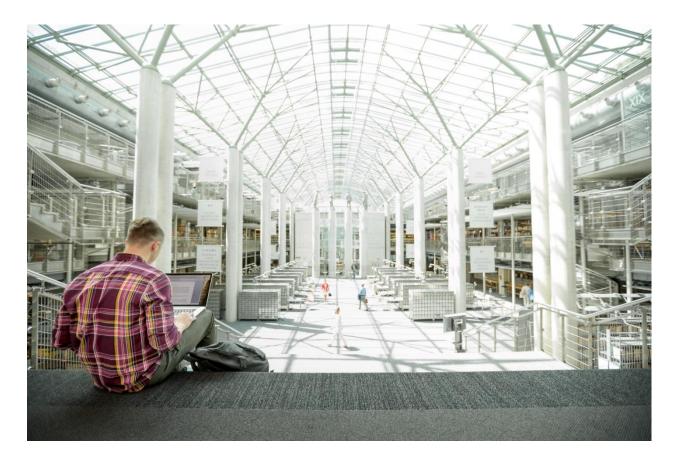
cisco.



Cisco HyperFlex Hyperconverged System with VMware Horizon 7

Design and Deployment of Cisco HyperFlex for Virtual Desktop Infrastructure with VMware Horizon 7

Last Updated: February 8, 2017



About Cisco Validated Designs

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2017 Cisco Systems, Inc. All rights reserved.

Table of Contents

About Cisco Validated Designs	2
Executive Summary	6
Solution Overview	7
Introduction	7
Audience	7
Purpose of this Document	7
What's New?	7
Solution Summary	
Cisco Desktop Virtualization Solutions: Data Center	11
The Evolving Workplace	11
Cisco Desktop Virtualization Focus	
Use Cases	14
Physical Topology	15
Fabric Interconnects	17
Cisco UCS B-Series Blade Servers	
Configuration Guidelines	
Solution Design	
Cisco Unified Computing System	
Cisco Unified Computing System Components	
Cisco Ucs 5108 Blade Chassis	
VMware vSphere 6.0	
VMware ESXi 6.0 Hypervisor	
VMware Horizon	
Advantages of Using VMware Horizon	
What are VMware RDS Hosted Sessions?	
Farms, RDS Hosts, Desktop and Application Pools	
Cisco HyperFlex Data Platform	45
Architecture and Design of VMware Horizon on Cisco Unified Computing System and Ci Fundamentals	
Understanding Applications and Data	
Project Planning and Solution Sizing Sample Questions	
Desktop Virtualization Design Fundamentals	
VMware Horizon Design Fundamentals	
Horizon VDI Pool and RDSH Servers Pool	

Designing a VMware Horizon Environment for Various Workload Types	53
Deployment Hardware and Software	
Products Deployed	
Hardware Deployed	
Software Deployed	
Logical Architecture	
VLANs	
Jumbo Frames	
VMware Clusters	
ESXi Host Design	60
Solution Configuration	
Cisco UCS Compute Platform	
Physical Infrastructure	
Cisco Unified Computing System Configuration	72
Deploy and Configure HyperFlex Data Platform	73
Prerequisites	73
Deploy Cisco HyperFlex Data Platform Installer VM	77
Cisco HyperFlex Cluster Configuration	
Building the Virtual Machines and Environment for Workload Testing	
Horizon 7 Infrastructure Components Installation	
Install VMware Horizon Composer Server	
Install Horizon Connection/Replica Servers	
Create a Microsoft Management Console Certificate Request	
Configure the Horizon 7 Environment	
Configure Event Database	131
Configure Horizon 7 Licenses	
Configure vCenter	
Master Image Creation for Tested Horizon Deployment Types	
Prepare Microsoft Windows 10 and Server 2012 R2 with Microsoft Office 2016	
Optimization of Base Windows 10 or Server 2012 R2 Guest OS	141
Virtual Desktop Agent Software Installation for Horizon	141
Install Additional Software	
Create a Native Snapshot for Automated Desktop Pool Creation	
Create Customization Specification for Virtual Desktops	
VMware Horizon Farm and Pool Creation	

RDSH Farm Creation	162
Create the Horizon 7 RDS Published Desktop Pool	173
VMware Horizon Linked-Clone Windows 10 Desktop Pool Creation	179
VMware Horizon Instant-Clone Windows 10 Desktop Pool Creation	192
VMware Horizon Persistent Windows 10 Desktop Pool Creation	203
Test Setup and Configurations	216
Testing Methodology and Success Criteria	217
Testing Procedure	217
Pre-Test Setup for Testing	217
Test Run Protocol	218
Success Criteria	219
Test Results	224
Boot Storms	224
Recommended Maximum Workload and Configuration Guidelines for an Eight Node HX220c-M4S Rack Server Hyp Cluster	
	225
Cluster	225 226
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster	225 226 229
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster 1000 Windows 10 Linked-clone Desktop Pool testing on eight node Cisco HyperFlex Cluster	225 226 229 233
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster	225 226 229 233 236
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster 1000 Windows 10 Linked-clone Desktop Pool testing on eight node Cisco HyperFlex Cluster 1000 Windows 10 Instant-clone Desktop Pool testing on Eight Node Cisco HyperFlex Cluster 1000 Windows 10 Full Clone Desktop Pool Testing on Eight Node Cisco HyperFlex Cluster	225 226 229 233 236 240
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster 1000 Windows 10 Linked-clone Desktop Pool testing on eight node Cisco HyperFlex Cluster 1000 Windows 10 Instant-clone Desktop Pool testing on Eight Node Cisco HyperFlex Cluster 1000 Windows 10 Full Clone Desktop Pool Testing on Eight Node Cisco HyperFlex Cluster Summary	225 226 229 233 236 240 241
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster	225 226 229 233 236 240 241 241
Cluster RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster	225 226 229 233 236 240 241 241 242
Cluster	225 226 229 233 236 240 241 241 241 242 242



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 software-defined computing in the form of Cisco HyperFlex HX-Series Nodes, software-defined storage with the powerful Cisco HyperFlex HX Data Platform, and software-defined networking with the Cisco UCS fabric that integrates smoothly with Cisco® Application Centric Infrastructure (Cisco ACI™).

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 a 1200 seat workload on an 8node Cisco HyperFlex system. We provide deployment guidance and performance data for VMware Horizon 7 deployed Microsoft Windows 10 with Office 2016 Linked-Clone, Instant-Clone and Persistent virtual desktops as well as Windows Server 2012 R2 RDS server-based sessions on vSphere 6. The solution is a pre-integrated, best-practice data center architecture built on the Cisco Unified Computing System (UCS), the Cisco Nexus® 9000 family of switches and Cisco HyperFlex Data Platform software version 1.8.1b.

The solution payload is 100 percent virtualized on Cisco HyperFlex HX220c-M4S rack server booting via onboard Flex-Flash controller SD cards running VMware vSphere 6.0 U2 patch03 hypervisor. The virtual desktops are configured with VMware Horizon 7 which incorporates both traditional persistent and nonpersistent virtual Windows 7/8/10 desktops, hosted applications and remote desktop service (RDS) server 2008 R2 or server 2012 R2 based desktops. The solution provides unparalleled scale and management simplicity. VMware Horizon linked-clone or instant-clone floating assignment Windows 10 desktops (1000,) full clone desktops (1000) or RDSH server based desktops (1200) can be provisioned on an eight node Cisco HyperFlex cluster. Where applicable, this document provides best practice recommendations and sizing guidelines for customer deployment of this solution.

The solution boots 1000 virtual desktops or the RDSH virtual server machines in 5 minutes or less, insuring that users will not experience delays in accessing their virtual workspace on HyperFlex.

The solution provides outstanding virtual desktop end user experience as measured by the Login VSI 4.1 Knowledge Worker workload running in benchmark mode. Average end-user response times for all tested delivery methods is under 1 second, representing the best performance in the industry.

Solution Overview

Introduction

A 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 Hyper Converged Solution can be quickly deployed, thereby increasing agility and reducing costs. Cisco HyperFlex uses best of breed storage, server and network components to serve as the foundation for desktop virtualization workloads, enabling efficient architectural designs that can be quickly and confidently deployed and scaled out.

Audience

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

Purpose of this Document

This document provides a step by step design, configuration and implementation guide for the Cisco Validated Design for a Cisco HyperFlex system running four different VMware Horizon 7 workloads with Cisco UCS 6248UP Fabric Interconnects and Cisco Nexus 9300 series switches.

What's New?

This is the first Cisco Validated Design with Cisco HyperFlex system running Virtual Desktop Infrastructure. It incorporates the following features:

- Validation of Cisco Nexus 9000 with Cisco HyperFlex
- Support for the Cisco UCS 3.1(2) release and Cisco HyperFlex v1.8.1
- VMware vSphere 6.0 U2 Hypervisor
- VMware Horizon 7 Linked Clones, Instant Clones, Persistent Desktops and RDSH shared server sessions

The data center market segment is shifting toward heavily virtualized private, hybrid and public cloud computing models running on industry-standard systems. These environments require uniform design points that can be repeated for ease if management and scalability.

These factors have led to the need predesigned computing, networking and storage building blocks optimized to lower the initial design cost, simply management, and enable horizontal scalability and high levels of utilization.

The use cases include:

• Enterprise Data Center (small failure domains)

- Service Provider Data Center (small failure domains)
- Commercial Data Center
- Remote Office/Branch Office
- SMB Standalone Deployments

Solution Summary

This Cisco Validated Design prescribes a defined set of hardware and software that serves as an integrated foundation for both Horizon Microsoft Windows 10 virtual desktops and Horizon RDSH server desktop sessions based on Microsoft Server 2012 R2. The mixed workload solution includes Cisco HyperFlex hardware and Data Platform software, Cisco Nexus® switches, the Cisco Unified Computing System (Cisco UCS®), VMware Horizon and VMware vSphere software in a single package. The design is efficient enough that the networking, computing, and storage can fit in a 12 rack unit footprint in a single rack. Port density on the Cisco Nexus switches and Cisco UCS Fabric Interconnects enables the networking components to accommodate multiple HyperFlex clusters in a single Cisco UCS domain.

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

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

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

- More power, same size. Cisco HX-series rack server with dual 14-core 2.6 GHz Intel Xeon (E5-2690v4) processors and 512GB of memory for VMware Horizon supports more virtual desktop workloads than the previously released generation processors on the same hardware. The Intel Xeon E5-2690 v4 14-core processors used in this study provided a balance between increased per-server capacity and cost.
- Fault-tolerance with high availability built into the design. The various designs are based on multiple Cisco HX-Series rack server for virtualized desktop and infrastructure workloads. The design provides N+1 server fault tolerance for virtual desktops, hosted shared desktops and infrastructure services.
- Stress-tested to the limits during aggressive boot scenario. The 1000 user mixed hosted virtual desktop and 1200 user hosted shared desktop environment booted and registered with the Horizon 7 in under 5 minutes, providing our customers with an extremely fast, reliable cold-start desktop virtualization system.
- Stress-tested to the limits during simulated login storms. All 1000 or 1200 users logged in and started running workloads up to steady state in 48-minutes without overwhelming the processors, exhausting memory or exhausting the storage subsystems, providing customers with a desktop virtualization system that can easily handle the most demanding login and startup storms.
- Ultra-condensed computing for the datacenter. The rack space required to support the initial 1000 or 1200 user system is 12 rack units, including Cisco Nexus Switching and Cisco Fabric interconnects. Incremental Cisco HyperFlex clusters can be added in 8 rack unit groups to add additional 1000 user capability, conserving valuable data center floor space.

- 100 percent virtualized: This CVD presents a validated design that is 100 percent virtualized on VMware ESXi 6.0. All of the virtual desktops, user data, profiles, and supporting infrastructure components, including Active Directory, SQL Servers, VMware Horizon components, Horizon VDI desktops and RDSH servers were hosted as virtual machines. This provides customers with complete flexibility for maintenance and capacity additions because the entire system runs on the Cisco HyperFlex hyper-converged infrastructure with stateless Cisco UCS HX-series servers. (Infrastructure VMs were hosted on two Cisco UCS C220 Rack Servers outside of the HX cluster to deliver the highest capacity and best economics for the solution.)
- Cisco datacenter management: Cisco maintains industry leadership with the new Cisco UCS Manager 3.1(2) software that simplifies scaling, guarantees consistency, and eases maintenance. Cisco's ongoing development efforts with Cisco UCS Manager, Cisco UCS Central, and Cisco UCS Director insure that customer environments are consistent locally, across Cisco UCS Domains and across the globe, our software suite offers increasingly simplified operational and deployment management, and it continues to widen the span of control for customer organizations' subject matter experts in compute, storage and network.
- Cisco 10G Fabric: Our 10G unified fabric story gets additional validation on 6200 Series Fabric Interconnects as Cisco runs more challenging workload testing, while maintaining unsurpassed user response times.
- Cisco HyperFlex storage performance: Cisco HyperFlex provides industry-leading hyper converged storage performance that efficiently handles the most demanding I/O bursts (for example, login storms), high write throughput at low latency, delivers simple and flexible business continuity and helps reduce storage cost per desktop.
- Cisco HyperFlex agility: Cisco HyperFlex System enables users to seamlessly add, upgrade or remove storage from the infrastructure to meet the needs of the virtual desktops.
- Cisco HyperFlex vCenter integration: Cisco HyperFlex plugin for VMware vSphere provides easybutton automation for key storage tasks such as storage provisioning and storage resize, cluster health status and performance monitoring directly from the VCenter web client in a single pane of glass. Experienced vCenter administrators have a near zero learning curve when HyperFlex is introduced into the environment.
- VMware Horizon 7 advantage: VMware Horizon 7 follows a new unified product architecture that supports both hosted-shared desktops and applications (RDS) and complete virtual desktops (VDI). This new Horizon release simplifies tasks associated with large-scale VDI management. This modular solution supports seamless delivery of Windows apps and desktops as the number of user increase. In addition, PCoIP and Blast extreme enhancements help to optimize performance and improve the user experience across a variety of endpoint device types, from workstations to mobile devices including laptops, tablets, and smartphones.
- Optimized for performance and scale. For hosted shared desktop sessions, the best performance was achieved when the number of vCPUs assigned to the Horizon 7 RDSH virtual machines did not exceed the number of hyper-threaded (logical) cores available on the server. In other words, maximum performance is obtained when not overcommitting the CPU resources for the virtual machines running virtualized RDS systems.

Provisioning desktop machines made easy: VMware Horizon 7 provisions hosted virtual desktops as well as hosted shared desktop virtual machines for this solution using a single method for both, the "Automated floating assignment desktop pool". Persistent desktops were handled in same the unified Horizon 7 administrative console. Horizon 7 introduces a new provisioning technique for non-persistent virtual desktops called "Instant-clone." The new method greatly reduces the amount of life-cycle spend and the maintenance windows for the guest OS.

Cisco Desktop Virtualization Solutions: Data Center

The Evolving Workplace

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

This workforce is also increasingly mobile, conducting business in traditional offices, conference rooms across the enterprise campus, home offices, on the road, in hotels, and at the local coffee shop. This workforce wants to use a growing array of client computing and mobile devices that they can choose based on personal preference. These trends are increasing pressure on IT to ensure protection of corporate data and prevent data leakage or loss through any combination of user, endpoint device, and desktop access scenarios (Figure 1).

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

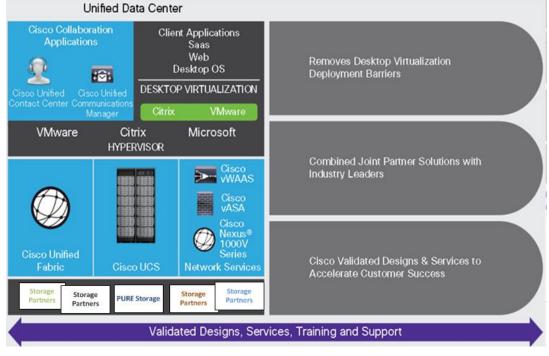


Figure 1 Cisco Data Center Partner Collaboration

Some of the key drivers for desktop virtualization are increased data security and reduced TCO through increased control and reduced management costs.

Cisco Desktop Virtualization Focus

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

Simplified

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

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

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

Secure

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

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

Scalable

Growth of a desktop virtualization solution is all but inevitable, so a solution must be able to scale, and scale predictably, with that growth. The Cisco Desktop Virtualization Solutions support high virtual-desktop density

(desktops per server), and additional servers scale with near-linear performance. Cisco data center infrastructure provides a flexible platform for growth and improves business agility. Cisco UCS Manager service profiles allow on-demand desktop provisioning and make it just as easy to deploy dozens of desktops as it is to deploy thousands of desktops.

Cisco HyperFlex servers provide near-linear performance and scale. Cisco UCS implements the patented Cisco Extended Memory Technology to offer large memory footprints with fewer sockets (with scalability to up to 1 terabyte (TB) of memory with 2- and 4-socket servers). Using unified fabric technology as a building block, Cisco UCS server aggregate bandwidth can scale to up to 80 Gbps per server, and the northbound Cisco UCS fabric interconnect can output 2 terabits per second (Tbps) at line rate, helping prevent desktop virtualization I/O and memory bottlenecks. Cisco UCS, with its high-performance, low-latency unified fabric-based networking architecture, supports high volumes of virtual desktop traffic, including high-resolution video and communications traffic. In addition, Cisco HyperFlex helps maintain data availability and optimal performance during boot and login storms as part of the Cisco Desktop Virtualization Solutions. Recent Cisco Validated Designs based on VMware Horizon, Cisco HyperFlex solutions have demonstrated scalability and performance, with up to 1000 hosted virtual desktops or 1200 hosted shared desktops up and running in 5 minutes.

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

Savings and Success

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

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

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

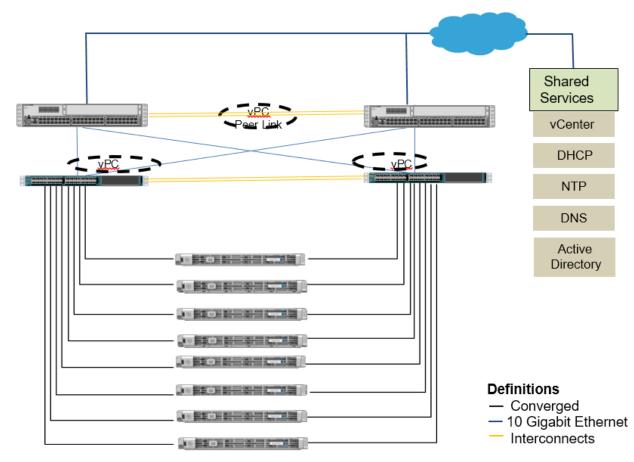
The ultimate measure of desktop virtualization for any end user is a great experience. Cisco HyperFlex delivers class-leading performance with sub-second base line response times and index average response times at full load of just over one second.

Use Cases

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

Figure 2 shows the VMware Horizon 7 on vSphere 6 built on Cisco Validated Design components and the network connections. The reference architecture reinforces the "wire-once" strategy, because as additional storage is added to the architecture, no re-cabling is required from the hosts to the Cisco UCS fabric interconnect.

Figure 2 Architecture



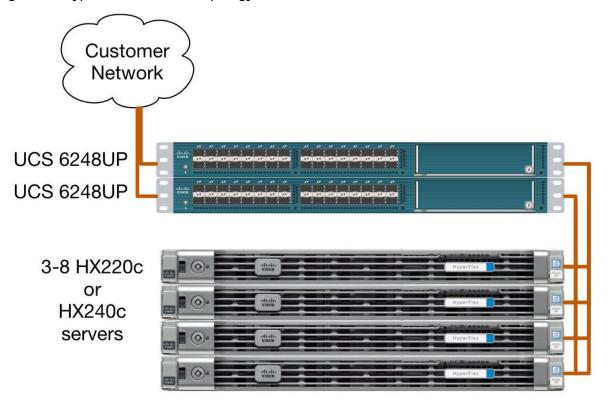
Physical Topology

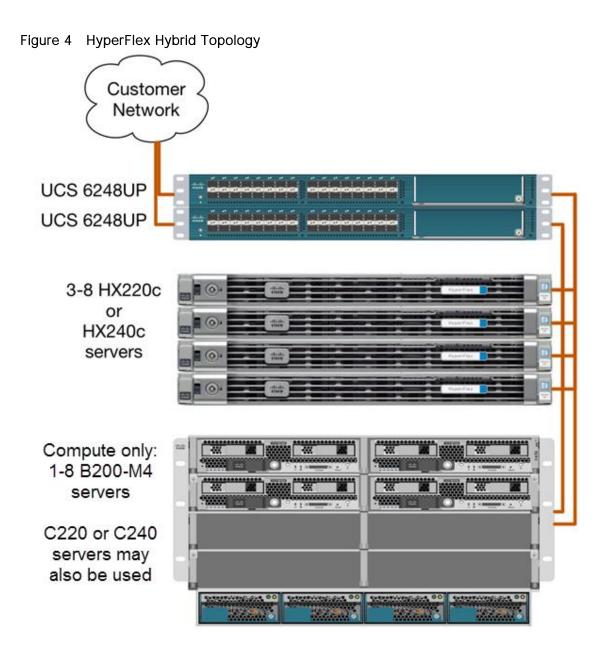
The Cisco HyperFlex system is composed of a pair of Cisco UCS 6248UP Fabric Interconnects, along with up to 8 HX-Series rack mount servers per cluster. In addition, up to 8 compute only servers can also be added per cluster. Adding Cisco UCS 5108 Blade chassis allows use of Cisco UCS B200-M4 blade servers for additional compute resources in a hybrid cluster design. Cisco UCS C240 and C220 servers can also be used for additional compute resources. Up to 8 separate HX clusters can be installed under a single pair of Fabric Interconnects. The Fabric Interconnects both connect to every HX-Series rack mount server, and both connect to every Cisco UCS 5108 blade chassis. Upstream network connections, also referred to as **"northbound" network connections are made from the Fabric Interconnects to the customer datacenter** network at the time of installation.

For this study, we uplinked the Cisco 6248UP Fabric Interconnects to Cisco Nexus 9372PX switches.

The Figure 3 and Figure 4 illustrate the hyperconverged and hybrid hyperconverged, plus compute only topologies.

Figure 3 HyperFlex Standard Topology





Fabric Interconnects

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

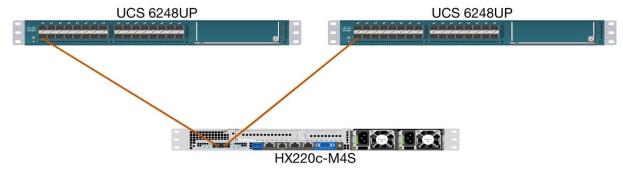
Fabric Interconnects have the following ports, which must be connected for proper management of the Cisco UCS domain:

- Mgmt: A 10/100/1000 Mbps port for managing the Fabric Interconnect and the Cisco UCS domain via GUI and CLI tools. Also used by remote KVM, IPMI and SoL sessions to the managed servers within the domain. This is typically connected to the customer management network.
- L1: A cross connect port for forming the Cisco UCS management cluster. This is connected directly to the L1 port of the paired Fabric Interconnect using a standard CAT5 or CAT6 Ethernet cable with RJ45 plugs. It is not necessary to connect this to a switch or hub.
- L2: A cross connect port for forming the Cisco UCS management cluster. This is connected directly to the L2 port of the paired Fabric Interconnect using a standard CAT5 or CAT6 Ethernet cable with RJ45 plugs. It is not necessary to connect this to a switch or hub.
- Console: An RJ45 serial port for direct console access to the Fabric Interconnect. Typically used during the initial FI setup process with the included serial to RJ45 adapter cable. This can also be plugged into a terminal aggregator or remote console server device.

HX-Series Rack Mount Servers

The HX-Series converged servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode. This option enables Cisco UCS Manager to manage the HX-Series rack-mount Servers using a single cable for both management traffic and data traffic. Both the HX220c-M4S and HX240c-M4SX servers are configured with the Cisco VIC 1227 network interface card (NIC) installed in a modular LAN on motherboard (MLOM) slot, which has dual 10 Gigabit Ethernet (GbE) ports. The standard and redundant connection practice is to connect port 1 of the VIC 1227 to a port on FI A, and port 2 of the VIC 1227 to a port on FI B (Figure 5). Failure to follow this cabling practice can lead to errors, discovery failures, and loss of redundant connectivity.

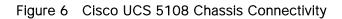


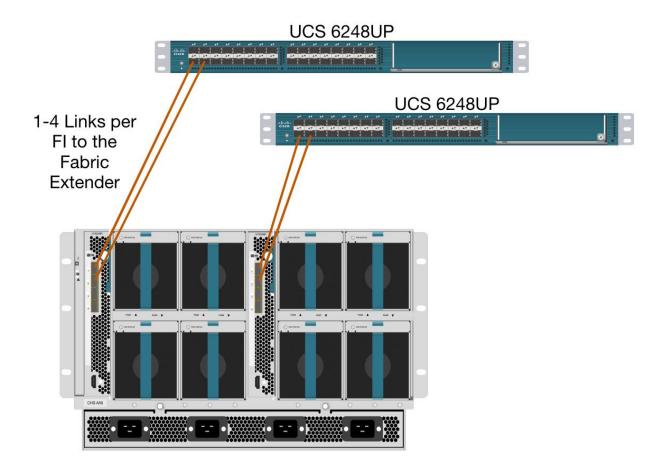


Cisco UCS B-Series Blade Servers

Hybrid HyperFlex clusters also incorporate 1-8 Cisco UCS B200-M4 blade servers for additional compute capacity. Like all other Cisco UCS B-series blade servers, the Cisco UCS B200-M4 must be installed within a Cisco UCS 5108 blade chassis. The blade chassis comes populated with 1-4 power supplies, and 8 modular cooling fans. In the rear of the chassis are two bays for installation of Cisco Fabric Extenders. The Fabric Extenders (also commonly called IO Modules, or IOMs) connect the chassis to the Fabric Interconnects. Internally, the Fabric Extenders connect to the Cisco VIC 1340 card installed in each blade server across the chassis backplane. The standard connection practice is to connect 1-4 10 GbE links from the left side IOM, or IOM 1, to FI A, and to connect the same number of 10 GbE links from the right side IOM,

or IOM 2, to FI B (Figure 6). All other cabling configurations are invalid, and can lead to errors, discovery failures, and loss of redundant connectivity.





Logical Network Design

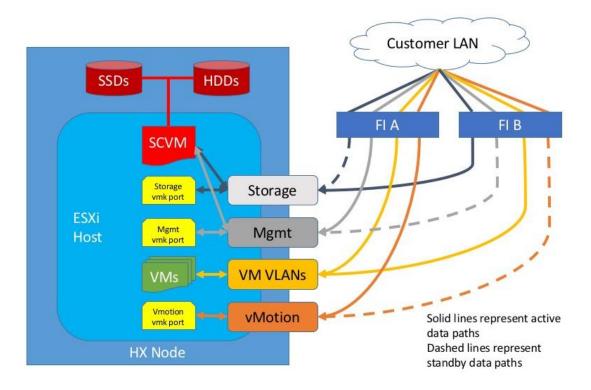
The Cisco HyperFlex system has communication pathways that fall into four defined zones (Error! Reference source not found.):

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

- Storage Controller VM management interfaces.
- A roaming HX cluster management interface.
- VM Zone: This zone comprises the connections needed to service network IO to the guest VMs that will
 run inside the HyperFlex hyperconverged system. This zone typically contains multiple VLANs, that are
 trunked to the Cisco UCS Fabric Interconnects via the network uplinks, and tagged with 802.10 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 for 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 storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa.

Refer to the following figure for an illustration of the logical network design:

Figure 7 Logical Network Design



The reference hardware configuration includes:

- Two Cisco Nexus 9372PX switches
- Two Cisco UCS 6248UP fabric interconnects
- Eight Cisco HX-series Rack server running HyperFlex data platform version 1.8.1b

For desktop virtualization, the deployment includes VMware Horizon 7 running on VMware vSphere 6. The design is intended to provide a large scale building block for both RDSH and persistent/non-persistent desktops with following density per eight node configuration:

- 1200 Horizon 7 RDSH server desktop sessions
- 1000 Horizon 7 Windows 10 non-persistent virtual desktops
- 1000 Horizon 7 Windows 10 persistent virtual desktops

All of the Windows 10 virtual desktops were provisioned with 2GB of memory for this study. Typically, persistent desktop users may desire more memory. If 3GB or more of memory is needed, the third memory channel on the Cisco HX220c M4 servers should be populated.

Data provided here will allow customers to run RDSH server sessions and VDI desktops to suit their environment. For example, additional Cisco HX server can be deployed in compute-only manner to increase compute capacity or additional drives can be added in existing server to improve I/O capability and throughput, and special hardware or software features can be added to introduce new features. This

document guides you through the low-level steps for deploying the base architecture, as shown in Figure 1. These procedures covers everything from physical cabling to network, compute and storage device configurations.

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration for a Cisco Validated Design for various type of Virtual Desktop workloads on Cisco HyperFlex. Configuration guidelines are provided that refer to which redundant component is being configured with each step. For example, Cisco Nexus A or Cisco Nexus B identifies a member in the pair of Cisco Nexus switches that are configured. Cisco UCS 6248UP Fabric Interconnects are similarly identified. Additionally, this document details the steps for provisioning multiple Cisco UCS and HyperFlex hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-RDSH-01, VM-Host-VDI-01 and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure.

Solution Design

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

Cisco Unified Computing System

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

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

Cisco Unified Computing System Components

The main components of Cisco UCS are:

- Compute: The system is based on an entirely new class of computing system that incorporates blade, rack and hyperconverged servers based on Intel® Xeon® processor E5-2600/4600 v4 and E7-2800 v4 family CPUs.
- Network: The system is integrated on a low-latency, lossless, 10-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing (HPC) networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables needed, and by decreasing the power and cooling requirements.
- Virtualization: The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- Storage: The Cisco HyperFlex rack servers provide high performance, resilient storage using the powerful HX Data Platform software. Customers can deploy as few as two nodes (replication factor 2) or three nodes (replication factor 3,) depending on their fault tolerance requirements. These nodes form a HyperFlex storage and compute cluster. The onboard storage of each node is aggregated at the cluster level and automatically shared with all of the nodes. Storage resources are managed from the familiar VMware vCenter web client, extending the capability of vCenter administrators.
- Management: Cisco UCS uniquely integrates all system components, enabling the entire solution to be managed as a single entity by Cisco UCS Manager. The manager has an intuitive GUI, a CLI, and a robust API for managing all system configuration processes and operations.

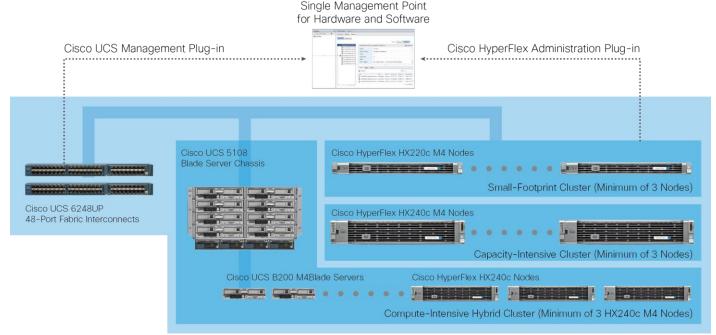


Figure 8 Cisco HyperFlex Family Overview

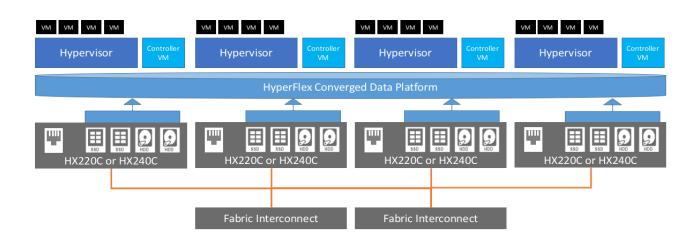
Cisco UCS is designed to deliver:

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

Cisco UCS Manager provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System across multiple chassis, rack servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a commandline interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager Functions.

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

Figure 9 HyperFlex System Overview



Cisco UCS Fabric Interconnect

The Cisco UCS 6200 Series Fabric Interconnects are a core part of Cisco UCS, providing both network connectivity and management capabilities for the system. The Cisco UCS 6200 Series offers line-rate, low-latency, lossless 10 Gigabit Ethernet, FCoE, and Fibre Channel functions.

The fabric interconnects provide the management and communication backbone for the Cisco UCS B-Series Blade Servers, Cisco UCS C-Series and HX-Series rack servers and Cisco UCS 5100 Series Blade Server Chassis. All servers, attached to the fabric interconnects become part of a single, highly available management domain. In addition, by supporting unified fabric, the Cisco UCS 6200 Series provides both LAN and SAN connectivity for all blades in the domain.

For networking, the Cisco UCS 6200 Series uses a cut-through architecture, supporting deterministic, lowlatency, line-rate 10 Gigabit Ethernet on all ports, 1-terabit (Tb) switching capacity, and 160 Gbps of bandwidth per chassis, independent of packet size and enabled services. The product series supports Cisco low-latency, lossless, 10 Gigabit Ethernet unified network fabric capabilities, increasing the reliability, efficiency, and scalability of Ethernet networks. The fabric interconnects support multiple traffic classes over a lossless Ethernet fabric, from the blade server through the interconnect. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

Figure 10 Cisco UCS 6200 Series Fabric Interconnect



Cisco HyperFlex HX-Series Nodes

A HyperFlex cluster requires a minimum of three HX-Series nodes (with disk storage). Data is replicated across at least two of these nodes, and a third node is required for continuous operation in the event of a 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 up to **the platform's physical capacity of spinning disks for maximum data capacity. At first rele**ase, we offer three tested cluster configurations:

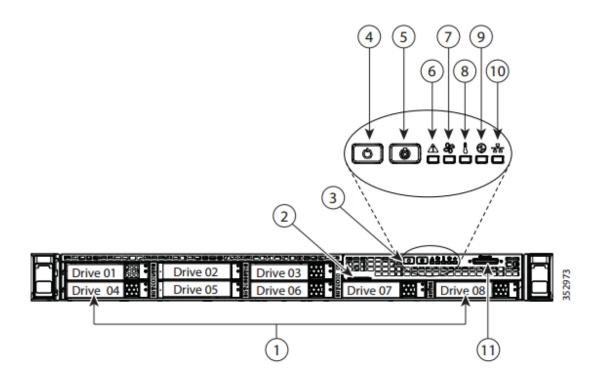
Cisco UCS HX220c-M4S Rack Server

The Cisco UCS HX220c-M4S Rack Server (Figure 11 and Figure 12) is a density-optimized, half-width blade server that supports two CPU sockets for Intel Xeon processor E5-2600 v4 series CPUs and up to 24 DDR4 DIMMs. It supports one modular LAN-on-motherboard (LOM) dedicated slot for a Cisco virtual interface card (VIC) and one mezzanine adapter. In additions, the Cisco UCS B200 M4 supports an optional storage module that accommodates up to two SAS or SATA hard disk drives (HDDs) or solid-state disk (SSD) drives. You can configure up to eight Cisco UCS HX220c-M4S Rack Server in a single HX cluster.

http://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/datasheet-c78-736817.pdf



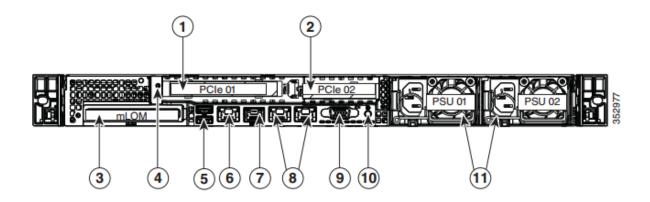
Figure 11 Cisco UCS HX220c-M4S Rack Server Front View



1	Drives	7	Fan status LED
	 Up to 6 x 1.2 TB SAS HDDs (for data) Drives 03 through 08 		
	 1 x 120 GB SATA SSD drive (for SDS logs) Drive 01 		
	 1 x 480 GB SATA SSD drive (for caching) Drive 02 		
2	Pull-out asset tag	8	Temperature status LED
3	Operations panel buttons and LEDs	9	Power supply status LED
4	Power button/Power status LED	10	Network link activity LED
5	Unit identification button/LED	11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector) ¹
6	System status LED	-	-

Figure 12 Cisco UCS B200 M4 Rear View





1	PCIe riser 1/slot 1	7	Serial port (RJ-45 connector) ¹
2	PCIe riser 2/slot 2	8	Two embedded (on the motherboard) Intel i350 GbE Ethernet controller ports (LAN1, LAN2)
3	Modular LAN-on-motherboard (mLOM) card slot	9	VGA video port (DB-15)
4	Grounding-lug hole (for DC power supplies)	10	Rear unit identification button/LED
5	USB 3.0 ports (two)	11	Power supplies (up to two, redundant as 1+1)
6	1-Gb Ethernet dedicated management port	-	-

Cisco UCS combines Cisco UCS B-Series Blade Servers and C-Series Rack Servers with networking and storage access into a single converged system with simplified management, greater cost efficiency and agility, and increased visibility and control. The Cisco UCS HX-Series Rack Servers are one of the newest servers in the Cisco UCS portfolio.

The Cisco UCS HX220c-M4S delivers performance, flexibility, and optimization for data centers and remote sites. This enterprise-class server offers market-leading performance, versatility, and density without compromise for workloads ranging from web infrastructure to distributed databases. The Cisco UCS HX220c-M4S can quickly deploy stateless physical and virtual workloads with the programmable ease of use of the Cisco UCS Manager software and simplified server access with Cisco® Single Connect technology. Based on the Intel Xeon processor E5-2600 v4 product family, it offers up to 768 GB of memory using 32-GB DIMMs, up to eight disk drives, and up to 20 Gbps of I/O throughput. The Cisco UCS HX220c-M4S offers exceptional levels of performance, flexibility, and I/O throughput to run your most demanding applications.

The Cisco UCS HX220c-M4S provides:

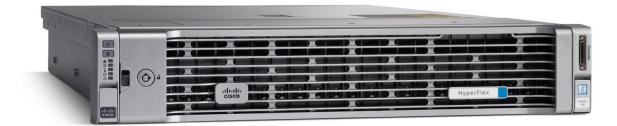
- Up to two multicore Intel Xeon processor E5-2600 v4 series CPUs for up to 44 processing cores
- 24 DIMM slots for industry-standard DDR4 memory at speeds up to 2400 MHz, and up to 768 GB of total memory when using 32-GB DIMMs
- Eight hot-pluggable SAS and SATA HDDs or SSDs

- Cisco UCS VIC 1227, a 2-port, 20 Gigabit Ethernet and FCoE-capable modular (mLOM) mezzanine adapter
- Cisco FlexStorage local drive storage subsystem, with flexible boot and local storage capabilities that allow you to install and boot Hypervisor from.
- Enterprise-class pass-through RAID controller
- Easily add, change, and remove Cisco FlexStorage modules

Cisco HyperFlex HX240c-M4SX Nodes

This capacity optimized configuration contains a minimum of three nodes, a minimum of fifteen and up to twenty-three 1.2 TB SAS drives that contribute to cluster storage, a single 120 GB SSD housekeeping drive, a single 1.6 TB SSD caching drive, and two FlexFlash SD cards that act as the boot drives.

Figure 13 HX240c-M4SX Node



Cisco VIC 1227 MLOM Interface Card

The Cisco UCS Virtual Interface Card (VIC) 1227 is a dual-port Enhanced Small Form-Factor Pluggable (SFP+) 10-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LANon-motherboard (mLOM) adapter installed in the Cisco UCS HX-Series Rack Servers (Error! Reference source not found.). The mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases. The card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). The personality of the card is determined dynamically at boot time using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and World Wide Name [WWN]), failover policy, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all determined using the service profile.

Figure 14 Cisco VIC 1227 mLOM Card



Cisco UCS B200-M4 Nodes

For workloads that require additional computing and memory resources, but not additional storage capacity, a compute-intensive hybrid cluster configuration is allowed. This configuration contains a minimum of three HX240c-M4SX Nodes with up to four Cisco UCS B200-M4 Blade Servers for additional computing capacity. The HX240c-M4SX Nodes are configured as described previously, and the Cisco UCS B200-M4 servers are equipped with boot drives. Use of the B200-M4 compute nodes also requires the Cisco UCS 5108 blade server chassis, and a pair of Cisco UCS 2204XP Fabric Extenders.

Figure 15 Cisco UCS B200 M4 Node



Cisco Ucs 5108 Blade Chassis

The Cisco UCS 5100 Series Blade Server Chassis is a crucial building block of the Cisco Unified Computing System, delivering a scalable and flexible blade server chassis. The Cisco UCS 5108 Blade Server Chassis, is six rack units (6RU) high and can mount in an industry-standard 19-inch rack. A single chassis can house up to eight half-width Cisco UCS B-Series Blade Servers and can accommodate both half-width and full-width blade form factors.

Four single-phase, hot-swappable power supplies are accessible from the front of the chassis. These power supplies are 92 percent efficient and can be configured to support non-redundant, N+1 redundant, and grid redundant configurations. The rear of the chassis contains eight hot-swappable fans, four power connectors (one per power supply), and two I/O bays for Cisco UCS Fabric Extenders. A passive mid-plane provides up to 40 Gbps of I/O bandwidth per server slot from each Fabric Extender. The chassis is capable of supporting 40 Gigabit Ethernet standards.

Figure 16 Cisco UCS 5108 Blade Chassis Front and Rear Views



Cisco UCS 2204XP Fabric Extender

The Cisco UCS 2200 Series Fabric Extenders multiplex and forward all traffic from blade servers in a chassis to a parent Cisco UCS fabric interconnect over from 10-Gbps unified fabric links. All traffic, even traffic between blades on the same chassis or virtual machines on the same blade, is forwarded to the parent interconnect, where network profiles are managed efficiently and effectively by the fabric interconnect. At the core of the Cisco UCS fabric extender are application-specific integrated circuit (ASIC) processors developed by Cisco that multiplex all traffic.

The Cisco UCS 2204XP Fabric Extender has four 10 Gigabit Ethernet, FCoE-capable, SFP+ ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2204XP has sixteen 10 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 80 Gbps of I/O to the chassis.

Figure 17 Cisco UCS 2204XP Fabric Extender



Cisco HyperFlex Converged Data Platform Software

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

- Replication replicates data across the cluster so that data availability is not affected if single or multiple components fail (depending on the replication factor configured).
- Deduplication is always on, helping reduce storage requirements in virtualization clusters in which multiple operating system instances in client virtual machines result in large amounts of replicated data.
- Compression further reduces storage requirements, reducing costs, and the log- structured file system is designed to store variable-sized blocks, reducing internal fragmentation.

- Thin provisioning allows large volumes to be created without requiring storage to support them until the need arises, simplifying data volume growth and making storage a "pay as you grow" proposition.
- Fast, space-efficient clones rapidly replicate storage volumes so that virtual machines can be replicated simply through metadata operations, with actual data copied only for write operations.
- Snapshots help facilitate backup and remote-replication operations: needed in enterprises that require always-on data availability.

Cisco HyperFlex HX Data Platform Administration Plug-in

The Cisco HyperFlex HX Data Platform is administered through a VMware vSphere web client plug-in. 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. For customers that prefer a light weight web interface there is a tech preview URL management interface available by opening a browser to the IP address of the HX cluster interface. Additionally, there is an interface to assist in running cli commands through a web browser.

