Cisco HyperFlex 3.0 for Virtual Server Infrastructure with Microsoft Hyper-V

Deployment Guide for Cisco HyperFlex 3.0 for Virtual Server Infrastructure using Microsoft Hyper-V Hypervisor, Cisco UCS 6000 Fabric Interconnect, and Cisco HyperFlex Data Platform Software

Last Updated: December 18, 2018
About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, visit:


ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

(0809R)

© 2018 Cisco Systems, Inc. All rights reserved.
# Table of Contents

Executive Summary .................................................................................................................. 7

Solution Overview ....................................................................................................................... 8
  Introduction ................................................................................................................................. 8
  Audience .................................................................................................................................. 9
  Purpose of this Document ......................................................................................................... 9
  Solution Summary ..................................................................................................................... 9

Technology Overview ................................................................................................................ 11
  Cisco Unified Computing System ............................................................................................ 11
  Cisco UCS Fabric Interconnect ................................................................................................ 11
    Cisco UCS 6248UP Fabric Interconnect .................................................................................. 12
    Cisco UCS 6296UP Fabric Interconnect ................................................................................ 12
    Cisco UCS 6332 Fabric Interconnect ..................................................................................... 13
    Cisco UCS 6332–16UP Fabric Interconnect .......................................................................... 13
  Cisco HyperFlex HX–Series Nodes ......................................................................................... 13
    Cisco HyperFlex HXAF220c–M5SX All-Flash Node .............................................................. 13
    Cisco HyperFlex HXAF240c–M5SX All-Flash Node .............................................................. 14
    Cisco HyperFlex HX220c–M5SX Hybrid Node ..................................................................... 14
    Cisco HyperFlex HX240c–M5SX Hybrid Node ..................................................................... 14
    Cisco VIC 1387 MLOM Interface Cards .............................................................................. 15

All-Flash versus Hybrid ............................................................................................................. 15

Cisco HyperFlex Data Platform Software ............................................................................... 16
  Cisco HyperFlex Connect HTML5 Management Web Page .................................................. 17
  Cisco Intersight Cloud Based Management .......................................................................... 17
  Cisco HyperFlex HX Data Platform Controller ...................................................................... 18
  Data Operations and Distribution ............................................................................................. 18

Solution Design .......................................................................................................................... 22
  Requirements .............................................................................................................................. 22
    Physical Components ............................................................................................................... 22
    Software Components ............................................................................................................. 25
    Licensing ................................................................................................................................. 26

Considerations .............................................................................................................................. 26
  Version Control .......................................................................................................................... 26
  Microsoft Windows Active Directory ...................................................................................... 27
  Scale ....................................................................................................................................... 27
  Capacity .................................................................................................................................. 27

Physical Topology ....................................................................................................................... 29
  Topology Overview .................................................................................................................. 29
Assign a Static IP Address to the HX Data Platform Installer VM

---

Microsoft Hyper-V Host Design

---

Virtual Networking Design

---

Discrete Device Assignment (I/O Passthrough)

---

Storage Platform Controller VMs

---

Installation

---

Prerequisites

---

IP Addressing

---

Configure the Active Directory for Constrained Delegation

---

Prepopulate AD DNS with Records

---

NTP

---

VLANs

---

Network Uplinks

---

Usernames and Passwords

---

Physical Installation

---

Cabling

---

Cisco UCS Installation

---

Cisco UCS Fabric Interconnect A

---

Cisco UCS Fabric Interconnect B

---

Cisco UCS Manager

---

Cisco UCS Configuration

---

Cisco UCS Firmware

---

NTP

---

Uplink Ports

---

Uplink Port Channels

---

Server Ports

---

Server Discovery

---

Deploying HX Data Platform Installer on Hyper-V Infrastructure

---

Assign a Static IP Address to the HX Data Platform Installer VM
Appendix

HyperFlex Installation ........................................................................................................ 75
HyperFlex Installation - Phase 1 ......................................................................................... 76
HyperFlex Installation - Phase 2 ......................................................................................... 81
Post Installation Tasks ........................................................................................................ 90
Create Datastores ................................................................................................................ 90
Constrained Delegation (Optional) ...................................................................................... 91
Assign IP Addresses to Live Migration and VM Network Interfaces .................................. 94
Rename the Cluster Network in Windows Failover Cluster - Optional .............................. 95
Configure the Windows Failover Cluster Network Roles .................................................... 96
Configure the Windows Failover Cluster Network for Live Migration ............................... 97
Create Folders on the HX Datastore .................................................................................... 98
Configure the Default Folder to Store VM Files on Hyper-V ........................................... 98
Validate the Windows Failover Cluster Configuration ....................................................... 99
Configure Quorum in Windows Server Failover Cluster ..................................................... 100
Initial Tasks and Testing .................................................................................................... 101
Ready Clones ..................................................................................................................... 101
Auto-Support and Notifications ......................................................................................... 102
Smart Licensing .................................................................................................................. 104
Management ....................................................................................................................... 107
HyperFlex Connect ............................................................................................................. 107
Dashboard .......................................................................................................................... 108
Monitor .............................................................................................................................. 108
Analyze ............................................................................................................................... 109
Manage .............................................................................................................................. 109
Microsoft Hyper-V Manager ............................................................................................... 112
Change the Default Location to Store the VM Files using Hyper-V Manager .................. 113
Create Virtual Machines using Hyper-V Manager .............................................................. 114
Windows Failover Cluster Manager .................................................................................... 117
Microsoft System Center Virtual Machine Manager 2016 ................................................ 120
Create Run-As Account for Managing the Hyper-V Cluster .............................................. 120
Manage Servers and Clusters ............................................................................................. 120
Networking ........................................................................................................................ 123
Storage ............................................................................................................................... 124
Create a VM using SCVMM ............................................................................................... 126
Microsoft Windows Admin Center (WAC) ..................................................................... 131
Connecting to Managed Nodes and Clusters .................................................................. 132
Manage Servers with WAC ............................................................................................... 134
Manage a Failover Cluster with WAC .............................................................................. 135
Appendix ............................................................................................................................. 136
With the proliferation of virtualized environments across most IT landscapes, other technology stacks which have traditionally not offered the same levels of simplicity, flexibility, and rapid deployment as virtualized compute platforms have come under increasing scrutiny. In particular, networking devices and storage systems have lacked the agility of hypervisors and virtual servers. With the introduction of Cisco HyperFlex, Cisco has brought the dramatic enhancements of hyperconvergence to the modern data center.

Cisco HyperFlex systems are based on the Cisco UCS platform, combining Cisco HX-Series x86 servers and integrated networking technologies through the Cisco UCS Fabric Interconnects, into a single management domain, along with industry leading virtualization hypervisor software from Microsoft, and next-generation software defined storage technology. The combination creates a complete virtualization platform, which provides the network connectivity for the guest virtual machine (VM) connections, and the distributed storage to house the VMs, spread across all of the Cisco UCS x86 servers, versus using specialized storage or networking components. The unique storage features of the HyperFlex log based filesystem enable rapid cloning of VMs, snapshots without the traditional performance penalties, and data deduplication and compression. All configuration, deployment, management, and monitoring of the solution can be done with existing tools for Cisco UCS and Microsoft, such as Cisco UCS Manager and Microsoft Hyper-V Manager, PowerShell, SCVMM, and new integrated HTML based management tools, such as Cisco HyperFlex Connect and Cisco Intersight. This powerful linking of advanced technology stacks into a single, simple, rapidly deployed solution makes Cisco HyperFlex a true second generation hyperconverged platform.
Introduction

The Cisco HyperFlex System provides an all-purpose virtualized server platform, with hypervisor hosts, networking connectivity, and virtual server storage across a set of Cisco UCS HX-Series x86 rack-mount servers. Legacy datacenter deployments have relied on a disparate set of technologies, each performing a distinct and specialized function, such as network switches connecting endpoints and transferring Ethernet network traffic, and Fibre Channel (FC) storage arrays providing block-based storage via a dedicated storage array network (SAN). Each of these systems had unique requirements for hardware, connectivity, management tools, operational knowledge, monitoring, and ongoing support. A legacy virtual server environment was often divided up into areas commonly referred to as silos, within which only a single technology operated, along with their correlated software tools and support staff. Silos could often be divided between the x86 computing hardware, the networking connectivity of those x86 servers, SAN connectivity and storage device presentation, the hypervisors and virtual platform management, and finally the guest VM themselves along with their OS and applications. This model proves to be inflexible, difficult to navigate, and is susceptible to numerous operational inefficiencies.

A more modern datacenter model was developed called a converged infrastructure. Converged infrastructures attempt to collapse the traditional silos by combining these technologies into a more singular environment, which has been designed to operate together in pre-defined, tested, and validated designs. A key component of the converged infrastructure was the revolutionary combination of x86 rack and blade servers, along with converged Ethernet and Fibre Channel networking offered by the Cisco UCS platform. Converged infrastructures leverage Cisco UCS, plus new deployment tools, management software suites, automation processes, and orchestration tools to overcome the difficulties deploying traditional environments, and do so in a much more rapid fashion. These new tools place the ongoing management and operation of the system into the hands of fewer staff, with more rapid deployment of workloads based on business needs, while still remaining at the forefront of flexibility to adapt to workload needs, and offering the highest possible performance. Cisco has had incredible success in these areas with our various partners, developing leading solutions such as Cisco FlexPod, FlashStack, VersaStack, and VxBlock architectures. Despite these advances, because these converged infrastructures contained some legacy technology stacks, particularly in the storage subsystems, there often remained a division of responsibility amongst multiple teams of administrators. Alongside, there is also a recognition that these converged infrastructures can still be a somewhat complex combination of components, where a simpler system would suffice to serve the workloads being requested.

Significant changes in the storage marketplace have given rise to the software defined storage (SDS) system. Legacy FC storage arrays often contained a specialized subset of hardware, such as Fibre Channel Arbitrated Loop (FC-AL) based controllers and disk shelves along with optimized Application Specific Integrated Circuits (ASIC), read/write data caching modules and cards, plus highly customized software to operate the arrays. With the rise of Serial Attached SCSI (SAS) bus technology and its inherent benefits, storage array vendors began to transition their internal hardware architectures to SAS, and with dramatic increases in processing power from recent x86 processor architectures, they also used fewer or no custom ASICs at all. As disk physical sizes shrank, x86 servers began to have the same density of storage per rack unit (RU) as the arrays themselves, and with the proliferation of NAND based flash memory solid state disks (SSD), they also now had access to input/output (IO) devices whose speed rivaled that of dedicated caching devices. If servers themselves now contained storage devices and technology to rival many dedicated arrays on the market, then the major differentiator between them was the software providing allocation, presentation and management of the storage, plus the advanced features many vendors offered. This has led to the rise of software defined storage, where the x86 servers with the storage devices ran software to effectively turn one or more of them, working cooperatively, into a storage array much the same as the traditional arrays were. In a somewhat unexpected turn of events, some of the major storage array vendors themselves were pioneers in this field, recognizing the technological shifts in the market, and attempting to
profit from the software features they offered versus their specialized hardware, as had been done in the past.

Some early uses of SDS systems simply replaced the traditional storage array in the converged architectures as described earlier. That configuration still had a separate storage system from the virtual server hypervisor platform, and depending on the solution provider, still remained separate from the network devices. If the servers that hosted the VMs, and also provided the SDS environment were in fact the same model of server, could they simply do both things at once and collapse the two functions into one? This ultimate combination of resources becomes what the industry has given the moniker of a hyperconverged infrastructure. Hyperconverged infrastructures coalesce the computing, memory, hypervisor, and storage devices of servers into a single platform for virtual servers. There is no longer a separate storage system, as the servers running the hypervisors also provide the software defined storage resources to store the virtual servers, effectively storing the virtual machines on themselves. Now nearly all the silos are gone, and a hyperconverged infrastructure becomes something almost completely self-contained, simpler to use, faster to deploy, easier to consume, yet still flexible and with very high performance. Many hyperconverged systems still rely on standard networking components, such as on-board network cards in the x86 servers, and top-of-rack switches. The Cisco HyperFlex system combines the convergence of computing and networking provided by Cisco UCS, along with next-generation hyperconverged storage software, to uniquely provide the compute resources, network connectivity, storage, and hypervisor platform to run an entire virtual environment, all contained in a single uniform system.

Some key advantages of hyperconverged infrastructures are the simplification of deployment, day to day management operations, as well as increased agility, thereby reducing the amount operational costs. Since hyperconverged storage can be easily managed by an IT generalist, this can also reduce technical debt going forward that is often accrued by implementing complex systems that need dedicated management teams and skillsets.

Audience

The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers deploying the Cisco HyperFlex System. External references are provided wherever applicable, but readers are expected to be familiar with Microsoft specific technologies, infrastructure concepts, networking connectivity, and security policies of the customer installation.

Purpose of this Document

This document describes the steps required to deploy, configure, and manage a Cisco HyperFlex system using the Microsoft Hyper-V hypervisor. The document is based on all known best practices using the software, hardware and firmware revisions specified in the document. As such, recommendations and best practices can be amended with later versions. This document showcases the installation and configuration of Cisco HyperFlex with Hyper-V in a typical customer datacenter environment. While readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are important to the deployment of this solution are provided in this CVD.

Solution Summary

The Cisco HyperFlex system provides a fully contained virtual server platform, with compute and memory resources, integrated networking connectivity, a distributed high-performance log based filesystem for VM storage, and the hypervisor software for running the virtualized servers, all within a single Cisco UCS management domain.
The following are the components of a Cisco HyperFlex system using Microsoft Hyper-V as the hypervisor:

- One pair of Cisco UCS Fabric Interconnects, choose from models:
  - Cisco UCS 6248UP Fabric Interconnect
  - Cisco UCS 6296UP Fabric Interconnect
  - Cisco UCS 6332 Fabric Interconnect
  - Cisco UCS 6332-16UP Fabric Interconnect

- Three to Eight Cisco HyperFlex HX-Series Rack-Mount Servers, choose from models:
  - Cisco HyperFlex HX220c-M5SX Rack-Mount Servers
  - Cisco HyperFlex HX240c-M5SX Rack-Mount Servers
  - Cisco HyperFlex HXAF220c-M5SX All-Flash Rack-Mount Servers
  - Cisco HyperFlex HXAF240c-M5SX All-Flash Rack-Mount Servers

- Cisco HyperFlex Data Platform Software
- Microsoft Windows Server 2016 Hyper-V Hypervisor
- Microsoft Windows Active Directory and DNS services, RSAT tools (end-user supplied)
- SCVMM – optional (end-user supplied)
Cisco Unified Computing System

The Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that unites compute, network, and storage access. The platform, optimized for virtual environments, is designed using open industry-standard technologies and aims to reduce total cost of ownership (TCO) and increase business agility. The system integrates a low-latency, lossless 10 Gigabit Ethernet or 40 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. It is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain.

The main components of Cisco Unified Computing System are:

- **Computing**: The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers based on Intel Xeon Processors.
- **Network**: The system is integrated onto a low-latency, lossless, 10-Gbps or 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks which are often separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- **Virtualization**: The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access**: The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying storage access, the Cisco Unified Computing System can access storage over Ethernet, Fibre Channel, Fibre Channel over Ethernet (FCoE), and iSCSI. This provides customers with their choice of storage protocol and physical architecture, and enhanced investment protection. In addition, the server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity, and management for increased productivity.
- **Management**: The system uniquely integrates all system components which enable the entire solution to be managed as a single entity by the Cisco UCS Manager (UCSM). The Cisco UCS Manager has an intuitive graphical user interface (GUI), a command-line interface (CLI), and a robust application programming interface (API) to manage all system configuration and operations.

The Cisco Unified Computing System is designed to deliver:

- A reduced Total Cost of Ownership and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.
- A cohesive, integrated system which unifies the technology in the data center. The system is managed, serviced and tested as a whole.
- Scalability through a design for hundreds of discrete servers and thousands of virtual machines and the capability to scale I/O bandwidth to match demand.
- Industry standards supported by a partner ecosystem of industry leaders.

Cisco UCS Fabric Interconnect

The Cisco UCS Fabric Interconnect (FI) is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. Depending on the model chosen, the Cisco UCS Fabric Interconnect offers line-rate, low-latency, lossless 10 Gigabit or 40 Gigabit Ethernet, Fibre
Technology Overview

Channel over Ethernet (FCoE) and Fibre Channel connectivity. Cisco UCS Fabric Interconnects provide the management and communication backbone for the Cisco UCS C-Series, S-Series and HX-Series Rack-Mount Servers, Cisco UCS B-Series Blade Servers and Cisco UCS 5100 Series Blade Server Chassis. All servers and chassis, and therefore all blades, attached to the Cisco UCS Fabric Interconnects become part of a single, highly available management domain. In addition, by supporting unified fabrics, the Cisco UCS Fabric Interconnects provide both the LAN and SAN connectivity for all servers within its domain.

From a networking perspective, the Cisco UCS 6200 Series uses a cut-through architecture, supporting deterministic, low latency, line rate 10 Gigabit Ethernet on all ports, up to 1.92 Tbps switching capacity and 160 Gbps bandwidth per chassis, independent of packet size and enabled services. The product family supports Cisco low-latency, lossless 10 Gigabit Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over the Ethernet fabric from the servers to the uplinks. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

The Cisco UCS 6300 Series offers the same features while supporting even higher performance, low latency, lossless, line rate 40 Gigabit Ethernet, with up to 2.56 Tbps of switching capacity. Backward compatibility and scalability are assured with the ability to configure 40 Gbps quad SFP (QSFP) ports as breakout ports using 4x10GbE breakout cables. Existing Cisco UCS servers with 10GbE interfaces can be connected in this manner, although Cisco HyperFlex nodes must use a 40GbE VIC adapter in order to connect to a Cisco UCS 6300 Series Fabric Interconnect.

Cisco UCS 6248UP Fabric Interconnect

The Cisco UCS 6248UP Fabric Interconnect is a one-rack-unit (1RU) 10 Gigabit Ethernet, FCoE and Fiber Channel switch offering up to 960 Gbps throughput and up to 48 ports. The switch has 32 1/10-Gbps fixed Ethernet, FCoE, or 1/2/4/8 Gbps FC ports, plus one expansion slot.

Figure 2 Cisco UCS 6248UP Fabric Interconnect

Cisco UCS 6296UP Fabric Interconnect

The Cisco UCS 6296UP Fabric Interconnect is a two-rack-unit (2RU) 10 Gigabit Ethernet, FCoE, and native Fibre Channel switch offering up to 1920 Gbps of throughput and up to 96 ports. The switch has 48 1/10-Gbps fixed Ethernet, FCoE, or 1/2/4/8 Gbps FC ports, plus three expansion slots.

Figure 3 Cisco UCS 6296UP Fabric Interconnect
Technology Overview

Cisco UCS 6332 Fabric Interconnect

The Cisco UCS 6332 Fabric Interconnect is a one-rack-unit (1RU) 40 Gigabit Ethernet and FCoE switch offering up to 2560 Gbps of throughput. The switch has 32 40-Gbps fixed Ethernet and FCoE ports. Up to 24 of the ports can be reconfigured as 4x10Gbps breakout ports, providing up to 96 10-Gbps ports.

Figure 4 Cisco UCS 6332 Fabric Interconnect

Cisco UCS 6332-16UP Fabric Interconnect

The Cisco UCS 6332-16UP Fabric Interconnect is a one-rack-unit (1RU) 10/40 Gigabit Ethernet, FCoE, and native Fibre Channel switch offering up to 2430 Gbps of throughput. The switch has 24 40-Gbps fixed Ethernet and FCoE ports, plus 16 1/10-Gbps fixed Ethernet, FCoE, or 4/8/16 Gbps FC ports. Up to 18 of the 40-Gbps ports can be reconfigured as 4x10Gbps breakout ports, providing up to 88 total 10-Gbps ports.

Figure 5 Cisco UCS 6332-16UP Fabric Interconnect

When used for a Cisco HyperFlex deployment, due to mandatory QoS settings in the configuration, the 6332 and 6332-16UP will be limited to a maximum of four 4x10Gbps breakout ports, which can be used for other non-HyperFlex servers.

Cisco HyperFlex HX-Series Nodes

A HyperFlex cluster requires a minimum of three HX-Series “converged” nodes (with disk storage). Data is replicated across at least two of these nodes, and a third node is required for continuous operation in the event of a single-node failure. Each node that has disk storage is equipped with at least one high-performance SSD drive for data caching and rapid acknowledgment of write requests. Each node also is equipped with additional disks, up to the platform’s physical limit, for long term storage and capacity.

In the below listed Cisco UCS HX server models, SED and NVMe cache drives are not supported on HyperFlex systems with Microsoft Hyper-V at the time of publishing this document.

Cisco HyperFlex HXAF220c-M5SX All-Flash Node

This small footprint Cisco HyperFlex 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 960 GB or 3.8 TB SATA SSD drives for storage capacity. For configurations requiring self-encrypting drives, the caching SSD is replaced with an 800 GB SAS SED SSD, and the capacity disks are also replaced with either 800 GB, 960 GB or 3.8 TB SED SSDs.
Technology Overview

Figure 6 HXAF220c-M5SX All-Flash Node

Cisco HyperFlex HXAF240c-M5SX All-Flash Node

This capacity optimized Cisco HyperFlex 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. For configurations requiring self-encrypting drives, the caching SSD is replaced with an 800 GB SAS SED SSD, and the capacity disks are also replaced with either 800 GB, 960 GB or 3.8 TB SED SSDs.

Figure 7 HXAF240c-M5SX Node

Cisco HyperFlex HX220c-M5SX Hybrid Node

This small footprint Cisco HyperFlex 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. For configurations requiring self-encrypting drives, the caching SSD is replaced with a 1.6 TB SAS SED SSD, and the capacity disks are replaced with 1.2TB SAS SED HDDs.

