Cisco HyperFlex 3.5 Systems HX Series

Common Criteria

Operational User Guidance

and

Preparative Procedures

Version 1.0

7 October 2019

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

The following acronyms and abbreviations are common and may be used in this Guidance document:

Table 1 Acronyms and Abbreviations

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CIMC	Cisco Integrated Management Controller
CIM-XML	Common Information Model XML
CLI	Command Line Interface
CM	Configuration Management
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
FC	Fibre Channel
HDD	Hard-disk drives
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface providing management access through the network
ISDN	Integrated Services Digital Network
LAN	Local Area Network
OS	Operating System
SAN	Storage Area Network
SAR	Security Assurance Requirement
SDN	Software-defined networking
SFP	Security Functional Policy
SFR	Security Functional Requirement
SM	Service Module
SSD	Solid-state disk
SSL	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UCS	[Cisco] Unified Computing System

Acronyms / Abbreviations	Definition
UCSM	UCS Manager
UDP	User datagram protocol
VIB	VMware ESXi vSphere Installation Bundles
VLAN	Virtual Local Area Network
VM	Virtual Machine, a virtualized guest operating system installed to a hypervisor.
VMM	Virtual Machine Manager, a hypervisor.
VSAN	Virtual Storage Area Network
XML	Extensible Markup Language
XML API	The UCS Manager XML API is a programmatic interface for managing UCS via CLI

Terminology

The following terms are common for this technology and may be used in this Guidance document:

Table 2 Terminology

Term	Definition
Cluster	A collection of hosts that are interconnected for the purpose of improving reliability, availability, serviceability, load balancing and performance. In this document, cluster implies the storage cluster, unless otherwise stated.
Cluster Access Policy	HX Data Platform (TOE) configurable feature that specifies storage cluster data management when the nodes or disks fail in the storage cluster. For example, when the storage cluster changes to read-only mode to protect data.
Datastore	A logical container, similar to a file system on a logical volume. Datastores are where the host places virtual disk files and other VM files. Datastores hide the specifics of physical storage devices and provide a uniform model for storing VM files.
Extended Cluster	The addition of Cisco UCS rack-mount servers and/or Cisco UCS 5108 Blade chassis, which house Cisco UCS blade servers that allows for additional compute resources in an extended cluster design.
Hyperconvergence	Turning standard servers of choice into a single pool of compute and storage resources.
HyperFlex HX Data Platform Controller (also referenced as controller VM)	The HyperFlex HX Data Platform controller resides on each node and implements the distributed file system. The controller VM runs in user space within a virtual machine, intercepts, and handles all I/O from guest virtual machines (VM).
IO Visor	This [TOE] VIB provides a network file system (NFS) mount point so that the ESXi hypervisor can access the virtual disk drives that are attached to individual virtual machines. From the hypervisor's perspective, it is simply attached to a network file system.
Layer 2 (L2)	Layer 2, also known as the Data Link Layer, is the second level in the seven-layer OSI reference model for network protocol design. Layer 2 is

Term	Definition
	equivalent to the link layer (the lowest layer) in the TCP/IP network model. Layer2 is the network layer used to transfer data between adjacent network nodes in a wide area network or between nodes on the same local area network.
Layer 3 (L3)	Layer 3 refers to the third layer of the Open Systems Interconnection (OSI) Model, which is the network layer. Layer 3 is responsible for all packet forwarding between intermediate routers, as opposed to Layer 2 (the data link layer), which is responsible for media access control and flow control, as well as error checking of Layer 1 processes. Traditional switching operates at layer 2 of the OSI model, where packets are sent to a specific switch port based on destination MAC addresses. Routing operates at layer 3, where packets are sent to a specific next-hop IP address, based on destination IP address. Devices in the same layer 2 segment do not need routing to reach local peers. What is needed however is the destination MAC address which can be resolved through the Address Resolution Protocol (ARP)
Private Fiber	The term Private Fiber' encompasses the leasing 'private' fiber optic cables from network providers. A client leases or purchases unused strands of 'private' fiber optic cable to create their own privately-operated optical fiber network rather than simply leasing bandwidth. The Private Fiber network is separate from the public (main) network and is controlled by the client and not the network provider. Private Fiber networks can be set up in a variety of ways, including Private Fiber rings, point to point or point-to-multipoint configurations. With Private Fiber, a client can expect higher levels of performance, a highly secure network and superfast speeds.
Split Brain	In the Stretched Cluster (SC) deployment this is where the two sides of the system lose communication with one another, but the system has not actually failed. In this circumstance, if either side has no secondary method besides network communication for determining if the other side has actually failed, in the interest of maximizing system availability it will decide that it is now the authoritative or active half. As such, both sides would make the same determination, therefore both sides would think they are active and in charge of the overall system, hence the term "split brain".
Standard Cluster	Composed of a pair of Cisco UCS Fabric Interconnects along with up to thirty-two HX-Series rack-mount servers per cluster.
Storage Cluster	The storage cluster created on hypervisor platform, such as vSphere. The storage cluster is independent of the associated vCenter cluster and spans across hosts and appliances. This storage cluster contains the converged nodes and their associated storage that the HX Data Platform (TOE) manages. This storage cluster can also include compute nodes, that do not include storage, and that the HX Data Platform (TOE) monitors.

Term	Definition
Stretched Cluster (SC)	Stretched Cluster (SC) allow nodes to be evenly split between two physical locations, keeping a duplicate copy of all data in both locations, thereby providing protection in case of an entire site failure. The connection between the two sites is secured using the Private Fiber for point-to-point network configuration.
Users	The users of the TOE are the processes and applications on the VMs that are on the TOE that access the storage clusters and datastores which are provided by the TOE.
Virtual Local Area Network (VLAN)	VLAN VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN. The most important requirement of VLANs is the ability to identify the origination point for packets with a VLAN tag to ensure packets can only travel to interfaces for which they are authorized, thus creating Layer 2 (data link) implementations of subnets.
Virtual Machines (VMs)	The virtual machines are the virtual servers on the TOE that access the storage clusters and datastores, which are provided by the TOE.
vMotion	Enables the live migration of running virtual machines from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It is transparent to users.
VMware vCenter	In the evaluated configuration, VMware vCenter functions as a remote authentication server providing the Authorized Administrator the capability of creating additional administrator accounts and storing the credentials.
VMware vStorage API for Array Integration (VAAI)	This storage offload [TOE] API allows vSphere to request advanced file system operations such as snapshots and cloning. The HyperFlex HX Data Platform controller causes these operations to occur through manipulation of metadata rather than actual data copying, providing rapid response, and thus rapid deployment of new application environments
Whitelist	A whitelist may consist of a list of users, applications or processes that are viewed with approval or being provided a particular privilege. Entities on the whitelist will be approved, recognized and/or accepted. For the TOE, the whitelist consists of IP addresses of the VMs that have access to the HyperFlex HX Data storage clusters and datastores that are controlled and enforced by the TOE.
Witness VM	A Witness VM is part of the Stretched Cluster (SC) to avoid 'Split Brain' scenario, a third system (Witness VM) is required to break this tie or provide additional information and decision-making logic to prevent simultaneous takeover by the two sides of the Stretched Cluster.

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco HyperFlex Systems HX Series running Cisco HyperFlex HX Data Platform Software, version 3.5(2a), VMware ESXi version. This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco HyperFlex Systems HX Series running Cisco HyperFlex HX Data Platform Software, version 3.5(2a) TOE certified under Common Criteria. The Cisco HyperFlex Systems HX Series running Cisco HyperFlex HX Data Platform Software, version 3.5(2a), VMware ESXi version. TOE may be referenced below as the HyperFlex HX Data Platform or TOE.

1.1 Audience

This document is written for administrators configuring and maintaining the TOE, specifically the HyperFlex HX Data Platform Software. This document assumes that you are familiar with the basic concepts and terminologies used in computing and storage in virtual environments, understand your network topology, that you are a trusted individual, and that you are familiar with and trained to use virtualization, networking, and storage setup and configuration.

For using the HyperFlex HX Data Platform command-line interfaces refer to **[4]b**.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, such as such as the type or quantity of VMs, the number of Authorized Administrators or which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining the TOE operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 7 of this document provides information for obtaining assistance in using Cisco HyperFlex Systems HX Series.

1.3 Document References

This document makes reference to several Cisco Systems product documents. The documents used are shown below.

