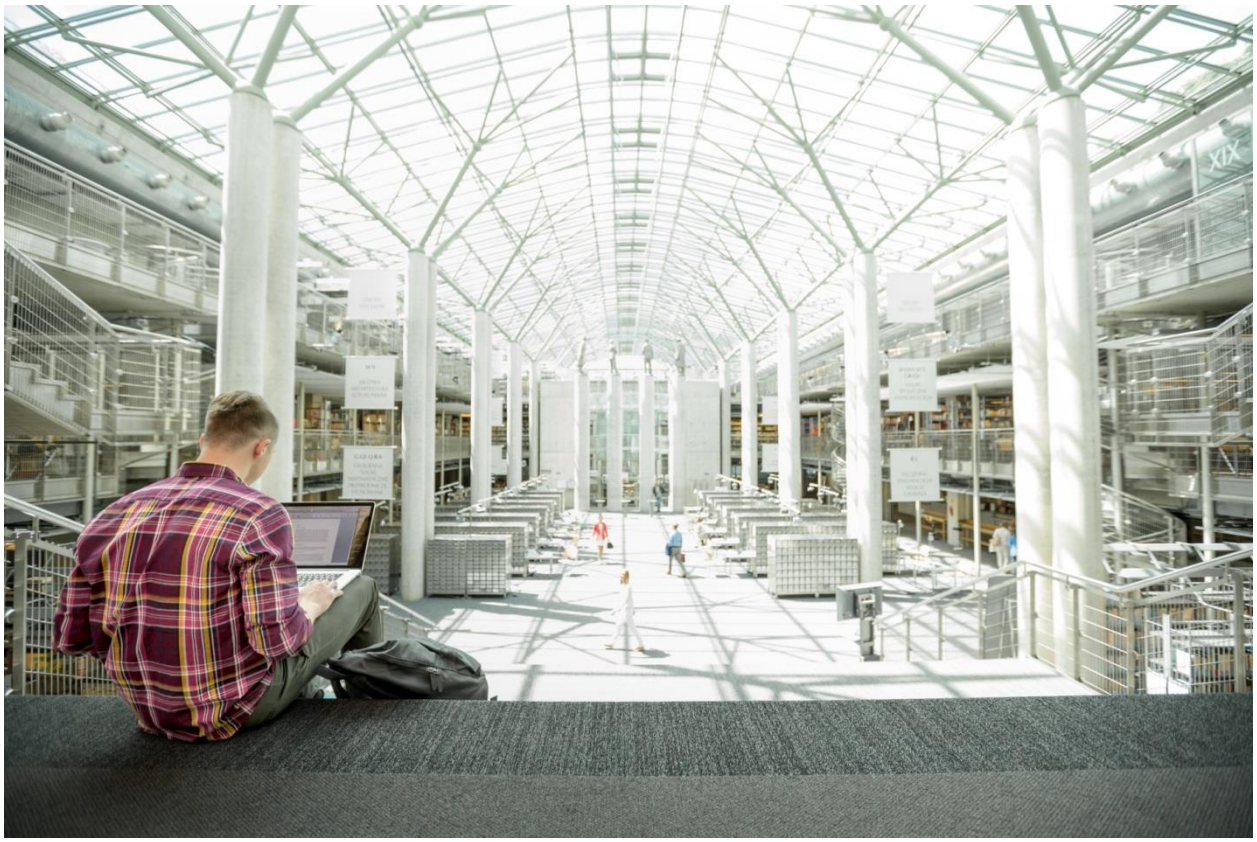


Cisco HyperFlex M5 All-Flash Hyperconverged System with up to 600 Citrix XenDesktop Users

Design and Deployment of Cisco HyperFlex for Virtual Desktop Infrastructure with Citrix XenDesktop 7.16

Last Updated: December 21, 2018

CISCO VALIDATED DESIGN

About the Cisco Validated Design Program

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

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

Table of Contents

Executive Summary 7
Solution Overview 8
Introduction 8
Audience 8
Purpose of this Document 8
What's New? 8
Solution Summary 10
Cisco Desktop Virtualization Solutions: Data Center 11
The Evolving Workplace 11
Cisco Desktop Virtualization Focus 12
Use Cases 14
Physical Topology 15
Fabric Interconnects 17
HX-Series Rack Mount Servers 18
Cisco UCS B-Series Blade Servers 18
Logical Network Design 19
Configuration Guidelines 21
Solution Design 22
Cisco Unified Computing System 22
Cisco Unified Computing System Components 22
Enhancements for Version 2.6.1 24
Cisco UCS Fabric Interconnect 25
Cisco HyperFlex HX-Series Nodes 26
Cisco HyperFlex Compute Nodes 32
Cisco UCS B200-M5 Blade 32
Cisco VIC1340 Converged Network Adapter 33
Cisco UCS 5108 Blade Chassis 34
Cisco UCS 2304XP Fabric Extender 34
Cisco UCS C220-M5 Rack Server 35
Cisco UCS C240-M5 Rack Server 36
Cisco HyperFlex Converged Data Platform Software 37
Cisco HyperFlex HX Data Platform Administration Plug-in 37
Cisco HyperFlex Connect HTML5 Management Web Page 38
Cisco Intersight Management Web Page 38
Cisco HyperFlex HX Data Platform Controller 40
Cisco Nexus 93108YCPX Switches 46
Architectural Flexibility 46
Feature-Rich 46
Real-Time Visibility and Telemetry 46

Highly Available and Efficient Design 46
Simplified Operations 47
Investment Protection 47
VMware vSphere 6.5 47
VMware vCenter Server 48
VMware ESXi 6.5 Hypervisor 48
Citrix XenApp™ and XenDesktop™ 7.16 48
Zones 50
Improved Database Flow and Configuration 50
Application Limits 50
Multiple Notifications before Machine Updates or Scheduled Restarts 50
API Support for Managing Session Roaming 51
API Support for Provisioning VMs from Hypervisor Templates 51
Support for New and Additional Platforms 51
Citrix Provisioning Services 7.16 52
Benefits for Citrix XenApp and Other Server Farm Administrators 52
Benefits for Desktop Administrators 53
Citrix Provisioning Services Solution 53
Citrix Provisioning Services Infrastructure 53
Architecture and Design of Citrix XenDesktop on Cisco Unified Computing System and Cisco HyperFlex Storage Design Fundamentals 55
Understanding Applications and Data 56
Project Planning and Solution Sizing Sample Questions 56
Citrix XenDesktop Design Fundamentals 57
Machine Catalogs 57
Delivery Groups 58
Citrix Provisioning Services 58
Example XenDesktop Deployments 61
Distributed Components Configuration 61
Multiple Site Configuration 62
Citrix Cloud Services 63
Designing a XenDesktop Environment for a Mixed Workload 63
Deployment Hardware and Software 65
Products Deployed 65
Hardware Deployed 67
Software Deployed 67
Logical Architecture 68
VLANs 69
Jumbo Frames 70
VMware Clusters 70
ESXi Host Design 71

Solution Configuration 77
Cisco UCS Compute Platform 77
Physical Infrastructure 77
Cisco Unified Computing System Configuration 80
Deploy and Configure HyperFlex Data Platform 80
Prerequisites 80
Deploy Cisco HyperFlex Data Platform Installer VM 86
Cisco HyperFlex Cluster Configuration 91
Build the Virtual Machines and Environment for Workload Testing 120
Software Infrastructure Configuration 120
Prepare the Master Images 121
Install and Configure XenDesktop and XenApp 122
Prerequisites 122
Install XenDesktop Delivery Controller, Citrix Licensing, and StoreFront 123
Install Citrix License Server 123
Install Citrix Licenses 127
Install the XenDesktop 128
Configure the XenDesktop Site 134
Configure the XenDesktop Site Administrators 140
Configure additional XenDesktop Controller 142
Add the Second Delivery Controller to the XenDesktop Site 146
Install and Configure StoreFront 147
Additional StoreFront Configuration 156
Install and Configure Citrix Provisioning Server 7.16 162
Prerequisites 162
Install Additional PVS Servers 180
Install XenDesktop Virtual Desktop Agents 190
Install the Citrix Provisioning Services Target Device Software 196
Create Citrix Provisioning Services vDisks 200
Provision Virtual Desktop Machines 209
Non-Persistent PVS streamed desktops 209
Non-persistent Random HVD Provisioned using MCS 223
Persistent Static Provisioned with MCS 231
Create Delivery Groups 239
Citrix XenDesktop Policies and Profile Management 243
Configure Citrix XenDesktop Policies 243
Configuring User Profile Management 244
Test Setup and Configurations 246
Testing Methodology and Success Criteria 247
Testing Procedure 247
Pre-Test Setup for Testing 247

Test Run Protocol 248
Success Criteria 249
Test Results 254
Boot Storms 254
Recommended Maximum Workload and Configuration Guidelines 255
Four Node Cisco HXAF220c-M5S Rack Server, HyperFlex All-Flash Cluster 255
Summary 273
About the Authors 274
Acknowledgements 274
Appendix A – Cisco Nexus 93108YC Switch Configuration 275
Switch A Configuration 275
Switch B Configuration 285

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 450 user mixed workload on a 4-node (4 Cisco HyperFlex HXAF220C-M5SX server) Cisco HyperFlex system. We provide deployment guidance and performance data for Citrix XenDesktop 7.16 virtual desktops running Microsoft Windows 10 with Office 2016 Machine Creation and Provisioning Services and Persistent virtual desktops as well as Windows Server 2016 RDS server-based sessions on VMware vSphere 6.5. 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 2.6.1a.

The solution payload is 100 percent virtualized on Cisco HyperFlex HXAF220C-M5SX hyperconverged nodes booting via on-board M.2 SATA SSD drive running VMware vSphere 6.5 U1 hypervisor and the Cisco HyperFlex Data Platform storage controller VM. The virtual desktops are configured with XenDesktop 7.16, which incorporates both traditional persistent and non-persistent virtual Windows 7/8/10 desktops, hosted applications and remote desktop service (RDS) Microsoft Server 2008 R2, Server 2012 R2 or Server 2016 based desktops. The solution provides unparalleled scale and management simplicity. Citrix XenDesktop Provisioning Services or Machine Creation Services Windows 10 desktops (450,) or full clone desktops (450) or XenApp server based desktops (600) can be provisioned on a four node Cisco HyperFlex cluster. Where applicable, this document provides best practice recommendations and sizing guidelines for customer deployment of this solution.

The solution boots 450 virtual desktops or 36 XENAPP virtual server machines in five minutes or less, making sure that users will not experience delays in accessing their virtual workspace on HyperFlex.

Our past Cisco Validated Design studies with HyperFlex show linear scalability out to the cluster size limits of 16 HyperFlex hyperconverged nodes plus 16 Cisco UCS B200 M5, Cisco UCS C220 M5, or Cisco UCS C240 M5 compute only nodes. You can expect that our new HyperFlex all flash system running HX Data Platform 2.6 on Cisco HXAF220 M5 or Cisco HXAF240 M5 nodes will scale up to 4800 knowledge worker users per cluster with N+1 server fault tolerance.

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

The solution provides outstanding virtual desktop end user experience as measured by the Login VSI 4.1.25 Knowledge Worker workload running in benchmark mode. Index average end-user response times for all tested delivery methods is under 1 second, representing the best performance in the industry.

Solution Overview

Introduction

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

Audience

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

Purpose of this Document

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

What's New?

This is the first Cisco Validated Design with Cisco HyperFlex All-Flash system running Virtual Desktop Infrastructure on Intel Xeon Scalable Family processor-based, fifth generation Cisco UCS HyperFlex system. It incorporates the following features:

- Validation of Cisco Nexus 9000 with Cisco HyperFlex Support for the Cisco UCS 3.2(2) release and Cisco HyperFlex Data Platform v 2.6.1a.
- VMware vSphere 6.5 U1 Hypervisor
- Citrix XenDesktop 7.16 Pooled desktops with Provisioning Services. Persistent desktops with Citrix Machine Creation Services and RDS sessions with Citrix XenApp Shared desktop.

Cisco HX Data Platform requires specific software and hardware versions, and networking settings for successful installation. See the Cisco HyperFlex Systems Getting Started Guide for a complete list of requirements.

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

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

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

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

The combination of technologies from Cisco Systems, Inc. and 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 nodes, dual 18-core 2.3 GHz Intel Xeon (Gold 6140) Scalable Family processors with 768GB of 2666Mhz memory with Citrix XenDesktop support more virtual desktop workloads than the previously released generation processors on the same hardware. The Intel Xeon Gold 6140 18-core scalable family processors used in this study provided a balance between increased per-server capacity and cost.

- **Fault-tolerance with high availability built into the design.** The various designs are based on multiple Cisco HX-Series nodes, Cisco UCS rack servers and Cisco UCS blade servers for virtual desktop and infrastructure workloads. The design provides N+1 server fault tolerance for every payload type tested.

- **Stress-tested to the limits during aggressive boot scenario.** The 450 user mixed hosted virtual desktop and 600 user hosted shared desktop environment booted and registered with the XenDesktop Studio in under 5 minutes, providing our customers with an extremely fast, reliable cold-start desktop virtualization system.

- **Stress-tested to the limits during simulated login storms.** All 450 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 450 user system is 8 rack units, including Cisco Nexus Switching and Cisco Fabric interconnects. Incremental Citrix XenDesktop users can be added to the Cisco HyperFlex cluster up to the cluster scale limits, currently 16 hyper converged and 16 compute only nodes, by adding one or more nodes.

- **100 percent virtualized:** This CVD presents a validated design that is 100 percent virtualized on VMware ESXi 6.5. All of the virtual desktops, user data, profiles, and supporting infrastructure components, including Active Directory, SQL Servers, Citrix XenDesktop components, XenDesktop VDI desktops and XENAPP servers were hosted as virtual machines. This provides customers with complete flexibility for maintenance and capacity additions because the entire system runs on the Cisco HyperFlex hyper-converged infrastructure with stateless Cisco UCS HX-series servers. (Infrastructure VMs were hosted on two Cisco UCS C220 M4 Rack Servers outside of the HX cluster to deliver the highest capacity and best economics for the solution.)

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

Cisco Desktop Virtualization Solutions: Data Center

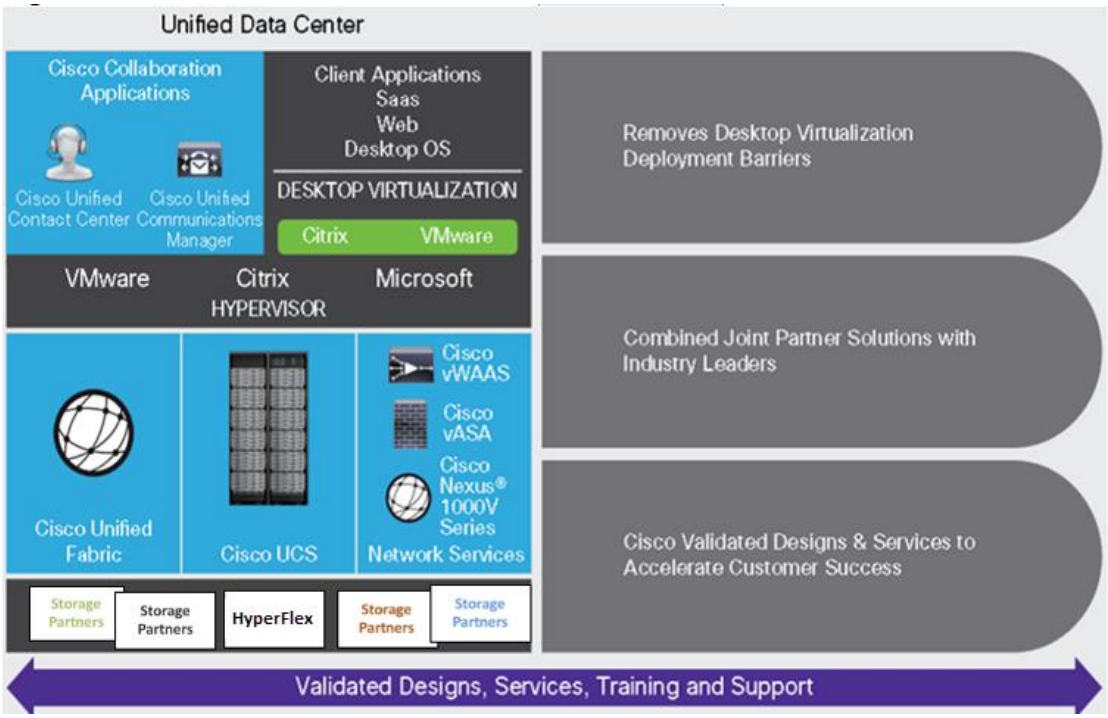
The Evolving Workplace

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

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

Cisco Desktop Virtualization Focus

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

Simplified

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

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

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

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

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

Savings and Success

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

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

The key measure of desktop virtualization for any organization is its efficiency and effectiveness in both the near term and the long term. The Cisco Desktop Virtualization Solutions are very efficient, allowing rapid deployment, requiring fewer devices and cables, and reducing costs. The solutions are also extremely effective, providing the services that end users need on their devices of choice while improving IT operations, control, and data security. Success is bolstered through Cisco's best-in-class partnerships with leaders in virtualization and through tested

and validated designs and services to help customers throughout the solution lifecycle. Long-term success is enabled through the use of Cisco's scalable, flexible, and secure architecture as the platform for desktop virtualization.

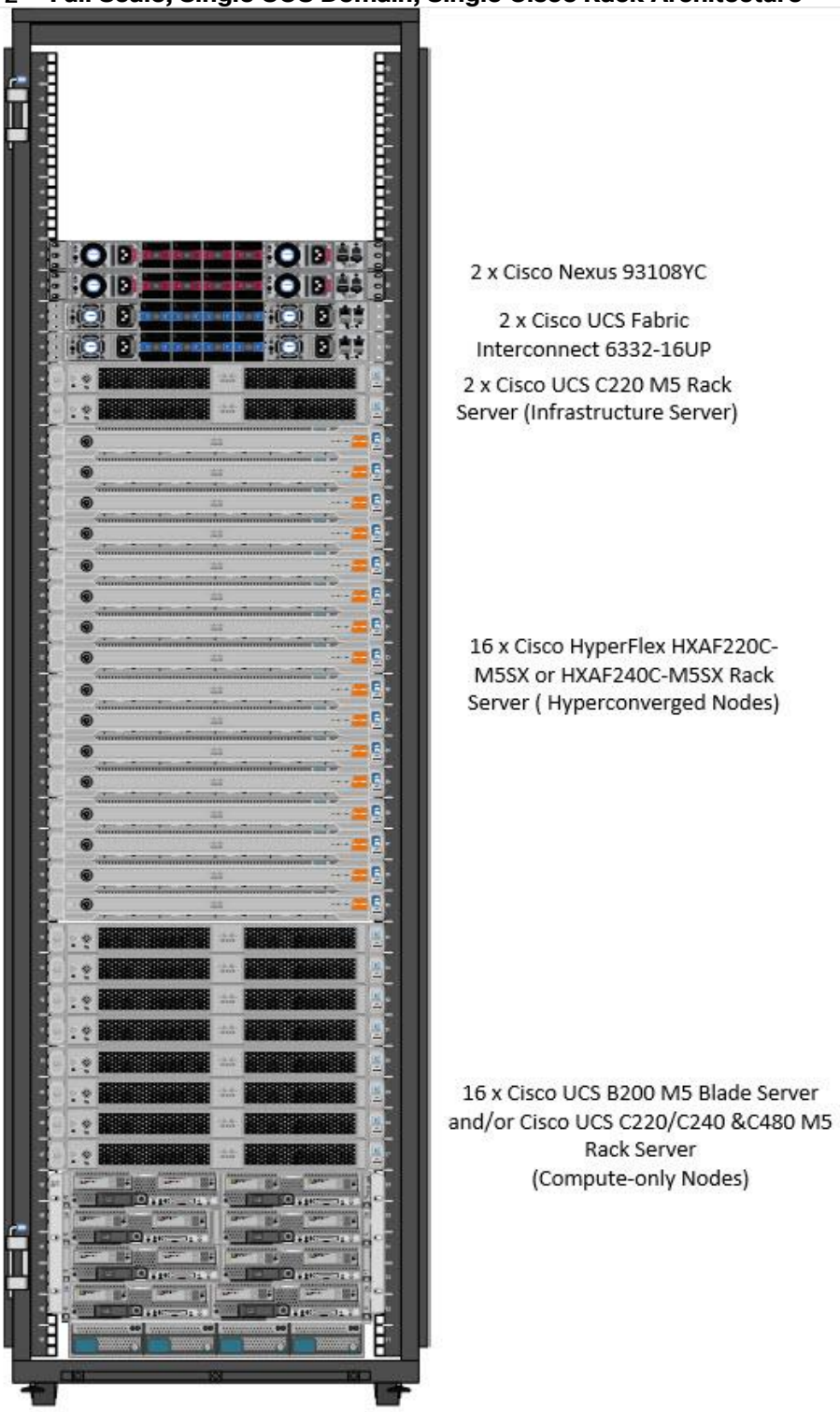
The ultimate measure of desktop virtualization for any end user is a great experience. Cisco HyperFlex delivers class-leading performance with sub-second base line response times and index average response times at full load of just under one second.

Use Cases

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

Figure 2 shows the Citrix XenDesktop on vSphere 6.5 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 **Full Scale, Single UCS Domain, Single Cisco Rack Architecture**



Physical Topology

The Cisco HyperFlex system is composed of a pair of Cisco UCS 6200/6300 series Fabric Interconnects, along with up to 16 HXAF-Series rack mount servers per cluster. In addition, up to 16 compute only servers can be added per cluster. Adding Cisco UCS 5108 Blade chassis allows use of Cisco UCS B200-M5 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 6332-16UP Fabric Interconnects to Cisco Nexus 93108YCPX switches.

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

Figure 3 **Cisco HyperFlex Standard Topology**

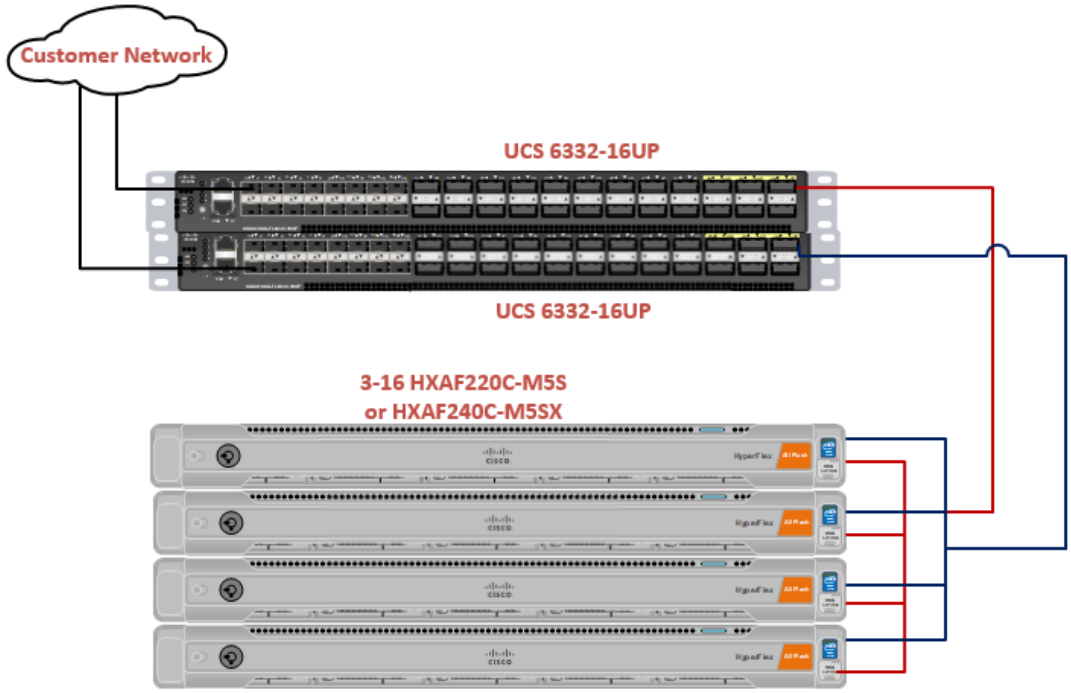
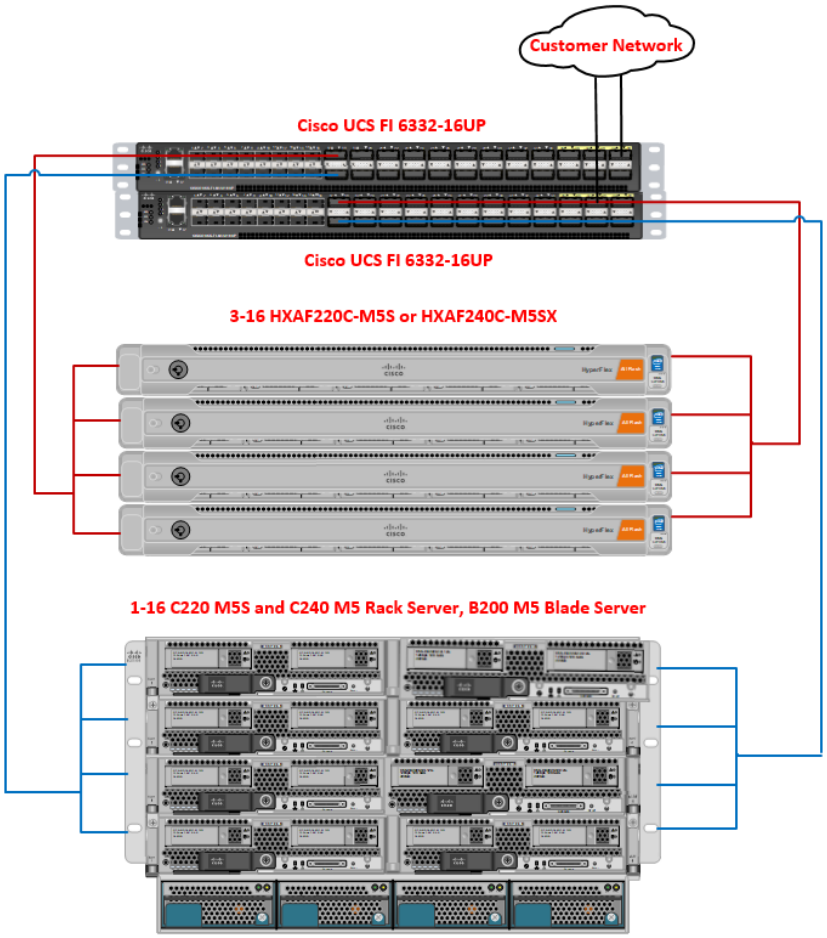


Figure 4 **Cisco HyperFlex Hyperconverged plus Compute Only Node Topology**



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.

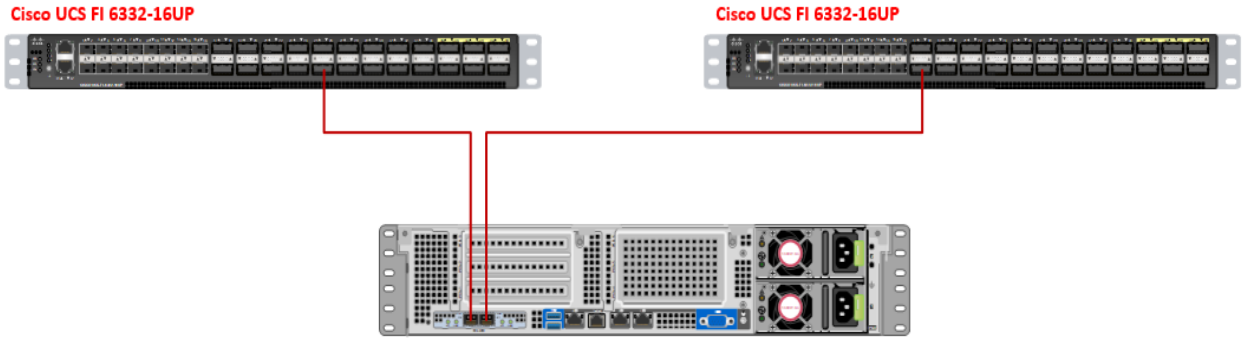
- **Console:** An RJ45 serial port for direct console access to the Fabric Interconnect. Typically used during the initial FI setup process with the included serial to RJ45 adapter cable. This can also be plugged into a terminal aggregator or remote console server device.

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 HXAF220C-M5SX and HXAF240C-M5SX servers are configured with the Cisco VIC 1387 network interface card (NIC) installed in a modular LAN on motherboard (MLOM) slot, which has dual 40 Gigabit Ethernet (GbE) ports. The standard and redundant connection practice is to connect port 1 of the VIC 1387 to a port on FI A, and port 2 of the VIC 1387 to a port on FI B (Figure 5).

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

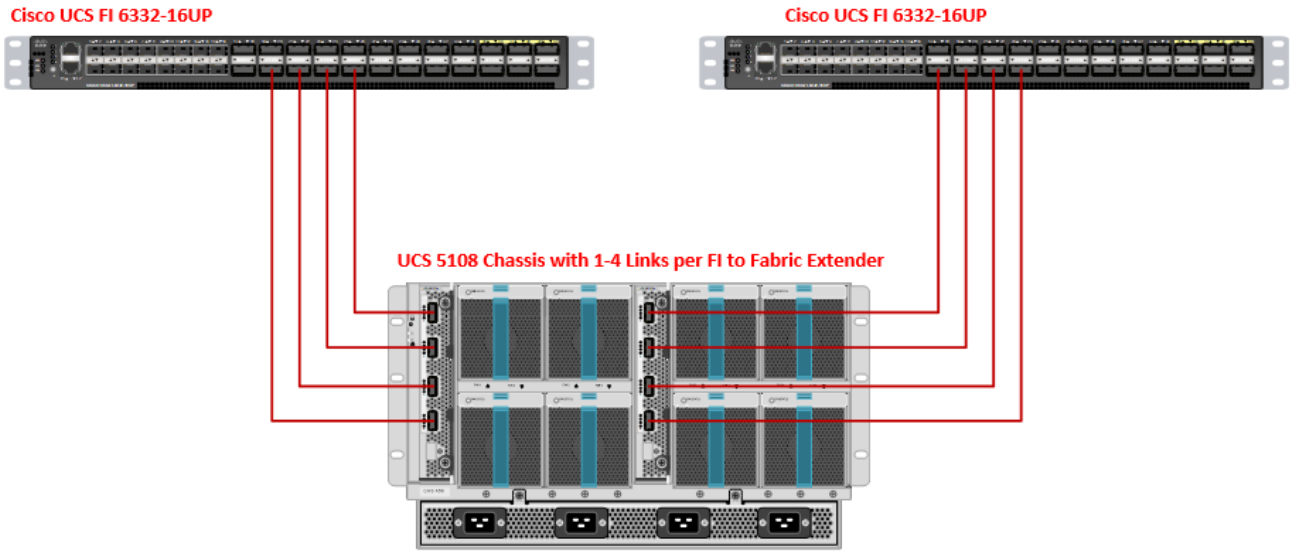
Figure 5 **HX-Series Server Connectivity**



Cisco UCS B-Series Blade Servers

Hybrid HyperFlex clusters also incorporate 1-8 Cisco UCS B200 M5 blade servers for additional compute capacity. Like all other Cisco UCS B-series blade servers, the Cisco UCS B200 M5 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 or 2 x 40 (native) 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.

Figure 6 **Cisco UCS 5108 Chassis Connectivity**



Logical Network Design

The Cisco HyperFlex system has communication pathways that fall into four defined zones (Figure 6):

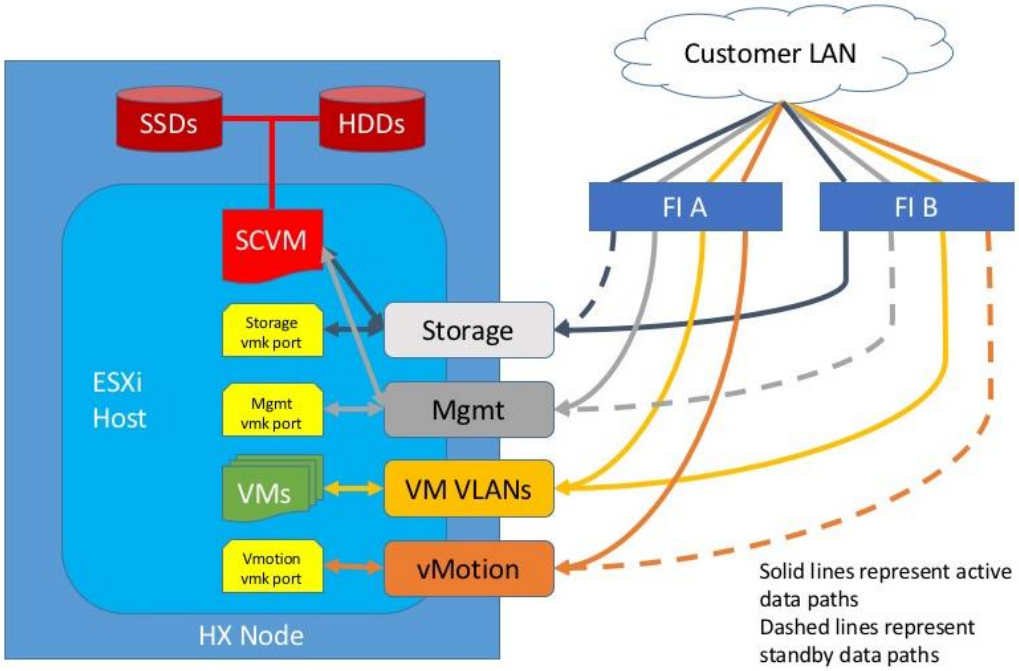
- **Management Zone:** This zone comprises the connections needed to manage the physical hardware, the hypervisor hosts, and the storage platform controller virtual machines (SCVM). These interfaces and IP addresses need to be available to all staff who will administer the HX system, throughout the LAN/WAN. 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 802.1Q VLAN IDs. These interfaces and IP addresses need to be available to all staff and other computer endpoints which need to communicate with the guest VMs in the HX system, throughout the LAN/WAN.
- **Storage Zone:** This zone comprises the connections used by the Cisco HX Data Platform software, ESXi hosts, and the storage controller VMs to service the HX Distributed Data Filesystem. These interfaces and IP addresses need to be able to communicate with each other at all times for proper operation. During normal operation, this traffic all occurs within the Cisco UCS domain, however there are hardware failure scenarios where this traffic would need to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa. This zone is primarily jumbo frame traffic therefore jumbo frames must be enabled on the Cisco UCS uplinks. In this zone are multiple components:
  - A vmkernel interface used for storage traffic 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.

Figure 7 illustrates the logical network design.

Figure 7 **Logical Network Design**



The reference hardware configuration includes:

- Two Cisco Nexus 93108YCPX switches
- Two Cisco UCS 6332-16UP fabric interconnects
- Four Cisco HX-series Rack server running HyperFlex data platform version 2.6.1a .

For desktop virtualization, the deployment includes Citrix XenDesktop running on VMware vSphere 6.5. The design is intended to provide a large scale building block for both XENAPP and persistent/non-persistent desktops with following density per Four node configuration:

- 600 Citrix XenApp server desktop sessions
- 450 Citrix XenDesktop Windows 10 non-persistent virtual desktops using PVS
- 450 Citrix XenDesktop Windows 10 non-persistent virtual desktops using MCS
- 450 Citrix XenDesktop Windows 10 persistent virtual desktops using MCS

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

Data provided here will allow customers to run XENAPP 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 12. 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-XENAPP-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 (UCSM) 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 40 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. It is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain.

Cisco Unified Computing System Components

The main components of Cisco UCS are:

- **Compute:** The system is based on an entirely new class of computing system that incorporates blade, rack and hyperconverged servers based on Intel® Xeon® scalable family processors.
- **Network:** The system is integrated on a low-latency, lossless, 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing (HPC) networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables needed, and by decreasing the power and cooling requirements.
- **Virtualization:** The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage**: The Cisco HyperFlex rack servers provide high performance, resilient storage using the powerful HX Data Platform software. Customers can deploy as few as three nodes (replication factor 2/3,) depending on their fault tolerance requirements. These nodes form a HyperFlex storage and compute cluster. The onboard storage of each node is aggregated at the cluster level and automatically shared with all of the nodes. 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. Our latest advancement offers a cloud-based management system called Cisco Intersight.

Figure 8 **Cisco HyperFlex Family Overview**

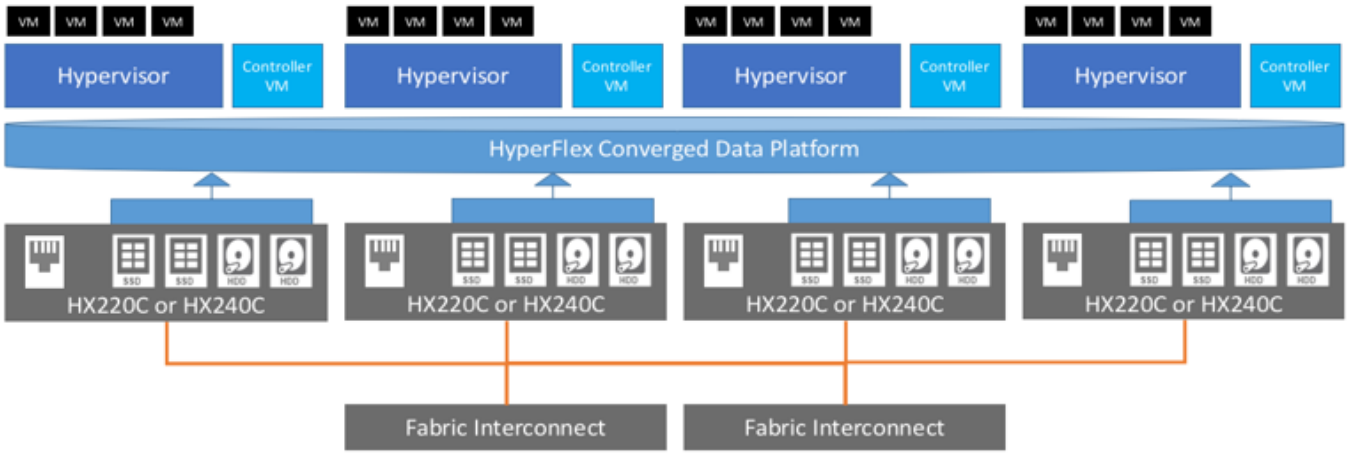
Cisco UCS and Cisco HyperFlex are designed to deliver:

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

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

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

Figure 9 **Cisco HyperFlex System Overview**



Enhancements for Version 2.6.1

The Cisco HyperFlex system has several new capabilities and enhancements in version 2.6.1:

- New All-Flash and Hybrid HX M5 server models are added to the Cisco HyperFlex product family
- Cisco HyperFlex now support the latest generation of Cisco UCS software, Cisco UCS Manager 3.2(2b) and beyond. For new All-Flash deployments on M5 servers, verify that Cisco UCS Manager 3.2(2b) or later is installed.
- Cisco Smart Licensing—Support for Cisco Smart Software Manager satellite. Please refer to the Cisco HyperFlex Getting Started Guide, Release 2.6, for more details.
- M5 Servers
- Key release highlights:
  - Same software feature set as HX 2.5
  - Support for M5 servers in HyperFlex
  - Enablement for Cisco HX240c M5 and HXAF240c M5 servers
  - Dual CPU—Intel Xeon processor scalable family
  - Up to 3TB DRAM—Recommended minimum of 256 GB DRAM
  - M.2 Drive—For ESX Boot and for Storage Controller VM
  - Up to 2 GPUs—M10, P40, AMD 7150 x 2
  - Dedicated rear slots for caching
- Enablement for Cisco HX220c M5 and HXAF220c M5 servers:
  - Dual CPU (Except Edge)—Intel Xeon processor scalable family
  - Up to 3TB DRAM—Recommended minimum of 256 GB DRAM
  - 8 x Data Drives (SATA/SAS)

  - M.2 Drive—For ESX Boot and for Storage Controller VM

- M4/M5 support in the same cluster:
  - A mixed cluster is defined by having both M4 and M5 HX converged nodes within the same storage cluster
  - HyperFlex Edge does not support mixed clusters
  - SED SKUs do not support mixed clusters
- Peripherals
  - Option for 6-8 drives in HX220C-M5S and HXAF220C-M5S nodes
  - Up to two GPUs for HX240C-M5SX and HXAF240C-M5SX nodes

Cisco UCS Fabric Interconnect

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

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

For networking, the Cisco UCS 6300 Series uses a cut-through architecture, supporting deterministic, low-latency, line-rate 40 Gigabit Ethernet on all ports, 2.56 terabit (Tb) switching capacity, and 320 Gbps of bandwidth per chassis, independent of packet size and enabled services. The product series supports Cisco low-latency, lossless, 40 Gigabit Ethernet unified network fabric capabilities, increasing the reliability, efficiency, and scalability of Ethernet networks. The fabric interconnects support multiple traffic classes over a lossless Ethernet fabric, from the blade server through the interconnect. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

Figure 10 **Cisco UCS 6332 Fabric Interconnect**

Figure 11 **Cisco UCS 6332-16UP Fabric Interconnect**

Cisco HyperFlex HX-Series Nodes

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

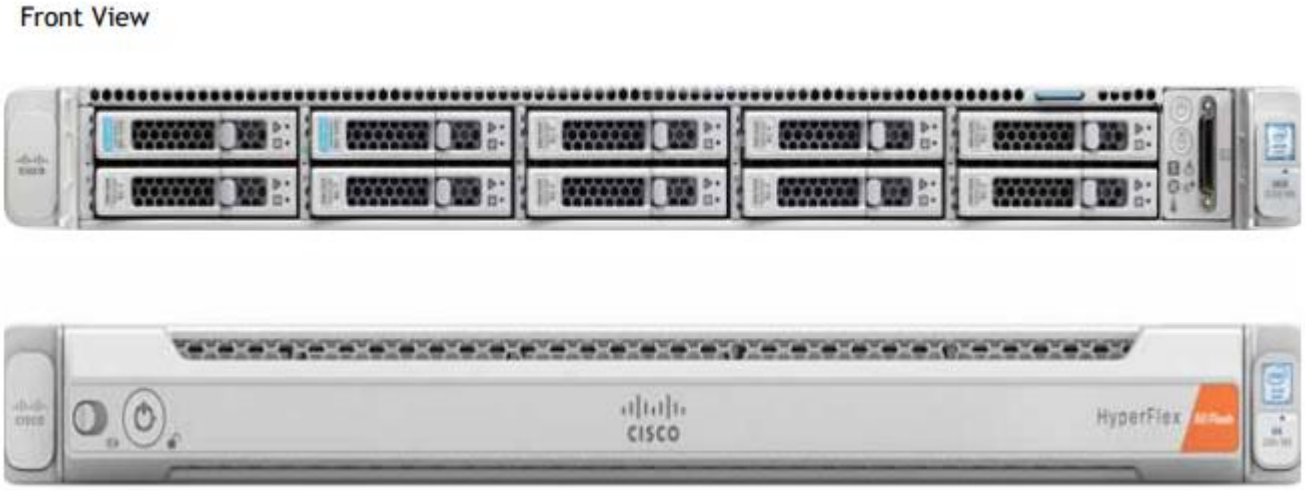
A Cisco HyperFlex cluster requires a minimum of three HX-Series nodes (with disk storage). Data is replicated across at least two of these nodes, and a third node is required for continuous operation in the event of a single-node failure. Each node that has disk storage is equipped with at least one high-performance SSD drive for data caching and rapid acknowledgment of write requests. Each node is also equipped with the platform's physical capacity of either spinning disks or enterprise-value SSDs for maximum data capacity.

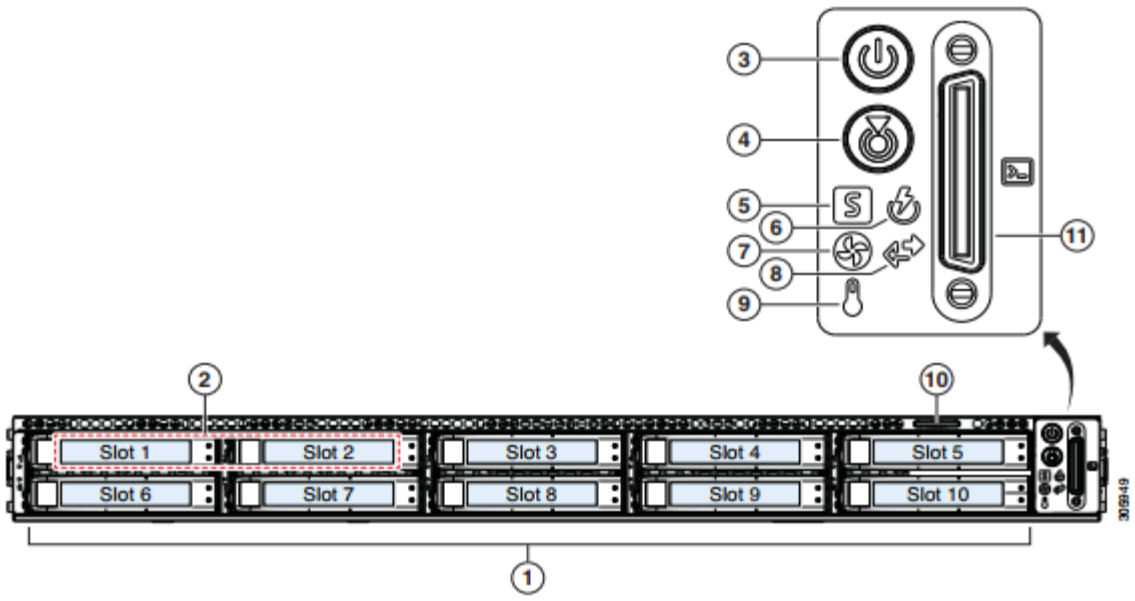
Cisco UCS HXAF220c-M5S Rack Server

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

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

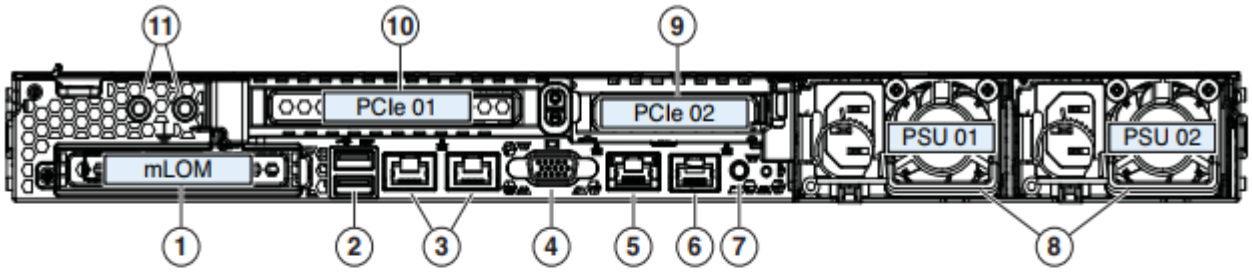
Figure 12 **Cisco UCS HXAF220c-M5SX Rack Server Front View**





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

Figure 13 **Cisco UCS HXAF220c-M5SX Rack Server Rear View**



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

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

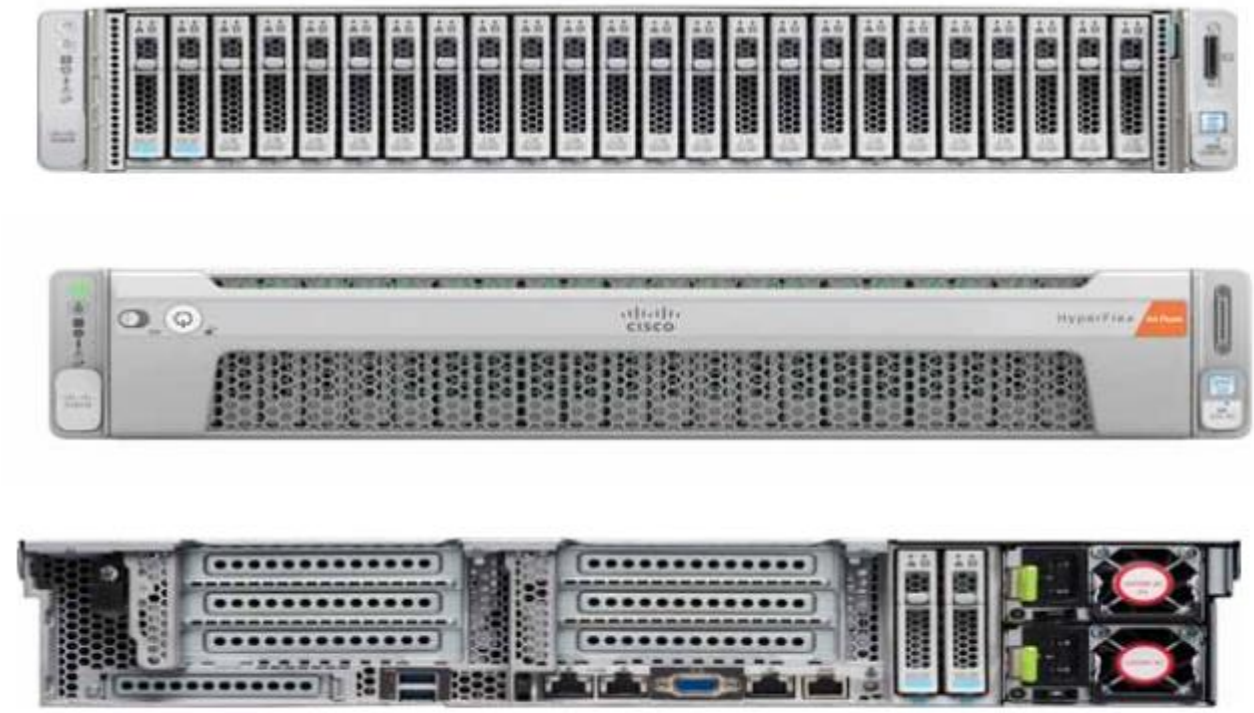
The Cisco UCS HXAF220c-M5S provides:

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

Cisco HyperFlex HXAF240c-M5SX Nodes

This capacity optimized configuration contains a minimum of three nodes, up to twenty three SED SATA or SAS SSD drives that contribute to cluster storage, a single 240 GB SATA SSD housekeeping drive, a single 400GB SAS SSD caching drive, and M.2 SATA SSD drive that acts as the boot drives. For detailed information, see the Cisco HyperFlex HXAF240c M5 Node Spec Sheet.

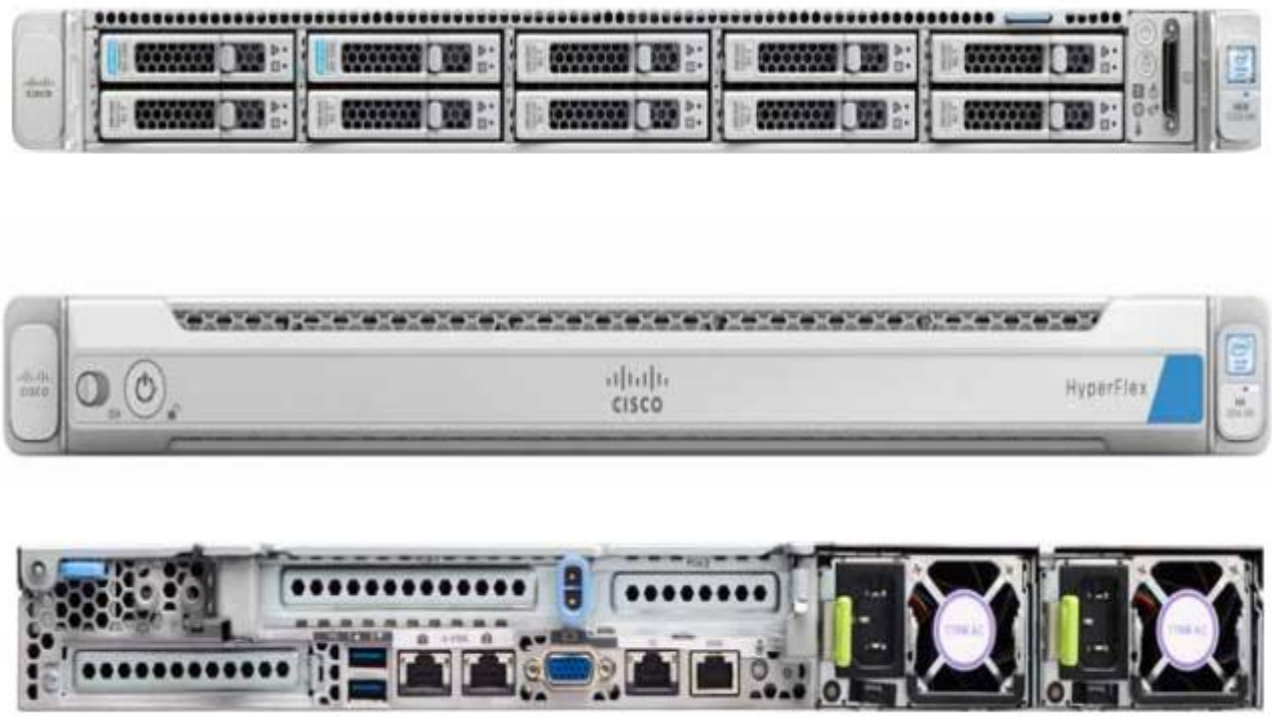
Figure 14 **HXAF240c-M4SX Node**



Cisco HyperFlex HX220c-M4S Hybrid Node

This small footprint configuration contains a minimum of three nodes with six 1.2 terabyte (TB) SAS drives that contribute to cluster storage capacity, a 240 GB SSD housekeeping drive, a 480 GB SSD caching drive, and 240Gb SATA M.2 SSD hat act as boot drives. For detailed information, see the Cisco HyperFlex HX220c M5 Node Spec Sheet.

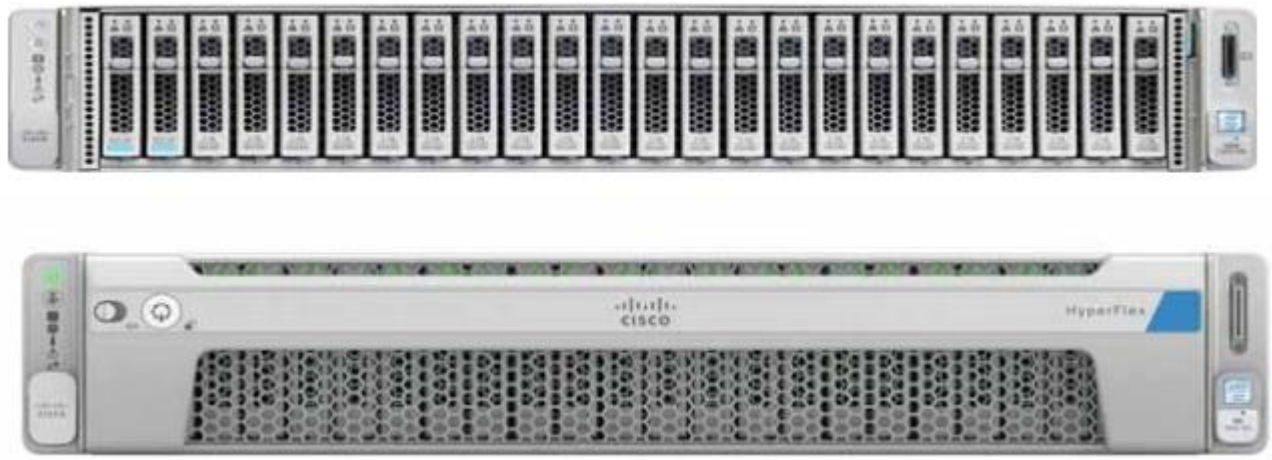
Figure 15 **HX220c-M4S Node**



Cisco HyperFlex HX240c-M4SX Hybrid Node

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 240 GB SSD housekeeping drive, a single 1.6 TB SSD caching drive, and 240Gb SATA M.2 SSD that act as the boot drives. For detailed information, see the Cisco HyperFlex HX240c M5 Node Spec Sheet.

Figure 16 **HX240c-M5SX Node**



Cisco VIC 1387 MLOM Interface Card

The Cisco UCS Virtual Interface Card (VIC) 1387 is a dual-port Enhanced Small Form-Factor Pluggable (QSFP+) 40-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)) in a modular LAN-on-motherboard (mLOM) adapter installed in the Cisco UCS HX-Series Rack Servers (**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 17 **Cisco VIC 1387 mLOM Card**

Cisco HyperFlex Compute Nodes

Cisco UCS B200-M5 Blade

For workloads that require additional computing and memory resources, but not additional storage capacity, a compute-intensive hybrid cluster configuration is allowed. This configuration requires a minimum of three (up to sixteen) HyperFlex converged nodes with one to sixteen Cisco UCS B200-M5 Blade Servers for additional computing capacity. The HX-series Nodes are configured as described previously, and the Cisco UCS B200-M5 servers are equipped with boot drives. Use of the Cisco UCS B200-M5 compute nodes also requires the Cisco UCS 5108 blade server chassis, and a pair of Cisco UCS 2300/2200 series Fabric Extenders. For detailed information, see the Cisco UCS B200 M5 Blade Server Spec Sheet.

Figure 18 **Cisco UCS B200 M5 Server**

Cisco VIC1340 Converged Network Adapter

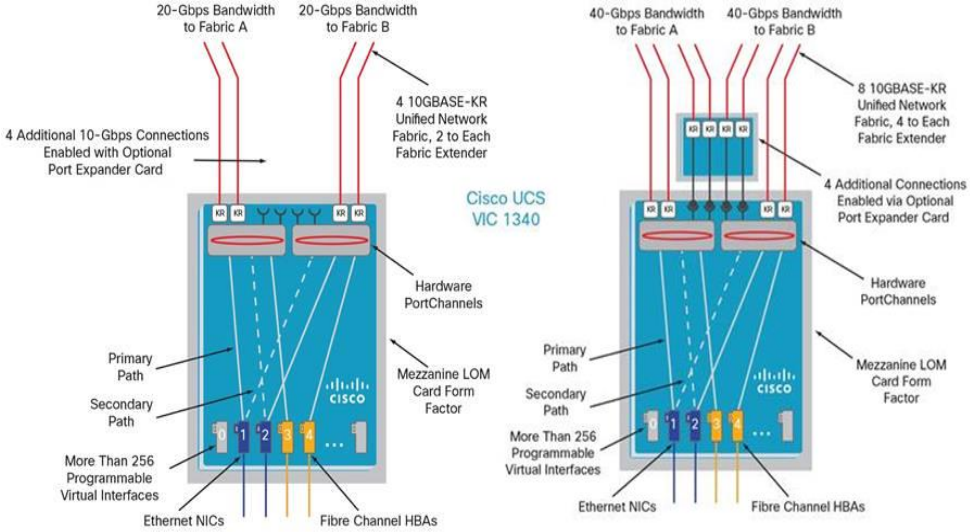
The Cisco UCS Virtual Interface Card (VIC) 1340 (Figure 19) is a 2-port 40-Gbps Ethernet or dual 4 x 10-Gbps Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed exclusively for the M4 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional port expander, the Cisco UCS VIC 1340 capabilities is enabled for two ports of 40-Gbps Ethernet.

The Cisco UCS VIC 1340 enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1340 supports Cisco® Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment and management.

Figure 19 **Cisco UCS VIC 1340**

Figure 20 illustrates the Cisco UCS VIC 1340 Virtual Interface Cards Deployed in the Cisco UCS B-Series B200 M4 Blade Servers.

Figure 20 **Cisco UCS VIC 1340 Deployed in the Cisco UCS B200 M4**



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 21 **Cisco UCS 5108 Blade Chassis Front and Rear Views**

Cisco UCS 2304XP Fabric Extender

Cisco UCS 2304 Fabric Extender brings the unified fabric into the blade server enclosure, providing multiple 40 Gigabit Ethernet connections between blade servers and the fabric interconnect, simplifying diagnostics, cabling, and management. It is a third-generation I/O Module (IOM) that shares the same form factor as the second-generation Cisco UCS 2200 Series Fabric Extenders and is backward compatible with the shipping Cisco UCS 5108 Blade Server Chassis.

The Cisco UCS 2304 connects the I/O fabric between the Cisco UCS 6300 Series Fabric Interconnects and the Cisco UCS 5100 Series Blade Server Chassis, enabling a lossless and deterministic Fibre Channel over Ethernet (FCoE) fabric to connect all blades and chassis together. Because the fabric extender is similar to a distributed line

card, it does not perform any switching and is managed as an extension of the fabric interconnects. This approach removes switching from the chassis, reducing overall infrastructure complexity and enabling Cisco UCS to scale to many chassis without multiplying the number of switches needed, reducing TCO and allowing all chassis to be managed as a single, highly available management domain.

The Cisco UCS 2304 also manages the chassis environment (power supply, fans, and blades) in conjunction with the fabric interconnect. Therefore, separate chassis management modules are not required.

Cisco UCS 2304 Fabric Extenders fit into the back of the Cisco UCS 5100 Series chassis. Each Cisco UCS 5100 Series chassis can support up to two fabric extenders, allowing increased capacity and redundancy (Figure 22).

The Cisco UCS 2304 Fabric Extender has four 40 Gigabit Ethernet, FCoE-capable, Quad Small Form-Factor Pluggable (QSFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2304 can provide one 40 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis, giving it a total eight 40G interfaces to the compute. Typically configured in pairs for redundancy, two fabric extenders provide up to 320 Gbps of I/O to the chassis.

Figure 22 **Cisco UCS 2304XP Fabric Extender**

Cisco UCS C220-M5 Rack Server

The Cisco UCS C220 M5 Rack Server is an enterprise-class infrastructure server in an 1RU form factor. It incorporates the Intel Xeon scalable family processor product family, next-generation DDR4 memory, and 12-Gbps SAS throughput, delivering significant performance and efficiency gains. Cisco UCS C220 M5 Rack Server can be used to build a compute-intensive hybrid HX cluster, for an environment where the workloads require additional computing and memory resources but not additional storage capacity, along with the HX-series converged nodes. This configuration contains a minimum of three (up to sixteen) HX-series converged nodes with one to sixteen Cisco UCS C220-M4 Rack Servers for additional computing capacity.

Figure 23 **Cisco UCS C220 M5 Rack Server**

Cisco UCS C240-M5 Rack Server

The Cisco UCS C240 M5 Rack Server is an enterprise-class 2-socket, 2-rack-unit (2RU) rack server. It incorporates the Intel Xeon scalable family processor product family, next-generation DDR4 memory, and 12-Gbps SAS throughput that offers outstanding performance and expandability for a wide range of storage and I/O-intensive infrastructure workloads. Cisco UCS C240 M5 Rack Server can be used to expand additional computing and memory resources into a compute-intensive hybrid HX cluster, along with the HX-series converged nodes. This configuration contains a minimum of three (up to sixteen) HX-series converged nodes with one to sixteen Cisco UCS C240-M4 Rack Servers for additional computing capacity.

Figure 24 **Cisco UCS C240 M5 Rack Server**

Cisco HyperFlex Converged Data Platform Software

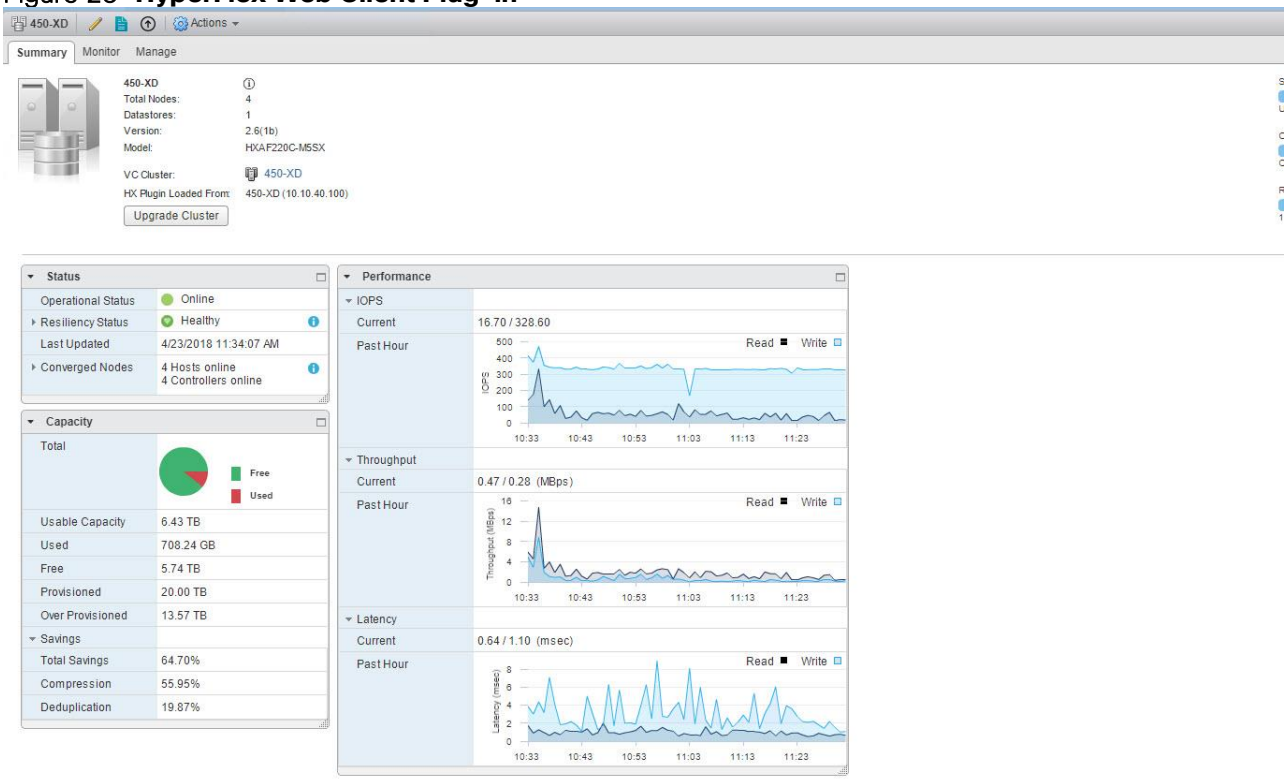
The Cisco HyperFlex HX Data Platform is a purpose-built, high-performance, distributed file system with a wide array of enterprise-class data management services. The data platform's innovations redefine distributed storage technology, exceeding the boundaries of first-generation hyperconverged infrastructures. 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 25 **HyperFlex Web Client Plug-in**

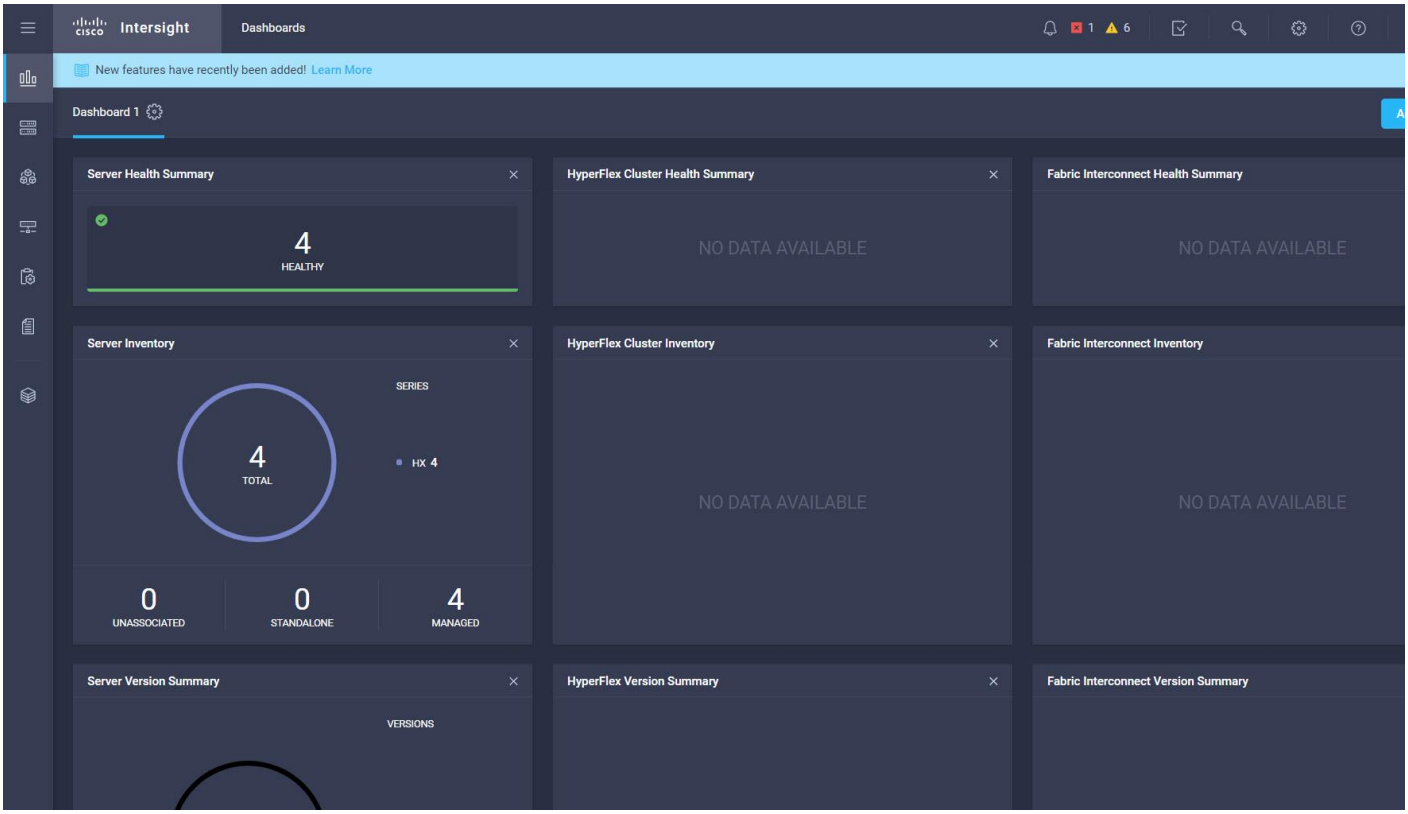


Cisco HyperFlex Connect HTML5 Management Web Page

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

Cisco Intersight Management Web Page

Cisco Intersight simplifies and automates IT operations management (ITOM) to make daily activities easier and more efficient. We have extended our vision of adaptive management to Cisco UCS and HyperFlex systems through the Cisco Intersight cloud-based platform. You can efficiently implement operations automation of your IT infrastructure from the data center to the edge.


Intersight
Dashboards
New features have recently been added! Learn More
Dashboard 1
Server Health Summary
4
HEALTHY
HyperFlex Cluster Health Summary
NO DATA AVAILABLE
Fabric Interconnect Health Summary
NO DATA AVAILABLE
Server Inventory
SERIES
4
TOTAL
HX 4
0
UNASSOCIATED
0
STANDALONE
4
MANAGED
HyperFlex Cluster Inventory
NO DATA AVAILABLE
Fabric Interconnect Inventory
NO DATA AVAILABLE
Server Version Summary
VERSIONS
HyperFlex Version Summary
Fabric Interconnect Version Summary

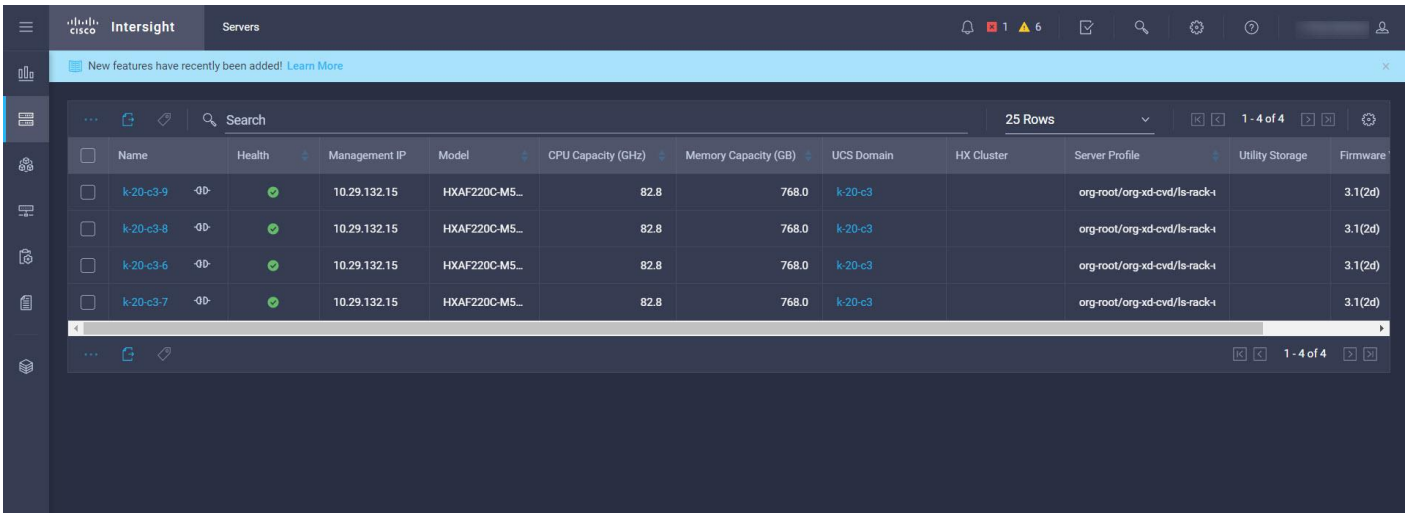
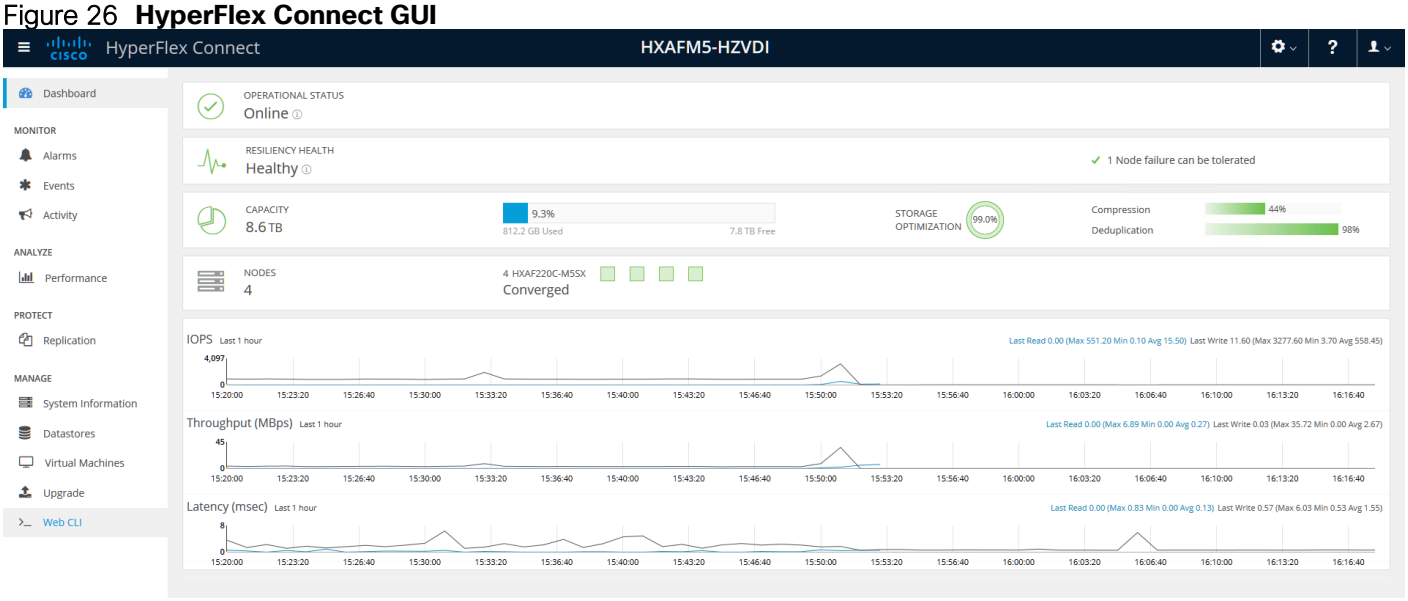

Intersight
Servers
New features have recently been added! Learn More
Search
25 Rows
1 - 4 of 4
Name
Health
Management IP
Model
CPU Capacity (GHz)
Memory Capacity (GB)
UCS Domain
HX Cluster
Server Profile
Utility Storage
Firmware
k-20-c3-9
10.29.132.15
HXAF220C-M5...
82.8
768.0
k-20-c3
org-root/org-xd-cvd/ls-rack-
3.1(2d)
k-20-c3-8
10.29.132.15
HXAF220C-M5...
82.8
768.0
k-20-c3
org-root/org-xd-cvd/ls-rack-
3.1(2d)
k-20-c3-6
10.29.132.15
HXAF220C-M5...
82.8
768.0
k-20-c3
org-root/org-xd-cvd/ls-rack-
3.1(2d)
k-20-c3-7
10.29.132.15
HXAF220C-M5...
82.8
768.0
k-20-c3
org-root/org-xd-cvd/ls-rack-
3.1(2d)
1 - 4 of 4

Figure 26 **HyperFlex Connect GUI**



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 pass-through control of the physical server's SAS disk controller. This method gives the controller VM full control of the physical disk resources, utilizing the SSD drives as a read/write caching layer, and the HDDs 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.

Replication Factor

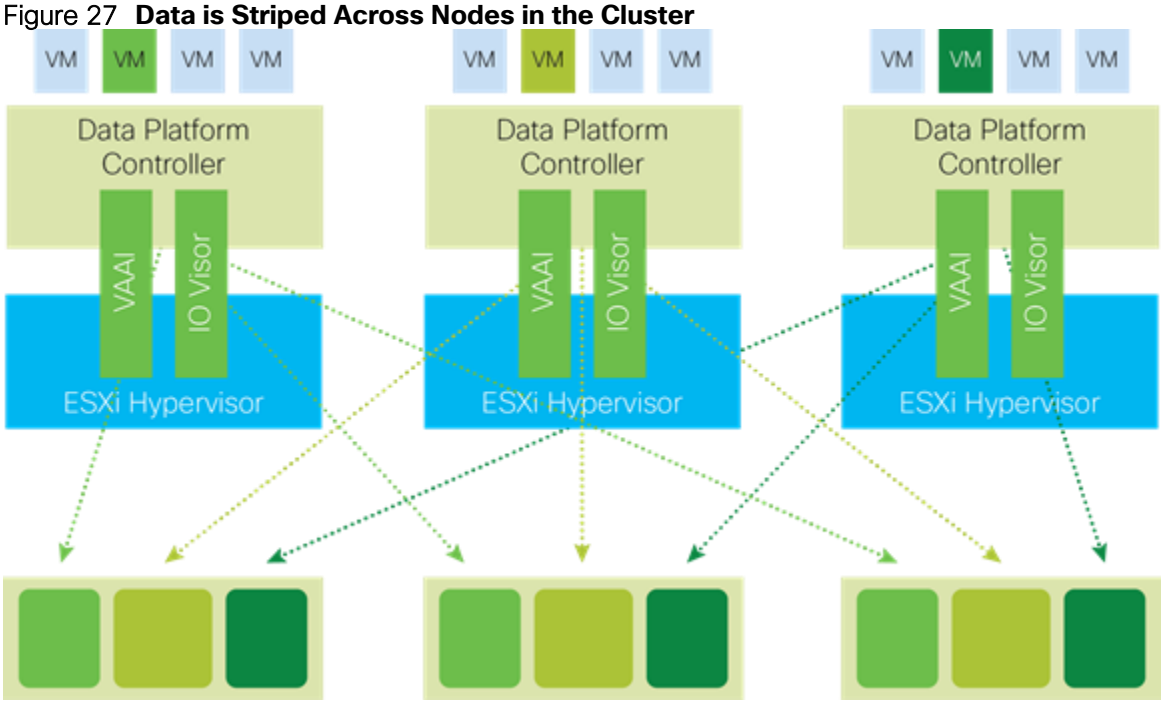
The policy for the number of duplicate copies of each storage block is chosen during cluster setup, and is referred to as the replication factor (RF).

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

Data Distribution

Incoming data is distributed across all nodes in the cluster to optimize performance using the caching tier (Figure 27). Effective data distribution is achieved by mapping incoming data to stripe units that are stored evenly across all nodes, with the number of data replicas determined by the policies you set. When an application writes data, the data is sent to the appropriate node based on the stripe unit, which includes the relevant block of information. This data distribution approach in combination with the capability to have multiple streams writing at the same time avoids both network and storage hot spots, delivers the same I/O performance regardless of virtual machine location, and gives you more flexibility in workload placement. This contrasts with other architectures that use a data locality approach that does not fully use available networking and I/O resources and is vulnerable to hot spots.

Figure 27 **Data is Striped Across Nodes in the Cluster**



When moving a virtual machine to a new location using tools such as VMware Dynamic Resource Scheduling (DRS), the Cisco HyperFlex HX Data Platform does not require data to be moved. This approach significantly reduces the impact and cost of moving virtual machines among systems.

Data Operations

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

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

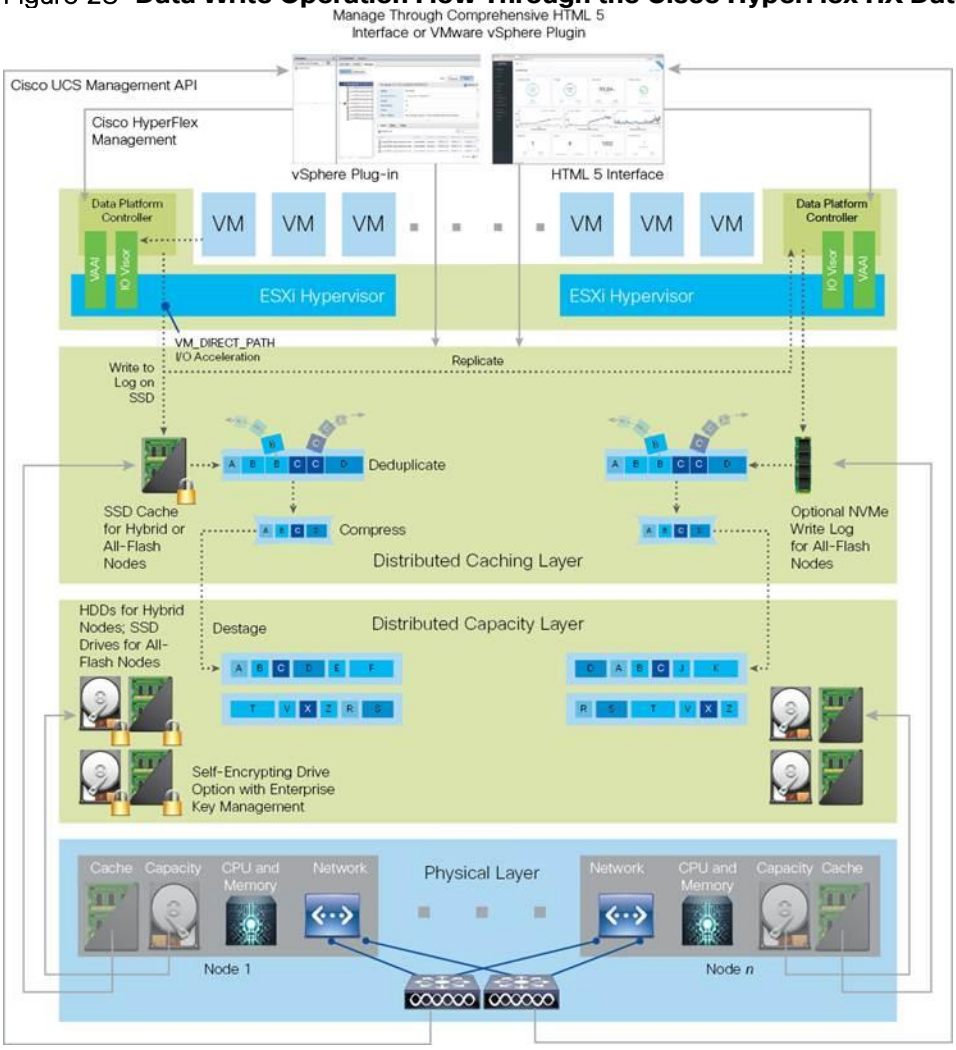
Incoming data is striped across the number of nodes required to satisfy availability requirements—usually two or three nodes. Based on policies you set, incoming write operations are acknowledged as persistent after they are replicated to the SSD drives in other nodes in the cluster. This approach reduces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

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

amplification levels of SSDs and the total number of writes the flash media experiences due to incoming writes and random overwrite operations of the data.

When data is de-staged to the capacity tier in each node, the data is deduplicated and compressed. This process occurs after the write operation is acknowledged, so no performance penalty is incurred for these operations. A small deduplication block size helps increase the deduplication rate. Compression further reduces the data footprint. Data is then moved to the capacity tier as write cache segments are released for reuse (Figure 28).

Figure 28 **Data Write Operation Flow Through the Cisco HyperFlex HX Data Platform**



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

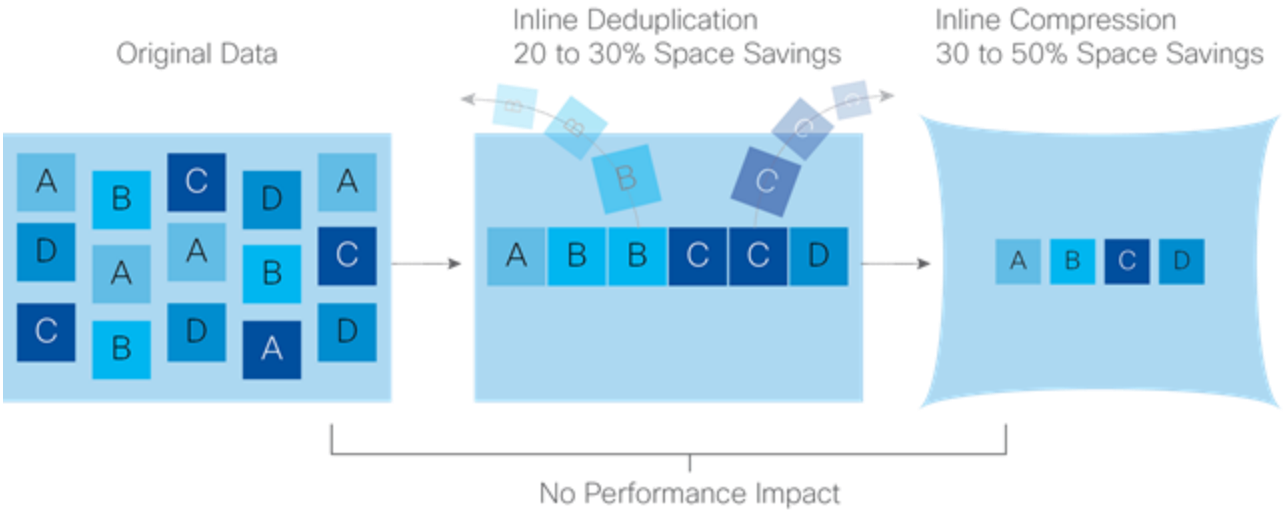
Data Optimization

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

Data Deduplication

Data deduplication is used on all storage in the cluster, including memory and SSD drives. Based on a patent-pending Top-K Majority algorithm, the platform uses conclusions from empirical research that show that most data, when sliced into small data blocks, has significant deduplication potential based on a minority of the data blocks. By fingerprinting and indexing just these frequently used blocks, high rates of deduplication can be achieved with only a small amount of memory, which is a high-value resource in cluster nodes (Figure 29).

Figure 29 **Cisco HyperFlex HX Data Platform Optimizes Data Storage with No Performance Impact**



Inline Compression

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

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

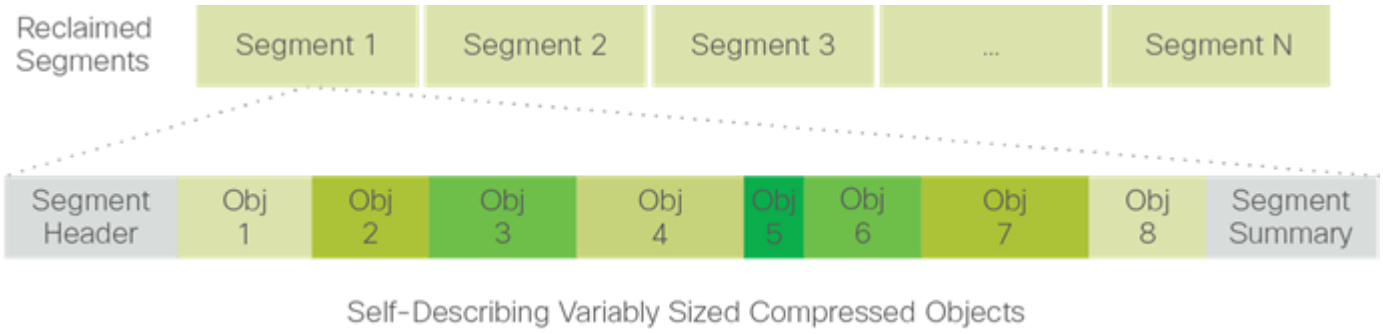
Log-Structured Distributed Objects

In the Cisco HyperFlex HX Data Platform, the log-structured distributed-object store layer groups and compresses data that filters through the deduplication engine into self-addressable objects. These objects are written to disk in a log-structured, sequential manner. All incoming I/O—including random I/O—is written sequentially to both the caching (SSD and memory) and persistent (SSD or HDD) tiers. The objects are distributed across all nodes in the cluster to make uniform use of storage capacity.

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

Data blocks are compressed into objects and sequentially laid out in fixed-size segments, which in turn are sequentially laid out in a log-structured manner (Figure 30). Each compressed object in the log-structured segment is uniquely addressable using a key, with each key fingerprinted and stored with a checksum to provide high levels of data integrity. In addition, the chronological writing of objects helps the platform quickly recover from media or node failures by rewriting only the data that came into the system after it was truncated due to a failure.

Figure 30 **Cisco HyperFlex HX Data Platform Optimizes Data Storage with No Performance Impact**



Encryption

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

Data Services

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

Thin Provisioning

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

Snapshots

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

- **Fast snapshot updates**: When modified-data is contained in a snapshot, it is written to a new location, and the metadata is updated, without the need for read-modify-write operations.
- **Rapid snapshot deletions**: You can quickly delete snapshots. The platform simply deletes a small amount of metadata that is located on an SSD, rather than performing a long consolidation process as needed by solutions that use a delta-disk technique.
- **Highly specific snapshots**: With the Cisco HyperFlex HX Data Platform, you can take snapshots on an individual file basis. In virtual environments, these files map to drives in a virtual machine. This flexible specificity allows you to apply different snapshot policies on different virtual machines.

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

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

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

Fast, Space-Efficient Clones

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

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

Data Replication and Availability

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

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

If a problem occurs in the Cisco HyperFlex HX controller software, data requests from the applications residing in that node are automatically routed to other controllers in the cluster. This same capability can be used to upgrade or perform maintenance on the controller software on a rolling basis without affecting the availability of the cluster or data. This self-healing capability is one of the reasons that the Cisco HyperFlex HX Data Platform is well suited for production applications.

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

Data Rebalancing

A distributed file system requires a robust data rebalancing capability. In the Cisco HyperFlex HX Data Platform, no overhead is associated with metadata access, and rebalancing is extremely efficient. Rebalancing is a non-disruptive online process that occurs in both the caching and persistent layers, and data is moved at a fine level of specificity to improve the use of storage capacity. The platform automatically rebalances existing data when nodes and drives are added or removed or when they fail. When a new node is added to the cluster, its capacity and

performance is made available to new and existing data. The rebalancing engine distributes existing data to the new node and helps ensure that all nodes in the cluster are used uniformly from capacity and performance perspectives. If a node fails or is removed from the cluster, the rebalancing engine rebuilds and distributes copies of the data from the failed or removed node to available nodes in the clusters.

Online Upgrades

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

Cisco Nexus 93108YCPX Switches

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

Architectural Flexibility

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

Feature-Rich

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

Real-Time Visibility and Telemetry

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

Highly Available and Efficient Design

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

Simplified Operations

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

Investment Protection

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

Figure 31 **Cisco Nexus 93108YC Switch**

VMware vSphere 6.5

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 6.5 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 vCenter Server

- Migration Tool
- Improved appliance management
- Native high availability
- Native backup and restore
- There are also general improvements to vCenter Server 6.5, including the vSphere Web Client and the fully supported HTML5-based vSphere Client.

VMware ESXi 6.5 Hypervisor

- With vSphere 6.5, administrators can find significant improvement in patching, upgrading and managing configuration of ESXi hosts through vSphere Update Manager which is enabled by default.
- VMware tool and virtual hardware upgrade
- Improvement in Host Profile, as well as in day to day operations
- Improvement in manageability and configuration rules for Auto-Deploy
- Enhanced monitoring, added option to monitor GPU usage.
- Dedicated Gateways for VMkernel Network Adapter
- VMware vSphere Storage I/O Control Using Storage Policy Based Management

Citrix XenApp™ and XenDesktop™ 7.16

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

The XenDesktop 7.16 release offers these benefits:

- **Comprehensive virtual desktop delivery for any use case**. The XenDesktop 7.16 release incorporates the full power of XenApp, delivering full desktops or just applications to users. Administrators can deploy both XenApp published applications and desktops (to maximize IT control at low cost) or personalized VDI desktops (with simplified image management) from the same management console. Citrix XenDesktop 7.16 leverages common policies and cohesive tools to govern both infrastructure resources and user access.
- **Simplified support and choice of BYO (Bring Your Own) devices**. XenDesktop 7.16 brings thousands of corporate Microsoft Windows-based applications to mobile devices with a native-touch experience and optimized performance. HDX technologies create a “high definition” user experience, even for graphics intensive design and engineering applications.
- **Lower cost and complexity of application and desktop management**. XenDesktop 7.16 helps IT organizations take advantage of agile and cost-effective cloud offerings, allowing the virtualized infrastructure to flex and meet seasonal demands or the need for sudden capacity changes. IT organizations can deploy XenDesktop application and desktop workloads to private or public clouds.

- **Protection of sensitive information through centralization**. XenDesktop decreases the risk of corporate data loss, enabling access while securing intellectual property and centralizing applications since assets reside in the datacenter.

- **Virtual Delivery Agent improvements.** Universal print server and driver enhancements and support for the HDX 3D Pro graphics acceleration for Windows 10 are key additions in XenDesktop 7.16

- **Improved high-definition user experience.** XenDesktop 7.16 continues the evolutionary display protocol leadership with enhanced Thinwire display remoting protocol and Framehawk support for HDX 3D Pro.

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

Citrix XenApp delivers:

- XenApp published apps, also known as server-based hosted applications: These are applications hosted from Microsoft Windows servers to any type of device, including Windows PCs, Macs, smartphones, and tablets. Some XenApp editions include technologies that further optimize the experience of using Windows applications on a mobile device by automatically translating native mobile-device display, navigation, and controls to Windows applications; enhancing performance over mobile networks; and enabling developers to optimize any custom Windows application for any mobile environment.

- XenApp published desktops, also known as server-hosted desktops: These are inexpensive, locked-down Windows virtual desktops hosted from Windows server operating systems. They are well suited for users, such as call center employees, who perform a standard set of tasks.

- Virtual machine–hosted apps: These are applications hosted from machines running Windows desktop operating systems for applications that can’t be hosted in a server environment.

- Windows applications delivered with Microsoft App-V: These applications use the same management tools that you use for the rest of your XenApp deployment.

- Citrix XenDesktop: Includes significant enhancements to help customers deliver Windows apps and desktops as mobile services while addressing management complexity and associated costs. Enhancements in this release include:

- Unified product architecture for XenApp and XenDesktop: The FlexCast Management Architecture (FMA). This release supplies a single set of administrative interfaces to deliver both hosted-shared applications (RDS) and complete virtual desktops (VDI). Unlike earlier releases that separately provisioned Citrix XenApp and XenDesktop farms, the XenDesktop 7.16 release allows administrators to deploy a single infrastructure and use a consistent set of tools to manage mixed application and desktop workloads.

- Support for extending deployments to the cloud. This release provides the ability for hybrid cloud provisioning from Microsoft Azure, Amazon Web Services (AWS) or any Cloud Platform-powered public or private cloud. Cloud deployments are configured, managed, and monitored through the same administrative consoles as deployments on traditional on-premises infrastructure.

Citrix XenDesktop delivers:

- VDI desktops: These virtual desktops each run a Microsoft Windows desktop operating system rather than running in a shared, server-based environment. They can provide users with their own desktops that they can fully personalize.

- Hosted physical desktops: This solution is well suited for providing secure access powerful physical machines, such as blade servers, from within your data center.

- Remote PC access: This solution allows users to log in to their physical Windows PC from anywhere over a secure XenDesktop connection.
- Server VDI: This solution is designed to provide hosted desktops in multitenant, cloud environments.
- Capabilities that allow users to continue to use their virtual desktops: These capabilities let users continue to work while not connected to your network.

This product release includes the following new and enhanced features:

 Some XenDesktop editions include the features available in XenApp.

Zones

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

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

For more information, see the Zones article.

Improved Database Flow and Configuration

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

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

For more information, see the Databases and Controllers articles.

Application Limits

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

For more information, see the Manage applications article.

Multiple Notifications before Machine Updates or Scheduled Restarts

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

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

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

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

API Support for Managing Session Roaming

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

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

For more information, see the Sessions article.

API Support for Provisioning VMs from Hypervisor Templates

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

Support for New and Additional Platforms

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

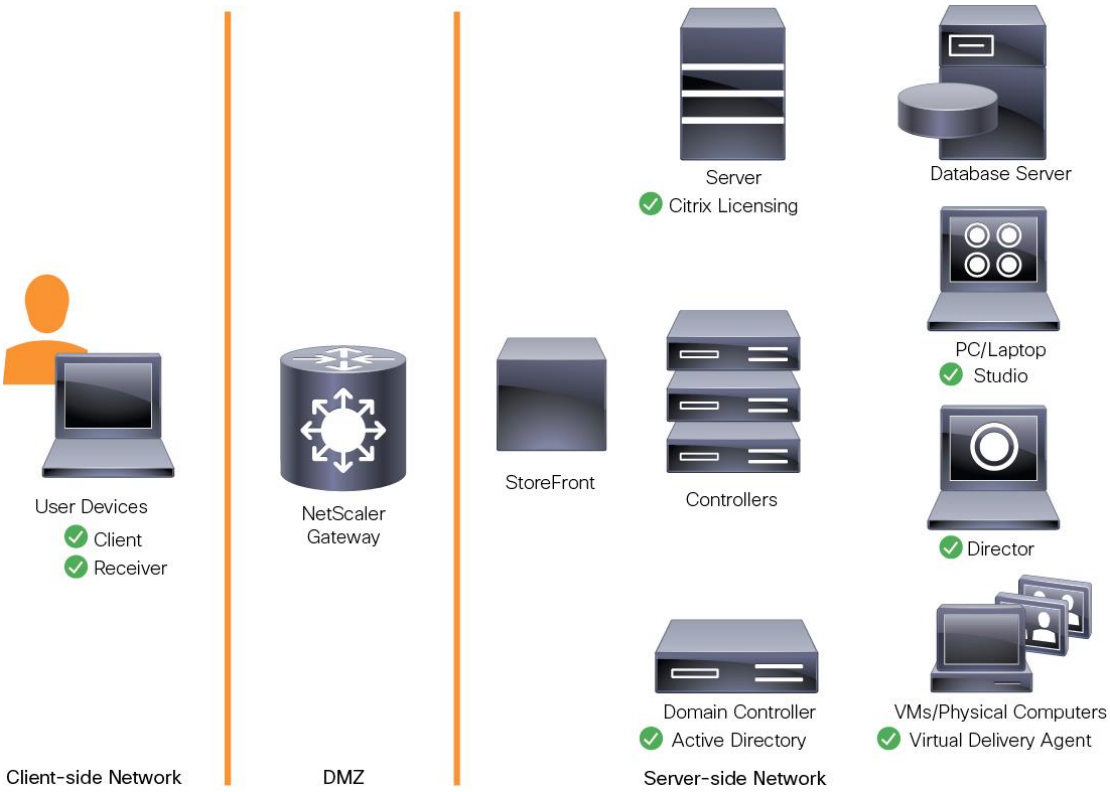
By default, SQL Server 2012 Express SP2 is installed when you install the Delivery Controller. SP1 is no longer installed.

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

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

You can create connections to Microsoft Azure virtualization resources.

Figure 32 **Logical Architecture of Citrix XenDesktop**



Citrix Provisioning Services 7.16

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

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

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

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

Benefits for Citrix XenApp and Other Server Farm Administrators

If you manage a pool of servers that work as a farm, such as Citrix XenApp servers or web servers, maintaining a uniform patch level on your servers can be difficult and time consuming. With traditional imaging solutions, you start with a clean golden master image, but as soon as a server is built with the master image, you must patch that individual server along with all the other individual servers. Rolling out patches to individual servers in your farm is not only inefficient, but the results can also be unreliable. Patches often fail on an individual server, and you may

not realize you have a problem until users start complaining or the server has an outage. After that happens, getting the server resynchronized with the rest of the farm can be challenging, and sometimes a full reimaging of the machine is required.

