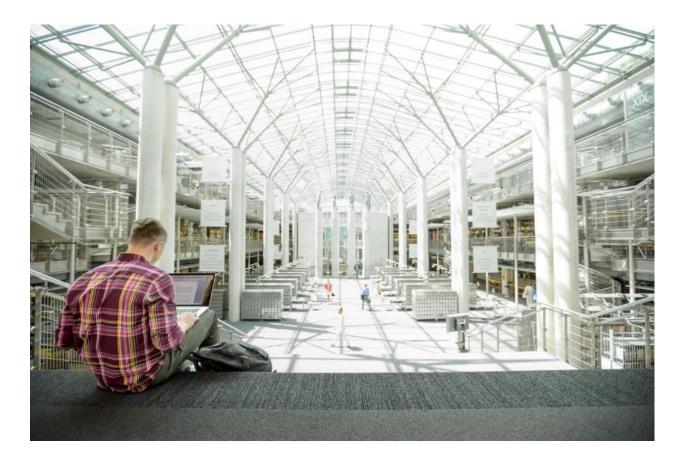
# cisco.



## Cisco HyperFlex M5 All-Flash Hyperconverged System with Hyper-V 2016 and Citrix XenDesktop

Deployment Guide for Cisco HyperFlex with Virtual Desktop Infrastructure for Citrix XenDesktop 7.16 using Cisco UCS 3.2(3), Cisco HyperFlex Data Platform v 3.0.1c, and Microsoft Hyper -V 2016

Last Updated: December 21, 2018

**IIIIIII CISCO** VALIDATED DESIGN

## 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, refer to:

#### http://www.cisco.com/go/designzone.

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 UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 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	
Introduction	
Audience	8
Purpose of this Document	
Summary	
Solution Summary	
Cisco Desktop Virtualization Solutions: Data Center	11
The Evolving Workplace	11
Cisco Desktop Virtualization Focus	
Use Cases	14
Physical Topology	14
Fabric Interconnects	
HX-Series Rack Mount Servers	
Logical Network Design	
Technology Overview	
Cisco Unified Computing System	19
Cisco Unified Computing System Components	
Supported Versions and System Requirements	
Hardware and Software Interoperability	
Software Requirements for Microsoft Hyper-V	
Cisco UCS Fabric Interconnect	21
Cisco HyperFlex HX-Series Nodes	
Cisco HyperFlex Converged Data Platform Software	
Cisco HyperFlex Connect HTML5 Management Web Page	27
Cisco Intersight Management Web Page	
Cisco Nexus 93108YCPX Switches	
Architectural Flexibility	
Feature-Rich	
Real-Time Visibility and Telemetry	
Highly Available and Efficient Design	
Simplified Operations	
Investment Protection	
Microsoft Hyper-V 2016	
Microsoft System Center 2016	
Citrix XenApp™ and XenDesktop™ 7.16	
Zones	
Improved Database Flow and Configuration	
Application Limits	

Multiple Notifications before Machine Updates or Scheduled Restarts	
API Support for Managing Session Roaming	
API Support for Provisioning VMs from Hypervisor Templates	
Support for New and Additional Platforms	
Citrix Provisioning Services 7.16	40
Benefits for Citrix XenApp and Other Server Farm Administrators	40
Benefits for Desktop Administrators	41
Citrix Provisioning Services Solution	41
Citrix Provisioning Services Infrastructure	42
Architecture and Design of Citrix XenDesktop on Cisco Unified Computing System and Cisco HyperFlex Storage Design Fundamentals	42
Understanding Applications and Data	43
Project Planning and Solution Sizing Sample Questions	44
Citrix XenDesktop Design Fundamentals	44
Machine Catalogs	45
Delivery Groups	45
Example XenDesktop Deployments	46
Distributed Components Configuration	46
Multiple Site Configuration	47
Citrix Cloud Services	48
Designing a XenDesktop Environment for a Mixed Workload	48
Deployment Hardware and Software	50
Physical Components	50
Software Components	51
Licensing	51
Considerations	52
Version Control	52
Microsoft Windows Active Directory	52
Scale	52
Capacity	53
Physical Topology	54
Topology Overview	54
Fabric Interconnects	55
HX-Series Rack-Mount Servers	56
Logical Architecture	56
Design Elements	57
Network Design	57
VLANs	58
Jumbo Frames	59
Cisco UCS Design	59
Cisco UCS Organization	59
Cisco UCS LAN Policies	60

Cisco UCS Service Profile Templates Solution Configuration Cisco UCS Compute Platform Physical Infrastructure	78 78 78 81
Cisco UCS Compute Platform	78 78 81
	78 81
Physical Infrastructure	81
Cisco Unified Computing System Configuration	
Cisco UCS Fabric Interconnect A	81
Cisco UCS Fabric Interconnect B	82
Cisco UCS Manager	83
Cisco UCS Configuration	83
Cisco UCS Firmware	83
NTP	84
Uplink Ports	84
Uplink Port Channels	85
Server Ports	86
Server Discovery	87
Deploying HX Data Platform Installer on Hyper-V Infrastructure	87
Assign a Static IP Address to the HX Data Platform Installer VM	91
HyperFlex Installation	92
HyperFlex Installation - Phase 1	93
HyperFlex Installation - Phase 2	110
Post Installation Tasks	118
Create Datastores	118
Constrained Delegation (Optional)	119
Post HyperFlex Cluster Installation for Hyper-V 2016	123
Microsoft System Center Virtual Machine Manager 2016	123
Create Run-As Account for Managing the Hyper-V Cluster	123
Manage Servers and Clusters	123
Networking	126
Assign IP Addresses to Live Migration and VM Network Interfaces	128
Rename the Cluster Network in Windows Failover Cluster - Optional	130
Configure the Windows Failover Cluster Network Roles	130
Configure the Windows Failover Cluster Network for Live Migration	131
Storage	132
Build the Virtual Machines and Environment for Workload Testing	135
Software Infrastructure Configuration	. 135
Prepare the Master Images	136
Install and Configure XenDesktop Delivery Controller, Citrix Licensing, and StoreFront	. 136
Install Citrix License Server	137
Install Citrix Licenses	140
Install XenDesktop	141

Configure the XenDesktop Site	1.47
Configure the XenDesktop Site Administrators.	
Configure Additional XenDesktop Controller	
Add the Second Delivery Controller to the XenDesktop Site	
Install and Configure StoreFront	
Additional StoreFront Configuration	
Install the Citrix Provisioning Services Target Device Software	
Create Citrix Provisioning Services vDisks	176
Provision Desktop Machines from Citrix Provisioning Services Console	
Install XenDesktop Virtual Desktop Agents	199
Create Delivery Groups	205
Citrix XenDesktop Policies and Profile Management	209
Configure Citrix XenDesktop Policies	209
Configuring User Profile Management	210
Test Setup and Configurations	212
Testing Methodology and Success Criteria	213
Testing Procedure	213
Pre-Test Setup for Testing	213
Test Run Protocol	214
Success Criteria	214
Test Results	219
Boot Storms	219
Recommended Maximum Workload and Configuration Guidelines	219
Eight Node Cisco HXAF220c-M5S Rack Server and HyperFlex All-Flash Cluster	219
Eight Node Cisco HXAF220c-M5S Rack Server and HyperFlex All-Flash Cluster	220
Summary	227
About the Authors	228
Acknowledgements	228
Appendix A – Cisco Nexus 93108YC Switch Configuration	229
Switch A Configuration	229
Switch B Configuration	239

## CISCO CITRIX

## **Executive Summary**

To keep pace with the market, you need systems that support rapid, agile development processes. Cisco HyperFlex<sup>™</sup> Systems let you unlock the full potential of hyper-convergence and adapt IT to the needs of your workloads. The systems use an end-to-end software-defined infrastructure approach, combining software-defined computing in the form of Cisco HyperFlex HX-Series Nodes, software-defined storage with the powerful Cisco HyperFlex HX Data Platform, and software-defined networking with the Cisco UCS fabric that integrates smoothly with Cisco® Application Centric Infrastructure (Cisco ACI<sup>™</sup>).

Together with a single point of connectivity and management, these technologies deliver a pre-integrated and adaptable cluster with a unified pool of resources that you can quickly deploy, adapt, scale, and manage to efficiently power your applications and your business

This document provides an architectural reference and design guide for up to 1250 VDI users and 1600 RDS session workload on an 8-node (8x Cisco HyperFlex HXAF220C-M5SX server) Cisco HyperFlex system. We provide deployment guidance and performance data for Citrix XenDesktop 7.16 virtual desktops running Microsoft Windows 10 with Office 2016 Machine Creation Services. The solution is a pre-integrated, best-practice data center architecture built on the Cisco Unified Computing System (UCS), the Cisco Nexus® 9000 family of switches and Cisco HyperFlex Data Platform software version 3.0.1c.

The solution payload is 100 percent virtualized on Cisco HyperFlex HXAF220C-M5SX hyperconverged nodes booting via on-board M.2 SATA SSD drive running Microsoft Hyper-V 2016 hypervisor and the Cisco HyperFlex Data Platform storage controller VM. The virtual desktops are configured with XenDesktop 7.16, which incorporates both traditional persistent and non-persistent virtual Windows 7/8/10 desktops, hosted applications and remote desktop service (RDS) Microsoft Server 2008 R2, Server 2012 R2 or Server 2016 based desktops. The solution provides unparalleled scale and management simplicity. Citrix XenDesktop Provisioning Services or Machine Creation Services Windows 10 desktops, full clone desktops or XenApp server based desktops can be provisioned on an eight node Cisco HyperFlex cluster. Where applicable, this document provides best practice recommendations and sizing guidelines for customer deployment of this solution.

The solution boots 1250 virtual desktops machines in 30 minutes or less, making sure that users will not experience delays in accessing their virtual workspace on HyperFlex.

Our past Cisco Validated Design studies with HyperFlex show linear scalability out to the cluster size limits of 8 HyperFlex hyperconverged nodes with Cisco UCS B200 M5, Cisco UCS C220 M5, or Cisco UCS C240 M5 servers. You can expect that our new HyperFlex all flash system running HX Data Platform 3.0.1 on Cisco HXAF220 M5 or Cisco HXAF240 M5 nodes will scale up to 1250 knowledge worker users per cluster with N+1 server fault tolerance.

The solution is fully capable of supporting hardware accelerated graphic workloads. Each Cisco HyperFlex HXAF240c M5 node and each Cisco UCS C240 M5 compute only server can support up to two NVIDIA M10 or P40 cards. The Cisco UCS B200 M5 server supports up to two NVIDIA P6 cards for high density, high performance graphics workload support. See our <u>Cisco Graphics White Paper</u> for our fifth generation servers with NVIDIA GPUs and software for details on how to integrate this capability with Citrix XenDesktop.

The solution provides outstanding virtual desktop end user experience as measured by the Login VSI 4.1.25 Knowledge Worker workload running in benchmark mode. Index average end-user response times for all tested delivery methods is under one second, representing the best performance in the industry.

### Solution Overview

#### Introduction

The current industry trend in data center design is towards small, granularly expandable hyperconverged infrastructures. By using virtualization along with pre-validated IT platforms, customers of all sizes have embarked on the journey to "just-in-time capacity" using this new technology. The Cisco HyperFlex hyper converged solution can be quickly deployed, thereby increasing agility and reducing costs. Cisco HyperFlex uses best of breed storage, server and network components to serve as the foundation for desktop virtualization workloads, enabling efficient architectural designs that can be quickly and confidently deployed and scaled-out.

#### Audience

The audience for this document includes, but is not limited to; sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

#### Purpose of this Document

This document provides a step-by-step design, configuration, and implementation guide for the Cisco Validated Design for a Cisco HyperFlex All-Flash system running four different Citrix XenDesktop/XenApp workloads with Cisco UCS 6300 series Fabric Interconnects and Cisco Nexus 9300 series switches.

#### 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.

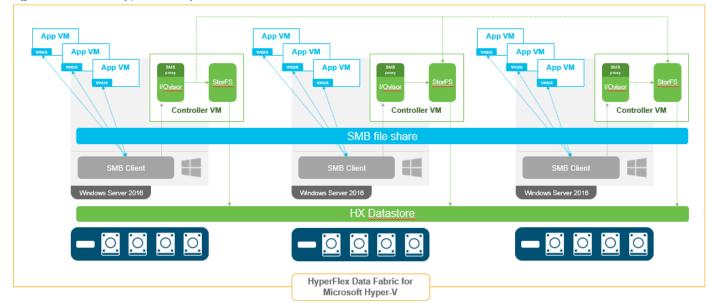


Figure 1 Cisco HyperFlex System Overview

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 6332 Fabric Interconnect
- Cisco UCS 6332-16UP Fabric Interconnect
- Eight Cisco HyperFlex HX-Series Rack-Mount Servers, choose from models:
  - Cisco HyperFlex HXAF220c-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 Needed for XenDesktop (end-user supplied)
    - Citrix XenApp/XenDesktop 7.16
    - Citrix Provisioning Services 7.16

## Solution Summary

This Cisco Validated Design prescribes a defined set of hardware and software that serves as an integrated foundation for both Citrix XenDesktop Microsoft Windows 10 virtual desktops and Citrix XenApp server desktop sessions based on Microsoft Server 2016. The mixed workload solution includes Cisco HyperFlex hardware and Data Platform software, Cisco Nexus® switches, the Cisco Unified Computing System (Cisco UCS®), Citrix XenDesktop and Microsoft Hyper-V software in a single package. The design is efficient such that the networking, computing, and storage components occupy an 8-rack unit footprint in an industry standard 42U rack. Port density on the Cisco Nexus switches and Cisco UCS Fabric Interconnects enables the networking components to accommodate multiple HyperFlex clusters in a single Cisco UCS domain.

A key benefit of the Cisco Validated Design architecture is the ability to customize the environment to suit a customer's requirements. A Cisco Validated Design scales easily as requirements and demand change. The solution can be scaled both up (adding resources to a Cisco Validated Design unit) and out (adding more Cisco Validated Design units).

The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of a hyper-converged desktop virtualization solution. A solution capable of consuming multiple protocols across a single interface allows for customer choice and investment protection because it truly is a wire-once architecture.

The combination of technologies from Cisco Systems, Inc. and Microsoft Inc. produced a highly efficient, robust and affordable desktop virtualization solution for a virtual desktop, hosted shared desktop or mixed deployment supporting different use cases. Key components of the solution include the following:

- More power, same size. Cisco HX-series nodes, dual 18-core 2.3 GHz Intel Xeon (Gold 6140) Scalable Family processors with 768GB of 2666Mhz memory with Citrix XenDesktop support more virtual desktop workloads than the previously released generation processors on the same hardware. The Intel Xeon Gold 6140 18-core scalable family processors used in this study provided a balance between increased perserver capacity and cost.
- Fault-tolerance with high availability built into the design. The various designs are based on multiple Cisco HX-Series nodes, Cisco UCS rack servers and Cisco UCS blade servers for virtual desktop and infrastructure workloads. The design provides N+1 server fault tolerance for every payload type tested.
- Stress-tested to the limits during aggressive boot scenario. The 1250 user mixed hosted virtual desktop and 1600 user hosted shared desktop environment booted and registered with the XenDesktop Studio in under 5 minutes, providing our customers with an extremely fast, reliable cold-start desktop virtualization system.
- Stress-tested to the limits during simulated login storms. All 1250 users logged in and started running workloads up to steady state in 48-minutes without overwhelming the processors, exhausting memory or exhausting the storage subsystems, providing customers with a desktop virtualization system that can easily handle the most demanding login and startup storms.
- Ultra-condensed computing for the data center. The rack space required to support the initial 1250 user system is 8 rack units, including Cisco Nexus Switching and Cisco Fabric interconnects. Incremental Citrix XenDesktop users can be added to the Cisco HyperFlex cluster up to the cluster scale limits, currently 16 hyper converged and 16 compute only nodes, by adding one or more nodes.
- 100 percent virtualized: This CVD presents a validated design that is 100 percent virtualized on Microsoft Hyper-V 2016. All of the virtual desktops, user data, profiles, and supporting infrastructure components, including Active Directory, SQL Servers, Citrix XenDesktop components, XenDesktop VDI desktops and XenApp servers were hosted as virtual machines. This provides customers with complete flexibility for maintenance and capacity additions because the entire system runs on the Cisco HyperFlex hyperconverged infrastructure with stateless Cisco UCS HX-series servers. (Infrastructure VMs were hosted on two Cisco UCS C220 M4 Rack Servers outside of the HX cluster to deliver the highest capacity and best economics for the solution.)

- Cisco data center management: Cisco maintains industry leadership with the new Cisco UCS Manager 3.2(2) software that simplifies scaling, guarantees consistency, and eases maintenance. Cisco's ongoing development efforts with Cisco UCS Manager, Cisco UCS Central, and Cisco UCS Director insure that customer environments are consistent locally, across Cisco UCS Domains and across the globe. Cisco UCS software suite offers increasingly simplified operational and deployment management, and it continues to widen the span of control for customer organizations' subject matter experts in compute, storage and network.
- **Cisco 40G Fabric:** Our 40G unified fabric story gets additional validation on 6300 Series Fabric Interconnects as Cisco runs more challenging workload testing, while maintaining unsurpassed user response times.
- **Cisco HyperFlex Connect (HX Connect):** An all-new HTML 5 based Web UI Introduced with HyperFlex v2.5 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.
- Cisco HyperFlex storage performance: Cisco HyperFlex provides industry-leading hyper converged storage performance that efficiently handles the most demanding I/O bursts (for example, login storms), high write throughput at low latency, delivers simple and flexible business continuity and helps reduce storage cost per desktop.
- **Cisco HyperFlex agility:** Cisco HyperFlex System enables users to seamlessly add, upgrade or remove storage from the infrastructure to meet the needs of the virtual desktops.
- **Optimized for performance and scale.** For hosted shared desktop sessions, the best performance was achieved when the number of vCPUs assigned to the virtual machines did not exceed the number of hyper-threaded (logical) cores available on the server. In other words, maximum performance is obtained when not overcommitting the CPU resources for the virtual machines running virtualized RDS systems.

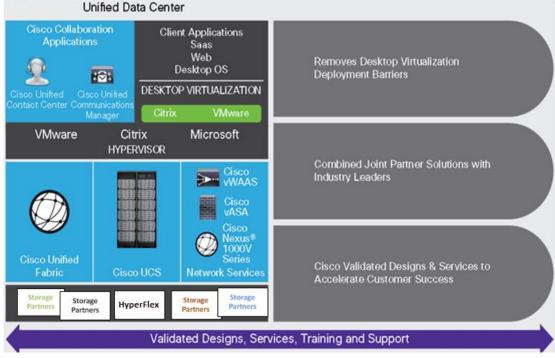
#### Cisco Desktop Virtualization Solutions: Data Center

#### The Evolving Workplace

Today's IT departments are facing a rapidly evolving workplace environment. The workforce is becoming increasingly diverse and geographically dispersed, including offshore contractors, distributed call center operations, knowledge and task workers, partners, consultants, and executives connecting from locations around the world at all times.

This workforce is also increasingly mobile, conducting business in traditional offices, conference rooms across the enterprise campus, home offices, on the road, in hotels, and at the local coffee shop. This workforce wants to use a growing array of client computing and mobile devices that they can choose based on personal preference. These trends are increasing pressure on IT to ensure protection of corporate data and prevent data leakage or loss through any combination of user, endpoint device, and desktop access scenarios (Figure 2).

These challenges are compounded by desktop refresh cycles to accommodate aging PCs and bounded local storage and migration to new operating systems, specifically Microsoft Windows 10 and productivity tools, specifically Microsoft Office 2016.



## Figure 2 Cisco Data Center Partner Collaboration

Some of the key drivers for desktop virtualization are increased data security, the ability to expand and contract capacity and reduced TCO through increased control and reduced management costs.

#### **Cisco Desktop Virtualization Focus**

Cisco focuses on three key elements to deliver the best desktop virtualization data center infrastructure: simplification, security, and scalability. The software combined with platform modularity provides a simplified, secure, and scalable desktop virtualization platform.

#### Simplified

Cisco UCS and Cisco HyperFlex provide a radical new approach to industry-standard computing and provides the core of the data center infrastructure for desktop virtualization. Among the many features and benefits of Cisco UCS are the drastic reduction in the number of servers needed and in the number of cables used per server, and the capability to rapidly deploy or re-provision servers through Cisco UCS service profiles. With fewer servers and cables to manage and with streamlined server and virtual desktop provisioning, operations are significantly simplified. Thousands of desktops can be provisioned in minutes with Cisco UCS Manager service profiles and Cisco storage partners' storage-based cloning. This approach accelerates the time to productivity for end users, improves business agility, and allows IT resources to be allocated to other tasks.

Cisco UCS Manager automates many mundane, error-prone data center operations such as configuration and provisioning of server, network, and storage access infrastructure. In addition, Cisco UCS B-Series Blade Servers, C-Series and HX-Series Rack Servers with large memory footprints enable high desktop density that helps reduce server infrastructure requirements.

Simplification also leads to more successful desktop virtualization implementation. Cisco and its technology partners like Microsoft have developed integrated, validated architectures, including predefined hyper-converged architecture infrastructure packages such as HyperFlex. Cisco Desktop Virtualization Solutions have been tested with Microsoft Hyper-V.

#### Secure

Although virtual desktops are inherently more secure than their physical predecessors, they introduce new security challenges. Mission-critical web and application servers using a common infrastructure such as virtual desktops are now at a higher risk for security threats. Inter–virtual machine traffic now poses an important security consideration that IT managers need to address, especially in dynamic environments in which virtual machines, using Microsoft Live Migration, move across the server infrastructure.

Desktop virtualization, therefore, significantly increases the need for virtual machine–level awareness of policy and security, especially given the dynamic and fluid nature of virtual machine mobility across an extended computing infrastructure. The ease with which new virtual desktops can proliferate magnifies the importance of a virtualization-aware network and security infrastructure. Cisco data center infrastructure (Cisco UCS and Cisco Nexus Family solutions) for desktop virtualization provides strong data center, network, and desktop security, with comprehensive security from the desktop to the hypervisor. Security is enhanced with segmentation of virtual desktops, virtual machine–aware policies and administration, and network security across the LAN and WAN infrastructure.

#### Scalable

Growth of a desktop virtualization solution is accelerating, so a solution must be able to scale, and scale predictably, with that growth. The Cisco Desktop Virtualization Solutions support high virtual-desktop density (desktops per server) and additional servers scale with near-linear performance. Cisco data center infrastructure provides a flexible platform for growth and improves business agility. Cisco UCS Manager service profiles allow on-demand desktop provisioning and make it just as easy to deploy dozens of desktops as it is to deploy thousands of desktops.

Cisco HyperFlex servers provide near-linear performance and scale. Cisco UCS implements the patented Cisco Extended Memory Technology to offer large memory footprints with fewer sockets (with scalability to up to 1.5 terabyte (TB) of memory with 2- and 4-socket servers). Using unified fabric technology as a building block, Cisco UCS server aggregate bandwidth can scale to up to 80 Gbps per server, and the northbound Cisco UCS fabric interconnect can output 2 terabits per second (Tbps) at line rate, helping prevent desktop virtualization I/O and memory bottlenecks. Cisco UCS, with its high-performance, low-latency unified fabric-based networking architecture, supports high volumes of virtual desktop traffic, including high-resolution video and communications traffic. In addition, Cisco HyperFlex helps maintain data availability and optimal performance during boot and login storms as part of the Cisco Desktop Virtualization Solutions. Recent Cisco Validated Designs based on Citrix XenDesktop, Cisco HyperFlex solutions have demonstrated scalability and performance, with up to 450 hosted virtual desktops and hosted shared desktops up and running in 5 minutes.

Cisco UCS and Cisco Nexus data center infrastructure provides an excellent platform for growth, with transparent scaling of server, network, and storage resources to support desktop virtualization, data center applications, and cloud computing.

#### Savings and Success

The simplified, secure, scalable Cisco data center infrastructure for desktop virtualization solutions saves time and money compared to alternative approaches. Cisco UCS enables faster payback and ongoing savings (better ROI and lower TCO) and provides the industry's greatest virtual desktop density per server, reducing both capital expenditures (CapEx) and operating expenses (OpEx). The Cisco UCS architecture and Cisco Unified Fabric also enables much lower network infrastructure costs, with fewer cables per server and fewer ports required. In addition, storage tiering and deduplication technologies decrease storage costs, reducing desktop storage needs by up to 50 percent.

The simplified deployment of Cisco HyperFlex for desktop virtualization accelerates the time to productivity and enhances business agility. IT staff and end users are more productive more quickly, and the business can respond to new opportunities quickly by deploying virtual desktops whenever and wherever they are needed. The high-performance Cisco systems and network deliver a near-native end-user experience, allowing users to be productive anytime and anywhere.

The key measure of desktop virtualization for any organization is its efficiency and effectiveness in both the near term and the long term. The Cisco Desktop Virtualization Solutions are very efficient, allowing rapid deployment, requiring fewer devices and cables, and reducing costs. The solutions are also extremely effective, providing the services that end users need on their devices of choice while improving IT operations, control, and data security. Success is bolstered through Cisco's best-in-class partnerships with leaders in virtualization and through tested and validated designs and services to help customers throughout the solution lifecycle. Long-term success is enabled through the use of Cisco's scalable, flexible, and secure architecture as the platform for desktop virtualization.

The ultimate measure of desktop virtualization for any end user is a great experience. Cisco HyperFlex delivers class-leading performance with sub-second base line response times and index average response times at full load of just under one second.

#### **Use Cases**

- Healthcare: Mobility between desktops and terminals, compliance, and cost
- Federal government: Teleworking initiatives, business continuance, continuity of operations (COOP), and training centers
- Financial: Retail banks reducing IT costs, insurance agents, compliance, and privacy
- Education: K-12 student access, higher education, and remote learning
- State and local governments: IT and service consolidation across agencies and interagency security
- Retail: Branch-office IT cost reduction and remote vendors
- Manufacturing: Task and knowledge workers and offshore contractors
- Microsoft Windows 10 migration
- Graphic intense applications
- Security and compliance initiatives
- Opening of remote and branch offices or offshore facilities
- Mergers and acquisitions

#### Physical Topology

The Cisco HyperFlex system is composed of a pair of Cisco UCS 6200/6300 series Fabric Interconnects, along with up to 8 HXAF-Series rack mount servers per cluster Up to 8 separate HX clusters can be installed under a single pair of Fabric Interconnects. The Fabric Interconnects both connect to every HX-Series rack mount server, and both connect to every Cisco UCS 5108 blade chassis. Upstream network connections, also referred to as "northbound" network connections are made from the Fabric Interconnects to the customer datacenter network at the time of installation.



For this study, we uplinked the Cisco 6332-16UP Fabric Interconnects to Cisco Nexus 93108YCPX switches.

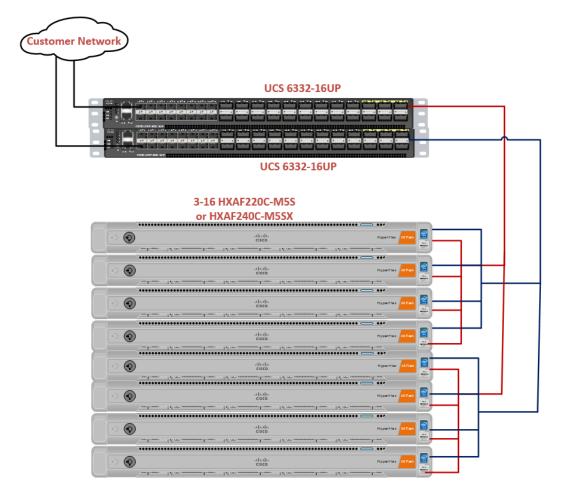


Figure 3 Cisco HyperFlex Standard Topology

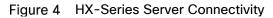
#### **Fabric Interconnects**

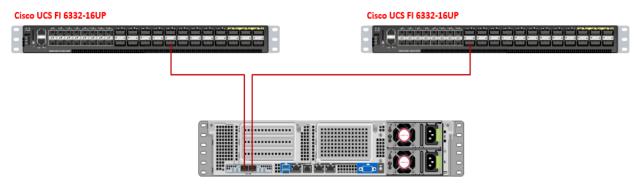
Fabric Interconnects (FI) are deployed in pairs, wherein the two units operate as a management cluster, while forming two separate network fabrics, referred to as the A side and B side fabrics. Therefore, many design elements will refer to FI A or FI B, alternatively called fabric A or fabric B. Both 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.

#### **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. Both the HXAF220C-M5SX and HXAF240C-M5SX servers are configured with the Cisco VIC 1387 network interface card (NIC) installed in a modular LAN on motherboard (MLOM) slot, which has dual 40 Gigabit Ethernet (GbE) ports. The standard and redundant connection practice is to connect port 1 of the VIC 1387 to a port on FI A, and port 2 of the VIC 1387 to a port on FI B (Figure 4).

Failure to follow this cabling practice can lead to errors, discovery failures, and loss of redundant connectivity.





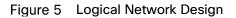
#### Logical Network Design

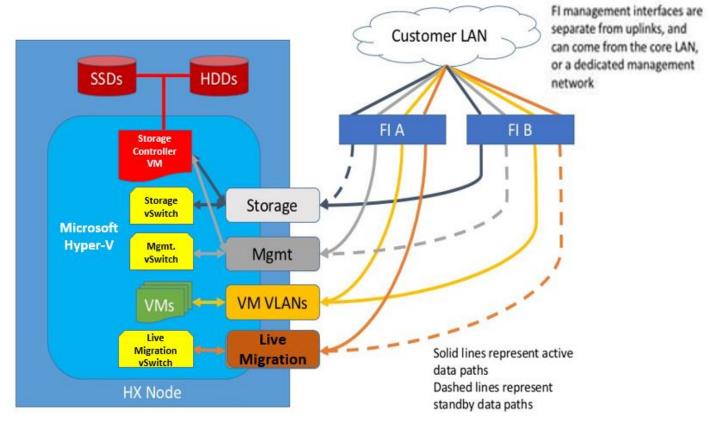
The Cisco HyperFlex system has communication pathways that fall into four defined zones (Figure 5):

- **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 and blades, which answer through the FI management ports.
  - Hyper-V host management interfaces.
  - Storage Controller VM management interfaces.
  - A roaming HX cluster management interface.
- 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 vmnic interface used for storage traffic for 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 LiveMigration 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 storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa.

Figure 5 illustrates the logical network design.





The reference hardware configuration includes:

- Two Cisco Nexus 93108YCPX switches
- Two Cisco UCS 6332-16UP fabric interconnects
- Eight Cisco HX-series Rack server running HyperFlex data platform version 3.0.1c.

For desktop virtualization, the deployment includes Citrix XenDesktop running on Microsoft Hyper-V. The design is intended to provide a large scale building block for persistent/non-persistent desktops with following density per four-node configuration:

- 1250 Citrix XenDesktop Windows 10 non-persistent virtual desktops using PVS
- 1600 Citrix XenApp Windows 2016 Server Desktops using PVS



All of the Windows 10 virtual desktops were provisioned with 4GB of memory for this study. Typically, persistent desktop users may desire more memory. If more than 4GB memory is needed, the second memory channel on the Cisco HXAF220c-M5SX HX-Series rack server should be populated.

Data provided here will allow customers to run VDI desktops to suit their environment. For example, additional drives can be added in existing server to improve I/O capability and throughput, and special hardware or software features can be added to introduce new features. This document guides you through the low-level steps for deploying the base architecture, as shown in Figure 3. These procedures covers everything from physical cabling to network, compute and storage device configurations.

## Technology Overview

This section describes the infrastructure components used in the solution outlined in this study.

### Cisco Unified Computing System

Cisco UCS Manager (UCSM) provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System<sup>™</sup> (Cisco UCS) and Cisco HyperFlex through an intuitive GUI, a command-line interface (CLI), and an XML API. The manager provides a unified management domain with centralized management capabilities and can control multiple chassis and thousands of virtual machines.

Cisco UCS is a next-generation data center platform that unites computing, networking, 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 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.

#### Cisco Unified Computing System Components

The main components of Cisco UCS are:

- **Compute:** The system is based on an entirely new class of computing system that incorporates blade, rack and hyperconverged servers based on Intel® Xeon® scalable family processors.
- **Network:** The system is integrated on a low-latency, lossless, 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing (HPC) networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables needed, 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**: The Cisco HyperFlex rack servers provide high performance, resilient storage using the powerful HX Data Platform software. Customers can deploy as few as three nodes (replication factor 2/3,) depending on their fault tolerance requirements. These nodes form a HyperFlex storage and compute cluster. The onboard storage of each node is aggregated at the cluster level and automatically shared with all of the nodes.
- **Management:** Cisco UCS uniquely integrates all system components, enabling the entire solution to be managed as a single entity by Cisco UCS Manager. The manager has an intuitive GUI, a CLI, and a robust API for managing all system configuration processes and operations. Our latest advancement offers a cloud-based management system called Cisco Intersight.

Cisco UCS and Cisco HyperFlex are designed to deliver:

- Reduced TCO and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.
- A cohesive, integrated system that 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 Manager provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System across multiple chassis, rack servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager Functions.

The Cisco HyperFlex system provides a fully contained virtual server platform, with compute and memory resources, integrated networking connectivity, a distributed high performance log-structured file system for VM storage, and the hypervisor software for running the virtualized servers, all within a single Cisco UCS management domain.

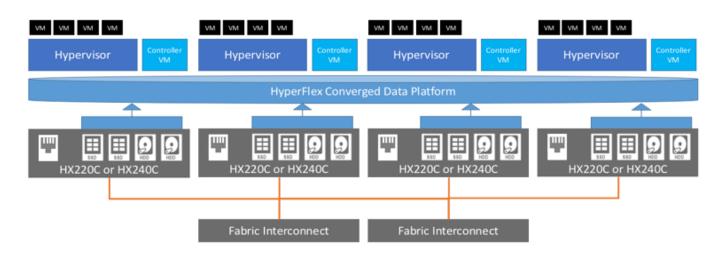


Figure 6 Cisco HyperFlex System Overview

#### Supported Versions and System Requirements

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

For a complete list of requirements, see: Cisco HyperFlex Systems Installation Guide on Microsoft Hyper-V

#### Hardware and Software Interoperability

For a complete list of hardware and software inter-dependencies, refer to respective Cisco UCS Manager release version of <u>Hardware and Software Interoperability for Cisco HyperFlex HX-Series</u>.

#### Software Requirements for Microsoft Hyper-V

The software requirements include verification that you are using compatible versions of Cisco HyperFlex Systems (HX) components and Microsoft Server components.

#### HyperFlex Software Versions

The HX components—Cisco HX Data Platform Installer, Cisco HX Data Platform, and Cisco UCS firmware—are installed on different servers. Verify that each component on each server used with and within an HX Storage Cluster are compatible.

- Verify that the preconfigured HX servers have the same version of Cisco UCS server firmware installed. If the Cisco UCS Fabric Interconnects (FI) firmware versions are different, see the <u>Cisco HyperFlex Systems</u> <u>Upgrade Guide</u> for steps to align the firmware versions.
- M5: For NEW hybrid or All Flash (Cisco HyperFlex HX240c M5 or HX220c M5) deployments, verify that Cisco UCS Manager 3.2(3b) or later is installed.

#### **Cisco UCS Fabric Interconnect**

The Cisco UCS 6300 Series Fabric Interconnects are a core part of Cisco UCS, providing both network connectivity and management capabilities for the system. The Cisco UCS 6300 Series offers line-rate, low-latency, lossless 40 Gigabit Ethernet, FCoE, and Fibre Channel functions.

The fabric interconnects provide the management and communication backbone for the Cisco UCS B-Series Blade Servers, Cisco UCS C-Series and HX-Series rack servers and Cisco UCS 5100 Series Blade Server Chassis. All servers, attached to the fabric interconnects become part of a single, highly available management domain. In addition, by supporting unified fabric, the Cisco UCS 6300 Series provides both LAN and SAN connectivity for all blades in the domain.

For networking, the Cisco UCS 6300 Series uses a cut-through architecture, supporting deterministic, low-latency, line-rate 40 Gigabit Ethernet on all ports, 2.56 terabit (Tb) switching capacity, and 320 Gbps of bandwidth per chassis, independent of packet size and enabled services. The product series supports Cisco low-latency, lossless, 40 Gigabit Ethernet unified network fabric capabilities, increasing the reliability, efficiency, and scalability of Ethernet networks. The fabric interconnects support multiple traffic classes over a lossless Ethernet fabric, from the blade server through the interconnect. 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.

Figure 7 Cisco UCS 6332 Fabric Interconnect

#### Front View



#### **Rear View**



#### Figure 8 Cisco UCS 6332-16UP Fabric Interconnect

#### Front View



#### Cisco HyperFlex HX-Series Nodes

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

A Cisco HyperFlex cluster requires a minimum of three HX-Series 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 singlenode 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 is also equipped with the platform's physical capacity of either spinning disks or enterprise-value SSDs for maximum data capacity.

#### Cisco UCS HXAF220c-M5S Rack Server

The HXAF220c M5 servers extend the capabilities of Cisco's HyperFlex portfolio in a 1U form factor with the addition of the Intel<sup>®</sup> Xeon<sup>®</sup> Processor Scalable Family, 24 DIMM slots for 2666MHz DIMMs, up to 128GB individual DIMM capacities and up to 3.0TB of total DRAM capacities.

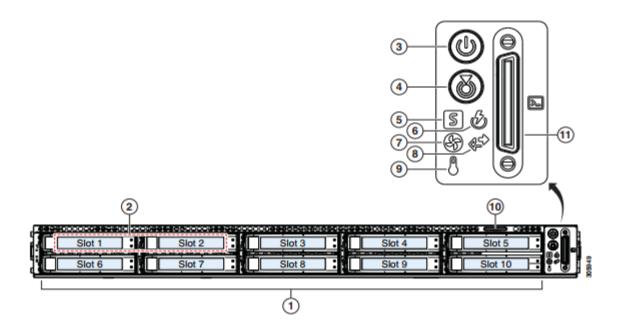
This small footprint configuration of Cisco HyperFlex all-flash nodes contains one M.2 SATA SSD drive that act as the boot drives, a single 240-GB solid-state disk (SSD) data-logging drive, a single 400-GB SSD write-log drive, and up to eight 3.8-terabyte (TB) or 960-GB SATA SSD drives for storage capacity. A minimum of three nodes and a maximum of eight nodes can be configured in one HX cluster. For detailed information, see the <u>Cisco</u> <u>HyperFlex HXAF220c-M5S specsheet</u>.

#### Figure 9 Cisco UCS HXAF220c-M5SX Rack Server Front View

Front View

100	 	 ***************	
1			
1003			AND IN COLUMN

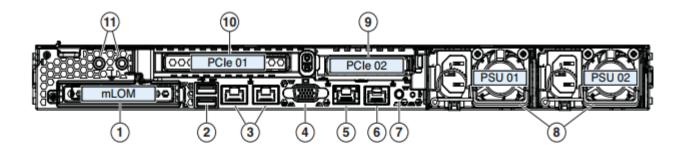
WATER A COLORADO		TATAVATATATATATA
0.0.	altala cisco	HyperFlex



1	Drive Slots	7	Fan status LED
	Slot 01 (For System/Log drive)		
	• 1 x SATA SSD		
	Slot 02 (For Cache drive)		
	1 x NVMe SSD OR		
	• 1 x SAS SSD OR		
	• 1 x SED SAS SSD		
	Slot 03 through 10 (For Capacity drives)		
	Upto 8 x SATA SSD OR		
	• Upto 8 x SED SATA SSD OR		
	• upto 8 x SED SAS SSD		
2	N/A	8	Network link activity LED
3	Power button/Power status LED	9	Temperature status LED
4	Unit identification button/LED	10	Pull-out asset tag
5	System status LED	11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)
6	Power supply status LED	-	-

Figure 10 Cisco UCS HXAF220c-M5SX Rack Server Rear View





1	Modular LAN-on-motherboard (mLOM) card bay (x16)	7	Rear unit identification button/LED
2	USB 3.0 ports (two)	8	Power supplies (two, redundant as 1+1)
3	Dual 1/10-Gb Ethernet ports (LAN1 and LAN2). LAN1 is left connector and LAN2 is right connector	9	PCIe riser 2 (slot 2) (half-height, x16);
4	VGA video port (DB-15)	10	PCIe riser 1 (slot 1) (full-height, x16)
5	1-Gb Ethernet dedicated management port	11	Threaded holes for dual-hole grounding lug
6	Serial port (RJ-45 connector)	-	-

The Cisco UCS HXAF220c-M5S delivers performance, flexibility, and optimization for data centers and remote sites. This enterprise-class server offers market-leading performance, versatility, and density without compromise for workloads ranging from web infrastructure to distributed databases. The Cisco UCS HXAF220c-M5SX can quickly deploy stateless physical and virtual workloads with the programmable ease of use of the Cisco UCS Manager software and simplified server access with Cisco® Single Connect technology. Based on the Intel Xeon scalable family processor product family, it offers up to 1.5TB of memory using 64-GB DIMMs, up to ten disk drives, and up to 40 Gbps of I/O throughput. The Cisco UCS HXAF220c-M5Soffers exceptional levels of performance, flexibility, and I/O throughput to run your most demanding applications.

