cisco.



Cisco HyperFlex 4.0 for Citrix VDI with VMware ESXi for up to 500 Users

Deployment Guide for Cisco HyperFlex 4.0 for Citrix VDI Using Stretch Cluster Converged Nodes for High Availability

Published: July 2021



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, go 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 DIS-CLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FIT-NESS 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 CIS-CO 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 PROFES-SIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, Giga-Drive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, Power-Panels, 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. (LDW_P1).

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)

© 2021 Cisco Systems, Inc. All rights reserved.

Contents

Executive Summary	4
Solution Overview	5
Technology Overview	7
Solution Design	34
Design Elements	43
nstallation	48
Vanagement	92
Validation	96
Build the Virtual Machines and Environment for Workload Testing	98
Test Setup and Configurations	191
Test Methodology and Success Criteria	193
Test Results	207
Summary	219
About the Author	220
Feedback	221

Executive Summary

To keep pace with the market, you need systems that support rapid, agile development processes. Cisco HyperFlex[™] 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 softwaredefined 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[™]).

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 500 VDI session workload on an 8-node Cisco HyperFlex system Stretch Cluster. We provide deployment guidance and performance data for Citrix Virtual Desktops 1912 LTSR virtual desktops running Microsoft Windows 10 with Office 2016 and Windows Server 2019 for HSD. The solution is a pre-integrated, best-practice data center architecture built on the Cisco Unified Computing System (Cisco UCS), the Cisco Nexus[®] 9000 family of switches and Cisco HyperFlex Data Platform software version 4.0.2b.

The solution payload is 100 percent virtualized on Cisco HyperFlex HXAF220C-M5SX hyperconverged nodes booting through on-board M.2 SATA SSD drive running VMware hypervisor and the Cisco HyperFlex Data Plat-form storage controller virtual machine. The virtual desktops are configured with Virtual Desktops 1912 LTSR, which incorporates both traditional persistent and non-persistent virtual Windows 10 desktops, hosted applications, and remote desktop service (RDS) Microsoft Server 2019 based desktops. The solution provides unparalleled scale and management simplicity. Citrix Virtual Desktops Provisioning Services or Machine Creation Services Windows 10 desktops, full clone desktops or Virtual Apps 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.

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

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 Stretch Cluster system running three different Citrix Virtual Desktops/Virtual Apps workloads with Cisco UCS 6400 series Fabric Interconnects and Cisco Nexus 9000 series switches.

Documentation Roadmap

For the comprehensive documentation suite, refer to the following for the Cisco UCS HX-Series Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/HX_D ocumentation_Roadmap/HX_Series_Doc_Roadmap.html



A login is required for the Documentation Roadmap.

For more information about Hyperconverged Infrastructure, go to: http://hyperflex.io

Solution Summary

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

Figure 1. HyperFlex System Overview



The following are the components of a Cisco HyperFlex system using the VMware ESXi Hypervisor:

- One pair of Cisco UCS Fabric Interconnects, choose from models:
 - Cisco UCS 6454 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
- VMware vSphere ESXi Hypervisor
- VMware vCenter Server (end-user supplied)

Technology Overview

Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that unites compute, network, and storage access. The platform, optimized for virtual environments, is designed using open industry-standard technologies and aims to reduce total cost of ownership (TCO) and increase business agility. The system integrates a low-latency, lossless 10 Gigabit Ethernet, 25 Gigabit Ethernet or 40 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. It is an integrated, scalable, multi chassis platform in which all resources participate in a unified management domain.

The main components of Cisco Unified Computing System are:

- Computing: The system is based on an entirely new class of computing system that incorporates rackmount and blade servers based on Intel Xeon Processors.
- Network: The system is integrated onto a low-latency, lossless, 10-Gbps, 25-Gbps or 40-Gbps unified network fabric, with an option for 100-Gbps uplinks. This network foundation consolidates LANs, SANs, and high-performance computing networks which are often separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- Virtualization: The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- Storage access: The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying storage access, the Cisco Unified Computing System can access storage over Ethernet, Fibre Channel, Fibre Channel over Ethernet (FCoE), and iSCSI. This provides customers with their choice of storage protocol and physical architecture, and enhanced investment protection. In addition, the server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity, and management for increased productivity.
- Management: The system uniquely integrates all system components which enable the entire solution to be managed as a single entity by the Cisco UCS Manager (UCSM). The Cisco UCS Manager has an intuitive graphical user interface (GUI), a command-line interface (CLI), and a robust application programming interface (API) to manage all system configuration and operations. Cisco UCS can also be managed by Cisco Intersight, a cloud-based management and monitoring platform which offers a single pane of glass portal for multiple Cisco UCS systems across multiple locations.

The Cisco Unified Computing System is designed to deliver:

- A reduced Total Cost of Ownership and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.

- A cohesive, integrated system which unifies the technology in the data center. The system is managed, serviced, and tested as a whole.
- Scalability through a design for hundreds of discrete servers and thousands of virtual machines and the capability to scale I/O bandwidth to match demand.
- Industry standards supported by a partner ecosystem of industry leaders.

Cisco UCS Fabric Interconnect

The Cisco UCS Fabric Interconnect (FI) is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. Depending on the model chosen, the Cisco UCS Fabric Interconnect offers line-rate, low-latency, lossless Ethernet, Fibre Channel over Ethernet (FCoE) and Fibre Channel connectivity. Cisco UCS Fabric Interconnects provide the management and communication backbone for the Cisco UCS C-Series, S-Series and HX-Series Rack-Mount Servers, Cisco UCS B-Series Blade Servers, and Cisco UCS 5100 Series Blade Server Chassis. All servers and chassis, and therefore all blades, attached to the Cisco UCS Fabric Interconnects become part of a single, highly available management domain. In addition, by supporting unified fabrics, the Cisco UCS Fabric Interconnects provide both the LAN and SAN connectivity for all servers within its domain. The product family supports Cisco low-latency, lossless Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over the Ethernet fabric from the servers to the uplinks. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

Cisco UCS 6454 Fabric Interconnect

The Cisco UCS 6454 54-Port Fabric Interconnect is a One-Rack-Unit (1RU) 10/25/40/100 Gigabit Ethernet, FCoE and Fibre Channel switch offering up to 3.82 Tbps throughput and up to 54 ports. The switch has 28 10/25-Gbps Ethernet ports, 4 1/10/25-Gbps Ethernet ports, 6 40/100-Gbps Ethernet uplink ports and 16 unified ports that can support 10/25-Gbps Ethernet ports or 8/16/32-Gbps Fibre Channel ports. All Ethernet ports are capable of supporting FCoE. Cisco HyperFlex nodes can connect at 10-Gbps or 25-Gbps speeds depending on the model of Cisco VIC card in the nodes and the SFP optics or cables chosen.





Cisco HyperFlex HX-Series Nodes

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

Figure 3. HXAF220c-M5SX All-Flash Node



Cisco HyperFlex HXAF220c-M5SX All-Flash Node

This small footprint Cisco HyperFlex all-flash model contains a 240 GB M.2 form factor solid-state disk (SSD) that acts as the boot drive, a 240 GB housekeeping SSD drive, either a single 375 GB Optane NVMe SSD, a 1.6 TB NVMe SSD or 1.6 TB SAS SSD write-log drive, and six to eight 960 GB or 3.8 TB SATA SSD drives for storage capacity. For configurations requiring self-encrypting drives, the caching SSD is replaced with an 800 GB SAS SED SSD, and the capacity disks are also replaced with 960 GB or 3.8 TB SED SSDs.

Figure 4. HXAF220c-M5SX All-Flash Node



In HX-series all-flash nodes either a 375 GB Optane NVMe SSD, a 1.6 TB SAS SSD or 1.6 TB NVMe SSD caching drive may be chosen. While the Optane and NVMe options can provide a higher level of performance, the partitioning of the three disk options is the same, therefore the amount of cache available on the system is the same regardless of the model chosen. Caching amounts are not factored in as part of the overall cluster capacity, only the capacity disks contribute to total cluster capacity.

Cisco HyperFlex HX220c-M5SX Hybrid Node

This small footprint Cisco HyperFlex hybrid model contains a minimum of six, and up to eight 2.4 terabyte (TB), 1.8 TB or 1.2 TB SAS hard disk drives (HDD) that contribute to cluster storage capacity, a 240 GB SSD house-keeping drive, a 480 GB or 800 GB SSD caching drive, and a 240 GB M.2 form factor SSD that acts as the boot drive. For configurations requiring self-encrypting drives, the caching SSD is replaced with an 800 GB SAS SED SSD, and the capacity disks are replaced with 1.2TB SAS SED HDDs.

Figure 5. HX220c-M5SX Node

Vererererererer			
	diala cisco	HyperFlex	-
			-

- 199
A DECK OF A

Either a 480 GB SATA or 800 GB SAS caching SSD may be chosen. This option is provided to allow flexibility in ordering based on product availability, pricing, and lead times. While the SAS option may provide a slightly higher level of performance, the partitioning of the two disk options is the same, therefore the amount of cache available on the system is the same regardless of the model chosen. Caching amounts are not factored in as part of the overall cluster capacity, only the capacity disks contribute to total cluster capacity.

Cisco VIC 1457 MLOM Interface Cards

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

The Cisco UCS VIC 1457 is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 10-Gbps or 25-Gbps Ethernet and FCoE, where the speed of the link is determined by the model of SFP optics or cables used. The card can be configured to use a pair of single links, or optionally to use all four links as a pair of bonded links. The Cisco UCS VIC 1457 is used in conjunction with the Cisco UCS 6454 model Fabric Interconnect.

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

Figure 6. Cisco VIC 1457 mLOM Card



Cisco HyperFlex Data Platform Software

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

• **Data protection** creates multiple copies of the data across the cluster so that data availability is not affected if single or multiple components fail (depending on the replication factor configured).

- **Stretched clusters** allow nodes to be evenly split between two physical locations, keeping a duplicate copy of all data in both locations, thereby providing protection in case of an entire site failure.
- **Logical availability zones** provide multiple logical grouping of nodes and distributes the data across these groups in such a way that no single group has more than one copy of the data. This enables enhanced protection from node failures, allowing for more nodes to fail while the overall cluster remains online.
- **Deduplication** is always on, helping reduce storage requirements in virtualization clusters in which multiple operating system instances in guest virtual machines result in large amounts of replicated data.
- **Compression** further reduces storage requirements, reducing costs, and the log-structured file system is designed to store variable-sized blocks, reducing internal fragmentation.
- **Replication** copies virtual machine level snapshots from one Cisco HyperFlex cluster to another, to facilitate recovery from a cluster or site failure, via a failover to the secondary site of all VMs.
- **Encryption** stores all data on the caching and capacity disks in an encrypted format, to prevent accidental data loss or data theft. Key management can be done using local Cisco UCS Manager managed keys, or third-party Key Management Systems (KMS) via the Key Management Interoperability Protocol (KMIP).
- **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 duplicate virtual storage volumes so that virtual machines can be cloned simply through metadata operations, with actual data copied only for write operations.
- **Snapshots** help facilitate backup and remote-replication operations, which are needed in enterprises that require always-on data availability.

Cisco HyperFlex Connect HTML5 Management Web Page

An HTML 5 based Web UI named HyperFlex Connect 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: <a href="http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://<hyperhaustrators.http://state.http://



Figure 7. HyperFlex Connect GUI

Cisco Intersight Cloud Based Management

Cisco Intersight (<u>https://intersight.com</u>) 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, and can be used to deploy and manage Cisco HyperFlex clusters. Cisco Intersight offers direct links to Cisco UCS Manager and Cisco HyperFlex Connect for systems it is managing and monitoring. The Cisco Intersight website and framework is being constantly upgraded and extended 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. This unique combination of embedded and online technologies results in a complete cloud-based management solution that can care for Cisco HyperFlex throughout the entire lifecycle, from deployment through retirement.





Cisco HyperFlex HX Data Platform Administration Plug-in

The Cisco HyperFlex HX Data Platform is also administered secondarily through a VMware vSphere web client plug-in, which is either deployed automatically by the Cisco HyperFlex installer or the HTML 5 plugin can be downloaded separately from CCO.

vm vSphere Client	Menu 🗸 🛛 🔍 Search in all environ	iments			C ©~	Administraton@VSPHE	
Cisco HyperFlex	← 畿 hx1scip Summary Events Alarms	s Datastore					hx1scip ~
	hxtscip Total Nodes Datastore HyperFlex Version Model vCenter Cluster ESXI Version Uptime	8 2 4.0(2d) HXAF220C-MSSX hxfscip VMware ESXi 6.7.0 U3 (16316930) 7 days, 2 hours, 24 minutes				Storage	3.93%
	Status		^	Network Details			~
	Operational Status	0% Online					
	V Resiliency Status	S Healthy	G				
	Host(s) failure can be tolerated	2					
	Replication Factor	Four Copies					
	Creation Time	1 Dec 2020 157 32 PM					
	Persistent Device failures tolerable	3					
	Caching Device failures tolerable	â					
	√ Nodes	8					
	Node Type	Converged					
	Version	4.0(2d)					
	Capacity		^				
	Total						

Figure 9. HyperFlex Web Client Plugin

Cisco HyperFlex HX Data Platform Controller

A Cisco HyperFlex HX Data Platform controller resides on each node and implements the distributed file system. The controller runs as software in user space within a virtual machine, and intercepts and handles all I/O from the guest virtual machines. The Storage Controller Virtual Machine (SCVM) uses the VMDirectPath I/O feature to provide direct PCI passthrough control of the physical server's SAS disk controller, or direct control of the PCI attached NVMe based SSDs. This method gives the controller VM full control of the physical disk resources, utilizing the SSD drives as a read/write caching layer, and the HDDs or SDDs as a capacity layer for distributed storage. The controller integrates the data platform into the VMware vSphere cluster through the use of three preinstalled VMware ESXi vSphere Installation Bundles (VIBs) on each node:

- **IO Visor:** This VIB provides a network file system (NFS) mount point so that the ESXi hypervisor can access the virtual disks that are attached to individual virtual machines. From the hypervisor's perspective, it is simply attached to a network file system. The IO Visor intercepts guest VM IO traffic, and intelligently redirects it to the HyperFlex SCVMs.
- VMware API for Array Integration (VAAI): This storage offload API allows vSphere to request advanced file system operations such as snapshots and cloning. The controller implements these operations via manipulation of the filesystem metadata rather than actual data copying, providing rapid response, and thus rapid deployment of new environments.

 stHypervisorSvc: This VIB adds enhancements and features needed for HyperFlex data protection and VM replication.

Cisco HyperFlex HX Stretch Clusters

This section provides an overview of Cisco HyperFlex stretch clusters. It details some of the business reasons for deploying such a cluster. It also discusses some of the physical limitations of such a cluster.

What is a Stretch Cluster?

A stretch cluster is distinct from a non-stretch, or normal, cluster, in that it is designed to offer business continuance in the event of a significant disaster at a data center location. A stretch cluster is geographically redundant, meaning that part of the cluster resides in one physical location and another part resides in a second location. The cluster also requires a "tie breaker" or "witness" component, which should reside in a third, separate location. The goal of this design is to help ensure that the virtual infrastructure remains available even in the event of the complete loss of one site. Of course, many lesser types of failures also can occur, and the system is highly available in the event of these as well. All of these scenarios are discussed later in this document.

People often mistakenly think that a stretch cluster is a set of multiple single clusters. This is not the case. A stretch cluster is, in fact, a single distributed entity and behaves as such in most circumstances. There are a few differences between a normal cluster and a stretch cluster, however. These arise solely from the fact that a stretch cluster must meet some special requirements to provide geographical redundancy for deployments that require it. Georedundancy introduces a few new requirements for the cluster so that certain conditions, such as split brain and node quorum, are handled properly. These are discussed in the following sections.

Figure 10 shows the main features of a stretch cluster.

Figure 10. Three Main Components of a Stretch Cluster Deployment





The following are the characteristics of a stretch cluster:

- A stretch cluster is a single cluster with nodes geographically distributed at different locations.
- Storage is mirrored locally and across each site (but not to the tie-breaker witness).
- Sites need to be connected over a low-latency network to meet the write requirements for applications and for a good end-user experience.
- Geographic failover (virtual machine) is like failover in a regular cluster.
- Node failure in a site is like node failure in a regular cluster.

- Split brain is a condition in which nodes at either site cannot see each other. This condition can lead to problems if a node quorum cannot be determined (so that virtual machines know where to run). Split brain is caused by:
 - Network failure
 - Site failure
- Stretch clusters have a witness: an entity hosted on a third site that is responsible for deciding which site becomes primary after a split-brain condition.

Businesses Need a Stretch Cluster

Businesses require planning and preparation to help ensure business continuity after serious incidents or disasters and to resume normal operations within a reasonably short period. Business continuity is the capability of an organization to maintain essential functions during, as well as after, a disaster. It includes three main elements:

- **Resilience:** Critical business functions and the supporting infrastructure must be designed so that that they are materially unaffected by relevant disruptions: for example, through the use of redundancy and spare capacity.
- **Recovery:** Organizations must have in place arrangements to recover or restore critical and less critical business functions that fail for some reason.
- Contingency: An organization must establish a generalized capability and readiness to allow it cope effectively with whatever major incidents and disasters may occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

Stretch Cluster Physical Limitations

Some applications, specifically databases, require write latency of less than 20 milliseconds (ms). Many other applications require latency of less 10 ms to avoid problems with the application. To meet these requirements, the round-trip time (RTT) network latency on the stretch link between sites in a stretch cluster should be less than 5 ms. The speed of light (3e8 m/s) at the maximum recommended stretch cluster site distance of 100 km (approximately 62 miles) introduces about 1 ms of latency by itself. In addition, time is needed for code path and link hops (from node to fabric interconnect to switch), which also plays a role in determining the maximum site-to-site recommended distance.

Solution Components

A traditional Cisco HyperFlex single-cluster deployment consists of HX-Series nodes in Cisco UCS connected to each other and the upstream switch through a pair of fabric interconnects. A fabric interconnect pair may include one or more clusters. A stretch cluster requires two independent Cisco UCS domains: one for each site. There-fore, a total of four fabric interconnects (two pairs) are required for a stretch cluster. Other clusters can share the same fabric interconnects.

Figure 11 and Figure 12 show typical physical layouts for this kind of deployment. Figure 11 shows a single site with its cabling and independent Cisco UCS domain. Figure 12 shows the racks for site A and site B in a stretch cluster with their respective fabric interconnects and upstream switches. This is an 8-node (4+4) stretch cluster with Cisco HyperFlex HX220c nodes at each location.

Figure 11. Site a for a Stretch Cluster Deployment Showing a Single-Site Rack: the Site Contains 4 HX220c M5 Nodes and 2 Fabric Interconnects with a Single Uplink Switch for the Stretch Layer 2 Network Connecting to Site B





Figure 12. Rack Diagram Showing Site A and Site B with their respective Fabric Interconnects and a Logical Third Site at Another Location for the Stretch Cluster Witness

Stretch Cluster Architecture

This section discusses the specific deployment needs for a stretch cluster, including hardware, networking configuration, VMware requirements (ESXi and vCenter), failure sizing, and characteristics of the witness (Figure 13). VMware vSphere Enterprise Plus is required because Cisco HyperFlex stretch clusters rely on advanced DRS capabilities available only in that premium edition. The requirements are the same across all stacks (even for non-hyperconverged infrastructure [HCI] or traditional storage) that implement stretch or metropolitan clusters on VMware.



Figure 13. General Stretch Cluster Network

The first consideration in deploying a stretch cluster is building the proper site-to-site network. A stretch cluster requires a minimum of 10 Gigabit Ethernet connectivity and 5-ms RTT latency on the link. The link needs to be stretch Layer 2 to help ensure network space adjacency for the data storage VLAN network that is used for storage communication. The network between sites requires the following characteristics:

- 10 Gbps (dedicated) for the storage data VLAN.
- 5-ms RTT latency between the two active sites.
- Data VLAN and management VLAN on a stretch Layer 2 VLAN.
- Stretch Layer 2 VLAN between the two sites:
 - Dark fiber and dense wavelength-division multiplexing (DWDM) Layer 2 and 3 technologies are supported.
 - The solution is not currently qualified for Virtual Extensible LAN (VXLAN) unless used with ACI.
 - Stretch Layer 2 characteristics.

- The stretch data VLAN should use jumbo maximum transmission units (MTUs) for best performance. The installer allows for deployment using an MTU of 1500, however.
- The Cisco Nexus[®] 5000 Series Switches are slightly different than the Cisco Nexus 7000 and 9000 Series Switches. The default network-QoS policy does not accept jumbo MTUs, but you can set up jumbo switch policy across the switches.
- Test the RTT ping using VMkping -I VMk1 -d -s 8972 x.x.x from any ESXi host in your cluster. This check is also performed by the installer, and if it fails, the installation process will not proceed.
- 100 Mbps and 100-ms RTT latency between the active sites and the witness site.
- Different drives types are supported with different nodes limits. See the release notes for your running or target version to determine which drives and nodes you can use. For example, there are LFF drive restrictions and NVME drives began support in 4.0.2x and onward for the HX220 node type.

Deployment Prerequisites

Some deployment prerequisites exist for stretch clusters related to the qualified hardware. Most of these prerequisites are not based on technical factors but simply reflect test bandwidth and the release cycle. After these items have been qualified, they will be removed from the unsupported-features list, and these capabilities will be available for general deployment.

Æ

Check the minor version release notes periodically for changes in the support listings.

Minimum and maximum configuration limitations are as follows:

- Minimum
 - Two fabric interconnects per site
 - Two nodes per site
 - One witness
 - One vCenter instance
 - Replication factor: 2+2
- Maximum
 - Two fabric interconnects per site
 - · 2:1 maximum ratio for compute to converged nodes
 - · Compute nodes can be added asymmetrically with no restriction
 - 16 small-form-factor (SFF) converged nodes per site (32 total, max cluster 64 with compute)
 - 8 large-form-factor (LFF) converged nodes per site (16 total, max cluster 48 with compute)
 - One witness
 - One vCenter or vCenter with HA instance if there is no database update lag
 - Replication factor: 2+2

Stretch cluster support prerequisites are as follows:

• Self-encrypting drives (SEDs) are not supported.

- Compute-only nodes are supported in HyperFlex 3.5 or higher with a 2:1 ratio to converged nodes. Verify the ratio in the Release Notes for your version.
- ESXi is the only supported hypervisor at this time. Check the release notes for your HX version to see the recommended ESXi version.
- Cisco HyperFlex native replication is supported in HyperFlex 3.5 and greater.
- Expansion of an existing cluster to a stretch cluster is not supported.
- Stretch clusters are supported only in fresh installations. Upgrade from a standalone cluster to a stretch cluster configuration is not supported.
- Stretch Clusters must be symmetric (converged nodes). For production environments, this includes Fabric Interconnects.
- Stretch Clusters must be expanded symmetrically (converged nodes). See the admin guide for your version of HX for workflow details.
- Stretch Clusters can be built and/or expanded asymmetrically with compute nodes.
- Online rolling upgrades are supported only for the HX Data Platform. Cisco UCS Manager upgrades must be performed manually one node at a time.
- Stretch clusters are supported on Cisco M5 nodes only. M4 nodes are not supported.
- Logical availability zones are not currently supported in stretch clusters.
- The witness requires ESXi at the third site (cloud deployment is not currently supported).
- Disk reshuffling is not supported (for example, adding empty nodes and "leveling" the disks out)
- Hardware offload (acceleration) cards are supported starting in HXDP version 4.0.2b and greater
- Node removal is not supported
- Single Socket nodes may or may not be supported, depending on your version of HX. Please see the Release Notes.

About Zones

While logical availability zones are not currently supported in stretch cluster deployments, you may notice that zone information is available when running the stcli cluster get-zone command as show below:

```
root@SpringpathControllerOHCWUK9X3N:~# stcli cluster get-zone
zones:
    _____
pNodes:
    state: ready
    name: 192.168.53.136
    ______
state: ready
```

```
name: 192.168.53.135
       _____
  zoneId: 51733a6b98df9784:4f8fc27070894bf4
  numNodes: 2
  _____
  pNodes:
     _____
     state: ready
     name: 192.168.53.138
     _____
     state: ready
     name: 192.168.53.137
      _____
  zoneId: 7b04a6600e3e3ee5:54c7224773a14a9a
  numNodes: 2
  _____
isClusterZoneCompliant: True
zoneType: physical
isZoneEnabled: True
numZones: 2
```

LAZ and stretch cluster both are implemented using a basic feature called "zones" and that's why you see 'zone' in some of the output. You will not see "logical zones" which is what would appear under LAZ.

note the "zoneType" on the get-zone output.

On stretch cluster: "zoneType: physical"

On Cluster with LAZ : "zoneType: logical"

Hardware Matching

Stretch Clusters require identical hardware at both sites. This includes node count, type, and drives per node as well. This also applies to expansion. You must expand in converged node pairs.

There are some exceptions to the hardware symmetry requirement. Compute resources are not required to be symmetric between sites. You can have more compute-only nodes on one site than the other. However, care should be taken since a failure scenario from one site with large compute resources to another site with reduced resources may not be sized properly to run the VMs that are started on the surviving site.

Mixing CPU generations is supported within the same family as well. For example, it is ok to mix 8180 Skylake CPUs with 6258R Cascade Lake CPUs. You must, however, size for the less powerful CPU.

A Stretch Cluster will work, such as, deploy properly and functional as expected, if the FIs are different between sites, but identical within the site. This can be useful for lab and testing environments but is not supported by Cisco for production. FIs must be identical within a site and between sites for production.

Overlay Networks

Only certain overlay networks are currently qualified for use with Stretch Clusters.

OTV is qualified for use with Stretch Cluster. This means however, that VXLAN and NSX are not supported as stand-alone overlay protocols. VXLAN is supported only with ACI. See the "More Information" section for the CVD describing this deployment.

Cisco Overlay Transport Virtualization (OTV), supported on Nexus Switches, is a networking technology that allows relaying layer 2 (L2) networks over layer 3 (L3) network segments. OTV is important for Stretch Clusters that require stretched L2 storage and management networks when a dedicated dark fiber type site-to-site connection is not available. The tested and validated OTV design is shown below.



This OTV design was tested for the various failure modes discussed later. It was configured to meet the bandwidth and latency requirements necessary for the proper operation of the Stretch Cluster. It is important to note that layering over L3 can introduce latency since the routed network will necessarily have additional device to device hops. When designing and deploying this type of architecture you must ensure that you are still within the site-to-site communication specification for bandwidth and latency.

The following references are for OTV on Cisco Nexus:

https://www.cisco.com/c/en/us/solutions/data-center-virtualization/overlay-transport-virtualizationotv/index.html https://community.cisco.com/t5/data-center-documents/understanding-overlay-transport-virtualization-otv/tap/3151502

Fabric Interconnects

Stretch clusters have a specific set of fabric interconnect requirements. Each site is built using its own pair of fabric interconnects in an independent Cisco UCS domain. Therefore, a total of four fabric interconnects are required. The stretch cluster requires a symmetric deployment, meaning that each site must have the same number and type of fabric interconnects and converged nodes. If site A has 4 hybrid nodes, then site B must also have 4 hybrid nodes. As of Cisco HyperFlex 3.0, the maximum cluster size is 8 nodes per site, for a total of 16 (8 + 8). This has increased in 3.5 and above to 16 converged nodes per site (SFF) with up to a 2:1 compute node ratio for a maximum mixed count of 32 per site. Limits for LFF drives are different. See the release notes for your version of HX to get the latest information on the number and type of supported nodes.

Fabric interconnect and node configuration details are as follows:

- A total of four fabric interconnects are required, one pair at each site) in unique Cisco UCS domains.
- Do not mix fabric interconnect models within a domain.
- For the fabric interconnects, Cisco UCS Manager Release 3.2(3e) is required.
- Existing fabric interconnects are supported as long as they work with Cisco M5 nodes.
- Node requirements are as follows:
 - You must have the same number and type of nodes per site: All flash or all hybrid.
 - The maximum cluster size is 16 converged nodes per site starting in 3.5 with a 2:1 maximum compute ratio (max 32 mixed nodes per site).
 - These requirements and maximums change frequently, consult the Release Notes for your version.

Fabric Interconnects Uplink Best Practices

Care should be taken with all deployments of HX when uplinking the Fabric Interconnects to your TOR/edge switches. The best practice surrounding this is designed to make sure that Spanning Tree Protocol (STP) loops are avoided. In a normal cluster these loops will cause FI takeover problems. Due to the multi-domain nature of a stretch cluster, STP storms can bring the system down. When uplinking the FIs to your redundant switches, the virtual port channel (VPC) ports should be set to edge trunk mode so that they do not participate in STP.

This behavior is called out in several location within Cisco documentation but is reiterated here for convenience. For example, the following document call out using spanning-tree port type edge trunk or the need to disable spanning tree on ports connecting to the FIs from upstream switches:

<u>https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/_Net-_</u>
 <u>work_External_Storage_Management_Guide/b_HyperFlex_Systems_Network_and_External_Storage_Manage-_</u>

ment Guide 3 0/b HyperFlex Systems Network and External Storage Management Guide 3 0 chap ter 01.html

Cisco FIs appear on the network as a collection of endpoints versus another network switch. Internally, the FIs do not participate in spanning-tree protocol (STP) domains, and the FIs cannot form a network loop, as they are

not connected to each other with a layer 2 Ethernet link. The upstream root bridges make all link up/down decisions through STP.

Uplinks need to be connected and active from both FIs. For redundancy, you can use multiple uplinks 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, make uplinks 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. This also 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 unavailable.

When setting the uplinks from the FI as VPC port channels you also need to set the downlink ports, for example, on the Cisco Nexus 9k, to "spanning tree edge" instead of "spanning tree normal", since the FIs don't participate in STP. In the absence of this configuration, a spanning tree storm in the N9k will cause a traffic blackhole for HX storage traffic. This in turn will affect all HX traffic in a stretch cluster. In standard clusters, the problem happens only when there is an FI failover.

In clusters without the ability to use vPC or LACP based link aggregation for redundancy, you should use disjoint layer 2.

VMware vCenter

VMware vCenter is a critical component for normal clusters and is vital for a stretch cluster. vCenter, with HA and DRS configured automatically manages virtual machine movement in the event of a site failure. The use of virtual machine host groups in the preferred mode, in which virtual machines are pinned to a site for the purpose of local computing and read I/O, is required for optimal performance in a stretch deployment. Site host groups and the corresponding affinities are created automatically at build time by the Cisco HyperFlex installer.

Data stores also maintain site affinity using host groups as the mechanism to locate the primary copy of virtual machine data. This approach is used to facilitate the asymmetric I/O mechanism that a stretch cluster uses to increase the cluster response time by localizing read I/O while distributing write I/O (two local-site copies and two remote-site copies). Because both sites in a stretch cluster are active, virtual machines at one site or the other do not suffer any "second-class citizen" type scenarios, in which one site has preferential performance relative to another.

