Cisco HyperFlex Systems Upgrade Guide for VMware ESXi, Release 4.0

First Published: 2019-04-23

Last Modified: 2021-08-06

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

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

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

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

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

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

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

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

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.

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
Host Upgrade Utility (HUU)	Updated CIMC, and Host Upgrade Utility (HUU) for M5 to UCS 4.1(1h) for HX 4.0(2c).	September 14, 2020	HyperFlex Edge and Firmware Compatibility Matrix for 4.x Deployments
Update to the HyperFlex Software Versions table	Updated Recommended FI/Server Firmware and Software Requirements for Microsoft Hyper-V to 4.0(4i) for 4.0(1a), 4.0(1b), 4.0 (2a), and 4.0(2b) releases.	September 4, 2020	Recommended FI/Server Firmware - 4.0(x) Releases
Update to the HyperFlex Software Versions table	M4/M5 Qualified FI/Server Firmware. Listed USC-M 4.1(2a) as qualified for HX 4.0(2c), 4.0(2b), and 4.0(1b).	August 11, 2020	Recommended FI/Server Firmware - 4.0(x) Releases
Update to the HyperFlex Software Versions table	Added qualification for Cisco UCS Manager 4.0(4i), and 4.1(1d).	July 23, 2020	Recommended FI/Server Firmware - 4.0(x) Releases
Updated ESXi support	Updated Release 4.0(2b) support for ESXi 6.7 3 EP19 and ESX 6.7 U3 EP15.	July 1,2020	Recommended FI/Server Firmware - 4.0(x) Releases
Host Upgrade Utility (HUU)	Updated Host Upgrade Utility (HUU) for M5 to UCS 4.0(4k) for HX 4.0(2a).	May 5, 2020	HyperFlex Edge and Firmware Compatibility Matrix for 4.x Deployments

Feature	Description	HX Release or Date Added	Where Documented
Support for ESXi 6.7 3 EP19 and ESX 6.7 U3 EP15	Provides support for upgrading HyperFlex clusters to VMware vSphere Hypervisor ESXi 6.7 3 EP19 and ESX 6.7 U3 EP15	4.0(2b)	Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems
Dynamic self-signed certificate	Dynamic self-signed certificates are generated rather than static certificates within the upgrade workflow which provides extended validity of 1825 days and SHA256 algorithm for added security.	4.0(2a)	Online Upgrade Process Workflow, on page 34
Test Upgrade Eligibility	Checks your cluster readiness and infrastructure compatibility for an upgrade. Perform this test before upgrading the UCS server, HyperFlex data platform, and/or ESXi.	4.0(2a)	Test Upgrade Eligibility, on page 15
Host Upgrade Utility (HUU)	Updated HUU/CIMC info in the HyperFlex Edge and Firmware Compatibility Matrix for 4.x Deployments.	September 16,2019	HyperFlex Edge and Firmware Compatibility Matrix for 4.x Deployments
ESXi 6.7 U2 Support	Provides support for upgrading HyperFlex clusters to VMware vSphere Hypervisor (ESXi) 6.7 U2.	April 29, 2019	Recommended FI/Server Firmware - 4.0(x) Releases

CHAPTER 2

Overview

About This Guide

This document describes how to upgrade an existing installation of Cisco HyperFlex Data Platform.

Cisco HyperFlex Systems has several components that may be upgraded depending on your environment. The core components in a HyperFlex system are:

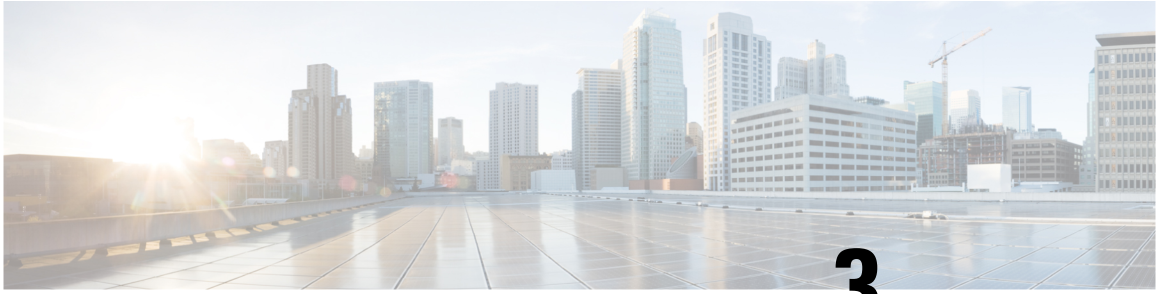
- Cisco UCS server firmware (the UCS C-bundle, which consists of UCS server, BIOS, CIMC, NIC, and so on)
- Cisco HyperFlex Data Platform software
- VMware ESXi software

Upgrade Features

Table 1: Upgrade Features for 4.0(1a) and Later

Feature	Description
Cisco customized VMware ESXi upgrade	You can upgrade VMware ESXi using the HX Connect UI.
No maintenance mode	You are not required to place the HyperFlex nodes in maintenance mode before initiating upgrade. When you upload the upgrade package in the HX Connect UI, you will see an informational pop-up.
Bootstrap Process	Manual cluster bootstrap is required for upgrade from a pre-3.5 release to 3.5(1a). Auto bootstrap is supported for upgrade from 3.5(1a) to later releases.

Feature	Description
Pre-upgrade validations	When you upload the upgrade package in HX Connect and click Upgrade, pre-upgrade validation checks are performed automatically.



CHAPTER 3

Prerequisites and Guidelines

Overview

Before you upgrade the Cisco HX Data Platform and the Cisco UCS server firmware in your Cisco HyperFlex System, consider the guidelines, best practices, and recommendations listed in this chapter.

Prerequisites

1. See *Resolved Caveats* and *Open Caveats* before upgrading and review the *New Features* for this release. Refer to the latest Cisco HX Data Platform Release Notes.

2. Review supported versions and system requirements.

Important

- Verify that you have the latest software bundle versions, review the software versions. Refer to the latest Cisco HX Data Platform Release Notes.

- Ensure that the operating systems on all servers have the right driver levels for the release of Cisco UCS to which you plan to upgrade. See Cisco UCS Driver Installation Guide for identifying the server hardware.

- A Server Firmware upgrade may be required when upgrading to newer Cisco HyperFlex HX Data Platform versions. See the supported versions for each HX Data Platform version in Recommended FI/Server Firmware - 4.0(x) Releases.

3. Back up the configuration into an **All Configuration** backup file. See Cisco UCS Manager Backing Up and Restoring the Configuration Guide for the detailed steps.

4. Before you perform firmware updates, use the Cisco UCS Manager Firmware Management interface to download relevant images to the fabric interconnect. Images are stored in bootflash partitions in the fabric interconnect. See Downloading Software, on page 21 for more details.

5. A 2-step ESXi upgrade may be required when upgrading from ESXi versions starting with 6.0 GA (Build: 2494585) but before 6.0 P07 (Build: 9239799) or versions starting with 6.5 GA (Build: 4564106) but before 6.5 U2 (Build: 8294253) to 6.5 releases post 23rd July 2020, 6.7 releases post 28th April 2020 or any 7.0 ESXi release. For more information, see Impact on ESXi upgrade to future ESXi releases of 2020 due to expired ESXi VIB Certificate.

6. Keep SSH enabled on all ESXi Hosts.

7. Disable Cisco HyperFlex Smart Call Home. For more information, see the Cisco HyperFlex Smart Call Home Quick Start Guide.

8. Only default TCP/IP stack is supported for vMotion vmkernel adapters.

9. Enable vMotion so that the VMs can be moved automatically during the upgrade and MTUs are set as required in the environment. See Configuring vMotion Interfaces, on page 19 for details on adding VMkernel interface.

10. Verify that the HyperFlex cluster is healthy. See HyperFlex Node Upgrade Validations, on page 16 for more details.

11. Verify that the cluster is in lenient mode. If not, set the cluster to lenient mode, refer Configure Lenient Mode, on page 19.

Guidelines and Limitations

- Starting with release 4.0(2a), SCVM is no longer needed on a Compute node.

- **HX REST API Access Token Management** – Applications leveraging HX REST APIs should re-use access tokens when making API calls. Once obtained using the AAA Obtain Access Token API, access tokens are valid for 18 days (1,555,200 seconds). In addition, AAA enforces rate limiting on Obtain Access Token API requests: in a 15 minute window, /auth can be invoked (successfully) a maximum of 5 times. A user is allowed to create a maximum of 8 unrevoked tokens. Subsequent call to /auth will automatically revoke the oldest issued token to make room for the new token. A maximum of 16 unrevoked tokens can be present in system. In order to prevent brute-force attacks, after 10 consecutive failed authentication attempts, a user account is locked for a period of 120 seconds. For more information, see Cisco HyperFlex Systems REST API Reference guide.

  HxConnect makes use of AAA Authentication REST API for login and the above rate limit applies to HxConnect also.

- Single socket stretch cluster nodes are not supported.

- Intersight Managed Mode is not currently supported for HyperFlex.

Upgrade Guidelines

The following list is a highlight of critical criteria for performing an upgrade of your HyperFlex system.

- **Upgrade Considerations for configurations using SFP-H25G-CU3M or SFP-H25G-CU5M cables**—If your configuration is a Fabric Interconnect 6400 connected to VIC 1455/1457 using SFP-H25G-CU3M or SFP-H25G-CU5M cables, then do not use the recommended UCS version of 4.0(4i) release or any other qualified releases. You must use UCS release 4.1(2a) with a qualified HXDP 3.5 or 4.0 version or the cluster may experience an outage. For information on any UCS issues that may affect your environment, see Release Notes for UCS Manager, Firmware/Drivers, and Blade BIOS.

- **Unsupported HX Data Platform 1.7.x, 1.8.x, 2.0, 2.1x, 2.5x, and 2.6x clusters**—Users from any version prior to 2.6(1a) must step through an intermediate version before upgrading to 4.0 or later releases. If you need to upgrade your 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, see Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases. For more information, see the Software Advisory for CSCvq66867: WARNING: Only Use HXDP 2.6(1e) Upgrade Package When Upgrading From HXDP 1.8(1a)-1.8(1e).

- **Hypercheck Health Check Utility**— Cisco recommends running this proactive health check utility on your HyperFlex cluster prior to upgrade. These checks provide early visibility into any areas that may need attention and will help ensure a seamless upgrade experience. For more information see the HyperFlex Health & Pre-Upgrade Check Tool TechNote for full instructions on how to install and run Hypercheck.

- **vSphere 6.7 Software Advisory**—Do not upgrade to Cisco HX Data Platform Release 4.0(1a) when running ESXi 6.7U1 EP06 (build # 11675023). Do not upgrade to 6.7U1 EP06 (build # 11675023) if running Cisco HX Data Platform Release 4.0(1a). See the Software Advisory CSCvo56350 for further details.

  The software build version posted at release will override any other local versions.

- **Required vCenter upgrade**—For enhanced security, Cisco HX Data Platform Release 3.5(1a) or later requires the use of TLS 1.2. Therefore, vCenter must be upgraded to 6.0 U3f or later before upgrading to Cisco HX Data Platform Release 3.5 or later. In addition, ESXi should be upgraded as required to meet HX Data Platform compatibility requirements.

- **Minimum HXDP version for upgrade**—HX Data Platform clusters running 2.6(1a) or later may upgrade directly to 4.0 using the HX Connect UI.

- **Cluster Readiness**—Ensure that the cluster is properly bootstrapped and the updated plug-in is loaded before proceeding. Manual cluster bootstrap is required for upgrade from a pre-3.5 release.

- **Cluster Readiness**—Ensure that the cluster is properly bootstrapped and the updated plug-in is loaded before proceeding. Manual cluster bootstrap is required for HX releases earlier than 3.5(1a). For more information, see the Manual Bootstrap Upgrade Process in the Cisco HyperFlex Systems Upgrade Guide for VMware ESXi, Release 4.0. Do not skip this cluster bootstrap step, it is required for all upgrades until HX Release 3.5(1a). Auto bootstrap is supported beginning with HX release 3.5(1a). For more information, see the Auto Bootstrap Upgrade Process from HX Connect UI in the Cisco HyperFlex Systems Upgrade Guide for VMware ESXi, Release 4.0.

  Manual bootstrap is not supported on Intersight clusters.

- **Initiating Upgrade—**Use the HX Connect UI or CLI `stcli` commands when upgrading from 2.5(1a) or later releases. Use either the CLI `stcli` commands or the HX Data Platform Plug-in to the vSphere Web Client when upgrading from a pre-2.5(1a) release. The vCenter plug-in should not be used for upgrades starting with the 2.5(1a) release.

  If the current cluster version is at 3.5(1a) or above, you do not need to use the `stcli` command. Direct upgrade to 4.0 is possible.

- **Complete your Upgrade—**The self-healing (or rebalance) capability is disabled temporarily during the upgrade window; If the upgrade fails, you should complete the upgrade as soon as possible.

