The bridge to possible

Deployment Guide
Cisco Public

FlexPod Datacenter with Citrix Virtual Apps and Desktops with VMware vSphere 7 for up to 2500 Seats

Deployment Guide for Virtual Desktop Infrastructure built on Cisco UCS B200 M6 with 3rd Generation Intel Xeon Scalable Processors, Cisco Intersight 4.2.(2a), NetApp Storage for Citrix Virtual Apps and Desktops 2203 LTSR, and VMware vSphere 7.0 U3 Hypervisor

Published: January 2023

In partnership with:

About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, go to: http://www.cisco.com/go/designzone.

Executive Summary

Cisco Validated Designs consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of our customers.

The solution explains the deployment of a predesigned, best-practice data center architecture with Citrix Virtual Apps and Desktops Remote Desktop Sever Hosted (RDSH) sessions and Windows 10 Virtual desktops and VMware vSphere built on the Cisco Unified Computing System (Cisco UCS), the Cisco Nexus 9000 family of switches, Cisco MDS 9000 family of Fibre Channel switches and NetApp Storage AFF A400 all flash array supporting Fibre Channel storage access.

Additionally, this FlexPod solution is also delivered as Infrastructure as Code (IaC) to eliminate error-prone manual tasks, allowing quicker and more consistent solution deployments. Cisco Intersight cloud platform delivers monitoring, orchestration, workload optimization and lifecycle management capabilities for the FlexPod solution.

When deployed, the architecture presents a robust infrastructure viable for a wide range of application workloads implemented as a Virtual Desktop Infrastructure (VDI).

This document provides a Reference Architecture for a virtual desktop and application design using VMware Remote Desktop Server Hosted (RDSH) and VMware Windows 10 Virtual Desktops built on Cisco UCS with a NetApp All Flash FAS (AFF) A400 storage and the VMware vSphere ESXi 7.0U3 hypervisor platform.

Customers interested in understanding the FlexPod design and deployment details, including the configuration of various elements of design and associated best practices, should refer to Cisco Validated Designs for FlexPod, here: https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html

The landscape of desktop and application virtualization is changing constantly. The high-performance Cisco UCS B series blade servers and Cisco UCS unified fabric combined as part of the FlexPod Proven Infrastructure with the latest generation NetApp AFF storage result in a more compact, more powerful, more reliable, and more efficient platform.

This document provides the architecture and design of a virtual desktop infrastructure for up to 2500 end user compute users. The solution virtualized on Cisco UCS B200 M6 blade server, booting VMware vSphere 7.0 Update 3 through FC SAN from the AFF A400 storage array. The virtual desktops are powered using VMware Remote Desktop Server Hosted sessions and VMWare Win 10 Virtual Desktops, with a mix of RDS hosted shared desktops (2500), pooled/non-persistent hosted virtual Windows 10 PVS (1700) and persistent Full clone virtual Windows 10 desktops.

The solution provides outstanding virtual desktop end-user experience as measured by the Login VSI 4.1.40 Knowledge Worker workload running in benchmark mode.

The 2500-seat solution provides a large-scale building block that can be replicated to confidently scale-out to tens of thousands of users.

Solution Overview

This chapter contains the following:

Introduction

The current industry trend in data center design is towards shared infrastructures. By using virtualization along with pre-validated IT platforms, enterprise customers have embarked on the journey to the cloud by moving away from application silos and toward shared infrastructure that can be quickly deployed, thereby increasing agility, and reducing costs. Cisco, NetApp storage, and VMware have partnered to deliver this Cisco Validated Design, which uses best of breed storage, server, and network components to serve for the foundation for desktop virtualization workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

The Cisco UCS B200 M6 Blade Server delivers performance, flexibility, and optimization for deployments in data centers,
cloud, and remote sites. This enterprise-class server offers market-leading versatility, and density without compromise for workloads, including web infrastructure, distributed databases, Virtual Desktop Infrastructure (VDI), converged infrastructure, and enterprise applications such as SAP HANA and Oracle. The Cisco UCS B200 M6 Blade Server can quickly deploy stateless physical and virtual workloads through a programmable, easy-to-use Cisco Intersight and Cisco Intersight and simplified server access through Cisco SingleConnect technology.

Audience

The intended audience for this document includes, but is not limited to IT architects, sales engineers, field consultants, professional services, IT managers, IT engineers, partners, and customers who are interested in learning about and deploying the Virtual Desktop Infrastructure (VDI)

Purpose of this Document

This document provides a step-by-step design, configuration, and implementation guide for the Cisco Validated Design for a large-scale Citrix Virtual Apps and Desktops Remote Desktop Server Hosted (RDSH) sessions and Windows 10 Virtual Desktops with NetApp AFF A400, NS224 NVMe Disk Shelf, Cisco UCS B200 M6 Blade Servers, Cisco Nexus 9000 Series Ethernet Switches and Cisco MDS 9000 Series Multilayer Fibre Channel Switches.

What's New in this Release?

This version of the FlexPod VDI Design based on the latest Cisco FlexPod Virtual Server Infrastructure and introduces the Cisco UCS M6 Servers featuring the 3rd Gen Intel Xeon Scalable processors.

Highlights for this design include:

- Deploying and managing Cisco UCS 5108 chassis equipped with Cisco UCS B200 M6 blade server using Cisco UCS (Cisco Unified Computing System)
- Support for Cisco UCS B200 M6 blade servers with 3rd Gen Intel Xeon Scalable Family processors and 3200 MHz memory
- Support for the Cisco Intersight 4.2
- Validation of Cisco Nexus 9000 with NetApp AFF A400 system
- Validation of Cisco MDS 9000 with NetApp AFF A400 system
- Support for NetApp Storage AFF A400 with ONTAP version 9.10.1P1
- Citrix Virtual Apps and Desktops 2203 LTSR Citrix Remote Desktop Sever Hosted Sessions
- Citrix Virtual Apps and Desktops 2203 LTSR Citrix Provisioning Server virtual machines
- Citrix Virtual Apps and Desktops 2203 LTSR Citrix persistent full desktops
- Support for VMware vSphere 7.0 U3
- Fully automated solution deployment covering FlexPod infrastructure and vSphere virtualization

FlexPod Cisco Validated Design Advantages for VDI

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 Microsoft Windows 10 virtual desktops and RDS server desktop sessions based on Microsoft Server 2022. The mixed workload solution includes Cisco UCS hardware and Data Platform software, Cisco Nexus switches, the Cisco Unified Computing System (Cisco UCS), Citrix Virtual Apps and Desktops and VMware vSphere software in a single package. The design is efficient such that the networking, computing, and storage components occupy 18-rack units 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 UCS 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 unit can be scaled both up (adding resources to a Cisco Validated Design unit) and out (adding more Cisco Validated Design units).

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

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

- **More power, same size**. Cisco UCS B200 M6 blade servers dual 32-core 2.0 GHz Intel Xeon (Gold 6338) Scalable Family processors with 1 TB of 3200 Mhz memory with Citrix Virtual Apps and Desktops support more virtual desktop workloads than the previously released generation processors on the same hardware. The Intel Xeon Gold 6338 32-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 UCS B200 M6 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 2500 user Remote Desktop Server Hosted (RDSH) sessions and 1700 Win 10 Virtual Desktops environment booted and registered with the Citrix Broker in under 10 minutes, providing our customers with an extremely fast, reliable cold-start desktop virtualization system.
- **Stress-tested to the limits during simulated login storms**. The 2500 user RDSH sessions and 1700 Win 10 Virtual Desktops environment ready 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 1700 user system is 8 rack units, including Cisco Nexus Switching and Cisco Fabric interconnects. Incremental seat Cisco converged solutions clusters can be added one at a time to a total of 32 nodes.
- **100 percent virtualized** This CVD presents a validated design that is 100 percent virtualized on VMware ESXi 7.0U3 All of the virtual desktops, user data, profiles, and supporting infrastructure components, including Active Directory, SQL Servers, Citrix Virtual Apps and Desktops Connection Server components, Citrix VDI virtual desktops and RDSH servers were hosted as virtual machines.
- **Cisco data center management**: Cisco maintains industry leadership with the new Cisco Intersight 4.2(2a) software that simplifies scaling, guarantees consistency, and eases maintenance. Cisco’s ongoing development efforts with Cisco Intersight, Cisco UCS Central, and Cisco UCS Director ensure 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 25G Fabric**: Our 25G unified fabric story gets additional validation on 6400 Series Fabric Interconnects as Cisco runs more challenging workload testing, while maintaining unsurpassed user response times.
- **NetApp AFF A400** array provides industry-leading storage solutions that efficiently handle the most demanding I/O bursts (for example, login storms), profile management, and user data management, deliver simple and flexible business continuance, and help reduce storage cost per desktop.
- **NetApp AFF A400** array provides a simple to understand storage architecture for hosting all user data components (VMs, profiles, user data) on the same storage array.
- **NetApp clustered Data ONTAP software** enables to seamlessly add, upgrade, or remove storage from the infrastructure to meet the needs of the virtual desktops.
- **Citrix Virtual Apps and Desktops advantage**: Citrix Virtual Apps and Desktops follows a new unified product architecture that supports both Virtual Desktops and Remote Desktop Server Hosted server sessions. This new Citrix release simplifies tasks associated with large-scale VDI management. This modular solution supports seamless delivery of Windows apps and desktops as the number of user increase.
- **Optimized for performance and scale**. For hosted shared desktop sessions, the best performance was achieved when the number of vCPUs assigned to the Citrix RDS virtual machines did not exceed the number of hyper-threaded (logical) cores available on the server. In other words, maximum performance is obtained when not overcommitting the CPU resources for the virtual machines running virtualized RDS systems.
- **Provisioning desktop machines made easy**: Citrix Virtual Apps and Desktops provisions Remote Desktop Hosted Sessions (RDS) virtual desktops as well as hosted shared desktop virtual machines for this solution using a single method for both, the “Automated floating assignment desktop pool.” “Dedicated user assigned desktop pool” for persistent desktops was provisioned in the same Citrix administrative console. The new method of Instant Clone greatly reduces the amount of life-cycle spend and the maintenance windows for the guest OS.

Cisco Desktop Virtualization Solutions: Data Center

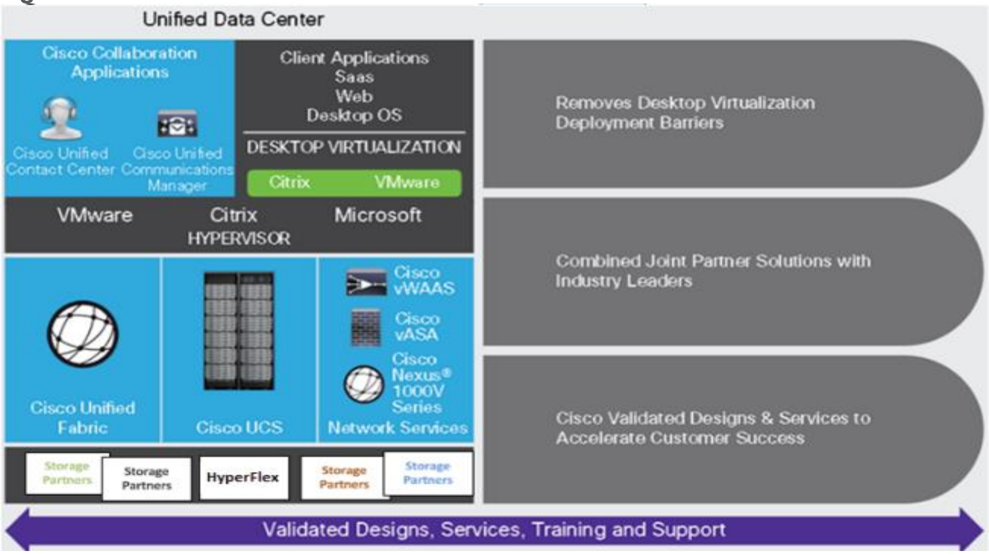
The Evolving Workplace

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

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

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

Figure 1. Cisco Data Center Partner Collaboration


Unified Data Center
Cisco Collaboration Applications
Cisco Unified Contact Center
Cisco Unified Communications Manager
Client Applications
Saas
Web
Desktop OS
DESKTOP VIRTUALIZATION
Citrix
VMware
VMware
Citrix
Microsoft
HYPERVISOR
Cisco Unified Fabric
Cisco UCS
Cisco vWAAS
Cisco vASA
Cisco Nexus® 1000V Series
Network Services
Storage Partners
Storage Partners
HyperFlex
Storage Partners
Storage Partners
Removes Desktop Virtualization Deployment Barriers
Combined Joint Partner Solutions with Industry Leaders
Cisco Validated Designs & Services to Accelerate Customer Success
Validated Designs, Services, Training and Support

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 NetApp 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, 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 Intersight 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 Intersight 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 converged architecture infrastructure packages such as FlexPod. 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

The growth of a desktop virtualization solution is all but inevitable, so a solution must be able to scale, and scale predictably, with that growth. The Cisco Desktop Virtualization Solutions built on FlexPod Datacenter infrastructure supports high virtual-desktop density (desktops per server), and additional servers and storage scale with near-linear performance. FlexPod Datacenter provides a flexible platform for growth and improves business agility. Cisco Intersight 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 UCS servers provide near-linear performance and scale. Cisco UCS implements the patented Cisco Extended Memory Technology to offer large memory footprints with fewer sockets (with scalability to up to 1 terabyte (TB) of memory with 2- and 4-socket servers). Using unified fabric technology as a building block, Cisco UCS server aggregate bandwidth can scale to up to 80 Gbps per server, and the northbound Cisco UCS fabric interconnect can output 2 terabits per second (Tbps) at line rate, helping prevent desktop virtualization I/O and memory bottlenecks. Cisco UCS, with its high-performance, low-latency unified fabric-based networking architecture, supports high volumes of virtual desktop traffic, including high-resolution video and communications traffic. In addition, Cisco storage partners NetApp help maintain data availability and optimal performance during boot and login storms as part of the Cisco Desktop Virtualization Solutions. Recent Cisco Validated Designs for End User Computing based on FlexPod solutions have demonstrated scalability and performance, with up to 2500 desktops up and running in less than 15 minutes.

FlexPod Datacenter 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.

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 NetApp FlexPod solution 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 NetApp deliver 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

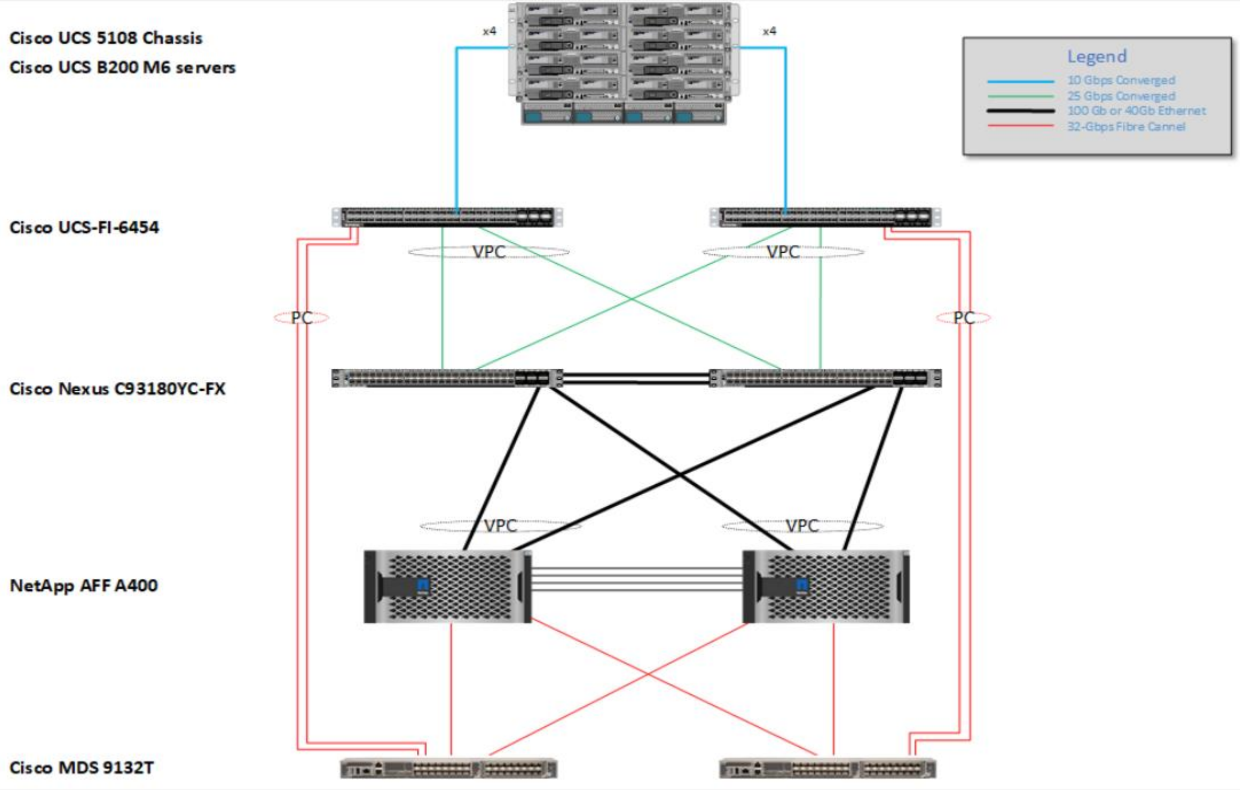
The following are some typical use cases:

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

Physical Topology

Figure 2 illustrates the physical architecture.

Figure 2. Physical Architecture



The reference hardware configuration includes:

- Two Cisco Nexus 93180YC-FX switches
- Two Cisco MDS 9132T 32GB Fibre Channel switches
- Two Cisco UCS 6454 Fabric Interconnects
- Eight Cisco UCS B200 M6 Blade Servers (for VDI workload)
- Infrastructure VMs for VDI were housed on an external cluster
- One NetApp AFF A400 Storage System (HA Pair)
- Two NetApp NS224 Disk Shelves

For desktop virtualization, the deployment includes Citrix Virtual Apps and Desktops Remote Desktop Session Hosts (RDSH) Sessions and Win 10 virtual desktops running on VMware vSphere 7.03.

The design is intended to provide a large-scale building block for Citrix Virtual Apps and Desktops Remote Desktop Session Hosted (RDSH) Sessions workloads consisting of Remote Desktops Server Hosted (RDSH) sessions with Windows Server 2019 hosted shared desktop sessions and Windows 10 non-persistent and persistent hosted desktops in the following:

- 2500 Random Hosted Shared (RDSH) Server 2019 user sessions with Microsoft Office 2016 (Citrix Provisioning Server)
- 1700 Random Pooled Windows 10 Desktops with Microsoft Office 2016 (Citrix Provisioning Server)
- 1700 Static Full Copy Windows 10 Desktops with Microsoft Office 2016 (MCS Full Clone virtual machines)

The data provided in this document will allow our customers to adjust the mix of Remote Desktop Server Hosted (RDSH) Sessions and Win 10 Virtual Desktops to suit their environment. For example, additional blade servers and chassis can be deployed to increase compute capacity, additional disk shelves can be deployed 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 detailed steps for deploying the base architecture. This procedure explains everything from physical cabling to network, compute, and storage device configurations.

Configuration Guidelines

This Cisco Validated Design provides details for deploying a fully redundant, highly available 2500 seats workload virtual sessions /desktop solution with VMware on a FlexPod Datacenter architecture. Configuration guidelines are provided that refer the reader to which redundant component is being configured with each step. For example, storage controller 01 and storage controller 02 are used to identify the two AFF A400 storage controllers that are provisioned with this document, Cisco Nexus A or Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured, and Cisco MDS A or Cisco MDS B identifies the pair of Cisco MDS switches that are configured.

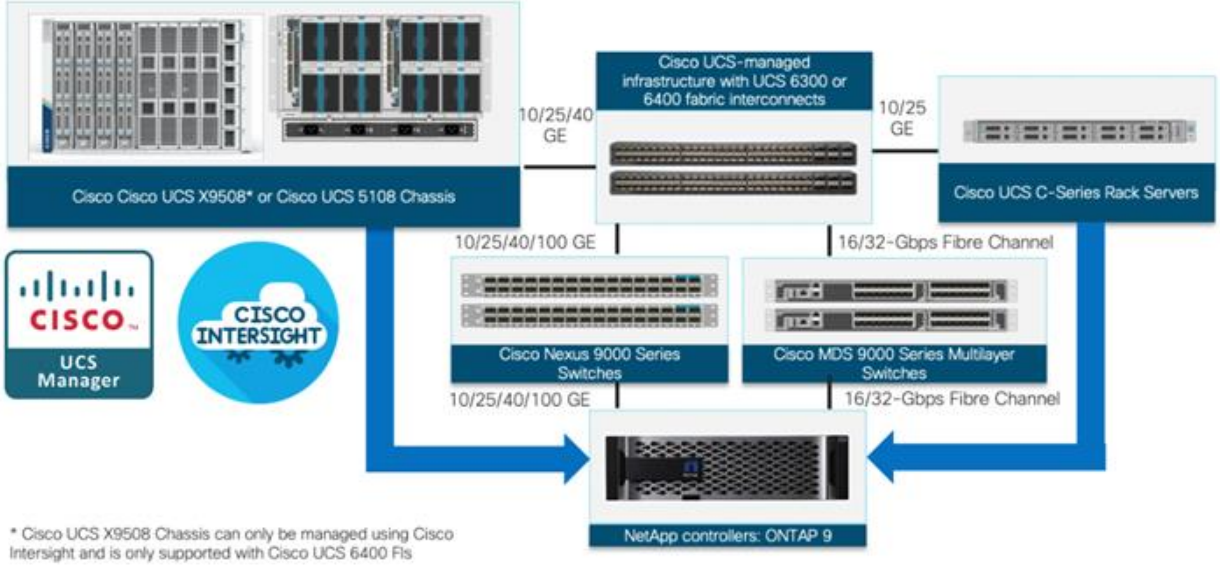
The Cisco UCS 6454 Fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-RDSH-01, VM-Host-VDI-01 and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure.

What is FlexPod?

FlexPod is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. VMware vSphere built on FlexPod includes NetApp AFF storage, Cisco Nexus networking, Cisco MDS storage networking, the Cisco Unified Computing System (Cisco UCS), and VMware vSphere software in a single package. The design is flexible enough that the networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations of this kind.

One benefit of the FlexPod architecture is the ability to customize or " flex" the environment to suit a customer's requirements. A FlexPod can easily be scaled as requirements and demand change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding more FlexPod units). The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of a Fibre Channel and IP-based storage solution. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it truly is a wire-once architecture.

Figure 3. FlexPod Component Families


Cisco UCS-managed infrastructure with UCS 6300 or 6400 fabric interconnects
10/25/40 GE
10/25 GE
Cisco Cisco UCS X9508* or Cisco UCS 5108 Chassis
Cisco UCS C-Series Rack Servers
10/25/40/100 GE
16/32-Gbps Fibre Channel
CISCO UCS Manager
CISCO INTERSIGHT
Cisco Nexus 9000 Series Switches
Cisco MDS 9000 Series Multilayer Switches
10/25/40/100 GE
16/32-Gbps Fibre Channel
NetApp controllers: ONTAP 9
* Cisco UCS X9508 Chassis can only be managed using Cisco Intersight and is only supported with Cisco UCS 6400 FIs

The following lists the benefits of FlexPod:

- Consistent Performance and Scalability
  - Consistent sub-millisecond latency with 100% flash storage
  - Consolidate 100's of enterprise-class applications in a single rack
  - Scales easily, without disruption
  - Continuous growth through multiple FlexPod CI deployments
- Operational Simplicity
  - Fully tested, validated, and documented for rapid deployment
  - Reduced management complexity
  - Auto-aligned 512B architecture removes storage alignment issues
  - No storage tuning or tiers necessary
- Lowest TCO
  - Dramatic savings in power, cooling, and space with 100 percent Flash
  - Industry leading data reduction
- Enterprise-Grade Resiliency
  - Highly available architecture with no single point of failure
  - Nondisruptive operations with no downtime
  - Upgrade and expand without downtime or performance loss
  - Native data protection: snapshots and replication
  - Suitable for even large resource-intensive workloads such as real-time analytics or heavy transactional databases

Technology Overview

This chapter contains the following:

- Cisco Unified Computing System

Cisco Unified Computing System

This subject contains the following:

- Cisco UCS Differentiators
- Cisco Intersight
- Cisco Intersight

Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that integrates computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce total cost of ownership and increase business agility. The system integrates a low-latency, lossless 10-100 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform with a unified management domain for managing all resources.

Cisco Unified Computing System consists of the following subsystems:

- **Compute** - The compute piece of the system incorporates servers based on the Second-Generation Intel Xeon Scalable processors. Servers are available in blade and rack form factor, managed by Cisco Intersight.
- **Network** - The integrated network fabric in the system provides a low-latency, lossless, 10/25/40/100 Gbps Ethernet fabric. Networks for LAN, SAN and management access are consolidated within the fabric. The unified fabric uses the innovative Single Connect technology to lowers costs by reducing the number of network adapters, switches, and cables. This in turn lowers the power and cooling needs of the system.
- **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 virtual environments to support evolving business needs.
- **Storage access** – Cisco UCS system provides consolidated access to both SAN storage and Network Attached Storage over the unified fabric. This provides customers with storage choices and investment protection. Also, the server administrators can pre-assign storage-access policies to storage resources, for simplified storage connectivity and management leading to increased productivity.
- **Management:** The system uniquely integrates compute, network, and storage access subsystems, enabling it to be managed as a single entity through Cisco Intersight software. Cisco Intersight increases IT staff productivity by enabling storage, network, and server administrators to collaborate on Service Profiles that define the desired physical configurations and infrastructure policies for applications. Service Profiles increase business agility by enabling IT to automate and provision resources in minutes instead of days.

Cisco UCS Differentiators

Cisco Unified Computing System is revolutionizing the way servers are managed in the datacenter. The following are the unique differentiators of Cisco Unified Computing System and Cisco Intersight:

- **Embedded Management** – In Cisco UCS, the servers are managed by the embedded firmware in the Fabric Interconnects, eliminating the need for any external physical or virtual devices to manage the servers.
- **Unified Fabric** – In Cisco UCS, from blade server chassis or rack servers to FI, there is a single Ethernet cable used for LAN, SAN, and management traffic. This converged I/O results in reduced cables, SFPs and adapters - reducing capital and operational expenses of the overall solution.
- **Auto Discovery** – By simply inserting the blade server in the chassis or connecting the rack server to the fabric interconnect, discovery and inventory of compute resources occurs automatically without any management intervention. The combination of unified fabric and auto-discovery enables the wire-once architecture of Cisco UCS, where compute capability of Cisco UCS can be extended easily while keeping the existing external connectivity to LAN, SAN, and management networks.
- **Policy Based Resource Classification** – Once Cisco Intersight discovers a compute resource, it can be automatically classified to a given resource pool based on policies defined. This capability is useful in multi-tenant cloud computing. This CVD highlights the policy-based resource classification of Cisco Intersight.
- **Combined Rack and Blade Server Management** – Cisco Intersight can manage Cisco UCS B-series blade servers and Cisco UCS C-series rack servers under the same Cisco UCS domain. This feature, along with stateless computing makes compute resources truly hardware form factor agnostic.
- **Model based Management Architecture** – The Cisco Intersight architecture and management database is model based, and data driven. An open XML API is provided to operate on the management model. This enables easy and scalable integration of Cisco Intersight with other management systems.
- **Policies, Pools, Templates** – The management approach in Cisco Intersight is based on defining policies, pools, and templates, instead of cluttered configuration, which enables a simple, loosely coupled, data driven approach in managing compute, network, and storage resources.
- **Loose Referential Integrity** – In Cisco Intersight, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each other. This provides great flexibility where different experts from different domains, such as network, storage, security, server, and virtualization work together to accomplish a complex task.
- **Policy Resolution** – In Cisco Intersight, a tree structure of organizational unit hierarchy can be created that mimics the real-life tenants and/or organization relationships. Various policies, pools and templates can be defined at different levels of organization hierarchy. A policy referring to another policy by name is resolved in the organizational hierarchy with closest policy match. If no policy with specific name is found in the hierarchy of the root organization, then the special policy named "default" is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibility to owners of different organizations.
- **Service Profiles and Stateless Computing** – A service profile is a logical representation of a server, carrying its various identities and policies. This logical server can be assigned to any physical compute resource as far as it meets the resource requirements. Stateless computing enables procurement of a server within minutes, which used to take days in legacy server management systems.
- **Built-in Multi-Tenancy Support** – The combination of policies, pools and templates, loose referential integrity, policy resolution in the organizational hierarchy and a service profiles-based approach to

compute resources makes Cisco Intersight inherently friendly to multi-tenant environments typically observed in private and public clouds.

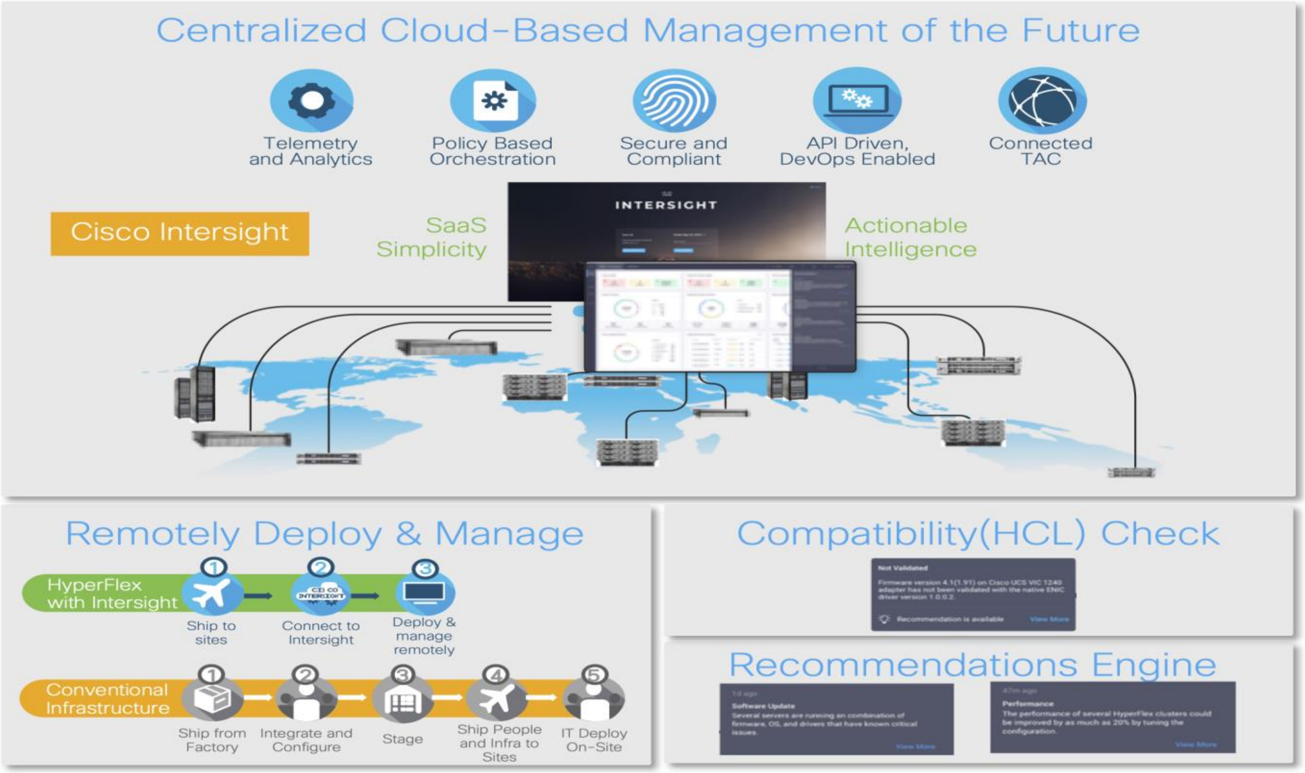
- **Extended Memory** – The enterprise-class Cisco UCS Blade server extends the capabilities of the Cisco Unified Computing System portfolio in a half-width blade form factor. It harnesses the power of the latest Intel Xeon Scalable Series processor family CPUs and Intel Optane DC Persistent Memory (DCPMM) with up to 18 TB of RAM (using 256GB DDR4 DIMMs and 512GB DCPMM).
- **Simplified QoS** – Even though Fibre Channel and Ethernet are converged in the Cisco UCS fabric, built-in support for QoS and lossless Ethernet makes it seamless. Network Quality of Service (QoS) is simplified in Cisco Intersight by representing all system classes in one GUI panel.

Cisco Intersight

Cisco Intersight is a lifecycle management platform for your infrastructure, regardless of where it resides. In your enterprise data center, at the edge, in remote and branch offices, at retail and industrial sites–all these locations present unique management challenges and have typically required separate tools. Cisco Intersight Software as a Service (SaaS) unifies and simplifies your experience of the Cisco Unified Computing System (Cisco UCS).

Intersight software delivers a new level of cloud-powered intelligence that supports lifecycle management with continuous improvement. It is tightly integrated with the Cisco Technical Assistance Center (TAC). Expertise and information flow seamlessly between Cisco Intersight and IT teams, providing global management of Cisco infrastructure, anywhere. Remediation and problem resolution are supported with automated upload of error logs for rapid root-cause analysis.

Figure 4. Cisco Intersight



Not Validated

Firmware version 4.1(1.91) on Cisco UCS VIC 1240 adapter has not been validated with the native ENIC driver version 1.0.0.2.

Recommendation is available

1 d ago

Software Update

Several servers are running an combination of firmware, OS, and drivers that have known critical issues.

47m ago

Performance

The performance of several HyperFlex clusters could be improved by as much as 20% by tuning the configuration.

- Automate your infrastructure

  Cisco has a strong track record for management solutions that deliver policy-based automation to daily operations. Intersight SaaS is a natural evolution of our strategies. Cisco designed Cisco UCS to be 100 percent programmable. Cisco Intersight simply moves the control plane from the network into the cloud. Now you can manage your Cisco UCS infrastructure wherever it resides through a single interface.

- Deploy your way

  If you need to control how your management data is handled, comply with data locality regulations, or consolidate the number of outbound connections from servers, you can use the Cisco Intersight Virtual Appliance for an on-premises experience. Cisco Intersight Virtual Appliance is continuously updated just like the SaaS version, so regardless of which approach you implement, you never have to worry about whether your management software is up to date.

- DevOps ready

  If you are implementing DevOps practices, you can use the Cisco Intersight API with either the cloud-based or virtual appliance offering. Through the API you can configure and manage infrastructure as code—you are not merely configuring an abstraction layer; you are managing the real thing. Through the API and support of cloud-based RESTful API, Terraform providers, Microsoft PowerShell scripts, or Python software, you can automate the deployment of settings and software for both physical and virtual layers. Using the API, you can simplify infrastructure lifecycle operations and increase the speed of continuous application delivery.

- Pervasive simplicity
  - Simplify the user experience by managing your infrastructure regardless of where it is installed.
  - Automate updates to Cisco UCS Data Platform software, reducing complexity and manual efforts.
- Actionable intelligence
  - Use best practices to enable faster, proactive IT operations.
  - Gain actionable insight for ongoing improvement and problem avoidance.
- Manage anywhere
  - Deploy in the data center and at the edge with massive scale.
  - Get visibility into the health and inventory detail for your Intersight Managed environment on-the-go with the Cisco Intersight Mobile App.

For more information about Cisco Intersight and the different deployment options, go to: Cisco Intersight – Manage your systems anywhere.

Solution Components

This chapter contains the following:

- Cisco UCS Fabric Interconnect
- Cisco UCS B200 M6 Blade Server
- Cisco Switches
- Cisco Intersight
- Citrix Virtual App and Desktops 7 2203 LTSR
- Citrix Cloud
- NetApp A-Series All Flash FAS
- VMware vSphere 7.0
- Cisco Intersight Assist Device Connector for VMware vCenter and NetApp ONTAP
- ONTAP Tools for VMware vSphere
- NetApp NFS Plug-in for VMware VAAI
- NetApp SnapCenter Plug-In for VMware vSphere
- NetApp Active IQ Unified Manager 9.10P1
- NetApp XCP File Analytics

Cisco UCS Fabric Interconnect

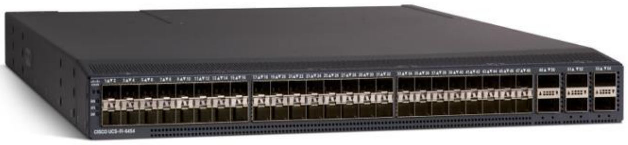
The Cisco UCS Fabric Interconnect (FI) is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. Depending on the model chosen, the Cisco UCS Fabric Interconnect offers line-rate, low-latency, lossless 10 Gigabit, 25 Gigabit, 40 Gigabit, or 100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE) and Fibre Channel connectivity. Cisco UCS Fabric Interconnects provide the management and communication backbone for the Cisco UCS C-Series, S-Series and HX-Series Rack-Mount Servers, Cisco UCS B-Series Blade Servers, and Cisco UCS 5100 Series Blade Server Chassis. All servers and chassis, and therefore all blades, attached to the Cisco UCS Fabric Interconnects become part of a single, highly available management domain. In addition, by supporting unified fabrics, the Cisco UCS Fabric Interconnects provide both the LAN and SAN connectivity for all servers within its domain.

For networking performance, the Cisco UCS 6454 Series uses a cut-through architecture, supporting deterministic, low latency, line rate 10/25/40/100 Gigabit Ethernet ports, 3.82 Tbps of switching capacity, and 320 Gbps bandwidth per Cisco 5108 blade chassis when connected through the IOM 2408 model. The product family supports Cisco low-latency, lossless 10/25/40/100 Gigabit Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over the Ethernet fabric from the servers to the uplinks. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

Cisco UCS 6454 Fabric Interconnect

The Cisco UCS 6454 Fabric Interconnect is a one-rack-unit (1RU) 10/25/40/100 Gigabit Ethernet, FCoE and Fiber Channel switch offering up to 3.82 Tbps throughput and up to 54 ports. The switch has eight (8) 10/25-Gbps fixed Ethernet ports, which can optionally be configured as 8/16/32-Gbps FC ports (ports 1 to 8), thirty-six (36) 10/25-Gbps fixed Ethernet ports (ports 9 to 44), four (4) 1/10/25-Gbps Ethernet ports (ports 45 to 48), and finally six (6) 40/100-Gbps Ethernet uplink ports (ports 49 to 54). For more information , refer to the Cisco UCS 6454 Fabric Interconnect spec sheet: (https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/6400-specsheet.pdf

Figure 5. **Cisco UCS 6454 Fabric Interconnect**

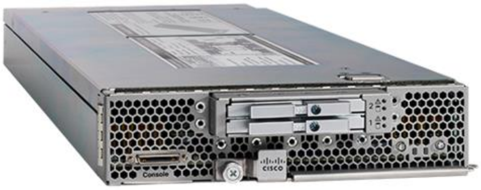


Cisco UCS B200 M6 Blade Server

The Cisco UCS B200 M6 Blade Server delivers performance, flexibility, and optimization for deployments in data centers, in the cloud, and at remote sites. This enterprise-class server offers market-leading performance, versatility, and density without compromise for workloads, including Virtual Desktop Infrastructure (VDI), web infrastructure, distributed databases, converged infrastructure, and enterprise applications such as Oracle and SAP HANA. The Cisco UCS B200 M6 blade server can quickly deploy stateless physical and virtual workloads through programmable, easy-to-use Cisco Intersight and Cisco Intersight and simplified server access through Cisco SingleConnect technology. It includes:

- 3rd Gen Intel Xeon Scalable and processors with up to 40 cores per socket
- Up to 32 DDR4 DIMMs for improved performance with up to 16 DIMM slots ready for Intel Optane PMem
- Up to 2 Small Form-Factor (SFF) drives or up to 4 M.2 SATA drives
- Up to 80 Gbps of I/O throughput

Figure 6. **Cisco UCS B200 M6 Blade Server**



Cisco UCS VIC 1440 mLOM Interface Card

The Cisco UCS VIC 1440 mLOM Interface Card is a quad-port Enhanced Small Form-Factor Pluggable (SFP+) 10/25/40-Gbps Ethernet, and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter installed in the Cisco UCS C-Series Rack Servers. The Cisco UCS VIC 1440 mLOM is used in conjunction with the Cisco UCS 6454 model Fabric Interconnects. The mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases. The card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host, each dynamically configured as either a network interface card (NICs) or host bus adapter (HBA). The personality of the interfaces is set programmatically using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and Worldwide Name [WWN]), failover policy, adapter settings, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all specified using the service profile.

Figure 7. **Cisco UCS VIC 1440 mLOM Interface Card**

Cisco Switches

Cisco Nexus 93180YC-FX Switches

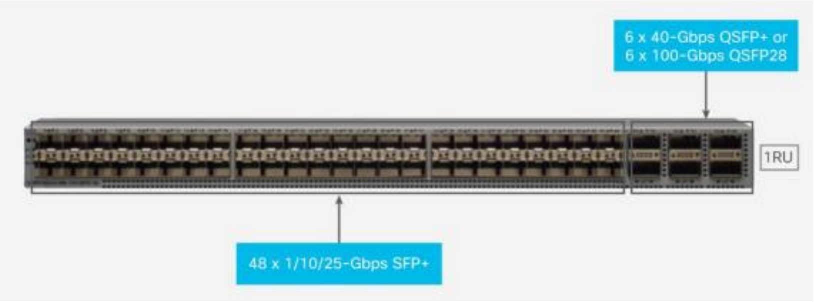
The 93180YC-FX Switch provides a flexible line-rate Layer 2 and Layer 3 feature set in a compact form factor. Designed with Cisco Cloud Scale technology, it supports highly scalable cloud architectures. With the option to operate in Cisco NX-OS or Application Centric Infrastructure (ACI) mode, it can be deployed across enterprise, service provider, and Web 2.0 data centers.

- Architectural Flexibility
    - Includes top-of-rack or middle-of-row fiber-based server access connectivity for traditional and leaf-spine architectures
    - Leaf node support for Cisco ACI architecture is provided in the roadmap
    - Increase scale and simplify management through Cisco Nexus 2000 Fabric Extender support
- Feature Rich
    - Enhanced Cisco NX-OS Software is designed for performance, resiliency, scalability, manageability, and programmability
    - ACI-ready infrastructure helps users take advantage of automated policy-based systems management
    - Virtual Extensible LAN (VXLAN) routing provides network services
    - 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
- Highly Available and Efficient Design
    - High-density, non-blocking architecture
    - Easily deployed into either a hot-aisle and cold-aisle configuration
    - Redundant, hot-swappable power supplies and fan trays
- Simplified Operations
    - Power-On Auto Provisioning (POAP) support allows for simplified software upgrades and configuration file installation
    - An intelligent API offers switch management through remote procedure calls (RPCs, JSON, or XML) over a HTTP/HTTPS infrastructure
    - Python Scripting for programmatic access to the switch command-line interface (CLI)
    - Hot and cold patching, and online diagnostics
- Investment Protection

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

- 1.8 Tbps of bandwidth in a 1 RU form factor
- 48 fixed 1/10/25-Gbe SFP+ ports
- 6 fixed 40/100-Gbe QSFP+ for uplink connectivity
- Latency of less than 2 microseconds
- Front-to-back or back-to-front airflow configurations
- 1+1 redundant hot-swappable 80 Plus Platinum-certified power supplies
- Hot swappable 3+1 redundant fan trays

Figure 8. Cisco Nexus 93180YC-FX Switch



Cisco MDS 9132T 32-Gb Fiber Channel Switch

The next-generation Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switch (Figure 9) provides high-speed Fibre Channel connectivity from the server rack to the SAN core. It empowers small, midsize, and large enterprises that are rapidly deploying cloud-scale applications using extremely dense virtualized servers, providing the dual benefits of greater bandwidth and consolidation.

Small-scale SAN architectures can be built from the foundation using this low-cost, low-power, non-blocking, line-rate, and low-latency, bi-directional airflow capable, fixed standalone SAN switch connecting both storage and host ports.

Medium-size to large-scale SAN architectures built with SAN core directors can expand 32-Gb connectivity to the server rack using these switches either in switch mode or Network Port Virtualization (NPV) mode.

Additionally, investing in this switch for the lower-speed (4- or 8- or 16-Gb) server rack gives you the option to upgrade to 32-Gb server connectivity in the future using the 32-Gb Host Bus Adapter (HBA) that are available today. The Cisco MDS 9132T 32-Gb 32-Port Fibre Channel switch also provides unmatched flexibility through a unique port expansion module (Figure 9) that provides a robust cost-effective, field swappable, port upgrade option.

This switch also offers state-of-the-art SAN analytics and telemetry capabilities that have been built into this next-generation hardware platform. This new state-of-the-art technology couples the next-generation port ASIC with a fully dedicated Network Processing Unit designed to complete analytics calculations in real time. The telemetry data extracted from the inspection of the frame headers are calculated on board (within the switch) and, using an industry-leading open format, can be streamed to any analytics-visualization platform. This switch also includes a dedicated 10/100/1000BASE-T telemetry port to maximize data delivery to any telemetry receiver including Cisco Data Center Network Manager.

Figure 9. Cisco MDS 9132T 32-Gb 32-Port Fabric Channel Switch

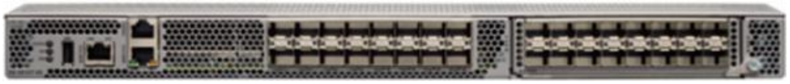
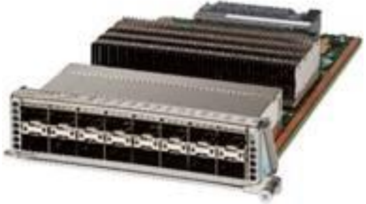


Figure 10. Cisco MDS 9132T 32-Gb 16-Port Fibre Channel Port Expansion Module



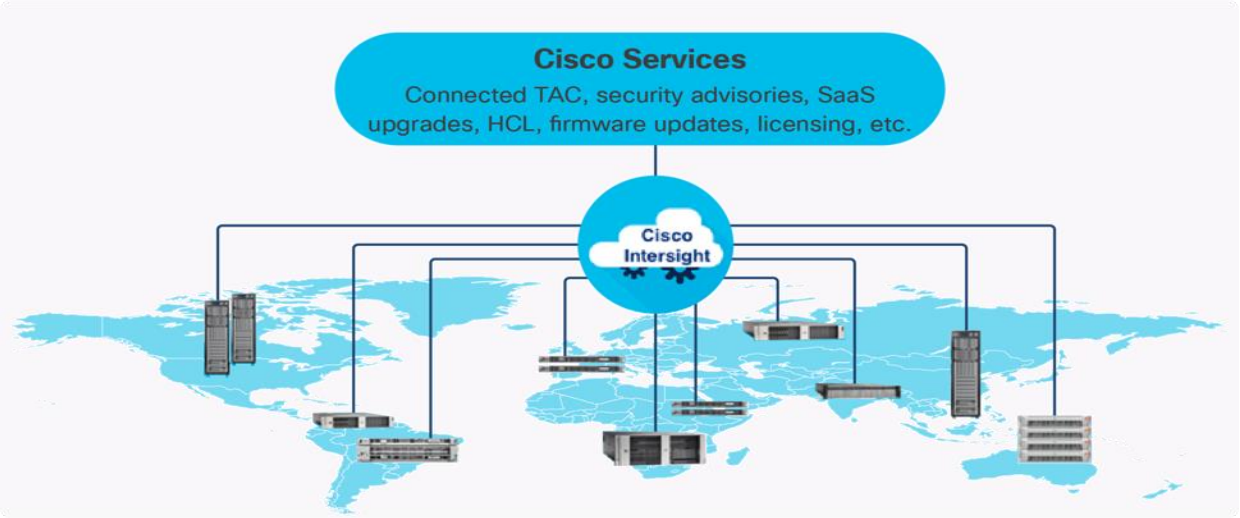
- Features
  - High performance: MDS 9132T architecture, with chip-integrated nonblocking arbitration, provides consistent 32-Gb low-latency performance across all traffic conditions for every Fibre Channel port on the switch.
  - Capital Expenditure (CapEx) savings: The 32-Gb ports allow users to deploy them on existing 16- or 8-Gb transceivers, reducing initial CapEx with an option to upgrade to 32-Gb transceivers and adapters in the future.
  - High availability: MDS 9132T switches continue to provide the same outstanding availability and reliability as the previous-generation Cisco MDS 9000 Family switches by providing optional redundancy on all major components such as the power supply and fan. Dual power supplies also facilitate redundant power grids.
  - Pay-as-you-grow: The MDS 9132T Fibre Channel switch provides an option to deploy as few as eight 32-Gb Fibre Channel ports in the entry-level variant, which can grow by 8 ports to 16 ports, and thereafter with a port expansion module with sixteen 32-Gb ports, to up to 32 ports. This approach results in lower initial investment and power consumption for entry-level configurations of up to 16 ports compared to a fully loaded switch. Upgrading through an expansion module also reduces the overhead of managing multiple instances of port activation licenses on the switch. This unique combination of port upgrade options allow four possible configurations of 8 ports, 16 ports, 24 ports and 32 ports.
  - Next-generation Application-Specific Integrated Circuit (ASIC): The MDS 9132T Fibre Channel switch is powered by the same high-performance 32-Gb Cisco ASIC with an integrated network processor that powers the Cisco MDS 9700 48-Port 32-Gb Fibre Channel Switching Module. Among all the advanced features that this ASIC enables, one of the most notable is inspection of Fibre Channel and Small Computer System Interface (SCSI) headers at wire speed on every flow in the smallest form-factor Fibre Channel switch without the need for any external taps or appliances. The recorded flows can be analyzed on the switch and also exported using a dedicated 10/100/1000BASE-T port for telemetry and analytics purposes.
  - Intelligent network services: Slow-drain detection and isolation, VSAN technology, Access Control Lists (ACLs) for hardware-based intelligent frame processing, smart zoning, and fabric wide Quality of Service (QoS) enable migration from SAN islands to enterprise-wide storage networks. Traffic encryption is optionally available to meet stringent security requirements.
  - Sophisticated diagnostics: The MDS 9132T provides intelligent diagnostics tools such as Inter-Switch Link (ISL) diagnostics, read diagnostic parameters, protocol decoding, network analysis tools, and integrated Cisco Call Home capability for greater reliability, faster problem resolution, and reduced service costs.

    - Virtual machine awareness: The MDS 9132T provides visibility into all virtual machines logged into the fabric. This feature is available through HBAs capable of priority tagging the Virtual Machine Identifier (VMID) on every FC frame. Virtual machine awareness can be extended to intelligent fabric services such as analytics[1] to visualize performance of every flow originating from each virtual machine in the fabric.
    - Programmable fabric: The MDS 9132T provides powerful Representational State Transfer (REST) and Cisco NX-API capabilities to enable flexible and rapid programming of utilities for the SAN as well as polling point-in-time telemetry data from any external tool.
    - Single-pane management: The MDS 9132T can be provisioned, managed, monitored, and troubleshot using Cisco Data Center Network Manager (DCNM), which currently manages the entire suite of Cisco data center products.
    - Self-contained advanced anticounterfeiting technology: The MDS 9132T uses on-board hardware that protects the entire system from malicious attacks by securing access to critical components such as the bootloader, system image loader and Joint Test Action Group (JTAG) interface.
- Cisco DCNM-SAN
    - Cisco DCNM-SAN can be used to monitor, configure, and analyze Cisco 32Gbps Fibre Channel fabrics and show information about the Cisco Nexus switching fabric. Cisco DCNM-SAN is deployed as a virtual appliance from an OVA and is managed through a web browser. Once the Cisco MDS and Nexus switches are added with the appropriate credentials and licensing, monitoring of the SAN and Ethernet fabrics can begin. Additionally, VSANs, device aliases, zones, and zone sets can be added, modified, and deleted using the DCNM point-and-click interface. Device Manager can also be used to configure the Cisco MDS switches. SAN Analytics can be added to Cisco MDS switches to provide insights into the fabric by allowing customers to monitor, analyze, identify, and troubleshoot performance issues.
- Cisco DCNM integration with Cisco Intersight
    - The Cisco Network Insights Base (Cisco NI Base) application provides several TAC assist functionalities which are useful when working with Cisco TAC. The Cisco NI Base app collects the CPU, device name, device product id, serial number, version, memory, device type, and disk usage information for the nodes in the fabric. Cisco NI Base application is connected to the Cisco Intersight cloud portal through a device connector which is embedded in the management controller of the Cisco DCNM platform. The device connector provides a secure way for connected Cisco DCNM to send and receive information from the Cisco Intersight portal, using a secure Internet connection.

Cisco Intersight

The Cisco Intersight platform is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. The Cisco Intersight platform is designed to be modular, so customers can adopt services based on their individual requirements. The platform significantly simplifies IT operations by bridging applications with infrastructure, providing visibility and management from bare-metal servers and hypervisors to serverless applications, thereby reducing costs and mitigating risk. This unified SaaS platform uses a unified Open API design that natively integrates with third-party platforms and tools.

Figure 11. **Cisco Intersight Overview**


Cisco Services
Connected TAC, security advisories, SaaS upgrades, HCL, firmware updates, licensing, etc.
Cisco Intersight

The main benefits of Cisco Intersight infrastructure services are as follows:

- Simplify daily operations by automating many daily manual tasks
- Combine the convenience of a SaaS platform with the capability to connect from anywhere and manage infrastructure through a browser or mobile app
- Stay ahead of problems and accelerate trouble resolution through advanced support capabilities
- Gain global visibility of infrastructure health and status along with advanced management and support capabilities
- Upgrade to add workload optimization and Kubernetes services when needed

Cisco Intersight Virtual Appliance and Private Virtual Appliance

In addition to the SaaS deployment model running on Intersight.com, on-premises options can be purchased separately. The Cisco Intersight Virtual Appliance and Cisco Intersight Private Virtual Appliance are available for organizations that have additional data locality or security requirements for managing systems. The Cisco Intersight Virtual Appliance delivers the management features of the Cisco Intersight platform in an easy-to-deploy VMware Open Virtualization Appliance (OVA) or Microsoft Hyper-V Server virtual machine that allows you to control the system details that leave your premises. The Cisco Intersight Private Virtual Appliance is provided in a form factor specifically designed for users who operate in disconnected (air gap) environments. The Private Virtual Appliance requires no connection to public networks or back to Cisco to operate.

Cisco Intersight Assist

Cisco Intersight Assist helps customers add endpoint devices to Cisco Intersight. A data center could have multiple devices that do not connect directly with Cisco Intersight. Any device that is supported by Cisco Intersight, but does not connect directly with it, will need a connection mechanism. Cisco Intersight Assist provides that connection mechanism. In FlexPod, VMware vCenter and NetApp Active IQ Unified Manager connect to Intersight with the help of Intersight Assist VM.

Cisco Intersight Assist is available within the Cisco Intersight Virtual Appliance, which is distributed as a deployable virtual machine contained within an Open Virtual Appliance (OVA) file format. More details about the Cisco Intersight Assist VM deployment configuration is covered in later sections.

Licensing Requirements

The Cisco Intersight platform uses a subscription-based license with multiple tiers. Customers can purchase a subscription duration of one, three, or five years and choose the required Cisco UCS server volume tier for the selected subscription duration. Each Cisco endpoint automatically includes a Cisco Intersight Base license at no additional cost when customers access the Cisco Intersight portal and claim a device. Customers can purchase any of the following higher-tier Cisco Intersight licenses using the Cisco ordering tool:

- **Cisco Intersight Essentials:** Essentials includes all the functions of the Base license plus additional features, including Cisco UCS Central Software and Cisco Integrated Management Controller (IMC) supervisor entitlement, policy-based configuration with server profiles, firmware management, and evaluation of compatibility with the Cisco Hardware Compatibility List (HCL).
- **Cisco Intersight Advantage:** Advantage offers all the features and functions of the Base and Essentials tiers. It includes storage widgets and cross-domain inventory correlation across compute, storage, and virtual environments (VMWare ESXi). It also includes OS installation for supported Cisco UCS platforms.
- **Cisco Intersight Premier:** In addition to all of the functions provided in the Advantage tier, Premier includes full subscription entitlement for Intersight Orchestrator, which provides orchestration across Cisco UCS and third-party systems.
    - Servers in the Cisco Intersight managed mode require at least the Essentials license. For more information about the features provided in the various licensing tiers, go to: https://intersight.com/help/getting_started#licensing_requirements

Citrix Virtual App and Desktops 7 2203 LTSR

The virtual app and desktop solution designed for an exceptional experience.

Today's employees spend more time than ever working remotely, causing companies to rethink how IT services should be delivered. To modernize infrastructure and maximize efficiency, many are turning to desktop as a service (DaaS) to enhance their physical desktop strategy, or they are updating on-premises virtual desktop infrastructure (VDI) deployments. Managed in the cloud, these deployments are high-performance virtual instances of desktops and apps that can be delivered from any datacenter or public cloud provider.

DaaS and VDI capabilities provide corporate data protection as well as an easily accessible hybrid work solution for employees. Because all data is stored securely in the cloud or datacenter, rather than on devices, end-users can work securely from anywhere, on any device, and over any network—all with a fully IT-provided experience. IT also gains the benefit of centralized management, so they can scale their environments quickly and easily. By separating endpoints and corporate data, resources stay protected even if the devices are compromised.

As a leading VDI and DaaS provider, Citrix provides the capabilities organizations need for deploying virtual apps and desktops to reduce downtime, increase security, and alleviate the many challenges associated with traditional desktop management.

Citrix Cloud

Citrix Cloud is a platform that hosts and administers Citrix cloud services. It connects to your resources through connectors on any cloud or infrastructure you choose (on-premises, public cloud, private cloud, or hybrid cloud). It allows you to create, manage, and deploy workspaces with apps and data to your end-users from a single console.

Note: This CVD provides a disaster recovery solution with Citrix Cloud and Microsoft Azure.

NetApp A-Series All Flash FAS

Powered by NetApp ONTAP data management software, NetApp AFF A-Series systems (NetApp AFF) deliver the industry's highest performance, superior flexibility, and best-in-class data services and cloud integration to help you accelerate, manage, and protect business-critical data across your hybrid cloud. It is a robust scale-out platform built for virtualized environments, combining low-latency performance with best-in-class data management, built-in efficiencies, integrated data protection, multiprotocol support, and nondisruptive operations. Deploy as a stand-alone system or as a high-performance tier in a NetApp ONTAP configuration.

A wide range of organizations, from enterprise to midsize businesses, rely on NetApp AFF A-Series to:

- Simplify operations with seamless data management, on the premises and in the cloud.
- Accelerate traditional and new-generation applications.
- Keep business-critical data available, protected, and secure.
- Accelerates applications and future-proofs your infrastructure

In the modern data center, IT is charged with driving maximum performance for business-critical workloads, scaling without disruption as the business grows, and enabling the business to take on new data-driven initiatives. NetApp AFF A-Series systems handle all of it with ease.

The NetApp AFF A-Series lineup includes the A250, A400, A700, A800 and A900. These controllers and their technical specifications are listed in Table 1. For more information about the A-Series AFF controllers, see:

http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx

https://hwu.netapp.com/Controller/Index?platformTypeId=5265148

Table 1. NetApp AFF Technical Specifications

Specifications	AFF A250	AFF A400	AFF A800	AFF A900
Maximum scale-out	2-24 nodes (12 HA pair)	2-24 nodes (12 HA pair)	2-24 nodes (12 HA pair)	2-24 nodes (12 HA pair)
Maximum SSDs	576	5760	2880	5760
Max effective capacity	35PB	702.7PB	316.3PB	702.7PB
Controller form factor	2U	4U	4U with 48 SSD slots	8U
PCIe expansion slots	4	10	8	20
FC target ports (32Gb autoranging)	16	24	32	64
FC target ports (16Gb autoranging)	n/a	32(with FC mezzanine card)	32	64
FCoE target ports, UTA2	n/a	n/a	n/a	64

Specifications	AFF A250	AFF A400	AFF A800	AFF A900
100GbE ports (40GbE autoranging)	4	16	20	32
25GbE ports (10GbE autoranging)	20	16	16	64
10GbE ports	n/a	32	32	64
12Gb/6Gb SAS ports	8	32	n/a	64
Storage networking supported	NVMe/TCP, NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB, Amazon s3	NVMe/RDMA, NVMe/TCP, NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB, Amazon s3	NVMe/RDMA, NVMe/TCP, NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB, Amazon s3	NVMe/TCP, NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB, Amazon s3
OS version	ONTAP 9.8 RC1 or later	ONTAP 9.7 RC1 or later	ONTAP 9.7 RC1 or later	ONTAP 9.10.1 RC2 or later

Below are few advantages of NetApp AFF:

- Maximum performance for your most demanding applications

  NetApp AFF A-Series systems deliver industry-leading performance proven by SPC-1 and SPEC SFS industry benchmarks, making them ideal for demanding, highly transactional applications such as Oracle, Microsoft SQL Server, MongoDB databases, VDI, and server virtualization.

  With the power of front-end NVMe/FC and NVMe/TCP host connectivity and back-end NVMe-attached SSDs, our high-end AFF A900 systems deliver latency as low as 100µs. Based on a high-resiliency design, the A900 also delivers high RAS and enables non-disruptive in-chassis upgrade from its predecessor A700. The A800 delivers high performance in a compact form factor and is especially suited for EDA and Media and Entertainment workloads. The midrange, most versatile NetApp AFF A400 system features hardware acceleration technology that significantly enhances performance and storage efficiency. And our entry-level, budget-friendly NetApp AFF A250, provides 40% more performance and 33% more efficiency at no extra cost compared with its predecessor.

  NetApp AFF A-Series also lets you:

  - Drive mission-critical SAN workloads with symmetric active-active host connectivity for continuous availability and instant failover.
  - Consolidate workloads to deliver up to 14.4 million IOPS at 1ms latency in a cluster with a truly unified scale-out architecture. Built-in adaptive quality of service (QoS) safeguards SLAs in multi-workload and multitenant environments.
  - Manage massively scalable NAS containers of up to 20PB and 400 billion files with a single namespace.
  - Improve the speed and productivity of collaboration across multiple locations and increase data throughput for read-intensive applications with NetApp FlexCache software.
  - Modernize with advanced connectivity

NetApp AFF A-Series all-flash systems deliver industry-leading performance, density, scalability, security, and network connectivity. As the first enterprise-grade storage systems to support both NVMe/TCP and NVMe/FC, NetApp AFF A-Series systems boost performance with modern network connectivity. With NVMe/TCP, which uses the commonly available Ethernet infrastructure, you don't have to invest in new hardware to take advantage of the faster host connectivity. With NVMe/FC, you can get twice the IOPS and cut application response time in half compared with traditional FC. These systems support a range of ecosystems, including VMware, Microsoft Windows 10, and Linux, with storage path failover. For most customers, integrating NVMe/FC into an existing SAN is a simple, nondisruptive software upgrade.

- Scale without disruption

  With NetApp AFF A-Series, you can integrate new technologies and private or public cloud into your infrastructure nondisruptively. NetApp AFF A-Series is the only all-flash array that enables you to combine different controllers, SSD sizes, and new technologies so that your investment is protected. The NVMe-based AFF systems also support SAS SSDs, maximizing the flexibility and cost effectiveness of your upgrade:

  ◦ Best balance between price, technology, features, and performance.

  ◦ Increase operational efficiency

    IT departments are striving to make budgets go further and to allow IT staff to focus on new value-added projects rather than on day-to-day IT management. NetApp AFF systems simplify IT operations, which therefore reduces data center cost. In particular, our entry-level system, the NetApp AFF A250, delivers best-in-class performance and efficiency to mid-size business customers so they can consolidate more workloads and eliminate silos.

- Provision storage in minutes

  NetApp AFF systems offer broad application ecosystem support and deep integration for enterprise applications, virtual desktop infrastructure (VDI), database, and server virtualization, supporting Oracle, Microsoft SQL Server, VMware, SAP, MySQL, and more. You can quickly provision storage in less than 10 minutes with NetApp ONTAP System Manager. In addition, infrastructure management tools simplify and automate common storage tasks so you can:

  ◦ Easily provision and rebalance workloads by monitoring clusters and nodes.

  ◦ Use one-click automation and self-service for provisioning and data protection.

  ◦ Upgrade OS and firmware with a single-click

  ◦ Import LUNs from third-party storage arrays directly into an AFF system to seamlessly migrate data.

  Additionally, the NetApp Active IQ Digital Advisor engine enables you to optimize your NetApp systems with predictive analytics and proactive support. Fueled by the massive NetApp user base, AI and machine learning create actionable insights that help you prevent problems, optimize your configuration, save time, and make smarter decisions.

- Achieve outstanding storage savings

  NetApp employs various capabilities to promote optimal capacity savings and to drive down your TCO. AFF A-Series system's support for solid-state drives (SSDs) with multistream write technology, combined with advanced SSD partitioning, provides maximum usable capacity, regardless of the type of data that you store. Thin provisioning; NetApp Snapshot copies; and inline data reduction features, such as deduplication, compression, and compaction, provide substantial additional space savings—without affecting performance—enabling you to purchase the least amount of storage capacity possible.

- Build your hybrid cloud with ease

  Your data fabric built by NetApp helps you simplify and integrate data management across cloud and on-premises environments to meet business demands and gain a competitive edge. With AFF A-Series, you can connect to more clouds for more data services, data tiering, caching, and disaster recovery. You can also:

  - Maximize performance and reduce overall storage costs by automatically tiering cold data to the cloud with FabricPool.
  - Instantly deliver data to support efficient collaboration across your hybrid cloud
  - Protect your data by taking advantage of Amazon Simple Storage Service (Amazon S3) cloud resources—on premises and in the public cloud.
  - Accelerate read performance for data that is shared widely throughout your organization and across hybrid cloud deployments.
  - Keep data available, protected, and secure

  As organizations become more data driven, the business impact of data loss can be increasingly dramatic—and costly. IT must protect data from both internal and external threats, ensure data availability, eliminate maintenance disruptions, and quickly recover from failures.

- Integrated data protection

  AFF A-Series systems come with a full suite of acclaimed NetApp integrated and application-consistent data protection software. Key capabilities include:

- Native space efficiency with cloning and NetApp Snapshot copies reduce storage costs and minimize performance impact. Up to 1,023 copies are supported.
- NetApp SnapCenter software provides application-consistent data protection and clone management to simplify application management.
- NetApp SnapMirror technology replicates to any NetApp FAS or AFF system on the premises or in the cloud, reducing overall system costs.
- Business continuity and fast disaster recovery

  With AFF, you can maintain constant data availability with zero data loss and zero downtime. NetApp MetroCluster software provides synchronous replication to protect your entire system, and NetApp SnapMirror Business Continuity provides a more flexible, cost-effective business continuity to even with more granular replication of selected critical data.

- Security everywhere

  Flexible encryption and key management help guard your sensitive data on the premises, in the cloud, and in transit. The market-leading anti-ransomware protection for both preemption and post-attack recovery safeguards your critical data from ransomware attacks and can prevent catastrophic financial consequences. With the simple and efficient security solutions, you can:

  - Achieve FIPS 140-2 compliance (Level 1 and Level 2) with self-encrypting drives and use any type of drives with software-based encryption.
  - Meet governance, risk, and compliance requirements with security features such as secure purge; logging and auditing monitors; and write once, read many (WORM) file locking.
  - Protect against threats with multifactor authentication, role-based access control, secure multitenancy, and storage-level file security.

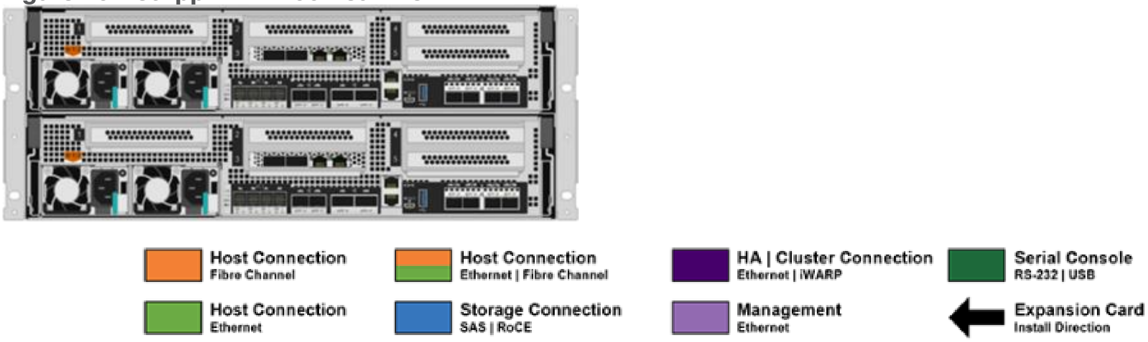
NetApp AFF A400

The NetApp AFF A400 offers full end-to-end NVMe support. The frontend NVMe/FC connectivity makes it possible to achieve optimal performance from an all-flash array for workloads that include artificial intelligence, machine learning, and real-time analytics as well as business-critical databases. On the back end, the A400 supports both serial-attached SCSI (SAS) and NVMe-attached SSDs, offering the versatility for current customers to move up from their legacy A-Series systems and satisfying the increasing interest that all customers have in NVMe-based storage.

The NetApp AFF A400 offers greater port availability, network connectivity, and expandability. The NetApp AFF A400 has 10 PCIe Gen3 slots per high availability pair. The NetApp AFF A400 offers 25GbE or 100GbE, as well as 32Gb/FC and NVMe/FC network connectivity. This model was created to keep up with changing business needs and performance and workload requirements by merging the latest technology for data acceleration and ultra-low latency in an end-to-end NVMe storage system.

Figure 15.NetApp AFF A400 Front View

Figure 16.NetApp AFF A400 Rear View



Note: We used 4 port 32Gb FC HBA on slot 1 (1a,1b, other two ports unused) for front-end FC SAN connection, 4x25Gb Ethernet NICs on slot 0 (e0e, e0f, e0g, e0h) for NAS connectivity, 2x100Gb ethernet ports on slot 3 (e3a, e3b) used for cluster interconnect, 2x25Gb ethernet on slot 0 (e0a, e0b) used for Node HA interconnect, 2x100Gb ethernet on slot 0 (e0c, e0d) and 2x100Gb ethernet on slot 5 (e5a, e5b) are used for backend NVMe storage connectivity.

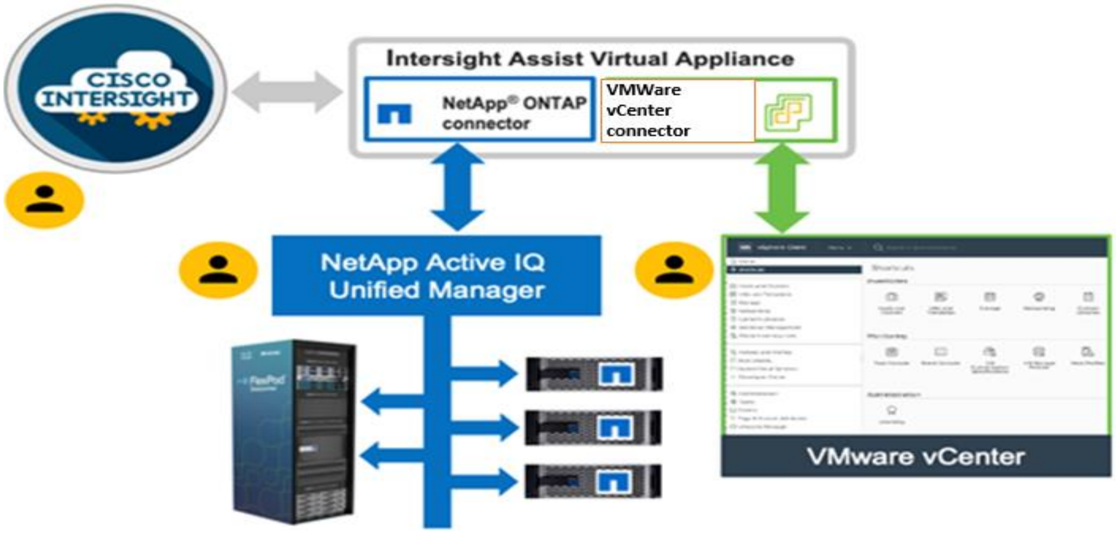
NetApp ONTAP 9

NetApp storage systems harness the power of ONTAP to simplify the data infrastructure from edge, core, and cloud with a common set of data services and 99.9999 percent availability. NetApp ONTAP 9 data management software from NetApp enables customers to modernize their infrastructure and transition to a cloud-ready data center. ONTAP 9 has a host of features to simplify deployment and data management, accelerate and protect critical data, and make infrastructure future-ready across hybrid-cloud architectures.

NetApp ONTAP 9 is the data management software that is used with the NetApp AFF A400 all-flash storage system in this solution design. ONTAP software offers secure unified storage for applications that read and write data over block- or file-access protocol storage configurations. These storage configurations range from high-speed flash to lower-priced spinning media or cloud-based object storage. ONTAP implementations can run on NetApp engineered AFF,FAS or ASA series arrays and in private, public, or hybrid clouds (NetApp Private Storage and NetApp Cloud Volumes ONTAP). Specialized implementations offer best-in-class converged infrastructure, featured here as part of the FlexPod Datacenter solution or with access to third-party storage arrays (NetApp FlexArray virtualization). Together these implementations form the basic framework of the NetApp Data Fabric, with a common software-defined approach to data management, and fast efficient replication across systems. FlexPod and ONTAP architectures can serve as the foundation for both hybrid cloud and private cloud designs.

Read more about all the capabilities of ONTAP data management software here: https://www.netapp.com/us/products/data-management-software/ontap.aspx.

Figure 17.Cisco Intersight and vCenter/NetApp Integration



NetApp ONTAP 9.10.1P1

ONTAP Features for VDI

The following are the ONTAP features for VDI:

- Secure Multi-Tenancy—Tenants can be in overlapping subnet or can use identical IP subnet range.
- Multi-Protocol—Same storage system can be used for Block/File/Object storage demands.
- FlexGroup Volumes—High performance and massive capacity (~20PB and ~40 billion files) for file shares and for hosting VDI pools.
- FlexCache—Enables Single Global Namespace can be consumed around the clouds or multi-site.
- File System Analytics—Fast query to file metadata on the SMB file share.
- Ease of management with vCenter Plugins—Best practices are validated and implemented while provisioning. Supports VAAI and VASA for fast provisioning and storage capability awareness.
- SnapCenter integration with vCenter—Space efficient data protection with snapshots and FlexClones.
- Automation support—Supports RESTapi, has modules for Ansible, PowerShell, and so on.

- Storage Efficiency—Supports inline dedupe, compression, thin provisioning, etc. Guaranteed dedupe of 8:1 for VDI.
- Adaptive QoS—Adjusts QoS setting based on space consumption.
- ActiveIQ Unified Manager—Application based storage provisioning, Performance Monitoring, End-End storage visibility diagrams.

Storage Efficiency

Storage efficiency has always been a primary architectural design point of ONTAP. A wide array of features allows businesses to store more data using less space. In addition to deduplication and compression, businesses can store their data more efficiently by using features such as unified storage, multi-tenancy, thin provisioning, and NetApp Snapshot technology.

Starting with ONTAP 9, NetApp guarantees that the use of NetApp storage efficiency technologies on AFF systems reduce the total logical capacity used to store customer data by 75 percent, a data reduction ratio of 4:1. This space reduction is a combination of several different technologies, such as deduplication, compression, and compaction, which provide additional reduction to the basic features provided by ONTAP.

Compaction, which is introduced in ONTAP 9, is the latest patented storage efficiency technology released by NetApp. In the NetApp WAFL file system, all I/O takes up 4KB of space, even if it does not actually require 4KB of data. Compaction combines multiple blocks that are not using their full 4KB of space together into one block. This one block can be more efficiently stored on the disk-to-save space. This process is illustrated in Figure 12.

Storage Efficiency Features

The storage efficiency features are as follows:

- Deduplication

  Deduplication reduces the amount of physical storage required for a volume (or all the volumes in an AFF aggregate) by discarding duplicate blocks and replacing them with references to a single shared block. Reads of deduplicated data typically incur no performance charge. Writes incur a negligible charge except on overloaded nodes.

  As data is written during normal use, WAFL uses a batch process to create a catalog of block signatures. After deduplication starts, ONTAP compares the signatures in the catalog to identify duplicate blocks. If a match exists, a byte-by-byte comparison is done to verify that the candidate blocks have not changed since the catalog was created. Only if all the bytes match is the duplicate block discarded and its disk space reclaimed.

- Compression

  Compression reduces the amount of physical storage required for a volume by combining data blocks in compression groups, each of which is stored as a single block. Reads of compressed data are faster than in traditional compression methods because ONTAP decompresses only the compression groups that contain the requested data, not an entire file or LUN.

  You can perform inline or postprocess compression, separately or in combination:

  - Inline compression compresses data in memory before it is written to disk, significantly reducing the amount of write I/O to a volume, but potentially degrading write performance. Performance-intensive operations are deferred until the next postprocess compression operation, if any.
  - Postprocess compression compresses data after it is written to disk, on the same schedule as deduplication.