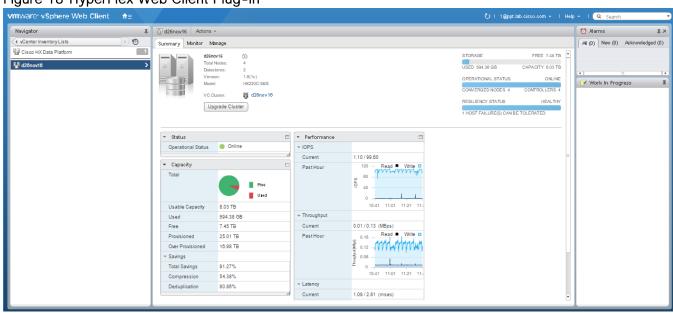


Figure 18 HyperFlex Web Client Plug-in

For Tech Preview Web UI connect to HX controller cluster IP:

http://hx controller cluster ip/ui

Figure 19 HyperFlex Tech Preview UI

dialo HyperFlex	E Search	٩		A REAL AREAL
Dashboard Datastores	1107			HOME > DASHBOARD
Servers				
MONITOR	Operational Status (1)	Storage	Optimization	Resiliency Status 0
 ☐ Performance ↓ Alarms ↓ Events DATA SERVICES 	\bigcirc	98.98% Free	46.38 % Total Savings	Healthy
 Virtual Machines VM Folders Resource Pools 	Online Cluster Status	15.9 TB 167.4 GB Free Used	42.58% 6.62% Compression De-duplication	2 Node failure tolerance
ADMINISTRATION © System Services <	IOPS Read 0.70 Write	= 35.70 ○ 🔅 Throughput (MBps)	Read 0.01 Write 0.17 () 23	nsec) Read 5.00 Write 1.06 🔿 🔗
⊙ Upgrade >_ Web CLI				
https://10.20.151.100//#.	03.50 09.33.30	10:03 03:50 09:33		09:33:30 10:03

To run CLI commands via HTTP, connect to HX controller cluster IP:

Figure 20 Web CLI

diado HyperFlex	E Search. Q	407A
Dashboard Datastores	Web CLI Command Line Interface	HOME > WEB CL
Servers MONITOR D In Performance	Command Je. stcli cluster info	
 ↓ Alarms ♦ Events 	Output	
DATA SERVICES C Virtual Machines C VM Folders		
Resource Pools		
 System Services Upgrade Web CLI 		

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 in user space within a virtual machine and intercepts and handles all I/O from guest virtual machines. The platform controller VM uses the VMDirectPath I/O feature to provide PCI passthrough control of the physical server's SAS disk controller. This method gives the controller VM full control of the physical disk resources, utilizing the SSD drives as a read/write caching layer, and the HDDs as a capacity layer for distributed storage. The controller integrates the data platform into VMware software through the use of two preinstalled VMware ESXi vSphere Installation Bundles (VIBs):

- 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.
- 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 through manipulation of metadata rather than actual data copying, providing rapid response, and thus rapid deployment of new environments.

Data Operations and Distribution

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

Replication Factor

The policy for the number of duplicate copies of each storage block is chosen during cluster setup, and is referred to as the replication factor (RF). The default setting for the Cisco HyperFlex HX Data Platform is replication factor 3 (RF=3).

- Replication Factor 3: For every I/O write committed to the storage layer, 2 additional copies of the blocks written will be created and stored in separate locations, for a total of 3 copies of the blocks. Blocks are distributed in such a way as to ensure multiple copies of the blocks are not stored on the same disks, nor on the same nodes of the cluster. This setting can tolerate simultaneous failures 2 entire nodes without losing data and resorting to restore from backup or other recovery processes.
- Replication Factor 2: For every I/O write committed to the storage layer, 1 additional copy of the blocks written will be created and stored in separate locations, for a total of 2 copies of the blocks. Blocks are distributed in such a way as to ensure multiple copies of the blocks are not stored on the same disks, nor on the same nodes of the cluster. This setting can tolerate a failure 1 entire node without losing data and resorting to restore from backup or other recovery processes.

Data Write Operations

For each write operation, data is written to the SSD of the node designated as it's primary, and replica copies of that write are written to the caching SSD of the remote nodes in the cluster, according to the replication factor setting. For example, at RF=3 a write will be written locally where the VM originated the write, and two additional writes will be committed in parallel on two other nodes. The write operation will not be acknowledged until all three copies are written to the caching layer SSDs. Written data is also cached in a write log area resident in memory in the controller VM, along with the write log on the caching SSDs (Figure 15). This process speeds up read requests when reads are requested of data that has recently been written.

Data Destaging, Deduplication and Compression

The Cisco HyperFlex HX Data Platform constructs multiple write caching segments on the caching SSDs of each node in the distributed cluster. As write cache segments become full, and based on policies accounting for I/O load and access patterns, those write cache segments are locked and new writes roll

over to a new write cache segment. The data in the now locked cache segment is destaged to the HDD capacity layer of the node. During the destaging process, data is deduplicated and compressed before being written to the HDD capacity layer. The resulting data after deduplication and compression can now be written in a single sequential operation to the HDDs of the server, avoiding disk head seek thrashing and accomplishing the task in the minimal amount of time (Figure 21). Since the data is already deduplicated and compressed before being written, the platform avoids additional I/O overhead often seen on competing systems, which must later do a read/dedupe/compress/write cycle. Deduplication, compression and destaging take place with no delays or I/O penalties to the guest VMs making requests to read or write data.

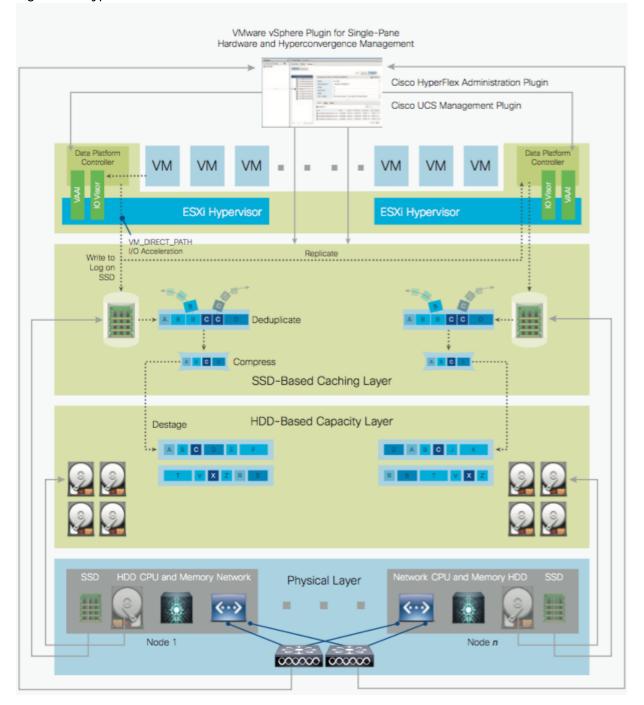


Figure 21 HyperFlex HX Data Platform Data Movement

Data Read Operations

For data read operations, data may be read from multiple locations. For data that was very recently written, the data is likely to still exist in the write log of the local platform controller memory, or the write log of the local caching SSD. If local write logs do not contain the data, the distributed filesystem metadata will be queried to see if the data is cached elsewhere, either in write logs of remote nodes, or in the dedicated read cache area of the local and remote SSDs. Finally, if the data has not been accessed in a significant amount of time, the filesystem will retrieve the data requested from the HDD capacity layer. As requests for reads are made to the distributed filesystem and the data is retrieved from the HDD capacity layer, the caching SSDs populate their dedicated read cache area to speed up subsequent requests for the same data. This multi-tiered distributed system with several layers of caching techniques, insures that data is served at the highest possible speed, leveraging the caching SSDs of the nodes fully and equally.

Cisco Nexus 9372PX Switches

The Cisco Nexus 9372PX/9372PX-E Switches has 48 1/10-Gbps Small Form Pluggable Plus (SFP+) ports and 6 Quad SFP+ (QSFP+) uplink ports. All the ports are line rate, delivering 1.44 Tbps of throughput in a 1-rack-unit (1RU) form factor. Cisco Nexus 9372PX benefits are listed below.

Architectural Flexibility

- Includes top-of-rack or middle-of-row fiber-based server access connectivity for traditional and leafspine architectures
- Leaf node support for Cisco ACI architecture is provided in the roadmap
- Increase scale and simplify management through Cisco Nexus 2000 Fabric Extender support

Feature Rich

- Enhanced Cisco NX-OS Software is designed for performance, resiliency, scalability, manageability, and programmability
- ACI-ready infrastructure helps users take advantage of automated policy-based systems management
- Virtual Extensible LAN (VXLAN) routing provides network services
- Cisco Nexus 9372PX-E supports IP-based endpoint group (EPG) classification in ACI mode

Highly Available and Efficient Design

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

Simplified Operations

- Power-On Auto Provisioning (POAP) support allows for simplified software upgrades and configuration file installation
- An intelligent API offers switch management through remote procedure calls (RPCs, JSON, or XML) over a HTTP/HTTPS infrastructure

- Python Scripting for programmatic access to the switch command-line interface (CLI)
- Hot and cold patching, and online diagnostics

Investment Protection

A Cisco 40 Gb bidirectional transceiver allows reuse of an existing 10 Gigabit Ethernet multimode cabling plant for 40 Gigabit Ethernet Support for 1 Gb and 10 Gb access connectivity for data centers migrating access switching infrastructure to faster speed. The following is supported:

- 1.44 Tbps of bandwidth in a 1 RU form factor
- 48 fixed 1/10-Gbps SFP+ ports
- 6 fixed 40-Gbps QSFP+ for uplink connectivity that can be turned into 10 Gb ports through a QSFP to SFP or SFP+ Adapter (QSA)
- Latency of 1 to 2 microseconds
- Front-to-back or back-to-front airflow configurations
- 1+1 redundant hot-swappable 80 Plus Platinum-certified power supplies
- Hot swappable 2+1 redundant fan tray

Figure 22 Cisco Nexus 9372PX Switch



VMware vSphere 6.0

VMware provides virtualization software. VMware's enterprise software hypervisors for servers–VMware vSphere ESX, vSphere ESXi, and VSphere–are bare-metal hypervisors that run directly on server hardware without requiring an additional underlying operating system. VMware vCenter Server for vSphere provides central management and complete control and visibility into clusters, hosts, virtual machines, storage, networking, and other critical elements of your virtual infrastructure.

VMware vSphere 6.0 introduces many enhancements to vSphere Hypervisor, VMware virtual machines, vCenter Server, virtual storage, and virtual networking, further extending the core capabilities of the vSphere platform.

VMware ESXi 6.0 Hypervisor

vSphere 6.0 introduces a number of new features in the hypervisor:

• Scalability Improvements

ESXi 6.0 dramatically increases the scalability of the platform. With vSphere Hypervisor 6.0, clusters can scale to as many as 64 hosts, up from 32 in previous releases. With 64 hosts in a cluster, vSphere 6.0 can support 8000 virtual machines in a single cluster. This capability enables greater consolidation ratios, more efficient use of VMware vSphere Distributed Resource Scheduler (DRS), and fewer

clusters that must be separately managed. Each vSphere Hypervisor 6.0 instance can support up to 480 logical CPUs, 12 terabytes (TB) of RAM, and 1024 virtual machines. By using the newest hardware advances, ESXi 6.0 enables the virtualization of applications that previously had been thought to be non-virtualizable.

- Security Enhancements
 - ESXi 6.0 offers these security enhancements:
 - Account management: ESXi 6.0 enables management of local accounts on the ESXi server using new ESXi CLI commands. The capability to add, list, remove, and modify accounts across all hosts in a cluster can be centrally managed using a vCenter Server system. Previously, the account and permission management functions for ESXi hosts were available only for direct host connections. The setup, removal, and listing of local permissions on ESXi servers can also be centrally managed.
 - Account lockout: ESXi Host Advanced System Settings have two new options for the management of failed local account login attempts and account lockout duration. These parameters affect Secure Shell (SSH) and vSphere Web Services connections, but not ESXi direct console user interface (DCUI) or console shell access.
 - Password complexity rules: In previous versions of ESXi, password complexity changes had to be made by manually editing the /etc/pam.d/passwd file on each ESXi host. In vSphere 6.0, an entry in Host Advanced System Settings enables changes to be centrally managed for all hosts in a cluster.
 - Improved auditability of ESXi administrator actions: Prior to vSphere 6.0, actions at the vCenter Server level by a named user appeared in ESXi logs with the vpxuser username: for example, [user=vpxuser]. In vSphere 6.0, all actions at the vCenter Server level for an ESXi server appear in the ESXi logs with the vCenter Server username: for example, [us-er=vpxuser: DOMAIN\User]. This approach provides a better audit trail for actions run on a vCenter Server instance that conducted corresponding tasks on the ESXi hosts.
 - Flexible lockdown modes: Prior to vSphere 6.0, only one lockdown mode was available.
 Feedback from customers indicated that this lockdown mode was inflexible in some use cases. With vSphere 6.0, two lockdown modes are available:
- In normal lockdown mode, DCUI access is not stopped, and users on the DCUI access list can access the DCUI.
- In strict lockdown mode, the DCUI is stopped.
 - Exception users: vSphere 6.0 offers a new function called exception users. Exception users are
 local accounts or Microsoft Active Directory accounts with permissions defined locally on the host
 to which these users have host access. These exception users are not recommended for general
 user accounts, but they are recommended for use by third-party applications—for service accounts,
 for example—that need host access when either normal or strict lockdown mode is enabled.
 Permissions on these accounts should be set to the bare minimum required for the application to
 perform its task and with an account that needs only read-only permissions on the ESXi host.
 - Smart card authentication to DCUI: This function is for U.S. federal customers only. It enables DCUI login access using a Common Access Card (CAC) and Personal Identity Verification (PIV). The ESXi host must be part of an Active Directory domain.

VMware Horizon

VMware Horizon desktop virtualization solutions built on a unified architecture so they are simple to manage and flexible enough to meet the needs of all your organization's users. You use the same architecture and management tools to manage public, private, and hybrid cloud deployments as you do for on premises deployments

- VMware Horizon Virtual machines and RDSH known as server-based hosted sessions: These are applications hosted from Microsoft Windows servers to any type of device, including Windows PCs, Macs, smartphones, and tablets. Some VMware editions include technologies that further optimize the experience of using Windows applications on a mobile device by automatically translating native mobile-device display, navigation, and controls to Windows applications; enhancing performance over mobile networks; and enabling developers to optimize any custom Windows application for any mobile environment.
- VMware Horizon RDSH session users also known as server-hosted desktops: These are inexpensive, locked-down Windows virtual desktops hosted from Windows server operating systems. They are well suited for users, such as call center employees, who perform a standard set of tasks.

Advantages of Using VMware Horizon

VMware Horizon 7 version 7.0.1 provides the following new features and enhancements:

- Instant Clones
 - A new type of desktop virtual machines that can be provisioned significantly faster than the traditional View Composer linked clones.
 - A fully functional desktop can be provisioned in two seconds or less.
 - Recreating a desktop pool with a new OS image can be accomplished in a fraction of the time it takes a View Composer desktop pool because the parent image can be prepared well ahead of the scheduled time of pool recreation.
 - Clones are automatically rebalanced across available datastores.
 - View storage accelerator is automatically enabled.
- VMware Blast Extreme
 - VMware Blast Extreme is now fully supported on the Horizon platform.
 - Administrators can select the VMware Blast display protocol as the default or available protocol for pools, farms, and entitlements.
 - End users can select the VMware Blast display protocol when connecting to remote desktops and applications.
 - VMware Blast Extreme features include:
 - TCP and UDP transport support
 - o H.264 support for the best performance across more devices

- o Reduced device power consumption for longer battery life
- NVIDIA GRID acceleration for more graphical workloads per server, better performance, and a superior remote user experience
- True SSO
 - For VMware Identity Manager integration, True SSO streamlines the end-to-end login experience. After users log in to VMware Identity Manager using a smart card or an RSA SecurID or RADIUS token, users are not required to also enter Active Directory credentials in order to use a remote desktop or application.
 - Uses a short-lived Horizon virtual certificate to enable a password-free Windows login.
 - Supports using either a native Horizon Client or HTML Access.
 - System health status for True SSO appears in the Horizon Administrator dashboard.
 - Can be used in a single domain, in a single forest with multiple domains, and in a multiple-forest, multiple-domain setup.
- Smart Policies
 - Control of the clipboard cut-and-paste, client drive redirection, USB redirection, and virtual printing desktop features through defined policies.
 - PCoIP session control through PCoIP profiles.
 - Conditional policies based on user location, desktop tagging, pool name, and Horizon Client registry values.
- Configure the Clipboard Memory Size for VMware Blast and PCoIP Sessions

Horizon administrators can configure the server clipboard memory size by setting GPOs for VMware Blast and PCoIP sessions. Horizon Client 4.1 users on Windows, Linux, and Mac OS X systems can configure the client clipboard memory size. The effective memory size is the lesser of the server and client clipboard memory size values.

• VMware Blast Network Recovery Enhancements

Network recovery is now supported for VMware Blast sessions initiated from iOS, Android, Mac OS X, Linux, and Chrome OS clients. Previously, network recovery was supported only for Windows client sessions. If you lose your network connection unexpectedly during a VMware Blast session, Horizon Client attempts to reconnect to the network and you can continue to use your remote desktop or application. The network recovery feature also supports IP roaming, which means you can resume your VMware Blast session after switching to a WiFi network.

• Configure Horizon Administrator to not remember the login name

Horizon administrators can configure not to display the Remember user name check box and therefore not remember the administrator's login name.

• Allow Mac OS X Users to Save Credentials

Horizon administrators can configure Connection Server to allow Horizon Client Mac OS X systems to remember a user's user name, password, and domain information. If users choose to have their credentials saved, the credentials are added to the login fields in Horizon Client on subsequent connections.

- Windows 10
 - Windows 10 is supported as a desktop guest operating system
 - Horizon Client runs on Windows 10
 - Smart card is supported on Windows 10.
 - The Horizon User Profile Migration tool migrates Windows 7, 8/8.1, Server 2008 R2, or Server 2012 R2 user profiles to Windows 10 user profiles.
- RDS Desktops and Hosted Apps
 - View Composer. View Composer and linked clones provide automated and efficient management of RDS server farms.
 - Graphics Support. Existing 3D vDGA and GRID vGPU graphics solutions on VDI desktops have been extended to RDS hosts, enabling graphics-intensive applications to run on RDS desktops and Hosted Apps.
 - Enhanced Load Balancing. A new capability provides load balancing of server farm applications based on memory and CPU resources.
 - One-Way AD Trusts

One-way AD trust domains are now supported. This feature enables environments with limited trust relationships between domains without requiring Horizon Connection Server to be in an external domain.

- Cloud Pod Architecture (CPA) Enhancements
 - Hosted App Support. Support for application remoting allows applications to be launched using global entitlements across a pod federation.
 - HTML Access (Blast) Support. Users can use HTML Access to connect to remote desktops and applications in a Cloud Pod Architecture deployment.
- Access Point Integration
 - Access Point is a hardened Linux-based virtual appliance that protects virtual desktop and application resources to allow secure remote access from the Internet. Access Point provides a new authenticating DMZ gateway to Horizon Connection Server. Smart card support on Access Point is available as a Tech Preview. Security server will continue to be available as an alternative configuration. For more information, see <u>Deploying and Configuring Access Point</u>.

- FIPS
 - Install-time FIPS mode allows customers with high security requirements to deploy Horizon 6.
- Graphics Enhancements
 - AMD vDGA enables vDGA pass-through graphics for AMD graphics hardware.
 - 4K resolution monitors (3840x2160) are supported.
- Horizon Administrator Enhancements
 - Horizon Administrator shows additional licensing information, including license key, named user and concurrent connection user count.
 - Pool creation is streamlined by letting Horizon administrators clone existing pools.
- Horizon 6 for Linux Desktop Enhancements
 - Several new features are supported on Horizon 6 for Linux desktops, including NVIDIA GRID vGPU, vSGA, RHEL 7.1 and Ubuntu 14.04 guest operating systems, and View Agent installation of JRE 8 with no user steps required.
 - Support for managed virtual machines
 - Support for smart card redirection with SSO
 - Support for Horizon Client for iOS
 - Support for SLES 12 SP1
 - Support for H.264 encoder software
- Additional Features
 - Support for IPv6 with VMware Blast Extreme on security servers.
 - Horizon Administrator security protection layer. See VMware Knowledge Base (KB) article 2144303 for more information.
 - Protection against inadvertent pool deletion.
 - RDS per-device licensing improvements.
 - Support for Intel vDGA.
 - Support for AMD Multiuser GPU Using vDGA.
 - More resilient upgrades.
 - Display scaling for Windows Horizon Clients.
 - DPI scaling is supported if it is set at the system level and the scaling level is greater than 100.

What are VMware RDS Hosted Sessions?

The following describes the VMware RDS Hosted Sessions:

- An RDS host is a server computer that hosts applications and desktop sessions for remote access. An RDS host can be a virtual machine or a physical server.
- An RDS host has the Microsoft Remote Desktop Services role, the Microsoft Remote Desktop Session Host service, and Horizon Agent installed. Remote Desktop Services was previously known as Terminal Services. The Remote Desktop Session Host service allows a server to host applications and remote desktop sessions. With Horizon Agent installed on an RDS host, users can connect to applications and desktop sessions by using the display protocol PCoIP or Blast Extreme. Both protocols provide an optimized user experience for the delivery of remote content, including images, audio and video.
- The performance of an RDS host depends on many factors. For information on how to tune the performance of different versions of Windows Server, see http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx.
- Horizon 7 supports at most one desktop session and one application session per user on an RDS host.
- When users submit print jobs concurrently from RDS desktops or applications that are hosted on the same RDS host, the ThinPrint server on the RDS host processes the print requests serially rather than in parallel. This can cause a delay for some users. Note that the print server does not wait for a print job to complete before processing the next one. Print jobs that are sent to different printers will print in parallel.
- If a user launches an application and also an RDS desktop, and both are hosted on the same RDS host, they share the same user profile. If the user launches an application from the desktop, conflicts may result if both applications try to access or modify the same parts of the user profile, and one of the applications may fail to run properly.
- The process of setting up applications or RDS desktops for remote access involves the following tasks:
- Installing Applications
 - If you plan to create application pools, you must install the applications on the RDS hosts. If you want Horizon 7 to automatically display the list of installed applications, you must install the applications so that they are available to all users from the Start menu. You can install an application at any time before you create the application pool. If you plan to manually specify an application, you can install the application at any time, either before or after creating an application pool.
- Important
 - When you install an application, you must install it on all the RDS hosts in a farm and in the same location on each RDS host. If you do not, a health warning will appear on the View Administrator dashboard. In such a situation, if you create an application pool, users might encounter an error when they try to run the application.
 - When you create an application pool, Horizon 7 automatically displays the applications that are available to all users rather than individual users from the Start menu on all of the RDS hosts in a farm. You can choose any applications from that list. In addition, you can manually specify an

application that is not available to all users from the Start menu. There is no limit on the number of applications that you can install on an RDS host.

Farms, RDS Hosts, Desktop and Application Pools

With VMware Horizon, you can create desktop and application pools to give users remote access to virtual machine-based desktops, session-based desktops, physical computers, and applications. Horizon takes advantage of Microsoft Remote Desktop Services (RDS) and VMware PC-over-IP (PCoIP) technologies to provide high-quality remote access to users.

- RDS Hosts
 - RDS hosts are server computers that have Windows Remote Desktop Services and View Agent installed. These servers host applications and desktop sessions that users can access remotely. To use RDS desktop pools or applications, your end users must have access to Horizon Client 3.0 or later software.
- Desktop Pools
 - There are three types of desktop pools: automated, manual, and RDS. Automated desktop pools use a vCenter Server virtual machine template or snapshot to create a pool of identical virtual machines. Manual desktop pools are a collection of existing vCenter Server virtual machines, physical computers, or third-party virtual machines. In automated or manual pools, each machine is available for one user to access remotely at a time. RDS desktop pools are not a collection of machines, but instead, provide users with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously.
- Application Pools
 - Application pools let you deliver applications to many users. The applications in application pools run on a farm of RDS hosts.
- Farms
 - Farms are collections of RDS hosts and facilitate the management of those hosts. Farms can have a variable number of RDS hosts and provide a common set of applications or RDS desktops to users. When you create an RDS desktop pool or an application pool, you must specify a farm. The RDS hosts in the farm provide desktop and application sessions to users.

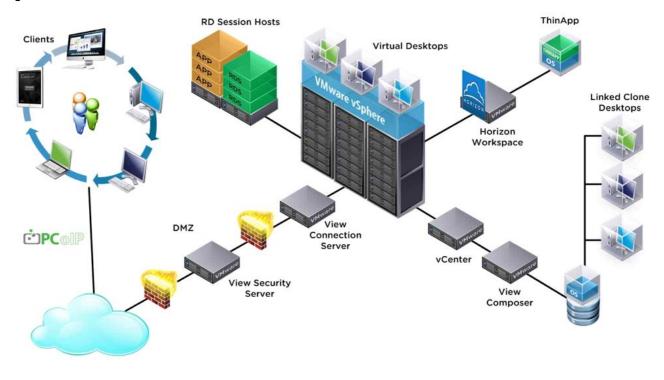


Figure 23 VMware Horizon Architectural Overview

Cisco HyperFlex Data Platform

- In a Cisco HyperFlex System, the data platform requires a minimum of three Cisco HyperFlex HX-Series converged nodes for the default three-way mirroring of data. To create a highly available cluster with N+1 resiliency, the solution considers a minimum of four hyperconverged nodes per cluster. Each node includes a Cisco HyperFlex HX Data Platform controller that implements the distributed file system using internal flash-based SSD drives and high-capacity HDDs to store data. The controllers communicate with each other over 10 Gigabit Ethernet to present a single pool of storage that spans the nodes in the cluster. Individual nodes access data through a data layer using file, block, object, or API plug-ins. As nodes are added, the cluster scales to deliver computing, storage capacity, and I/O performance.
- In the VMware vSphere environment, the controller occupies a virtual machine with a dedicated number
 of processor cores and memory, allowing it to deliver consistent performance and not affect the
 performance of the other virtual machines in the cluster. The controller can access all storage resources
 without hypervisor intervention through the VMware VMDirectPath feature. It uses the node's memory
 and SSD drives as part of a distributed caching layer, and it uses the node's HDDs for distributed
 capacity storage. The controller integrates the data platform into VMware software through the use of
 two preinstalled VMware ESXi vSphere Installation Bundles (VIBs):
 - IO Visor: This VIB provides a network file system (NFS) mount point so that the ESXi hypervisor can access the virtual disk drives that are attached to individual virtual machines. From the hypervisor's perspective, it is simply attached to a network file system.

vStorage API for Array Integration (VAAI): This storage offload API mechanism is used by 0 vSphere to request advanced file system operations related to snapshots and cloning from the underlying storage subsystem. The controller causes these operations to occur by manipulating the metadata rather than actually copying data, providing rapid response and thus rapid deployment of new application environments.

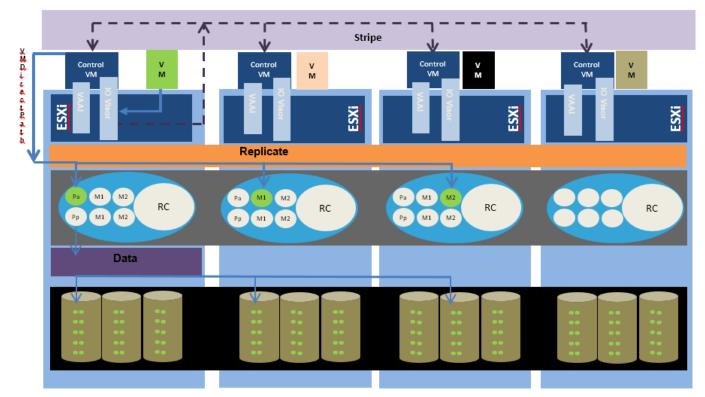


Figure 24 Cisco HyperFlex Data Flow

Definitions

- Primary Active Write Log (2 GB) Pa
- Pp M1a Primary Passive Write Log (2 GB)
- Mirror 1 Active Log (2 GB)
- M1p Mirror 1 Passive Log (2 GB) M2a
- Mirror 2 Active Log (2 GB) Mirror 2 Passive Log (2 GB)
- M2p Read Cache (Rest of Cache SSD) RC
 - 0 As shown in Figure 24, the IO Visor intercepts workload traffic and stripes the block across available nodes in the cluster. The data then bypasses the hypervisor using VMDirectPath and is cached on the larger cache disk in one of the dedicated partitions. Replication across nodes takes place at this layer. Write blocks continue to be written to write logs until they are full, at which time they are marked as passive and destaged to disk. Data optimization processes such as deduplication and compression occur when the data is destaged from the cache and before it is written to disks.
 - The data platform implements a log-structured file system (LogFS) that uses a caching layer 0 in the SSDs to accelerate read requests and write responses, and a persistence layer implemented with HDDs for capacity. The log-structured layer replicates incoming data to one or more SSDs located in different nodes before the write operation is acknowledged to the application. This process allows incoming write operations to be acknowledged quickly while

protecting data from SSD or node failures. If an SSD or node fails, the replica is quickly recreated on other SSDs or nodes using the available copies of the data.

 The log-structured distributed object layer also replicates data that is moved from the write cache to the capacity layer. This replicated data is likewise protected from hard disk or node failures. There are a total of three data copies to survive disk or node failures without risk of data loss. See the <u>Cisco HyperFlex Data Platform system administration guide</u> for a complete list of fault-tolerant configurations and settings.

Architecture and Design of VMware Horizon on Cisco Unified Computing System and Cisco HyperFlex Storage Design Fundamentals

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

- Knowledge Workers today do not just work in their offices all day they attend meetings, visit branch
 offices, work from home, and even coffee shops. These anywhere workers expect access to all of their
 same applications and data wherever they are.
- External Contractors are increasingly part of your everyday business. They need access to certain portions of your applications and data, yet administrators still have little control over the devices they use and the locations they work from. Consequently, IT is stuck making trade-offs on the cost of providing these workers a device vs. the security risk of allowing them access from their own devices.
- Task Workers perform a set of well-defined tasks. These workers access a small set of applications and have limited requirements from their PCs. However, since these workers are interacting with your customers, partners, and employees, they have access to your most critical data.
- Mobile Workers need access to their virtual desktop from everywhere, regardless of their ability to connect to a network. In addition, these workers expect the ability to personalize their PCs, by installing their own applications and storing their own data, such as photos and music, on these devices.
- Shared Workstation users are often found in state-of-the-art university and business computer labs, conference rooms or training centers. Shared workstation environments have the constant requirement to re-provision desktops with the latest operating systems and applications as the needs of the organization change, tops the list.

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

- Traditional PC: A traditional PC is what -typicallyll constituted a desktop environment: physical device with a locally installed operating system.
- Hosted Shared Desktop: A hosted, server-based desktop is a desktop where the user interacts through a delivery protocol. With hosted, server-based desktops, a single installed instance of a server operating system, such as Microsoft Windows Server 2012, is shared by multiple users simultaneously.

Each user receives a desktop "session" and works in an isolated memory space. Changes made by one user could impact the other users.

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

For the purposes of the validation represented in this document both Horizon Virtual Desktops and Remote Desktop sever Hosted Sessions were validated. Each of the sections provides some fundamental design decisions for this environment.

Understanding Applications and Data

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

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

Project Planning and Solution Sizing Sample Questions

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

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

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

- How will we measure success or failure?
- What is the future implication of success or failure?

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

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

Desktop Virtualization Design Fundamentals

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

VMware Horizon Design Fundamentals

VMware Horizon 7 integrates Remote Desktop Server Hosted sessions users and VDI desktop virtualization technologies into a unified architecture that enables a scalable, simple, efficient, mixed users and manageable solution for delivering Windows applications and desktops as a service.

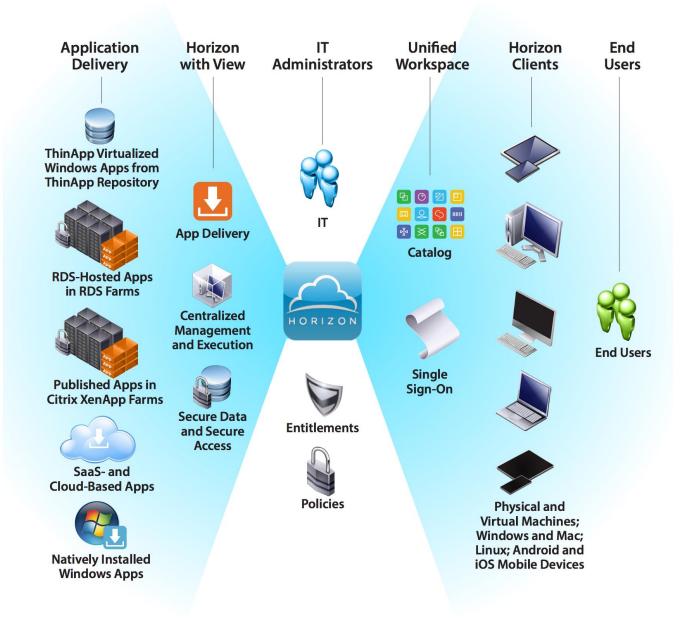
Users can select applications from an easy-to-**use "store" that is accessible from tablets, smartphones, PCs,** Macs, and thin clients. VMware Horizon delivers a native touch-optimized experience via PCoIP or Blast Extreme high-definition performance, even over mobile networks.

Horizon VDI Pool and RDSH Servers Pool

Collections of identical Virtual Machines (VMs) or physical computers are managed as a single entity called a Desktop Pool. In this CVD, VM provisioning relies on VMware View Composer aligning with VMware Horizon View Connection Server and vCenter Server components. Machines in these Pools are configured to run either a Windows Server 2012 OS (for RDSH hosted shared sessions) or a Windows 10 Desktop OS (for linked clone, instant clone and persistent VDI desktops).

Server OS and Desktop OS Machines were configured in this CVD to support RDSH hosted shared desktops and a variety of VDI hosted virtual desktops.

Figure 25 VMware Horizon Design Overview



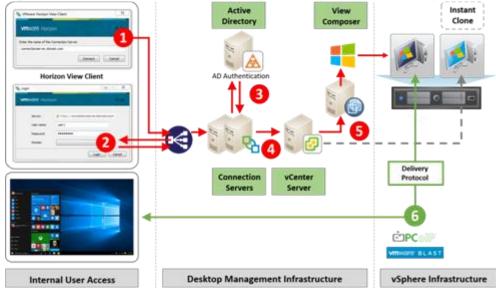


Figure 26 Horizon VDI and RDSH desktop Delivery based on display protocol (PCoIP/Blast/RDP)

VMware Horizon Composer

VMware Horizon Composer is a feature in Horizon that gives administrators the ability to manage virtual machine pools or the desktop pools that share a common <u>virtual disk</u>. An administrator can update the <u>master image</u>, then all desktops using <u>linked clones</u> of that master image can also be patched. Updating the master image will patch the cloned desktops of the users without touching their applications, data or settings.

The VMware View Composer pooled desktops solution's infrastructure is based on software-streaming technology. After creating and configuring the Master Image for a virtual desktop pool, a snapshot is taken of the OS and applications that is accessible to host(s).

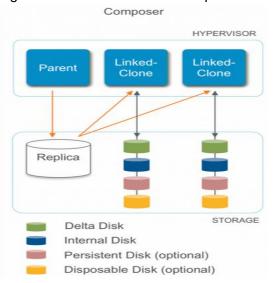


Figure 27 VMware Horizon Composer Overview

VMware View Storage Accelerator

VMware View Storage Accelerator is an in-memory host caching capability that uses the content-based read cache (CBRC) feature in ESXi hosts. CBRC provides a per-host RAM-based solution for View desktops, which greatly reduces the number of read I/O requests that are issued to the storage layer. It also addresses boot storms—when multiple virtual desktops are booted at the same time—which can cause a large number of read operations. CBRC is beneficial when administrators or users load applications or data frequently. Note that CBRC was used in all tests that were performed on the solution described here: Horizon running pooled linked-clone desktops hosted on Cisco HyperFlex system.

Multiple Site Configuration

If you have multiple regional sites, you can use any of the Load Balances Tools (Ex:- Big-IP Global Traffic Manager) to direct the user connections to the most appropriate site to deliver the desktops and application to users.

In Figure 28, The image depicting sites, a site was created in two data centers. Having two sites globally, rather than just one, minimizes the amount of unnecessary WAN traffic. Two Cisco blade servers host the required infrastructure services (Domain Controllers, DNS, DHCP, Profile, SQL, VMware Horizon View Connection Servers, View Composer server and web servers).

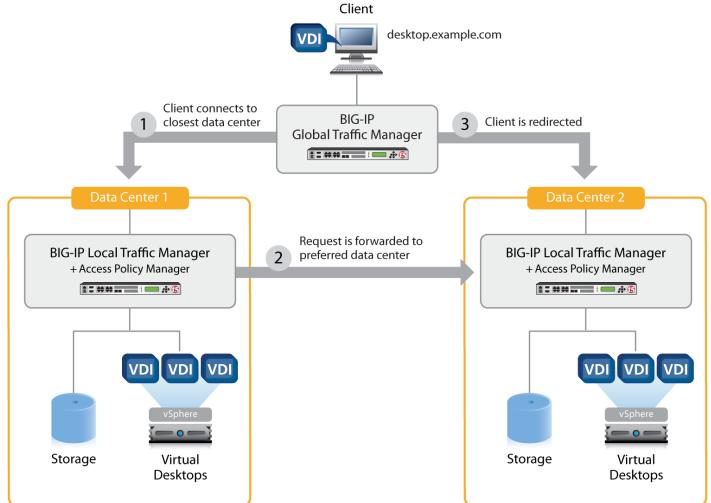


Figure 28 Multisite Configuration Overview

Based on the requirement and no of data centers or remote location, we can chose any of the available Load balancing software or tools accelerates the application performance, load balances servers, increases security, and optimizes the user experience. In this example, two Big-IP Local Traffic Manager are used to provide a high availability configuration.

4

BIG-IP Local Traffic Manager has been shown as example for presentation purpose.

Designing a VMware Horizon Environment for Various Workload Types

With VMware Horizon 7, the method you choose to provide applications or desktops to users depends on the types of applications and desktops you are hosting and available system resources, as well as the types of users and user experience you want to provide.

Server OS mach	nines	 You want: Inexpensive server-based delivery to minimize the cost of delivering applications to a large number of users, while providing a secure, high-definition user experience. Your users: Perform well-defined tasks and do not require personalization or offline access to applications. Users may include task workers such as call center operators and retail workers, or users that share workstations. Application types: Any application.
Desktop machines	OS	You want: A client-based application delivery solution that is secure, provides central- ized management, and supports a large number of users per host server (or hypervi- sor), while providing users with applications that display seamlessly in high-definition.

Your users: Are internal, external contractors, third-party collaborators, and other provisional team members. Users do not require off-line access to hosted applications.

Application types: Applications that might not work well with other applications or might interact with the operating system, such as .NET framework. These types of applications are ideal for hosting on virtual machines.

Applications running on older operating systems such as Windows XP or Windows Vista, and older architectures, such as 32-bit or 16-bit. By isolating each application on its own virtual machine, if one machine fails, it does not impact other users.

Remote PC Ac- cess	You want: Employees with secure remote access to a physical computer without using a VPN. For example, the user may be accessing their physical desktop PC from home or through a public WIFI hotspot. Depending upon the location, you may want to restrict the ability to print or copy and paste outside of the desktop. This method enables BYO device support without migrating desktop images into the datacenter.
	access to specific software or data on their corporate desktops to perform their jobs remotely.
	Host: The same as Desktop OS machines.
	Application types: Applications that are delivered from an office computer and display seamlessly in high definition on the remote user's device.

For the Cisco Validated Design described in this document, individual configuration of Remote Desktop Server Hosted sessions (RDSH) using RDS-based Server OS machines and Hosted Virtual Desktops (HVDs) using Desktop OS machines via Linked-clone and Instant-clone automated pool were configured and tested. The following sections discuss design decisions relative to the VMware Horizon deployment, including the CVD test environment.

Deployment Hardware and Software

Products Deployed

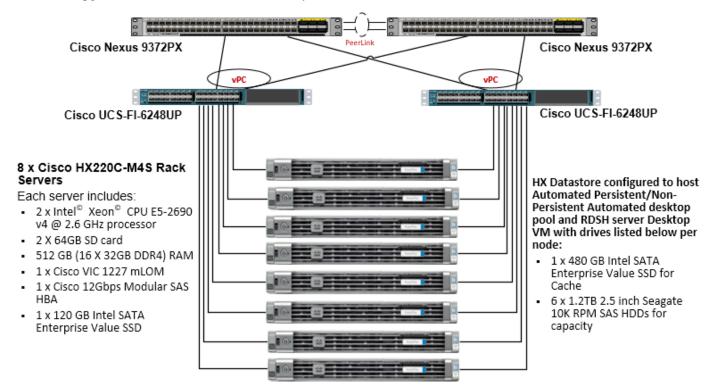
The architecture deployed is highly modular. While each customer's environment might vary in its exact configuration, the reference architecture contained in this document once built, can easily be scaled as requirements and demands change. This includes scaling both up (adding additional resources within existing Cisco HyperFlex system) and out (adding additional Cisco UCS HX-series nodes).

The solution includes Cisco networking, Cisco UCS and Cisco HyperFlex hyper-converged storage, which efficiently fits into a single data center rack, including the access layer network switches.

This validated design document details the deployment of the multiple configurations extending to 1000 or 1200 users for Horizon virtual desktop or Horizon RDSH published desktop workload respectively featuring the following software:

- VMware Horizon 7 Shared Remote Desktop Server Hosted sessions(RDSH) on Cisco HyperFlex.
- VMware Horizon 7 Non-Persistent Hosted Virtual Desktops (VDI) on Cisco HyperFlex.
- Microsoft Windows Server 2012 R2 for User Profile Manager.
- Microsoft Windows 2012 R2 Server for Login VSI Management and data servers to simulate real world VDI workload.
- VMware vSphere ESXi 6.0 Update 2 patch03 Hypervisor
- Windows Server 2012 R2 for RDSH Servers & Windows 10 64-bit Operating Systems for VDI virtual machines
- Microsoft SQL Server 2012
- Cisco HyperFlex data platform v1.8.1b.
- VMware Horizon 7 Connection Server and Replica Servers for redundancy and support up to 1200 seat scale.
- VMware Horizon 7 View Composer Server

Figure 29 Detailed reference Architecture with Physical hardware cabling configured to enable the solution



Cisco HyperFlex and VMware Horizon 7, Detailed Architecture

Hardware Deployed

The solution contains the following hardware as shown in Figure 29:

- Two Cisco Nexus 9372PX Layer 2 Access Switches
- Two Cisco UCS C220 M4 Rack servers with dual socket Intel Xeon E5-2620v4 2.1-GHz 8-core processors, 128GB RAM 2133-MHz and VIC1227 mLOM card for the hosted infrastructure with N+1 server fault tolerance. (Not show in the diagram).
- Eight Cisco UCS HX220c-M4S Rack servers with Intel Xeon E5-2690v4 2.6-GHz 14-core processors, 512GB RAM 2400-MHz and VIC1340 mLOM cards running Cisco HyperFlex data platform v1.8.1b for the virtual desktop workloads with N+1 server fault tolerance

Software Deployed

Table 1 lists the software and firmware version used in the study.

Table 1Software and Firmware Versions

Vendor	Product	Version
Cisco	UCS Component Firmware	3.1(2b) bundle release

Vendor	Product	Version	
Cisco	UCS Manager	3.1(2b) bundle release	
Cisco	UCS HX220c-M4S Blades	3.1(2b) bundle release	
Cisco	VIC 1227	4.1(2d)	
Cisco	HyperFlex Data Platform	1.8.1b-19547	
Cisco	Cisco eNIC	2.3.0.10	
Cisco	Cisco fNIC	1.6.0.28	
Network	Cisco Nexus 9000 NX-OS	7.0(3)I2(2d)	
VMware	Horizon Connection Server	7.0.1-3988955	
VMware	Horizon Composer Server	7.0.1-3978853	
VMware	Horizon Agent	7.0.1-3989057	
VMware	Horizon Client	4.1.0-3977225	
VMware	vCenter Server Appliance	6.0.0-3634788	
VMware	vSphere ESXi 6.0 Update 2 patch03	6.0.0.4192238	

Logical Architecture

The logical architecture of this solution is designed to support up to 1000 Hosted Virtual Microsoft Windows 10 Desktops or 1200 RDSH hosted shared server desktop users within an eight node Cisco UCS HX220c-M4S HyperFlex cluster, which provides physical redundancy for each workload type.

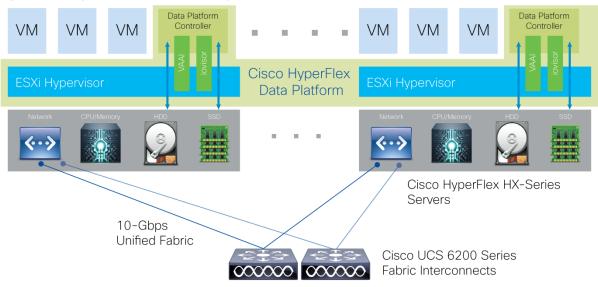


Figure 30 Logical Architecture Design

Table 1 lists the software revisions for this solution.

This document is intended to allow you to fully configure your environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. **Error! Reference source not found.** through **Error! Reference source not found.** lists the information you need to configure your environment.

VLANs

The VLAN configuration recommended for the environment includes a total of seven VLANs as outlined in Error! Reference source not found.2.

