Cisco HyperFlex Systems Upgrade Guide for VMware ESXi, Release 5.5

First Published: 2023-08-22

Last Modified: 2023-09-27

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

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

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

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

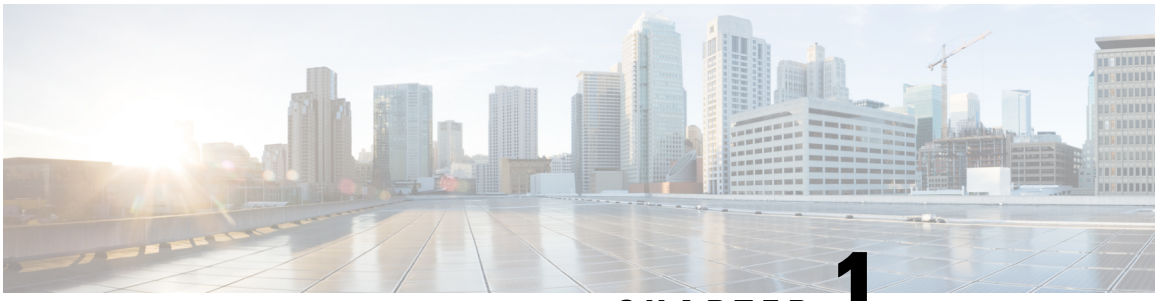
Cisco Bug Search Tool

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

Bias-Free Language

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

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



CHAPTER 1

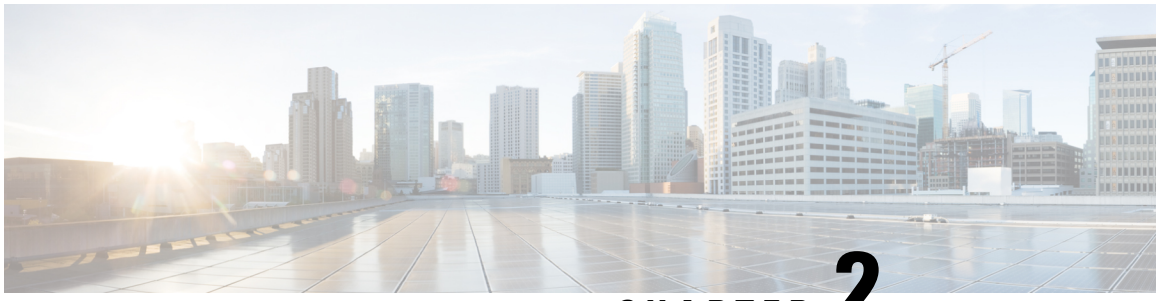
New and Changed Information

New and Changed Information

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

Feature	Description	HX Release or Date Added	Where Documented
Cisco HyperFlex Systems Upgrade Guide for VMware ESXi	First release of the 5.5(x) guide	HX 5.5(1a)	n/a

New and Changed Information



CHAPTER 2

Overview

About this Guide

This document is designed to guide Cisco HyperFlex (HX) users who are currently running HX Release 3.5(1a) or later and want to upgrade their environment to a more recent HX release.

If your cluster is managed by Intersight, please refer to Upgrading Cisco HyperFlex Edge Systems with Cisco Intersight.

On-premises HyperFlex upgrade:

- HyperFlex Data Platform Upgrades using HyperFlex Connect
- HyperFlex Edge Upgrades
- Upgrades for HyperFlex Stretched Clusters
- Split upgrade procedures

Determining the Correct Upgrade Path for my HX Deployment

Note Upgrades from HXDP Release 5.5(x) and earlier, should upgrade using the installer based upgrade.

Many of the upgrade tasks are the same for Edge and Stretched Cluster configurations, but there are differences that should be noted. Use the information below to navigate through this document based on your specific configuration.

1. Select the Cisco HyperFlex Data Center release currently running in your environment and follow the upgrade workflow for your specific upgrade.

Cisco HyperFlex Data Center release currently running in your environment	Cisco Upgrade Guide	Supporting Upgrade Videos
Cisco HX Release 4.5(2x) or 5.0(2x) and later.	Cisco HyperFlex System Upgrade Guide for VMware ESXi (this guide). Continue to the next table to select your Deployment type.	-
Cisco HX Release 3.5(2x), 4.0(x), 4.5(1x) or 5.0(1x) [1]	Cisco HyperFlex System Upgrade Guide for VMware ESXi (this guide). Continue to the next table to select your Deployment type.	-
Cisco HX Release 3.5(1x) and earlier	Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases	Cisco Communities Data Center Videos

[1] These releases have reached the end of their support, but the Cisco HyperFlex System Upgrade Guide for VMware ESXi (this guide) provides the proper upgrade workflow.

2. Verify the minimum supported version of ESXi (vSphere) for your target upgrade release, then proceed to step 3.

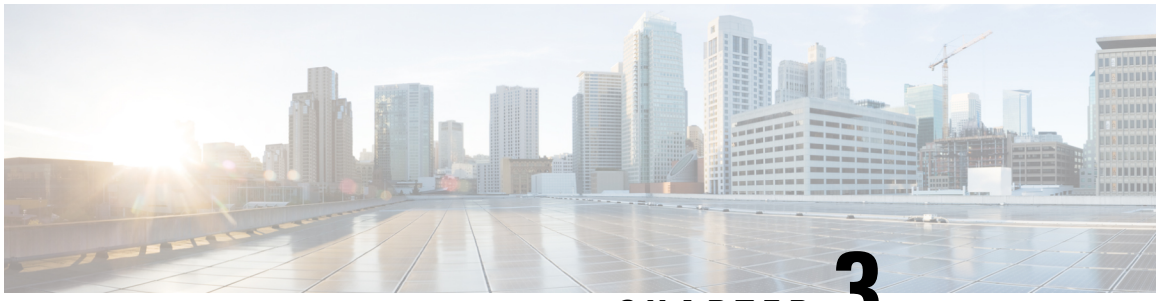
Target Release	Minimum Supported Version of ESXi (vSphere)
3.5(1a) - 4.0(2x)	6.0 U3
4.5(1a) -5.0(2x)	6.5 U3
5.5(x)	7.0 U2
6.0(1a) and later	7.0 U2

3. Select your deployment type:

Deployment Type	Link to chapter in this guide
Classic HyperFlex Deployment	Prerequisites for Upgrading HyperFlex Software, on page 7
HyperFlex Edge Deployment	HyperFlex Edge Upgrade Overview, on page 35
HyperFlex Edge Upgrade through Intersight	Upgrading Cisco HyperFlex Edge Systems with Cisco Intersight
HyperFlex Stretched Clusters	Stretched Cluster Upgrade Overview, on page 43

Upgrading from an Unsupported Cisco HyperFlex HX Data Platform Software Release

Cisco HyperFlex users who need to upgrade their environment from a Cisco HyperFlex HX Data Platform software release that is past the last date of support, to the latest suggested release on the Cisco Software Download site, should follow the upgrade steps for their current release as defined in the Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases Guide. The steps in this guide are not applicable for clusters running older software



CHAPTER 3

Prerequisites and Guidelines

Prerequisites for Upgrading HyperFlex Software

The following tasks should be performed prior to beginning the upgrade process:

Important Using VMware Update Manager (VUM) or VMware Lifecycle Manager (vLCM) for upgrading the ESXi on HyperFlex node is not supported. Using these upgrade methods may delete Cisco custom drivers and cause cluster outages. We recommend using Cisco Intersight or HyperFlex Connect for ESXi upgrades including the security patches from VMware or manually installing patches using the offline zip bundle with ESXCLI commands.

- Ensure Storage I/O Control (SIOC) is completely disabled on each HyperFlex datastore and the local datastore on each ESXi host in the HyperFlex cluster. This can be confirmed through the vCenter Web Client:

  Datastores -> <datastore name> -> Configure -> General -> Datastore Capabilities -> Storage I/O Control -> Verify > both **Status** and **Statistics Collection** is set to **Disabled**.

Note Please refer to the VMware documentation site for more details and steps to disable SIOC.

Datastore Requirements:

- Clusters running HXDP Release 4.5(2a) or later can upgrade directly to 6.0(1a).
- Clusters running HXDP Release 4.0(2x) through 4.5(1x) can upgrade directly to 5.5(1a).
- HXDP Release 5.5(x) supports ESXi version 7.0 U2, 7.0 U3 and 8.0 U1 and later only. If your current ESXi version is earlier than 7.0 U2, make sure to perform a combined upgrade of HXDP and ESXi to a target level 7.0 U2 or later.

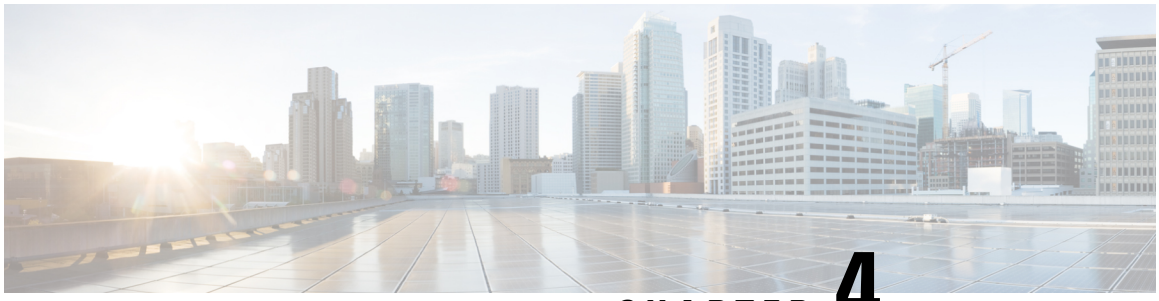
- If the HXDP is already upgraded to 5.5(x) and an ESXi upgrade is attempted from 7.0 to 8.0, user needs to upload HXDP bundle and select HXDP along with the target ESXi 8.0 bundle.
- Migrate all M4 nodes to HyperFlex M5 or higher before attempting to upgrade to HXDP Release 5.5(x). Attempts to upgrade to HXDP Release 5.5(x) with HyperFlex M4 nodes in your cluster will fail.
- Review the Cisco HyperFlex Upgrade Guidelines in the Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems.
- Beginning with Cisco HXDP Release 5.0(2a), full feature functionality and configuration changes require a valid Cisco HyperFlex Software License. HX Connect users with expired or insufficient licenses at the end of the evaluation or the grace period after the license compliance date, view a prominent countdown banner that alerts the user to the license compliance need and provides a link to the license renewal page until the license expiration is remedied.

  In the event a license passes both the license expiration date and the grace period countdown, the current configurations will operate as expected with limited information. Renewing the license allows a user to resume full feature functionality, and make configuration changes. For details and examples of the banners, see the License Compliance and Feature Functionality section of the Cisco HyperFlex Systems Ordering and Licensing Guide.
- **SCVM Support**
  - SCVM VMware Tools upgrade: not supported
  - SCVM Hardware Version upgrade: not supported
  - SCVM VMware Tools are used when creating HX native snapshots using the quiesce option.
- vCenter version check: Verify that the vCenter meets the minimum requirement for the ESXi version being upgraded to. See, VMware Product Interoperability Matrices to ensure compatibility between vCenter and ESXi.
- Ensure all VM network port groups exist on all nodes in the cluster for vMotion compatibility.
- Ensure that the management and storage data VLANs are configured on the top-of-rack network switches to ensure uninterrupted connectivity during planned fabric failover.
- If using jumbo frames in your environment, ensure jumbo frames are enabled on the vMotion and data networks on the top of rack switch.
- Verify that the ESXi hosts are not in lockdown mode and SSH service is enabled and set to start and stop with the host for the duration of the upgrade. Lockdown mode can be re-enabled after the upgrade is complete along with disabling SSH service.
- Blade Package and Rack Package versions are not displayed in the Host Firmware Package: **HyperFlex-m5-con** and **HyperFlex-m6-con** for M6 nodes.
- Upgrading the VM compatibility version or hardware version of the Storage Controller Virtual Machine (SCVM) is not supported and should not be performed. This action is detrimental to the SCVM and will require a rebuild of the SCVM if performed.