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

Benefits for Desktop Administrators

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

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

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

Citrix Provisioning Services Solution

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

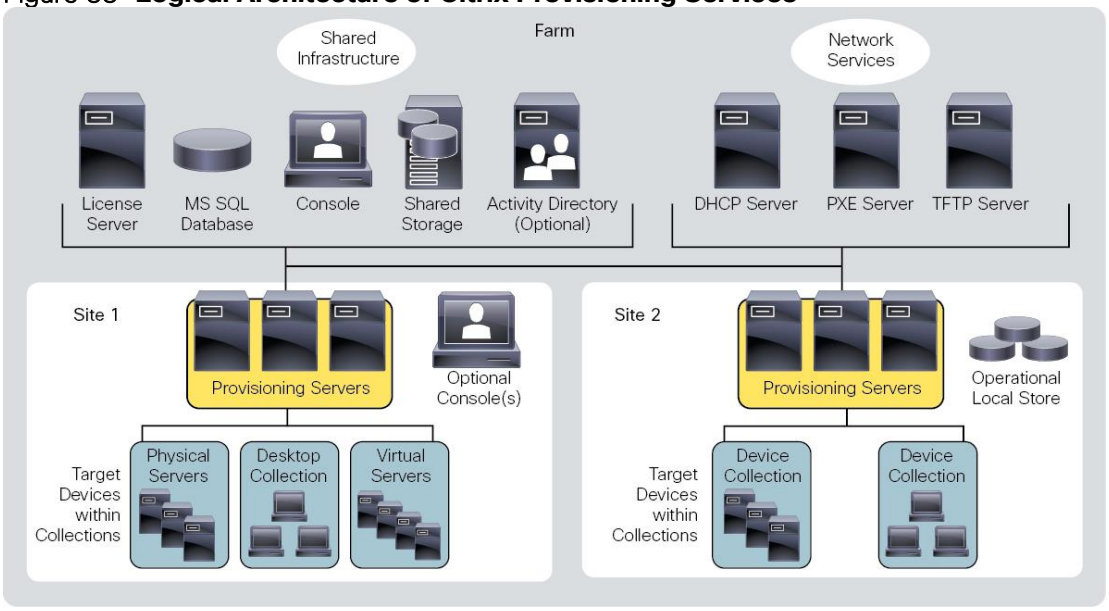
The PVS solution's infrastructure is based on software-streaming technology. After PVS components are installed and configured, a vDisk is created from a device's hard drive by taking a snapshot of the OS and application image and then storing that image as a vDisk file on the network. A device used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

Citrix Provisioning Services Infrastructure

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

A PVS farm contains several components. 0 provides a high-level view of a basic PVS infrastructure and shows how PVS components might appear within that implementation.

Figure 33 **Logical Architecture of Citrix Provisioning Services**



The following new features are available with Provisioning Services 7.16:

- Linux streaming
- XenServer proxy using PVS-Accelerator

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

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

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

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

- Traditional PC: A traditional PC is what —typicallyǁ 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 XENAPP Session Hosts and the user interacts through a delivery protocol. With published applications, a single installed instance of an application, such as Microsoft, is shared by multiple users simultaneously. Each user receives an application "session" and works in an isolated memory space.
- Streamed Applications: Streamed desktops and applications run entirely on the user‘s local client device and are sent from a server on demand. The user interacts with the application or desktop directly but the resources may only available while they are connected to the network.
- Local Virtual Desktop: A local virtual desktop is a desktop running entirely on the user‘s local device and continues to operate when disconnected from the network. In this case, the user’s local device is used as a type 1 hypervisor and is synced with the data center when the device is connected to the network.

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

Understanding Applications and Data

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

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

Project Planning and Solution Sizing Sample Questions

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

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

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

- Do we have end user experience performance metrics identified for each desktop sub-group?
- How will we measure success or failure?
- What is the future implication of success or failure?

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

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

Citrix XenDesktop Design Fundamentals

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

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

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

Machine Catalogs

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

a Windows Server OS (for RDS hosted shared desktops) or a Windows Desktop OS (for hosted pooled VDI desktops).

Delivery Groups

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

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

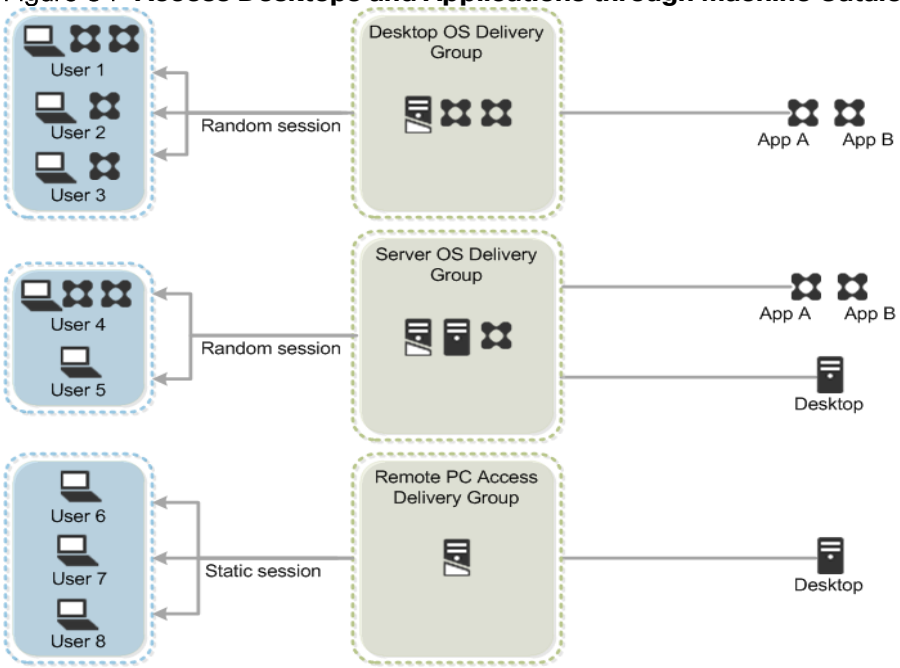
As part of the creation process, you specify the following Delivery Group properties:

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

Figure 34 illustrates how users access desktops and applications through machine catalogs and delivery groups.

The Server OS and Desktop OS Machines configured in this CVD support the hosted shared desktops and hosted virtual desktops (both non-persistent and persistent).

Figure 34 **Access Desktops and Applications through Machine Catalogs and Delivery Groups**



Citrix Provisioning Services

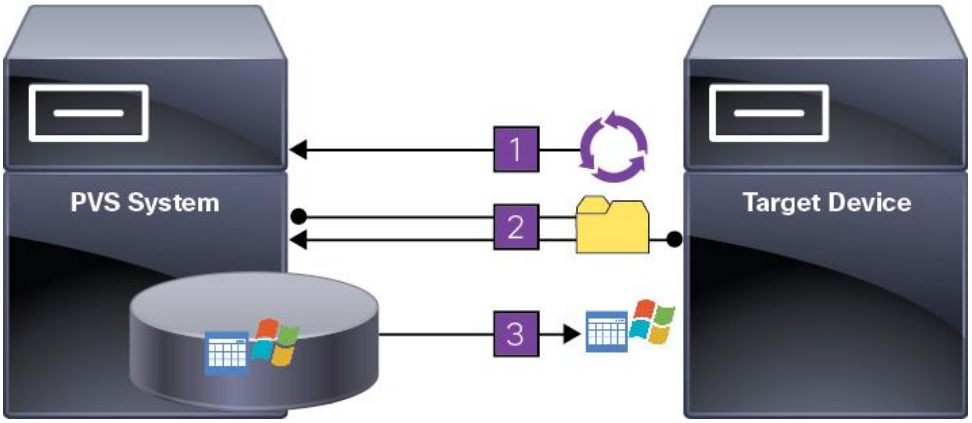
Citrix XenDesktop 7.16 can be deployed with or without Citrix Provisioning Services (PVS). The advantage of using Citrix PVS is that it allows virtual machines to be provisioned and re-provisioned in real-time from a single

shared-disk image. In this way administrators can completely eliminate the need to manage and patch individual systems and reduce the number of disk images that they manage, even as the number of machines continues to grow, simultaneously providing the efficiencies of a centralized management with the benefits of distributed processing.

The Provisioning Services solution's infrastructure is based on software-streaming technology. After installing and configuring Provisioning Services components, a single shared disk image (vDisk) is created from a device's hard drive by taking a snapshot of the OS and application image, and then storing that image as a vDisk file on the network. A device that is used during the vDisk creation process is the Master target device. Devices or virtual machines that use the created vDisks are called target devices.

When a target device is turned on, it is set to boot from the network and to communicate with a Provisioning Server. Unlike thin-client technology, processing takes place on the target device.

Figure 35 **Citrix Provisioning Services Functionality**



The target device downloads the boot file from a Provisioning Server (Step 2) and boots. Based on the boot configuration settings, the appropriate vDisk is mounted on the Provisioning Server (Step 3). The vDisk software is then streamed to the target device as needed, appearing as a regular hard drive to the system.

Instead of immediately pulling all the vDisk contents down to the target device (as with traditional imaging solutions), the data is brought across the network in real-time as needed. This approach allows a target device to get a completely new operating system and set of software in the time it takes to reboot. This approach dramatically decreases the amount of network bandwidth required and making it possible to support a larger number of target devices on a network without impacting performance

Citrix PVS can create desktops as Pooled or Private:

- Pooled Desktop: A pooled virtual desktop uses Citrix PVS to stream a standard desktop image to multiple desktop instances upon boot.
- Private Desktop: A private desktop is a single desktop assigned to one distinct user.

The alternative to Citrix Provisioning Services for pooled desktop deployments is Citrix Machine Creation Services (MCS), which is integrated with the XenDesktop Studio console.

Locating the PVS Write Cache

When considering a PVS deployment, there are some design decisions that need to be made regarding the write cache for the target devices that leverage provisioning services. The write cache is a cache of all data that the target device has written. If data is written to the PVS vDisk in a caching mode, the data is not written back to the base vDisk. Instead it is written to a write cache file in one of the following locations:

- Cache on device hard drive. Write cache exists as a file in NTFS format, located on the target-device's hard drive. This option frees up the Provisioning Server since it does not have to process write requests and does not have the finite limitation of RAM.
- Cache on device hard drive persisted. (Experimental Phase) This is the same as "Cache on device hard drive", except that the cache persists. At this time, this method is an experimental feature only, and is only supported for NT6.1 or later (Windows 10 and Windows 2008 R2 and later). This method also requires a different bootstrap.
- Cache in device RAM. Write cache can exist as a temporary file in the target device's RAM. This provides the fastest method of disk access since memory access is always faster than disk access.
- Cache in device RAM with overflow on hard disk. This method uses VHDX differencing format and is only available for Windows 10 and Server 2008 R2 and later. When RAM is zero, the target device write cache is only written to the local disk. When RAM is not zero, the target device write cache is written to RAM first. When RAM is full, the least recently used block of data is written to the local differencing disk to

accommodate newer data on RAM. The amount of RAM specified is the non-paged kernel memory that the target device will consume.

- Cache on a server. Write cache can exist as a temporary file on a Provisioning Server. In this configuration, all writes are handled by the Provisioning Server, which can increase disk I/O and network traffic. For additional security, the Provisioning Server can be configured to encrypt write cache files. Since the write-cache file persists on the hard drive between reboots, encrypted data provides data protection in the event a hard drive is stolen.
- Cache on server persisted. This cache option allows for the saved changes between reboots. Using this option, a rebooted target device is able to retrieve changes made from previous sessions that differ from the read only vDisk image. If a vDisk is set to this method of caching, each target device that accesses the vDisk automatically has a device-specific, writable disk file created. Any changes made to the vDisk image are written to that file, which is not automatically deleted upon shutdown.

In this CVD, Provisioning Server 7.16 was used to manage Pooled/Non-Persistent VDI Machines and XenApp RDS Machines with "Cache in device RAM with Overflow on Hard Disk" for each virtual machine. This design enables good scalability to many thousands of desktops. Provisioning Server 7.16 was used for Active Directory machine account creation and management as well as for streaming the shared disk to the hypervisor hosts.

Example XenDesktop Deployments

Two examples of typical XenDesktop deployments are the following:

- A distributed components configuration
- A multiple site configuration

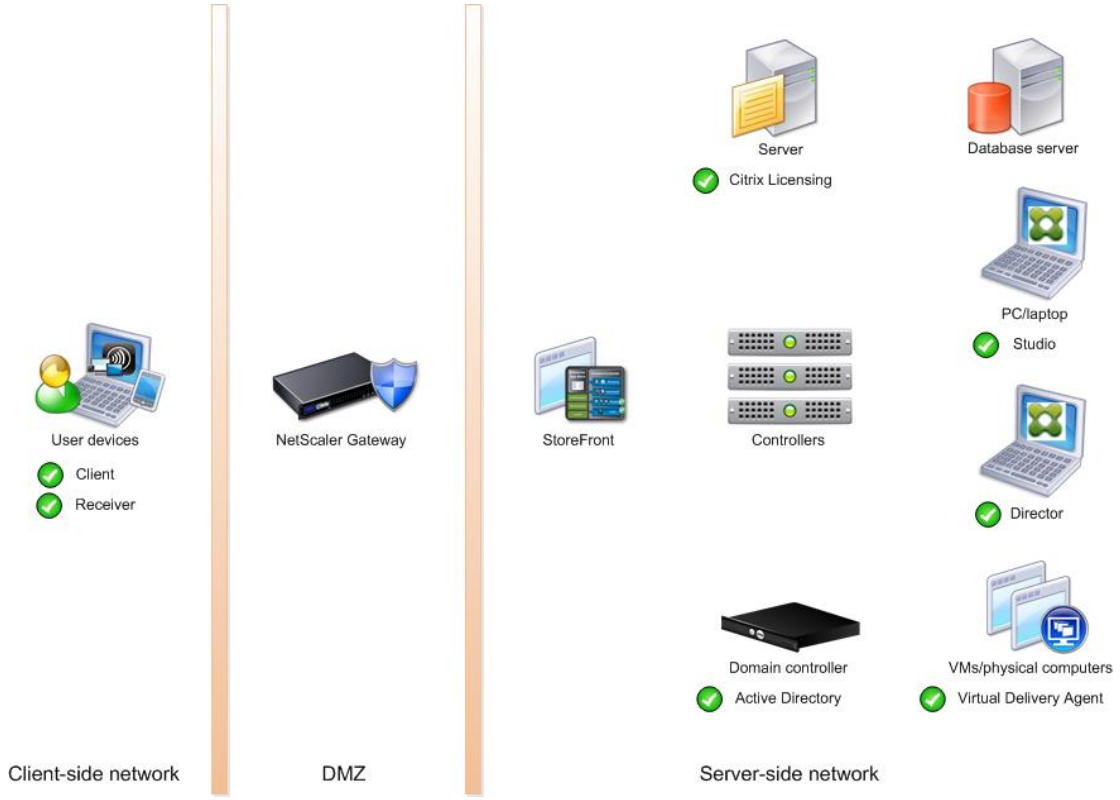
Since XenApp and XenDesktop 7.16 are based on a unified architecture, combined they can deliver a combination of Hosted Shared Desktops (HSDs, using a Server OS machine) and Hosted Virtual Desktops (HVDs, using a Desktop OS).

Distributed Components Configuration

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

Figure 36 shows an example of a distributed components configuration. A simplified version of this configuration is often deployed for an initial proof-of-concept (POC) deployment. The CVD described in this document deploys Citrix XenDesktop in a configuration that resembles this distributed components configuration shown. Two Cisco C220 rack servers host the required infrastructure services (AD, DNS, DHCP, Profile, SQL, Citrix XenDesktop management, and StoreFront servers).

Figure 36 **Example of a Distributed Components Configuration**

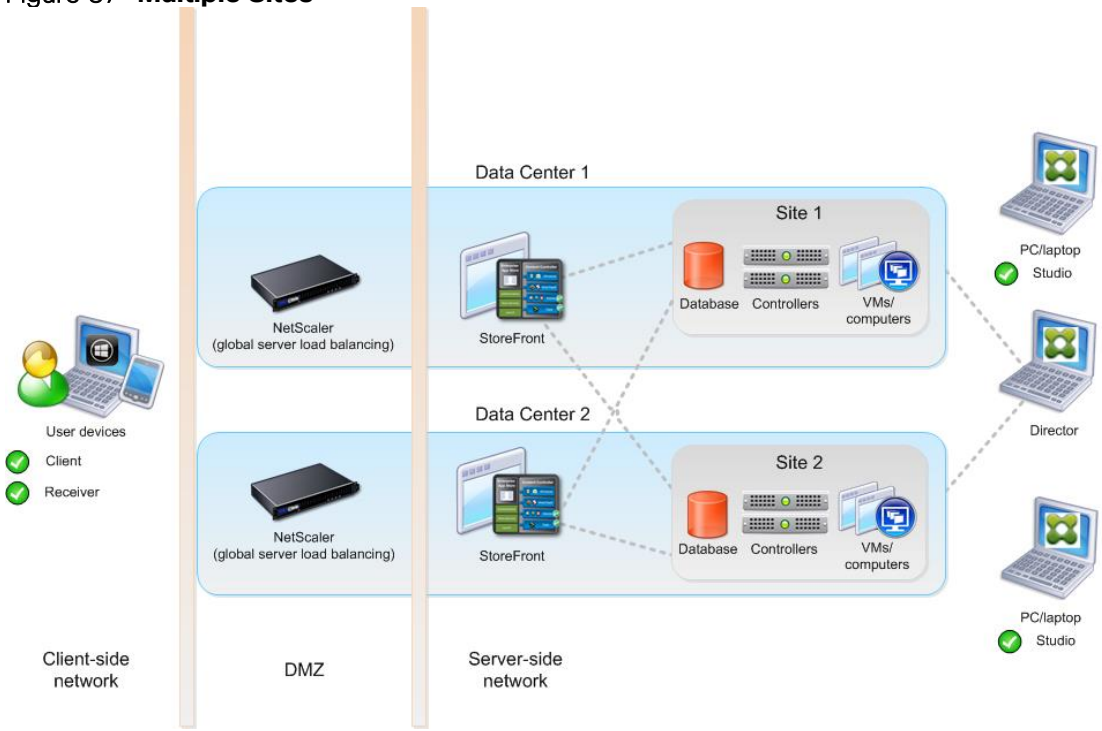


Multiple Site Configuration

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

In Figure 37 depicting multiple sites, a site was created in two data centers. Having two sites globally, rather than just one, minimizes the amount of unnecessary WAN traffic.

Figure 37 **Multiple Sites**



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

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

Citrix Cloud Services

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

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

Designing a XenDesktop Environment for a Mixed Workload

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

Server OS machines	**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 OS machines	**You want**: A client-based application delivery solution that is secure, provides centralized management, and supports a large number of users per host server (or hypervisor), while providing users with applications that display seamlessly in high-definition. **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 Access	**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. Your users: Employees or contractors that have the option to work from home, but need access to specific software or data on their corporate desktops to perform their jobs remotely. 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.

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, or Cisco UCS B/C-series as compute 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 4000 users for virtual desktop and hosted shared desktop workload featuring the following deployment methods:

- Citrix XenDesktop 7.16 Non-Persistent Hosted Virtual Desktops (HVD) provisioned with Citrix Provisioning Services (PVS) with Write Cache in device RAM with Overflow on Hard Disk on Cisco HyperFlex
- Citrix XenDesktop 7.16 persistent HVDs provisioned with Citrix Machine Creation Services (MCS) and using full copy on Cisco HyperFlex
- Citrix XenDesktop 7.16 Hosted Shared Virtual Desktops (HSD) provisioned with Citrix Provisioning Services (PVS) with Write Cache in device RAM with Overflow on Hard Disk on Cisco HyperFlex
- Microsoft Windows Server 2016 for User Profile Manager
- Microsoft Windows 2016 Server for Login VSI Management and data servers to simulate real world VDI workload
- VMware vSphere ESXi 6.5 Update 1 Hypervisor
- Windows Server 2016 for XenApp Servers & Windows 10 64-bit Operating Systems for VDI virtual machines
- Microsoft SQL Server 2016
- Cisco HyperFlex data platform v2.6.1b

Figure 38 **Detailed Reference Architecture with Physical Hardware Cabling Configured to Enable the Solution**

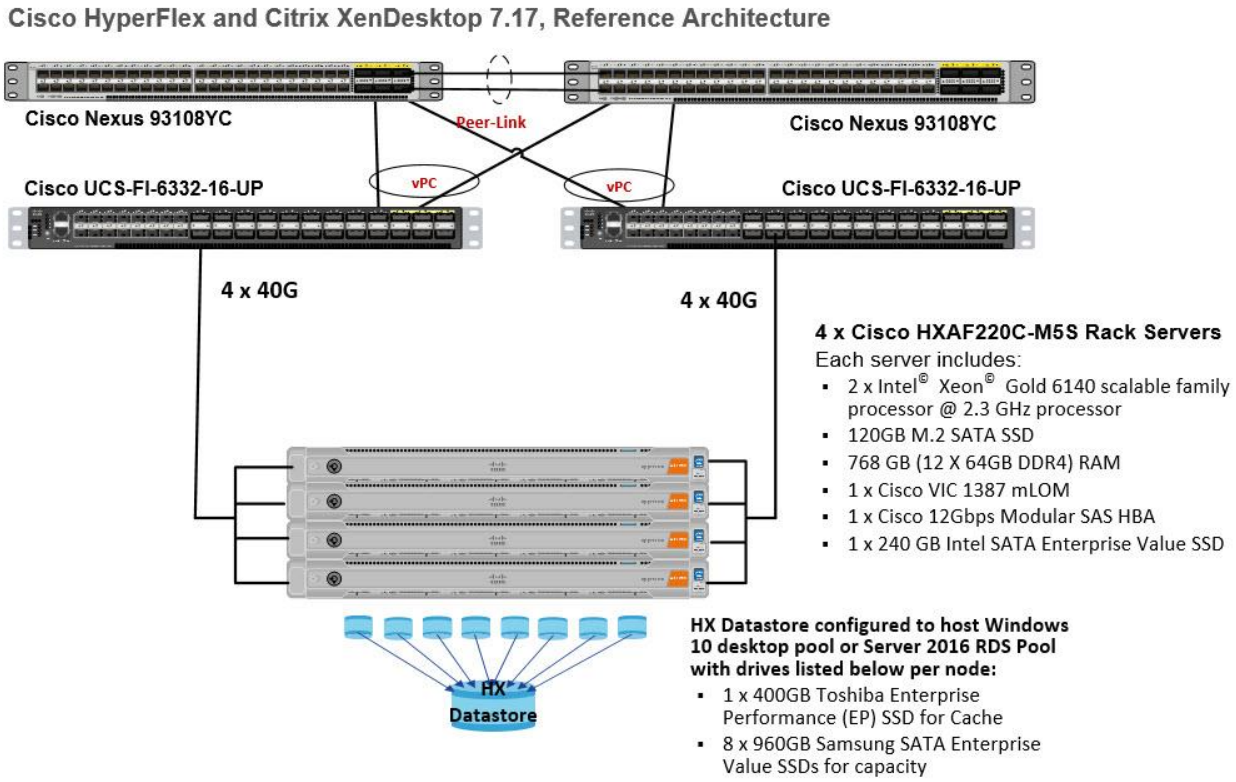
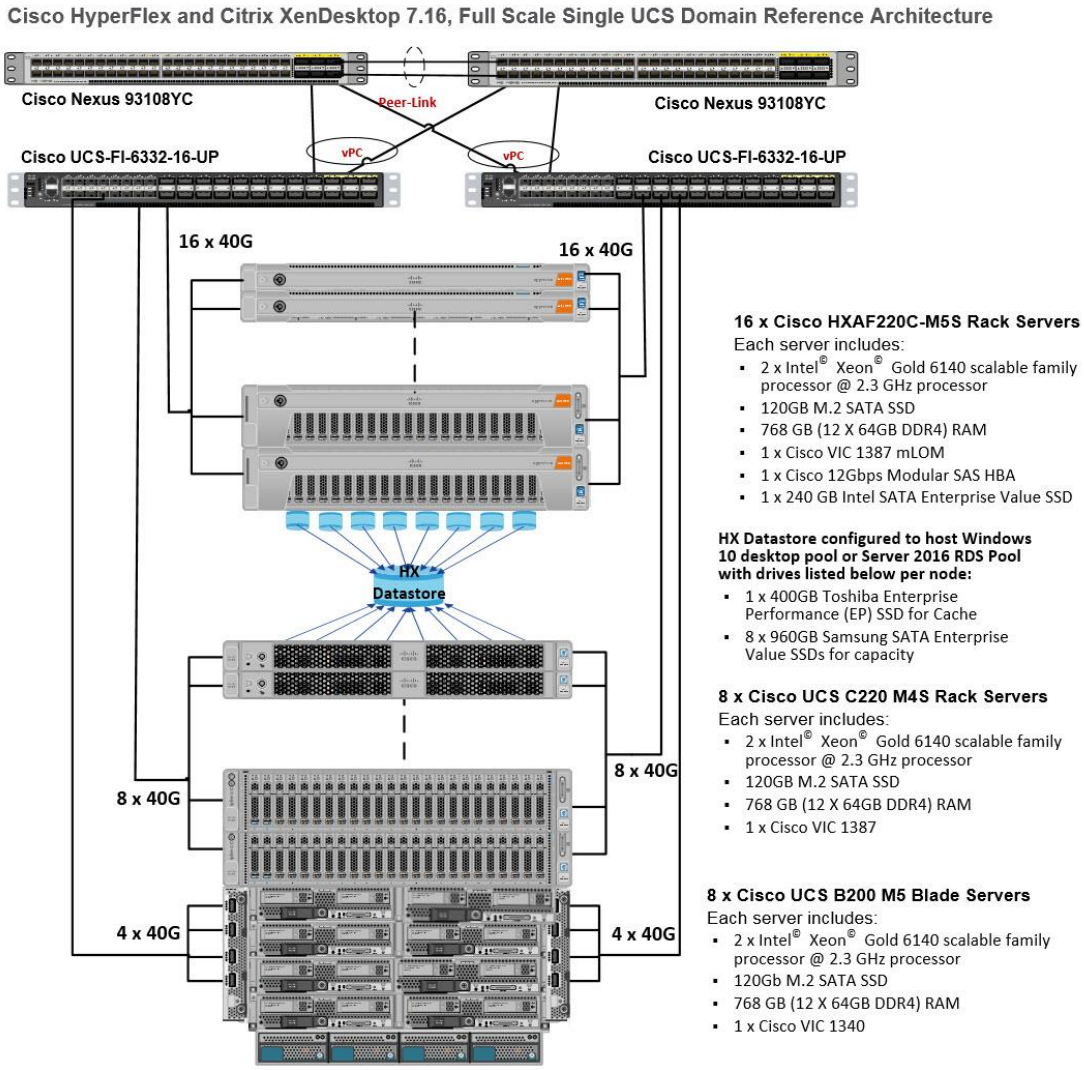


Figure 39 **Detailed Reference Architecture with Physical Hardware Cabling Configured to Enable the Scale-Out Solution as Per the Current Cluster Limit**



Hardware Deployed

The solution contains the following hardware as shown in Figure 39:

- Two Cisco Nexus 93108YC 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).
- Four Cisco UCS HXAF220c-M5S Rack Servers with Intel Xeon Gold 6140 scalable family 2.3-GHz 18-core processors, 768GB RAM 2666-MHz and VIC1387 mLOM cards running Cisco HyperFlex data platform v2.6.1a 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 1 Software and Firmware Versions

Vendor	Product	Version
Cisco	UCS Component Firmware	3.2(2d) bundle release
Cisco	UCS Manager	3.2(2d) bundle release
Cisco	UCS HXAF220c-M5S rack server	3.2(2d) bundle release
Cisco	VIC 1387	4.2(2d)
Cisco	HyperFlex Data Platform	2.6.1b-26588
Cisco	Cisco NENIC	1.0.2.02
Cisco	Cisco fNIC	1.6.0.34
Network	Cisco Nexus 9000 NX-OS	7.0(3)I2(2d)
Citrix	XenDesktop	7.16
Citrix	Provisioning Services	7.16
Citrix	User Profile Manager	
Citrix	Receiver	4.11
VMware	vCenter Server Appliance	6.5.0-5973321
VMware	vSphere ESXi 6.5 Update 1	6.5 U1-5969303

Logical Architecture

The logical architecture of this solution is designed to support up to 450 Hosted Virtual Microsoft Windows 10 Desktops and 600 XenApp hosted shared server desktop users within a four node Cisco UCS HXAF220c-HyperFlex cluster, which provides physical redundancy for each workload type.

Figure 40 **Logical Architecture Design**

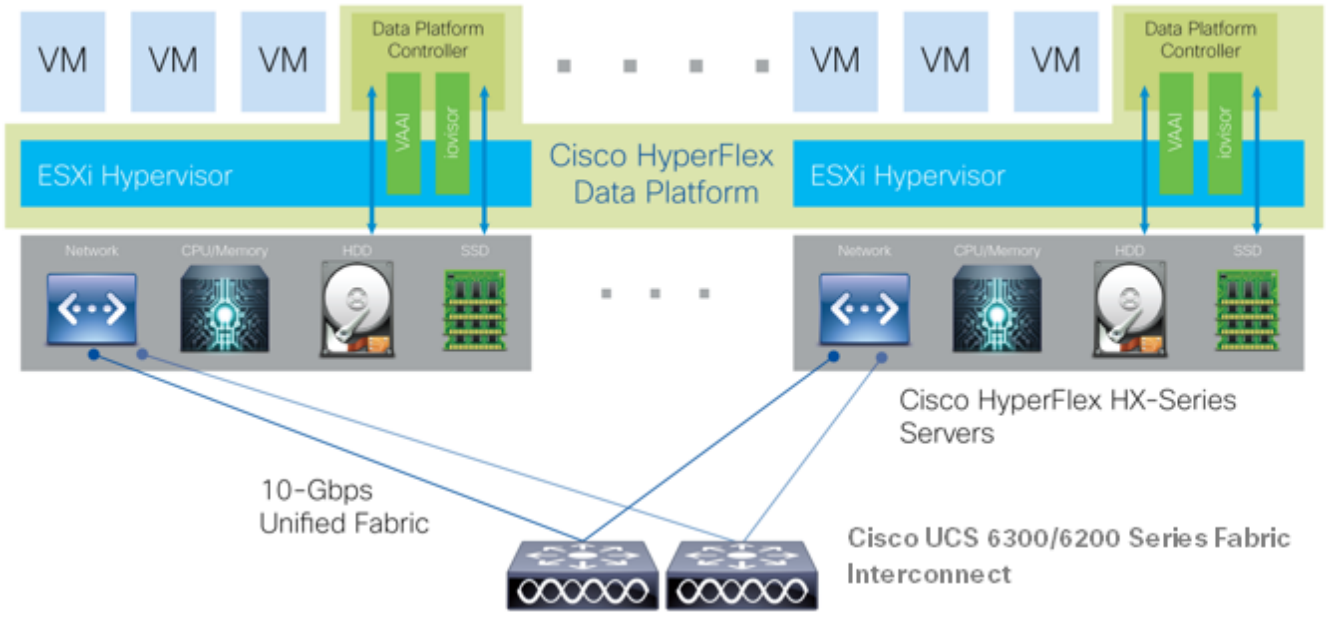


Table 1 lists the software revisions for this solution.

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. Table 2 through Table 6 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 interfaces
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
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

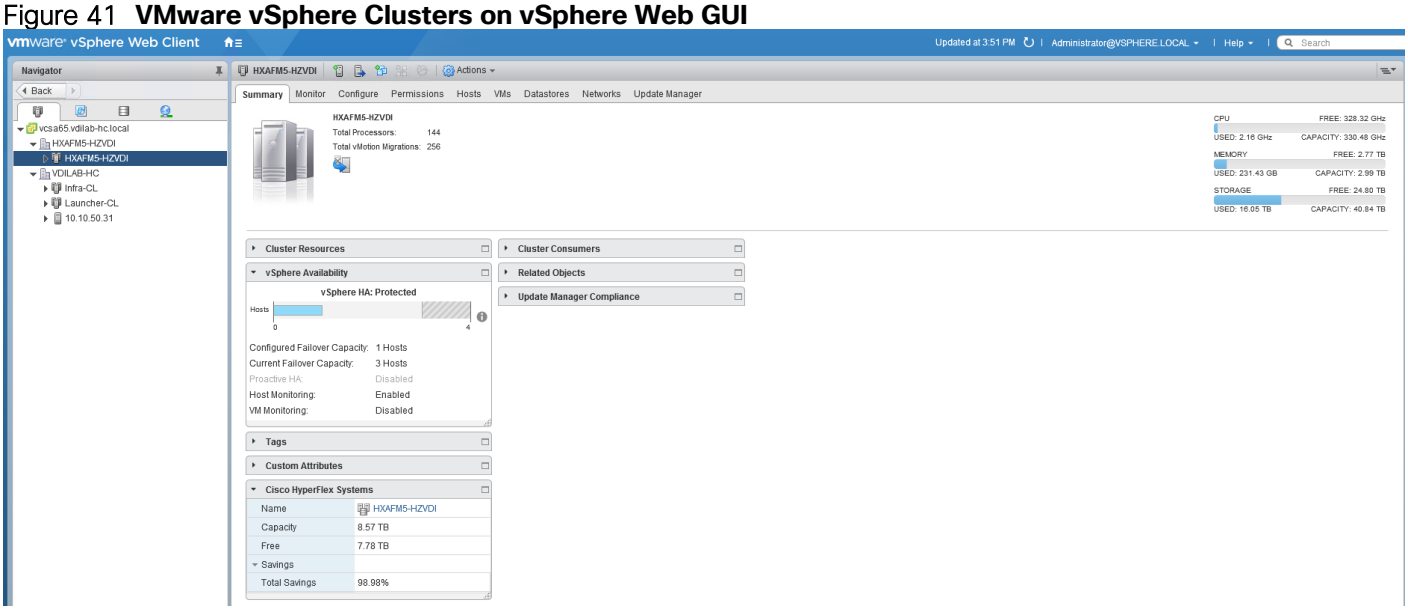
All HyperFlex storage traffic traversing the hx-storage-data VLAN and subnet is configured to use jumbo frames, or to be precise all communication is configured to send IP packets with a Maximum Transmission Unit (MTU) size of 9000 bytes. Using a larger MTU value means that each IP packet sent carries 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, Cisco Nexus 1000v Virtual Supervisor Module, and VSMs, etc.)
- HyperFlex Cluster: Citrix XenDesktop VMs (Windows Server 2016) or Persistent/Non-Persistent VDI VM Pools (Windows 10 64-bit)
- 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 41 **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

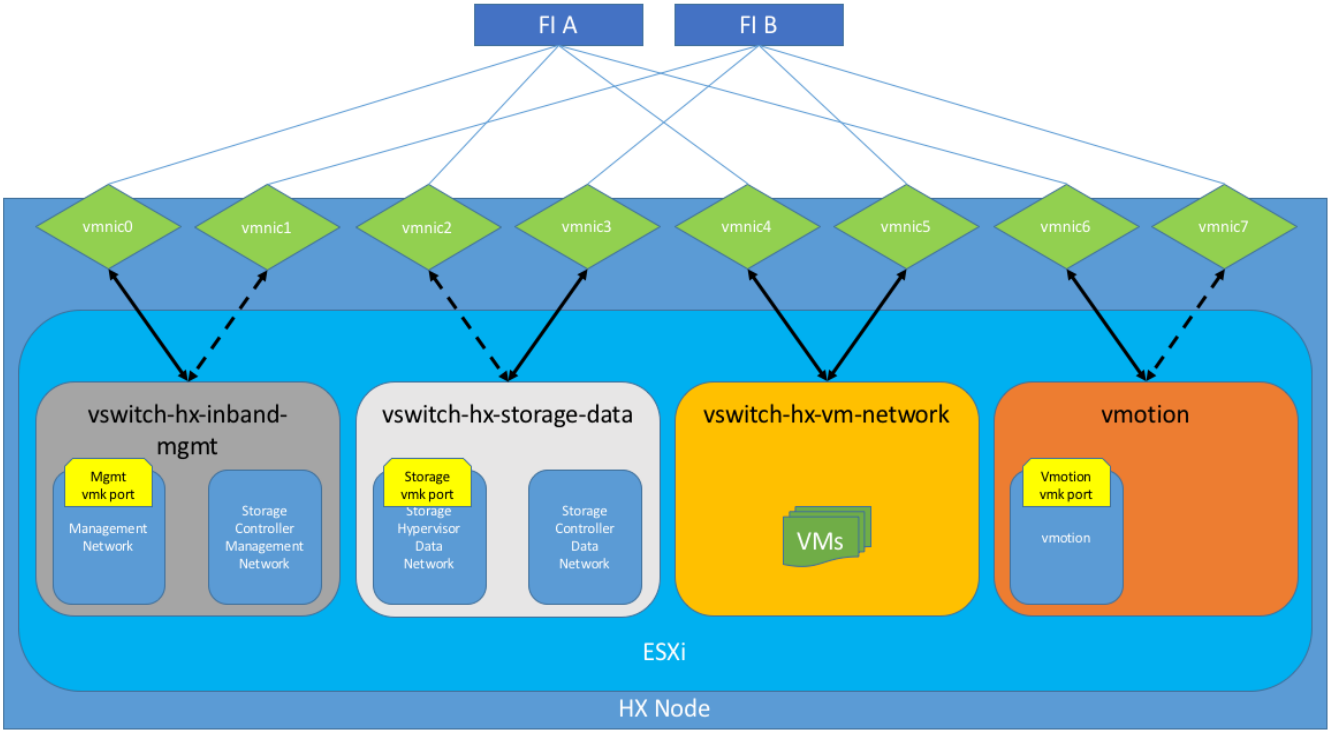
- **vmotion**: This vSwitch is created as part of the automated installation. The switch has two uplinks, active on fabric A and standby on fabric B, with jumbo frames required. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in ESXi/vSphere

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

Table 3 Table ESXi Host Virtual Switch Configuration

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

Figure 42 **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 Virtual Machines

A key component of the Cisco HyperFlex system is the Storage Platform Controller Virtual Machine running on each of the nodes in the HyperFlex cluster. The controller VMs cooperate to form and coordinate the Cisco HX Distributed Filesystem, and service all the guest VM IO requests. The controller VMs are deployed as a 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

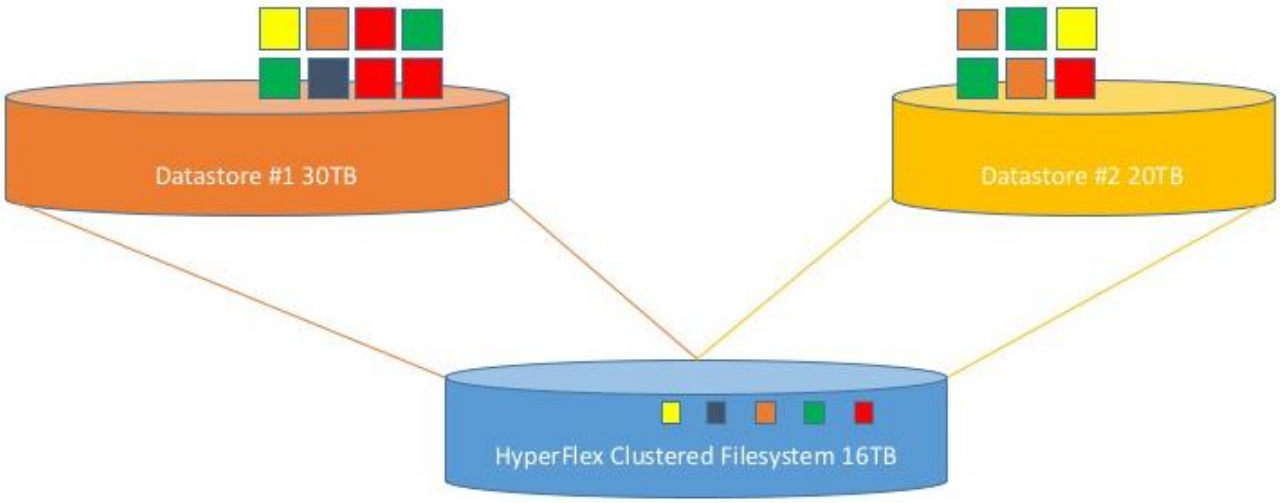
The physical storage location of the controller VM is similar between the Cisco HXAF220c-M5S and HXAF240c-M5SX model servers. The storage controller VM is operationally no different from any other typical virtual machines in an ESXi environment. The VM must have a virtual disk with the bootable root 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:

The Cisco UCS compute-only Nodes also place a lightweight storage controller VM on a 3.5 GB VMFS datastore, provisioned from the M.2 SATA SSD drive.

Cisco 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 or HyperFlex Connect GUI. 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 43 **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. Table 4 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.

Table 5 details the memory resource reservation of the storage controller VMs.

Table 5 Controller VM Memory Reservations

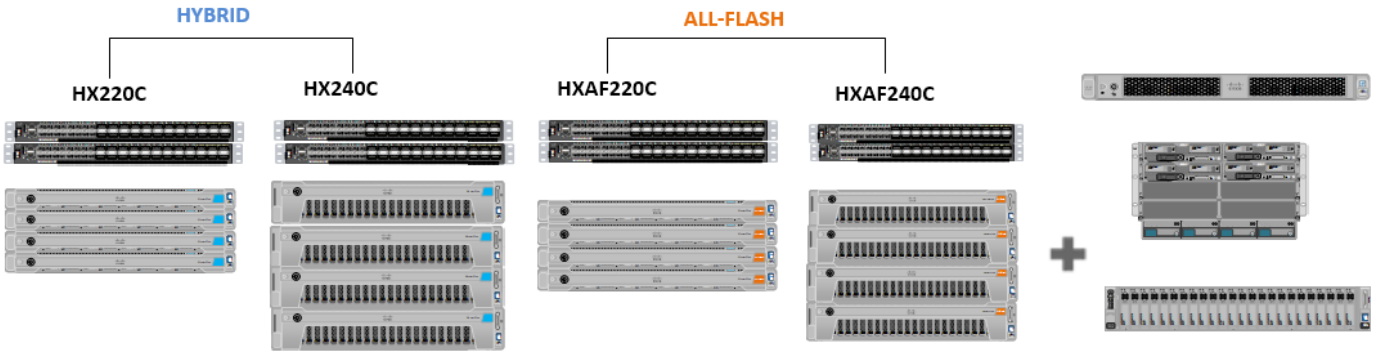
Server Model	Amount of Guest Memory	Reserve All Guest Memory
HX220c-M5 HXAF220c-M5	48 GB	Yes
HX240c-M5SX HXAF240c-M5SX	72 GB	Yes

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

Solution Configuration

This section details the configuration and tuning that was performed on the individual components to produce a complete, validated solution. Figure 44 illustrates the configuration topology for this solution.

Figure 44 **Configuration Topology for Scalable Citrix XenDesktop 7.16 Workload with HyperFlex**



Cisco UCS Compute Platform

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

Physical Infrastructure

Solution Cabling

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

The tables in this section 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 45 shows a cabling diagram for a Citrix XenDesktop configuration using the Cisco Nexus 9000 and Cisco UCS Fabric Interconnect.

Table 6 Cisco Nexus 93108YC-Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93108YC A	Eth1/1	10GbE	Cisco Nexus 93108YC B	Eth1/1
	Eth1/2	10GbE	Cisco Nexus 93108YC B	Eth1/2
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth1/13

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

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

Table 7 Cisco Nexus 93108YC-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93108YC B	Eth1/1	10GbE	Cisco Nexus 93108YC A	Eth1/1
	Eth1/2	10GbE	Cisco Nexus 93108YC A	Eth1/2
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth1/15
	Eth1/4	10GbE	Cisco UCS fabric interconnect A	Eth1/16
	Eth1/5	10GbE	Cisco UCS fabric interconnect B	Eth1/15
	Eth1/6	40GbE	Cisco UCS fabric interconnect B	Eth1/16
	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

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

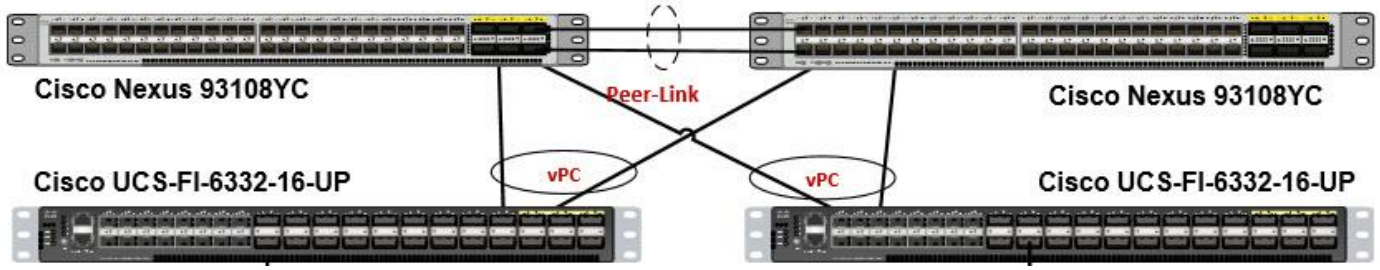
Table 8 Cisco UCS Fabric Interconnect A Cabling Information

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

Table 9 Cisco UCS Fabric Interconnect B Cabling Information

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

Figure 45 **Cable Connectivity Between Cisco Nexus 93108YC A and B to Cisco UCS 6248 Fabric A and B**



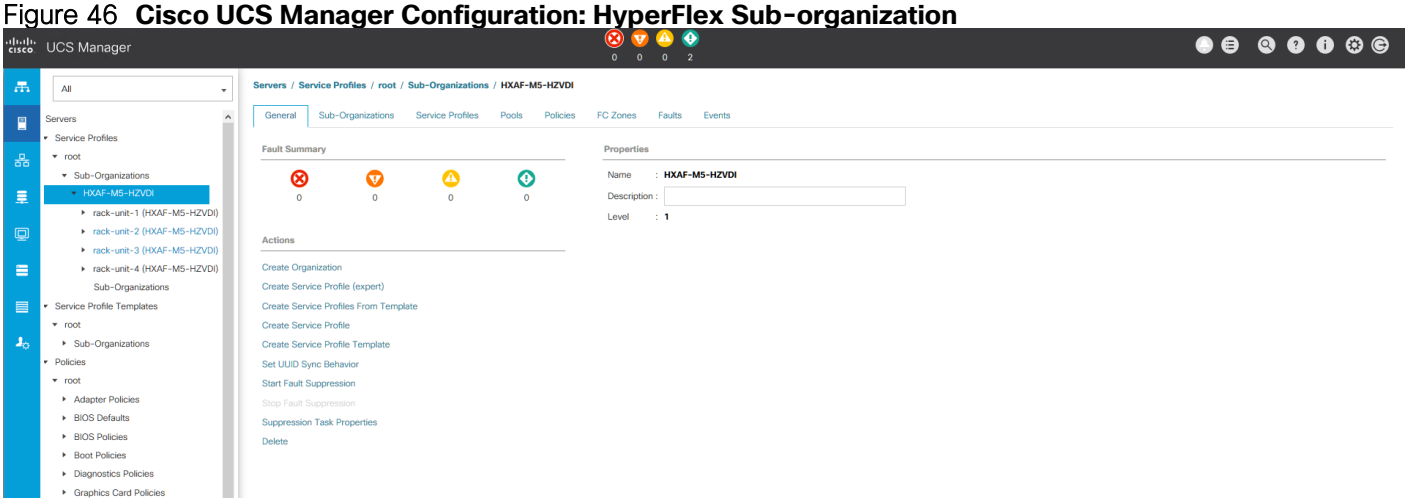
Cisco Unified Computing System Configuration

This section details the Cisco UCS configuration performed 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 www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-guides-list.html) 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) Cisco UCS Manager - Configuration Guides - Cisco

During the HyperFlex Installation a Cisco UCS Sub-Organization is created named “hx-cluster”. The sub-organization is created below the root level of the Cisco 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 46 **Cisco UCS Manager Configuration: HyperFlex Sub-organization**

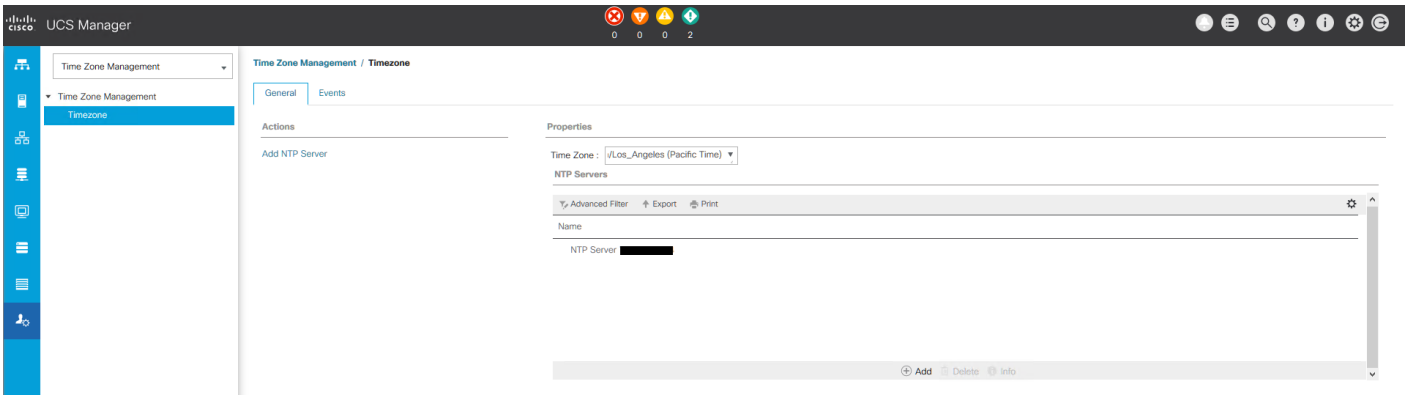


Deploy and Configure HyperFlex Data Platform

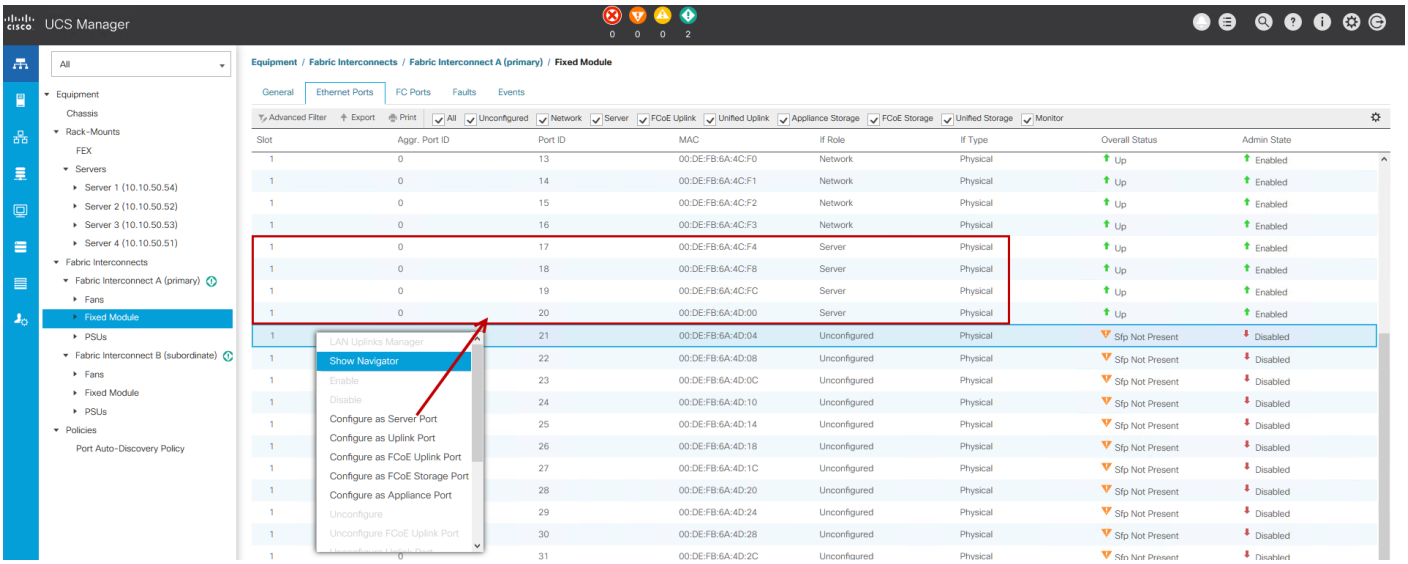
Prerequisites

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.

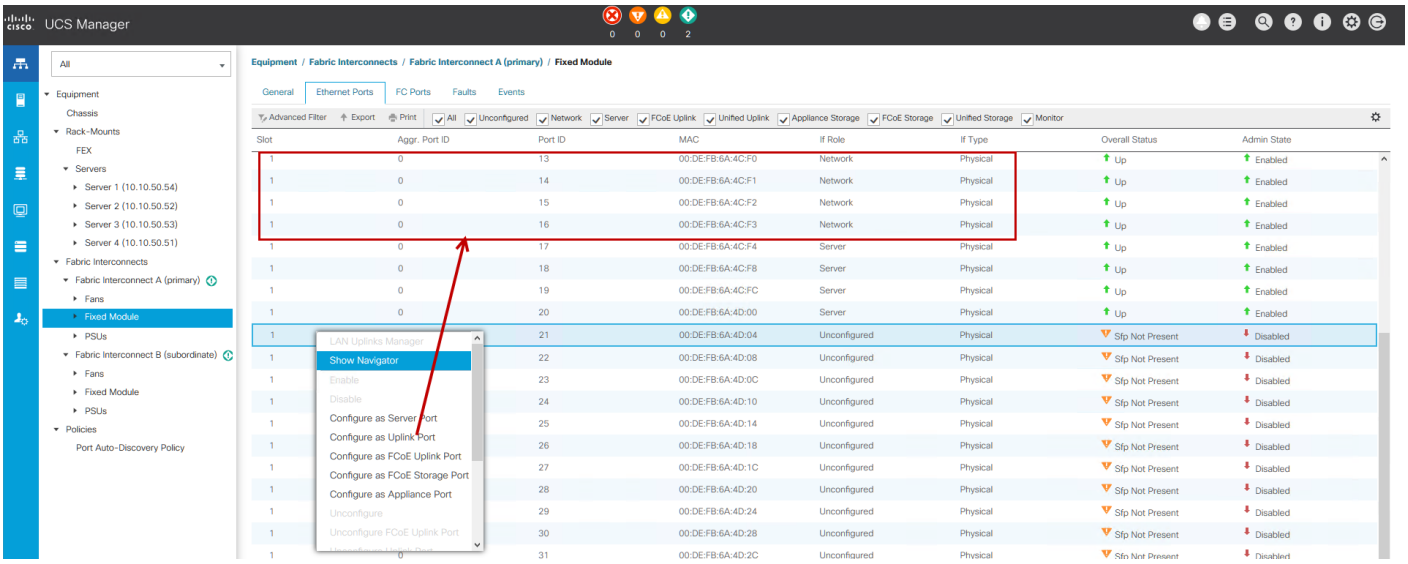


2. **Configure Server Ports:** Under the Equipment tab, Select Fabric A, select port to be configured as server port to manager HyperFlex rack server through Cisco UCS Manager.



3. Repeat this step to configure server port on Fabric B.

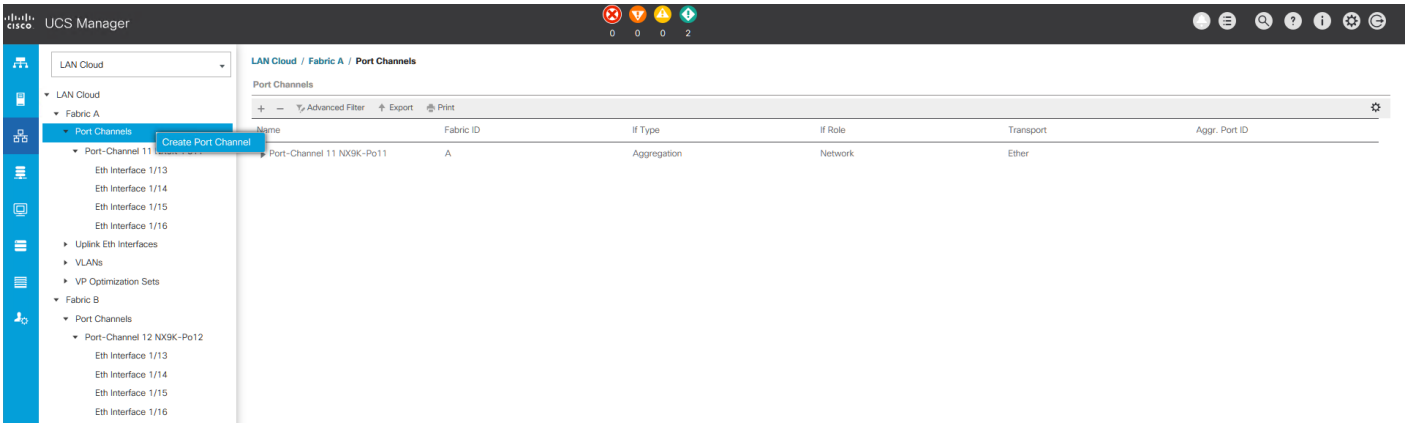
4. **Configure Uplink Ports:** On Fabric A, Select port to be configured as uplink port for network connectivity to north bound switch.



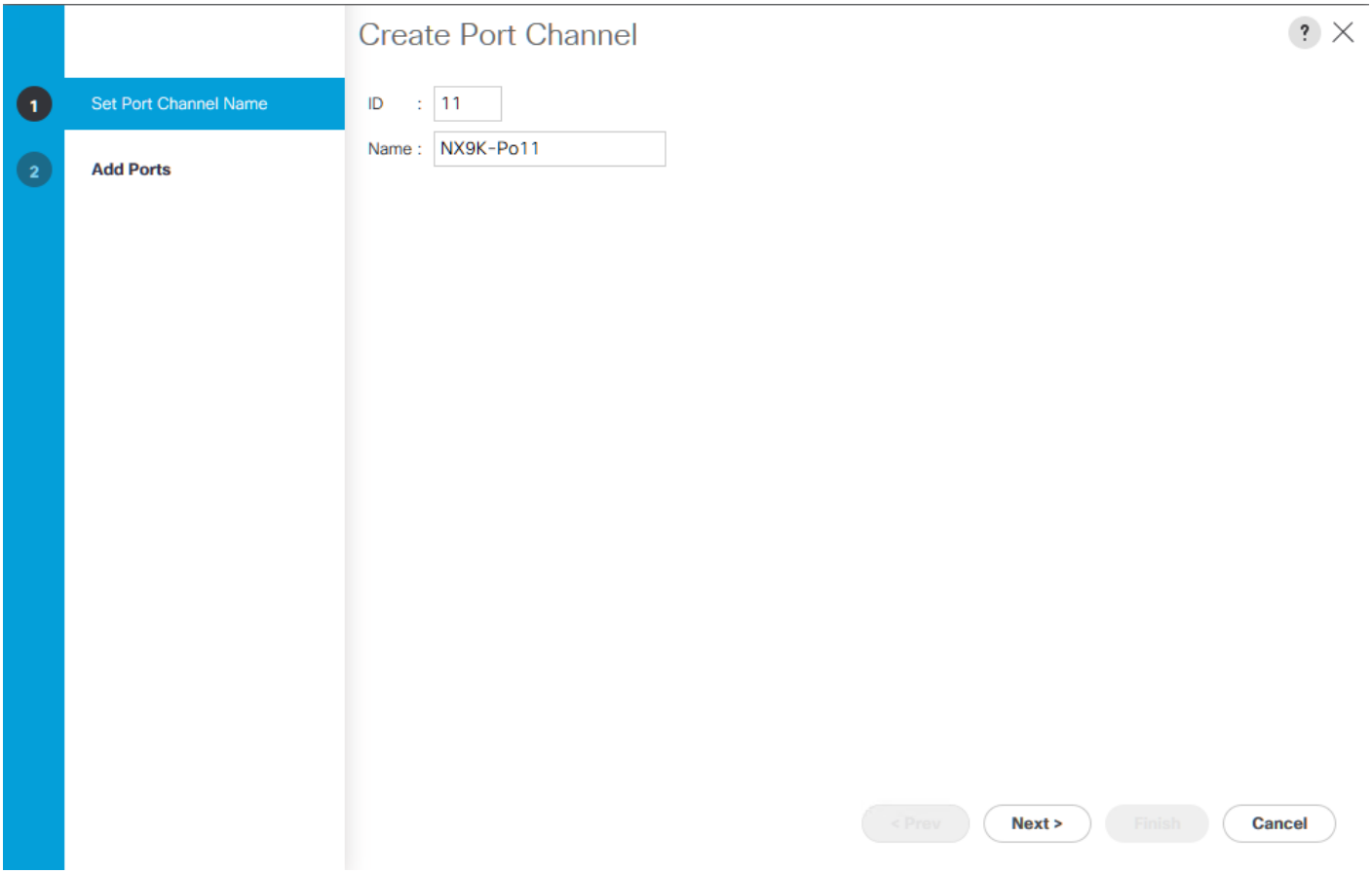
5. Repeat this same on Fabric B.

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 Cisco UCS best practice. For our reference architecture, we connected a pair of Nexus 93108YCPX switches.

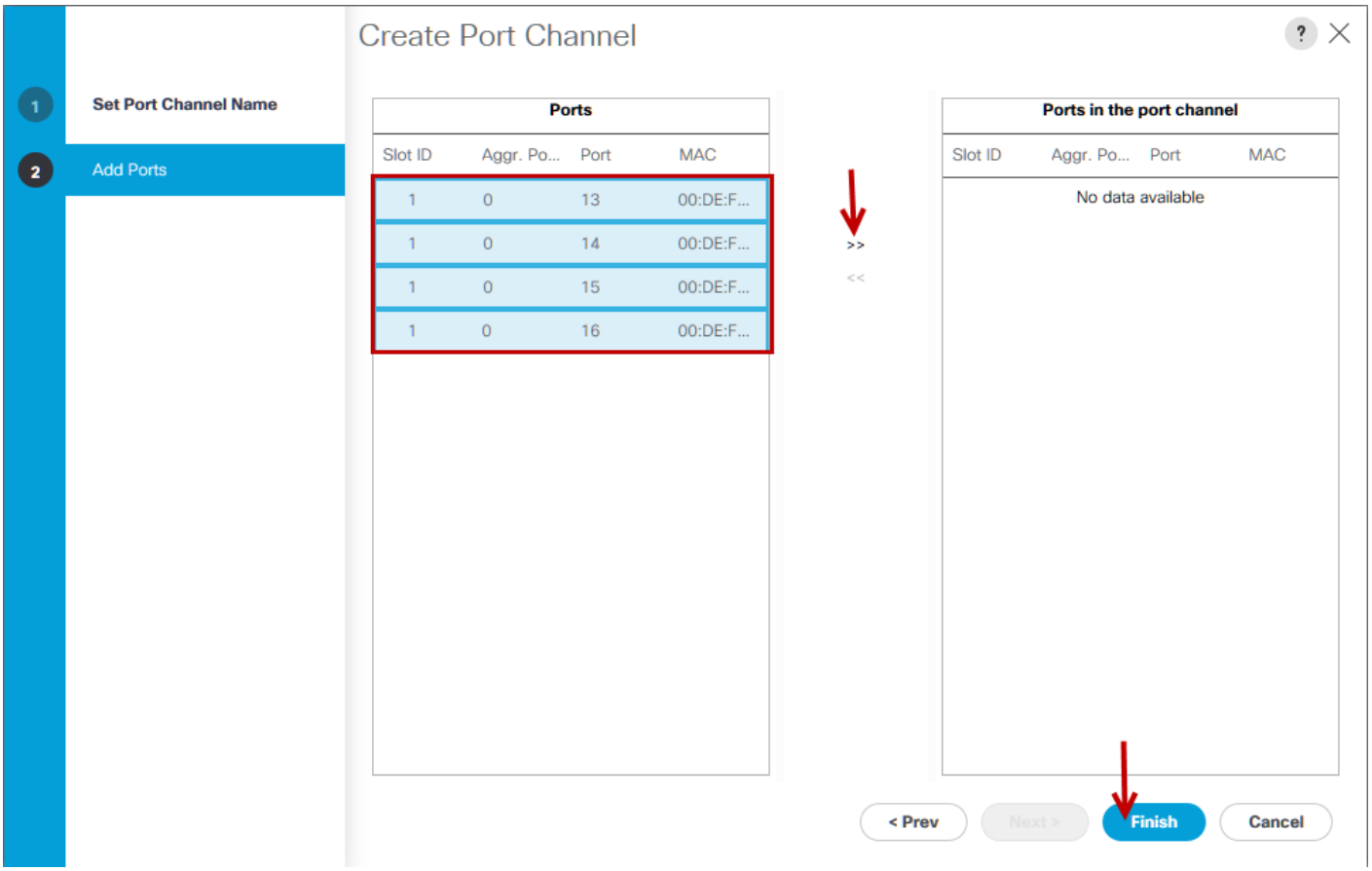


8. Enter port-channel ID number and name to be created, click Next.

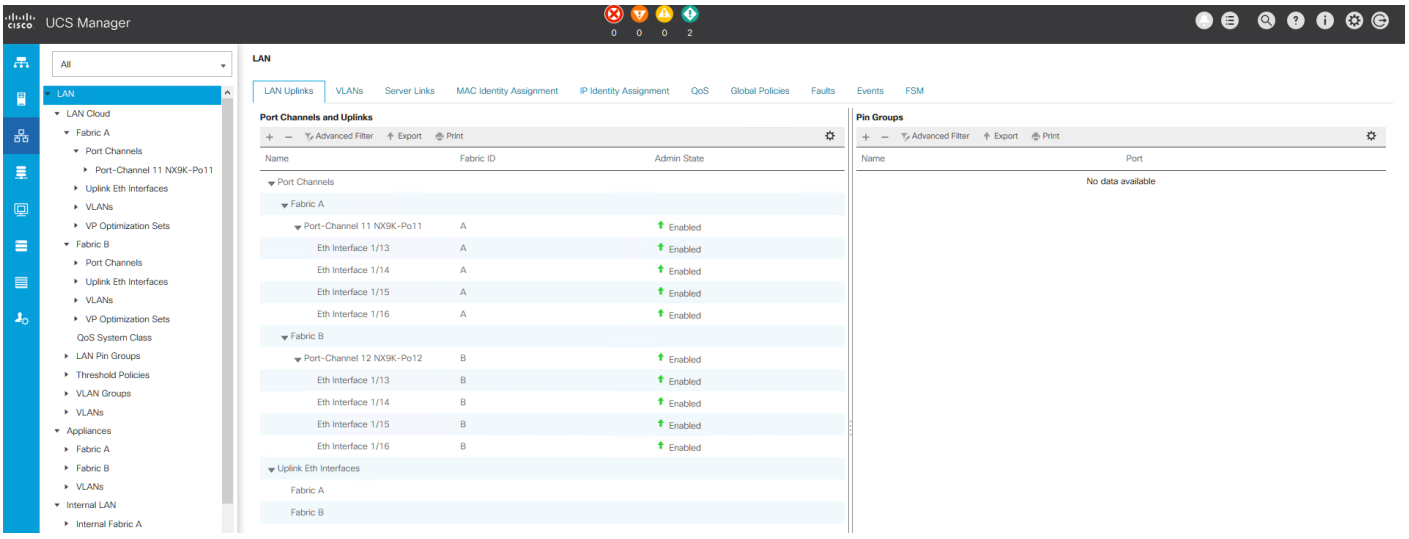


9. Select uplink ports to add as part of the port-channel.

10. Click Finish.



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

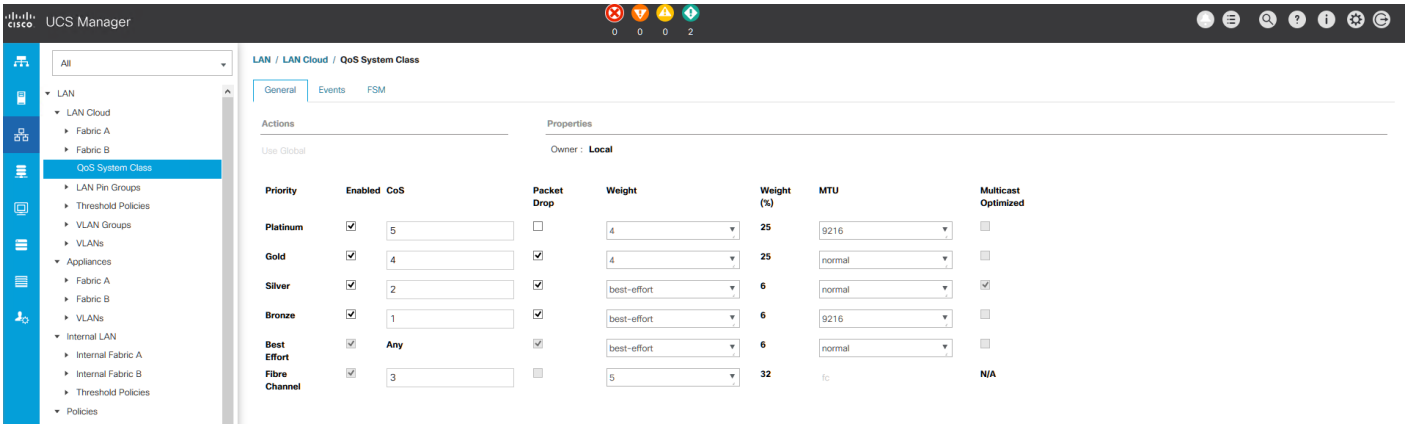


12. **Configure QoS System Classes:** From the LAN tab, below the Lan Cloud node, select QoS system class and configure the Platinum through Bronze system classes as shown in the following figure.

   – Set MTU to 9216 for Platinum (Storage data) and Bronze (vMotion)

   – Uncheck Enable Packet drop on the Platinum class

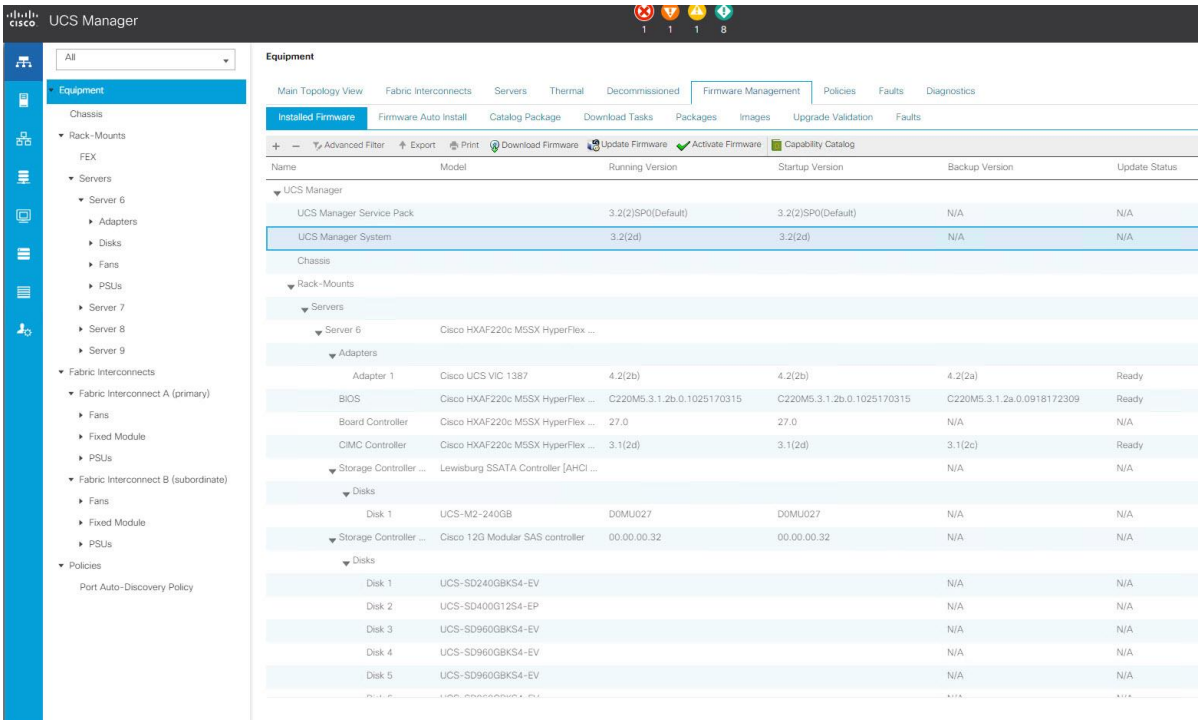
- Set Weight for Platinum and Gold priority class to 4 and everything else as best-effort.
- Enable multicast for silver class.



Changing QoS system class configuration on 6300 series Fabric Interconnect requires reboot of FIs.

13. **Verify UCS Manager Software Version:** In the Equipment tab, select Firmware Management > Installed Firmware.

14. Check and verify, both Fabric Interconnects and Cisco USC Manager are configure with Cisco UCS Manager v3.2.2d.



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 Cisco UCS Manager 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 the latest installer OVA from Cisco.com:

https://software.cisco.com/download/home/286305544/type/286305994/release/2.6%25281d%2529

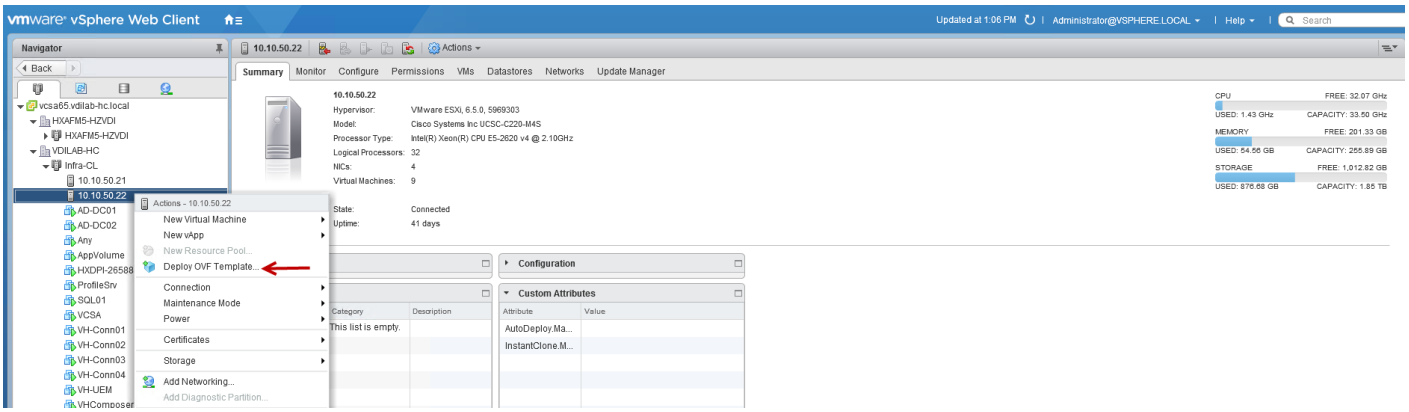
Deploy OVA to an existing host in the environment. Use either your existing vCenter Thick Client (C#) or vSphere Web Client to deploy OVA on ESXi host. This document outlines the procedure to deploy the OVA from the web client.

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: https://<FQDN or IP address for VC>:9443/vcenter-client.

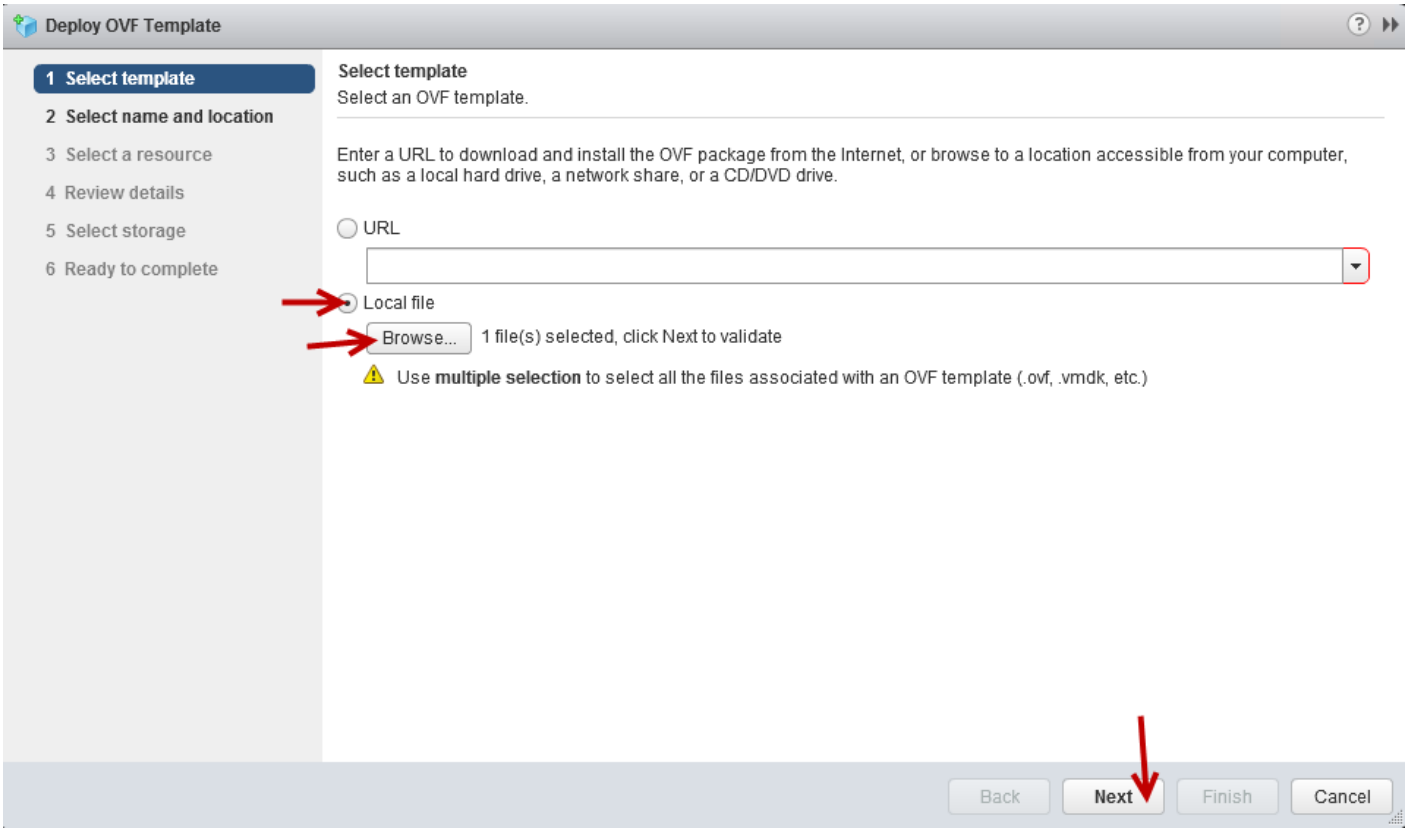
2. Select ESXi host under hosts and cluster when HyperFlex data platform installer VM to deploy.

3. Right-click ESXi host, select Deploy OVF Template.

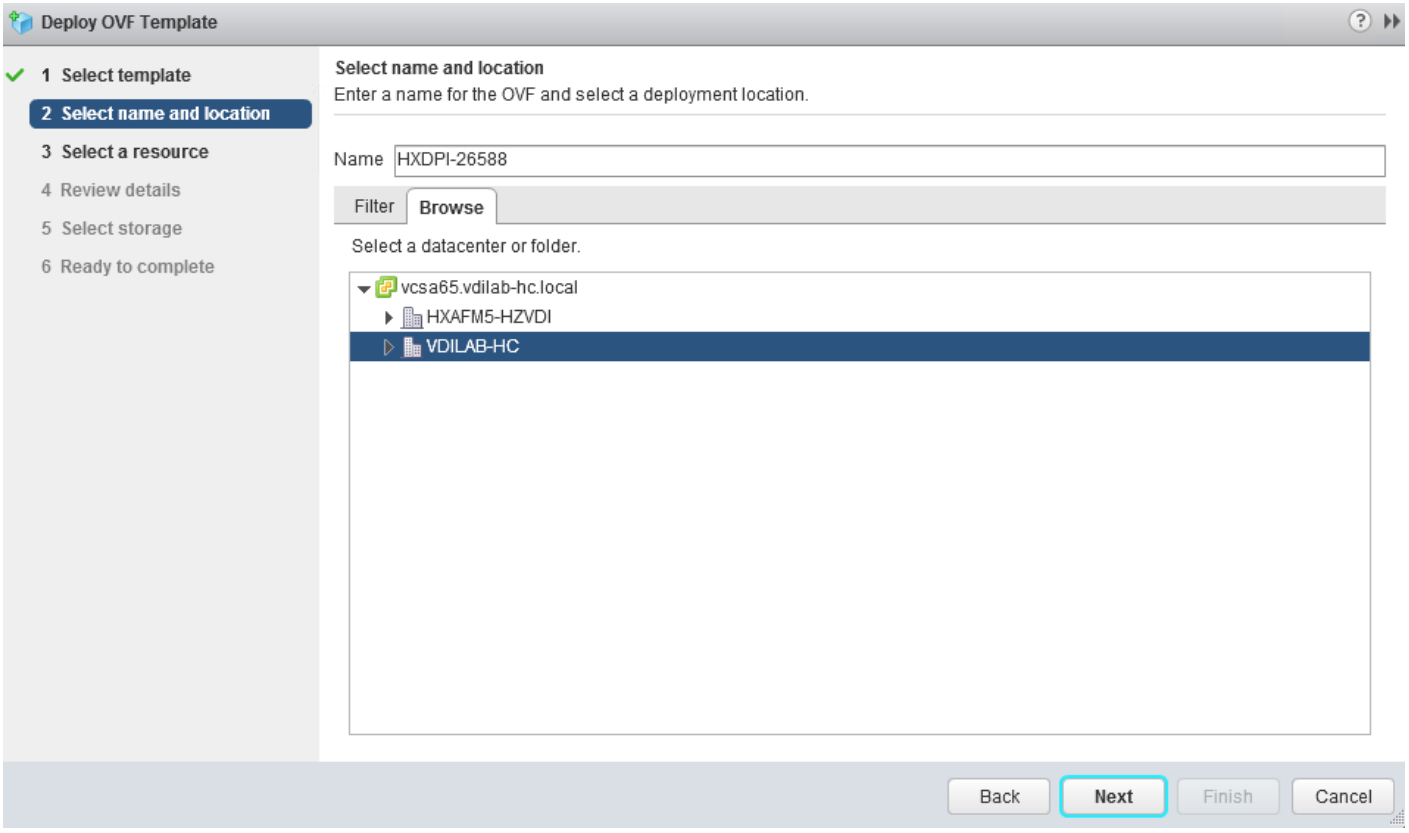


4. Follow the deployment steps to configure HyperFlex data-platform installer VM deployment.

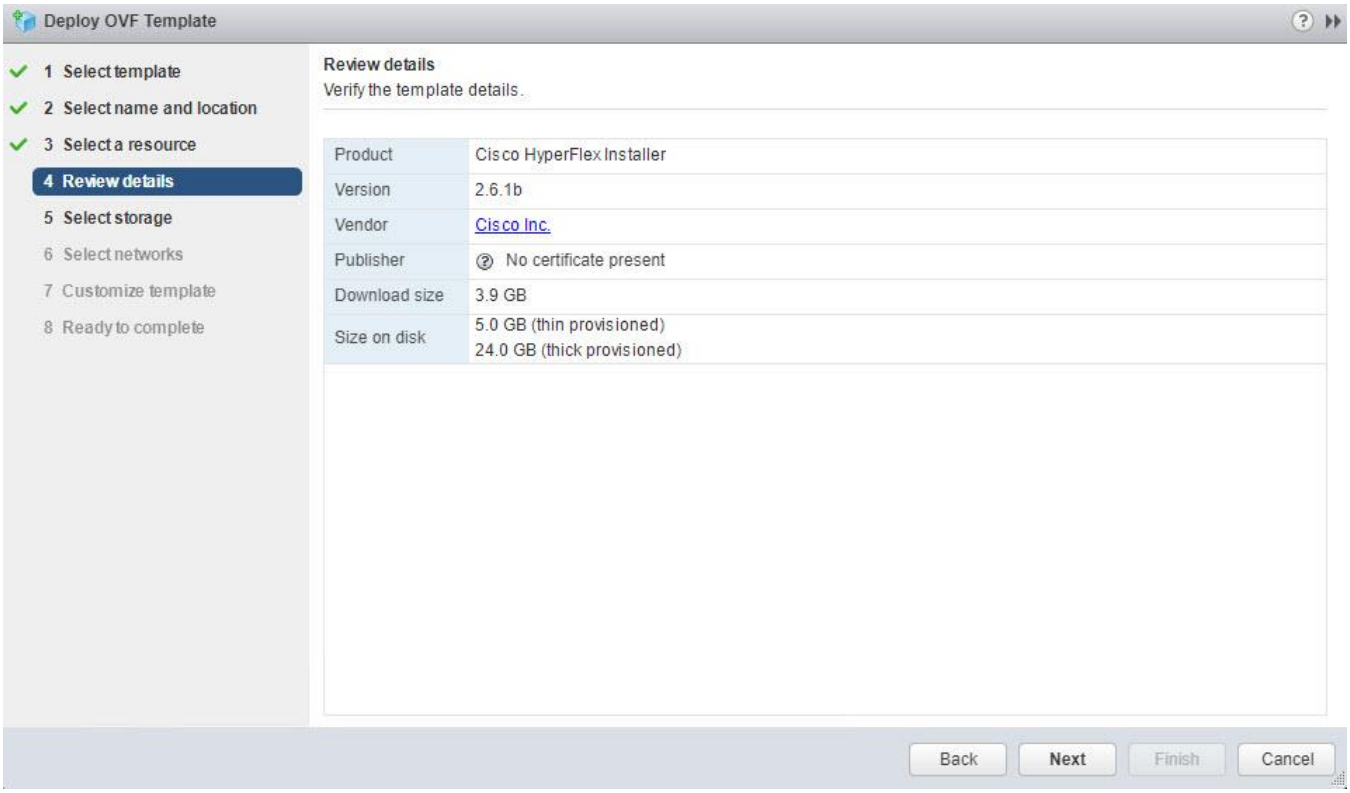
5. Select OVA file to deploy, click Next.



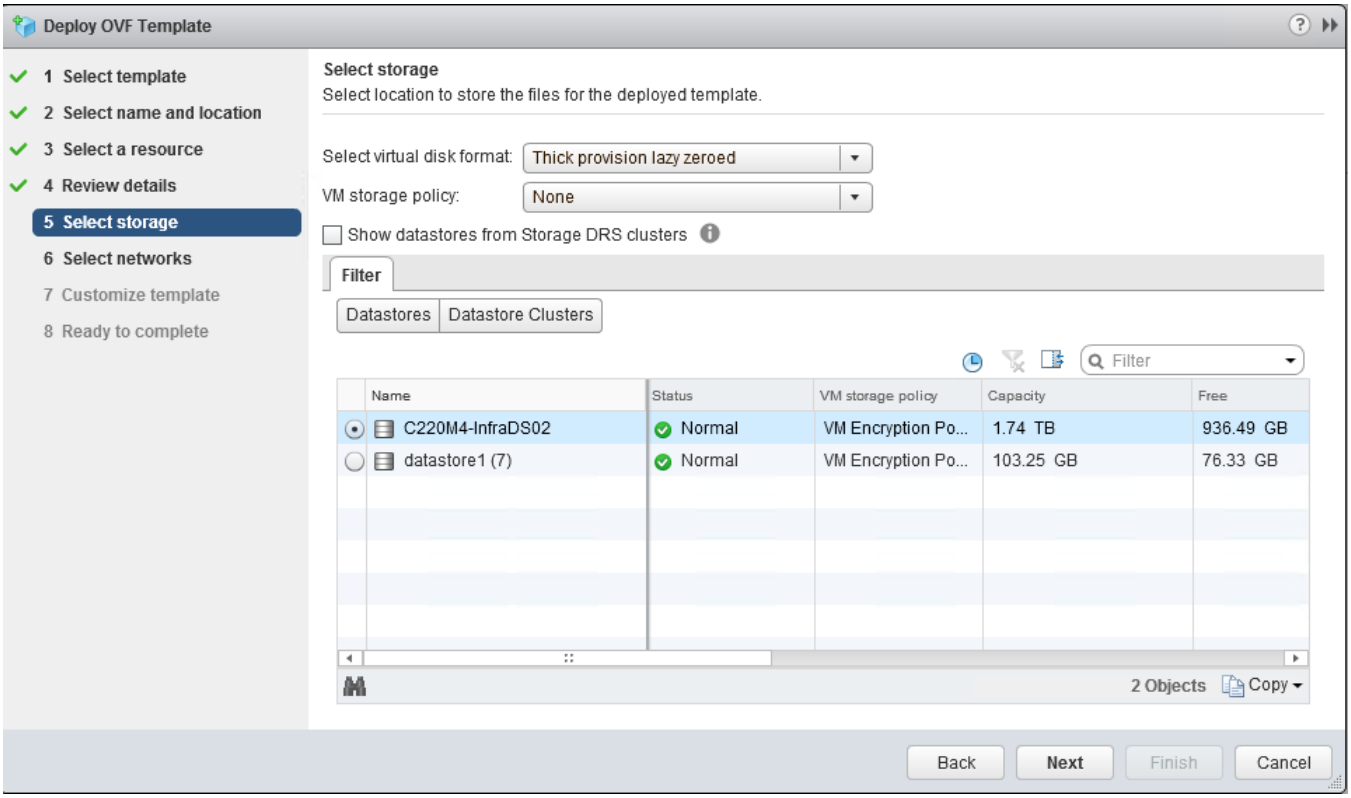
6. Enter name for OVF to template deploy, select datacenter and folder location. Click Next.



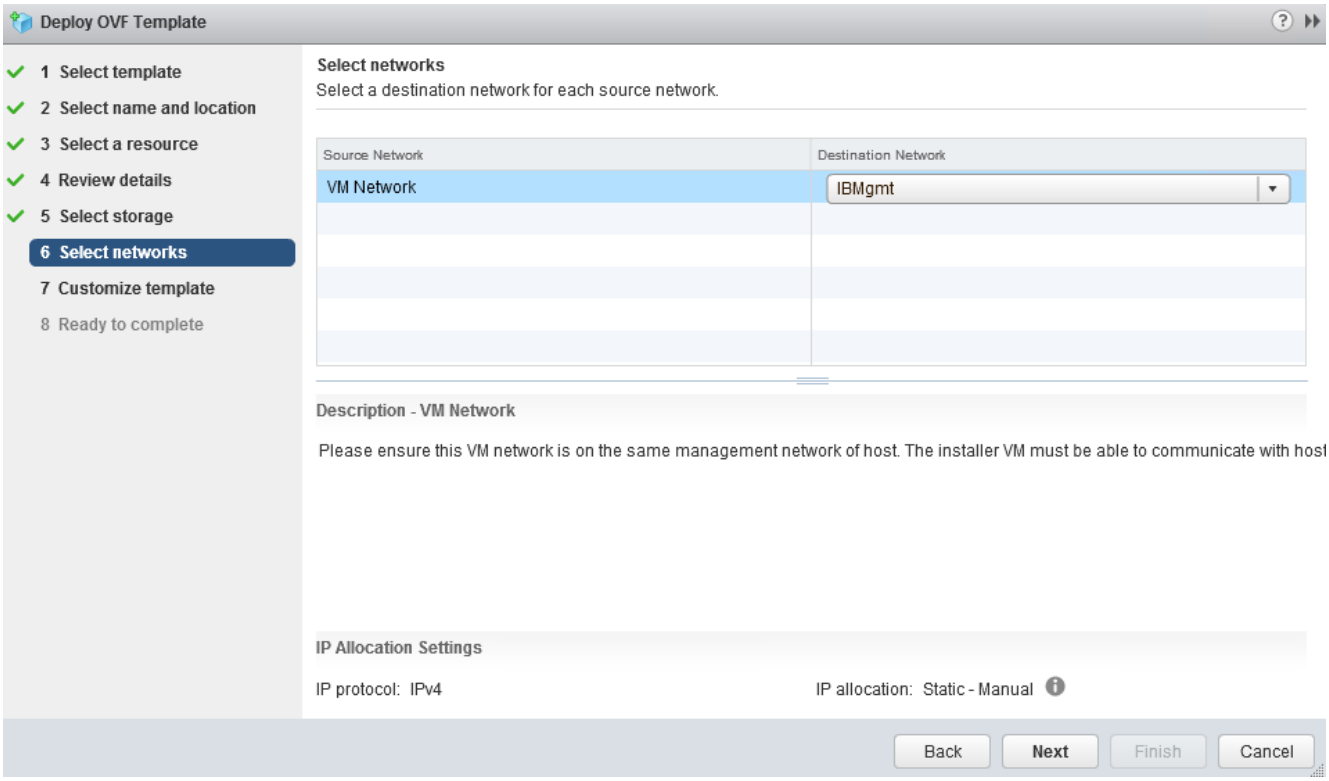
7. Review and verify the details for OVF template to deploy, click Next.



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

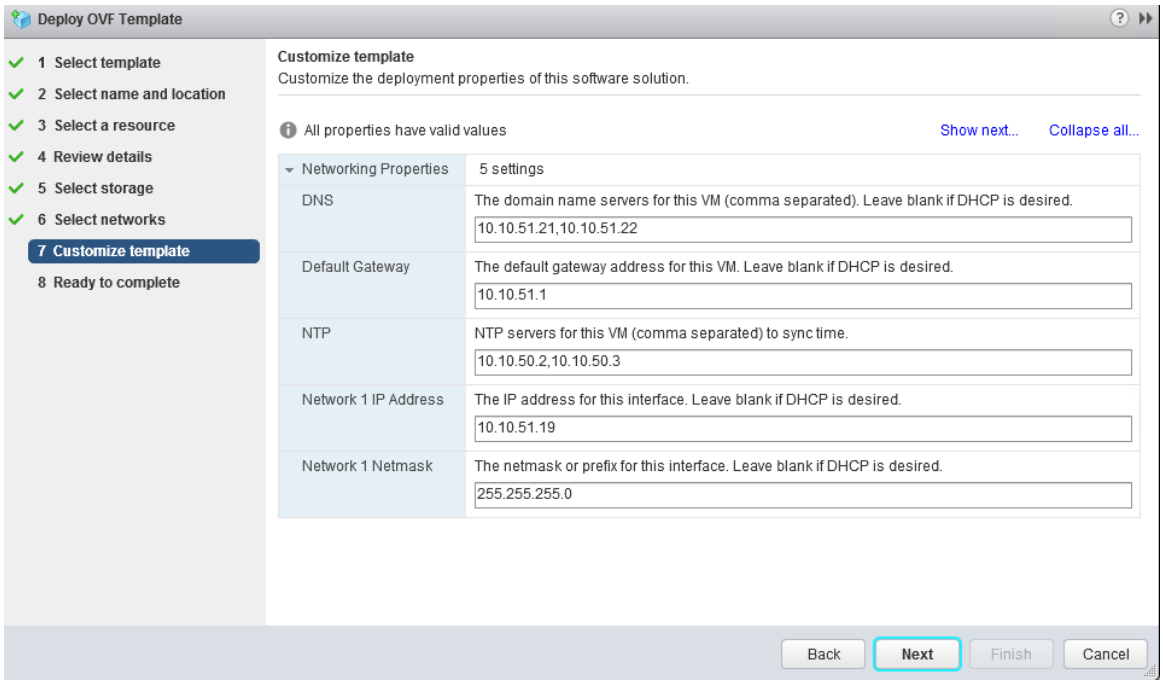


9. Select Network adapter destination port-group.

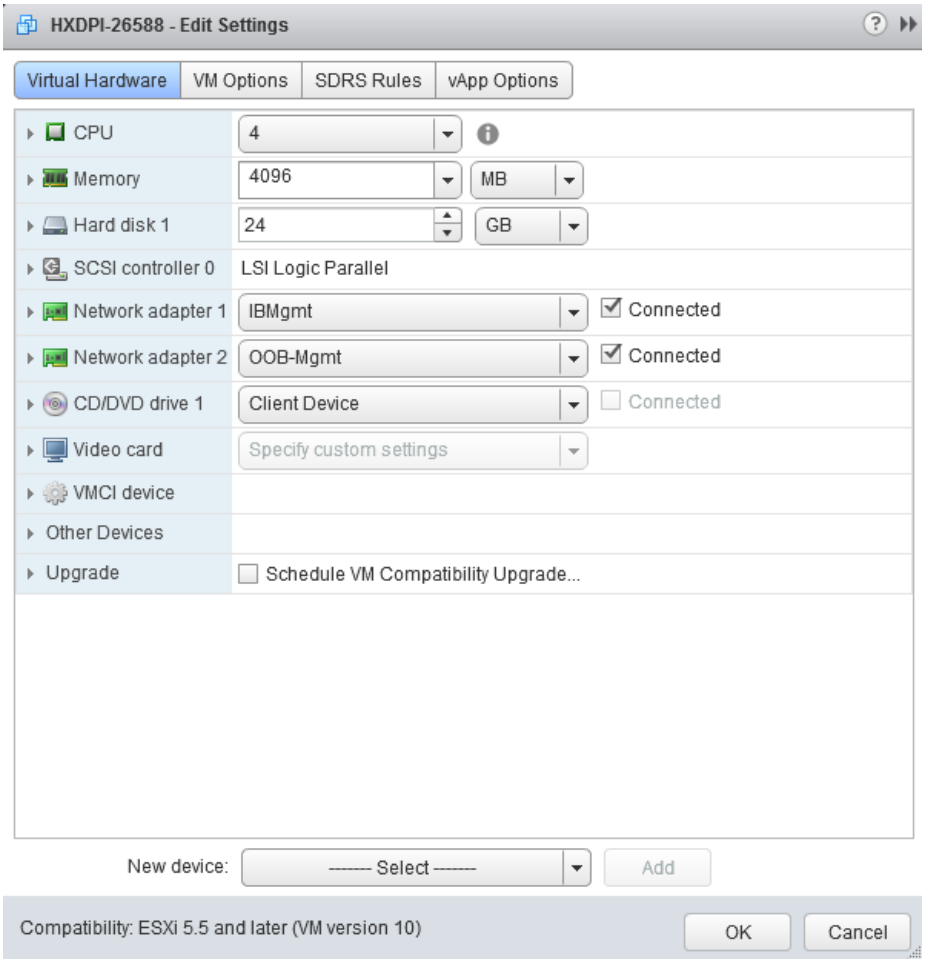


10. Fill out the parameters requested for hostname, gateway, DNS, IP address, and netmask. Alternatively, leave all blank for a DHCP assigned address.

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.