- **ESXi and HXDP Compatibility—**Ensure your cluster is running a compatible version of ESXi based on the running the HX Data Platform version (see the section Software Requirements for VMware ESXi). ESXi compatibility is determined by the major version and update release of ESXi. It is generally best to upgrade HXDP and ESXi together if combining the upgrade operations into a single optimized reboot. When running a split upgrade, first upgrade the HX Data Platform, then proceed to upgrade ESXi.

- Uplinks from the UCS Fabric Interconnects to all top of rack switch ports must configure spanning tree in **edge trunk** or **portfast edge** mode depending on the vendor and model of the switch. This extra configuration ensures that when links flap or change state, they do not transition through unnecessary spanning tree states and incur an extra delay before traffic forwarding begins. Failure to properly configure FI uplinks in **portfast edge** mode may result in network and cluster outages during failure scenarios and during infrastructure upgrades that leverage the highly available network design native to HyperFlex.

- **vSphere 6.0** VMware's last day of general support for vSphere 6.0 occurred on March 12, 2020. HXDP will continue to support vSphere 6.0 U3 on both 3.5(2x) and 4.0(2x) long lived releases. However, no bug or security fixes will be provided by VMware or Cisco for ESXi going forward due to reaching the last day of support. Cisco TAC will continue to support customers to the best of their ability on ESXi 6.0 builds that have already been released. Cisco strongly recommends upgrading as soon as possible to a supported VMware vSphere 6.5 or 6.7 release and follow Cisco's recommendations as outlined in Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems.

- **If Upgrading to vSphere 6.5:**

  Note

  - Certain cluster functions such as native and scheduled snapshots, ReadyClones, and Enter or Exit HX Maintenance Mode will not operate from the time the upgrade is started until the HX Data Platform upgrade is complete.

  - After upgrading ESXi using the offline zip bundle, use the ESX Exit Maintenance Mode option. The HX Exit Maintenance Mode option does not operate in the vSphere Web Client until the HX Data Platform upgrade is complete.

- **vSphere 6.0 Upgrades**—Users on vSphere 6.0 migrating to 6.5, upgrade components in the following order:

  1. Upgrade HX Data Platform and UCS firmware.
  2. Upgrade HX Data Platform and ESXi.
  3. Upgrade HX Data Platform only first, then upgrade ESXi or UCS firmware or both.

- **M4 Server Firmware Upgrades**—Upgrade server firmware to ensure smooth operation and to correct known issues. Specifically, newer SAS HBA firmware is available in this release and is recommended for long-term stability.

  - Users are encouraged to upgrade to 3.1(3c) C-bundle or later whenever possible.

  - Users running C-bundle versions before 3.1(2f) must upgrade server firmware by performing a combined upgrade of UCS server firmware (C-bundle) to 3.1(3c) or later and HX Data Platform to 2.5. Do not split the upgrade into two separate operations.

  - If the cluster is already on 3.1(2f) C-bundle or later, you may perform an HX Data Platform only or combined upgrade, as required.

- **M5 Server Firmware Upgrades**—M5 generation servers must run firmware version 3.2(2d) or later.
- **Firmware Downgrades** — Downgrading UCSM from the HX-installer is not supported.
- **M4/M5 Mixed Domains**—A mixed domain occurs when a new, separate M5 cluster is installed under the same UCS domain that contains existing M4 clusters. Under these conditions, orchestrated UCS server firmware upgrade will not operate until Cisco HX Data Platform Release 2.6 or later is installed on the M4 clusters. Therefore, it is best practice to first upgrade UCS server firmware to the latest 3.1(3) or 3.2(2) patch release before adding a new M5 cluster to the existing UCS domain. Additionally, any 1.7 HX Data Platform clusters must first be upgraded before adding any new M5 clusters to the same domain.
- **Maintenance Window**—If upgrading both HX Data Platform and UCS firmware, you can select either a combined or split upgrade through the vSphere HX Data Platform Plug-in depending on the length of the maintenance window. Cisco UCS Manager infrastructure upgrade is only supported using AutoInstall and the direct server firmware upgrade should be performed only through the upgrade orchestration framework provided by the HX Data Platform Plug-in.
- **Unsupported Self-Encrypting Drives (SEDs)**—If adding or replacing self-encrypting drives (SEDs) that have been recently qualified in newer versions of HX Data Platform, insert the new drives only after upgrading HX Data Platform to a compatible version. All drives must be SED drives, mixing SED and non-SED is not supported.
- **Enabling External Host Access**—With Cisco HX Data Platform Release 4.0(1a), port 445 on the management network is blocked for enhanced security. Note that prior to 4.0, port 445 port was open enabling external host access. If you are upgrading to 4.0(1a) from a prior release, and would like to continue external host access, you can use a utility to open select hosts. For more information about enabling external host access, see the "Configuring HyperFlex Share to SCVMM" section in the Installation Guide for Microsoft Hyper-V.

Supported Upgrade Paths

To upgrade from a supported release, see the upgrade recommendations in 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.

Cisco UCS Manager Upgrade Recommendations

Cisco HyperFlex does not enforce, or have any dependency on the UCSM upgrade path. For more information about upgrading Cisco USC Manager see the Cisco UCS Install and Upgrade Guides.

VMware ESXi Upgrade Recommendations

Cisco HyperFlex does not enforce, or have any dependency on the VMware ESXi Upgrade path outside of the VMware upgrade guidelines. The recommended VMware ESXi download is located on the Cisco Software Downloads page with your Cisco HyperFlex Software download.

- ESXi 5.5 support is deprecated with HXDP 2.5.

  - If running ESXi 5.5 U3 on HX220, contact TAC for upgrade guidance.
  - If running ESXi 5.5 U3 on HX240, see Guidelines and Limitations, on page 6 for further details.

- If you have the ESXi 6.0 U1 version, we recommend an ESXi upgrade. There is a known VMware issue where the node becomes unresponsive due to a PSOD and OS crash. See the VMware Knowledge Base article, VMware ESXi 6.0, Patch ESXi600-201608401-BG: Updates esx-base, vsanhealth, vsan VIBs (2145664).
- Upgrading the VM compatibility version or hardware version of the Storage Cluster 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.

Attention Upgrade to vCenter 6.0 U3f or later is required, due to TLS 1.2 support. Be sure to upgrade vCenter prior to upgrading the HX cluster.

Cisco HX Data Platform Versions Supported by Cisco UCS Manager

Cisco UCS Manager Version	Cisco HX Data Platform									
	4.0(2x)	4.0(1x)	3.5(1x)	3.0(1x)	2.6(1x)	2.5(1x)	2.1(1x)	2.0(1x)	1.8(1x)	1.7.x
4.1(1c)	Yes	—	—	—	—	—	—	—	—	—
4.0(4h)	Yes	—	—	—	—	—	—	—	—	—
4.0(4e)	Yes	—	—	—	—	—	—	—	—	—
3.2(3g)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	—	—	—	—	—
3.2(3g)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	—	—	—	—	—

Cisco UCS Manager Version	Cisco HX Data Platform									
3.2(3d)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	—	—	—	—	—
3.2(2d)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash and M4 servers	Yes Supports hybrid, All Flash, and M4 servers	Yes Supports hybrid, All Flash and M4 servers	Yes	—
3.1(3j)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, and M4 servers	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes	—
3.1(3h)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, and M4 servers	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes	—
3.1(3f)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, and M4 servers	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes	—

Cisco UCS Manager Version	**Cisco HX Data Platform**									
3.1(3c)		Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, M4 and M5 servers	Yes Supports hybrid, All Flash, and M4 servers	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes	—
3.1(2g)		—	—	—	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes Supports hybrid and All Flash	Yes	—
3.1(2f)		—	—	—	—	—	—	Yes Supports hybrid and All Flash	Yes	—
3.1(2b)		—	—	—	—	—	—	Yes Supports hybrid	Yes	—

Upgrading SED Ready Systems

SED-ready systems are HyperFlex clusters running HXDP 2.1(1b) with self encrypting drives (SEDs) installed. UCS Manager must be upgraded to 3.1(3c) or later. In addition, UCS server firmware (C-bundle) must be upgraded to 3.1(3c) or later. Either combined or split upgrade may be used, so long as all the cluster nodes are upgraded prior to enabling key management in HX Connect.

⚠

Caution During an upgrade, a flag-based check (True/False) is used to determine is the system is SED capable or not. If the system is SED-ready, this flag (set to true) will not allow the non-SED systems to become part of the cluster. If there is an issue when SED capability information for cluster is gathered, the upgrade script might toggle this flag to the default value (False). In which case, all the SED drives on the node are replaced with non-SED disks and the upgrade proceeds with non-SED disks as well. Eventually, this may result in the risk of writing data on that node in unencrypted form.

Cautions and Recommendations

Before you begin upgrade of a Cisco HyperFlex System, consider the following cautions, guidelines, and limitations.

Important

- If you have to upgrade from VMware ESXi version 5.5 U3 on HX220, contact Cisco TAC for assistance.
- For HX240, see Guidelines and Limitations, on page 6.

- If you are running HyperFlex release 3.5(1a) or later, you can upgrade the Cisco HX Data Platform by performing the auto-bootstrap process from the HX Connect UI (Auto Bootstrap Upgrade Process from HX Connect UI, on page 24).
- Cisco recommends using GUI upgrade over CLI for ease of use and better reporting.
- When Upgrade is complete, for each browser interface you use, empty the cache and reload the browser to page to refresh the HX content.
- Ensure that all nodes (including compute nodes) are up and running and the cluster is healthy before starting an upgrade or other maintenance activities.
- The Cisco HX Data Platform and Cisco UCS firmware bundles must be compatible. Refer UCS Hardware and Software Compatibility Matrix for more details.
- For a split upgrade, Cisco HX Data Platform should be updated first before updating the Cisco UCS firmware.
- During online upgrade, as one node is being upgraded (put into maintenance mode), the number of tolerated node failures is reduced based on the **Data Replication Factor** and **Access Policy** settings.
- Only default TCP/IP stack is supported for vMotion vmkernel adapters.
- All endpoints in a Cisco HyperFlex domain must be fully functional and all processes must be complete before you begin a firmware upgrade on those endpoints. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. Each endpoint is a component in the Cisco HyperFlex domain that requires firmware to function.
- In a three node cluster, if you shut down one node or put into maintenance mode it makes the cluster unhealthy, but the cluster is still online. If you need to perform manual maintenance, put the hosts in maintenance mode one at a time and move to the next host only after the cluster is healthy. For HXDP and UCS server firmware upgrades, this process is automatic.

  Note You cannot remove a node from 3-node cluster by doing **`stcli node remove`** operation. To replace a node on a 3-node cluster, please contact Cisco TAC for assistance with the node replacement procedure.

CHAPTER 4

Pre-Upgrade Validation Checks

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, 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.

Hypercheck Health Check Utility— Cisco recommends running this proactive health check utility on your HyperFlex cluster prior to upgrade. These checks provide early visibility into any areas that may need attention and will help ensure a seamless upgrade experience. For more information see the Hyperflex Health & Pre-Upgrade Check Tool TechNote for full instructions on how to install and run Hypercheck.

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.

HyperFlex Node Upgrade Validations

Perform the following validations on each HyperFlex node before moving on to upgrade the next node in the cluster.

- 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.
- Verify that vSphere services are running and ESXi Agent Manager (EAM) health is normal.
- Verify the health of the cluster in Cisco UCS Manager.