Upgrade Recommendations

For upgrading supported releases, see the Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems.

If you want to upgrade from a release that is no longer supported, see the Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases.



CHAPTER 4

Pre-Upgrade Intersight Health Check

Run the Health Check via Intersight

To better ensure a complete HyperFlex upgrade, it is essential to verify that the HyperFlex clusters you intent to upgrade are healthy before starting the upgrade process. The Health Check in Intersight allows you to view details and reports about the health of your HypeFlex clusters. To get started, continued to the Intersight Help Center "**Health Check for HyperFlex Clusters**.

Test Upgrade Eligibility

Beginning with Cisco HyperFlex Release 4.0(2a), the Upgrade page displays the last cluster upgrade eligibility test result and last tested version of UCS server, HX data platform, and/or ESXi.

Before upgrading UCS server firmware, HyperFlex data platform, and/or ESXi, perform upgrade eligibility test in the Upgrade page to validate and check the cluster readiness and the infrastructure compatibility for an upgrade.

Note The Upgrade Eligibility test uses the validations included in the current running HyperFlex Data Platform version. It does not include newer validations that are present in the target HX version.

To perform upgrade eligibility test:

1. Select **Upgrade** > **Test Upgrade Eligibility**.
2. Select the **UCS Server Firmware** check box to test upgrade eligibility of UCS server firmware.

   Enter the Cisco UCS Manager FQDN or IP address, username, and password. In the **Current Version** field, click **Discover** to choose the UCS firmware package version that need to be validated before upgrade.
3. Select the **HX Data Platform** check box to test upgrade eligibility of HyperFlex Data Platform.

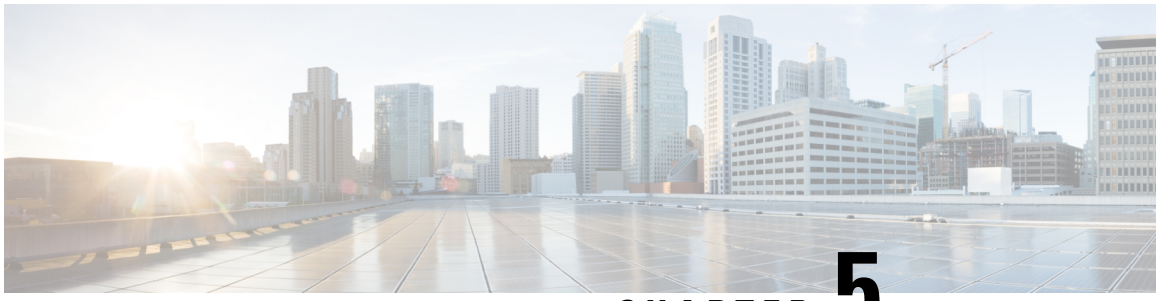
   Enter the vCenter username and password. Upload the Cisco HyperFlex Data Platform Upgrade Bundle that need to be validated before upgrade.

4. Select the **ESXi** check box to test upgrade eligibility of ESXi.

   Enter the vCenter username and password. Upload the Cisco HyperFlex Custom Image Offline Bundle that need to be validated before upgrade.

5. Click **Validate**.

   The progress of the upgrade eligibility test is displayed.



CHAPTER 5

Preparing for Upgrade

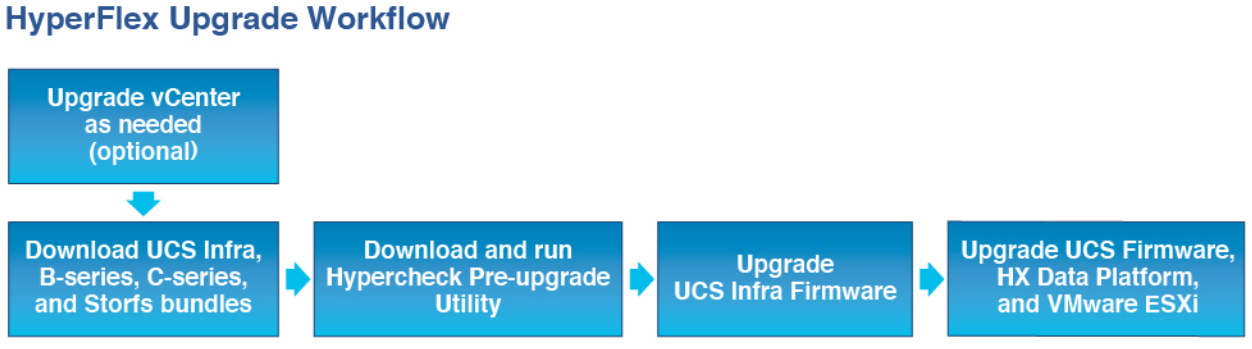
HyperFlex Upgrade Preparation

Note The following upgrade process only applies to when a user is upgrading from Cisco HX Release 3.5(2x) or later.

Note If you are upgrading one of the following rather than a HyperFlex standard cluster:

- For HyperFlex Edge clusters, see HyperFlex Edge Upgrade, on page 35.
- For Stretched clusters, see Stretched Cluster Upgrade, on page 43.
- For split-upgrade procedures, see HyperFlex Offline Upgrade Workflow , on page 51.

The following image describes the general upgrade workflow for a full-stack HyperFlex standard cluster.



The upgrade requires you to complete the following tasks in this order:

1. Complete all tasks in the Prerequisites section of this guide.
2. Run the Hypercheck Health & Pre-Upgrade tool to on your HyperFlex systems to ensure its stability and resiliency Hypercheck : Hyperflex Health & Pre-Upgrade Check Tool
3. Verify that your VMware vCenter version is 7.0 U2, 7.0 U3, or 8.0 or later and that vCenter and your target ESXi version are compatible. See, *VMware Product Interoperability Matrices* on the VMware site. Also, verify the vCenter version is compatible with the target HXDP version.

Checking Cluster Storage Capacity

Cisco recommends that you check the cluster storage capacity before starting the upgrade of an existing installation of Cisco HX Data Platform. If the storage utilization in the cluster is equal to 76% or more (capacity + overhead), the upgrade validation fails.

Refer to the *HX Storage Cluster Overview* chapter in the Cisco HyperFlex Data Platform Administration Guide for background details about checking cluster storage capacity.

Perform the following validations on each HyperFlex node before starting the upgrade.

- Verify that the HyperFlex cluster is healthy and online.
- Verify all HyperFlex cluster nodes are connected to the vCenter and are online.
- Verify that DRS is enabled and set to fully automated if licensed for DRS. If DRS is Disabled, manual intervention is required to vMotion the VMs manually when prompted by the upgrade process.
- Verify vMotion is configured on all the nodes, If vMotion is not configured, see Verify vMotion Configuration for HX Cluster before starting the upgrade.
- Verify that ESXi Agent Manager (EAM) health is normal.
- Verify the health of the UCSM Fabric Interconnect cluster in Cisco UCS Manager.

Verify Health of an UCS Fabric Interconnect Cluster in Cisco UCS Manager

Step 1 Verify if the high availability status of the fabric interconnects shows that both the fabric interconnects are up and running. See the Cisco UCS Manager System Monitoring Guide for more information.

Step 2 Verify that all servers have been discovered.

Step 3 Verify that the HyperFlex servers have no faults.

Step 4 Verify that vNIC faults are cleared to ensure VMware ESXi vSwitch uplinks are up and operational.

Step 5 Verify that the data path is up and running. See the Cisco UCS Manager Firmware Management Guide for more information.

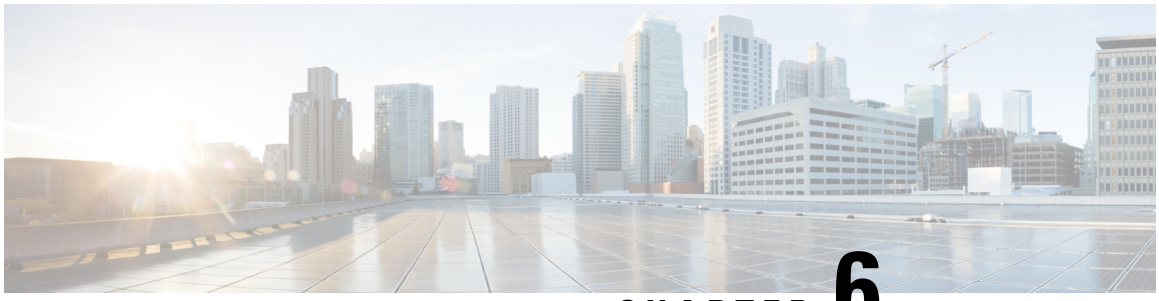
Viewing HyperFlex Cluster Health

Using CLI

Log into any controller VM in the storage cluster. Run the command `hxcli cluster info [flags]`.

```
address: 192.168.100.82
name: HX-Cluster01
state: online
uptime: 0 days 12 hours 16 minutes 44 seconds
activeNodes: 5 of 5
compressionSavings: 78.1228617455
deduplicationSavings: 0.0
freeCapacity: 38.1T
healingInfo:
    inProgress: False
resiliencyDetails:
        current ensemble size:5
        # of ssd failures before cluster shuts down:3
        minimum cache copies remaining:3
        minimum data copies available for some user data:3
        minimum metadata copies available for cluster metadata:3
        # of unavailable nodes:0
        # of nodes failure tolerable for cluster to be available:2
        health state reason:storage cluster is healthy.
        # of node failures before cluster shuts down:3
        # of node failures before cluster goes into readonly:3
        # of hdd failures tolerable for cluster to be available:2
       # of node failures before cluster goes to enospace warn trying to move the existing
 data:na
        # of hdd failures before cluster shuts down:3
        # of hdd failures before cluster goes into readonly:3
        # of ssd failures before cluster goes into readonly:na
        # of ssd failures tolerable for cluster to be available:2
resiliencyInfo:
    messages:
     Storage cluster is healthy.
     state: healthy
     hddFailuresTolerable: 2
     nodeFailuresTolerable: 1
     ssdFailuresTolerable: 2
spaceStatus: normal
totalCapacity: 38.5T
totalSavings: 78.1228617455
usedCapacity: 373.3G
clusterAccessPolicy: lenient
dataReplicationCompliance: compliant
dataReplicationFactor: 3
```

Sample response that indicates the HyperFlex storage cluster is online and healthy.



CHAPTER 6

Download Software Bundles

Downloading Software

For a successful HyperFlex upgrade, the Cisco HyperFlex System component bundles can be downloaded from the Cisco HyperFlex Download website:

Step 1 Navigate to https://www.cisco.com/support and enter **HX Data Platform** in the Select a Product search bar. Click on the HyperFlex HX Data Platform downloads link

Step 2 Click on the current **Suggested Release** version.

Step 3 Click the cart icon for the latest Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing HyperFlex clusters from a previous release (`.tgz` file).

Note Read through any Software Advisories to confirm whether any issues may apply to your environment before proceeding with the download.

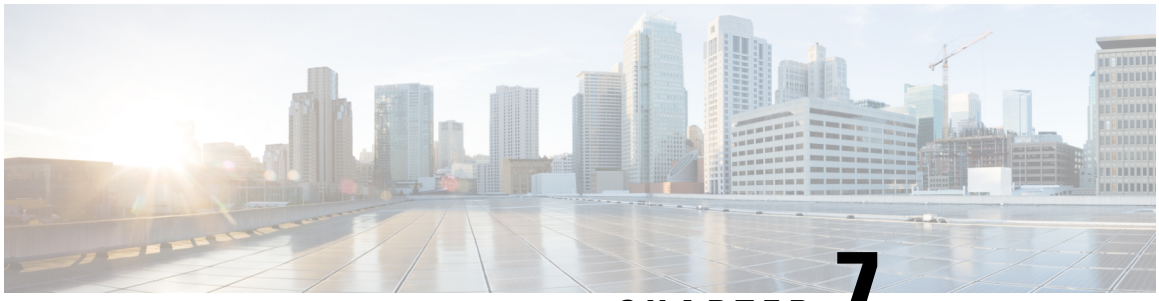
Step 4 Click the cart icon for the corresponding UCS Infrastructure Software Bundle based on the FI model.