Table 2	Table 2 VLANs Configured in this Study	

VLAN Name	VLAN ID	VLAN Purpose
Default	1	Native VLAN
Hx-in-Band- Mgmt	50	VLAN for in-band management inter- faces
Infra-Mgmt	51	VLAN for Virtual Infrastructure
Hx-storage- data	52	VLAN for HyperFlex Storage
Hx-vmotion	53	VLAN for VMware vMotion
Vm-network	54	VLAN for VDI Traffic

VLAN Name	VLAN ID	VLAN Purpose
OOB-Mgmt	132	VLAN for out-of-band management interfaces

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

Jumbo Frames

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

VMware Clusters

Three VMware Clusters were configured in one vCenter datacenter instance to support the solution and testing environment:

- Infrastructure Cluster: Infrastructure VMs (vCenter, Active Directory, DNS, DHCP, SQL Server, VMware Connection Servers, VMware Replica Servers, View Composer Server, Nexus 1000v Virtual Supervisor Module, and VSMs, etc.)
- HyperFlex Cluster: VMware Horizon RDSH VMs (Windows Server 2012 R2) or Persistent/Non-Persistent VDI VM Pools (Windows 10 64-bit)



HyperFlex release v1.8.1 supports 16 nodes in single VMware cluster. Which can support a combination of up to eight converged nodes and eight compute-only nodes.

• VSI Launcher Cluster: Login VSI Cluster (The Login VSI launcher infrastructure was connected using the same set of switches and vCenter instance, but was hosted on separate local storage and servers.)

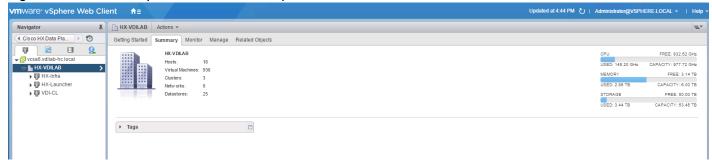


Figure 31 VMware vSphere Clusters on vSphere Web GUI

ESXi Host Design

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

Virtual Networking Design

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

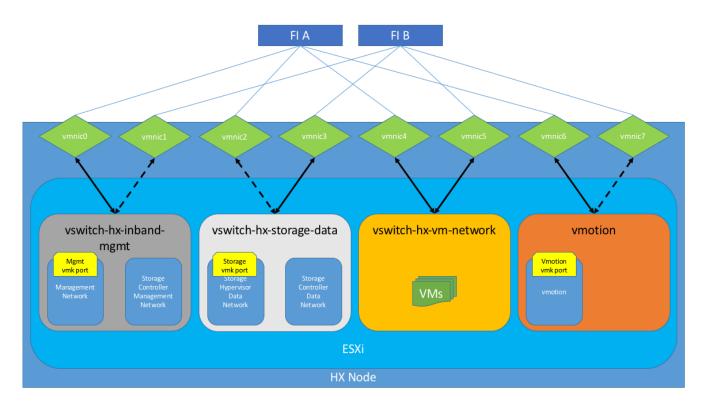
- vswitch-hx-inband-mgmt: This is the default vSwitch0 which is renamed by the ESXi kickstart file as
 part of the automated installation. The default vmkernel port, vmk0, is configured in the standard
 Management Network port group. The switch has two uplinks, active on fabric A and standby on fabric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

The following table and figures help give more details into the ESXi virtual networking design as built by the HyperFlex installer:

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

Table 3 Table ESXi Host Virtual Switch Configuration

Figure 32 ESXi Network Design



VMDirectPath I/O Pass-through

VMDirectPath I/O allows a guest VM to directly access PCI and PCIe devices in an ESXi host as though they were physical devices belonging to the VM itself, also referred to as PCI pass-through. With the appropriate driver for the hardware device, the guest VM sends all I/O requests directly to the physical device, bypassing the hypervisor. In the Cisco HyperFlex system, the Storage Platform Controller VMs use this feature to gain full control of the Cisco 12Gbps SAS HBA cards in the Cisco HX-series rack-mount servers. This gives the controller VMs direct hardware level access to the physical disks installed in the servers, which they consume to construct the Cisco HX Distributed Filesystem. Only the disks connected directly to the Cisco SAS HBA or to a SAS extender, in turn connected to the SAS HBA are controlled by the controller VMs. Other disks, connected to different controllers, such as the SD cards, remain under the control of the ESXi hypervisor. The configuration of the VMDirectPath I/O feature is done by the Cisco HyperFlex installer, and requires no manual steps.

Storage Platform Controller VMs

A key component of the Cisco HyperFlex system is the Storage Platform Controller Virtual Machine running on each of the nodes in the HyperFlex cluster. The controller VMs cooperate to form and coordinate the Cisco HX Distributed Filesystem, and service all the guest VM IO requests. The controller VMs are deployed as a vSphere ESXi agent, which is similar in concept to that of a Linux or Windows service. ESXi agents are tied to a specific host, they start and stop along with the ESXi hypervisor, and the system is not considered to be online and ready until both the hypervisor and the agents have started. Each ESXi hypervisor host has a single ESXi agent deployed, which is the controller VM for that node, and it cannot be moved or migrated to another host. The collective ESXi agents are managed via an ESXi agency in the vSphere cluster. The storage controller VM runs custom software and services that manage and maintain the Cisco HX Distributed Filesystem. The services and processes that run within the controller VMs are not exposed as part of the ESXi agents to the agency, therefore the ESXi hypervisors nor vCenter server have any direct knowledge of the storage services provided by the controller VMs. Management and visibility into the function of the controller VMs, and the Cisco HX Distributed Filesystem is done via a plugin installed to the vCenter server or appliance managing the vSphere cluster. The plugin communicates directly with the controller VMs to display the information requested, or make the configuration changes directed, all while operating within the same web-based interface of the vSphere Web Client. The deployment of the controller VMs, agents, agency, and vCenter plugin are all done by the Cisco HyperFlex installer, and requires no manual steps.

Controller VM Locations

The physical storage location of the controller VMs differs between the Cisco HX220c-M4S and HX240c-M4SX model servers, due to differences with the physical disk location and connections on the two models of servers. The storage controller VM is operationally no different from any other typical virtual machines in an ESXi environment. The VM must have a virtual disk with the bootable root filesystem available in a location separate from the SAS HBA that the VM is controlling via VMDirectPath I/O. The configuration details of the models are as follows:

- HX220c: The controller VM's root filesystem is stored on a 2.2 GB virtual disk, /dev/sda, which is
 placed on a 3.5 GB VMFS datastore, and that datastore is provisioned from the internal mirrored SD
 cards. The controller VM has full control of all the front facing hot-swappable disks via PCI passthrough control of the SAS HBA. The controller VM operating system sees the 120 GB SSD, also
 commonly called the "housekeeping" disk as /dev/sdb, and places HyperFlex binaries, logs, and
 zookeeper partitions on this disk. The remaining disks seen by the controller VM OS are used by the HX
 Distributed filesystem for caching and capacity layers.
- HX240c: The HX240c-M4SX server has a built-in SATA controller provided by the Intel Wellsburg
 Platform Controller Hub (PCH) chip, and the 120 GB housekeeping disk is connected to it, placed in an
 internal drive carrier. Since this model does not connect the 120 GB housekeeping disk to the SAS
 HBA, the ESXi hypervisor remains in control of this disk, and a VMFS datastore is provisioned there,
 using the entire disk. On this VMFS datastore, a 2.2 GB virtual disk is created and used by the controller
 VM as /dev/sda for the root filesystem, and an 87 GB virtual disk is created and used by the controller
 VM as /dev/sdb, placing the HyperFlex binaries, logs, and zookeeper partitions on this disk. The frontfacing hot swappable disks, seen by the controller VM OS through PCI pass-through control of the SAS
 HBA, are used by the HX Distributed filesystem for caching and capacity layers.

The following figures detail the Storage Platform Controller VM placement on the ESXi hypervisor hosts.

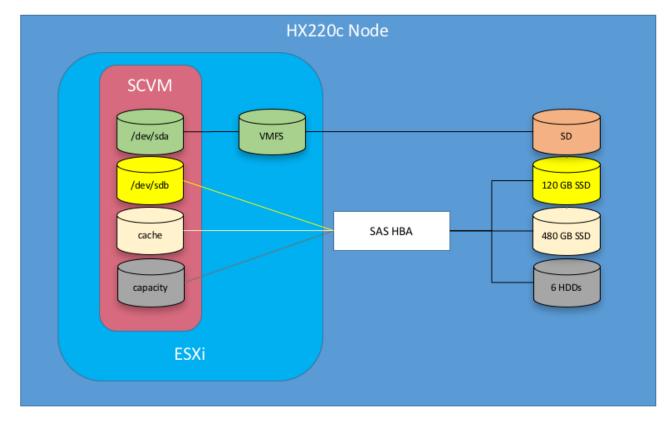


Figure 33 HX220c Controller VM Placement

The Cisco UCS B200-M4 compute-only blades also place a lightweight storage controller VM on a 3.5 GB VMFS datastore, provisioned from the SD cards.

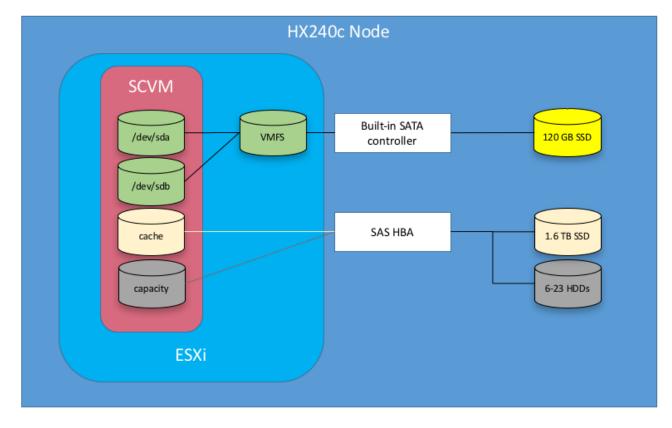
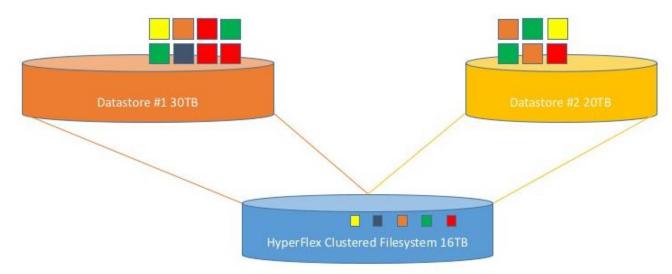


Figure 34 HX240c Controller VM Placement

HyperFlex Datastores

The new HyperFlex cluster has no default datastores configured for virtual machine storage, therefore the datastores must be created using the vCenter Web Client plugin. A minimum of two datastores is recommended to satisfy vSphere High Availability datastore heartbeat requirements, although one of the two datastores can be very small. 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 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.

Figure 35 Datastore Example



CPU Resource Reservations

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

Table 4 Controller VM CPU Reservations

Number of vCPU	Shares	Reservation	Limit
8	Low	10800 MHz	unlimited

Memory Resource Reservations

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

The following table details the memory resource reservation of the storage controller VMs:

Table 5 Controller VM Memory Reservations

	5	
Server Model	Amount of Guest Memory	Reserve All Guest Memory
HX220c-M4S	48 GB	Yes
HX240c-M4SX	72 GB	Yes



The Cisco UCS B200-M4 compute-only blades have a lightweight storage controller VM, it is configured with only 1 vCPU and 512 MB of memory reservation.

Solution Configuration

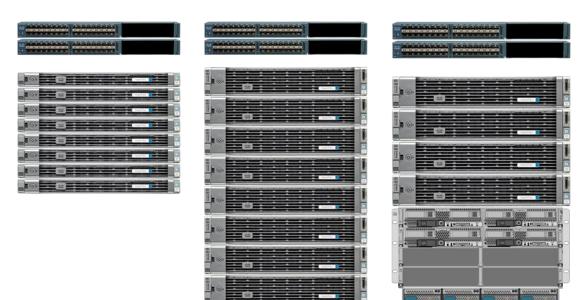
This section details the configuration and tuning that was performed on the individual components to produce a complete, validated solution. Figure 36 illustrates the configuration topology for this solution.

Figure 36 Configuration Topology for Scalable VMware Horizon 7 Workload with HyperFlex

HX220c

HX240c

B200 & HX240c



Cisco UCS Compute Platform

The following subsections detail the physical connectivity configuration of the VMware Horizon 7 environment.

Physical Infrastructure

Solution Cabling

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

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

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps.

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

Figure 29 shows a cabling diagram for a VMware Horizon configuration using the Cisco Nexus 9000 and Cisco UCS Fabric Interconnect.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9372 A	Eth1/1	10GbE	Cisco Nexus 9372 B	Eth1/1
	Eth1/2	10GbE	Cisco Nexus 9372 B	Eth1/2
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth2/13
	Eth1/4	10GbE	Cisco UCS fabric interconnect A	Eth2/14
	Eth1/5	10GbE	Cisco UCS fabric interconnect B	Eth2/15
	Eth1/6	10GbE	Cisco UCS fabric interconnect B	Eth2/16
	Eth1/25	10GbE	Infra-host-01	Port01
	Eth1/26	10GbE	Infra-host-02	Port01
	Eth1/27	10GbE	Launcher-host-01	Port01
	Eth1/28	10GbE	Launcher-host-02	Port01
	Eth1/29	10GbE	Launcher-host-03	Port01
	Eth1/30	10GbE	Launcher-host-04	Port01
	MGMTO	GbE	GbE management switch	Any

Table 6Table 3 Cisco Nexus 9372-Cabling Information

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

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9372 B	Eth1/1	10GbE	Cisco Nexus 9372 A	Eth1/1
	Eth1/2	10GbE	Cisco Nexus 9372 A	Eth1/2
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth2/13
	Eth1/4	10GbE	Cisco UCS fabric interconnect A	Eth2/14
	Eth1/5	10GbE	Cisco UCS fabric interconnect B	Eth2/15

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/6	40GbE	Cisco UCS fabric interconnect B	Eth2/16
	Eth1/25	10GbE	Infra-host-01	Port02
	Eth1/26	10GbE	Infra-host-02	Port02
	Eth1/27	10GbE	Launcher-host-01	Port02
	Eth1/28	10GbE	Launcher-host-02	Port02
	Eth1/29	10GbE	Launcher-host-03	Port02
	Eth1/30	10GbE	Launcher-host-04	Port02
	MGMTO	GbE	GbE management switch	Any

Table 8 Cisco UCS Fabric Interconnect A Cabling Information

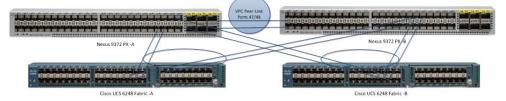
Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Eth2/13	10GbE	Cisco Nexus 9372 A	Eth1/3
	Eth2/14	10GbE	Cisco Nexus 9372 A	Eth1/4
	Eth2/15	10GbE	Cisco Nexus 9372 B	Eth1/5
	Eth2/16	10 GbE	Cisco Nexus 9372 B	Eth 1/6
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2
	Eth2/1	10GbE	HyperFlex-host-01	Port01
	Eth2/2	10GbE	HyperFlex-host-02	Port01
	Eth2/3	10GbE	HyperFlex-host-03	Port01
	Eth2/4	10GbE	HyperFlex-host-04	Port01
	Eth2/5	10GbE	HyperFlex-host-05	Port01
	Eth2/6	10GbE	HyperFlex-host-06	Port01

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth2/7	10GbE	HyperFlex-host-07	Port01
	Eth2/8	10GbE	HyperFlex-host-08	Port01

Table 9 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect B	Eth2/13	10GbE	Cisco Nexus 9372 B	Eth1/3
	Eth2/14	10GbE	Cisco Nexus 9372 B	Eth1/4
	Eth2/15	10GbE	Cisco Nexus 9372 A	Eth1/5
	Eth2/16	10GbE	Cisco Nexus 9372 A	Eth 1/6
	MGMTO	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A	L1
	L2	GbE	Cisco UCS fabric interconnect A	L2
	Eth2/1	10GbE	HyperFlex-host-01	Port02
	Eth2/2	10GbE	HyperFlex-host-02	Port02
	Eth2/3	10GbE	HyperFlex-host-03	Port02
	Eth2/4	10GbE	HyperFlex-host-04	Port02
	Eth2/5	10GbE	HyperFlex-host-05	Port02
	Eth2/6	10GbE	HyperFlex-host-06	Port02
	Eth2/7	10GbE	HyperFlex-host-07	Port02
	Eth2/8	10GbE	HyperFlex-host-08	Port02

Figure 37 Cable Connectivity Between Cisco Nexus 9372 A and B to Cisco UCS 6248 Fabric A and B



Cisco Unified Computing System Configuration

This section details the Cisco UCS configuration that was done as part of the infrastructure build out by the Cisco HyperFlex installer. Many of the configuration elements are fixed in nature, meanwhile the HyperFlex installer does allow for some items to be specified at the time of creation, for example VLAN names and IDs, IP pools and more. Where the elements can be manually set during the installation, those items will be noted in << >> brackets.

For complete detail on racking, power, and installation of the chassis is described in the install guide (see <u>www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-guides-list.html</u>) and it is beyond the scope of this document. For more information about each step, refer to the following documents: Cisco UCS Manager Configuration Guides – GUI and Command Line Interface (CLI) <u>Cisco UCS Manager - Configuration Guides - Cisco</u>

During the HyperFlex Installation a UCS Sub-**Organization is created named "hx-cluster". The** suborganization is created below the root level of the UCS hierarchy, and is used to contain all policies, pools, templates and service profiles used by HyperFlex. This arrangement allows for organizational control using Role-Based Access Control (RBAC) and administrative locales at a later time if desired. In this way, control can be granted to administrators of only the HyperFlex specific elements of the Cisco UCS domain, separate from control of root level elements or elements in other sub-organizations.

Figure 38 Cisco UCSM configuration: HyperFlex Sub-organization

Deploy and Configure HyperFlex Data Platform

Prerequisites

To deploy and configure the HyperFlex Data Platform, you must complete the following prerequisites:

1. Set Time Zone and NTP: From the Cisco UCS Manager, from the Admin tab, Configure TimeZone and add NTP server. Save changes.

Fault Summary				10	🗃 🎒 🖽 New 🚽 🕞 Options	0	Pending Activities O Exit			
🛛 😣 🔍		Δ	Δ	10						
0 2		0	0		>> 🗿 Time Zone Management 🕨	9	Timezone			
Equipment		Servers	LAN		General Events					
	orage	Chassis	Admin		Actions	P	roperties			
Filter: Time	one Mar	nagement	-		Add NTP Server					
• •							Time Zone: America/Los_Angeles (Pacific Time)		-	
							NTP Servers			
Time Zone Ma	nagemer	n					🕰 Filter 👄 Export 😸 Print			
							Name	₽		
									Ð	
								~		

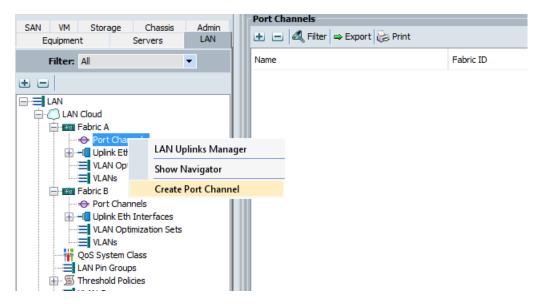
2. Configure Server Ports: Under the Equipment tab, Select Fabric A, select port to be configured as server port to manager HyperFlex rack server through Cisco UCS Manager.

Cisco Unified Computing System M	anager - K22-HXView								o ×
ault Summary	🔓 🏐 📫 New 🔪 🎴 Qotion	ns 🛛 😧 🕕 📥 Pending Activities 📗	0 Exit						ajar Cito
0 2 0 0		c Interconnects + 🔤 Fabric Interconnec	ct A (primary) 🕨 🎟	Fixed Module + 📲 Ethernet Ports					-Ethernet Ports
SAN VM Storage Chassis Admin	Ethernet Ports								
Equipment Servers LAN	🕰 Filter 👄 Export 😸 Print	If Role: 🗸 All 🗸 Unconfigured 🗸	Network 🔽 Serv	er 🔽 FCoE Uplink 🔽 Unified Uplink 🔽 Appliance	Storage 🖌 FCoE Storage 🖌 Unified Stor	rage 🖌 Monitor			
Filter: Al 💌	Slot	Aggr. Port ID	Port ID	MAC	If Role	IfType	Overall Status	Admin State	10
	1				Unconfigured		Admin Down	Disabled	^
	- III -						🐥 Admin Down	Disabled	
Equipment	1						Admin Down	Disabled	
Rack-Mounts	1						👃 Admin Down	Disabled	
FEX	1						👃 Admin Down	Disabled	
Servers	1						Admin Down	Disabled	
E Fabric Interconnects	1						Admin Down	Disabled	
Fabric Interconnect A (primary)	1		8	Enable	Unconfigured		👃 Admin Down	Disabled	
Fixed Module	1	0	9	Disable	Unconfigured	Physical	Admin Down	Disabled	
Ethernet Ports	1	0	10		Unconfigured	Physical	Admin Down	Disabled	
FC Ports	1	0	11	Configure as Server Port	Unconfigured	Physical	Admin Down	Disabled	
Expansion Module 1	1	0	12	Configure as Uplink Port	Unconfigured	Physical	Admin Down	Disabled	
PSUs	1	0	13	Configure as FCoE Uplink Port	Unconfigured	Physical	Admin Down	Disabled	
Fabric Interconnect 8 (subordinate)	1	0	14	, ,	Unconfigured	Physical	Admin Down	Disabled	
Fixed Module	1	0	15	Configure as FCoE Storage Port	Unconfigured	Physical	Admin Down	Disabled	
E- III Expansion Module 1	1	0	16	Configure as Appliance Port	Unconfigured	Physical	Admin Down	Disabled	
🕀 🔛 Fans	1	0	17	Unconfigure	Unconfigured	Physical	Admin Down	Disabled	
🗄 🎆 PSUs	1	0	18		Unconfigured	Physical	Admin Down	Disabled	
	1	0	19	Unconfigure FCoE Uplink Port	Unconfigured	Physical	Admin Down	Disabled	
	1	0	20	Unconfigure Uplink Port	Lincoofig red	Physical	Admin Down	Disabled	

- 3. Repeat this step to configure server port on Fabric B.
- 4. Configure Uplink Ports: On Fabric A, Select port to be configured as uplink port for network connectivity to north bound switch.

	nt 🕴 💼 Fabric Interconnects 👂 📷 Fabric Interconn	ect A (primary) + IIII Fixed Module +	- Ethernet Ports				-1 0 Etha
VM Storage Chassis Admin Ethernet Ports	s cort 🍪 Print If Role: 🔽 All 🔽 Unconfigured [distant discus	halinda 🖂 (half and) halinda 🖂 Amerikanana Starana		ana di Marian		
					_	Overal Status	
Filter: Al 💌 Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type		Admin State
1	0	1	8C:60:4F:A9:A7:08	Unconfigured	Physical	Admin Down	Disabled
Equipment	0	2	8C:60:4F:A9:A7:09	Unconfigured	Physical	Admin Down	Disabled
tell Chassis	0	3	8C:60:4F:A9:A7:0A	Unconfigured	Physical	Admin Down	Disabled
T Rack-Mounts	0	4	8C:60:4F:A9:A7:08	Unconfigured	Physical	Admin Down	Disabled
- Rg PEX 1	0	5	8C:60:4F:A9:A7:0C	Unconfigured	Physical	Admin Down	Disabled
Servers 1	0	6	8C:60:4F:A9:A7:0D	Unconfigured	Physical	Admin Down	Disabled
Fabric Interconnects Fabric Interconnect A (orimary)	0	7	8C:60:4F:A9:A7:0E	Unconfigured	Physical	Admin Down Admin Down	Disabled Disabled
E Bit Paone Interconnect A (primary)	o	8	8C:60:4F:A9:A7:0F	Unconfigured	Physical		
E	0	9	8C:60:4F:A9:A7:10	Unconfigured	Physical	Admin Down	Disabled
PC Ports	0	10	8C:60:4F:A9:A7:11	Unconfigured	Physical	Admin Down Admin Down	Disabled
Expansion Module 1	0	11	8C:60:4F:A9:A7:12	Unconfigured	Physical	Admin Down Admin Down	Disabled Disabled
E B Fans	0	12	8C:60:4F:A9:A7:13 8C:60:4F:A9:A7:14	Unconfigured	Physical	Admin Down Admin Down	Disabled Disabled
E B PSUs	0	13	8C:60:4F:A9:A7:14 8C:60:4F:A9:A7:15	Unconfigured	Physical	Admin Down Admin Down	Disabled Disabled
Fixed Module	0	19	8C:60:4F:A9:A7:15 8C:60:4F:A9:A7:16	Unconfigured	Physical	Admin Down Admin Down	Usabled Isabled
Fixed Module	0	15	8C:60:4F:A9:A7:10 8C:60:4F:A9:A7:17	Unconfigured	Physical Physical	Admin Down Admin Down	Disabled Disabled
Big Fans	0	16	BC:60:4F:A9:A7:17 BC:60:4F:A9:A7:18	Unconfigured	Physical	Admin Down Admin Down	Disabled
E PSUs	0	18	8C:60:4F:A9:A7:18			Admin Down Admin Down	Disabled
1	0	18	8C:60:4F:A9:A7:19 8C:60:4F:A9:A7:1A	Unconfigured	Physical	Admin Down Admin Down	Usabled Isabled
1	0	20	8C:60:4F:A9:A7:1A 8C:60:4F:A9:A7:1B	Unconfigured	Physical Physical	Admin Down Admin Down	Disabled
1	0		BC:60:4F:A9:A7:10 BC:60:4F:A9:A7:10			Admin Down Admin Down	Disabled
1	0	21		Unconfigured	Physical	Admin Down Admin Down	Disabled Disabled
1	0	22	8C:60:4F:A9:A7:1D	Unconfigured	Physical		
1	0	23	8C:60:4F:A9:A7:1E	Unconfigured	Physical	Admin Down	Disabled Disabled
1	0	24	8C:60:4F:A9:A7:1F	Unconfigured	Physical	Admin Down	
1	0	25	8C:60:4F:A9:A7:20	Unconfigured	Physical	Admin Down	Disabled
1	0	26	8C:60:4F:A9:A7:21	Unconfigured	Physical	Admin Down	Disabled
1	0	27	8C:60:4F:A9:A7:22	Unconfigured	Physical	Admin Down	Disabled
1	ø	28	8C:60:4F:A9:A7:23	Unconfigured	Physical	Admin Down	Disabled
			8C:60:4F:A9:A7:24	Unconfigured		Admin Down	Disabled Disabled
		30	8C:60:4F:A9:A7:25	Unconfigured		Admin Down Admin Down	Disabled Disabled
		31 En	able	Unconfigured		Admin Down Admin Down	Usabled Disabled
1	9		sable	Unconfigured	Physical	Admin Down	Disabled
			onfigure as Server Port				
		Co	onfigure as Uplink Port				
		Ce	onfigure as FCoE Uplink Port				
			onfigure as FCoE Storage Port				

- 5. Repeat this same on Fabric B.
- 6. Create Port Channels: Under LAN tab, select expand LAN → LAN cloud → Fabric A. Right-click Port Channel.
- 7. Select Create port-channel to connect with upstream switch as per UCS best practice. For our reference architecture, we connected a pair of Nexus 9372PX switches.



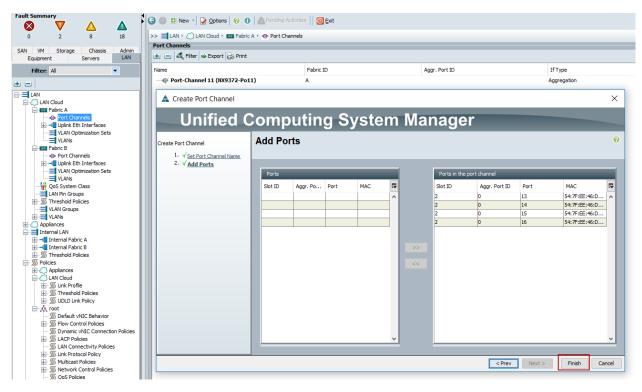
8. Enter port-channel ID number and name to be created, click Next.

SAN VM Storage Chassis Admin	Port Channels					
Equipment Servers LAN	🛨 😑 💐 Filter 👄 Export 👌	Print				
Filter: All	Name		Fabric ID	Aggr. Port ID	IfType	If Role
± =		72-Po11)	A		Aggregation	Network
LAN						
EAN Cloud		Create Port	Channel			X
Port Channels			channer			~
VLAN Optimization Sets		Uni	ried Comp	uting System Ma	anager	
VLANs						
- 🔤 Fabric B		Create Port Channel	Set Port	Channel Name		()
Uplink Eth Interfaces						
VLAN Optimization Sets			Channel Name			
VLANs		2. Add Port	L I			
LAN Pin Groups						
Threshold Policies ULAN Groups						
ULANS						
Appliances			ID: 11			
🖨 🚍 Internal LAN						
🖶 📲 Internal Fabric A						
Policies						
Appliances						
AN Cloud						
庄 🚿 Link Profile						
1 S Threshold Policies						
S Default vNIC Behavior			Name: NX93	72-Po11		
Flow Control Policies			0			
🗊 Dynamic vNIC Connection Policies						
LACP Policies						
LAN Connectivity Policies						
Ink Protocol Policy Multicast Policies						
Network Control Policies						
S QoS Policies					< Prev Next >	Finish Cancel
the exclusion terror						

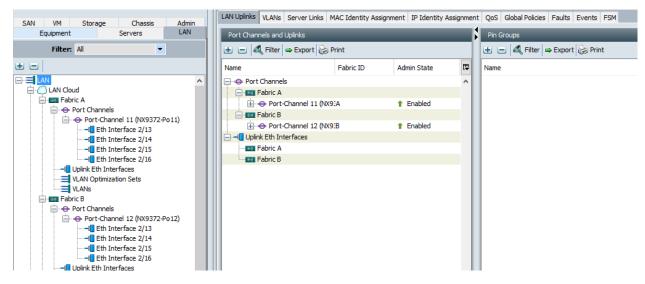
9. Select uplink ports to add as part of the port-channel.

SAN VM Storage Chassis Admin Equipment Servers LAN	🛨 🖃 🍕 Filter 👄 Export 🗞 Print									
Filter: All	Name		Fabric ID		Agg	gr. Port ID			If Type	
• -		11)	A						Aggregation	
	Create Port Channel	Compu	ting S	ystem	Mai	nage	r	_	_	×
VLAN Optimization Sets VLANs Image: Set	Create Port Channel 1. √ <u>Set Port Channel Name</u> 2. √ <u>Add Ports</u>	Add Ports								0
VLAN Optimization Sets		Ports			1	Ports in the	port channel			
		Slot ID Ar 2 0 2 0 2 0 2 0 2 0	ygr. Po Port 33 14 15 16 16	MAC ID 547.7125 5 547.7125 5 547.7125 5 547.7725 5	**	Slot ID	Aggr. Port ID	Port	MAC	9
S LAN Connectivity Policies										
Survey Control Policies							< Prev	Next >	Finish	Cancel

10. Click Finish.



11. Follow the previous steps to create the port-channel on Fabric B, using a different port-channel ID.



- 12. Configure QoS System Classes: From the LAN tab, below the Lan Cloud node, select QoS system class and configure the Platinum through Bronze system classes as shown in the following figure.
- Set MTU to 9216 for Platinum (Storage data) and Bronze (vMotion)
- Uncheck Enable Packet drop on the Platinum class
- Set Weight for Platinum and Gold priority class to 4 and everything else as best-effort.
- Enable multicast for silver class.

Equipment Servers LAN SAN VM Storage Chassis Admin	General Events F	SM						
Filter: All	Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	мти	Multicast Optimized
• =	Platinum	✓	5		4	33	9216	-
E- = LAN	Gold	✓	4	✓	4	33	normal	-
Fabric A	Silver	✓	2	✓	best-effort	8	normal	• •
	Bronze	✓	1	✓	best-effort	8	9216	-
LAN Pin Groups	Best Effort	✓	Any	✓	best-effort	8	normal	-
VLAN Groups	Fibre Channel	✓	3		best-effort	10	fc	▼ N/A
Appliances								
🗈 – 🗓 Internal Fabric A								
Internal Fabric B S Threshold Policies								
Policies								

- 13. Verify UCS Manager Software Version: In the Equipment tab, select Firmware Management → Installed Firmware.
- 14. Check and verify, both Fabric Interconnects and UCSM are configure with UCSM v3.1.2b.

Filter: Al	😑 🛃 Filter 🛥 Export 🍪 Print 🛞 Download Fin	8	and a second sec				
- Ner		Model	Running Version	Startup Version	Backup Version	Update Status	Activate Status
Equipment B.	🛕 UCS Manager		3.1(2b)	3.1(2b)	N/A	N/A	Ready
- Sector Chassis	- mjil Chassis						
FEX	Fabric Interconnects						
	Fabric Interconnect A (primary)	Cisco UCS 6248UP					
Tabric Interconnects	- 🛞 Kernel		5.0(3)N2(3.12b)	5.0(3)N2(3.12b)	N/A	N/A	Ready
E Fabric Interconnect A (primary)	- 🛞 System		5.0(3)N2(3.12b)	5.0(3)N2(3.12b)	N/A	N/A	Ready
Fixed Module	Fabric Interconnect B (subordinate)	Cisco UCS 6248UP					
Expansion Module 1	- 😵 Kernel		5.0(3)N2(3.12b)	5.0(3)N2(3.12b)	N/A	N/A	Ready
🕀 🛄 Fans			5.0(3)N2(3.12b)	5.0(3)N2(3.12b)	N/A	N/A	Ready
🕀 🙀 PSUs	😑 🐗 Rack-Mounts						
Fabric Interconnect 8 (subordinate)	🚍 🐗 Servers						
marked Module Expansion Module 1	😑 🐗 Server 1	Cisco HX220c M45 HyperFlex Syst.					
E - Mar Expansion Mobule 1	Adapters						
🕀 🙀 PSUs	Adapter 1	Cisco UCS MLOM 1227	4.1(2d)	4.1(2d)	4.1(1h)	Ready	Ready
	- TTT BIOS	Cisco HX220c M45 HyperFlex Syst.	. C220M4.2.0.13d.0.0812161113	C220M4.2.0.13d.0.0812161113	C220M4.2.0.10h.0.0812161111	Ready	Ready
	Board Controller	Cisco HX220c M45 HyperFlex Syst	. 32.0	NA	N/A	N/A	Ready
	CIMC Controller	Cisco HX220c M45 HyperFlex Syst.	. 2.0(13e)	2.0(13e)	2.0(10f)	Ready	Ready
	FlexFlash Controller 1		1.3.2 build 165		N/A	N/A	N/A
	Storage Controller PCH 3				N/A	N/A	
	Disks						
	Storage Controller SAS 1	Cisco 12G Modular SAS Pass thro	11.00.00.07	11.00.00.07	N/A	N/A	Ready
	😑 📕 Disks						
	- @ Disk 1	120 GB 2.5 inch Enterprise Value	C501	C501	N/A	N/A	Ready
	- Disk 2	480GB 2, 5 inch Enterprise perfor	C501	C501	N/A	N/A	Ready
	Disk 3	1.2TB 12G SAS 10K RPM SFF HDD	N003	N003	N/A	N/A	Ready
	- Disk 4	1.2 TB 12G SAS 10K RPM SFF HDD		A703	N/A	N/A	Ready
	- Disk 5	1.2 TB 12G SAS 10K RPM SFF HDD		A703	N/A	N/A	Ready
	Disk 6	1.2 TB 12G SAS 10K RPM SEE HDD	A703	A703	N/A	N/A	Ready
	Disk 7	1.2 TB 12G SAS 10K RPM SFF HDD	A703	A703	N/A	N/A	Ready
	Disk 8	1.2 TB 12G SAS 10K RPM SFF HDD		A703	N/A	N/A	Ready
	E-Server 2	Cisco HX220c M45 HyperFlex Syst.					,
	Server 3	Cisco HX220c M45 HyperFlex Syst.					
	- Contraction of the second se	Cisco HX220c M45 HyperFlex Syst.					
	Server 5	Cisco HX220c M46 HyperFlex Syst.					
	B Server 6	Cisco HX220c M4S HyperFlex Syst.					
	Server 7	Cisco HK220c M45 HyperFlex Syst.					
	A Server 8	Cisco HV220c M45 HyperFlex Syst					

Æ

It is recommended to let the HX Installer handle upgrading the server firmware automatically as designed. This will occur once the service profiles are applied to the HX nodes during the automated deployment process.

15. Optional: If you are familiar with UCSM or you wish to break the install into smaller pieces, you can use the server auto firmware download to pre-stage the correct firmware on the nodes. This will speed up the association time in the HyperFlex installer at the cost of running two separate reboot operations. This method is not required or recommended if doing the install in one sitting.

Deploy Cisco HyperFlex Data Platform Installer VM

Download latest installer OVA from Cisco.com. Software Download Link: <u>https://software.cisco.com/download/release.html?mdfid=286305544&flowid=79522&softwareid=2863059</u> 94&release=1.8(1c)&relind=AVAILABLE&rellifecycle=&reltype=latest

Deploy OVA to an existing host in the environment. Use either your existing vCenter Thick Client (C#) or vSphere Web Client to deploy OVA on ESXi host. This document outlines the procedure to deploy the OVA from the web client.

To deploy the OVA from the web client, complete the following steps:

- 1. Log into vCenter web client via login to web browser with vCenter management IP address: <u>https://<FQDN or IP address for VC>:9443/vcenter-client</u>
- 2. Select ESXi host under hosts and cluster when HyperFlex data platform installer VM to deploy.
- 3. Right-click ESXi host, select Deploy OVF Template.

vmware [®] vSphere Web Client	nt≣						
Navigator 🖡	🕝 vcsa6-c1.vdilab	hc.local Actions	*				
Home 🕑 🔞	Summary Monito	or Manage Rela	ated Objects				
Image: Constraint of the state of		vcsa6-c1.vdilab-hc Virtual Machines: 1 Hosts: {	135				
🖶 C1-VSIS 💛 New Resource Po				- Versio	on Information		
FileSrv0 Connection HX-Win Connection HX-Win Maintenance Mod		Category This list is empty.	Description	Version Build	6.0.0 3634794	att	
LoginVS Certificates Persona PVS01 Storage SoL-01 Add Networking		 • • • 					
VCSA6 Add Diagnostic Pa			Assign Remove				

- 4. Follow the deployment steps to configure HyperFlex data-platform installer VM deployment.
- 5. Select OVA file to deploy, click Next.

Deploy OVF Template		? ₩
1 Source	Select source Select the source location	
 1a Select source 1b Review details 2 Destination 2a Select name and folder 2b Select storage 3 Ready to complete 	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer such as a local hard drive, a network share, or a CD/DVD drive. URL • Local file Browse D:\Stryker-software\HX1.8.1B\Cisco-HX-Data-Platform-Installer-v1.8.1b-19547.ova	r,
	Back Next Finish Ca	ncel

6. Review and verify the details for OVF template to deploy, click Next.

Deploy OVF Template			? **
1 Source ✓ 1a Select source	Review details Verify the OVF tem	late details	
 Ib Review details 2 Destination 2a Select name and folder 2b Select storage 2c Setup networks 2d Customize template 3 Ready to complete 	Product Version Vendor Publisher Download size Size on disk Description	Cisco HyperFlex Installer 1.8.1b-19547 () Cisco Inc. (2) No certificate present 3.2 GB 5.0 GB (thin provisioned) 30.0 GB (thick provisioned)	
		Back	Next Finish Cancel

7. Enter name for OVF to template deploy, select datacenter and folder location. Click Next.

Deploy OVF Template		? >>
Deploy OVF Template	Select name and folder Specify a name and location for the deployed template Name: HXDPI-19547 Select a folder or datacenter Search Search Search ConePrepInternalTemplateFolder ConePrepRepInternalTemplateFolder ConePrepRepInternalTemplateFolder ConePrepRepInternalTemplateFolder ConePrepRepInternalTemplateFolder Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search Search S	The folder you select is where the entity will be located, and will be used to apply permissions to it. The name of the entity must be unique within each vCenter Server VM folder.
		Back Next Finish Cancel

8. Select virtual disk format, VM storage policy set to datastore default, select datastore for OVF deployment. Click Next.

1 Source 1a Selectsource	Select storage Select location to store the files for the deployed template									
1b Review details	Select virtual disk format:	Thick Provision Lazy Ze	roed							
2 Destination	VM Storage Policy:	Datastore Default	•	•						
2a Select name and folder	The following datastores a	re accessible from the de	m the destination resource that you selected. Select the destination datastore							
2b Select storage	virtual machine configurat									
2c Setup networks	Name	Capacity	Provisioned	Free	Туре	Storage DRS				
2d Customize template	C220M4-InfraDS01	1.74 TB	1.00 TB	761.86 GB	VMFS					
3 Ready to complete	datastore1 (5)	103.25 GB	18.73 GB	84.52 GB	VMFS					
	4					•				

9. Select Network adapter destination port-group.

De	ploy OVF Template							(?) ₩
	1 Source 1a Select source	Setup networks Configure the netwo	rks the deployed templ	ate should use				
÷	1b Review details		ource		Destinat	ion		Configuration
	2 Destination	VM Network		IBMgmt			-	O
~	2a Select name and folder							
~	2b Select storage							
~	2c Setup networks							
	2d Customize template 3 Ready to complete	IP protocol: IPv4		IP al	llocation:	Static - Manual 🚯		
		host. Destination: IBMgm	VM network is on the sa t-Protocol settings	me management network o	of host. Th	e installer VM must be able	to com	municate with
		No configuration ne	eded for this network					
						Back Next	Finish	Cancel

10. Fill out the parameters requested for hostname, gateway, DNS, IP address, and netmask. Alternatively, leave all blank for a DHCP assigned address.

Provide a single DNS server only. Inputting multiple DNS servers will cause queries to fail. You must connect to vCenter to deploy the OVA file and provide the IP address properties. Deploying directly from an ESXi host will not allow you to set these values correctly.

Deploy OVF Template		9				
1 Source ✓ 1a Selectsource	Customize template Customize the deployment	properties of this software solution				
 1b Review details 	All properties have valid	I values Show next Collapse all.				
2 Destination	* Name	1 setting				
 2a Select name and folder 	Hostname	The hostname for this VM Leave blank to try to reverse lookup the IP address.				
 2b Select storage 		HXDPI-19547				
 2c Setup networks 	+ Networking Properties	4 settings				
2d Customize template	Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired.				
3 Ready to complete		10.10.50.1				
	DNS	The domain name servers for this VM (comma separated). Leave blank if DHCP is desired.				
		10.10.51.21				
	Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 10.10.50.19 The netmask or prefix for this interface. Leave blank if DHCP is desired.				
	Network 1 Netmask					
		255.255.255.0				
		Back Next Finish Cancel				

If you have internal firewall rules between these networks, please contact TAC for assistance.