Viewing HyperFlex Cluster Health

Using CLI

Log in to any controller VM in the storage cluster. Run the command `stcli cluster storage-summary --detail`.

```
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.

Checking Cluster Storage Capacity

We recommend that you check the cluster storage capacity before starting the upgrade of an existing installation of Cisco HX Data Platform. If the storage cluster capacity is above 70%, it is highly recommended to either reduce the amount of storage capacity used or increase the storage capacity by adding new nodes or disks. This confirmation of cluster storage capacity is important because if a node goes down in such a situation, the cluster will not be able to rebalance and will stay unhealthy (online).

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

Verifying If DRS Is Enabled

Click the **vSphere DRS** tab.

Check if **Migration Automation Level** is set to **Fully Automated**.

Verifying and Configuring the Net.TeamPolicyUpDelay Default Value

Step 1 From the vSphere Web Client Navigator, click on each ESXi Host > **Configure** > **System** > **Advanced System Settings**.

Step 2 In **Advanced System** Settings, scroll down to **Net.TeamPolicyUpDelay**.

Step 3 If needed, change the value to *30000*. The default value is 100.

a) For ESXi 6.7 versions below build 16075168, SSH to each ESXi host in the cluster.

b) Run **netdbg vswitch runtime set TeamPolicyUpDelay 30000**.

c) Verify the settings by running **netdbg vswitch runtime get,** and verify **Net.TeamPolicyUpDelay** equals *30000*.

d) As this setting is not retained after a reboot of ESXi host, add the command **netdbg vswitch runtime set TeamPolicyUpDelay 30000** to ESXi local.sh file per Vmware KB https://kb.vmware.com/s/article/2043564.

Viewing ESX Agent Manager

From the vSphere Web Client Navigator, select **Administration** > **vCenter Server Extensions** > **vSphere ESX Agent Manager** > **Summary**.

Verify the Health of a HyperFlex 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 the data path is up and running. See the Cisco UCS Manager Firmware Management Guide for more information.

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 if all servers have been discovered.

Verify UCS Server Firmware (C-Bundle) Version

Using UCS Manager

1. Log in to UCS Manager.
2. Select the **Server** tab.
3. Select the Host Firmware Package policy by navigating to, **Policies** > **Root** > **Sub-Organizations** > ***<hx-cluster>*** > **Host Firmware Packages** > **HyperFlex**.

   Note Ensure that you select the desired cluster under the sub-org list.

4. Under properties, note the current Rack Package version. It is listed as X.Y(Z)C. For example, *3.1(2g)C*.

Configuring vMotion Interfaces

Complete the following steps to add the VMkernel interface necessary for vMotion to work:

Before you begin

Only default TCP/IP stack is supported for vMotion vmkernel adapters.

You must pre-define vMotion networking by creating a vSwitch and defining the vNICs and VLANs in UCS Manager.

Step 1 In the vSphere Web Client Navigator, click on **Host** > **Inventory** > **Manage** > **Networking** > **VMkernel adapters**.

Step 2 Click **Add Host Networking**.

Step 3 Select **VMkernel Network Adapter**.

Step 4 Select the existing **vmotion vSwitch** by selecting browse.

Step 5 Provide a name, and refer to table below to enter the appropriate **VLAN ID**.

Cluster Installation Version	VLAN ID
1.7.x	0 (default)
1.8.x and later	same as vMotion network

Step 6 Provide a **Static IP Address** and complete the wizard.

Step 7 (Optional) To use jumbo frames, edit the **vmk2** and set the **MTU** to `9000`. Your upstream switch must be configured to pass jumbo frames on the **`vMotion VLAN`**.

Step 8 Repeat steps 1 to 6 for all hosts in the cluster.

Configure Lenient Mode

Cluster access policy is set by default to `lenient mode`. To manually set the cluster access policy to lenient, use the following procedure.

SUMMARY STEPS

1. SSH to any one of the controller VMs and login as root.
2. Check if lenient mode is already configured.
3. If set to strict, change to lenient. If already set to lenient, no further action is required.
4. Confirm the change.

DETAILED STEPS

	Command or Action	Purpose
Step 1	SSH to any one of the controller VMs and login as root.	

	Command or Action	Purpose
Step 2	Check if lenient mode is already configured.	`#stcli cluster get-cluster-access-policy`
Step 3	If set to strict, change to lenient. If already set to lenient, no further action is required.	`~/#stcli cluster set-cluster-access-policy --name lenient`
Step 4	Confirm the change.	`stcli cluster info | grep -i policy`

Example

```
~/#stcli cluster get-cluster-access-policy strict
~/#stcli cluster set-cluster-access-policy --name lenient
stcli cluster info | grep -i policy
```

CHAPTER 5

Detailed Pre-Upgrade Procedures

Important

Warning This chapter contains a list of procedures required by various upgrade workflows. Follow only the procedures that are required for the specific upgrade workflow you intend to use. For step-by-step guidance on online and offline upgrades, refer to the Upgrade Procedures, on page 33 chapter.

Downloading Software

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

1. HX Data Platform upgrade bundle (`.tgz` file)
2. VMware ESXi Offline Zip bundle
3. Cisco UCS infrastructure bundle, blade firmware bundle, and rack firmware bundle.

After the Cisco UCS bundles and firmware are downloaded, they need to be copied to Cisco UCS Manager.

To copy UCS software bundles to CIsco UCS Manager

Step 1 Log in to the Cisco UCS Manager GUI.

Step 2 Enter the username and password.

Step 3 In the Navigation pane, click the **Equipment** tab.

Step 4 On the **Equipment** tab, click the **Equipment** node.

Step 5 In the Work pane, click **Firmware Management** > **Installed Firmware** > **Download Firmware**.

Step 6 In the **Download Firmware** dialog box, click the **Local File System** radio button in the **Location of the Image File** field and fill in the required fields.

Step 7 In the **Filename** field, enter the full path and name of the image file.

If you do not know the exact path to the folder where the firmware image file is located, click **Browse** and navigate to the file.

Step 8 Click **OK**. The Cisco UCS Manager GUI begins downloading the firmware bundle to the fabric interconnect.

Step 9 Monitor the status of the download on the **Download Tasks** tab.

Note If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete bundles on the **Packages** tab to free up space. To view the available space in bootflash, navigate to **Equipment** > **Fabric Interconnect** > **Local Storage Information** and look in the Work pane area under the **General** tab.

Step 10 Repeat this task until all the required firmware and bundles are downloaded to the fabric interconnect.

Test Upstream Network Connectivity

Ensure that the hx-storage-data and vMotion upstream switches are configured for Jumbo Frames. Skipping this step could lead to input/output interruption during Cisco UCS infrastructure upgrade.

Step 1 Put a node in Cisco HX Maintenance mode (see Entering Cisco HyperFlex Maintenance Mode, on page 30).

Step 2 SSH to the ESXi host in step 1.

Step 3 Verify that the ping is working by pinging the corresponding vmk1 IP interface of another host.

If using Jumbo Frames:

```
vmkping -I vmk1 -d -s 8972 <data IP of address of another host>
```

If not using Jumbo Frames:

```
vmkping -I vmk1 -d -s 1472 <data IP of address of another host>
```

Note Early Hyperflex installs used **vmnic2** and **vmnic3** for hx-storage-data Vswitch. **vmnic5** and **vmnic1** are supported from HX 3.5(x) and later releases.

Please verify which interfaces are used for testing the hx-storage-data Vswitch failover either through Vcenter GUI, or SSH to the ESXi host using **esxcfg-vswitch-l** command for your clusters ESXi hosts.

Step 4 Swap the active interfaces in *vswitch-hx-storage-data* to force traffic upstream.

```
esxcli network vswitch standard policy failover set -a vmnic2 -s vmnic3 -v vswitch-hx-storage-data
```

Step 5 Again, verify that the ping is working by pinging the corresponding vmk1 IP interface of another host.

If using Jumbo Frames:

```
vmkping -I vmk1 -d -s 8972 <data IP of address of another host>
```

If the ping fails, try again with:

```
vmkping -I vmk1 -d -s 1472 <data IP of address of another host>
```

If not using Jumbo Frames:

```
vmkping -I vmk1 -d -s 1472 <data IP of address of another host>
```

Note If the ping fails, do not proceed to upgrade the Cisco UCS firmware. Investigate the network configuration including upstream switch to identify cause of failure.

Step 6 Swap interface back to defaults even if ping fails.