Step 5 Click the cart icon for the Software for UCS B-Series and C-Series blade and rack-mounted servers.

Step 6 For upgrading vSphere, click on the cart icon for the latest HX Custom Image for ESXi Offline Bundle for Upgrading from prior ESXi versions.

Step 7 Click on the cart icon at the stop of the screen to confirm the bundles and click **Download All**.

Step 8 Accept the license agreement and click **Ok** for each file to save it.



CHAPTER 7

Upgrade UCS Infrastructure Firmware

Upgrading UCS Infrastructure Firmware Workflow

Upgrade Type	Procedure
HyperFlex Clusters	See the workflow below.
HyperFlex Edge Upgrade Clusters	HyperFlex Edge Upgrade, on page 35
HyperFlex Stretched Clusters	Stretched Cluster Upgrade, on page 43
Split Upgrade Procedures	HyperFlex Offline Upgrade Workflow , on page 51

Perform the following tasks to upgrade UCS Infra Firmware:

- Review Prerequisites for Upgrading HyperFlex Software, on page 7 before beginning upgrade.
- Log into the UCSM Fabric Interconnect cluster IP address.
- Upload the appropriate Infra, B-Series, and C-Series bundles to the Fabric Interconnect.

Guidelines and Limitations

Consider the following before performing the UCS Infra Firmware upgrade:

- Ensure that the hx-storage-data and vMotion upstream switches are configured for **Jumbo Frames** before proceeding forward, otherwise the HyperFlex Cluster could suffer a network and storage outage during the upgrade window.
- You will lose connectivity to UCS Manager throughout the entire UCS infrastructure firmware upgrade. This is normal behavior.
- Verify that the Data path is ready. For for more information, see the Verification that the Data Path is Ready section in the Cisco UCS Manager Firmware Management Guide..

Upgrade UCS Infrastructure Firmware

Before you begin

Download the Infra, B-Series, and C-Series Fabric Interconnect upgrade bundles. For details, see Downloading Software, on page 17.

Step 1 Log on to UCS Manager to the Fabric Interconnect cluster IP address using admin privileges.

Step 2 Navigate to **Equipment** > **Firmware Management** > **Installed Firmware**.

Step 3 Expand **UCS Manager** and confirm the UCS Manager running version.

Step 4 Navigate to **Download Tasks** > **Download Firmware**.

Step 5 Browse to your saved Fabric Interconnect bundles and select the Infra A, B-Series, and C-Series bundles you previously saved click **Open** and **OK**.

Step 6 Once the files have transferred, click on **Firmware Auto Install** and then **Install Infrastructure Firmware** under **Actions**.

Note Review carefully all warnings and resolve any issues if required before proceeding.

Step 7 Once any issues are resolved (if any) select **Ignore All** and click **Next**.

Step 8 Select the appropriate **Infra Pack** from the drop-down and check **Upgrade Now** and click **Finish**.

Note You can click **Yes** to disregard the warning for the Service Pack not being selected.

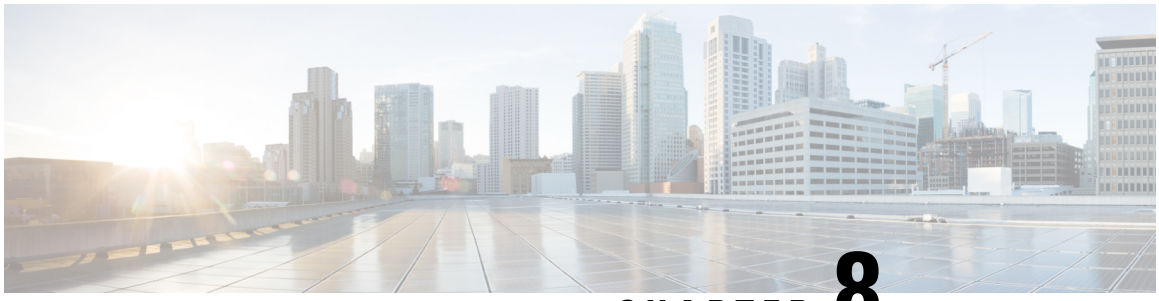
Step 9 Click on the **FSM** tab to follow the upgrade progress. The upgrade takes some time to proceed.

Step 10 Click on the **Pending Activities** tab at the top and then **Fabric Interconnects** to verify that the data path is successfully restored from the Secondary Fabric Interconnect before you acknowledge the reboot of the Primary Fabric Interconnect.

Step 11 Click **Reboot Now** and then click **Yes** and **OK**.

Note During the course of the upgrade process, you will be logged out of the Fabric Interconnect UI. Log back into view the upgrade progress.

Step 12 Once the Upgrade process is completed, view the updated versions on the **Installed Firmware** tab.



CHAPTER 8

Upgrade UCS Server Firmware, HX Data Platform and VMware vSphere - Combined Upgrade

Upgrade Cisco UCS Firmware, HX Data Platform, and VMware vSphere Workflow

The Cisco HyperFlex “full-stack” upgrade process involves upgrading the following 3 components:

- Cisco HyperFlex Data Platform
- VMware vSphere ESXi
- Cisco UCS Server Firmware

Cisco recommends upgrading all these 3 components in a combined upgrade from HyperFlex Connect. You can choose to upgrade one, two or all three components in the same upgrade workflow. If you are combining two or more components in a single upgrade process, follow the procedure below. Otherwise, navigate to Chapter 9 for individual component upgrade procedures.

This section describes the steps to perform a combined upgrade of HyperFlex Data Platform Software, VMware ESXi, and UCS Server firmware . In this process, the HyperFlex nodes will go through an optimized rolling reboot without any workload disruptions, by use of VMware vMotion.

Note As part of the Server Firmware upgrade operation initiated from HX Connect, some of the UCS policies may be updated to be compatible with the new HXDP version. These changes are applied only to the nodes that are part of the cluster being upgraded. It is highly recommended to use HX Connect to initiate the Server Firmware upgrade to avoid any policy drift.

Upgrade Type	Procedure
HyperFlex Clusters	See the workflow below.

Upgrade Type	Procedure
HyperFlex Edge Clusters	HyperFlex Edge Upgrade, on page 35
HyperFlex Stretched Clusters	Stretched Cluster Upgrade, on page 43
Split Upgrade Procedures	HyperFlex Offline Upgrade Workflow , on page 51

Perform the following tasks to upgrade UCS Firmware and HX Data Platform:

- Review Prerequisites for Upgrading HyperFlex Software, on page 7 before beginning upgrade.
- Log into HX Connect with admin privileges.
- Select the appropriate options from the Upgrade page.
- Upload the required files and complete the necessary user inputs.

Guidelines and Limitations

Consider the following before performing the upgrade:

- If DRS is *Enabled* and set to fully automatic mode, the VMs are automatically vMotioned to other hosts during the rolling upgrade process.

Note If DRS is *Disabled*, vMotion the VMs manually to continue the upgrade process when prompted. For more information, see VMware Documentation for Migration with vMotion.

- Downgrading ESXi and HXDP is not supported.
- Refer to the Release Notes for software compatibilities of HXDP, UCS firmware, and VMware ESX. Additionally, ensure vCenter is upgraded to a compatible version before upgrading ESXi. For details, see the Cisco HyperFlex Release Notes that correspond with your installation,Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems, and the *VMware Product Interoperability Matrix* on the VMware site.
- Do not manually upgrade UCS server firmware using the tools available in UCS Manager. Changes to policies in UCS Manager for HyperFlex servers are delivered through the orchestrated server firmware upgrade process. Manually performing firmware updates out of band will result in these important configuration updates being missing.

Upgrading HyperFlex Data Platform Software, VMware ESXi, and Cisco UCS Server Firmware using HX Connect

Before you begin

- Download the latest Cisco HX Data Platform Upgrade Bundle for upgrading existing clusters from previous release, from Downloading Software.
- Download the appropriate HX custom ESXi offline upgrade bundle from https://www.cisco.com/.
- Disable snapshot schedule, on the storage controller VM. SSH to HyperFlex cluster IP and run the command `stcli snapshot-schedule -disable` snapshot schedule.

Step 1 Log into HX Connect.

a) Enter the administrative username and password.

b) Click **Login**.

Step 2 In the Navigation pane, select **Upgrade**.

Step 3 On the **Select Upgrade Type** page, select **HX Data Platform**, **ESXi**, and **UCS Server Firmware** and complete the following fields:

Field	Essential Information
UCS Manager Connectivity	
UCS Manager FQDN/IP	Enter the Cisco UCS Manager FQDN or IP address. Example: 10.193.211.120.
User Name	Enter the Cisco UCS Manager <admin> username.
Admin Password	Enter the Cisco UCS Manager <admin> password
HX Server Firmware	
Discover	Click **Discover** to view the current UCS firmware package version.
M5/M6 Desired Version (Depending on the nodes in the cluster)	Select the appropriate C-Series firmware versions. Optionally, if you have Compute only B-Series UCS blades in the cluster select the appropriate B-Series firmware version. Only C & B bundles uploaded to UCS Manager will be shown in the list. Return to Upgrading UCS Infrastructure Firmware Workflow, on page 19 if the desired version is not shown. Only compatible firmware versions are shown in the dropdown list. If the desired version is not displayed, confirm the compatibility between HXDP & Server Firmware in the Cisco HyperFlex Software Requirements and Recommendations document.

Note If the UI doesn't show your desired UCS server firmware version in dropdown, see HX Connect UCS Server Firmware Selection Dropdown Doesn't List the Firmware Version 4.1 or Above, on page 58.

Step 4 Upload the HyperFlex Data Platform upgrade package (storfs-package).

Field	Essential Information
Drag the HX file here or click to browse	Upload the latest Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing clusters with previous release.tgz package file from Download Software -HyperFlex HX Data Platform. Sample file name format: `storfs-packages-4.5.1a-31601.tgz`.
Current version	Displays the current HyperFlex Data Platform version.
Current cluster details	Lists the HyperFlex cluster details like the **HyperFlex release**and **cluster upgrade state**.
Bundle version	Displays the HyperFlex Data Platform version of the uploaded bundle.
(Optional) **Checksum**	The MD5 Checksum number is available by hovering over the filename in the Cisco.com Software Download section. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle

Step 5 Upload the ESXi offline upgrade bundle.

Step 6 Provide vCenter login credentials.

Field	Essential Information
User Name	Enter the vCenter <*admin*> username.
Admin Password	Enter the vCenter <*admin*> password.

Step 7 Click **Upgrade** to begin the first step of the combined upgrade process.

Step 8 The **Validation Screen** on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any.

Note At this point, all pre-upgrade checks and validations will run, along with the initial upgrade stage. Within a few minutes, HX Connect returns and prompts the user to confirm and start the second stage of the upgrade. The upgrade is not complete until both steps are performed in the UI. The system should never be left in a state where only the first step of the upgrade is complete.

Note Do not manually acknowledge servers in UCS Manager. While the servers enter a pending-ack state, the administrator should not manually intervene. The HyperFlex platform will automatically acknowledge each server at the correct time.