The Cisco UCS HXAF220c-M5S provides:

- Up to two multicore Intel Xeon scalable family processor for up to 56 processing cores
- 24 DIMM slots for industry-standard DDR4 memory at speeds 2666 MHz, and up to 1.5TB of total memory when using 64-GB DIMMs
- Ten hot-pluggable SAS and SATA HDDs or SSDs
- Cisco UCS VIC 1387, a 2-port, 80 Gigabit Ethernet and FCoE-capable modular (mLOM) mezzanine adapter
- Cisco FlexStorage local drive storage subsystem, with flexible boot and local storage capabilities that allow you to install and boot Hypervisor
- Enterprise-class pass-through RAID controller
- Easily add, change, and remove Cisco FlexStorage modules

#### Cisco VIC 1387 MLOM Interface Card

The Cisco UCS Virtual Interface Card (VIC) 1387 is a dual-port Enhanced Small Form-Factor Pluggable (QSFP+) 40-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)) in a modular LAN-on-motherboard (mLOM) adapter installed in the Cisco UCS HX-Series Rack Servers (Figure 10). 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 that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile.

Figure 11 Cisco VIC 1387 mLOM Card



#### Cisco HyperFlex Converged 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 that you would expect of 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:

- **Replication** replicates 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 client 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.

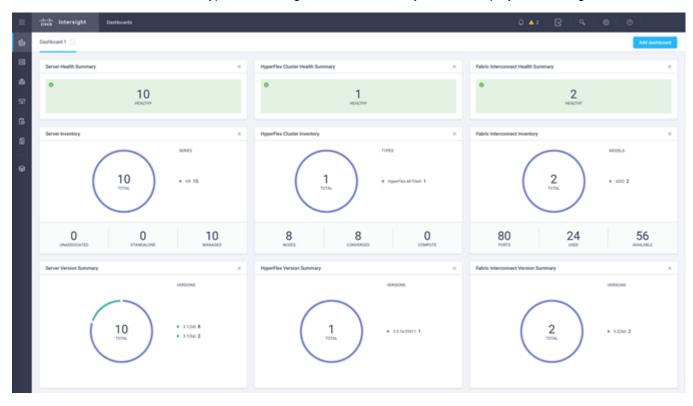
- **Fast, space-efficient clones** rapidly replicate storage volumes so that virtual machines can be replicated simply through metadata operations, with actual data copied only for write operations.
- **Snapshots** help facilitate backup and remote-replication operations: needed in enterprises that require always-on data availability.

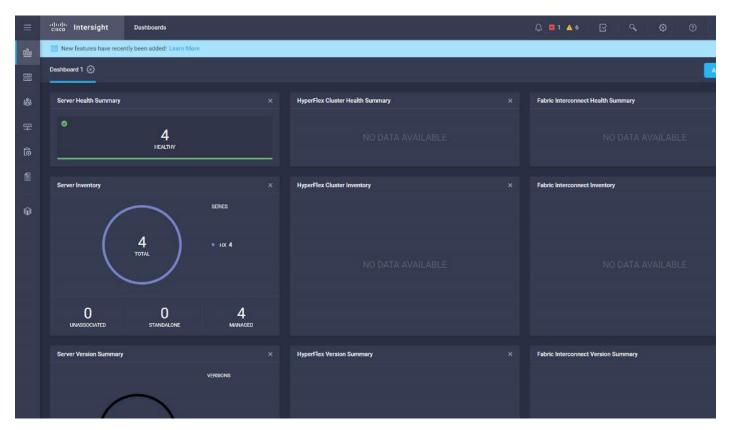
#### Cisco HyperFlex Connect HTML5 Management Web Page

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: <u>http://<hx controller cluster ip></u>.

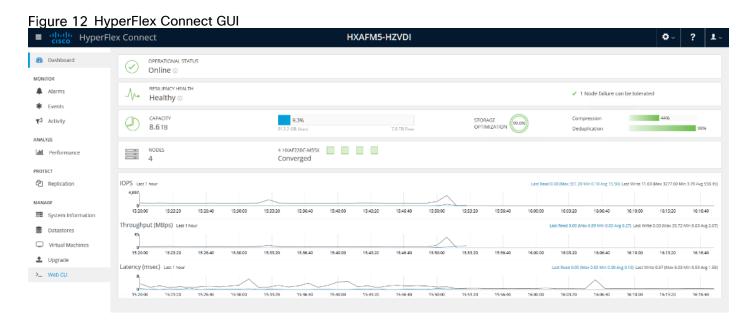
#### Cisco Intersight Management Web Page

Cisco Intersight (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.





≡	altalia cisco	Intersight		Servers					Q 🖬 1 🔺 6	₽ ¢	0	0	<u>گ</u>
<u>080</u>	🗃 New	v features have P	ecently	ly been added! Learn	More								*
				。 Search					25 Rows			1-4of4 🕞 🛙	I O
4		Name		Health	Management IP	Model	CPU Capacity (GHz)	Memory Capacity (GB)	HX Cluster	Server Profile		Utility Storage	Firmware'
<b>P</b>					10.29.132.15	HXAF220C-M5	82.8	768.0		org-root/org-xd-c	vd/ls-rack-i		3.1(2d)
					10.29.132.15	HXAF220C-M5	82.8	768.0		org-root/org-xd-c	vd/ls-rack-t		3.1(2d)
6					10.29.132.15	HXAF220C-M5	82.8	768.0		org-root/org-xd-c	vd/ls-rack-i		3.1(2d)
9					10.29.132.15	HXAF220C-M5	82.8	768.0		org-root/org-xd-c	vd/ls-rack-ı		3.1(2d)
8	•	G Ø										区 1-4of4	4 🛛 🖂



#### **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).

- **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 2 entire nodes without losing data and resorting to restore from backup or other recovery processes.
- 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 1 entire node without losing data and resorting to restore from backup or other recovery processes.

#### **Data Distribution**

Incoming data is distributed across all nodes in the cluster to optimize performance using the caching tier. Effective data distribution is achieved by mapping incoming data to stripe units that are stored evenly across all nodes, with the number of data replicas determined by the policies you set. When an application writes data, the data is sent to the appropriate node based on the stripe unit, which includes the relevant block of information. This data distribution approach in combination with the capability to have multiple streams writing at the same time avoids both network and storage hot spots, delivers the same I/O performance regardless of virtual machine location, and gives you more flexibility in workload placement. This contrasts with other architectures that use a data locality approach that does not fully use available networking and I/O resources and is vulnerable to hot spots.

When moving a virtual machine to a new location using tools such as Hyper-V Cluster Optimization, the Cisco HyperFlex HX Data Platform does not require data to be moved. This approach significantly reduces the impact and cost of moving virtual machines among systems.

#### **Data Operations**

The data platform implements a distributed, log-structured file system that changes how it handles caching and storage capacity depending on the node configuration.

In the all-flash-memory configuration, the data platform uses a caching layer in SSDs to accelerate write responses, and it implements the capacity layer in SSDs. Read requests are fulfilled directly from data obtained from the SSDs in the capacity layer. A dedicated read cache is not required to accelerate read operations.

Incoming data is striped across the number of nodes required to satisfy availability requirements—usually two or three nodes. Based on policies you set, incoming write operations are acknowledged as persistent after they are replicated to the SSD drives in other nodes in the cluster. This approach reduces the likelihood of data loss due to SSD or node failures. The write operations are then de-staged to SSDs in the capacity layer in the all-flash memory configuration for long-term storage.

The log-structured file system writes sequentially to one of two write logs (three in case of RF=3) until it is full. It then switches to the other write log while de-staging data from the first to the capacity tier. When existing data is (logically) overwritten, the log-structured approach simply appends a new block and updates the metadata. This layout benefits SSD configurations in which seek operations are not time consuming. It reduces the write amplification levels of SSDs and the total number of writes the flash media experiences due to incoming writes and random overwrite operations of the data.

When data is de-staged to the capacity tier in each node, the data is deduplicated and compressed. This process occurs after the write operation is acknowledged, so no performance penalty is incurred for these operations. A small deduplication block size helps increase the deduplication rate. Compression further reduces the data footprint. Data is then moved to the capacity tier as write cache segments are released for reuse (Figure 13).

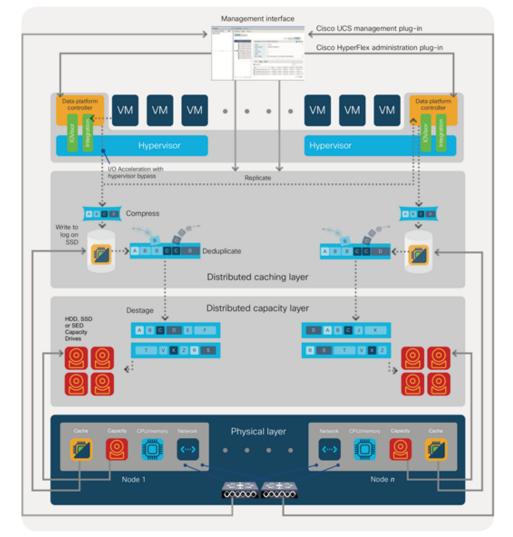


Figure 13 Data Write Operation Flow Through the Cisco HyperFlex HX Data Platform

Hot data sets, data that are frequently or recently read from the capacity tier, are cached in memory. All-Flash configurations, however, does not use an SSD read cache since there is no performance benefit of such a cache; the persistent data copy already resides on high-performance SSDs. In these configurations, a read cache implemented with SSDs could become a bottleneck and prevent the system from using the aggregate bandwidth of the entire set of SSDs.

#### **Data Optimization**

The Cisco HyperFlex HX Data Platform provides finely detailed inline deduplication and variable block inline compression that is always on for objects in the cache (SSD and memory) and capacity (SSD or HDD) layers. Unlike other solutions, which require you to turn off these features to maintain performance, the deduplication and compression capabilities in the Cisco data platform are designed to sustain and enhance performance and significantly reduce physical storage capacity requirements.

#### Data Deduplication

Data deduplication is used on all storage in the cluster, including memory and SSD drives. Based on a patentpending Top-K Majority algorithm, the platform uses conclusions from empirical research that show that most data, when sliced into small data blocks, has significant deduplication potential based on a minority of the data blocks. By fingerprinting and indexing just these frequently used blocks, high rates of deduplication can be achieved with only a small amount of memory, which is a high-value resource in cluster nodes (Figure 14).

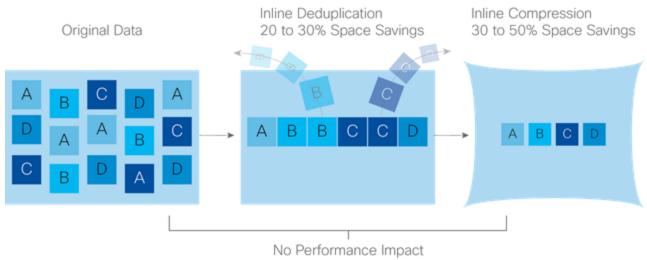


Figure 14 Cisco HyperFlex HX Data Platform Optimizes Data Storage with No Performance Impact

#### **Inline Compression**

The Cisco HyperFlex HX Data Platform uses high-performance inline compression on data sets to save storage capacity. Although other products offer compression capabilities, many negatively affect performance. In contrast, the Cisco data platform uses CPU-offload instructions to reduce the performance impact of compression operations. In addition, the log-structured distributed-objects layer has no effect on modifications (write operations) to previously compressed data. Instead, incoming modifications are compressed and written to a new location, and the existing (old) data is marked for deletion, unless the data needs to be retained in a snapshot.

The data that is being modified does not need to be read prior to the write operation. This feature avoids typical read-modify-write penalties and significantly improves write performance.

#### Log-Structured Distributed Objects

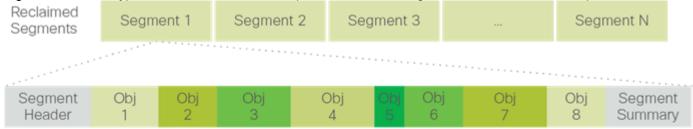
In the Cisco HyperFlex HX Data Platform, the log-structured distributed-object store layer groups and compresses data that filters through the deduplication engine into self-addressable objects. These objects are written to disk in a log-structured, sequential manner. All incoming I/O—including random I/O—is written sequentially to both the

caching (SSD and memory) and persistent (SSD or HDD) tiers. The objects are distributed across all nodes in the cluster to make uniform use of storage capacity.

By using a sequential layout, the platform helps increase flash-memory endurance. Because read-modify-write operations are not used, there is little or no performance impact of compression, snapshot operations, and cloning on overall performance.

Data blocks are compressed into objects and sequentially laid out in fixed-size segments, which in turn are sequentially laid out in a log-structured manner (Figure 15). Each compressed object in the log-structured segment is uniquely addressable using a key, with each key fingerprinted and stored with a checksum to provide high levels of data integrity. In addition, the chronological writing of objects helps the platform quickly recover from media or node failures by rewriting only the data that came into the system after it was truncated due to a failure.

Figure 15 Cisco HyperFlex HX Data Platform Optimizes Data Storage with No Performance Impact





#### Encryption

Securely encrypted storage optionally encrypts both the caching and persistent layers of the data platform. Integrated with enterprise key management software, or with passphrase-protected keys, encrypting data at rest helps you comply with HIPAA, PCI-DSS, FISMA, and SOX regulations. The platform itself is hardened to Federal Information Processing Standard (FIPS) 140-1 and the encrypted drives with key management comply with the FIPS 140-2 standard.

#### **Data Services**

The Cisco HyperFlex HX Data Platform provides a scalable implementation of space-efficient data services, including thin provisioning, space reclamation, pointer-based snapshots, and clones, without affecting performance.

#### Thin Provisioning

The platform makes efficient use of storage by eliminating the need to forecast, purchase, and install disk capacity that may remain unused for a long time. Virtual data containers can present any amount of logical space to applications, whereas the amount of physical storage space that is needed is determined by the data that is written. You can expand storage on existing nodes and expand your cluster by adding more storage-intensive nodes as your business requirements dictate, eliminating the need to purchase large amounts of storage before you need it.

#### Snapshots

The Cisco HyperFlex HX Data Platform uses metadata-based, zero-copy snapshots to facilitate backup operations and remote replication: critical capabilities in enterprises that require always-on data availability. Space-efficient snapshots allow you to perform frequent online data backups without worrying about the consumption of physical storage capacity. Data can be moved offline or restored from these snapshots instantaneously.

• **Fast snapshot updates**: When modified-data is contained in a snapshot, it is written to a new location, and the metadata is updated, without the need for read-modify-write operations.

- **Rapid snapshot deletions**: You can quickly delete snapshots. The platform simply deletes a small amount of metadata that is located on an SSD, rather than performing a long consolidation process as needed by solutions that use a delta-disk technique.
- **Highly specific snapshots**: With the Cisco HyperFlex HX Data Platform, you can take snapshots on an individual file basis. In virtual environments, these files map to drives in a virtual machine. This flexible specificity allows you to apply different snapshot policies on different virtual machines.

Many basic backup applications, read the entire dataset, or the changed blocks since the last backup at a rate that is usually as fast as the storage, or the operating system can handle. This can cause performance implications since HyperFlex is built on Cisco UCS with 10GbE which could result in multiple gigabytes per second of backup throughput. These basic backup applications, such as Windows Server Backup, should be scheduled during off-peak hours, particularly the initial backup if the application lacks some form of change block tracking.

Full featured backup applications, such as <u>Veeam Backup and Replication v9.5</u>, have the ability to limit the amount of throughput the backup application can consume which can protect latency sensitive applications during the production hours. With the release of v9.5 update 2, Veeam is the first partner to <u>integrate HX native</u> <u>snapshots</u> into the product. HX Native snapshots do not suffer the performance penalty of delta-disk snapshots, and do not require heavy disk IO impacting consolidation during snapshot deletion.

Particularly important for SQL administrators is the <u>Veeam Explorer for SQL</u> which can provide transaction level recovery within the <u>Microsoft VSS framework</u>. The three ways Veeam Explorer for SQL Server works to restore SQL Server databases include; from the backup restore point, from a log replay to a point in time, and from a log replay to a specific transaction – all without taking the VM or SQL Server offline.

#### Fast, Space-Efficient Clones

In the Cisco HyperFlex HX Data Platform, clones are writable snapshots that can be used to rapidly provision items such as virtual desktops and applications for test and development environments. These fast, space-efficient clones rapidly replicate storage volumes so that virtual machines can be replicated through just metadata operations, with actual data copying performed only for write operations. With this approach, hundreds of clones can be created and deleted in minutes. Compared to full-copy methods, this approach can save a significant amount of time, increase IT agility, and improve IT productivity.

Clones are deduplicated when they are created. When clones start diverging from one another, data that is common between them is shared, with only unique data occupying new storage space. The deduplication engine eliminates data duplicates in the diverged clones to further reduce the clone's storage footprint.

#### Data Replication and Availability

In the Cisco HyperFlex HX Data Platform, the log-structured distributed-object layer replicates incoming data, improving data availability. Based on policies that you set, data that is written to the write cache is synchronously replicated to one or two other SSD drives located in different nodes before the write operation is acknowledged to the application. This approach allows incoming writes to be acknowledged quickly while protecting data from SSD or node failures. If an SSD or node fails, the replica is quickly re-created on other SSD drives or nodes using the available copies of the data.

The log-structured distributed-object layer also replicates data that is moved from the write cache to the capacity layer. This replicated data is likewise protected from SSD or node failures. With two replicas, or a total of three data copies, the cluster can survive uncorrelated failures of two SSD drives or two nodes without the risk of data loss. Uncorrelated failures are failures that occur on different physical nodes. Failures that occur on the same node affect the same copy of data and are treated as a single failure. For example, if one disk in a node fails and subsequently another disk on the same node fails, these correlated failures count as one failure in the system. In this case, the cluster could withstand another uncorrelated failure on a different node. See the Cisco HyperFlex HX Data Platform system administrator's guide for a complete list of fault-tolerant configurations and settings.

If a problem occurs in the Cisco HyperFlex HX controller software, data requests from the applications residing in that node are automatically routed to other controllers in the cluster. This same capability can be used to upgrade or perform maintenance on the controller software on a rolling basis without affecting the availability of the cluster

or data. This self-healing capability is one of the reasons that the Cisco HyperFlex HX Data Platform is well suited for production applications.

In addition, native replication transfers consistent cluster data to local or remote clusters. With native replication, you can snapshot and store point-in-time copies of your environment in local or remote environments for backup and disaster recovery purposes.

#### Data Rebalancing

A distributed file system requires a robust data rebalancing capability. In the Cisco HyperFlex HX Data Platform, no overhead is associated with metadata access, and rebalancing is extremely efficient. Rebalancing is a nondisruptive online process that occurs in both the caching and persistent layers, and data is moved at a fine level of specificity to improve the use of storage capacity. The platform automatically rebalances existing data when nodes and drives are added or removed or when they fail. When a new node is added to the cluster, its capacity and performance is made available to new and existing data. The rebalancing engine distributes existing data to the new node and helps ensure that all nodes in the cluster are used uniformly from capacity and performance perspectives. If a node fails or is removed from the cluster, the rebalancing engine rebuilds and distributes copies of the data from the failed or removed node to available nodes in the clusters.

#### Online Upgrades

Cisco HyperFlex HX-Series systems and the HX Data Platform support online upgrades so that you can expand and update your environment without business disruption. You can easily expand your physical resources; add processing capacity; and download and install BIOS, driver, hypervisor, firmware, and Cisco UCS Manager updates, enhancements, and bug fixes.

#### Cisco Nexus 93108YCPX Switches

The Cisco Nexus 93180YC-EX Switch has 48 1/10/25G-Gbps Small Form Pluggable Plus (SFP+) ports and 6 40/100-Gbps Quad SFP+ (QSFP+) uplink ports. All ports are line rate, delivering 3.6 Tbps of throughput in a 1-rack-unit (1RU) form factor.

#### Architectural Flexibility

- Includes top-of-rack, fabric extender aggregation, or middle-of-row fiber-based server access connectivity for traditional and leaf-spine architectures
- Includes leaf node support for Cisco ACI architecture
- Increase scale and simplify management through Cisco Nexus 2000 Fabric Extender support

#### Feature-Rich

- Enhanced Cisco NX-OS Software is designed for performance, resiliency, scalability, manageability, and programmability
- ACI-ready infrastructure helps users take advantage of automated policy-based systems management
- Virtual extensible LAN (VXLAN) routing provides network services
- Rich traffic flow telemetry with line-rate data collection
- Real-time buffer utilization per port and per queue, for monitoring traffic micro-bursts and application traffic patterns

#### Real-Time Visibility and Telemetry

- Cisco Tetration Analytics Platform support with built-in hardware sensors for rich traffic flow telemetry and line-rate data collection
- Cisco Nexus Data Broker support for network traffic monitoring and analysis
- Real-time buffer utilization per port and per queue, for monitor traffic micro-bursts and application traffic patterns

#### Highly Available and Efficient Design

- High-performance, non-blocking architecture
- Easily deployed into either a hot-aisle and cold-aisle configuration
- Redundant, hot-swappable power supplies and fan trays

#### Simplified Operations

- Pre-boot execution environment (PXE) and Power-On Auto Provisioning (POAP) support allows for simplified software upgrades and configuration file installation
- Automate and configure switches with DevOps tools like Puppet, Chef, and Ansible
- An intelligent API offers switch management through remote procedure calls (RPCs, JSON, or XML) over a HTTP/HTTPS infrastructure
- Python scripting gives programmatic access to the switch command-line interface (CLI)
- Includes hot and cold patching, and online diagnostics

#### **Investment Protection**

- A Cisco 40-Gb <u>bidirectional transceiver</u> allows for reuse of an existing 10 Gigabit Ethernet multimode cabling plant for 40 Gigabit Ethernet
- Support for 10-Gb and 25-Gb access connectivity and 40-Gb and 100-Gb uplinks facilitate data centers
  migrating switching infrastructure to faster speeds
- 1.44 Tbps of bandwidth in a 1 RU form factor
- 48 fixed 1/10-Gbps SFP+ ports
- 6 fixed 40-Gbps QSFP+ for uplink connectivity that can be turned into 10 Gb ports through a QSFP to SFP or SFP+ Adapter (QSA)
- Latency of 1 to 2 microseconds
- Front-to-back or back-to-front airflow configurations
- 1+1 redundant hot-swappable 80 Plus Platinum-certified power supplies
- Hot swappable 2+1 redundant fan tray

#### Figure 16 Cisco Nexus 93108YC Switch



#### Microsoft Hyper-V 2016

Hyper-V is Microsoft's hardware virtualization product. It lets you create and run a software version of a computer, called a virtual machine. Each virtual machine acts like a complete computer, running an operating system and programs. When you need computing resources, virtual machines give you more flexibility, help save time and money, and are a more efficient way to use hardware than just running one operating system on physical hardware.

Hyper-V runs each virtual machine in its own isolated space, which means you can run more than one virtual machine on the same hardware at the same time. You might want to do this to avoid problems such as a crash affecting the other workloads, or to give different people, groups or services access to different systems.

#### Microsoft System Center 2016

This document does not cover the steps to install Microsoft System Center Operations Manager (SCOM) and Virtual Machine Manager (SCVMM). Follow the Microsoft guidelines to install SCOM and SCVMM 2016:

- SCOM: <u>https://docs.microsoft.com/en-us/system-center/scom/deploy-overview</u>
- SCVMM: <a href="https://docs.microsoft.com/en-us/system-center/vmm/install-console">https://docs.microsoft.com/en-us/system-center/vmm/install-console</a>

#### Citrix XenApp<sup>™</sup> and XenDesktop<sup>™</sup> 7.16

Enterprise IT organizations are tasked with the challenge of provisioning Microsoft Windows apps and desktops while managing cost, centralizing control, and enforcing corporate security policy. Deploying Windows apps to users in any location, regardless of the device type and available network bandwidth, enables a mobile workforce that can improve productivity. With Citrix XenDesktop 7.16, IT can effectively control app and desktop provisioning while securing data assets and lowering capital and operating expenses.

The XenDesktop 7.16 release offers these benefits:

- **Comprehensive virtual desktop delivery for any use case**. The XenDesktop 7.16 release incorporates the full power of XenApp, delivering full desktops or just applications to users. Administrators can deploy both XenApp published applications and desktops (to maximize IT control at low cost) or personalized VDI desktops (with simplified image management) from the same management console. Citrix XenDesktop 7.16 leverages common policies and cohesive tools to govern both infrastructure resources and user access.
- Simplified support and choice of BYO (Bring Your Own) devices. XenDesktop 7.16 brings thousands of corporate Microsoft Windows-based applications to mobile devices with a native-touch experience and optimized performance. HDX technologies create a "high definition" user experience, even for graphics intensive design and engineering applications.

- Lower cost and complexity of application and desktop management. XenDesktop 7.16 helps IT organizations take advantage of agile and cost-effective cloud offerings, allowing the virtualized infrastructure to flex and meet seasonal demands or the need for sudden capacity changes. IT organizations can deploy XenDesktop application and desktop workloads to private or public clouds.
- **Protection of sensitive information through centralization**. XenDesktop decreases the risk of corporate data loss, enabling access while securing intellectual property and centralizing applications since assets reside in the datacenter.
- Virtual Delivery Agent improvements. Universal print server and driver enhancements and support for the HDX 3D Pro graphics acceleration for Windows 10 are key additions in XenDesktop 7.16
- **Improved high-definition user experience.** XenDesktop 7.16 continues the evolutionary display protocol leadership with enhanced Thinwire display remoting protocol and Framehawk support for HDX 3D Pro.

Citrix XenApp and XenDesktop are application and desktop virtualization solutions built on a unified architecture so they're simple to manage and flexible enough to meet the needs of all your organization's users. XenApp and XenDesktop have a common set of management tools that simplify and automate IT tasks. You use the same architecture and management tools to manage public, private, and hybrid cloud deployments as you do for on premises deployments.

Citrix XenApp delivers:

- XenApp published apps, also known as server-based hosted applications: These are applications hosted from Microsoft Windows servers to any type of device, including Windows PCs, Macs, smartphones, and tablets. Some XenApp editions include technologies that further optimize the experience of using Windows applications on a mobile device by automatically translating native mobile-device display, navigation, and controls to Windows applications; enhancing performance over mobile networks; and enabling developers to optimize any custom Windows application for any mobile environment.
- XenApp published desktops, also known as server-hosted desktops: These are inexpensive, locked-down Windows virtual desktops hosted from Windows server operating systems. They are well suited for users, such as call center employees, who perform a standard set of tasks.
- Virtual machine-hosted apps: These are applications hosted from machines running Windows desktop operating systems for applications that can't be hosted in a server environment.
- Windows applications delivered with Microsoft App-V: These applications use the same management tools that you use for the rest of your XenApp deployment.
- Citrix XenDesktop: Includes significant enhancements to help customers deliver Windows apps and desktops as mobile services while addressing management complexity and associated costs. Enhancements in this release include:
- Unified product architecture for XenApp and XenDesktop: The FlexCast Management Architecture (FMA). This release supplies a single set of administrative interfaces to deliver both hosted-shared applications (RDS) and complete virtual desktops (VDI). Unlike earlier releases that separately provisioned Citrix XenApp and XenDesktop farms, the XenDesktop 7.16 release allows administrators to deploy a single infrastructure and use a consistent set of tools to manage mixed application and desktop workloads.
- Support for extending deployments to the cloud. This release provides the ability for hybrid cloud provisioning from Microsoft Azure, Amazon Web Services (AWS) or any Cloud Platform-powered public or private cloud. Cloud deployments are configured, managed, and monitored through the same administrative consoles as deployments on traditional on-premises infrastructure.

Citrix XenDesktop delivers:

- VDI desktops: These virtual desktops each run a Microsoft Windows desktop operating system rather than running in a shared, server-based environment. They can provide users with their own desktops that they can fully personalize.
- Hosted physical desktops: This solution is well suited for providing secure access powerful physical machines, such as blade servers, from within your data center.
- Remote PC access: This solution allows users to log in to their physical Windows PC from anywhere over a secure XenDesktop connection.
- Server VDI: This solution is designed to provide hosted desktops in multitenant, cloud environments.
- Capabilities that allow users to continue to use their virtual desktops: These capabilities let users continue to work while not connected to your network.

This product release includes the following new and enhanced features:



Some XenDesktop editions include the features available in XenApp.

### Zones

Deployments that span widely-dispersed locations connected by a WAN can face challenges due to network latency and reliability. Configuring zones can help users in remote regions connect to local resources without forcing connections to traverse large segments of the WAN. Using zones allows effective Site management from a single Citrix Studio console, Citrix Director, and the Site database. This saves the costs of deploying, staffing, licensing, and maintaining additional Sites containing separate databases in remote locations.

Zones can be helpful in deployments of all sizes. You can use zones to keep applications and desktops closer to end users, which improves performance.

For more information, see the <u>Zones</u> article.

### Improved Database Flow and Configuration

When you configure the databases during Site creation, you can now specify separate locations for the Site, Logging, and Monitoring databases. Later, you can specify different locations for all three databases. In previous releases, all three databases were created at the same address, and you could not specify a different address for the Site database later.

You can now add more Delivery Controllers when you create a Site, as well as later. In previous releases, you could add more Controllers only after you created the Site.

For more information, see the <u>Databases</u> and <u>Controllers</u> articles.

### **Application Limits**

Configure application limits to help manage application use. For example, you can use application limits to manage the number of users accessing an application simultaneously. Similarly, application limits can be used to manage the number of simultaneous instances of resource-intensive applications, this can help maintain server performance and prevent deterioration in service.

For more information, see the <u>Manage applications</u> article.

### Multiple Notifications before Machine Updates or Scheduled Restarts

You can now choose to repeat a notification message that is sent to affected machines before the following types of actions begin:

- Updating machines in a Machine Catalog using a new master image
- Restarting machines in a Delivery Group according to a configured schedule

If you indicate that the first message should be sent to each affected machine 15 minutes before the update or restart begins, you can also specify that the message be repeated every five minutes until the update/restart begins.

For more information, see the Manage Machine Catalogs and Manage machines in Delivery Groups articles.

## API Support for Managing Session Roaming

By default, sessions roam between client devices with the user. When the user launches a session and then moves to another device, the same session is used and applications are available on both devices. The applications follow, regardless of the device or whether current sessions exist. Similarly, printers and other resources assigned to the application follow.



You can now use the PowerShell SDK to tailor session roaming. This was an experimental feature in the previous release.

For more information, see the <u>Sessions</u> article.

## API Support for Provisioning VMs from Hypervisor Templates

When using the PowerShell SDK to create or update a Machine Catalog, you can now select a template from other hypervisor connections. This is in addition to the currently-available choices of VM images and snapshots.

### Support for New and Additional Platforms

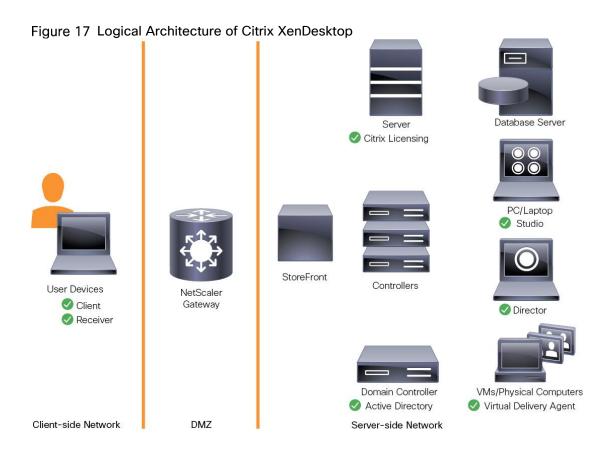
See the <u>System requirements</u> article for full support information. Information about support for third-party product versions is updated periodically.

By default, SQL Server 2012 Express SP2 is installed when you install the Delivery Controller. SP1 is no longer installed.

The component installers now automatically deploy newer Microsoft Visual C++ runtime versions: 32-bit and 64-bit Microsoft Visual C++ 2013, 2010 SP1, and 2008 SP1. Visual C++ 2005 is no longer deployed.

You can install Studio or VDAs for Windows Desktop OS on machines running Windows 10.

You can create connections to Microsoft Azure virtualization resources.



## Citrix Provisioning Services 7.16

Most enterprises struggle to keep up with the proliferation and management of computers in their environments. Each computer, whether it is a desktop PC, a server in a data center, or a kiosk-type device, must be managed as an individual entity. The benefits of distributed processing come at the cost of distributed management. It costs time and money to set up, update, support, and ultimately decommission each computer. The initial cost of the machine is often dwarfed by operating costs.

Citrix PVS takes a very different approach from traditional imaging solutions by fundamentally changing the relationship between hardware and the software that runs on it. By streaming a single shared disk image (vDisk) rather than copying images to individual machines, PVS enables organizations to reduce the number of disk images that they manage, even as the number of machines continues to grow, simultaneously providing the efficiency of centralized management and the benefits of distributed processing.

In addition, because machines are streaming disk data dynamically and in real time from a single shared image, machine image consistency is essentially ensured. At the same time, the configuration, applications, and even the OS of large pools of machines can be completed changed in the time it takes the machines to reboot.

Using PVS, any vDisk can be configured in standard-image mode. A vDisk in standard-image mode allows many computers to boot from it simultaneously, greatly reducing the number of images that must be maintained and the amount of storage that is required. The vDisk is in read-only format, and the image cannot be changed by target devices.

## Benefits for Citrix XenApp and Other Server Farm Administrators

If you manage a pool of servers that work as a farm, such as Citrix XenApp servers or web servers, maintaining a uniform patch level on your servers can be difficult and time consuming. With traditional imaging solutions, you start with a clean golden master image, but as soon as a server is built with the master image, you must patch that individual server along with all the other individual servers. Rolling out patches to individual servers in your farm is

not only inefficient, but the results can also be unreliable. Patches often fail on an individual server, and you may not realize you have a problem until users start complaining or the server has an outage. After that happens, getting the server resynchronized with the rest of the farm can be challenging, and sometimes a full reimaging of the machine is required.

With Citrix PVS, patch management for server farms is simple and reliable. You start by managing your golden image, and you continue to manage that single golden image. All patching is performed in one place and then streamed to your servers when they boot. Server build consistency is assured because all your servers use a single shared copy of the disk image. If a server becomes corrupted, simply reboot it, and it is instantly back to the known good state of your master image. Upgrades are extremely fast to implement. After you have your updated image ready for production, you simply assign the new image version to the servers and reboot them. You can deploy the new image to any number of servers in the time it takes them to reboot. Just as important, rollback can be performed in the same way, so problems with new images do not need to take your servers or your users out of commission for an extended period of time.

## Benefits for Desktop Administrators

Because Citrix PVS is part of Citrix XenDesktop, desktop administrators can use PVS's streaming technology to simplify, consolidate, and reduce the costs of both physical and virtual desktop delivery. Many organizations are beginning to explore desktop virtualization. Although virtualization addresses many of IT's needs for consolidation and simplified management, deploying it also requires deployment of supporting infrastructure. Without PVS, storage costs can make desktop virtualization too costly for the IT budget. However, with PVS, IT can reduce the amount of storage required for VDI by as much as 90 percent. And with a single image to manage instead of hundreds or thousands of desktops, PVS significantly reduces the cost, effort, and complexity for desktop administration.

Different types of workers across the enterprise need different types of desktops. Some require simplicity and standardization, and others require high performance and personalization. XenDesktop can meet these requirements in a single solution using Citrix FlexCast delivery technology. With FlexCast, IT can deliver every type of virtual desktop, each specifically tailored to meet the performance, security, and flexibility requirements of each individual user.

Not all desktops applications can be supported by virtual desktops. For these scenarios, IT can still reap the benefits of consolidation and single-image management. Desktop images are stored and managed centrally in the data center and streamed to physical desktops on demand. This model works particularly well for standardized desktops such as those in lab and training environments and call centers and thin-client devices used to access virtual desktops.

## **Citrix Provisioning Services Solution**

Citrix PVS streaming technology allows computers to be provisioned and re-provisioned in real time from a single shared disk image. With this approach, administrators can completely eliminate the need to manage and patch individual systems. Instead, all image management is performed on the master image. The local hard drive of each system can be used for runtime data caching or, in some scenarios, removed from the system entirely, which reduces power use, system failure rate, and security risk.

The PVS solution's infrastructure is based on software-streaming technology. After PVS components are installed and configured, a vDisk is created from a device's hard drive by taking a snapshot of the OS and application image and then storing that image as a vDisk file on the network. A device used for this process is referred to as a master target device. The devices that use the vDisks are called target devices. vDisks can exist on a PVS, file share, or in larger deployments, on a storage system with which PVS can communicate (iSCSI, SAN, network-attached storage [NAS], and Common Internet File System [CIFS]). vDisks can be assigned to a single target device in private-image mode, or to multiple target devices in standard-image mode.

## Citrix Provisioning Services Infrastructure

The Citrix PVS infrastructure design directly relates to administrative roles within a PVS farm. The PVS administrator role determines which components that administrator can manage or view in the console.

A PVS farm contains several components. Figure 18 provides a high-level view of a basic PVS infrastructure and shows how PVS components might appear within that implementation.

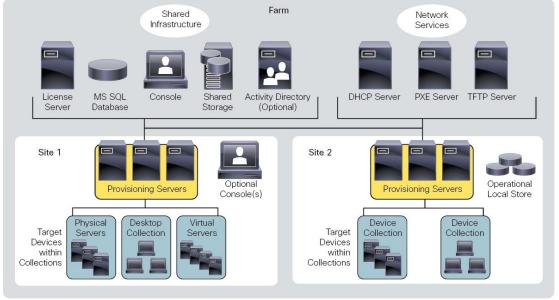


Figure 18 Logical Architecture of Citrix Provisioning Services

The following new features are available with Provisioning Services 7.16:

- Linux streaming
- XenServer proxy using PVS-Accelerator

# Architecture and Design of Citrix XenDesktop on Cisco Unified Computing System and Cisco HyperFlex Storage Design Fundamentals

There are many reasons to consider a virtual desktop solution such as an ever growing and diverse base of user devices, complexity in management of traditional desktops, security, and even Bring Your Own Computer (BYOC) to work programs. The first step in designing a virtual desktop solution is to understand the user community and the type of tasks that are required to successfully execute their role. The following user classifications are provided:

- Knowledge Workers today do not just work in their offices all day they attend meetings, visit branch
  offices, work from home, and even coffee shops. These anywhere workers expect access to all of their
  same applications and data wherever they are.
- External Contractors are increasingly part of your everyday business. They need access to certain portions of your applications and data, yet administrators still have little control over the devices they use and the locations they work from. Consequently, IT is stuck making trade-offs on the cost of providing these workers a device vs. the security risk of allowing them access from their own devices.
- Task Workers perform a set of well-defined tasks. These workers access a small set of applications and have limited requirements from their PCs. However, since these workers are interacting with your customers, partners, and employees, they have access to your most critical data.

- Mobile Workers need access to their virtual desktop from everywhere, regardless of their ability to connect to a network. In addition, these workers expect the ability to personalize their PCs, by installing their own applications and storing their own data, such as photos and music, on these devices.
- Shared Workstation users are often found in state-of-the-art universities and business computer labs, conference rooms or training centers. Shared workstation environments have the constant requirement to re-provision desktops with the latest operating systems and applications as the needs of the organization change, tops the list.

After the user classifications have been identified and the business requirements for each user classification have been defined, it becomes essential to evaluate the types of virtual desktops that are needed based on user requirements. There are essentially five potential desktops environments for each user:

- Traditional PC: A traditional PC is what typically constituted a desktop environment; physical device with a locally installed operating system.
- Hosted Shared Desktop: A hosted, server-based desktop is a desktop where the user interacts through a
  delivery protocol. With hosted, server-based desktops, a single installed instance of a server operating
  system, such as Microsoft Windows Server 2012, is shared by multiple users simultaneously. Each user
  receives a desktop "session" and works in an isolated memory space. Changes made by one user could
  impact the other users.
- Hosted Virtual Desktop: A hosted virtual desktop is a virtual desktop running either on virtualization layer (ESX) or on bare metal hardware. The user does not work with and sit in front of the desktop, but instead the user interacts through a delivery protocol.
- Published Applications: Published applications run entirely on the Microsoft Session Hosts and the user interacts through a delivery protocol. With published applications, a single installed instance of an application, such as Microsoft, is shared by multiple users simultaneously. Each user receives an application "session" and works in an isolated memory space.
- Streamed Applications: Streamed desktops and applications run entirely on the user's local client device and are sent from a server on demand. The user interacts with the application or desktop directly but the resources may only available while they are connected to the network.
- Local Virtual Desktop: A local virtual desktop is a desktop running entirely on the user's local device and continues to operate when disconnected from the network. In this case, the user's local device is used as a type 1 hypervisor and is synced with the data center when the device is connected to the network.

For the purposes of the validation represented in this document, both XenDesktop Virtual Desktops and XenApp Hosted Shared Desktop server sessions were validated. Each of the sections provides some fundamental design decisions for this environment.

## Understanding Applications and Data

When the desktop user groups and sub-groups have been identified, the next task is to catalog group application and data requirements. This can be one of the most time-consuming processes in the VDI planning exercise, but is essential for the VDI project's success. If the applications and data are not identified and co-located, performance will be negatively affected.

The process of analyzing the variety of application and data pairs for an organization will likely be complicated by the inclusion cloud applications, like SalesForce.com. This application and data analysis is beyond the scope of this Cisco Validated Design, but should not be omitted from the planning process. There are a variety of third party tools available to assist organizations with this crucial exercise.

## Project Planning and Solution Sizing Sample Questions

Now that user groups, their applications, and their data requirements are understood, some key project and solution sizing questions may be considered.

General project questions should be addressed at the outset, including:

- Has a VDI pilot plan been created based on the business analysis of the desktop groups, applications, and data?
- Is there infrastructure and budget in place to run the pilot program?
- Are the required skill sets to execute the VDI project available? Can we hire or contract for them?
- Do we have end user experience performance metrics identified for each desktop sub-group?
- How will we measure success or failure?
- What is the future implication of success or failure?