```
esxcli network vswitch standard policy failover set -a vmnic3 -s vmnic2 -v vswitch-hx-storage-data
```

Step 7 Exit the node from Cisco HX Maintenance mode (see Exiting Cisco HyperFlex Maintenance Mode, on page 31).

Graceful Shutdown of a HX Cluster

Warning This chapter contains a list of procedures required by various upgrade workflows. Follow only the procedures that are required for the specific upgrade workflow you intend to use. For step-by-step guidance on online and offline upgrades, refer to the Upgrade Procedures, on page 33 chapter.

Step 1 SSH to any controller VM in the cluster.

Step 2 Check cluster health `~#stcli cluster info | grep health`.

Step 3 If healthy, shutdown the cluster `~#stcli cluster shutdown`.

Step 4 Shutdown takes a few minutes, wait for the prompt to return.

Modifying Host Firmware Package Using Cisco UCS Manager

Host Firmware Package is set automatically, during CIsco UCS infrastructure upgrade. To manually stage the correct firmware version before starting the upgrade process use the following procedure.

Step 1 Sign in to Cisco UCS Manager.

Step 2 In the Navigation pane, click **Servers**.

Step 3 Expand **Servers** > **Policies** > **Sub-Organizations** > **hx-cluster**.

Step 4 Expand **Host Firmware Packages** and choose the policy you want to update.

Step 5 In the Work pane, click the **General** tab.

Step 6 To modify the components in the host firmware package, click **Modify Package Versions**.

Step 7 Modify value for **Blade Package** and **Rack Package**, to the latest firmware version. See Recommended FI/Server Firmware - 4.0(x) Releases for the list of recommended UCS FI firmware.

Step 8 In the **Excluded Components** area, check the boxes corresponding to the components that you want to exclude from this host firmware package.

Step 9 Click **OK**. Click **yes** for all the warnings.

What to do next

Verify pending activities.

User acknowledgement of each server is performed automatically during upgrade. Optionally, you can manually acknowledge pending activities on the HyperFlex node.

On the Cisco UCS Manager toolbar, click **Pending Activities**.

The **User Acknowledged Activities** tab lists the HyperFlex nodes that require user acknowledgment within the selected sub-org. They are in `Pending Reboot` status.

Note Do not acknowledge service profiles.

Auto Bootstrap Upgrade Process from HX Connect UI

Before you begin

If you are running HyperFlex release 3.5(1a) or later, you can upgrade the Cisco HX Data Platform by performing the auto-bootstrap process from the HX Connect UI. However, if you are running a HyperFlex release that is earlier than release 3.5(1a) you must run the manual bootstrap process to upgrade the Cisco HX Data Platform as outlined in Manual Bootstrap Upgrade Process, on page 28.

Step 1 Log in to HX Connect.

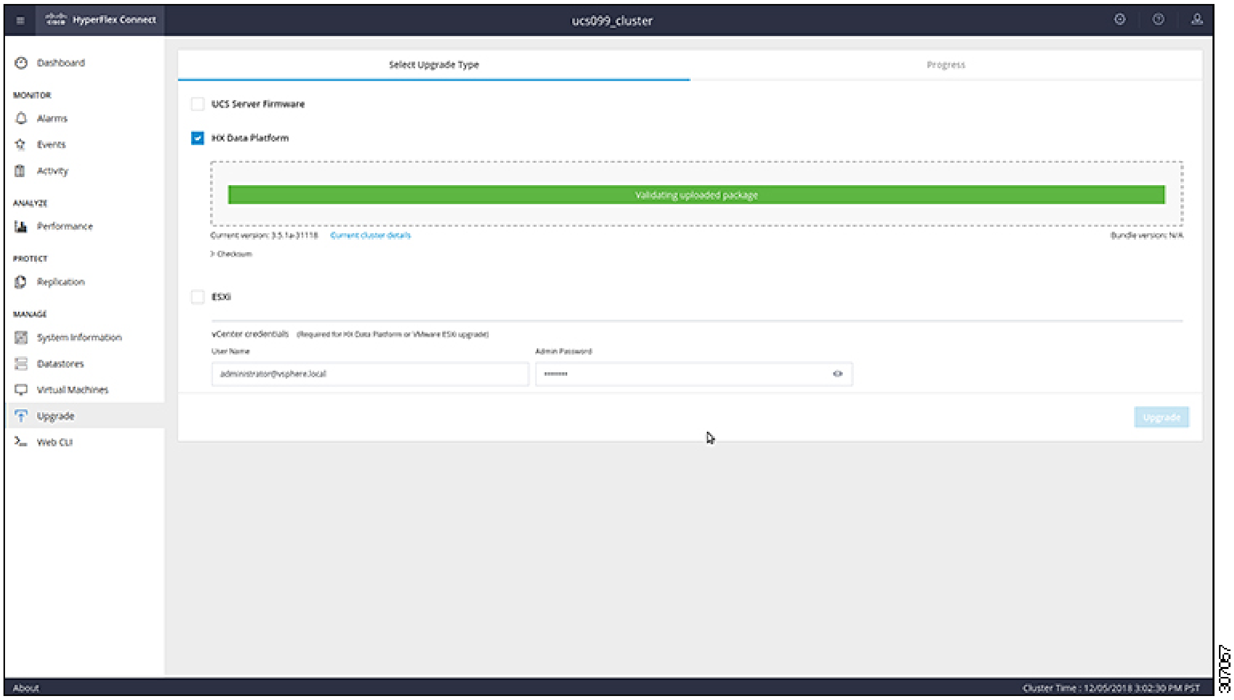
a) Enter the HX Storage Cluster management IP address in a browser. Navigate to *https://<storage-cluster-management-ip>*.

b) Enter the administrative username and password.

c) Click **Login**.

Step 2 In the Navigation pane, select **Upgrade**. The Select Upgrade Type page appears.

Figure 1: Select Upgrade Type Page



□ UCS Server Firmware

☑ HX Data Platform

Validating uploaded package

Current version: 3.5.1a-31118

Bundle version: N/A

□ ESXi

vCenter credentials (Required for HX Data Platform or VMware ESXi upgrade)

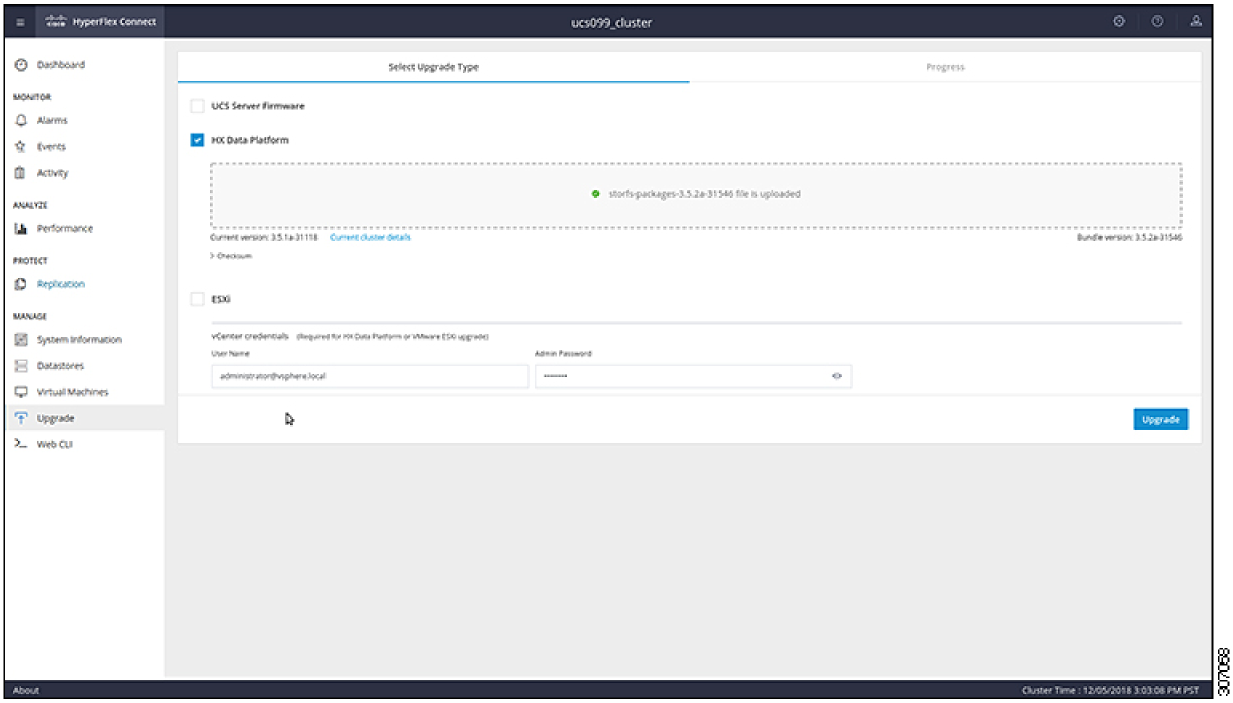
User Name: administrator@vsphere.local

Admin Password: ••••••••

Cluster Time : 12/05/2018 3:02:30 PM PST

Step 3 Upload the new Cisco HX Data Platform upgrade package, specify vCenter credentials, and then click **Upgrade**.

Figure 2: Uploading a Cisco HX Data Platform Upgrade File



□ UCS Server Firmware

☑ HX Data Platform

storfs-packages-3.5.2a-31546 file is uploaded

Current version: 3.5.1a-31118 Current cluster details

Bundle version: 3.5.2a-31546

> Checksum

□ ESXi

vCenter credentials (Required for HX Data Platform or VMware ESXi upgrade)

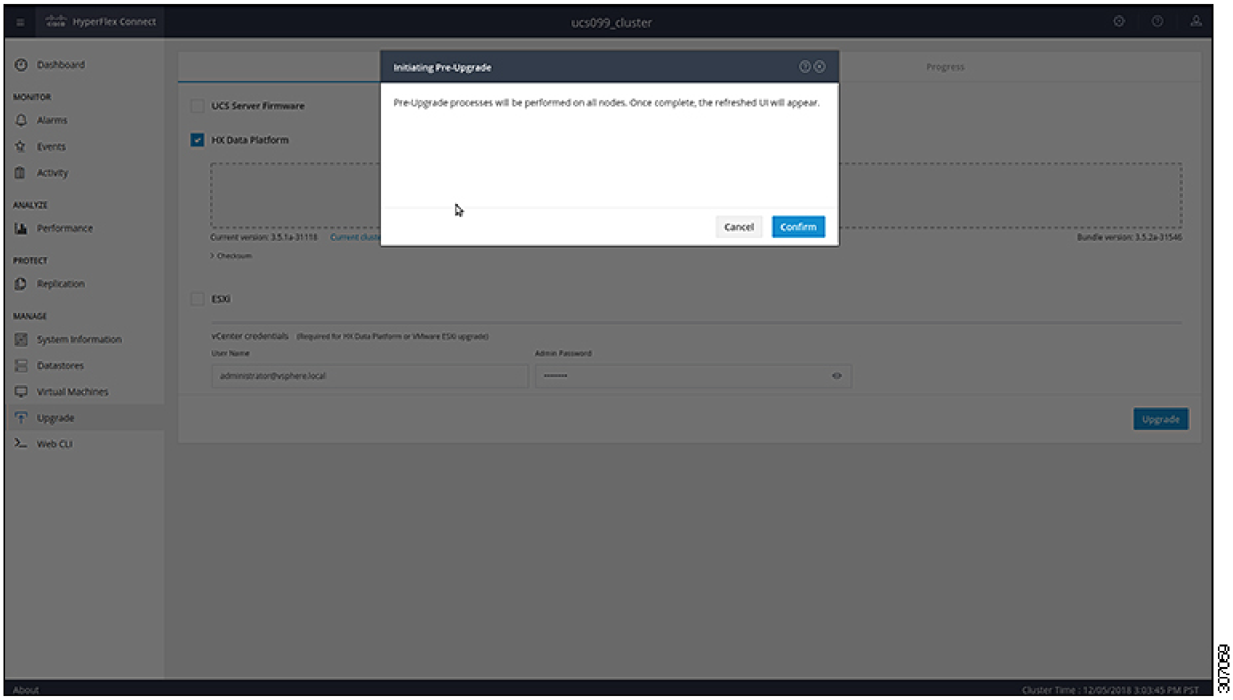
User Name: administrator@vsphere.local

Admin Password: ••••••••

Cluster Time : 12/05/2018 3:03:08 PM PST

Step 4 Click **Confirm** in the Initiating Pre-Upgrade message box. The Pre-Upgrade process begins and will be performed on all nodes.

Figure 3: Initiating the Pre-Upgrade Process

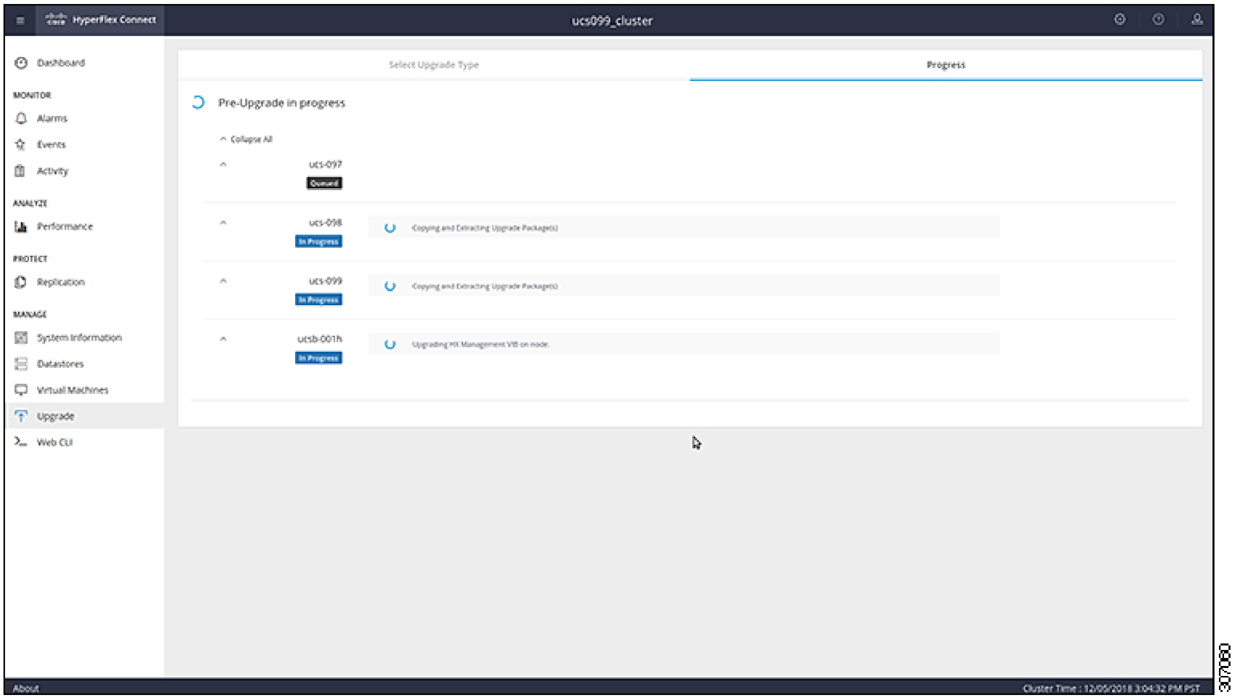


Initiating Pre-Upgrade

Pre-Upgrade processes will be performed on all nodes. Once complete, the refreshed UI will appear.

Cluster Time : 12/05/2018 3:03:45 PM PST

Figure 4: Pre-Upgrade Progress Screen



Pre-Upgrade in progress

ucs-097 Queued

ucs-098 In Progress — Copying and Extracting Upgrade Package(s)

ucs-099 In Progress — Copying and Extracting Upgrade Package(s)

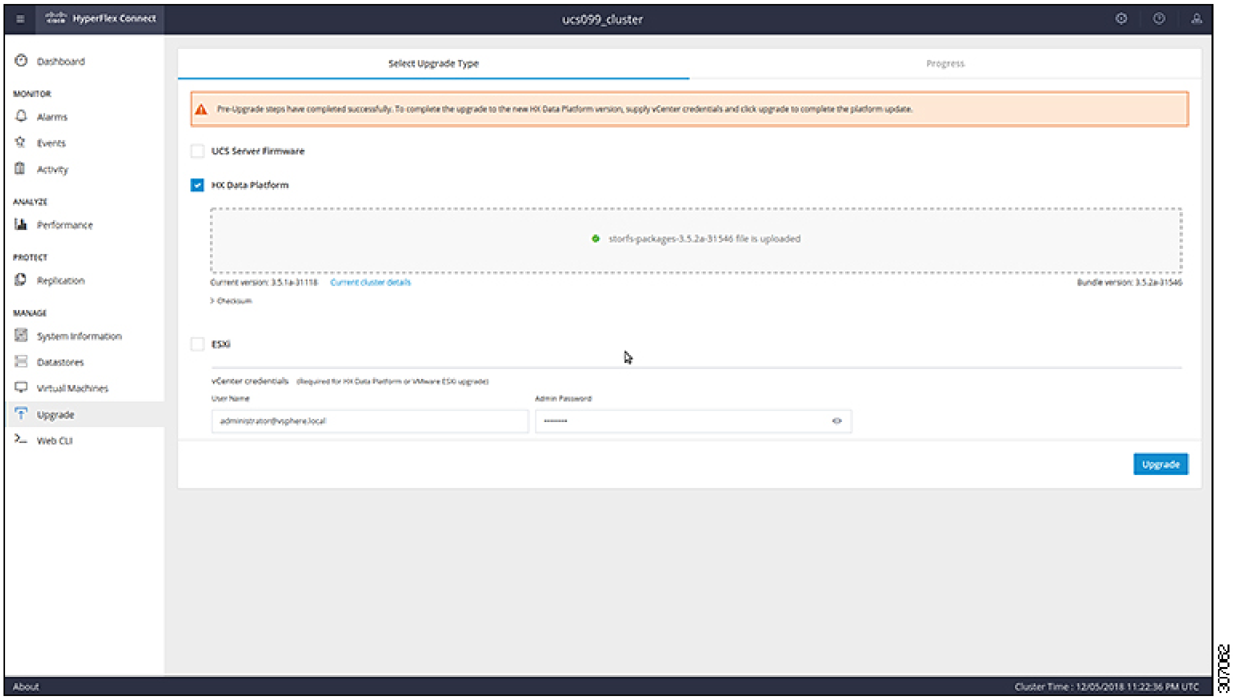
ucsb-001h In Progress — Upgrading HX Management VIB on node.

Cluster Time : 12/05/2018 3:04:32 PM PST

Step 5 When the Pre-Upgrade upgrade (management packages upgrade) process is completed, the HX Connect UI prompts you so with an onscreen message. The software will again ask you which component you want to upgrade. Click **Upgrade** again the complete the HX data platform part of the upgrade.

Note The cluster upgrade is not complete until the full upgrade is initiated. The upgrade is only partially complete after the pre-upgrade process (as outlined in step 4).

Figure 5: Completing the Pre-Upgrade Process



Pre-Upgrade steps have completed successfully. To complete the upgrade to the new HX Data Platform version, supply vCenter credentials and click upgrade to complete the platform update.

□ UCS Server Firmware

☑ HX Data Platform

storfs-packages-3.5.2a-31546 file is uploaded

Current version: 3.5.1a-31118 Current cluster details

Bundle version: 3.5.2a-31546

> Checksum

□ ESXi

vCenter credentials (Required for HX Data Platform or VMware ESXi upgrade)

User Name: administrator@vsphere.local

Admin Password: ••••••••

Cluster Time : 12/05/2018 11:22:36 PM UTC

Manual Bootstrap Upgrade Process

The manual bootstrap process enables you to upgrade the Cisco HX Data Platform and the Cisco HX Data Platform Plug-in.

Note Perform this procedure on the node that has the Cluster Management IP address.

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

Step 2 Navigate to **Actions** > **Summary** and note the **Cluster Management IP address**.

Step 3 SSH to the cluster management IP address with *root* privileges.

Step 4 Transfer the latest HX Data Platform upgrade bundle to the controller VM's /tmp directory.

Depending on your operating system, use you can either use SCP directly or download third-party tools, such as WinSCP or MobaXterm.

Step 5 From the controller VM shell, change to the `/tmp` directory.

Warning Do not use any folder other than `/tmp` and do not create any subfolders.

Step 6 Un-compress the package using `tar -zxvf <storfs package name>.tgz`.

Example:

This un-compresses and extracts all files to the root of the `/tmp` folder.

Step 7 Invoke the **cluster-bootstrap.sh** script to bootstrap packages for upgrade. Execute the command