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 the screenshot below:

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

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

Verify or Set DNS Resolution

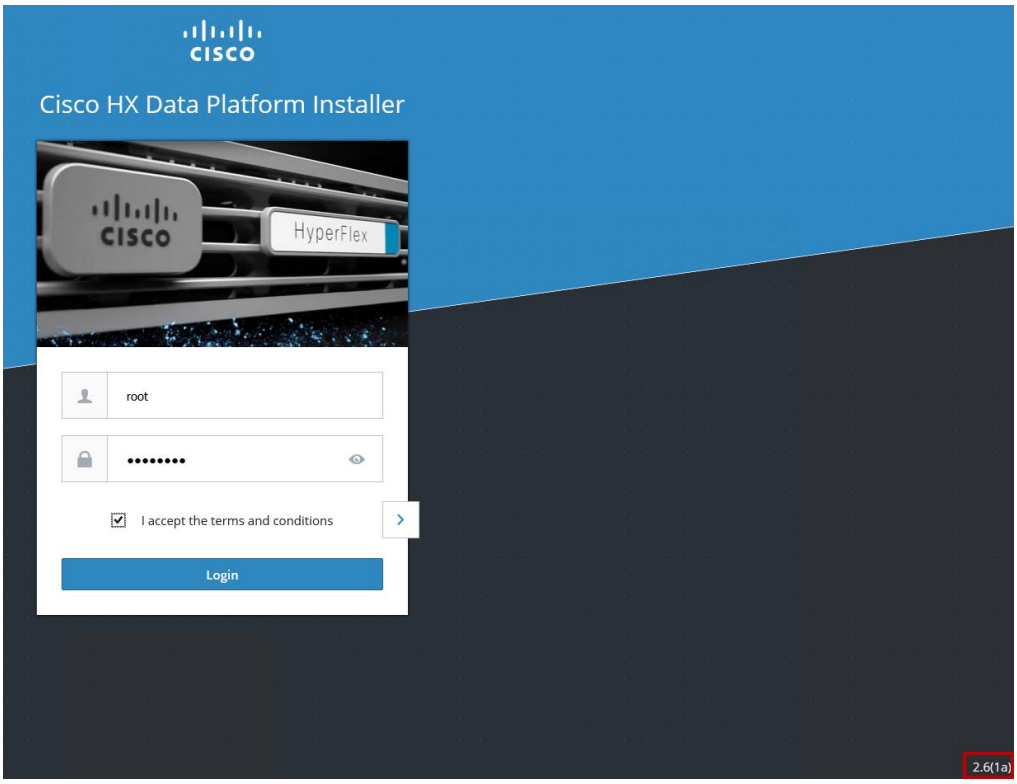
SSH to HX installer VM, verify or set DNS resolution is set on HyperFlex Installer VM:

```
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 configure the Cisco HyperFlex Cluster, complete the following steps:

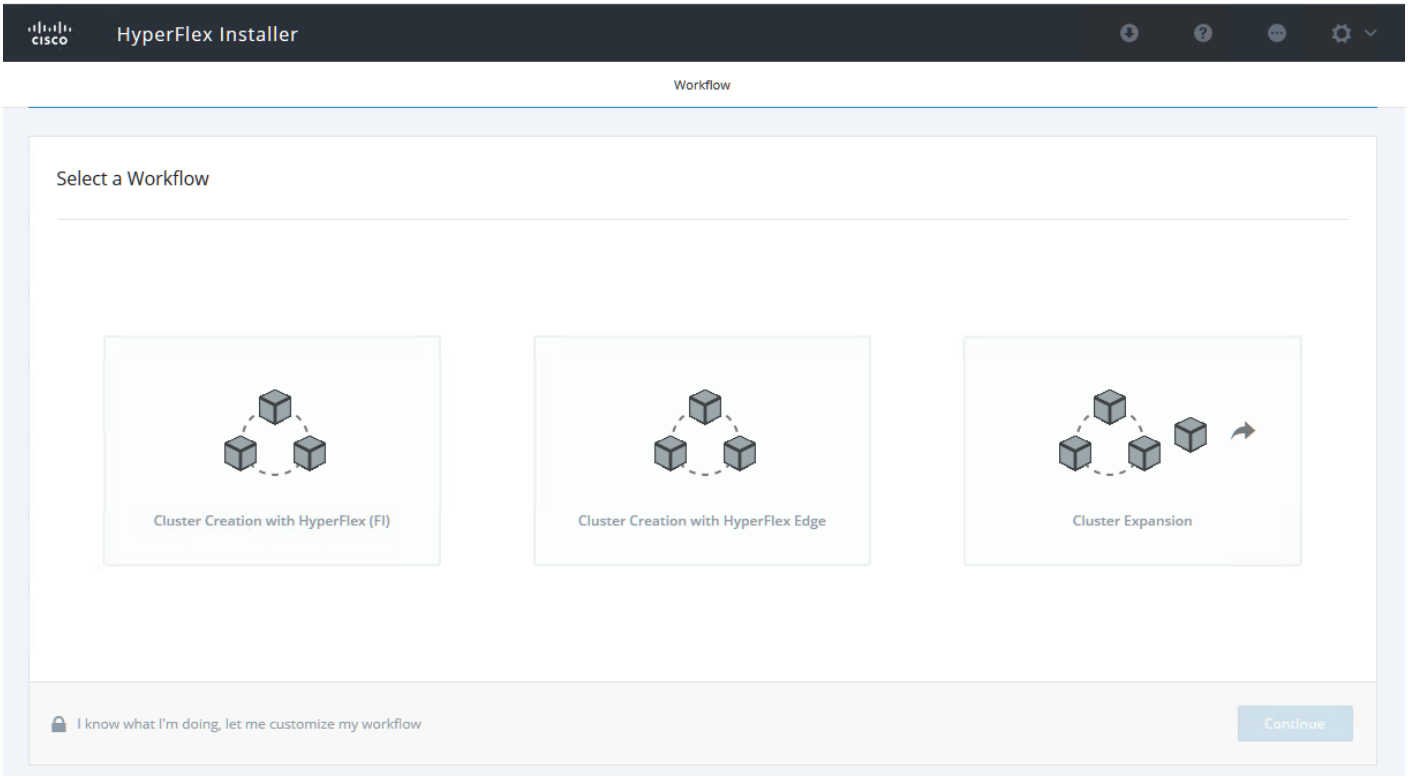
1. Login to HX Installer VM through a web browser: http://<Installer_VM_IP_Address>



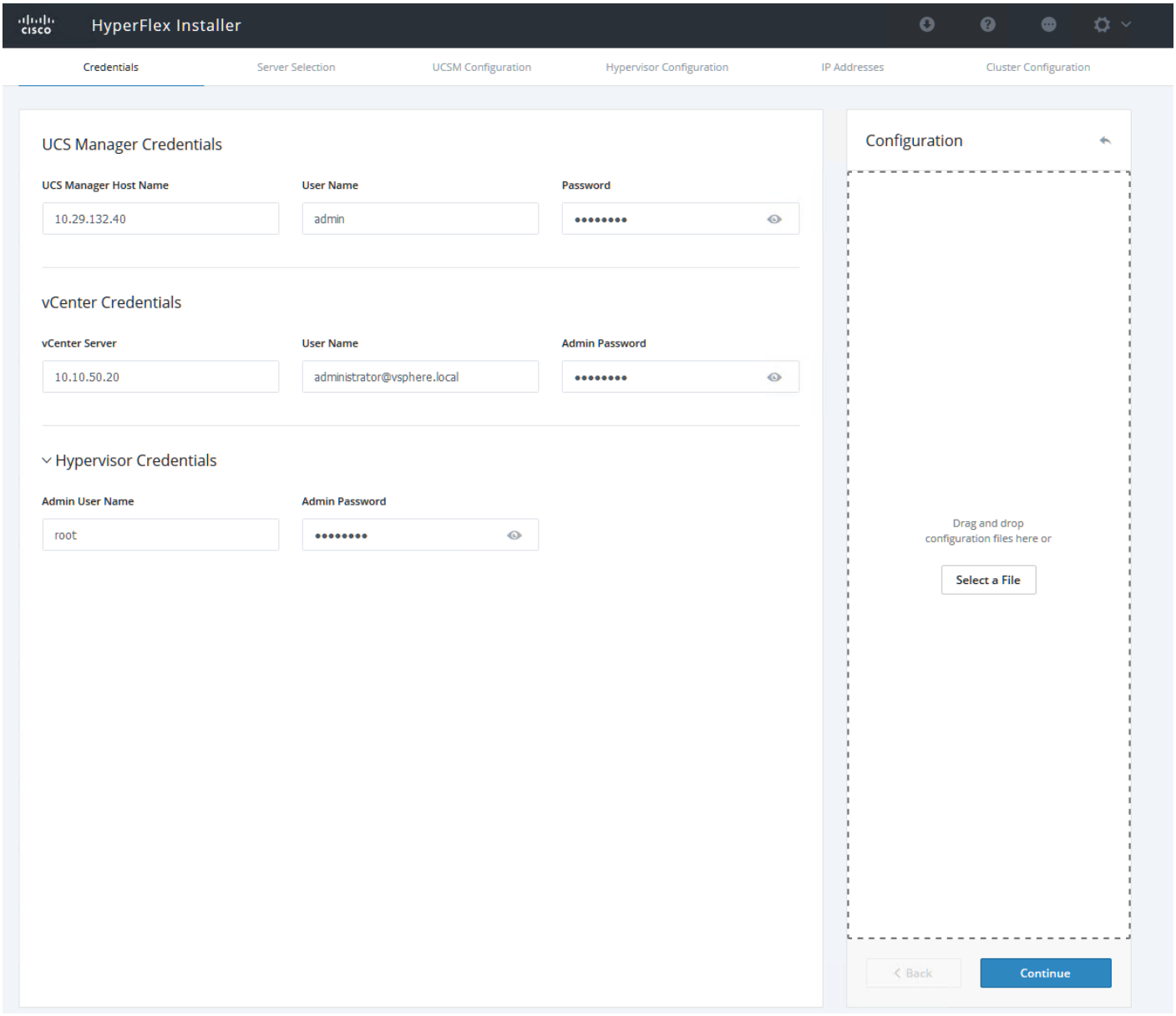
Create a HyperFlex Cluster

To create a HyperFlex Cluster, complete the following steps:

1. Select the workflow for cluster creation to deploy a new HyperFlex cluster on sixteen Cisco HXAF220c-M5S nodes.

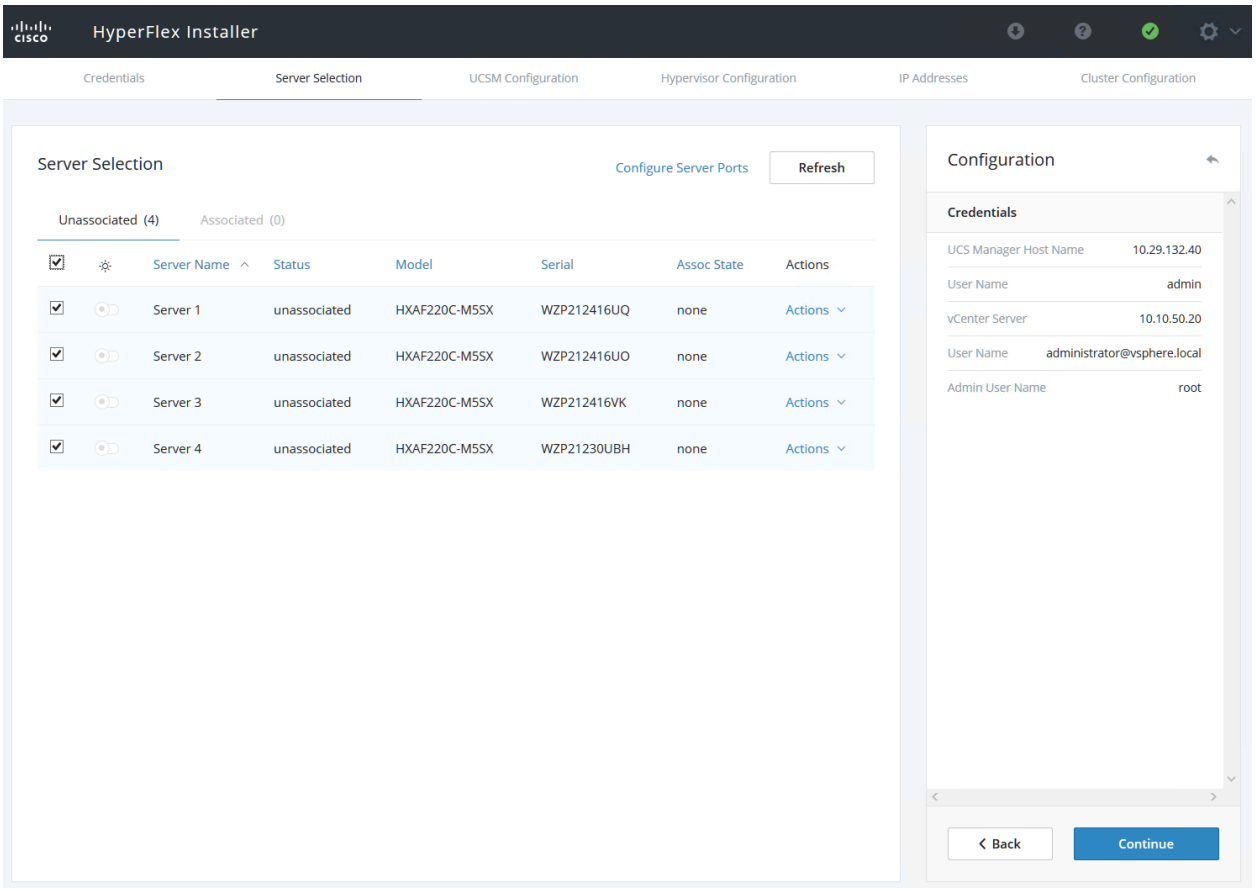


2. On the credentials page, enter the access details for Cisco UCS Manager, vCenter server, and Hypervisor. Click Continue.



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 checkbox for individual servers.)

4. Click Continue after completing server selection.



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.

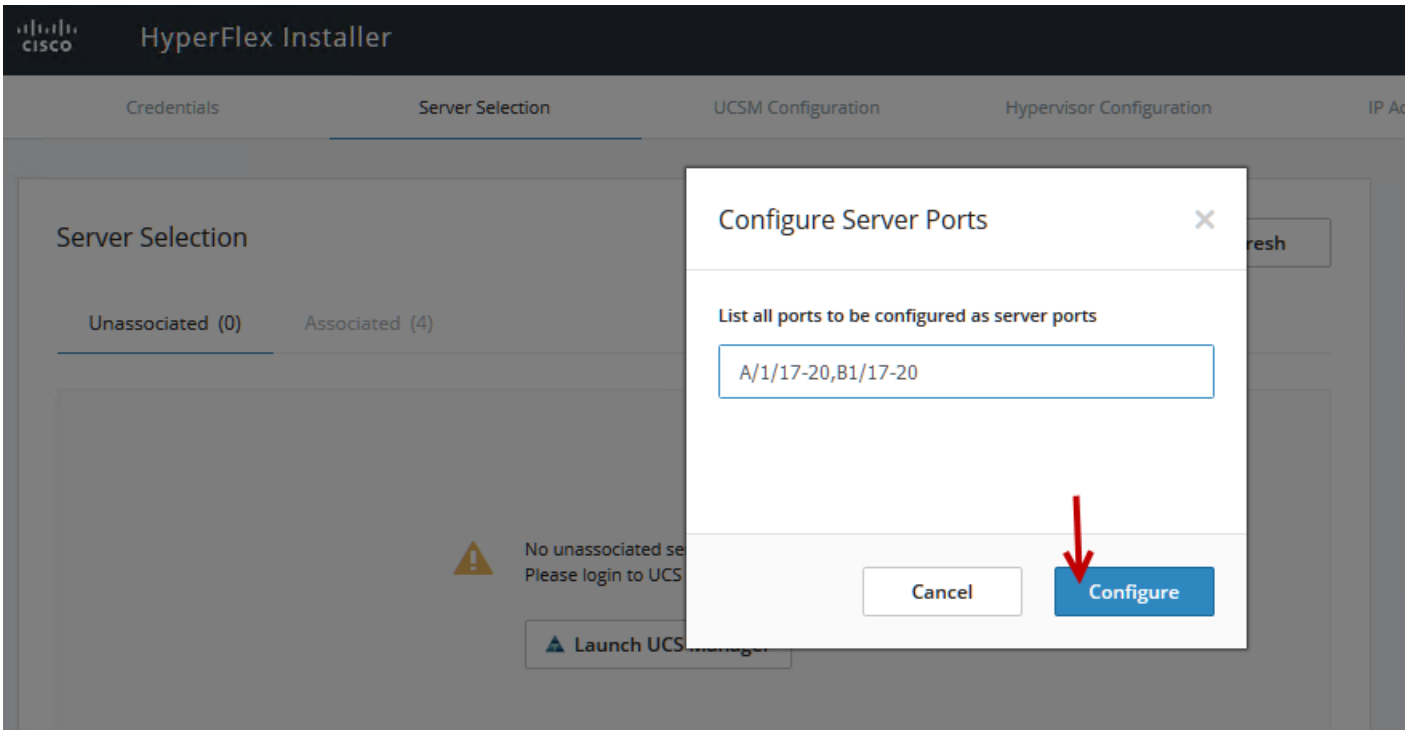
Configure Server Ports (Optional)

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.



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

   a. Enter VLAN ID for hx-inband-mgmt, hx-storage-data, hx-vmotion, vm-network.

   b. MAC Pool Prefix: The prefix to use for each HX MAC address pool. Please select a prefix that does not conflict with any other MAC address pool across all Cisco UCS domains.

   c. The blocks in the MAC address pool will have the following format:

      – ${prefix}:${fabric_id}${vnic_id}:{service_profile_id}

      – The first three bytes should always be “00:25:B5”.

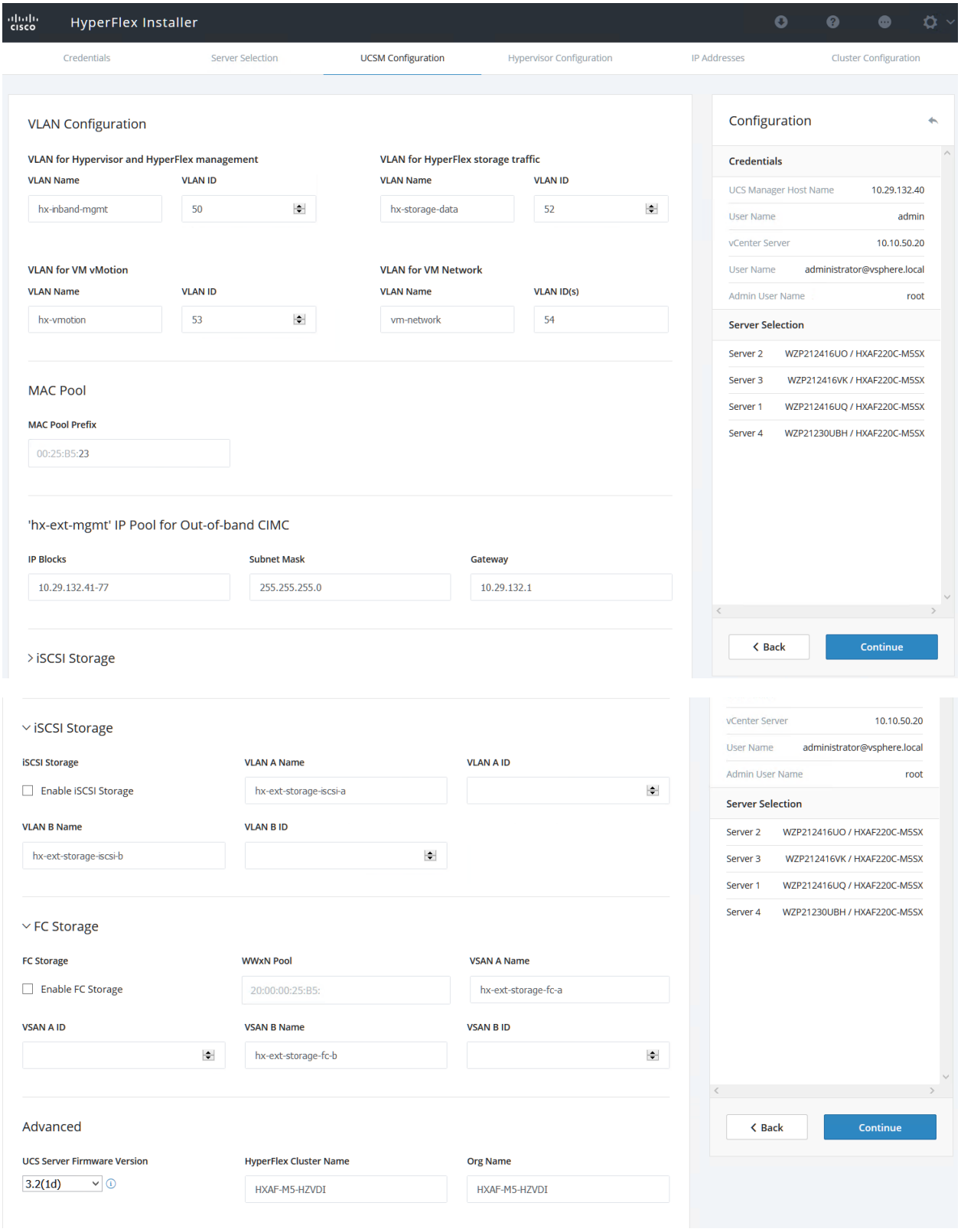
5. Enter range of IP address to create a block of IP addresses for external management and access to CIMC/KVM.

6. Cisco UCS firmware version is set to 3.2(2d) which is the required Cisco UCS Manager release for HyperFlex v2.6.1b installation.

7. Enter HyperFlex cluster name.

8. Enter Org name to be created in Cisco UCS Manager.

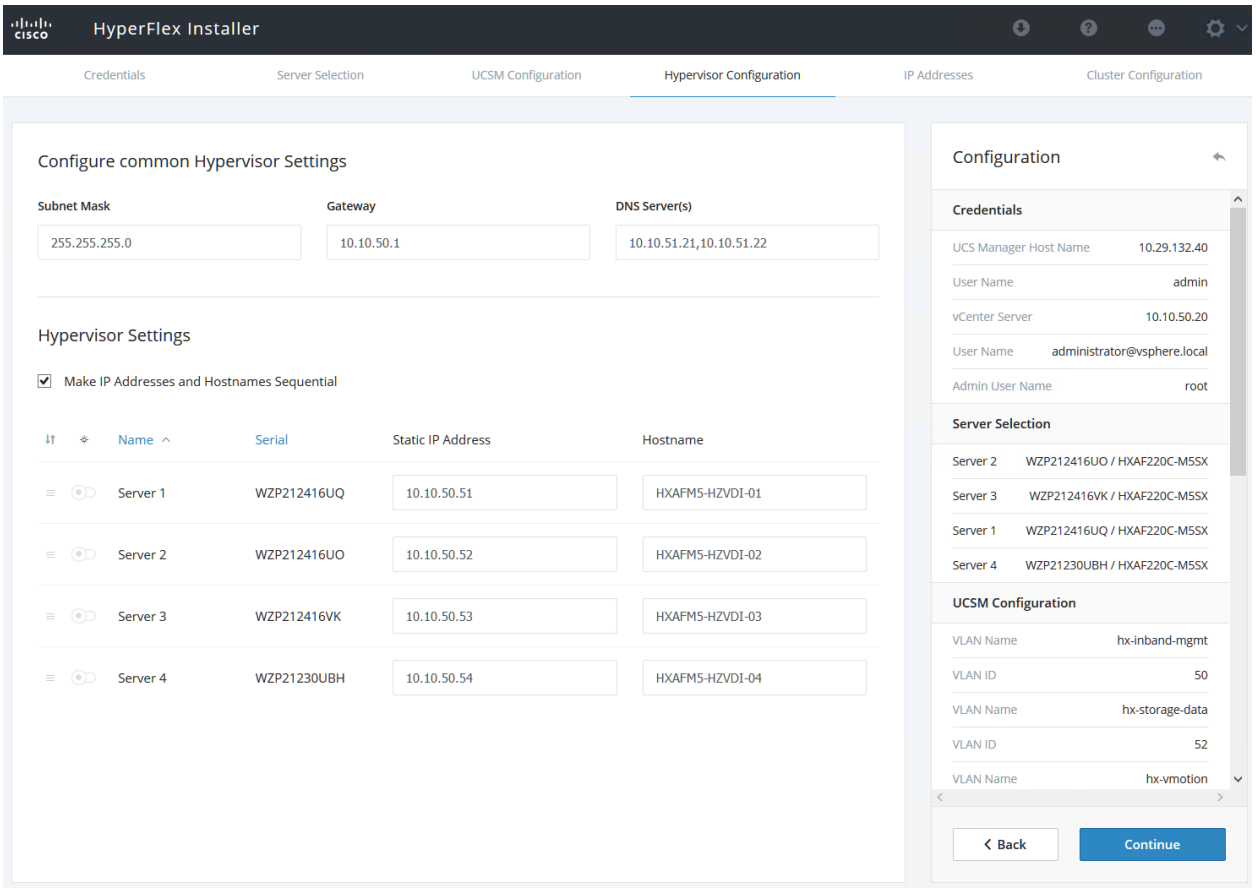
9. Click Continue.



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.



IP Addresses

To add the IP addresses, complete the following steps:

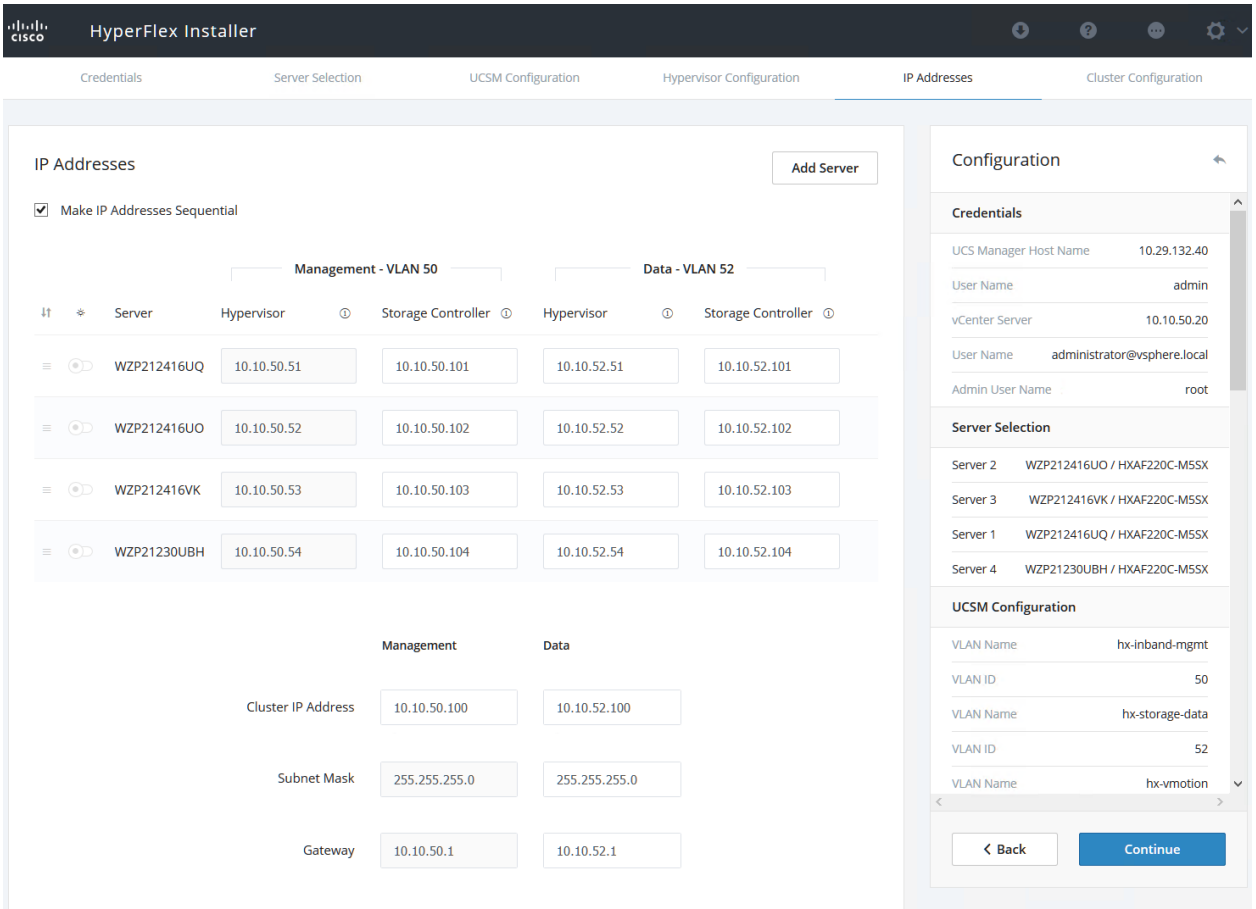
When the IP Addresses page appears, the hypervisor IP address for each node that was configured in the Hypervisor Configuration tab, appears under the Management Hypervisor column.

Three additional columns appear on this page:

- Storage Controller/Management
- Hypervisor/Data
- Storage Controller/Data

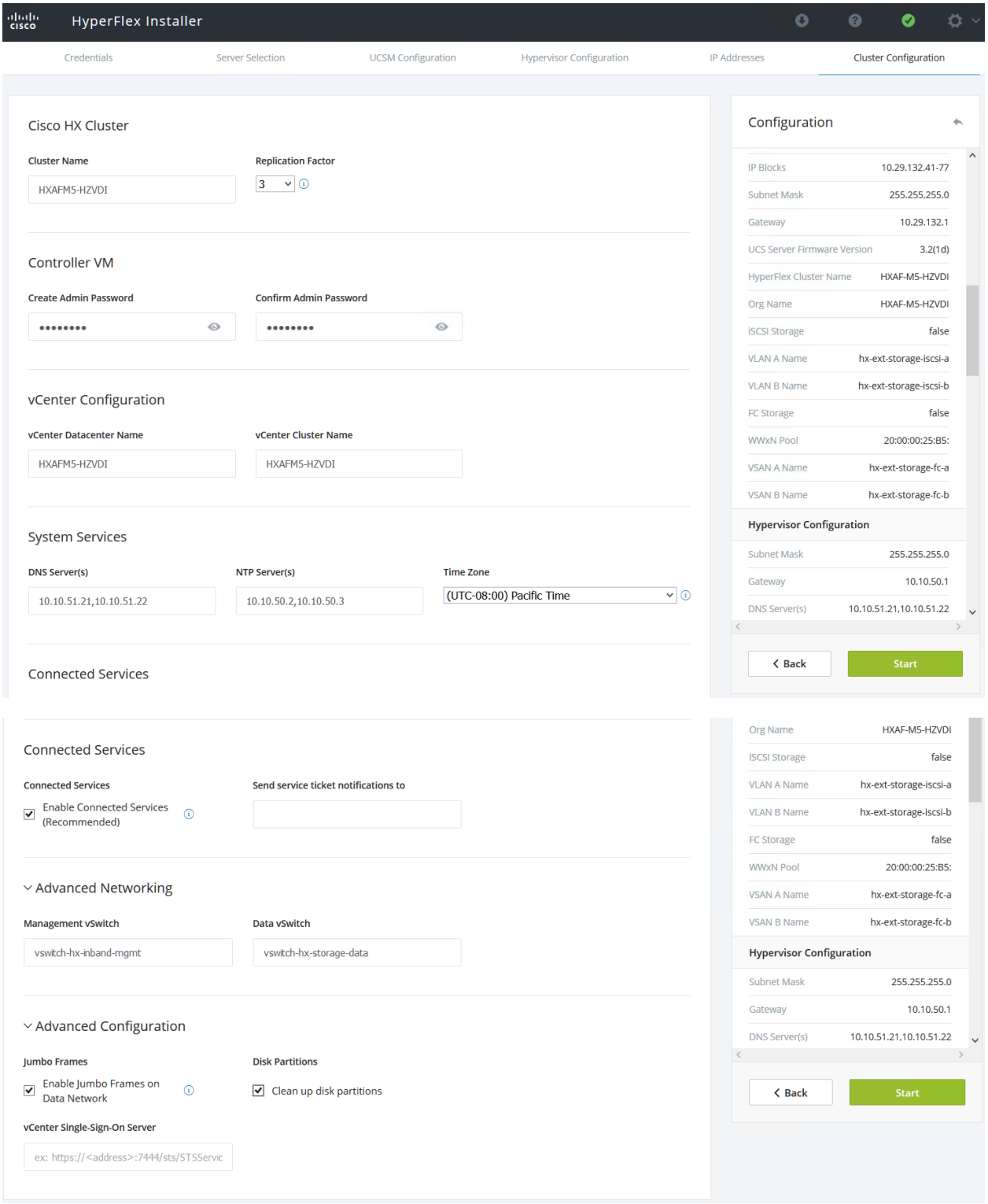
The Data network IP addresses are for vmkernel addresses for storage access by the hypervisor and storage controller virtual machine.

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.



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

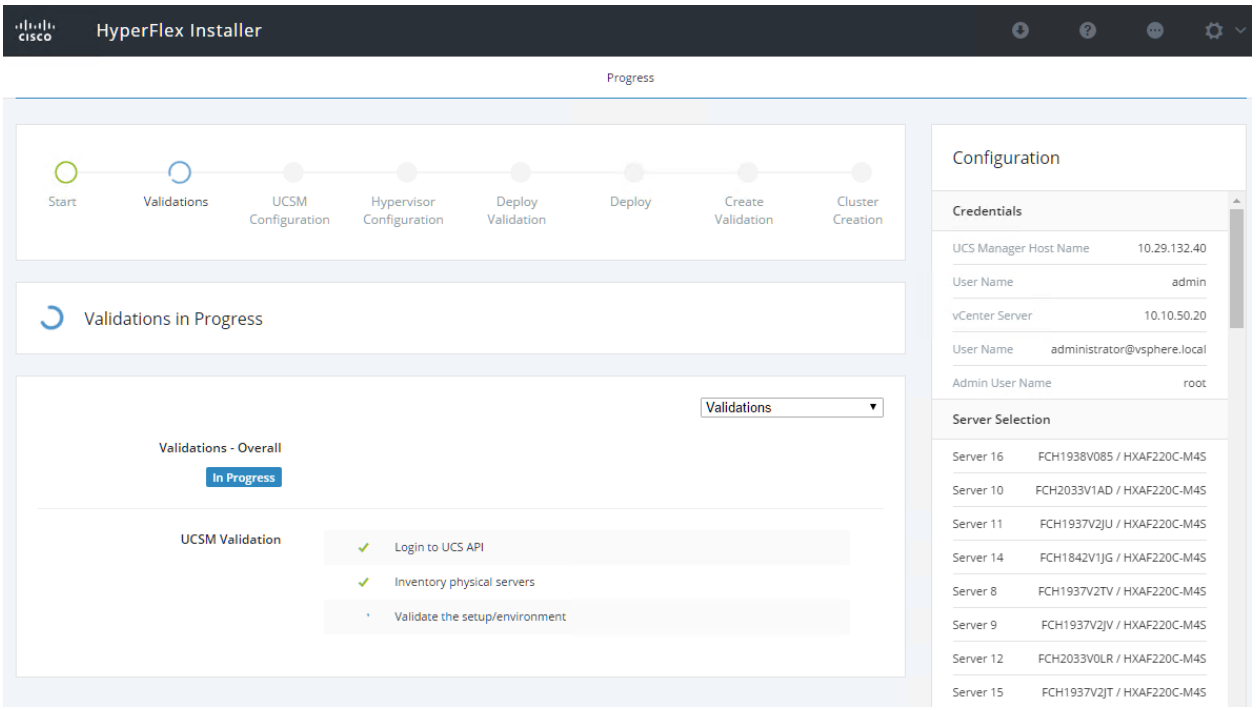


5. The configuration details can be exported to a JSON file by clicking the down arrow icon in the top right corner of the Web browser page as shown in the screenshot below.

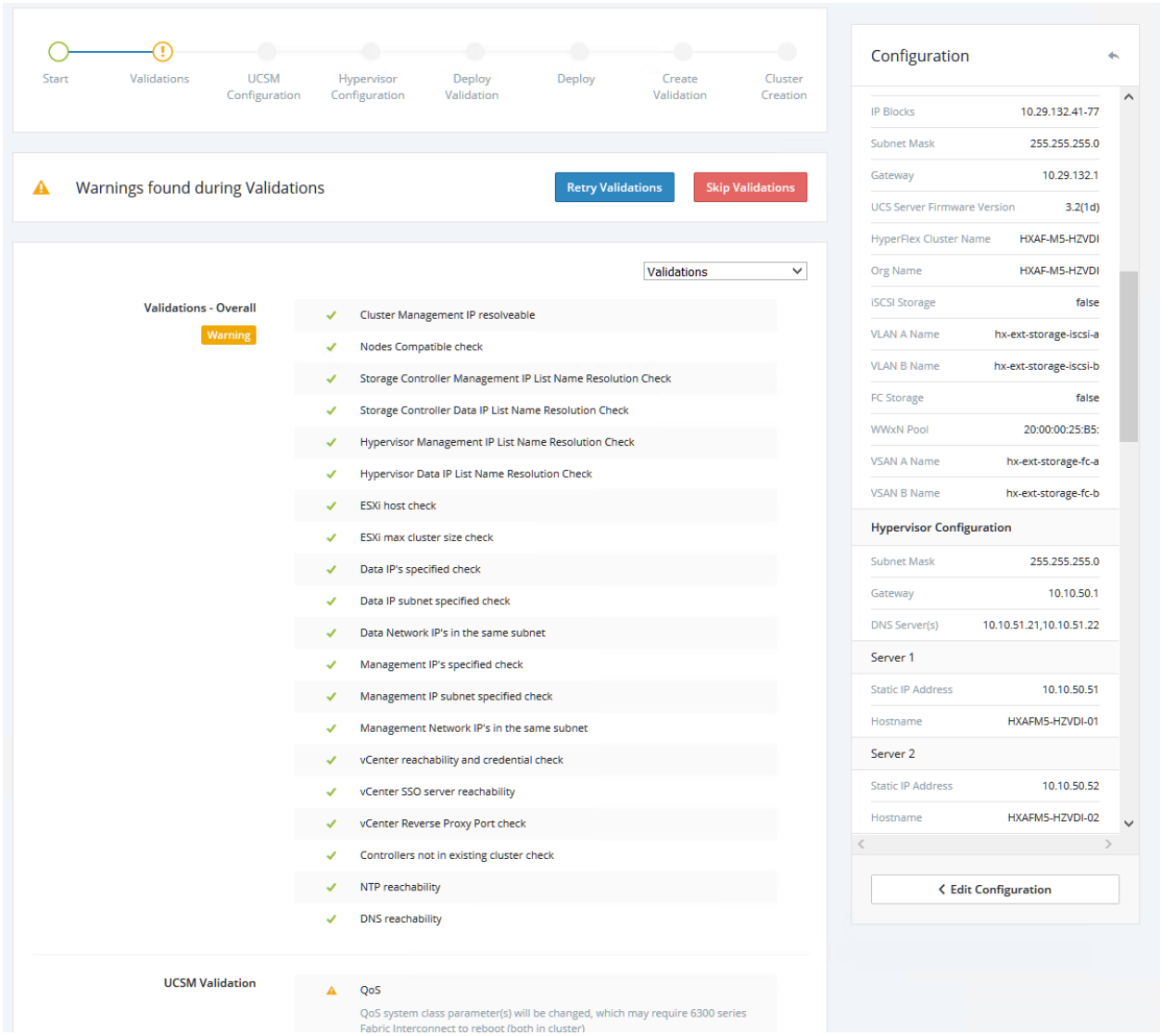
6. Configuration details can be reviewed on Configuration page on right side section. Verify entered details for IP address entered in Credentials page, server selection for cluster deployment and creation workflow, Cisco UCS Manager configuration, Hypervisor Configuration, IP addresses.

7. Click Start after verifying details.

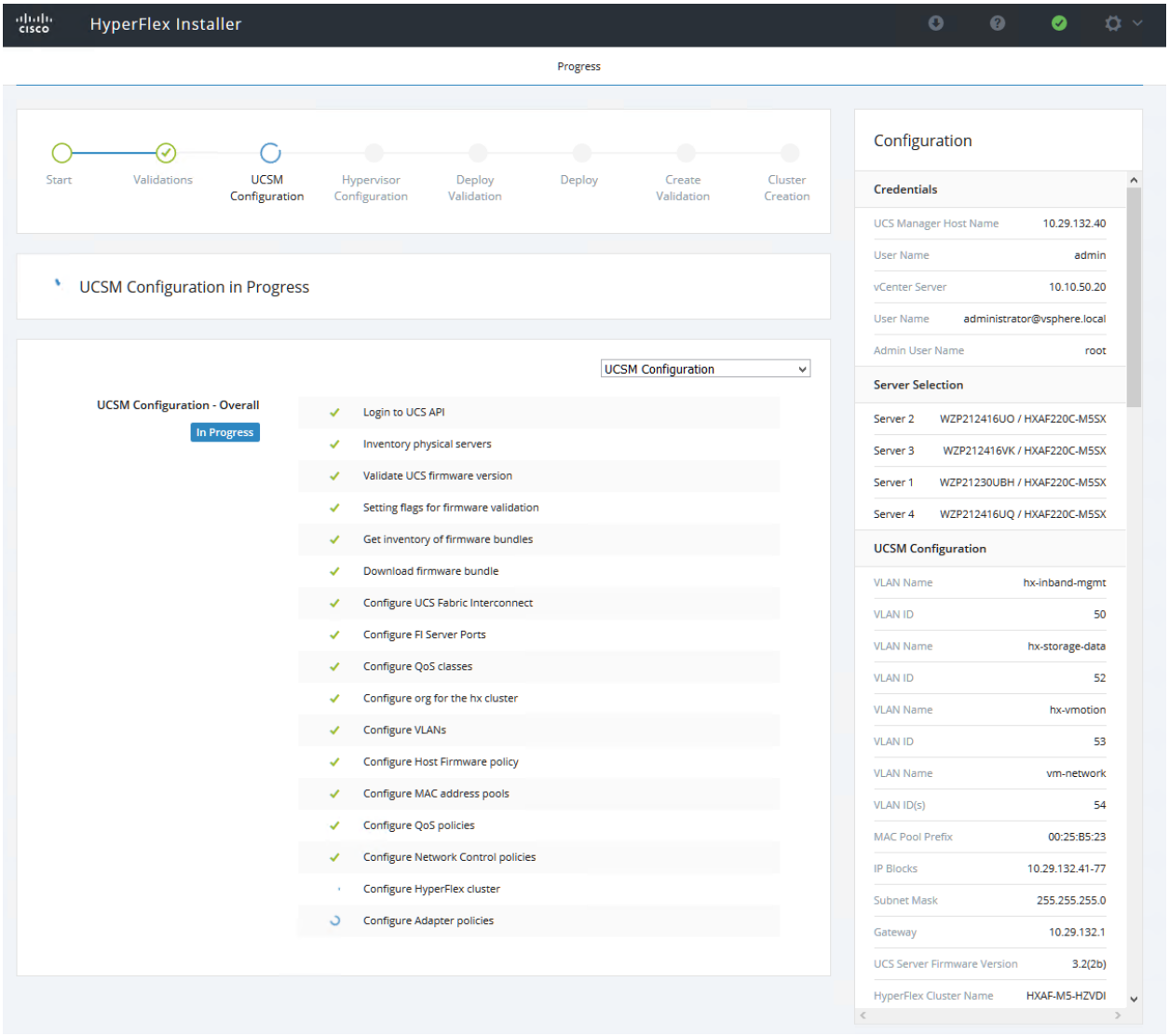
When the installation workflow begins, it will go through the Cisco UCS Manager validation.



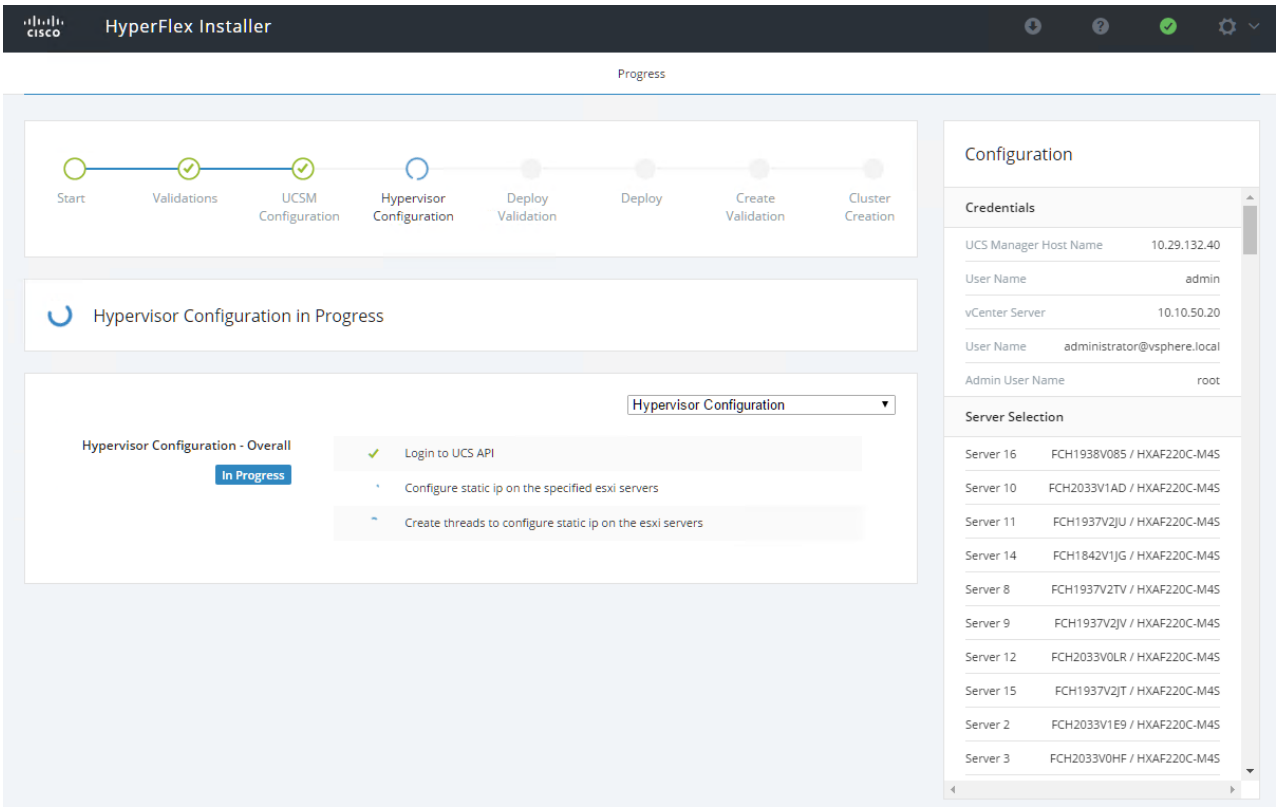
If QoS system class is not defined as per the requirement HyperFlex installer will go ahead and make required changes. There will be a warning generated accordingly in HyperFlex Installer workflow. For 6300 series Fabric Interconnect change in QoS system class requires reboot of FIs.



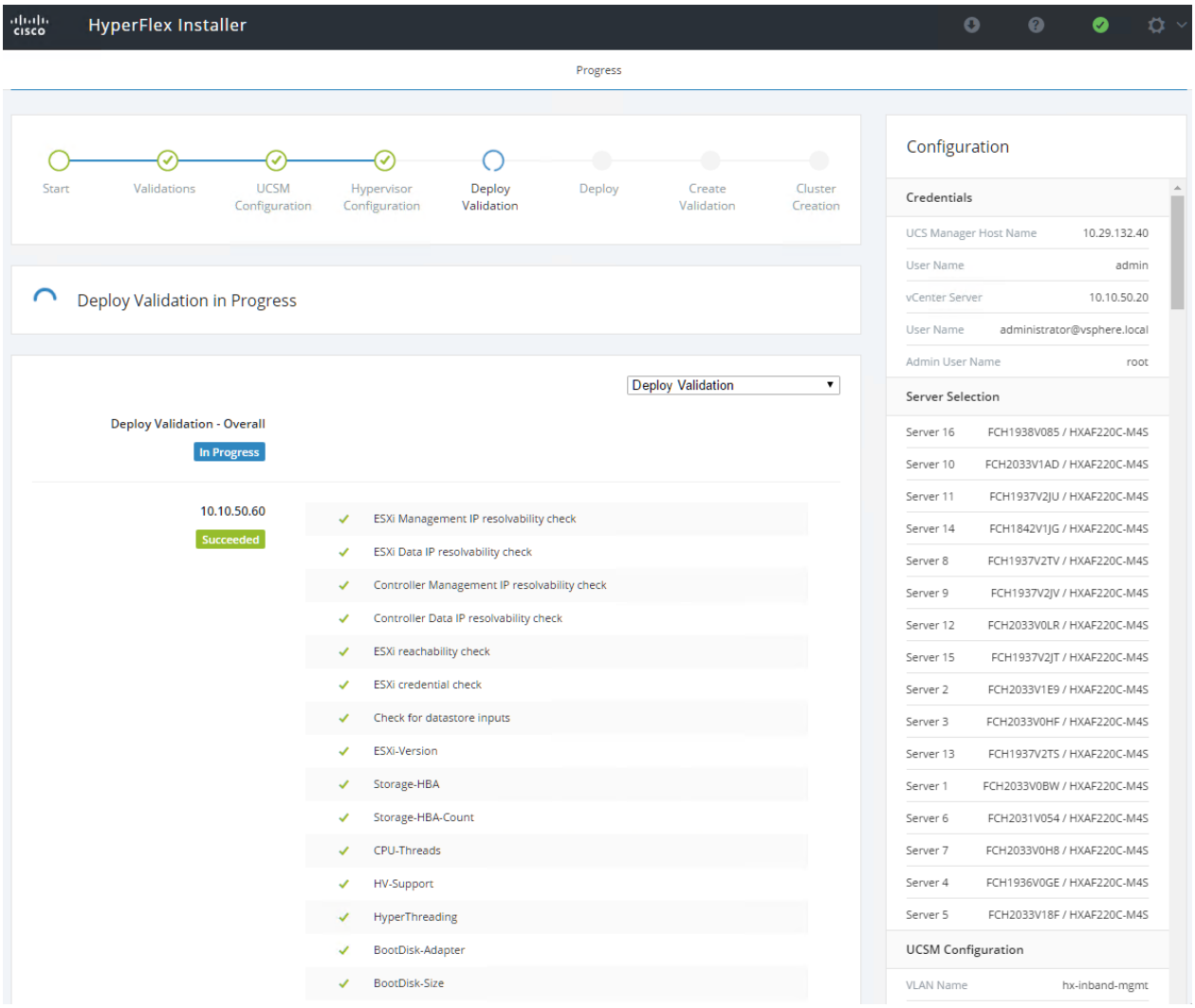
8. After a successful validation, the workflow continues with the Cisco UCS Manager configuration.



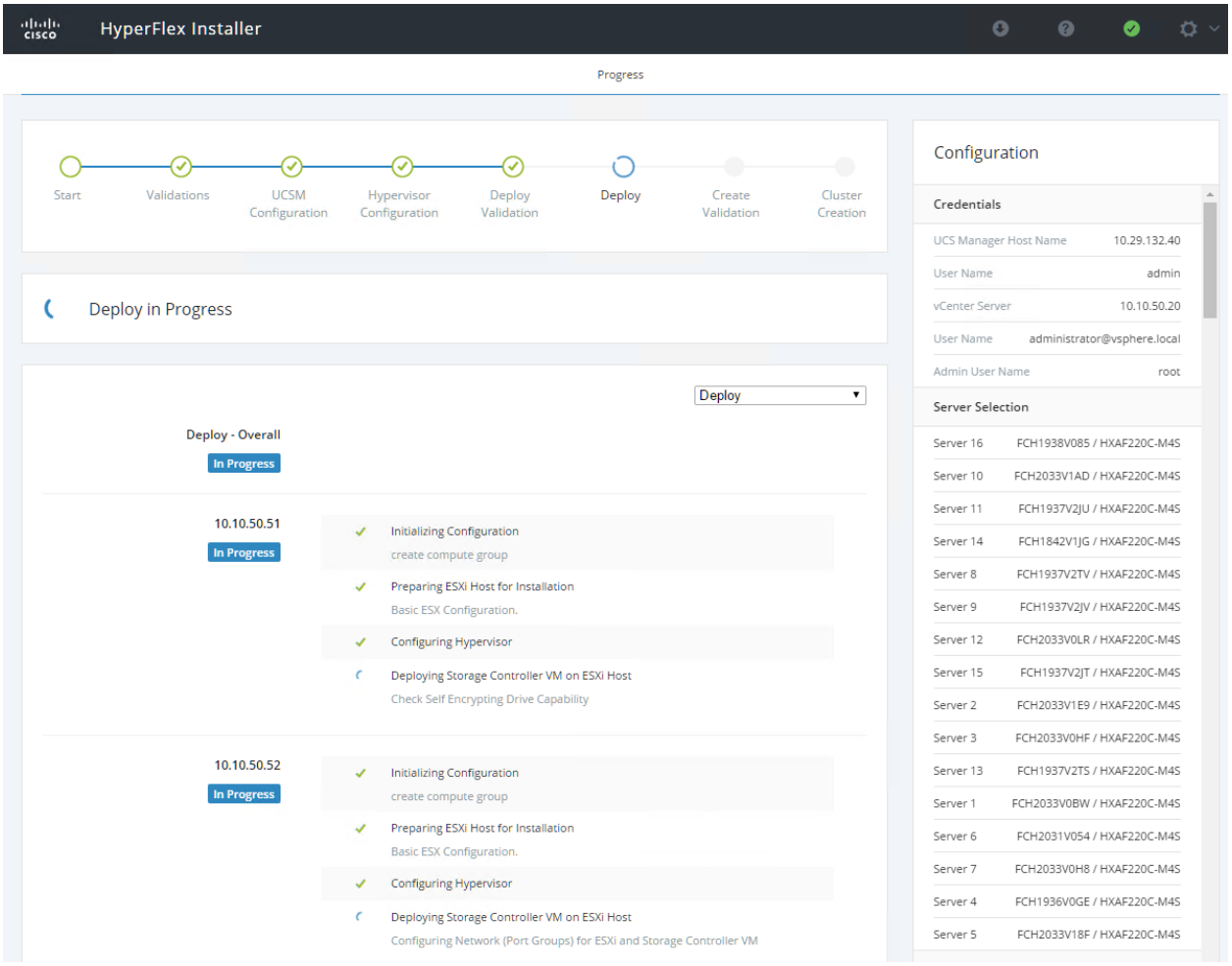
9. After a successful Cisco UCS Manager configuration, the installer proceeds with the Hypervisor configuration.



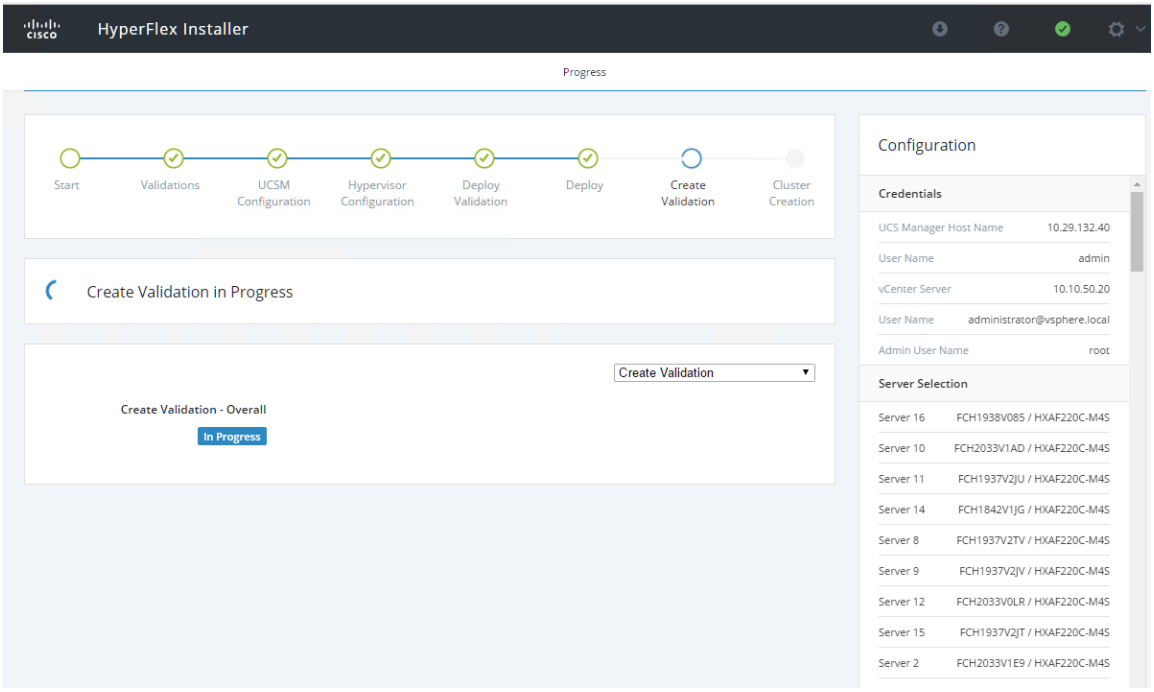
10. After a successful Hypervisor configuration, deploy validation task is performed which checks for required compoenent and accessibilty prior Deploy task is performed on Storage Controller VM.



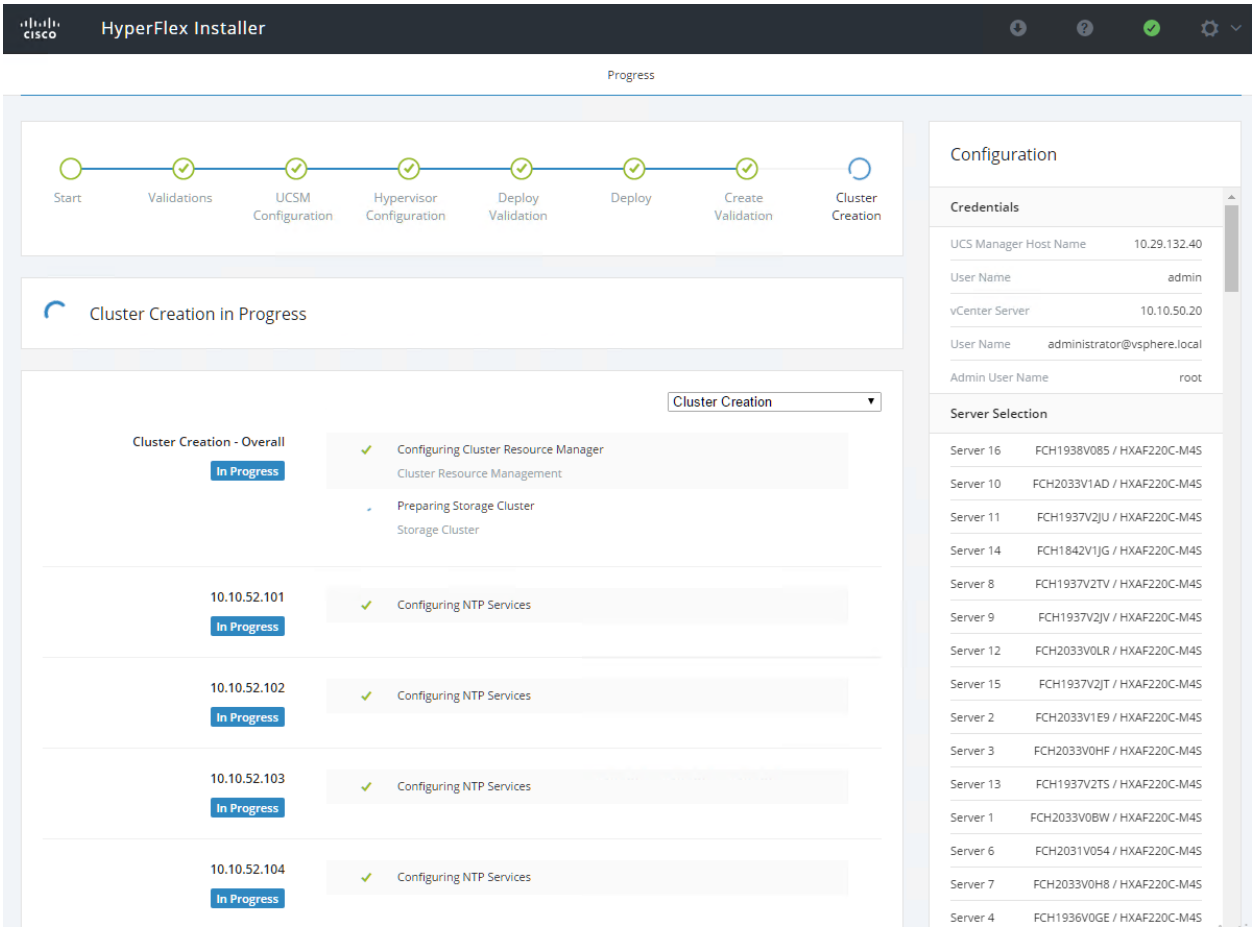
11. Installer performs deployment task after successfully validating Hypervisor configuration.



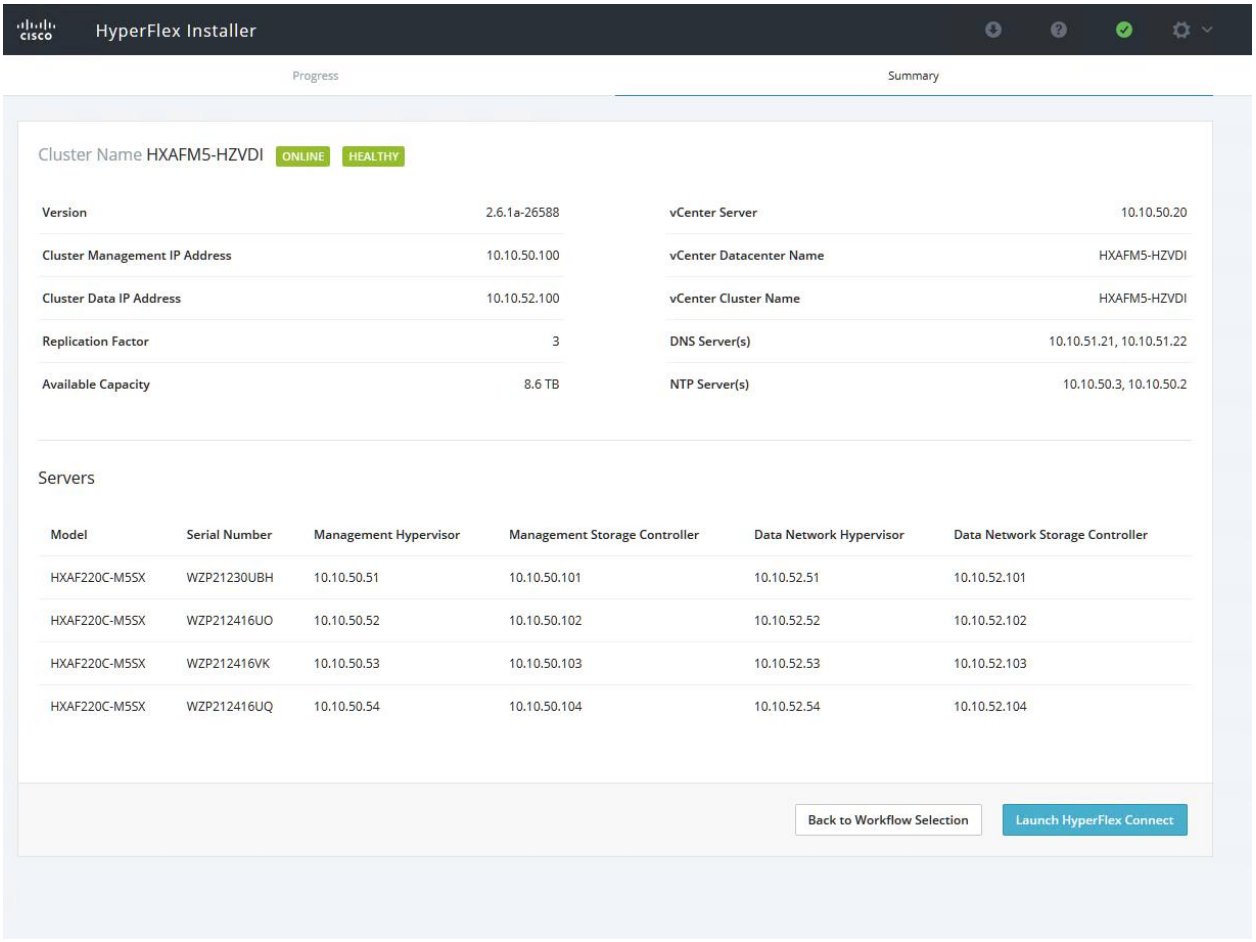
12. After a successful deployment of the ESXi hosts configuration, the Controller VM software components for HyperFlex installer checks for validation prior to creating the cluster.



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



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

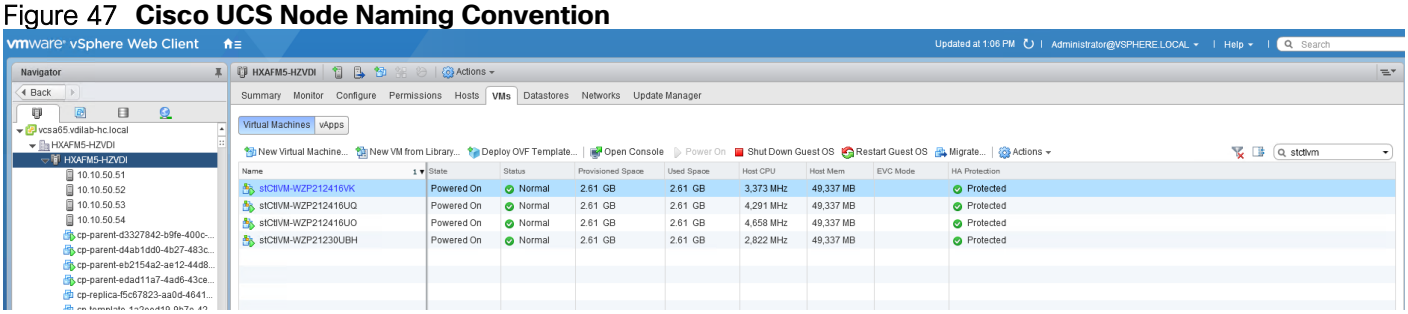


15. Click Launch vSphere Web Client.

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 47.

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

Figure 47 **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 10.10.50.29
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:
```

16. To run the script, 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.

17. Authenticate with the credentials provided earlier. (user name: root with password Cisco 123 if you did not change the defaults.)

18. When authenticated, enter **post_install** at the command prompt, then press **Enter.**

19. Provide a valid vCenter administrator user name and password and the vCenter url IP address.

20. 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.

21. 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.

22. 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

Add vmotion interfaces? (y/n) y

 Netmask for vMotion: 255.255.255.0
```

```
 VLAN ID: (0-4096) 53
  vMotion IP for 10.10.50.51: 10.10.53.51
 Adding vmotion-53 to 10.10.50.51
 Adding vmkernel to 10.10.50.51
 vMotion IP for 10.10.50.52: 10.10.53.52
 Adding vmotion-53 to 10.10.50.52
 Adding vmkernel to 10.10.50.52
 vMotion IP for 10.10.50.53: 10.10.53.53
 Adding vmotion-53 to 10.10.50.53
 Adding vmkernel to 10.10.50.53
 vMotion IP for 10.10.50.54: 10.10.53.54
 Adding vmotion-53 to 10.10.50.54
 Adding vmkernel to 10.10.50.54
Add VM network VLANs? (y/n) n
Send test email? (y/n) n
Validating cluster health and configuration...
 Found UCSM 10.29.132.40, logging with username admin.  Org is HXAF-M5-HZVDI
 UCSM Password:
Could not connect to UCSM at 10.29.132.40 - coercing to Unicode: need string
or buffer, NoneType found.  Skipping UCSM check
Checking MTU settings
 Pinging 169.254.254.2 from vmk1
 Pinging 10.10.50.52 from vmk0
 Pinging 10.10.50.51 from vmk0
 Pinging 10.10.50.53 from vmk0
 Pinging 10.10.50.54 from vmk0
 Setting vmnic1 to active and vmnic0 to standby
 Pinging 10.10.50.52 from vmk0
 Pinging 10.10.50.51 from vmk0
 Pinging 10.10.50.53 from vmk0
 Pinging 10.10.50.54 from vmk0
 Setting vmnic0 to active and vmnic1 to standby
```

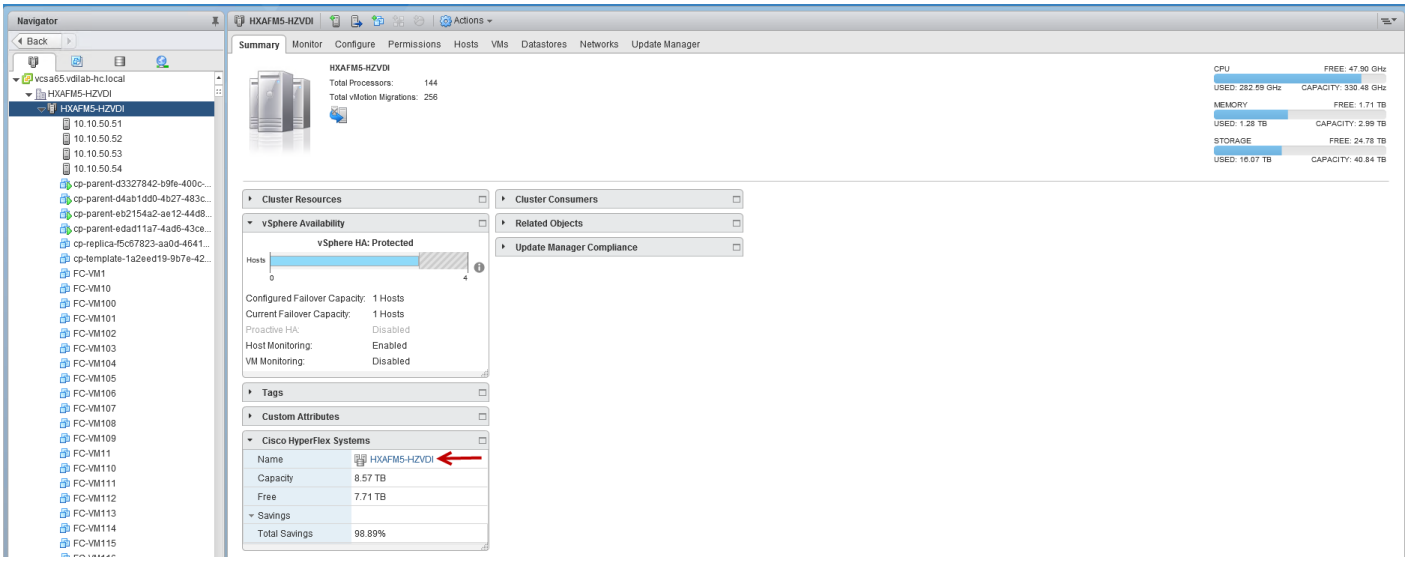
```
Network Summary:
 Host: 10.10.50.51
    vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance_srcid
       vmnic0 - 1 - AAK23-VDIXD-A - active
       vmnic1 - 1 - AAK23-VDIXD-B - standby
         Portgroup Name  -  VLAN
         VM Network - 0
         Storage Controller Management Network - 50
         Storage Controller Replication Network - 0
         Management Network - 50
    vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance_srcid
       vmnic4 - 1 - AAK23-VDIXD-A - active
       vmnic5 - 1 - AAK23-VDIXD-B - active
         Portgroup Name  -  VLAN
         vm-network-54 - 54
    vswitch: vmotion - mtu: 9000 - policy: loadbalance_srcid
       vmnic6 - 1 - AAK23-VDIXD-A - active
       vmnic7 - 1 - AAK23-VDIXD-B - standby
         Portgroup Name  -  VLAN
         vmotion-53 - 53
    vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance_srcid
       vmnic2 - 1 - AAK23-VDIXD-A - standby
       vmnic3 - 1 - AAK23-VDIXD-B - active
         Portgroup Name  -  VLAN
         Storage Controller Data Network - 52
         Storage Hypervisor Data Network - 52


 Host: 10.10.50.52
    vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance_srcid
       vmnic0 - 1 - AAK23-VDIXD-A - active
       vmnic1 - 1 - AAK23-VDIXD-B - standby
         Portgroup Name  -  VLAN
```

```
            VM Network - 0
            Storage Controller Management Network - 50
            Storage Controller Replication Network - 0
            Management Network - 50
      vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance_srcid
         vmnic4 - 1 - AAK23-VDIXD-A - active
         vmnic5 - 1 - AAK23-VDIXD-B - active
            Portgroup Name  -  VLAN
            vm-network-54 - 54
      vswitch: vmotion - mtu: 9000 - policy: loadbalance_srcid
         vmnic6 - 1 - AAK23-VDIXD-A - active
         vmnic7 - 1 - AAK23-VDIXD-B - standby
            Portgroup Name  -  VLAN
            vmotion-53 - 53
      vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance_srcid
         vmnic2 - 1 - AAK23-VDIXD-A - standby
         vmnic3 - 1 - AAK23-VDIXD-B - active
            Portgroup Name  -  VLAN
            Storage Controller Data Network - 52
            Storage Hypervisor Data Network - 52

   Host: 10.10.50.53
      vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance_srcid
         vmnic0 - 1 - AAK23-VDIXD-A - active
         vmnic1 - 1 - AAK23-VDIXD-B - standby
            Portgroup Name  -  VLAN
            VM Network - 0
            Storage Controller Management Network - 50
            Storage Controller Replication Network - 0
            Management Network - 50
      vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance_srcid
         vmnic4 - 1 - AAK23-VDIXD-A - active
```

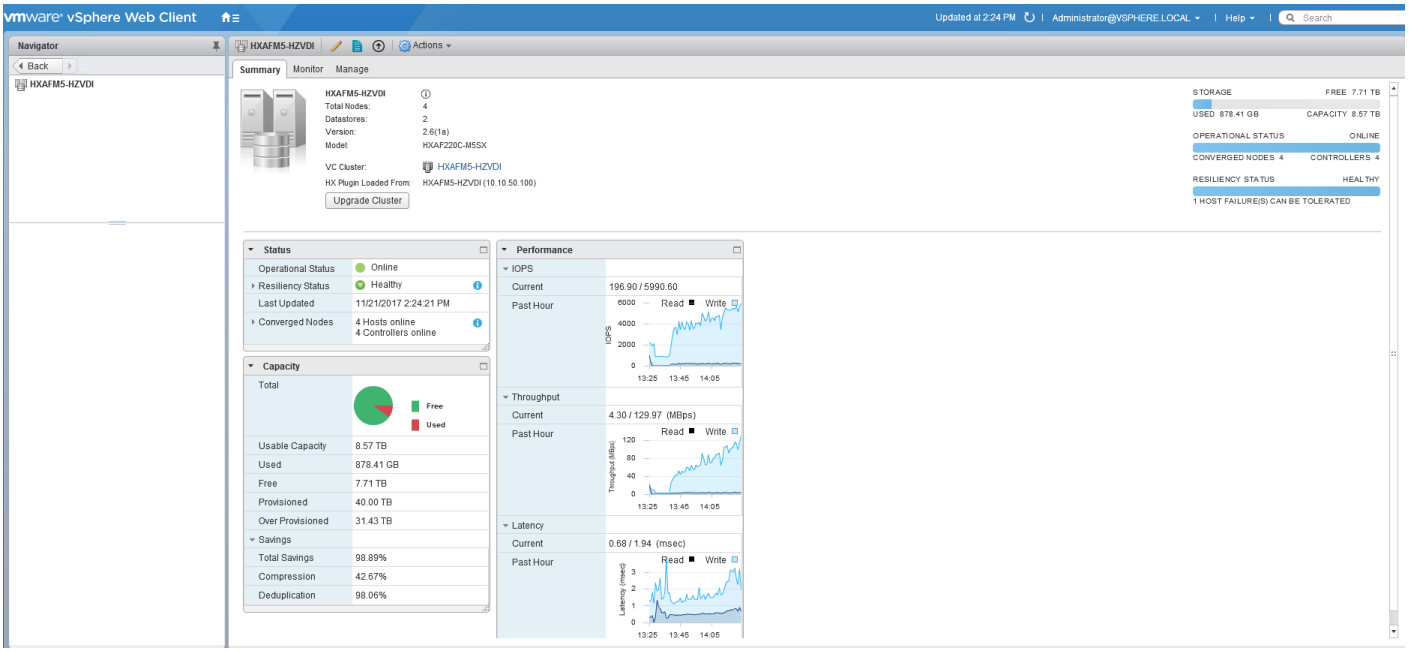
```
      vmnic5 - 1 - AAK23-VDIXD-B - active
        Portgroup Name  -  VLAN
        vm-network-54 - 54
    vswitch: vmotion - mtu: 9000 - policy: loadbalance_srcid
      vmnic6 - 1 - AAK23-VDIXD-A - active
      vmnic7 - 1 - AAK23-VDIXD-B - standby
        Portgroup Name  -  VLAN
        vmotion-53 - 53
    vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance_srcid
      vmnic2 - 1 - AAK23-VDIXD-A - standby
      vmnic3 - 1 - AAK23-VDIXD-B - active
        Portgroup Name  -  VLAN
        Storage Controller Data Network - 52
        Storage Hypervisor Data Network - 52

Host: 10.10.50.54
    vswitch: vswitch-hx-inband-mgmt - mtu: 1500 - policy: loadbalance_srcid
      vmnic0 - 1 - AAK23-VDIXD-A - active
      vmnic1 - 1 - AAK23-VDIXD-B - standby
        Portgroup Name  -  VLAN
        VM Network - 0
        Storage Controller Management Network - 50
        Storage Controller Replication Network - 0
        Management Network - 50
    vswitch: vswitch-hx-vm-network - mtu: 1500 - policy: loadbalance_srcid
      vmnic4 - 1 - AAK23-VDIXD-A - active
      vmnic5 - 1 - AAK23-VDIXD-B - active
        Portgroup Name  -  VLAN
        vm-network-54 - 54
    vswitch: vmotion - mtu: 9000 - policy: loadbalance_srcid
      vmnic6 - 1 - AAK23-VDIXD-A - active
      vmnic7 - 1 - AAK23-VDIXD-B - standby
```

```
          Portgroup Name  -  VLAN
          vmotion-53 - 53
      vswitch: vswitch-hx-storage-data - mtu: 9000 - policy: loadbalance_srcid
        vmnic2 - 1 - AAK23-VDIXD-A - standby
        vmnic3 - 1 - AAK23-VDIXD-B - active
          Portgroup Name  -  VLAN
          Storage Controller Data Network - 52
          Storage Hypervisor Data Network - 52


 Host: 10.10.50.51
     Could not ping IP 169.254.254.2 from vmk1, verify network connectivity