Below is a short, non-exhaustive list of sizing questions that should be addressed for each user sub-group:

- What is the desktop OS planned? Windows 7, Windows 8, or Windows 10?
- 32-bit or 64-bit desktop OS?
- How many virtual desktops will be deployed in the pilot? In production? All Windows 7/8/10?
- How much memory per target desktop group desktop?
- Are there any rich media, Flash, or graphics-intensive workloads?
- What is the end point graphics processing capability?
- Will Citrix XenApp for Remote Desktop Server Hosted Sessions used?
- What is the hypervisor for the solution?
- What is the storage configuration in the existing environment?
- Are there sufficient IOPS available for the write-intensive VDI workload?
- Will there be storage dedicated and tuned for VDI service?
- Is there a voice component to the desktop?
- Is anti-virus a part of the image?
- Is user profile management (for example, non-roaming profile based) part of the solution?
- What is the fault tolerance, failover, disaster recovery plan?
- Are there additional desktop sub-group specific questions?

# Citrix XenDesktop Design Fundamentals

An ever growing and diverse base of user devices, complexity in management of traditional desktops, security, and even Bring Your Own (BYO) device to work programs are prime reasons for moving to a virtual desktop solution.

Citrix XenDesktop 7.16 integrates Hosted Shared and VDI desktop virtualization technologies into a unified architecture that enables a scalable, simple, efficient, and manageable solution for delivering Windows applications and desktops as a service.

Users can select applications from an easy-to-use "store" that is accessible from tablets, smartphones, PCs, Macs, and thin clients. XenDesktop delivers a native touch-optimized experience with HDX high-definition performance, even over mobile networks.

### Machine Catalogs

Collections of identical Virtual Machines (VMs) or physical computers are managed as a single entity called a Machine Catalog. In this CVD, VM provisioning relies on Citrix Provisioning Services to make sure that the machines in the catalog are consistent. In this CVD, machines in the Machine Catalog are configured to run either a Windows Server OS (for RDS hosted shared desktops) or a Windows Desktop OS (for hosted pooled VDI desktops).

### **Delivery Groups**

To deliver desktops and applications to users, you create a Machine Catalog and then allocate machines from the catalog to users by creating Delivery Groups. Delivery Groups provide desktops, applications, or a combination of desktops and applications to users. Creating a Delivery Group is a flexible way of allocating machines and applications to users. In a Delivery Group, you can:

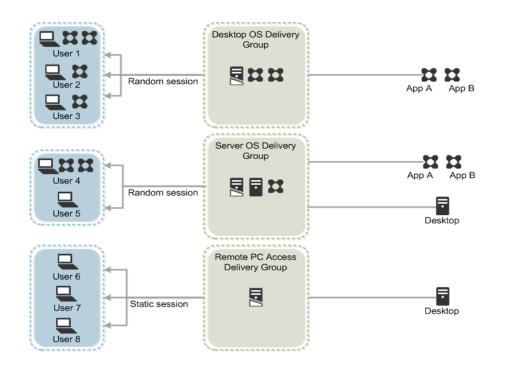
- Use machines from multiple catalogs
- Allocate a user to multiple machines
- Allocate multiple users to one machine

As part of the creation process, you specify the following Delivery Group properties:

- Users, groups, and applications allocated to Delivery Groups
- Desktop settings to match users' needs
- Desktop power management options

Figure 19 illustrates how users access desktops and applications through machine catalogs and delivery groups.

Figure 19 Access Desktops and Applications through Machine Catalogs and Delivery Groups



# Example XenDesktop Deployments

Two examples of typical XenDesktop deployments are:

- A distributed components configuration
- A multiple site configuration

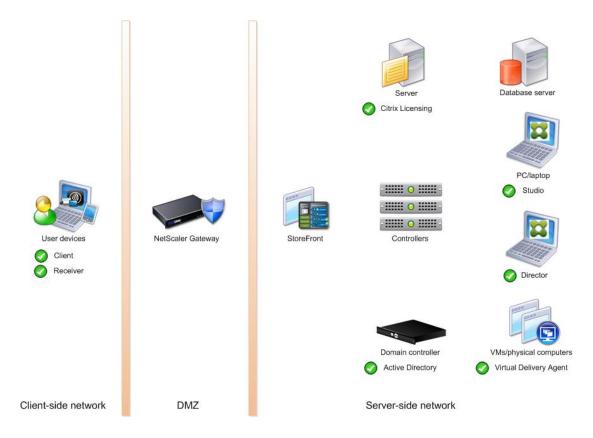
Since XenApp and XenDesktop 7.16 are based on a unified architecture, combined they can deliver a combination of Hosted Shared Desktops (HSDs, using a Server OS machine) and Hosted Virtual Desktops (HVDs, using a Desktop OS).

## **Distributed Components Configuration**

You can distribute the components of your deployment among a greater number of servers, or provide greater scalability and failover by increasing the number of controllers in your site. You can install management consoles on separate computers to manage the deployment remotely. A distributed deployment is necessary for an infrastructure based on remote access through NetScaler Gateway (formerly called Access Gateway).

Figure 20 shows an example of a distributed components configuration. A simplified version of this configuration is often deployed for an initial proof-of-concept (POC) deployment. The CVD described in this document deploys Citrix XenDesktop in a configuration that resembles this distributed components configuration shown. Two Cisco C220 rack servers host the required infrastructure services (AD, DNS, DHCP, Profile, SQL, Citrix XenDesktop management, and StoreFront servers).

Figure 20 Example of a Distributed Components Configuration

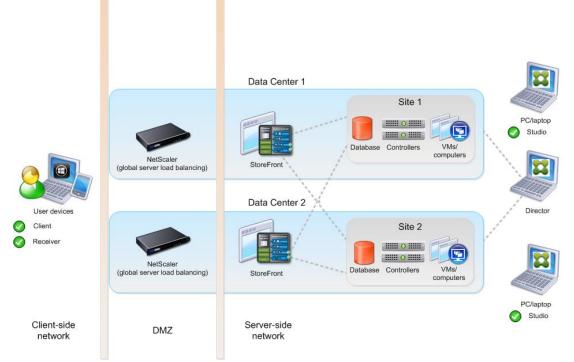


## **Multiple Site Configuration**

If you have multiple regional sites, you can use Citrix NetScaler to direct user connections to the most appropriate site and StoreFront to deliver desktops and applications to users.

In Figure 21 depicting multiple sites, a site was created in two data centers. Having two sites globally, rather than just one, minimizes the amount of unnecessary WAN traffic.

### Figure 21 Multiple Sites



You can use StoreFront to aggregate resources from multiple sites to provide users with a single point of access with NetScaler. A separate Studio console is required to manage each site; sites cannot be managed as a single entity. You can use Director to support users across sites.

Citrix NetScaler accelerates application performance, load balances servers, increases security, and optimizes the user experience. In this example, two NetScalers are used to provide a high availability configuration. The NetScalers are configured for Global Server Load Balancing and positioned in the DMZ to provide a multi-site, fault-tolerant solution.

### **Citrix Cloud Services**

Easily deliver the Citrix portfolio of products as a service. Citrix Cloud services simplify the delivery and management of Citrix technologies extending existing on-premises software deployments and creating hybrid workspace services.

- Fast: Deploy apps and desktops, or complete secure digital workspaces in hours, not weeks.
- Adaptable: Choose to deploy on any cloud or virtual infrastructure or a hybrid of both.
- Secure: Keep all proprietary information for your apps, desktops and data under your control.
- Simple: Implement a fully-integrated Citrix portfolio via a single-management plane to simplify administration

### Designing a XenDesktop Environment for a Mixed Workload

With Citrix XenDesktop 7.16, the method you choose to provide applications or desktops to users depends on the types of applications and desktops you are hosting and available system resources, as well as the types of users and user experience you want to provide.

Server OS machines	<ul> <li>You want: Inexpensive server-based delivery to minimize the cost of delivering applications to a large number of users, while providing a secure, high-definition user experience.</li> <li>Your users: Perform well-defined tasks and do not require personalization or offline access to applications. Users may include task workers such as call center operators and retail workers, or users that share workstations.</li> <li>Application types: Any application.</li> </ul>
Desktop OS machines	<ul> <li>You want: A client-based application delivery solution that is secure, provides centralized management, and supports a large number of users per host server (or hypervisor), while providing users with applications that display seamlessly in high-definition.</li> <li>Your users: Are internal, external contractors, third-party collaborators, and other provisional team members. Users do not require off-line access to hosted applications.</li> <li>Application types: Applications that might not work well with other applications or might interact with the operating system, such as .NET framework. These types of applications are ideal for hosting on virtual machines.</li> <li>Applications running on older operating systems such as Windows XP or Windows Vista, and older architectures, such as 32-bit or 16-bit. By isolating each application on its own virtual machine, if one machine fails, it does not impact other users.</li> </ul>
Remote PC Access	<ul> <li>You want: Employees with secure remote access to a physical computer without using a VPN. For example, the user may be accessing their physical desktop PC from home or through a public WIFI hotspot. Depending upon the location, you may want to restrict the ability to print or copy and paste outside of the desktop. This method enables BYO device support without migrating desktop images into the datacenter.</li> <li>Your users: Employees or contractors that have the option to work from home, but need access to specific software or data on their corporate desktops to perform their jobs remotely.</li> <li>Host: The same as Desktop OS machines.</li> <li>Application types: Applications that are delivered from an office computer and display seamlessly in high definition on the remote user's device.</li> </ul>

# **Deployment Hardware and Software**

# **Physical Components**

#### Table 1 HyperFlex System Components

Component	Hardware Required
	Two Cisco UCS 6332 Fabric Interconnects, or
Fabric Interconnects	Two Cisco UCS 6332-16UP Fabric Interconnects
Servers	Eight Cisco HyperFlex HXAF220c-M5SX All-Flash rack servers

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

#### Compare Models:

http://www.cisco.com/c/en/us/products/hyperconverged-infrastructure/hyperflex-hx-series/index.html#compare-models

#### HXAF220c-M5SX Spec Sheet:

https://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/hxaf-220c-m5-specsheet.pdf

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

#### Table 2 HXAF220c-M5SX Server Options

HXAF220c-M5SX Hardware Required options		Hardware Required	
Processors A		A pair of Intel Xeon Processor Scalable Family CPUs (6140 Gold)	
Memory		768GB of total memory using 64 GB DDR4 2666 MHz 1.2v modules	
Disk C	ontroller	Cisco 12Gbps Modular SAS HBA	
SSDs	Standard	One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD One 400 GB 2.5 Inch Enterprise Performance 12G SAS SSD 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	
Netwo	rk	Cisco UCS VIC1387 VIC MLOM	
Boot D	evice	One 240 GB M.2 form factor SATA SSD	
microSD Card		One 32GB microSD card for local host utilities storage	

HXAF220c-M5SX options	Hardware Required
Optional	Cisco QSA module to convert 40 GbE QSFP+ to 10 GbE SFP+

## Software Components

Table 3 lists the software components and the versions required for the Cisco HyperFlex system for Microsoft Hyper-V.

Table 3	Software	Components
---------	----------	------------

Component	Software Required
	Hyper-V - Microsoft Windows Server 2016 Datacenter
Hypervisor	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
Active Directory	A Windows 2012 or later domain and forest functionality level with AD integrated DNS server.
	Windows 10 or Windows Server 2016 with PowerShell and RSAT tools installed.
	System Center VMM 2016
Management Server	Windows Admin Center (Optional)
Cisco HyperFlex Data Platform	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
	Cisco HyperFlex Data Platform System Preparation Script for Microsoft Windows Server 2016 with Cisco Drivers - HXInstall-HyperV-DatacenterCore-v3.0.1c-29681.img, or
Microsoft Windows Server 2016 System Preparation Script	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
Ready Clone PowerShell	Cisco HyperFlex Data Platform Hyper-V ReadyClone PowerShell Script
Script	HxClone-HyperV-v3.0.1c-29681.ps1
Cisco UCS Firmware	Cisco UCS Infrastructure software, Cisco UCS B-Series and C-Series bundles, revision 3.2(3g) or later.

## 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: <a href="https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html">https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html</a>

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

Table 4 lists the licensing editions and the features available with each type of license.

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

 Table 4
 HyperFlex System License Editions

## Considerations

## Version Control

The software revisions listed in Table 3 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 make sure 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 5 lists the minimum and maximum scale for various installations of the Cisco HyperFlex system with Microsoft Hyper-V:

Table 5	HyperFlex	Cluster	Scale
---------	-----------	---------	-------

Cluster Type	Minimum Converged Nodes	Maximum Converged Nodes	Maximum Compute-only Nodes
	Required	Allowed	Allowed
Standard with SFF disks	3	8	Not supported

#### Capacity

2

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:

Value	Symbol	Name
1000 bytes	kB	Kilobyte
1000 kB	MB	Megabyte
1000 MB	GB	Gigabyte
1000 GB	ТВ	Terabyte

 Table 6
 SI Unit Values (Decimal Prefix)

The <u>International Organization for Standardization (ISO)</u> and the <u>International Electrotechnical</u> <u>Commission (IEC)</u> defines values and binary prefix by powers of 2 in ISO/IEC 80000-13:2008 Clause 4 listed in Table 7

**Table 7**IEC Unit Values (binary prefix)

Value	Symbol	Name
1024 bytes	KiB	Kibibyte
1024 KiB	MiB	Mebibyte

Value	Symbol	Name
1024 MiB	GiB	Gibibyte
1024 GiB	ТіВ	Tebibyte

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 8 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 <u>Appendix A: Cluster Capacity Calculations</u>.

HX-Series Server Model	Node Quantity	Capacity Disk Size (each)	Capacity Disk Quantity (per node)	Cluster Usable Capacity at RF=2	Cluster Usable Capacity at RF=3	
		3.8 TB	8	102.8 TiB	68.6 TiB	
HXAF220c- M5SX	8	960 GB	8	25.7 TiB	17.1 TiB	
			6	77.1 TiB	51.4 TiB	
			15	192.8 TiB	128.5 TiB	
		3.8 TB	23	295.7 TiB	197.1 TiB	
			6	19.3 TiB	12.9 TiB	
HXAF240c- M5SX (Not used in this			15	48.2 TiB	32.1 TiB	
solution)	8	960 GB	23	73.9 TiB	49.3 TiB	

 Table 8
 Cluster Usable Capacities



Calculations are based on the number of nodes, the number of capacity disks per node, and the size of the capacity disks. Table 8 is not a comprehensive list of all capacities and models available.

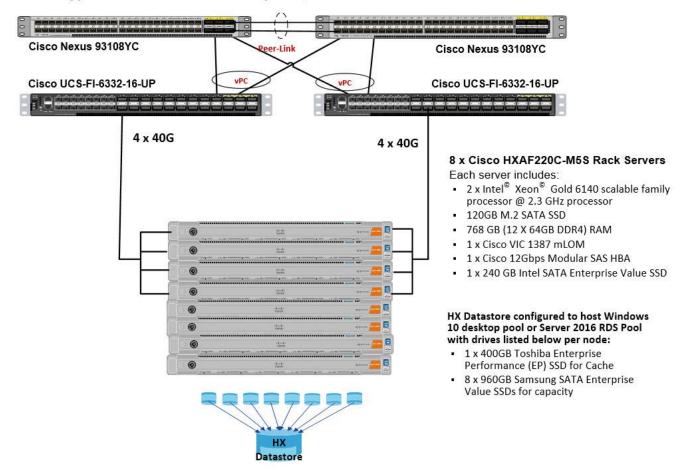
# Physical Topology

## **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.

#### Figure 22 HyperFlex Standard Cluster Topology

Cisco HyperFlex and Citrix XenDesktop 7.18, Reference Architecture



#### 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

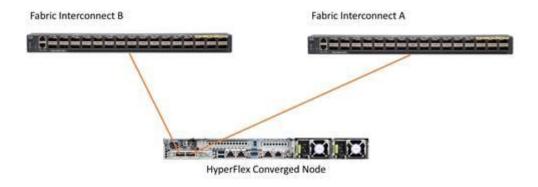
The HX-Series converged servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode. This option enables Cisco UCS Manager to manage the HX-Series Rack-Mount Servers using a single cable for both management traffic and data traffic. Cisco HyperFlex M5 generation servers 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 23). 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 9 lists the possible connections, and which of these methods is supported.

Fabric Interconnect Model	6248	6296	6332		6332-16UP			
Port Type	10GbE	10GbE	40GbE 10GbE Breakout		40GbE	10GbE Breakout	10GbE onboard	
M5 with VIC 1387	×	×	~	×	~	×	×	
M5 with VIC 1387 + QSA	V	V	×	×	×	×	×	

Table 9	Supported	Physical	Connectivity
---------	-----------	----------	--------------

Figure 23 HX-Series Server Connectivity



#### Logical Architecture

The logical architecture of this solution is designed to support up to 1250 Hosted Virtual Microsoft Windows 10 Desktops users or 1600 RDS users within an eight node Cisco UCS HXAF220c- HyperFlex cluster, which provides physical redundancy for each workload type.

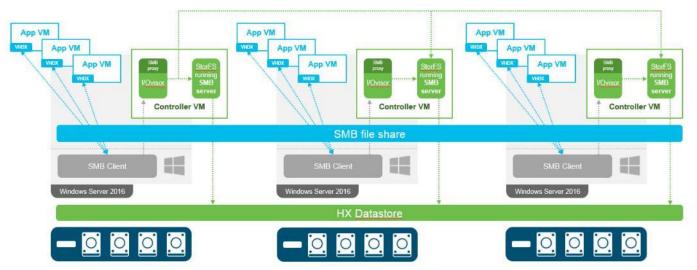


Figure 24 Logical Architecture Design

Table 3 lists the software revisions for this solution.

This document is intended to allow you to fully configure your environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 10 through Table 23 lists the information you need to configure your environment.

## **Design Elements**

<u>6</u>-

Installing the HyperFlex system is primarily done through a deployable HyperFlex installer virtual machine, available for download at <u>cisco.com</u> 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.

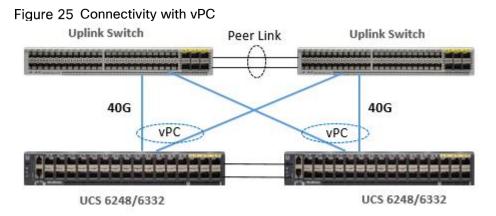
Uplinks need to be connected and active from both Fabric Interconnects. For redundancy, multiple uplinks can be used on each FI, either as 802.3ad Link Aggregation Control Protocol (LACP) port-channels, or using individual links. For the best level of performance and redundancy, uplinks can be made as 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.



### **VLANs**

The VLAN configuration recommended for the environment includes a total of seven VLANs as outlined in Table 10 .

VLAN Name	VLAN ID	VLAN Purpose
Default	1	Native VLAN
Hx-in-Band-Mgmt	30	VLAN for in-band management interfaces
Infra-Mgmt	32	VLAN for Virtual Infrastructure
Hx-storage-data	101	VLAN for HyperFlex Storage
Hx-livemigration	33	VLAN for Hyper-V Live Migration
Vm-network	34	VLAN for VDI Traffic
OOB-Mgmt	132	VLAN for out-of-band management 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**

2

All HyperFlex storage traffic traversing the hx-storage-data VLAN and subnet is configured 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. 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 requirement also means that the Cisco UCS uplinks 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, particularly when cable or port failures would cause storage traffic to traverse the northbound Cisco UCS uplink switches.

## **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 suborganization 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 Manager
ж	All
8	Servers     Service Profiles
88	▼ root
æ	Sub-Organizations     hxThybrid
Q	<ul> <li>hx2sed</li> <li>Sub-Organizations</li> </ul>
=	<ul> <li>Service Profile Templates</li> </ul>
=	<ul> <li>root</li> <li>Sub-Organizations</li> </ul>
J <sub>0</sub>	<ul> <li>hx1hybrid</li> <li>hx2sed</li> </ul>

#### Figure 26 Cisco UCS HyperFlex Sub-Organization

# 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 11 and Figure 27 list the QoS System Class settings configured for HyperFlex.

Priority	Enabled	CoS	Packet Drop	Weight	MTU	Multicast Optimized
Platinum	Yes	5	No	4	9216	No
Gold	Yes	4	Yes	4	Normal	No
Silver	Yes	2	Yes	Best-effort	Normal	Yes
Bronze	Yes	1	Yes	Best-effort	9216	No
Best Effort	Yes	Any	Yes	Best-effort	Normal	No
Fibre Channel	Yes	3	No	5	FC	N/A

Table 11QoS System Classes

#### Figure 27 QoS System Classes

Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	мти		Multicast Optimized
Platinum	۲	5		4	25	9216	Ψ.	
Gold	۲	4		4	25	normal	Ψ.	
Silver	۲	2		best-effort	6	normal	Ψ.	8
Bronze	۲	1		best-effort v	6	9216	Ψ.	
Best Effort		Any	×.	best-effort	6	normal	Ψ.	
Fibre Channel	×	3		5 .	32	fc		N/A

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 12 details the QoS Policies configured for HyperFlex, and their default assignment to the vNIC templates created:

Policy	Priority	Burst	Rate	Host Control	Used by vNIC Template
Platinum	Platinum	10240	Line-rate	None	storage-data-a storage-data-b
Gold	Gold	10240	Line-rate	None	vm-network-a vm-network-b
Silver	Silver	10240	Line-rate	None	hv-mgmt-a hv-mgmt-b
Bronze	Bronze	10240	Line-rate	None	hv-livemigrate-a hv- livemigrate -b
Best Effort	Best Effort	10240	Line-rate	None	N/A

Table 12HyperFlex QoS Policies

#### **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 13 and Figure 28 details the Multicast Policy configured for HyperFlex:

#### Table 13Multicast Policy

Name	IGMP Snooping State	IGMP Snooping Queries State
HyperFlex	Enabled	Disabled

#### Figure 28 Multicast Policy

Propercies	
Name	HyperFlex
IGMP Snooping State	Enabled      Disabled
IGMP Snooping Querier State :	C Enabled   Disabled
Owner	Local

#### **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 Fls do not participate in VLAN Trunk Protocol (VTP). Table 14 and Figure 29 list the VLANs configured for HyperFlex.

Name	ID	Туре	Transport	Native	VLAN Sharing	Multicast Policy
< <hx-inband-mgmt>&gt;</hx-inband-mgmt>	<user_defined></user_defined>	LAN	Ether	No	None	HyperFlex
< <hx-storage-data>&gt;</hx-storage-data>	<user_defined></user_defined>	LAN	Ether	No	None	HyperFlex
< <vm-network>&gt;</vm-network>	<user_defined></user_defined>	LAN	Ether	No	None	HyperFlex
< <hx-livemigrate>&gt;</hx-livemigrate>	<user_defined></user_defined>	LAN	Ether	No	None	HyperFlex

#### Table 14 Cisco UCS VLANs

#### Figure 29 Cisco UCS VLANs LAN / LAN Cloud / VLANs

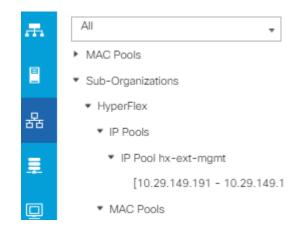
#### VLANs

Te Advanced Filter 🔶 Export 🚔 Print							
Name 🔻	ID	Туре	Transport	Native	VLAN Sharing	Primary VLAN Na	Multicast Policy Name
VLAN default (1)	1	Lan	Ether	Yes	None		
VLAN hx-inband-mgmt (31	3175	Lan	Ether	No	None		HyperFlex
VLAN hx-livemigrate (3173)	3173	Lan	Ether	No	None		HyperFlex
VLAN hx-storage-data (3172)	3172	Lan	Ether	No	None		HyperFlex
VLAN vm-network (3174)	3174	Lan	Ether	No	None		HyperFlex

#### 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 30 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 (for example, 00:25:B5:<u>xx</u>) 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.

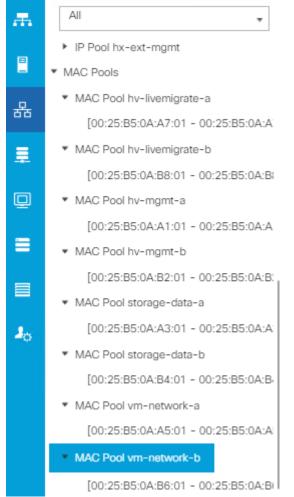
Table 15 list the MAC Address Pools configured for HyperFlex and their default assignment to the vNIC templates created.

Name	Block Start	Size	Assignment Order	Used by vNIC Template
hv-mgmt-a	00:25:B5: <xx>:A1:01</xx>	100	Sequential	hv-mgmt-a
hv-mgmt-b	00:25:B5: <xx>:B2:01</xx>	100	Sequential	hv-mgmt-b
hv-livemigrate-a	00:25:B5: <xx>:A7:01</xx>	100	Sequential	hv-livemigrate-a
hv-livemigrate-b	00:25:B5: <xx>:B8:01</xx>	100	Sequential	hv-livemigrate-b
storage-data-a	00:25:B5: <xx>:A3:01</xx>	100	Sequential	storage-data-a
storage-data-b	00:25:B5: <xx>:B4:01</xx>	100	Sequential	storage-data-b
vm-network-a	00:25:B5: <xx>:A5:01</xx>	100	Sequential	vm-network-a

Table 15MAC Address Pools

Name	Block Start	Size	Assignment Order	Used by vNIC Template
vm-network-b	00:25:B5: <xx>:B6:01</xx>	100	Sequential	vm-network-b

#### Figure 31 MAC Address Pools



### **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 16 details the Network Control Policies configured for HyperFlex, and their default assignment to the vNIC templates created:

		-			
Name	CDP	MAC Register Mode	Action on Uplink Fail	MAC Security	Used by vNIC Template
	Enabled	Only Native VLAN	Link-down	Forged: Allow	hv-mgmt-a
					hv-mgmt-b
					hv-livemigrate-a
					hv-livemigrate-b
HyperFlex- infra					storage-data-a

 Table 16
 Network Control Policy

Name	CDP	MAC Register Mode	Action on Uplink Fail	MAC Security	Used by vNIC Template
					storage-data-b
	Enabled	Only Native VLAN	Link-down	Forged: Allow	vm-network-a
HyperFlex- vm					vm-network-b

#### Figure 32 Network Control Policy

Properties	
Name :	HyperFlex-infra
Description :	Network Control policy for infrastructure vNICs Hype
Owner :	Local
CDP :	Olisabled  Enabled
MAC Register Mode :	Only Native Vlan   All Host Vlans
Action on Uplink Fail:	Link Down   Warning
MAC Security	
Forge:  Allow	Deny
LLDP	
Transmit :      Disab Receive :      Disab	

#### 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:

		plate in mgn	, -					
vNIC Template Name:	hv-mgmt-a	hv-mgmt-b	storage-data-a		hv-livemigrate- a	•	vm-network-a	vm-network-b
Setting	Value	Value	Value	Value	Value	Value	Value	Value
Fabric ID	А	В	A	В	A	В	A	В

Table 17vNIC Template hv-mgmt-a/b

Fabric Failover	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Target	Adapter	Adapter	Adapter	Adapter	Adapter	Adapter	Adapter	Adapter
Туре	Updating Template	Updating Template	Updating Template	Updating Template	Updating Template	Updating Template	Updating Template	Updating Template
MTU	1500	1500	9000	9000	9000	9000	1500	1500
MAC Pool	hv-mgmt-a	hv-mgmt-b	storage-data-a	storage-data-b	hv-livemigrate- a	hv-livemigrate- b	vm-network-a	vm-network-ł
QoS Policy	silver	silver	platinum	platinum	bronze	bronze	gold	gold
Network Control Policy	HyperFlex- infra	HyperFlex- infra	HyperFlex-infra	HyperFlex- infra	HyperFlex- infra	HyperFlex- infra	HyperFlex- vm	HyperFlex- vm
VLANs	< <hx- inband- mgmt&gt;&gt;</hx- 	< <hx- inband- mgmt&gt;&gt;</hx- 	< <hx-storage- data&gt;&gt;</hx-storage- 	< <hx-storage- data&gt;&gt;</hx-storage- 	< <hx- livemigrate&gt;&gt;</hx- 	< <hx- livemigrate&gt;&gt;</hx- 	< <vm- network&gt;&gt;</vm- 	< <vm- network&gt;&gt;</vm- 
Native VLAN	No	No	No	No	No	No	No	No

### 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 18 lists the LAN Connectivity Policy configured for HyperFlex.

Table 18	LAN Connectivity Policy
----------	-------------------------

Policy Name	Use vNIC Template	vNIC Name	vNIC Template Used	Adapter Policy
		hv-mgmt-a	hv-mgmt-a	
		hv-mgmt-b	hv-mgmt-b	
		hv-livemigrate-a	hv-livemigrate-a	
		hv-livemigrate-b	hv-livemigrate-b	
		storage-data-a	storage-data-a	
HyperFlex	Yes	storage-data-b	storage-data-b	HyperFlex

Policy Name	Use vNIC Template	vNIC Name	vNIC Template Used	Adapter Policy
		vm-network-a	vm-network-a	
		vm-network-b	vm-network-b	

## **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 33	Cisco L	JCS Ada	pter Pc	licy Re	sources

<ul> <li>Resources</li> </ul>			
Pooled	:	<ul> <li>Disabl</li> </ul>	ed 🔾 Enabled
Transmit Queues	:	1	[1-1000]
Ring Size	:	256	[64-4096]
Receive Queues	:	4	[1-1000]
Ring Size	:	512	[64-4096]
Completion Queues	s :	5	[1-2000]
			[1-1024]
Interrupts	:	8	[1-1024]

#### Figure 34 Cisco UCS Adapter Policy Options

Transmit Checksum Offload	:	O Disabled   Enabled	
Receive Checksum Offload	:	O Disabled   Enabled	
TCP Segmentation Offload	:	O Disabled   Enabled	
TCP Large Receive Offload	:	O Disabled   Enabled	
Receive Side Scaling (RSS)	:	O Disabled   Enabled	
Accelerated Receive Flow Steering	:	Disabled      Enabled	
Network Virtualization using Generic Routing Encapsulation	1:	Disabled      Enabled	
Virtual Extensible LAN	:	Disabled      Enabled	
Failback Timeout (Seconds)	:	5	[0-600]
Interrupt Mode	:	MSI X      MSI      IN Tx	
Interrupt Coalescing Type	:	Min      Idle	
Interrupt Timer (us)	:	125	[0-65535]
RoCE	:	Disabled	
Advance Filter	:	Disabled      Enabled	
Interrupt Scaling	:	Disabled      Enabled	

#### **BIOS Policies**

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: <u>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</u>

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 35 details the HyperFlex Boot Policies for Cisco HX-Series M5 generation rack-mount servers.

#### Figure 35 Cisco UCS M5 Boot Policy Actions Properties : HyperFlex-m5 Name Delete Recommended boot policy for HyperFlex servers Description Show Policy Usage Owner : Local : 🗆 Reboot on Boot Order Change Enforce vNIC/vHBA/iSCSI Name : Boot Mode Legacy O Uefi

#### 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.

⊕ Local Devices	Boot Order		
	+ - Te Advanced F	Filter 🛉 Export 🖷 Print	
⊕ CIMC Mounted vMedia	Name	Order 🔺 vNIC/vH Type	LUN Name WWN
+ vNICs	CD/DVD	1	
0 11103	Embedded Disk	2	
(+) vHBAs			

#### 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 36 shows the Host Firmware Package configured by the HyperFlex installer for Cisco HX-Series M5 generation rack-mount servers.

Figure 36 (	Cisco UCS	M5 Host	Firmware	Package
-------------	-----------	---------	----------	---------

Actions	Properties	
Delete	Name : HyperFlex-m5	
Show Policy Usage	Description : Recommended Host Firmware Pack	ages for M5 Hyp
Use Global	Owner : Local	
Modify Package Versions	Blade Package: 3.2(3g)B	Blade Backup Package:
Modify Backup Package Versions	Rack Package : 3.2(3g)C	Rack Backup Package :
	Service Pack :	

#### 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 37 details the Local Disk Configuration Policies configured by the HyperFlex installer.

Figure 37 Cisco UCS M5 Local Disk Configuration Pol	icy
---	-----

Name	: HyperFlex-m5
Description	: Recommended Local Disk policy for M5 HyperFlex s
Owner	: Local
Mode	: Any Configuration
Protect Configuration	: 🖉
with the server. In that case	set, the local disk configuration is preserved if the service profile is disassociat ), a configuration error will be raised when a new service profile is associated w configuration in that profile is different

that belief in the local disk conlige	
FlexFlash	
FlexFlash State :	Disable      Enable
	cards will become unavailable immediately. use before disabling the FlexFlash State. Disable      Enable
	changed, SD cards will become unavailable temporarily. use before changing the FlexFlash Removable State. Ves No  No No Change

#### 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 38 details the Maintenance Policy configured by the HyperFlex installer:

#### Figure 38 Cisco UCS Maintenance Policy

Properties	
Name	: HyperFlex
Description	: Recommended maintenance policy for HyperFlex se
Owner	: Local
Soft Shutdown Timer	: 150 Secs
Storage Config. Deployment P	Policy: Immediate  User Ack
Reboot Policy	: OImmediate OUser Ack Timer Automatic
<ul> <li>On Next</li> </ul>	Boot (Apply pending changes at next reboot.)

#### **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 39 details the Power Control Policy configured by the HyperFlex installer.

Figure 39 Cisco UCS Power Control Policy

Name	:	HyperFlex
Description	:	Recommended Power control policy for HyperFlex
Owner	:	Local
Fan Speed Polic	y:	Any
Power Capping	g	

#### **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 40 details the Scrub Policy configured by the HyperFlex installer.

Properties		
Name	:	HyperFlex
Description	:	Recommended Scrub policy for HyperFlex servers
Owner	:	Local
Disk Scrub	:	No      Yes
BIOS Settings Scrub	:	● No ◯ Yes
FlexFlash Scrub	:	No      Yes

#### 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

 Table 19
 Cisco UCS Service Profile Template Settings and Values

Service Profile Template Name:	hx-nodes-m5
Setting	Value
vMedia Policy	Not defined

### 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 UCS service profile. The vSwitches created are:

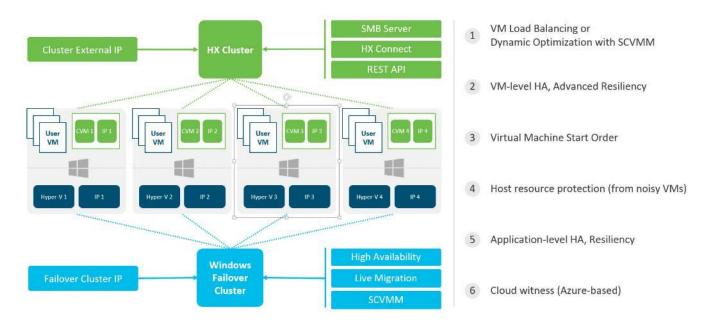
- **vswitch-hx-inband-mgmt**: This is the default vSwitch0 which is renamed by the Hyper-V kickstart file as part of the automated installation. The default vmkernel port, vmk0, is configured in the standard Management Network port group. The switch has two uplinks, active on fabric A and standby on fabric B, without jumbo frames. A second port group is created for the Storage Platform Controller VMs to connect to with their individual management interfaces. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V/Hyper-V
- vswitch-hx-storage-data: This vSwitch is created as part of the automated installation. A vmkernel port, vmk1, is configured in the Storage Hypervisor Data Network port group, which is the interface used for connectivity to the HX Datastores via NFS. The switch has two uplinks, active on fabric B and standby on fabric A, with jumbo frames required. A second port group is created for the Storage Platform Controller VMs to connect to with their individual storage interfaces. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V/Hyper-V
- **vswitch-hx-vm-network**: This vSwitch is created as part of the automated installation. The switch has two uplinks, active on both fabrics A and B, and without jumbo frames. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V/Hyper-V
- **live-migration**: This vSwitch is created as part of the automated installation. The switch has two uplinks, active on fabric A and standby on fabric B, with jumbo frames required. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V/Hyper-V

The following tables and figures help give more details into the Hyper-V virtual networking design as built by the HyperFlex installer:

Virtual Switch	Port Groups	Active vmnic(s)	Passive vmnic(s)	VLAN IDs	Jumbo
vswitch-hx-inband- mgmt	Management Network Storage Controller Management Network	vmnic0	vmnic1	hx-inband-mgmt	no
vswitch-hx-storage- data	Storage Controller Data Network Storage Hypervisor Data Network	vmnic3	vmnic2	hx-storage-data	yes
vswitch-hx-vm- network	none	vmnic4,vmnic5	none	vm-network	no
Live-migration	none	vmnic6	vmnic7	33	yes

 Table 20
 Table Hyper-V Host Virtual Switch Configuration

#### Figure 41 SCVMM Network Design



### Storage Platform Controller Virtual Machines

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 are deployed as a Hyper-V agent, which is similar in concept to that of a Linux or Windows service. Hyper-V agents 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 agents have started. Each Hyper-V hypervisor host has a single Hyper-V agent deployed, which is the controller VM for that node, and it cannot be moved or migrated to another host. The collective Hyper-V agents are managed via a Hyper-V agency in the Hyper-V cluster.

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 as part of the Hyper-V agents to the agency, therefore the Hyper-V hypervisors nor SCVMM server 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 a plugin installed to the SCVMM server or appliance managing the Hyper-V cluster. The plugin communicates directly with the controller VMs to display the information requested.

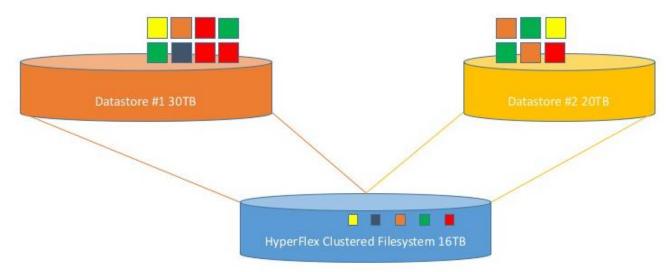
#### **Controller VM Locations**

The physical storage location of the controller VM is similar between the Cisco HXAF220c-M5S and HXAF240c-M5SX model servers. 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 SR-IOV. The configuration details of the models are described in the following subsections.

#### **Cisco HyperFlex Datastores**

The new HyperFlex cluster has no default datastores configured for virtual machine storage, therefore the datastores must be created using the HyperFlex Connect GUI. Overall space consumption in the HyperFlex clustered filesystem is optimized by the default deduplication and compression features.

#### Figure 42 Datastore Example



#### CPU Resource Reservations

Since the storage controller VMs provide critical functionality of the Cisco HX Distributed Data Platform, the HyperFlex installer will configure CPU resource reservations for the controller VMs. This reservation 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 21 details the CPU resource reservation of the storage controller VMs.

#### Table 21Controller VM CPU Reservations

Number of vCPU	Shares	Reservation	Limit
8	Low	10800 MHz	unlimited

#### Memory Resource Reservations

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

Table 22 lists the memory resource reservation of the storage controller VMs.

Table 22 Controller VIVI IVIE	emory Reservations	
Server Model	Amount of Guest Memory	Reserve All Guest Memory
HX220c-M5 HXAF220c-M5	48 GB	Yes
HX240c-M5SX HXAF240c-M5SX	72 GB	Yes

#### Table 22 Controller VM Memory Reservations

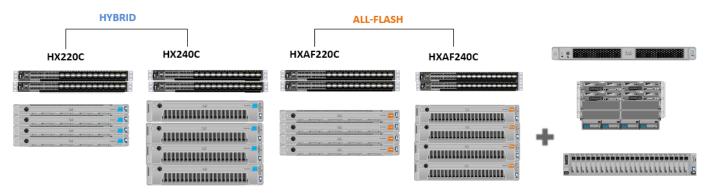


The Cisco UCS compute-only nodes have a lightweight storage controller VM; it is configured with only 1 vCPU and 512 MB of memory reservation.

# Solution Configuration

This section details the configuration and tuning that was performed on the individual components to produce a complete, validated solution. Figure 43 illustrates the configuration topology for this solution.

Figure 43 Configuration Topology for Scalable Citrix XenDesktop 7.16 Workload with HyperFlex



# Cisco UCS Compute Platform

The following subsections detail the physical connectivity configuration of the Citrix XenDesktop environment.

# **Physical Infrastructure**

### Solution Cabling

The information in this section is provided as a reference for cabling the physical equipment in this Cisco Validated Design environment. To simplify cabling requirements, the tables include both local and remote device and port locations.

The tables in this section list the details for the prescribed and supported configuration.

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.

Be sure to follow the cabling directions in this section. Failure to do so will result in necessary changes to the deployment procedures that follow because specific port locations are mentioned.

Figure 44 shows a cabling diagram for a Citrix XenDesktop configuration using the Cisco Nexus 9000 and Cisco UCS Fabric Interconnect.