Table 3 Document Reference

Reference number	Document Name	Link
[1]	Release Notes for Cisco HX Data Platform, Release 3.5	https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatfor

Reference number	Document Name	Link
		mSoftware/Cisco_HXDataPlatform_RN_3_5.html
[2]	Installation guides (a) Cisco HyperFlex HXAF220c – M5SX All – Flash Node (b) Cisco HyperFlex HXAF240c – M5SX All – Flash Node (c) Cisco HyperFlex HX220c – M5SX Hybrid Node (d) Cisco HyperFlex HX240c – M5SX Hybrid Node (e) Cisco HyperFlex HX240c – M5L Hybrid Node (f) Cisco HyperFlex HXAF220c – M4S All-Flash Node (g) Cisco HyperFlex HXAF240c – M4SX All-Flash Node	(a) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX220c_M5/HX220c_M5.html (b) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX240c_M5/HX240c_M5/HX240c_M5_chapter_00.html (c) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX220c_M5/HX220c_M5.html (d) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX240c_M5/HX240c_M5/HX240c_M5_chapter_00.html (e) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX240c_M5/HX240c_M5/HX240c_M5_chapter_00.html (f) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX240c_M4/HX240c.html (g) https://www.cisco.com/c/en/us/td/docs/hyperconverged_syste

Reference number	Document Name	Link
		ms/HX_series/HX240c_M4/HX240c/overview.html
	(h) Cisco HyperFlex HX220c – M4S Hybrid Node	(h) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX220c_M4/HX220c.html
	(i) Cisco HyperFlex HX240c – M4SX Hybrid Node	(i) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HX_series/HX240c_M4/HX240c.html
[3]	(a) Preinstallation Checklist for Cisco HX Data Platform	(a) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_Preinstall_Checklist/b_HX_Data_Platform_Preinstall_Checklist.html
	(b) Cisco HyperFlex Systems Installation Guide for ESXi, Release 3.5	(b) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/Installation_VMWare_ESXi/3_5/b_HyperFlexSystems_Installation_Guide_for_VMware_ESXi_3_5.html
	(c) Cisco HyperFlex Systems Upgrade Guide for VMware ESXi, Release 3.5	(c) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_upgrade_guide/3-5/b_HyperFlexSystems_Upgrade_Guide_for_VMware_ESXi_3_5.html
	(d) Cisco HyperFlex Systems Stretched Cluster Guide, Release 3.5	(d) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HyperFlex_Stretched_Cluster/3_5/b_HyperFlex_Sy

Reference number	Document Name	Link
		stems_Stretched_Cluster_Guide_3_5.pdf
[4]	(a) Cisco HyperFlex Data Platform Administration Guide, Release 3.5 (Includes HX Connect Interface) (b) Cisco HyperFlex Data Platform CLI Guide, 3.5 (c) Cisco HyperFlex 3.0 for Virtual Server Infrastructure with VMware ESXi	(a) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/AdminGuide/3_5/b_HyperFlexSystems_AdministrationGuide_3_5.html (b) https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/CLIGuide/3_5/b_HyperFlexSystems_CLIReferenceGuide_3_5.html (c) https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/hyperflex_30_vsi_esxi.html
[5]	Cisco HyperFlex Systems Documentation Roadmap	https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HX_Documentation_Roadmap/HX_Series_Doc_Roadmap.html https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/tsd-products-support-series-home.html
[6]	vSphere Virtual Machine Administration ESXi 5.5 vCenter Server 5.5	https://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-virtual-machine-admin-guide.pdf
[7]	VMware vCenter Operations Manager Administration Guide Custom User Interface vCenter Operations Manager 5.7	https://www.vmware.com/pdf/vcops-57-custom-ui-admin-guide.pdf
[8]	VMware vSphere 5.1 Documentation Center	https://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.doc/GUID-1B959D6B-

Reference number	Document Name	Link
		41CA-4E23-A7DB-E9165D5A0E80.html
[9]	Cisco HyperFlex Systems Troubleshooting Reference Guide, 3.0	https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HX_TroubleshootingGuide/3-0/b_HyperFlexSystems_TroubleshootingGuide_3_0.html

1.4 Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria Cisco HyperFlex Systems HX Series running Cisco HyperFlex HX Data Platform Software, version 3.5(2a) EAL2 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

1.4.1 Supported HyperFlex Systems HX Series Nodes and Software

The HyperFlex Systems HX Series Nodes that comprises the TOE is the:

- Cisco HyperFlex HXAF220c – M5SX All – Flash Node
- Cisco HyperFlex HXAF240c – M5SX All – Flash Node
- Cisco HyperFlex HX220c – M5SX Hybrid Node
- Cisco HyperFlex HX240c – M5SX Hybrid Node
- Cisco HyperFlex HX240c – M5L Hybrid Node
- Cisco HyperFlex HXAF220c – M4S All-Flash Node
- Cisco HyperFlex HXAF240c – M4SX All-Flash Node
- Cisco HyperFlex HX220c – M4S Hybrid Node
- Cisco HyperFlex HX240c – M4SX Hybrid Node

The Nodes have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the HyperFlex HX (such as the number and types of SSDs and hard drives and throughput) and therefore support security equivalency of the HyperFlex HX in terms of hardware.

The TOE consists of any one of a number of hardware configurations for the HyperFlex HX-Series Servers, each running the same version of Cisco HyperFlex HX Data Platform Software, version 3.5(2a), VMware ESXi version respectively. The evaluated configurations consist of the following Nodes, each providing power, cooling and backplane connections:

- The small footprint Cisco HyperFlex HXAF220c-M5SX all-flash model contains:
  - a 240 GB M.2 form factor solid-state disk (SSD) that acts as the boot drive,
  - a 240 GB housekeeping SSD drive,

  - either a single 375 GB Optane NVMe SSD, a 1.6 TB NVMe SSD or 400GB SAS SSD write-log drive,
  - and six to eight 960GB or 3.8TB SATA SSD drives for storage capacity.

- This capacity optimized Cisco HyperFlex HXAF240c-M5SX all-flash model contains:
  - a 240 GB M.2 form factor solid-state disk (SSD) that acts as the boot drive,
  - a 240 GB housekeeping SSD drive, either a single 375 GB Optane NVMe SSD, a 1.6 TB NVMe SSD or 400GB SAS SSD write-log drive installed in a rear hot swappable slot,
  - and six to twenty-three 960 GB or 3.8 TB SATA SSD drives for storage capacity.

- This small footprint Cisco HyperFlex HX220c-M5SX hybrid model contains:
  - a minimum of six, and up to eight 1.8 terabyte (TB) or 1.2 TB SAS hard disk drives (HDD) that contribute to cluster storage capacity,
  - a 240 GB SSD housekeeping drive, a 480 GB or 800 GB SSD caching drive,
  - and a 240 GB M.2 form factor SSD that acts as the boot drive

- This capacity optimized Cisco HyperFlex HX240c-M5SX hybrid model contains:
  - a minimum of six and up to twenty-three 1.8 TB or 1.2 TB SAS small form factor (SFF) harddisk drives (HDD) that contribute to cluster storage,
  - a 240 GB SSD housekeeping drive, a single 1.6 TB SSD caching drive installed in a rear hot swappable slot,
  - and a 240 GB M.2 form factor SSD that acts as the boot drive

- This density optimized Cisco HyperFlex HX240c-M5L hybrid model contains:
  - a minimum of six and up to twelve 6 TB or 8 TB SAS large form factor (LFF) hard disk drives (HDD) that contribute to cluster storage,
  - a 240 GB SSD housekeeping drive and a single 3.2 TB SSD caching drive, both installed in the rear hot swappable slots,
  - and a 240 GB M.2 form factor SSD that acts as the boot drive

- This small footprint Cisco HyperFlex HXAF220c-M4S all-flash model contains:
  - two Cisco Flexible Flash (FlexFlash) Secure Digital (SD) cards that act as the boot drives,

  - a single 120 GB or 240 GB solid-state disk (SSD) data-logging drive,
  - a single 400 GB NVMe or a 400GB or 800 GB SAS SSD write-log drive,
  - and six 960 GB or 3.8 terabyte (TB) SATA SSD drives for storage capacity.

- This capacity optimized Cisco HyperFlex HXAF240c-M4SX all-flash model contains:
  - two FlexFlash SD cards that act as boot drives, a single 120 GB or 240 GB solid-state disk (SSD) data-logging drive,
  - a single 400 GB NVMe or a 400GB or 800 GB SAS SSD write-log drive,
  - and six to twenty-three 960 GB or 3.8 terabyte (TB) SATA SSD drives for storage capacity

- This small footprint Cisco HyperFlex HX220c-M4S hybrid model contains:
  - six 1.8 terabyte (TB) or 1.2 TB SAS HDD drives that contribute to cluster storage capacity,
  - a 120 GB or 240 GB SSD housekeeping drive,
  - a 480 GB SAS SSD caching drive,
  - and two Cisco Flexible Flash (FlexFlash) Secure Digital (SD) cards that act as boot drives.

- This capacity optimized Cisco HyperFlex HX240c-M4SX hybrid model contains:
  - a minimum of six and up to twenty-three 1.8 TB or 1.2 TB SAS HDD drives that contribute to cluster storage,
  - a single 120 GB or 240 GB SSD housekeeping drive,
  - a single 1.6 TB SAS SSD caching drive,
  - and two FlexFlash SD cards that act as the boot drives.

Each node includes a Cisco HyperFlex HX Data Platform controller that implements the distributed file system using internal flash-based SSD drives and high-capacity HDDs to store data. The controllers communicate with each other over 10 Gigabit Ethernet to present a single pool of storage that spans the nodes in the cluster.

Cisco HyperFlex HX Data Platform Software, version 3.5(2a) is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective enterprise-class data management that includes data protection in distributed storage, simplified data management with continuous data optimization and dynamic data placement in node memory.