Figure 8 HX220c-M5SX Node

Cisco HyperFlex HX240c-M5SX Hybrid Node

This capacity optimized Cisco HyperFlex hybrid model contains a minimum of six and up to twenty-three 1.8 TB or 1.2 TB SAS small form factor (SFF) hard disk 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. For configurations requiring self-encrypting drives, the caching SSD is replaced with a 1.6 TB SAS SED SSD, and the capacity disks are replaced with 1.2TB SAS SED HDDs.
Cisco VIC 1387 mLOM Interface Cards

The Cisco UCS VIC 1387 Card is a dual-port Enhanced Quad Small Form-Factor Pluggable (QSFP+) 40-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter installed in the Cisco UCS HX-Series Rack Servers. The VIC 1387 is used in conjunction with the Cisco UCS 6332 or 6332-16UP model Fabric Interconnects.

The mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases. The card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host, each dynamically configured as either a network interface card (NICs) or host bus adapter (HBA). The personality of the interfaces is set programmatically using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, adapter settings, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all specified using the service profile.

All-Flash versus Hybrid

The initial HyperFlex product release featured hybrid converged nodes, which use a combination of solid-state disks (SSDs) for the short-term storage caching layer, and hard disk drives (HDDs) for the long-term storage capacity layer. The hybrid HyperFlex system is an excellent choice for entry-level or midrange storage solutions, and hybrid solutions have been successfully deployed in many non-performance sensitive virtual environments. Meanwhile, there is significant growth in deployment of highly performance sensitive and mission critical applications. The primary challenge to the hybrid HyperFlex system from these highly performance sensitive applications, is their increased sensitivity to high storage latency. Due to the characteristics of the spinning hard disks, it is unavoidable that their higher latency becomes the bottleneck in the hybrid system. Ideally, if all of the storage operations were to occur in the caching SSD layer, the hybrid system’s performance will be excellent. But in several scenarios, the amount of data being written and
read exceeds the caching layer capacity, placing larger loads on the HDD capacity layer, and the subsequent increases in latency will naturally result in reduced performance.

Cisco All-Flash HyperFlex systems are an excellent option for customers with a requirement to support high performance, latency sensitive workloads. With a purpose built, flash-optimized and high-performance log based filesystem, the Cisco All-Flash HyperFlex system provides:

- Predictable high-performance across all the virtual machines on HyperFlex All-Flash.
- Highly consistent and low latency, which benefits data-intensive applications and databases such as Microsoft SQL and Oracle.
- Future ready architecture that is well suited for flash-memory configuration:
  - Cluster-wide SSD pooling maximizes performance and balances SSD usage so as to spread the wear.
  - A fully distributed log-structured filesystem optimizes the data path to help reduce write amplification.
  - Large sequential writing reduces flash wear and increases component longevity.
  - Inline space optimization, for example; deduplication and compression, minimizes data operations and reduces wear.
- Lower operating cost with the higher density drives for increased capacity of the system.
- Cloud scale solution with easy scale-out and distributed infrastructure and the flexibility of scaling out independent resources separately.

Cisco HyperFlex support for hybrid and all-flash models now allows customers to choose the right platform configuration based on their capacity, applications, performance, and budget requirements. All-flash configurations offer repeatable and sustainable high performance, especially for scenarios with a larger working set of data, in other words, a large amount of data in motion. Hybrid configurations are a good option for customers who want the simplicity of the Cisco HyperFlex solution, but their needs focus on capacity-sensitive solutions, lower budgets, and fewer performance-sensitive applications.

Cisco HyperFlex Data Platform Software

The Cisco HyperFlex HX Data Platform is a purpose-built, high-performance, distributed file system with a wide array of enterprise-class data management services. The data platform’s innovations redefine distributed storage technology, exceeding the boundaries of first-generation hyperconverged infrastructures. The data platform has all the features expected in an enterprise shared storage system, eliminating the need to configure and maintain complex Fibre Channel storage networks and devices. The platform simplifies operations and helps ensure data availability. Enterprise-class storage features include the following:

- **Data protection** creates multiple copies of the data across the cluster so that data availability is not affected if single or multiple components fail (depending on the replication factor configured).
- **Deduplication** is always on, helping reduce storage requirements in virtualization clusters in which multiple operating system instances in guest virtual machines result in large amounts of replicated data.
- **Compression** further reduces storage requirements, reducing costs, and the log-structured file system is designed to store variable-sized blocks, reducing internal fragmentation.
- **Thin provisioning** allows large volumes to be created without requiring storage to support them until the need arises, simplifying data volume growth and making storage a “pay as you grow” proposition.
Technology Overview

- **Fast, space-efficient clones** rapidly duplicate virtual storage volumes so that virtual machines can be cloned simply through metadata operations, with actual data copied only for write operations.

Cisco HyperFlex Connect HTML5 Management Web Page

An all-new HTML 5 based Web UI is available for use as the primary management tool for Cisco HyperFlex. Through this centralized point of control for the cluster, administrators can create volumes, monitor the data platform health, and manage resource use. Administrators can also use this data to predict when the cluster will need to be scaled. To use the HyperFlex Connect UI, connect using a web browser to the HyperFlex cluster IP address: http://<hx controller cluster ip>.

Figure 11  HyperFlex Connect GUI

![HyperFlex Connect GUI](image)

Cisco Intersight Cloud Based Management

Cisco Intersight ([https://intersight.com](https://intersight.com)), previously known as Starship, is the latest visionary cloud-based management tool, designed to provide a centralized off-site management, monitoring and reporting tool for all of your Cisco UCS based solutions. In the initial release of Cisco Intersight, monitoring and reporting is enabled against Cisco HyperFlex clusters. The Cisco Intersight website and framework can be upgraded with new and enhanced features independently of the products that are managed, meaning that many new
features and capabilities can come with no downtime or upgrades required by the end users. Future releases of Cisco HyperFlex will enable further functionality along with these upgrades to the Cisco Intersight framework. This unique combination of embedded and online technologies will result in a complete cloud-based management solution that can care for Cisco HyperFlex throughout the entire lifecycle, from deployment through retirement.

Figure 12  Cisco Intersight

Cisco HyperFlex HX Data Platform Controller

A Cisco HyperFlex HX Data Platform controller resides on each node and implements the distributed file system. The controller runs as software in user space within a virtual machine, and intercepts and handles all I/O from the guest virtual machines. The Storage Controller Virtual Machine (SCVM) uses the new Microsoft Hyper-V discrete device assignment (DDA) feature to provide PCI pass-through control of the physical server’s SAS disk controller. This method gives the controller VM full control of the physical disk resources, utilizing the SSD drives as a read/write caching layer, and the HDDs or SDDs as a capacity layer for distributed storage. The controller exposes the distributed storage as SMB share to each node Hyper-V node.

Data Operations and Distribution

The Cisco HyperFlex HX Data Platform controllers handle all read and write operation requests from the guest VMs to their virtual disks (VHD/VHDX) stored in the distributed datastores in the cluster. The data platform distributes the data across multiple nodes of the cluster, and also across multiple capacity disks of each node, according to the replication level policy selected during the cluster setup. This method avoids storage hotspots on specific nodes, and on specific disks of the nodes, and thereby also avoids networking hotspots or congestion from accessing more data on some nodes versus others.

Replication Factor

The policy for the number of duplicate copies of each storage block is chosen during cluster setup, and is referred to as the replication factor (RF).
Technology Overview

- **Replication Factor 3:** For every I/O write committed to the storage layer, 2 additional copies of the blocks written will be created and stored in separate locations, for a total of 3 copies of the blocks. Blocks are distributed in such a way as to ensure multiple copies of the blocks are not stored on the same disks, nor on the same nodes of the cluster. This setting can tolerate simultaneous failures of 2 entire nodes in a cluster of 5 nodes or greater, without losing data and resorting to restore from backup or other recovery processes. RF3 is recommended for all production systems.

- **Replication Factor 2:** For every I/O write committed to the storage layer, 1 additional copy of the blocks written will be created and stored in separate locations, for a total of 2 copies of the blocks. Blocks are distributed in such a way as to ensure multiple copies of the blocks are not stored on the same disks, nor on the same nodes of the cluster. This setting can tolerate a failure of 1 entire node without losing data and resorting to restore from backup or other recovery processes. RF2 is suitable for non-production systems, or environments where the extra data protection is not needed.

Data Write and Compression Operations

Internally, the contents of each virtual disk are subdivided and spread across multiple servers by the HXDP software. For each write operation, the data is intercepted by the IO Visor module on the node where the VM is running, a primary node is determined for that particular operation via a hashing algorithm, and then sent to the primary node via the network. The primary node compresses the data in real time, writes the compressed data to its caching SSD, and replica copies of that compressed data are written to the caching SSD of the remote nodes in the cluster, according to the replication factor setting. For example, at RF=3 a write will be written to the primary node for that virtual disk address, and two additional writes will be committed in parallel on two other nodes. Because the virtual disk contents have been divided and spread out via the hashing algorithm, this method results in all writes being spread across all nodes, avoiding the problems with data locality and “noisy” VMs consuming all the IO capacity of a single node. The write operation will not be acknowledged until all three copies are written to the caching layer SSDs. Written data is also cached in a write log area resident in memory in the controller VM, along with the write log on the caching SSDs. This process speeds up read requests when reads are requested of data that has recently been written.

Data Destaging and Deduplication

The Cisco HyperFlex HX Data Platform constructs multiple write caching segments on the caching SSDs of each node in the distributed cluster. As write cache segments become full, and based on policies accounting for I/O load and access patterns, those write cache segments are locked and new writes roll over to a new write cache segment. The data in the now locked cache segment is destaged to the HDD capacity layer of the nodes for the Hybrid system or to the SSD capacity layer of the nodes for the All-Flash system. During the destaging process, data is deduplicated before being written to the capacity storage layer, and the resulting data can now be written to the HDDs or SDDs of the server. On hybrid systems, the now deduplicated and compressed data is also written to the dedicated read cache area of the caching SSD, which speeds up read requests of data that has recently been written. When the data is destaged to a HDD, it is written in a single sequential operation, avoiding disk head seek thrashing on the spinning disks and accomplishing the task in the minimal amount of time. Since the data is already deduplicated and compressed before being written, the platform avoids additional I/O overhead often seen on competing systems, which must later do a read/dedupe/compress/write cycle. Deduplication, compression and destaging take place with no delays or I/O penalties to the guest VMs making requests to read or write data, which benefits both the HDD and SDD configurations.
For data read operations, data may be read from multiple locations. For data that was very recently written, the data is likely to still exist in the write log of the local platform controller memory, or the write log of the local caching layer disk. If local write logs do not contain the data, the distributed filesystem metadata will be queried to see if the data is cached elsewhere, either in write logs of remote nodes, or in the dedicated read cache area of the local and remote caching SSDs of hybrid nodes. Finally, if the data has not been accessed in a significant amount of time, the filesystem will retrieve the requested data from the distributed capacity layer. As requests for reads are made to the distributed filesystem and the data is retrieved from the capacity layer, the caching SSDs of hybrid nodes populate their dedicated read cache area to speed up subsequent requests for the same data. This multi-tiered distributed system with several layers of caching techniques, ensures that data is served at the highest possible speed, leveraging the caching SSDs of the nodes fully and equally. All-flash configurations, however, do not employ a dedicated read cache because such caching does not provide any performance benefit; the persistent data copy already resides on high-performance SSDs.
In summary, the Cisco HyperFlex HX Data Platform implements a distributed, log-structured file system that performs data operations via two configurations:

- In a Hybrid configuration, the data platform provides a caching layer using SSDs to accelerate read requests and write responses, and it implements a storage capacity layer using HDDs.
- In an All-Flash configuration, the data platform provides a dedicated caching layer using high endurance SSDs to accelerate write responses, and it implements a storage capacity layer also using SSDs. Read requests are fulfilled directly from the capacity SSDs, as a dedicated read cache is not needed to accelerate read operations.
Requirements

The following sections detail the physical hardware, software revisions, and firmware versions required to install a single cluster of the Cisco HyperFlex system. A maximum of 8 converged nodes are supported on Cisco HyperFlex with Microsoft Hyper-V.

Physical Components

Table 1  HyperFlex System Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Interconnects</td>
<td>Two Cisco UCS 6248UP Fabric Interconnects, or</td>
</tr>
<tr>
<td></td>
<td>Two Cisco UCS 6296UP Fabric Interconnects, or</td>
</tr>
<tr>
<td></td>
<td>Two Cisco UCS 6332 Fabric Interconnects, or</td>
</tr>
<tr>
<td></td>
<td>Two Cisco UCS 6332-16UP Fabric Interconnects</td>
</tr>
<tr>
<td>Servers</td>
<td>Three to Eight Cisco HyperFlex HXAF220c-M5SX All-Flash rack servers, or</td>
</tr>
<tr>
<td></td>
<td>Three to Eight Cisco HyperFlex HXAF240c-M5SX All-Flash rack servers, or</td>
</tr>
<tr>
<td></td>
<td>Three to Eight Cisco HyperFlex HX220c-M5SX Hybrid rack servers, or</td>
</tr>
<tr>
<td></td>
<td>Three to Eight Cisco HyperFlex HX240c-M5SX Hybrid rack servers,</td>
</tr>
</tbody>
</table>

For complete server specifications and more information, please refer to the links below:

Compare Models:


HXAF220c-M5SX Spec Sheet:


HXAF240c-M5SX Spec Sheet:


HX220c-M5SX Spec Sheet:


HX240c-M5SX Spec Sheet:

Table 2 lists the hardware component options for the HXAF220c-M5SX server model.

<table>
<thead>
<tr>
<th>HXAF220c-M5SX Options</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Chose a matching pair of Intel Xeon Processor Scalable Family CPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>192 GB to 3 TB of total memory using 16 GB, 32 GB, 64 GB, or 128 GB DDR4 2666 MHz 1.2v modules</td>
</tr>
<tr>
<td>Disk Controller</td>
<td>Cisco 12Gbps Modular SAS HBA</td>
</tr>
<tr>
<td>SSDs</td>
<td>One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD</td>
</tr>
<tr>
<td></td>
<td>One 400 GB 2.5 Inch Enterprise Performance 12G SAS SSD</td>
</tr>
<tr>
<td></td>
<td>Six to eight 3.8 TB 2.5 Inch Enterprise Value 6G SATA SSDs, or six to eight 960 GB 2.5 Inch Enterprise Value 6G SATA SSDs</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco UCS VIC1387 VIC MLOM</td>
</tr>
<tr>
<td>Boot Device</td>
<td>One 240 GB M.2 form factor SATA SSD</td>
</tr>
<tr>
<td>microSD Card</td>
<td>One 32GB microSD card for local host utilities storage</td>
</tr>
<tr>
<td>Optional</td>
<td>Cisco QSA module to convert 40 GbE QSFP+ to 10 GbE SFP+</td>
</tr>
</tbody>
</table>

Table 3 lists the hardware component options for the HXAF240c-M5SX server model.

<table>
<thead>
<tr>
<th>HXAF240c-M5SX Options</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Chose a matching pair of Intel Xeon Processor Scalable Family CPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>192 GB to 3 TB of total memory using 16 GB, 32 GB, 64 GB, or 128 GB DDR4 2666 MHz 1.2v modules</td>
</tr>
<tr>
<td>Disk Controller</td>
<td>Cisco 12Gbps Modular SAS HBA</td>
</tr>
<tr>
<td>SSDs</td>
<td>One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD</td>
</tr>
<tr>
<td></td>
<td>One 400 GB 2.5 Inch Enterprise Performance 12G SAS SSD</td>
</tr>
<tr>
<td></td>
<td>Six to twenty-three 3.8 TB 2.5 Inch Enterprise Value 6G SATA SSDs, or six to twenty-three 960 GB 2.5 Inch Enterprise Value 6G SATA SSDs</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco UCS VIC1387 VIC MLOM</td>
</tr>
<tr>
<td>Boot Device</td>
<td>One 240 GB M.2 form factor SATA SSD</td>
</tr>
</tbody>
</table>
### Solution Design

<table>
<thead>
<tr>
<th>HXAF240c-M5SX Options</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>microSD Card</td>
<td>One 32GB microSD card for local host utilities storage</td>
</tr>
<tr>
<td>Optional</td>
<td>Cisco QSA module to convert 40 GbE QSFP+ to 10 GbE SFP+</td>
</tr>
</tbody>
</table>

Table 4 lists the hardware component options for the HX220c-M5SX server model.

<table>
<thead>
<tr>
<th>HX220c-M5SX Options</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Chose a matching pair of Intel Xeon Processor Scalable Family CPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>192 GB to 3 TB of total memory using 16 GB, 32 GB, 64 GB, or 128 GB DDR4 2666 MHz 1.2v modules</td>
</tr>
<tr>
<td>Disk Controller</td>
<td>Cisco 12Gbps Modular SAS HBA</td>
</tr>
<tr>
<td>SSDs</td>
<td>One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD</td>
</tr>
<tr>
<td></td>
<td>One 480 GB 2.5 Inch Enterprise Performance 6G SATA SSD, or one 800 GB 2.5 Inch Enterprise Performance 12G SAS SSD</td>
</tr>
<tr>
<td>HDDs</td>
<td>Six to eight 1.8 TB or 1.2 TB SAS 12Gbps 10K rpm SFF HDD</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco UCS VIC1387 VIC MLOM</td>
</tr>
<tr>
<td>Boot Device</td>
<td>One 240 GB M.2 form factor SATA SSD</td>
</tr>
<tr>
<td>microSD Card</td>
<td>One 32GB microSD card for local host utilities storage</td>
</tr>
<tr>
<td>Optional</td>
<td>Cisco QSA module to convert 40 GbE QSFP+ to 10 GbE SFP+</td>
</tr>
</tbody>
</table>

Table 5 lists the hardware component options for the HX240c-M5SX server model.

<table>
<thead>
<tr>
<th>HX240c-M5SX Options</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Chose a matching pair of Intel Xeon Processor Scalable Family CPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>192 GB to 3 TB of total memory using 16 GB, 32 GB, 64 GB, or 128 GB DDR4 2666 MHz 1.2v modules</td>
</tr>
<tr>
<td>Disk Controller</td>
<td>Cisco 12Gbps Modular SAS HBA</td>
</tr>
<tr>
<td>SSDs</td>
<td>One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD</td>
</tr>
</tbody>
</table>
## Solution Design

### HX240c-M5SX Options

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>One 1.6 TB 2.5 Inch Enterprise Performance 12G SAS SSD</td>
<td></td>
</tr>
</tbody>
</table>

### HDDs Standard

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Six to twenty-three 1.8 TB or 1.2 TB SAS 12Gbps 10K rpm SFF HDD</td>
<td></td>
</tr>
</tbody>
</table>

### Network

CISCO UCS VIC1387 VIC MLOM

### Boot Device

One 240 GB M.2 form factor SATA SSD

### microSD Card

One 32GB microSD card for local host utilities storage

### Optional

Cisco QSA module to convert 40 GbE QSFP+ to 10 GbE SFP+

## Software Components

Table 6 lists the software components and the versions required for the Cisco HyperFlex system for Microsoft Hyper-V.

### Table 6: Software Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Software Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>Hyper-V - Microsoft Windows Server 2016 Datacenter</td>
</tr>
<tr>
<td></td>
<td>Note: Microsoft Windows Server with Hyper-V will NOT be installed in Cisco Factory. Customers need to bring their own Windows Server ISO image that needs to be installed at deployment site</td>
</tr>
<tr>
<td>Active Directory</td>
<td>A Windows 2012 or later domain and forest functionality level with AD integrated DNS server.</td>
</tr>
<tr>
<td>Management Server</td>
<td>Windows 10 or Windows Server 2016 with PowerShell and RSAT tools installed. System Center VMM 2016 (optional) Windows Admin Center (Optional)</td>
</tr>
<tr>
<td>Cisco HyperFlex Data Platform</td>
<td>Cisco HyperFlex HX Data Platform Installer for Microsoft Hyper-V 3.0(1c) - Cisco-HX-Data-Platform-Installer-v3.0.1c-29681-hyperv.vhdx.zip</td>
</tr>
<tr>
<td>Microsoft Windows Server 2016 System Preparation Script</td>
<td>Cisco HyperFlex Data Platform System Preparation Script for Microsoft Windows Server 2016 with Cisco Drivers - HXInstall-HyperV-DatacenterCore-v3.0.1c-29681.img, or Cisco HyperFlex Data Platform System Preparation Script for Microsoft Windows Server 2016 Desktop Experience with Cisco Drivers - HXInstall-HyperV-DatacenterDE-v3.0.1c-29681.img</td>
</tr>
<tr>
<td>Ready Clone PowerShell Script</td>
<td>Cisco HyperFlex Data Platform Hyper-V ReadyClone PowerShell Script HxClone-HyperV-v3.0.1c-29681.ps1</td>
</tr>
</tbody>
</table>
Solution Design

<table>
<thead>
<tr>
<th>Component</th>
<th>Software Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Firmware</td>
<td>Cisco UCS Infrastructure software, Cisco UCS B-Series and C-Series bundles, revision 3.2(3g) or later.</td>
</tr>
</tbody>
</table>

Licensing

Cisco HyperFlex systems must be properly licensed using Cisco Smart Licensing, which is a cloud-based software licensing management solution used to automate many manual, time consuming and error prone licensing tasks. Cisco HyperFlex 2.5 and later communicate with the Cisco Smart Software Manager (CSSM) online service via a Cisco Smart Account, to check out or assign available licenses from the account to the Cisco HyperFlex cluster resources. Communications can be direct via the internet, they can be configured to communicate via a proxy server, or they can communicate with an internal Cisco Smart Software Manager satellite server, which caches and periodically synchronizes licensing data. In a small number of highly secure environments, systems can be provisioned with a Permanent License Reservation (PLR) which does not need to communicate with CSSM. Contact your Cisco sales representative or partner to discuss if your security requirements will necessitate use of these permanent licenses. New HyperFlex cluster installations will operate for 90 days without licensing as an evaluation period, thereafter the system will generate alarms and operate in a non-compliant mode. Systems without compliant licensing will not be entitled to technical support.

For more information about the Cisco Smart Software Manager satellite server, see: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

Beginning with Cisco HyperFlex 3.0, licensing of the system requires one license per node - Standard license.

