replication snapshot copy of the VM becomes the working VM.
2. On the source cluster, unprotect the VM on the source cluster. This includes removing it from protection groups.
3. Configure replication protection for the VM from the new source (formerly target) cluster.
4. Remove the VM from the original source cluster.

---

**Migrating Protected Virtual Machines**

Migration removes the ownership of VMs from the source cluster to the target cluster.

On the target cluster, perform the following to migrate the virtual machine from the source cluster to the target cluster.

**Before you begin**
- The target cluster is up and in good health.
- The protected virtual machines completed a recent replication to the target cluster. These replicated virtual machines are stored as snapshots on the target clusters.

**Step 1**
Login to the controller VM of a node in the target cluster.
The target cluster where the replication snapshots were copied to. The source cluster was the cluster where the virtual machines resided.
Step 2  Identify the virtual machines to migrate. Run the command.

```bash
# stcli dp vm list --brief
```

This command lists the VMs unique identifier, the BIOS UUID.

Step 3  Stop any potential replication from the source cluster to the target cluster. Run the command on the target cluster.

```bash
# stcli dp vm halt
```

```bash
stcli dp vm halt [-h] --vmid VMID [--force]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--vmid VMID</td>
<td>Required.</td>
<td>Run command on the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td></td>
<td>--force</td>
<td>Optional.</td>
<td>Do not validate the arguments and perform recovery</td>
</tr>
</tbody>
</table>

Step 4  If both the target and source clusters are on the same vCenter, the unregister the VM on the source cluster.

This ensures that vCenter no longer has a record of the VM, but it retains the data for the VM. vCenter stops managing the VM.

Step 5  Perform the migration. Run the command.

```bash
# stcli dp vm recover failover
```

- Provide any optional parameters, such as `folder`, `resourcepool`, `newname`, `poweron`, `test-network` or `network-mapping` to customize the test recovery.

- This command returns the `job-id`. Use the `job-id` to monitor the recovery status.

```bash
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--vmid VMID</td>
<td>Required.</td>
<td>Run command on the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td></td>
<td>--resourcepool-id RESOURCEPOOL-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed ID.</td>
</tr>
<tr>
<td></td>
<td>--resourcepool-name RESOURCEPOOL-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed name.</td>
</tr>
<tr>
<td></td>
<td>--folder-id FOLDER-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed ID.</td>
</tr>
<tr>
<td></td>
<td>--folder-name FOLDER-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed name.</td>
</tr>
</tbody>
</table>
### Migrating Virtual Machines in Protection Groups

Migration removes the ownership of VMs from the source cluster to the target cluster.

On the target cluster, perform the following to migrate the virtual machine from the source cluster to the target cluster.

**Before you begin**

- The target cluster is up and in good health.
- The protected virtual machines completed a recent replication to the target cluster. These replicated virtual machines are stored as snapshots on the target clusters.

**Step 1**

Login to the controller VM of a node in the target cluster.

The target cluster where the replication snapshots were copied to. The source cluster was the cluster where the virtual machines resided.

**Step 2**

Identify the virtual machines to migrate. Run the command.

```bash
# stcli dp group list --brief
```
This command lists the VMs unique identifier, the BIOS UUID.

**Step 3**
Stop any potential replication from the source cluster to the target cluster. Run the command on the target cluster.

```
# stcli dp group halt
```

```
stcli dp group halt [-h] --groupid GROUPID [--force]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>--groupid GROUPID</code></td>
<td>Required.</td>
<td>Halt replication of the virtual machines in the protection group with the listed groupid.</td>
</tr>
<tr>
<td></td>
<td><code>--force</code></td>
<td>Optional.</td>
<td>Halt replication without validating the arguments.</td>
</tr>
</tbody>
</table>

**Step 4**
If both the target and source clusters are on the same vCenter, the unregister the VM on the source cluster. This ensures that vCenter no longer has a record of the VM, but it retains the data for the VM. vCenter stops managing the VM.

**Step 5**
Perform the migration. Run the command.