- Compaction
- Small files or I/O padded with zeros are stored in a 4 KB block whether or not they require 4 KB of physical storage. Inline data compaction combines data chunks that would ordinarily consume multiple 4 KB blocks into a single 4 KB block on disk. Compaction takes place while data is still in memory, so it is best suited to faster controllers

Figure 12. Storage Efficiency Features

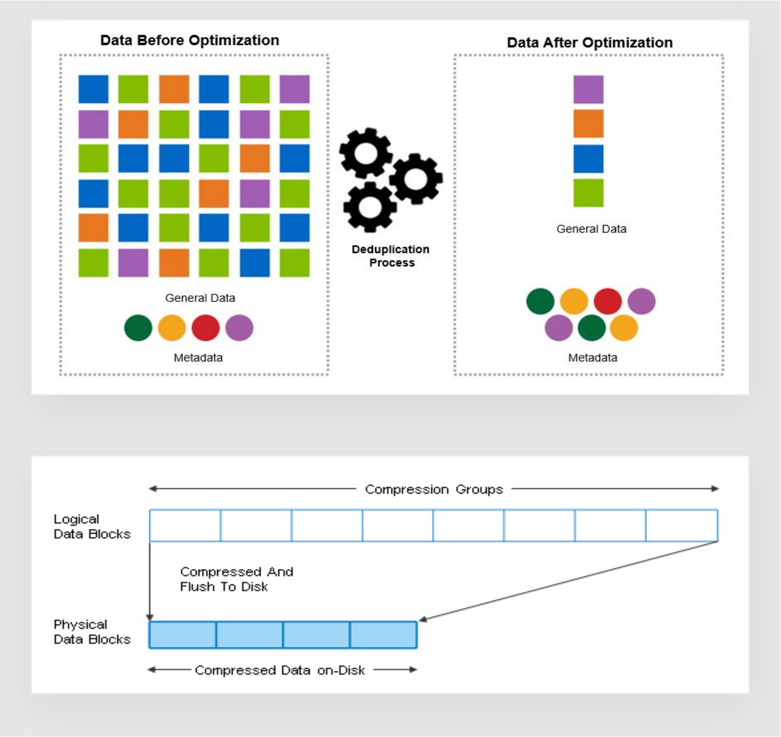
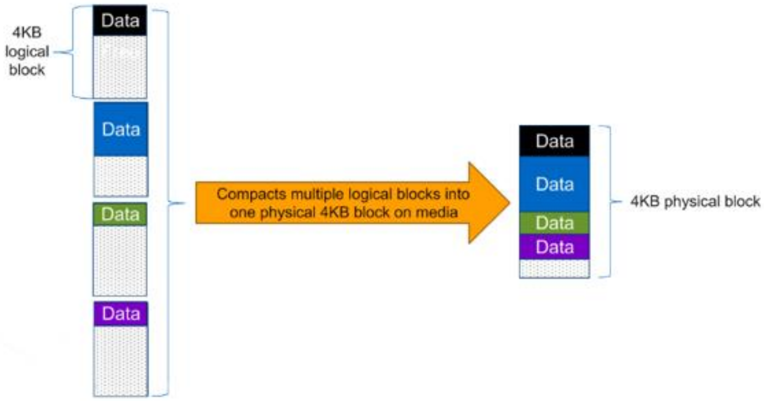
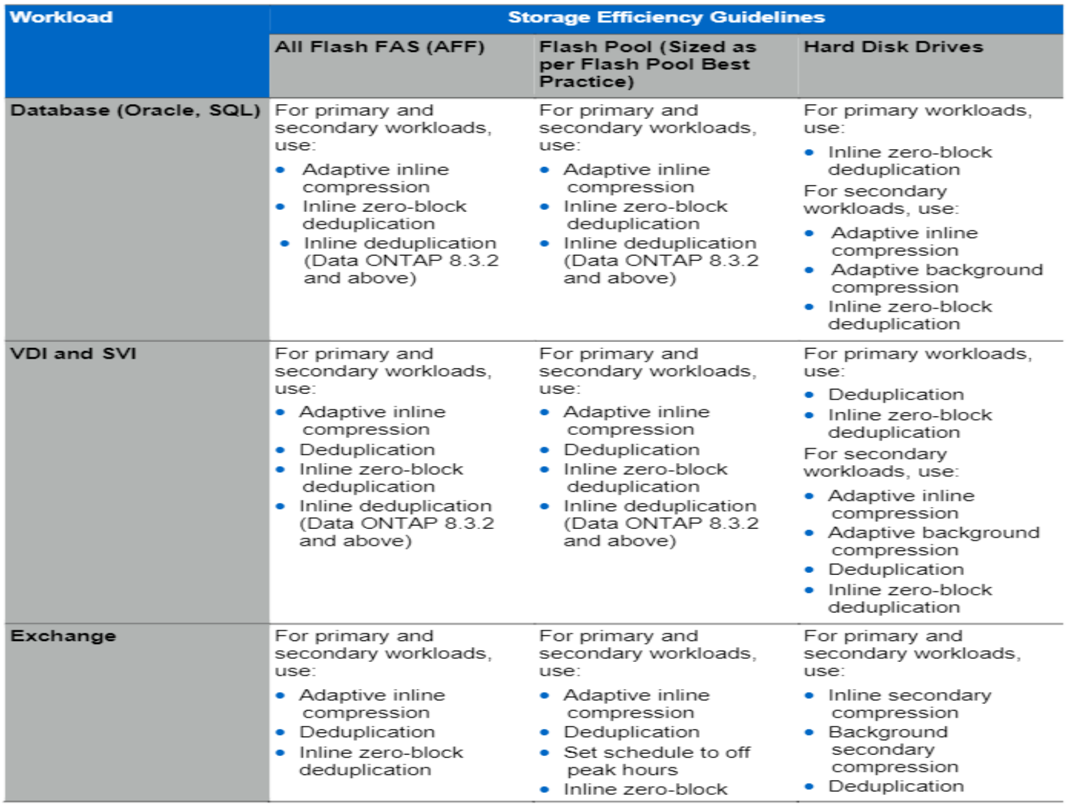


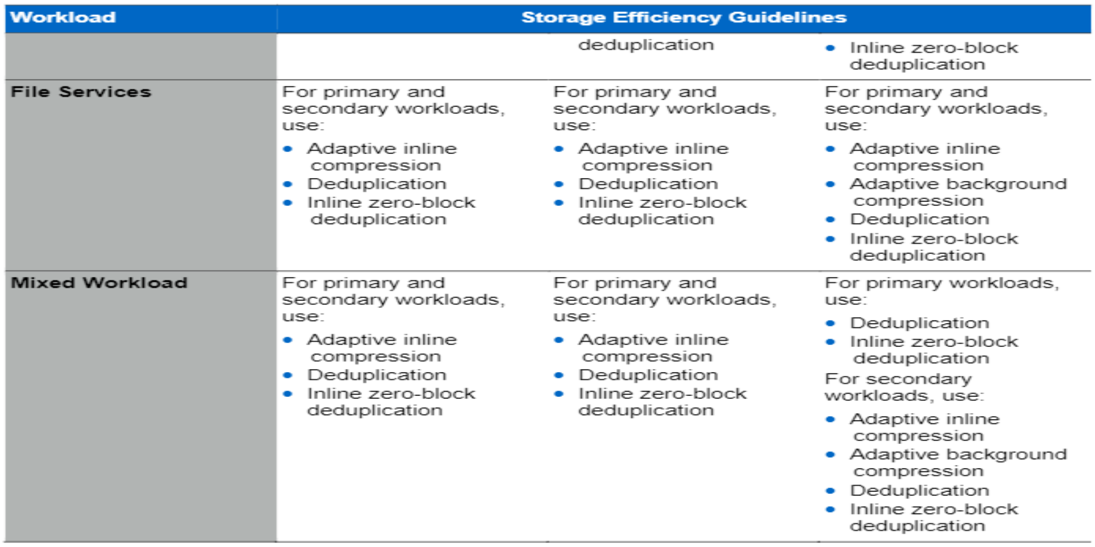
Figure 13. Storage Efficiency


4KB logical block
Data
Data
Data
Data
Compacts multiple logical blocks into one physical 4KB block on media
Data
Data
Data
Data
4KB physical block

Note: Some applications such as Oracle and SQL have unique headers in each of their data blocks that prevent the blocks to be identified as duplicates. So, for such applications, enabling deduplication does not result in significant savings. So, deduplication is not recommended to be enabled for databases. However, NetApp data compression works very well with databases, and we strongly recommend enabling compression for databases. Table 2 lists some guidelines where compression, deduplication and/or inline Zero block deduplication can be used. These are guidelines, not rules; environment may have different performance requirements and specific use cases.

Table 2. Compression and Deduplication Guidelines





Workload	Storage Efficiency Guidelines		
	All Flash FAS (AFF)	Flash Pool (Sized as per Flash Pool Best Practice)	Hard Disk Drives
Database (Oracle, SQL)	For primary and secondary workloads, use: • Adaptive inline compression • Inline zero-block deduplication • Inline deduplication (Data ONTAP 8.3.2 and above)	For primary and secondary workloads, use: • Adaptive inline compression • Inline zero-block deduplication • Inline deduplication (Data ONTAP 8.3.2 and above)	For primary workloads, use: • Inline zero-block deduplication For secondary workloads, use: • Adaptive inline compression • Adaptive background compression • Inline zero-block deduplication
VDI and SVI	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication • Inline deduplication (Data ONTAP 8.3.2 and above)	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication • Inline deduplication (Data ONTAP 8.3.2 and above)	For primary workloads, use: • Deduplication • Inline zero-block deduplication For secondary workloads, use: • Adaptive inline compression • Adaptive background compression • Deduplication • Inline zero-block deduplication
Exchange	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Set schedule to off peak hours • Inline zero-block deduplication	For primary and secondary workloads, use: • Inline secondary compression • Background secondary compression • Deduplication • Inline zero-block deduplication
File Services	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication	For primary and secondary workloads, use: • Adaptive inline compression • Adaptive background compression • Deduplication • Inline zero-block deduplication
Mixed Workload	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication	For primary and secondary workloads, use: • Adaptive inline compression • Deduplication • Inline zero-block deduplication	For primary workloads, use: • Deduplication • Inline zero-block deduplication For secondary workloads, use: • Adaptive inline compression • Adaptive background compression • Deduplication • Inline zero-block deduplication

Space Savings

Table 3 lists the storage efficiency data reduction ratio ranges for different applications. A combination of synthetic datasets and real-world datasets has been used to determine the typical savings ratio range. The savings ratio range mentioned is only indicative.

Table 3. Typical Savings Ratios with ONTAP 9–Sample Savings Achieved with Internal and Customer Testing

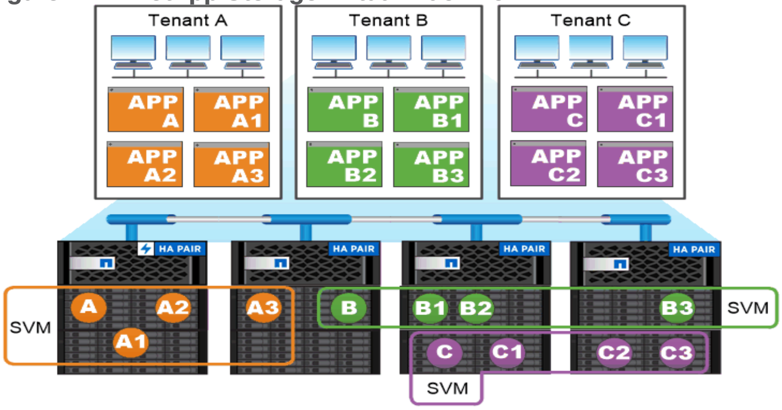
Typical Savings Ratios with ONTAP 9	
Workload [with deduplication, data compaction, adaptive compression and FlexClone volumes (where applicable) technologies]	**Ratio Range**
Home directories	1.5:1.-.2:1
Software development	2:1 - 10:1
VDI Citrix Virtual Apps and Desktops full clone desktops (persistent)	6:1 - 10:1
VDI Citrix Virtual Apps and Desktops linked clone desktops (nonpersistent)	5:1 - 7:1
VDI Citrix Virtual Apps and Desktops Remote Desktop Server Hosted (RDSH) sessions Instant clone desktops (nonpersistent)	6:1 - 10:1
Virtual Servers (OS and Applications)	2:1.-.4:1
Oracle databases (with no database compression)	2.1 - 4:1
SQL 2014 databases (with no database compression)	2.1 - 4:1
Microsoft Exchange	1.6:1
Mongo DB	1.3:1 - 1.5:1
Recompressed data (such as video and image files, audio files, pdfs, and so on)	No Savings

NetApp Storage Virtual Machine (SVM)

An SVM is a logical abstraction that represents the set of physical resources of the cluster. This adds extra security and peace of mind to your VDI environment, giving you another place besides vCenter to apply HA, High Availability. Data volumes and network logical interfaces (LIFs) are created and assigned to an SVM and may reside on any node in the cluster to which the SVM has been given access. An SVM may own resources on multiple nodes concurrently, and those resources can be moved non-disruptively from one node to another. For example, a flexible volume can be non-disruptively moved to a new node and aggregate, or a data LIF can be transparently reassigned to a different physical network port. The SVM abstracts the cluster hardware, and it is not tied to any specific physical hardware.

An SVM can support multiple data protocols concurrently. Volumes within the SVM can be joined together to form a single NAS namespace, which makes all of an SVM's data available through a single share or mount point to create a VMware NFS datastore for your VDI desktop folders. SVMs also support block-based protocols, and LUNs can be created and exported by using iSCSI, FC, or FCoE. Any or all of these data protocols can be configured for use within a given SVM to support your VDI needs.

Figure 14. NetApp Storage Virtual Machine



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

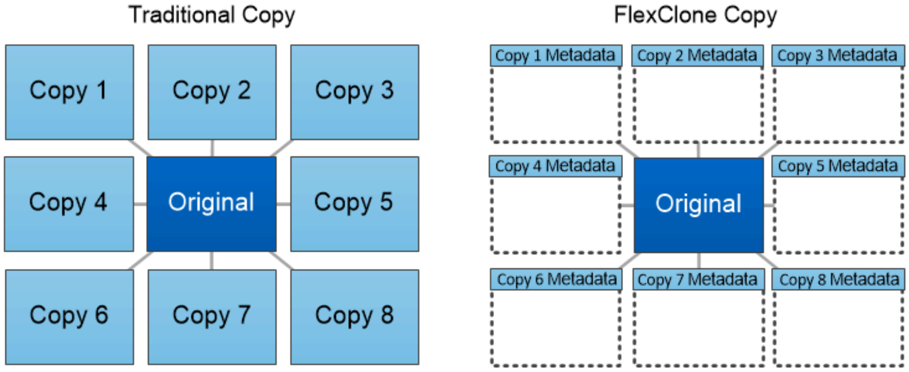
FlexClones

FlexClone technology references Snapshot metadata to create writable, point-in-time copies of a volume. Copies share data blocks with their parents, consuming no storage except what is required for metadata until changes are written to the copy. FlexClone files and FlexClone LUNs use identical technology, except that a backing Snapshot copy is not required.

Where traditional copies can take minutes or even hours to create, FlexClone software lets you copy even the largest datasets almost instantaneously. That makes it ideal for situations in which you need multiple copies of identical datasets (a virtual desktop deployment, for example) or temporary copies of a dataset (testing an application against a production dataset).

You can clone an existing FlexClone volume, clone a volume containing LUN clones, or clone mirror and vault data. You can split a FlexClone volume from its parent, in which case the copy is allocated its own storage.

Figure 15. Traditional Copy vs FlexClone Copy



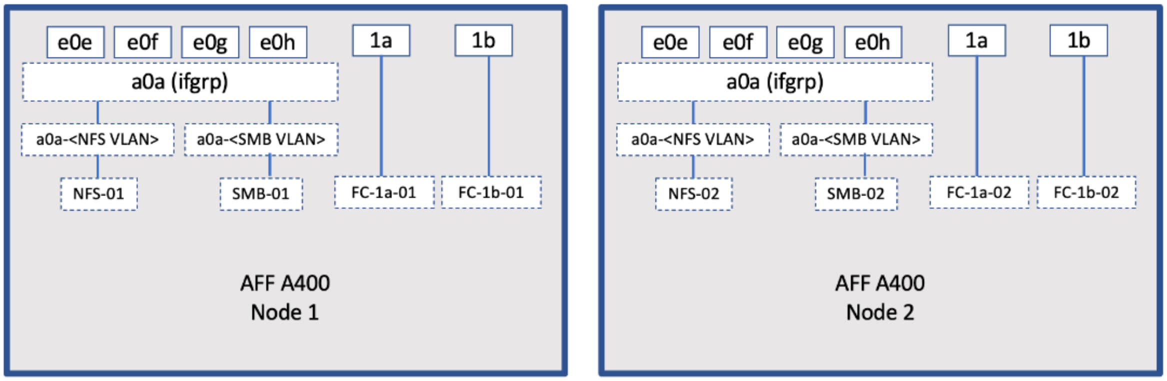
FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

SAN Boot

NetApp recommends implementing SAN boot for Cisco UCS servers in the FlexPod Datacenter solution. Doing so enables the ESXI host to be safely secured by the NetApp All Flash FAS storage system, providing better performance. In this design, FC SAN boot is validated.

In FC SAN boot, each Cisco UCS server boots by connecting the NetApp All Flash FAS storage to the Cisco MDS switch. The 32G FC storage ports, in this example 0g and 0h, are connected to Cisco MDS switch. The FC LIFs are created on the physical ports and each FC LIF is uniquely identified by its target WWPN. The storage system target WWPNs can be zoned with the server initiator WWPNs in the Cisco MDS switches. The FC boot LUN is exposed to the servers through the FC LIF using the MDS switch; this enables only the authorized server to have access to the boot LUN.

Figure 16. FC - SVM ports and LIF layout



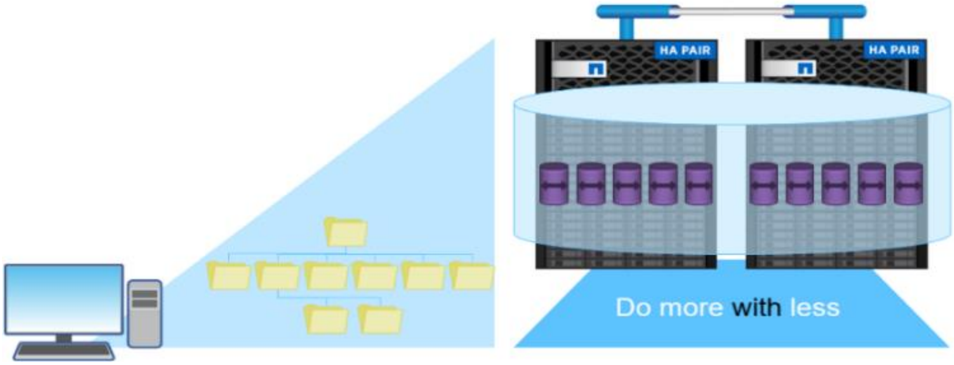
Unlike NAS network interfaces, the SAN network interfaces are not configured to fail over during a failure. Instead if a network interface becomes unavailable, the ESXI host chooses a new optimized path to an available network interface. ALUA is a standard supported by NetApp used to provide information about SCSI targets, which allows a host to identify the best path to the storage.

FlexGroups

ONTAP 9.3 brought an innovation in scale-out NAS file systems: NetApp FlexGroup volumes, which plays a major role to give ONTAP the ability to be scaled nondisruptively out to 24 storage nodes while not degrading the performance of the VDI infrastructure.

With FlexGroup volumes, a storage administrator can easily provision a massive single namespace in a matter of seconds. FlexGroup volumes have virtually no capacity or file count constraints outside of the physical limits of hardware or the total volume limits of ONTAP. Limits are determined by the overall number of constituent member volumes that work in collaboration to dynamically balance load and space allocation evenly across all members. There is no required maintenance or management overhead with a FlexGroup volume. You simply create the FlexGroup volume and share it with your NAS clients. ONTAP does the rest.

Figure 17. NetApp FlexGroups



Storage QoS

Storage QoS (Quality of Service) can help you manage risks around meeting your performance objectives. You use Storage QoS to limit the throughput to workloads and to monitor workload performance. You can reactively limit workloads to address performance problems and you can pro-actively limit workloads to prevent performance problems.

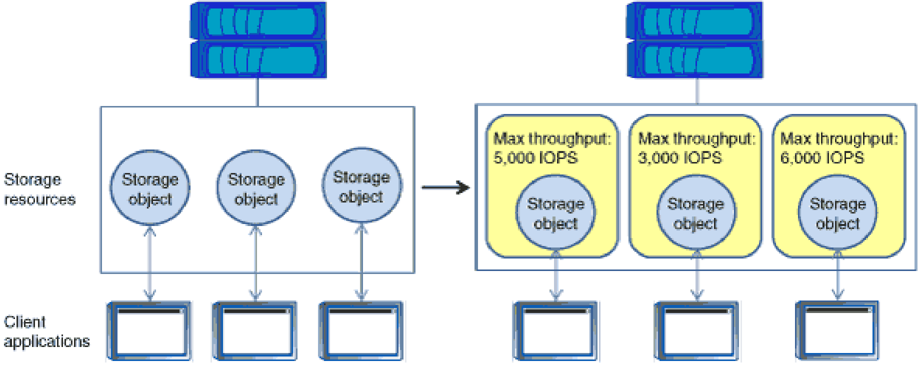
A workload represents the input/output (I/O) operations to one of the following kinds of storage objects:

- FlexVol volumes
- LUNs

You assign a storage object to a policy group to control and monitor a workload. You can monitor workloads without controlling them.

Figure 18 illustrates an example environment before and after using Storage QoS. On the left, workloads compete for cluster resources to transmit I/O. These workloads get " best effort" performance, which means you have less performance predictability (for example, a workload might get such good performance that it negatively impacts other workloads). On the right are the same workloads assigned to policy groups. The policy groups enforce a maximum throughput limit.

Figure 18. Before and After using Storage QoS



NetApp storage quality of service (QoS) works with both SAN and NAS storage, and it runs across the entire NetApp product line from entry to enterprise. Storage QoS offers significant benefits for all types of VDI environments. It lets you:

- Achieve greater levels of consolidation
- Set maximum and minimum limits on multiple VDI workloads that require separate service level agreements (SLAs)
- Add additional workloads with less risk of interference
- Make sure your customers get what they pay for, but not more

Adaptive QoS

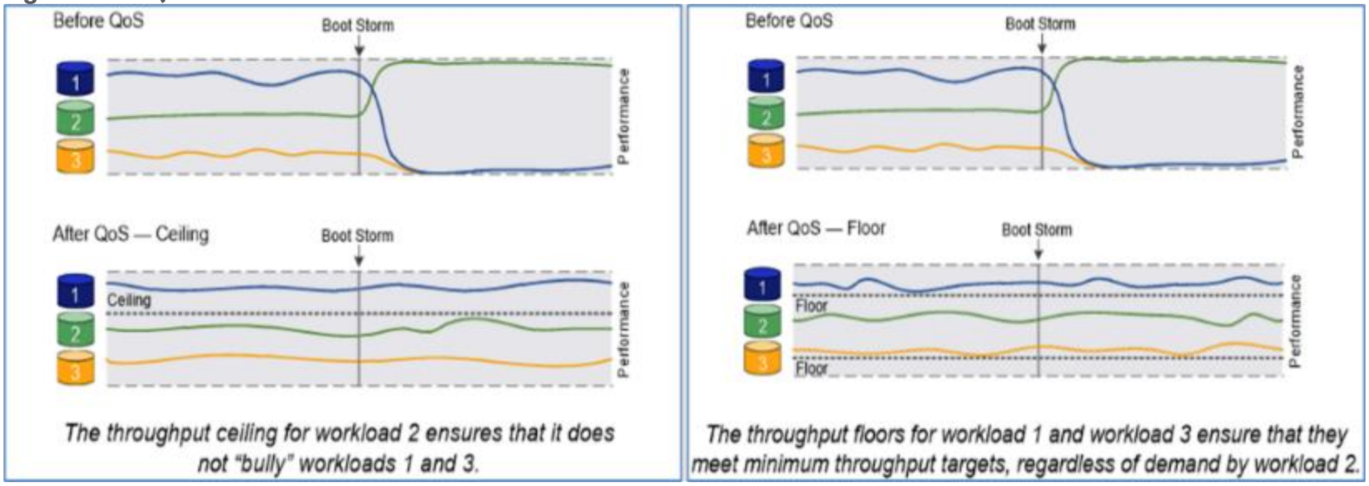
Adaptive QoS automatically scales the policy group (A *policy group* defines the throughput ceiling for one or more workloads) value to workload (*A workload represents the I/O operations for a storage object: a volume, file, qtree or LUN, or all the volumes, files, qtrees, or LUNs in an SVM*) size, for the size of the workload changes. That is a significant advantage when you are managing hundreds or thousands of workloads in a VDI deployment. With Adaptive QoS, Ceiling and Floor limit can be set using allocated or used space. The QoS also address HA and Scaling as it will assist in both efforts to produce a non-disruptive change during VDI growth by maintaining the ratio of IOPS to TBs/GBs. To assist in managing your QOS, Active IQ unified manager will provide QOS suggestions based on historical performance and usage.

Three default adaptive QoS policy groups are available, as listed in Table 4. You can apply these policy groups directly to a volume.

Table 4. Available Default Adaptive QoS Policy Groups

Default Policy Group	Expected IOPS/TB	Peak IOPS/TB	Absolute Min IOPS
extreme	6,144	12,288	1000
performance	2,048	4,096	500
Value	128	512	75

Figure 19. QOS boot storm illustration



The throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.

The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

Security and Data Protection

Vscan

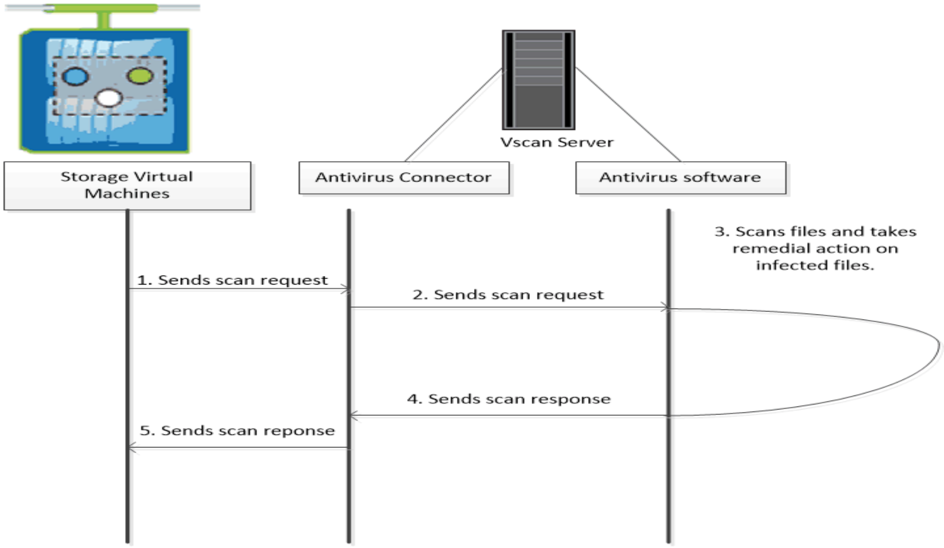
With Vscan you can use integrated antivirus functionality on NetApp storage systems to protect data from being compromised by viruses or other malicious code. NetApp virus scanning, called Vscan, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.

You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over CIFS. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.

You can use *on-demand scanning* to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over CIFS. You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

Typically, you enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.

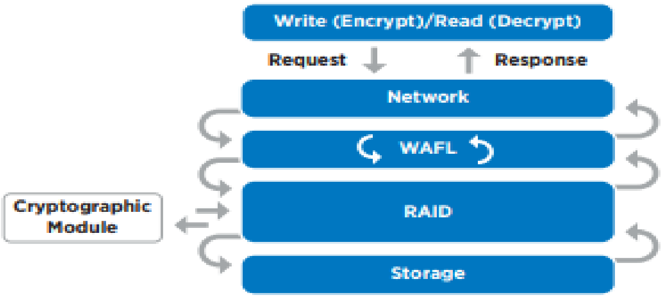


NetApp Volume Encryption(NVE) and NetApp Aggregate Encryption (NAE)

NetApp Volume Encryption is a software-based, data-at-rest encryption solution that is FIPS 140-2 compliant. NVE allows ONTAP to encrypt data for each volume for granularity. NAE, is an outgrowth of NVE; it allows ONTAP to encrypt data for each volume, and the volumes can share keys across the aggregate. NVE and NAE enable you to use storage efficiency features that would be lost with encryption at the application layer. For greater storage efficiency, you can use aggregate deduplication with NAE.

Here's how the process works: The data leaves the disk encrypted, is sent to RAID, is decrypted by the CryptoMod, and is then sent up the rest of the stack. This process is illustrated in Figure 20.

Figure 20. NVE and NAE Process



To view the latest security features for ONTAP 9, go to: Security Features in ONTAP 9 | NetApp.

ONTAP Rest API

ONTAP Rest API enables you to automate the deployment and administration of your ONTAP storage systems using one of several available options. The ONTAP REST API provides the foundation for all the various ONTAP automation technologies.

Beginning with ONTAP 9.6, ONTAP includes an expansive workflow-driven REST API that you can use to automate deployment and management of your storage. In addition, NetApp provides a Python client library, which makes it easier to write robust code, as well as support for ONTAP automation based on Ansible.

AutoSupport and Active IQ Digital Advisor

ONTAP offers artificial intelligence-driven system monitoring and reporting through a web portal and through a mobile app. The AutoSupport component of ONTAP sends telemetry that is analyzed by Active IQ Digital Advisor. Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

The following are some things you can do with Active IQ:

- Plan upgrades. Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.
- View system wellness. Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space.
- Manage performance. Active IQ shows system performance over a longer period than you can see in ONTAP System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Active IQ displays complete inventory and software and hardware configuration information. View when service contracts are expiring to ensure you remain covered.

VMware vSphere 7.0

VMware vSphere is a virtualization platform for holistically managing large collections of infrastructures (resources including CPUs, storage, and networking) as a seamless, versatile, and dynamic operating environment. Unlike traditional operating systems that manage an individual machine, VMware vSphere aggregates the infrastructure of an entire data center to create a single powerhouse with resources that can be allocated quickly and dynamically to any application in need.

VMware vSphere 7.0 has several improvements and simplifications including, but not limited to:

- Fully featured vSphere Client (HTML5) client. (The flash-based vSphere Web Client has been deprecated and is no longer available.)
- Improved Distributed Resource Scheduler (DRS) – a very different approach that results in a much more granular optimization of resources
- Assignable hardware – a new framework that was developed to extend support for vSphere features when customers utilize hardware accelerators
- vSphere Lifecycle Manager – a replacement for VMware Update Manager, bringing a suite of capabilities to make lifecycle operations better
- Refactored vMotion – improved to support today's workloads

For more information about VMware vSphere and its components, see: https://www.vmware.com/products/vsphere.html.

VMware vSphere vCenter

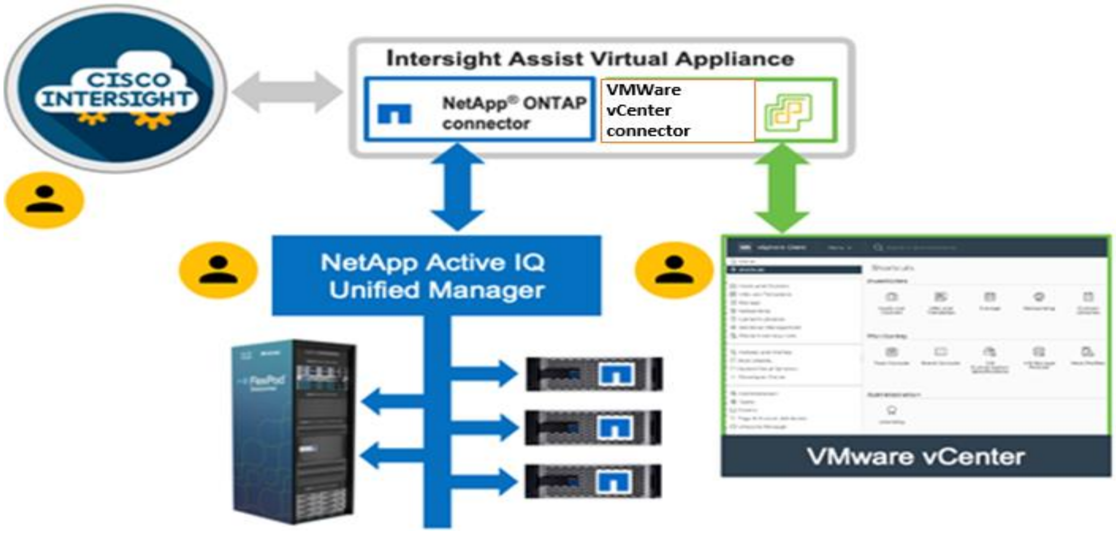
VMware vCenter Server provides unified management of all hosts and VMs from a single console and aggregates performance monitoring of clusters, hosts, and VMs. VMware vCenter Server gives administrators a deep insight into the status and configuration of compute clusters, hosts, VMs, storage, the guest OS, and other critical components of a virtual infrastructure. VMware vCenter manages the rich set of features available in a VMware vSphere environment.

Cisco Intersight Assist Device Connector for VMware vCenter and NetApp ONTAP

Cisco Intersight integrates with VMware vCenter and NetApp storage as follows:

- Cisco Intersight uses the device connector running within Cisco Intersight Assist virtual appliance to communicate with the VMware vCenter.
- Cisco Intersight uses the device connector running within a Cisco Intersight Assist virtual appliance to integrate with NetApp Active IQ Unified Manager. The NetApp AFF A400 should be added to NetApp Active IQ Unified Manager.

Figure 21. Cisco Intersight and vCenter/NetApp Integration



The device connector provides a secure way for connected targets to send information and receive control instructions from the Cisco Intersight portal using a secure internet connection. The integration brings the full value and simplicity of Cisco Intersight infrastructure management service to VMware hypervisor and ONTAP data storage environments.

Enterprise SAN and NAS workloads can benefit equally from the integrated management solution. The integration architecture enables FlexPod customers to use new management capabilities with no compromise in their existing VMware or ONTAP operations. IT users will be able to manage heterogeneous infrastructure from a centralized Cisco Intersight portal. At the same time, the IT staff can continue to use VMware vCenter and NetApp Active IQ Unified Manager for comprehensive analysis, diagnostics, and reporting of virtual and storage environments. The functionality provided through this integration is covered in the upcoming solution design section.

ONTAP Tools for VMware vSphere

NetApp ONTAP tools for VMware vSphere is a unified appliance that includes vSphere Storage Console (VSC),VASA Provider and SRA Provider. This vCenter web client plug-in that provides Context sensitive menu to provision traditional datastores and Virtual Volume (vVol) datastore.

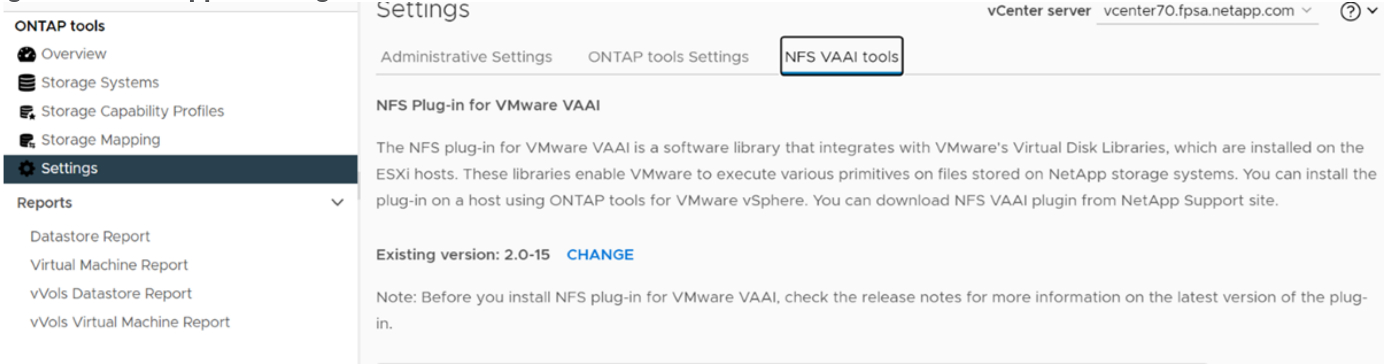
ONTAP tools provides visibility into the NetApp storage environment from within the vSphere web client. VMware administrators can easily perform tasks that improve both server and storage efficiency while still using role-based access control to define the operations that administrators can perform. It includes enhanced REST APIs that provide vVols metrics for SAN storage systems using ONTAP 9.7 and later. So, NetApp OnCommand API Services is no longer required to get metrics for ONTAP systems 9.7 and later.

To download ontap tools for vmware vsphere, go to: https://mysupport.netapp.com/site/products/all/details/otv/downloads-tab.

NetApp NFS Plug-in for VMware VAAI

The NetApp NFS Plug-in for VMware vStorage APIs - Array Integration (VAAI) is a software library that integrates the VMware Virtual Disk Libraries that are installed on the ESXi host. The VMware VAAI package enables the offloading of certain tasks from the physical hosts to the storage array. Performing those tasks at the array level can reduce the workload on the ESXi hosts.

Figure 22. NetApp NFS Plug-in for VMware VAAI



NFS Plug-in for VMware VAAI

The NFS plug-in for VMware VAAI is a software library that integrates with VMware's Virtual Disk Libraries, which are installed on the ESXi hosts. These libraries enable VMware to execute various primitives on files stored on NetApp storage systems. You can install the plug-in on a host using ONTAP tools for VMware vSphere. You can download NFS VAAI plugin from NetApp Support site.

Existing version: 2.0-15

Note: Before you install NFS plug-in for VMware VAAI, check the release notes for more information on the latest version of the plug-in.

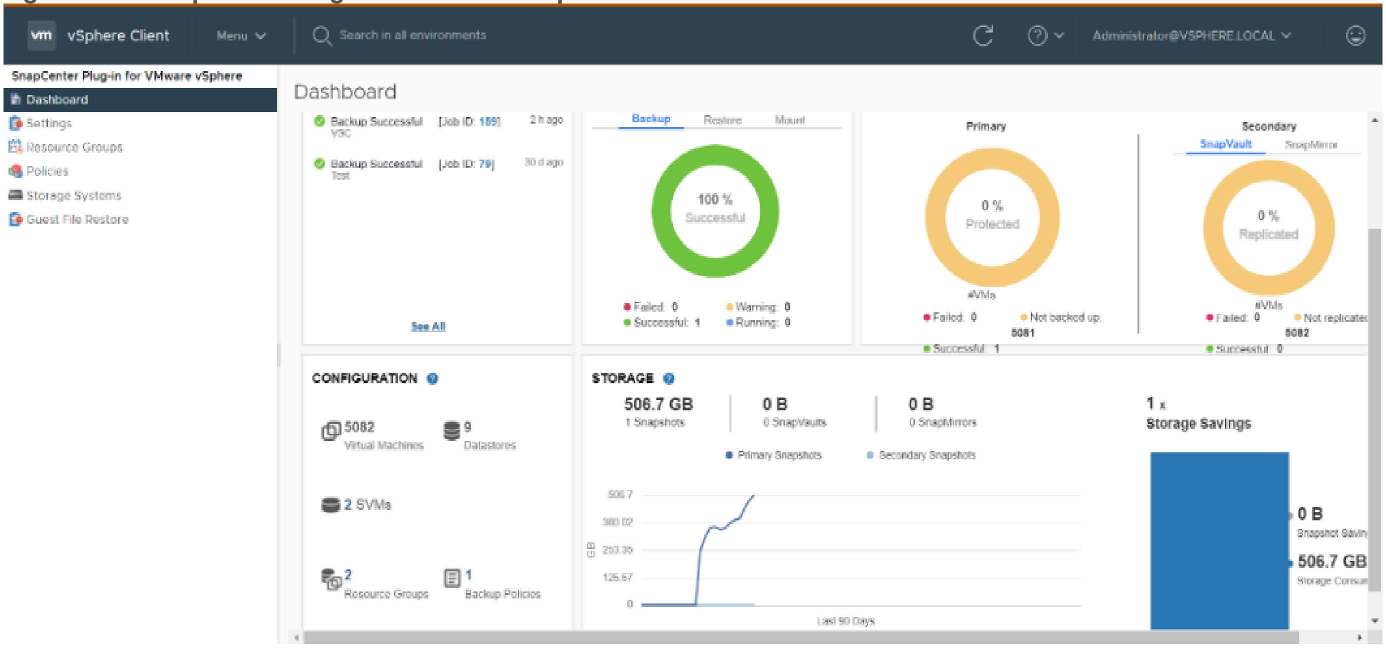
The copy offload feature and space reservation feature improve the performance of VSC operations. The NetApp NFS Plug-in for VAAI is not shipped with VSC, but you can install it by using VSC. You can download the plug-in installation package and obtain the instructions for installing the plug-in from the NetApp Support Site.

For more information about the NetApp VSC for VMware vSphere, see the NetApp Virtual Infrastructure Management Product Page.

NetApp SnapCenter Plug-In for VMware vSphere

NetApp SnapCenter Plug-in for VMware vSphere enables VM-consistent and crash-consistent backup and restore operations for VMs and datastores from the vCenter server. The SnapCenter plug-in is deployed as a virtual appliance, and it integrates with the vCenter server web client GUI.

Figure 23. SnapCenter Plug-In for VMware vSphere



Here are some of the functionalities provided by the SnapCenter plug-in to help protect your VMs and datastores:

- Backup VMs, virtual machine disks (VMDKs), and datastores
    - You can back up VMs, underlying VMDKs, and datastores. When you back up a datastore, you back up all the VMs in that datastore.
    - You can create mirror copies of backups on another volume that has a SnapMirror relationship to the primary backup or perform a disk-to-disk backup replication on another volume that has a NetApp SnapVault relationship to the primary backup volume.
    - Backup operations are performed on all the resources defined in a resource group. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.
- Restore VMs and VMDKs from backups
    - You can restore VMs from either a primary or secondary backup to the same ESXi server. When you restore a VM, you overwrite the existing content with the backup copy that you select.
    - You can restore one or more VMDKs on a VM to the same datastore. You can restore existing
- VMDKs, or deleted or detached VMDKs from either a primary or a secondary backup
    - You can attach one or more VMDKs from a primary or secondary backup to the parent VM (the same VM that the VMDK was originally associated with) or an alternate VM. You can detach the VMDK after you have restored the files you need.
    - You can restore a deleted VM from a datastore primary or secondary backup to an ESXi host that you select.

Note: For application-consistent backup and restore operations, the NetApp SnapCenter Server software is required.

Note: For additional information, requirements, licensing, and limitations of the NetApp SnapCenter Plug-In for VMware vSphere, see the NetApp Product Documentation.

NetApp Active IQ Unified Manager 9.10.1P1

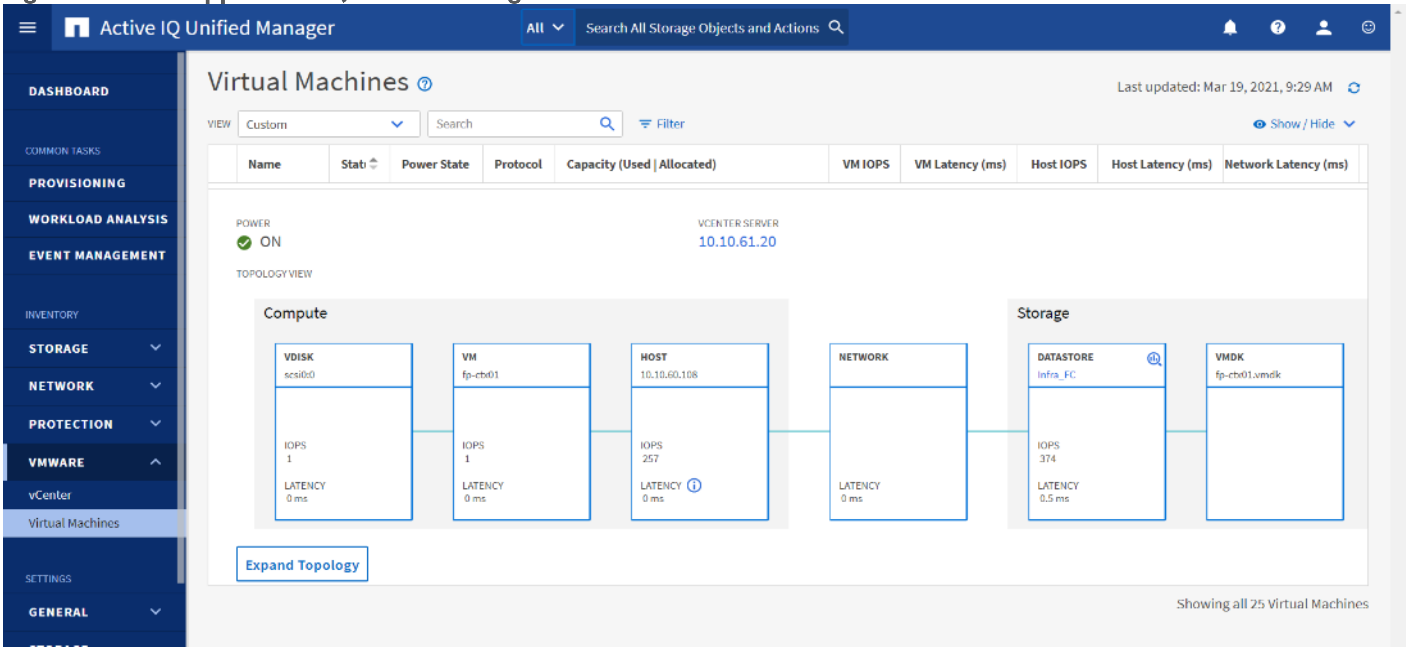
NetApp Active IQ Unified Manager (Unified Manager) is a comprehensive monitoring and proactive management tool for NetApp ONTAP systems to help manage the availability, capacity, protection, and performance risks of your storage systems and virtual infrastructure. You can deploy Unified Manager on a Linux server, on a Windows server, or as a virtual appliance on a VMware host.

Active IQ Unified Manager enables monitoring your ONTAP storage clusters, VMware vCenter server and VMs from a single redesigned, intuitive interface that delivers intelligence from community wisdom and AI analytics. It provides comprehensive operational, performance, and proactive insights into the storage environment and the VMs running on it. When an issue occurs on the storage or virtual infrastructure, Active IQ Unified Manager can notify you about the details of the issue to help with identifying the root cause.

Unified Manager enables to manage storage objects in your environment by associating them with annotations. You can create custom annotations and dynamically associate clusters, SVMs, and volumes with the annotations through rules.

The VM dashboard gives you a view into the performance statistics for the VM so that you can investigate the entire I/O path from the vSphere host down through the network and finally to the storage. Some events also provide remedial actions that can be taken to rectify the issue. You can also configure custom alerts for events so that when issues occur, you are notified through email and SNMP traps.

Figure 24.   NetApp Active IQ Unified Manager Virtual Machine Dashboard



NetApp XCP File Analytics

NetApp XCP file analytics is host-based software to scan the file shares, collect and analyzes the data and provide insights into the file system. NetApp XCP file analytics works for both NetApp and non-NetApp systems and runs on Linux or Windows host. For more info, go to: http://docs.netapp.com/us-en/xcp/index.html

Architecture and Design Considerations for Desktop Virtualization

This chapter contains the following:

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 Device (BYOD) 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 University and business computer labs, conference rooms or training centers. Shared workstation environments have the constant requirement to re-provision desktops with the latest operating systems and applications for the needs of the organization change, tops the list.

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

- Traditional PC: A traditional PC is what typically constitutes a desktop environment: a 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 2022, is shared by multiple users simultaneously. Each user receives a desktop " session" and works in an isolated memory space. Remoted Desktop Server Hosted Server sessions: A hosted virtual desktop is a virtual desktop running on a virtualization layer (ESX). 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 Citrix Virtual Apps and Desktops Remote Desktop Server Hosted (RDSH) sessions, RDS server virtual machines, and the user interacts through a delivery protocol. With published applications, a single installed instance of an application, such as Microsoft Office, 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 primary type and is synchronized with the data center when the device is connected to the network.

For the purposes of the validation represented in this document, both Citrix Virtual Apps and Desktops Remote Desktop Server Hosted (RDSH) sessions and Win 10 Virtual Desktops 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, for example, 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 10 or Windows 11?
- 32 bit or 64 bit desktop OS?

- How many virtual desktops will be deployed in the pilot? In production? All Windows 10?
- How much memory per target desktop group desktop?
- Are there any rich media, Flash, or graphics-intensive workloads?
- Are there any applications installed? What application delivery methods will be used, Installed, Streamed, Layered, Hosted, or Local?
- What is the OS planned for RDS Server Roles? Windows Server 2019 or Server 2022?
- 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?
- What is the SQL server version for the database? SQL server 2017 or 2019?
- Is user profile management (for example, non-roaming profile based) part of the solution?
- What is the fault tolerance, failover, disaster recovery plan?
- Are there additional desktop sub-group specific questions?

Hypervisor Selection

VMware vSphere has been identified for the hypervisor for both Citrix Virtual Apps and Desktops Remoted Server Desktop Hosted (RDSH) sessions and Win 10 Virtual Desktops.

VMware vSphere: VMware vSphere comprises the management infrastructure or virtual center server software and the hypervisor software that virtualizes the hardware resources on the servers. It offers features like Distributed Resource Scheduler, vMotion, high availability, Storage vMotion, VMFS, and a multi-pathing storage layer. More information on vSphere can be obtained at the VMware website: http://www.vmware.com/products/datacentervirtualization/vsphere/overview.html.

Note: For this CVD, the hypervisor used was VMware ESXi 7.0. Update 3.

Storage Considerations

Boot from SAN

When utilizing Cisco UCS Server technology, it is recommended to configure Boot from SAN and store the boot partitions on remote storage, this enabled architects and administrators to take full advantage of the stateless nature of service profiles for hardware flexibility across lifecycle management of server hardware generational changes, Operating Systems/Hypervisors, and overall portability of server identity. Boot from SAN also removes the need to populate local server storage creating more administrative overhead.

NetApp AFF Storage Considerations

Note: Make sure each NetApp AFF Controller is connected to BOTH storage fabrics (A/B).

Within NetApp, the best practice to map Hosts to iGroups and then iGroups to Volumes, this ensures the Volume is presented on the same LUN ID to all hosts and allows for simplified management of ESXi Clusters across multiple nodes.

Port Connectivity

10/25/40/100 Gbe connectivity support – while both 10 and 25 Gbe is provided through 2 onboard NICs on each AFF controller, if more interfaces are required or if 40Gbe connectivity is also required, then make sure to provision for additional NICs have been included in the original AFF BOM.

16/32Gb Fiber Channel supports the NetApp Storage up to 32Gb FC support on the latest AFF A400 series arrays. Always make sure the correct number of HBAs and the speed of SFPs are included in the original AFFBOM.

Overprovision

To reduce the impact of an outage or maintenance scheduled downtime it Is good practice when designing fabrics to provide oversubscription of bandwidth, this enables a similar performance profile during component failure and protects workloads from being impacted by a reduced number of paths during a component failure or maintenance event. Oversubscription can be achieved by increasing the number of physically cabled connections between storage and compute. These connections can be utilized to deliver performance and reduced latency to the underlying workloads running on the solution.

Topology

When configuring your SAN, it’s important to remember that the more hops you have, the more latency you will see. For best performance, the ideal topology is a “Flat Fabric” where the AFF is only one hop away from any applications being hosted on it.

VMware Virtual Volumes Considerations

vCenters that are in Enhanced Linked Mode will each be able to communicate with the same AFF, however vCenters that are not in Enhanced Linked Mode must use CA-Signed Certificates using the same AFF. If multiple vCenters need to use the same AFF for vVols, they should be configured in Enhanced Linked Mode.

There are some AFF limits on Volume Connections per Host, Volume Count, and Snapshot Count. For more information about NetApp AFF limits review the following: https://hwu.NetApp.com/Controller/Index

When a Storage Policy is applied to a vVol VM, the volumes associated with that VM are added to the designated protection group when applying the policy to the VM. If replication is part of the policy, be mindful of the amount of VMs using that storage policy and replication group. A large amount of VMs with a high change rate could cause replication to miss its schedule due to increased replication bandwidth and time needed to complete the scheduled snapshot. NetApp Storage recommends vVol VMs that have Storage Policies applied be balanced between protection groups.

Citrix Virtual Apps and Desktops 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 Virtual Apps and Desktops 7 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.

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

Machine Catalogs

Collections of identical virtual machines or physical computers are managed as a single entity called a Machine Catalog. In this CVD, virtual machine provisioning relies on Citrix Provisioning Services and Machine Creation 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 Multi-session OS VDA (Windows Server OS) or a Single-session OS VDA (Windows Desktop OS).

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:

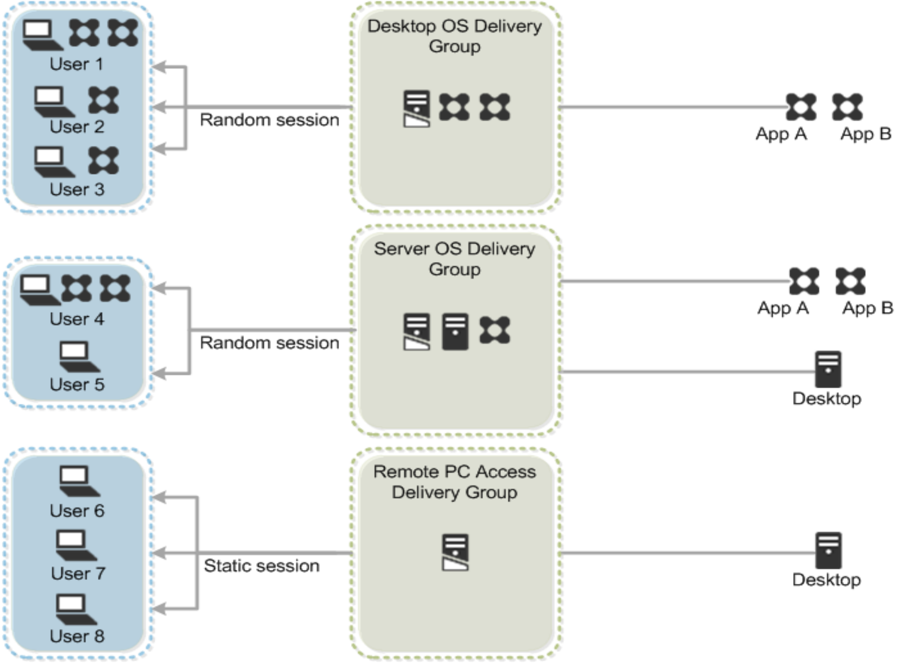
- Use machines from multiple catalogs
- Allocate a user to multiple machines
- Allocate multiple users to one machine

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

Figure 25. Access Desktops and Applications through Machine Catalogs and Delivery Groups



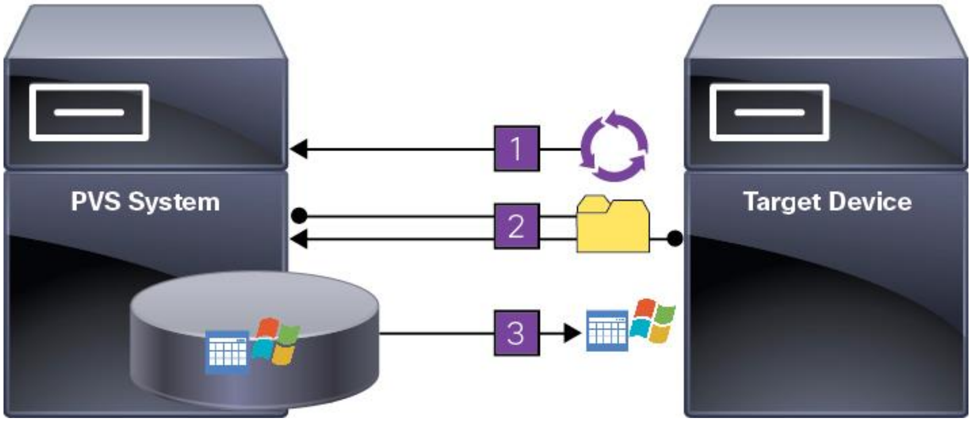
Citrix Provisioning Services

Citrix Virtual Apps and Desktops 7 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 26. 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 Virtual Apps and Desktops 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.

Note: In this CVD, Provisioning Server 2019 was used to manage Pooled/Non-Persistent Single-session OS 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 2019 was used for Active Directory machine account creation and management as well as for streaming the shared disk to the hypervisor hosts.

Example Citrix Virtual Apps and Desktops Deployments

Two examples of typical Virtual Apps and Desktops deployments are as follows:

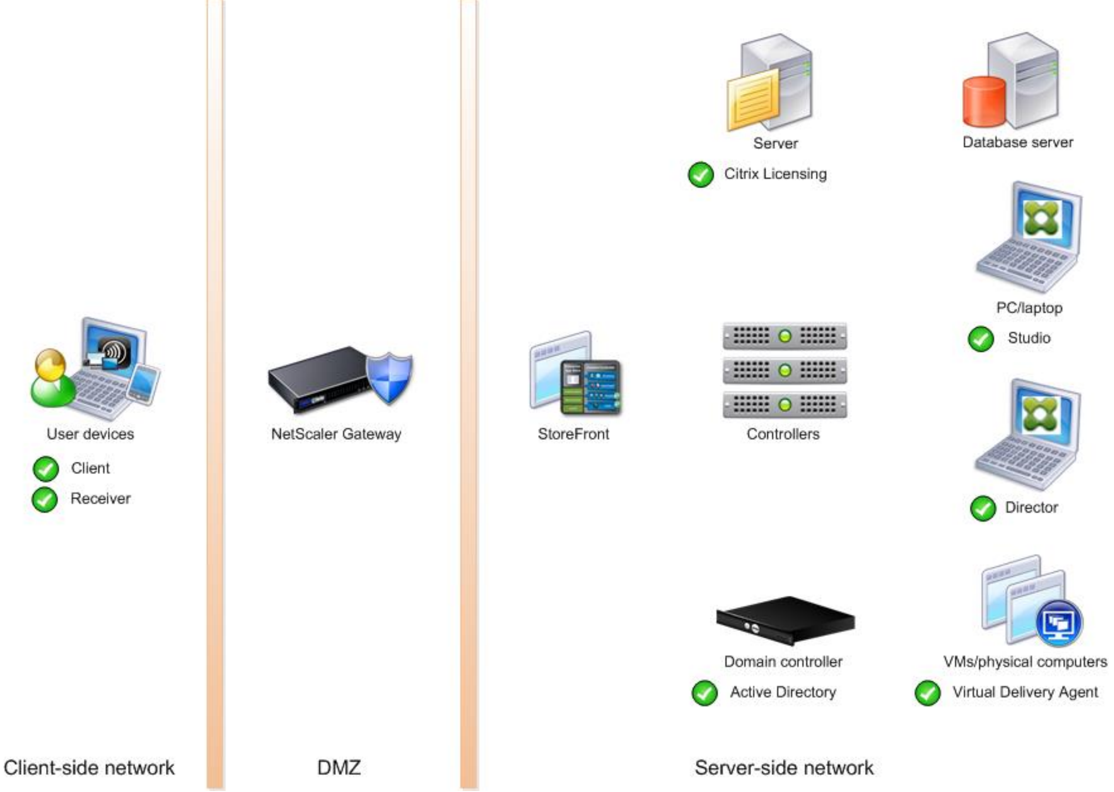
- A distributed components configuration
- A multiple site configuration

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 27 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 Virtual Apps and Desktops in a configuration that resembles this distributed component configuration shown.

Figure 27. Example of a Distributed Components Configuration

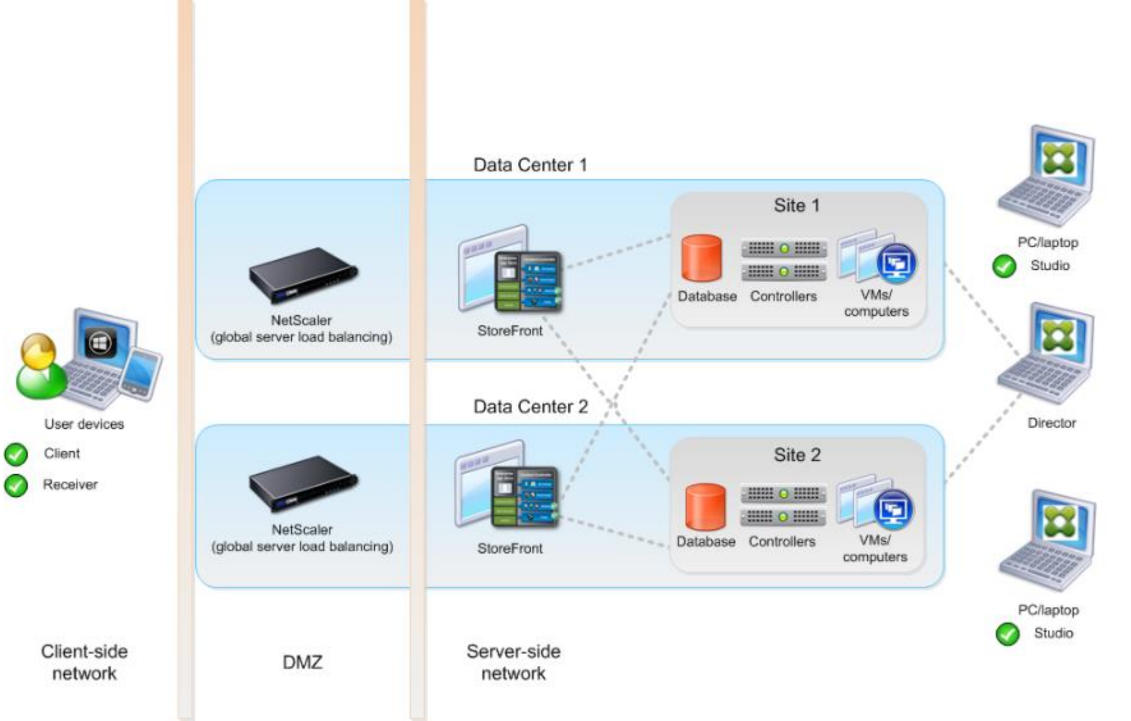


Multiple Site Configuration

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.

Figure 28 depicts 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 28. 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.

Note: The CVD was done based on single site and did not use NetScaler for its infrastructure and testing.

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 through a single-management plane to simplify administration

Designing a Virtual Apps and Desktops Environment for Different Workloads

With Citrix Virtual Apps and Desktops, 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.

Desktop Type	User Experience
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 data center. 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.

For this Cisco Validated Design, the following designs are included:

- Single-session OS Solution:
  - MCS: 2000 Windows 10 Virtual desktops random pooled were configured and tested
  - PVS: 2000 Windows 10 Virtual desktops random pooled were configured and tested
- Multi-session OS Solution:
  - RDS: 2500Windows Server 2019 random pooled desktops were configured and tested

Deployment Hardware and Software

This chapter contains the following:

Architecture

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 a Cisco UCS Domain) and out (adding additional Cisco UCS Domains and NetApp storage).

The FlexPod Datacenter solution includes Cisco networking, Cisco UCS and NetApp AFF A400, which efficiently fit into a single data center rack, including the access layer network switches.

Products Deployed

This CVD details the deployment of up to 2500 Multi-session OS, 2000 Single-session OS VDI users featuring the following software:

This CVD details the deployment of up to 2500 Multi-session OS, 2000 Single-session OS VDI users featuring the following software:

- VMware vSphere ESXi 7.0 U3 Hypervisor
- Microsoft SQL Server 2019
- Microsoft Windows Server 2019 and Windows 10 64-bit virtual machine Operating Systems
- Citrix Virtual Apps and Desktops 2203 LTSR
- Citrix Provisioning Server 2203 LTSR
- FSLogix 2105 HF_01
- Citrix StoreFront 2203 LTSR
- NetApp ONTAP Tools for VMware vSphere 9.11P1
- NetApp ONTAP 9.10.1P1

FlexPod with Cisco UCS M6 servers, Citrix Virtual Apps and Desktops Remote Desktop Server Hosted (RDSH) sessions and Windows 10 virtual desktops on vSphere 7.0 U3 delivers a Virtual Desktop Infrastructure that is redundant, using the best practices of Cisco and NetApp Storage. The solution includes VMware vSphere 7.0 U3 hypervisor installed on the Cisco UCS M6 blade server configured for stateless compute design using boot from SAN. NetApp Storage AFF A400 provides the storage infrastructure required for setting up the VDI workload. Cisco Intersight is utilized to configure and manage the Cisco UCS infrastructure with Cisco Intersight providing lifecycle management capabilities. The solution requirements and design details are covered in this section.

Physical Topology

FlexPod VDI with Cisco UCS M6 servers is a Fibre Channel (FC) based storage access design. NetApp Storage AFF and Cisco UCS are connected through Cisco MDS 9132T switches and storage access utilizes the FC network. For VDI IP based file share storage access NetApp Storage AFF Cisco UCS are connected through Cisco Nexus 93180YC-FX switches. The physical connectivity details are explained below.

Figure 29. FlexPod VDI – Physical Topology

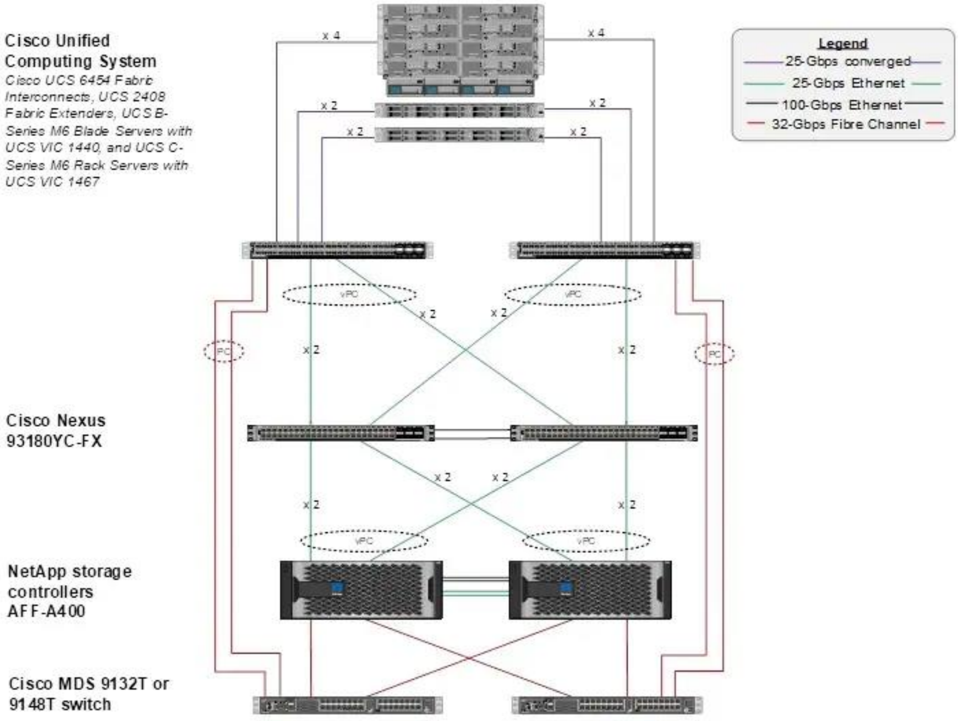

Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS 2408 Fabric Extenders, UCS B-Series M6 Blade Servers with UCS VIC 1440, and UCS C-Series M6 Rack Servers with UCS VIC 1467
Cisco Nexus 93180YC-FX
NetApp storage controllers AFF-A400
Cisco MDS 9132T or 9148T switch
Legend
25-Gbps converged
25-Gbps Ethernet
100-Gbps Ethernet
32-Gbps Fibre Channel
x 4
x 4
x 2
x 2
x 2
x 2
vPC
vPC
vPC
vPC
FC
FC
x 2
x 2
x 2
x 2
x 2
x 2
x 2
x 2

Figure 29 details the physical hardware and cabling deployed to enable this solution:

- 2 Cisco Nexus 93180YC-FX Switches in NX-OS Mode.
- 2 Cisco MDS 9132T 32-Gb Fibre Channel Switches.
- 1 Cisco UCS 5108 Blade Server Chassis with two Cisco UCS-IOM-2408 IO Modules.
- 8 Cisco UCS B200 M6 Blade Servers with Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM, and one Cisco VIC1440 mezzanine card, providing N+1 server fault tolerance.
- NetApp AFF A400 Storage System with dual redundant controllers, 2x disk shelves, and 48 x 1.75 TB solid-state NVMe drives providing storage and NVME/FC/NFS/CIFS connectivity.

Note: The common services and LoginVSI Test infrastructure are not a part of the physical topology of this solution.

Table 5 lists the software versions of the primary products installed in the environment.

Table 5. Software and Firmware Versions

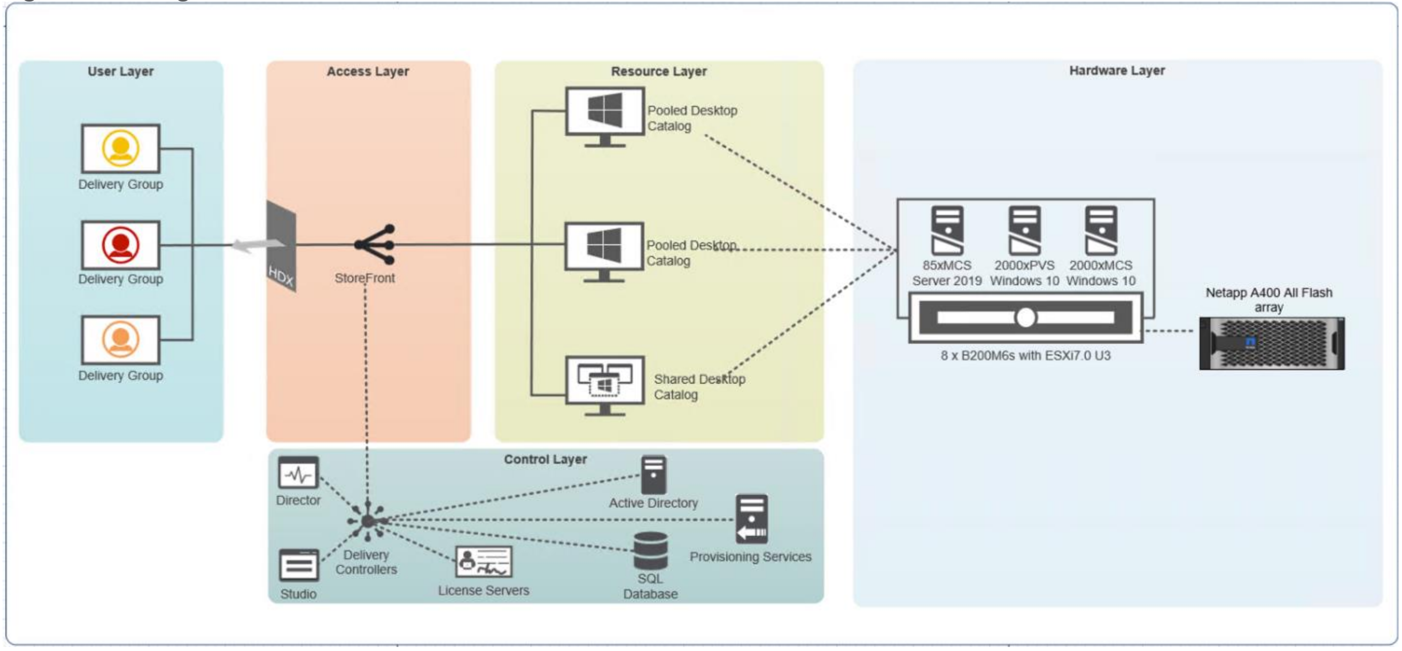
Vendor	Product / Component	Version / Build / Code
Cisco	UCS Component Firmware	4.2(2a) bundle release

Vendor	Product / Component	Version / Build / Code
Cisco	Intersight	4.2(2a) bundle release
Cisco	UCS B200 M6 Blades	4.2(2a) bundle release
Cisco	VIC 1440	4.2(2a) bundle release
Cisco	Cisco Nexus 93180YC-FX	9.3(7a)
Cisco	Cisco MDS 9132T	8.5(1a)
NetApp	AFF A400	ONTAP 9.10.1P1
NetApp	ONTAP Tools for VMWare vSphere	9.11
NetApp	NetApp NFS Plug-in for VMWare VAAI	2.0
NetApp	Active IQ Unified Manager	9.10P1
NetApp	SnapCenter Plug-In for VMware vSphere	4.6
VMware	vCenter Server Appliance	7..03.20150588
VMware	vSphere 7. U3	7.0.3.19193900
VMware	Tools	11.2.5.17337674
Citrix	Broker	2203 LTSR
Citrix	Agent	2203 LTSR
Citrix	Provisioning Server	2203 LTSR

Logical Architecture

The logical architecture of the validated solution which is designed to support up to 1700 users on a single chassis containing Eight Cisco UCS B200 M6 blade servers, with physical redundancy for the blade servers for each workload type is illustrated in Figure 30.

Figure 30. Logical Architecture Overview



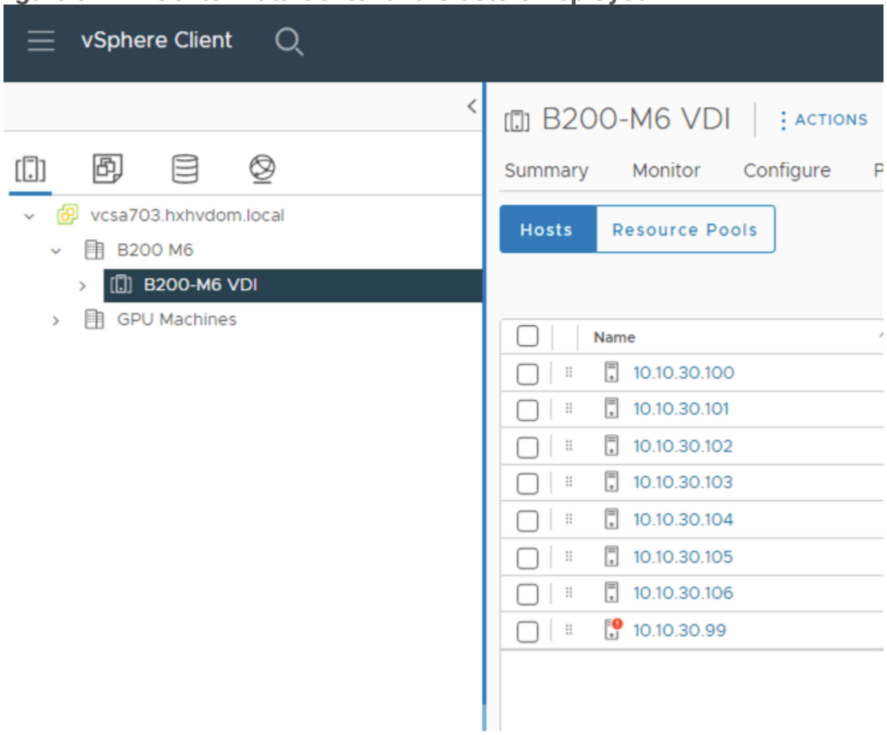
VMware Clusters

Two VMware Clusters in one vCenter data center were utilized to support the solution and testing environment:

- VDI Cluster FlexPod Data Center with Cisco UCS
    - Infrastructure: Infra VMs (vCenter, Active Directory, DNS, DHCP, SQL Server, VMware and Desktops Controllers, Provisioning Servers, and NetApp ONTAP Tools for VMware vSphere, ActiveIQ Unified Manager, VSMs, and so on)
    - VDI Workload VMs (Windows Server 2019 streamed with Citrix Virtual Apps and Desktops, Windows 10 Streamed with Citrix Virtual Apps and Desktops Windows 10 Instant Clones and Persistent desktops)
- VSI Launchers and Launcher Cluster

  For Example, the cluster(s) configured for running LoginVSI workload for measuring VDI End User Experience is LVS-Launcher-CLSTR: (The Login VSI infrastructure cluster consists of Login VSI data shares, LVSI Web Servers and LVSI Management Control VMs and so on. were connected using the same set of switches and vCenter instance but was hosted on separate storage. LVS-Launcher-CLSTR configured and used for the purpose of testing LoginVSI End User Experience for VDI multi session users and VDI Win 10 users.

Figure 31. vCenter Data Center and Clusters Deployed



Configuration Guidelines

The Citrix Virtual Apps and Desktops solution described in this document provides details for configuring a fully redundant, highly-available configuration. Configuration guidelines are provided that refer to which redundant component is being configured with each step, whether that be A or B. For example, Nexus A and Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS Fabric Interconnects are configured similarly.

