Cisco HyperFlex Data Platform Administration Guide, Release 3.0

First Published: 2018-04-24

Last Modified: 2020-02-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Full Cisco Trademarks with Software License

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 6

CHAPTER 7

CHAPTER 8

CHAPTER 1

HX Storage Cluster Overview

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, ESXi servers, and vCenter; and the Cisco HX 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, after specifying 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 to 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 HyperFlex 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 HX 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.

  Run the *Cluster Expansion* workflow from the HX Data Platform Installer to add converged nodes to your storage cluster. You can remove converged nodes using *stcli* commands.

- **Compute nodes**—Compute nodes add compute resource but not storage capacity to the storage cluster. They are used as a 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 in a HX 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.

  Run the *Cluster Expansion* workflow from the HX Data Platform Installer to add compute nodes to your storage cluster. You can remove compute nodes using *stcli* commands.

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

  Adding HDD to existing converged nodes, also adds storage capacity to the storage cluster. When storage is added to a HX 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 resources.

  Adding or removing disks on your converged nodes is not performed through the HX Data Platform. Before 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.

  Datastores are logical containers that are 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.

HX Data Platform Capacity Overview

Note Capacity addition in a cluster through the addition of disks or nodes can result in a rebalance. This background activity can cause interference with regular User IO on the cluster and increase the latency. You must note the time duration for the storage capacity at the time where performance impact can be tolerated. Also, this operation may be performed in urgent situations that may warrant capacity addition.

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**.
- **Available 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 and 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 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

   ```
   = (1 - TUUS/TAS) * 100
   ```

   ```
   = (1 - 100GB / 200GB) *100
   ```

   ```
   = 50%
   ```

3. Compression Savings

```
= (1 - TUB/TUUS) * 100

= (1 - 25GB / 100GB) * 100

= 75%
```

4. Total savings calculated

```
= (1 - TUB/TAS) * 100

= (1 - 25GB / 200GB) * 100

= 87.5%
```

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 to 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.

Note **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 an 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 an 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 the following 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. Describes how well the storage cluster can perform operations.
- **Resiliency Status**—Describes the ability of the storage clusters to tolerate node failures within the storage cluster. Describes how well the storage cluster can handle disruptions.

The following settings take effect 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 HX 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**—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 of 3 is recommended.

- **Access Policy**—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

Replication Factor	Access Policy	Number of Failed Nodes		
		Read/Write	Read-Only	Shutdown
3	Lenient	2	--	3

Replication Factor	Access Policy	Number of Failed Nodes		
		Read/Write	Read-Only	Shutdown
3	Strict	1	2	3
2	Lenient	1	--	2
2	Strict	--	1	2

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

Replication Factor	Access Policy	Number of Failed Nodes		
		Read/Write	Read-Only	Shutdown
3	Lenient or Strict	1	--	2
2	Lenient	1	--	2
2	Strict	--	1	2

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

Replication Factor	Access Policy	Failed Disks on Number of Different Nodes		
		Read/Write	Read Only	Shutdown
3	Lenient	2	--	3
3	Strict	1	2	3
2	Lenient	1	--	2

Replication Factor	Access Policy	Failed Disks on Number of Different Nodes		
		Read/Write	Read Only	Shutdown
2	Strict	--	1	2

Data Replication Factor Settings

Note 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 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.

Cluster Size	Number of Simultaneous Failures	Entity Failed	Maintenance Action to Take
3 nodes	1	One node.	The storage cluster does not automatically heal. Replace the failed node to restore storage cluster health.

Cluster Size	Number of Simultaneous Failures	Entity Failed	Maintenance Action to Take
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

Cluster Size	Number of Simultaneous Failures	Entity Failed	Maintenance Action to Take
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.

Cluster Size	Number of Simultaneous Failures	Entity Failed	Maintenance Action to Take
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 Ready Clones Overview

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

A Ready Clone, 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 Ready Clone is a separate guest VM.

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

Installing a guest operating system and applications can be time consuming. With Ready Clone, 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 is 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 can revert to the saved state.

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 2

Logging in to HX Data Platform Interfaces

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, and VM ready clones.
- 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, deploying and expanding HX Storage Cluster cluster, deploying stretched cluster, and deploying Hyper-V clusters.
- 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.

When a user attempts to login with wrong credentials for 10 successive times, the account will be locked for two minutes. If the failed login attempts were made through SSH, the error message will not indicate that the account is locked. If the failed login attempts were made through HX Connect or REST API, the error message during the 10th attempt will indicate that the account is locked.

Component	Permission Level	Username	Password	Notes
HX Data Platform OVA	root	root	Cisco123 **Important** Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.	

Component	Permission Level	Username	Password	Notes
HX Data Platform Installer VM	root	root	Cisco123 **Important** Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.	
HX Connect	administrator or read-only	User defined through vCenter.	User defined through vCenter.	
		Predefined `admin` or `root` users.	As specified during HX installation.	
HX Storage Controller VM	root	User defined during HX installation. User defined through vCenter. Predefined `admin` or `root` users.	As specified during HX installation. Strong password required.	Must match across all nodes in storage cluster. Use the `stcli` command when changing the password after installation.
vCenter	admin	administrator@vsphere.local default. SSO enabled. As configured, MYDOMAIN\name or name@mydomain.com	SSO enabled. As configured.	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.
ESXi Server	root	SSO enabled. As configured.	SSO enabled. As configured.	Must match across all ESX servers in storage cluster.

Component	Permission Level	Username	Password	Notes
Hypervisor	root	root	As specified during HX installation.	Use vCenter or `esxcli` command when changing the password after HX installation.
UCS Manager	admin	As configured.	As configured.	
Fabric Interconnect	admin	As configured.	As configured.	

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!'. It is not required to place passwords within single quotes in the HyperFlex Installer password form field.

HX Storage Cluster Name

HX cluster names cannot exceed 50 characters.

HX Storage Cluster Host Names

HX cluster host names cannot exceed 80 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 80 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 ($), dot (.), double quotation ("), equal sign (=), 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 (_)

Username Requirements

Usernames can be specific to the HX Data Platform component and must meet UCS Manager username requirements.

UCS Manager username requirements.

- Number of characters: between 6 and 32 characters
- Must be unique within Cisco UCS Manager.
- 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]

   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 ESX 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.

  XhUwPcNu - 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, å, ø, ü, ö, œ, 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

Important

- 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.
- 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.

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 username format is: `<name>@domain.local` and specified in the User Principal Name Format (UPN). For example, `administrator@vsphere.local`. Do not add a prefix such as "ad:" to the username.

- **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.

You may login to the HX Data Platform command line interface in the Storage Controller VM in the following ways:

- 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.

a. Select a **VM** > **Summary** > **DNS Name**.

b. From vSphere Web Client **Home** > **VMs and Templates** > **vCenter server** > ***datacenter*** > **ESX Agents** > **VVM**.

c. 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.

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.
```

```
ECDSA key fingerprint is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx.
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—Log in to HX Connect, select **Web CLI**.

Note Only non-interactive commands can be executed from the HX Connect Web CLI.

Changing Storage Controller Password

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

Step 1 Log in to a storage controller VM.

Step 2 Change the Cisco HyperFlex storage controller password.

```
# stcli security password set
```

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

Note If you add new compute nodes and try to reset the cluster password using the **`scli security password set`** command, the converged nodes get updated, but the compute nodes may still have the default password. To change the compute node password, use the following procedure.

To change the password on compute nodes:

a. Vmotion all the user VMs off the ESXi hosts.

b. Launch the storage controller VM console from vCenter and log in as the root user.

c. Run the **`passwd`** command to change the password.

d. Log out and re-login to confirm that the password changed successfully.

e. Run the **`stcli node add -f`** command to add the node back into the cluster.

Step 3 Type in the new password.

Step 4 Press **Enter**.

Logging Into 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 ESXi 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 is 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 Enter the following credentials:

- **Username**: *root*
- **Password** (Default): Cisco123

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

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 The HX Data Platform Installer Workflow page provides two options to navigate further.

- **Create Cluster** drop-down list—You can deploy a standard cluster,Stretched Cluster, or a Hyper-V cluster.
- **Cluster Expansion**—You can provide the data to add converged nodes and compute nodes to an existing standard storage cluster.

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/docs/ucs-dev-center-hyperflex/.

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

Accessing the Cisco HX Data Platform Plug-in

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

Note

- HX Data Platform Plug-in works with non-English vCenter for Japanese, Korean, and Simplified Chinese languages.
- If you are using the Firefox browser, ensure that 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.
- Use the latest Java version to access the HX Data Platform Plug-in.
- The HX Data Platform Plug-in is not displayed in the vCenter HTML client. You must use the vCenter flash client.

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.

Tab Option	Description
Getting Started	Read introductory information and access basic actions.
Summary	Monitor basic status and configuration for HX Data Platform storage objects.
Monitor	Monitor HX storage cluster, host, and datastore performance and events.
Manage	Monitor HX storage cluster details, create and manage datastores, copy and export information.

CHAPTER 3

Monitoring HX Storage Clusters

Monitoring HyperFlex Clusters

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

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

Monitoring HyperFlex Clusters with HX Connect

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

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

- **Dashboard**—Overall Cisco 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 51 for entering and exiting maintenance mode, and Setting a Beacon, on page 53 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 Cisco 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

Important If you are a read-only user, you may not see all of the options available in the Help. To perform most actions in HyperFlex (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.

UI Element	Essential Information
Operational Status section	Provides the functional status of the HX storage cluster and application performance. Click **Information** (ⓘ) to access the HX storage cluster name and status data.
Cluster License Status section	Displays the following link when you log into the HX storage cluster for the first time or till the HX storage cluster license is registered: **Cluster License not registered** link—Appears when the HX storage cluster is not registered. To register a cluster license, click this link and provide product instance registration token in the **Smart Software Licensing Product Registration** screen. For more information on how to get a product instance registration token, refer the **Registering a Cluster with Smart Licensing** section in the Cisco HyperFlex Systems Installation Guide for Mircrosoft Hyper-V.
Resiliency Health section	Provides the data health status and ability of the HX storage cluster to tolerate failures. Click **Information** (ⓘ) to access the resiliency status, and replication and failure data.
Capacity section	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.
Nodes section	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.

UI Element	Essential Information
Performance section	Displays an HX storage cluster performance snapshot for a configurable amount of time, showing IOPS, throughput, and latency data. For full details, see **Performance Page**.
Cluster Time field	System date and time for the cluster.

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.

UI Element	Essential Information
Refresh field and icon	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.
Filter field	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.
Export menu	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: `cvs`, `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.

Activity Page

Displays a list of recent activity on the HX storage cluster allowing you to monitor the progress of VM operations, Cluster upgrade/expansion, enter/exit maintenance mode, and recovery jobs.

UI Element	Essential Information
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 list shows the task's step name and status. Click the circular icon to refresh the content and fetch recent activity. The page refreshes automatically every 2 minutes.
Recovery list	Displays progress of all recovery-related jobs (for example, migration, recovery, test recovery, re-protect) including the following details: • ID • Description • Task status: • **In Progress** • **Success** • **Failed** • Date and time stamp • Progress bar An expanded list shows the task's step name and status. Click the circular icon to refresh the content and fetch recent activity. The page refreshes automatically every 2 minutes.
Expand All / Collapse All button	Toggles the view of the job list to display top-level task information or task details. You can also expand and collapse individual tasks.

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.

UI Element	Essential Information
HX storage cluster field	Name of this storage cluster.
Cluster License Status section	Displays the **Register Now** link when you log into the HX storage cluster for the first time or till the HX storage cluster license is registered: **Register Now** link—To register a cluster license, click this link and provide product instance registration token in the **Smart Software Licensing Product Registration** screen. For more information on how to get a product instance registration token, refer the **Registering a Cluster with Smart Licensing** section in the Cisco HyperFlex Systems Installation Guide for VMware ESXi. **Note** To register a cluster license, you can also choose **Register Cluster** from the **Actions** drop-down field.
License section	• **License Type**—Displays Evaluation, Edge, Standard, or Enterprise as the HX storage cluster license type. • **License Status**—Displays one of the following as the HX storage cluster license status: • In compliance • License expires in <n> days. Cluster not registered - Register Now. (This status appears only for Evaluation type license) • License expired. Cluster not registered - Register Now. (This status appears only for Evaluation type license) • Out of compliance - Insufficient license • Authentication expired—This status appears when HX is unable to communicate with Cisco Smart Software Manager or Smart Software Manager satellite for more than 90 days. **Note** To refresh license certificate or renew license authorization, choose the respective options from the **Actions** drop-down field.

UI Element	Essential Information
HX storage cluster status field	Provides functional status of the HX storage cluster. • **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.

Controller VM Access

You can access the controller VM using SSH as an administrator. To enable access, click **Actions** at the top of the page to enable SSH access.

Node Data

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

UI Element	Essential Information
Node	Name of a node on this cluster.
Model	Physical hardware model number of this node.
Disks	Number of caching versus persistent disks in this node.

UI Element	Essential Information
Node status	• **Online** • **Offline** • **In Maintenance** • **Healthy** • **Warning**
HXDP Version	Installer package version installed on this node.
Type	• **Hyper Converged** • **Compute**
Hypervisor Status	• **Online** • **Offline** • **In Maintenance** • **In Progress**
Hypervisor Address	IP address for the management network to this HX storage cluster.

For nodes with disks, you can place your cursor over a disk to view an interactive display of information including the following.

Disks

UI Element	Essential Information
Slot Number	Location of the drive, for example Slot Number 2.
Type of Disk	System, Cache or Persistent
Disk State	• **Claimed** • **Available** • **Ignored** • **Blacklisted** • **Ok to Remove** • **Unknown**
Locator LED	Activates a physical light on the host to help locate a disk; options are **On** and **Off**.
Capacity	Total disk size.

UI Element	Essential Information
Used / Total Capacity (Persistent Disks only)	Amount of the disk used versus the total disk size.
Serial Number	Physical serial number of this disk.
Storage Usage (Persistent Disks only)	Percentage of disk storage used.
Version	Version of the disk drive.
Disk Drive Interface	The disk drive interface type, for example SAS or SATA.

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.

UI Element	Essential Information
Enter HX Maintenance Mode button	Select a node to access this button. Opens the **Confirm HX Maintenance Mode** dialog box.
Exit HX Maintenance Mode button	Select a node to access this button. After you complete any maintenance tasks, you must manually exit HX maintenance mode.
Node column	Name of a node in this HX storage cluster.
Hypervisor Address column	IP address for the management network of the Node referred in the Node column.
Hypervisor Status column	• **Online**—Node is available. • **Offline**—Node is not available. • **In Maintenance**—The running (and powered off) node is Maintenance disconnected from the host. • **In Progress**—a backup job is in progress.
Controller Address column	IP address for the HX storage controller VM of the Node referred in the Node column.
Controller Status column	• **Online**—The connection between the VM and the disk is available. • **Offline**—The connection between the VM and the disk is not available. • **In Maintenance**—the connection between the VM and the disk is powered off from the host.

UI Element	Essential Information
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.

UI Element	Essential Information
Node column	Name of the node where the disk resides.
Slot column	Location of the SED drive. This identifies the drive for maintenance procedures.
Capacity column	Total disk size.