```
# stcli dp vm recover failover
```

- Provide any optional parameters, such as `folder`, `resourcepool`, `newname`, `poweron`, `test-network` or `network-mapping` to customize the test recovery.
- This command returns the job-id. Use the job-id to monitor the recovery status.

```
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>--vmid VMID</code></td>
<td>Required.</td>
<td>Run command on the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td></td>
<td><code>--resourcepool-id RESOURCEPOOL-ID</code></td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed ID.</td>
</tr>
<tr>
<td></td>
<td><code>--resourcepool-name RESOURCEPOOL-NAME</code></td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed name.</td>
</tr>
<tr>
<td></td>
<td><code>--folder-id FOLDER-ID</code></td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed ID.</td>
</tr>
<tr>
<td></td>
<td><code>--folder-name FOLDER-NAME</code></td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed name.</td>
</tr>
</tbody>
</table>
**Data Protection Recovery Workflow**

Disaster recovery is performed when the source site is unreachable and you want to failover the VMs and protected groups to the target cluster. The process of failover shifts the primary cluster association for the VMs from the source to the target cluster. Once the VMs and protected groups are recovered, replication protection can be configured again with a newer cluster.

Recovering virtual machines is restoring a most recent replication snapshot from the recovery (target) cluster using the `stcli dp vm` commands.

The recovery process, to distinguish from a migration process, involves removing (forget) the pairing between the source and target cluster, so the new source (formerly target) cluster can form a replication pair with a new cluster.
The recovery process is used in the event of a disaster, when you do not expect the original source site to return. Once `forget` is applied, applying protection to the VMs requires the full pairing and protecting process.

**Recovery**

Used after a disaster. In a recovery, similar to migration, a recent replication snapshot copy of the VM becomes the working VM. Dissimilar to migration, the paring between the original source and target cluster is removed (forgotten). Allowing for the new source (formerly target) cluster to pair with another cluster. This requires:

1. Generate a list of protected VMs and protection groups.
2. Halt any replication activity. Run the command on the target cluster.
   - This ensures no partial or corrupt VMs are used to create a newer replication snapshot.
3. Recover failover of the VMs, from VM replication snapshot to working VM.
5. Verify the recovered VM contents.
6. Repeat Step 3 through Step 5 as needed to recover all VMs.
7. If the task is recovering from a disaster, remove (`forget`) the replication pair configuration.
   - This removes the datastore and cluster pairing between the original source and target clusters, and allows the new source (formerly target) cluster to pair with another healthy cluster.

**Note**

This command is used in the event of a disaster only, when you do not expect the original source site to return. Once `forget` is applied, applying protection to the VMs requires the full pairing and protecting process.

8. Unprotect the VMs and delete protection groups.
9. Pair the new source (formerly target) cluster with a new cluster and reprotect the VMs, individually or in a protection group.

**Testing Virtual Machine Recovery**

Virtual machine and data recovery is through the `stcli dp vm` command. To test if the recovery methods are working. All test recovery commands are run on the target cluster only.

**Note**

Testing recovery does not disrupt the running clusters. The intent is to verify, in the event of an actual disaster, that the VMs are recoverable.

**Before you begin**

The target cluster is up and in good health.
The protected virtual machines completed a recent replication to the target cluster. These replicated virtual machines are stored as snapshots on the target clusters.

**Step 1**
Login to the controller VM of a node in the recovery cluster.

The recovery cluster is the target cluster where the replication snapshots were copied to. The source cluster was the cluster where the virtual machines resided.

**Step 2**
Identify the virtual machines to recover. Run the command.

```
# stcli dp vm list --brief
```

This command lists the VMs unique identifier, the BIOS UUID.

