Release Notes for Cisco HX Data Platform, Release 4.5

First Published: 2021-01-06

Last Modified: 2023-08-07

Introduction

Cisco HyperFlex™ Systems unlock the full potential of hyperconvergence. The systems are based on an end-to-end software-defined infrastructure, combining software-defined computing in the form of Cisco Unified Computing System (Cisco UCS) servers, software-defined storage with the powerful Cisco HX Data Platform, and software-defined networking with the Cisco UCS fabric that integrates smoothly with Cisco Application Centric Infrastructure (Cisco ACI). Together with a single point of connectivity and hardware management, these technologies deliver a pre-integrated and adaptable cluster that is ready to provide a unified pool of resources to power applications as your business needs dictate.

These release notes pertain to the Cisco HX Data Platform, Release 4.5, and describe the features, limitations and caveats for the Cisco HX Data Platform.

Recent Revisions

For the complete revision history, see Revision History, on page 36.

Release	Date	Description
4.5(2e)	September 6, 2022	Updated the 4.5 Release notes for Cisco HX Data Platform Software, Release 4.5(2e).
4.5(2d)	July 19, 2022	Updated the 4.5 Release notes for Cisco HX Data Platform Software, Release 4.5(2d).
4.5(2c)	April 19, 2022	Updated the 4.5 Release notes for Cisco HX Data Platform Software, Release 4.5(2c).
4.5(1a)	January 31, 2022	The last date of support for Cisco HX Data Platform Software Version 4.5(1x).
4.5(2b)	December 9, 2021	Created release notes for Cisco HX Data Platform Software, Release 4.5(2b).

New Features

New Features in Release 4.5(2e)

There are no new features in this release.

New Features in Release 4.5(2d)

There are no new features in this release.

New Features in Release 4.5(2c)

- **Support for ESXi 7.0 U3**—HXDP 4.5(2c) provides support for VMware ESXi 7.0 U3.
- **Intel® Optane™ NVMe Cache support** for DC-no-FI on M5 servers.
- New drives are qualified in HX 4.5(2c). For more information, see New Supported Drives, on page 5.

New Features in Release 4.5(2b)

New drives are qualified in HX 4.5(2b). For more information, see New Supported Drives, on page 5.

New Features in Release 4.5(2a)

The following new features are in HX 4.5(2a):

- **HX Native Snapshots with ESXi 7.0 U2**—introduces the following enhancements:

  Beginning with HXDP version 4.5(2a) with ESXi 7.0U2, HX Sentinel snapshots are no longer created. Prior versions of HXDP will continue to utilize HX Sentinel snapshots. This is applicable to HX native snapshots created with the HX Connect UI, REST API, vSphere HyperFlex HTML client plugin, or stcli commands.

  If there are no user or 3rd party backup snapshots, HX Sentinel snapshot(s), if present, are deleted when snapshots are created through the HX Connect UI, REST API, vSphere HyperFlex HTML client plugin, or stcli commands. This enables the usage of HX Sentinel-free HX native snapshots (VAAI).

  If there are user or 3rd party backup snapshots, HX Sentinel snapshot(s) will ***not*** be deleted. We recommend a 1-time deletion of user and 3rd party backup generated snapshots to take advantage of the following improvements:

  - Reduced stun times due to the delta disk being eliminated from all HX native Snapshot workflows.
  - Improved quiescing support – vCenter will report quiesced snapshots as quiesced.
  - Support for large VMDKs, and greater than 3TB VMDK disks.
  - Support for VMs spanning HX datastores.
  - VM snapshot consolidation is now a meta-data only operation and does not involve data movement. VM consolidation times are no longer proportional to VM I/O workloads.

Note Cisco strongly recommends to utilize the HX Connect UI, REST API, vSphere HyperFlex HTML client plugin, or stcli commands to create snapshots and schedules. Using the vCenter Snapshot Manager bypasses these operations which are designed to minimize the cases where a user has to perform manual workarounds. Manual workarounds, such as adding the VM attributes *snapshot.alwaysAllowNative* or *snapshot.ayncConsolidate* flags, are neither recommended nor required.

For more information, see Managing HX Native Snapshots in the Cisco HyperFlex Data Platform Administration Guide, Release 4.5.

- **1:1 Replication with 2-Node HX Edge cluster**—Support added for 1:1 replication with 2-Node HX Edge cluster. Supported configurations for native replication (NRDR 1:1) are 2N/3N/4N Edge and FI-based clusters to 2N/3N/4N Edge and FI-based clusters, including stretched clusters, all managed through HX Connect.
- **Single Socket for Stretched Cluster configurations**—allows users to optimize the hardware configuration cost and licensing cost for certain applications for a stretched cluster configuration. This support was introduced in HXDP 4.5(2a).

New Features in Release 4.5(1a)

The following new features are in Release 4.5(1a).

- **iSCSI Support**—HX 4.5(1a) introduces native iSCSI protocol support for workloads that require block storage (such as, databases) or shared disk access (such as, failover clusters). HX 4.5(1a) supports these software initiators: Windows Server 2016 and 2019, RedHat Enterprise Linux 7, Oracle Linux 8, Ubuntu 18.04 and 20.04. HX 4.5(1a) supports a rich set of iSCSI features, including: centralized login portal, direct logins, out-of-box Windows (DSM) and Linux (dm-multipath) drivers (active-active and active-passive), app-consistent and crash-consistent LUN clones, and target-side CHAP authentication.
- **Cisco HyperFlex HTML5 Plugin for VMware vCenter**—Provides users the ability to manage and monitor your HyperFlex clusters from the VMware vCenter Web UI. Additional functionally in version 2.1.0 includes:
  - Snapshot Scheduler
  - iSCSI Management
  - Nodes and Disk View
  - Virtual Machines Summary
  - Events and Tasks
  - VLAN Creation
  - Rename Cluster
  - HyperFlex Stretched Clusters
  - Support for VMware vCenter Linked Mode

Note HXDP Release 4.5(1a) is the final release that supports the Cisco HyperFlex Flash Plugin. This change coincides with the end of flash support in popular browsers. It is recommended that users upgrade to the Cisco HyperFlex HTML5 Plugin 2.1.0

- **HyperFlex Edge 240 Full Depth Servers**—New, full depth server offerings are now available for HyperFlex Edge. Both All-flash (HXAF-E-240-M5SX) and Hybrid (HX-E-240M5SX) configuration options are available. For more details, see the HyperFlex HX240 M5 Edge Hybrid and All Flash spec sheet.

- **HX CSI Support**—Cisco HyperFlex Container Storage Interface (CSI) adds support for the following features in HX 4.5(1a): Block access, Clone volume (when source volume is from the same Datastore), PV support with different file systems (Ext4, Ext3, XFS), Volume space statistics reporting per CSI specs, Multi-writer support (ReadWriteMany) for Block Mode only, Kubernetes 1.18 support, Kubernetes Cluster multi-tenancy target/lun masking using dedicated initiator group, Support for CSI 1.2 Spec APIs, Volume resize support for block mode volumes and ext3, ext4 filesystem volumes (expansion), CSI Plug-in installation and upgrade through Helm chart.

Note When using HX CSI, if you don't need to preserve the persistent volume claim, see Cisco HyperFlex Systems Administration Guide for Kubernetes. If the persistent volume claim needs to be preserved then contact TAC.

- **RAID Support for Boot Drives**—Support for Hardware RAID M.2 boot drives in HyperFlex converged and compute-only nodes. Requires optional HX-M2-HWRAID controller with two boot drives. Existing single boot drive option remains supported.
- **UEFI Secure Boot Mode**—HX 4.5(1a) simplifies the hardening of hypervisor (ESXi) boot security by providing an automated workflow that non-disruptively changes the boot mode of converged and compute nodes in the cluster to Unified Extensible Firmware Interface (UEFI) Secure Boot, in which the chain of trust is anchored by a hardware trust anchor (for example the Cisco Trust Anchor module) built-in to UCS rack and blade servers. HX 4.5(1a) also allows UI and API-based queries of each node's secure boot status so customers can audit the cluster's security posture on-demand.

Note UEFI secure boot should only be enabled on HX Edge clusters running Cisco IMC version 4.1(2a) and later. If secure boot is enabled on earlier Cisco IMC versions, secure boot will need to be temporarily disabled during firmware updates.