UI Element	Essential Information	
Status column	• **Claimed**—State when a disk is recognized and in use. • **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. • **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. • **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**. • **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.	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**
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**	

UI Element	Essential Information
Type column	• **Unknown** • **Rotational**—Hybrid drive • **Solid State**—SSD drive
Usage column	• **Unknown** • **Cache** • **Persistent**
Turn On Locator LED and **Turn Off Locator LED** radio buttons	Select a disk to access the radio buttons. Activates or deactivates a physical light, or beacon, on the host to help locate the disk.
(Optional) **Secure erase** button	This button in visible only if your HX storage cluster is encrypted using local-key encryption. Select a disk to access the button. 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.

Using the Cisco HX Data Platform Plug-in Interface

There are several Cisco 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 Cisco 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 Cisco HX Data Platform plug-in through the vSphere vCenter Inventory Lists. Select storage clusters to manage from the Cisco HX Data Platform plug-in. The Cisco 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 Cisco HX Data Platform plug-in and vSphere.

Important The Cisco HX Data Platform Plug-in is not compatible with the VMware vSphere vCenter HTML5 interface. You cannot perform HX-related tasks such as HX Maintenance mode using the VMware vSphere vCenter HTML5 interface. Use the vSphere Web Client flash interface instead.

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

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

Note that following a link from either the Cisco 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 Cisco HX Data Platform plug-in monitoring information and managing functions are distributed among three tabs. The following is a list of all the Cisco HX Data Platform plug-in tabs and panels that display Cisco 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 Cisco 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 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

You must use HX Connect or HX Plug-in to view storage capacity and not vCenter.

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 choose 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 choose 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.

Option	Description
IOPS	Input/Output Operations per Second.
Throughput	The rate of data transfer in the storage cluster. Measured in MBps.
Latency	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 milli second.
Current	The most recent data point value for the chart.
Past Hour	A chart of the last hour of data points.

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

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td>Modify the performance charts to display all or some of the listed options.</td><td>
<table>
<tr><th>Customize Item</th><th>Description</th></tr>
<tr><td><b>Time period</b></td><td>Choose from hour, days, week, month, all, or custom. See Specifying Performance Time Period section in this chapter.</td></tr>
<tr><td><b>Cluster objects</b></td><td>Choose from a list of storage clusters, hosts, or datastores.</td></tr>
<tr><td><b>Chart type</b></td><td>Choose from IOPS, Throughput, or Latency.</td></tr>
<tr><td><b>Show objects</b></td><td>Choose which listed object’s data to display. See Selecting Performance Charts section in this chapter.</td></tr>
</table>
</td></tr>
</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.

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

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.

Field	Description
Chart types	Click the check box to select which charts and table columns to view or hide. Options are: • IOPS • Throughput • Latency
Show	For each storage cluster, hosts, and datastores, click the check boxes to select the specific object to include or exclude from the charts.
Read/Write	Indicates the color representation in the chart for the read and write values of each object.
Storage Cluster	Names of the storage clusters in the charts.

Field	Description
Hosts	Names of the hosts in the charts. This includes both converged nodes and compute nodes.
Datastores	Names of the datastores in the charts.
IOPS Read/Write	Latest data point for Input/Output Operations per Second.
Throughput Read/Write (Mbps)	Latest data point for the rate of data transfer in the storage cluster.Measured in Mbps.
Latency Read/Write (msec)	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.

Audit Logging with HX Connect

Audit logging implies storing all audit logs to a remote syslog server. Currently, each controller VM stores audit logs, but these logs are not stored indefinitely. The logs are overwritten based on the retention policy set for the controller VM. By configuring a remote syslog server to store audit logs, you can ensure that the logs are retained for a longer period of time.

Following are the audit logs that you can export to the remote syslog server:

- REST-related logs
    - `/var/log/springpath/audit-rest.log`
    - `/var/log/springpath/hxmanager.log`
    - `/var/log/springpath/hx_device_connector.log`
    - `/var/log/shell.log`
    - `/var/log/springpath/stSSOMgr.log`
    - `/var/log/springpath/stcli.log`
    - `/var/log/springpath/hxcli.log`
- `/var/log/nginx/ssl-access.log`

After you enable audit logging, these logs are exported to the remote syslog server. If the logs from the controller VM are not pushed to the remote sylog server, or if the remote syslog server is not reachable, an alarm is generated in the HX-Connect user interface. However, HX Connect does not monitor the disk space available on the remote syslog server. The HX Connect user interface will not display an alarm if the disk on the remote syslog server is full.

⚠

Attention

- Only an administrator user can enable audit logging.
- Logs from the compute-only nodes and witness nodes are not pushed to the remote syslog server.

After you enable audit logging, you can choose to either temporarily disable audit logging, or you can choose to delete the audit logging server configuration details. See Disabling Audit Logging, on page 49 and Deleting Audit Logging Server Configuration, on page 49.

Enabling Audit Logging

Before you begin

- Configure the remote syslog server. You must have the server details such as the server IP, the port number and certificate files to enable audit logging in HX-Connect.
- To configure an encrypted connection between the controller VM and the remote syslog server, you must generate a self-signed certificate or a CA-signed certificate and a private key for the syslog client in the controller VM.
- Configure the remote syslog server to categorize different types of logs into respective files. See Configuring the Remote Syslog Server, on page 47

Step 1 Choose **Settings** > **Audit Log Export Settings**.

Step 2 Check the **Enable audit log export to an external syslog server** check box.

Step 3 Complete the following details:

UI Element	Essential Information
Syslog Server	Enter the IP address of the syslog server.
Port	Enter the port number for the syslog server.
Connection Type drop-down list	Choose **TLS** or **TCP** as the connection type. The default and recommended value is TLS. The TLS connection type is for encrypted transport over TLS. The TCP connection type is for unencrypted transport over TCP.
Client Certificate	Click **Choose** to search and locate a certificate file that must be stored on the controller VM. This certificate creates a TLS connection between the controller VM and the remote syslog server. A TLS connection ensures that the log files are encrypted. You must upload either a user-generated self-signed certificate or a CA-signed certificate.

UI Element	Essential Information
Private Key	Click **Choose** to search and locate a generated private key file to be stored on the controller VM. This key creates a TLS connection between the controller VM and the remote syslog server. Choosing a certificate and private key for the syslog server ensures that the log files are encrypted. The certificate for the syslog server can either be a CA certificate or a self-signed certificate.
Are you using a self-signed certificate?	Check this check box if the syslog server uses a self-signed certificate. Click **Choose** to search and locate the self-signed certificate for the syslog server.

Step 4 Click **OK**.

Configuring the Remote Syslog Server

Prior to enabling audit logging, you must create a configuration file on the remote syslog server to categorize different log files into separate files. You could create a file titled `hx-audit.conf` in the `/etc/syslog-ng/conf.d` directory.

Following is a sample of the configuration file to establish an encrypted connection with the syslog server:

```
## Audit Logging Configuration ###
    source demo_tls_src {
            tcp(ip(0.0.0.0) port(6515)
                tls(
                     key-file("/etc/syslog-ng/CA/serverkey.pem")
                     cert-file("/etc/syslog-ng/CA/servercert.pem")
                     peer-verify(optional-untrusted)
                )
            ); };


    filter f_audit_rest { match("hx-audit-rest" value("MSGHDR")); };
    filter f_device_conn { match("hx-device-connector" value("MSGHDR")); };
    filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); };
    filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); };
    filter f_hxmanager { match("hx-manager" value("MSGHDR")); };
    filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
    filter f_stcli { match("hx-stcli" value("MSGHDR")); };
    filter f_hxcli { match("hx-cli" value("MSGHDR")); };

    destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
    destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
    destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
    destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
    destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
    destination d_hx_shell { file("/var/log/syslog-ng/shell.log"); };
    destination d_stcli { file("/var/log/syslog-ng/stcli.log"); };
    destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };
```

```
   log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest); flags(final);
 };
    log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn);
flags(final); };
    log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final);
 };
   log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access); flags(final);
 };
   log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager); flags(final);
 };
    log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final);
 };
    log { source(demo_tls_src); filter(f_stcli); destination(d_stcli); flags(final); };
    log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };

########################
```

Following is a sample of the configuration file to establish a TCP connection with the remote syslog server:

```
#######################
## Audit Logging Configuration ###
    source demo_tls_src {
            tcp(ip(0.0.0.0) port(6515)
            ); };

    filter f_audit_rest { match("hx-audit-rest" value("MSGHDR")); };
    filter f_device_conn { match("hx-device-connector" value("MSGHDR")); };
    filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); };
    filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); };
    filter f_hxmanager { match("hx-manager" value("MSGHDR")); };
    filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
    filter f_stcli { match("hx-stcli" value("MSGHDR")); };
    filter f_hxcli { match("hx-cli" value("MSGHDR")); };

    destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
    destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
    destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
    destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
    destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
    destination d_hx_shell { file("/var/log/syslog-ng/shell.log"); };
    destination d_stcli { file("/var/log/syslog-ng/stcli.log"); };
    destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };

   log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest); flags(final);
 };
    log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn);
flags(final); };
    log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final);
 };
   log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access); flags(final);
 };
   log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager); flags(final);
 };
    log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final);
 };
    log { source(demo_tls_src); filter(f_stcli); destination(d_stcli); flags(final); };
    log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };

########################
```

Disabling Audit Logging

You can choose to temporarily disable audit logging. By doing so, the remote syslog server details such as the server IP and the port, that you previously configured are retained in the system. You need not enter the server details again when you re-enable audit logging at a later time. You will only need to upload the certificate and private key files to enable audit logging. See Enabling Audit Logging, on page 46.

Step 1 Choose **Settings** > **Audit Log Export Settings**.

Step 2 Clear the **Enable audit log export to an external syslog server** check box.

Step 3 Click **OK**.

Audit logging is disabled.

Deleting Audit Logging Server Configuration

As an administrator, you can delete the remote syslog server configuration details from the system. When you do so, the system does not push server logs to the remote syslog server. To enable audit logging, you will have to provide the server details again. See Enabling Audit Logging, on page 46.

Step 1 Choose **Settings** > **Audit Log Export Settings**.

Step 2 Click **Delete**.

Step 3 In the **Confirm Delete** dialog box, click **Delete**.

The remote syslog server details are deleted from the system.

CHAPTER 4

Preparing for HX Storage Cluster Maintenance

Storage Cluster Maintenance Operations Overview

Maintaining the Cisco HyperFlex (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 Cisco HX Data Platform Installer. All new nodes must meet the same system requirements as when you installed the Cisco HX Data Platform and created the initial storage cluster. For a complete list of requirements and steps for using the Expand Cluster feature, see the appropriate Cisco HX Data Platform Install Guide.

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.
- 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. See Serial vs. Parallel Operations, on page 53 for more information on these tasks.. You can perform only some tasks 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 Cisco HX Maintenance Mode and the storage cluster needs to be restarted. In addition, some changes to the Cisco HX storage cluster require additional post maintenance tasks. For example, if you change the vNICs or vHBAs, the PCI Passthrough needs to be reconfigured. For more information describing how to reconfigure the PCI Passthrough, see Configure PCI Passthrough After Changing vNIC or vHBAs, on page 69.

Ensure the following:

- The ESX host is exited from Cisco 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 Cisco 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.

```
# stcli cluster info
```

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

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

Step 3 Verify the number of node failures.

```
# 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 Cisco 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 Cisco 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 Cisco HyperFlex (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.

Note The static IP address is defined as a VMKernel interface.

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 Cisco 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 Cisco HX Maintenance Mode.
- When Cisco HX Maintenance Mode is entered to enable performing tasks on an ESX host, be sure to exit Cisco 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, on page 57 for steps.

VMware ESX Maintenance Mode

This mode is used when you are installing Cisco 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

Using the Cisco HyperFlex (HX) Connect User Interface

Note Maintenance Mode is supported on Cisco HyperFlex Release 2.5(1a)/2.5(1b) and later.

1. Log in to Cisco 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.
    a. Identify the node ID and IP address.

    ```
    # stcli node list --summary
    ```

    b. Enter the node into HX Maintenance Mode.

    ```
    # 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.

   ```
   # 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.

Exiting Cisco HyperFlex Maintenance Mode

Using the Cisco HyperFlex (HX) Connect User Interface

Note Maintenance Mode is supported on Cisco HyperFlex Release 2.5(1a)/2.5(1b) and later.

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.
   a. Identify the node ID and IP address.

      ```
      # stcli node list --summary
      ```

   b. 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 in to 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.

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 address and authentication credentials.

Note All IP addresses must be IPv4. HyperFlex does not support IPv6 addresses.

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Configuration** dialog box, click **Create Backup Operation**.

Step 6 In the **Create Backup Operation** dialog box, complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled**—Cisco UCS Manager runs the backup operation as soon as you click **OK**. • **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.

Name	Description
Type field	The information saved in the backup configuration file. This can be one of the following: • **Full state**—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. **Note** 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. • **All configuration**—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. • **System configuration**—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. • **Logical configuration**—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.

Name	Description
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.

Name	Description
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 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 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. **Note** All IP addresses must be IPv4. HyperFlex does not support IPv6 addresses.
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 Cisco HX Storage Cluster

Some storage cluster maintenance tasks require that the storage cluster be shut down. 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 shut-down 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.

To shut down the Cisco HX storage cluster, perform the following steps:

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 58.

Step 1 Gracefully shut down all workload VMs on all the Cisco HX datastores.

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

Note Do not shut down or move the storage controller VMs (stCtlVMs).

Step 2 Gracefully shut down the Cisco HX storage cluster.

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

Note For clusters with a nested vCenter, performing an stcli cluster shutdown may have certain limitations. For more details, see Known Constraints with vCenter Deployment. For the procedure on how to shutdown nested vCenter, see Shut Down Nested vCenter, on page 64.

```
# stcli cluster shutdown
```

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

```
# stcli cluster info
```

In the command response text, check the cluster subsection and verify the `healthstate` is `unknown`.

This Cisco HX cluster shutdown procedure does not shut down 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 3 **To power off the HX storage cluster**, complete Step 2 and Step 3, then complete the rest of the following steps.

Step 4 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 controllerVM 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 5 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 6 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 Cisco HX Maintenance Mode, and powering down the servers, as directed.

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

2. To restart the Cisco HX storage cluster, proceed to Power On and Start Up the Cisco HX Storage Cluster, on page 65.

Shut Down Nested vCenter

This section captures the procedure to shutdown a netsted vCenter within a cluster.

Step 1 Shutdown all VMs on a cluster.

Step 2 Shutdown vCenter.

Step 3 Note down the name of host on which vCenter is running as the host has to be manually started.

Step 4 Stop Storfs on all controllers using Mobaxterm, by running the following command:

```
stop storfs
```

Step 5 Shutdown controllers using Mobaxterm, by running the following command:

```
shutdown -P now
```

Step 6 Put all individual hosts in maintenance mode, by running the following comamnd:

```
esxcli system maintenanceMode set -e true
```

Step 7 Shutdown the ESX hosts.

Step 8 Boot up the ESX hosts.

Step 9 Exit all hosts from maintenance mode, by running the following command:

```
esxcli system maintenanceMode set -e false
```

Step 10 Manually start the stCTLVMs (as vCenter is down, they may not start automatically).