Although HyperFlex HX Data Platform Software performs many networking functions, this TOE only addresses the functions that satisfy the requirements as defined in this Security Target (ST). For example,

- Security audit – The TOE generates audit records to assist the Authorized Administrator in monitoring the security state of the HyperFlex HX Data Platform as well as trouble shooting various problems that arise throughout the operation of the TOE in its evaluated configuration.
- User Data Protection – The TOE provides access controls to the TOE Converged hosts, clusters and datastores.
- Identification and authentication – The TOE ensures that all Authorized Administrators are successfully identified and authenticated prior to gaining access to the TOE and terminates connection after a configured period of inactivity.
- Secure Management – The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs through the HX Connect (GUI) (over HTTPS) and/or the HXCLI (over SSHv2). All the TOE management functions are restricted to Authorized Administrator. The term "Authorized Administrator" is used in this ST to refer to any user account that has been assigned the privileges to perform the relevant action. The TOE provides the ability to perform the following actions:
    - Administer the TOE locally and remotely
    - Manage access control attributes
    - Manage Authorized Administrator's security attributes, noting the TOE allows for more than one administrator account to be configured. Each Authorized Administrator must be assigned a unique username and password
    - Review audit record logs
    - Configure and manage the system time
- Protection of the TSF - The TOE protects against interference and tampering by untrusted subjects by implementing identification and authentication, access control to the TOE Converged hosts, clusters and datastores and limits configuration options to the Authorized Administrator. Additionally, Cisco HyperFlex HX Series is not a general-purpose operating system and access to Cisco HyperFlex HX Series memory space is restricted to only Cisco HyperFlex HX Series functions. The TOE also provides the capability to protect unavailability of capabilities and system resources and to revert to a saved space in the case of hardware or system disruption of failure. Finally, the TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Authorized Administrator can update the TOE's clock manually or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source.
- TOE access - The TOE can enforce the termination of inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated, the TOE requires the Authorized Administrator to re-authenticate to establish a new session.
- Resource Utilization - Ensures the system, resources and data is preserved in case of a failure or degradation of services.

- Trusted Path/Channel – Ensures a trusted path is established between the TOE and the HX Connect (GUI) using HTTPS and for the HXCLI using SSHv2.

1.4.2 Supported HyperFlex Systems HX Series Configurations

The following diagram, Figure 1 Cisco HyperFlex Standard Cluster Topology illustrates the Cisco HyperFlex system, composed of a pair of Cisco UCS Fabric Interconnects along with up to thirty-two HX-Series rack-mount servers per cluster. Up to thirty-two compute-only, servers can also be added per HyperFlex cluster. The HyperFlex cluster is a group of HX-Series Servers. Each HX-Series Server in the cluster is referred to as a HX node or a Host. Refer to **3[a][b][c]**

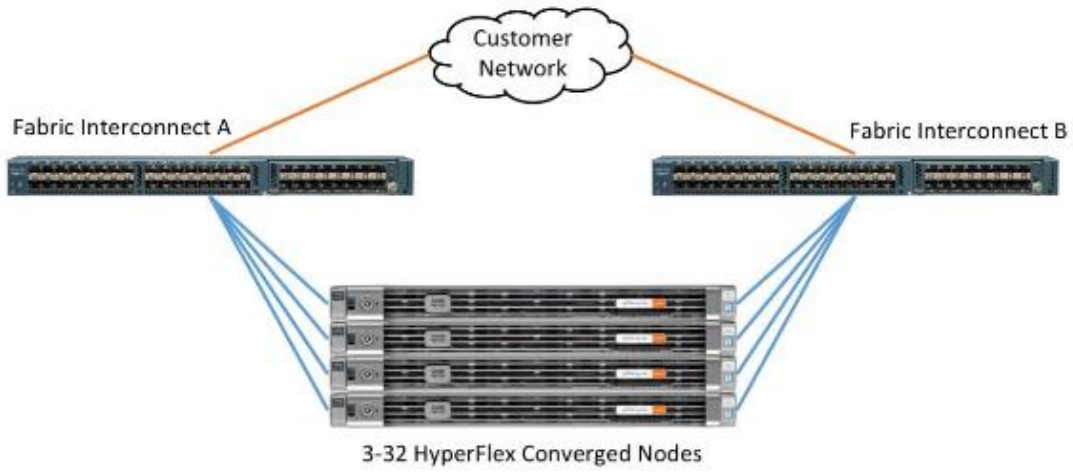


Figure 1 Cisco HyperFlex Standard Cluster Topology

The diagram Figure 2 Cisco HyperFlex Extended Cluster Topology illustrates the addition of Cisco UCS rack-mount servers and/or Cisco UCS 5108 Blade chassis, which house Cisco UCS blade servers that allows for additional compute resources in an extended cluster design. Up to eight separate HX clusters can be installed under a single pair of Fabric Interconnects. The two Fabric Interconnects, [both] connect to every HX-Series rack-mount server and both connect to every Cisco UCS 5108 blade chassis, and Cisco UCS rack-mount server. Refer to **3[a][b][c]**

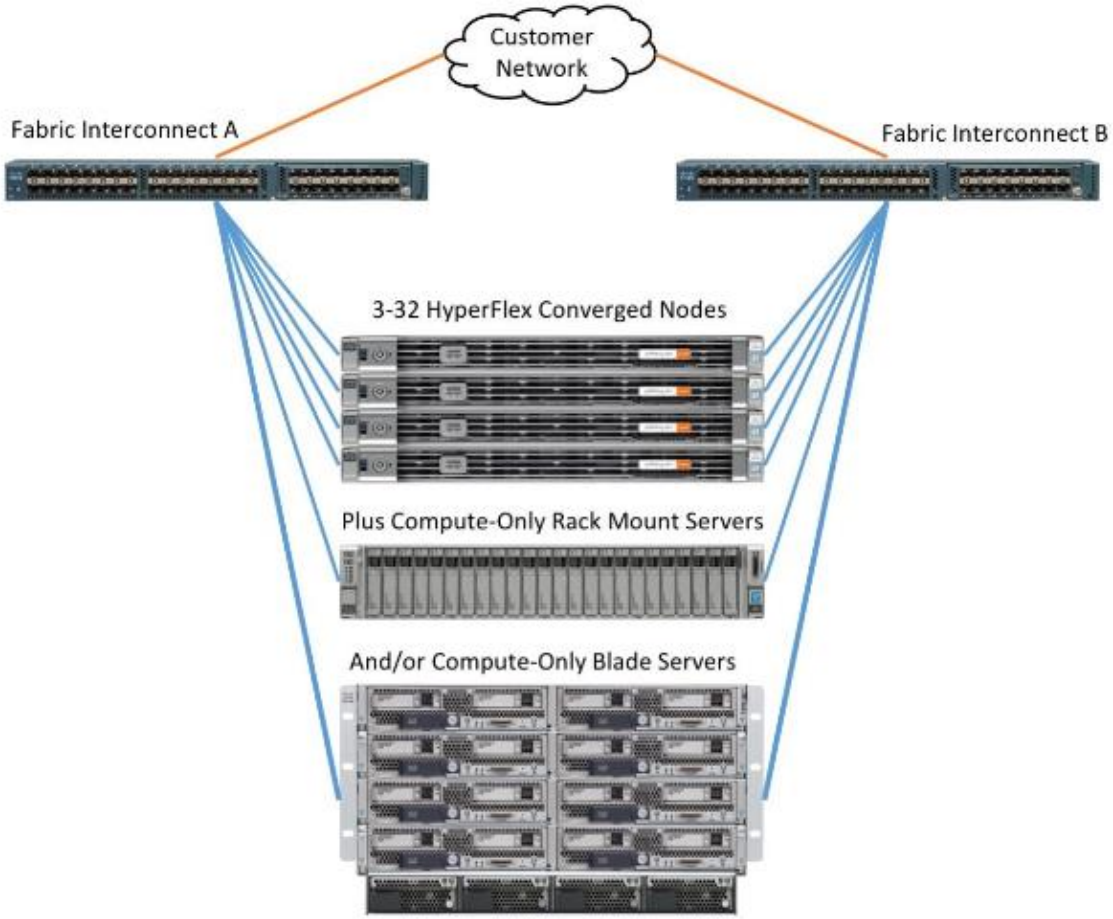


Figure 2 Cisco HyperFlex Extended Cluster Topology

The following diagram, Figure 3 Cisco HyperFlex Stretched Cluster (SC) Topology illustrates the Stretched Cluster (SC). Stretched Cluster (SC) physically locate half of the cluster nodes in one location, while the remaining half are located in a distant secondary location. The data written to the stretched HyperFlex cluster is stored concurrently in both physical locations, therefore this system design provides for additional data protection and availability because the data in the cluster remains available and the cluster remains online, even if an entire site experiences a failure. Since all data written to the cluster is written simultaneously to the two sites, this design can be considered an active/active disaster recovery design. The recovery point objective (RPO), or the maximum amount of data that can potentially be lost prior to a failure is essentially zero, due to all data being immediately and continuously available in both sites. Refer to **3[d] Replication**

The connection between the two sites is a dedicated (Private Fiber) Layer 2 (L2) data link that is protected by virtue of the VLAN that is stretched on the L2 as well. The storage data VLAN on the L2 is non-routed and isolated the same as it is on the switches locally in the standard or extended deployments. As such, all communication on the Storage Controller Data Network is between cluster components that are L2 adjacent on the same

network segment. There are no other components on this network and there is no mechanism for outside devices to access this private network

The management VLAN also behaves the same as it is on the switches locally in the standard or extended deployments and routed to places that have management access. As such, the management network is also extended over the L2 connection.