If required, an additional network adapter can be added to the HyperFlex Platform Installer VM after OVF deployment is completed successfully. For example, in case of a separate Inband and Out-Of-Mgmt network, see below:

🗄 HXDPI-19547 - Edit S	ettings	? »
Virtual Hardware VM C	Options SDRS Rules vApp Options	
F 🔲 CPU	3 🔹 🖬	
Memory	4096 V MB V	
▶ 🛄 Hard disk 1	30 GB 🗸	
▶ 🛃 SCSI controller 0	LSI Logic Parallel	
Network adapter 1	IBMgmt 🗸 Connected	
Network adapter 2	OOB-Mgmt 🗸 Connected	
▶ ▶ OD/DVD drive 1 	Client Device Connected	
Video card	Specify custom settings	
 المجافق المحافظة محافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة محافظة محافظة المحافظة محافظة المحافظة المحافظة محافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة محافظة محافظة محافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة محافظة المحافظة المحافظة محافظة محافظة محافظة محافظة محافظة محافظة محافظة محافظة محافظة المحافظة المحافظة محافظة مح محافظة محافظة محا		
 Other Devices 		
Upgrade	Schedule VM Compatibility Upgrade	

11. Review settings selected part of the OVF deployment, click on check box for Power on after deployment. Click Finish.

De	ploy OVF Template			? »
	1 Source	Ready to complete Review your settings selections before	ore finishing the wizard.	
~	1a Select source			
× .	1b Review details	OVF file	D:\Stryker-software\HX1.8.1B\Cisco-HX-Data-Platform-Installer-v1.8.1b-19547.ova	
	2 Destination	Download size	3.2 GB	
~	2a Select name and folder	Size on disk	30.0 GB	
1	2b Select storage	Name	HXDPI_19547	
	-	Datastore	C220M4-InfraDS01	
\sim	2c Setup networks	Target	10.10.50.67	
\checkmark	2d Customize template	Folder	Discovered virtual machine	
~	3 Ready to complete	Disk storage Network mapping IP allocation Properties	Thick Provision Lazy Zeroed VM Network to IBMgmt Static - Manual, IPv4 Hostname = HXDPI-19547 Default Gateway = 10.10.50.1 DNS = 10.10.51.21,10.10.51.22 Network 1 IP Address = 10.10.50.19 Network 1 Netmask = 255.255.255.0	
		✓ Power on after deployment		
			Back Next Finish Ca	ancel

The default credentials for the HyperFlex installer VM are: user name: root password: Cisco123

Verify or Set DNS Resolution

SSH to HX installer VM, verify or set DNS resolution is set on HyperFlex Installer VM:

```
root@Cisco-HX-Data-Platform-Installer: # more /etc/network/eth0.interface
auto eth0
iface eth0 inet static
metric 100
address 10.10.50.19
netmask 255.255.255.0
gateway 10.10.50.1
dns-search vdilab-hc.local
dns-nameservers 10.10.51.21 10.10.51.22
root@Cisco-HX-Data-Platform-Installer:~# more /run/resolvconf/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#
      DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.10.51.21
nameserver 10.10.51.22
search vdilab-hc.local
```

Cisco HyperFlex Cluster Configuration

To configuring the Cisco HyperFlex Cluster, complete the following steps:

1. Login to HX Installer VM through a web browser: http://staller_VM_IP_Address

ریابی) cisco Cisco HX Data Platform Installer	
tiltuite cisco HyperFlex	
L USERNAME PASSWORD ©	
I accept the terms and conditions Login	
	1.8(1b)

Create a HyperFlex Cluster

1. Select the workflow for cluster creation to deploy a new HyperFlex cluster on eight Cisco HX220c-M4S nodes.

alialia cisco	HyperFlex Installer		0	?	ø	\$ ~
		Workflow				
Se	lect a Workflow					-
		۵ م	, Ø. Ø. Ø			
	Cluster Creation	Cluster Exp	ansion			
	know what I'm doing, let me customize my workflow					

2. On the credentials page, enter the access details for UCSM, vCenter server, and Hypervisor. Click Continue.

HyperFlex Installer					0			¢ ~
Credentials	Server Selection	UCSM Configuration	Hypervisor Configuration	IP Addresses		Cluster	Configurati	on
Credentials UCS Manager Credentials UCS Manager Host Name 10.29.132.11 vCenter Credentials vCenter Server 10.10.50.20	Server Selection User Name admin User Name administrator@vsph		Hypervisor Configuration Password Admin Password		iguration	Cluster	Configurati	on the second seco
Hypervisor Credentials Admin User Name root	Admin Password				configur	ag and drop ation files ho	ere or	

- 3. Select the top-most check box at the top right corner of the HyperFlex installer to select all unassociated servers. (To configure a subset of available of the HyperFlex servers, manually click the check box for individual servers.)
- 4. Click Continue after completing server selection.

	Credentia	ls	Server Selection	UCSM	Configuration	Hypervisor Configu	iration	IP Addro	25565	Cluster	Configuration
Serve	er Select	tion			Со	nfigure Server Ports	Refresh		Configuratio	on	
Una	associated	i (8) Associated	I (0)						Credentials		
	-ġ-	Server Name	Status	Model	Serial	Assoc State	Actions		UCS Manager Ho	st Name	10.29.132.1
۲	0	Server 1	unassociated	HX220C-M4S	FCH1938V085	none	Actions ~		User Name vCenter Server		admi 10.10.50.2
•		Server 2	unassociated	HX220C-M4S	FCH1937V2JV	none	Actions ~		Üser Name	administrate	or@vsphere.loca
	(0))	Server 3	unassociated	HX220C-M4S	FCH1937V2TV	none	Actions ~		Admin User Nam	e	roc
•		Server 4	unassociated	HX220C-M4S	FCH1936V0GE	none	Actions ~				
		Server 5	unassociated	HX220C-M4S	FCH1937V2JU	none	Actions ~				
•		Server 6	unassociated	HX220C-M4S	FCH1937V2TS	none	Actions ~				
	00	Server 7	unassociated	HX220C-M4S	FCH1937V2JT	none	Actions ~				
	•	Server 8	unassociated	HX220C-M4S	FCH1842V1JG	none	Actions ~				
								4			
									< Back		Continue

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 Pre-requisites section above prior starting workflow for HyperFlex installer.

Configure Server Ports (Optional)

If you choose to allow the installer to configure the server ports, complete the following 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.

			Server Selection	UCSM					
erve	er Select	tion			> Confi	gure Server Ports	Refresh	Configuration	
Un	associated	d (8) Associated		Conf	figure Server Ports		×	Credentials	
		Server Name		Model List all			5		Name 10.29.132.11
	390	Server ristric		List an	ports to be configured as	server ports		User Name	admin
2		Server 1	unassociated	HX2200 A/1/	1-8, <u>B1</u> /1-8 ←		s ~	vCenter Server	10.10.50.20
2		Server 2	unassociated	HX2204			s ~	User Name	administrator@vsphere.local
		Server 3	unassociated	HX2200			s ~	Admin User Name	root
2		Server 4	unassociated	HX2200	Cancel	Config	ure s ~		
Z		Server 5	unassociated	HX2206-1414-5	rcn1957¥2ju	none	Actions ~		
		Server 6	unassociated	HX220C-M4S	FCH1937V2TS	none	Actions 🛩		
		Server 7	unassociated	HX220C-M45	FCH1937V2JT	none	Actions ~		
		Server 8	unassociated	HX220C-M45	FCH1842V1JG	none	Actions ~		

- 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 prerfix that does not conflict with any other MAC address pool across all 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".

- 5. 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 3.1(2b) which is the required Cisco UCS Manager release for HyperFlex v1.8.1 installation.
- 7. Enter HyperFlex cluster name.
- 8. Enter Org name to be created in UCSM.
- 9. Click Continue.

HyperFlex Inst	taller				0 0	0
Credentials	Server Selection	UCSM Configuration	Hypervisor Configuration	IP Addresses	Clus	ter Configuration
/LAN Configuration				Configu	ıration	
/LAN for Hypervisor and Hyp	erFlex management	VLAN for HyperFlex sto	orage traffic	Credentia	als	
/LAN Name	VLAN ID	VLAN Name	VLAN ID	LICS Manag	ger Host Name	10.29.132.
hx-inband-mgmt	→ 50	hx-storage-data	→ 52			
				User Name		adm
				vCenter Se		10.10.50.
/LAN for VM vMotion	VLAN ID	VLAN for VM Network	VLAN ID	User Name		ator@vsphere.lo
/LAN Name		VLAN Name		Admin Use	r Name	rc
hx-vmotion -	→ 53	vm-network	→ 54	Server Se	lection	
				Server 8	FCH1842	v1JG / HX220C-M
MAC Pool				Server 2	FCH1937	V2JV / HX220C-M
VIAC FOOI				Server 3	FCH1937	/2TV / HX220C-M
MAC Pool Prefix				Server 1	FCH1938	/085 / HX220C-M
00:25:B5: 22				Server 6	FCH1937	/2TS / HX220C-M
				Server 7	FCH1937	V2JT / HX220C-M
				Server 4	FCH1936V	/0GE / HX220C-M
ext-mgmt' IP Pool for (Out-of-band CIMC			Server 5	FCH1937	V2JU / HX220C-M
P Blocks	Subnet Mask	Gat	teway			
10.29.132.40-79	255.255.255.0	1	0.29.132.1			
Advanced						
	United States		g Name	4		
JCS Firmware Version	HyperFlex Cluster N	ame Org	givame	K Ba		Continue

Configure Hypervisor Settings

To configure the Hypervisor settings, complete the following steps:

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

s Server mmon Hypervisor Sett ettings esses and Hostnames Seque ne Serial er 1 FCH1938V er 2 FCH1937V	tings Gateway 10.10.50.1 ntial V085 10.10.50.27	JCSM Configuration	Hypervisor Configuration DNS Server(s) 10.10.51.22 Hostname HXVDI-01	IP Addresses Configurat USAN ID ULAN Name ULAN ID ULAN Name	hx-inband-mgn hx-inband-mgn hx-storage-da hx-vrmotic s hx-vrmotic s hx-vrmotic s
ettings esses and Hostnames Seque ne A Serial er 1 FCH1938V	Gateway 10.10.50.1 ntial Static IP Addres /085	55	10.10.51.22 Hostname	VLAN ID VLAN Name VLAN ID VLAN Name VLAN ID VLAN Name VLAN ID VLAN Name VLAN ID VLAN Name	hx-inband-mgn hx-inband-mgn hx-storage-da hx-vmotic hx-vmotic tix 00:25:B5:2
esses and Hostnames Seque ne - Serial er 1 FCH1938\	10.10.50.1 ntial V085 10.10.50.27	55	10.10.51.22 Hostname	VLAN ID VLAN Name VLAN ID VLAN Name VLAN ID VLAN Name VLAN ID MAC Pool Prefi	hx-storage-da
esses and Hostnames Seque ne - Serial er 1 FCH1938\	ntial Static IP Addres 10.10.50.27	55	Hostname	VLAN Name VLAN ID VLAN Name VLAN ID VLAN Name VLAN ID MAC Pool Prefi	hx-storage-da
esses and Hostnames Seque ne - Serial er 1 FCH1938\	Static IP Addres 0005 0.10.10.50.27	55		VLAN ID VLAN Name VLAN ID VLAN ID MAC Pool Prefi	s hx-vmotic vm-netwo s ix 00:25:B5:2
esses and Hostnames Seque ne - Serial er 1 FCH1938\	Static IP Addres 0005 0.10.10.50.27	55		VLAN Name VLAN ID VLAN Name VLAN ID MAC Pool Prefi	hx-vmotic ym-netwo ix 00:25:B5:2
ne A Serial	Static IP Addres 0005 0.10.10.50.27	55		VLAN ID VLAN Name VLAN ID MAC Pool Prefi	s vm-netwo s ix 00:25:85:2
ne A Serial	Static IP Addres 0005 0.10.10.50.27	SS		VLAN Name VLAN ID MAC Pool Prefi	vm-netwo 5 ix 00:25:85:2
er 1 FCH1938\	/085 10.10.50.27	SS		VLAN ID MAC Pool Prefi	š× 00:25:B5:2
			HXVDI-01	MAC Pool Prefi	īx 00:25:B5:2
			HXVDI-01		
er 2 FCH1937\	V2JV 10.10.50.28				10 29 132 40-7
C12 1C1115574	10110100120		HXVDI-02	IP Blocks	10.25.152.401
				Subnet Mask	255.255.255
er 3 FCH1937\	V2TV 10.10.50.29		HXVDI-03	Gateway	10.29.132
				UCS Firmware	Version 3.1(2
er 4 FCH1936	V0GE 10.10.50.30		HXVDI-04	HyperFlex Clus	ster Name HX-VDI-C
				Org Name	HX-VDI-O
er 5 FCH1937\	V2JU 10.10.50.31		HXVDI-05	Hypervisor Co	onfiguration
er 6 ECH1937	/2TS 10 10 50 32		HXVDI-06	Subnet Mask	255.255.255
				Gateway	10.10.50
er 7 FCH1937\	V2JT 10.10.50.33		HXVDI-07	DNS Server(s)	10.10.51.2
	10 10 50 24			4	
	er 5 FCH1937 er 6 FCH1937 er 7 FCH1937	er 5 FCH1937V2JU 10.10.50.31 er 6 FCH1937V2TS 10.10.50.32 er 7 FCH1937V2JT 10.10.50.33	er 5 FCH1937V2JU 10.10.50.31 er 6 FCH1937V2TS 10.10.50.32 er 7 FCH1937V2JT 10.10.50.33	er 5 FCH1937V2JU 10.10.50.31 HXVDI-05 er 6 FCH1937V2TS 10.10.50.32 HXVDI-06 er 7 FCH1937V2JT 10.10.50.33 HXVDI-07	FCH1937V2JU 10.10.50.31 HXVDI-05 Hypervisor C er 6 FCH1937V2TS 10.10.50.32 HXVDI-06 Subnet Mask er 7 FCH1937V2JT 10.10.50.33 HXVDI-07 DNS Server(s)

IP Addresses

To add the IP addresses, complete the following 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:
- Storage Controller/Management

- Hypervisor/Data
- Storage Controller/Data
- 2. Enter subnet and gateway details for the Management and Data subnets configured.
- 3. Click Continue to proceed.

cree	dentials	Server Selection	o com co	nfiguration	Hypervisor Configuration	IP Addresses	Cluster Configuration
P Addre					Add Server	Configuratio	
Make I	P Addresses Seque	ential				VLAN Name	hx-inband-mgn
		Manag	ement		Data	VLAN ID	5
lt ∻ 11	Server	Hypervisor 🕕	Storage Controller ①	Hypervisor	Storage Controller	VLAN Name	hx-storage-da
		,,				VLAN ID	5
= (0)	FCH1938V085	10.10.50.27	10.10.50.101	10.10.52.27	10.10.52.101	VLAN Name	hx-vmotic
	5511100710011	40.40.50.00	10.10.50.102	10.10.50.00	10.10.52.102	VLAN ID	5
= •	FCH1937V2JV	10.10.50.28	10.10.50.102	10.10.52.28	10.10.52.102	VLAN Name	vm-netwo
= (0)	FCH1937V2TV	10.10.50.29	10.10.50.103	10.10.52.29	10.10.52.103	VLAN ID	
						MAC Pool Prefix	00:25:B5:
•	FCH1936V0GE	10.10.50.30	10.10.50.104	10.10.52.30	10.10.52.104	IP Blocks	10.29.132.40-
						Subnet Mask	255.255.255
= 00	FCH1937V2JU	10.10.50.31	10.10.50.105	10.10.52.31	10.10.52.105	Gateway	10.29.132
	FCUI 027V2TC	10.10.50.32	10.10.50.106	10.10.52.32	10.10.52.106	UCS Firmware Ve	rsion 3.1(2
= (0.0)	FCH1937V2TS	10.10.50.32	10.10.50.106	10.10.52.32	10.10.52.106	HyperFlex Cluster	Name HX-VDI-
= 0D	FCH1937V2JT	10.10.50.33	10.10.50.107	10.10.52.33	10.10.52.107	Org Name	HX-VDI-O
						Hypervisor Con	figuration
= 00	FCH1842V1JG	10.10.50.34	10.10.50.108	10.10.52.34	10.10.52.108	Subnet Mask	255.255.255
						Gateway	10.10.50
						DNS Server(s)	10.10.51.2
			Management	Data		4	
		Subnet Mask	255.255.255.0	255.255.255.0		< Back	Continue
			Management	Data			
		Gateway	10.10.50.1	10.10.52.1			

- 4. On the Cluster Configuration page, enter the following:
 - Cluster Name
 - Cluster management IP address
 - Cluster data IP Address
 - Set Replication Factor: 2 or 3
 - Controller VM password
 - vCenter configuration
 - o vCenter Datacenter name

- o vCenter Cluster name
- System Services
 - DNS Server(s)
 - NTP Server(s)
 - o Time Zone
- Auto Support
 - o Click on check box for Enable Auto Support
 - o Mail Server
 - o Mail Sender
 - ASUP Recipient(s)
- Advanced Networking
 - o Management vSwitch
 - o Data vSwitch
- Advanced Configuration
 - o Click on check box to Optimize for VDI only deployment
 - o Enable jumbo Frames on Data Network
 - Clean up disk partitions (optional)
- vCenter Single-Sign-On server

<mark>២</mark> HyperFlex Instal	ler				• •		
Credentials	Server Selection U	JCSM Configuration	Hypervisor Configuration	IP Addresses	(Cluster Configurati	ion
Cisco HX Cluster					guration		
luster Name	Cluster Management IP Ad	dress Clus	ter Data IP Address	VLAN Na	-	by inband a	
HX-VDI-CL	10.10.50.100	1	0.10.52.100			hx-inband-n	
eplication Factor				VLAN ID			5
				VLAN Na		hx-storage	
				VLAN ID			5
				VLAN Na	me	hx-vm	otio
ontroller VM				VLAN ID			5
reate Admin Password	Confirm Admin Password			VLAN Na	me	vm-net	wor
				VLAN ID			5
				MAC Poo	l Prefix	00:25:8	85:2
				IP Blocks	2	10.29.132.4	40-7
Center Configuration				Subnet I	Mask	255.255.2	255.
Center Datacenter Name	vCenter Cluster Name			Gateway		10.29.1	132.
				UCS Firm	nware Version	3.	.1(2t
VDILAB-HX	HX-VDI-CL			HyperFle	ex Cluster Name	HX-V	DI-C
				Org Nan	ne	HX-VD	I-Or
ystem Services				Hyperv	isor Configurati	on	
NS Server(s)	NTP Server(s)	Time Zone		Subnet I	Mask	255.255.2	255.
10.10.51.22	10.10.50.2	(UTC-08:	00) Pacific Time	▼ Gateway	1	10.10).50.
10.10.01.22	10.10.50.2			DNS Ser	ver(s)	10.10.5	5

				A Paul (Aquite	HX-VITIOU011
Auto Support				VLAN ID	53
Auto 6	Mail Server	Mail Sender		VLAN Name	vm-network
Auto Support	Mail Server	Mali Sender		VLAN ID	54
Enable Auto Support				MAC Pool Prefix	00:25:B5:22
ASUP Recipient(s)	-			IP Blocks	10.29.132.40-79
				Subnet Mask	255.255.255.0
]			Gateway	10.29.132.1
				UCS Firmware Version	3.1(2b)
Advanced Networking				HyperFlex Cluster Name	HX-VDI-CL
Management vSwitch	Data vSwitch			Org Name	HX-VDI-Org
vswitch-hx-inband-mgmt	vswitch-hx-storage-data			Hypervisor Configuration	
				Subnet Mask	255.255.255.0
				Gateway	10.10.50.1
Advanced Configuration				DNS Server(s)	10.10.51.22
Virtual Desktop (VDI)	Jumbo Frames	Disk Partitions	4		÷
Optimize for VDI only deployment	闭 Enable Jumbo Frames on Data Network	 Clean up disk partitions 		< Back	Start
vCenter Single-Sign-On Server	-				
https:// <address>:7444/sts/STSService</address>					

- 5. The configuration details can be exported to a JSON file by clicking the down arrow icon in the top right corner of the Web browser page as shown in the screenshot below.
- 6. Configuration details can be reviewed on Configuration page on right side section. Verify entered details for IP address entered in Credentials page, server selection for cluster deployment and creation workflow, UCSM configuration, Hypervisor Configuration, IP addresses.
- 7. Click Start after verifying details.

HyperFlex Insta	ller				• •	
Credentials	Server Selection	UCSM Configuration	Hypervisor Configuration	IP Addresses	Tech Support	Onfiguration
Cisco HX Cluster				Configura	ation	
Cluster Name	Cluster Managen	nent IP Address	Cluster Data IP Address	Credentials		
HX-VDI-CL	10.10.50.100		10.10.52.100	UCS Manager	Host Name	10.29.132.1
eplication Factor				User Name		adm
3 🔻				vCenter Serve	۶r	10.10.50.2
				User Name	administrato	r@vsphere.loc
Controller VM				Admin User N	lame	ro
				Server Selec	tion	
reate Admin Password	Confirm Admin P	assword		Server 8	FCH1842V1J	G / HX220C-M4
				Server 2	FCH1937V2J	V / HX220C-M4
				Server 3	FCH1937V2T	V / HX220C-M4
Center Configuration				Server 1	FCH1938V08	5 / HX220C-M4
Center Datacenter Name	vCenter Cluster N	Jame		Server 6		S / HX220C-M4
VDILAB-HX	HX-VDI-CL			Server 7		T / HX220C-M4
				Server 4		E / HX220C-M4
				UCSM Confi		J / HX220C-M4
System Services				VLAN Name		ıx-inband-mgn
DNS Server(s)	NTP Server(s)	Tim	e Zone	VLAN Name VLAN ID	ſ	ix-inband-mgn
10.10.51.22	10.10.50.2	(U	TC-08:00) Pacific Time	V		

Once started installation workflow, it will go through Cisco UCS Manager validation.

11: 10:	yperFlex Inst							0	8 📀 1	1
					Progress					_
0	0							Configuration		
Start	UCSM	UCSM	Hypervisor	Deploy	Deploy	Create	Cluster	VLAN Name	hx-vmotion	1
	Validation	Configuration	Configuration	Validation		Validation	Creation	VLAN ID	53	3
								VLAN Name	vm-network	ĸ
2	characterization of	2						VLAN ID	54	4
) uc	SM Validation i	n Progress						MAC Pool Prefix	00:25:B5:22	2
								IP Blocks	10.29.132.40-79	э
					U	CSM Validation	•	Subnet Mask	255.255.255.0	0
	UCSM Validation	- Overall						Gateway	10.29.132.1	1
	_	Progress	 Login to UCS 					UCS Firmware Version	3.1(2b))
			 Inventory physical 	ysical servers				HyperFlex Cluster Name	HX-VDI-CL	L
			 Validate the state 	etup/environment				Org Name	HX-VDI	1
								Hypervisor Configura	tion	
								Subnet Mask	255.255.255.0	0
								Gateway	10.10.50.1	1
								DNS Server(s) 1	0.10.51.21,10.10.51.22	2
								IP Addresses		
								Management	255.255.255.0	D
								Data	255.255.255.0	D
								Management	10.10.50.1	ŗ
								Data	10.10.52.1	ſ
								Cluster Configuration		
								Cluster Name	HX-VDI-CL	L

After a successful validation, the workflow continues with the Cisco UCS Manager configuration.

HyperFlex Installer						0 (
			Progress				
0-00						Configuration	
Start UCSM UCSM Validation Configura	Hypervisor ion Configuration	Deploy Validation	Deploy	Create Validation	Cluster Creation	Management	255.255.255.0
Teles C	0					Data	255.255.255.0
						Management	10.10.50.1
C UCSM Configuration in Prog	ess					Data	10.10.52.1
						Cluster Configuration	
						Cluster Name	HX-VDI-CL
			UCSN	I Configuration	•	Cluster Management IP A	ddress 10.10.50.100
UCSM Configuration - Overall	 Login to UCS A 	API				Cluster Data IP Address	10.10.52.100
In Progress	 Validate UCS fi 	irmware version				Replication Factor	3
	✓ Get inventory	of firmware bundles				vCenter Datacenter Nam	vDILAB-HX
	 Download firm 	nware bundle				vCenter Cluster Name	HX-VDI-CL
	 Activating infra 	a bundle version				DNS Server(s) 10	0.10.51.21,10.10.51.22
	✓ Configure UCS	Fabric Interconnect				NTP Server(s)	10.10.50.2,10.10.50.3
	 Configure FI Set 	erver Ports				Time Zone	America/Los_Angeles
	✓ Configure QoS	classes				Auto Support	
	 Configure org 	for the hx cluster				Management VLAN Tag	0
	 Inventory physical 	sical servers				Management vSwitch vsv	vitch-hx-inband-mgmt
	 Configure VLA 	Ns				Data VLAN Tag	0
	 Configure Hos 	t Firmware policy					witch-hx-storage-data
	✓ Configure MAC	Caddress pools				Virtual Desktop (VDI)	VDI
	 Configure QoS 	policies				Jumbo Frames	
	✓ Configure Net	work Control policies				Disk Partitions	

After a successful Cisco UCS Manager configuration, the installer proceeds with the Hypervisor configuration.

HyperFlex Installer					0 0	Ø
		Progress				
○ ─── ⊘ ─── ⊘ =	0				Configuration	
Start UCSM UCSM Validation Configuratio	Hypervisor Deploy on Configuration Validation	Deploy	Create Validation	Cluster Creation	IP Addresses	
					Management	255.255.255.
					Data	255.255.255.
Hypervisor Configuration in Pr	rogress				Management	10.10.50.
,, ,	5				Data	10.10.52.
					Cluster Configuration	
		Hypervisor	Configuration	•	Cluster Name	HX-VDI-C
Hypervisor Configuration - Overall	 Login to UCS API 				Cluster Management IP Addres	s 10.10.50.10
In Progress	 Configure static ip on the specified 	esxi servers			Cluster Data IP Address	10.10.52.10
	C Create threads to configure static ip	on the esxi servers			Replication Factor	
					vCenter Datacenter Name	VDILAB-H
					vCenter Cluster Name	HX-VDI-C
					DNS Server(s) 10.10.5	1.21,10.10.51.2
					NTP Server(s) 10.10	0.50.2,10.10.50.
					Time Zone Ame	rica/Los_Angele
					Auto Support	
					Management VLAN Tag	
					Management vSwitch vswitch-	hx-inband-mgm
					Data VLAN Tag	
					Data vSwitch vswitch	-hx-storage-dat
					Virtual Desktop (VDI)	VE
					Jumbo Frames	
					Disk Partitions	

After a successful Hypervisor configuration and deploy validation, the installer begins to configure the HyperFlex controller VMs on each HX220c nodes with the IP address information provided earlier.

					Progress					
0		(С			Configuration		
Start	UCSM Validation	UCSM Configuration	Hypervisor Configuration	Deploy Validation	Deploy	Create Validation	Cluster Creation	IP Addresses		
		0						Management	255.255.	255.0
								Data	255.255.	255.0
Deploy	in Progress							Management	10.10).50.1
								Data	10.10).52.1
								Cluster Configuratio	on	
						Deploy	•	Cluster Name	HX-V	DI-CL
	Deploy -	Overall						Cluster Management I	IP Address 10.10.5	0.100
	In Pi	rogress						Cluster Data IP Addres	ss 10.10.5	2.100
	10.10.50.27							Replication Factor		3
	_	rogress	 Configuring 	Hypervisor				vCenter Datacenter N	ame VDILA	B-HX
			 Preparing E Basic ESX Co 	SXi Host for Installatio	on			vCenter Cluster Name	HX-V	DI-CL
			 Initializing C 					DNS Server(s)	10.10.	51.22
			create comp					NTP Server(s)	10.10.50.2,10.10).50.3
				torage Controller VM				Time Zone	America/Los_An	geles
			Configuring	Network (Port Group	os) for ESXi and Stora	ge Controller VM		Auto Support		- 1
								Management VLAN Ta	ig	0
		10.50.28	 Configuring 	Hypervisor				Management vSwitch	vswitch-hx-inband-r	- 1
	In Pi	rogress		5Xi Host for Installatio	on			Data VLAN Tag		0
			Basic ESX Co					Data vSwitch	vswitch-hx-storage	- 1
			 Initializing C create comp 	onfiguration ute group				Virtual Desktop (VDI)		VDI
			_ Deploying S	torage Controller VM	on ESXi Host			Jumbo Frames		- 1

After a successful deployment of the ESXi hosts configuration, the Controller VM software components for HyperFlex installer checks for validation prior to creating the cluster.

' HyperFlex Installer						0 0	Ø
			Progress				
0	(>			C		Configuration	
Start Validations UCSM Configuration	Hypervisor Configuration	Deploy Validation	Deploy	Create Validation	Cluster Creation	Credentials	
						UCS Manager Host Name	10.29.132.1
						User Name	adm
Create Validation in Progress						vCenter Server	10.10.50.2
						User Name administ	rator@vsphere.loc
						Admin User Name	ro
			Cr	eate Validation	•	Server Selection	
Create Validation - Overall						Server 8 FCH1936	V0GE / HX220C-M4
In Progress						Server 2 FCH193	7V2JT / HX220C-M4
						Server 3 FCH193	7V2JU / HX220C-M4
						Server 1 FCH1937	7V2TV / HX220C-M4
						Server 6 FCH1937	7V2TS / HX220C-M4
						Server 7 FCH193	7V2JV / HX220C-M4
						Server 4 FCH1938	3V085 / HX220C-M4
						Server 5 FCH184	2V1JG / HX220C-M4
						UCSM Configuration	
						VLAN Name	hx-inband-mgn

After a successful validation, the installer creates and starts the HyperFlex cluster service.

lili. cisco	HyperFlex Insta	aller						0		0	\$ ~
					Progress						
								_			
0-		(>					0	Configuration	on		
Start	Validations	UCSM Configuration	Hypervisor Configuration	Deploy Validation	Deploy	Create Validation	Cluster Creation	Credentials			^
								UCS Manager Ho	st Name	10.29.13	2.11
								User Name		ad	min
\mathbf{C}	Cluster Creation ir	n Progress						vCenter Server		10.10.5	0.20
								User Name	administrate	or@vsphere.l	ocal
								Admin User Nam	e	I	root
					CI	uster Creation	•	Server Selectio	n		
	Cluster Creation							Server 8	FCH1936V00	GE / HX220C-I	44S
	In	Progress						Server 2	FCH1937V2	JT / HX220C-I	V145
								Server 3	FCH1937V2	JU / HX220C-I	VI45
								Server 1	FCH1937V2	TV / HX220C-I	VI4S
								Server 6	FCH1937V2	TS / HX220C-I	V145
								Server 7	FCH1937V2	JV / HX220C-I	VI45
								Server 4	FCH1938V0	85 / HX220C-I	VI45
								Server 5	FCH1842V1	JG / HX220C-I	VI4S
								UCSM Configur	ation		
								VLAN Name		hx-inband-m	gmt 🖕
								4			÷

After a successful HyperFlex Installer VM workflow completion, the installer GUI provides a summary of the cluster that has been created.

		Progress			Summary	
Cluster Name	HX-VDI-CL ONLI	INE HEALTHY				
Version			1.8.1b-19537	vCenter Server		10.10.50.2
Cluster Manager	ment IP Address		10.10.50.100	vCenter Datacenter Name	e	VDILAB-H
Cluster Data IP A	Address		10.10.52.100	vCenter Cluster Name		HX-VDI-C
Replication Facto	or		3	DNS Server(s)		10.10.51.2
Available Capaci	ty		17.7 TB	NTP Server(s)		10.10.50.3, 10.10.50.
Servers						
Model	Serial Number	Management Hypervisor	Management Storage (Controller Data Networ	k Hypervisor Data Network	Storage Controller
HX220C-M4S	FCH1937V2TV	10.10.50.27	10.10.50.101	10.10.52.27	10.10.52.101	
HX220C-M4S	FCH1937V2JT	10.10.50.28	10.10.50.102	10.10.52.28	10.10.52.102	
		10 10 50 31	10.10.50.105	10.10.52.31	10.10.52.105	
HX220C-M45	FCH1842V1JG	10.10.50.31	10.10.50.105		10.10.52.105	
	FCH1842V1JG FCH1937V2JU	10.10.50.29	10.10.50.103	10.10.52.29	10.10.52.103	
HX220C-M4S						
HX220C-M4S HX220C-M4S	FCH1937V2JU	10.10.50.29	10.10.50.103	10.10.52.29	10.10.52.103	
HX220C-M4S HX220C-M4S HX220C-M4S	FCH1937V2JU FCH1937V2TS	10.10.50.29	10.10.50.103	10.10.52.29	10.10.52.103	
HX220C-M45 HX220C-M45 HX220C-M45 HX220C-M45	FCH1937V2JU FCH1937V2TS FCH1938V085	10.10.50.29 10.10.50.32 10.10.50.30	10.10.50.103 10.10.50.106 10.10.50.104	10.10.52.29 10.10.52.32 10.10.52.30	10.10.52.103 10.10.52.106 10.10.52.104	

As part of the cluster creation operations, the HyperFlex Installer adds HyperFlex functionality to the vSphere vCenter identified in earlier steps. This functionality allows vCenter administrators to manage the HyperFlex cluster entirely from their vSphere Web Client.

8. Click Launch vSphere Web Client.

Cisco HyperFlex installer creates and configured a controller VM on each converged or compute-only node. Naming convention used is as "stctlvm-<Serial Number for Cisco UCS Node>" shown in Figure 39.



Do **not** to change name or any resource configuration for controller VM.

avigator I	VDI-CL Actions -										-
Home > 🔊	Summary Monitor Manage Related	Dhiects									
	Communy monitor manage Related	bljects									
vcsa6.vdilab-hc.local	Top Level Objects Hosts Virtual Machine	s vApps Datas	tores Datastor	e Clusters Networks	Distributed Switc	hes					
HX-VDILAB					1						
▶ 🗊 HX-Infra	🔰 🔁 🐌 📝 🕨 🔳 🧐 🖧	🔯 Actions 👻								📡 📑 (Q Filter	
HX-Launcher	Name 1	▲ State	Status	Provisioned Space	Used Space	Host CPU	Host Mem	EVC Mode	HA Protection		
⇒¶ VDI-CL >	1 W10-FC99	Powered On	O Normal	78.06 GB	44.93 GB	103 MHz	1,444 MB		Protected		
10.10.50.27	W10-FC98	Powered On	O Normal	78.06 GB	44.93 GB	103 MHz	1,445 MB		Protected		
10.10.50.28	W10-FC97	Powered On	Normal	78.06 GB	44.98 GB	103 MHz	1,455 MB		Protected		
10.10.50.29	W10-FC96	Powered On	Normal	78.06 GB	44.97 GB	129 MHz	1,252 MB		Protected		
10.10.50.30	3 W10-FC95	Powered On	 Normal 	78.06 GB	44.94 GB	0 MHz	77 MB		Protected		
10.10.50.31	W10-FC94	Powered On	Normal	78.06 GB	44.9 GB	0 MHz	81 MB		Protected		
10.10.50.32	W10-FC93	Powered On	 Normal 	78.04 GB	44.9 GB	0 MHz	0 MB		Protected		
10.10.50.33	W10-FC92	Powered On	Normal	78.06 GB	44.95 GB	103 MHz	1,457 MB		Protected		
10.10.50.34	M W10-FC91	Powered On	Normal	78.06 GB	44.94 GB	103 MHz	1,406 MB		Protected		
	W10-FC90	Powered On	Normal	78.06 GB	44.96 GB	0 MHz	79 MB		Protected		
stCtIVM-FCH1842V	W10-FC9	Powered On	Normal	78.06 GB	44.94 GB	103 MHz	1,536 MB		Protected		
stCtlVM-FCH1937V	W10-FC89	Powered On	Normal	78.05 GB	44.94 GB	0 MHz	77 MB		Protected		
stCtlVM-FCH1937V	W10-FC88	Powered On	Normal	78.06 GB	44.97 GB	103 MHz	1.307 MB		Protected		
stCtlVM-FCH1937V	W10-FC87	Powered On	Normal	78.06 GB	44.96 GB	0 MHz	990 MB		Protected		
stCtIVM-FCH1937V	W10-FC86	Powered On	Normal	78.05 GB	44.96 GB	0 MHz	988 MB		Protected		
stCtlVM-FCH1937V	W10-FC85	Powered On	Normal	78.06 GB	44.97 GB	0 MHz	1,109 MB		Protected		
stCtIVM-FCH1938V	W10-FC84	Powered On	Normal	78.06 GB	44.98 GB	103 MHz	1,634 MB		Protected		
🕨 🚰 (819) Virtual Machines		Powered On	Normal	78.06 GB	44.95 GB	0 MHz	902 MB		Protected		
	W10-FC82	Powered On	 Normal 	78.06 GB	44.95 GB	0 MHz	669 MB		Protected		
	W10-FC81	Powered On	 Normal 	78.06 GB	44.97 GB	103 MHz	1,666 MB		 Protected 		
	W10-FC80	Powered On	 Normal 	78.06 GB	44.97 GB	0 MHz	107 MB		Protected		
	W10-FC8	Powered On	 Normal 	78.06 GB	44.93 GB	103 MHz	1,447 MB		 Protected Protected 		
	M WID-FC8	1 owered On	Vivornal	70.00 GB	44.95 GB	103 WHZ	1,447 1018		- Flotected	827 Object	

Figure 39 Cisco UCS Node Naming Convention

Run Cluster Post Installation Script

After a successful installation of HyperFlex cluster, run the post_install script by loging into the Data Platform Installer VM via SSH, using the credentials configured earlier.

A built-in post install script automates basic final configuration tasks like enabling HA/DRS on HyperFlex cluster, configuring vmKernel for vMotion interface, creating datastore for ESXi logging, etc., as shown in the following figures.

root@Cisco-HX-Data-Platform-Installer:~# post install Getting ESX hosts from HX cluster... vCenter URL: 10.10.50.20 Enter vCenter username (user@domain): administrator@vsphere.local vCenter Password: Found datacenter VDILAB-HX Found cluster HX-VDI-CL Enable HA/DRS on cluster? (y/n) y Disable SSH warning? (y/n) y Configure ESXi logging onto HX datastore? (y/n) y No datastores found Creating datastore ... Name of datastore: HX-Logs Size (GB): 100 Storing logs on datastore HX-Logs Creating folder [HX-Logs]/esxi logs Add vmotion interfaces? (y/n) y Netmask for vMotion: 255.255.255.0 VLAN ID: (0-4096) 53 vMotion IP for 10.10.50.27: 10.10.53.27 Adding vmotion to 10.10.50.27 Adding vmkernel to 10.10.50.27 vMotion IP for 10.10.50.28: 10.10.53.28 Adding vmotion to 10.10.50.28 Adding vmkernel to 10.10.50.28 vMotion IP for 10.10.50.29: 10.10.53.29 Adding vmotion to 10.10.50.29 Adding vmkernel to 10.10.50.29 vMotion IP for 10.10.50.30: 10.10.53.30 Adding vmotion to 10.10.50.30 Adding vmkernel to 10.10.50.30 vMotion IP for 10.10.50.31: 10.10.53.31 Adding vmotion to 10.10.50.31 Adding vmkernel to 10.10.50.31 vMotion IP for 10.10.50.32: 10.10.53.32 Adding vmotion to 10.10.50.32 Adding vmkernel to 10.10.50.32 vMotion IP for 10.10.50.33: 10.10.53.33 Adding vmotion to 10.10.50.33 Adding vmkernel to 10.10.50.33 vMotion IP for 10.10.50.34: 10.10.53.34 Adding vmotion to 10.10.50.34 Adding vmkernel to 10.10.50.34

```
Add VM network VLANs? (y/n) n
Enable NTP on ESX hosts? (y/n) y
Starting ntpd service on 10.10.50.27
Starting ntpd service on 10.10.50.28
Starting ntpd service on 10.10.50.30
Starting ntpd service on 10.10.50.31
Starting ntpd service on 10.10.50.32
Starting ntpd service on 10.10.50.33
Starting ntpd service on 10.10.50.34
Send test email? (y/n) n
Validating cluster health and configuration...
Found UCSM 10.29.132.11, logging with username admin. Org is hx-vdi-org
UCSM Password:
```

- 1. To run the script, first use your tool of choice to make a secure connection to the Cisco HyperFlex Data Platform installer using it's IP address and port 22.
- 2. Authenticate with the credentials provided earlier. (user name: root with password Cisco 123 if you did not change the defaults.)
- 3. Once authenticated, enter post_install at the command prompt, then press Enter.
- 4. Provide a valid vCenter administrator user name and password and the vCenter url IP address.
- 5. Type y for yes to each of the promts that follow except Add VM network VLANs? (y/n) where you can choose whether or not to send health status data via SMS to Cisco support.
- 6. Provide the requested user credentials, the vMotion netmask, VLAN ID and an IP address on the vMotion VLAN for each host when prompted for the vmkernel IP.
- 7. Sample post install input and output:

```
root@Cisco-HX-Data-Platform-Installer:root@Cisco-HX-Data-Platform-
Installer:~#post_install Getting ESX hosts from HX cluster...
vCenter URL: 10.10.50.20
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Found datacenter VDILAB-HX
Found cluster HX-VDI-CL
Enable HA/DRS on cluster? (y/n) y
Disable SSH warning? (y/n) y
Configure ESXi logging onto HX datastore? (y/n) y
```

No datastores found Creating datastore... Name of datastore: HX-Logs Size (GB): 100 Storing logs on datastore HX-Logs Creating folder [HX-Logs]/esxi_logs Add vmotion interfaces? (y/n) y Netmask for vMotion: 255.255.255.0 VLAN ID: (0-4096) 53 vMotion IP for 10.10.50.27: 10.10.53.27 Adding vmotion to 10.10.50.27 Adding vmkernel to 10.10.50.27 vMotion IP for 10.10.50.28: 10.10.53.278 Adding vmotion to 10.10.50.28 Adding vmkernel to 10.10.50.28 vMotion IP for 10.10.50.29: 10.10.53.289 Adding vmotion to 10.10.50.29 Adding vmkernel to 10.10.50.29 vMotion IP for 10.10.50.30: 10.10.53.2930 Adding vmotion to 10.10.50.30 Adding vmkernel to 10.10.50.30 vMotion IP for 10.10.50.31: 10.10.53.301 Adding vmotion to 10.10.50.31 Adding vmkernel to 10.10.50.31 vMotion IP for 10.10.50.32: 10.10.53.312 Adding vmotion to 10.10.50.32 Adding vmkernel to 10.10.50.32 vMotion IP for 10.10.50.33: 10.10.53.323 Adding vmotion to 10.10.50.33 Adding vmkernel to 10.10.50.33 vMotion IP for 10.10.50.34: 10.10.53.334 Adding vmotion to 10.10.50.34

Adding vmkernel to 10.10.50.34 Add VM network VLANs? (y/n) n Enable NTP on ESX hosts? (y/n) y Starting ntpd service on 10.10.50.27 Starting ntpd service on 10.10.50.28 Starting ntpd service on 10.10.50.29 Starting ntpd service on 10.10.50.30 Starting ntpd service on 10.10.50.31 Starting ntpd service on 10.10.50.32 Starting ntpd service on 10.10.50.33 Starting ntpd service on 10.10.50.34 Send test email? (y/n) n Validating cluster health and configuration... Found UCSM 10.29.132.11, logging with username admin. Org is hx-vdi-org UCSM Password: TChecking MTU settings Pinging 10.10.52.107 from vmk1 Pinging 10.10.52.101 from vmk1 Pinging 10.10.52.105 from vmk1 Pinging 10.10.52.108 from vmk1 Pinging 10.10.52.102 from vmk1 Pinging 10.10.52.104 from vmk1 Pinging 10.10.52.106 from vmk1 Pinging 10.10.52.103 from vmk1 Setting vnic2 to active and vmnic3 to standby Pinging 10.10.52.107 from vmk1 Pinging 10.10.52.107 with mtu 8972 from vmk1 Pinging 10.10.52.101 from vmk1 Pinging 10.10.52.101 with mtu 8972 from vmk1 Pinging 10.10.52.105 from vmk1 Pinging 10.10.52.105 with mtu 8972 from vmk1 Pinging 10.10.52.108 from vmk1

Pinging 10.10.52.108 with mtu 8972 from vmk1 Pinging 10.10.52.102 from vmk1 Pinging 10.10.52.102 with mtu 8972 from vmk1 Pinging 10.10.52.104 from vmk1 Pinging 10.10.52.104 with mtu 8972 from vmk1 Pinging 10.10.52.106 from vmk1 Pinging 10.10.52.106 with mtu 8972 from vmk1 Pinging 10.10.52.103 from vmk1 Pinging 10.10.52.103 with mtu 8972 from vmk1 Setting vmnic3 to active and vnic2 to standby Pinging 10.10.50.33 from vmk0 Pinging 10.10.50.27 from vmk0 Pinging 10.10.50.31 from vmk0 Pinging 10.10.50.34 from vmk0 Pinging 10.10.50.28 from vmk0 Pinging 10.10.50.30 from vmk0 Pinging 10.10.50.32 from vmk0 Pinging 10.10.50.29 from vmk0 Setting vnic1 to active and vmnic0 to standby Pinging 10.10.50.33 from vmk0 Pinging 10.10.50.27 from vmk0 Pinging 10.10.50.31 from vmk0 Pinging 10.10.50.34 from vmk0 Pinging 10.10.50.28 from vmk0 Pinging 10.10.50.30 from vmk0 Pinging 10.10.50.32 from vmk0 Pinging 10.10.50.29 from vmk0 Setting vmnic0 to active and vnic1 to standby Pinging 10.10.53.27 from vmk2 Pinging 10.10.53.28 from vmk2 Pinging 10.10.53.29 from vmk2 Pinging 10.10.53.30 from vmk2