This document is intended to allow the reader to configure the Citrix Virtual Apps and Desktops 2203 LTSR customer environment as a stand-alone solution.

VLANs

The VLAN configuration recommended for the environment includes a total of six VLANs as listed in Table 6.

Table 6. VLANs Configured in this Study

VLAN Name	VLAN ID	VLAN Purpose
Default	1	Native VLAN
In-Band-Mgmt	30	In-Band management interfaces
Infra-Mgmt	31	Infrastructure Virtual Machines
NFS- VLAN	32	VLAN for Infrastructure NFS traffic
CIFS-VLAN	33	CIFS Storage access
VCC/VM-Network	34	RDSH, VDI Persistent and Non-Persistent
vMotion	36	VMware vMotion

VLAN Name	VLAN ID	VLAN Purpose
OOB-Mgmt	132	Out-of-Band management interfaces

VSANs

Two virtual SANs configured for communications and fault tolerance in this design as outlined in Table 7.

Table 7. VSANs Configured in this Study

VSAN Name	VSAN ID	VSAN Purpose
VSAN 400	400	VSAN for Primary SAN communication
VSAN 401	401	VSAN for Secondary SAN communication

Solution Configuration

This chapter contains the following:

- Solution Cabling
- Network Switch Configuration
- Physical Connectivity
- FlexPod Cisco Nexus Base
- FlexPod Cisco Nexus Switch Configuration

Solution Cabling

The following sections detail the physical connectivity configuration of the FlexPod VMware VDI environment.

The information provided in this section is 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 of the NetApp Storage AFF A400 storage array to the Cisco 6454 Fabric Interconnects through Cisco MDS 9132T 32-Gb FC switches.

Note: 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.

IMPORTANT! Be sure to follow the cabling directions in this section. Failure to do so will result in unnecessary changes to the deployment since specific port locations are mentioned.

Figure 32 details the cable connections used in the validation lab for FlexPod topology based on the Cisco UCS 6454 fabric interconnect. Four 32Gb uplinks connect as port-channels to each Cisco UCS Fabric Interconnect from the MDS switches, and a total of eight 32Gb links connect the MDS switches to the NetApp AFF A400 controllers, four of these have been used for scsi-fc and the other four to support nvme-fc. Also, 40Gb links connect the Cisco UCS Fabric Interconnects to the Cisco Nexus Switches and the NetApp AFF A400 controllers to the Cisco Nexus Switches. Additional 1Gb management connections will be needed for an out-of-band network switch that sits apart from the FlexPod infrastructure. Each Cisco UCS fabric interconnect and Cisco Nexus switch is connected to the out-of-band network switch, and each All Flash Array controller has a connection to the out-of-band network switch. Layer 3 network connectivity is required between the Out-of-Band (OOB) and In-Band (IB) Management Subnets.

The architecture is divided into three distinct layers:

1. Cisco UCS Compute Platform
2. Network Access layer and LAN
3. Storage Access to the NetApp AFF400

Figure 32. FlexPod Solution Cabling Diagram

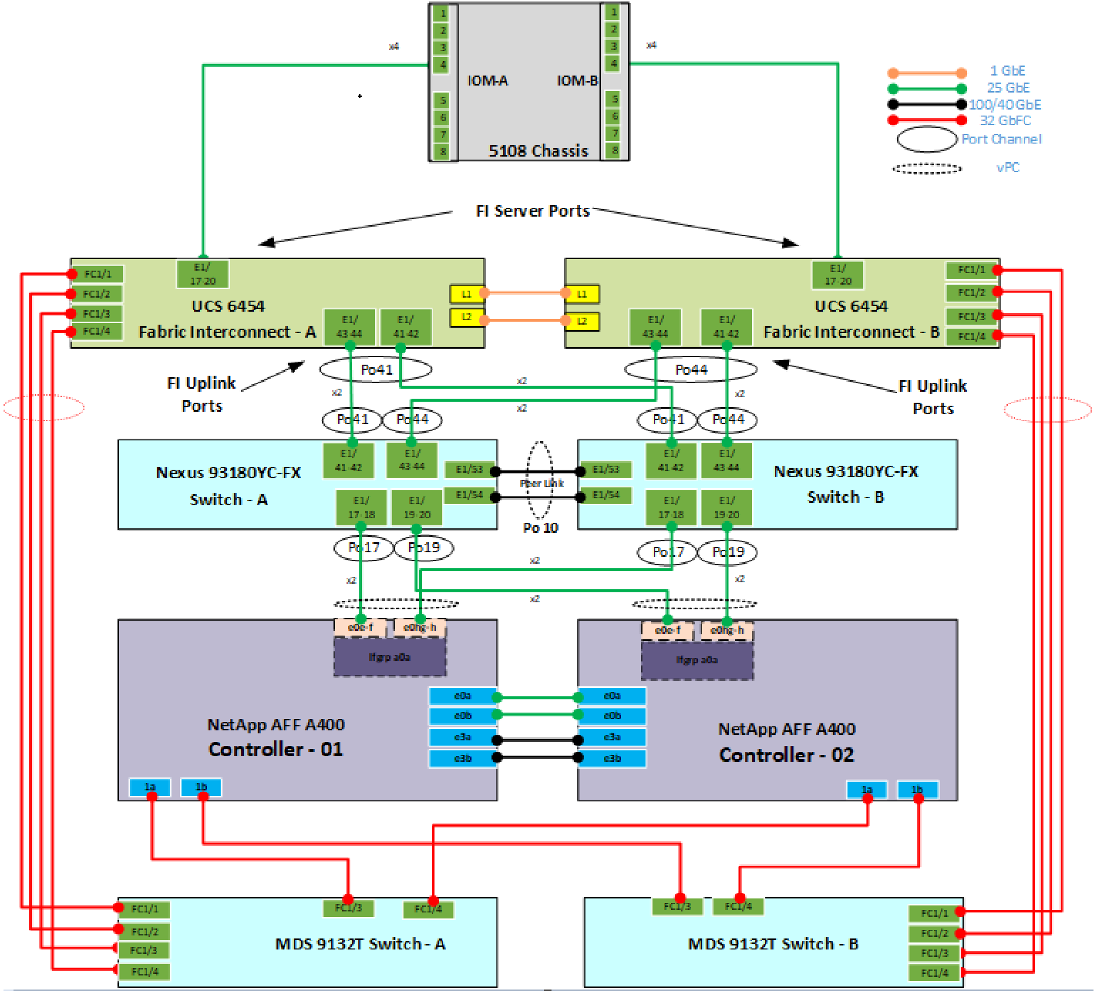


Table 8. Cisco Nexus 93180YC-FX-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93180YC-FX A	Eth1/19	25GbE	NetApp Controller 2	e0e
	Eth1/20	25GbE	NetApp Controller 2	e0f
	Eth1/17	25GbE	NetApp Controller 1	e0e
	Eth1/18	25GbE	NetApp Controller 1	e0f
	Eth1/41	25GbE	Cisco UCS fabric interconnect A	P0 1/43
	Eth1/42	25GbE	Cisco UCS fabric interconnect A	P0 1/44
	Eth1/43	25GbE	Cisco UCS fabric interconnect B	P0 1/43
	Eth1/44	25GbE	Cisco UCS fabric interconnect B	P0 1/44
	Eth1/53	40GbE	Cisco Nexus 93180YC-FX B	Eth1/53
	Eth1/54	40GbE	Cisco Nexus 93180YC-FX B	Eth1/54

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

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

Table 9. Cisco Nexus 93180YC-FX-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93180YC-FX B	Eth1/17	25GbE	NetApp Controller 1	e0g
	Eth1/18	25GbE	NetApp Controller 1	e0h
	Eth1/19	25GbE	NetApp Controller 2	e0g
	Eth1/20	25GbE	NetApp Controller 2	e0h
	Eth1/41	25GbE	Cisco UCS fabric interconnect A	P0 1/41
	Eth1/42	25GbE	Cisco UCS fabric interconnect A	P0 1/42
	Eth1/43	25GbE	Cisco UCS fabric interconnect B	P0 1/43
	Eth1/44	25GbE	Cisco UCS fabric interconnect B	P0 1/44
	Eth1/53	40GbE	Cisco Nexus 93180YC-FX A	Eth1/53
	Eth1/54	40GbE	Cisco Nexus 93180YC-FX A	Eth1/54
	MGMT0	GbE	GbE management switch	Any

Table 10. NetApp Controller-1 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp AFF400 Node 1	e0M	1GbE	1GbE management switch	Any
	e0s	GbE	GbE management switch	Any
	e0a	25GbE	NetApp Controller 2	e0a
	e0b	25GbE	NetApp Controller 2	e0b
	e0c	100GbE	NS224-1	e0a
	e0d	100GbE	NS224-2	e0b
	e0e	25GbE	Cisco Nexus 93180YC-FX B	Eth1/17
	e0f	25GbE	Cisco Nexus 93180YC-FX B	Eth1/18
	e0g	25GbE	Cisco Nexus 93180YC-FX A	Eth1/18
	e0h	25GbE	Cisco Nexus 93180YC-FX A	Eth1/17

Local Device	Local Port	Connection	Remote Device	Remote Port
	e3a	100GbE	NetApp Controller 2	e3a
	e3b	100GbE	NetApp Controller 2	e3b
	e1a	100GbE	NS224-2	e0a
	e1b	100GbE	NS224-1	e0b

Note: When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

Table 11. NetApp Controller 2 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp AFF400 Node 2	e0M	100E	100MbE management switch	Any
	e0s	GbE	GbE management switch	Any
	e0a	25GbE	NetApp Controller 1	e0a
	e0b	25GbE	NetApp Controller 1	e0b
	e0c	100GbE	NS224-1	e0a
	e0d	100GbE	NS224-2	e0b
	e0e	40GbE	Cisco Nexus 93180YC-FX A	Eth1/19
	e0f	40GbE	Cisco Nexus 93180YC-FX B	Eth1/19
	e0g	40GbE	Cisco Nexus 93180YC-FX B	Eth1/20
	e0h	40GbE	Cisco Nexus 93180YC-FX A	Eth1/20
	e3a	100GbE	NetApp Controller 1	e3a
	e3b	100GbE	NetApp Controller 1	e3b
	e1a	100GbE	NS224-2	e0a
	e1b	100GbE	NS224-1	e0b

Table 12. Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/41	25GbE	Cisco Nexus 93180YC-FX B	Eth1/41
	Eth1/42	25GbE	Cisco Nexus 93180YC-FX B	Eth1/42
	Eth1/43	25GbE	Cisco Nexus 93180YC-FX A	Eth1/41

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/44	25GbE	Cisco Nexus 93180YC-FX A	Eth1/42
	FC1/1	32GbE	Cisco MDS 9132T A	IOM 1/1
	FC1/2	32GbE	Cisco MDS 9132T A	IOM 1/2
	FC1/3	32GbE	Cisco MDS 9132T A	IOM 1/3
	FC1/4	32GbE	Cisco MDS 9132T A	IOM 1/4
	MGMT0	GbE	GbE Management switch	
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2

Table 13. Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect B	Eth1/41	25GbE	Cisco Nexus 93180YC-FX B	Eth1/43
	Eth1/42	25GbE	Cisco Nexus 93180YC-FX B	Eth1/44
	Eth1/43	25GbE	Cisco Nexus 93180YC-FX A	Eth1/43
	Eth1/44	25GbE	Cisco Nexus 93180YC-FX A	Eth1/44
	FC1/1	32GbE	Cisco MDS 9132 T B	FC 1/1
	FC1/2	32GbE	Cisco MDS 9132 T B	FC 1/2
	FC1/3	32GbE	Cisco MDS 9132 T B	FC 1/3
	FC1/4	32GbE	Cisco MDS 9132 T B	FC 1/4
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A	L1
	L2	GbE	Cisco UCS fabric interconnect A	L2

Network Switch Configuration

This subject contains the following procedures:

- Set Up Initial Configuration on Cisco Nexus A
- Set Up Initial Configuration on Cisco Nexus B

This section provides a detailed procedure for configuring the Cisco Nexus 93180YC-FX switches for use in a FlexPod environment. The Cisco Nexus 93180YC-FX will be used LAN switching in this solution.

IMPORTANT! Follow these steps precisely because failure to do so could result in an improper configuration.

Physical Connectivity

Follow the physical connectivity guidelines for FlexPod as explained in section Solution Cabling.

FlexPod Cisco Nexus Base

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod environment. This procedure assumes the use of Cisco Nexus 9000 9.3(7a), the Cisco suggested Nexus switch release at the time of this validation.

The following procedure includes the setup of NTP distribution on both the mgmt0 port and the in-band management VLAN. The interface-vlan feature and ntp commands are used to set this up. This procedure also assumes that the default VRF is used to route the in-band management VLAN.

Note: In this validation, port speed and duplex are hard set at both ends of every 100GE connection.

Procedure 1. Set Up Initial Configuration on Cisco Nexus A

Set up the initial configuration for the Cisco Nexus A switch on <nexus-A-hostname>

Step 1. On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass
password and basic configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no)[no]: yes

Disabling POAP.......Disabling POAP

poap: Rolling back, please wait... (This may take 5-15 minutes)

         ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]: Enter

Enter the password for "admin": <password>

Confirm the password for "admin": <password>

Would you like to enter the basic configuration dialog (yes/no): yes

Create another login account (yes/no) [n]: Enter

Configure read-only SNMP community string (yes/no) [n]: Enter

Configure read-write SNMP community string (yes/no) [n]: Enter

Enter the switch name: <nexus-A-hostname>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter

Mgmt0 IPv4 address: <nexus-A-mgmt0-ip>

Mgmt0 IPv4 netmask: <nexus-A-mgmt0-netmask>

Configure the default gateway? (yes/no) [y]: Enter

IPv4 address of the default gateway: <nexus-A-mgmt0-gw>

Configure advanced IP options? (yes/no) [n]: Enter

Enable the telnet service? (yes/no) [n]: Enter

Enable the ssh service? (yes/no) [y]: Enter

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter

Number of rsa key bits <1024-2048> [1024]: Enter

Configure the ntp server? (yes/no) [n]: Enter

Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Enter basic FC configurations (yes/no) [n]: yes
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter

Would you like to edit the configuration? (yes/no) [n]: Enter
```

Step 2. Review the configuration summary before enabling the configuration.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

Procedure 2. Set Up Initial Configuration on Cisco Nexus B

Set up the initial configuration for the Cisco Nexus B switch on <nexus-B-hostname>.

Step 1. On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass
password and basic configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no)[no]: yes

Disabling POAP.......Disabling POAP

poap: Rolling back, please wait... (This may take 5-15 minutes)

         ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]: Enter

Enter the password for "admin": <password>

Confirm the password for "admin": <password>

Would you like to enter the basic configuration dialog (yes/no): yes

Create another login account (yes/no) [n]: Enter

Configure read-only SNMP community string (yes/no) [n]: Enter

Configure read-write SNMP community string (yes/no) [n]: Enter

Enter the switch name: <nexus-B-hostname>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter

Mgmt0 IPv4 address: <nexus-B-mgmt0-ip>

Mgmt0 IPv4 netmask: <nexus-B-mgmt0-netmask>

Configure the default gateway? (yes/no) [y]: Enter

IPv4 address of the default gateway: <nexus-B-mgmt0-gw>

Configure advanced IP options? (yes/no) [n]: Enter

Enable the telnet service? (yes/no) [n]: Enter

Enable the ssh service? (yes/no) [y]: Enter

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter

Number of rsa key bits <1024-2048> [1024]: Enter

Configure the ntp server? (yes/no) [n]: Enter

Configure default interface layer (L3/L2) [L2]: Enter

Configure default switchport interface state (shut/noshut) [noshut]: shut

Enter basic FC configurations (yes/no) [n]: yes

Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter

Would you like to edit the configuration? (yes/no) [n]: Enter
```

Step 2. Review the configuration summary before enabling the configuration.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

FlexPod Cisco Nexus Switch Configuration

This subject contains the following procedures:

- Enable Features on Cisco Nexus A and Cisco Nexus B
- Set Global Configurations on Cisco Nexus A and Cisco Nexus B
- Create VLANs on Cisco Nexus A and Cisco Nexus B
- Add NTP Distribution Interface on Cisco Nexus A
- Add NTP Distribution Interface on Cisco Nexus B
- Add Individual Port Descriptions for Troubleshooting and Enable UDLD for Cisco UCS Interfaces on Cisco Nexus A
- Add Individual Port Descriptions for Troubleshooting and Enable UDLD for Cisco UCS Interfaces on Cisco Nexus B
- Create Port Channels on Cisco Nexus A and Cisco Nexus B
- Configure Port Channel Parameters on Cisco Nexus A and Cisco Nexus B
- Configure Virtual Port Channels on Cisco Nexus A
- Configure Virtual Port Channels on Cisco Nexus B

Procedure 1. Enable Features on Cisco Nexus A and Cisco Nexus B

SAN switching requires both the SAN_ENTERPRISE_PKG and FC_PORT_ACTIVATION_PKG licenses. Please ensure these licenses are installed on each Cisco Nexus 93180YC-FX switch.

Step 1. Log in as admin.

Step 2. Since basic FC configurations were entered in the setup script, feature-set fcoe has been automatically installed and enabled. Run the following commands:

```
config t
feature udld

feature interface-vlan

feature lacp

feature vpc

feature lldp
```

Procedure 2. Set Global Configurations on Cisco Nexus A and Cisco Nexus B

Step 1. Run the following commands to set global configurations:

```
spanning-tree port type network default

spanning-tree port type edge bpduguard default

spanning-tree port type edge bpdufilter default

port-channel load-balance src-dst l4port

ntp server <global-ntp-server-ip> use-vrf management

ntp master 3

clock timezone <timezone> <hour-offset> <minute-offset>

clock summer-time <timezone> <start-week> <start-day> <start-month> <start-time> <end-week> <end-day> <end-month> <end-time> <offset-minutes>
```

```
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

Tech tip

It is important to configure the local time so that logging time alignment and any backup schedules are correct. For more information on configuring the timezone and daylight savings time or summer time, please see Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x). Sample clock commands for the United States Eastern timezone are:

clock timezone EST -5 0

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

Procedure 3. Create VLANs on Cisco Nexus A and Cisco Nexus B

Step 1. From the global configuration mode, run the following commands:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
vlan <infra-CIFS-vlan-id>
name Infra-CIFS-VLAN
exit
```

Procedure 4. Add NTP Distribution Interface on Cisco Nexus A

Step 1. From the global configuration mode, run the following commands:

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exit
ntp peer <switch-b-ntp-ip> use-vrf default
```

Procedure 5. Add NTP Distribution Interface on Cisco Nexus B

Step 1. From the global configuration mode, run the following commands:

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exit
ntp peer <switch-a-ntp-ip> use-vrf default
```

Procedure 6. Add Port Profiles on Cisco Nexus A and Cisco Nexus B

This version of the FlexPod solution uses port profiles for virtual port channel (vPC) connections to NetApp Storage, Cisco UCS, and the vPC peer link.

Step 1. From the global configuration mode, run the following commands:

```
port-profile type port-channel FP-ONTAP-Storage
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>,<infra-CIFS-vlan-id>
spanning-tree port type edge trunk
mtu 9216
state enabled

port-profile type port-channel FP-UCS
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <infra-CIFS-vlan-id>,  <vmotion-vlan-id>, <vm-traffic-vlan-id>
spanning-tree port type edge trunk
mtu 9216
state enabled

port-profile type port-channel vPC-Peer-Link
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <infra-CIFS-vlan-id>, <vmotion-vlan-id>, <vm-traffic-vlan-id>
spanning-tree port type network
speed 100000
duplex full
state enabled
```

Procedure 7. Add Individual Port Descriptions for Troubleshooting and Enable UDLD for Cisco UCS Interfaces on Cisco Nexus A

Note: In this step and in the following sections, configure the AFF nodename <st-node> and Cisco UCS 6454 fabric interconnect clustername <ucs-clustername> interfaces as appropriate to your deployment.

Step 1. From the global configuration mode, run the following commands:

```
interface Eth1/41
description <ucs-clustername>-a:1/43
udld enable
interface Eth1/42
description <ucs-clustername>-a:1/44
udld enable
interface Eth1/43
```

```
description <ucs-clustername>-b:1/43
udld enable
interface Eth1/44
description <ucs-clustername>-b:1/44
udld enable
```

Step 2. For fibre optic connections to Cisco UCS systems (AOC or SFP-based), entering `udld enable` will result in a message stating that this command is not applicable to fiber ports. This message is expected. If you have fibre optic connections, do not enter the `udld enable` command.

```
interface Eth1/17
description <st-clustername>-01:e0e
interface Eth1/18
description <st-clustername>-01:e0f
interface Eth1/19
description <st-clustername>-02:e0e
interface Eth1/20
description <st-clustername>-02:e0f
interface Eth1/53
description <nexus-b-hostname>:1/53
interface Eth1/54
description <nexus-b-hostname>:1/54
exit
```

Procedure 8.Add Individual Port Descriptions for Troubleshooting and Enable UDLD for Cisco UCS Interfaces on Cisco Nexus B

Step 1. From the global configuration mode, run the following commands:

```
interface Eth1/41
description <ucs-clustername>-a:1/41
udld enable
interface Eth1/42
description <ucs-clustername>-a:1/42
udld enable
interface Eth1/43
description <ucs-clustername>-b:1/41
udld enable
interface Eth1/44
description <ucs-clustername>-b:1/42
udld enable
```

Step 2. For fibre optic connections to Cisco UCS systems (AOC or SFP-based), entering `udld enable` will result in a message stating that this command is not applicable to fiber ports. This message is expected.

```
interface Eth1/17
description <st-clustername>-01:e0g
interface Eth1/18
description <st-clustername>-01:e0h
interface Eth1/19
```

```
description <st-clustername>-02:e0g
interface Eth1/20
description <st-clustername>-02:e0h
interface Eth1/53
description <nexus-a-hostname>:1/53
interface Eth1/54
description <nexus-a-hostname>:1/54
exit
```

Procedure 9.Create Port Channels on Cisco Nexus A and Cisco Nexus B

Step 1. From the global configuration mode, run the following commands:

```
interface Po10
description vPC peer-link
interface Eth1/53-54
channel-group 10 mode active
no shutdown
interface Po117
description <st-clustername>-01
interface Eth1/17-18
channel-group 117 mode active
no shutdown
interface Po119
description <st-clustername>-02
interface Eth1/19-20
channel-group 119 mode active
no shutdown
interface Po141
description <ucs-clustername>-a
interface Eth1/41-42
channel-group 121 mode active
no shutdown
interface Po142
description <ucs-clustername>-b
interface Eth1/43-44
channel-group 123 mode active
no shutdown
exit
copy run start
```

Procedure 10. Configure Port Channel Parameters on Cisco Nexus A and Cisco Nexus B

Step 1. From the global configuration mode, run the following commands:

```
interface Po10
```

```
inherit port-profile vPC-Peer-Link

interface Po117
inherit port-profile FP-ONTAP-Storage
interface Po119
inherit port-profile FP-ONTAP-Storage

interface Po141
inherit port-profile FP-UCS
interface Po142
inherit port-profile FP-UCS

exit
copy run start
```

Procedure 11. Configure Virtual Port Channels on Cisco Nexus A

Step 1. From the global configuration mode, run the following commands:

```
vpc domain <nexus-vpc-domain-id>
role priority 10
peer-keepalive destination <nexus-B-mgmt0-ip> source <nexus-A-mgmt0-ip>
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
interface Po10
vpc peer-link
interface Po117
vpc 117
interface Po119
vpc 119
interface Po141
vpc 121
interface Po142
vpc 123
exit
copy run start
```

Procedure 12. Configure Virtual Port Channels on Cisco Nexus B

Step 1. From the global configuration mode, run the following commands:

```
vpc domain <nexus-vpc-domain-id>
role priority 20
peer-keepalive destination <nexus-A-mgmt0-ip> source <nexus-B-mgmt0-ip>
```

```
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
interface Po10
vpc peer-link
interface Po117
vpc 117
interface Po119
vpc 119
interface Po141
vpc 121
interface Po142
vpc 123
exit
copy run start
```

Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod environment. If an existing Cisco Nexus environment is present, we recommend using vPCs to uplink the Cisco Nexus switches included in the FlexPod environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run copy run start to save the configuration on each switch after the configuration is completed.

Switch Testing Commands

The following commands can be used to check for correct switch configuration:

Note: Some of these commands need to run after further configuration of the FlexPod components are complete to see complete results.

```
show run
show vpc
show port-channel summary
show ntp peer-status
show cdp neighbors
show lldp neighbors
show run int
show int
show udld neighbors
show int status
```

Storage Configuration

This chapter contains the following:

- NetApp Hardware Universe
- NetApp ONTAP 9.10.1P1

NetApp Hardware Universe

The NetApp Hardware Universe (HWU) application provides supported hardware and software components for any specific ONTAP version. It also provides configuration information for all the NetApp storage appliances currently supported by ONTAP software and a table of component compatibilities.

To confirm that the hardware and software components that you would like to use are supported with the version of ONTAP that you plan to install, follow these steps at the NetApp Support site.

1. Access the HWU application to view the System Configuration guides. Click the Platforms menu to view the compatibility between different version of the ONTAP software and the NetApp storage appliances with your desired specifications.

2. Alternatively, to compare components by storage appliance, click Compare Storage Systems.

Controllers

Follow the physical installation procedures for the controllers found here: https://docs.netapp.com/us-en/ontap-systems/index.html.

Disk Shelves

NetApp storage systems support a wide variety of disk shelves and disk drives. The complete list of disk shelves that are supported by the AFF A400 and AFF A800 is available at the NetApp Support site.

When using SAS disk shelves with NetApp storage controllers, refer to: https://docs.netapp.com/us-en/ontap-systems/sas3/index.html for proper cabling guidelines.

When using NVMe drive shelves with NetApp storage controllers, refer to: https://docs.netapp.com/us-en/ontap-systems/ns224/index.html for installation and servicing guidelines.

NetApp ONTAP 9.10.1P1

This subject contains the following procedures:

- Configure Node 01
- Configure Node 02
- Set Up Node
- Log into the Cluster
- Verify Storage Failover
- Set Auto-Revert on Cluster Management
- Zero All Spare Disks
- Set Up Service Processor Network Interface
- Create Manual Provisioned Aggregates (Optional)

- Remove Default Broadcast Domains
- Disable Flow Control on 25/100GbE Data Ports
- Disable Auto-Negotiate on Fibre Channel Ports (Required only for FC configuration)
- Enable Cisco Discovery Protocol
- Enable Link-layer Discovery Protocol on all Ethernet Ports
- Create Management Broadcast Domain
- Create NFS Broadcast Domain
- Create CIFS Broadcast Domain
- Create ISCSI Broadcast Domains (Required only for iSCSI configuration)
- Create Interface Groups
- Change MTU on Interface Groups
- Create VLANs
- Configure Time Synchronization on the Cluster
- Configure Simple Network Management Protocol (SNMP)
- Configure SNMPv3 Access
- Create an infrastructure SVM
- Configure CIFS Servers
- Modify Storage Virtual Machine Option
- Create Load-Sharing Mirrors of a SVM Root Volume
- Create FC Block Protocol Service (required only for FC configuration)
- Create iSCSI Block Protocol Service (required only for iSCSI configuration)
- Vserver Protocol Verification
- Configure HTTPS Access to the Storage Controller
- Configure NFSv3 and NFSv4.1
- Create CIFS Export Policy
- Create a NetApp FlexVol Volume
- Create a NetApp FlexGroup Volume
- Modify Volume Efficiency
- Create CIFS Shares
- Create NFS LIFs
- Create CIFS LIFs
- Create FC LIFs (required only for FC configuration)
- Create iSCSI LIFs (required only for iSCSI configuration)

- Configure FC-NVMe Datastore for vSphere 7U3 on existing SVM (Infra-SVM) for FC-NVMe configuration only
- Add Infrastructure SVM Administrator and SVM Administration LIF to In-band Management Network
- Configure and Test AutoSupport

Complete Configuration Worksheet

Before running the setup script, complete the Cluster setup worksheet in the ONTAP 9 Documentation Center. You must have access to the NetApp Support site to open the cluster setup worksheet.

Configure ONTAP Nodes

Before running the setup script, review the configuration worksheets in the Software setup section of the ONTAP 9 Documentation Center to learn about configuring ONTAP. Table 14 lists the information needed to configure two ONTAP nodes. Customize the cluster-detail values with the information applicable to your deployment.

Table 14. ONTAP Software Installation Prerequisites

Cluster Detail	Cluster Detail Value
Cluster node 01 IP address	<node01-mgmt-ip>
Cluster node 01 netmask	<node01-mgmt-mask>
Cluster node 01 gateway	<node01-mgmt-gateway>
Cluster node 02 IP address	<node02-mgmt-ip>
Cluster node 02 netmask	<node02-mgmt-mask>
Cluster node 02 gateway	<node02-mgmt-gateway>
ONTAP 9.10.1P1 URL (http server hosting ONTAP software)	<url-boot-software>

Procedure 1. Configure Node 01

Step 1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when the following message displays: Starting AUTOBOOT press Ctrl-C to abort…

Step 2. Allow the system to boot up.

```
autoboot
```

Step 3. Press Ctrl-C when prompted.

Note: If ONTAP 9.10.1P1 is not the version of software being booted, continue with the following steps to install new software. If ONTAP 9.10.1P1 is the version being booted, select option 8 and `y` to reboot the node. Continue with section Set Up Node.

Step 4. To install new software, select option 7 from the menu.

Step 5. Enter `y` to continue the installation.

Step 6. Select `e0M` for the network port for the download.

Step 7. Enter `n` to skip the reboot.

Step 8. Select option 7 from the menu: `Install new software first`

Step 9. Enter `y` to continue the installation.

Step 10. Enter the IP address, netmask, and default gateway for `e0M`.

Step 11. Enter the IP address for port e0M: <node01-mgmt-ip>

Step 12. Enter the netmask for port e0M: <node01-mgmt-mask>

Step 13. Enter the IP address of the default gateway: <node01-mgmt-gateway>

Step 14. Enter the URL where the software can be found.

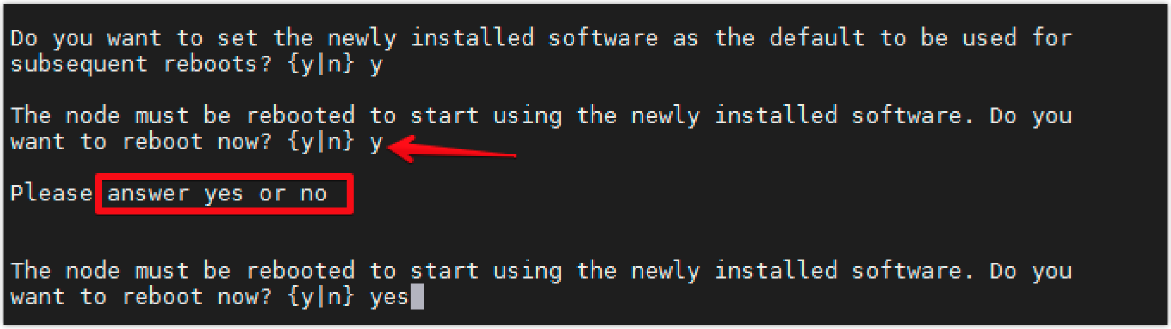
Step 15. The e0M interface should be connected to management network and the web server must be reachable (using ping) from node 01.

```
<url-boot-software>
```

Step 16. Press Enter for the user name, indicating no user name.

Step 17. Enter `y` to set the newly installed software as the default to be used for subsequent reboots.

Step 18. Enter `yes` to reboot the node.



```
Do you want to set the newly installed software as the default to be used for
subsequent reboots? {y|n} y

The node must be rebooted to start using the newly installed software. Do you
want to reboot now? {y|n} y

Please answer yes or no


The node must be rebooted to start using the newly installed software. Do you
want to reboot now? {y|n} yes
```

Note: When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the Loader-A prompt. If these actions occur, the system might deviate from this procedure.

Note: During the ONTAP installation, a prompt to reboot the node requests a Y/N response. The prompt requires the entire Yes or No response to reboot the node and continue the installation.

Step 19. Press Ctrl-C when the following message displays:

```
Press Ctrl-C for Boot Menu
```

Step 20. Select option 4 for Clean Configuration and Initialize All Disks.

Step 21. Enter `y` to zero disks, reset config, and install a new file system.

Step 22. Enter `yes` to erase all the data on the disks.

Note: When the initialization and creation of the root aggregate is complete, the storage system reboots. You can continue with the configuration of node 02 while the initialization and creation of the root aggregate for node 01 is in progress. For more information about root aggregate and disk partitioning, refer to the ONTAP documentation on root-data partitioning: https://docs.netapp.com/us-en/ontap/concepts/root-data-partitioning-concept.html.

Procedure 2. Configure Node 02

Step 1. Connect to the storage system console port. You should see a Loader-B prompt. However, if the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when the following message displays: Starting AUTOBOOT press Ctrl-C to abort...

Step 2. Allow the system to boot up.

```
autoboot
```

Step 3. Press Ctrl-C when prompted.

Note: If ONTAP 9.10.1P1 is not the version of software being booted, continue with the following steps to install new software. If ONTAP 9.10.1P1 is the version being booted, select option 8 and `y` to reboot the node, then continue with section Set Up Node.

Step 4. To install new software, select option 7.

Step 5. Enter y to continue the installation.

Step 6. Select e0M for the network port you want to use for the download.

Step 7. Enter n to skip the reboot.

Step 8. Select option 7: Install new software first

Step 9. Enter `y` to continue the installation

Step 10. Enter the IP address, netmask, and default gateway for e0M.

Step 11. Enter the IP address for port e0M: <node02-mgmt-ip>

Step 12. Enter the netmask for port e0M: <node02-mgmt-mask>

Step 13. Enter the IP address of the default gateway: <node02-mgmt-gateway>

Step 14. Enter the URL where the software can be found.

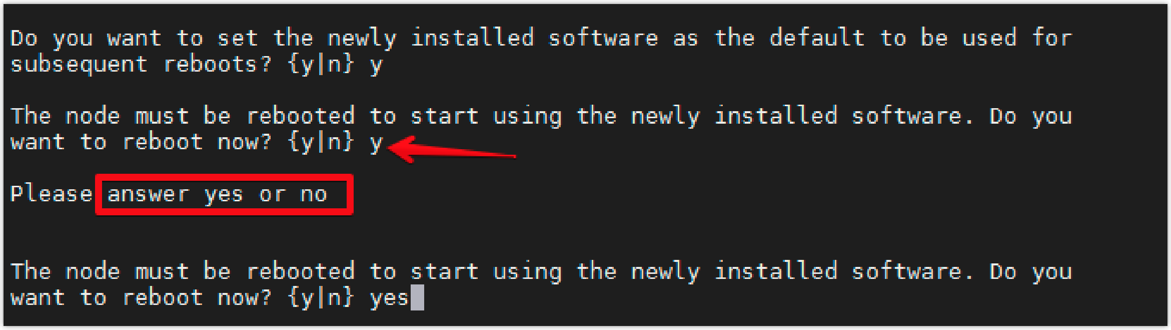
Step 15. The web server must be reachable (ping) from node 02.

```
<url-boot-software>
```

Step 16. Press `Enter` for the username, indicating no user name.

Step 17. Enter `y` to set the newly installed software as the default to be used for subsequent reboots.

Step 18. Enter `yes` to reboot the node.



```
Do you want to set the newly installed software as the default to be used for
subsequent reboots? {y|n} y

The node must be rebooted to start using the newly installed software. Do you
want to reboot now? {y|n} y

Please answer yes or no


The node must be rebooted to start using the newly installed software. Do you
want to reboot now? {y|n} yes
```

Note: When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the Loader-A prompt. If these actions occur, the system might deviate from this procedure.

Note: During the ONTAP installation a prompt to reboot the node requests a Y/N response. The prompt requires the entire `Yes` or `No` response to reboot the node and continue the installation.

Step 19. Press Ctrl-C when you see this message: Press Ctrl-C for Boot Menu.

Step 20. Select option 4 for Clean Configuration and Initialize All Disks.

Step 21. Enter `y` to zero disks, reset config, and install a new file system.

Step 22. Enter `yes` to erase all the data on the disks.

Note: When the initialization and creation of the root aggregate is complete, the storage system reboots. You can continue with the configuration of node 02 while the initialization and creation of the root aggregate for node 01 is in progress. For more information about root aggregate and disk partitioning, refer to the ONTAP documentation on root-data partitioning: https://docs.netapp.com/us-en/ontap/concepts/root-data-partitioning-concept.html.

Procedure 3. Set Up Node

Step 1. From a console port program attached to the storage controller A (node 01) console port, run the node setup script. This script appears when ONTAP 9.10.1P1 boots on the node for the first time.

Step 2. Follow the prompts to set up node 01.

Step 3. Welcome to node setup.

- You can enter the following commands at any time:
  - " help" or " ?" - if you want to have a question clarified,
  - " back" - if you want to change previously answered questions, and
  - " exit" or " quit" - if you want to quit the setup wizard.

Tech tip

Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing “cluster setup.”

To accept a default or omit a question, do not enter a value.

This system will send event messages and weekly reports to NetApp Technical Support.

To disable this feature, enter " autosupport modify -support disable" within 24 hours.

Enabling AutoSupport can significantly speed problem determination and resolution should a problem occur on your system.

For further information on AutoSupport, see: http://support.netapp.com/autosupport/

Step 4. Type yes to confirm and continue {yes}: yes

Step 5. Enter the node management interface port [e0M]: Enter

Step 6. Enter the node management interface IP address: <node01-mgmt-ip>

Step 7. Enter the node management interface netmask: <node01-mgmt-mask>

Step 8. Enter the node management interface default gateway: <node01-mgmt-gateway>

Step 9. A node management interface on port e0M with IP address <node01-mgmt-ip> has been created

Step 10. Use your web browser to complete cluster setup by accesing https://<node01-mgmt-ip>. Otherwise press Enter to complete cluster setup using the command line interface.

Step 11. To complete cluster setup, open a web browser and navigate to https://<node01-mgmt-ip>.

Table 15. Cluster Create in ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	<clustername>
Cluster Admin SVM	<cluster-adm-svm>
Infrastructure Data SVM	<infra-data-svm>
ONTAP base license	<cluster-base-license-key>
Cluster management IP address	<clustermgmt-ip>
Cluster management netmask	<clustermgmt-mask>
Cluster management gateway	<clustermgmt-gateway>
Cluster node 01 IP address	<node01-mgmt-ip>
Cluster node 01 netmask	<node01-mgmt-mask>
Cluster node 01 gateway	<node01-mgmt-gateway>
Cluster node 02 IP address	<node02-mgmt-ip>
Cluster node 02 netmask	<node02-mgmt-mask>
Cluster node 02 gateway	<node02-mgmt-gateway>
Node 01 service processor IP address	<node01-sp-ip>
Node 01 service processor network mask	<node01-sp-mask>
Node 01 service processor gateway	<node01-sp-gateway>
Node 02 service processor IP address	<node02-sp-ip>
Node 02 service processor network mask	<node02-sp-mask>
Node 02 service processor gateway	<node02-sp-gateway>
Node 01 node name	<st-node01>
Node 02 node name	<st-node02>
DNS domain name	<dns-domain-name>
DNS server IP address	<dns-ip>
NTP server A IP address	<switch-a-ntp-ip>
NTP server B IP address	<switch-b-ntp-ip>
SNMPv3 User	<snmp-v3-usr>
SNMPv3 Authentication Protocol	<snmp-v3-auth-proto>
SNMPv3 Privacy Protocol	<snmpv3-priv-proto>

Note: Cluster setup can also be performed using the CLI. This document describes the cluster setup using the NetApp ONTAP System Manager guided setup.

Step 12. Complete the required information on the Initialize Storage System screen:

Step 13. In the Cluster screen, enter the cluster name and administrator password.

Step 14. Complete the Networking information for the cluster and each node.

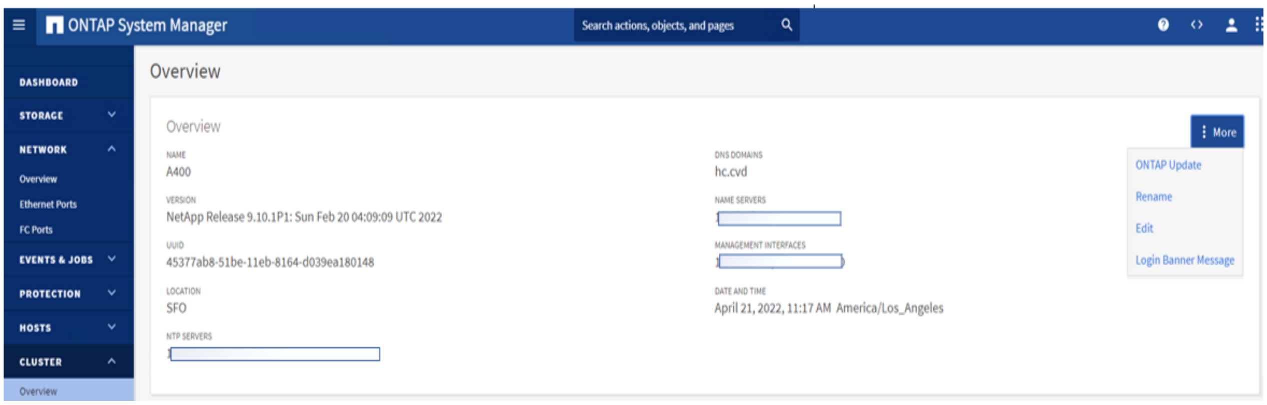
Tech tip
The nodes should be discovered automatically; if they are not, Refresh the browser page. By default, the cluster interfaces are created on all the new factory shipping storage controllers. If all the nodes are not discovered, then configure the cluster using the command line. The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet. In this document, we assume that it is on the same subnet.

Step 15. Click Submit.

Step 16. A few minutes will pass while the cluster is configured. When prompted, login to ONTAP System Manager to continue the cluster configuration.

Step 17. From the Dashboard click the Cluster menu and click Overview.

Step 18. Click the More ellipsis button in the Overview pane and click Edit.



Overview

Overview

NAME
A400

VERSION
NetApp Release 9.10.1P1: Sun Feb 20 04:09:09 UTC 2022

UUID
45377ab8-51be-11eb-8164-d039ea180148

LOCATION
SFO

NTP SERVERS
[redacted]

DNS DOMAINS
hc.cvd

NAME SERVERS
[redacted]

MANAGEMENT INTERFACES
[redacted]

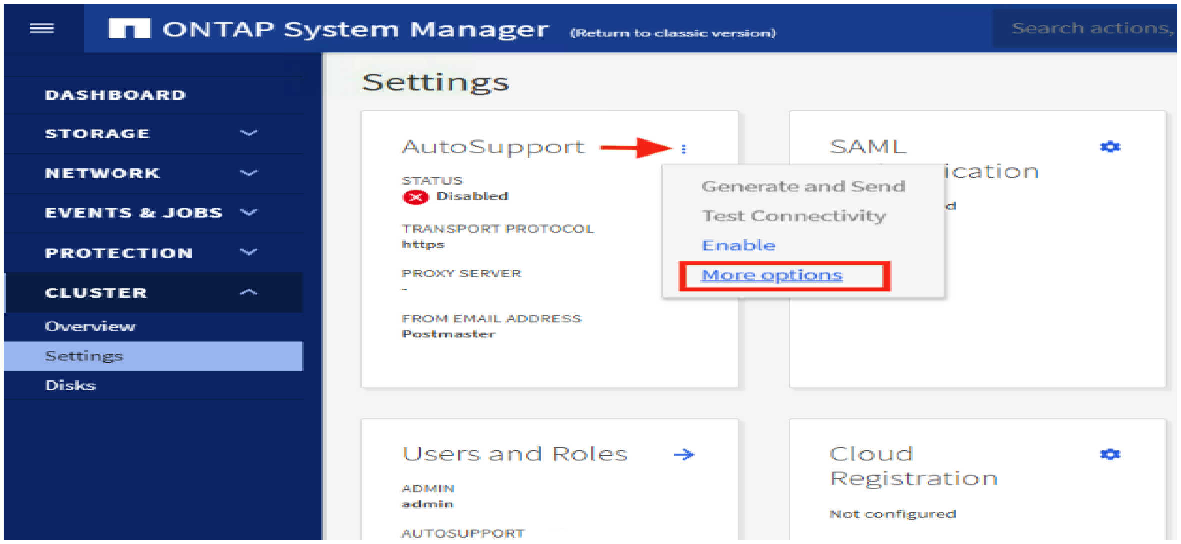
DATE AND TIME
April 21, 2022, 11:17 AM America/Los_Angeles

Step 19. Add additional cluster configuration details and click Save to make the changes persistent:

- Cluster location
- DNS domain name
- DNS server IP addresses
- DNS server IP addresses can be added individually or with a comma separated list on a single line.

Step 20. Click Save to make the changes persistent.

Step 21. Select the Settings menu under the Cluster menu.



AutoSupport

STATUS
Disabled

TRANSPORT PROTOCOL
https

PROXY SERVER
-

FROM EMAIL ADDRESS
Postmaster

ADMIN
admin

AUTOSUPPORT

Not configured

Step 22. If AutoSupport was not configured during the initial setup, click the ellipsis in the AutoSupport tile and select More options.

Step 23. To enable AutoSupport click the slider.

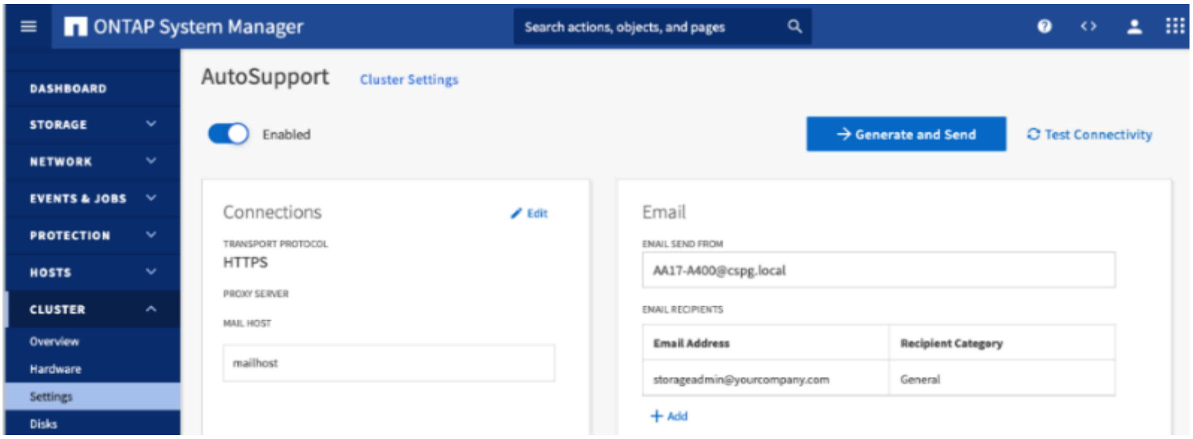
Step 24. Click Edit to change the transport protocol, add a proxy server address and a mail host as needed.

Step 25. Click Save to enable the changes.

Step 26. In the Email tile to the right, click Edit and enter the desired email information:

- Email send from address
- Email recipient addresses
- Recipient Category

Step 27. Click Save when complete.



Enabled

Connections

TRANSPORT PROTOCOL
HTTPS

PROXY SERVER

MAIL HOST
mailhost

Email

EMAIL SEND FROM
AA17-A400@cspg.local

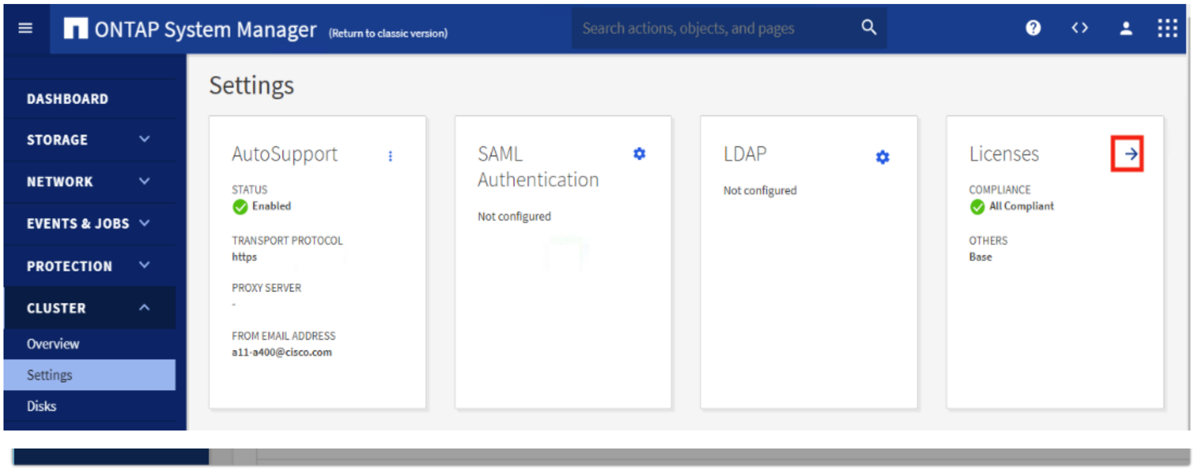
EMAIL RECIPIENTS

Email Address	Recipient Category
storageadmin@yourcompany.com	General

Step 28. Select CLUSTER > Settings at the top left of the page to return to the cluster settings page.

Step 29. Locate the Licenses tile on the right and click the detail arrow.

Step 30. Add the desired licenses to the cluster by clicking Add and entering the license keys in a comma separated list.


ONTAP System Manager (Return to classic version)
Search actions, objects, and pages
DASHBOARD
STORAGE
NETWORK
EVENTS & JOBS
PROTECTION
CLUSTER
Overview
Settings
Disks

Settings

AutoSupport
STATUS
Enabled
TRANSPORT PROTOCOL
https
PROXY SERVER
-
FROM EMAIL ADDRESS
a11-a400@cisco.com

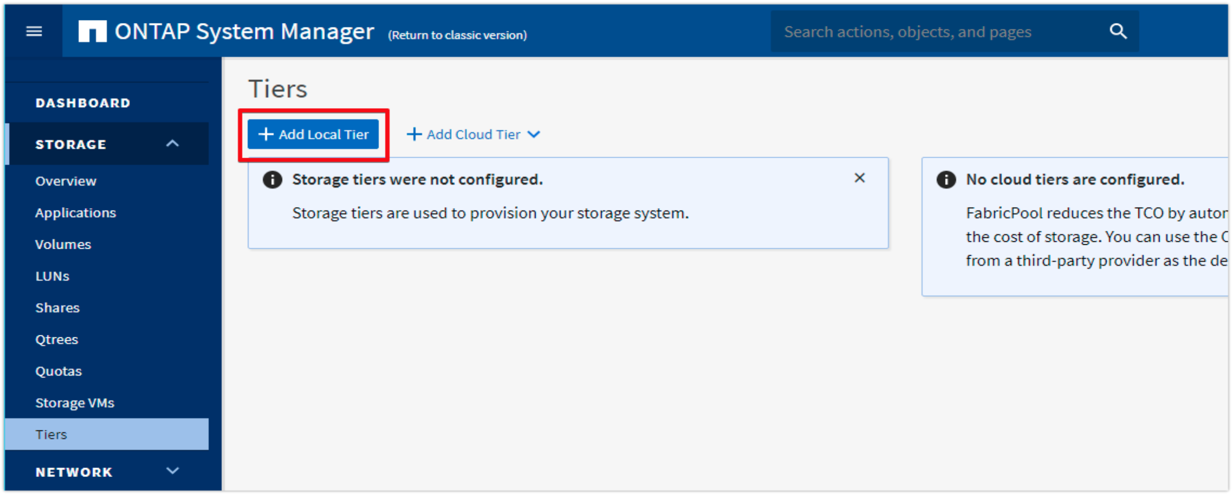
SAML Authentication
Not configured

LDAP
Not configured

Licenses
COMPLIANCE
All Compliant
OTHERS
Base

Step 31. Configure storage aggregates by selecting the Storage menu on the left and selecting Tiers.

Step 32. Click Add Local Tier and allow ONTAP System Manager to recommend a storage aggregate configuration.



Tiers

Storage tiers were not configured.

Storage tiers are used to provision your storage system.

No cloud tiers are configured.

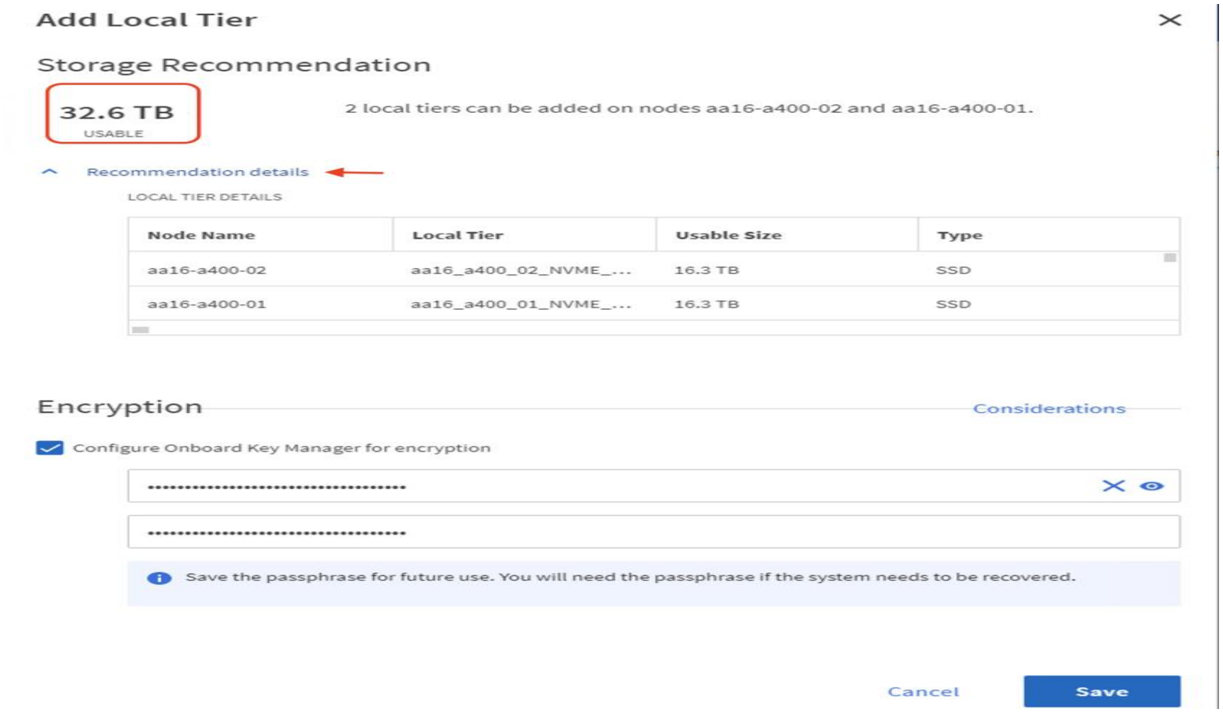
FabricPool reduces the TCO by autor
the cost of storage. You can use the C
from a third-party provider as the de

Step 33. ONTAP will use best practices to recommend an aggregate layout. Click the Recommended details link to view the aggregate information.

Step 34. Optionally, enable NetApp Aggregate Encryption (NAE) by checking the box for Configure Onboard Key Manager for encryption.

Step 35. Enter and confirm the passphrase and save it in a secure location for future use.

Step 36. Click Save to make the configuration persistent.



Add Local Tier

Storage Recommendation

32.6 TB USABLE

2 local tiers can be added on nodes aa16-a400-02 and aa16-a400-01.

Recommendation details

LOCAL TIER DETAILS

Node Name	Local Tier	Usable Size	Type
aa16-a400-02	aa16_a400_02_NVME_...	16.3 TB	SSD
aa16-a400-01	aa16_a400_01_NVME_...	16.3 TB	SSD

Encryption

Considerations

☑ Configure Onboard Key Manager for encryption

••••••••••••••••••••••••••••••••••••

••••••••••••••••••••••••••••••••••••

Save the passphrase for future use. You will need the passphrase if the system needs to be recovered.

Note: Aggregate encryption may not be supported for all deployments. Please review the NetApp Encryption Power Guide and the Security Hardening Guide for NetApp ONTAP 9 (TR-4569) to help determine if aggregate encryption is right for your environment.

Procedure 4. Log into the Cluster

Step 1. Open an SSH connection to either the cluster IP or the host name.

Step 2. Log into the admin user with the password you provided earlier.

Procedure 5. Verify Storage Failover

Step 1. Verify the status of the storage failover:

```
VDI-A400::> storage failover show
                                    Takeover
Node              Partner           Possible State Description
-------------- -------------- --------- -------------------------------------
VDI-A400-01    VDI-A400-02    true      Connected to VDI-A400-02
VDI-A400-02    VDI-A400-01    true      Connected to VDI-A400-01
2 entries were displayed.
```

Note: Both <st-node01> and <st-node02> must be capable of performing a takeover. Continue with step 2 if the nodes can perform a takeover.

Step 2. Enable failover on one of the two nodes if it was not completed during the installation:

```
storage failover modify -node <st-node01> -enabled true
```

Note: Enabling failover on one node enables it for both nodes.

Step 3. Verify the HA status for a two-node cluster:

Note: This step is not applicable for clusters with more than two nodes.

```
VDI-A400::> cluster ha show
High-Availability Configured: true
```

Note: If HA is not configured use the following commands. Only enable HA mode for two-node clusters. Do not run this command for clusters with more than two nodes because it causes problems with failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

Step 4. Verify that hardware assist is correctly configured:

```
VDI-A400::> storage failover hwassist show
Node
-----------------
VDI-A400-01
                             Partner: VDI-A400-02
                    Hwassist Enabled: true
                         Hwassist IP: 192.x.x.84
                       Hwassist Port: 162
                      Monitor Status: active
                     Inactive Reason: -
                   Corrective Action: -
                   Keep-Alive Status: healthy
VDI-A400-02
                             Partner: VDI-A400-01
                    Hwassist Enabled: true
                         Hwassist IP: 192.x.x.85
                       Hwassist Port: 162
                      Monitor Status: active
                     Inactive Reason: -
                   Corrective Action: -
                   Keep-Alive Status: healthy
2 entries were displayed.
```

Step 5. If hwassist storage failover is not enabled, enable using the following commands:

```
storage failover modify -hwassist-partner-ip <node02-mgmt-ip> -node <st-node01>
storage failover modify -hwassist-partner-ip <node01-mgmt-ip> -node <st-node02>
```

Procedure 6.Set Auto-Revert on Cluster Management

Step 1. Set the `auto-revert` parameter on the cluster management interface:

Note: A storage virtual machine (SVM) is referred to as a Vserver or `vserver` in the GUI and CLI.

```
net interface modify -vserver <clustername> -lif cluster_mgmt_lif_1 -auto-revert true
```

Procedure 7.Zero All Spare Disks

Step 1. Zero all spare disks in the cluster by running the following command:

```
disk zerospares
```

Tech tip
Advanced Data Partitioning creates a root partition and two data partitions on each SSD drive in an AFF configuration. Disk autoassign should have assigned one data partition to each node in an HA pair. If a different disk assignment is required, disk autoassignment must be disabled on both nodes in the HA pair by running the disk option modify command. Spare partitions can then be moved from one node to another by running the disk removeowner and disk assign commands.

Procedure 8. Set Up Service Processor Network Interface

Step 1. Assign a static IPv4 address to the Service Processor on each node by running the following commands:

```
system service-processor network modify -node <st-node01> -address-family IPv4 -enable
true -dhcp none -ip-address <node01-sp-ip> -netmask <node01-sp-mask> -gateway <node01-
sp-gateway>


system service-processor network modify -node <st-node02> -address-family IPv4 -enable
true -dhcp none -ip-address <node02-sp-ip> -netmask <node02-sp-mask> -gateway <node02-
sp-gateway>
```

Note: The Service Processor IP addresses should be in the same subnet as the node management IP addresses.

Procedure 9. Create Manual Provisioned Aggregates - Optional

Note: An aggregate containing the root volume is created during the ONTAP setup process. To manually create additional aggregates, determine the aggregate name, the node on which to create it, and the number of disks it should contain.

Step 1. Create new aggregates by running the following commands:

```
storage aggregate create -aggregate <aggr1_node01> -node <st-node01> -diskcount <num-
disks> -disktype SSD-NVM

storage aggregate create -aggregate <aggr1_node02> -node <st-node02> -diskcount <num-
disks> -disktype SSD-NVM
```

Note: You should have the minimum number of hot spare disks for the recommended hot spare disk partitions for their aggregate.

Note: For all-flash aggregates, you should have a minimum of one hot spare disk or disk partition. For non-flash homogenous aggregates, you should have a minimum of two hot spare disks or disk partitions. For Flash Pool aggregates, you should have a minimum of two hot spare disks or disk partitions for each disk type.

Tech tip
In an AFF configuration with a small number of SSDs, you might want to create an aggregate with all, but one remaining disk (spare) assigned to the controller.

Step 2. The aggregate cannot be created until disk zeroing completes. Run the `storage aggregate show` command to display the aggregate creation status. Do not proceed until both `aggr1_node1` and `aggr1_node2` are online.

Procedure 10. Remove Default Broadcast Domains

Note: By default, all network ports are included in separate default broadcast domain. Network ports used for data services (for example, `e0e`, `e0f`, and so on) should be removed from their default broadcast domain and that broadcast domain should be deleted.

Step 1. Run the following commands:

```
network port broadcast-domain delete -broadcast-domain <Default-N> -ipspace Default
network port broadcast-domain show
```

Step 2. Delete the Default broadcast domains with Network ports (Default-1, Default-2, and so on).

Procedure 11. Disable Flow Control on 25/100GbE Data Ports

Step 1. Disable the flow control on 25 and 100GbE data ports by running the following command to configure the ports on node 01:

```
network port modify -node <st-node01> -port e3a,e3b -flowcontrol-admin none
network port modify -node <st-node01> -port e0e,e0f,e0g,e0h -flowcontrol-admin none
```

Step 2. Run the following command to configure the ports on node 02:

```
network port modify -node <st-node02> -port e3a,e3b -flowcontrol-admin none
network port modify -node <st-node02> -port e0e,e0f,e0g,e0h -flowcontrol-admin none


VDI-A400::> net port show -node * -port e0e,e0f,e0g,e0h -fields speed-admin,duplex-
admin,flowcontrol-admin
  (network port show)
node         port duplex-admin speed-admin flowcontrol-admin
------------ ---- ------------ ----------- -----------------
VDI-A400-01 e0e  auto         auto        none
VDI-A400-01 e0f  auto         auto        none
VDI-A400-01 e0g  auto         auto        none
VDI-A400-01 e0h  auto         auto        none
VDI-A400-02 e0e  auto         auto        none
VDI-A400-02 e0f  auto         auto        none
VDI-A400-02 e0g  auto         auto        none
VDI-A400-02 e0h  auto         auto        none
8 entries were displayed.

VDI-A400::> net port show -node * -port e3a,e3b -fields speed-admin,duplex-
admin,flowcontrol-admin    (network port show)
node         port duplex-admin speed-admin flowcontrol-admin
------------ ---- ------------ ----------- -----------------
VDI-A400-01 e3a  auto         auto        none
VDI-A400-01 e3b  auto         auto        none
VDI-A400-02 e3a  auto         auto        none
VDI-A400-02 e3b  auto         auto        none
4 entries were displayed.
```

Procedure 12. Disable Auto-Negotiate on Fibre Channel Ports - Required only for FC configuration

Step 1. Disable each FC adapter in the controllers with the `fcp adapter modify` command:

```
fcp adapter modify -node <st-node01> -adapter 1a -status-admin down
fcp adapter modify -node <st-node01> -adapter 1b -status-admin down
fcp adapter modify -node <st-node02> -adapter 1a -status-admin down
fcp adapter modify -node <st-node02> -adapter 1b -status-admin down
```

Step 2. Set the desired speed on the adapter and return it to the online state:

```
fcp adapter modify -node <st-node01> -adapter 1a -speed 32 -status-admin up
fcp adapter modify -node <st-node01> -adapter 1b -speed 32 -status-admin up
fcp adapter modify -node <st-node02> -adapter 1a -speed 32 -status-admin up
fcp adapter modify -node <st-node02> -adapter 1b -speed 32 -status-admin up
```

Procedure 13. Enable Cisco Discovery Protocol

Step 1. Enable the Cisco Discovery Protocol (CDP) on the NetApp storage controllers by running the following command to enable CDP in ONTAP:

```
node run -node * options cdpd.enable on
```

Procedure 14. Enable Link-layer Discovery Protocol on all Ethernet Ports

Step 1. Enable the exchange of Link-layer Discovery Protocol (LLDP) neighbor information between the storage and network switches, on all ports, of all nodes in the cluster, by running the following command:

```
node run * options lldp.enable on
```

Procedure 15. Create Management Broadcast Domain

Step 1. If the management interfaces are required to be on a separate VLAN, create a new broadcast domain for those interfaces by running the following command:

```
network port broadcast-domain create -broadcast-domain IB-MGMT -mtu 1500
```

Procedure 16. Create NFS Broadcast Domain

Step 1. To create an NFS, data broadcast domain with a maximum transmission unit (MTU) of 9000, run the following commands to create a broadcast domain for NFS in ONTAP:

```
network port broadcast-domain create -broadcast-domain Infra-NFS -mtu 9000
```

Procedure 17. Create CIFS Broadcast Domain

Step 1. To create a CIFS data broadcast domain with a maximum transmission unit (MTU) of 9000, run the following commands to create a broadcast domain for CIFS in ONTAP:

```
network port broadcast-domain create -broadcast-domain Infra-CIFS -mtu 9000
```

Procedure 18. Create ISCSI Broadcast Domains - Required only for iSCSI configuration

Step 1. To create an ISCSI-A and ISCSI-B data broadcast domain with a maximum transmission unit (MTU) of 9000, run the following commands to create a broadcast domain for NFS in ONTAP:

```
network port broadcast-domain create -broadcast-domain Infra-ISCSI-A -mtu 9000
network port broadcast-domain create -broadcast-domain Infra-ISCSI-B -mtu 9000
```

Procedure 19. Create Interface Groups

Step 1. To create the LACP interface groups for the 25GbE data interfaces, run the following commands:

```
network port ifgrp create -node <st-node01> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <st-node01> -ifgrp a0a -port e0e
network port ifgrp add-port -node <st-node01> -ifgrp a0a -port e0f
network port ifgrp add-port -node <st-node01> -ifgrp a0a -port e0g
network port ifgrp add-port -node <st-node01> -ifgrp a0a -port e0h
network port ifgrp create -node <st-node02> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <st-node02> -ifgrp a0a -port e0e
network port ifgrp add-port -node <st-node02> -ifgrp a0a -port e0f

network port ifgrp add-port -node <st-node02> -ifgrp a0a -port e0g
network port ifgrp add-port -node <st-node02> -ifgrp a0a -port e0h
```

Step 2. To verify, run the following:

```
VDI-A400::> network port ifgrp show

         Port       Distribution                   Active

Node     IfGrp      Function     MAC Address       Ports    Ports

-------- ---------- ------------ ----------------- -------- -------------------

VDI-A400-01

         a0a        port         d2:39:ea:29:d4:4a full     e0e, e0f, e0g, e0h

VDI-A400-02

         a0a        port         d2:39:ea:29:ce:d5 full     e0e, e0f, e0g, e0h

2 entries were displayed.
```

Procedure 20. Change MTU on Interface Groups

Step 1. To change the MTU size on the base interface-group ports before creating the VLAN ports, run the following commands:

```
network port modify –node <st-node01> –port a0a –mtu 9000
network port modify –node <st-node02> –port a0a –mtu 9000
```

Procedure 21. Create VLANs

Step 1. Create the management VLAN ports and add them to the management broadcast domain:

```
network port vlan create –node <st-node01> -vlan-name a0a-<ib-mgmt-vlan-id>

network port vlan create –node <st-node02> -vlan-name a0a-<ib-mgmt-vlan-id>


network port broadcast-domain add-ports -broadcast-domain IB-MGMT -ports <st-
node01>:a0a-<ib-mgmt-vlan-id>,<st-node02>:a0a-<ib-mgmt-vlan-id>
```

Step 2. To verify, run the following command:

```
VDI-A400::> network port vlan show

                 Network Network

Node   VLAN Name Port    VLAN ID  MAC Address

------ --------- -------- -------- -----------------

VDI-A400-01

       a0a-60    a0a      60       d2:39:ea:29:d4:4a

       a0a-61
```

```
                 a0a       61    d2:39:ea:29:d4:4a
       a0a-62
                 a0a       62     d2:39:ea:29:d4:4a
       a0a-63
                 a0a     63     d2:39:ea:29:d4:4a
VDI-A400-02
       a0a-60    a0a     60       d2:39:ea:29:ce:d5
       a0a-61
                 a0a       61     d2:39:ea:29:ce:d5
       a0a-62
                 a0a     62    d2:39:ea:29:ce:d5
       a0a-63
                 a0a     63    d2:39:ea:29:ce:d5
8 entries were displayed.
```

Step 3. Create the NFS VLAN ports and add them to the `Infra-NFS` broadcast domain:

```
network port vlan create –node <st-node01> -vlan-name a0a-<infra-nfs-vlan-id>
network port vlan create –node <st-node02> -vlan-name a0a-<infra-nfs-vlan-id>

network port broadcast-domain add-ports -broadcast-domain Infra-NFS -ports <st-
node01>:a0a-<infra-nfs-vlan-id>,<st-node02>:a0a-<infra-nfs-vlan-id>
```

Step 4. Create the CIFS VLAN ports and add them to the `Infra-CIFS` broadcast domain:

```
network port vlan create –node <st-node01> -vlan-name a0a-<infra-cifs-vlan-id>
network port vlan create –node <st-node02> -vlan-name a0a-<infra-cifs-vlan-id>

network port broadcast-domain add-ports -broadcast-domain Infra-CIFS -ports <st-
node01>:a0a-<infra-cifs-vlan-id>,<st-node02>:a0a-<infra-cifs-vlan-id>
```

Step 5. If configuring iSCSI, create VLAN ports for the iSCSI LIFs on each storage controller and add them to the broadcast domain:

```
network port vlan create –node <st-node01> -vlan-name a0a-<infra-iscsi-a-vlan-id>
network port vlan create –node <st-node01> -vlan-name a0a-<infra-iscsi-b-vlan-id>
network port vlan create –node <st-node02> -vlan-name a0a-<infra-iscsi-a-vlan-id>
network port vlan create –node <st-node02> -vlan-name a0a-<infra-iscsi-b-vlan-id>


network port broadcast-domain add-ports -broadcast-domain Infra-iSCSI-A -ports <st-
node01>:a0a-<infra-iscsi-a-vlan-id>
network port broadcast-domain add-ports -broadcast-domain Infra-iSCSI-B -ports <st-
node01>:a0a-<infra-iscsi-b-vlan-id>


network port broadcast-domain add-ports -broadcast-domain Infra-iSCSI-A -ports <st-
node02>:a0a-<infra-iscsi-a-vlan-id>
network port broadcast-domain add-ports -broadcast-domain Infra-iSCSI-B -ports <st-
node02>:a0a-<infra-iscsi-b-vlan-id>
```

Procedure 22. Configure Time Synchronization on the Cluster

Step 1. Set the time zone for the cluster:

```
timezone -timezone <timezone>
```

Note: For example, in the eastern United States, the time zone is America/New_York.

Procedure 23. Configure Simple Network Management Protocol - SNMP

Step 1. Configure basic SNMP information, such as the location and contact. When polled, this information is visible as the `sysLocation` and `sysContact` variables in SNMP:

```
snmp contact <snmp-contact>
snmp location “<snmp-location>”
snmp init 1
options snmp.enable on
```

Step 2. Configure SNMP traps to send to remote hosts, such as an Active IQ Unified Manager server or another fault management system:

```
snmp traphost add <oncommand-um-server-fqdn>
```

Procedure 24. Configure SNMPv3 Access

Note: SNMPv3 offers advanced security by using encryption and passphrases. The SNMPv3 user can run SNMP utilities from the traphost using the authentication and privacy settings that you specify.

Step 1. Configure the SNMPv3 access by running the following command:

```
security login create -user-or-group-name <<snmp-v3-usr>> -application snmp -
authentication-method usm
```

Step 2. Enter the authoritative entity's EngineID [local EngineID]:

```
Which authentication protocol do you want to choose (none, md5, sha, sha2-256) [none]:
<<snmp-v3-auth-proto>>
Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]: <<snmpv3-priv-
proto>>

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```

Refer to the NetApp SNMP Configuration Express Guide for additional information when configuring SNMPv3 security users.

Procedure 25. Create an Infrastructure SVM

Step 1. Run the `vserver create` command:

```
vserver create -vserver Infra-SVM -rootvolume infra_svm_root -aggregate aggr1_node01 –
rootvolume-security-style unix
```

Note: It is recommended to remove iSCSI or FCP protocols if the protocol is not in use.

Step 2. Add the two data aggregates to the Infra-SVM aggregate list for the NetApp ONTAP Tools:

```
vserver modify -vserver Infra-SVM -aggr-list <aggr1_node01>,<aggr1_node02>
```

Step 3. Enable and run the NFS protocol in the Infra-SVM:

```
vserver nfs create -vserver Infra-SVM -udp disabled -v3 enabled -v4.1 enabled -vstorage
enabled
```

Note: If the NFS license was not installed during the cluster configuration, make sure to install the license before starting the NFS service.

Step 4. Verify the NFS vstorage parameter for the NetApp NFS VAAI plug-in was enabled:

```
VDI-A400::> vserver nfs show -fields vstorage

vserver   vstorage

--------- --------

Infra-SVM enabled
```

Procedure 26. Configure CIFS Servers

Note: You can enable and configure CIFS servers on storage virtual machines (SVMs) with NetApp FlexVol®□ volumes to let SMB clients access files on your cluster. Each data SVM in the cluster can be bound to exactly one Active Directory domain. However, the data SVMs do not need to be bound to the same domain. Each data SVM can be bound to a unique Active Directory domain.

Step 1. Configure the DNS for your SVM.

```
dns create -vserver Infra-SVM -domains <domain_name> -name-servers <dns_server_ip>
```

Note: The node management network interfaces should be able to route to the Active Directory domain controller to which you want to join the CIFS server. Alternatively, a data network interface must exist on the SVM that can route to the Active Directory domain controller.

Step 2. Create a network interface on the IB-MGMT VLAN:

```
network interface create -vserver Infra-SVM -lif <<svm_mgmt_lif_name>> -role data -data-
protocol none -home-node <<st-node-01>> -home-port a0a-<IB-MGMT-VLAN> -address <svm-
mgmt-ip> -netmask <svm-mgmt-mask> -failover-policy broadcast-domain-wide -firewall-
policy mgmt -auto-revert true
```

Step 3. Create the CIFS service:

```
vserver cifs create -vserver Infra-SVM -cifs-server Infra-CIFS -domain <domain.com>In
order to create an Active Directory machine account for the CIFS server, you must supply
the name and  password of a Windows account with sufficient privileges to add computers
to the "CN=Computers" container  within the"DOMAIN.COM" domain.