```
~# ./cluster-bootstrap.sh
```

Enter the vCenter FQDN or IP address and administrator level username and password.

Wait for the system management service to restart and the bootstrap process to complete. Verify if the HX Data Platform Plug-in is now updated.

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 `vmnic3` 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>`

Entering Cisco HyperFlex Maintenance Mode

Using the Cisco HyperFlex (HX) Connect User Interface

Note Maintenance Mode was introduced in Cisco HyperFlex Release 2.5(1a) and 2.5(1b).

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 was introduced in Cisco HyperFlex Release 2.5(1a) and 2.5(1b).

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.

CHAPTER 6

Upgrade Procedures

Recommended Upgrade Method

For both combined upgrade and split upgrade, Cisco recommends upgrading the HyperFlex components in the following order for optimizing the upgrade time:

Note Make sure to upgrade the vCenter to the desired version based on the ESXi version and recommendation from VMware before upgrading ESXi.

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.

1. Upgrade Cisco UCS Infrastructure
2. Upgrade Cisco HX Data Platform
3. Upgrade Cisco customized VMware ESXi
4. Upgrade Cisco UCS firmware

Post vCenter Upgrade Tasks

If the extension is not working, and HyperFLex and vCenter are upgraded to compatible version, perform the following steps:

Note If you have more than one HyperFlex cluster, then you must first update all HX clusters to compatible HX versions for the corresponding vCenter versions prior to attempting to reregister. Do not unregister com.springpath.sysmgmt unless all clusters are removed from the vCenter.

Before you begin

Verify the extension is working. If so, then there is no need to perform any post upgrade tasks.

Step 1 Try to reregister the extenstion. If the extension still does not work, then continue with the next steps.

Step 2 Unregister the extension.

Example:

```
com.springpath.sysmgmt.domain-<id>
```

```
com.springpath.sysmgmt
```

Use the mob browser https://<vCenter IP or FQDN>/mob (content > extensionManager path and Invoke UnregisterExtension method).

Note We recommend to remove the cluster before unregistering extensions.

Step 3 Re-register the Springpath plug-in using:

Example:

```
stcli cluster reregister
```

Note You can use **`stcli cluster reregister --h`** for help and then continue with the reregistration.

Online Upgrade Process Workflow

Attention If you are running HyperFlex release 3.5(1a) or later, you can upgrade the Cisco HX Data Platform by performing the auto-bootstrap process from the HX Connect UI (Auto Bootstrap Upgrade Process from HX Connect UI, on page 24). However, if you are running a HyperFlex release that is earlier than release 3.5(1a) you must run the manual bootstrap process to upgrade the Cisco HX Data Platform (Manual Bootstrap Upgrade Process, on page 28).

When using the online upgrade process workflow, consider the following:

- First upgrade Cisco UCS infrastructure to the latest version and then use the automated upgrade workflow for a combined upgrade of Cisco UCS firmware and Cisco UCS Data Platform. Online upgrade uses host firmware packages to upgrade all server endpoints.
- During online upgrade, as one node is being upgraded (placed into maintenance mode), the number of tolerated node failures is reduced based on the **Data Replication Factor** and the **Access Policy settings**.

See Entering Cisco HyperFlex Maintenance Mode, on page 30 for the procedures on how to access Cisco HyperFlex Maintenance Mode.

- If upgrading both HXDP and UCS firmware, combined upgrade can be selected through HX Connect depending on the length of the maintenance window.
- Do not use Firefox browser. It is not supported due to an outdated version of flash that is bundled with the browser.

Note Cisco UCS Manager infrastructure upgrade is only supported using AutoInstall and the direct server firmware upgrade should be performed only through the upgrade orchestration framework provided by the HX Data Platform Plug-in.

Note During the online upgrade process, do not acknowledge server reboot pending activities from UCS Manager. Doing so will interrupt the upgrade process and can cause storage outage. HyperFlex will automatically reboot each node.

The following table summarizes the online upgrade 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. **Note** HyperFlex Infrastructure Upgrade (fabric interconnect, rack-server, blade chassis) requires that you upload A, B and C packages to UCSM prior to initiating upgrade.	Downloading Software, on page 21
2.	Ensure that the *hx-storage-data* and *vMotion* upstream switches are configured for full network failover capability before proceeding forward. Otherwise the HyperFlex Cluster becomes offline and all datastores unmount from the ESXi hosts.	Test Upstream Network Connectivity, on page 22
3.	Upgrade Cisco UCS Infrastructure bundle as required. **Note** It is important that you manually upgrade the UCS infrastructure first before initiating the upgrade sequence of the HyperFlex components as outlined in Recommended Upgrade Method, on page 33. The upgrade feature of the HX Platform software will not upgrade the UCS infrastructure bundle. This upgrade is a manual process.	Upgrading Cisco UCS Infrastructure Using Cisco UCS Manager, on page 45

Step	Description	Reference
4.	Bootstrap to upgrade Cisco HX Data Platform. Use the bootstrap procedure that matches your current deployment.	HX Release 3.5(1a) and later: • Auto bootstrap is supported beginning with HX release 3.5(1a). Auto Bootstrap Upgrade Process from HX Connect UI, on page 24 HX Release earlier than 3.5(1a): • Manual cluster bootstrap is required HX releases earlier than 3.5(1a).Manual Bootstrap Upgrade Process, on page 28
5.	Disable snapshot schedule, on the bootstrapped storage controller VM. **Note** It is enough to run this script on one of the controller nodes.	Run the command `stcli snapshot-schedule --disable`.
6.	Log in to HX Connect with administrator credentials.	
7.	Start combined upgrade of: • HX Data Platform and UCS Firmware • HX Data Platform and Hypervisor Software	Upgrading Your HyperFlex Cluster Using the HX Connect UI, on page 42
	Attention To perform a split upgrade, you must upgrade HX Data Platform first. After HX Data Platform is upgraded to 3.5(1x), you can perform a split upgrade of UCSM only and/or ESXi only. When only UCS firmware is being upgraded, you may see the upgrade process pause at the validation screen after the fabric interconnect discovery. It may be a network connectivity failure issue, however, in most cases, it just requires waiting for the process to finish.	Upgrading Cisco UCS Server Firmware Using the HX Connect UI, on page 50
8.	Confirm that the upgrade task is complete.	Post Upgrade Tasks, on page 71
9.	Dynamic certificate creation.	Starting with 4.0(2a) release, Dynamic self-signed certificate are generated rather than static certificates.

Step	Description	Reference
10.	On the same controller VM, enable snapshot schedule.	Run the command `stcli snapshot-schedule --enable`.

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.	Downloading Software, on page 21
2.	Ensure that the *hx-storage-data* and *vMotion* upstream switches are configured for full network failover capability before proceeding forward. Otherwise the HyperFlex Cluster becomes offline and all datastores unmount from the ESXi hosts.	Test Upstream Network Connectivity, on page 22
3.	Upgrade Cisco UCS Infrastructure bundle as required. **Note** It is important that you manually upgrade the UCS infrastructure first before initiating the upgrade sequence of the HyperFlex components as outlined in Recommended Upgrade Method, on page 33. The upgrade feature of the HX Platform software will not upgrade the UCS infrastructure bundle. This upgrade is a manual process.	Upgrading Cisco UCS Infrastructure Using Cisco UCS Manager, on page 45

Step	Description	Reference
4.	Launch the vSphere Web Client and power down all user VMs residing on HX servers and all user VMs running on HX datastores. This includes VMs running on compute-only nodes. After the VMs have been shut down, verify the health state of the cluster and perform a graceful shutdown. **Important** HyperFlex controller VMs (stCtlVMs) must remain powered on.	Graceful Shutdown of a HX Cluster, on page 23
5.	Manually stage the correct firmware version before starting the upgrade process.	Modifying Host Firmware Package Using Cisco UCS Manager, on page 24
6.	Shutdown the HyperFlex Controller VMs (stCtlVMs).	In vCenter, right-click on each HX Controller VM (stCtlVM) and select **Power** > **Shut Down Guest OS**.
7.	Once the Controller VMs are shutdown, place the ESXi hosts into Maintenance Mode.	In vCenter, right-click on each ESXi host select **Maintenance Mode** > **Enter Maintenance Mode**.
8.	Acknowledge the pending reboot on the servers that comprise your HX cluster nodes, including both converged nodes and compute-only nodes connected to the cluster. Wait until all nodes are upgraded. Confirm that correct firmware packages have been installed before proceeding.	
9.	Once the ESXi hosts have booted, take them out of Maintenance Mode. Now the controller VM should come back online.	In vCenter, right-click on each ESXi host select **Maintenance Mode** > **Exit Maintenance Mode**.

Step	Description	Reference
10.	Bootstrap to upgrade the Cisco HX Data Platform Plug-in. **Important** • Be sure to copy the bootstrap file to the controller VM `/tmp` directory. • Ensure that you confirm the version of the plug-in in the vCenter **Administration** > **Client Plug-Ins** page.	Manual Bootstrap Upgrade Process, on page 28
11.	Disable snapshot schedule, on the bootstrapped storage controller VM. **Note** It is enough to run this script on one of the controller nodes.	Run the command `stcli snapshot-schedule --disable`.
12.	From the same controller VM, begin the upgrade.	Upgrading Your HyperFlex Cluster Using the HX Connect UI, on page 42 Offline Upgrade Using CLI, on page 40
13.	Confirm that upgrade is complete.	Post Upgrade Tasks, on page 71
14.	After the upgrade is complete, start the cluster and power on VMs.	Start Cluster and Power On VMs , on page 41
15.	On the same controller VM, enable snapshot schedule.	Run the command `stcli snapshot-schedule --enable`.

Offline Upgrade Guidelines

Important

- --ucsm-host and --ucsm-user parameters are required when you are upgrading from 1.7x to 1.8x. These parameters must not be used when moving up from 1.8(1a)/1.8(1b) to 2.0(1a) as we are not changing the Cisco UCS server firmware version.

Before you proceed, with either combined or split upgrade consider the following guidelines:

- The package name must match the file that you uploaded to the controller VM.
- Enter passwords when prompted.
- 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 Using CLI

Important If you need to perform a split upgrade, you must upgrade HX Data Platform first. After HX Data Platform is upgraded to Release 3.5(1x), you can perform a split upgrade of UCSM only and/or ESXi only.

Combined Upgrade of Cisco Cisco HX Data Platform, ESXi and Cisco UCS Firmware

M5 Servers

```
# stcli cluster upgrade --components ucs-fw, hxdp, hypervisor --location/tmp/
<storfs package name,ESXi package name> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsm5-fw-version <UCSM Firmware Version>
```

Example for M5 Servers:

```
~# stcli cluster upgrade --components ucs-fw, hxdp, hypervisor --location
/tmp/storfs-packages-3.5.1a-19712.tgz
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucs5fw-version '3.1(2g)'
```

M4 Servers

```
# stcli cluster upgrade --components ucs-fw, hxdp, hypervisor --location/tmp/
<storfs package name, ESXi package name> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsfw-version <UCSM Firmware Version>
```

Example for M4 Servers:

```
~# stcli cluster upgrade --components ucs-fw, hxdp, hypervisor --location
/tmp/storfs-packages-3.5.1a-19712.tgz
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucsfw-version '3.1(2g)'
```

Combined Upgrade of Cisco Cisco HX Data Platform and ESXi

M5 Servers

```
# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/hxupgrade_bundle.tgz
--hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

Example for M5 Servers:

```
~# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/hxupgrade_bundle.tgz
 --hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

M4 Servers

```
# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/hxupgrade_bundle.tgz
--hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

Example for M4 Servers:

```
~# stcli cluster upgrade --components hxdp,hypervisor --location /tmp/hxupgrade_bundle.tgz
 --hypervisor-bundle /tmp/esxiupgrade_bundle.zip
```

Combined Upgrade of Cisco HX Data Platform and Cisco UCS Firmware

M5 Servers

```
# stcli cluster upgrade --components hxdp,ucs-fw --location/tmp/
<storfs package name> --vcenter-user <vcuser> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsm5-fw-version <UCSM Firmware Version>
```

M4 Servers

```
# stcli cluster upgrade --components hxdp,ucs-fw --location/tmp/
<storfs package name> --vcenter-user <vcuser> --ucsm-host <IP/FQDN of UCSM>
--ucsm-user <UCSM User> --ucsfw-version <UCSM Firmware Version>
```

Example for M4 Servers:

```
~# stcli cluster upgrade --components hxdp,ucs-fw --location
/tmp/storfs-packages-1.8.1c-19712.tgz --vcenter-user administrator@vsphere.local
--ucsm-host eng-fi16.eng.storvisor.com --ucsm-user admin --ucsfw-version '3.1(2b)'
```

Start Cluster and Power On VMs

After the upgrade is complete and the cluster has been upgraded, log out and log back in to vCenter to see upgrade changes.