A Witness VM is part of the Stretched Cluster (SC) to avoid 'Split Brain' scenario, a third system (Witness VM) is required to break this tie or provide additional information and decision-making logic to prevent simultaneous takeover by the two sides of the Stretched Cluster. The Witness VM is a platform running ESXi server in the environment that is installed with the Cisco HyperFlex Data Platform Stretched Cluster Witness software. It is recommended that the Witness VM is physically separated from the two halves of the stretched cluster, installed within a protected area. The connection from the Witness VM is also a dedicated network connection to both of the other two sites within the Stretched Cluster (SC) and is managed through the HyperFlex dashboard the same as are the HyperFlex clusters. Refer to **3[d]**

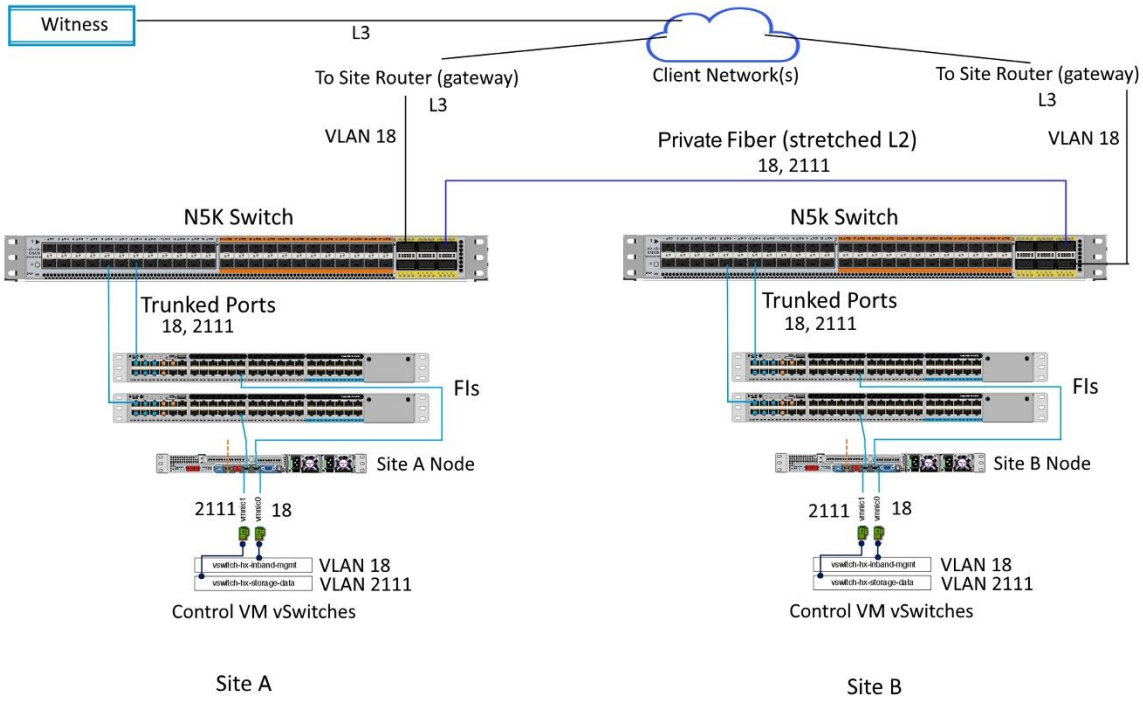


Figure 3 Cisco HyperFlex Stretched Cluster (SC) Topology

As seen in the diagram above, the management network VLAN is shared and accessible externally since it is routed. The data network (2111) is not useable or visible to anyone outside the non-routed 2111 VLAN.

For each of the deployment scenarios, the Fabric Interconnects (FI) are deployed in pairs, wherein the two units operate as a management cluster, while forming two separate network fabrics, referred to as the A side and B side fabrics. Therefore, many design

elements will refer to FI A or FI B, alternatively called fabric A or fabric B. Both Fabric Interconnects are active at all times, passing data on both network fabrics for a redundant and highly available configuration. Management services, including Cisco UCS Manager, are also provided by the two FIs but in a clustered manner, where one FI is the primary, and one is secondary, with a roaming clustered IP address. This primary/secondary relationship is only for the management cluster and has no effect on data transmission.

The diagram below shows the vswitch to FI connectivity on their respective VLANs.

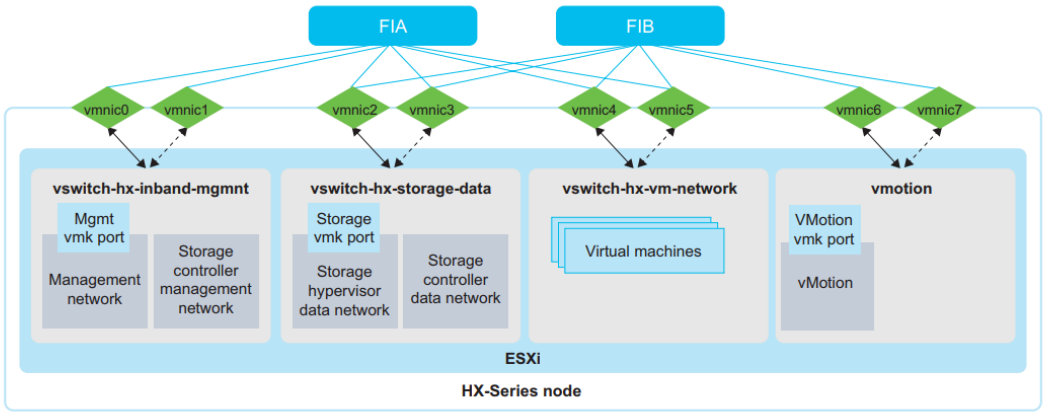


Figure 4 vswitch to FI connectivity

1.5 Operational Environment

1.5.1 Required components and software for the operational environment

Following is the list of required environment components and software for the secure and functional operation of the TOE. It is recommended the operational environment components be installed in a controlled environment where implementation of security policies can be enforced and access controlled. The Authorized Administrator is responsible for the secure operation of the TOE. While the Authorized Administrator may be assigned responsibility of some or all of the operational environment components that responsibility is not covered by this document unless specifically document within.

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
DNS Server	Yes	The DNS Server is required to support IP addresses that are provided as host names for the various components that may be used for traffic and access control.
Fabric Interconnects (FI) (Cisco UCS)	Yes	The FIs provides the connections to the larger network including the switches and servers. The TOE deployment requires a minimum of two FIs for each Cisco HyperFlex Cluster to create high availability.

Component	Required	Usage/Purpose Description for TOE performance
		The FI provides the single point of connectivity and hardware management that integrates Cisco HyperFlex HX Series nodes and Cisco UCS B-Series Blade Servers into a single unified cluster. The two FIs must be directly connected together using Ethernet cables between the two FI ports. This allows both the FIs to continuously monitor the status of each other. Cisco UCS Manager is an embedded software on the pair of fabric interconnects.
Management Workstation	Yes	To manage the TOE via the HXCLI, this includes any IT Environment Management workstation installed with the SSHv2 client to support the TOE HXCLI interface for management of the TOE. The connection of the HXCLI management workstation to the TOE is protected through SSHv2 channel. To manage the TOE via the HX Connect (GUI), this includes any IT Environment Management workstation that supports the following browsers, Microsoft IE 11 or higher, Google Chrome, 54 or higher and Mozilla Firefox 52 or higher. The connection of the HX Connect management workstation to the TOE is protected through HTTPS channel.
NTP Server	Yes	The TOE supports communications with an NTP server to receive clock updates.
Private Fiber	Yes	In Stretched Cluster configuration, Private Fiber from the network provider is required to create the secured, privately-operated optical fiber network connection between the two sites.
SNMP Server	No	The server is required for the AutoSupport service, an alert notification service that is an optional service.
Switches	Yes	The switches provide data transmission and tracking
VMware vSphere[1]	Yes	VMware vSphere ESXi 6.0 software preinstalled (ESXi 6.5 is supported but is not preinstalled). vSphere Editions include Enterprise, Enterprise Plus, Standard, Essentials Plus, ROBO.
VMware vCenter	Yes	In the evaluated configuration, VMware vCenter functions as a remote authentication server providing the Authorized Administrator the capability of creating additional administrator accounts and storing the credentials.

[1] HyperFlex Systems may be pre-installed with VMware vSphere with licensing applied at purchase

1.6 Excluded Functionality

Following is the functionality that is excluded from the evaluated configuration. Not including this functionality does not affect the requirements being claimed.

Table 5 Excluded Functions

Excluded Functionality and Rationale
Telnet sends authentication data in plain text. This feature is disabled by default and must remain disabled in the evaluated configuration.

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that it has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Record the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also verify that the unit has the following external identification:

Table 6 Evaluated Products and their External Identification

Product Name	External Identification
Cisco HyperFlex HXAF220c – M5SX All – Flash Node	Cisco HyperFlex HXAF220c – M5SX
Cisco HyperFlex HXAF240c – M5SX All – Flash Node	Cisco HyperFlex HXAF240c – M5SX
Cisco HyperFlex HX220c – M5SX Hybrid Node	Cisco HyperFlex HX220c – M5SX
Cisco HyperFlex HX240c – M5SX Hybrid Node	Cisco HyperFlex HX240c – M5SX

Product Name	External Identification
Cisco HyperFlex HX240c – M5L Hybrid Node	Cisco HyperFlex HX240c – M5L
Cisco HyperFlex HXAF220c – M4S All-Flash Node	Cisco HyperFlex HXAF220c – M4S
Cisco HyperFlex HXAF240c – M4SX All-Flash Node	Cisco HyperFlex HXAF240c – M4SX
Cisco HyperFlex HX220c – M4S Hybrid Node	Cisco HyperFlex HX220c – M4S
Cisco HyperFlex HX240c – M4SX Hybrid Node	Cisco HyperFlex HX240c – M4SX

Once the TOE has been inspected and external identification has been verified, follow the installation prerequisites for the environmental requirements in **[3](a)(b)**. Upon completion of the environment, following the Node installation instructions and node components firmware update steps in **[2]** for the related Node.