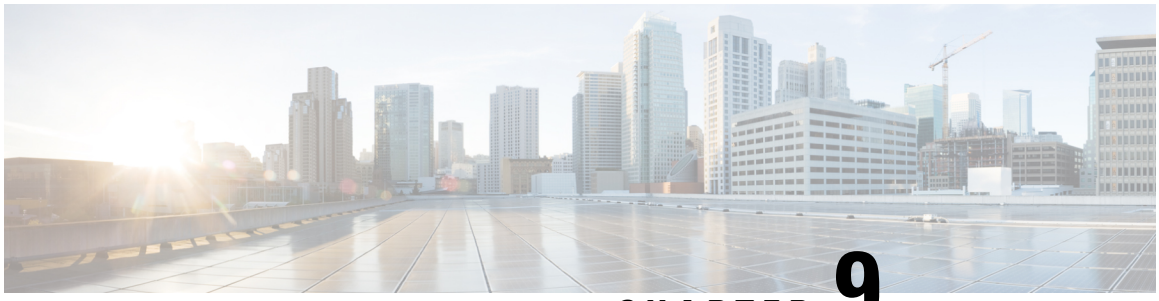
Note As of HX 5.0(1b), an upgrade status appears providing the result of the last upgrade along with the versions that were upgraded (source and target versions for each component selected in the upgrade). You can dismiss this status only if it is successful. If the last upgrade fails, you will need to fix the issue. This banner is a reminder to take action to correct the upgrade.

Step 9 The HyperFlex Connect UI refreshes after the first step of the upgrade, and a banner pops up prompting you to provide the UCS and vCenter credentials and start the second stage of the upgrade process. Monitor the upgrade page and confirm that the upgrade is complete.

When upgrade is in progress, you may see an error message, `Websocket connection failed. Automatic refresh disabled`. You can either refresh the page or log out and log back in to clear the error message. You can safely ignore this error message.

What to do next

Proceed to Confirm That Upgrade Is Complete, on page 33 for post upgrade tasks once the upgrade is complete. If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance. Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.



CHAPTER 9

Upgrade UCS Firmware, HX Data Platform and VMware vSphere - Individual Component Upgrade

Overview

Cisco recommends upgrading all these 3 components in a combined full-stack upgrade from HyperFlex Connect. You can choose to upgrade one, two or all three components at a time. If you are combining 2 or more components in a single upgrade process, follow procedures described in the previous chapter. Otherwise, follow below procedures for individual component upgrade one at a time.

Cisco HyperFlex Data Platform Upgrade

Before you begin

- Download the latest *Cisco HX Data Platform Upgrade Bundle for upgrading existing clusters from previous releases*, from Downloading Software, on page 17.
- Disable snapshot schedule, on the storage controller VM. SSH to the HyperFlex cluster IP and run the command `stcli snapshot-schedule -disable` snapshot schedule.

Step 1 Log into HX Data Platform.

a) Enter the administrative username and password.

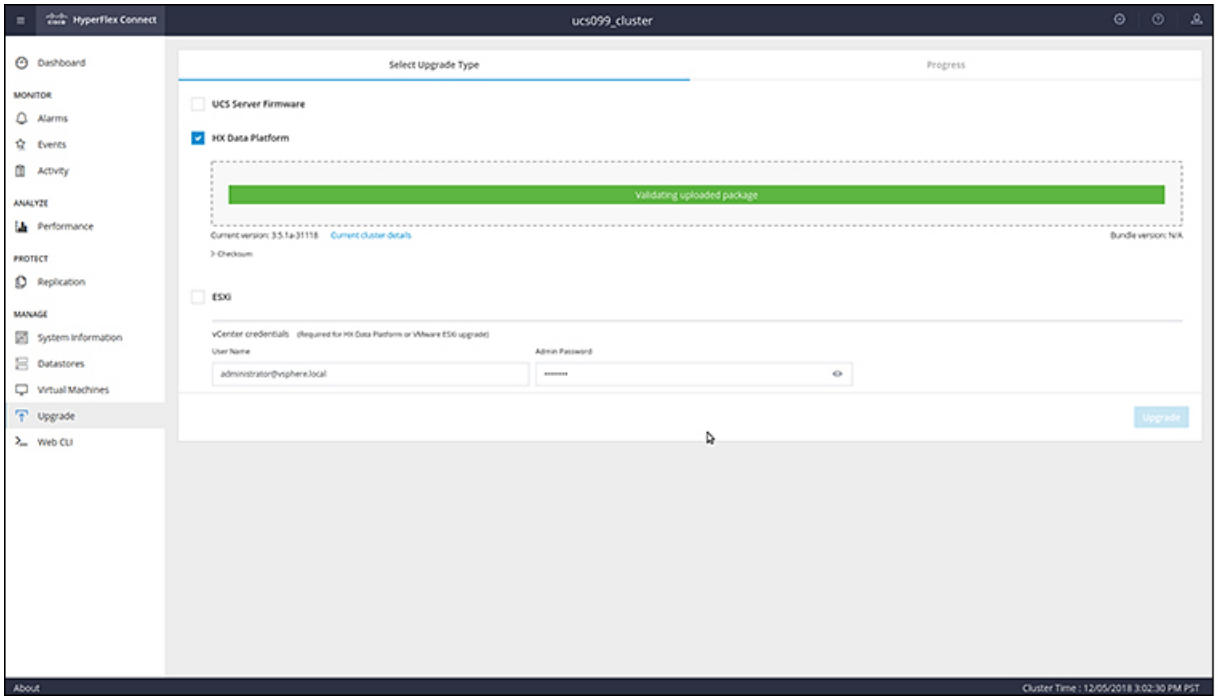
b) Click **Login**.

Step 2 In the Navigation pane, select **Upgrade**.

Step 3 On the **Select Upgrade Type** page, select **HX Data Platform** and complete the following fields:

UI Element	Essential Information
Drag the HX file here or click to browse	Upload the latest *Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing clusters with previous release.tgz* package file from Download Software - HyperFlex HX Data Platform. Sample file name format: *storfs-packages-4.5.1a-31601.tgz*.
(Optional) **Checksum** field	The *MD5 Checksum number* is available by hovering over the filename in the Cisco Software Download section. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle.

Figure 1: Select Upgrade Type Page



Step 4 Enter the **vCenter credentials**.

UI Element	Essential Information
User Name field	Enter the vCenter <*admin*> username.
Admin Password field	Enter the vCenter <*admin*> password.

Step 5 Click **Upgrade** to begin the cluster upgrade process.

Step 6 The Validation screen on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any.

Note At this point, all pre-upgrade checks and validations are run, along with the initial upgrade stage. Within a few minutes, HX Connect returns and prompts you to confirm and start the second stage of the upgrade. The upgrade is not complete until both steps are performed in the UI. The system should never be left in a state where only the first step of the upgrade is complete.

Step 7 The HyperFlex Connect UI refreshes after the first step of the upgrade, and a banner pops up prompting you to provide the UCS and vCenter credentials and start the second stage of the upgrade process. Monitor the upgrade page and confirm that the upgrade is complete.

When upgrade is in progress, you may see an error message **Websocket connection failed. Automatic refresh disabled**. You can either refresh the page or log out and log back in to clear the error message. You can safely ignore this error message.

What to do next

Proceed to Confirm That Upgrade Is Complete, on page 33 for post upgrade tasks once the upgrade is complete. If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance.

Note Running a cluster without remediation after an upgrade failure is not recommended. Care should be taken to fully complete the upgrade as soon as possible.

Cisco HXDP Upgrade using HX Installer

The ability to upgrade HXDP and ESXi (optional) using the HX Installer was introduced in Cisco HyperFlex Release 6.0(1a).

Perform the following steps to upgrade HXDP and (optional) ESXi using the HX Data Platform Installer (OVA).

Before you begin

- Download the HXDP bundle from CCO https://software.cisco.com/download/home/286305544/type/286305994/.

SUMMARY STEPS

1. Log in to the HX Data Platform Installer.
2. Follow the **Upgrade Cluster** workflow for a standard cluster.
3. On the **Credentials** view, type your vCenter and Hypervisor credentials in the field boxes for the cluster you intend to upgrade. Use the eye icon to show or hide the passwords.
4. Click the **Continue** button to discover the cluster and advance to the **Upgrade Cluster** view.
5. Type the cluster password in the **Password** box and click the **Continue** button.
6. Check the box to start the optional ESXi upgrade on all nodes in the cluster. Once checked, either drag or browse to the local ESXi bundle to the highlighted box.
7. Use the **Test Upgrade Eligibility** button to test the HXDP and ESXi combination.

8. Click the **Upgrade** button to complete the upgrade.

DETAILED STEPS

Step 1 Log in to the HX Data Platform Installer.

Step 2 Follow the **Upgrade Cluster** workflow for a standard cluster.

Step 3 On the **Credentials** view, type your vCenter and Hypervisor credentials in the field boxes for the cluster you intend to upgrade. Use the eye icon to show or hide the passwords.

Step 4 Click the **Continue** button to discover the cluster and advance to the **Upgrade Cluster** view.
The **Select a Cluster to Upgrade** box appears.

Step 5 Type the cluster password in the **Password** box and click the **Continue** button.
The workflow advances to the Optional **ESXi Upgrade Configuration** view.

Step 6 Check the box to start the optional ESXi upgrade on all nodes in the cluster. Once checked, either drag or browse to the local ESXi bundle to the highlighted box.

Step 7 Use the **Test Upgrade Eligibility** button to test the HXDP and ESXi combination.

To validate or upgrade the firmware version, use HX Connect.

Step 8 Click the **Upgrade** button to complete the upgrade.

Cisco UCS Server Firmware Upgrade

Before you begin

- Check and confirm the UCS B-Series and C-Series server firmware packages have been downloaded to the Fabric Interconnects.
- Disable snapshot schedule, on the storage controller VM. SSH to HyperFlex cluster IP and run the command `stcli snapshot-schedule -disable` snapshot schedule.

Step 1 Log into HX Connect.

a) Enter the administrative username and password.
b) Click **Login**.

Step 2 In the Navigation pane, select **Upgrade**.

Step 3 On the **Select Upgrade Type** page, select **UCS Server Firmware**, and complete the following fields:

Field	Essential Information
UCS Manager Connectivity	
UCS Manager FQDN/IP	Enter the Cisco UCS Manager FQDN or IP address. Example: 10.193.211.120.
User Name	Enter the Cisco UCS Manager <admin> username.

Field	Essential Information
Admin Password	Enter the Cisco UCS Manager <admin> password
HX Server Firmware	
Discover	Click **Discover** to view the current UCS firmware package version.
M5/M6 Desired Version(Depending on the nodes in the cluster)	Select the appropriate C-Series firmware versions. Optionally, if you have Compute only B-Series UCS blades in the cluster select the appropriate B-Series firmware version. Only C & B bundles uploaded to UCS Manager will be shown in the list. Return to Upgrading UCS Infrastructure Firmware Workflow, on page 19 if the desired version is not shown. Only compatible firmware versions are shown in the dropdown list. If the desired version is not displayed, confirm the compatibility between HXDP & Server Firmware in the Cisco HyperFlex Software Requirements and Recommendations document.

Step 4 Click **Upgrade** to begin the UCS firmware upgrade process.

Step 5 The **Validation Screen** on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any. Monitor the upgrade page and confirm that the upgrade is complete.

When upgrade is in progress, you may see an error message, `Websocket connection failed. Automatic refresh disabled`. You can either refresh the page or log out and log back in to clear the error message. You can safely ignore this error message.

Note Do not manually acknowledge servers in UCS Manager. While the servers will enter a pending-ack state, the administrator should not manually intervene. The HyperFlex platform will automatically acknowledge each server at the correct time.

VMware vSphere/ESXi Upgrade

Important Using VMware Update Manager (VUM) or VMware Lifecycle Manager (vLCM) for upgrading the ESXi on HyperFlex node is not supported. Using these upgrade methods may delete Cisco custom drivers and cause cluster outages. We recommend using Cisco Intersight or HyperFlex Connect for ESXi upgrades including the security patches from VMware or manually installing patches using the offline zip bundle with ESXCLI commands.