Table 7 lists the licensing editions and the features available with each type of license.

Table 7  HyperFlex System License Editions

<table>
<thead>
<tr>
<th>HyperFlex Licensing Edition</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features Available</td>
<td>8 Converged Nodes standard cluster with Fabric Interconnects (Compute-only nodes not supported)</td>
</tr>
<tr>
<td></td>
<td>All Cisco UCS M5 with SFF server models</td>
</tr>
<tr>
<td></td>
<td>Replication Factor 3</td>
</tr>
<tr>
<td></td>
<td>10 GbE or 40 GbE Ethernet</td>
</tr>
</tbody>
</table>

Considerations

Version Control

The software revisions listed in Table 6 are the only valid and supported configuration at the time of the publishing of this validated design. Special care must be taken not to alter the revision of the hypervisor, vCenter server, Cisco HX platform software, or the Cisco UCS firmware without first consulting the appropriate release notes and compatibility matrixes to ensure that the system is not being modified into an unsupported configuration.
Microsoft Windows Active Directory

The Microsoft Windows Active Directory 2012 or later is required due to the requirement Cisco HyperFlex for Microsoft Hyper-V. The Active Directory with integrated DNS server must be installed and operational prior to the installation of the Cisco HyperFlex HX Data Platform software.

This document does not cover the installation and configuration of Microsoft Windows Active Directory and DNS server.

Scale

Cisco HyperFlex for Microsoft Hyper-V standard clusters currently scale from a minimum of 3 to a maximum of 8 Cisco HX-series converged nodes with small form factor (SFF) disks per cluster. A converged node is a member of the cluster which provides storage resources to the HX Distributed Filesystem. Once the maximum size of a single cluster has been reached, the environment can be “scaled out” by adding additional HX model servers to the Cisco UCS domain, installing an additional HyperFlex cluster on them, and controlling them via the same management host with PowerShell and RSAT tools installed.

At the time of the publication of this document, Cisco HyperFlex for Microsoft Hyper-V does not support the following: Adding compute-only nodes to a cluster or expanding an existing cluster and Cisco UCS M4 server models and LFF disks are not supported.

Table 8 lists the minimum and maximum scale for various installations of the Cisco HyperFlex system with Microsoft Hyper-V:

<table>
<thead>
<tr>
<th>Cluster Type</th>
<th>Minimum Converged Nodes Required</th>
<th>Maximum Converged Nodes Allowed</th>
<th>Maximum Compute-only Nodes Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard with SFF disks</td>
<td>3</td>
<td>8</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

Capacity

Overall usable cluster capacity is based on a number of factors. The number of nodes in the cluster, the number and size of the capacity layer disks, and the replication factor of the HyperFlex HX Data Platform, all affect the cluster capacity.

Disk drive manufacturers have adopted a size reporting methodology using calculation by powers of 10, also known as decimal prefix. As an example, a 120 GB disk is listed with a minimum of 120 x 10^9 bytes of usable addressable capacity, or 120 billion bytes. However, many operating systems and filesystems report their space based on standard computer binary exponentiation, or calculation by powers of 2, also called binary prefix. In this example, 2^10 or 1024 bytes make up a kilobyte, 2^10 kilobytes make up a megabyte, 2^10 megabytes make up a gigabyte, and 2^10 gigabytes make up a terabyte. As the values increase, the disparity between the two systems of measurement and notation get worse, at the terabyte level, the deviation between a decimal prefix value and a binary prefix value is nearly 10 percent.

The International System of Units (SI) defines values and decimal prefix by powers of 10 as follows:
### Table 9  SI Unit Values (Decimal Prefix)

<table>
<thead>
<tr>
<th>Value</th>
<th>Symbol</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 bytes</td>
<td>kB</td>
<td>Kilobyte</td>
</tr>
<tr>
<td>1000 kB</td>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>1000 MB</td>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>1000 GB</td>
<td>TB</td>
<td>Terabyte</td>
</tr>
</tbody>
</table>

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) defines values and binary prefix by powers of 2 in ISO/IEC 80000-13:2008 Clause 4 listed in Table 10

### Table 10  IEC Unit Values (binary prefix)

<table>
<thead>
<tr>
<th>Value</th>
<th>Symbol</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024 bytes</td>
<td>KiB</td>
<td>Kibibyte</td>
</tr>
<tr>
<td>1024 KiB</td>
<td>MiB</td>
<td>Mebibyte</td>
</tr>
<tr>
<td>1024 MiB</td>
<td>GiB</td>
<td>Gibibyte</td>
</tr>
<tr>
<td>1024 GiB</td>
<td>TiB</td>
<td>Tebibyte</td>
</tr>
</tbody>
</table>

For the purpose of this document, the decimal prefix numbers are used only for raw disk capacity as listed by the respective manufacturers. For all calculations where raw or usable capacities are shown from the perspective of the HyperFlex software, filesystems or operating systems, the binary prefix numbers are used. This is done primarily to show a consistent set of values as seen by the end user from within the HyperFlex Connect GUI when viewing cluster capacity, allocation and consumption, and also within most operating systems.

Table 11 lists a set of HyperFlex HX Data Platform cluster usable capacity values, using binary prefix, for an array of cluster configurations. These values provide an example of the capacity calculations, for determining the appropriate size of HX cluster to initially purchase, and how much capacity can be gained by adding capacity disks. The calculations for these values are listed in Appendix A: Cluster Capacity Calculations.

### Table 11  Cluster Usable Capacities

<table>
<thead>
<tr>
<th>HX-Series Server Model</th>
<th>Node Quantity</th>
<th>Capacity Disk Size (each)</th>
<th>Capacity Disk Quantity (per node)</th>
<th>Cluster Usable Capacity at RF=2</th>
<th>Cluster Usable Capacity at RF=3</th>
</tr>
</thead>
<tbody>
<tr>
<td>HXAF220c-M5SX</td>
<td>8</td>
<td>3.8 TB</td>
<td>8</td>
<td>102.8 TiB</td>
<td>68.6 TiB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>960 GB</td>
<td>8</td>
<td>25.7 TiB</td>
<td>17.1 TiB</td>
</tr>
<tr>
<td>HXAF240c-M5SX</td>
<td>8</td>
<td>3.8 TB</td>
<td>6</td>
<td>77.1 TiB</td>
<td>51.4 TiB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15</td>
<td>192.8 TiB</td>
<td>128.5 TiB</td>
</tr>
</tbody>
</table>
### Solution Design

<table>
<thead>
<tr>
<th>HX-Series Server Model</th>
<th>Node Quantity</th>
<th>Capacity Disk Size (each)</th>
<th>Capacity Disk Quantity (per node)</th>
<th>Cluster Usable Capacity at RF=2</th>
<th>Cluster Usable Capacity at RF=3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>23</td>
<td>960 GB</td>
<td>6</td>
<td>295.7 TiB</td>
<td>197.1 TiB</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>15</td>
<td>19.3 TiB</td>
<td>12.9 TiB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>23</td>
<td>48.2 TiB</td>
<td>32.1 TiB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>73.9 TiB</td>
<td>12.9 TiB</td>
<td>32.1 TiB</td>
<td></td>
</tr>
</tbody>
</table>

Calculations will be based upon the number of nodes, the number of capacity disks per node, and the size of the capacity disks. Table 11 is not a comprehensive list of all capacities and models available.

### Physical Topology

#### Topology Overview

The Cisco HyperFlex for Microsoft Hyper-V system is composed of a pair of Cisco UCS Fabric Interconnects along with up to 8 HX-Series rack-mount servers as converged nodes per cluster. 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. Upstream network connections, also referred to as “northbound” network connections are made from the Fabric Interconnects to the customer data center network at the time of installation.

![HyperFlex Standard Cluster Topology](image-url)

Figure 14  HyperFlex Standard Cluster Topology
Fabric Interconnects

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.

Fabric Interconnects have the following ports, which must be connected for proper management of the Cisco UCS domain:

- **Mgmt**: A 10/100/1000 Mbps port for managing the Fabric Interconnect and the Cisco UCS domain via GUI and CLI tools. This port is also used by remote KVM, IPMI and SoL sessions to the managed servers within the domain. This is typically connected to the customer management network.

- **L1**: A cross connect port for forming the Cisco UCS management cluster. This port is connected directly to the L1 port of the paired Fabric Interconnect using a standard CAT5 or CAT6 Ethernet cable with RJ45 plugs. It is not necessary to connect this to a switch or hub.

- **L2**: A cross connect port for forming the Cisco UCS management cluster. This port is connected directly to the L2 port of the paired Fabric Interconnect using a standard CAT5 or CAT6 Ethernet cable with RJ45 plugs. It is not necessary to connect this to a switch or hub.

- **Console**: An RJ45 serial port for direct console access to the Fabric Interconnect. This port is typically used during the initial FI setup process with the included serial to RJ45 adapter cable. This can also be plugged into a terminal aggregator or remote console server device.

HX-Series Rack-Mount Servers

The HX-Series converged servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode. This option enables Cisco UCS Manager to manage the HX-Series Rack-Mount Servers using a single cable for both management traffic and data traffic. Cisco HyperFlex M5 generation servers can be configured only with the Cisco VIC 1387 card. The standard and redundant connection practice is to connect port 1 of the VIC card (the right-hand port) to a port on FI A, and port 2 of the VIC card (the left-hand port) to a port on FI B (Figure 15). The HyperFlex installer checks for this configuration, and that all servers’ cabling matches. Failure to follow this cabling practice can lead to errors, discovery failures, and loss of redundant connectivity.

Various combinations of physical connectivity between the Cisco HX-series servers and the Fabric Interconnects are possible, but only specific combinations are supported. For example, use of the Cisco QSA module to convert a 40 GbE QSFP+ port into a 10 GbE SFP+ port is allowed for M5 generation servers in order to configure M5 generation servers along with model 6248 or 6296 Fabric Interconnects. Table 12 lists the possible connections, and which of these methods is supported.

<table>
<thead>
<tr>
<th>Table 12  Supported Physical Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Interconnect Model</td>
</tr>
<tr>
<td>Port Type</td>
</tr>
<tr>
<td>M5 with VIC 1387</td>
</tr>
</tbody>
</table>
Logical Topology

Logical Network Design

The Cisco HyperFlex system has communication pathways that fall into four defined zones (Figure 16):

- **Management Zone:** This zone comprises the connections needed to manage the physical hardware, the hypervisor hosts, and the storage platform controller virtual machines (SCVM). These interfaces and IP addresses need to be available to all staff who will administer the HX system, throughout the LAN/WAN. This zone must provide access to Domain Name System (DNS) and Network Time Protocol (NTP) services, and allow Secure Shell (SSH) communication. In this zone are multiple physical and virtual components:
  - Fabric Interconnect management ports.
  - Cisco UCS external management interfaces used by the servers, which answer via the FI management ports.
  - Hyper-V host management interfaces.
  - Storage Controller VM management interfaces.
  - A roaming HX cluster management interface.
  - Storage Controller VM Management interfaces.

- **VM Zone:** This zone comprises the connections needed to service network IO to the guest VMs that will run inside the HyperFlex hyperconverged system. This zone typically contains multiple VLANs that are trunked to the Cisco UCS Fabric Interconnects via the network uplinks, and tagged with 802.1Q VLAN IDs. These interfaces and IP addresses need to be available to all staff and other computer endpoints which need to communicate with the guest VMs in the HX system, throughout the LAN/WAN.

- **Storage Zone:** This zone comprises the connections used by the Cisco HX Data Platform software, Hyper-V hosts, and the storage controller VMs to service the HX Distributed Data Filesystem. These interfaces and IP addresses need to be able to communicate with each other at all times for proper operation. During normal operation, this traffic all occurs within the Cisco UCS domain, however there
are hardware failure scenarios where this traffic would need to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa. This zone is primarily jumbo frame traffic therefore jumbo frames must be enabled on the Cisco UCS uplinks. In this zone are multiple components:

- A teamed interface is used for storage traffic on each Hyper-V host in the HX cluster.
- Storage Controller VM storage interfaces.
- A roaming HX cluster storage interface.

- **Live Migration Zone:** This zone comprises the connections used by the Hyper-V hosts to enable live migration of the guest VMs from host to host. During normal operation, this traffic all occurs within the Cisco UCS domain, however there are hardware failure scenarios where this traffic would need to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX live migration traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa.

Figure 16 illustrates the logical network design.

**Figure 16  Logical Network Design**

---

**Design Elements**

Installing the HyperFlex system is primarily done through a deployable HyperFlex installer virtual machine, available for download at [cisco.com](http://cisco.com) as an OVA file. The installer VM performs most of the Cisco UCS configuration work, it can be leveraged to simplify the installation of Windows Server 2016 on the HyperFlex hosts, and also performs significant portions of the configuration. Finally, the installer VM is used to install the HyperFlex HX Data Platform software and create the HyperFlex cluster. Because this simplified installation method has been developed by Cisco, this CVD will not give detailed manual steps for the
configuration of all the elements that are handled by the installer. Instead, the elements configured will be described and documented in this section, and the subsequent sections will guide you through the manual steps needed for installation, and how to utilize the HyperFlex Installer for the remaining configuration steps.

Network Design

Cisco UCS Uplink Connectivity

Cisco UCS network uplinks connect “northbound” from the pair of Cisco UCS Fabric Interconnects to the LAN in the customer datacenter. All Cisco UCS uplinks operate as trunks, carrying multiple 802.1Q VLAN IDs across the uplinks. The default Cisco UCS behavior is to assume that all VLAN IDs defined in the Cisco UCS configuration are eligible to be trunked across all available uplinks.

Cisco UCS Fabric Interconnects appear on the network as a collection of endpoints versus another network switch. Internally, the Fabric Interconnects do not participate in spanning-tree protocol (STP) domains, and the Fabric Interconnects cannot form a network loop, as they are not connected to each other with a layer 2 Ethernet link. All link up/down decisions via STP will be made by the upstream root bridges.

Uplinks need to be connected and active from both Fabric Interconnects. For redundancy, multiple uplinks can be used on each FI, either as 802.3ad Link Aggregation Control Protocol (LACP) port-channels, or using individual links. For the best level of performance and redundancy, uplinks can be made as LACP port-channels to multiple upstream Cisco switches using the virtual port channel (vPC) feature. Using vPC uplinks allows all uplinks to be active passing data, plus protects against any individual link failure, and the failure of an upstream switch. Other uplink configurations can be redundant, but spanning-tree protocol loop avoidance may disable links if vPC is not available.

All uplink connectivity methods must allow for traffic to pass from one Fabric Interconnect to the other, or from fabric A to fabric B. There are scenarios where cable, port or link failures would require traffic that normally does not leave the Cisco UCS domain, to now be forced over the Cisco UCS uplinks. Additionally, this traffic flow pattern can be seen briefly during maintenance procedures, such as updating firmware on the Fabric Interconnects, which requires them to be rebooted. The following section detail the uplink connectivity option used for this solution.

vPC to Multiple Switches

This recommended connection design relies on using Cisco switches that have the virtual port channel feature, such as Catalyst 6000 series switches running VSS, Cisco Nexus 5000 series, and Cisco Nexus 9000 series switches. Logically the two vPC enabled switches appear as one, and therefore spanning-tree protocol will not block any links. This configuration allows for all links to be active, achieving maximum bandwidth potential, and multiple redundancy at each level.

**Figure 17 Connectivity with vPC**
Solution Design

VLANs and Subnets

For the base HyperFlex system configuration, multiple VLANs need to be carried to the Cisco UCS domain from the upstream LAN, and these VLANs are also defined in the Cisco UCS configuration. The hx-storage-data VLAN must be a separate VLAN ID from the remaining VLANs. Table 13 lists the VLANs created by the HyperFlex installer in Cisco UCS, and their functions:

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>VLAN ID</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| hx-inband-mgmt  | Customer supplied | Hyper-V host management interfaces  
                      | HX Storage Controller VM management interfaces  
                      | HX Storage Cluster roaming management interface |
| hx-storage-data | Customer supplied | Hyper-V host storage interfaces  
                      | HX Storage Controller storage network interfaces  
                      | HX Storage Cluster roaming storage interface |
| vm-network      | Customer supplied | Guest VM network interfaces |
| hx-livemigrate  | Customer supplied | Hyper-V host live migration interfaces |

A dedicated network or subnet for physical device management is often used in datacenters. In this scenario, the mgmt0 interfaces of the two Fabric Interconnects would be connected to that dedicated network or subnet. This is a valid configuration for HyperFlex installations with the following caveat; wherever the HyperFlex installer is deployed it must have IP connectivity to the subnet of the mgmt0 interfaces of the Fabric Interconnects, and also have IP connectivity to the subnets used by the hx-inband-mgmt VLANs listed above.

Jumbo Frames

All HyperFlex storage traffic traversing the hx-storage-data VLAN and subnet is configured by default to use jumbo frames, or to be precise, all communication is configured to send IP packets with a Maximum Transmission Unit (MTU) size of 9000 bytes. In addition, the default MTU for the hx-livemigrate VLAN is also set to use jumbo frames. Using a larger MTU value means that each IP packet sent carries a larger payload, therefore transmitting more data per packet, and consequently sending and receiving data faster. This configuration also means that the Cisco UCS uplink switches must be configured to pass jumbo frames. Failure to configure the Cisco UCS uplink switches to allow jumbo frames can lead to service interruptions during some failure scenarios, including Cisco UCS firmware upgrades, or when a cable or port failure would cause storage traffic to traverse the northbound Cisco UCS uplink switches.

HyperFlex clusters can be configured to use standard size frames of 1500 bytes, however Cisco recommends that this configuration only be used in environments where the Cisco UCS uplink switches are not capable of passing jumbo frames, and that jumbo frames be enabled in all other situations.

Cisco UCS Design

This section describes the elements within Cisco UCS Manager that are configured by the Cisco HyperFlex installer. Many of the configuration elements are fixed in nature, meanwhile the HyperFlex installer does allow for some items to be specified at the time of creation, for example VLAN names and IDs, external
management IP pools and more. Where the elements can be manually set during the installation, those items will be noted in << >> brackets.

Cisco UCS Organization

During the HyperFlex installation a new Cisco UCS Sub-Organization is created. You must specify a unique Sub-Organization name for each cluster during the installation, for example “hx1hybrid”, or “hx2sed”. The sub-organization is created underneath the root level of the Cisco UCS hierarchy, and is used to contain all policies, pools, templates and service profiles used by HyperFlex, which prevents problems from overlapping settings across policies and pools. This arrangement also allows for organizational control using Role-Based Access Control (RBAC) and administrative locales within Cisco UCS Manager at a later time if desired. In this way, control can be granted to administrators of only the HyperFlex specific elements of the Cisco UCS domain, separate from control of root level elements or elements in other sub-organizations.

![Cisco UCS HyperFlex Sub-Organization](image)

Cisco UCS LAN Policies

QoS System Classes

Specific Cisco UCS Quality of Service (QoS) system classes are defined for a Cisco HyperFlex system. These classes define Class of Service (CoS) values that can be used by the uplink switches north of the Cisco UCS domain, plus which classes are active, along with whether packet drop is allowed, the relative weight of the different classes when there is contention, the maximum transmission unit (MTU) size, and if there is multicast optimization applied. QoS system classes are defined for the entire Cisco UCS domain, the classes that are enabled can later be used in QoS policies, which are then assigned to Cisco UCS vNICs. Table 14 and Figure 19 list the QoS System Class settings configured for HyperFlex:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Enabled</th>
<th>CoS</th>
<th>Packet Drop</th>
<th>Weight</th>
<th>MTU</th>
<th>Multicast Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum</td>
<td>Yes</td>
<td>5</td>
<td>No</td>
<td>4</td>
<td>9216</td>
<td>No</td>
</tr>
<tr>
<td>Gold</td>
<td>Yes</td>
<td>4</td>
<td>Yes</td>
<td>4</td>
<td>Normal</td>
<td>No</td>
</tr>
<tr>
<td>Silver</td>
<td>Yes</td>
<td>2</td>
<td>Yes</td>
<td>Best-effort</td>
<td>Normal</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Changing the QoS system classes on a Cisco UCS 6332 or 6332-16UP model Fabric Interconnect requires both FIs to reboot in order to take effect.

**QoS Policies**

In order to apply the settings defined in the Cisco UCS QoS System Classes, specific QoS Policies must be created, and then assigned to the vNICs, or vNIC templates used in Cisco UCS Service Profiles. Table 15 details the QoS Policies configured for HyperFlex, and their default assignment to the vNIC templates created:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Priority</th>
<th>Burst</th>
<th>Rate</th>
<th>Host Control</th>
<th>Used by vNIC Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum</td>
<td>Platinum</td>
<td>10240</td>
<td>Line-rate</td>
<td>None</td>
<td>storage-data-a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>storage-data-b</td>
</tr>
<tr>
<td>Gold</td>
<td>Gold</td>
<td>10240</td>
<td>Line-rate</td>
<td>None</td>
<td>vm-network-a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>vm-network-b</td>
</tr>
<tr>
<td>Silver</td>
<td>Silver</td>
<td>10240</td>
<td>Line-rate</td>
<td>None</td>
<td>hv-mgmt-a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>hv-mgmt-b</td>
</tr>
<tr>
<td>Bronze</td>
<td>Bronze</td>
<td>10240</td>
<td>Line-rate</td>
<td>None</td>
<td>hv-livemigrate-a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>hv-livemigrate-b</td>
</tr>
<tr>
<td>Best Effort</td>
<td>Best Effort</td>
<td>10240</td>
<td>Line-rate</td>
<td>None</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Solution Design

Multicast Policy

A Cisco UCS Multicast Policy is configured by the HyperFlex installer, which is referenced by the VLANs that are created. The policy allows for future flexibility if a specific multicast policy needs to be created and applied to other VLANs that may be used by non-HyperFlex workloads in the Cisco UCS domain. Table 16 and Figure 20 details the Multicast Policy configured for HyperFlex:

<table>
<thead>
<tr>
<th>Name</th>
<th>IGMP Snooping State</th>
<th>IGMP Snooping Queries State</th>
</tr>
</thead>
<tbody>
<tr>
<td>HyperFlex</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Figure 20 Multicast Policy

VLANs

VLANs are created by the HyperFlex installer to support a base HyperFlex system, with a VLAN for live migrate, and a single or multiple VLANs defined for guest VM traffic. Names and IDs for the VLANs are defined in the Cisco UCS configuration page of the HyperFlex installer web interface. The VLANs listed in Cisco UCS must already be present on the upstream network, and the Cisco UCS FIs do not participate in VLAN Trunk Protocol (VTP). Table 17 and Figure 21 list the VLANs configured for HyperFlex.