Enter the user name: Administrator@active_diectory.local

Enter the password:
```

Procedure 27. Modify Storage Virtual Machine Option

Note: NetApp ONTAP can use automatic node referrals to increase SMB client performance on SVMs with FlexVol volumes. This feature allows the SVM to automatically redirect a client request to a network interface on the node where the FlexVol volume resides.

Step 1. Run the following command to enable automatic node referrals on your SVM:

```
set -privilege advanced

vserver cifs options modify -vserver Infra-SVM -is-referral-enabled true
```

Procedure 28. Create Load-Sharing Mirrors of a SVM Root Volume

Step 1. Create a volume to be the load-sharing mirror of the infrastructure SVM root volume on each node:

```
volume create –vserver Infra-SVM –volume infra_svm_root_m01 –aggregate <aggr1_node01> –
size 1GB –type DP

volume create –vserver Infra-SVM –volume infra_svm_root_m02 –aggregate <aggr1_node02> –
size 1GB –type DP
```

Step 2. Create a job schedule to update the root volume mirror relationships every 15 minutes:

```
job schedule interval create -name 15min -minutes 15
```

Step 3. Create the mirroring relationships:

```
snapmirror create –source-path Infra-SVM:infra_svm_root -destination-path Infra-
SVM:infra_svm_root_m01 –type LS -schedule 15min


snapmirror create –source-path Infra-SVM:infra_svm_root –destination-path Infra-
SVM:infra_svm_root_m02 –type LS -schedule 15min

Initialize the mirroring relationship.

snapmirror initialize-ls-set –source-path Infra-SVM:infra_svm_root
```

Step 4. To verify, run the following:

```
VDI-A400::> snapmirror show -type ls

                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
VDI-A400://Infra-SVM/Infra_SVM_root
            LS   VDI-A400://Infra-SVM/infra_svm_root_m01
                              Snapmirrored
                                      Idle           -         true    -
                 VDI-A400://Infra-SVM/infra_svm_root_m02
                              Snapmirrored
                                      Idle           -         true    -
2 entries were displayed.
```

Procedure 29. Create FC Block Protocol Service -required only for FC configuration

Step 1. Run the following command to create the FCP service. This command also starts the FCP service and sets the worldwide name (WWN) for the SVM:

```
vserver fcp create -vserver Infra-SVM -status-admin up
```

Step 2. To verify, run the following:

```
VDI-A400::> vserver fcp show
                                        Status
Vserver     Target Name                 Admin
---------- ---------------------------- ------
Infra-SVM  20:00:d0:39:ea:29:ce:d4      up
```

Note: If the FC license was not installed during the cluster configuration, make sure to install the license before creating the FC service.

Procedure 30. Create iSCSI Block Protocol Service - required only for iSCSI configuration

Step 1. Run the following command to create the iSCSI service:

```
vserver iscsi create -vserver <infra-data-svm>
```

Step 2. To verify, run the following:

```
VDI-A400::> vserver iscsi show
           Target                           Target                       Status
Vserver    Name                             Alias                        Admin
---------- -------------------------------- ---------------------------- ------
Infra-SVM  iqn.1992-08.com.netapp:sn.63144a05ad1211eb8a7ad039ea29d44a:vs.3
                                            Infra-SVM                    up
```

Note: If the iSCSI license was not installed during the cluster configuration, make sure to install the license before creating the iSCSI service.

Procedure 31. Vserver Protocol Verification

Step 1. Verify the protocols are added to the Infra vserver by running the following:

```
VDI-A400::> vserver show-protocols -vserver Infra-SVM
  Vserver: Infra-SVM
Protocols: nfs, fcp, iscsi, ndmp, nvme
```

Step 2. If a protocol is not present, use the following command to add the protocol to the vserver:

```
vserver add-protocols -vserver <infra-data-svm>  -protocols < iscsi or fcp >
```

Procedure 32. Configure HTTPS Access to the Storage Controller

Step 1. Increase the privilege level to access the certificate commands:

```
set -privilege diag
Do you want to continue? {y|n}: y
```

Step 2. Generally, a self-signed certificate is already in place. Verify the certificate and obtain parameters (for example, the <serial-number>) by running the following command:

```
security certificate show
```

Step 3. For each SVM shown, the certificate common name should match the DNS fully qualified domain name (FQDN) of the SVM. Delete the two default certificates and replace them with either self-signed certificates or certificates from a certificate authority (CA). To delete the default certificates, run the following commands:

```
security certificate delete -vserver Infra-SVM -common-name Infra-SVM -ca Infra-SVM -
type server -serial <serial-number>
```

Step 4. Deleting expired certificates before creating new certificates is a best practice. Run the `security certificate delete command` to delete the expired certificates. In the following command, use TAB completion to select and delete each default certificate.

Step 5. To generate and install self-signed certificates, run the following commands as one-time commands. Generate a server certificate for the Infra-SVM and the cluster SVM. Use TAB completion to aid in the completion of these commands:

```
security certificate create -common-name <cert-common-name> -type  server -size 2048 -
country <cert-country> -state <cert-state> -locality <cert-locality> -organization
<cert-org> -unit <cert-unit> -email-addr <cert-email> -expire-days <cert-days> -protocol
SSL -hash-function SHA256 -vserver Infra-SVM
```

Step 6. To obtain the values for the parameters required in step 5 (<cert-ca> and <cert-serial>), run the security certificate show command.

Step 7. Enable each certificate that was just created by using the –server-enabled true and –client-enabled false parameters. Use TAB completion to aid in the completion of these commands:

```
security ssl modify -vserver <clustername> -server-enabled true -client-enabled false -
ca <cert-ca> -serial <cert-serial> -common-name <cert-common-name>
```

Step 8. Disable HTTP cluster management access:

```
system services firewall policy delete -policy mgmt -service http –vserver <clustername>
```

Note: It is normal for some of these commands to return an error message stating that the entry does not exist.

Step 9. Return to the normal admin privilege level and verify that the system logs are available in a web browser:

```
set –privilege admin
```

```
https://<node01-mgmt-ip>/spi
https://<node02-mgmt-ip>/spi
```

Procedure 33. Configure NFSv3 and NFSv4.1

Step 1. Create a new rule for the infrastructure NFS subnet in the default export policy:

```
vserver export-policy rule create –vserver Infra-SVM -policyname default –ruleindex 1 –
protocol nfs -clientmatch <infra-nfs-subnet-cidr> -rorule sys –rwrule sys -superuser sys
–allow-suid true
```

Step 2. Assign the FlexPod export policy to the infrastructure SVM root volume:

```
volume modify –vserver Infra-SVM –volume infra_svm_root –policy default
```

Procedure 34. Create CIFS Export Policy

Note: Optionally, you can use export policies to restrict CIFS access to files and folders on CIFS volumes. You can use export policies in combination with share level and file level permissions to determine effective access rights.

Step 1. Run the following command to create an export policy that limits access to devices in the domain:

```
export-policy create -vserver Infra-SVM -policyname cifs
```

```
export-policy rule create -vserver Infra-SVM -policyname cifs -clientmatch <domain_name>
-rorule
```

```
krb5i,krb5p -rwrule krb5i,krb5p
```

Procedure 35. Create a NetApp FlexVol Volume

The following information is required to create a NetApp FlexVol volume:

- The volume name
- The volume size

- The aggregate on which the volume exists

Step 1. Run the following commands:

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate <aggr1_node01> -
size 1TB -state online -policy default -junction-path /infra_datastore_01 -space-
guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate <aggr1_node02> -
size 1TB -state online -policy default -junction-path /infra_datastore_02 -space-
guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume infra_swap -aggregate <aggr1_node01> -size
100GB -state online -policy default -junction-path /infra_swap -space-guarantee none -
percent-snapshot-space 0 -snapshot-policy none.

volume create -vserver Infra-SVM -volume esxi_boot -aggregate <aggr1_node01> -size 320GB
-state online -policy default -space-guarantee none -percent-snapshot-space 0

snapmirror update-ls-set -source-path Infra-SVM:infra_svm_root
```

Step 2. If you are going to setup and use SnapCenter to backup the infra_datastore volume, add "-snapshot-policy none" to the end of the volume create command for the infra_datastore volume.

Procedure 36. Create a NetApp FlexGroup Volume

Tech tip

A FlexGroup volume is a scale-out NAS container that provides high performance along with automatic load distribution and scalability. A FlexGroup Volume contains several constituents that automatically and transparently share the traffic. A FlexGroup volume is a single namespace container that can be managed in a similar way as FlexVol volumes.

Step 1. Run the following commands to create FlexGroup volumes:

```
volume create -vserver Infra-SVM -volume cifs_vol_01 -aggr-list
aggr01_node01,aggr01_node02-aggr-list-multiplier4-state online -policy cifs_policy -size
800GB -junction-path /cifs_vol_01 -space-guarantee none -percent-snapshot-space 0


volume create -vserver Infra-SVM -volume cifs_vol_02 -aggr-list
aggr01_node01,aggr01_node02-aggr-list-multiplier4-state online -policy cifs_policy -size
800GB -junction-path /cifs_vol_02 -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume cifs_vol_03 -aggr-list
aggr01_node01,aggr01_node02-aggr-list-multiplier4-state online -policy cifs_policy -size
800GB -junction-path /cifs_vol_03 -space-guarantee none -percent-snapshot-space 0
```

Procedure 37. Modify Volume Efficiency

Step 1. On NetApp AFF systems, deduplication is enabled by default. To disable the efficiency policy on the infra_swap volume, run the following command:

```
volume efficiency off -vserver Infra-SVM -volume infra_swap
```

Procedure 38. Create CIFS Shares

Note: A CIFS share is a named access point in a volume that enables CIFS clients to view, browse, and manipulate files on a file server.

Step 1. Run the following commands to create CIFS shares:

```
cifs share create -vserver Infra-SVM -share-name <CIFS_share_1> -path
/infra_datastore_01 -share properties oplocks,browsable,continuously-
available,showsnapshot
```

```
cifs share create -vserver Infra-SVM -share-name <CIFS_share_2> -path
/infra_datastore_02 -share properties oplocks,browsable,continuously-
available,showsnapshot
```

```
cifs share create -vserver Infra-SVM -share-name <CIFS_share_3> -path /cifs_vol_03 -
share properties oplocks,browsable,continuously-available,showsnapshot
```

Procedure 39. Create NFS LIFs

Step 1. Run the following commands to create NFS LIFs:

```
network interface create -vserver Infra-SVM -lif nfs-lif-01 -role data -data-protocol
       nfs -home-node <st-node01> -home-port a0a-<infra-nfs-vlan-id> –address <node01-
nfs-lif-01-ip> -netmask <node01-nfs-lif-01-mask> -status-admin up –failover-policy
broadcast-domain-wide –firewall-policy data –auto-revert true


network interface create -vserver Infra-SVM -lif nfs-lif-02 -role data -data-protocol
nfs -home-node <st-node02> -home-port a0a-<infra-nfs-vlan-id> –address <node02-nfs-lif-
02-ip> -netmask <node02-nfs-lif-02-mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
```

Step 2. Run the following commands to verify:

```
VDI-A400::> network interface show -vserver Infra-SVM -data-protocol nfs
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Infra-SVM
            nfs-lif-01   up/up    192.168.30.1/24    VDI-A400-01  a0a-62
                                                                           true
            nfs-lif-02   up/up    192.168.30.2/24    VDI-A400-02  a0a-62
                                                                           true
2 entries were displayed.
```

Procedure 40. Create CIFS LIFs

Step 1. Run the following commands to create CIFS LIFs:

```
network interface create -vserver Infra-SVM -lif cifs_lif01 -role data -data-protocol
cifs -home-node <st-node01> -home-port a0a-<infra-cifs-vlan-id> -address <node01-
cifs_lif01-ip> -netmask <node01-cifs_lif01-mask> -status-admin up –failover-policy
broadcast-domain-wide –firewall-policy data –auto-revert true
```

```
network interface create -vserver Infra-SVM -lif cifs_lif02 -role data -data-protocol
cifs -home-node <st-node02> -home-port a0a-<infra-cifs-vlan-id> -address <node02-
cifs_lif02-ip> -netmask <node02-cifs_lif02-mask>> -status-admin up –failover-policy
broadcast-domain-wide –firewall-policy data –auto-revert true
```

Procedure 41. Create FC LIFs - required only for FC configuration

Step 1. Run the following commands to create four FC LIFs (two on each node):

```
network interface create -vserver Infra-SVM -lif fcp-lif-01a -role data -data-protocol
fcp -home-node <st-node01> -home-port 1a –status-admin up
```

```
network interface create -vserver Infra-SVM -lif fcp-lif-01b -role data -data-protocol
fcp -home-node <st-node01> -home-port 1b –status-admin up
```

```
network interface create -vserver Infra-SVM -lif fcp-lif-02a -role data -data-protocol
fcp -home-node <st-node02> -home-port 1a –status-admin up
```

```
network interface create -vserver Infra-SVM -lif fcp-lif-02b -role data -data-protocol
fcp -home-node <st-node02> -home-port 1b        –status-admin up
```

Step 2. Run the following commands to verify:

```
VDI-A400::> network interface show -vserver Infra-SVM -data-protocol fcp
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Infra-SVM
            fcp-lif-01a  up/up    20:01:d0:39:ea:29:ce:d4
                                                     VDI-A400-01  1a      true
            fcp-lif-01b  up/up    20:02:d0:39:ea:29:ce:d4
                                                     VDI-A400-01  1b      true
            fcp-lif-02a  up/up    20:03:d0:39:ea:29:ce:d4
                                                     VDI-A400-02  1a      true
            fcp-lif-02b  up/up    20:04:d0:39:ea:29:ce:d4
                                                     VDI-A400-02  1b      true
4 entries were displayed.
```

Procedure 42. Create iSCSI LIFs - required only for iSCSI configuration

Step 1. To create four iSCSI LIFs, run the following commands (two on each node):

```
network interface create -vserver <infra-data-svm> -lif iscsi-lif-01a -role data -data-
protocol iscsi -home-node <st-node01> -home-port a0a-<infra-iscsi-a-vlan-id> -address
<st-node01-infra-iscsi-a-ip> -netmask <infra-iscsi-a-mask> -status-admin up
```

```
network interface create -vserver <infra-data-svm> -lif iscsi-lif-01b -role data -data-
protocol iscsi -home-node <st-node01> -home-port a0a-<infra-iscsi-b-vlan-id> -address
<st-node01-infra-iscsi-b-ip> -netmask <infra-iscsi-b-mask> –status-admin up
```

```
network interface create -vserver <infra-data-svm> -lif iscsi-lif-02a -role data -data-
protocol iscsi -home-node <st-node02> -home-port a0a-<infra-iscsi-a-vlan-id> -address
<st-node02-infra-iscsi-a-ip> -netmask <infra-iscsi-a-mask> –status-admin up
```

```
network interface create -vserver <infra-data-svm> -lif iscsi-lif-02b -role data -data-
protocol iscsi -home-node <st-node02> -home-port a0a-<infra-iscsi-b-vlan-id> -address
<st-node02-infra-iscsi-b-ip> -netmask <infra-iscsi-b-mask> –status-admin up
```

Procedure 43. Configure FC-NVMe Datastore for vSphere 7U3 on existing SVM - Infra-SVM - for FC-NVMe configuration only

Note: To Configure FC-NVMe Datastores for vSphere 7U3, enable the FC-NVMe protocol on an existing SVM or create a separate SVM for FC-NVMe workloads. In this deployment, Infra-SVM was used for FC-NVMe datastore configuration.

Step 1. Verify NVMe Capable adapters are installed in the cluster:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

Step 2. Add the NVMe protocol to the SVM and list it:

```
vserver add-protocols -vserver Infra-SVM  -protocols nvme
```

Step 3. To verify, run the following:

```
VDI-A400::> vserver show -vserver Infra-SVM -fields allowed-protocols
vserver   allowed-protocols
--------- -----------------------
Infra-SVM nfs,fcp,iscsi,ndmp,nvme
```

Step 4. Create NVMe service:

```
vserver nvme create -vserver Infra-SVM
```

Step 5. To verify, run the following:

```
VDI-A400::> vserver nvme show -vserver Infra-SVM
          Vserver Name: Infra-SVM
Administrative Status: up
```

Step 6. Create NVMe FC LIFs:

```
network interface create -vserver Infra-SVM -lif fc-nvme-lif-01a -role data -data-protocol fc-nvme -home-node <st-node01> -home-port 1a –status-admin up

network interface create -vserver Infra-SVM -lif fc-nvme-lif-01b -role data -data-protocol fc-nvme -home-node <st-node01> -home-port 1b –status-admin up

network interface create -vserver Infra-SVM -lif fcp-nvme-lif-02a -role data -data-protocol fc-nvme -home-node <st-node02> -home-port 1a –status-admin up

network interface create -vserver Infra-SVM -lif fcp-nvme-lif-02b -role data -data-protocol fc-nvme -home-node <st-node02> -home-port 1b –status-admin up
```

Step 7. To verify, run the following:

```
VDI-A400::> network interface show -vserver Infra-SVM -data-protocol fc-nvme
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Infra-SVM
            fc-nvme-lif-01a
                         up/up    20:06:d0:39:ea:29:ce:d4
                                                     VDI-A400-01   1b      true
            fc-nvme-lif-01b
                         up/up    20:08:d0:39:ea:29:ce:d4
                                                     VDI-A400-01   1a      true
            fc-nvme-lif-02a
                         up/up    20:07:d0:39:ea:29:ce:d4
                                                     VDI-A400-02   1b      true
            fc-nvme-lif-02b
                         up/up    20:09:d0:39:ea:29:ce:d4
                                                     VDI-A400-02   1a      true
```

Note: You can only configure two NVMe LIFs per node on a maximum of four nodes.

Step 8. Create volume:

```
vol create -vserver Infra-SVM -volume NVMe_Datastore_01 -aggregate
VDI_A400_01_NVME_SSD_1 -size 500G -state online -space-guarantee none -percent-snapshot-space 0
```

Procedure 44. Add Infrastructure SVM Administrator and SVM Administration LIF to In-band Management Network

Step 1. Run the following commands:

```
network interface create –vserver Infra-SVM –lif svm-mgmt –role data –data-protocol none
–home-node <st-node02> -home-port  a0a-<ib-mgmt-vlan-id> –address <svm-mgmt-ip> –netmask
<svm-mgmt-mask> -status-admin up –failover-policy broadcast-domain-wide –firewall-policy
mgmt –auto-revert true
```

Step 2. Create a default route that enables the SVM management interface to reach the outside world:

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 –gateway <svm-mgmt-gateway>
```

Step 3. To verify, run the following:

```
VDI-A400::> network route show -vserver Infra-SVM

Vserver             Destination     Gateway         Metric

------------------- --------------- --------------- ------

Infra-SVM

                    0.0.0.0/0       192.168.17.254  20
```

Step 4. Set a password for the SVM vsadmin user and unlock the user:

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password:  <password>
Enter it again:  <password>


security login unlock –username vsadmin –vserver Infra-SVM
```

A cluster serves data through at least one and possibly several SVMs. By completing these steps, you have created a single data SVM. You can create additional SVMs depending on their requirement.

Procedure 45. Configure and Test AutoSupport

Note: NetApp AutoSupport sends support summary information to NetApp through HTTPS.

Step 1. To configure AutoSupport, run the following command:

```
system node autosupport modify -node * -state enable –mail-hosts <mailhost> -transport
https -support enable -noteto <storage-admin-email>
```

Step 2. Test the AutoSupport configuration by sending a message from all nodes of the cluster:

```
autosupport invoke -node * -type all -message “FlexPod storage configuration completed”
```

Below is the configuration information that was modified from the platform guide to validate this solution:

- 32 Gbps HBA on slot 1 which was used for boot from SAN using FC. It can also be used for NVMe when required. By default, it stays in initiator type. You will need to change the type to target for the fcp adapter to be listed under network ports:

  ```
  system node hardware unified-connect modify -node * -adapter <adapter-port>
  ```

- 3 FlexVol volumes are created for hosting virtual desktops, PVS share, and SMB share:

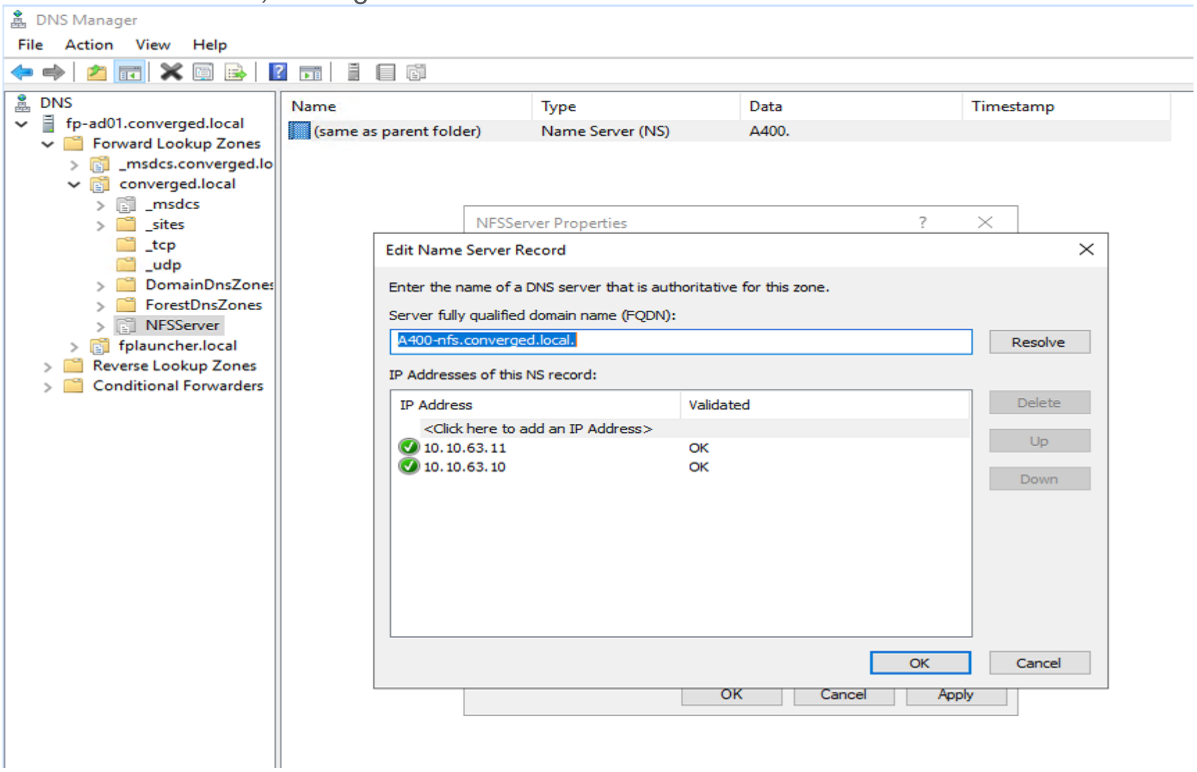
  ```
  volume create -server <vserver> -volume <volumename> -aggr-list <aggr-node-01>,<aggr-node-
  ```

```
02> -aggr-list-multiplier <number_of_member_volume/aggr> -size <allocation_size> -security-
style <unix/ntfs> -qos-adaptive-policy-group <aqos_policy>
```

Name	Number of Members	Size	Adaptive QoS Policy	Expected IOPS (2048 * Allocated Space)	Peak IOPS (4096 * Used Space)
VDI	8	30TB (12% used)	performance	61440	14745.6
Data	8	10TB (25% used)	performance	20480	10240

For NFS, the DNS Load balancing feature was used and is available on ONTAP. (physical, interface groups, and VLANs). With DNS load balancing, LIFs are associated with the load balancing zone of an SVM. A site-wide DNS server is configured to forward all DNS requests and return the least-loaded LIF based on the network traffic and the availability of the port resources (CPU usage, throughput, open connections, and so on). DNS load balancing provides the following benefits:

- New client connections balanced across available resources.
- No manual intervention required for deciding which LIFs to use when mounting a particular SVM.
- DNS load balancing supports NFSv3, NFSv4, NFSv4.1, CIFS, SMB 2.0, SMB 2.1, and SMB 3.0.
- network interface modify -vserver <vserver_name> -lif <lif_name> -dns-zone <zone_name>
  for example, network interface modify -vserver Infra-FC -lif NFS-1-A400-01 -dns-zone nfsserver.converged.local
  On AD domain, a delegation was created for the subdomain.



Name	Type	Data	Timestamp
(same as parent folder)	Name Server (NS)	A400.	

Edit Name Server Record

Enter the name of a DNS server that is authoritative for this zone.

Server fully qualified domain name (FQDN): A400-nfs.converged.local.

IP Addresses of this NS record:

IP Address	Validated
<Click here to add an IP Address>	
10.10.63.11	OK
10.10.63.10	OK

Cisco Intersight Managed Mode Configuration

This chapter contains the following:

- Cisco Intersight Managed Mode on Cisco UCS Fabric Interconnects
- Configure a Cisco UCS Domain Profile
- UCS Domain Configuration
- Configure Cisco UCS Chassis Profile
- Configure Server Profile Template
- Management Configuration
- FlexPod Cisco MDS Switch Configuration

The Cisco Intersight platform is a management solution delivered as a service with embedded analytics for Cisco and third-party IT infrastructures. The Cisco Intersight managed mode (also referred to as Cisco IMM or Intersight managed mode) is a new architecture that manages Cisco Unified Computing System (Cisco UCS) fabric interconnect-attached systems through a Redfish-based standard model. Cisco Intersight managed mode standardizes both policy and operation management Cisco UCS B200 M6 compute nodes used in this deployment guide.

Cisco Intersight Managed Mode on Cisco UCS Fabric Interconnects

This subject contains the following procedures:

- Set up Cisco Intersight Managed Mode on Cisco UCS Fabric Interconnects
- Set up a new Cisco Intersight account
- Set up Cisco Intersight account and associate it with Cisco Smart Licensing
- Set up Cisco Intersight Resource Group
- Set up Cisco Intersight Organization
- Claim Cisco UCS Fabric Interconnects in Cisco Intersight
- Verify the addition of Cisco UCS fabric interconnects to Cisco Intersight

Note: Cisco UCS C-Series M6 servers, connected and managed through Cisco UCS FIs, are also supported by IMM. For a complete list of supported platforms, visit: https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide/b_intersight_managed_mode_guide_chapter_01010.html

Procedure 1. Set up Cisco Intersight Managed Mode on Cisco UCS Fabric Interconnects

Note: The Cisco UCS fabric interconnects need to be set up to support Cisco Intersight managed mode. When converting an existing pair of Cisco UCS fabric interconnects from Cisco UCS Manager mode to Intersight Mange Mode (IMM), first erase the configuration and reboot your system.

WARNING! Converting fabric interconnects to Cisco Intersight managed mode is a disruptive process, and configuration information will be lost. You are encouraged to make a backup of their existing configuration.

Step 1. Configure Fabric Interconnect A (FI-A). On the Basic System Configuration Dialog screen, set the management mode to Intersight. All the remaining settings are similar to those for the Cisco UCS Manager managed mode (UCSM-Managed).

```
Cisco UCS Fabric Interconnect A
To configure the Cisco UCS for use in a FlexPod environment in intersight managed mode, follow these steps:
```

Step 2. Connect to the console port on the first Cisco UCS fabric interconnect.

```
  Enter the configuration method. (console/gui) ? console

  Enter the management mode. (ucsm/intersight)? intersight

  You have chosen to setup a new Fabric interconnect in "intersight" managed mode. Continue? (y/n): y

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

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

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

  Enter the system name:  <ucs-cluster-name>

  Physical Switch Mgmt0 IP address : <ucsa-mgmt-ip>

  Physical Switch Mgmt0 IPv4 netmask : <ucsa-mgmt-mask>

  IPv4 address of the default gateway : <ucsa-mgmt-gateway>

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

    DNS IP address : <dns-server-1-ip>

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

    Default domain name : <ad-dns-domain-name>
<SNIP>

  Verify and save the configuration.
```

Step 3. After applying the settings, make sure you can ping the fabric interconnect management IP address. When Fabric Interconnect A is correctly set up and is available, Fabric Interconnect B will automatically discover Fabric Interconnect A during its setup process as shown in the next step.