Table 23 Claco Nexus 33		ig internation		
Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93108YC A	Eth1/1	10GbE	Cisco Nexus 93108YC B	Eth1/1
	Eth1/2	10GbE	Cisco Nexus 93108YC B	Eth1/2
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth1/13

Table 23Cisco Nexus 93108YC-Cabling Information

么

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/4	10GbE	Cisco UCS fabric interconnect A	Eth1/14
	Eth1/5	10GbE	Cisco UCS fabric interconnect B	Eth1/13
	Eth1/6	10GbE	Cisco UCS fabric interconnect B	Eth1/14
	Eth1/25	10GbE	Infra-host-01	Port01
	Eth1/26	10GbE	Infra-host-02	Port01
	Eth1/27	10GbE	Launcher-host-01	Port01
	Eth1/28	10GbE	Launcher-host-02	Port01
	Eth1/29	10GbE	Launcher-host-03	Port01
	Eth1/30	10GbE	Launcher-host-04	Port01
	MGMT0	GbE	GbE management switch	Any

# For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93108YC B	Eth1/1	10GbE	Cisco Nexus 93108YC A	Eth1/1
	Eth1/2	10GbE	Cisco Nexus 93108YC A	Eth1/2
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth1/1
	Eth1/4	10GbE	Cisco UCS fabric interconnect A	Eth1/16
	Eth1/5	10GbE	Cisco UCS fabric interconnect B	Eth1/1
	Eth1/6	40GbE	Cisco UCS fabric interconnect B	Eth1/1
	Eth1/25	10GbE	Infra-host-01	Port02
	Eth1/26	10GbE	Infra-host-02	Port02
	Eth1/27	10GbE	Launcher-host-01	Port02
	Eth1/28	10GbE	Launcher-host-02	Port02
	Eth1/29	10GbE	Launcher-host-03	Port02
	Eth1/30	10GbE	Launcher-host-04	Port02

Local Device	Local Port	Connection	Remote Device	Remote Port
	MGMT0	GbE	GbE management switch	Any

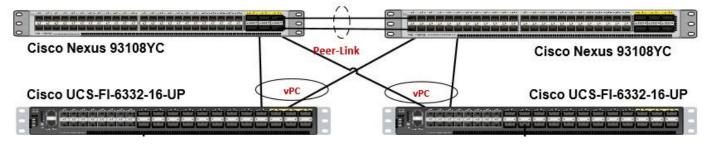
### Table 25 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Eth1/13	10GbE	Cisco Nexus 93108YC A	Eth1/3
	Eth1/14	10GbE	Cisco Nexus 93108YC A	Eth1/4
	Eth1/15	10GbE	Cisco Nexus 93108YC B	Eth1/5
	Eth1/16	10 GbE	Cisco Nexus 93108YC B	Eth 1/6
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2

 Table 26
 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect B	Eth1/13	10GbE	Cisco Nexus 93108YC B	Eth1/3
	Eth1/14	10GbE	Cisco Nexus 93108YC B	Eth1/4
	Eth1/15	10GbE	Cisco Nexus 93108YC A	Eth1/5
	Eth1/16	10GbE	Cisco Nexus 93108YC A	Eth 1/6
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A	L1
	L2	GbE	Cisco UCS fabric interconnect A	L2

Figure 44 Cable Connectivity Between Cisco Nexus 93108YC A and B to Cisco UCS 6248 Fabric A and B



# **Cisco Unified Computing System Configuration**

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:

- 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.
- 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.
- 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/qui) ? 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 : hxhvdom.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.
 Configuration file - Ok
```

#### Cisco UCS Fabric Interconnect B

To configure Fabric Interconnect B, complete the following steps:

- 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.
- 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:

Open a web browser and navigate to the Cisco UCS Manager Cluster IP address, for example https://10.29.149.205

cisc	
UCS Ma	anager
3.2(3	a)
Launch UCS Manager	Launch KVM Manager
Inve KUM Investment requires Tous	Durting Environment 1.7 or higher
Java KVM launch requires Java I	Runtime Environment 1.7 or higher
	Runtime Environment 1.7 or higher
© 2009-2018 Cisco Systems, Inc. All rights reserved.	
© 2009-2018 Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are own	ed by other third parties and used and distributed under license
Java KVM launch requires Java I © 2009-2018 Cisco Systems, Inc. All rights reserved. The copyrights to certain works contained in this software are own Certain components of this software are licensed under the GNU G Lesser General Public License (LGPL) Version 2.1	ed by other third parties and used and distributed under license

- 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(3a). 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:

https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/ucs-manager/GUI-User-Guides/Firmware-Mgmt/3-2/b\_UCSM\_GUI\_Firmware\_Management\_Guide\_3\_2.html

#### 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.
- 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 46 Uplinks Ports

æ	All	Equipmen	nt / Fabric Interco	nnects / Fa	bric Interconnect	A ( / Fixed	d Module / Ethe	ernet Ports	
	▼ Equipment	Ethernet	Ports						
	Chassis	Te Advance	ed Filter 🔺 Expor	t 🖷 Print	All Unco	nfigured 🗸	Network Ser	ver FCoE Upl	nk
윪	<ul> <li>Rack-Mounts</li> </ul>	Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Sta	Admin State
	FEX	1	0	25	00:DE:FB:E	Network	Physical	🕇 Up	1 Enabled
<u>.</u>	<ul> <li>Servers</li> </ul>	1	0	26	00:DE:FB:E	Network	Physical	🕇 Up	1 Enabled
	<ul> <li>Fabric Interconnects</li> </ul>								
▣	🔹 Fabric Interconnect A (primary) 😯								
	Fans								
	▼ Fixed Module								
	Ethernet 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 portchannel 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 portchannel 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 47 Uplink Port Channels

æ	All	LAN / LAN Cloud / Fabric A / Port Chann	nels / Port-Channe	
	▼ LAN	General Ports Faults Events	s Statistics	
	▼ LAN Cloud			
몲	<ul> <li>Fabric A.</li> </ul>	Status	Properties	
	▼ Port Channels	Overall Status :   Up	ID	: 45
重	Port-Channel 45 HXHV-A	Additional Info :	Fabric ID	: <b>A</b>
	Eth Interface 1/25	Actions	Port Type Transport Type	: Aggregation : Ether
₽	Eth Interface 1/26	Enable Port Channel	Name	: HXHV-A
=	<ul> <li>Uplink Eth Interfaces</li> </ul>	Disable Port Channel	Description	:
	► VLANs	Add Ports	Flow Control Policy	: default
	<ul> <li>VP Optimization Sets</li> </ul>		LACP Policy	: default
	▶ Fabric B		Note: Changing LACP pol	icy may flap the port-channel if the suspend
20	<ul> <li>QoS System Class</li> </ul>		Admin Speed	: 🔘 1 Gbps 🔵 10 Gbps 💿 40 Gbps
			Operational Speed(Gbps	): 80

### 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.
- 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.

Figure 48 Port Auto-Discovery Policy

æ	Policies	Policies / Port Auto-Discovery Policy
	<ul> <li>Policies</li> </ul>	Actions
	Port Auto-Discovery Policy	
格		Properties
		Owner : Local Auto Configure Server Port : Oisabled Enabled

#### 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.
- 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.
- 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.

Hyper-V Manager		
File Action View	Help	
🗢 🄿 🖄 📰 🛛		
Hyper-V Manager	Virtual Machines	
	New >	Virtual Machine
	Import Virtual Machine	Hard Disk
	Hyper-V Settings	Floppy Disk
	Virtual Switch Manager	Off
	Virtual SAN Manager	Running 1%
	Edit Disk	

#### Figure 49 Hyper-V Manager - New VM

- 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**.

Figure 50 Hyper-V Manager - Specify VM Name

Specify Nan	e and Location				
Before You Begin	Choose a name and lo	ocation for this virtual machine.			
Specify Name and Location	cation The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easil				
Specify Generation		chine, such as the name of the guest operation			
Assign Memory	Name: HXDP-Insta	aller			
Configure Networking	You can create a folde	er or use an existing folder to store the virtual	machine. If you don't select a		
Connect Virtual Hard Disk		chine is stored in the default folder configured			
Installation Options	Store the virtual m	nachine in a different location			
Summary	Location: C:\Program	nData Wicrosoft\Windows\Hyper-V\	Browse		

#### As a best practice, store the VM together with the .vhdx file.

7. In the Specify Generation page, select Generation 1. Click Next.

Figure 51 Hyper-V Manger – Specify VM Generation

🚪 New Virtual Machine Wizar	rd X
Specify Gene	ration
Before You Begin	Choose the generation of this virtual machine.
Specify Name and Location	Generation 1
Specify Generation Assign Memory	This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.
Configure Networking	O Generation 2
Connect Virtual Hard Disk	This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.
Installation Options Summary	⚠️ Once a virtual machine has been created, you cannot change its generation.

8. In the Assign Memory page, set the startup memory value to 4096 MB. Click Next.

🖳 New Virtual Machine Wiza	ard
🔤 🛛 Assign Mem	ory
Before You Begin Specify Name and Location Specify Generation	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.
Assign Memory	
Configure Networking Connect Virtual Hard Disk Installation Options	<ul> <li>Use Dynamic Memory for this virtual machine.</li> <li>When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.</li> </ul>

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**.

Figure 53 Hyper-V Manager - Configure VM Networking

🖳 New Virtual Machine Wizard					
🖳 Configure Ne	etworking				
Before You Begin Specify Name and Location Specify Generation Assign Memory		tual machine includes a network adapter. You can configure t , or it can remain disconnected. Team-Ext-SW	he network adapter to use a		
Configure Networking					

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**.

۰

#### Figure 54 Hyper-V Manager - Connect Virtual Hard Disk

**Connect Virtual Hard Dick** 

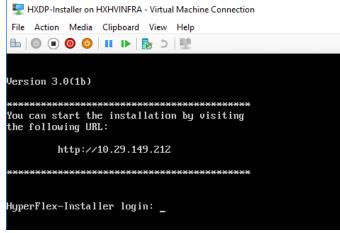
🖳 New Virtual Machine Wizard

Before You Begin Specify Name and Location Specify Generation Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties. Create a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.			
Configure Networking	Name: HXDP-Installer.vhdx			
onnect Virtual Hard Disk	Location: D:\Hyper-V\VHDs\	Browse		
iummary	Size: 127 GB (Maximum: 64 TB)			
	Use an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format	t.		
	Location: hdx\Cisco-HX-Data-Platform-Installer-v3.0.1b-29665-hyperv.vhdx	Browse.		

×

- 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.
- 14. Choose Action > Start (Ctrl+S).
- 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.

#### Figure 55 HXDP Installer



# 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 make sure 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.XXXX #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 56 Show Interfaces

root@HyperFlex-Installer:~# ifconfig
eth0 Link encap:Ethernet HWaddr 00:15:5d:fc:33:0e
inet addr:10.104.252.48
inet6 addr: fe80::215:5dff:fefc:330e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9880615 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:915866025 (915.8 MB) TX bytes:12398400970 (12.3 GB)

Figure 57 Routing Table

oot@HyperFlex-Installer:~# route -n							
Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
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	Θ	eth0
239.255.255.253	0.0.0.0	255.255.255.255	UH	0	0	Θ	eth0

Figure 58 /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 a media for the installation. The HyperFlex installation for Microsoft Hyper-V is completed in two phases using the customized version of the HX installation workflow:

么

- In the phase one, only 'Run UCS Configuration" workflow is executed to prepare and install Windows OS, and
- In phase two, 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 the HyperFlex installation will guide you through the process of configuring Cisco UCS Manager using HyperFlex installer and installation of Windows OS on the HX nodes. The following high-level steps are covered in this phase of the installation:

- 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 configure Cisco UCS Manager using HX Installer, complete the following steps:

- 1. Launch 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 Ciscol23 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 59 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.

	rFlex Installer <sup>Wor</sup>	C kfow
ielect a Work	flow	
		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$
	Cluster Creation with HyperFlex (FI)	Cluster Expansion (Not Supported)

Figure 60 HyperFlex Installer - Workflow

6. On the next screen, click Run UCS Manager Configuration and then click Continue.



Do not choose any other workflow options.

#### Figure 61 HyperFlex Installer – Select a Workflow

cisco	HyperFlex Installer			0		•
			Workflow			
Sele	ect a Workflow					
		×	Run UCS Manager Configuration			
		0	Run Hypervisor Configuration			
		D	Deploy HX Software			
		Create HK Cluster	Expand HX Ouster (Not Supported)			
i s	how me the standard workflows				Continu	

- 7. Click Confirm in the popup that displays.
- 8. Enter the UCS Manager credentials.

6

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 27Cisco UCS Manager Details

Field	Description
Cisco UCS Manager Host Name	FQDN or the VIP address of Cisco UCS Manager
Cisco UCS Manager User Name and Password	Administrator user and password or an user with Cisco UCS Manager admin rights

HyperFlex Installer				0			¢
Credentials		Server Selection			UCSM Confi	guration	
UCS Manager Credentials				Con	figuratio		
UCS Manager Host Name	UCS Manager User Name	Password					 
10.29.149.205	admin		۵				
		Password for UCS Manager con	nection				
						Drag and dro; uration files h	
				- i	coning.		

#### Figure 62 HyperFlex Installer - Cisco UCS Manager Credentials

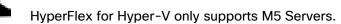
#### 10. Click Continue.

The installer connects to Cisco UCS Manager and queries 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.

Figure 63	HyperFlex	Installer -	Server	Selection
-----------	-----------	-------------	--------	-----------

		Credentials			Server Selectio	n			UCSM Con	figuration		
	r Seleci					re Server Ports	Refresh	c	onfiguratio	n		
	for Hype ssociated			ow is restricted to M5 se	rvers.			0	edentials			
	~	Server Name	Status	Model	Serial	Assoc State	Actions	U	CS Manager Ho	st Name	10.29.1	49.20
	÷	perver Name I A	DOMOUN	NICCHI	Serial	Assoc State	Accord	U	CS Manager Us	er Name		admi
2	00	Server 1	unassociated	HXAF220C-M55X	WZP2143105K	none	none					
2	00	Server 2	unassociated	HXAF220C-M55X	WZP2143102Y	none	none					
		Server 3	unassociated	HXAF220C-M55X	WZP2143103M	none	none					
2												

11. Choose all the servers that you want to install in the cluster and click **Continue**.



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).



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



Renaming the 4 core networks is not supported.

Figure 64 shows the various fields in the VLAN Configuration pane where you need to enter values.

#### Figure 64 HyperFlex Installer - Cisco UCS Manager Configuration

Crede	entials	Serve	er Selection	UCSM Configuration
VLAN Configuration				Configuration *
VLAN for Hypervisor and Hyp VLAN Name ho-inband-mgmt	erFlex management VLAN ID 3175	VLAN for HyperFlex VLAN Name hv-storage-data	x storage traffic VLAN ID 3172	Credentials UCS Manager Host Name 10.29.149.205 UCS Manager User Name admin
VLAN for VM Live Migration VLAN Name Inc-livemigrate	VLAN ID 3173	VLAN for VM Netw VLAN Name vm-network	VLAN ID(s) 3174	Server Selection           Server 2         WZP2143102Y / HXAF220C-M55X           Server 3         WZP2143103M / HXAF220C-M55X           Server 1         WZP2143105K / HXAF220C-M55X
MAC Pool MAC Pool Prefix 00:25:85:0A				Server 4 WZP2143101H / HXAF220C-M55X
'hx-ext-mgmt' IP Pool fi	or Out-of-band CIMC		Gateway	
10.29.149.191-194	255 255 255 0		10.29.149.1	
> FC Storage				
Advanced UCS Server Firmware Version 3.2(3a)	HyperFlex Cluster No HXCLUS	ame	Org Name	K Back Start

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.

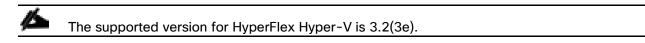
iSCSI Storage and FC Storage are used for adding external storage to the HyperFlex cluster.



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.



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.

dialo cisco HyperFlex Installer	Progress	0000
O- Start	Validations UCS	M Contentints
		UCS Manager Host Name 10.29.149.205 UCS Manager User Name admin
✓ UCSM Configuration Successful	4	Server 2 WZP2143102Y / HXAF220C-MS5X
UCSM Configuration - Overall	UCSM Configuration	Server 3 WZP2143103M / HX4F220C-M55X     Server 1 WZP2143105K / HX4F220C-M55X
Succeeded	Login to UCS API     Inventorying physical servers	Server 4 WZP2143101H / HXAF220C-M55X UCSM Configuration
	Validate UCS firmware version     Setting flags for firmware validation	VLAN Name hx-inband-mgmt VLAN ID 3175
	Downloading firmware bundle     Continuing IICS fabric interconnect	VLAN Name hx-storage-data

Figure 65 HyperFlex Installer - Cisco UCS Manager Configuration Progress

#### Configure Cisco UCS vMedia and Boot Policies

By using a Cisco UCS vMedia policy, the Windows Server 2016 media ISO file and <u>Cisco HyperFlex Driver</u> <u>image</u> 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

0

will automatically boot from the remotely 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.

Figure 66 Upload Windows ISO and Cisco Driver and System Preparation Script

🌆 3.0.1b - root@10.29.149.212 - WinSCP				5				- 🗆
Local Mark Files Commands Session Options Remote Help								
🖶 🔁 📚 Synchronize 🗾 🦑 🔝 🚳 🎒	Queue 🝷	Transfer Settings	Default	• 💋 •				
📮 root@10.29.149.212 💣 New Session								
📲 C: Local Disk 🔹 🖻 😨 🛭 🗢 🔹 🗟 🛣 🏠 🥵 📴 🔚 🔚 🔚 📑 📴 👘 🖉 🖗 👘 🖓								
🕼 Upload 👻 📝 Edit 👻 🔀 🕞 Properties	🛗 New 🗸	+ - V		🛙 😭 Download 👻 📝 Edit 👻 😭 🕞 Properties	督 New 🕶	+ - V		
C:\Software\HXHV\HXHV-GA\3.0.1b\				/var/www/localhost/images/				
Name	Size	Туре	Changed	Name	Size	Changed	Rights	Owner
<b>t</b>		Parent directory	5/18/2018 2:10:40 AM	<b>t</b>		5/11/2018 1:24:27 PM	rwxr-xr-x	root
Cisco-HX-Data-Platform-Installer-v3.0.1b-2966		File folder	5/18/2018 2:10:40 AM	en_windows_server_2016_x64_dvd_9327751.iso	5,521,12	10/12/2016 11:33:44 AM	rw-rr	root
ucs-k9-bundle-c-series.3.2.3b.C.bin	1,469,54	BIN File	5/17/2018 6:22:07 AM	HXInstall-HyperV-DatacenterCore-v3.0.1b-29665	640,000 KB	5/17/2018 1:31:03 AM	rw-rr	root
ucs-k9-bundle-b-series.3.2.3b.B.bin	600,166 KB	BIN File	5/17/2018 6:24:31 AM					
ucs-6300-k9-bundle-infra.3.2.3b.A.bin	975,868 KB	BIN File	5/17/2018 6:26:34 AM					
HXInstall-HyperV-DatacenterDE-v3.0.1b-29665	640,000 KB	Disc Image File	5/17/2018 1:31:14 AM					
HXInstall-HyperV-DatacenterCore-v3.0.1b-296	640,000 KB	Disc Image File	5/17/2018 1:31:03 AM					
MxClone-HyperV-v3.0.1b-29665.ps1	3 KB	Windows PowerS	5/17/2018 1:27:46 AM					
Cisco-HX-Data-Platform-Installer-v3.0.1b-2966	4,807,53	Compressed (zipp	5/17/2018 2:23:01 AM					
<u> </u>								



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.
- Expand Servers > Policies > root > Sub-Organizations > hx-cluster\_name>vMedia Policies to view the list of vMedia Policies.

Policies 👻	Policies / root / Sub-Organizations / Hyp
▶ vMedia Policies	vMedia Policies
<ul> <li>vNIC/vHBA Placement Policies</li> </ul>	+ - Ty Advanced Filter 🔶 Export
- Sub-Organizations	Name
	vMedia Policy HyperFlex
<ul> <li>Adapter Policies</li> </ul>	
<ul> <li>BIOS Policies</li> </ul>	
<ul> <li>Boot Policies</li> </ul>	
<ul> <li>Diagnostics Policies</li> </ul>	
<ul> <li>Graphics Card Policies</li> </ul>	
<ul> <li>Host Firmware Packages</li> </ul>	
<ul> <li>IPMI Access Profiles</li> </ul>	
<ul> <li>KVM Management Policies</li> </ul>	
<ul> <li>Local Disk Config Policies</li> </ul>	
<ul> <li>Maintenance Policies</li> </ul>	
<ul> <li>Management Firmware Package:</li> </ul>	
<ul> <li>Power Control Policies</li> </ul>	
<ul> <li>Power Sync Policies</li> </ul>	
<ul> <li>Scrub Policies</li> </ul>	
<ul> <li>Serial over LAN Policies</li> </ul>	
<ul> <li>Server Pool Policies</li> </ul>	
<ul> <li>Server Pool Policy Qualifications</li> </ul>	
<ul> <li>Threshold Policies</li> </ul>	
<ul> <li>ISCSI Authentication Profiles</li> </ul>	
► vMedia Policies Creat	e vMedia Policy

### Figure 67 Cisco UCS Manager - Create vMedia Policy

- 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:

	a Mount Details	L
Field Name	Action	Example Value
Name	Name for the mount point.	Windows -ISO
Description	Can be used for more information.	
Device Type	Type of image that you want to mount	CDD
Protocol	The protocol used for accessing the share where the ISO files are located.	HTTP
Hostname/IP Address	IP address or FQDN of the server hosting the images.	10.29.149.212

#### Table 28 Create vMedia Mount Details

Field Name	Action	Example Value
Image Name Variable	This value is not used in HyperFlex installation.	None
Remote File	The filename of the ISO file that you want to mount.	
Remote Path	The path on the remote server to where the file resides	
Username	If you use CIFS or NFS a username might be necessary	
Password	If you use CIFS or NFS a password might be necessary	

#### Figure 68 Cisco UCS Manager - Create vMedia Mount CDD

Create vMed	a Mount	? ×
Name	: Windows-ISO	
Description	Windows Server 2016 Image	
Device Type		
Protocol		
Hostname/IP Address	: 10.29.149.212	
Image Name Variable	:      None      Service Profile Name	
Remote File	en_windows_server_2016_x64_dvd_9327751.isd	D
Remote Path	: /images/	
Username	*	
Password	:	
Remap on Eject	: 0	
	ок	Cancel

- 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.

Create vMed	ia	Mount	? ×
Name	:	HX-Cisco-Driver	
Description	:	Cisco Driver Image for HX	
Device Type	:		
Protocol	:		
Hostname/IP Address	:	10.29.149.212	
Image Name Variable	:	None      Service Profile Name	
Remote File	:	HXInstall-HyperV-DatacenterCore-v3.0.1b-29665.ir	
Remote Path	:	/images/	
Username	:		
Password	:		
		ОК	Cancel

# Figure 69 Cisco UCS Manager - Create vMedia Mount HDD

13. On completion, the following screen displays:

lame Description	: t Failure : N	vMedia					?
+ - 7/	Advanced Filter	♠ Export	🖶 Print				\$
Name	Туре	Protocol	Authentica	Server	Filename	Remote Pa User	Remap on
HX-Cis	HDD	HTTP	Default	10.29.149	HXInstall	/images/	No
			(+) Ad	dd 🗊 Delete	Info		
						ок	Cancel

Figure 70 Cisco UCS Manager - Create vMedia Policy

14. In the left navigation pane, select Servers > Service Profile Templates > root > Sub-Organizations > hxcluster name > Service Template hx-nodes name (example:hx-nodes-m5).

Figure 71 Cisco UCS Manager - Service Template

altalta cisco	UCS Manager	
æ	Service Profile Templates	0 4 1 1 Service Profil / root / Sub- Organizations / HyperFlex / Service Tem
	<ul> <li>Service Profile Templates</li> <li>root</li> </ul>	General Storage Network ISCSI vNICs VMedia Policy Boot Order Policies Actions
**	<ul> <li>Sub-Organizations</li> <li>HyperFlex</li> </ul>	Modify vMedia Policy Global vMedia Policy
Ŧ	Service Template compute-nodes     Service Template compute-nodes     Service Template compute-nodes	Name : HyperFlex vMedia Policy Instance : org-root/org-HyperFlex/mnt-clg-policy-HyperFlex
=	Service Template hx-nodes     Service Template hx-nodes-m5	Description : vMedia policy to install or re-install software on HyperFlex servers Retry on Mount Failure : Yes vMedia Mounts
	<ul> <li>Sub-Organizations</li> </ul>	a

15. Choose the HyperFlex vMedia Policy from the drop-down list and click OK twice.

Figure 72 Cisco UCS Manager – Modify vMedia Policy

Modify \	/Media Pol	icy					
vMedia Policy:				1			
C C Create a Specific vMedia Policy							
Name	vMedia Policies						
Description Retry on Mo	HX-vMedia			nstall software of	n HyperFlex ser	vers	
vMedia M							
+ -	Te Advanced Filter	♠ Export	🖶 Print				
Name	Туре	Protocol	Authent	icat Server	Filename	Remote Path	User
				No data avail	able		

The vMedia policy is assigned to the HyperFlex Template during the Cisco UCS Manager phase of the HyperFlex deployment.

- 16. Select Servers > Policies > root > Sub-Organizations > hx-cluster\_name > Boot Policies Boot Policy HyperFlex-m5.
- 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.

Boot Order									
+ - Ty Advanced Filter	r 🔶 Expo	ort 🛛 🖶 Print							\$
Name	Ord▲	vNIC/v	Туре	LUN N	WWN	Slot N	Boot N	Boot P	Descri
CD/DVD	1								
Embedded Disk	2								
CIMC Mounted CD/	3								
				14. D.					
		T Move	Up 🔸	Move Dowr	n 🗉 Dele	ete			

Figure 73 Cisco UCS Manager - Boot Order

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.

#### Figure 74 Cisco UCS Manager - Validate vMedia Mount

isco.	UCS Manager			O 4 1	1		•	<b>Q90</b> 86
æ	All	Equipment / R	ack-Mounts	/ Servers / Server 1				
	▼ Equipment	< General	Inventory	Virtual Machines	Hybrid Display Installed F	Firmware SEL Logs	CIMC Sessions VIF F	Paths Power Control Monitor>
	Chassis	Motherboard	CIMC	CPUs GPUs	Memory Adapters HE	BAs NICs iSCSI v	NICs Storage	
몲	<ul> <li>Rack-Mounts</li> </ul>				Boot-loader Version: 3.1	(3a)		
	FEX				Running Version : 3.1(3a)			
	▼ Servers				Package Version: 3.2(3a) Backup Version: 3.1(2d)	IC .		
	Server 1				Update Status : Ready			
2	<ul> <li>Server 2</li> </ul>				Startup Version : 3.1(3a)			
	► Server 3				Activate Status : Ready			
	<ul> <li>Server 4 10</li> </ul>				Actual vMedia Mounts			
	<ul> <li>Fabric Interconnects</li> </ul>				Actual Mount Entry 1			
-	<ul> <li>Fabric Interconnect A (primary) 👽</li> </ul>				Mapping Name :	Windows-ISO	Туре	CDD
0	► Fans				Protocol :	HTTP	Server	10.29.149.212
	<ul> <li>Fixed Module</li> </ul>				Port :	80	Filename : en_window	vs_server_2016_x64_dvd_93277{
	► PSUs				Remote Path :	/images/	User	
	<ul> <li>Fabric Interconnect B (subordinate)</li> </ul>				Status :	Mounted	Mount Failure Reason	. News
	▶ Fans				Authentication Protocol :			: No
	<ul> <li>Fixed Module</li> </ul>					None	Kernap on Eject	. NO
	<ul> <li>Ethernet Ports</li> </ul>				Actual Mount Entry 2			
	FC Ports				Mapping Name :	HX-Cisco-Driver	Туре	HDD
	▶ PSUs				Protocol :	нттр	Server	10.29.149.212
	<ul> <li>Policies</li> </ul>				Port :	80	Filename	HXInstall-HyperV-
	Port Auto-Discovery Policy							DatacenterCore-v3.0.1b- 29665.img
					Remote Path :	/images/	User	
					Status :	Mounted	Mount Failure Reason	None
					Authentication Protocol :	None	Remap on Eject	: No

#### Install Microsoft Windows Server 2016 OS

In the menu bar, click Servers and choose the first HyperFlex service profile.

1. Click the General tab and choose Actions > KVM Console.

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 75 Cisco UCS Manager – Launch KVM Console

cisco	UCS Manager			0	4 1	1	
æ	Service Profiles	Service Profiles / root	t / Sub-Org	ganizatio	ns / HyperFle	x / Service Profile	rack-un
	<ul> <li>Service Profiles</li> <li>root</li> </ul>	General Stora	age Net	work	iSCSI vNICs	vMedia Policy	Boot Order Virtual Ma
윪	<ul> <li>Sub-Organizations</li> </ul>	Fault Summary				Properties	
66	<ul> <li>HyperFlex</li> </ul>	8 0		)	0		
≣	<ul> <li>rack-unit-1 (HXCLUS)</li> </ul>	0 0	0		0		This service pro
▣	<ul> <li>rack-unit-2 (HXCLUS)</li> <li>rack-unit-3 (HXCLUS)</li> </ul>	Status					the sen To modify this sen
_	▶ rack-unit-4 (HXCLUS)	Overall Status : 🛉 🕻	ок			Name	: rack-unit-1
=	Sub-Organizations	(+) Status Details	S			User Label Description	: HXCLUS
		Actions	KVN	1 Cons	sole-Selec	t IP Address	
<b>1</b> 0		Set Desired Power St Boot Server	Service Pr		ived: 91 (Outband)		×
		Shutdown Server Reset		<b>e</b> 1	Launch Java K	VM Console OK	Cancel
		KVM Console >>				Template Instance	: org-root/org-Hyp
						Assigned S	Server or Server Pool

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

Figure 76 Cisco UCS Manager - Server KVM Console

A FI-6332-A / root / HyperFlex / rack-unit-1[HXCLUS] (Rack -1) - KVM Console(Launched By: admin)

File View Macros Tools Virtual Media Help Boot Server 🔩 Shutdown Server 🧟 Reset KVM Console Properties

- 3. Choose Power Cycle.
- 4. When the server is rebooting, remember to press any key to start the Windows installation.

Figure 77 Cisco UCS Manager – KVM Console Server Boot

2

File View	v Macros	Tools Virtu	al Media 🛛 🖁	lelp	
📣 Boot Se	erver 📑 Sh	utdown Server	🤐 Reset		
KVM Conso	Properti	es			
Press	any ke	y to boo	ot from	CD or	DVD

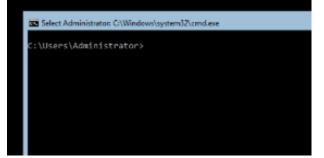
If you miss pressing any key, the server will display in the windows installation or an error page displays stating no OS is installed.

5. 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 78 System Preparation
File View Macros Tools Virtual Media Help
KVM Console Properties
Recycle Bin
Administrator: Ci/Windows/system32/cmd.exe
The system cannot find the file specified.
Start Installation 73% [coorceacececececececececececececececececece

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

Figure 79 Windows Server Command Prompt



7. 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.

Solution Configuration

Figure 80 Validate Windows Server Installation Completion

Fil	e View	Macros	Tools	Virtual Mee	dia H	lelp					
4	Boot Serv	er 🛃 Sh	utdown	Server 🧕 R	eset						
K\	/M Console	Properti	es								
i	🐝 Admin	istrator: C	:\Wind	ows\system	32\cm	d.exe -	powersh	ell	t		
F	PS C:\U	sers\A	dmini	strator>	Get	-Sche	duledT	ask	-TaskN	ame	hx*
٦	[askPat	h Taski	Vame				S	tate			
	\	HXIn	stall	bootstra	plaur	ncher	Task R	unni	ng		

Undo vMedia and Boot Policy Changes

- 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-Organizations > 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.

diadia cisco	UCS Manager	8 💙	4 4 4					•		0 🛞
ж	Al v	Servers / Policies / root / Sub- Organizationa	/ HX-EAP-01	/ vMedia	Polic / vMedi	a PolL.				
∎ ぷ ₹	<ul> <li>KVM Management Palloles</li> <li>Local Disk Config Policies</li> <li>Maintenance Policies</li> <li>Management Firmware Peckag</li> </ul>	Cenand Events Actions Create vi//celo Moent Delate	Properties Nama Description		Hyperflex Weds policy to it	nutuiller ne inut	ali poltwore on P	-1004		
	Power Control Policies     Power Sync Policies     South Policies     South Policies     South Policies	Show Policy Usage Use Stobal	Owner Hotty on Mour Wiedla Mour	; t⊫alure : rts	Local					
	<ul> <li>Server Pool Policies</li> <li>Server Pool Policy Qualification</li> </ul>		+ - ту- Name	Advanced I Type	Photopol	-6 Print Authentic	Server	Rierame	Remote P., User	Remaip o.
<b>3</b> 0	<ul> <li>Threshold Policies</li> <li>ISCS: Authentication Profiles</li> </ul>		HX_Or		HTTP HTTP	Nane Nane		HX0nstall		No No
	<ul> <li>vVeda Policies</li> <li>vVeda Policy HyperFlox</li> <li>vVC/MEA Decement Policies</li> </ul>									
	Sub-Organizations					⊕ ∧s	d 🗍 Delete	0 into		

Figure 81 Cisco UCS Manager - Undo vMedia and Boot Policy Changes

- 3. Go to the boot policy by selecting Servers > Polices > Root > Sub-Organizations > HX-Cluster\_name > boot polices > Boot Policy HyperFlex-m5.
- 4. Select the CIMC mounted CD/DVD, click Delete and accept the changes.

#### HyperFlex Installation - Phase 2

After installing 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:

- 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.

# cisco HyperFlex Installer Workflow Select a Workflow Cluster Creation with HyperFlex (FI) Cluster Expansion (Not Supported) I know what I'm doing, let me customize my workflow

Figure 82 HyperFlex Installer - Workflow

4. Select Run Hypervisor Configuration, Deploy HX Software and Create HX Cluster and click Continue.

#### Figure 83 HyperFlex Installer - Select a Workflow

ului cise	b' HyperFlex Installer	0	8	•	\$
	Workflow				
	Select a Workflow				
	Run UCS Manager Configuration				
	Run Hypervisor Configuration				
	Deploy HX Software				
	Create HX Cluster Expand HX Cluster (Not Supported)				
	Show me the standard workflows			Continu	Je

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.

Figure 84 HyperFlex Installer - Cisco UCS Manager Credentials

Credentials	Server Selection	UCSM Configuration	Hypervisor Configuration	IP Addresses	Cluster Config	ruration
			.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			,
UCS Manager Credentia	ils			Configu	ıration	*
UCS Manager Host Name	UCS Manager Us	er Name	Password			
10.29.149.205	admin					
Domain Information				_		
Domain Name ①						
HXHVDOM.LOCAL						
HX Service Account	Password					
hxadmin		۵			Drag and drop configuration files here or	
Configure Constrained D	elegation now (recommended)	Configure	Constrained Delegation later		Select a File	
Use HX Service Account	©					
~ Advanced Attributes (	optional)					
Domain Controller 🕕	Organization Uni	it ①				
10.29.149.222	OU=HyperFle:	x,DC=HXHVDOM,DC=LOC				
				_		
Hypervisor Credentials					rck Contin	nue
Hypervisor Credentials	Local Administra	tor Password		< Ba	contin	nue

- 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.

#### Figure 85 HyperFlex Installer – Server Selection

	Нур	erFlex Inst	aller							•	0	8	<b>S</b>	\$
	Credent	tials –	Se	rver Selection	UCSM	Configuration	Hypervisor Configurat	ion	IP Add	resses		Cluste	r Configurati	on
	er Sele						Configure Server Ports	Refresh		Conf	iguration			*
	<b>X for Hy</b>		on M5 serve ociated (4)	ers. The list below	v is restricted to M5	servers.			Crede	ntials				
/	-ô-	Server Name	∧ Status	Model	Serial	Assoc State	Service Profile	Actions		UCS M	anager Host Na	ame	10.29.1	49.205
	Ť		5.0105		2021101					UCS M	anager User Na	ame		admin
		Server 1	ok	HXAF220C- M5SX	WZP2143105K	associated	org-root/org-HyperFlex/ls- rack-unit-1	Actions ${\scriptstyle \lor}$		Domai	n Name		HXHVDOM.	LOCAL
				HXAF220C-			org-root/org-HyperFlex/ls-			HX Ser	vice Account		h>	xadmin
		Server 2	ok	M5SX	WZP2143102Y	associated	rack-unit-2	Actions ~		Time Z	one	Pa	cific Standar	rd Time
0		Server 3	ok	HXAF220C-	WZP2143103M	associated	org-root/org-HyperFlex/ls-	Actions ~		Domai	n Controller		10.29.1	49.222
				M5SX			rack-unit-3			Organi Unit	zationOU=Hyp	erFlex,DC	=HXHVDOM,	DC=LC
/		Server 4	ok	HXAF220C- M5SX	WZP2143101H	associated	org-root/org-HyperFlex/ls- rack-unit-4	Actions ${\scriptstyle \lor}$		Local A	dministrator U	ser Name	admini	ístrator
										<	( Back		Continue	

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.

Å

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.

 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. 6

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.

HyperFlex Ins	taller			<b>G</b>	0 0
Credentials	Server Selection	UCSM Configuration	Hypervisor Configuration	IP Addresses	Cluster Configuration
onfigure common Hy	pervisor Settings			Configuration	
ibnet Mask	Gateway		DNS Server(s)	Credentials	
255.255.255.0	10.29.149.1		10.29.149.222	UCS Manager Host N	lame 10.29.149.205
				UCS Manager User N	ame admin
				Domain Name	HXHVDOM.LOCAL
pervisor Settings				HX Service Account	hxadmin
Mala ID Address and II				Time Zone	Pacific Standard Time
Make IP Addresses and H	ostnames sequential			Domain Controller	10.29.149.222
t 🍝 Name 🗠	Serial Sta	atic IP Address	Hostname	OrganizationOU-Hyp Unit	erFlex,DC=HXHVDOM,DC
Server 1	WZP2143105K	10.29.149.228	hxhv1		Jser Name administrator
				Server Selection	
Server 2	WZP2143102Y	10.29.149.227	hxhv2		3102Y / HXAF220C-M5SX
					3103M / HXAF220C-M5SX
Server 3	WZP2143103M	10.29.149.228	hxhv3		3105K / HXAF220C-M5SX
				UCSM Configuratio	
Server 4	WZP2143101H	10.29.149.229	hxhv4	VLAN Name	hx-inband-mgmt
				VLAN ID	3175
mary DNS Suffix 💿	Additional DNS	Suffixes		VLAN Name	hx-storage-data
HXHVDOM.LOCAL				VLAN ID	3172
				VLAN Name	hx-livemigrate
				VLAN ID	3173
				VLAN Name	vm-network
				VLAN ID(s)	3174
				MAC Pool Prefix	00:25:B5:0A

Figure 86 HyperFlex Installer – Hypervisor Configuration

10. Assign the additional IP addresses for the Management and Data networks as well as the cluster IP addresses, then click Continue.

#### Figure 87 HyperFlex Installer – IP Addresses

Credentials Server Selection UCSM Configuration Hypervisor Configuration IP A	ddresses Cluster Configuration
IP Addresses Add Server	Configuration *
Make Hypervisor Names and IP Address Sequential	Credentials
Management - VLAN 3175 Data - VLAN 3172	UCS Manager Host Name 10.29.149.205
(HXHVDOMLOCAL) (FQDN or IP Address)	UCS Manager User Name admin
If & Server Hypervisor ① Storage Controller ② Hypervisor ② Storage Controller ③	Domain Name HXHVDOM.LOCAL
	HX Service Account hxadmin
= (b) WZP2143105K hxhv1 hxhv1scvm 192.188.11.226 192.188.11.232	Time Zone Pacific Standard Time
	Domain Controller 10.29.149.222
= D WZP2143102Y hxhv2 hxhv2scvm 192.168.11.227 192.168.11.233	OrganizationOU=HyperFlex,DC=HXHVDOM,DC=LC Unit
	Local Administrator User Name administrator
= O WZP2143103M hxhv3 hxhv3scvm 192.168.11.228 192.168.11.234	Server Selection
	Server 2 WZP2143102Y / HXAF220C-M55X
e  WZP2143101H hxhv4 hxhv4scvm 192.168.11.229 192.168.11.235	Server 3 WZP2143103M / HXAF220C-M5SX
	Server 1 WZP2143105K / HXAF220C-M55X
	Server 4 WZP2143101H / HXAF220C-M5SX
Management Data	UCSM Configuration
Cluster Address hxhvoip 192 188.11 230	VLAN Name hx-inband-mgmt
	VLAN ID 3175
Subnet Mask 255.255.255.0 255.255.0	VLAN Name hx-storage-data
	VLAN ID 3172
Gateway 10.29.149.1 192.168.11.1	VLAN Name hx-livemigrate
	VLAN ID 3173
	VLAN Name vm-network
	VLAN ID(s) 3174
	MAC Pool Prefix 00:25:85:0A 🗸
	K Back Continue

A default gateway is not required for the data network, as those interfaces normally will not communicate with any other hosts or networks, and the subnet can be non-routable.

- 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.

6

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.

Credentials	Server Selection	UCSM Configuration	Hypervisor Configuration	IP Addresses	Cluster Configurati
isco HX Cluster				Configura	tion
uster Name (SMB Access Point)	Replication Facto	r	Failover Cluster Name 🕕	Credentials	
hxhvsmb	2 🔻 🛈		hxhvwfc	UCS Manager	Host Name 10.29.149.2
				UCS Manager	User Name adm
				Domain Name	HXHVDOM.LOC
ontroller VM				HX Service Acc	count hxadm
eate Admin Password	Confirm Admin P	assword		Time Zone	Pacific Standard Tir
	••••••••	•		Domain Contr	oller 10.29.149.2
				OrganizationC	U-HyperFlex,DC-HXHVDOM,
stem Services				Local Administ	trator User Name administrat
stem services				Server Select	tion
IS Server(s)	NTP Server(s)		DNS Domain Name	Server 2 V	VZP2143102Y / HXAF220C-M5
10.29.149.222	HXHVDOM.LC	DCAL	HXHVDOM.LOCAL		ZP2143103M / HXAF220C-M5
ne Zone				Server 1 V	VZP2143105K / HXAF220C-M5
JTC-08:00) Pacific Time (US	and Canada)	▼ 3		Server 4 W	/ZP2143101H / HXAF220C-M5
				UCSM Config	uration
uto Support				VLAN Name	hx-inband-mg
to Support	Send service tick	et notifications to		VLAN ID	31
Enable Connected Services (Recommended)	0			VLAN Name	hx-storage-da
(Reconfinenceo)				VLAN ID	31
				VLAN Name	hx-livemigra
Advanced Configuratio	n			VLAN ID	31
nbo Frames	Disk Partitions			VLAN Name	vm-netwo
Enable Jumbo Frames on Data Network	① Clean up dis	k partitions		VLAN ID(s)	31
				MAC Pool Prei	ix 00:25:B5:

Figure 88 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.

illilli cisco HyperFlex Installer		00000
	Progress	
Start Hypervisor Configuration	Deploy Deploy Create Cluster Validation Creation	Configuration Credentials Domain Name HXHVDOM.LOCAL
Deploy in Progress		HX Service Account hxadmin Domain Administrator User administrator Name Time Zone Pacific Standard Time
Deploy - Overall In Progress	Deploy	Domain Controller 10.29.149.222 OrganizationOU=HyperFlex.DC=HXHVDOM.DC=LC Unit Local Administrator User Name administrator
hxhv1.HXHVDOM.LOCAL	HyperV Host Add     Getting Ready to Copy Required Powershell, Task and XML files to Windows Host     Validate HyperV Hosts     Main Playbook [HyperV Host Configuration]     Rebooting Host (Scheduled Tasks)	Server 2         WZP2143102Y / HXAF220C-M55X           Server 3         WZP2143103M / HXAF220C-M55X           Server 1         WZP2143105K / HXAF220C-M55X           Server 4         WZP2143101H / HXAF220C-M55X           Hypervisor Configuration         Hypervisor
hxhv2.HXHVDOM.LOCAL	<ul> <li>HyperV Host Add</li> <li>Getting Ready to Copy Required Powershell, Task and XML files to Windows Host</li> <li>Validate HyperV Hosts</li> <li>Main Playbook (HyperV Host Configuration) Rebooting Host (Scheduled Tasks)</li> </ul>	Subnet Mask         255.255.255.0           Gateway         10.29.149.1           DNS Server(s)         10.29.149.222           Primary DNS Suffix         HXHVDOMLOCAL           Server 1         Static IP Address
hxhv3.HXHVDOM.LOCAL In Progress	<ul> <li>HyperV Host Add</li> <li>Getting Ready to Copy Required Powershell, Task and XML files to Windows Host</li> <li>Validate HyperV Hosts</li> <li>Main Playbook [HyperV Host Configuration] Rebooting Host (Scheduled Tasks)</li> </ul>	Hostname hxhv1 Server 2 Static IP Address 10.29.149.227 Hostname hxhv2 Server 3

#### Figure 89 HyperFlex Installer – Installation Progress

19. Review the Summary screen after the install completes by selecting Summary on the top right of the window.

#### Figure 90 HyperFlex Installer – Installation Summary

cisco	HyperFle	x Installer							0			ø	0
		I	Progress					Sum	imary				
Clus	ter Name <b>hxł</b>	NVSMD ONLINE	HEALTHY										
Versi	ion			3.0.1b-29665		Domain Na	ime				H	XHVDOM.L	OCAL
Clust	ter Management	IP Address	hxhvcip.HXH	VDOM.LOCAL		Failover clu	ister Nam	e				hx	hvwfc
Clust	ter Data IP Addre	SS	1	92.168.11.230		DNS Server	(s)					10.29.14	19.222
Repli	ication Factor			Two copies		NTP Server	(s)					10.29.14	19.222
Avail	lable Capacity			9.6 TB									
Serv	vers												
Mo	del	Serial Number	Management Hypervisor	Managemen	t Storage Con	ntroller	Data N	etwork Hypervisor	D	Data Networ	k Storage (	Controller	
HXA	AF220C-M55X	WZP2143101H	10.29.149.229	10.29.149.23	5		10.29.1	49.229	1	92.168.11.23	35		
HXA	AF220C-M5SX	WZP2143105K	10.29.149.226	10.29.149.23	2		10.29.1	49.226	1	92.168.11.23	32		
HXA	AF220C-M5SX	WZP2143102Y	10.29.149.227	10.29.149.23	3		10.29.1	49.227	1	92.168.11.23	33		
HXA	AF220C-M5SX	WZP2143103M	10.29.149.228	10.29.149.23	4		10.29.1	49.228	1	92.168.11.23	34		
								Back to Workflow	Selectio	on La	unch Hype	erFlex Conr	nect

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.

Figure 91 HyperFlex Installer - Export Configuration

cisco HyperFlex Installer			0 0		0	0
Progress		Export Co	ninguration			
Cluster Name hxhvsmb ONLINE HEALT	W					
Version	3.0.1d-29754	Domain Name		HOHVE	DOM1.LC	DCAL
Cluster Management IP Address	hxhiveip.HXHVDOM1.LOCAL	Failover cluster Name			hxh	wwfc
Cluster Data IP Address	192.168.11.135	DNS Server(s)		1	0.104.29	52.44
Replication Factor	Three copies	NTP Server(s)		1	0.104.29	52.44

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

#### Figure 92 HX Connect UI

≡	dialle HyperFlex Connect			hxhvsmb		≣ 5	¢	0	Ŋ
	Dashboard	$\oslash$	operational status Online						
*	Events Activity	_\/_•	RESILIENCY HEALTH Healthy ①		✓ 1 Node failure	can be tol	erated		
ANAL		Ð	CAPACITY 9.6 TB	1.0% STORAGE 101.5 GB Used 9.5 TB Free OPTIMIZ/	E compress ATION (1) ratios will have suff	optimization, sion and dec l be calculate ficient inform g cluster USA	luplication ed once we nation		
MANA	GE System Information		NODES 4	4 HXAF220C-M55X					
-	Datastores	IOPS Last 1	hour		Read Max: 0 Min:0	0 Avg: 0 • V	Vrite Max: 5 N	tin:1.8 Avg: 3.	.14
<u>*</u>	Upgrade	4	$\sim$				$\overline{}$	<u> </u>	
		Throughput	(MBps) Last 1 hour		Read Max: 0 Min:0 Avg	g: 0 • Write	Max: 0.02 Mi	n:0.01 Avg: 0.	.01
		0.02	$\overline{\mathbf{v}}$	$\Delta$			$\sim$	<u> </u>	
		Latency (ms	ec) Last 1 hour		Read Max: 0 Min:0 Avg:	0 • Write )	Max: 13.09 Mi	n:1.94 Avg: 2.	.56

# Post Installation Tasks

#### Create Datastores

You need to create a datastore to store 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.

#### Figure 93 HX Connect - Datastores

≡	المانية: HyperFlex Connect			hxhvsmb		🖽 1	Ø	?	৫
æ	Dashboard	Datastores				Last refreshed at:	05/25/201	8 2:53:16 AM	θN
MON	ITOR	🖬 Create Datastore	∕Edit ×Del						
	Events	Name	^	Status	Size	Used	Free	2	
	Activity			No recor	rds found				
ANAL	YZE								
<u>lut</u>	Performance								
MANA	AGE								
	System Information								
9	Datastores								
<b>1</b>	Upgrade								

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.

Figure 94 HX Connect - Create Datastore

Create Datastore				⊙⊗
Datastore Name HXDS1				
Size			Block Siz	ze
1	ТВ	Ŧ	8K	Ŧ
	Cancel	C	reate Data	astore

#### 6. Click Create Datastore.

Figure 95 HX Connec	t - Datasto	ore Status							
$\equiv \operatorname{cusc}^{\mathrm{abab}}$ HyperFlex Connect			hxhvsmb		∎4	• 0			
B Dashboard	Datastore	5		Last refreshed at: 05/25/2018 2:57:17 A					
MONITOR	🖬 Create Data	istore 🖉 Edit 🗆 X Delet			tiv ∽ Filter				
* Events						_			
Activity		Name ^	Status	Size	Used	Free			
ANALYZE		HXDS1	Normal	1 TB	0 B	1 TB			
dil Performance	Showing 1 - 1 of 1								

#### 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.

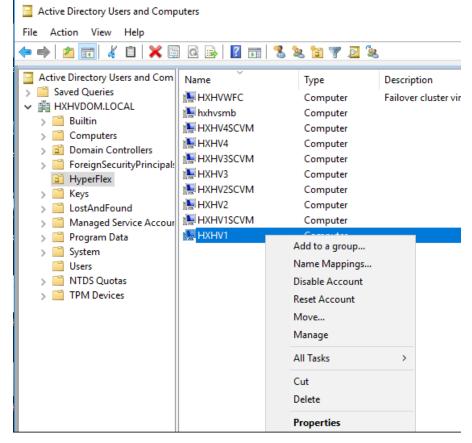
Constrained Delegation requires that the option for the security setting User Account Control: Behavior of the elevation prompt for Administrators in Admin Approval Mode is set to Elevate without Prompting. This will prevent the global AD policy from overriding policy on HX OU.

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 the 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 96 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.

XHV1 Prop	erties				?		×
Location	Managed By	Object	Security	Dial-in	Attribu	ıte Ed	litor
General	Operating System	Member O	f Delega	tion Pa	ssword R	eplica	tion
	is a security-sensitiv nother user.	e operation, w	nich allows s	ervices to ac	t on		
O Do not t	rust this computer fo	or delegation					
O Trust thi	is computer for dele	gation to any se	ervice (Kerbe	ros only)			
-	is computer for dele	gation to specif	ied services	only			
-	Kerberos only						
<u> </u>	any authentication						
Service	s to which this acco	ount can preser	nt delegated	credentials:			
Servio	ce Type User or	Computer	Po	rt	Se		
cifs cifs WSM	hxhv1	D.HXHVDOM.L	OCAL				
<					>		
🗌 Ехр	anded		Add	Remov	е		
		ок	Cancel	Apply		Hel	_

Figure 97 Active Directory Users and Computers - Server Properties

- 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.

HXHV1 Prop	erties					?	×
Location	Managed By	Object	Security	Dial-in	Attri	bute Ed	litor
General	Operating System	Member 0		tion Pas	ssword	Replica	tion
behalf of ar Do not f Trust th Trust th Use Use	is a security-sensitive nother user. trust this computer for is computer for deleg is computer for deleg kerberos only any authentication p	r delegation ation to any s ation to speci protocol	ervice (Kerbe fied services	ros only) only	t on		
	es to which this acco ce Type	unt can prese		credentials: r Computer	~		
cifs	ce Type			nb HXHVDO			
cifs			hxhv1				
	soft Virtual System M	igration Servi		2			
	soft Virtual System M			3			
Micro	soft Virtual System M	igration Servi	ce HXHV	4			
WSM	IAN		HXHV	1	$\sim$		
<				>			
Ехр	anded		Add	Remov	e		
	C	Ж	Cancel	Apply		Hel	p

#### Figure 98 Active Directory Users and Computers - Constrained Delegation

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.

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.

# Post HyperFlex Cluster Installation for Hyper-V 2016

The HyperFlex installer configures all components of the environment from the UCS policies to the Hyper-V networking. In order to manage the environment from SCVMM for the purpose of VDI, you must perform some post-installation steps to allow Citrix XenDesktop to use the environment.

This section detail the steps to prepare the environment for VDI use.

# 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

23

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.

#### Figure 99 SCVMM – Create a Host Group

Hon	ne Fold	ler			/lachine Mana				
• Res	Add ources • Add	Colored and Colored	abric sources Show	ance	Scan Re				
Fabric		< Hosts (0)							
<ul> <li>M Servers</li> <li>All Host</li> </ul>	s	Name	Host Sta	- F	Role				
🗎 Hyper					h				
Infrastrukture		1233	Add Hyper-V Hosts and Clusters Add VMware ESX Hosts and Clusters						
Networking	0.0	Create Host Group							

- 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.

#### Figure 100 SCVMM - Discovery Scope

H Add Resource Wizard	×
📬 Discovery	Scope
Resource Location Credentials Discovery Scope Target Resources Host Settings Summary	Specify the search scope for virtual machine host candidates         Search for computers by whole or partial names, FQDNs, and IP addresses. Alternative generate an Active Directory query to discover the desired computers. <ul> <li>Specify Windows Server computers by names</li> <li>Specify an Active Directory query to search for Windows Server computers</li> </ul> Enter the computer names of the hosts or host candidates that you want VMM to macomputer name must be on a separate line.         Computer names:              hxhvwfc.hxhvdom.local             Skip AD verification         Examples: server1             server1             server1.2a01:110:1e:3:f8ffcfe44:23
	Previous Next Cancel

6. In the Target Resources page, select all the discovered hosts and click Next.

#### Figure 101 SCVMM - Target Resources

省 Add Resource Wizard		×
📬 Target Res	ources	
Resource Location	Select the computers that you	want to add as hosts
Credentials	Discovered computers:	
Discovery Scope	Computer Name	Operating System
Target Resources	✓ ₩ HXHVWFC.HXHVDOM.LOCAL	Windows Server 2016 Datacenter
Host Settings	hxhv2.HXHVDOM.LOCAL	Windows Server 2016 Datacenter
_	hxhv4.HXHVDOM.LOCAL	Windows Server 2016 Datacenter
Summary	hxhv1.HXHVDOM.LOCAL	Windows Server 2016 Datacenter
	hxhv3.HXHVDOM.LOCAL	Windows Server 2016 Datacenter
	Select all Refresh Stop	
		Previous Next Cancel

7. In the Host Settings page, select the appropriate Host group and click Next.

Figure 102 SCVMM	
Add Resource Wizard	×
背 Host Settir	ngs
Resource Location Credentials	Specify a host group and virtual machine placement path settin Assign the selected computers to the following host group:
Discovery Scope	Host group:
Target Resources	
Host Settings	If any of the selected hosts are currently managed by another Virtual Machine Mana environment, select this option to reassociate the hosts with this VMM management
Summary	Reassociate this host with this VMM environment
	Previous Next Cancel

8. In the summary page, confirm the settings and click Finish.

guie roo et	CVMM - Ser									
	Cluster Tools Sen	ver Tools Administrato	r - SCVN	MM2016.HXHVDOM.LOCAL -	Virtual	Machine Ma	nager (Evaluation Vers	sion - 180 c	lays remainir	ap X
Home Fold	er Host Cluster	Host								
afrech Refrech Virtual	Shut Down U Power O Restart O Power O Reset View Sta	-06	nce Moo	de 🜘 Apply Latest Code Inte de 찬 Move to Host Group	grity P	olicy 📑	Remove Cluster Node	Window	Remove	Properties
Machines 4	View Sta	Host	intanta				Cluster	•	Remove	Properties
oric <	Hosts (4)									
Servers										
All Hosts	Name	Host Status 👻	Role	Job Status 👻	CPU	Average	Available Me 👻	Operating	System	
🔺 🚞 HyperFlex	hxhv1.HXHVDOM.LC	OCAL OK	Host	Completed w/ Info	0 %		0 КВ	Microsoft	Windows Se	rver 2016 Dat
HXHVWFC	hxhv2.HXHVDOM.LC	DCAL OK	Host	Completed w/ Info	0%		0 KB	Microsoft	Windows Se	rver 2016 Dat
🛂 Infrastructure	hxhv4.HXHVDOM.LC	DCAL OK	Host	Completed	0 %		0 KB	Microsoft	Windows Se	rver 2016 Dat
- Networking	hxhv3.HXHVDOM.LC	DCAL OK	Host	Completed w/ Info	0 %		0 KB	Microsoft	Windows Se	rver 2016 Dat
3 Storage										
- Storage	hxhv1.HXHVDOM.LOC	AL								
	Status			Virtual machine			Recent job			
	Host status: OK			Virtual machines: 2			Managed com	puter job:	No recent jo	ь
	Date modified: 5/29/2	018 10:44:08 AM					Job status:			
	Cluster service: 🥑 Ru	inning					Host job:		Refresh virtu properties	al machine
	Host			Fabric			Job status:	1	00 % Comp	eted w/ Info
	Operating system: Microsoft Windows Server 2016 Datacenter			Storage disks: 1 Storage used: 134.34 GB			Compliance			
	Virtualization software	: Microsoft Hyper-V		Storage used. 154.54 Ob			Compliance sta	atus:		
	Processor:	(40) 2.20 GHz Intel X	eon				Operational sta	atus:		
	Memory:	190.66 GB					Last scan:			
VMs and Services										

#### Figure 103 SCVMM - Server View

#### Networking

6

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.

When the teams are created, the Network Sites must be created and added to the logical networks created by the installer.

To create the Network Sites, complete the following steps:

1. Under Fabric > Networking > Logical Networks, find the Logical Network created by the installer.



In this example, it is 'vswitch-hx-vm-network'.

Administrator - HX-34, VMM, Issted	m.local - Yirtual Machine Manager (svaluation Version - 1J days remaining)
Home	
este Lopical Network	MC Pool 1977 Ceste Ceste Add Overview Fator Winas Machines Listes View Departeriet Remove Properties Remove Properties Remove Properties
e :	Logisli Networks and IP Pools (7)
PP Servers	
All Hosts	Name Fortwork Compliance Submit Begin Address Ausliable Address Ausliable Addresses
+ THXEAP	mhuhvdom fully consilant
HIRVIWEC	mVDI Fully congliant
Anfrestructure	whydi-rateorik fully complant
I Library Servers	infromethe hard-regent Fully compliant
FXI Servers	rifrivisitch-be-liversignation Fully compliant
🔒 Update Server	inh vavitch-fu-storage-data Fully compliant
ill vCenter Servers	22 visiki, b. far ver metwark Euly complaint
VMM Server	W
- Networking	
🛁 Logical Networks	
MAC Address Pools	
St Load Balancers	
I VP Templates 로 Logical Switches	
Port Profiles	
Port Classifications	
2 Network Service	
Storage	
Classifications and Pools	
Providers	
Artais	
2 File Servers	
Fibre Channel Fabrics	
& QoS Policies	
	weekb ha we welsook
	Logical network information
	Description
gr VMs and Services	
🛃 Tabric	
Library	
Jobs	

2. Right-click and select 'Properties' of the logical network.

Administrator - HX-SCVMM.hxi	hvdom.local -	Virtual Machine M	Manager (Evaluati	on Ver	sion - 13 days rer	naining)				
Create Logical Create VM Network Network	ate IP Pool ate MAC Pool ate VIP Templ Create	I Create Iate Logical Swite	Create h Res	Add ource Add	Overview s •		않 Services @ Virtual Machines 한 Hosts	Power Jobs PRO Windo		
Fabric	< Log	ogical Networks a	nd IP Pools (7)							
▲ 🏦 Servers										
🔺 🛄 All Hosts	Na	lame	*			Ne	twork Compliance	Sub		
🔺 🚞 HX EAP		the hydrom				Fu	lly compliant			
HXHV1WFC		<del>nh</del> rVDI				Fu	lly compliant			
A infrastructure		v∰vdi-network				Fu	lly compliant			
Library Servers		rth vswitch-hx-inband-mgmt					Fully compliant			
PXE Servers		thrvswitch-hx-livemigration					Fully compliant			
Update Server		very vswitch-hx-storage-data					Fully compliant			
VCenter Servers		Thrvswitch-hx-vr	m-network			Fo	llu.comolizaț			
J VMM Server				-	Create IP Pool					
🔺 📥 Networking				4	Create VM Net	work				
the Logical Networks				R	View Depender	nt Resourc	es			
MAC Address Pools				-	Remove					
Load Balancers					Properties	Dr.				
VIP Templates			L			63				
R Logical Switches										
Port Profiles										
Port Classifications										
2 Natural Canica										

6

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

In this example VLAN 34 was used for the VM network and VLAN 33 was used for Live Migration

Fully comp Fully comp					
Fully comp					
The vswitch-hx-vm-r					×
Name Network Site	Network sites Network sites can be added to a I Enter IP subnets using CIDR notat	Host groups	e: 192.168.1.0/24, FD4A:290 that can use this network s	CD:184F:3A2C::/64.	
		Associated V VLAN 34	LANs and IP subnets:	Insert row Delete row	
View Script		Network site	name: vswitch-hx-vm-net	Work_0	
				UK Cancel	24

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'

General		Hardware			
Status		Switch port det Unknown	*	Logical network connectivity Associate logical networks, IP su	ibnets and VI ANs:
Hardware	1	H Microsoft Network team-hx-storage		Subnet	VLAN
Host Access		vswitch-bx-stor		hxhvdom	
Virtual Machine Paths		Switch port det		vdi-network	34
Reserves		E Microsoft Network		10.34.0.0/20     vswitch-hx-inband-mgmt	34
Storage Virtual Switches	=	۲ <del>أ۱</del> Logical networ vswitch-hx-vm		vswitch-hx-livemigration	33
Migration Settings		Switch port det Unknown		vswitch-hx-storage-data	34
Placement Paths		H Microsoft Network team-hx-livemigra			<i></i>
Servicing Windows		vswitch-hx-live			
Host Guardian Service		Switch port det Unknown			ot show up in the list, you need to
Enhanced Session		B DVD / CD-ROM drives	÷	configure it in the correspor	naing network site.

#### 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

Figure 104 PowerShell - Get VMSwitch