- **vCenter Re-Registration**—is a user-interface based feature that you can use to move to a new vCenter. You may need to re-register vCenter in the following scenarios: the Controller VM certificate is changed; it is recommended to re-register vCenter extensions whenever a vCenter upgrade is performed; re-registration is required when the extensions are manually removed due to misconfigurations.
- **HyperCheck 4.5**— The HyperCheck script is now included with the product and Rest APIs integration has improved performance. Run the **hypercheck** command to start the checks. You can perform HyperCheck at any time. It is recommended that you perform HyperCheck prior to upgrades. New features and checks include: Cluster Information table, DR (local and remote network) and SED checks for users who have them enabled. To update health check, use the framework provided in Intersight.
- **Scheduled Snapshots on HxConnect**—Provides users the ability to manage and monitor Snapshot and Schedule Snapshot from the HxConnect Web UI. New Functionally includes:
  - Improved VM Summary - Added counts for total count for VMs with Snapshots and VMs with Snapshot schedules.
  - VM Details - Introduce action buttons to Create HX Snapshot Now and Schedule Snapshot
- **Compute node automated boot policy selection**—Compute-only nodes are now easier to deploy with automatic detection and configuration of disk and boot policies based on the boot hardware discovered.

- **Replication Factor 3 support for HX Edge**—New HyperFlex Edge deployments can be configured with Replication Factor (RF)3 for higher resiliency and availability. RF3 is the default setting for 3 & 4 node Edge clusters and follows Cisco's best practices for production clusters.
- **Compatibility Catalog**—This new capability simplifies the introduction of new drives by allowing customers to perform an HX drive catalog-only upgrade to start consuming new drives and models introduced in the future, without requiring a HyperFlex Data Platform upgrade. Please note that you may need to update a separate UCS drive catalog update as well.
- **Secure Admin Shell**—HX 4.5(1a) introduces a new command-line shell, the Admin Shell, which restricts commands executable by an authenticated “admin” user login to a set of allow-listed administrative commands. Command-line login to the Controller VM as the “root” user is also removed. The Admin Shell improves the built-in security posture of the Controller VM by reducing its attack surface. An advance shell for troubleshooting can be requested from within the Admin Shell, which requires a Cisco Consent Token from Cisco TAC, and should only be used with guidance by Cisco TAC.
- **HX Hardware Acceleration Card Support with Native Replication**—HX 4.5.(1a) enables support for HX Hardware Acceleration cards (PID: HX-PCIE-OFFLOAD-1) with Native Replication pairing between a source and target cluster to provide DR capabilities. Both the source and the target HyperFlex clusters must have HX Hardware Acceleration enabled and should be on the HX 4.5.(1a) release.

Intersight-Powered Features

- **N:1 Replication for HyperFlex Edge Clusters**—Provides the ability for HyperFlex Edge clusters to take snapshots of Virtual Machines and restore using Intersight. Users can configure multiple HyperFlex Edge clusters at different sites with backup policies to create snapshots of virtual machine data which is replicated to a centralized HyperFlex backup target cluster. The VM snapshots are retained locally on the Edge cluster and a backup target cluster. These VMs snapshots are critical tools in the event that you need to recover from logical corruption, accidental deletion of data, a cluster or site outage, or planned VM migration from one edge cluster to another. For more information, see N:1 Replication for Cisco HyperFlex Edge Clusters.
- **External Witness**—Introducing new external witness support for HyperFlex Edge 2-Node Clusters. This feature increases cluster availability and flexibility for remote sites. For more information, see Configuring Device Connector.
- For more information on Intersight-Powered features, see Cisco Intersight What's New.

New Supported Drives

New drives are qualified for HX 4.5(x). For expansion of existing clusters or general information about interoperability of different drives, see Cisco HyperFlex Drive Compatibility.

Table 1: Supported Drives

Drive Function	Drive PID	Applicable Platforms	Version
960GB SATA SSD	HX-SD960G6S1X-EV	All Flash M5 220 and 240, All Flash M5 Edge 220, 240 and HXAF240C-M5SD	HXDP 4.5(2c)
1.9TB SATA SSD	HX-SD19T6S1X-EV	All Flash M5 220 and 240, All Flash M5 Edge 220, 240 and HXAF240C-M5SD	HXDP 4.5(2c)

Drive Function	Drive PID	Applicable Platforms	Version
3.8TB SATA SSD	HX-SD38T6S1X-EV	All Flash M5 220 and 240, All Flash M5 Edge 220, 240 and HXAF240C-M5SD	HXDP 4.5(2c)
7.6TB SATA SSD	HX-SD76T6S1X-EV	All Flash M5 220 and 240, All Flash M5 Edge 220, 240 and HXAF240C-M5SD	HXDP 4.5(2c)
800G FIPS Compliant SED Cache drive	HX-SD800GBKNK9	All Flash M5 220 and All Flash M5 240	HXDP 4.5(2b)
1.6TB FIPS Compliant SED Cache drive	HX-SD16TBKNK9	All Flash M5 220 and All Flash M5 240	HXDP 4.5(2b)
960G FIPS compliant SED SSD	HX-SD960GBKNK9	All Flash M5 220 and All Flash M5 240	HXDP 4.5(2b)
3.8TB FIPS compliant SED SSD	HX-SD38TBKNK9	All Flash M5 220 and All Flash M5 240	HXDP 4.5(2b)
2.4TB SAS SED HDD	HX-HD24T10NK9	Hybrid 220 and 240	HXDP 4.5(1a)
7.6TB SSD	HX-SD76T61X-EV	AF 220 and 240	Adding support for Hyper-V in HXDP 4.5(1a).

Cisco HyperFlex CSI Versions

New versions of the Cisco HyperFlex Container Storage Interface (CSI) are qualified for HX 4.5(2b).

Table 2: Cisco HX CSI Versions

HX CSI Version	File Name	Notes
hxcsi-1.2.1b-615	`hxcsi-1.2.1b-615.tar.gz`	IKS Tenant Cluster shipped with `hxcsi-1.2.1b-615` (this version to be used on ESXi setup).

Supported Versions and System Requirements for Cisco HXDP Release 4.5(x)

Cisco HX Data Platform requires specific software and hardware versions, and networking settings for successful installation.

For a complete list of requirements, see:

- Cisco HyperFlex Systems Installation Guide for VMware ESXi, or
- Cisco HyperFlex Systems Installation Guide for Microsoft Hyper-V

Requirement	Link to Details
For a complete list of hardware and software inter-dependencies,	Hardware and Software Interoperability for Cisco HyperFlex HX-Series
Details on cluster limits and Cisco HX Data Platform Compatibility and Scalability Details	Cisco HX Data Platform Compatibility and Scalability Details - 4.5(x) Releases
Verify that each component, on each server used with and within an HX Storage Cluster is compatible.	FI/Server Firmware - 4.5(x) Releases
Confirm the component firmware on the server meets the minimum versions supported.	HyperFlex Edge and Firmware Compatibility Matrix for 4.5(x) Deployments
HX Data Platform Software Versions for HyperFlex Witness Node for Stretched Cluster	HX Data Platform Software Versions for HyperFlex Witness Node for Stretched Cluster - 4.5(x) Releases
Verify that you are using compatible versions of Cisco HyperFlex Systems (HX) components and VMware vSphere, VMware vCenter, and VMware ESXi.	Software Requirements for VMware ESXi - 4.5(x) Releases
To verify that you are using compatible versions of Cisco HyperFlex Systems (HX) components and Microsoft Hyper-V (Hyper-V) components.	Software Requirements for Microsoft Hyper-V - 4.5(x) Releases
To verify that you are using compatible versions of Microsoft Software.	Supported Microsoft Software
List of recommended browsers.	Browser Recommendations

Guidelines and Limitations

Upgrade Guidelines

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

Prerequisites for Upgrading HyperFlex Software

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

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

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

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

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

- HXDP Release 4.5 supports ESXi version 6.5 U3 and later only. If your current ESXi version is earlier than 6.5 U3, make sure to perform a combined upgrade of HXDP and ESXi to a target level 6.5 U3 or later.
- Review the Cisco HyperFlex Upgrade Guidelines in the Recommended Cisco HyperFlex HX Data Platform Software Releases - for Cisco HyperFlex HX-Series Systems.
- vCenter version check: Verify that the vCenter is version 6.5 U3 or later and meets the minimum requirements for the ESXi version being upgraded to. See, VMware Product Interoperability Matrices to ensure compatibility between vCenter and ESXi.
- Ensure all VM network port groups exist on all nodes in the cluster for vMotion compatibility.
- Ensure that the management and storage data VLANs are configured on the top-of-rack network switches to ensure uninterrupted connectivity during planned fabric failover.
- If using jumbo frames in your environment, ensure jumbo frames are enabled on the vMotion and data networks on the top of rack switch.
- Verify that the ESXi hosts are not in lockdown mode for the duration of the upgrade. Lockdown mode can be re-enabled after the upgrade is complete.
- Upgrading the VM compatibility version or hardware version of the Storage Controller Virtual Machine (SCVM) is not supported and should not be performed. This action is detrimental to the SCVM and will require a rebuild of the SCVM if performed.
- If you are using HX CSI then contact TAC.