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
<th>Type</th>
<th>Transport</th>
<th>Native</th>
<th>VLAN Sharing</th>
<th>Multicast Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&lt;hx-inband-mgmt&gt;&gt;</td>
<td>&lt;user_defined&gt;</td>
<td>LAN</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
<tr>
<td>&lt;&lt;hx-storage-data&gt;&gt;</td>
<td>&lt;user_defined&gt;</td>
<td>LAN</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
<tr>
<td>&lt;&lt;vm-network&gt;&gt;</td>
<td>&lt;user_defined&gt;</td>
<td>LAN</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
<tr>
<td>&lt;&lt;hx-livemigrate&gt;&gt;</td>
<td>&lt;user_defined&gt;</td>
<td>LAN</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
</tbody>
</table>
Solution Design

Figure 21  Cisco UCS VLANs
LAN / LAN Cloud / VLANs

VLANs

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
<th>Type</th>
<th>Transport</th>
<th>Native</th>
<th>VLAN Sharing</th>
<th>Primary VLAN No.</th>
<th>Multicast Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN default (1)</td>
<td>1</td>
<td>Lan</td>
<td>Ether</td>
<td>Yes</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>VLAN hx-inband-mgmt (31...)</td>
<td>3175</td>
<td>Lan</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
<tr>
<td>VLAN hx-ilivemigrate (3173)</td>
<td>3173</td>
<td>Lan</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
<tr>
<td>VLAN hx-storage-data (3172)</td>
<td>3172</td>
<td>Lan</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
<tr>
<td>VLAN vm-network (3174)</td>
<td>3174</td>
<td>Lan</td>
<td>Ether</td>
<td>No</td>
<td>None</td>
<td>None</td>
<td>HyperFlex</td>
</tr>
</tbody>
</table>

Management IP Address Pool

A Cisco UCS Management IP Address Pool must be populated with a block of IP addresses. These IP addresses are assigned to the Cisco Integrated Management Controller (CIMC) interface of the rack mount and blade servers that are managed in the Cisco UCS domain. The IP addresses are the communication endpoints for various functions, such as remote KVM, virtual media, Serial over LAN (SoL), and Intelligent Platform Management Interface (IPMI) for each rack mount or blade server. Therefore, a minimum of one IP address per physical server in the domain must be provided. The IP addresses are considered to be an “out-of-band” address, meaning that the communication pathway uses the Fabric Interconnects’ mgmt0 ports, which answer ARP requests for the management addresses. Because of this arrangement, the IP addresses in this pool must be in the same IP subnet as the IP addresses assigned to the Fabric Interconnects’ mgmt0 ports. A new IP pool, named “hx-ext-mgmt” is created in the HyperFlex sub-organization, and populated with a block of IP addresses, a subnet mask, and a default gateway by the HyperFlex installer.

Figure 22  Management IP Address Pool

MAC Address Pools

One of the core benefits of the Cisco UCS and Virtual Interface Card (VIC) technology is the assignment of the personality of the card via Cisco UCS Service Profiles. The number of virtual NIC (vNIC) interfaces, their VLAN associations, MAC addresses, QoS policies and more are all applied dynamically as part of the service profile association process. Media Access Control (MAC) addresses use 6 bytes of data as a unique address to identify the interface on the layer 2 network. All devices are assigned a unique MAC address, which is ultimately used for all data transmission and reception. The Cisco UCS and VIC technology picks a MAC address from a pool of addresses, and assigns it to each vNIC defined in the service profile when that service profile is created.
Best practices mandate that MAC addresses used for Cisco UCS domains use 00:25:B5 as the first three bytes, which is one of the Organizationally Unique Identifiers (OUI) registered to Cisco Systems, Inc. The fourth byte (e.g. 00:25:B5:xx) is specified during the HyperFlex installation. The fifth byte is set automatically by the HyperFlex installer, to correlate to the Cisco UCS fabric and the vNIC placement order. Finally, the last byte is incremented according to the number of MAC addresses created in the pool. To avoid overlaps, when you define the values in the HyperFlex installer you must ensure that the first four bytes of the MAC address pools are unique for each HyperFlex cluster installed in the same layer 2 network, and also different from MAC address pools in other Cisco UCS domains which may exist.

Table 18 lists the MAC Address Pools configured for HyperFlex and their default assignment to the vNIC templates created.

<table>
<thead>
<tr>
<th>Name</th>
<th>Block Start</th>
<th>Size</th>
<th>Assignment Order</th>
<th>Used by vNIC Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>hv-mgmt-a</td>
<td>00:25:B5:&lt;xx&gt;:A1:01</td>
<td>100</td>
<td>Sequential</td>
<td>hv-mgmt-a</td>
</tr>
<tr>
<td>hv-mgmt-b</td>
<td>00:25:B5:&lt;xx&gt;:B2:01</td>
<td>100</td>
<td>Sequential</td>
<td>hv-mgmt-b</td>
</tr>
<tr>
<td>hv-livemigrate-a</td>
<td>00:25:B5:&lt;xx&gt;:A7:01</td>
<td>100</td>
<td>Sequential</td>
<td>hv-livemigrate-a</td>
</tr>
<tr>
<td>hv-livemigrate-b</td>
<td>00:25:B5:&lt;xx&gt;:B8:01</td>
<td>100</td>
<td>Sequential</td>
<td>hv-livemigrate-b</td>
</tr>
<tr>
<td>storage-data-a</td>
<td>00:25:B5:&lt;xx&gt;:A3:01</td>
<td>100</td>
<td>Sequential</td>
<td>storage-data-a</td>
</tr>
<tr>
<td>storage-data-b</td>
<td>00:25:B5:&lt;xx&gt;:B4:01</td>
<td>100</td>
<td>Sequential</td>
<td>storage-data-b</td>
</tr>
<tr>
<td>vm-network-a</td>
<td>00:25:B5:&lt;xx&gt;:A5:01</td>
<td>100</td>
<td>Sequential</td>
<td>vm-network-a</td>
</tr>
<tr>
<td>vm-network-b</td>
<td>00:25:B5:&lt;xx&gt;:B6:01</td>
<td>100</td>
<td>Sequential</td>
<td>vm-network-b</td>
</tr>
</tbody>
</table>
Network Control Policies

Cisco UCS Network Control Policies control various aspects of the behavior of vNICs defined in the Cisco UCS Service Profiles. Settings controlled include enablement of Cisco Discovery Protocol (CDP), MAC address registration, MAC address forging, and the action taken on the vNIC status if the Cisco UCS network uplinks are failed. Two policies are configured by the HyperFlex Installer, HyperFlex-infra is applied to the “infrastructure” vNIC interfaces of the HyperFlex system, and HyperFlex-vm, which is only applied to the vNIC interfaces carrying guest VM traffic. This allows for more flexibility, even though the policies are currently configured with the same settings. Table 19 details the Network Control Policies configured for HyperFlex, and their default assignment to the vNIC templates created:

<table>
<thead>
<tr>
<th>Table 19</th>
<th>Network Control Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td><strong>CDP</strong></td>
</tr>
<tr>
<td>HyperFlex-infra</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
vNIC Templates

Cisco UCS Manager has a feature to configure vNIC templates, which can be used to simplify and speed up configuration efforts. VNIC templates are referenced in service profiles and LAN connectivity policies, versus configuring the same vNICs individually in each service profile, or service profile template. VNIC templates contain all the configuration elements that make up a vNIC, including VLAN assignment, MAC address pool selection, fabric A or B assignment, fabric failover, MTU, QoS policy, Network Control Policy, and more. Templates are created as either initial templates, or updating templates. Updating templates retain a link between the parent template and the child object, therefore when changes are made to the template, the changes are propagated to all remaining linked child objects. An additional feature named “vNIC Redundancy” allows vNICs to be configured in pairs, so that the settings of one vNIC template, designated as a primary template, will automatically be applied to a configured secondary template. For all HyperFlex vNIC templates, the “A” side vNIC template is configured as a primary template, and the related “B” side vNIC template is a secondary. In each case, the only configuration difference between the two templates is which fabric they are configured to connect through. The following tables list the initial settings in each of the vNIC templates created by the HyperFlex installer:

**Figure 24  Network Control Policy**

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>HyperFlex-infra</td>
</tr>
<tr>
<td>Description</td>
<td>Network Control policy for infrastructure vNICs Hyper</td>
</tr>
<tr>
<td>Owner</td>
<td>Local</td>
</tr>
<tr>
<td>CDP</td>
<td>Enabled</td>
</tr>
<tr>
<td>MAC Register Mode:</td>
<td>Only Native VLAN, All Host Vlans</td>
</tr>
<tr>
<td>Action on Uplink Fail:</td>
<td>Link Down, Warning</td>
</tr>
<tr>
<td>MAC Security</td>
<td>Forged: Allow</td>
</tr>
<tr>
<td>LLDP transmit:</td>
<td>Enabled</td>
</tr>
<tr>
<td>LLDP receive:</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Table 20  vNIC Template hv-mgmt-a/b**

<table>
<thead>
<tr>
<th>vNIC Template Name:</th>
<th>hv-mgmt-a</th>
<th>hv-mgmt-b</th>
<th>storage-data-a</th>
<th>storage-data-b</th>
<th>hv-livemigrate-a</th>
<th>hv-livemigrate-b</th>
<th>vm-network-a</th>
<th>vm-network-b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td>Value</td>
<td>Value</td>
<td>Value</td>
<td>Value</td>
<td>Value</td>
<td>Value</td>
<td>Value</td>
<td>Value</td>
</tr>
<tr>
<td>Fabric ID</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>B</td>
</tr>
</tbody>
</table>
LAN Connectivity Policies

Cisco UCS Manager has a feature for LAN Connectivity Policies, which aggregates all of the vNICs or vNIC templates desired for a service profile configuration into a single policy definition. This simplifies configuration efforts by defining a collection of vNICs or vNIC templates once, and using that policy in the service profiles or service profile templates. The HyperFlex installer configures a LAN Connectivity Policy named HyperFlex, which contains all of the vNIC templates defined in the previous section, along with an Adapter Policy named HyperFlex, also configured by the HyperFlex installer. Table 21 lists the LAN Connectivity Policy configured for HyperFlex:

Table 21  LAN Connectivity Policy

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Use vNIC Template</th>
<th>vNIC Name</th>
<th>vNIC Template Used</th>
<th>Adapter Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>HyperFlex</td>
<td>Yes</td>
<td>hv-mgmt-a</td>
<td>hv-mgmt-a</td>
<td>HyperFlex</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hv-mgmt-b</td>
<td>hv-mgmt-b</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hv-livemigrate-a</td>
<td>hv-livemigrate-a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hv-livemigrate-b</td>
<td>hv-livemigrate-b</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>storage-data-a</td>
<td>storage-data-a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>storage-data-b</td>
<td>storage-data-b</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vm-network-a</td>
<td>vm-network-a</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vm-network-b</td>
<td>vm-network-b</td>
<td></td>
</tr>
</tbody>
</table>
Cisco UCS Servers Policies

Adapter Policies

Cisco UCS Adapter Policies are used to configure various settings of the Converged Network Adapter (CNA) installed in the Cisco UCS blade or rack-mount servers. Various advanced hardware features can be enabled or disabled depending on the software or operating system being used. The following figures detail the Adapter Policy named “HyperFlex” configured for HyperFlex.

Figure 25  Cisco UCS Adapter Policy Resources

<table>
<thead>
<tr>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pooled</td>
</tr>
<tr>
<td>Transmit Queues</td>
</tr>
<tr>
<td>Ring Size</td>
</tr>
<tr>
<td>Receive Queues</td>
</tr>
<tr>
<td>Ring Size</td>
</tr>
<tr>
<td>Completion Queues</td>
</tr>
<tr>
<td>Interrupts</td>
</tr>
</tbody>
</table>
Cisco HX-Series M5 generation servers no longer use pre-defined BIOS setting defaults derived from Cisco UCS Manager, instead the servers have default BIOS tokens set from the factory. The current default token settings can be viewed at the following website: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/Reference-Docs/Server-BIOS-Tokens/3-2/b_UCS_BIOS_Tokens.html

A BIOS policy, named “HyperFlex-m5” is created by the HyperFlex installer to modify the setting of M5 generation servers. The settings modified are as follows:

- System altitude is set to “Auto”
- CPU performance is set to “HPC”
- Processor C1E state is set to “Disabled”
- Power Technology is set to “Performance”
- Energy Performance is set to “Performance”
- Serial Port A is enabled
- Console Redirection is set to Serial Port A

Boot Policies

Cisco UCS Boot Policies define the boot devices used by rack-mount servers, and the order that they are attempted to boot from. Cisco HX-Series M5 generation rack-mount servers have their Hyper-V hypervisors installed to an internal M.2 SSD boot drive, therefore they require a unique boot policy defining that the servers should boot from that location. The HyperFlex installer configures a boot policy named “HyperFlex-m5” specifying boot from the M.2 SSDs, referred to as “Embedded Disk” which is used by the HyperFlex M5 converged nodes, and should not be modified.
Figure 27 details the HyperFlex Boot Policies for Cisco HX-Series M5 generation rack-mount servers.

### Figure 27: Cisco UCS M5 Boot Policy

<table>
<thead>
<tr>
<th>Actions</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Name: HyperFlex-m5</td>
</tr>
<tr>
<td></td>
<td>Description: Recommended boot policy for HyperFlex servers</td>
</tr>
<tr>
<td>Show Policy Usage</td>
<td>Owner: Local</td>
</tr>
<tr>
<td>Use Global</td>
<td>Reboot on Boot Order Change:</td>
</tr>
<tr>
<td></td>
<td>Enforce vNIC/vHBA/iSCSI Name:</td>
</tr>
<tr>
<td></td>
<td>Boot Mode: Legacy, UEFI</td>
</tr>
</tbody>
</table>

**Warning**

The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order. If Enforce vNIC/vHBA/iSCSI Name is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported. If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

### Host Firmware Packages

Cisco UCS Host Firmware Packages represent one of the most powerful features of the Cisco UCS platform; the ability to control the firmware revision of all the managed blades and rack-mount servers via a policy specified in the service profile. Host Firmware Packages are defined and referenced in the service profiles. Once a service profile is associated to a server, the firmware of all the components defined in the Host Firmware Package are automatically upgraded or downgraded to match the package. The HyperFlex installer creates a Host Firmware Packages named “HyperFlex-m5” which use the simple package definition method, applying firmware revisions to all components that matches a specific Cisco UCS firmware bundle, versus defining the firmware revisions part by part. Figure 28 detail the Host Firmware Package configured by the HyperFlex installer for Cisco HX-Series M5 generation rack-mount servers.

### Figure 28: Cisco UCS M5 Host Firmware Package

<table>
<thead>
<tr>
<th>Actions</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Name: HyperFlex-m5</td>
</tr>
<tr>
<td></td>
<td>Description: Recommended Host Firmware Packages for M5 Hyp</td>
</tr>
<tr>
<td></td>
<td>Owner: Local</td>
</tr>
<tr>
<td>Show Policy Usage</td>
<td>Blade Package: 3.2(3g)B</td>
</tr>
<tr>
<td>Use Global</td>
<td>Blade Backup Package:</td>
</tr>
<tr>
<td>Modify Package Versions</td>
<td>Rack Package: 3.2(3g)C</td>
</tr>
<tr>
<td>Modify Backup Package Versions</td>
<td>Rack Backup Package:</td>
</tr>
<tr>
<td></td>
<td>Service Pack:</td>
</tr>
</tbody>
</table>
Local Disk Configuration Policies

Cisco UCS Local Disk Configuration Policies are used to define the configuration of disks installed locally within each blade or rack-mount server, most often to configure Redundant Array of Independent/Inexpensive Disks (RAID levels) when multiple disks are present for data protection. Since HX-Series converged nodes providing storage resources do not require RAID, the HyperFlex installer creates a Local Disk Configuration Policies, named “HyperFlex-m5” which allows any local disk configuration. The policy named “HyperFlex-m5” is used by the service profile template named “hx-nodes-m5”, which is for the HyperFlex M5 generation converged servers, and should not be modified.

Figure 29 details the Local Disk Configuration Policies configured by the HyperFlex installer.

Maintenance Policies

Cisco UCS Maintenance Policies define the behavior of the attached blades and rack-mount servers when changes are made to the associated service profiles. The default Cisco UCS Maintenance Policy setting is “Immediate” meaning that any change to a service profile that requires a reboot of the physical server will result in an immediate reboot of that server. The Cisco best practice is to use a Maintenance Policy set to “user-ack”, which requires a secondary acknowledgement by a user with the appropriate rights within Cisco UCS Manager, before the server is rebooted to apply the changes. The HyperFlex installer creates a Maintenance Policy named “HyperFlex” with the setting changed to “user-ack”. In addition, the On Next Boot setting is enabled, which will automatically apply changes the next time the server is rebooted, without any secondary acknowledgement. Figure 30 details the Maintenance Policy configured by the HyperFlex installer:
Power Control Policies

Cisco UCS Power Control Policies allow administrators to set priority values for power application to servers in environments where power supply may be limited, during times when the servers demand more power than is available. The HyperFlex installer creates a Power Control Policy named “HyperFlex” with all power capping disabled, and fans allowed to run at full speed when necessary. Figure 31 details the Power Control Policy configured by the HyperFlex installer.

Scrub Policies

Cisco UCS Scrub Policies are used to scrub, or erase data from local disks, BIOS settings and FlexFlash SD cards. If the policy settings are enabled, the information is wiped when the service profile using the policy is disassociated from the server. The HyperFlex installer creates a Scrub Policy named “HyperFlex” which has all settings disabled, therefore all data on local disks, SD cards and BIOS settings will be preserved if a service profile is disassociated. Figure 32 details the Scrub Policy configured by the HyperFlex installer.
vMedia Policies

Cisco UCS Virtual Media (vMedia) Policies automate the connection of virtual media files to the remote KVM session of the Cisco UCS blades and rack-mount servers. Using a vMedia policy can speed up installation time by automatically attaching an installation ISO file to the server, without having to manually launch the remote KVM console and connect them one-by-one. The HyperFlex installer creates a vMedia Policy named “HyperFlex” for future use, with no media locations defined.

Cisco UCS Service Profile Templates

Cisco UCS Manager has a feature to configure service profile templates, which can be used to simplify and speed up configuration efforts when the same configuration needs to be applied to multiple servers. Service profile templates are used to spawn multiple service profile copies to associate with a group of servers, versus configuring the same service profile manually each time it is needed. Service profile templates contain all the configuration elements that make up a service profile, including vNICs, vHBAs, local disk configurations, boot policies, host firmware packages, BIOS policies and more. Templates are created as either initial templates, or updating templates. Updating templates retain a link between the parent template and the child object, therefore when changes are made to the template, the changes are propagated to all remaining linked child objects. The HyperFlex installer creates a service profile templates, named “hx-nodes-m5”. The following tables list the service profile template configured by the HyperFlex installer.

| Service Profile Template Name: | hx-nodes-m5 |
| Setting | Value |
| UUID Pool | Hardware Default |
| Associated Server Pool | None |
| Maintenance Policy | HyperFlex |
| Management IP Address Policy | hx-ext-mgmt |
| Local Disk Configuration Policy | HyperFlex-m5 |
| LAN Connectivity Policy | HyperFlex |
| Boot Policy | HyperFlex-m5 |
| BIOS Policy | HyperFlex-m5 |
| Firmware Policy | HyperFlex-m5 |
| Power Control Policy | HyperFlex |
| Scrub Policy | HyperFlex |
| Serial over LAN Policy | HyperFlex |
Microsoft Hyper-V Host Design

The following sections detail the design of the elements within the Microsoft Hyper-V hypervisors, system requirements, virtual networking and the configuration of Hyper-V for the Cisco HyperFlex HX Distributed Data Platform.

Virtual Networking Design

The Cisco HyperFlex system has a pre-defined virtual network design at the Hyper-V hypervisor level. Four different virtual switches are created by the HyperFlex installer, each using two uplinks, which are each serviced by a vNIC defined in the Cisco UCS service profile.

The vSwitches created are:

- **vswitch-hx-inband-mgmt**: This vSwitch is created as part of the automated installation. As shown in the below figure, it is configured to use a teamed interface named “team-hx-inband-mgmt” with “hv-mgmt-a” and “hv-mgmt-b” as member adapters, without jumbo frames. The teaming and load balancing mode are configured for ‘Switch Independent’ and ‘Hyper-V Port’ respectively with “hv-mgmt-b” as Standby adapter. The management interfaces of Hyper-V host and Storage Platform Controller VMs connect to this vSwitch. The VLANs are not Native VLANs as assigned to the vNIC templates, and therefore they are defined in Hyper-V virtual switch manager.

- **vswitch-hx-storage-data**: This vSwitch is created as part of the automated installation. As shown in the below figure, it is configured to use a teamed interface named “team-hx-storage-data” with “storage-data-a” and “storage-data-b” as member adapters, with jumbo frames highly recommended. The teaming and load balancing mode are configured for ‘Switch Independent’ and ‘Hyper-V Port’ respectively with “storage-data-b” adapter in Standby mode. The storage interfaces of Hyper-V host connected to this vSwitch is used for connecting to the HX Datastore via SMB. The VLANs are not Native VLANs as assigned to the vNIC templates, and therefore they are defined in Hyper-V virtual switch manager.