```
[hxhv1]: PS C:\Users\Administrator.HXHVDOM\Documents> Get-VMSwitch
Name SwitchType NetAdapterInterfaceDescription
vswitch-hx-livemigration External Microsoft Network Adapter Multiplexor Driver #4
vswitch-hx-vm-network External Nicrosoft Network Adapter Multiplexor Driver #2
vswitch-hx-inband-mgmt External Microsoft Network Adapter Multiplexor Driver #3
```

2. Remove the vSwitch named 'vswitch-hx-livemigration' using the following PowerShell command.

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

Figure 105 PowerShell - Remove VMSwitch

[hxhv1]: PS C:\Users\Adr	ministrator.	HXHVDOM\Documents	> Remove-	-VMSwitch -Na	ame vswi	tch-hx-livemigrat	ion
[hxhv1]: P5 C:\Users\Add	ministrator.	HXHVDOM\Documents	> Get-VMS	Switch			
Name	SwitchType	NetAdapterInterfa	ceDescrip	otion			
vswitch-hx-storage-data vswitch-hx-vm-network vswitch-hx-inband-mgmt	External	Microsoft Network	Adapter	Multiplexor	Driver	#2 #3	

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

New-NetIPAddress -ifAlias "team-hx-livemigration" -IPAddress 192.168.73.127 -PrefixLength 24

Figure 106 PowerShell - Assign Static IP

[hxhv1]: P5 C:\Us	ers\Administrator.HXHVDOM\Documents> New-NetIPAddress -ifAlias "team-hx-livemigration" -IPAddress 192.168.73.21 -PrefixLength 2
IPAddress	: 192.168.73.21
InterfaceIndex	: 7
InterfaceAlias	: team-hx-livemigration
ddressFamily	: IPv4
ype	: Unicast
refixLength	: 24
refixOrigin	: Manual
uffixOrigin	: Manual
ddressState	: Tentative
/alidLifetime	: Infinite ([TimeSpan]::MaxVa]ue)
referredLifetime	: Infinite ([Timespan]::MaxValue)
kipAsSource	: False : ActiveStore
PolicyStore	: Activestore
PAddress	: 192.168.73.21
nterfaceIndex	: 7
nterfaceAlias	: team-hx-livemigration
ddressFamily	: IPv4
ype	: Unicast
refixLength	: 24
refixorigin	: Manual
uffixOrigin	: Manual
ddressState	: Invalid
alidLifetime	: Infinite ([TimeSpan]::Maxvalue)
	: Infinite ([Timespan]::Maxvalue)
kipAsSource	: False
PolicyStore	: PersistentStore

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.

New-NetIPAddress – if Alias "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 107 PowerShell - Get Cluster Network
```

```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator.HXHVDOM> Get-ClusterNetwork
Name
                  State Metric
                                            Role
                     Up 69760 ClusterAndClient
Cluster Network 1
Cluster Network 3
                     Up 69761 ClusterAndClient
Cluster Network 4
                     Up 29761
                                         Cluster
Cluster Network 5
                     Up
                         29762
                                         Cluster
PS C:\Users\Administrator.HXHVDOM> Get-ClusterNetworkInterface
Name
                                   Node
                                         Network
                                                            State
hxhv1 - vswitch-hx-inband-mgmt
                                   hxhv1 Cluster Network 1
                                                               Up
hxhv2 - vswitch-hx-inband-mgmt
                                   hxhv2 Cluster Network 1
                                                               Up
                                   hxhv3 Cluster Network 1
hxhv3 - vswitch-hx-inband-mgmt
                                                               Up
                                   hxhv4 Cluster Network 1
hxhv4 - vswitch-hx-inband-mgmt
                                                               Up
hxhv1 - vswitch-hx-storage-data
                                   hxhv1 Cluster Network 3
                                                               Up
hxhv2 - vswitch-hx-storage-data
                                   hxhv2 Cluster Network 3
                                                               Up
hxhv3 - vswitch-hx-storage-data
                                   hxhv3 Cluster Network 3
                                                               Up
hxhv4 - vswitch-hx-storage-data
                                   hxhv4 Cluster Network 3
                                                               Up
hxhv1 - vswitch-hx-vm-network
                                   hxhv1 Cluster Network 4
                                                               Up
hxhv2 - vswitch-hx-vm-network
                                   hxhv2 Cluster Network 4
                                                               Up
hxhv3 - vswitch-hx-vm-network
                                   hxhv3 Cluster Network 4
                                                               Up
hxhv4 - vswitch-hx-vm-network
                                   hxhv4 Cluster Network 4
                                                               Up
hxhv1 - team-hx-livemigration (1) hxhv1 Cluster Network 5
                                                               Up
hxhv2 - team-hx-livemigration (1) hxhv2 Cluster Network 5
                                                               Up
hxhv3 - team-hx-livemigration (1) hxhv3 Cluster Network 5
                                                               Up
hxhv4 - team-hx-livemigration (1) hxhv4 Cluster Network 5
                                                               Up
```

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

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 108 PowerShell - Rename the Cluster Network

```
[hxhv1]: PS C:\Users\Administrator.HXHVDOM\Documents> (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"
```

#### 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 109 PowerShell – Configure Cluster Network Roles

```
[hxhv1]: PS C:\Users\Administrator.HXHVDOM\Documents> (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
```

Role = 0 to disable cluster communication

Role = 1 to enable only cluster communication

Role = 3 to enable both cluster & client communication

Figure 110 Failover Cluster Manager - Networks

📲 Failover Cluster Manager				
File Action View Help				
🗢 🔿 🖄 🖬 🛛 🖬				
📲 Failover Cluster Manager	Networks (4)			
✓ 闘 HXHVWFC.HXHVDOM.L Roles	Search			🔎 Queries 🔻 📘 🔻
Nodes	Name	Status	Cluster Use	Information
> 📇 Storage	🗓 hx-storage-data	🕥 Up	None	
Networks	👫 hx-inband-mgmt	🕑 Up	Cluster and Clie	int
	👯 vm-network	💽 Up	None	
	🔢 LiveMigration	💿 Up	Cluster Only	
	<			
	♥ intervention with the wi	gmt		
	Name		Status	Owner Node Info
	🗈 🌉 hxhv3 - vswitch-h	x-inband-mgmt	🕑 Up	hxhv3
	🕀 🌉 hxhv4 - vswitch-h	x-inband-mgmt	💽 Up	hxhv4
	🕀 🌉 hxhv 1 - vswitch-h	x-inband-mgmt	💽 Up	hxhv1
	🗈 🌉 hxhv2 - vswitch-h	x-inband-mgmt	🕑 Up	hxhv2

#### 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 111 PowerShell - Configure Live Migration Network
[https://www.configure.config



Live Migration Settings	×
Networks for Live Migration	
Select one or more networks for virtual machines to use Use the buttons to list them in order from most preferred least preferred at the bottom.	for live migration. I at the top to
Name	Up
LiveMigration hx-inband-mgmt hx-storage-data wr-network	Down
OK Cancel	Apply

### Storage

The data stores created in the HyperFlex Connect interface, creates an SMB share to use to place Virtual Machines. The naming convention is '\\hxClustername\DatastoreName'.

To add the HX Datastores to the HX cluster, complete the following steps:

1. Right-click the Cluster 'HXHV1WFC', select Properties and click 'File Share Storage'.

	JN-0127				Nunning	Nunning
Level VM Networks	i JN-0979				Running	Running
Storage	🧞 JN-0627				Running	Running
All Hosts	🚲 JN-0115				Running	Running
A in hosis	🧞 JN-0411				Running	Running
A B HXHV1WFC	HXHV1WFC.hxhvdom.ld	cal Properties				
hxhv1						
# hxhv2	General	File Share Storage				
hxhv3	1.	The share storage				
hxhv4	🚮 Status	The following file shares will be av	ailable as storage	locations for VMs	deployed to not	les in this cluster:
hxhv5	2.	File Share Path	Access Status	Classification	Free Space	Total Capacity
hxhv6	Available Storage	\\hxhv1cip.hxhvdom.local\Write.	. 0	Remote Storage	20,333.89 GB	20,480.00 GB
hxhv7	File Share Storage	\\hxhv1cip.hxhvdom.local\Infra	0	Remote Storage	2,005.94 GB	2,048.00 GB
hxhv8	il.					
	Shared Volumes					
	5					
	Virtual Switches					
	Custom Properties					
	1. Calcul rioperaci					
	1.					
	1.					
	5					
	16					
	1.					
	1.					
	1.					
	2.					
	8					
	6			(Providence)	r Add	Remove
	1.			Repai	Add	remove
	6					
	View Script				OK	Cancel
	IN-0816				Running	Running

2. Click Add to specify the UNC path for the datastore.

Status	The following file shares will be a	and the second s	And a second state of the second state	and the second se	Concentration of the second
vailable Storage	File Share Path	Access Status	Classification	Free Space	Total Capacity
-	\\hxhv1cip.hxhvdom.local\Write		Remote Storage	OWNERS TO	20,480.00 GB
le Share Storage	\\hxhv1cip.hxhvdom.local\Infra		Remote Storage	2,005.94 GB	2,048.00 GB
	To register a file share t list or enter the UNC pa	th for an unmanage	a managed file sh	ive Directory	
	computer account for t management account. Directory computer acc cluster management ac	he virtualization clu For unmanaged file ount for the virtuali	shares, ensure tha zation cluster and	t the Active	

3. Click OK.

# Build the Virtual Machines and Environment for Workload Testing

# Software Infrastructure Configuration

This section details how to configure the software infrastructure components that comprise this solution.

Install and configure the infrastructure virtual machines by following the process provided in Table 29

Configuration	Citrix XenDesktop Controllers Virtual Machines	Citrix Profile Servers Virtual Machines
Operating System	Microsoft Windows Server 2016	Microsoft Windows Server 2016
Virtual CPU amount	6	8
Memory amount	8 GB	8 GB
Network	VMNIC	Network
Disk-1 (OS) size and location	40 GB	Disk-1 (OS) size and location
Disk-2 size and location	-	
Configuration	Microsoft Active Directory DC's Virtual Machines	
Operating system	Microsoft Windows Server 2016	Operating system
Virtual CPU amount	4	
Memory amount	4 GB	
Network	VMNIC	
Disk size and location	40 GB	
Configuration	Microsoft SQL Server Virtual Machine	Citrix StoreFront Virtual Machine
Operating system	Microsoft Windows Server 2016	Operating system
Virtual CPU amount	4	4
Memory amount	16 GB	8 GB
Network	VMNIC	Network
Disk-1 (OS) size and location	40 GB	Disk-1 (OS) size and location
Disk-2 size and location	200 GB Infra-DS volume	Disk-2 size and location
Configuration	Citrix License Server Virtual Machine	NetScaler VPX Appliance Virtual Machine
Operating system	Microsoft Windows Server 2016	NS11.1 52.13.nc
Virtual CPU amount	4	2
Memory amount	4 GB	2 GB
Network	VMNIC	Network

 Table 29
 Test Infrastructure Virtual Machine Configuration

Disk size and leasting	40.00	20 CP
Disk size and location	40 GB	20 GB

## Prepare the Master Images

This section details how to create the golden (or master) images for the environment. VMs for the master images must first be installed with the software components needed to build the golden images. For this CVD, the images contain the basics needed to run the Login VSI workload.

To prepare the master VMs for the Hosted Virtual Desktops (HVDs) and Hosted Shared Desktops (HSDs), there are three major steps to complete when the base virtual machine has been created:

- Installing OS
- Installing application software
- Installing the Virtual Delivery Agents (VDAs)

The master image HVD and HSD VMs were configured as listed in Table 30 :

Configuration	HVDI	HSD
	Virtual Machines	Virtual Machines
Operating system	Microsoft Windows 10 64-bit	Microsoft Windows Server 2016
Virtual CPU amount	2	8
Memory amount	4.0 GB (reserved)	24 GB (reserved)
Network	VMNIC	VMNIC
	vm-network	vm-network
Citrix PVS vDisk size and location	24 GB	40 GB
	WriteCache Volume	WriteCache Volume
Citrix PVS write cache	6 GB	24 GB
Disk size		
Additional software used for	Microsoft Office 2016	Microsoft Office 2016
testing	Login VSI 4.1.32 (Knowledge Worker Workload)	Login VSI 4.1.32 (Knowledge Worker Workload)

 Table 30
 HVD and HSD Configurations

# Install and Configure XenDesktop Delivery Controller, Citrix Licensing, and StoreFront

This section details the installation of the core components of the XenDesktop/XenApp 7.16 system. This CVD provides the process to install two XenDesktop Delivery Controllers to support hosted shared desktops (HSD), non-persistent virtual desktops (VDI), and persistent virtual desktops (VDI).

The process of installing the XenDesktop Delivery Controller also installs other key XenDesktop software components, including Studio, which is used to create and manage infrastructure components, and Director, which is used to monitor performance and troubleshoot problems.

#### Install Citrix License Server

To install the Citrix License Server, complete the following steps:

- 1. To begin the installation, connect to the first Citrix License server and launch the installer from the Citrix XenDesktop 7.16 ISO.
- 2. Click Start.

Deliver applications and desktops to any user, anywhere, on any device. • Hybrid cloud, cloud and enterprise provisioning • Centralized and flexible management Manage your delivery according to your needs: XenApp Deliver applications Start XenDesktop Deliver applications and desktops Start	
CITRIX	

3. Click "Extend Deployment - Citrix License Server."

Get Started		Prepare Machi	Prepare Machines and Images			
Delivery Controller		Virtual Delive	ery Ag	ent for Windows Server OS		
Start here. Select and install the essential services like License S				eliver applications and desktops from s al machines.	server-	
Extend Deployment Citrix Director	0	Citrix Studio	•	Self-Service Password Reset	()	
Citrix License Server	۰	Universal Print Server		Session Recording	6	
Citrix StoreFront		Federated Authentication Service				

- 4. Read the Citrix License Agreement.
- 5. If acceptable, indicate your acceptance of the license by selecting the "I have read, understand, and accept the terms of the license agreement" radio button.
- 6. Click Next.

XenDesktop 7.16	Software License Agreement	
Licensing Agreement	Printable ver	sior
Core Components Firewall Summary Install Finish	CITRIX LICENSE AGREEMENT This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"), Your location of receipt of the Citrix providing-entities him. BY INSTALLING AND OR USING THE PRODUCT, YOU ARE AGREENG TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT. 1. PRODUCT LICENSES. a. End User Licenses. The software in a software PRODUCT and the software installed in an appliance PRODUCT is made available by CITRIX under the license models identified at http://www.citrix.com/buylicensing/ producthml. Any experimental features delivered with such software mans a Citrix proprietary and/or open source software program in object Code form licensee Meeting envertimes early are draware appliance with installed Software. Netwithstending envertimes early and/or open source software program in object Code form licensee Meeting envertimes early active active agreement	×.
	I do not accept the terms of the license agreement	

#### 7. Click Next.

XenDesktop 7.16	Core Components
<ul> <li>Licensing Agreement</li> <li>Core Components</li> </ul>	For scale and performance reasons, it is recommended that Director and the License Server be installed on separate servers.
Firewall Summary	Location: C:\Program Files\Citrix Change
Install	License Server (Required)
Finish	Manages product licenses.

- 8. Select the default ports and automatically configured firewall rules.
- 9. Click Next.

XenDesktop 7.16	Firewall	
Licensing Agreement	The default ports are listed below.	Printable version
✓ Core Components Firewall Summary Install Finish	License Server 7279 TCP 27000 TCP 8083 TCP 8082 TCP	
	Configure firewall rules: Automatically Select this option to automatically create the rules in the W created even if the Windows Firewall is turned off.	Vindows Firewall. The rules will be
	Manually Select this option if you are not using Windows Firewall or yourself.	if you want to create the rules
	Ba	ick Next Cancel

10. Click Install.

XenDesktop 7.16	Summary Review the prerequisites and confirm the components you want to install.
<ul> <li>✓ Core Components</li> <li>✓ Firewall</li> <li>Summary</li> <li>Install</li> <li>Finish</li> </ul>	Installation directory C\Program Files\Citrix Core Components License Server Firewall TCP Ports: 7279, 27000, 8083, 8082
	Back Install Cancel

11. Click Finish to complete the installation.

<ul> <li>Licensing Agreement</li> <li>Core Components</li> <li>Firewall</li> <li>Summary</li> <li>Install</li> <li>Post Install</li> <li>Component Initialization</li> <li>Initialized</li> </ul>	XenDesktop 7.16	Finish Installation	
	✓ Core Components ✓ Firewall ✓ Summary ✓ Install	Core Components ✓ License Server Post Install	

#### Install Citrix Licenses

To install the Citrix Licenses, complete the following steps:

1. Copy the license files to the default location (C:\Program Files (x86)\Citrix\Licensing\ MyFiles) on the license server.

€ 💿 🔹 ↑	🎳 « Program Files (x86) 🕨 Citrix 🕨 Lice	ensing 🕨 MyFiles	v 0	Search MyFiles	۶
🚖 Favorites	Name	Date modified	Туре	Size	
	CITRIX.opt	10/10/2016 4:00 PM	OPT File	1 KB	
🖳 This PC	citrix_startup.lic	10/10/2016 4:01 PM	LIC File	7 KB	
	LicenseXD1000_071315_18mo_e.lic	10/10/2016 4:29 PM	LIC File	16 KB	

- 2. Restart the server or Citrix licensing services so that the licenses are activated.
- 3. Run the application Citrix License Administration Console.

Apps Citrix License Administration Console	
Citrix License Administration Co	
Citrix Licensing Manager	
Citrix Studio NEW	
Citrix StoreFront NEW	
Citrix Scout NEW	

4. Confirm that the license files have been read and enabled correctly.

		Dashboard	Administrat
Alerts	Concurrent Licenses	Vendor Daen	nore CITRIX
🔇 🔺	Product SA Date In Use (Available)	Expiration	
0 Critical	Otrix Start-up License(Server		
	<ul> <li>Obrik StorageLink EnterprisejConcurrent</li> </ul>		
	► Citrix XenApp Enterprise[Concurrent		
	► Oltrix XenApp Platinum)Concurrent		
	Otrix XenDesktop Enterprise(Concurrent		
	<ul> <li>Oltrix XenDesktop Enterprise/Concurrent (Legacy)</li> </ul>		
	Otrix XenDesktop Enterprise User/Device		
	Otric XenDesktop Platinum/Concurrent		
	+ Otrix XenDesktop Platinum/Concurrent (Legacy)		
	+ Otrix XenDesktop Platinum/User/Device		
	► Otrix XenDesktop VDI/Concurrent		
	<ul> <li>Citrix XenDesktop VDI/Concurrent (Legacy)</li> </ul>		
	<ul> <li>Otrik XenDesktop VDI/User/Device</li> </ul>		

#### Install XenDesktop

To install XenDesktop, complete the following steps:

- 1. To begin the installation, connect to the first XenDesktop server and launch the installer from the Citrix XenDesktop 7.16 ISO.
- 2. Click Start.

Deliver applications and desktops to any user, anywhere, on any device. • Hybrid cloud, cloud and enterprise provisioning • Centralized and flexible management Manage your delivery according to your needs:
XenApp Deliver applications
XenDesktop Deliver applications and desktops Start
Cancel
CITRIX

The installation wizard presents a menu with three subsections.

3. Click "Get Started - Delivery Controller."

Get Started		Prepare	Prepare Machines and Images			
Delivery Controller		Virtual I	Virtual Delivery Agent for Windows Server OS			
Modify or remove Delivery Controller compon			is agent to di Ms or physica	eliver applications and desktops from s Il machines.	erver-	
		Citrix Studio	0	Self-Service Password Reset	(1)	
Extend Deployment Citrix Director	0	Citrix Studio	۵	Self-Service Password Reset	.0	
	0	Citrix Studio Universal Print Server	6	Self-Service Password Reset Session Recording	•	

- 4. Read the Citrix License Agreement.
- 5. If acceptable, indicate your acceptance of the license by selecting the "I have read, understand, and accept the terms of the license agreement" radio button.
- 6. Click Next.