Step 11 Verify if Storfs is running on each controller, by running the following command:

```
# pidof storfs
```

If the `pidof` command does not retun any output, start Storfs by running the following command:

```
# start storfs
```

Step 12 From the controller, check for the cluster status by running the following command:

```
sysmtool --ns cluster --cmd info
```

Wait for cluster to be healthy.

Step 13 Power on vCenter from the host (use the host name note down in step 3).

Wait for vCenter to be up. Check if the cluster is healthy by running the following command:

```
stcli cluster info  | grep -A 1 vCluster
```

After vCenter is up and running, you will get a state of online from this command.

Note If the `stcli cluster storage-summary command` fails and the cluster is in the healthy state, start the cluster using the `stcli cluster start` command.

Power On and Start Up the Cisco HX Storage Cluster

The steps here are for use in restarting the Cisco 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 Cisco HX Storage Cluster, on page 62.

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.

a. Log in to each Fabric Interconnect using SSH.

b. 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 Exit each node from maintenance mode.

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

Step 5 If all the controller VMs are not automatically powerd on, power on all the controller VMs (`stCtlVM`) using one of the following methods:

Using vSphere Client

a) From the vSphere Client, view a storage controller host.
b) Right-click the `stCtrlVM` 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 6 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 7 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 8 Start 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.

Restoring the Configuration for a Fabric Interconnect

It is recommended that you 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. You can also use a full state backup to restore a system if they have the same release train. For example, you can use a full state backup taken from a system running Release 2.1(3a) to restore a system running Release 2.1(3f).

To avoid issues with VSAN or VLAN configuration, a backup should be restored on the fabric interconnect that was the primary fabric interconnect at the time of backup.

Before you begin

Collect the following information to restore the system configuration:

- Fabric interconnect management port IPv4 address and subnet mask.
- Default gateway IPv4 address.

Note All IP address must be IPv4. IPv6 addresses are not supported.

- Backup server IPv4 address and authentication credentials.
- Fully-qualified name of a Full State backup file

Note You must have access to a Full State configuration file to perform a system restore. You cannot perform a system restore with any other type of configuration or backup file.

SUMMARY STEPS

1. Connect to the console port.
2. If the fabric interconnect is off, power on the fabric interconnect.
3. At the installation method prompt, enter `gui`.
4. If the system cannot access a DHCP server, you may be prompted to enter the following information:
5. Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.
6. On the launch page, select **Express Setup**.
7. On the **Express Setup** page, select **Restore From Backup** and click **Submit**.
8. In the **Protocol** area of the **Cisco UCS Manager Initial Setup** page, select the protocol you want to use to upload the full state backup file:

- **SCP**
- **TFTP**
- **FTP**
- **SFTP**

9. In the **Server Information** area, complete the following fields:
10. Click **Submit**.

DETAILED STEPS

Step 1 Connect to the console port.

Step 2 If the fabric interconnect is off, power on the fabric interconnect.

You will see the power on self-test message as the fabric interconnect boots.

Step 3 At the installation method prompt, enter `gui`.

Step 4 If the system cannot access a DHCP server, you may be prompted to enter the following information:

- IPv4 address for the management port on the fabric interconnect
- Subnet mask or prefix for the management port on the fabric interconnect
- IPv4 address for the default gateway assigned to the fabric interconnect

Step 5 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 6 On the launch page, select **Express Setup**.

Step 7 On the **Express Setup** page, select **Restore From Backup** and click **Submit**.

Step 8 In the **Protocol** area of the **Cisco UCS Manager Initial Setup** page, select the protocol you want to use to upload the full state backup file:

- **SCP**
- **TFTP**
- **FTP**
- **SFTP**

Step 9 In the **Server Information** area, complete the following fields:

Name	Description
Server IP	The IPv4 address of the computer where the full state backup file is located. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.
Backup File Path	The file path where the full state backup file is located, including the folder names and filename. **Note** 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.

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

Step 10 Click **Submit**.

You can return to the console to watch the progress of the system restore.

The fabric interconnect logs in to the backup server, retrieves a copy of the specified full-state backup file, and restores the system configuration.

For a cluster configuration, you do not need to restore the secondary fabric interconnect. As soon as the secondary fabric interconnect reboots, Cisco UCS Manager synchronizes the configuration with the primary fabric interconnect.

Configure PCI Passthrough After Changing vNIC or vHBAs

Description

After vNIC or vHBA are manually added to an Cisco HyperFlex (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 pass through.
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**.

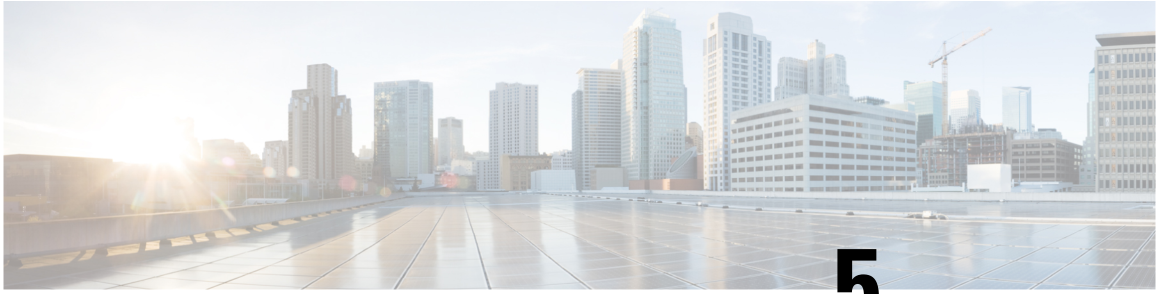
b) Locate and re-add the LSI Logic PCI device.

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.



CHAPTER 5

Managing HX Storage Clusters

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 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.

Important Rebalance typically occurs only when a single disk usage exceeds 50% or cluster aggregate disk usage is greater than 50%.

You can check rebalance status through the HX Data Platform plug-in or through the storage controller VM command line.

Step 1 Check the rebalance status through HX Data Platform plug-in.

a) From the vSphere Web Client Navigator, select **vCenter Inventory Lists** > **Cisco HyperFlex Systems** > **Cisco HX Data Platform** > ***cluster*** > **Summary**.

The **Status** portlet lists the **Self healing status**.

b) Expand the 'Resiliency Status' to see the 'Self Healing status' section. The Self healing status field lists the rebalance activity or N/A, when rebalance is not currently active.

Step 2 Check the rebalance status through the storage controller VM command line.

a) Login to a controller VM using `ssh`.

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

```
# stcli rebalance status
```

The following output indicates that rebalance is not currently running on the storage cluster.

```
rebalanceStatus:
percentComplete: 0
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. `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.

Step 2 View the cleaner schedule.

```
# stcli cleaner get-schedule --id ID | --ip NAME
```

Parameter	Description
`--id ID`	ID of storage cluster node
`--ip NAME`	IP address of storage cluster node

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 74.

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 74.

3. Unregister HX Data Platform using the vCenter Extension Manager. See Unregistering a Storage Cluster from a vCenter Cluster, on page 75

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 77.

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.

  ```
  # 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 75.

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 74.

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 Removing HX Data Platform Files from the vSphere Client, on page 75.

Step 2 Complete the steps in Verifying HX Cluster is Unregistered from vCenter, on page 76.

What to do next

Proceed to Registering a Storage Cluster with a New vCenter Cluster, on page 77.

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.

```
# service vsphere-client restart
```

Windows vCenter

a) Login to the Windows vCenter system command line using Remote Desktop Protocol (RDP).
b) Change to the folder containing the HX Data Platform Plug-in folder.

```
# cd "%PROGRAMDATA%\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity
```

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

```
# rmdir /com.springpath*
```

d) Open the Service screen.

```
# services.msc
```

e) Restart the vSphere Web Client to logout of vCenter.

```
# serviceLogout
```

Verifying HX Cluster is Unregistered from vCenter

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

Verify that the HX cluster is no longer on the old vCenter.

Before you begin

Complete the steps in:

- Removing HX Data Platform Files from the vSphere Client, on page 75

Step 1 Clear your cache before logging back into vCenter.
Step 2 Log out of the old vCenter.
Step 3 Log 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 75.

Step 1 Login to a controller VM.

Step 2 Run the `stcli cluster reregister` command.

stcli cluster reregister [-h] --vcenter-datacenter NEWDATACENTER --vcenter-cluster NEWVCENTERCLUSTER --vcenter-url NEWVCENTERURL [--vcenter-sso-url NEWVCENTERSSOURL] --vcenter-user NEWVCENTERUSER

Apply additional listed options as needed.

Syntax Description

Option	Required or Optional	Description
--vcenter-cluster NEWVCENTERCLUSTER	Required	Name of the new vCenter cluster.
--vcenter-datacenter NEWDATACENTER	Required	Name of the new vCenter datacenter.
--vcenter-sso-url NEWVCENTERSSOURL	Optional	URL of the new vCenter SSO server. This is inferred from `--vcenter-url`, if not specified.
--vcenter-url NEWVCENTERURL	Required	URL of the new vCenter, <*vcentername*>. Where <*vcentername*> can be FQDN or IP.
--vcenter-user NEWVCENTERUSER	Required	User name of the new vCenter administrator. Enter vCenter administrator password when prompted.

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 in vCenter, then run the command below to re-add the compute only nodes:

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

Contact TAC for assistance if required.

Step 3 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.

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.

Replacing Self-Signed Certificate

Replacing Self-Signed Certificate with External CA Certificate on a vCenter Server

Set the certMgmt mode in vCenter to **Custom** to add the ESXi hosts with third party certificate to vCenter.

Note By default, the certMgmt mode is **vmsa**. In the default **vmsa** mode, you can add only the ESX host with self signed certificates. If you try to add an ESX with CA certificate to a vCenter, it will not alllow you to add the ESX host unless CA certificate is replaced with self-signed certificate.

To update the certMgmt mode:

a) Select the vCenter server that manages the hosts and click **Settings**.
b) Click **Advanced Settings**, and click **Edit**.
c) In the **Filter** box, enter **certmgmt** to display only certificate management keys.
d) Change the value of **vpxd.certmgmt.mode** to **custom** and click **OK**.
e) Restart the vCenter server service.

   To restart services, enter the following link in a browser and then click **Enter**:

```
https://<VC URL>:5480/ui/services
```

Note The behavior of host addition in vCenter varies according to the certificate and certMgmt mode.

- When the host has self-signed certificate with the certMgmt mode set to the default value of **vmsa** in vCenter:
  - Only ESX host with self-signed certificate can be added.
  - The addition of ESX with third party CA certficate is not allowed.
  - If you try to add an ESX to a vCenter after replacing the self-signed certificate with a third party CA certificate, the system will prompt you to replace third party CA certificate with self-signed certificate. You can add the ESX host after replacing CA certificate with self-signed certificate.
- When the host has self-signed certificate with the certMgmt mode set to **custom** in vCenter:
  - If you try to add an ESX to a vCenter after replacing the self-signed certificate with a third party CA certificate, the system throws an error: `ssl thumbprint mismatch and add host fails`. In this case, do the following to replace the third party CA certificate with the self-signed certificate:
    1. Place the host in the maintenance mode (MM mode).
    2. Replace the certified rui.crt and rui.key files with the backed up previous key and certificate.
    3. Restart the hostd and vpxa service. The CA certificate comes up in the new node.
    4. Right-click and connect to vCenter. The host losts the CA certificate and gets replaced with self-signed certification in VMware.
- When the host has third party CA certificate with the certMgmt mode set to the default value of **vmsa** in vCenter:
  - ESX host with self-signed certificate can be added.
  - The addition of ESX with third party CA certficate is not allowed.
- When the host has third party CA certificate with the certMgmt mode set to **custom** in vCenter:
  - ESX host with self-signed certificate cannot be added.
  - The self-signed certificate in ESX host needs to be replaced with a CA certificate of vCenter.

Replacing Self-Signed Certificate with External CA Certificate on a ESXi Host

Step 1 Generate the host certificate (rui.crt) and key (rui.key) files and send the files to the certificate authority.

Note Ensure that a proper hostname or FQDN of the ESX host is provided while generating the rui.key and rui.crt files.

Step 2 Replace the certified host certificate (rui.crt) and key (rui.key) files in the /etc/vmware/ssl directory on each ESXi host after taking backup of the original host certificate (rui.crt) and key (rui.key) files.

Note Replace host certificate (rui.crt) and key (rui.key) files in a rolling fashion by placing only one host in maintenance mode and then wait for the cluster to be healthy and then replace the certificates for the other nodes.

a) Log in to the ESXi host from an SSH client with administrator privileges.
b) Place the host in the maintenance mode (MM mode).
c) Take a backup of the previous key and certificate to the rui.bak file in the /etc/vmware/ssl/ directory.
d) Upload the new certified rui.crt and rui.key files to the /etc/vmware/ssl/ directory.
e) Restart the hostd and vpxa service, and check the running status using the following commands:

```
/etc/init.d/hostd restart
/etc/init.d/vpxa restart
/etc/init.d/hostd status
/etc/init.d/vpxa status
```

f) Reconnect the host to vCenter and exit the maintenance mode.

Note Repeat the same procedure on all the nodes. You can verify the certificate of each node by accessing it through web.

Reregistering a HyperFlex cluster

After adding all the hosts to the vCenter after replacing the certified files, reregister the HX cluster to the vCenter using the following command:

```
stcli cluster reregister
```

Recreating a Self-Signed Certificate

If you face any issue with the host certificate after replacing external CA certificate, you can recreate the self-signed certificate by executing the following procedure:

1. Log in to the ESXi host from an SSH client.

2. Delete the rui.key and rui.crt files from the /etc/vmware/ssl/ directory.

3. Recreate the self-signed certificate for the host using the following command:

   ```
   /sbin/generate-certificates
   ```

4. Restart the hostd and vpxa service using the following commands:

   ```
   /etc/init.d/hostd restart
   /etc/init.d/vpxa restart
   ```

CHAPTER 6

Managing Encryption

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 **Global Inventory Lists > Cisco Hyperflex Systems > Cisco HX Data Platform > Cluster_Name > 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 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.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	*<admin>* username
Password field	*<admin>* password

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.

UI Element	Essential Information
UCS Manager host name field	For example, *10.193.211.120*.
User name field	<*admin*> username.
Password field	<*admin*> password.

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.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. <*eng-fi12.eng.storvisor.com*>
User name field	<*admin*> username
Password field	<*admin*> password

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**.

Step 6 To confirm disabling the encryption key on the cluster, in the **Disable encryption?** dialog box, click **Yes, 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.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	*<admin>* username
Password field	*<root>* password

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.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	*<admin>* username
Password field	*<admin>* password

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.

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

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.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	*<admin>* username
Password field	*<root>* password

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.

UI Element	Essential Information
Primary key management server field	Enter the primary Key Management Server IP address.
(Optional) **Secondary key management server** field	If you have a secondary key management server set up for redundancy, enter the details here.
Port number field	Enter the port number you wish to use for the key management servers.
Public key field	Enter the public root certificate of the certificate authority that you generated during KMIP server configuration.

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.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	<*admin*> username
Password field	<*root*> password

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.