Step 1 After the upgrade is complete, start your cluster.

Step 2 Login to any controller VM through SSH.

```
# stcli cluster start
```

Example:

```
HyperFlex StorageController 1.8(1c)
Last login: Wed Sept 21 23:54:23 2016 from pguo-dev.eng.storvisor.com
 root@ucs-stclivm - 384 -1;~# stcli cluster upgrade-status
Cluster upgrade succeeded. Cluster version: 1.8(1c)
root@ucs-stctlvm-384;~# stcli cluster start
waiting for Cluster to start on nodes: [ucs-383, ucs-384, ucs-385, ucs-386]
```

This will start the cluster and mount the HX datastores. Wait for cluster to come online. You will see the prompt:

```
Started cluster on nodes; [ucs-383, ucs-384, ucs-385, ucs-386]
Cluster is online
root@ucs-stctlvm-384-1;~#
```

Step 3 Wait for cluster to become healthy before starting the VMs. Run command:

```
~# stcli clustr info| grep health
```

Example:

```
root@SpringpathControllerZRVF040451;~# stcli cluster info | grep health
healthState: healthy
state: healthy
 storage cluster is healthy
```

Step 4 After the cluster is healthy, launch vSphere Web Client or Thick Client, navigate to **Hosts and Cluster** > **Datacenter** > **Cluster** > . Right click, select **Power**> **Power On** to start the VMs.

Upgrading Your HyperFlex Cluster Using the HX Connect UI

Note **Hypercheck Health Check Utility**— Cisco recommends running this proactive health check utility on your HyperFlex cluster prior to upgrade. These checks provide early visibility into any areas that may need attention and will help ensure a seamless upgrade experience. For more information see the Hyperflex Health & Pre-Upgrade Check Tool TechNote for full instructions on how to install and run Hypercheck.

Important Use the HX Connect UI when upgrading from a current HX Data Platform version of 2.5(1a) or later releases.

Step 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. See Downloading Software, on page 21 for more details.

Step 2 Ensure that the *hx-storage-data* and *vMotion* upstream switches are configured for full network failover capability before proceeding forward. Otherwise the HyperFlex Cluster becomes offline and all datastores unmount from the ESXi hosts. See Test Upstream Network Connectivity, on page 22 for more details.

Step 3 Upgrade Cisco UCS Infrastructure bundle as required. See Upgrading Cisco UCS Infrastructure Using Cisco UCS Manager, on page 45 for more details.

Note It is important that you manually upgrade the UCS infrastructure first before initiating the upgrade sequence of the HyperFlex components as outlined in Recommended Upgrade Method, on page 33. The upgrade feature of the HX Platform software will not upgrade the UCS infrastructure bundle. This upgrade is a manual process.

Step 4 Bootstrap to upgrade Cisco HX Data Platform.

Note If you are running HyperFlex release 3.5(1a) or later, you can upgrade the Cisco HX Data Platform by performing the auto-bootstrap process from the HX Connect UI (Auto Bootstrap Upgrade Process from HX Connect UI, on page 24). However, if you are running a HyperFlex release that is earlier than release 3.5(1a) you must run the manual bootstrap process to upgrade the Cisco HX Data Platform (Manual Bootstrap Upgrade Process, on page 28).

Step 5 Log in to HX Connect.

a) Enter the HX Storage Cluster management IP address in a browser. Navigate to *https://<storage-cluster-management-ip>*.
b) Enter the administrative username and password.
c) Click **Login**.

Step 6 In the Navigation pane, select **Upgrade**.

Step 7 Choose the type of upgrade from the **Select Upgrade Type** page.

Caution After manual bootstrap, validation will fail if you perform UCS only, ESXi only, or UCS and ESXi combined upgrade. For successful upgrade, Cisco recommends the following upgrade types:

- **HX Data Platform** only upgrade, followed by **UCS Firmware** and/or **Hypervisor Software** upgrade
- **HX Data Platform** and **UCS Firmware**
- **HX Data Platform** and **Hypervisor Software**
- **HX Data Platform**, **UCS Firmware**, and **Hypervisor Software**

Step 8 Depending on the type of upgrade you want to perform, complete the following fields on the **Enter Credentials** tab.

UCS Server Firmware

Field	Essential Information
UCS Manager Hostname field	Enter the Cisco UCS Manager FQDN or IP address. Example: *10.193.211.120*.
User Name field	Enter the Cisco UCS Manager <*admin*> username.
Admin Password field	Enter the Cisco UCS Manager <*admin*> password.
Discover button	Click **Discover** to view the *current UCS firmware package* version, in the **Current Version** field.

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-3.5.2a-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 stored in a separate text file at the `/tmp` directory where the upgrade package was downloaded. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle.

ESXi

Note The ESXi upgrade option is supported in the HyperFlex Connect UI for HyperFlex release 3.5(1a) or later.

UI Element	Essential Information
Drag the ESXi file here or click to browse field	Upload the latest *Cisco HyperFlex Custom Image Offline Bundle for upgrading existing ESXi* hosts from Download Software - HyperFlex HX Data Platform. Example: *HX-ESXi-6.5U2-10884925-Cisco-Custom-6.5.2.4-upgrade-bundle.zip*.
Current version field	Displays the current ESXi version.
Current hypervisor details field	Lists the HyperFlex cluster details like the **Hypervisor version** and **Cluster upgrade state**.
Bundle details field	Displays the ESXi version of the uploaded bundle.

vCenter Credentials

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

Step 9 Click **Upgrade** to begin the cluster upgrade process.

Step 10 The **Validation Screen** on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any. 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.

CHAPTER 7

Upgrading Cisco HyperFlex Software Components

Overview

This chapter provides detailed instructions to upgrade the supported HyperFlex software components once your HyperFlex cluster has been upgraded.

Note 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 use the Cisco HyperFlex Systems Upgrade Guide for Unsupported Cisco HX Releases guide.

Upgrading Cisco UCS Infrastructure Using Cisco UCS Manager

Note Ensure that the hx-storage-data and vMotion upstream switches are configured for **Jumbo Frames** before proceeding forward, otherwise the HyperFlex Cluster will become offline and all datastore will unmount from the ESXi hosts.

Step 1 Open the UCS Manager GUI.

Step 2 Select **Equipment** > **Firmware Management > Firmware auto-install**.

Step 3 Click **Install Infrastructure Firmware**.

Step 4 Check **Upgrade Now** box.

Step 5 Wait for IOM to be upgraded (if the UCS blade server chassis is present).

a. Select **Equipment** > **Installed Firmware**, expand each chassis and check the **Update Status** of the IO Module.

b. During upgrade, the **Update Status** of the IO Modules will be **Upgrading**.

c. IOMs will be in a Pending Next Boot for Activate Status once the Update process completes. When IOM upgrade has completed, the Update Status of the IO Modules is set to **Ready**.

Step 6 Wait for Subordinate FI to be activated.

a. Select **Equipment** > **Installed Firmware > Fabric Interconnects**.

b. Check the **Activate Status** of the kernel and switch images. During upgrade, the Activate Status is set to **Activating**.

Step 7 During FI reboot, all HX traffic will be forwarded to primary FI (based on ESXi vSwitch failover policy). This will cause a brief traffic interruption. This will not cause storage IO failures.

Step 8 Verify subordinate FI has rebooted and joined the UCS cluster.

a. Select **Equipment** > **Installed Firmware > Fabric Interconnects**.

b. After activation, the Activate Status of the FI is set to Ready.

c. Check the Overall Status of the FI is **operable**.

d. Check the kernel and switch versions of the FI match the desired and updated version.

e. Check the FI has no fault.

f. Check the FI cluster membership is **Subordinate**.

Step 9 If the UCS blade server chassis is present, wait for IOM activation to complete. Only the IOMs connected to the subordinate FI will enter Ready state, IOMs attached to the Primary FI will remain in *Pending Next Boot* Activate Status.

a. Select **Equipment** > **Blade Chassis > IO Module**.

b. Wait for the Activate Status of IO module to change to Ready.

Step 10 Wait until HX traffic is re-pinned to both FIs.

Wait for UCS Manager vNIC faults to be cleared. The fault clearing indicates ESXi has loaded the ENIC driver and the interface is up. The traffic is not re-pinned immediately when the network interface goes up because ESXi has a fail back timer. But the Net.teampolicyupdelay timer is very low by default (100ms).

Step 11 Verify the HX Cluster is online, and healthy before rebooting the primary fabric interconnect.

Access summary tab from the vSphere Web Client Navigator. Select **Home** > **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary**.

Step 12 In the UCS manager GUI, on the toolbar, click **Pending Activities**. Click on **Fabric Interconnects** tab that display the tasks requiring user acknowledgment before they can complete.

a. Click **Reboot Now** for each pending activity that you want to deploy immediately.

b. Click **OK**. Cisco UCS Manager immediately reboots the primary FI. This will cause the subordinate FI to become primary (FI failover).

Step 13 During FI reboot, all HX traffic will be forwarded to the new primary FI. This will cause a brief traffic interruption. However, this will not cause storage IO failures.

Step 14 Wait for UCS Manager to be disconnected, then reconnected on the other FI. This is because a UCS Manager fail over occurs due to primary FI reboot.

Step 15 Check subordinate FI has become primary.

Check that the FI cluster membership is **Primary**.

Step 16 Wait for FI to be activated.

a. Select **Equipment** > **Installed Firmware** > **Fabric Interconnects**.

b. Wait for the **Activate Status** of the FI to be **Ready**.

c. Check the **Overall Status** of FI is **operable**.

d. Check the FI has no fault.

Step 17 Verify FI has rebooted and joined the UCS cluster as subordinate.

Check that the FI cluster membership is **Subordinate**.

Step 18 Wait for IOM activation to complete

a) Select **Equipment** > **Blade Chassis > IO Module**.
b) Wait for the **Activate Status** of the IP module to be **Ready**.
c) You can monitor the status on the FSM tab.

Note You will lose connectivity to UCS Manager throughout the entire upgrade. This is a normal behavior.

Step 19 Wait until HX traffic is re-pinned to both FIs.

In the UCS manager GUI, wait until all server vNIC faults have been cleared.

Step 20 Verify the HX Cluster is online, and healthy after rebooting the FI.

Access summary tab from the vSphere Web Client Navigator. Select **Home** > **vCenter Inventory Lists > Cisco HyperFlex Systems > Cisco HX Data Platform > cluster > Summary**.

Upgrading Cisco HX Data Platform

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 .
- Complete steps 1 to 6 in the *Online Upgrade Process Work flow*.

  - Upgrade Cisco UCS Infrastructure.
  - Bootstrap to upgrade Cisco HX Data Platform plug-in.
  - Disable snapshot schedule, on the bootstrapped storage controller VM.
  - Log in to the Cisco HX Data Platform plug-in with administrator credentials.

- Pause replication using the run the `stcli dp schedule pause` command and enable it after upgrade using the `stcli dp schedule resume` command. For more detailed steps, see Pausing Replication.
- If DRS is *Enabled*, the VMs are automatically vMotioned to other hosts.

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

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

Step 2 Select **Upgrade Cluster**.

Step 3 Select only **HX Data Platform**.

Step 4 Navigate to the `.tgz` package file on your local PC.

Upload the Cisco HX Data Platform upgrade bundle. This is the same .tgz package file that was used to upgrade the HX Data Platform Plug-in.

Step 5 Enter administrator level vCenter credentials.