XenDesktop 7.16	Software License Agreement
Licensing Agreement	Printable version
Core Components Features Firewall Summary Install Smart Tools Finish	CITRIX LICENSE AGREEMENT This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix.providing.entities.html. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT.
	PRODUCT LICENSES.     a. End User Licenses. The software in a software PRODUCT and the software installed in an appliance PRODUCT is made available by CITRIX under the license models identified at http://www.citrix.com/buy/licensing/ product.html. Any experimental features delivered with such software will be identified and are licensed only for internal testing purposes. "Software" means a Citrix proprietary and/or open source software program in object code form licensed hereunder. "Appliance" means a hardware appliance with installed Software. Natwithsteading sources of beth in this AGPETMENT or at the license difference. In the license agreement of lot not accept the terms of the license agreement     Back Next Cancel

7. Select the components to be installed on the first Delivery Controller Server:

- a. Delivery Controller
- b. Studio
- c. Director
- 8. Click Next.

XenDesktop 7.16	Core Components
<ul> <li>Licensing Agreement</li> <li>Core Components</li> </ul>	For scale and performance reasons, it is recommended that Director and the License Server be installed on separate servers.
Features Firewall Summary Install Smart Tools Finish	Location: C:\Program Files\Citrix Change
	Component (Select all)
	Delivery Controller  Distributes applications and desktops, manages user access, and optimizes connections.
	Studio Create, configure, and manage infrastructure components, applications, and desktops.
	Director Monitor performance and troubleshoot problems.
	License Server A This component must be installed at least once.
	□ StoreFront ▲ This component must be installed at least once.
	Back Next Cancel

Dedicated StoreFront and License servers should be implemented for large scale deployments.

- 9. Since a SQL Server will be used to Store the Database, leave "Install Microsoft SQL Server 2012 SP1 Express" unchecked.
- 10. Click Next.

<u>6</u>

(enDesktop 7.16	Feature	25
Licensing Agreement		Feature
Core Components Features		Install Windows Remote Assistance Select this only if you need the shadowing feature of Director Server.
Firewall		
Summary		
Install		
Smart Tools		
Finish		
	E.	

- 11. Select the default ports and automatically configured firewall rules.
- 12. Click Next.

The default ports are listed below. Delivery Controller 80 TCP	Director	Printable version
	Director	
00 700		
	80 TCP	
443 TCP	443 TCP	
Configure firewall rules:		
Automatically		
Select this option to automaticall		rewall. The rules will be
Manually Select this option if you are not u yourself.	sing Windows Firewall or if you war	it to create the rules
	<ul> <li>Automatically Select this option to automatically created even if the Windows Fired</li> <li>Manually Select this option if you are not u</li> </ul>	<ul> <li>Automatically Select this option to automatically create the rules in the Windows Fi created even if the Windows Firewall is turned off.</li> <li>Manually Select this option if you are not using Windows Firewall or if you ware</li> </ul>

13. Click Install to begin the installation.

#### Build the Virtual Machines and Environment for Workload Testing

	Summary	
<ul> <li>Licensing Agreement</li> <li>Core Components</li> <li>Features</li> <li>Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	Review the prerequisites and confirm the components you want to install.  Installation directory C\Program Files\Citrix  Prerequisites  Microsoft Visual x64 C++ 2015 Runtime Local Host Cache Storage (LocalDB) Microsoft Visual x86 C++ 2015 Runtime Microsoft SQL CLR Types (x86) Microsoft SMO Objects (x86) Microsoft SMO Objects (x64)	
	Microsoft SMO Objects (x04) Microsoft Internet Information Services Windows Remote Assistance Feature Core Components Delivery Controller Studio Director Features	

- 14. (Optional) Click the Call Home participation.
- 15. Click Next.

KenDesktop 7.16	Smart Tools
<ul> <li>Licensing Agreement</li> <li>Core Components</li> <li>Features</li> </ul>	Automate deployment tasks, health checks, and power management on-premises and in the cloud.
≠ Firewall ≠ Summary ≠ Install	Run health checks and turn on Call Home to diagnose issues and find recommended fixes. Learn more about Call Home Smart Scale Keep your cloud Site costs under control with smart power management for VMs.
Smart Tools Finish	Simart Migrate Simplify migration to the latest XenApp and XenDesktop versions. Simplify migration to the latest XenApp and XenDesktop versions. Simart Build Quickly build sites on-premises and in the cloud using ready-made or custom blueprints I want to connect to Smart Tools and Call Home. I do not want to connect to Smart Tools or Call Home You will need Citrix Cloud or citrix.com credentials. View your privacy policy here. Connect
	Next

- 16. Click Finish to complete the installation.
- 17. (Optional) Check Launch Studio to launch Citrix Studio Console.

<ul> <li>Licensing Agreement</li> <li>Core Components</li> <li>Features</li> <li>Microsoft Visual x64 C++ 2015 Runtime</li> <li>Installed</li> <li>Local Host Cache Storage (LocalDB)</li> <li>Installed</li> <li>Microsoft Visual x86 C++ 2015 Runtime</li> <li>Installed</li> <li>Microsoft SQL CLR Types (x86)</li> <li>Microsoft SQL CLR Types (x64)</li> <li>Microsoft Internet Information Services</li> <li>Installed</li> <li>Windows Remote Assistance Feature</li> <li>Installed</li> <li>Delivery Controller</li> <li>Studio</li> <li>Director</li> <li>Installed</li> <li>Microsoft Installed</li> <li>Component Initialization</li> <li>Initialized</li> </ul>	XenDesktop 7.16	Finish Installation	
Prerequisites       Installed         Firewall       Local Host Cache Storage (LocalDB)       Installed         Summary       Microsoft Visual x86 C++ 2015 Runtime       Installed         Install       Microsoft SQL CLR Types (x86)       Installed         Smart Tools       Microsoft SQL CLR Types (x64)       Installed         Windows Remote Assistance Feature       Installed         Core Components       Delivery Controller       Installed         Studio       Director       Installed         Post Install       Post Install       Post Installed	<ul> <li>Licensing Agreement</li> </ul>	The installation completed successfully.	Succes
	<ul> <li>✓ Features</li> <li>✓ Firewall</li> <li>✓ Summary</li> <li>✓ Install</li> <li>✓ Smart Tools</li> </ul>	<ul> <li>Microsoft Visual x64 C++ 2015 Runtime</li> <li>Local Host Cache Storage (LocalDB)</li> <li>Microsoft Visual x86 C++ 2015 Runtime</li> <li>Microsoft SQL CLR Types (x86)</li> <li>Microsoft SMO Objects (x86)</li> <li>Microsoft SQL CLR Types (x64)</li> <li>Microsoft SMO Objects (x64)</li> <li>Microsoft Internet Information Services</li> <li>Windows Remote Assistance Feature</li> <li>Core Components</li> <li>Delivery Controller</li> <li>Studio</li> <li>Director</li> <li>Post Install</li> </ul>	Installed Installed Installed Installed Installed Installed Installed Installed Installed Installed
Caunch Studio		✓ Launch Studio	

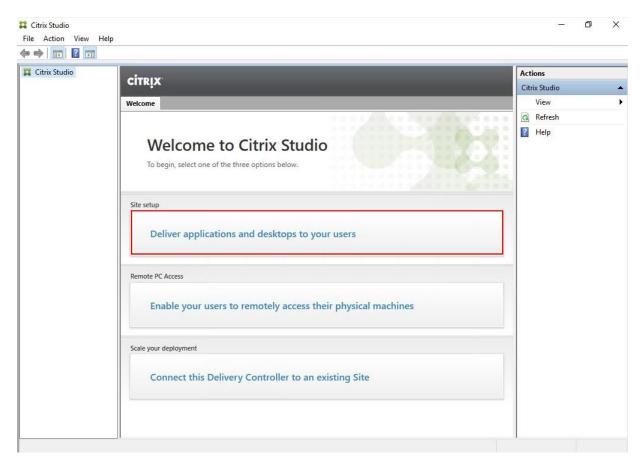
### Configure the XenDesktop Site

Citrix Studio is a management console that allows you to create and manage infrastructure and resources to deliver desktops and applications. Replacing Desktop Studio from earlier releases, it provides wizards to set up your environment, create workloads to host applications and desktops, and assign applications and desktops to users.

Citrix Studio launches automatically after the XenDesktop Delivery Controller installation, or if necessary, it can be launched manually. Citrix Studio is used to create a Site, which is the core XenDesktop 7.16 environment consisting of the Delivery Controller and the Database.

To configure XenDesktop, complete the following steps:

1. From Citrix Studio, click the Deliver applications and desktops to your users button.



- 2. Select the "A fully configured, production-ready Site" radio button.
- 3. Enter a site name.
- 4. Click Next.

Studio	Introduction
Introduction Databases Licensing Connection Network	You have two options when creating a new Site. The simplest option is to automatically create a fully configured, production-ready Site. The second, more advanced option is to create an empty Site, which you must configure yourself. What kind of Site do you want to create? <ul> <li>A fully configured, production-ready Site (recommended for new users)</li> <li>An empty, unconfigured Site</li> </ul>
Additional Features Summary	Site name:
	Стхр

5. Provide the Database Server Locations for each data type and click Next.

Studio	Databases				
		information about Site setup, config u want to set up the databases. Lean			
<ul> <li>Introduction</li> <li>Databases</li> <li>Licensing</li> </ul>		set up databases from Studio ( rovide details of existing empty	Generate scripts to manually set up databases on the database server		
Connection	Provide database details				
Network Additional Features Summary	Data type Site:	Database name CTXD713_site	Location (formats)		
	Monitoring:	CTXD713_monitoring	CTXD-HA		
	Logging: CTXD713_logging CTXD-HA				
	1 For an Alw	vaysOn Availability Group, specify the	e group's listener in the location.		
	Specify addition 1 selected	al Delivery Controllers for this Site L	earn more Select		

6. For an AlwaysOn Availability Group, use the group's listener DNS name.

📱 Availability Group Listener	Properties - CTXD-HA		2 <u></u> 2		×
Select a page	🖵 Script 🔻 ? Help				
🔎 General	🔄 Script 🔹 😽 Help				
	Listener DNS Name:	-HA			
	Port: 1433				
	Network Mode: Static	10			~
	Network Mode: Static	IF			
	Subnet	IP Address			
	10.10.31.0/24	10.10.31.27			
		24 0000000000000000			
Connection					
Server: ISQL-1					
Connection: VDILAB-XD\administrator					
View connection properties					
Progress					
Ready					
			Add	Remo	ve
			OK	Can	ool
			UK	Lan	201

- 7. Provide the FQDN of the license server.
- 8. Click Connect to validate and retrieve any licenses from the server.

If no licenses are available, you can use the 30-day free trial or activate a license file.

9.	Select the	appropriate	product	edition	using the	e license	radio button.

#### 10. Click Next.

Ø.

Studio	Licensing	
	License server address:	Connect
<ul> <li>Introduction</li> </ul>		Connected to trusted serve View certificat
✓ Databases	I want to:	
Licensing Connection Network Additional Features	<ul> <li>Use the free 30-day trial</li> <li>You can add a license later.</li> <li>Use an existing license</li> <li>The product list below is generated by</li> </ul>	the license server.
	Product	Model
Summary	Oitrix XenDesktop Platinum	User/Device
	Citrix XenApp Platinum	Concurrent
	Allocate and download Browse for I	icense file

- 11. Select the Connection type of System Center Virtual Machine Manager.
- 12. Enter the FQDN of the SCVMM server (in Server\_FQDN/sdk format).
- 13. Enter the username (in domain\username format) for the Hyper-V account.
- 14. Provide the password for the Domain Admin account.
- 15. Provide a connection name.
- 16. Select the Other tools radio button.

Studio	Connection	
	Select a Connection type. If m hardware), select 'No machine	achine management is not used (for example when using physical e management."
V Introduction	Connection type:	Microsoft® System Center Virtual Machine Mana *
<ul> <li>✓ Databases</li> <li>✓ Licensing</li> </ul>	Connection address:	10.10.31.23
Connection	User name:	administrator
Storage Management	Password:	•••••
Storage Selection	Connection name:	SCVMM
Additional Features Summary	Create virtual machines using Studio tools (Machine Select this option whe Other tools	
		Back Next Cancel

- 17. Click Next.
- 18. Select HyperFlex Cluster that will be used by this connection.
- 19. Check Studio Tools radio button required to support desktop provisioning task by this connection.
- 20. Click Next.

Studio Introduction Databases Licensing Connection Storage Management Storage Selection Network Additional Features	Storage Management Configure virtual machine storage resources for t Select a cluster: HX-21B-CTX1 Select an optimization method for available site OUse storage shared by hypervisors Optimize temporary data on available local storage Use storage local to the hypervisor Manage personal data centrally on shared storage	Browse
Summary		Back Next Cancel

21. Make Storage selection to be used by this connection.

22. Click Next.

Studio	Storage Selectio	n		
Introduction	device; machine of	perating system data, perso	the type of data to store on onal user data, and if not sto nust be selected for each dat	ring temporary data
Databases	Select data storage	locations:		
Licensing	Name	♣ OS	Personal vDisk	Temporary
Connection	\\hxhv1cip.hxhvd	om.local\Infr 🗹	<b>V</b>	2
Storage Management				
Storage Selection				
Network				
Additional Features				
Summary				
				6
				12

23. Make Network selection to be used by this connection.

#### 24. Click Next.

Studio			
✓ Introduction	HV-3		
✔ Databases ✔ Licensing		esources name helps identify this storage and network combination in Studio. e or more networks for the virtual machines to use:	
Connection Storage Management Storage Selection Network Additional Features Summary		Name vswitch-hx-inband-mgmt vswitch-hx-storage-data vswitch-hx-vm-network	4

- 25. Select Additional features.
- 26. Click Next.

Studio	ional Features e following features to customize your Site. You can also enable/disable and configure
	es later.
<ul> <li>Introduction</li> <li>Databases</li> <li>Licensing</li> </ul>	Feature AppDNA Enable this feature to allow analysis of applications and operating systems, review compatibility issues, and take remedial actions to resolve them.
<ul> <li>✓ Connection</li> <li>✓ Storage Management</li> <li>✓ Storage Selection</li> </ul>	App-V Publishing Enable this feature if you will use applications from packages on App-V servers. If you will use only applications from App-V packages on network share locations, you do not need to enable this feature.
<ul> <li>Network</li> <li>Additional Features</li> <li>Summary</li> </ul>	

27. Review Site configuration Summary and click Finish.

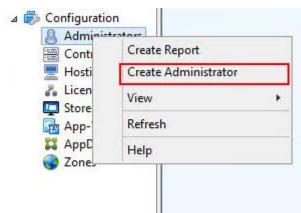
Studio	Summary		
	Site name:	HX-HV	<b>^</b>
<ul> <li>Introduction</li> </ul>	Site database:	CitrixHX-HVSite SQL1 (no high availability)	
🖉 Databases		SQLT (no high availability)	
Licensing	Monitoring database:	CitrixHX-HVMonitoring	
Connection		SQL1 (no high availability)	
Storage Management	Logging database:	CitrixHX-HVLogging	
Storage Selection		SQL1 (no high availability)	.0
<ul> <li>Network</li> </ul>	Delivery Controllers:	XDC1.hxhvdom.local	
Additional Features	License server:	ANY:27000	
Summary	Connection type:	Microsoft® System Center Virtual Machine Manager	
	Connection address:	10.10.31.23	
	Connection name:	SCVMM	
	Create virtual machines with:	Studio tools (Machine Creation Services)	
	Networks:	vswitch-hx-vm-network	
	Virtual machine OS storage:	\\hxhv1cip.hxhvdom.local\Infra on	+

# Configure the XenDesktop Site Administrators

To configure the XenDesktop site administrators, complete the following steps:

1. Connect to the XenDesktop server and open Citrix Studio Management console.

2. From the Configuration menu, right-click Administrator and select Create Administrator from the drop-down list.



3. Select/Create appropriate scope and click Next.

Studio	Administrator and Scope		
	Select an administrator:		
	VDILAB-XD\Domain Admins	Browse	
Administrator and Scope	Select a Scope:		
Role	Scopes are objects that represent something		
Summary	administrator is allowed to manage (for exan team). Click a scope to see the objects in it.	nple, a set of Delivery Groups used by the F	inance
	Scope name		_
	All		
	All objects		
	Create scope		

4. Choose an appropriate Role.

Studio	Role		
	Select	a role. Click a role name to view its permissions.	
Administrator and Scope		Name 4	Туре
Role	0	Delivery Group Administrator Can deliver applications, desktops, and machines; can also manage the	Built In
Summary	۰	Full Administrator Can perform all tasks and operations.	Built In
	0	Help Desk Administrator Can view Delivery Groups, and manage the sessions and machines ass	Built In
	0	Host Administrator Can manage host connections and their associated resource settings.	Built In
	٢	Machine Catalog Administrator Can create and manage Machine Catalogs and provision machines.	Built In
		Read Only Administrator Can see all objects in specified scopes as well as global information, b	Built In

5. Review the Summary, check Enable administrator, and click Finish.

Studio	Summary	
Administrator and Scope	Administrator: Scope: Role:	VDILAB-XD\Domain Admins All Full Administrator
♥ Role Summary		
	Enable administrator	
	Clear check box to dis Save full permissions rep	able the administrator. No settings will be lost.

# Configure Additional XenDesktop Controller

After the first controller is completely configured and the Site is operational, you can add additional controllers.



In this CVD, we created two Delivery Controllers.

To configure additional XenDesktop controllers, complete the following steps:

- 1. To begin the installation of the second Delivery Controller, connect to the second XenDesktop server and launch the installer from the Citrix XenDesktop 7.16 ISO.
- 2. Click Start.

Deliver applications and desktops to any user, anywhere, on any device. • Hybrid cloud, cloud and enterprise provisioning. • Centralized and flexible management Manage your delivery according to your needs: Manage your deliver applications Manage Deliver applications and desktops Start Cancel	
citrix	

3. Click Delivery Controller.

		Prepare Machin	Prepare Machines and Images			
Delivery Controller		Virtual Delive	Virtual Delivery Agent for Windows Server OS			
Modify or remove Delivery Controller component		ents. Install this age based VMs or		eliver applications and desktops from s al machines.	erver-	
Extend Deployment		Citrix Studio		Self-Service Password Reset	6	
				Sen-Service Password Reset		
Citrix Director						
Citrix License Server Already Installed		Universal Print Server		Session Recording		

- 4. Repeat the same steps used to install the first Delivery Controller, including the step of importing an SSL certificate for HTTPS between the controller and Hyper-V.
- 5. Review the Summary configuration.
- 6. Click Install.

XenDesktop 7.16	Summary	
Licensing Agreement	Review the prerequisites and confirm the components you want to install.	
<ul> <li>✓ Core Components</li> <li>✓ Features</li> <li>✓ Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	Installation directory C:\Program Files\Citrix Prerequisites Microsoft Visual x64 C++ 2015 Runtime Local Host Cache Storage (LocalD8) Microsoft Visual x86 C++ 2015 Runtime Microsoft SQL CLR Types (x86) Microsoft SQL OLB; Types (x64) Microsoft SQL CLR Types (x64) Microsoft SMO Objects (x86) Microsoft SMO Objects (x64) Microsoft Internet Information Services Windows Remote Assistance Feature Core Components	
	Delivery Controller Studio Director Features Back Install	Cancel

7. (Optional) Click the "I want to participate in Call Home."

#### 8. Click Next.

XenDesktop 7.16	Smart Tools
<ul> <li>Licensing Agreement</li> <li>Core Components</li> </ul>	Automate deployment tasks, health checks, and power management on-premises and in the cloud.
<ul> <li>✓ Features</li> <li>✓ Firewall</li> </ul>	Smart Check Run health checks and turn on Call Home to diagnose issues and find recommended fixes. Learn more about Call Home
✓ Summary ✓ Install	지, Smart Scale 그다. Keep your cloud Site costs under control with smart power management for VMs.
Smart Tools Finish	Simplify migrate Simplify migration to the latest XenApp and XenDesktop versions.  Smart Build Quickly build sites on-premises and in the cloud using ready-made or custom blueprint I want to connect to Smart Tools and Call Home. (Recommended) I want to connect to only Call Home. I do not want to connect to Smart Tools or Call Home You will need Citrix Cloud or citrix.com credentials. View your privacy policy here. Connect
	Next

- 9. Verify the components installed successfully.
- 10. Click Finish.

Licensing Agreement               The installation completed successfully. <ul> <li>Succession</li> <li>Features</li> <li>Microsoft Visual x64 C++ 2015 Runtime             <ul> <li>Local Host Cache Storage (LocalDB)</li> <li>Installed</li> <li>Local Host Cache Storage (LocalDB)</li> <li>Installed</li> <li>Microsoft Visual x86 C++ 2015 Runtime</li> <li>Installed</li> <li>Microsoft SQL CLR Types (x86)</li> <li>Installed</li> <li>Microsoft SNO Objects (x86)</li> <li>Installed</li> <li>Microsoft SQL CLR Types (x64)</li> <li>Installed</li> <li>Microsoft SNO Objects (x64)</li> <li>Installed</li> <li>Windows Remote Assistance Feature</li> <li>Installed</li> <li>Delivery Contoller</li> <li>Installed</li> <li>Director</li> <li>Installed</li> <li>Director</li> <li>Installed</li> <li>Orreponent Initialization</li> <li>Initialized</li> </ul> </li> </ul>	XenDesktop 7.16	Finish Installation	
Prerequisites       Prerequisites	✓ Licensing Agreement	The installation completed successfully.	Succes
	<ul> <li>✓ Features</li> <li>✓ Firewall</li> <li>✓ Summary</li> <li>✓ Install</li> <li>✓ Smart Tools</li> </ul>	<ul> <li>Microsoft Visual x64 C++ 2015 Runtime</li> <li>Local Host Cache Storage (LocalDB)</li> <li>Microsoft Visual x86 C++ 2015 Runtime</li> <li>Microsoft SQL CLR Types (x86)</li> <li>Microsoft SQL CLR Types (x64)</li> <li>Microsoft SQL CLR Types (x64)</li> <li>Microsoft SMO Objects (x64)</li> <li>Microsoft Internet Information Services</li> <li>Windows Remote Assistance Feature</li> <li>Core Components</li> <li>Delivery Controller</li> <li>Studio</li> <li>Director</li> <li>Post Install</li> </ul>	Installed Installed Installed Installed Installed Installed Installed Installed Installed Installed
Launch Studio		Launch Studio	

## Add the Second Delivery Controller to the XenDesktop Site

To add the second Delivery Controller to the XenDesktop Site, complete the following steps:

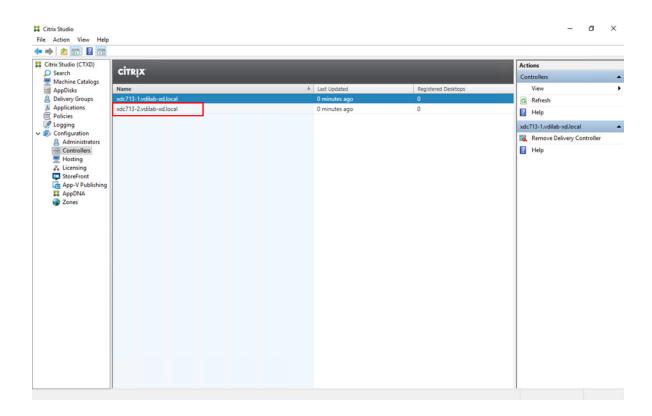
1. In Desktop Studio click the "Connect this Delivery Controller to an existing Site" button.

CITRIX	
Welcome	
Welcome to Citrix Studio To begin, select one of the three options below.	
Site setup	
Deliver applications and desktops to your users	
Remote PC Access	
Enable your users to remotely access their physical machines	
Scale your deployment	
Connect this Delivery Controller to an existing Site	

- 2. Enter the FQDN of the first delivery controller.
- 3. Click OK.

ect Site		
Specify the address of a Delivery Contr	oller in the Sit	e you wish to
join		
xdc713-1.vdilab-xd.loca		
Example: deliverycontroller.example.com		
	r	Cancel

- 4. Click Yes to allow the database to be updated with this controller's information automatically.
- 5. When complete, test the site configuration and verify the Delivery Controller has been added to the list of Controllers.



### Install and Configure StoreFront

Citrix StoreFront stores aggregate desktops and applications from XenDesktop sites, making resources readily available to users.

In this CVD, we created two StoreFront servers on dedicated virtual machines.

To install and configure StoreFront, complete the following steps:

- 1. To begin the installation of the StoreFront, connect to the first StoreFront server and launch the installer from the Citrix XenDesktop 7.16 ISO.
- 2. Click Start.

ø



3. Click Extend Deployment Citrix StoreFront.

	Prepare Machi	Prepare Machines and Images			
Delivery Controller		Virtual Delive	Virtual Delivery Agent for Windows Server OS		
Modify or remove Delivery Con	troller compor	ents. Install this age based VMs or		eliver applications and desktops from s al machines.	erver-
Extend Deployment					
		Charles Charles		Call Cardina December 1 Decemb	
Citrix Director		Citrix Studio Already Installed		Self-Service Password Reset	0
Citrix Director Already Installed Citrix License Server				Self-Service Password Reset Session Recording	4

- 4. If acceptable, indicate your acceptance of the license by selecting the "I have read, understand, and accept the terms of the license agreement" radio button.
- 5. Click Next.

### Build the Virtual Machines and Environment for Workload Testing

XenDesktop 7.16	Software License Agreement
Licensing Agreement	Printable vers
Core Components Firewall Summary Install	CITRIX LICENSE AGREEMENT This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix.providing-entities.html. BY
Smart Tools Finish	identified at https://www.citrix.com/butylicensing/citrix.providing-entities.html. BY INSTALLING AND/OR USING THE PRODUCT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT. 1. PRODUCT LICENSES.
	a. End User Licenses. The software in a software PRODUCT and the software installed in an appliance PRODUCT is made available by CITRIX under the license models identified at http://www.citrix.com/buy/licensing/ product.html. Any experimental features delivered with such software will be identified and are licensed only for internal testing purposes. "Software" means a Citrix proprietary and/or open source software program in object code form licensed hereunder. "Appliance" means a hardware appliance with installed Software. Nativitational availation configuration of the first order form
	I have read, understand, and accept the terms of the license agreement I do not accept the terms of the license agreement
	Back

### 6. Click Next.

Licensing Agreement Core Components Firewall Summary Install Smart Tools Finish	For scale and performance reasons, it is recommended that Director and the License Server be installed on separate servers. StoreFront (Required) Provides authentication and resource delivery services for Citrix Receiver, enabling yo to create centralized enterprise stores to deliver applications, desktops, and other resources to users on any device, anywhere.
Summary Install Smart Tools	Provides authentication and resource delivery services for Citrix Receiver, enabling yo to create centralized enterprise stores to deliver applications, desktops, and other

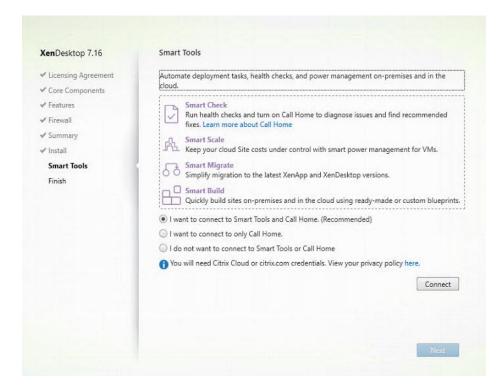
- 7. Select the default ports and automatically configured firewall rules.
- 8. Click Next.

XenDesktop 7.16	Firewall	
<ul> <li>✓ Licensing Agreement</li> <li>✓ Core Components</li> <li>Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	The default ports are listed below. StoreFront 80 TCP 443 TCP	Printable version
	Configure firewall rules: Automatically Select this option to automatically create the rules in the created even if the Windows Firewall is turned off.	Windows Firewall. The rules will be

9. Click Install.

XenDesktop 7.16	Summary
<ul> <li>Licensing Agreement</li> <li>Core Components</li> <li>Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	Review the prerequisites and confirm the components you want to install.  Installation directory C:\Program Files\Citrix Core Components StoreFront Firewall TCP Ports: 80, 443
	Back

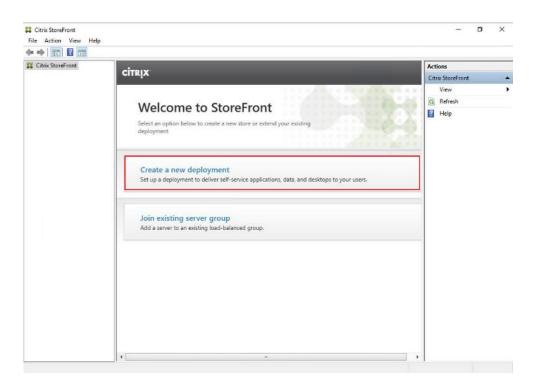
- 10. (Optional) Click "I want to participate in Call Home."
- 11. Click Next.



- 12. Check "Open the StoreFront Management Console."
- 13. Click Finish.

XenDesktop 7.16	Finish Installation	
<ul> <li>Licensing Agreement</li> <li>Core Components</li> <li>Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	The installation completed successfully. Core Components StoreFront Post Install Component Initialization	✓ Success Installed Initialized
	✔ Open the StoreFront Management Console	Finish

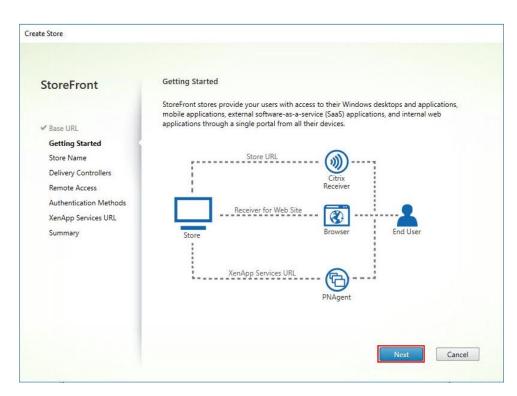
14. Click Create a new deployment.



15. Specify the URL of the StoreFront server and click Next.

New Deployment	
StoreFront	Enter a Base URL Confirm the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.
Base URL Getting Started Store Name Delivery Controllers Remote Access Authentication Methods XenApp Services URL Summary	Base URL http://sf-713-1/
	Next Cancel

16. Click Next.



17. Specify a name for your store and click Next.

ite Store	
StoreFront	Store name and access
	Enter a name that helps users identify the store. The store name appears in Citrix Receiver as part of the user's account.
✓ Base URL	
✓ Getting Started	Store name and access type cannot be changed, once the store is created.
Store Name	
Delivery Controllers	Store Name: hxdesktop
Remote Access	
Authentication Methods	Allow only unauthenticated (anonymous) users to access this store Unauthenticated users can access the store without presenting credentials.
XenApp Services URL	onderenteded daes en deess the store motore presenting creatings
Summary	Receiver for Web Site Settings
	Set this Receiver for Web site as IIS default
	When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.
	Back Next Cancel

18. Add the required Delivery Controllers to the store and click Next.

StoreFront	Delivery Controller		
Base URL		op delivery controllers, XenApp servers ar e. Citrix recommends grouping delivery c	
Getting Started	Name	Туре	Servers
✓ Store Name	НХ	XenDesktop	XD-713-1.vdilab-x
Delivery Controllers			
Remote Access			
Authentication Methods			
XenApp Services URL			
Summary			
Summary	Add Ed	it Remove	

19. Specify how connecting users can access the resources, in this environment only local users on the internal network are able to access the store, and click Next.

StoreFront	Remote Access
	Enabling remote access will allow users outside the firewall to access resources securely. You need to add a NetScaler Gateway once remote access is enabled.
Base URL Getting Started	Enable Remote Access
/ Store Name	Select the permitted level of access to internal resources
Delivery Controllers	Allow users to access only resources delivered through StoreFront (No VPN tunnel)
Remote Access Authentication Methods	Allow users to access all resources on the internal network (Full VPN tunnel) Users may require the NetScaler Gateway Plug-in to establish a full VPN tunnel.
XenApp Services URL Summary	NetScaler Gateway appliances:
	Add
	Default appliance:

20. On the "Authentication Methods" page, select the methods your users will use to authenticate to the store and click Next. You can select from the following methods:

Select the methods which users will use to authenticate and access resources.	0
Method	
✓ User name and password	<u> </u>
Land	
	-
Can be enabled / disabled separately on Receiver for Web sites	
HTTP Basic	
Pass-through from NetScaler Gateway	•
	User name and password     SAML Authentication     Omain pass-through     Can be enabled / disabled separately on Receiver for Web sites     Smart card     Can be enabled / disabled separately on Receiver for Web sites     HTTP Basic

- 21. Username and password: Users enter their credentials and are authenticated when they access their stores.
- 22. Domain pass-through: Users authenticate to their domain-joined Windows computers and their credentials are used to log them on automatically when they access their stores.
- 23. Configure the XenApp Service URL for users who use PNAgent to access the applications and desktops and click Create.

StoreFront	Configure XenApp Services URL
	URL for users who use PNAgent to access applications and desktops.
Base URL	Enable XenApp Services URL
Getting Started	URL: http://sf-713-1/Citrix/hxdesktop/PNAgent/config.xml
✔ Store Name	
Delivery Controllers	Make this the default Store for PNAgent
Remote Access	PNAgent will use this store to deliver resources.
Authentication Methods	
XenApp Services URL	
Summary	

24. After creating the store click Finish.

Store created successfully
Store Name: hxdesktop
Remote Access: Disabled
Authentication Methods: User name and password, Domain pass-through
Store URL Export Provisioning File
Citrix Receiver
Receiver for Web Site
Store Browser
XenApp Services URL
PNAgent

## Additional StoreFront Configuration

After the first StoreFront server is completely configured and the Store is operational, you can add additional servers.

To configure additional StoreFront server, complete the following steps:

- 1. To begin the installation of the second StoreFront, connect to the second StoreFront server and launch the installer from the Citrix XenDesktop 7.16 ISO.
- 2. Click Start.

Deliver applications and desktops to any user on any device. • Hybrid cloud, cloud and enterprise provisioning • Centralized and flexible management Manage your delivery according to your needs:	r, anywhere,
	Start
XenDesktop Deliver applications and desktops	Start
	Cancel
сіткіх	

3. Click Extended Deployment Citrix StoreFront.

		Prepare Machin	nes and	l Images	
Delivery Controller		Virtual Delive	ery Ag	ent for Windows Server OS	
Madify or remove Delivery Cor	ntroller compon	ents. Install this age based VMs or		eliver applications and desktops from s al machines.	erver-
Extend Deployment		Citrix Studio		Self-Service Password Reset	
Citrix Director Already Installed		Already Installed		Self-Service Password Reset	
Aneady instaned					
Citrix License Server		Universal Print Server		Session Recording	
		Federated Authentication Service			

- 4. Repeat the same steps used to install the first StoreFront.
- 5. Review the Summary configuration.
- 6. Click Install.

XenDesktop 7.16	Summary Review the prerequisites and confirm the components you want to install.
<ul> <li>✓ Core Components</li> <li>✓ Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	Installation directory CAProgram Files/Citrix Core Components StoreFront Firewall TCP Ports: 80, 443

- 7. (Optional) Click "I want to participate in Call Home."
- 8. Click Next.

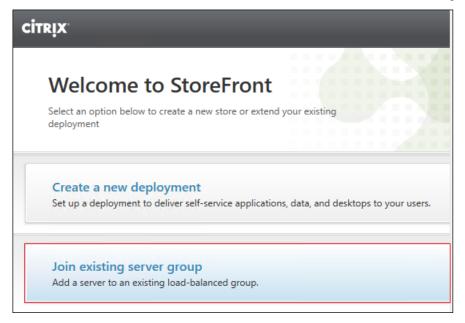
KenDesktop 7.16	Smart Tools
Licensing Agreement	Automate deployment tasks, health checks, and power management on-premises and in the cloud.
Core Components Features Firewall Summary Install	Smart Check Run health checks and turn on Call Home to diagnose issues and find recommended fixes. Learn more about Call Home Smart Scale Keep your cloud Site costs under control with smart power management for VMs.
Smart Tools Finish	Simplify migration to the latest XenApp and XenDesktop versions.  Simplify migration to the latest XenApp and XenDesktop versions.  Simplify migration to the latest XenApp and XenDesktop versions.  Simplify migration to the latest XenApp and XenDesktop versions.  Name of the second secon
	Connect

- 9. Check "Open the StoreFront Management Console."
- 10. Click Finish.

XenDesktop 7.16	Finish Installation	
<ul> <li>Licensing Agreement</li> <li>Core Components</li> </ul>	The installation completed successfully.	<ul> <li>Succes</li> </ul>
✔ Firewall	Core Components  StoreFront	Installed
🖌 Summary 🖌 Install	Post Install Component Initialization	Initialized
✔ Smart Tools		

To configure the second StoreFront if used, complete the following steps:

1. From the StoreFront Console on the second server select "Join existing server group."



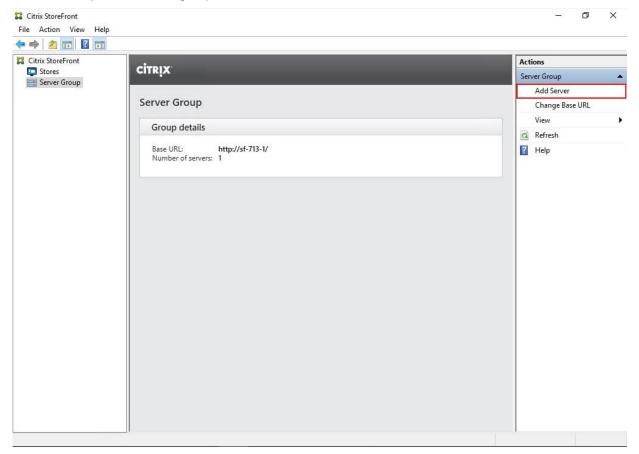
2. In the Join Server Group dialog, enter the name of the first Storefront server.

To authorize this sen	ver first connect t	o a server in th	e group and cho	ose "Add
Server". Enter the pr				USC AUU
Authorizing server:	sf-713-1			
Authorization code:				

- 3. Before the additional StoreFront server can join the server group, you must connect to the first Storefront server, add the second server, and obtain the required authorization information.
- 4. Connect to the first StoreFront server.
- 5. Using the StoreFront menu on the left, you can scroll through the StoreFront management options.
- 6. Select Server Group from the menu.



7. To add the second server and generate the authorization information that allows the additional StoreFront server to join the server group, select Add Server.



8. Copy the Authorization code from the Add Server dialog.

Add Server	
Authorize New Server	
Enter authorization information for the server you want to add.	
Authorizing server: SF-713-1 Authorization code: 95671399	
Please wait	
	Cancel

- 9. Connect to the second Storefront server and paste the Authorization code into the Join Server Group dialog.
- 10. Click Join.

in Server Group				
To authorize this serv Server". Enter the pro	and the second sec	-		e "Add
Authorizing server:	sf-713-1			
Authorization code:	95671399			
			Join	Cancel

- 11. A message appears when the second server has joined successfully.
- 12. Click OK.



The second StoreFront is now in the Server Group.

### Install the Citrix Provisioning Services Target Device Software

For non-persistent Windows 10 virtual desktops and Server 2016 XenApp virtual machines, Citrix Provisioning Services (PVS) is used for deployment. The Master Target Device refers to the target device from which a hard disk image is built and stored on a vDisk. Provisioning Services then streams the contents of the vDisk created to

other target devices. This procedure installs the PVS Target Device software that is used to build the RDS and VDI golden images.

To install the Citrix Provisioning Server Target Device software, complete the following steps:

The instructions below outline the installation procedure to configure a vDisk for VDI desktops. When you have completed these installation steps, repeat the procedure to configure a vDisk for RDS.

- 1. On the Window 10 Master Target Device, launch the PVS installer from the Provisioning Services 7.16 ISO.
- 2. Click the Target Device Installation button.

-		
G	Console Installation	
0	Server Installation	
	Target Device Installation	
	Help and Support	
	Browse DVD	<b>Exit</b>
Inst	call the Console.	EXIL
_		

The installation wizard will check to resolve dependencies and then begin the PVS target device installation process.

3. Click Next.



- 4. Confirm the installation settings and click **Install**.
- 5. Deselect the checkbox to launch the Imaging Wizard and click Finish.

Installation Wizard Completed
The Installation Wizard has successfully installed Citrix Provisioning Services Target Device. Click Finish to exit the wizard.
🔲 Launch Imaging Wizard

6. Reboot the machine.

### Create Citrix Provisioning Services vDisks

The PVS Imaging Wizard automatically creates a base vDisk image from the master target device. To create the Citrix Provisioning Server vDisks, complete the following steps:

The instructions below describe the process of creating a vDisk for VDI desktops. When you have completed these steps, repeat the procedure to build a vDisk for RDS.

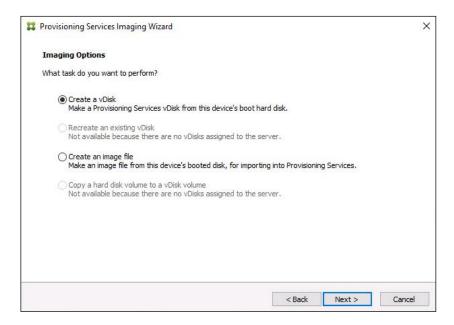
- 1. The PVS Imaging Wizard's Welcome page appears.
- 2. Click Next.

Contract Provisioning Services Image	aging Wizard	×
CITRIX	Welcome to the Imaging Wizard	
	The Imaging Wizard automates the process of imaging the boot and additional partitions into a virtual disk.	
	The Imaging Wizard can image from a vDisk to the boot hard disk for upgrades and back to the vDisk.	
	The Imaging Wizard supports imaging a single hard disk volume to a vDisk volume.	
	< Back Next > Cancel	

- 3. The **Connect to Farm** page appears. Enter the name or IP address of a Provisioning Server within the farm to connect to and the port to use to make that connection.
- 4. Use the Windows credentials (default) or enter different credentials.
- 5. Click Next.