**Step 3**
Perform the recovery test. Run the command.

```
# stcli dp vm recover test
```

- This command returns a job-id.
- By default test recovery recovers the VM and places the recovered VM, using the same name, in the HxTestRecovery folder.

```
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vmid VMID</td>
<td>Required.</td>
<td>Lists the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td>--resourcepool-id RESOURCEPOOL-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed ID.</td>
</tr>
<tr>
<td>--resourcepool-name RESOURCEPOOL-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed name.</td>
</tr>
<tr>
<td>--folder-id FOLDER-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed ID.</td>
</tr>
<tr>
<td>--folder-name FOLDER-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed name.</td>
</tr>
<tr>
<td>--test-network TESTNETWORK</td>
<td>Optional.</td>
<td>Test network to be used for test recovery. All source networks are assigned to this network after recovery.</td>
</tr>
</tbody>
</table>
| --network-mapping NETWORKMAPPING [NETWORKMAPPING ...] | Optional. | Map the source to destination network. Format source_network:destination_network. For example: 
  --network-mapping 
  "source network1:destination network1", "source network2:destination network2" |
Recovering Virtual Machines

Recovering virtual machines is restoring a most recent replication snapshot from the target (recovery) cluster using the `stcli dp vm` commands.

The recovery process, to distinguish from a migration process, involves removing (forget) the pairing between the source and target cluster.

**Note**

When running recovery on virtual machines that are individually protected, or that are in different protection groups, the maximum number of concurrent recovery operations on a cluster is 20.

**Before you begin**

- The target cluster is up and in good health.
- The protected virtual machines completed a recent replication to the target cluster. These replicated virtual machines are stored as snapshots on the target clusters.

On the target cluster, perform the following to do disaster recovery.

**Step 1**

Login to the controller VM of a node in the target (recovery) cluster.

The recovery cluster is the target cluster where the replication snapshots were copied to. The source cluster was the cluster where the virtual machines resided.

**Step 2**

Identify the virtual machines to recover. Run the command on the target cluster.

```
# stcli dp vm list --brief
```

This command lists the VMs unique identifier, the BIOS UUID.

**Step 3**

Stop any potential replication from the source cluster to the target cluster. Run the command on the target cluster.

```
# stcli dp vm halt
```
stcli dp vm halt [-h] --vmid VMID [--force]

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vmid VMID</td>
<td>Required.</td>
<td>Run command on the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td>--force</td>
<td>Optional.</td>
<td>Do not validate the arguments and perform recovery.</td>
</tr>
</tbody>
</table>

#### Step 4
Perform the recovery. Run the command on the target cluster.

```bash
# stcli dp vm recover failover --vmid VMID
```

- Provide any optional parameters, such as `folder`, `resourcepool`, `newname`, `poweron`, `test-network` or `network-mapping` to customize the test recovery.

- This command returns the `job-id`. Use the `job-id` to monitor the recovery status.


### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vmid VMID</td>
<td>Required.</td>
<td>Run command on the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td>--resourcepool-id RESOURCEPOOL-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed ID.</td>
</tr>
<tr>
<td>--resourcepool-name RESOURCEPOOL-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed name.</td>
</tr>
<tr>
<td>--folder-id FOLDER-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed ID.</td>
</tr>
<tr>
<td>--folder-name FOLDER-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed name.</td>
</tr>
</tbody>
</table>
| --network-mapping NETWORKMAPPING [NETWORKMAPPING ...] | Optional. | Map the source to destination network. Format `source_network:destination_network`. For example:
  ```bash
  --network-mapping
  "source_network1:destination_network1","source_network2:destination_network2"
  ```
| --poweron                      | Optional.            | Power on the VM after recovery.                                            |
| --force                        | Optional.            | Do not validate the arguments and perform recovery.                        |

#### Step 5
Monitor the status of the job, referencing the `job-id` from the previous command. Run the command on the target cluster.

```bash
# stcli dp vm recover status --id <job-id> --list
```
Step 6 Verify the contents of the recovered VM on the target cluster.

If the `--poweron` option was used and the virtual machine does not automatically power on, power on the virtual machine through vCenter.

Step 7 Remove (forget) the replication pair configuration. Run the command on a single controller VM in the target cluster.

**Note** This command is used in the event of a disaster, when you do not expect the original source site to return. Once forget is applied, applying protection to the VMs requires the full pairing and protecting process.

```
# stcli dp peer forget
```

- Ensure the replication network is up and running as originally configured for replication. Do not run this on all the controller VMs simultaneously.
- This removes the datastore and cluster pairing between the original source and target clusters, and allows the new source (formerly target) cluster to pair with another healthy cluster.
- Repeat this step on the original source cluster, if it returns from failed state.