In a stretch cluster deployment, a single instance of vCenter is used for both sites. The best approach is to locate this instance at a third location so that it is not affected by site loss. Co-residency with the witness is often the preferred choice because the witness site is required anyway. Nested vCenter (such as, running the cluster's vCenter instance on the cluster itself) is not supported. vCenter HA (VCHA) is supported with Stretch Cluster. Be aware the VCHA is a high availability deployment of vCenter itself and does not refer to the enabling HA on vCenter (which is a separate requirement for proper cluster failover behavior).

In the vCenter instance, the stretch cluster corresponds to a single ESXi cluster. Be sure to verify that HA and DRS are set up for the stretch cluster.

If the need arises to move the cluster from one vCenter to a new vCenter deployment or a different existing vCenter instance, it will be necessary to perform a cluster re-register. Be sure to see the admin guide for detailed notes, but the general workflow is as follows: Create the cluster object in the new vCenter instance and add the cluster ESXi hosts manually. Be sure the HA/DRS is enabled. The re-register is conducted using STCLI from any node or the CIP-M address.

admin@ControllerE2L5LYS7JZ:~\$ stcli cluster reregister

usage: stcli cluster reregister [-h] --vcenter-datacenter NEWDATACENTER

--vcenter-cluster NEWVCENTERCLUSTER

--vcenter-url NEWVCENTERURL

[--vcenter-sso-url NEWVCENTERSSOURL]

--vcenter-user NEWVCENTERUSER

stcli cluster reregister: error: argument --vcenter-datacenter is required

In a non-stretched cluster this is all that is required to remove the cluster from one vCenter instance and move it to a new one. A stretch cluster, however, requires a few manual steps to complete the process. This is because Host Groups and Affinity Rules are not transferred in the re-registration process. Please note that ICPM needs to be accessible between hosts and vCenter for re-registration to function properly.

A stretch cluster relies on a specific naming convention when interfacing with vCenter for implementation of the affinity rules. This is set up automatically, in advance, with the HX Installer when the cluster sites are built. The host group and affinity group naming must follow this convention: <site name>_{HostGroup, VmGroup, SiteAffinityRule} when rebuilding the groups and rules on the new vCenter host. See the screens below for an example. Here, site 1 is called fi47 and site 2 is fi48. Note the naming convention.

Sed1-cl	NS ~		
Summary Monitor C	configure Permissions Hosts VMs Datastores	Networks Updates	
 Services vSphere DRS vSphere Availability 	VM/Host Groups ♣ Add X Delete		▼ Filter
	Name	Туре	
Quickstart	即 fi47_VmGroup	VM Group	
General	fil47_HostGroup	Host Group	
Licensing	即 fi48_VmGroup	VM Group	
VMware EVC	filla_HostGroup	Host Group	
VM/Host Groups			
VM/Host Rules	🕂 Add 🔀 Remove		
VM Overrides	fi47_VmGroup Group Members		
Host Options	🕞 ubu-vdbench-852-1-clone4		
Host Profile	🕞 ubu2-fio-844-1-clone1		
I/O Filters	ubu2-fio-850-1-clone3		
▼ More	En under and an and a second started		

Sed1-cl Actions ~					
Summary Monitor C	onfigure Permissions	Hosts VMs Datast	ores Networks Update	es	
▼ Services	VM/Host Rules				
vSphere DRS	📕 Add 🕜 Edit 💙 Du	oloto			
vSphere Availability	Name	Type	Enabled	Conflicts	Defined By
Configuration Ouislatent	G fi47 AffinityPulo	Run V/Ms on Hosts	Voc	0	System
Quickstart	§ fi47_AmmityRule	Run VMs on Hosts	Ves	0	System
General	146_Annitykule	Run VIVIS ON HOSIS	res	0	System
Licensing					
VMware EVC					
VM/Host Bulos					
VM/Host Rules					
Host Options					
Host Profile	VM/Host Rule D	etails			
I/O Filters	Virtual Machines that are m	nembers of the VM Group show	uld run on hosts that are membe	ers of the Host Group.	
▼ More	🕂 Add 💥 Remove		🕂 Add 😒	Remove	

VMware vCenter HA Settings

The settings below are recommended for use in HX Stretch Clusters. This table details the most common settings in vSphere HA that are typically asked about during custom configuration. The screenshots are representative of vCenter 6.5. The cluster will work as designed using the default installation values. If you do not see a value listed below, keep it at the default.

vSphere HA	Turn on HA. Keep Pr	oactive HA disabled.				
	BASC-Purple - Edit Cluster Set	ttings				
	vSphere DRS	vSphere Availability				
	vSphere Availability Failures and Responses	vSphere Availability is comprised of v	Sphere HA and Proactive HA. To	o enable Proactive HA you must also enable DRS on the cluster.		
	Proactive HA Failures	✓ Turn ON vSphere HA				
	and Responses	Turn on Proactive HA 0				
	Heartbeat Datastores	Failure	Response	Details		
	Advanced Options	Hostfailure	 Restart VMs 	Restart VMs using VM restart priority ordering.		
		Proactive HA	Disabled	Proactive HA is not enabled.		
		Host Isolation	Disabled	VMs on isolated hosts will remain powered on.		
		Datastore with Permanent Device Loss	Disabled	Datastore protection for All Paths Down and Permanent Device Loss is disabled.		
		Datastore with All Paths Down	Disabled	Datastore protection for All Paths Down and Permanent Device Loss is disabled.		
		Guest not heartbeating	Disabled	VM and application monitoring disabled.		

Image: HXSC-Purple - Edit Cluster Settings vSphere DRS vSphere Availability Failures and Responses Proactive HA Failures and Responses Proactive HA Failures and Responses Admission Control Heartbeat Datastores Advanced Options	?
vSphere DRS Failure conditions and responses vSphere Availability Failures and Responses Proactive HA Failures and Responses You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure condition to host isolation, VM component protection (datastore with PDL and APD), VM and application. Proactive HA Failures and Responses Admission Control Heartbeat Datastores Host Failure Response Advanced Options Response for Host Isolation Datastore with PDL Disabled	
Failures and Responses host is olation, VM component protection (datastore with PDL and APD), VM and application. Proactive HA Failures and Responses Admission Control Heartbeat Datastores Host Failure Response Advanced Options Response for Host Isolation Datastore with PDL Disabled	s are supported: host,
and Responses Admission Control Host Failure Response Restart VMs Response for Host Isolation Disabled Datastore with PDL Disabled T Disabled	
Heartbeat Datastores Response for Host Isolation Disabled Disabled > Datastore with PDL Disabled	
Advanced Options Datastore with PDL Disabled T	
► Datastore with APD Disabled ▼	
► VM Monitoring Disabled ▼	
Virtual Machine Customer Preference – Disabled by default	
HXSC-Purple - Edit Cluster Settings	(?) }
vSphere DRS vSphere Availability Response delay: 3 * minutes	
Failures and Responses VM Monitoring	
Proactive HA Failures and Responses Enable heartbeat monitoring VM monitoring resets individual VMs if their VMware tools heartbeats are not rec time. Application monitoring resets individual VMs if their in-guest heartbeats are	eived within a set not received
Admission Control within a set time.	
Advanced Options Turns on VMware tools heartbeats. When heartbeats are not received within uest OS is restarted	a set time, the
Application Monitoring	
Turns on application heartbeats. When heartbeats are not received within a s OS is restarted.	et time, the guest
Heartbeat monitoring sensitivity O Preset Low — High	
⊙ Custom	
Failure interval 30 seconds	
Minimum uptime 120 - seconds	
Maximum per-vivi resets 3	
Maximum resets time window	
	-
	OK Cancel

Feilure	Light monitoring is one	blad Deeperson for LL	est legistion is est to Dewar off	and Dectort \/Ma Far		
conditions and	PDL and APD, select F	Power off and Restart	from the drop-down lists.	and Restart VIVIS. For		
VM Response	HXSC_Purple - Edit Cluster Settings		•	2 1		
	venhorn DP s	Follow and these and management		0 "		
	vSphere Availability	Failure conditions and responses				
	Failures and Responses You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.					
	Proactive HA Failures and Responses	🗹 Enable Host Monitoring 🚯				
	Admission Control	 Host Failure Response 	Restart VMs 🔹			
	Heartbeat Datastores	Response for Host Isolation	Power off and restart VMs			
	Advanced Options	 Datastore with PDL 	Power off and restart VMs			
		 Datastore with APD 	Power off and restart VMs (conservative)			
		▶ VM Monitoring	Disabled 🔹			
				OK Cancel		
	<u> </u>					
Admission Control	Set to disable					
Datastore	"Use datastores only f	rom the specified list"	' and select HX datastores.			
Heartbeats						
	nttps://kb.vmware.cor	<u>n/s/article/2004/39</u>				
	- Datastore for Heartbeating	g				
		vSphere HA uses network has faile and datastore pre Heartbeat datast	datastores to monitor hosts and virtual d. vCenter Server selects two datastores eferences specified below. ore selection policy:	machines when management for each host using the policy		
		Automatically Automatically	select datastores accessible from the no	351		
		Use datastore	es from the specified list and complement	nt automatically if needed		
		Use datastores from the specified list and complement automatically if neede				
		Name	Datastore Cluster	Hosts Mountion Datastore		
		name		Tore mounting parasone		
Advanced Settings						
das.usedefaultisc	plationaddress False					

das.isolationaddress0	IP address for Management Network Gateway
das.isolationaddress1	Existing IP address that is outside cluster. Do not use FI VIPs, Cluster IP (CIP), or cluster host IP

Witness Configuration

A quorum is the minimum number of votes that a distributed transaction must obtain to be allowed to perform an operation in a distributed system. A quorum-based technique is implemented to enforce consistent operation in a distributed system. The witness node serves this function. In the event of a split-brain condition, in which both sites are still available but unable to communicate with each other, a virtual machine site leader must be established so that two instances of the same virtual machine are not brought online by HA.

The witness is deployed at a third site and is delivered as an open virtual appliance (OVA) file for use in an infrastructure ESXi deployment at that location. The witness runs an instance of ZooKeeper and becomes a cluster member and contributes its vote when needed to break a tie.

The witness node must have the following characteristics:

- A third independent site is needed to host the witness virtual machine.
- IP address and connectivity for the witness virtual machine is needed to each stretch cluster site.
- The witness must be on a routable Layer 3 network.
- The minimum requirements for the witness node are as follows:
 - Virtual CPUs (vCPUs): 4
 - Memory: 8 GB
 - Storage: 40 GB
 - HA: Optional for the witness node
- Latency of at most 100-ms RTT to each site is required.
- Bandwidth of at least 100 Mbps to each site is required.
- For fastest site-to-site failover times, an RTT latency to the witness of less than 10ms is optimal.
- The node must be deployed separately before the Cisco HyperFlex installer stretch cluster workflow is run.
- The witness behaves as a quorum node, if you are reinstalling the cluster the witness must be reinstalled as well.

There is one witness per cluster. Multiple clusters cannot use the same witness.

While no user data is being sent between the sites and the witness, some storage-cluster metadata traffic is transmitted to the witness site. This traffic is the reason for the 100-Mbps requirement and is in line with competitive products. The witness connection to each site requires 100 Mbps bandwidth with a 100 ms RTT in order to function properly. It is recommended to use a connection with a 100 ms latency for proper system failover behavior. For large clusters and for the best site-to-site failover performance, Cisco recommends witness-to-site latency on the order of 10 ms.

The witness is currently not supported in cloud deployments because of testing limitations. The OVA file has been tested and is supported for the ESXi platform.

If you need to patch the witness virtual machine for any reason, you can take the witness offline temporarily, implement the update, and bring the witness back online. Cisco recommends that you stage this process and practice it on a test witness to help ensure timely reintroduction of the production system when you implement the actual update. The cluster must be in a healthy condition to conduct this operation. If you need assistance, please contact the Cisco Technical Assistance Center (TAC).

I/O Path in a Stretch Cluster

A stretch cluster is in active-active mode at each site: that is, primary copies and read traffic occur for each virtual machine at each site. There is no concept of an active-standby configuration in a stretch cluster. IO Visor, the Cisco HyperFlex file system proxy manager, dictates which nodes service which read and write requests. In general, a stretch cluster behaves the same way as a normal cluster with modifications for host affinity and certain failure scenarios (see section <u>Stretch Cluster Failure Modes</u>). With virtual machine affinity and a replication factor of 2 + 2, the read and write dynamics are as described in the following sections.

Read Path

Taking advantage of the host group affinity, all read operations for virtual machine data are served locally, meaning that they come from the nodes at the site to which the data store for the virtual machine is assigned. Read operations are first serviced by the node cache if they are available there. If they are not available, they are read from persistent disk space (in a hybrid node) and served to the end user. The read cache in a stretch cluster behaves the same way as in a normal hybrid or all-flash cluster with the exception of local service based on host affinity.

Write Path

Write operations in a stretch cluster are a little more complicated than read operations. This is the case because to achieve data integrity, a write operation is not acknowledged as committed to the virtual machine guest operating system until all copies, local and remote, are internally committed to disk. This means that a virtual machine with affinity to site A will write its two local copies to site A while synchronously writing its two remote copies to site B. Again, IO Visor determines which nodes are used to complete each write operation.

The Cisco HyperFlex file system waits indefinitely for write operations to be acknowledged from all active copies. Thus, if certain nodes or disks that host a copy of data for which a write operation is being implemented are removed, write operations will stall until a failure is detected (based on a timeout value of 10 seconds) or the failure heals automatically without detection. There will be no inconsistency in either case.

I/O operations from virtual machines on site A will be intercepted by IO Visor on site A. IO Visor on site B is not be involved. The write I/O operations are replicated to site B at the data platform level. In the event of virtual machine migration from one site to another–for example, through VMware Storage vMotion from site A to another data store with affinity to site B–IO Visor will conduct a hand-off. When a virtual machine migrates to site B, IO Visor on site B will intercept the I/O operations. This procedure is also part of the virtual machine failover process internally. After the virtual machines have migrated from site A to site B, virtual machine I/O operations will not be intercepted by the site A IO Visor, but rather by the site B IO Visor.

Sizing

Typically, you start sizing exercises by profiling the workload or already knowing the requirements for the virtual machines that you need to run. However, you come by this information, the next step is to use a sizing tool (un-

less you want to do the math yourself). Cisco provides a sizing tool that can run workload estimates for a stretch cluster with a typical VSI profile:

Cisco HyperFlex sizer tool: https://HyperFlexsizer.cloudapps.cisco.com/ui/index.html#/scenario

Sizing a stretch cluster requires an understanding of the replication factor used for data protection. Each site runs a replication factor of 2: that is, each site has is a primary copy and a replica. Each site also runs a replication factor of 2 for the complementary site, so that for each virtual machine, across both sites, there is a primary copy and three replicas: equivalent to a replication factor of 4. This configuration is required so that any individual site can tolerate the loss of its complementary site and still be able to run. Note that the loss of a site and does not guarantee the ability of the surviving site to tolerate a disk or node loss because the affected node might be a zookeeper node. When the cluster is created, a zookeeper leader is elected at a given site. The leader is used to make updates to the ensemble. In the event of a site or zookeeper leader failure, a new leader is elected. This is not configurable.

Survivability while maintaining online status requires a majority zookeeper quorum and more than 50% of nodes (the witness counts as both an active zookeeper node). It is possible that the surviving site could tolerate a node or disk loss (in a cluster greater than 2+2) if that node is not a zookeeper node, but it is not guaranteed.

The data protection and workload profile (I/O requirement) considerations allow you to determine the number and type of disks required to meet your capacity needs. You then need to determine the node count needed to meet your vCPU and virtual machine memory needs.

Here are some sizing guidelines:

- For VSI an option is available in the sizer for selecting the stretch cluster. Use this option for your sizing exercises.
- In general, a stretch cluster uses a replication factor of 4: that is, replication factor 2 + replication factor 2 (a replication factor of 2 at each site with full replication to the complementary site, also at a replication factor of 2). This configuration effectively results in a replication factor of 4.
- You can use a replication factor of 2 for one site and then apply the same factor to the second site. If you
 want to be able to run all workloads from either site, then you must be sure that you have enough capacity
 at each site by accounting for the overall workloads and thresholds. The sizer automatically performs this
 verification for you.
- Consider the virtual machine and vCPU capacity: everything must be able to run comfortably at one site.
- The total virtual machine vCPU capacity is required.
- The total virtual machine memory capacity is required.

Failure Sizing

It is not enough to size your deployment for normal operations. Ideally, you should size your deployment for a scenario in which you have lost a site and the surviving site has lost a non-zookeeper node. This is the worst-case continuous-operation scenario for resource distribution to your overall virtual machine workload. Everything must be able to run comfortably on one site for a stretch cluster deployment to offer true business continuance in the event of a disaster.

If it is sufficient to run only certain virtual machines at the surviving site, you may be able to undersize the system, but you need to be aware of this and take it into consideration when planning disaster-recovery runbooks. Keep in mind that the automated recovery mechanism of the stretch cluster will launch virtual machines from failed sites without user intervention. You may find yourself in a situation in which you need to turn off failover virtual machines if they exceed the capacity of the surviving site.

Bandwidth Considerations for the Inter-Site Link Based on Workloads

Read bandwidth is normally local only, so there is no dependence or impact on the site-to-site link. Non-local VMs, such as, VMs running on nodes that do not have the assigned datastore affinity, will incur link read traffic. This is not the typical situation but should be considered in corner-case scenarios.

Write bandwidth is necessarily relevant to the link: Replicas traverse the link (2 copies). There is also meta data overhead for the filesystem that traverses the link making the write bandwidth some multiplier greater than 2. A typical good estimate is 2.2.

Workloads are almost never 100% read or 100% write. Typical benchmarks use a 70% Read/ 30% Write workload distribution. This means that for a 100,000 IOPS workload, 70,000 would be reads and 30,000 would be writes with a typical block size of 4k in the application. While the cluster writes do not map one-to-one with application writes (they are concatenated and written in chunks), the overall size of the write(s) match.

Link Bandwidth = WIOPS(2 replicas)(0.2 metadata overhead)(4kB) + RIOPS(4kB) + ResynchIOPS(2 replicas)(4kB) + vMotionBW

Where WIOPS are Write IOPS, RIOPS are Read IOPS, ResynchIOPS are resynchronization operations from any potential failure recoveries, and vMotionBW is the bandwidth taken up by a VM move (both compute and storage to account for datastore affinity when moved between sites). Resynchronizations only happen on failure recovery and are transitory operations so we will ignore them here. Storage vMotion is also typically not undertaken, but we will consider it in the example below.

Example: 20,000 IOPS total cluster workload, one affinity-displaced VMs contributing 1000 IOPS in 4kB Reads, no resynchronization, and 1 full SVMotion running at 500Mb/s. Assume 70/30 breakdown for the read and writes.

Link BW = 0.7(20000)(2)(0.2)(4kB)+1000(4kB) + 0 + 500Mb/s

Link BW = 123,200 kB/s + 4000 kB/s + 500Mb/s = 127,200 kB/s + 500 Mb/s = (127,200)*8/1024 Mb/s + 500 Mb/s

Link BW = 993.4 Mb/s + 500 Mb/s

Link BW ≈ 1500 Mbps

Since you will not often do resync or vMotion, this can be considered a peak link value for the 20000 IOPS workload examined. There are times, for example, during large, frequent deletes, where the file system cleaner can incur larger metadata traffic on the link. To estimate those, you can use a multiplier of 1 to 1.5 instead of 0.2 for the (temporary peak) metadata value.

Solution Design

Requirements

The following sections detail the physical hardware, software revisions, and firmware versions required to install a single cluster of the Cisco HyperFlex system. This solution's stretch cluster will have a four nodes on each site.

Physical Components

Table 1. HyperFlex System Components

Component	Hardware Required
Fabric Interconnects	Four Cisco UCS 6454 Fabric Interconnects (Two at each Site)
Servers	Eight Cisco HyperFlex HXAF220c-M5SX All-Flash rack servers (Four at each Site)

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

For the HXAF220c-M5SX Spec sheet, go to:

https://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hxseries/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 options		Hardware Required	
Processors		Chose a matching pair of 2 nd Generation Intel Xeon 6230 Processor Scalable Family CPUs	
Memory		786 GB total memory using 64 GB DDR4 2933 MHz 1.2v modules depending on CPU type	
Disk Controller		Cisco 12Gbps Modular SAS HBA	
SSDs	Standard	One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD	
		1.6 TB 2.5 Inch Extreme Performance 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	
	SED	One 240 GB 2.5 Inch Enterprise Value 6G SATA SSD	
		One 800 GB 2.5 Inch Enterprise Performance 12G SAS SED SSD	
		Six to eight 3.8 TB 2.5 Inch Enterprise Value 6G SATA SED SSDs, or six to eight 960 GB 2.5 Inch Enterprise Value 6G SATA SED SSDs	
Network		Cisco UCS VIC1387 VIC MLOM, or	

HXAF220c-M5SX options	Hardware Required
	Cisco UCS VIC1457 VIC MLOM
Boot Device	One 240 GB M.2 form factor SATA SSD
microSD Card	One 32GB microSD card for local host utilities storage (Not used in this study)
Optional	

Software Components

The software components of the Cisco HyperFlex system must meet minimum requirements for the Cisco UCS firmware, hypervisor version, and the Cisco HyperFlex Data Platform software in order to interoperate properly.

For additional hardware and software combinations, refer to the public Cisco UCS Hardware Compatibility here: https://ucshcltool.cloudapps.cisco.com/public/

Table 3 lists the software components and the versions required for the Cisco HyperFlex 4.0 system.

Table 3. Software Components

Component	Software Required		
Hypervisor	VMware ESXi 6.7 Update 3		
	Cisco Custom Image for ESXi 6.7 Update 3 for HyperFlex:		
	HX-ESXi-6.7U3-16316930-Cisco-Custom-6.7.3.3-install-only.iso		
	Using a published Cisco custom ESXi ISO installer file is required when installing/reinstalling ESXi or upgrading to a newer version prior to installing HyperFlex. An offline bundle file is also provided to upgrade ESXi on running clusters.		
	ESXi 6.0 is not supported on servers equipped with the Cisco VIC1457 card, or the HXAF220c-M5N model servers. Each of these requires ESXi 6.5 Update 3 or higher.		
	VMware vSphere Standard, Essentials Plus, ROBO, Enterprise or Enterprise Plus licensing is required from VMware.		
Management Server	VMware vCenter Server for Windows or vCenter Server Appliance 6.0 U3c or later.		
	Refer to <u>http://www.vmware.com/resources/compatibility/sim/interop_matrix.php</u> for interoperability of your ESXi version and vCenter Server.		

Component	Software Required	
	Using ESXi 6.5 on the HyperFlex nodes also requires using vCenter Server 6.5. Accordingly, using ESXi 6.7 hosts requires using vCenter Server 6.7.	
Cisco HyperFlex Data Platform	Cisco HyperFlex HX Data Platform Software 4.0(2b)	
Cisco UCS Firmware	Cisco UCS Infrastructure software, B-Series and C-Series bundles, revision 4.0(4g) 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 Hyper-Flex 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 on the Cisco Smart Software Manager satellite server, go to: <u>https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html</u>

Licensing of the system requires one license per node from one of three different licensing editions; Edge licenses, Standard licenses, or Enterprise licenses. Depending on the type of cluster being installed, and the desired features to be activated and used in the system, licenses must be purchased from the appropriate licensing tier. Additional features in the future will be added to the different licensing editions as they are released, the features listed below are current only as of the publication of this document.

<u>Table 4</u> lists an overview of the licensing editions, and the features available with each type of license.

HyperFlex Licensing Edition	Edge	Advantage (in addition to Edge)	Premier (in addition to Standard)
Features Available	HyperFlex Edge clusters	HyperFlex standard clusters	Stretched clusters
	without Fabric Interconnects	with Fabric Interconnects	220 all-NVMe server models Cisco HyperFlex Acceleration Engine
	220 SFF model servers only	220 and 240 SFF server	
	Hybrid or All-Flash	models and 240 LFF server models	
	ESXi Hypervisor only		

Table 4. HyperFlex System License Editions
HyperFlex Licensing Edition	Edge	Advantage (in addition to Edge)	Premier (in addition to Standard)
	Replication Factor 2 only	Replication Factor 3	cards
	1 Gb or 10 Gb Ethernet only	Hyper-V and Kubernetes	Compute-only nodes up
	Compression	platforms	to 2:1 ratio
	Deduplication	Cluster expansions	
	HyperFlex native snapshots	Compute-only nodes up to 1:1 ratio	
	Rapid Clones	10 Gb, 25 Gb or 40 Gb	
	HyperFlex native replication	Ethernet	
	Management via vCenter plugin, HyperFlex Connect,	Data-at-rest encryption using self-encrypting disks	
	or Cisco Intersight	Logical Availability Zones	

For a comprehensive guide to licensing and all the features in each edition, consult the Cisco HyperFlex Licensing Guide here:

https://www.cisco.com/c/en/us/td/docs/hyperconverged systems/HyperFlex HX DataPlatformSoftware/b Cis co HyperFlex Systems Ordering and Licensing Guide/b Cisco HyperFlex Systems Ordering and Licensing Guide chapter 01001.html

Physical Topology

Topology Overview

The Cisco HyperFlex system is composed of a pair of Cisco UCS Fabric Interconnects along with up to thirtytwo HX-Series rack-mount servers per cluster. Up to thirty-two compute-only servers can also be added per HyperFlex cluster. Adding Cisco UCS rack-mount servers and/or Cisco UCS 5108 Blade chassis, which house Cisco UCS blade servers, allows for additional compute resources in an extended cluster design. The two Fabric Interconnects both connect to every HX-Series rack-mount server, and both connect to every Cisco UCS 5108 blade chassis, and Cisco UCS rack-mount server. 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.

Figure 14. HyperFlex Stretch Cluster Topology



Fabric Interconnects

Fabric Interconnects (FI) are deployed in pairs, wherein the two units operate as a management cluster, while forming two separate network fabrics, referred to as the A side and B side fabrics. Therefore, many design elements will refer to FI A or FI B, alternatively called fabric A or fabric B. Both Fabric Interconnects are active at all times, passing data on both network fabrics for a redundant and highly available configuration. Management services, including Cisco UCS Manager, are also provided by the two FIs but in a clustered manner, where one FI is the primary, and one is secondary, with a roaming clustered IP address. This primary/secondary relationship is only for the management cluster and has no effect on data transmission. In this Stretch Cluster, there are a total of 4 fabric interconnects, a pair at each site.

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 with the Cisco UCS VIC 1387 or Cisco UCS VIC 1457 cards. The standard and redundant connection practice for the Cisco UCS VIC 1387 is to connect port 1 of the Cisco UCS VIC card (the right-hand port) to a port on FI A, and port 2 of the VIC card (the left-hand port) to a port on FI B (Figure 15). For the Cisco UCS VIC 1457 card, the standard and redundant practice is to connect port 1 of the VIC card (the left-hand most port) to a port on FI A and connect port 3 (the right-center port) to a port on FI B (Figure 16). An optional configuration method for servers containing the Cisco VIC 1457 card is to cable the servers with 2 links to each FI, using ports 1 and 2 to FI A, and ports 3 and 4 to FI B. The HyperFlex installer checks for these configurations, and that all servers' cabling matches. Failure to follow this cabling best practice can lead to errors, discovery failures, and loss of redundant connectivity. All nodes within a Cisco HyperFlex cluster must be connected at the same communication speed, for example, mixing 10 Gb with 25 Gb interfaces is not allowed. In addition, for clusters that contain only M5 generation nodes, all of the nodes within a cluster must contain the same model of Cisco VIC cards.

Various combinations of physical connectivity between the Cisco HX-series servers and the Fabric Interconnects are possible, but only specific combinations are supported. <u>Table 5</u> lists the possible connections, and which of these methods is supported.

Fabric Interconnect Model	6248	6296	6332	5332 6332-16UP 6							
Port Type	10GbE	10GbE	40GbE	10GbE Breakout	40GbE	10GbE Breakout	10GbE onboard	10GbE	25GbE		
M4 with VIC 1227	\checkmark	\checkmark	×	×	×	×	×	\checkmark	×		
M4 with VIC 1387	×	×	\checkmark	×	\checkmark	√ ×		×	×		
M4 with VIC 1387 + QSA	\checkmark	\checkmark	×	×	×	× ×		\checkmark	×		
M5 with VIC 1387	×	×	\checkmark	×	\checkmark	×	×	×	×		
M5 with VIC 1387 + QSA	\checkmark	\checkmark	×	×	×	×	×	\checkmark	×		
M5 with VIC 1457	\checkmark	\checkmark	×	×	×	×××		\checkmark	\checkmark		

 Table 5.
 Supported Physical Connectivity

Figure 15. HX-Series Server with Cisco UCS VIC 1387 Connectivity



Figure 16. HX-Series Server with Cisco UCS VIC 1457 Connectivity



Cisco UCS C-Series Rack-Mount Servers

HyperFlex extended clusters can also incorporate 1-32 Cisco UCS Rack-Mount Servers for additional compute capacity. The Cisco UCS C-Series Rack-Mount Servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode. Internally the Cisco UCS C-Series servers are configured with the Cisco VIC 1227, 1387 or 1457 network interface card (NIC) installed in a modular LAN on motherboard (MLOM) slot, which have dual 10 Gigabit Ethernet (GbE), quad 10/25 Gigabit Ethernet (GbE) ports or dual 40 Gigabit Ethernet (GbE) ports. The standard and redundant connection practice for connecting standard Cisco UCS C-Series servers to the Fabric Interconnects is identical to the method described earlier for the HX-Series servers.

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

Figure 17. Cisco UCS C-Series Server Connectivity



Logical Topology

Logical Network Design

The Cisco HyperFlex system has communication pathways that fall into four defined zones (Figure 18):

- 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 also 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 via the FI management ports.
 - ESXi host management interfaces.
 - Storage Controller VM management interfaces.
 - A roaming HX cluster management interface.
 - Storage Controller VM replication interfaces.
 - A roaming HX cluster replication 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, which 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, ESXi 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 VMkernel interface used for storage traffic on each ESXi host in the HX cluster.
 - Storage Controller VM storage interfaces.
 - A roaming HX cluster storage interface.
- VMotion Zone: This zone comprises the connections used by the ESXi hosts to enable vMotion 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 vMotion traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa.

Figure 18. Logical Network Design



Design Elements

Installing the HyperFlex system is done via the Cisco Intersight online management portal, or through a deployable HyperFlex installer virtual machine, available for download at <u>cisco.com</u> as an OVA file. The installer performs most of the Cisco UCS configuration work, and also performs significant portions of the ESXi configuration. Finally, the installer will 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 prerequisite steps needed for installation, and how to then utilize the HyperFlex Installer for the remaining configuration steps. This document focuses on the use of Cisco Intersight for the initial deployment of a Cisco Hyper-Flex cluster.