Step 7 After the TOE hardware has been installed and setup, follow the steps below for the approved methods for obtaining a Common Criteria evaluated software image:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html [Login to CCO is required to download, but not to search.]
- The TOE ships with the correct software images installed. When a new software version is released, refer to **[3](c)** Upgrading Cisco HyperFlex System.

Step 8 Once the file is downloaded, you may choose to verify the software image from the trusted system. To verify the published hash you can use a checksum utility of your choice to compute the hash for the downloaded image file and then comparing the results against the image hash listed below.

If the hashes do not match, contact Cisco Technical Assistance Center (TAC) http://tools.cisco.com/ServiceRequestTool/create/launch.do. Login to CCO is required.

Step 10 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the "**stcli cluster version [-h]**" command **[4](b)** to display the currently running version on each Node in the storage cluster. See below for the detailed hash value that must be checked to ensure the software has not been modified in anyway. It is assumed the end-user has acquired a permanent license is valid for the lifetime of the system on which it is installed. If the licenses have not been activated, contact Cisco Technical Assistance Center (TAC) at:

http://tools.cisco.com/ServiceRequestTool/create/launch.do.

Login to CCO is required.

Table 7 Evaluated Software Images

Software Version	Image Name	Image hash values
Cisco HyperFlex HX Data Platform Software, version 3.5(2a), VMware ESXi	Cisco-HX-Data-Platform-Installer-v3.5.21-31601-esx.ova	SHA512 hash – ecdf9d5812dcb6ec3e510209ba1b28352ca808f00b05ea8aa607b801bd08e3dee5007caec26e10db1a1a9b13fa389443d33cc817a927e1924c45440c83a43932

Deploying the TOE in the stretched cluster configuration, you will need to download the following software package to install on the Witness VM.

Table 8 Evaluated Software Images

Software Version	Image Name	Image hash values
Cisco HyperFlex Data Platform Stretched Cluster Witness	HyperFlex-Witness-1.0.3.ova	SHA512 hash – e0053a77e0eca99b79285569fc9b724800bff9b614a9b1ae45e5264057d865fb17e5fc38100d187bb3a5f4de1bd52a7161f065fbf240196a176917c0be041f56

3. Secure Installation and Configuration

Refer to the Preinstallation Checklist and the Installation Guide **[3](a)(b)** for the pre-install checklist for the physical site and the required environment components.

3.1 Physical Installation

Ensure there is adequate power and rack space for your deployment scenario. Also, ensure there is sufficient space for servicing and airflow space. Airflow for the HyperFlex Node is from front to back.

Follow the TOE Hardware Installation Guide **[2](a) thru [2](i)** for preparation of the HyperFlex Node hardware installation.

3.2 Initial HyperFlex HX Setup Requirements

The Cisco HyperFlex Cluster contains a minimum of three and a maximum of eight converged HX-nodes (Cisco HyperFlex HXAF220c–M5SX All-Flash Node, Cisco HyperFlex HXAF240c–M5SX All-Flash Node, Cisco HyperFlex HX220c–M5SX Hybrid Node, Cisco HyperFlex HX240c–M5SX Hybrid Node, Cisco HyperFlex HX240c–M5L Hybrid Node, Cisco HyperFlex HXAF220c–M4S All-Flash Node, Cisco HyperFlex HXAF240c–M4SX All-Flash Node, Cisco HyperFlex HX220c–M4S Hybrid Node or Cisco HyperFlex HX240c–M4SX Hybrid Node). Note, the Stretched Cluster (SC) can only be deployed on the M5 Nodes, M4/M5 mixed cluster is not supported.

Each server in a HyperFlex HX Cluster may also be referred as a Converged host or HX node in this document. The minimum configuration is a single cluster and the maximum configuration supports up to 32 clusters.

The Cisco HyperFlex HX Data Platform requires the following supported versions of non-TOE software:

- VMware vSphere Versions include 6.0 U3, 6.5 U1, 6.5 U2 with VMware vSphere Editions of Enterprise, Enterprise Plus, Standard, Essentials Plus, ROBO. vSphere contains both vCenter and ESXi. The vCenter version must always be equal to or higher than the ESXi version[2].

Refer to the Preinstallation Checklist and the Installation Guide **[3](a)(b)** for a complete checklist of requirements, TOE Hardware Installation Guide **[2](a)-[2](i)** for detail installation specifications specific for the specific Node deployed and the Administration Guides **[4](a)** for the HX Connect GUI and **[4](b)** for the CLI operational configuration settings.

[2] HyperFlex Systems may be pre-installed VMware vSphere with licensing applied at purchase and can be changed after the setup

3.2.1 HyperFlex HX Credential Requirements

During the installation and configuration of the HyperFlex HX-series servers in the Cluster, the same administrator login credentials must be used as all the ESX servers across the storage cluster, all of the HyperFlex HX-series servers must have DNS and NTP configured and all of the HyperFlex HX-series servers in the Cluster must have same VLAN IDs.

All of the HyperFlex HX-series servers must also have SSH enabled. It is recommended that SSHv2 be configured to ensure a secure connection for remote administration using the HXCLI. The HyperFlex HX-series servers must also support HTTPS to ensure a secure connection for remote administration using the HX Connect GUI.

3.2.2 HyperFlex HX Disk Requirements

All of the disks in the HyperFlex HX-series servers in the Cluster must have same amount of storage capacity and have the same number of disk.

The disk partitions must be removed. If the partitions are not removed, they will be ignored and will not be included in the storage cluster. The HDDs must be either SATA or SAS type and be set to pass-through mode and all SSDs must support TRIM and have TRIM enabled.

3.2.3 Environment Hardware Requirements

The following IT entities are non-TOE hardware components and services that are required in the environment. These devices and services are required to be configured prior to the installation of the TOE:

- Cisco UCS Fabric Interconnects (FI) provides the connections to the larger network including the switches and servers.
    - The FI provides the single point of connectivity and hardware management that integrates Cisco HyperFlex HX-Series nodes and Cisco UCS B-Series Blade Servers into a single unified cluster. The two FIs must be directly connected together using Ethernet cables between the two FI ports. This allows both the FIs to continuously monitor the status of each other. Cisco UCS Manager is an embedded software on the pair of fabric interconnects. Refer to **4(c)**.
- Switches provide data transmission and tracking.
- Server4, a Management Workstation to support the CLI for remote administration
- DNS Server to support IP addresses that are provided as host names
- NTP Server for time stamp/synchronization
- Private Fiber from the network provider is required to create the secured, privately-operated optical fiber network connection between the two sites.
- SNMP Server for AutoSupport, an alert notification service that is an optional service
- Trunk ports with VLANs are the access points between the physical and virtual environments. The VLANs are VLAN tagged External Switch VLAN Tagging (EST). The VLAN used for HX storage traffic must be able to traverse the network uplinks from the UCS domain, reaching FI A from FI B, and vice-versa. The

VLANs are configured during install of the TOE, and then managed by VMware ESXi. There are four required zones, though other VLANs may be configured.

- Management Zone: This zone comprises the connections needed to manage the physical hardware, the hypervisor hosts, and the storage platform controller virtual machines (SCVM).
- VM Zone: This zone comprises the connections needed to service network IO to the guest VMs that will run inside the HyperFlex hyperconverged system.
- Storage Zone: This zone comprises the connections used by the Cisco HX Data Platform software, ESXi hosts, and the storage controller VMs to service the HX Distributed Data Filesystem.
- VMotion Zone: This zone comprises the connections used by the ESXi hosts to enable vMotion of the guest VMs from host to host.

Following is a diagram illustrates the logical data path and network design

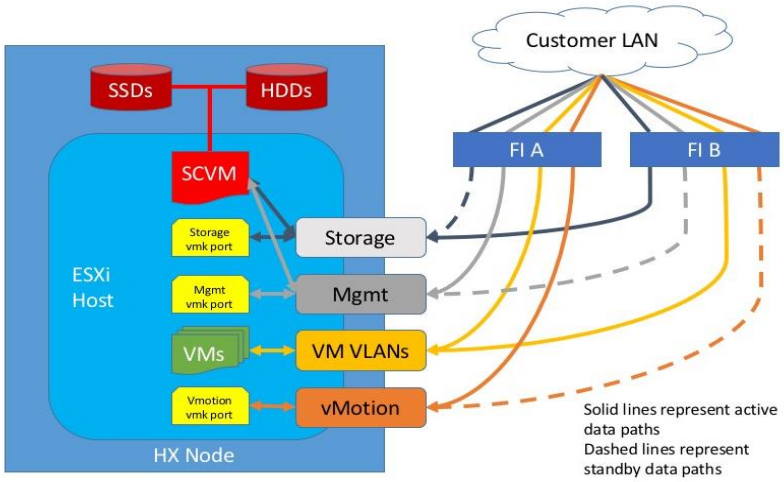


Figure 5 Cisco HX Data logical data paths

To configure the VLANS, cluster and datastores associations and traffic flow controls, refer to **[4](a)(b)(c)**.