Security Fixes

The following security issues are resolved:

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvz22127	Multiple third-party vulnerabilities - QlyAug2021.	4.5(1a)	4.5(2b) 5.0(1a)
CSCvx17208	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ct ...	3.5(2h) 4.0(2d)	4.5(2b) 5.0(1a)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvy53153	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2020-26160 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26160 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	4.5(1a) 5.0(1a)	4.5(2b) 5.0(1a)
CSCvy19321	A vulnerability in the command line interface (CLI) of HyperFlex System could allow an authenticated, local attacker to bypass the Consent Token authentication. The vulnerability is due to improper enforcement of the Secure Shell restrictions for specific users. An attacker could exploit this vulnerability by sending a crafted command to the affected system. An exploit could allow the attacker to execute arbitrary commands with root privileges on the HyperFlex Storage Controller VM (SCVM). An attacker needs valid privileged user credentials to exploit this vulnerability	4.5(1a)	4.5(2b) 5.0(1a)
CSCvy19261	A vulnerability in the command line interface (CLI) of HyperFlex System could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to improper enforcement of the Secure Shell restrictions for specific users. An attacker could exploit this vulnerability by sending a crafted command to the affected system after having connected to it via a Secure Shell connection. An exploit could allow the attacker to execute arbitrary commands on the HyperFlex Storage Controller VM (SCVM). These commands will be executed with the same privileges as the user account used to connect to the affected system. An attacker needs valid privileged user credentials to exploit this vulnerability.	4.5(1a)	4.5(2b) 5.0(1a)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvx52126	A vulnerability in the web-based management interface of Cisco HyperFlex HX Data Platform could allow an unauthenticated, remote attacker to upload files to an affected device. This vulnerability is due to missing authentication for the upload function. An attacker could exploit this vulnerability by sending a specific HTTP request to an affected device. A successful exploit could allow the attacker to upload files to the affected device with the permissions of the tomcat8 user. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link.	4.5(1a) 4.0(2a) 4.0(1a) 3.5(1a)	4.5(2a) 4.0(2e)
CSCvx37435	A vulnerability in the web-based management interface of Cisco HyperFlex HX Data Platform could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the tomcat8 user. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link.	4.5(1a) 4.0(2a) 4.0(1a) 3.5(1a)	5.0(1a) 4.5(2a) 4.0(2e)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvx36028	A vulnerability in the web-based management interface of Cisco HyperFlex HX Data Platform could allow an unauthenticated, remote attacker to upload files to an affected device. This vulnerability is due to missing authentication for the upload function. An attacker could exploit this vulnerability by sending a specific HTTP request to an affected device. A successful exploit could allow the attacker to upload files to the affected device with the permissions of the tomcat8 user. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link.	4.5(1a) 4.0(2a) 4.0(1a) 3.5(1a)	4.5(2a) 4.0(2e)
CSCvx36019	A vulnerability in the web-based management interface of Cisco HyperFlex HX Installer Virtual Machine could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the root user. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:	4.5(1a) 4.0(2a) 4.0(1a) 3.5(1a)	5.0(1a) 4.5(2a) 4.0(2e)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvx36014	A vulnerability in the web-based management interface of Cisco HyperFlex HX Installer Virtual Machine could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device as the root user. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:	4.5(1a) 4.0(2a) 4.0(1a) 3.5(1a)	5.0(1a) 4.5(2a) 4.0(2e)
CSCvv75781	Multiple vulnerabilities from multiple TPS components - NESEP2020 This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	4.0(2c)	4.5(2a) 4.0(2e)
CSCvv46591	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link.	4.0(2c)	4.5(1a)
CSCvv46556	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. This bug was opened to address the potential impact on this product.	4.0(2c)	4.5(1a)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvu33080	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. This bug was opened to address the potential impact on this product.	3.5(2a)	4.5(1a) 4.0(2c)
CSCvp36364	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. This bug was opened to address the potential impact on this product.	4.0(1a)	4.5(1a)
HyperFlex CSI			
CSCvw88821	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2020-29361 CVE-2020-29362 CVE-2020-29363 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68880	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2019-10329 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvw68879	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2018-16869 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68878	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2018-7169 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68877	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2019-18276 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68868	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2018-1000654 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)

Defect ID	Description	Known Affected Releases	Open or Known Fixed Releases
HXDP			
CSCvw68867	This product includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2020-10543 CVE-2020-10878 CVE-2020-12723 The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68866	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68813	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)
CSCvw68809	This product includes Third-party Software that is affected by the vulnerabilities identified by Common Vulnerability and Exposures (CVE) IDs. To review the full list of affected CVEs, click the Defect ID link. The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.	1.2(569)	1.2(1a)

Caveats in Release 4.5(x)

The following table lists non-security HXDP, Hyper-V and HXCSI caveats for the Cisco HyperFlex Release 4.5(x). Caveats are listed in decending order to keep the newest additions at the top. Each caveat number is

linked to the Cisco Bug Search Tool. Use the link to access additional details about the symptom, conditions and workarounds that apply.

HXDP Caveats

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCwd61729	Improve handling of stuck APSwitch request/response	4.0(2c) 5.0(1a) 5.0(2a)	5.0(2b)
CSCwd38819	Stretched Cluster - Improper indexing into the cache vnode list history map leading to PANIC CONDITION	4.5(2e)	5.0(2b)
CSCwd10169	SAMSUNG MZ7L37T6HBLA-00AK1 model disks ignored in supported HXDP version	4.5(2e)	5.0(2b)
CSCwc88571	HyperFlex ENH: HyperFlex Connect should have cluster name in HTML title	4.5(2b) 5.0(2a)	Open
CSCwc76298	When storage n/w has MTU 1500, iSCSI n/w config should prevent enabling jumbo frames	4.5(1a)	Open
CSCwc68011	Cleaner may stop after upgrade to 4.5(2c) or 4.5(2d) if upgrade is performed using HxConnect.	4.5(2c) 4.5(2d)	4.5(2e) 5.0(2a)
CSCwc43343	HX Connect not displaying System Information and some Dashboard values	4.5(2c)	See defect ID for details.
CSCwc26162	storfs PANIC due to fatal flusher error	4.5(2b) 4.5(2c)	5.0(2b)
CSCwc05932	Upgrade to 7.0 u2 failed due to AHCI driver disabled	4.5(2b)	Open
CSCwc03496	iSCSI Reservation Conflict due to non-zero active_write_count.	4.5(2a)	4.5(2d) 5.0(2a)
CSCwb92071	Expansion of clusters upgraded to 5.01b may result in a storfs process crash	3.5(2i)	5.0(2a)
CSCwb74053	During deployment Installer throws ambiguous error message when housekeeping disk is bad.	4.5(2b)	5.0(2a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCwb62377	HyperFlex post install script should have clear messages when hostnames can't be resolved	4.5(2b)	5.0(2a)
CSCwb59556	HX Installer 4.5.2b disorders IPs and Hostnames if select all checkbox is used	4.5(2b) 4.5(2c)	See defect ID for details.
CSCwb57788	Bootstrap to 4.5(2b) fails with vague error message due to service syslog-ng being stopped.	4.5(2b)	5.0(2a)
CSCwb47745	Incorrect Interrupt Count in HyperFlex Ethernet Adapter Policy.	4.0(2e) 4.5(1a) 4.5(2a)	4.5(2d) 5.0(2a)
CSCwb47054	HyperFlex local installer does not handle special characters in passwords properly.	4.5(2b)	5.0(2a)
CSCwb28122	RAID Storage controller changed to passthrough in compute nodes after HXDP upgrade to 5.0(1b)	4.5(2b) 5.0(1b)	5.0(2a)
CSCwb25993	Upgrade failing in pre-upgrade-hooks for 3-node edge cluster for classic upgrade	4.5(2b)	5.0(2a)
CSCwb14314	HX SCVM /dev/sda1 partition having 100% usage due to hproof file	4.5(2a)	5.0(2a)
CSCwb06370	Inadvertently passed parameters cause storfs to PANIC.	4.5(1a) 4.5(2b)	4.5(2d) 5.0(2a)
CSCwb01433	Upgrade from 4.5.2b CCO to 5.0.1b CCO failed - Migrating Controller VM to New Template	4.5(2b) 5.0(1a) 5.0(1b)	See defect ID for details.
CSCwa95540	Upgrade to 4.5(2b) storfs-hsu fails to deploy debain package.	4.5(2b)	4.5(2d) 5.0(2a)
CSCwa92213	Improve / Correct Error Message: failed in Task: Configuring Network (Port Groups) for ESXi and Storage Controller VM with Error: `Configure networking failed with error: Error while connecting to ESXi host. Please check the connection and retry.`	4.5(2a) 4.5(2b)	Open