Network Design for a Stretch Cluster

For detailed guidance on Network Design for stretch clusters, please refer to the HyperFlex Stretch Cluster for Infrastructure CVD here:

https://www.cisco.com/c/en/us/td/docs/unified computing/ucs/UCS CVDs/hx 40 vsi aci multipod design.ht ml

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, however 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 instead be directed over the Cisco UCS uplinks because that traffic must travel from fabric A to fabric B, or vice-versa. 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. Cisco recommends that the uplink bandwidth configured is greater than or equal to double the bandwidth available to each Hyperflex converged node. For example, if the nodes are connected at 10 Gigabit speeds, then each Fabric Interconnect should have at least 20 Gigabit of uplink bandwidth available. The following sections and figures detail several uplink connectivity options.

Single Uplinks to Single Switch

This connection design is susceptible to failures at several points; single uplink failures on either Fabric Interconnect can lead to connectivity losses or functional failures, and the failure of the single uplink switch will cause a complete connectivity outage.



Figure 19. Connectivity with Single Uplink to Single Switch

Port Channels to Single Switch

This connection design is now redundant against the loss of a single link but remains susceptible to the failure of the single switch.





Single Uplinks or Port Channels to Multiple Switches

This connection design is redundant against the failure of an upstream switch, and redundant against a single link failure. In normal operation, STP is likely to block half of the links to avoid a loop across the two upstream switches. The side effect of this is to reduce bandwidth between the Cisco UCS domain and the LAN. If any of the active links were to fail, STP would bring the previously blocked link online to provide access to that Fabric Interconnect via the other switch. It is not recommended to connect both links from a single FI to a single switch, as that configuration is susceptible to a single switch failure breaking connectivity from fabric A to fabric B. For enhanced redundancy, the single links in the figure below could also be port-channels.





vPC to Multiple Switches

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



Figure 22. Connectivity with vPC

VLANs and Subnets

For the base HyperFlex system configuration, multiple VLANs need to be carried to the Cisco UCS domain from the upstream LAN, and these VLANs are also defined in the Cisco UCS configuration. The hx-storage-data VLAN must be a separate VLAN ID from the remaining VLANs. <u>Table 6</u> lists the VLANs created by the HyperFlex installer in Cisco UCS, and their functions:

Table 6. VLANs

VLAN Name	VLAN ID	Purpose
hx-inband-mgmt	Customer supplied	ESXi host management interfaces
		HX Storage Controller VM management interfaces
		HX Storage Cluster roaming management interface

VLAN Name	VLAN ID	Purpose
hx-inband-repl	Customer supplied	HX Storage Controller VM Replication interfaces
		HX Storage Cluster roaming replication interface
hx-storage-data	Customer supplied	ESXi host storage VMkernel interfaces
		HX Storage Controller storage network interfaces
		HX Storage Cluster roaming storage interface
vm-network	Customer supplied	Guest VM network interfaces
hx-vmotion	Customer supplied	ESXi host vMotion VMkernel interfaces

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

Jumbo Frames

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

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

HyperFlex Datastores for Stretch Clusters

A new HyperFlex cluster has no default datastores configured for virtual machine storage, therefore the datastores must be created using the vCenter Web Client plugin or the HyperFlex Connect GUI. When creating a datastore on Site-A the site affinity must be configured for site-a and the same goes for Site-B. Both sites will write copies to its stretch cluster partner site, so the data is available in the event of a site failure. It is important to recognize that all HyperFlex datastores are thinly provisioned, meaning that their configured size can far exceed the actual space available in the HyperFlex cluster. Alerts will be raised by the HyperFlex system in Hyper-Flex Connect or the vCenter plugin when actual space consumption results in low amounts of free space, and alerts will be sent via auto support email alerts. Overall space consumption in the HyperFlex clustered filesystem is optimized by the default deduplication and compression features.





Installation

Cisco UCS Installation for Stretch Clusters

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

Cisco UCS Fabric Interconnect A

To configure Fabric Interconnect A, follow these steps:

- 1. Make sure the Fabric Interconnect cabling is properly connected, including the L1 and L2 cluster links, and power the Fabric Interconnects on by inserting the power cords.
- 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.
- 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/gui) ? console

Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup

You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

Enforce strong password? (y/n) [y]: y

Enter the password for "admin": Confirm the password for "admin":

Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes

Enter the switch fabric (A/B) []: A

Enter the system name: HX1-FI

Physical Switch Mgmt0 IP address : 10.29.132.104

Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.29.132.1

Cluster IPv4 address : 10.29.132.106

Configure the DNS Server IP address? (yes/no) [n]: yes

DNS IP address : 10.29.132.110

Configure the default domain name? (yes/no) [n]: yes

Default domain name : hxdom.local

Join centralized management environment (UCS Central)? (yes/no) [n]: no

Following configurations will be applied:

Switch Fabric=A System Name=HX1-FI Enforced Strong Password=no Physical Switch Mgmt0 IP Address=10.29.132.104 Physical Switch Mgmt0 IP Netmask=255.255.255.0 Default Gateway=10.29.132.1 Ipv6 value=0 DNS Server=10.29.132.110 Domain Name=hxdom.local

```
Cluster Enabled=yes
Cluster IP Address=10.29.132.106
NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized
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, follow these 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.
- 2. Start your terminal emulator software.
- 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: 10.29.132.104
Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
Cluster IPv4 address : 10.29.132.106
```

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address

Physical Switch Mgmt0 IP address : 10.29.132.105

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

To log into the Cisco UCS Manager environment, follow these steps:

1. Open a web browser and navigate to the Cisco UCS Manager Cluster IP address, for example: https://10.29.132.106

			in the		
		c	ISCO		
		UCS N	lanage	er	
6			-		-
	Launch UCS Mar	nager		Launch KVM Manager	
	Launch UCS Mar	nager Inch requires Jav	va Runtime E	Launch KVM Manager	ır
\$ 2009-201	Java KVM lau	nager Inch requires Jav . All rights reserved.	va Runtime E	Launch KVM Manager	r
© 2009-201 The copyrig	Java KVM lau Java KVM lau 9 Cisco Systems, Inc. hts to certain works	nager Inch requires Jav All rights reserved. contained in this s	va Runtime E	Launch KVM Manager nvironment 1.7 or higher med by other third parties	ir and used an
© 2009-201 The copyrig distributed (Java KVM lau Java KVM lau 9 Cisco Systems, Inc. hts to certain works inder license. Certain	nager Inch requires Jav All rights reserved. contained in this s n components of th	va Runtime E oftware are ow	Launch KVM Manager nvironment 1.7 or higher med by other third parties is e licensed under the GNU G	nr and used an ieneral Publi
© 2009-201 The copyrig distributed (License (GP	Java KVM lau Java KVM lau 9 Cisco Systems, Inc. Ints to certain works - under license. Certain L) version 2.0 or the 0	All rights reserved. contained in this s n components of th GNU gpl 2.0 and Let	oftware are ow is software are sser General Pi	Launch KVM Manager nvironment 1.7 or higher med by other third parties is e licensed under the GNU G ublic License (LGPL) Version	r and used an ieneral Publi

- 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.

alialia cisco	UCS Manager		8	V 🛆 2 0	⊕ 0				•	Q ?	0 3 C
æ	All	Equipment									
	 Equipment 	Main Topology View	Fabric Interconnects	Servers	Thermal	Decommissioned	Firmware Management	Policies Fa	ults Diagnostic	28	
	Chassis										
뫎	* Rack-Mounts										(^`)
	Enclosures										\checkmark
	FEX										+
_	Servers										
	 Fabric Interconnects 										Ť
	 Fabric Interconnect A (subordinate) 										
	 Fabric Interconnect B (primary) 										-
20	* Policies		FORMONICATING Paraticipal	INFIN FUNDING			- Martana	MANUALINE INCLUSION OF THE	nanneadd = = = =		K 7
	Port Auto-Discovery Policy		Fabric Interconne	ect A (subordin	nate)		annan	Fabric Interconnect	B (primary)		

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 <u>Software</u> <u>Components</u> section. This document is based on Cisco UCS infrastructure, B-series bundle, and C-Series bundle software versions 4.0(4d). 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/4-0/b_UCSM_GUI_Firmware_Management_Guide_4-0.html

NTP

To synchronize the Cisco UCS environment time to the NTP server, follow these steps:

- 1. In Cisco UCS Manager, click Admin.
- 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.

#	All +	All / Time Zone Management / Timezone General Events	
뮮	Collection Policy Host Collection Policy Port Collection Policy Server	Actions Add NTP Server	Properties Time Zone : America/Los_Angeles (Pacif *
- -	 Fabric ► Internal LAN ► LAN Cloud 		Tr Advanced Filter ↑ Export ⊕ Print
=	 SAN Cloud root 		NTP Server ntp1.hx.lab.cisco.com NTP Server ntp2.hx.lab.cisco.com
	 Time Zone Management Timezone 		
	 Capability Catalog Adapters 		🕀 Add 🗊 Delete 🍈 Info
	Blade Servers CPUs		

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, follow these steps:

- 1. In Cisco UCS Manager, click Equipment.
- 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, then click OK.
- 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."

ж	All 🔹	Equipment / Fabr	ic Interconnects / Fat	oric Interconnect A (su	bo / Fixed Module / Eth	ernet Ports					
	* Equipment	Ethernet Ports									
	Chassis	T∉ Advanced Filter	🕈 Export 🛛 🖶 Print	All Unconfigure	ed 🖌 Network Server	FCoE Uplink	k Unified Uplink A	ppliance Storage FCoE S	Storage Unified Storag	e »	¢
몲	Rack-Mounts	Slot	Aggr. Part ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer	
	 Fabric Interconnects 	1	0	39	00:DE:FB:DF:B7:A0	Network	Physical	t Up	1 Enabled		
1	🔻 Fabric Interconnect A (subordinate) 🦁	1	0	40	00:DE:FB:DF:B7:A1	Network	Physical	t Up	1 Enabled		
	Fans										
9	▼ Fixed Module										
	Ethernet Ports										
	FC Ports										
	► PSUs										
	 Fabric Interconnect B (primary) 🦁 										
-0	* Policies										
	Port Auto-Discovery Policy										

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, follow these steps:

- 1. In Cisco UCS Manager, click LAN.
- 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, then 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, then 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.

æ	All	LAN / LAN Cloud / Fabric A / Port Channels / F	Port-Channel 10 po10	
	* LAN	General Ports Faults Events St	tatistics	
	▼ LAN Cloud	Chantura		
몲	▼ Fabric A	Status	Properties	
	 Port Channels 	Overall Status : 🕇 Up	ID	: 10
I	Port-Channel 10 po10	Additional Info :	Fabric ID	: A
	Eth Interface 1/39	Actions	Port Type	: Aggregation
	Eth Interface 1/40		Transport Type	: Ether
	Eth Interface 1/40		Name	: po10
	 Uplink Eth Interfaces 	Disable Port Channel	Description	:
	▶ VLANs	Add Ports	Flow Control Policy	default 🔻
	VP Optimization Sets		LACP Policy	dofouit V
	▼ Fabric B		Note: Changing LACP n	olicy may flan the port-channel if the suspend-individual value changes!
-0	▼ Port Channels		Admin Speed	: O 1 Gbps O 10 Gbps () 40 Gbps
	 Port-Channel 20 po20 		Operational Speed(Gb)	ps): 80
	Eth Interface 1/39			
	Eth Interface 1/40			

Chassis Discovery Policy

If the Cisco HyperFlex system will use blades as compute-only nodes in an extended cluster design, additional settings must be configured for connecting the Cisco UCS 5108 blade chassis. The Chassis Discovery policy defines the number of links between the Fabric Interconnect and the Cisco UCS Fabric Extenders which must be connected and active, before the chassis will be discovered. This also effectively defines how many of those connected links will be used for communication. The Link Grouping Preference setting specifies if the links will operate independently, or if Cisco UCS Manager will automatically combine them into port-channels. Cisco best practices recommends using link grouping, and the number of links per side is dependent on the hardware used in Cisco UCS 5108 chassis, and the model of Fabric Interconnects. For 10 GbE connections Cisco recommends 4 links per side, and for 40 GbE connections Cisco recommends 2 links per side.

To configure the necessary policy and setting, follow these steps:

- 1. In Cisco UCS Manager, click Equipment, and click Equipment.
- 2. In the properties pane, click the Policies tab.
- 3. Under the Global Policies sub-tab, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled per side, between the chassis and the Fabric Interconnects.
- 4. Set the Link Grouping Preference option to Port Channel.
- 5. Set the backplane speed preference to 4x10 Gigabit or 40 Gigabit.

6. Click Save Changes.

7. Click OK.

Main Topology Vie	ew Fabric Interconn	Interconnects Servers		Decommissioned	Firmware Managen	Policies
Global Policies	Autoconfig Policies	Server Inheritance	e Policies	Server Discovery Polic	cies SEL Policy	Power Groups
Chassis/FEX Disc	overy Policy					
Action	: 1 Link		•			
Link Grouping Pre	eference : ONNO	OPort Channel				
Backplane Speed	Preference : 40G	4x10G				

Server Ports

The Ethernet ports of a Cisco UCS Fabric Interconnect connected to the rack-mount servers, or to the blade chassis 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 and blade chassis 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. The same numbering procedure applies to blade server chassis, although chassis and rack-mount server numbers are separate from each other.

Auto Configuration

Server Port Auto-Discovery, which automates the configuration of ports on the Fabric Interconnects as server ports when a Cisco UCS rack-mount server or blade chassis is connected to them. The firmware on the rack-mount servers or blade chassis Fabric Extenders 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, how-ever it can configure the servers in a somewhat random order depending upon the circumstances. An example of how to use this feature in an orderly manner would be to have the policy already set, then to mount, cable and apply power to each new server one-by-one. In this scenario the servers should be automatically discovered in the order you racked them and applied power.

An example of how the policy can result in unexpected ordering would be when the policy has not been enabled, then all of the new servers are racked, cabled, and have power applied to them. If the policy is enabled afterwards, it will likely not discover the servers in a logical 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 in this scenario, the manual configuration steps listed in the next section must be followed.

To configure automatic server port definition and discovery, follow these steps:

- 1. In Cisco UCS Manager, click Equipment.
- 2. In the navigation tree, under Policies, click Port Auto-Discovery Policy.

- 3. In the properties pane, set Auto Configure Server Port option to Enabled.
- 4. Click Save Changes.
- 5. Click OK.
- 6. Wait for a brief period, until the rack-mount servers appear in the Equipment tab underneath Equipment > Rack Mounts > Servers, or the chassis appears underneath Equipment > Chassis.



Manual Configuration

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

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

æ	All 👻	Equipment / Fabr	ic Interconnects / Fal	pric Interconnect A (subo.	. / Fixed Module / Eth	ernet Ports				
	* Equipment	Ethernet Ports								
	Chassis	Ty Advanced Filter	🕈 Export 🛛 🖶 Print	All Unconfigured	Network V Server	FCoE Uplink	Unified Uplink	Appliance Storage FCoE St	orage Unified Storage	>> ⊅
몲	Rack-Mounts	Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
	▼ Fabric Interconnects	1	0	17	00:DE:FB:DF:B7:54	Server	Physical	1 Up	1 Enabled	sys/rack-unit-1/ad
	 Fabric Interconnect A (subordinate) 🦁 	1	0	18	00:DE:FB:DF:B7:58	Server	Physical	1 Up	1 Enabled	sys/rack-unit-2/ad
	▶ Fans	1	0	19	00:DE:FB:DF:B7:5C	Server	Physical	1 Up	1 Enabled	sys/rack-unit-3/ad
▣	▼ Fixed Module 🦁	1	0	20	00:DE:FB:DF:B7:60	Server	Physical	t Up	1 Enabled	sys/rack-unit-4/ad
=	Ethernet Ports	1	0	21	00:DE:FB:DF:B7:64	Server	Physical	1 Up	1 Enabled	sys/rack-unit-5/ad
	▶ FC Ports	1	0	22	00:DE:FB:DF:B7:68	Server	Physical	1 Up	1 Enabled	sys/rack-unit-6/ad
	▶ PSUs	1	0	23	00:DE:FB:DF:B7:6C	Server	Physical	t Up	1 Enabled	sys/rack-unit-7/ad
	Fabric Interconnect B (primary) 👽	1	0	24	00:DE:FB:DF:B7:70	Server	Physical	t Up	1 Enabled	sys/rack-unit-8/ad
-0	* Policies									
	Port Auto-Discovery Policy									

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.

To view the servers' discovery status, follow these steps:

- 1. In Cisco UCS Manager, click Equipment, and click Equipment in the top of the navigation tree on the left.
- 2. In the properties pane, click the Servers tab.
- 3. Click the Blade Servers or Rack-Mount Servers sub-tab as appropriate, then view the servers' status in the Overall Status column.

alialia cisco	UCS Manager			8 👽	(0 2										•	€ €	9	0	9 ©
ж	All 👻	Equipment																	
	Equipment	Main Topology Vie	ew Fabric Intercon	nects Servers	Thermal	Decomr	missioned	d Firm	ware Mai	nagement	Polic	ies Fa	aults	Diagnosti	cs				
	Chassis	Blade Servers	Rack-Mount Servers																
윪	▼ Rack-Mounts	+ - Ty Advanc	ed Filter 🕆 Export	🖶 Print															\$
_	Enclosures	Name	Overall Status	PID	Model	Serial	Profile	User	Cores	Core	Threa	Mem	Adap	NICs	HBAs	Oper	Powe	Asso	Fault
-	FEX	Enclosures																	
	* Servers	- Servers																	
_	Server 1	Server 1	Unassociated	HXAF240C-M5SX	Cisc	WZP			36	36	72	3932	1	0	0	t o.	∔ or	∔ N.	N/A
=	Server 2	Server 2		HXAF240C-M5SX	Cisc	WZP			36	36	72	3932	1	0	0	10	+ or	4 N	N/A
	Server 3	Server 3	Linseenristed	HXAF240C-M5SX	Cisc	WZP			36	36	72	3932	1	0	0	t 0	1 of	4 N	N/A
	Server 4	Server 4		HYAE240C-M5SX	Ciec	W7P			36	36	72	3032	1	0	0	t 0	1 of	1 M	NZA
1.	Server 5	Sature 5	Unassociated	HYAE240C-MSEX	Cierc	W7D			36	26	72	2022	1	0	0	• 0	1 0#	- No.	NUA
-0	▶ Server 6	Cerver 5	• Unassociated	HXAF240C-MSSX	Cine .	V62.P			30	30	72	3332	1	0	0	• 0	• Un	• N	NUA
	Server 7	Server 6	Unassociated	HAAF240G-MISSA	Clac	V#ZP			30	30	72	3932		0	0	• 0	• on	• N	15024
	Server 8	Server /	Unassociated	HXAP240C-MSSX	Cisc	V6ZP			36	36	72	3932	1	0	0	• 0	• Off	• N	N/A
	 Fabric Interconnects 	Server 8	 Unassociated 	HXAF240C-M5SX	Cisc	WZP			36	36	72	3932	1	0	0	T 0	◆ Off	* N	N/A
	 Fabric Interconnect A (primary) 																		
	 Fabric Interconnect B (subordinate) 																		
	* Policies																		
	Port Auto-Discovery Policy																		

HyperFlex Installer VM Deployment

The Cisco HyperFlex software is distributed as a deployable virtual machine, contained in an Open Virtual Appliance (OVA) file format. The HyperFlex OVA file is available for download at cisco.com:

https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(1b)

This document is based on the Cisco HyperFlex 4.0(2b) release filename: Cisco-HX-Data-Platform-Installer-v4.0.2b-33133-esx.ova

The HyperFlex installer OVA file can be deployed as a virtual machine in an existing VMware vSphere environment, VMware Workstation, VMware Fusion, or other virtualization environment which supports importing of OVA format files. For the purpose of this document, the process described uses an existing ESXi server managed by vCenter to run the HyperFlex installer OVA and deploying it via the VMware vSphere Web Client.

Installer Connectivity

The Cisco HyperFlex Installer VM must be deployed in a location that has connectivity to the following network locations and services:

- Connectivity to the vCenter Server which will manage the HyperFlex cluster(s) to be installed.
- Connectivity to the management interfaces of the Fabric Interconnects that contain the HyperFlex cluster(s) to be installed.
- Connectivity to the management interface of the ESXi hypervisor hosts which will host the HyperFlex cluster(s) to be installed.
- Connectivity to the DNS server(s) which will resolve host names used by the HyperFlex cluster(s) to be installed.
- Connectivity to the NTP server(s) which will synchronize time for the HyperFlex cluster(s) to be installed.
- Connectivity from the staff operating the installer to the webpage hosted by the installer, and to log in to the installer via SSH.

For complete details of all ports required for the installation of Cisco HyperFlex, refer to Appendix A of the HyperFlex 4.0 Hardening Guide: <u>https://www.cisco.com/c/dam/en/us/support/docs/hyperconverged-infrastructure/hyperflex-hx-data-platform/HX-Hardening_Guide.pdf</u>

If the network where the HyperFlex installer VM is deployed has DHCP services available to assign the proper IP address, subnet mask, default gateway, and DNS servers, the HyperFlex installer can be deployed using DHCP. If a static address must be defined, use <u>Table 7</u> to document the settings to be used for the HyperFlex installer VM.

Table 7. HyperFlex Installer Settings

Setting	Value
IP Address	
Subnet Mask	
Default Gateway	

Setting	Value
DNS Server	
NTP Server(s)	
Root Password	

Deploy Installer OVA

To deploy the HyperFlex installer OVA, follow these steps:

- 1. Open the vSphere HTML5 Web Client webpage of a vCenter server where the installer OVA will be deployed and log in with admin privileges.
- 2. In the vSphere Web Client, from the Home view, click Hosts and Clusters.
- 3. From the Actions menu, click Deploy OVF Template.
- 4. Select the Local file option, then click Choose Files and locate the Cisco-HX-Data-Platform-Installerv4.0.2b-33133-esx.ova file, click the file and click Open.
- 5. Click Next.
- 6. Modify the name of the virtual machine to be created if desired and click a folder location to place the virtual machine, then click Next.
- 7. Click a specific host or cluster to locate the virtual machine and click Next.
- 8. After the file validation, review the details and click Next.
- 9. Select a Thin provision virtual disk format, and the datastore to store the new virtual machine, then click Next.
- 10. Modify the network port group selection from the drop-down list in the Destination Networks column, choosing the network the installer VM will communicate on, and click Next.
- 11. If DHCP is to be used for the installer VM, leave the fields blank, except for the NTP server value and click Next. If static address settings are to be used, fill in the fields for the DNS server, Default Gateway, NTP Servers, IP address, and subnet mask.
- 12. Enter and confirm a new password used to log in to the installer VM after it is deployed, then click Next.



- 13. Review the final configuration and click Finish.
- 14. The installer VM will take a few minutes to deploy, once it has deployed, power on the new VM and proceed to the next step.

HyperFlex Installer Web Page

The HyperFlex installer is accessed via a webpage using your local computer and a web browser. If the Hyper-Flex installer was deployed with a static IP address, then the IP address of the website is already known. If DHCP was used, open the local console of the installer VM. In the console, you will see an interface similar to the example shown in <u>Figure 24</u>, showing the IP address that was leased. Figure 24. HyperFlex Installer VM IP Address



To access the HyperFlex installer webpage, follow these steps:

- 1. Open a web browser on the local computer and navigate to the IP address of the installer VM. For example, open http://10.29.132.115
- 2. Click Accept or Continue to bypass any SSL certificate errors.
- 3. At the login screen, enter the username: root
- 4. At the login screen, enter the password which was set during the OVA deployment.
- 5. Verify the version of the installer in the lower right-hand corner of the Welcome page is the correct version.
- 6. Check the box for "I accept the terms and conditions" and click Login.

Cisco HyperFlex Stretch Cluster Configuration

To configuring the Cisco HyperFlex Cluster, follow this step:

1. Log into the HX Installer virtual machine through a web browser: http://<Installer VM IP Address>.



Create a HyperFlex Stretch Cluster

To create a HyperFlex cluster, follow these steps:

1. Select the workflow for cluster creation to deploy a new HyperFlex cluster on eight Cisco HXAF220c-M5S nodes. From the drop-down list select Stretch Cluster.

Select a Workflow				
ſ				
	¢ ¢	\$ ` \$ ` \$		
	Create Cluster Standard Cluster	Expand Cluster 🔹		
	Edge Cluster Stretch Cluster			

2. On the credentials page, enter the access details for Cisco UCS Manager and the Site information. (The Configure Site option must be run on both sites before the Stretch Cluster workflow can be run.) Click Continue.

	Credentials	Server Selection	UCSM Configuration		Hyper	visor Configu	uration	
Te و د ا	o setup stretch cluster you have to • Run the "Configure Site" workflor • Download and deploy the Witner stretch cluster. • Run the "Create Stretch Cluster" onfigure Site OCC	w once for each site. ss VM, per the user documentation. Provide the workflow, after both sites have been configured Greate Stretch Cluster this site	IP address of the Witness VM when you create the	Con	figuratio	n		+
uc	CS Manager Host Name	UCS Manager User Name	Password					
Sit	te Name	avenue						
	Site-A							
					JSON co	Drag and dro nfiguration fi lect a ISON	ie here or	

- 3. Select the unassociated servers for the site in the HyperFlex installer. To configure a subset of available of the HyperFlex servers, manually click the checkbox for individual servers.
- 4. Click Continue after completing server selection.

Server Selection Server Nodes for this site. Unassociated (0) Server 2 Unassociated NKAF220C-M55X VZ2P21230UBH none Server 7 Unassociated NKAF220C-M55X VZ2P2120C6B none Server 10 Unassociated NKAF220C-M55X VZ2P22120C85 none NKKAF220C-M55X NKKAF220C-M55X VZ2P22120C85 NONE NKKAF220C-M55X NKKAF220C		Cred	fentials		Server Selection	UCSM Con	figuration	Hypervisor Configu	ation
Unassociated (5) Associated (6) Servier Name A Status Model Serial Actions Image: Associated (1) Server 2 unassociated HKAF220C-M5SK WZP21230UBH none Image: Associated (1) Image: Associated (1) HKAF220C-M5SK WZP2120C68 none Image: Associated (1) Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) HKAF220C-M5SK WZP22120C81 none Image: Associated (1) Image: Associated	Server	Selection	this site.			Configure Server Ports	Refresh	Configuration	*
Image: Server Name In Status Model Serval Actions: Image: Server 2 unessociated MKAF220C-M5SX WZP21230UBH none Image: Server 7 unessociated MKAF220C-M5SX WZP22120C6B none Image: Server 7 unessociated HKAF220C-M5SX WZP22120C6B none Image: Server 7 unessociated HKAF220C-M5SX WZP22120C6B none Image: Server 7 unessociated HKAF220C-M5SX WZP22120C61 none Image: Server 7 unessociated HKAF220C-M5SX WZP22120C61 none	Unas	ssociated (5)	Associated (6)					UCS Manager Host Name	10 29 132 50
Image: Server 2 unessociated HXAF220C-M55X WZP21230UBH none Image: Server 7 unessociated HXAF220C-M55X WZP22120C6B none Image: Server 8 unessociated HXAF220C-M55X WZP22120C8J none Image: Server 10 unessociated HXAF220C-M55X WZP22120C8J none Image: Server 11 unessociated HXAF220C-M55X WZP22120C6J none		-\$-	Server Name	Status	Model	Serial	Actions	UCS Manager User Name	admin
Image: Server 7 unessociated HXAF220C-M5SX WZP22120C68 none Image: Server 8 unessociated HXAF220C-M5SX WZP22120C83 none Image: Server 10 unessociated HXAF220C-M5SX WZP22120C85 none Image: Server 11 unessociated HXAF220C-M5SX WZP22120C61 none		(812)	Server 2	unassociated	HXAF220C-M55X	WZP21230UBH	none	Site Name	SiceA
Image: Server 8 unassociated HXAF220C-M55X WZP22120C85 none Image: Server 10 unassociated HXAF220C-M55X WZP22120C85 none Image: Server 11 unassociated HXAF220C-M55X WZP22120C61 none		60	Server 7	unassociated	HXAF220C-M55X	WZP22120C68	none		
Image: Server 10 unassociated HXAF220C-M55X WZP22120C85 none Image: Server 11 unassociated HXAF220C-M55X WZP22120C61 none		(07)	Server 8	unassociated	HXAF220C-M55X	WZP22120C8J	none		
Server 11 unassociated HX4F220C-M55X WZP22120C61 none			Server 10	unassociated	HXAF220C-M55X	WZP22120C85	none		
		.	Server 11	unassociated	HXAF220C-M55X	WZP22120C61	none		

The required server ports can be configured from Installer workflow but it will extend the time to complete server discovery. Therefore, we recommend configuring the server ports and complete HX node discovery in Cisco UCS Manager as described in the <u>Prerequisites</u> section prior to starting the workflow for HyperFlex installer.

Configure Server Ports (Optional)

If you choose to allow the installer to configure the server ports, follow these steps:

- 1. Click Configure Server Ports at the top right corner of the Server Selection window.
- 2. Provide the port numbers for each Fabric Interconnect in the form:

A1/x-y,B1/x-y where A1 and B1 designate Fabric Interconnect A and B and where x=starting port number and y=ending port number on each Fabric Interconnect.

3. Click Configure.

<u>6</u>

Credentials	Server Selection		Hypervisor Configuration	IP A:
rver Selection		Configure Server Ports	s ×	n line line line line line line line lin
		List all ports to be configured a	r repart ports	
Unassociated (0) Associated ((4)	A/1/17-20.B1/17-20	is server ports	
		HALF COULT CO		
	No unassociated se			
	Please login to UCS	Cancel	Configure	
	Launch UCS			
ulu HyperElex Installer	4.0(2d) ESXL			0 0 0 0 0
sco HyperFlex Installer	4.0(20) LONI			• • • • •
Credendals	5	erver Selection	UCSM Configuration	n Hypervisor Configuration
VLAN Configuration				Configuration *
VLAN for Hypervisor and HyperFlex	nanagement	VLAN for HyperFlex st	corage traffic	Credentials
VLAN Name VLA	NID	VLAN Name	VLAN ID	UCS Menager Host Name 10.29132.50
hx-inband-mgmt 3	0	hx-storage-data	101	UCS Manager User Name admir
				Site Name Site
VLAN for VM vMotion		VLAN for VM Network	C	Server Selection
VLAN Name VLA	NID	VLAN Name(s)	VLAN ID(s)	Server 7 W7273120C68 / HX40220C.M553
hx-vmotion 3	3	vm-network	34	Server 8 WZP22120C8I / HX4F220C-M551
				Server 10 WZP22120C85 / HXAF220C-M55X
				Server 11 WZP22120C61 / HXAF220C-M557
MAC POOL				
MAC Pool Prefix				
00:25:85: 08				
'hx-ext-mgmt' IP Pool for Cis	co IMC			
IP Blocks	Subnet Mask	G	Sateway	
10.29.132.41-44	255.255.255.0		10.29.132.1	
Cisco IMC access manageme	ent (Out of band or Inband	d)		
	0			
Uut of band 💿	○ In band ③			
> ISCSI Storage				
				K Back Continue
> FC Storage				
> FC Storage				
> FC Storage vanced				
> FC Storage vanced	HyperFlex Cluster Nam	16 0	irg Name	

4. Enter the Details for the Cisco UCS Manager Configuration:

- a. Enter VLAN ID for hx-inband-mgmt, hx-storage-data, hx-vmotion, vm-network.
- b. MAC Pool Prefix: The prefix to use for each HX MAC address pool. Please select a prefix that does not conflict with any other MAC address pool across all Cisco UCS domains.
- c. The blocks in the MAC address pool will have the following format:
 - \${prefix}:\${fabric_id}\${vnic_id}:{service_profile_id}
 }
 - The first three bytes should always be "00:25:B5".