Pinging 10.10.53.31 from vmk2 Pinging 10.10.53.32 from vmk2 Pinging 10.10.53.33 from vmk2 Pinging 10.10.53.34 from vmk2 Setting vnic7 to active and vmnic6 to standby Pinging 10.10.53.27 from vmk2 Pinging 10.10.53.27 with mtu 8972 from vmk2 Pinging 10.10.53.28 from vmk2 Pinging 10.10.53.28 with mtu 8972 from vmk2 Pinging 10.10.53.29 from vmk2 Pinging 10.10.53.29 with mtu 8972 from vmk2 Pinging 10.10.53.30 from vmk2 Pinging 10.10.53.30 with mtu 8972 from vmk2 Pinging 10.10.53.31 from vmk2 Pinging 10.10.53.31 with mtu 8972 from vmk2 Pinging 10.10.53.32 from vmk2 Pinging 10.10.53.32 with mtu 8972 from vmk2 Pinging 10.10.53.33 from vmk2 Pinging 10.10.53.33 with mtu 8972 from vmk2 Pinging 10.10.53.34 from vmk2 Pinging 10.10.53.34 with mtu 8972 from vmk2 Setting vmnic6 to active and vnic7 to standby Network Summary: Host: 10.10.50.27 vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance srcid vmnic0 - 1 - K22-HXVDI-A - active vmnic1 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN Storage Controller Management Network - 50 Management Network - 50 vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid vmnic4 - 1 - K22-HXVDI-A - active

vmnic5 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN vm-network-54 - 54 vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid vmnic6 - 1 - K22-HXVDI-A - active vmnic7 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN vmotion - 53 vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid vmnic2 - 1 - K22-HXVDI-A - standby vmnic3 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN Storage Controller Data Network - 52 Storage Hypervisor Data Network - 52 Host: 10.10.50.28 vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance_srcid vmnic0 - 1 - K22-HXVDI-A - active vmnic1 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN Storage Controller Management Network - 50 Management Network - 50 vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid vmnic4 - 1 - K22-HXVDI-A - active vmnic5 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN vm-network-54 - 54 vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid vmnic6 - 1 - K22-HXVDI-A - active vmnic7 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN vmotion - 53 vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid

```
vmnic2 - 1 - K22-HXVDI-A - standby
      vmnic3 - 1 - K22-HXVDI-B - active
       Portgroup Name - VLAN
       Storage Controller Data Network - 52
        Storage Hypervisor Data Network - 52
Host: 10.10.50.29
   vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance srcid
      vmnic0 - 1 - K22-HXVDI-A - active
      vmnic1 - 1 - K22-HXVDI-B - standby
       Portgroup Name - VLAN
       Storage Controller Management Network - 50
       Management Network - 50
   vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid
      vmnic4 - 1 - K22-HXVDI-A - active
      vmnic5 - 1 - K22-HXVDI-B - active
       Portgroup Name - VLAN
       vm-network-54 - 54
   vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid
      vmnic6 - 1 - K22-HXVDI-A - active
     vmnic7 - 1 - K22-HXVDI-B - standby
       Portgroup Name - VLAN
       vmotion - 53
   vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid
      vmnic2 - 1 - K22-HXVDI-A - standby
      vmnic3 - 1 - K22-HXVDI-B - active
       Portgroup Name - VLAN
       Storage Controller Data Network - 52
        Storage Hypervisor Data Network - 52
Host: 10.10.50.30
  vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance srcid
     vmnic0 - 1 - K22-HXVDI-A - active
      vmnic1 - 1 - K22-HXVDI-B - standby
```

Portgroup Name - VLAN Storage Controller Management Network - 50 Management Network - 50 vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid vmnic4 - 1 - K22-HXVDI-A - active vmnic5 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN vm-network-54 - 54 vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid vmnic6 - 1 - K22-HXVDI-A - active vmnic7 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN vmotion - 53 vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid vmnic2 - 1 - K22-HXVDI-A - standby vmnic3 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN Storage Controller Data Network - 52 Storage Hypervisor Data Network - 52 Host: 10.10.50.31 vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance srcid vmnic0 - 1 - K22-HXVDI-A - active vmnic1 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN Storage Controller Management Network - 50 Management Network - 50 vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid vmnic4 - 1 - K22-HXVDI-A - active vmnic5 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN vm-network-54 - 54 vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid

```
vmnic6 - 1 - K22-HXVDI-A - active
     vmnic7 - 1 - K22-HXVDI-B - standby
       Portgroup Name - VLAN
       vmotion - 53
   vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid
      vmnic2 - 1 - K22-HXVDI-A - standby
     vmnic3 - 1 - K22-HXVDI-B - active
       Portgroup Name - VLAN
       Storage Controller Data Network - 52
       Storage Hypervisor Data Network - 52
Host: 10.10.50.32
  vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance srcid
     vmnic0 - 1 - K22-HXVDI-A - active
     vmnic1 - 1 - K22-HXVDI-B - standby
       Portgroup Name - VLAN
       Storage Controller Management Network - 50
       Management Network - 50
   vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid
      vmnic4 - 1 - K22-HXVDI-A - active
     vmnic5 - 1 - K22-HXVDI-B - active
       Portgroup Name - VLAN
       vm-network-54 - 54
   vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid
      vmnic6 - 1 - K22-HXVDI-A - active
      vmnic7 - 1 - K22-HXVDI-B - standby
       Portgroup Name - VLAN
       vmotion - 53
   vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid
     vmnic2 - 1 - K22-HXVDI-A - standby
     vmnic3 - 1 - K22-HXVDI-B - active
       Portgroup Name - VLAN
        Storage Controller Data Network - 52
```

Storage Hypervisor Data Network - 52 Host: 10.10.50.33 vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance srcid vmnic0 - 1 - K22-HXVDI-A - active vmnic1 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN Storage Controller Management Network - 50 Management Network - 50 vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid vmnic4 - 1 - K22-HXVDI-A - active vmnic5 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN vm-network-54 - 54 vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid vmnic6 - 1 - K22-HXVDI-A - active vmnic7 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN vmotion - 53 vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance srcid vmnic2 - 1 - K22-HXVDI-A - standby vmnic3 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN Storage Controller Data Network - 52 Storage Hypervisor Data Network - 52 Host: 10.10.50.34 vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance_srcid vmnic0 - 1 - K22-HXVDI-A - active vmnic1 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN Storage Controller Management Network - 50 Management Network - 50 vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance srcid

vmnic4 - 1 - K22-HXVDI-A - active vmnic5 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN vm-network-54 - 54 vswitch: vmotion - mtu: 9000 - policy: loadbalance srcid vmnic6 - 1 - K22-HXVDI-A - active vmnic7 - 1 - K22-HXVDI-B - standby Portgroup Name - VLAN vmotion - 53 vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance_srcid vmnic2 - 1 - K22-HXVDI-A - standby vmnic3 - 1 - K22-HXVDI-B - active Portgroup Name - VLAN Storage Controller Data Network - 52 Storage Hypervisor Data Network - 52 Host: 10.10.50.27 No errors found Host: 10.10.50.28 No errors found Host: 10.10.50.29 No errors found Host: 10.10.50.30 No errors found Host: 10.10.50.31 No errors found Host: 10.10.50.32 No errors found Host: 10.10.50.33 No errors found Host: 10.10.50.34

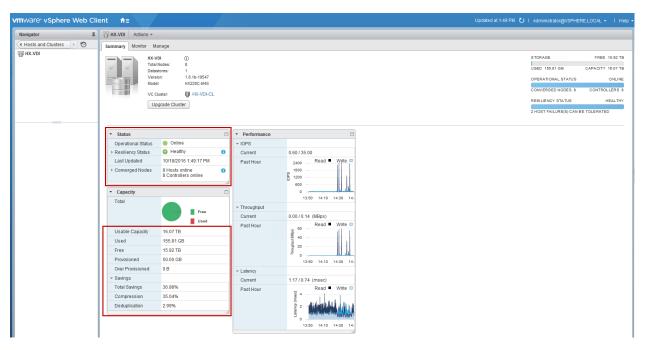
No errors found

```
Controller VM Clocks:
    stCtlVM-FCH1937V2JV - 2016-10-07 05:32:09
    stCtlVM-FCH1937V2TV - 2016-10-07 05:32:25
    stCtlVM-FCH1842V1JG - 2016-10-07 05:32:41
    stCtlVM-FCH1936V0GE - 2016-10-07 05:32:57
    stCtlVM-FCH1937V2JT - 2016-10-07 05:33:14
    stCtlVM-FCH1938V085 - 2016-10-07 05:33:30
    stCtlVM-FCH1937V2TS - 2016-10-07 05:33:46
    stCtlVM-FCH1937V2JU - 2016-10-07 05:34:02
Cluster:
    Version - 1.8.1b-19537
    Model - HX220C-M4S
    Health - HEALTHY
    Access Policy - LENIENT
    ASUP enabled - False
    SMTP Server -
root@Cisco-HX-Data-Platform-Installer:~#
```

- 8. Login to vSphere WebClient to create additional shared datastore.
- 9. Go to the Summary tab on the cluster created via the HyperFlex cluster creation workflow.
- 10. On Cisco HyperFlex Systems click the cluster name.

avigator 🗸	HX-VDI-CL Actions	-						7
Cisco HX Data Pla 🕨 🕲	Summary Monitor Ma	anage Related Objects						
Image: Construction Image: Construction Image: Construction of the co	Tota Tota	VDI-CL 224 Il Processors: 224 Il vMotion Migrations: 0					CPU USED: 2.66 GHz MEMORY USED: 430.75 GB STORAGE USED: 48.48 GB	FREE: 578.17 GH CAPACITY: 580.83 GH FREE: 3.58 T CAPACITY: 40.03 T FREE: 40.03 T CAPACITY: 40.08 T
 10.10.50.29 10.10.50.30 10.10.50.31 10.10.50.32 	Cluster Resources vSphere HA			vSphere DRS Cluster Consumers				
10.10.50.33 10.10.50.34	• Tags			Related Objects				
► @ ESX Agents B HX-Win10	Cisco HyperFlex Sy Name Capacity Free Savings Total Savings	Image: stems Image: stems 16.07 TB 15.92 TB 36.98%	Dat	atacenter <u>A</u> HX-VDILAB	More Related Objects			

The Summary tab shows details about the cluster status, capacity and performance.



11. Click Manage, select Datastores. Click the Add datastore icon, select the datastore name and size to provision.

vmware [,] vSphere Web Cli	ent f i≘						Updated at 1:49 PM 👌 Administrator@VSPHERE.LOCAL + Help		
Navigator I	HX-VDI Actions -				Create New Datastore				
📢 Hosts and Clusters 🕞 🧐	Summary Monitor	anage ←							
립 HX-VDI	Cluster Datastores			_	Datastore name: hx-vdl-ds				
_	▶3 ୯ 🗸 🗟 🗟	🛃 🎡 Actions 🕶			Size:		Q Filter		
	Name		Mount Status			Used	Free		
	HX-ESXILogs		Normal		OK Cancel	2.48 MB	50.00 GB		
							1 of 1 🔒 🛩		
	Summary Hosts Details		Trends						
	Total	Free Used	IOPs	14 — 12 — 10 —					
	Status	Normal		_{رہ} 8 –					
	Provisioned	50.00 GB		S IOPS	hard a low hard a hearth war is a datable				
	Used	2.48 MB		4	hit in the second second in the second s				
	Free	50.00 GB		2 -					
	Hosts	8		m-m	and an an analysis and the second second second second				
	VMs	0			14:01 14:11 14:21 14:31 14:41 14:51				
	Top VMs by Disk Us	age							
	Name	Size							

We created 40TB datastore for Horizon pooled persistent/non-persistent and RDSH server desktop performance test.

Building the Virtual Machines and Environment for Workload Testing

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

Horizon 7 Infrastructure Components Installation

The prerequisites for installing the view connection server, replica server(s) and composer server is to have Windows 2008, 2012 or 2012 R2 virtual machines ready. In this study, we used Windows Server 2012 R2 virtual machines for all Horizon infrastructure servers.

Download the VMware Horizon 7 installation package from this link: https://my.vmware.com/web/vmware/info?slug=desktop_end_user_computing/vmware_horizon/7_0

This section provides a detailed, step-by-step installation process for Horizon 7 v7.0.1.

Install VMware Horizon Composer Server

To install the VMware Horizon Composer Server, complete the following steps:

- 1. Open installer for Horizon composer. VMware-viewcomposer-7.0.1-3978853.exe
- 2. Click Next to continue.

岁 VN	Nware Horizon 7 Composer
	Welcome to the Installation Wizard for VMware Horizon 7 Composer
	The installation wizard will install VMware Horizon 7 Composer on your computer. To continue, click Next.
VMware Horizon™7	Copyright © 1998-2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and
Composer ലpcത്ര	intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
	< Back Next > Cancel

3. Accept the EULA. Click Next.



4. Click Next to accept the default installation folder.

虔	VMware Horizon 7 Composer
	tion Folder xt to install to this folder, or click Change to install to a different folder.
	Install VMware Horizon 7 Composer to: C:\Program Files (x86)\VMware\VMware View Composer\ Change
InstallShield	< Back Next > Cancel

5. Enter the database information. The ODBC database can be configured during the installation by clicking ODBC DSN Setup.

VMware Horizon 7 Composer
abase Information Iter additional database configuration information.
ter the Data Source Name (DSN) for the VMware Horizon 7 Composer database. To set up DSN dick the ODBC Setup button.
orizonComposer ODBC DSN Setup
iter the username that you entered in the ODBC Data Source Administrator. IorizonService
eter the password for this database connection.

Configure the ODBC Source Name

1. Open 64bit ODBC, select System DSN tab and click Add.

ODBC Data Source Administrator (64-bi	t)
User DSN System DSN File DSN Drivers Tracing Connection Pooling About	E
System Data Sources:	
Name Platform Driver	Add
	Remove
	Configure
An ODBC System data source stores information about how to connect to A System data source is visible to all users on this machine, including NT s	the indicated data provider. services.
OK Cancel	Apply Help

2. Create new Data source, select SQL server native client. We are using existing instanace of Mircosoft SQL server 2012 for current deployment. Click Finish.

	Name SQL Server	Versi	ion .9600.17415	Com Micro
011	SQL Server Native	and the second se		Micro
	< 111			>

3. Create a name for data source, select SQL server, click Next.

SQL Server 2012	SQL Server.	you create an ODBC data source that you cr vant to use to refer to the data source?	an use to connect to
	Description:	describe the data source?	
	Which SQL Server d	o you want to connect to? SQL01.vdilab-hc.local	~
	[Finish Next > Cancel	Help

4. Enter login credentails for SQL server authentication or use Windows Authentication. Click Next.

	Create a New Data Source to SQL Server
SQL Server 2012	How should SQL Server verify the authenticity of the login ID? O With Integrated Windows authentication. SEN (Optional): With SQL Server authentication using a login ID and password entered by the user.
	Login ID: HorizonService Password:
	< <u>B</u> ack <u>N</u> ext > Cancel Help

5. Select Default Database, click Next.

No.	Change the default database to:	
en la	HorizonComposer	Y
SQL Server 2012	Mirror server:	
	SPN for mirror server (Optional):	
	Attach database filename:	
	✓ Use ANSI quoted identifiers.	
	Use ANSI nulls, paddings and warnings.	
	Application intent:	
	READWRITE	~
	Multi-subnet failover.	

6. Check the box to select language for SQL server system messages. Click Finish.

SQL Server 2012	English	
	Perform translation for character data	
	Use regional settings when outputting currency, numbers, d	ates and times.
	Save long running queries to the log file:	
	C:\Users\ADMINI~1\AppData\Local\Temp\1\QUEI	Browse
	Long query time (milliseconds): 300)00
	Log ODBC driver statistics to the log file:	
	C:\Users\ADMINI~1\AppData\Local\Temp\1\STA1	Browse

- 7. Click Test datastore to verify connectivity between SQL server and newly create Data source.
- 8. Since this a new instanace of Composer server installation, a new SSL certificate will be created. In case of update or existing composer server installation either create new SSL certificate or use existing certificate.
- 9. Leave default port configuration for SOAP port.
- 10. Click Next.

B	VMware Horizon 7 Composer	x
And the second s	con 7 Composer Port Settings nection information for the VMware Horizon 7 Composer.	6
Specify the wel	o access port and security settings for VMware Horizon 7 Composer.	
SOAP Port:	18443	
SSL Certificate:	No SSL certificates were found on your machine. A default SSL certificate will be created for you.	
InstallShield	< Back Next >	Cancel

11. Click Install .

閿	VMware Horizon 7 Composer
R	The wizard is ready to begin installation.
	VMware Horizon 7 Composer will be installed in:
	C:\Program Files (x86)\VMware\VMware View Composer\
	If you want to review or change any of your installation settings, click Back. Click Install to begin the installation or Cancel to exit the wizard.
Inst	allShield < Back Install Cancel

12. Click Finish.

岁 VN	Iware Horizon 7 Composer	x
	Installer Completed The installer has successfully installed VMware Horizon 7 Composer. Click Finish to exit the wizard.	
vMware Horizon™7 Composer ല്₽c⊚ഈ		
	< Back Finish Cancel	

Install Horizon Connection/Replica Servers

To install the Horizon Connection/Replica Servers, complete the following steps:

- 1. Open view connection server installation, VMware-viewconnectionserver-x86_64-7.0.1-3988955.exe.
- 2. Click Next.

岁 VMwar	e Horizon 7 Connection Server
P	Welcome to the Installation Wizard for VMware Horizon 7 Connection Server
	The installation wizard will install VMware Horizon 7 Connection Server on your computer. To continue, click Next.
vMware Horlzon™7 Connection Server	Copyright (c) 1998-2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
Product version: 7.0.1-3988955 >	x64 < Back Next > Cancel

3. Accpet the EULA, click Next.

谩	VMware Horizon 7 Connection Server	x
	Agreement ead the following license agreement carefully.	6
VMWAR	RE END USER LICENSE AGREEMENT	-
LICENS THE SO	E NOTE THAT THE TERMS OF THIS END USER SE AGREEMENT SHALL GOVERN YOUR USE OF OF TWARE, REGARDLESS OF ANY TERMS THAT PPEAR DURING THE INSTALLATION OF THE IARE.	~
● I accept t	the terms in the license agreement	
○ I do not a	accept the terms in the license agreement	
2	< Back Next > Cancel	

4. Leave default destination folder, click Next.

闄	VMware Horizon 7 Connection Server
	nation Folder Next to install to this folder, or click Change to install to a different folder.
	Install VMware Horizon 7 Connection Server to: C:\Program Files\VMware\VMware View\Server\ Change
	< Back Next > Cancel

- 5. Select type of instance intended to install.
- 6. Select Standard Server instance for primary connection server installation.

B VMwa	re Horizon 7 Connection Server	
Installation Options	Ū,	
Select the type of Horizon 7 (Connection Server instance you want to install.	
Select the type of Horizon 7 C	Connection Server instance you want to install.	
Horizon 7 Standard Server	TRACES AND	
Horizon 7 Replica Server Horizon 7 Security Server Horizon 7 Enrollment Server	Install HTML Access	
Connection Server or the first instance of a group of servers. Specify what IP protocol version shall be used to configure this Horizon 7 Connection Se instance:		
IPv4	This server will be configured to choose the IPv4	
IPv6	protocol for establishing all connections.	

7. Select Replica server instance for fault tolerant connection server configration after completion of Standard Server instance installation.

B VMware I	Horizon 7 Connection Server	
Installation Options Select the type of Horizon 7 Conr	nection Server instance you want to install.	
Select the type of Horizon 7 Conn	ection Server instance you want to install.	
Horizon 7 Standard Server Horizon 7 Replica Server Horizon 7 Security Server Horizon 7 Enrollment Server	☑ Install HTML Access	
Perform a replica instance install joining an existing server instance. This is used to install a second or subsequent server in a group of servers that all automatically share the same directory configuration. Specify what IP protocol version shall be used to configure this Horizon 7 Connection Server instance:		
IPv4 IPv6	This server will be configured to choose the IPv4 protocol for establishing all connections.	
<u></u>	< Back Next > Cancel	

8. Enter Data recovery password.

👸 VMware Horiz	zon 7 Connection Server
Data Recovery Enter data recovery password details.	69
This password protects data backups of y will require entry of this password.	our Horizon 7 Connection Server. Recovering a backup
Enter data recovery password:	•••••
Re-enter password:	•••••
Enter password reminder (optional):	Default
-	< Back Next > Cancel

9. Click Next.

B	VMware Horizon 7 Connection Server
Autom	Il Configuration matically configure the Windows Firewall to allow incoming TCP protocol ections.
ports for th (JMS	der for Horizon 7 Connection Server to operate on a network, specific incoming TCP s must be allowed through the local Windows Firewall service. The incoming TCP ports he Standard Server are 8009 (AJP13), 80 (HTTP), 443 (HTTPS), 4001 (JMS), 4002 -SSL), 4100 (JMSIR), 4101 (JMSIR-SSL), 4172 (PCoIP), 8472 (Inter-pod API), and 8 (HTML Access). UDP packets on port 4172 (PCoIP) are allowed through as well.
	 Configure Windows Firewall automatically Do not configure Windows Firewall
	< Back Next > Cancel

10. Select authorized users and group, click Next.

₿	VMware Horizon 7 Connection Server
Initial	Horizon 7 Administrators
Speci	ify the domain user or group for initial Horizon 7 administration.
Adminis	to Horizon 7 Administrator, you will need to be authorized. Select the local trators group option or enter the name of a domain user or group that will be initially to login and will be granted full admistrative rights.
The list Adminis	of authorized administrator users and groups can be changed later in Horizon 7 trator.
C	Authorize the local Administrators group
(Authorize a specific domain user or domain group
	VDILAB-VS \administrator
	(domainname\username, domainname\groupname or UPN format)
	< Back Next > Cancel

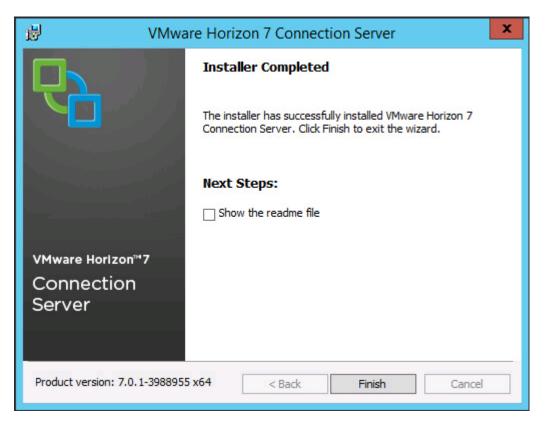
- 11. Opt-in or Opt-out of User Experience Improvement Program.
- 12. Click Next.

₿	VMware Horizon 7 Con	nection Server	x
	rience Improvement Program tomer Demographics		₽
help us in th completely a	onstantly trying to improve the user experie is effort by agreeing to send product usage anonymous, and is restricted to product usa the VMware user experience improvement	e statistics. This data is ge metrics. For more details	
Partici	pate anonymously in the user experience in	nprovement program	
Select your (organization industry type:		~
Select locati	on of your organization's headquarter:		~
Select appro	wimate number of employees:		~
. <u> </u>			
	< Back	Next > C	ancel

13. Click Install.

谩	VMware Horizon 7 Connection Server
	Install the Program rd is ready to begin installation.
VMware	Horizon 7 Connection Server will be installed in:
C:\Prog	ram Files\VMware\VMware View\Server\
Click Ins	tall to begin the installation or Cancel to exit the wizard.
	< Back Install Cancel

14. Click Finish.



Create a Microsoft Management Console Certificate Request

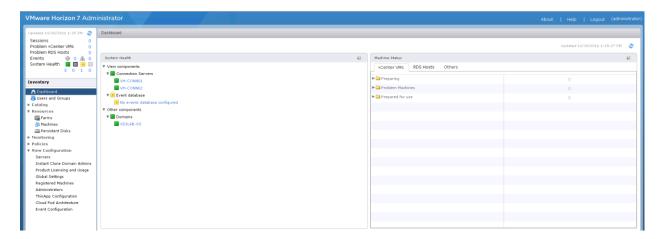
To generate a Horizon View SSL certificate request, use the Microsoft Management Console (MMC) Certificates snap-in:

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=206 8666

Configure the Horizon 7 Environment

To configure the Horizon 7 environment, complete the following steps:

1. Open WebUI, Login to https://<Horizon_Connection_server_Management_IP_Address>/admin.



Configure Event Database

To configure the Event Database, complete the following steps:

- 1. Configure the Event Database by adding Database Server, Database name, login credentials and prefix for the table from the Horizon 7 Administrator, View Configuration, Event Configuration node of the Inventory pane.
- 2. Click Edit in the action pane.

	VMware Horizon 7 Adm					
	Updated 11/30/2016 1:25 PM 👌	Event Configuration				
	Sessions 0 Problem vCenter VMs 0 Problem RDS Hosts 0	Event Database			Syslog	
	Events 0 0 A 0 System Health	Edit No database has been defined, events will not be recorded. Click 'Edit' to spec	ify a databaco corvor		Configure syslog event la recommended.	ogging using one o
	3 0 1 0	Event Settings			Send to syslog servers:	Add
I	Inventory	Event settings cannot be configured until a database server has been specified.				
I	🖓 Dashboard					
I	👸 Users and Groups					
I	▶ Catalog				Log to file:	Enable
I	▼ Resources				Copy to location:	
I	Machines					Add
I	Persistent Disks		Edit Event Database	9		
I	▶ Monitoring					
I	► Policies		Database server:			
I	▼ View Configuration		Database type:	Microsoft SQL Serve	er 💌	
I	Servers Instant Clone Domain Admins		Database type.			
I	Product Licensing and Usage		Port:	1433		
I	Global Settings		Database name:			
I	Registered Machines				<u> </u>	
I	Administrators		User name:			
I	ThinApp Configuration		Password:			
I	Cloud Pod Architecture				<u> </u>	
I	Event Configuration		Confirm password:		(
			Table prefix:			
				ок С	ancel	

Details are shown below:

Edit Event Database	
Database server:	SQL01
Database type:	Microsoft SQL Server 🗸 –
Port:	1433
Database name:	HorizonEvent
User name:	HorizonAgent
Password:	****
Confirm password:	****
Table prefix:	VE_
	OK Cancel

Configure Horizon 7 Licenses

To configure the Horizon 7 licenses, complete the following steps:

1. Click View Configuration.

- 2. Select Product Licensing and Usage.
- 3. Click Edit License in the action pane.
- 4. Add the License Serial Number.
- 5. Click OK

VMware Horizon 7 Adm	inistrator					
Updated 11/30/2016 1:25 PM	Licensing and Usage					
Sessions 0 Problem vCenter VMs 0 Problem RDS Hosts 0	Licensing					Customer Experience Program
Events 🛛 🕼 0 🛕 0 System Health 📕 🔲 💌	Edit License					Edit Settings
3010	A No valid license present for View	Manager. Click Edit to ad	d a valid license.			Send anonymous data to VMware Off
Inventory						Geographic Location:
R Dashboard						Business Vertical:
📇 Users and Groups						Number of Employees:
► Catalog						
▼ Resources	Usage					
📸 Parins 🚰 Machines 🚐 Persistent Disks	Reset Highest Count Reset Named U	sers Count			æ	
► Monitoring	Session Mode	Cu	urrent	н	ighest	
 Policies View Configuration 	Total Concurrent Connections	0		0		
Servers	Total Named Users	1		N/A		
Instant Clone Domain Admins	Detailed Connection Breakdown					
Product Licensing and Usage	Total Remote	0	Edit Li	cense		
Global Settings	Active - full virtual machines	0	Licons	e serial number: *		
Registered Machines Administrators	Active - linked clone	0	Licens	e senai number:		
Administrators ThinApp Configuration	Active - other machine sources	0				
Cloud Pod Architecture	Active - applications	0				OK Cancel
Event Configuration				1		

Configure vCenter

To configure the vCenter, complete the following steps:

- 1. In View Configuration, Select Servers. Click Add vCenter Server tab.
- 2. Enter vCenter Server IP Address or FQDN, login credentials.
- 3. Advanced Settings options can be modified to change existing operations limit. We left advanced settings options to default.

Add vCenter Server	vCenter Server Inform	ation	
VC Information	vCenter Server Setti	nas	vCenter Server Settings
View Composer Storage Ready to Complete	Server address:	vcsa6u2.vdilab-vs.local	Before you add vCenter Server to View, install a valid SSL certificate signed by a trusted CA. In a test
Ready to Complete	User name:	administrator@vsphere.local	environment, you can use the
	Password:	*****	default, self-signed certificate that is installed with vCenter Server, but
	Description:		you must accept the certificate thumbprint.
	Port:	443	Provide the vCenter Server FQDN or IP address, user name, and password.
	Advanced Settings		Concurrent Operations Limits
	Specify the concurrent Max concurrent vCent	ar	Max concurrent vCenter provisioning operations: the maximum number of concurrent VM cloning and deletion
	provisioning operation	20	operations on this vCenter server (full clones).
	Max concurrent power operations:	50	Max concurrent power operations:
	Max concurrent View Composer maintenant operations:	12	the maximum number of concurrent VM power-on, power-off, reset, and configuration operations (full clones and linked clones).
	Max concurrent View Composer provisionin operations:	g 8	Max concurrent View Composer maintenance operations: the
	May consurrant Insta-	t Clana	maximum number of concurrent View

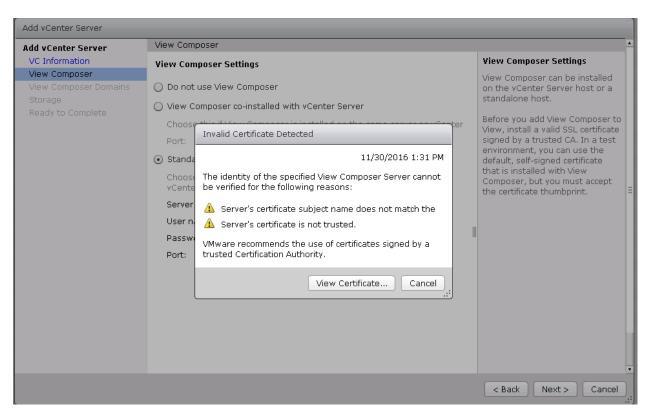
4. Click View certificate. Accept the certificate.

Add vCenter Server			
Add vCenter Server	vCenter Server Informa	ition	
VC Information	vCenter Server Settin	qs	vCenter Server Settings
View Composer Storage Ready to Complete	Server address: User name:	vcsa6u2.vdilab-vs.local administrator@vsphere.local	Before you add vCenter Server to View, install a valid SSL certificate signed by a trusted CA. In a test environment, you can use the
	Password Invalid Cert	ificate Detected	default, self-signed certificate that is installed with vCenter Server, but
	Descriptio	11/30/2016 1:30 PM	you must accept the certificate thumbprint.
	Port: verified for	r of the specified vCenter Server cannot be the following reasons:	Provide the vCenter Server FQDN or IP address, user name, and password.
	Advanced Advanced Specify th Max concu provisioni VMware rec	8	Concurrent Operations Limits Max concurrent vCenter provisioning operations: the maximum number of concurrent VM cloning and deletion operations on this vCenter server (full clones). Max concurrent power operations:
			Next > Cancel

- 5. Add View composer settings, View composer server FQDN or Management IP address, login credentials.
- 6. Click Next.

Add vCenter Server			
Add vCenter Server	View Composer		
VC Information	View Composer Set	ttings	View Composer Settings
View Composer View Composer Domains Storage Ready to Complete	 Do not use View View Composer of Choose this if Vie Port: 18443 Standalone View 	Composer co-installed with vCenter Server w Composer is installed on the same server as vCenter	View Composer can be installed on the vCenter Server host or a standalone host. Before you add View Composer to View, install a valid SSL certificate signed by a trusted CA. In a test environment, you can use the default, self-signed certificate that is installed with View Composer, but you must accept the certificate thumbprint.
			< Back Next > Cancel

7. View and accept certificate.



- 8. Click Add a new domain or Edit existing domain.
- 9. Click Next.

Add vCenter Server	View Composer Domai	ns		
Add vCenter Server VC Information View Composer	View Composer Doma	sins		View Composer Domains View Composer adds computer
View Composer Domains Storage Ready to Complete	Add Edit	Remove User administrator	Desktop Pool De	accounts for linked-clone machines in the AD domains configured here. The View Composer user accounts for the domains must have Create Computer Objects , Delete Computer Objects , and Write All Properties permissions in the domains. When you create a linked-clone desktop pool, you select a domain from this list to store the computer accounts.
				< Back Next > Cancel

- 10. In Storage settings, select Reclaim VM disk space and View Storage Accelarator.
- 11. Configure default host cache size between 100MB and 2048MB. We configured the maximum, which is 2048MB.
- 12. Click Next.

Add vCenter Server					
Add vCenter Server	Storage				
VC Information	Storage Settings		Storage Settings		
View Composer View Composer Domains Storage	✓ Reclaim VM disk space	ESXi hosts can be configured to cache virtual machine disk data, which improves performance			
Ready to Complete	Enable View Storage Accelerator		during I/O storms such as when		
	Default host cache size: 2048	MB	many machines power on and run anti-virus scans at once. Hosts		
	Cache must be between 100 MB ar	read common data blocks from cache instead of reading the OS			
	Hosts	from disk.			
	Edit cache size		By reducing IOPS during boot storms, View Storage Accelerator		
			lowers the demand on the storage array and uses less		
	Host	Cache Size	storage I/O bandwidth.		
	/VDILAB-VS/host/VDI-GPU/10.10.10.	Default	Disk Space Reclamation		
	/VDILAB-VS/host/VDI-GPU/10.10.10.	Default	With vSphere 5.x, virtual		
	/VDILAB-VS/host/VDI-Infra-CL/10.10	Default	machines can be configured to use a space efficient disk format		
	/VDILAB-VS/host/VDI-Infra-CL/10.10	Default	that supports reclamation of		
	/VDILAB-VS/host/VDI-Launchers/10.:	Default	unused disk space (such as deleted files). This option reclaims		
	/VDILAB-VS/host/VDI-Launchers/10.:	Default	unused disk space on each virtual		
	/VDILAB-VS/host/VDI-VSAN/10.10.10	Default	machine. The operation is initiated when an estimate of		
	/VDILAB-VS/host/VDI-VSAN/10.10.10	Default	used disk space exceeds the		
	/VDILAB-VS/host/VDI-VSAN/10.10.10	Default	specified threshold.		
			< Back Next > Cancel		

13. Review Add vCenter Server settings, click Finish.

dd vCenter Server	Ready to Complete			
VC Information	vCenter Server	vcsa6u2.vdilab-vs.local		
View Composer	User name	administrator@vsphere.local		
View Composer Domains	Password	****		
Storage Ready to Complete	Description			
Ready to Complete	Server Port	443		
	Max Provision	20		
	Max Power	50		
	Max View Composer Operations	12		
	Max View Composer Provision	8		
	Max Instant Clone Engine Provision	20		
	View Composer State	Standalone View Composer Server		
	View Composer Address	vh-comp.vdilab-vs.local		
	View Composer Password	****		
	View Composer User Name	administrator		
	View Composer Port	18443		
	Enable View Storage Accelerator	Yes		
	Default host cache size:	2048		
	VM Disk Space Reclamation	Yes		

Master Image Creation for Tested Horizon Deployment Types

To create the Master Image for the tested Horizon deployment types, complete the following steps:

1. Select an ESXi host in an existing infrastructure cluster and create the virtual machines to use as Golden Images with Windows 10 and Office 2016 for Linked-Clone, Instant Clone and Full Clone desktops.

We used 64 bit version of OS and Office for our testing.



A fourth Golden Image was created using Microsoft Windows Server 2012 R2 for RDSH session host virtual machines.

For the Golden Image virtual machines, the following parameters were used (Table 10).

Attribute	Linked-Clone/Instant- clone	Persistent/Full Clone	RDSH server
Desktop operating system	Microsoft Windows 10 En- terprise (64-bit)	Microsoft Windows 10 Enterprise (64-bit)	Microsoft Windows Server 2012 R2 standard (64-bit)
Hardware	VMware Virtual Hardware Version 11	VMware Virtual Hardware Version 11	VMware Virtual Hardware Version 11
VCPU	2	2	6
Memory	2048 MB	3072 MB*	24576MB
Memory reserved	2048 MB	3072 MB*	24576MB
Video RAM	35 MB	35 MB	4MB
3D graphics	Off	Off	Off
NIC	1	1	1
Virtual network adapter 1	VMXNet3 adapter	VMXNet3 adapter	VMXNet3 adapter
Virtual SCSI con- troller 0	Paravirtual	Paravirtual	Paravirtual
Virtual disk: VMDK 1	24 GB	40 GB	40 GB
Virtual disk: VMDK 2	3 GB	-	-
(non-persistent			

 Table 10
 Golden Image Virtual Machine Parameters

Attribute	Linked-Clone/Instant- clone	Persistent/Full Clone	RDSH server
disk)			
Virtual floppy drive 1	Removed	Removed	Removed
Virtual CD/DVD drive 1	-	-	-
Applications	 Login VSI 4.1.5 application installation Adobe Acrobat 11 Adobe Flash Player 16 Doro PDF 1.82 FreeMind Microsoft Internet Explorer Microsoft Office 2016 	 Login VSI 4.1.5 application installation Adobe Acrobat 11 Adobe Flash Player 16 Doro PDF 1.82 FreeMind Microsoft Internet Explorer Microsoft Office 2016 	 Login VSI 4.1.5 application installation Adobe Acrobat 11 Adobe Flash Player 16 Doro PDF 1.82 FreeMind Microsoft Internet Explorer Microsoft Office 2016
VMware tools	Release 10.0.9.3917699	Release 10.0.9.3917699	Release 10.0.9.3917699
VMware View Agent	Release 7.0.1 - 3989057	Release 7.0.1 - 3989057	Release 7.0.1 - 3989057

* For 1000 Persistent Desktops, we were limited to 3GB of RAM given our HyperFlex node configuration with 512GB of total memory. By adding memory to each HyperFlex node, for example eight additional 32GB DIMMs per node, we could allocate up to 5GB of RAM per VM at the same user density. By using 64GB DIMMs in all three memory channels, we could support 1000 VMs in an eight node HyperFlex cluster with 10GB of RAM per virtual desktops.

Prepare Microsoft Windows 10 and Server 2012 R2 with Microsoft Office 2016

Prepare your master image for one or more of the following use cases:

- VMware Horizon 7 Linked Clones
- VMware Horizon 7 Instant Clones
- VMware Horizon 7 Full clones
- VMware Horizon 7 RDSH Virtual Machines

Include Microsoft Office 2016 and other applications used by all pool users in your organization into your master image.

Apply Microsoft updates to your master images.

For this study, we added Login VSI target software to enable the use the Login VSI Knowledge Worker workload to benchmark end user experience for each use case.

Optimization of Base Windows 10 or Server 2012 R2 Guest OS

Select the links below to optimize windows 10 for VDI deployment:

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmware-viewoptimizationguidewindows7-en-white-paper.pdf

VMware Optimization tool for HVD or HSD deployment: <u>https://labs.vmware.com/flings/vmware-os-optimization-tool</u>

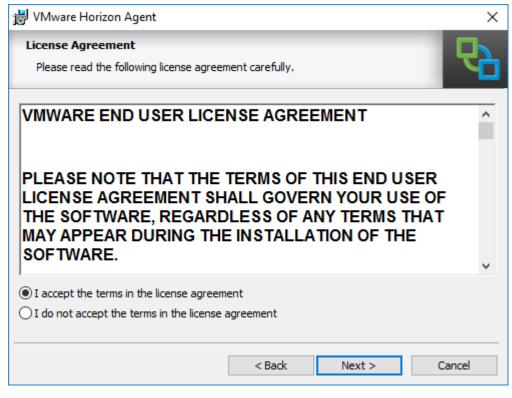
Virtual Desktop Agent Software Installation for Horizon

To install the Virtual Desktop Agent software for Horizon, complete the following steps:

1. For each master image created, open the Horizon View Agent Installer, VMware-viewagent-7.0.1-3989057.exe. Click Next to install.

闄 VMware Horizon Agent		Х
P	Welcome to the Installation Wizard for VMware Horizon Agent	
	The installation wizard will install VMware Horizon Agent on your computer. To continue, click Next.	
vMware Horizon™ Agent	Copyright © 1998-2016 VMware, Inc. All rights reserved. Th product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.	
Ċ PC @IP`		_
Product version: 7.0.1-3989057	x64 < Back Next > Cancel	

2. Review and accept the EULA Agreement. Click Next.



3. Select Network protocol configuration, click Next.

😸 VMware Horizon Agent	×
Network protocol configuration Select the communication protocol	P
Specify the protocol to be used to configure this Horizon Agent instance:	
IPv4 This agent will be configured to choose the IPv4 protocol for est IPv6 all connections.	tablishing
< Back Next >	Cancel

4. Based on the Desktop pool you want to create, select either View Composer Agent or Instant Clone Agent installation. Do not install both features on the same master image.

5. Enable installation of the VMware Horizon View Composer Agent for linked-clone VDI virtual machines.

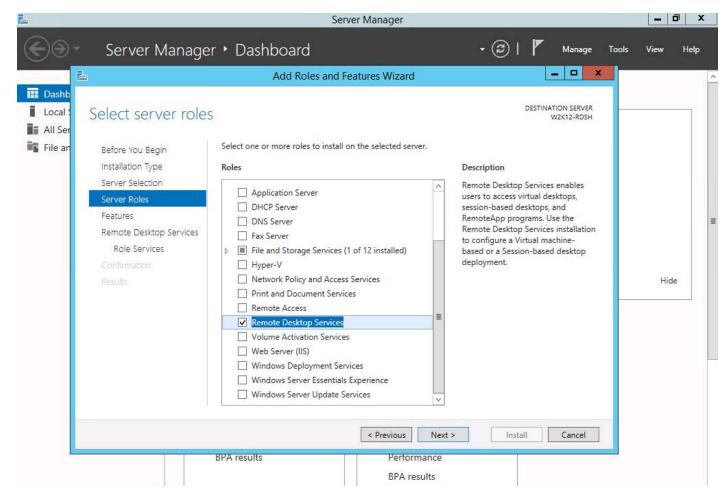
Select the p	up program features you want installe	ı. 🤤
lick on an ico	 Real-Time Audio-Video VMware Horizon View Compose 	Feature Description VMware Horizon View Composer Agent RDSH installs: This machine can be used as the parent image for provisioning Automated Farms This feature requires 1703KB on your hard drive.
nstall to:		Change

6. Disable the Horizon View Composer Agent and enable the Horizon Instant Clone Agent for Instant Clone floating assigned desktop pool creation.

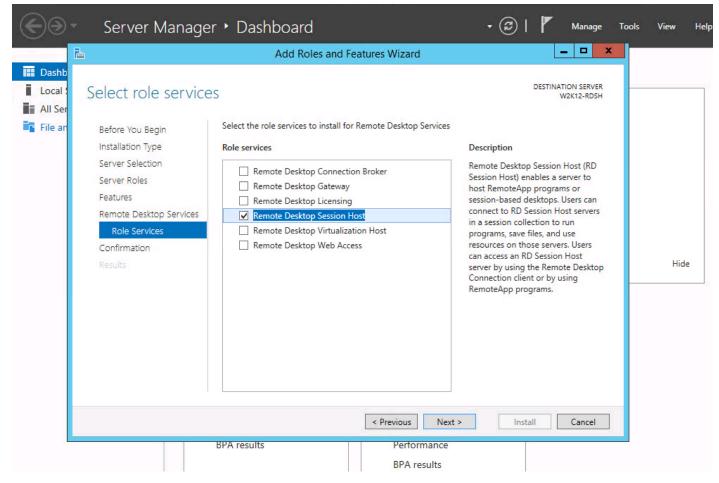
Select the program features you want installed	
Core USB Redirection Real-Time Audio-Video VMware Horizon Instant Clone Client Drive Redirection Virtual Printing vRealize Operations Desktop A	Feature Description Horizon Instant Clone Agent should only be installed on a virtual machine running on VMware vSphere 2015 U1 or later. It cannot be co-installed with Horizon View Composer Agent. This feature requires 3175KB on your hard drive.
stall to:	Change

Prior to installing the Horizon View Agent on a Microsoft Server 2012 R2 virtual machine, you must add the Remote Desktop Services role and the Remote Desktop Session Host role service.