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCwa90056	HX datastore shows unmounted after HXDP upgrade from 4.0(2d) to 4.5(2a)	4.5(2a)	5.0(2a)
CSCwa88530	2N ROBO: Maintenance mode did not complete successfully (auxzk failed to start due to bad epoch)	4.5(2b)	4.5(2c) 5.0(2a)
CSCwa81186	HX Install Fails During Deploy Phase (Another task is already in progress)	4.5(2a)	4.5(2c) 5.0(2a)
CSCwa74124	HyperFlex catalogs are not present on CCO to download	4.5(2a) 4.5(2b) 5.0(1a)	5.0(2a)
CSCwa65843	HyperFlex Installer displays incorrect server order for Hypervisor Settings	4.5(2b)	5.0(2a)
CSCwa60352	Non-supported HyperFlex Edge expansion is allowed via HyperFlex OVA Installer custom workflow	4.0(2d) 4.5(2b) 5.0(1a)	5.0(2a)
CSCwa58180	HyperFlex installer error message needs more clarity	4.5(2b)	5.0(2a)
CSCwa57487See also CSCwa43861	When additional vnics/vmnics are configured on an HX cluster to carry external non-HX iscsi or nfs traffic and assigned to a vswitch with a customized vswitch name, then node expansion may fail during deploy phase.	4.5(2a)	4.5(2c) 5.0(2a)
CSCwa58805	Unable to configure Stretched Cluster for UCS FW Upgrade on 4.5 and later	4.5(2a)	Open
CSCwa53907	Upgrading from HX release 4.0(2f) to 4.5(2a) got stuck installing the VIB in the EXSI host.	4.5(2a)	See defect ID for details.
CSCwa37062	eth1:0 and eth0:mgmt interfaces are no longer present. Unable to start the cip-monitor service manually with the following error: # service cip-monitor start start: Job failed to start	3.5(2h) 4.5(2a)	5.0(2a)
CSCwa27812	A replaced disks show up in UI even when removed completely and replaced.	4.5(2a)	5.0(2a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCwa23681	User VM ethernet traffic is not going through with default vSwitch setting.	4.5(2a)	Open
CSCwa10699	Storage Controller VM is failing to power on after an upgrade of the server firmware	4.0(2a) 4.5(1a)	Open
CSCwa10525	Enable Packet Loss monitoring by default on HyperFlex Storage Controller	4.5(2a)	Open
CSCwa08806	VM Tool version 11.3.5 support for Quiesce Snapshot	4.5(2a)	5.0(2b)
CSCwa07450	Removed some compute nodes from a cluster still the \"stcli cluster info\" is showing \"size=old value\".	4.5(2a)	4.5(2c)
CSCwa05540	NFSAccess Firewall Rules lost after HX 4.5(2a) Upgrade. This may impact users of Veeam Backup and Replication where backup proxies are configured to use the Direct Storage Access transport mode	4.5(2a)	See defect ID for details.
CSCvz97198	Disk blocklisted and removed but still in ZK db and causing state 3.	4.0(2e)	See defect ID for details.
CSCvz94288	UCS upgrade from HX connect failing	4.5(2a)	4.5(2b) 5.0(1b)
CSCvz87215	[M6]:SCVM redeploy-Deploy only workflow fails in deploy stage.	4.5(2c)	5.0(1a) 5.0(1c)
CSCvz84442	Unable to remove 'exclude local-disk' from Host Firmware Package during HyperFlex upgrade.	4.5(2a)	5.0(1a) 5.0(1b) 5.0(1c)
CSCvz83828	HyperFlex Upgrade validation fails at 'Checking vCenter configuration' stage with error "Message: Failed to get the host config details of Datacenter.	4.5(2a)	5.0(1c)
CSCvz68328	HyperFlex post_install does not properly test upstream MTU.	4.0(2c)	4.0(2f) 5.0(1b) 5.0(1c)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvz62013	Perform Upgrade of HX cluster, however move your ESXi hosts out of the datacenter where they are currently residing. Execute the pre-upgrade eligibility checks and observe error message encounter.	4.0(2e)	4.5(2c) 5.0(1a)
CSCvz37947	While attempting to expand a cluster you receive the error in the installer "HX Catalog upgrade required".	4.5(2a)	5.0(1a)
CSCvz20569	HyperFlex EOS drives not compatible with direct replacement drives during installation.	4.5(1a)	4.5(2b) 5.0(1a)
CSCvz03926 CSCvu66192	HyperFlex Cluster does not have a node which has ownership of the Cluster Management or Cluster Data IP Addresses.	3.5(2h) 4.0(2e) 5.0(1b)	Open
CSCvy91050	If Eth0, Eth1, or Eth2, and iSCSI are assigned to the same VLAN, the random SCVM reboot occurs bringing down the cluster.	4.5(1a)	4.5(2b) 5.0(1a)
CSCvy89315	HX upgrade to 4.5(2a) errors out when uploading storfs-packages-4.5.2a.39429.tgz. Remote copy failed.	4.5(2a)	See defect ID for details.
CSCvy84658	ESXi 7.0 U2 and U3 Upgrade Fails on Servers with Older CPUs	See defect ID for details.	Open
CSCvy67439	admin user cannot complete a "stcli license reservation install" command. It will fail with the following message; admin:~$ stcli license reservation install '..... ' *** forbidden syntax -> "stcli license reservation install ' ..... '" *** You have 3 warning(s) left, before getting kicked out. This incident has been reported.	4.5(1a)	5.0(1a) 4.5(2c)
CSCvy62844	Converged Node Expansion failed when root and admin have different password.	4.5(2a) 4.5(2b) 5.0(1b)	Open
CSCvy52540	Running the **sendasup -t** command to test the email alerting hangs.	4.5(1a)	4.5(2b) 5.0(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvy42299	In HyperFlex HTML5 plugin, DNS Server(s) in **Summary** > **Network Details** > **Network Services** is empty.	4.0(2a)	5.0(1a)
CSCvy39279	Remove Assumption On CIMC Access Type.	4.5(1a)	5.0(1a)
CSCvy36458	In vCenter under plugins, HX Flash plugin status show as Incompatible.	4.5(1a)	4.5(2b) 5.0(1a)
CSCvy32736	In large drive configurations (e.g.. 3.8, 7.6 T etc) sometimes user vm experiences downtime (e.g. APD) or extremely high latency.	4.0(2d) 4.0(2e)	4.5(2b) 5.0(1a)
CSCvy11074	hxtoolbox account generation (hxuser) fails due to missing fields in nodeIPSettings	4.0(2e)	5.0(1a)
CSCvy07554	Drives are showing in an 'Ignored' state as seen from HyperFlex Connect pages.	4.5(1a) 4.0(2e) 4.0(2d)	Open
CSCvx81122	ASUP generate support bundle including esx-asup-default causes full /var/stv when vmware.log of esx host are of bigger size.	4.0(2c)	4.5(2a) 5.0(1a)
CSCvx78025	HXDP Controller VM on a host will be powered off only when all the VMs on that Host are either migrated off to another Host in cluster, or Powered off. So, if we have a configuration with few VMs which are EAM managed, VMs will not migrate out of the host we want to put in maintenance mode. This in turn leads to failure in entering a host into maintenance mode.	4.0(2e)	4.5(2a) 5.0(1a)
CSCvx67455	Cluster not online after a power-cycle of all nodes in a cluster and SED drives remain in locked state.	4.0(2e)	4.5(2a) 5.0(1a)
CSCvx52703	As of today, the Controller VM will be powered off only when all the VMs on that Host are either migrated off to another Host in cluster, or in Power off state. However, there are few VMs which are EAM managed, so they do not migrate, and Customer can't power them down due to security requirements.	4.0(2e)	4.0(2e) 4.5(2a) 5.0(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvx44542	Replication recovery configuration using the HX Connect user interface did not appear to allow the user to display network, vm folders, or resource groups nested within the root folder. The down arrow icon that appears to the left of the root folder was not displayed, but instead appeared as a dot.	4.0(2d)	4.5(2a) 5.0(1a)
CSCvx39042	iSCSI initiator may not be able to mount the iSCSI target due to upper/mixed case letters in the IQNs.	4.5(1a)	5.0(1a)
CSCvx37435	A vulnerability in the web-based management interface of Cisco HyperFlex HX Data Platform could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device.	3.5(1a) 4.0(1a) 4.0(2a) 4.5(1a)	4.0(2e) 4.5(2a) 5.0(1a)
CSCvx34833	After an upgrade to HX 4.0(2d) release, sometimes list of disks (drives) may not show up in HX Connect UI.	4.0(2d)	See defect ID for details.
CSCvx26687	Need to introduce timeout for Enter Maintenance Mode (MM) task to avoid parallel task check error.	4.0(2d) 4.0(2e)	5.0(1a)
CSCvx17718	HyperFlex cluster expansion will fail validation step of "vCenter and ESXi uniform version check", Cluster 'XXXX' not found in datacenter. Please create the cluster on the targeted datacenter in vCenter Installer expects HX cluster object to be in root of datacenter.	4.0(2d)	4.0(2e) 4.5(2a) 5.0(1a)
CSCvx15151	Unable to view support bundles on HX Connect when logging into HX Connect with DNS Short Name. All other HX Connect pages function properly. Support bundles are also visible when logging into HX Connect with FQDN or Cluster Management IP address.	4.0(2b)	See defect ID for details.