Follow the procedure below to upgrade only VMware ESXi from HyperFlex Connect. This procedure can be followed for ESXi patch upgrades as well.

Upgrading vSphere requires you to complete the following tasks:

- Refer to the release documents for software compatibilities of HXDP, UCS, and VMware and confirm your vCenter is upgraded before you upgrade. For details, see the Release Notes for Cisco HX Data

Platform for your release, Cisco HyperFlex Recommended Software Release and Requirements Guide, and VMware Product Interoperability Matrices.

- Log into HX Connect using admin privileges and navigate to the Upgrade page.

Before you begin

Download the appropriate HX custom ESXi offline upgrade bundle. For details, see Downloading Software, on page 17. Cisco does not recommend use of non-HX customized ESXi bundles, although it is supported. Using HX customized bundles ensures all the latest drivers are updated and compatibility with the HyperFlex hardware.

Step 1 Log into HX Connect with admin privileges.

Step 2 Navigate to the System Information tab and confirm the running Hypervisor version.

Step 3 Click on the Upgrade tab and select **ESXi**.

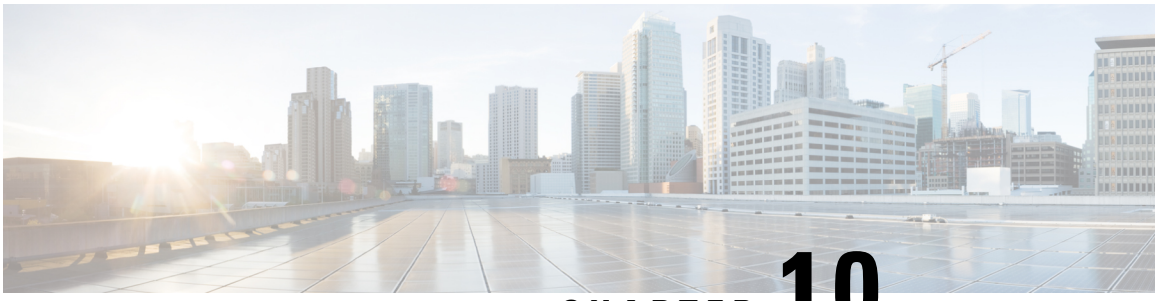
Step 4 Click in the bundle version window and navigate to your previously saved ESXi offline bundle and click **Open**.

Step 5 Once the bundle is uploaded, enter your vCenter credentials and click **Upgrade**.

Note The upgrade process is non-disruptive and upgrades one server at a time.

Step 6 Refresh your browser screen to view the upgrade changes on the Dashboard tab.

Note Click on the System Information tab to confirm that all the nodes are online.



CHAPTER 10

Post Upgrade Tasks

Confirm That Upgrade Is Complete

Step 1 Log into Cisco UCS Manager to ensure that the HX nodes have no pending server activities.

From **Servers tab** > **Servers** > **Pending Activities** tab check for all server activities.

Step 2 Confirm that the HX nodes match the expected firmware version.

In Cisco UCS Manager, from **Equipment** > **Firmware Management** > **Installed Firmware** tab, verify for the correct firmware version.

Step 3 Log into any controller VM through SSH.

```
# ssh admin@controller_vm_ip
```

Step 4 Confirm the HyperFlex Data Platform version.

```
# hxcli cluster version


Cluster version: 5.5(1a)
Node hx220-m5-node1 version: 5.5(1a)
Node hx220-m5-node3 version: 5.5(1a)
Node hx220-m5-node3 version: 5.5(1a)
Node hx220-m5-node4 version: 5.5(1a)
```

Step 5 Verify that the HX storage cluster is online and healthy.

```
# hxcli cluster info|grep -i health

Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

Step 6 Verify that the upgrade is complete and is successful.

```
stcli cluster upgrade-status
```

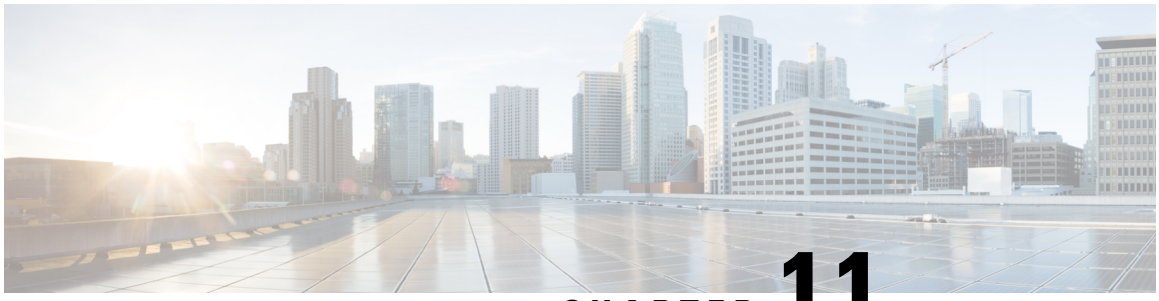
```
Nodes up to date:
[HX-Cluster, HX-Node-1(1.1.1.1), HX-Node-2(1.1.1.2), HX-Node-3(1.1.1.3)]
Cluster upgrade succeeded.
```

Step 7 For each browser interface you use, empty the cache and reload the browser page to refresh the HX Connect content.

Enable HyperFlex Software Encryption

HyperFlex Software Encryption provides file-level end-to-end AES 256-bit encryption of data at-rest. You can leverage the capability of HyperFlex Software Encryption to protect the confidentiality of your data against device theft, such as drives, servers, or entire clusters. Encryption keys are securely and remotely stored by the Intersight Key Manager, available in both the Intersight SaaS and the Intersight virtual appliance.

To enable HyperFlex Software Encryption on your cluster, check that you meet the HX Data Platform and Intersight license requirements, see Cisco HyperFlex Systems Ordering and Licensing Guide. After confirming license requirements are met, to enable HyperFlex Software Encryption, you need to download the encryption package from My Cisco Entitlement, install the package, and then enable encryption from Intersight. For more information, see HyperFlex Software Encryption.



CHAPTER 11

HyperFlex Edge Upgrade

Overview

This section provides information related to upgrading a Cisco HyperFlex Edge system from the HX Connect. If your cluster was deployed using Cisco Intersight, please use Intersight to perform the cluster upgrade. For detailed upgrade prerequisites and instructions about upgrading Edge Clusters using Intersight.

Important

- Upgrading a HyperFlex Edge system involves upgrading the server firmware, HyperFlex Data Platform Software, and VMware ESXi.
- You can perform a combined upgrade of HyperFlex Data Platform and VMware ESXI using HyperFlex Connect or you can choose to perform a split upgrade.
- UCS Server firmware upgrade is not supported from HX Connect. Instead, perform the UCS server firmware upgrade separately using the Host Upgrade Utility (HUU) tool or the Integrated Management Controller (IMC) Supervisor.

Cisco HyperFlex Edge Firmware Recommended Versions

- Review the Cisco HyperFlex Release Notes for Cisco HX Data Platform that corresponds to the release for your planned upgrade.
- For upgrading supported releases, see the Cisco HyperFlex Software Requirements and Recommendations document.

- If you want to upgrade from a release that is no longer supported, see the Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases.
- For HyperFlex Edge clusters that are upgraded using HX Connect, the HyperFlex Data Platform upgrade includes upgrade of the embedded storage firmware in addition to the HyperFlex Data Platform software. This embedded firmware upgrade includes updates to the SAS passthrough storage controller and associated drives (housekeeping, cache, and capacity) that run the distributed storage platform. A manual upgrade of these embedded firmware storage components via the HUU should not be performed. It is recommended to complete the server firmware upgrade using HX Connect. If a manual upgrade or downgrade of these storage components is required, ensure that you do the following:
  - If you are using the Host Update Utility (HUU) to upgrade chassis firmware, be sure to uncheck the option to upgrade the SAS controller and do not upgrade drives (except for the boot drive, if desired).
  - Avoid using the Upgrade All button in the HUU as this will include the storage controller by default.
  - Firmware management for these devices is handled by HyperFlex Data Platform automatically and should not be manually changed using other utilities. Only use the HUU to upgrade these components when deemed necessary for troubleshooting or as instructed by Cisco TAC.
  - For clusters running Cisco IMC version prior to version 4.1(3b), secure boot must be temporarily disabled to perform server firmware upgrade. Once Cisco IMC version 4.1(3b) version or later is running on all nodes in the cluster, secure boot can be enabled for firmware upgrade.

Server Firmware Upgrade Using the Cisco Host Upgrade Utility Tool

The following table summarizes the server firmware upgrade workflow on Cisco HX Servers:

Step	Description	Reference
1.	Place a node in HX maintenance mode. **Note** Upgrade one node at a time, for the cluster to stay online during upgrade.	Entering Cisco HyperFlex Maintenance Mode
2.	Upgrade server firmware using the Host Upgrade Utility tool.	See Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU in the Cisco Host Upgrade Utility User Guide.
3.	Reboot the node back into ESXi. Exit HX maintenance mode.	
4.	Wait until the cluster becomes fully healthy.	Viewing HyperFlex Cluster Health, on page 15

Step	Description	Reference
5.	Repeat steps 1-4 on the remaining HX nodes in a rolling fashion. **Note** Ensure that you check the health state before entering maintenance mode on the next host in the cluster.	

You can find current and previous releases of the *Cisco Host Upgrade Utility User Guide* at this location: https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html.

Server Firmware Upgrade Using Cisco Integrated Management Controller Supervisor

The following table summarizes the server firmware upgrade workflow on Cisco HX Servers:

Step	Description	Reference
1.	Place a node in HX maintenance mode. **Note** Upgrade one node at a time, for the cluster to stay online during upgrade.	
2.	Create a rack group. Add servers to the IMC Supervisor inventory.	See Managing Server Discovery, Rack Groups, and Rack Accounts in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*.
3.	Configure auto-discovery profile.	See Configuring Auto Discovery Profile in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*.
4.	Run inventory on the rack group.	See Collecting Inventory for Rack Accounts or Rack Groups in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*.
5.	Create firmware profile.	Refer to the following tasks in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*: • Adding Images to a Local Server • Uploading Images from a Local File System • Adding Images from a Network Sever

Step	Description	Reference
6.	Upgrade firmware using IMC Supervisor, on the node put in maintenance mode.	See Upgrading Firmware in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*.
7.	Reboot the node back into ESXi. Exit HX maintenance mode.	
8.	Wait until the cluster becomes fully healthy.	
9.	Repeat step 6 on the remaining HX nodes in a rolling fashion. **Note** Ensure that you check the health state before entering maintenance mode on the next host in the cluster.	

You can find current and previous releases of the *Cisco IMC Supervisor Rack-Mount Servers Management Guide* here: https://www.cisco.com/c/en/us/support/servers-unified-computing/integrated-management-controller-imc-supervisor/products-installation-and-configuration-guides-list.html.

Upgrading Server Firmware on a Cisco UCS C-Series Server Using the Cisco IMC Supervisor

Note Before upgrading Cisco IMC Supervisor and if a firmware profile was already set up, ensure that the Cisco.com credentials and proxy details are configured.

Step 1 Choose **Systems** > **Firmware Management**.

Step 2 On the **Firmware Management** page, click **Firmware Upgrades**.

Step 3 Click **Run Upgrade**. A warning message appears, advising you that running the upgrade on the selected servers will cause the host to reboot into the firmware update tool. On completion of the firmware update, the servers will reboot back to the host OS.

Step 4 Click **OK** to confirm.

Step 5 On the **Upgrade Firmware** screen, complete the following:

Field	Description
Select Profile drop-down list	Choose a profile from the drop-down list.

Field	Description
Platform field	Click **Select** and choose the servers from the list. The list displays only those servers whose platforms match the one configured in the selected profile.
Image Version field	
Image Path field	
Schedule later check box	Check this check box and select an existing schedule to run an upgrade. You can also click the + icon to create a new schedule.

Step 6 Click **Submit**.

Upgrading HyperFlex Edge Using HX Connect

Cisco HyperFlex Edge cluster upgrade process involves upgrading the below 2 components:

- Cisco HyperFlex Data Platform
- VMware vSphere ESXi

You can combine HyperFlex Data Platform and VMware ESXi upgrade in a single combined upgrade for HyperFlex Edge clusters. Cisco recommends upgrading these 2 components in a combined upgrade from HyperFlex Connect. You can choose to upgrade one or two of these components at a time.

If you prefer to upgrade individual components one at a time, see VMware vSphere/ESXi Upgrade, on page 31. The component upgrade process for standard cluster and HyperFlex Edge cluster are the same.

This section describes the steps to perform a combined upgrade of HyperFlex Data Platform and VMware vSphere ESXi. In this process, the HyperFlex nodes will go through an optimized rolling reboot without any workload disruptions by use of VMware vMotion.

Note HyperFlex Edge clusters deployed via Intersight do not have upgrade capability from HyperFlex Connect. The upgrade is only supported through Intersight.

Step 1 Log into HX Connect.

a) Enter the administrative username and password.

b) Click **Login**.

Step 2 In the Navigation pane, select **Upgrade**.

Step 3 On the **Select Upgrade Type** page, select **HX Data Platform** and **ESXi** and complete the following fields:

Step 4 Upload the HyperFlex Data Platform upgrade package (storfs-package).

Table 1: Upgrade HX Data Platform

UI Element	Essential Information
Drag the HX file here or click to browse	Upload the latest Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing clusters with previous release.tgz package file from Download Software - HyperFlex HX Data Platform. Sample file name format: storfs-packages-5.5.1a-31601.tgz.
Current version	Displays the current HyperFlex Data Platform version.
Current cluster details	Lists the HyperFlex cluster details like the **HyperFlex release** and **cluster upgrade state**.
Bundle version	Displays the HyperFlex Data Platform version of the uploaded bundle.
(Optional) **Checksum** field	The MD5 Checksum number is available by hovering over the filename in the Cisco.com Software Download section. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle

Step 5 Upload the VMware ESXi custom image offline upgrade bundle.

Step 6 Provide vCenter login credentials:

Essential Information	Essential Information
User Name field	Enter the vCenter <admin> username.
Admin Password field	Enter the vCenter <admin> password.

Step 7 Click **Upgrade** to begin the combined upgrade process.

Step 8 The Validation screen on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any.

Note At this point, all pre-upgrade checks and validations are running, along with the initial upgrade stage. Within a few minutes, HX Connect returns and prompts you to confirm and start the second stage of the upgrade. The upgrade is not complete until both steps are performed in the UI. The system should never be left in a state where only the first step of the upgrade is complete.

Step 9 The HyperFlex Connect UI refreshes after the first step of the upgrade, and a banner pops up prompting you to provide the UCS and vCenter credentials and start the second stage of the upgrade process. Monitor the upgrade page and confirm that the upgrade is complete.

When upgrade is in progress, you may see an error message **Websocket connection failed. Automatic refresh disabled**. You can either refresh the page or log out and log back in to clear the error message. You can safely ignore this error message.

Note Proceed to Confirm That Upgrade Is Complete, on page 33 for post upgrade tasks once the upgrade is complete. If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance.

Post Upgrade Tasks for HyperFlex Edge

After the upgrade is complete and the HyperFlex Edge cluster has been upgraded, log out and log back in to HX Connect to see the upgrade changes.

Step 1 Confirm that the HX nodes match the expected firmware version.

Check the firmware version in the IMC supervisor GUI or Cisco IMC UI to verify for the correct firmware version.

To view the firmware version, in the IMC Supervisor GUI, navigate to the **Systems** > **Firmware Management** tab. See Upgrading Firmware using IMC Supervisor for more details.

Step 2 Log into any controller VM through SSH.