 Host: 10.10.50.52
 Host: 10.10.50.53
 Host: 10.10.50.54
 Controller VM Clocks:
     stCtlVM-WZP212416UO  -  2017-11-13 17:57:21 - Have not recently synced
with NTP server
     stCtlVM-WZP21230UBH  -  2017-11-13 17:57:22 - Have not recently synced
with NTP server
     stCtlVM-WZP212416VK  -  2017-11-13 17:57:24 - Have not recently synced
with NTP server
     stCtlVM-WZP212416UQ  -  2017-11-13 17:57:25 - Have not recently synced
with NTP server
 Cluster:
     Version - 2.6.1a-26588
     Model - HXAF220C-M5SX
     Health - HEALTHY
     ASUP enabled - False
     SMTP Server -
root@Cisco-HX-Installer-Appliance: ~root@Cisco-HX-Installer-Appliance:~#
```

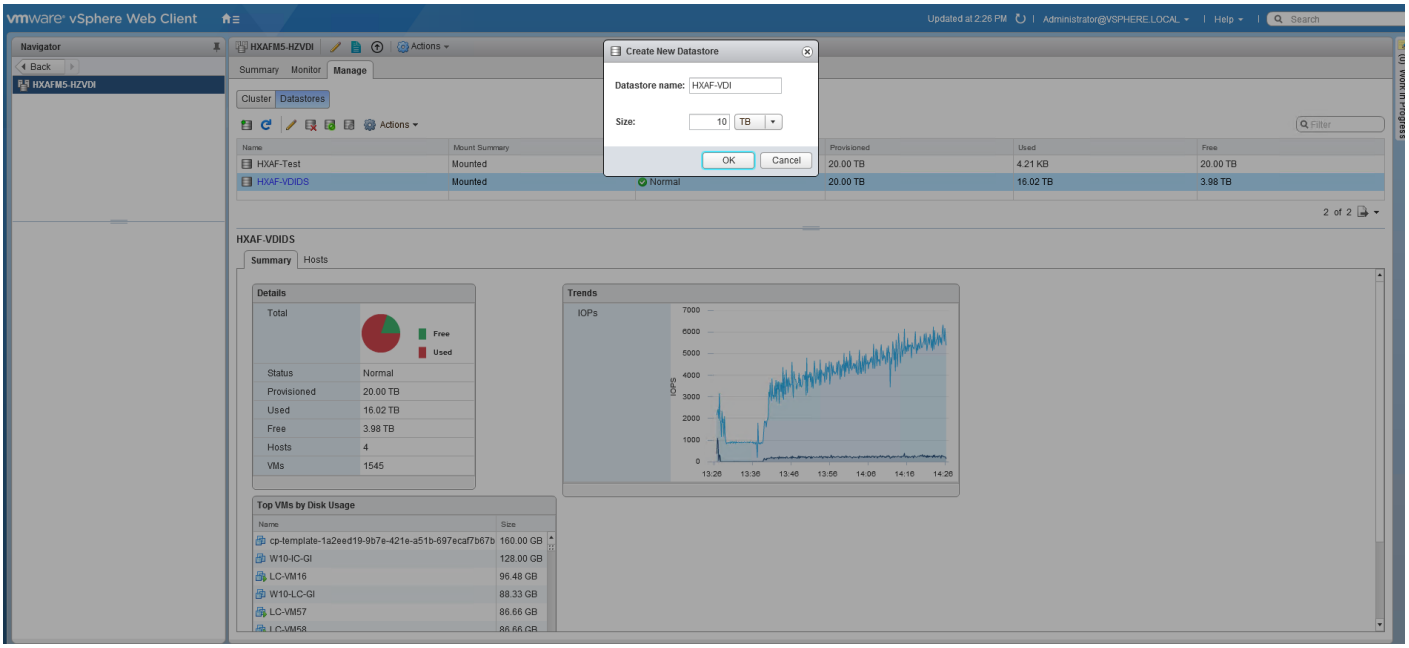
23. Login to vSphere WebClient to create additional shared datastore.
24. Go to the Summary tab on the cluster created via the HyperFlex cluster creation workflow.
25. On Cisco HyperFlex Systems click the cluster name.



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

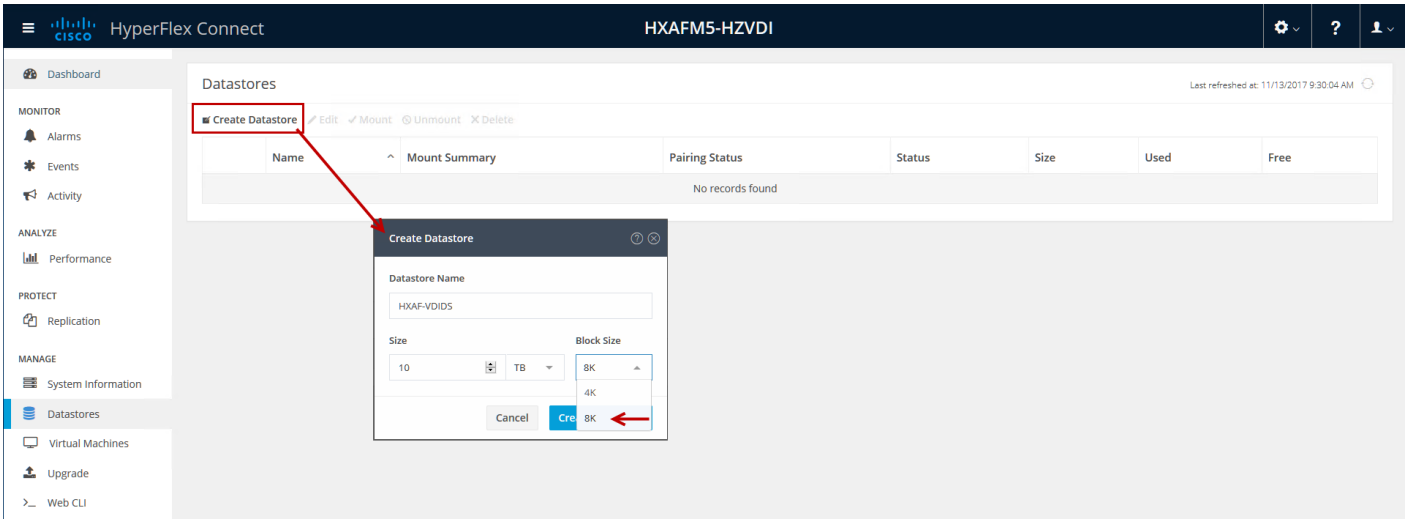


26. Click Manage, select Datastores. Click the Add datastore icon, select the datastore name and size to provision.



You have now created a 20TB datastore for the Citrix pooled, persistent/non-persistent, and XenApp server desktop performance test.

Alternatively HyperFlex connect WebUI can be utilized as well to create a datastore. While using HyperFlex Connect UI to create a datastore there is an option to select Block size. By default datastores are created with 8K Block size using vSphere WebClient.



Build the Virtual Machines and Environment for Workload Testing

Software Infrastructure Configuration

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

Install and configure the infrastructure virtual machines by following the process provided in Table 10

Table 10 Test Infrastructure Virtual Machine Configuration

Configuration	**Citrix XenDesktop Controllers** Virtual Machines	**Citrix Provisioning Servers** Virtual Machines
Operating system	Microsoft Windows Server 2016	Microsoft Windows Server 2016
Virtual CPU amount	6	8
Memory amount	8 GB	8 GB
Network	VMXNET3 InBand-Mgmt	VMXNET3 InBand-Mgmt
Disk-1 (OS) size and location	40 GB Infra-DS volume	40 GB Infra-DS volume
Disk-2 size and location	–	200 GB
Configuration	**Microsoft Active Directory DCs** Virtual Machines	**vCenter Server Appliance** Virtual Machine
Operating system	Microsoft Windows Server 2012 R2	VCSA – SUSE Linux
Virtual CPU amount	4	8
Memory amount	4 GB	24 GB
Network	VMXNET3 InBand-Mgmt	VMXNET3 InBand-Mgmt
Disk size and location	40 GB	460 GB (across 11 VMDKs)

Configuration	Microsoft SQL Server Virtual Machine	Citrix StoreFront Virtual Machines
Operating system	Microsoft Windows Server 2016 Microsoft SQL Server 2016	Microsoft Windows Server 2016
Virtual CPU amount	4	4
Memory amount	16 GB	8 GB
Network	VMXNET3 InBand-Mgmt	VMXNET3 InBand-Mgmt
Disk-1 (OS) size and location	40 GB Infra-DS volume	40 GB Infra-DS volume
Disk-2 size and location	200 GB Infra-DS volume SQL Logs	–
Configuration	**Citrix License Server** Virtual Machines	**NetScaler VPX Appliance** Virtual Machine
Operating system	Microsoft Windows Server 2012 R2	NS11.1 52.13.nc
Virtual CPU amount	4	2
Memory amount	4 GB	2 GB
Network	VMXNET3 InBand-Mgmt	VMXNET3 InBand-Mgmt Infra-Mgmt
Disk size and location	40 GB	20 GB

Prepare the Master Images

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

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

- Installing OS and application software
- Installing the PVS Target Device x64 software

- Installing the Virtual Delivery Agents (VDAs)

The master image HVD and HSD VMs were configured as follows in Table 11 :

Table 11 HVD and HSD Configurations

Configuration	HVDI Virtual Machines	HSD Virtual Machines
Operating system	Microsoft Windows 10 64-bit	Microsoft Windows Server 2016
Virtual CPU amount	2	6
Memory amount	2.0 GB (reserved)	24 GB (reserved)
Network	VMXNET3 vm-network	VMXNET3 vm-network
Citrix PVS vDisk size and location	24 GB (thick) Infra-DS volume	100 GB (thick) Infra-DS volume
Citrix PVS write cache Disk size	6 GB	24 GB
Additional software used for testing	Microsoft Office 2016 Login VSI 4.1.32 (Knowledge Worker Workload)	Microsoft Office 2016 Login VSI 4.1.32 (Knowledge Worker Workload)

Install and Configure XenDesktop and XenApp

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

Prerequisites

Citrix recommends that you use Secure HTTP (HTTPS) and a digital certificate to protect vSphere communications. Citrix recommends that you use a digital certificate issued by a certificate authority (CA) according to your organization's security policy. Otherwise, if security policy allows, use the VMware-installed self-signed certificate.

To install vCenter Server self-signed Certificate, complete the following steps:

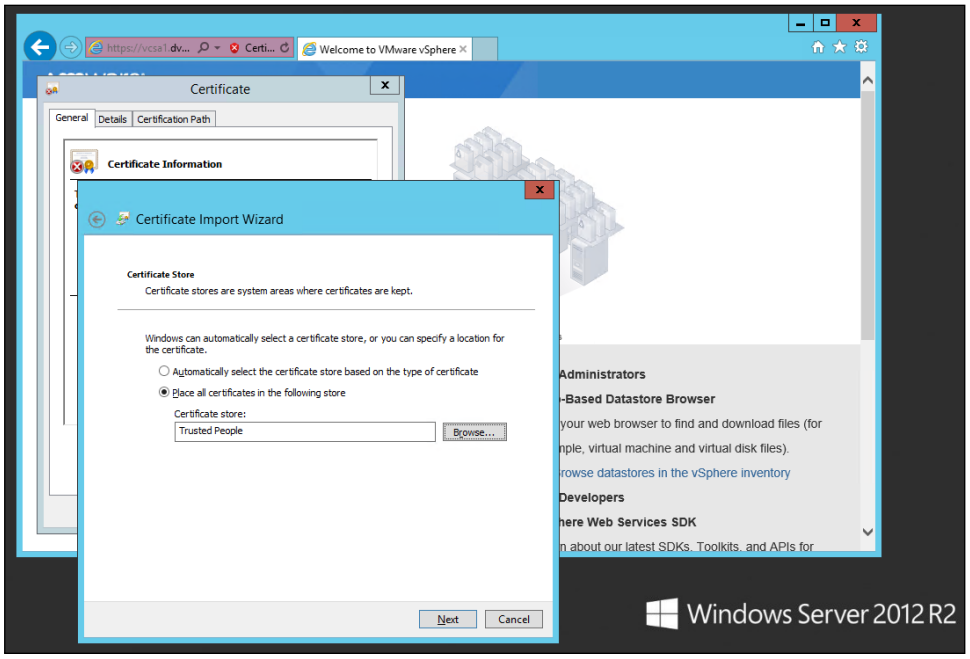
1. Add the FQDN of the computer running vCenter Server to the hosts file on that server, located at SystemRoot/WINDOWS/system32/Drivers/etc/. This step is required only if the FQDN of the computer running vCenter Server is not already present in DNS.

2. Open Internet Explorer and enter the address of the computer running vCenter Server (e.g., https://FQDN as the URL).

3. Accept the security warnings.

4. Click the Certificate Error in the Security Status bar and select View certificates.

5. Click Install certificate, select Local Machine, and then click Next.
6. Select Place all certificates in the following store and then click Browse.
7. Select Show physical stores.
8. Select Trusted People.



9. Click Next and then click Finish.
10. Perform the above steps on all Delivery Controllers and Provisioning Servers.

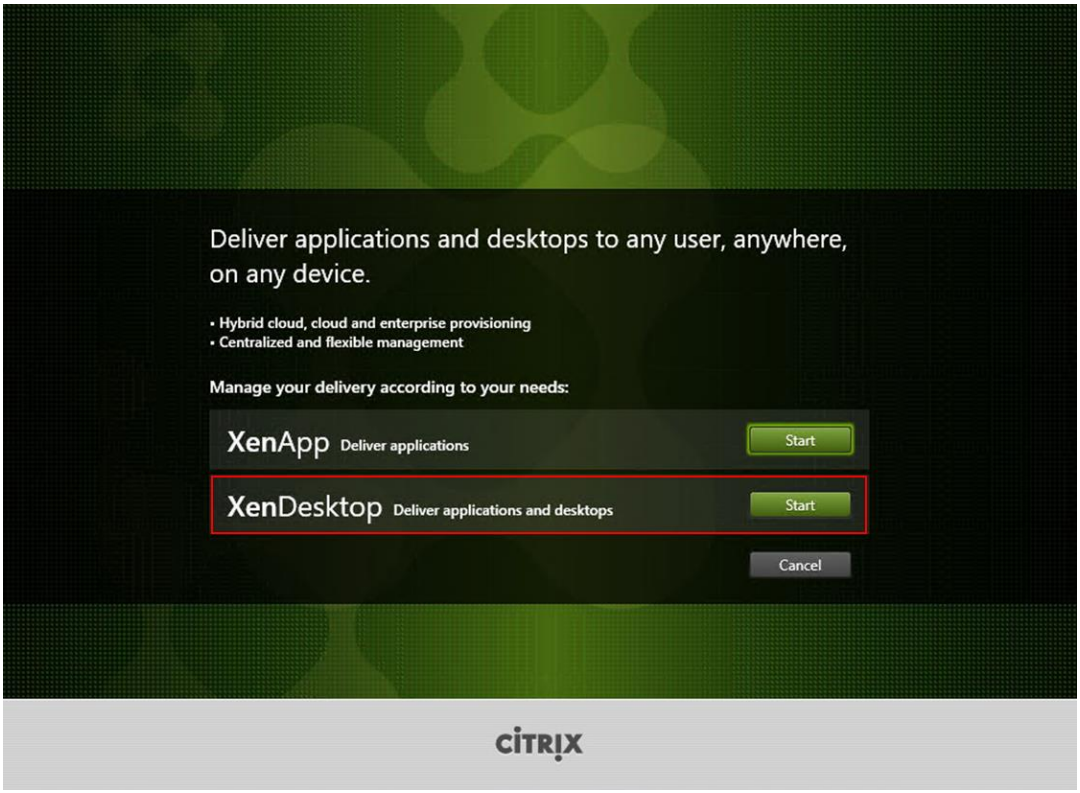
Install XenDesktop Delivery Controller, Citrix Licensing, and StoreFront

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

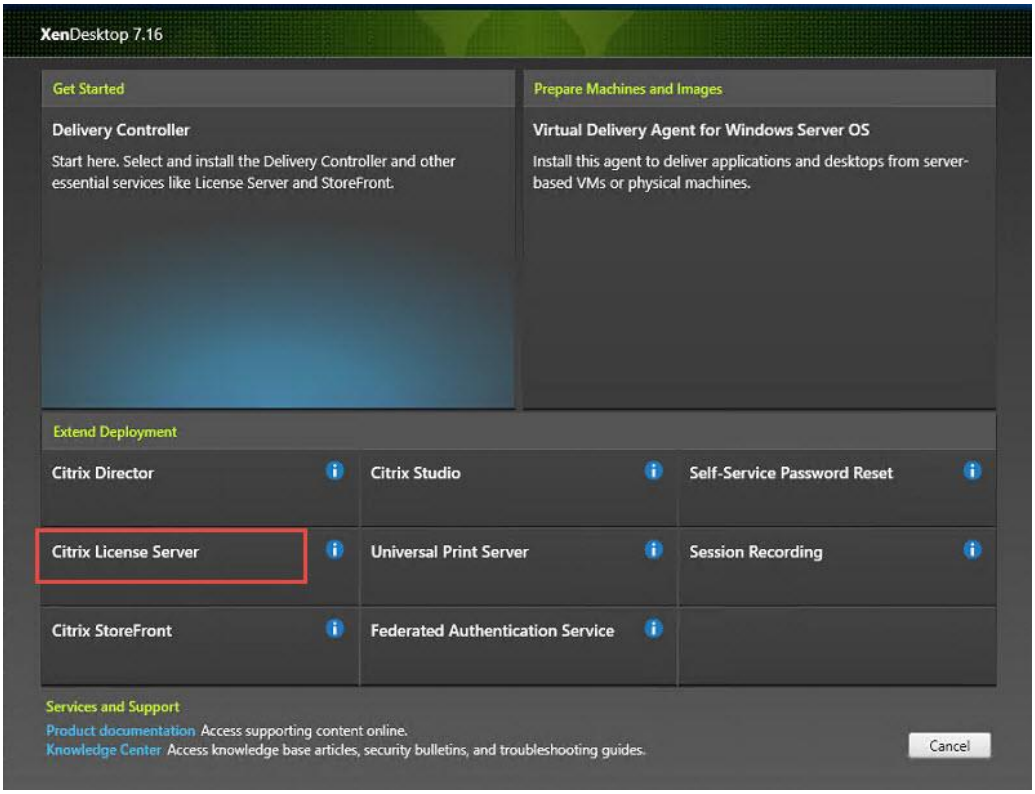
Install Citrix License Server

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

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



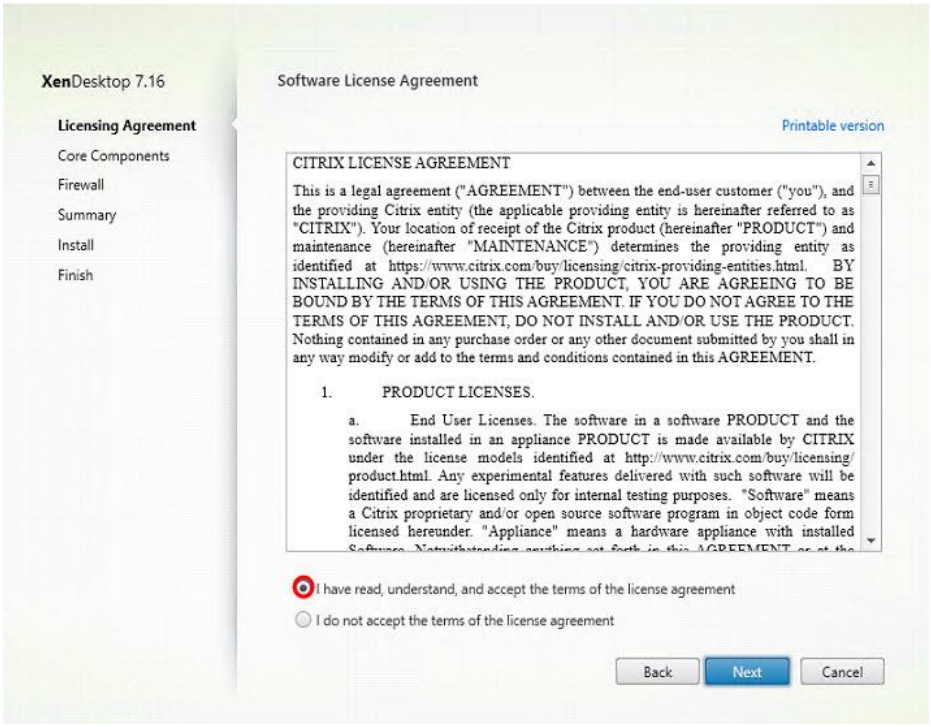
3. Click “Extend Deployment – Citrix License Server.”



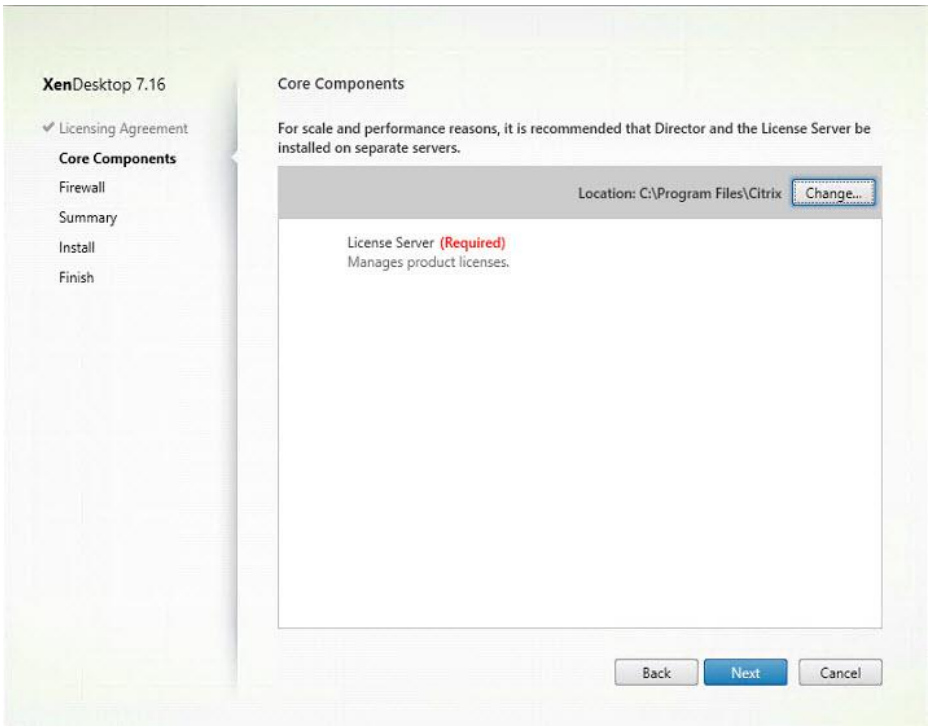
4. Read the Citrix License Agreement.

5. If acceptable, indicate your acceptance of the license by selecting the “I have read, understand, and accept the terms of the license agreement” radio button.

6. Click Next.

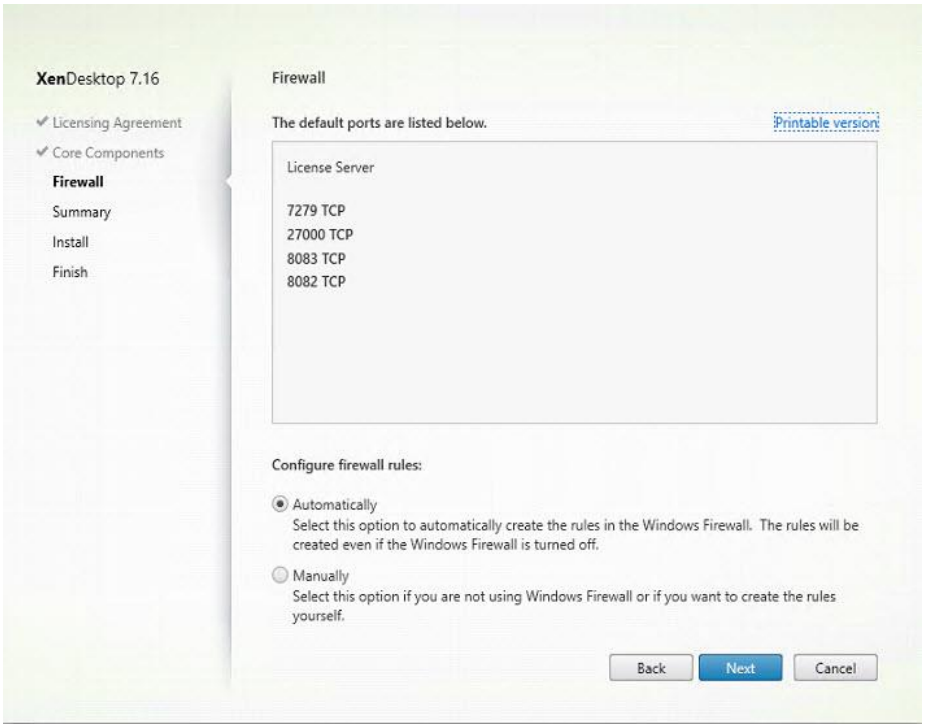


7. Click Next.

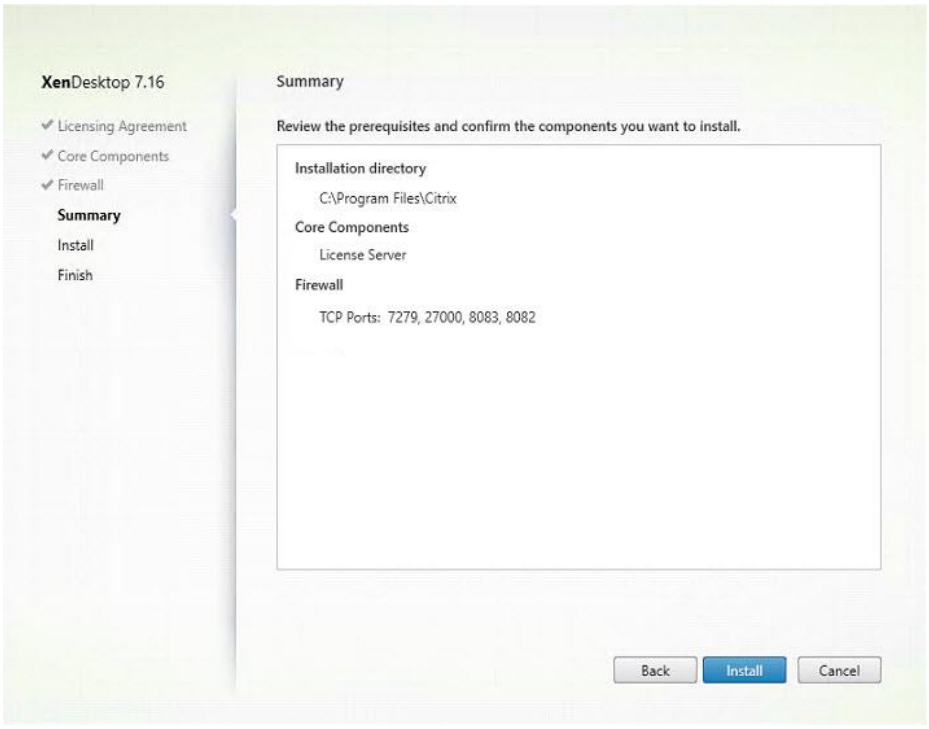


8. Select the default ports and automatically configured firewall rules.

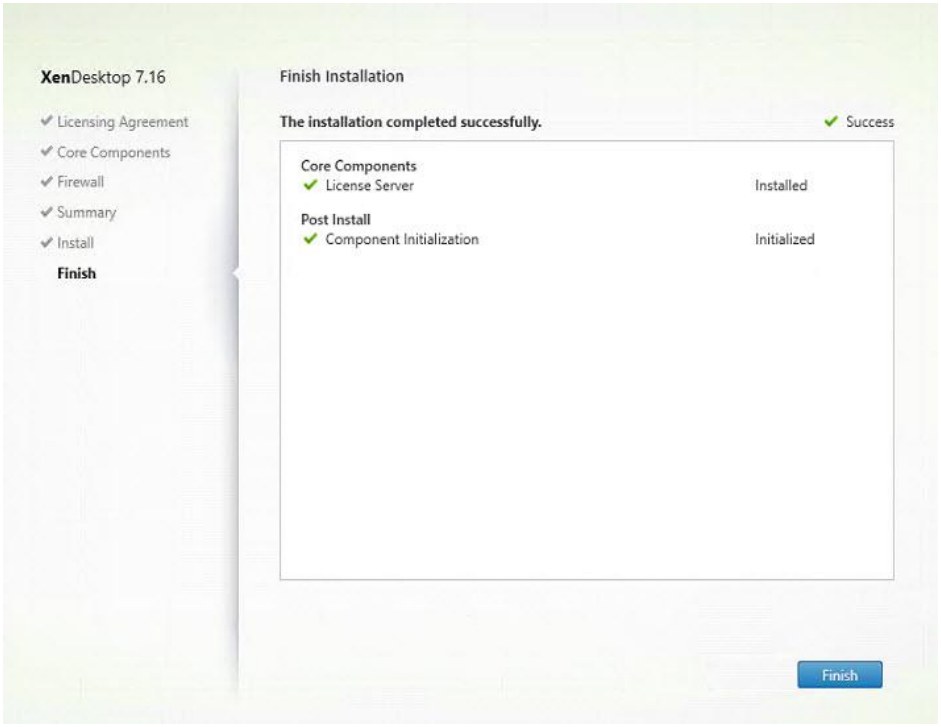
9. Click Next



10. Click Install.



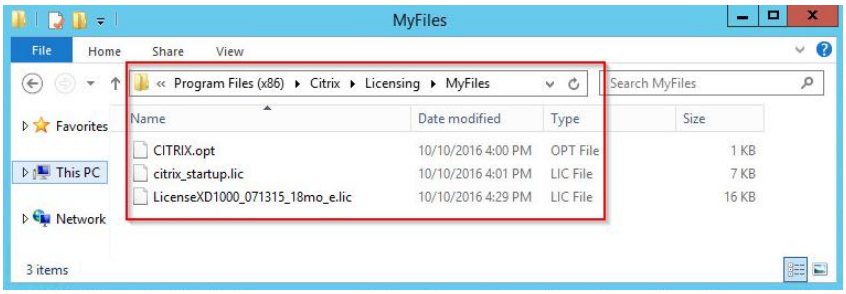
11. Click Finish to complete the installation.



Install Citrix Licenses

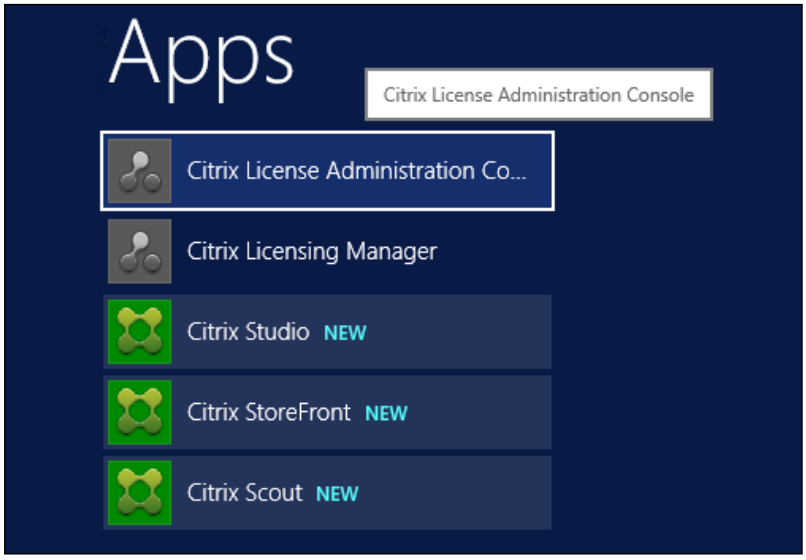
To install the Citrix Licenses, complete the following steps:

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

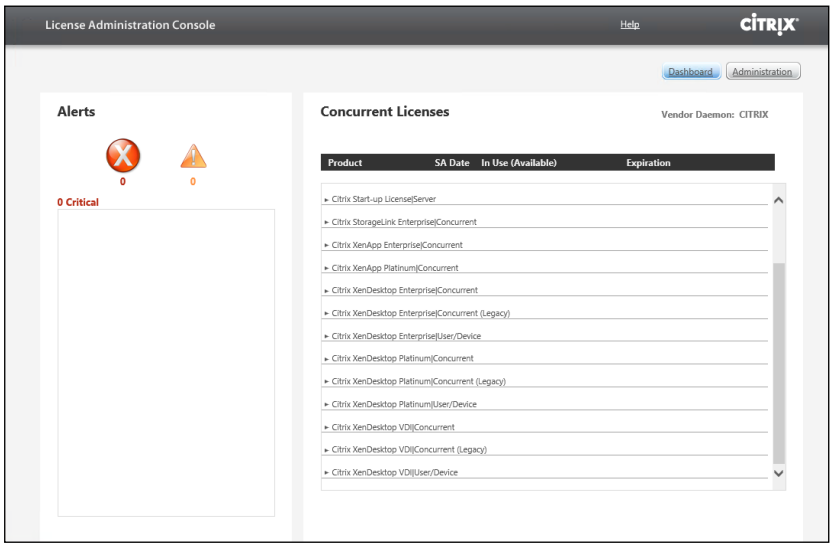


2. Restart the server or Citrix licensing services so that the licenses are activated.

3. Run the application Citrix License Administration Console.



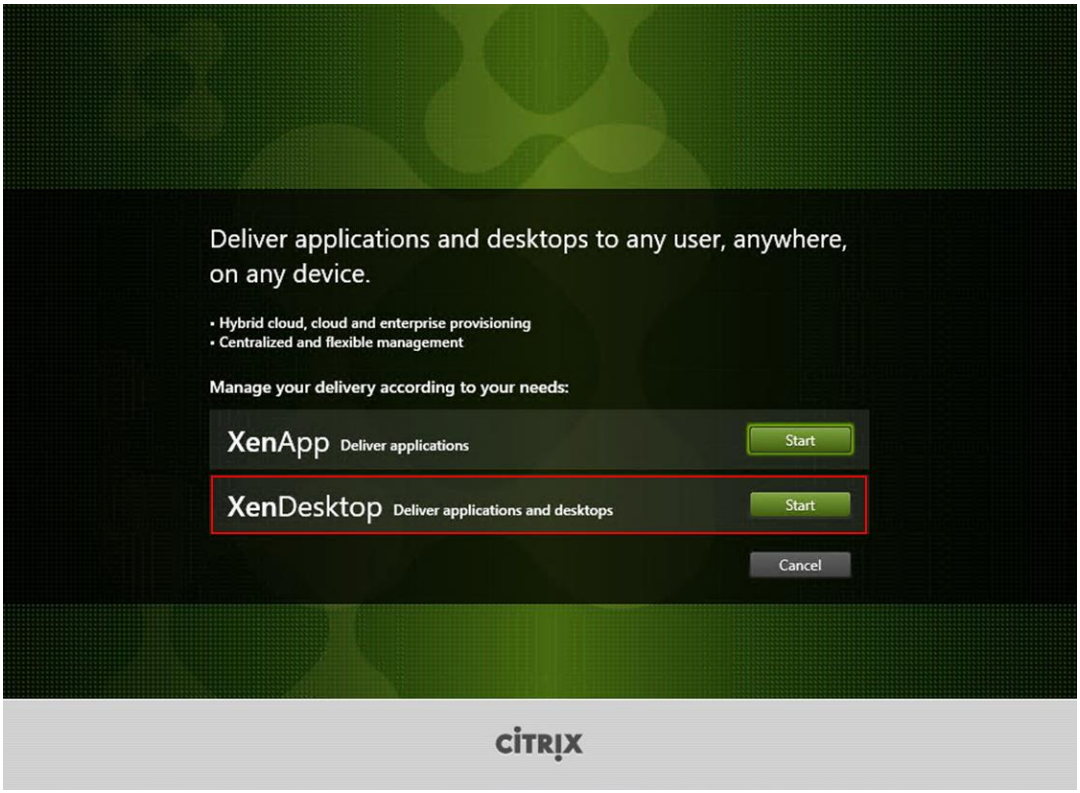
4. Confirm that the license files have been read and enabled correctly.



Install the XenDesktop

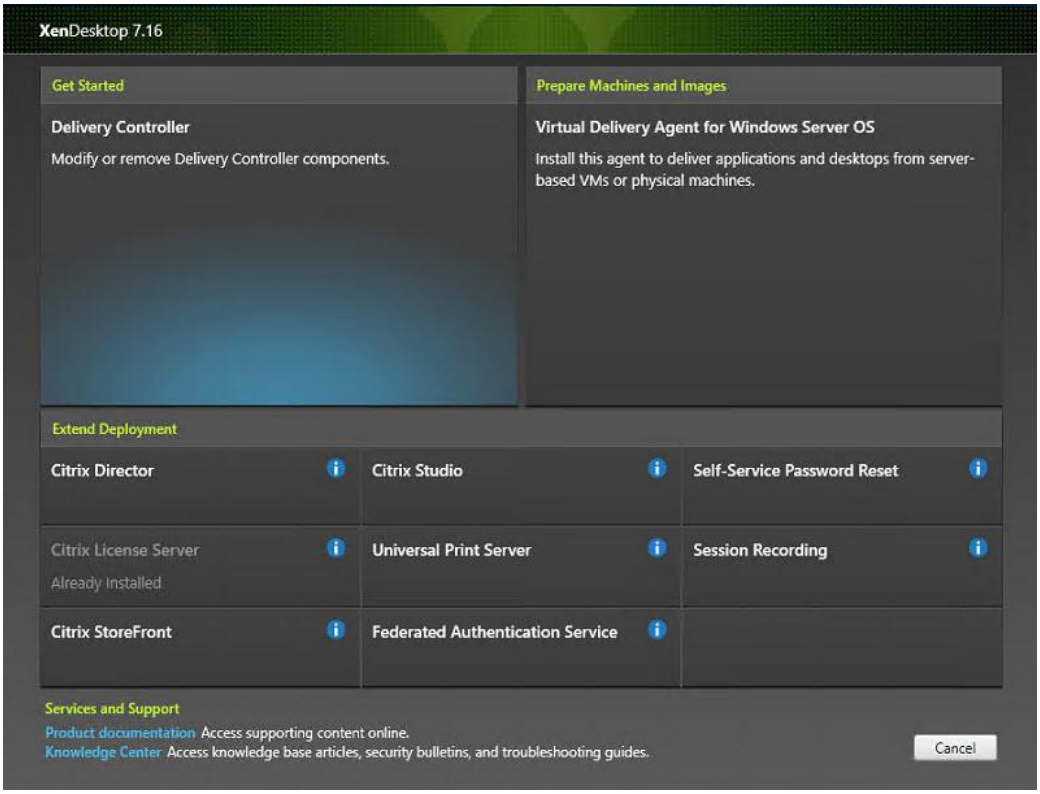
1. To begin the installation, connect to the first XenDesktop server and launch the installer from the Citrix XenDesktop 7.16 ISO.

2. Click Start.



The installation wizard presents a menu with three subsections.

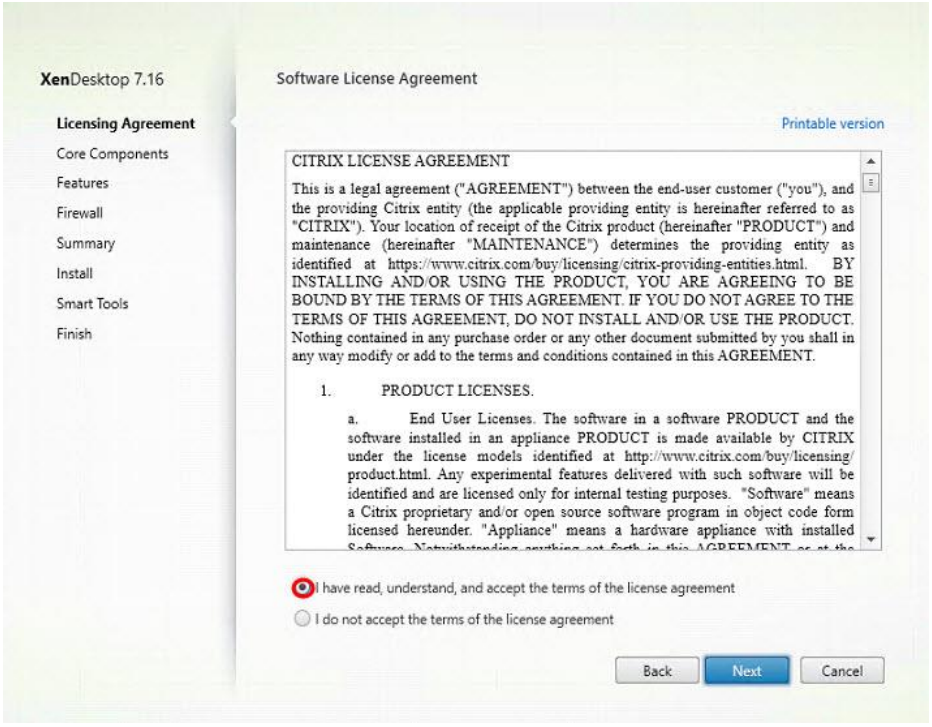
3. Click “Get Started - Delivery Controller.”



4. Read the Citrix License Agreement.

5. If acceptable, indicate your acceptance of the license by selecting the “I have read, understand, and accept the terms of the license agreement” radio button.

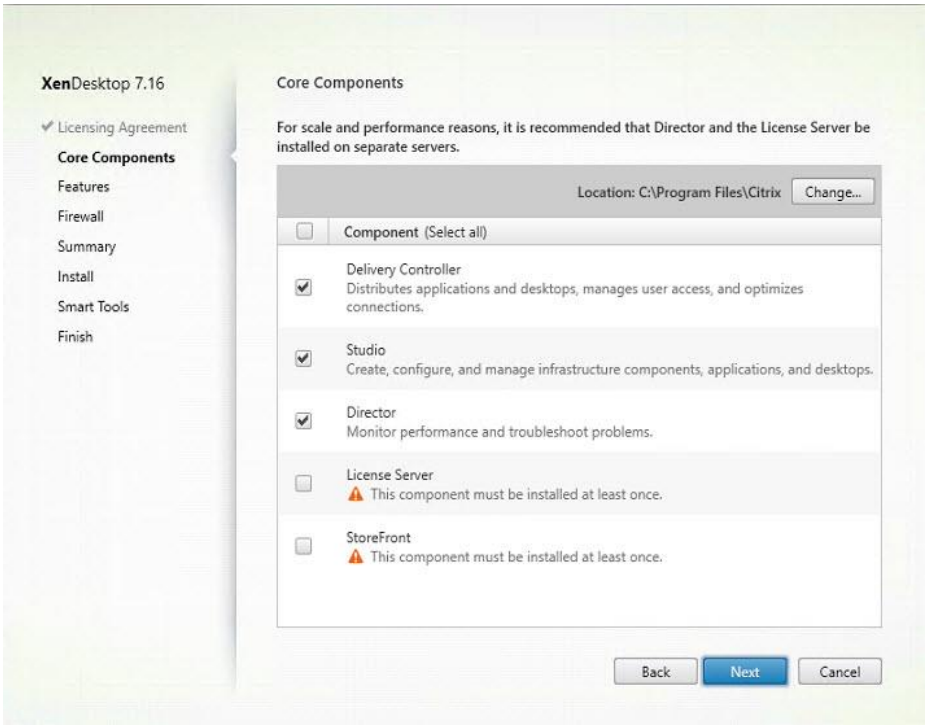
6. Click Next.



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

   a. Delivery Controller
   b. Studio
   c. Director

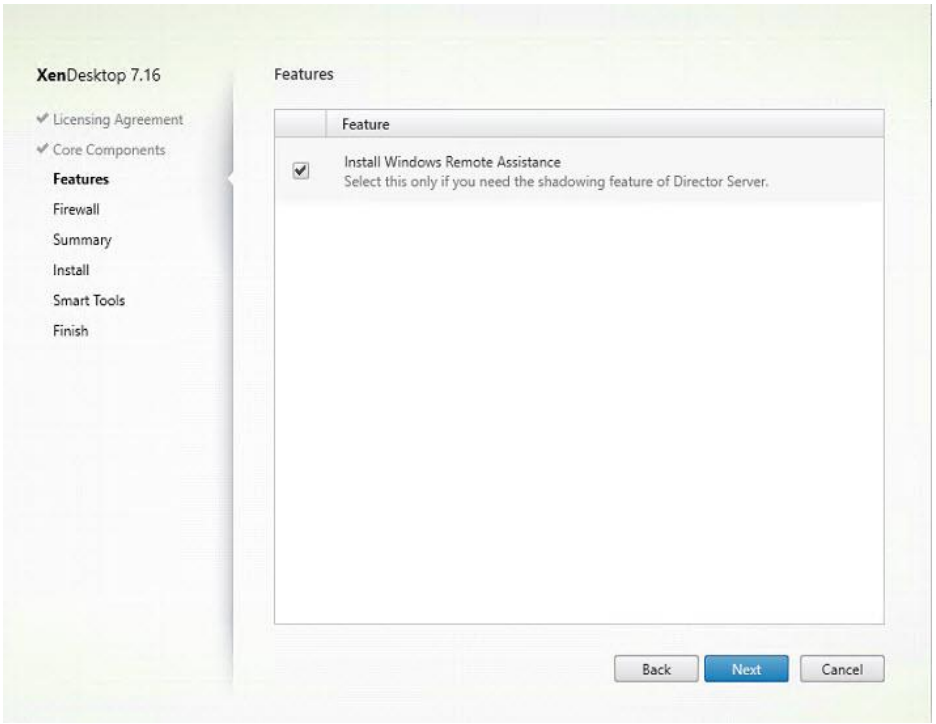
8. Click Next.



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

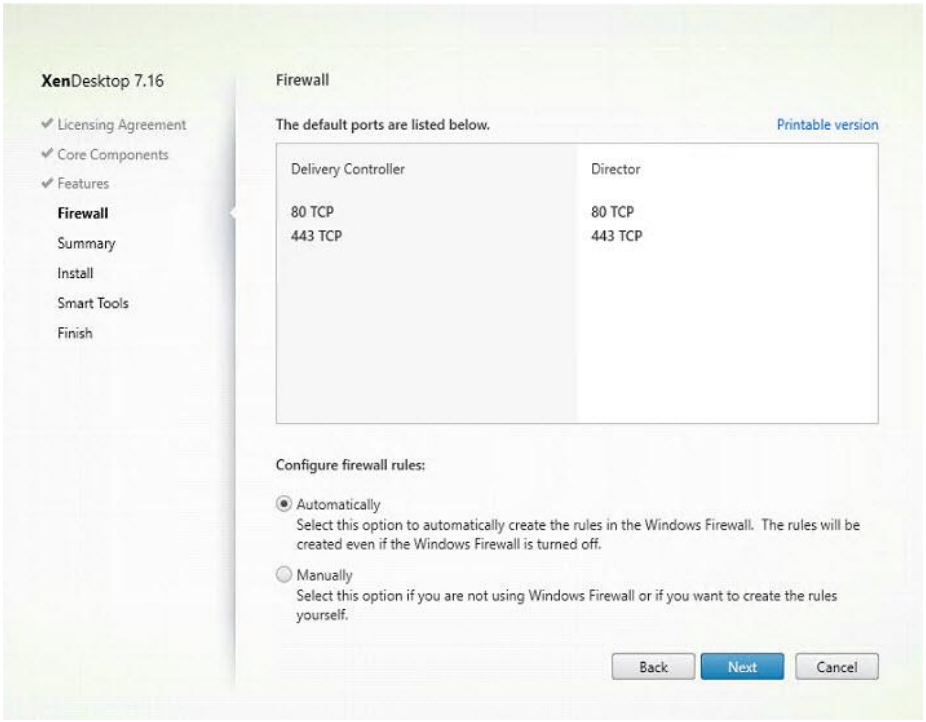
9. Since a SQL Server will be used to Store the Database, leave “Install Microsoft SQL Server 2012 SP1 Express” unchecked.

10. Click Next.

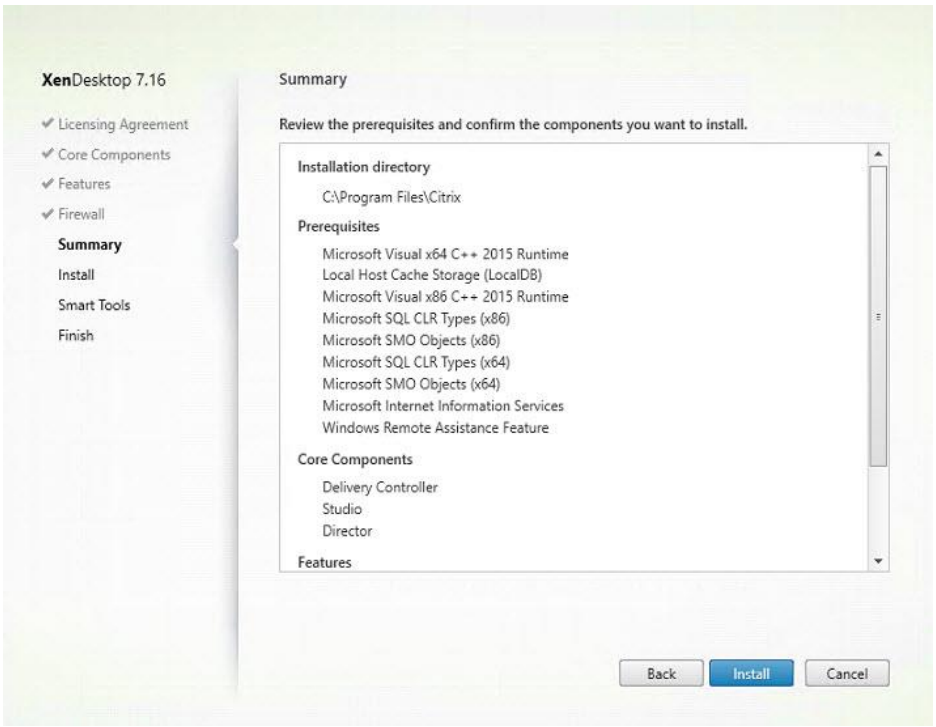


11. Select the default ports and automatically configured firewall rules.

12. Click Next.

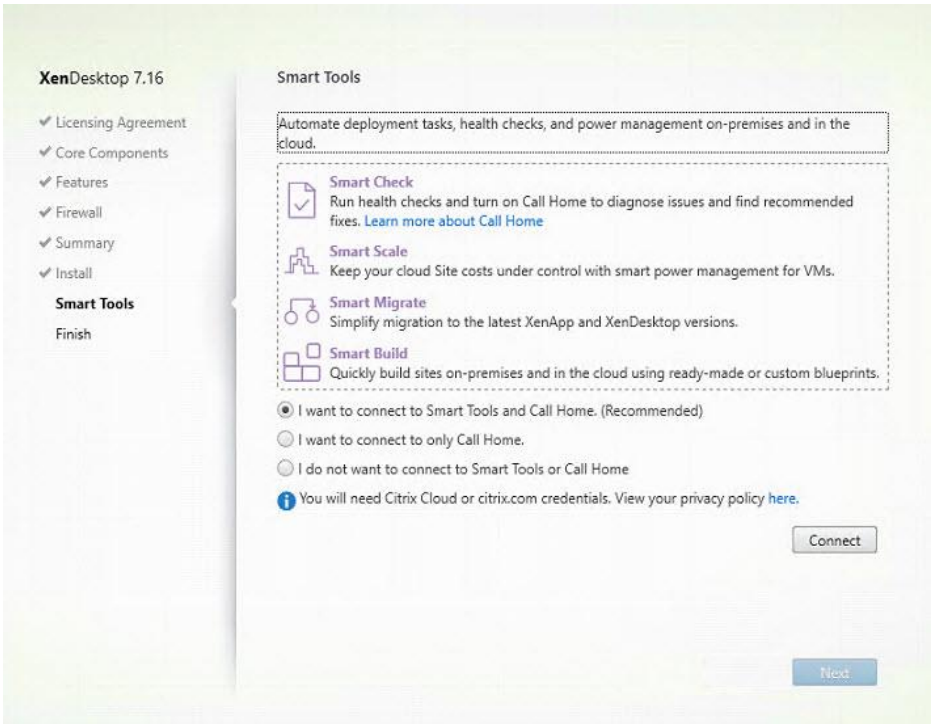


13. Click Install to begin the installation.



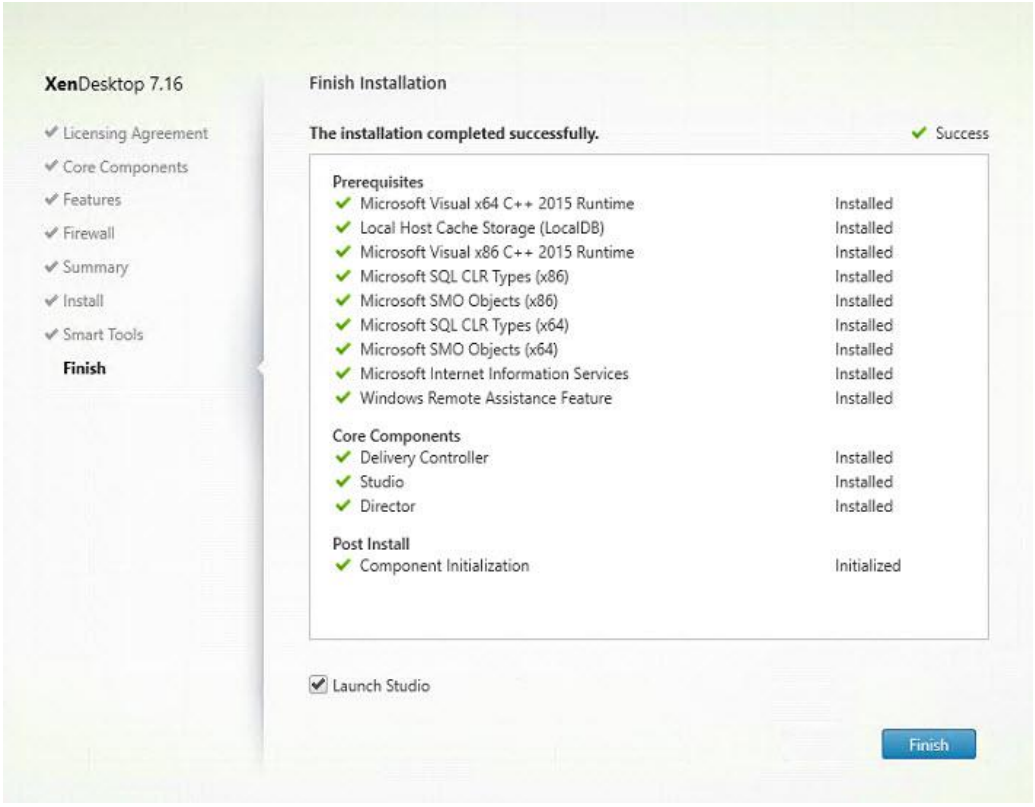
14. (Optional) Click the Call Home participation.

15. Click Next.



16. Click Finish to complete the installation.

17. (Optional) Check Launch Studio to launch Citrix Studio Console.



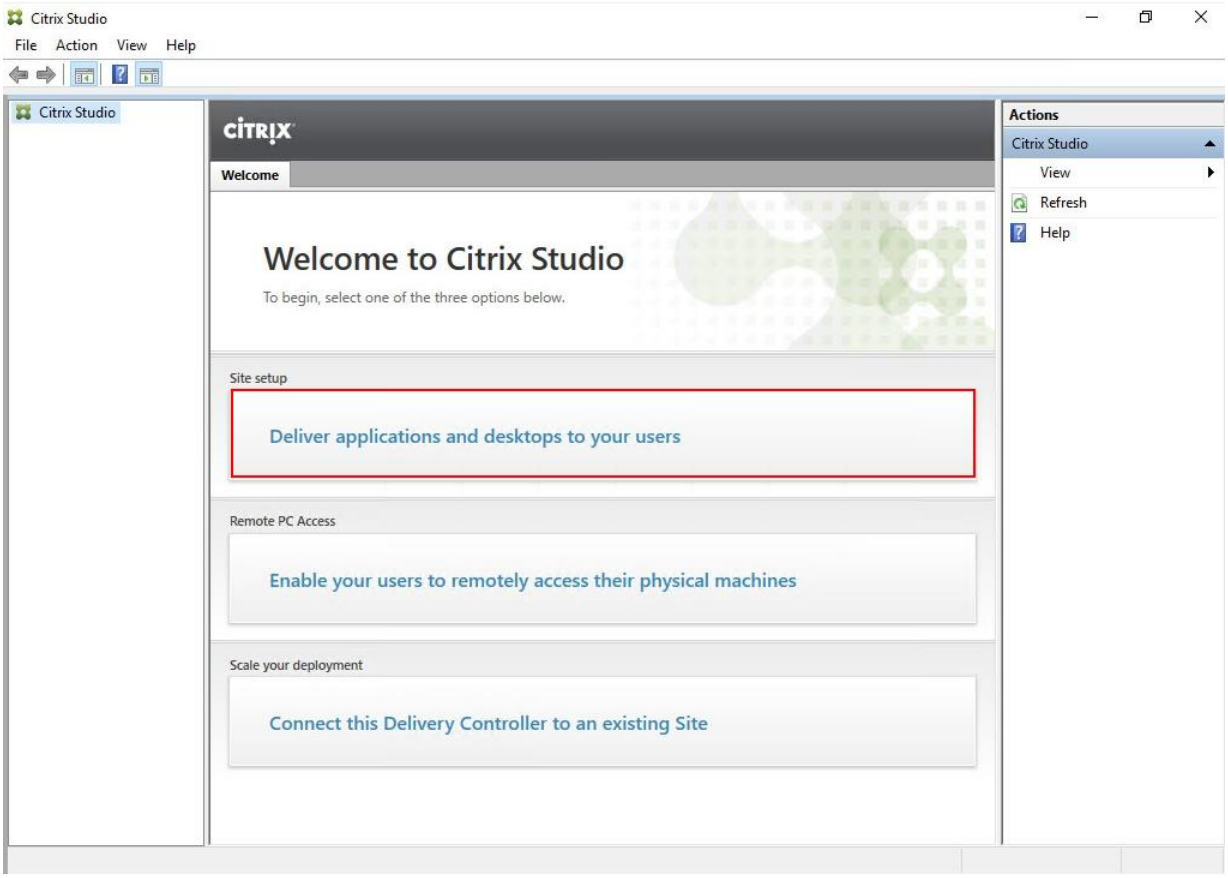
Configure the XenDesktop Site

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

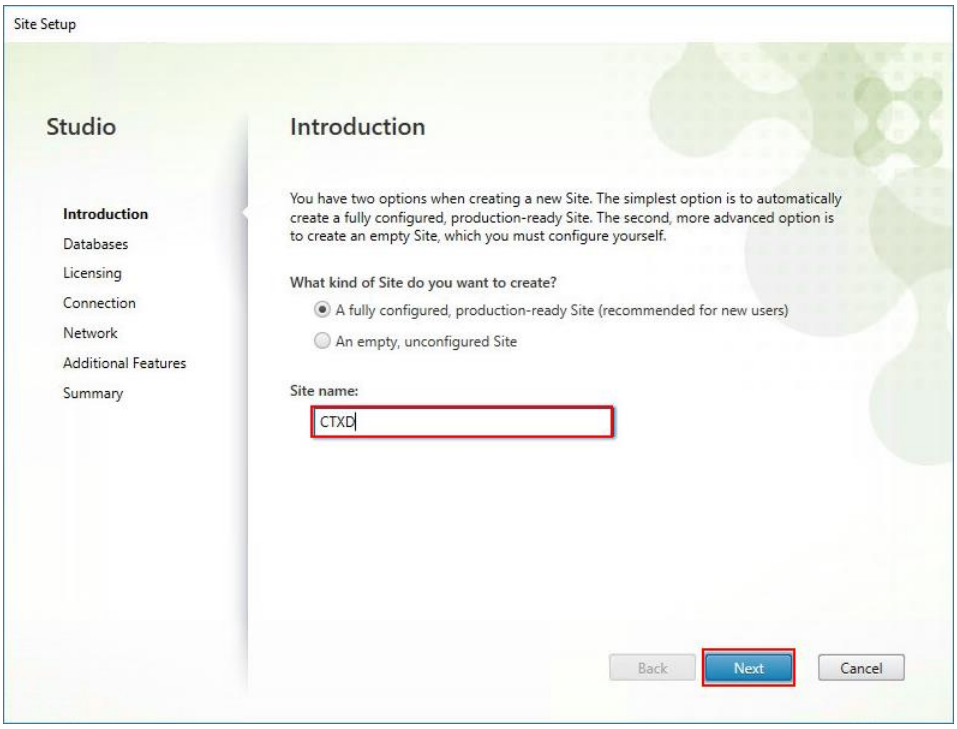
Citrix Studio launches automatically after the XenDesktop Delivery Controller installation, or if necessary, it can be launched manually. Citrix Studio is used to create a Site, which is the core XenDesktop 7.16 environment consisting of the Delivery Controller and the Database.

To configure XenDesktop, complete the following steps:

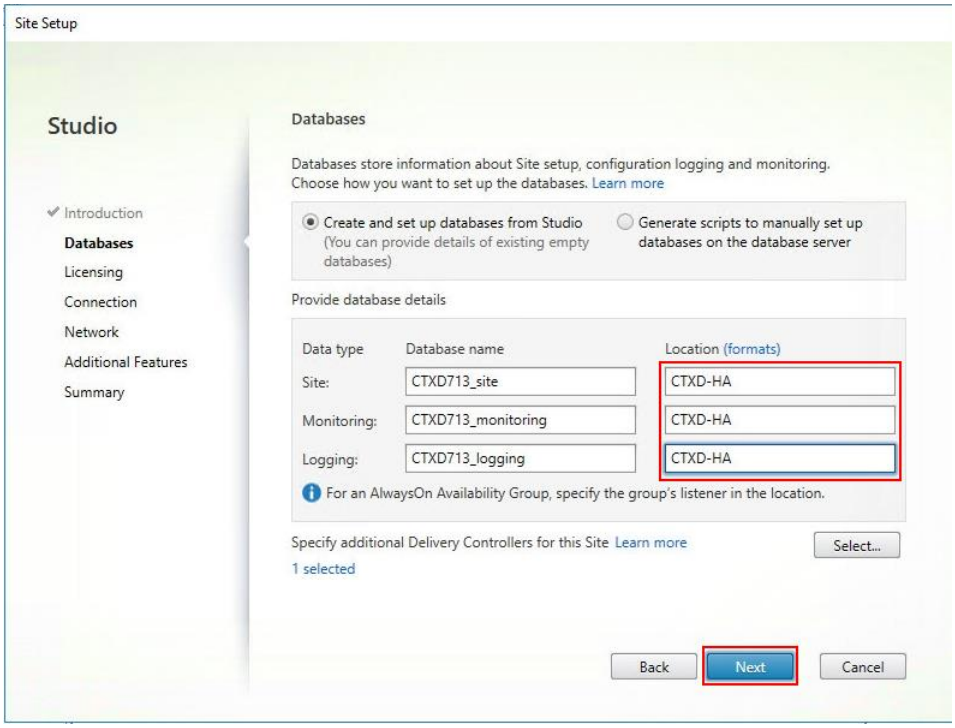
1. From Citrix Studio, click the Deliver applications and desktops to your users button.



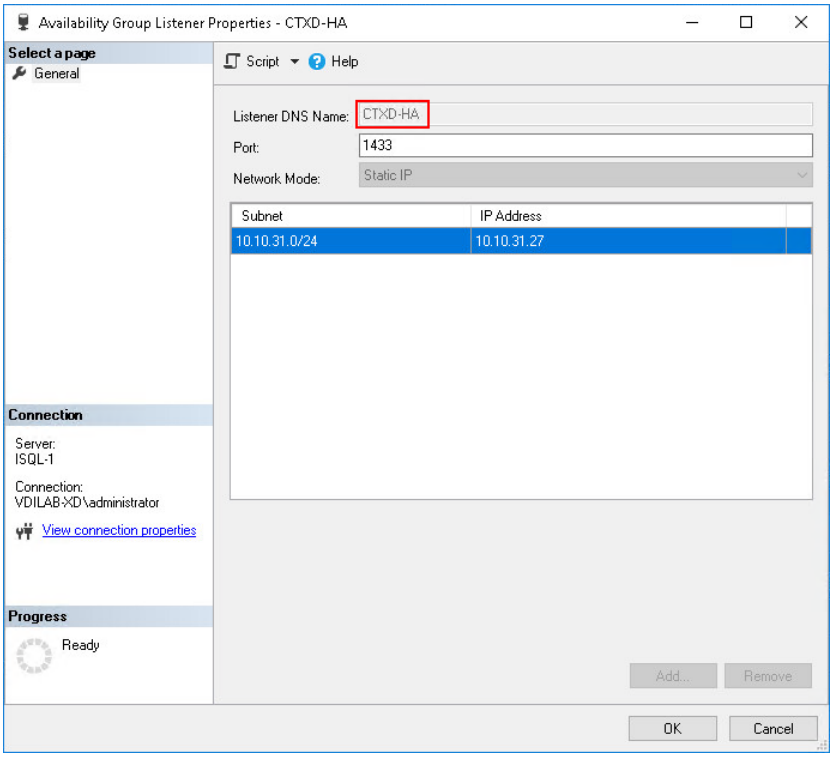
2. Select the “A fully configured, production-ready Site” radio button.
3. Enter a site name.
4. Click Next.



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



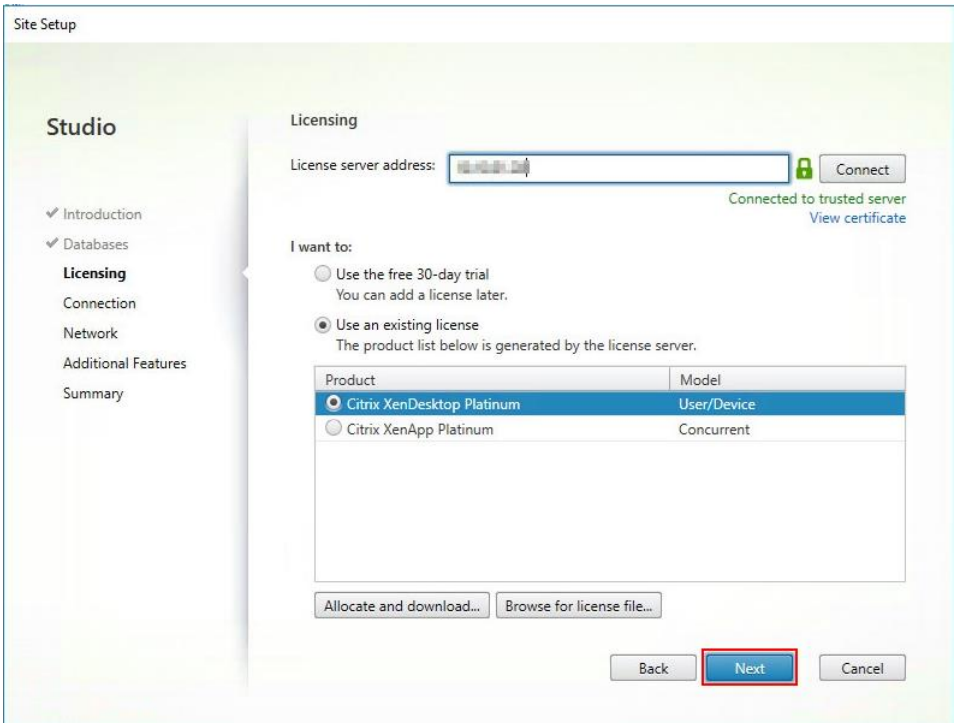
6. For an AlwaysOn Availability Group, use the group's listener DNS name.



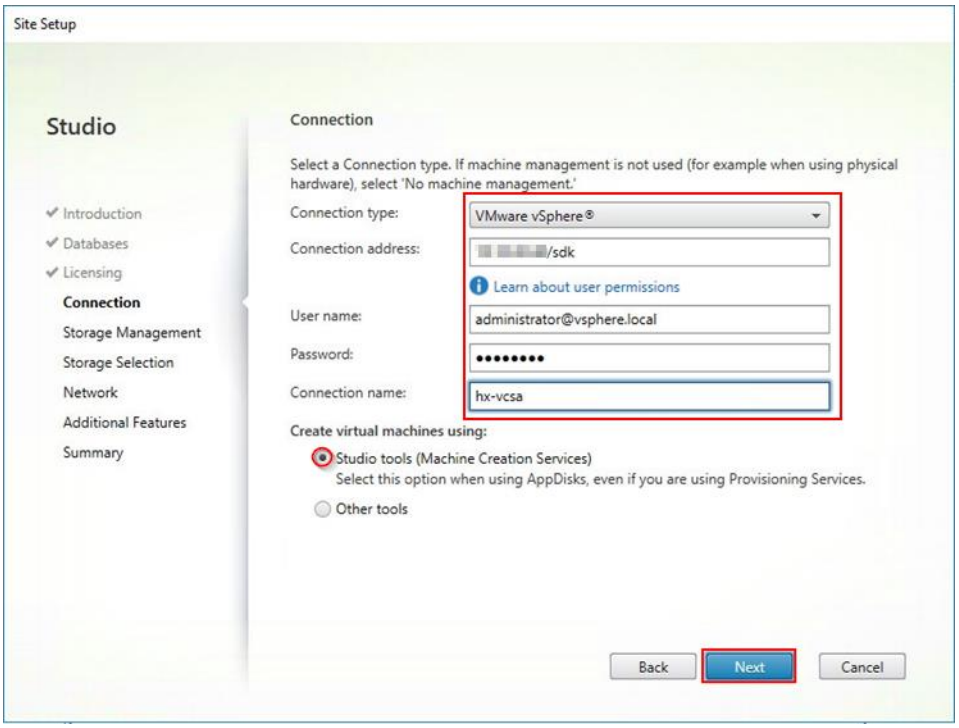
7. Provide the FQDN of the license server.
8. Click Connect to validate and retrieve any licenses from the server.

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

9. Select the appropriate product edition using the license radio button.
10. Click Next.



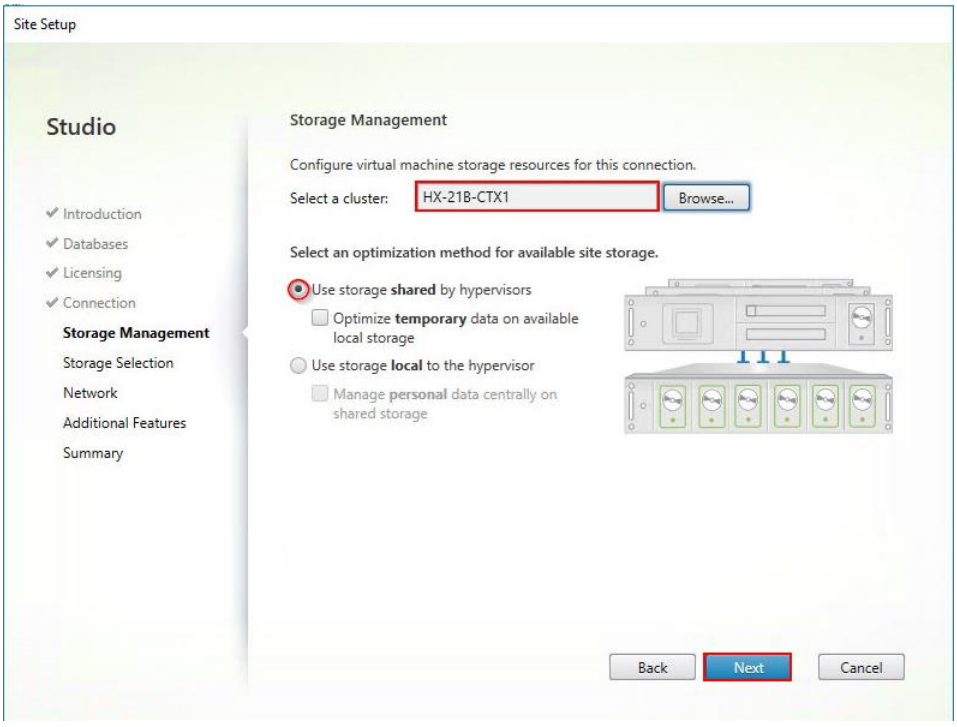
11. Select the Connection type of VMware vSphere®.
12. Enter the FQDN of the vCenter server (in Server_FQDN/sdk format).
13. Enter the username (in domain\username format) for the vSphere account.
14. Provide the password for the vSphere account.
15. Provide a connection name.
16. Select the Other tools radio button.
17. Click Next.



18. Select HyperFlex Cluster that will be used by this connection.

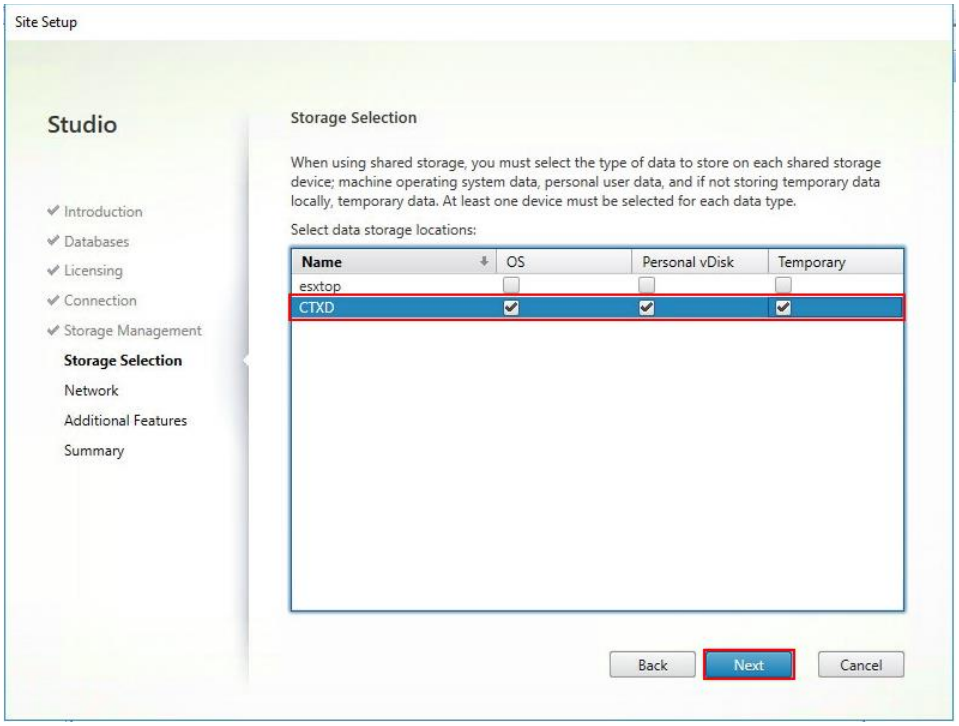
19. Check Studio Tools radio button required to support desktop provisioning task by this connection.

20. Click Next.



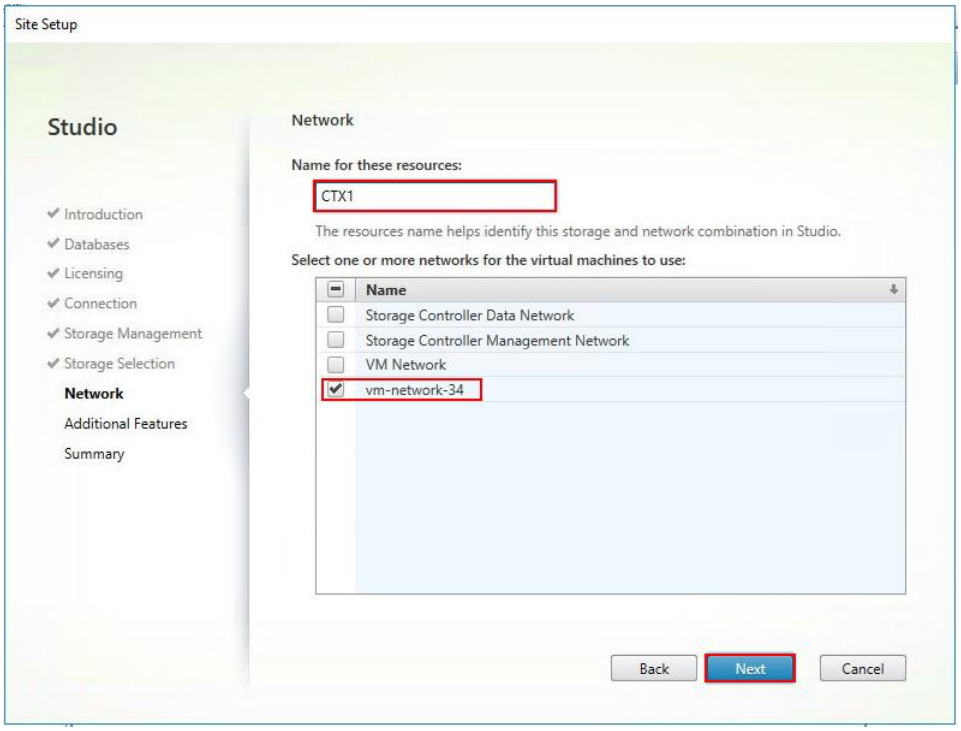
21. Make Storage selection to be used by this connection.

22. Click Next.



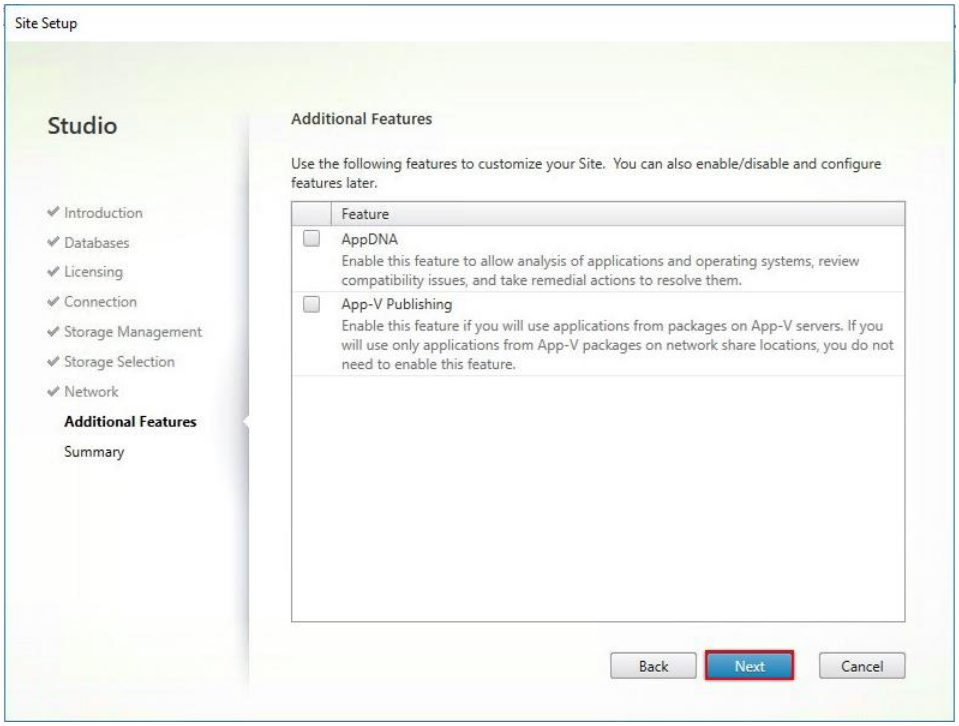
23. Make Network selection to be used by this connection.

24. Click Next.

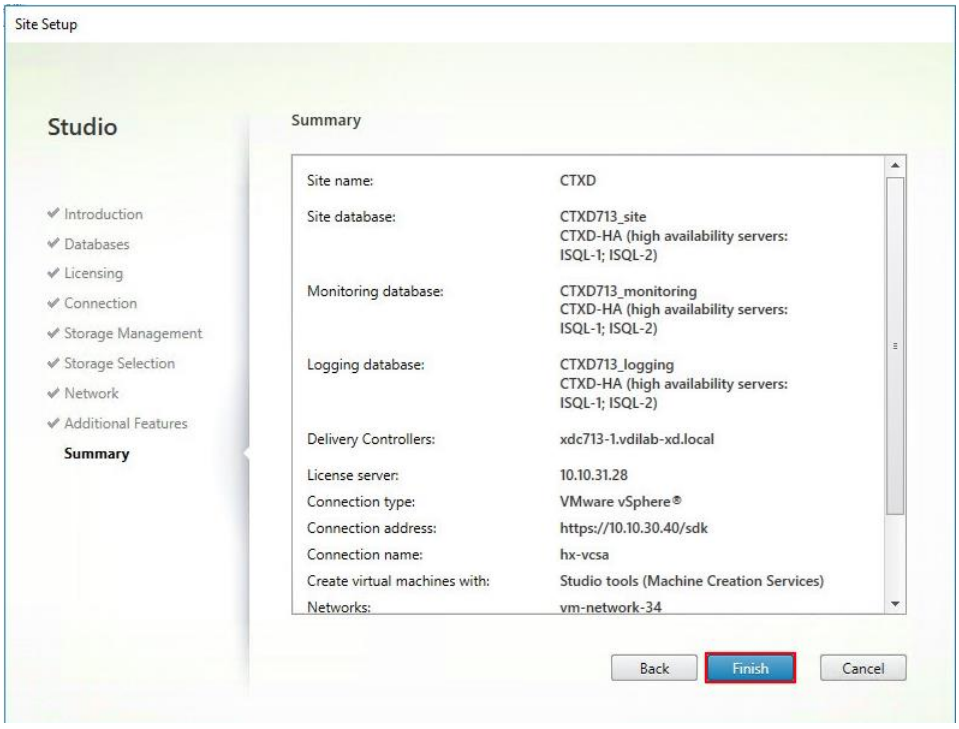


25. Select Additional features.

26. Click Next.



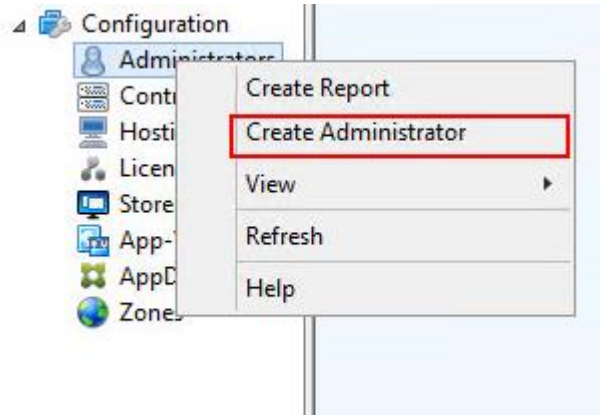
27. Review Site configuration Summary and click Finish.



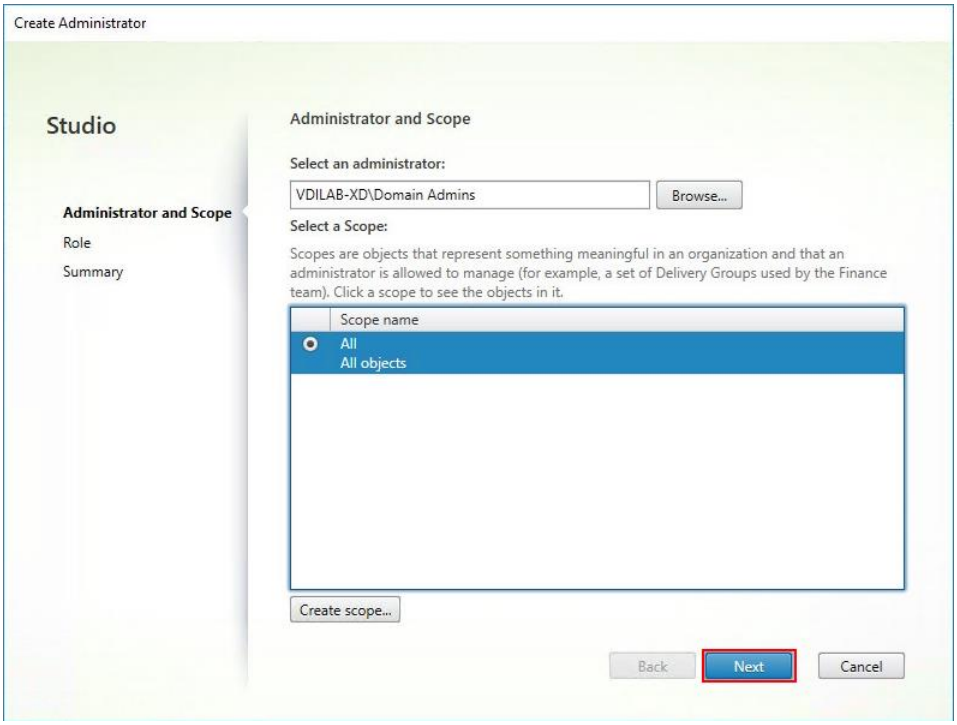
Configure the XenDesktop Site Administrators

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

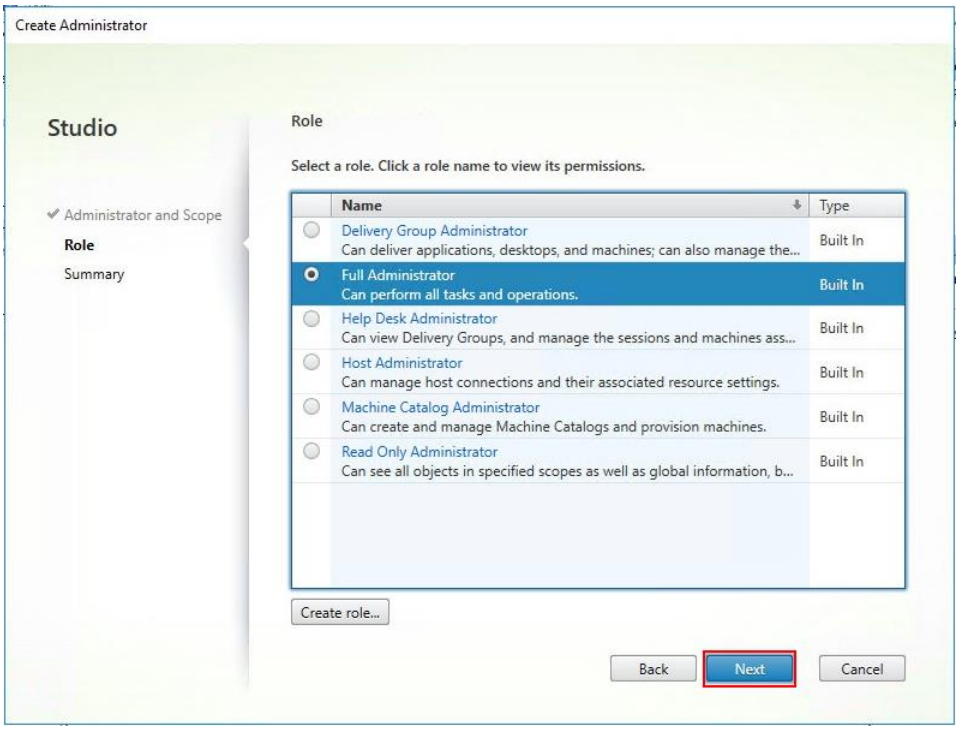
2. From the Configuration menu, right-click Administrator and select Create Administrator from the drop-down list.



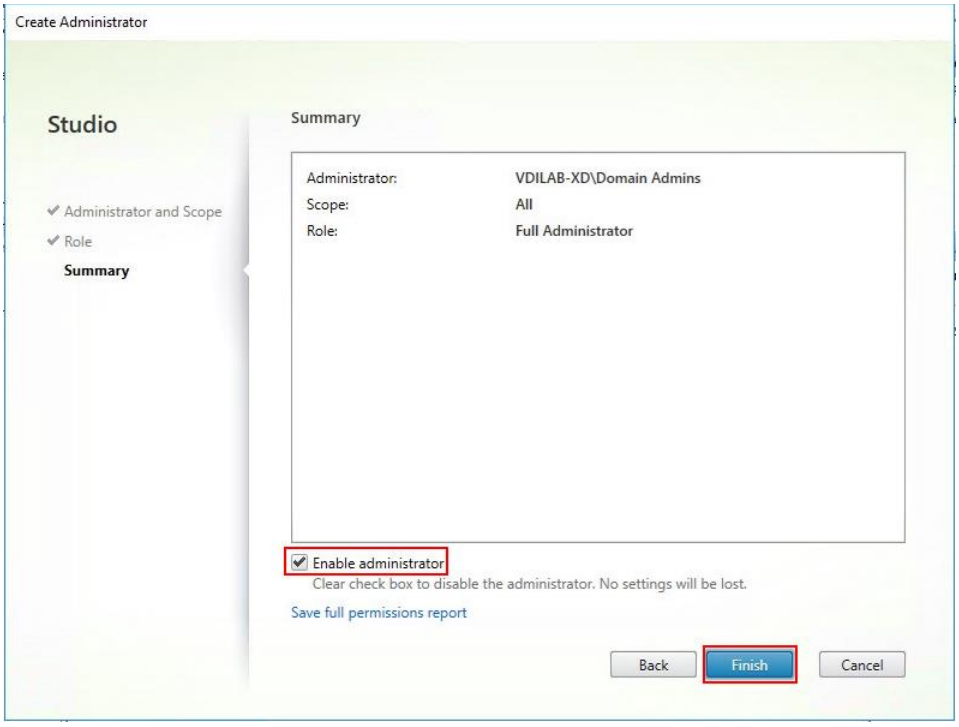
3. Select/Create appropriate scope and click Next.



4. Choose an appropriate Role.



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



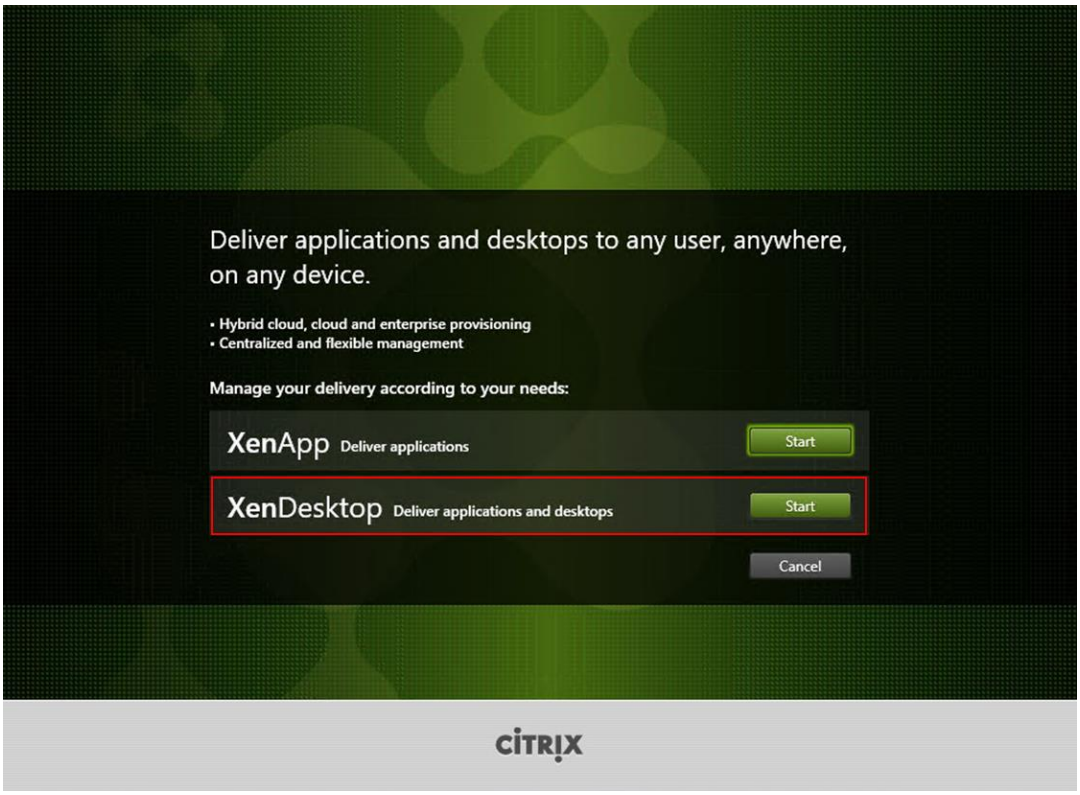
Configure additional XenDesktop Controller

After the first controller is completely configured and the Site is operational, you can add additional controllers. In this CVD, we created two Delivery Controllers.

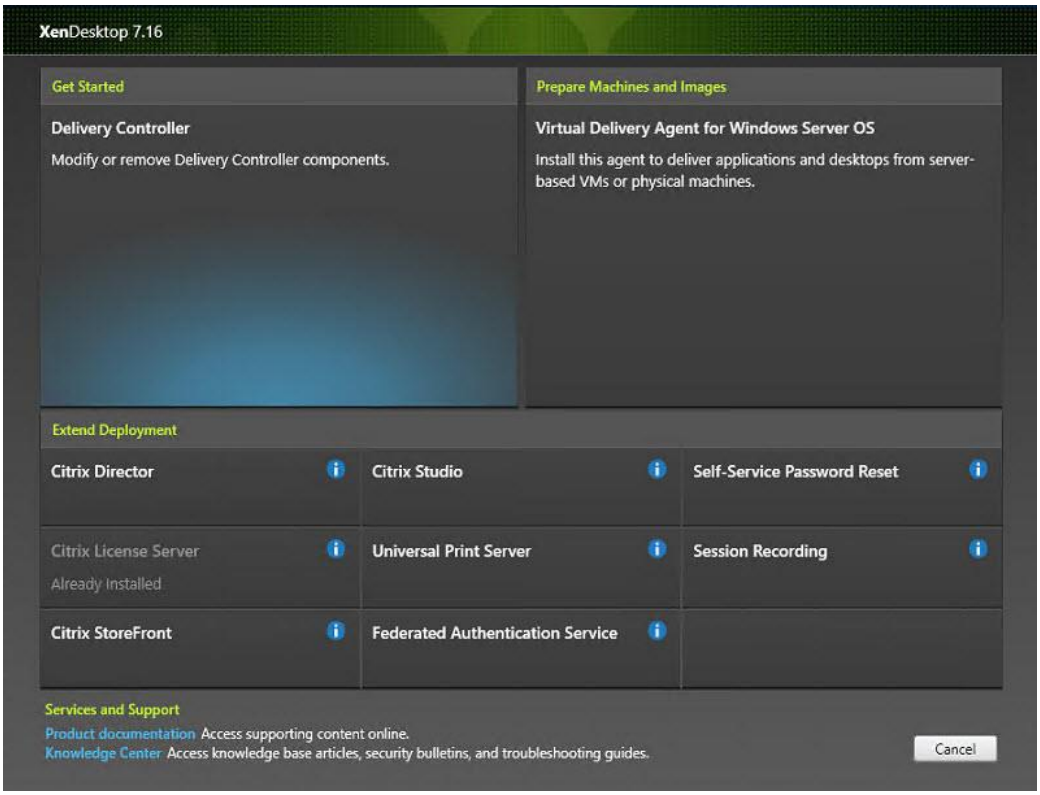
To configure additional XenDesktop controllers, complete the following steps:

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

2. Click Start.



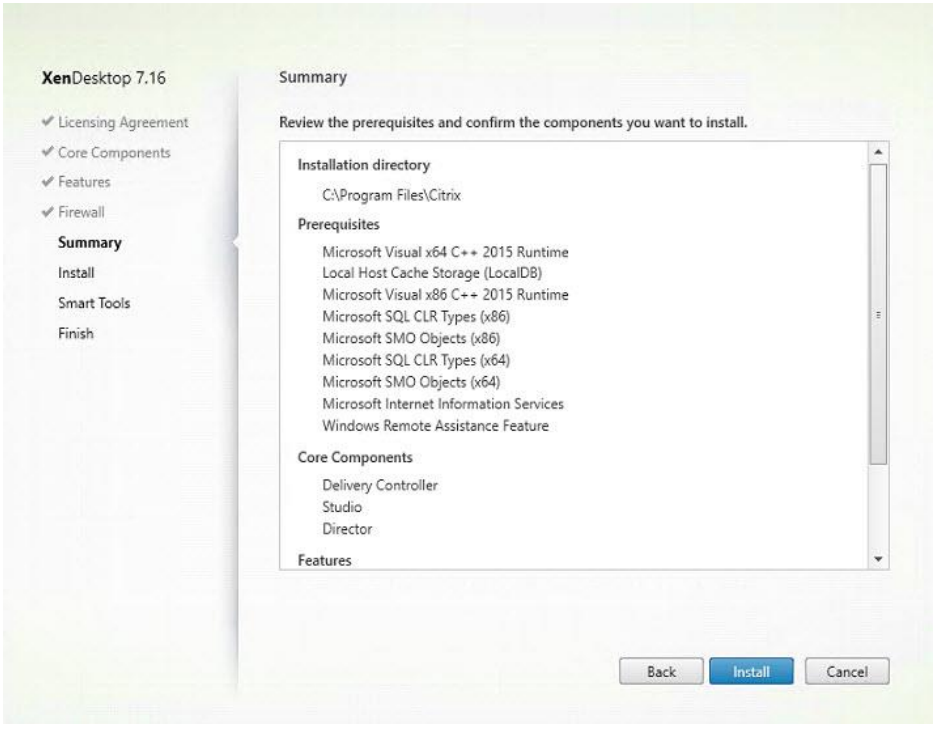
3. Click Delivery Controller.



4. Repeat the same steps used to install the first Delivery Controller, including the step of importing an SSL certificate for HTTPS between the controller and vSphere.

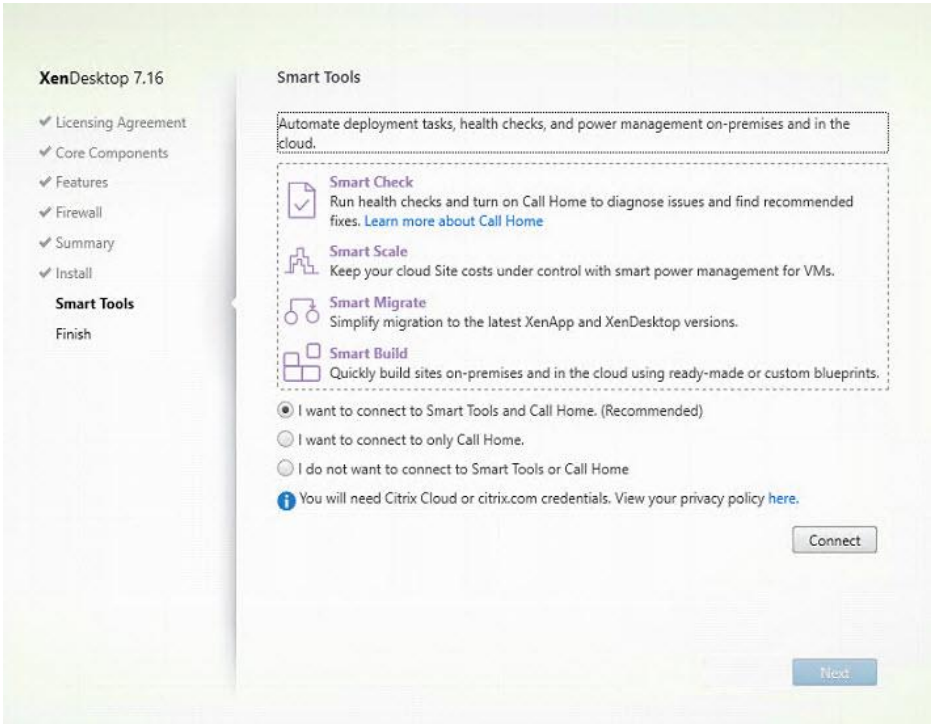
5. Review the Summary configuration.

6. Click Install.



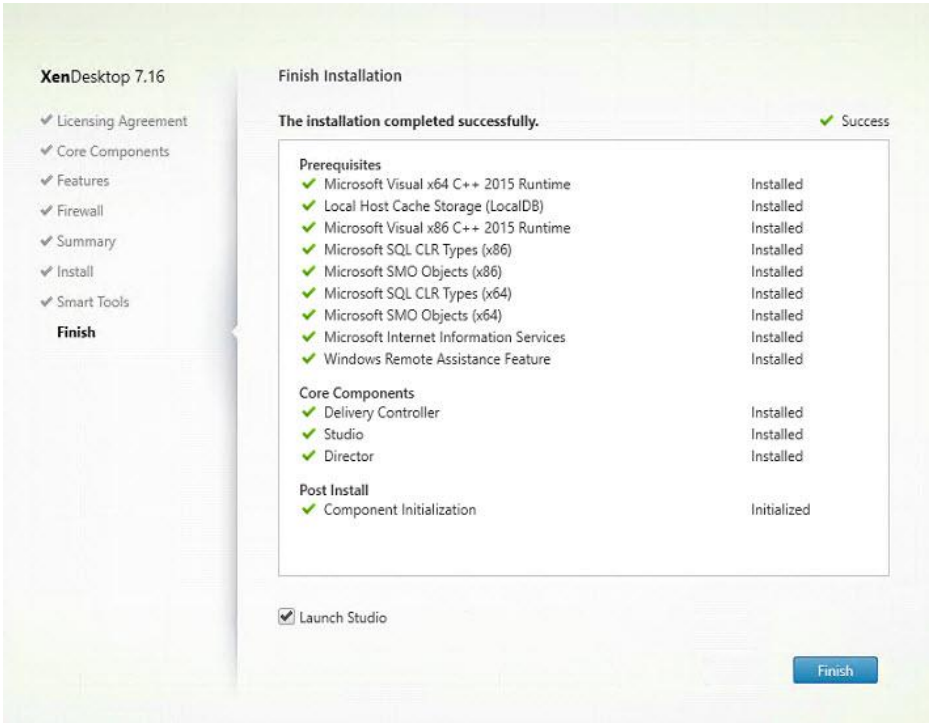
7. (Optional) Click the “I want to participate in Call Home.”

8. Click Next.



9. Verify the components installed successfully.

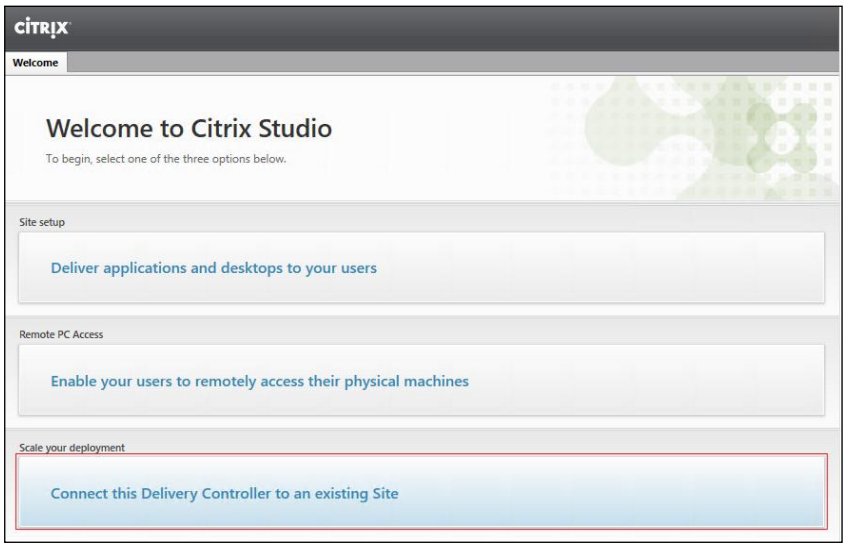
10. Click Finish.



Add the Second Delivery Controller to the XenDesktop Site

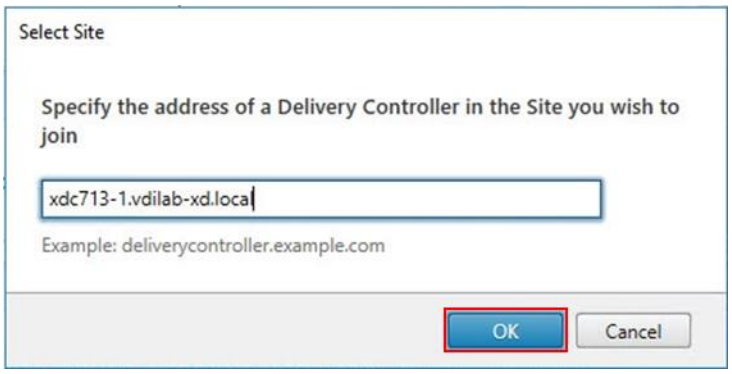
To add the second Delivery Controller to the XenDesktop Site, complete the following steps:

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



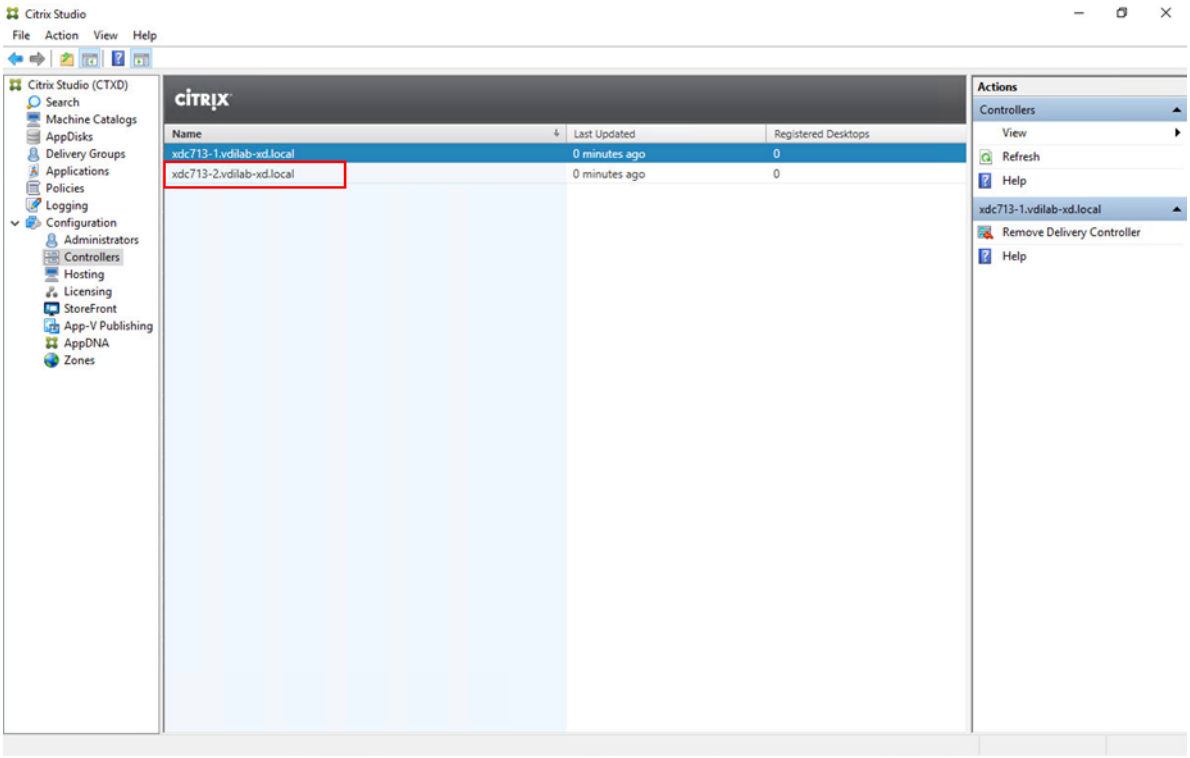
2. Enter the FQDN of the first delivery controller.

3. Click OK.



4. Click Yes to allow the database to be updated with this controller’s information automatically.

5. When complete, test the site configuration and verify the Delivery Controller has been added to the list of Controllers.



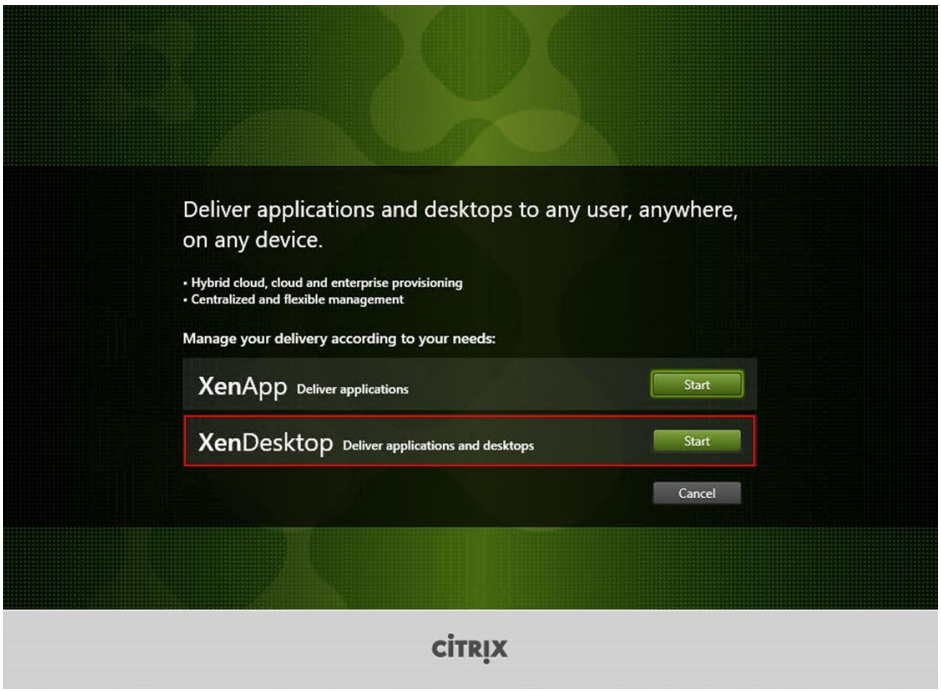
Install and Configure StoreFront

Citrix StoreFront stores aggregate desktops and applications from XenDesktop sites, making resources readily available to users. In this CVD, we created two StoreFront servers on dedicated virtual machines.

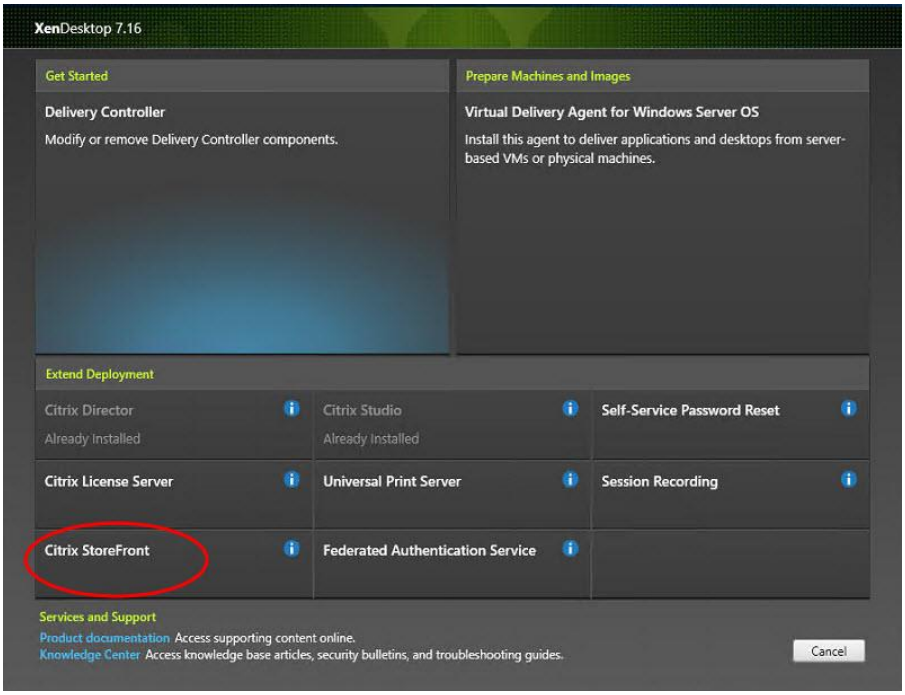
To install and configure StoreFront, complete the following steps:

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

2. Click Start.

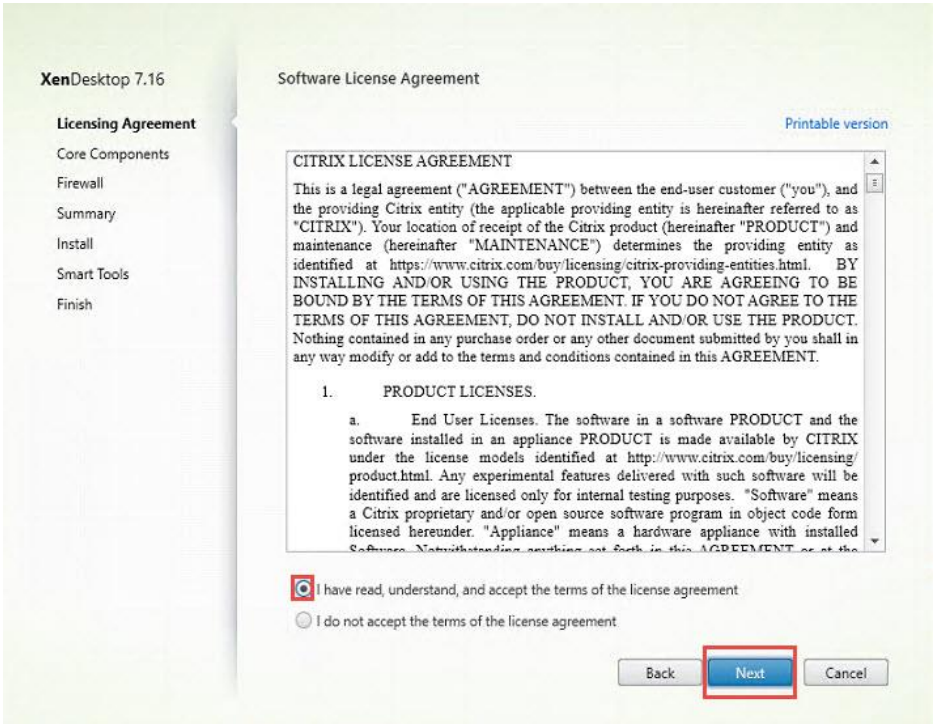


3. Click Extend Deployment Citrix StoreFront.

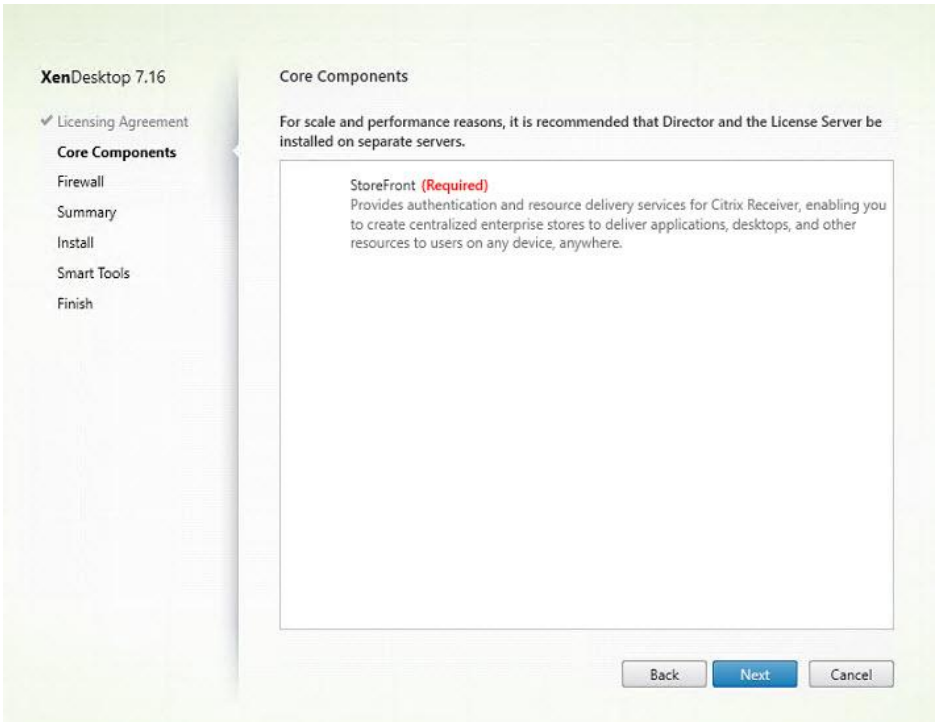


4. If acceptable, indicate your acceptance of the license by selecting the “I have read, understand, and accept the terms of the license agreement” radio button.

5. Click Next.

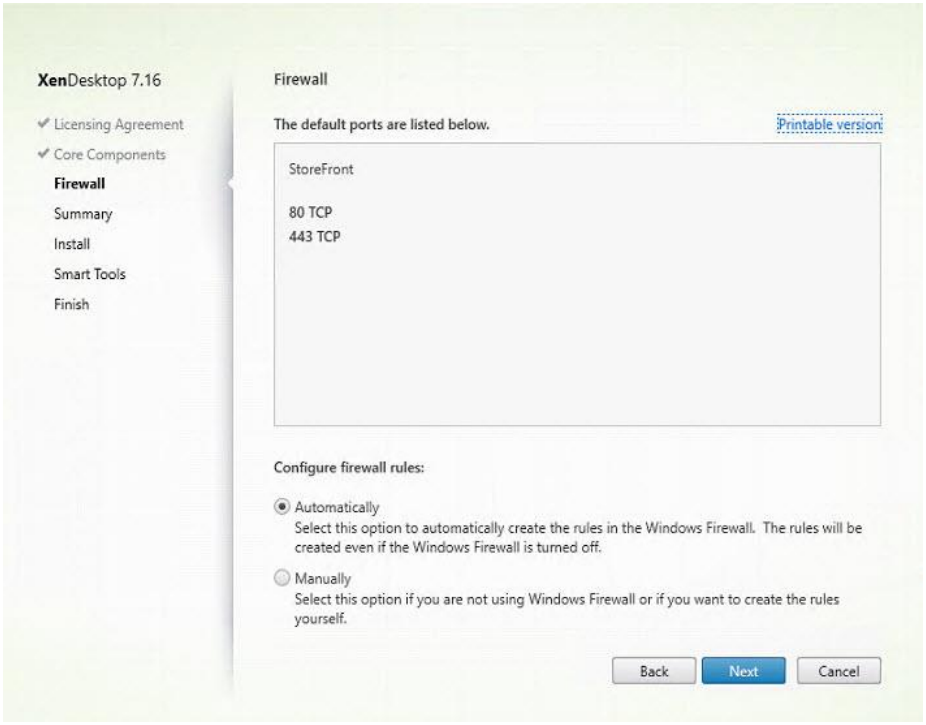


6. Click Next.

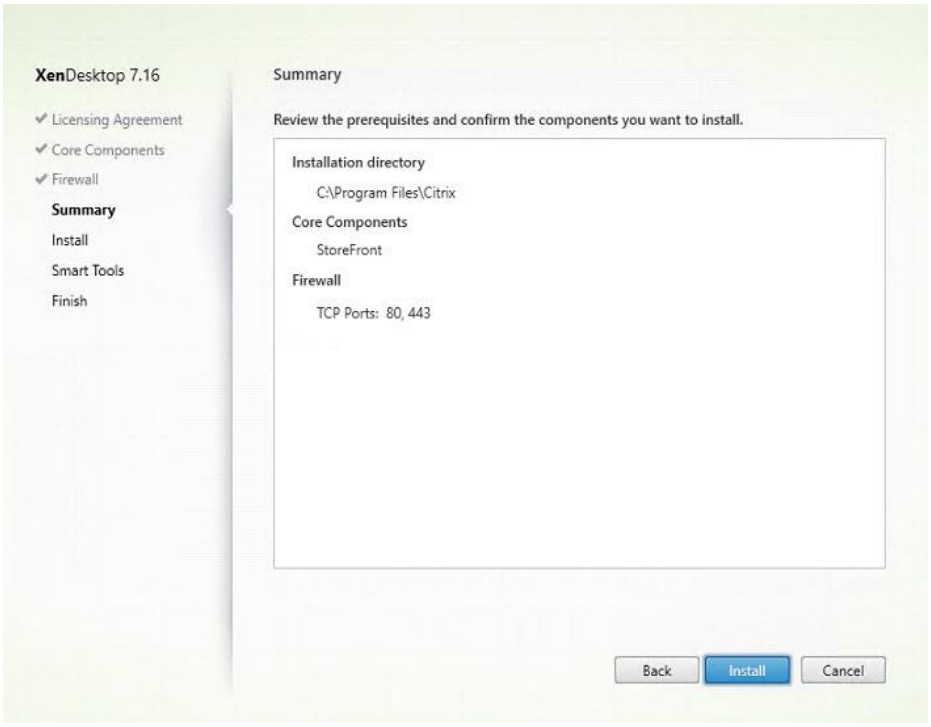


7. Select the default ports and automatically configured firewall rules.

8. Click Next.

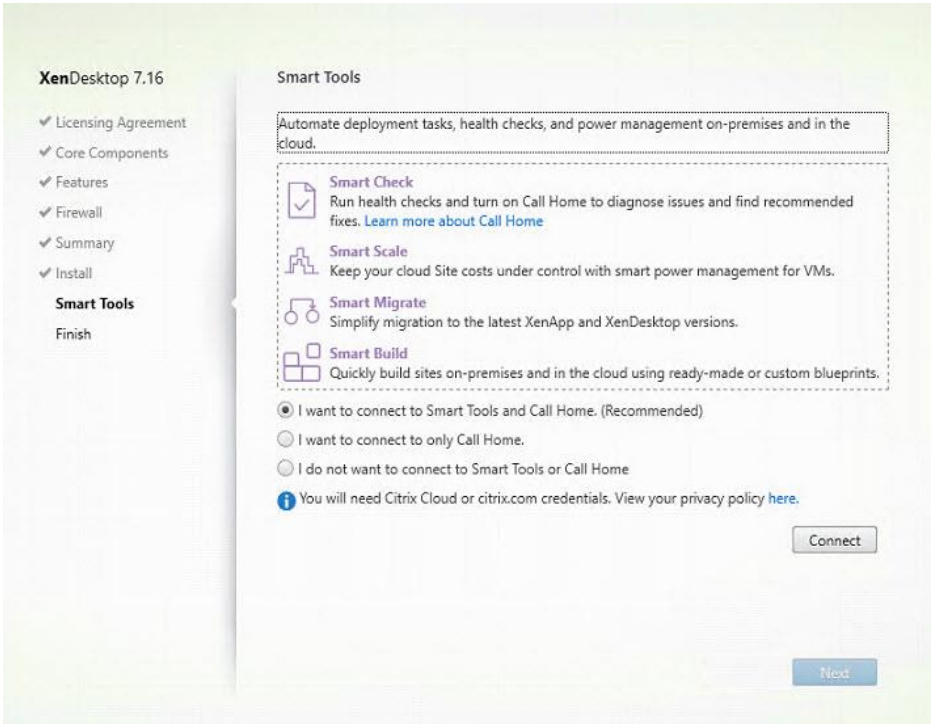


9. Click Install.



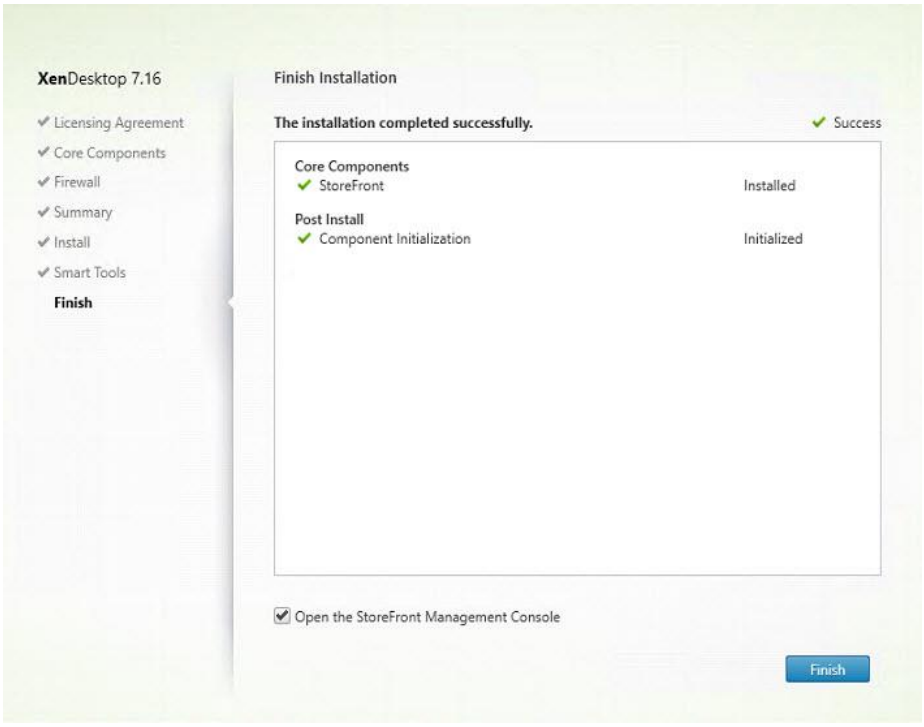
10. (Optional) Click “I want to participate in Call Home.”

11. Click Next.

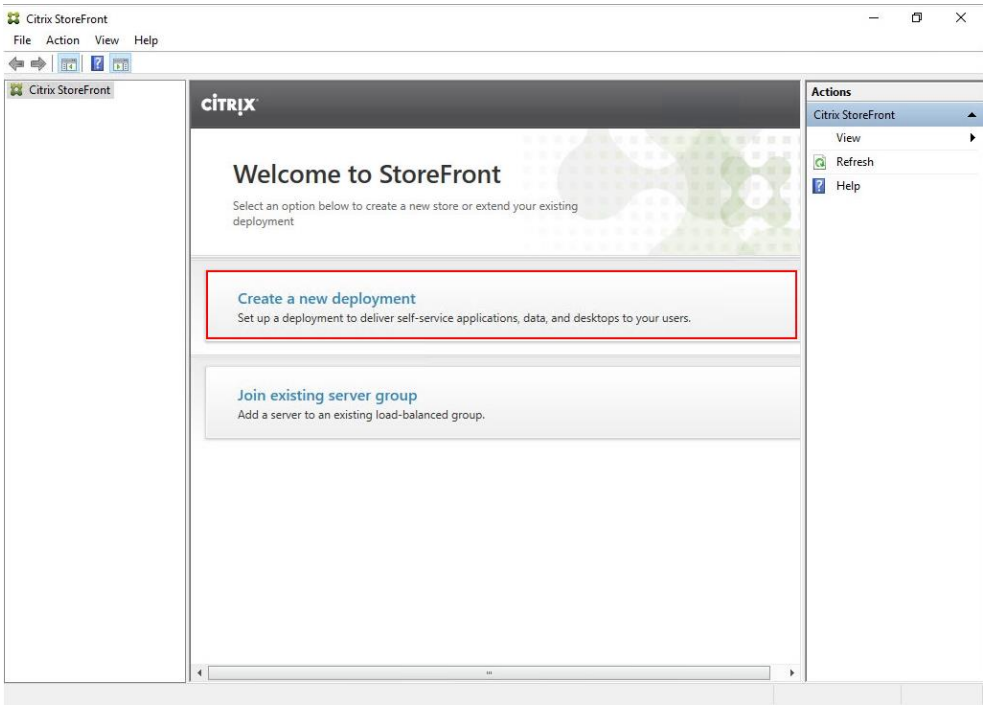


12. Check “Open the StoreFront Management Console.

13. Click Finish.

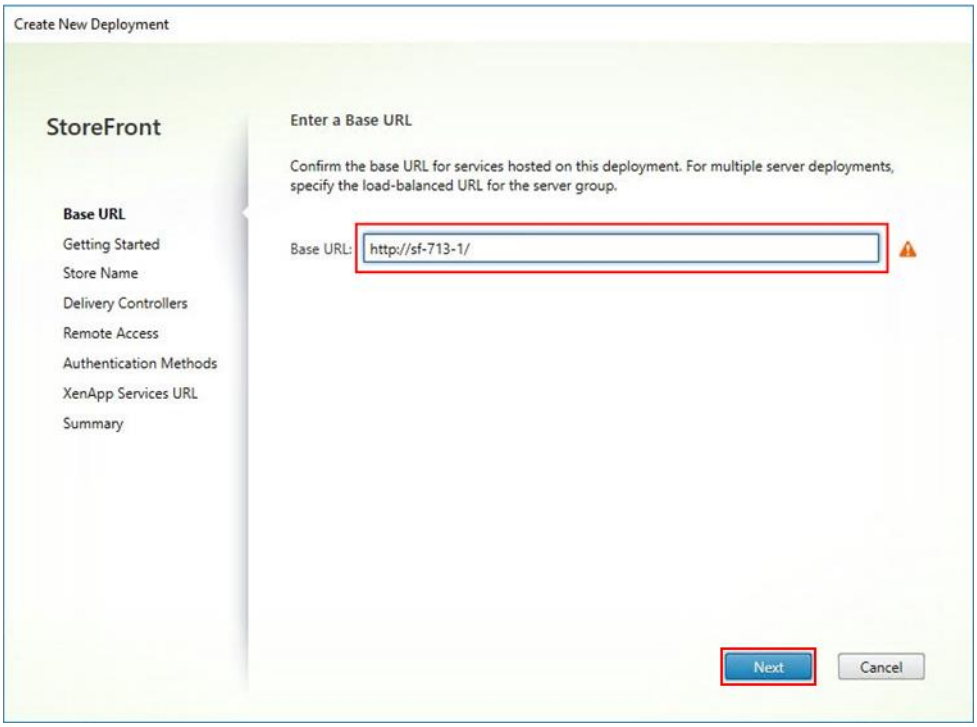


14. Click Create a new deployment.

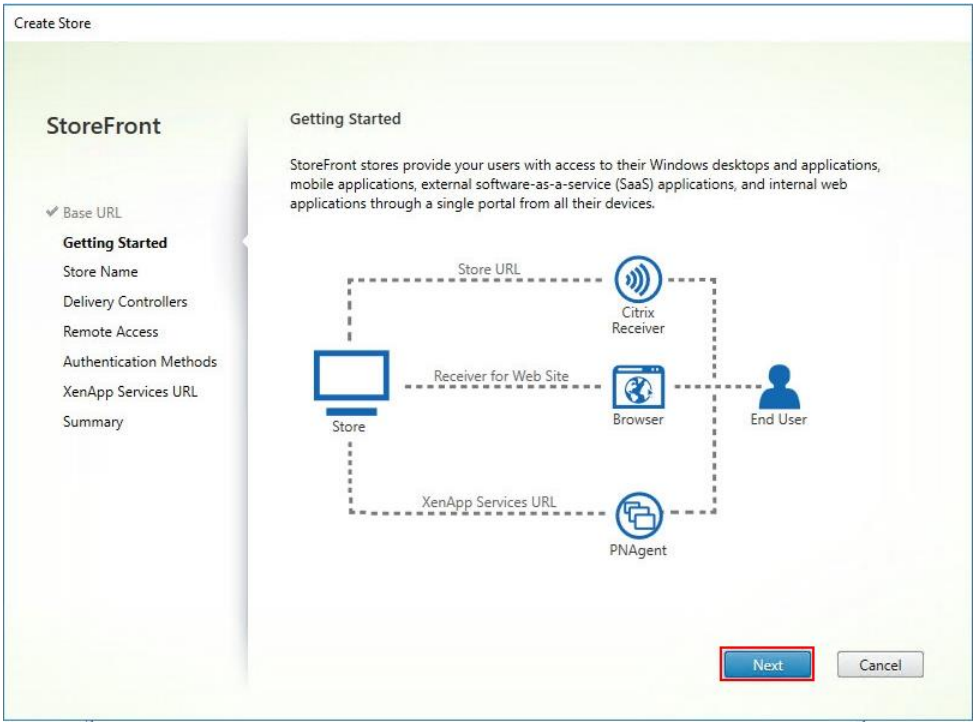


15. Specify the URL of the StoreFront server and click Next.

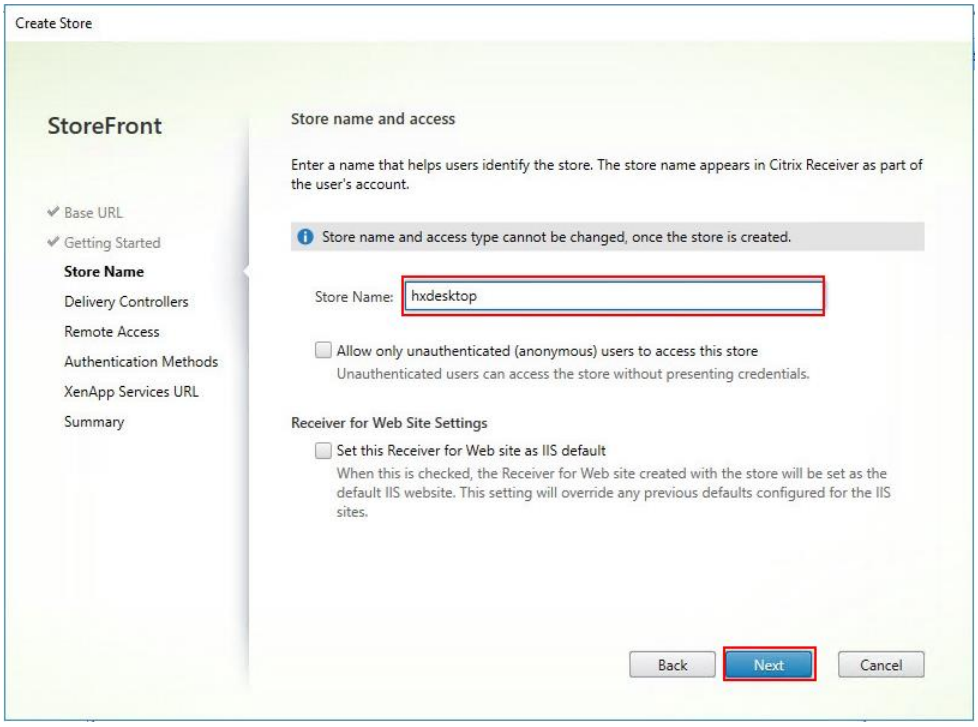
For a multiple server deployment use the load balancing environment in the Base URL box.



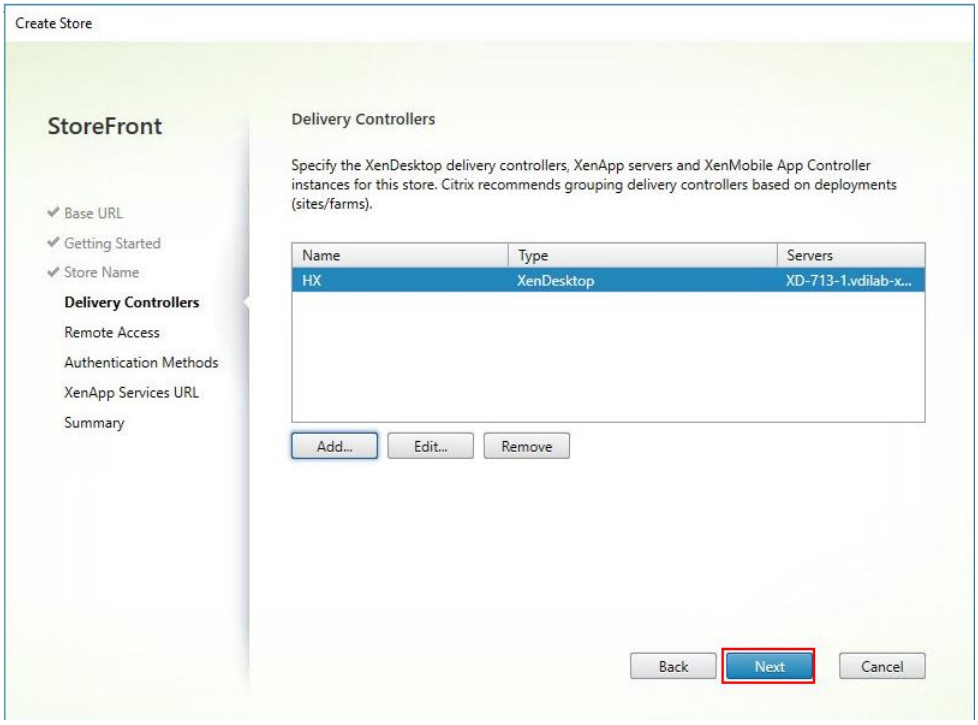
16. Click Next.



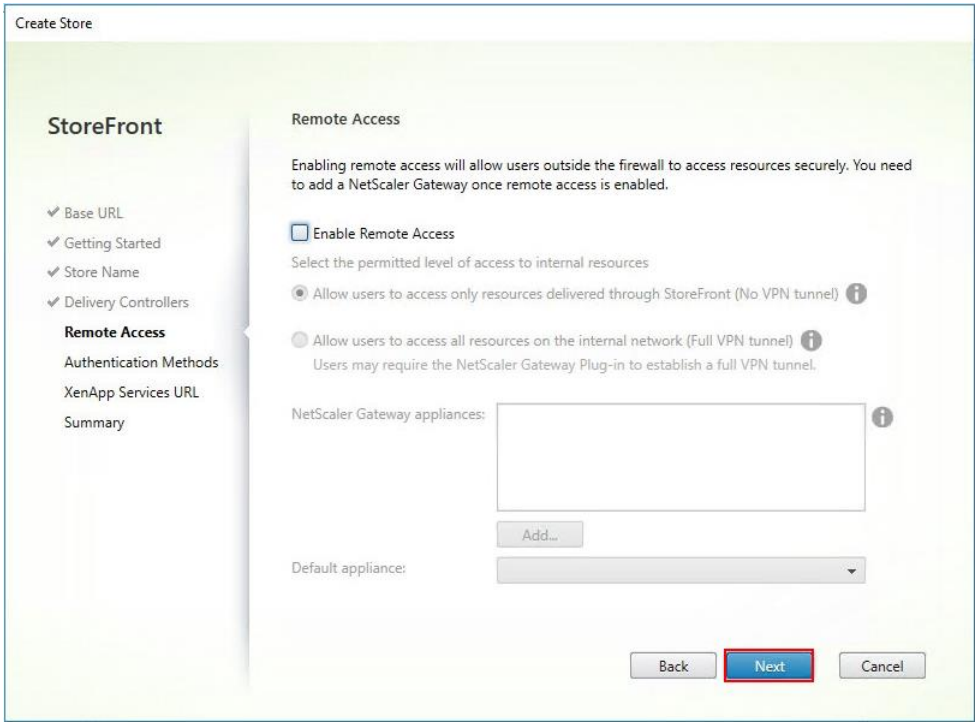
17. Specify a name for your store and click Next.



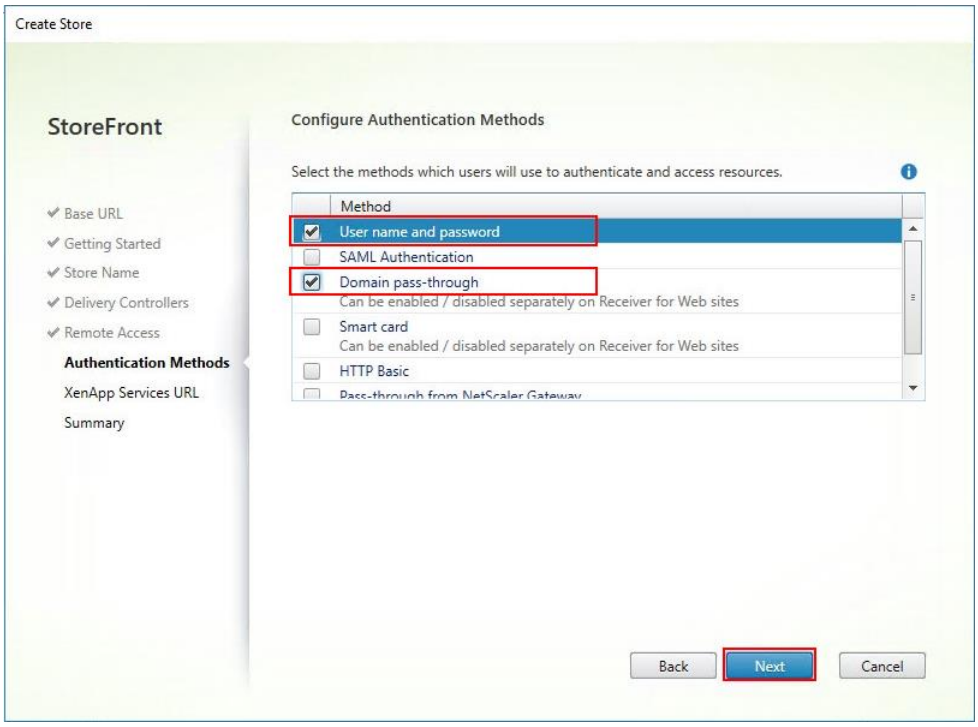