UI Element	Essential Information
Email address field	<*admin*> email address.
Organization name field	The organization requesting the certificate. Enter up to 32 characters.
Organization unit name field	The organizational unit. Enter up to 64 characters.
Locality field	The city or town in which the company requesting the certificate is headquartered. Enter up to 32 characters.
State field	The state or province in which the company requesting the certificate is headquartered. Enter up to 32 characters.

UI Element	Essential Information
Country field	The country in which the company resides. Enter two alphabetic characters in uppercase.
Valid for (days) field	The validity period of the certificate.

Step 6 To generate self-signed certificates 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 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.

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

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

Step 3 From the **Edit configuration** drop-down list, select **Manage certificates**.

Step 4 Enter the following Cisco UCS Manager credentials, to set up a primary key management (KMIP) server and optionally a secondary KMIP server.

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	*<admin>* username
Password field	*<admin>* password

Click **Next**.

Step 5 Enter the primary and secondary key management (KMIP) server credentials.

UI Element	Essential Information
Primary key management server field	Enter the primary Key Management Server IP address.
(Optional) **Secondary key management server** field	If you have a secondary key management server set up for redundancy, enter the details here.
Port number field	Enter the port number you wish to use for the key management servers.
Public key field	Enter the public root certificate of the certificate authority that you generated during KMIP server configuration.

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

Restart Encryption

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

UI Element	Essential Information
UCS Manager host name field	Cisco UCS Manager cluster host name. Enter an IP address or FQDN. *<eng-fi12.eng.storvisor.com>*
User name field	*<admin>* username
Password field	*<admin>* password

CHAPTER 7

Managing Datastores

Managing Datastores

Datastores are logical containers used by the HX Data Platform to manage your storage usage 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 UI or the HX Data Platform Plug-in UI. You can only rename an unpaired datastore that is unmounted. Renaming the datastore is not supported by the vCenter administrator interface.

Important

- Keep the number of datastores to as few as possible to avoid startup delay and to keep clone savings high.
- Configuring more than 10 datastores could result in excessive startup delay.

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 blocksize. 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: 1. Change the datastore name, or 2. Change the datastore storage allocation. That is, the size of the datastore.

Note Do not rename datastores with controller VMs.

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.

Note You can not select an NFS datastore as a destination for the persistent scratch location on ESXi. If you select the HX datastore for the persistent scratch location, it will be removed after the ESXi host reloads.

For all M5 servers, M.2 boot SSD is automatically selected for use as scratch. This is configured out of the box on any new install.

For HX240M4 (non-SED), Intel SSD is used for persistent logs/scratch (same applies on 220M5/240M5, but on a different local SSD).

For HX220M4 and HX240M4 (SED), there is no location to store the scratch partition. So, the only option is to use syslog for persistent logging over the network.

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.**

a) Go through the above checklist and unmount or delete through one of the UIs or CLI again.

b) Use the UI or CLI to re-mount the datastore.

For additional information on recovering from partial unmounts, see Recovering from Partially Unmounted Datastores, on page 95.

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 **Delete**.

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

Recovering from Partially Unmounted Datastores

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

Step 1 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.

Step 2 Retry to mount, unmount, or delete the datastore through the HX Connect or HX Data Platform Plug-in UI or CLI again.

Step 3 If the datastore is not in the desire mount, unmount, or deleted state, complete the following.

a) Ensure VMs are not running on the datastore.

b) From ESX host, check to see if the HX Data Platform datastore is being used by VMware service, `storageRM`.

```
# ls -ltra /vmfs/volumes/stfs-ds1/ | grep -i iorm
```

Sample response

```
-rwxr-xr-x 1 root root 16511 Jan 20 20:05 .iormstats.sf
drwxr-xr-x 1 root root 1125 Jan 20 20:06 .iorm.sf
```

c) Check the `storagerm` status.

```
# /etc/init.d/storageRM status
```

Sample response

```
storageRM is running
```

d) Stop the `storagerm` service.

```
# /etc/init.d/storageRM stop
```

Sample response

```
watchdog-storageRM: Terminating watchdog process with PID 34096
storageRM stopped
```

e) Try to mount, unmount, or delete the datastore again.

f) This is one possible solution, if this doesn't resolve the issue, contact Technical Assistance Center (TAC).

CHAPTER 8

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 from different vendors or of different types, pause for a few moments (30 seconds) between each action. Pull, pause for about 30 seconds and replace a drive, pause for 30 seconds. Then, pull, pause for 30 seconds 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

Component	Qty	Hybrid	All Flash	Hybrid SED	All Flash SED
System SSD for logs	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
Cache SSD	1 (back)	1.6 TB SSD	1.6 TB NVMe 400 GB SSD	1.6 TB SSD	800 GB SSD
Persistent	6-23	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

Note For information on disk requirements for HX240 M5 LFF servers, see Disk Requirements for LFF Converged NodesHardware and Software Requirements, on page 100.

HX240 M4 Servers

Component	Qty	Hybrid	All Flash	Hybrid SED	All Flash SED
System SSD for logs	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
Cache SSD	1	1.6 TB SSD	1.6 TB NVMe 400 GB SSD	1.6 TB SSD	1.6 TB NVMe 800 GB SSD
Persistent	6-23	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX220 M5 Servers

Component	Qty	Hybrid	All Flash	Hybrid SED	All Flash SED
System SSD for logs	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
Cache SSD	1	480 GB SSD 800 GB SSD	1.6 TB NVMe 400 GB SSD	800 GB SSD	800 GB SSD
Persistent	6-8	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX 220 M4 Servers

Component	Qty	Hybrid	All Flash	Hybrid SED	All Flash SED
System SSD for logs	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
Cache SSD	1	480 GB SSD	400 GB SSD	800 GB SSD	800 GB SSD
Persistent	6	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX220 M5 Servers for Edge Clusters

Component	Qty	Hybrid	All Flash	Hybrid SED	All Flash SED
System SSD for logs	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
Cache SSD	1	480 GB SSD 800 GB SSD	1.6 TB NVMe 400 GB SSD	800 GB SSD	800 GB SSD
Persistent	3-8	1.2 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX 220 M4 Servers for Edge Clusters

Component	Qty	Hybrid	All Flash	Hybrid SED	All Flash SED
System SSD for logs	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
Cache SSD	1	480 GB SSD	400 GB SSD	800 GB SSD	800 GB SSD
Persistent	3-6	1.2 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

Disk Requirements for LFF Converged Nodes

The following table lists the supported HX240 M5 Server Large-Form-Factor (LFF) converged node configurations:

Table 1: HX240 M5 Server Large-Form-Factor (LFF) Configuration

	Description	Part Number	Quantity
Memory	16GB or 32GB or 64GB or 128GB DDR4-2666-MHz	HX-MR-X16G1RS-H HX-MR-X32G2RS-H HX-MR-X64G4RS-H HX-MR-128G8RS-H	Min. 128 MB
Processor	Processor Choices: Supported Skylake parts on HX 240 M5	Varies	2
Drive Controller	Cisco 12Gbps Modular SAS HBA	HX-SAS-M5	1
SSD1 (Boot SSD)	240GB 2.5 inch Enterprise Value 6G SATA SSD	HX-SD240G61X-EV	1
SSD2 (Cache/WL)	3.2TB 2.5 inch Enterprise Performance 12G SAS SSD(3X)	HX-SD32T123X-EP	
HDD (Capacity/Data)	6TB 12G SAS 7.2K RPM LFF HDD (4K) **OR** 8TB 12G SAS 7.2K RPM LFF HDD (4K)	HX-HD6T7KL4KN **OR** HX-HD8T7KL4KN	6 - 12
Network	Cisco VIC 1387 Dual Port 40GB QSFP CNA MLOM	HX-MLOM-C40Q-03	1
Boot Device	240GB SATA M.2	HX-M2-240GB	1
Software	Cisco HX Data Platform 1, 2, 3, or 4 or 5yr SW subscription	HXDP-001-xYR	1
Optional VMware License	Factory Installed – VMware vSphere6 Enterprise Plus/Standard SW License & Subscription		2
FI Support	2G FI and 3G FI		

Hardware and Software Requirements

Hardware

- Memory Configurable
- CPU Configurable
- HDD Storage Quantity

Software

- Storage Controller
  - Reserves 72GB RAM
  - Reserves 8 vCPU, 10.800 GHz CPU

- VAAI VIB
- IO Visor VIB

Compute-Only Nodes

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.

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. **Note** HW RAID M.2 (UCS-M2-HWRAID and HX-M2-HWRAID) is not supported on Compute-only nodes.

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 Cluster 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 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 104 or Replacing or Adding Hard Disk Drives, on page 108 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.

Step 2 Login to HX Connect.

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

Step 4 Identify and verify the disk to remove.

a. Use the Turn On Locator LED button.

b. Physically view the disks on the server.

c. 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

Note 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.

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 104 and the hardware guide for your server.
   - **Rotational** (hybrid drives)—See Replacing or Adding Hard Disk Drives, on page 108 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 53.

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 105.
- 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** > **Equipment** > **Server** > **Inventory** > **Storage** tab, re-acknowledge the server node. This applies to cache and persistent disks.

Note Re-acknowledging a server is disruptive. Place the server into HX Maintenance Mode before doing so.

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 104.

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 > Equipment > Server > Inventory > Storage** tab, re-acknowledge the server node. This applies to cache and persistent disks.

Note Re-acknowledging a server is disruptive. Place the server into HX Maintenance Mode before doing so.

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

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 (scsi)
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.

```
# df -ah
```

Sample response

```
...........
/dev/sdb1 63G 324M 60G 1%
/var/stv /dev/sdb2 24G 173M 23G 1% /var/zookeeper
```

Step 6 Identify the HX Data Platform installer package version installed on the existing storage cluster.

```
# stcli cluster version
```

The same version must be installed on all the storage cluster nodes. Run this command on the controller VM of any node in the storage cluster, but not the node with the new SSD.

Step 7 Copy the HX Data Platform installer packages into the storage controller VM in `/tmp` folder.

```
# scp <hxdp_installer_vm_ip>:/opt/springpath/packages/storfs-packages-<hxdp_installer>.tgz /tmp
```

```
# cd /tmp
```

```
# tar zxvf storfs-packages-<hxdp_installer>.tgz
```

Step 8 Run the HX Data Platform installer deployment script.

```
# ./inst-packages.sh
```

For additional information on installing the HX Data Platform, see the appropriate Cisco HX Data Platform Install Guide.

Step 9 After the package installation, HX Data Platform starts automatically. Check the status.

```
# status storfs
```

Sample response

```
storfs running
```

The node with the new SSD re-joins the existing cluster and the cluster returns to a healthy state.

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 > Equipment > Server > Inventory > Storage** tab, re-acknowledge the server node.

Note Re-acknowledging a server is disruptive. Place the server into HX Maintenance Mode before doing so.

CHAPTER 9

Managing Nodes

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.

Note A replication factor of three is highly recommended for all environments except HyperFlex Edge. A replication factor of two has a lower level of availability and resiliency. The risk of outage due to component or node failures should be mitigated by having active and regular backups.

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; and collecting and analyzing logs.

Step 3 Complete the identified tasks.

- Reinstall or upgrade software.

  For steps to reinstall ESXi or the HX Data Platform see *Cisco HyperFlex Systems Installation Guide for VMware ESXi*. 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. For more information, see Removing a Node, on page 118.

- 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. For more information, see Replacing a Node, on page 126.

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.

- **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 There are several considerations to keep in mind before replacing a node. For more information, see Replacing a Node, on page 126.

The following tables lists the methods available to perform the associated node maintenance task.

Repair Node Software

ESX and HX Data Platform software is installed on every node in the storage cluster. If it is determined after node failure analysis that either software item needs to be re-installed, see the *Cisco HyperFlex Systems Installation Guide for VMware ESXi*. 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.

No. Nodes in Cluster	No. Failed Nodes in Cluster	Method	Notes
3	1 or more	TAC assisted only node repair.	Node does not need to be removed to perform repair. Includes replacing disks on node.
4-8	1	Online or Offline node repair.	Node does not need to be removed to perform repair. Includes replacing disks on node.

Remove Node

A non-reparable item on node fails. Disks on the removed node are not reused in the storage cluster.

No. Nodes in Cluster	No. Failed Nodes in Cluster	Method	Notes
4	1	Offline node remove.	A 4 node cluster with 2 nodes down, requires TAC assistance.
5 or more	1	Online or Offline node remove.	
5 or more	2	Offline 2 node remove.	A 5 node cluster with 3 nodes down, requires TAC assistance.

Replace Node and Discard Storage

A non-reparable item on node fails. Disks on the removed node are not reused in the storage cluster.

No. Nodes in Cluster	No. Failed Nodes in Cluster	Method	Notes
3	1	TAC assisted only node replace.	TAC assisted node replacement required to return cluster to minimum 3 nodes. A 3 node cluster with 1 node down, requires TAC assistance.
4	1	Offline replace node. Not reusing the disks.	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.
5 or more	1	Online or offline replace node. Not reusing the disks.	Use Expand cluster to add new nodes. All other nodes must be up and running.
5 or more	2	Offline replace 1 or 2 nodes. Not reusing the disks.	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.

Replace Node and Reuse Storage

A non-reparable item on node fails. Disks on the removed node are reused in the storage cluster.

No. Nodes in Cluster	No. Failed Nodes in Cluster	Method	Notes
3 or more	1 or more	TAC assisted only.	TAC assisted node replacement required to return cluster to minimum 3 nodes. **Note** Reusing disks requires assigning old node UUID to new node. Disks UUIDs to node UUID relationship is fixed and cannot be reassigned. This is a TAC assisted task.

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 DNSserver 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.

b) Edit `resolv.conf.d` file.

```
# vi /etc/resolvconf/resolv.conf.d/base
```

c) Confirm the change.

```
# resolvconf -u
# cat /etc/resolv.conf
```

d) Confirm the DNS server can be queried from either the IP address or the host name.

```
# 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.

```
# vi /etc/hosts
```

c) Add the following line and save the file.

```
ip_address ubuntu newhostname
```

For each host *ip_address*, enter the host *newhostname*.

a) Add the *newhostname* to `hostname`.

```
# hostname newhostname
```

Changing ESXi Host Root Password

You can change the default ESXi password for the following scenarios:

- During creation of a standard and stretch cluster (supports only converged nodes)
- During expansion of a standard cluster (supports both converged or compute node expansion)
- During Edge cluster creation

Note In the above cases, the ESXi root password is secured as soon as installation is complete. In the event a subsequent password change is required, the procedure outlined below may be used after installation to manually change the root password.

As the ESXi comes up with the factory default password, you should change the password for security reasons. 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 in to 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 Lookup 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.

```
#  stcli cluster reregister
--vcenter-datacenter <datacenter_name>
--vcenter-cluster <hx_cluster_name>
--vcenter-url <FQDN_name>
--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 77 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 Managing Disks 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 drive. Front bay 1

    See Managing Disks 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

    Both the storage cluster tasks and hardware focused tasks are required to replace this component.

  - RTC Battery on motherboard

    Note The motherboard itself is not a replaceable component. You must purchase a battery from your local hardware store and replace it.

  - 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 your account team 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.

Table 2: Removing a Node Workflows

Cluster Size	Nodes Removed	Workflow
3 node cluster	1 or more	Workflow requires TAC assistance.
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.
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.