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvx09397	Following a full cluster power outage, in rare situations the cluster may not recover on its own.	4.0(2a)	4.0(2e) 4.5(2a) 5.0(1a)
CSCvx02895	The deployment failed with error " failed in Task: 'Verify Configure Server Profile Association.' with Error: 'Unknown error occurred'	4.5(1a)	4.5(2a) 5.0(1a)
CSCvx01406	In stretch clusters, we might see APDs after upgrading from HX release 3.5(2c) and earlier releases or from HX release 4.0(1a). Other upgrades should not have this problem.	4.0(2d)	4.0(2e) 4.5(2a) 5.0(1a)
CSCvx01200 CSCwa10699	Storage Controller VM is failing to power on after an upgrade of the server firmware.	4.0(2a) 4.5(1a)	4.5(2a) 5.0(1a)
CSCvw99328	LUN Creation Task fails with datastore not found.	4.5(1a)	See defect ID for details.
CSCvw99280	Initial iSCSI IP assignment configuration failed due to overlapping IP.	4.5(1a)	4.5(2a) 5.0(1a)
CSCvw89325	During the retry of deploy step, successfully deployed nodes from the previous runs are failing.	4.5(1a)	See defect ID for details.
CSCvw84976	When DR Replication is configured on the cluster, replication network tests (inter and intra cluster) fails due to missing replIpSettings in the nodes inventory. Datastores cannot be mapped from the UI.	4.0(2c)	4.0(2e) 4.5(2a) 5.0(1a)
CSCvw80237	When a reservation of type 7 (write exclusive all registrants) or 8 (exclusive access all registrants) is issued, not all registrants show up as reservation holder.	4.5(1a)	4.5(2a) 5.0(1a)
CSCvw76885	New iSCSI network configuration is displayed in the UI, but old configuration is retained on the nodes in the cluster	4.5(1a)	4.5(2a) 5.0(1a)
CSCvw64458	VM network performance degraded and/or Poor HyperFlex storage performance Significant and incrementing rx_no_buf errors seen on HyperFlex Storage Data VNIC's which correlate to the above.	3.5(2a)	4.5(2a) 5.0(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvw58166	Full upgrade phase failed "Node Management policy not found".	4.0(2a) 4.0(2d)	4.0(2e) 4.5(1a) 5.0(1a)
CSCvw55448	Changing maximum bandwidth for replication seems to have no effect.	4.0(2b)	See defect ID for details.
CSCvw53657	vSphere may report all paths down (APD) event under following condition A reboot of an ESX that was previously put into maintenance mode, either due to scheduled maintenance of any of HyperFlex upgrade workflow. Since the host has been into maintenance mode there will not be any virtual machines running. This APD event reported by the ESX in maintenance mode, will not impact any user application.	4.5(1a)	See defect ID for details.
CSCvw51654	The HyperFlex System does not include ssl-ciphers for port 8997 similar to nginx port 443. So port 8997 responding to DR Replication Network and triggering security issues with DES.	4.0(2c)	4.0(2e) 4.5(1a) 5.0(1a)
CSCvw49752	During Fresh install in deploy phase, user gets error "Cannot complete operation because VMware Tools is not running in this virtual machine." This Error is displayed in step "Configuring storage controller Node". Error occurs when it goes to power off controller vm after virtual machine configuration.	4.5(1a) 4.0(2d) 4.0(2c)	4.0(2d) 4.0(2e) 4.5(2a) 5.0(1a)
CSCvw49055	HX Connect displays an NTP alert for a controller and then clears after an hour. Following messages and events are also seen in HX Connect. "One or more ntp servers not reachable from node SpringpathController..... " "All configured NTP servers reachable from node"	4.0(2d) 4.0(2c) 4.0(2b) 4.0(2a)	4.5(2a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvw42012	Upgrade failing with error Node upgrade failed: Failed ansible task = 'Setting the Target Node ID'. Failure reason = 'the field 'args' has an invalid value, which appears to include a variable that is undefined. The error was: No first item, sequence was empty.nn. The error appears to have been in '/opt/springpath/storfs-upgrade-bootstrap/playbooks/bootstrap-node.yml line 103, column 8, but maybe elsewhere in the file depending on the exact syntax problem.nn. The offending line appears to be:nnn - name: Setting the Target Node IDn ^ heren'.	4.0(1b)	See defect ID for details.
CSCvw41926	Low Free Memory or OOM due to storfs memory fragmentation.	4.0(2e) 4.5(1a) 4.5(1b) 4.5(2a)	4.5(2b) 5.0(1a)
CSCvw39210	4.0(2c) cluster install may fail in the "Create Cluster Validation" step with the error message: "ERROR c.s.s.c.http.HttpDownStreamService - Unable to post the content to the down stream, url: /coreapi/v1/hypervisor/platformSeed Error Response: java.lang.Exception: Bad Request". This may result in the Control VM hostnames being configured as 'none'.	4.5(1a) 4.0(2c)	4.5(2a) 5.0(1a)
CSCvw39100	Replication (and possibly local storage traffic) are negatively impacted by lack of TCP SACK.	4.5(1a)	4.0(2e) 4.5(1a)
CSCvw23077	If a bad disk is present then during upgrade if it fully goes bad, then upgrade gets stuck.	3.5(2b) 3.5(2h) 4.0(2c) 4.5(1a)	4.0(2e) 4.5(1a) 5.0(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvw01432	HyperFlex Controller VMs Are Deleted After Being Added to vCenter 7.0 U1 HyperFlex Controller VMs may suddenly power off and be deleted from disk by the EAM service running in vCenter. This will result in a loss of cluster availability and in some cases could result in un-recoverability of the HyperFlex storage cluster.	4.5(1a) 4.5(2a)	5.0(1a)
CSCvv81146	When Expanding a HyperFlex Cluster the newly added node shows less info and some "method: dhcp" on "stcli cluster info" output. When checking manually all IPs are Static and there are no operational impacts.	4.0(2b)	5.0(1a)
CSCvv62359	M3 Nodes does not bootup with ESX 7.X if its present in a cluster when ESX upgrade is performed. M3 Nodes with ESXi 7.X cannot be used in the expansion workflow as well. It doesn't boot up after installation of ESX.	4.5(1a)	4.5(2a) 5.0(1a)
CSCvv59521	You may see the following error message during a HyperFlex install or expand using the local OVA installer: Installing Software Packages on Storage Controller VM failed in Task: 'Initializing Storage Controller VM for Installation' with Error: 'The conditional check '(not packagesinstalled.stat.exists) or (not existingBuildManifest.stat.exists) or (not targetBuildManifest.stat.exists) or (targetBuildManifest.stat.md5 != existingBuildManifest.stat.md5)' failed. The error was: error while evaluating conditional ((not packagesinstalled.stat.exists) or (not existingBuildManifest.stat.exists) or (not targetBuildManifest.stat.exists) or (targetBuildManifest.stat.md5 != existingBuildManifest.stat.md5)): 'dict object' has no attribute 'md5'	4.0(2c)	4.5(1a) 4.0(2e)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvv57352	DR pairing gives error(completes successfully) from 4.0(2a) to 4.5(1a). Datastore mapping fails from 4.0.2a to 4.5(1a).	4.5(1a) 4.0(2c)	4.0(2e)
CSCvv54531	HyperFlex node remove fails should ask user to rebalance, wait for healthy, and then node remove	4.5(1a)	See defect ID for details.
CSCvv27048	Test Upgrade Eligibility in HX Connect and getting Unrecognized field "isClusterUpgradePrecheck" error	4.0(2a)	See defect ID for details.
CSCvv19737	On some HyperFlex Edge clusters, when registering them with Smart Licensing they will consume the "Cisco SP HyperFlex HX Data Platform SW v2.0" license instead of the "HyperFlex Data Platform Edge Edition Subscription"	4.0(2c)	4.5(1a) 4.0(2e)
CSCvu93214	Recover page in Hx Connect shows error, but the recovery of VM operation is successful in the backend and displayed in the Activity tab.	4.0(2c)	4.5(1a) 4.0(2e)
CSCvu85439	HyperFlex Cluster may remain online, but datastores are not available and VM's become inaccessible APDs seen on multiple nodes	3.5(2d)	See defect ID for details.
CSCvu73740	Case generated via Smart Call Home attaches a SCH CLI Output that only contains the cluster_info. ssh command outputs for diagnosing issues weren't part of the payload sent to SCH. It meant insufficient information was being sent to the case.	4.0(2b) 3.5(2h)	4.5(1a) 4.0(2c)
CSCvu58785	Performing an API call for a token refresh fails on HyperFlex clusters encounters a failure response	4.0(2a)	4.5(1a) 4.0(2c)
CSCvu58631	3.5(2h) SED stretch cluster expansion failed as converged node is not listed in server selection page	3.5(2h)	3.5(2i) 4.0(2c) 4.0(2d) 4.5(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvu52699	User can observe following symptoms after replacing HyperFlex server system board. 1) Intersight UI - Node is not listed in HyperFlex cluster detailed inventory view page 2) Change of License tier for HyperFlex cluster will fail and reverts back to old value (example - If changing from Base to Essentials , it will fail and remain at Base) On the intersight UI, user can notice that the hyperflex.Node (server) object has old server serial number and PhysicalServer object has null value UCSM, UCSM inventory in Intersight has updated new server details and issue is only with HX inventory in Intersight. HXDP Zookeeper is not updated with correct (new) Serial Number	3.5(2h)	See defect ID for details.