- **vswitch-hx-vm-network**: This vSwitch is created as part of the automated installation. As shown in the below figure, it is configured to use a teamed interface named “team-vm-network-data” with “vm-network-a” and “vm-network-b” as member adapters, without jumbo frames. The teaming and load balancing mode are configured for ‘Switch Independent’ and ‘Hyper-V Port’ respectively with both adapters in active mode. The VLANs are not Native VLANs as assigned to the vNIC templates, and therefore they are defined in Hyper-V virtual switch manager.

- **vswitch-hx-livemigration**: This vSwitch is created as part of the automated installation. As shown in the below figure, it is configured to use a teamed interface named “team-hx-livemigration” with “hv-livemigrate-a” and “hv-livemigrate-b” as member adapters, with jumbo frames highly recommended. The teaming and load balancing mode are configured for ‘Switch Independent’ and ‘Hyper-V Port’ respectively with “hv-livemigrate-b” adapter in Standby mode. The VLANs are not Native VLANs as assigned to the vNIC templates, and therefore they are defined in Hyper-V virtual switch manager. The IP addresses to this interface are assigned post installation.

Table 23 and Figure 33 provide more details into the Hyper-V virtual networking design as built by the HyperFlex installer by default.
Table 23  Virtual Switches

<table>
<thead>
<tr>
<th>Virtual Switch</th>
<th>Interfaces Connected</th>
<th>Active adapter</th>
<th>Passive adapter</th>
<th>VLAN IDs</th>
<th>Jumbo</th>
</tr>
</thead>
<tbody>
<tr>
<td>vswitch-hx-inband-mgmt</td>
<td>Management Network</td>
<td>hv-mgmt-a</td>
<td>hv-mgmt-b</td>
<td>&lt;&lt;hx-inband-mgmt&gt;&gt;</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>Storage Controller Management Network</td>
<td>storage-data-a</td>
<td>storage-data-b</td>
<td>&lt;&lt;hx-storage-data&gt;&gt;</td>
<td>yes</td>
</tr>
<tr>
<td>vswitch-hx-storage-data</td>
<td>Storage Controller Data Network</td>
<td>vm-network-a</td>
<td>vm-network-b</td>
<td>&lt;&lt;vm-network&gt;&gt;</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>Storage Hypervisor Data Network</td>
<td>storage-data-a</td>
<td>storage-data-b</td>
<td>&lt;&lt;hx-storage-data&gt;&gt;</td>
<td>yes</td>
</tr>
<tr>
<td>vswitch-hx-vm-network</td>
<td>vm-network-&lt;&lt;VLAN ID&gt;&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vswitch-hx-livemigration</td>
<td>livemigrate-&lt;&lt;VLAN ID&gt;&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 33  Hyper-V Network Design
Discrete Device Assignment (I/O Passthrough)

Discrete Device Assignment (DDA) is a feature introduced in Windows Server 2016 Hyper-V allowing access to an entire PCIe device into a VM as though they were physical devices belonging to the VM itself. With the appropriate driver for the hardware device, the guest VM sends all I/O requests directly to the physical device, bypassing the hypervisor. In the Cisco HyperFlex system, the Storage Platform Controller VMs use this feature to gain full control of the Cisco 12Gbps SAS HBA cards in the Cisco HX-series rack-mount servers. This gives the controller VMs direct hardware level access to the physical disks installed in the servers, which they consume to construct the Cisco HX Distributed Filesystem. Only the disks connected directly to the Cisco SAS HBA are controlled by the controller VMs. Other disks, connected to different controllers, such as the M.2 drives, remain under the control of the Hyper-V hypervisor.

- Configuring the DDA feature is done by the Cisco HyperFlex installer and requires no manual steps.

Storage Platform Controller VMs

A key component of the Cisco HyperFlex system is the Storage Platform Controller Virtual Machine running on each of the nodes in the HyperFlex cluster. The controller VMs cooperate to form and coordinate the Cisco HX Distributed Filesystem, and service all the guest VM IO requests. The controller VMs deployed on the Hyper-V host are tied to a specific host, they start and stop along with the Hyper-V hypervisor, and the system is not considered to be online and ready until both the hypervisor and the Controller VMs have started.

- Each Hyper-V host has a single Controller VM deployed, and it cannot be moved or migrated to another host, nor should its settings be manually modified in any way.

The storage controller VM runs custom software and services that manage and maintain the Cisco HX Distributed Filesystem. The services and processes that run within the controller VMs are not exposed, therefore the Hyper-V hosts have any direct knowledge of the storage services provided by the controller VMs. Management and visibility into the function of the controller VMs, and the Cisco HX Distributed Filesystem is done via the HyperFlex Connect HTML management webpage.

- Deploying the controller VMs is all done by the Cisco HyperFlex installer, and requires no manual steps.

Controller VM Locations

The physical storage location of the controller VMs across all the Cisco HX-Series M5 generation rack servers (HX220c M5, HXAF220c M5, HX240c M5 and HXAF240c M5) is same due to the physical disk location and connections on those server models. The storage controller VM is operationally no different from any other typical virtual machines in a Hyper-V environment. The VM must have a virtual disk with the bootable root filesystem available in a location separate from the SAS HBA that the VM is controlling via DDA feature of Windows Server 2016 Hyper-V.

- The server boots the Windows Server 2016 Hyper-V from the internal M.2 form factor SSD.
- The Windows installer creates three partitions on the M.2 SSD – 500 MB for recovery partition, 90 GB for Windows OS boot partition and 30 GB partition where controller VM’s root filesystem is stored on a 2.5 GB virtual disk, /dev/sda. Both 90 GB and 30 GB partitions are formatted using NTFS file system. The controller VM has full control of all the front and rear facing hot-swappable disks via DDA control of the SAS HBA. The controller VM operating system sees the 240 GB SSD, also commonly called the “housekeeping” disk as /dev/sdb, and places HyperFlex binaries and logs on this disk. The remaining disks seen by the controller VM OS are used by the HX Distributed filesystem for caching and capacity layers.
The following figures detail the Storage Platform Controller VM placement on the Hyper-V hosts for Cisco HX M5 generation servers.

Figure 34  HX220c M5 Controller VM Placement

Figure 35  HX240c M5 Controller VM Placement

HyperFlex Datastores

A new HyperFlex cluster has no default datastores configured for virtual machine storage, therefore the datastores must be created using the vCenter Web Client plugin or the HyperFlex Connect GUI. It is important to recognize that all HyperFlex datastores are thinly provisioned, meaning that their configured size can far exceed the actual space available in the HyperFlex cluster. Alerts will be raised by the HyperFlex system in HyperFlex Connect when actual space consumption results in low amounts of free space, and
alerts will be sent via auto support email alerts. Overall space consumption in the HyperFlex clustered filesystem is optimized by the default deduplication and compression features.

Figure 36  Datastore Example

CPU Resource Control
Since the storage controller VMs provide critical functionality of the Cisco HX Distributed Data Platform, the HyperFlex installer will configure CPU resource control for the controller VMs. This resource control guarantees that the controller VMs will have CPU resources at a minimum level, in situations where the physical CPU resources of the Hyper-V hypervisor host are being heavily consumed by the guest VMs. Table 24 details the CPU resource control settings of the storage controller VMs.

Table 24  Controller VM CPU Reservations

<table>
<thead>
<tr>
<th>Number of vCPU</th>
<th>VM Reserve (percentage)</th>
<th>VM Limit (percentage)</th>
<th>Relative Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

Memory Resource Reservations
Since the storage controller VMs provide critical functionality of the Cisco HX Distributed Data Platform, the HyperFlex installer will configure by allocating static amount of memory for the controller VMs. This guarantees that the controller VMs will have access to all the memory resources allocated to it at power on. Table 25 details the memory resource reservation of the storage controller VMs.

Table 25  Controller VM Memory Reservations

<table>
<thead>
<tr>
<th>Server Models</th>
<th>Amount of Static Memory for SCVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX220c-M5SX</td>
<td></td>
</tr>
<tr>
<td>HXAF220c-M5SX</td>
<td>48 GB</td>
</tr>
<tr>
<td>HX240c-M5SX</td>
<td></td>
</tr>
<tr>
<td>HXAF240c-M5SX</td>
<td>72 GB</td>
</tr>
</tbody>
</table>
Installing the Cisco HyperFlex system on Hyper-V is primarily done via a deployable HyperFlex installer virtual machine available for download at cisco.com as a vhdx file. The installer VM performs the Cisco UCS configuration work, the configuration of Hyper-V on the HyperFlex hosts, the installation of the HyperFlex HX Data Platform software and creation of the HyperFlex cluster. Because this simplified installation method has been developed by Cisco, this CVD will not give detailed manual steps for the configuration of all the elements that are handled by the installer. The following sections will guide you through the prerequisites and manual steps needed prior to using the HyperFlex installer, how to utilize the HyperFlex Installer, and finally how to perform the remaining post-installation tasks.

**Prerequisites**

The following sections provide the required prerequisites.

**IP Addressing**

To install the HX Data Platform, an OVF installer appliance must be deployed on a separate virtualization host, which is not a member of the HyperFlex cluster. The HyperFlex installer requires one IP address on the management network and the HX installer appliance IP address must be able to communicate with Cisco UCS Manager, Hyper-V management IP addresses on the HX hosts, Windows Active Directory and DNS server and any management server IP addresses from where the Windows failover cluster will be managed.

Additional IP addresses for the Cisco HyperFlex system need to be allocated from the appropriate subnets and VLANs to be used. IP addresses that are used by the system fall into the following groups:

- **Cisco UCS Manager**: These addresses are used and assigned by Cisco UCS Manager. Three IP addresses are used by Cisco UCS Manager; one address is assigned to each Cisco UCS Fabric Interconnect, and the third IP address is a roaming address for management of the Cisco UCS cluster. In addition, at least one IP address per Cisco UCS blade or HX-series rack-mount server is required for the hx-ext-mgmt IP address pool, which are assigned to the CIMC interface of the physical servers. Since these management addresses are assigned from a pool, they need to be provided in a contiguous block of addresses. These addresses must all be in the same subnet.

- **HyperFlex and Hyper-V Management**: These addresses are used to manage the Hyper-V hypervisor hosts, and the HyperFlex Storage Platform Controller VMs. Two IP addresses per node in the HyperFlex cluster are required from the same subnet, an additional IP address is required for roaming HyperFlex cluster management interface and another additional IP address is required for the Windows failover cluster. These addresses can be assigned from the same subnet at the Cisco UCS Manager addresses, or they may be separate.

- **HyperFlex Storage**: These addresses are used by the HyperFlex Storage Platform Controller VMs, and also the Hyper-V hypervisor hosts, for sending and receiving data to/from the HX Distributed Data Platform Filesystem. Two IP addresses per node in the HyperFlex cluster are required from the same subnet, and a single additional IP address is needed as the roaming HyperFlex cluster storage interface. It is recommended to provision a subnet that is not used in the network for other purposes, and it is also possible to use non-routable IP address ranges for these interfaces. Finally, if the Cisco UCS domain is going to contain multiple HyperFlex clusters, it is recommended to use a different subnet and VLAN ID for the HyperFlex storage traffic for each cluster. This is a safer method, guaranteeing that storage traffic from multiple clusters cannot intermix.

- **Live Migration**: These IP addresses are used by the Hyper-V hypervisor hosts on interfaces to enable live migration capabilities. One or more IP addresses per node in the HyperFlex cluster are required from the same subnet.
Installation

The following tables provide space to input the required IP addresses for the installation of an 8 node standard HyperFlex cluster by listing the addresses required, plus an example IP configuration.

Table cells shaded in black do not require an IP address.

<table>
<thead>
<tr>
<th>Table 26 HyperFlex Standard Cluster IP Addressing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address Group:</strong></td>
</tr>
<tr>
<td>VLAN ID</td>
</tr>
<tr>
<td>Subnet</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Gateway</td>
</tr>
<tr>
<td><strong>Device</strong></td>
</tr>
<tr>
<td>Fabric Interconnect A</td>
</tr>
<tr>
<td>Fabric Interconnect B</td>
</tr>
<tr>
<td>Cisco UCS Manager</td>
</tr>
<tr>
<td>HyperFlex Cluster</td>
</tr>
<tr>
<td>Windows Failover Cluster</td>
</tr>
<tr>
<td>HyperFlex Node #1</td>
</tr>
<tr>
<td>HyperFlex Node #2</td>
</tr>
<tr>
<td>HyperFlex Node #3</td>
</tr>
<tr>
<td>HyperFlex Node #4</td>
</tr>
<tr>
<td>HyperFlex Node #5</td>
</tr>
<tr>
<td>Device</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Fabric Interconnect A</td>
</tr>
<tr>
<td>Fabric Interconnect B</td>
</tr>
<tr>
<td>UCS Manager</td>
</tr>
<tr>
<td>HyperFlex Cluster</td>
</tr>
<tr>
<td>Windows Failover Cluster</td>
</tr>
<tr>
<td>HyperFlex Node #1</td>
</tr>
<tr>
<td>HyperFlex Node #2</td>
</tr>
</tbody>
</table>

Table 27 HyperFlex Standard Cluster Example IP Addressing for a 4-Node Cluster

<table>
<thead>
<tr>
<th>Address Group:</th>
<th>UCS Management</th>
<th>HyperFlex and Hyper-V Management</th>
<th>HyperFlex Storage</th>
<th>Live Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID:</td>
<td>3175</td>
<td>3175</td>
<td>3172</td>
<td>3173</td>
</tr>
<tr>
<td>Subnet:</td>
<td>10.29.149.0</td>
<td>10.29.149.0</td>
<td>192.168.11.0</td>
<td>192.168.73.0</td>
</tr>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway:</td>
<td>10.29.149.1</td>
<td>10.29.149.1</td>
<td>192.168.11.1</td>
<td></td>
</tr>
</tbody>
</table>
IP addresses for Cisco UCS Management, plus HyperFlex and Hyper-V Management can come from the same subnet, or can be separate subnets, as long as the HyperFlex installer can reach them both.

**Configure the Active Directory for Constrained Delegation**

A Windows 2008 R2 and above forest/domain level Active Directory (AD) is required for the successful installation and operation of Cisco HyperFlex system with Hyper-V.

The steps in this topic must be completed to enable constrained delegation. Constrained delegation is used to join computers to the Active Directory. You provide constrained delegation information through the HX Data Platform Installer. Constrained delegation uses a service account, which is created manually. This service account is used to then log in to Active Directory, join the computers, and perform the authentications from the HyperFlex Storage Controller VM.

The Active Directory computer accounts applied to every node in the HyperFlex cluster include:

- Hyper-V host
- HyperFlex Storage Controller VM
- Hyper-V host Cluster namespace
- Server Message Block (SMB) Share namespace for the HyperFlex cluster

To configure constrained delegation, complete the following steps:

1. Create an hxadmin domain user account as HX service account.
2. Create an Organization Unit (OU) in Active Directory (AD), for example, HyperFlex:
   a. Use the Active Directory Users and Computers management tool to create the OU. Select View > Advanced Features to enable advance features. Select the OU that you created. For example, HyperFlex > Properties > Attribute Editor.
   b. Find the distinguished name attribute in the OU, and record the information as this will be required in the Constrained Delegation wizard of the HX Data Platform Installer wizard. The values will look like this: OU=HyperFlex,DC=contoso,DC=com.
   c. Use the Get-ADOrganizationalUnit cmdlet to get an organizational unit (OU) object or to perform a search to get multiple OUs.

   ```powershell
   Get-ADOrganizationalUnit -Filter 'Name -like "Hyp*"' | Format-Table Name, DistinguishedName
   ```

   Figure 37 PowerShell Get-ADOrganizationalUnit
3. Use Active Directory Users and Computers management tool to grant full permissions for the hxadmin user for the newly created OU. Make sure that Advanced features are enabled. If not, go back to Step 2.
   a. Select the OU that you created. For example, HyperFlex > Properties > Security > Advance.
   b. Click Change Owner and choose your hxadmin user.
   c. Click Add in the Advanced view.
   d. Select the principal and choose the hxadmin user. Choose Full Control and click OK.

**Figure 38 Change Ownership of the AD OU**

Prepopulate AD DNS with Records

The AD integrated DNS server is also required to resolve Fully Qualified Domain Names (FQDN).

To create DNS records, complete the following steps:

1. Create a record and reverse the PTR records for the listed devices to avoid installation failures:
   - For each Hyper-V hosts' management and storage interfaces
   - For each Storage Controller Nodes’ management and storage interfaces
   - HX Cluster CIP
   - Windows Failover Cluster IP

Standalone and non-Windows DNS servers are not supported.

The following tables provide a place to input the required DNS information for the installation and also lists the information required, and provide an example configuration.

**Table 28 DNS Server Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server #1</td>
<td></td>
</tr>
<tr>
<td>AD DNS Domain</td>
<td></td>
</tr>
<tr>
<td>UCS Domain Name</td>
<td></td>
</tr>
</tbody>
</table>
NTP

Consistent time clock synchronization is required across the components of the HyperFlex system, provided by reliable NTP servers, accessible for querying in the Cisco UCS Management network group, and the HyperFlex and Hyper-V Management group. NTP is used by Cisco UCS Manager, the Hyper-V hypervisor hosts, and the HyperFlex Storage Platform Controller VMs. For HyperFlex System with Hyper-V, AD Domain Controller IP or domain name is required to be used as reliable NTP source for consistent time clock synchronization.
VLANs

Prior to the installation, the required VLAN IDs need to be documented, and created in the upstream network if necessary. At a minimum, there are 4 VLANs that need to be trunked to the Cisco UCS Fabric Interconnects that comprise the HyperFlex system; a VLAN for the HyperFlex and Hyper-V Management group, a VLAN for the HyperFlex Storage group, a VLAN for the Live Migration group, and at least one VLAN for the guest VM traffic. The VLAN IDs must be supplied during the HyperFlex Cisco UCS configuration step, and the VLAN names can optionally be customized.

The following tables provide a place to input the required VLAN information and also provide an example configuration.

<table>
<thead>
<tr>
<th>Table 30 VLAN Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>&lt;&lt;hx-inband-mgmt&gt;&gt;</td>
</tr>
<tr>
<td>&lt;&lt;hx-storage-data&gt;&gt;</td>
</tr>
<tr>
<td>&lt;&lt;hx-vm-network&gt;&gt;</td>
</tr>
<tr>
<td>&lt;&lt;hx-livemigrate&gt;&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 31 VLAN Example Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>hx-inband-mgmt</td>
</tr>
<tr>
<td>hx-inband-repl</td>
</tr>
<tr>
<td>hx-storage-data</td>
</tr>
<tr>
<td>vm-network</td>
</tr>
<tr>
<td>hx-livemigrate</td>
</tr>
</tbody>
</table>

Network Uplinks

The Cisco UCS uplink connectivity design needs to be finalized prior to beginning the installation. One of the early manual tasks to be completed is to configure the Cisco UCS network uplinks and verify their operation, prior to beginning the HyperFlex installation steps. Refer to the network uplink design possibilities in the Network Design section.

The following tables provide a place to input the required network uplink information for the installation and provide an example configuration:

<table>
<thead>
<tr>
<th>Table 32 Network Uplink Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Interconnect Port</td>
</tr>
<tr>
<td>A</td>
</tr>
</tbody>
</table>
### Installation

<table>
<thead>
<tr>
<th>Fabric Interconnect Port</th>
<th>Port Channel</th>
<th>Port Channel Type</th>
<th>Port Channel ID</th>
<th>Port Channel Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes No</td>
<td>vPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes No</td>
<td>vPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes No</td>
<td>vPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>Yes No</td>
<td>LACP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes No</td>
<td>vPC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Table 33  Network Uplink Example Configuration

<table>
<thead>
<tr>
<th>Fabric Interconnect Port</th>
<th>Port Channel</th>
<th>Port Channel Type</th>
<th>Port Channel ID</th>
<th>Port Channel Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1/25</td>
<td>Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1/26</td>
<td>Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LACP</td>
<td>10</td>
<td>vpc-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vPC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>1/25</td>
<td>Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1/26</td>
<td>Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LACP</td>
<td>20</td>
<td>vpc-20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vPC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usernames and Passwords

Several usernames and passwords need to be defined or known as part of the HyperFlex installation process. The following tables provide a place to input the required username and password information and also provide an example configuration.

#### Table 34  Usernames and Passwords

<table>
<thead>
<tr>
<th>Account</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Installer Administrator</td>
<td>root</td>
<td>&lt;&lt;hx_install_root_pw&gt;&gt;</td>
</tr>
<tr>
<td>UCS Administrator</td>
<td>admin</td>
<td>&lt;&lt;ucs_admin_pw&gt;&gt;</td>
</tr>
</tbody>
</table>
### Installation

<table>
<thead>
<tr>
<th>Account</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyper-V Local Administrator</td>
<td>root</td>
<td>&lt;&lt;hyperv_local_pw&gt;&gt;</td>
</tr>
<tr>
<td>HyperFlex Administrator</td>
<td>root</td>
<td>&lt;&lt;hx_admin_pw&gt;&gt;</td>
</tr>
<tr>
<td>AD Domain Admin or Service Account</td>
<td>&lt;&lt;administrator&gt;&gt;</td>
<td>&lt;&lt;ad_admin_pw&gt;&gt;</td>
</tr>
</tbody>
</table>

#### Table 35  Example Usernames and Passwords

<table>
<thead>
<tr>
<th>Account</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>HX Installer Administrator</td>
<td>root</td>
<td>Cisco123</td>
</tr>
<tr>
<td>UCS Administrator</td>
<td>admin</td>
<td>Cisco123</td>
</tr>
<tr>
<td>Hyper-V Local Administrator</td>
<td>root</td>
<td>Cisco123</td>
</tr>
<tr>
<td>HyperFlex Administrator</td>
<td>root</td>
<td>Cisco123!!</td>
</tr>
<tr>
<td>AD Domain Admin or Service Account</td>
<td><a href="mailto:administrator@domain.local">administrator@domain.local</a></td>
<td>!QAZ2wsx</td>
</tr>
</tbody>
</table>

### Physical Installation

Install the Fabric Interconnects, the HX-Series rack-mount servers according to their corresponding hardware installation guides listed below.