Since VLANs exist in their own layer 3 subnet, routing will need to occur for traffic to flow in between VLANs. In a Stretch Cluster, the management VLAN is configured to be routed from the switch to the gateway. The data network VLAN is not routed and can only access layer 2 adjacent nodes (same VLAN same subnet connected by the switch).

The following figure provides a visual depiction of an example TOE deployment. The required environment devices are identified and described above.

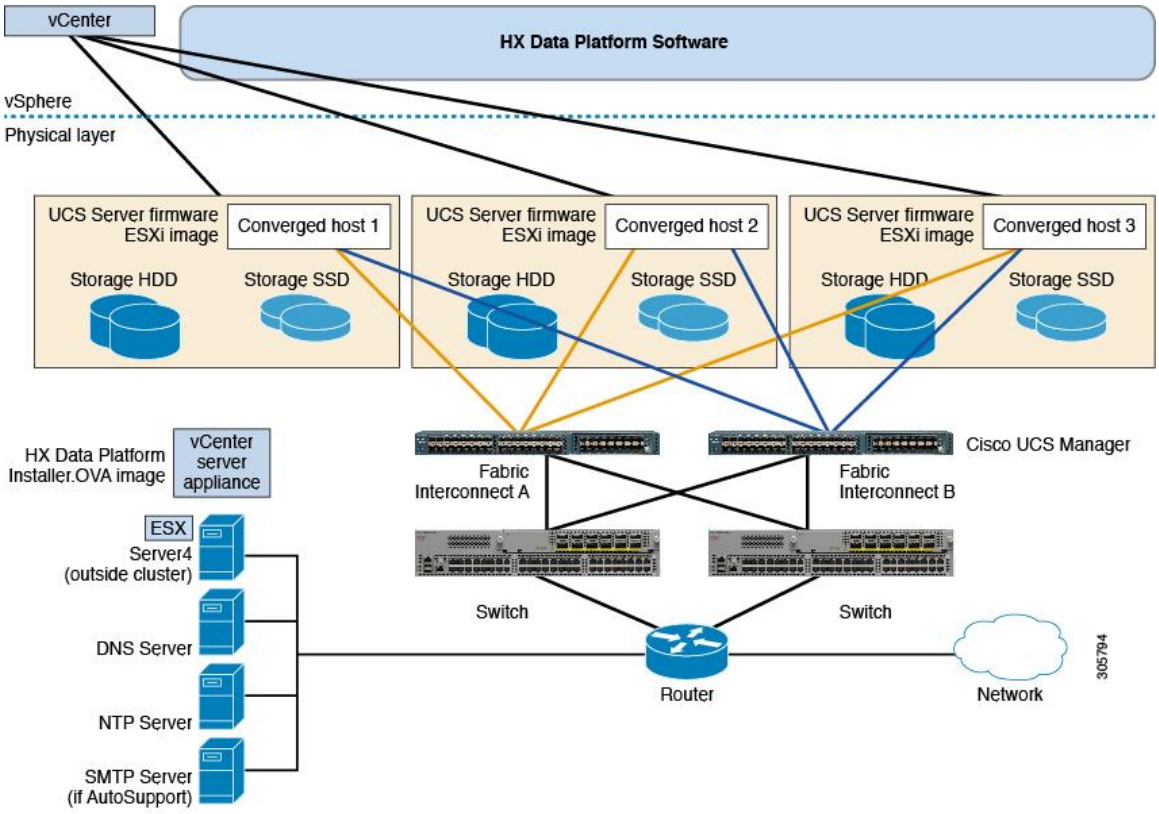


Figure 6 TOE Component Details

The diagram below shows the physical connectivity of the cluster node to the FI. The FI's have uplinks to the site physical switches that service the stretched L2 connection. Only the vSwitches that are traversing the L2 site-to-site connection are shown.

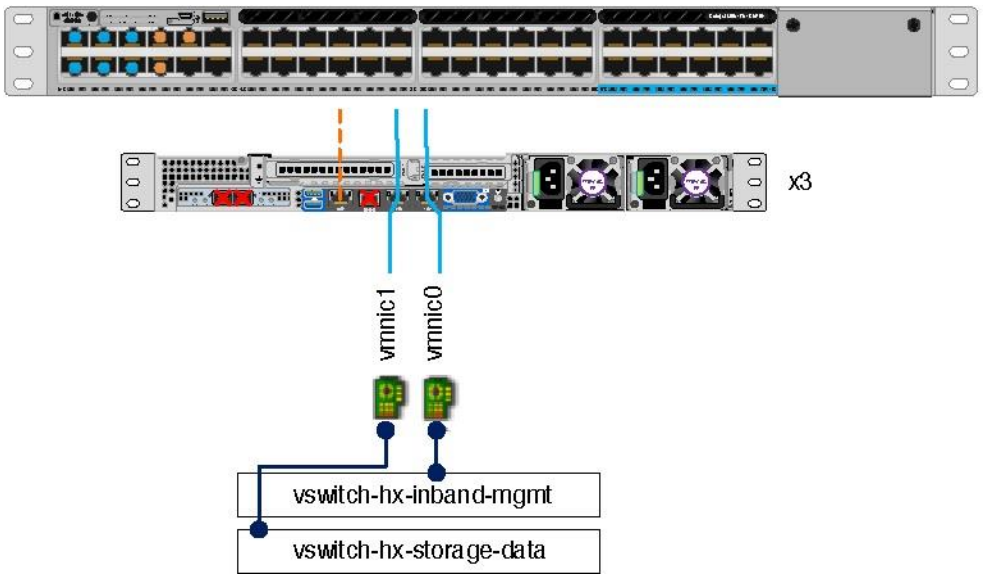


Figure 7 TOE Component Details

3.2.4 Network and Port Settings

Static IP addresses for the Hypervisor for both management and data networks, the subnet mask, default gateway and VLAN tag will be required. Refer to **4(c)**.

If the network and TOE setup is behind a firewall, additional ports will need to be opened. For example, port 443 for HTTPS/TCP, port 123 for NTP and port 22 for SSH. Refer to **4(c)**.

3.3 Administration of Self-Tests

The TOE provides self-tests for the functions in the TOE are run automatically during power-on as part of the POST. These self-test include the following:

Power-on Self-Tests:

- Power up bypass test
- Firmware Integrity Test

Conditional Self-Tests:

- Conditional Bypass Test

3.4 Remote Administration Protocols

3.4.1 HyperFlex CLI (HXCLI)

The HXCLI is the command line interface that is used by the Administrator to manage and trouble shoot the HyperFlex HX-series servers.

To ensure SSH is enabled, from the System Customization panel on the HyperFlex HX-series servers select "Troubleshooting Options". If SSH is disabled, select "Enable SSH" and press Enter. If SSH is already enabled, press "Esc.".

If SSH needs to be configured, use the HXCLI **stctlvm** command. Refer to Administration Guides **[4](b).**

To check that SSHv2 has been configured, you can inspect the **sshd.config** file at **/etc/ssh/sshd_config** by issuing the command:

TOE# **ssh -v localhost**

In the file you will want to see references to *Remote protocol version 2.0*, *SSH2_MSG*.

3.4.2 HyperFlex Connect (HX Connect)

The Cisco HyperFlex Connect (HX Connect) is the GUI interface that is used by the Administrator to manage and monitor HX Storage Clusters, replication, encryption, datastores task and trouble shoot the HyperFlex HX-series servers **[4](a)**.

The requirements for the supported browser include minimum recommended resolution of 1024 X 768 and any one of the following:

Microsoft Internet Explorer 11 or higher, Google Chrome 54 or higher and Mozilla Firefox 52 or higher

Each login to HX Connect is a session. Sessions are the period of activity between time when you log into HX Connect and when you log out. Do not manually clear cookies in a browser during a session, because this also drops the session. Do not close the browser to close a session, though dropped, the session is still counted as an open session. To logout, of HX Connect and properly close the session, select USER (menu top right) -> Logout. Default session maximums include:

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

To login to HX Connect and access the HX Storage Cluster,

Step 1 Start your preferred browser

Step 2 Locate the HX Storage Cluster management IP address. Note, use fully qualified domain name (FQDN) for the management IP address, rather than individual Storage Controller VM.

Step 3 Enter the HX Storage Cluster management IP address in a browser.

Step 4 Enter username and password login credentials.

Refer to Administration Guides **[4](a).**

3.5 Logging Configuration

The TOE generates audit records whenever an audited event occurs. The events include Authorized Administrator actions and system actions that occur on the storage cluster, hosts, or datastores, for example, adding a node to the storage cluster, removing a node from the storage cluster, or reconfiguring a VM resource.

The following are examples of fields that are displayed for the various events that occur on the TOE.

Table 8 Logging Fields

Field	Description
Description	Event message content. See the section for each event type.
Type	Type of message
Date/Time	Timestamp of when the event occurred
Target	Name of the target. Target type options include: storage cluster, host, datastore, or disk
User	The consumer of the resource for the event
VC Cluster Events	Link to vSphere storage cluster Events
Event Detail	The Event detail displays the same content for the event as the Event table. Target link. The Target object in the Event detail links to the vSphere target Summary page.

Field	Description
	For example, the storage cluster Summary page or node Summary page.

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled and the audit records are being generated for the required auditable events.

3.5.1 Reviewing Audited Events

Using the HXCLI, the Authorized Administrator can review audited events. The information provided in the audit records include the date and time of the event, the type of event, subject identity (if applicable), the outcome of the event, and additional information related to the event.