```
stcli dp peer forget [-h] [--name NAME] [--all]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--all</td>
<td>One of set required.</td>
<td>Remove the pairing between peers, for all partially-paired and successfully paired clusters.</td>
</tr>
<tr>
<td></td>
<td>--name NAME</td>
<td>One of set required.</td>
<td>Remove the pairing between peers, (the source and target clusters), for the cluster pair with the listed name.</td>
</tr>
</tbody>
</table>

Step 8 Unprotect the virtual machines. Run the command on the target cluster.

```
# stcli dp vm delete --vmid VMID
```

Alternatively, use HX Connect to unprotect the virtual machines.

Step 9 Pair the target cluster with a new cluster. Then re-apply protection on the virtual machines, individually or through protection groups.

---

**Recovering Virtual Machines in Protection Groups**

Recovering virtual machines is restoring a most recent replication snapshot from the target (recovery) cluster using the `stcli dp group` commands.
The recovery process, to distinguish from a migration process, involves removing (forget) the pairing between the source and target cluster.

**Note**

When running recovery on virtual machines in the same protection group, run the recovery command on one virtual machine one at a time, and not in parallel. This is a serial operation. Parallel recovery on virtual machines within the same protection group is not supported.

**Before you begin**

- The target cluster is up and in good health.
- The protected virtual machines completed a recent replication to the target cluster. These replicated virtual machines are stored as snapshots on the target clusters.

On the target cluster, perform the following to migrate the virtual machine from the source cluster to the target cluster.

**Step 1**

Login to the controller VM of a node in the target (recovery) cluster.

The recovery cluster is the target cluster where the replication snapshots were copied to. The source cluster was the cluster where the virtual machines resided.

**Step 2**

Identify the virtual machines to migrate. Run the command on the target cluster.

```
# stcli dp group list --brief
```

This command lists the VMs unique identifier, the BIOS UUID.

**Step 3**

Stop any potential replication to the target cluster from the source cluster. Run the command on the target cluster.

```
# stcli dp group halt
```

```
stcli dp group halt [-h] --groupid GROUPID [--force]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--groupid GROUPID</td>
<td>Required.</td>
<td>Halt replication of the virtual machines in the protection group with the listed groupid.</td>
</tr>
<tr>
<td></td>
<td>--force</td>
<td>Optional.</td>
<td>Halt replication without validating the arguments.</td>
</tr>
</tbody>
</table>

**Step 4**

Perform the recovery. Run the command on the target cluster.

```
# stcli dp vm recover failover
```

This command returns the job-id. Use the job-id to monitor the recovery status.

```
```
### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vmid VMID</td>
<td>Required.</td>
<td>Run command on the virtual machine that matches the specified BIOS UUID.</td>
</tr>
<tr>
<td>--resourcepool-id</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed ID.</td>
</tr>
<tr>
<td>RESOURCEPOOL-ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--resourcepool-name</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) on the resource pool with the listed name.</td>
</tr>
<tr>
<td>RESOURCEPOOL-NAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--folder-id FOLDER-ID</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed ID.</td>
</tr>
<tr>
<td>FOLDER-ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--folder-name FOLDER-NAME</td>
<td>One of optional pair.</td>
<td>Place the recovered VM(s) in the folder with the listed name.</td>
</tr>
<tr>
<td>--network-mapping</td>
<td>Optional.</td>
<td>Map the source to destination network. Format source_network:destination_network. For example:</td>
</tr>
<tr>
<td>NETWORKMAPPING</td>
<td></td>
<td>--network-mapping</td>
</tr>
<tr>
<td>[NETWORKMAPPING ...]</td>
<td></td>
<td>&quot;source_network1:destination_network1&quot;,&quot;source_network2:destination_network2&quot;</td>
</tr>
<tr>
<td>--poweron</td>
<td>Optional.</td>
<td>Power on the VM after recovery</td>
</tr>
<tr>
<td>--force</td>
<td>Optional.</td>
<td>Do not validate the arguments and perform recovery</td>
</tr>
</tbody>
</table>

### Step 5

Monitor the status of the job, referencing the `job-id` from the previous command. Run the command on the target cluster.