Cisco UCS 6200 Series Fabric Interconnect:


Cisco UCS 6300 Series Fabric Interconnect:


HX220c M5 Server:


HX240c M5 Server:


### Cabling

The physical layout of the HyperFlex system is described in the Physical Topology section. The Fabric Interconnects and HX-series rack-mount servers need to be cabled properly before beginning the installation activities. The information in this section is provided as a reference for cabling the physical equipment in this Cisco Validated Design environment.
This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps.

The following tables provide an example cabling map to install a Cisco HyperFlex system with four HyperFlex converged servers.

### Table 36  Cisco Nexus 9396PX-A Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9396PX-A</td>
<td>Eth1/15</td>
<td>10GbE</td>
<td>Cisco Nexus 9396PX-B</td>
<td>Eth1/15</td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>10GbE</td>
<td>Cisco Nexus 9396PX-B</td>
<td>Eth1/16</td>
</tr>
<tr>
<td></td>
<td>Eth2/5</td>
<td>40GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth1/26</td>
</tr>
<tr>
<td></td>
<td>Eth2/6</td>
<td>40GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth1/25</td>
</tr>
<tr>
<td></td>
<td>Eth1/31</td>
<td>10GbE</td>
<td>Infra-host-01</td>
<td>Port01</td>
</tr>
<tr>
<td>MGMT0</td>
<td>GbE</td>
<td></td>
<td>GbE management switch</td>
<td>Any</td>
</tr>
</tbody>
</table>

### Table 37  Cisco Nexus 9396PX-B Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9396PX-B</td>
<td>Eth1/15</td>
<td>10GbE</td>
<td>Cisco Nexus 9396PX-A</td>
<td>Eth1/15</td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>10GbE</td>
<td>Cisco Nexus 9396PX-A</td>
<td>Eth1/16</td>
</tr>
<tr>
<td></td>
<td>Eth2/5</td>
<td>40GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth1/26</td>
</tr>
<tr>
<td></td>
<td>Eth2/6</td>
<td>40GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth1/25</td>
</tr>
<tr>
<td></td>
<td>Eth1/31</td>
<td>10GbE</td>
<td>Infra-host-01</td>
<td>Port02</td>
</tr>
<tr>
<td>MGMT0</td>
<td>GbE</td>
<td></td>
<td>GbE management switch</td>
<td>Any</td>
</tr>
</tbody>
</table>

### Table 38  Cisco UCS Fabric Interconnect A Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth1/25</td>
<td>40GbE</td>
<td>Cisco Nexus 9396PX-A</td>
<td>Eth2/6</td>
</tr>
<tr>
<td></td>
<td>Eth1/26</td>
<td>40GbE</td>
<td>Cisco Nexus 9396PX-B</td>
<td>Eth2/5</td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>40GbE</td>
<td>HX Server #1</td>
<td>mLOM Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>40GbE</td>
<td>HX Server #2</td>
<td>mLOM Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>40GbE</td>
<td>HX Server #3</td>
<td>mLOM Port 1</td>
</tr>
</tbody>
</table>
Cisco UCS Installation

This section describes the steps to initialize and configure the Cisco UCS Fabric Interconnects and how to prepare them for the HyperFlex installation.

Cisco UCS Fabric Interconnect A

To configure Fabric Interconnect A, complete the following steps:

1. Make sure the Fabric Interconnect cabling is properly connected, including the L1 and L2 cluster links, and power the Fabric Interconnects on by inserting the power cords.
2. Connect to the console port on the first Fabric Interconnect, which will be designated as the A fabric device. Use the supplied Cisco console cable (CAB-CONSOLE-RJ45-), and connect it to a built-in DB9 serial port, or use a USB to DB9 serial port adapter.
3. Start your terminal emulator software.
4. Create a connection to the COM port of the computer’s DB9 port, or the USB to serial adapter. Set the terminal emulation to VT100, and the settings to 9600 baud, 8 data bits, no parity, and 1 stop bit.
5. Open the connection just created. You may have to press ENTER to see the first prompt.

Table 39  Cisco UCS Fabric Interconnect B Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth1/25</td>
<td>40GbE</td>
<td>Cisco Nexus 9396PX-B</td>
<td>Eth2/6</td>
</tr>
<tr>
<td></td>
<td>Eth1/26</td>
<td>40GbE</td>
<td>Cisco Nexus 9396PX-A</td>
<td>Eth2/5</td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>40GbE</td>
<td>HX Server #1</td>
<td>mLOM Port 2</td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>40GbE</td>
<td>HX Server #2</td>
<td>mLOM Port 2</td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>40GbE</td>
<td>HX Server #3</td>
<td>mLOM Port 2</td>
</tr>
<tr>
<td></td>
<td>Eth1/20</td>
<td>40GbE</td>
<td>HX Server #4</td>
<td>mLOM Port 2</td>
</tr>
<tr>
<td>MGMT0</td>
<td>GbE</td>
<td></td>
<td>GbE management switch</td>
<td>Any</td>
</tr>
<tr>
<td>L1</td>
<td>GbE</td>
<td></td>
<td>Cisco UCS fabric interconnect B</td>
<td>L1</td>
</tr>
<tr>
<td>L2</td>
<td>GbE</td>
<td></td>
<td>Cisco UCS fabric interconnect B</td>
<td>L2</td>
</tr>
</tbody>
</table>
6. Configure the first Fabric Interconnect, using the following example as a guideline:

---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values, complete input till
end of section and answer no when prompted to apply configuration.

Enter the configuration method. (console/gui) ? console
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) \[y\]: y
Enter the password for "admin":
Confirm the password for "admin":
Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) \[n\]: yes
Enter the switch fabric (A/B) \[\]: A
Enter the system name: HXHV-FI-A
Physical Switch Mgmt0 IP address : 10.29.149.203
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPV4 address of the default gateway : 10.29.149.1
Cluster IPv4 address : 10.29.149.205
Configure the DNS Server IP address? (yes/no) \[n\]: yes
  DNS IP address : 10.29.149.222
Configure the default domain name? (yes/no) \[n\]: yes
  Default domain name : hxhvd0m.local
Join centralized management environment (UCS Central)? (yes/no) \[n\]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=HXHV-FI-A
  Enforced Strong Password=no
  Physical Switch Mgmt0 IP Address=10.29.149.203
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=10.29.149.1
  Ipv6 value=0
  DNS Server=10.29.149.222
  Domain Name=hx.lab.cisco.com
  Cluster Enabled=yes
  Cluster IP Address=10.29.149.205
  NOTE: Cluster IP will be configured only after both Fabric Interconnects are ini-
  tialized
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.
Cisco UCS Fabric Interconnect B

To configure Fabric Interconnect B, complete the following steps:

1. Connect to the console port on the first Fabric Interconnect, which will be designated as the B fabric device. Use the supplied Cisco console cable (CAB-CONSOLE-RJ45=), and connect it to a built-in DB9 serial port, or use a USB to DB9 serial port adapter.

2. Start your terminal emulator software.

3. Create a connection to the COM port of the computer’s DB9 port, or the USB to serial adapter. Set the terminal emulation to VT100, and the settings to 9600 baud, 8 data bits, no parity, and 1 stop bit.

4. Open the connection just created. You may have to press ENTER to see the first prompt.

5. Configure the second Fabric Interconnect, using the following example as a guideline:

   ---- Basic System Configuration Dialog ----

   This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps. Type Ctrl-C at any time to abort configuration and reboot system.

   To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

   Enter the configuration method. (console/gui) ? console
   Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be added to the cluster. Continue (y/n) ? y

   Enter the admin password of the peer Fabric interconnect:
   Connecting to peer Fabric interconnect... done
   Retrieving config from peer Fabric interconnect... done
   Peer Fabric interconnect Mgmt0 IPv4 Address: 10.29.149.204
   Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
   Cluster IPv4 address = 10.29.149.205
   Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address
   Physical Switch Mgmt0 IP address : 10.29.149.204
   Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
   Applying configuration. Please wait.
   Configuration file - Ok

Cisco UCS Manager

Log in to the Cisco UCS Manager environment and complete the following steps:

1. Open a web browser and navigate to the Cisco UCS Manager Cluster IP address, for example https://10.29.149.205
2. Click the “Launch UCS Manager” HTML link to open the Cisco UCS Manager web client.

3. At the login prompt, enter “admin” as the username, and enter the administrative password that was set during the initial console configuration.

4. Click No when prompted to enable Cisco Smart Call Home. This feature can be enabled at a later time.

Cisco UCS Configuration

Configure the following ports, settings, and policies in the Cisco UCS Manager interface prior to beginning the HyperFlex installation.

Cisco UCS Firmware

Your Cisco UCS firmware version should be correct as shipped from the factory, as documented in the Software Components section. This document is based on Cisco UCS infrastructure, B-series bundle, and C-Series bundle software versions 3.2(3d). If the firmware version of the Fabric Interconnects is older than this version, the firmware must be upgraded to match the requirements prior to completing any further steps.

To upgrade the Cisco UCS Manager version, the Fabric Interconnect firmware, and the server bundles, refer to these instructions:


NTP

To synchronize the Cisco UCS environment time to the NTP server, complete the following steps:

1. In Cisco UCS Manager, click the Admin button on the left-hand side.

2. In the navigation pane, select All > Time Zone Management, and click the carat next to Time Zone Management to expand it.

3. Click Timezone.

4. In the Properties pane, select the appropriate time zone in the Time Zone menu.

5. Click Add NTP Server.
6. Enter the NTP server IP address and click OK.
7. Click OK.
8. Click Save Changes and then click OK.

**Uplink Ports**

The Ethernet ports of a Cisco UCS Fabric Interconnect are all capable of performing several functions, such as network uplinks or server ports, and more. By default, all ports are unconfigured, and their function must be defined by the administrator. To define the specified ports to be used as network uplinks to the upstream network, complete the following steps:

1. In Cisco UCS Manager, click the Equipment button on the left-hand side.
2. Select Fabric Interconnects > Fabric Interconnect A > Fixed Module or Expansion Module as appropriate > Ethernet Ports.
3. Select the ports that are to be uplink ports, right click them, and click Configure as Uplink Port.
4. Click Yes to confirm the configuration, and click OK.
5. Select Fabric Interconnects > Fabric Interconnect B > Fixed Module or Expansion Module as appropriate > Ethernet Ports.
6. Select the ports that are to be uplink ports, right-click them, and click Configure as Uplink Port.
7. Click Yes to confirm the configuration and click OK.
8. Verify all the necessary ports are now configured as uplink ports, where their role is listed as “Network.”

**Figure 40  Uplinks Ports**

**Uplink Port Channels**

If the Cisco UCS uplinks from one Fabric Interconnect are to be combined into a port channel or vPC, you must separately configure the port channels, which will use the previously configured uplink ports. To configure the necessary port channels in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN button on the left-hand side.
2. Under LAN > LAN Cloud, click the carat to expand the Fabric A tree.
3. Right-click Port Channels underneath Fabric A, then click Create Port Channel.
4. Enter the port channel ID number as the unique ID of the port channel (this does not have to match the port-channel ID on the upstream switch).
5. Enter the name of the port channel.
6. Click Next.
7. Click each port from Fabric Interconnect A that will participate in the port channel, and click the >> button to add them to the port channel.
8. Click Finish.
9. Click OK.
10. Under LAN > LAN Cloud, click the carat to expand the Fabric B tree.
11. Right-click Port Channels underneath Fabric B, then click Create Port Channel.
12. Enter the port channel ID number as the unique ID of the port channel (this does not have to match the port-channel ID on the upstream switch).
13. Enter the name of the port channel.
14. Click Next.
15. Click each port from Fabric Interconnect B that will participate in the port channel and click the >> button to add them to the port channel.
16. Click Finish.
17. Click OK.
18. Verify the necessary port channels have been created. It can take a few minutes for the newly formed port channels to converge and come online.

Figure 41  Uplink Port Channels

Server Ports

The Ethernet ports of a Cisco UCS Fabric Interconnect connected to the rack-mount servers must be defined as server ports. When a server port is activated, the connected server or chassis will begin the discovery process shortly afterwards. Rack-mount servers are automatically numbered in Cisco UCS Manager in the order which they are first discovered. For this reason, it is important to configure the server ports sequentially in the order you wish the physical servers and/or chassis to appear within Cisco UCS Manager. For example, if you installed your servers in a cabinet or rack with server #1 on the bottom, counting up as you go higher in the cabinet or rack, then you need to enable the server ports to the bottom-most server first, and enable them one-by-one as you move upward. You must wait until the server appears in the Equipment tab of Cisco UCS Manager before configuring the ports for the next server.
Auto Configuration

A new feature in Cisco UCS Manager 3.1(3a) and later is Server Port Auto-Discovery, which automates the configuration of ports on the Fabric Interconnects as server ports when a Cisco UCS rack-mount server is connected to them. The firmware on the rack-mount servers must already be at version 3.1(3a) or later in order for this feature to function properly. Enabling this policy eliminates the manual steps of configuring each server port, however it does configure the servers in a somewhat random order. For example, the rack-mount server at the bottom of the stack, which you may refer to as server #1, and you may have plugged into port 1 of both Fabric Interconnects, could be discovered as server 2, or server 5, etc. In order to have fine control of the rack-mount server or chassis numbering and order, the manual configuration steps listed in the next section must be followed.

To configure automatic server port definition and discovery, complete the following steps:

1. In Cisco UCS Manager, click the Equipment button on the left-hand side.
2. In the navigation tree, under Policies, click Port Auto-Discovery Policy.
3. In the properties pane, set Auto Configure Server Port option to Enabled.
4. Click Save Changes.
5. Click OK.
6. Wait for a brief period, until the rack-mount servers appear in the Equipment tab underneath Equipment > Rack Mounts > Servers, or the chassis appears underneath Equipment > Chassis.

Manual Configuration

To manually define the specified ports to be used as server ports and have control over the numbering of the servers, complete the following steps:

1. In Cisco UCS Manager, click the Equipment button on the left-hand side.
2. Select Fabric Interconnects > Fabric Interconnect A > Fixed Module or Expansion Module as appropriate > Ethernet Ports.
3. Select the first port that is to be a server port, right click it, and click Configure as Server Port.
4. Click Yes to confirm the configuration and click OK.
5. Select Fabric Interconnects > Fabric Interconnect B > Fixed Module or Expansion Module as appropriate > Ethernet Ports.
6. Select the matching port as chosen for Fabric Interconnect A that is to be a server port, right-click it, and click Configure as Server Port.
7. Click Yes to confirm the configuration and click OK.
8. Wait for a brief period, until the rack-mount server appears in the Equipment tab underneath Equipment > Rack Mounts > Servers, or the chassis appears underneath Equipment > Chassis.
9. Repeat Steps 1–8 for each pair of server ports, until all rack-mount servers and chassis appear in the order desired in the Equipment tab.

Server Discovery

As previously described, when the server ports of the Fabric Interconnects are configured and active, the servers connected to those ports will begin a discovery process. During discovery, the servers’ internal hardware inventories are collected, along with their current firmware revisions. Before continuing with the HyperFlex installation processes, which will create the service profiles and associate them with the servers, wait for all of the servers to finish their discovery process and to show as unassociated servers that are powered off, with no errors.

Deploying HX Data Platform Installer on Hyper-V Infrastructure

To deploy HX Data Platform Installer using Microsoft Hyper-V Manager to create a HX Data Platform Installer virtual machine, complete the following steps:

1. Locate and download the HX Data Platform Installer.vhdx zipped file (for example, Cisco-HX-Data-Platform-Installer-v3.0.1c-29681-hyperv.vhdx) from the Cisco Software Downloads site.
2. Extract the zipped folder to your local computer and copy the .vhdx file to the Hyper-V host where you want to host the HX Data Platform Installer. For example, \hyp-v-host01\....\HX-Installer\Cisco-HX-Data-Platform-Installer-v3.0.1c-29681-hyperv.vhdx
3. In Hyper-V Manager, navigate to one of the Hyper-V servers.
4. Select the Hyper-V server, and right-click and select New > Create a virtual machine. The Hyper-V Manager New Virtual Machine Wizard displays.

5. In the Before you Begin page, click Next.
6. In the Specify Name and Location page, enter a name and location for the virtual machine where the virtual machine configuration files will be stored. Click Next.
As a best practice, store the VM together with the .vhdx file.


8. In the Assign Memory page, set the startup memory value to 4096 MB. Click Next.
9. In the **Configure Networking** page, select a network connection for the virtual machine to use from a list of existing virtual switches. Click **Next**.

10. In the **Connect Virtual Hard Disk** page, select **Use an existing virtual hard disk**, and browse to the folder on your Hyper-V host that contains the `.vhdx` file. Click **Next**.
11. In the Summary page, verify that the list of options displayed are correct. Click Finish.

12. After the VM is created, power it ON, and launch the GUI.

13. Right-click the VM and choose Connect.


15. When the VM is booted, make a note of the URL (IP address of the VM). You will need this information in the following steps in the installation.

Assign a Static IP Address to the HX Data Platform Installer VM

During a default installation of the VM, the HX Installer will try and automatically obtain an IP address using DHCP. To ensure that you have the same IP address at every boot, you can assign a static IP address on the VM.

To configure your network interface (/etc/network/interfaces) with a static IP address. Make sure you change the relevant settings to suit your network and complete the following steps:
1. Log in to your Installer machine via the Hyper-V Console.

2. Open the /etc/network/interfaces file and add the following lines to the file:
   ```
   auto eth0 # eth0 interface
   iface eth0 inet static # configures static IP for the eth0 interface
   address XX.XX.XX.XX # Static IP address for the installer VM
   netmask 255.255.0.0 # netmask for the Static IP address
   gateway XX.XX.X.X # gateway for the Static IP address
   metric 100
   dns-nameservers XX.XX.X.XXX #DNS name servers used by the HX installer
   dns-search <DNS_Search_Name>.local # DNS search domain name used by the installer
   ```

3. Save the file.

4. Reboot the VM for changes to take effect.

5. Verify the settings as shown in the following figures.

**Figure 50** Show Interfaces

```
root@HyperFlex-Installer:~# ifconfig
eth0   Link encap:Ethernet  HWaddr 00:15:5d:fe:33:0e
       inet addr:10.104.252.40 Bcast:10.104.252.255 Mask:255.255.255.0
       inet6 addr: fe80::215:5dff:feec:330e/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:9886615 errors:0 dropped:3 overruns:0 frame:0
       TX packets:1102137 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:915397262 (915.8 MB) TX bytes:1239840970 (12.3 GB)
```

**Figure 51** Routing Table

```
root@HyperFlex-Installer:~# route -n
Kernel IP routing table
    Destination     Gateway         Genmask     Flags Metric Ref    Use Iface
0.0.0.0          10.104.252.1    0.0.0.0     UG  0    0      0 eth0
10.104.252.0     0.0.0.0         255.255.255.0 U    0    0      0 eth0
239.255.255.253  0.0.0.0         255.255.255.255 UH   0    0      0 eth0
```

**Figure 52** /etc/resolv.conf file for Nameserver and Search Domain

```
root@HyperFlex-Installer:~# cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.29.149.222
search HXHVDOM.LOCAL
```

**HyperFlex Installation**

The HyperFlex installer will guide you through the process of setting up your cluster. The Windows OS is not factory installed and requires the customer to provide media for the installation. Before you begin with the HX installation, make sure Windows Server 2016 is installed on the HX nodes; for more information about OS installation, refer to Appendix B section, “Install Microsoft Windows Server 2016.” The HyperFlex installation for Microsoft Hyper-V is completed in two phases using the customized version of the HX installation workflow:
Installation

- In phase 1 of the HX installation, only ‘Run UCS Configuration” workflow is executed to prepare and configure the Cisco UCS environment, and
- In phase 2 of HX installation, the remaining three workflows (Hypervisor Configuration, HX Deploy Software and Create HX Cluster) are executed to complete the deployment of HX Cluster.

HyperFlex Installation - Phase 1

This phase of HyperFlex installation will guide you through the process of Configuring Cisco UCS Manager using HyperFlex installer.

Configure Cisco UCS Manager using HX Installer

1. Launch the HX Data Platform Installer. In a browser, enter the URL for the VM where HX Data Platform Installer was installed.
2. Use the credentials: username: root, password: Cisco123

   Important! Systems ship with a default password of Cisco123 that must be changed during installation; you cannot continue installation unless you specify a new user supplied password.
3. Read the EULA. Click I accept the terms and conditions.
4. Verify the product version listed in the lower right corner is correct. This version must be 3.0(1c) or later. Enter the credentials and click Login.

   [Figure 53 Cisco HX Data Platform Installer Login Page]

5. From the HX Data Platform Installer Workflow page, select I know what I’m doing, let me customize my workflow.
6. On the next screen, click Run UCS Manager Configuration and then click Continue.
   Do not choose any other workflow options.

7. Click Confirm in the popup that displays.
Installation

8. Enter the UCS Manager credentials.

The right side of the page is unused. Further in the setup process a configuration JSON is saved, so in subsequent installations the JSON file can be imported to add the data quickly.

9. Click Confirm and Proceed to bypass the warning. Complete the following fields for Cisco UCS Manager.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Manager Host Name</td>
<td>FQDN or the VIP address of Cisco UCS Manager</td>
</tr>
<tr>
<td>Cisco UCS Manager User Name</td>
<td>Administrator user and password or an user with</td>
</tr>
<tr>
<td>and Password</td>
<td>Cisco UCS Manager admin rights</td>
</tr>
</tbody>
</table>

Figure 56   HyperFlex Installer – Cisco UCS Manager Credentials

10. Click Continue.

The installer will connect to Cisco UCS Manager and query for available servers. The configuration pane is populated as the installer progresses. You can at any time save the JSON file so you can re-use it for subsequent installations. This feature works on all the different workflows in the installer. After the query finishes a screen displays showing the available servers.
11. Choose all the servers that you want to install in the cluster and click **Continue**.

   HyperFlex for Hyper-V only supports M5 Servers.

12. In the VLAN Configuration section, enter the details as shown in the following screenshot.

13. HyperFlex needs to have at least 4 VLANs to function; each VLAN needs to be on different IP subnets and extended from the fabric interconnects to the connecting uplink switches, to make sure that traffic can flow from Primary Fabric Interconnect (Fabric A) to Subordinate Fabric Interconnect (Fabric B).