7. To add Remote Desktop Services role on Windows Server OS from the Server Manager, use the Add Roles and Features wizard:



8. Add Remote Desktop Session Host services.



9. Click Install.

Confirm installation	on selections	DESTINATION SERVE W2K12-RDS
Before You Begin Installation Type	To install the following roles, role services, or features on selec	ted server, click Install.
Server Selection Server Roles Features	Optional features (such as administration tools) might be displ been selected automatically. If you do not want to install these their check boxes.	
Remote Desktop Services Role Services	Remote Desktop Services Remote Desktop Session Host	
Confirmation	Remote Server Administration Tools Role Administration Tools	
Results	Remote Desktop Services Tools	
	Remote Desktop Licensing Diagnoser Tools	
	Export configuration settings Specify an alternate source path	

₿	VMware Horizo	on Agent
	tom Setup elect the program features you want installed.	
Click		re is installed. Feature Description VMware Horizon Agent core functionality This feature requires 262MB on your hard drive.
	all to: rogram Files\VMware\VMware View\Agent\	Change
[Help Space < Bac	
		Windows Server 2012 R2

10. View Agent is will report as Install in "Desktop Mode" if Remote Desktop Services not installed.

岁 VMwa	re Horizon Ag	ent	x
Desktop OS Configuration The following information is used to con feature	nfigure the VMware	Horizon 7 Desktop	6
and the second	a decident		n Dán Abu
The Remote Desktop Session Host role is Agent in RDS mode restart the installer a			
Please check the box to continue installin	g VMware Horizon A	Agent in 'desktop moo	de'.
Install VMware Horizon Agent in 'desk	top mode'		
	< Back	Next >	Cancel

11. Add FQDN or IP address for Connection Server Instance to register the RDSH server.

ان	VMware Horizo	n Agent 🛛 🗙							
-	Register with Horizon 7 Connection Server Enter the Horizon 7 Connection Server that this machine will connect to.								
	er name of a Horizon 7 Connection Serv ogin credentials to register this machine	with the Horizon 7 Connection Server.							
vh-conn01.vd	ilab-hc.local	(hostname or IP address)							
Authentication	O Authenticate as the currently log O Specify administrator credentials Username: Password:								
	< Bad	: Next > Cancel							

12. Click Install.

🖡 VMware Horizon Agent		×
Ready to Install the Program		
The wizard is ready to begin installati	on.	
VMware Horizon Agent will be installer	d in:	
C:\Program Files\VMware\VMware Vie	ew\Agent\	
Click Install to begin the installation o	r Cancel to exit the wizard.	
	< Back Install	Cancel

13. Click Finish and restart the VM.

🛃 VMware Horizon Agent	X
	Installer Completed
	The installer has successfully installed VMware Horizon Agent. Click Finish to exit the wizard.
vMware Horizon™ Agent	
ĊPC@₽°	
	< <u>B</u> ack <u>Einish</u> Cancel

Install Additional Software

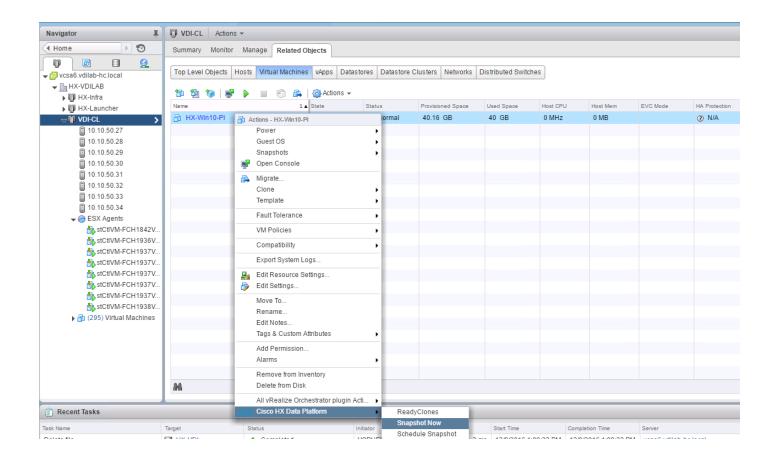
To install additional software required for your base windows image, complete the following steps:

- 1. For testing, we installed Office 2016 64bit version.
- 2. Log into the VSI Target software package to facilitate workload testing.
- 3. Install service packs and hot fixes required for the additional software components that were added.
- 4. Reboot or shut down the VM as required.

Create a Native Snapshot for Automated Desktop Pool Creation

To create a native snapshot for the automated desktop pool, complete the following steps:

- 1. Log into vCenter WebUI.
- 2. Select the master image for the automated desktop pool creation.
- 3. Right-click, select Cisco HX Data Platform \rightarrow SnapshotNow.



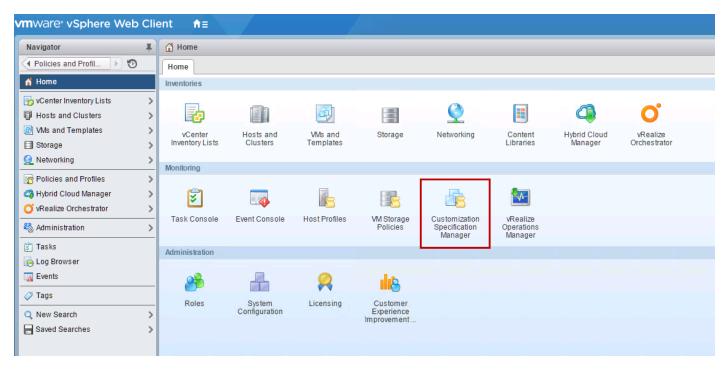
4. Enter a name for the HX native snapshot.

Navigator I	VDI-CL Actions -				Take VM Nativ	ve Snapshot for HX-Win10-PI	×	
Home 🕨 🔊	Summary Monitor Manage Related O	bjects			News	Networket	-	
					Name	NativeSnapshot		
✓ @ vcsa6.vdilab-hc.local	Top Level Objects Hosts Virtual Machines	vApps Datas	stores Datastore	Clusters Netwo	Description:			
HX-VDILAB					Description.			
HX-Infra		🎯 Actions 👻						
🕨 🗊 HX-Launcher		State	Status	Provisioned Spa			Nor	de HA Protection
, VDI-CL >	🗗 HX-Win10-PI	Powered Off	Normal	40.16 GB				⑦ N/A
10.10.50.27								
10.10.50.28								
10.10.50.29								
10.10.50.30							_	
10.10.50.31						OK Cancel		
10.10.50.32								
10.10.50.33								
10.10.50.34								
🖵 🥏 ESX Agents								
stCtiVM-FCH1842V								
stCtIVM-FCH1936V								
stCtlVM-FCH1937V								
stCtlVM-FCH1937V								
stCtIVM-FCH1937V								
stCtiVM-FCH1937V								
stCtiVM-FCH1937V								
stCtiVM-FCH1938V								
🕨 🛅 (295) Virtual Machines								

Create Customization Specification for Virtual Desktops

To create Customization Specification for virtual desktops, complete the following steps:

1. On vCenter WebUI, select Customization Specification Manager.



2. Select VM Operating System as Windows for Windows based guest OS optimization. Enter a name.

vmware vSphere Web Cli					
Navigator I	Customization Specification Man				
Home 🔊 🔊	vCenter Server: vcsa6.vdilab-hc.local				
Policies and Profiles					
🚰 Customization Specifica	Name		Guest OS	Last Modified	
To VM Storage Policies	New VM Guest Customization Sp	ec		(?)	•
Host Profiles	 Specify Properties Set Registration Information Set Computer Name Enter Windows License Set Administrator Password Time Zone Run Once Configure Network Set Workgroup or Domain Set Operating System Options Ready to complete 	New Customization Spe Enter a name for the customize Target VM Operating System: Customization Spec Name: Description:	cification ation specification and select the OS of the targ Windows Use custom SysPrep answer file	jet.	
				Back Next Finish Cancel)

3. Provide name and organization details.

	New VM Guest Customization Spe	ec						(?) H
~	1 Specify Properties		ration Information stration information for this copy of the	quest operating system				
	2 Set Registration Information	Linter the regis	suadon mormadon for ans copy of the	guest operating system.				
	3 Set Computer Name	Name:	Administrator]				
	4 Enter Windows License	Organization:	vdilab-hc					
	5 Set Administrator Password			•				
	6 Time Zone							
	7 Run Once							
	8 Configure Network							
	9 Set Workgroup or Domain							
1	0 Set Operating System Options							
1	1 Ready to complete							
					Back	Next	Finish	Cancel

4. Provide a computer name. For this solution, we selected the radio button for Use the virtual machine name.

New VM Guest Customization Sp	ec	? ₩
 1 Specify Properties 2 Set Registration Information 	Computer Name Enter a computer name that will identify this virtual machine on a network.	
 2 Set Registration Information 3 Set Computer Name 4 Enter Windows License 5 Set Administrator Password 6 Time Zone 7 Run Once 8 Configure Network 9 Set Workgroup or Domain 10 Set Operating System Options 11 Ready to complete 	 Enter a name: The name cannot exceed 15 characters. Append a numeric value to ensure uniqueness The name will be truncated if combined with the numeric value, it exceed 15 characters. Use the virtual machine name If the name exceeds 15 characters, it will be truncated. Enter a name in the Clone/Deploy wizard Generate a name using the custom application configured with the vCenter Server Argument: 	
	Back Next Finish	Cancel

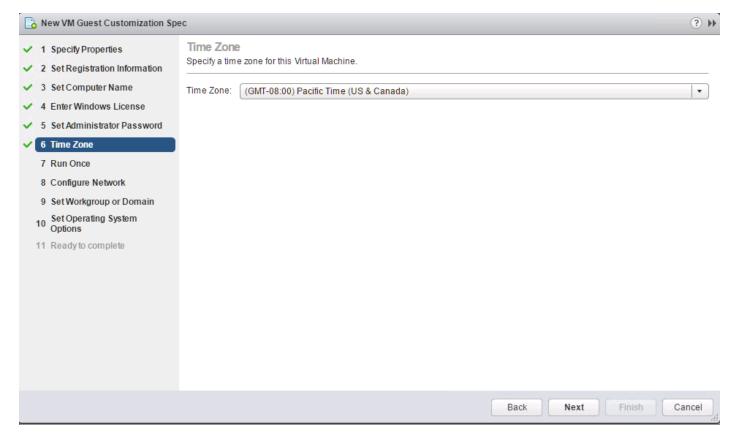
5. Provide the product License key if required.

New VM Guest Customization Sp	ec	? >>
 ✓ 1 Specify Properties ✓ 2 Set Registration Information 	Enter Windows License Enter the Windows licensing information for this copy of the guest operating system. If this virtual machine does not require licensing information, leave these fields blank.	
 3 Set Computer Name 4 Enter Windows License 5 Set Administrator Password 6 Time Zone 7 Run Once 8 Configure Network 9 Set Workgroup or Domain 10 Set Operating System 	Product Key: ✓ Include Server License Information (Required for customizing a server guest OS) Server License Mode: OPer seat • Per server Max connections: 5	
10 Options 11 Ready to complete		
	Back Next Finish C	ancel

6. Provide Password credentials.

New VM Guest Customization Sp	pec	? ₩
 1 Specify Properties 2 Set Registration Information 	Set Administrator Password Enter the password and auto logon option for the administrator account.	
 2 Set Registration Information 3 Set Computer Name 4 Enter Windows License 5 Set Administrator Password 6 Time Zone 7 Run Once 8 Configure Network 9 Set Workgroup or Domain 10 Set Operating System Options 11 Ready to complete 	Enter the password and auto logon option for the administrator account. Password: Confirm password: Automatically logon as Administrator Number of times to logon automatically: 1	
	Back Next Finish (Cancel

7. Select the Timezone.



8. Add the commands to run when the first-time user logs in, if there are any.

 ✓ 5 Set Administrator Password ✓ 6 Time Zone 	Add
 4 Enter Windows License 5 Set Administrator Password 6 Time Zone 	
 ✓ 5 Set Administrator Password ✓ 6 Time Zone 	
✓ 6 Time Zone	Delete
V 6 Time Zone	ove Up
	ve Down
	Ve Down
8 Configure Network	
9 Set Workgroup or Domain	
10 Set Operating System Options	
11 Ready to complete	
Back Next Finish	Cancel

9. Provide the network information whether to use the DHCP server to assign IP address, or manual configuration.

🔒 New VM Guest Customization	n Spec			? >>				
 1 Specify Properties 2 Set Registration Information 	Configure Network Use default network setti	ngs or customize properties for each	network interface.					
 ✓ 3 Set Computer Name 		• Use standard network settings for the guest operating system, including enabling DHCP on all network interfaces						
✓ 4 Enter Windows License	 Manually select custo 	m settings						
✓ 5 Set Administrator Password	• • / ×							
✓ 6 Time Zone	Description	IPv4 Address	IPv6 Address					
✓ 7 Run Once	NIC1	Use DHCP	Notused					
8 Configure Network								
9 Set Workgroup or Domain								
10 Set Operating System Options								
11 Ready to complete								
			Dealy Next	oish Conset				
			Back Next Fir	nish Cancel				

10. Provide the domain name and user credentials.

New VM Guest Customization Sp	ec		? >>		
 1 Specify Properties 2 Set Registration Information 	Set Workgroup or Domain How will this virtual machine participate in a network?				
 3 Set Computer Name 4 Enter Windows License 	 Workgroup: Windows Server Domain: 	WORKGROUP vdilab-hc.local]		
 ✓ 5 Set Administrator Password ✓ 6 Time Zone 	Specify a user account that	at has permission to add a computer to the domain.			
 ✓ 7 Run Once ✓ 8 Configure Network 	Username: Password:	administrator ********]		
9 Set Workgroup or Domain Set Operating System Options	Confirm Password:		1		
11 Ready to complete					
		Back Next Finish C	ancel		

11. Select the checkbox Generate New Security ID (SID).

New VM Guest Customization Spe	ec	? ••
 1 Specify Properties 2 Set Registration Information 	Set Operating System Options Configure these optional parameters for the guest operating system.	
 3 Set Computer Name 4 Enter Windows License 	Generate New Security ID (SID) Select this item to generate a new security identity.	
 5 Set Administrator Password 6 Time Zone 		
 7 Run Once 8 Configure Network 		
 ✓ 9 Set Workgroup or Domain ✓ 10 Set Operating System Options 		
✓ 11 Ready to complete		
	Back Next Finish Cano	el

- 12. Review and click Next to complete creating the Customization Specs.
- 13. Click Finish.

🔒 New VM Guest Customization Sp	bec		- ? H
 New VM Guest Customization Sp 1 Specify Properties 2 Set Registration Information 3 Set Computer Name 4 Enter Windows License 5 Set Administrator Password 6 Time Zone 7 Run Once 8 Configure Network 9 Set Workgroup or Domain 10 Set Operating System Options 11 Ready to complete 	Ready to complete Review your settings selections b Name: OS Type: Registration Info: Computer Name: Product Key: Server License Mode: Administrator Log In: Time Zone: Network Type: NIC1 IPv4 NIC1 IPv4 NIC1 IPv6 Windows Server Domain: Username: OS Options:	before finishing the wizard. Windows User: Administrator Organization: vdilab-hc Use Virtual Machine name Per Server (Maximum Connections: 5) Do not log in automatically as Administrator (GMT-08:00) Pacific Time (US & Canada) Custom Use DHCP Not used vdilab-hc.local administrator Generate new security ID	
		Back Next Finish	Cancel

VMware Horizon Farm and Pool Creation

RDSH Farm Creation

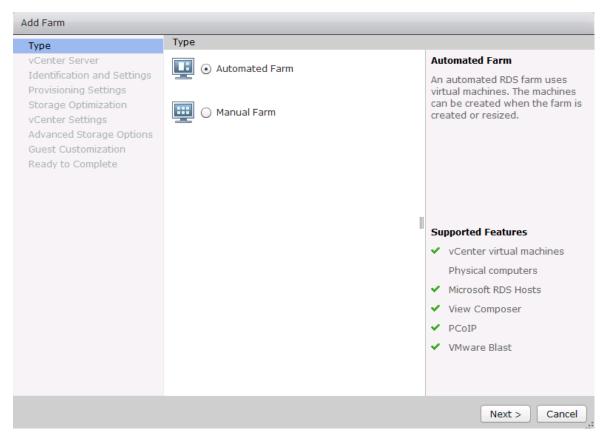
Before you can create an RDSH desktop pool, you must first create a RDSH Farm. To create a RDSH Farm, complete the following steps:

- 1. In the VMware Horizon Administration console, select Farms under the Resource node of the Inventory pane.
- 2. Click Add in the action pane to create a new RDSH Farm.

VMware Horizon 7 Administrator					
Updated 11/29/2016 1:55 PM 🥏 Sessions 0	Farms				
Problem vCenter VMs 0 Problem RDS Hosts 0 Events 0 1 0	Add Edit Delete	More Commands Access Grou	qt		
Events 0 1 0 System Health 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Filter 👻	Find Clear Access	Group: All 🔻		
Inventory	ID	Туре	RDS Hosts		
Signal Dashboard Signal Dashboard Signal Dashboard Signal Dashboard Catalog ▼ Resources Image: Farms Signal Dashboard Persistent Disks ► Monitoring ► Policies					
 View Configuration 					

3. Select either to create an Automated or Manual Farm. In this solution, we selected Automated Farm.

A Manual Farm requires a manual registration of each RDSH server to Horizon Connection or Replica Server instance.



- 4. Select the vCenter Server and Horizon Composer server that you will use to deploy the Horizon RDSH Farm.
- 5. Click Next.

Add Farm						
Туре	vCenter Server					
vCenter Server	View Composer linked clone	es	View Composer			
Identification and Settings Provisioning Settings Storage Optimization vCenter Settings Advanced Storage Options	vCenter Server	View Composer	View Composer linked clones share the same base image and			
	vcsa6.vdilab- hc.local(administrator@vs phere.local)	vh-comp.vdilab- hc.local	use less storage space than full virtual machines.			
Guest Customization Ready to Complete						
			Supported Features			
			✓ PCoIP			
			✓ VMware Blast			
			 Storage savings 			
	Description: None		 Recompose SysPrep guest customization 			
			< Back Next > Cancel			

- 6. Enter the RDSH Farm ID, Access group, Default Display Protocol (Blast/PCoIP/RDP).
- 7. Select if users are allowed to change the default display protocol, Session timeout, Logoff Disconnected users, and select the checkbox to Enable HTML access.
- 8. Click Next.

Add Farm - HX-RDSHPool			
Туре	Identification and Settings		
vCenter Server	General		
Identification and Settings Provisioning Settings	ID:	HX-RDSHPool	
Storage Optimization	Description:	Windows server 2012 R2 RDS Pool	
vCenter Settings			
Advanced Storage Options Guest Customization			
Ready to Complete			
	Access group:	VDI-User 🔹	
	Farm Settings		
	Default display protocol:	VMware Blast 💌 📀	
	Allow users to choose protocol:	Yes 🔻	
	Empty session timeout (applications only):	Never 🛛 🔹	
	When timeout occurs:	Disconnect 💌	
	Log off disconnected sessions:	Never 🗸	
	Allow HTML Access to desktops and applications on this farm:	Enabled ③	
		Requires installation of HTML Access.	
		< Back Next > Cancel	

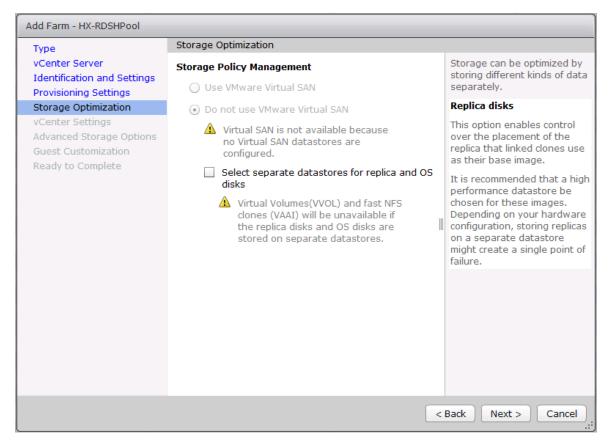
9. Select the provisioning settings, naming convention for RDSH server VM to deploy, and the number of VMs to deploy.

In this study, we deployed 64 RDSH virtual machines across our 8 node HyperFlex Cluster.

10. Click Next.

Add Farm - HX-RDSHPool					
Type vCenter Server	Provisioning Settings Basic Naming Pattern				
Identification and Settings Provisioning Settings Storage Optimization vCenter Settings Advanced Storage Options Guest Customization Ready to Complete	 Enable provisioning Stop provisioning on error Virtual Machine Naming Naming Pattern: HX-RDS Farm Sizing Max number of machines Minimum number of ready(provisioned) machines during View Composer maintenance operations: Ø 	 Virtual machines will be named according to the specified naming pattern. By default, View Manager appends a unique number to the specified pattern to provide a unique name for each virtual machine. To place this unique number can unuber elsewhere in the pattern, use '{n}'. (For example: vm-{n}-sales.). The unique number can also be made a fixed length. (For example: vm-{n:fixed=3}-sales). See the help for more naming pattern syntax options. 			
		< Back Next > Cancel			

11. Click Next.



- 12. Select vCenter settings, for example; Master Image, snapshot, folder, Host or Cluster, resource pool, storage selection.
- 13. Click Next.

Add Farm - HX-RDSHPool			
Туре	vCenter Settings		
vCenter Server Identification and Settings	Default Image		
Provisioning Settings	1 Parent VM:	/HX-VDILAB/vm/Discovered virtual mac	Browse
Storage Optimization vCenter Settings	2 Snapshot:	/SENTINEL/RDSHsnap00	Browse
Advanced Storage Options	Virtual Machine Location		
Guest Customization Ready to Complete	3 VM folder location:	/HX-VDILAB/vm	Browse
	Resource Settings		
	4 Host or cluster:	/HX-VDILAB/host/VDI-CL	Browse
	5 Resource pool:	/HX-VDILAB/host/VDI-CL/Resources	Browse
	6 Datastores:	1 selected	Browse
		< Back	Next > Cancel

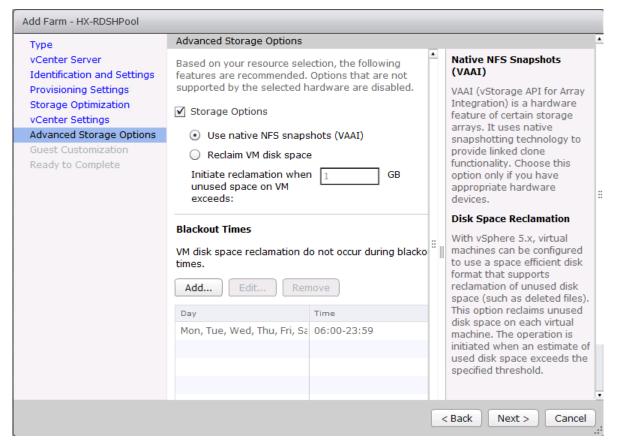
14. For Step 6 Datastores: Browse and choose Unbounded for the Storage Overcommit field.

15. Click OK.

dd Farm -	- HX-RDSHPool							
Type vCenter S Identifica	Server ation and Settings	vCenter Settings Default Image						
Select Linked Clone Datastores								
selecte	the linked clone datas d host or cluster can w all datastores (inclu	be selected.					used by the	re 🍣
	Datastore	Capacity (GB)			Drive Typ		Overcommit (
\checkmark	<u>員</u> HX-VDI	40,960.00	40,878.51	NFS		Unbounded		-
Data Ty	ype	Selected Free Space	e (GB) Min R	ecommende	ed (GB) 509	% utilization (C	Max Recomme	nded (
Linked	l clones	40,878.51	104.	40	10	1.00	122.00	
							ОК Са	incel .
						< Back	Next >	Cance

16. In the Advanced Storage Options, select Use native NFS snapshot (VAAI).

17. Click Next.



- 18. Select the Active Directory Domain, the Active Directory OU into which the RDSH machines will be provisioned, and the Sysprep file created as part of the customization specific configuration performed earlier.
- 19. Click Next.

Add Farm - HX-RDSHPool					
Туре	Guest Customization				
vCenter Server					
Identification and Settings Provisioning Settings	Domain:	pr) 🛛 🔻			
Storage Optimization vCenter Settings	AD container:	OU=Computers,OU=LoginV	SI Browse		
Advanced Storage Options	✓ Allow reuse of pre-existin	g computer accounts (🔋			
Guest Customization	Using a customization specifi	ication (SysPrep)			
Ready to Complete					
	Name	Guest OS	Description		
	Horizon-RDS	Windows			
	InfraVM-Specs	Windows			
	RDSH-Customization	Windows			
	Win10-Custom	Windows	Windows 10 customization f		
		<	Back Next > Cancel		

- 20. Review the pool creation information.
- 21. Click Finish.

Add Farm - HX-RDSHPool		
Туре	Ready to Complete	<u>▲</u>
vCenter Server	vCenter Server:	vcsa6.vdilab-hc.local(administrator@vsphere.local)
Identification and Settings Provisioning Settings	Use View Composer:	Yes
Storage Optimization	ID:	HX-RDSHPool
vCenter Settings	Description:	Windows server 2012 R2 RDS Pool
Advanced Storage Options	Access Group:	VDI-User
Guest Customization	Default display protocol:	VMware Blast
Ready to Complete	Allow users to choose protocol:	Yes
	Empty session timeout (applications only):	Never
	When timeout occurs:	Disconnect
	Log off disconnected sessions:	Never
	Allow HTML Access to desktops and applications on this farm:	Disabled
	Enable provisioning:	Yes
	Stop provisioning on error:	Yes
	Virtual Machine Naming:	Use a naming pattern
	VM naming pattern:	HX-RDS
	Default image:	HX-RDS-GI - RDSHsnap00
	Virtual Machine Folder:	/HX-VDILAB/vm
		< Back Finish Cancel

VMware Horizon Administration console displays the status of the provisioning task and pool settings:

VMware Horizon 7 Adm	ninistrator		
Updated 11/29/2016 2:05 PM 2 Sessions 0 Problem vCenter VMs 0	Farms	✓ More Commands	
Problem RDS Hosts 0 Events 0 &	Filter -	Find Clear Access 0	Sroup: All
Inventory	ID HX-RDSHPool	Type	RDS Hosts
Image: Second system Image: Second system <th></th> <th></th> <th></th>			

Updated 11/29/2016 2135 PM	HX-RDSHPool							
	0 Summary RDS Hosts R	DS Pools Sessions						
Events 0 1 System Health 1 10 10 10 10 10 10 10 10 10 10 10 10 1		Commands						
Inventory	Filter 👻	Find Clear						a
R Dashboard	DNS Name	1. Туре	Max number of connections	Agent Version	Enabled		Status	
B Users and Groups	hx-rds1.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
Catalog	hx-rds10.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
Desktop Pools	hx-rds11.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
E Application Pools	ho-rds12.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
📌 ThinApps	hx-rds13.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
Resources	hx-rds14.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	4	Available		
Farms	hx-rds15.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
Persistent Disks	hx-rds16.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
Monitoring	hx-rds17-vdilab-hc-local	Windows Server 2012	Unlimited	7.0.1	~	Available		
Policies	hx-rds18.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
View Configuration	hx-rds19.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
	hx-rds2.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	4	Available		
	hx-rds20.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
	hx-rds21.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	-	Available		
	hx-rds22.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	-	Available		
	hx-rds23.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	4	Available		
	hx-rds24-vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
	hx-rds25.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	-	Available		
	hx-rds26.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	~	Available		
	hx-rds27.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	-	Available		
	hx-rds28.vdilab-hc.local	Windows Server 2012	Unlimited	7.0.1	-	Available		

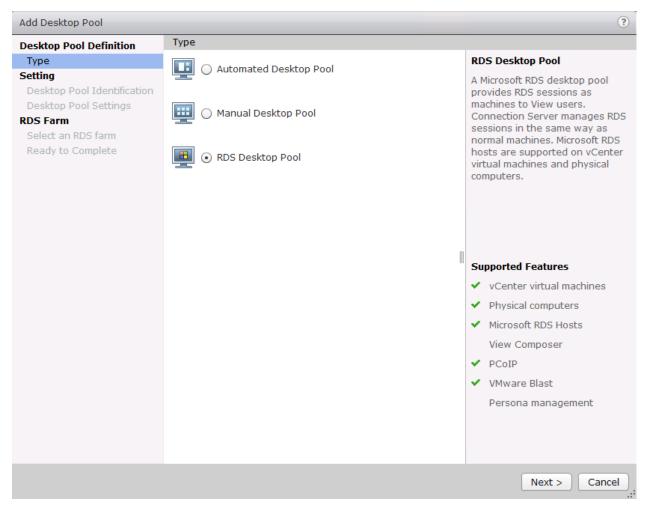
Create the Horizon 7 RDS Published Desktop Pool

To create the Horizon 7 RDS Published Desktop Pool, complete the following steps:

- 1. In the Horizon Administrator console, select Desktop Pools in the Catalog node of the Inventory pane.
- 2. Click Add in the action pane.

Updated 11/29/2016 2:30 PM 🛛 🞅	Desktop Pools				
Sessions 0 Problem vCenter VMs 0 Problem RDS Hosts 6	Add Edit	Clone Delete 🔻 Entitler	nents 🔻 Status 🔍 🕶 Ac	cess Group 🛛 🔻 More C	Commands
Events () () () () () () () () () (Filter 👻	Find Clear	Access Group: All	▼	
	ID	Display Name	Туре	Source	User Assi
Inventory					
💦 Dashboard					
器 Users and Groups					
Catalog					
🛄 Desktop Pools					
Application Pools					
📌 ThinApps					
Resources					
Farms					
🔂 Machines					
Persistent Disks					
 Monitoring 					

- 3. Select RDS Desktop pool.
- 4. Click Next.



- 5. Enter Pool ID and display name.
- 6. Click Next.

esktop Pool Definition	Desktop Pool Ider	ntification	
Туре	ID:	HXRDS-Pool	ID
etting Desktop Pool Identification	Display name:	HXRDS-Pool	The desktop pool ID is the unique name used to identify this
Desktop Pool Settings	Description:		 desktop pool.
DS Farm			Display Name
Select an RDS farm Ready to Complete			The display name is the name that users will see when they connect to View Client. If the display name is left blank, the ID will be used.
			Access groups can organize the desktop pools in your organization. They can also be used for delegated administration.
			Description
			This description is only shown or the Settings tab for a desktop pool within View Administrator.

- 7. Accept the default settings on Desktop Pool Settings page.
- 8. Click Next.

Desktop Pool Definition Desktop Pool Settings Setting General State: Enabled • Desktop Pool Identification Connection Server restrictions: None Browse RDS Farm Select an RDS farm Adobe Flash Settings for Sessions Adobe Flash quality: Do not control • Image: Control • Adobe Flash throttling: Disabled • Image: Control • None Image: Control • Image: Control • Image: Control • Adobe Flash throttling: Disabled • Image: Control • Image: Control • Adobe Flash throttling: Disabled • Image: Control • Image: Control • Image: Control • Adobe Flash throttling: Disabled • Image: Control •	Add Desktop Pool - HXRDS-Poo	bl		?
Type Setting Desktop Pool Identification Desktop Pool Settings SDS Farm Select an RDS farm Ready to Complete Adobe Flash quality: Do not control • Adobe Flash throttling: Disabled • Stable •	Desktop Pool Definition	Desktop Pool Settings		
Adobe Flash Quality: Do not control Adobe Flash throtting: Disabled Other Plash Quality: Disabled Other Plash Qu	Type Setting Desktop Pool Identification Desktop Pool Settings RDS Farm	State: Connection Server		
		Adobe Flash quality:	Do not control 🔻 ③	
< Back Next > Cancel			< Back Next > Car	ncel

- 9. Click the "Select an RDS farm for this desktop pool" radio button.
- 10. Click the farm created in the previous section.
- 11. Click Next.

Add Desktop Pool - HXRDS-Poo	l				?	
Desktop Pool Definition	Select an RDS f	arm				
Type Setting	Create a new RDS farm					
Desktop Pool Identification Desktop Pool Settings RDS Farm	⊙ Select an RD	S farm for this desktop	pool			
Select an RDS farm	Filter 🔻			Find	Clear 🎅	
Ready to Complete	Flicel +			Find		
	Farm ID	Description	RDS Hosts	Max number of	Status	
	HX-RDSHPool	Windows server 2	64	Unlimited	No problem detect	
				< Back	lext > Cancel	

- 12. Review the pool settings.
- 13. Select the checkbox "Entitle users after this wizard finishes" to authorize users for the newly create RDSH desktop pool.
- 14. Click Finish.

Desktop Pool Definition Type Setting Desktop Pool Identification Desktop Pool Settings RDS Farm Select an RDS farm	Ready to Complete Type: Unique ID:	✓ Entitle users after the RDS Desktop Pool	is wizard finishes
Getting Desktop Pool Identification Desktop Pool Settings RDS Farm		RDS Desktop Pool	is wizard finishes
Desktop Pool Identification Desktop Pool Settings RDS Farm		•	
Desktop Pool Settings RDS Farm		•	
RDS Farm	Unique ID.	HXRDS-Pool	
	Display name:	HXRDS-Pool	
	Desktop pool state:	Enabled	
Ready to Complete	Connection Server restrictions:	None	
	Adobe Flash quality:	Do not control	
	Adobe Flash throttling:	Disabled	
	Description:		
	RDS Farm:	HX-RDSHPool	
	Number of RDS hosts in the farm:	64	

15. Select the Users or Groups checkbox, use the search tools to locate the user or group to be authorized, highlight the user or group in the results box.

16. Click OK.

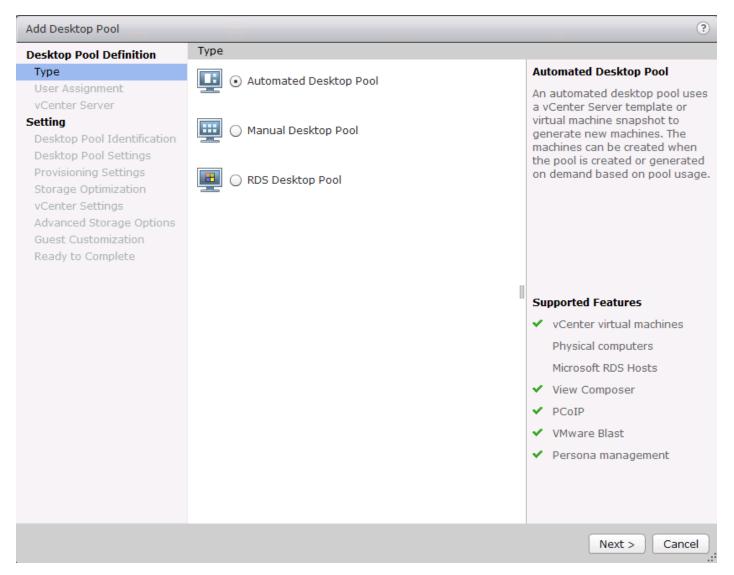
Add new users	and groups who can	use the selected poo	ol(s).		
Add Re	emove		æ		
Name	Dor	nains	Email		
	Find User or Group			_	_
	Туре:	Users	Groups		
	Domain:	Entire Directory	•		
	Name/User name:	Contains 🛛 🔻	LoginVSI		
	Description:	Contains 🛛 🔻			
			Find		
	Name	User Name	Email	Description	In Folder
	LoginVSI	LoginVSI/vdilab-hc.			vdilab-hc.local/Log

17. You now have a functional RDSH Farm and Desktop Pool with users identified who are authorized to utilize Horizon RDSH sessions.

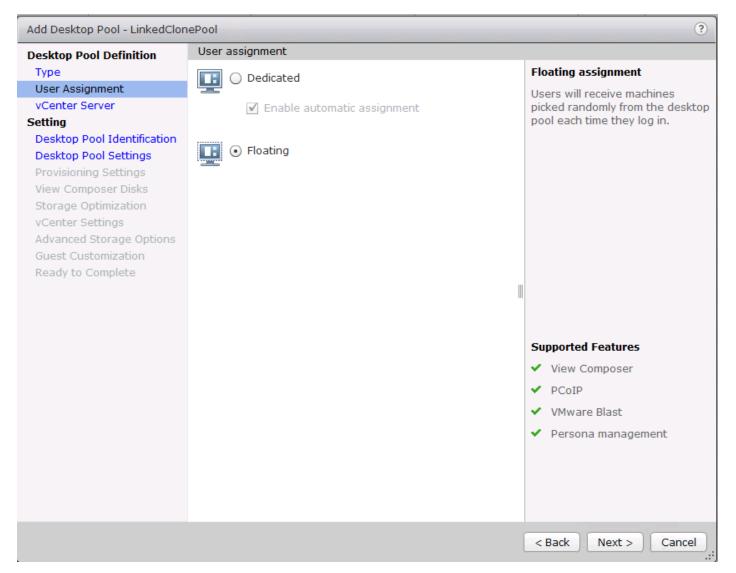
VMware Horizon Linked-Clone Windows 10 Desktop Pool Creation

To create a VMware Horizon linked-clone Windows 10 Desktop Pool, complete the following steps:

- 1. In Horizon Administrator console, select Desktop Pools in the Catalog node of the Inventory pane.
- 2. Click Add in the action pane.
- 3. Select assignment type for pool.
- 4. Click Next.



- 5. Select Floating or Dedicated user assignment.
- 6. Click Next.



- 7. Select View Composer Linked Clones, highlight your vCenter and View Composer virtual machine.
- 8. Click Next.

Desktop Pool Definition	vCenter Server						
Туре	Full virtual machines		View Composer				
User Assignment vCenter Server	 View Composer linked clones 		View Composer linked clones share the same base image and				
Setting Desktop Pool Identification	O Instant clones		use less storage space than full virtual machines.				
Desktop Pool Settings	vCenter Server	View Composer	The user profile for linked clones				
Provisioning Settings View Composer Disks Storage Optimization	vcsa6.vdilab- hc.local(administrator@vsphere.lo cal)	vh-comp.vdilab- hc.local	can be redirected to persistent disks that will be unaffected by OS updates and refreshes.				
vCenter Settings Advanced Storage Options Guest Customization							
Ready to Complete			Supported Features				
			✓ PCoIP				
			✓ VMware Blast				
			✓ Storage savings				
			 Recompose and refresh 				
			Push Image				
			 QuickPrep guest customization 				
			✓ SysPrep guest customization				
	Description: None		ClonePrep guest customization				
			 Persona management 				

9. Enter pool identification details.

Desktop Pool Definition	Desktop Pool Ider	ntification		
Type	ID:			ID
User Assignment	10.	LinkedClonePool		The desktop pool ID is the uniqu
vCenter Server	Display name:	LinkedClonePool		name used to identify this
Setting	Access group:	VDI-User		desktop pool.
Desktop Pool Identification			1.	Display Name
Desktop Pool Settings	Description:			The display name is the name
Provisioning Settings				that users will see when they
View Composer Disks				connect to View Client. If the
Storage Optimization				display name is left blank, the II
vCenter Settings				will be used.
Advanced Storage Options				Access Group
Guest Customization				Access groups can organize the
Ready to Complete				desktop pools in your
				organization. They can also be
				used for delegated administration.
				Description
				This description is only shown o
				the Settings tab for a desktop pool within View Administrator.
				poor within view Administrator.
				< Back Next > Cancel

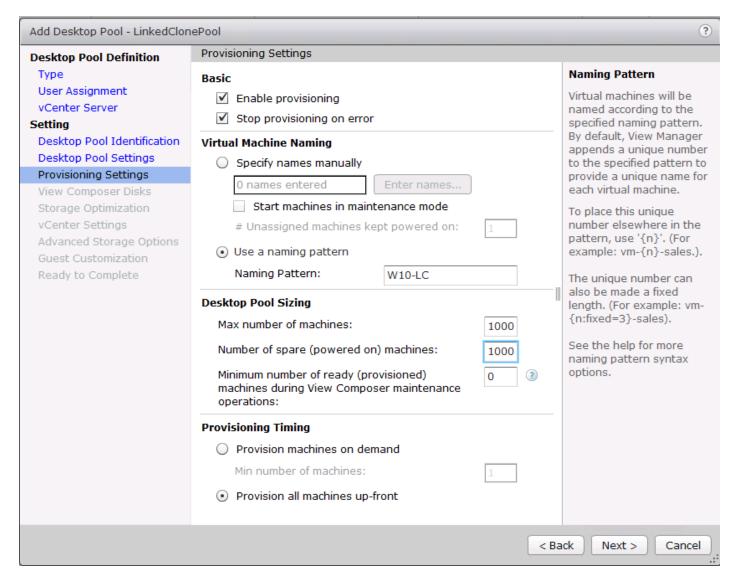
11. Select Desktop Pool settings.



Be sure to scroll down in this dialogue to configure all options.

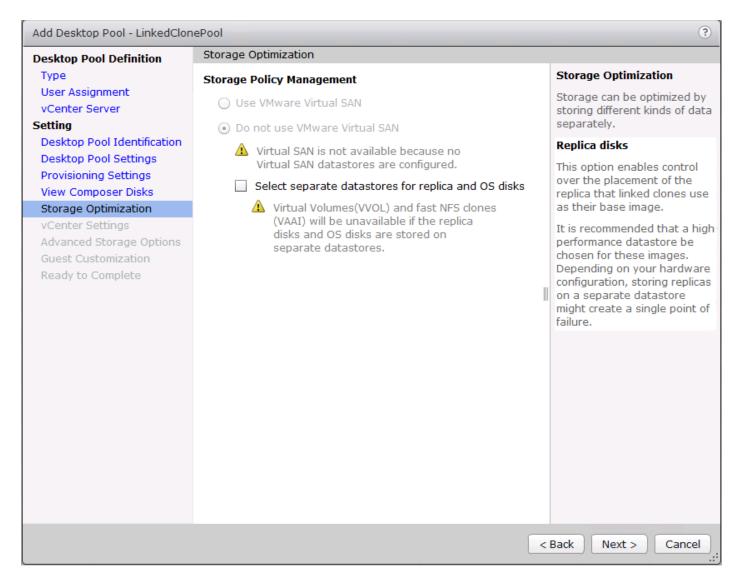
Add Desktop Pool - LinkedClon	ePool	?	
Desktop Pool Definition	Desktop Pool Settings		•
Туре	General		
User Assignment vCenter Server	State:	Enabled 🛛	
Setting Desktop Pool Identification	Connection Server restrictions:	None Browse	
Desktop Pool Settings	Remote Settings		
Provisioning Settings View Composer Disks	Remote Machine Power Policy:	Ensure machines are always powered on $ \bullet $	
Storage Optimization vCenter Settings Advanced Storage Options	Automatically logoff after disconnect:	Never 🔹	
Guest Customization Ready to Complete	Allow users to reset their machines:	No 🗸 🔻	
Ready to complete	Allow user to initiate separate sessions from different client devices:	No 🛛 🔻 😨	
	Delete or refresh machine on logoff:	Never 3	
	Remote Display Protocol		
	Default display protocol:	VMware Blast 🛛 🔻	
	Allow users to choose protocol:	Yes 🔻	
	3D Renderer:	Disabled Configure ?	
	Max number of monitors:	2 • 3	
		May require power-cycle of related virtual machines 👔	
	May recolution of any one-	< Back Next > Cancel	•

- 13. Select Provisioning Settings.
- 14. Click Next.