CSCvu36042	Storfs process on Springpath Controller VM will panic in inconsistent Network condition (such as disconnects, varying bandwidth or latency) when replication is forced to reconnect to the destination cluster.	4.0(2b)	4.5(1a) 4.0(2c)
CSCvu29049	8-node cluster with SED enabled - upgrading from 3.5(2b) to 3.5(2h) - Auto-boostrap failed, so manual bootstrap tried but still it was giving error	4.0(2c) 3.5(2h)	4.5(1a)
CSCvu27654	Sometimes, witness VM fills up the volume containing Zookeeper logs and transactions. This may lead to Zookeeper service misbehaving within the witness VM and could also potentially result in an unresponsive Zookeeper service. Also, filling up the folder will prevent Zookeeper from logging any further.	4.0(2a) 4.0(1a) 3.5(2h)	4.5(1a) 4.0(2c)
CSCvu17828	Notice APD events and Cluster may go down.	4.5(1a) 3.5(2g)	See defect ID for details.
CSCvu07899	During post upgrade task, vCenter reregistration fails with "unknown host" message if the specified host name format is "https://"	4.0(2a)	4.5(1a) 4.0(2c)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvt87832	Residual sentinel snapshot disk-files are marking the cluster out of space	4.0(2a)	See defect ID for details.
CSCvt63306	The size of support bundle is very large when collected with storfs-support command.	4.0(2b) 3.5(2g)	4.5(1a) 4.0(2c)
CSCvt61403	3.5(2g) 5 node hit APD with a bad disk in the cluster	3.5(2g)	4.5(1a) 4.0(2c)
CSCvt61297	Panic on storage controller	4.0(2a)	4.5(1a) 4.0(2b)
CSCvt45344	HyperFlex Stretch Cluster saw poor application performance due to write latency, cluster remained unhealthy and rebalance was stuck	4.0(2a) 4.0(2b) 3.5(2g) 3.5(2a)	4.5(1a) 4.0(2b)
CSCvt41200	When using Mgmt IP Address change we may hit - Unsupported KEX algorithm "diffie-hellman-group1-sha1".	4.0(1b)	4.5(1a)
CSCvt35006	HyperFlex datastores may report high IO latency during CRM primary failover. If current CRM primary node reboots, the new CRM primary initialization can take more time and results in IO latency.	3.5(2h) 3.5(2g)	4.5(1a) 4.0(2e)
CSCvt20203	During an upgrade process the following error is seen: Error while checking cluster upgrade validation details: ... HTTP Status 500 - Internal Server Error ...	4.0(2a) 4.0(1b) 4.0(1a)	See defect ID for details.
CSCvt13929	When running "stcli license..." commands on HyperFlex, the following error is seen: root@SpringpathController:/tmp# stcli license show all Show smart licensing failed: Smart Agent is not ready, please wait a minute and try again	4.0(2a)	4.5(1a) 4.0(2b)
CSCvt06983	Panic while upgrading ESXi.	3.5(2g)	4.5(1a) 4.0(2b)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvs97460	When the cross data-center replication link bandwidth varies from value set by the customer in the HX UI pane for replication during pairing, Springpath controllers would not auto-tune the rate of transmission. This would lead to missing heartbeats and failure to replicate the data across the cluster. We would see replication failures at the UI layer. In addition, in low bandwidth and high latency network, large number of failures would occur due to non-adaptive nature of the replication rate. This enhancement would support varying link bandwidth and a bandwidth drop in link of up to 50% of configured replication bandwidth in HX by automatically controlling rate of transmission.	4.0(2a)	4.5(1a) 4.0(2c)
CSCvs96526	Normal operation when storfs and/or other services consume more than pre-defined or estimated (by HX developers) virtual memory for certain type of cluster.	3.5(2g)	See defect ID for details.
CSCvs86562	On a cluster where VMware EAM manages the controller VMs upgrade fails with exit maintenance mode step failing. You will see more than 3 attempts to power on controller VM fail with error "No host is compatible with the virtual machine" and controller VM gets powered on more than 30 sec after exit maintenance mode.	4.0(2a)	4.5(1a) 4.0(2c)
CSCvs70967	stcli services dns remove should remove the DNS server info from the interface files.	4.0(1a)	4.5(1a) 4.0(2b)
CSCvs69317	Cluster expansion fails at Config Installer stage when the root and admin password for the storage controller(SCVM) are different, and installer doesn't throw any appropriate error message to indicate that the failure is due to an auth failure or passwords mismatch.	3.5(2g)	3.5(2i) 4.0(2b) 4.0(2d) 4.5(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvs69154	After successfully changing(remove/add/update) the DNS server on the HX controller using stcli, but still can see the original DNS entry that was added during the deployment in /etc/network/eth0.interface. The new entries will not be updated in /etc/network/eth0.interface. and /etc/network/eth1.interface.	3.5(2d)	4.5(1a) 4.0(2b)
CSCvs69007	In stretched cluster or with LAZ clusters, rebalance will start even though it not required and sometime may fail.	4.0(2a) 3.5(2g)	4.5(1a) 4.0(2b)
CSCvs54285	A cluster node running HX release 4.0.1b, may hang in the Linux kernel. This is classified as an oops and a deviation from the expected behavior.	4.0(1b) 3.5(2h)	4.5(1a) 4.0(2b) 3.5(2i)
CSCvs53555	You may see this error message after a failed upgrade or other task such as attempting to enter a node into HX maintenance mode: getClusterLocalizableMessage(Operation did not complete in expected time and maybe executing in the background.,None,None,Operation did not complete in expected time and maybe executing in the background.,ArrayBuffer())	3.5(2g) 3.5(2e)	4.5(1a)
CSCvs31606	HX installation QoS warning message is misleading: QoS : Validating QoS class parameter(s) change for system class: 'platinum'. 'weight' will be changes from '24.0%' to '25%'.	4.5(1a) 4.0(2c) 3.5(2e)	4.5(2a) 5.0(1a)
CSCvs08667	HX All-NVME cluster should fail earlier during deployment stage of install/expand	4.0(1b)	5.0(2a)
CSCvr83056	HyperFlex Datastore NFS Queue Depth shows as 256, which can lead to performance (including latency) issues	3.5(2e)	4.5(1a)
CSCvr54687	The cluster becomes inaccessible to the IOVisor.	4.0(2a) 3.5(2d)	4.5(1a) 4.0(2b)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvr47174	HX cluster registration to vCenter requires ping to succeed.	3.5(1a), 3.5(1b), 3.5(1d) 3.5(2a), 3.5(2b), 3.5(2c), 3.5(2d), 3.5(2e), 3.5(2f), 3.5(2g), 3.5(2h) 4.0(1a),4.0(1b), 4.0(2a), 4.0(2b)	5.0(1a)
CSCvr37846	A node in the cluster stopped processing I/Os from clients and other nodes. This caused an All Paths Down timeout in ESX NFS hosts.	3.5(2e)	5.0(1a) 4.0(2c)
CSCvr31746	This defect tracks the condition where bank or rank level ADDDC/VLS Sparing copy causes a temporary stall of HX Controller VM on the impacted node to trigger one or more of the following failure symptoms: 1. If the impacted node had the Zookeeper Leader process running, it can potentially terminate multiple Zookeeper sessions leading to storfs restarts on multiple nodes and eventually an APD 2. The stalling may cause Zookeeper client running on the impacted node to timeout and the session could expire leading to storfs process on that node to restart. This will result in a temporary unhealthy event. 3. The stalling may cause storfs process to observe a high IO latency on one or more drives with active IO requests pending on those drives. This could lead to drives being marked as block listed and the cluster would become unhealthy until the drives are auto-repaired.	2.5(1a) 3.5(1a) 3.5(2a) 3.5(2e) 3.5(2h) 4.0(1a) 4.0(1b) 4.0(2a)	4.5(1a) 4.0(2e)
CSCvr23328	HX node might be removed from HX cluster with a "Node X.X.X.X removed from cluster" message and cluster health degrades	3.0(1h)	4.5(2a) 5.0(1a)
CSCvq96093	Option to Mount multiple datastores together from HX Connect	2.5(1a) 3.0(1a) 3.5(2d)	5.0(2a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvq94466	Node expansion fails due to timeout	3.5(2d)	4.5(1a) 4.0(2e)
CSCvq38092	After manual node removal procedure, stale entries of the removed node continue to exit in the Zookeeper database. Side effect: stcli shows no extra nodes, however node is still present in CRM.	1.7(1) 3.0(1a) 3.5(2a) 3.5(2b) 3.5(2h) 4.0(1a) 4.0(1b) 4.0(2a) 4.0(2e)	4.5(1a)
CSCvh09129	Cluster Expansion: Validation (sufficient DR IP) should occur before adding the node to the cluster.	2.6(1a)	4.5(1a)
CSCve98692	When collecting logs from installer, if the UCSM password is entered incorrectly, it cannot be updated.	2.1(1b)	5.0(1a)
CSCvc74908	Having the cleaner service stopped can result in high HyperFlex space consumption and possibly the cluster going into READONLY state.	3.5(2a), 1.8(1c), 3.0(1i)	5.0(1a)