Below are the various required auditable events.

Table 9 Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	None
FMT_MTD.1	All modifications to the values of TSF data	The identity of the authorized administrator performing the operation.
FMT_SMF.1	Use of the management functions	The identity of the authorized administrator performing the operation.
FPT_FLS.1	Failure of the TSF	None

Requirement	Auditable Events	Additional Audit Record Contents
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FRU_FLT.2	Any failure detected by the TSF	None
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	None
FTP_TRP.1	Attempts to use the trusted path functions.	Identification of the user associated with all trusted path invocations including failures, if available.

3.5.2 Reviewing Audit Records

The audit log files are stored in one the following directories: /var/log/springpath/audit.log, stMgrAudit.log, stcli.log and /var/log/auth.log. The /var/log/Springpath/audit.log and stcli.log have records of the HX Connect and HXCLI command events and /var/log/auth.log is for all SSH and HTTPS connections and the stMgrAudit.log includes operations perform and configuration changes to security management functions.

To view the audit logs, use a text editor.

The TOE also generates support bundles that include all system event and audit logs from the TOE platform itself, as well as several components within the TOE boundary and used by the TOE platform. The support bundle includes:

- HX Data Platform Installer VM—Logs provide information about installation.
- Controller VM—Logs provide information about the HX Data Platform file system, cluster creation, and cluster expansion.
- VMware ESXi host—Logs provide information about the nodes in the HX storage cluster.
- VMware vCenter—Logs provide information about the HX Data Platform Plug-in and the vCenter server.

To generate a support bundle using the HX Connect:

- In the dashboard view of HX Connect, click the gear in the top right.
- Select generate support bundle.
- When the bundle is complete, download and use a text editor to view the audit and event logs.

3.5.3 Deleting Audit Records

The TOE provides the Authorized Administrator the ability to delete audit records stored within the TOE to manage the audit space. This is done by deleting the stored audit log file.

3.6 Access Control

After the TOE is installed and configured, the storage clusters are created. The HX Data Platform must be installed before a storage cluster can be created. When the storage cluster is created, all the network connections are configured and established, at which time the TOE storage and access is being managed. The HX Data Platform Controller resides on each node and handles all read and write operation requests from the VMs and implements the distributed file system using internal flash-based SSD drives and high-capacity HDDs to store data.

To control the VMs access to the storage clusters and datastores, whitelists are used to control that access. Once configured, these protected resources are only mountable (accessible) by HX nodes participating in the cluster. The whitelist is an IP table that includes the IP addresses of the Host VMs that have access to the HX nodes clusters and datastores. If the IP address is included on the whitelist and if there is sufficient storage capacity, access is granted otherwise access is denied.

The whitelist access is configured during installation. Once the TOE is operational, updates to the whitelist cannot be modified. Changes that would be allowed would only be allowed during expansion (adding nodes) or removal of nodes.

Following is a diagram that illustrates the Controller and VM access to the node and the datastores.

To configure the whitelist, use the CLI commands, security whitelist to add, clear, remove and list the IP addresses. Refer to **[4](b)**.

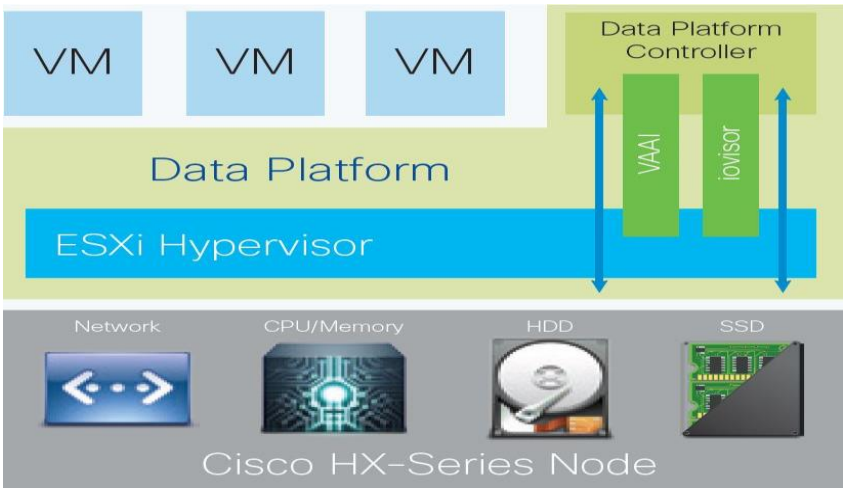


Figure 8 HX Controller and VM access

To configure the clusters and datastores associations refer to **[4](a)(b)(c)**.

To configure the policies, pools, templates and service profiles refer to **[4](a)(b)(c).**

4. Secure Management

4.1 User Roles

The TOE maintains an Authorized Administrator role to administer the TOE remotely. During the installation of the TOE, the Authorized Administrator user is created and has all the required permissions to manage and administer the TOE in the evaluated configuration as defined in this document. Additional Authorized Administrator users may be created, noting that each Authorized Administrator user must be assigned a unique user name and password. The TOE also includes a 'root' user that is created by default during install. This root user should not be used to administer the TOE on a daily basis since this user has full control of the TOE. The root user would be used in cases where an Authorized Administrator was locked out.

All users of the TOE are considered Authorized Administrators. It is assumed all administrators are trusted, trained and knowledgeable and will follow the guidance to ensure the TOE is properly monitored and operated in a secure manner.

4.2 Passwords

By default, there are no restrictions or rules in choosing a password. To prevent users from choosing insecure passwords, password should meet the following requirements:

- At least eight characters long
- Includes a mix of upper and lower alpha characters
- Includes alpha numeric characters
- Does not contain more than three consecutive characters, such as abcd
- Does not contain more than two repeating characters, such as aaabbb
- Does not contain dictionary words
- Does not contain common proper names

This requirement applies to the local password database and on the password selection functions provided by the TOE.

To set password complexity for both management interfaces:

For the HXCLI, is set and configured using HXCLI /etc/pam.d/common-password command. Edit file /etc/pam.d/common-password file, and append the following line to end of file to enforce the complexity rules.

password requisite pam_cracklib.so retry=3 minlen=10 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1

For the HX Connect, is set and configured using vCenter. Log into vCenter with the Administrator account that was created during installation of the TOE. Browse to Administration > Single Sign-On > Configuration, click the Policies tab and select Password Policies, click Edit and edit the password policy parameters to meet the requirements above.

4.3 Administrator Accounts

To add additional HX Connect authorized administrator accounts, log into vCenter with the Administrator account that was created during installation of the TOE. Click on the home icon and select Administration, then select users and groups under single sign on and click the plus icon and create a new Authorized Administrator user. Next click the plus icon and add a new user, noting each authorized administrator must have a unique user and password. Click the plus sign to add permissions, click add in the pop-up and select the user name you just added, then select administrator from drop down box. Next click on Users and Groups, select the groups tab and select the group Administrators and add the user name you just added. Refer to **[7]** for additional information.

4.4 Clock Management

Clock management is restricted to the Authorized Administrator.

The NTP server is required to be setup and configured in the environment prior to creating the Cisco HyperFlex storage cluster. In addition, the NTP server must run continuously after the Cisco HyperFlex storage cluster is created. When nodes are added, whether converged or compute, to the Cisco HyperFlex storage cluster, the new nodes inherit the NTP server configuration from the existing Cisco HyperFlex storage cluster.

To configure the NTP server, perform the following steps:

Step 1 Login to vSphere to ensure NTP is enabled.

Step 2 Select hx-cluster > host > Configuration > Software >Time Configuration > Properties.

Step 3 Enable NTP, click NTP Client Enabled checkbox.

Step 4 Click Options.

Step 5 Select Startup Policy > Start and stop with host.

Step 6 Click NTP Settings > Add.

Step 7 Enter IP address. Click OK.

Step 8 Click Restart NTP service to apply changes. Click OK.

Step 9 Exit Time Configuration dialog, click OK.

Step 10 Repeat Step 2 through Step 9 for each host in the cluster.

For further details, refer to Configuring Cisco HyperFlex Systems -> Preparing the ESX Server -> Ensure NTP is Enabled in **[4](a)**.

The date/time can also be set using the ‘date’ command in the CLI **[4](b)**.

You must also set the time zone. The time zone is used to determine when to take scheduled snapshots. By default, the HyperFlex Controller VM storage controller VM uses UTC time zone.

From the Cluster Configuration page in the HX Data Platform installer, click the down arrow () and select the local time zone for your HX Data Platform plug-in on your vCenter server.

You can also set the time zone using the CLI Services Time Zone Commands **[4](b)**.

4.5 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the Authorized Administrator.

The TOE is configured to use local authentication and authorization. The Authorized Administrator must be successfully identified and authenticated prior to gaining access to the TOE and the TOE security management functions.