Step 4. Configure Fabric Interconnect B (FI-B). For the configuration method, choose console. Fabric Interconnect B will detect the presence of Fabric Interconnect A and will prompt you to enter the admin password for Fabric Interconnect A. Provide the management IP address for Fabric Interconnect B and apply the configuration.

```
Cisco UCS Fabric Interconnect A
Enter the configuration method. (console/gui) ? console

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

  Enter the admin password of the peer Fabric interconnect: <password>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <ucsa-mgmt-ip>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <ucsa-mgmt-mask>

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

  Physical Switch Mgmt0 IP address : <ucsb-mgmt-ip>

  Local fabric interconnect model(UCS-FI-6454)
  Peer fabric interconnect is compatible with the local fabric interconnect. Continuing with the installer...

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

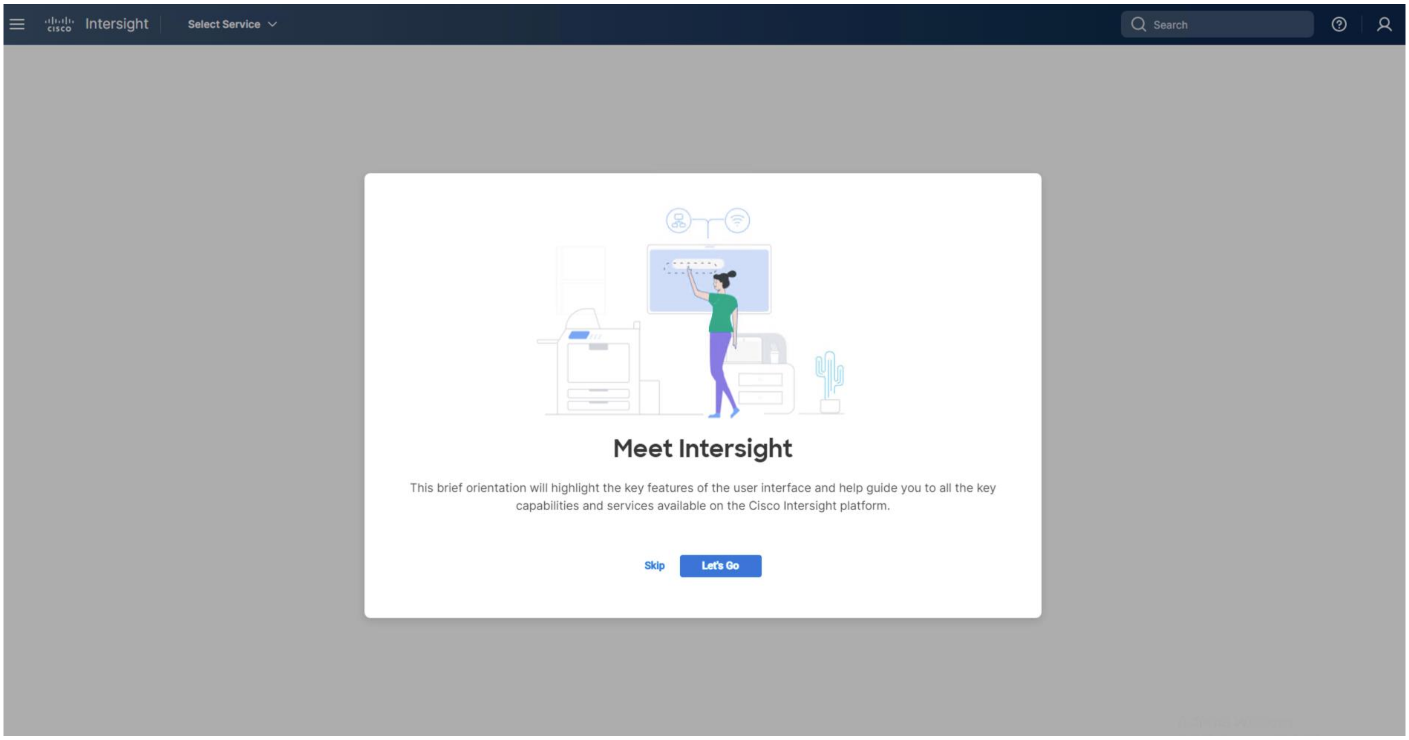
Procedure 2. Set up a new Cisco Intersight account

Step 1. Go to https://intersight.com and click **Create an account**.

Step 2. Read and accept the license agreement. Click **Next**.

Step 3. Provide an Account Name and click **Create**.

On successful creation of the Intersight account, following page will be displayed:



Meet Intersight

This brief orientation will highlight the key features of the user interface and help guide you to all the key capabilities and services available on the Cisco Intersight platform.

Note: You can also choose to add the Cisco UCS FIs to an existing Cisco Intersight account.

Procedure 3. Set up Cisco Intersight account and associate it with Cisco Smart Licensing

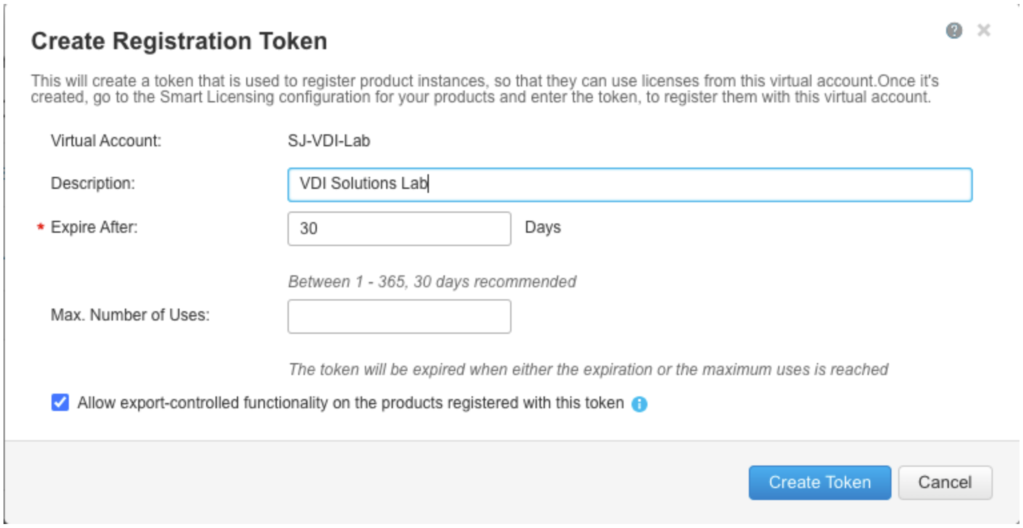
Note: When setting up a new Cisco Intersight account (as described in this document), the account needs to be enabled for Cisco Smart Software Licensing.

Step 1. Log into the Cisco Smart Licensing portal: https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#module/SmartLicensing.

Step 2. Verify that the correct virtual account is selected.

Step 3. Under **Inventory > General**, generate a new token for product registration.

Step 4. Copy this newly created token.



Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account.Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: SJ-VDI-Lab

Description: VDI Solutions Lab

* Expire After: 30 Days

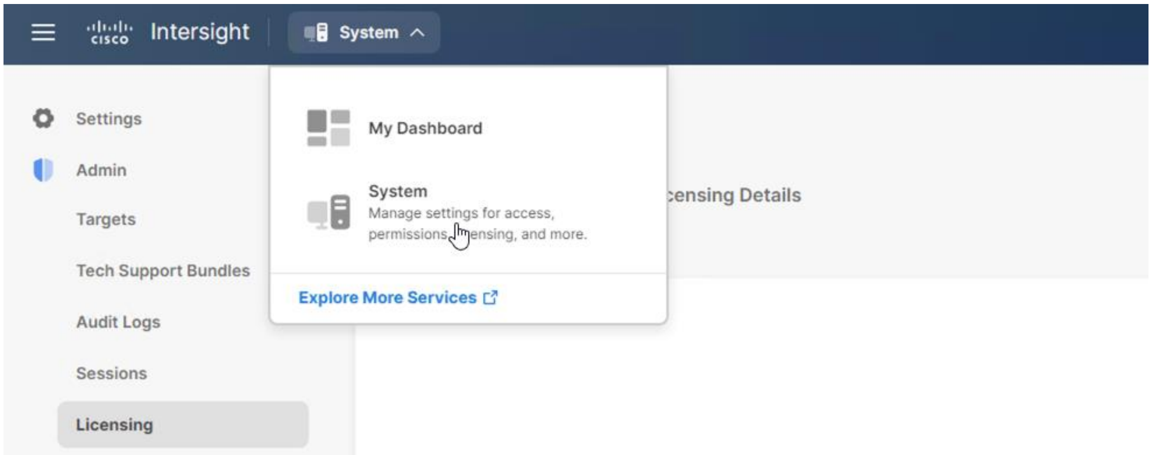
Between 1 - 365, 30 days recommended

Max. Number of Uses:

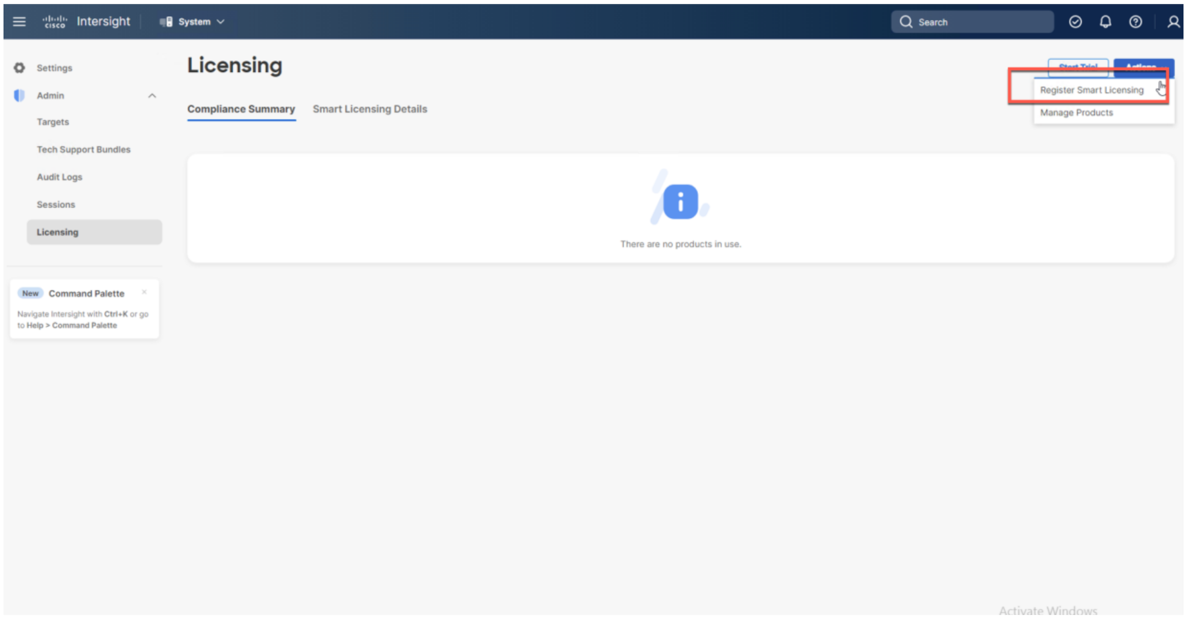
The token will be expired when either the expiration or the maximum uses is reached

☑ Allow export-controlled functionality on the products registered with this token

Step 5. Log into the Cisco Intersight portal and click the **drop-down list** in the top-left corner. Click **System**.



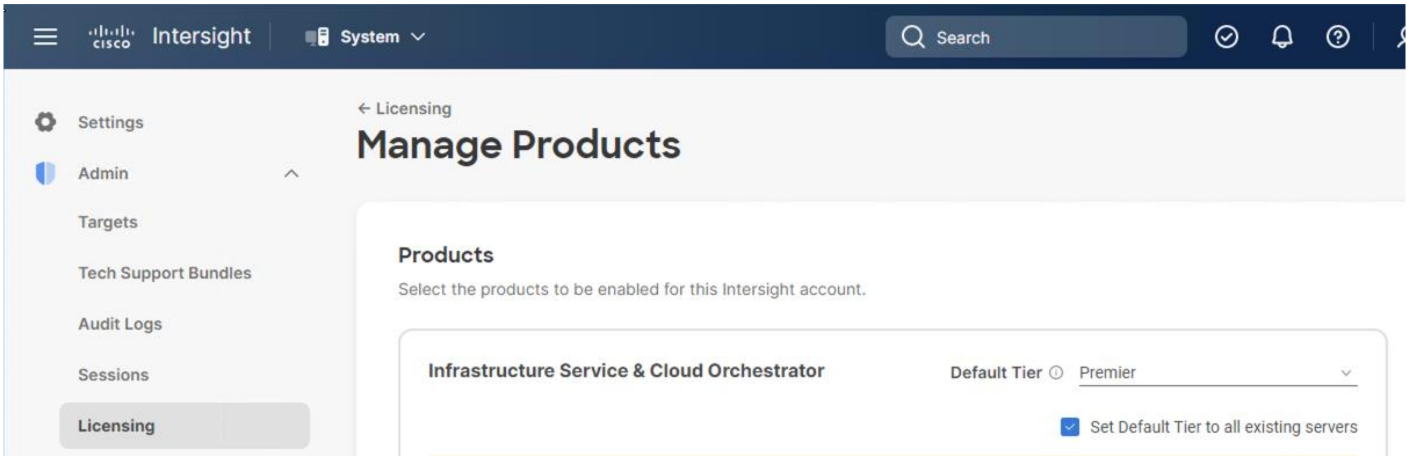
Step 6. Under **Cisco Intersight** > **Licensing**, click **Register**.



Step 7. Enter the copied token from the Cisco Smart Licensing portal. Click **Next**.

Step 8. From the drop-down list, select the pre-selected Default Tier * and select the license type (for example, Premier).

Step 9. Select **Move All Servers to Default Tier**.



Manage Products

Products

Select the products to be enabled for this Intersight account.

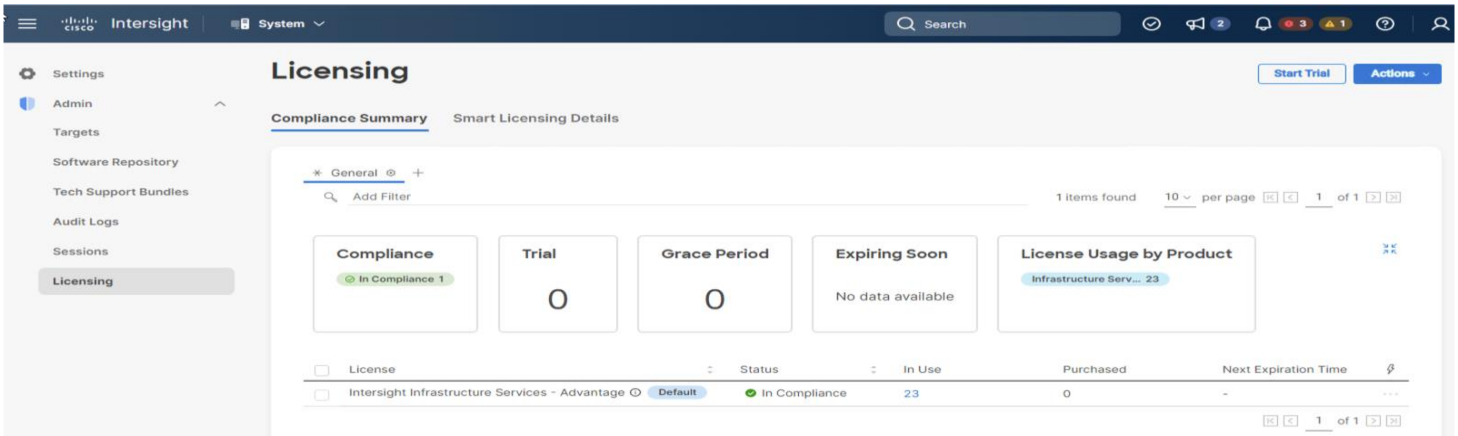
Infrastructure Service & Cloud Orchestrator

Default Tier: Premier

☑ Set Default Tier to all existing servers

Step 10. Click **Proceed**.

When the registration is successful (takes a few minutes), the information about the associated Cisco Smart account and default licensing tier selected in the last step is displayed.



Licensing

Compliance	Trial	Grace Period	Expiring Soon	License Usage by Product
In Compliance 1	0	0	No data available	Infrastructure Serv... 23

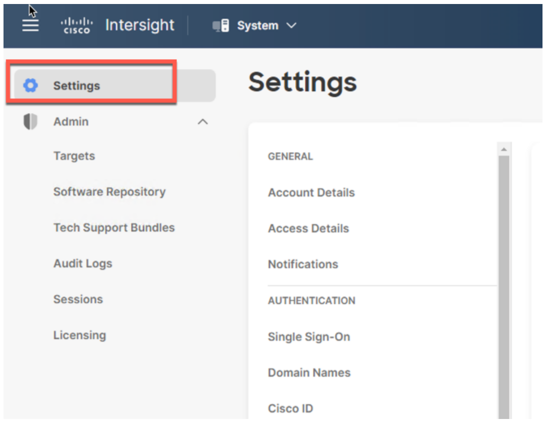
License	Status	In Use	Purchased	Next Expiration Time
Intersight Infrastructure Services - Advantage Default	In Compliance	23	0	-

Procedure 4.Set up Cisco Intersight Resource Group

Note: In this step, a Cisco Intersight resource group is created where resources such as targets will be logically grouped. In this deployment, a single resource group is created to host all the resources, but customers can choose to create multiple resource groups for granular control of the resources.

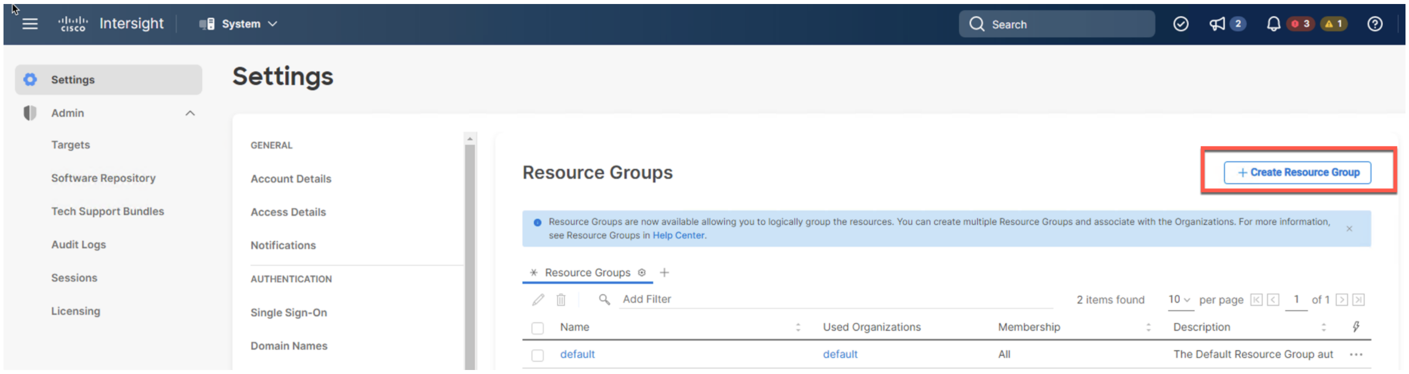
Step 1. Log into **Cisco Intersight**.

Step 2. Click **Settings** (the gear icon) and click **Settings**.



Step 3. Click **Resource Groups** in the middle panel.

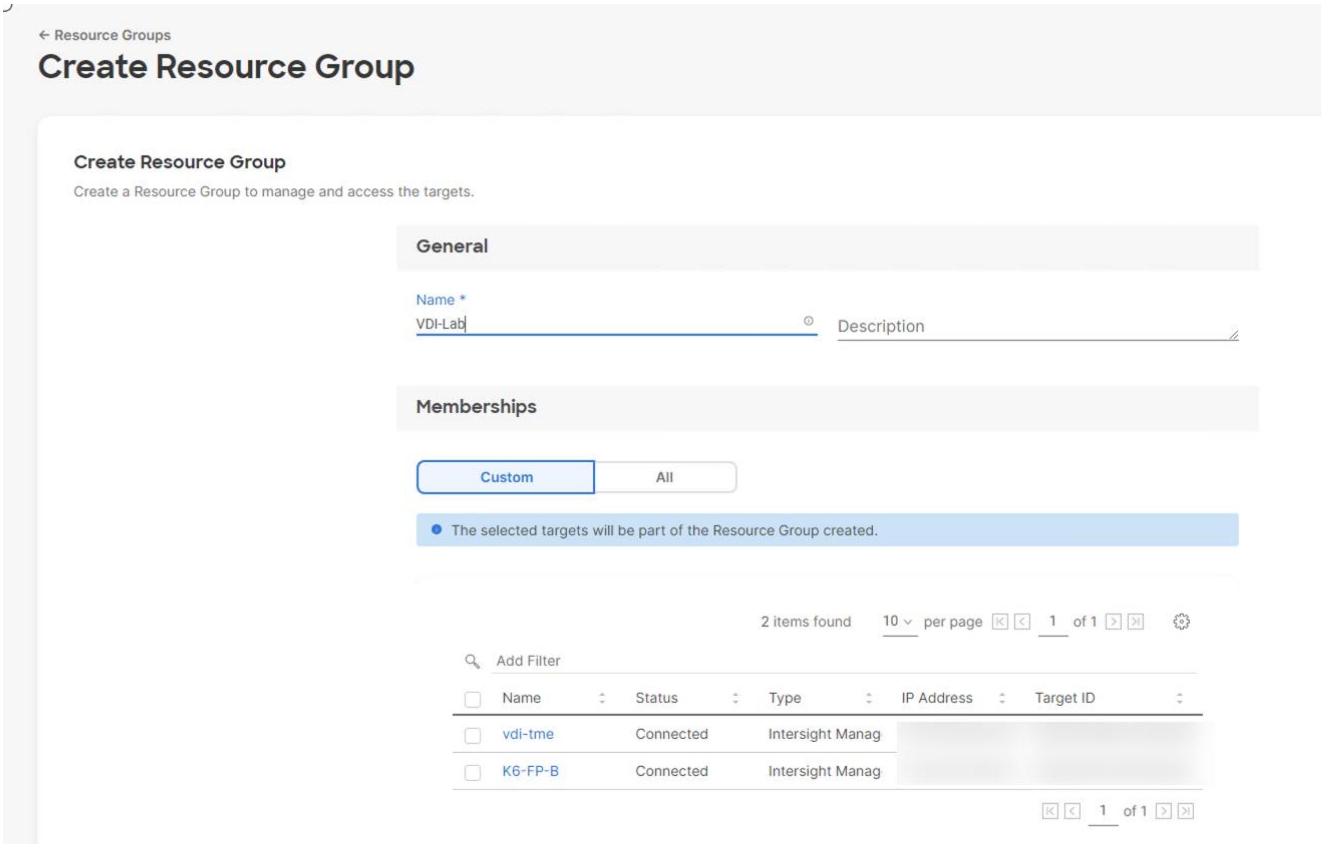
Step 4. Click **+ Create Resource Group** in the top-right corner.



Resource Groups are now available allowing you to logically group the resources. You can create multiple Resource Groups and associate with the Organizations. For more information, see Resource Groups in Help Center.

Name	Used Organizations	Membership	Description
default	default	All	The Default Resource Group aut

Step 5. Provide a name for the Resource Group (for example, VDI-Lab).



← Resource Groups

Create Resource Group

Create Resource Group

Create a Resource Group to manage and access the targets.

General

Name *: VDI-Lab

Description

Memberships

Custom | All

The selected targets will be part of the Resource Group created.

2 items found 10 per page 1 of 1

Add Filter

Name	Status	Type	IP Address	Target ID
vdi-tme	Connected	Intersight Manag	[redacted]	[redacted]
K6-FP-B	Connected	Intersight Manag	[redacted]	[redacted]

1 of 1

Step 6. Under Memberships, click **Custom**.

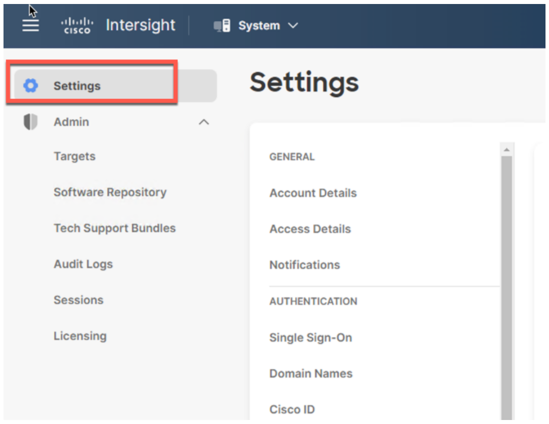
Step 7. Click **Create**.

Procedure 5. Set up Cisco Intersight Organization

Note: In this step, a Cisco Intersight organization is created where all Cisco Intersight managed mode configurations including policies are defined.

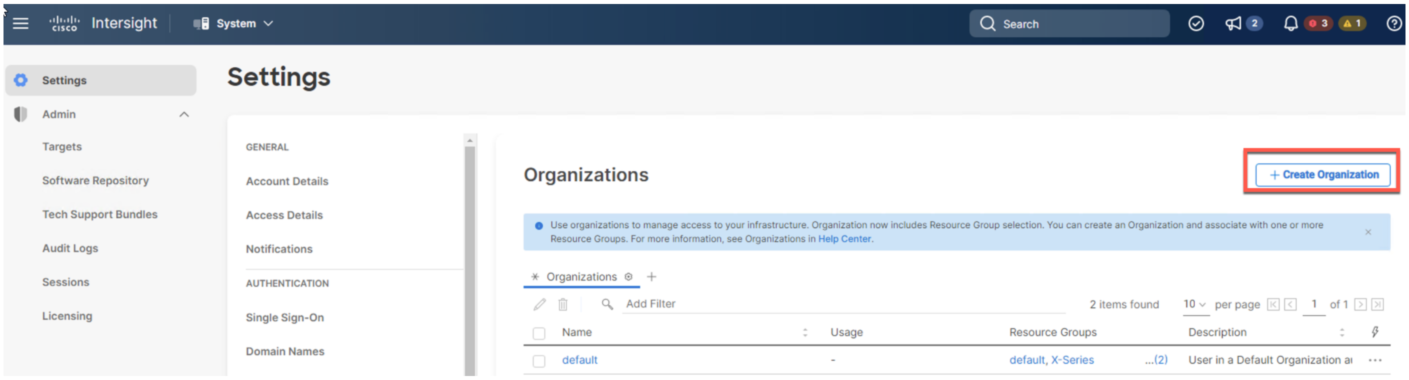
Step 1. Log into the Cisco Intersight portal.

Step 2. Click **Settings** (the gear icon) and choose **Settings**.



Step 3. Click **Organizations** in the middle panel.

Step 4. Click **+ Create Organization** in the top-right corner.



Settings

Organizations

Use organizations to manage access to your infrastructure. Organization now includes Resource Group selection. You can create an Organization and associate with one or more Resource Groups. For more information, see Organizations in Help Center.

Organizations

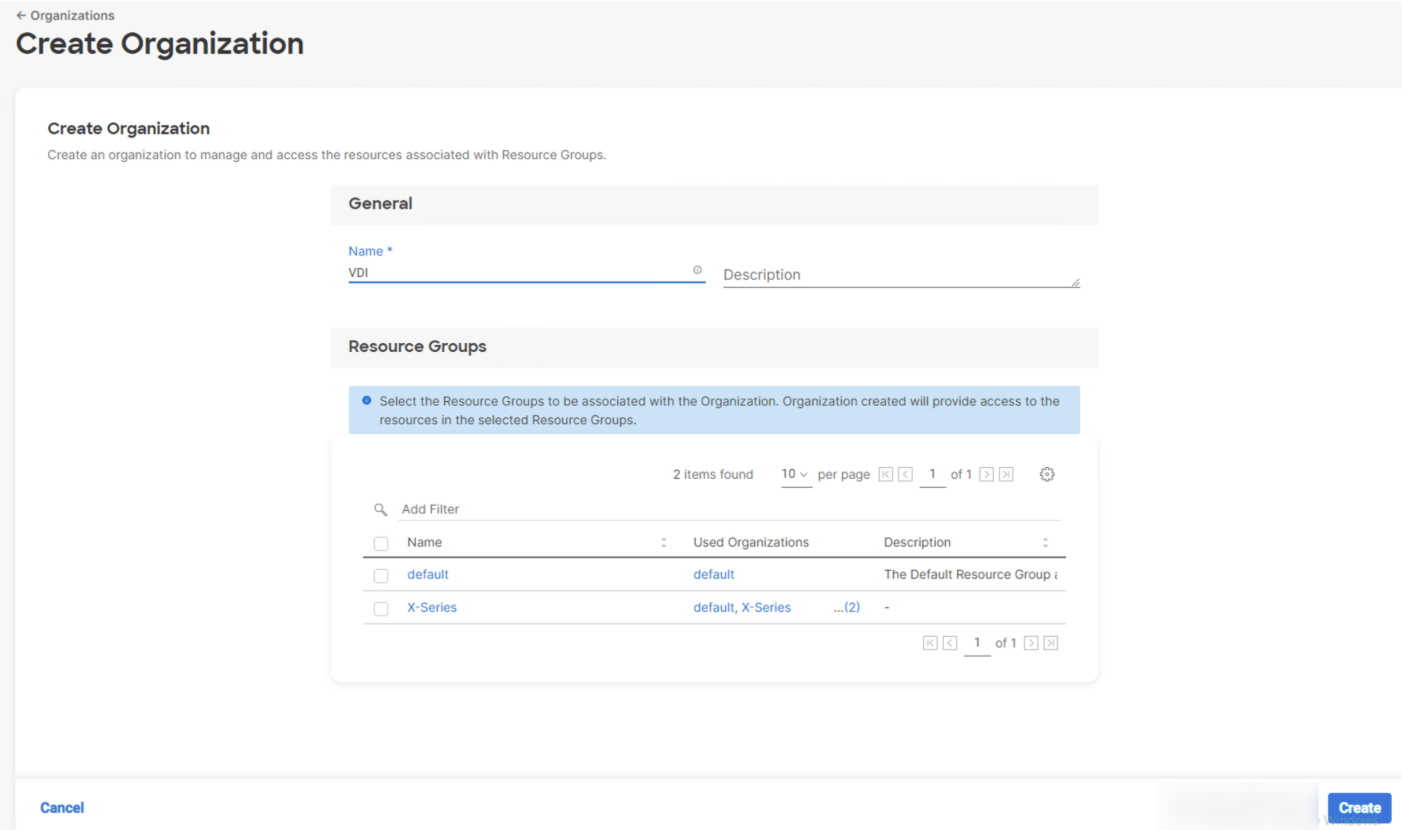
Add Filter — 2 items found — 10 per page — 1 of 1

Name	Usage	Resource Groups	Description
default	-	default, X-Series ...(2)	User in a Default Organization a

Step 5. Provide a name for the organization (for example, VDI).

Step 6. Select the Resource Group created in the last step (for example, VDI Lab).

Step 7. Click **Create.**



Create Organization

Create Organization

Create an organization to manage and access the resources associated with Resource Groups.

General

Name *: VDI

Description

Resource Groups

Select the Resource Groups to be associated with the Organization. Organization created will provide access to the resources in the selected Resource Groups.

2 items found — 10 per page — 1 of 1

Add Filter

Name	Used Organizations	Description
default	default	The Default Resource Group a
X-Series	default, X-Series ...(2)	-

Procedure 6. Claim Cisco UCS Fabric Interconnects in Cisco Intersight

Note: Make sure the initial configuration for the fabric interconnects has been completed. Log into Fabric Interconnect A using a web browser to capture the Cisco Intersight connectivity information.

Step 1. Use the management IP address of Fabric Interconnect A to access the device from a web browser and the previously configured admin password to Log into the device.

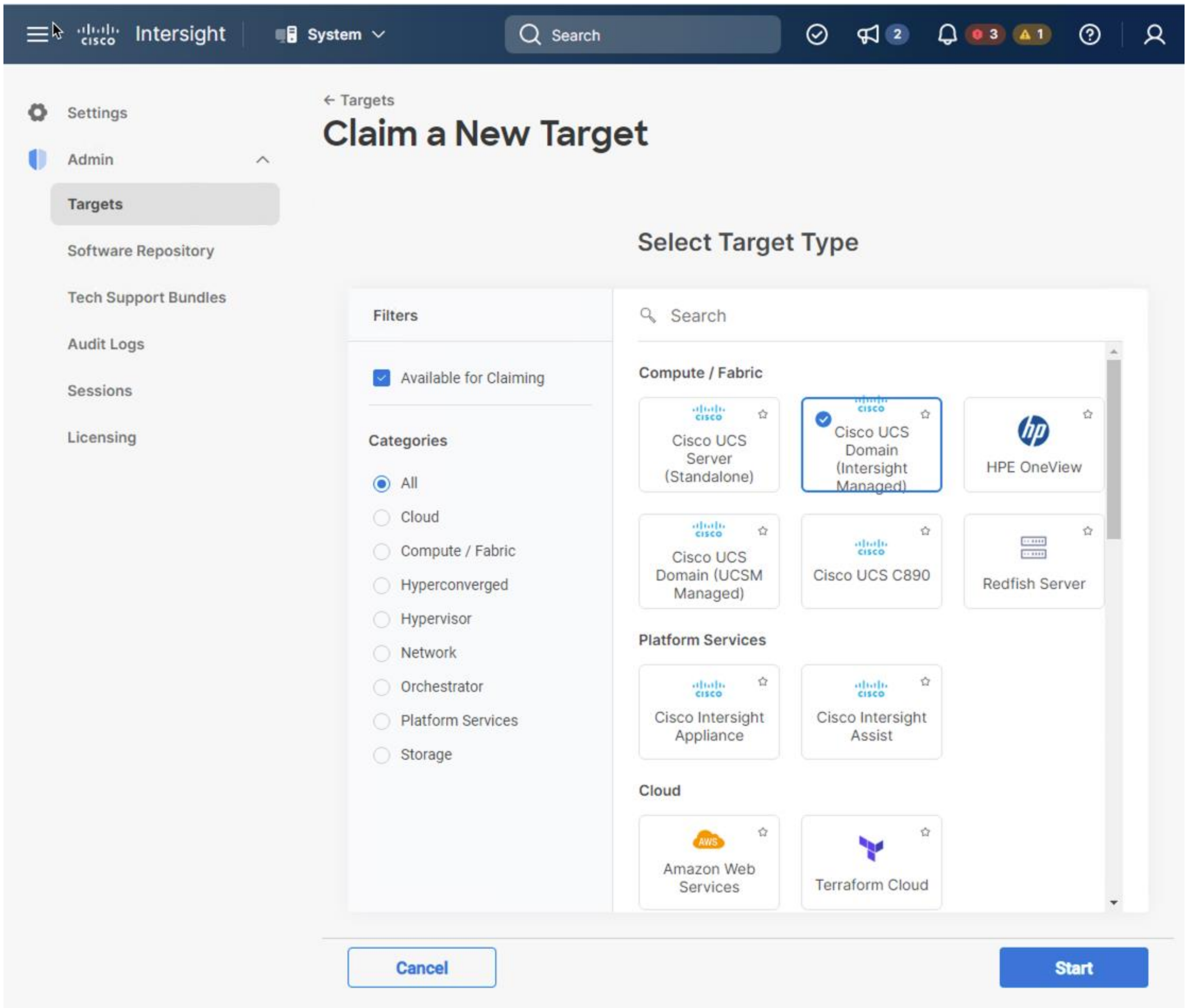
Step 2. Under DEVICE CONNECTOR, the current device status will show “Not claimed.” Note, or copy, the Device ID, and Claim Code information for claiming the device in Cisco Intersight.

Step 3. Log into **Cisco Intersight**.

Step 4. Click **Targets** from the left menu.

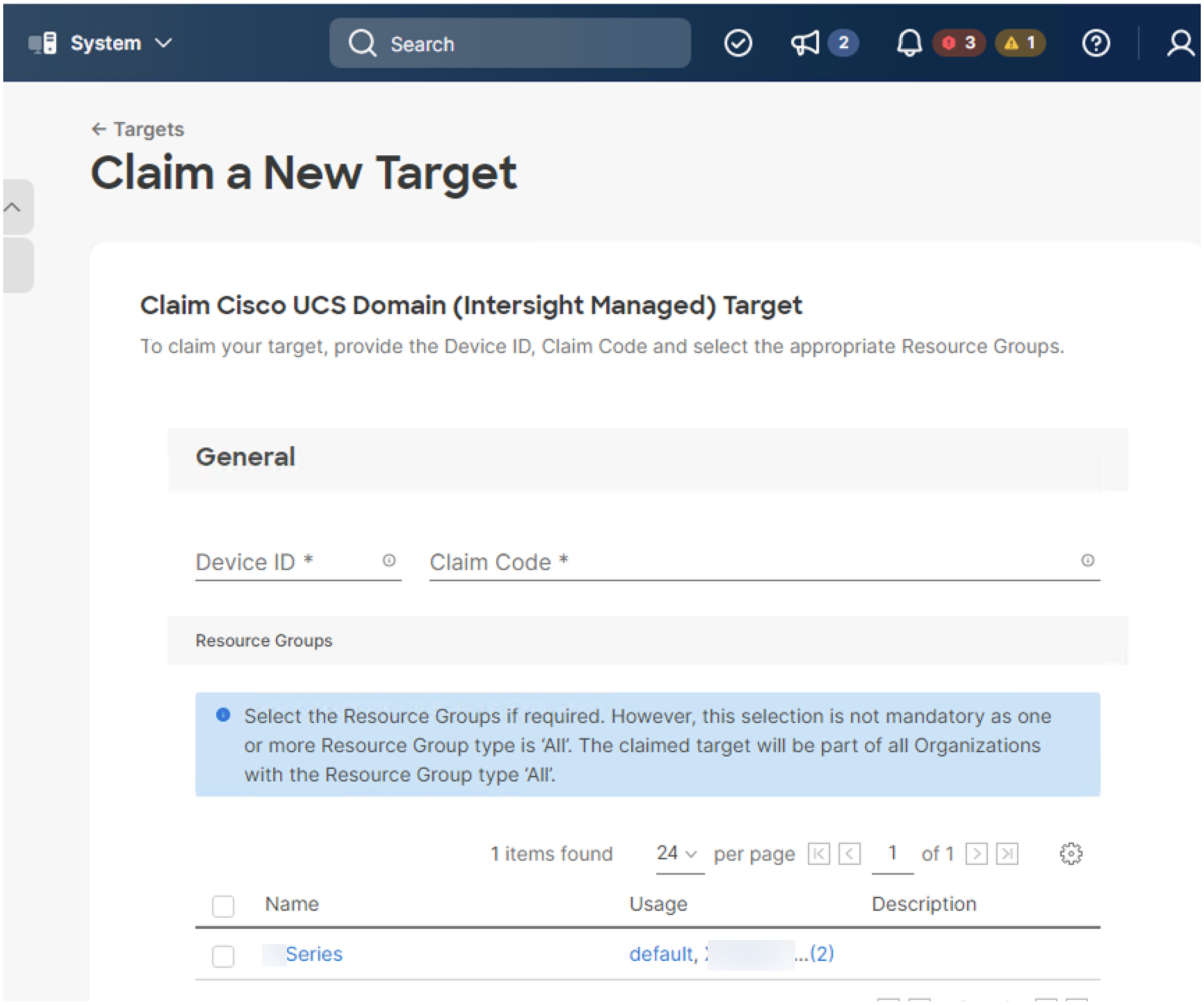
Step 5. Click **Claim New Target**.

Step 6. Select **Cisco UCS Domain (Intersight Managed)** and click **Start**.



Step 7. Enter the Device ID and Claim Code captured from the Cisco UCS FI.

Step 8. Select the previously created Resource Group and click **Claim**.



← Targets

Claim a New Target

Claim Cisco UCS Domain (Intersight Managed) Target

To claim your target, provide the Device ID, Claim Code and select the appropriate Resource Groups.

General

Device ID *

Claim Code *

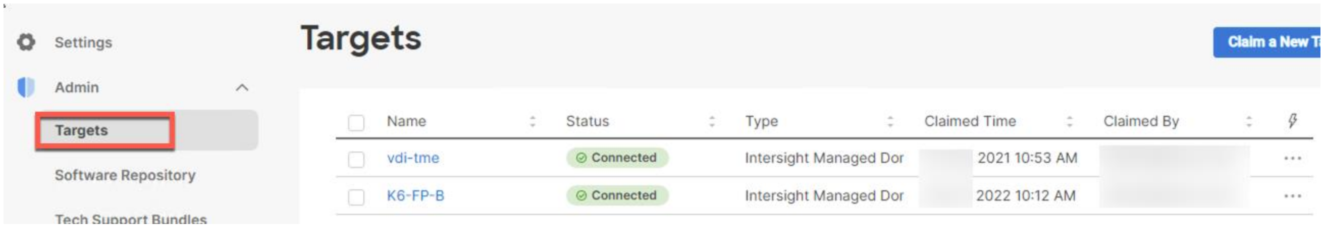
Resource Groups

Select the Resource Groups if required. However, this selection is not mandatory as one or more Resource Group type is 'All'. The claimed target will be part of all Organizations with the Resource Group type 'All'.

1 items found 24 per page 1 of 1

□	Name	Usage	Description
□	[redacted] Series	default, [redacted] ...(2)	

On successfully device claim, Cisco UCS FI should appear as a target in Cisco Intersight.



Targets

□	Name	Status	Type	Claimed Time	Claimed By
□	vdi-tme	Connected	Intersight Managed Dor	[redacted] 2021 10:53 AM	[redacted]
□	K6-FP-B	Connected	Intersight Managed Dor	[redacted] 2022 10:12 AM	[redacted]

Procedure 7. Verify the addition of Cisco UCS Fabric Interconnects to Cisco Intersight

Step 1. Log back into the web GUI of the Cisco UCS fabric interconnect and click **Refresh**.

The fabric interconnect status should now be set to **Claimed**.

Configure a Cisco UCS Domain Profile

This subject contains the following procedures:

- Create a Cisco UCS Domain Profile
- General Configuration

- Cisco UCS Domain Assignment
- Create and apply the VLAN Policy
- Create and apply VSAN policy (FC configuration only)
- Configure the Ports on the Fabric Interconnects
- Configure FC Port Channel (FC configuration only)
- Port Configuration for Fabric Interconnect B

A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, allows configuration of the ports and port channels, and configures the VLANs and VSANs in the network. It defines the characteristics of and configured ports on fabric interconnects. The domain-related policies can be attached to the profile either at the time of creation or later. One Cisco UCS domain profile can be assigned to one fabric interconnect domain.

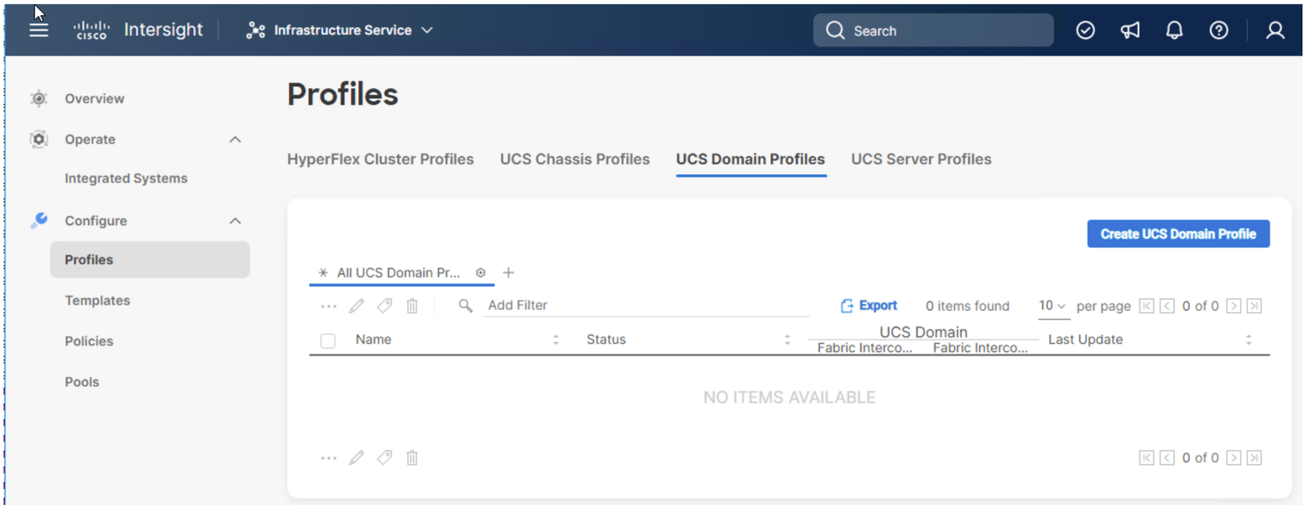
Procedure 1. Create a Cisco UCS Domain Profile

Step 1. Log into the **Cisco Intersight** portal.

Step 2. From the drop-down list, click **Infrastructure Services**.

Step 3. Under **CONFIGURE** in the left pane and click **Profiles**.

Step 4. In the main window, click **UCS Domain Profiles** and click **Create UCS Domain Profile**.

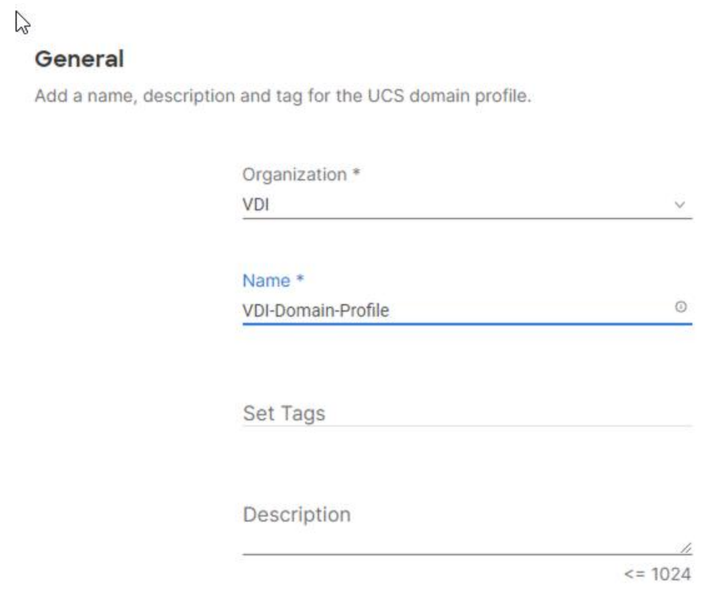


Procedure 2. General Configuration

Step 1. Select the organization from the drop-down list (for example, VDI).

Step 2. Provide a name for the domain profile (for example, VDI-Domain-Profile).

Step 3. Provide an optional Description.



General

Add a name, description and tag for the UCS domain profile.

Organization *
VDI

Name *
VDI-Domain-Profile

Set Tags

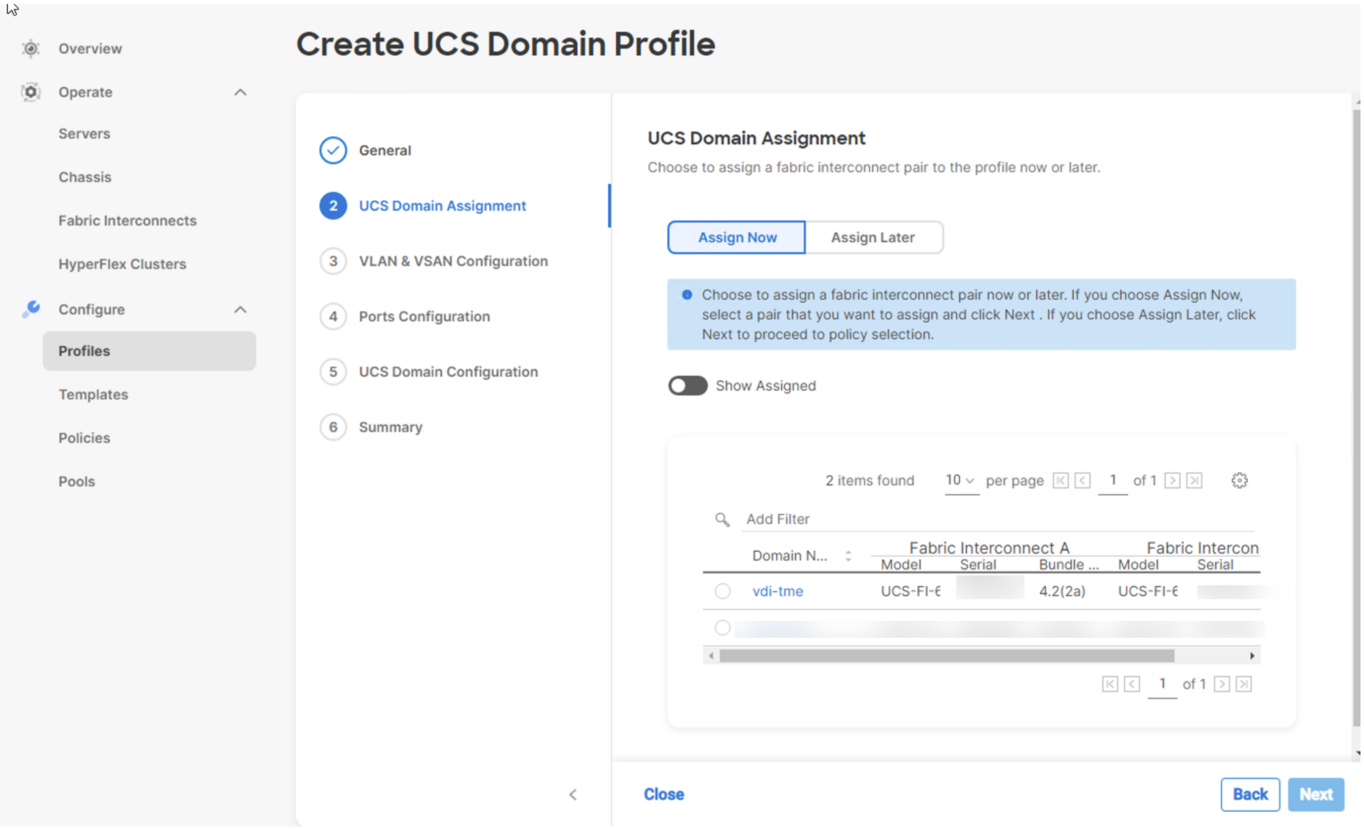
Description

<= 1024

Step 4. Click **Next.**

Procedure 3. Cisco UCS Domain Assignment

Step 1. Assign the Cisco UCS domain to this new domain profile by clicking **Assign Now** and selecting the previously added Cisco UCS domain (for example, vdi-tme).



Create UCS Domain Profile

UCS Domain Assignment

Choose to assign a fabric interconnect pair to the profile now or later.

Choose to assign a fabric interconnect pair now or later. If you choose Assign Now, select a pair that you want to assign and click Next . If you choose Assign Later, click Next to proceed to policy selection.

Show Assigned

2 items found 10 per page 1 of 1

Add Filter

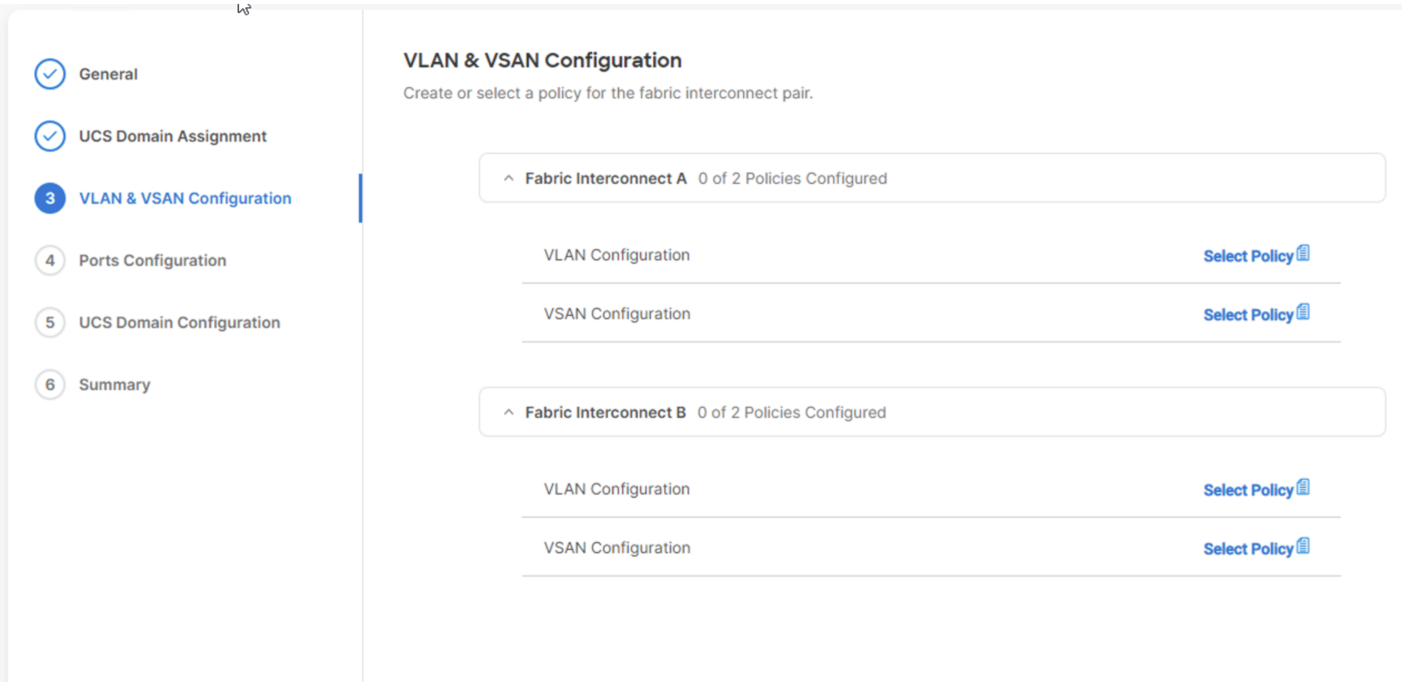
		Fabric Interconnect A			Fabric Intercon	
	Domain N...	Model	Serial	Bundle ...	Model	Serial
○	vdi-tme	UCS-FI-€		4.2(2a)	UCS-FI-€	
○						

Step 2. Click **Next.**

Procedure 4. Create and apply the VLAN Policy

Note: In this step, a single VLAN policy is created for both fabric interconnects and two individual VSAN policies are created because the VSAN IDs are unique for each fabric interconnect.

Step 1. Click **Select Policy** next to VLAN Configuration under Fabric Interconnect A.



VLAN & VSAN Configuration

Create or select a policy for the fabric interconnect pair.

Fabric Interconnect A 0 of 2 Policies Configured

VLAN Configuration — Select Policy

VSAN Configuration — Select Policy

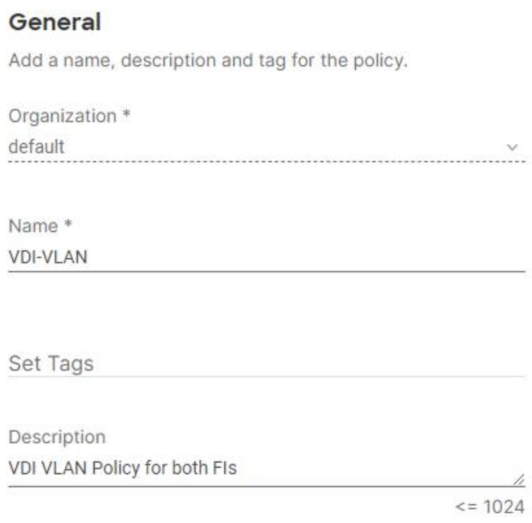
Fabric Interconnect B 0 of 2 Policies Configured

VLAN Configuration — Select Policy

VSAN Configuration — Select Policy

Step 2. In the pane on the right, click **Create New**.

Step 3. Verify correct organization is selected from the drop-down list (for example, default) and provide a name for the policy (for example, VDI-VLAN).



General

Add a name, description and tag for the policy.

Organization *
default

Name *
VDI-VLAN

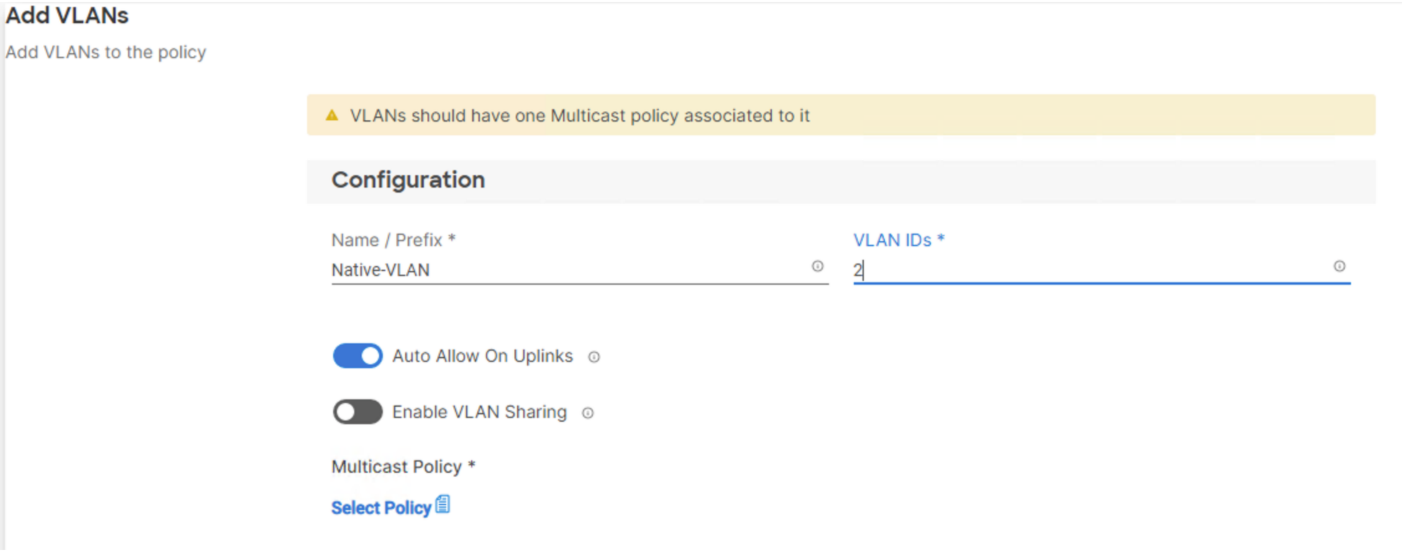
Set Tags

Description
VDI VLAN Policy for both FIs
<= 1024

Step 4. Click **Next**.

Step 5. Click **Add VLANs**.

Step 6. Provide a name and VLAN ID for the native VLAN.



Add VLANs

Add VLANs to the policy

⚠ VLANs should have one Multicast policy associated to it

Configuration

Name / Prefix * Native-VLAN

VLAN IDs * 2

● Auto Allow On Uplinks

○ Enable VLAN Sharing

Multicast Policy *

Step 7. Make sure **Auto Allow On** Uplinks is enabled.

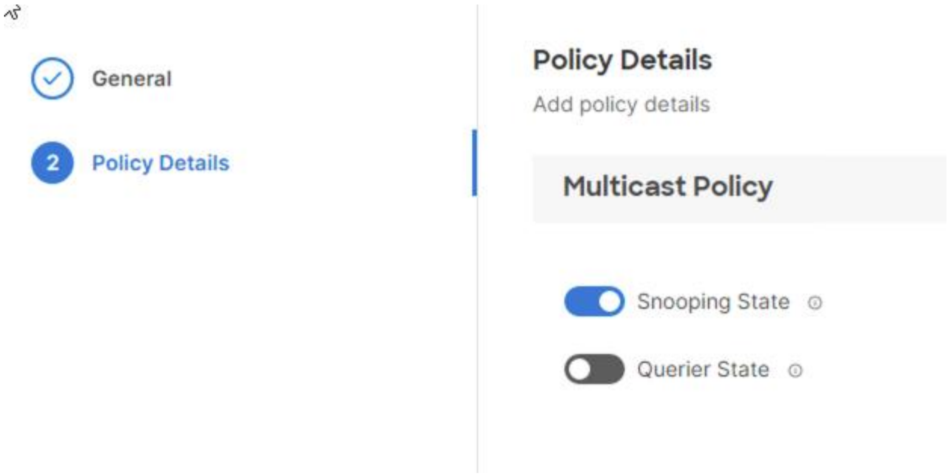
Step 8. To create the required Multicast policy, click **Select Policy** under Multicast*.

Step 9. In the window on the right, click **Create New** to create a new Multicast Policy.

Step 10. Provide a Name for the Multicast Policy (for example, VDI-MCAST-Pol).

Step 11. Provide optional Description and click **Next**.

Step 12. Leave the Snooping State selected and click **Create**.



Policy Details

Add policy details

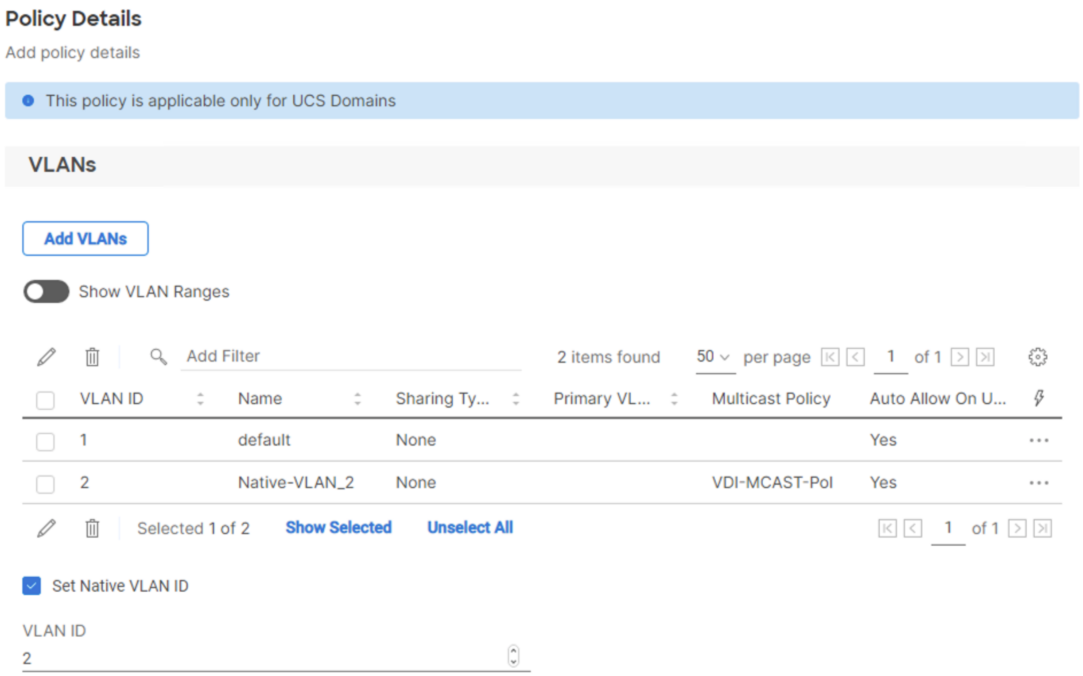
Multicast Policy

● Snooping State

○ Querier State

Step 13. Click **Add** to add the VLAN.

Step 14. Select **Set Native VLAN ID** and enter the VLAN number (for example, 2) under VLAN ID.



Policy Details

Add policy details

● This policy is applicable only for UCS Domains

VLANs

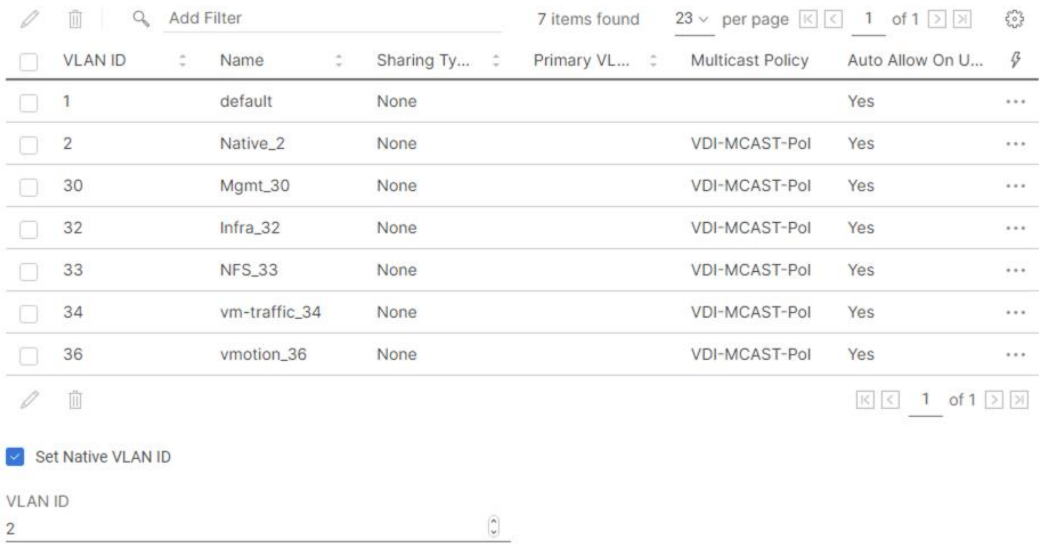
☐	VLAN ID	Name	Sharing Ty...	Primary VL...	Multicast Policy	Auto Allow On U...
☐	1	default	None			Yes
☐	2	Native-VLAN_2	None		VDI-MCAST-Pol	Yes

☑ Set Native VLAN ID

VLAN ID
2

Step 15. Add the remaining VLANs for FlexPod by clicking Add VLANs and entering the VLANs one by one. Reuse the previously created multicast policy for all the VLANs.

The VLANs created during this validation are shown below:



☐	VLAN ID	Name	Sharing Ty...	Primary VL...	Multicast Policy	Auto Allow On U...
☐	1	default	None			Yes
☐	2	Native_2	None		VDI-MCAST-Pol	Yes
☐	30	Mgmt_30	None		VDI-MCAST-Pol	Yes
☐	32	Infra_32	None		VDI-MCAST-Pol	Yes
☐	33	NFS_33	None		VDI-MCAST-Pol	Yes
☐	34	vm-traffic_34	None		VDI-MCAST-Pol	Yes
☐	36	vmotion_36	None		VDI-MCAST-Pol	Yes

☑ Set Native VLAN ID

VLAN ID
2

Step 16. Click **Create** to finish creating the VLAN policy and associated VLANs.

Step 17. Click **Select Policy** next to VLAN Configuration for Fabric Interconnect B and select the same VLAN policy.

Procedure 5.Create and apply VSAN policy (FC configuration only)

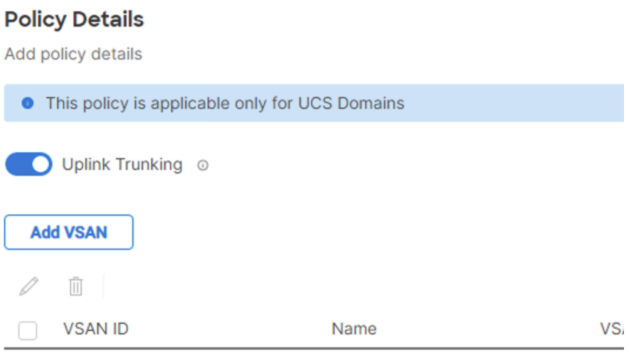
Note: A VSAN policy is only needed when configuring Fibre Channel and can be skipped when configuring IP-only storage access.

Step 1. Click **Select Policy** next to VSAN Configuration under Fabric Interconnect A. Click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-VSAN-Pol-A).

Step 3. Click **Next**.

Step 4. Enable **Uplink Trunking**.



Policy Details

Add policy details

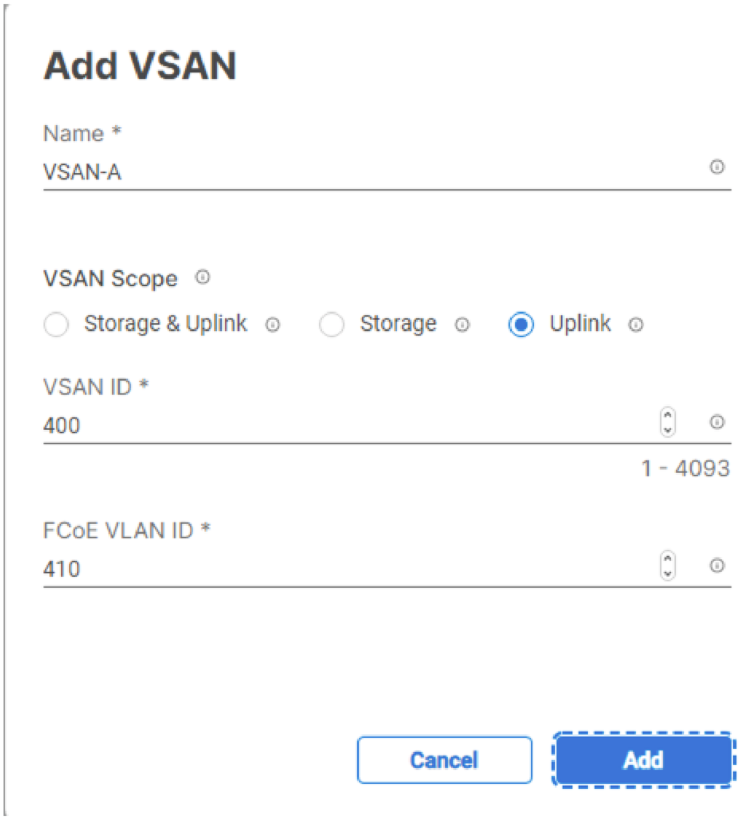
This policy is applicable only for UCS Domains

Uplink Trunking: enabled

□	VSAN ID	Name	VS

Step 5. Click **Add VSAN** and provide a name (for example, VSAN-A), VSAN ID (for example, 400), and associated Fibre Channel over Ethernet (FCoE) VLAN ID (for example, 410) for SAN A.

Step 6. Set VLAN Scope as **Uplink**.



Add VSAN

Name *: VSAN-A

VSAN Scope: ○ Storage & Uplink ○ Storage ● Uplink

VSAN ID *: 400 (1 - 4093)

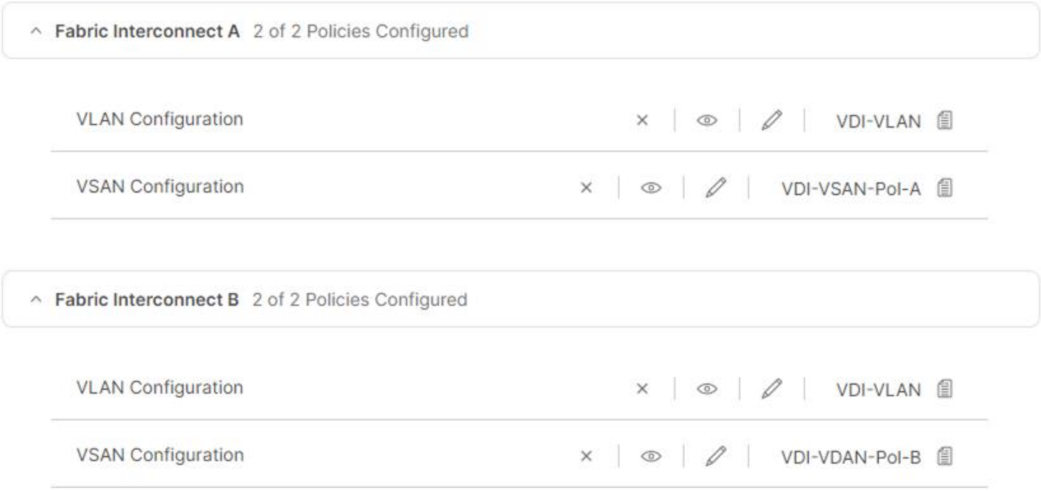
FCoE VLAN ID *: 410

Step 7. Click **Add**.

Step 8. Click **Create** to finish creating VSAN policy for fabric A.

Step 9. Repeat steps 1 – 9 to create a new VSAN policy for SAN-B. Name the policy to identify the SAN-B configuration (for example, VDI-VSAN-Pol-B) and use appropriate VSAN and FCoE VLAN (for example, 401).

Step 10. Verify that a common VLAN policy and two unique VSAN policies are associated with the two fabric interconnects.



^ Fabric Interconnect A 2 of 2 Policies Configured

VLAN Configuration × VDI-VLAN

VSAN Configuration × VDI-VSAN-Pol-A

^ Fabric Interconnect B 2 of 2 Policies Configured

VLAN Configuration × VDI-VLAN

VSAN Configuration × VDI-VDAN-Pol-B

Step 11. Click **Next.**

Procedure 6. Configure the Ports on the Fabric Interconnects

Step 1. Click **Select Policy** for Fabric Interconnect A.

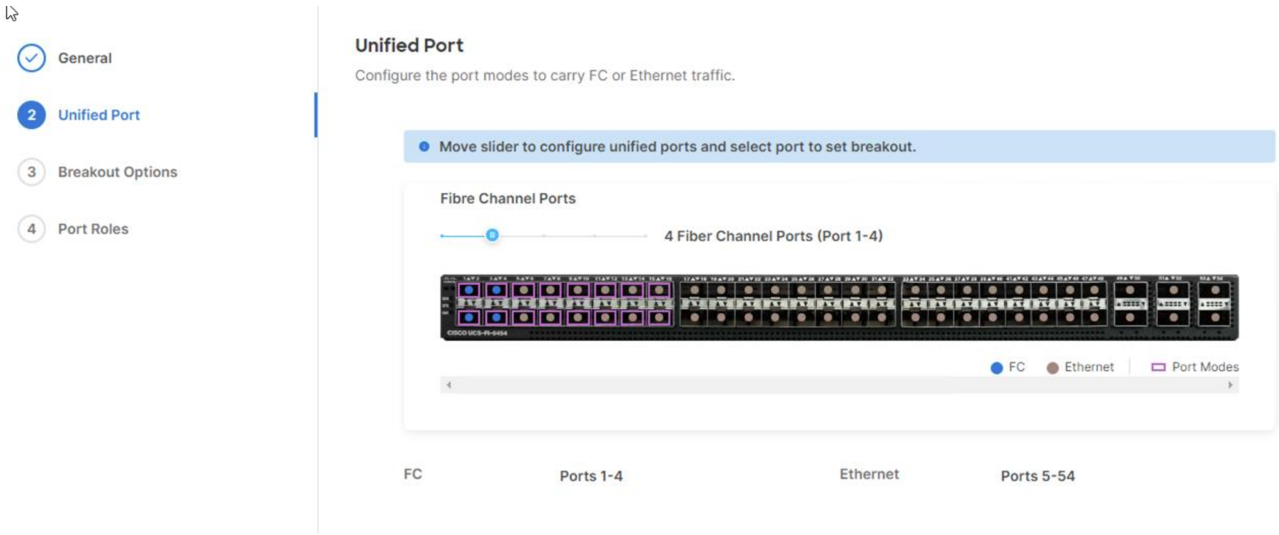
Step 2. Click **Create New** in the pane on the right to define a new port configuration policy.

Note: Use two separate port policies for the fabric interconnects. Using separate policies provide flexibility when port configuration (port numbers or speed) differs between the two FIs. When configuring Fibre Channel, two port policies are required because each fabric interconnect uses unique Fibre Channel VSAN ID.

Step 3. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-PortPol-A).

Step 4. Click **Next.**

Step 5. Move the slider to set up unified ports. In this deployment, the first four ports were selected as Fibre Channel ports. Click **Next**.



✓ General

2 Unified Port

3 Breakout Options

4 Port Roles

Unified Port

Configure the port modes to carry FC or Ethernet traffic.

● Move slider to configure unified ports and select port to set breakout.

Fibre Channel Ports

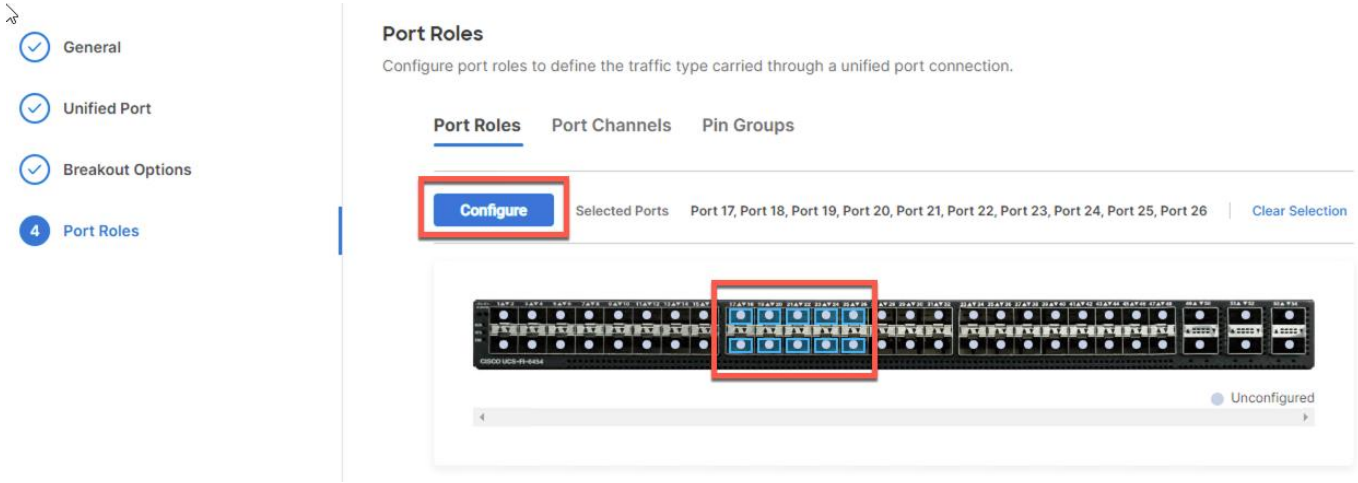
4 Fiber Channel Ports (Port 1-4)

● FC ● Ethernet ▭ Port Modes

FC	Ports 1-4	Ethernet	Ports 5-54

Step 6. Click **Next** to pass the Breakout Options page.

Step 7. Select the ports that need to be configured as server ports by clicking the ports in the graphics (or select from the list below the graphic). When all ports are selected, click **Configure**.



✓ General

✓ Unified Port

✓ Breakout Options

4 Port Roles

Port Roles

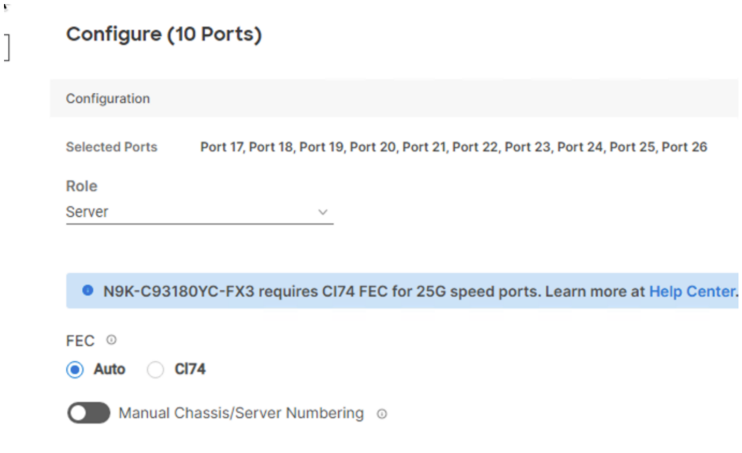
Configure port roles to define the traffic type carried through a unified port connection.

Port Roles | Port Channels | Pin Groups

Configure | Selected Ports Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26 | Clear Selection

● Unconfigured

Step 8. From the drop-down list, select **Server** as the role.



Configure (10 Ports)

Configuration

Selected Ports Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26

Role

Server

● N9K-C93180YC-FX3 requires Cl74 FEC for 25G speed ports. Learn more at Help Center.

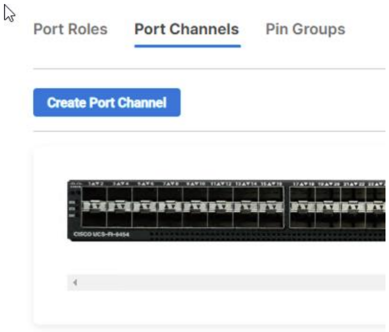
FEC

● Auto ○ Cl74

Manual Chassis/Server Numbering

Step 9. Click **Save**.

Step 10. Configure the Ethernet uplink port channel by selecting the Port Channel in the main pane and then clicking **Create Port Channel**.



Step 11. Select **Ethernet Uplink Port Channel** as the role, provide a port-channel ID (for example, 11), and select a value for Admin Speed from drop down menu (for example, Auto).

Note: You can create the Ethernet Network Group, Flow Control, Ling Aggregation or Link control policy for defining disjoint Layer-2 domain or fine tune port-channel parameters. These policies were not used in this deployment and system default values were utilized.

Step 12. Scroll down and select uplink ports from the list of available ports (for example, port 49 and 50)

Step 13. Click **Save**.

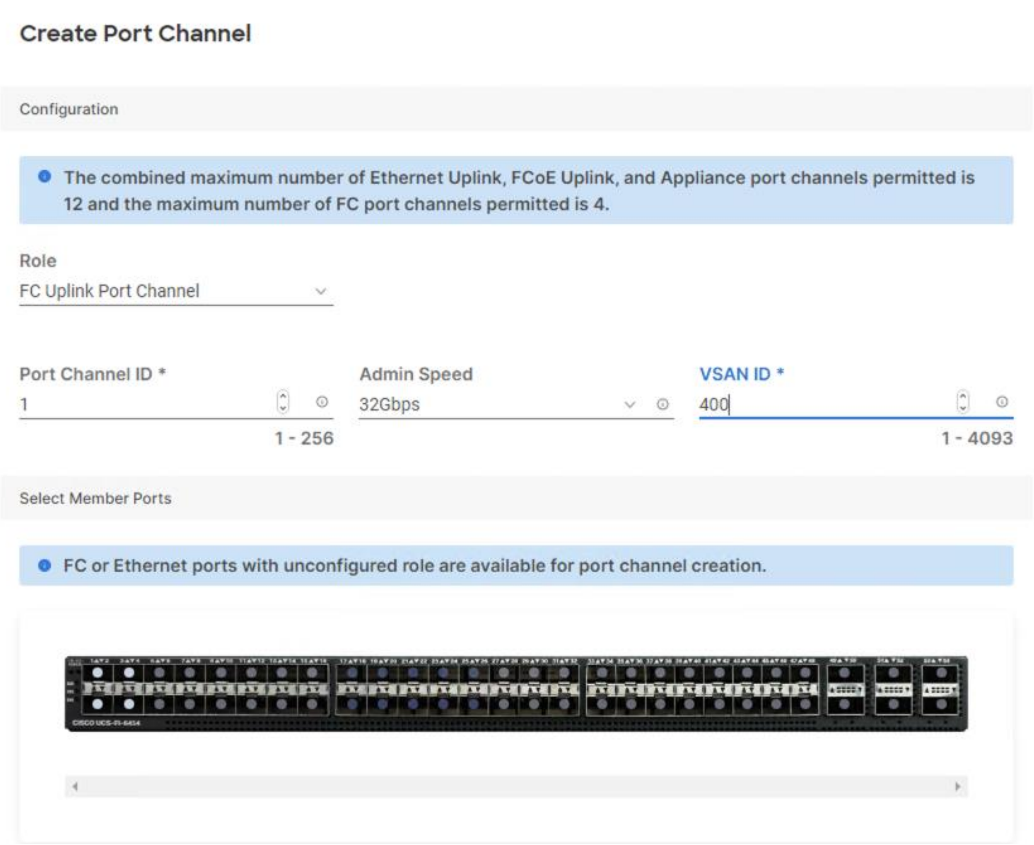
Procedure 7. Configure FC Port Channel (FC configuration only)

Note: FC uplink port channel is only needed when configuring FC SAN and can be skipped for IP-only (iSCSI) storage access.

Step 1. Configure a Fibre Channel Port Channel by selecting the **Port Channel** in the main pane again and clicking **Create Port Channel**.

Step 2. In the drop-down list under Role, choose **FC Uplink Port Channel**.

Step 3. Provide a port-channel ID (for example, 1), select a value for Admin Speed (for example, 32Gbps), and provide a VSAN ID (for example, 400).



Create Port Channel

Configuration

The combined maximum number of Ethernet Uplink, FCoE Uplink, and Appliance port channels permitted is 12 and the maximum number of FC port channels permitted is 4.

Role
FC Uplink Port Channel

Port Channel ID *
1
1 - 256

Admin Speed
32Gbps

VSAN ID *
400
1 - 4093

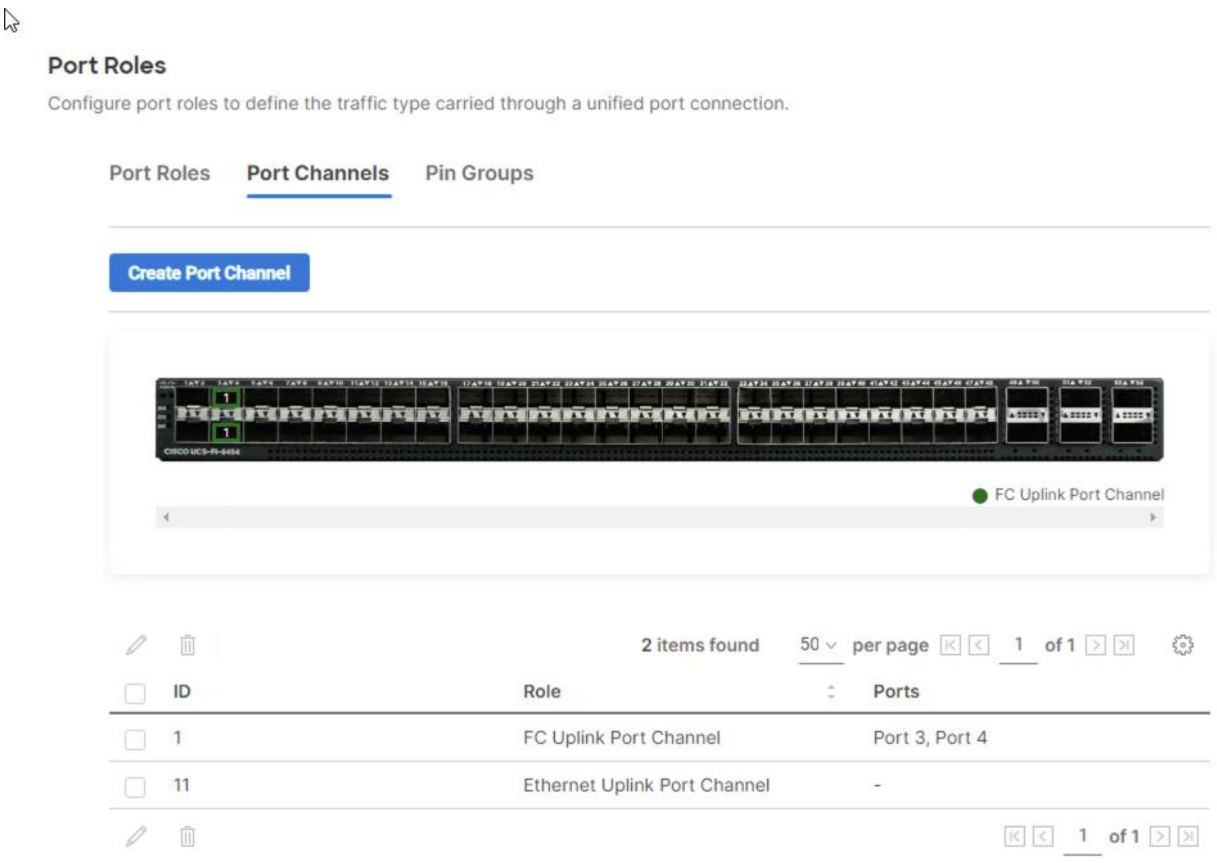
Select Member Ports

FC or Ethernet ports with unconfigured role are available for port channel creation.

Step 4. Select ports (for example, 3 and 4).

Step 5. Click **Save**.

Step 6. Verify the port-channel IDs and ports after both the Ethernet uplink port channel and the Fibre Channel uplink port channel have been created.



Port Roles

Configure port roles to define the traffic type carried through a unified port connection.

ID	Role	Ports
1	FC Uplink Port Channel	Port 3, Port 4
11	Ethernet Uplink Port Channel	-

Step 7. Click **Save** to create the port policy for Fabric Interconnect A.

Note: Use the summary screen to verify that the ports were selected and configured correctly.

Procedure 8. Port Configuration for Fabric Interconnect B

Step 1. Repeat the steps from Procedure 7. Configure FC Port Channel (FC configuration only) to create the port policy for Fabric Interconnect B including the Ethernet port-channel and the FC port-channel (if configuring SAN). Use the following values for various parameters:

- Name of the port policy: VDI-PortPol-B
- Ethernet port-Channel ID: 12
- FC port-channel ID: 2
- FC VSAN ID: 401

Step 2. When the port configuration for both fabric interconnects is complete and looks good, click **Next.**

Cisco UCS Domain Configuration

This subject contains the following procedures:

- Configure NTP Policy for the Cisco UCS Domain
- Configure Network Connectivity Policy
- Configure System QoS Policy
- Verify Settings
- Deploy the Cisco UCS Domain Profile

- Verify Cisco UCS Domain Profile Deployment

Note: Under UCS domain configuration, additional policies can be configured to setup NTP, Syslog, DNS settings, SNMP, QoS and UCS operating mode (end host or switch mode). For this deployment, three policies (NTP, Network Connectivity and System QoS) will be configured.

Procedure 1. Configure NTP Policy for the Cisco UCS Domain

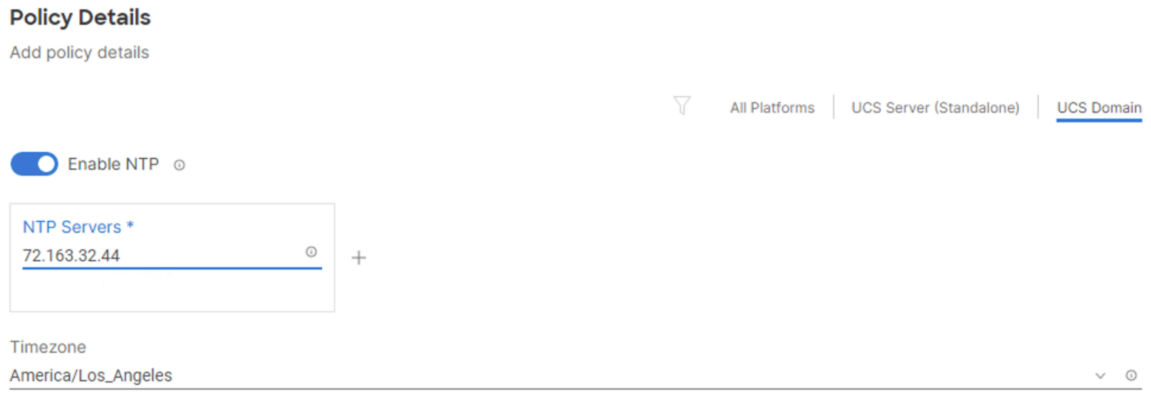
Step 1. Click **Select Policy** next to NTP and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-NTPPol).

Step 3. Click **Next**.

Step 4. **Enable NTP**, provide the NTP server IP addresses, and select the **Timezone** from the drop-down list.

Step 5. If required, add a second NTP server by clicking **+** next to the first NTP server IP address.



Policy Details

Add policy details

Enable NTP

NTP Servers *
72.163.32.44

Timezone
America/Los_Angeles

Step 6. Click **Create**.

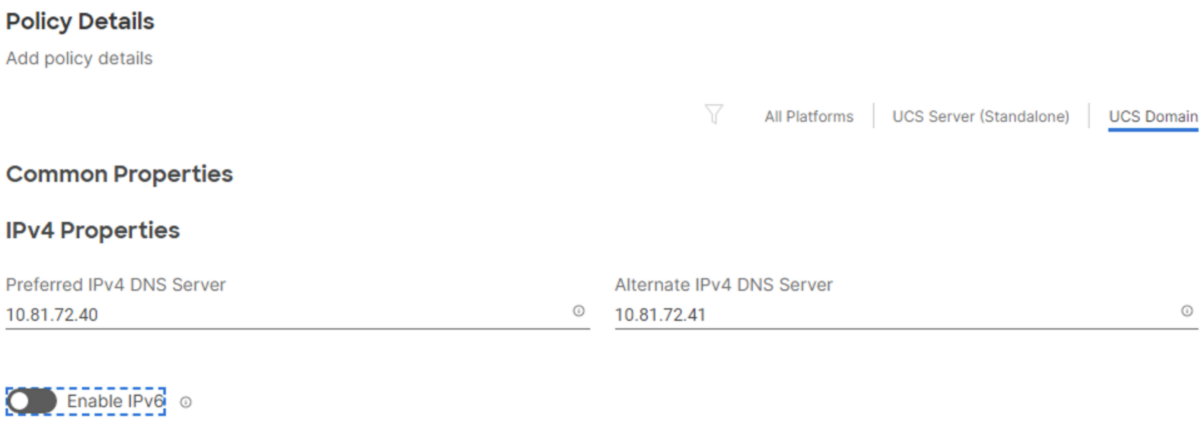
Procedure 2. Configure Network Connectivity Policy

Note: To define the Doman Name Service (DNS) servers for Cisco UCS, configure network connectivity policy.

Step 1. Click **Select Policy** next to Network Connectivity and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-NetConn-Pol).

Step 3. Provide DNS server IP addresses for Cisco UCS.



Policy Details

Add policy details

Common Properties

IPv4 Properties

Preferred IPv4 DNS Server: 10.81.72.40

Alternate IPv4 DNS Server: 10.81.72.41

Enable IPv6

Step 4. Click **Create.**

Procedure 3. Configure System QoS Policy

To define the QoS settings for Cisco UCS, configure System QoS policy.

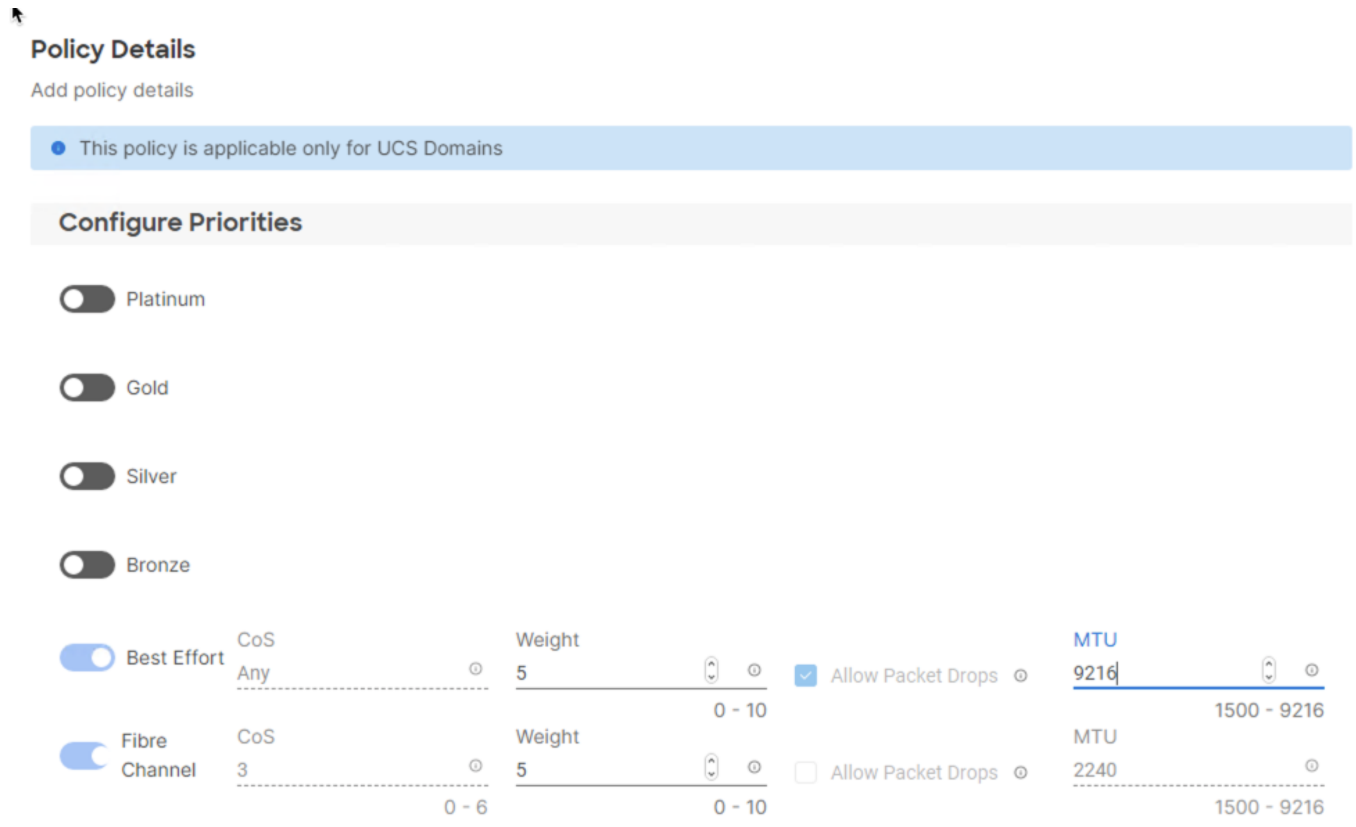
Step 1. Click **Select Policy** next to System QoS* and click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-QoSPol).

Step 3. Click **Next.**

Step 4. Change the MTU for Best Effort class to **9216**.

Step 5. Keep the default selections or change the parameters if necessary.



Policy Details

Add policy details

This policy is applicable only for UCS Domains

Configure Priorities

Platinum

Gold

Silver

Bronze

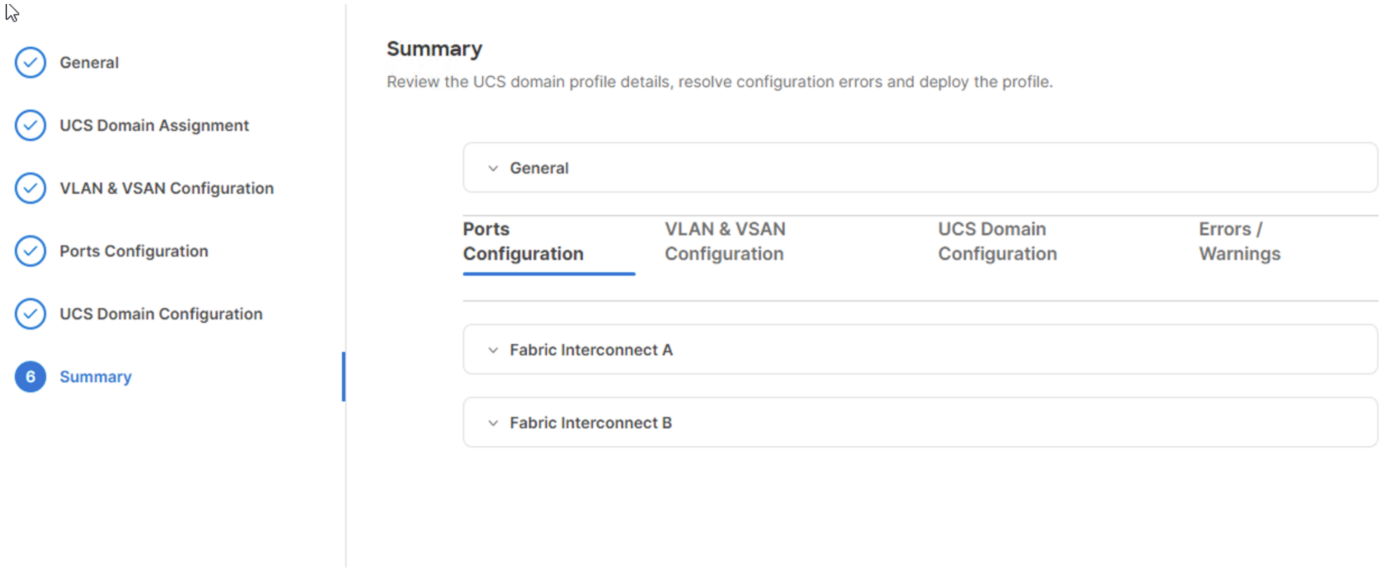
	CoS	Weight		MTU
Best Effort	Any	5 0 - 10	☑ Allow Packet Drops	9216 1500 - 9216
Fibre Channel	3 0 - 6	5 0 - 10	□ Allow Packet Drops	2240 1500 - 9216

Step 6. Click **Create.**

Step 7. Click **Next.**

Procedure 4. Verify Settings

Step 1. Verify all the settings including the fabric interconnect settings, by expanding the settings and make sure that the configuration is correct.



Summary

Review the UCS domain profile details, resolve configuration errors and deploy the profile.

Procedure 5. Deploy the Cisco UCS Domain Profile

Note: After verifying the domain profile configuration, deploy the Cisco UCS profile.

Step 1. From the UCS domain profile Summary view, Click **Deploy**.

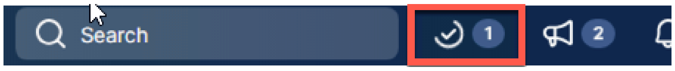
Step 2. Acknowledge any warnings and click **Deploy** again.

Step 3. The system will take some time to validate and configure the settings on the fabric interconnects. Log into the console servers to see when the Cisco UCS fabric interconnects have finished configuration and are successfully rebooted.

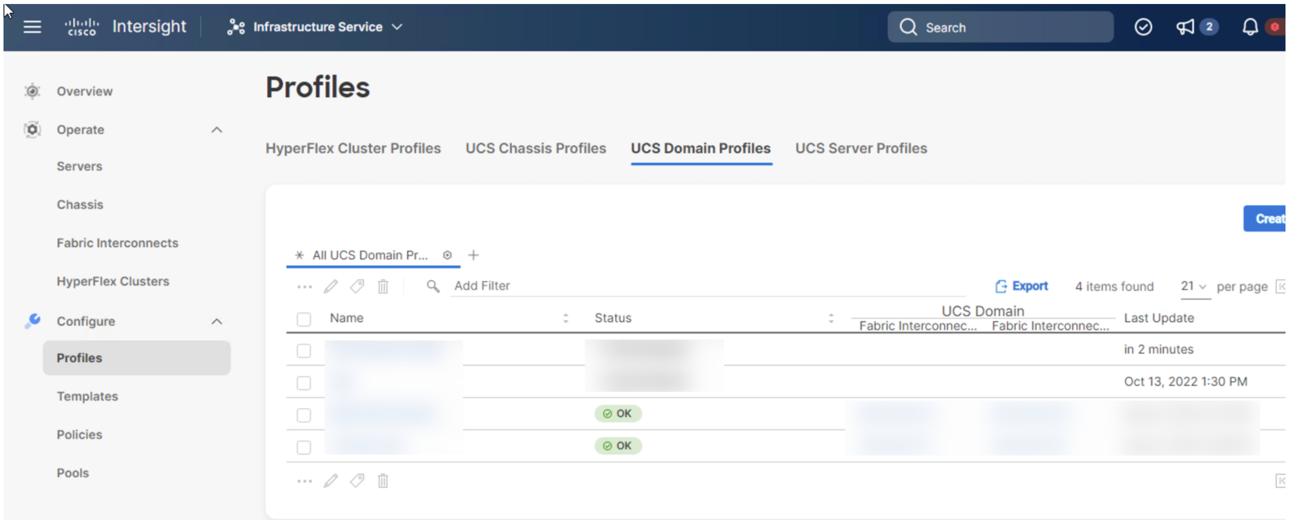
Procedure 6. Verify Cisco UCS Domain Profile Deployment

When the Cisco UCS domain profile has been successfully deployed, the Cisco UCS chassis and the blades should be successfully discovered.

Note: It takes a while to discover the blades for the first time. Watch the number of outstanding tasks in Cisco Intersight:

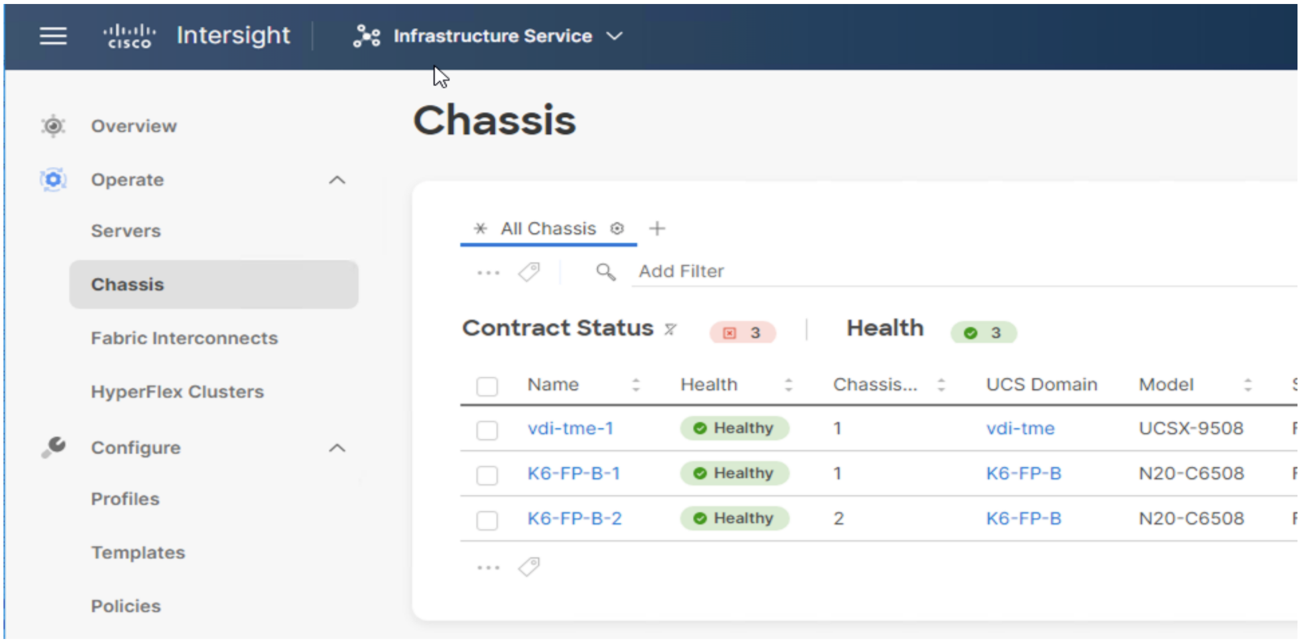


Step 1. Log into **Cisco Intersight**. Under **CONFIGURE > Profiles > UCS Domain Profiles**, verify that the domain profile has been successfully deployed.



Name	Status	UCS Domain Fabric Interconnec...	 Fabric Interconnec...	Last Update
[redacted]	[redacted]			in 2 minutes
[redacted]	[redacted]			Oct 13, 2022 1:30 PM
[redacted]	OK	[redacted]	[redacted]	[redacted]
[redacted]	OK	[redacted]	[redacted]	[redacted]

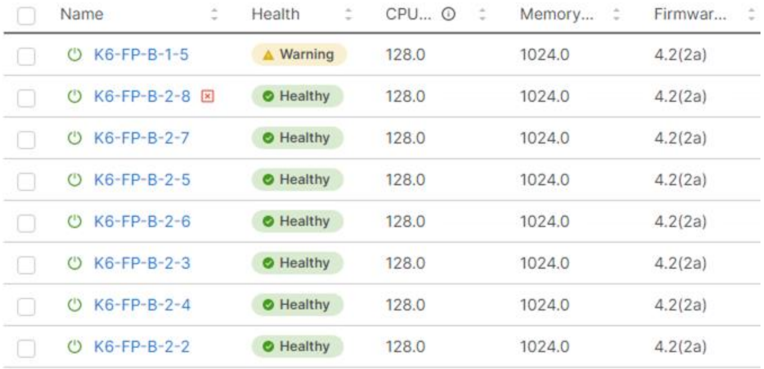
Step 2. Verify that the chassis has been discovered and is visible under **OPERATE > Chassis**.



Chassis

	Name	Health	Chassis...	UCS Domain	Model	S
□	vdi-tme-1	Healthy	1	vdi-tme	UCSX-9508	F
□	K6-FP-B-1	Healthy	1	K6-FP-B	N20-C6508	F
□	K6-FP-B-2	Healthy	2	K6-FP-B	N20-C6508	F

Step 3. Verify that the servers have been successfully discovered and are visible under **OPERATE > Servers**.



□	Name	Health	CPU...	Memory...	Firmwar...
□	K6-FP-B-1-5	Warning	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-8	Healthy	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-7	Healthy	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-5	Healthy	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-6	Healthy	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-3	Healthy	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-4	Healthy	128.0	1024.0	4.2(2a)
□	K6-FP-B-2-2	Healthy	128.0	1024.0	4.2(2a)

Configure Cisco UCS Chassis Profile

Cisco UCS Chassis profile in Cisco Intersight allows you to configure various parameters for the chassis, including:

- IMC Access Policy: IP configuration for the in-band chassis connectivity. This setting is independent of Server IP connectivity and only applies to communication to and from chassis.
- SNMP Policy, and SNMP trap settings.
- Power Policy to enable power management and power supply redundancy mode.
- Thermal Policy to control the speed of FANs (only applicable to Cisco UCS 5108)

A chassis policy can be assigned to any number of chassis profiles to provide a configuration baseline for a chassis. In this deployment, no chassis profile was created or attached to the chassis, but you can configure policies to configure SNMP or Power parameters and attach them to the chassis.

Configure Server Profile Template

This subject contains the following procedures:

- Configure a Server Profile Template

- Configure UUID Pool
- Configure BIOS Policy
- Configure Boot Order Policy for FC Hosts

In the Cisco Intersight platform, a server profile enables resource management by simplifying policy alignment and server configuration. The server profiles are derived from a server profile template. The server profile template and its associated policies can be created using the server profile template wizard. After creating server profile template, you can derive multiple consistent server profiles from the template.

vNIC and vHBA Placement for Server Profile Template

In this deployment, separate server profile templates are created for iSCSI connected storage and for FC connected storage. The vNIC and vHBA layout is explained below. While most of the policies are common across various templates, the LAN connectivity and SAN connectivity policies are unique and will use the information in the tables below.

Four vNICs and two vHBAs are configured to support FC boot from SAN. These devices are manually placed as follows:

Table 16. vHBA and vNIC placement for FC connected storage

vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-A	MLOM	A	0
vHBA-B	MLOM	B	1
01-vSwitch0-A	MLOM	A	2
02-vSwitch0-B	MLOM	B	3
03-VDS0-A	MLOM	A	4
04-VDS0-B	MLOM	B	5

Four vNICs and four vHBAs are configured to support FC boot from SAN. Two vHBAs (vHBA-A and vHBA-B) are used for boot from SAN connectivity and the remaining two vHBAs are used to support NVMe-o-FC. These devices are manually placed as follows:

Table 17. vHBA and vNIC placement for FC with NVMe-o-FC connected storage

vNIC/vHBA Name	Slot	Switch ID	PCI Order	Comment
vHBA-A	MLOM	A	0	Used for boot from SAN
vHBA-B	MLOM	B	1	Used for boot from SAN
01-vSwitch0-A	MLOM	A	2	
02-vSwitch0-B	MLOM	B	3	
03-VDS0-A	MLOM	A	4	
04-VDS0-B	MLOM	B	5	

vNIC/vHBA Name	Slot	Switch ID	PCI Order	Comment

Procedure 1. Configure a Server Profile Template

Step 1. Log into **Cisco Intersight**.

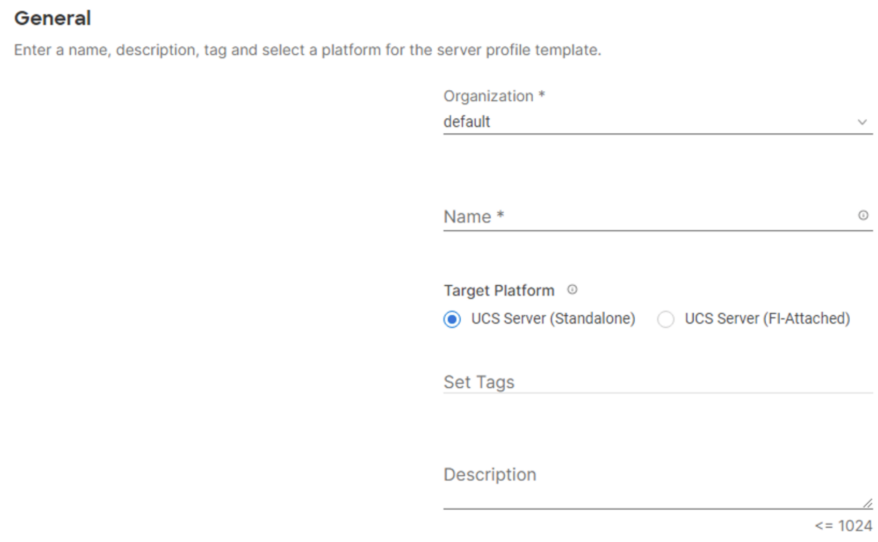
Step 2. Go to **CONFIGURE** > **Templates** and in the main window click **Create UCS Server Profile Template**.

Step 3. Select the organization from the drop-down list (for example, VDI).

Step 4. Provide a name for the server profile template. The name used in this deployment is FC-Boot-Template (FC boot from SAN).

Step 5. Click **UCS Server (FI-Attached)**.

Step 6. Provide an optional description.



General

Enter a name, description, tag and select a platform for the server profile template.

Organization *
default

Name *

Target Platform
● UCS Server (Standalone) ○ UCS Server (FI-Attached)

Set Tags

Description

<= 1024

Step 7. Click **Next.**

Procedure 2. Configure UUID Pool

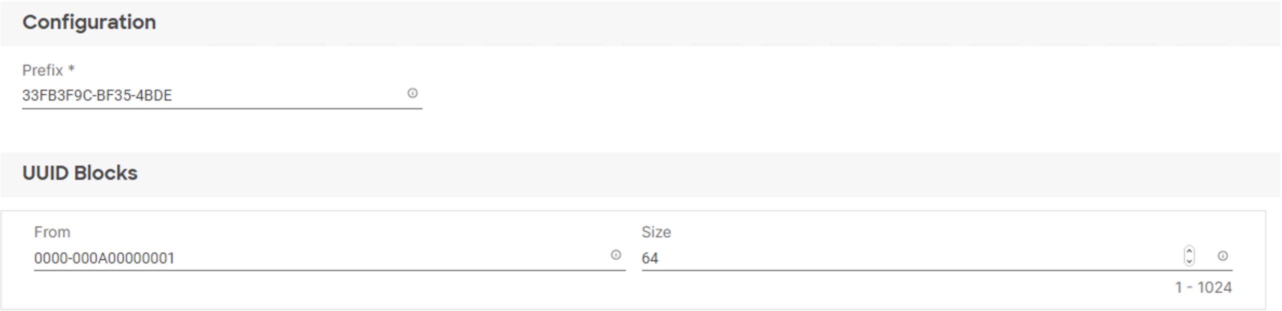
Step 1. Click **Select Pool** under UUID Pool and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the UUID Pool (for example, VDI-UUID-Pool).

Step 3. Provide an optional Description and click **Next.**

Step 4. Provide a UUID Prefix (for example, a random prefix of 33FB3F9C-BF35-4BDE was used).

Step 5. Add a UUID block.



Configuration

Prefix *

33FB3F9C-BF35-4BDE

UUID Blocks

From

0000-000A00000001

Size

64

1 - 1024

Step 6. Click **Create.**

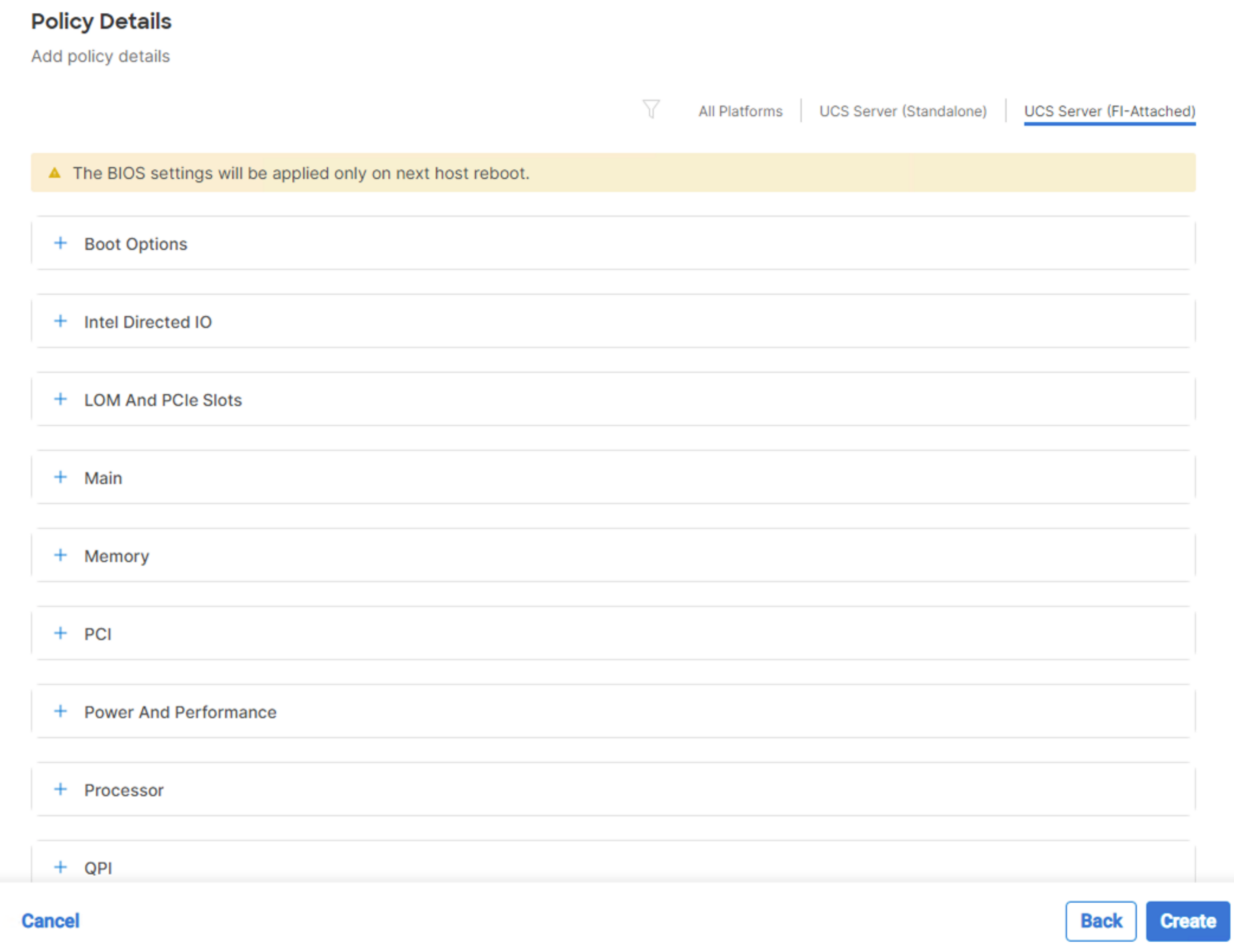
Procedure 3. Configure BIOS Policy

Step 1. Click **Select Policy** next to BIOS and in the pane on the right, click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-BIOSPol).

Step 3. Click **Next.**