The first three bytes should always be "00:25:B5."

- Enter range of IP address to create a block of IP addresses for external management and access to CIMC/KVM.
- 6. Cisco UCS firmware version is set to 4.0 (4g) which is the required Cisco UCS Manager release for Hyper-Flex v4.0(2d) installation.
- 7. Enter HyperFlex cluster name.
- 8. Enter Org name to be created in Cisco UCS Manager.
- 9. Click Continue.

Credenti	ia -	Server Selection	UCSM Configuration	Hypervisor Configuration
Configure common	Hypervisor Settings			Configuration
Subnet Mask	6	steway	DNS Server(s)	Credentials
255 255 255 0		10 10 30 1	10.10.31.21	UCS Manager Host Name 10.29.152.50
				UCS Manager User Name admin
				Site Name SiteA
Hypervisor Settings				Admin User name root
Make IP Addresses an	d Hostnames Sequential			Server Selection
				Server 7 WZP22120C6B / HXAF220C-M55X
41 + Name	Serial	Static IP Address	Hostname	Server 8 WZP22120C8J / HXAF220C-M55X
1	10.00000000000			Server 10 WZPZ2120C85 / HXAF220C-M55X
= (el) Server 7	WZP22120C6B	10.10.30.80	SiteA-1	Server 11 WZP22120C61 / HXAF220C-M55X
	4/7020100/08			UCSM Configuration
Server 8	WZPZZIZOCAJ	10.10.30.81	SiteA-2	VLAN Name hx-inband-mgmt
Source 10	4/7022120/285		OL Dimension	VLAN ID 30
Server 10	WEPZETEOCOJ	10.10.30.82	SteA-3	VLAN Name holstorage-data
- Server 11	W7022120/61	40.40.00.00	2014	VLAN ID 101
Server 1	THE LETEOLOGY	10.10.30.83	5084-4	VLAN Name bx-ymotion
				Video Manageria
				VLAN ID(S) 34
Hypervisor Credent	ials			MAC Pool Prefix 00:25:85:08
Admin User name	н	pervisor Password		IP Blocks 10.29.132.41-44
root			a	Subnet Mask 255.255.255.0
	1. J.			Gateway 10.29.132.1
				UCS Server Rimware Version 4.0(4g)

10. Repeat steps 1 - 9 for Site-B to configure both sites.

Configure Hypervisor Settings

To configure the Hypervisor settings, follow these steps:

- 1. In the Configure common Hypervisor Settings section, enter:
 - a. Subnet Mask
 - b. Gateway
 - c. DNS server(s)
- 2. In the Hypervisor Settings section:
 - a. Select check box Make IP Address and Hostnames Sequential if they are following in sequence.
 - b. Provide the starting IP Address.
 - c. Provide the starting Host Name or enter Static IP address and Host Names manually for each node
- 3. Click Configure Site.
- 4. Repeat steps 1 3 on Site B.

Deploy Cluster Witness Machine

Download the HyperFlex-Witness-1.x.x.ova appliance at https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(2b)

Complete the Deploy OVF Template wizard for the appliance to an ESX host that is NOT in the Stretch Cluster that will be used for VDI.

Be prepared to provide the following to customize the appliance:

- Appliance IP Address
- Subnet Mask
- Default Gateway
- DNS and NTP servers
- Search domains (i.e. cisco.com)
- Root password for the appliance

Notate the Witness appliance IP address to use when configuring the stretch cluster in the next steps.

Create Stretch Cluster

To create the Stretch Cluster, follow these steps:

1. On the installer screen, from the drop-down list select Stretch Cluster.

Select a Workflow			
		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	
	Create Cluster A Standard Cluster Edge Cluster	Expand Cluster	

- 2. Enter the Cluster information for both sites:
 - a. UCSM hostname or IP
 - b. UCSM username and password
 - c. Site Name
 - d. Org Name
 - e. Vcenter IP/Hostname, username and password.
 - f. Hypervisor username and password (the default password from the factory is Cisco123 and must be changed)

NUCLEAR CO. 000				uma 45769182507 •• 08104181919	
To setup stretch cluster you have to • Run the "Configure Site" wor • Download and deploy the Wi stretch cluster. • Run the "Create Stretch Clust	kilow ance for each site. Inness VM, per the user documentation. Provide the I ter" workflow, after both sites have been configured.	P address of the Witness VM when you	create the	Configuration	
 Configure Site UCS Manager Credentials for 	Create Stretch Cluster				
UCS Manager Host Name	User Name	Password			
UCSM-Site-A.sc.local	ədmin		0		
Site Name	Org Name				
Site-A	Site-A-Org				
				Drag and drop	
UCS Manager Credentials fo	or Site 7			Select a ISON File	
ocs manager credentials it	or site 2				
UCS Manager Host Name	User Name	Password			
UCSM-Site-B.sc.local	admin		0		
Site Name	Org Name				
Site-B	Site-B-Org				
vCenter Credentials					
vCenter Server	User Name	Admin Password			
vcenter.sc.local	administrator@vpshere.local		۰		
				Continue	
1999 - 1992 - 2014 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 -					
Hypervisor Credentials	5				
Admin User name					
1001					
The hypervisor on this node	e uses the factory default password	rd for the hypervisor			
New Password	Confirm New Password				
1		1000 C			

3. Select the servers from each site and click Continue.

		Credentials			Server	Selection	IP Addre	200		Our	er Configura	ten l	
Serve	er Selec	tion					Configure Server Parts	Refresh	Cont	figuratio	1		
 Se Ass 	rlect Node	rs for this site.							Crede	ntials			
-	1.000	Sac in March	E hea	Contract of	Model	Ladal	Canita Broffla	Arriana	UCS N	ler ager Hunt	Name 3	10.29	13
-	*	server merne y	- site	2101/05	(WIDDE)	achai	Service Prane	- Academia	User P	lama:			ad
	1080	Server 1	Site B	ok	HKAF220C-M5SX	WZP21480PQ5	org-root/org-Site-B/Is-rack-unit-1	Actions ~	UCS N	lor ager Hast	Name 2	10.29	.132
	80	Server 2	Site-B	ok	IDIAF220C-M55X	WZP21480PPD	org-root/org-Site-B/Is-rack-unit-2	Actions ~	UserN	lame			adr
	100	Server 3	Site-B	ok	HX4F220C-M5SX	WZP22310DPL	urg-root/org-Site-B/h-rack-unit-3	Autions ~	Site N	ame			S
		20000						1000000000	Org N	ame I			3
		Server 4	Site-B	OR	H04F220C-M35X	W2P21480PP3	orgrootiong site bits race unit-4	Actions V	Ore N	ame 2			
	140	Server 7	StreA	ok	HKAF220C-M55X	WZP22120C68	org-root/org-SiteA/Is-rack-unit-7	Actions ~	vCento	er Server		10.1	0.31
	(82)	Server 8	SiteA.	uk	H0/IF220C M5SX	WZP22120CBJ	org-root/org-SiteA/Is-rack-unit-8	Actions 9	Usert	lame	edministra	tor©xsphe	reir
	81	Server 10	SiteA	ok	HKAF220C-M5SX	W2P22120C85	org-root/org-SiteA/Is-rack-unit-10	Actions ~	Admin	Userrame			-
	100	Server 11	StreA.	ok	HKAF220C-M55X	WZP22120C61	org-root/org-StreA/Is-rack-unit-11	Actions ~					
												1000	_

4. Provide the IP addresses for the management and data networks on both sites.

IP Addresses

To add the IP addresses, follow these steps:

When the IP Addresses page appears, the hypervisor IP address for each node that was configured in the Hypervisor Configuration tab, appears under the Management Hypervisor column.

Three additional columns appear on this page:

- Storage Controller/Management
- Hypervisor/Data

• Storage Controller/Data

The Data network IP addresses are for vmkernel addresses for storage access by the hypervisor and storage controller virtual machine.

- 1. On the IP Addresses page, check the box Make IP Addresses Sequential or enter the IP address manually for each node for the following requested values:
 - a. Storage Controller/Management
 - b. Hypervisor/Data
 - c. Storage Controller/Data
- 2. Enter subnet and gateway details for the Management and Data subnets configured.

3. Click Continue.

			Credentia			Server	Selection		3	IP Addresses	Cluster Configuration
	IP a	Addre	isses								Configuration *
		Makel	P Addresses Sec	pential							Credentials
										UCS Manager Host Name 1 10.29:132:50	
					Managem	ent - VLAI	N 30		(FQDN or IP	Address)	User Name admin
							Stocare			Storage	UCS Manager Host Name 2 10.29.132.55
	12	•	Name	Sken	Hypervisor	G	Controller	9	Hypervisar	Controller @	User Name admin
											Site Name SiteA
	1.5	82	Server 11	SiteA	10.10.30,80		10.10.30.100		192.168,11.80	192.168.11.100	Org Name 1 SteA
											Site Name Site-B
		100	Server 10	SneA	10.10.30.81		10.10.30.101		192,168.11.81	192,168,11.101	Org Name 2 Site-B
											vCenter Server 10.10.31.40
	1.0	(80)	Server 7	SteA	10.10.30.82		10.10.30.102		192.168.11.82	192.168.11.102	User Name administrator@vsphere.local
											Admin User name root
	1.00	(1)	Server 8	SiteA	10.10.30.83		10.10.30.103		192,168.11.83	192.168.11.103	Server Selection
											Server 11 WZP22120C61 / HXAF220C-M55X
	1.04	80	Server 3	Site-B	10.10.30.84		10.10.30.104		192.168.11.84	192 168 11 104	Server 10 WZP22120C85 / HXAF220C-M55X
											Server 7 WZP22120C68 / HXAF220C-M55X
	-	185	Server 4	Site-B	10.10.30.85		10.10.30.105		192.158.11.85	192.168.11.105	Server 8 WZP22120C8) / HXAF220C-M55X
											Server 3 WZP22310DPL / HXAF220C-M55X
	1.0	160	Server 2	Site-B	10 10 30 86		10 10 30 106		192 168 11 86	192 168 11 106	Server 4 WZP21480PP3 / HXAF220C-M55X
											Server 2 WZP21480PPD / HXAF220C-M55X
		100	Server 1	Site-B	10 10 30 87		10 10 30 107		107 168 11 87	102 163 11 107	Server 1 WZP21480PQ5 / HXAF220C-M55X
						Managen	ment		Data		Continue Continue
	1	19	Server 2	See-B	10.10.30.86		10.10.30.1	106	192.168.11.86	192.168.11.106	Server 4 WZP21480PP3 / HXAF220
											Server 2 WZP21480PPD / HXAF220
			Server 1	Site-B	10,10,30.87		10.10.30.1	107	192.168.11.87	192.168.11.107	Server 1 WZP21480PQ5 / HXAF220
						Man	ugement		Data		< Back Continue
				0	star ID Address	1405-007-0	0.240	1.0	02 169 11 240		
					ALL A CARLESS	10.10.5	0.6.10		00.100.11.0.10		
					CubourMark	266.264	1.266.0	1.0	55 255 255 0		
					Journey Bridger.			1			
					German	10.10.3	0.1				
					Gateway'	20.10.3	40.1				
					in the second						
					Witness IP	10.10.3	4.134				

- 4. On the Cluster Configuration page, enter the following:
 - a. Cluster Name
 - b. Cluster management IP address
 - c. Cluster data IP Address
 - d. Replication Factor for Stretch Cluster is : 2 + 2
 - e. Controller virtual machine password
- f. vCenter configuration
 - vCenter Datacenter name
 - vCenter Cluster name
- g. System Services
 - DNS Server(s)
 - NTP Server(s)
 - Time Zone
- h. Auto Support
 - Click the check box for Enable Auto Support
 - Mail Server
 - Mail Sender
 - ASUP Recipient(s)
- i. Advanced Networking
 - Management vSwitch
 - Data vSwitch
- j. Advanced Configuration
 - · Click the check box to Optimize for VDI only deployment
 - Enable jumbo Frames on Data Network
 - Clean up disk partitions (optional)
 - vCenter Single-Sign-On server

Credentials	Server Selection	IP Addresses	Cluster Configuration
Cisco HX Cluster			Configuration
Cluster Name	Replication Factor		Credentials
hx1scip T	2+2 🗸 🗘		UCS Manager Host Name 1 10.29.1
*			User Name a
			UCS Manager Host Name 2 10.29.3
Controller VM			User Name a
Create Admin Password	Confirm Admin Password		Site Name
			Org Name 1
			Site Name 3
vCenter Configuration			Org Name 2
			vCenter Server 10.10.
vCenter Datacenter Name	vCenter Cluster Name		User Name administrator@vsphere
Stretch Cluster	Stretchuluster		Admin Uper name
			Server Selection
System Services			Server 11 WZP22120C61 / HXAF220C-
DNS Server(s)	NTP Server(s)	DNS Domain Name	Server 10 WZP22120C85 / HXAF220C-
10.10.31.21	10.10.31.21	hxhvdom local	Server 8 WZP22120C8I / HX4E220C4
Time Texa			Server 3 WZP22310DPL / HXAF220C/
UTC 09:00 Desite Tor			Server 4 WZP21480PP3 / HXAF220C-
(010-00.00) Pacine Time	u		Server 2 WZP21480PPD / HXAF220C-
Auto Support. Enable Cannected Services (Recommended)	Send service ticket notifications to		K Back Start
Auto Support. Canable Connected Services (Recommended) When Connected Services are enabled. Cisco of	Send service ticket notifications to	and its deployment environment for the	K Back Start
Auto Support. Chable Connected Services (Recommended) When Connected Services are enabled. Cisco of	Send service ticket notifications to	and its deployment environment for the	K Back Start
Auto Support. Carbon Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco of purpose of delivering a better product and su	Send service ticket notifications to periodically collects information about the cluster speriodically collects information about the cluster upport experience.	and its deployment environment for the	K Beck Stert
Auto Support. Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco of purpose of delivering a better product and so	Send service ticket notifications to periodically collects information about the cluster periodically collects information about the cluster upport experience.	and its deployment environment for the	K Back Start
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco purpose of delivering a better product and su Web Proxy Settings for Connected Services	Send service ticket notifications to eriodically collects information about the cluster periodically collects information about the cluster upport experience.	and its deployment environment for the	C Back Start
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server ©	Send service ticket notifications to enriodically collects information about the cluster speriodically collects information about the cluster upport experience.	and its deployment environment for the	K Back Scart
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Web Proxy Server	Send service ticket notifications to enriodically collects information about the cluster periodically collects information about the cluster upport experience. Port	and its deployment environment for the	C Back Start
Auto Support.	Send service ticket notifications to periodically collects information about the cluster operiodically collects information about the cluster upport experience. Port	and its deployment environment for the	C Back Start
Auto Support. Enable Connected Services (Recommended) When Connected Services are enabled. Cisco or When Connected Services are enabled. Cisco purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Use Proxy Server 10.10.30.127 Username	Send service ticket notifications to Deriodically collects information about the cluster speriodically collects information about the cluste upport experience. Port 0 Password Password	and its deployment environment for the	C Back Start
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Use Proxy Server 10.10.30.127 Username	Send service ticket notifications to ceriodically collects information about the cluster aperiodically collects information about the cluste upport experience. Port 80 Password	and its deployment environment for the r and its deployment environment for the	K Back Start
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Use Proxy Server 10.10.30.127 Username	Send service ticket notifications to enriodically collects information about the cluster periodically collects information about the cluste upport experience. Port 0 Password	and its deployment environment for the	K Back Start
Auto Support	Send service ticket notifications to aeriodically collects information about the cluster upport experience. Port 80 Password	and its deployment environment for the	EF Addresses
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco of purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Use Proxy Server 10.10.30.127 Username Advanced Networking Management VLANTar - Gar 1	Send service ticket notifications to aeriodically collects information about the cluster periodically collects information about the cluste upport experience. Port 0 Pars Management VI AN Tap., Sup 3	and its deployment environment for the	C Back Start
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco or When Connected Services are enabled. Cisco or purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Use Proxy Server 10.10.30.127 Username Advanced Networking Management VLAN Tag - Site 1 30	Send service ticket notifications to eriodically collects information about the cluster upport experience. Port 0 Port Nanagement VLAN Tag - Site 2 30	and its deployment environment for the r and its deployment environment for the	C Back Store
Auto Support	Send service ticket notifications to ceriodically collects information about the cluster aperiodically collects information about the cluste upport experience. Port 0 Password Management VLAN Tag - Site 2 30	and its deployment environment for the r and its deployment environment for the	C Back Start
Auto Support Enable Connected Services Recommended) When Connected Services are enabled. Cisco or When Connected Services are enabled. Cisco or purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server Username Advanced NetWorking Management VLAN Tag - Site 1 30 Data VLAN Tag - Site 1	Send service ticket notifications to aeriodically collects information about the cluster aperiodically collects information about the cluste upport experience. Port 80 Password Management VLAN Tag - Site 2 30 Data VLAN Tag - Site 2	and its deployment environment for the r and its deployment environment for the Management vSwitch vswitch-tw-inband-regmt Data vSwitch	C Back Stert
Auto Support Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco of purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server 10.10.30.127 Username Advanced Networking Management VLAN Tag - Site 1 30 Data VLAN Tag - Site 1 101	Send service ticket notifications to enriodically collects information about the cluster periodically collects information about the cluste upport experience. Port 0 Port 0 Management VLAN Tag - Site 2 101	and its deployment environment for the r and its deployment environment for the Management vSwitch vswitch-to:-inband-mgmt Data vSwitch vswitch-to:-storage-date	EF ADDRESSES
Auto Support	Send service ticket notifications to aeriodically collects information about the cluster periodically collects information about the cluste upport experience. Port 80 Password Management VLAN Tag - Site 2 30 Data VLAN Tag - Site 2 101	and its deployment environment for the r and its deployment environment for the management vSwitch vswitch-hu-inband-mgmt Data vSwitch vswitch-hu-istorage-data	EF Addresses
Auto Support	Send service ticket notifications to aeriodically collects information about the cluster periodically collects information about the cluste upport experience. Port 0 Pars Pars Management VLAN Tag - Site 2 101	and its deployment environment for the r and its deployment environment for the management viswitch www.tch-tou-iband-mgmt Data viswitch www.tch-tou-iborage-data	C Back Stert
Auto Support	Send service ticket notifications to aeriodically collects information about the cluster periodically collects information about the cluste upport experience. Port 0 Password Management VLAN Tag - Site 2 101 Disk Partitions	and its deployment environment for the r and its deployment environment for the Management vSwitch vswitch-tou-inband-regmt Data vSwitch vswitch-tou-storage-data	C Back Stert
Auto Support	Send service ticket notifications to eriodically collects information about the cluster aperiodically collects information about the cluste upport experience. Port 80 Password B0 Password Data VLAN Tag - Site 2 101 Disk Partitions Clean up disk partitions Clean up disk partitions	and its deployment environment for the r and its deployment environment for the Management vSwitch vswitch-to-inband-mgmt Data vSwitch vswitch-ho-istorage-data	C Back Store
Auto Suppor: Enable Connected Services (Recommended) When Connected Services are enabled. Cisco of When Connected Services are enabled. Cisco of purpose of delivering a better product and so Web Proxy Settings for Connected Services Use Proxy Server 10.10.30.127 Username Advanced Networking Management VLAN Teg - Site 1 30 Data VLAN Tag - Site 1 101 Advanced Configuration Jumbo Frames Enable Jumbo Frames on Data Network Venter Single-Sign On Server	Send service ticket notifications to ceriodically collects information about the cluster partiodically collects information about the cluster port Port 80 Password Management VLAN Tag - Site 2 30 Data VLAN Tag - Site 2 101 Disk Partitions Clean up disk partitions	and its deployment environment for the r and its deployment environment for the management vSwitch vswitch-to:-inband-mgmt Data vSwitch vswitch-to:-storage-data	C Back Start

If the QoS system class is not defined as per the requirement HyperFlex installer will go ahead and make required changes. A warning is generated accordingly in HyperFlex Installer workflow. Post-install Con-figuration.

Prior to putting a new HyperFlex cluster into production, a few post-install tasks must be completed. To automate the post installation procedures and verify the HyperFlex cluster configuration, a post_install script has been provided on the HyperFlex Controller VMs. To run this script, follow these steps:

1. SSH to the cluster management IP address and login using <root> username and the controller VM password provided during installation. Verify the cluster is online and healthy using "stcli cluster info" or "stcli cluster storage-summary."



2. Run the following command in the shell, and press enter:

/usr/share/springpath/storfs-misc/hx-scripts/post_install.py

- 3. Select the first post_install workflow type New/Existing Cluster.
- 4. Enter the HX Storage Controller VM root password for the HX cluster (use the one entered during the HX Cluster installation).
- 5. Enter the vCenter server username and password.

<pre>root@SpringpathControllerT7DB8MDX0A:~# /usr/share/springpath/storfs-misc/hx-scripts/post_install.py</pre>
Select post_install workflow-
 New/Existing Cluster Expanded Cluster Generate Certificate
Note: Workflow No.3 is mandatory to have unique SSL certificate in the cluster. By Generating this certificate, it will replace your current certificate. If you're performing cluster expansion, then this option is not required.
Selection: 1 Logging in to controller localhost
HX CVM admin password: Getting FSX hosts from HX cluster
VCenter URL: 10.29.133.120
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Found Gatacenter Datacenter
post_install to be run for the following hosts:
hxaf220m5n-01.hx.lab.cisco.com
hxaf220m5n-02.hx.lab.cisco.com
hxaf220m5h.04 by lab cisco.com
hxaf220m5n-05.hx.lab.cisco.com
hxaf220m5n-06.hx.lab.cisco.com
hxaf220m5n-07.hx.lab.cisco.com
hxaf220m5n-08.hx.lab.cisco.com

- 6. Enter ESXi host root password (use the one entered during the HX Cluster installation).
- 7. You must license the vSphere hosts through the script or complete this task in vCenter before continuing. Failure to apply a license will result in an error when enabling HA or DRS in subsequent steps. Enter "n" if you have already registered the license information in vCenter.
- 8. Enter "y" to enable HA/DRS.
- 9. Enter "y" to disable the ESXi hosts' SSH warning. SSH running in ESXi is required in HXDP 2.6.
- 10. Add the vMotion VMkernel interfaces to each node by entering "y." Input the netmask, the vMotion VLAN ID, and the vMotion IP addresses for each of the hosts as prompted.

```
Enter ESX root password:
Enter vSphere license key? (y/n) n
Enable HA/DRS on cluster? (y/n) y
Successfully completed configuring cluster HA.
Successfullý completed configuring cluster DRS.
Disable SSH warning? (y/n) y
Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.255.0
VLAN ID: (0-4096) 200
vMotion MTU is set to use jumbo frames (9000 bytes). Do you want to change to 1500 bytes? (y/n) n
vMotion IP for hxaf220m5n-01.hx.lab.cisco.com: 192.168.200.61
Adding vmotion-200 to hxaf220m5n-01.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-01.hx.lab.cisco.com
vMotion IP for hxaf220m5n-02.hx.lab.cisco.com: 192.168.200.62
Adding vmotion-200 to hxaf220m5n-02.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-02.hx.lab.cisco.com
vMotion IP for hxaf220m5n-03.hx.lab.cisco.com: 192.168.200.63
Adding vmotion-200 to hxaf220m5n-03.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-03.hx.lab.cisco.com
vMotion IP for hxaf220m5n-04.hx.lab.cisco.com: 192.168.200.64
Adding vmotion-200 to hxaf220m5n-04.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-04.hx.lab.cisco.com
vMotion IP for hxaf220m5n-05.hx.lab.cisco.com: 192.168.200.65
Adding vmotion-200 to hxaf220m5n-05.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-05.hx.lab.cisco.com
vMotion IP for hxaf220m5n-06.hx.lab.cisco.com: 192.168.200.66
Adding vmotion-200 to hxaf220m5n-06.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-06.hx.lab.cisco.com
vMotion IP for hxaf220m5n-07.hx.lab.cisco.com: 192.168.200.67
Adding vmotion-200 to hxaf220m5n-07.hx.lab.cisco.com
Adding vmkernel to hxaf220m5n-07.hx.lab.cisco.com
vMotion IP for hxaf220m5n-08.hx.lab.cisco.com: 192.168.200.68
Adding vmotion-200 to hxaf220m5n-08.hx.lab.cisco.com
 Adding vmkernel to hxaf220m5n-08.hx.lab.cisco.com
```

- 11. You may add VM network portgroups for guest VM traffic. Enter "n" to skip this step and create the portgroups manually in vCenter. Or if desired, VM network portgroups can be created and added to the vmnetwork vSwitch. This step will add identical network configuration to all nodes in the cluster.
- 12. Enter "y" to run the health check on the cluster.
- 13. A summary of the cluster will be displayed upon completion of the script. Make sure the cluster is healthy.

Initial Tasks and Testing

Datastores for a Stretch Cluster

When creating datastores for a stretch cluster, we recommend creating two datastores, one on each site with 50% of the total workload residing on each site datastore. For example, for 500 total VDI users, 250 desktops would be on datastore-site-A and 250 desktops would be on datastore-site-B.

Create a datastore for storing the virtual machines. This task can be completed by using the HyperFlex Connect HTML management webpage. To configure a new datastore via the HyperFlex Connect webpage, follow these steps:

- 1. Use a web browser to open the HX cluster IP management URL.
- 2. Enter a local credential or a vCenter RBAC credential with administrative rights for the username, and the corresponding password.

- 3. Click Login.
- 4. Click Datastores in the left pane and click Create Datastore.
- In the popup, enter the Datastore Name and size. For most applications, leave the Block Size at the default of 8K. Only dedicated Virtual Desktop Infrastructure (VDI) environments should choose the 4K Block Size option.
- 6. Select Site Affinity for each site (datastore-site-A would have 'Site-A' for Site Affinity, datastore-site-B would have 'Site-B' for Site Affinity.)
- 7. Click Create Datastore.

НX	(Conn	ect							
			1	Create Datastore		08			
				Datastore Name					
				Size		Block Size			
				1	GB 👻	8К т			
				Site Affinity					
				< Site A >		÷			
					Cancel	eate Datastore			
Datastore	2S							Last refreshed a	e: 10/31/2017 4:30:16 PM ⊖
🖬 Create Data	astore 🖉 Edit 🗸 Mount 🔇	Ounmount × Delete						÷ ~	Filter
	Name ^	Mount Summary	Site Affinit	ty	Status		Size	Used	Free
	DS1	MOUNTED	Site A		Normal		100 TB	245 GB	100 TB
	DS2	MOUNTED	Site B		Normal		100 GB	0 B	100 GB

Showing 1 - 2 of 2

Create VM

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

vm vSphe	ere Client Menu 🗸	Q Search in all environments	
	■ <u>9</u> ■ 8x1	6-ESX ACTIONS -	
✓ ☐ 10.10.31.40	Summary	Monitor Configure Permissions	Hosts VN
✓ ■ 8×16-F	cy	Resource Pools	
10.	Actions - 8x16-ESX	Readine Pools	
10.	1 Add Hosts		
10.	Dow Virtual Machine	~	State
10.	D New Virtual Machine		Connected
10.	New Resource Pool		Connected
10.	Deploy OVF Template		Connected
10.	H New vApp		Connected
10.	Storage		Connected
10.	Storage		Connected
10.	Host Profiles	•	Connected
10.	Edit Default VM Compatibilit	v	Connected
10.	201 10 10 10 10 10 10 10 10 10 10 10 10 1		Connected
10.		-	Connected
10			

Audit Logging

By default, the HyperFlex controller VMs store logs locally for many functions, including the filesystem logs, security auditing, CLI commands and shell access, single sign-on logs, and more. These logs are rotated periodically and could be lost if there were a total failure of a controller VM. In order to store these logs externally from the HyperFlex cluster, audit logging can be enabled in HX Connect to send copies of these logs to an external syslog server. From this external location, logs can be monitored, generate alerts, and stored long term. HX Connect will not monitor the available disk space on the syslog destination, nor will it generate an alarm if the destination server is full. To enable audit logging, follow these steps:

- 1. Use a web browser to open the HX cluster IP management URL.
- 2. From the HyperFlex Connect webpage, click the gear shaped icon in the upper right-hand corner, and click Audit Log Export Settings.
- 3. Click to check the box to Enable audit log export to an external syslog server.
- 4. Enter the syslog server IP address and TCP port.
- 5. Choose TCP or TLS as the connection type. If using TLS, client certificate and private key pair files must be provided. Alternatively, a self-signed certificate can be used. Click browse to select the appropriate files.
- 6. Click OK.

Enable audit log export	t to an external syslog :	server		
Syslog server	10.29.132.145			
Port	6514			
Connection Type	тср	~	0	

7. Audit log exports can be temporarily disabled or completely deleted at a later time from the same location.

To store ESXi diagnostic logs in a central location in case they are needed to help diagnose a host failure, it is recommended to enable a syslog destination for permanent storage of the ESXi host logs for all Cisco HyperFlex hosts. It is possible to use the vCenter server as the log destination in this case, or another syslog receiver of your choice.