Cluster Size	Nodes Removed	Workflow
5 node cluster	2	**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 nodes. Use the `stcli node remove` command. Specify both nodes. **5.** Restart the cluster. Use the `stcli cluster start` command.
5 node cluster	3 or more	Workflow requires TAC assistance.

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.

Note 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 heathy:

```
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 node from a storage cluster while the cluster remains online has 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.

Number of nodes in cluster	Method
3 node cluster	See TAC to remove and replace the node.
4 node cluster	Cluster must be offline. See Removing a Node from an Offline Storage Cluster, on page 123.
5 node cluster, removing 2 nodes	Cluster must be offline. See Removing a Node from an Offline Storage Cluster, on page 123.
5 node cluster, removing 1 node from a healthy cluster	Cluster can be online. Continue with the steps listed here.

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

Option	Required or Optional	Description
--id-1 ID1	One of set required.	A unique ID number for the storage cluster node. The ID is listed in the `stcli cluster info` command under the `stNode` field `id`.
--ip-1 NAME1	One of set required.	IP address of storage cluster node. The IP is listed in the `stcli cluster info` command under the `stNode` field `name`.
--id-2 ID2	Optional.	A unique ID number for the storage cluster node. The ID is listed in the `stcli cluster info` command under the `stNode` field `id`.
--ip-2 NAME2	Optional.	IP address of storage cluster node. The IP is listed in the `stcli cluster info` command under the `stNode` field `name`. The `--ip` option is currently not supported.
-f, --force	Optional.	Forcibly remove storage cluster nodes.

```
Example:
stNodes for a 5 node cluster:
    ----------------------------------------
    type: node
    id: 569c03dc-9af3-c646-8ac5-34b1f7e04b5c
    name: example1
    ----------------------------------------
    type: node
    id: 0e0701a2-2452-8242-b6d4-bce8d29f8f17
    name: example2
    ----------------------------------------
    type: node
    id: a2b43640-cf94-b042-a091-341358fdd3f4
    name: example3
----------------------------------------
    type: node
    id: c2d43691-fab5-30b2-a092-741368dee3c4
    name: example4
----------------------------------------
    type: node
    id: d2d43691-daf5-50c4-d096-941358fede374
    name: example5
```

The **stcli node remove** command to remove nodes from the 5 node cluster are:

- To remove 1 node

  - **stcli node remove –ip-1 example5** or
  - **stcli node remove –id-1 d2d43691-daf5-50c4-d096-941358fede374**

- To remove 2 nodes at the same time:
  - **stcli node remove –ip-1 example5 –ip-2 example4** or
  - **stcli node remove –id-1 d2d43691-daf5-50c4-d096-941358fede374 –id-2 c2d43691-fab5-30b2-a092-741368dee3c4**

    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 the vCenter and it does not 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.

Step 6 Remove the host from the vCenter **Hosts and Cluster** view.

a) Log in to vSphere Web Client Navigator. Navigate to **Host** in the vSphere Inventory.
b) Right-click the host and select **Enter Maintenenace Mode**. Click **Yes**.
c) Right-click the host and select **All vCenter Actions** > **Remove from Inventory**. Click **Yes**.

Step 7 Decommission the host from UCS Manager.

a) Log in to UCS Manager. In the Navigation pane, click **Equipment**.
b) Expand **Equipment** > **Chassis**>*Chassis Number*>**Servers**.
c) Choose the HX server you want to decommission. In the work pane, click the **General** tab.
d) In the **Actions** area, click **Server Maintenance**. In the **Maintenance** dialog box, click **Decommission**. Click **OK**.

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.

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.

Number of nodes in cluster	Method
3 node cluster	See TAC to remove and replace the node.
4 node cluster	Cluster must be offline.
5 node cluster, removing 2 nodes	Cluster must be offline.
5 node cluster, removing 1 node from a healthy cluster	Cluster can be online. See Removing a Node from an Online Storage Cluster, on page 121.

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 needed 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.

```
# 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.

```
# 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
```

Removing a Compute Node

Step 1 Migrate all the VMs from a compute node that needs to be removed.

Step 2 Unmount the datastore from the compute node.

Step 3 Check if the cluster is in the healthy state, by running the following command:

```
stcli cluster info --summary
```

Step 4 Put ESXi host in the HX Maintenance mode.

Step 5 Remove the compute node using the `stcli node remove` command, from CMIP (use the Cisco HX connect IP address as it is the cluster IP address).

```
stcli node remove --ip-1
```

Where, IP is the IP address of the node to be removed.

Step 6 Remove any DVS from the EXSi host in vCenter, if there is a DVS.

Step 7 Remove the ESXi host from vCenter.

Step 8 Check if the cluster is in the healthy state, by running the following command:

```
stcli cluster info --summary
```

Step 9 Clear stale entries in the compute node by logging out of Cisco HX Connect and then logging into Cisco HX Connect.

Step 10 Disable and re-enable the High Availability (HA) and Distributed Resource Scheduler (DRS) services to reconfigure the services after node removal.

Deleting the Removed Node Data from a Disk and a Storage Controller VM

After removing a node from a storage cluster, you have to delete the removed node details from the disk and storage controller VM using the following procedure.

Warning Be aware that once the data is deleted you cannot recover it.

Step 1 Destroy the cluster by running the following command:

```
run destroycluster -sxy
```

Step 2 Remove the `stvboot.cfg` configuration file from the `/etc/` folder.

Step 3 Reboot the controller VM.

Note The reboot process takes few minutes.

Step 4 After rebooting the controller VM, run the following command:

```
# for d in $(/bin/lsblk -dpn -e 1,2,7,11 | awk '{ print $1 }');do  grep -qE "$d[0-9]"
/proc/mounts && continue; dd if=/dev/zero of=$d bs=1M oflag=direct & done;
```

The data deletion action takes few fours. On completion of the drive data deletion, you will get the message: `No space left on device`. Ignore this message.

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.

Workflows for Replacing a Node

The affecting context is based on the number of converged nodes. The number of compute nodes does not affect the replacing a node workflow.

Cluster Size	Nodes Replaced	Workflow
3 node cluster	1 or more	Workflow requires TAC assistance.

Cluster Size	Nodes Replaced	Workflow
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.

Cluster Size	Nodes Replaced	Workflow
5 node cluster	2	**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 nodes. Use the `stcli node remove` command. Specify both nodes. **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.
5 node cluster	3 or more	Workflow requires TAC assistance.

Replacing a node and discarding the failed node's disks.

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*.

Replacing a Compute Node

If a compute node boot disk or blade is corrupted and the node needs to be replaced, perform the following steps:

1. Remove the compute node from the existing Hyper-V Hyperflex Cluster.
2. Reinstall OS and re-add the compute node into the cluster.

Note Compute nodes are supported in Hyperflex release 3.5.2 and later releases.

This section provides the procedure for replacing a compute node that needs to be replaced due to faulty boot disk or blade.

Step 1 Use Hyper-V failover cluster manager and remove the bad compute node from the failover cluster manager.

Step 2 Clean up the computer object of the compute node from the Active Directory.

Note There is no need to clean up DNS entry of the compute node.

Step 3 Navigate to any controller VM and run the `remcomputenode.py` script to clean up the stale entries associated with the compute node.

The remove compute node Python script can be executed by providing either the UUID or host name of the compute node as an argument.

The following sample shows how to run the script with UUID of the compute node:

```
python remcomputenode.py -u C2581942-55D2-8021-B1B1-A117F396D671
```

The following sample shows how to run the script with host name of the compute node:

```
python remcomputenode.py -n node-hv1.cloud.local
```

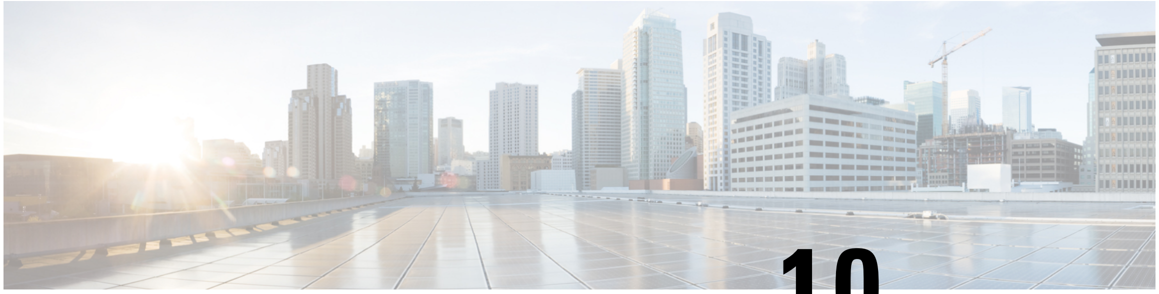
Note Ensure that the following .egg files are available in the controller VM:

- /usr/share/thrift-0.9.1.a-py2.7-linux-x86_64.egg
- /opt/springpath/storfs-mgmt-cli/stCli-1.0-py2.7.egg

Step 4 Replace the faulty MB, compute blade, or boot disk.

Step 5 Run the compute node expansion workflow from the Installer VM.

a) Install Windows 2016.
b) On the **HX Data Platform Installer** page, select the **I know what I’m doing...** check box.
c) Select the expansion workflow and complete the procedure.



CHAPTER 10

Managing HX Controller VMs

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, **Global 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
  ubuntu64Guest   vmx-11
3   Cisco HyperFlex Installer  [test]  Cisco HyperFlex Installer/Cisco HyperFlex Installer.vmx
 ubuntu64Guest   vmx-09
Retrieved runtime info
Powered off
```

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
```

Disabling HA VM Monitoring in HX Controller VMs

To avoid All Paths Down (APD) state in an HX cluster, use the vSphere Web Client to disable HA VM Monitoring for all the HX Controller VMs.

Step 1 Login to the vSphere Web Client.

Step 2 Select the HX cluster that you want to modify.

Step 3 Select **Configure** > **VM Overrides** from the menu.

Step 4 Click **Add**.

Add VM Override Sandbox window is displayed along with the list of VMs in vCenter.

Step 5 Select all the available HX Controller VMs in the window.

Note The HX Controller VM names begin with `stCtlVM-`.

Step 6 Click **Next**.

Add VM Override dialog box is displayed.

Step 7 Locate the **vSphere HA - VM Monitoring** option and select the following:

- **Override** checkbox
- **Disabled** from the drop-down list

Step 8 Click **Finish** to apply the configuration changes.

HA VM Monitoring is disabled for all the HX controller VMs.

CHAPTER 11

Managing Ready Clones

HX Data Platform Ready Clones Overview

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

A Ready Clone, 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 Ready Clone is a separate guest VM.

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

Installing a guest operating system and applications can be time consuming. With Ready Clone, 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 Ready Clones

HX Data Platform Ready Clones 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 Ready Clones feature.

- **Rapid cloning -** HX Data Platform Ready Clones are extremely fast and more 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 Ready Clones 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 Ready Clones feature automates the task to create each guest VM.
- **VDI deployment support -** Ready Clones are supported for desktop VMs on VDI deployments which are using VMware native technology.
- **Datastore access -** Ready Clone 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 Ready Clones from one base VM
- Maximum 256 Ready Clones 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

Ready Clone 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.

  Ready Clones fail for any VM that is not on a HX Data Platform datastore. This applies to Ready Clones on a VM level, VM folder level, or resource pool level.
- VMs can have only native snapshots. Ready Clones 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 Ready Clones.

Ready Clone 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 Ready Clone 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 Ready Clones Using HX Connect

Use HX Data Platform Ready Clones feature to populate your cluster by creating multiple clones of a VM, each with different static IP addresses.

Note If you click **Ready Clones** to clone a VM when the OVA deployment of that VM is in progress, you will get an error message. You can clone a VM only after the successful VM deployment.

Step 1 Login to HX Connect as an administrator.

Step 2 From **Virutal Machines** page, select a ***virtual machine***, then click **Ready Clones**.

Step 3 Complete the **Ready Clone** dialog fields.

UI Element	Essential Information
Number of clones	Enter the number of Ready Clones that you want to create. You can create a batch of 1 through 256 clones at a given time.
Customization Specification	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.

UI Element	Essential Information
Resource Pool	Optional field. If you have resource pools defined in your HX Storage Cluster, you can select one to store the Ready Clones of the selected virtual machine.
VM Name Prefix	Enter a prefix for the guest virtual machine name. This prefix is added to the name of each Ready Clone created.
Starting clone number	Enter a clone number for the starting clone. Each Ready Clone must have a unique name, numbering is used to ensure a unique element in the name.
Increment clone numbers by	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 Ready Clones (such as clone1, clone2, and clone3). By default, the number starts from 1. You can change this value to any number.
Use same name for Guest Name	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.
Preview	After required fields are completed, HX Data Platform lists the proposed Ready Clones names. As you change the content in the required fields, the **Clone Name** and **Guest Name** fields update.
Power on VMs after cloning	Select this check box to turn the guest virtual machines on after the cloning process completes.

Step 4 Click **Clone**.

HX Data Platform creates the number of Ready Clones with the naming and location specified.

Creating Ready Clones 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 Ready Clones 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 **Global Inventory Lists** > **Virtual Machines**. This displays the list of VMs in vCenter.

Step 2 Select the VM to clone, 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 > Ready Clones** to display the Ready Clones dialog box.

Step 4 Specify the following information in the Ready Clones dialog box:

Control	Description
Number of clones	Type the number of clones that you want to create. You can create a batch of 1 through 256 clones at a given time.
Customization Specification	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.
VM name prefix	Type a prefix for the guest VM name.
Starting clone number	Type a clone number for the starting clone.
Use same name for 'Guest Name'	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 Ready Clone batch customization process overrides the option that you specify in the Customization Specification option. • If the Customization Specification contains a NIC or network adapter that uses a static gateway and static subnet and the guest name resolves to a static IP address, then the system assigns the network adapter the static IP address associated with the guest name. It also sets the storage cluster name or host name to the guest name specified. • If the Customization Specification contains a NIC or network adapter that obtains the IP address using DHCP, then the systems sets only the storage cluster name or host name to the guest name specified.
Increment clone number by	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.
Power on VMs after cloning	Select this check box to turn the guest VMs on after the cloning process completes.

Step 5 Click **OK** to apply your configuration changes.

The vSphere Web Client Recent Tasks tab displays the status of the Ready Clones 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 Ready Clone workflow a temporary snapshot is listed in vCenter and HXConnect. This is listed as an extra powered off VM transiently, only while the Ready Clones are being created.

Prepare to Customize HX Data Platform Ready Clones

- 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 Ready Clones feature to overwrite the guest name that you specify in when you create the customization specification.
- HX Data Platform Ready Clones 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 Ready Clone customization process overwrites this address.

  - HX Data Platform Ready Clones 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.

Note 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 Ready Clone 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 Ready Clones 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 Ready Clones 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 Ready Clones 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.

See the VLANs chapter in the *Cisco UCS Manager Network Management Guide* at, http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/3-1/b_UCSM_Network_Mgmt_Guide_3_1/b_UCSM_Network_Mgmt_Guide_3_1_chapter_0110.html.

Step 2 Verify the vNICs are configured correctly.