18. Add the required Delivery Controllers to the store and click Next.



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



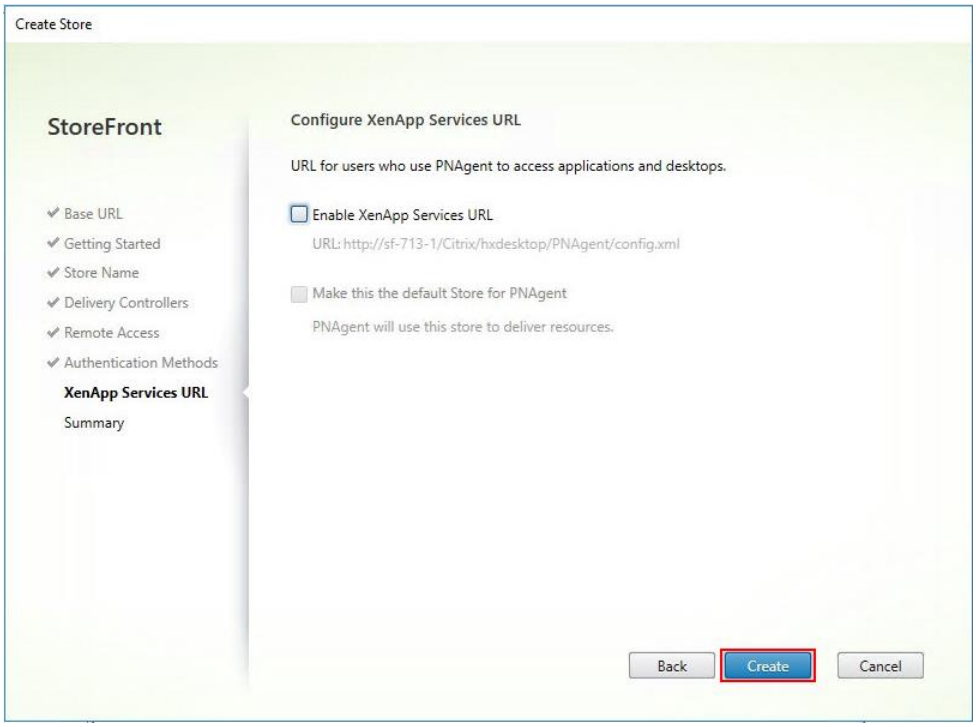
20. On the ”Authentication Methods” page, select the methods your users will use to authenticate to the store and click Next. You can select from the following methods:



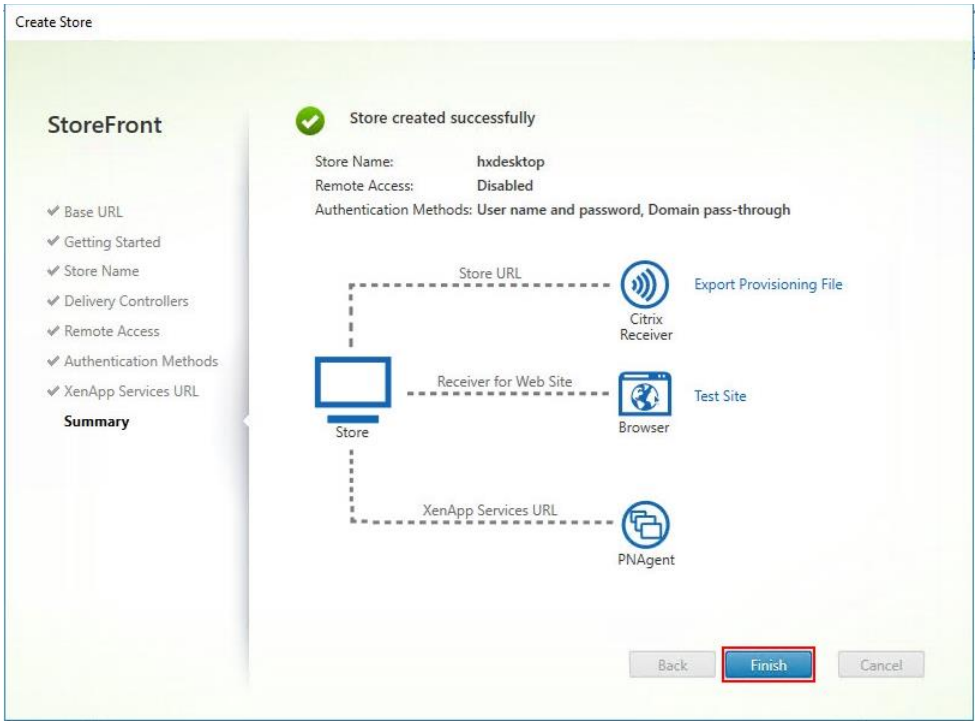
21. Username and password: Users enter their credentials and are authenticated when they access their stores.

22. Domain passthrough: Users authenticate to their domain-joined Windows computers and their credentials are used to log them on automatically when they access their stores.

23. Configure the XenApp Service URL for users who use PNAgent to access the applications and desktops and click Create.



24. After creating the store click Finish.



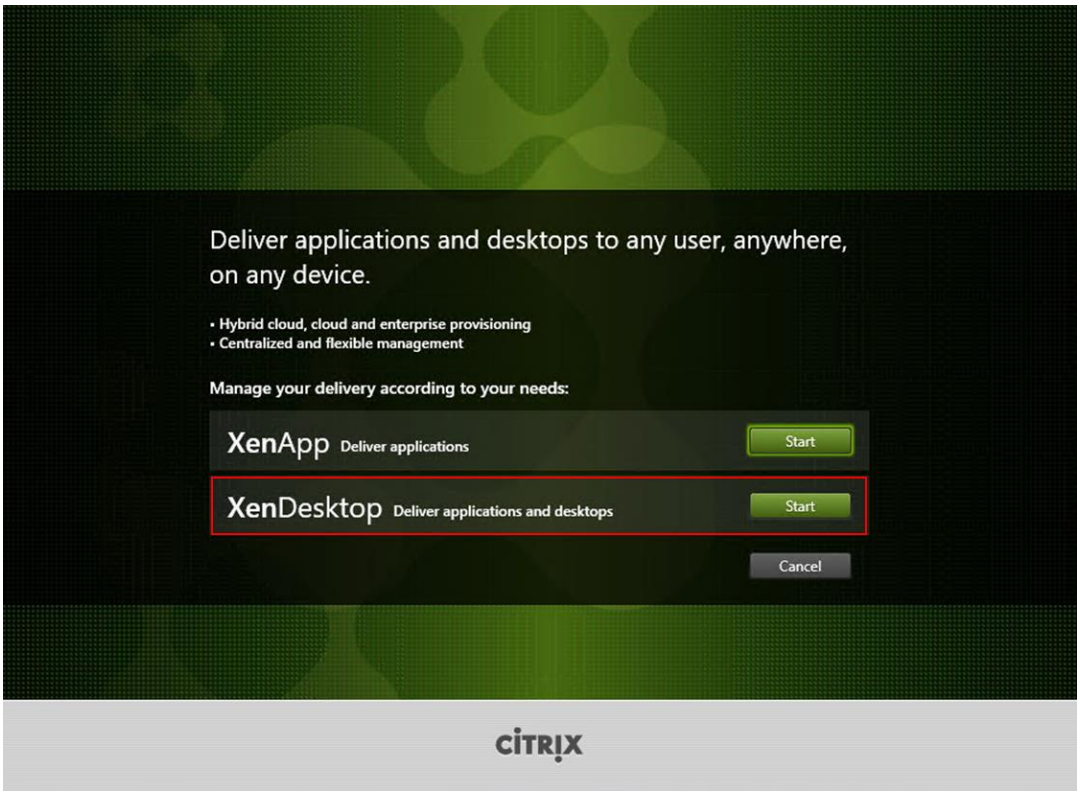
Additional StoreFront Configuration

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

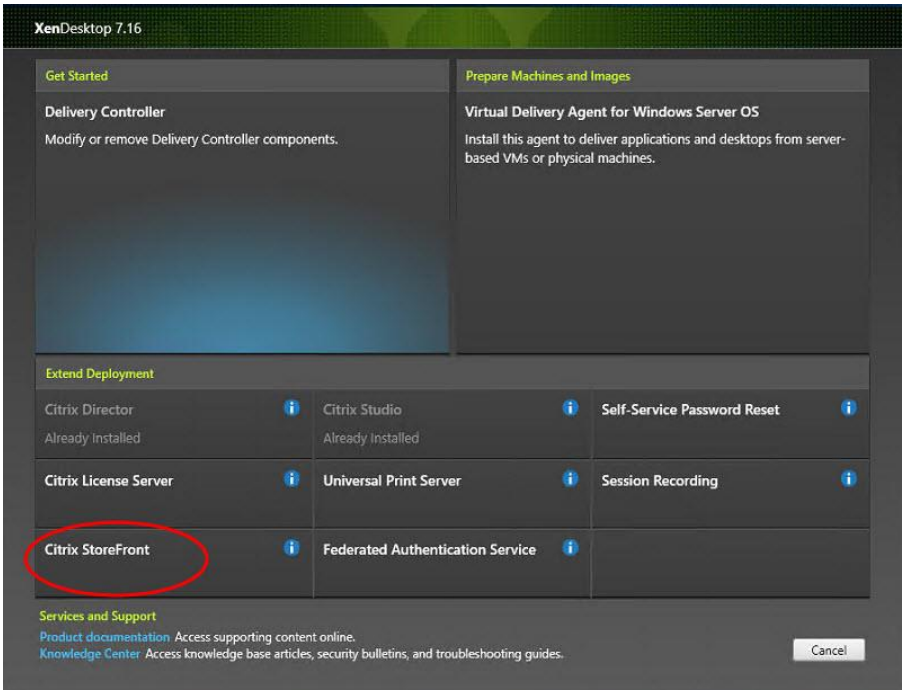
To configure additional StoreFront server, complete the following steps:

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

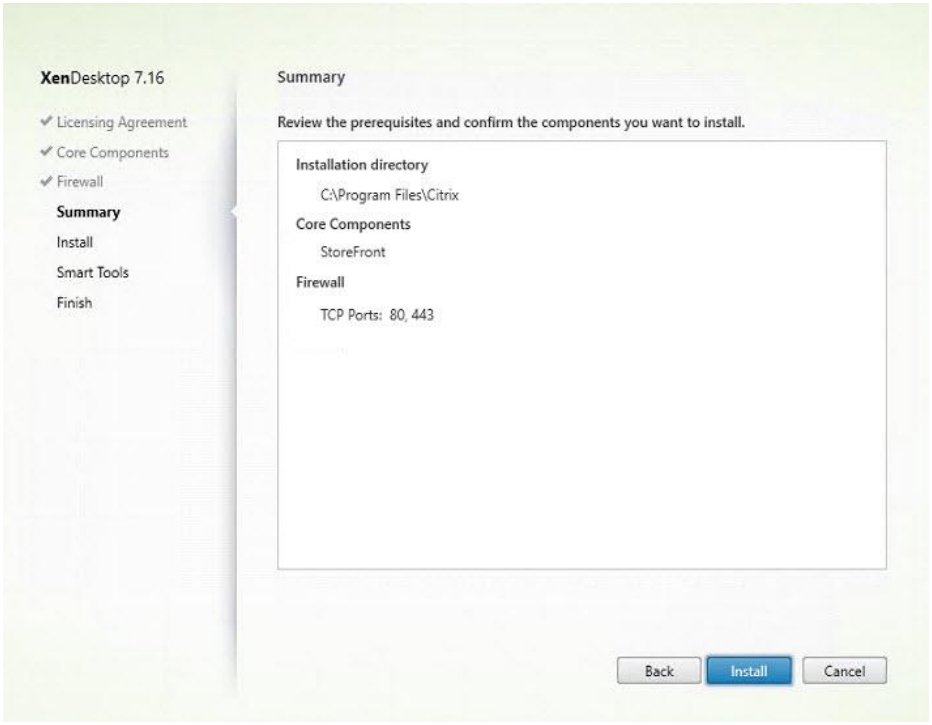
2. Click Start.



3. Click Extended Deployment Citrix StoreFront.

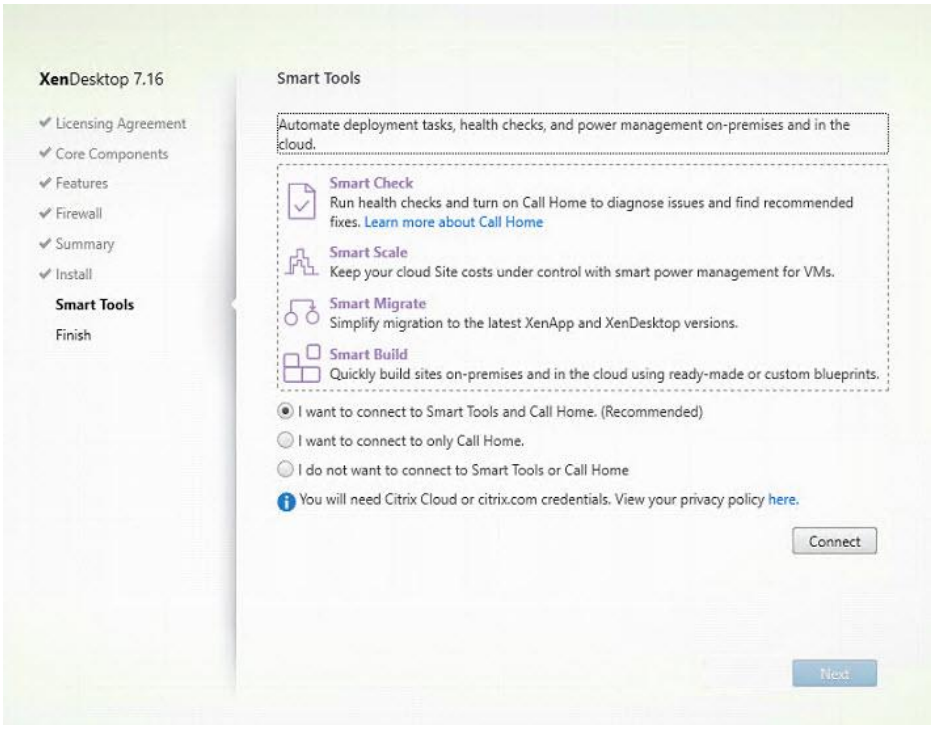


4. Repeat the same steps used to install the first StoreFront.
5. Review the Summary configuration.
6. Click Install.



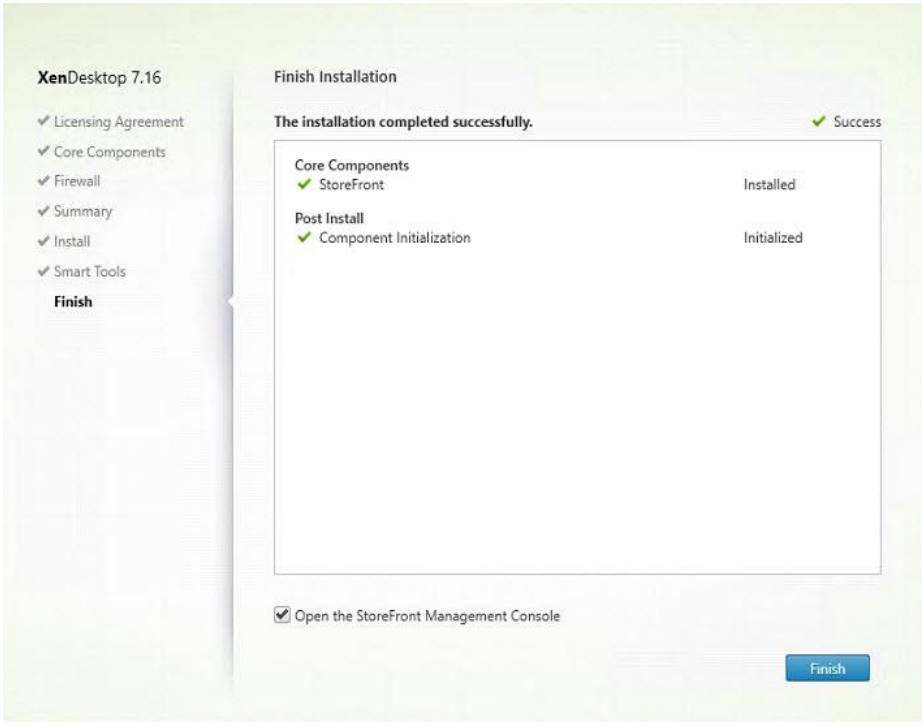
7. (Optional) Click “I want to participate in Call Home.”

8. Click Next.



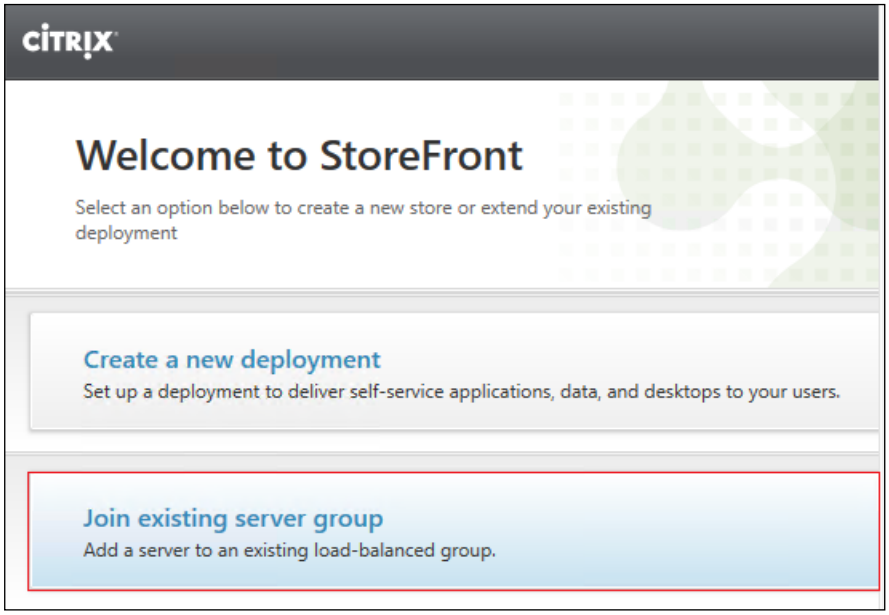
9. Check “Open the StoreFront Management Console."

10. Click Finish.

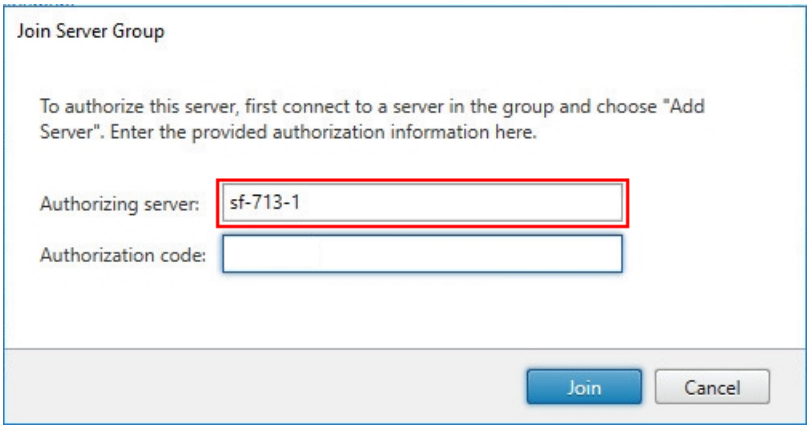


To configure the second StoreFront if used, complete the following steps:

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



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



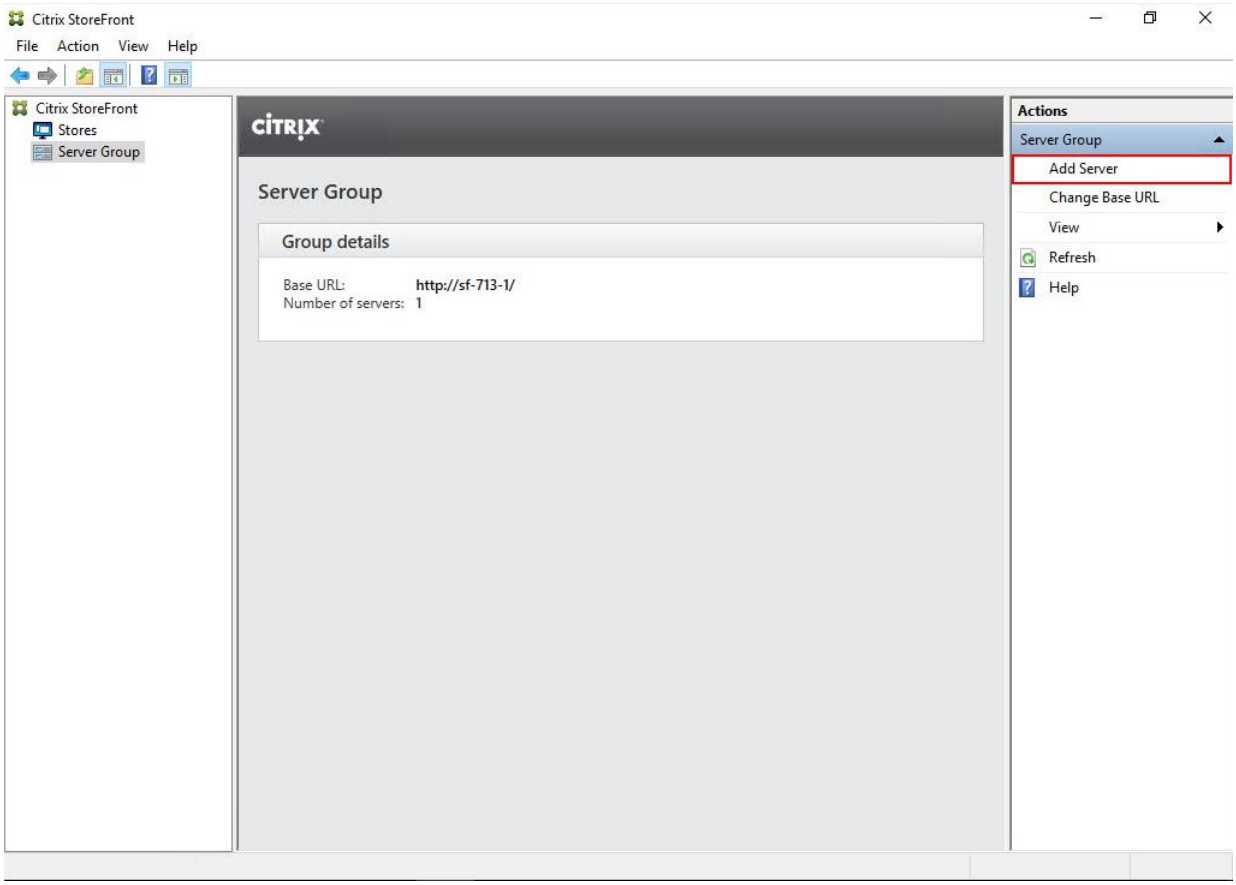
3. Before the additional StoreFront server can join the server group, you must connect to the first Storefront server, add the second server, and obtain the required authorization information.

4. Connect to the first StoreFront server.

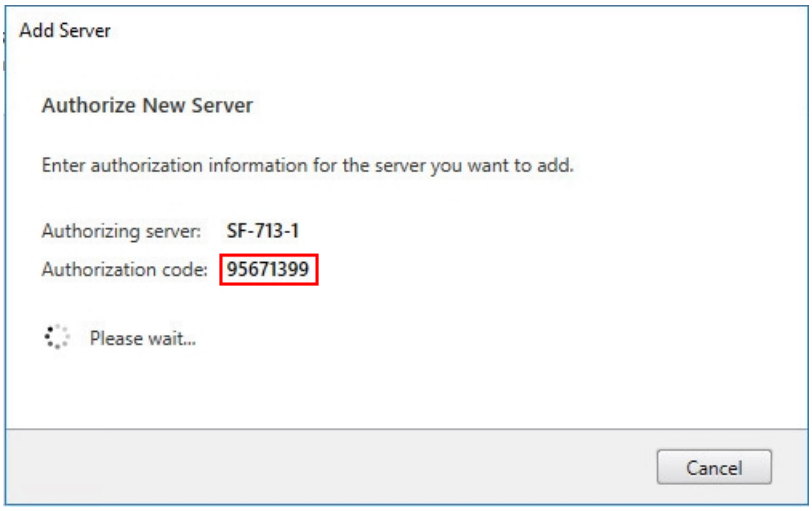
5. Using the StoreFront menu on the left, you can scroll through the StoreFront management options.

6. Select Server Group from the menu.

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

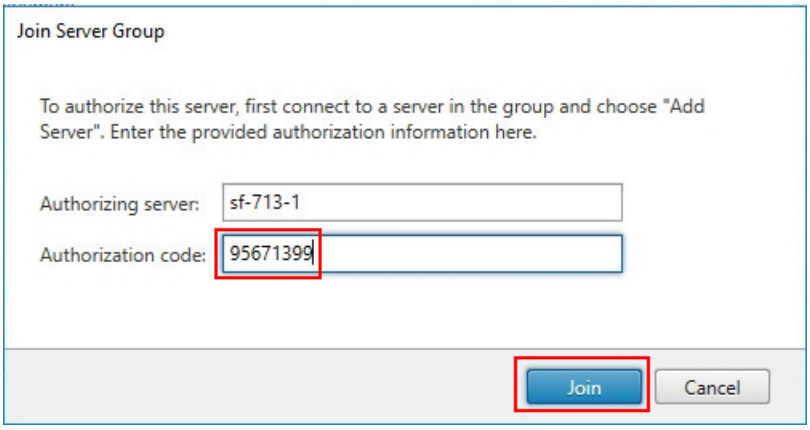


8. Copy the Authorization code from the Add Server dialog.



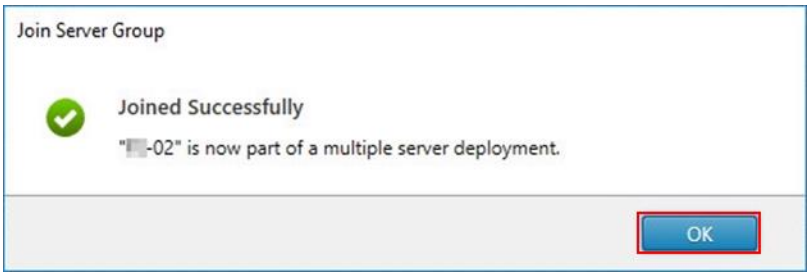
9. Connect to the second Storefront server and paste the Authorization code into the Join Server Group dialog.

10. Click Join.



11. A message appears when the second server has joined successfully.

12. Click OK.



The second StoreFront is now in the Server Group.

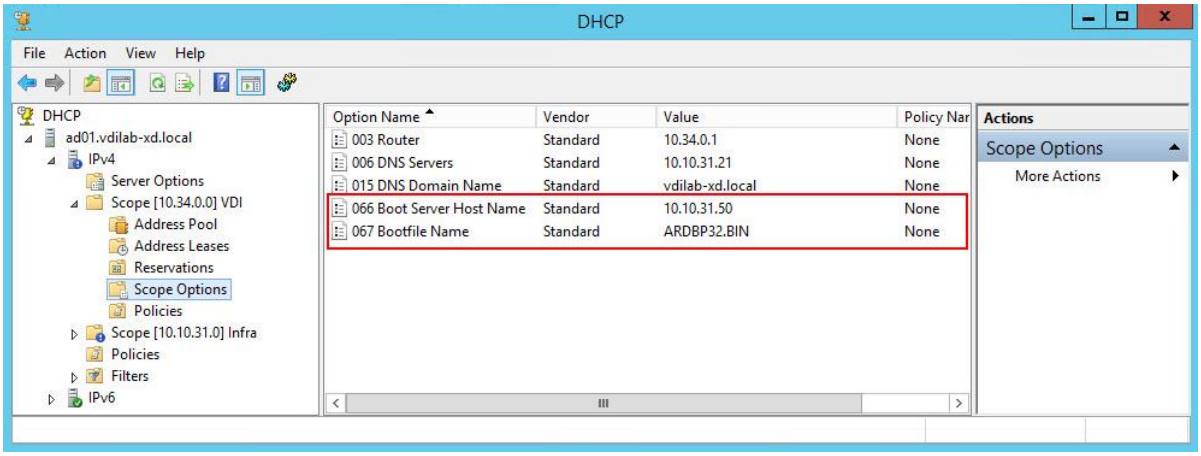
Install and Configure Citrix Provisioning Server 7.16

In most implementations, there is a single vDisk providing the standard image for multiple target devices. Thousands of target devices can use a single vDisk shared across multiple Provisioning Services (PVS) servers in the same farm, simplifying virtual desktop management. This section describes the installation and configuration tasks required to create a PVS implementation.

The PVS server can have many stored vDisks, and each vDisk can be several gigabytes in size. Your streaming performance and manageability can be improved using a RAID array, SAN, or NAS. PVS software and hardware requirements are available at: https://docs.citrix.com/en-us/provisioning/7-13/system-requirements.html.

Prerequisites

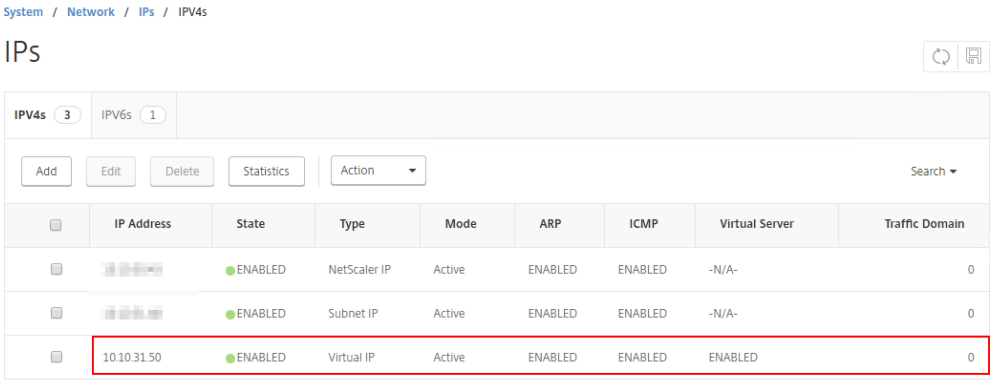
Set the following Scope Options on the DHCP server hosting the PVS target machines (for example, VDI, RDS).



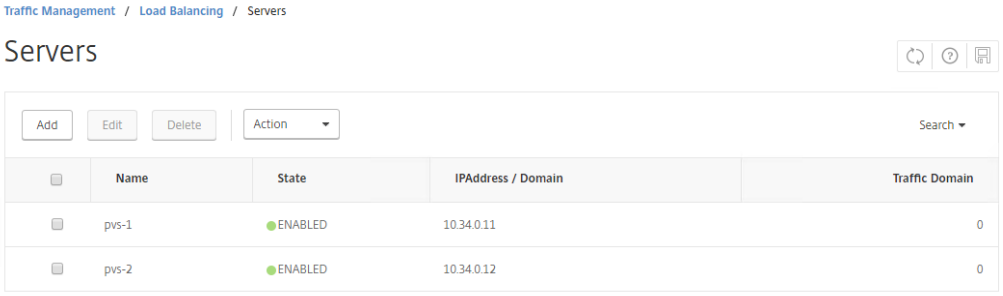
The Boot Server IP was configured for Load Balancing by NetScaler VPX to support High Availability of TFTP service.

To Configure TFTP Load Balancing, complete the following steps:

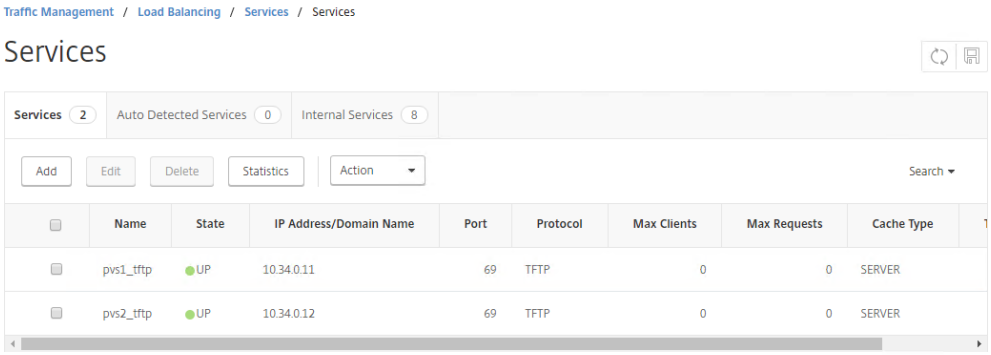
1. Create Virtual IP for TFTP Load Balancing.



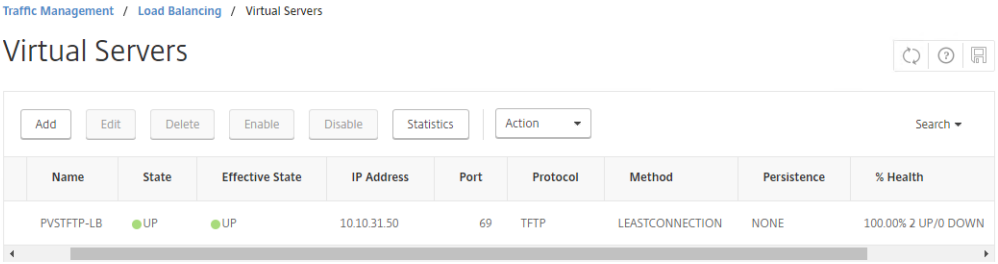
2. Configure servers that are running TFTP (your Provisioning Servers).



3. Define TFTP service for the servers (Monitor used: **udp-ecv**).



4. Configure TFTP for load balancing.



5. As a Citrix best practice cited in this CTX article, apply the following registry setting both the PVS servers and target machines:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\
   Key: "DisableTaskOffload" (dword)
   Value: "1"

Only one MS SQL database is associated with a farm. You can choose to install the Provisioning Services database software on an existing SQL database, if that machine can communicate with all Provisioning Servers within the farm, or with a new SQL Express database machine, created using the SQL Express software that is free from Microsoft.

The following databases are supported: Microsoft SQL Server 2008 SP3 through 2016 (x86, x64, and Express editions). Microsoft SQL 2016 was installed separately for this CVD.

High availability will be available for the databases once added to the SQL AlwaysOn Availability Group CTX201203.

To install and configure Citrix Provisioning Service 7.16, complete the following steps:

1. Insert the Citrix Provisioning Services 7.16 ISO and let AutoRun launch the installer.

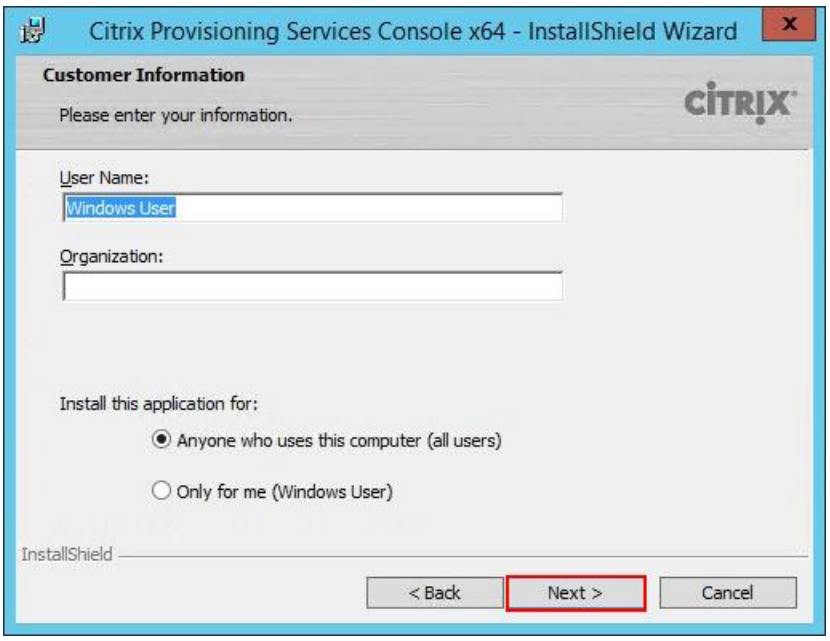
2. Click the Console Installation button.

3. Click Install to install the required prerequisites.

4. Read the Citrix License Agreement.
5. If acceptable, select the radio button labeled “I accept the terms in the license agreement.”
6. Click Next.

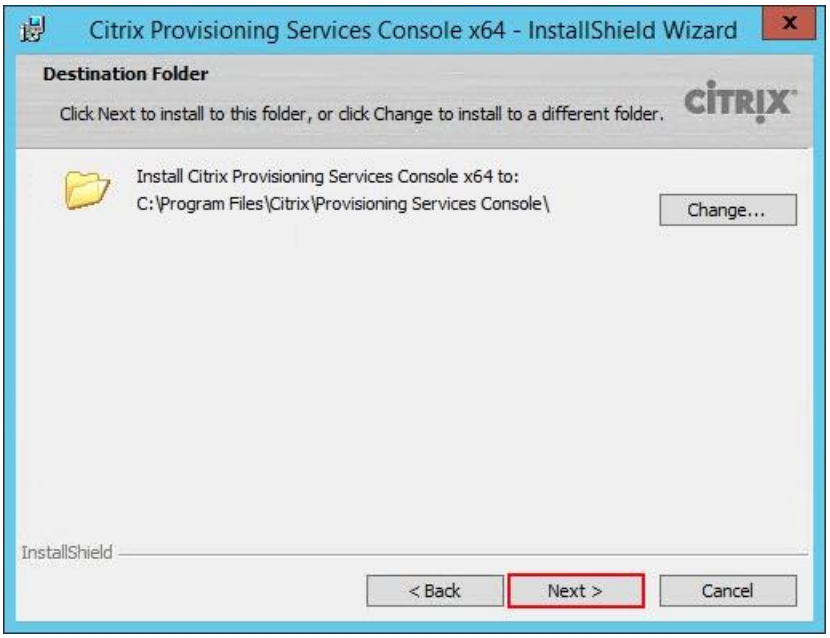
7. Optionally provide User Name and Organization.

8. Click Next.

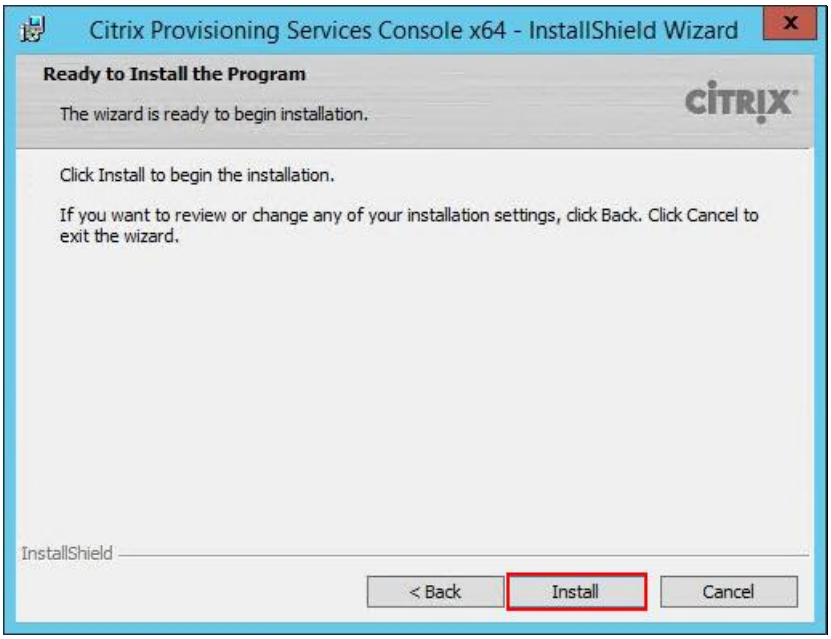


9. Accept the default path.

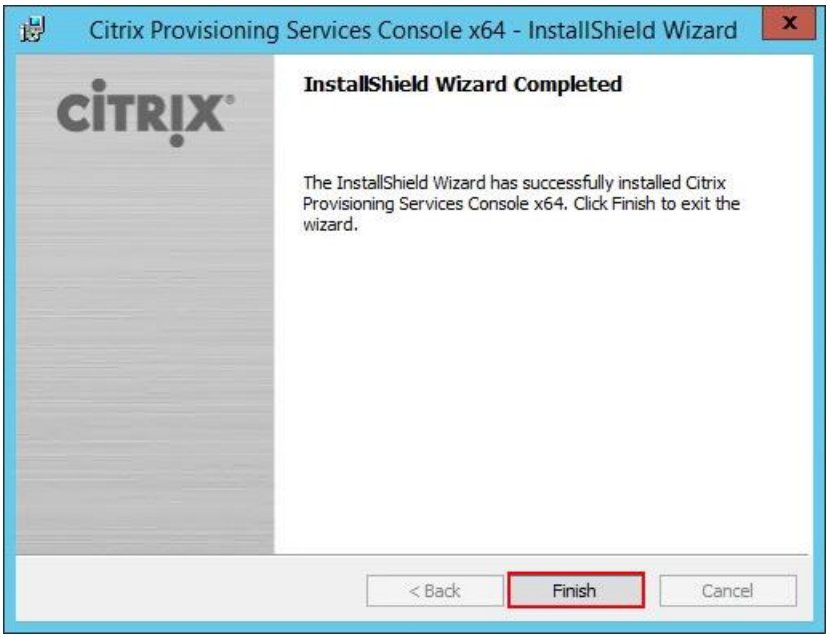
10. Click Next.



11. Click Install to start the console installation.

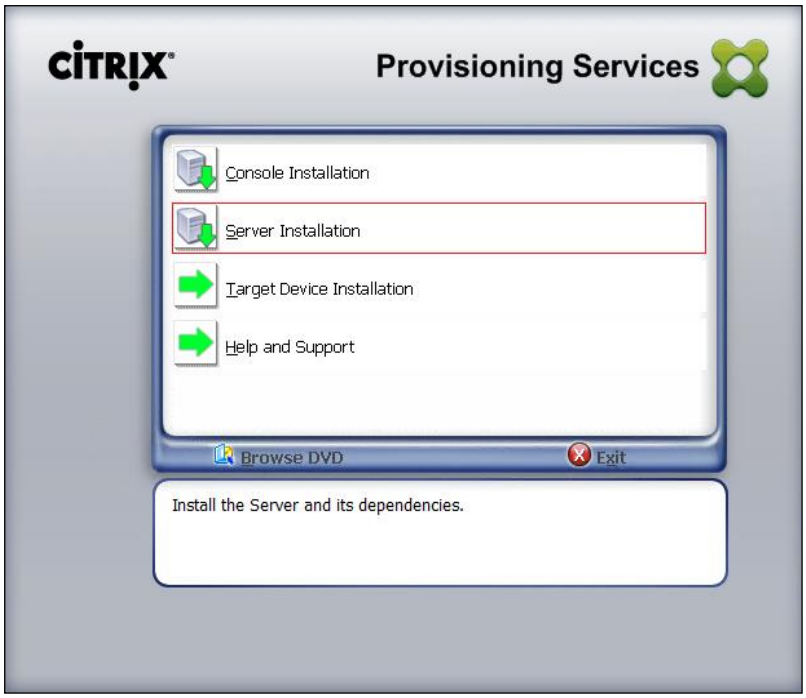


12. Click Finish.



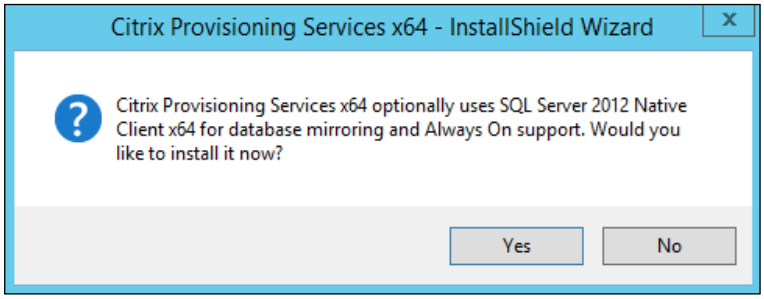
13. From the main installation screen, select Server Installation.

14. The installation wizard will check to resolve dependencies and then begin the PVS server installation process.

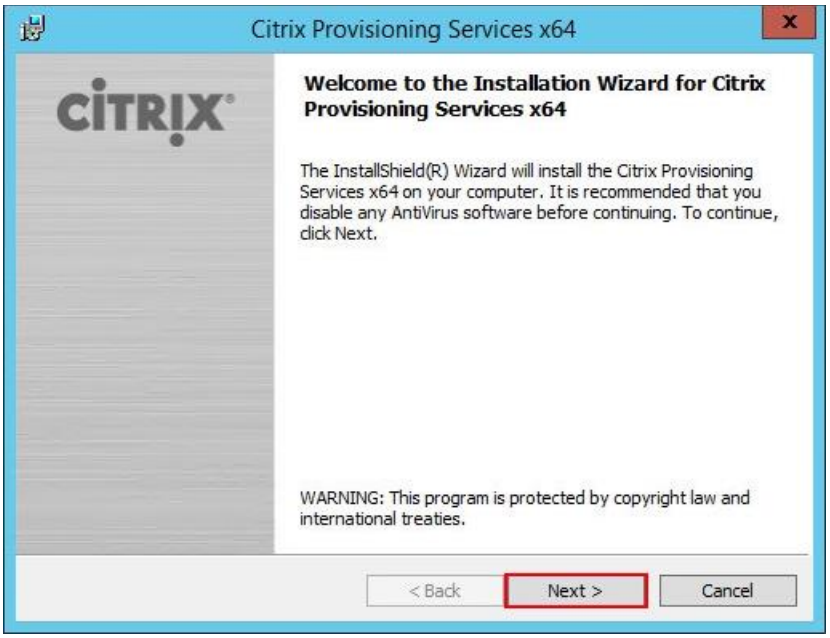


15. Click Install on the prerequisites dialog.

16. Click Yes when prompted to install the SQL Native Client.



17. Click Next when the Installation wizard starts.

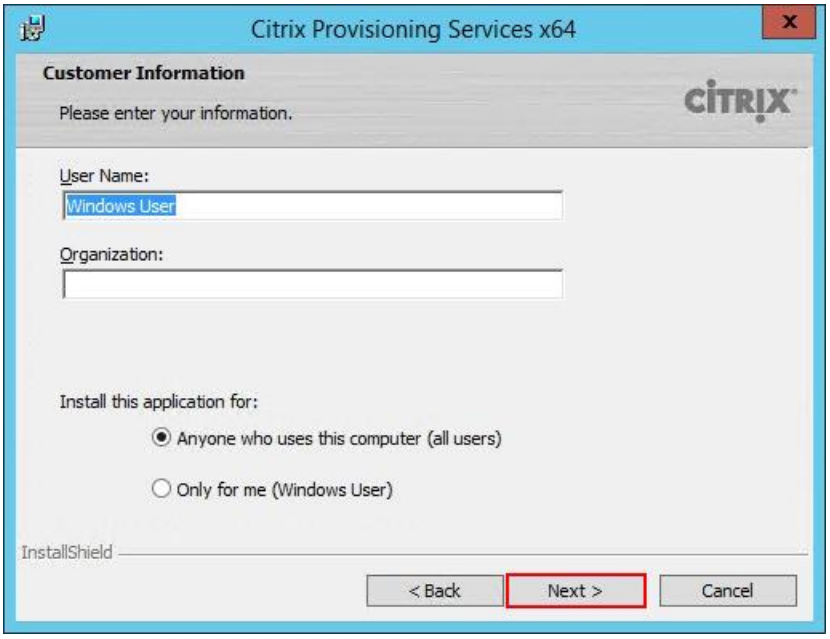


18. Review the license agreement terms. If acceptable, select the radio button labeled “I accept the terms in the license agreement.”

19. Click Next.

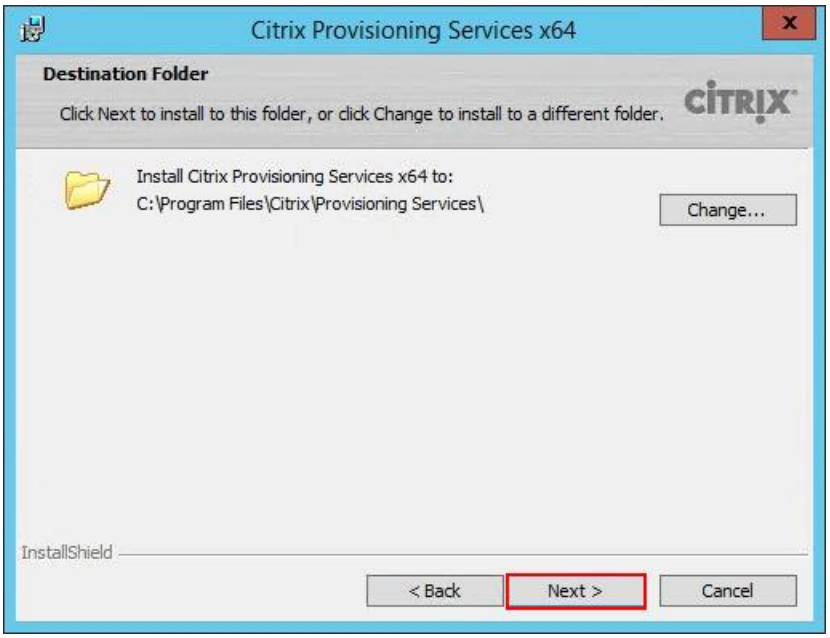
20. Provide User Name and Organization information. Select who will see the application.

21. Click Next.

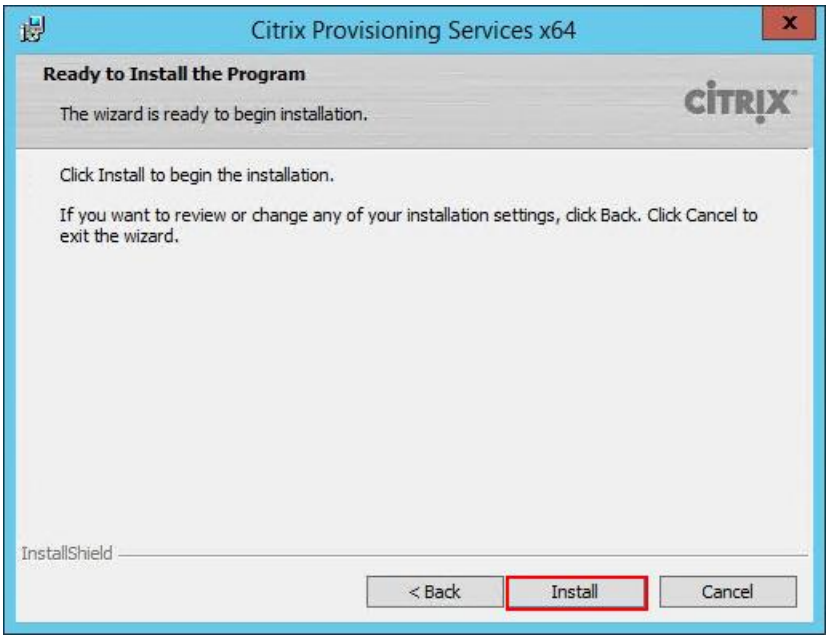


22. Accept the default installation location.

23. Click Next.



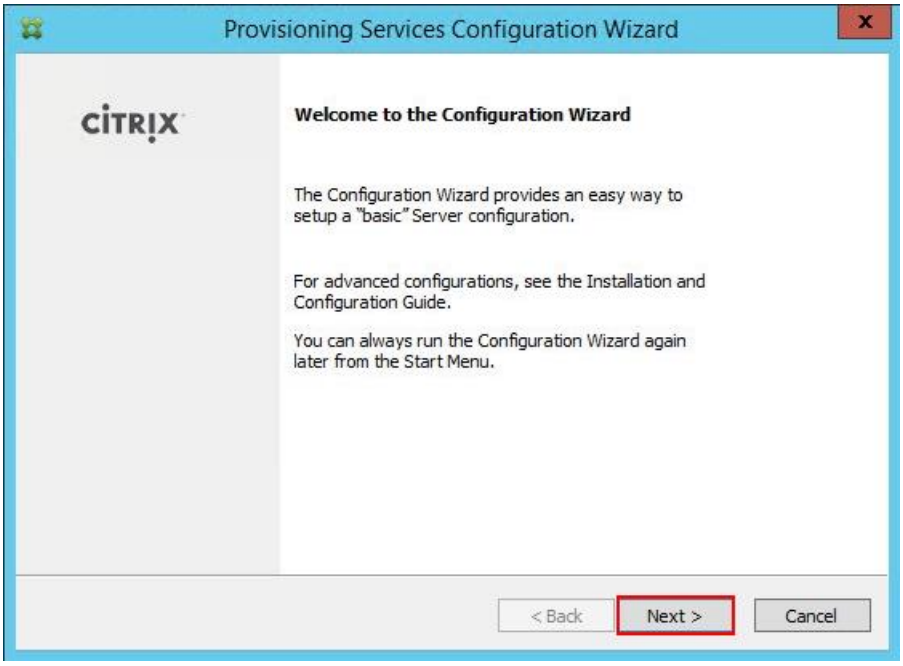
24. Click Install to begin the installation.



25. Click Finish when the install is complete.

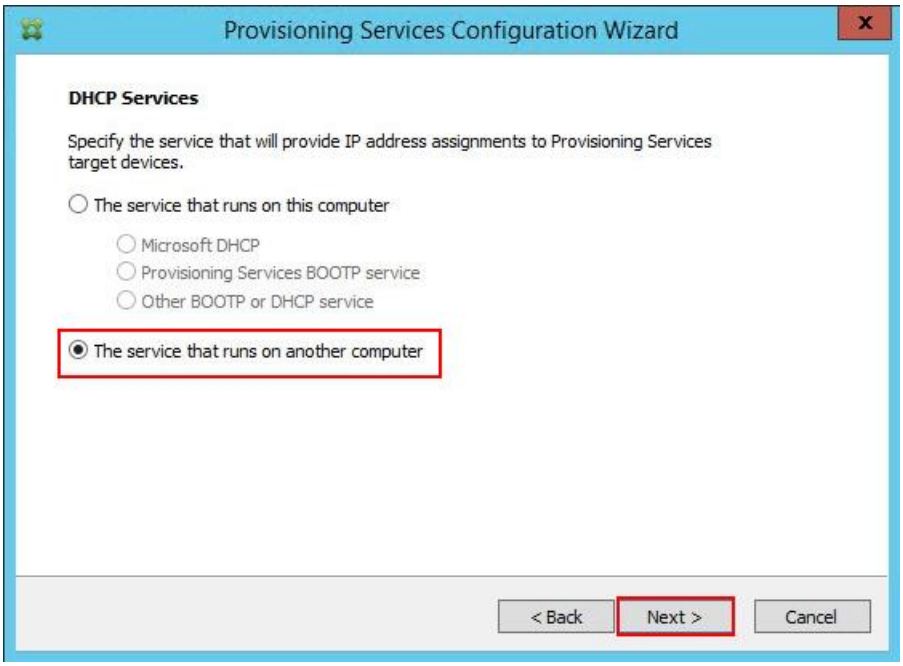
26. The PVS Configuration Wizard starts automatically.

27. Click Next.



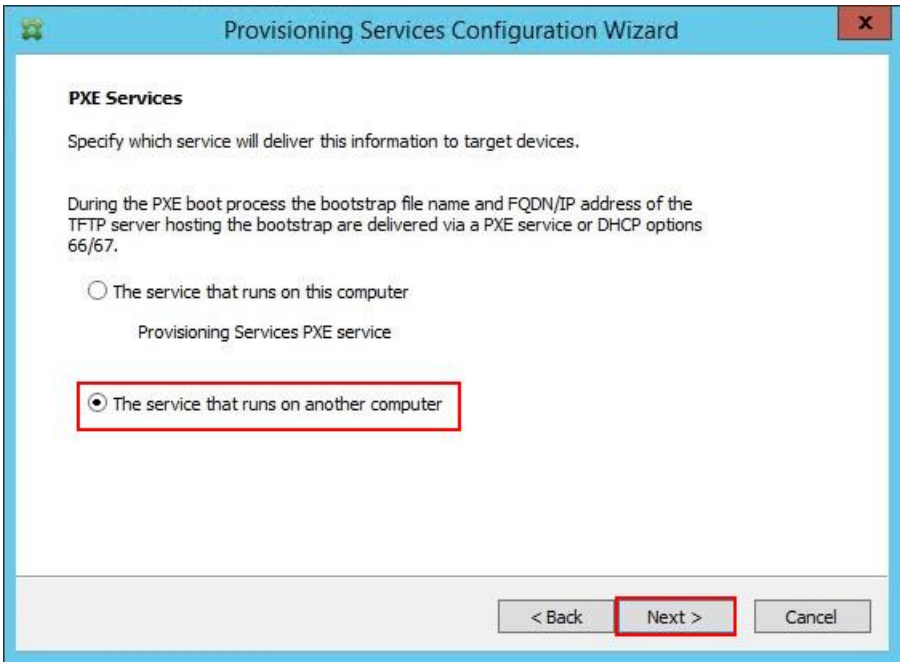
28. Since the PVS server is not the DHCP server for the environment, select the radio button labeled, “The service that runs on another computer.”

29. Click Next.



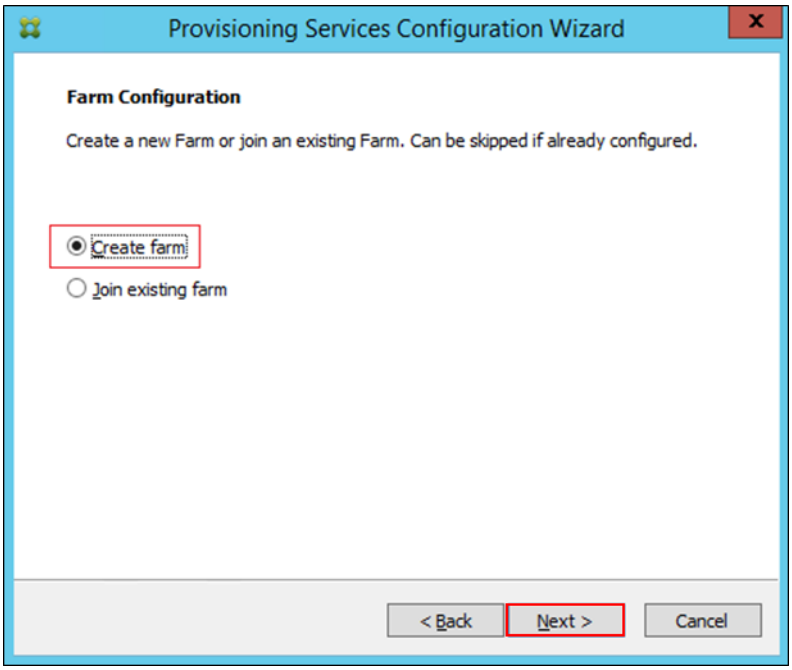
30. Since DHCP boot options 66 and 67 are used for TFTP services, select the radio button labeled, “The service that runs on another computer.”

31. Click Next.



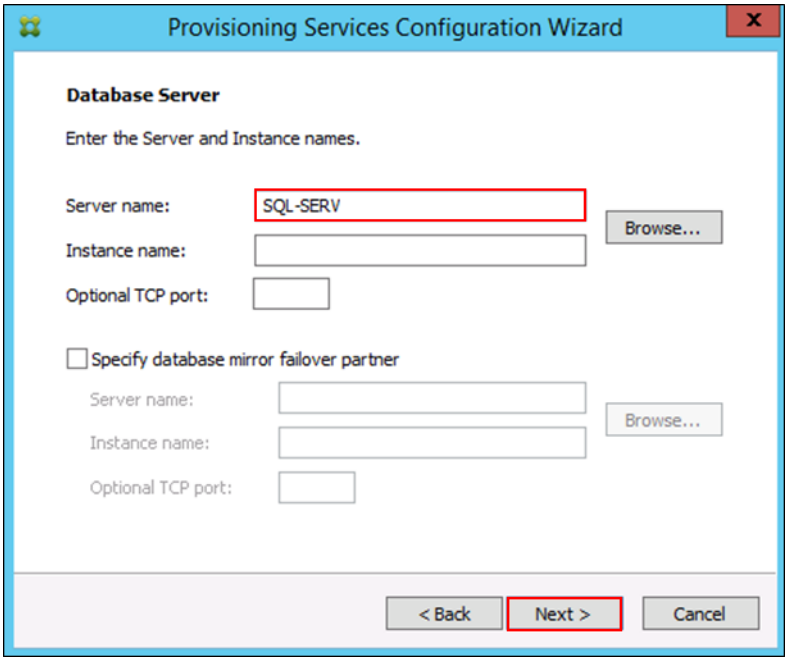
32. Since this is the first server in the farm, select the radio button labeled, “Create farm.”

33. Click Next.



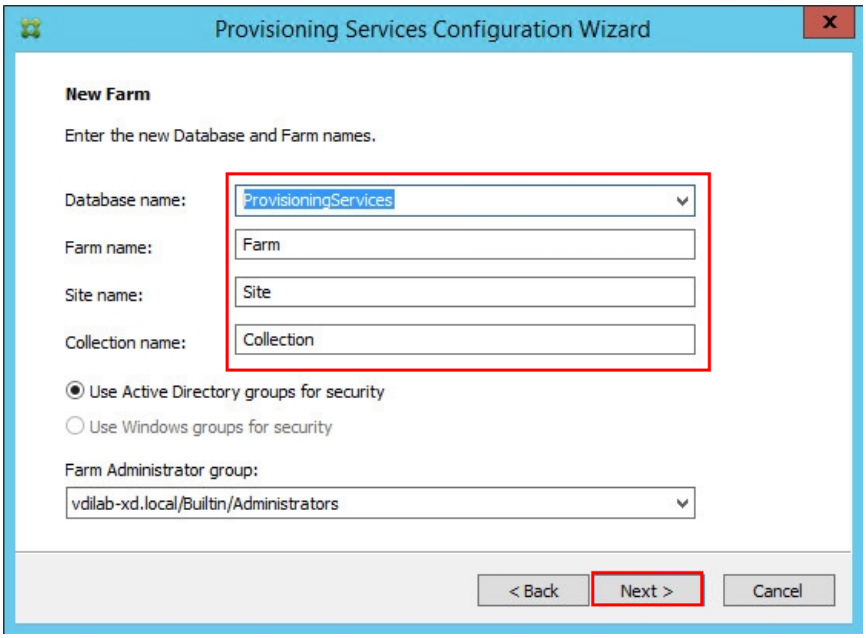
34. Enter the FQDN of the SQL server.

35. Click Next.



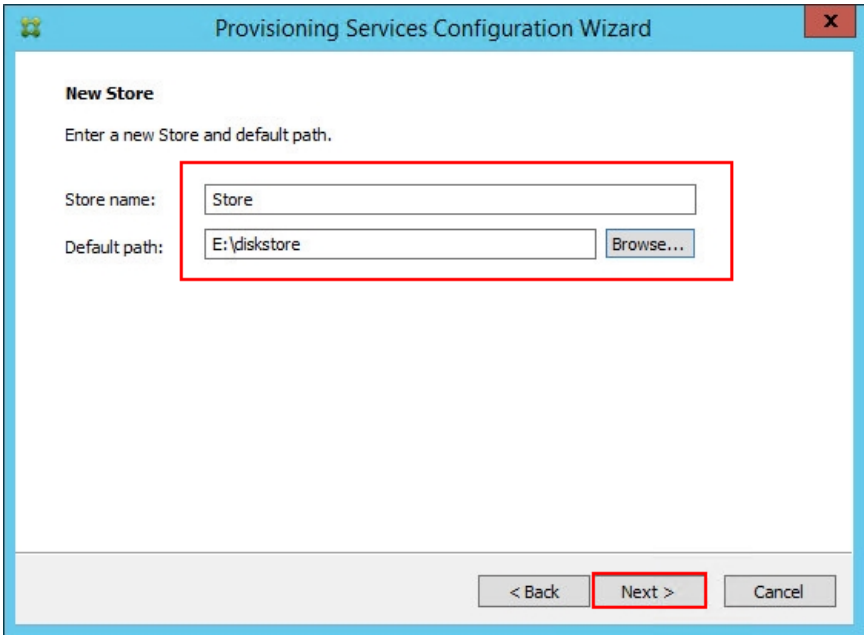
36. Provide the Database, Farm, Site, and Collection names.

37. Click Next.



38. Provide the vDisk Store details.

39. Click.

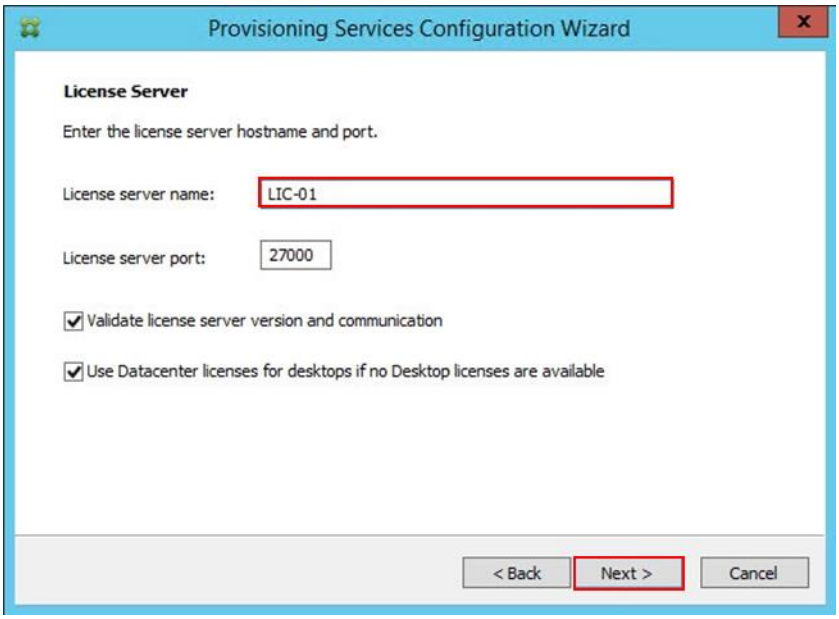


For large scale PVS environment, it is recommended to create the share using support for CIFS/SMB3 on an enterprise ready File Server.

40. Provide the FQDN of the license server.

41. Optionally, provide a port number if changed on the license server.

42. Click Next.

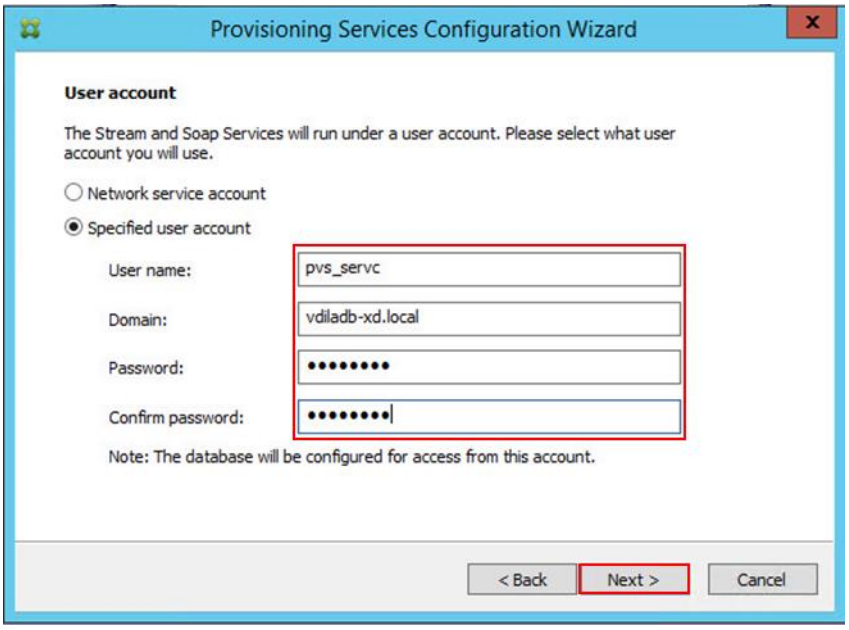


If an Active Directory service account is not already setup for the PVS servers, create that account prior to clicking Next on this dialog.

43. Select the Specified user account radio button.

44. Complete the User name, Domain, Password, and Confirm password fields, using the PVS account information created earlier.

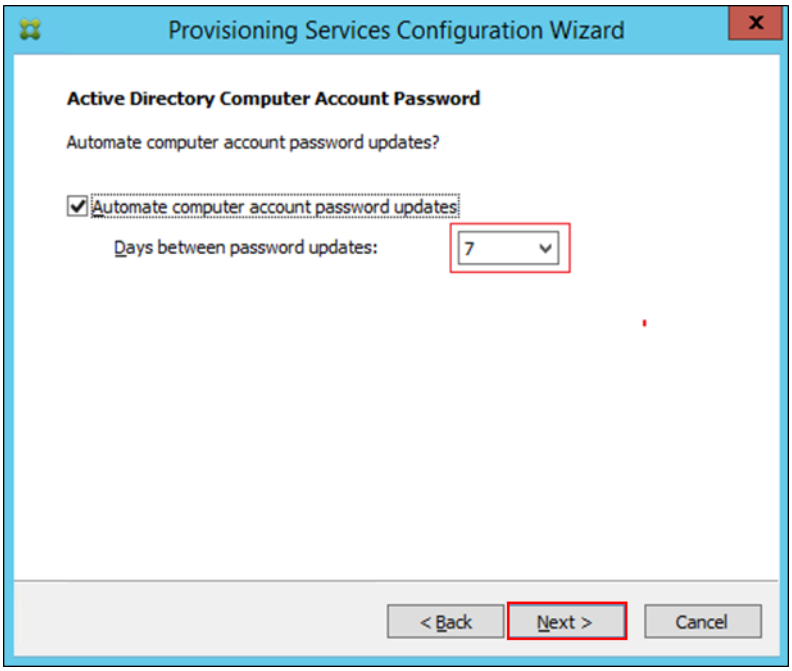
45. Click Next.



46. Set the Days between password updates to 7.

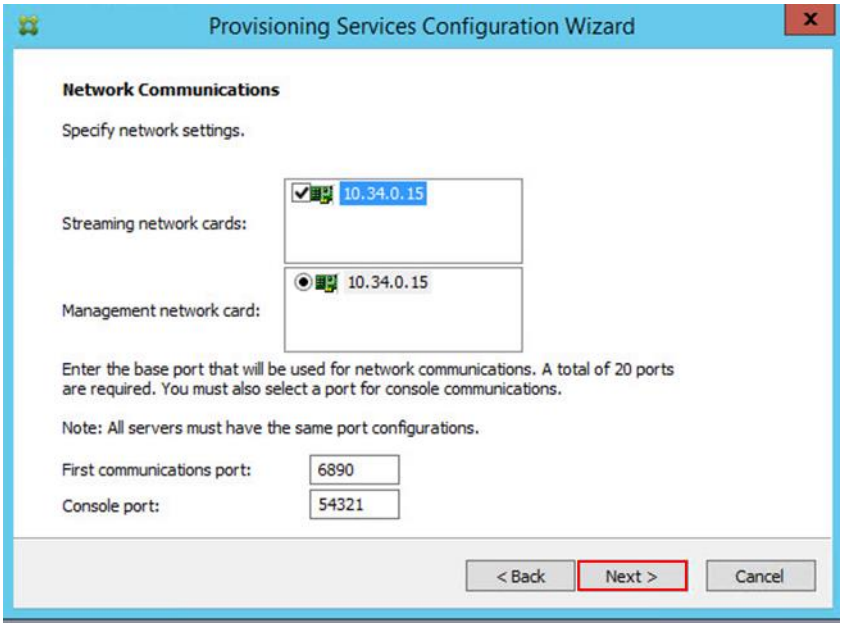
The updates will vary per environment. “7 days” for the configuration was appropriate for testing purposes.

47. Click Next.



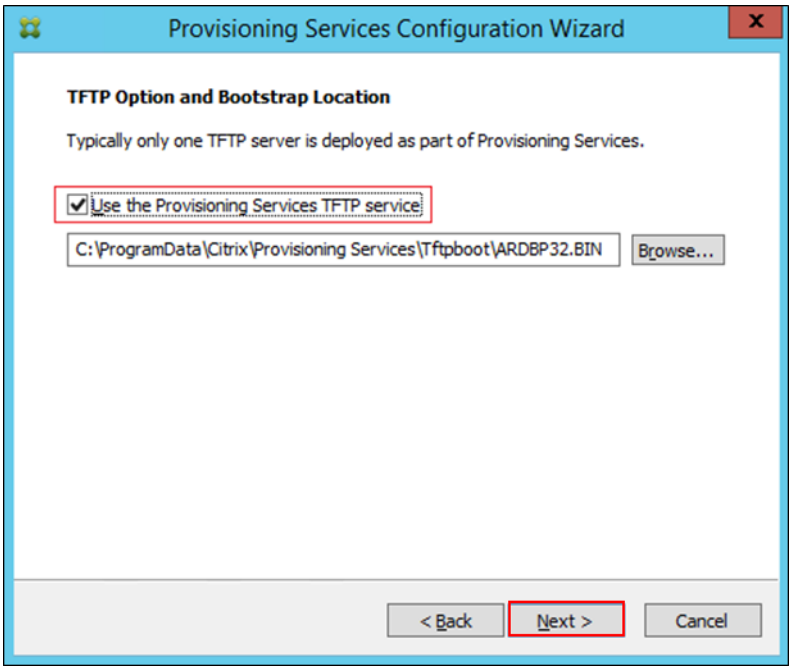
48. Keep the defaults for the network cards.

49. Click Next.



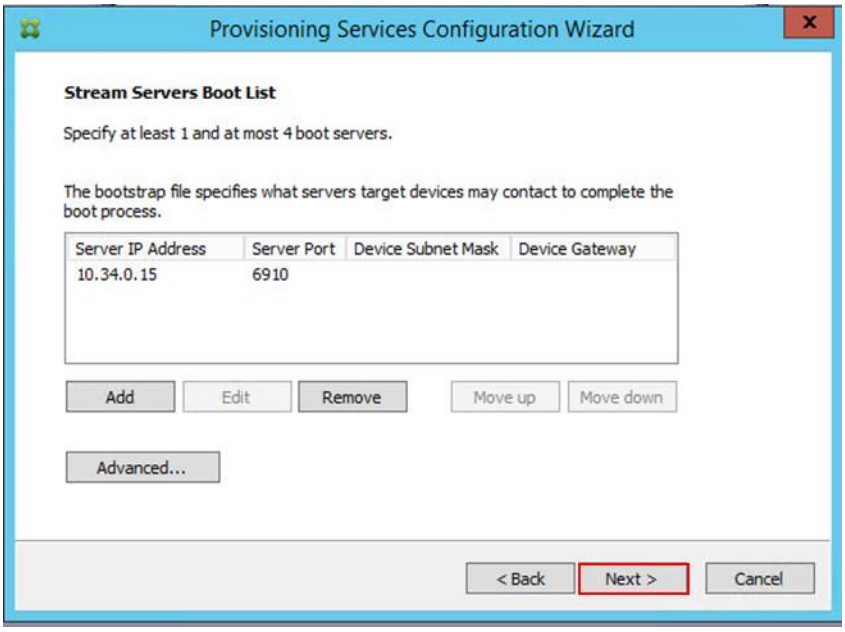
50. Select Use the Provisioning Services TFTP service checkbox.

51. Click Next.



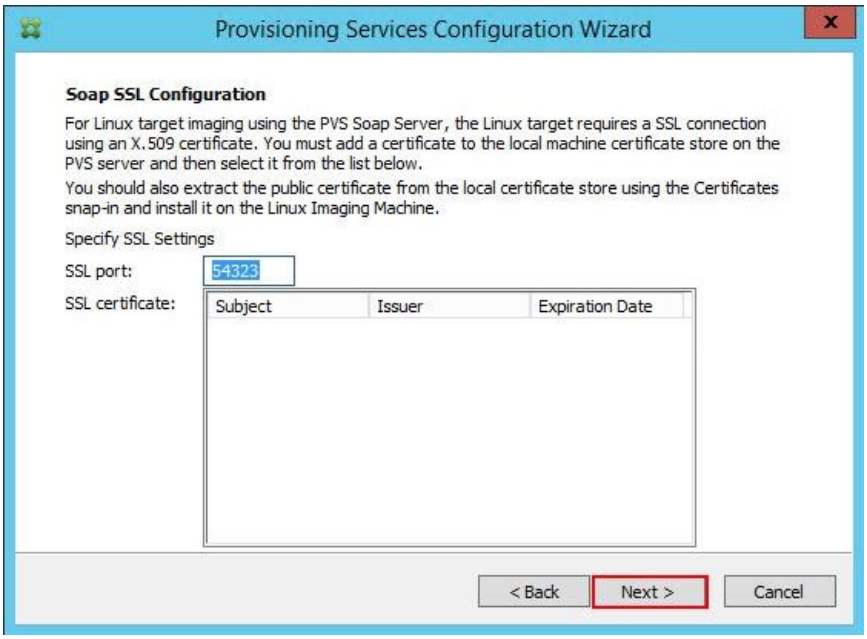
52. Make sure that the IP Addresses for all PVS servers are listed in the Stream Servers Boot List.

53. Click Next.



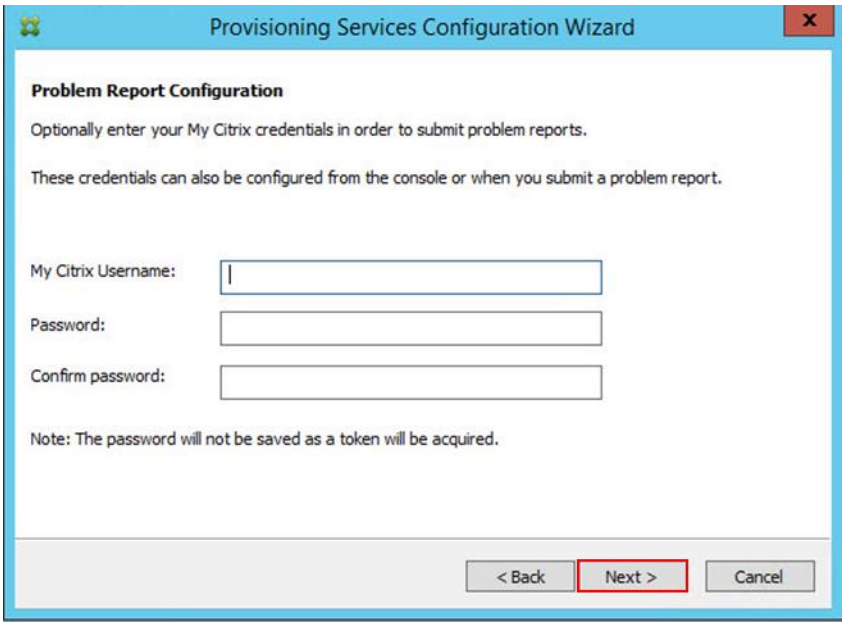
54. If Soap Server is used, provide details.

55. Click Next.

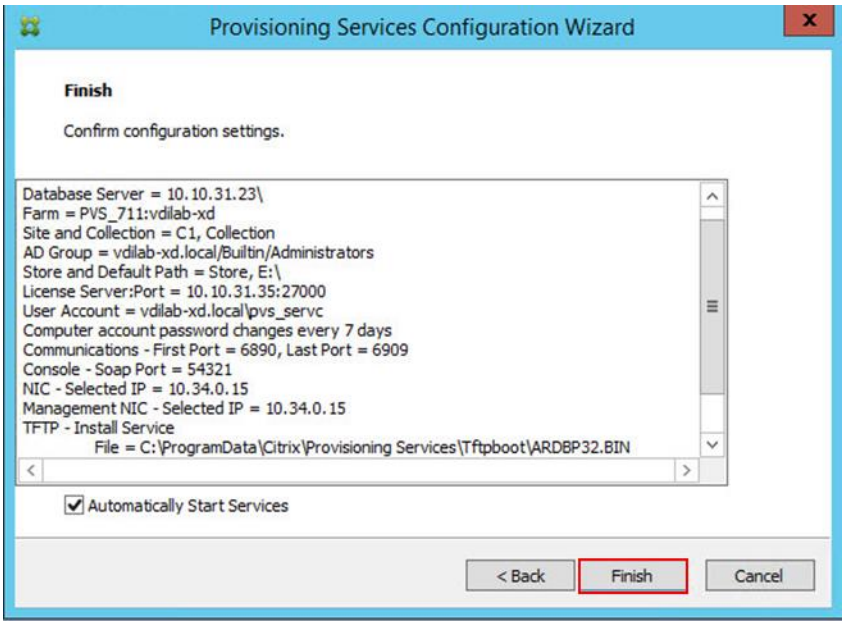


56. If desired fill in Problem Report Configuration.

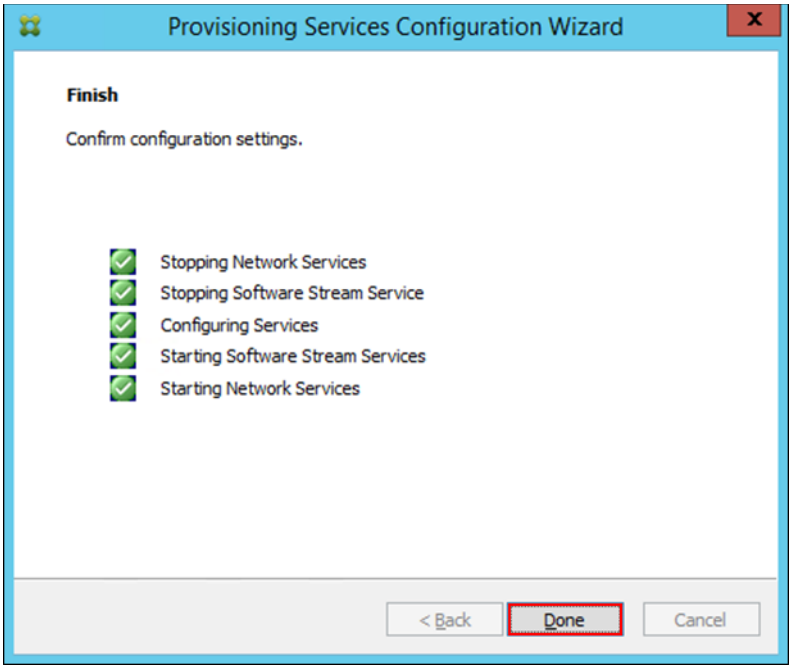
57. Click Next.



58. Click Finish to start the installation.



59. When the installation is completed, click Done.

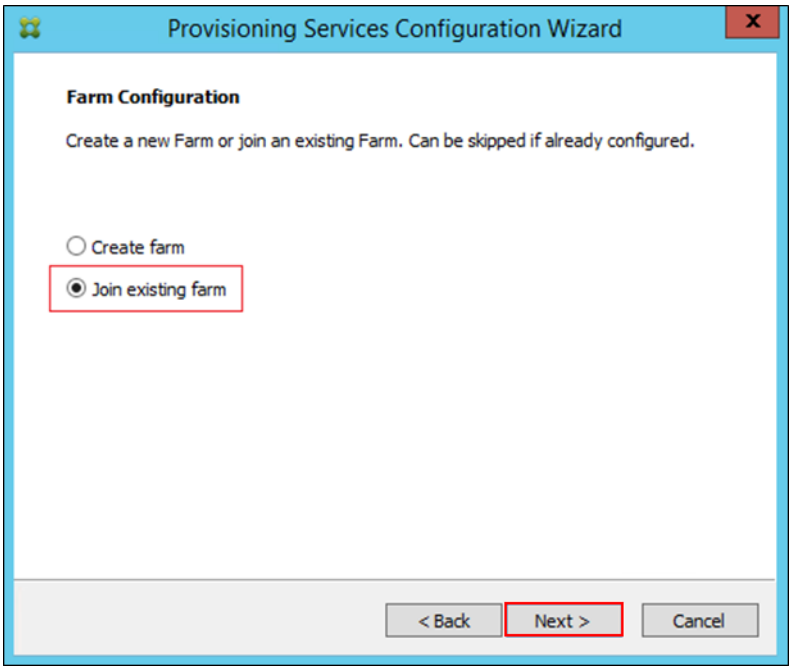


Install Additional PVS Servers

Complete the installation steps on the additional PVS servers up to the configuration step where it asks to Create or Join a farm. In this CVD, we repeated the procedure to add a total of two PVS servers. To install additional PVS server, complete the following steps:

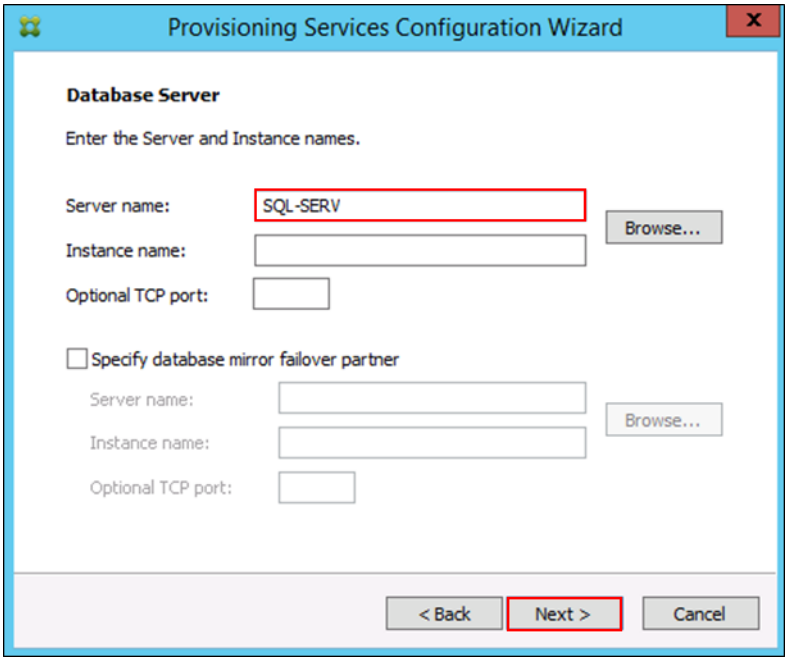
1. On the Farm Configuration dialog, select “Join existing farm.”

2. Click Next.



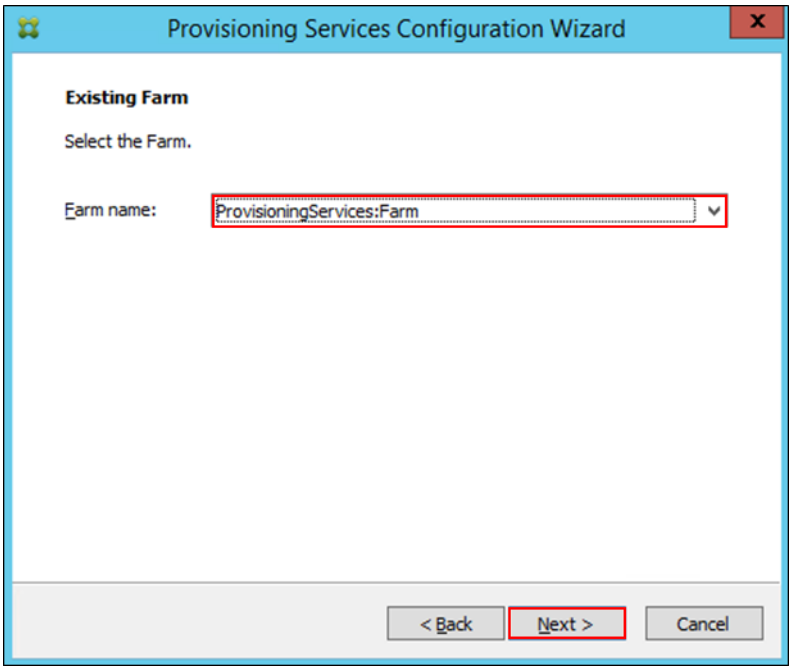
3. Provide the FQDN of the SQL Server.

4. Click Next.

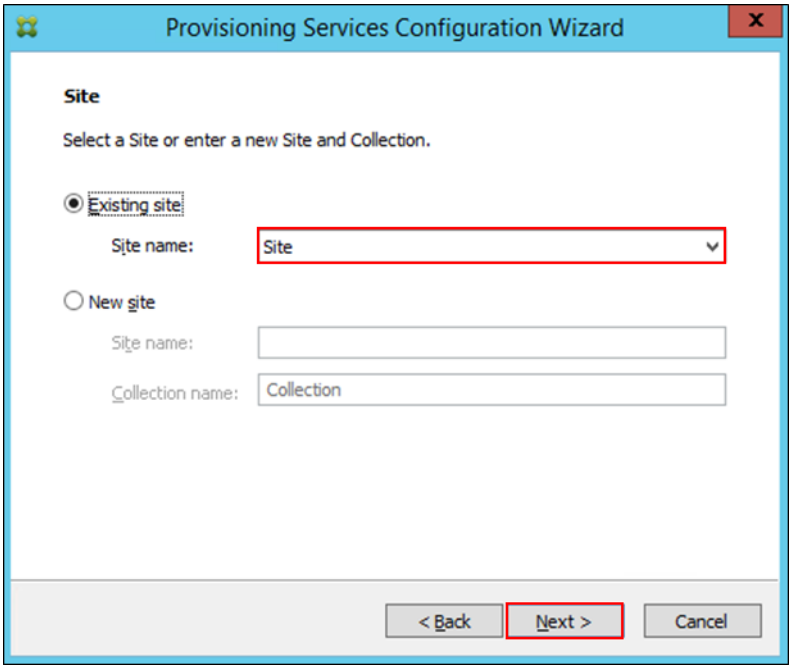


5. Accept the Farm Name.

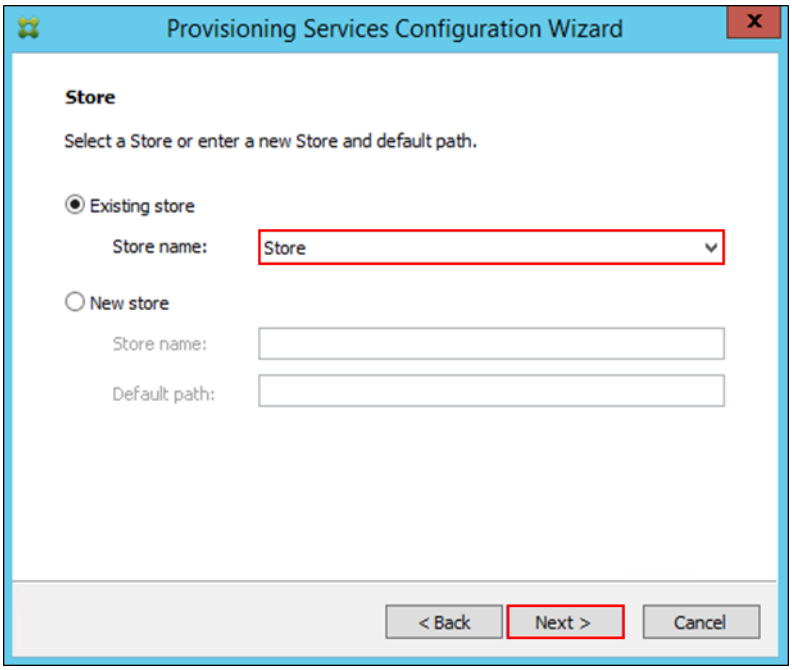
6. Click Next.



7. Accept the Existing Site.
8. Click Next.

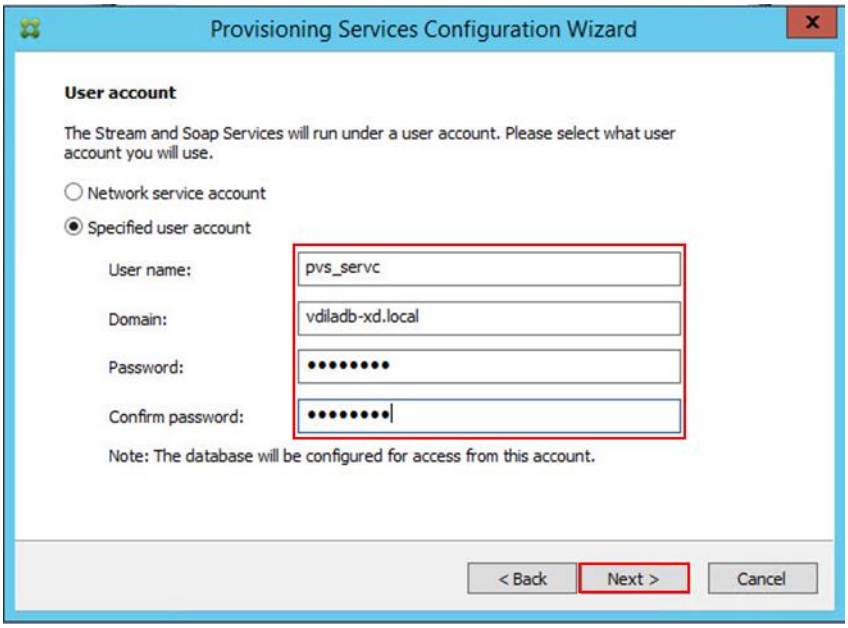


9. Accept the existing vDisk store.
10. Click Next.



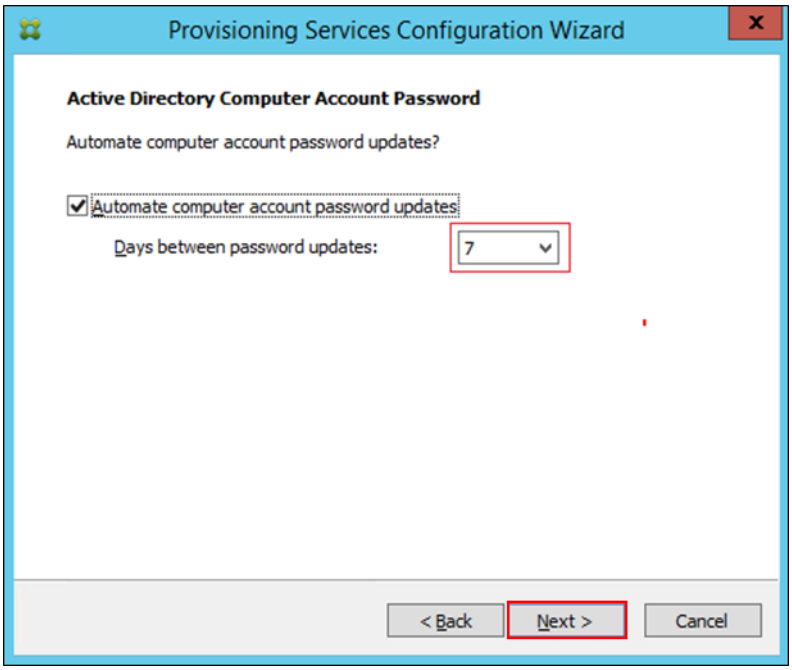
11. Provide the PVS service account information.

12. Click Next.



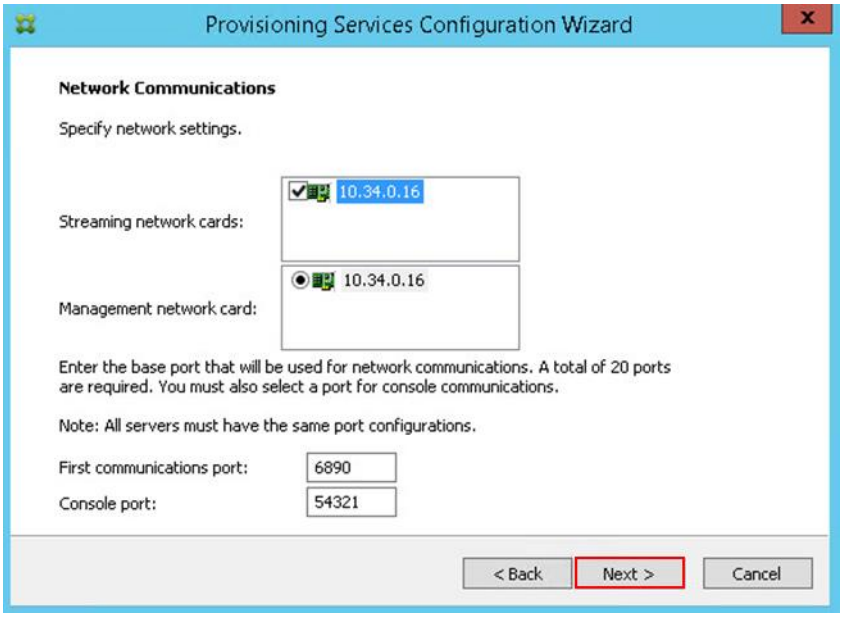
13. Set the Days between password updates to 7.

14. Click Next.



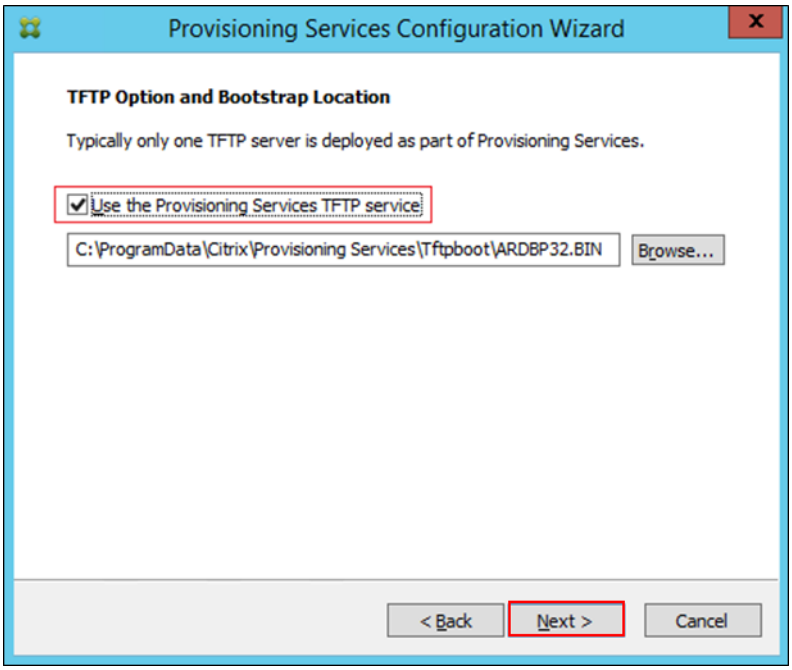
15. Accept the network card settings.

16. Click Next.



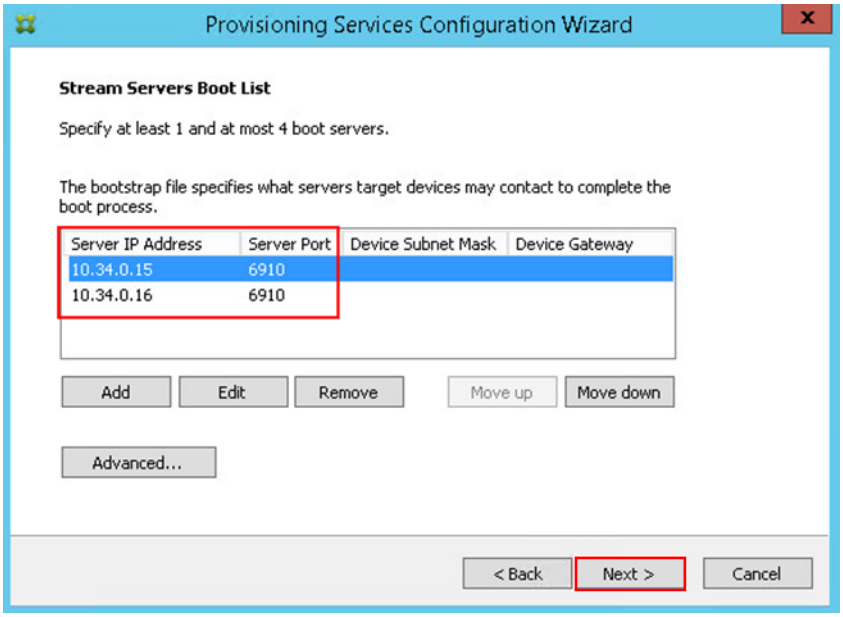
17. Select Use the Provisioning Services TFTP service checkbox.

18. Click Next.



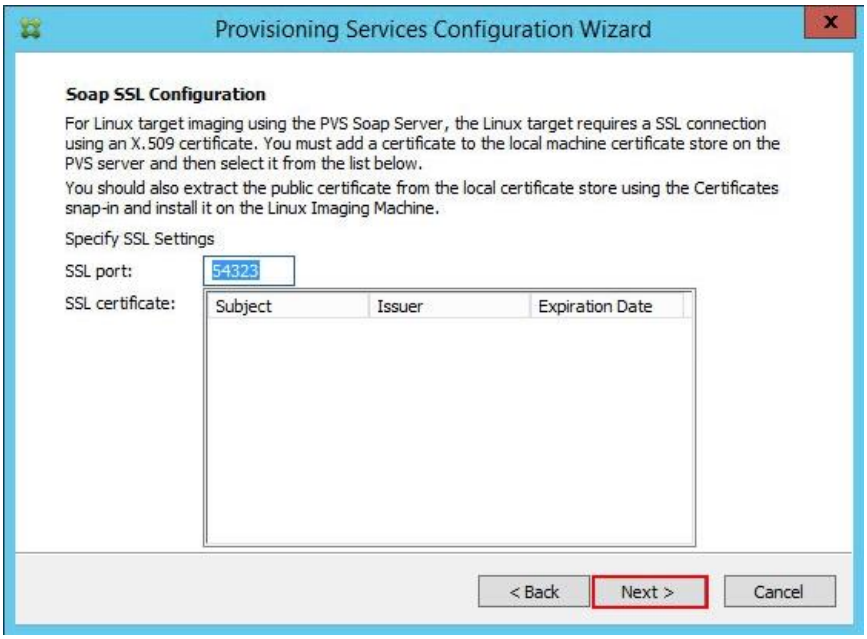
19. Make sure that the IP Addresses for all PVS servers are listed in the Stream Servers Boot List.

20. Click Next.



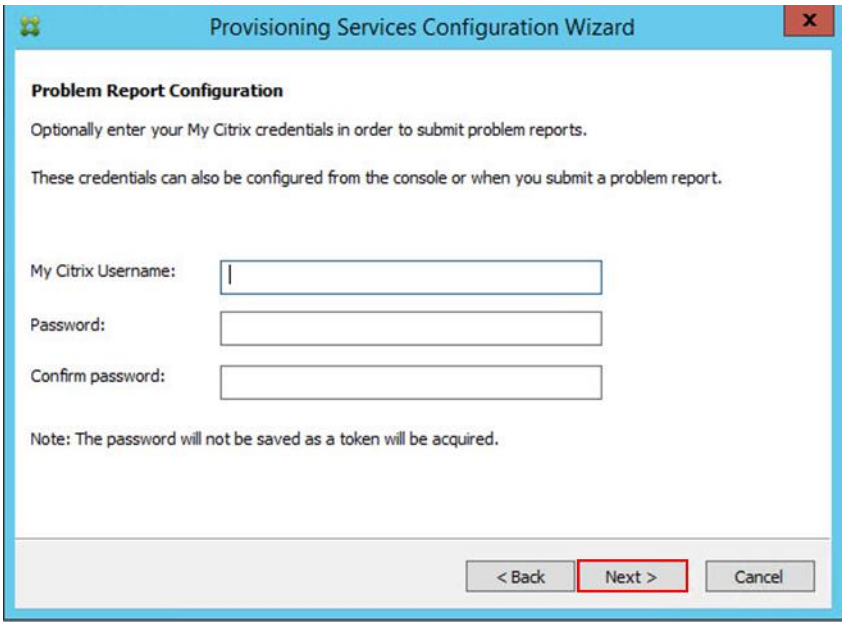
21. If Soap Server is used, provide details.

22. Click Next.

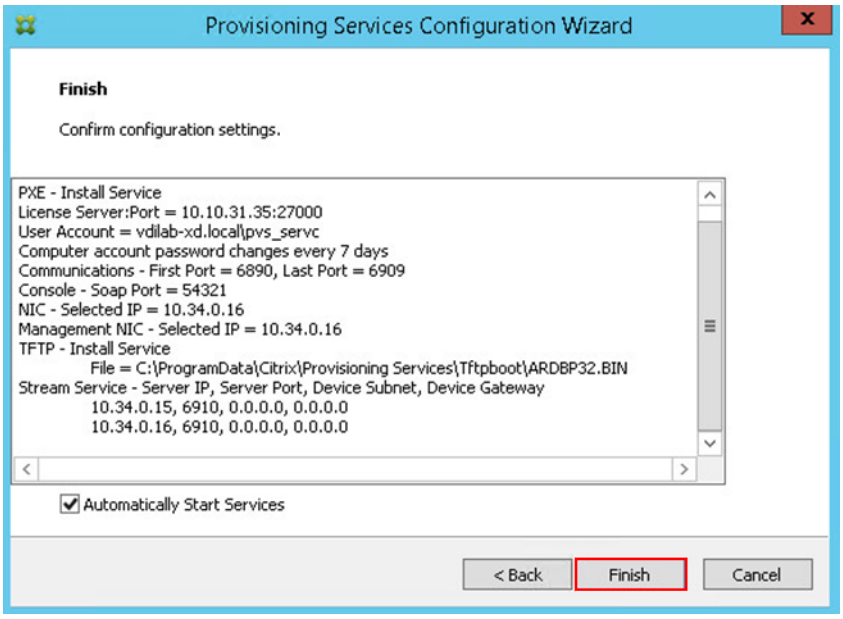


23. If desired fill in Problem Report Configuration.

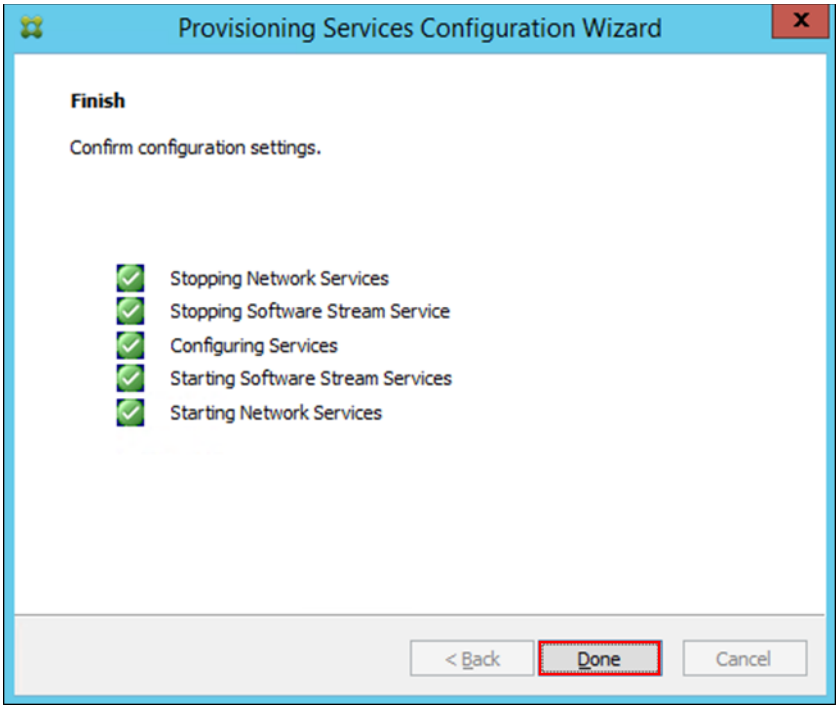
24. Click Next.



25. Click Finish to start the installation process.



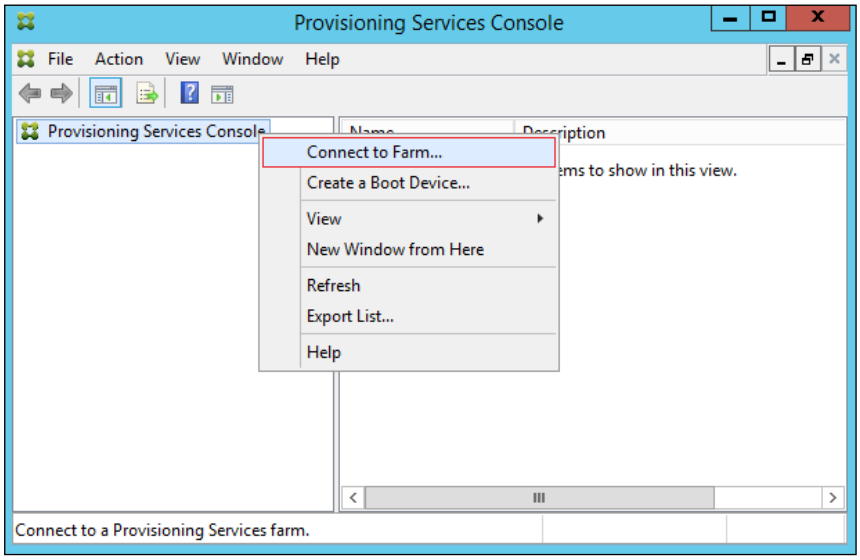
26. Click Done when the installation finishes.



You can optionally install the Provisioning Services console on the second PVS server following the procedure in the section Installing Provisioning Services.

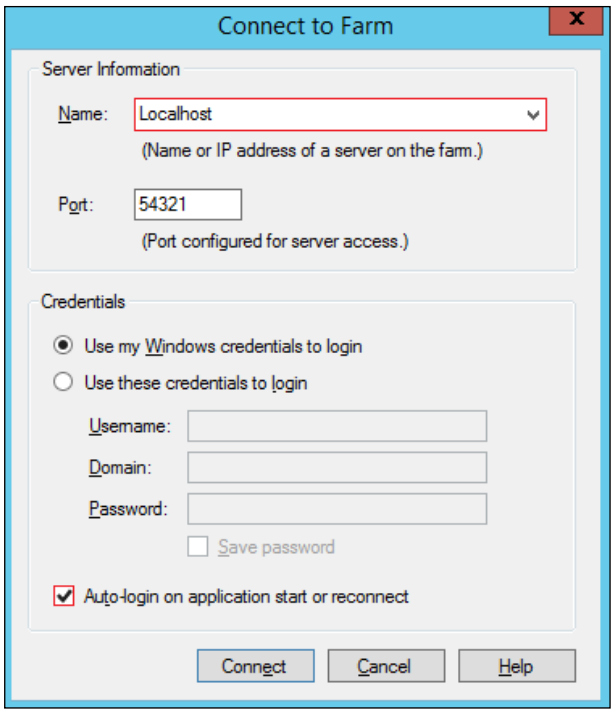
After completing the steps to install the second PVS server, launch the Provisioning Services Console to verify that the PVS Servers and Stores are configured and that DHCP boot options are defined.

27. Launch Provisioning Services Console and select Connect to Farm.

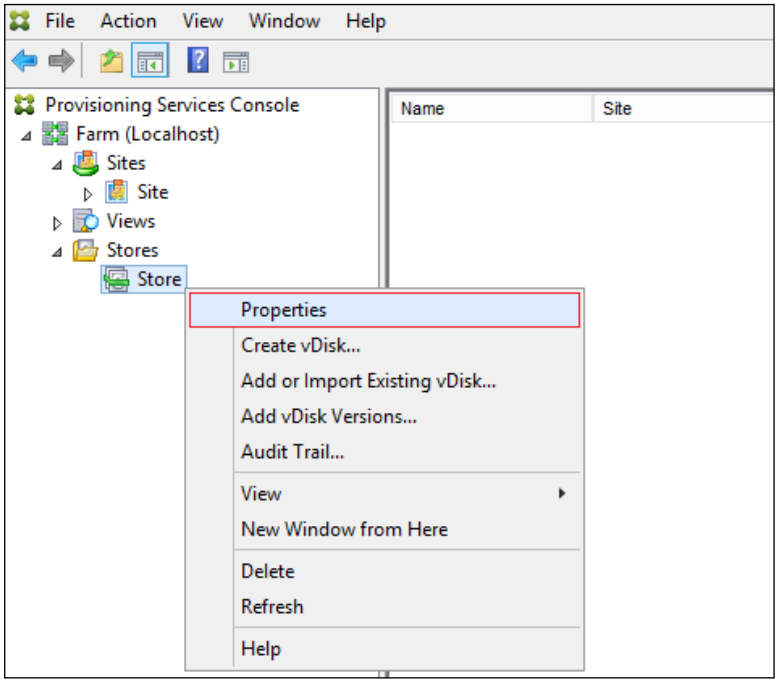


28. Enter localhost for the PVS1 server.

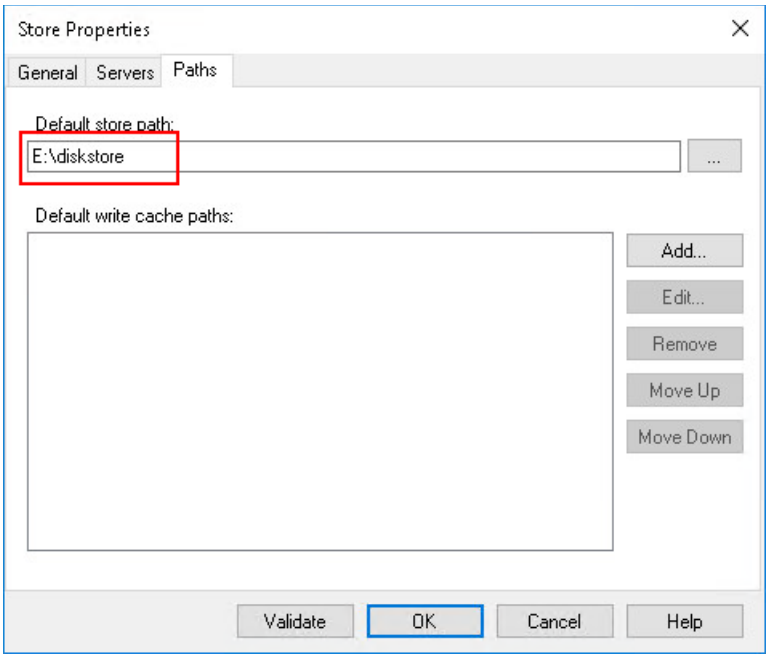
29. Click Connect.



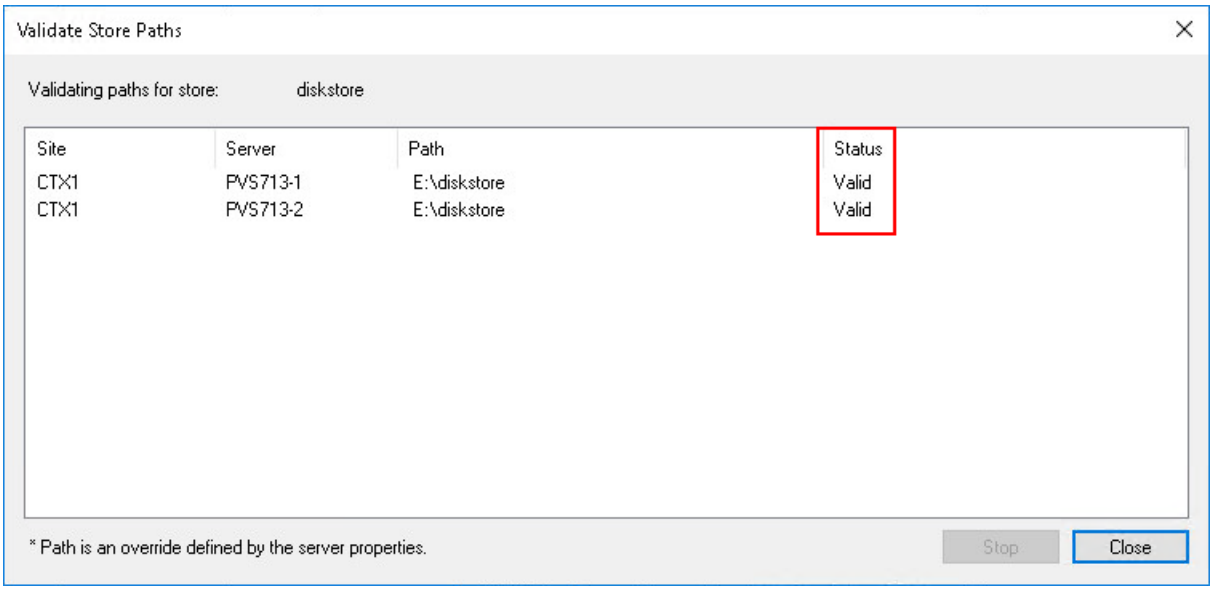
30. Select Store Properties from the drop-down list.



31. In the Store Properties dialog, add the Default store path to the list of Default write cache paths.



32. Click Validate. If the validation is successful, click Close and click OK to continue.



Install XenDesktop Virtual Desktop Agents

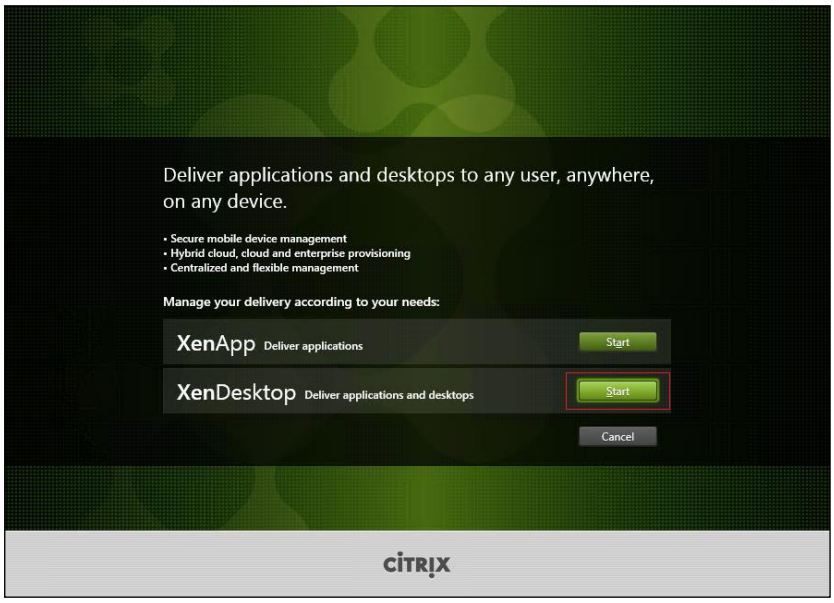
Virtual Delivery Agents (VDAs) are installed on the server and workstation operating systems, and enable connections for desktops and apps. The following procedure was used to install VDAs for both HVD and HSD environments.

By default, when you install the Virtual Delivery Agent, Citrix User Profile Management is installed silently on master images. (Using profile management as a profile solution is optional but was used for this CVD, and is described in a later section.)

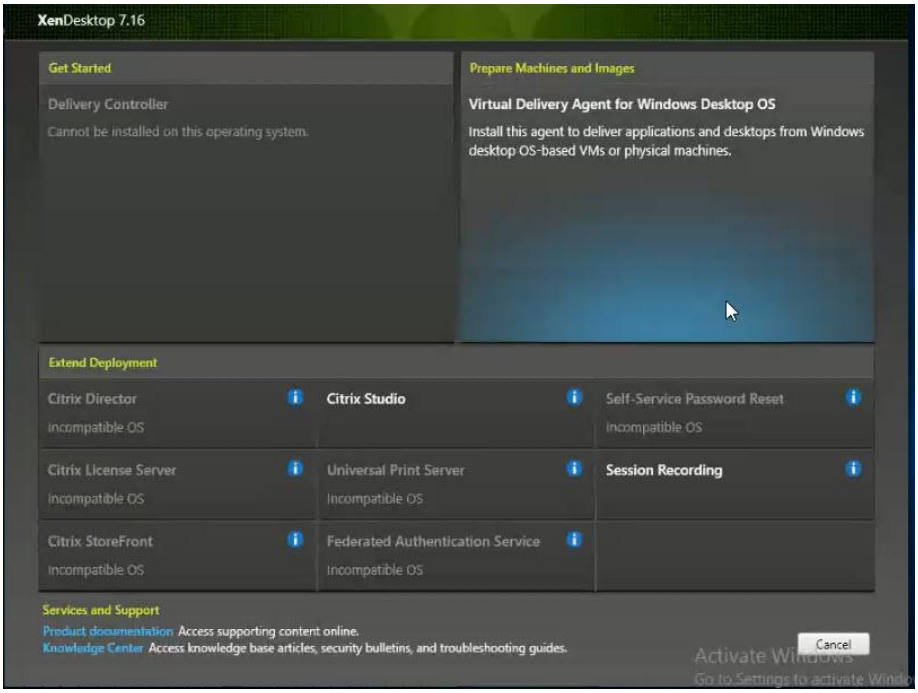
To install XenDesktop Virtual Desktop Agents, complete the following steps:

1. Launch the XenDesktop installer from the XenDesktop 7.16 ISO.

2. Click Start on the Welcome Screen.

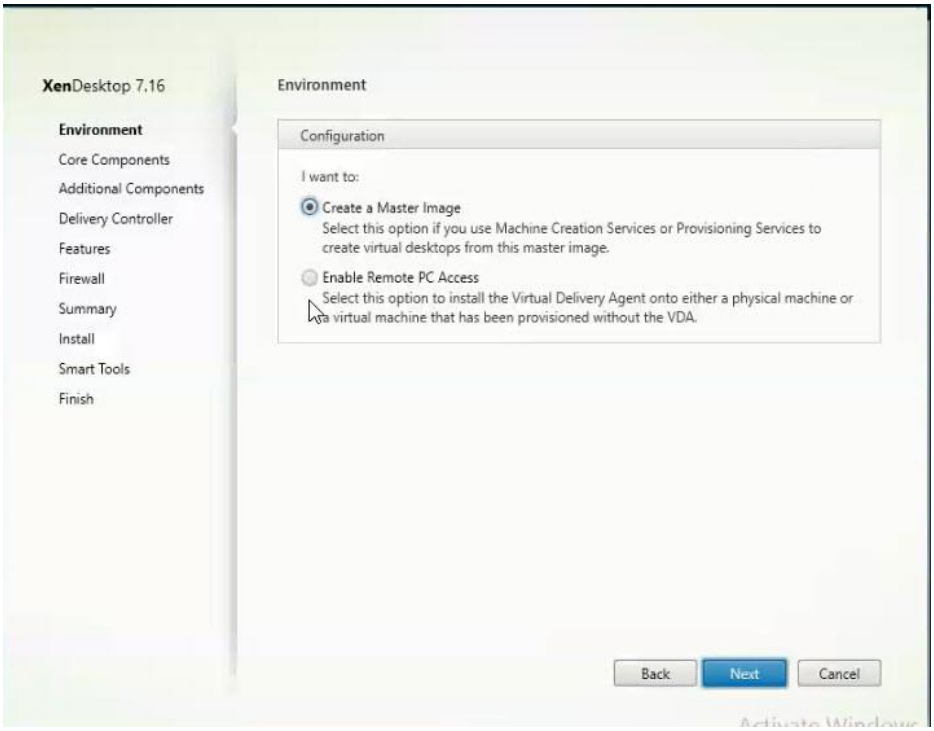


3. To install the VDA for the Hosted Virtual Desktops (VDI), select Virtual Delivery Agent for Windows Desktop OS. After the VDA is installed for Hosted Virtual Desktops, repeat the procedure to install the VDA for Hosted Shared Desktops (RDS). In this case, select Virtual Delivery Agent for Windows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



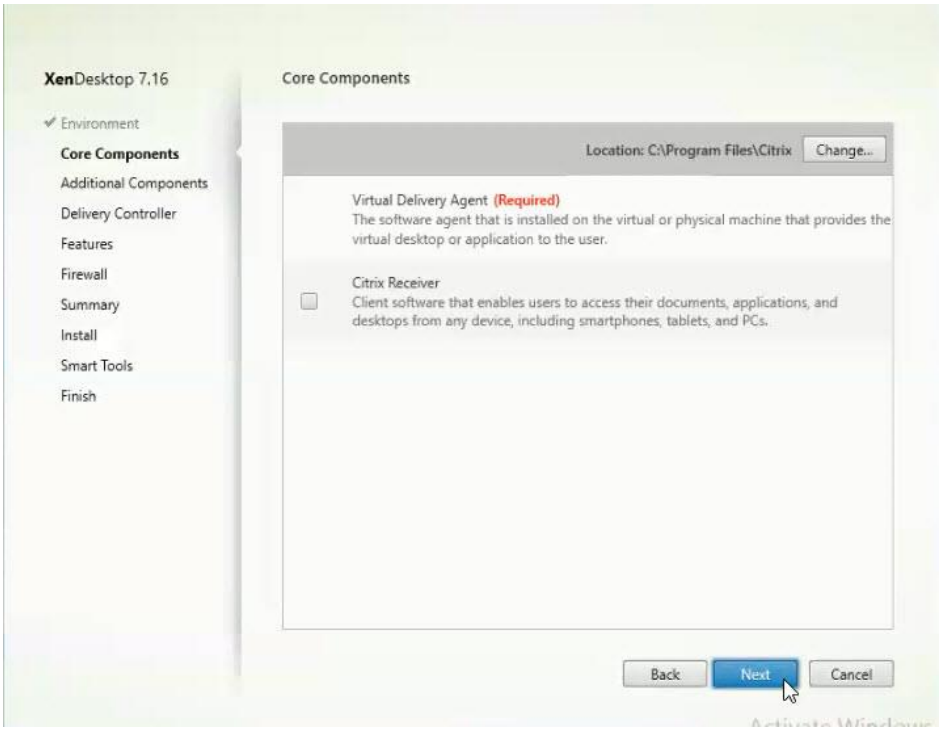
4. Select “Create a Master Image.”

5. Click Next.

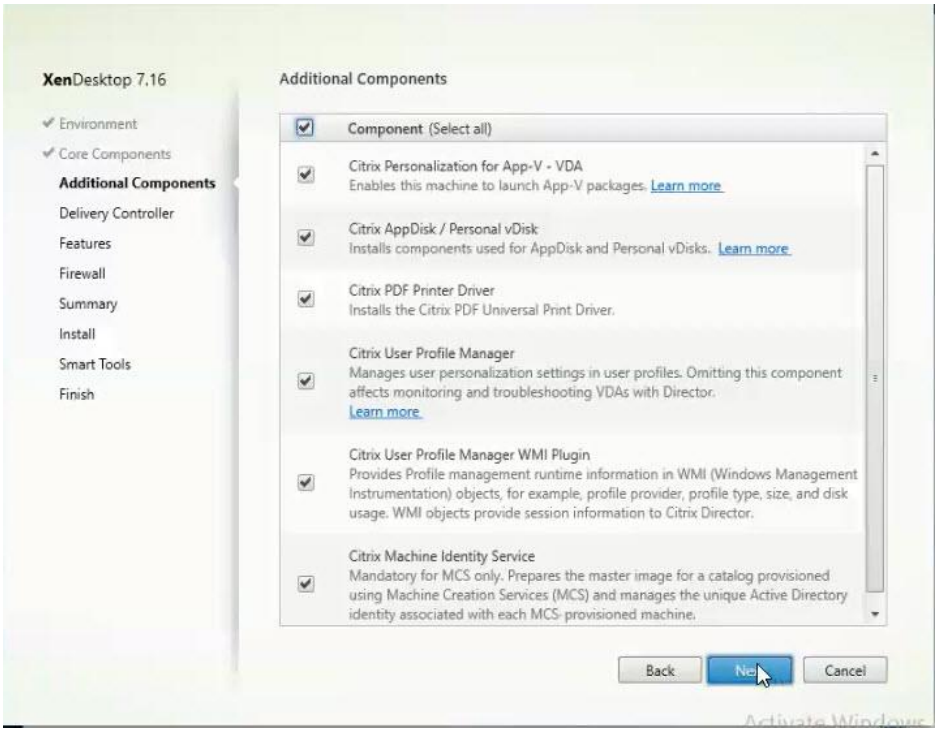


6. Optional: Select Citrix Receiver.

7. Click Next.

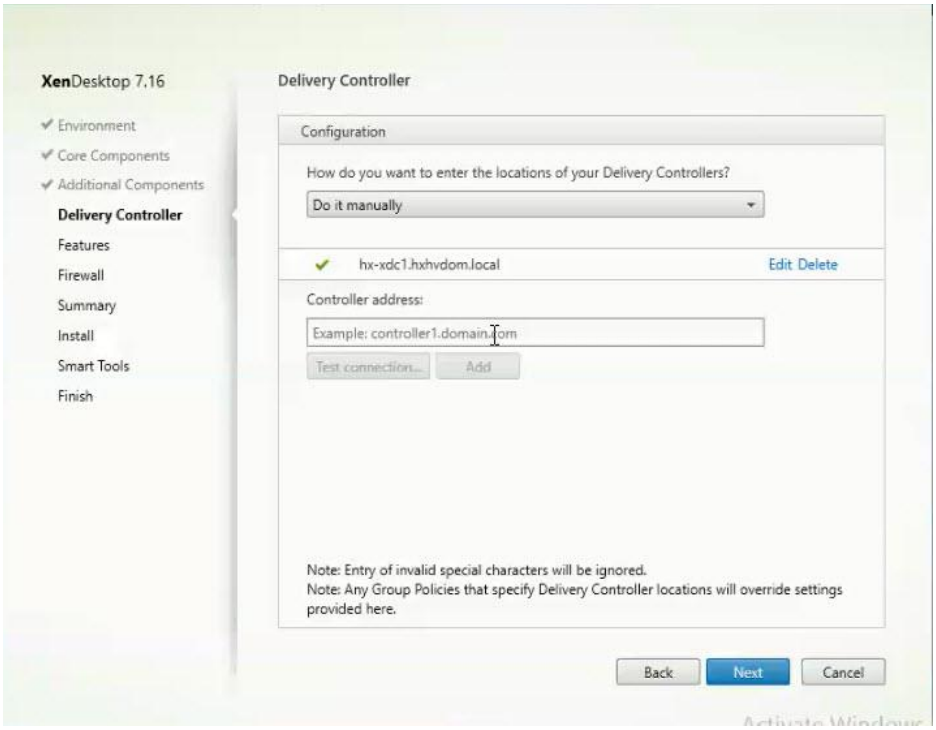


8. Click Next.



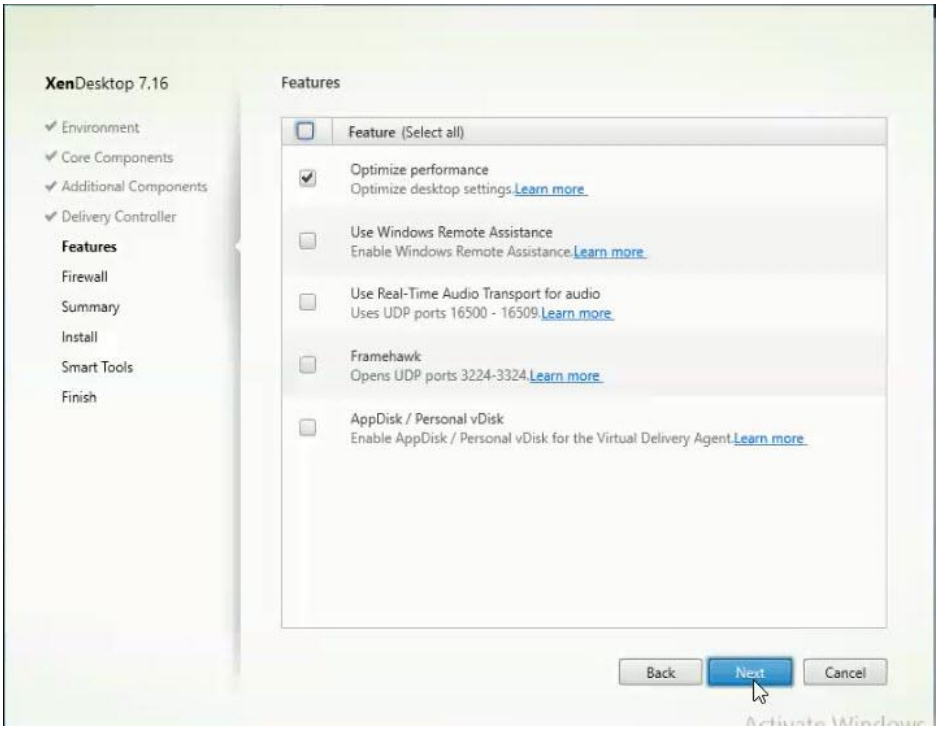
9. Select “Do it manually” and specify the FQDN of the Delivery Controllers.

10. Click Next.



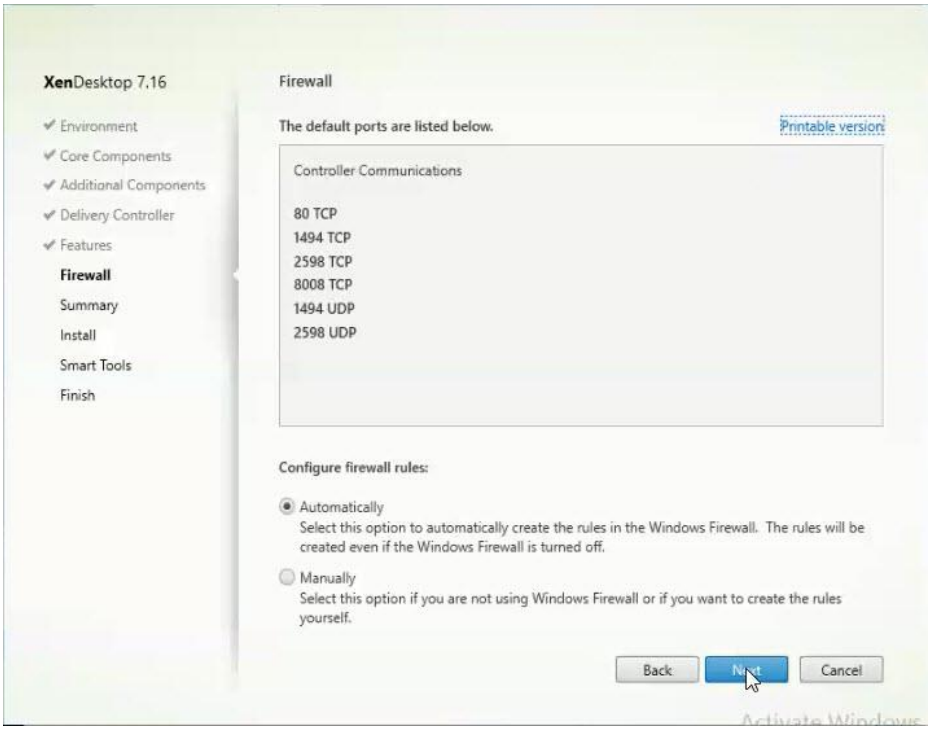
11. Accept the default features.

12. Click Next.

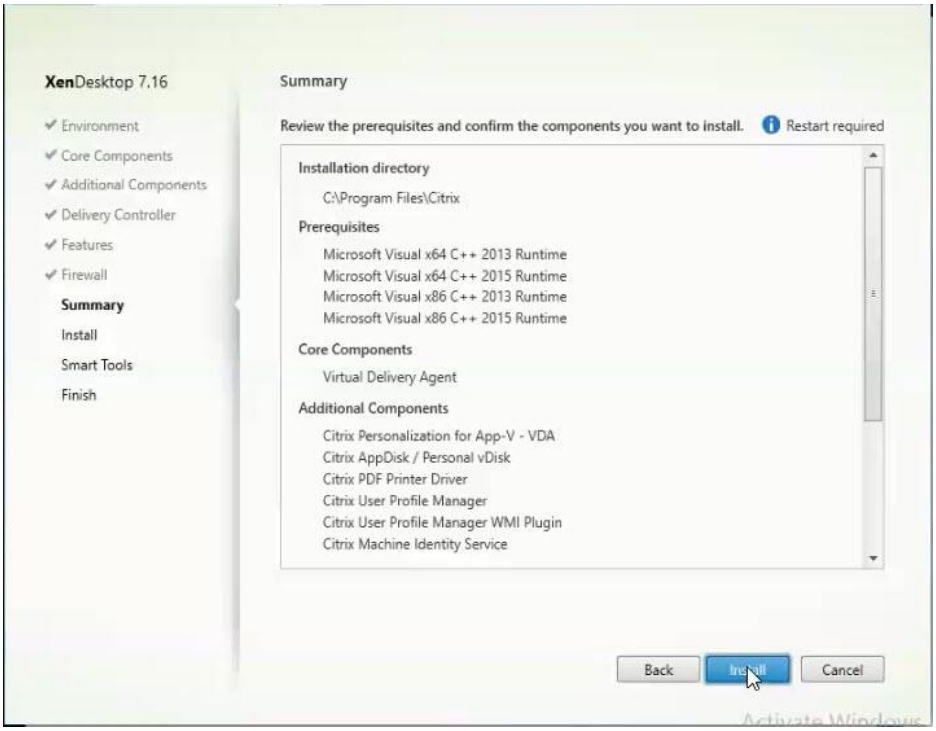


13. Allow the firewall rules to be configured Automatically.

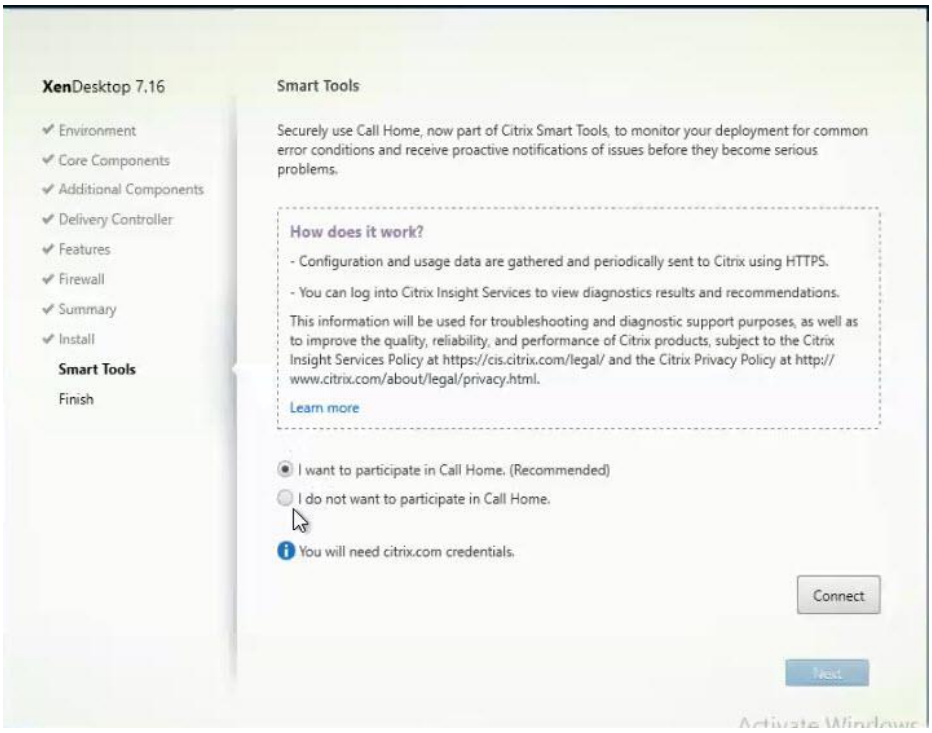
14. Click Next.



15. Verify the Summary and click Install.

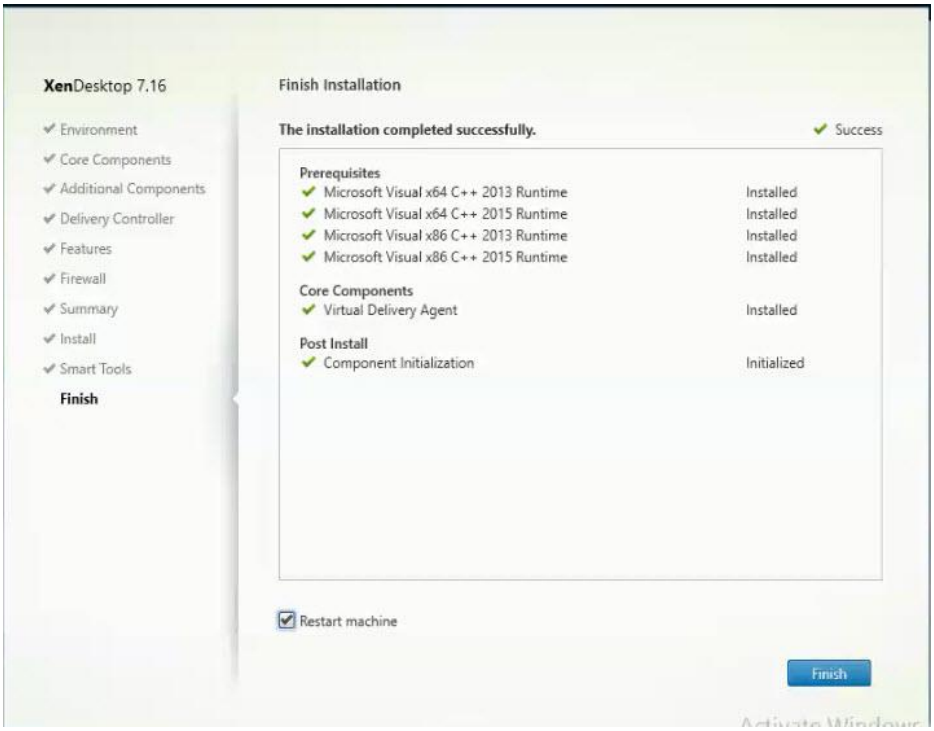


16. (Optional) Select Call Home participation.



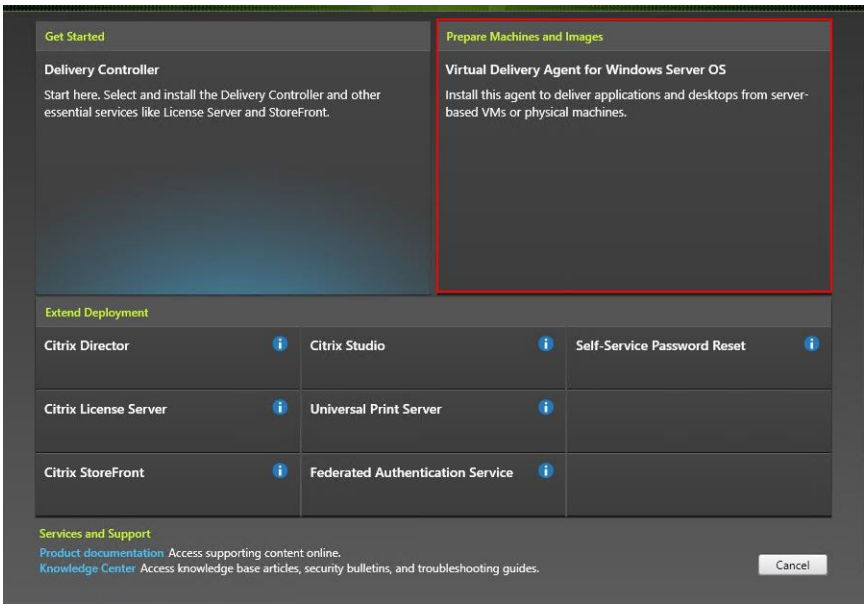
17. (Optional) check “Restart Machine.”

18. Click Finish.



19. Repeat the procedure so that VDAs are installed for both HVD (using the Windows 10 OS image) and the HSD desktops (using the Windows Server 2016 image).

20. Select an appropriate workflow for the HSD desktop.



Install the Citrix Provisioning Services Target Device Software

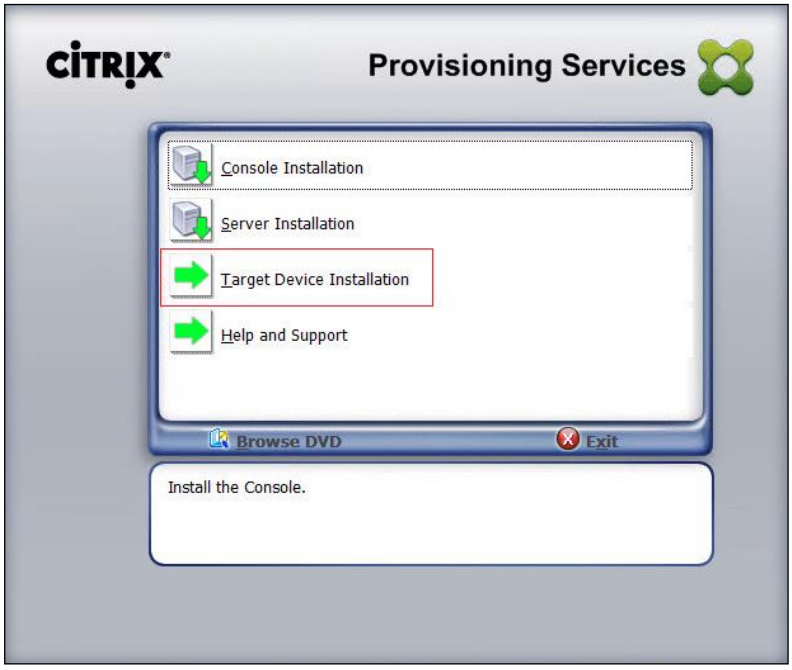