To configure syslog for ESXi, follow these steps:

- 1. Log on to the ESXi host via SSH as the root user.
- 2. Enter the following commands, replacing the IP address in the first command with the IP address of the vCenter server that will receive the syslog logs:

```
[root@hx220-01:~] esxcli system syslog config set --loghost='udp://10.29.132.120'
[root@hx220-01:~] esxcli system syslog reload
[root@hx220-01:~] esxcli network firewall ruleset set -r syslog -e true
[root@hx220-01:~] esxcli network firewall refresh
```

3. Repeat these steps for each ESXi host.

Auto-Support and Notifications

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

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

- Cluster Capacity Changed
- Cluster Unhealthy
- Cluster Health Critical
- Cluster Read Only

- Cluster Shutdown
- Space Warning
- Space Alert
- Space Critical
- Disk Blacklisted
- Infrastructure Component Critical
- Storage Timeout

To change Auto-Support settings, follow these steps:

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

=	cisco HyperFlex Connect		Al	I-NVMe			@ 0 A
0	Dashboard	VIRTUA 1 VM	Auto-Support Settings	(38		
	TOR Alarms	Virtual Mach	Enable Auto-Support (Recommended) Send service ticket notifications to	alerts@customer.com		Last refreshed a	с 09/24/2019 3:35:44 Рм
iii	Activity	Ready Clones	When Connected Services are enabled, Cisco periodica environment for the purpose of delivering a better pro	Illy collects information about the cluster and its deploymer iduct and support experience	nt	₽~ (
ANAL	rze	Name	Enable Remote Support 🕕 📥		or	age Provisioned	Storage Used
PROT	Performance	UM1	Web Proxy Settings Use Proxy Server		5 G	В	16 GB
¢	Replication	Showing 1 - 1 of		Cancel	ок		
MANA	GE			concer			
	System Information Datastores						
Ģ	Virtual Machines						



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

To enable direct email notifications, follow these steps:

1. From the HyperFlex Connect webpage, click the gear shaped icon in the upper right-hand corner, and click Notifications Settings.

- 2. Enter the DNS name or IP address of the outgoing email server or relay, the email address the notifications will come from, and the recipients.
- 3. Click OK.

Notifications Settings		⊘⊗
Send email notifications for alarms		
Mail Server Address	outbound.cisco.com	
From Address	AFCluster8node@hx.lab.cisco.com	
Recipient List (Comma separated)	@cisco.com	
		A
	Cancel	ОК

Smart Licensing

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

To create a Smart Account, see Cisco Software Central > Request a Smart Account: <u>https://webapps.cisco.com/software/company/smartaccounts/home?route=module/accountcreation</u>.

To activate and configure smart licensing, follow these steps:

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

```
# stcli license show status
Smart Licensing is ENABLED
Registration:
Status: UNREGISTERED
Export-Controlled Functionality: Not Allowed
License Authorization:
Status: EVAL MODE
Evaluation Period Remaining: 88 days, 1 hr, 33 min, 41 sec
Last Communication Attempt: NONE
```

```
License Conversion:
Automatic Conversion Enabled: true
Status: NOT STARTED
Utility:
Status: DISABLED
Transport:
```

```
Type: TransportCallHome
```

- 2. Feedback will show Smart Licensing is ENABLED, Status: UNREGISTERED, and the amount of time left during the 90-day evaluation period (in days, hours, minutes, and seconds).
- 3. Navigate to Cisco Software Central (https://software.cisco.com/) and log in to your Smart Account.
- 4. From Cisco Smart Software Manager, generate a registration token.
- 5. In the License pane, click Smart Software Licensing to open Cisco Smart Software Manager.
- 6. Click Inventory.
- From the virtual account where you want to register your HX storage cluster, click General, and then click New Token.
- 8. In the Create Registration Token dialog box, add a short Description for the token, enter the number of days you want the token to be active and available to use on other products, and check Allow export-controlled functionality on the products registered with this token.
- 9. Click Create Token.
- 10. From the New ID Token row, click the Actions drop-down list, and click Copy.
- 11. Log into a controller VM.
- 12. Register your HX storage cluster, where *idtoken-string* is the New ID Token from Cisco Smart Software Manager.

stcli license register --idtoken idtoken-string

13. Confirm that your HX storage cluster is registered.

stcli license show summary

The cluster is now ready. You may run any other preproduction tests that you wish to run at this point.

ESXi Hypervisor Installation

HX nodes come from the factory with a copy of the ESXi hypervisor pre-installed, however there are scenarios where it may be necessary to redeploy or reinstall ESXi on an HX node. In addition, this process can be used to

deploy ESXi on rack mount or blade servers that will function as HX compute-only nodes. The HyperFlex system requires a Cisco custom ESXi ISO file to be used, which has Cisco hardware specific drivers pre-installed, and customized settings configured to ease the installation process. The Cisco custom ESXi ISO file is available to download at cisco.com.

ESXi Kickstart ISO

The HX custom ISO is based on the Cisco custom ESXi 6.7 Update 3 ISO release with the filename: HX-ESXi-6.7U3-15160138-Cisco-Custom-6.7.3.3-install-only.iso and is available on the Cisco web site:

https://software.cisco.com/download/home/286305544/type/286305994/release/4.0(2a)

The custom Cisco HyperFlex ESXi ISO will automatically perform the following tasks with no user interaction required:

- Accept the End User License Agreement
- Configure the root password to: Cisco123
- Install ESXi to the internal mirrored Cisco FlexFlash SD cards, or the internal M.2 SSD
- Set the default management network to use vmnic0, and obtain an IP address via DHCP
- Enable SSH access to the ESXi host
- Enable the ESXi shell
- Enable serial port com1 console access to facilitate Serial over LAN access to the host
- Configure the ESXi configuration to always use the current hardware MAC address of the network interfaces, even if they change
- Rename the default vSwitch to vswitch-hx-inband-mgmt

Reinstall HyperFlex Cluster

If a Cisco HyperFlex cluster needs to be reinstalled, contact your local Cisco account or support team in order to be provided with a cluster cleanup guide.



This process will be destructive and result in the loss of all the VMs and all the data stored in the Hyper-Flex distributed filesystem.

To reinstall a HyperFlex cluster, follow these steps:

- 1. Clean up the existing environment by:
 - a. Delete the existing HX virtual machines and HX datastores.
 - b. Destroy the HX cluster.
 - c. Remove the HX cluster from vCenter.
 - d. Remove the vCenter MOB entries for the HX extension.
 - e. Delete the HX sub-organization and HX VLANs in Cisco UCS Manager.

2. Using the HX OVA-based installer VM, use the customized version of the installation workflow by selecting the "I know what I am doing" link.

ılıılı cısco	HyperFlex Installer	0	0	•	ø ~
	Workflow				
Selec	t a Workflow				
		*			
	Create Cluster 🔻				
🔒 l kr	ow what I'm doing, let me customize my workflow				

3. Use customized workflow and only choose the "Run UCS Manager Configuration" option, click Continue.

cisco HyperFlex Installer			0			ø -
		Workflow				
Select a Workflow						
		Run UCS Manager Configuration				
		Run Hypervisor Configuration				
		Deploy HX Software				
	Create HX Cluster	Expand HX Cluster				
Show me the standard workflows				1	Continue	2

- 4. When the Cisco UCS Manager configuration is complete, HX hosts are associated with HX service profiles and powered on. Now perform a fresh ESXi installation using the custom ISO image and following the steps in section <u>Cisco UCS vMedia and Boot Polices</u>.
- 5. When the ESXi fresh installations are all finished, use the customized workflow, and select the remaining 3 options; ESXi Configuration, Deploy HX Software, and Create HX Cluster, to continue and complete the HyperFlex cluster installation.

diality HyperFlex Installer			0	0	Ø ~
		Workflow			
Select a Workflow					
		Run UCS Manager Configuration			
	×	Run Hypervisor Configuration			
	2	Deploy HX Software			
	Create HX Cluster	Expand HX Cluster			
Show me the standard workflows				Contin	ue

Cisco UCS vMedia and Boot Policies

Ô

By using a Cisco UCS vMedia policy, the custom Cisco HyperFlex ESXi installation ISO file can be mounted to all of the HX servers automatically. The existing vMedia policy, named "HyperFlex" must be modified to mount this file, and the boot policy must be modified temporarily to boot from the remotely mounted vMedia file. Once these two tasks are completed, the servers can be rebooted, and they will automatically boot from the remotely mounted vMedia file, installing and configuring ESXi on the servers.

WARNING! While vMedia policies are very efficient for installing multiple servers, using vMedia policies as described could lead to an accidental reinstall of ESXi on any existing server that is rebooted with this policy applied. 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 ESXi 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, follow these steps:

- 1. Copy the *HX-ESXi-6.7U3-15160138-Cisco-Custom-6.7.3.3-install-only.iso* file to an available web server folder, NFS share or CIFS share. In this example, an open internal web server folder is used.
- 2. In Cisco UCS Manager, click Servers.
- 3. Expand Servers > Policies > root > Sub-Organizations > <<HX_ORG>> > vMedia Policies and click vMedia Policy HyperFlex.
- 4. In the configuration pane, click Create vMedia Mount.
- 5. Enter a name for the mount, for example: ESXi.
- 6. Select the CDD option.
- 7. Select CIFS as the protocol.
- 8. Enter the IP address of the CIFS server where the file was copied, for example: 10.29.132.120
- 9. Select None as the Image Variable Name.
- 10. Enter HX-ESXi-6.7U3-15160138-Cisco-Custom-6.7.3.3-install-only.iso as the Remote File.
- 11. Enter the Remote Path to the installation file.

Vame	ESXI	
Description		
evice Type		
Protocol		
Authentication Protoco	Ntim	
lostname/IP Address	10.29.132.145	
nage Name Variable	None Service Profile Name	
emote File	HX-ESXi-6.7U3-15160138-Cisco-C	ustom-6.7.3.3-
emote Path	iso	
lsemame		
Password		
eman on Fiect		

- 12. Click OK.
- 13. Select Servers > Service Profile Templates > root > Sub-Organizations > <<HX_ORG>> > Service Template hx-nodes.

- 14. In the configuration pane, click the vMedia Policy tab.
- 15. Click Modify vMedia Policy.
- 16. Chose the HyperFlex vMedia Policy from the drop-down selection and click OK twice.
- 17. For Compute-Only nodes (if necessary), select Servers > Service Profile Templates > root > Sub-Organizations > <<HX_ORG>> > Service Template compute-nodes.
- 18. In the configuration pane, click the vMedia Policy tab.
- 19. Click Modify vMedia Policy.
- 20. Chose the HyperFlex vMedia Policy from the drop-down selection and click OK twice.
- 21. Select Servers > Policies > root > Sub-Organizations > <<HX_ORG>> > Boot Policy HyperFlex.
- 22. In the navigation pane, expand the section titled CIMC Mounted vMedia.
- 23. Click the entry labeled Add CIMC Mounted CD/DVD.
- 24. Select the CIMC Mounted CD/DVD entry in the Boot Order list and click the Move Up button until the CIMC Mounted CD/DVD entry is listed first.
- 25. Click Save Changes and click OK.

Local Devices	Boot Order						
	+ - Te Advanced Filter	♠ Export	🖶 Prin	t			
\ominus	Name	Or▲	vNIC	Туре	WWN	LUN	S
CIMC Mounted vMedia	CIMC Mounted CD/DVD	1					
Add CIMC Mounted CD/DVD	CD/DVD	2					
Add CIMC Mounted HDD	SD Card	3					
(+) vNICs							
+ vHBAs		t	Move Up	Mov	ve Down	🗊 Delete	Э
(+) iSCSI vNICs							
+ EFI Shell							

Install ESXi

To begin the installation after modifying the vMedia policy, Boot policy and service profile template, the servers need to be rebooted. To complete the reinstallation, it is necessary to open a remote KVM console session to each server being worked on. To open the KVM console and reboot the servers, follow these steps:

- 1. In Cisco UCS Manager, click Equipment.
- 2. Expand Equipment > Rack mounts > Servers > Server 1.
- 3. In the configuration pane, click KVM Console.

- 4. The remote KVM Console window will open in a new browser tab. Click Continue to any security alerts that appear and click the hyperlink to start the remote KVM session.
- 5. Repeat Steps 2-4 for all additional servers whose console you need to monitor during the installation.
- 6. In Cisco UCS Manager, click Equipment.
- 7. Expand Equipment > Rack-Mount Servers > Servers.
- 8. In the configuration pane, click the first server to be rebooted, then shift+click the last server to be rebooted, selecting all of the servers.
- 9. Right-click the mouse and click Reset.

Equipment



10. Click OK.

- 11. Select Power Cycle and click OK.
- 12. Click OK. The servers you are monitoring in the KVM console windows will now immediately reboot, and boot from the remote vMedia mount. Alternatively, the individual KVM consoles can be used to perform a power cycle one-by-one.
- 13. When the server boots from the installation ISO file, you will see a customized Cisco boot menu. In the Cisco customized installation boot menu, select "HyperFlex Converged Node HX PIDs Only" and press enter.



14. Enter "ERASE" in all uppercase letters, and press Enter to confirm and install ESXi.



- 15. (Optional) When installing Compute-Only nodes, the appropriate Compute-Only Node option for the boot location to be used should be selected. The "Fully Interactive Install" option should only be used for debug-ging purposes.
- 16. The ESXi installer will continue the installation process automatically, there may be error messages seen on screen temporarily, but they can be safely ignored. When the process is complete, the standard ESXi console screen will be seen as below:



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, follow these steps:

- 1. Select Servers > Policies > root > Sub-Organizations > <<HX_ORG>> > Boot Policy HyperFlex.
- 2. Select the CIMC Mounted CD/DVD entry in the Boot Order list and click Delete.
- 3. Click Save Changes and click OK.

The changes made to the vMedia policy and service profile template may also be undone once the ESXi installations have all completed fully, or they may be left in place for future installation work.

Management

HyperFlex Connect

HyperFlex Connect is the new, easy to use, and powerful primary management tool for HyperFlex clusters. HyperFlex Connect is an HTML5 web-based GUI tool which runs on all of the HX nodes and is accessible via the cluster management IP address.

Local Access

Logging into HyperFlex Connect can be done using pre-defined local accounts. The default predefined administrative account is named "admin". The password for the default admin account is set during the cluster creation as the cluster password. Using local access is only recommended when vCenter direct or SSO credentials are not available.

Role-Based Access Control

HyperFlex Connect provides Role-Based Access Control (RBAC) via integrated authentication with the vCenter Server managing the HyperFlex cluster. You can have two levels of rights and permissions within the HyperFlex cluster:

- Administrator: Users with administrator rights in the managing vCenter server will have read and modify rights within HyperFlex Connect. These users can make changes to the cluster settings and configuration.
- Read-Only: Users with read-only rights in the managing vCenter server will have read rights within Hyper-Flex Connect. These users cannot make changes to the cluster settings and configuration.

Users can log into HyperFlex Connect using direct vCenter credentials, for example, <u>administra-</u> <u>tor@vsphere.local</u>, or using vCenter Single Sign-On (SSO) credentials such as an Active Directory user, for example, domain\user. Creation and management of RBAC users and rights must be done via the vCenter Web Client or vCenter 6.5 HTML5 vSphere Client.

To manage the HyperFlex cluster using HyperFlex Connect, follow these steps:

- 1. Using a web browser, open the HyperFlex cluster's management IP address via HTTPS.
- 2. Enter a local credential, such as local/root, or a vCenter RBAC credential for the username, and the corresponding password.
- 3. Click Login.
- 4. The Dashboard view will be shown after a successful login.

Dashboard

From the Dashboard view, several elements are presented:

- Cluster operational status, overall cluster health, and the cluster's current node failure tolerance.
- Cluster storage capacity used and free space, compression and deduplication savings, and overall cluster storage optimization statistics.
- Cluster size and individual node health.

• Cluster IOPs, storage throughput, and latency for the past 1 hour.

Monitor

HyperFlex Connect provides for additional monitoring capabilities, including:

- Alarms: Cluster alarms can be viewed, acknowledged, and reset.
- Event Log: The cluster event log can be viewed, specific events can be filtered for, and the log can be exported.
- Activity Log: Recent job activity, such as ReadyClones can be viewed, and the status can be monitored.

=	cisco HyperFlex Connect			All-NVMe							
Ø	Dashboard	Alarms						Last refreshed at: 09/19	V2019 9:10	207 AM 🗧	>
мог	NITOR	Acknowledge 🔸 Re									
۵	Alarms	Severity	Source Des	cription	Time ~	Acknowledged		Acknowledged By			
坹	Events	Severity	bounce bes	criperon.		ActionicaBea		, leaded by			
Û	Activity			No ri	ecords found						
	1976										
E.L.	Barformanco										
Entti	Performance										
=	ျမား ငေးငစ် HyperFlex Connect			All-NVMe							
Ø	Dashboard	Filter Filter listed	events								
мог	NITOR										
۵	Alarms	Events 🖻 🗸		09/13/2019 11:00:	12 AM - 09/19/2019 9:07:3	4 AM All 🚺 🙆	00	Last refreshed at: 09/19/20)19 9:10:31	iam O	
会	Events										
Ê	Activity	3 minutes ago	warning: Local user login is no 09/19/2019 9:07:34 AM MDT	t preferred							
ana Edh	Performance	4 minutes ago	warning: Local user login is no 09/19/2019 9:06:33 AM MDT	t preferred							

Analyze

The historical and current performance of the HyperFlex cluster can be analyzed via the built-in performance charts. The default view shows read and write IOPs, bandwidth, and latency over the past 1 hour for the entire cluster. Views can be customized to see individual nodes or datastores, and change the timeframe shown in the charts.



Protect

HyperFlex Connect is used as the management tool for all configuration of HyperFlex Data Protection features, including VM replication and data-at-rest encryption.

Manage

HyperFlex Connect presents several views and elements for managing the HyperFlex cluster:

- System Information: Presents a detailed view of the cluster configuration, software revisions, hosts, disks, and cluster uptime. Support bundles can be generated to be shared with Cisco TAC when technical support is needed. Views of the individual nodes and the individual disks are available. In these views, nodes can be placed into HX Maintenance Mode, and self-encrypting disks can be securely erased.
- Datastores: Presents the datastores present in the cluster, and allows for datastores to be created, mounted, unmounted, edited or deleted, as described earlier in this document as part of the cluster setup.
- Virtual Machines: Presents the VMs present in the cluster and allows for the VMs to be powered on or off, cloned via HX ReadyClone, Snapshots taken, and protected via native replication.
- Upgrade: One-click upgrades to the HXDP software, ESXi host software and Cisco UCS firmware can be initiated from this view.
- Web CLI: A web-based interface, from which CLI commands can be issued and their output seen, as opposed to directly logging into the SCVMs via SSH.

≡ ^{•(])•(])•} HyperFlex Connect	All-NVMe	© © £
🕐 Dashboard	System Overview Nodes Disks	Last refreshed at: 09/19/2019 9:18:58 AM
MONITOR	All-NVMe ONLINE vCenter https://vcenter.htulab.cisco.com Hypervisor 6.7.0-12473784 Total Capacity 13.39 TB Uptime 5 days, 22 hours, 7 minutes, 38 seconds HXOP Version 4.0.1b-33133 Available Capacity 13.25 TB Data Replication Factor 3	Actions ~ DNS Server(s) 10.29.133.110 NTP ntp2.hclab.ciso.com.r/p1.hcla Server(s) bclsco.com Controller Access over SSH Enabled
ANALYZE In Performance PROTECT Protect	hxaf220m5n-01 HXAF220C-M5SN 7 Disks (1 Caching, 6 Persistent) Online O HXDP Version 4.0(1b) Type Hyper Converged	
MANAGE	Hypervisor Status Online Hypervisor Address 10.29.133.174	
System Information Datastores Virtual Machines T Upgrade	hxaf220m5n-02 HXAF220C-M55N 7 Disks (1 Caching, 6 Persistent) Online O HDOP Version 4.0(1b) Type Hyper Converged	
>_ Web CLI	Hypervisor Status Online Hypervisor Address 10.29.133.175 hxaf220m5n-03 HXAF220C-M5SN 7 Disks (1 Caching, 6 Persistent) Online HODP Version 4.0(1b)	
	Hypervisor Status Online Hypervisor Address 10.29.133.176	

Validation

This section provides a list of items that should be reviewed after the HyperFlex system has been deployed and configured. The goal of this section is to verify the configuration and functionality of the solution and ensure that the configuration supports core availability requirements.

Post Install Checklist

The following tests are critical to functionality of the solution, and should be verified before deploying for production:

- 1. Verify the expected number of converged storage nodes and compute-only nodes are members of the HyperFlex cluster in the vSphere Web Client plugin manage cluster screen.
- 2. Verify the expected cluster capacity is seen in the HX Connect Dashboard summary screen.
- Create a test virtual machine that accesses the HyperFlex datastore and is able to perform read/write operations.
- 4. Perform a virtual machine migration (vMotion) of the test virtual machine to a different host on the cluster.
- 5. During the vMotion of the virtual machine, make sure the test virtual machine can perform a continuous ping to its default gateway and to check if the network connectivity is maintained during and after the migration.

Verify Redundancy

The following redundancy checks can be performed to verify the robustness of the system. Network traffic, such as a continuous ping from VM to VM, or from vCenter to the ESXi hosts should not show significant failures (one or two ping drops might be observed at times). Also, all of the HyperFlex datastores must remain mounted and accessible from all the hosts at all times.

- 1. Administratively disable one of the server ports on Fabric Interconnect A which is connected to one of the HyperFlex converged storage hosts. The ESXi virtual switch uplinks for fabric A should now show as failed, and the standby uplinks on fabric B will be in use for the management and vMotion virtual switches. Upon administratively re-enabling the port, the uplinks in use should return to normal.
- 2. Administratively disable one of the server ports on Fabric Interconnect B which is connected to one of the HyperFlex converged storage hosts. The ESXi virtual switch uplinks for fabric B should now show as failed, and the standby uplinks on fabric A will be in use for the storage virtual switch. Upon administratively re-enabling the port, the uplinks in use should return to normal.
- 3. Place a representative load of guest virtual machines on the system. Put one of the ESXi hosts in maintenance mode, using the HyperFlex HX maintenance mode option. All the VMs running on that host should be migrated via vMotion to other active hosts through vSphere DRS, except for the storage platform controller VM, which will be powered off. No guest VMs should lose any network or storage accessibility during or after the migration. This test assumes that enough RAM is available on the remaining ESXi hosts to accommodate VMs from the host put in maintenance mode. The HyperFlex cluster will show in an unhealthy state in the HX Connect Dashboard.
- 4. Reboot the host that is in maintenance mode and exit it from maintenance mode after the reboot. The storage platform controller will automatically start when the host exits maintenance mode. The HyperFlex cluster

will show as healthy in the HX Connect Dashboard after a brief time to restart the services on that node. vSphere DRS should rebalance the VM distribution across the cluster over time.



Many vCenter alerts automatically clear when the fault has been resolved. Once the cluster health is verified, some alerts may need to be manually cleared.

5. Reboot one of the two Cisco UCS Fabric Interconnects while traffic is being sent and received on the storage datastores and the network. The reboot should not affect the proper operation of storage access and network traffic generated by the VMs. Numerous faults and errors will be noted in Cisco UCS Manager, but all will be cleared after the FI comes back online.

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 8.

Table 8.	Test Infrastructure	Virtual Machine	Configuration
----------	----------------------------	------------------------	---------------

Configuration	Citrix Virtual Desktops Controllers Virtual Machines	Citrix Provisioning Services Servers Virtual Machines
Operating System	Microsoft Windows Server 2019	Microsoft Windows Server 2019
Virtual CPU amount	6	8
Memory amount	8 GB	12 GB
Network	VMNIC	Network
Disk-1 (OS) size and location	40 GB	Disk-1 (OS) size and location
Disk-2 size and location	500GB	Disk-2 (Data) Paravirtual SCSI adapter with ReFS format
Configuration	Microsoft Active Directory DC's Virtual Machines	Citrix Profile Servers Virtual Machines
Operating system	Microsoft Windows Server 2019	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 2019	Microsoft Windows Server 2019
Virtual CPU amount	8	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 2019	NS11.1 52.13.nc
Virtual CPU amount	4	2
Memory amount	4 GB	2 GB
Network	VMNIC	Network
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. virtual machines 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 virtual machines 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 virtual machines were configured as listed in Table 9.

Table 9.	HVD	and HSD	Configurations
----------	-----	---------	----------------

Configuration	HVDI Virtual Machines	HSD Virtual Machines
Operating system	Microsoft Windows 10 64-bit	Microsoft Windows Server 2019
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
Citrix PVS write cache	6 GB	24 GB
Disk size		
Additional software used for	Microsoft Office 2016	Microsoft Office 2016

Configuration	HVDI Virtual Machines	HSD Virtual Machines
testing	Login VSI 4.1.32 (Knowledge Worker Workload)	Login VSI 4.1.32 (Knowledge Worker Workload)

Install and Configure Citrix Desktop Delivery Controller, Citrix Licensing, and StoreFront

This section details the installation of the core components of the Citrix Virtual Apps and Desktops 1912 LTSR system. This CVD provides the process to install two Desktop Delivery Controllers to support hosted shared desktops (HSD), non-persistent virtual desktops (VDI), and persistent virtual desktops (VDI).

The process of installing the Desktop Delivery Controller also installs other key Citrix Desktop 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, follow these steps:

- 1. To begin the installation, connect to the first Citrix License server and launch the installer from the Citrix Virtual Apps and Desktops 1912 LTSR ISO.
- 2. Click Start.

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

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

Get Started		Prepare Machines	s and	Images		
Delivery Controller		Virtual Delivery Agent for Windows Multi-session OS				
Start here. Select and install th essential services like License 5	e Delivery Cont Server and Store	roller and other Front.	Install this agent multi-session OS	: to de 5 virtu	eliver applications and desktops from Wi al machines or physical machines.	indows
Extend Deployment						
Extend Deployment Citrix Director	•	Citrix Studio		•	Self-Service Password Reset	0
Extend Deployment Citrix Director Citrix License Server	•	Citrix Studio Universal Print Serve	er	•	Self-Service Password Reset	0

- 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.

	Software License Agreement
Licensing Agreement	Printable vers
Core Components	Last Revised: March 1, 2018
Firewall	CITRIX LICENSE AGREEMENT
Summary Install Smart Tools Finish	 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"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. 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 AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TREMS 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. Citrix hereby grants Customer a non-exclusive worldwide license to use the software in a software PRODUCT and the software installed in an appliance PRODUCT under the license models identified at https://www.citrix.com/buy/licensing/product.html. Any experimental features
	 I have read, understand, and accept the terms of the license agreement I do not accept the terms of the license agreement

7. Click Next.

	Core Components		
Licensing Agreement	_		
Core Components		Location: C:\Program Files\Citrix	Change
Firewall	License Server (Required)		
Summary	Manages product licenses.		
Install			
Finish			
		De als	6.1

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

	Firewall	
 Licensing Agreement 	The default ports are listed below.	Printable versio
Core Components	Lizzana Saman	
Firewall	License server	
Summary	7279 TCP	
Install	27000 TCP	
Finish	8083 TCP	
	Configure firewall rules: • Automatically Select this option to automatically create the rules in be created even if the Windows Firewall is turned off Manually Select this option if you are not using Windows Firewall	the Windows Firewall. The rules will

10. Click Install.

	Junitary
 Licensing Agreement Core Components Firewall Summary Install Finish 	Review the prerequisites and confirm the components you want to install. Installation directory CAProgram Files\Citrix Core Components License Server Delivery Controllers Not specified Firewall
	Until you specify the location of the Delivery Controller, the Virtual Delivery Agent cannot register with it and users cannot access their applications and desktops. Back Finish Cancel

11. Click Finish to complete the installation.

	Summary
Licensing Agreement Core Components Firewall Summary Install Finish	Review the prerequisites and confirm the components you want to install. Installation directory C:\Program Files\Citrix Core Components License Server Firewall TCP Ports: 7279, 27000, 8083, 8082

Install Citrix Licenses

To install the Citrix Licenses, follow these steps:

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

📕 🗋 🗐 = I		MyFiles		-	×
File Home	Share View				~ O
€ 🗇 🔹 ↑	🍶 « Program Files (x86) 🕨 Citrix 🕨 Lice	ensing 🕨 MyFiles	V C	Search MyFiles	P
▷ 🚖 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	
Þ 🗣 Network	LicenseXD1000_071315_18mo_e.lic	10/10/2016 4:29 PM	LIC File	16 KB	
3 items					

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



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



Install Citrix Desktop Broker/Studio

To install Citrix Desktop, follow these steps:

- 1. Connect to the first Citrix VDI server and launch the installer from the Citrix Desktop 1912 LTSR 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:	
Virtual Apps Deliver applications	Start
Virtual Apps and Desktops 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 Machines an	d Images	
Delivery Controller			Virtual Delivery A	gent for Windows Multi-session OS	
Start here. Select and install th essential services like License !	e Delivery Contu Server and Store	roller and other Front.	Install this agent to multi-session OS vir	deliver applications and desktops from W tual machines or physical machines.	Vindows
Extend Deployment					
Extend Deployment Citrix Director	•	Citrix Studio	•	Self-Service Password Reset 🖡	•
Extend Deployment Citrix Director Citrix License Server	6	Citrix Studio Universal Print Serve	() er ()	Self-Service Password Reset k	6

- 4. Read the Citrix License Agreement and 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.

	Software License Agreement
Licensing Agreement	Printable ve
Core Components Features Firewall Summary Install Diagnostics Finish	Last Revised: January 1, 2019 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"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your View Citrix com buy/licensing/citrix-providing-entities tham. BY INSTALLING AND/OR USE There PRODUCT, You AGREE TO BE BOUND BY 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 LICENSE . 1. Bed User Licenses. Citrix hereby grants Customer a non-exclusive worldwide license to use the software in a software PRODUCT and the software installed in an appliance PRODUCT moder the license models identified at https://www.citrix.com/buy/licensing/product.html 1. How read, understand, and accept the terms of the license agreement 1. Ido not accept the terms of the license agreement

- 6. Select the components to be installed on the first Delivery Controller Server:
 - a. Delivery Controller
 - b. Studio
 - c. Director
- 7. Click Next.

	core components
Licensing Agreement	
Core Components	Location: C:\Program Files\Citrix Change
Features	Component (Select all)
Firewall Summary Install	Delivery Controller Distributes applications and desktops, manages user access, and optimizes connections.
Diagnostics Finish	Studio Create, configure, and manage infrastructure components, applications, and desktops
	Director Monitor performance and troubleshoot problems.
	□ License Server ▲ This component must be installed at least once.
	 StoreFront This component must be installed at least once.