15. Select View Composer disk configuration.

Add Desktop Pool - LinkedClon	ePool	?
Desktop Pool Definition	View Composer Disks	
Type User Assignment vCenter Server	Disposable File Redirection 3 O Redirect disposable files to a non-persistent disk	Disposable File Redirection
vCenter Server Setting Desktop Pool Identification Desktop Pool Settings Provisioning Settings View Composer Disks Storage Optimization vCenter Settings Advanced Storage Options Guest Customization Ready to Complete	Network Disk size: 3072 MB (minimum 512 MB) Drive letter: Auto O not redirect disposable files	Use this option to redirect disposable files to a non- persistent disk that will be deleted automaticall y when a user's session ends.
	< Back Next >	Cancel



18. Select each of the six required vCenter Settings by using the Browse button next to each field.

Add Desktop Pool - LinkedClon	ePool	?						
Desktop Pool Definition	vCenter Settings							
Type User Assignment vCenter Server Setting Desktop Pool Identification Desktop Pool Settings Provisioning Settings	Default Image							
	1 Parent VM: /HX-VDILAB/vm/Discovered virtual mac Browse							
	2 Snapshot: /SENTINEL/Snapshot01 Browse							
	Virtual Machine Location							
View Composer Disks Storage Optimization	3 VM folder location: /HX-VDILAB/vm Browse							
vCenter Settings	Resource Settings							
Advanced Storage Options Guest Customization	4 Host or cluster: /HX-VDILAB/host/VDI-CL Browse							
Ready to Complete	5 Resource pool: /HX-VDILAB/host/VDI-CL/Resources Browse							
	6 Datastores: 1 selected Browse							
	< Back Next > C	ancel						

19. For Datastore selection, select the correct datastore and set the Storage Overcommit as "Unbounded."

20. Click OK.

esktop Pool Definition	vCenter Se	ttings					
Туре	Default Im	age					
Jser Assignment							
Center Server		rent VM: /HX-VDILAB/vm/Discovered virtual mac Browse					
esktop Pool Identificat	ion 2 Sna	2 Snapshot: /SENTINEL/Snapshot01 Browse					
Select Linked C	lone Datastores						
rovisi							
	d clone datastore can be selected.	s to use for this	desktop po	ol. Only da	tastores th	hat can be used by the select	ted
Cente							~
dvanc 🗌 Show all dat	astores (including	local datastore	es) 🕐	E	Local data	astore 📃 Shared datastore	e 😴
iuest (Datastore	Capacity (GB)	Free (GB)	FS Type	Drive Typ	Storage Overcommit 💿)
eady 🛛 👤 HX	VDI	40,960.00	40 746 14	NEC			
		40,500.00	40,746.14	INFS		Unbounded	-
		40,500.00	40,740.14	NES		Unbounded	•
		40,500.00	40,740.14	NF5		Unbounded	•
		40,500.00	40,740.14	NF5		Unbounded	•
		40,300.00	40,740.14	NFS		Unbounded	•
		40,300.00	40,746.14	NF5		Unbounded	•
					ed (GB) 50°		
Data Type Linked clones	Se	elected Free Space		ecommende		Unbounded	
Data Type	Se	elected Free Space	e (GB) Min R	ecommende		% utilization (C Max Recommen	
Data Type	Se	elected Free Space	e (GB) Min R	ecommende		% utilization (C Max Recommen	nded (
Data Type	Se	elected Free Space	e (GB) Min R	ecommende		% utilization (C Max Recommen ,080.00 40,080.00	nded (
Data Type	Se	elected Free Space	e (GB) Min R	ecommende		% utilization (C Max Recommen ,080.00 40,080.00	nded (

22. Set the Advanced Storage Options using the settings in the following screen shot.

Desktop Pool Definition	Advanced Storage Options	
Туре	Based on your resource selection, the following features	
User Assignment vCenter Server	recommended. Options that are not supported by the se hardware are disabled.	elected vSphere 5.x hosts can be configured to improve
Setting Desktop Pool Identification	✓ Use View Storage Accelerator	performance by caching certain desktop pool data.
Desktop Pool Settings	Disk Types: OS disks 🔻	Enable this option to use View Storage Accelerator for
Provisioning Settings View Composer Disks Storage Optimization	Regenerate storage accelerator 7 Days after:	this pool. View Storage Accelerator is most useful for shared disks that are read frequently, such as View
vCenter Settings	Other Options	Composer OS disks.
Advanced Storage Options Guest Customization	Use native NFS snapshots (VAAI)	Native NFS Snapshots (VAAI)
Ready to Complete	Reclaim VM disk space	VAAI (vStorage API for Array
	Initiate reclamation when unused space on VM exceeds:	Integration) is a hardware feature of certain storage arrays. It uses native snapshotting technology to
	Blackout Times	provide linked clone functionality. Choose this
	Storage accelerator regeneration and VM disk space reclamation do not occur during blackout times. The sam blackout policy applies to both operations.	option only if you have
	Add Edit Remove	Disk Space Reclamation
	Day Time	With vSphere 5.x, virtual machines can be configured
		to use a space efficient disk format that supports reclamation of unused disk space (such as deleted files)

- 24. Select Guest optimization settings.
- 25. Select the Active Directory domain, browse to the Active Directory Container where the virtual machines will be provisioned and then choose either the QuickPrep or Sysprep option you would like to use. Highlight the Customization Spec previously prepared.

Add Desktop Pool - LinkedClon	ePool					?
Desktop Pool Definition	Guest Customization					
Туре						æ
User Assignment	Domain:	vdilab-hc.local(administrator)	•		
vCenter Server						
Setting	AD container:	OU=Users,OU=I	LoginVSI Brov	vse		
Desktop Pool Identification	Allow reuse of pre-existing	a computer accou	ints 🛞			
Desktop Pool Settings		g compacer accou				
Provisioning Settings View Composer Disks	🔘 Use QuickPrep					
Storage Optimization	Power-off script name:					
vCenter Settings						
Advanced Storage Options	Power-off script paramete	Ins:			Example: p1 p2 p3	
Guest Customization	Post-synchronization scrip	t name:				
Ready to Complete						
	Post-synchronization scrip	t parameters:			Example: p1 p2 p3	
	 Use a customization speci 	ification (SysPrep))			
	Name		Guest OS		Description	
	Horizon-RDS	Window	WS			
	InfraVM-Specs	Window	ws			
	RDSH-Customization	Window	ws			
	Win10-Custom	Window	WS	Window	s 10 customization f	or
	Win10-Persistent	Window	WS			
				4 Davels	Next 2	
				< Back	Next > Cano	er j.

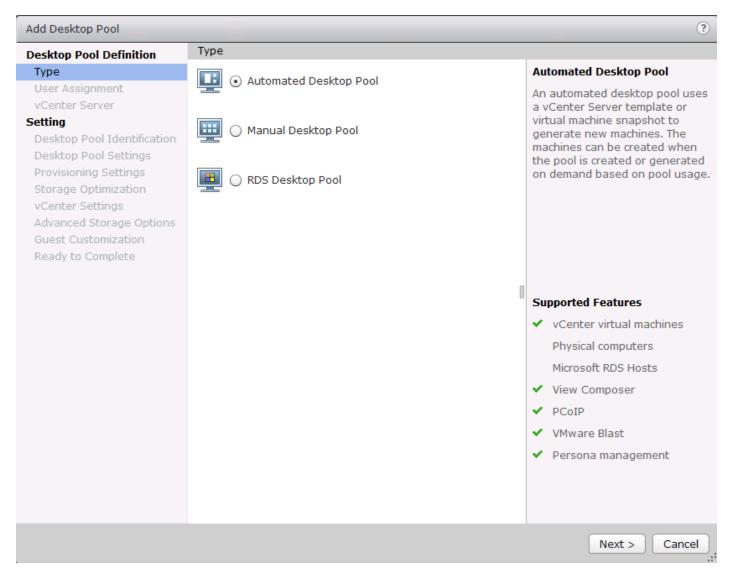
- 27. Select the checkbox "Entitle users after pool creation wizard completion" if you would like to authorize users as part of this process. Follow instructions provided in the Create Horizon 7 RDS Desktop Pool to authorize users for the Linked Clone Pool.
- 28. Click Finish to complete the Linked Clone Pool creation process.

esktop Pool Definition	Ready to Complete	
Туре		Entitle users after this wizard finishes
User Assignment		
vCenter Server	Type:	Automated
Setting	User assignment:	Floating assignment
Desktop Pool Identification	vCenter Server:	vcsa6.vdilab-hc.local(administrator@vsphere.local)
Desktop Pool Settings	Use View Composer:	Yes
Provisioning Settings	Unique ID:	LinkedClonePool
View Composer Disks	Display name:	LinkedClonePool
Storage Optimization	Access Group:	VDI-User
vCenter Settings	Desktop pool state:	Enabled
Advanced Storage Options	Remote Machine Power	Ensure machines are always powered on
Guest Customization	Policy:	
Ready to Complete	Automatic logoff after disconnect:	Never
	Connection Server restrictions:	None
	Allow users to reset their machine:	No
	Allow user to initiate separate sessions from different client devices:	No
	Delete or refresh machine on logoff:	Never
	Default display protocol:	VMware Blast
	Allow users to choose protocol:	Yes
	3D Renderer:	Disabled
	Max number of monitors:	2
		< Back Finish Cancel

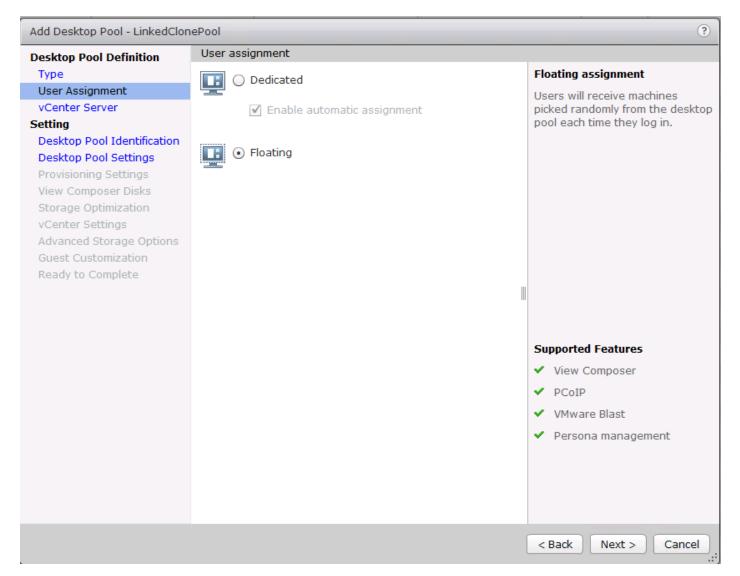
VMware Horizon Instant-Clone Windows 10 Desktop Pool Creation

To create the VMware Horizon Instant-Clone Windows 10 Desktop Pool, complete the following steps:

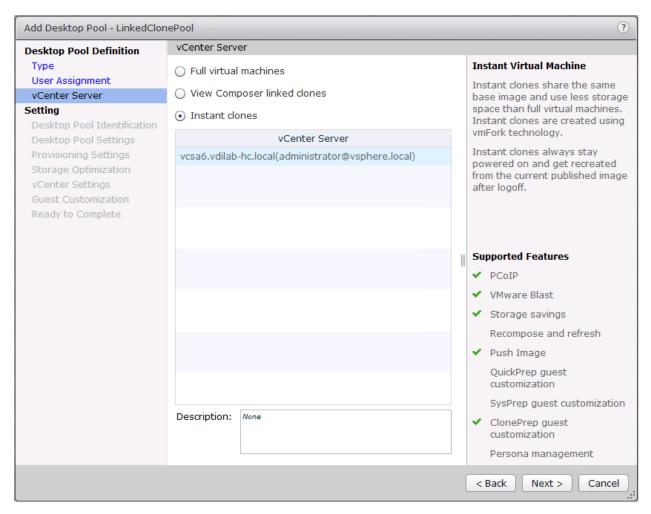
- 1. In Horizon Administrator console, select Desktop Pools in the Catalog node of the Inventory pane.
- 2. Click Add in the action pane.
- 3. Select Automated assignment type for pool.
- 4. Click Next.



- 5. Select Floating or Dedicate user assignment.
- 6. Click Next.



7. Select Instant Clones, highlight your vCenter server, then click Next.



- 8. Enter pool identification details.
- 9. Click Next.

Add Desktop Pool - InstantClo	nePool		?
Desktop Pool Definition	Desktop Pool Identi	fication	
Туре	ID:	InstantClonePool	ID
User Assignment	Display name:	InstantClonePool	The desktop pool ID is the unique
vCenter Server Setting			name used to identify this desktop pool.
Desktop Pool Identification	Access group:	VDI-User 🗸 🔻	Display Name
Desktop Pool Settings	Description:		
Provisioning Settings Storage Optimization vCenter Settings Guest Customization			The display name is the name that users will see when they connect to View Client. If the display name is left blank, the ID will be used.
Ready to Complete			Access Group
			Access groups can organize the desktop pools in your organization. They can also be used for delegated administration.
			Description
			This description is only shown on the Settings tab for a desktop pool within View Administrator.
			< Back Next > Cancel

10. Select Desktop Pool settings.

Be sure to scroll down to choose the Acrobat Flash settings.

11. Click Next.

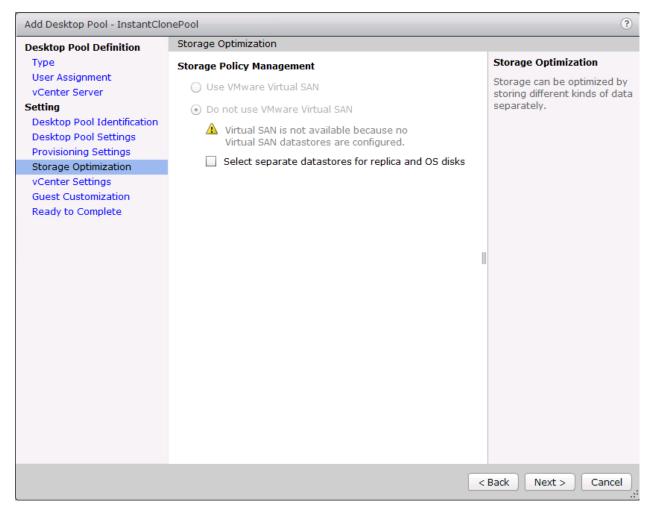
么

Add Desktop Pool - InstantClor	nePool	3
Desktop Pool Definition	Desktop Pool Settings	▲
Type User Assignment vCenter Server Setting Desktop Pool Identification	General State: Connection Server restrictions:	Enabled None Browse
Desktop Pool Settings	Remote Settings	
Provisioning Settings Storage Optimization vCenter Settings Guest Customization	Automatically logoff after disconnect: Allow user to initiate separate sessions from	Never No
Ready to Complete	different client devices:	
	Remote Display Protocol	
	Default display protocol:	VMware Blast 🛛 🔻
	Allow users to choose protocol:	Yes 🔻
	3D Renderer:	Disabled 🔻 Configure 🗿
	Max number of monitors:	2 • 2
		May require power-cycle of related virtual machines 👔
	Max resolution of any one	2560x1600 💌 🔇
	monitor:	May require power-cycle of related virtual machines ③
	HTML Access:	Enabled 3
		Requires installation of HTML Access.
	Adobe Flash Settings for Ses	isions
		< Back Next > Cancel

- 12. Select provisioning settings.
- 13. Click Next.

Add Desktop Pool - InstantClo	nePool			?	
Desktop Pool Definition	Provisioning Settings				
Туре	Basic			Naming Pattern	
User Assignment	Enable provisioning			Virtual machines will be named according to the	
Setting	vCenter Server Stop provisioning on error				
Desktop Pool Identification	Virtual Machine Naming			specified naming pattern. By default, View Manager	
Desktop Pool Settings	Use a naming pattern			appends a unique number to the specified pattern to	
Provisioning Settings	Naming Pattern:	W10-IC		provide a unique name for	
Storage Optimization		WIDTO		each virtual machine.	
vCenter Settings Guest Customization	Desktop Pool Sizing			To place this unique number elsewhere in the	
Ready to Complete	Max number of machines: 1000 Number of spare (powered on) machines: 1			pattern, use '{n}'. (For	
				example: vm-{n}-sales.).	
	Provisioning Timing			The unique number can also be made a fixed	
	Provision machines on demand			length. (For example: vm-	
	Min number of machines:	1		{n:fixed=3}-sales).	
				See the help for more	
	 Provision all machines up-fr 	ront		naming pattern syntax options.	
				optionor	
			< Ba	ck Next > Cancel	

14. Click Next.



15. Select the vCenter Settings and browse for each of the six required inputs.

Add Desktop Pool - LinkedClon	ePool	?
Desktop Pool Definition	vCenter Settings	
Туре	Default Image	
User Assignment vCenter Server	1 Parent VM: /HX-VDILAB/vm/Discovered virtual mac	Browse
Setting Desktop Pool Identification	2 Snapshot: /SENTINEL/Snapshot01	Browse
Desktop Pool Settings	Virtual Machine Location	
Provisioning Settings View Composer Disks Storage Optimization	3 VM folder location: /HX-VDILAB/vm	Browse
vCenter Settings	Resource Settings	
Advanced Storage Options Guest Customization	4 Host or cluster: /HX-VDILAB/host/VDI-CL	Browse
Ready to Complete	5 Resource pool: /HX-VDILAB/host/VDI-CL/Resources	Browse
	6 Datastores: 1 selected	Browse
	< Back	Next > Cancel

17. For Datastore selection, select the datastore with the storage overcommit as "Unbounded".

18. Click OK.

Add Desktop Pool - InstantClor	nePool						(?)	
Desktop Pool Definition	vCenter Sett	vCenter Settings						
Туре	Default Ima	ge						
User Assignment	Dara	nt VM:		1 15.	1.11			
vCenter Server	1 Pare	nt vm:	/HX-VDILAB	/vm/Disco	vered virtu	al mad	wse	
Setting Desktop Pool Identification	2 Snap	shot:	/SENTINEL/Snapshot01			Bro	Browse	
Desktop Pool Settings	Virtual Mach	ine Location						
Provisioning Settings	> VM fr	older location:	/HX-VDILAE	4000		Dro	wse	
Storage Optimization	3 1011	nder location.	/HX-VDILAB	/ vm		ВГО	wse	
Guest Closed Select Instant Clore	e Datastores							
Ready to								
Select the instant of host or cluster can		es to use for thi	is desktop p	ool. Only d	atastores	that can be u	sed by the selected	
host of cluster can	De selected.							
Show all datast	ores (including	local datastore	es) 🕐		Local dat	astore 🖳 S	hared datastore	
Dat	astore	Capacity (GB)	Free (GB)	FS Type	Drive Typ	Storag	e Overcommit	
🗹 📃 HX-VDI		40,960.00	40,746.14	NFS		Unbounded		
Data Type	Se	lected Free Space	e (GB) Min R	ecommende	ed (GB) 50	% utilization (6	Max Recommended (
Instant clones	40	,746.14	4,080	0.00	20	,080.00	40,080.00	
							OK Cancel	
		_						

- 19. Select Guest Customization.
- 20. Browse to your Active Directory Domain and to the AD container into which you want your Instant Clone machines provisioned.
- 21. Click Next.

Add Desktop Pool - InstantClo	nePool	(?)
Desktop Pool Definition	Guest Customization	p
Type User Assignment vCenter Server	Domain:	vdilab-hc.local(administrator) ▼
Setting	AD container:	OU=Computers,OU=LoginVSI Browse
Desktop Pool Identification Desktop Pool Settings Provisioning Settings	Use ClonePrep Power-off script name:	
Storage Optimization		
vCenter Settings	Power-off script parameters:	Example: p1 p2 p3
Guest Customization	parameters:	
Ready to Complete	Post-synchronization script name:	3
	Post-synchronization script parameters:	Example: p1 p2 p3
		< Back Next > Cancel

- 22. Review the summary of the pool configuration.
- 23. Select the checkbox "Entitle users after pool creation wizard completion" to authorize users or groups for the new pool.
- 24. Click Finish.

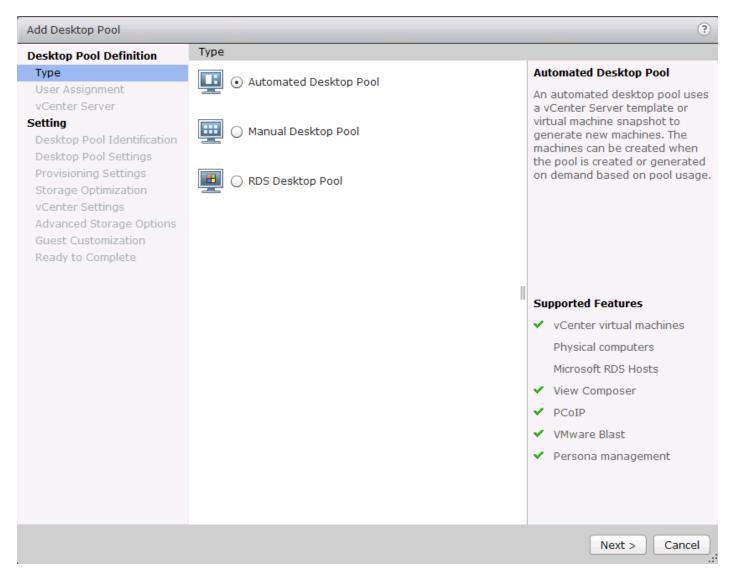
Desktop Pool Definition	Ready to Complete		
Туре		Entitle users after this wizard finished	
User Assignment		Endde dsers arter this wizard missie	:5
vCenter Server	Type:	Automated	
Getting	User assignment:	Floating assignment	
Desktop Pool Identification	vCenter Server:	vcsa6.vdilab-hc.local(administrator@vsphere.local)	
Desktop Pool Settings	Use View Composer:	No	
Provisioning Settings	Unique ID:	InstantClonePool	
Storage Optimization	Display name:	InstantClonePool	
vCenter Settings	Access Group:	VDI-User	
Guest Customization	Desktop pool state:	Enabled	
Ready to Complete	Automatic logoff after disconnect:	Never	
	Connection Server restrictions:	None	_
	Allow user to initiate separate sessions from different client devices:	No	
	Default display protocol:	VMware Blast	_
	Allow users to choose protocol:	Yes	
	3D Renderer:	Disabled	
	Max number of monitors:	2	
	Max resolution of any one monitor:	2560x1600	
	HTML Access:	Disabled	
	Adobe Flash quality:	Disabled	
	Enable provisioning:	Yes	
	Stop provisioning on error:	Yes	
		< Back Finish Cano	ام

25. Follow the instructions provided in the Create Horizon 7 RDS Desktop Pool to authorize users for the Linked Clone Pool.

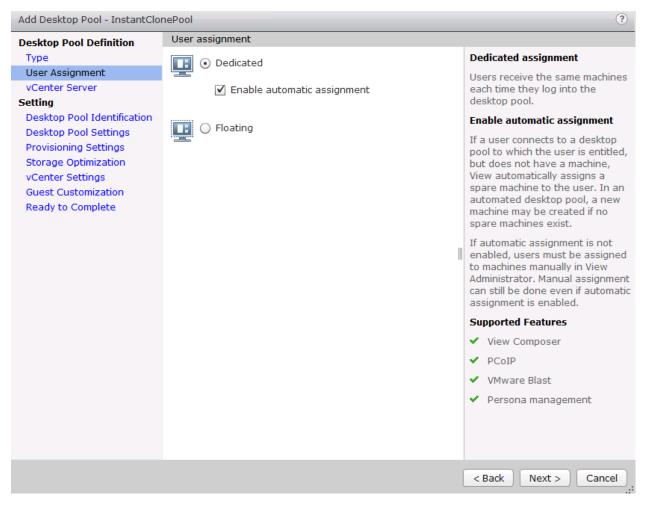
VMware Horizon Persistent Windows 10 Desktop Pool Creation

To create the VMware Horizon Persistent Windows 10 Desktop Pool, complete the following steps:

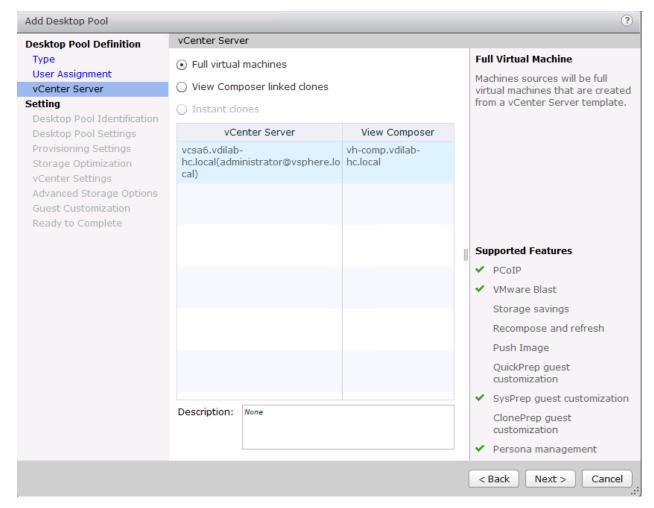
- 1. In Horizon Administrator console, select Desktop Pools in the Catalog node of the Inventory pane.
- 2. Click Add in the action pane.
- 3. Select assignment type for pool.
- 4. Click Next.



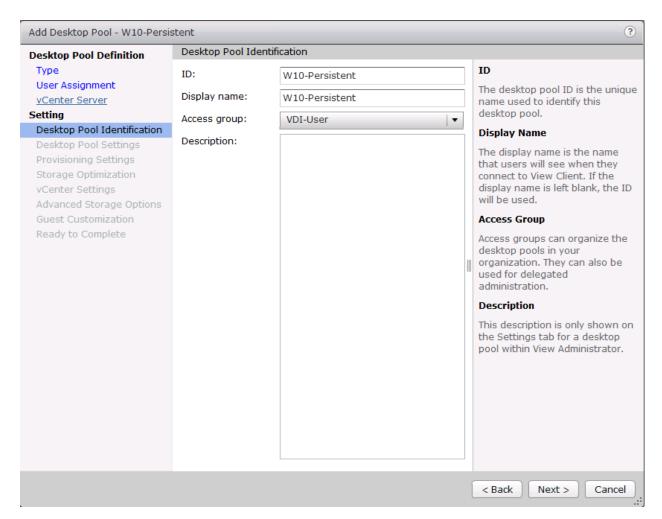
- 5. Select the Dedicated radio button.
- 6. Select the Enable automatic assignment checkbox if desired.
- 7. Click Next.



- 8. Select the Full Virtual Machines radio button and highlight your vCenter and Composer.
- 9. Click Next.



- 10. Enter the pool identification details.
- 11. Click Next.

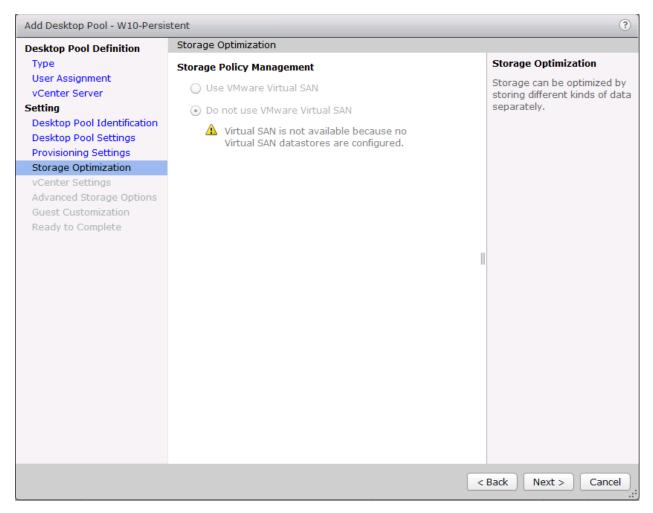


- 12. Select Desktop Pool settings.
- 13. Click Next.

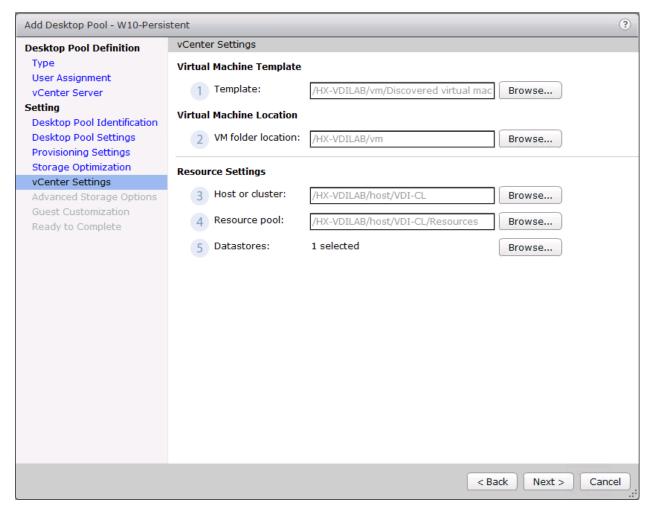
Add Desktop Pool - W10-Persis	stent		?
Desktop Pool Definition	Desktop Pool Settings		•
Type User Assignment	General		
vCenter Server	State:	Enabled 🔻	
Setting Desktop Pool Identification	Connection Server restrictions:	None Browse	
Desktop Pool Settings	Remote Settings		
Provisioning Settings Storage Optimization	Remote Machine Power Policy:	Ensure machines are always powered on $ \bullet $	
vCenter Settings Advanced Storage Options Guest Customization	Automatically logoff after disconnect:	Never 🗸 🔻	:
Ready to Complete	Allow users to reset their machines:	No 🗸 🔻	
	Remote Display Protocol		
	Default display protocol:	VMware Blast 🔻	
	Allow users to choose protocol:	Yes -	
	3D Renderer:	Disabled Configure 3	
	Max number of monitors:	2 🔻 3	
		May require power-cycle of related virtual machines 👔	
	Max resolution of any one monitor:	1920x1200 🔻 🔇	
	inonicor.	May require power-cycle of related virtual machines 👔	
	HTML Access:	Enabled ③	
		Requires installation of HTML Access.	
		< Back Next > Cancel).

- 14. Select the provisioning settings to meet your requirements.
- 15. Click Next.

Add Desktop Pool - W10-Persis	stent			?		
Desktop Pool Definition	Provisioning Settings					
Туре	Basic			Naming Pattern		
User Assignment	 Enable provisioning 			Virtual machines will be		
vCenter Server Setting	Stop provisioning on erro	r		named according to the specified naming pattern.		
Desktop Pool Identification	Virtual Machine Naming			By default, View Manager appends a unique number		
Desktop Pool Settings	Specify names manually			to the specified pattern to		
Provisioning Settings Storage Optimization	0 names entered	Enter names		provide a unique name for each virtual machine.		
vCenter Settings	Start machines in main	ntenance mode		To place this unique		
Advanced Storage Options	# Unassigned machines k	ept powered on:	1	number elsewhere in the pattern, use '{n}'. (For		
Guest Customization Ready to Complete	 Use a naming pattern 			example: vm-{n}-sales.).		
Ready to complete	Naming Pattern:	W10-PI		The unique number can		
	Desktop Pool Sizing			also be made a fixed length. (For example: vm-		
	Max number of machines:		1000	{n:fixed=3}-sales).		
	Number of spare (powered o	n) machines:	1000	See the help for more naming pattern syntax		
	Provisioning Timing			options.		
	Provision machines on de	emand				
	Min number of machines:		1			
	Provision all machines up	-front				
			< Ba	ack Next > Cancel		



- 17. Select each of the five vCenter Settings.
- 18. Click Next.

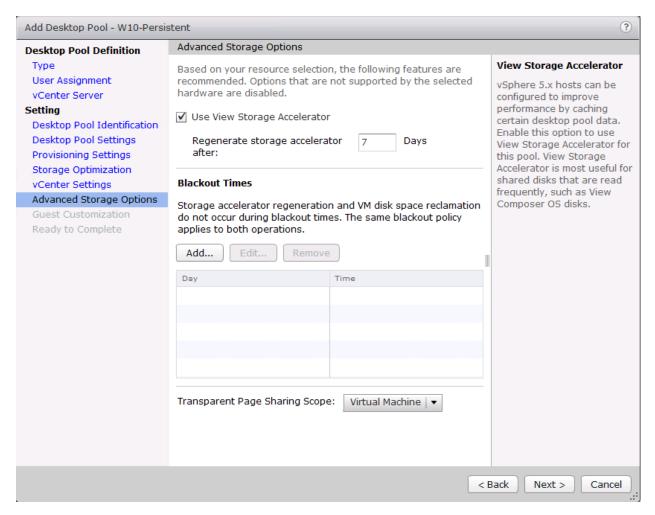


19. For Datastore selection, select the datastore with storage overcommit as "Unbounded."

20. Click OK.

Add D	esktop F	Pool - W10-Persis	stent						?
Desk	Desktop Pool Definition VCenter Settings								
Туре			Virtual Machine	Femplate					
	r Assignr		1 Template		B/vm/Discovere	vd virtual ma	Brows		
Settir	nter Serv	ver		/HA-VDILA	b/viii/Discovere	u virtuarma	BIOWS		
Des		Datastores	Vietual Machine I	acation					
Des	Select	Datastores							_
Pro				op pool. Only datastor	es that can be	used by the	selected l	nost or	
Sto	cluster	can be selected.							
vCe Adv					🗐 Local da	atastore 具	Shared o	latastore	2
Gue			Datastore		Capacity (GB)	Free (GB)	FS Type	Drive Type	
Rea	~	■ HX-VDI			40,960.00	40,746.06	NFS		•
		Springpath	DS-FCH1842V1JG		3.50	0.44	VMFS5	Non-SSD	
		🗐 Springpath	DS-FCH1936V0GE		3.50	0.44	VMFS5	Non-SSD	8
		🗐 Springpath	DS-FCH1937V2JT		3.50	0.44	VMFS5	Non-SSD	
		🗐 Springpath	DS-FCH1937V2JU		3.50	0.44	VMFS5	Non-SSD	
		🗐 Springpath	OS-FCH1937V2JV		3.50	0.44	VMFS5	Non-SSD	•
	Free s	space selected:	40.746.06	(A minimum of 44,000	.00 GB is recom	mended for	new virtu	al machines	5
			,.						<u></u>
							ОК	Cancel	
l									
						_			
						<	Back	Vext >	Cancel .:

- 21. Select Advance Storage Options and enable the View Storage Accelerator.
- 22. Click Next.



- 23. Select Guest optimization settings.
- 24. Click Next.

Add Desktop Pool - W10-Persis	stent			?			
Desktop Pool Definition	Guest Customization						
Type User Assignment vCenter Server Setting Desktop Pool Identification Desktop Pool Settings	 None - Customization will be done manually Do not power on virtual machines after creation Use this customization specification: 			2			
Provisioning Settings Storage Optimization vCenter Settings	Name Guest OS Description Horizon-RDS Windows						
Advanced Storage Options	InfraVM-Specs	Windows					
Guest Customization Ready to Complete	RDSH-Customization						
Ready to complete	Win10-Custom	Windows	Windows 10 customization for Horizon testbed.				
	Win10-Persistent	Windows					
			< Back Next >	Cancel			

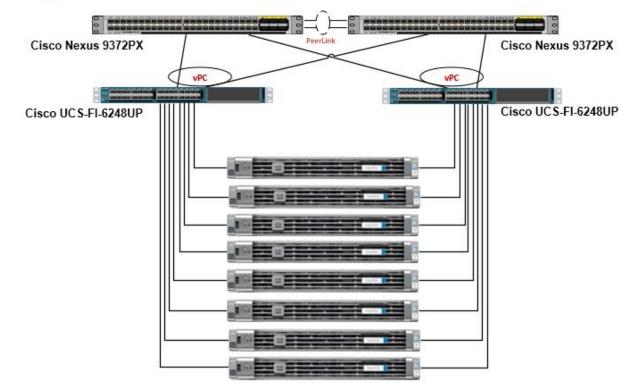
- 25. Review the summary of the pool you are creating.
- 26. Select the checkbox "Entitle users after pool creation wizard completion" to authorize users for the pool.
- 27. Click Finish.

Desktop Pool Definition	Ready to Complete	
Type User Assignment		 Entitle users after this wizard finishes
vCenter Server	Туре:	Automated
Setting	User assignment:	Dedicated assignment
Desktop Pool Identification	Assign on first login:	Yes
Desktop Pool Settings	vCenter Server:	vcsa6.vdilab-hc.local(administrator@vsphere.local)
Provisioning Settings	Use View Composer:	No
Storage Optimization	Unique ID:	W10-Persistent
vCenter Settings	Display name:	W10-Persistent
Advanced Storage Options	Access Group:	VDI-User
Guest Customization	Desktop pool state:	Enabled
Ready to Complete	Remote Machine Power Policy:	Ensure machines are always powered on
	Automatic logoff after disconnect:	Never
	Connection Server restrictions:	None
	Allow users to reset their machine:	No
	Default display protocol:	VMware Blast
	Allow users to choose protocol:	Yes
	3D Renderer:	Disabled
	Max number of monitors:	2
	Max resolution of any one monitor:	1920x1200
	HTML Access:	Disabled
	Adobe Flash quality:	Disabled

28. Follow the instructions provided in the Create Horizon 7 RDS Desktop Pool to authorize users for the Linked Clone Pool.

Test Setup and Configurations

In this project, we tested a single Cisco HyperFlex cluster running eight Cisco UCS HX220c-MS4 Rack Servers in a single Cisco UCS domain. This solution is tested to illustrate linear scalability for each workload studied.



Cisco HyperFlex and VMware Horizon 7, Detailed Architecture

Hardware Components:

- 2 x Cisco UCS 6248UP Fabric Interconnects
- 2 x Cisco Nexus 9372PX Access Switches
- 8 x Cisco UCS HX220c-M4 Rack Servers (2 Intel Xeon processor E5-2690 v4 CPUs at 2.6 GHz, with 512 GB of memory per server [32 GB x 16 DIMMs at 2400 MHz]).
- Cisco VIC 1227 mLOM
- 120GB 2.5" 6G SATA SSD drive
- 480GB 2.5" 6G SATA SSD drive
- 6 x 1.2TB 2.5" 12G 10K RPM SAS drive
- 2 x 64GB SD card

Software components:

- Cisco UCS firmware 3.1(2b)
- Cisco HyperFlex data platform 1.8.1b
- VMware vSphere 6.0
- VMware Horizon 7 Hosted Virtual Desktops and Hosted Shared Desktops.
- VMware Horizon View Composer Server
- v-File Server for User Profiles
- Microsoft SQL Server 2012
- Microsoft Windows 10
- Microsoft Windows 2012 R2
- Microsoft Office 2016
- Login VSI 4.1.5.115

Testing Methodology and Success Criteria

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

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

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

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

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

Testing Procedure

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

Pre-Test Setup for Testing

All machines were shut down utilizing the VMware Horizon 7 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 1000 full scale test users to become active within two minutes after the last session is launched.

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

- 1. Time 0:00:00 Start PerfMon Logging on the following systems:
 - Infrastructure and VDI Host Blades used in test run
 - All Infrastructure VMs used in test run (AD, SQL, View Connection brokers, image mgmt., etc.)
- 2. Time 0:00:10 Start Storage Partner Performance Logging on Storage System.
- 3. Time 0:05: Boot RDS Machines using VMware Horizon 7 Administrator Console.
- 4. Time 0:06 First machines boot.
- 5. Time 0:35 Single Server or Scale target number of RDS Servers registered on XD.

No more than 60 Minutes of rest time is allowed after the last desktop is registered and available on VMware Horizon 7 Administrator Console dashboard. Typically a 20-30 minute rest period for Windows 7 desktops and 10 minutes for RDS VMs is sufficient.

- 6. Time 1:35 Start Login VSI 4.1.4 Office Worker Benchmark Mode Test, setting auto-logoff time at 900 seconds, with Single Server or Scale target number of desktop VMs utilizing sufficient number of Launchers (at 20-25 sessions/Launcher).
- 7. Time 2:23 Single Server or Scale target number of desktop VMs desktops launched (48 minute benchmark launch rate).
- 8. Time 2:25 All launched sessions must become active.

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

- 9. Time 2:40 Login VSI Test Ends (based on Auto Logoff 900 Second period designated above).
- 10. Time 2:55 All active sessions logged off.

All sessions launched and active must be logged off for a valid test run. The VMware Horizon 7 Administrator Dashboard must show that all desktops have been returned to the registered/available state as evidence of this condition being met.

11. Time 2:57 All logging terminated; Test complete.

- 12. Time 3:15 Copy all log files off to archive; Set virtual desktops to maintenance mode through broker; Shutdown all Windows 7 machines.
- 13. Time 3:30 Reboot all hypervisors.
- 14. Time 3:45 Ready for new test sequence.

Success Criteria

Our "pass" criteria for this testing follows is Cisco will run tests at a session count level that effectively utilizes the blade capacity measured by CPU utilization, memory utilization, storage utilization, and network utilization. We will use Login VSI version 4.1.5 to launch Knowledge Worker workloads. 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 VMware Horizon Connection Server Dashboard 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. Stuck sessions define a test failure condition.

Cisco requires three consecutive runs with results within +/-1% variability to pass the Cisco Validated Design performance criteria. For white papers written by partners, two consecutive runs within +/-1% 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 VMware Horizon 7 Hosted Shared Desktop with VMware Horizon 7 Composer provisioning using Microsoft Windows Server 2012 R2 sessions on Cisco UCS HX220c-M4S.

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 VMware products.

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

VSImax 4.1.x Description

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

Login VSI is different in approach. Login VSI is not primarily designed to be a steady state benchmark (however, if needed, Login VSI can act like one). Login VSI was designed to perform benchmarks for SBC or

VDI workloads through system saturation. Login VSI loads the system with simulated user workloads using well known desktop applications like Microsoft Office, Internet Explorer and Adobe PDF reader. By gradually increasing the amount of simulated users, the system will eventually be saturated. Once the system is saturated, the response time of the applications will increase significantly. This latency in application response times show a clear indication whether the system is (close to being) overloaded. As a result, by nearly overloading a system it is possible to find out what its true maximum user capacity is.

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

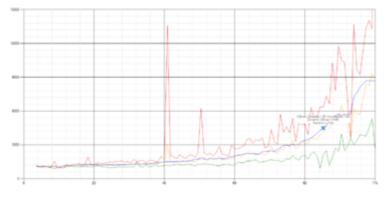
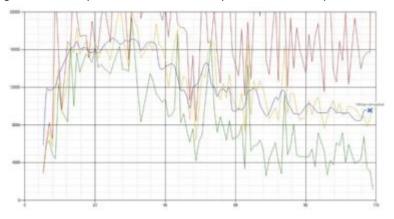


Figure 41 Sample of a VSI Test Response Time Graph with a Clear Performance Issue



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

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

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

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

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

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

With the introduction of Login VSI 4.1 we also created a new method to calculate the base phase of an environment. With the new workloads (Taskworker, Powerworker, etc.) enabling 'base phase' for a more reliable baseline has become obsolete. The calculation is explained below. In total 15 lowest VSI response time samples are taken from the entire test, the lowest 2 samples are removed and the 13 remaining samples are averaged. The result is the Baseline. The calculation is as follows:

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

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

Always a 5 Login VSI response time samples are averaged + 40% of the amount of "active" sessions. For example, if the active sessions is 60, then latest 5 + 24 (=40% of 60) = 31 response time measurement are used for the average calculation.

To remove noise (accidental spikes) from the calculation, the top 5% and bottom 5% 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% of 31 = 1.55, rounded to 2). At 60 users the average is then calculated over the 27 remaining results.

VSImax v4.1.x is reached when the VSIbase + a 1000 ms latency threshold is not reached by the average VSI response time result. Depending on the tested system, VSImax response time can grow 2 - 3x the baseline average. In end-user computing, a 3x increase in response time in comparison to the baseline is typically regarded as the maximum performance degradation to be considered acceptable.

In VSImax v4.1.x this latency threshold is fixed to 1000ms, this allows better and fairer comparisons between two different systems, especially when they have different baseline results. Ultimately, in VSImax v4.1.x, the performance of the system is not decided by the total average response time, but by the latency is has under load. For all systems, this is now 1000ms (weighted).

The threshold for the total response time is: average weighted baseline response time + 1000ms.

When the system has a weighted baseline response time average of 1500ms, the maximum average response time may not be greater than 2500ms (1500+1000). If the average baseline is 3000 the maximum average response time may not be greater than 4000ms (3000+1000).

When the threshold is not exceeded by the average VSI response time during the test, VSImax is not hit and the amount of sessions ran successfully. This approach is fundamentally different in comparison to previous VSImax methods, as it was always required to saturate the system beyond VSImax threshold.

Lastly, VSImax v4.1.x is now always reported with the average baseline VSI response time result. For **example: "The VSImax v4.1 was 125 with a baseline of 1526ms". This helps considerably in the comparison** of systems and gives a more complete understanding of the system. The baseline performance helps to understand the best performance the system can give to an individual user. VSImax indicates what the total user capacity is for the system. These two are not automatically connected and related:

When a server with a very fast dual core CPU, running at 3.6 GHZ, is compared to a 10 core CPU, running at 2,26 GHZ, the dual core machine will give and individual user better performance than the 10 core machine. This is indicated by the baseline VSI response time. The lower this score is, the better performance an individual user can expect.

However, the server with the slower 10 core CPU will easily have a larger capacity than the faster dual core system. This is indicated by VSImax v4.1.x, and the higher VSImax is, the larger overall user capacity can be expected.

With Login VSI 4.1.x a new VSImax method is introduced: VSImax v4.1. This methodology gives much better insight in system performance and scales to extremely large systems.

Test Results

Boot Storms

A key performance metric for desktop virtualization environments is the ability to boot the virtual machines quickly and efficiently to minimize user wait time for their desktop.