```
# ssh admin@controller_vm_ip
```

Step 3 Confirm the HyperFlex Data Platform version.

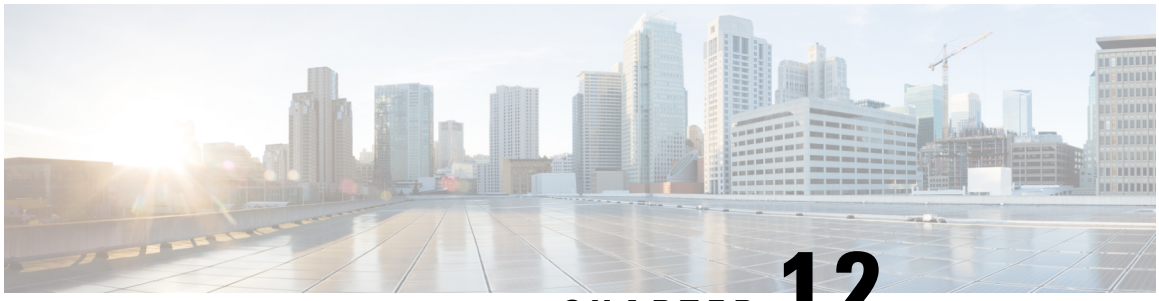
```
# hxcli cluster version


Cluster version: 5.5(1a)
Node hx220-m5-node-1 version: 5.5(1a)
Node hx220-m5-node-3 version: 5.5(1a)
Node hx220-m5-node-2 version: 5.5(1a)
Node hx220-m5-node-4 version: 5.5(1a)
```

Step 4 Verify that the HX storage cluster is online and healthy.

```
# hxcli cluster info|grep -i health
```

```
Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

Step 5 For each browser interface you use, empty the cache and reload the browser page to refresh the HX Connect content.



CHAPTER 12

Stretched Cluster Upgrade

Overview

This section provides information related to upgrading a Cisco HyperFlex Stretched Cluster. The procedure for performing a Stretched Cluster upgrade is similar to the regular HyperFlex cluster upgrade procedure.

Cisco HyperFlex Stretched cluster upgrade process involves upgrading the below 3 components:

- Cisco HyperFlex Data Platform
- VMware vSphere ESXi
- Cisco UCS Server Firmware

You can combine HyperFlex Data Platform and VMware ESXi upgrade in a single combined upgrade for HyperFlex Stretched clusters. Cisco recommends upgrading these 2 components in a combined upgrade from HyperFlex Connect. You can choose to upgrade one or two of these components at a time.

If you prefer to upgrade individual components one at a time, see Upgrade UCS Firmware, HX Data Platform and VMware vSphere - Individual Component Upgrade, on page 27. The component upgrade process for standard cluster and HyperFlex Stretched cluster are the same.

This section describes the steps to perform a combined upgrade of HyperFlex Data Platform and VMware vSphere ESXi. In this process, the HyperFlex nodes will go through an optimized rolling reboot without any workload disruptions by use of VMware vMotion.

Upgrade Guidelines for Stretched Cluster

Important Do not upgrade HyperFlex Stretch clusters to HXDP 5.0(2b) See Software Advisory https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/sw-advisory-hyperflex-release-5-0-2b.html

- Upgrade of UCS server firmware is not supported through HX Connect. UCS firmware upgrade must be done manually using Cisco UCS Manager. See Manage Firmware through Cisco UCS Manager.
- Upgrade of the HyperFlex Witness node is not required when upgrading stretched clusters but is strongly recommended. Refer to the Cisco HyperFlex Software Requirements and Recommendations for the latest witness version available.
- Health Check — Cisco recommends running this proactive health check on your HyperFlex cluster prior to upgrade. For more details, see Pre-Upgrade Intersight Health Check, on page 11

Upgrading HyperFlex Stretched Cluster Using HX Connect

Before you begin

- Complete pre-upgrade validation checks.
- Download the latest *Cisco HX Data Platform Upgrade Bundle for upgrading existing clusters from previous releases*, from Software Download .
- Upgrade Cisco UCS Infrastructure.
- Upgrade UCS server firmware. For more information, see Manage Firmware through Cisco UCS Manager.
- Disable snapshot schedule, on the storage controller VM. SSH to HyperFlex cluster IP and run the command **stcli snapshot-schedule –disable** snapshot schedule.
- If DRS is *Enabled* and set to fully automatic mode, the VMs are automatically migrated to other hosts with vMotion.

Note If DRS is *Disabled*, vMotion the VMs manually to continue the upgrade process when prompted. For more information, see VMware Documentation for Migration with vMotion.

Step 1 Log in to HX Connect.
a) Enter the administrative username and password.
b) Click **Login**.

Step 2 In the Navigation pane, select **Upgrade**.

Step 3 On the **Select Upgrade Type** page, select **HX Data Platform** and **ESXi** and complete the following fields:

Step 4 On the **Select Upgrade Type** page, select **HX Data Platform** and complete the following fields:

UI Element	Essential Information
Drag the HX file here or click to browse	Upload the latest Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing clusters with previous release.tgz package file from Download Software - HyperFlex HX Data Platform. Sample file name format: storfs-packages-4.5.1a-31601.tgz.
Current version	Displays the current HyperFlex Data Platform version.
Current cluster details	Lists the HyperFlex cluster details like the **HyperFlex version** and **Cluster upgrade state**.
Bundle version	Displays the HyperFlex Data Platform version of the uploaded bundle.
(Optional) **Checksum** field	The MD5 Checksum number is available by hovering over the filename in the Cisco.com Software Download section. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle.

Step 5 Upload the VMware ESXi custom image offline upgrade bundle.

Step 6 Provide vCenter login credentials:

Essential Information	Essential Information
User Name field	Enter the vCenter <admin> username.
Admin Password field	Enter the vCenter <admin> password.

Step 7 Click **Upgrade** to begin the combined upgrade process.

Step 8 The Validation screen on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any.

Note At this point, all pre-upgrade checks and validations are running, along with the initial upgrade stage. Within a few minutes, HX Connect returns and prompts you to confirm and start the second stage of the upgrade. The upgrade is not complete until both steps are performed in the UI. The system should never be left in a state where only the first step of the upgrade is complete.

Step 9 The HyperFlex Connect UI refreshes after the first step of the upgrade, and a banner pops up prompting you to provide the UCS and vCenter credentials and start the second stage of the upgrade process. Monitor the upgrade page and confirm that the upgrade is complete.

When upgrade is in progress, you may see an error message **Websocket connection failed. Automatic refresh disabled**. You can either refresh the page or log out and log back in to clear the error message. You can safely ignore this error message.

Note Perform post upgrade tasks once the upgrade is complete. If the upgrade fails, you can re-try the upgrade or contact Cisco TAC for further assistance.

Upgrading a Witness VM for HXDP Release 5.0(x) and Earlier

Before you begin

Attention This workflow is for use with existing Stretched Cluster installs (HXDP Release 5.0(x) and earlier). New Stretched Clusters installed using HXDP 5.5(1a) and later will auto-configure an Invisible Cloud Witness for site arbitration. Invisible Cloud Witness automatically runs the latest version, user maintenance of this component is not required.

- Select the Witness VM version that supports the HXDP version you are upgrading to.

  For supported versions see the *HX Data Platform Software Versions for HyperFlex Witness Node for Stretched Cluster* section of the Cisco HyperFlex Software Requirements and Recommendations

  for your respective upgrade.
- Upgrade HyperFlex Stretched Cluster.
- The upgraded HyperFlex Stretched Cluster must be in healthy state. To check the health state of Stretched Cluster after upgrade, run the following command:

  ```
  root@StCtlVM:~# hxcli cluster info | grep healthy
  ```

Step 1 Log into the witness VM using SSH and execute the following command to stop the service exhibitor.

```
root@WitnessVM:~# service exhibitor stop
```

Step 2 Copy the `exhibitor.properties` file available in the `/usr/share/exhibitor/` path to a remote machine from where you can retrieve the `exhibitor.properties` file.

```
scp root@<Witness-VM-IP>:
/usr/share/exhibitor/exhibitor.properties user@<Remote-Machine>:
/directory/exhibitor.properties
```

Step 3 Log out from the Witness VM. Power off and rename the Witness VM to WitnessVM.old.