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

- 8. Since a SQL Server will be used to Store the Database, leave "Install Microsoft SQL Server 2012 SP1 Express" unchecked.
- 9. Click Next.
| 415 A. | |
|----------------------|--|
| Licensing Agreement | Feature (Select all) |
| Features
Firewall | Install Microsoft SQL Server 2017 Express CU16
This is an optional component. If you have an existing SQL Server for storing desktop
and application configurations and settings, do not select this option. |
| Summary
Install | Install Windows Remote Assistance
Select this only if you need the shadowing feature of Director Server. |
| Diagnostics | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

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

	Firewall		
 Licensing Agreement 	The default ports are listed below		Printable versio
 ✓ Core Components ✓ Features 	Delivery Controller	Director	
Firewall Summary Install Diagnostics Finish	80 TCP 89 TCP 443 TCP	80 TCP 443 TCP	
	Configure firewall rules: Automatically Select this option to automatica created even if the Windows Fir Manually Select this option if you are not yourself.	ally create the rules in the Windows Fi rewall is turned off. : using Windows Firewall or if you war	rewall. The rules will be it to create the rules

12. Click Install.

Licensing Agreement Core Components Features	Review the prerequisites and confirm the components you want to install.	
 Firewall Summary Install Diagnostics Finish 	CAProgram Files\Citrix Prerequisites Microsoft Visual x64 C++ 2017 Runtime Local Host Cache Storage (LocalDB) Microsoft Visual x86 C++ 2017 Runtime Microsoft Visual x86 C++ 2017 Runtime Microsoft SQL CLR Types (x86) Microsoft SQL CLR Types (x86) Microsoft SQL CLR Types (x64) Microsoft SQL CLR Types (x64) Microsoft SMO Objects (x64) Microsoft SMO Objects (x64) Microsoft Internet Information Services Core Components Delivery Controller Studio Director M Until you specify the location of the Delivery Controller, the Virtual Delivery Agent can	not

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

	Diagnostics
 Licensing Agreement Core Components Features Firewall Summary Install Diagnostics Finish 	Collect diagnostic information Citrix Call Home periodically collects information about system and product configuration performance, errors, and more. The information is transmitted to Citrix so our support and product teams can resolve issues proactively. Lean more about Call Home. MTE: The feature can be disabled later. Connect *Requires Citrix Cloud login

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

	Finish Installation	
Licensing Agreement	The installation completed successfully.	✓ Succes
Core Components		
✓ Features	Prerequisites	Installed
/ Firewall	 Microsoft Visual X04 C++ 2017 Kuntime Local Host Cache Storage (LocalDB) 	Installed
	 Microsoft Visual x86 C++ 2017 Runtime 	Installed
Summary	Microsoft SQL CLR Types (x86)	Installed
🖊 İnstall	 Microsoft SMO Objects (x86) 	Installed
Diagnostics	 Microsoft SQL CLR Types (x64) 	Installed
Einich	Microsoft SMO Objects (x64)	Installed
rillisu	 Microsoft Internet Information Services 	Installed
	Core Components	
	 Delivery Controller 	Installed
	🖌 Studio	Installed
	✓ Director	Installed
	Post Install	
	 Component Initialization 	Initialized
	Launch Studio	

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

To configure Citrix VDI, follow these steps:

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

Citrix Studio	-ten us	Actions	
	citrix	Citrix Studio	
	Welcome	View	•
	1117 Ab. 4	Refresh	
	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. Select the "A fully configured, production-ready Site" radio button.
- 3. Enter a site name.
- 4. Click Next.

te Setup	
Studio	Introduction
Introduction Databases Licensing Connection Network Additional Features Summary	You have two options when creating a new Site. The simplest option is to automatically create an empty Site, which you must configure yourself. What kind of Site do you want to create? A fully configured, production-ready Site (recommended for new users) A nempty, unconfigured Site Site name: 1912-LTSC
	Back Next Cancel

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

Studio	Databases		
	Databases store Choose how you	information about Site setup, co u want to set up the databases. L	nfiguration logging and monitoring. earn more
 Introduction Databases Licensing 	Create and set up databases from Studio (You can provide details of existing empty databases) Generate scripts to manually set up databases on the database server		
Connection	Provide databas	e details	
Network Additional Features Summary	Data type Site:	Database name Citrix1912-LTSCSite	Location (formats)
	Monitoring:	Citrix1912-LTSCMonitoring	SQL01
	Logging:	Citrix1912-LTSCLogging	SQL01
	1 For an Alw	aysOn Availability Group, specify	the group's listener in the location.
	Specify addition 1 selected	al Delivery Controllers for this Sit	te Learn more Select

- 6. For an AlwaysOn Availability Group, use the group's listener DNS name.
- 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 license radio button.
- 10. Click Next.

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

- 11. Select the Connection type of 'Microsoft System Center Virtual Machine Manager'.
- 12. Enter the Connection Address to the SCVMM Server.
- 13. Enter the username (in username@domain format) for the vCenter account.
- 14. Provide the password for the Domain Admin account.
- 15. Provide a connection name.
- 16. Select the Studio tools radio button.

Connection and Resources		
Studio	Connection	n
	8x16	φ.]
Connection Storage Management	Create a new Connection	
Storage Selection Network	Connection address:	VMware vSphere® * Example: https://vmware.example.com/sdk
Summary	User name:	Learn about user permissions Example: domain\username
	Password:	
	Connection name:	Example: MyConnection
	Create virtual machines Studio tools (Mar Select this option Other tools	using: hine Creation Services) when using AppDisks, even if you are using Citrix Provisionii
		Back Next Ca

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	Storage Management	
	Configure virtual machine storage resources for	this connection.
Connection	Select a cluster: 8x16-ESX	Browse
Storage Management	Select an optimization method for available site	e storage.
Network	Use storage shared by hypervisors	to ta a a a
Summary	Optimize temporary data on available local storage	
	Use storage local to the hypervisor	111
	Manage personal data centrally on shared storage	

- 21. Make Storage selection to be used by this connection.
- 22. Click Next.

Studio	Storage Selection				
	When using shared sto device; machine operat	ting syste	must select the m data, persona	type of data to store on o l user data, and if not store the selected for each dat	each shared storage ring temporary data a type
Connection	Select data storage loc	ations:			- Jk-
Storage Management	Name	+	OS	Personal vDisk	Temporary
Storage Selection	esxtop				
Network	vdi_workload		~	 Image: A set of the /li>	
Summary	vdi-workload-2				

- 23. Make Network selection to be used by this connection.
- 24. Click Next.

Studio	Network	
Connection	Name for these resources: two-to-one The resources name helps identify this storage and network combination	in Studio.
Storage Selection Network Summary	Select one of more networks for the virtual machines to use: Name Storage Controller Data Network Storage Controller Ranagement Network Storage Controller Replication Network vm-34 vm-network-34	*

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

Studio	Addit Use th	tional Features ne following features to customize your Site. You can also enable/disable and configure
Introduction	featur	es later.
 Databases Licensing 		AppDNA Enable this feature to allow analysis of applications and operating systems, review compatibility issues, and take remedial actions to resolve them.
 Connection Storage Management Storage Selection 		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.
Network Additional Features		
Summary		

27. Review Site configuration Summary and click Finish.

Configure the Citrix VDI Site Administrators

To configure the Citrix VDI site administrators, follow these steps:

- 1. Connect to the Citrix VDI 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:	
Kole Summary	Scopes are objects that represent someth administrator is allowed to manage (for e team). Click a scope to see the objects in	hing meaningful in an organization and that an example, a set of Delivery Groups used by the Finance it.
	Scope name	
_	All All	
_	All objects	
_		
_		
_		
_		
_		
_		

4. Choose an appropriate Role.

Studio	Role		
	Select	a role. Click a role name to view its permissions.	
Administrator and Scope		Name \$	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
	0	Machine Catalog Administrator Can create and manage Machine Catalogs and provision machines.	Built In
	0	Read Only Administrator Can see all objects in specified scopes as well as global information, b	Built In
	Crea	te role	

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

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

Configure Additional Desktop Controller

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



To configure additional Citrix Desktop controllers, follow these steps:

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

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

3. Click Delivery Controller.

Get Started			Prepare Machines and Images		
Delivery Controller			Virtual Delivery Agent for Windows Multi-session OS		
Start here. Select and install the Delivery Controller and ot essential services like License Server and StoreFront.		roller and other Front.	Install this agent to d multi-session OS virti	eliver applications and desktops from Wi Jal machines or physical machines.	ndow
Extend Deployment					
Extend Deployment Citrix Director		Citrix Studio	•	Self-Service Password Reset	•
Extend Deployment Citrix Director Citrix License Server	•	Citrix Studio Universal Print Server	•	Self-Service Password Reset 🖡	

- 4. Repeat these 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.

	Summary	
 Licensing Agreement 	Review the prerequisites and confirm the components you want to install.	
 Core Components Features Firewall Summary Install Diagnostics Finish 	Installation directory C\Program Files\Citrix Prerequisites Microsoft Visual x64 C++ 2017 Runtime Local Host Cache Storage (LocalDB) Microsoft Visual x86 C++ 2017 Runtime Microsoft SQL CLR Types (x86) Microsoft SQL CLR Types (x86) Microsoft SQL CLR Types (x64) Microsoft SQL CLR Types (x64) Microsoft SQL CLR Types (x64) Microsoft SQL Objects (x64) Microsoft Internet Information Services Core Components Delivery Controller Studio Director	
	Until you specify the location of the Delivery Controller, the Virtual Delivery Agent can register with it and users cannot access their applications and desktops.	iot

- 7. (Optional) Click "Collect diagnostic information."
- 8. Click Next.



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

Licensing Agreement The installation completed successfully. Successfully. Core Components Prerequisites Microsoft Visual x64 C++ 2017 Runtime Installed Firewall Summary Installed Microsoft Visual x66 C++ 2017 Runtime Installed Diagnostics Microsoft SMO Objects (x86) Installed Microsoft SUL CLR Types (x64) Installed Microsoft SMO Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Objects (x64) Microsoft SMO Objects (x64)		Finish Installation	
Prerequisites	 Licensing Agreement 	The installation completed successfully.	✓ Succes
* Features • Microsoft Visual x64 C++ 2017 Runtime Installed • Firewall • Local Host Cache Storage (LocalDB) Installed • Summary • Microsoft Visual x86 C++ 2017 Runtime Installed • Microsoft SQL CLR Types (x86) Installed • Diagnostics • Microsoft SMO Objects (x64) Installed • Delivery Controller Installed • Director Installed • Director Installed • Component Initialization Initialized	 Core Components 	Prerequicites	
* Firewall Local Host Cache Storage (LocalDB) Installed Microsoft Visual x86 C++ 2017 Runtime Installed Microsoft SQL CLR Types (x86) Installed Microsoft SQL CLR Types (x86) Installed Microsoft SQL CLR Types (x64) Installed Microsoft SMO Objects (x64) Installed Finish Core Components Delivery Controller Installed Director Installed Post Install Component Initialization Initialized 	✓ Features	Microsoft Visual x64 C++ 2017 Runtime	Installed
Summary Microsoft Visual x86 C++ 2017 Runtime Install Microsoft SQL CLR Types (x86) Installed Microsoft SQL CLR Types (x86) Installed Microsoft SQL CLR Types (x64) Installed Microsoft SMO Objects (x64) Installed Microsoft Internet Information Services Installed Objector Installed Delivery Controller Delivery Controller Installed Director Installed Post Install Component Initialization Initialized Microsoft Internet Information Services Installed Delivery Controller Installed Director Installed Director Installed Microsoft Initialization Initialized Microsoft Initialization Microsoft Initialized Microsoft Initialization Microsoft Initialized Microsoft Initialization Microsoft Initialized Microsoft	✓ Firewall	Local Host Cache Storage (LocalDB)	Installed
Microsoft SQL CLR Types (x86) Installed Microsoft SMO Objects (x86) Installed Microsoft SMO Objects (x86) Installed Microsoft SMO Objects (x64) Installed Microsoft SMO Objects (x64) Installed Microsoft Internet Information Services Installed Ore Components Delivery Controller Installed Director Installed Post Install Component Initialization Initialized	Summany	Microsoft Visual x86 C++ 2017 Runtime	Installed
Install Microsoft SMO Objects (x86) Installed Diagnostics Microsoft SQL CLR Types (x64) Installed Finish Microsoft SMO Objects (x64) Installed Core Components Installed Studio Installed Director Installed Post Install Component Initialization Component Initialization Initialized	+ Summary	 Microsoft SQL CLR Types (x86) 	Installed
• Diagnostics • Microsoft SQL CLR Types (x64) Installed • Microsoft SMO Objects (x64) Installed • Microsoft Internet Information Services Installed • Delivery Controller Installed • Director Installed • Director Installed • Component Initialization Initialized	🖌 İnstall	 Microsoft SMO Objects (x86) 	Installed
Finish Microsoft SMO Objects (x64) Microsoft SMO Objects (x64) Microsoft Internet Information Services Installed Core Components Delivery Controller Installed Studio Director Installed Post Install Component Initialization Initialized <li< td=""><td>✓ Diagnostics</td><td> Microsoft SQL CLR Types (x64) </td><td>Installed</td></li<>	✓ Diagnostics	 Microsoft SQL CLR Types (x64) 	Installed
Microsoft Internet Information Services Installed Core Components Delivery Controller Installed Studio Director Installed Post Install Component Initialization Initialized	Finish	 Microsoft SMO Objects (x64) 	Installed
Delivery Controller Installed Studio Installed Director Installed Post Install Component Initialization Initialized		Microsoft Internet Information Services Core Components	Installed
 Studio Director Post Install Component Initialization Initialized 		V Delivery Controller	Installed
Director Installed Post Install Component Initialization Initialized		🖌 Studio	Installed
Post Install Component Initialization Initialized		V Director	Installed
Component Initialization Initialized		Post Install	
		Component Initialization	Initialized
🗹 Launch Studio		🗹 Launch Studio	

Add the Second Delivery Controller to the Citrix Desktop Site

To add the second Delivery Controller to the Citrix Desktop Site, follow these steps:

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

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.

Specify the address of a Delivery Controller	in the Site you wish
DIN	
xdc06.hxhvdom.local	
xample: deliverycontroller.example.com	

- 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.

Jerich Sterifiert Here 4 Lat Updated Registered Registered Registered Registered 1334 Applications Applications O minutes ago 1334 Administration O minutes ago 1331 Administration O minutes ago 1331 Administration O minutes ago 1331	Varting Machine Catalogy Machine Catalogy Machine Catalogy Machine Catalogy Definery Groups Applications Pathodom.local Policies Policies Policies Configuration Configuration	Last Updated O minutes ago O minutes ago	Registered Desktops 1354 1286 1351
AppCus Introdem local Ormades ago 1334 ApsCrations ApsCrations Ormades ago 1286 Mondom local Ormades ago 1331 ApsCrations Administrators Administrators Introdem local Ormades ago 1331 ApsCrations Administrators Administrators Administrators Introdem local Ormades ago 1331 According and appCration Administrators Administrators Administrators Introdem local 0 1331 According and appCration Administrators Administrators Introdem local 0 1331 AppCration Administrators Administrators Introdem local 0 1331 AppCration Administrators Administrators Introdem local 0 1331 AppCration Administrators Administrators Introdem local 0 1331 AppCration Administrators Introdem local 0 1331 1331 AppCration Administrators Introdem local 0 1331 1331 AppCration Introdem local	AppDias Introdem local Delivey Groups Introdem local Applicitions /nutrodem local Policies /nutrodem local Policies /nutrodem local Policies /nutrodem local Configuration Configuration	0 minutes ago 0 minutes ago 0 minutes ago	1354 1286 1351
Debrey troups Inhudom.local Ormote ago 1286 Policie Policie Ormote ago 1331 Configuration A chaininatarcs A chaininatarcs Inhudom.local Ormote ago 1331 Configuration A poly Policia A poly Policia A poly Policia Inhudom.local Ormote ago 1331	a) Delivery Groups hahvdom.local À Applications huhvdom.local ∰ Policies huhvdom.local ∰ Loging © Configuration	0 minutes ago 0 minutes ago	1286
Privation Administrators Administrators Administrators ApplVA ApplVA ApplVA I ApplVA	Policie Policie Configuration Configuration	0 minutes ago	1351
Centrological Administrators Centrological App-VP-Molifoli App-VP-Molifoli App-VP-Molifoli Centra StoreFront	Configuration		
Controllers Controllers A Licensing Soverient A App-V Publicit H AppUNA Cons T Cons Soverient	Configuration		
Controllers Hoting StoreFont AppNA AppNA Craix StoreFont	1. Administration I		
Hoting StoreFront App: VPublici App: VPublici Crist StoreFront Crist StoreFront	Controllers		
Licensing SoveFoot App VP Multini App VP App NA Zones Texts StoreFoot	🗮 Hosting		
ApplNA ApplNA ApplNA Craix SoreFront	A Licensing		
T AppRMA T AppRMA T Cerex StoreFront	App-V Publishi		
> Chris StoreFront	AppDNA		
	Chini ShareFrank		
	China Surerium		

Install and Configure StoreFront

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

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

To install and configure StoreFront, follow these steps:

- 1. To begin the installation of the StoreFront, connect to the first StoreFront server and launch the installer from the Citrix Desktop 1912 LTSR 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:	3.
Virtual Apps Deliver applications	tart
Virtual Apps and Desktops Deliver applications and desktops	tort
a	incel
CITRIX	

3. Click Extend Deployment Citrix StoreFront.

Get Started			Prepare Machin	nes and	Images	
Delivery Controller			Virtual Delive	ery Ag	ent for Windows Multi-session OS	
Start here. Select and install th essential services like License S	e Delivery Cont ierver and Store	troller and other eFront.	Install this age multi-session (nt to d OS virti	eliver applications and desktops from Win Jai machines or physical machines.	idow
Extend Deployment						
Extend Deployment Citrix Director	•	Citrix Studio		•	Self-Service Password Reset 📐	.a
Extend Deployment Citrix Director Citrix License Server	•	Citrix Studio Universal Print Ser	ver	•	Self-Service Password Reset A	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.

	Software License Agreement
Licensing Agreement Core Components	Printable ver
Features Firewall Summary Install Diagnostics Finish	CITRIX LICENSE AGREEMENT 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"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. 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 AGREE 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. Citrix hereby grants Customer a non-exclusive worldwide license to use the software in a software PRODUCT and the software installed in an appliance PRODUCT under the license models identified at https://www.citrix.com/buy/licensing/product.html. Unless otherwise noted, each I have read, understand, and accept the terms of the license agreement I do not accept the terms of the license agreement Back Mext Cance

6. Select Storefront and click Next.

	Summary
 Licensing Agreement 	Review the prerequisites and confirm the components you want to install.
 ✓ Core Components ✓ Firewall Summary Install Diagnostics Finish 	Installation directory C:\Program Files\Citrix Core Components StoreFront Delivery Controllers Not specified Firewall
	Until you specify the location of the Delivery Controller, the Virtual Delivery Agent cannot register with it and users cannot access their applications and desktops.

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

- 9. Click Install.
- 10. (Optional) Click Collect diagnostic information.
- 11. Click Next.

	Diagnostics
 Licensing Agreement Core Components Features Firewall Summary Install Diagnostics Finish 	Collect diagnostic information Crivic Call Home periodically collects information about system and product configuration performance, errors, and more. The information is transmitted to Citrix so our support and product teams can resolve issues proactively. Lem more about Call Home. MoTE: The feature can be disabled later. Connect Prepared Citrix Cloud login

12. Click Finish.

	Finish Installation	
 Licensing Agreement Core Components Firewall Summary Install Diagnostics Finish 	The installation completed successfully. Core Components * StoreFront Post Install * Component Initialization	✓ Succes Installed Initialized
	Open the StoreFront Management Console	

13. Click Create a new deployment.

🗱 Citrix StoreFront		Actions	
	cirkix	Citrix StoreFront	1 A
		View	
	Welcome to StoreFront	G Refresh	
	Select an option below to create a new store or extend your existing deployment	Help	
	Create a new deployment Set up a deployment to deliver self-service applications, data, and desktops to your users.		
	Join existing server group Add a server to an existing load-balanced group.		

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

For a multiple server deployment use the load balancing environment in the Base URL box.

Confirm the specify the l	base URL for services hosted on th load-balanced URL for the server gr	is deployment. For multiple server dep oup.	ployments,
Base URL:	http://storefront/		A
	Base URL:	lase URL: http://storefront/	lase URL: http://storefront/

15. Click Next.

StoreFront Base URL Getting Started Store Name Delivery Controllers Remote Access Authentication Methods XenApp Services URL Summary	Getting Started StoreFront stores provide your users with access to their Windows desktops and applications, applications, external software-as-a-service (SaaS) applications, and internal web applications through a single portal from all their devices. Store URL Receiver Receiver for Web Site Store KenApp Services URL KenApp Services URL NAgent

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

StoreFront	Store name and access
StoreFront	Enter a name that helps users identify the store. The store name appears in Citrix Receiver as part of
✓ Base URL	the user's account.
✓ 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
XenApp Services URL	Unauthenticated users can access the store without presenting credentials.
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.

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

toreFront	Delivery Controllers		
	Specify the Citrix Virtua Citrix recommends gro	al Apps and Desktops delivery controllers or Xi uping delivery controllers based on deployme	enApp servers for this store. nts.
Getting Started	Name	Type	Servers
Store Name	Controller	Citrix Virtual Apps and Desktops	10.10.30.230
Johning	Add Edit	Remove	
	Photos: Los		

18. 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 nee to add a NetScaler Gateway once remote access is enabled.
Base URL	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 tunne) Users may require the NetScaler Gateway Plug-in to establish a full VPN tunnel.
Summary	NetScaler Gateway appliances:
	Add
	Default appliance:

19. 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 as shown below:

StoreFront		
	Select the methods which users will use to authenticate and access resources.	0
Base URL	Method	
Getting Started	Ser name and password	_
d Store Name	SAML Authentication	
v store wante	Domain pass-through	
 Delivery Controllers 	Can be enabled / disabled separately on Receiver for Web sites	
Remote Access	Smart card Can be enabled / disabled separately on Receiver for Web sites	
Authentication Methods	HTTP Basic	- 1
XenApp Services URL	Pass-through from NetScaler Gateway	
summary		

- 20. Username and password: Users enter their credentials and are authenticated when they access their stores.
- 21. 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.
- 22. Configure the XenApp Service URL for users who use PNAgent to access the applications and desktops and click Create.

	Canfleure Van Ann Camilan (10)
StoreFront	Configure XenApp Services OKL
	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	Make this the default Store for PNAgent
Beinvery Controllers Remote Access	PNAgent will use this store to deliver resources.
Authentication Methods	
XenApp Services URL	
Summary	

23. After creating the store click Finish.



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, follow these steps:

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

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

3. Click Extended Deployment Citrix StoreFront.

Get Started			Prepare Machines and Images			
Delivery Controller			Virtual Delivery Agent for Windows Multi-session OS			
Start here. Select and install the essential services like License S	Delivery Cont	trolier and other ef ront.	Install this age multi-session (nt to d OS virti	leliver applications and desktops from Wir ual machines or physical machines.	ndow
Extend Deployment	1					
Extend Deployment Citrix Director	•	Citrix Studio		0	Self-Service Password Reset	•
Extend Deployment Citrix Director Citrix License Server	•	Citrix Studio Universal Print St	nver	•	Self-Service Password Reset	•

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

6. Click Install.

	Core Components
Licensing Agreement	
Core Components Firewall Summary Install	StoreFront (Required) Provides authentication and resource delivery services for Citrix Workspace app, enabling you to create centralized enterprise stores to deliver applications, desktops and other resources to users on any device, anywhere.
Diagnostics	

- 7. (Optional) Click Collect diagnostic information.
- 8. Click Next.

	Diagnostics
 Licensing Agreement Core Components Features Firewall Summary Install Diagnostics Finish 	Collect diagnostic information Citrix Call Home periodically collects information about system and product configuration, product teams can resolve issues proactively. Learn more about Call Home. More: The feature can be disabled later. Connect *Requires Citrix Cloud login

9. Check the box for Open the StoreFront Management Console.

10. Click Finish.

	Finish Installation	
 Licensing Agreement 	The installation completed successfully.	✓ Succes
 ✓ Core Components ✓ Firewall ✓ Summary ✓ Install ✓ Diagnostics Finish 	Core Components StoreFront Post Install Component Initialization	Installed

To configure the second StoreFront if used, follow these steps:

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



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

To authorize this serv	/er, first conn	ect to a serv	er in the gro	up and choo	se "Add
Server". Enter the pro	ovided autho	rization infor	mation here		
		-			
Authorizing server:	CIX-VDI				
Authorization code:					
					3
					Ь

- 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.

	CITRIX	Actions
Christ Storeront	CİTRİX Server Group Group details Base URL: http:///////////////////////////////////	Actions Server Group Add Server Change Base URL View Refresh Help

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: HX Authorization code: 80587665	
Please wait	
	\}
	Cancel

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

10. Click Join.

To authorize this serv	er, first connect to a serv	er in the group and	choose "Add
Server". Enter the pro	vided authorization info	rmation here.	
Authorizing server:	CTX-VDI		
	00507665		=
Authorization code:	80387005		

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

Join Serve	r Group	
0	Joined Successfully "-02" is now part of a multiple server deployment.	
		ОК

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 2019 RDS 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, follow these 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 ISO.
- 2. Click Target Device Installation.

Server Installation Target Device Installation Help and Support Browse DVD		Console Installation	
Help and Support		Server Installation	
Rowse DVD Strit	•	Help and Support	
		Browse DVD	Exit

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

3. Click Next.

citDIX.	Welcome to the Installation Wizard for Citrix
CIIRIN	The InstallShield(R) Wizard will install the Citrix Provisioning Services Target Device on your computer. It is recommended that you disable any AntiVirus software before continuing. To continue, dirk Next.
	WARNING: This program is protected by copyright law and international treaties.

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



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, follow these steps:



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


- 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.

	ning Services Site	
Enter the Provisioning Only stores supported	Services site server name or IP, port, and credentials. 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 Credent	tials for the Server	
Use my Windo	ws credentials	
OUse these crea	dentials	
User name:		
Domain:		
Domain: Password:		
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.

Provisioning Services	s Imaging Wizard	
Add Target Device		
This device is not a me	mber of the site and needs to be added.	
Target device name:	Win 10-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 se	rver.
Collection name:	Collection	~
	Select the site collection that this device will be added to.	
	< Back N	lext > Cancel

- 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 list. (This CVD used Dynamic rather than Fixed vDisks.)

13. Click Next.

11	Provisioning Service	s Imaging Wizard	×
	New vDisk The new vDisk will be	created in the store you select.	
	vDisk name:	Win10-vDisk	
	Store name:	Store - 949.67 GB Free Supported by Server: CTX-PVS1	
	vDisk type:	Dynamic (recommended)	
		< Back Next > Cancel	

- 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)	
Multiple Activation Key (MAK)	
< Back Next >	Cancel

16. Select Image entire boot disk on the Configure Image Volumes page.

2 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			
	<u>y</u>	77. NY	520
	< 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.

22 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?	
O Do not optimize the hard disk again	
Optimize the hard disk again for Provisioning Services before imaging	
Edit Optimization Settings	
Note: Citrix recommends that partitions be defragmented before imaging.	
< Back Next >	Cancel

20. Select Create on the Summary page.

Provisionin	j services imaging wizard		
Summary			
Confirm that	t all settings are correct.		
Connect to Task: Crea	Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 te a vDisk	^	ľ
Target dev Network co	ice name : Win10-TD nnection : Ethernet0, 10.10.208.100, 00-50-56-AE-53-7B		
Collection: vDisk name	Collection :: Win 10-vDisk		
Store: Stor Format: VH	e IDX, type: Dynamic (recommended), sector size: 512 B, block size: 32 MB		
Image enti Optimize ha	re boot disk ard disk for Provisioning Services prior to imaging		
op and a start			
		\checkmark	
<		>	I.
Status:	Ready to Start]
Progress:			ĺ
Progress:		8	
Progress:		_	

21. Review the configuration and click Continue.

🗱 Provisionin	g Services Imaging Wizard		×
Restart No	zeded		
During device After device	ce restart, configure the machine settings for network boot. e restart, the Imaging Wizard will continue.		
Connect to Task: Crea Target dev Network of Collection: vDisk name Store: Sto Format: V Image ent Optimize h	o Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 te a vDisk <i>ice</i> name : Win10-TD onnection : Ethernet0, 10.10.208.100, 00-50-56-AE-53-7B Collection :: Win10-vDisk re HDX, type: Dynamic (recommended), sector size: 512 B, block size: 32 MB re boot disk ard disk for Provisioning Services prior to imaging	^	
		~	
Status: Progress:	Successful!	,	
	Log Continue	Cancel	

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



- 23. Edit the virtual machine settings and select Boot options under VM Options.
- 24. Select Force BIOS setup.

General Options	VM Name: TEST0015
VMware Remote Console Options	 Lock the guest operating system when the last remote user disconnects
Encryption	Expand for encryption settings
Power management	Expand for power management settings
VMware Tools	Expand for VMware Tools settings
Virtualization Based Security	Enable
Boot Options	
Firmware	BIOS 🗸
Boot Delay	When powering on or resetting, delay boot order by 0 milliseconds
Force BIOS setup	During the next boot, force entry into the BIOS setup screen
Failed Boot Recovery	 If the VM fails to find boot device, automatically retry after seconds
Advanced	Expand for advanced settings
Fibre Channel NPIV	Expand for Fibre Channel NPIV settings

- 25. Restart Virtual Machine.
- 26. When the VM boots into the BIOS, got to Boot menu to move the Network boot from VMware VMXNET3 to the top of the list.

			PhoenixB	OS Setup	Utility	
Main	Advan	ced	Security	Boot	Exit	
	etwork boo	nt from	UMware UMXI	(ET3		Item Specific Help
	ard Drive emovable D D-ROM Driv	e ices e				Keys used to view or configure devices: <enter> expands or collapses devices with a + or - <ctrl+enter> expands all <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.</d></n></ctrl+enter></enter>
F1 H Esc E	elp †↓ xit ↔	Select Select	Item -/+ Menu Ente	Change er Select	e Values t ► Sub-Me	F9 Setup Defaults enu F10 Save and Exit

27. Restart Virtual Machine

么

After restarting the virtual machine, 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.

28. If prompted to Restart select Restart Later.

🗱 Provisioning	g Services Imaging Wizard		×
Processing	1		
Imaging is li	ely to take a long time.		
Connect to Task: Imag Existing vD	Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 e created vDisk isk: Store\Win10-vDisk	^	
<		~	
Status: Progress:	Copying C:		
		Log Cance	I

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

🗱 Provisionin	g Services Imaging Wizard		×
Finished			
The log of t	he processing done can be viewed by clicking the Log button.		
Connect to Task: Imag Existing vE	o Site: Server: CTX-PVS1.vdilab-v.local, Port: 54321 je created vDisk Disk: Store\Win10-vDisk		~
<		>	~
Status: Progress:	Successful!		
		Log	one

- 30. Shutdown the virtual machine used as the VDI or RDS master target.
- 31. Connect to the PVS server and validate that the vDisk image is available in the Store.
- 32. Right-click the newly created vDisk and select Properties.



33. On the vDisk Properties dialog, change Access mode to "Private" mode so the Citrix Virtual Desktop Agent can be installed.

Install Citrix Virtual Apps and Desktop 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.