See the Configuring vNIC Templates topics in the *Cisco UCS Manager Network Management Guide* at, http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Network-Mgmt/3-1/b_UCSM_Network_Mgmt_Guide_3_1/b_UCSM_Network_Mgmt_Guide_3_1_chapter_0111.html#d24564e315a1635.

Step 3 Verify the Virtual Port Groups are configured correctly.

See the Add a Virtual Machine Port Group topic in the *VMware vSphere 6.0 Documentation* at, http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-004E2D69-1EE8-453E-A287-E9597A80C7DD.html

CHAPTER 12

Managing Native Snapshots

HX Data Platform Native Snapshots Overview

HX Data Platform Native Snapshots is 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 can revert to the saved state.

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 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 HyperFlex Data Platform CLI Guide*.

  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.

Upgrade

- HX native snapshots are not supported while upgrade of HX, ESXi, or UCS is in progress.

VMs

Note For 3.5.2(a) and previous releases, all powered on VMs use synchronous consolidation (asynConsolidate = false) when taking HX snapshots.

For 3.5.2(b) and later releases, all powered on VMs use asynchronous consolidation (asyncConsolidate = true) when taking HX snapshots. If the VM is powered off, the settings remain unchanged.

- **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.
- **VM Size -** The maximum size of the Virtual Machine Disk (VMDK) that an HyperFlex snapshot is 3TB. The time taken to snapshot vary depending on the cluster model, cluster load, and I/O workload on the VM.
- **VM Name -** The VM name must be unique per vCenter for taking a snapshot.

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

Object	Maximum Number
Snapshots	30 per storage cluster VMware limit is 31. One snapshot is consumed by SENTINEL.
Datastores	8 per storage cluster
VMs	1024 per host
Powered on VMs	100 per host
vDisks per VM	60 per VM

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 using the HX Data Platform plug-in, the scheduled times are converted to UTC from the storage controller VM timezone. When you view the schedule through the Web Client Schedule Tasks it displays the tasks in browser time zone.

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 Tasks 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.

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.

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 based on the timezone

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 https://en.wikipedia.org/wiki/List_of_tz_database_time_zones

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`.

```
snapshot.asyncConsolidate="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 4:15 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.

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. See the following table for more details.

Table 3: VM Power State After Restoring a HX VM Snapshot

VM State When HX VM Snapshot is Taken	VM State After Restoration
Powered on (includes memory)	Reverts to the HX VM snapshot, and the VM is powered on and running.
Powered on (does not include memory)	Reverts to the HX VM snapshot, and the VM is powered off.
Powered off (does not include memory)	Reverts to the HX VM snapshot, and the VM is powered off.

Step 6 If the reverted VM is powered off, then select the 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.

CHAPTER 13

Managing Clusters Running on Different HXDP Versions

Managing Clusters Running on Different HXDP Versions

Scenario—Site A at HXDP 3.0 and Site B at HDXP 2.6

The following terms and abbreviations are used:

- **Site A**—Source cluster
- **Site B**—Target cluster
- **dr_cleanup tool**—Contact Cisco TAC to obtain this tool available in the 3.0 internal support package.

Prerequisites

- Before upgrading make sure, there are no VMs or groups in **Recovered** or **Halted** state.
- If the VMs are in **Halted** State, recover and unprotect the VMs or groups.
- If the VMs are in **Recovered** state, then unprotect the VMs or groups.

Step	Site A	Site B	Result
1.	At HXDP version 2.6 or lower.	At HXDP version 2.6 or lower.	—

Step	Site A	Site B	Result
2.	Upgrade to HXDP 3.0.	—	• Ongoing replication continues. • Planned migration for VMs is not supported. • See Functionality Limitations, on page 156 for more details.
3.	Before upgrading Site B, if a disaster happens on Site A.	**1.** Execute the command: *stcli dp peer forget* **2.** Recover VMs that are required. **3.** Run the **dr_cleanup** tool to delete all the VM information from the disaster recovery database.	Workloads are now running on Site B.
4.	Restore Site A. After Site A is restored, do the following: **1.** Execute the command: *stcli dp peer forget* **2.** Run the **dr_cleanup** tool to delete all the VM information from the disaster recovery database.	—	Sites are unpaired.
5.	—	Upgrade to HXDP 3.0.	—
6.	Pair the sites.	—	Site A and Site B can now be re-paired and workloads can be protected.

Scenario—Site A at HXDP 2.6 and Site B at HXDP 3.0

The following terms and abbreviations are used:

- **Site A**—Source cluster
- **Site B**—Target cluster
- **dr_cleanup tool**—Contact Cisco TAC to obtain this tool available in the 3.0 internal support package.

Prerequisites

- Before upgrading make sure, there are no VMs or groups in **Recovered** or **Halted** state.
- If the VMs are in **Halted** State, recover and unprotect the VMs or groups.
- If the VMs are in **Recovered** state, then unprotect the VMs or groups.

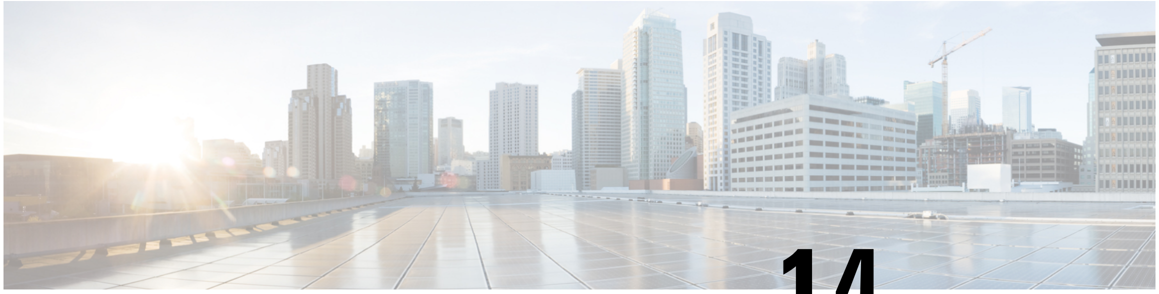
Step	Site A	Site B	Result
1.	At HXDP version 2.6 or lower.	At HXDP version 2.6 or lower.	—
2.	—	Upgrade to HXDP 3.0.	• Ongoing replication continues. • Planned migration for VMs is not supported. • See Functionality Limitations, on page 156 for more details.
3.	Before upgrading Site A, if a disaster happens on Site A.	**1.** Execute the command: *stcli dp peer forget* **2.** Recover VMs that are required. **3.** Run the **dr_cleanup** tool to delete all the VM information from the disaster recovery database.	• Not all recovery options are available. • See Functionality Limitations, on page 156 for more details. • Workloads are now running on Site B.

Step	Site A	Site B	Result
4.	Restore Site A. After Site A is restored, do the following: **1.** Execute the command: *stcli dp peer forget* **2.** Run the **dr_cleanup** tool to delete all the VM information from the disaster recovery database.	—	Sites are unpaired.
5.	Upgrade Site A to HXDP 3.0.	—	—
6.	—	Pair the sites.	Site A and Site B can now be re-paired and workloads can be protected.

Functionality Limitations

Newer functionality in release 3.0 is supported ONLY when both the source and target clusters are on the same HXDP version. It can take a while during upgrade for both the source and target to be on the same version. Review the following functionality limitations:

- Planned migration for VMs is not supported when peer sites have mismatched versions, such as when the target cluster is on 2.6, and source cluster is on 3.0.
- When the source is upgraded, all the newer features in release 3.0, such as movein and moveout of group VMs, migration are blocked on the source cluster until the peer is upgraded.
- If only the target cluster is upgraded, in **HX Connect** UI, **Network Mapping** options in the **Recovery** dialog box will not available until the source cluster is upgraded.



CHAPTER 14

Managing Virtual Machine Disaster Recovery

Data Protection

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, you may use the most recently replicated snapshot of each protected VM 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.

Note Only one snapshot retention is supported for backup workflows.

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 5 minutes and 24 hours.

Protection group is a group of VMs that have a common replication schedule and snapshot properties.

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. Use HX Connect to provide a set of IP addresses to be used by local cluster nodes to replicate to the remote cluster. HX Connect creates VLANs through UCS Manager, for dedicated replication network use.

Note When this option is chosen in HX Connect, UCSM is configured only when both UCS Manager and fabric interconnect are associated with the HyperFlex cluster. When UCSM and FI are not present, you must enter the VLAN ID, and not select UCSM configuration in HX Connect.

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.

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 the 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.

Port Requirements for Replication

Verify that the following firewall ports are open when configuring native HX asynchronous cluster to cluster replication:

Port Number	Service/Protocol	Source	Port Destinations	Essential Information
9338	Data Services Manager Peer/TCP	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses
3049	Replication for CVM/TCP	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses
4049	Cluster Map/TCP	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses
4059	NR NFS/TCP	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses
9098	Replication Service	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses

Port Number	Service/Protocol	Source	Port Destinations	Essential Information
8889	NR Master for Coordination/TCP	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses
9350	Hypervisor Service/TCP	Each CVM Node	Each CVM Node	Bidirectional, include cluster management IP addresses

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 with administrator privileges on the local cluster. For tasks involving a remote cluster, both the local and remote user must have administrator privileges and should be configured with the vCenter SSO on their respective clusters.
-
- **Storage Space—**Ensure that 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 and compression), each replicated virtual machine will 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 73. Pause all replication schedules until you have appropriately adjusted the space available on the HX Cluster. Always ensure that your cluster capacity consumption is below the space utilization warning threshold.
- **Supported Clusters—**Replication is supported between the following HyperFlex clusters:
  - 1:1 replication between HX clusters running under fabric interconnects.
  - 1:1 replication between All Flash and Hybrid HX cluster running under fabric interconnects.
  - 1:1 replication between 3-Node and 4-Node HX Edge and another 3-Node and 4-Node HX Edge cluster.
  - 1:1 replication between All Flash 3-Node and 4-Node Edge and Hybrid 3-Node and 4-Node HX Edge clusters.
  - 1:1 replication between 3-Node and 4-Node HX Edge and an HX cluster running under fabric interconnects.

  Note 1:1 replication with 2-Node HX Edge 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 64.
  - Do not add VMs with ISOs or floppies to protection groups.
- **Non-HX Datastores—**If you have protected a VM with storage on a non-HX datastore, periodical replication will fail on this. You can either unprotect this VM or remove its non-HX storage.

  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.
- **Templates—**Templates are not supported for Disaster Recovery.
- **Protection and Recovery of Virtual Machines with Snapshots**
  - A VM with no Snapshots—When replication is enabled the entire content of the VM is replicated.
  - A VM with VMware Redolog snapshots—When replication is enabled the entire content including the snapshot data is replicated. When a VM with redolog snapshots is recovered, all previous snapshots are preserved.
  - A VM with Hyperflex Snapshots—When replication is enabled only the latest data is replicated, and the snapshot data is not replicated. When the VM is recovered, previous snapshots are not preserved.
- **Data Protection and Disaster Recovery (DR) snapshots** are stored on the same datastore as the protected VMs. Deleting these snapshots manually by an Admin, is not supported. Deleting the snapshot directories would compromise HX data protection and disaster recovery.

Caution As in any VMware environment, not restricted to HX on VMware, datastores can be accessed by the Admin via VCenter browser or by logging into the ESX host. Because of this, snapshot directory and contents are browse-able and accessible to Admins. VMware does not restrict operations on datastores by Admin. Please be aware of this to avoid deleting snapshots manually.

Replication Network and Pairing Considerations

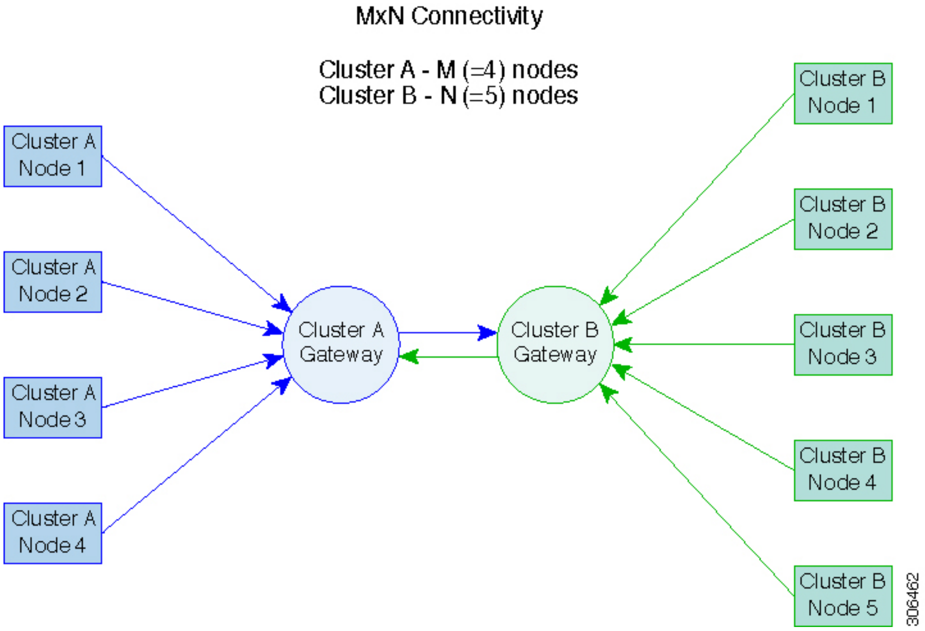
A replication network must be established between clusters that are expected to use replication for Data Protection. This Replication network is created to isolate inter-cluster replication traffic from other traffic within each cluster and site.

The following is a list of considerations when configuring replication network and pairing:

- To support efficient replication, all M nodes of cluster A have to communicate with all N nodes of cluster B, as illustrated in the *M x N connectivity between clusters* figure.

- To enable replication traffic between clusters to cross the site-boundary and traverse the internet, each node on Cluster A should be able to communicate with each node on Cluster B across the site boundary and the internet.
- The replication traffic must be isolated from other traffic within the cluster and the data center.
- To create this isolated replication network for inter-cluster traffic, complete these steps:
  - Create a replication network on each cluster.
  - Pair clusters to associate the clusters and establish M x N connectivity between the clusters.
- IP addresses, Subnet, VLAN, and Gateway are associated with each replication network of each cluster. You must configure the corporate firewall and routers on both sites, to allow communication between the clusters and the sites on TCP ports *9338,3049,9098,4049,4059*.

M*N Connectivity Between Clusters



Data Protection Terms

Interval—Part of the replication schedule configuration, used to enforce how often the protected VMs replication snapshot must be taken and copied to the target cluster.

Local cluster—The cluster you are currently logged into through HX Connect, in a VM replication cluster pair. From the local cluster, you can 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 do not change.

Primary cluster—An alternative name for the source cluster in VM disaster recovery.

Protected virtual machine—A VM that has replication configured. The protected VMs Reside on a datastore in the local cluster of a replication pair. They 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—The 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 is 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 Protected VMs in the local cluster.

Replication pair—Two clusters that together provide a remote cluster location for storing the 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, which is 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 replication cluster pair. The source cluster is where the protected VMs reside.

Target cluster—One of a VM replication cluster pair. The target cluster receives the replication snapshots from the VMs of the source cluster. The target cluster is used to recover the VMs in the event of a disaster on the source cluster.

Protecting Virtual Machines

Protecting Virtual Machines Overview

To protect a virtual machine, specify the following protection attributes:

- Replication interval, which is the frequency of replication.
- A start time (within the next 24 hours), which specifies the first-time replication is attempted for that virtual machine.
- Specify if the replication snapshot should be taken with the virtual machine quiesced or not.

Protection attributes can be created and assigned to protection groups. To assign the protection attributes to virtual machines, they can be added to a protection group.

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 5 or 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, you can choose from the following methods:

Note When you select multiple virtual machines, you must add them to a protection group.

- **Independently—**Select one virtual machine and configure. Set the replication schedule and the VMware quiesce option for the specific virtual machine. Changes to the replication settings will 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 add 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

To protect VMs and their data using replication, perform the following steps:

- Configure two clusters and pair them to each other, to support the replication network activity.
- Assign replication schedule for the VMs to set the frequency (interval) for creating replication snapshots on the source cluster and copy them to the target cluster. Set replication schedule on individual VMs and on protection groups.

Replication Workflow

1. Install HX Data Platform, create two clusters.
2. Create at least one datastore on each cluster.
3. Log in to HX Connect.
4. Before creating the replication network, verify the IP addresses, subnet mask, VLAN, gateway, and IP range to be used for the replication network. After the replication network is created, validate connectivity within the cluster over this new replication network.
5. The default value of MTU is 1500. If your HyperFlex cluster uses OTV or other tunneling mechanisms, ensure that you choose an MTU which will work for inter-site or inter-cluster connectivity.
6. Configure cluster replication network 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.
7. An intra-cluster network test is performed to validate connectivity between the nodes in the cluster, after the replication network is configured. If the intra-cluster network test fails, the replication network configuration is rolled back. Reconfigure the replication network after fixing the issue.

8. Before creating the replication pair, ensure that you have updated the corporate network to support this pairing.

9. Create a replication pair from one cluster to the other, connecting the two clusters. After the replication pair is created, a test of the inter-cluster pair network is performed to validate bidirectional connectivity between the clusters. Set the datastore mapping from both clusters.

10. Optionally, you can create protection groups.
    - Set the schedule. Each protection group must have one schedule.
    - Create multiple protection groups if you want to have various replication intervals (schedules) for different virtual machines. A virtual machine can only belong to one protection group.

11. Select virtual machines to protect, as individual virtual machines or virtual machines assigned to protection groups.

12. Set protection, do the following:
    a. Select one or more virtual machines. Click Protect.
    b. From the Protect Virtual Machine wizard, the 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 a new protection group.

          Create new protection group and set schedule.

Configuring the Replication Network in HX Connect

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 log in to the remote cluster and complete the configuration there.

Before you begin

Ensure that the following prerequisites are met, before configuring the replication network:

- A minimum of N + 1 IP addresses is required, where N is the number of converged nodes. An IP subnet spanning these new IP addresses, the gateway, and VLAN associated with this subnet is also required.
- To accommodate future cluster expansion, ensure that there are sufficient IP addresses in the subnet provided, for later use. Any new converged nodes in the expanded cluster would also need to be assigned IP addresses for replication. The subnet provided in the previous step should span the potentially new IP range as well.
- Additional IP-pool ranges can be added to the network later, however IP-pools already configured in the replication network cannot be modified.

- Make sure that the IP addresses to be used for the replication network are not already in use by other systems.
- Before creating the replication network, verify IP addresses, Subnet, VLAN, and Gateway to be used for the replication network.

Step 1 Log in to HX Connect as administrator.

Step 2 Select **Replication** > **Replication Configuration** > **Configure Network**.

Note You can only configure the replication network once. Once configured, you can edit the available IP addresses and the networking bandwidth.

Step 3 In the **Configure Replication Network** dialog box, under the tab, enter the network information.

UI Element	Essential Information
Select an existing VLAN radio button	Click this radio button to add an existing VLAN. If you manually configured a VLAN for use by the replication network through Cisco UCS Manager, enter that VLAN ID.
Create a new VLAN radio button	Click this radio button 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. 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, *3*. 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.
VLAN Name field	This field is automatically populated with a default VLAN name when the **Create a new VLAN** radio button is selected. The VLAN ID is concatenated to the name.
For Stretched Cluster, provide Cisco UCS Manager credentials for primary and secondary FIs (site A and site B).For normal cluster, provide Cisco UCS Manager credential for single FI.	
UCS Manager host IP or FQDN field	Enter Cisco UCS Manager FQDN or IP address. For example, *10.193.211.120*.
Username field	Enter administrative username for Cisco UCS Manager.
Password field	Enter administrative password for Cisco UCS Manager.

Step 4 Click **Next**.

Step 5 In the **IP & Bandwidth Configuration** tab, set the network parameters and the replication bandwidth.

UI Element	Essential Information

Subnet field	Enter the subnet for use by the replication network in network prefix notation. The subnet is separate from the HX Data Platform Management traffic network and Data traffic network.
	`Format example:`
	`x.x.x.x/<number of bits>`
	`1.1.1.1/20`

Gateway field	Enter the gateway IP address for use by the replication network. The gateway is separate from the HX Data Platform Management traffic network and Data traffic network. For example, *1.2.3.4*. **Note** The gateway IP address must be accessible even if the disaster recovery is being setup for a flat network.
IP Range field	Enter a range of IP addresses for use by the replication network. • The minimum number of IP addresses required is the number of nodes in your HX Storage Cluster plus one more. For example, if you have a 4 node HX Storage Cluster, enter a range of at least 5 IP addresses. • The **from** value must be lower than the **to** value. For example, *From 10.10.10.20 To 10.10.10.30*. • If you plan to add nodes to your cluster, include sufficient number of IP addresses to cover any additional nodes. You can add IP addresses at any time. **Note** The IP address range excludes compute-only nodes.
Add IP Range button	Click to add the range of IP addresses entered in **IP Range** `From` and `To` fields.

UI Element	Essential Information
Set Replication Bandwidth Limit check box	Enter the maximum network bandwidth that the replication network is allowed to consume for inbound and outbound traffic. Acceptable value is 33,000 Mbits/sec. The default value is `unlimited`, which sets the maximum network bandwidth to the total available to the network. The replication bandwidth is used to copy replication snapshots from this local HX Storage Cluster to the paired remote HX Storage Cluster. **Note** • At lower bandwidth (typically, lesser than 50 Mbits/sec), the replications of multiple VMs may exit without executing the replication process due to high data transfer rate. To overcome this issue, either increase the bandwidth or stagger VM replication schedule so that VMs do not replicate in the same window. • The bandwidth setting must be close to the link speed. The bandwidth setting for the clusters in the pair must be same. • The set bandwidth is applicable only for the incoming and outgoing traffic of the cluster to which the bandwidth is set to. For example, setting the bandwidth limit as 100Mb means that the 100Mb is set for incoming traffic and 100Mb is set for outgoing traffic. • The set bandwidth limit must not exceed the physical bandwidth. • The bandwidth configured must be same on both sites of the disaster recovery environment. • The allowed low bandwidth is 10Mb and the maximum latency supported with 10Mb is 75ms. If the initial replication of VMs fails due to lossy network or unstable HX clusters, the VM replication will be initiated again in the next schedule as a fresh replication job. In this case, you have to size the schedule accordingly to protect VMs.
Set non-default MTU check box	Default MTU value is 1500. Select the check box to set a custom MTU size for the replication network. MTU can be set in the range 1024 to 1500. **Note** • Ensure to use the same MTU value on both sides of the cluster. • After configuring the cluster, if the MTU value needs to be changed, you must reconfigure the cluster.

Note When you use an existing VLAN for replication network, the replication network configuration fails. You must add the self-created replication VLAN to the management vNIC templates in Cisco UCS Manager.

Step 6 Click **Next**.

Step 7 In the **Test Configuration tab**, check the replication network configuration.

Step 8 Click **Configure**.

What to do next

- Be sure to configure the replication network on both HX Storage Clusters for the replication pair.
- After the replication network is created on the cluster, each converged node on the cluster would be configured with an IP address on the eth2 interface.
- Check for duplicate IP assignment using *'arp-scan'*.