Note Confirm that the IP address of the old Witness VM is unreachable, using the ping command.

Step 4 Deploy a new Witness VM and configure the same IP address as the old Witness VM.

Note If the IP address is not reachable, the Witness OVA deployment may contain stale entries in the `/var/run/network` directory. You must manually remove these entries and reboot the VM to have the assigned IP address become reachable on the network.

To reboot the VM, open the VM console in vCenter/vSphere and execute the following command:

```
rm -rf /var/run/network/*
reboot
```

Step 5 Log into the new witness VM using SSH and execute the following command to stop the service exhibitor.

```
root@WitnessVM:~# service exhibitor stop
```

Step 6 Copy the `exhibitor.properties` file from the remote machine (copied in Step 2) to the `/usr/share/exhibitor/` path of the new Witness VM.

```
scp /directory/exhibitor.properties root@<Witness-VM-IP>:
/usr/share/exhibitor/exhibitor.properties
```

Step 7 Verify if the following symlinks are preserved in the new Witness VM:

```
root@Cisco-HX-Witness-Appliance:~# cd /etc/exhibitor/
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ls -al
total 8
drwxr-xr-x 2 root root 4096 Sep 11 13:00 .
drwxr-xr-x 88 root root 4096 Sep 11 12:55 ..
lrwxrwxrwx 1 root root 41 Sep 11 13:00 exhibitor.properties
lrwxrwxrwx 1 root root 37 Jul 24 16:49 log4j.properties
```

If the symlinks are not available, execute the following command:

```
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ln
 -s /usr/share/exhibitor/exhibitor.properties exhibitor.properties
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ln -s /usr/share/
exhibitor/log4j.properties log4j.properties
root@Cisco-HX-Witness-Appliance:/etc/exhibitor# ls -al total 8
drwxr-xr-x 2 root root 4096 Sep 11 13:00 .
drwxr-xr-x 88 root root 4096 Sep 11 12:55 ..
lrwxrwxrwx 1 root root 41 Sep 11 13:00 exhibitor.properties
-> /usr/share/exhibitor/exhibitor.properties
lrwxrwxrwx 1 root root 37 Jul 24 16:49 log4j.properties
 -> /usr/share/exhibitor/log4j.pr
```

Step 8 **Important** Skip this step if your upgrade is an HX Release prior to version 4.5(2a).

Get the cluster UUID value from `/etc/springpath/clusteruuid` file on any Controller VM and then edit `/usr/share/zookeeper/conf/server.jaas.conf` and replace `HX_PLACEHOLDER` with Cluster UUID.

Example:

```
On any Storage Controller VM, get the contents of clusteruuid
 file -cat /etc/springpath/clusteruuid 5b4f718033594dad:663273adab09777a
On the Witness VM, replace the HX_PLACEHOLDER value with the cluster
UUID -Before -QuorumServer {
       org.apache.zookeeper.server.auth.DigestLoginModule required
user_hyperflex="HX_PLACEHOLDER";};QuorumLearner {
       org.apache.zookeeper.server.auth.DigestLoginModule required
       username="hyperflex"
       password="HX_PLACEHOLDER";};
After -QuorumServer {org.apache.zookeeper.server.auth.DigestLoginModule
 required user_hyperflex="5b4f718033594dad:663273adab09777a";};
 QuorumLearner { org.apache.zookeeper.server.auth.DigestLoginModule
 required
       username="hyperflex"
       password="5b4f718033594dad:663273adab09777a";};
```

Step 9 **Note** This step is required for users that are moving to Witness VM Node version 1.1.1 and later, if the Witness VM being upgraded is a version previous to 1.1.1.

Run the `/usr/share/springpath/storfs-misc/setexhibitorconfig.sh` command to upgrade the Witness exhibitor configuration.

Note The `setexhibitorconfig.sh` automates the process of editing the `exhibitor.properties` file, and replaces all of the data IP addresses with the management IP addresses for each corresponding controller VM.

Note It is normal for this command to not show any output when upgrading from a Witness VM that is older than 1.1.1.

Step 10 Start the service exhibitor by executing the following command:

```
root@Cisco-HX-Witness-Appliance:~# service exhibitor start
exhibitor start/running, process <ID>
```

Manually Upgrading ESXi for Cisco HyperFlex Stretched Cluster

Step 1 Select one of the hosts and put it in HX maintenance mode using the vSphere Web Client. After the host enters maintenance mode, complete the following steps.

Step 2 Copy files using SCP, start the SSH service in the destination ESXi hosts as well.

Note
- On HX240, you can use the local SpringpathDS datastore or a mounted HX datastore.
- On HX220, you can use either a mounted HX datastore or create a temporary RAM disk.

```
scp local_filename user@server:/path/where/file/should/go
```

Step 3 Log into ESXi, and execute the following command to query the list of available image profiles and for profile name verification.

```
esxcli software sources profile list -d <location_of_the_esxi_zip_bundle_on_the_datastore>
```

Attention Full path must be used when running the `esxcli` software command.

Example:

```
[root@localhost:~] esxcli software sources profile list -d /vmfs/volumes/5d3a21da-7f370812-ca58-0025
b5a5a102/HX-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10-upgrade-bundle.zip
Name                                        Vendor  Acceptance Level  Creation Time       Modification
 Time
------------------------------------------  ------  ----------------  ------------------
------------------
HX-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10  Cisco   PartnerSupported  2019-04-02T00:14:56
2019-04-02T13:38:34
```

Step 4 Run the following command to perform the upgrade.

```
esxcli software profile update -d <path_to_profile_ZIP_file> -p < profile name>
```

Example:

```
[root@HX-ESXi-01:/vmfs/volumes/1a234567-89bc1234] esxcli software profile update -d
/vmfs/volumes/1a234567-89bc1234/HX-Vmware-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10.zip
-p HX-ESXi-7.0U3-20328353-Cisco-Custom-7.3.0.10
```

Step 5 After the ESXi host comes up, verify that the host has booted up with the correct version.

```
vmware -vl
```

Step 6 Exit maintenance mode using the vSphere Web Client.

Step 7 Ensure that the cluster becomes healthy between each ESXi upgrade.

```
hxcli cluster info [flags]
```

Step 8 Repeat this process for all hosts in the cluster in a sequence.

Note Make sure that the cluster becomes healthy between each ESXi upgrade.

Configuring Stretched Cluster for UCS FW Upgrade

During upgrade, the following customized UCS policies are validated and adjusted for HyperFlex:

- HFP (Host Firmware Package) - Host Firmware Packages provide consistent firmware files for the multiple components of a HyperFlex node. This includes CIMC, BIOS, HBA and SAS Expander firmware, VIC and other components. Unlike typical UCS Host Firmware Packages, they also control disk firmware, due to the criticality of this to HyperFlex Data Platform. Note that Self Encrypting Drives (SED) firmware is controlled by HyperFlex Data Platform directly and not UCS Manager policies.
- VNIC Templates - Virtual NIC (VNIC) templates provide consistent configuration of VNIC's between UCS fabrics. HyperFlex VNIC Templates are configured as redundancy pairs to ensure changes to HyperFlex VNIC's on one UCS fabric is applied to the other.
- Ethernet Adaptor Policies - Ethernet Adaptor Policies provide performance related properties for HyperFlex VNIC's.
- BIOS Policies - BIOS policies control configuration and performance of key hardware resources on a HyperFlex node, such as CPU and Memory. HyperFlex uses specific configuration to provide consistent high performance.
- VNIC/VHBA Placement Policies - VNIC/VHBA placement policies determine the PCI addresses presented to the HyperFlex node for a given VNIC/VHBA. HyperFlex sets this in a consistent manner so further configuration can proceed successfully.

Step 1 SSH to any CVM on a site and change directory into /tmp

Step 2 Use the `su diag` Enter into the diag shell on a storage controller VM.[2]

Step 3 Run the following command: `/usr/local/bin/hx.py --upgrade-cluster-config`. This generates a file called "`customer_site_config.json`" and saves it in the /tmp directory.

Step 4 Edit the `customer_site_config.json` file to change the firmware version and the org name appropriately. For example:

Example:

```
{
    "id": "Advanced",
    "collapse": true,
    "label": "Advanced",
    "groups": [
      {
        "id": "firmware",
        "label": "UCS Firmware",
        "items": [
```

[2] HXDP Release 5.0(2a) and later support the `su diag` command. For more information, see the Diag User Overview.

```
          {
            "id": "version",
            "label": "UCS Firmware Version",
            "type": "text",
            "description": "UCS Firmware Version to be used on the HX servers",
            "placeholder": "ex: 3.2(2d)",
            "defaultValue": "3.2(2d)",
            "value": "4.1(1d)"  #<<<<<----------------- Change this
          },
          {
            "id": "version-m5",
            "label": "UCS Firmware Version",
            "type": "text",
            "description": "UCS Firmware Version to be used on the M5 HX servers",
            "placeholder": "ex: 3.2(2d)",
            "defaultValue": "3.2(2d)",
            "value": "4.1(1i)" #<<<<<----------------- Change this
          }
        ]
      },
      {
        "id": "org",
       "items": [
                  {
                        "id": "name",
                        "label": "Hyperflex Org name",
                        "type": "text",
                        "value": "Faridabad", #<<<<<----------------- Change this
                       "description": "The name of the org in ucsm which is to be used for creation
 of all the policies and profiles for this Hyperflex cluster"
                  }
        ]
      }
    ]
```

Step 5 Execute the command again and enter the UCSM IP and credentials.

For example:

```
/usr/local/bin/hx.py --upgrade-cluster-config
```

Example:

```
[root@SpringpathControllerVP0RX5DWTC:/# /usr/local/bin/hx.py --upgrade-cluster-config
                [UCS Manager] [in_progress][  0.00%][ETA:  0:18:00] Login to UCS API
                 UCS host name or virtual IP address: 10.42.17.11
                 Connecting to admin@10.42.17.11...
                Password:
```

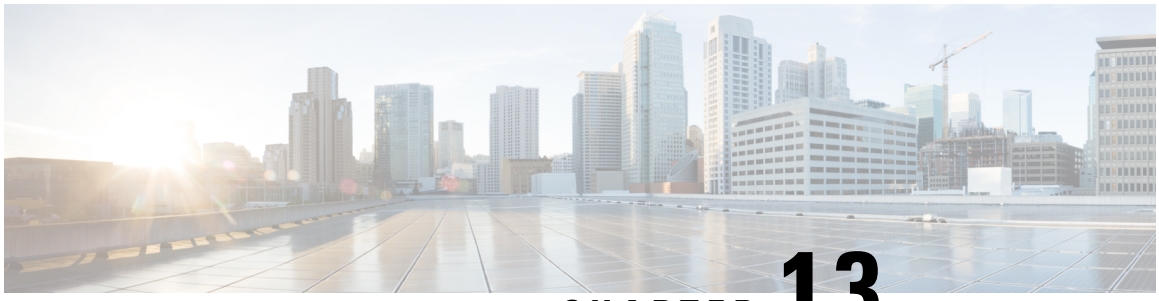
Step 6 Ensure that the command runs without any error. If there is an error, contact Cisco TAC.

Note Note that this command (hx.py) is being run for the first site FI domain. You need to run the same steps for the second site FI domain later.

Step 7 Perform the following steps in vCenter and UCSM:

a) Verify that Pending reboot appears in the pending activities of the UCSM.
b) Put one host in maintenance mode.
c) Reboot the server and then wait for the server to come online and cluster to be online/healthy.
d) Perform the same steps for the remaining nodes.

Step 8 Repeat Steps 4, 5 and 6 again for the other site.