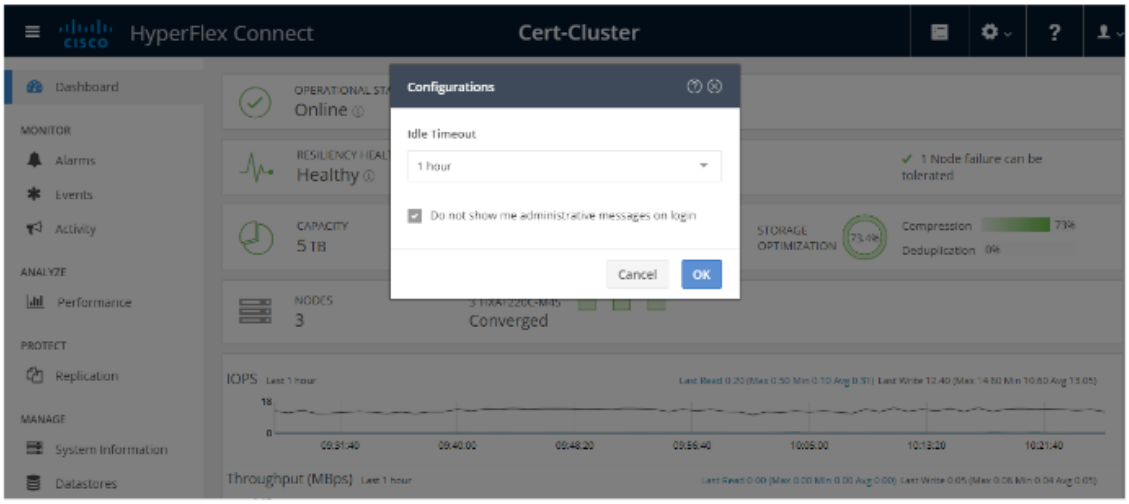
Each Authorized Administrator of the TOE must have a unique username and password.

4.6 Use of Administrative Session Lockout and Termination

The TOE allows the Authorized Administrator to configure the length of time that an inactive administrative session remains open. After the configured period of time, the administrative session is terminated. No further activity is allowed to until the administrator has successfully re-authenticated **[8]**.

The HXCLI, by default does not have an inactivity timeout value set. To set the inactive timeout value, edit the /usr/share/springpath/storfs-misc/sshtimeout.sh file. This script controls SSH session's inactivity timeout to the TOE and controller VM. The settings are in seconds, TMOUT = [seconds].

To set the inactivity timeout on the HX Connect, click on the user icon in the upper right corner of the dashboard.



4.7 Data Preservation with Snapshots

To ensure the TOE is available and resources and data are preserved in case of a failure or degradation of services, the native snapshot function provides the state of the data at a point in time.

A native snapshot is reproduction of a VM that includes the state of the data on all VM disks and the VM power state (on, off, or suspended) at the time the native snapshot is

taken. Take a native snapshot to save the current state of the VM on regular bases, so that you have the option to revert to the saved state.

Refer to **[4](a)(b)(c)** regarding the use of Native Snapshots.

Following is a diagram that illustrates the relative connections and how the data is striped across the Converged Hosts for data preservation.

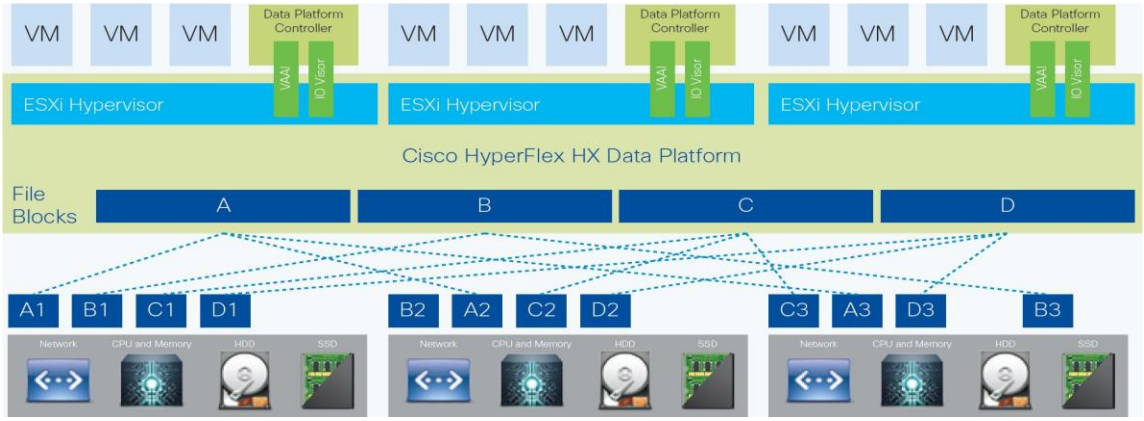


Figure 9 Data Preservation

4.8 Expanding Cluster and Disks Operations

To ensure the TOE resources and storage capabilities are sufficient, the TOE provides the ability to expand and modify the storage and nodes on the storage clusters. This includes adding and removing converged nodes, compute nodes, and disk drives.

To provide increased datastores capacity, storage clusters may be expanded by adding additional Nodes and/or by adding hard drives. There may also be failure of a SSD or HHD that require replacements. Refer to **[4](a)(b)(c)** regarding Expanding the HX Data Platform Cluster and Preparing to Perform Maintenance Operations.

4.9 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See Section 2 Secure Acceptance of the TOE in this document for the method to download and verify an image prior to running it on the TOE. Also refer to **[5]**, Cisco HyperFlex Systems Documentation Roadmap.

5. Modes of Operation

The TOE has several modes of operation, these modes are as follows:

Booting – while booting, the TOE does not allow access the Nodes, Clusters or Datastores until the TOE has been setup and configuration has been saved.

Normal - The TOE image and configuration is complete, and the TOE is operating as configured. All levels of administrative access occur in this mode and that all TOE based security functions are operating. Once in the normal operating mode and fully configured, the Authorized Administrator monitors the Nodes, Clusters and Datastores to ensure they are operating correctly and adequate space allocation is available. The configuration of the TOE can have a detrimental effect on security; therefore, adherence to the guidelines in this document should be followed. Misconfiguration of the TOE could result in the unauthorized access and disruption of space.

Maintenance – Before you perform storage cluster maintenance operations such as adding or removing nodes, disks, or network maintenance, ensure that the storage cluster is healthy and operational using the following steps:

- Serial vs. Parallel Operations
- Checking Cluster Status
- Checking Cluster Rebalance Status
- Checking Cleaner Schedule

Adding nodes to the storage cluster requires that the nodes meet same system requirements as when you installed the HX Data Platform and created the initial storage cluster. See the Cisco HX Data Platform Installation Guide for a complete list of requirements.

This mode also includes upgrading software versions or upgrading the software versions of the ESX server or your vCenter server, contact Technical Assistance Center (TAC), refer to 7.2 Obtaining Technical Assistance in this document.

Degraded - HX Data Platform cluster state is Offline or the Platform health state is Average or there may be at least one failure (such as disk, node, or network) in the storage cluster. You must replace one or more disks to rebalance the storage cluster. Data is still available. If the HX Data Platform controller VM is not operational, the status of the storage cluster changes to Degraded and the node is listed as Missing.

Offline - The storage cluster is not operational.

5.1 Network Processes Available During Normal Operation

The following network-based processes are running, or can be run in the evaluated configurations of the TOE, except where restricted by access policies.

- SSHv2 is supported inbound for remote administrative CLI access to the TOE.
- HTTPS is supported inbound for remote administrative GUI access to the TOE.
- NTP is supported for time synchronization (NTP connections are recommended to be through a secure connection).

Infrastructure services

- Cisco HyperFlex HX Data Platform Software, version 3.5(2a) software; to be configured for use as described in this document.
- Redundant components, such as power supplies and fans.
- Automation through Embedded Event Manager (EEM); no claims are made in the evaluated configuration.
- AutoQoS (quality of services responding to traffic flows); no claims are made in the evaluated configuration.

Processes that should not be used in the evaluated configuration are SSH or HTTPS as a client (outbound connections) as process provides man-in-the-middle protection.

6. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. The following identifies the requirements and the associated security measures of the authorized users.

Table 10 Environment Objectives

Security Objective for the Operational Environment (from the Security Target)	**Definition of the Security Objective** (from the Security Target)	**Responsibility of the Administrators**
OE.ADMIN	The Authorized Administrator are well trained and trusted to manage the TOE and to configure the IT environment and required non-TOE devices for the proper network support.	Authorized Administrators must be trained and must read, understand and follow the guidance in this document to securely install and operate the TOE.
OE.CONNECTION	The operational environment will have the required protected network support for the operation of the TOE to prevent unauthorized access to the TOE.	Authorized Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE.
OE_SC.CONNECTION	The operational environment will have the required Private Fiber network when the TOE is deployed in the Stretched Cluster configuration to prevent unauthorized access to the TOE.	Authorized Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE when deployed in the Stretched Cluster using the Private Fiber for point-to-point network configuration.
OE.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.	The TOE and the operational environment components are required to be installed in a controlled environment where access is controlled. The Authorized Administrator is responsible for the secure operation of the TOE. While the Authorized Administrator may be assigned responsibility of some or all of the operational environment

Security Objective for the Operational Environment (from the Security Target)	**Definition of the Security Objective** (from the Security Target)	**Responsibility of the Administrators**
		components that responsibility is not covered by this document unless specifically document within. The operational environment components include the following: DNS Server for IP addressing, Fabric Interconnects (FI) for networking, Remote administration of the TOE using the HXCLI, this remote connection is secured with SSHv2, Remote administration of the TOE using the HX Connect GUI, this remote connection is secured with HTTPS, NTP for timestamp synchronization, Private Fiber from the network provider to to create the secure connection when the TOE is deployed in the Stretched Cluster configuration, Switches for traffic tracking, VMware vSphere for the virtual environment

7. Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

7.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

7.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in

the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com