The Master Target Device refers to the target device from which a hard disk image is built and stored on a vDisk. Provisioning Services then streams the contents of the vDisk created to other target devices. This procedure installs the PVS Target Device software that is used to build the RDS and VDI golden images.

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

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

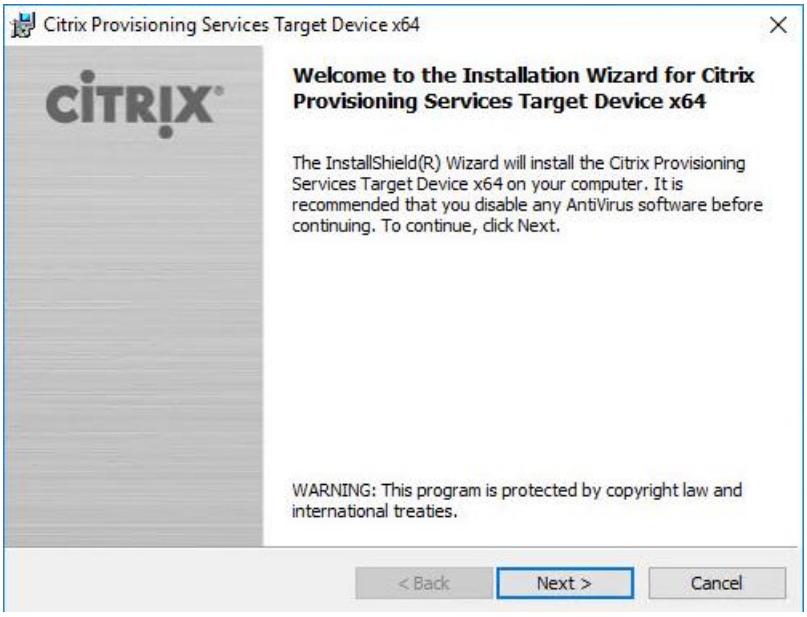
1. On the Window 10 Master Target Device, launch the PVS installer from the Provisioning Services 7.16 ISO.

2. Click the Target Device Installation button.

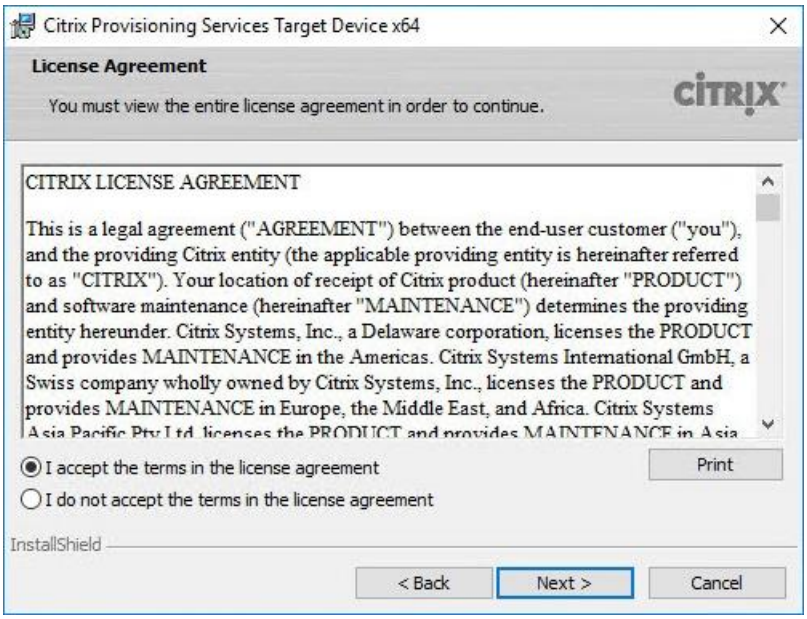


The installation wizard will check to resolve dependencies and then begin the PVS target device installation process.

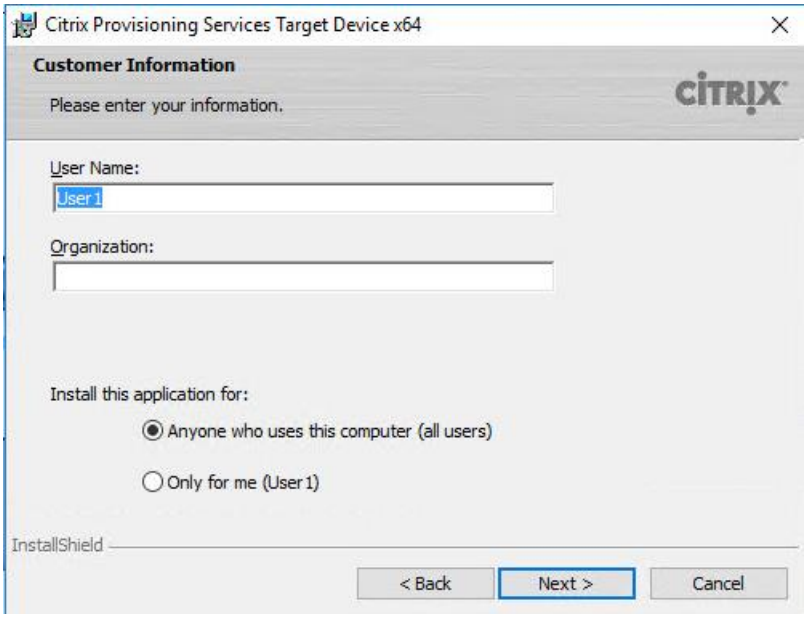
3. Click Next.



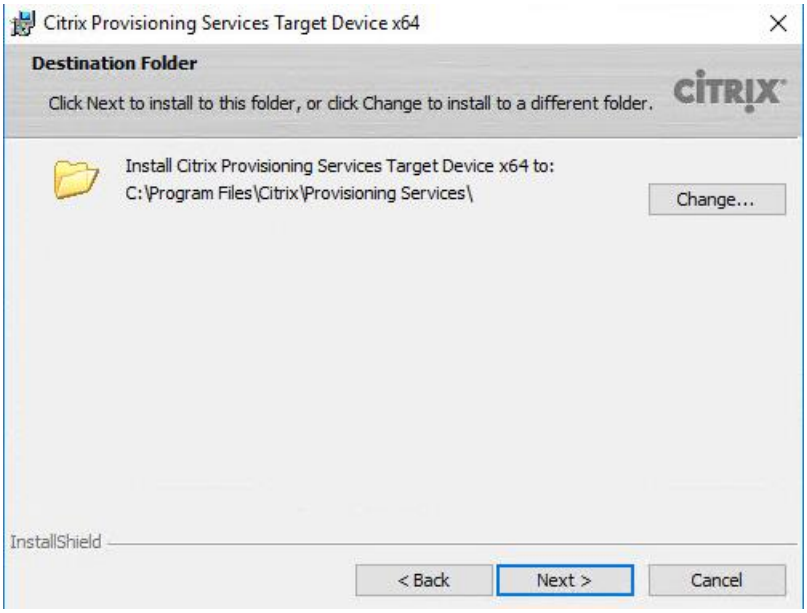
4. Accept License Agreement and click Next.



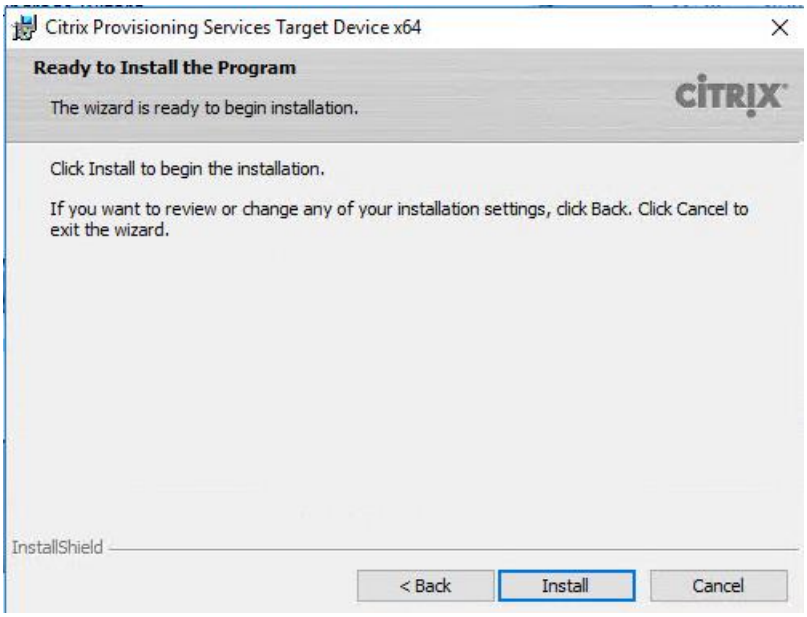
5. Click Next.



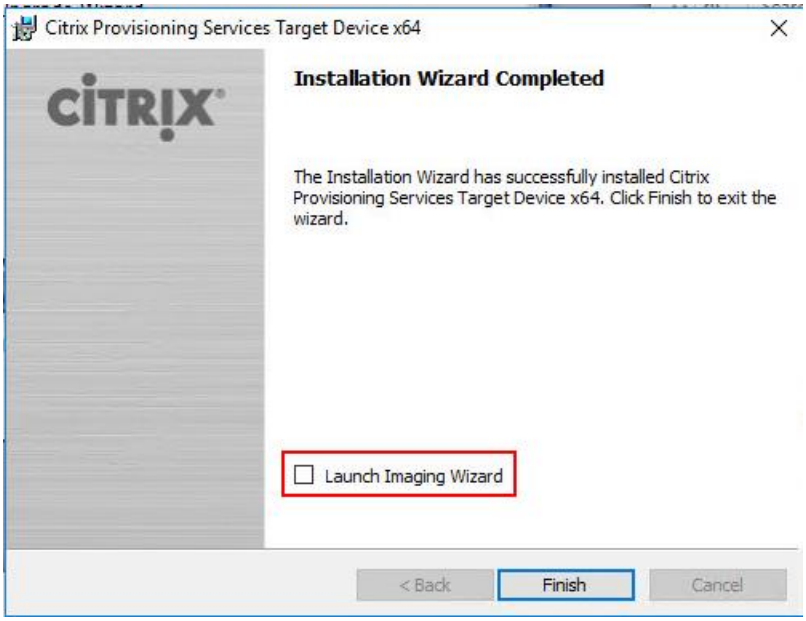
6. Confirm the installation settings and click Next.



7. Click Install.



8. Deselect the checkbox to launch the Imaging Wizard and click Finish.



9. Reboot the machine.

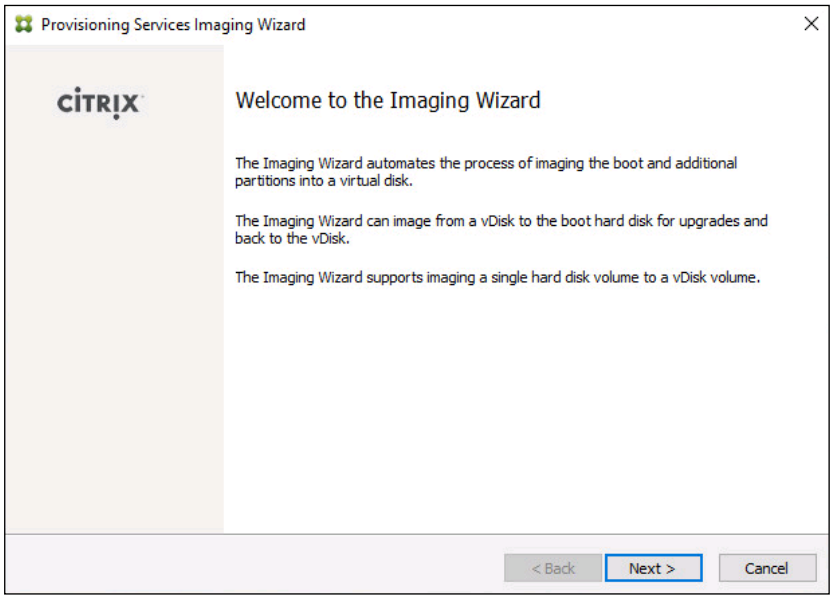
Create Citrix Provisioning Services vDisks

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

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

1. The PVS Imaging Wizard's Welcome page appears.

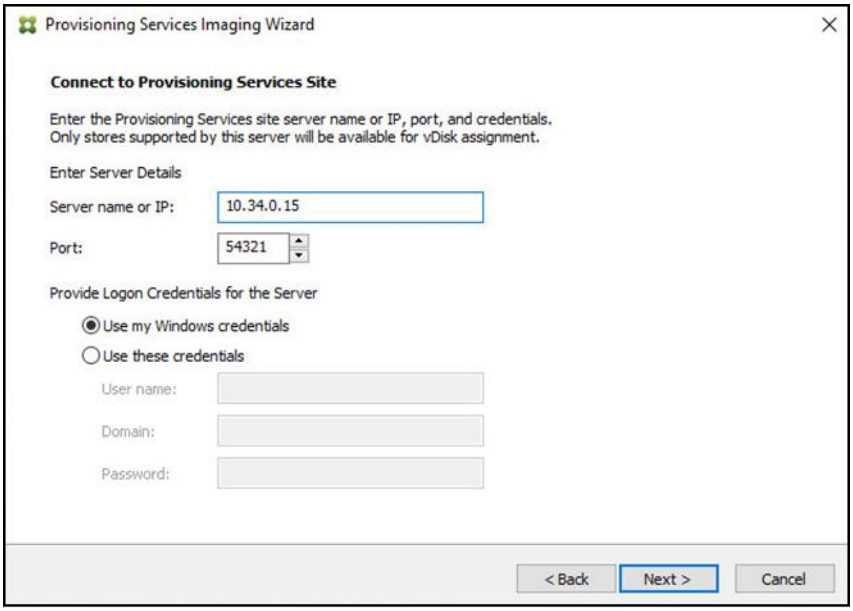
2. Click Next.



3. The Connect to Farm page appears. Enter the name or IP address of a Provisioning Server within the farm to connect to and the port to use to make that connection.

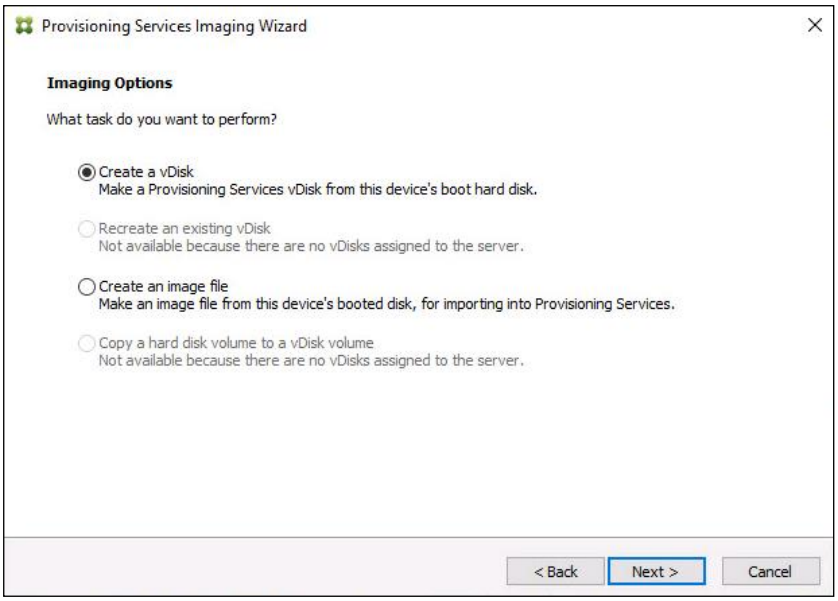
4. Use the Windows credentials (default) or enter different credentials.

5. Click Next.



6. Select Create new vDisk.

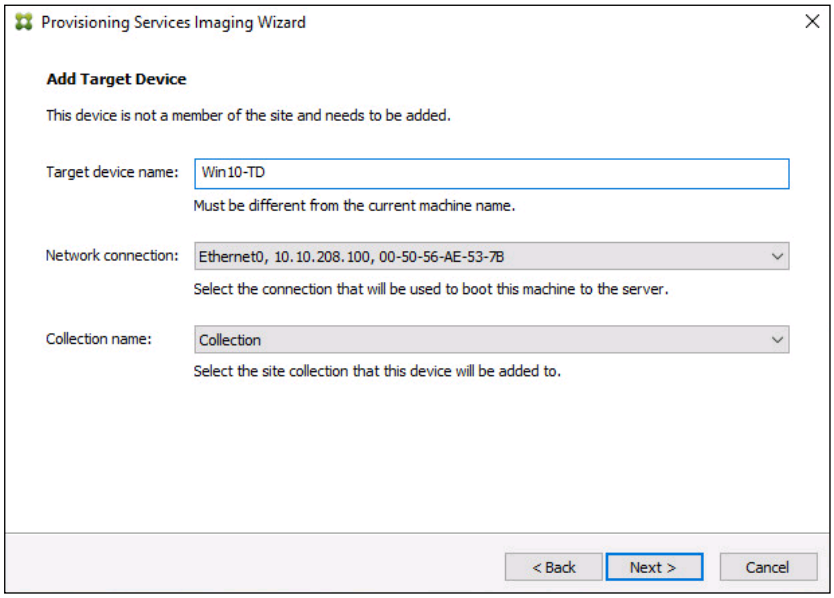
7. Click Next.



8. The Add Target Device page appears.

9. Select the Target Device Name, the MAC address associated with one of the NICs that was selected when the target device software was installed on the master target device, and the Collection to which you are adding the device.

10. Click Next.

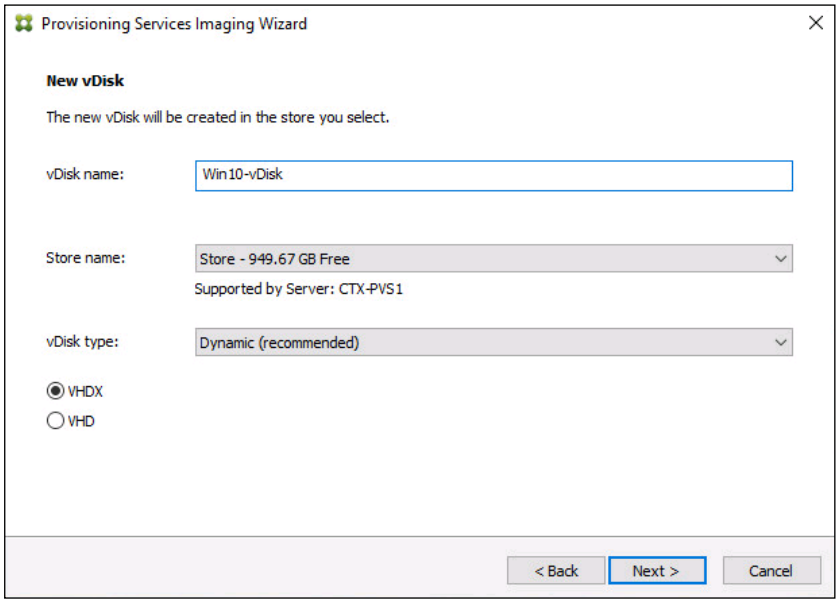


11. The New vDisk dialog displays. Enter the name of the vDisk.

12. Select the Store where the vDisk will reside. Select the vDisk type, either Fixed or Dynamic, from the drop-down list.

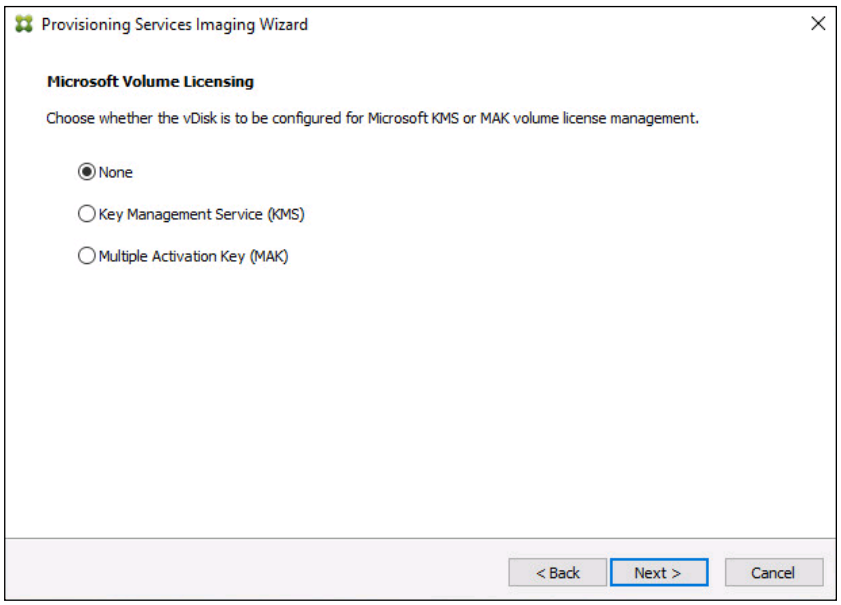
This CVD used Dynamic rather than Fixed vDisks.

13. Click Next.



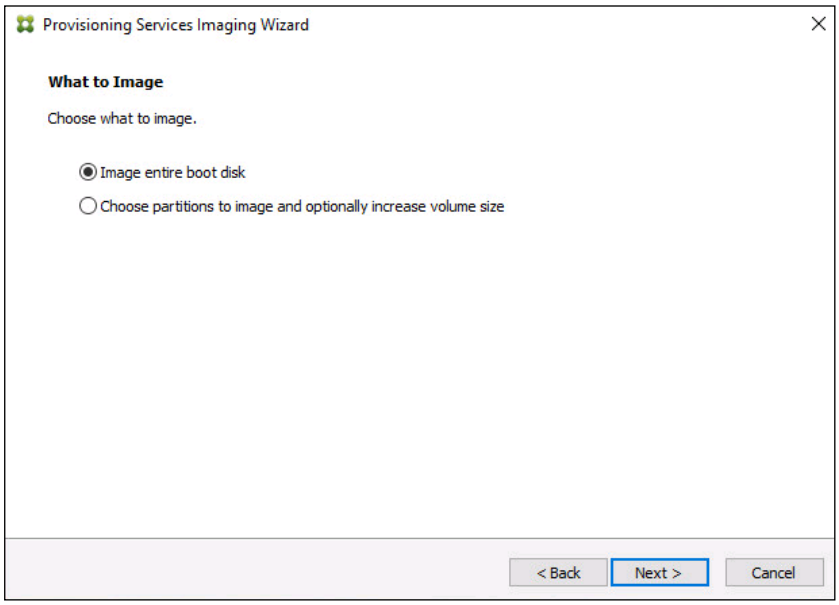
14. On the Microsoft Volume Licensing page, select the volume license option to use for target devices. For this CVD, volume licensing is not used, so the None button is selected.

15. Click Next.



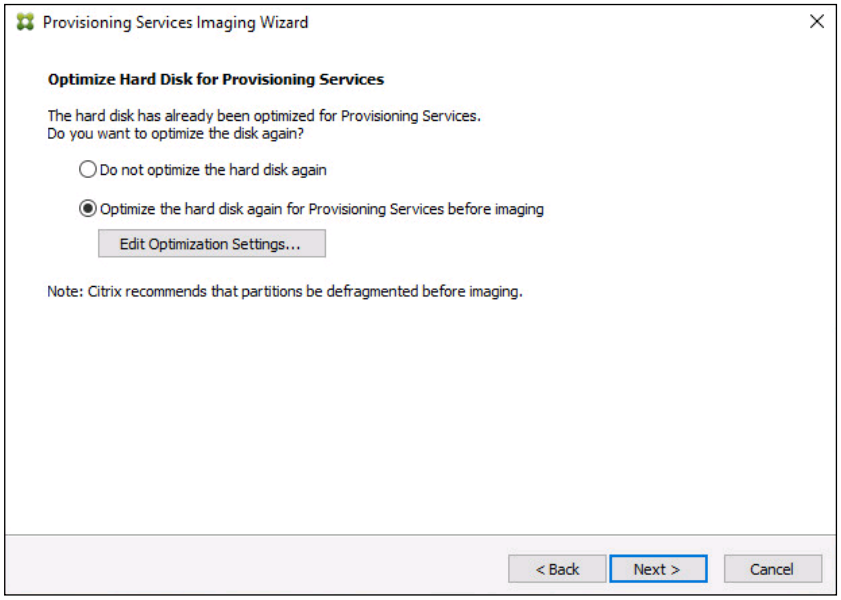
16. Select Image entire boot disk on the Configure Image Volumes page.

17. Click Next.

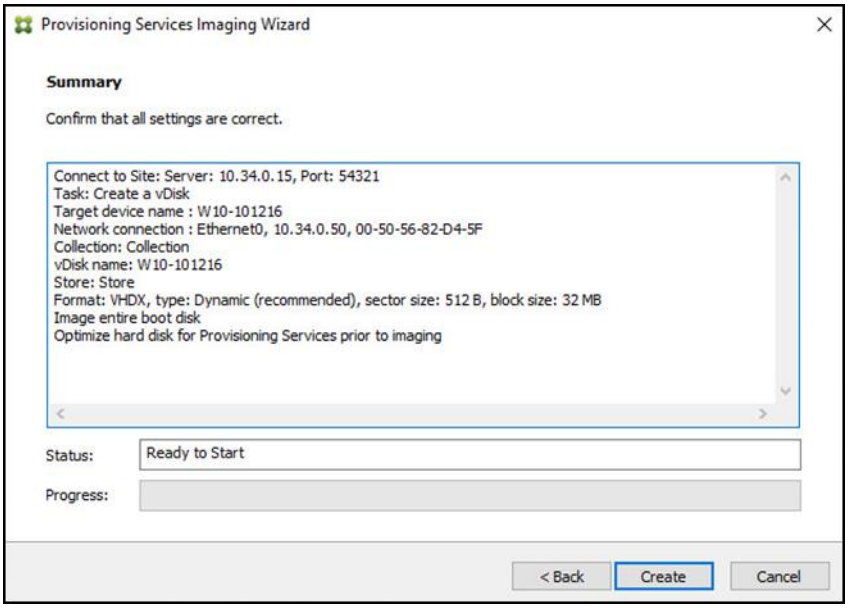


18. Select Optimize for hard disk again for Provisioning Services before imaging on the Optimize Hard Disk for Provisioning Services.

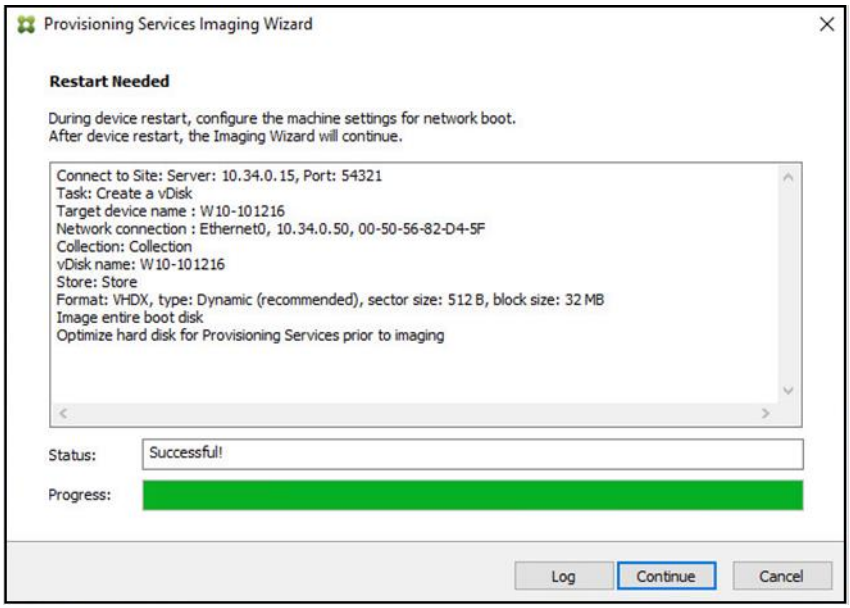
19. Click Next.



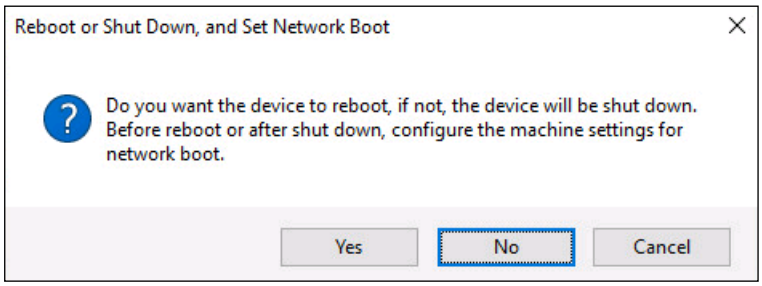
20. Select Create on the Summary page.



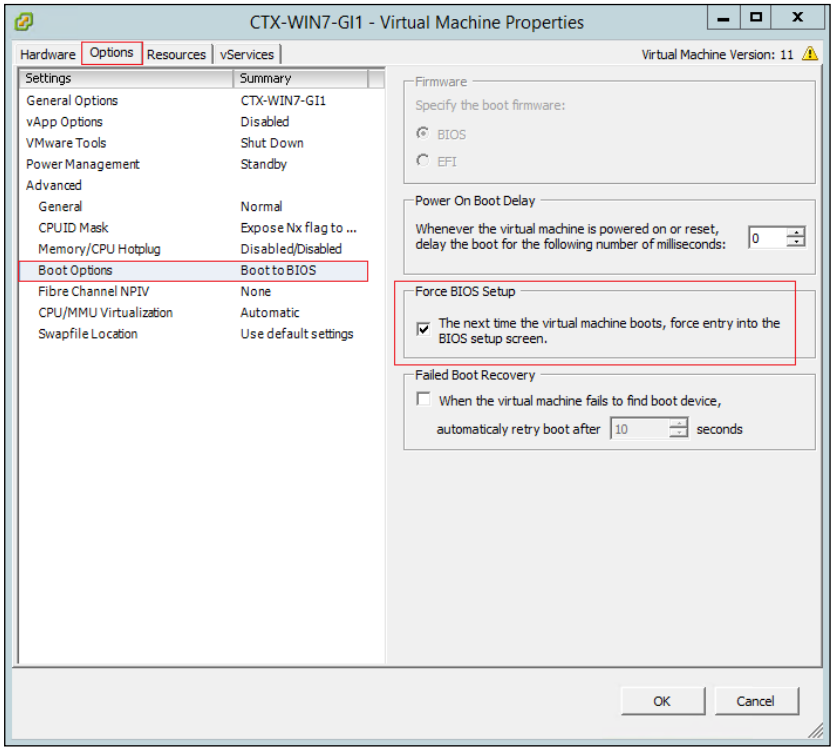
21. Review the configuration and click Continue.



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



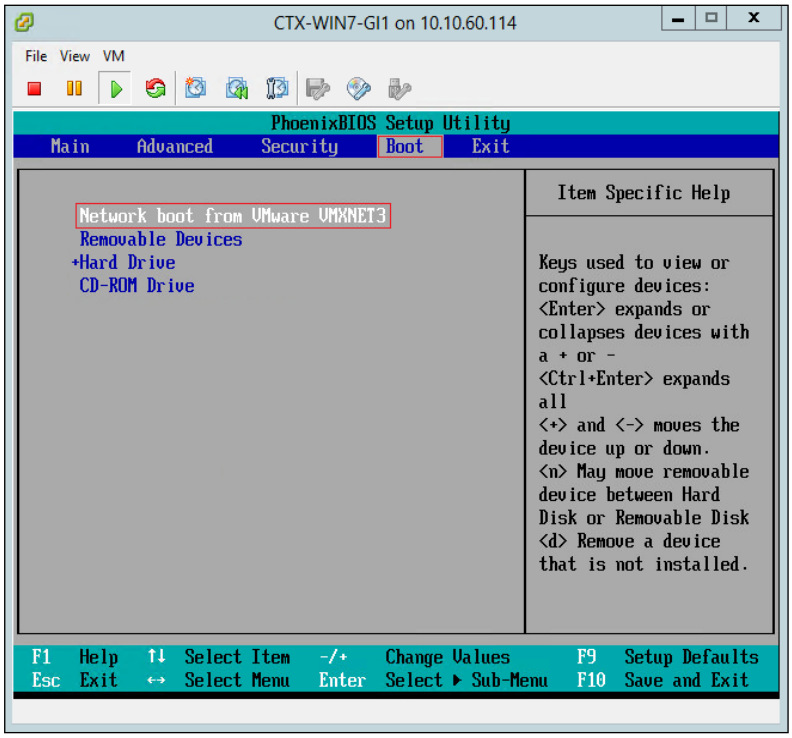
23. Edit the VM settings and select Force BIOS Setup under Boot Options.



24. Restart Virtual Machine.

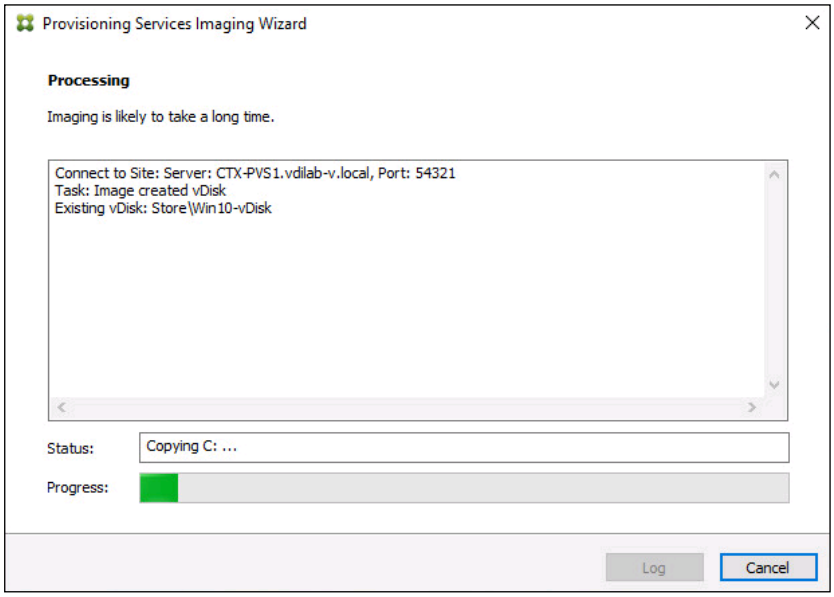
25. Configure the BIOS/VM settings for PXE/network boot, putting Network boot from VMware VMXNET3 at the top of the boot device list.

26. Select Exit Saving Changes.

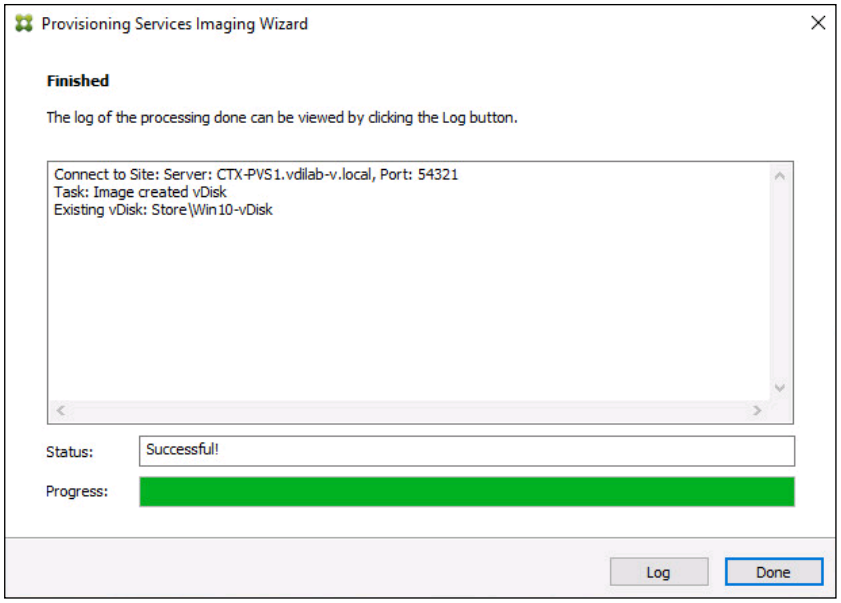


After restarting the VM, log into the VDI or RDS master target. The PVS imaging process begins, copying the contents of the C: drive to the PVS vDisk located on the server.

27. If prompted to restart select Restart Later.



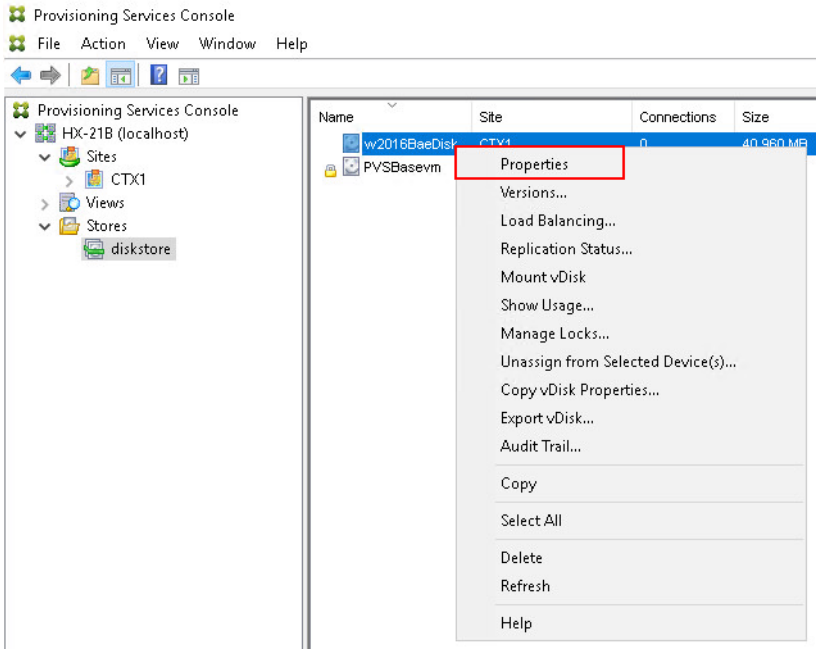
28. A message is displayed when the conversion is complete, click Done.



29. Shutdown the VM used as the HVD or HSD master target.

30. Connect to the PVS server and validate that the vDisk image is available in the Store.

31. Right-click the newly created vDisk and select Properties.

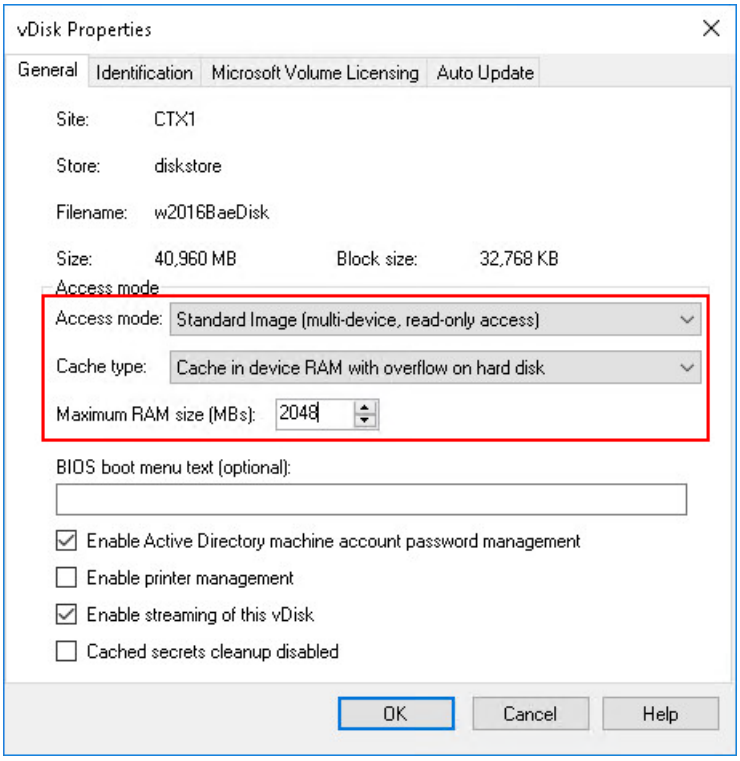


32. On the vDisk Properties dialog, change Access mode to “Standard Image (multi-device, read-only access)”.

33. Set the Cache Type to “Cache in device RAM with overflow on hard disk.”

34. Set Maximum RAM Size (for testing 2GB was used for Windows Server 2016 and 128 MB was used Windows 10 virtual machines).

35. Click OK.



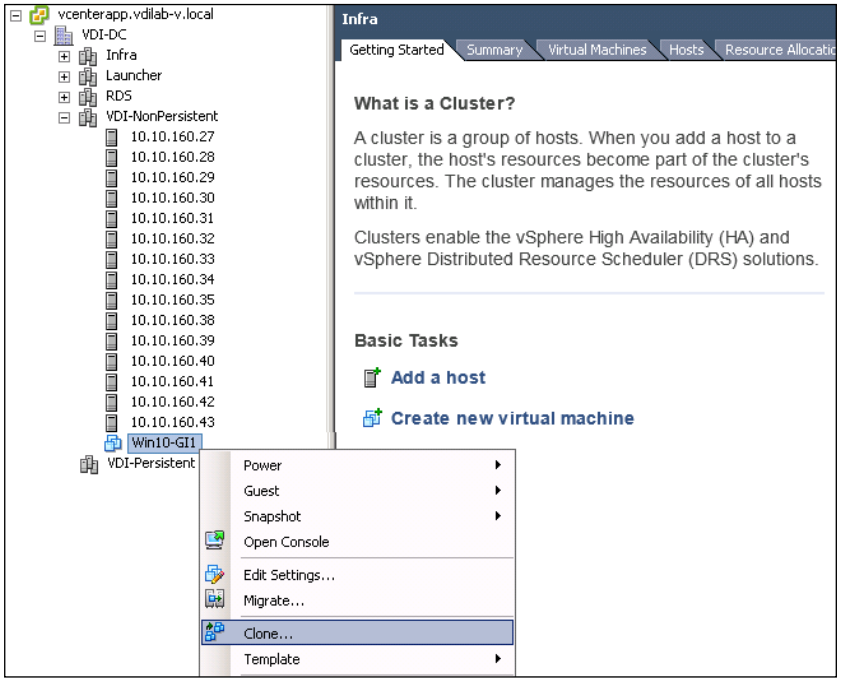
Repeat this procedure to create vDisks for both the Hosted VDI Desktops (using the Windows 10 OS image) and the Hosted Shared Desktops (using the Windows Server 2016 image).

Provision Virtual Desktop Machines

Non-Persistent PVS streamed desktops

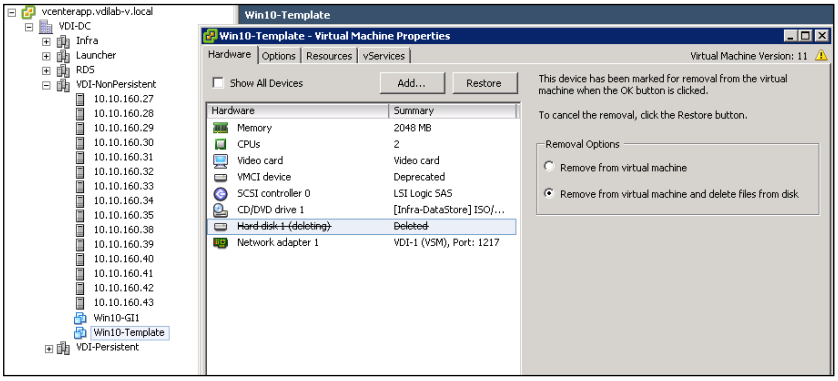
To create HVD and HSD machines, complete the following steps:

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

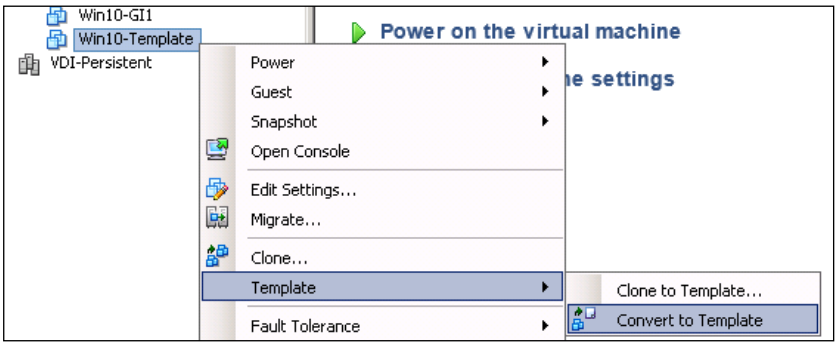


5. Remove Hard disk 1 from the Template VM.

Hard disk 1 is not required to provision desktop machines as the XenDesktop Setup Wizard dynamically creates the write cache disk.



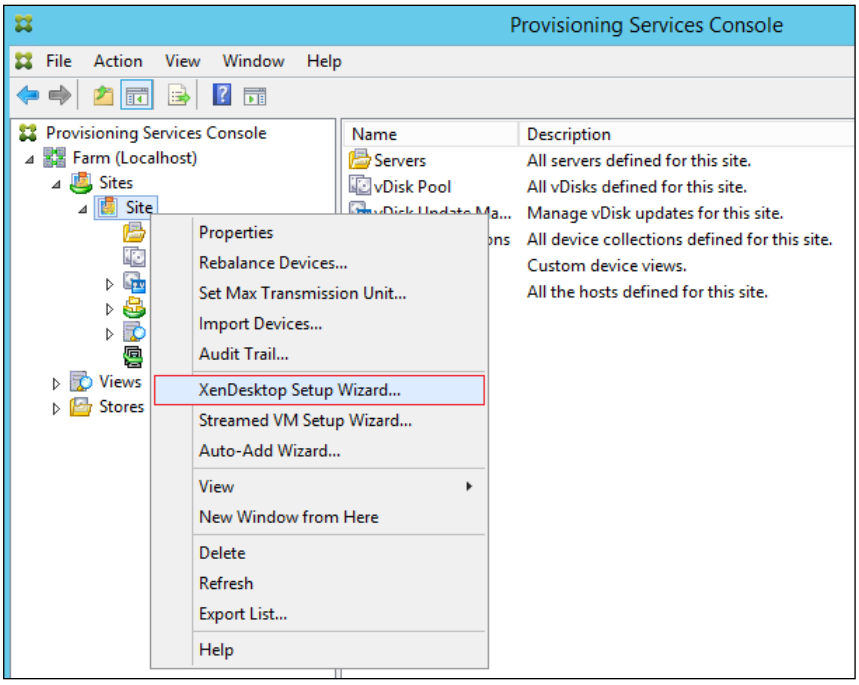
6. Convert to the Desktop-Template VM to a Template.



7. Start the XenDesktop Setup Wizard from the Provisioning Services Console.

8. Right-click the Site.

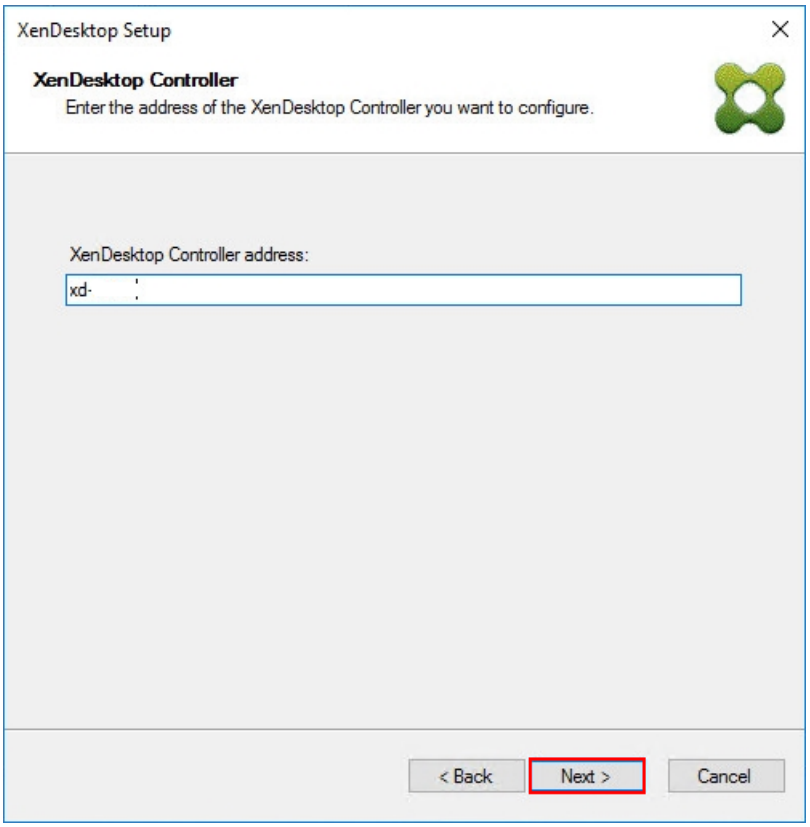
9. Choose XenDesktop Setup Wizard… from the context menu.



10. Click Next.

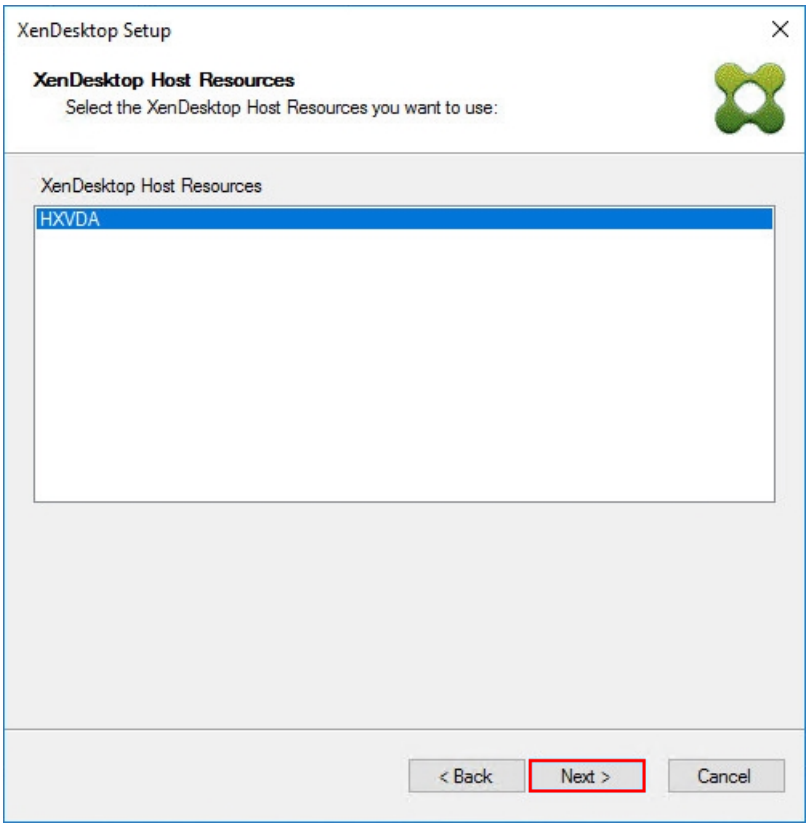
11. Enter the XenDesktop Controller address that will be used for the wizard operations.

12. Click Next.



13. Select the Host Resources on which the virtual machines will be created.

14. Click Next.

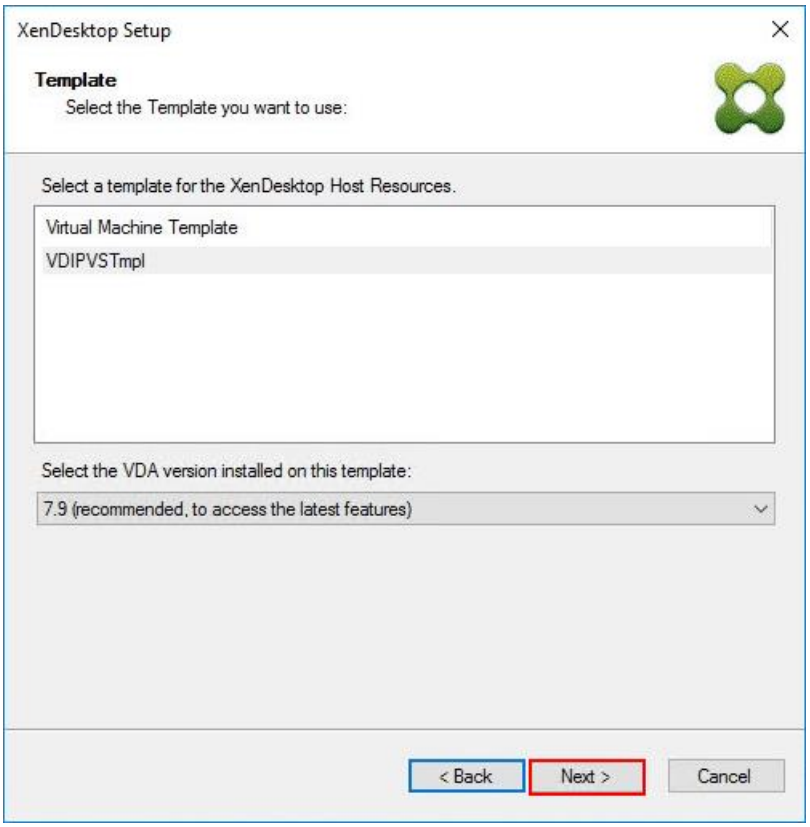


15. Provide the Host Resources Credentials (Username and Password) to the XenDesktop controller when prompted.

16. Click OK.

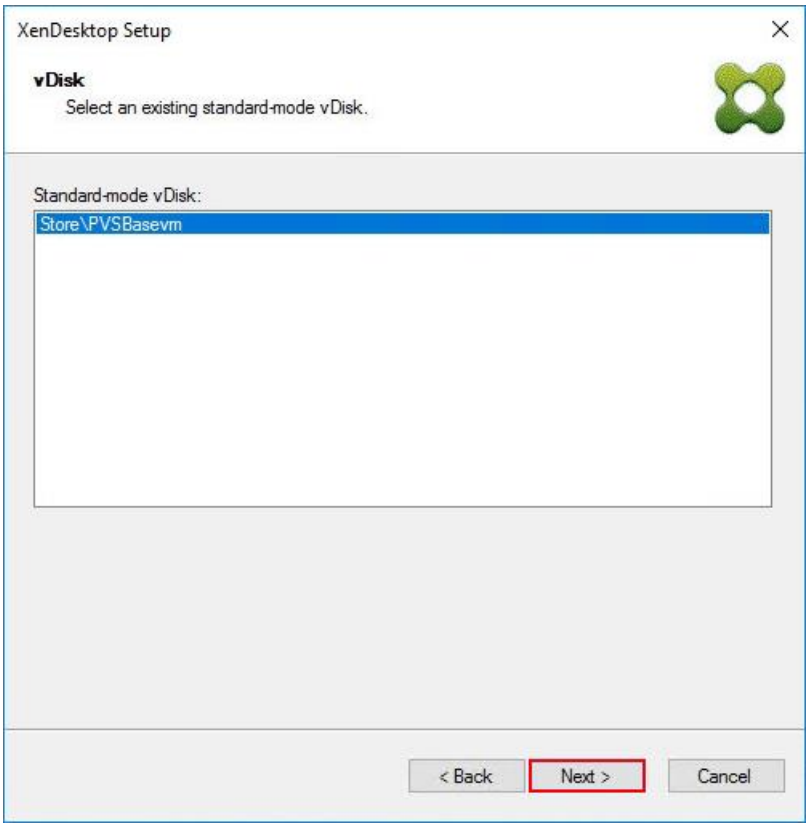
17. Select the Template created earlier.

18. Click Next.



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

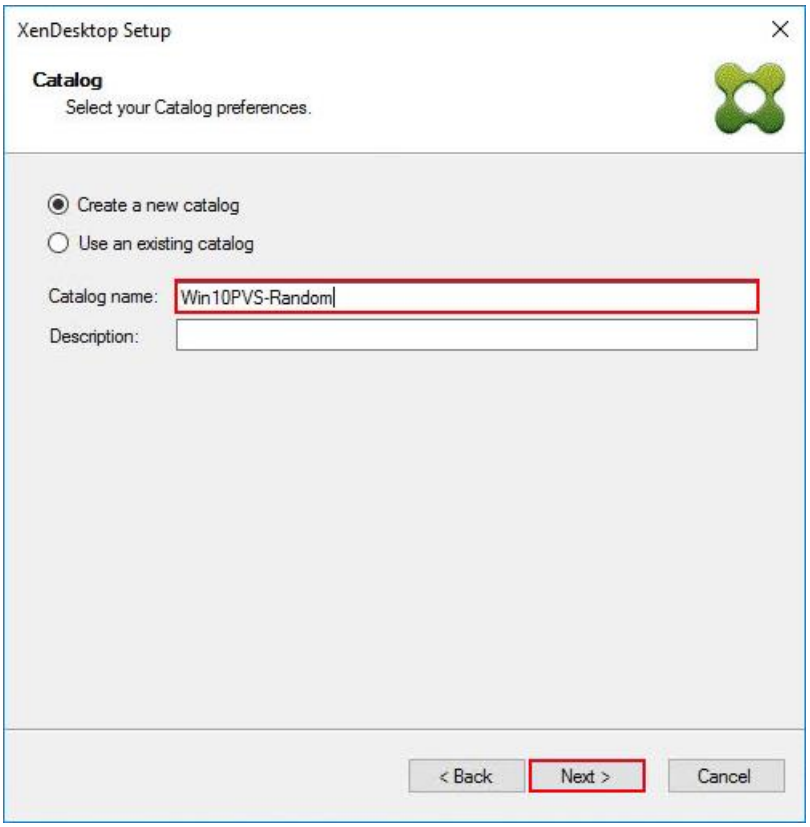
20. Click Next.



21. Select “Create a new catalog” and provide catalog name.

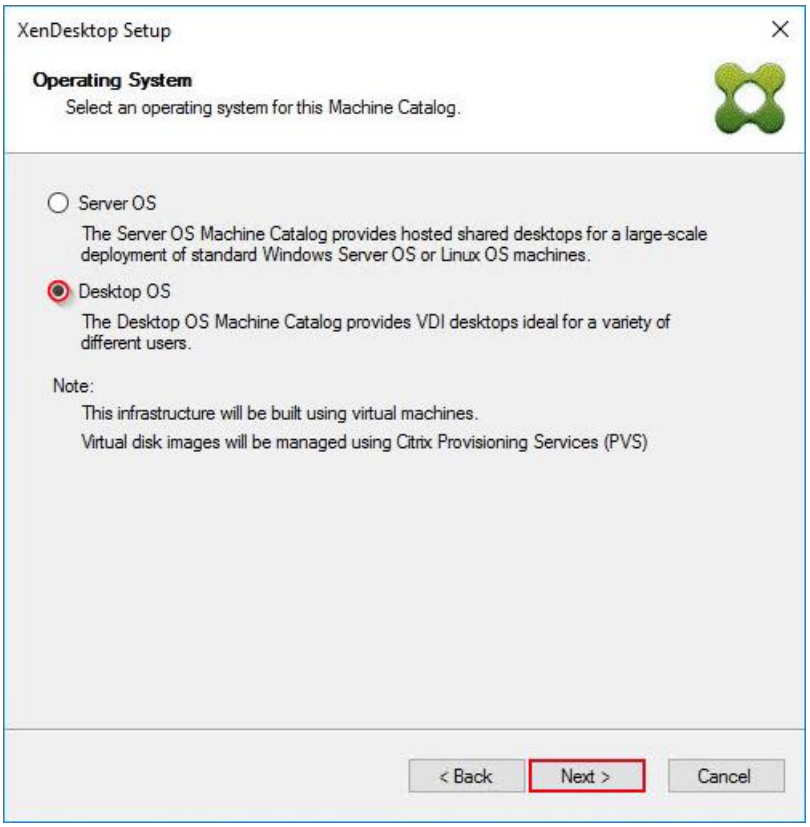
The catalog name is also used as the collection name in the PVS site.

22. Click Next.



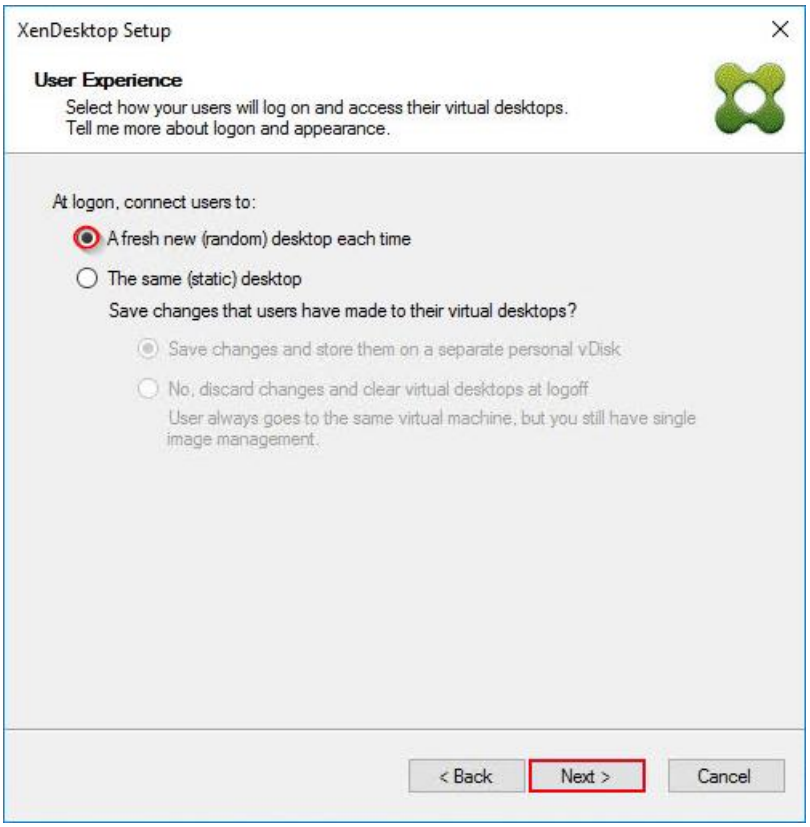
23. On the Operating System dialog, specify the operating system for the catalog. Specify Desktop OS for VDI and Server OS for RDS.

24. Click Next.



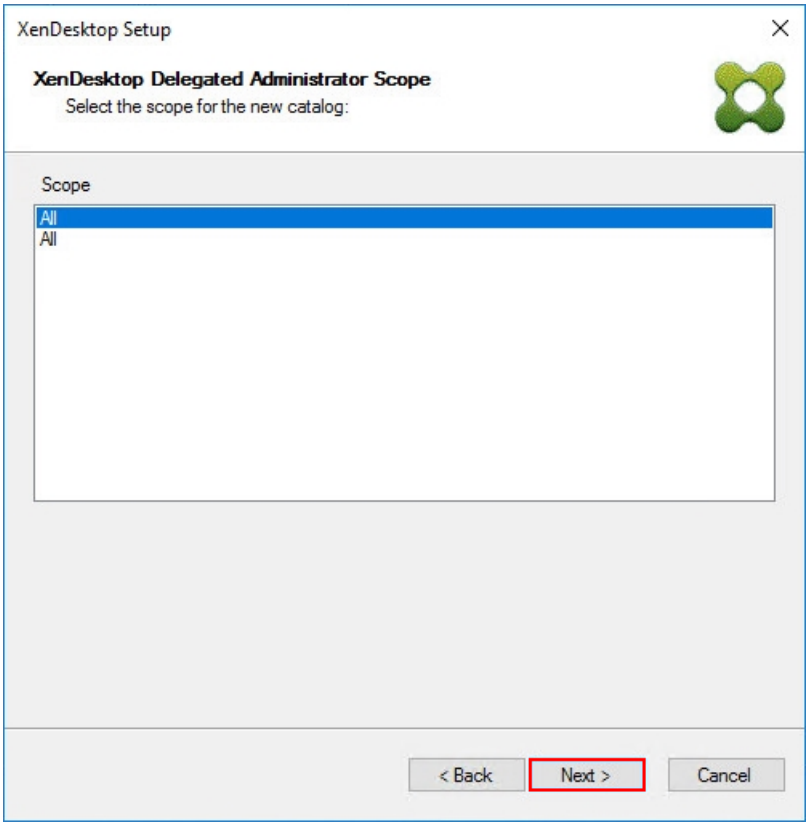
25. If you specified a Windows Desktop OS for VDIs, a User Experience dialog appears. Specify that the user will connect to “A fresh new (random) desktop each time.”

26. Click Next.



27. Chose a Scope for the new Catalog.

28. Click Next.



29. On the Virtual machines dialog, specify:

    a. The **number** of VMs to create. (Note that it is recommended to create 200 or less per provisioning run. Create a single VM at first to verify the procedure.)

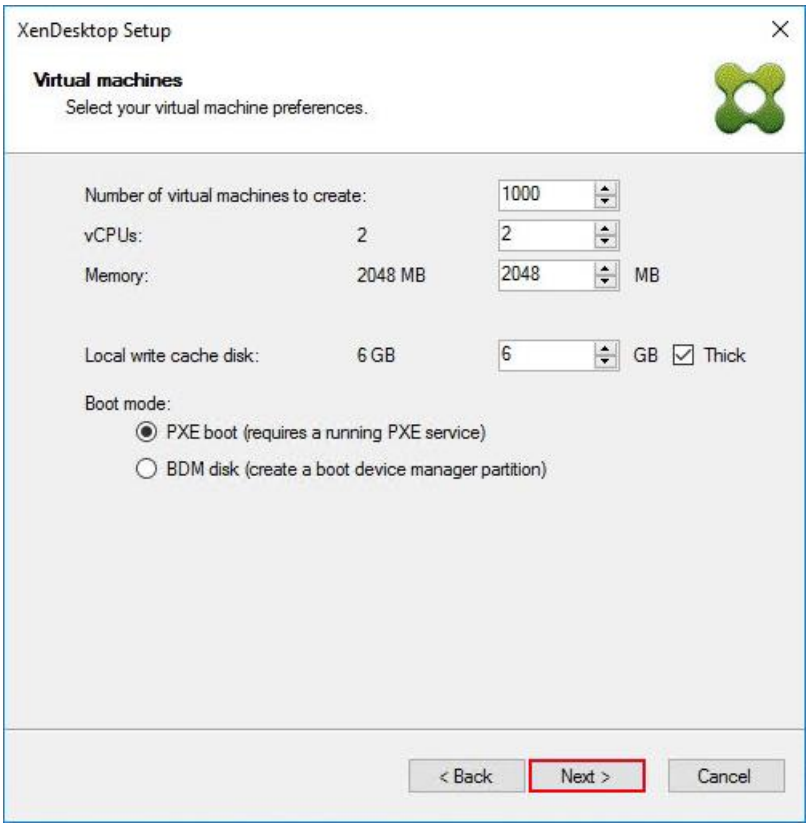
    b. Number of **vCPUs** for the VM (2 for VDI, 6 for RDS)

    c. The amount of **memory** for the VM (1.7GB for VDI, 24GB for RDS)

    d. The write-cache **disk size** (10GB for VDI, 30GB for RDS)

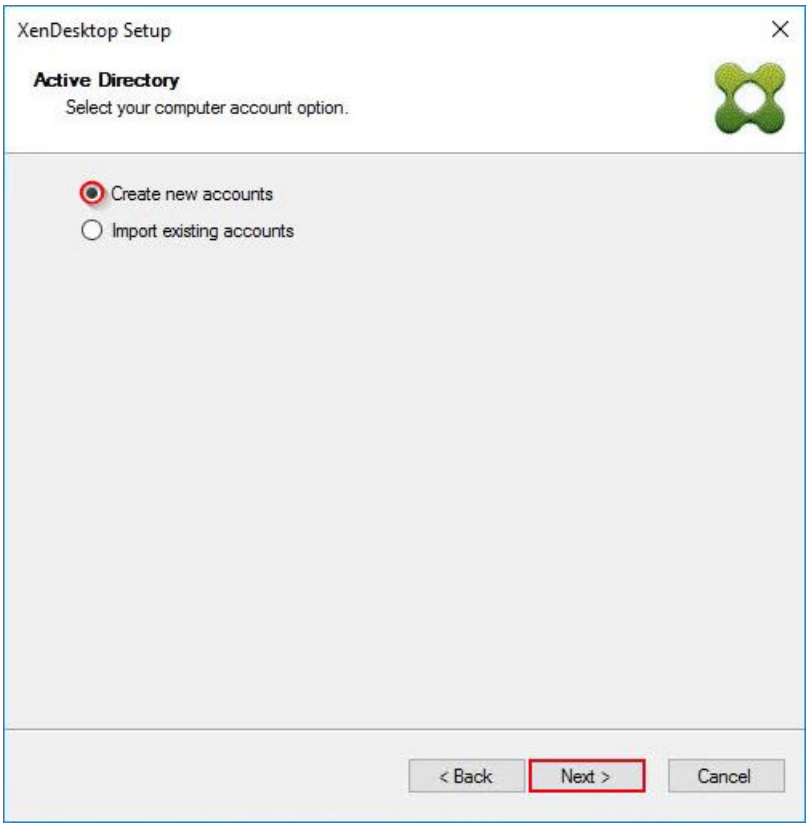
    e. PXE boot as the **Boot Mode**

30. Click Next.



31. Select the Create new accounts radio button.

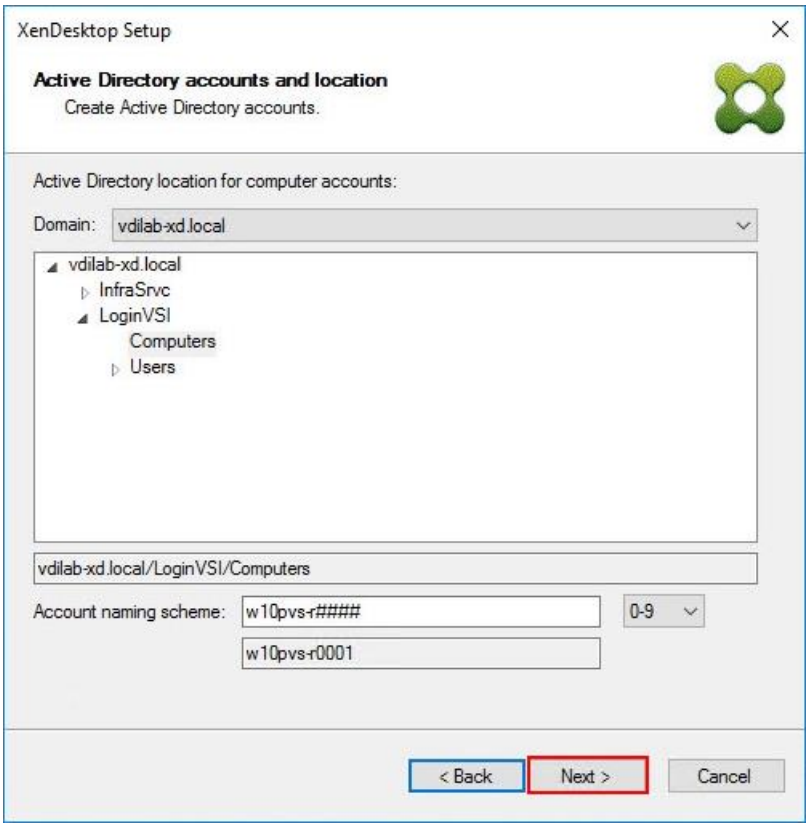
32. Click Next.



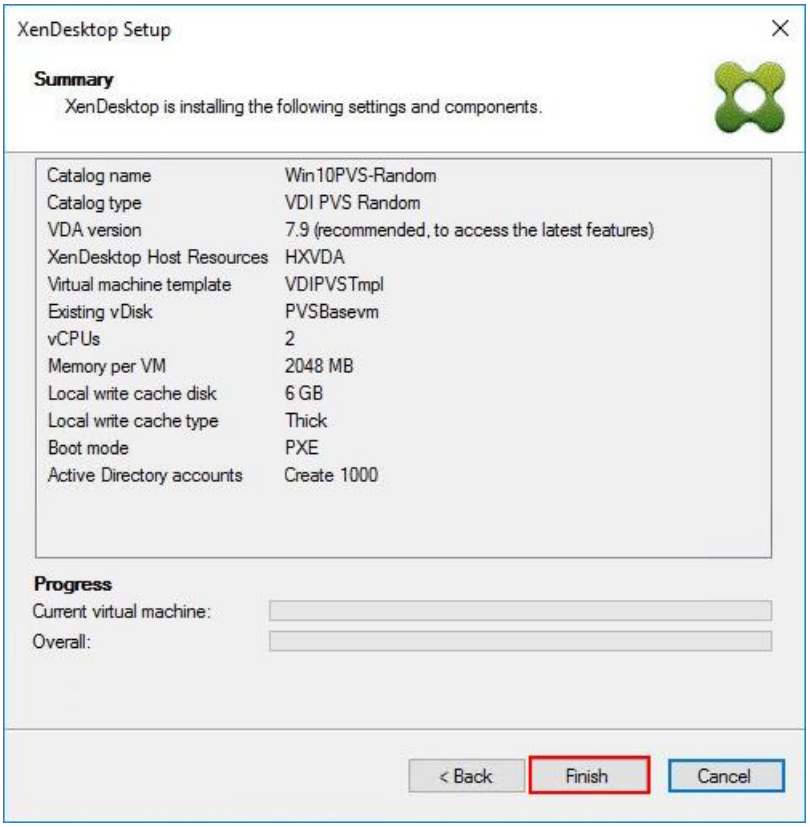
33. Specify the Active Directory Accounts and Location. This is where the wizard should create the computer accounts.

34. Provide the Account naming scheme. An example name is shown in the text box below the naming scheme selection location.

35. Click Next.



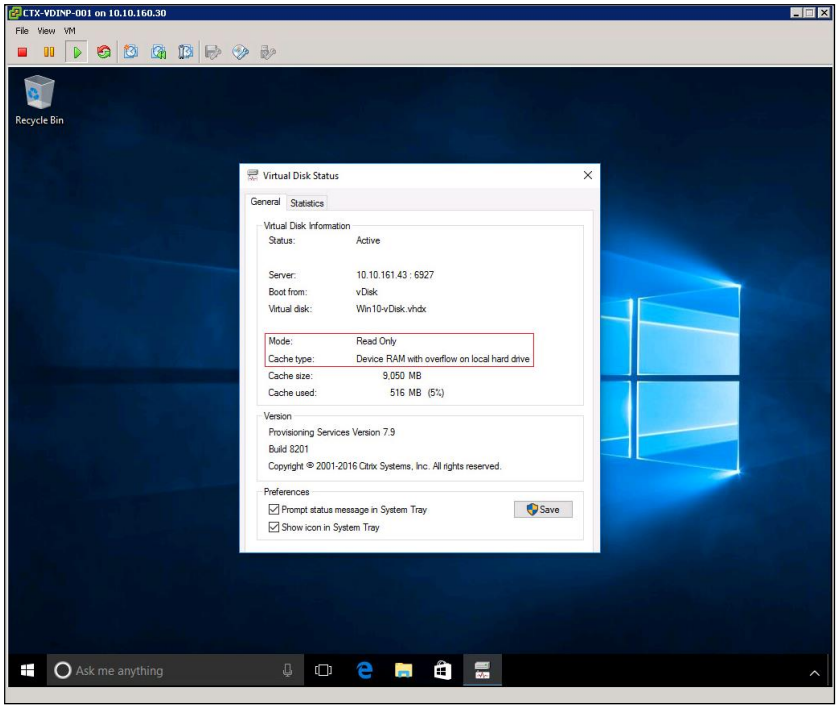
36. Click Finish to create the virtual machine.



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

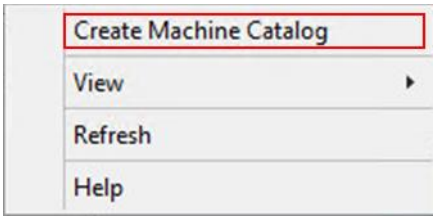
Provisioning process takes ~10 seconds per machine.

38. Verify the desktop machines were successfully created in the following locations:
    - Provisioning Server > Provisioning Services Console > Farm > Site > Device Collections
    - Delivery Controller > Citrix Studio > Machine Catalogs
    - Domain Controller > Active Directory Users and Computers
39. Logon to the newly provisioned desktop machine, using the Virtual Disk Status verify the image mode is set to Ready Only and the cache type as Device Ram with overflow on local hard drive.

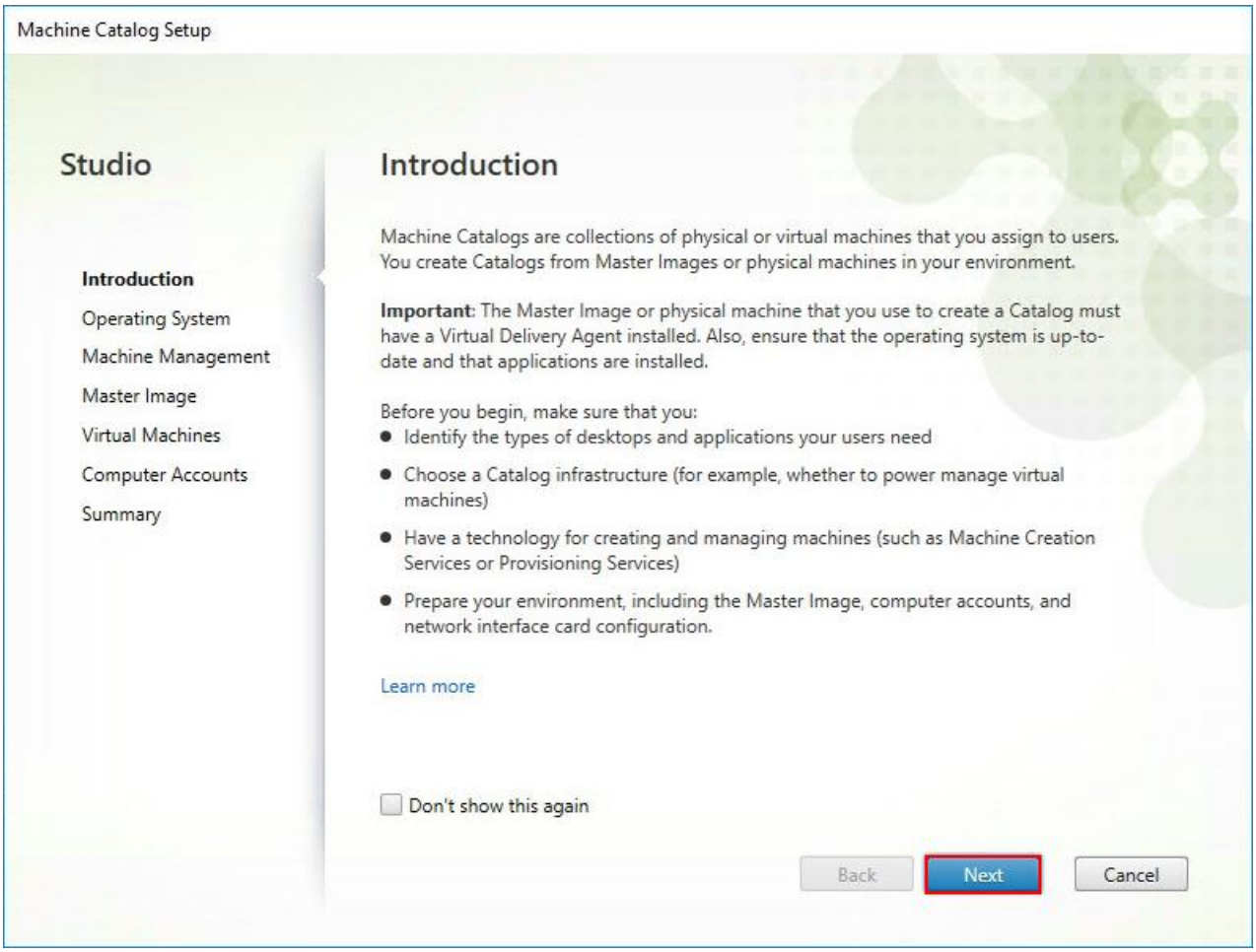


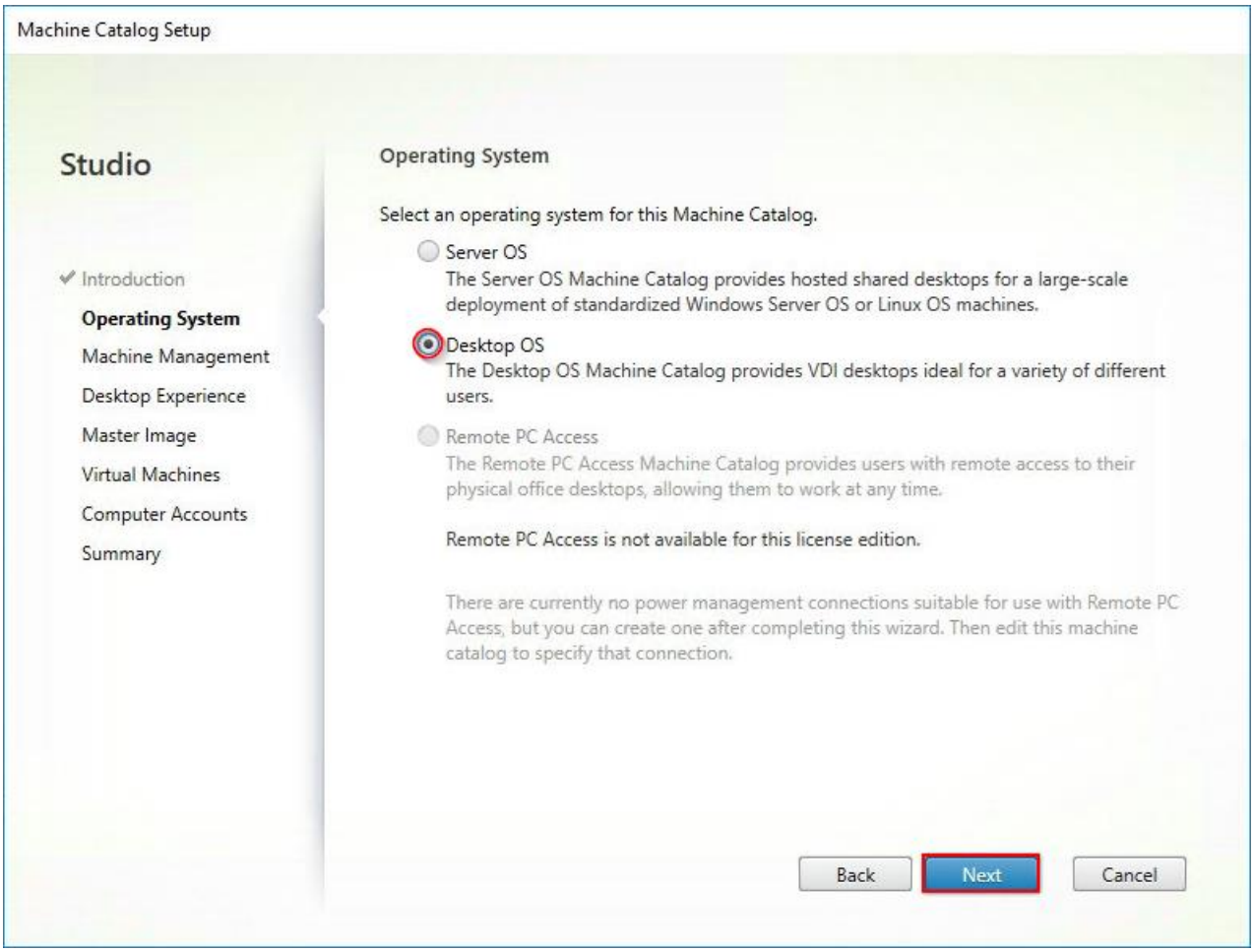
Non-persistent Random HVD Provisioned using MCS

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

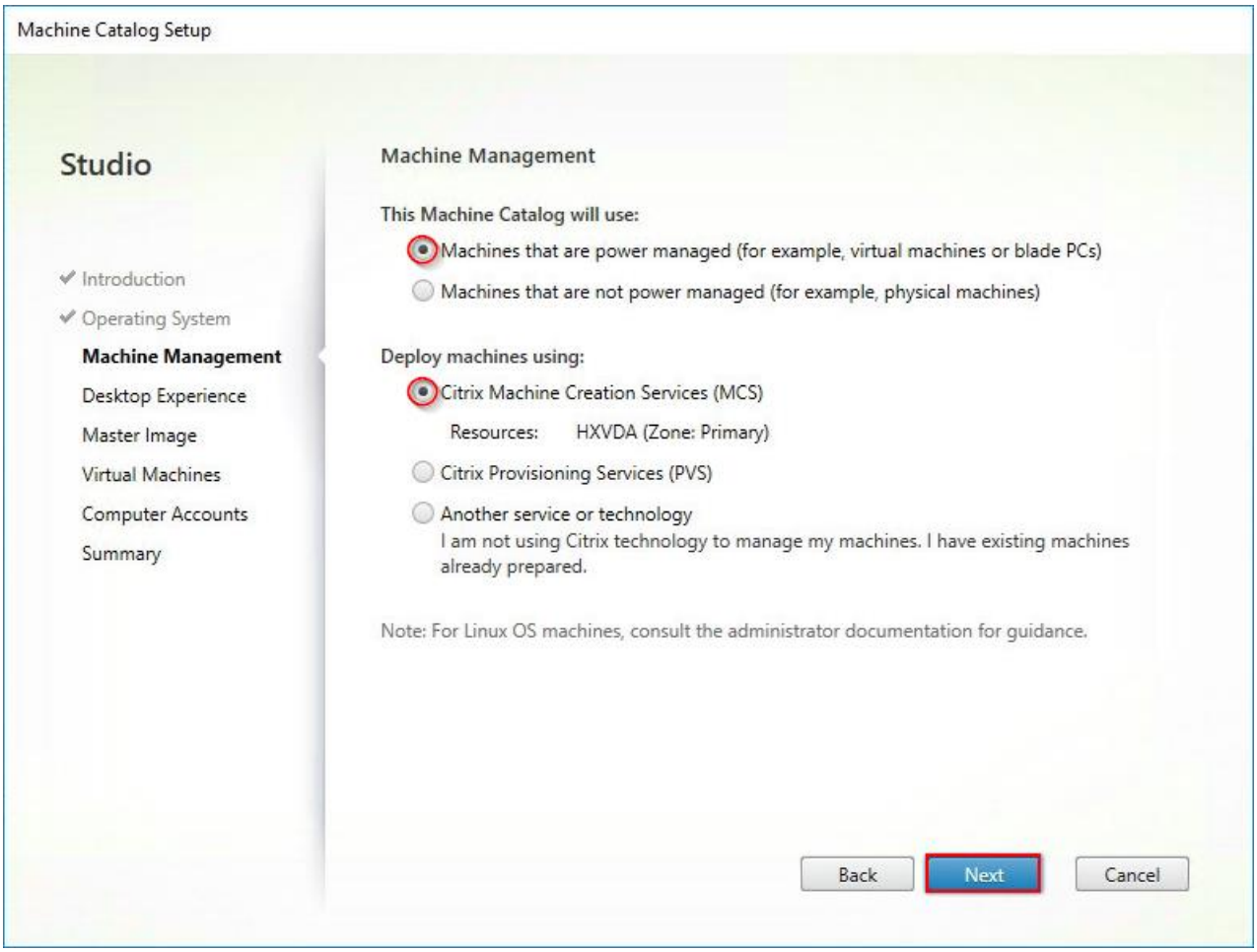


3. Select Desktop OS and click Next.

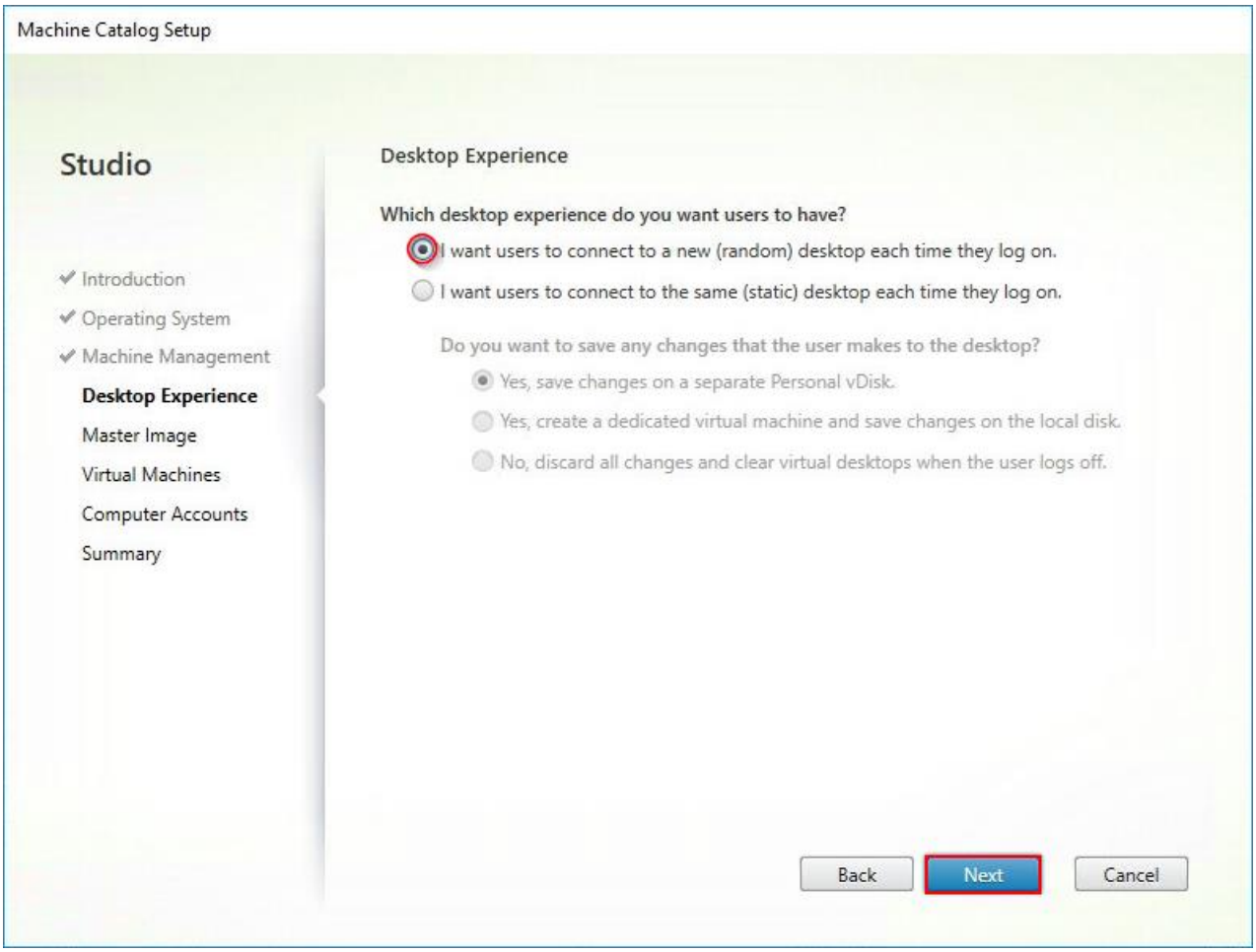

Machine Catalog Setup
Studio
Introduction
Operating System
Machine Management
Master Image
Virtual Machines
Computer Accounts
Summary
Introduction
Machine Catalogs are collections of physical or virtual machines that you assign to users. You create Catalogs from Master Images or physical machines in your environment.
Important: The Master Image or physical machine that you use to create a Catalog must have a Virtual Delivery Agent installed. Also, ensure that the operating system is up-to-date and that applications are installed.
Before you begin, make sure that you:
Identify the types of desktops and applications your users need
Choose a Catalog infrastructure (for example, whether to power manage virtual machines)
Have a technology for creating and managing machines (such as Machine Creation Services or Provisioning Services)
Prepare your environment, including the Master Image, computer accounts, and network interface card configuration.
Learn more
Don't show this again
Back
Next
Cancel



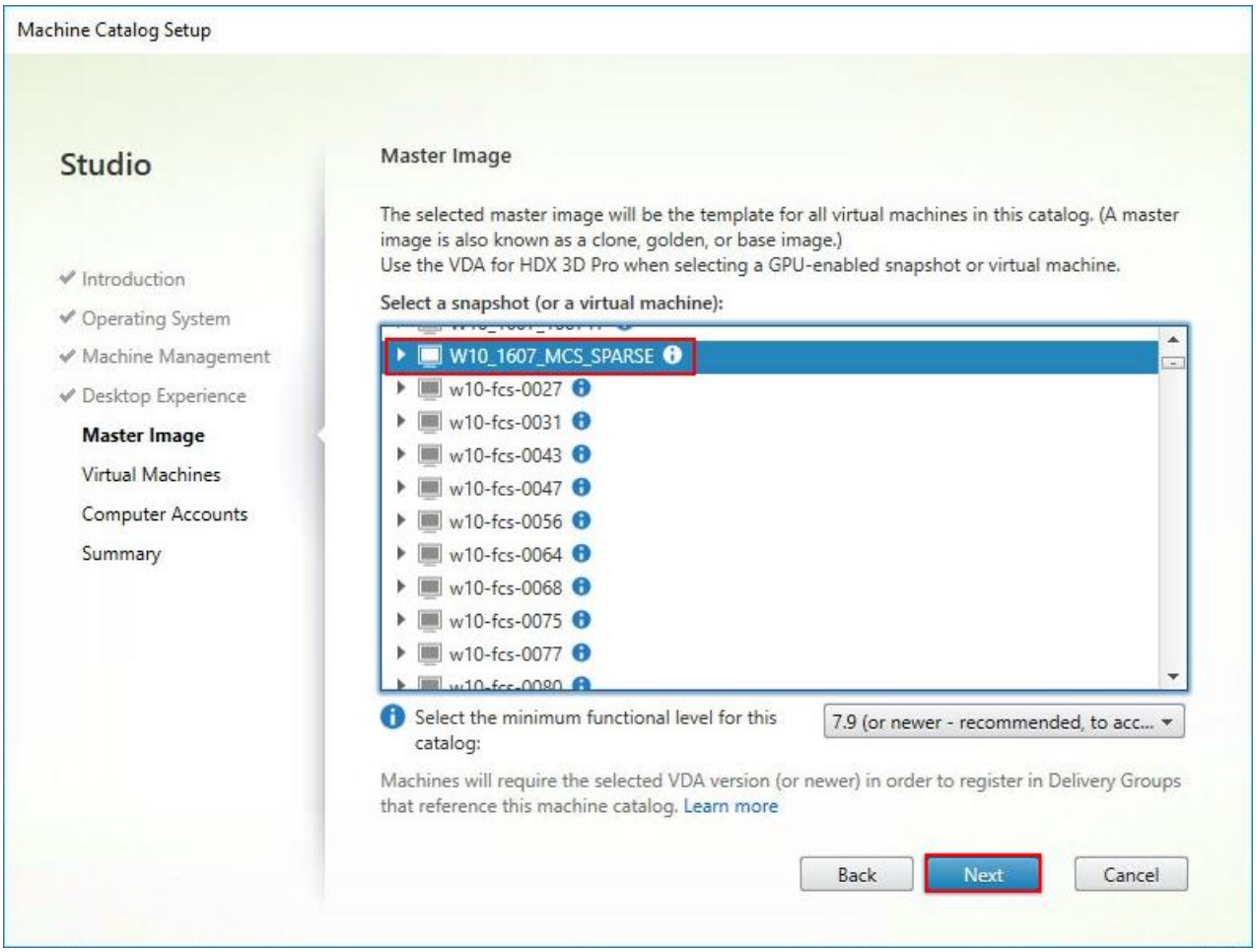
4. Select appropriate machine management and click Next.



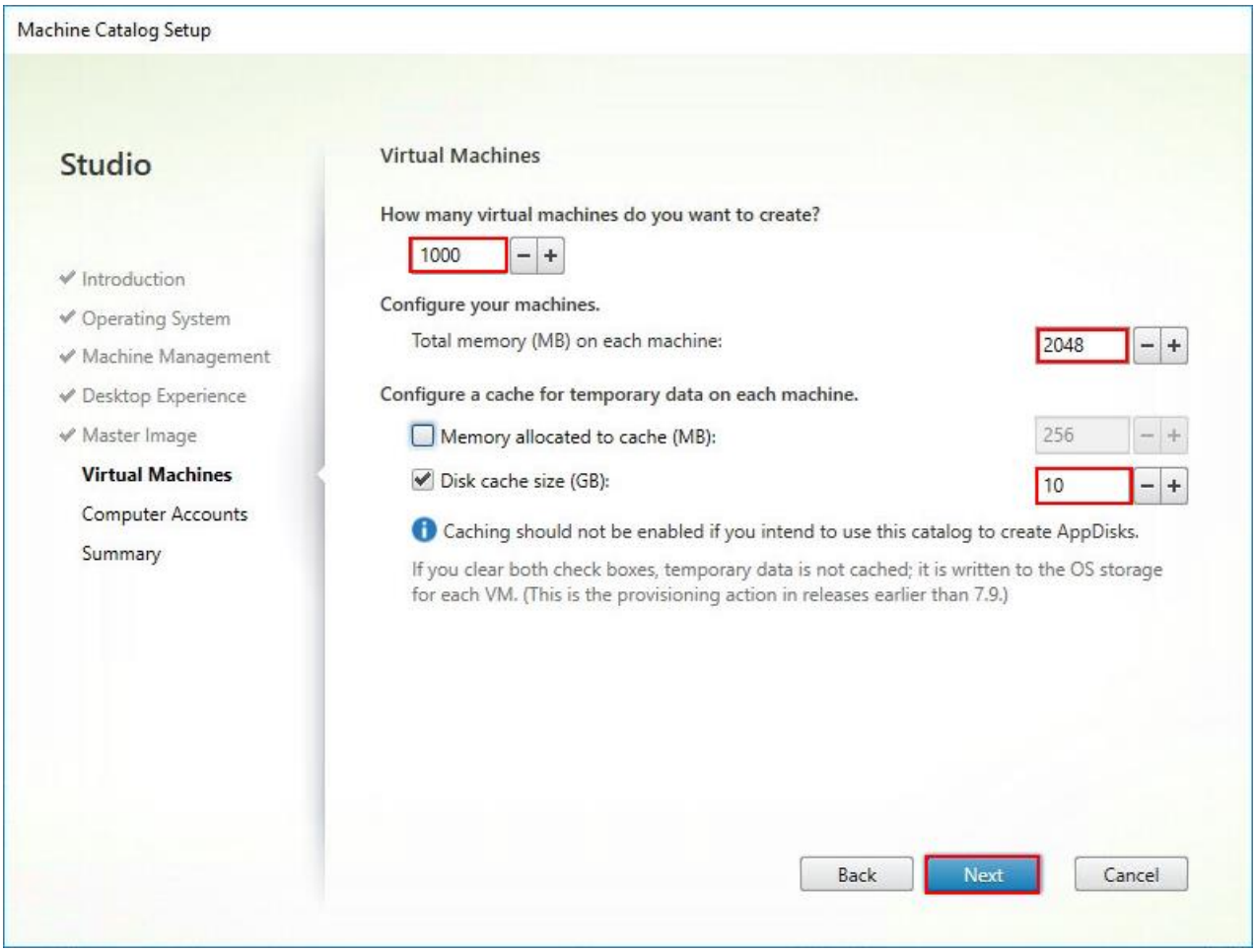
5. Select Random for the Desktop Experience.



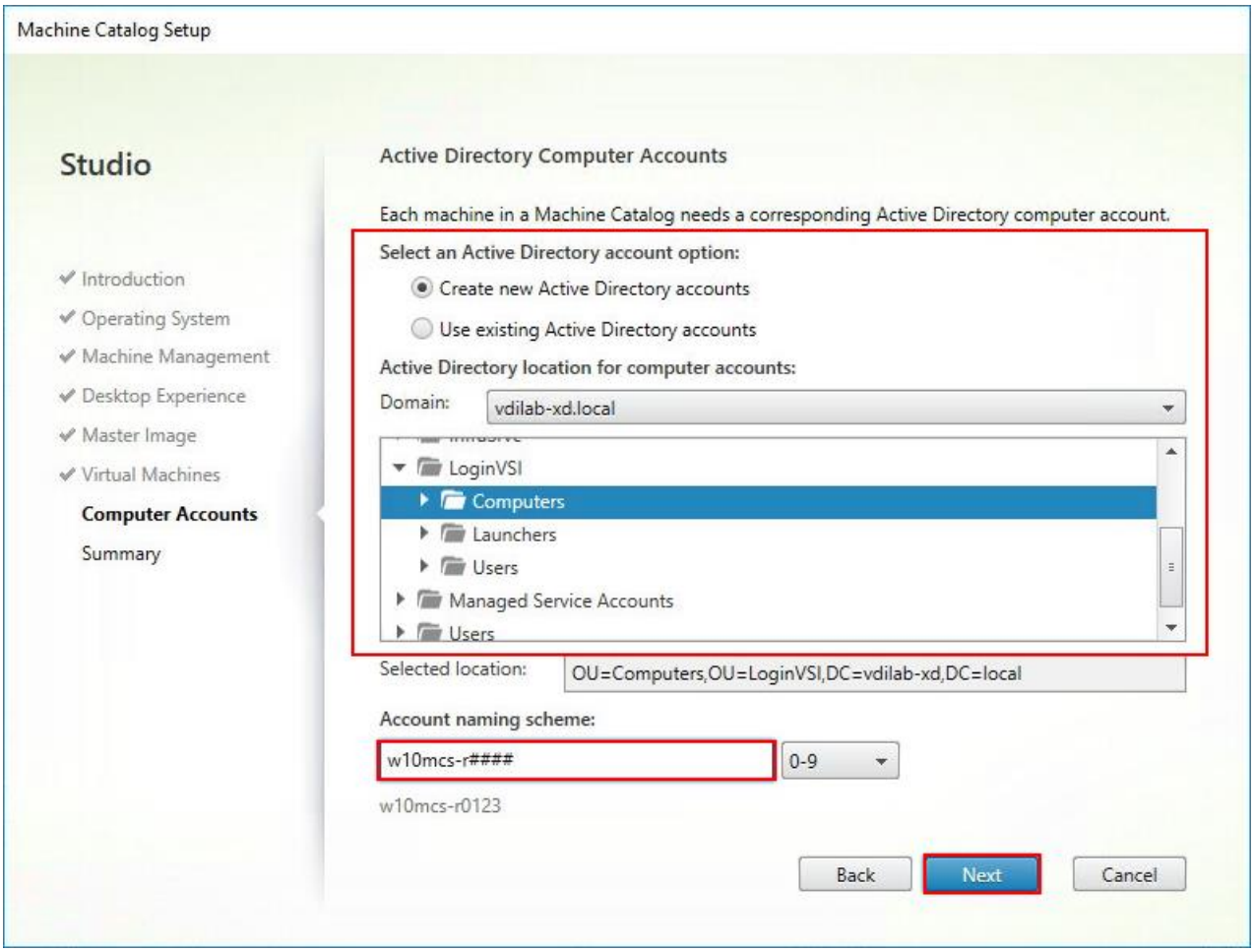
6. Master Image; select a VM and click Next.



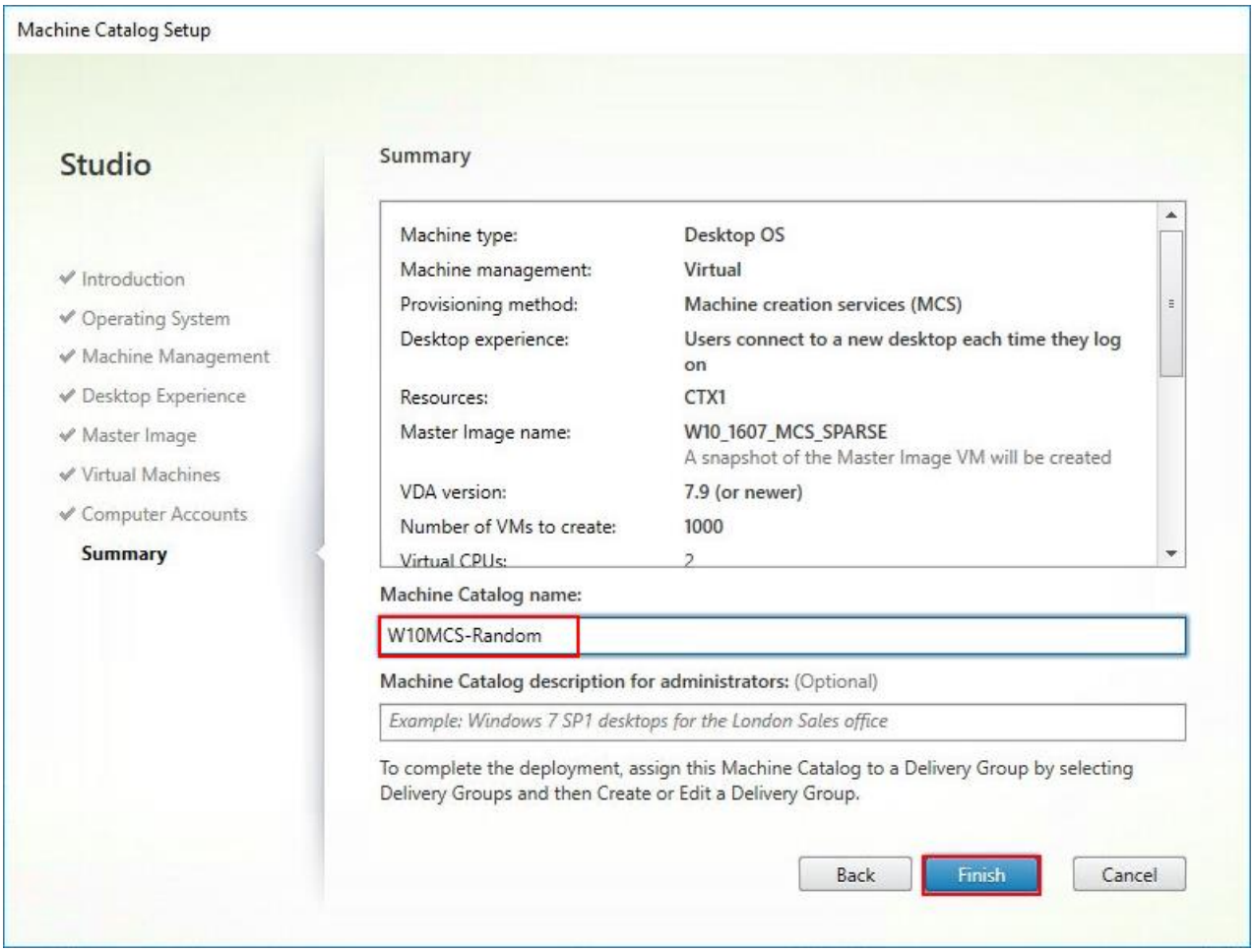
7. Specify the number of the desktops to create and machine configuration. Click Next.



8. Specify AD account naming scheme and OU where accounts will be created.



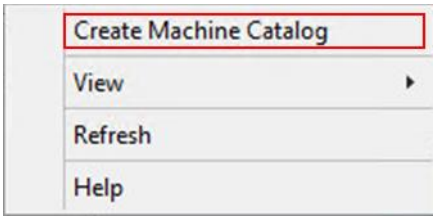
9. On Summary page specify Catalog name and click Finish to start deployment.



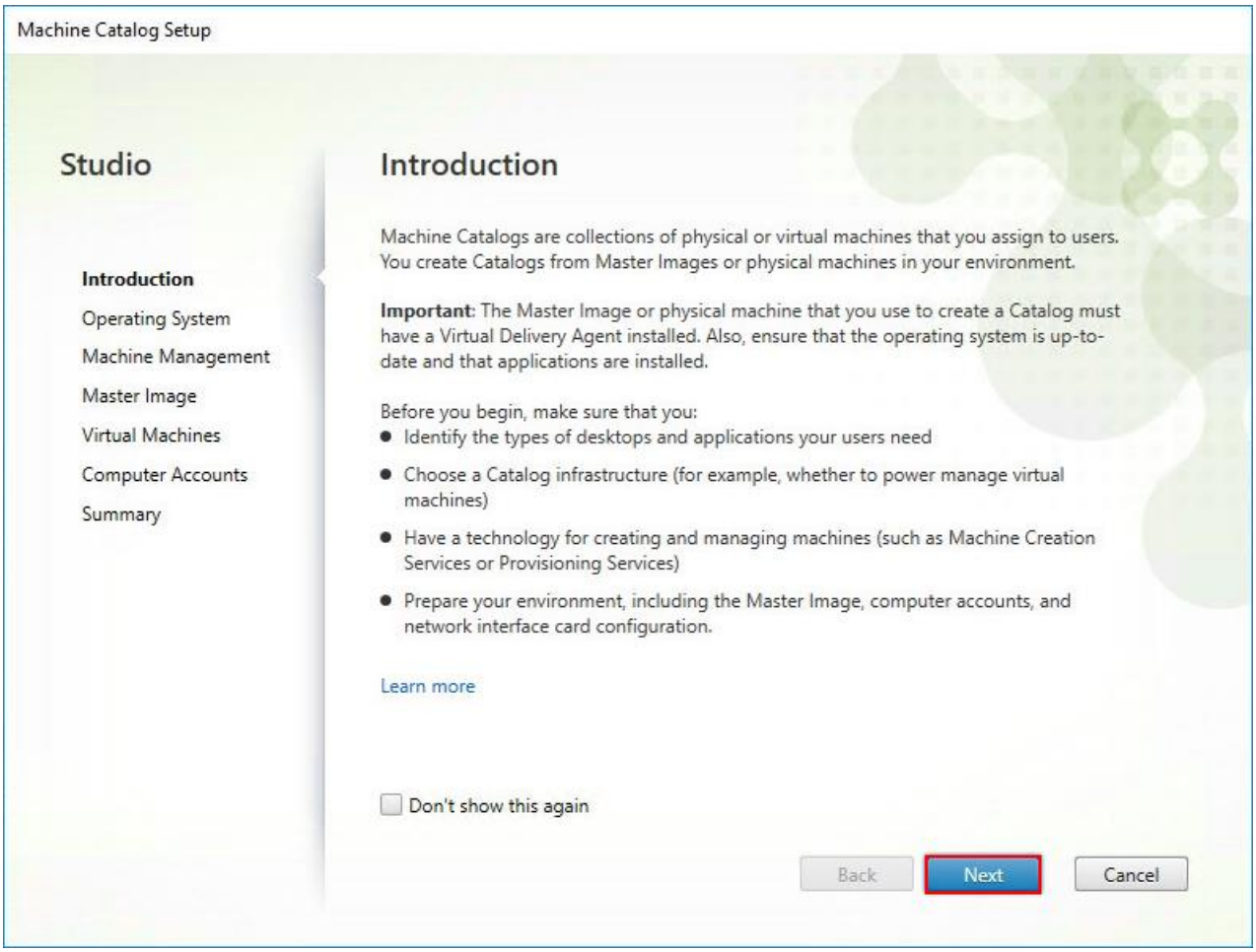
10. Verify the desktop machines were successfully created in the following locations:
    - Provisioning Server > Provisioning Services Console > Farm > Site > Device Collections
    - Delivery Controller > Citrix Studio > Machine Catalogs
    - Domain Controller > Active Directory Users and Computers

Persistent Static Provisioned with MCS

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

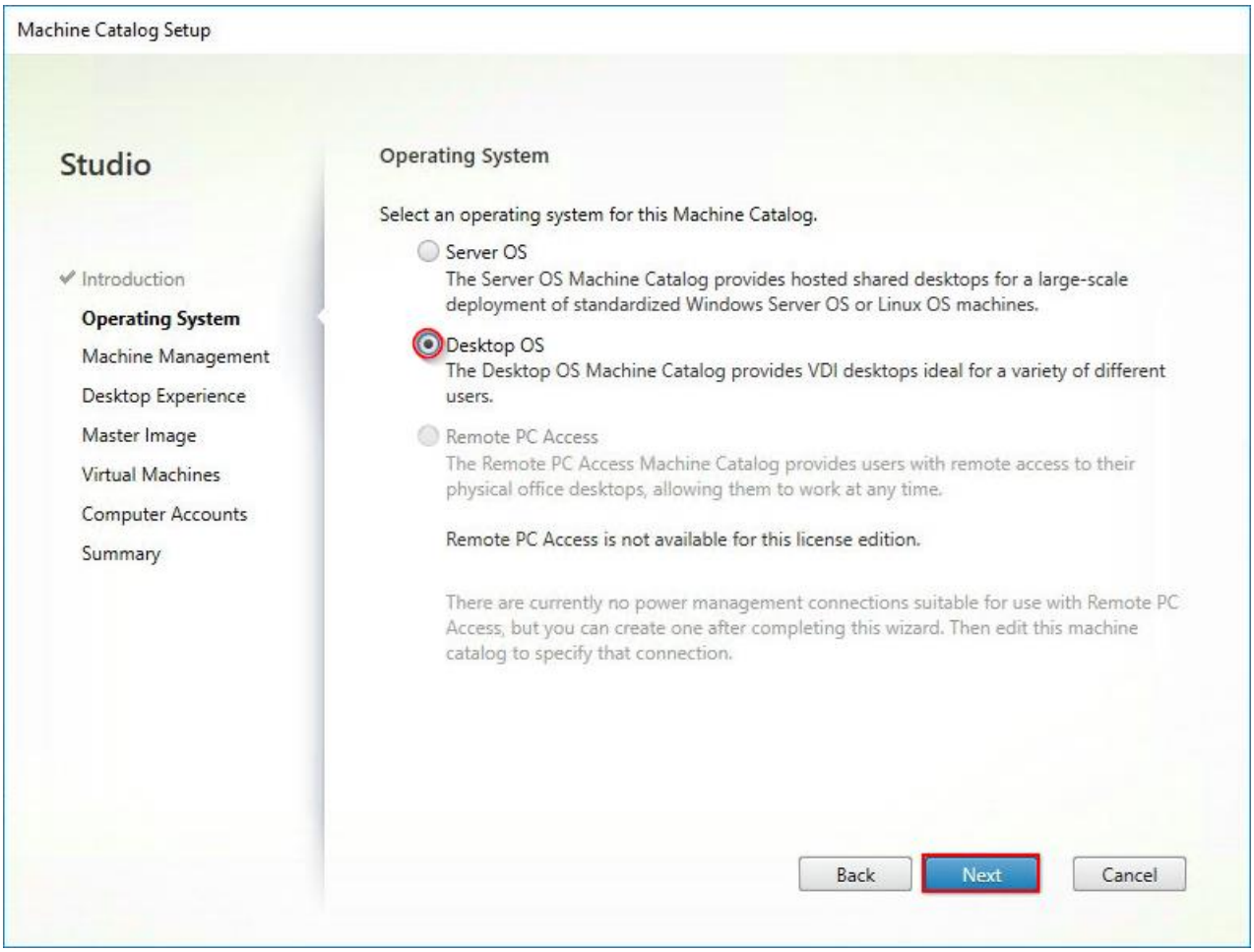


3. Click Next.



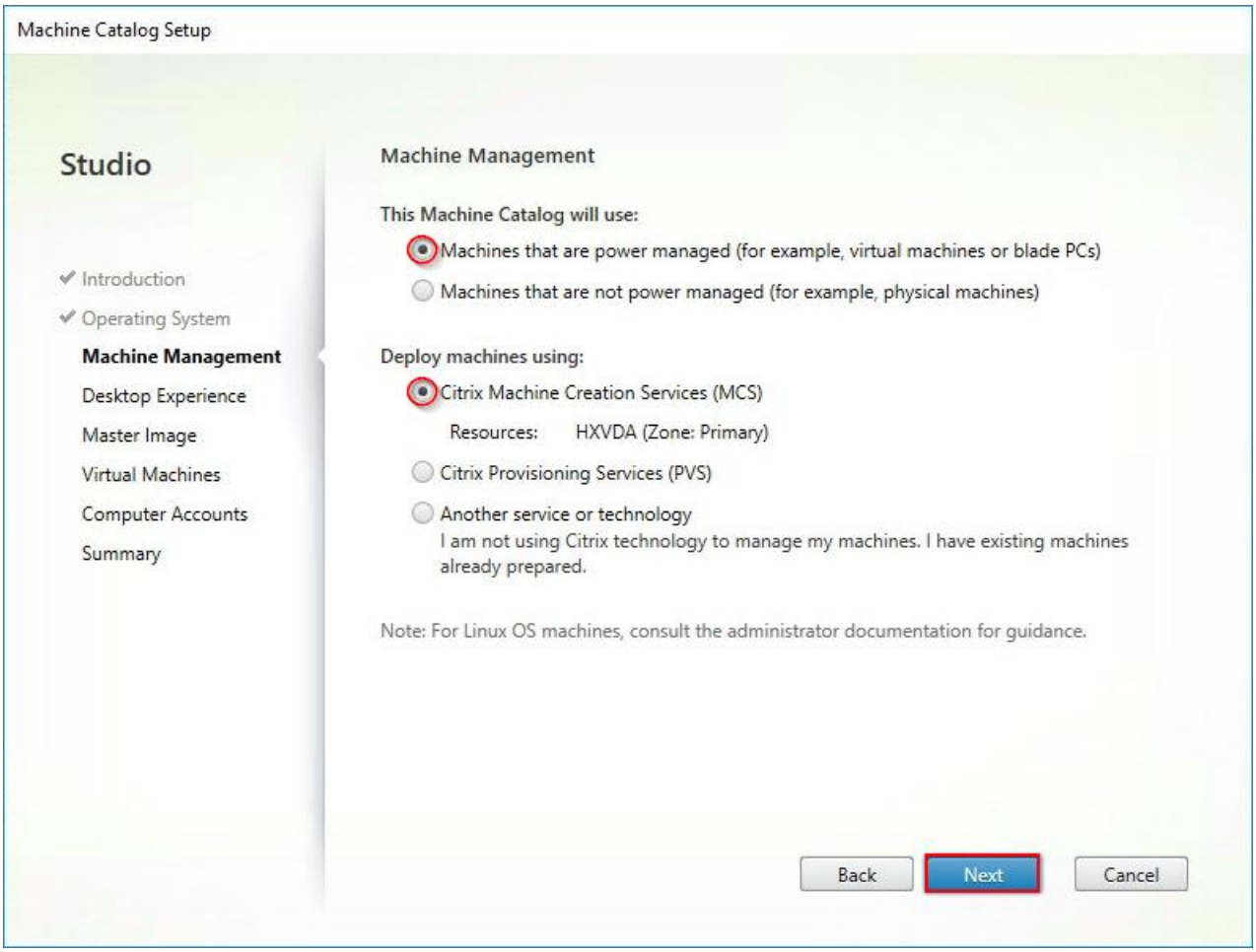
4. Select Desktop OS.

5. Click Next.



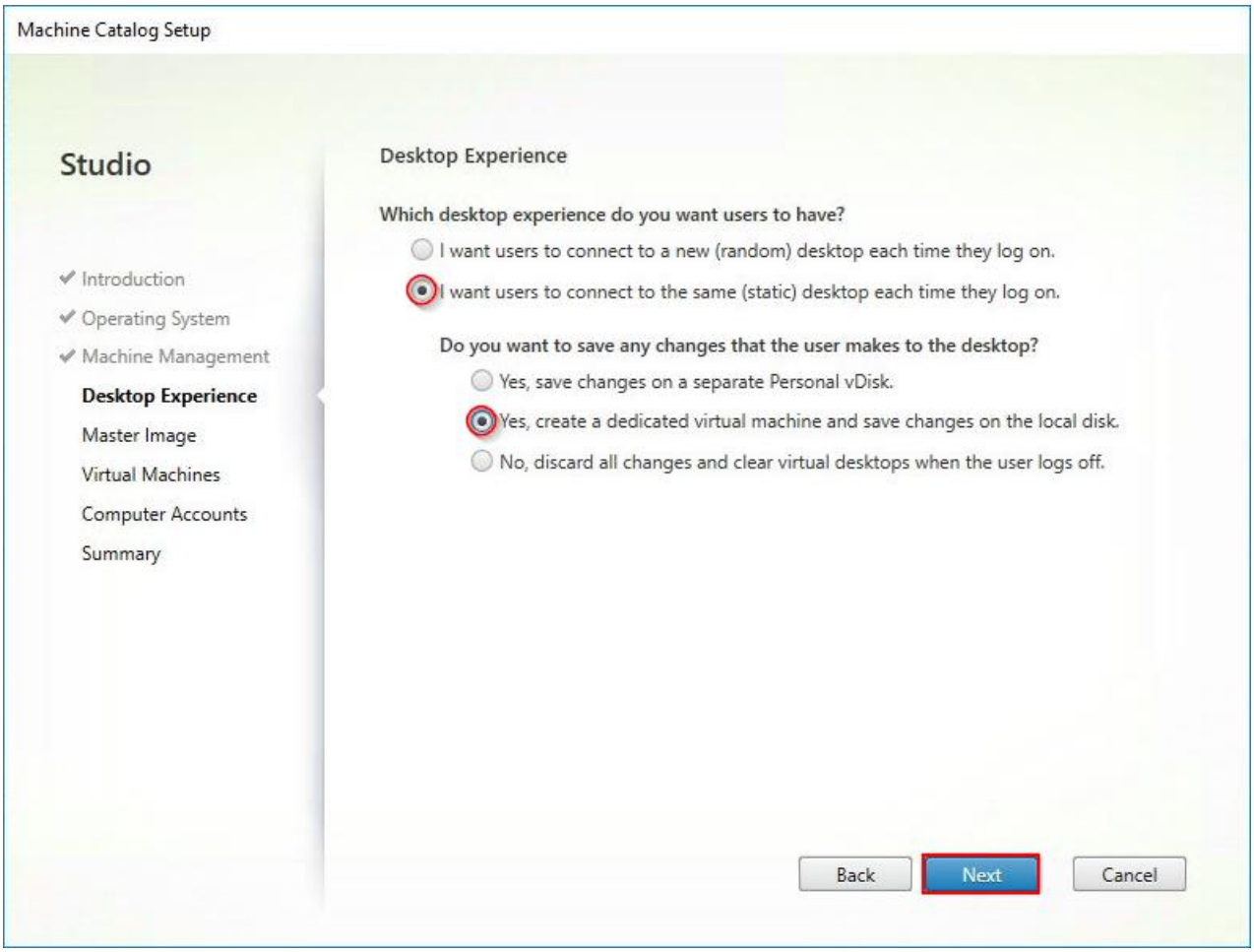
6. Select appropriate machine management.

7. Click Next.



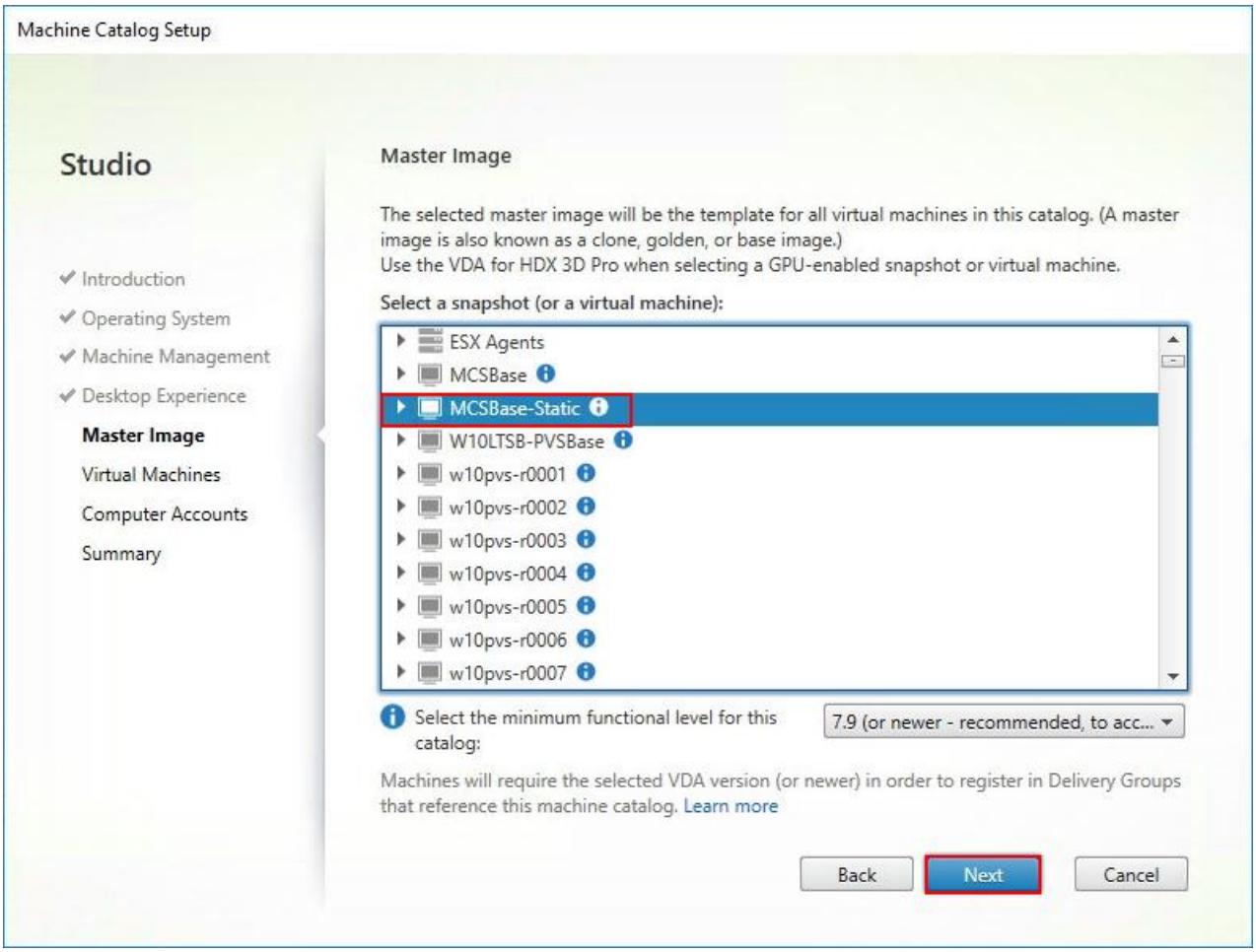
8. Select Static, Dedicated Virtual Machine for Desktop Experience.

9. Click Next.



10. Select a Virtual Machine to be used for Catalog Master image.

11. Click Next.

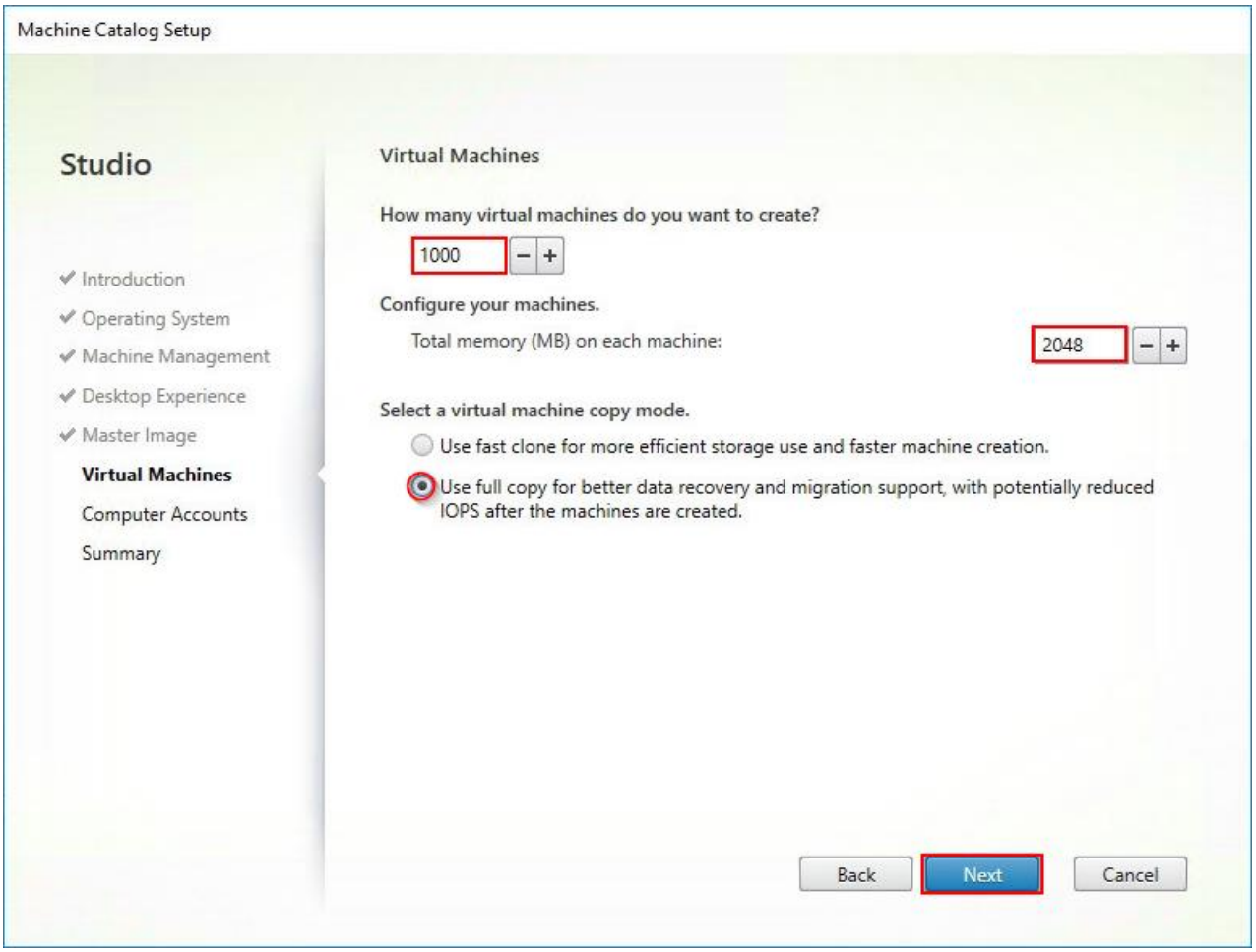


12. Specify the number of the desktops to create and machine configuration.

13. Set amount of memory (MB) to be used by virtual desktops.

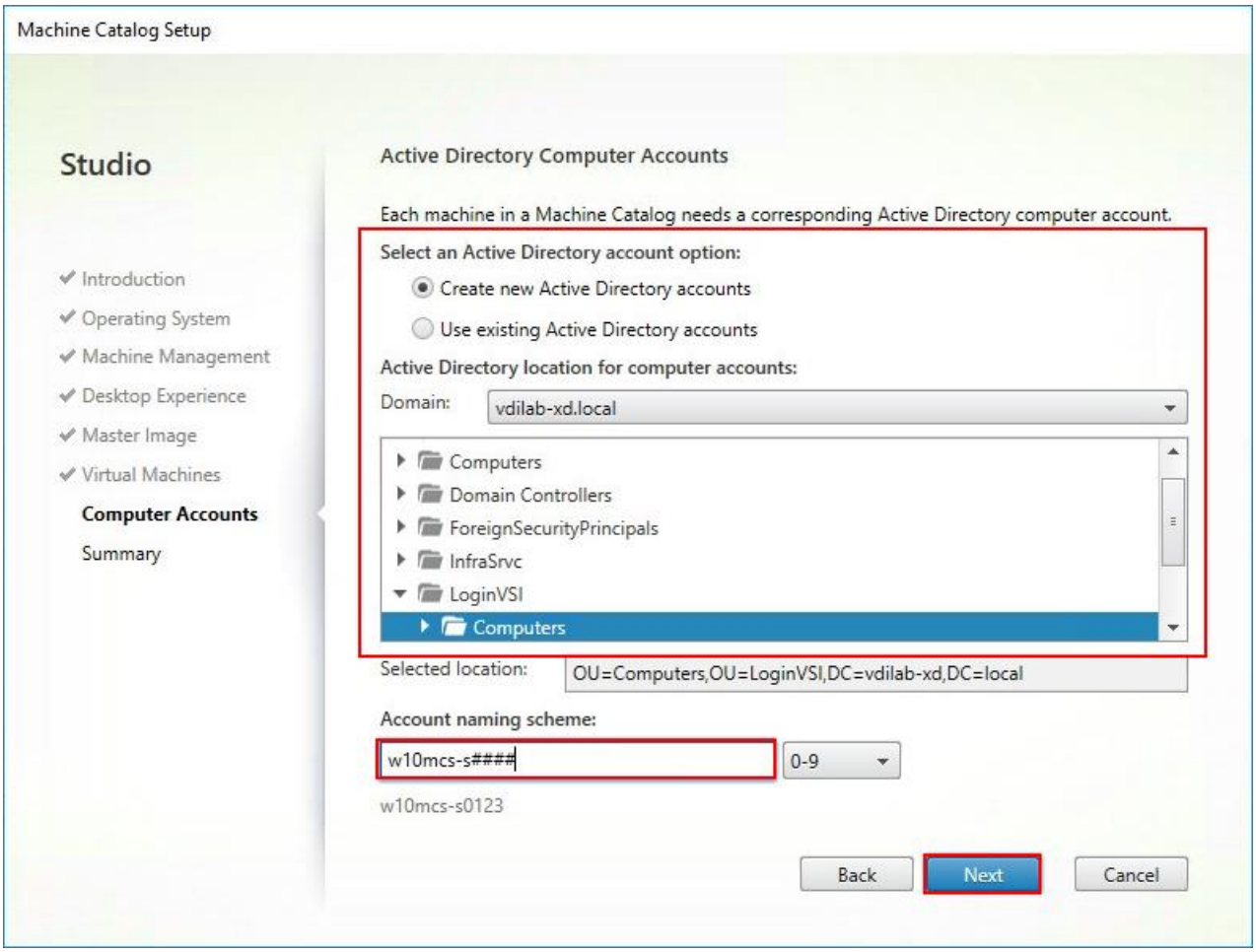
14. Select Full Copy for machine copy mode.

15. Click Next.

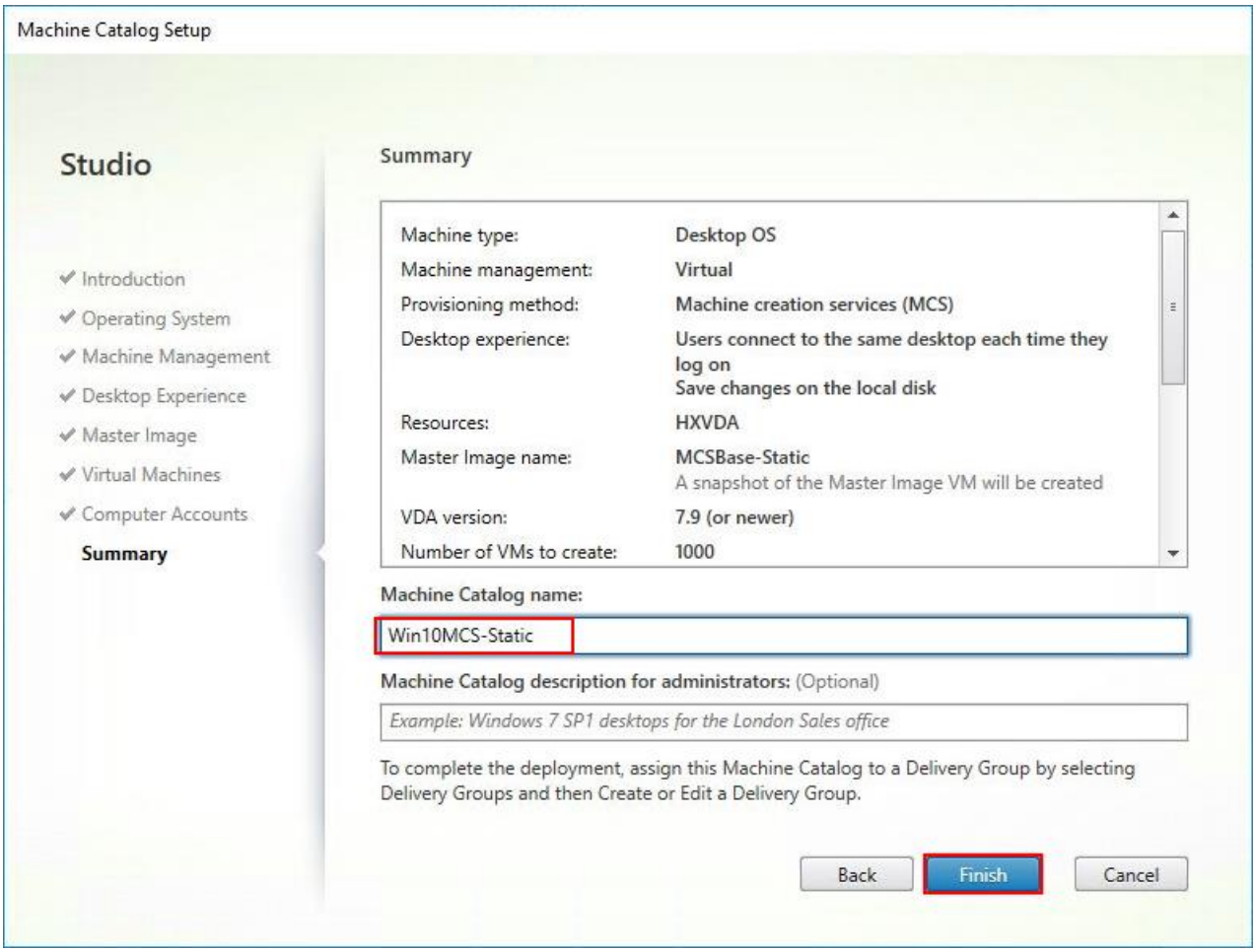


16. Specify AD account naming scheme and OU where accounts will be created.

17. Click Next.



18. On Summary page specify Catalog name and click Finish to start deployment.



19. Verify the desktop machines were successfully created in the following locations:

    - Provisioning Server > Provisioning Services Console > Farm > Site > Device Collections
    - Delivery Controller > Citrix Studio > Machine Catalogs
    - Domain Controller > Active Directory Users and Computers

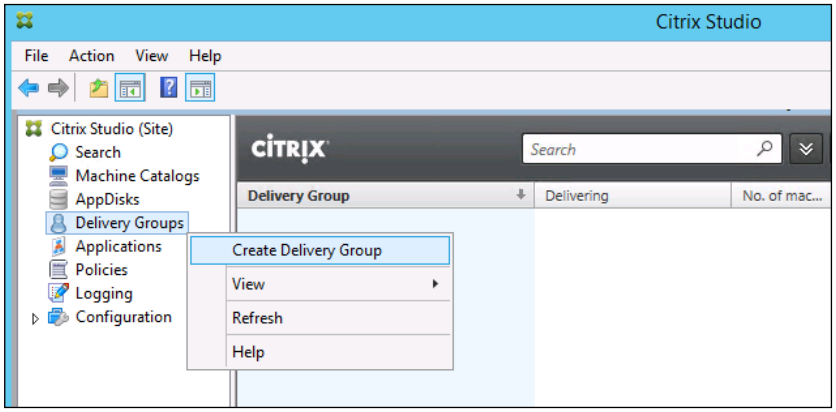
Create Delivery Groups

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

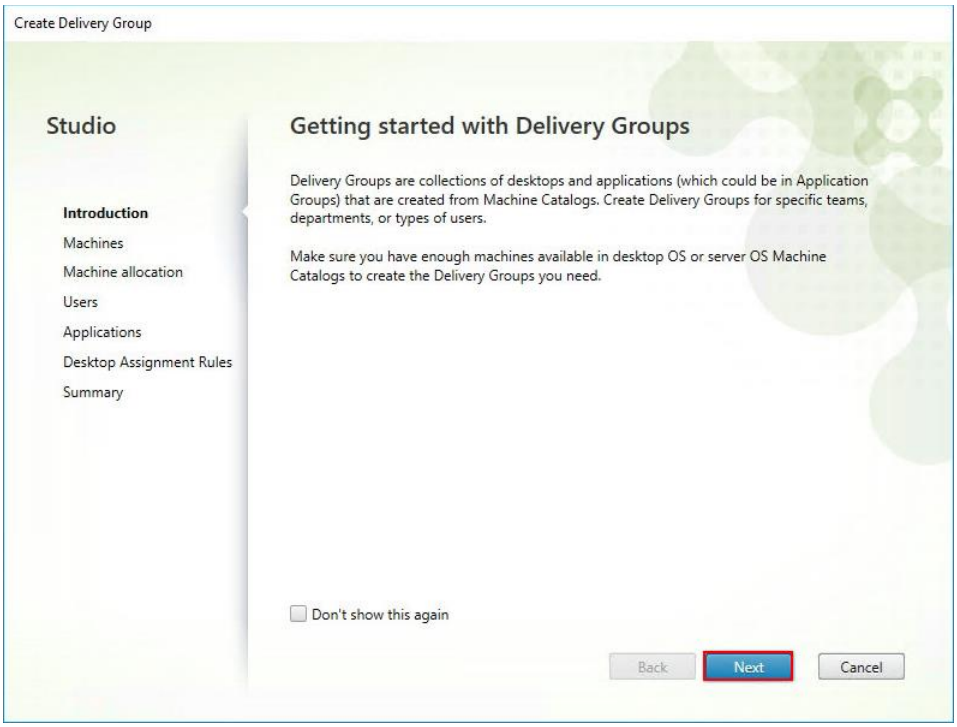
To create delivery groups, complete the following steps:

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

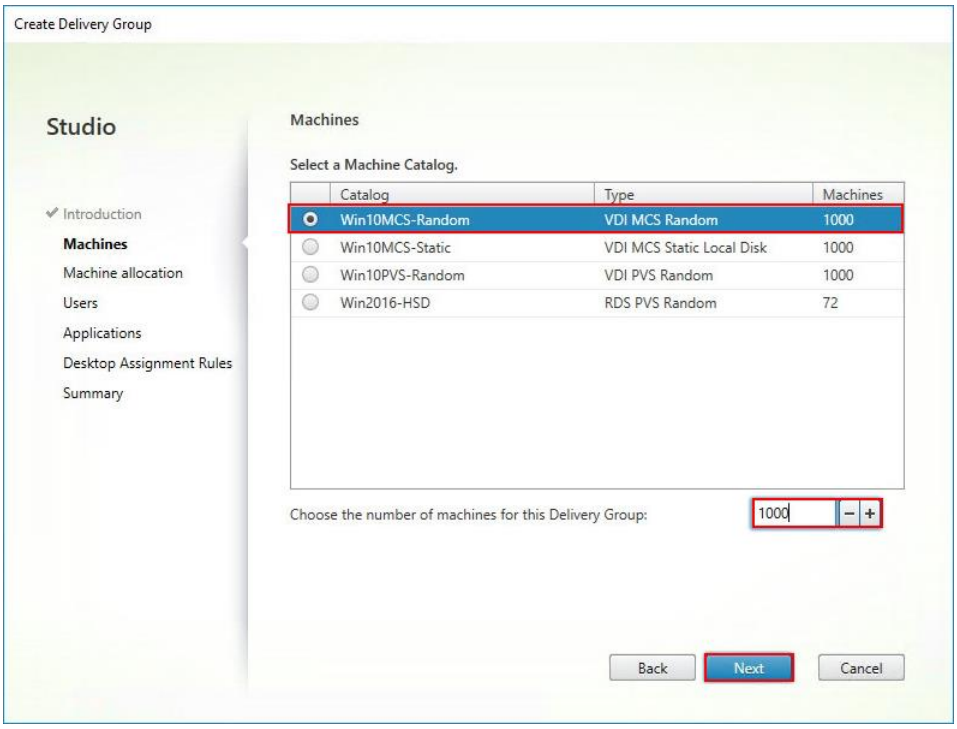
1. Connect to a XenDesktop server and launch Citrix Studio.
2. Choose Create Delivery Group from the drop-down list.



3. Click Next.

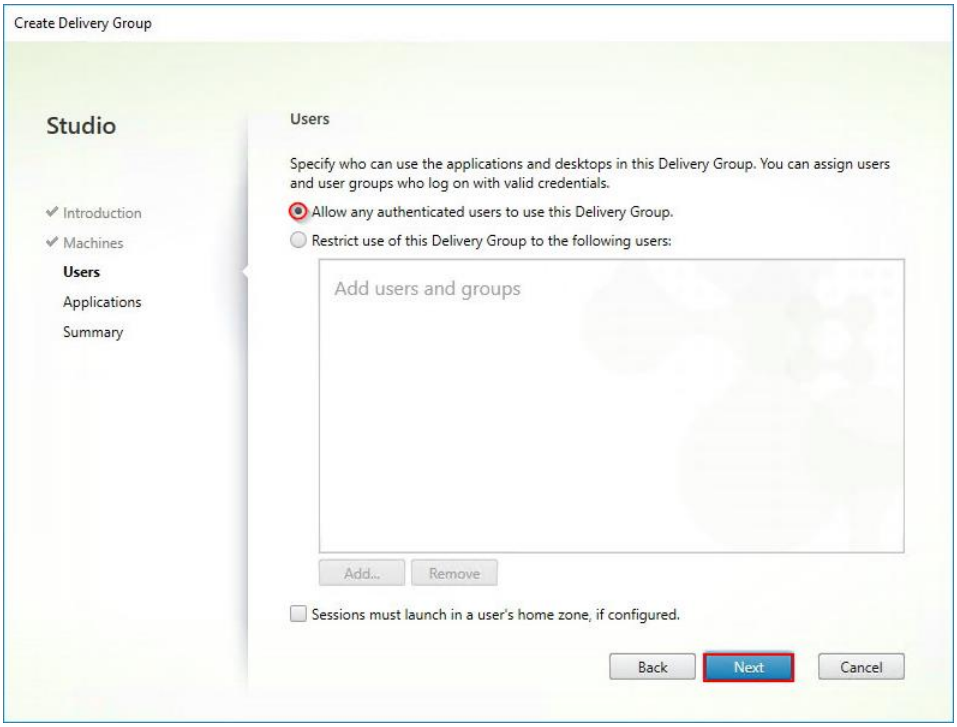


4. Select Machine catalog.
5. Provide the number of machines to be added to the delivery Group.
6. Click Next.



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

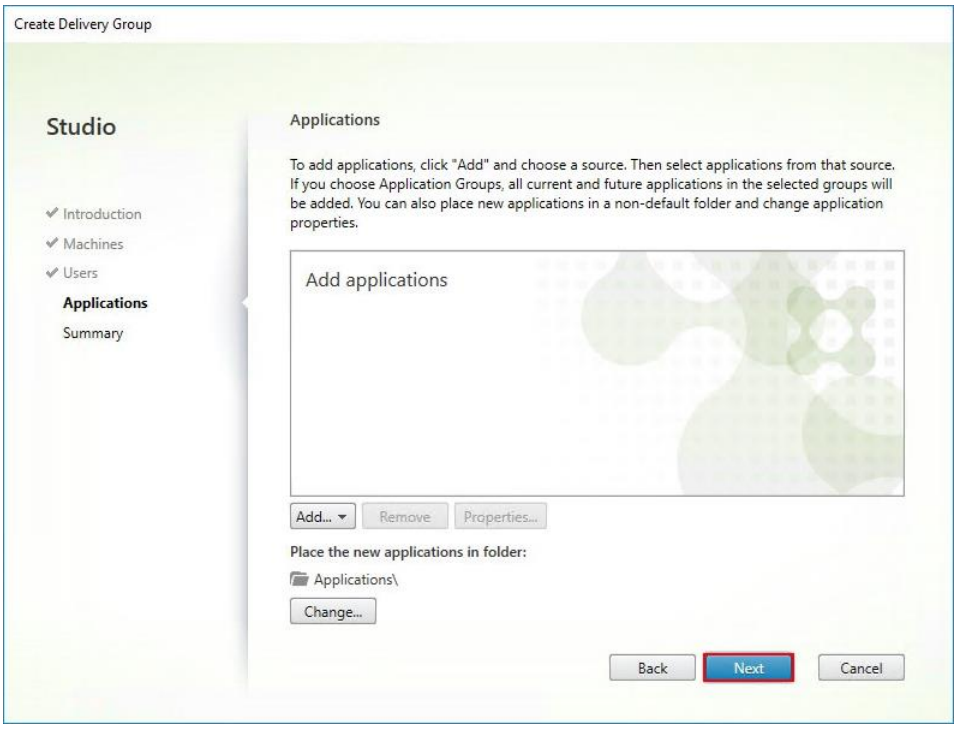
8. Click Next.



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

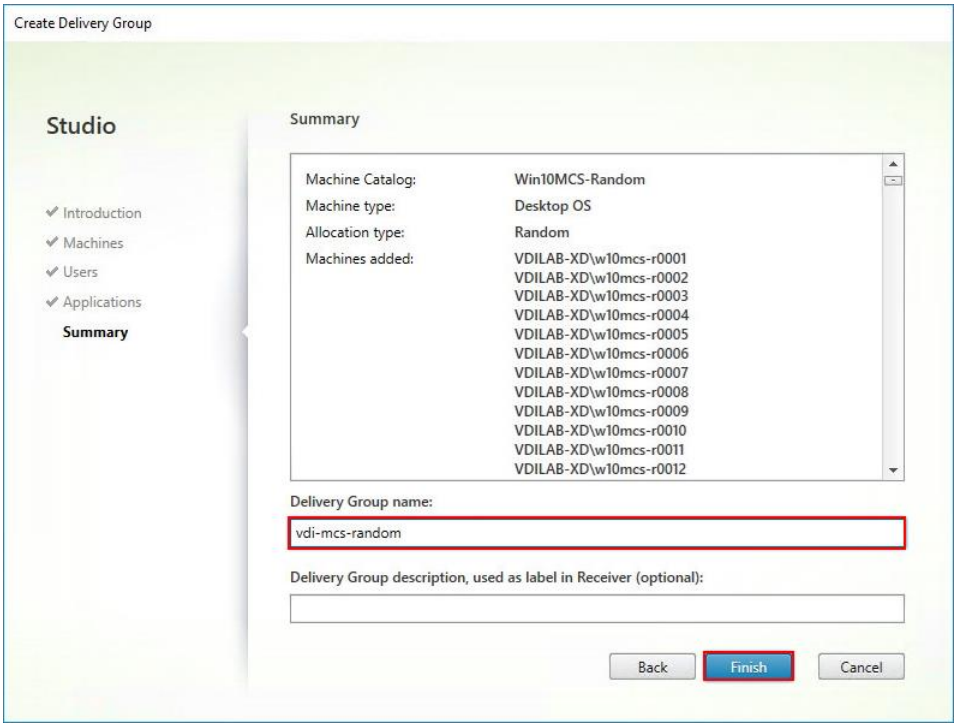
9. (Optional) specify Applications catalog will deliver.

10. Click Next.

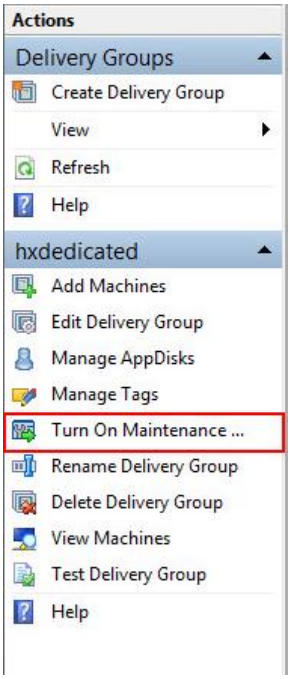


11. On the Summary dialog, review the configuration. Enter a Delivery Group name and a Display name (for example, HVD or HSD).

12. Click Finish.



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



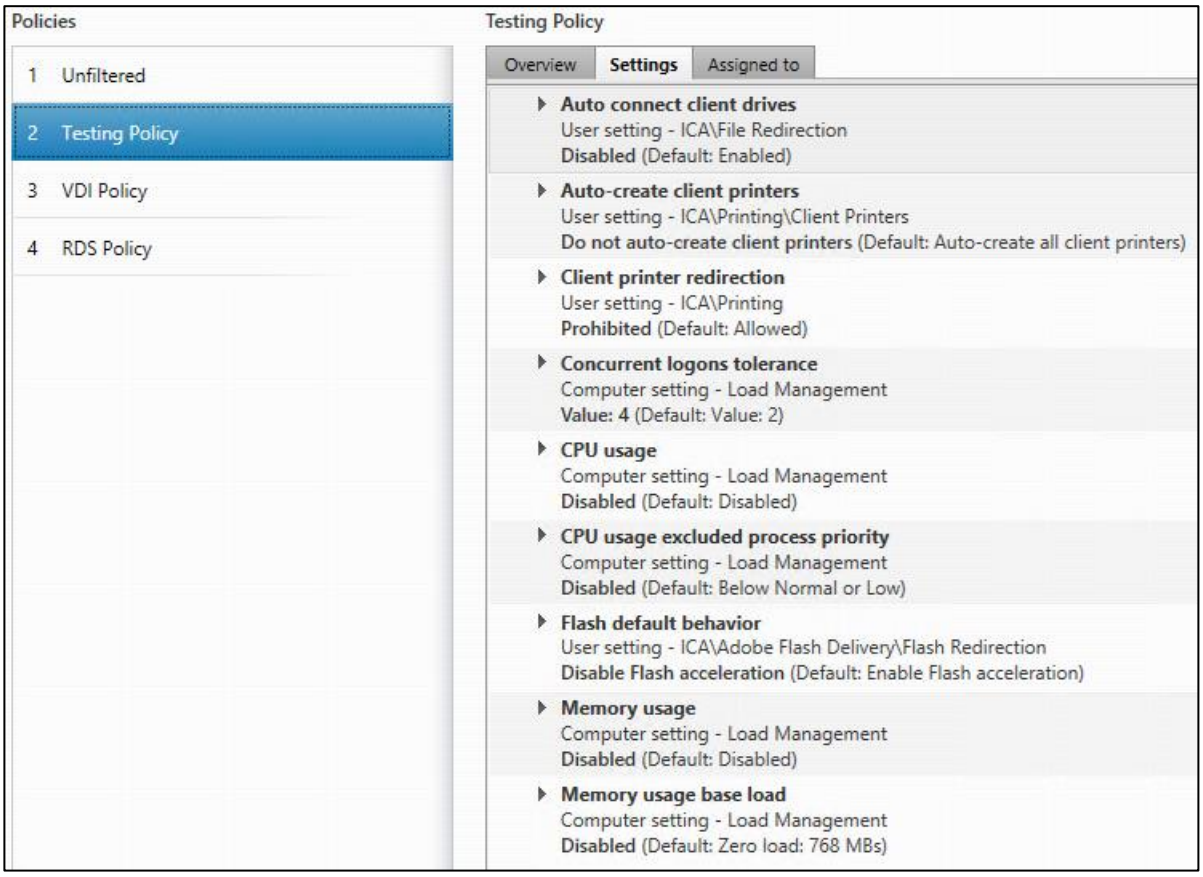
Citrix XenDesktop Policies and Profile Management

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

Configure Citrix XenDesktop Policies

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

Figure 48 **XenDesktop Policy**



Configuring User Profile Management

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

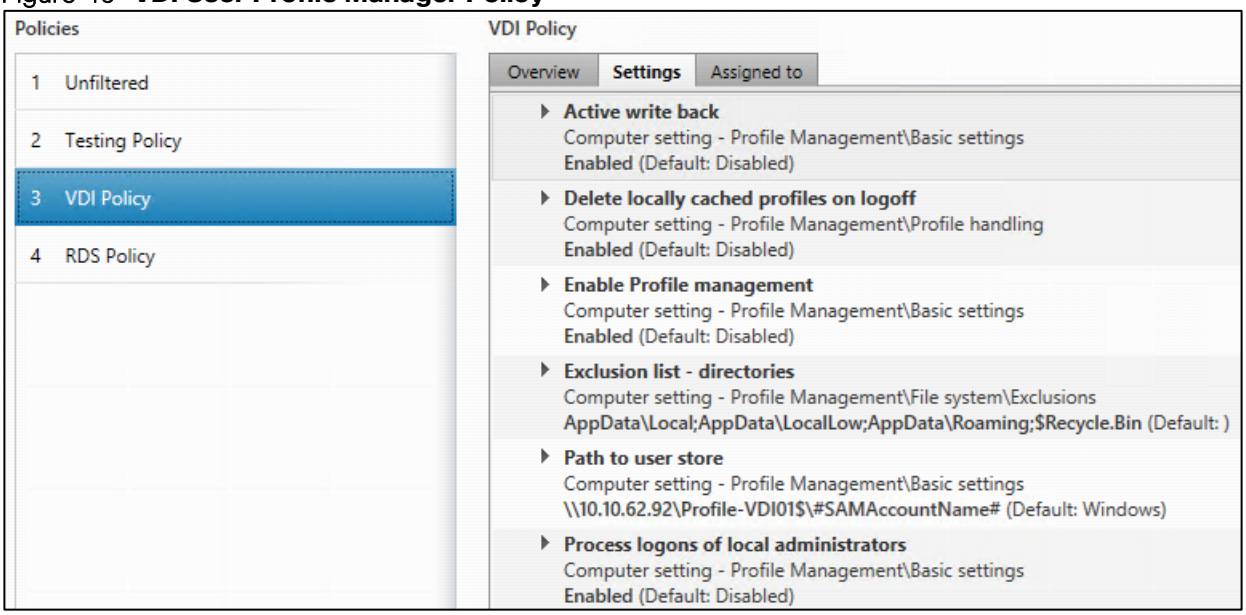
- Desktop settings such as wallpaper and screen saver
- Shortcuts and Start menu setting
- Internet Explorer Favorites and Home Page
- Microsoft Outlook signature
- Printers

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

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

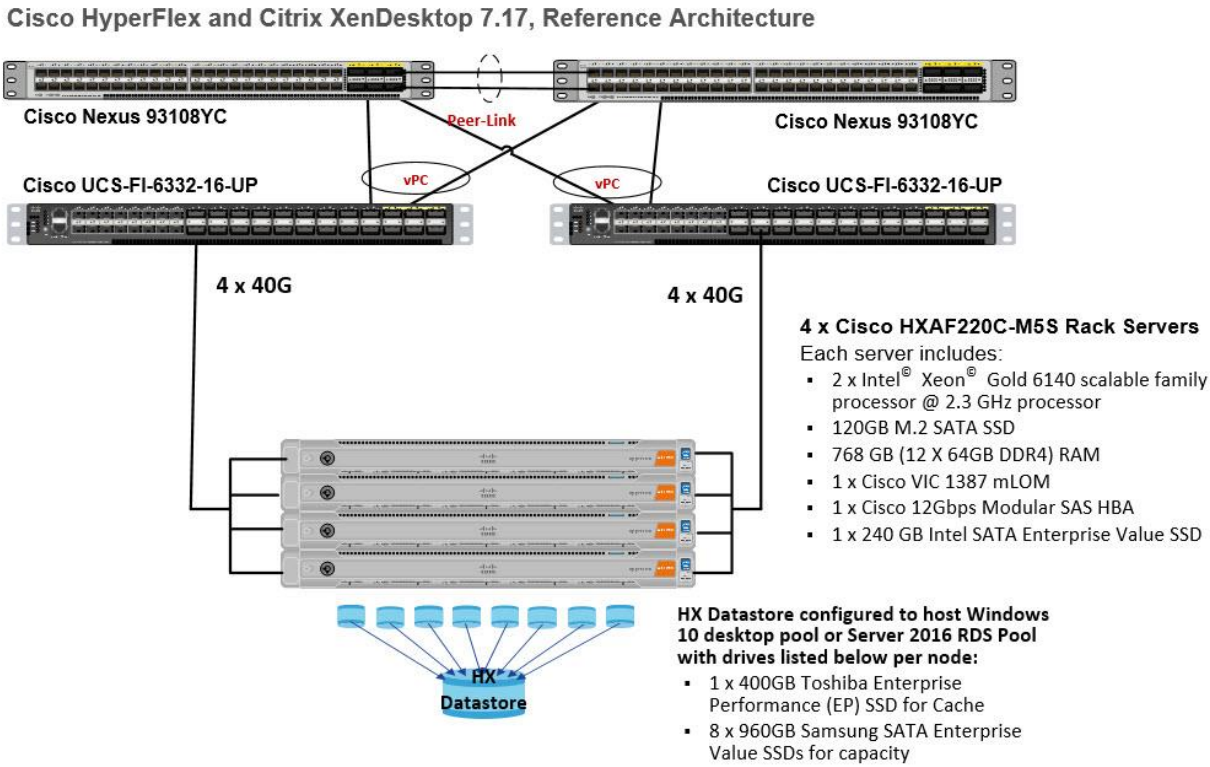
http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11.html

Figure 49 **VDI User Profile Manager Policy**



Test Setup and Configurations

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



Hardware Components:

- 2 x Cisco UCS 6332-16UP Fabric Interconnects
- 2 x Cisco Nexus 93108YCPX Access Switches
- 4 x Cisco UCS HXAF220c-M5SX Rack Servers (2 Intel Xeon Gold 6140 scalable family processor at 2.3 GHz, with 768 GB of memory per server [32 GB x 24 DIMMs at 2666 MHz])
- Cisco VIC 1387 mLOM
- 12G modular SAS HBA Controller
- 240GB M.2 SATA SSD drive (Boot and HyperFlex Data Platform controller VM)
- 240GB 2.5” 6G SATA SSD drive (Housekeeping)
- 400GB 2.5” 6G SAS SSD drive (Cache)
- 8 x 960GB 2.5” SATA SSD drive (Capacity)