```
# stcli dp vm recover status --id <job-id> --list
```

**Summary:**
- **Step state:** SUCCEEDED
- **Description:** Successfully completed Failover recovery for VMID 564d3432-d4fd-5cdc-b742-b3cfad73144c
- **time_submitted:** 08/31/17_23:07
- **time_elapsed_millis:** 588097052
- **Jobid:** ebf813ff-a91a-40b2-a6dd-51564c8092c0
- **state:** COMPLETED
- **Message:** Performing Failover recovery for VMID 564d3432-d4fd-5cdc-b742-b3cfad73144c
- **time_started:** 08/31/17_23:07

### Step 6

For every VM in the protection group, repeat Step 4 and Step 5.

### Step 7

Verify the contents of the recovered VM on the target cluster.

If the `--poweron` option was used and the virtual machine does not automatically power on, power on the virtual machine through vCenter.

### Step 8

Remove (forget) the replication pair configuration. Run the command on a single controller VM in the target cluster.

**Note:** This command is used in the event of a disaster, when you do not expect the original source site to return.

Once forget is applied, applying protection to the VMs requires the full pairing and protecting process.

```
# stcli dp peer forget
```

- Ensure the replication network is up and running as originally configured for replication. Do not run this on all the controller VMs simultaneously.
This removes the datastore and cluster pairing between the original source and target clusters, and allows the new source (formerly target) cluster to pair with another healthy cluster.

Repeat this step on the original source cluster, if it returns from failed state.

```bash
stcli dp peer forget [-h] [--name NAME] [--all]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Option</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--all</td>
<td>One of set required.</td>
<td>Remove the pairing between peers, for all partially-paired and successfully paired clusters.</td>
</tr>
<tr>
<td></td>
<td>--name NAME</td>
<td>One of set required.</td>
<td>Remove the pairing between peers, (the source and target clusters), for the cluster pair with the listed name.</td>
</tr>
</tbody>
</table>

**Step 9**

Delete the protection group. Run the command on the target cluster.

```bash
# stcli dp group delete --groupid GROUPID
```

Alternatively, use HX Connect to delete the protection group.

**Step 10**

Pair the target cluster with a new cluster. Then re-apply protection on the virtual machines, individually or protection through groups.

---

**Replication Maintenance Overview**

Replication, when configured, runs in the background per the defined schedule. Replication maintenance tasks include:

- **Testing recovery**—Testing if the recovery methods are working.
  
  Use the `stcli dp vm recover test` command.

- **Pausing replication**—When you are preparing to do maintenance on the HX Storage Cluster and you have replication configured, you need to pause the replication activity.

  HX Storage Cluster maintenance activities include adding or rebooting a node, or upgrading the HX Storage Cluster. Typically, when the HX Cluster requires a node to enter HX maintenance mode, pause and resume replication.

  Use the `stcli dp schedule pause` command.

- **Resuming replication**—After HX Storage Cluster maintenance activities are complete, resume the replication schedule.

  Use the `stcli dp schedule resume` command.

- **Migration**—The option to shift VMs from one source cluster to the replication paired target cluster, making the target cluster the new source cluster for the migrated VMs.

  Use the `stcli dp vm recover failover` command.
Migration

Used at anytime, for routine system maintenance and management, that is not a disaster. In a migration, similar to recovery, a recent replication snapshot copy of the VM becomes the working VM. The pairing between the source and target cluster remains. This requires:

1. Generating a list of protected VMs.
   ```
   # stcli dp vm list --brief
   ```
2. Halt any replication activity on the source cluster.
   ```
   # stcli dp vm halt
   ```
   This ensures no partial or corrupt VMs are used to create a newer replication snapshot.
3. Recover failover of the VMs, from replication VM to working VM.
   ```
   # stcli dp vm recover failover --vmid VMID
   ```
   This performs the process of changing the replication snapshot copies on the target cluster into the working VMs.
   The cluster replication pair remains in tact. The forget peer is not used.
   ```
   # stcli dp vm recover status --id JOB-ID
   ```
5. Verifying the recovered VM contents.