CHAPTER 13

HyperFlex Offline Upgrade Workflow

Offline Upgrade Guidelines

Important

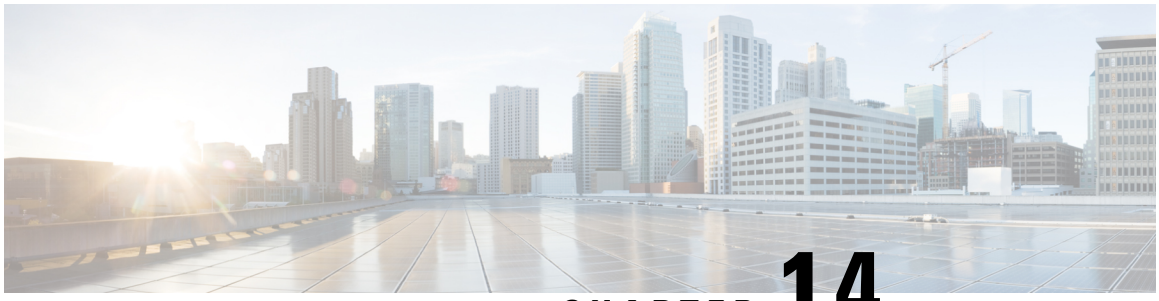
- Offline upgrade can be performed from HX Connect UI for either combined or split upgrade. Before you proceed, consider following guidelines:

- Cisco recommends performing online upgrade from HX Connect UI for hitless upgrade experience without any impact operations.
- Offline upgrade requires the cluster to be shutdown.
- Offline cluster upgrades require the node(s) to reboot. Applications running on the cluster during an offline upgrade are impacted because they do not have access to the HyperFlex storage during the cluster reboot.
- Nodes are upgraded with the new version of the Cisco HX Data Platform software and rebooted one at a time.
- Offline cluster upgrades with nested vCenter is not supported.

Offline Upgrade Process Workflow

Step	Description	Reference
1.	If UCSM (A-bundle) or UCS Server Firmware (C-bundle) upgrade is required, download Cisco UCS Infrastructure A, blade bundle B, and rack bundle C.	Software Download
2.	Upgrade Cisco UCS Infrastructure bundle as required.	Upgrade UCS Infrastructure Firmware, on page 20

Step	Description	Reference
3.	Launch the vSphere Web Client and power down all user VMs (HyperFlex Controller VMs should stay powered on) residing on HX servers and all user VMs running on HX datastores. This includes VMs running on Compute-only nodes. After the VMs are shut down, verify the health state of the cluster and perform a graceful shutdown. **Important** HyperFlex controller VMs (stCtlVMs) must remain powered on.	For more details, see Shut Down and Power Off the Cisco HX Storage Cluster.
4.	(Optional) SSH to cluster management IP as admin user and disable the snapshot schedule.	Run the command `stcli snapshot-schedule --disable`.
5.	Log into HX Connect as admin user and perform either a combined upgrade or an individual component upgrade.	For a combined upgrade see Upgrading HyperFlex Data Platform Software, VMware ESXi, and Cisco UCS Server Firmware using HX Connect, on page 23. For an individual component upgrade see Overview.
6.	Confirm the upgrade is complete and perform the post upgrade tasks .	Post Upgrade Tasks, on page 33
7.	Start the cluster.	Preparing for HX Storage Cluster Maintenance



CHAPTER 14

Manual Pre-Upgrade Validations

Overview

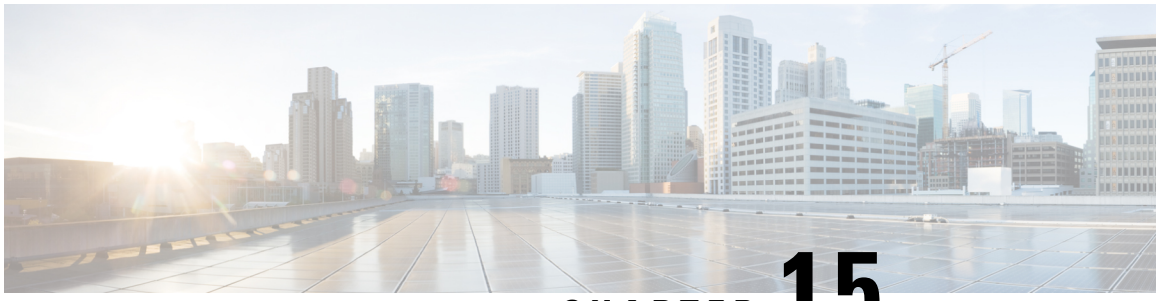
This section describes the manual pre-upgrade validations if you are unable to run the Hypercheck Health Check described in Pre-Upgrade Intersight Health Check, on page 11. Running Hypercheck is highly recommended over performing these checks manually.

Checking Cluster Storage Capacity

Cisco recommends that you check the cluster storage capacity before starting the upgrade of an existing installation of Cisco HX Data Platform. If the storage utilization in the cluster is above 70%, the upgrade validation fails.

When storage utilization in the cluster is above 70%, an offline upgrade is recommended.

Refer to the *HX Storage Cluster Overview* chapter in the Cisco HyperFlex Data Platform Administration Guide for background details about checking cluster storage capacity.



CHAPTER 15

HyperFlex Upgrade Troubleshooting

HXDP Release 5.5(1a) Upgrade Error on M4 Servers

Description

Starting with Cisco HyperFlex Release 5.5(1a), M4 servers are not supported. Attempts to upgrade clusters containing M4 or earlier HX generation servers to HXDP Release 5.5(1a) or later will fail in the pre-upgrade phase.

The upgrade and activity pages display an error in the **Bootstrap Upgrade** step. In some cases, the user is unable to view the error message and is shown a successful upgrade whenin reality the upgrade has failed.

The fallback mechanism is to display a **ClusterUpgradeFailed** event along with a banner stating that the attempted upgrade is disallowed.

Symptom

An alert is generated and a banner appears stating that *One or more M4 platform nodes was detected in the cluster which is not supported starting HXDP 5.5(1a). Please follow the graceful node removal procedure to remove these nodes from the cluster or work with TAC to migrate from these nodes and retry the upgrade*.

Note The message center is populated with the same error message.

Action

Gracefully remove the upsupported nodes and retry the upgrade or contact TAC for further assistance.

Upgrade to HXDP Release 6.0(1a) Fails or the hxupgrade_bundle persists

Description

In the event the upgrade fails or the hxupgrade_bundle persists prior to doing kernel migration upgrade using the installer, manually remove the the hxupgrade_bundle from cvms and retry the kernel upgrade.

VMs Do Not Migrate During Upgrade

Description

Upgrading ESXi cluster fails with error "Node maintenance mode failed". This occurs in an online and healthy ESXi cluster where DRS and HA is enabled.

Action

Try the following workarounds in the following order:

1. If HA admission control policy is enabled and set to slot policy, change it to cluster resource percentage to tolerate one host failure and then retry upgrade.
2. Disable HA admission control policy or disable HA and then retry upgrade.
3. Try powering off a few VMs to make sure there is enough failover capacity in the cluster to tolerate at least one node failure and then retry upgrade.

ESXi Host or HyperFlex Controllers In Lockdown Mode

Description

If the ESXi host is in lockdown mode, pre-upgrade validation will fail with the error message *auth cancel*.

Action

Enable/Disable Lockdown Mode mode on the ESXi host and enable it after the upgrade is successful.

Using HyperFlex Controller VMs

1. Log into HX Connect.
2. On the Navigation pane, select **System Overview**.
3. On the **System Overview** tab, from the **Actions** drop-down list, you can enable or disable access to the controller VM using SSH as an administrator.

Using ESXi Hosts

1. Log into vSphere Web Client.
2. Browse to the host in the vSphere Web Client inventory.
3. Click the **Manage** tab and click Settings.
4. Under System, select **Security Profile**.
5. In the Lockdown Mode panel, click **Edit**.
6. Click **Lockdown Mode** and set the mode to Disabled.

Failed to Upgrade HyperFlex VIBs

Description

HXDP Upgrade to HX 4.5(1a) or above fails with error - "*Failed to upgrade HyperFlex VIBs . Reason: Some(System error)*".

The following error logs appear in the ESXi `esxupdate.log` file:

```
2020-12-01T11:59:22Z esxupdate: 333049: root: ERROR:
vmware.esximage.Errors.LiveInstallationError: ([], '([], "Error in running rm
/tardisks/scvmclie.v00:\\nReturn code: 1\\nOutput: rm: can\'t remove
\'/tardisks/scvmclie.v00\': Device or resource busy\\n\\nIt is not safe to continue. Please
reboot the host immediately to discard the unfinished update."
```

Action

Follow these steps to kill the process corresponding to `getstctlvmlogs` and retry the upgrade.

1. SSH to ESXi with root login.
2. Run the command `ps -c | grep -e cisco -e springpath` and note the process ID (PID). For example:

   ```
   ps -c | grep -e cisco -e springpath
   ```

   ```
   112056 112056 sh /bin/sh /opt/springpath/support/getstctlvmlogs
   ```

3. Kill the process using the command `kill -9 <PID from previous command>`. For example:

   ```
   kill -9 112056
   ```

4. Go back to HX Connect or Intersight and retry the upgrade. If the issue still persists, please contact Cisco TAC for assistance.

HX Connect UCS Server Firmware Selection Dropdown Doesn't List the Firmware Version 4.1 or Above

Description

When you try to perform a combined upgrade from the HX Connect UI, the dropdown to select UCS server firmware doesn't show version 4.1 or later.

Action

Log into UCS Manager and confirm you have uploaded the UCS B and C firmware bundles to the Fabric Interconnect. If not, upload them and re-try the upgrade. If the UCS B and C firmware bundles are already uploaded to the Fabric Interconnect, apply below workaround to continue with upgrade.

1. From the HX Connect upgrade page, select **HX Data Platform** only.
2. Browse and select the appropriate HXDP upgrade package for your upgrade.[3]
3. Enter your vCenter credentials.
4. Click **Upgrade**. This will bootstrap the management components. Refresh the UI screen.
5. Once the UI is refreshed, try the combined upgrade procedure. You should now be able to see the UCS server firmware version 4.1 or above listed in the dropdown menu.

Upgrade Fails in the Step - Entering Cluster Node into Maintenance Mode

Description

Failure at the **Entering Cluster Node into Maintenance Mode** step is caused because of a MTU mismatch in the vSwitch and port-groups. If the cluster has a node that was added at a later point using the node expansion method, the newly added node may have the MTU set to 9000 while other nodes are set to MTU 1500.

Note Below remediation is applicable only if your cluster has one or more nodes that were added as part of a cluster expansion, and they have the MTU set to 9000 while your original cluster nodes are set at a MTU of 1500. If this is not the scenario, please contact TAC for further assistance.

Action

- Log into vCenter.
- Check and confirm the MTU value set on all nodes.

[3] The version must be HXDP 4.5 or later.

- If the nodes that were part of the originally built cluster are set at a MTU of 1500 and some of the other nodes (nodes added later as part of cluster expansion) have the MTU set to 9000, change the MTU on all such nodes to 1500.
- Retry the upgrade.

Maintenance Mode Not Automatic for Cluster Containing VMs with vGPUs Configured

Description

For clusters that contain VMs with vGPUs configured, entering maintenance mode does not occur automatically even with DRS fully enabled. During rolling upgrades, it is necessary to manually handle these VMs to ensure that each ESXi host can enter maintenance mode and continue with the upgrade at the appropriate time.

Action

You can use one of these methods to proceed forward:

1. Manually vMotion the vGPU configured VMs to another ESXi host in the cluster.
2. Temporarily power off the vGPU configured VMs. They can be powered on again after the ESXi host reboots and rejoins the cluster

Note This is a limitation of DRS host evacuation and is documented, see "DRS fails to migrate vGPU enabled VM's automatically (66813) topic" on the VMware documentation site.