- 1 x 32GB mSD card (Upgrades temporary cache)

Software Components:

- Cisco UCS firmware 3.2(2d)
- Cisco HyperFlex Data Platform 2.6.1b
- VMware vSphere 6.5 U1
- Citrix XenDesktop 7.16
- Citrix Provisioning Server 7.16
- Citrix User Profile Management
- Citrix NetScaler VPX NS11.1 52.13.nc
- Microsoft SQL Server 2016
- Microsoft Windows 10
- Microsoft Windows 2016
- Microsoft Office 2016
- Login VSI 4.1.25.6

Testing Methodology and Success Criteria

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

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

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

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

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

Testing Procedure

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

Pre-Test Setup for Testing

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

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

Test Run Protocol

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

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

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

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

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

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

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

15. Time 3:45 Ready for new test sequence.

Success Criteria

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

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

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

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

Cisco requires three consecutive runs with results within +/-1% 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 Citrix XenDesktop 7.16 Hosted Shared Desktop with Citrix XenDesktop 7.16 Composer provisioning using Microsoft Windows Server 2016 sessions on Cisco UCS HXAF220c-M4S, Cisco UCS 220 M4 and Cisco UCS B200 M4 servers.

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

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

VSImax 4.1.x Description

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

Login VSI is different in approach. Login VSI is not primarily designed to be a steady state benchmark (however, if needed, Login VSI can act like one). Login VSI was designed to perform benchmarks for SBC or VDI workloads through system saturation. Login VSI loads the system with simulated user workloads using well known desktop applications like Microsoft Office, Internet Explorer and Adobe PDF reader. By gradually increasing the amount of simulated users, the system will eventually be saturated. Once the system is saturated, the response time of the applications will increase significantly. This latency in application response times show a clear indication whether the system is (close to being) overloaded. As a result, by nearly overloading a system it is possible to find out what 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 50 **Sample of a VSI Max Response Time Graph, Representing a Normal Test**

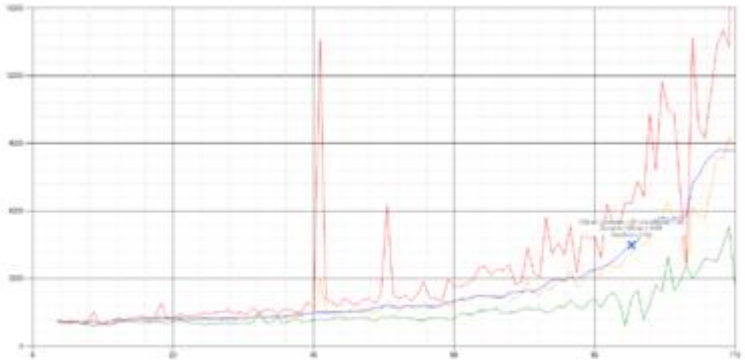
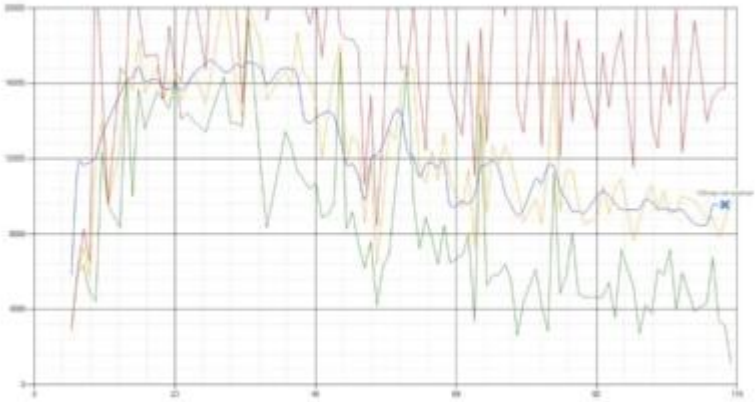


Figure 51 **Sample of a VSI Test Response Time Graph with a Clear Performance Issue**



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 450 desktops and measure the time it takes for the 450th virtual machine to register as available in the XenDesktop Administrator console.

The Cisco HyperFlex HXAF220c-M5SX based All-Flash cluster running Data Platform version 2.6(1b) software can accomplish this task in **5 minutes** as shown in the following charts:

Figure 52 **450 XenDesktop PVS Windows 10 Sessions with Office 2016 Virtual Desktops Boot and Register as Available in Less Than 5 Minutes**

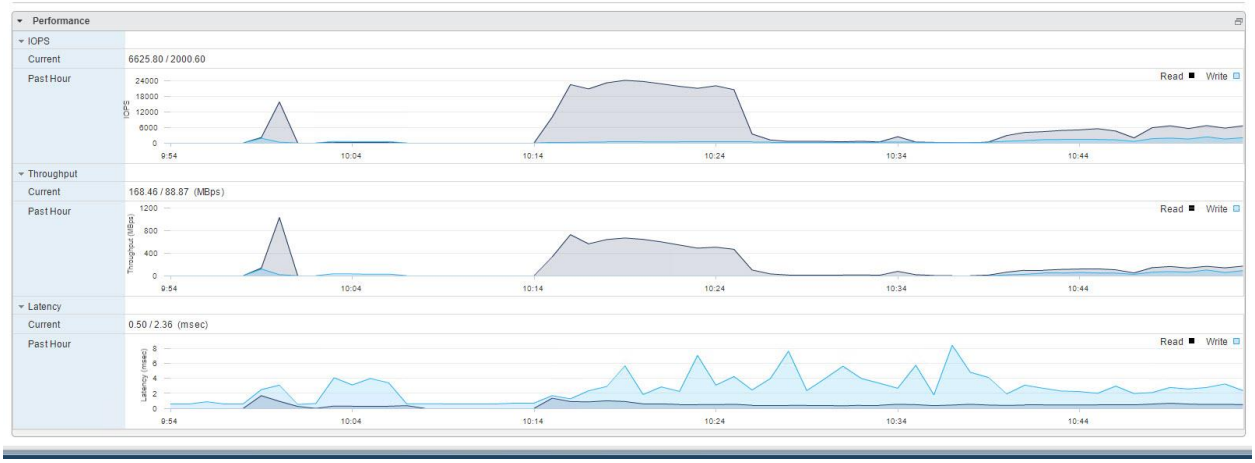
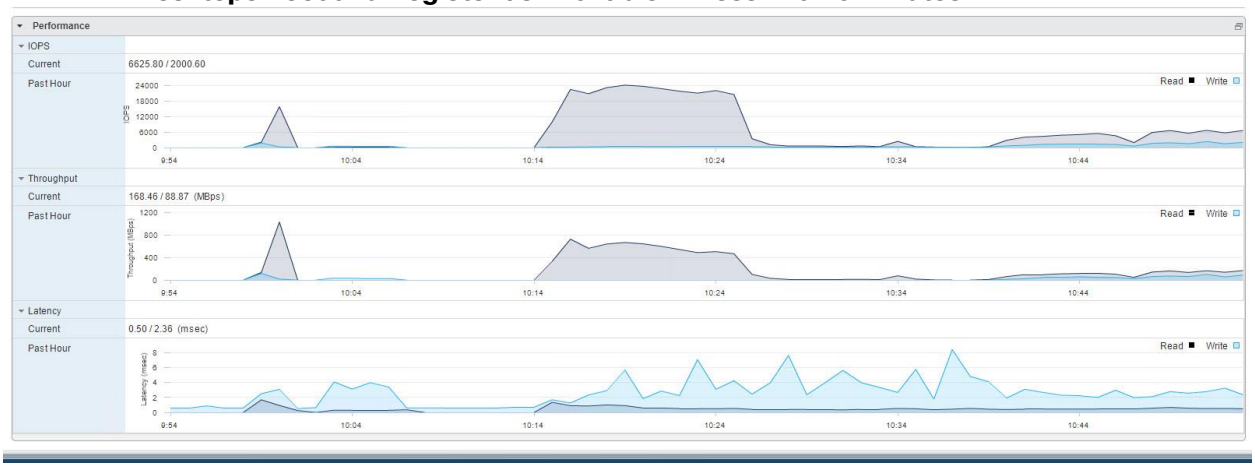


Figure 53 **450 XenDesktop MCS Persistent (Full Clone) Windows 10 Sessions with Office 2016 Virtual Desktops Boot and Register as Available in Less Than 5 Minutes**



Recommended Maximum Workload and Configuration Guidelines

Four Node Cisco HXAF220c-M5S Rack Server, HyperFlex All-Flash Cluster

For Citrix XenApp RDS Hosted Shared Desktop and Hosted Virtual Desktop use case, the recommended maximum workload was determined based on both Login VSI Knowledge Worker workload end user experience measures and HXAF220c-M5SX server operating parameters.

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

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

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
Boot	Start all RDS and/or VDI virtual machines at the same time.
Login	The Login VSI phase of test is where sessions are launched and start executing the workload over a 48 minutes duration.

Test Phase	Description
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 Cisco HyperFlex cluster configured on Cisco HXAF2240c-M5SX with Intel Xeon Gold 6140 scalable family processors and 768GB of RAM for Windows Server 2016 Hosted Sessions is 600 sessions with Office 2016 virtual desktops respectively.

XenApp Server Pool Testing on Four Node Cisco HyperFlex Cluster

This section shows the key performance metrics that were captured on the Cisco UCS HyperFlex storage cluster configured with four HXAF220c-M5SX converged node running XENAPP VMs. The full-scale testing with 600 user session on 32 Windows Server 2016 XENAPP VMs on four HXAF220c-M5SX HyperFlex cluster.

Test result highlights include:

- 0.610 second baseline response time
- 0.832 second average response time with 450 desktop sessions running
- Average CPU utilization of 70 percent during steady state
- Average of 250 GB of RAM used out of 768 GB available
- 3000Mbps peak network utilization per host.
- Average Read Latency 0.5ms/Max Read Latency 1.8ms
- Average Write Latency 4.5ms/Max Write Latency 8.7ms
- 2800 peak I/O operations per second (IOPS) per cluster at steady state
- 125MBps peak throughput per cluster at steady state

Figure 54 **LoginVSI Analyzer Chart for 600 Users on XenApp Server Desktop Test**

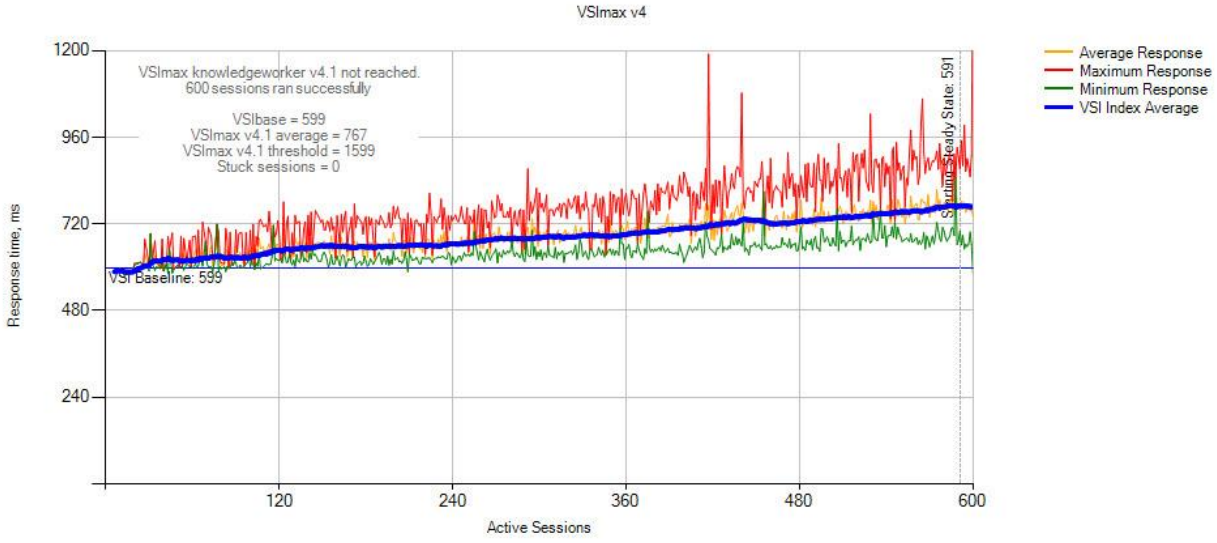


Figure 55 **LoginVSI Analyzer Chart for Three Consecutive Test Running 600 Knowledge Worker Workload on Four Node HyperFlex Cluster**

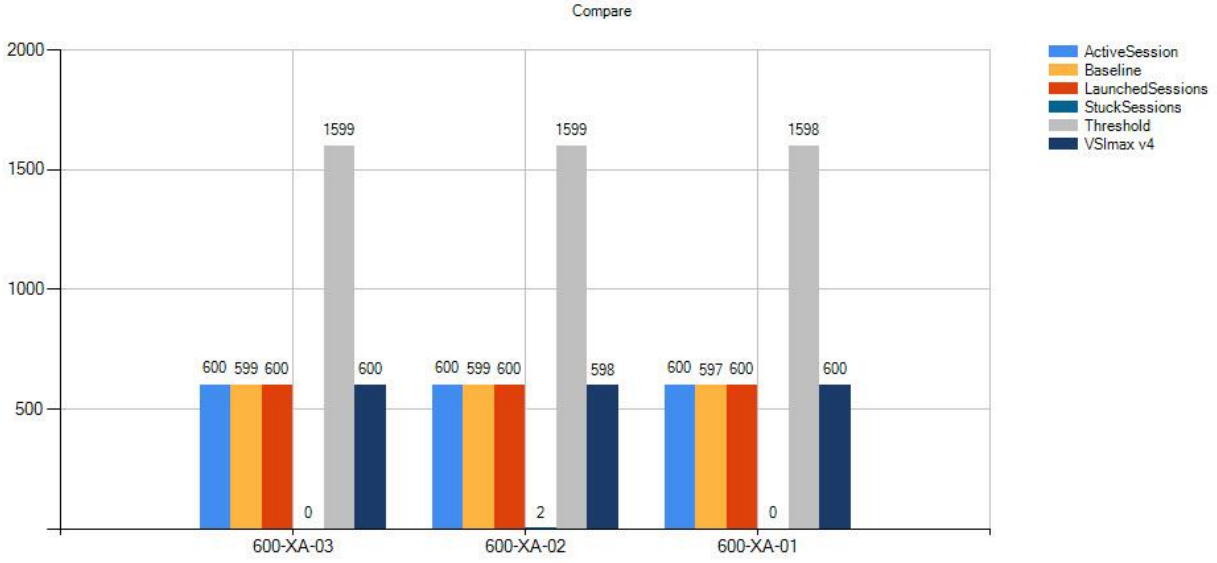


Figure 56 **Sample ESXi Host CPU Core Utilization Running 600 User Test with 32 XenApp Server VMs on Four Nodes**

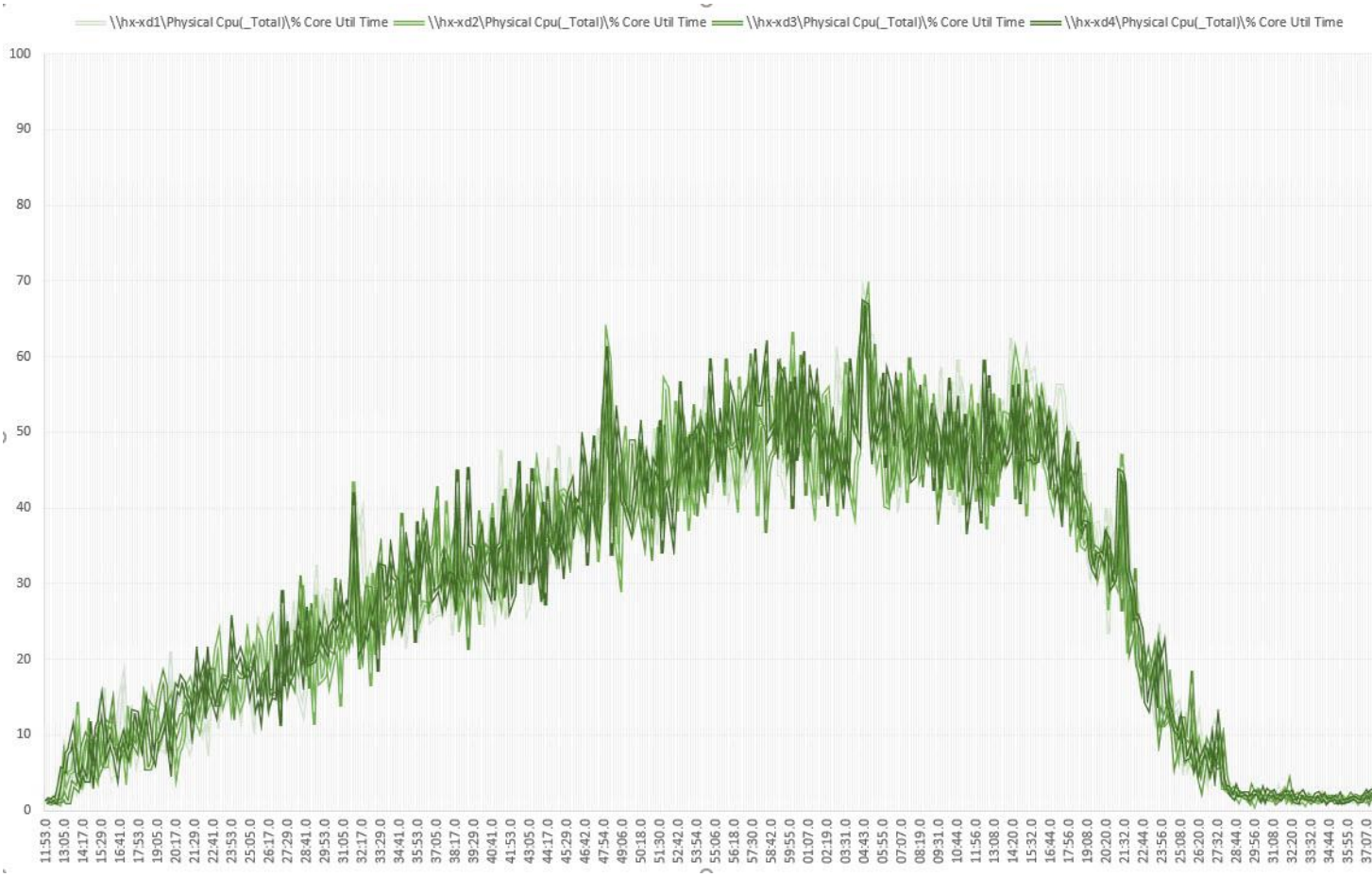


Figure 57 **Sample ESXi Host Network Adapter (VMNICs) Mbits Received/ Transmitted Per Sec Running 600 User Test with 32 XenApp Server VMs on Four Nodes**

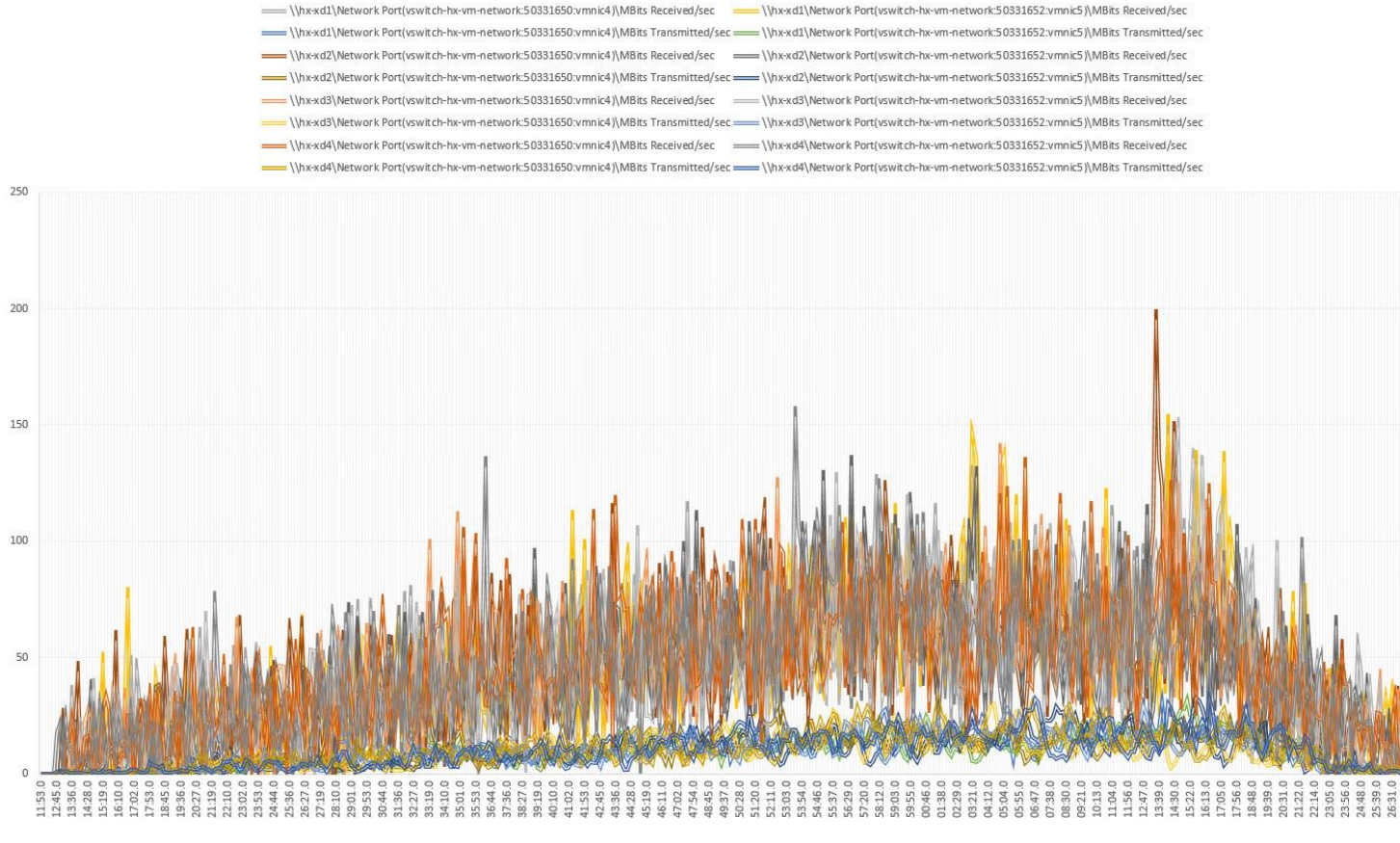


Figure 58 **HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 600 User Test with 32 XenApp Server VMs on Four Nodes**

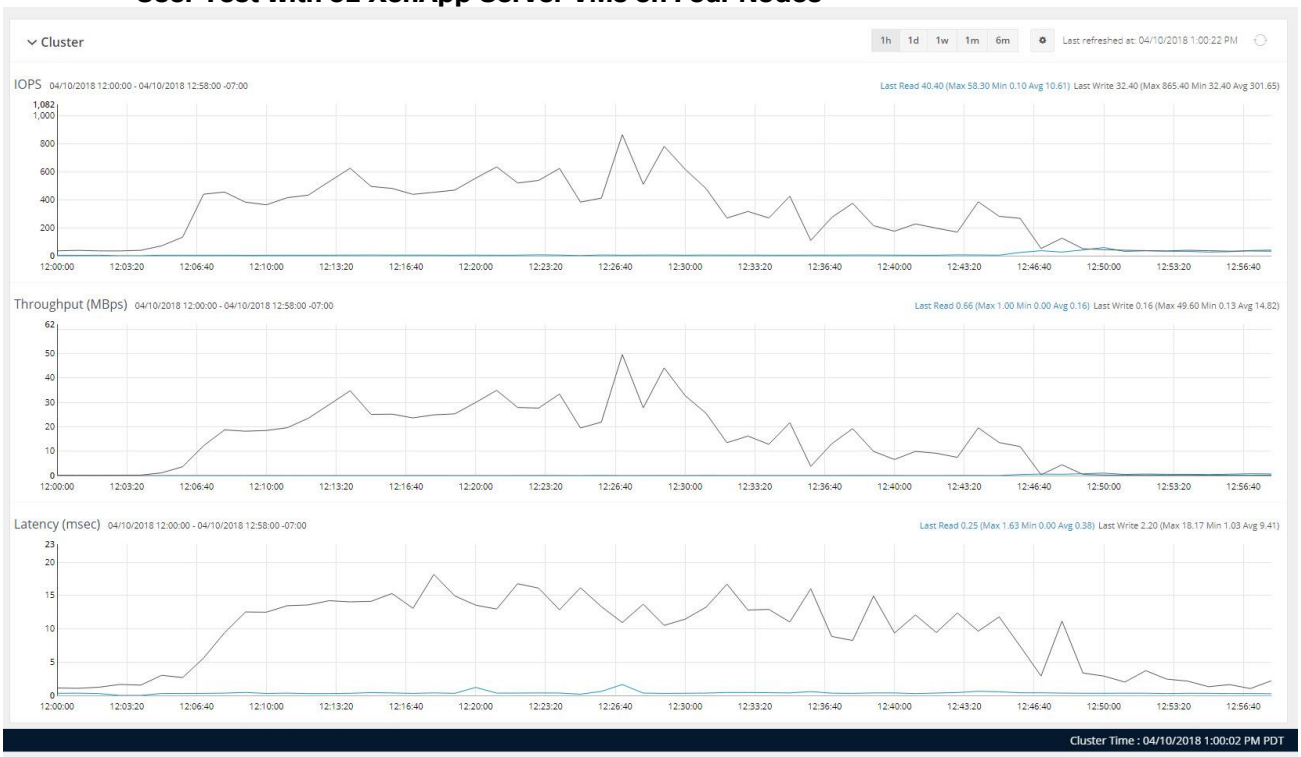
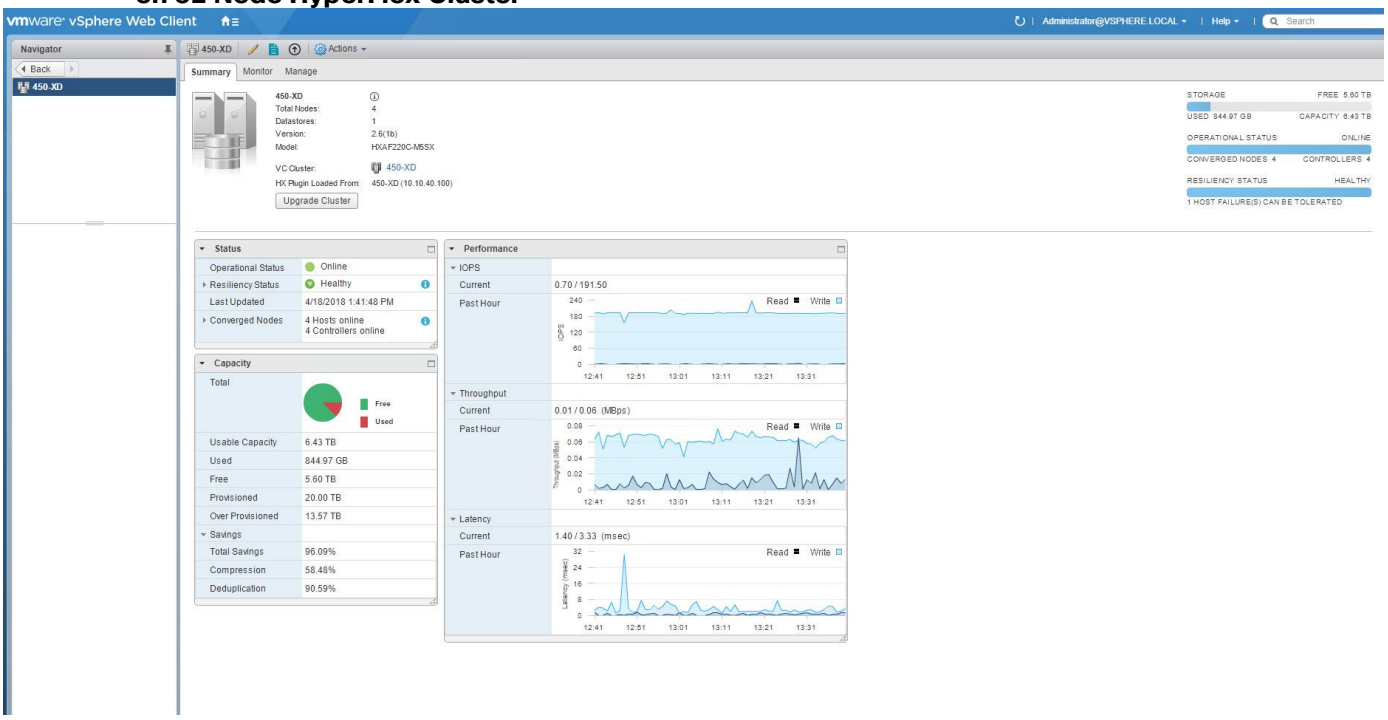


Figure 59 **vCenter WebUI Reporting HyperFlex Cluster De-duplication and Compression Savings for 600 User Sessions Supported on Windows Server 2016 Based Hosted Shared Sessions Deployed on 32 Node HyperFlex Cluster**



450 Windows 10 Citrix PVS Desktop Pool Testing on Four Node Cisco HyperFlex Cluster

Floating assigned automated Citrix XenDesktop PVS desktop pool with 450 Windows 10 VMs hosting 450 User Sessions on four HXAF220c-M5SX HyperFlex cluster

Test result highlights include:

- 0.599 second baseline response time
- 0.767 second average response time with 450 desktops running
- Average CPU utilization of 60 percent during steady state
- Average of 342 GB of RAM used out of 768 GB available
- 1500Mbps peak network utilization per host.
- Average Read Latency 0.4ms/Max Read Latency 0.7ms
- Average Write Latency 2.0ms/Max Write Latency 5.0ms
- 6000 peak I/O operations per second (IOPS) per cluster at steady state
- 130MBps peak throughput per cluster at steady state

Figure 60 **Login VSI Analyzer Chart for 450 Windows 10 Citrix XenDesktop PVS Sessions**

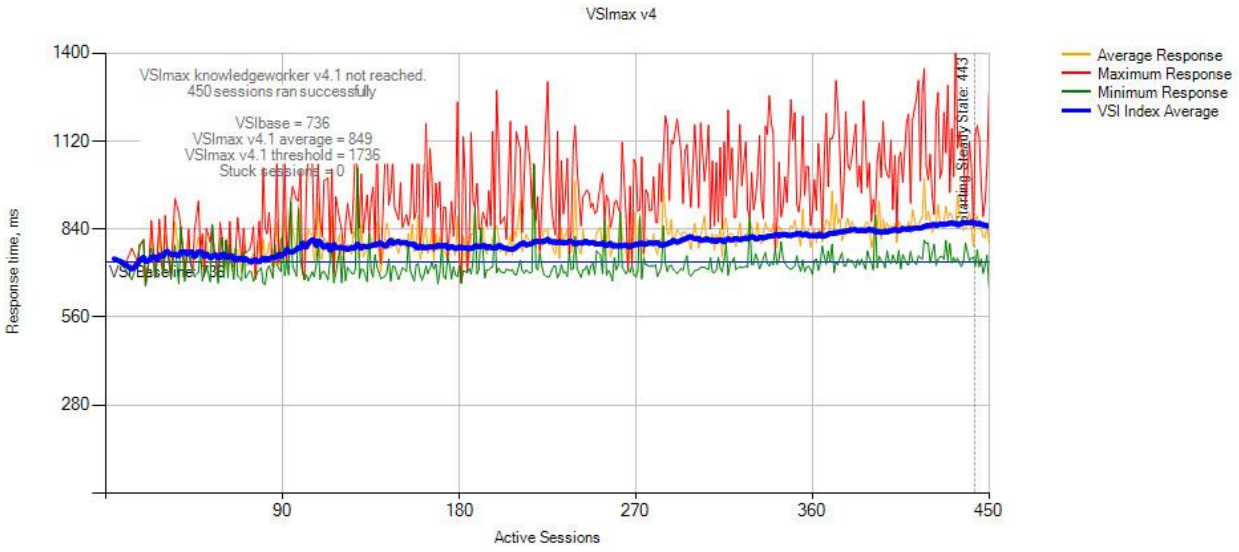


Figure 61 **Three Consecutive Login VSI Analyzer Chart for 450 Windows 10 Citrix XenDesktop PVS Sessions**

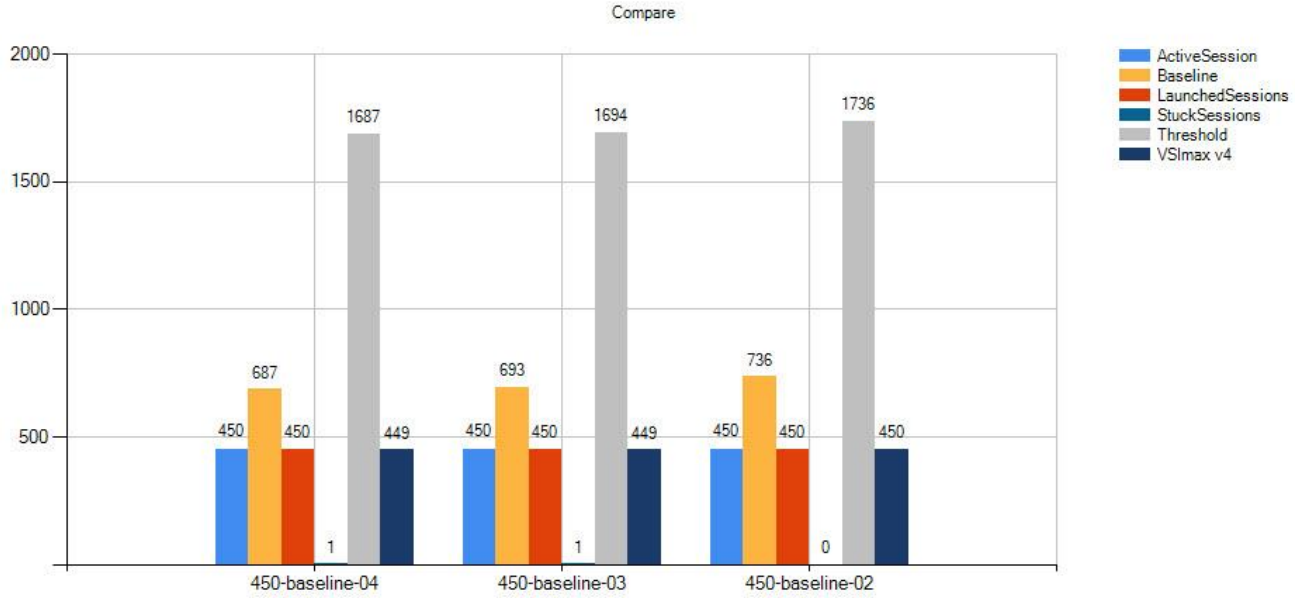


Figure 62 **Sample ESXi Host CPU Core Utilization Running 450 Windows 10 Citrix XenDesktop PVS Sessions**

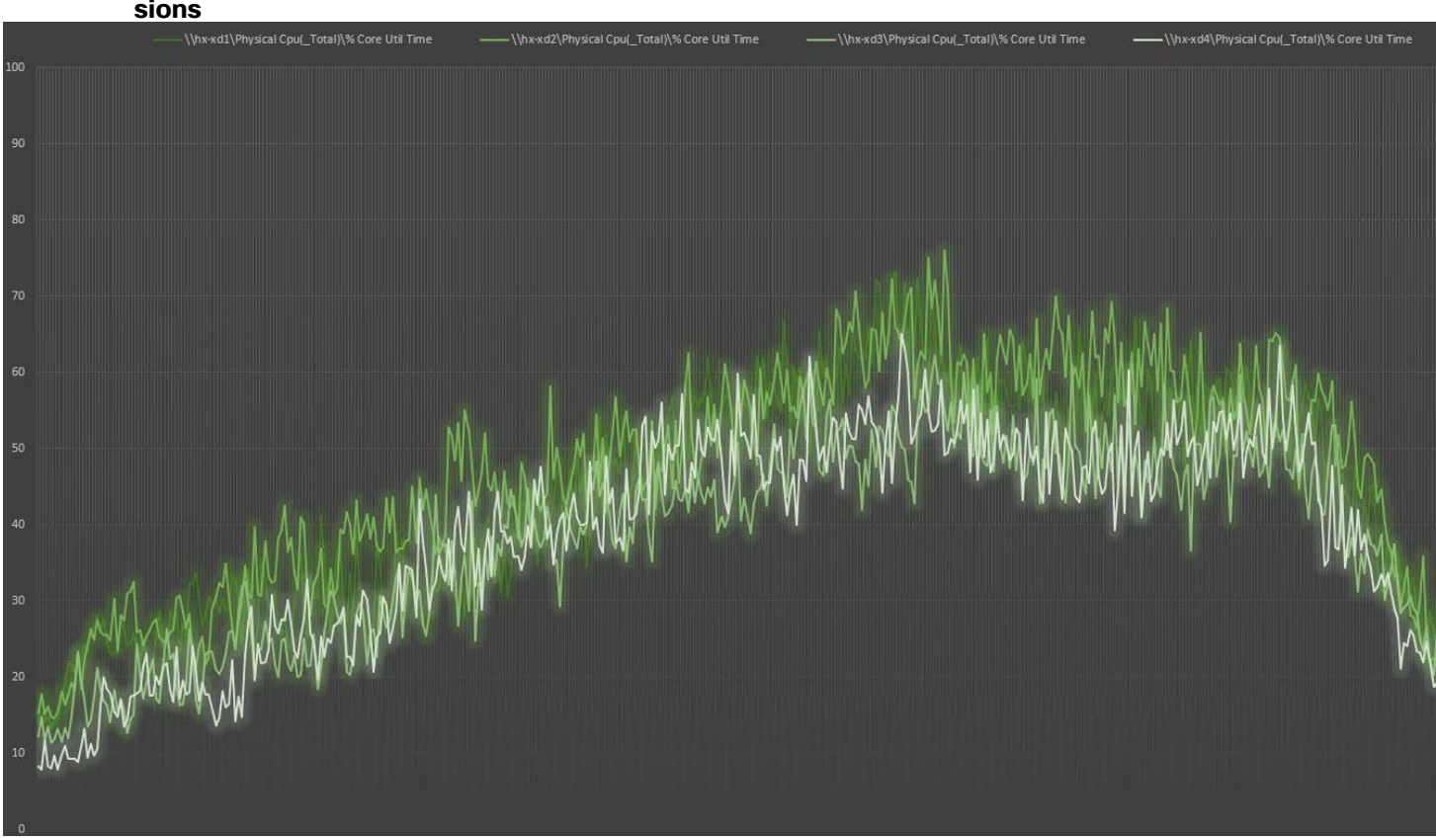


Figure 63 **ESXi Host Network Adapter (VMNICs) Mbits Received/Transmitted Per Sec Running 450 Windows 10 Citrix XenDesktop PVS Sessions**

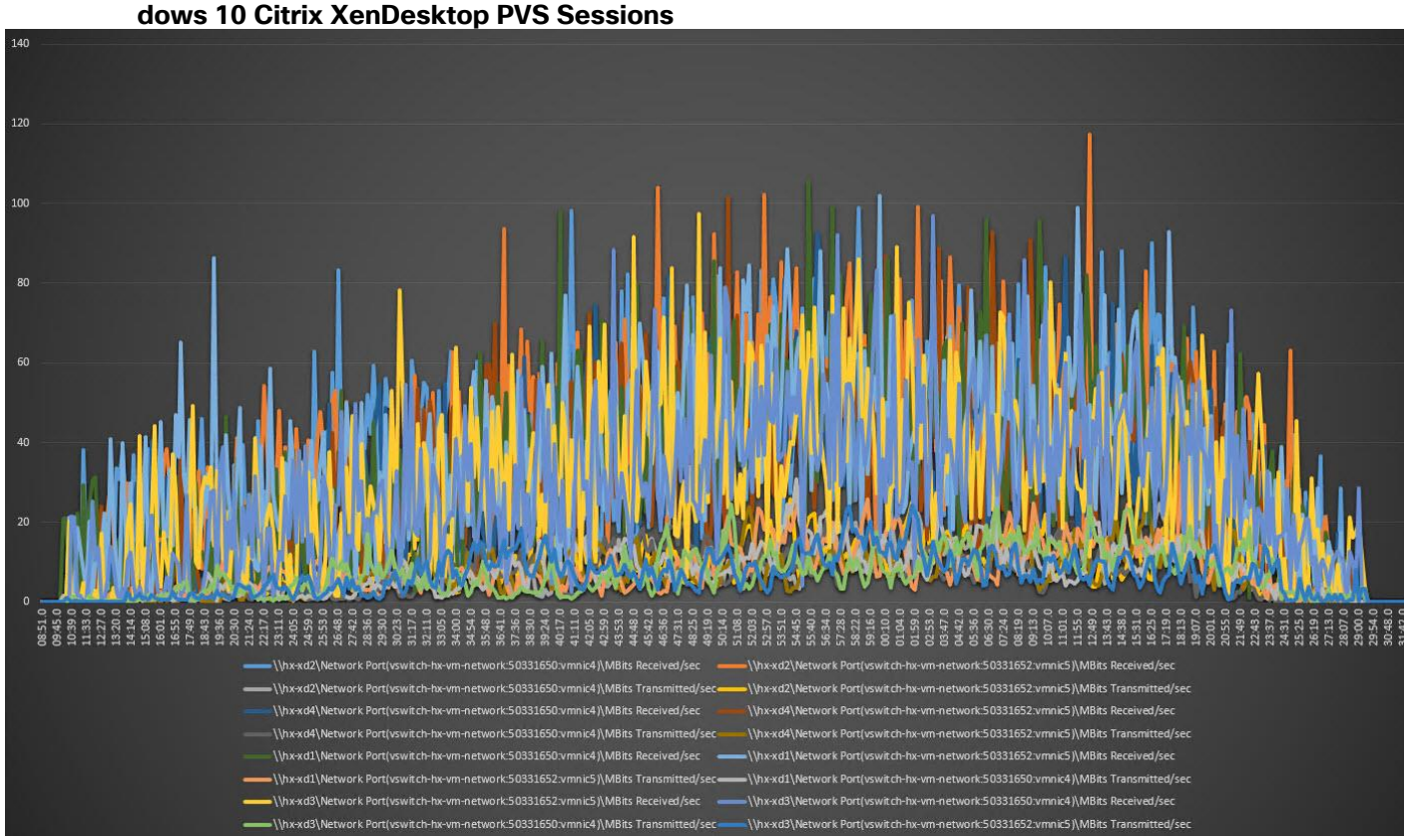


Figure 64 **HyperFlex Cluster Performance Chart for Knowledge Worker Workload Running 450 User Test on Citrix XenDesktop PVS Sessions**

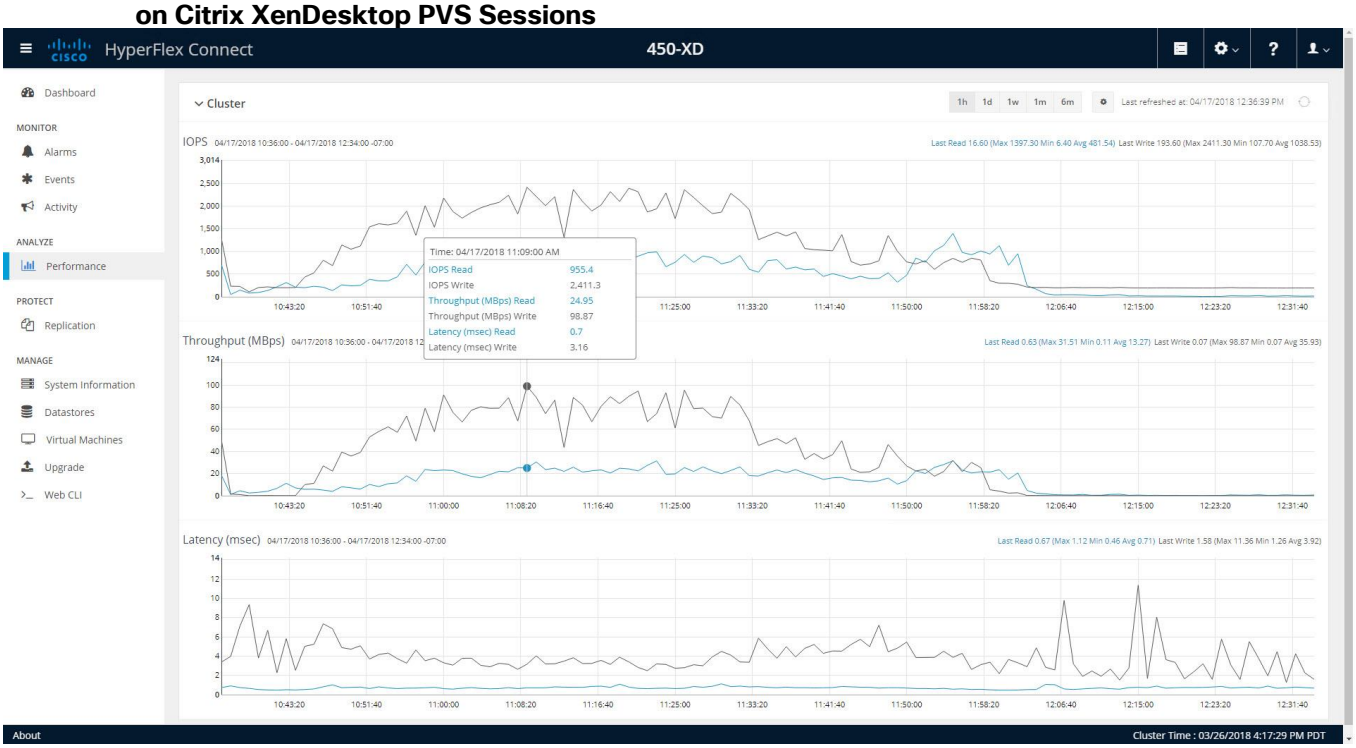
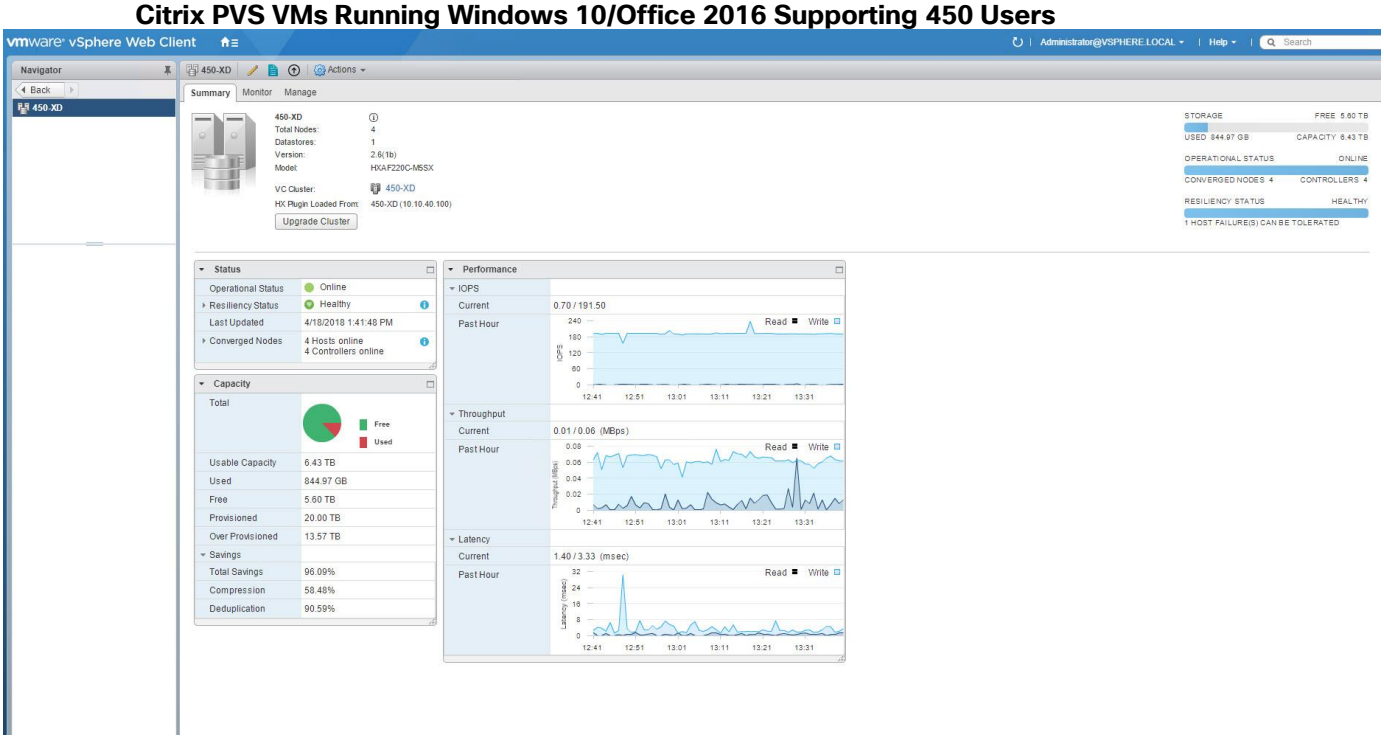


Figure 65 **vCenter WebUI Reporting HyperFlex Cluster Deduplication and Compression Savings for 450 Citrix PVS VMs Running Windows 10/Office 2016 Supporting 450 Users**



450 Windows 10 Citrix MCS Persistent Testing on Four Node Cisco HyperFlex Cluster

Floating assigned automated Linked-Clone desktop pool with 450 Windows 10 VMs hosting 450 User Sessions on four HXAF220c-M5SX HyperFlex cluster

Test result highlights include:

- 0.849 second baseline response time
- 0.736 second average response time with 450 desktops running
- Average CPU utilization of 65 percent during steady state
- Average of 320 GB of RAM used out of 768 GB available
- 1000Mbps peak network utilization per host.
- Average Read Latency 0.7ms/Max Read Latency 1.4ms
- Average Write Latency 1.9ms/Max Write Latency 4.4ms
- 3500 peak I/O operations per second (IOPS) per cluster at steady state
- 80MBps peak throughput per cluster at steady state

Figure 66 **Login VSI Analyzer Chart for 450 Windows 10 Citrix MCS Persistent Virtual Desktops**

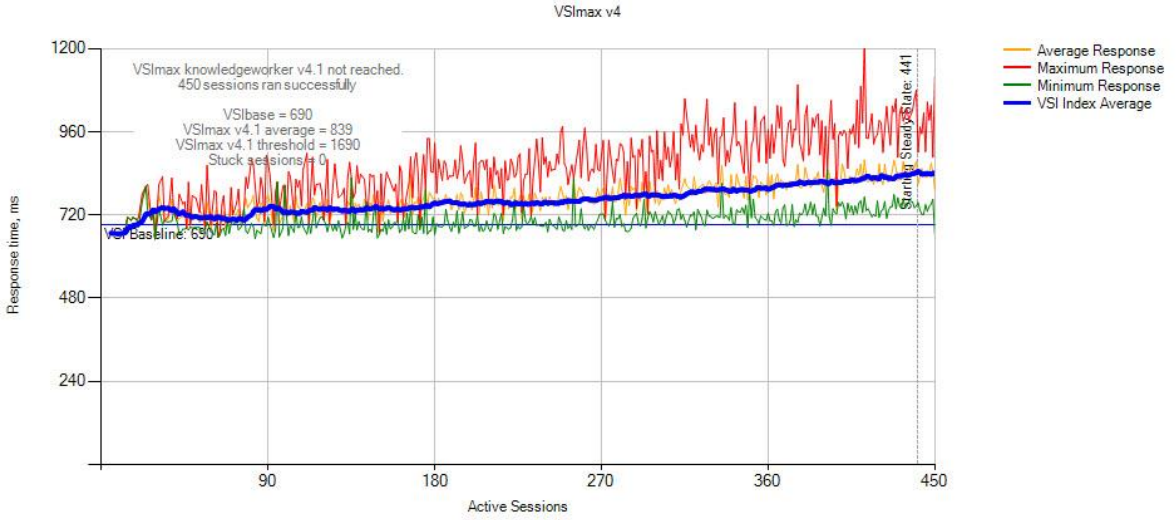


Figure 67 **Three Consecutive Login VSI Analyzer Chart for 450 Windows 10 Citrix MCS Persistent Virtual Desktops**

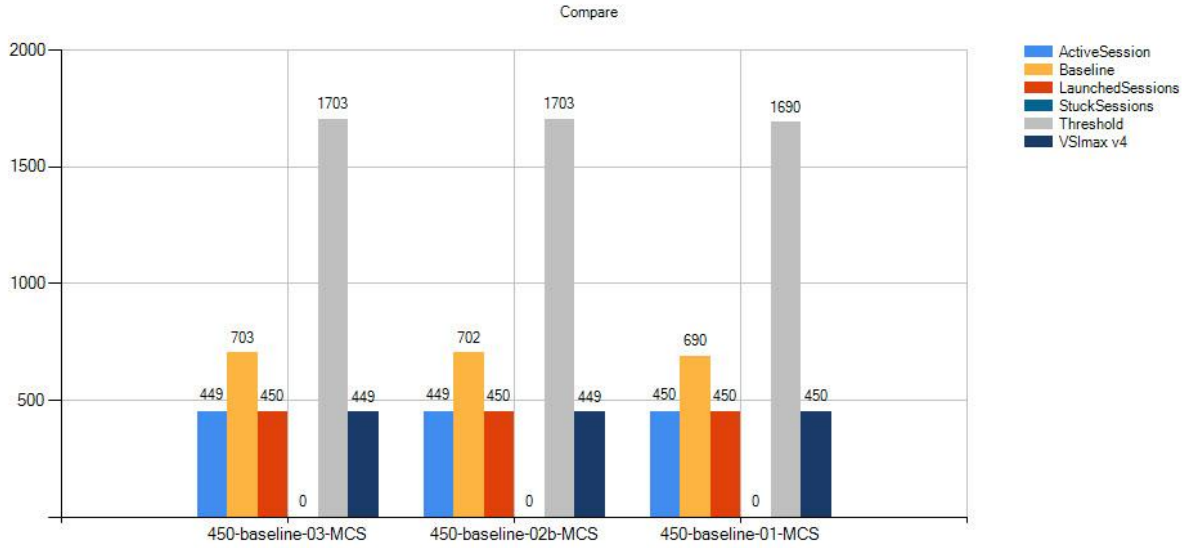


Figure 68 **Sample ESXi host CPU Core Utilization Running 450 Windows 10 Citrix MCS Persistent Virtual Desktops**

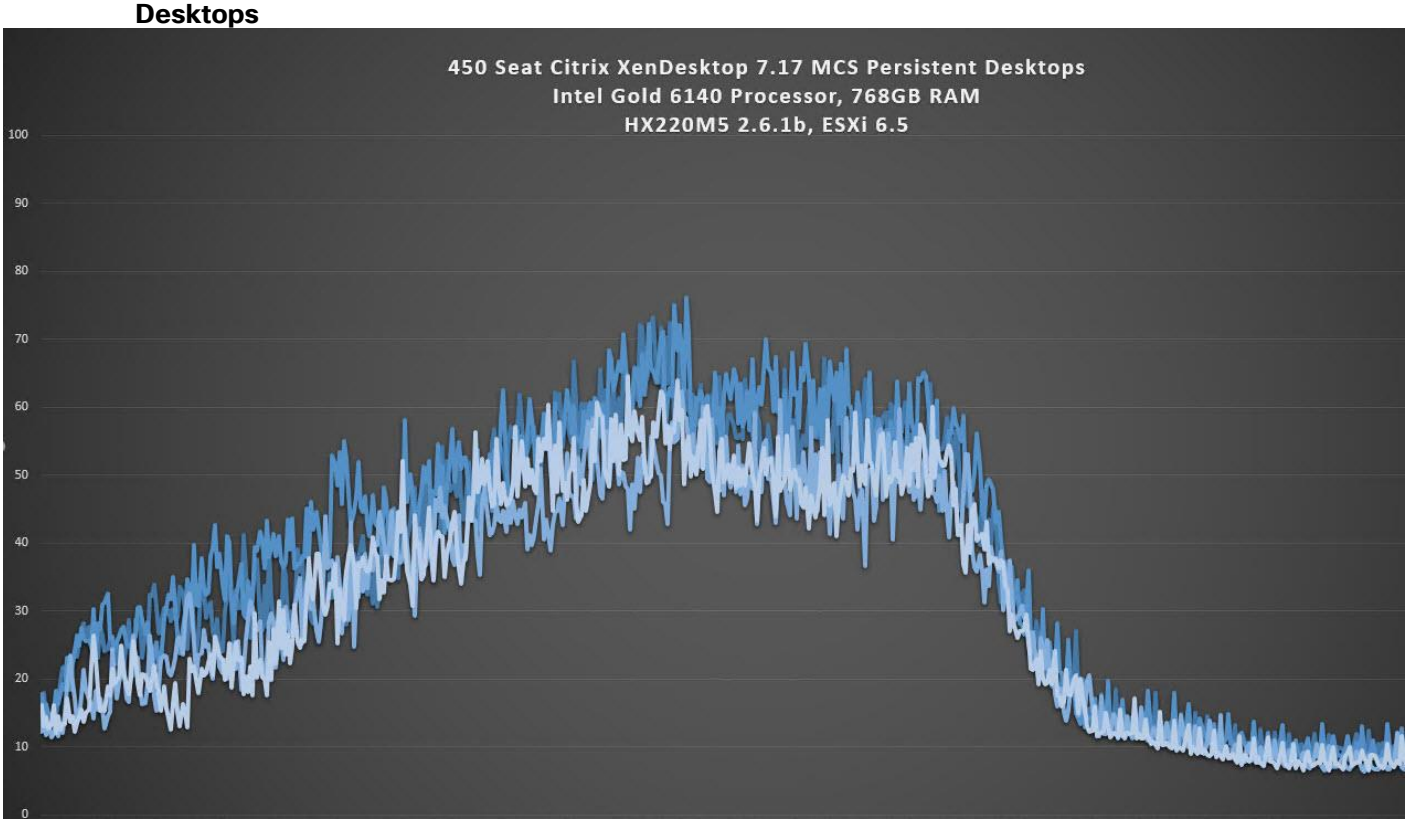


Figure 69 **ESXi Host Network Adapter (VMNICs) Mbits Received/Transmitted Per Sec Running 450 Windows 10 Citrix MCS Persistent Virtual Desktops**

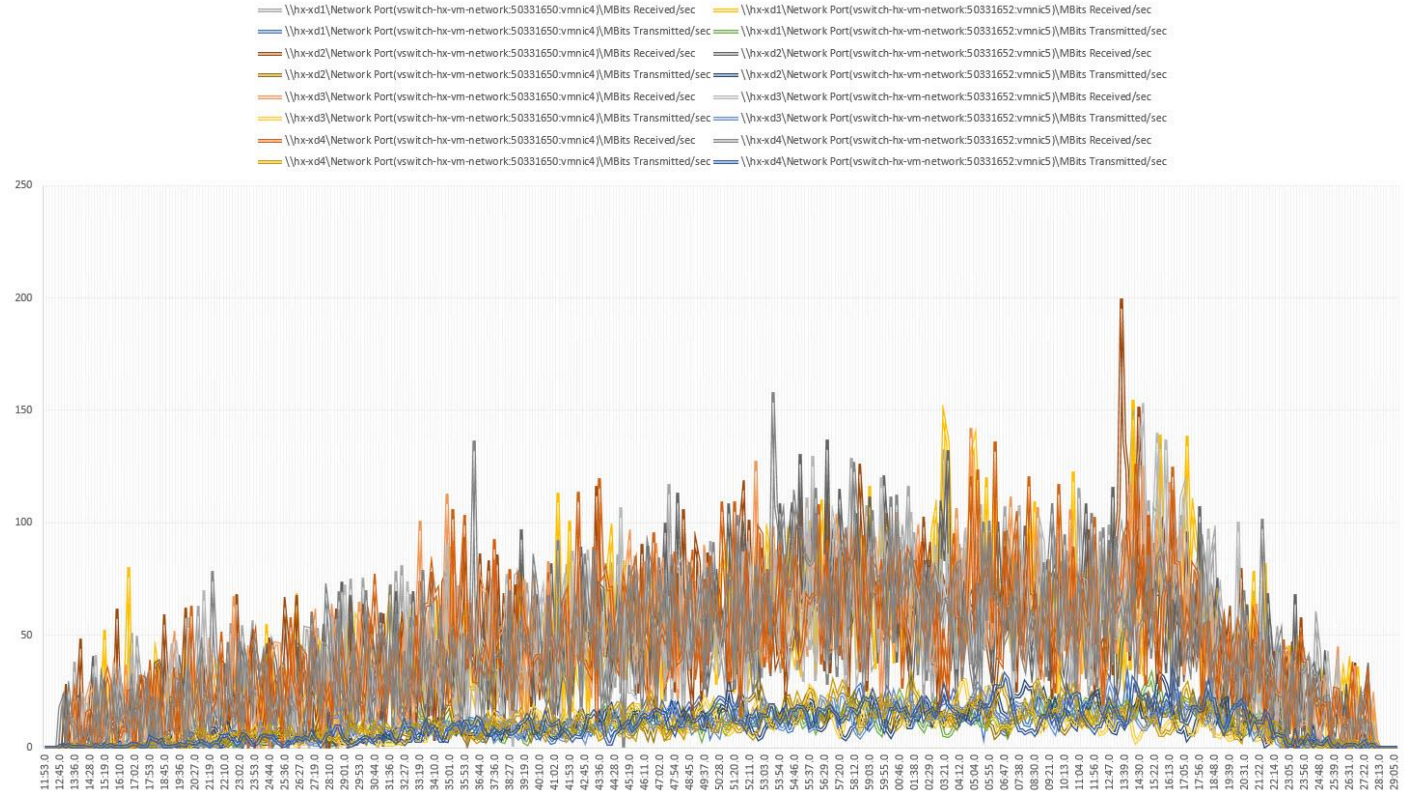
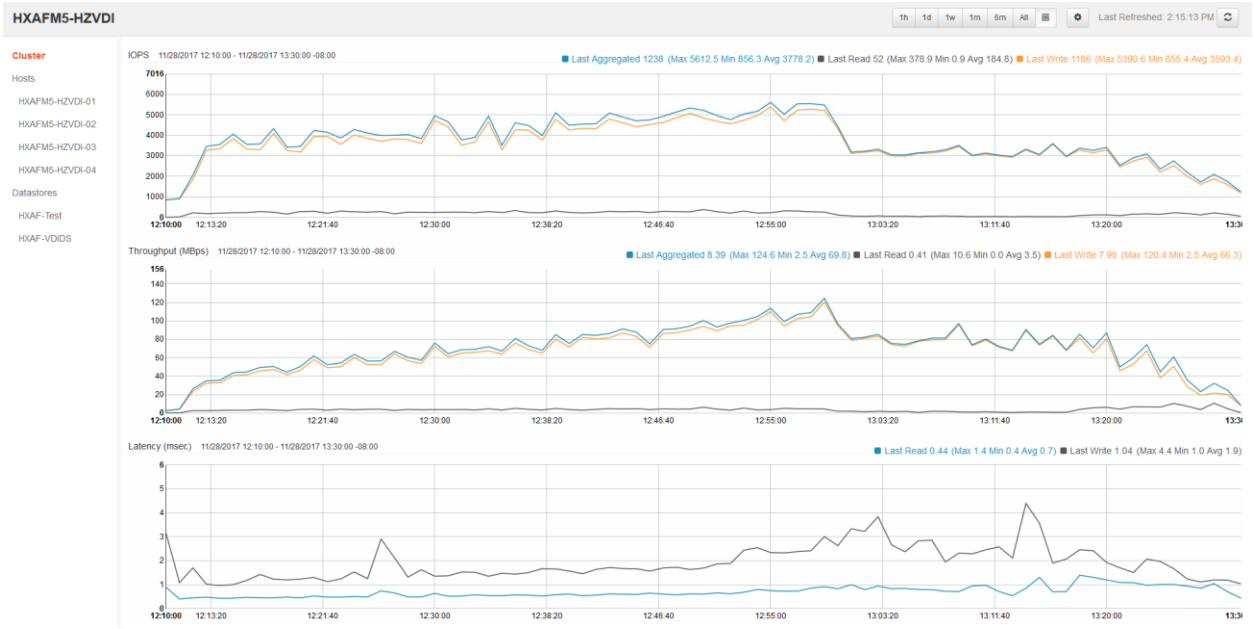


Figure 70 **HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 450 User Test on Citrix MCS Persistent Windows 10**



450 Windows 10 Citrix MCS Desktop Pool Testing on Four Node Cisco HyperFlex Cluster

450 user dedicated assignment automated pool, Windows 10 with Office 2016 full clone desktops on four HXAF220c-M5SX HyperFlex Cluster.

Test result highlights include:

- 0.690 second baseline response time
- 0.839 second average response time with 450 desktops running
- Average CPU utilization of 65 percent during steady state
- Average of 340GB of RAM used out of 768 GB available per node
- 1000Mbps peak network utilization per host.
- Average Write Latency 1.8ms/Max Write Latency 4.7ms
- Average Read Latency 0.8ms/Max Read Latency 1.4ms
- 3000 peak I/O operations per second (IOPS) at steady state
- 117MBps peak throughput at steady state

Figure 71 **Login VSI Analyzer Chart for 450 User Citrix MCS Pooled Windows 10 Virtual Desktops**

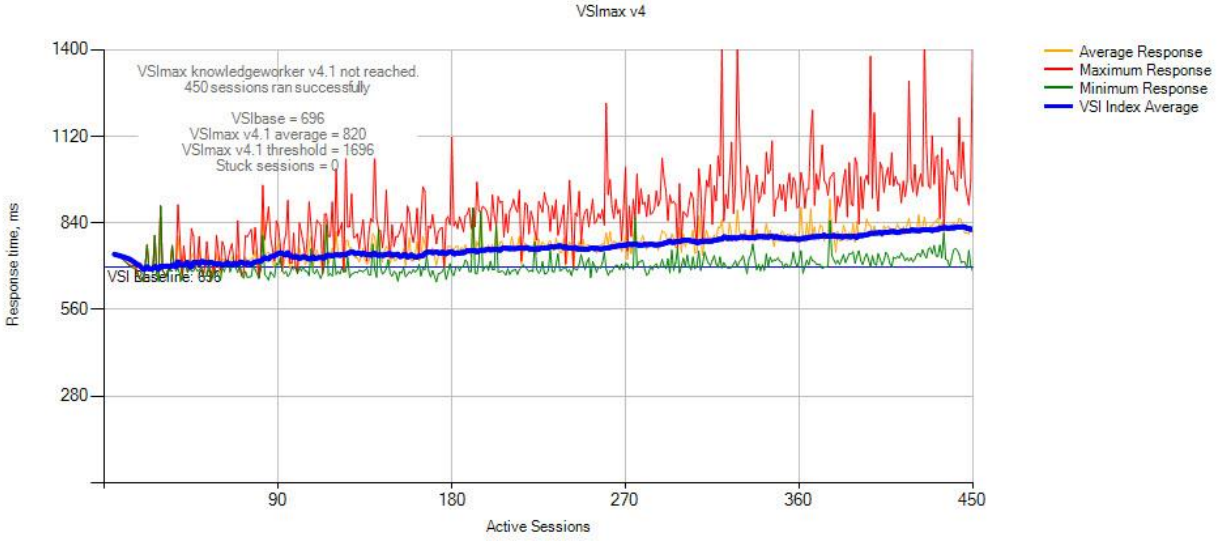


Figure 72 **Three Consecutive Test Login VSI Analyzer Chart for 450 User Citrix MCS Pooled Windows 10 Virtual Desktops**

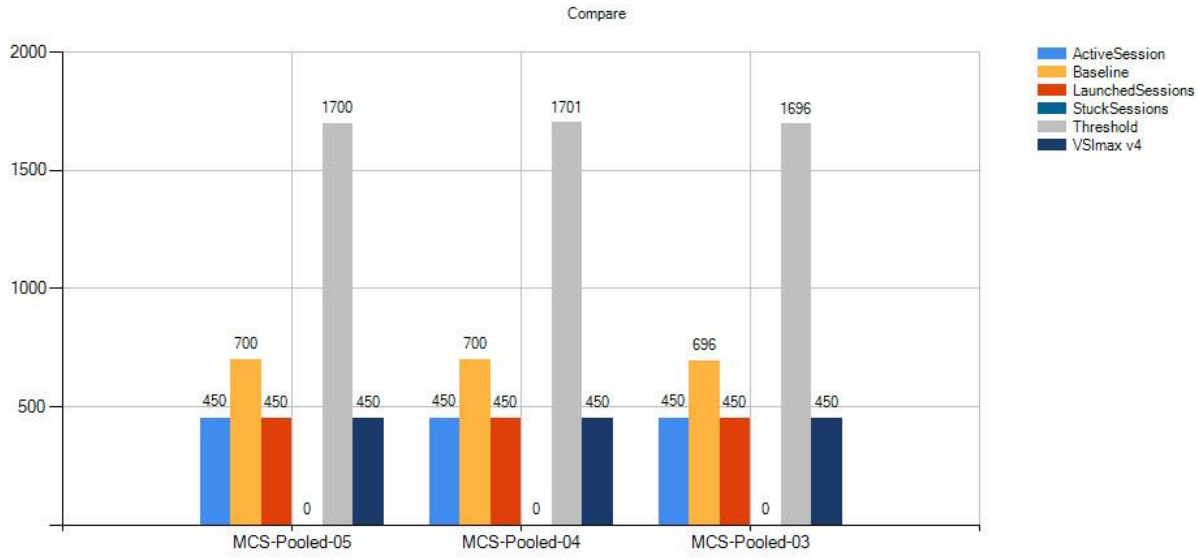


Figure 73 **Sample ESXi Host CPU Core Utilization Running 450 User Citrix MCS Pooled Windows 10 Virtual Desktops**

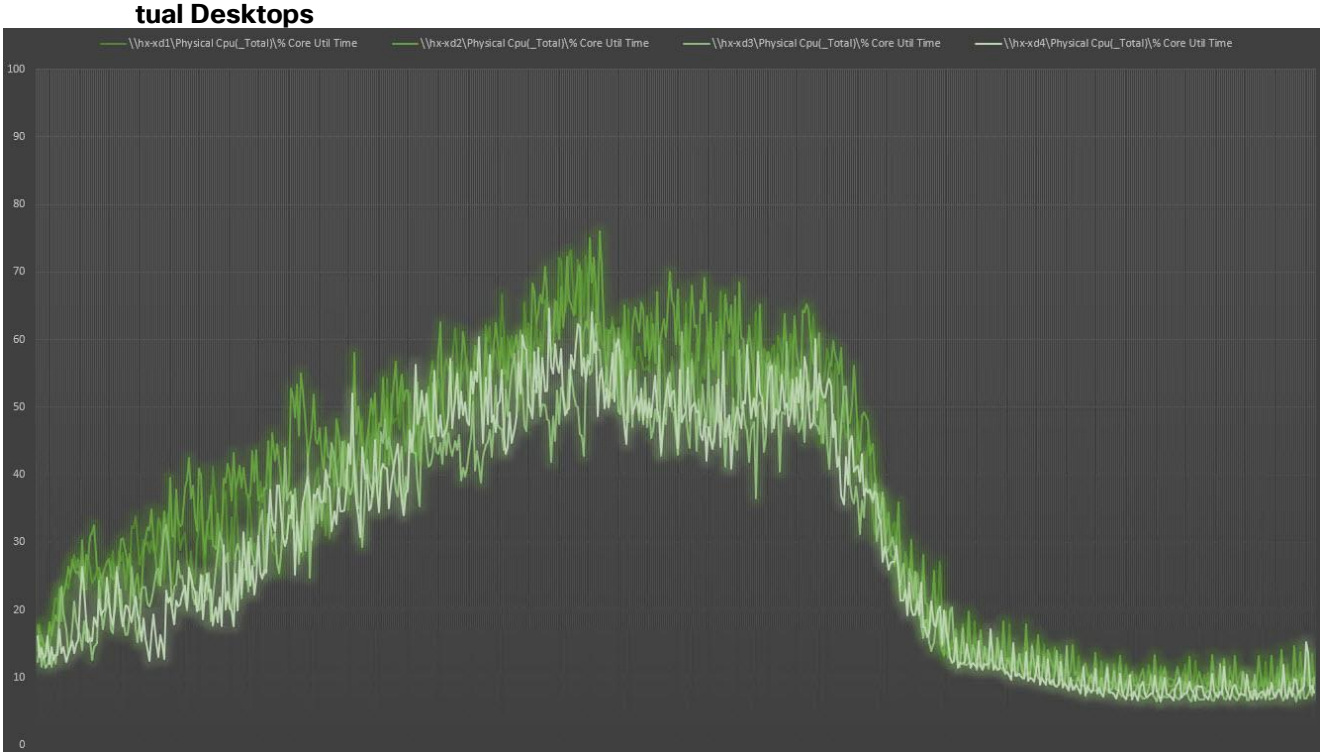


Figure 74 **Sample ESXi Host Network Adapter (VMNICs) Mbits Received /Transmitted Per Sec Running 450 User Citrix MCS Pooled Windows 10 Virtual Desktops**

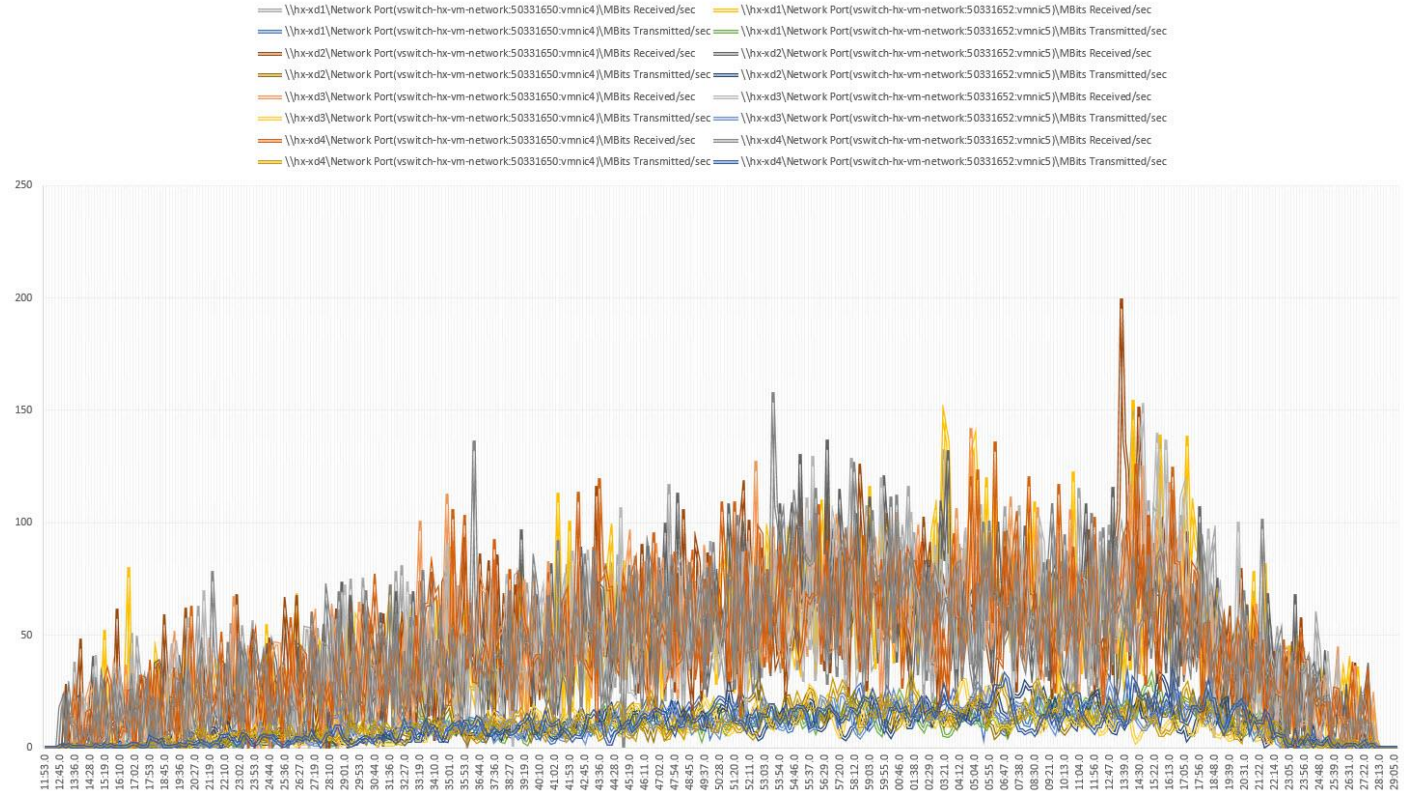


Figure 75 **HyperFlex Cluster WebUI Performance Chart for Knowledge Worker Workload Running 450 User Test on Citrix MCS Pooled Windows 10 Virtual Desktops**

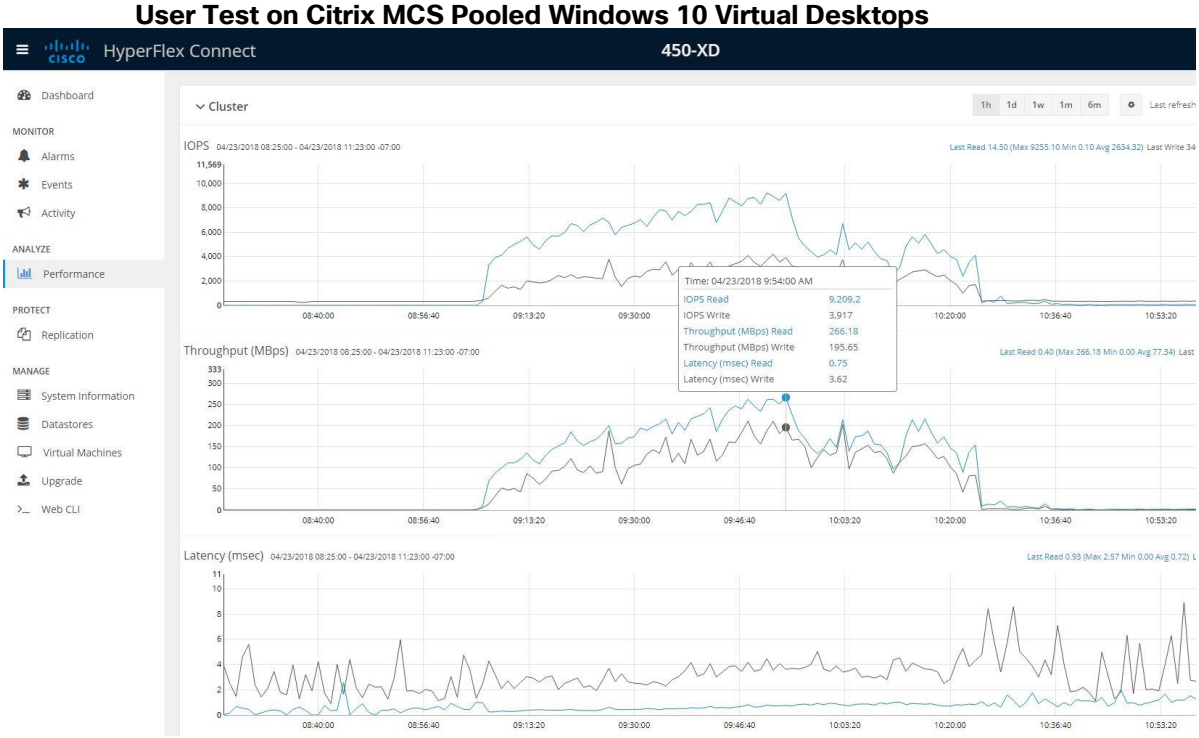
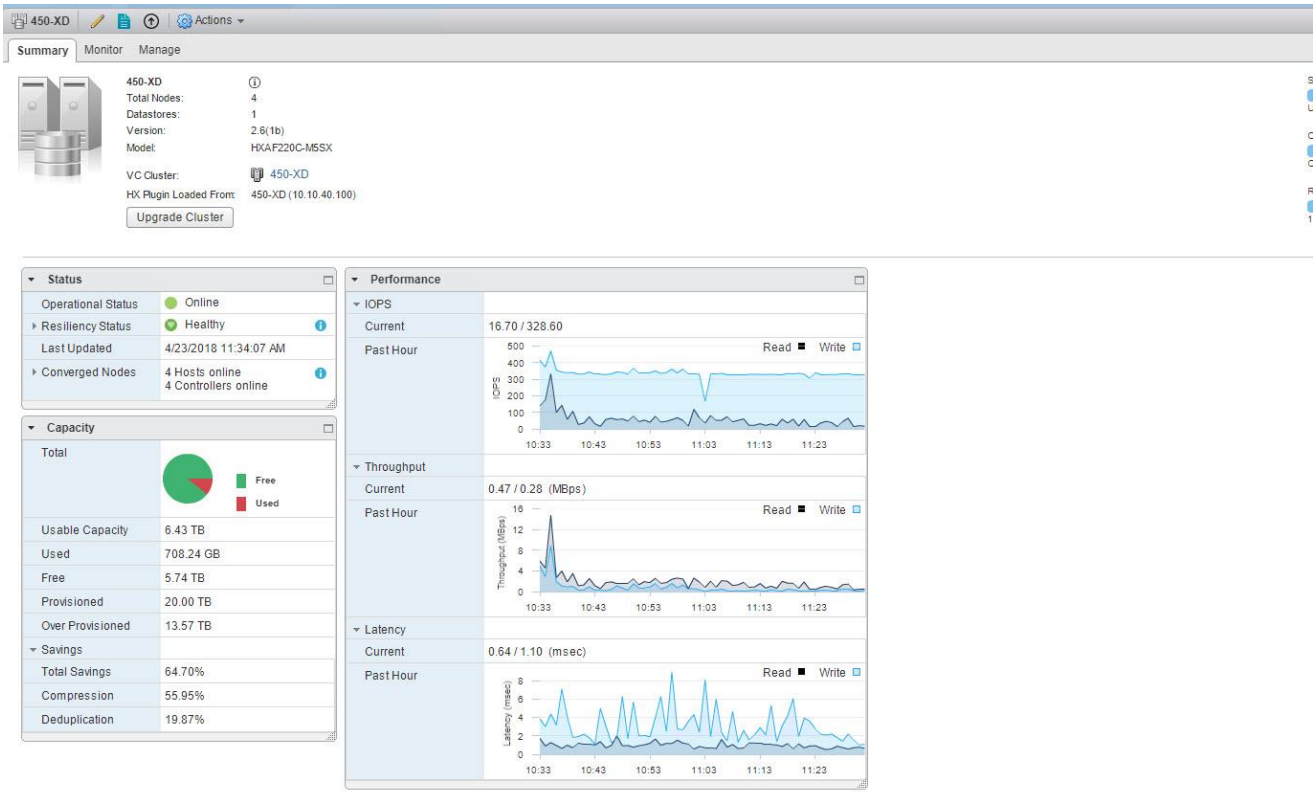


Figure 76 **vCenter WebUI Reporting HyperFlex Cluster De-duplication and Compression Savings for 450 Citrix MCS Pooled VMs running Windows 10/Office 2016 Supporting 450 Users.**


450-XD
Actions
Summary
Monitor
Manage
450-XD
Total Nodes: 4
Datastores: 1
Version: 2.6(1b)
Model: HXAF220C-M5SX
VC Cluster: 450-XD
HX Plugin Loaded From: 450-XD (10.10.40.100)
Upgrade Cluster
Status
Operational Status: Online
Resiliency Status: Healthy
Last Updated: 4/23/2018 11:34:07 AM
Converged Nodes: 4 Hosts online, 4 Controllers online
Capacity
Total
Free
Used
Usable Capacity: 6.43 TB
Used: 708.24 GB
Free: 5.74 TB
Provisioned: 20.00 TB
Over Provisioned: 13.57 TB
Savings
Total Savings: 64.70%
Compression: 55.95%
Deduplication: 19.87%
Performance
IOPS
Current: 16.70 / 328.60
Past Hour
Read
Write
IOPS
500
400
300
200
100
0
10:33
10:43
10:53
11:03
11:13
11:23
Throughput
Current: 0.47 / 0.28 (MBps)
Past Hour
Read
Write
Throughput (MBps)
16
12
8
4
0
10:33
10:43
10:53
11:03
11:13
11:23
Latency
Current: 0.64 / 1.10 (msec)
Past Hour
Read
Write
Latency (msec)
8
6
4
2
0
10:33
10:43
10:53
11:03
11:13
11:23

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.

Only Cisco offers the flexibility to add compute only nodes to a true hyperconverged cluster for compute intensive workloads like desktop virtualization. This translates to lower cost for the customer, since no hyperconvergence licensing is required for those nodes.

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

The four node tested system can be expanded to 32 nodes (16 hyper converged plus 16 compute only nodes) for an expected user capacity of 4800 knowledge worker users.

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

Virtual desktop end-user experience, as measured by the Login VSI tool in benchmark mode, is outstanding with Intel Xeon scalable family processors and Cisco 2666Mhz memory. In fact, we have set a new industry standard in performance for Desktop Virtualization on a hyper-converged platform.

About the Authors

Jeff Nichols, Technical Marketing Engineer, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.

Jeff Nichols is a Cisco Unified Computing System architect, focusing on Virtual Desktop and Application solutions with extensive experience with VMware ESX/ESXi, XenDesktop, XenApp and Microsoft Remote Desktop Services. He has expert product knowledge in application, desktop and server virtualization across all three major hypervisor platforms and supporting infrastructures including but not limited to Windows Active Directory and Group Policies, User Profiles, DNS, DHCP and major storage platforms.

Acknowledgements

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

- Mike Brennan, Product Manager, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.

Appendix A – Cisco Nexus 93108YC Switch Configuration

Switch A Configuration