Enter the Provisioning Services site server name or IP, port, and credentials. Only stores supported by this server will be available for vDisk assignment. Enter Server Details Server name or IP: CTX-PVS1.vdilab-v.local Port: 54321 • Provide Logon Credentials for the Server	
Server name or IP: CTX-PVS1.vdilab-v.local Port: 54321   Provide Logon Credentials for the Server  © Use my Windows credentials	
Port: 54321  Provide Logon Credentials for the Server © Use my Windows credentials	
Provide Logon Credentials for the Server      O Use my Windows credentials	
Provide Logon Credentials for the Server      O Use my Windows credentials	
Use my Windows credentials	
O Use these credentials	
User name:	
Domain:	
Password:	

- 6. Select Create new vDisk.
- 7. Click Next.



- 8. The Add Target Device page appears.
- Select the Target Device Name, the MAC address associated with one of the NICs that was selected when the target device software was installed on the master target device, and the Collection to which you are adding the device.
- 10. Click Next.

	ember of the site and needs to be added.	
Target device name:	Win10-TD	
	Must be different from the current machine name.	
Network connection:	Ethernet0, 10.10.208.100, 00-50-56-AE-53-7B	~
	Select the connection that will be used to boot this machine to the server.	
Collection name:	Collection	~
	Select the site collection that this device will be added to.	

- 11. The New vDisk dialog displays. Enter the name of the vDisk.
- 12. Select the **Store** where the vDisk will reside. Select the **vDisk type**, either Fixed or Dynamic, from the dropdown menu. (This CVD used Dynamic rather than Fixed vDisks.)
- 13. Click Next.

New vDisk			
New VDISK			
The new vDisk wi	I be created in the store you select.		
vDisk name:	Win 10-vDisk		
Store name:	Store - 949.67 GB Free		~
blare Hamer	Supported by Server: CTX-PVS1		
vDisk type:	Dynamic (recommended)		~
VHDX			

- 14. On the **Microsoft Volume Licensing** page, select the volume license option to use for target devices. For this CVD, volume licensing is not used, so the None button is selected.
- 15. Click Next.

22 Provisioning Services Imaging Wizard	×
Microsoft Volume Licensing Choose whether the vDisk is to be configured for Microsoft KMS or MAK volume license management.	
None	
◯ Key Management Service (KMS)	
O Multiple Activation Key (MAK)	
< Back Next > Cancel	

- 16. Select Image entire boot disk on the Configure Image Volumes page.
- 17. Click Next.

Provisioning Services Imaging Wizard			>
What to Image			
Choose what to image.			
Image entire boot disk			
$\bigcirc$ Choose partitions to image and optionally increase volume	size		
	< Back	Next >	Cancel

- 18. Select Optimize for hard disk again for Provisioning Services before imaging on the Optimize Hard Disk for Provisioning Services.
- 19. Click Next.

Contract Provisioning Services Imaging Wizard			×
Optimize Hard Disk for Provisioning Services			
The hard disk has already been optimized for Provisioning Services. Do you want to optimize the disk again?			
◯ Do not optimize the hard disk again			
Optimize the hard disk again for Provisioning Services before im	naging		
Edit Optimization Settings			
Note: Citrix recommends that partitions be defragmented before imagin	ng.		
	< Back	Next >	Cancel

20. Select Create on the Summary page.

Summary	
Confirm that all settings are correct.	
Constant to City Constant CTV DVC1 with the share Depth D4221	
Connect to Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 Task: Create a vDisk	
Target device name : Win 10-TD	
Network connection : Ethernet0, 10.10.208.100, 00-50-56-AE-53 Collection: Collection	3-78
vDisk name: Win10-vDisk	
Store: Store	
Format: VHDX, type: Dynamic (recommended), sector size: 512 B, Image entire boot disk	, block size: 32 MB
Optimize hard disk for Provisioning Services prior to imaging	
<	>
Status: Ready to Start	
Progress:	
rogress:	

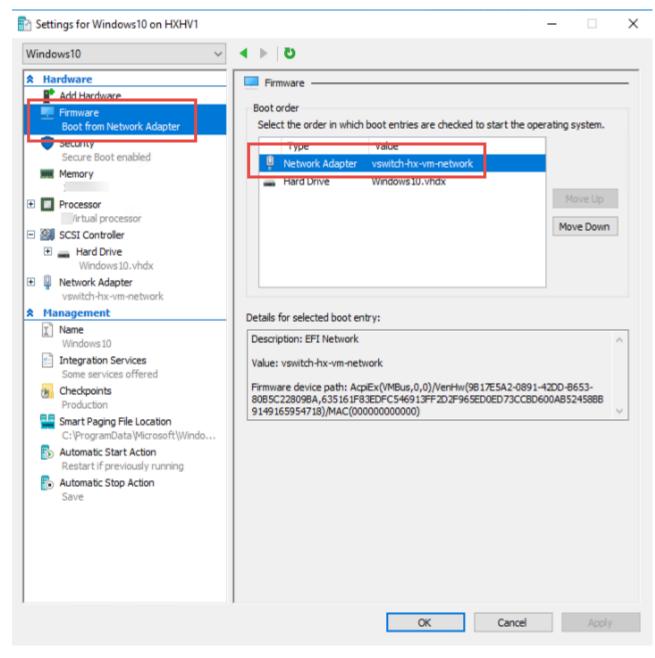
## 21. Review the configuration and click **Continue.**

Restart Ne	eded	
	e restart, configure the machine settings for network boot. restart, the Imaging Wizard will continue.	
Task: Crea Target dev Network co Collection: vDisk name Store: Stor Format: VH Image enti	ce name : Win10-TD nnection : Ethernet0, 10.10.208.100,00-50-56-AE-53-78 Collection : Win10-VDisk	2 MB
<		>
Status:	Successful!	

22. When prompted, click No to shut down the machine.

Reboot o	r Shut Down, and S	et Network Boot		×
?			f not, the device will onfigure the machine	
		Yes	No	Cancel

23. Edit the VM settings and select **Boot from Network Adapter** under Boot Order.



24. Restart Virtual Machine.

After restarting the VM, log into the VDI or RDS master target. The PVS imaging process begins, copying the contents of the C: drive to the PVS vDisk located on the server.

25. If prompted to Restart select Restart Later.

Processing	
Imaging is likely to take a long time.	
Connect to Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 Task: Image created vDisk Existing vDisk: Store\Win10-vDisk	^
<	•
< Status: Copying C:	× >
	>
Status: Copying C:	~

26. A message is displayed when the conversion is complete, click **Done**.

The lass of		
The log of t	the processing done can be viewed by clicking the Log button.	
Task: Ima	o Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 ge created vDisk Disk: Store\Win10-vDisk	~
<		3
< Status:	Successful!	>

- 27. Shutdown the VM used as the VDI or RDS master target.
- 28. Connect to the PVS server and validate that the vDisk image is available in the Store.
- 29. Right-click the newly created vDisk and select Properties.

a		Provisioning Servi	ces Console	
<ul> <li>File Action View Window Help</li> <li>File Action View Window Help</li> <li>File Action View Window Help</li> <li>File Provisioning Services Console</li> <li>Farm (localhost)</li> <li>Sites</li> <li>Sites</li> <li>Site</li> <li>Site</li> <li>View Site</li> <li>Povice Collections</li> <li>Views</li> <li>Hosts</li> <li>News</li> <li>Stores</li> </ul>	Name	Provisioning Servi Site Site Properties Versions Load Balancing Replication Status Mount vDisk Show Usage Manage Locks Unassign from Set	Connections 0	Size 32.767 MB
store		Copy vDisk Prope Export vDisk Audit Trail Copy Delete Refresh Help	rties	

- 30. On the vDisk Properties dialog, change Access mode to "Standard Image (multi-device, read-only access)".
- 31. Set the Cache Type to "Cache in device RAM with overflow on hard disk."
- 32. Set Maximum RAM size (MBs): 256 for VDI and set 1024 MB for RDS vDisk.

		vDisk Propert	ies	x
General	Identification	Microsoft Volume Licensing	Auto Update	
Site	: Site			
Stor	e: Store			
Filer	name: Win10	-vDisk		
	: 32,76	7 MB Block size:	32,768 KB	
		ndard Image (multi-device, rea	ad-only access)	~
Cac	he type: Cao	che in device RAM with overfl	ow on hard disk	~
Max	imum RAM size	(MBs): 64		
BIO	S boot menu te	¢ (optional):		
	Enable Active I Enable printer r Enable streamir	-	ssword management	
		ОК	Cancel	Help

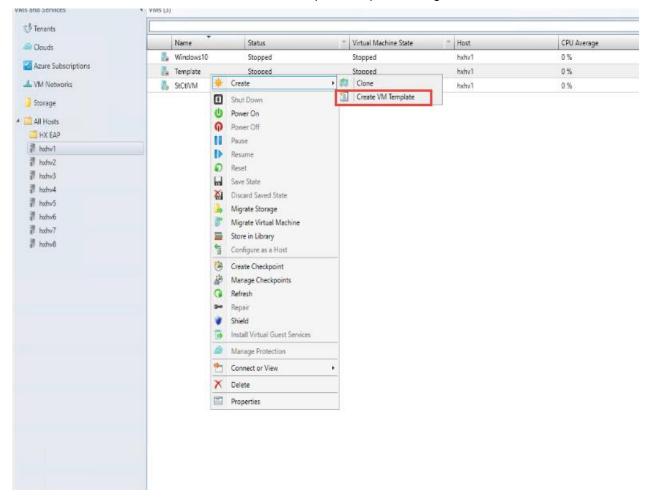
33. Click OK.

Repeat this procedure to create vDisks for both the Hosted VDI Desktops (using the Windows 10 OS image) and the Hosted Shared Desktops (using the Windows Server 2016 image).

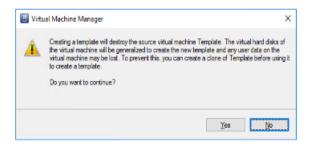
#### **Provision Virtual Desktop Machines**

To create VDI and RDS machines, complete the following steps:

- 1. Select the Master Target Device VM from the SCVMM Client.
- 2. Right-click the VM and select Create -> Create VM Template.
- 3. Name the cloned 'Template'.
- 4. Select the cluster and datastore where the first phase of provisioning will occur.



5. Click Yes to the warning that your machine will be destroyed by the Template process.



🔠 Create VM Template Wiza	ard X
Identity	
Identity	VM Template Identity
Configure Hardware Configure Operating Select Library Server Select Path Summary	VM Template name:     Windows_Template       Description:
	Previous Next Cancel

6. Click Next.

Configure	Operating System		
dentity Configure Hardware		k settings, and scripts for the new virtual machine. est OS profile or save a new profile based on your s	
onfigure Operating	Guest OS profile: [None - custom	ization not required]	٧
elect Library Server	H Save As		
elect Path	A General Settings		
	🔎 Operating System	Specify the operating system of the virtual machine.	
ummary	Windows Server Standar	Operating system:	
	ldentity Information	Windows Server Standard Version 1709	×.
	Admin Password		
	Product Key None		
	Pacific Standard Time		
	Roles and Features		
	None None		
	None Features		
	None		
	* Networking		
	Domain / Workgroup		
	* Scripta		
	Answer File		
	None [GUIRunOnce] Comma		
	[oununonce] comma		

- 7. Under 'Configure Operating System', ensure that customization is disabled.
- 8. Click Next through the remaining screens
- 9. Click Finish to create the template
- 10. From Citrix Studio on the Desktop Controller, select Hosting and Add Connection and Resources.
- 11. Select Use an existing Connection and click Next.
- 12. Correspond the name of the resource with desktop machine clusters.

<b>#</b>			Citrix Studi	D				x
<u>File Action View H</u> elp								
🗢 🏟 🙇 🖬 🔢 📰						_		
Console Root	CITRIX					Ac	tions	
Citrix Studio (Site)	CIIRIN					н	osting	
Machine Catalogs	Name	Type	Address		State	2	Add Connection and Resources	
Belivery Groups	vSphere Connection	VMware	vS https://vcsa	1.dvpod2.local	Enabled		View	•
Policies	RDS					a	Refresh	
Logging	VDI-NP							
⊿						?	Help	
Controllers						vS	Sphere Connection	
Hosting							Edit Connection	
🔏 Licensing						1	Turn On Maintenance Mode	
StoreFront								
👍 App-V Publishi 🥥 Zones	Details - vSphere Conne	ction						
D Citrix StoreFront	Details Administrators							
	Connection						Test Connection	
	Name:	vSphere Connect				?	Help	
		https://vcsa1.dvp						
	Username:	administrator@v						
		All						
		Primary						
		-						
< III >						-		

13. Browse and select the Hyper-V cluster for desktop provisioning and use the default storage method Use storage shared by hypervisors.

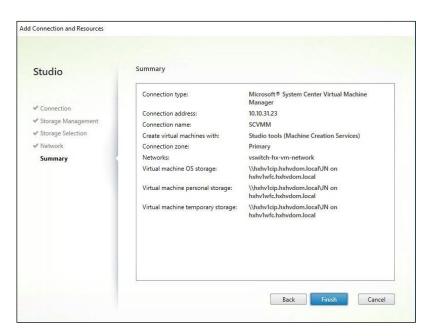
Studio Connection Storage Management Storage Selection Network Summary	Add Connect Storage Management Configure virtual mach Select a cluster: Select an optimization © Use storage sharec Optimize temp local storage Use storage local t Manage person shared storage	tion and Resources  Select a cluster  Select a cluster  VDI-DC  N Infra  VDI-DC  N Infra  N Clauncher  N RDS  VDI-NonPersistent  VDI-Persistent
	shared storage	OK Cancel

14. Select the data storage location for the corresponding resource.

Studio	Storage Selectio	n		
Connection	device; machine op	erating system data, data. At least one dev	elect the type of data to store on personal user data, and if not sto ice must be selected for each da	oring temporary data
Storage Management	Name	+ OS	Personal vDisk	Temporary
Storage Selection	\\hxhv1cip.hxhvd	om.local\JN 🗹		

15. Select the VDI networks for the desktop machines and click Next.

Studio	Network	
	Name for these resources:	
<ul> <li>✓ Connection</li> <li>✓ Storage Management</li> </ul>	Hyper-V-HX The resources name helps identify this storage and network combination i	n Studio.
✓ Storage Selection	Select one or more networks for the virtual machines to use:	
Network	Name     LiveMigrate	4
Summary	vswitch-hx-inband-mgmt	
	vswitch-hx-storage-data	
	vswitch-hx-vm-network	



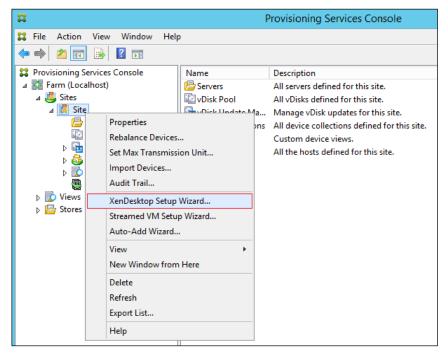
16. Click Finish.



Return to these settings to alter the datastore selection for each set of provisioned desktop machines.

## Provision Desktop Machines from Citrix Provisioning Services Console

- 1. Start the XenDesktop Setup Wizard from the Provisioning Services Console.
- 2. Right-click the Site.
- 3. Choose XenDesktop Setup Wizard... from the context menu.



4. Click Next.

- 5. Enter the XenDesktop Controller address that will be used for the wizard operations.
- 6. Click Next.

XenDesktop Setup
XenDesktop Controller Enter the address of the XenDesktop Controller you want to configure.
XenDesktop Controller address: CTX-XD1.vdilab-v.local
< Back Next > Cancel

- 7. Select the Host Resources on which the virtual machines will be created.
- 8. Click Next.

XenDesktop Setup	x
XenDesktop Host Resources Select the XenDesktop Host Resources you want to use:	22
XenDesktop Host Resources	
NonPersistent	
< <u>B</u> ack <u>N</u> ext >	<u>C</u> ancel

- 9. Provide the Host Resources Credentials (Username and Password) to the XenDesktop controller when prompted.
- 10. Click OK.

nter your c	redentials for the Xe	enDesktop Host I	Resources.
Jsemame:	hxhvdom\adminis	trator	
assword:	1		

- 11. Select the Template created earlier.
- 12. Click Next.

XenDeskt	op Setup		×
Template Select the Template you want to use:			
Select a template for the XenDesktop Host Reso	ources.		
Virtual Machine Template			
Win10-Template			
Select the VDA version installed on this template	:		
7.9 (recommended, to access the latest features	)		~
	< Back	Next >	Cancel

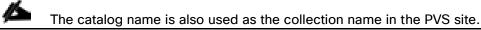
13. Select the network that will be used for the provisioned virtual machines.

XenDesktop Setup
XenDesktop Host Resources Network Select the network for Provisioning Services streaming:
Network
nnections\vSphere Connection\VDI-DC.datacenter\VDI-NonPersistent.cluster\VDI-1.network nnections\vSphere Connection\VDI-DC.datacenter\VDI-NonPersistent.cluster\VDI-2.network nnections\vSphere Connection\VDI-DC.datacenter\VDI-NonPersistent.cluster\VDI-3.network
< III >
< Back Next > Cancel

- 14. Select the vDisk that will be used to stream virtual machines.
- 15. Click Next.

XenDesktop Setup	x
<b>vDisk</b> Select an existing standard-mode vDisk.	
Standard-mode vDisk:	
Store\Win10-vDisk	
< Back Next >	Cancel

16. Select "Create a new catalog."



17. Click Next.

	XenDesktop Setup
<b>Catalog</b> Select your Ca	atalog preferences.
Oreate a new Oreate a new Use an exist	
Ca <u>t</u> alog name:	VDI-NP
Description:	NonPersistent VDI Machines
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

- 18. On the Operating System dialog, specify the operating system for the catalog. Specify Windows Desktop Operating System for VDI and Windows Server Operating System for RDS.
- 19. Click Next.

XenDesktop Setup	×
Operating System Select an operating system for this catalog.	
<ul> <li>Windows Desktop Operating System         Best for delivering personalized desktops to users, or applications from desktop         operating systems.</li> <li>Windows Server Operating System         Best for delivering applications or hosted shared desktops to users.         Note:         This infrastructure will be built using virtual machines.         Desktop images will be managed using Citrix Provisioning Services (PVS)</li> </ul>	
< <u>B</u> ack <u>N</u> ext > <u>C</u> and	:el

- 20. If you specified a Windows Desktop OS for VDIs, a User Experience dialog appears. Specify that the user will connect to "A fresh new (random) desktop each time."
- 21. Click Next.



- 22. On the Virtual machines dialog, specify:
  - a. The number of VMs to create.
  - b. Number of vCPUs for the VM (2 for VDI, 8 for RDS)
  - c. The amount of memory for the VM (4GB for VDI, 24GB for RDS)
  - d. The write-cache disk size (10GB for VDI, 30GB for RDS)
  - e. PXE boot as the Boot Mode
- 23. Click Next.

	XenDesktop Se	etup 🛛 🗙
Virtual machines Select your virtual machine pref	erences.	<b>11</b>
Number of virtual machines to	o create:	1
vCPUs:	2	2
Memory:	2048 MB	2048 🗘 MB
Local write cache disk:	6 GB	10 🗘 GB 🗌 Thick
Boot mode:		
PXE boot (requires	s a running PXE servi	ice)
O BDM disk (create	a boot device manag	per partition)
	< B	Back Next > Cancel

- 24. Select the Create new accounts radio button.
- 25. Click Next.

XenD	esktop Setup	X
Active Directory Select your computer account option.		
Create new <u>a</u> ccounts     Import existing accounts		
	< Back Next >	<u>C</u> ancel

- 26. Specify the Active Directory Accounts and Location. This is where the wizard should create the computer accounts.
- 27. Provide the Account naming scheme. An example name is shown in the text box below the name scheme selection location.
- 28. Click Next.

		XenDesktop Setup	X
	Directory account e Active Directory	unts and location v accounts.	
Active Di	rectory location fo	r computer accounts:	
Domain:	vdilab-v.local		~
_	ab-v.local LoginVSI Computers		
vdilab-v.	Launchers	omouters	~
	naming scheme:	CTX-VDINP-#### 0-9 v CTX-VDINP-001	
		< Back Next > C	ancel

29. Click Finish to begin the virtual machine creation.

Catalog name		VDI-NP	^
Catalog type		VDI PVS Random	
VDA version		7.9 (recommended, to access the latest fea	tures) ≡
XenDesktop Host Resource			
Network for VDI NonPersis	stent	x	5
Virtual machine template		Win10-Template	
Existing vDisk		Win10-vDisk	
vCPUs <	Ш	2	>
rogress			
urrent virtual machine:			
verall			

30. When the wizard is done provisioning the virtual machines, click Done.

Catalog type V VDA version 7 XenDesktop Host Resources V	/DI-NP //DI PVS Random ?.9 (recommended, //DI NonPersistent	-				
Catalog type V VDA version 7 XenDesktop Host Resources V	/DI PVS Random 7.9 (recommended,	, to acce	ess the la			^
VDA version 7 XenDesktop Host Resources V	.9 (recommended,	, to acce	ess the la			
XenDesktop Host Resources V	•	to acce	ess the la			
	/DI NonPersistent			itest featu	res)	≡
Network for VDI NonPersistent						
Virtual machine template V	Vin 10-Template					
Existing vDisk V	Vin 10-v Disk					
vCPUs 2	)					~
< 111						>
rogress urrent virtual machine: verall:						
Setup complete						
1 device created, 0 de	evice failed.					
	<	< Back	1	Vext >		Done

Provisioning process takes ~10 seconds per machine.

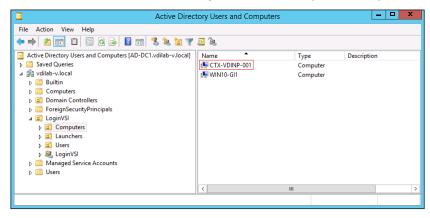
- 31. Verify the desktop machines were successfully created in the following locations:
  - a. PVS1 > Provisioning Services Console > Farm > Site > Device Collections > VDI-NP > CTX-VDI-001

#	Pro	ovisioning Service	es Console			-	D X
😫 File Action View Window Help							_ # ×
🗢 🔿 🙍 🖬 🛛 🖬							
Provisioning Services Console	Name	MAC	Туре	Disk	vDisk	IP Address	Server
⊿ 🗱 Farm (localhost)	CTX-VDINP-001	00-50-56-AE-AE-0D	Production	vDisk	Store\Win10-vDisk	Down	
🛛 😃 Sites							
⊿ 🛄 Site							
📇 Servers							
VDisk Pool							
VDisk Update Management							
a 😂 Device Collections							
Collection							
VDI-NP							
Views							
Hosts							
Views							
⊿ 📴 Stores							
Store Store							
_	1						

b. CTX-XD1 > Citrix Studio > Machine Catalogs > VDI-NP

#			Citrix Studio				_ 🗆 X
File Action View Help							
⇒ ≥ □ 2 □				_			
🗱 Citrix Studio (Site)	CITRIX					Actions	
Search Machine Catalogs	CIIRIN					Machine Catalogs	•
AppDisks	Machine Catalog	Machine type	No. of machines	Allocated machines	1	Create Machine Catalog	
B Delivery Groups	VDI-NP	Desktop OS (Virtual)			0	View	•
Applications Policies	Allocation Type: Random	User data: Discard	Provisioning metho	d: Citrix provisioning service	25	Refresh	
Logging					- 11	Help	
Configuration						VDI-NP	
						Add Machines	-
						Edit Machine Catalog	
						So the Machine Catalog View Machines	
						Rename Machine Catalog	
	Details - VDI-NP					Test Machine Catalog	
	Details Machines Adn	ninistrators				Help	
	Machine Catalog		Machine		^		
	Machine Type: Provisioning Method: Allocation Type: Set to VDA version: Scopes:	VDI-NP Desktop OS (Virtual) Citrix provisioning servi Random 7.9 All Primary	Installed VDA version: Operating System:	7.9.0.101 Windows 10	Ŧ		

c. AD-DC1 > Active Directory Users and Computers > dvpod2.local > Computers > CTX-VDI-001



32. Logon to newly provisioned desktop machine, using the Virtual Disk Status verify the image mode is set to Ready Only and the cache type as Device Ram with overflow on local hard drive.

Recycle Bin		
	🛒 Virtual Disk Status	×
	General Statistics	
	Virtual Disk Information	
	Status: Active	
	Server: 10.10.161.43 : 6927	
	Boot from: vDisk	
	Virtual disk: Win10-vDisk.vhdx	
	Mode: Read Only	
	Cache type: Device RAM with overflow on local hard drive	
	Cache size: 9,050 MB	
	Cache used: 516 MB (5%)	
A DESCRIPTION OF THE OWNER OF THE	Version	
	Provisioning Services Version 7.9	
	Build 8201	
	Copyright © 2001-2016 Citrix Systems, Inc. All rights reserved.	
	Preferences	
	Prompt status message in System Tray	
	Show icon in System Tray	
ويحجو فأحيط والمتقاعيهم والانتظار ومحاطاته		
Ask me anything	4 🗆 😋 🧮 🚍	~

# Install XenDesktop Virtual Desktop Agents

Virtual Delivery Agents (VDAs) are installed on the server and workstation operating systems, and enable connections for desktops and apps. The following procedure was used to install VDAs for both HVD and HSD environments.

By default, when you install the Virtual Delivery Agent, Citrix User Profile Management is installed silently on master images.

Using profile management as a profile solution is optional but was used for this CVD and is described in a subsequent section.

To install XenDesktop Virtual Desktop Agents, complete the following steps:

- 1. Launch the XenDesktop installer from the XenDesktop 7.16 ISO.
- 2. Click Start on the Welcome Screen.

2

Deliver applications and desktops to any user, anywh on any device. • Secure mobile device management • Hybrid cloud, cloud and enterprise provisioning • Centralized and flexible management Manage your delivery according to your needs: XenApp Deliver applications	
XenDesktop Deliver applications and desktops	
CITRIX	

 To install the VDA for the Hosted Virtual Desktops (VDI), select Virtual Delivery Agent for Windows Desktop OS. After the VDA is installed for Hosted Virtual Desktops, repeat the procedure to install the VDA for Hosted Shared Desktops (RDS). In this case, select Virtual Delivery Agent for Windows Server OS and follow the same basic steps.

Get Started	Prepare Machi	nes and	Images					
Delivery Controller	Jelivery Controller			Virtual Delivery Agent for Windows Desktop OS				
				ieliver applications and desktops from V Ms or physical machines.	Vindows			
Extend Deployment				k				
Citrix Director incompatible OS		Citrix Studio		Self-Service Password Reset Incompatible OS				
Citrix License Server Incompatible OS		Universal Print Server Incompatible OS		Session Recording				
Citrix StoreFront incompatible OS		Federated Authentication Service Incompetible OS						

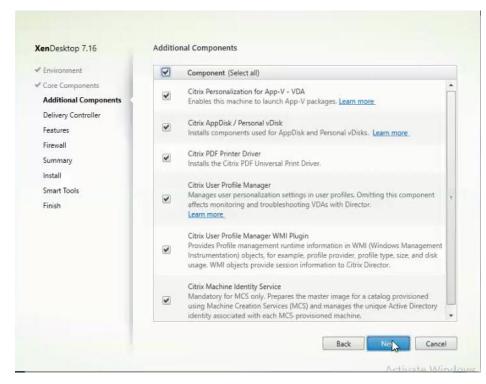
- 4. Select "Create a Master Image."
- 5. Click Next.

KenDesktop 7.16	Environment
Environment Core Components Additional Components Delivery Controller Features Firewall Summary Install Smart Tools Finish	Configuration I want to:  Create a Master Image Select this option if you use Machine Creation Services or Provisioning Services to create virtual desktops from this master image.  Control Enable Remote PC Access Select this option to install the Virtual Delivery Agent onto either a physical machine or var virtual machine that has been provisioned without the VDA.
	Back Next Cancel

- 6. Optional: Select Citrix Receiver.
- 7. Click Next.

XenDesktop 7.16	Core Components
Environment     Core Components	Location: C:\Program Files\Citrix Change
Additional Components Delivery Controller Features	Virtual Delivery Agent (Required) The software agent that is installed on the virtual or physical machine that provides the virtual desktop or application to the user.
Firewall Summary Install Smart Tools	Citrix Receiver Client software that enables users to access their documents, applications, and desktops from any device, including smartphones, tablets, and PCs.
Finish	
	Back Next Cancel

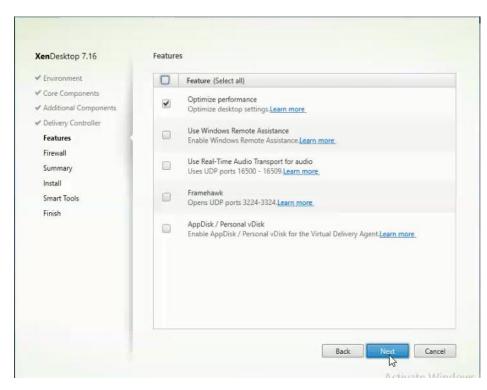
8. Click Next.



- 9. Select "Do it manually" and specify the FQDN of the Delivery Controllers.
- 10. Click Next.

<ul> <li>Environment</li> </ul>	Configuration	
✓ Core Components	How do you want to enter the locations of your Delivery C	ontrollers?
Additional Components	Do it manually	
Delivery Controller		
Features Firewall	hx-xdc1.hxhvdom.local	Edit Delete
Summary	Controller address:	
Install	Example: controller1.domain.com	
Smart Tools	Test connection Add	
Finish	Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller Ic	

- 11. Accept the default features.
- 12. Click Next.



- 13. Allow the firewall rules to be configured automatically.
- 14. Click Next.

XenDesktop 7.16	Firewall	
Environment	The default ports are listed below.	Printable version
Core Components     Additional Components	Controller Communications	
Delivery Controller	80 TCP 1494 TCP	
Features	2598 TCP	
Firewall	8008 TCP	
Summary	1494 UDP	
Install	2598 UDP	
Smart Tools		
Finish	Configure firewall rules: Automatically Select this option to automatically create the rules in the W created even if the Windows Firewall is turned off. Manually Select this option if you are not using Windows Firewall or yourself.	
	Ba	ck: Nrxt Cancel

15. Verify the Summary and click Install.

XenDesktop 7.16	Summary	
Environment     Core Components     Additional Components     Delivery Controller     Features     Firewall	Review the prerequisites and confirm the components you want to install. Installation directory C\Program Files\Citrix Prerequisites Microsoft Visual x64 C++ 2013 Runtime Microsoft Visual x64 C++ 2015 Runtime Microsoft Visual x64 C++ 2015 Runtime	rt required
Summary Install Smart Tools Finish	Microsoft Visual x86 C++ 2013 Runtime Microsoft Visual x86 C++ 2015 Runtime Core Components Virtual Delivery Agent Additional Components Citrix Personalization for App-V - VDA Citrix PopDisk / Personal vDisk Citrix VDF Printer Driver Citrix User Profile Manager Citrix User Profile Manager WMI Plugin	
	Citrix Machine Identity Service	• Cancel

16. (Optional) Select Call Home participation.

enDesktop 7.16	Smart Tools
<ul> <li><sup>e</sup> Environment</li> <li><sup>e</sup> Core Components</li> <li><sup>e</sup> Additional Components</li> <li><sup>e</sup> Delivery Controller</li> <li><sup>e</sup> Frewall</li> <li><sup>e</sup> Summary</li> <li><sup>e</sup> Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	Securely use Call Home, now part of Citrix Smart Tools, to monitor your deployment for common proor conditions and receive proactive notifications of issues before they become serious problems. How does it work? • Configuration and usage data are gathered and periodically sent to Citrix using HTTPS. • You can log into Citrix Insight Services to view diagnostics results and recommendations. This information will be used for troubleshooting and diagnostic support purposes, as well as to improve the quality, reliability, and performance of Citrix products, subject to the Citrix Nuw.citrix.com/about/legal/privacy.html. Learn more • I want to participate in Call Home. (Recommended) I do not want to participate in Call Home. • You will need citrix.com credentials. Connect

- 17. (Optional) check "Restart Machine."
- 18. Click Finish.

XenDesktop 7.16	Finish Installation	
<ul> <li>Environment</li> <li>Core Components</li> <li>Additianal Components</li> <li>Delivery Controller</li> <li>Features</li> <li>Firewall</li> <li>Summary</li> <li>Install</li> <li>Smart Tools</li> <li>Finish</li> </ul>	The installation completed successfully.  Prerequisites Microsoft Visual x64 C++ 2013 Runtime Microsoft Visual x86 C++ 2013 Runtime Microsoft Visual x86 C++ 2013 Runtime Microsoft Visual x86 C++ 2015 Runtime Core Components Virtual Delivery Agent Post Install Component Initialization	<ul> <li>✓ Success</li> <li>Installed</li> <li>Installed</li> <li>Installed</li> <li>Installed</li> <li>Installed</li> <li>Installed</li> </ul>
	Restart machine	Finish

- 19. Repeat the procedure so that VDAs are installed for both HVD (using the Windows 10 OS image) and the HSD desktops (using the Windows Server 2016 image).
- 20. Select an appropriate workflow for the HSD desktop.

Delivery Controller		Virtual Delivery Agent for Windows Server OS		
				eliver applications and desktops from server- al machines.
	Citrix Studio			Self-Service Password Reset
	Universal Print Serve	er		
	Federated Authentic	ation Service		
	Server and Store	1 Universal Print Serv	e Delivery Controller and other Jerver and StoreFront.	e Delivery Controller and other Server and StoreFront. Install this agent to d based VMs or physic Citrix Studio ( Citrix Studio ( Universal Print Server ()

# **Create Delivery Groups**

Delivery Groups are collections of machines that control access to desktops and applications. With Delivery Groups, you can specify which users and groups can access which desktops and applications.

To create delivery groups, complete the following steps:

The instructions below outline the steps to create a Delivery Group for VDI desktops. When you have completed these steps, repeat the procedure to a Delivery Group for HVD desktops.

- 1. Connect to a XenDesktop server and launch Citrix Studio.
- 2. Choose Create Delivery Group from the drop-down list.

8				Citrix Studio
File     Action     View     H       Image: second seco	Help			
Citrix Studio (Site)	CITRIX		Search	۶ 😵
AppDisks	Delivery Group	+	Delivering	No. of mac
Applications	Create Delivery Group			
Icogging▷ isotematical configuration	View	-		
	Help			

#### 3. Click Next.

么

ate Delivery Group	
Studio	Getting started with Delivery Groups
Introduction Machines Machine allocation	Delivery Groups are collections of desktops and applications (which could be in Application Groups) that are created from Machine Catalogs. Create Delivery Groups for specific teams, departments, or types of users. Make sure you have enough machines available in desktop OS or server OS Machine Catalogs to create the Delivery Groups you need.
Users Applications Desktop Assignment Rules Summary	
	Don't show this again Back Next Cancel

- 4. Select Machine catalog.
- 5. Provide the number of machines to be added to the delivery Group.
- 6. Click Next.

Studio	Mach	ines		
	Select	a Machine Catalog.		
		Catalog	Туре	Machines
Introduction	۲	Win10MCS-Random	VDI MCS Random	1000
Machines	0	Win10MCS-Static	VDI MCS Static Local Disk	1000
Machine allocation	0	Win10PVS-Random	VDI PVS Random	1000
Users	0	Win2016-HSD	RDS PVS Random	72
Summary	Choos	e the number of machines for th	is Delivery Group: 1000	1 -+

- 7. To make the Delivery Group accessible, you must add users, select Allow any authenticated users to use this Delivery Group.
- 8. Click Next.

te Delivery Group	
Studio	Users
	Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.
✓ Introduction	Allow any authenticated users to use this Delivery Group.
✓ Machines	Restrict use of this Delivery Group to the following users:
Users Applications Summary	Add users and groups
	Add Remove Sessions must launch in a user's home zone, if configured. Back Next Cancel



User assignment can be updated any time after Delivery group creation by accessing Delivery group properties in Desktop Studio.

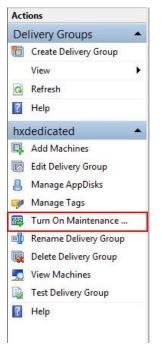
- 9. (Optional) specify Applications catalog will deliver.
- 10. Click Next.

Studio	Applications
<ul> <li>✓ Introduction</li> <li>✓ Machines</li> </ul>	To add applications, click "Add" and choose a source. Then select applications from that source. If you choose Application Groups, all current and future applications in the selected groups will be added. You can also place new applications in a non-default folder and change application properties.
🗸 Users	Add applications
Applications	
Summary	
	Add  Remove Properties
	Add •     Remove     Properties       Place the new applications in folder:
	Place the new applications in folder:
	Place the new applications in folder:

- 11. On the Summary dialog, review the configuration. Enter a Delivery Group name and a Display name (for example, HVD or HSD).
- 12. Click Finish.

Studio	Summary		
<ul> <li>Introduction</li> <li>Machines</li> <li>Users</li> <li>Applications</li> <li>Summary</li> </ul>	Machine Catalog: Machine type: Allocation type: Machines added:	Win10MCS-Random Desktop OS Random VDILAB-XD\w10mcs-r0001 VDILAB-XD\w10mcs-r0002 VDILAB-XD\w10mcs-r0003 VDILAB-XD\w10mcs-r0005 VDILAB-XD\w10mcs-r0005 VDILAB-XD\w10mcs-r0006 VDILAB-XD\w10mcs-r0008 VDILAB-XD\w10mcs-r0008 VDILAB-XD\w10mcs-r0019 VDILAB-XD\w10mcs-r0010 VDILAB-XD\w10mcs-r0011 VDILAB-XD\w10mcs-r0012	
	Delivery Group name: vdi-mcs-random Delivery Group description	n, used as label in Receiver (optional): Back Finish Car	ncel

13. Citrix Studio lists the created Delivery Groups and the type, number of machines created, sessions, and applications for each group in the Delivery Groups tab. Select Delivery Group and in Action List, select "Turn on Maintenance Mode."



# Citrix XenDesktop Policies and Profile Management

Policies and profiles allow the Citrix XenDesktop environment to be easily and efficiently customized.

## Configure Citrix XenDesktop Policies

Citrix XenDesktop policies control user access and session environments, and are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types with each policy. Policies can contain multiple settings and are typically defined through Citrix Studio. (The Windows Group Policy Management Console can also be used if the network environment includes Microsoft Active Directory and permissions are set for managing Group Policy Objects). Figure 113 shows policies for Login VSI testing in this CVD.

Policies	Testing Policy		
1 Unfiltered	Overview Settings Assigned to		
2 Testing Policy	Auto connect client drives     User setting - ICA\File Redirection     Disabled (Default: Enabled)		
3 VDI Policy	<ul> <li>Auto-create client printers         User setting - ICA\Printing\Client Printers         Do not auto-create client printers (Default: Auto-create all client printer)     </li> </ul>		
4 RDS Policy	Client printer redirection     User setting - ICA\Printing     Prohibited (Default: Allowed)		
	<ul> <li>Concurrent logons tolerance Computer setting - Load Management Value: 4 (Default: Value: 2)</li> </ul>		
	<ul> <li>CPU usage Computer setting - Load Management Disabled (Default: Disabled)</li> </ul>		
	<ul> <li>CPU usage excluded process priority</li> <li>Computer setting - Load Management</li> <li>Disabled (Default: Below Normal or Low)</li> </ul>		
	<ul> <li>Flash default behavior</li> <li>User setting - ICA\Adobe Flash Delivery\Flash Redirection</li> <li>Disable Flash acceleration (Default: Enable Flash acceleration)</li> </ul>		
	<ul> <li>Memory usage Computer setting - Load Management Disabled (Default: Disabled)</li> </ul>		
	<ul> <li>Memory usage base load</li> <li>Computer setting - Load Management</li> <li>Disabled (Default: Zero load: 768 MBs)</li> </ul>		

#### Figure 113 XenDesktop Policy

### Configuring User Profile Management

Profile management provides an easy, reliable, and high-performance way to manage user personalization settings in virtualized or physical Windows environments. It requires minimal infrastructure and administration, and provides users with fast logons and logoffs. A Windows user profile is a collection of folders, files, registry settings, and configuration settings that define the environment for a user who logs on with a particular user account. These settings may be customizable by the user, depending on the administrative configuration. Examples of settings that can be customized are:

- Desktop settings such as wallpaper and screen saver
- Shortcuts and Start menu setting
- Internet Explorer Favorites and Home Page
- Microsoft Outlook signature
- Printers

Some user settings and data can be redirected by means of folder redirection. However, if folder redirection is not used these settings are stored within the user profile.

The first stage in planning a profile management deployment is to decide on a set of policy settings that together form a suitable configuration for your environment and users. The automatic configuration feature simplifies some of this decision-making for XenDesktop deployments. Screenshots of the User Profile Management interfaces that establish policies for this CVD's RDS and VDI users (for testing purposes) are shown below.