Recovery Test

A maintenance task that ensures the recovery process would be successful in the event of a disaster. This requires.

1. Generating a list of protected VMs.
   ```
   # stcli dp vm list --brief
   ```
2. Recover test on each protected VM.
   ```
   # stcli dp vm recover test
   ```
   ```
   # stcli dp vm recover status --id JOB-ID
   ```
4. Verifying the recovered VM contents.

Pausing Replication

When you are preparing to do maintenance on the HX Storage Cluster and you have replication configured, you need to pause the replication activity.

HX Storage Cluster maintenance activities include adding or rebooting a node, or upgrading the HX Storage Cluster. Typically, when the HX Cluster requires a node to enter HX maintenance mode, pause and resume replication.

Step 1
Login to a Storage Controller VM.
Step 2  From the command line, run the `stcli dp schedule pause` command.

Step 3  Perform your maintenance or upgrade tasks.

---

**What to do next**

Proceed to complete the maintenance or upgrade tasks. The resume the replication schedule.

---

**Resuming Replication**

When you are preparing to do maintenance on the HX Storage Cluster and you have replication configured, you need to pause the replication activity.

HX Storage Cluster maintenance activities include adding or rebooting a node, or upgrading the HX Storage Cluster. Typically, when the HX Cluster requires a node to enter HX maintenance mode, pause and resume replication.

After the activities are complete, resume the replication schedule.

**Before you begin**

Ensure your HX Storage Cluster is paused and you have completed your maintenance or upgrade tasks.

---

Step 1  Login to a Storage Controller VM.

Step 2  From the command line, run the `stcli dp schedule resume` command.

---

The previously configured replication schedule for all the protected virtual machines begins.
Managing Users

• Managing HyperFlex Users Overview, on page 173
• Creating HX Data Platform RBAC Users, on page 175
• Assigning Users Privileges, on page 176

Managing HyperFlex Users Overview

The user types allowed to perform actions on or view content in the HX Data Platform, include:

• admin——A predefined user included with HX Data Platform. The password is set during HX Cluster creation. Same password is applied to root. This user has read and modify permissions.

• root——A predefined user included with HX Data Platform. The password is set during HX Cluster creation. Same password is applied to admin. This user has read and modify permissions.

• administrator——A created HX Data Platform user. This user is created through vCenter and assigned the RBAC role, administrator. This user has read and modify permissions. The password is set during user creation.

• read-only——A created HX Data Platform user. This user is created through vCenter and assigned the RBAC role, read-only. This user only has read permissions. The password is set during user creation.

<table>
<thead>
<tr>
<th>HX Interface</th>
<th>admin</th>
<th>root</th>
<th>hx_admin</th>
<th>hx_readonly</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Data Platform Installer</td>
<td>Required</td>
<td>Optional</td>
<td>Not valid</td>
<td>Not valid</td>
</tr>
<tr>
<td>HX Interface</td>
<td>admin</td>
<td>root</td>
<td>hx_admin</td>
<td>hx_readonly</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Storage Controller</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can only run non-interactive</td>
</tr>
<tr>
<td>VM with stcli command line</td>
<td></td>
<td></td>
<td></td>
<td>stcli commands to view status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cannot perform HX tasks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vc- prefix required for login.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example: vc-hx_admin</td>
</tr>
<tr>
<td>vCenter</td>
<td></td>
<td></td>
<td></td>
<td>Cannot view HX Data Platform</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Plug-in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A vCenter SSO user.</td>
</tr>
<tr>
<td>HX REST API</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can perform most HX tasks.</td>
<td>Can only run status level REST</td>
</tr>
<tr>
<td></td>
<td>local/ prefix required for login.</td>
<td>local/ prefix required for login.</td>
<td>vc- prefix required for login.</td>
<td>APIs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Example:</td>
<td>Example:</td>
<td>Cannot perform HX tasks.</td>
</tr>
<tr>
<td></td>
<td>local/admin</td>
<td>local/root</td>
<td>vc-hx_admin</td>
<td>vc- prefix required for login.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example: vc-hx_readonly</td>
</tr>
</tbody>
</table>

User Management Terms

- **Authentication**—For login credentials. These processes verify user credentials for a named user, usually based on a username and password. Authentication generally verifies user credentials and associates a session with the authenticated user.