To install Citrix Desktop Virtual Desktop Agents, follow these steps:

- 1. Launch the Citrix Desktop installer from the CVA Desktop 1912 LTSR ISO.
- 2. Click Start on the Welcome Screen.

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: Virtual Apps Deliver applications Virtual Apps and Docktops are according to your needs:	
Virtual Apps and Desktops Deliver applications and desktops Cancel	
CITRIX	

3. 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			Aachines and	Images			
			Virtual Delivery Agent for Windows Server OS				
		roller and other install th Front. based VA		eliver applications and desktops from I machines.			
Extend Deployment		_			C		
Citrix Director		Citrix Studio		Self-Service Password Reset			
Citrix License Server		Universal Print Server		Session Recording			
Citrix StoreFront		Federated Authentication Serv					

- 4. Select Create a Master Image.(Be sure to select the proper provisioning technology)
- 5. Click Next.

	Environment
Environment Core Components Additional Components Delivery Controller Features Firewall Summary Install Smart Tools Finish	Configuration I want to: I want to: <t< th=""></t<>
	Back Next Cance

- 6. Optional: Select Citrix Workspace App.
- 7. Click Next.



Environment	Component (Select all)
Core Components Additional Components	Citrix Personalization for App-V - VDA Enables this machine to launch App-V packages, <u>Learn more</u>
Delivery Controller Features	Citrix AppDisk / Personal vDisk (Deprecated) Installs components used for AppDisk and Personal vDisks. <u>Learn more</u>
Firewall Summary Install Smart Tools Finish	Citrix Supportability Tools Installs the Citrix Health Assistant and VDA Clean Up Utility Learn more
	Citrix User Profile Manager Manages user personalization settings in user profiles. Omitting this component affects monitoring and troubleshooting VDAs with Director. Learn more.
	Citrix User Profile Manager WMI Plugin Provides Profile management runtime information in WMI (Windows Management Instrumentation) objects, for example, profile provider, profile type, size, and disk usage. WMI objects provide session information to Citrix Director.
	Citrix Files for Windows Allows users to connect to their ShareFile account and interact with ShareFile via a "mapped drive" in the Windows file system, without performing a full sync of

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

	Delivery Controller	
🛩 Environment	Configuration	
Core Components	How do you want to enter the locations of your Delivery C	ontrollers?
 Additional Components 	Do it manually	•
Delivery Controller		9
Firewall	CTX1-1808.vdilab-hx.local	Edit Delete
Summary	CTX2-1808.vdilab-hx.local	Edit Delete
Install	Controller address:	
Smart Tools	Example: controller1.domain.com	
Finish	lest connection Add	

11. Accept the default features.

12. Click Next.

	reatures
Environment	Feature (Select all)
Core Components Additional Components	Optimize performance Optimize desktop settings. <u>Learn more</u>
Delivery Controller Features	Use Windows Remote Assistance Enable Windows Remote Assistance. <u>Learn more</u>
Summary	Use Real-Time Audio Transport for audio Uses UDP ports 16500 - 16509. <u>Learn more</u>
Install Smart Tools Einich	Framehawk Opens UDP ports 3224-3324.Learn more.

13. Allow the firewall rules to be configured automatically.

14. Click Next.

	Firewall	
 Environment Core Components Additional Components Delivery Controller Features Firewall Summary Install Smart Tools Finish 	The default ports are listed below. Controller Communications 80 TCP 1494 TCP 2598 TCP 8008 TCP 1494 UDP 2598 UDP	Printable version
	Configure firewall rules: Automatically Select this option to automatically create the rules be created even if the Windows Firewall is turned o Manually Select this option if you are not using Windows Fire yourself.	in the Windows Firewall. The rules will Iff. ewall or if you want to create the rules

15. Verify the Summary and click Install.

	Summary	
Environment Core Components	Review the prerequisites and confirm the components you want to install.	Restart required
Additional Components Delivery Controller Features	Installation directory C:\Program Files\Citrix	Î
 ✓ Delivery Controller ✓ Features ✓ Firewall Summary Install Smart Tools Finish 	Microsoft .NET Framework 4.7.1 Microsoft Remote Desktop Session Host Microsoft Remote Desktop Connection Windows Remote Assistance Feature Microsoft Visual x64 C++ 2013 Runtime Microsoft Visual x66 C++ 2015 Runtime Microsoft Visual x86 C++ 2013 Runtime Microsoft Visual x86 C++ 2013 Runtime Core Components Virtual Delivery Agent Additional Components Citrix Supportability Tools Citrix Supportability Tools	

16. (Optional) Select Call Home participation.

	Smart Tools
 Licensing Agreement Core Components Features Firewall Summary Install Smart Tools Finish 	Automate deployment tasks, health checks, and power management on-premises and in the cloud. Smart Check Run health checks and turn on Call Home to diagnose issues and find recommended fixes. Learn more about Call Home Smart Scale Smart Migrate Simplify migration to the latest Virtual Apps and Desktops versions. Smart Build Quickly build sites on-premises and in the cloud using ready-made or custom blueprints. I want to connect to Smart Tools. (Recommended) I do not want to connect to Smart Tools You will need Citrix Cloud or citrix.com credentials. View your privacy policy here.

- 17. (Optional) Check Restart Machine.
- 18. Click Finish.
- 19. Repeat steps 1 18 so that VDAs are installed for both HVD (using the Windows 10 OS image) and the HSD desktops (using the Windows Server 2019 image).
- 20. Select an appropriate workflow for the HSD desktop.

Delivery Controller Start here. Select and install the I essential services like License Ser	Delivery Conti ver and Store	Virtual Delh roller and other Install this ag Front. based VMs o	very Ag ent to d r physic	ent for Windows Server OS leliver applications and desktops from serve al machines.	a-
Extend Deployment Citrix Director		Citrix Studio	•	Self-Service Password Reset	4
Citrix License Server		Universal Print Server			
Citrix StoreFront		Federated Authentication Service			

- 21. Once the Citrix VDA is installed, on the vDisk Properties dialog, change Access mode to "Standard Image (multi-device, read-only access)."
- 22. Set the Cache Type to Cache in device RAM with overflow on hard disk.
- 23. Set Maximum RAM size (MBs): 256 for VDI and set 1024 MB for RDS vDisk.

	vDisk Properties							
General	Identification	Microsoft Volume Licensing	Auto Update					
Site	: Site							
Stor	e: Store							
Filer	name: Win10)-vDisk						
Size	32,76	7 MB Block size:	32,768 KB					
Acc	ess mode ess mode: Sta	andard Image (multi-device, re	ad-only access)	~				
Cac	Cache type: Cache in device RAM with overflow on hard disk 🗸							
Max	imum RAM size	e (MBs): 64 🔹						
BIO	S boot menu te	xt (optional):						
Enable Active Directory machine account password management Enable printer management Enable streaming of this vDisk								
		ОК	Cancel	Help				

- 24. Click OK.
- 25. Repeat steps 1 24 to create vDisks for both the Hosted VDI Desktops (using the Windows 10 OS image) and the Hosted Shared Desktops (using the Windows Server 2019 image).

Provision Virtual Desktop Machines

To create VDI and RDS machines, follow these steps:

- 1. Select the Master Target Device virtual machine from the VCenter Client.
- 2. Right-click the virtual machine and select Clone -> Clone to Template.
- 3. Name the clone Template.
- 4. Select the cluster and datastore where the first phase of provisioning will occur.

vm vSphere	Client Menu 🗸	Q Searc	h in all environments			
	■ 9 B N	ewMCS		ACTIONS ~		
~ 🗗 10.10.31.40	📩 Summa	ry Monitor	Configure Permis	sions Datastores	Networks Updates	
∽ 🖪 8x16		-	1	Carlos Carlos Carlos		
∽ 🛄 8x16-ESX			Guest OS: Micro Compatibility: ESXI	soft Windows 10 (64-bit) 6.7 and later (VM version 1	4)	
10.10.3	0.128		VMware Tools: Not n	unning, version:11265 (Curr	ent)	
10.10.3	0.129	owered Off	More	info		
10.10.3	0.130		DNS Name:			
10.10.3	0.131		Host: 10.10.	30.130		
10.10.3	0.132 Launch	Web Console Demote Console				
10.10.3	Actions - NewMCS	Remote Console				
10.10.3	Dower					
10.10.3	Fower	e				
10.10.3	Guest OS	•				
10.10.3	Snapshots	▶ ects				1
10.10.3	Popen Remote Console			Rx16-ESX		
10.10.3	Bh Minute			Chie Carlo Con		
10.10.3	Migrate	_		10.10.30.130		
10.10.3	Clone	 g^a Clone 	to Virtual Machine	vm-network	-34	
10.10.3	Fault Tolerance	► gD Clone	to Template	- -	and the second second second second second second second second second second second second second second second	
10.10.3	VM Policies	A AR CINE		U vdi-workioa	3-2	
10.10.3	VIII I OICICS	- S- Clore	as remplate to Library			
10.10.3	Template	•				
10.10.3	Compatibility					
10.10.3	Export System Logs		C	ategory	Description	
10.10.3						
10.10.3	Dy Edit Settings					
🗗 AA-1	Move to folder					
🗗 New V	Rename					
B NewMo	Edit Notes					

5. Name the template and click Next.

Select a name and folder Select a compute resource	Select a name and folder Specify a unique name and target location				
3 Select storage 4 Ready to complete	VM template name:	Template		2	
	Select a location for	the template.			
	V 🔂 10.10.31.40				
	> 1 8x16				
	L		CANCEL	aver I No	

6. Select a host in the cluster to place the template.

1 Select a name and folder 2 Select a compute resource 3 Select storage	Select a compute resource Select the destination compute resource for this operation	
4 Ready to complete	✓ □18×16	
	✓ □ 8×16-ESX	
	10.10.30.128	
	10.10.30.129	
	10.10.30.130	
	10.10.30.131	
	10.10.30.132	
	10.10.30.133	
	10.10.30.134	
	10.10.30.135	
	10.10.30.130	
	10.10.30.137	
	10.10.30.139	
	10.10.30.139	
	10.10.30.140	
	Compatibility	
	Compatibility checks succeeded.	

2 Select a compute resource	Select storage Select the storage for the configuration and disk files				
3 Select storage 4 Ready to complete	Select virtual disk format:		Same format as so	Configure per di ource ~	sk 🔾
	VM Storage Policy:		Keep existing VM storage policies		icies v
	Name	Capacity	Provisioned	Free	Туј
	esxtop	1 TB	67.5 GB	960.7 GB	NE
	SpringpathDS-WZP22121	216 GB	12.16 GB	203.84 GB	V?
	vdi-workload-2	60 TB	46.25 TB	58.2 TB	NF
	Vdi_workload	40 TB	46.49 TB	38.04 TB	NF
	4				
	< Compatibility	_			
	< Compatibility Compatibility checks succe	eeded.			

- 8. Click Next.
- 9. Click Next through the remaining screens
- 10. Click Finish to create the template.

 1 Select a name and folder 2 Select a compute resource 	Ready to complete Click Finish to start creation.				
 3 Select storage 4 Ready to complete 					
	Provisioning type	Clone virtual machine to template			
	Source virtual machine	AA-1			
	Template name	Template			
	Folder	8x16			
	Host	10.10.30.128			
	Datastore	vdi_workload			
	Disk storage	Same format as source			
		CANCEL BACK FINIS			

- 11. From Citrix Studio on the Desktop Controller, select Hosting and Add Connection and Resources.
- 12. Select Use an existing Connection and click Next.
- 13. Correspond the name of the resource with desktop machine clusters.



14. Browse and select the VCenter cluster for desktop provisioning and use the default storage method Use storage shared by hypervisors.

Studio Connection Storage Management Storage Selection Network Summary	Storage Management Configure virtual mach Select a cluster: Select an optimization © Use storage shared © Optimize temp local storage © Use storage local t @ Manage persor shared storage	Select a cluster Select a cluster VDI-DC N Control N Control N Control

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

Studio	Storage Selection When using shared storage, you must select the type of data to store on each shared storage device; machine operating system data, personal user data, and if not storing temporary data				
Connection	locally, temporary data. At least one device must be selected for each data type.				
Storage Management	Select data storage loc	ations:			
Storage Selection	Name	+	OS	Personal vDisk	Temporary
Natwork	esxtop		1		
	vdi_workfoad		2	Z	<u> </u>

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

Studio	Network	
✓ Connection	Name for these resources: two-to-one	
✓ Storage Management	The resources name helps identify this storage and network combination in Select one or more networks for the virtual machines to use:	s Studio.
Network Summary	Name Storage Controller Data Network Storage Controller Management Network Storage Controller Replication Network vm-34 vm-setwork-34	*

17. Click Finish.

Return to these settings to alter the datastore selection for each set of provisioned desktop machines if you want to create a separate datastore for each image

Provision Desktop Machines from Citrix Provisioning Services Console

To provision the desktop machines using the Citrix Provisioning Service Console, follow these steps:

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



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

Citrix Virtual Desktops Setup	×
	Welcome to Citrix Virtual Desktops
CITRIX	
	This setup allows you to create virtual machines and Citrix Provisioning devices in a Collection that matches the name of the Catalog, assign a standard mode virtual disk, and add virtual desktops to a Citrix Virtual Desktops Catalog.
	Requirements: * Citrix Virtual Desktops Controller with permissions for the current user. * Configured Citrix Virtual Desktops Host Resources. * A standard-mode vDisk for the selected VM template.
	< Back Next > Cancel

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

Citrix Virtual Desktops Setup	×
Citrix Virtual Desktops Controller Enter the address of the Citrix Virtual Desktops Controller you want to configure.	
Citrix Virtual Desktops Controller address: 10.34.0.89	
< Back Next >	Cancel

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

iter your o	redentials for the Citrix Virtual Desktops Host Res
emame:	hxhvdom\administrator
ssword:	

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

itrix Virtual Desktops Setup		>
Template		
Select the Template you want to use:		
Select a template for the Citrix Virtual Deskto	ps Host Resources.	
Virtual Machine Template		
Final		
Select the VDA version installed on this temp	plate:	
7.9 (recommended, to access the latest feat	ures)	~

13. Select the vDisk that will be used to stream virtual machines.

Citrix Virtual Desktops Setup		×
vDisk		
Select an existing standard-mode vDisk.		
Standard-mode vDisk:		
Store\Gen1-W10v1		
Store Win 10-1811V1		
L		

15. Select Create a new catalog.



Citrix Virtual Deskt	ops Setup			×
Catalog Select your Ca	atalog preferences.			
Create a ner	w catalog			
Use an exist	ing catalog			
Catalog name:	VDI			
Description:	Windows 10 Desktops			
		< Back	Next >	Cancel

- 17. 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.
- 18. Click Next.

Citrix Virtual Desktops Setup	×
Operating System	
Select an operating system for this Machine Catalog.	~
⊖ Server OS	
The Server OS Machine Catalog provides hosted shared desktops for a large deployment of standard Windows Server OS or Linux OS machines.	e-scale
Desktop OS	
The Desktop OS Machine Catalog provides VDI desktops ideal for a variety different users.	of
Note:	
This infrastructure will be built using virtual machines.	
Virtual disk images will be managed using Citrix Provisioning (PVS)	
	-
< Back Next >	Cancel

19. 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.

User Experience Tell me more about logon and appearance. Image: Comparison of the series of the	rix Virtual Desktops Setup	
Select how your users will log on and access their virtual desktops. Tell me more about logon and appearance. At logon, connect users to: A fresh new (random) desktop each time The same (static) desktop Save changes that users have made to their virtual desktops? Save changes and store them on a separate personal vDisk No. discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management. 	Jser Experience	\sim
At logon, connect users to: (a) A fresh new (random) desktop each time (b) The same (static) desktop Save changes that users have made to their virtual desktops? (c) Save changes and store them on a separate personal vDisk (c) No. discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management.	Select how your users will log on and access their virtual desktops. Tell me more about logon and appearance.	<u> </u>
 A fresh new (random) desktop each time The same (static) desktop Save changes that users have made to their virtual desktops? Save changes and store them on a separate personal vDisk No. discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management. 	At logon, connect users to:	
 The same (static) desktop Save changes that users have made to their virtual desktops? Save changes and store them on a separate personal vDisk No, discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management. 	A fresh new (random) desktop each time	
 Save changes that users have made to their virtual desktops? Save changes and store them on a separate personal vDisk No. discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management. 	◯ The same (static) desktop	
 Save changes and store them on a separate personal vDisk No. discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management. 	Save changes that users have made to their virtual desktops?	
No, discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have single image management.	Save changes and store them on a separate personal vDisk	
	No. discard changes and clear virtual desktops at logoff User always goes to the same virtual machine, but you still have image management.	: single

21. On the Virtual machines dialog, specify:

- a. The number of virtual machines to create.
- b. Number of vCPUs for the virtual machine (2 for VDI, 8 for RDS).
- c. The amount of memory for the virtual machine (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.
- 22. Click Next.

Citrix Virtual Desktops Setup				×
Virtual machines Select your virtual machine pref	erences.			
Number of virtual machines to	create:	800	-	
vCPUs:	2	2	÷	
Memory:	4096 MB	4096	MB	
Local write cache disk:	6 GB	6	🖨 GB	
Boot mode:	a running PXE servi	ce)		
O BDM disk (create	a boot device manag	er partition)		
	< E	Back N	ext >	Cancel

23. Select the Create new accounts radio button.

		×
		640
< Back	Next >	Cancel
	< Back	< Back Next >

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

				and the second s
Creat	Directory accou	unts and location	1	Y
Great	e Active Directory	accounts.		
ctive Di	rectory location fo	r computer account	s:	
)omain:	hxhvdom.local			~
⊿ hxhv	dom.local			
🔺 l	LoginVSI			
	▲ Computers			
	Launcher			
	Larget			
9	p Users Servers			
8	FestOU			
whydom	ı.local/LoginVSI/0	Computers/Target		
whvdom vccount i	1.local/LoginVSI/	Computers/Target		0-9 V
nxhvdom Iccount i	n.local/LoginVSI/ naming scheme:	Computers/Target		0-9 ~
vchvdom ccount i	n.local/LoginVSI/ naming scheme:	Computers/Target NP-### NP-001		0-9 ~
oxhvdom .ccount i	n.local/LoginVSI/	Computers/Target NP-### NP-001		0-9 ~

28. Click Finish to begin the virtual machine creation.

Catalog name	1811
Catalog type	VDI PVS Random
VDA version	7.9 (recommended, to access the latest features)
Citrix Virtual Desktops Host Resources	i hx
Virtual machine template	Yes
Existing vDisk	Win10-1811v1
vCPUs	2
Memory per VM	4096 MB
Local write cache disk	6 GB
Boot mode	PXE
Active Directory accounts	Create 200
ogress	

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

30. 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			-	• ×
🗱 File Action View Window Help							- 8 ×
🗢 🔿 🙍 📰 📓 🖬							
Console Provisioning Services Console	Name	MAC	Туре	Disk	vDisk	IP Address	Server
a 🔛 Farm (localhost)	CTX-VDINP-001	00-50-56-AE-AE-0D	Production	vDisk	Store/Win10-vDisk	Down	
4 😃 Sites							
a 🛄 Site							
E Servers							
VDisk Pool							
Im vDisk Update Management							
Device Collections							
Collection							
VDI-NP							
Views							
Hosts							
p L views							
4 w stores							
See Store							

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

#		Citrix Studio	l	- 🗆 X
File Action View Help				
← → 🖄 🖬 📓 📼				
🗱 Citrix Studio (Site)	elenar		Actions	
Search	cirkix		Machine Catalogs	•
AppDisks	Machine Catalog	No. of machines Allocated machines	📹 Create Machine Catalog	
B Delivery Groups	VDI-NP Desktop OS (Virtual)		View	•
Applications	Allocation Type: Random User data: Discard	Provisioning method: Citrix provisioning services	Refresh	
Logging			Help	
Configuration			VDI-NP	
			Add Machines	
			Edit Machine Catalog	
			View Machines	
			Delete Machine Catalog	
			Rename Machine Catalog	
	Details - VDI-NR		Test Machine Catalog	
			Help	
	Details Machines Woministrators			
	Machine Catalog	Machine		
	Name: VDI-NP Machine Type: Desktop OS (Virtual) Provisioning Method: Cirris provisioning servi Allocation Type: Random Setto VOA version: 7.9 Scopes: All Zone: Primary	Installed VDA version: 7.9.0.101 Operating System: Windows 10		
	Details - VDI-NP Details Machine: Administrators Machine Catalog Name: Desktop OS (Virtual) Name: Desktop OS (Virtual) Critic provisioning servi Allocation Type: Desktop OS (Virtual) Randem Settor VOA version: 7.9 Scope:: All Zone: Primary Primary Primary	Machine A Installed VDA version: 7.9.0.301 Operating System: Windows 10	 Edit Machine Catalog View Machines Delete Machine Catalog Rename Machine Catalog Test Machine Catalog Test Machine Catalog Help 	

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



31. Log into the 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.



Install Citrix Virtual Apps and Desktop 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 Citrix Desktop Virtual Desktop Agents, follow these steps:

- 1. Launch the Citrix Desktop installer from the CVA Desktop 1912 LTSR ISO.
- 2. Click Start on the Welcome Screen.

23

	Res	
Deliver applications a - Hybrid cloud, cloud and enterprise - Centralized and flexible managemo Manage your delivery accordin	Ind desktops to any user, anywhere, provisioning mt g to your needs:	on any device.
Virtual Apps Deliver as	uplications	Start
Virtual Apps and	Desktops Deliver applications and desktops	Start
	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.

			Prepare Machines a	nd Images		
			Virtual Delivery A			
					plications and desktops from s res.	
Extend Deployment						<
Extend Deployment Citrix Director	•	Citrix Studio		Self-5	ervice Password Reset	< (1
Extend Deployment Citrix Director Citrix License Server	•	Citrix Studio Universal Print Serve	er (Self-S Sessio	ervice Password Reset	< (1)

- 4. Select Create a Master Image. (Be sure to select the proper provisioning technology)
- 5. Click Next.

	Environment
Environment Core Components Additional Components Delivery Controller Fastures	Configuration I want to: Create a master MCS image Select this option if you plan to use Citrix Machine Creation Services (MCS) to provision virtual servers from this master image
Firewall Summary Install Smart Tools Finish	 Create a master image using Citrix Provisioning or third-party provisioning tools Select this option if you plan to use Citrix Provisioning or a third-party provisioning tool (such as Microsoft SCCM) to provision virtual servers from this master image. Enable Brokered Connections to a Server Select this option to install the VDA on a physical or virtual server that will NOT be used by any provisioning tools.

- 6. Optional: Select Citrix Workspace App.
- 7. Click Next.

	core components
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 provide the virtual desktop or application to the user.
Firewall Summary Install	Citrix Workspace App Client software that enables users to access their documents, applications, and desktops from any device, including smartphones, tablets, and PCs.
Smart Tools Finish	


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

Environment Configuration Core Components How do you want to enter the locations of your Delivery Controllers? Delivery Controller Do it manually Features CTX1-1808.vdilab-hx.local Firewall CTX2-1808.vdilab-hx.local Summary CTX2-1808.vdilab-hx.local Install Controller address: Smart Tools Example: controller1.domain.com Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override		Delivery Controller			
Core Components How do you want to enter the locations of your Delivery Controllers? Delivery Controller Do it manually Features CTX1-1808.vdilab-hx.local Firewall CTX2-1808.vdilab-hx.local Summary CTX2-1808.vdilab-hx.local Install Controller address: Smart Tools Example: controller1.domain.com Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override	* Environment	Configuration			
Additional Components Delivery Controller Features Firewall Summary Install Controller address: Smart Tools Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override	Core Components	How do you want to enter the locations of your Delivery (Controllers?		
Delivery Controller Controller Features CTX1-1808.vdilab-hx.local Firewall CTX2-1808.vdilab-hx.local Summary CTX2-1808.vdilab-hx.local Install Controller address: Smart Tools Example: controller1.domain.com Finish Test connection Add	Additional Components	Do it manually	•		
Features CTX1-1808.vdilab-hx.local Edit Delete Summary CTX2-1808.vdilab-hx.local Edit Delete Install Controller address: Example: controller1.domain.com Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override	Delivery Controller Features Firewall	bo t mandany			
Summary CTX2-1808.vdilab-hx.local Edit Delete Install Controller address: Smart Tools Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override		CTX1-1808.vdilab-hx.local	Edit Delete		
Install Controller address: Smart Tools Example: controller 1.domain.com Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override	Summary	CTX2-1808.vdilab-hx.local	Edit Delete		
Smart Tools Example: controller1.domain.com Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override	Install Smart Tools	Controller address:			
Finish Test connection Add Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override		Example: controller1.domain.com			
Note: Entry of invalid special characters will be ignored. Note: Any Group Policies that specify Delivery Controller locations will override	Finish	Test connection Add			
settings provided here.					

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

	Features
Environment Core Components Additional Components Delivery Controller Features Firewall Summary Install Smart Tools Finish	□ Feature (Select all) ✓ Optimize performance Optimize desktop settings.Learn more. □ Use Windows Remote Assistance Enable Windows Remote Assistance.Learn more. □ Use Real-Time Audio Transport for audio Uses UDP ports 16500 - 16509.Learn more. □ Framehawk Opens UDP ports 3224-3324.Learn more.

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

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

15. Verify the Summary and click Install.



16. (Optional) Select Call Home participation.

	Smart Tools
Licensing Agreement Core Components Features Firewall Summary Install Smart Tools Finish	Automate deployment tasks, health checks, and power management on-premises and in the cloud. 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 Migrate Simplify migration to the latest Virtual Apps and Desktops versions.
	Quickly build sites on-premises and in the cloud using ready-made or custom blueprints. I want to connect to Smart Tools. (Recommended) I do not want to connect to Smart Tools You will need Citrix Cloud or citrix.com credentials. View your privacy policy here. Connect
	Back Net Carea

- 17. (Optional) Check Restart Machine.
- 18. Click Finish.

- 19. Repeat steps 1 18 so that VDAs are installed for both HVD (using the Windows 10 OS image) and the HSD desktops (using the Windows Server 2019 image).
- 20. Select an appropriate workflow for the HSD desktop.

Delivery Controller Start here. Select and install the essential services like License S	Delivery Cont	Virtual Del roller and other install this a Front. based VMs i	very Ag gent to d or physic	ent for Windows Server OS leliver applications and desktops from server- al machines.
Extend Deployment Citrix Director		Citrix Studio	•	Self-Service Password Reset
Citrix License Server		Universal Print Server		
Citrix StoreFront		Federated Authentication Service		

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, follow these 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 Virtual Desktops server and launch Citrix Studio.
- 2. Choose Create Delivery Group from the drop-down list.

#				Citrix Studio
File Action View Image: Constraint of the second s	Help			
Citrix Studio (Site)	citrix		Search	۶ 🛛
AppDisks	Delivery Group	+	Delivering	No. of mac
Applications Policies Policies Policies	Create Delivery Group]		
Configuration	Refresh Help	-		
		_		

3. Click Next.

Studio	Getting started with Delivery Groups
Introduction	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.
Machines Machine allocation	Make sure you have enough machines available in desktop OS or server OS Machine Cataloos 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.

Juano	Wach	ines		
	Select	a Machine Catalog.		
		Catalog	Туре	Machines
Introduction	•	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	- +

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

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



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
 Introduction Machines 	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
	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		
	Machine Catalog:	Win10MCS-Random	
* Introduction	Machine type:	Desktop OS	
Machinar	Allocation type:	Random	
* Machines	Machines added:	VDILAB-XD\w10mcs-r0001	
✓ Users		VDILAB-XD\w10mcs-r0002 VDILAB-XD\w10mcs-r0003	
 Applications 		VDILAB-XD\w10mcs-r0004	
Summary	5	VDILAB-XD\w10mcs-r0005	
		VDILAB-XD\w10mcs-r0006 VDILAB-XD\w10mcs-r0007	
		VDILAB-XD\w10mcs-r0008	
		VDILAB-XD\w10mcs-r0009 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):	

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.

	liver Cround	
De	Greeke Delivery Groups	-
	Create Delivery Group	
	View	•
a	Refresh	
?	Help	
hxo	dedicated	*
P	Add Machines	
6	Edit Delivery Group	
8	Manage AppDisks	
9	Manage Tags	
2	Turn On Maintenance	
1	Rename Delivery Group	
	Delete Delivery Group	
0	View Machines	
D	Test Delivery Group	
?	Help	

Citrix Virtual Desktops Policies and Profile Management

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

Configure Citrix Virtual Desktops Policies

Citrix Virtual Desktops 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 25 shows policies for Login VSI testing in this CVD.

Figure	25	Virtual	Desktons	Policy
Iguie	ZJ .	viituai	Desktops	FUILT

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	Auto-create client printers User setting - ICA\Printing\Client Printers Do not auto-create client printers (Default: Auto-create all client printers)
4 KDS Policy	Client printer redirection User setting - ICA\Printing Prohibited (Default: Allowed)
	 Concurrent logons tolerance Computer setting - Load Management Value: 4 (Default: Value: 2)
	 CPU usage Computer setting - Load Management Disabled (Default: Disabled)
	 CPU usage excluded process priority Computer setting - Load Management Disabled (Default: Below Normal or Low)
	 Flash default behavior User setting - ICA\Adobe Flash Delivery\Flash Redirection Disable Flash acceleration (Default: Enable Flash acceleration)
	 Memory usage Computer setting - Load Management Disabled (Default: Disabled)
	 Memory usage base load Computer setting - Load Management Disabled (Default: Zero load: 768 MBs)

Configure 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 Virtual Desktops 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: <u>https://docs.citrix.com/en-us/citrix-virtual-apps-desktops</u>

Figure 26. VDI User Profile Manager Policy

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

Test Setup and Configurations

In this project, we tested a single Cisco HyperFlex stretch cluster running four Cisco UCS HXAF220C-M5SX Rack Servers in two separate Cisco UCS domains for a combined 8 node HX cluster. This solution is tested to illustrate linear scalability for each workload studied. We tested failover and resiliency of the stretch cluster, as well as VDI performance.



Hardware Components:

- 4 x Cisco UCS 6454 Fabric Interconnects
- 4 x Cisco Nexus 93108YCPX Access Switches
- 8 x Cisco UCS HXAF220c-M5SX Rack Servers (2 Intel Xeon Gold 6230 scalable family processor at 2.3 GHz, with 768 GB of memory per server [32 GB x 24 DIMMs at 2666 MHz])
- Cisco VIC 1457 mLOM
- 12G modular SAS HBA Controller
- 240GB M.2 SATA SSD drive (Boot and HyperFlex Data Platform controller virtual machine)
- 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 4.0(4g)

- Cisco HyperFlex Data Platform 4.0.2b
- Citrix Virtual Desktops 1912 LTSR
- Citrix User Profile Management
- Microsoft SQL Server 2016
- Microsoft Windows 10
- Microsoft Windows 2019
- Microsoft Office 2016
- Login VSI 4.1.40

Test Methodology and Success Criteria

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

Along with regular performance testing for VDI workloads, we also tested disaster recovery and failover functionality of a stretched cluster environment.