```
!Command: show running-config

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

feature telnet
cfs eth distribute

feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc
feature lldp
clock protocol ntp vdc 1
```

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

rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 10.10.50.2
ntp peer 10.10.50.3
ntp server 171.68.38.66 use-vrf management
ntp logging
ntp master 8


vlan 1,50-54
vlan 50
  name InBand-Mgmt-C1
vlan 51
  name Infra-Mgmt-C1
vlan 52
  name StorageIP-C1
vlan 53
  name 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 10.29.132.20 source 10.29.132.19



interface Vlan1
  no shutdown
  ip address 10.29.132.2/24

interface Vlan50
  no shutdown
  ip address 10.10.50.2/24
  hsrp version 2
  hsrp 50
    preempt
    priority 110
    ip 10.10.50.1

  ip dhcp relay address 10.10.51.21
  ip dhcp relay address 10.10.51.22

interface Vlan51
  no shutdown
```

```
  ip address 10.10.51.2/24
  hsrp version 2
  hsrp 51
    preempt
    priority 110
    ip 10.10.51.1

interface Vlan52
  no shutdown
  ip address 10.10.52.2/24
  hsrp version 2
  hsrp 52
    preempt
    priority 110
    ip 10.10.52.1

interface Vlan53
  no shutdown

  ip address 10.10.53.2/24
  hsrp version 2
  hsrp 53
    preempt
    priority 110
    ip 10.10.53.1

interface Vlan54
  no shutdown
  ip address 10.54.0.2/20
  hsrp version 2
  hsrp 54
    preempt
    priority 110
```

```
    ip 10.54.0.1
  ip dhcp relay address 10.10.51.21
  ip dhcp relay address 10.10.51.22

interface port-channel10
  description vPC-PeerLink
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  spanning-tree port type network

  service-policy type qos input jumbo
  vpc peer-link

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

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

interface Ethernet1/1
  switchport mode trunk
```

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

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

interface Ethernet1/3
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  channel-group 10 mode active

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

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

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

interface Ethernet1/7
  switchport mode trunk
```

```
  switchport trunk allowed vlan 1,50-54
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/8
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20
```

```
interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  spanning-tree port type edge trunk

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

interface Ethernet1/27
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  spanning-tree port type edge trunk

interface Ethernet1/28
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54

  spanning-tree port type edge trunk

interface Ethernet1/29
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
```

```
  spanning-tree port type edge trunk

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

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

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

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40
```

```
interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44


interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0
  vrf member management
  ip address 10.29.132.19/24
```

```
clock timezone PST -8 0
clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60
line console
line vty
boot nxos bootflash:/nxos.7.0.3.I2.2d.bin
```

Switch B Configuration

```
!Command: show running-config
!Time: Fri Dec 15 17:18:36 2017

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

feature telnet
cfs eth distribute

feature interface-vlan
feature hsrp
feature lacp
```

```
feature dhcp
feature vpc
feature lldp
clock protocol ntp vdc 1

no password strength-check
username admin password 5 $1$jEwHqUvM$gpOec2hramkyX09KD3/Dn.  role network-admin
ip domain-lookup
no service unsupported-transceiver
class-map type qos match-all class-fcoe
policy-map type 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 10.10.50.2
ntp server 10.10.50.3
ntp server 171.68.38.66 use-vrf management
ntp logging
ntp master 8

vlan 1,50-54
vlan 50
  name InBand-Mgmt-C1
vlan 51
  name Infra-Mgmt-C1
```

```
vlan 52
  name StorageIP-C1
vlan 53
  name 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 10.29.132.19 source 10.29.132.20


interface Vlan1
  no shutdown
  ip address 10.29.132.3/24

interface Vlan50
  no shutdown
  ip address 10.10.50.3/24
  hsrp version 2
  hsrp 50
    preempt
    priority 110
    ip 10.10.50.1

  ip dhcp relay address 10.10.51.21
```

```
  ip dhcp relay address 10.10.51.22

interface Vlan51
  no shutdown
  ip address 10.10.51.3/24
  hsrp version 2
  hsrp 51
    preempt
    priority 110
    ip 10.10.51.1

interface Vlan52
  no shutdown
  ip address 10.10.52.3/24
  hsrp version 2
  hsrp 52
    preempt
    priority 110
    ip 10.10.52.1

interface Vlan53
  no shutdown
  ip address 10.10.53.3/24
  hsrp version 2
  hsrp 53
    preempt
    priority 110
    ip 10.10.53.1

interface Vlan54
  no shutdown
  ip address 10.54.0.3/20
```

```
  hsrp version 2
  hsrp 54
    preempt
    priority 110
    ip 10.54.0.1
  ip dhcp relay address 10.10.51.21
  ip dhcp relay address 10.10.51.22

interface port-channel10
  description vPC-PeerLink
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  spanning-tree port type network

  service-policy type qos input jumbo
  vpc peer-link

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

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

```
  vpc 12

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

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

interface Ethernet1/3
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  channel-group 10 mode active

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

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

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

```
interface Ethernet1/7
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/8
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18
```

```
interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  spanning-tree port type edge trunk

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

interface Ethernet1/27
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54
  spanning-tree port type edge trunk

interface Ethernet1/28
  switchport mode trunk
  switchport trunk allowed vlan 1,50-54

  spanning-tree port type edge trunk
```

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

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

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

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

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38
```

```
interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44


interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48
  switchport access vlan 50

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53
```

```
interface Ethernet1/54


interface mgmt0
  vrf member management

  ip address 10.29.132.20/24
clock timezone PST -8 0
clock summer-time PDT 2 Sunday March 02:00 1 Sunday November 02:00 60
line console
line vty
boot nxos bootflash:/nxos.7.0.3.I2.2d.bin
```