```
For example if your replication subnet is 10.89.1.0/24:
$ sudo arp-scan 192.168.0.0/24 | cut -f1 | sort | uniq -d
```

If there is a duplicate IP assignment, it is necessary to remove the replication network assignments.

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. For example, in a 3 node cluster, four IP addresses are required. If you are adding one more node to the cluster, five IP addresses are minimum. Edit the replication network to add IP addresses.

Step 1 Log in to HX Connect as administrator.

Step 2 In the Navigation pane, Select **Replication**.

Step 3 From the **Actions** drop-down list, select **Edit Replication Network**.

Step 4 In the **Edit Network Configuration** dialog box, you can edit the range of IPs to use and set the replication bandwidth limit for replication traffic. The replication network subnet and gateway are displayed for reference only and cannot be edited.

UI Element	Essential Information
Subnet field	The subnet that is configured for the replication network in network prefix notation. This value cannot be edited.
Gateway field	The gateway that is configured for the replication network. This is value cannot be edited.

UI Element	Essential Information
IP Range field	Enter a range of IP addresses for use by the replication network. • The minimum number of IP addresses required is the number of nodes in your HX Storage Cluster plus one more. For example, if you have a 4 node HX Storage Cluster, enter a range of at least 5 IP addresses. • The **from** value must be lower than the **to** value. For example, *From 10.10.10.20 To 10.10.10.30*. • If you plan to add nodes to your cluster, include sufficient number of IP addresses to cover any additional nodes. You can add IP addresses at any time. **Note** The IP address range excludes compute-only nodes.
Add IP Range field	Click to add the range of IP addresses that are entered in **IP Range** `From` and `To` fields.
Set replication bandwidth limit check box (Optional)	Enter the maximum network bandwidth that the replication network is allowed to consume for outbound traffic. Acceptable value is between 10 and 10,000. The default is `unlimited`, which sets the maximum network bandwidth to the total available to the network. The replication bandwidth is used to copy replication snapshots from this local HX Storage Cluster to the paired remote HX Storage Cluster.

Step 5 Click **Save Changes**.

The replication network is now updated. The added IP addresses are available for new nodes when they are added to the storage cluster. Replication traffic adjusts to any changes made to the bandwidth limit.

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 1.

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. After the replication pair is configured, you can begin protecting virtual machines. See the **Virtual Machines** tab.

Important When pairing or mapping clusters at different versions, cluster pairing must be initiated on the 3.5 cluster and then the datastore mapping must be initiated from the 3.0 cluster.

- Cluster pairing must be initiated only from a 3.5 cluster to a 3.0 cluster.
- Datastore mapping must be initiated only from a 3.0 cluster to a 3.5 cluster.

Before you begin

- Create a datastore on both the local and the remote cluster.
- Configure the replication network.

Step 1 From HX Connect, log in to either the local or remote cluster as a user with administrator privileges. Select **Replication** > **Replication Pairs** > **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**.

Once the Test Cluster Pair job is succesful, you can proceed to the next step. On the Activity page, you can view the progress of the Test Cluster Pair job.

UI Element	Essential Information
Management IP or FQDN field	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*.
User Name and **Password** fields	Enter vCenter single sign-on or cluster specific administrator credentials for the remote HX Storage Cluster.

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.
- Moving virtual machine to another paired datastore is supported. If the VMs are moved to unpaired datastore, replication schedule fails.

Step 5 Review the Summary information and click **Map Datastores**.

Editing a Replication Pair

Editing a replication pair is changing the datastores for the replication pair.

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
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. **a.** 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**. **b.** 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.

Log in to the local and the remote HX storage cluster and perform the following:

- Unprotect all virtual machines. Remove virtual machines from protection groups.
- Remove protection groups. If the protection group does not have a VM, deleting protection group is not required.

Step 1 Log in to HX Connect as an administrator.

Step 2 Unmap the datastores in the replication pair.

a) Select **Replication** > **Replication Pairs** > **Edit**.

After the test cluster pair job is successful, you can proceed to the next step. You can view the progress of the Test Cluster Pair job on the Activity page.

b) From the **Edit Replication Pair** dialog box, select **Do not map this datastore** from the **Remote Datastore** menu.

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.

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**.

UI Element	Essential Information
User Name field	Enter the administrator user name for the remote HX Storage Cluster.
Password field	Enter the administrator password for the remote HX Storage Cluster.

Creating a Protection Group

A protection group is a group of VMs with the same replication scheme.

Create protection groups on a local cluster. Protection groups provide protection to the VMs where they are created. If protection groups have protected virtual machines that replicate to the remote cluster, these protection groups are listed in HX Connect.

Note You can only manage a protection group from its local cluster, the cluster where it is created.

Before you begin

Ensure that replication network and replication pair are configured.

Step 1 Log in to HX Connect as an administrator.

Step 2 Select **Replication** > **Protection Groups** > **Create Protection Group**.

Step 3 Enter the information in the dialog fields.

UI Element	Essential Information
Protection Group Name field	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.
Protect virtual machines in this group every field	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
Start protecting the virtual machines immediately radio button	Select this radio button if you want the first replication to start immediately after you add the first virtual machine to this protection group.
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: **a.** Check the **Start protecting the virtual machines at** radio button. **b.** 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.

If the number of VMs is zero, 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.

UI Element	Essential Information
Protect virtual machines in this group every field	Select from the pull-down list how often the virtual machines are to be replicated to the paired cluster. The options are: 5 minutes, 15 minutes, 30 minutes, 1 hour, 90 minutes, 2 hours, 4 hours, 8 hours, 12 hours, 24 hours
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.

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 Select **Replication** > **Protection Groups** > ***protection_group_name***

Step 2 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 add 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 Log in 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 machines from the list.

Click in the virtual machine row to select it. As you click a virtual machine row, the corresponding virtual machine check box 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**

UI Element	Essential Information
Set the protection parameters table	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.
Add to an existing protection group radio button	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.
Create a new protection group radio button	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.

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**.

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 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**.

UI Element	Essential Information
Protect virtual machines in this group every field	Select how often the virtual machines are to be replicated to the paired cluster. Default is every 1 hour.
Start protecting the virtual machines immediately radio button	Select this radio button if you want the first replication to start immediately after you add the first virtual machine to this protection group.

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: **a.** Check the **Start protecting the virtual machines at** radio button. **b.** 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 machines 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 in not included in a protection group.
- **Existing protection group—**Select one or more virtual machines and add 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 Log in to HX Connect with administrator privileges and select **Virtual Machines**.

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 check box is selected.

Step 3 Click **Protect**.

The **Protect Virtual Machine** dialog box is displayed.

Step 4 Complete the fields as needed.

UI Element	Essential Information
Add to an existing protection group radio button	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 **Protect Virtual Machine**.
Protect this virtual machine independently radio button	Enables the interval, schedule options, and VMware Tools option for defining protection for this virtual machine.
Protect this virtual machine every field	Select from the pull-down list how often the virtual machines are to be replicated to the paired cluster. The options are: 5 minutes, 15 minutes, 30 minutes, 1 hour, 90 minutes, 2 hours, 4 hours, 8 hours, 12 hours, 24 hours
Start protecting the virtual machines immediately radio button	Select this radio button if you want the first replication to start immediately after you add the first virtual machine to this protection group.

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: **a.** Check the **Start protecting the virtual machines at** radio button. **b.** 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

Note You do not need to unprotect virtual machines to pause replication for cluster activities. See Pausing Replication, on page 188.

Step 1 Log in to HX Connect as an administrator.

Step 2 Select **Virtual Machines**.

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**.

Data Protection Recovery

Disaster Recovery Overview

Disaster recovery is performed when the source site is unreachable and you want to failover the VMs and the protected groups to the target cluster. The process of recovery recovers the VM on the target cluster. Recovering virtual machines is restoring a most recent replication snapshot from the recovery (target) cluster.

Testing VM recovery—Testing VM recovery gives you the ability to test recovery without breaking replication. It can bring up your VM workload on the target to verify the contents of the VM.

Recovering virtual machines—Recovering virtual machines is restoring a most recent replication snapshot from the target (recovery) cluster. Once you start Recovery, all the scheduled replication will be stopped.

Planned migration—Performing planned migration pauses the replication schedule, replicates the most recent copy, recovers on the target, switches the ownership from the source to the target, and resumes replication on the target that is now the new source.

Disaster Recovery and Reprotect—Recovers the VM on the target, switches the ownership from the source to the target, and resumes replication on the target that is now the new source.

Protecting VMs after disaster—In the event of a disaster, you may lose the source site altogether. After the recovery is performed, complete this task to protect the recovered VMs to a newer cluster.

Testing Virtual Machine Recovery

Testing VM recovery gives you the ability to test recovery without breaking replication. It can bring up your VM workload on the target to verify the contents of the VM.

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.
- Using the HX Connect user interface, to test VM recovery, you can run a maximum of 10 tasks in a sequence without waiting for the previously submitted task to complete.

Before you begin

Before you begin the test virtual machine recovery process, ensure the following:

- 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.

Important Only one copy of the test recovered VM can be made at any point. If you need to have another test recovered VM, please delete the previously created VM.

Step 1 Log in to HX Connect on the target cluster as administrator.

Step 2 Navigate to **Replication** > **Remote VMs Tab** > ***protected_vm***.

Step 3 To test the recovery process, click the **Test Recovery** button.

Note When you configure recovery settings, the following fields are auto-populated.

UI Element	Essential Information
Resource Pool drop-down list	Select a location for the test VM to be stored.
Folders drop-down list	Select a location for the test VM to be stored, for example: • Discovered Virtual Machine • HX Test Recovery
Power On/Off radio button	By default Power ON option is selected. The recovered VM is powered on or left off after it is created as per the selected option.
VM Name field	Enter a new name for the created test VM.
Test Networks radio button	Select which HX Storage Cluster network to use for transferring the data from the replication snapshot. Network options for example: • Storage Controller Data Network • Storage Controller Management Network • Storage Controller Replication Network • VM Network
Map Networks radio button	Select to create a map between the source and the target cluster networks. • Source Network—Network name at the source side on which the VM is connected. • Target Network—Select target network from the drop-down list, where the VM has to be connected.

Step 4 Click **Recover VM**.

Step 5 For VMs that are part of a protection group, perform a test recovery on each VM in the group.

Step 6 Verify the contents of the recovered VM.

Recovering Virtual Machines

Recovering virtual machines is restoring a most recent replication snapshot from the target (recovery) cluster.

⚠

Attention

- You may configure the folder, network, or resource pool parameters to be used during recovery, test recovery and migrate operations. If the global recovery setting is not configured, you will need to explicitly map individual VMs at the time of recovery.
- Recover VM is not supported between different vSphere versions. If the Target is at a lower version vSphere environment and does not support the hardware version of a protected VM on the primary, VM test recovery and recovery may fail. Cisco recommends to test recover each protected VM to validate the support on the target site.

  Upgrade the target environment to enable recovery of protected VMs.
- When running recovery on virtual machines, you may specify explicit network mapping when recovering the VMs to avoid unintentional network connections to recovered VMs.

  You can skip specifying network mapping in the following cases:

  - If the source VMs use vSphere Standard Switches and if all ESXi hosts on the recovery side have standard switch networks with the same name.
  - If the source VMs use vSphere Distributed Switch (vDS) port groups and if the recovery site has identically named vDS port groups.
- If you want to specify network mapping, ensure that both the name and the type of the VM network matches between the source and the target.
- 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

Ensure the following:

- 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 Log in to HX Connect as administrator.

Step 2 Select **Replication > > Remote VMs tab > >** ***protected_vm*** and click **Recover**.

Step 3 To recover the VM and build a new VM on the local cluster, click the **Recover VM** button.

Note When you configure recovery settings, the following fields are auto-populated.

UI Element	Essential Information
Resource Pool drop-down list	Select a location for the new VM to be stored.
Folders drop-down list	Select a location for the new VM to be stored.
Power On/Off radio button	By default Power ON option is selected. The recovered VM is powered on or left off after it is created as per the selected option.
Map Networks	Select to create a map between the source and target cluster networks. • Source Network—Network name at the source side on which the VM is connected. • Target Network—Select target network from the drop-down list, where the VM has to be connected. Network options for example: • Storage Controller Data Network • Storage Controller Management Network • Storage Controller Replication Network • VM Network

Step 4 Click **Recover VM**.

Step 5 Wait for the recovery to complete. View the recovered VM in the target vCenter.

Recovering Virtual Machines in Protection Groups

Step 1 Select a *protected-vm* and click **Recover**.

All VMs will be moved from the protection group and the selected VMs will be recovered. Recovered VMs show protection status as *Recovered* and the remaining (protection group) VMs show protection status as *Recovering*. The protection group will go in *Recovered* state and is not reusable. You can delete it from the primary site.

The recovered VMs are displayed in the **Standalone Protected VMs** subpane.

Step 2 Recover the remaining virtual machines from the **Standalone Protected VMs** subpane, which were a part of the protection group. See Recovering Virtual Machines, on page 182 for more details.

Planned Migration Workflow

Performing planned migration pauses the replication schedule, replicates the most recent copy, recovers on the target, switches the ownership from the source to the target, and resumes replication on the target that is now the new source.

Use the following procedure to migrate the protected VM from the source to the target. At the end of the migration process, the same schedule will be used and the direction of protection is reversed from target to source.

Attention

- This process cannot be rolled back.
- For successful mapping of the datastore in the replication network, atleast one snapshot of the source and target cluster is required.

Step 1 Log in to HX connect of the source and the target. The target cluster is where the replication snapshots were copied to. The source cluster is the cluster where the virtual machines reside.

Step 2 Using the WebCLI, run the following command to prepare for failover on the source:

```
# stcli dp vm prepareFailover -vmid <VMID>
```

Result: The task ID is returned.

The source VMs are powered off and the final differences are replicated. The protection status changes to **Recovering**.

Step 3 Using the WebCLI, monitor the status of prepareFailover task:

```
stcli dp vm hxtask -vmid <VMID> -id <task id>
```

Use the task ID from the previous step.

Step 4 Select a VM from the remote VM list. Execute Recover VM on this cluster workflow.

Note If both the target and source clusters are on the same vCenter, then unregister the VM on the source cluster. This ensures that vCenter no longer has a record of the VM and it stops managing the VM, but it retains the data for the VM.

Step 5 Select **Replication >** > **Remote VMs tab > >** ***protected_vm*** and click **Recover**.

Step 6 To recover on the target VM and build a new VM on the local cluster, click the **Recover VM** button.

Complete the following fields in the **Recover VM on this cluster** dialog box.

UI Element	Essential Information
Resource Pool drop-down list	Select a location for the new VM to be stored.
Folders drop-down list	Select a location for the new VM to be stored.
Power On/Off radio button	By default Power ON option is selected. The recovered VM is powered on or left off after it is created as per the selected option.

UI Element	Essential Information
Map Networks	Select to create a map between the source and target cluster networks. • Source Network—Network name at the source side on which the VM is connected. • Target Network—Select target network from the drop-down list, where the VM has to be connected. Network options for example: • Storage Controller Data Network • Storage Controller Management Network • Storage Controller Replication Network • VM Network

Step 7 Click **Recover VM**.

Step 8 Execute the following command on the source cluster to unregister the source VM and transfer the VM ownership:

```
stcli dp vm prepareReverseProtect –vmid <VMID>
```

Result: The task ID is returned.

Protection status of the VM shows as **Protecting**.

Step 9 Using the WebCLI, monitor the status of preparereverseProtect task:

```
stcli dp vm hxtask -vmid<VMID> -id <task id>
```

Use the task ID from the previous step.

Step 10 Execute the following command on the target cluster:

```
stcli dp vm reverseProtect –vmid <VMID>
```

Result: The task ID is returned

Protection status of the VM shows as **Protected**.

Step 11 Using the WebCLI, monitor the status of reverseProtect task:

```
stcli dp vm hxtask -vmid <VMID> -id <task id>
```

Use the task ID from the previous step.

Unplanned Migration Workflow

Performing unplanned migration recovers the VM on the target, switches the ownership from the source to the target, and resumes replication on the target that is now the new source.

Unplanned migration is typically done when disaster occurs, and when you want to reverse the direction of protection.

⚠

Attention This process cannot be rolled back.

Step 1 Log in to HX connect of the source and the target. The target cluster is where the replication snapshots were copied to. The source cluster is the cluster where the virtual machines reside.

Step 2 Select a VM from the remote VM list. Execute Recover VM on this cluster workflow.

Note If both the target and source clusters are on the same vCenter, then unregister the VM on the source cluster. This ensures that vCenter no longer has a record of the VM and it stops managing the VM, but it retains the data for the VM.

Step 3 Select **Replication >** > **Remote VMs tab >** > ***protected_vm*** and click **Recover**.

Step 4 To recover on the target VM and build a new VM on the local cluster, click the **Recover VM** button.

Complete the following fields in the **Recover VM on this cluster** dialog box.

UI Element	Essential Information
Resource Pool drop-down list	Select a location for the new VM to be stored.
Folders drop-down list	Select a location for the new VM to be stored.
Power On/Off radio button	By default Power ON option is selected. The recovered VM is powered on or left off after it is created as per the selected option.
Map Networks	Select to create a map between the source and target cluster networks. • Source Network—Network name at the source side on which the VM is connected. • Target Network—Select target network from the drop-down list, where the VM has to be connected. Network options for example: • Storage Controller Data Network • Storage Controller Management Network • Storage Controller Replication Network • VM Network

Step 5 Click **Recover VM**.

Step 6 Execute the following command on the source cluster to unregister the source VM and transfer the VM ownership:

```
stcli dp vm prepareReverseProtect -vmid <VMID>
```

Result: The task ID is returned.

Protection status of the VM shows as **Protecting**.

Step 7 Using the WebCLI, monitor the status of preparereverseProtect task:

```
stcli dp vm hxtask -vmid<VMID> -id <task id>
```

Use the task ID from the previous step.

Step 8 Execute the following command on the target cluster:

```
stcli dp vm reverseProtect -vmid <VMID>
```

Result: The task ID is returned

Protection status of the VM shows as **Protected**.

Step 9 Using the WebCLI, monitor the status of reverseProtect task:

```
stcli dp vm hxtask -vmid <VMID> -id <task id>
```

Use the task ID from the previous step.

Protecting Virtual Machines After Disaster

In the event of a disaster, you may lose the source site altogether. After the recovery is performed, you may want to protect the recovered VMs to a newer cluster.

Step 1 Recover the Virtual Machines. Perform standalone recovery (Recovering VMs) or group recovery (Recovering VMs in protection groups). See Recovering Virtual Machines, on page 182 for more details.

Step 2 Forget the pairing, run the following command in the HX Connect WebCLI:

```
stcli dp peer forget --all
```

Now the cluster is no longer paired to the original source.

Step 3 Unprotect all the local and remote VMs. See Unprotecting Virtual Machines, on page 179 for more details.

Step 4 Pair to the new cluster. See the *Creating a Replication Pair* section for more details.

Step 5 Protect the virtual machines.

Failback Virtual Machines

Failback is the process that is used to migrate virtual machines back to their original source.

Failback can be done in the following scenarios:

Scenario 1 - During Maintenance Window

1. Perform planned migration from the source to the target.
2. Perform planned migration from the new source to the newer target.

See Planned Migration Workflow, on page 183 for more details.

Scenario 2- After a Disaster Incident

1. Perform unplanned migration from the source to the target. See Unplanned Migration Workflow, on page 185 for more details.
2. Perform planned migration from the new source to the newer target. See Planned Migration Workflow, on page 183 for more details.

Replication Maintenance

Replication Maintenance Overview

Replication, when configured, runs in the background as per the defined schedule. Replication maintenance tasks include:

- **Testing recovery—**Testing if the recovery methods are working. See Testing Virtual Machine Recovery, on page 180 for more details.
- **Pausing replication—**When you are preparing to upgrade the HX Storage Cluster and you have replication configured, you must pause the replication activity.

  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. See Planned Migration for more details.

Pausing Replication

Before you perform a storfs or platform upgrade, if replication is configured in the network, you must pause the replication activity.

Step 1 Log in to a Storage Controller VM.

Step 2 From the command line, run the `stcli dp schedule pause` command.

Step 3 Perform your upgrade task.

Step 4 Resume the replication schedule.

Resuming Replication

After successfully upgrading the HX Storage Cluster which had replication configured, do the following to 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.

CHAPTER 15

Managing Users

Managing Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco 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.

HX Interface	admin	root	*hx_admin*	*hx_readonly*
HX Data Platform Installer	Required	Optional	Not valid	Not valid
HX Connect	Can perform most HX tasks. `local/` prefix required for login. Example: `local/admin`	Not valid	Can perform most HX tasks. A preferred user.	Can only view monitoring information. Cannot perform HX tasks. A preferred user.

HX Interface	admin	root	*hx_admin*	*hx_readonly*
Storage Controller VM with `stcli` command line	Can perform most HX tasks.	Can perform most HX tasks.	Can perform most HX tasks. `vc-` prefix required for login. Example: `vc-hx_admin`	Can only run non-interactive `stcli` commands to view status. Cannot perform HX tasks. `vc-` prefix required for login. Example: `vc-hx_readonly`
HX Data Platform Plug-in through vCenter	Can perform most HX tasks.	Can perform most HX tasks.	Can perform most HX tasks. A vCenter SSO user.	Can only view vCenter information. Cannot view HX Data Platform Plug-in. A vCenter SSO user.
HX REST API	Can perform most HX tasks. `local/` prefix required for login. Example: `local/admin`	Can perform most HX tasks. `local/` prefix required for login. Example: `local/root`	Can perform most HX tasks. `vc-` prefix required for login. Example: `vc-hx_admin`	Can only run status level REST APIs. Cannot perform HX tasks. `vc-` prefix required for login. Example: `vc-hx_readonly`

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 Cisco HX Connect or other Cisco 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, or Rename a datastore.
- **Resource—**The entire Cisco 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, or Resource Pool Administrator. Role is assigned to a given Identity.

Audit Logs for AAA Accounting

To support AAA accounting, Cisco 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 Cisco HX Connect.

- **stMgrAudit.log—**Contains audit recoreds 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 Cisco HX Data Platform RBAC Users

Cisco 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 18 for user name and password requirements.

What to do next

Add the user to an RBAC role group. See Assigning Users Privileges, on page 194.

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 the Cisco 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.