- **Authorization**—For access permissions. These processes allow a user/client application to perform some action, such as create, read, update, or delete a managed entity or execute a program, based on the user's identity. Authorization defines what an authenticated user is allowed to do on the server.

- **Accounting**—For tracking user actions. These processes perform record-keeping and track user activities including login sessions and command executions. The information is stored in logs. These logs are included in the support bundle that can be generated through HX Connect or other HX Data Platform interface.

- **Identity**—Individuals are provisioned with identities that are assigned roles with granted permissions.

- **Permission**—Settings given to roles to use the Resource. It is the link between roles, resource and the function exposed by the resource. For example, Datastore is a resource and a modifying role is granted permission to mount the datastore, while a read only role can only view that the datastore exists.
Privilege—The link between Identity and the application. It is used in the context of specific interaction with the application. Examples: Power On a Virtual Machine, Create a Datastore, Rename a datastore and so on.

Resource—The entire HX Platform, whose functionality and management controls are exposed over HTTP using GET, POST, PUT, DELETE, HEAD and other HTTP verbs. Datastores, Disks, Controller Nodes, Cluster Attributes, are all resources that are exposed to client applications using REST API.

Role—Defines an authority level. An application function may be performed by one or more roles. Examples: Administrator, Virtual Machine Administrator, Resource Pool Administrator etc. Role is assigned to a given Identity.

Audit Logs for AAA Accounting

To support AAA accounting, HX Data Platform implements audit logs of user activity. These logs are included in the generated support bundle.

See the Cisco HyperFlex Systems Troubleshooting Guide for information on generating the support bundles through HX Data Platform interfaces, including HX Connect.

• stMgrAudit.log—Contains audit records of stcli activity.
  
  Sample entry. Note the keyword, Audit.
  
  2017-03-27-22:10:02.528 [pool-1-thread-1] INFO Audit - 2017-03-27-03.10.02 127.0.0.1 --> 127.0.0.1 POST /stmgr 200 : root 27ms

  This file contains other information as well. To filter for audit events, use a script to filter for the word, Audit.

• audit.log—Contains audit records for REST API activity.
  
  Sample entry. Note the user name, administrator@vsphere.local
  
  2017-03-29-01:47:28.779 - 127.0.0.1 -> 127.0.0.1 - GET /rest/clusters 200; administrator@vsphere.local 454ms

Creating HX Data Platform RBAC Users

HX Data Platform supports two users: Administrator and Read Only. New users are created for the HX Data Platform through the VMware vCenter interface.

Before you begin

Creating users requires Administrator privileges.

| Step 1 | Login to vSphere Web Client as a vCenter administrator. |
| Step 2 | From Navigator Home, Administration > Users and Groups > Users. |
| Step 3 | Click Add (+) icon to add a user. Then complete the New User information and click OK. |

Specify a user name and password for the new user.
For passwords, do not use escape character (\), dollar sign ($), question mark (?), equal sign (=). In user names, the only special characters allowed are underscore (_), dash (-), dot (.). See HX Data Platform Names, Passwords, and Characters, on page 21 for user name and password requirements.

What to do next
Add the user to an RBAC role group. See Assigning Users Privileges, on page 176.

Assigning Users Privileges
Privileges are assigned to users through the RBAC roles in vCenter. To assign privileges, add users to either the Administrator or Read-only group.

Before you begin
Create the user.

Step 1  From vSphere Web Client, select Navigator Home > Administration > Global Permissions > Manage.
Step 2  Click Add (+) icon to assign roles.
Step 3  Select an Assigned Role.
        In the Global Permission Root - Add Permission dialog box, select from the Assigned Role drop down menu. Choose one:
        • Administrator
        • Read only
Step 4  In the Users and Groups area, click Add.
Step 5  In the Select Users/Groups dialog box, select the user_name and click Add.
Step 6  Click Check names button, to verify the user name.
Step 7  Then click OK to close out of each dialog box.