   Do not use vlan 1 as it is not best practice and can cause issues with disjoint layer 2.

   vm-network can be multiple VLANs added as a comma separated list.

   Renaming the 4 core networks is not supported.

Figure 58 shows the various fields in the VLAN Configuration pane where you need to enter values.
14. In the MAC Pool and ‘hx-ext-mgmt’ IP Pool for Out-of-band CIMC sections, enter the details as shown below.

The Out-Of-Band network needs to be on the same subnet as the Cisco UCS Manager.

You can add multiple blocks of addresses as a comma separated line.

iSCSI Storage and FC Storage are used for adding external storage to the HyperFlex cluster.

---

iSCSI Storage and FC Storage are currently not supported for Cisco HyperFlex with Microsoft Hyper-V.

15. Use the details from the table below to complete the fields in the Advanced section.

---

The Cisco UCS B and C packages must exist on the Fabric interconnect otherwise the installation will fail. If the right version is not available in the drop-down list, then upload it to Cisco UCS Manager before continuing.

---

The supported version for HyperFlex Hyper-V is 3.2(3e).
Installation

16. Click Start. The installer validates your input and then begins configuring Cisco UCS Manager.

When the HX Data Platform Installer is finished, then you are ready to proceed to next step of installing the Windows OS

![HyperFlex Installer – Cisco UCS Manager Configuration Progress](image)

HyperFlex Installation - Phase 2

After the installation of Windows OS, use the customized workflow of HX installer and select the remaining three options: Run Hypervisor Configuration, HX Deploy Software and Create HX Cluster to continue and complete the deployment of HyperFlex Cluster.

To deploy HX cluster, complete the following steps:

- Before continuing on the following steps, make sure Windows Server 2016 is installed and Cisco HyperFlex driver image is applied on all HX nodes. To install Windows Server 2016 OS and apply Cisco HyperFlex driver image, refer to the Appendix B section “Install Microsoft Windows Server 2016.”

1. Open the HX Data Platform Installer and log in.

2. You might need to “start over” since the previous workflow was finished. Click the gear icon in the top right corner and select Start Over.

3. In the main menu, select I know what I'm doing, let me customize my workflow. In the Warning dialog box, click Confirm and Proceed.
4. Select Run Hypervisor Configuration, Deploy HX Software and Create HX Cluster and click Continue.

5. Enter the information for the Cisco UCS Manager, Domain Information, and Hypervisor Credentials. Optionally, you can import a JSON file that has the configuration information, except for the appropriate passwords.
6. Click Continue

7. Select the Unassociated HX server models that are to be used in the new HX cluster and click Continue. If the Fabric Interconnect server ports were not enabled in the earlier step, you have the option to enable them here to begin the discovery process by clicking the Configure Server Ports link.

Using this option of enabling server ports within HX installer, limits fine control of server order sequence, which is possible in manual configuration. The server discovery can take several minutes to complete, and it will be necessary to periodically click the Refresh button to see the unassociated servers appear once discovery is completed.
8. In the Cisco UCS Manager Configuration section, enter the network information as you have done in the Error! Reference source not found. section and make sure the data is the same. Click Continue.

When deploying a second or any additional clusters, you must put them into a different sub-org, use a different MAC Pool prefix, a unique pool of IP addresses for the CIMC interfaces, and you should also create new VLAN names for the additional clusters. Even if reusing the same VLAN ID, it is prudent to create a new VLAN name to avoid conflicts.

9. In the Hypervisor Configuration section, enter the subnet mask, gateway, and IP addresses and hostnames for the Hypervisors. The IP addresses will be assigned via Serial over LAN (SoL) through Cisco UCS Manager to the Hyper-V host systems as their management IP addresses. Click Continue

If you leave the checkbox Make IP Addresses and Hostnames Sequential as checked then the installer will automatically fill the rest of the servers sequentially.
10. Assign the additional IP addresses for the Management and Data networks as well as the cluster IP addresses, then click Continue.
11. Enter the HX Cluster Name and Replication Factor setting.

12. Enter the Password that will be assigned to the Controller VMs.

13. Enter the System Services information for DNS, NTP, and Time Zone. Make sure to use the Active Directory domain name for NTP.

14. Enable Connected Services in order to enable management via Cisco Intersight, and enter the email address to receive service ticket alerts, then scroll down.

15. Under Advanced Configuration, validate that VDI is not checked (applicable to hybrid nodes only). Jumbo Frames should be enabled to ensure the best performance, unless the upstream network is not capable of being configured to transmit jumbo frames. It is not necessary to select Clean up disk partitions for a new cluster installation, but an installation using previously used converged nodes should have the option checked.

16. Click Start.
17. Validation of the configuration will now start. If there are warnings, you can review them and click “Skip Validation” if the warnings are acceptable. If there are no warnings, the installer will automatically continue on to the configuration process.

**Figure 66  HyperFlex Installer – Cluster Configuration**

18. After the pre-installation validations, the HX installer will proceed to complete the deployment and perform all the steps listed at the top of the screen along with their status.
19. Review the Summary screen after the install completes by selecting Summary on the top right of the window.
20. After the install completes, you may export the cluster configuration by clicking the downward arrow icon in the top right of the screen. Click OK to save the configuration to a JSON file. This file can be imported to save time if you need to rebuild the same cluster in the future, and stored as a record of the configuration options and settings used during the installation.

21. After the installation completes, you can click the Launch HyperFlex Connect button to immediately log in to the HTML5 management GUI.
Post Installation Tasks

Create Datastores

Create a datastore for storing the virtual machines. This task can be completed by using the HyperFlex Connect HTML management webpage. The Datastores created using HX Connect creates a SMB share which the HyperFlex Hyper-V nodes can use it to store virtual machine files. To configure a new datastore via the HyperFlex Connect webpage, complete the following steps:

- Cisco recommends 8K block size for best performance and as few datastores as possible for ease of management.

1. Use a web browser to open the HX cluster IP management URL.
2. Enter the credentials.
3. Click Login.
4. Click Datastores in the left pane and click Create Datastore.
5. In the popup, enter the Datastore Name and size. For most applications, leave the Block Size at the default of 8K. Only dedicated Virtual Desktop Infrastructure (VDI) environments should choose the 4K Block Size option.

6. Click Create Datastore.

Constrained Delegation (Optional)

Windows provides a safer form of delegation that could be used by services. When it is configured, constrained delegation restricts the services to which the specified server can act on the behalf of a user. In other words. Constrained Delegation gives granular control over impersonation. When the remote management requests are made to the Hyper-V hosts, it needs to make those requests to the storage on
behalf of the caller. This is allowed if that host is trusted for delegation for the CIFS service principal of HX Storage.

Constrained Delegation requires that the option for the security setting User Account Control: Behavior of the elevation prompt for Administrators in Admin Approval Mode is set to Elevate without Prompting. This will prevent the global AD policy from overriding policy on HX OU.

This step must be performed only if Constrained Delegation was not configured during initial installation. It is recommended that you perform this procedure using the HX Installer and not as part of post-installation.

To configure constrained delegation using domain administrator, complete the following steps on each Hyper-V host in the HX Cluster and also on management hosts (with RSAT tools from where you want to remotely perform administrator tasks):

1. Open the Active Directory Users and Computers snap-in. (From Server Manager, select the server if it is not selected, click Tools >> Active Directory Users and Computers).
2. From the navigation pane in Active Directory Users and Computers, select the domain and double-click the Computers folder.
3. From the Computers folder, right-click the computer account of the source server and then click Properties.

Figure 74  Active Directory Users and Computers

4. From the Properties tab, click the Delegation tab.
5. On the delegation tab, select Trust this computer for delegation to the specified services only and then select Use any authentication protocol.
6. Click Add.
7. From Add Services, click Users or Computers.
8. From Select Users or Computers, type the name of the destination server.
9. Click Check Names to verify it and then click OK.
10. From Add Services, in the list of available services, do the following and then click OK:
   a. To move virtual machine storage, select `cifs`. This is required if you want to move the storage along with the virtual machine, as well as if you want to move only a virtual machine's storage. If the server is configured to use SMB storage for Hyper-V, this should already be selected.
   b. To move virtual machines, select Microsoft Virtual System Migration Service.
11. On the Delegation tab of the Properties dialog box, verify that the services you selected in the previous step are listed as the services to which the destination computer can present delegated credentials. Click OK.

12. From the Computers folder, select the computer account of the destination server and repeat the process. In the Select Users or Computers dialog box, be sure to specify the name of the source server.

Assign IP Addresses to Live Migration and VM Network Interfaces

To assign a static IP address to Live Migration and Network Interfaces, log into each Hyper-V node and execute the following commands in PowerShell, complete the following steps:

1. Use the following PowerShell command to check if there is vSwitch created for Live Migration network on Hyper-V hosts by the HX installer.
   
   Get-VMSwitch
2. Remove the vSwitch named ‘vswitch-hx-livemigration’ using the following PowerShell command.

   ```powershell
   Remove-VMSwitch -Name 'vswitch-hx-livemigration'
   ```

3. Assign a static IP address to the teamed interface named “team-hx-livemigration” using the following PowerShell command.

   ```powershell
   New-NetIPAddress -IfAlias "team-hx-livemigration" -IPAddress 192.168.73.127 -PrefixLength 24
   ```

4. This step is optional. If there is a requirement for the Hyper-V host also to communicate on VM network, then assign a static IP address to “team-hx-livemigration” using the following PowerShell command.

   ```powershell
   New-NetIPAddress -IfAlias "vswitch-hx-vm-network" -IPAddress 192.168.74.21 -PrefixLength 24
   ```

Rename the Cluster Network in Windows Failover Cluster - Optional

To rename the default cluster network names assigned during cluster creation to more meaningful names, execute the following PowerShell commands from any one HyperFlex Hyper-V host:
1. Execute the “Get-ClusterNetwork” and “Get-ClusterNetworkInterface” as shown below to view information on the cluster network.

![Figure 80 PowerShell – Get Cluster Network](image)

2. Execute the below PowerShell command to rename the cluster networks.

```powershell
Get-ClusterNetwork | Where-Object {$_._Address -eq "10.29.149.0"}).Name = "hx-inband-mgmt"

(Get-ClusterNetwork | Where-Object {$_._Address -eq "192.168.11.0"}).Name = "hx-storage-data"

(Get-ClusterNetwork | Where-Object {$_._Address -eq "192.168.73.0"}).Name = "LiveMigration"

(Get-ClusterNetwork | Where-Object {$_._Address -eq "172.18.0.0"}).Name = "vm-network"
```

![Figure 81 PowerShell – Rename the Cluster Network](image)

**Configure the Windows Failover Cluster Network Roles**

Cluster networks are automatically configured during the cluster creation. To manually configure the cluster network roles based on their type of function, execute the following PowerShell commands on any one HyperFlex Hyper-V host:
Execute the following PowerShell commands to configure the cluster networks roles:

(Get-ClusterNetwork -Name "hx-inband-mgmt").Role = 3
(Get-ClusterNetwork -Name "hx-storage-data").Role = 0
(Get-ClusterNetwork -Name "LiveMigration").Role = 1
(Get-ClusterNetwork -Name "vm-network").Role = 0

**Figure 82   PowerShell – Configure Cluster Network Roles**

Role = 0 to disable cluster communication
Role = 1 to enable only cluster communication
Role = 3 to enable both cluster & client communication

**Figure 83   Failover Cluster Manager - Networks**

Configure the Windows Failover Cluster Network for Live Migration

To make sure that you are using the appropriate cluster network for Live Migration traffic configure the Live Migration settings by completing the following steps:

Execute the PowerShell command shown below to configure the cluster network for live migration traffic:

Get-ClusterResourceType -Name "Virtual Machine" | Set-ClusterParameter -Name MigrationExcludeNetworks -Value ([String]::Join(";", (Get-ClusterNetwork | Where-Object {$_._Name -ne "LiveMigration"}).ID))

**Figure 84   PowerShell – Configure Live Migration Network**
Create Folders on the HX Datastore

To create folders on the newly created HX Datastore, complete the following steps:

1. To create a folder log in to a HyperFlex Hyper-V node and execute the below command:
   ```bash
   mkdir \uxxhvsmb.hxhvdom.local\HXDS1\<folder Name>
   ```

2. Create folders for different purposes and requirements.

Configure the Default Folder to Store VM Files on Hyper-V

By default Hyper-V stores VM files at the following specified location:

- “C:\ProgramData\Microsoft\Windows\Hyper-V” for virtual machine configuration files
Installation

- “C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks” for virtual hard drives

To store the virtual machine files on the newly created highly available HX Datastore as the default folder. Complete the following step on each HyperFlex Hyper-V hosts:

Use the following PowerShell command to set/change the Hyper-V default store location for virtual hard disk and virtual machine configuration files:

```
SET-VMHOST -virtualharddiskpath "\<FQDN_SMB_AccessPoint><Datastore_Name><Folder_Name>"
```

```
SET-VMHOST -virtualmachinopath "\<FQDN_SMB_AccessPoint><Datastore_Name><Folder_Name>"
```

Figure 87  PowerShell – Configure VM Files Store Location

Validate the Windows Failover Cluster Configuration

It is a good practice to validate the Windows failover cluster by running the Validate a Configuration Wizard from the Failover Cluster Manager, or the Test-Cluster Windows PowerShell cmdlet and fix any errors or warnings reported in the results page. Figure 89 shows the command to run the cluster validation.
**Configure Quorum in Windows Server Failover Cluster**

The quorum is automatically configured during the creation of a new cluster based on the number of nodes and the availability of shared storage. However, as a best practice run the cluster validation tool as shown in the above section and review the quorum configuration and fix any warnings related to quorum configuration.

Review the information about quorum resources using the “Get-ClusterQuorum” PowerShell cmdlet or from the summary page of failover cluster manager as shown below:

**Figure 90** PowerShell – Get Cluster Quorum

**Figure 91** Failover Cluster Manager

Execute the below PowerShell command to configure the cluster quorum by placing the witness on a file share residing on the HX Datastore:

```
Set-ClusterQuorum -NodeAndFileShareMajority "\\fileserver\fsw"
```

**Figure 92** PowerShell – Configure Cluster Quorum
The file server can run on a virtual or physical machine as long as it is not hosted on the same cluster that uses the file share witness.

**Initial Tasks and Testing**

In order to perform initial testing and learn about the features in the HyperFlex cluster, create a test virtual machine stored on your new HX datastore in order to take a snapshot and perform a cloning operation.

**Ready Clones**

To create few clones of our test virtual machine, download the Cisco HyperFlex Data Platform Hyper-V ReadyClone PowerShell Script.

To create the Ready Clones, complete the following steps:

1. Log into a HX Hyper-V node or a management station with RSAT tools
2. Open Powershell and execute the downloaded script as shown below.
3. Input the VMName, ClonePrefix, CloneCount and enter to create the clones in seconds.

4. The command provided below with the new switch, creates a clustered virtual machine; a virtual machine that can be failed over if necessary to a different server in the failover cluster.

    HX-PS-ReadyClone.ps1 -addtocluster $true

**Auto-Support and Notifications**

Auto-Support should be enabled for all clusters during the initial HyperFlex installation. Auto-Support enables Call Home to automatically send support information to Cisco TAC, and notifications of tickets to the email address specified. If the settings need to be modified, they can be changed in the HyperFlex Connect HTML management webpage.

A list of events that automatically open a support ticket with Cisco TAC are as follows:

- Cluster Capacity Changed
- Cluster Unhealthy
- Cluster Health Critical
- Cluster Read Only
- Cluster Shutdown
- Space Warning
- Space Alert
- Space Critical
- Disk Blacklisted
- Infrastructure Component Critical
Installation

- Storage Timeout

To change Auto-Support settings, complete the following steps:

1. From the HyperFlex Connect webpage, click the gear shaped icon in the upper right-hand corner, and click Auto-Support Settings.
2. Enable or disable Auto-Support as needed.
3. Enter the email address to receive alerts when Auto-Support events are generated.
4. Enable or disable Remote Support as needed. Remote support allows Cisco TAC to connect to the HX cluster and accelerate troubleshooting efforts.
5. Enter in the information for a web proxy if needed.
6. Click OK.

**Figure 95  HyperFlex Connect – Auto Support Settings**

Email notifications that come directly from the HyperFlex cluster can also be enabled.

To enable direct email notifications, complete the following steps:

1. From the HyperFlex Connect webpage, click the gear shaped icon in the upper right-hand corner, and click Notifications Settings.
2. Enter the DNS name or IP address of the outgoing email server or relay, the email address the notifications will come from, and the recipients.
3. Click OK.
Smart Licensing

HyperFlex 2.5 and later utilizes Cisco Smart Licensing, which communicates with a Cisco Smart Account to validate and check out HyperFlex licenses to the nodes, from the pool of available licenses in the account. At the beginning, Smart Licensing is enabled but the HX storage cluster is unregistered and in a 90-day evaluation period or EVAL MODE. For the HX storage cluster to start reporting license consumption, it must be registered with the Cisco Smart Software Manager (SSM) through a valid Cisco Smart Account. Before beginning, verify that you have a Cisco Smart account, and valid HyperFlex licenses are available to be checked out by your HX cluster.

To create a Smart Account, go to Create Smart Accounts.

To activate and configure smart licensing, complete the following steps:

1. Log into a controller VM. Confirm that your HX storage cluster is in Smart Licensing mode by entering the following:

   stcli license show status
Feedback will show Smart Licensing is ENABLED, Status: UNREGISTERED, and the amount of time left during the 90-day evaluation period (in days, hours, minutes, and seconds).

2. Navigate to Cisco Software Central (https://software.cisco.com/) and log in to your Smart Account.
3. From Cisco Smart Software Manager, generate a registration token.
4. In the License pane, click Smart Software Licensing to open Cisco Smart Software Manager.
5. Click Inventory.
6. From the virtual account where you want to register your HX storage cluster, click General, and then click New Token.
7. In the Create Registration Token dialog box, add a short Description for the token, enter the number of days you want the token to be active and available to use on other products, and check Allow export-controlled functionality on the products registered with this token.
8. Click Create Token.
9. From the New ID Token row, click the Actions drop-down list, and click Copy.
10. Log into a controller VM.
11. Register your HX storage cluster, where idtoken-string is the New ID Token from Cisco Smart Software Manager.
# stcli license register --idtoken idtoken-string

12. Confirm that your HX storage cluster is registered.
   # stcli license show summary
HyperFlex Connect

Cisco HyperFlex Connect provides robust, secure, and simple management in an intuitive user interface. It lets you manage and monitor your clusters anywhere, anytime, and delivers metrics to support your entire HyperFlex management lifecycle. HyperFlex Connect is an HTML5 web-based GUI tool which runs on all of the HX nodes, and is accessible via the cluster management IP address.

To manage the HyperFlex cluster using HyperFlex Connect, complete the following steps:

1. Using a web browser, open the HyperFlex cluster’s management IP address via HTTPS, for example, https://10.29.149.230
2. Enter a local credential, such as local/root, and the password.
3. Click Login.
4. The Dashboard view will be shown after a successful login.

Figure 98  Cisco HyperFlex Connect – Login Page
**Dashboard**

From the Dashboard view, the following elements are presented:

- Cluster operational status, overall cluster health, and the cluster’s current node failure tolerance.
- Cluster storage capacity, used and free space, compression and deduplication savings, and overall cluster storage optimization statistics.
- Cluster size and individual node health.
- Cluster IOPs, storage throughput, and latency for the past 1 hour.

**Monitor**

HyperFlex Connect provides for additional monitoring capabilities, including:

- Event Log: The cluster event log can be viewed, specific events can be filtered for, and the log can be exported.
- Activity Log: Recent job activity, such as ReadyClones can be viewed and the status can be monitored.
The historical and current performance of the HyperFlex cluster can be analyzed via the built-in performance charts. The default view shows read and write IOPs, bandwidth, and latency over the past 1 hour for the entire cluster. Views can be customized to see individual nodes or datastores, and change the timeframe shown in the charts.

HyperFlex Connect presents several views and elements for managing the HyperFlex cluster:
- System Information: Presents a detailed view of the cluster configuration, software revisions, hosts, disks, and cluster uptime. Support bundles can be generated to be shared with Cisco TAC when technical support is needed. Views of the individual nodes and the individual disks are available. In these views, nodes can be placed into HX Maintenance Mode, and disks can be securely erased, as described later in this document.

- Datastores: Presents the datastores present in the cluster, and allows for datastores to be created, mounted, unmounted, edited or deleted, as described earlier in this document as part of the cluster setup.

- Upgrade: Upgrades to the HXDP software, and Cisco UCS firmware can be initiated from this view.

**Figure 102  Cisco HyperFlex Connect – System Information**

**Upgrade the HX Data Platform**

To upgrade HX Data Platform software to a latest version, complete the following steps

1. Download the “Cisco HyperFlex Data Platform Upgrade Bundle for upgrading existing clusters from previous release”. For example “storfs-packages-3.0.1c-29681.tgz”

2. From a browser, launch HX Connect and log in.

3. In the HX Connect web page, click Upgrade as shown in below.
4. In the Select Upgrade Type page, select the HX Data Platform and click Continue.

5. In the Enter Credentials Page, drag or browse the file downloaded in step 1 and click Upgrade.
After validating Upgrade and Preparing Upgrade, the Upgrade process begins.