Hyper-V Caveats

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvy98639	Hyper-V: Datastore becomes inaccessible from a host as result of smbscvmclient being unresponsive.	4.0(2b)	4.5(2b) 5.0(1a)
CSCvy16092	HyperFlex support bundles for Hyper-V do not collect a backtrace of Hyper-V smbscvmclient, rather scvmclient which is not used for datapath in Hyper-V.	4.0(2b)	5.0(1a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvx00104	Management and Data should be on different networks. Ensure that the management IPs entered are in the same subnet... This error is blocks cluster expansion.	4.5(1a)	4.5(2a) 5.0(1a)
CSCvw79576	Hyper-V UCSM downgrade is failing with the error "Error initiating validations for upgrade.". On the browser developer tools network tab there will 500 errors for "/hx/api/clusters/1/upgrade/clusterVersionDetails" API.	4.5(1a)	See defect ID for details.
CSCvw77025	Upgrade will timeout or get error on larger clusters. Upgrade fails with error "Upgrade validation failed. Unable to fetch controller vm state information"	4.0(2e) 4.5(1a)	4.5(2a) 5.0(1a)
CSCvw26610	During HX Hyper-V cluster creation using Windows Server 2019, the HX installer may fail in Hypervisor configuration step stating it was unable to acquire IP address. Inspecting the failed node(s) using KVM console reveals that Windows roles such as Hyper-V, Failover cluster etc. did not get enabled.	4.5(1a)	4.0(2e) 4.5(2a) 5.0(1a)
CSCvt22494	Error while expanding cluster through classic installer: - The time zone name " was not found on the computer. Applicable to Hyper-V environment only	4.0(2a)	4.5(1a)

HXCSI 1.2 Caveats

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvw80780	Resizing of Persistent Volumes fails sometimes for Pods using XFS file system.	1.2(569)	1.2(1a)
CSCvw75518	When editing iSCSI network from HX CLI, the old IP ranges get replaced by the new IP ranges. Only the new IP ranges will be displayed in the network info.	4.5(1a)	4.5(2a)

Defect ID(s)	Symptom Summary	Known Affected Releases	Open, Closed or Fix Applied to:
CSCvw75427	"Running" pod recreated after delete using "kubectl delete pod", got stuck in "Terminating" state on deleting its name space.	4.5(1a)	1.2(1a)
CSCvv68273	When attempting to mount volumes during the HXCSI component deployment, this fails with the error `NodePublishVolumeFSModeError` in 4.5.1a release.	4.5(1a)	1.2(1a)
CSCvu23442	Application pods gets stuck in container creating state or multi attach error state and not able to mount the volumes	4.5(2a)	See defect ID for details.

Related Caveats

The following table list caveats that affect the HXDP product, but are not filed under the HXDP product for Cisco HyperFlex Release 4.5(x). Caveats are listed in descending order to keep the newest additions at the top. Each caveat number is linked to the Cisco Bug Search Tool. Use the link to access additional details about the symptom, conditions and workarounds that apply.

Defect ID(s)	Symptom Summary	Known Affected Releases	Open or Known Fixed Releases
CSCvy84658	Upgrading ESXi to 7.0 U2 may fail on servers running older generation CPUs. The upgrade initiated through HX Connect or through Intersight will display the following failure message: "CPU_SUPPORT WARNING: The CPU in this host may not be supported in future ESXi releases. Please plan accordingly".	1.0 1.0(1)	Open

Mixed Cluster Expansion Guidelines - Cisco HX Release 4.5(x)

- 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 help ensure a seamless **upgrade** experience. For more information, see the HyperFlexHealth & Pre-Upgrade Check Tool TechNote for full instructions on how to install and run Hypercheck.
- Expanding existing M4 cluster with M5 converged nodes is supported.
- Expanding existing M5 cluster with M4 converged nodes is not supported.
- Expanding existing mixed M4/M5 cluster with M4 or M5 converged nodes is supported.