As part of Cisco's virtual desktop test protocol, we shut down each virtual machine at the conclusion of a benchmark test. When we run a new test, we cold boot all 1000 desktops and measure the time it takes for the 1000th virtual machine to register as available in the Horizon Administrator console.

The Cisco HyperFlex HX220c M4S hybrid cluster running Data Platform version 1.8(1b) software can accomplish this task in 5 minutes as shown in the following charts:

Figure 42 1000 Horizon 7 Linked-Clone Windows 10 with Office 2016 Virtual Desktops Boot and Register as Available in less than 5 minutes

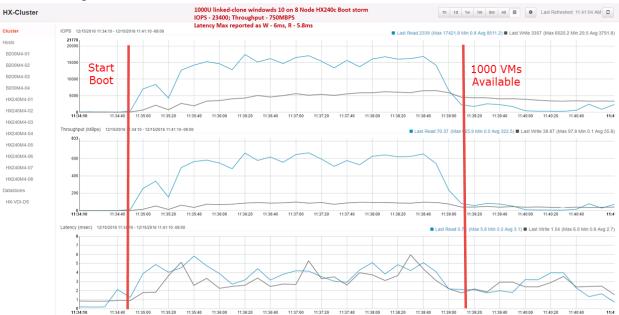




Figure 43 1000 Horizon 7 Full-Clone Windows 10 with Office 2016 Boot and Register as Available in less than 5 minutes

Recommended Maximum Workload and Configuration Guidelines for an Eight Node HX220c-M4S Rack Server HyperFlex Cluster

For VMware Horizon 7 RDS Hosted Shared Desktop use cases, the recommended maximum workload was determined based on both Login VSI Knowledge Worker workload end user experience measures and HX220c M4S server operating parameters.

This recommended maximum workload approach allows you to determine the server N+1 fault tolerance load the blade can successfully support in the event of a server outage for maintenance or upgrade.

Our recommendation is that the Login VSI Average Response and VSI Index Average should not exceed the Baseline plus 2000 milliseconds to insure that end user experience is outstanding. Additionally, during steady state, the processor utilization should average no more than 90-95%.



Memory should never be oversubscribed for Desktop Virtualization workloads.

Callouts have been added throughout the data charts to indicate each phase of testing.

Test	
Phase	Description

Test Phase	Description
Boot	Start all RDS or VDI virtual machines at the same time.
Login	The Login VSI phase of test is where sessions are launched and start executing the work- load 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.

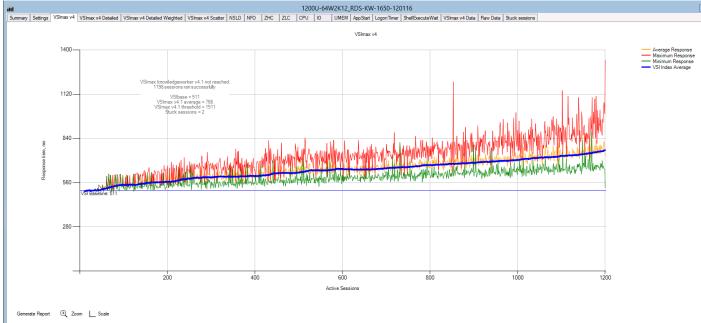
The recommended maximum workload for a HyperFlex cluster configured on HX220c-M4S nodes with E2690 v4 processors and 512GB of RAM for Windows Server 2012 R2 RDS Hosted Sessions and persistent/non-persistent Hosted Virtual Desktop users is 1200 sessions and 1000 Windows 10 with Office 2016 virtual desktops respectively.

RDSH Server Pool Testing on Eight Node Cisco HyperFlex Cluster

RDS Farm configured with 64 Windows 2012 R2 server in automated desktop pool hosting 1200 User Sessions on 8 HX220c-M4S Servers.

Test result highlights include:

- 0.511 second baseline response time
- 0.766 second average response time with 1000 desktops running
- Average CPU utilization of 70 percent during steady state
- Average of 180 GB of RAM used out of 512 GB available
- 2867Mbps peak network utilization per host.
- Average Read Latency 3.3ms/Max Read Latency 17.9ms
- Average Write Latency 6.5ms/Max Write Latency 10.4ms
- 6500 peak I/O operations per second (IOPS) per cluster at steady state
- 260MBps peak throughput per cluster at steady state





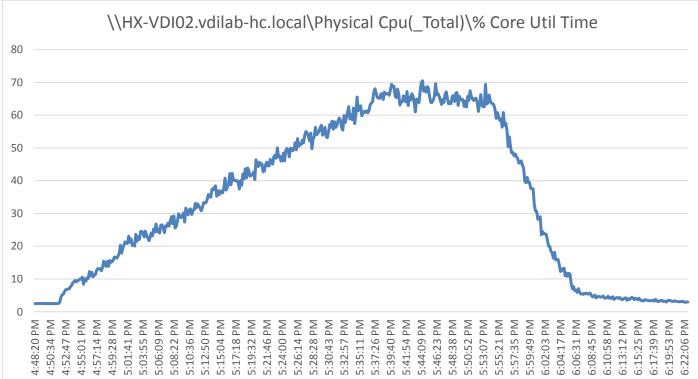
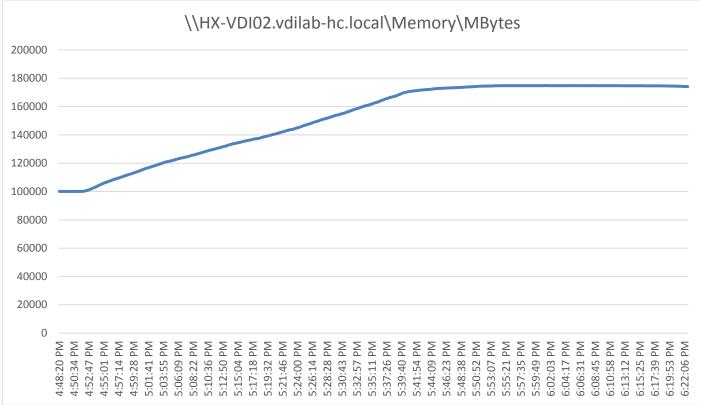


Figure 45 Sample ESXi host CPU Core Utilization Running 1200 User Test with 8 RDSH Server VMs



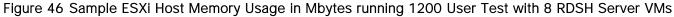
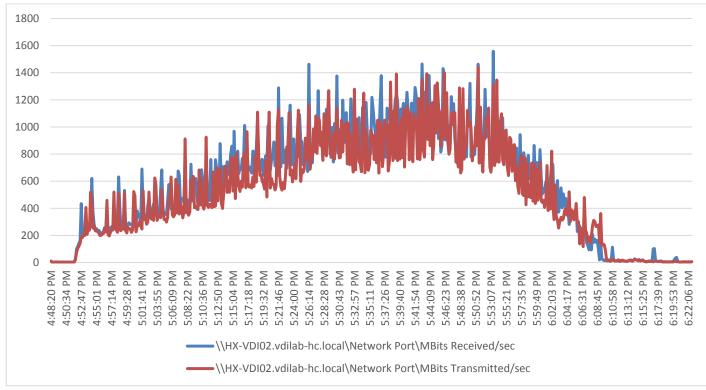


Figure 47 Sample ESXi Host Network Adapter (VMNICs) Mbits Received /Transmitted Per Sec Running 1200 User Test with 8 RDSH Server VMs



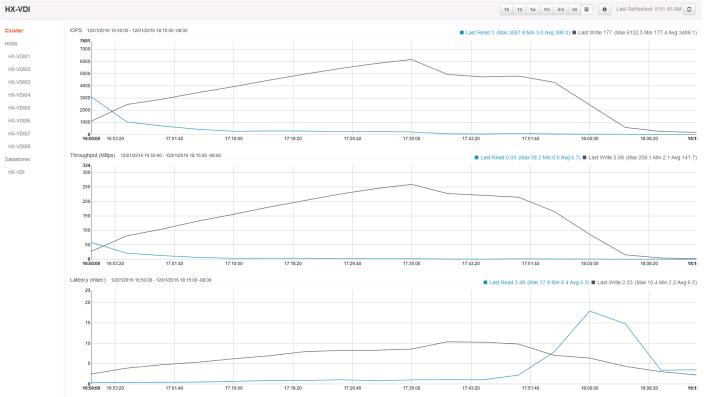


Figure 48 HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 1200 User Test on RDSH Server Windows Server 2012 R2

1000 Windows 10 Linked-clone Desktop Pool testing on eight node Cisco HyperFlex Cluster

Floating assignment automated Linked-clone desktop pool with 1000 Windows 10 VMs hosting 1000 User Sessions on 8 x HX220c-M4S Servers.

Test result highlights include:

- 0.627 second baseline response time
- 0.977 second average response time with 1000 desktops running
- Average CPU utilization of 80 percent during steady state
- Average of 300 GB of RAM used out of 512 GB available
- 3326Mbps peak network utilization per host.
- Average Read Latency 2.3ms/Max Read Latency 5.1ms
- Average Write Latency 4.1ms/Max Write Latency 7.3ms
- 12280 peak I/O operations per second (IOPS) at steady state
- 267MBps peak throughput per cluster at steady state

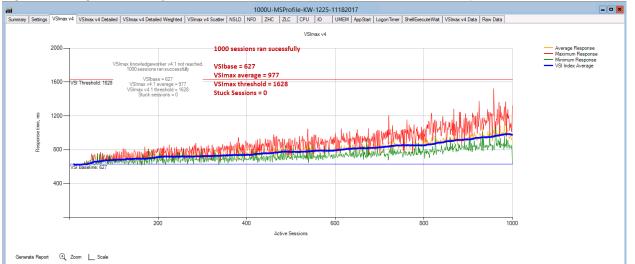
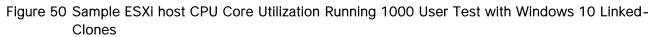
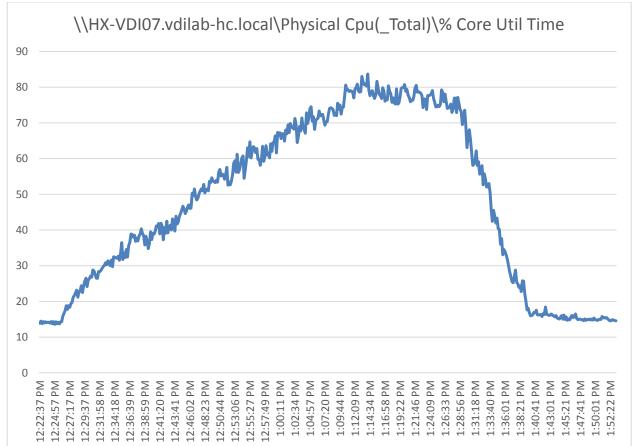


Figure 49 Login VSI Analyzer Chart for 1000 Users Linked-Clone Desktop Test





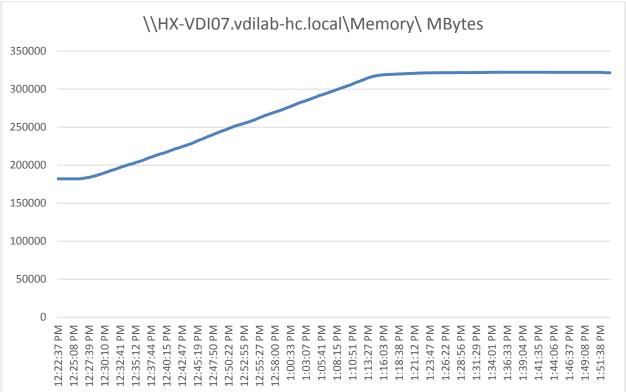


Figure 51 Sample ESXi Host Memory Usage in Mbytes Running 1000 User Test with Windows 10 Linked-Clones

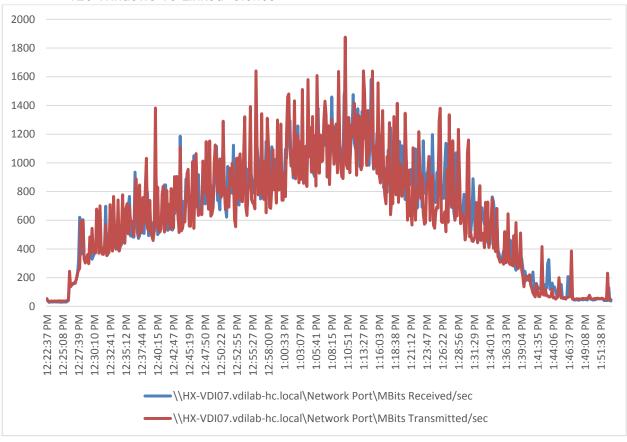
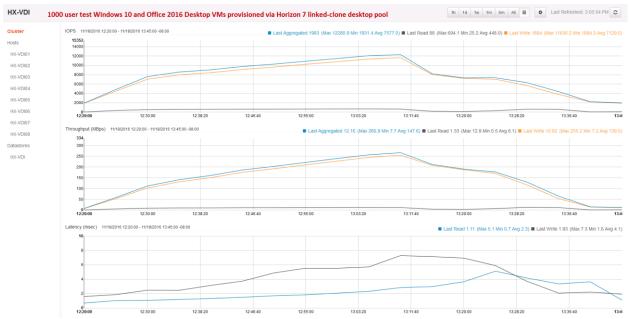


Figure 52 Sample ESXi host Network Adapter (VMNICs) Mbits Received /Transmitted Per Sec Running 125 Windows 10 Linked-Clones

Figure 53 HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 1000 User Test on Linked-Clone Windows 10



1000 Windows 10 Instant-clone Desktop Pool testing on Eight Node Cisco HyperFlex Cluster

Travis Wood from VMware describes Instant Clones this way in his <u>blog</u> on the subject. Horizon 7 has introduced a new method of provisioning with Instant Clones. Instant Clones are similar to linked clones in that all desktops read from a replica disk and write to their own disk, but Instant Clone takes it one step further by doing the same thing with memory. Instant Clones utilize a new feature of vSphere 6 where desktop VMs are forked (that is, Instant Clones are created) off a running VM–instead of cloning a powered-off VM–which provides savings for provisioning, updates, and memory utilization.

Instant Clones are convenient for virtual desktop infrastructure administrators, because these desktops don't need Refresh, Recompose and Rebalance operations. The reason is that after the user logs out the VM, his desktop is deleted, and linked clone recomposition is not needed.

Instant Clone provisioning time is generally one third of the time for the same size desktop pool provisioned as linked clones with the Horizon Composer. In this study, we provisioned 1000 Instant Clones in 22 minutes.

Floating assigned automated Instant-clone desktop pool with 1000 Windows 10 VMs hosting 1000 User Sessions on 8 x HX220c-M4S Servers.

Test result highlights include:

- 0.625 second baseline response time
- 0.967 second average response time with 1000 desktops running
- Average CPU utilization of 75 percent during steady state
- Average of 320 GB of RAM used out of 512 GB available
- 3720Mbps peak network utilization per host.
- Average Read Latency 3.3ms/Max Read Latency 17.9ms
- Average Write Latency 6.5ms/Max Write Latency 10.4ms
- 21000 peak I/O operations per second (IOPS) per cluster at steady state
- 323MBps peak throughput per cluster at steady state

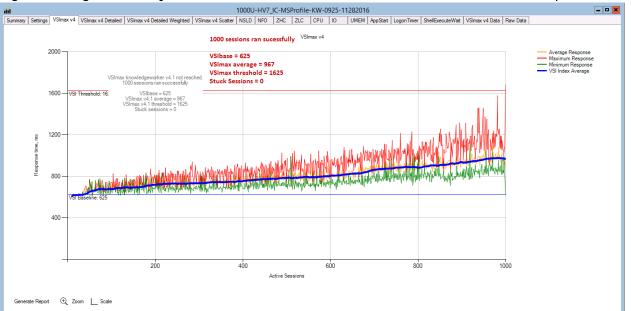
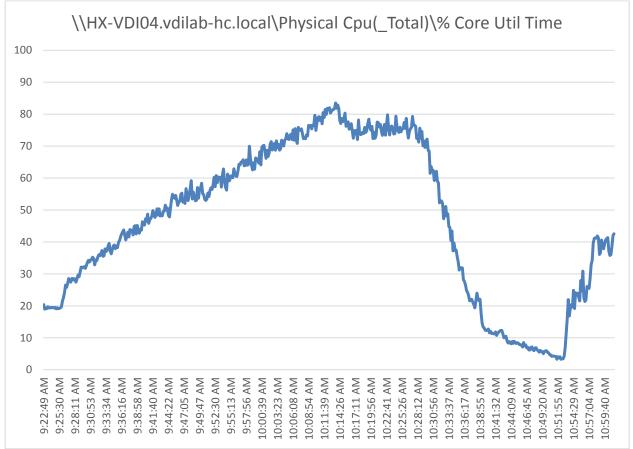


Figure 54 Login VSI Analyzer Chart for 1000 Windows 10 Instant-Clone Virtual Desktops

Figure 55 Sample ESXi host CPU Core Utilization Running 1000 Windows 10 Instant-Clone Virtual Desktops



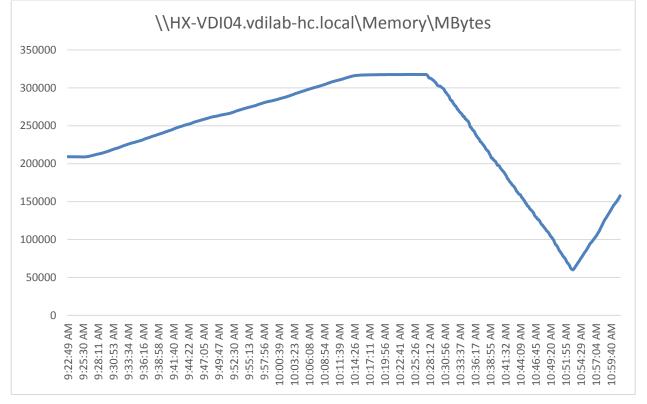
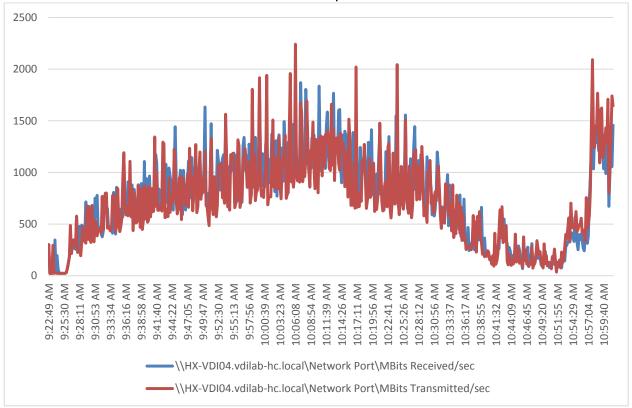




Figure 57 ESXi Host Network Adapter (VMNICs) Mbits Received /Transmitted Per Sec Running 1000 Windows 10 Instant-Clone Virtual Desktops



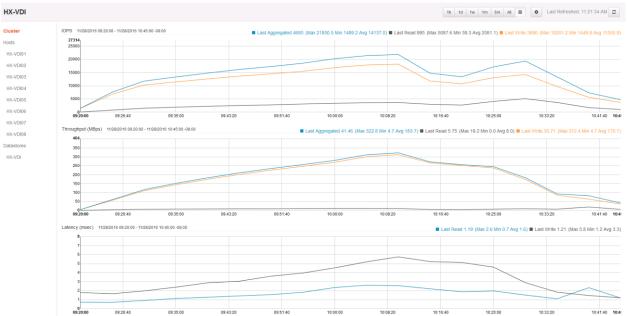


Figure 58 HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 1000 User Test on Instant-Clone Windows 10

1000 Windows 10 Full Clone Desktop Pool Testing on Eight Node Cisco HyperFlex Cluster

1000 User Dedicated assignment automated pool Windows 10 with Office 2016 full clone desktops on 8 x HX220c-M4S Server HyperFlex Cluster.

Test result highlights include:

- 0.628 second baseline response time
- 0.979 second average response time with 1000 desktops running
- Average CPU utilization of 78 percent during steady state
- Average of 320GB of RAM used out of 512 GB available per node
- 1625Mbps peak network utilization per host.
- Average Write Latency 2.9ms/Max Write Latency 4.3ms
- Average Read Latency 2.0ms/Max Read Latency 3.2ms
- 10500 peak I/O operations per second (IOPS) at steady state
- 250MBps peak throughput at steady state

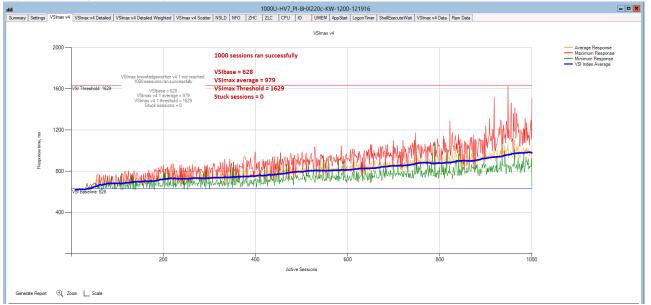
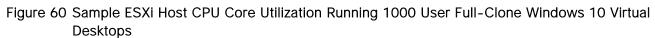
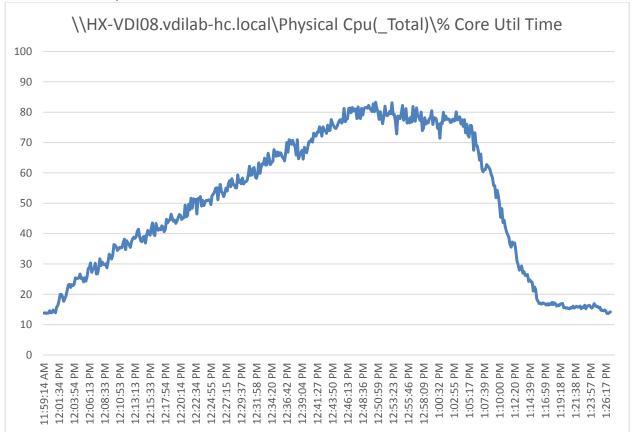


Figure 59 Login VSI Analyzer Chart for 1000 User Full-Clone Desktops





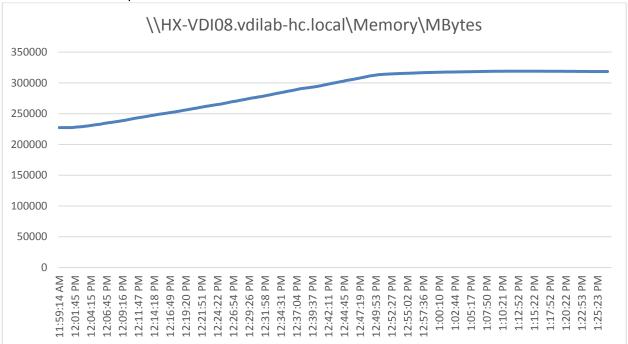
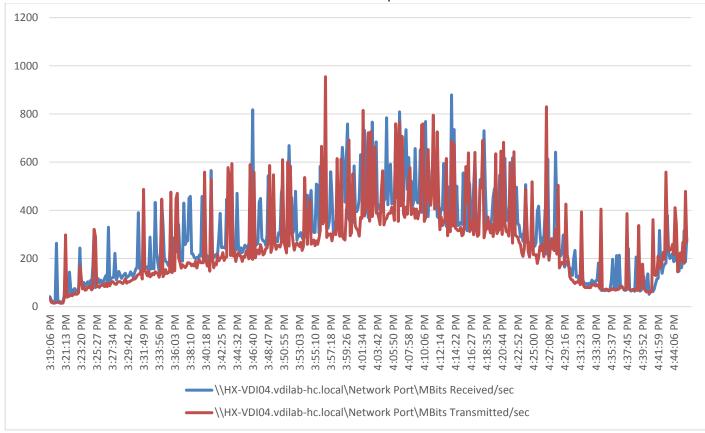


Figure 61 Sample ESXi Host Memory Usage in Mbytes Running 1000 User Full-Clone Windows 10 Virtual Desktops

Figure 62 Sample ESXi Host Network Adapter (VMNICs) Mbits Received /Transmitted Per Sec Running 1000 User Full-Clone Windows 10 Virtual Desktops



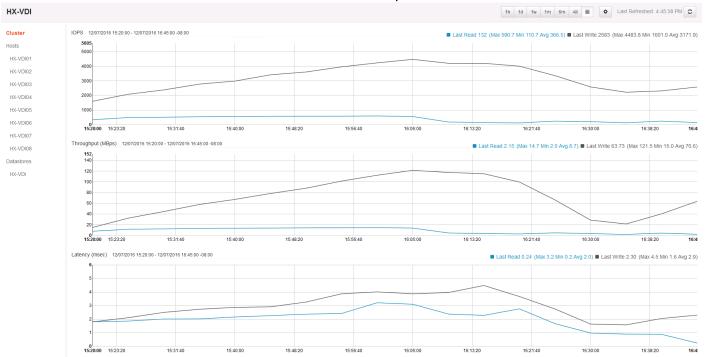


Figure 63 HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 750 User Test on Full Clone Windows 10 Virtual Desktops

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 hyperconverged system.

Delivering responsive, resilient, high performance VMware Horizon 7 provisioned Windows 10 Virtual Machines and 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 Broadwell E5-2600 v4 processors and Cisco 2400Mhz memory. In fact, we have set the industry standard in performance for Desktop Virtualization on a hyper-converged platform.

About the Authors

Hardik Patel, Senior Technical Marketing Engineer, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.

Hardik is a subject matter expert on Cisco HyperFlex, Cisco Unified Computing System, Cisco Nexus Switching, VMware vSphere and VMware Horizon end user computing. Hardik is a **member of the Cisco's** Computer Systems Product Group team.

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, we would like to acknowledge the significant contribution and expertise that resulted in developing this document:

- Mike Brennan, Product Manager, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.
- Swapnil Deshmukh, Technical Marketing Engineer, Springpath, Inc.

Appendix A - Cisco Nexus 9372 Switch Configuration

Switch A Configuration

!Command: show running-config !Time: Fri Dec 9 17:17:40 2016

version 7.0(3)I2(2d) switchname XXXXXXXXXXXX class-map type network-qos class-fcoe match qos-group 1 class-map type network-gos class-all-flood match qos-group 2 class-map type network-qos class-ip-multicast match qos-group 2 vdc XXXXXXXXXX id 1 limit-resource vlan minimum 16 maximum 4094 limit-resource vrf minimum 2 maximum 4096 limit-resource port-channel minimum 0 maximum 511 limit-resource u4route-mem minimum 248 maximum 248 limit-resource u6route-mem minimum 96 maximum 96 limit-resource m4route-mem minimum 58 maximum 58 limit-resource m6route-mem minimum 8 maximum 8

feature telnet

cfs eth distribute

feature interface-vlan

feature hsrp

feature lacp

feature dhcp

feature vpc

feature lldp

clock protocol ntp vdc 1

no password strength-check username admin password 5 \$1\$MSJwTJtn\$Bo0IrVnESUVxLcbRHg86j1 role network-admin ip domain-lookup no service unsupported-transceiver class-map type qos match-all class-fcoe policy-map type qos jumbo class class-default set qos-group 0 copp profile strict snmp-server user admin network-admin auth md5 0x71d6a9cf1ea007cd3166e91a6f3807e5 priv 0x71d6a9cf1ea007cd3166e91a6f3807e5 localizedkey rmon event 1 log trap public description FATAL(1) owner PMON@FATAL rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL rmon event 3 log trap public description ERROR(3) owner PMON@ERROR rmon event 4 log trap public description WARNING(4) owner PMON@WARNING

rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

ntp server 10.10.30.2

ntp peer 10.10.30.3

ntp server 10.10.40.2

ntp peer 10.10.40.3

ntp server 10.10.50.2

ntp peer 10.10.50.3

ntp server 171.68.38.66 use-vrf management

ntp logging

ntp master 8

vlan 1,50-54

vlan 50

name InBand-Mgmt-C1

vlan 51

name Infra-Mgmt-C1

vlan 52

name StorageIP-C1

vlan 53

name vMotion-C1

vlan 54

name VM-Data-C1

service dhcp

ip dhcp relay

ip dhcp relay information option

ipv6 dhcp relay

vrf context management

ip route 0.0.0.0/0 10.29.132.1

vpc domain 50

role priority 1000

peer-keepalive destination 10.29.132.5 source 10.29.132.4

interface Vlan1

no shutdown

ip address 10.29.132.2/24

interface Vlan50

no shutdown

ip address 10.10.50.2/24

hsrp version 2

hsrp 50

preempt

priority 110

ip 10.10.50.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface Vlan51

no shutdown

ip address 10.10.51.2/24

hsrp version 2

hsrp 51

preempt

priority 110

ip 10.10.51.1

interface Vlan52

no shutdown

ip address 10.10.52.2/24

hsrp version 2

hsrp 52

preempt

priority 110

ip 10.10.52.1

interface Vlan53

no shutdown

ip address 10.10.53.2/24

hsrp version 2

hsrp 53

preempt

priority 110

ip 10.10.53.1

interface Vlan54

no shutdown

ip address 10.54.0.2/20

hsrp version 2

hsrp 54

preempt

priority 110

ip 10.54.0.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface port-channel10

description vPC-PeerLink

switchport mode trunk

switchport trunk allowed vlan 1,50-54

spanning-tree port type network

service-policy type qos input jumbo vpc peer-link

interface port-channel11 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 11

interface port-channel12 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 12

interface Ethernet1/1

switchport mode trunk

switchport trunk allowed vlan 1,50-54

channel-group 10 mode active

interface Ethernet1/2 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/3

switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/4

switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/5

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 11 mode active

interface Ethernet1/6

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 11 mode active

interface Ethernet1/7

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 12 mode active

interface Ethernet1/8

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 12 mode active

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/26 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/27

switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

switchport mode trunk switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/29 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/30 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/31 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/32 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/33

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0

vrf member management

ip address 10.29.132.4/24

clock timezone PST -8 0

clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60

line console

line vty

boot nxos bootflash:/nxos.7.0.3.12.2d.bin

Switch B Configuration

!Command: show running-config !Time: Fri Dec 9 17:18:36 2016

version 7.0(3)I2(2d) switchname XXXXXXXXXXX class-map type network-gos class-fcoe match qos-group 1 class-map type network-qos class-all-flood match qos-group 2 class-map type network-qos class-ip-multicast match qos-group 2 vdc XXXXXXXXX id 1 limit-resource vlan minimum 16 maximum 4094 limit-resource vrf minimum 2 maximum 4096 limit-resource port-channel minimum 0 maximum 511 limit-resource u4route-mem minimum 248 maximum 248 limit-resource u6route-mem minimum 96 maximum 96 limit-resource m4route-mem minimum 58 maximum 58 limit-resource m6route-mem minimum 8 maximum 8

feature telnet

cfs eth distribute

feature interface-vlan

feature hsrp

feature lacp

feature dhcp

feature vpc

feature lldp

clock protocol ntp vdc 1

no password strength-check

username admin password 5 \$1\$jEwHqUvM\$gpOec2hramkyX09KD3/Dn. role network-admin

ip domain-lookup

no service unsupported-transceiver

class-map type qos match-all class-fcoe

policy-map type qos jumbo

class class-default

set qos-group 0

copp profile strict

snmp-server user admin network-admin auth md5 0x9046c100ce1f4ecdd74ef2f92c4e83f9

priv 0x9046c100ce1f4ecdd74ef2f92c4e83f9 localizedkey

rmon event 1 log trap public description FATAL(1) owner PMON@FATAL

rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL

rmon event 3 log trap public description ERROR(3) owner PMON@ERROR

rmon event 4 log trap public description WARNING(4) owner PMON@WARNING

rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

ntp peer 10.10.30.2

ntp server 10.10.30.3

ntp peer 10.10.40.2

ntp server 10.10.40.3

ntp peer 10.10.50.2

ntp server 10.10.50.3

ntp server 171.68.38.66 use-vrf management

ntp logging

ntp master 8

vlan 1,50-54

vlan 50

name InBand-Mgmt-C1

vlan 51

name Infra-Mgmt-C1

vlan 52

name StoragelP-C1

vlan 53

name vMotion-C1

vlan 54

name VM-Data-C1

service dhcp

ip dhcp relay

ip dhcp relay information option

ipv6 dhcp relay

vrf context management

ip route 0.0.0.0/0 10.29.132.1

vpc domain 50

role priority 2000

peer-keepalive destination 10.29.132.4 source 10.29.132.5

interface Vlan1

no shutdown

ip address 10.29.132.3/24

interface Vlan50

no shutdown

ip address 10.10.50.3/24

hsrp version 2

hsrp 50

preempt

priority 110

ip 10.10.50.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface Vlan51

no shutdown

ip address 10.10.51.3/24

hsrp version 2

hsrp 51

preempt

priority 110

ip 10.10.51.1

interface Vlan52

no shutdown

ip address 10.10.52.3/24

hsrp version 2

hsrp 52

preempt

priority 110

ip 10.10.52.1

interface Vlan53

no shutdown

ip address 10.10.53.3/24

hsrp version 2

hsrp 53

preempt

priority 110

ip 10.10.53.1

interface Vlan54

no shutdown

ip address 10.54.0.3/20

hsrp version 2

hsrp 54

preempt

priority 110

ip 10.54.0.1

ip dhcp relay address 10.10.51.21

ip dhcp relay address 10.10.51.22

interface port-channel10

description vPC-PeerLink

switchport mode trunk

switchport trunk allowed vlan 1,50-54

spanning-tree port type network

service-policy type qos input jumbo vpc peer-link

interface port-channel11 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 11

interface port-channel12 description FI-Uplink-K22 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk mtu 9216 service-policy type qos input jumbo vpc 12

interface Ethernet1/1

switchport mode trunk

switchport trunk allowed vlan 1,50-54

channel-group 10 mode active

switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/3

switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/4 switchport mode trunk switchport trunk allowed vlan 1,50-54 channel-group 10 mode active

interface Ethernet1/5 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 11 mode active

interface Ethernet1/6 switchport mode trunk switchport trunk allowed vlan 1,50-54 mtu 9216 channel-group 11 mode active

interface Ethernet1/7

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 12 mode active

interface Ethernet1/8

switchport mode trunk

switchport trunk allowed vlan 1,50-54

mtu 9216

channel-group 12 mode active

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

switchport mode trunk switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/26 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/27

switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

switchport mode trunk switchport trunk allowed vlan 1,50-54

spanning-tree port type edge trunk

interface Ethernet1/29 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/30 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/31 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/32 switchport mode trunk switchport trunk allowed vlan 1,50-54 spanning-tree port type edge trunk

interface Ethernet1/33

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

switchport access vlan 50

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0

vrf member management

ip address 10.29.132.5/24

clock timezone PST -8 0

clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60

line console

line vty

boot nxos bootflash:/nxos.7.0.3.12.2d.bin

Appendix B – Cisco HyperFlex HX220c-M4S 8-Node Cluster Horizon 7 Instant Clone In-Flight Performance Metrics

The following charts delineate performance parameters for the 8-node cluster during a Login VSI 4.1 1000 Horizon 7 Instant Clone benchmark test.

The CPU and memory charts show all 8 nodes' performance on a single chart. Individual charts for each node are included for network throughput for clarity.

The performance charts indicates that the HyperFlex hybrid nodes running Data Platform version 1.8(1b) were operating consistently from node to node and well within normal operating parameters for hardware in this class. The data also supports the even distribution of the workload across all 8 servers.

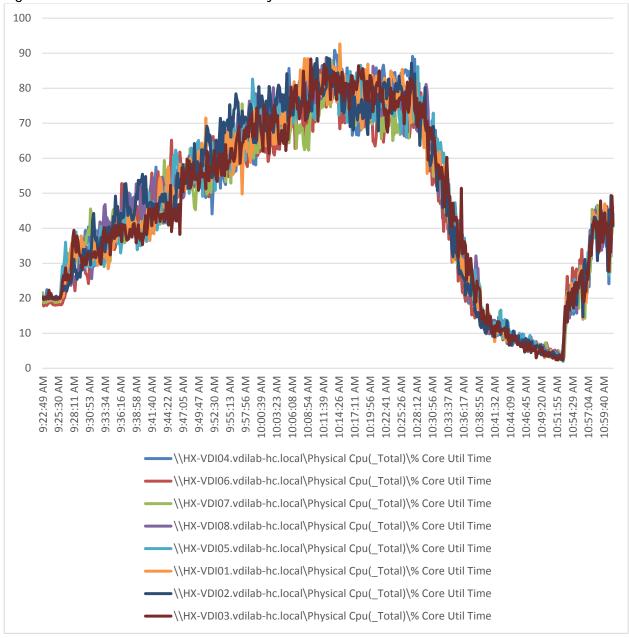


Figure 64 Percent CPU Core Utilization by Node

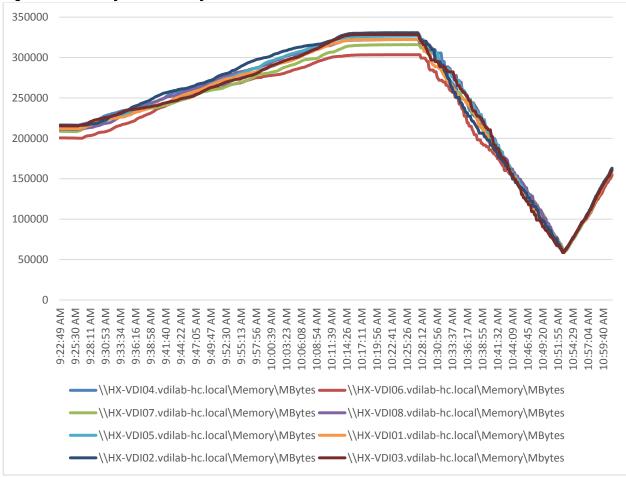
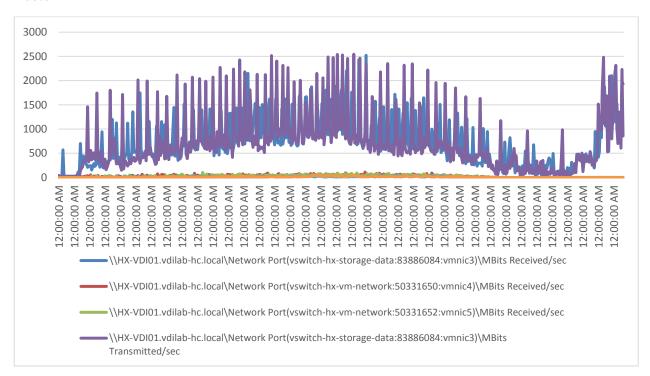
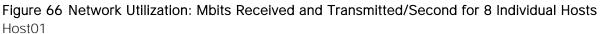


Figure 65 Memory Utilization by Node





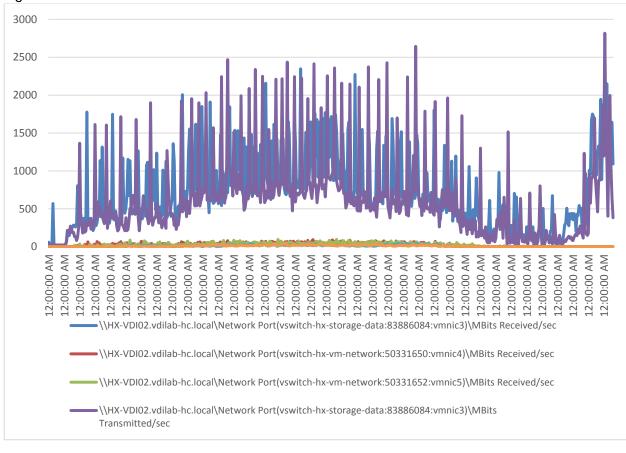


Figure 67 Host02

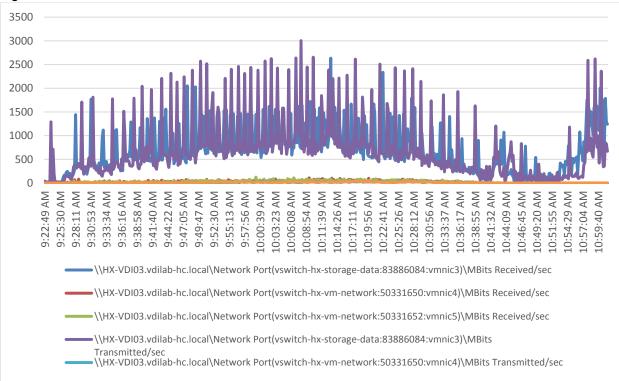


Figure 68 Host03

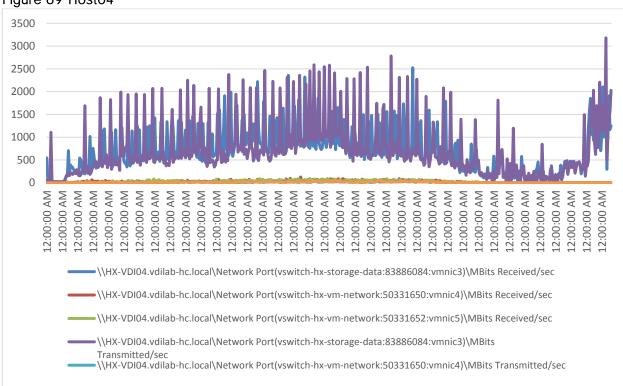


Figure 69 Host04

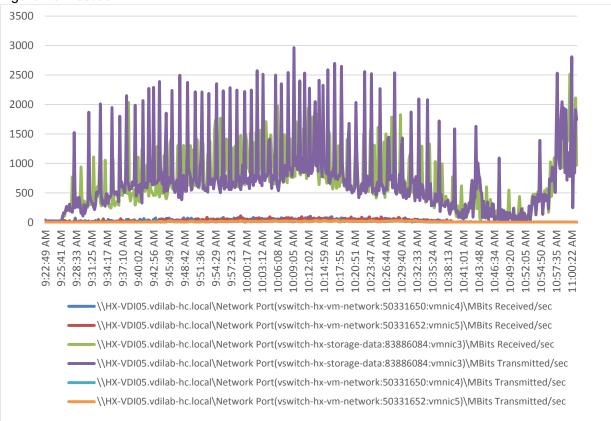


Figure 70 Host05

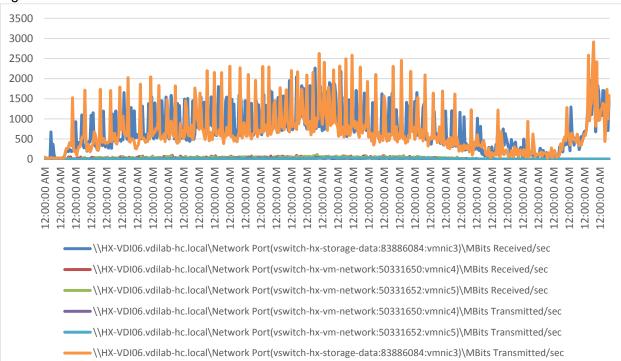
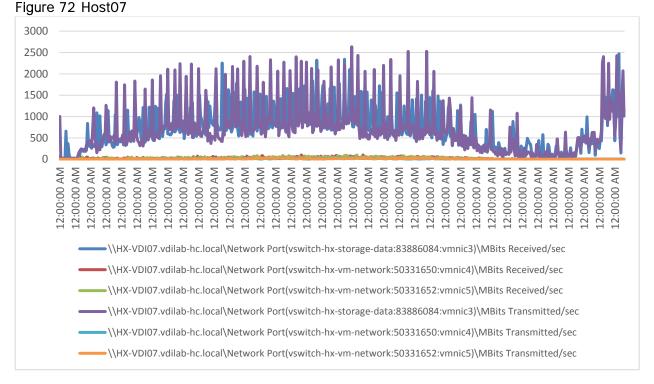


Figure 71 Host06



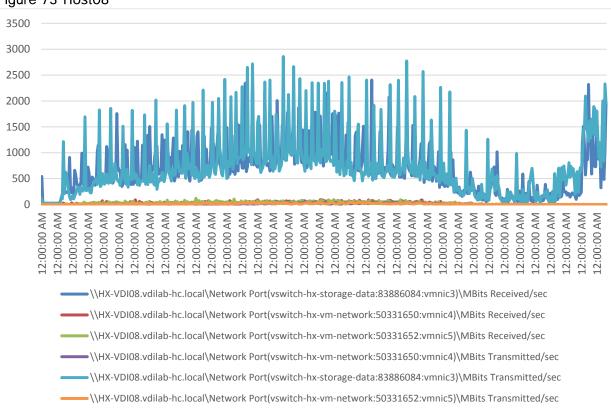


Figure 73 Host08