(Optional) Enter the MD5 **Checksum #** information under **Advanced Options**. The file checksum can be found on the Cisco.com download page by clicking on the download title to reveal the md5 checksum.

This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle.

Step 6 Click **Upgrade**.

The Validation screen shows the progress of checks performed. Fix validation errors, if any.

The upgrade process proceeds as follows:

- HyperFlex cluster readiness for upgrade is checked.
- One by one, the HX nodes enter maintenance mode.
- HyperFlex vSphere Installation Bundles on Hypervisor are upgraded.
- Cisco HX Data Platform is upgraded.
- HX node exits maintenance mode.
- Cluster will begin to rebuild back to full health.
- Once the cluster is healthy, upgrade moves on to the next node in the HyperFlex cluster.

During cluster upgrade, if the orchestration node reboots or power cycles due to power issue, the cluster upgrade will be stuck. Once the node is up, restart the cluster upgrade process after cleaning the cluster system using the following command:

```
stcli cluster upgrade --components hxdp –clean
```

If the clean-up command fails, restart the stMgr service on all control VMs (ctrlVM) by running the following command:

```
#restart stMgr
```

Then, clean the cluster system by rerunning the following command:

```
stcli cluster upgrade --components hxdp –clean
```

Here is a sample code:

```
root@ucs-stctlvm-385-1:~# stcli cluster upgrade --clean --components hxdp
##Forcefully cleaned up upgrade progress
root@ucs-stctlvm-385-1:~# stcli cluster upgrade --status
##No active upgrade found. Upgrade progress available after triggering an upgrade
```

Upgrading Cisco UCS Firmware

Important

- Do not manually acknowledge the pending activities in Cisco UCS Manager.
- Make sure that the HX Data Platform is already upgraded. When performing a split upgrade, ensure Cisco UCS Firmware is upgraded around the same time as the HX Data Platform upgrade.

Before you begin

- Complete pre-upgrade validation checks.
- Complete steps 1 to 3 in the *Online Upgrade Process Work flow*.
- Upgrade Cisco UCS Infrastructure.
- If DRS is *Enabled*, the VMs are automatically vMotioned to other hosts.

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

- Downgrading the UCSM firmware is not supported.

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

Step 2 Select **Upgrade Cluster**.

Step 3 Select only, **UCS Firmware**. Click **Next**.

Step 4 Enter administrator level UCS Manager credentials.

Field	Data
UCS Manager Host Name	For example: `eng-fi12.eng.storvisor.com`
User Name	<*admin*> username
Password	<*admin*> password

Step 5 Click **Discover** to view the *current firmware package* version.

Step 6 Type in the exact, latest version of Cisco UCS firmware in the **Target version** field.

Step 7 Click **Upgrade**.

The Cisco UCS servers are now upgraded with the desired firmware packages. The pending activities will be automatically acknowledged in a rolling fashion.

Note You can monitor the progress in the Cisco UCS Manager GUI, under the **FSM** tab for the service profile.

The Validation screen shows the progress of checks performed. Fix validation errors, if any.

The upgrade process proceeds as follows:

- HyperFlex cluster readiness for upgrade is checked.
- One by one, the HX nodes enter maintenance mode.
- The HX Data Platform requests Cisco UCS Manager to begin firmware upgrade. This process can take up to 1 hour.

  Note You can monitor the progress in the Cisco UCS Manager GUI, under the **FSM** tab for the service profile.
- HX node exits maintenance mode.
- Cluster begins to rebuild back to full health.
- Once the cluster is healthy, upgrade moves on to the next node in the HyperFlex cluster.

What to do next

Confirm that the upgrade is complete. See *Post Upgrade Tasks* for more details.

Upgrading Cisco UCS Server Firmware Using the HX Connect UI

Before you begin

- Complete pre-upgrade validation checks.
- Complete steps 1 to 3 in the *Online Upgrade Process Work flow*. See Online Upgrade Process Workflow, on page 34 for more details.

- Upgrade Cisco UCS Infrastructure.
- If DRS is *Enabled*, the VMs are automatically vMotioned to other hosts.

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

- Downgrading the UCSM firmware is not supported.

Step 1 Log in to HX Connect.

a) Enter the HX Storage Cluster management IP address in a browser. Navigate to *https://<storage-cluster-management-ip>*.

b) Enter the administrative username and password.

c) 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 Hostname field	Enter the Cisco UCS Manager FQDN or IP address. Example: *10.193.211.120*.
User Name field	Enter the Cisco UCS Manager <*admin*> username.
Admin Password field	Enter the Cisco UCS Manager <*admin*> password.
Discover button	Click **Discover** to view the *current UCS firmware package* version, in the **Current Version** field.

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. 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.

Upgrading ESXi

⚠ Caution **Using VMware Update Manager (VUM) to upgrade ESXi is discouraged.**

If you are using VUM to upgrade ESXi do the following:

- Use VUM one host at a time.
- Make sure that the cluster is in healthy state before moving on to the next node.
- Do not use VUM to upgrade ESXi across a cluster, as there is no guarantee that the cluster will be healthy by the time VUM moves on to the next node.

The ESXi hypervisor version can be upgraded with no disruption to the HyperFlex cluster workload. This is achieved by performing an online rolling upgrade of each node in the HX cluster.

Important

- ESXi upgrade requires a manual online upgrade.
- When upgrading VMware ESXi from 5.5 U3b through any version up to 6.0 U2, please contact Cisco TAC.
- Use the ESXi command line interface `esxcli` for upgrading or updating ESXi.
- Replace the build numbers provided in the examples below with the latest version.

Before you begin

- Complete pre-upgrade validation checks. See *upgrade prerequisites*.
- Ensure that you upgrade vCenter to a compatible version before beginning ESXi upgrades on the hosts.

ESXi Patch Only Upgrade

It is not recommended to use VMware vSphere Update Manager to upgrade the ESXi running on a HyperFlex cluster. Always use the HX Connect Upgrade method to upgrade the ESXi (including the ESXi patch builds) running on HyperFlex cluster. This upgrade method requires no manual intervention if the VMware DRS is enabled on the cluster. This automated process puts the nodes in maintenance mode and reboots one at a time.

1. Check the HyperFlex upgrade guide for currently running HXDP version and confirm the ESXi patch is supported with current HXDP and UCS Manager versions.
2. Check the VMware vCenter and ESXi compatibility matrix and confirm the vCenter version is supported with the new ESXi patch.
3. Before starting the ESXi upgrade, upgrade the vCenter to VMware supported version.
4. If DRS is Enabled, the VMs are automatically vMotioned to other hosts.

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

Step 1 Download ESXi upgrade package. When upgrading ESXi from 6.0 Ux to any newer version, use the offline zip file from Download Software.

Example filename: `HX-Vmware-ESXi-60U2-4192238-Cisco-Custom-Bundle-6.0.2.3.zip`

Attention Do not use the HX ISO file or any other VMware ISO to attempt an ESXi upgrade.

Step 2 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 3 Remote secure copy the ESXi upgrade bundle to an appropriate folder with sufficient space.

To 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 4 Log in to 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-6.0U3-13003896-Cisco-Custom-6.0.3.9-upgrade-bundle.zip
Name                                       Vendor  Acceptance Level  Creation Time
Modification Time
-----------------------------------------  ------  ----------------  -------------------
-------------------
HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9  Cisco   PartnerSupported  2019-04-02T00:14:56
2019-04-02T13:38:34
```

Step 5 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-60U2-4192238-Cisco-Custom-Bundle-6.0.2.3.zip

-p HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9
```

Step 6 Once the upgrade completes, restart the ESXi host.

```
esxcli system shutdown reboot -r Update -d 10
```

Step 7 After the ESXi host comes up, verify that the host has booted up with the correct version.

```
vmware -vl
```

Step 8 Wait for the ESXi host to auto reconnect to vCenter. In some upgrade scenarios it may be necessary to force ESXi to reconnect from vCenter. Right-click on the host and select **Connection** > **Connect**.

Step 9 Exit maintenance mode using the vSphere Web Client.

Step 10 Ensure that the cluster becomes healthy between each ESXi upgrade.

```
stcli cluster storage-summary --detail
```

Step 11 Repeat this process for all hosts in the cluster in a sequence.

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

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.

CHAPTER 8

HyperFlex Edge Upgrade

Overview

This section provides information related to upgrading a Cisco HyperFlex Edge system.

Important

- For upgrading a HyperFlex Edge system, use split upgrade only. Do not use combined upgrade.
- Automated ESXi upgrade should be performed via HX Connect or Intersight.
- When upgrading a HyperFlex Edge system, only HyperFlex Data Platform can be upgraded from the HX Connect UI. Do not select the UCS Server firmware option. Instead, perform the firmware upgrade separately using the Host Upgrade Utility (HUU) tool or the Integrated Management Controller (IMC) Supervisor.
- Review the Cisco HyperFlex Upgrade Guidelines in the Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems.

Upgrading HyperFlex Edge Using vSphere Web Client from 2.1 or Earlier Releases

Follow these steps when upgrading from a HyperFlex Data Platform version prior to 2.5(1a):

Step 1 Bootstrap to upgrade Cisco HX Data Platform Plug-in. See Manual Bootstrap Upgrade Process, on page 28.

Important
- Be sure to copy the bootstrap file to the controller VM `/tmp` directory.
- Ensure that you confirm the version of the plug-in in the vCenter **Administration** > **Client Plug-Ins** page.

Step 2 Disable snapshot schedule, on the bootstrapped storage controller VM. Run the command `stcli snapshot-schedule --disable`.

It is enough to run this script on one of the controller nodes.

Step 3 Log in to the vSphere Web Client Plug-in with administrator credentials.

Step 4 Perform a split upgrade of the HX Data Platform only.

Step 5 Confirm that upgrade is complete. See Post Upgrade Tasks for HyperFlex Edge, on page 59 for more details.

Step 6 On the same controller VM, to enable snapshot schedule, run the command `stcli snapshot-schedule --enable`.

Upgrading HyperFlex Edge Using HX Connect from 2.5(1a) or Later Releases

When upgrading a HyperFlex Edge system not managed by Cisco Intersight or prior to a HX release 4.0(2a) use the HX Connect procedure below.

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

For upgrading a HyperFlex Edge system managed using Cisco Intersight or for systems running HX release 4.0(2a), follow the steps listed here.

Upgrade guidelines:

- Only Cisco HyperFlex Edge clusters that are deployed through Cisco Intersight can be upgraded.
- Additionally, upgrade can be initiated only from the Organization to which the HyperFlex Cluster Profile belongs to. For example, if a cluster is shared between Org A and Org B and the Cluster Profile belongs to Org A, upgrade can be performed only from Org A.
- All clusters that are selected for the upgrade must be HyperFlex Edge clusters.
- Ensure that the cluster is at HyperFlex Data Platform version 4.0(1a) or later.

See full procedure here: Upgrading Cisco HyperFlex Edge Systems with Cisco Intersight.

Step 1 Bootstrap to upgrade Cisco HX Data Platform Plug-in. See Manual Bootstrap Upgrade Process, on page 28 for more details.

Important Be sure to copy the bootstrap file to the controller VM `/tmp` directory.

Step 2 Log in to HX Connect.

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

Step 4 On the **Select Upgrade Type** page, select **HX Data Platform** only. Click **Continue**.

Step 5 Complete the following fields on the **Enter Credentials** page.

Upgrade HX Data Platform

UI Element	Essential Iformation
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-3.5.2a-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 stored in a separate text file at the `/tmp` directory where the upgrade package was downloaded. This is an optional step that helps you verify the integrity of the uploaded upgrade package bundle.

vCenter Credentials

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

Step 6 Click **Upgrade**.

Step 7 The **Validation Screen** on the **Upgrade Progress** page displays the progress of the checks performed. Fix validation errors, if any. Confirm that the upgrade is complete.

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.	Verify vMotion Configuration for HX Cluster, on page 29 Entering Cisco HyperFlex Maintenance Mode, on page 30
2.	Upgrade server firmware using the Host Upgrade Utility tool.	See Updating the Firmware on Cisco UCS C-Series Servers in the *Cisco Host Upgrade Utility User Guide*.
3.	Reboot the node back into ESXi. Exit HX maintenance mode.	Exiting Cisco HyperFlex Maintenance Mode, on page 31
4.	Wait until the cluster becomes fully healthy.	Viewing HyperFlex Cluster Health, on page 16
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.

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

If you are upgrading to Cisco IMC version 2.0(x), you must change the default Cisco IMC password.

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.
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**.

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 vCenter 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 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 in to any controller VM through SSH.

```
# ssh root@controller_vm_ip
```

Step 3 Confirm the HyperFlex Data Platform version.

```
# stcli cluster version


Cluster version: 2.5(1c)
Node HX02 version: 2.5(1c)
Node HX01 version: 2.5(1c)
Node HX03 version: 2.5(1c)
```

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

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

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

Step 5 Verify that the datastores are up and are mounted properly on the ESXi host.