Basic profile management policy settings are documented here:

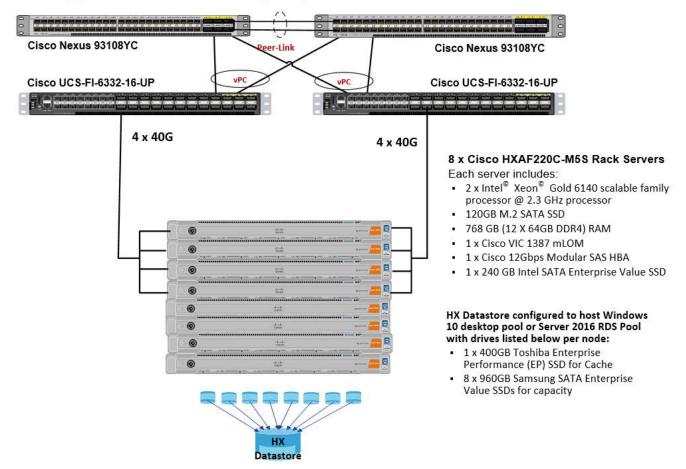
## http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11.html

## Figure 114 VDI User Profile Manager Policy

Policies	VDI Policy	
1 Unfiltered	Overview Settings Assigned to	
2 Testing Policy	<ul> <li>Active write back Computer setting - Profile Management\Basic settings Enabled (Default: Disabled)</li> </ul>	
3 VDI Policy	Delete locally cached profiles on logoff     Computer activity - Reafile Management Reafile handling	
4 RDS Policy	Computer setting - Profile Management\Profile handling Enabled (Default: Disabled)	
	<ul> <li>Enable Profile management</li> <li>Computer setting - Profile Management\Basic settings</li> <li>Enabled (Default: Disabled)</li> </ul>	
	<ul> <li>Exclusion list - directories</li> <li>Computer setting - Profile Management\File system\Exclusions</li> <li>AppData\Local;AppData\LocalLow;AppData\Roaming;\$Recycle.Bin (Default: )</li> </ul>	
	<ul> <li>Path to user store Computer setting - Profile Management\Basic settings \\10.10.62.92\Profile-VDI01\$\#SAMAccountName# (Default: Windows)</li> </ul>	
	<ul> <li>Process logons of local administrators</li> <li>Computer setting - Profile Management\Basic settings</li> <li>Enabled (Default: Disabled)</li> </ul>	

# **Test Setup and Configurations**

In this project, we tested a single Cisco HyperFlex cluster running four Cisco UCS HXAF220C-M5SX Rack Servers in a single Cisco UCS domain. This solution is tested to illustrate linear scalability for each workload studied.



Cisco HyperFlex and Citrix XenDesktop 7.18, Reference Architecture

Hardware Components:

- 2 x Cisco UCS 6332-16UP Fabric Interconnects
- 2 x Cisco Nexus 93108YCPX Access Switches
- 8 x Cisco UCS HXAF220c-M5SX Rack Servers (2 Intel Xeon Gold 6140 scalable family processor at 2.3 GHz, with 768 GB of memory per server [32 GB x 24 DIMMs at 2666 MHz])
- Cisco VIC 1387 mLOM
- 12G modular SAS HBA Controller
- 240GB M.2 SATA SSD drive (Boot and HyperFlex Data Platform controller VM)
- 240GB 2.5" 6G SATA SSD drive (Housekeeping)

- 400GB 2.5" 6G SAS SSD drive (Cache)
- 8 x 960GB 2.5" SATA SSD drive (Capacity)
- 1 x 32GB mSD card (Upgrades temporary cache)

Software Components:

- Cisco UCS firmware 3.2(3e)
- Cisco HyperFlex Data Platform 3.0.1c
- Microsoft Hyper-V 2016
- Citrix XenDesktop 7.16
- Citrix User Profile Management
- Microsoft SQL Server 2016
- Microsoft Windows 10
- Microsoft Windows 2016
- Microsoft Office 2016
- Login VSI 4.1.25.6

# Testing Methodology and Success Criteria

All validation testing was conducted on-site within the Cisco labs in San Jose, California.

The testing results focused on the entire process of the virtual desktop lifecycle by capturing metrics during the desktop boot-up, user logon and virtual desktop acquisition (also referred to as ramp-up,) user workload execution (also referred to as steady state), and user logoff for the Hosted Shared Desktop Session under test.

Test metrics were gathered from the virtual desktop, storage, and load generation software to assess the overall success of an individual test cycle. Each test cycle was not considered passing unless all of the planned test users completed the ramp-up and steady state phases (described below) and unless all metrics were within the permissible thresholds as noted as success criteria.

Three successfully completed test cycles were conducted for each hardware configuration and results were found to be relatively consistent from one test to the next.

You can obtain additional information and a free test license from http://www.loginvsi.com.

# **Testing Procedure**

The following protocol was used for each test cycle in this study to insure consistent results.

# Pre-Test Setup for Testing

All machines were shut down utilizing the Citrix XenDesktop 7.16 Administrator Console.

All Launchers for the test were shut down. They were then restarted in groups of 10 each minute until the required number of launchers was running with the Login VSI Agent at a "waiting for test to start" state.

## Test Run Protocol

To simulate severe, real-world environments, Cisco requires the log-on and start-work sequence, known as Ramp Up, to complete in 48 minutes. Additionally, we require all sessions started, whether 60 single server users or 4000 full scale test users to become active within two minutes after the last session is launched.

In addition, Cisco requires that the Login VSI Benchmark method is used for all single server and scale testing. This assures that our tests represent real-world scenarios. For each of the three consecutive runs on single server tests, the same process was followed. Complete the following steps:

- 1. Time 0:00:00 Start esxtop Logging on the following systems:
  - Infrastructure and VDI Host Blades used in test run
  - All Infrastructure VMs used in test run (AD, SQL, View Connection brokers, image mgmt., etc.)
- 2. Time 0:00:10 Start Storage Partner Performance Logging on Storage System.
- 3. Time 0:05: Boot RDS Machines using Citrix XenDesktop 7.16 Administrator Console.
- 4. Time 0:06 First machines boot.
- 5. Time 0:35 Single Server or Scale target number of RDS Servers registered on XD.

No more than 60 Minutes of rest time is allowed after the last desktop is registered and available on Citrix XenDesktop 7.16 Administrator Console dashboard. Typically a 20-30 minute rest period for Windows 10 desktops and 10 minutes for RDS VMs is sufficient.

- 6. Time 1:35 Start Login VSI 4.1.5 Knowledge Worker Benchmark Mode Test, setting auto-logoff time at 900 seconds, with Single Server or Scale target number of desktop VMs utilizing sufficient number of Launchers (at 20-25 sessions/Launcher).
- 7. Time 2:23 Single Server or Scale target number of desktop VMs desktops launched (48 minute benchmark launch rate).
- 8. Time 2:25 All launched sessions must become active.



All sessions launched must become active for a valid test run within this window.

- 9. Time 2:40 Login VSI Test Ends (based on Auto Logoff 900 Second period designated above).
- 10. Time 2:55 All active sessions logged off.
- 11. All sessions launched and active must be logged off for a valid test run. The Citrix XenDesktop 7.16 Administrator Dashboard must show that all desktops have been returned to the registered/available state as evidence of this condition being met.
- 12. Time 2:57 All logging terminated; Test complete.
- 13. Time 3:15 Copy all log files off to archive; Set virtual desktops to maintenance mode through broker; Shutdown all Windows 7 machines.
- 14. Time 3:30 Reboot all hypervisors.
- 15. Time 3:45 Ready for new test sequence.

### Success Criteria

Our "pass" criteria for this testing is as follows: Cisco will run tests at a session count levels that effectively utilize the server capacity measured by CPU, memory, storage and network utilization. We use Login VSI version 4.1.25 to launch Knowledge Worker workload sessions. The number of launched sessions must equal active sessions within two minutes of the last session launched in a test as observed on the VSI Management console.

The Citrix XenDesktop Studio will be monitored throughout the steady state to make sure of the following:

- All running sessions report In Use throughout the steady state
- No sessions move to unregistered, unavailable or available state at any time during steady state

Within 20 minutes of the end of the test, all sessions on all launchers must have logged out automatically and the Login VSI Agent must have shut down. Cisco's tolerance for Stuck Sessions is 0.5 percent (half of one percent.) If the Stuck Session count exceeds that value, we identify it as a test failure condition.

Cisco requires three consecutive runs with results within +/-1 percent variability to pass the Cisco Validated Design performance criteria. For white papers written by partners, two consecutive runs within +/-1 percent variability are accepted. (All test data from partner run testing must be supplied along with proposed white paper.)

We will publish Cisco Validated Designs with our recommended workload following the process above and will note that we did not reach a VSImax dynamic in our testing.

The purpose of this testing is to provide the data needed to validate Citrix XenDesktop 7.16 Hosted Shared Desktop with Citrix XenDesktop 7.16 Composer provisioning using Microsoft Windows Server 2016 sessions on Cisco UCS HXAF220c-M4S, Cisco UCS 220 M4 and Cisco UCS B200 M4 servers.

The information contained in this section provides data points that a customer may reference in designing their own implementations. These validation results are an example of what is possible under the specific environment conditions outlined here and do not represent the full characterization of Citrix and Microsoft products.

Four test sequences, each containing three consecutive test runs generating the same result, were performed to establish system performance and linear scalability.

### VSImax 4.1.x Description

The philosophy behind Login VSI is different to conventional benchmarks. In general, most system benchmarks are steady state benchmarks. These benchmarks execute one or multiple processes, and the measured execution time is the outcome of the test. Simply put: the faster the execution time or the bigger the throughput, the faster the system is according to the benchmark.

Login VSI is different in approach. Login VSI is not primarily designed to be a steady state benchmark (however, if needed, Login VSI can act like one). Login VSI was designed to perform benchmarks for SBC or VDI workloads through system saturation. Login VSI loads the system with simulated user workloads using well known desktop applications like Microsoft Office, Internet Explorer and Adobe PDF reader. By gradually increasing the amount of simulated users, the system will eventually be saturated. Once the system is saturated, the response time of the applications will increase significantly. This latency in application response times show a clear indication whether the system is (close to being) overloaded. As a result, by nearly overloading a system it is possible to find out what is its true maximum user capacity.

After a test is performed, the response times can be analyzed to calculate the maximum active session/desktop capacity. Within Login VSI this is calculated as VSImax. When the system is coming closer to its saturation point, response times will rise. When reviewing the average response time it will be clear the response times escalate at saturation point.

This VSImax is the "Virtual Session Index (VSI)". With Virtual Desktop Infrastructure (VDI) and Terminal Services (RDS) workloads this is valid and useful information. This index simplifies comparisons and makes it possible to understand the true impact of configuration changes on hypervisor host or guest level.

### Server-Side Response Time Measurements

It is important to understand why specific Login VSI design choices have been made. An important design choice is to execute the workload directly on the target system within the session instead of using remote sessions. The scripts simulating the workloads are performed by an engine that executes workload scripts on every target system, and are initiated at logon within the simulated user's desktop session context.

An alternative to the Login VSI method would be to generate user actions client side through the remoting protocol. These methods are always specific to a product and vendor dependent. More importantly, some protocols simply do not have a method to script user actions client side.

For Login VSI the choice has been made to execute the scripts completely server side. This is the only practical and platform independent solutions, for a benchmark like Login VSI.

#### Calculating VSImax v4.1.x

The simulated desktop workload is scripted in a 48-minute loop when a simulated Login VSI user is logged on, performing generic Office worker activities. After the loop is finished it will restart automatically. Within each loop the response times of sixteen specific operations are measured in a regular interval: sixteen times in within each loop. The response times of these five operations are used to determine VSImax.

The five operations from which the response times are measured are:

• Notepad File Open (NFO)

Loading and initiating VSINotepad.exe and opening the openfile dialog. This operation is handled by the OS and by the VSINotepad.exe itself through execution. This operation seems almost instant from an end-user's point of view.

• Notepad Start Load (NSLD)

Loading and initiating VSINotepad.exe and opening a file. This operation is also handled by the OS and by the VSINotepad.exe itself through execution. This operation seems almost instant from an end-user's point of view.

• Zip High Compression (ZHC)

This action copy's a random file and compresses it (with 7zip) with high compression enabled. The compression will very briefly spike CPU and disk IO.

• Zip Low Compression (ZLC)

This action copy's a random file and compresses it (with 7zip) with low compression enabled. The compression will very briefly disk IO and creates some load on the CPU.

• CPU

Calculates a large array of random data and spikes the CPU for a short period of time.

These measured operations within Login VSI do hit considerably different subsystems such as CPU (user and kernel), Memory, Disk, the OS in general, the application itself, print, GDI, etc. These operations are specifically short by nature. When such operations become consistently long: the system is saturated because of excessive queuing on any kind of resource. As a result, the average response times will then escalate. This effect is clearly visible to end-users. If such operations consistently consume multiple seconds the user will regard the system as slow and unresponsive.

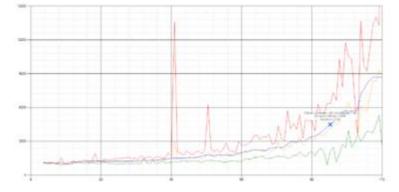
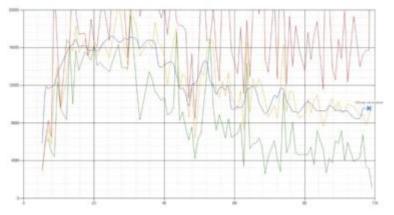


Figure 115 Sample of a VSI Max Response Time Graph, Representing a Normal Test

Figure 116 Sample of a VSI Test Response Time Graph with a Clear Performance Issue



When the test is finished, VSImax can be calculated. When the system is not saturated, and it could complete the full test without exceeding the average response time latency threshold, VSImax is not reached and the amount of sessions ran successfully.

The response times are very different per measurement type, for instance Zip with compression can be around 2800 ms, while the Zip action without compression can only take 75ms. This response time of these actions are weighted before they are added to the total. This ensures that each activity has an equal impact on the total response time.

In comparison to previous VSImax models, this weighting much better represent system performance. All actions have very similar weight in the VSImax total. The following weighting of the response times are applied.

The following actions are part of the VSImax v4.1 calculation and are weighted as follows (US notation):

- Notepad File Open (NFO): 0.75
- Notepad Start Load (NSLD): 0.2
- Zip High Compression (ZHC): 0.125
- Zip Low Compression (ZLC): 0.2
- CPU: 0.75

This weighting is applied on the baseline and normal Login VSI response times.

With the introduction of Login VSI 4.1 we also created a new method to calculate the base phase of an environment. With the new workloads (Taskworker, Powerworker, etc.) enabling 'base phase' for a more reliable

baseline has become obsolete. The calculation is explained below. In total 15 lowest VSI response time samples are taken from the entire test, the lowest 2 samples are removed and the 13 remaining samples are averaged. The result is the Baseline. The calculation is as follows:

- Take the lowest 15 samples of the complete test
- From those 15 samples remove the lowest 2
- Average the 13 results that are left is the baseline

The VSImax average response time in Login VSI 4.1.x is calculated on the amount of active users that are logged on the system.

Always a 5 Login VSI response time samples are averaged + 40 percent of the amount of "active" sessions. For example, if the active sessions is 60, then latest 5 + 24 (=40 percent of 60) = 31 response time measurement are used for the average calculation.

To remove noise (accidental spikes) from the calculation, the top 5 percent and bottom 5 percent of the VSI response time samples are removed from the average calculation, with a minimum of 1 top and 1 bottom sample. As a result, with 60 active users, the last 31 VSI response time sample are taken. From those 31 samples the top 2 samples are removed and lowest 2 results are removed (5 percent of 31 = 1.55, rounded to 2). At 60 users the average is then calculated over the 27 remaining results.

VSImax v4.1.x is reached when the VSIbase + a 1000 ms latency threshold is not reached by the average VSI response time result. Depending on the tested system, VSImax response time can grow 2 - 3x the baseline average. In end-user computing, a 3x increase in response time in comparison to the baseline is typically regarded as the maximum performance degradation to be considered acceptable.

In VSImax v4.1.x this latency threshold is fixed to 1000ms, this allows better and fairer comparisons between two different systems, especially when they have different baseline results. Ultimately, in VSImax v4.1.x, the performance of the system is not decided by the total average response time, but by the latency is has under load. For all systems, this is now 1000ms (weighted).

The threshold for the total response time is: average weighted baseline response time + 1000ms.

When the system has a weighted baseline response time average of 1500ms, the maximum average response time may not be greater than 2500ms (1500+1000). If the average baseline is 3000 the maximum average response time may not be greater than 4000ms (3000+1000).

When the threshold is not exceeded by the average VSI response time during the test, VSImax is not hit and the amount of sessions ran successfully. This approach is fundamentally different in comparison to previous VSImax methods, as it was always required to saturate the system beyond VSImax threshold.

Lastly, VSImax v4.1.x is now always reported with the average baseline VSI response time result. For example: "The VSImax v4.1 was 125 with a baseline of 1526ms". This helps considerably in the comparison of systems and gives a more complete understanding of the system. The baseline performance helps to understand the best performance the system can give to an individual user. VSImax indicates what the total user capacity is for the system. These two are not automatically connected and related:

When a server with a very fast dual core CPU, running at 3.6 GHZ, is compared to a 10 core CPU, running at 2,26 GHZ, the dual core machine will give and individual user better performance than the 10 core machine. This is indicated by the baseline VSI response time. The lower this score is, the better performance an individual user can expect.

However, the server with the slower 10 core CPU will easily have a larger capacity than the faster dual core system. This is indicated by VSImax v4.1.x, and the higher VSImax is, the larger overall user capacity can be expected.

With Login VSI 4.1.x a new VSImax method is introduced: VSImax v4.1. This methodology gives much better insight in system performance and scales to extremely large systems.

# Test Results

## **Boot Storms**

A key performance metric for desktop virtualization environments is the ability to boot the virtual machines quickly and efficiently to minimize user wait time for their desktop.

As part of Cisco's virtual desktop test protocol, we shut down each virtual machine at the conclusion of a benchmark test. When we run a new test, we cold boot all 450 desktops and measure the time it takes for the 450<sup>th</sup> virtual machine to register as available in the XenDesktop Administrator console.

The Cisco HyperFlex HXAF220c-M5SX based All-Flash cluster running Data Platform version 3.0.1c software can accomplish this task in **5 minutes**.

# Recommended Maximum Workload and Configuration Guidelines

## Eight Node Cisco HXAF220c-M5S Rack Server and HyperFlex All-Flash Cluster

For Citrix XenApp RDS Hosted Shared Desktop and Hosted Virtual Desktop use case, the recommended maximum workload was determined based on both Login VSI Knowledge Worker workload end user experience measures and HXAF220c-M5SX server operating parameters.

This recommended maximum workload approach allows you to determine the server N+1 fault tolerance load the blade can successfully support in the event of a server outage for maintenance or upgrade.

Our recommendation is that the Login VSI Average Response and VSI Index Average should not exceed the Baseline plus 2000 milliseconds to insure that end-user experience is outstanding. Additionally, during steady state, the processor utilization should average no more than 90-95 percent.



and the

Memory should never be oversubscribed for Desktop Virtualization workloads.

Test Phase	Description
Boot	Start all RDS and/or VDI virtual machines at the same time.
Login	The Login VSI phase of test is where sessions are launched and start executing the workload over a 48 minutes duration.
Steady state	The steady state phase is where all users are logged in and performing various workload tasks such as using Microsoft Office, Web browsing, PDF printing, playing videos, and compressing files.
Logoff	Sessions finish executing the Login VSI workload and logoff.

## Eight Node Cisco HXAF220c-M5S Rack Server and HyperFlex All-Flash Cluster

For Citrix XenApp RDS Hosted Shared Desktop and Hosted Virtual Desktop use case, the recommended maximum workload was determined based on both Login VSI Knowledge Worker workload end user experience measures and HXAF220c-M5SX server operating parameters.

This recommended maximum workload approach allows you to determine the server N+1 fault tolerance load the blade can successfully support in the event of a server outage for maintenance or upgrade.

Our recommendation is that the Login VSI Average Response and VSI Index Average should not exceed the Baseline plus 2000 milliseconds to insure that end-user experience is outstanding. Additionally, during steady state, the processor utilization should average no more than 90-95 percent.

Test Phase	Description	
Boot	Start all RDS and/or VDI virtual machines at the same time.	
Login	The Login VSI phase of test is where sessions are launched and start executing the workload over a 48 minutes duration.	
Steady state	The steady state phase is where all users are logged in and performing various workload tasks such using Microsoft Office, Web browsing, PDF printing, playing videos, and compressing files.	
Logoff	Sessions finish executing the Login VSI workload and logoff.	

The recommended maximum workload for a Cisco HyperFlex cluster configured on Cisco HXAF220c-M5SX with Intel Xeon Gold 6140 scalable family processors and 768GB of RAM for Windows 10 desktops is 1250 users with Office 2016 virtual desktops respectively.

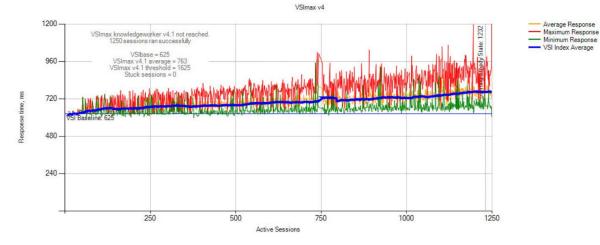
#### 1250 Windows 10 Citrix PVS Non-Persistent Testing on Eight Node Cisco HyperFlex Cluster

Pooled desktops with 1250 Windows 10 VMs hosting 1250 User Sessions on four HXAF220c-M5SX HyperFlex cluster.

Test result highlights include:

ß

- 0.625 second baseline response time
- 0.763 second average response time with 1250 desktops running
- Average CPU utilization of 55 percent during steady state
- Average of 500 GB of RAM used out of 768 GB available
- 3500 peak I/O operations per second (IOPS) per cluster at steady state
- 250MBps peak throughput per cluster at steady state



#### Figure 117 Login VSI Analyzer Chart for 1250 Windows 10 Citrix PVS Non-persistent Virtual Desktops

1250-01

Successfully completed Login VSI test with 1250 knowledgeworker sessions. VSImax (system saturation) was not reached. All Login VSI users completed the test.

PASS

LoginVSI Results VSI Baseline: 625ms

Stuck Sessions: 0

VSI Baseline

0-799 800-1299

1200-1999

2000-9999

VSI Average: 763ms

VSI Threshold: 1625ms

Performance Very Good

Good

Reasonable

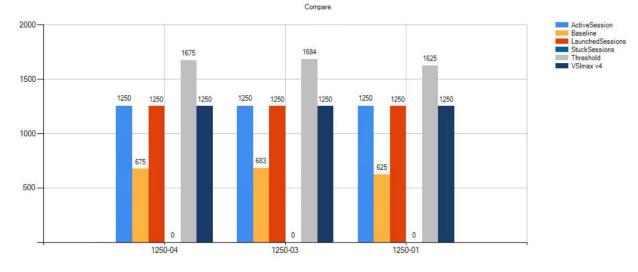
Bad



Login VSI index average score is 674 lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance of 625 is: Very good





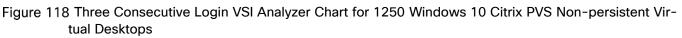
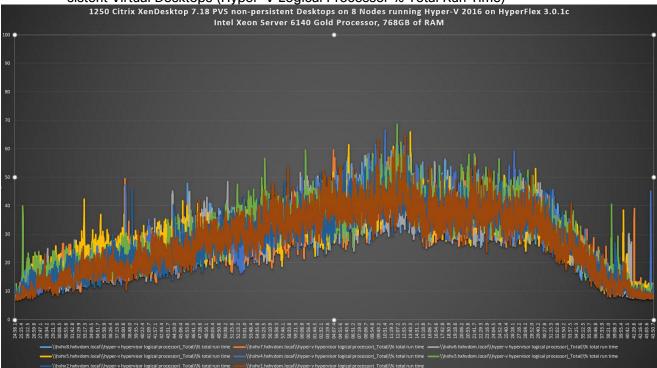


Figure 119 Sample 8x Hyper-V Hosts CPU Core Utilization Running 1250 Windows 10 Citrix PVS Non-persistent Virtual Desktops (Hyper-V Logical Processor % Total Run Time)



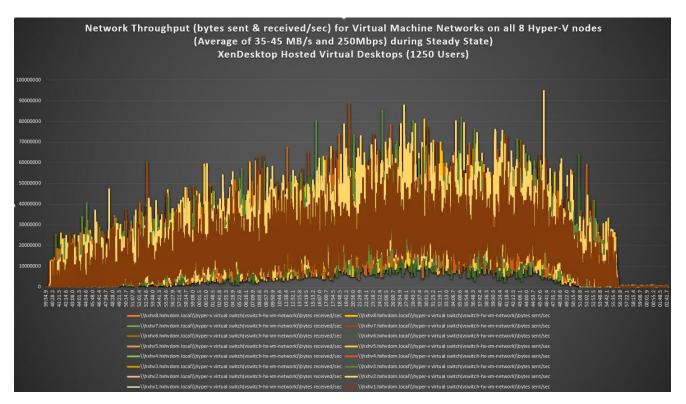


Figure 120 HyperFlex Cluster UI Performance Chart for Knowledge Worker Workload Running 1250 User Test on Citrix PVS Non-persistent Windows 10

≡ <sup>•i  •i  •</sup> HyperFlex Connect	hxhv1	cip	E8 @ 0 L		
🚯 Dashboard	Cluster	1h 1d 1w 1m 6m jul 12,2018-jul 12,2018	Last refreshed at: 07/12/2018 1:55:21 PM 🔿		
MONITOR					
* Events	0 12:27 PM 12:37 PM 12:48 F	РМ 12:59 РМ 1:10 РМ	1:20 PM		
Activity	10P5 07/12/2018 12:16:00 PM • 07/12/2018 1:30:00 PM • Read Mac 389.5 Min:4.2 Avg: 197.15 • Write Max 3679.7 Min:83.1 Avg 2246.1 • Aggregated Max 3959.3 Min:82.7 Avg 2443.25				
ANALYZE	3.75K	• Write • Read			
Ltd. Performance	25%	OP5 3,464.5 243.7			
MANAGE	1.25K	Throughput (MBps) 139.0 2.0	$\sim$		
MANAGE		Latency (msec) 6.3 2.1			
System Information	Throughput (MBps) 07/12/2018 12:16:00 PM - 07/12/2018 1:30:00 PM	Read Max: 4.55 Min:0.02 Avg: 1.89     Write Max: 155.56 Min:2.37 Avg:	92 94 • Appreciated Marc 157 96 Min/2 & Avor 94 82		
Datastores	150	^ ~~~~~			
2. Upgrade	100				
	50		$\sim$ $\checkmark$		
	Latency (msec) 07/12/2018 12:16:00 PM - 07/12/2018 1:30:00 PM 9	Read Max: 4.4 Min:1.86 Avg; 2.28     Write Max: 8.56 Min:5.2	22 Avg: 6.69 • Average Max: 5.97 Min:3.56 Avg: 4.48		
	3				

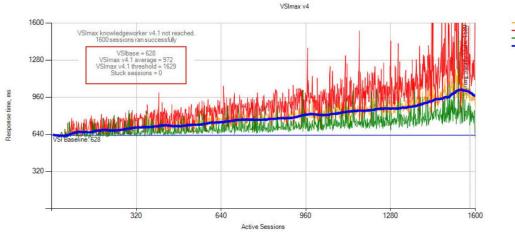
Æ

The recommended maximum workload for a Cisco HyperFlex cluster configured on Cisco HXAF220c-M5SX with Intel Xeon Gold 6140 scalable family processors and 768GB of RAM for Windows Server 2016 Hosted Sessions is 1250 sessions with Office 2016 virtual desktops respectively.

1600 Windows 2016 Citrix PVS Non-Persistent HSD Testing on Eight Node Cisco HyperFlex Cluster Pooled hosted shared desktops with 1600 User Sessions on four HXAF220c-M5SX HyperFlex cluster. Test result highlights include:

- 0.676 second baseline response time
- 0.839 second average response time with 450 desktops running
- Average CPU utilization of 45 percent during steady state
- Average of 320 GB of RAM used out of 768 GB available
- 3500 peak I/O operations per second (IOPS) per cluster at steady state
- 80MBps peak throughput per cluster at steady state

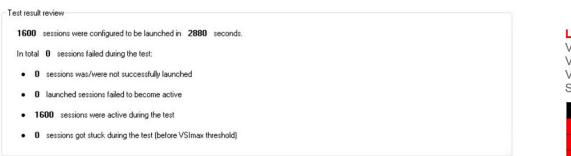
### Figure 121 Login VSI Analyzer Chart for 1600 Windows 2016 Citrix PVS Non-persistent HSD



Average Response Maximum Response Minimum Response VSI Index Average

XA-1600-01

Successfully completed Login VSI test with 1600 knowledgeworker sessions. VSImax (system saturation) was not reached. All Login VSI users completed the test.



With 1600 sessions the maximum capacity VSImax (v4.1) knowledgeworker was not reached with a Login VSI baseline performance score of 628

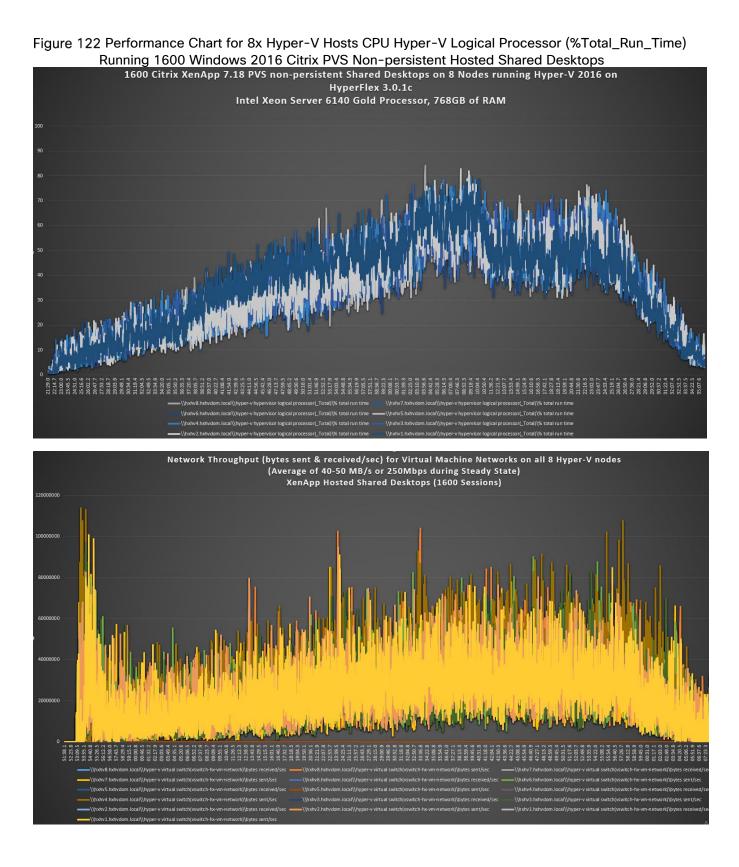
Baseline performance of 628 is: Very good



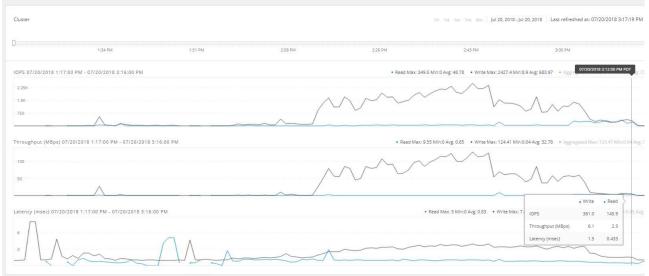
#### LoginVSI Results

VSI Baseline: 628ms VSI Average: 972ms VSI Threshold: 1629ms Stuck Sessions: 0

VSI Baseline	Performance
0-799	Very Good
800-1299	Good
1200-1999	Reasonable
2000-9999	Bad



#### Figure 123 HyperFlex Cluster UI Performance Chart for Knowledge Worker Workload Running 1600 User Test on Citrix PVS Non-persistent Windows 2016 HSD



# Summary

This Cisco HyperFlex solution addresses urgent needs of IT by delivering a platform that is cost effective and simple to deploy and manage. The architecture and approach used provides for a flexible and high-performance system with a familiar and consistent management model from Cisco. In addition, the solution offers numerous enterprise-class data management features to deliver the next-generation hyper-converged system.

Only Cisco offers the flexibility to add compute only nodes to a true hyper-converged cluster for compute intensive workloads like desktop virtualization. This translates to lower cost for the customer, since no hyper-convergence licensing is required for those nodes.

Delivering responsive, resilient, high-performance Citrix XenDesktop provisioned Microsoft Windows 10 Virtual Machines and Microsoft Windows Server for hosted Apps or desktops has many advantages for desktop virtualization administrators.

The solution if fully capable of supporting graphics accelerated workloads. Each Cisco HyperFlex HXAF240c M5 node and each Cisco UCS C240 M5 server can support up to two NVIDIA M10 or P40 cards. The Cisco UCS B200 M5 server supports up to two NVIDIA P6 cards for high density, high performance graphics workload support. See our <u>Cisco Graphics White Paper</u> for our fifth generation servers with NVIDIA GPUs and software for details on how to integrate this capability with Citrix XenDesktop.

Virtual desktop end-user experience, as measured by the Login VSI tool in benchmark mode, is outstanding with Intel Xeon scalable family processors and Cisco 2666Mhz memory. In fact, we have set a new industry standard in performance for Desktop Virtualization on a hyper-converged platform.

# About the Authors

# Jeff Nichols, Technical Marketing Engineer, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.

Jeff Nichols is a Cisco Unified Computing System architect, focusing on Virtual Desktop and Application solutions with extensive experience with Microsoft ESX/Hyper-V, XenDesktop, XenApp and Microsoft Remote Desktop Services. He has expert product knowledge in application, desktop and server virtualization across all three major hypervisor platforms and supporting infrastructures including but not limited to Windows Active Directory and Group Policies, User Profiles, DNS, DHCP and major storage platforms.

## Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, we would like to acknowledge their contribution and expertise that resulted in developing this document:

- Mike Brennan, Product Manager, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.
- Sanjeev Naldurgkar, Technical Marketing Engineer, Cisco UCS Datacenter Solutions Group, Cisco Systems, Inc.

# Appendix A - Cisco Nexus 93108YC Switch Configuration

# Switch A Configuration

!Command: show running-config

version 7.0(3)I2(2d) switchname XXXXXXXXXXXXX class-map type network-qos class-fcoe match qos-group 1 class-map type network-gos class-all-flood match qos-group 2 class-map type network-gos class-ip-multicast match qos-group 2 vdc XXXXXXXXXX id 1 limit-resource vlan minimum 16 maximum 4094 limit-resource vrf minimum 2 maximum 4096 limit-resource port-channel minimum 0 maximum 511 limit-resource u4route-mem minimum 248 maximum 248 limit-resource u6route-mem minimum 96 maximum 96 limit-resource m4route-mem minimum 58 maximum 58 limit-resource m6route-mem minimum 8 maximum 8

feature telnet cfs eth distribute feature interface-vlan feature hsrp feature lacp feature dhcp feature vpc feature lldp clock protocol ntp vdc 1 no password strength-check username admin password 5 \$1\$MSJwTJtn\$Bo0IrVnESUVxLcbRHg86j1 role network-admin ip domain-lookup no service unsupported-transceiver class-map type qos match-all class-fcoe policy-map type qos jumbo class class-default set qos-group 0 copp profile strict snmp-server user admin network-admin auth md5 0x71d6a9cf1ea007cd3166e91a6f3807e5 priv 0x71d6a9cf1ea007cd3166e91a6f3807e5 localizedkey rmon event 1 log trap public description FATAL(1) owner PMON@FATAL rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL rmon event 3 log trap public description ERROR(3) owner PMON@ERROR rmon event 4 log trap public description WARNING(4) owner PMON@WARNING rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO ntp server 10.10.50.2 ntp peer 10.10.50.3 ntp server 171.68.38.66 use-vrf management ntp logging ntp master 8 vlan 1,50-54 vlan 50 name InBand-Mgmt-C1 vlan 51 name Infra-Mgmt-C1 vlan 52 name StorageIP-C1 vlan 53 name LiveMigration-C1

vlan 54

name VM-Data-C1

service dhcp

ip dhcp relay

ip dhcp relay information option

ipv6 dhcp relay

vrf context management

ip route 0.0.0.0/0 10.29.132.1

vpc domain 50

role priority 1000

peer-keepalive destination 10.29.132.20 source 10.29.132.19

interface Vlan1

no shutdown

ip address 10.29.132.2/24

interface Vlan50

no shutdown

ip address 10.10.50.2/24

hsrp version 2

hsrp 50

preempt

priority 110

ip 10.10.50.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface Vlan51

no shutdown

ip address 10.10.51.2/24

hsrp version 2

hsrp 51

preempt

priority 110

ip 10.10.51.1

interface Vlan52

no shutdown

ip address 10.10.52.2/24

hsrp version 2

hsrp 52

preempt

priority 110

ip 10.10.52.1

interface Vlan53

no shutdown

ip address 10.10.53.2/24

hsrp version 2

hsrp 53

preempt

priority 110

ip 10.10.53.1

interface Vlan54

no shutdown

ip address 10.54.0.2/20

hsrp version 2

hsrp 54

preempt

priority 110

ip 10.54.0.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface port-channel10 description vPC-PeerLink switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type network

service-policy type qos input jumbo vpc peer-link

interface port-channel11 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 11

interface port-channel12 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 12

interface Ethernet1/1 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/2 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/3 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/4 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/5 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 11 mode active interface Ethernet1/6 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 11 mode active

interface Ethernet1/7 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 12 mode active

interface Ethernet1/8

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 12 mode active

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25 switchport mode trunk switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/26 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/27 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/28

switchport mode trunk

switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/29

switchport mode trunk

switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/30 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/31 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/32 switchport mode trunk switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0

vrf member management

ip address 10.29.132.19/24

clock timezone PST -8 0 clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60 line console line vty boot nxos bootflash:/nxos.7.0.3.I2.2d.bin

# Switch B Configuration

Command: show running-config Time: Fri Dec 15 17:18:36 2017

version 7.0(3)I2(2d) switchname XXXXXXXXXXXX class-map type network-qos class-fcoe match qos-group 1 class-map type network-qos class-all-flood match qos-group 2 class-map type network-qos class-ip-multicast match qos-group 2 vdc XXXXXXXXXX id 1 limit-resource vlan minimum 16 maximum 4094 limit-resource vrf minimum 2 maximum 4096 limit-resource port-channel minimum 0 maximum 511 limit-resource u4route-mem minimum 248 maximum 248 limit-resource u6route-mem minimum 96 maximum 96 limit-resource m4route-mem minimum 58 maximum 58 limit-resource m6route-mem minimum 8 maximum 8

feature telnet cfs eth distribute feature interface-vlan feature hsrp feature lacp feature dhcp feature vpc feature lldp clock protocol ntp vdc 1 no password strength-check username admin password 5 \$1\$jEwHqUvM\$gpOec2hramkyX09KD3/Dn. role network-admin ip domain-lookup no service unsupported-transceiver class-map type qos match-all class-fcoe policy-map type gos jumbo class class-default set qos-group 0 copp profile strict snmp-server user admin network-admin auth md5 0x9046c100ce1f4ecdd74ef2f92c4e83f9 priv 0x9046c100ce1f4ecdd74ef2f92c4e83f9 localizedkey rmon event 1 log trap public description FATAL(1) owner PMON@FATAL rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL rmon event 3 log trap public description ERROR(3) owner PMON@ERROR rmon event 4 log trap public description WARNING(4) owner PMON@WARNING rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO ntp peer 10.10.50.2 ntp server 10.10.50.3 ntp server 171.68.38.66 use-vrf management ntp logging ntp master 8 vlan 1,50-54 vlan 50 name InBand-Mgmt-C1 vlan 51

name Infra-Mgmt-C1

vlan 52 name StorageIP-C1 vlan 53 name LiveMigration-C1 vlan 54 name VM-Data-C1

service dhcp ip dhcp relay ip dhcp relay information option ipv6 dhcp relay vrf context management ip route 0.0.0.0/0 10.29.132.1 vpc domain 50 role priority 2000 peer-keepalive destination 10.29.132.19 source 10.29.132.20

interface Vlan1

no shutdown

ip address 10.29.132.3/24

interface Vlan50

no shutdown

ip address 10.10.50.3/24

hsrp version 2

hsrp 50

preempt

priority 110

ip 10.10.50.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface Vlan51

no shutdown

ip address 10.10.51.3/24

hsrp version 2

hsrp 51

preempt

priority 110

ip 10.10.51.1

interface Vlan52

no shutdown

ip address 10.10.52.3/24

hsrp version 2

hsrp 52

preempt

priority 110

ip 10.10.52.1

interface Vlan53

no shutdown

ip address 10.10.53.3/24

hsrp version 2

hsrp 53

preempt

priority 110

ip 10.10.53.1

interface Vlan54

no shutdown

ip address 10.54.0.3/20

hsrp version 2 hsrp 54 preempt priority 110 ip 10.54.0.1 ip dhcp relay address 10.10.51.21 ip dhcp relay address 10.10.51.22

interface port-channel10 description vPC-PeerLink switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type network

service-policy type qos input jumbo vpc peer-link

interface port-channel11 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 11

interface port-channel12 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type gos input jumbo

#### vpc 12

interface Ethernet1/1 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/2 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/3 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/4 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/5 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 11 mode active

interface Ethernet1/6 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 11 mode active interface Ethernet1/7 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 12 mode active

interface Ethernet1/8 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 12 mode active

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/26 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/27 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/28 switchport mode trunk switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/29 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/30 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/31 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/32 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

switchport access vlan 50

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0

vrf member management

ip address 10.29.132.20/24

clock timezone PST -8 0

clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60

line console

line vty

boot nxos bootflash:/nxos.7.0.3.I2.2d.bin