- Adding any supported compute-only nodes is permitted with all M4, M5, and mixed M4/M5 clusters using the HX Data Platform 2.6 or later Installer. Some example combinations are listed here, many other combinations are possible.

```
Example combinations:
Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5
Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5
```

- Only expansion workflow is supported to create a mixed cluster. Initial cluster creation with mixed M4/M5 servers is not supported.
- All M5 servers must match the form factor (220/240), type (Hybrid/AF), security capability (Non-SED only) & disk configuration (QTY, capacity, and non-SED) of the existing M4 servers. For more information on drive compatibility, refer to the Cisco Hyperflex Drive Compatibility document.
  - HX220-M5 will use a maximum of 6 capacity disks (2 disk slots to remain empty) when mixed with HX220-M4.
- HX Edge, SED, LFF, Hyper-V, and Stretched Clusters do not support mixed M4/M5 clusters.

Revision History

Release	Date	Description
4.5(2e)	September 6, 2022	Updated the 4.5 Release notes for Cisco HX Data Platform Software, Release 4.5(2e).
4.5(2d)	July 19, 2022	Updated the 4.5 Release notes for Cisco HX Data Platform Software, Release 4.5(2d).
4.5(2c)	April 19, 2022	Updated the 4.5 Release notes for Cisco HX Data Platform Software, Release 4.5(2c).
4.5(1a)	January 31, 2022	The last date of support for Cisco HX Data Platform Software Version 4.5(1x).
4.5(2b)	December 9, 2021	Created release notes for Cisco HX Data Platform Software, Release 4.5(2b).
4.5(1a)	October 6, 2021	Software maintenance support for 4.5(1x) software release ended on October 6, 2021. No bug fixes, patches or maintenance releases will be provided for this Cisco HyperFlex Data Platform release after that date. For more information, see End-of-Life and End-of-Support Dates for Cisco HyperFlex Data Platform Software Release 4.5(1x)
4.5(2a)	August 30, 2021	Updated Supported Versions and System Requirements for Cisco HXDP Release 4.5(x), on page 6 to indicate UCSM 4.1(3e) qualified for HX 4.5(2a).

Release	Date	Description
4.5(2a)	August 9, 2021	Updated Supported Versions and System Requirements for Cisco HXDP Release 4.5(x), on page 6 to indicate UCSM 4.0(4m) and 4.1(3d) qualified for HX 4.5(2a).
4.5(2a)	June 30, 2021	Created release notes for Cisco HX Data Platform Software, Release 4.5(2a).
4.5(1a)	April 29, 2021	Introduced the Compatibility Catalog Feature. Added support for UCSM 4.1(3c) in Supported Versions and System Requirements for Cisco HXDP Release 4.5(x), on page 6.
4.5(1a)	April 28, 2021	Added new feature description for Cisco HyperFlex HTML5 Plugin for VMware vCenter.
4.5(1a)	March 30, 2021	Updated Supported Versions and System Requirements for Cisco HXDP Release 4.5(x), on page 6 to indicate support for VMware ESXi and vCenter Versions 7.0 U1c through 7.0 U1d builds.
4.5(1a)	March 19, 2021	Added CSCvr31746 to the list of Resolved Caveats. Updated Supported Versions and System Requirements for Cisco HXDP Release 4.5(x), on page 6 to indicate UCSM 4.1(2f) is the recommended Host Upgrade Utility (HUU) for M5.
4.5(1a)	February 19, 2021	Updated Supported Versions and System Requirements for Cisco HXDP Release 4.5(x), on page 6 to indicate UCSM 4.1(2c) qualified for HX 4.5(1a).
4.5(1a)	February 11, 2021	Added CSCvw89325 to list of Caveats in Release 4.5(x), on page 15.
4.5(1a)	January 22, 2021	Added description of HX Hardware Acceleration card support with Native Replication in New Features. Added 7.6TB (HX-SD76T61X-EV) in New Supported Drives, on page 5.
4.5(1a)	January 6, 2021	Created release notes for Cisco HX Data Platform Software, Release 4.5(1a).

Related Documentation

Document	Description
Preinstallation Checklist for Cisco HX Data Platform	Provides an editable file for gathering **required** configuration information prior to starting an installation. This checklist must be filled out and returned to a Cisco account team.
Cisco HyperFlex Systems Installation Guide for VMware ESXi, Release 4.5	Provides detailed information about Day 0 configuration of HyperFlex Systems and related post cluster configuration tasks. It also describes how to set up multiple HX clusters, expand an HX cluster, set up a mixed HX cluster, and attach external storage.
Cisco HyperFlex Systems Stretched Cluster Guide, Release 4.5	Provides installation and configuration procedures for HyperFlex Stretched cluster, enabling you to deploy an Active-Active disaster avoidance solution for mission critical workloads.
Cisco HyperFlex Systems Installation Guide for Microsoft Hyper-V, Release 4.5	Provides installation and configuration procedures on how to install and configure Cisco HyperFlex Systems on Microsoft Hyper-V.
Cisco HyperFlex Edge Deployment Guide, Release 4.5	Provides deployment procedures for HyperFlex Edge, designed to bring hyperconvergence to remote and branch office (ROBO) and edge environments.
Cisco HyperFlex Data Platform Administration Guide, Release 4.5	Provides information about how to manage and monitor the cluster, encryption, data protection (replication and recovery), ReadyClones, Native snapshots, and user management. Interfaces include HX Connect, HX Data Platform Plug-in, and the `stcli` commands.
Cisco HyperFlex Data Platform Administration Guide, Release 4.5	Provides information about how to manage and monitor the Hyper-V cluster, encryption, data protection (replication and recovery), ReadyClones, Hyper-V Checkpoints, and user management. Interfaces include Cisco HyperFlex Systems, and the `hxcli` commands.
Cisco HyperFlex Systems Administration Guide for Kubernetes, Release 4.5	Provides information about HyperFlex storage integration for Kubernetes and instructions on how to configure Cisco HyperFlex Container Storage Interface (CSI) storage integration.
Cisco HyperFlex Systems Administration Guide for Citrix Workspace Appliance, Release 4.5	Provides installation, configuration, and deployment procedures for a HyperFlex system to connect to Citrix Workspaces and associated Citrix Cloud subscription services such as Citrix Virtual Apps and Desktops Services. The Citrix Ready HCI Workspace Appliance program enables a Cisco HyperFlex System deployed on Microsoft Hyper-V to connect to Citrix Cloud.
Cisco HyperFlex Systems Installation Guide for Cisco Intersight	Provides installation, configuration, and deployment procedures for HyperFlex Intersight, designed to deliver secure infrastructure management anywhere from the cloud.
Cisco HyperFlex Systems Upgrade Guide for VMware ESXi, Release 4.5	Provides information on how to upgrade an existing installation of Cisco HX Data Platform, upgrade guidelines, and information about various upgrade tasks.

Document	Description
Cisco HyperFlex Systems Network and External Storage Management Guide	Provides information about HyperFlex Systems specific network and external storage management tasks.
Cisco HyperFlex Data Platform CLI Guide, 4.5	Provides CLI reference information for HX Data Platform `stcli` and `hxcli`commands.
Cisco HyperFlex PowerShell Cmdlets for Disaster Recovery	Provides information on how to use the Cisco PowerShell Cisco HXPowerCLI cmdlets for Data Protection.
REST API Getting Started Guide REST API Reference	Provides information related to REST APIs that enable external applications to interface directly with the Cisco HyperFlex management plane.
Cisco HyperFlex Systems Troubleshooting Reference Guide, 4.5	Provides troubleshooting for installation, configuration, to configuration, and to configuration. In addition, this guide provides information about understanding system events, errors, Smart Call Home, and Cisco support.
TechNotes	Provides independent knowledge base articles.
Release Notes for UCS Manager, Release 4.1	Provides information on recommended FI/Server firmware.

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.