From HX controller VMs run the command:

```
# stcli datastore list
```

From the ESXi host run:

```
# esxcfg-nas -l
```

Step 6 For each browser interface you use, empty the cache and reload the browser page to refresh the HX Connect content.

Replace Static Self-signed Certificate with Dynamic Self-signed Certificate

Description

When upgrading your Edge cluster to HyperFlex release 4.0(2a), the static self-signed certificates on the controller VMs are replaced with dynamically generated self-signed certificates and VC re-registration takes place during upgrade. However, if your cluster is upgraded to HX 4.0(2x) via Intersight, the static self-signed certificates do not get replaced.

Action

To manually replace the static self-signed certificates for dynamic self-signed certificates perform the following actions:

1. SSH to the cluster management IP.
2. Upload the contents from `/etc/springpath/secure/root_file.pub` which is used as the X-RootSessionID in the next step.
3. Run the following command to generate and install dynamic certificate on all the controller VMs.

   ```
   curl -v -X PUT -H "Accept: application/json" -H "Content-Type: application/json" -H
   "X-RootSessionID: <Contents_from_previous step>" -H "X-LoggedInUser: admin" -H "X-Scope:
   READ,MODIFY" -H "X-RequestInitiator: Internal"
   http://localhost:8000/securityservice/v1/certificate?option=dynamic
   ```

Note The above steps can be run in admin shell for post HX 4.5 clusters where **secureshell** is enabled.

Example

```
root@SpringpathController4AL5TXVEYU:~# curl -v -X PUT -H "Accept: application/json" -H
"Content-Type: application/json" -H "X-RootSessionID: 23cb2f3a806a31f3516e47357b5c6784" -H
 "X-LoggedInUser: admin" -H "X-Scope: READ,MODIFY" -H "X-RequestInitiator: Internal"
```

```
http://localhost:8000/securityservice/v1/certificate?option=dynamic
*   Trying 127.0.0.1...
* Connected to localhost (127.0.0.1) port 8000 (#0)
> PUT /securityservice/v1/certificate?option=dynamic HTTP/1.1
> Host: localhost:8000
> User-Agent: curl/7.47.0
> Accept: application/json
> Content-Type: application/json
> X-RootSessionID: 23cb2f3a806a31f3516e47357b5c6784
> X-LoggedInUser: admin
> X-Scope: READ,MODIFY
> X-RequestInitiator: Internal
>
< HTTP/1.1 200
< Content-Type: application/json
< Content-Length: 56
< Date: Wed, 03 Mar 2021 07:18:57 GMT
<
* Connection #0 to host localhost left intact
{"code":4,"type":"ok","message":"Installed certificate"}
```

CHAPTER 9

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.

Upgrade Guidelines for Stretched Cluster

- Review the Cisco HyperFlex Upgrade Guidelines in the Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems.
- Combined HXDP and UCS FW is not supported.
- UCS FW upgrade from HX-Connect is not supported.
- Manual cluster bootstrap is required for upgrade from a pre-3.5 release to 3.5(1a).

  Auto bootstrap is supported for upgrade from 3.5(1a) to later releases.
- When upgrading to any release from 3.0.x to 3.5.x or later releases:
  - If you manually bootstrap only one node, the **ESXi** checkbox will not appear under the **Select Upgrade Type** section of the **Cluster Upgrade** page. The ESXi upgrade option appears only after upgrading HX Data Platform to release 3.5.x or later releases.
  - If you manually bootstrap all the nodes to 3.5.x or later release, the **ESXi** checkbox will appear under the **Select Upgrade Type** section of the **Cluster Upgrade** page. However, you cannot perform an ESXi only upgrade at this point. You can do a combined upgrade of HX Data platform + ESXi.
- HyperFlex Witness node version 1.0.2 is supported from 3.5(1a) or later releases. An upgrade of the HyperFlex Witness node is not required when upgrading stretched clusters to 3.5(1a) or later releases.

- Hypercheck Health Check Utility— Cisco recommends running this proactive health check utility on your HyperFlex cluster prior to upgrade. These checks provide early visibility into any areas that may need attention and will help ensure a seamless upgrade experience. For more information see the Hyperflex Health & Pre-Upgrade Check Tool TechNote for full instructions on how to install and run Hypercheck.

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.
- 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**.

UI Element	Essential Information
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.

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 automatically acknowledges each server at the correct time.

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

Before you begin

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 Recommended Software Release and Requirements Guide.

- For supported versions see the *HX Data Platform Software Versions for HyperFlex Witness Node for Stretched Cluster* section of the Cisco HyperFlex Recommended Software Release and Requirements Guide
- 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:~# stcli cluster info | grep healthy
  ```

Step 1 Log in to 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 in to 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 r
oot@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.properties
```

Step 8 **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 9 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 Stretch Cluster 4.0(x)

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 in to 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-6.0U3-13003896-Cisco-Custom-6.0.3.9-upgrade-bundle.zip
Name                                        Vendor  Acceptance Level  Creation Time        Modification
 Time
-------------------------------------------  ------  ----------------  -------------------
-------------------
HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9  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-60U2-4192238-Cisco-Custom-Bundle-6.0.2.3.zip

-p HX-ESXi-6.0U3-13003896-Cisco-Custom-6.0.3.9
```

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.

```
stcli cluster storage-summary --detail
```

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 succesfully.

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

Step 2 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 3 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": [
          {
            "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 4 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 5 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 6 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 7 Repeat Steps 4, 5 and 6 again for the other site.

CHAPTER 10

Post Upgrade Tasks

Running Post Install Script

After the installation of a Stretched Cluster using the HX Data Platform Installer, run the post installation script to finalize the configuration and set the vMotion network up. You can also run this script at a future time if needed.

1. Log into a Cluster IP (CIP) through an SSH server using admin login.
2. Run the `hx_post_install` script.
3. Follow the prompts and enter the required information.

Confirm That Upgrade Is Complete

Step 1 Log in to 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 in to any controller VM through SSH.

```
# ssh root@controller_vm_ip
```

Step 4 Confirm the HyperFlex Data Platform version.

```
# stcli cluster version
```

```
Cluster version: 2.5(1c)
Node HX02 version: 2.5(1c)
Node HX05 version: 2.5(1c)
Node HX01 version: 2.5(1c)
Node HX03 version: 2.5(1c)
Node HX04 version: 2.5(1c)
```

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

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

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

Step 6 Verify that the datastores are up and are mounted properly on the ESXi host.

From the HX controller VMs:

```
# stcli datastore list
```

From the ESXi host:

```
# esxcfg-nas -l
```

Step 7 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 8 For each browser interface you use, empty the cache and reload the browser page to refresh the HX Connect content.

Check Firmware Versions in UCSM

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

For a complete list of hardware and software inter-dependencies, refer to respective UCSM release version using the UCS Hardware and Software Compatibility tool.

Verify If Cleaner Is Running

If Upgrade Fails

If upgrade fails, run cleaner. This is required even if you do not want to continue with an upgrade.

To run cleaner manually, restart the storage cluster cleaner using the following command.

stcli cleaner start [-h] [--id ID | --ip NAME]

Syntax Description

Option	Required or Optional	Description
--id ID	Optional.	ID of storage cluster node. The ID is listed in the `stcli cluster info` command.
--ip NAME	Optional.	IP address of storage cluster node. The IP is listed in the `stcli cluster info` command.

If Upgrade Completes

If upgrade completes, verify if cleaner is running. To obtain information about the storage cluster cleaner for the specified node, use the following command.

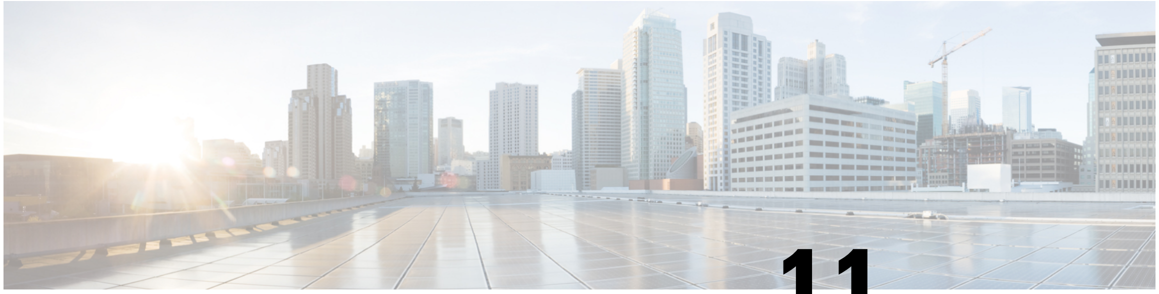
stcli cleaner info [-h] [--id ID | --ip NAME]

Syntax Description

Option	Required or Optional	Description
--id ID	Optional.	ID of storage cluster node. The ID is listed in the `stcli cluster info` command.
--ip NAME	Optional.	IP address of storage cluster node. The IP is listed in the `stcli cluster info` command.

Additional Post Upgrade Tasks

After verifying that your upgrade is complete, enable Cisco HyperFlex Smart Call Home. For more information, see the Cisco HyperFlex Smart Call Home Quick Start Guide.



CHAPTER 11

Known Issues

Overview

This chapter provides information to help you troubleshoot common problems that may occur during the Cisco HyperFlex upgrade process.

Offline Upgrade Cluster Start Command Error: Node Not Available

Description

After an offline upgrade, due to a VMware EAM issue, sometimes all the controller VMs do not restart. The `stcli start cluster` command returns an error: `Node not available`.

Action: Manually power on the controller VMs, then start the storage cluster.

Step 1 Manually power on the controller VMs.

a) Login to the vSphere Web Client.

b) Locate the controller VMs that are not powered on.

From the Navigator select, **vCenter Inventory Lists** > **Virtual Machines** > ***vm***.

Storage controller VMs, have the prefix, `stCtlVM`.

c) From the right-click or Actions menu select, **Power** > **Power On**.

d) Repeat until all the storage controller VMs are powered on.

Step 2 Restart the storage cluster.

a) Login to the command line of any controller VM.

b) Run the command.

```
# stcli cluster start
```

A Node Fails to Upgrade due to vCenter Issues

Description

Sometimes during an online upgrade the vCenter daemon crashes on a node. When this happens, the node cannot enter HX maintenance mode. Without entering HX maintenance mode, the node cannot complete the upgrade. All other nodes, with properly functioning vCenter, complete the upgrade.

Action: Re-run the Upgrade on the Affected Node

1. Correct the vCenter issue.
2. Re-run the upgrade on the affected node.

vCenter Plugin shows Upgrade button after Cluster Upgrade

Description:

After a cluster upgrade to HXDP release 3.5, the vCenter Plugin continues to show the **Upgrade** button.

Action: If you see this issue, perform a vCenter cleanup.

Cluster Reregistration Fails After VCSA Upgrade

Description

After upgrade of VCSA, cluster reregistration to the upgraded vCenter fails due to the controller IP not populating in vCenter. This is a known issue in a docker VM with multiple NICs where the IP does not populate in VC, causing upgrades to HX which immediately follow a VCSA upgrade, to fail because the IP can not be retrieved.

Action: Open a web console session to the controller VM to trigger it.

SUMMARY STEPS

1. There are three suggested steps to workaround this issue.

DETAILED STEPS

There are three suggested steps to workaround this issue.

a) Launch the VMRC/web console to the guest to view a list of all IP addresses.

b) Connect to the host directly to identify/ find all the IP for the Virtual Machine

For more information, see the VMware KB article, Summary page does not show all IP address on VM's after vCenter upgrade.

Option to upgrade UCS does not appear in HX Connect

Description: Option to upgrade UCS does not appear in HX Connect.

Action: Verify that all backend services are up and running:

1. Verify that stNodeMgr is running on ESX clusters.
2. Verify that stMgr is running on ESX clusters.
3. If any of the services are stopped, start them by running start <service-name>, where <service-name> is stNodeMgr or stMgr or stUpgradeSvc.

Connection to HX Connect Lost During Upgrade

Description: Connection to HX Connect lost after pre-upgrade step from HX 3.5(2g) to HX 4.0(2a). During the upgrade, if there is an expired certificate in the upgrade source version, the browser will log user out after pre-upgrade step. This is accepted secure behavior since the certificate of the server has changed after pre-upgrade.

Action: Refresh the browser and login again.

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

Login to 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.[1]
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 Sequence for Fabric Interconnect 6400 Series using VIC 1455/1457 with SFP-H25G-CU3M or SFP-H25G-CU5M Cables

Use the following upgrade sequence ONLY if your cluster is connected to a Fabric Interconnect 6400 connected to VIC 1455/1457 using SFP-H25G-CU3M or SFP-H25G-CU5M cables:

1. Upgrade the UCS server firmware from HX Connect
2. Upgrade the UCS Infrastructure
3. Upgrade HXDP
4. Upgrade ESXi

Combined Upgrades: Supported after the UCS server firmware and UCS infrastructure firmware upgrade is complete

Release Notes for UCS Manager, Firmware/Drivers, and Blade BIOS
CSCvu25233

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