Microsoft Hyper-V Manager

Hyper-V hosts in a Cisco HyperFlex Systems can be managed both remotely and locally using the Hyper-V Manager. It’s installed when you install the Hyper-V Management Tools, which you can do either through a full Hyper-V installation or a tools-only installation on a remote Windows 10 or 2016 Server.
To manage HyperFlex Hyper-V nodes from a remote management host, complete the following steps:

1. Install the RSAT tools for Hyper-V using the following PowerShell command:
   ```powershell
   Install-WindowsFeature rsat-hyper-v-tools
   ```
2. Configure the remote management host with constrained delegation as described in the above “Post Installation Task > Constrained Delegation” section.
3. If the remote management host with RSAT tools is outside the HX cluster AD domain, pointing to the same DNS server and host file mapping between HyperFlex SMB namespace and Cluster management IP (CIP) may be required for successful name resolution. For example, add the following entry to the hosts file on the (remote) machine running Hyper-V manager/Failover Cluster Manager/SCVMM Console. Host file in windows is located here – C:\Windows\System32\drivers\etc\hosts
   
   ```plaintext
   cluster_mgmt_ip   \smb_namespace_name\datastore_name
   10.29.149.235     \hxcluster.company.com\ds1
   ```

   Basic management functions like changing the default store location for VM files and creating VMs are described in the following sections. For more information about managing Hyper-V using Hyper-V manager refer to the Microsoft website.

**Change the Default Location to Store the VM Files using Hyper-V Manager**

1. Open the Server Manager dashboard and click Tools. Click Hyper-V Manager. The Hyper-V Manager console appears.

**Figure 107** Hyper-V Manager – Connect to Server

```
Hyper-V Manager

File  Action  View  Help

Hyper-V Manager

Introduction

A virtualization server is a physical computer that provides the resources required to run virtual machines. You can use Hyper-V Manager to create, configure, and manage the virtual machine on the local computer.

Actions

Connect to Server

View

Help
```

2. In the left pane, select Hyper-V Manager and click Connect to Server....

**Figure 108** Hyper-V Manager – Select Computer

```
Select Computer

Connect to virtualization server

- Local computer

- Another computer: [text field]

- Connect as another user: [text field]

- Set User...

OK  Cancel
```
3. In the Select Computer dialog box, select Another computer and type in the name of the Hyper-V node (for example, HXHV1) that belongs to the Hyper-V cluster. Click OK.

4. Repeat these steps for each Hyper-V node in the HyperFlex cluster.

5. Select a Hyper-V server and click the Hyper-V settings and change the default folder location to store the virtual hard disk and virtual machine files as shown below.

Create Virtual Machines using Hyper-V Manager

To create Virtual machines using the Hyper-V manager, complete the following steps:

1. Open Hyper-V Manager from the Server Manager > Tools.

2. Select a Hyper-V server, and right-click and select New > Create a virtual machine. The Hyper-V Manager New Virtual Machine wizard displays.
3. In the Before you Begin page, click Next.

4. In the Specify Name and Location page, enter a name for the virtual machine configuration file. The location for the virtual machine click Next.

5. In the Specify Generation page, choose either Generation 1 or Generation 2.

6. In the Assign Memory page, set the start memory value 2048 MB. Click Next.

7. In the Configure Networking page, select a network connection for the virtual machine to use from a list of existing virtual switches.
8. In the Connect Virtual Hard Disk page, select Create a Virtual Hard Disk page, and enter the name, location and size for the virtual hard disk. Click Next.

9. In the Installation Options, you can leave the default option Install an operating system later selected. Click Next.

10. In the Summary page, verify that the list of options displayed are correct. Click Finish.

11. In Hyper-V Manager, right-click the virtual machine to perform various operations like Connect, Edit Settings, Start/Stop, etc.
Cisco HyperFlex installer creates the Hyper-V Failover Cluster and this can be managed both remotely and locally using the Failover Cluster Manager. It is installed when you install the Failover Clustering Tools, which you can do either through a full Failover Cluster installation or a tools-only installation on a remote Windows 10 or 2016 Server.

To manage the Hyper-V Failover Cluster in HyperFlex System from a remote management host, complete the following steps:

1. Install the RSAT tools for Failover Cluster using the below PowerShell command:
   ```powershell
   Install-WindowsFeature RSAT-Clustering-MGMT
   ```

2. Configure the remote management host with constrained delegation as described in the Constrained Delegation section.

3. If the remote management host with RSAT tools is outside the HX cluster AD domain, pointing to the same DNS server and host file mapping between HyperFlex SMB namespace and Cluster management IP (CIP) may be required for successful name resolution.

   For example, add the following entry to the hosts file on the (remote) machine running Hyper-V manager/Failover Cluster Manager/SCVMM Console. Host file in windows is located here - `C:\Windows\System32\drivers\etc\hosts`

   ```
   cluster_mgmt_ip \smb_namespace_name\datastore_name
   ```

   ```
   10.29.149.235 \hxcluster.company.com\ds1
   ```

To create the clustered virtual machine role using the Failover Cluster Manager, complete the following steps:

1. In the Failover Cluster Manager console, under the Actions pane, click Connect to Cluster...

   ![Failover Cluster Manager – Connect to Cluster](image)

2. In the Select Cluster dialog box, click Browse to navigate to the Hyper-V HX cluster. Click OK.
3. In the left pane, click Roles > Virtual Machines... > New Virtual Machines....

4. In the New Virtual Machine dialog box, search and select the Hyper-V node where you wish to create new VMs. Click OK. The New Virtual Machine wizard appears.
5. In the Before You Begin page, click Next.

6. In the Specify Name and Location page, choose a name for the VM, and specify the location or drive where the VM will be stored. Click Next.

7. In the Specify Generation page, select the generation of virtual machine you want to use (Generation 1 or Generation 2) and click Next.

8. In the Assign Memory page, enter the amount of memory that you want for the VM. Click Next.

9. In the Connect Virtual Hard Disk page, enter the name, location and hard drive size. Click Next.

10. In the Installation Options page, select the install location for the OS. Click Next.

11. In the Summary page, review the options selected and click Finish.

Figure 120  Failover Cluster Manager – New VM Summary
Microsoft System Center Virtual Machine Manager 2016

The Hyper-V Cluster created by the HyperFlex Installer can also be managed using the Microsoft System Center Virtual Manager. At the time of the publishing this document, there is no HX plug-in or SMI-S integration with the HX Storage. However, the Hyper-V Cluster can still be managed using the SCVMM without these features.

Installing Microsoft SCVMM is beyond the scope of this document. The following steps cover the basic procedure to add the HyperFlex Hyper-V Cluster to SCVMM and configure storage for managing.

Create Run-As Account for Managing the Hyper-V Cluster

A Run As account is a container for a set of stored credentials. In VMM a Run As account can be provided for any process that requires credentials. Administrators and Delegated Administrators can create Run As accounts. For this deployment, a Run As account should be created for adding Hyper-V hosts and clusters.

To create a Run As account, complete the following steps:

1. Click Settings and in Create click Create Run As Account.
2. In Create Run As Account specify name and optional description to identify the credentials in VMM.
3. In User name and Password specify the credentials. The credentials can be a valid Active Directory user or group account, or local credentials.
4. Clear Validate domain credentials if it is not required and click OK to create the Run As account.

Manage Servers and Clusters

To add the HyperFlex Hyper-V Cluster to the SCVMM, complete the following steps:

1. Open the SCVMM administrator Console and click on Fabric > Servers > All Hosts.
2. Right-click All Hosts and Create a folder for the HyperFlex Hyper-V Cluster.
3. Right-click the newly created folder and click on Add Hyper-V Hosts and Clusters.
4. In the Credentials section, select Use an existing Run As account and select the account created in the previous section.
5. In the Discovery scope, enter the FQDN of HyperFlex Hyper-V Cluster as shown below.
6. In the Target Resources page, select all the discovered hosts and click Next.

7. In the Host Settings page, select the appropriate Host group and click Next.
8. In the summary page, confirm the settings and click Finish.
Network switches and interfaces are created by the HyperFlex installer. A network team is created for the Management, Storage, VM Network and Live Migration networks specified during the installer.

To create the Network Sites and add them to the logical networks created by the installer, complete the following steps:

1. Under Fabric -> Networking -> Logical Networks, find the Logical Network created by the installer.
2. Right-click and select ‘Properties’ of the logical network.

Figure 126  SCVMM – Logical Network

3. Under Network Site, add a site so a VLAN can be specified on the Logical Network.

Figure 127  SCVMM – Network Site
4. When the network site is created, make sure each host in the cluster has the proper VLAN checked in its properties. This can be found under the properties of each host, under Hardware -> and scroll to the ‘team-hx-vm-network’.

Storage

The data stores created in the HyperFlex Connect, presents a SMB share to be used by the HyperFlex Hyper-V nodes to place Virtual Machine files on it. The naming convention is ‘\<hxClusternname>\DatastoreName’.

To add the HX Datastores (SMB Share path) to the Hyper-V Cluster nodes, complete the following steps:

1. Right-click the Cluster ‘HXHVWFC’, select Properties and click ‘File Share Storage’.

   Figure 128  SCVMM – Cluster Properties File Share Storage

2. Click Add to specify the UNC path for the datastore and enter the File share path.
3. Click OK.

4. Repeat steps 2 and 3 to add other datastores if you want to deploy new VMs from SCVMM.

5. Verify the above configuration is applied to all the Hyper-V nodes in the cluster by checking their properties by clicking the storage as shown below.
Create a VM using SCVMM

To create and deploy virtual machines in the System Center - Virtual Machine Manager (VMM) fabric, from an existing virtual hard disk (VHDX) that has been generalized using Sysprep and copied to the VMM library, complete the following steps:

1. Click VMs and Services > Create Virtual Machine > Create Virtual Machine.

2. In Create Virtual Machine Wizard > Select Source, click Use an existing virtual machine, VM template, or virtual hard disk > Browse. Select an existing VHD.
3. In Identity, specify the VM name and an optional description. If the VHD you choose is in the .vhdx format, in the Generation box, select Generation 1 or Generation 2. Click Next.

4. In Configure Hardware, either select the profile that you want to use from the Hardware profile list, or configure the hardware settings manually. Click Next.
5. In Select Destination, place the VM on a host by selecting the destination folder. Click Next.

6. In Select Host, select a Hyper-V host for the VM or leave with default selection. Click Next.
7. In Configure Settings, under locations browse to the HX Datastore SMB share mapped in previous sections and select a vSwitch for the Network Adapter under Networking. Click Next.
8. In Add Properties section, select appropriate actions and click Next.

9. In the Summary page, review and confirm the settings and click Create.
PowerShell

Windows PowerShell is a Windows command-line shell designed especially for system administrators. Windows PowerShell includes an interactive prompt and a scripting environment that can be used independently or in combination. It comes installed by default in every Windows, starting with Windows 7 SP1 and Windows Server 2008 R2 SP1. Using PowerShell, the HyperFlex Hyper-V cluster environment can be managed locally or remotely from a Windows management host running PowerShell (latest version recommended).

Figure 139 shows an example to create a VM on a HX Hyper-V node from a remote management station.

Microsoft Windows Admin Center (WAC)

Microsoft has recently launched a management tool called “Windows Admin Center”. It is a locally deployed, browser-based app for managing servers, clusters, hyper-converged infrastructure, and Windows 10 PCs. It comes at no additional cost beyond Windows and is ready to use in production. Windows Admin Center is the modern evolution of "in-box" management tools, like Server Manager and MMC. It complements System Center - it's not a replacement.
Microsoft Windows Admin Center is a management tool launched recently and it is evolving. Cisco has not extensively tested WAC to manage HyperFlex Hyper-V Cluster.

For more information about Windows Admin Center, refer to:
https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/what-is

Download Windows Admin Center refer to:

To install Windows Admin Center, refer to:
https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/deploy/install

Connecting to Managed Nodes and Clusters

After you have completed the installation of Windows Admin Center, you can add servers or clusters to manage from the main overview page. To add a single server or a cluster as a managed node, complete the following steps:

1. Open a browser and launch the Windows Admin Center.
2. Click + Add under All Connections.
3. Choose to add a Server, Failover Cluster connection.

Figure 140  WAC Page
4. Type the name of the server or cluster to manage and click Submit. The server or cluster will be added to your connection list on the overview page. In this example, Hyper-V cluster is added to manage.

5. Next Authenticate with a managed node using ‘Single Sign-on’ or ‘Manage As’ by entering the credentials.

6. Select a server/cluster and click on Edit Tags to organize your connections. This will help to filter your connection lists.
Manage Servers with WAC

To add and manage individual servers running Windows Server 2012 or later to Windows Admin Center with a comprehensive set of tools including Devices, Events, Processes, Roles and Features, Updates, Virtual Machines and more, complete the following steps:

1. Launch WAC from a browser.
2. Click a server under All Connections. The figure below shows the tools available to manage servers.
**Manage a Failover Cluster with WAC**

1. Add Failover clusters to view and manage cluster resources, storage, network, nodes, roles, virtual machines and virtual switches.

2. Launch WAC from a browser.

3. Select and click on the cluster under All Connections. The figure below shows the tools available to view and manage Cluster.

**Figure 145  WAC – Failover Cluster Manager**

```plaintext
<table>
<thead>
<tr>
<th>Tools</th>
<th>Overview</th>
<th>Cluster resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nodes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Machines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Switches</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Online</td>
<td>Network Name</td>
</tr>
<tr>
<td>Cluster IP Address</td>
<td>Online</td>
<td>IP Address</td>
</tr>
<tr>
<td>Virtual Machine Cluster WMI</td>
<td>Online</td>
<td>Virtual Machine Cluster WMI Provider</td>
</tr>
<tr>
<td>File Share Witness</td>
<td>Online</td>
<td>File Share Quorum Witness</td>
</tr>
</tbody>
</table>
```
A: Cluster Capacity Calculations

HyperFlex HX Data Platform cluster capacity is calculated as follows:

\[
\text{Result} = \frac{(((\text{capacity disk size in GB} \times 10^9) / 1024^3) \times \text{number of capacity disks per node} \times \text{number of HyperFlex nodes}} \times 0.92} / \text{replication factor}
\]

Divide the result by 1024 to get a value in TiB

The replication factor value is 3 if the HX cluster is set to RF=3, and the value is 2 if the HX cluster is set to RF=2.

The 0.92 multiplier accounts for an 8% reservation set aside on each disk by the HX Data Platform software for various internal filesystem functions.

Calculation example:

\[
\text{<capacity disk size in GB>} = 960
\]

\[
\text{<number of capacity disks per node>} = 8 \text{ for an HXAF220c-M5SX model server}
\]

\[
\text{<number of HyperFlex nodes>} = 8
\]

replication factor = 3

Result: \[\frac{(((960*10^9)/1024^3)*8*8*0.92)/3 = 17547.6074}{17547.6074/ 1024 = 17.14 \text{ TiB}}\]

B: Install Microsoft Windows Server 2016

To install Windows Server 2016 and apply Cisco HyperFlex driver image on all HX nodes, follow these high-level steps.

- Configure Cisco UCS Manager using HX Installer
- Configure Cisco UCS vMedia and Boot Policies
- Install Microsoft Windows Server 2016 OS
- Undo vMedia and Boot Policy Changes

Configure Cisco UCS Manager using HX Installer

To complete this step, refer to “Configure Cisco UCS Manager using HX Installer” under the “HyperFlex Installation – Phase 1” section.

Configure Cisco UCS vMedia and Boot Policies

By using a Cisco UCS vMedia policy, the Windows Server 2016 media ISO file and Cisco HyperFlex Driver image can be mounted to all of the HX servers automatically. The existing vMedia policy, named “HyperFlex” must be modified to mount this file, and the boot policy must be modified temporarily to boot from the remotely mounted vMedia file. Once these two tasks are completed, the servers can be rebooted, and they will automatically boot from the When mounted vMedia file, installing and configuring Windows Server 2016 on the HX nodes.
WARNING! While vMedia policies are very efficient for installing multiple servers, using vMedia policies as described could lead to an accidental reinstall of Windows on any existing server that is rebooted with this policy. Please be certain that the servers being rebooted while the policy is in effect are the servers you wish to reinstall. Even though the custom ISO will not continue without a secondary confirmation, extreme caution is recommended. This procedure needs to be carefully monitored and the boot policy should be changed back to original settings immediately after the intended servers are rebooted, and the Windows installation begins. Using this policy is only recommended for new installs or rebuilds. Alternatively, you can manually select the boot device using the KVM console during boot, and pressing F6, instead of making the vMedia device the default boot selection.

To configure the Cisco UCS vMedia and Boot Policies, complete the following steps:

1. Copy the Windows Server 2016 iso and Cisco HyperFlex Driver image files to the HX Installer VM via SCP or SFTP, placing it in the folder /var/www/localhost/images/ as shown below.

   ![Image](Figure 146 Upload Windows ISO and Cisco Driver and System Preparation Script)

   Make sure network connectivity exists between the file share and all server management IPs.

2. Configure the vMedia and Boot policies using Cisco UCS Manager to mount the above images

3. Launch Cisco UCS Manager by accessing the Cisco UCS Manager IP address in a browser of your choice.

4. Click Launch UCS Manager and log in with administrator username and the password you used at the beginning of the installation.

5. In the left navigation pane, click Servers.

6. Expand Servers > Policies > root > Sub-Organizations > hx-cluster_name>vMedia Policies to view the list of vMedia Policies.
7. Double-click vMedia Policy HyperFlex.

8. In the properties for vMedia Policy HyperFlex, click Create vMedia Mount to add the mount points.

9. In the Create vMedia Mount dialog box, complete the following fields:

| Table 41  Create vMedia Mount Details |
|-----------------|----------------|
| Field Name      | Action          |
| Name            | Name for the mount point. |
| Description     | Can be used for more information. |
| Device Type     | Type of image that you want to mount |
| Protocol        | The protocol used for accessing the share where the ISO files are located. |
| Hostname/IP Address | IP address or FQDN of the server hosting the images. |

Example Value

<table>
<thead>
<tr>
<th>Example Value</th>
<th>Windows -ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>Hostname/IP Address</td>
<td>10.29.149.212</td>
</tr>
<tr>
<td>Field Name</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Image Name Variable</td>
<td>This value is not used in HyperFlex installation.</td>
</tr>
<tr>
<td>Remote File</td>
<td>The filename of the ISO file that you want to mount.</td>
</tr>
<tr>
<td>Remote Path</td>
<td>The path on the remote server to where the file resides</td>
</tr>
<tr>
<td>Username</td>
<td>If you use CIFS or NFS a username might be necessary</td>
</tr>
<tr>
<td>Password</td>
<td>If you use CIFS or NFS a password might be necessary</td>
</tr>
</tbody>
</table>

**Figure 148  Cisco UCS Manager - Create vMedia Mount CDD**

10. Click Save Changes and click OK.

11. Click OK. When you click OK, you are returned to the vMedia policy and will see the information that you submitted.

12. Repeat steps 5 and 6 but change the type to HDD and the filename to the Cisco HyperFlex driver image.
13. On completion, the following screen displays:

![Figure 149 Cisco UCS Manager - Create vMedia Mount HDD](image1)

14. In the left navigation pane, select Servers > Service Profile Templates > root > Sub-O rganizations > hx-cluster_name > Service Template hx-nodes_name (example:hx-nodes-m5).
15. Choose the HyperFlex vMedia Policy from the drop-down list and click OK twice.


17. In the configuration pane, click CIMC Mounted vMedia. Click Add CIMC Mounted CD/DVD to add this to the boot order.

18. Select the CIMC Mounted CD/DVD entry in the list and move it to the top of the boot order by pressing the Move Up button.
19. Click Save Changes and click OK. The boot policy is saved.

To verify the images are mounted correctly, complete the following steps:

1. On the Equipment tab, select one of the servers.
2. Click Inventory > CIMC, scroll down and make sure for the mount entry #1 (OS image) and mount entry #2 (Cisco HyperFlex driver image) the status is Mounted and there are no failures.

Install Microsoft Windows Server 2016 OS

1. In the menu bar, click Servers and choose the first HyperFlex service profile.
2. Click the General tab and choose Actions > KVM Console.
Appendix

The KVM console will try to open in a new browser. Be aware of any pop-up blockers. Allow the Pop-Ups and re-open the KVM.

Figure 155  Cisco UCS Manager – Launch KVM Console

3. Reboot the server. In the KVM console choose Server Actions and press Reset.

Figure 156  Cisco UCS Manager – Server KVM Console


5. When the server is rebooting, remember to press any key to start the Windows installation.

Figure 157  Cisco UCS Manager – KVM Console Server Boot
6. When the Windows installation is complete, you will see some tasks running as shown in the below and the host will reboot a few times. Allow some time for the system preparation to complete.

**Figure 158  System Preparation**

![System Preparation](image)

7. The installation is complete when a clean command prompt with no activity is displayed as shown below.

**Figure 159  Windows Server Command Prompt**

![Command Prompt](image)

8. Repeat these steps on all the HX nodes in the cluster and verify the below task is running as shown in below. The ‘HXInstallbootstraplauncherTask’ in running state is an indication of successful installation Windows OS and system preparation.
Figure 160  Validate Windows Server Installation Completion

Undo vMedia and Boot Policy Changes

1. When all the servers have booted from the remote vMedia file and begun their installation process, the changes to the boot policy need to be quickly undone, to prevent the servers from going into a boot loop, constantly booting from the installation ISO file. To revert the boot policy settings, complete the following steps: In Cisco UCS Manager select Servers > Polices > Root > Sub-O rganizations > HX-Cluster_name > vMedia polices.

2. Click the vMedia Policy HyperFlex. Click the mount points one at a time and delete both of them. Accept the changes.

Figure 161  Cisco UCS Manager – Undo vMedia and Boot Policy Changes

3. Go to the boot policy by selecting Servers > Polices > Root > Sub-O rganizations > HX-Cluster_name > boot polices > Boot Policy HyperFlex-m5.

4. Select the CIMC mounted CD/DVD, click Delete and accept the changes.
About the Authors

Sanjeev Naldurgkar, Technical Marketing Engineer, Cisco UCS Datacenter Solutions Group, Cisco Systems, Inc.

Sanjeev has been with Cisco for six years focusing on delivering customer-driven solutions on Microsoft Hyper-V and VMware vSphere. He has over 16 years of experience in the IT Infrastructure, Server virtualization, and Cloud Computing. He holds a Bachelor Degree in Electronics and Communications Engineering, and leading industry certifications from Microsoft and VMware.

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the author would like to thank:

- Babu Mahadevan V - Cisco Systems, Inc.
- Robert Quimbey - Cisco Systems, Inc.
- Jeffrey Nichols - Cisco Systems, Inc.