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.

Test Procedure

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

Pre-Test Setup for Testing

Windows 10 virtual machines for VDI and Windows 2019 Server for RDS were deployed on both sites of the stretch cluster. Fifty percent of the total number on each site. All machines were shut down utilizing the Citrix Virtual Desktops 1912 LTSR 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 500 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. To run the test protocol, follow these steps:

- 1. Time 0:00:00 Start esxtop Logging on the following systems:
 - a. Infrastructure and VDI Host Blades used in test run
 - b. All Infrastructure virtual machines used in test run (AD, SQL, Citrix Connection brokers, image mgmt., and so on)
- 2. Time 0:00:10 Start Storage Partner Performance Logging on Storage System.

- 3. Time 0:05: Boot VDI Machines using Citrix Virtual Desktops 1912 LTSR Administrator Console.
- 4. Time 0:06 First machines boot.
- 5. Time 0:35 Single Server or Scale target number of VDI Servers registered on Desktop Studio.

No more than 60 Minutes of rest time is allowed after the last desktop is registered and available on Citrix Virtual Desktops 1912 LTSR Administrator Console dashboard. Typically, a 20-30 minute rest period for Windows 10 desktops and 10 minutes for RDS virtual machines is sufficient.

- Time 1:35 Start Login VSI 4.1.40 Knowledge Worker Benchmark Mode Test, setting auto-logoff time at 900 seconds, with Single Server or Scale target number of desktop virtual machines utilizing sufficient number of Launchers (at 20-25 sessions/Launcher).
- 7. Time 2:23 Single Server or Scale target number of desktop virtual machines 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 Virtual Desktops 1912 LTSR 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.

Stretch Cluster Failure Modes

One of the main precautions required for using a stretch or metropolitan (multisite) single cluster is the need to avoid a split-brain scenario. A split-brain condition indicates data or availability inconsistencies originating from the maintenance of two separate data sets with overlap in scope, either because of the loss of a site or a failure condition based on servers not communicating and synchronizing their data with each other (site link loss). The witness exists to prevent this scenario, and it is discussed in the various failure modes presented here.

Because a stretch cluster is a single cluster, for most failure situations you can simply ask yourself: How would a single cluster with a replication factor of 2 behave here? It is when you experience site losses (or more than two

simultaneous node failures on a single site) that the behavior diverges from that of the single-location RF 2 cluster because you actually have the advantage of an effective RF4.

To appreciate the failover mechanics of a stretch cluster, take a closer look at ZooKeeper. Architecturally, a stretch cluster contains five instances of ZooKeeper: two at each site and one on the witness server. So, in total there is one master ZK node and 4 followers. Only a storage node can be ZK nodes. Compute-only nodes will never be created with a ZK instance. The function of ZooKeeper is to maintain the cluster membership and a consistent cluster-wide file system configuration. So, if there are eight nodes at each site (a 16-node cluster), there will still be two ZooKeeper instances running on two nodes at each site and one more on the witness server.

Whenever a failure occurs, at least three ZooKeeper instances must be present to re-create the cluster membership and help ensure a consistent file system configuration. ZooKeeper achieves this behavior by using its built-in voting algorithm (based on the well-known Paxos algorithm).

If the witness goes down, then one ZooKeeper instance is lost. However, four more ZooKeeper instances are still running (2 at each site), which is more than the minimum of three ZooKeeper instances needed. Hence, the cluster will not be affected (no virtual machine failover or internal I/O hand-off occurs).

If a site goes offline, two ZooKeeper instances will go down. However, three more ZooKeeper instances are still running, which again is greater than or equal to the minimum of three ZooKeeper instances required. Hence, the cluster will not be affected. Virtual machines will automatically failover to the surviving site because of the presence of VMware HA. This failure will be treated as if half (minus one since the witness is still online) the number of nodes are lost in a single cluster.

If a ZK node at a site goes down that was hosting the ZooKeeper master, the ZooKeeper algorithm will elect another ZK node to be promoted to ZooKeeper master. The promotion of another ZK node happens only if the failed node is a master ZK node and the failover target is part of the ZK ensemble (which is always the case for a ZK master). If the failed node was a ZK follower (i.e. a stand-alone ZK node), then no election occurs, and you are running with one less ZK instance. Either way, four more ZooKeeper instances are still running, which is more than the minimum of three ZooKeeper instances required. The site and the cluster will still be online. Only the affected virtual machines will be restarted on the surviving nodes at the same site (with stretch cluster DRS rules managing the movement). The failure will be treated like a node lost in a single cluster.

It is expected that you will recover or replace any failed nodes. New ZK nodes will not be automatically created. If those nodes happen to be ZK nodes, then there is a manual process to reassign ZK membership if the node needs to be completely replaced. See your support representative for assistance. A recovered node will simply resume its previous role unless it was master (since a new master is now elected) in which case it will join as a follower.

Survivability while maintaining online status after node losses requires a majority zookeeper quorum and more than 50% of any nodes (the witness counts as an active zookeeper node). If one site has suffered multiple loss-es, it is possible that the surviving site could tolerate a node or disk loss (in a cluster greater than 2+2) if that node is not a zookeeper node, but it is not guaranteed.

Zookeeper has a notable dependence on NTP from the nodes to maintain cluster synchronization. The allowable ZK time drift between nodes is 300ms. If the skew exceeds this the cluster is subject to ZK errors and may not function properly. If is advisable to monitor NTP skew between CVMs using the HX APIs and alert on time drift issues.

Recovery of ZK Nodes that have Failed

As mentioned above, there are two types of ZK nodes: a single ensemble master and 4 followers. Zookeeper nodes that fail have to undergo a special process to be replaced. If they are recovered, then they resume their previous role unless they were the master since a new master is now in place. This node will become an ensemble follower.

- If the master ZK node fails, zookeeper will automatically elect a new master from the remaining ZK follower nodes. This will leave you with a cluster having 4 ZK instances.
- If a follower fails, a new follower is not created on rebuild. If the node that failed is recovered, your ZK instance will return, and you will be back to normal (5 ZK instances). If you are unable to recover the node, the manual node-remove workflow and node replacement will result in a new follower being created. Contact support for assistance.

Types of Failures

The types of failures and the responses to each are summarized here:

- Disk loss
 - Cache disk: This failure is treated the same way as in a normal cluster. Other cache disks in the site service requests, and overall cache capacity is reduced until the failed component is replaced.
 - Persistent disk: This failure is treated the same way as in a normal cluster. After a 2-minute timeout interval, the data from the failed disk is rebuilt using the remaining capacity.
- Node loss
 - 1x: The site will rebuild the failed node after a 2-hour timeout or earlier through manual intervention.
 - Nx: If the node losses are simultaneous and are not all the nodes in a site (e.g., lose 3 nodes out of 5 on a site), the site will remain online, and site failover will not occur. For example, if you have a 3+3 cluster, and you lose 2 nodes on site 1 (regardless of ZK type), then site 1 will still be active, VMs will migrate to the surviving node and the site will still function. There may not be enough resources on the surviving 1 node to restart all the VMs from the 2 failed nodes on the site. In that case, since the host affinity rules are "should run" and not "must run", DRS will restart the VMs that exceed the site capacity at the other site.
- Fabric interconnect loss
 - 1x: The redundant fabric interconnect at the site will handle data until its partner is recovered.
 - 2x: The site will be offline, and site failover will occur.
- Witness loss
 - Nothing happens; the cluster is not affected. Bring the witness back online after it is repaired.
 - Since the Witness is a ZK node, you are guaranteed to survive one node failure at either site (since in worst case that failed node will be ZK as well). This leaves 3 ZK's left. You cannot be guaranteed another failure because if that is a ZK node as well, you no longer have majority ZK surviving. You *may* survive these failures if you get lucky with no additional ZK node failures, but you are not guaranteed this condition. Only worst-case survivability is reported.
- · Accidental deletion of the witness virtual machine

- Restore from backup with identical networking. The cluster will discover the witness and resynchronize.
- Contact the Cisco TAC for a recovery process otherwise.
- Switch loss (single site)
 - 1x: For redundant switches at a site, the partner switch will handle data until the failure is repaired. If there is a single uplink switch per site, site failover will occur.
 - 2x: The site will be offline, and site failover will occur.
- Site loss
 - The site will be offline, and site failover will occur.
- Site link loss

For a scenario in which a fault occurs in the network between the two sites (a cable is damaged, a network port on either site fails, etc.) but the nodes on the two sites are still alive, the following process is implemented:

- When a stretch cluster is created, one site is biased to establish a ZooKeeper master. This is done by assigning a higher node ID. For the purpose of this discussion, the quorum site is site A.
- When the network disconnect occurs, the witness and the nodes of the site that have the ZooKeeper master form the quorum.
- The nodes at the other site (site B) will still stay powered on, and I/O operations from the local IO Visor instance from this site (site B) will not be able to perform write I/O operations successfully, which this will guarantee the isolated site's consistency. The stcli cluster-info command will show these nodes as unavailable in the cluster, even though physically they may be powered on.
- Because site A is the ZooKeeper quorum site, the updates to ZooKeeper will eventually (after a failure-detection timeout) be visible to site B. Eventually, the IO Visor on ESX at site B will see that it needs to talk to a different node, which is the actual I/O primary node (which is in the ZooKeeper quorum at site A). Because there is no network connection, site B will keep retrying those I/O operations and will eventually see "All Paths Down" (APD), assuming that there are still user virtual machines on this site (site B). Your intervention should verify that eventually no virtual machines remain on this site (because they have been failed over to other ESX hosts).
- Virtual machines fail over to the site having the ZooKeeper leader. VMware HA and DRS are responsible for the failover of virtual machines.
- If the network is restored, the nodes of site B that were fenced out will become available again in the cluster. Automatic resynchronization between the sites should occur. However, virtual machine failback is not automatic.

Scenario Walk Through - Failure of Multiple Nodes in a Site

If you have an 8-node cluster (4 nodes on each site) and you lose 2 nodes on site A, what happens to the remaining nodes? Do the VMs still continue to run on site A's remaining nodes?

In this scenario, the remaining nodes on site A restart the VMs that were running on the failed nodes. The site is still online and serving data, however, since the site is locally RF2 (globally RF4) you will have lost some part of the distributed local primary write logs that were running on the 2 nodes that failed. You will also have lost some local persistent data. HX will recognize this and switch the primaries over to Site B. This will incur a read penalty

for these VMs. Note also, depending on how heavily loaded the system is, the surviving nodes on Site A may be either at capacity or unable to restart all of the VMs. In that case, DRS can ignore the affinity rules (HX uses "should" rules for affinity not "must" rules) and restart the VMs on available resources in Site B. If there is capacity in Site A, rebuild will begin and attempt to reestablish local RF2.

This behavior is the same if you have a 10+10 cluster and lose, say, 5 nodes on Site A.

If you were to suffer multiple node failure at each site simultaneously, that would constitute a catastrophic loss and your cluster would be offline pending recovery.

Scenario Walk Through - Failure of a Site

In the event of site failover, operations should continue as intended after the virtual machines from the failed site boot on the surviving site. Virtual machine and IO Visor behavior is as described for site link loss in the preceding discussion. For example:

If you have an 8-node cluster (4 nodes on each site) and you lose site A, vCenter HA initiates a restart all of Site A's VMs on nodes in site B. Failback is not automatic. If sized at maximum capacity (50% per site) then Site B is now running at maximum capacity (100%).

After your downed site has been recovered and communications with the remaining site and the witness have been reestablished, you can move your virtual machines back to their original compute resource (based on site affinity) at the recovered site. Use vMotion for this process so that affinity and proper IO Visor routing occurs after the virtual machines are moved back to their preferred locations. Storage vMotion is not required, since the datastore is mounted on all nodes. Only a migration of the compute resource is needed to re-establish site storage affinity and compute resource parity. In short, during a site failover the affinity rule will not change so that you can quickly migrate back once the impacted site is recovered. However, if you manually Storage vMotion (SVMotion) VMs around outside of a failover event, the affinity rules will automatically be updated to reflect residence in the datastore with the correct rules.

Failure Response Summary

<u>Table 10</u> lists the failure modes discussed previously, with some additional information for particular situations. Note that double, separate catastrophic failures are not considered here (for example, both site loss and witness loss) because such failures always result in a cluster offline status.

Component Failure	Cluster Behavior	Quorum Update	Virtual Machine Restart	Site Status	Cluster Status
Single site single cache disk	Site is online, with diminished cache capacity.	No	No	Online	Online
Single site single persistent disk	Site is online, with diminished capacity, and is rebuilt after 2 minutes using the remaining capacity.	No	No	Online	Online
Single site double cache	Site is online, with diminished cache capacity.	No	No	Online	Online

Table 10. Failure Responses

Component Failure	Cluster Behavior	Quorum Update	Virtual Machine Restart	Site Status	Cluster Status
disk					
Single site double persistent disk	If failure is simultaneous and on different nodes. The site is still online but some VMs will switch primary write logs to the opposite site.	No	No	Online	Online
Single site single node loss	If the failure is not simultaneous on different nodes at different times, then the cluster behaves as with a single-disk failure with reduced capacity.	No	No	Online	Online
Single site multiple node loss	If the failure is simultaneous on the same node.	No	No	Online	Online
Single site single fabric interconnect loss	Node is rebuilt after 2 hours or through manual intervention.	Maybe	Yes	Online	Online
Single site double fabric interconnect loss	Site is online and will restart VMs on surviving nodes in the site.	Maybe	Yes	Online	Online
Double site single fabric interconnect loss	No impact on the site; recover the fabric interconnect.	No	No	Online	Online
Double site double fabric interconnect loss	Site is offline.	Yes	Yes	Offline	Online
Witness loss	No impact on the site; recover the fabric interconnects.	No	No	Online	Online
Single site single switch loss	Both sites are offline.	No	No	Offline	Offline
Single site double switch loss	No impact on the site; recover the witness.	No	No	Online	Online
Double site single switch loss	If redundant switching exists at the site, there is no impact; recover the switch.	No	No	Online	Online

Component Failure	Cluster Behavior	Quorum Update	Virtual Machine Restart	Site Status	Cluster Status
Double site double switch loss	If the site has only a single switch, site is offline.	Yes	Yes	Offline	Online
Site loss	Site is offline.	Yes	Yes	Offline	Online
Site link loss - sites still online and witness is reachable, but site-to- site link is down	If redundant switching exists at the sites, there is no impact; recover the switches.	No	No	Online	Offline
Site loss and disk or node loss on the surviving site in a 2+2 node cluster	If the sites have only a single switch, the sites are offline.	No	No	Offline	Offline
Site loss and disk or node loss on the surviving site in a n+n node cluster	Both sites are offline.	No	No	Offline	Online
Site Loss and witness loss (connectivity, VM failure and so on)	ZooKeeper instance maintains information about cluster groups and forms the quorum. When a site is lost, ZooKeeper communications disappear, site fencing is enforced, and the cluster quorum is redefined. ZooKeeper with DRS rules (affinity, groups, and so on) makes sure that the same virtual machine is never running on both sites simultaneously.	Yes	Yes	Offline	Online

Witness Failure and Restore from Backup

To increase the resiliency of a stretch cluster deployment, many users will back up their witness VM. If the witness were to fail, you can restore from back up (retaining identical network settings). The witness ZK instance will be stale but will re-synchronize with the surviving site(s). As mentioned in the failure scenario section, in the event that the witness fails after a site goes offline and the cluster fails over, the system will be offline. If the witness is subsequently restored from backup and communication is available between witness and either site, the cluster will synchronize zookeeper and come back online. It is also possible in this scenario to maintain a cold witness stand-by VM and promote it when needed. In order to properly integrate with the cluster, it will need to be an identical copy of the original witness and will have to retain the same networking. It will synchronize with the cluster when brought online.

Failure Response Times

Failure response times for disk loss are near-instantaneous. It is the same for active/passive standby links to the FIs. Node failures in a site are they typical node timeout values (approximately 17 seconds). For a site failover to occur, the timeout must happen for multiple nodes at the same time. Since connectivity loss to a site typically involves multiple simultaneous losses, the site time out is at best the same as a node time out. This value can increase due to other factors, such as heavy workloads (affecting ZK updates), latency to the witness, and intersite link latency.

Failure Capacity Considerations and Example

Failure of a node in a site reduces the overall capacity by the free space on the lost node symmetrically; that is, times two. In other words, the cluster capacity in general equals twice the minimum site cluster capacity at the cluster RF (4). This can be expressed as 2[min(site A capacity, site B capacity)]/4.

Take the following example for capacity after node loss on a 5+5 stretch cluster:

siteA/siteB

5 nodes/5 nodes = 10 nodes

At 10TB/node useable that is 100 TB usable total

50TB usable/ 50 TB usable per site

RF 2+2 usable / RF 2+2 usable data protection (RF 4 equivalent)

25TB usable after data protection (100 TB/4)

50 TB/4=12.5TB per site usable.

If site A loses a node, it has dropped by 20% capacity from 12.5 TB to 10 TB. Since the total cluster usable capacity is defined as 2[min(site A capacity, site B capacity)]/4. Site A is now the cluster site minimum at 10 TB (site B is still at 12.5TB) which means the total cluster capacity is now 2(10TB)/4 = 20 TB usable.

In the event of a site failure, the surviving site capacity is the total cluster capacity divided by two, however the remaining capacity is filled in a RF 2 manner until the failed site is recovered so the total free capacity remains constant before and after a site failure. Once the failed site is recovered changes made since the failure are synchronized across the cluster and RF 4 is re-established. Capacity reporting during this transitional interval (site loss, surviving site stabilization, surviving site production usage, failed site recovery) is in flux. The reported capacity will be variable as things like the file system cleaner, rebuilds, and transitions to temporary RF 2 for all VMs take place. In the steady state where the failed site is not recovered in a timely fashion, the surviving capacity will approach RF 2 for the free capacity that was available on the surviving site before the secondary site failure occurred

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 Virtual Desktops 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 Virtual Desktops 1912 LTSR Hosted Shared Desktop with Citrix Virtual Desktops 1912 LTSR 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.

All of these standard Login VSI CVD Testing results for VDI will be evaluated against each failure scenario in the Stretch Cluster. Each test should pass in each failure scenario for this to be considered a successful test.

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 number 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 27. Sample of a VSI Max Response Time Graph, Representing a Normal Test



Figure 28. 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 number 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 represents 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, and so on) 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 number of active users that are logged on the system.

Always a 5 Login VSI response time samples are averaged + 40 percent of the number of "active" sessions. For example, if the active sessions are 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 number 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

Eight Node Cisco HXAF220c-M5 Stretch Cluster

For Citrix Virtual Apps & Desktops, 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 for stretch clustering allows you to determine the cluster N+1 fault tolerance load the sites can successfully support in the event of a server/site 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 ensure that end-user experience is outstanding. Additionally, during steady state, the processor utilization should average no more than 90-95 percent.

¢

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.

Å

The recommended maximum workload for a Cisco HyperFlex cluster configured on Cisco HXAF220c-M5SX with Intel Xeon Gold 6230 scalable family processors and 768GB of RAM for Windows 10 desktops with Office 2016 is 500 virtual desktops.



The recommended maximum workload for a Cisco HyperFlex cluster configured on Cisco HXAF220c-M5SX with Intel Xeon Gold 6230 scalable family processors and 768GB of RAM for Windows Server 2019 RDS desktop sessions with Office 2016 is 500 virtual desktops. 500 Windows 10 VDI Workstations Testing on an 8 Node Cisco HyperFlex Stretch Cluster in Various Failure Scenarios

Figure 29. Test Results for 500 User Sessions with Both Sites Fully Functional



mmary Settings VSimax v4 VSimax v4 Detailed VSimax v4 Detailed Weighted VSimax v4 Scatter UMEM 10 CPU ZLC ZHC NFP NFO NSLD AppStat LogonTimer VSimax v4 Data Raw Data



II SCC	2-4															
Summa SC Gucces	Y Settin C2-4 sfully com	gs VSImax v4 oleted Login VSI	VSImax v	4 Detailed	VSimax v4 Detail worker session	ed Weighted is. VSImax (sy	VSImax v4 Scatter ystem saturation) was	UMEM	IO ed. All L	CPU .ogin VSI	ZLC users co	ZHC mpleted t	NFP he test.	NFO	NSLD	A
Test re	sult revier	N														
50 In t) session otal () s	is were configure essions failed du	ed to be laur iring the test	iched in 2	980 seconds.											
:	0 sess 0 laun	ions was/were r ched sessions fa	iot successf iled to beco	ully launcheo me active	1											
•	500 s	essions were act	ive during th	ne test	Im av threadward)											
	1000000															
Vith 5	600 sess	ions the maximu	m capacity \	/Slmax (v4.1) taskworker	was not read	ched with a Login VS	l baseline (perform	ance sco	re of 87	70				
.ogin V	SI index a	verage score is	958 lowe	r than thresh	iold. It might be p	ossible to laur	nch more sessions in	this configu	uration.							
Baselini	e performa	nce of 870 is	Good													

hx1scip	₽ 3 ⊕ ⊙ £
Cluster > 500 Citrix MCS Persistent Desktops running on Both Sites	1h 1d 1w 1m 6m Dec 10, 2020 - Dec 10, 2020 Last refreshed at: 12/10/2020 4:41:33 PM 🔿 👯
4:13 PM 4:13 PM	422 PM 439 PM
IOP5 12/10/2020 3:41:56 PM - 12/10/2020 4:41:56 PM	Read Max : 1688.1 Min : 0.3 Avg : 60.08 Write Max : 2751.4 Min : 406.4 Avg : 1953.3 Aggregated Max : 3986.9 Min : 406.8 Avg : 2013.38
3.75K 2.5K 1.25K 	
Throughput (MBps) 12/10/2020 3:41:56 PM - 12/10/2020 4:41:56 PM	Read Max : 35.96 Min : 0 Avg : 1.81 • Write Max : 51.83 Min : 1.48 Avg : 34.04 • Aggregated Max : 85.97 Min : 1.5 Avg : 35.84
Latency (msec) 12/10/2020 3:41:56 PM - 12/10/2020 4:41:56 PM	Read Max: 1.5 Min: 0.47 Avg: 0.64 Write Max: 1.58 Min: 0.89 Avg: 1.13 Average Max: 1.51 Min: 0.88 Avg: 1.11
3.43 PM 3.56 PM 12/10/2020 4.02:00 PM PST 4.13 PM	422 PM 430 PM 439 PM 446 PM

同3 ③ ② &

500 Windows 10 VDI Workstations Testing on an 8 Node Cisco HyperFlex Stretch Cluster in Various Failure Scenarios

Figure 30. Test Results for 500 User Sessions with a Witness Failure



Figure 31. Login VSI Analyzer Chart for 500 Windows 10 Citrix VDI Desktops



Summary	Settings	VSImax v4	VSImax v4 Detailed	VSImax v4 Detailed	Weighted	VSImax v4 Scatter	UMEM	10	CPU	ZLC	ZHC	NFP	NFO	NSLD	AppSta
MCS-	-KW-WI	TNESS	FAIL-01a												
Successful	lly complete	ed Login VSI	test with 504 kn	owledgeworker se	ssions. VS	ilmax (system saturatio	n) was no	ot reach	ied.						
-Test resul	it review														
505	sessions w	ere configure	ed to be launched in	2880 seconds.		Mayle			4	4				-	
In total	l 1 sessi	ons failed du	iring the test:		V DI	WOLK	105	a	tes	SUI	an	W	Ith	a	
• 0	0 sessions	was/were r	not successfully launch	ed		fa	leo		Nit	ne	SS				
• 0	0 launcheo	d sessions fa	ailed to become active												
• 5	505 sessio	ons were act	ive during the test												
• 1	1 sessions	got stuck d	uring the test (before \	/SImax threshold) > C	lick Her	e									
With 504	4 sessions	the maximu	m capacity VSImax (v-	.1) knowledgewor	ker was	not reached with a Lo	gin VSI b	aseline	performa	nce score	e of 878	3			

Login VSI index average score is 933 lower than threshold. It might be possible to launch more sessions in this configuration.



	hx1scip		4 🛛 8	3 🛞	© 4
Cluster ×	500 VDI Users using MCS Persistent desktops on 8 healthy cluster nodes	1h 1d 1w. 1m 6m. Jan 07, 2021 - Jan 07, 2021	Last refreshed at: 01/)7/2021 8:48:1:	3 AM 🕂 55
8:04 AM	0.12 AM	8.38 AM 8.38 AM	8:47 AM		
IOPS 01/07/2021 7:48:44 AM - 01/07/2021 8:48:44 AM		Read Max : 122.7 Min : 0.1 Avg : 58 Write Max : 3652.6 Min : 528.1 Avg : 2401.04	Aggregated Max : 37	12.4 Min : 528.4	Avg : 2459.04
2.5K		~~~~~	IOPS	• Write 3,652.6	• Read
1.25К			Throughput (ME	ps) 94.0	1.7
			Latency (msec)	1.4	0.577
Throughput (MBps) 01/07/2021 7:48:44 AM - 01/07/2021 8:	:48:44 AM	Read Max : 3.75 Min : 0 Avg : 1.74 Write Max : 94.03 Min : 2.61 Avg :	50.3 • Aggregated Ma		51 Avg : 52.04
50	~~~~~			\sim	\sim
Latency (msec) 01/07/2021 7:48:44 AM - 01/07/2021 8:48:4	14 AM	 Read Max : 2 Min : 0.33 Avg : 0.63 Write Max : 1.85 Min : 0.85 	Avg : 1.23 • Average I		
1				\sim	\sim
7:56 AM 8:04 AM	8:13 AM 8:21 AM	8-30 AM 8-38 AM 01/07	2021 8:45:00 AM PST		8:54 AM



Figure 32. Test Results for 500 Citrix VDI Desktops with a Single Node Failure



Figure 33. Login VSI Analyzer Chart for 4000 Windows 10 Citrix Virtual Desktops

Login VSI index average score is 915 lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance of 893 is: Good



Figure 34. Test Results for 500 Citrix VDI with a Whole Site Failure

Figure 35. HX Connect Dashboard with Site A in a Failed State

			hx1scip		ې د 🖬 ۹ 🗛	⊜5 ⊙ ⊙
\bigcirc	OPERATIONAL STATUS			① Cluster License not re	gistered	
	RESILIENCY HEALTH Warning ①				No Node failure can be tolerated	8
Ð	CAPACITY 9.6 TB	3.7% 363,7 GB Used	9,3 TB Free		Compression Deduplication	54%
	NODES 8	Site-B 4 HXAF220C-M55X Converged Site-B 4 HXAF220C-M55X Converged				
	VIRTUAL MACHINES	POWERED ON	SUSPENDED	POWERED OFF		
IOPS Les	t 1 hour				• Read Max : 22298 Min : 0.1 Avg : 1809.9 • Write M	ex : 4436.1 Min : 261.7 Avg : 1904.32
22.5K 158 7.5K					M	
Through	put (MBps) Last 1 hour				+ Read Max : 780.13 Min : 0 Avg : 50.47 + Writ	e Max : 114.31 Min : 0.98 Avg : 35.48
675 450 225					M	
Latency	(msec) Last 1 hour				 Read Max : 2 Min : 0 Avg : 0.59 	Write Max : 3.82 Min : 0.71 Avg : 1.27
3 2 3	~~~~			AA	Activate Go to Setter	Windows gs to activate Windows



Figure 36. Login VSI Analyzer Chart for 4000 Windows 10 Citrix Virtual Desktops using MCS Persistent
ESX Host Performance Counters

When running a VMware ESXi environment for our Citrix Virtual Desktop workloads, it's important to monitor a few key performance counters to ensure the best end-user experience. CPU Performance: With VMware ESXi, using esxtop, our main counter is % Core Utilization.



CPU for complete failure of Site-A (Site-B hosts running ALL Virtual Desktops)



\$2:53.0 \$3:47.0 1.26.0 3.18.0 4.14.0 5.09.0 6.04.0 6.59.0 7.54.0 8:49.0 8:22.0 4:16.0 5:11.0 4:03.0 1.42.0 2:52.0 3:47.0 4:42.0 3:19.0 1:15.0 :53.0 :45.0 3:33.0 1:03.0 7:45.0 8:41.0 1.28.0 5:06.0 1:41.0 4:28.0 22.0 33.6 3:07. 1.58 1-50

Cluster v In 1d 1W 1m 6m Jan 04, 2021-Jan 05, 2021 Last refreshed at: 01/05/2021 3: Site A Failure Image: Site A Failure Image: Site A Failure 1005 01/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM 128.4 M S42.4 M 908.4 M 128.4 PM 1005 01/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM • Read Max: 31721 65 Min: 0 Avg: 4734.41 • Write Max: 3532.6 Min: 349.8 Avg: 1894.1 • Aggregated Max: 35254.25 Min: 349.8 Avg: 1894.1 1005 01/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM • Read Max: 31721 65 Min: 0 Avg: 96.22 • Write Max: 65.13 Min: 1.37 Avg: 35.13 • Aggregated Max: 62.57 28 Min: 24 Avgregated Max: 62.57 28 Min: 24 Avg: 96.22	2:28 PM 🕂 💆
226 PM 125 ENI 2.18 AM 5.42 AM 908 AM 1234 PM 100 50 10/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM • Read Max: 31721 65 Min: 0 Avg: 4734.41 • Write Max: 3532.6 Min: 349.8 Avg: 1894.1 • Aggregated Max: 35254.25 Min: 3 30x -	
OPS 01/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM • Read Max: 35254 35 Min: 349 & Avg: 1594.1 • Aggregated Max: 35254 35 Min: 3 30x	
30К 20К 10К Тhroughput (MBps) 01/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM -	3.3 Avg : 6629.13
Throughput (MBps) 01/04/2021 3:52:39 PM - 01/05/2021 3	
	: 1.4 Avg : 131.36
500	
Latency (msec) 01/04/2021 3:52:39 PM - 01/05/2021 3:52:39 PM + 01/05/2021 3:52:39 PM + Average Max : 1.6	Min : 0 Avg : 0.9

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.

This solutions offers flexibility with creating site resiliency and adds an extra high availability component to ensure VDI workload resiliency.

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 hyperconvergence licensing is required for those nodes.

Delivering responsive, resilient, high-performance Citrix Virtual Desktops provisioned Microsoft Windows 10 Virtual Machines and Microsoft Windows Server for hosted Apps or desktops has many advantages for desktop virtualization administrators.

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 Author

Jeff Nichols, Technical Marketing Manager, 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, Virtual Desktops, Virtual Apps 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.

Feedback

For comments and suggestions about this guide and related guides, join the discussion on <u>Cisco Community</u> at <u>https://cs.co/en-cvds</u>.

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)