Step 4. On the Policy Details screen, select appropriate values for the BIOS settings. In this deployment, the BIOS values were selected based on recommendations in the performance tuning guide for Cisco UCS M6 BIOS: https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/performance-tuning-guide-ucs-m6-servers.html.



Policy Details

Add policy details

All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached)

▲ The BIOS settings will be applied only on next host reboot.

+ Boot Options

+ Intel Directed IO

+ LOM And PCIe Slots

+ Main

+ Memory

+ PCI

+ Power And Performance

+ Processor

+ QPI

Cancel | Back | Create

- LOM and PCIe Slot > CDN Support for LOM: Enabled
- Processor > Enhanced CPU performance: Auto
- Memory > NVM Performance Setting: Balanced Profile

Step 5. Click **Create**.

Procedure 4. Configure Boot Order Policy for FC Hosts

Note: The FC boot order policy applies to all FC hosts.

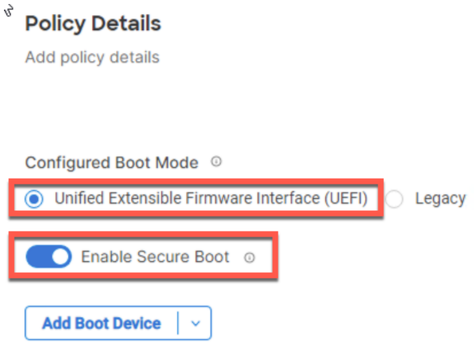
Step 1. Click **Select Policy** next to BIOS Configuration and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-FC-BootOrder-Pol).

Step 3. Click **Next**.

Step 4. For Configured Boot Mode, select **Unified Extensible Firmware Interface (UEFI)**.

Step 5. Turn on **Enable Secure Boot**.



Policy Details

Add policy details

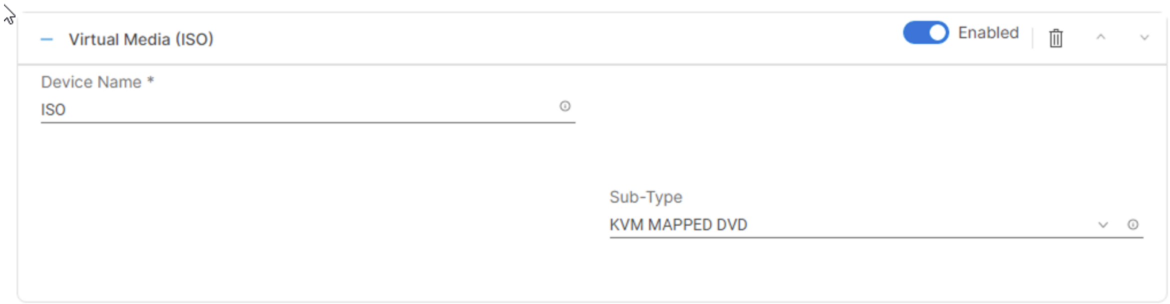
Configured Boot Mode

● Unified Extensible Firmware Interface (UEFI) ○ Legacy

Enable Secure Boot: Enabled

Step 6. Click **Add Boot Device** drop-down list and select **Virtual Media**.

Step 7. Provide a device name (for example, ISO) and then, for the subtype, select **KVM Mapped DVD**.



Virtual Media (ISO) — Enabled

Device Name * ISO

Sub-Type KVM MAPPED DVD

For Fibre Channel SAN boot, all four NetApp controller LIFs will be added as boot options. The four LIFs are as follows:

- **FCP-LIF01a**: NetApp Controller 1, LIF for Fibre Channel SAN A
- **FCP-LIF01b**: NetApp Controller 1, LIF for Fibre Channel SAN B
- **FCP-LIF02a**: NetApp Controller 2, LIF for Fibre Channel SAN A
- **FCP-LIF02b**: NetApp Controller 2, LIF for Fibre Channel SAN B

Step 8. From the **Add Boot Device** drop-down list, select **SAN Boot**.

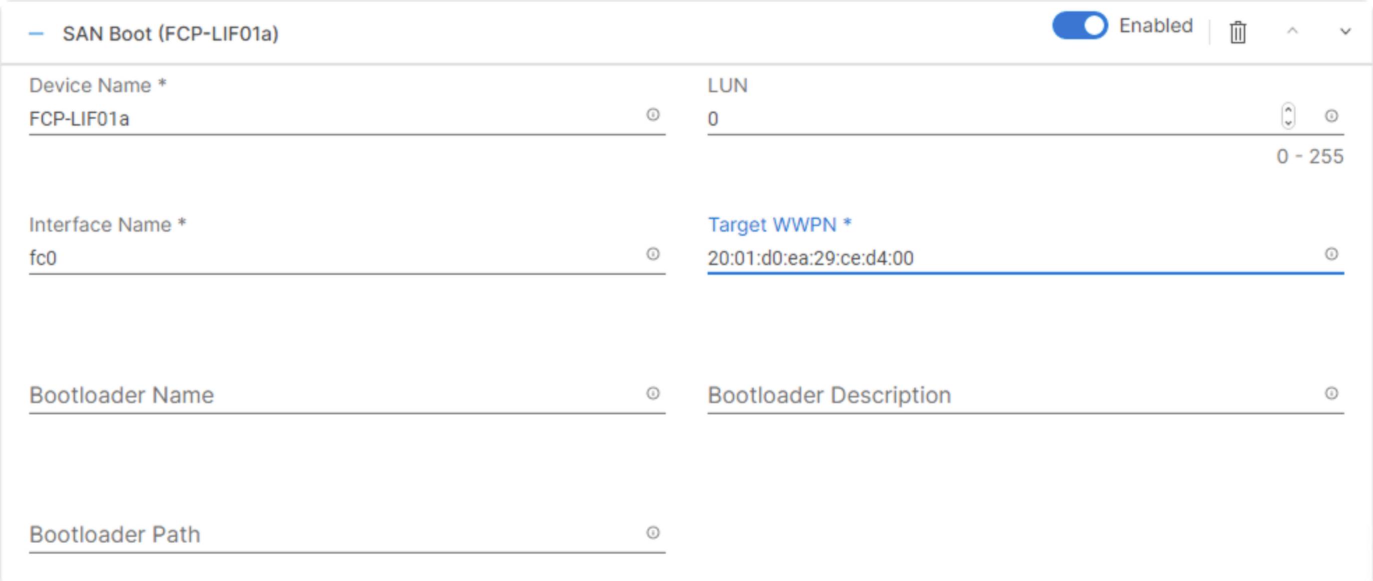
Step 9. Provide the Device Name: FCp-LIF01a and the Logical Unit Number (LUN) value (for example, 0).

Step 10. Provide an interface name vHBA-A. This value is important and should match the vHBA name.

Note: vHBA-A is used to access FCP-LIF01a and FCP-LIF02a and vHBA-B is used to access FCP-LIF01b and FCP-LIF02b.

Step 11. Add the appropriate World Wide Port Name (WWPN) as the Target WWPN.

Note: To obtain the WWPN values, log into NetApp controller using SSH and enter the following command: **network interface show -vserver Infra-SVM -data-protocol fcp**.



— SAN Boot (FCP-LIF01a)

Enabled

Device Name * FCP-LIF01a

LUN 0 (0 - 255)

Interface Name * fc0

Target WWPN * 20:01:d0:ea:29:ce:d4:00

Bootloader Name

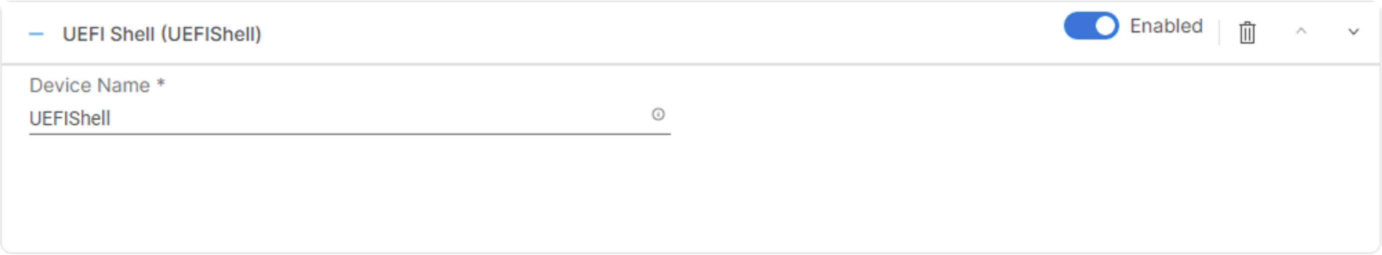
Bootloader Description

Bootloader Path

Step 12. Repeat steps 8-11 three more times to add all the NetApp LIFs.

Step 13. From the **Add Boot Device** drop-down list, select **UEFI Shell**.

Step 14. Add Device Name **UEFIShell**.

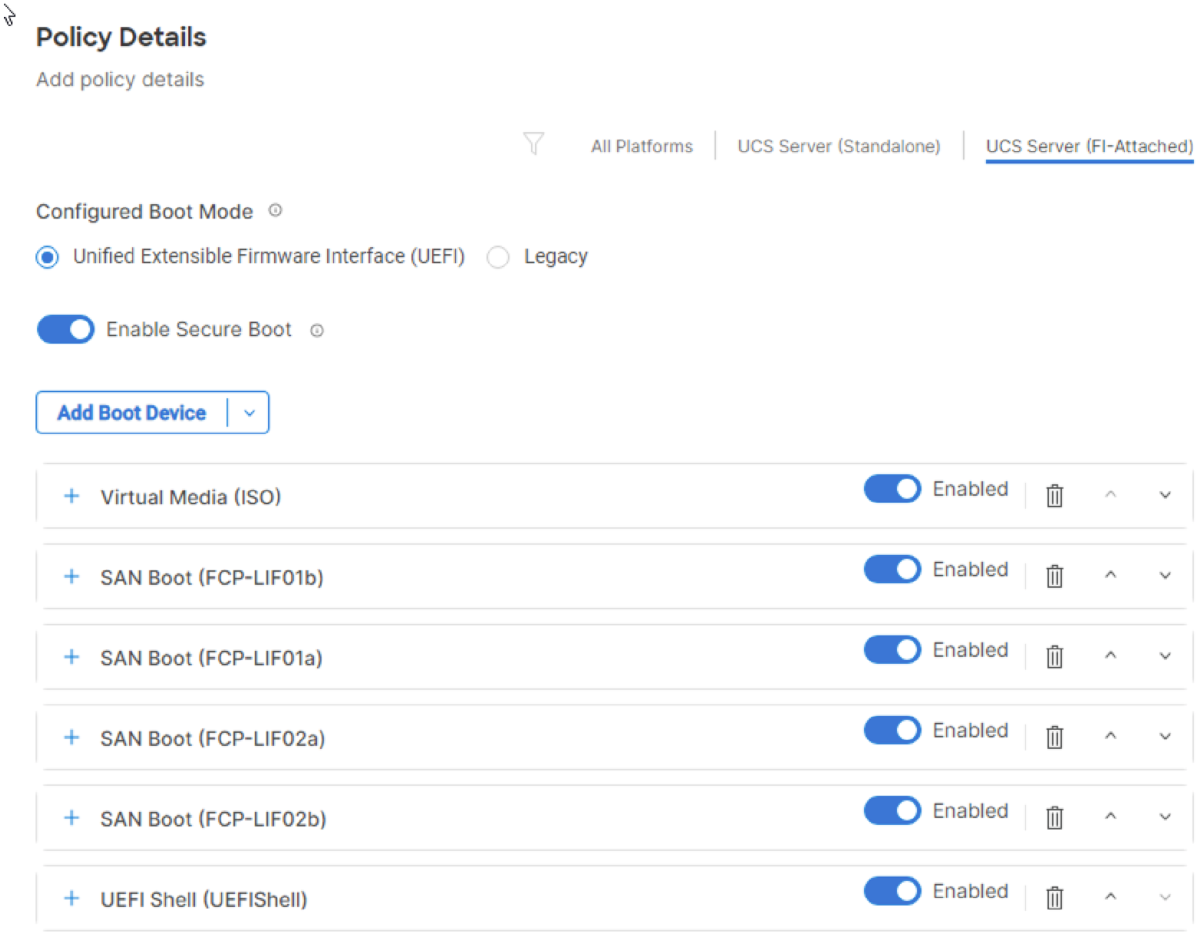


— UEFI Shell (UEFIShell)

Enabled

Device Name * UEFIShell

Step 15. Verify the order of the boot policies and adjust the boot order as necessary using arrows next to the delete button.



Policy Details

Add policy details

All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached)

Configured Boot Mode

● Unified Extensible Firmware Interface (UEFI) ○ Legacy

Enable Secure Boot: Enabled

Add Boot Device

Boot Device	State
Virtual Media (ISO)	Enabled
SAN Boot (FCP-LIF01b)	Enabled
SAN Boot (FCP-LIF01a)	Enabled
SAN Boot (FCP-LIF02a)	Enabled
SAN Boot (FCP-LIF02b)	Enabled
UEFI Shell (UEFIShell)	Enabled

Step 16. Click **Create**.

Step 17. Click **Next** to move to Management Configuration.

Management Configuration

This subject contains the following procedures:

- Configure Cisco IMC Access Policy
- Configure IPMI Over LAN Policy
- Configure Local User Policy
- Storage Configuration
- Create LAN Connectivity Policy for FC Hosts
- Create MAC Address Pool for Fabric A and B
- Create Ethernet Network Group Policy for a vNIC
- Create Ethernet Network Control Policy
- Create Ethernet QoS Policy
- Create Ethernet Adapter Policy
- Create the SAN Connectivity Policy

- Create the WWNN Address Pool
- Create the vHBA-A for SAN A
- Create the WWPN Pool for SAN A
- Create Fibre Channel Network Policy for SAN A
- Create Fibre Channel QoS Policy
- Create Fibre Channel Adapter Policy
- Create the vHBA for SAN B
- Create the WWPN Pool for SAN B
- Create Fibre Channel Network Policy for SAN B
- Configure vHBA-NVMe-A and vHBA-NVMe-B
- Configure vHBA-NVMe-A
- Configure vHBA-NVMe-B
- Verify Summary
- Derive Server Profile

Three policies will be added to the management configuration:

- IMC Access to define the pool of IP addresses for compute node KVM access
- IPMI Over LAN to allow Intersight to manage IPMI messages
- Local User to provide local administrator to access KVM

Procedure 5. Configure Cisco IMC Access Policy

Step 1. Click **Select Policy** next to IMC Access and then click **Create New**.

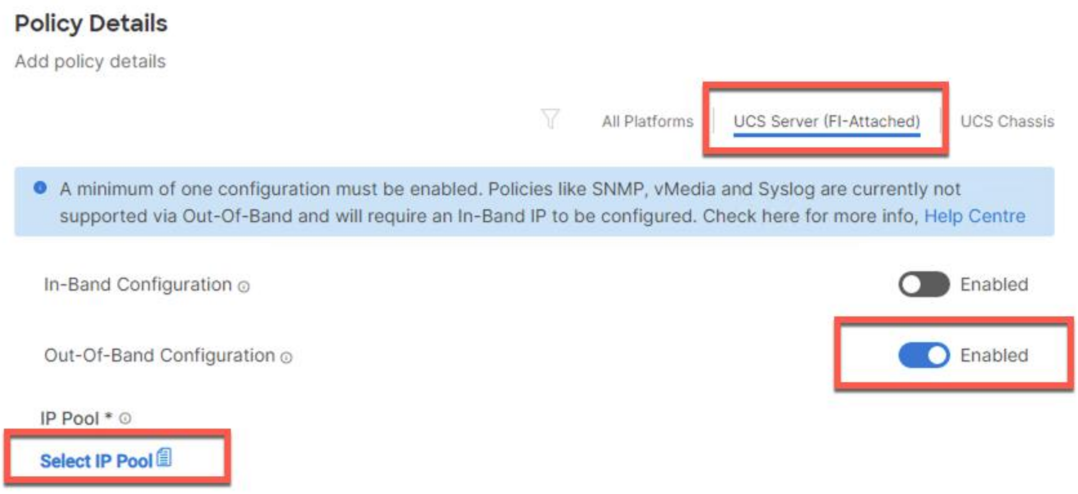
Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-IMC-Access).

Step 3. Click **Next**.

Note: You can select in-band management access to the compute node using an in-band management VLAN (for example, VLAN 30) or out-of-band management access via the Mgmt0 interfaces of the FIs. KVM Policies like SNMP, vMedia and Syslog are currently not supported via Out-Of-Band and will require an In-Band IP to be configured. Since these policies were not configured in this deployment, out-of-band management access was configured so that KVM access to compute nodes is not impacted by any potential switching issues in the fabric.

Step 4. Click **UCS Server (FI-Attached)**.

Step 5. **Enable** Out-Of-Band Configuration.



Policy Details

Add policy details

A minimum of one configuration must be enabled. Policies like SNMP, vMedia and Syslog are currently not supported via Out-Of-Band and will require an In-Band IP to be configured. Check here for more info, Help Centre

In-Band Configuration: Enabled

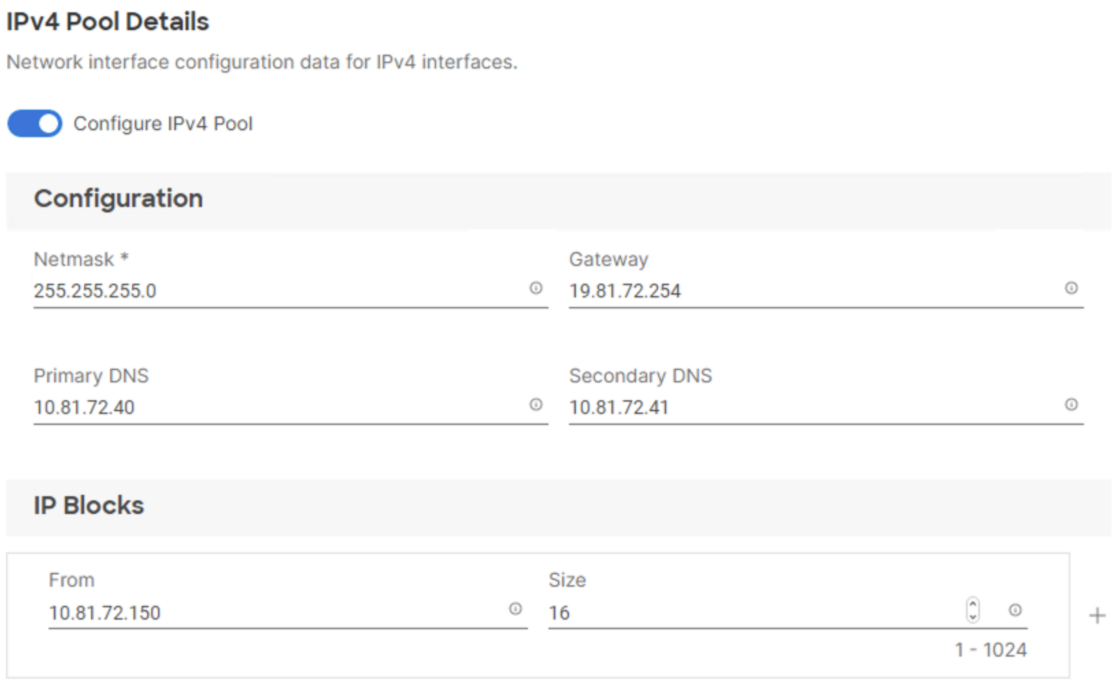
Out-Of-Band Configuration: Enabled

IP Pool *

Step 6. Under IP Pool, click **Select IP Pool** and then click **Create New.**

Step 7. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-IMC-OOB-Pool).

Step 8. Select **Configure IPv4 Pool** and provide the information to define a pool for KVM IP address assignment including an IP Block.



IPv4 Pool Details

Network interface configuration data for IPv4 interfaces.

Configure IPv4 Pool

Configuration

Netmask *: 255.255.255.0

Gateway: 19.81.72.254

Primary DNS: 10.81.72.40

Secondary DNS: 10.81.72.41

IP Blocks

From: 10.81.72.150

Size: 16

1 - 1024

Note: The management IP pool subnet should be accessible from the host that is trying to open the KVM connection. In the example shown here, the hosts trying to open a KVM connection would need to be able to route to 10.81.72.0/24 subnet.

Step 9. Click **Next.**

Step 10. Deselect **Configure IPv6 Pool**.

Step 11. Click **Create** to finish configuring the IP address pool.

Step 12. Click **Create** to finish configuring the IMC access policy.

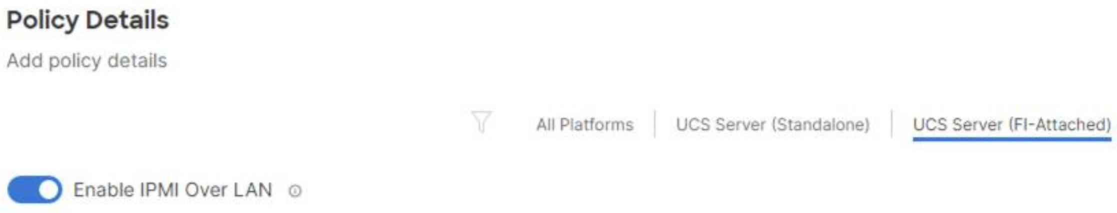
Procedure 6. Configure IPMI Over LAN Policy

Step 1. Click **Select Policy** next to IPMI Over LAN and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, Enable-IPMIoLAN).

Step 3. Turn on **Enable IPMI Over LAN**.

Step 4. Click **Create**.



Policy Details

Add policy details

Enable IPMI Over LAN

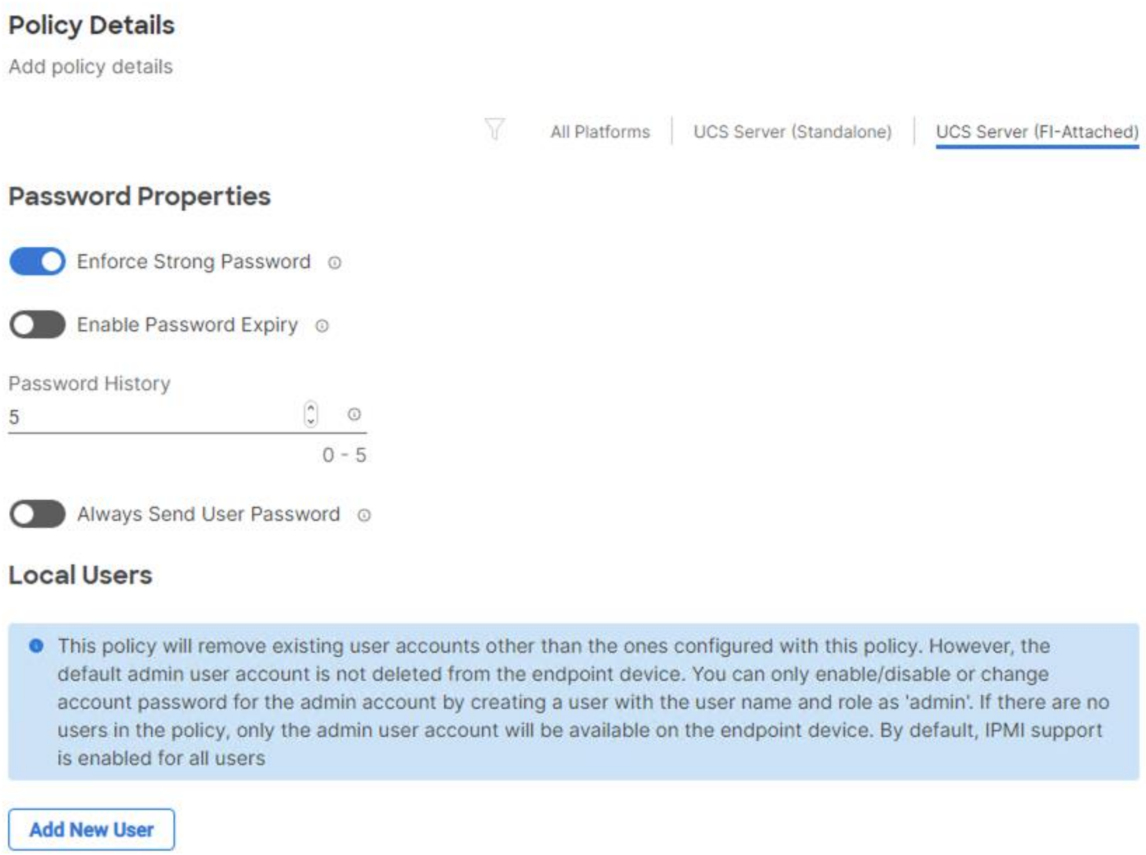
Procedure 7. Configure Local User Policy

Step 1. Click **Select Policy** next to Local User and the, in the pane on the right, click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-LocalUser-Pol).

Step 3. Verify that **UCS Server (FI-Attached)** is selected.

Step 4. Verify that **Enforce Strong Password** is selected.



Policy Details

Add policy details

Password Properties

Enforce Strong Password: on

Enable Password Expiry: off

Password History: 5 (0 - 5)

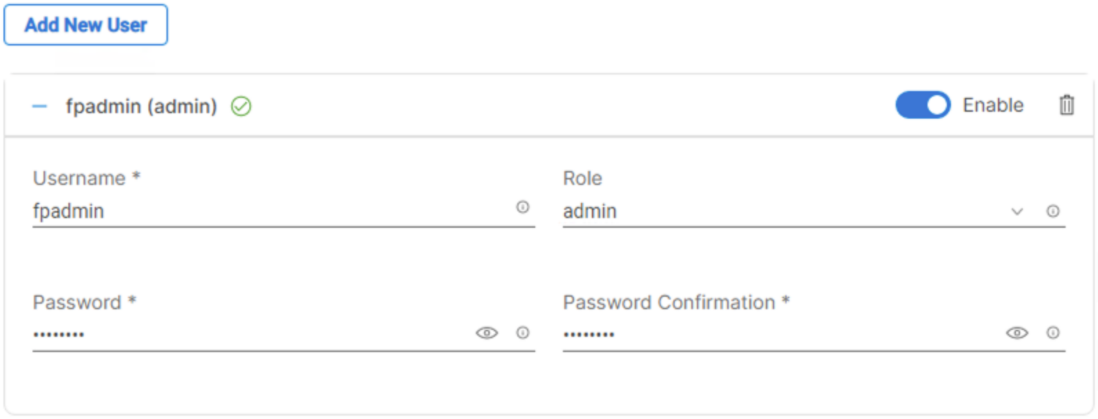
Always Send User Password: off

Local Users

This policy will remove existing user accounts other than the ones configured with this policy. However, the default admin user account is not deleted from the endpoint device. You can only enable/disable or change account password for the admin account by creating a user with the user name and role as 'admin'. If there are no users in the policy, only the admin user account will be available on the endpoint device. By default, IPMI support is enabled for all users

Step 5. Click **Add New User** and then click **+** next to the New User

Step 6. Provide the username (for example, fpadmin), choose a role for example, admin), and provide a password.



fpadmin (admin) ✓

Username *: fpadmin

Role: admin

Password *: ••••••••

Password Confirmation *: ••••••••

Note: The username and password combination defined here will be used to log into KVMs. The typical Cisco UCS admin username and password combination cannot be used for KVM access.

Step 7. Click **Create** to finish configuring the user.

Step 8. Click **Create** to finish configuring local user policy.

Step 9. Click **Next** to move to Storage Configuration.

Procedure 8. Storage Configuration

Step 1. Click **Next** on the Storage Configuration screen. No configuration is needed in the local storage system.

Step 2. **Network Configuration** > **LAN Connectivity**

LAN connectivity policy defines the connections and network communication resources between the server and the LAN. This policy uses pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network. For iSCSI hosts, this policy also defined an IQN address pool.

For consistent vNIC and vHBA placement, manual vHBA/vNIC placement is utilized. ISCSI boot from SAN hosts and FC boot from SAN hosts require different number of vNICs/vHBAs and different placement order therefore the iSCSI host and the FC host LAN connectivity policies are explained separately in this section.

Procedure 9. Create LAN Connectivity Policy for FC Hosts

The FC boot from SAN hosts uses 4 vNICs configured as follows:

Table 18. vNICs for FC LAN Connectivity

vNIC/vHBA Name	Slot ID	Switch ID	PCI Order	VLANs
01-vSwitch0-A	MLOM	A	2	IB-MGMT, NFS
02-vSwitch0-B	MLOM	B	3	IB-MGMT, NFS
03-VDS0-A	MLOM	A	4	VM Traffic, vMotion
04-VDS0-B	MLOM	B	5	VM Traffic, vMotion

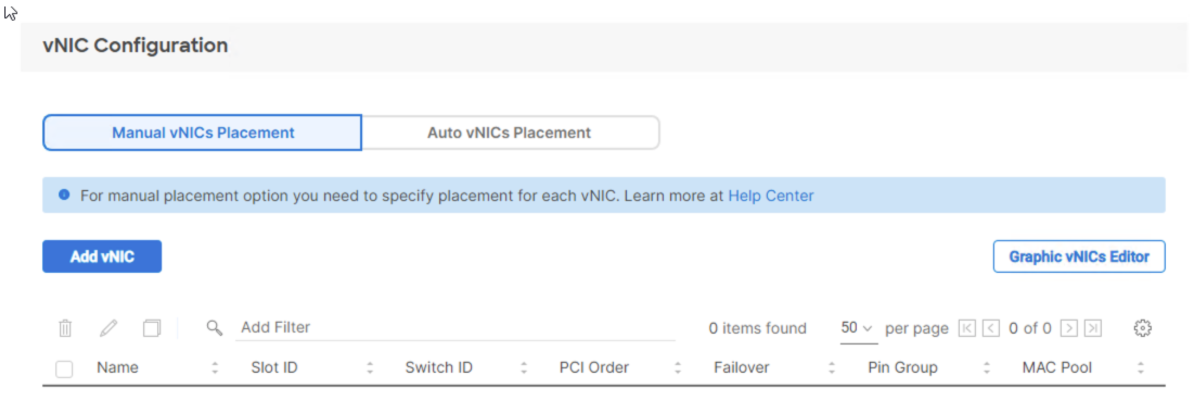
Note: The PCI order 0 and 1 will be used in the SAN Connectivity policy to create vHBA-A and vHBA-B.

Step 1. Click **Select Policy** next to LAN Connectivity and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-FC-ESXi-LanConn). Click **Next.**

Step 3. Under vNIC Configuration, select **Manual vNICs Placement**.

Step 4. Click **Add vNIC**.



vNIC Configuration

For manual placement option you need to specify placement for each vNIC. Learn more at Help Center

0 items found

50 per page

0 of 0

Name	Slot ID	Switch ID	PCI Order	Failover	Pin Group	MAC Pool

Procedure 10. Create MAC Address Pool for Fabric A and B

When creating the first vNIC, the MAC address pool has not been defined yet, therefore a new MAC address pool will need to be created. Two separate MAC address pools are configured for each Fabric. MAC-Pool-A will be reused for all Fabric-A vNICs, and MAC-Pool-B will be reused for all Fabric-B vNICs.

Table 19. MAC Address Pools

Pool Name	Starting MAC Address	Size	vNICs
MAC-Pool-A	00:25:B5:17:0A:00	64*	01-vSwitch0-A, 03-VDS0-A
MAC-Pool-B	00:25:B5:17:0B:00	64*	02-vSwitch0-B, 04-VDS0-B

Note: Each server requires 2 MAC addresses from the pool. Adjust the size of the pool according to your requirements.

Step 1. Click **Select Pool** under MAC Address Pool and then click **Create New**.

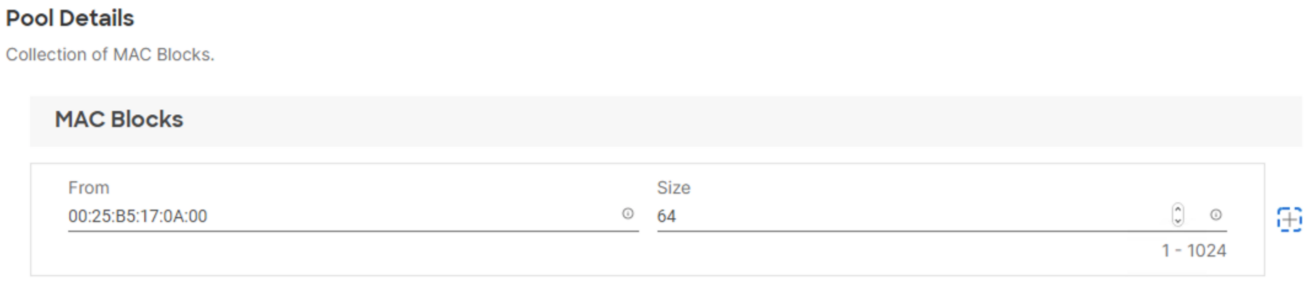
Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the pool from Table 19 depending on the vNIC being created (for example, MAC-Pool-A for Fabric A).

Step 3. Click **Next**.

Step 4. Provide the starting MAC address from Table 19 (for example, 00:25:B5:17:0A:00)

Note: For troubleshooting FlexPod, some additional information is always coded into the MAC address pool. For example, in the starting address 00:25:B5:17:0A:00, 17 is the rack ID and 0A indicates Fabric A.

Step 5. Provide the size of the MAC address pool from Table 19 (for example, 64).



Pool Details

Collection of MAC Blocks.

MAC Blocks

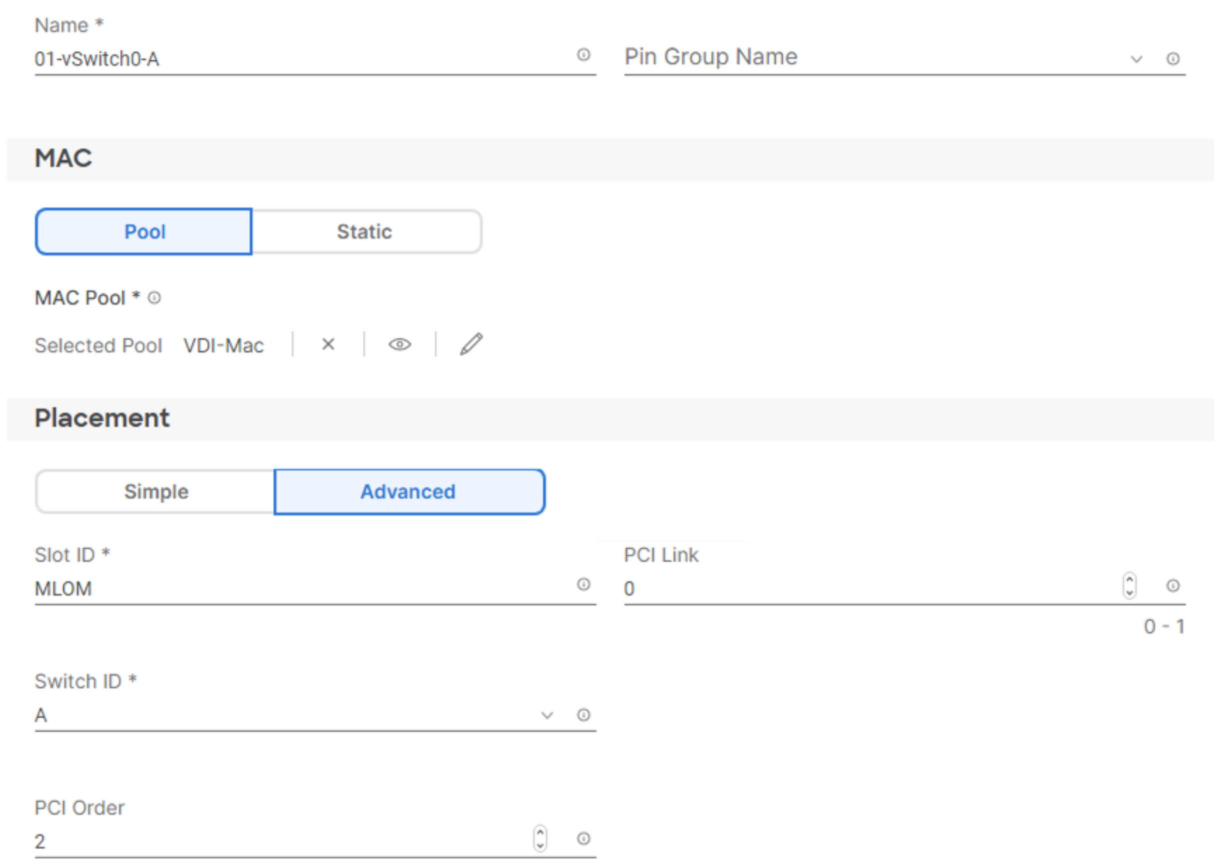
From: 00:25:B5:17:0A:00

Size: 64

1 - 1024

Step 6. Click **Create** to finish creating the MAC address pool.

Step 7. From the Add vNIC window, provide vNIC Name, Slot ID, Switch ID, and PCI Order information from Table 18.



Name *
01-vSwitch0-A

Pin Group Name

MAC

Pool | Static

MAC Pool *

Selected Pool VDI-Mac

Placement

Simple | Advanced

Slot ID *
MLOM

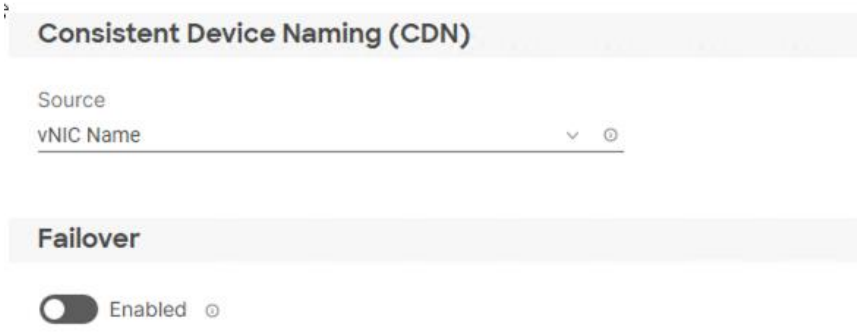
PCI Link
0
0 - 1

Switch ID *
A

PCI Order
2

Step 8. For Consistent Device Naming (CDN), from the drop-down list, select **vNIC Name**.

Step 9. Verify that Failover is disabled because the failover will be provided by attaching multiple NICs to the VMware vSwitch and VDS.



Consistent Device Naming (CDN)

Source
vNIC Name

Failover

Enabled

Procedure 11. Create Ethernet Network Group Policy for a vNIC

The Ethernet Network Group policies will be created and reused on applicable vNICs as explained below. The Ethernet Network Group policy defines the VLANs allowed for a particular vNIC, therefore multiple network group policies will be defined for this deployment as follows:

Table 20. Ethernet Group Policy Values

Group Policy Name	Native VLAN	Apply to vNICs	VLANs
VDI-vSwitch0-NetGrp	Native-VLAN (2)	01-vSwitch0-A, 02-vSwitch0-B	IB-MGMT, NFS

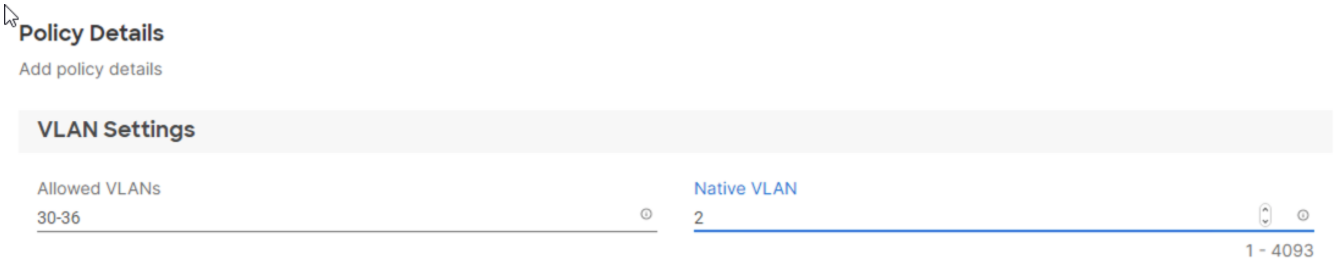
Group Policy Name	Native VLAN	Apply to vNICs	VLANs
VDI-VDS0-NetGrp	Native-VLAN (2)	03-VDS0-A, 04-VDS0-B	VM Traffic, vMotion

Step 10. Click **Select Policy** under Ethernet Network Group Policy and then click **Create New**.

Step 11. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy from Table 20 (for example, VDI-vSwitch0-NetGrp).

Step 12. Click **Next**.

Step 13. Enter the allowed VLANs from Table 20 (for example, 30-36) and the native VLAN ID from Table 20 (for example, 2).



Policy Details

Add policy details

VLAN Settings

Allowed VLANs: 30-36

Native VLAN: 2

1 - 4093

Step 14. Click **Create** to finish configuring the Ethernet network group policy.

Note: When ethernet group policies are shared between two vNICs, the ethernet group policy only needs to be defined for the first vNIC. For subsequent vNIC policy mapping, just click **Select Policy** and pick the previously defined ethernet group policy from the list on the right.

Procedure 12. Create Ethernet Network Control Policy

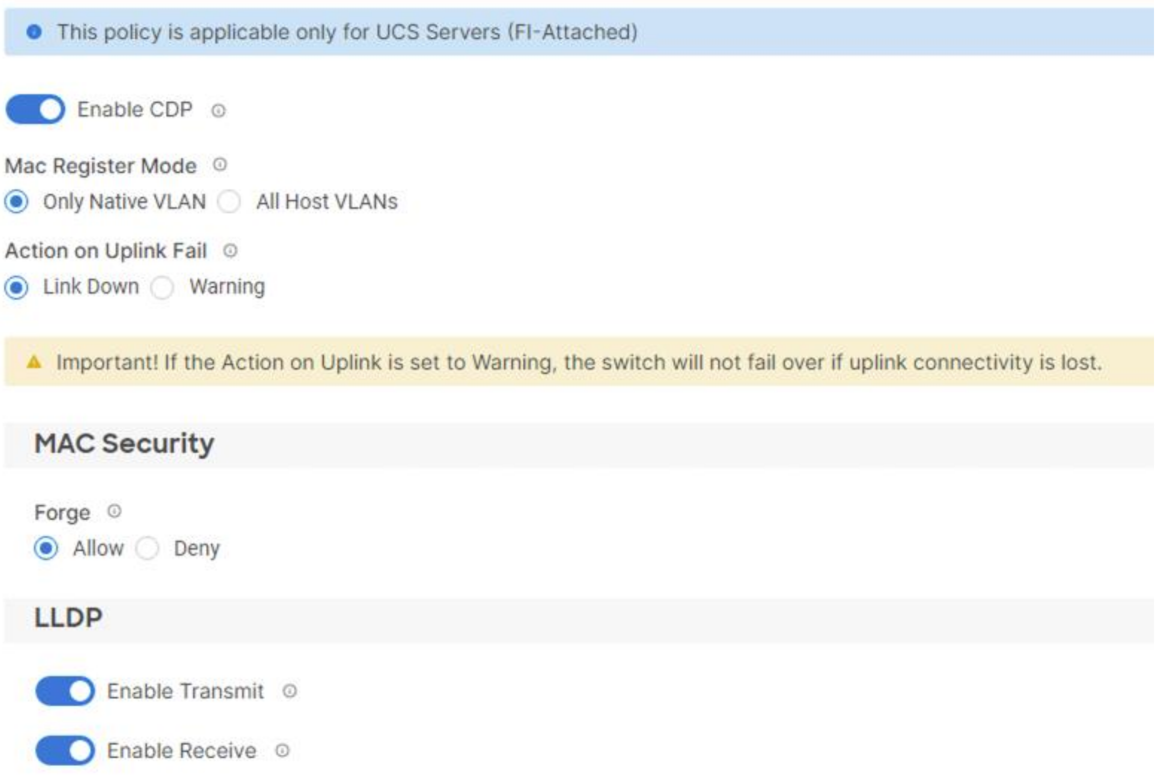
The Ethernet Network Control Policy is used to enable Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) for the vNICs. A single policy will be created and reused for all the vNICs.

Step 1. Click **Select Policy** under Ethernet Network Control Policy and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-Enable-CDP-LLDP).

Step 3. Click **Next**.

Step 4. **Enable Cisco Discovery Protocol** and both **Enable Transmit** and **Enable Receive** under LLDP.



This policy is applicable only for UCS Servers (FI-Attached)

Enable CDP: on

Mac Register Mode
● Only Native VLAN ○ All Host VLANs

Action on Uplink Fail
● Link Down ○ Warning

Important! If the Action on Uplink is set to Warning, the switch will not fail over if uplink connectivity is lost.

MAC Security

Forge
● Allow ○ Deny

LLDP

Enable Transmit: on

Enable Receive: on

Step 5. Click **Create** to finish creating Ethernet network control policy.

Procedure 13. Create Ethernet QoS Policy

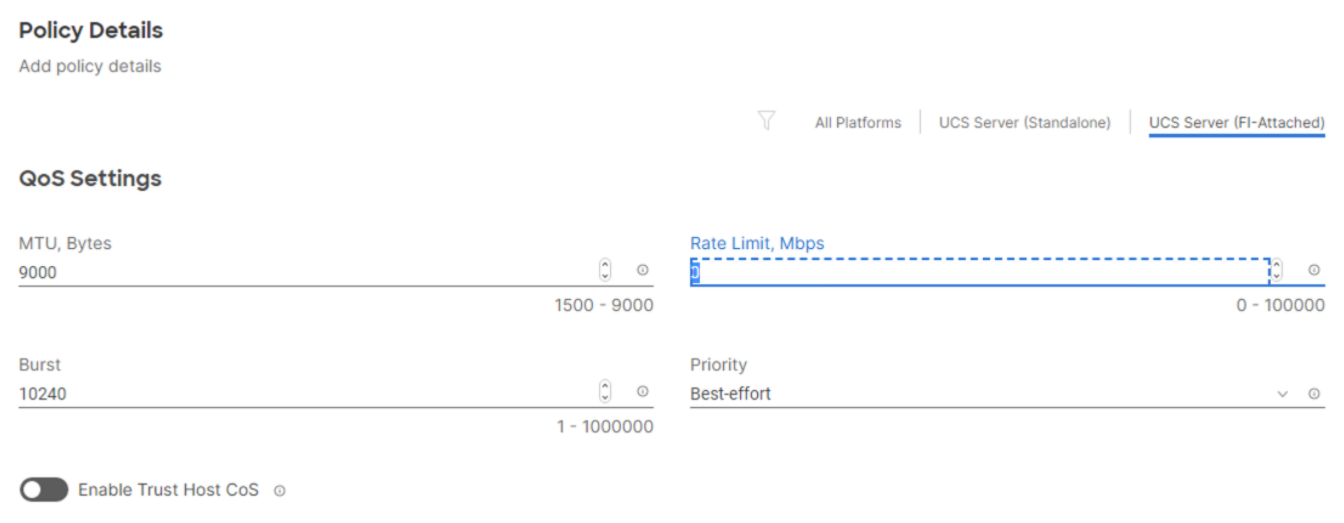
Ethernet QoS policy is used to enable jumbo maximum transmission units (MTUs) for all the vNICs. A single policy will be created and reused for all the vNICs.

Step 1. Click **Select Policy** under Ethernet QoS and click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-EthQos-Pol).

Step 3. Click **Next**.

Step 4. Change the MTU, Bytes value to **9000**.



Policy Details

Add policy details

QoS Settings

MTU, Bytes

9000

1500 - 9000

Rate Limit, Mbps

0

0 - 100000

Burst

10240

1 - 1000000

Priority

Best-effort

Enable Trust Host CoS

Step 5. Click **Create** to finish setting up the Ethernet QoS policy.

Procedure 14. Create Ethernet Adapter Policy

Ethernet adapter policy is used to set the interrupts and the send and receive queues. The values are set according to the best-practices guidance for the operating system in use. Cisco Intersight provides default VMware Ethernet Adapter policy for typical VMware deployments.

Optionally, you can configure a tweaked ethernet adapter policy for additional hardware receive queues handled by multiple CPUs in scenarios where there is a lot of vMotion traffic and multiple flows. In this deployment, a modified ethernet adapter policy, VDI-VMware-High-Traffic, is created and attached to the 03-VDS0-A and 04-VDS0-B interfaces which handle vMotion.

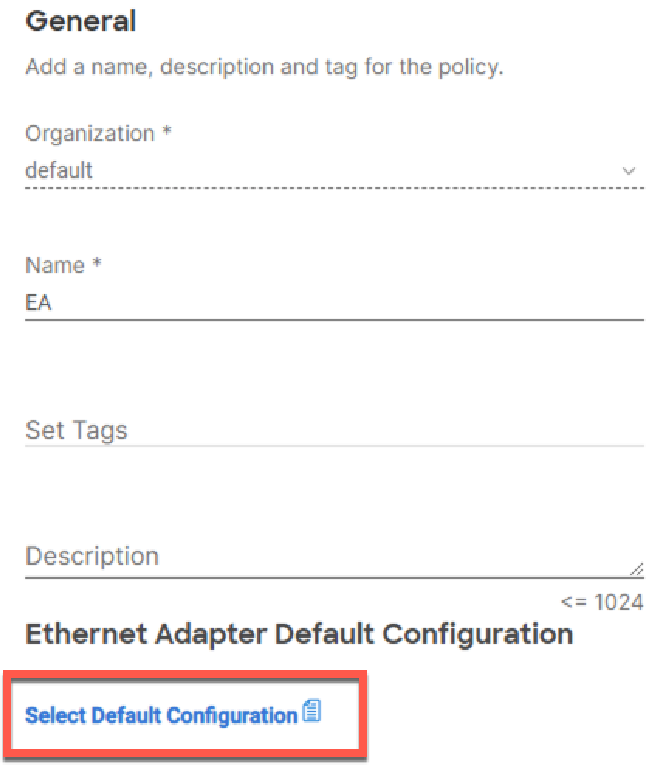
Table 21. Ethernet Adapter Policy association to vNICs

Policy Name	vNICs
VDI-EthAdapter-VMware	01-vSwitch0-A, 02-vSwitch0-B
VDI-VMware-High-Traffic	03-VDS0-A, 04-VDS0-B,

Step 1. Click **Select Policy** under Ethernet Adapter and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-EthAdapter-VMware).

Step 3. Click **Select Default Configuration** under Ethernet Adapter Default Configuration.



General

Add a name, description and tag for the policy.

Organization *
default

Name *
EA

Set Tags

Description

<= 1024

Ethernet Adapter Default Configuration

Select Default Configuration

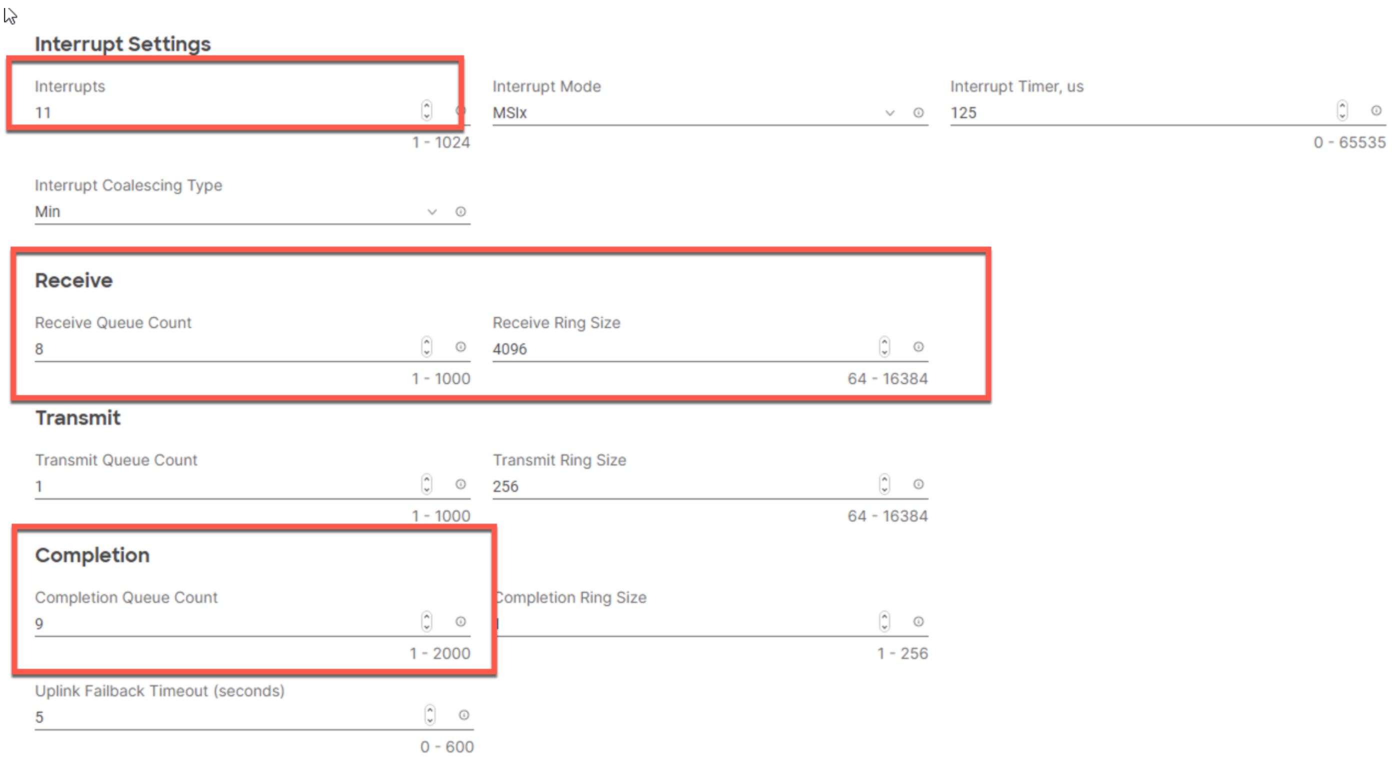
Step 4. From the list, select **VMware.**

Step 5. Click **Next.**

Step 6. For the VDI-EthAdapter-VMware policy, click **Create** and skip the rest of the steps in this section.

Step 7. For the optional VDI-VMware-High-Traffic policy (for VDS interfaces), make the following modifications to the policy:

- Increase Interrupts to 11
- Increase Receive Queue Count to 8
- Increase Completion Queue Count to 9
- Enable Receive Side Scaling



Interrupt Settings

Interrupts
11
1 - 1024

Interrupt Mode
MSIx

Interrupt Timer, us
125
0 - 65535

Interrupt Coalescing Type
Min

Receive

Receive Queue Count
8
1 - 1000

Receive Ring Size
4096
64 - 16384

Transmit

Transmit Queue Count
1
1 - 1000

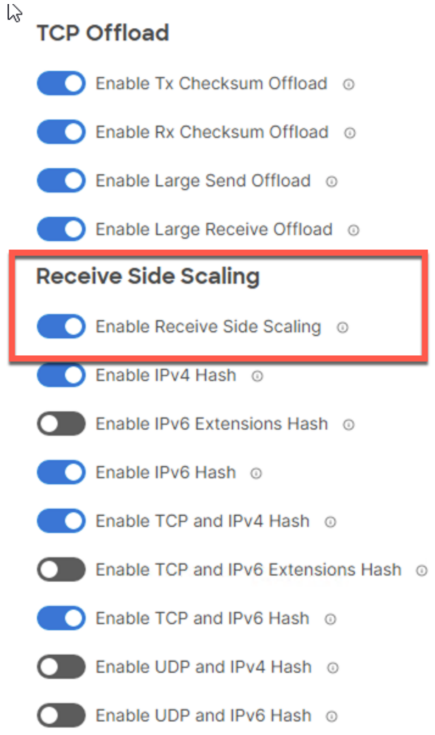
Transmit Ring Size
256
64 - 16384

Completion

Completion Queue Count
9
1 - 2000

Completion Ring Size
1 - 256

Uplink Failback Timeout (seconds)
5
0 - 600



TCP Offload

● Enable Tx Checksum Offload

● Enable Rx Checksum Offload

● Enable Large Send Offload

● Enable Large Receive Offload

Receive Side Scaling

● Enable Receive Side Scaling

● Enable IPv4 Hash

○ Enable IPv6 Extensions Hash

● Enable IPv6 Hash

● Enable TCP and IPv4 Hash

○ Enable TCP and IPv6 Extensions Hash

● Enable TCP and IPv6 Hash

○ Enable UDP and IPv4 Hash

○ Enable UDP and IPv6 Hash

Step 8. Click **Create.**

Step 9. Click **Create** to finish creating the vNIC.

Step 10. Go back to Step 1 and repeat vNIC creation for all four vNICs.

Step 11. Verify all four vNICs were successfully created.

Step 12. Click **Create** to finish creating the LAN Connectivity policy for FC hosts.

Procedure 15. Create the SAN Connectivity Policy

A SAN connectivity policy determines the network storage resources and the connections between the server and the storage device on the network. This policy enables customers to configure the vHBAs that the servers use to communicate with the SAN.

Note: SAN Connectivity policy is not needed for iSCSI boot from SAN hosts and can be skipped.

Table 22 lists the details of two vHBAs that are used to provide FC connectivity and boot from SAN functionality.

Table 22. vHBA for boot from FC SAN

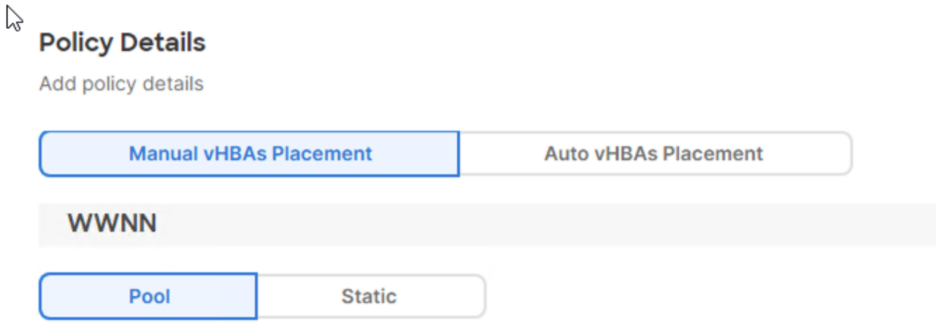
vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-A	MLOM	A	0
vHBA-B	MLOM	B	1

Step 1. Click **Select Policy** next to SAN Connectivity and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-SanConn-Pol).

Step 3. Select **Manual vHBAs Placement**.

Step 4. Select **Pool** under WWNN Address.



Procedure 16. Create the WWNN Address Pool

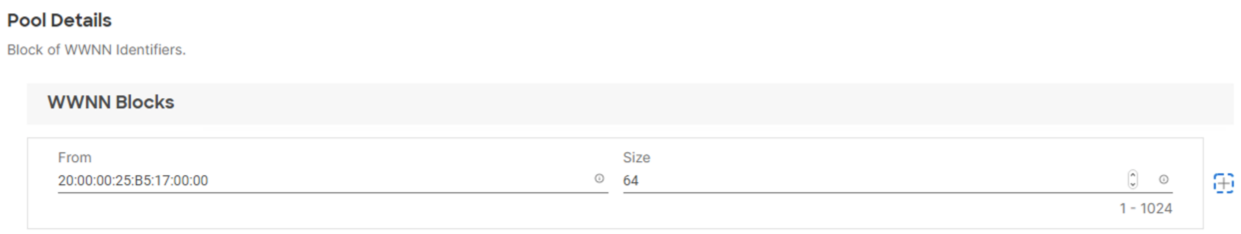
The WWNN address pools have not been defined yet therefore a new WWNN address pool has to be defined.

Step 1. Click **Select Pool** under WWNN Address Pool and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-WWNN-Pool).

Step 3. Click **Next**.

Step 4. Provide the starting WWNN block address and the size of the pool.



Pool Details

Block of WWNN Identifiers.

WWNN Blocks

From: 20:00:00:25:B5:17:00:00

Size: 64

1 - 1024

Note: As a best practice, in FlexPod some additional information is always coded into the WWNN address pool for troubleshooting. For example, in the address 20:00:00:25:B5:17:00:00, 17 is the rack ID.

Step 5. Click **Create** to finish creating the WWNN address pool.

Procedure 17. Create the vHBA-A for SAN A

Step 1. Click **Add vHBA**.

Step 2. For vHBA Type, select **fc-initiator** from the drop-down list.

Procedure 18. Create the WWPN Pool for SAN A

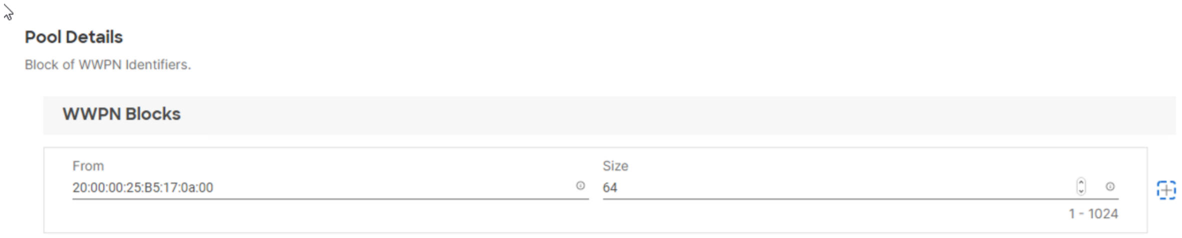
The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric A will be defined. This pool will also be used for the NVMe-o-FC vHBAs if the vHBAs are defined.

Step 1. Click **Select Pool** under WWPN Address Pool and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-WWPN-Pool-A).

Step 3. Provide the starting WWPN block address for SAN A and the size.

Note: As a best practice, in FlexPod some additional information is always coded into the WWPN address pool for troubleshooting. For example, in the address 20:00:00:25:B5:17:0A:00, 17 is the rack ID and 0A signifies SAN A.



Pool Details

Block of WWPN Identifiers.

WWPN Blocks

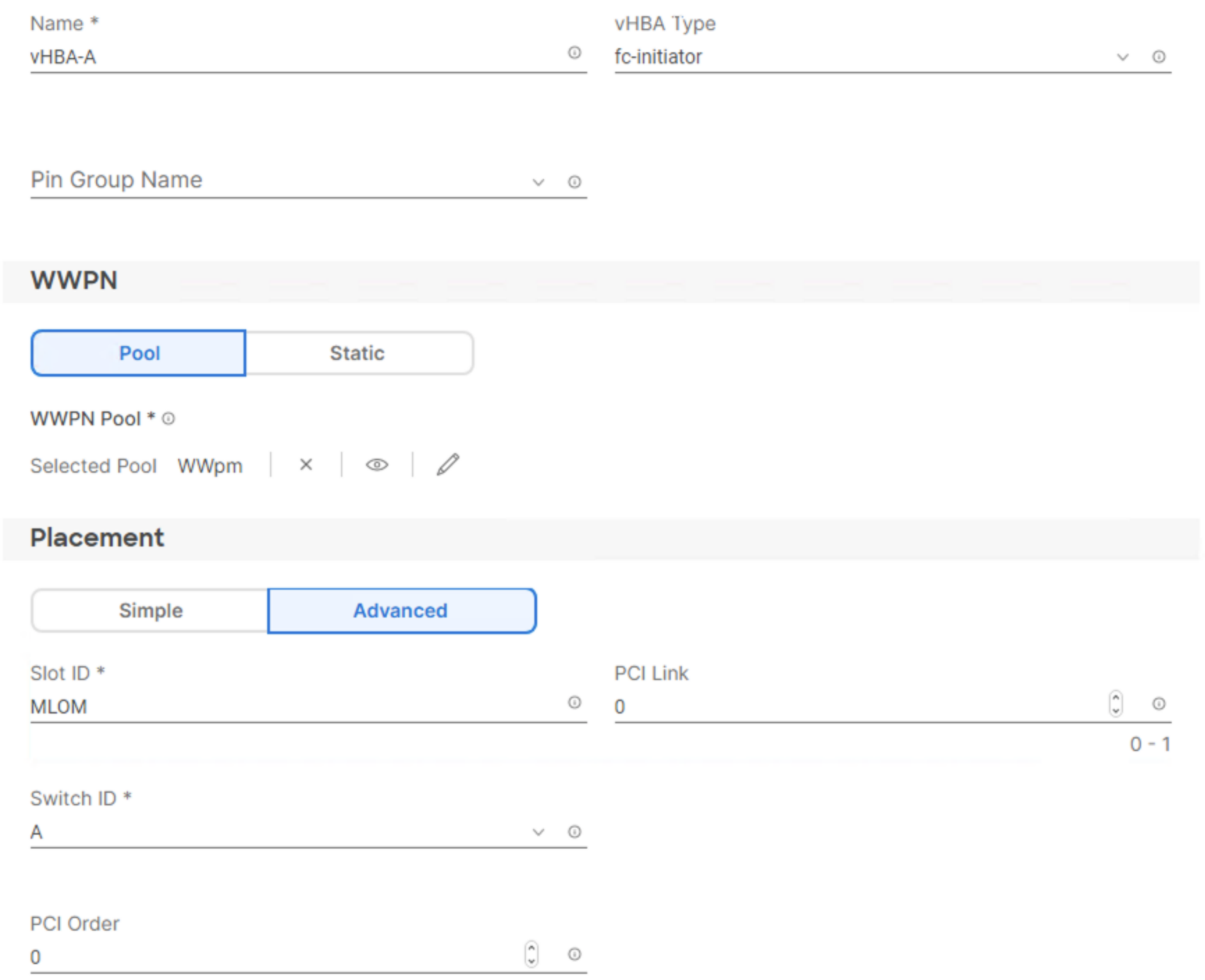
From: 20:00:00:25:B5:17:0a:00

Size: 64

1 - 1024

Step 4. Click **Create** to finish creating the WWPN pool.

Step 5. Back in the Create vHBA window, provide the Name (for example, vHBA-A), Switch ID (for example, A) and PCI Order from Table 21.



Name *
vHBA-A

vHBA Type
fc-initiator

Pin Group Name

WWPN

Pool | Static

WWPN Pool *
Selected Pool WWpm

Placement

Simple | Advanced

Slot ID *
MLOM

PCI Link
0
0 - 1

Switch ID *
A

PCI Order
0

Procedure 19. Create Fibre Channel Network Policy for SAN A

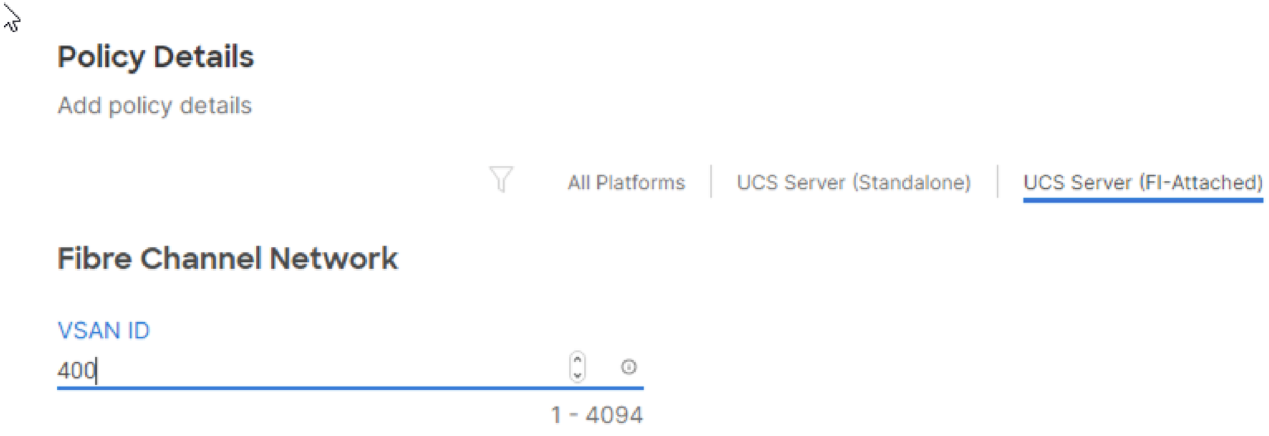
A Fibre Channel network policy governs the VSAN configuration for the virtual interfaces. In this deployment, VSAN 101 will be used for vHBA-A.

Step 1. Click **Select Policy** under Fibre Channel Network and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-SAN-A-Network).

Step 3. For the scope, select **UCS Server (FI-Attached)**.

Step 4. Under VSAN ID, provide the VSAN information (for example, 400).



Policy Details

Add policy details

Fibre Channel Network

VSAN ID

400

1 - 4094

Step 5. Click **Create** to finish creating the Fibre Channel network policy.

Procedure 20. Create Fibre Channel QoS Policy

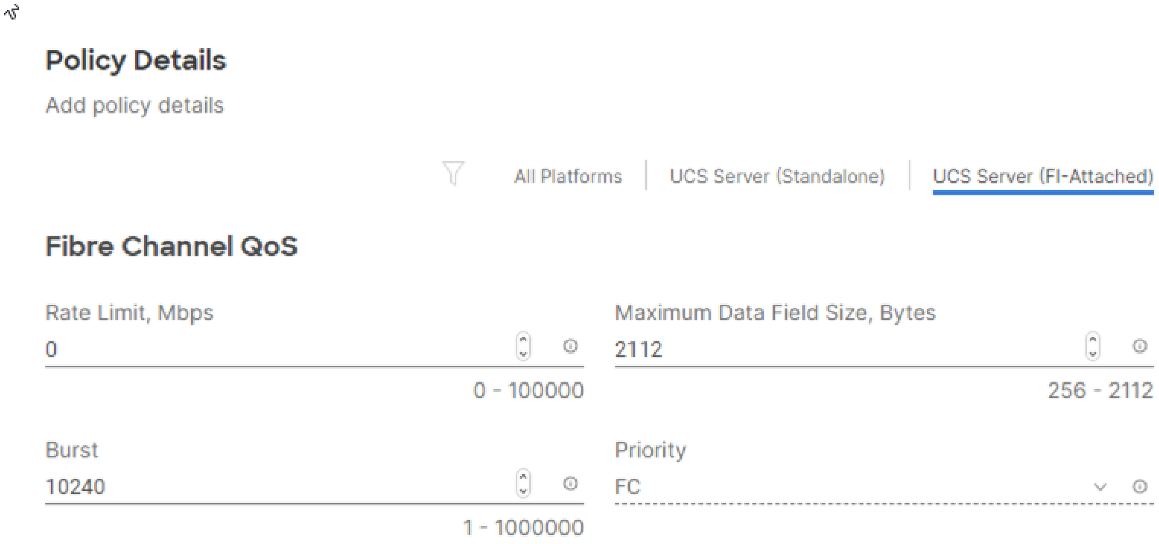
The Fibre Channel QoS policy assigns a system class to the outgoing traffic for a vHBA. This system class determines the quality of service for the outgoing traffic. The Fibre Channel QoS policy used in this deployment uses default values and will be shared by all vHBAs.

Step 1. Click **Select Policy** under Fibre Channel QoS and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-FC-QoS).

Step 3. For the scope, select **UCS Server (FI-Attached)**.

Step 4. Do not change the default values on the Policy Details screen.



Policy Details

Add policy details

Fibre Channel QoS

Rate Limit, Mbps

0

0 - 100000

Maximum Data Field Size, Bytes

2112

256 - 2112

Burst

10240

1 - 1000000

Priority

FC

Step 5. Click **Create** to finish creating the Fibre Channel QoS policy.

Procedure 21. Create Fibre Channel Adapter Policy

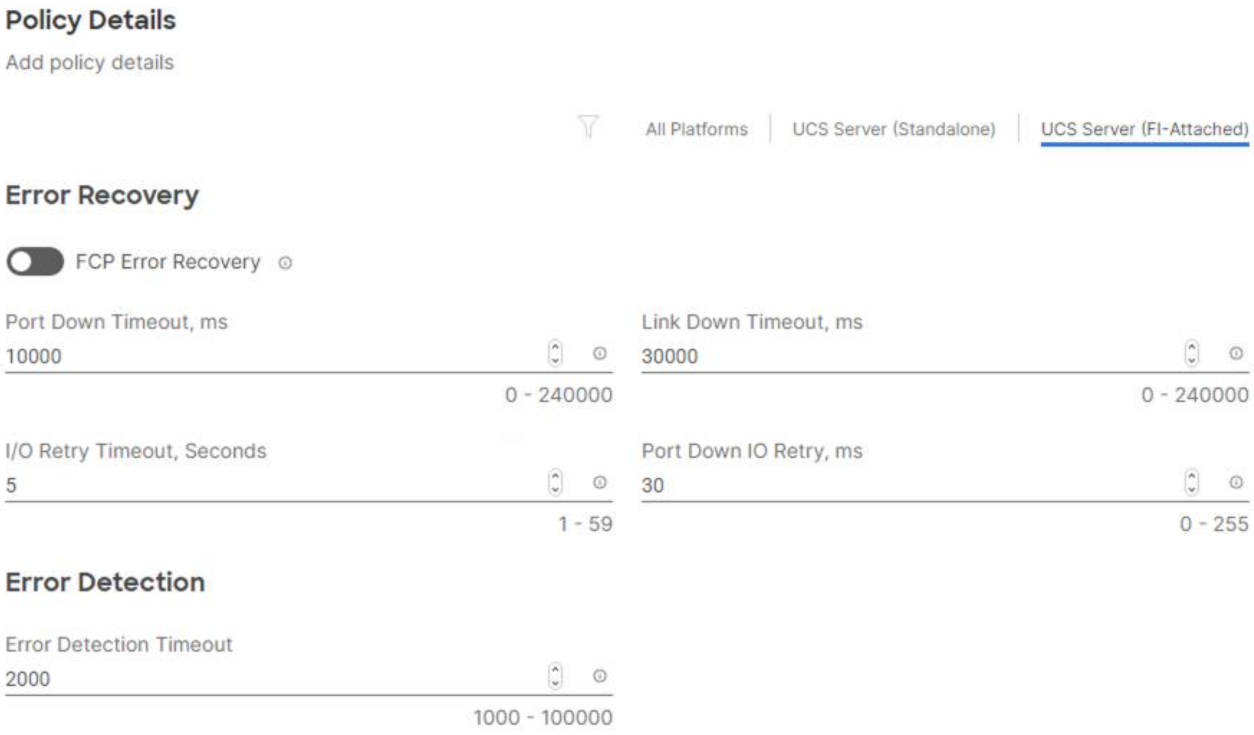
A Fibre Channel adapter policy governs the host-side behavior of the adapter, including the way that the adapter handles traffic. This validation uses the default values for the adapter policy, and the policy will be shared by all the vHBAs.

Step 1. Click **Select Policy** under Fibre Channel Adapter and then click **Create New.**

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-FC-Adapter).

Step 3. For the scope, select **UCS Server (FI-Attached)**.

Step 4. Do not change the default values on the Policy Details screen.



Policy Details

Add policy details

Error Recovery

FCP Error Recovery

Port Down Timeout, ms: 10000 (0 - 240000)

Link Down Timeout, ms: 30000 (0 - 240000)

I/O Retry Timeout, Seconds: 5 (1 - 59)

Port Down IO Retry, ms: 30 (0 - 255)

Error Detection

Error Detection Timeout: 2000 (1000 - 100000)

Step 5. Click **Create** to finish creating the Fibre Channel adapter policy.

Step 6. Click **Add** to create vHBA-A.

Procedure 22. Create the vHBA for SAN B

Step 1. Click **Add vHBA.**

Step 2. For vHBA Type, select **fc-initiator** from the drop-down list.

Procedure 23. Create the WWPN Pool for SAN B

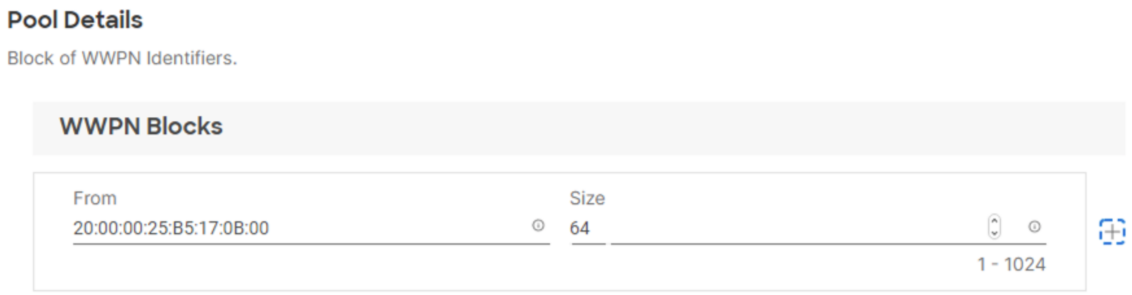
The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric B will be defined. This pool will also be used for the NVMe-o-FC vHBAs if the vHBAs are defined.

Step 1. Click **Select Pool** under WWPN Address Pool and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-WWPN-Pool-B).

Step 3. Provide the starting WWPN block address for SAN B and the size.

Note: As a best practice, in FlexPod some additional information is always coded into the WWPN address pool for troubleshooting. For example, in the address 20:00:00:25:B5:17:0B:00, 17 is the rack ID and 0B signifies SAN B.



Pool Details

Block of WWPN Identifiers.

WWPN Blocks

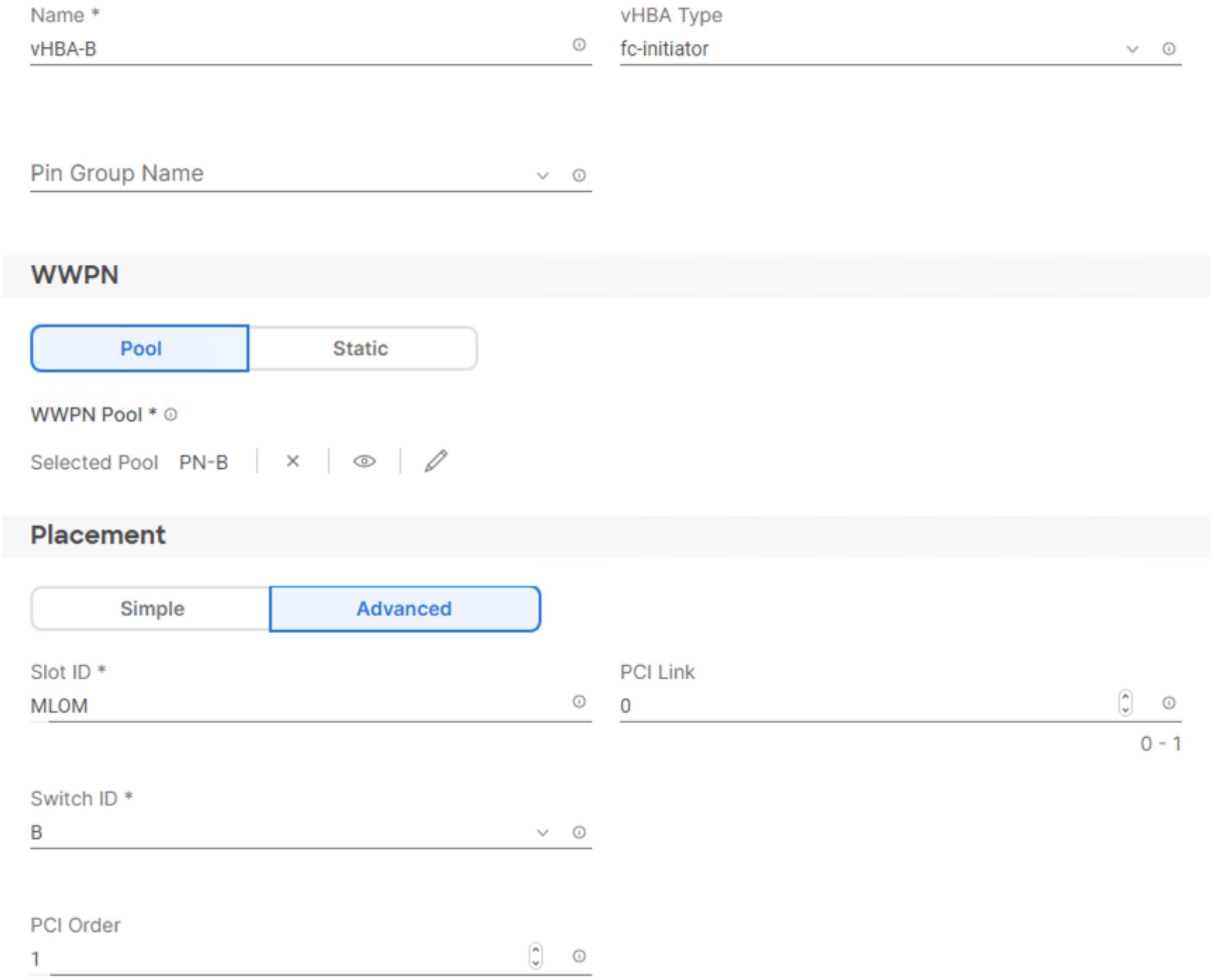
From: 20:00:00:25:B5:17:0B:00

Size: 64

1 - 1024

Step 4. Click **Create** to finish creating the WWPN pool.

Step 5. Back in the Create vHBA window, provide the Name (for example, vHBA-B), Switch ID (for example, B) and PCI Order from Table 21.



Name *: vHBA-B

vHBA Type: fc-initiator

Pin Group Name

WWPN

[✓ Pool] Static

WWPN Pool *

Selected Pool PN-B

Placement

Simple [✓ Advanced]

Slot ID *: MLOM

PCI Link: 0

0 - 1

Switch ID *: B

PCI Order: 1

Procedure 24. Create Fibre Channel Network Policy for SAN B

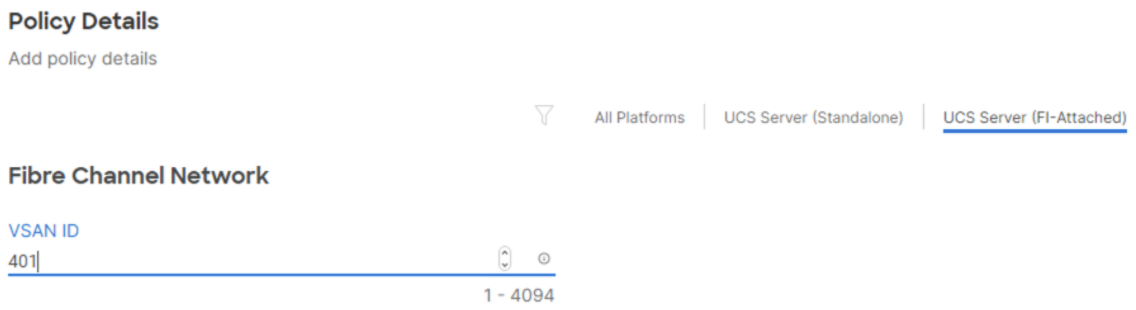
Note: In this deployment, VSAN 401 will be used for vHBA-B.

Step 1. Click **Select Policy** under Fibre Channel Network and then click **Create New**.

Step 2. Verify correct organization is selected from the drop-down list (for example, VDI) and provide a name for the policy (for example, VDI-SAN-B-Network).

Step 3. For the scope, select UCS Server (FI-Attached).

Step 4. Under VSAN ID, provide the VSAN information (for example, 401).



Policy Details

Add policy details

Fibre Channel Network

VSAN ID: 401

1 - 4094

Step 5. Click **Create**.

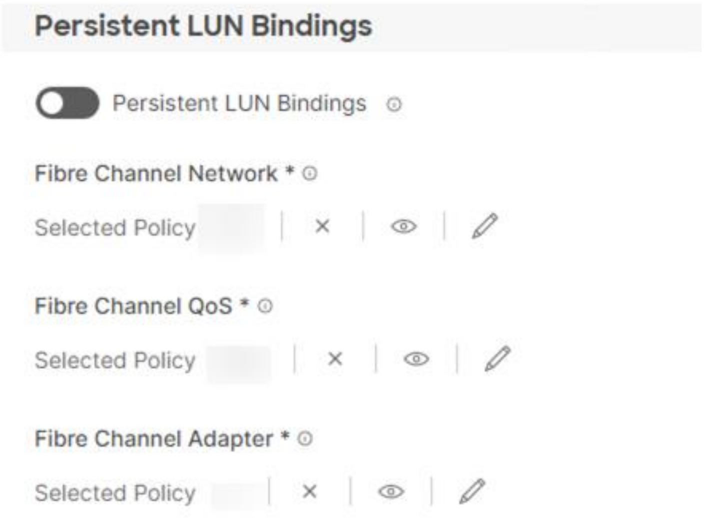
Step 6. Select Fibre Channel QoS policy for SAN B

Step 7. Click **Select Policy** under Fibre Channel QoS and then select the previously created QoS policy VDI-FC-QoS.

Step 8. Select Fibre Channel Adapter policy for SAN B

Step 9. Click **Select Policy** under Fibre Channel Adapter and then select the previously created Adapter policy VDI-FC-Adapter.

Step 10. Verify all the vHBA policies are mapped.



Persistent LUN Bindings

Persistent LUN Bindings

Fibre Channel Network *

Selected Policy

Fibre Channel QoS *

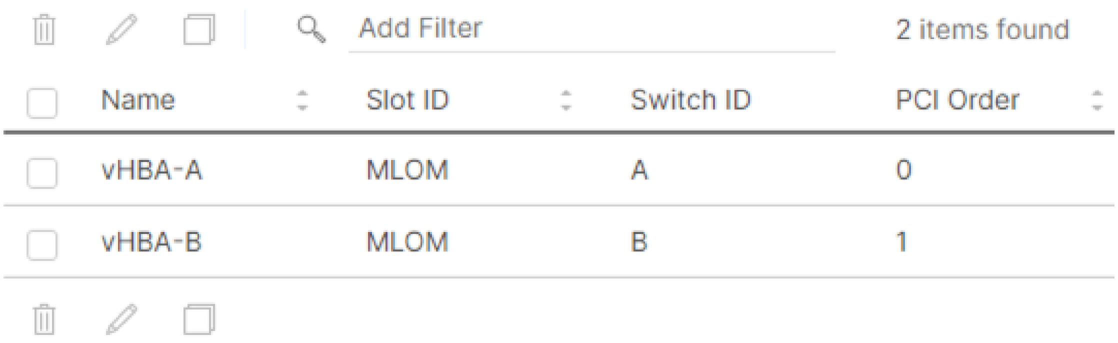
Selected Policy

Fibre Channel Adapter *

Selected Policy

Step 11. Click **Add** to add the vHBA-B.

Step 12. Verify both the vHBAs are added to the SAN connectivity policy.

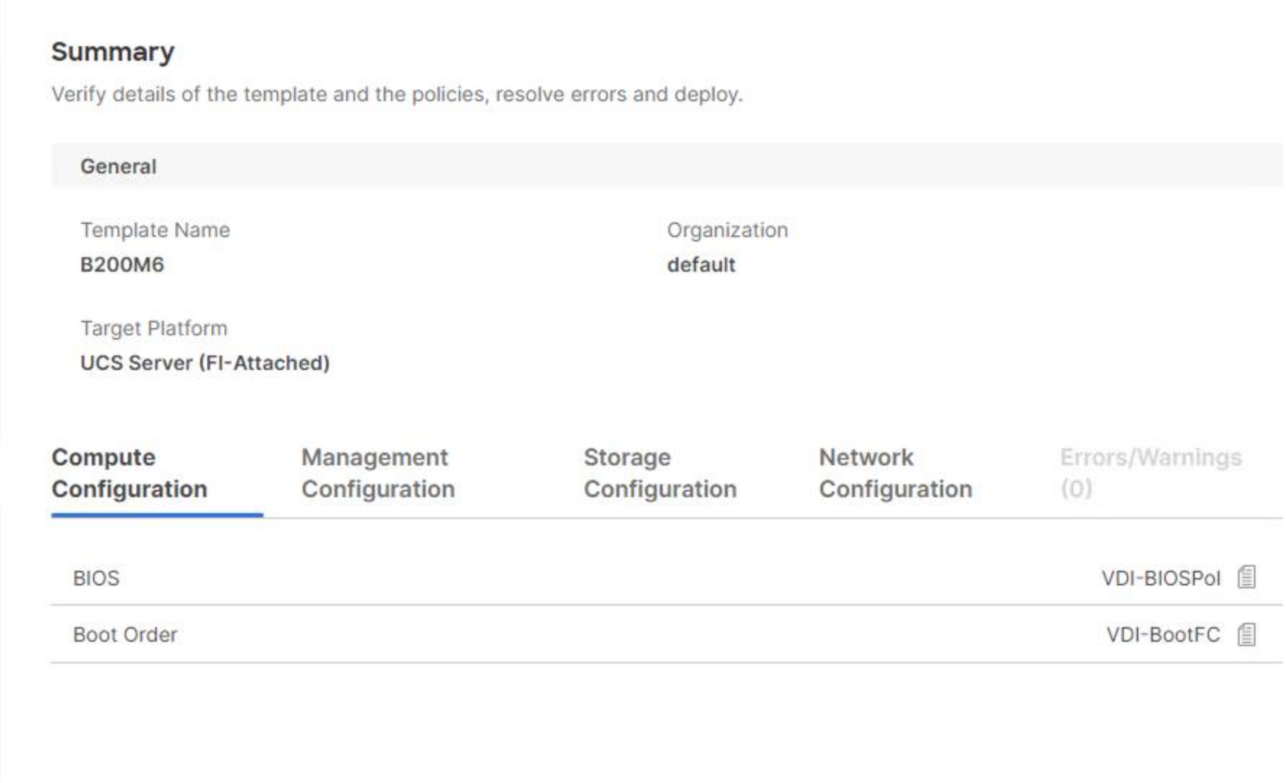


□	Name	Slot ID	Switch ID	PCI Order
□	vHBA-A	MLOM	A	0
□	vHBA-B	MLOM	B	1

Procedure 25. Verify Summary

Step 1. When the LAN connectivity policy and SAN connectivity policy (for FC) is created, click **Next** to move to the Summary screen.

Step 2. On the summary screen, verify policies mapped to various settings. The screenshots below provide summary view for a FC boot from SAN server profile template.



Summary

Verify details of the template and the policies, resolve errors and deploy.

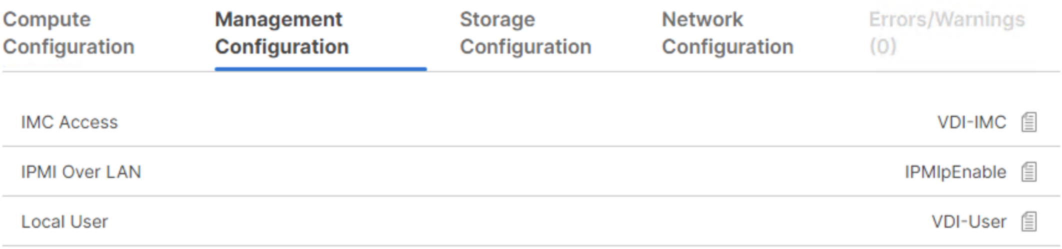
General

Template Name
B200M6

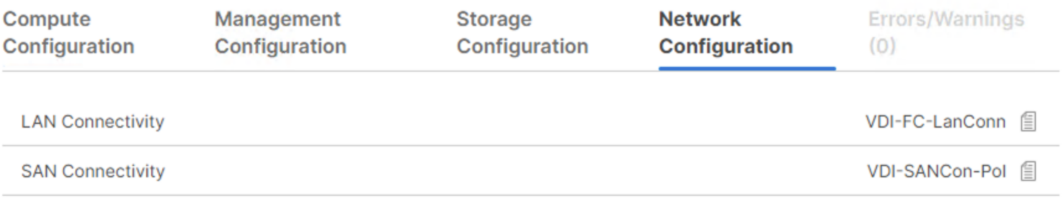
Organization
default

Target Platform
UCS Server (FI-Attached)

BIOS	VDI-BIOSPol
Boot Order	VDI-BootFC



IMC Access	VDI-IMC
IPMI Over LAN	IPMIpEnable
Local User	VDI-User



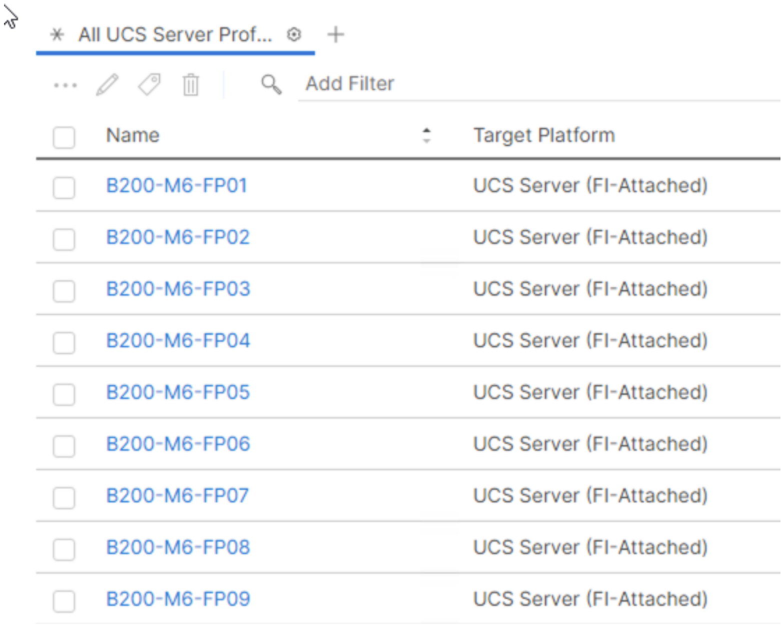
LAN Connectivity	VDI-FC-LanConn
SAN Connectivity	VDI-SANCon-Pol

Procedure 26. Derive Server Profile

Step 1. From the Server profile template Summary screen, click **Derive Profiles**.

Note: This action can also be performed later by navigating to **Templates**, clicking **"…"** next to the template name and selecting **Derive Profiles**.

Step 2. Under the Server Assignment, select **Assign Now** and click **Cisco UCS B200 M6** You can select one or more servers depending on the number of profiles to be deployed.



Name	Target Platform
B200-M6-FP01	UCS Server (FI-Attached)
B200-M6-FP02	UCS Server (FI-Attached)
B200-M6-FP03	UCS Server (FI-Attached)
B200-M6-FP04	UCS Server (FI-Attached)
B200-M6-FP05	UCS Server (FI-Attached)
B200-M6-FP06	UCS Server (FI-Attached)
B200-M6-FP07	UCS Server (FI-Attached)
B200-M6-FP08	UCS Server (FI-Attached)
B200-M6-FP09	UCS Server (FI-Attached)

Step 3. Click **Next**.

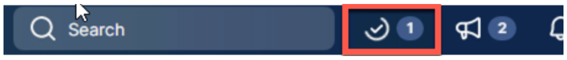
Note: Cisco Intersight will fill the default information for the number of servers selected.

Step 4. Adjust the Prefix and number if needed.

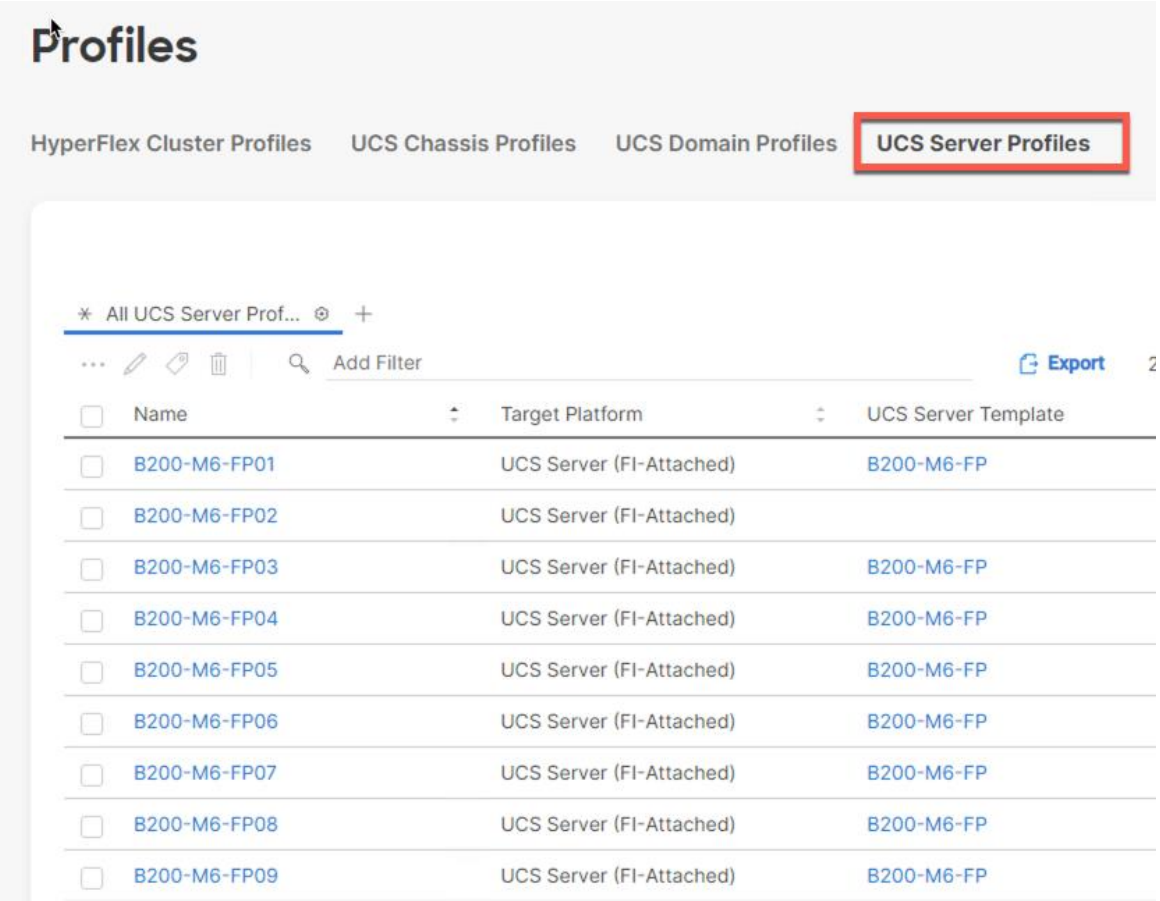
Step 5. Click **Next.**

Step 6. Verify the information and click **Derive** to create the Server Profiles.

Step 7. Cisco Intersight will start configuring the server profiles and will take some time to apply all the policies. Use the Requests tab to see the progress.



Step 8. When the Server Profiles are deployed successfully, they will appear under the Server Profiles with the status of OK.


Profiles

HyperFlex Cluster Profiles | UCS Chassis Profiles | UCS Domain Profiles | UCS Server Profiles

All UCS Server Prof... +

Add Filter | Export

□	Name	Target Platform	UCS Server Template
□	B200-M6-FP01	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP02	UCS Server (FI-Attached)	
□	B200-M6-FP03	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP04	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP05	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP06	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP07	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP08	UCS Server (FI-Attached)	B200-M6-FP
□	B200-M6-FP09	UCS Server (FI-Attached)	B200-M6-FP

FlexPod Cisco MDS Switch Configuration

This subject has the following procedures:

- Configure Cisco MDS 9132T A Switch
- Configure Cisco MDS 9132T B Switch
- Enable Features on Cisco MDS 9132T A and Cisco MDS 9132T B
- Configure the Second NTP Server and Add Local Time
- Configure Individual Ports for Cisco MDS 9132T A
- Configure Individual Ports for Cisco MDS 9132T B
- Create VSANs for Cisco MDS 9132T A

- Create VSANs for Cisco MDS 9132T B
- Create Device Aliases for Cisco MDS 9132T A
- Create Device Aliases for Cisco MDS 9132T B
- Create Zones and Zoneset for Cisco MDS 9132T A
- Create Zones and Zoneset for Cisco MDS 9132T B

Procedure 1. Configure Cisco MDS 9132T A Switch

Step 1. On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning. Enter y to get to the System Admin Account Setup.

Step 2. Configure the switch using the command line:

```
        ---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name : <mds-A-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address : <mds-A-mgmt0-ip>
Mgmt0 IPv4 netmask : <mds-A-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway : <mds-A-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Configure congestion/no_credit drop for fc interfaces? (yes/no)     [y]: Enter
Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]: Enter
Enter milliseconds in multiples of 10 for congestion-drop for logical-type edge
in range (<200-500>/default), where default is 500.  [d]: Enter
Enable the http-server? (yes/no) [y]: Enter
Configure clock? (yes/no) [n]: Enter
Configure timezone? (yes/no) [n]: Enter
Configure summertime? (yes/no) [n]: Enter
Configure the ntp server? (yes/no) [n]: yes
NTP server IPv4 address : <nexus-A-mgmt0-ip>
Configure default switchport interface state (shut/noshut) [shut]: Enter
Configure default switchport trunk mode (on/off/auto) [on]: auto
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: Enter
Enable full zoneset distribution? (yes/no) [n]: Enter
Configure default zone mode (basic/enhanced) [basic]: Enter
```

Step 3. Run the following commands to review the configuration:

```
Would you like to edit the configuration? (yes/no) [n]: Enter
Use this configuration and save it? (yes/no) [y]: Enter
```

Procedure 2. Configure Cisco MDS 9132T B Switch

Step 1. On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning. Enter y to get to the System Admin Account Setup.

Step 2. Configure the switch using the command line:

```
         ---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name : <mds-B-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address : <mds-B-mgmt0-ip>
Mgmt0 IPv4 netmask : <mds-B-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway : <mds-B-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Configure congestion/no_credit drop for fc interfaces? (yes/no)     [y]: Enter
Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]: Enter
Enter milliseconds in multiples of 10 for congestion-drop for logical-type edge
in range (<200-500>/default), where default is 500.  [d]: Enter
Enable the http-server? (yes/no) [y]: Enter
Configure clock? (yes/no) [n]: Enter
Configure timezone? (yes/no) [n]: Enter
Configure summertime? (yes/no) [n]: Enter
Configure the ntp server? (yes/no) [n]: yes
```

```
NTP server IPv4 address : <nexus-A-mgmt0-ip>
Configure default switchport interface state (shut/noshut) [shut]: Enter
Configure default switchport trunk mode (on/off/auto) [on]: auto
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: Enter
Enable full zoneset distribution? (yes/no) [n]: Enter
Configure default zone mode (basic/enhanced) [basic]: Enter
```

Step 3. Run the following commands to review the configuration:

```
Would you like to edit the configuration? (yes/no) [n]: Enter
Use this configuration and save it? (yes/no) [y]: Enter
```

Procedure 3. Enable Features on Cisco MDS 9132T A and Cisco MDS 9132T B

Step 1. Log in as admin.

Step 2. Run the following commands:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

Procedure 4. Configure the Second NTP Server and Add Local Time

Step 1. From the global configuration mode, run the following command:

```
ntp server <nexus-B-mgmt0-ip>
clock timezone <timezone> <hour-offset> <minute-offset>
clock summer-time <timezone> <start-week> <start-day> <start-month> <start-time> <end-week> <end-day> <end-month> <end-time> <offset-minutes>
```

Note: It is important to configure the local time so that logging time alignment, any backup schedules, and SAN Analytics forwarding are correct. For more information on configuring the timezone and daylight savings time or summer time, go to: Cisco MDS 9000 Series Fundamentals Configuration Guide, Release 8.x. Sample clock commands for the United States Eastern timezone are:
clock timezone EST -5 0
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60

Procedure 5. Configure Individual Ports for Cisco MDS 9132T A

Step 1. From the global configuration mode, run the following commands:

```
interface fc1/3
switchport description <st-clustername>-1:1a
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/4
switchport description <st-clustername>-2:1a
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/1
switchport description <ucs-clustername>-a:1/1
channel-group 15
no shutdown
exit

interface fc1/2
switchport description <ucs-clustername>-a:1/2
channel-group 15
no shutdown
exit

interface port-channel15
channel mode active
switchport trunk allowed vsan <vsan-a-id>
switchport description <ucs-clustername>-a
switchport speed 32000
no shutdown
exit
```

Note: If VSAN trunking is not being used between the Cisco UCS Fabric Interconnects and the MDS switches, do not enter "switchport trunk allowed vsan <vsan-a-id>" for interface port-channel15. The default setting of switchport trunk mode auto is being used for the port channel.

Procedure 6. Configure Individual Ports for Cisco MDS 9132T B

Step 1. From the global configuration mode, run the following commands:

```
interface fc1/5
switchport description <st-clustername>-1:1b
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/6
switchport description <st-clustername>-2:1b
switchport speed 32000
switchport trunk mode off
no shutdown
exit
```

```
interface fc1/1
switchport description <ucs-clustername>-b:1/1
channel-group 15
no shutdown
exit

interface fc1/2
switchport description <ucs-clustername>-b:1/2
channel-group 15
no shutdown
exit

interface port-channel15
channel mode active
switchport trunk allowed vsan <vsan-b-id>
switchport description <ucs-clustername>-b
switchport speed 32000
no shutdown
exit
```

Note: If VSAN trunking is not being used between the Cisco UCS Fabric Interconnects and the MDS switches, do not enter "switchport trunk allowed vsan <vsan-b-id>" for interface port-channel15. The default setting of switchport trunk mode auto is being used for the port channel.

Procedure 7. Create VSANs for Cisco MDS 9132T A

Step 1. From the global configuration mode, run the following commands:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/9
vsan <vsan-a-id> interface fc1/10
vsan <vsan-a-id> interface port-channel15
exit
```

Procedure 8. Create VSANs for Cisco MDS 9132T B

Step 1. From the global configuration mode, run the following commands:

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
```

```
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/9
vsan <vsan-b-id> interface fc1/10
vsan <vsan-b-id> interface port-channel15
exit
```

Step 2. At this point, it may be necessary to go into Cisco Intersight and disable and then enable the FC port-channel interfaces to get the port-channels to come up.

Procedure 9. Create Device Aliases for Cisco MDS 9132T A

Note: Device aliases for Fabric A will be used to create zones.

Step 1. From the global configuration mode, run the following commands:

```
device-alias mode enhanced
device-alias database
device-alias name Infra-SVM-fcp-lif-01a pwwn <fcp-lif-01a-wwpn>
device-alias name Infra-SVM-fcp-lif-02a pwwn <fcp-lif-02a-wwpn>
device-alias name VM-Host-Infra-01-A pwwn <vm-host-infra-01-wwpna>
device-alias name VM-Host-Infra-02-A pwwn <vm-host-infra-02-wwpna>
device-alias name VM-Host-Infra-03-A pwwn <vm-host-infra-03-wwpna>
device-alias commit
```

Procedure 10. Create Device Aliases for Cisco MDS 9132T B

Step 1. From the global configuration mode, run the following commands:

```
device-alias mode enhanced
device-alias database
device-alias name Infra-SVM-fcp-lif-01b pwwn <fcp-lif-01b-wwpn>
device-alias name Infra-SVM-fcp-lif-02b pwwn <fcp-lif-02b-wwpn>
device-alias name VM-Host-Infra-01-B pwwn <vm-host-infra-01-wwpnb>
device-alias name VM-Host-Infra-02-B pwwn <vm-host-infra-02-wwpnb>
device-alias name VM-Host-Infra-03-B pwwn <vm-host-infra-03-wwpnb>
device-alias commit
```

Procedure 11. Create Zones and Zoneset for Cisco MDS 9132T A

Step 1. To create the required zones and zoneset on Fabric A, run the following commands:

```
configure terminal
zone name Infra-SVM-Fabric-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias VM-Host-Infra-02-A init
member device-alias VM-Host-Infra-03-A init
member device-alias Infra-SVM-fcp-lif-01a target
member device-alias Infra-SVM-fcp-lif-02a target
```

```
exit
zoneset name Fabric-A vsan <vsan-a-id>
member Infra-SVM-Fabric-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
show zoneset active
copy r s
```

Note: Since Smart Zoning is enabled, a single zone is created with all host boot initiators and boot targets for the Infra-SVM instead of creating a separate zone for each host with the host initiator and boot targets. If a new host is added, its boot initiator can simply be added to the single zone in each MDS switch and then the zoneset reactivated. If another SVM is added to the FlexPod with FC targets, a new zone can be added for that SVM.

Procedure 12. Create Zones and Zoneset for Cisco MDS 9132T B

Step 1. To create the required zones and zoneset on Fabric B, run the following commands:

```
configure terminal
zone name Infra-SVM-Fabric-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias VM-Host-Infra-02-B init
member device-alias VM-Host-Infra-03-B init
member device-alias Infra-SVM-fcp-lif-01b target
member device-alias Infra-SVM-fcp-lif-02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member Infra-SVM-Fabric-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active
copy r s
```

Storage Configuration – Boot LUNs

This chapter contains the following:

- ONTAP Boot Storage Setup
- Install VMware ESXi 7.0
- VMware vCenter 7.0

ONTAP Boot Storage Setup

This subject contains the following procedures:

- Create Boot LUNs
- Create igroups
- Map Boot LUNs to igroups

Procedure 1. Create Boot LUNs

Step 1. Run the following commands to create three boot LUNs:

```
lun create -vserver Infra-SVM -path /vol/esxi_boot/VM-Host-Infra-01 -size 32GB -ostype
vmware -space-reserve disabled

lun create -vserver Infra-SVM -path /vol/esxi_boot/VM-Host-Infra-02 -size 32GB -ostype
vmware -space-reserve disabled

lun create -vserver Infra-SVM -path /vol/esxi_boot/VM-Host-Infra-03 -size 32GB -ostype
vmware -space-reserve disabled
```

Procedure 2. Create igroups

Step 1. Create initiator groups (igroups) by entering the following commands from the storage cluster management node Secure Shell (SSH) connection:

```
lun igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol fcp –ostype
vmware –initiator <vm-host-infra-01-wwpna>, <vm-host-infra-01-wwpnb>


lun igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol fcp –ostype
vmware –initiator <vm-host-infra-02-wwpna>, <vm-host-infra-02-wwpnb>

lun igroup create –vserver Infra-SVM –igroup VM-Host-Infra-03 –protocol fcp –ostype
vmware –initiator <vm-host-infra-03-wwpna>, <vm-host-infra-03-wwpnb>


lun igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol fcp –ostype vmware –
initiator <vm-host-infra-01-wwpna>, <vm-host-infra-01-wwpnb>, <vm-host-infra-02-wwpna>,
<vm-host-infra-02-wwpnb>, <vm-host-infra-03-wwpna>, <vm-host-infra-03-wwpnb>
```

Step 2. To view the three igroups just created, use the command lun igroup show:

```
lun igroup show -protocol fcp
```

Procedure 3. Map Boot LUNs to igroups

Step 1. From the storage cluster management SSH connection, enter the following commands:

```
lun mapping create -vserver Infra-SVM -path /vol/esxi_boot/VM-Host-Infra-01 -igroup VM-Host-Infra-01 -lun-id 0

lun mapping create -vserver Infra-SVM -path /vol/esxi_boot/VM-Host-Infra-02 -igroup VM-Host-Infra-02 -lun-id 0

lun mapping create -vserver Infra-SVM -path /vol/esxi_boot/VM-Host-Infra-03 -igroup VM-Host-Infra-03 -lun-id 0
```

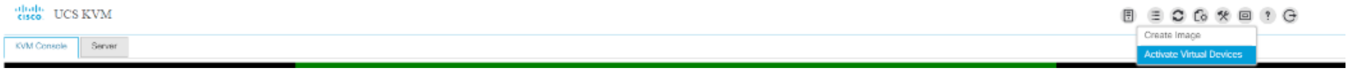
Step 2. Download the Cisco Custom Image for VMware ESXi 7.0 Update 2a, from the VMware vSphere Hypervisor 7.0 U3 page click the “Custom ISOs” tab.

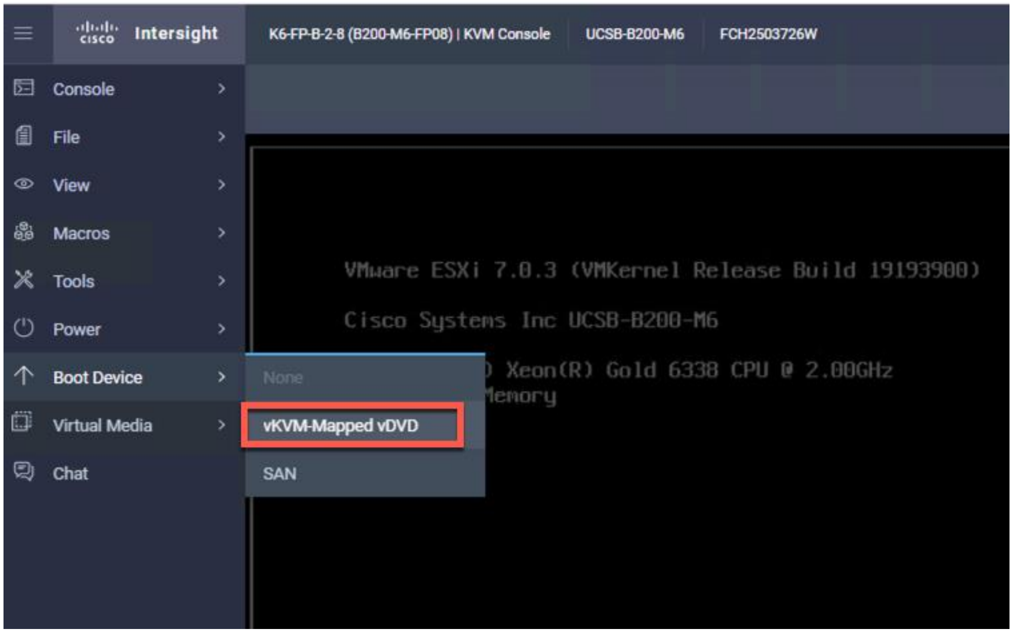
Step 3. In the Cisco Intersight navigation pane, click the Equipment tab.

Step 4. Under Servers > Service Profiles> VDI-Host1

Step 5. Right-click on VDI-Host1 and select KVM Console.

Step 6. Click Boot Device and then select CD/DVD.



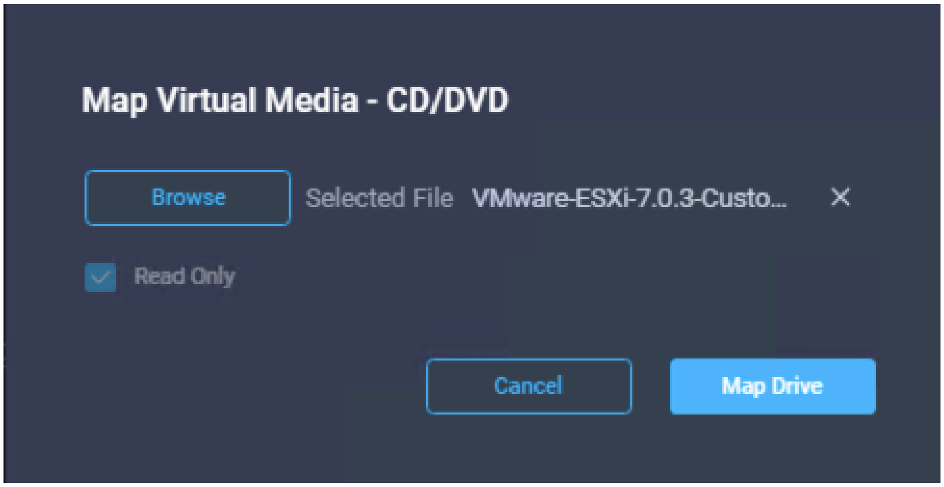


```
VMware ESXi 7.0.3 (VMKernel Release Build 19193900)

Cisco Systems Inc UCSB-B200-M6

) Xeon(R) Gold 6338 CPU @ 2.00GHz
Memory
```

Step 7. Click Virtual Media and Mount the ESXi ISO image.

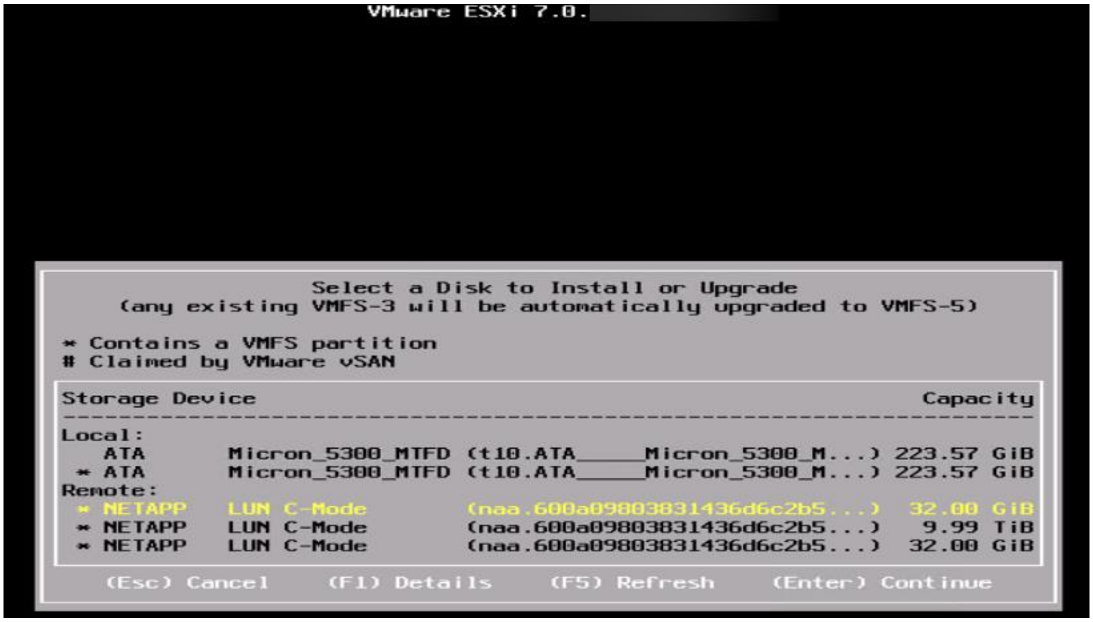


Selected File VMware-ESXi-7.0.3-Custo...

☑ Read Only

Step 8. Boot into ESXi installer and follow the prompts to complete installing VMware vSphere ESXi hypervisor.

Step 9. When selecting a storage device to install ESXi, select Remote LUN provisioned through NetApp Storage Administrative console and access through FC connection.



```
VMware ESXi 7.0.[redacted]

                    Select a Disk to Install or Upgrade
      (any existing VMFS-3 will be automatically upgraded to VMFS-5)

 * Contains a VMFS partition
 # Claimed by VMware vSAN

 Storage Device                                                  Capacity
 -------------------------------------------------------------------------
 Local:
    ATA       Micron_5300_MTFD (t10.ATA_____Micron_5300_M...) 223.57 GiB
  * ATA       Micron_5300_MTFD (t10.ATA_____Micron_5300_M...) 223.57 GiB
 Remote:
  * NETAPP    LUN C-Mode       (naa.600a09803831436d6c2b5...)  32.00 GiB
  * NETAPP    LUN C-Mode       (naa.600a09803831436d6c2b5...)   9.99 TiB
  * NETAPP    LUN C-Mode       (naa.600a09803831436d6c2b5...)  32.00 GiB

     (Esc) Cancel      (F1) Details      (F5) Refresh      (Enter) Continue
```

Note: Adding a management network for each VMware host is necessary for managing the host and connection to vCenter Server. Please select the IP address that can communicate with an existing or a new vCenter Server.

Step 10. After the server has finished rebooting, press F2 to enter into configuration wizard for ESXi Hypervisor.

Step 11. Log in as root and enter the corresponding password.

Step 12. Select the Configure the Management Network option and press Enter.

Step 13. Select the VLAN (Optional) option and press Enter. Enter the VLAN In-Band management ID and press Enter.

Step 14. From the Configure Management Network menu, select "IP Configuration" and press Enter.

Step 15. Select "Set Static IP Address and Network Configuration" option by using the space bar. Enter the IP address to manage the first ESXi host. Enter the subnet mask for the first ESXi host. Enter the default gateway for the first ESXi host. Press Enter to accept the changes to the IP configuration.

Step 16. IPv6 Configuration is set to automatic.

Step 17. Select the DNS Configuration option and press Enter.

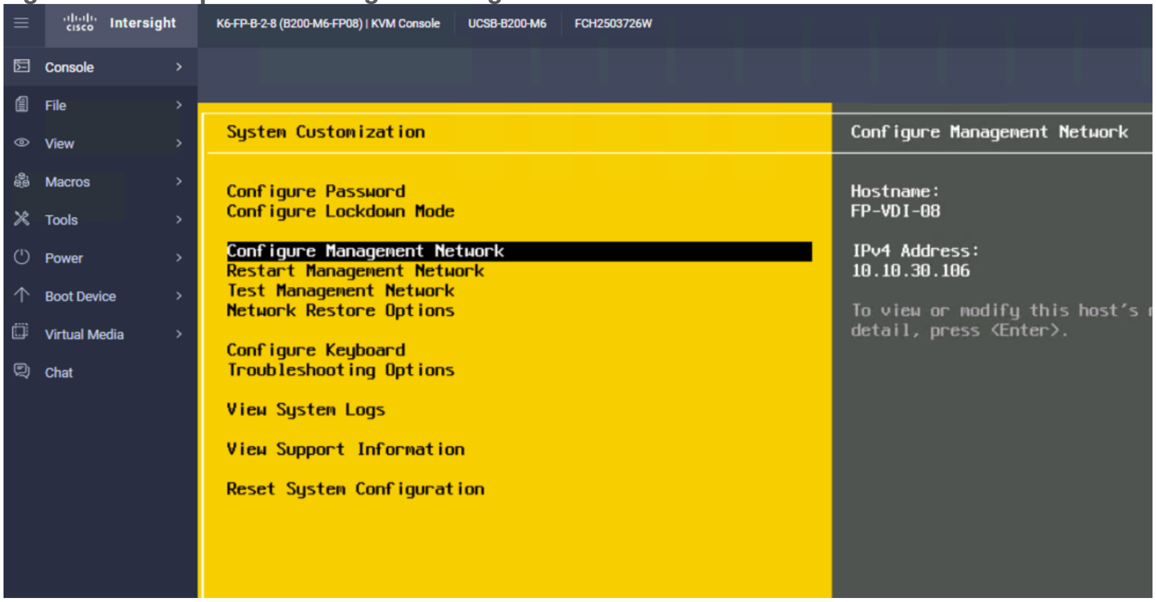
Step 18. Enter the IP address of the primary and secondary DNS server. Enter Hostname

Step 19. Enter DNS Suffixes.

Step 20. Since the IP address is assigned manually, the DNS information must also be entered manually.

Note: The steps provided vary based on the configuration. Please make the necessary changes according to your configuration.

Figure 33. Sample ESXi Configure Management Network



```
System Customization                              Configure Management Network

Configure Password                                Hostname:
Configure Lockdown Mode                           FP-VDI-08

Configure Management Network                      IPv4 Address:
Restart Management Network                        10.10.30.106
Test Management Network
Network Restore Options                           To view or modify this host's
                                                  detail, press <Enter>.
Configure Keyboard
Troubleshooting Options

View System Logs

View Support Information

Reset System Configuration
```

Install VMware ESXi 7.0

This subject contains the following procedures:

- Download ESXi 7.0 from VMware
- Log into the Cisco UCS Environment using Cisco Intersight
- Prepare the Server for the OS Installation
- Install VMware ESXi to the Bootable LUN of the Hosts
- Set Up Management Networking for ESXi Hosts
- Reset VMware ESXi Host VMkernel Port vmk0 MAC Address (Optional)
- Install VMware and Cisco VIC Drivers for the ESXi Host
- Install VMware VIC Drivers and the NetApp NFS Plug-in for VMware VAAI on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02
- Log into the First VMware ESXi Host by Using VMware Host Client
- Set Up VMkernel Ports and Virtual Switch for ESXi Host VM-Host-Infra-01
- Mount Required Datastores on ESXi Host VM-Host-Infra-01
- Configure NTP on First ESXi Host on ESXi Host VM-Host-Infra-01

- Configure ESXi Host Swap on ESXi Host VM-Host-Infra-01
- Configure Host Power Policy on ESXi Host VM-Host-Infra-01

This section provides detailed instructions for installing VMware ESXi 7.0 in a FlexPod environment. After the procedures are completed, three booted ESXi hosts will be provisioned.

Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in keyboard, video, mouse (KVM) console and virtual media features in Cisco Intersight to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs).

Procedure 1. Download ESXi 7.0 from VMware

Step 1. Click the following link: Cisco Custom ISO for UCS 4.2.2a. You will need a user id and password on vmware.com to download this software, https://customerconnect.vmware.com/downloads/details?downloadGroup=OEM-ESXI70U3-CISCO&productId=974

Note: The Cisco Custom ISO for UCS 4.2.2a should also be used for Cisco UCS software release 5.0(1b) and VMware vSphere 7.0.

Step 2. Download the .iso file.

Procedure 2. Log into the Cisco UCS Environment using Cisco Intersight

The Cisco UCS IP KVM enables the administrator to begin the installation of the operating system (OS) through remote media. It is necessary to log into the Cisco UCS environment to run the IP KVM.

Step 1. Open a web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco Intersight application.

Step 2. Click the Launch Intersight link to launch the HTML 5 Intersight GUI.

Step 3. If prompted to accept security certificates, accept, as necessary.

Step 4. When prompted, enter admin for the user name and enter the administrative password.

Step 5. To log into Cisco Intersight, click Login.

Step 6. From the main menu, click Servers.

Step 7. Click Servers > Service Profiles > root > Sub-Organizations > FlexPod Organization > VM-Host-Infra-01.

Step 8. In the Actions pane, click KVM Console.

Step 9. Follow the prompts to launch the HTML5 KVM console.

Step 10. Click Servers > Service Profiles > root > Sub-Organizations > FlexPod Organization > VM-Host-Infra-02.

Step 11. In the Actions pane, click KVM Console.

Step 12. Follow the prompts to launch the HTML5 KVM console.

Step 13. Go to Servers > Service Profiles > root > Sub-Organizations > FlexPod Organization > VM-Host-Infra-03.

Step 14. In the Actions pane, click KVM Console.

Step 15. Follow the prompts to launch the HTML5 KVM console.

Procedure 3. Prepare the Server for the OS Installation

Note: Skip this section if you're using vMedia policies; the ISO file will already be connected to KVM.

Step 1. In the KVM window, click Virtual Media.

Step 2. Select Activate Virtual Devices.

Step 3. If prompted to accept an Unencrypted KVM session, accept, as necessary.

Step 4. Click Virtual Media and select Map CD/DVD.

Step 5. Browse to the ESXi installer ISO image file and click Open.

Step 6. Click Map Device.

Step 7. Click the KVM Console tab to monitor the server boot.

Procedure 4. Install VMware ESXi to the Bootable LUN of the Hosts

Step 1. Boot the server by selecting Boot Server in the KVM and click OK, then click OK again.

Step 2. On boot, the machine detects the presence of the ESXi installation media and loads the ESXi installer.

Step 3. If the ESXi installer fails to load because the software certificates cannot be validated, reset the server, and when prompted, press F2 to go into BIOS and set the system time and date to current. Now the ESXi installer should load properly.

Step 4. After the installer is finished loading, press Enter to continue with the installation.

Step 5. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.

Step 6. It may be necessary to map function keys as User Defined Macros under the Macros menu in the Cisco UCS KVM console.

Step 7. Select the LUN that was previously set up for the installation disk for ESXi and press Enter to continue with the installation.

Step 8. Select the appropriate keyboard layout and press Enter.

Step 9. Enter and confirm the root password and press Enter.

Step 10. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.

Step 11. After the installation is complete, press Enter to reboot the server.

Step 12. The ESXi installation image will be automatically unmapped in the KVM when Enter is pressed.

Step 13. In Cisco Intersight, bind the current service profile to the non-vMedia service profile template to prevent mounting the ESXi installation iso over HTTP.

Procedure 5. Set Up Management Networking for ESXi Hosts

Note: Adding a management network for each VMware host is necessary for managing the host.

Step 1. After the server has finished rebooting, in the UCS KVM console, press F2 to customize VMware ESXi.

Step 2. Log in as root, enter the corresponding password, and press Enter to log in.

Step 3. Use the down arrow key to select Troubleshooting Options and press Enter.

Step 4. Select Enable ESXi Shell and press Enter.

Step 5. Select Enable SSH and press Enter.

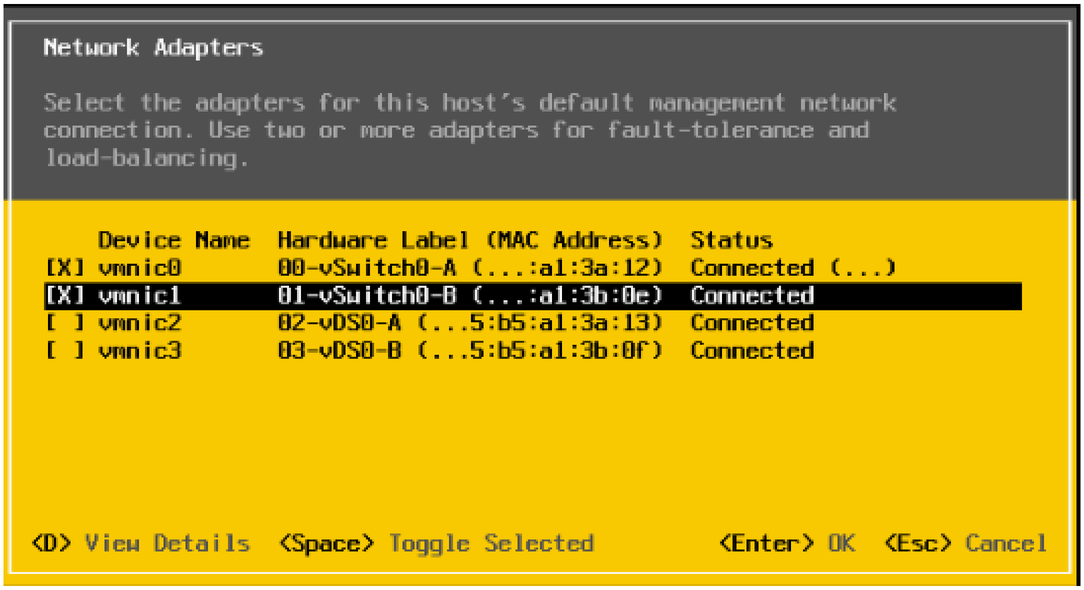
Step 6. Press Esc to exit the Troubleshooting Options menu.

Step 7. Select the Configure Management Network option and press Enter.

Step 8. Select Network Adapters and press Enter.

Step 9. Verify that the numbers in the Hardware Label field match the numbers in the Device Name field. If the numbers do not match, note the mapping of vmnic ports to vNIC ports for later use.

Step 10. Using the spacebar, select vmnic1.



```
Network Adapters

Select the adapters for this host's default management network
connection. Use two or more adapters for fault-tolerance and
load-balancing.

    Device Name   Hardware Label (MAC Address)  Status
[X] vmnic0        00-vSwitch0-A (...:a1:3a:12)  Connected (...)
[X] vmnic1        01-vSwitch0-B (...:a1:3b:0e)  Connected
[ ] vmnic2        02-vDS0-A (...5:b5:a1:3a:13)  Connected
[ ] vmnic3        03-vDS0-B (...5:b5:a1:3b:0f)  Connected

<D> View Details  <Space> Toggle Selected       <Enter> OK  <Esc> Cancel
```

Note: In lab testing, examples were seen where the vmnic and device ordering do not match. In this case, use the Consistent Device Naming (CDN) to note which vmnics are mapped to which vNICs and adjust the upcoming procedure accordingly.

Step 11. Press Enter.

Step 12. Select the VLAN (Optional) option and press Enter.

Step 13. Enter the <ib-mgmt-vlan-id> and press Enter.

Step 14. Select IPv4 Configuration and press Enter.

Step 15. Select the "Set static IPv4 address and network configuration" option by using the arrow keys and space bar.

Step 16. Move to the IPv4 Address field and enter the IP address for managing the ESXi host.

Step 17. Move to the Subnet Mask field and enter the subnet mask for the ESXi host.

Step 18. Move to the Default Gateway field and enter the default gateway for the ESXi host.

Step 19. Press Enter to accept the changes to the IP configuration.

Step 20. Select the IPv6 Configuration option and press Enter.

Step 21. Using the spacebar, select Disable IPv6 (restart required) and press Enter.

Step 22. Select the DNS Configuration option and press Enter.

Note: Since the IP address is assigned manually, the DNS information must also be entered manually.

Step 23. Using the spacebar, select "Use the following DNS server addresses and hostname:"

Step 24. Move to the Primary DNS Server field and enter the IP address of the primary DNS server.

Step 25. Optional: Move to the Alternate DNS Server field and enter the IP address of the secondary DNS server.

Step 26. Move to the Hostname field and enter the fully qualified domain name (FQDN) for the ESXi host.

Step 27. Press Enter to accept the changes to the DNS configuration.

Step 28. Press Esc to exit the Configure Management Network submenu.

Step 29. Press Y to confirm the changes and reboot the ESXi host.

Procedure 6. Reset VMware ESXi Host VMkernel Port vmk0 MAC Address (Optional)

Note: By default, the MAC address of the management VMkernel port vmk0 is the same for the MAC address of the Ethernet port it is placed on. If the ESXi host's boot LUN is remapped to a different server with different MAC addresses, a MAC address conflict will exist because vmk0 will retain the assigned MAC address unless the ESXi System Configuration is reset.

Step 1. From the ESXi console menu main screen, type Ctrl-Alt-F1 to access the VMware console command line interface. In the UCSM KVM, Ctrl-Alt-F1 appears in the list of Static Macros.

Step 2. Log in as root.

Step 3. Type esxcfg-vmknic –l to get a detailed listing of interface vmk0. vmk0 should be a part of the "Management Network" port group. Note the IP address and netmask of vmk0.

Step 4. To remove vmk0, type esxcfg-vmknic –d "Management Network".

Step 5. To add vmk0 with a random MAC address, type esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> "Management Network."

Step 6. Verify vmk0 has been re-added with a random MAC address by typing esxcfg-vmknic –l.

Step 7. Tag vmk0 for the management interface by typing esxcli network ip interface tag add -i vmk0 -t Management.

Step 8. When vmk0 was added, if a message popped up saying vmk1 was marked for the management interface, type esxcli network ip interface tag remove -i vmk1 -t Management.

Step 9. If this VMware ESXi host is iSCSI booted, the vmk1, iScsiBootPG-A interface's MAC address can also be reset to a random, VMware-assigned MAC address.

Step 10. Type esxcfg-vmknic –l to get a detailed listing of interface vmk1. vmk1 should be a part of the "iScsiBootPG-A" port group and should have a MAC address from the UCS MAC Pool. Note the IP address and netmask of vmk1.

Step 11. To remove vmk1, type esxcfg-vmknic –d "iScsiBootPG-A".

Step 12. To re-add vmk1 with a random MAC address, type esxcfg-vmknic –a –i <vmk1-ip> -n <vmk1-netmask> -m 9000 "iScsiBootPG-A".

Step 13. Verify vmk1 has been re-added with a random MAC address by typing esxcfg-vmknic –l.

Step 14. Type exit to log out of the command line interface.

Step 15. Type Ctrl-Alt-F2 to return to the ESXi console menu interface.

Procedure 7. Install VMware and Cisco VIC Drivers for the ESXi Host

Step 1. Download the offline bundle for the Cisco UCS Tools Component and the NetApp NFS Plug-in for VMware VAAI to the Management workstation: Cisco UCS Tools Component for ESXi 7.0 1.1.5 (ucs-tool-esxi_1.1.5-1OEM.zip) (NetAppNasPluginV2.0.zip)

Note: This document describes using the driver versions shown above along with Cisco VIC nenic version 1.0.33.0 and nfnic version 4.0.0.56 along with VMware vSphere version 7.0.U3, Cisco UCS version 4.2(2a), and the latest patch NetApp ONTAP 9.10.1P1. These were the versions validated and supported at the time this document was published. This document can be used as a guide for configuring future versions of software. Consult the [Cisco UCS Hardware Compatibility List]() and the [NetApp Interoperability Matrix Tool]() to determine supported combinations of firmware and software.

Procedure 8. Install VMware VIC Drivers and the NetApp NFS Plug-in for VMware VAAI on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02

Step 1. Using an SCP program such as WinSCP, copy the two offline bundles referenced above to the /tmp directory on each ESXi host.

Step 2. Using a ssh tool such as PuTTY, ssh to each VMware ESXi host. Log in as root with the root password.

Step 3. Type cd /tmp.

Step 4. Run the following commands on each host:

```
esxcli software component apply -d /tmp/ucs-tool-esxi_1.1.5-1OEM.zip

esxcli software vib install -d /tmp/NetAppNasPlugin.v23.zip

reboot
```

Step 5. After reboot, log back into each host and run the following commands and ensure the correct version is installed:

```
esxcli software component list | grep ucs

esxcli software vib list | grep NetApp
```

Procedure 9. Log into the First VMware ESXi Host by Using VMware Host Client

Step 1. Open a web browser on the management workstation and navigate to the VM-Host-Infra-01 management IP address.

Step 2. Enter root for the User name.

Step 3. Enter the root password.

Step 4. Click Login to connect.

Step 5. Decide whether to join the VMware Customer Experience Improvement Program and click OK.

Procedure 10. Set Up VMkernel Ports and Virtual Switch for ESXi Host VM-Host-Infra-01

Note: In this procedure, you're only setting up the first ESXi host. The second and third hosts will be added to vCenter and setup from the vCenter HTML5 Interface.

Step 1. From the Host Client Navigator, click Networking.

Step 2. In the center pane, click the Virtual switches tab.

Step 3. Highlight the vSwitch0 line.

Step 4. Click Edit settings.

Step 5. Change the MTU to 9000.

Step 6. Expand NIC teaming.

Step 7. In the Failover order section, click vmnic1 and click Mark active.

Step 8. Verify that vmnic1 now has a status of Active.

Step 9. Click Save.

Step 10. Click Networking, then click the Port groups tab.

Step 11. In the center pane, right-click VM Network and click Edit settings.

Step 12. Name the port group IB-MGMT Network and enter <ib-mgmt-vlan-id> in the VLAN ID field.

Step 13. Click Save to finalize the edits for the IB-MGMT Network.

Step 14. At the top, click the VMkernel NICs tab.

Step 15. Click Add VMkernel NIC.

Step 16. For New port group, enter VMkernel-Infra-NFS.

Step 17. For Virtual switch, click vSwitch0.

Step 18. Enter <infra-nfs-vlan-id> for the VLAN ID.

Step 19. Change the MTU to 9000.

Step 20. Click Static IPv4 settings and expand IPv4 settings.

Step 21. Enter the ESXi host Infrastructure NFS IP address and netmask.

Step 22. Leave TCP/IP stack set at Default TCP/IP stack and do not choose any of the Services.

Step 23. Click Create.

Step 24. Click Add VMkernel NIC.

Step 25. For New port group, enter VMkernel-vMotion.

Step 26. For Virtual switch, click vSwitch0.

Step 27. Enter <vmotion-vlan-id> for the VLAN ID.

Step 28. Change the MTU to 9000.

Step 29. Click Static IPv4 settings and expand IPv4 settings.

Step 30. Enter the ESXi host vMotion IP address and netmask.

Step 31. Click the vMotion stack for TCP/IP stack.

Step 32. Click Create.

Step 33. Optionally, create two more vMotion VMkernel NICs to increase the speed of multiple simultaneous vMotion on this solution’s 40 and 50GE vNICs:

a. Click Add VMkernel NIC.

b. For New port group, enter VMkernel-vMotion1.

c. For Virtual switch, click vSwitch0.

d. Enter <vmotion-vlan-id> for the VLAN ID.

e. Change the MTU to 9000.

f. Click Static IPv4 settings and expand IPv4 settings.

g. Enter the ESXi host’s second vMotion IP address and netmask.

h. Click the vMotion stack for TCP/IP stack.

i. Click Create.

j. Click Add VMkernel NIC.

k. For New port group, enter VMkernel-vMotion2.

l. For Virtual switch, click vSwitch0.

m. Enter <vmotion-vlan-id> for the VLAN ID.

n. Change the MTU to 9000.

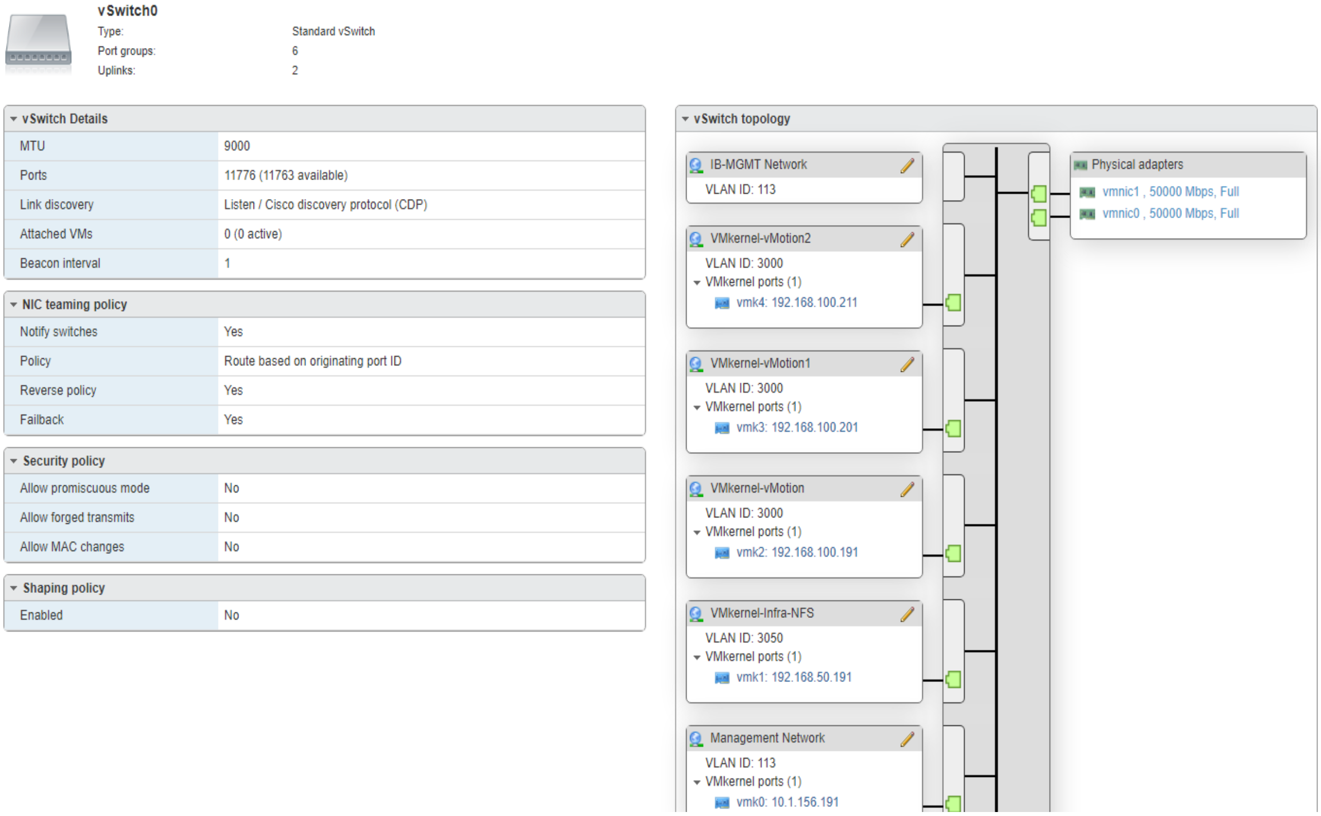
o. Click Static IPv4 settings and expand IPv4 settings.

p. Enter the ESXi host’s third vMotion IP address and netmask.

q. Click the vMotion stack for TCP/IP stack.

r. Click Create.

Step 34. Click the Virtual Switches tab, then vSwitch0. The properties for vSwitch0 VMkernel NICs should be similar to the following example:



vSwitch0

Type:	Standard vSwitch
Port groups:	6
Uplinks:	2

vSwitch Details	
MTU	9000
Ports	11776 (11763 available)
Link discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	0 (0 active)
Beacon interval	1

NIC teaming policy	
Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes
Failback	Yes

Security policy	
Allow promiscuous mode	No
Allow forged transmits	No
Allow MAC changes	No

Shaping policy	
Enabled	No

vSwitch topology

IB-MGMT Network
VLAN ID: 113

VMkernel-vMotion2
VLAN ID: 3000
VMkernel ports (1)
vmk4: 192.168.100.211

VMkernel-vMotion1
VLAN ID: 3000
VMkernel ports (1)
vmk3: 192.168.100.201

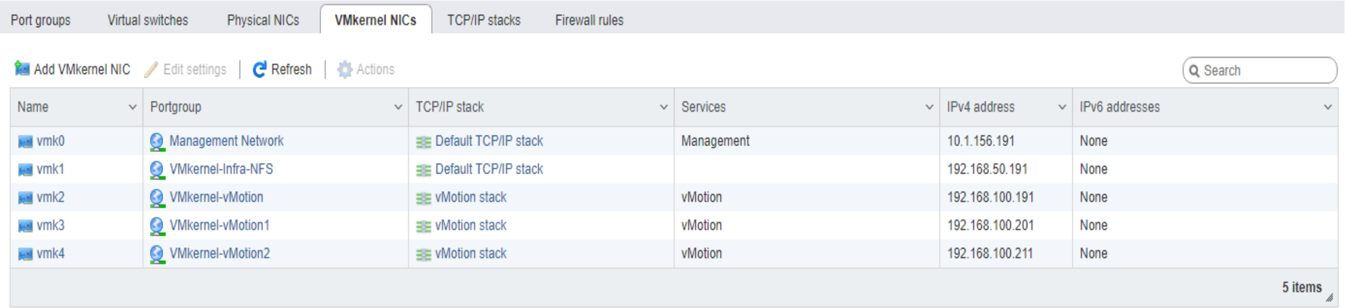
VMkernel-vMotion
VLAN ID: 3000
VMkernel ports (1)
vmk2: 192.168.100.191

VMkernel-Infra-NFS
VLAN ID: 3050
VMkernel ports (1)
vmk1: 192.168.50.191

Management Network
VLAN ID: 113
VMkernel ports (1)
vmk0: 10.1.156.191

Physical adapters
vmnic1 , 50000 Mbps, Full
vmnic0 , 50000 Mbps, Full

Step 35. Click Networking and the VMkernel NICs tab to confirm configured virtual adapters. The adapters listed should be similar to the following example:



Name	Portgroup	TCP/IP stack	Services	IPv4 address	IPv6 addresses
vmk0	Management Network	Default TCP/IP stack	Management	10.1.156.191	None
vmk1	VMkernel-Infra-NFS	Default TCP/IP stack		192.168.50.191	None
vmk2	VMkernel-vMotion	vMotion stack	vMotion	192.168.100.191	None
vmk3	VMkernel-vMotion1	vMotion stack	vMotion	192.168.100.201	None
vmk4	VMkernel-vMotion2	vMotion stack	vMotion	192.168.100.211	None

5 items

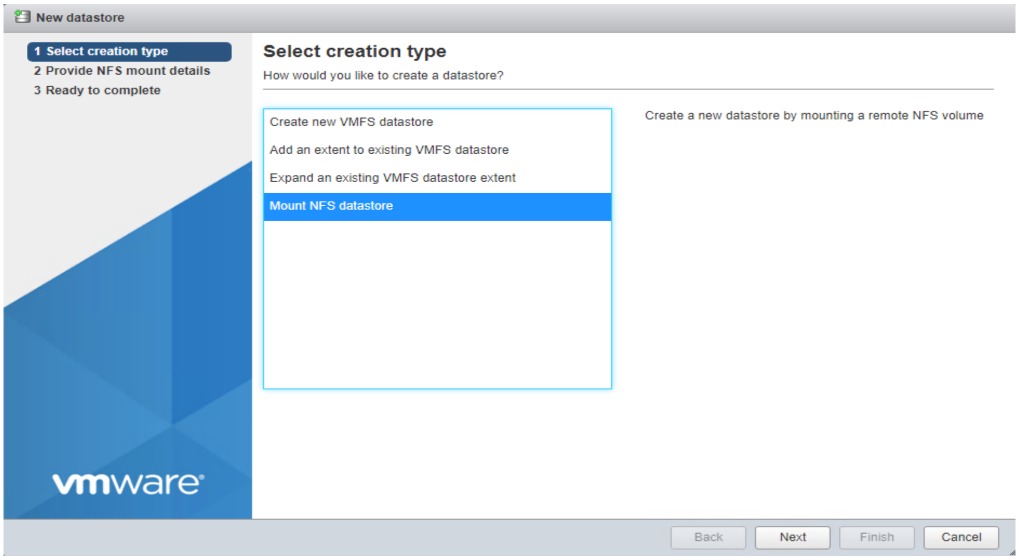
Procedure 11. Mount Required Datastores on ESXi Host VM-Host-Infra-01

Step 1. From the Host Client, click Storage.

Step 2. In the center pane, click the Datastores tab.

Step 3. In the center pane, click New Datastore to add a new datastore.

Step 4. In the New datastore popup, click Mount NFS datastore and click Next.



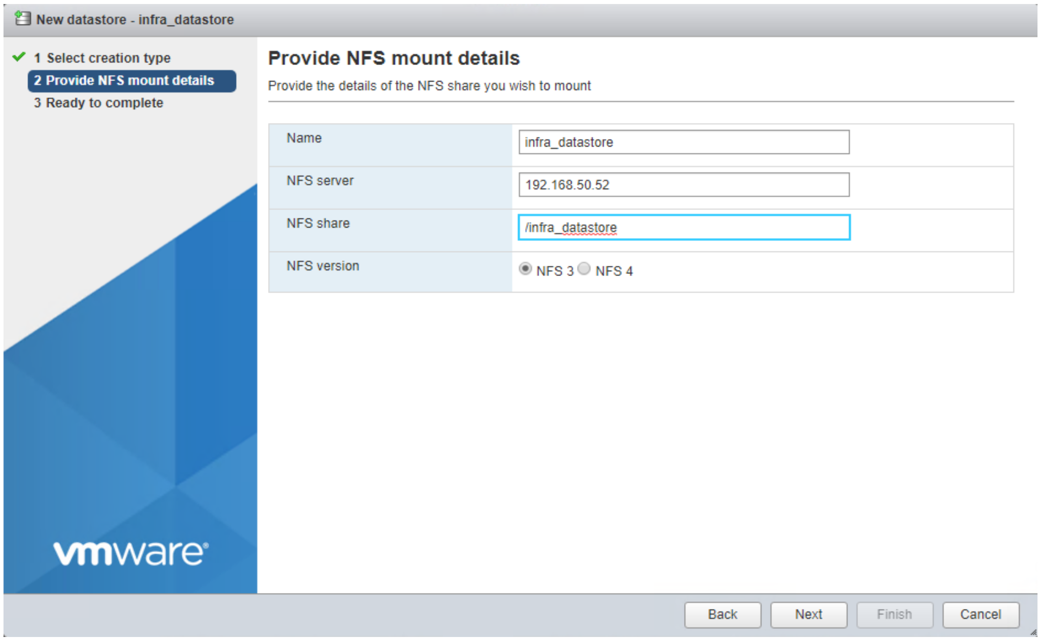
Select creation type

How would you like to create a datastore?

- Create new VMFS datastore
- Add an extent to existing VMFS datastore
- Expand an existing VMFS datastore extent
- Mount NFS datastore

Create a new datastore by mounting a remote NFS volume

Step 5. Input infra_datastore for the datastore name. Input the IP address for the nfs-lif-02 LIF for the NFS server. Input /infra_datastore for the NFS share. Leave the NFS version set at NFS 3. Click Next.



Provide NFS mount details

Provide the details of the NFS share you wish to mount

Name	infra_datastore
NFS server	192.168.50.52
NFS share	/infra_datastore
NFS version	● NFS 3 ○ NFS 4

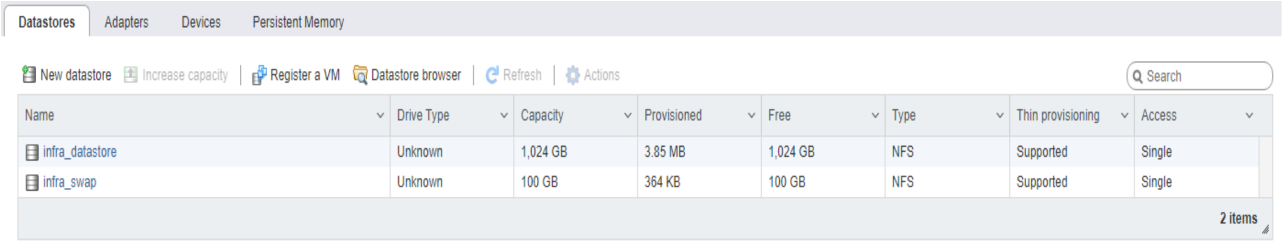
Step 6. Click Finish. The datastore should now appear in the datastore list.

Step 7. In the center pane, click New Datastore to add a new datastore.

Step 8. In the New datastore popup, click Mount NFS datastore and click Next.

Step 9. Input infra_swap for the datastore name. Input the IP address for the nfs-lif-01 LIF for the NFS server. Input /infra_swap for the NFS share. Leave the NFS version set at NFS 3. Click Next.

Step 10. Click Finish. The datastore should now appear in the datastore list.



Datastores | Adapters | Devices | Persistent Memory

New datastore | Increase capacity | Register a VM | Datastore browser | Refresh | Actions | Search

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provisioning	Access
infra_datastore	Unknown	1,024 GB	3.85 MB	1,024 GB	NFS	Supported	Single
infra_swap	Unknown	100 GB	364 KB	100 GB	NFS	Supported	Single

2 items

Procedure 12. Configure NTP on First ESXi Host on ESXi Host VM-Host-Infra-01

Step 1. From the Host Client, click Manage.

Step 2. In the center pane, click System > Time and date.

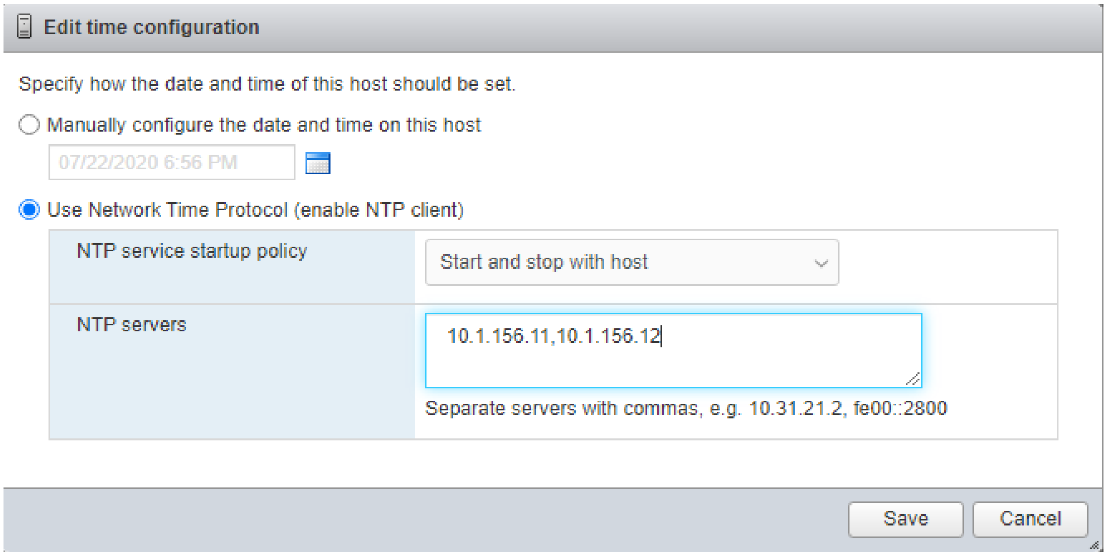
Step 3. Click Edit NTP settings.

Step 4. Make sure “Manually configure the date and time on this host and enter the approximate date and time.

Step 5. Select Use Network Time Protocol (enable NTP client).

Step 6. Use the drop-down list to click Start and stop with host.

Step 7. Enter the two Nexus switch NTP addresses in the NTP servers box separated by a comma.



Edit time configuration

Specify how the date and time of this host should be set.

○ Manually configure the date and time on this host

07/22/2020 6:56 PM

● Use Network Time Protocol (enable NTP client)

NTP service startup policy	Start and stop with host
NTP servers	10.1.156.11,10.1.156.12 Separate servers with commas, e.g. 10.31.21.2, fe00::2800

Save | Cancel

Step 8. Click Save to save the configuration changes.

Note: Currently, it isn’t possible to start NTP from the ESXi Host Client. NTP will be started from vCenter. The NTP server time may vary slightly from the host time.

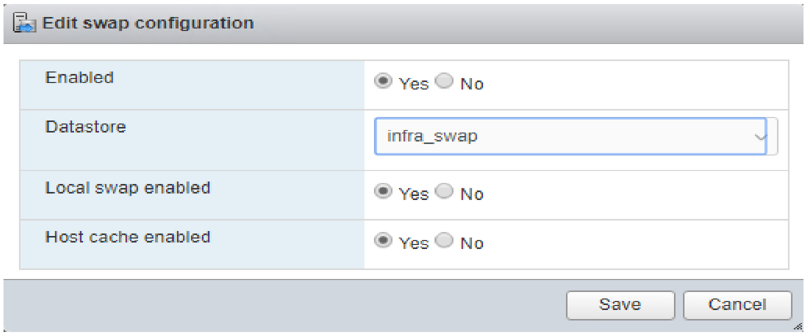
Procedure 13. Configure ESXi Host Swap on ESXi Host VM-Host-Infra-01

Step 1. From the Host Client, click Manage.

Step 2. In the center pane, click System > Swap.

Step 3. Click Edit settings.

Step 4. Use the drop-down list to click infra_swap. Leave all other settings unchanged.



Edit swap configuration

Enabled	● Yes ○ No
Datastore	infra_swap
Local swap enabled	● Yes ○ No
Host cache enabled	● Yes ○ No

Step 5. Click Save to save the configuration changes.

Procedure 14. Configure Host Power Policy on ESXi Host VM-Host-Infra-01

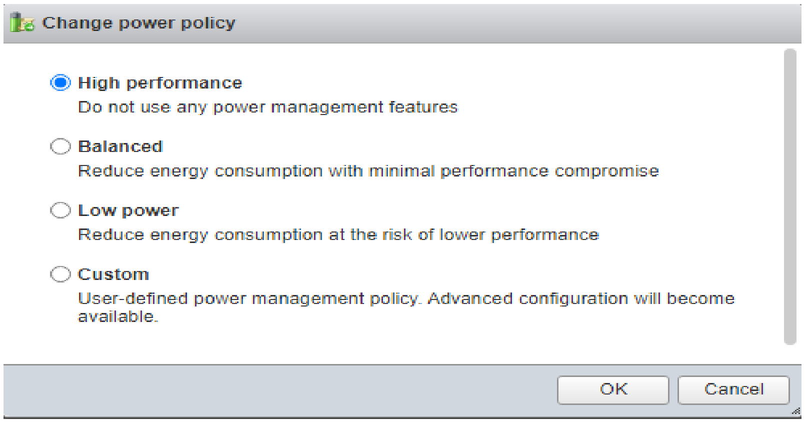
Note: Implementing this policy is recommended in Performance Tuning Guide for Cisco UCS M5 Servers for maximum VMware ESXi performance. If your organization has specific power policies, please set this policy accordingly.

Step 1. From the Host Client, click Manage.

Step 2. Go to Hardware > Power Management.

Step 3. Click Change policy.

Step 4. Click High performance and click OK.



Change power policy

● **High performance**
Do not use any power management features

○ **Balanced**
Reduce energy consumption with minimal performance compromise

○ **Low power**
Reduce energy consumption at the risk of lower performance

○ **Custom**
User-defined power management policy. Advanced configuration will become available.

VMware vCenter 7.0

This subject contains the following:

- Build the VMware vCenter Server Appliance
- Adjust vCenter CPU Settings
- Set up VMware vCenter Server

Procedure 1.Build the VMware vCenter Server Appliance

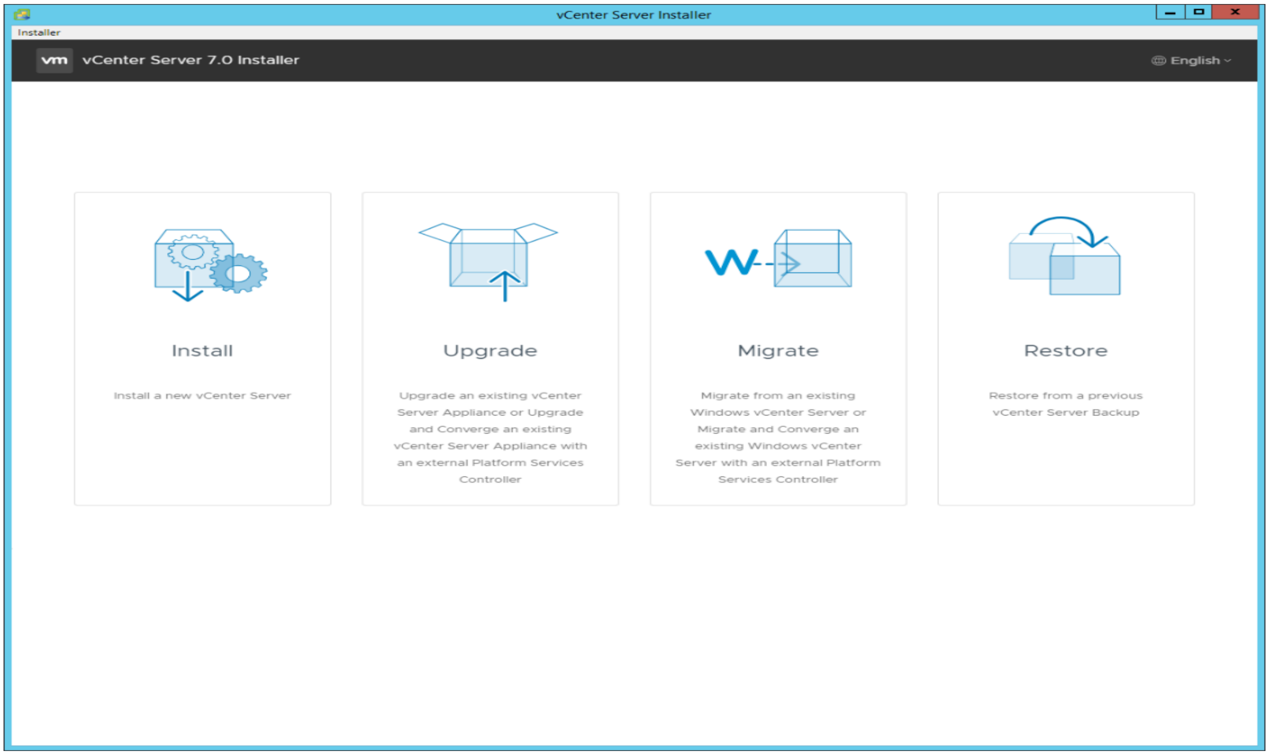
Note: The VCSA deployment consists of 2 stages: install and configuration.

Step 1. Locate and copy the VMware-VCSA-all-7.0.U3-20150588.iso file to the desktop of the management workstation. This ISO is for the VMware vSphere 7.0.U3 vCenter Server Appliance.

Note: It is important to use at minimum VMware vCenter release 7.0B to ensure access to all needed features.

Step 2. Using ISO mounting software, mount the ISO image as a disk on the management workstation. (For example, with the Mount command in Windows Server 2012 and above).

Step 3. In the mounted disk directory, navigate to the vcsa-ui-installer > win32 directory and double-click `installer.exe`. The vCenter Server Appliance Installer wizard appears.



vCenter Server Installer

Installer

vm vCenter Server 7.0 Installer

English

Install

Install a new vCenter Server

Upgrade

Upgrade an existing vCenter Server Appliance or Upgrade and Converge an existing vCenter Server Appliance with an external Platform Services Controller

Migrate

Migrate from an existing Windows vCenter Server or Migrate and Converge an existing Windows vCenter Server with an external Platform Services Controller

Restore

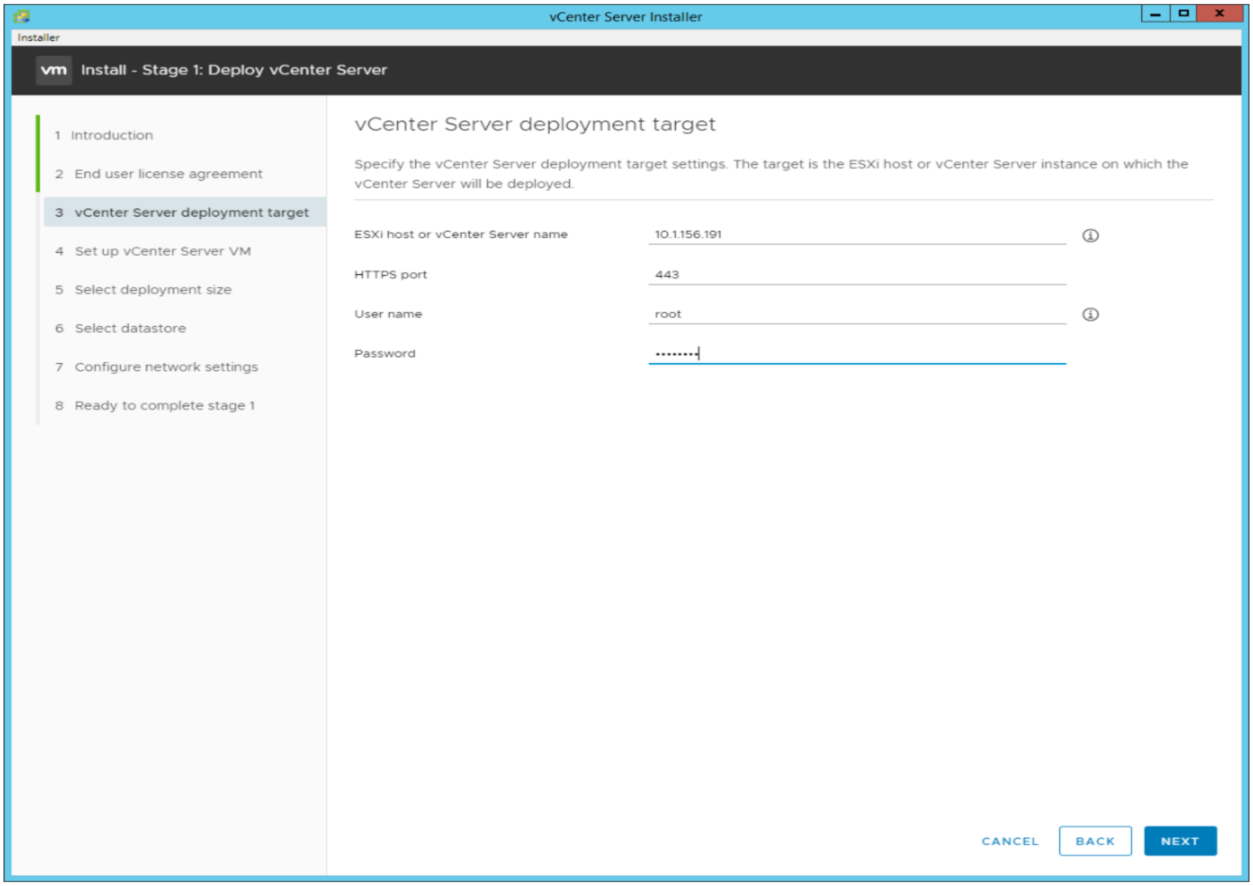
Restore from a previous vCenter Server Backup

Step 4. Click Install to start the vCenter Server Appliance deployment wizard.

Step 5. Click NEXT in the Introduction section.

Step 6. Read and accept the license agreement and click NEXT.

Step 7. In the “vCenter Server deployment target” window, enter the host name or IP address of the first ESXi host, Username (root) and Password. Click NEXT.


vCenter Server Installer
Installer
vm Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
CANCEL
BACK
NEXT

vCenter Server deployment target

Specify the vCenter Server deployment target settings. The target is the ESXi host or vCenter Server instance on which the vCenter Server will be deployed.

ESXi host or vCenter Server name: 10.1.156.191

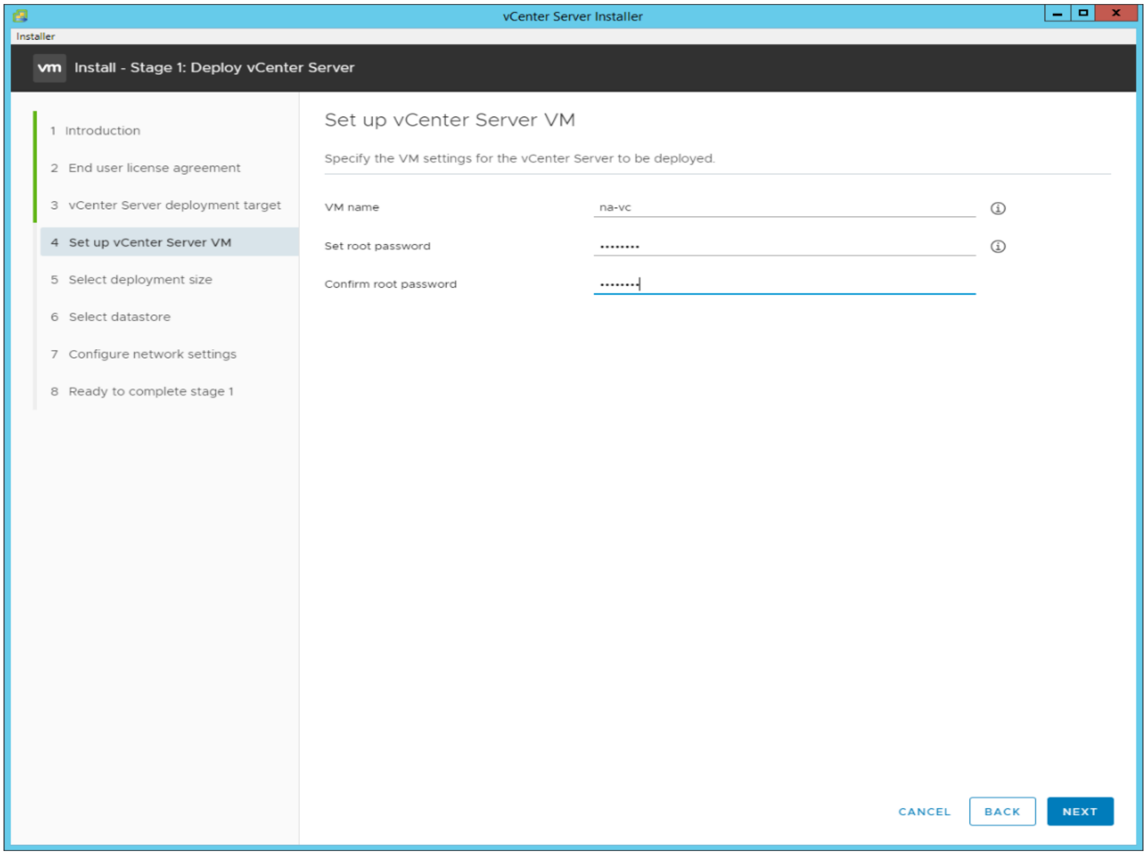
HTTPS port: 443

User name: root

Password: ••••••••

Step 8. Click YES to accept the certificate.

Step 9. Enter the Appliance VM name and password details in the “Set up vCenter Server VM” section. Click NEXT.



vCenter Server Installer
Installer
vm Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
CANCEL
BACK
NEXT

Set up vCenter Server VM

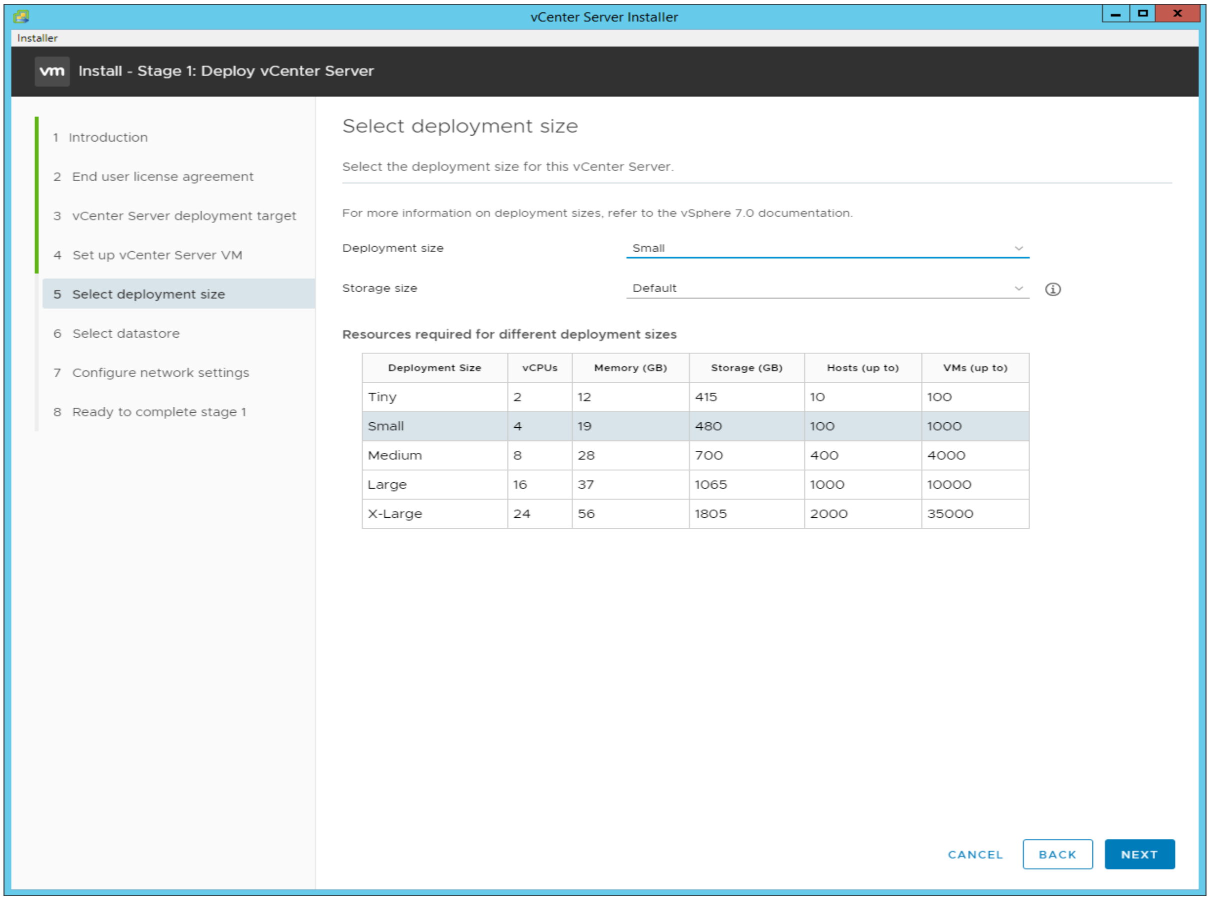
Specify the VM settings for the vCenter Server to be deployed.

VM name: na-vc

Set root password: ••••••••

Confirm root password: ••••••••

Step 10. In the “Select deployment size” section, click the Deployment size and Storage size. For example, click “Small” and “Default.” Click NEXT.


vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
CANCEL
BACK
NEXT

Select deployment size

Select the deployment size for this vCenter Server.

For more information on deployment sizes, refer to the vSphere 7.0 documentation.

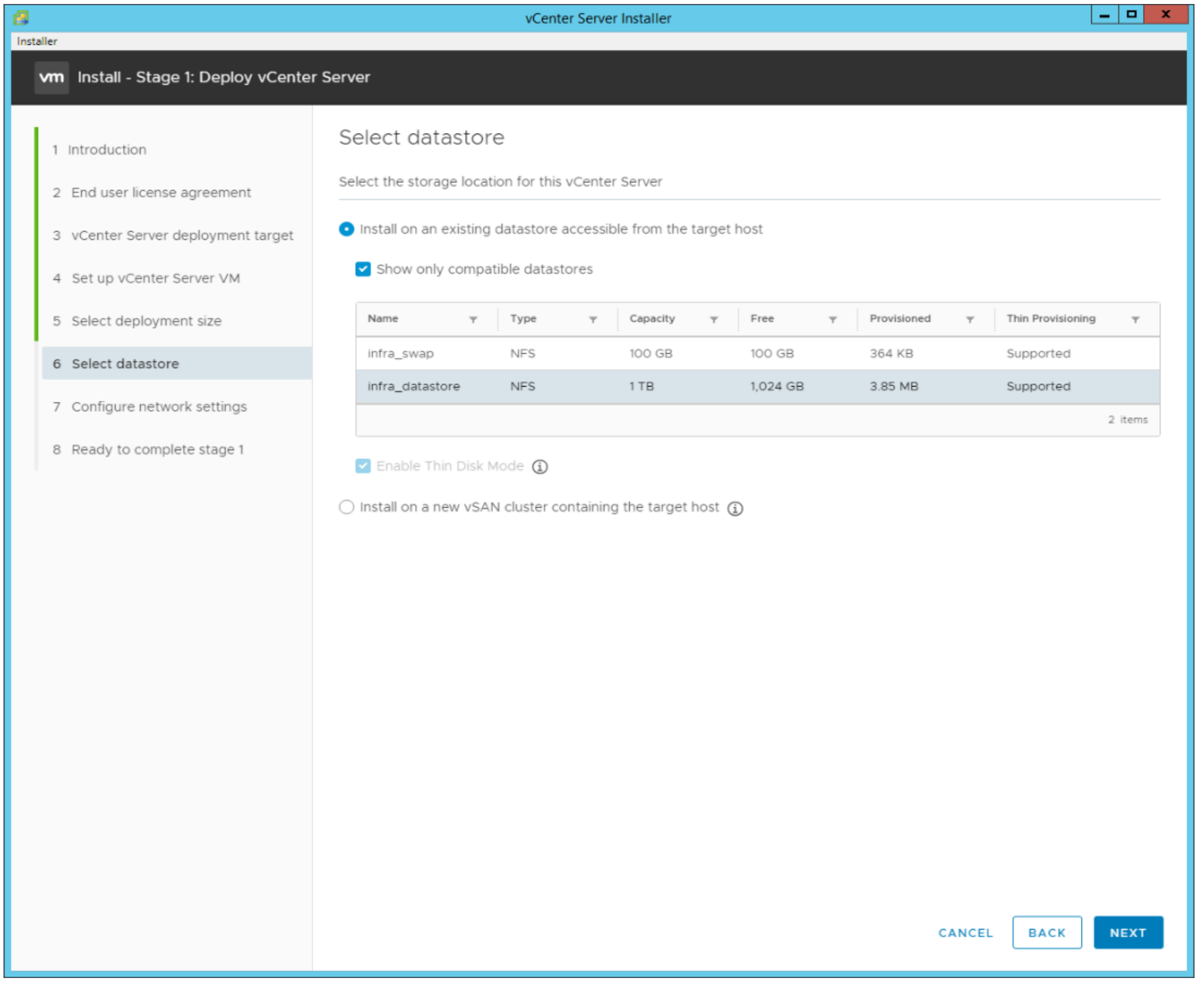
Deployment size: Small

Storage size: Default

Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	12	415	10	100
Small	4	19	480	100	1000
Medium	8	28	700	400	4000
Large	16	37	1065	1000	10000
X-Large	24	56	1805	2000	35000

Step 11. Click infra_datastore for storage. Click NEXT.


vCenter Server Installer
Installer
vm Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
CANCEL
BACK
NEXT

Select datastore

Select the storage location for this vCenter Server

● Install on an existing datastore accessible from the target host

☑ Show only compatible datastores

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
infra_swap	NFS	100 GB	100 GB	364 KB	Supported
infra_datastore	NFS	1 TB	1,024 GB	3.85 MB	Supported

2 items

☑ Enable Thin Disk Mode ⓘ

○ Install on a new vSAN cluster containing the target host ⓘ

Step 12. In the “Network Settings” section, configure the following settings:

a. Click a Network: IB-MGMT Network.

Note: It is important that the vCenter VM stay on the IB-MGMT Network on vSwitch0 and that it not get moved to a vDS. If vCenter is moved to a vDS and the virtual environment is completely shut down and then brought back up, and it is attempted to bring up vCenter on a different host than the one it was running on before the shutdown, vCenter will not have a functional network connection. With the vDS, for a virtual machine to move from one host to another, vCenter must be up and running to coordinate the move of the virtual ports on the vDS. If vCenter is down, the port move on the vDS cannot occur correctly. Moving vCenter to a different host on vSwitch0 to be brought up always occurs correctly without requiring vCenter to already be up and running.

b. IP version: IPV4

c. IP assignment: static

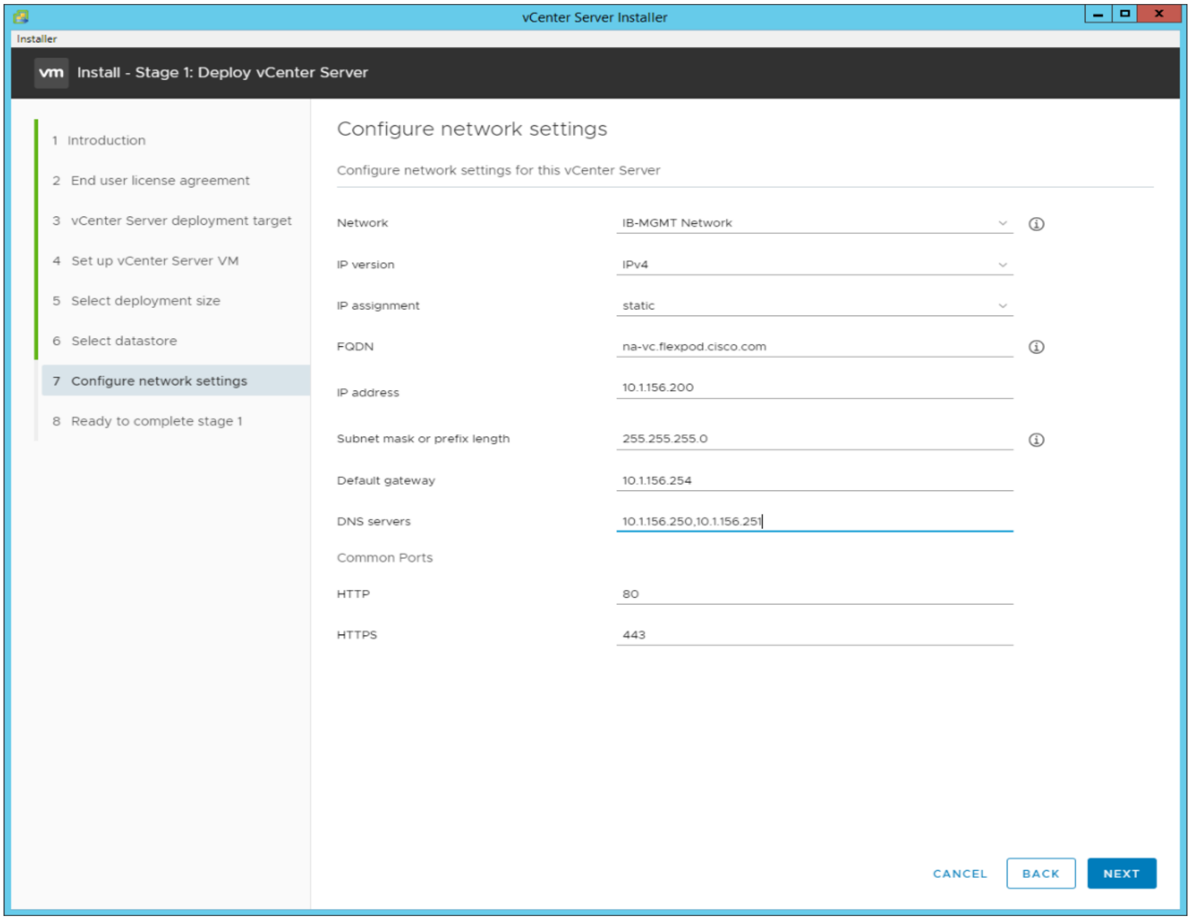
d. FQDN: <vcenter-fqdn>

e. IP address: <vcenter-ip>

f. Subnet mask or prefix length: <vcenter-subnet-mask>

g. Default gateway: <vcenter-gateway>

h. DNS Servers: <dns-server1>,<dns-server2>


vCenter Server Installer
Installer
vm Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
CANCEL
BACK
NEXT

Configure network settings

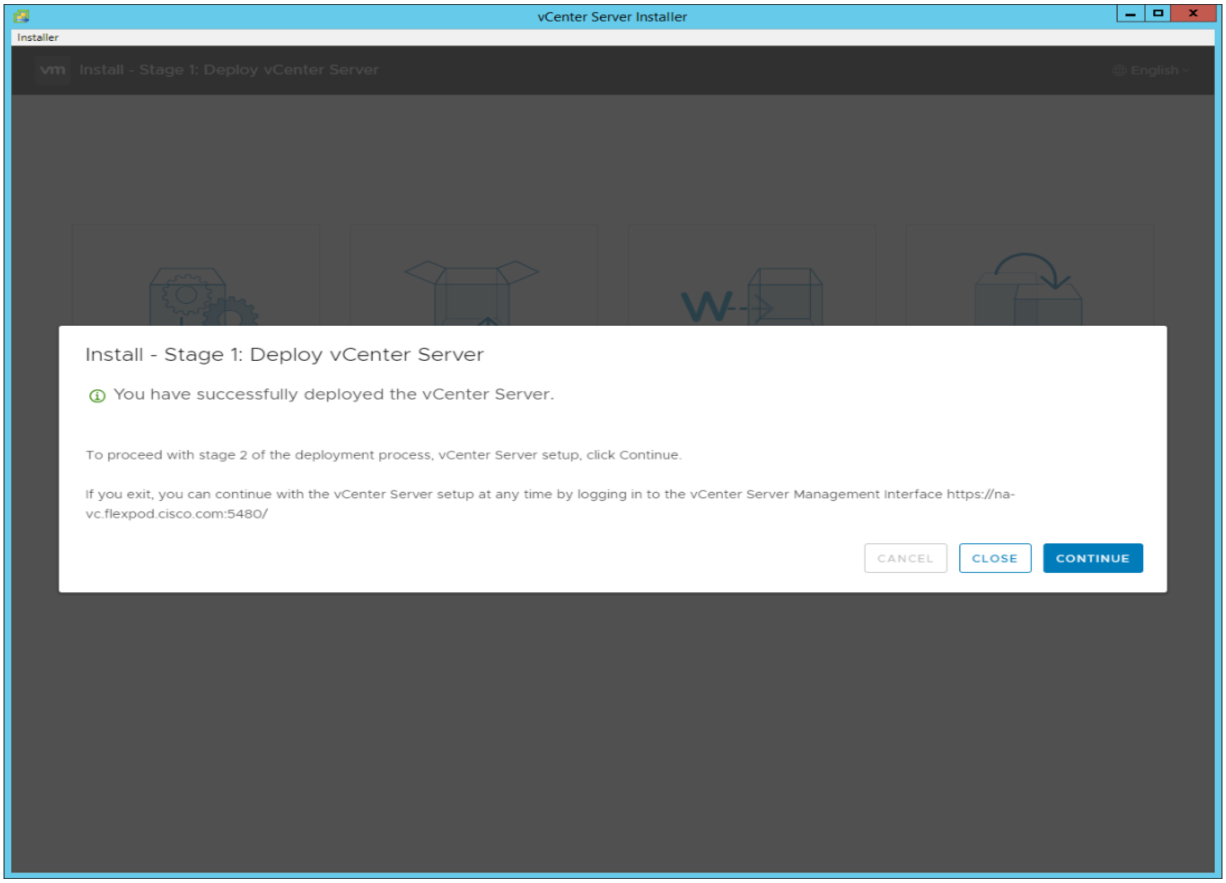
Configure network settings for this vCenter Server

Network	IB-MGMT Network
IP version	IPv4
IP assignment	static
FQDN	na-vc.flexpod.cisco.com
IP address	10.1.156.200
Subnet mask or prefix length	255.255.255.0
Default gateway	10.1.156.254
DNS servers	10.1.156.250,10.1.156.251
Common Ports	
HTTP	80
HTTPS	443

Step 13. Click NEXT.

Step 14. Review all values and click FINISH to complete the installation.

Note: The vCenter Server appliance installation will take a few minutes to complete.



Install - Stage 1: Deploy vCenter Server

You have successfully deployed the vCenter Server.

To proceed with stage 2 of the deployment process, vCenter Server setup, click Continue.

If you exit, you can continue with the vCenter Server setup at any time by logging in to the vCenter Server Management Interface https://na-vc.flexpod.cisco.com:5480/

Step 15. Click CONTINUE to proceed with stage 2 configuration.

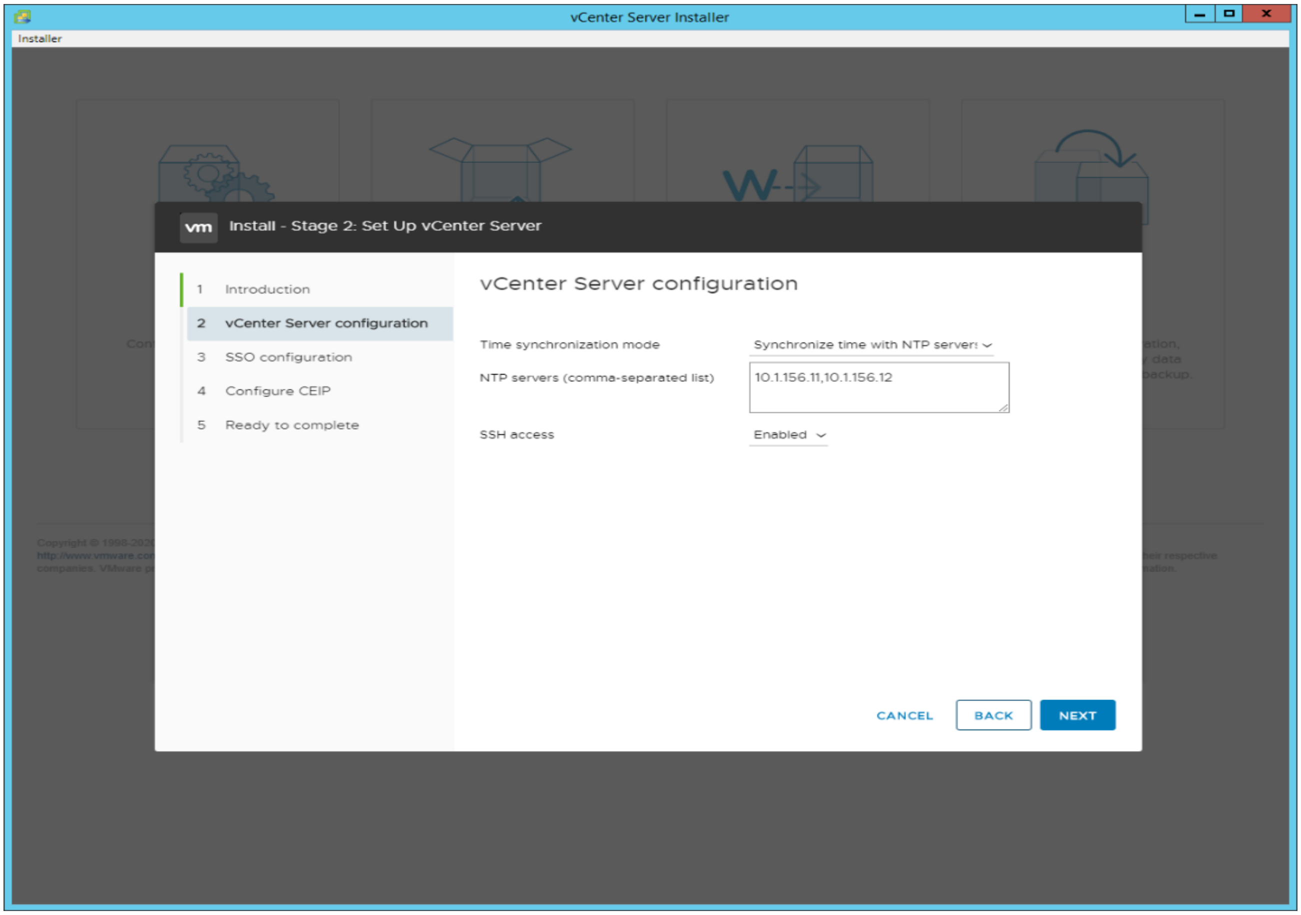
Step 16. Click NEXT.

Step 17. In the vCenter Server configuration window, configure these settings:

a. Time Synchronization Mode: Synchronize time with NTP servers.

b. NTP Servers: <nexus-a-ntp-ip>,<nexus-b-ntp-ip>

c. SSH access: Enabled.



vCenter Server configuration

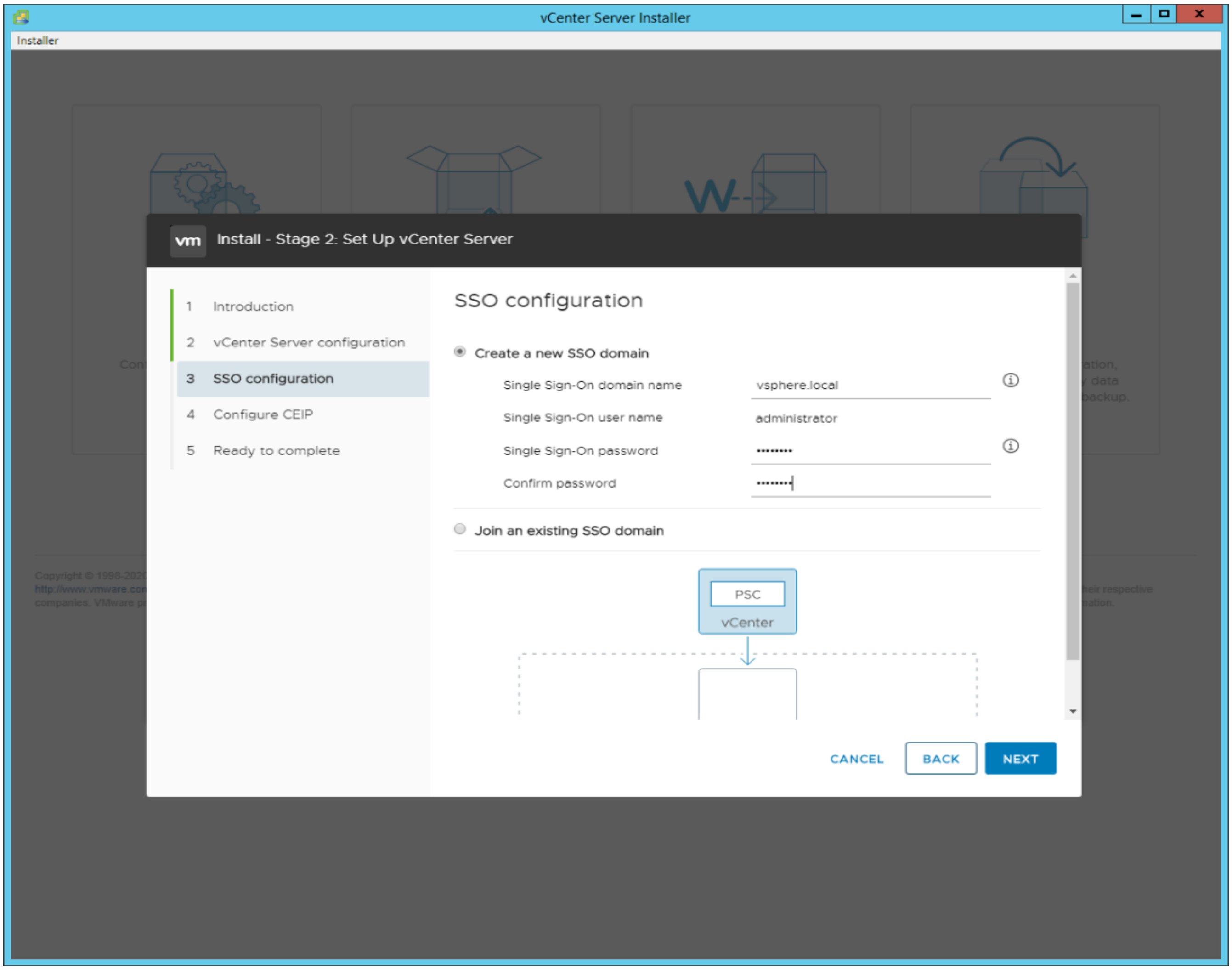
Time synchronization mode: Synchronize time with NTP servers

NTP servers (comma-separated list): 10.1.156.11,10.1.156.12

SSH access: Enabled

Step 18. Click NEXT.

Step 19. Complete the SSO configuration as shown below or according to your organization's security policies:



Install - Stage 2: Set Up vCenter Server

1 Introduction
2 vCenter Server configuration
3 SSO configuration
4 Configure CEIP
5 Ready to complete

SSO configuration

● Create a new SSO domain

Single Sign-On domain name: vsphere.local

Single Sign-On user name: administrator

Single Sign-On password: ••••••••

Confirm password: ••••••••

○ Join an existing SSO domain

Step 20. Click NEXT.

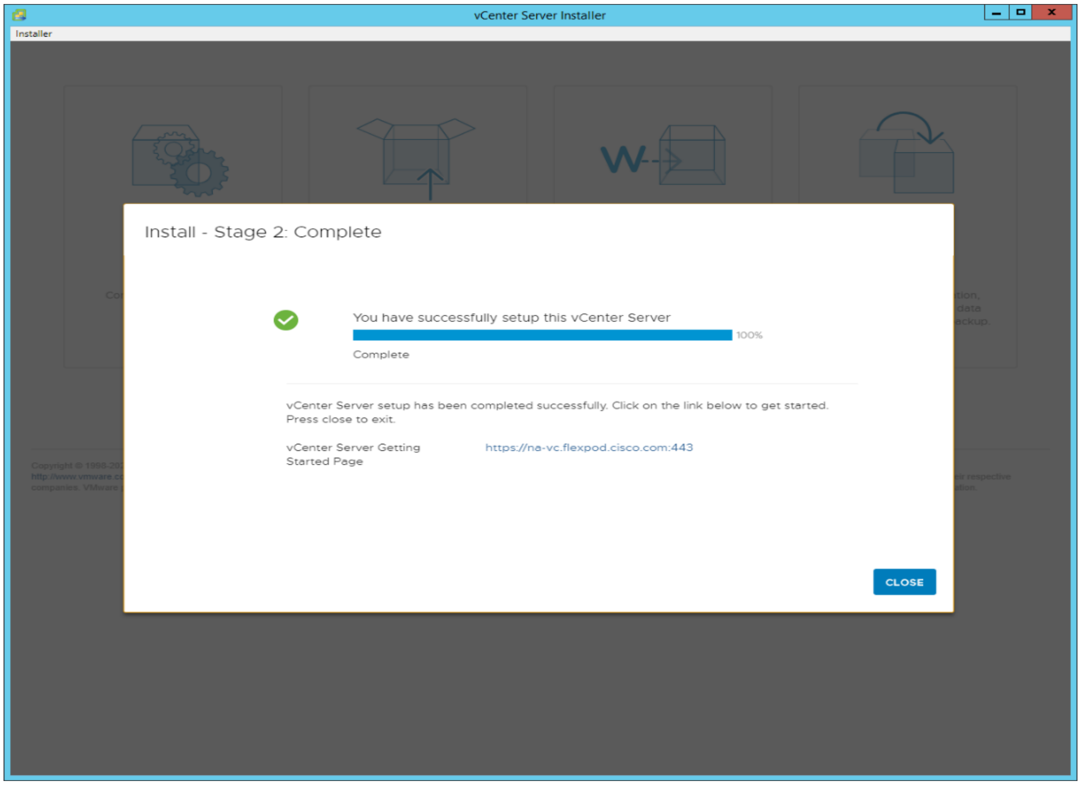
Step 21. Decide whether to join VMware's Customer Experience Improvement Program (CEIP).

Step 22. Click NEXT.

Step 23. Review the configuration and click FINISH.

Step 24. Click OK.

Note: The Server setup will take a few minutes to complete.



Install - Stage 2: Complete

You have successfully setup this vCenter Server

100%

Complete

vCenter Server setup has been completed successfully. Click on the link below to get started. Press close to exit.

vCenter Server Getting Started Page https://na-vc.flexpod.cisco.com:443

Step 25. Click CLOSE. Eject or unmount the VCSA installer ISO.

Procedure 2. Adjust vCenter CPU settings and resolve Admission Control issues

Note: If a vCenter deployment size Small or Larger was selected in the vCenter setup, it is possible that the VCSA's CPU setup does not match the Cisco UCS server CPU hardware configuration. Cisco UCS B and C-Series servers are normally 2-socket servers. In this validation, the Small deployment size was selected and vCenter was setup for a 4-socket server. This setup will cause issues in the VMware ESXi cluster Admission Control.

Step 1. Open a web browser on the management workstation and navigate to the VM-Host-Infra-01 management IP address.

Step 2. Enter root for the user name.

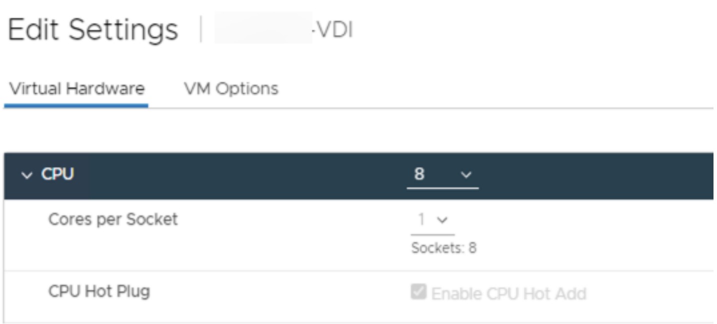
Step 3. Enter the root password.

Step 4. Click Login to connect.

Step 5. On the left, click Virtual Machines.

Step 6. In the center pane, right-click the vCenter VM and click Edit settings.

Step 7. In the Edit settings window, expand CPU and check the value of Sockets.



Edit Settings | [redacted]-VDI

CPU: 8

Cores per Socket: 1

Sockets: 8

CPU Hot Plug: ☑ Enable CPU Hot Add

Step 8. If the number of Sockets does not match your server configuration, it will need to be adjusted. Click Cancel.

Step 9. If the number of Sockets needs to be adjusted:

a. Right-click the vCenter VM and click Guest OS > Shut down. Click Yes on the confirmation.

b. Once vCenter is shut down, right-click the vCenter VM and click Edit settings.

c. In the Edit settings window, expand CPU and change the Cores per Socket value to make the Sockets value equal to your server configuration (normally 2).

d. Click Save.

e. Right-click the vCenter VM and click Power > Power on. Wait approximately 10 minutes for vCenter to come up.

Procedure 3. Set up VMware vCenter Server

Step 1. Using a web browser, navigate to https://<vcenter-ip-address>:5480.

Step 2. Log into the VMware vCenter Server Management interface as root with the root password set in the vCenter installation.

Step 3. In the menu on the left, click Time.

Step 4. Click EDIT.

Step 5. Select the appropriate Time zone and click SAVE.

Step 6. In the menu on the left click Administration.

Step 7. According to your Security Policy, adjust the settings for the root user and password.

Step 8. Click Update.

Step 9. Follow the prompts to STAGE AND INSTALL any available vCenter updates. In this validation, vCenter version 7.0.2.00500 was installed.

Step 10. Go to root > Logout to logout of the Appliance Management interface.

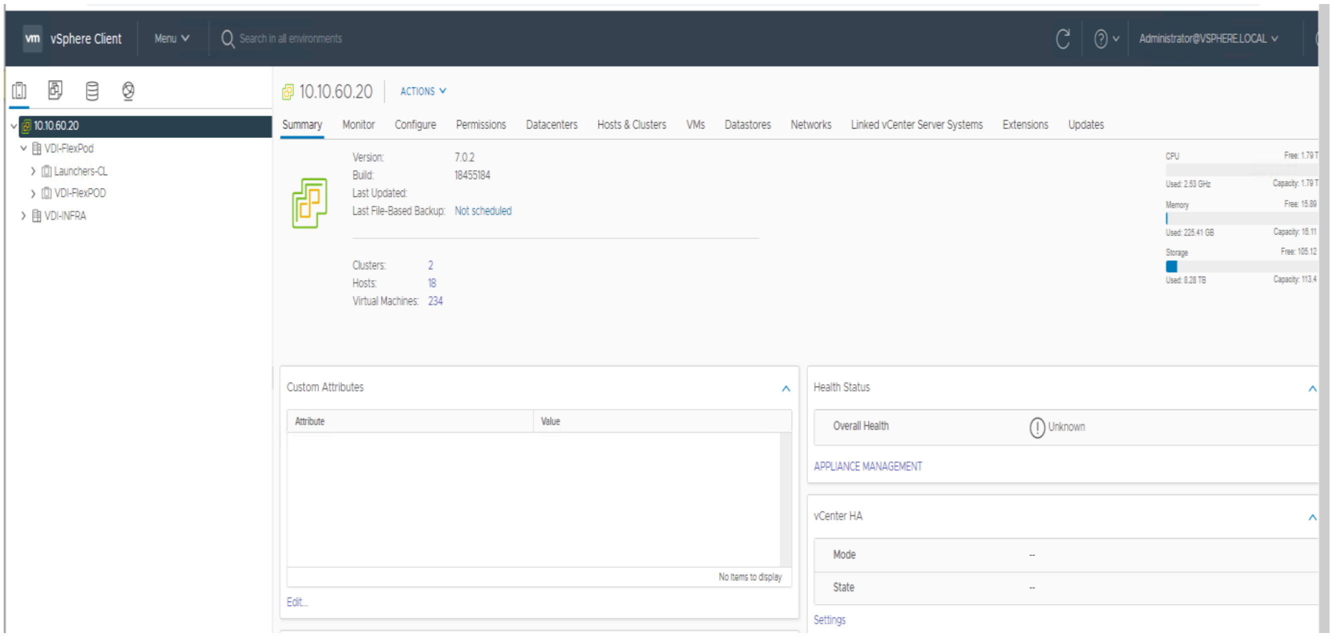
Step 11. Using a web browser, navigate to https://<vcenter-fqdn>. You will need to navigate security screens.

Note: With VMware vCenter 7.0.U3 the use of the vCenter FQDN is required.

Step 12. Click LAUNCH VSPHERE CLIENT (HTML5).

Note: Although the previous versions of this document used the FLEX vSphere Web Client, the VMware vSphere HTML5 Client is the only option in vSphere 7 and will be used going forward.

Step 13. Log in using the Single Sign-On username (administrator@vsphere.local) and password created during the vCenter installation. Dismiss the Licensing warning at this time.



10.10.60.20

Version: 7.0.2
Build: 18455184
Last Updated:
Last File-Based Backup: Not scheduled

Clusters: 2
Hosts: 18
Virtual Machines: 234

CPU Free: 1.79 T
Used: 2.53 GHz Capacity: 1.79 T
Memory Free: 15.89
Used: 225.41 GB Capacity: 16.11
Storage Free: 105.12
Used: 8.28 TB Capacity: 113.4

Custom Attributes

Attribute	Value

No items to display

Edit...

Health Status

Overall Health: Unknown

APPLIANCE MANAGEMENT

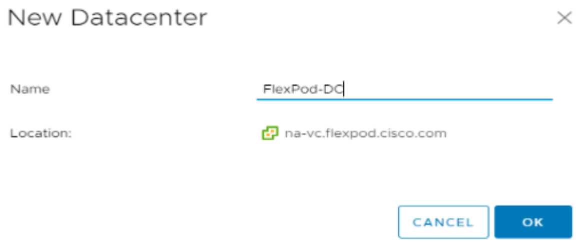
vCenter HA

Mode: --
State: --

Settings

Step 14. Click ACTIONS > New Datacenter.

Step 15. Type “FlexPod-DC” in the Datacenter name field.



New Datacenter

Name: FlexPod-DC
Location: na-vc.flexpod.cisco.com

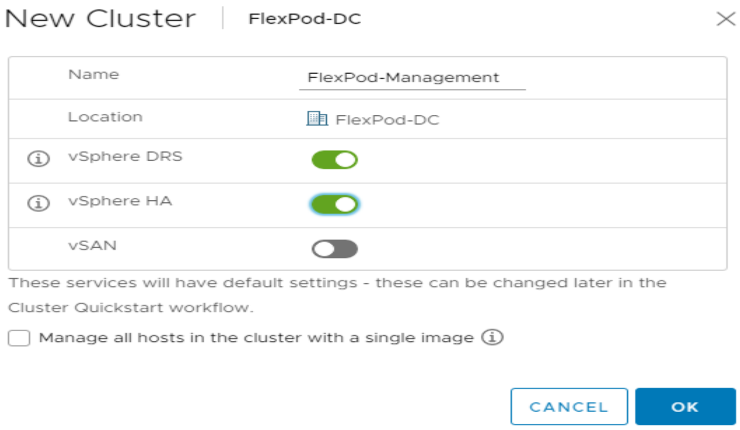
Step 16. Click OK.

Step 17. Expand the vCenter.

Step 18. Right-click the datacenter FlexPod-DC in the list in the left pane. Click New Cluster.

Step 19. Name the cluster FlexPod-Management.

Step 20. Turn on DRS and vSphere HA. Do not turn on vSAN.



New Cluster | FlexPod-DC

Name: FlexPod-Management
Location: FlexPod-DC
vSphere DRS: on
vSphere HA: on
vSAN: off

These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

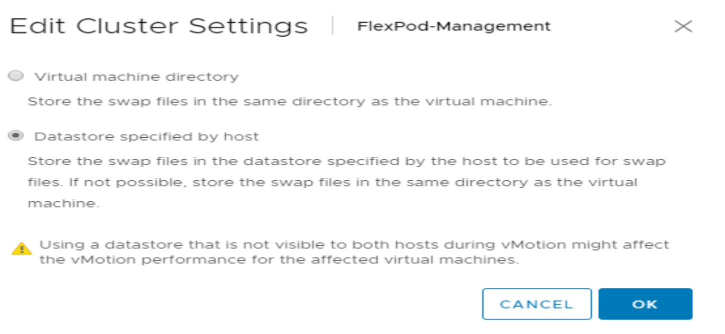
□ Manage all hosts in the cluster with a single image

Step 21. Click OK to create the new cluster.

Step 22. Right-click "FlexPod-Management" and click Settings.

Step 23. Click Configuration > General in the list located on the left and click EDIT located on the right of General.

Step 24. Click Datastore specified by host and click OK.



Edit Cluster Settings | FlexPod-Management

○ Virtual machine directory

Store the swap files in the same directory as the virtual machine.

● Datastore specified by host

Store the swap files in the datastore specified by the host to be used for swap files. If not possible, store the swap files in the same directory as the virtual machine.

⚠ Using a datastore that is not visible to both hosts during vMotion might affect the vMotion performance for the affected virtual machines.

Step 25. Right-click "FlexPod-Management" and click Add Hosts.

Step 26. In the IP address or FQDN field, enter either the IP address or the FQDN of the first VMware ESXi host. Enter root for the Username and the root password. Click NEXT.

Step 27. In the Security Alert window, click the host and click OK.

Step 28. Verify the Host summary information and click NEXT.

Step 29. Ignore warnings about the host being moved to Maintenance Mode and click FINISH to complete adding the host to the cluster.

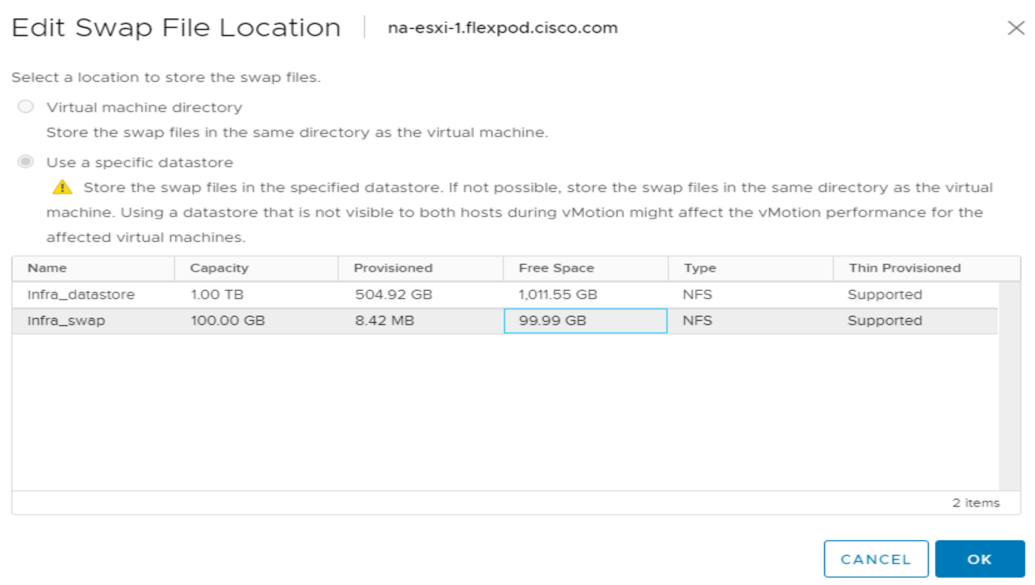
Step 30. The added ESXi host will have Warnings that the ESXi Shell and SSH have been enabled. These warnings can be suppressed.

Step 31. In the list, right-click the added ESXi host and click Settings.

Step 32. In the center pane under Virtual Machines, click Swap File location.

Step 33. Click EDIT.

Step 34. Click the infra_swap datastore and click OK.



Edit Swap File Location | na-esxi-1.flexpod.cisco.com

Select a location to store the swap files.

○ Virtual machine directory

Store the swap files in the same directory as the virtual machine.

● Use a specific datastore

⚠ Store the swap files in the specified datastore. If not possible, store the swap files in the same directory as the virtual machine. Using a datastore that is not visible to both hosts during vMotion might affect the vMotion performance for the affected virtual machines.

Name	Capacity	Provisioned	Free Space	Type	Thin Provisioned
Infra_datastore	1.00 TB	504.92 GB	1,011.55 GB	NFS	Supported
Infra_swap	100.00 GB	8.42 MB	99.99 GB	NFS	Supported

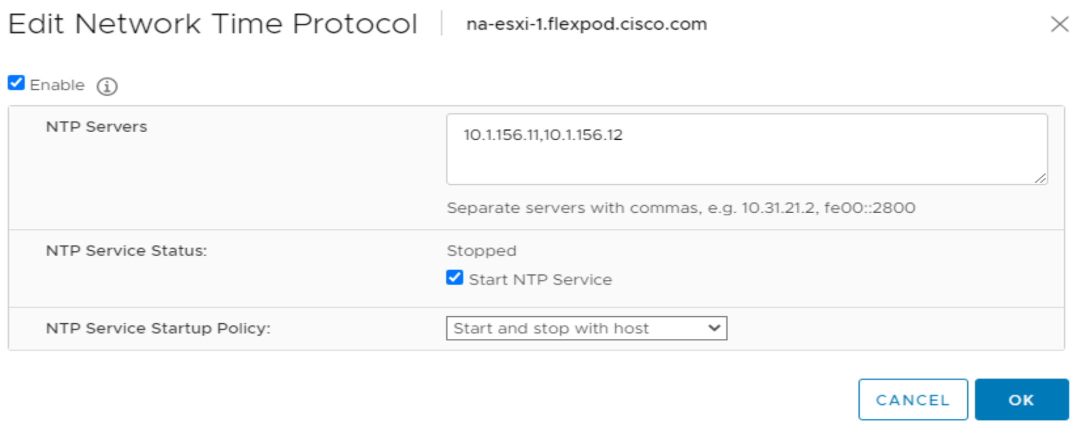
2 items

Step 35. In the list under System, click Time Configuration.

Step 36. Click EDIT to the right of Manual Time Configuration. Set the time and date to the correct local time and click OK.

Step 37. Click EDIT to the right of Network Time Protocol.

Step 38. In the Edit Network Time Protocol window, select Enable and then select Start NTP Service. Ensure the other fields are filled in correctly and click OK.



Edit Network Time Protocol | na-esxi-1.flexpod.cisco.com

☑ Enable

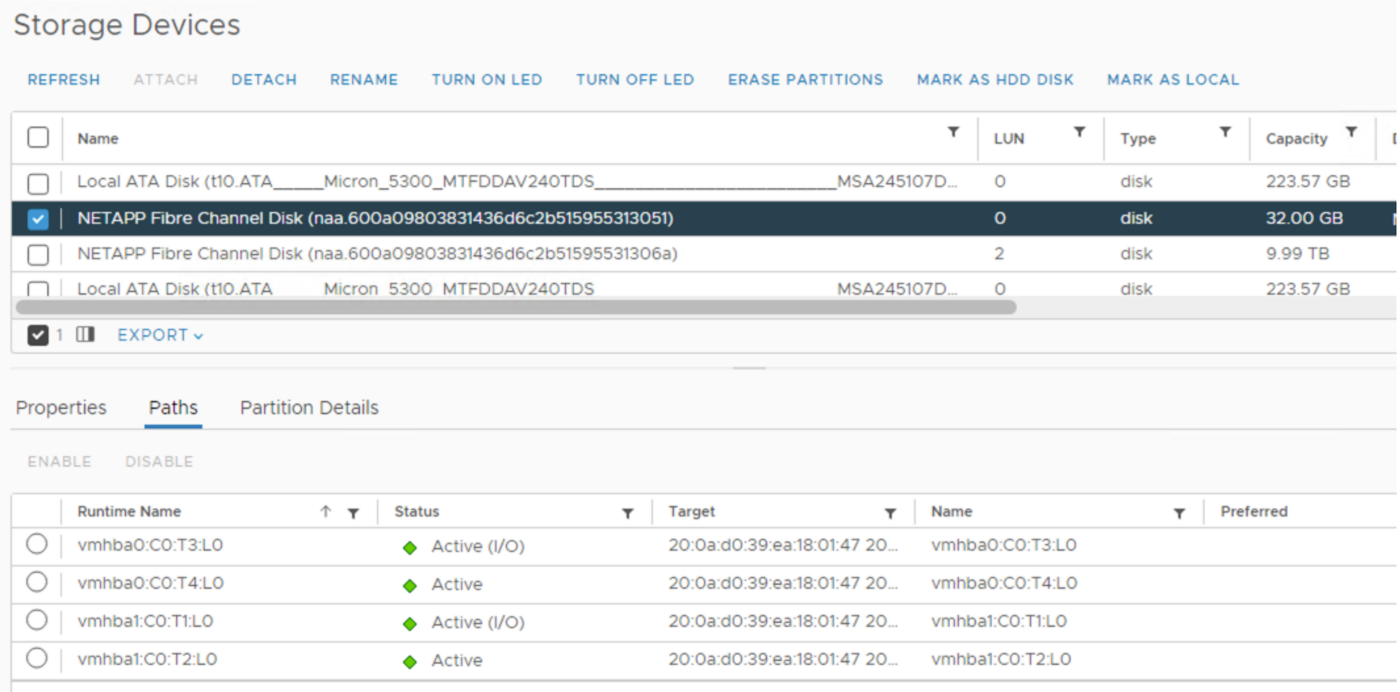
NTP Servers	10.1.156.11,10.1.156.12 Separate servers with commas, e.g. 10.31.21.2, fe00::2800
NTP Service Status:	Stopped ☑ Start NTP Service
NTP Service Startup Policy:	Start and stop with host

Step 39. In the list under Hardware, click Overview. Scroll to the bottom and ensure the Power Management Active policy is High Performance. If the Power Management Active policy is not High Performance, to the right of Power Management, click EDIT POWER POLICY. Click High performance and click OK.

Step 40. In the list under Storage, click Storage Devices. Make sure the NETAPP Fibre Channel Disk LUN 0 or NETAPP iSCSI Disk LUN 0 is selected.

Step 41. Click the Paths tab.

Step 42. Ensure that 4 paths appear, two of which should have the status Active (I/O).



Storage Devices

	Name	LUN	Type	Capacity
□	Local ATA Disk (t10.ATA_____Micron_5300_MTFDDAV240TDS_________________________MSA245107D...	0	disk	223.57 GB
☑	NETAPP Fibre Channel Disk (naa.600a09803831436d6c2b515955313051)	0	disk	32.00 GB
□	NETAPP Fibre Channel Disk (naa.600a09803831436d6c2b51595531306a)	2	disk	9.99 TB
□	Local ATA Disk (t10.ATA_____Micron_5300_MTFDDAV240TDS_________________________MSA245107D...	0	disk	223.57 GB

	Runtime Name	Status	Target	Name	Preferred
○	vmhba0:C0:T3:L0	Active (I/O)	20:0a:d0:39:ea:18:01:47 20...	vmhba0:C0:T3:L0	
○	vmhba0:C0:T4:L0	Active	20:0a:d0:39:ea:18:01:47 20...	vmhba0:C0:T4:L0	
○	vmhba1:C0:T1:L0	Active (I/O)	20:0a:d0:39:ea:18:01:47 20...	vmhba1:C0:T1:L0	
○	vmhba1:C0:T2:L0	Active	20:0a:d0:39:ea:18:01:47 20...	vmhba1:C0:T2:L0	

Configuration and Installation

This chapter contains the following:

- FlexPod Automated Deployment with Ansible
- Prerequisites

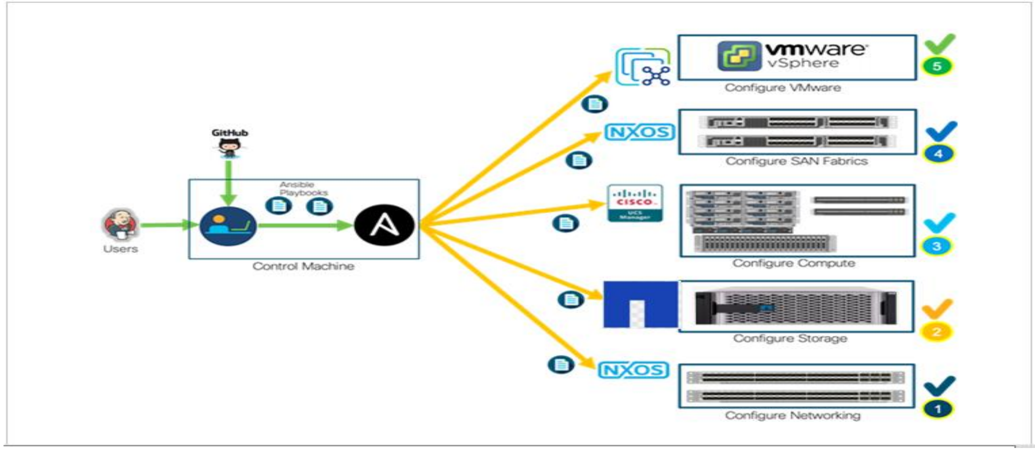
FlexPod Automated Deployment with Ansible

If using the published Ansible playbooks to configure the FlexPod infrastructure, follow the procedures detailed in this section.

Ansible Automation Workflow and Solution Deployment

This FlexPod with vSphere 7.0 U3 and Cisco UCS M6 solution uses a management workstation (control machine) to run Ansible playbooks to configure Cisco Nexus, Cisco UCS, NetApp Storage, and Install VMware Cluster.

Figure 34. High-level FlexPod Automation



Prerequisites

This subject contains the following procedure:

- Prepare Management Workstation (Control Machine)
- Update Cisco VIC Drivers for ESXi

Setting up the solution begins with a management workstation that has access to the internet and has a working installation of Ansible. The management workstation runs a variant of Linux or MacOS for ease of use with these command-line-based tools. Instructions for installing the workstation are not included in this document, but the basic installation and configuration of Ansible is explained. The following is a list of prerequisites:

- To use the Ansible playbooks demonstrated in this document (Getting Started with Red Hat Ansible), the management workstation must also have a working installation of Git and access to the Cisco DevNet public GitHub repository. The Ansible playbooks used in this document are cloned from the public repositories, located at the following links:
  - Cisco DevNet: https://developer.cisco.com/codeexchange/github/repo/ucs-compute-solutions/Flexpod-IaC-UCSM6

  - GitHub repository for FlexPod infrastructure setup: GitHub - ucs-compute-solutions/FlexPod-UCSM-M6: Ansible configuration of FlexPod with UCSM 4.2(2a), NetApp ONTAP 9.9.1, and VMware vSphere 7.0U3

- The Cisco Nexus Switches, NetApp Storage and Cisco UCS must be physically racked, cabled, powered, and configured with the management IP addresses before the Ansible-based installation procedure can begin as shown in the cabling diagram (Figure 34). If necessary, upgrade the Nexus Switches to release 9.3(7) and the Cisco UCS System to 4.2(2a) with the default firmware packages for both blades and rack servers set to 4.2(2a).
- Before running each Ansible Playbook to setup the Network, Storage, Cisco UCS and VMware, various variables must be updated based on the customers environment and specific implementation with values such as the VLANs, pools and ports on Cisco UCS, IP addresses for iSCSI interfaces and values needed for the ESXi installation and configuration.

Note: Day 2 Configuration tasks such as adding datastores or ESXi servers have been performed manually or with Cisco Intersight Cloud Orchestrator (ICO) and the information has been provided in the respective sections of this document.

Procedure 1. Prepare Management Workstation (Control Machine)

Note: In this section, the installation steps are performed on the CentOS management host to prepare the host for solution deployment to support the automation of Cisco UCS, Cisco Nexus, NetApp Storage and VMware installation using Ansible Playbooks.

Step 1. Install the EPEL repository on the management host:

```
[root@FSV-Automation ~]# yum install epel-release
```

Step 2. Install Ansible engine.

```
[root@FSV-Automation ~]# yum install ansible
```

Step 3. Verify the Ansible version to make sure it’s at least release 2.9:

```
  [root@FS-Automation tasks]# ansible --version
ansible 2.10.7
  config file = None
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/local/lib/python3.6/site-packages/ansible
  executable location = /usr/local/bin/ansible
  python version = 3.6.8 (default, Aug 24 2020, 17:57:11) [GCC 8.3.1 20191121 (Red Hat 8.3.1-5)]
```

Step 4. Install **pip** the package installer for Python:

```
[root@FSV-Automation ~]# yum install python-pip
```

Step 5. Install the UCS SDK:

```
[root@FSV-Automation ~]# pip3 install ucsmsdk
```

Step 6. Install the **paramiko** package for Cisco Nexus automation:

```
[root@FSV-Automation ~]# pip3 install paramiko
```

Step 7. SSH into each of the Cisco Nexus and Cisco MDS switches using Ansible so that the SSH keys are cached:

```
[root@FSV-Automation ~]# ssh admin@10.1.164.61
The authenticity of host '10.1.164.61 (10.1.164.61)' can't be established.
RSA key fingerprint is SHA256:mtomJluZVkcITgSLhVygocSnojlyPPDPmcJLQX2dfu4.
RSA key fingerprint is MD5:b4:e3:86:97:99:58:df:0d:5d:20:b2:5b:d5:69:aa:23.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.164.61' (RSA) to the list of known hosts.
User Access Verification
```

```
Password:
```

Step 8. Install the NetApp specific python module:

```
[root@FSV-Automation ~]# pip3 install netapp-lib
```

Step 9. Install ansible-galaxy collections for Cisco UCS, Cisco Nexus/MDS switches and NetApp Storage Array as follows:

```
[root@FSV-Automation ~]# ansible-galaxy collection install cisco.nxos
[root@FSV-Automation ~]# ansible-galaxy collection install cisco.ucs
[root@FSV-Automation ~]# ansible-galaxy collection install netapp.ontap
[root@FSV-Automation ~]# ansible-galaxy collection install community.vmware
```

Note: We validated the Ansible automation with both python 2.7.5 and python 3.6 as the python interpreter for Ansible.

Procedure 2. Update Cisco VIC Drivers for ESXi

Note: When ESXi is installed from Cisco Custom ISO, you might have to update the Cisco VIC drivers for VMware ESXi Hypervisor to match the current Cisco Hardware and Software Interoperability Matrix.

In this Validated Design the following drivers were used:

- Cisco-nenic- 1.0.33.0
- Cisco-nfnic- 4.0.0.56

Step 1. Log into your VMware Account to download required drivers for FNIC and NENIC as per the recommendation.

Step 2. Enable SSH on ESXi to run following commands:

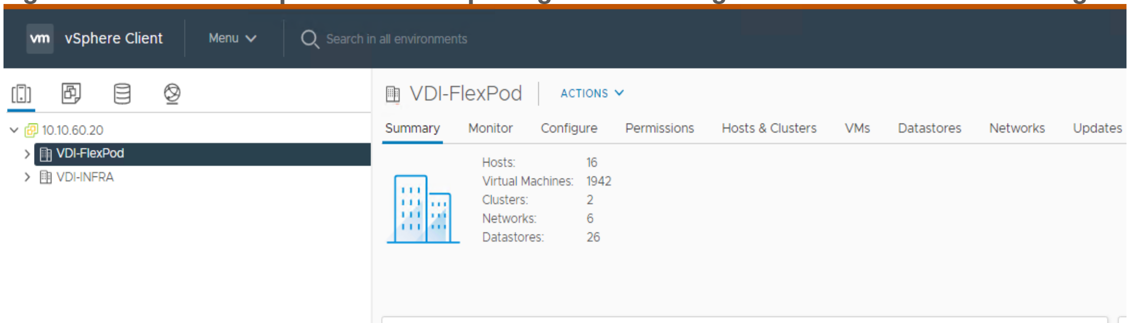
```
esxcli software vib update -d /path/offline-bundle.zip
```

VMware Clusters

The VMware vSphere Client was configured to support the solution and testing environment as follows:

- Datacenter: FlexPod - NetApp Storage AFF A400 with Cisco UCS
- Cluster: FlexPod-VDI - Single-session/Multi-session OS VDA workload
- Infrastructure Cluster: Infrastructure virtual machines (vCenter, Active Directory, DNS, DHCP, SQL Server, Citrix Virtual Apps and Desktops Connection Servers, and other common services), Login VSI launcher infrastructure were connected using the same set of switches.

Figure 35. VMware vSphere WebUI Reporting Cluster Configuration for this Validated Design



Hosts: 16
Virtual Machines: 1942
Clusters: 2
Networks: 6
Datastores: 26

Build the Virtual Machines and Environment for Workload Testing

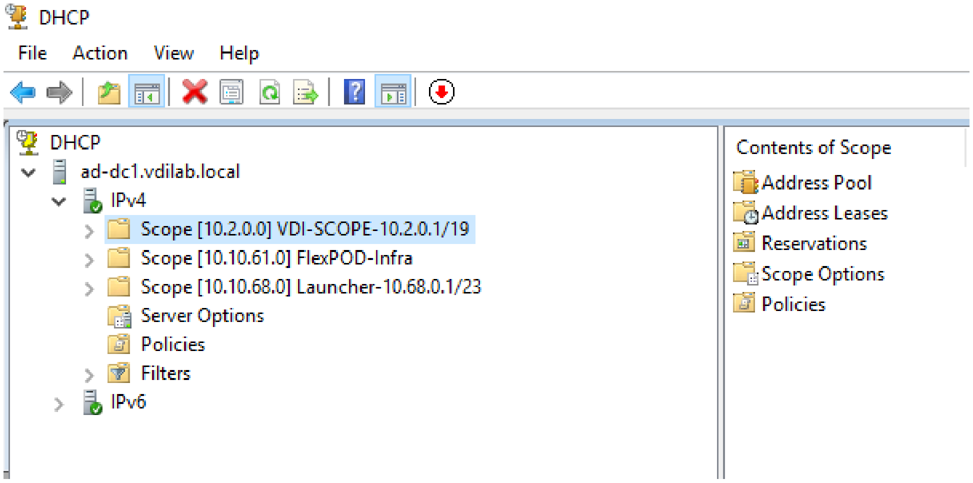
This chapter contains the following:

- Prerequisites
- Software Infrastructure Configuration
- Prepare the Master Targets
- Install and Configure Citrix Virtual Apps and Desktops
- Install Citrix Virtual Apps and Desktops Delivery Controller, Citrix Licensing, and StoreFront
- Install and Configure Citrix Provisioning Server 2203
- Install the Citrix Provisioning Server Target Device Software
- Provision Virtual Desktop Machines
- Citrix Virtual Apps and Desktops Policies and Profile Management
- FSLogix for Citrix Virtual Apps and Desktops Profile Management

Prerequisites

Create all necessary DHCP scopes for the environment and set the Scope Options.

Figure 36. Example of the DHCP Scopes used in this CVD



Software Infrastructure Configuration

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

Install and configure the infrastructure virtual machines by following the process listed in Table 23.

Table 23. Test Infrastructure Virtual Machine Configuration

Configuration	Citrix Virtual Apps and Desktops Controllers Virtual Machines	Citrix Provisioning Servers Virtual Machines
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2019

Virtual CPU amount	6	6
Memory amount	24 GB	24 GB
Network	VMXNET3 k23-Infra-Mgmt-71	VMXNET3 k23-Infra-Mgmt-71
Disk-1 (OS) size	40 GB	40 GB
Disk-2 size	-	200 GB Disk Store

Configuration	**Microsoft Active Directory DCs** **Virtual Machines**	**vCenter Server Appliance** **Virtual Machine**
Operating system	Microsoft Windows Server 2019	VCSA – SUSE Linux
Virtual CPU amount	4	8
Memory amount	8 GB	32 GB
Network	VMXNET3 k23-Infra-Mgmt-71	VMXNET3 k23-InBand-Mgmt-70
Disk size	40 GB	698.84 GB (across 13 VMDKs)

Configuration	**Microsoft SQL Server** **Virtual Machine**	**Citrix StoreFront Controller** **Virtual Machine**
Operating system	Microsoft Windows Server 2019 Microsoft SQL Server 2019	Microsoft Windows Server 2019
Virtual CPU amount	8	4
Memory amount	24GB	8 GB
Network	VMXNET3 k23-Infra-Mgmt-71	VMXNET3 k23-Infra-Mgmt-71
Disk-1 (OS) size	40 GB	40 GB
Disk-2 size	100 GB SQL Databases\Logs	-

Prepare the Master Targets

This section provides guidance regarding creating the golden (or master) images for the environment. Virtual machines for the master targets must first be installed with the software components needed to build the golden images. Additionally, all available security patches as of October 2021 for the Microsoft operating systems, SQL server and Microsoft Office 2016 were installed.

To prepare Single-session OS or Multi-session OS master virtual machine, there are three major steps: installing the PVS Target Device x64 software (if delivered with Citrix Provisioning Services), installing the Virtual Delivery Agents (VDAs), and installing application software.

Note: For this CVD, the images contain the basics needed to run the Login VSI workload.

The Single-session OS and Multi-session OS master target virtual machines were configured as detailed in Table 24.

Table 24. Single-session OS and Multi-session OS Virtual Machines Configurations

Configuration	Single-session OS Virtual Machines	Multi-session OS Virtual Machines
Operating system	Microsoft Windows 10 64-bit	Microsoft Windows Server 2016
Virtual CPU amount	2	8
Memory amount	4 GB	32 GB
Network	VMXNET3 10_10_72_NET	VMXNET3 10_10_72_NET
Citrix PVS vDisk size Citrix MCS Disk Size	48 GB (dynamic) 48 GB	90 GB (dynamic)
write cache Disk size	6 GB	6 GB
Citrix PVS write cache RAM cache size	256 MB	1024 MB
Additional software used for testing	Microsoft Office 2016 Office Update applied Login VSI 4.1.40 Target Software (Knowledge Worker Workload)	Microsoft Office 2016 Office Update applied Login VSI 4.1.40 Target Software (Knowledge Worker Workload)

Additional Configuration	Configure DHCP Add to domain Install VMWare tool Install .Net 3.5 Activate Office Install VDA Agent Run PVS Imaging Wizard (For non-persistent Desktops only)	Configure DHCP Add to domain Install VMWare tool Install .Net 3.5 Activate Office Install VDA Agent

Install and Configure Citrix Virtual Apps and Desktops

This section explains the installation of the core components of the Citrix Virtual Apps and Desktops system. This CVD installs two Citrix Virtual Apps and Desktops Delivery Controllers to support both hosted shared desktops (HSD), non-persistent hosted virtual desktops (HVD), and persistent hosted virtual desktops (HVD).

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 the security policy allows, use the VMware-installed self-signed certificate.

Procedure 1. Install vCenter Server Self-Signed Certificate

Step 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.

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

Step 3. Accept the security warnings.

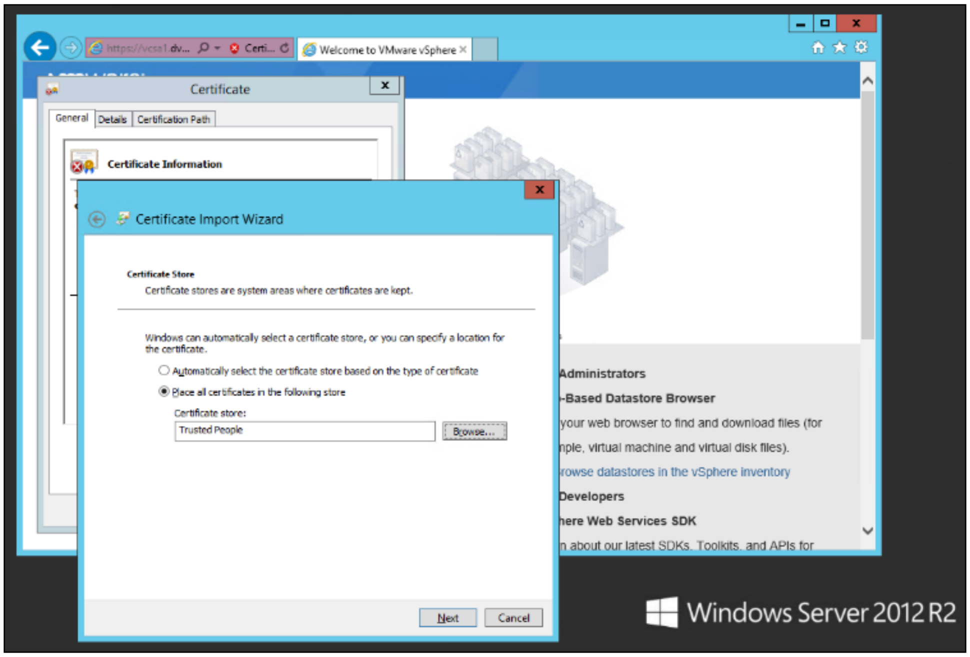
Step 4. Click the Certificate Error in the Security Status bar and select View certificates.

Step 5. Click Install certificate, select Local Machine, and then click Next.

Step 6. Select Place all certificates in the following store and then click Browse.

Step 7. Click Show physical stores.

Step 8. Click Trusted People.



https://vcsa1.dv...
Certi...
Welcome to VMware vSphere
Certificate
General
Details
Certification Path
Certificate Information
Certificate Import Wizard
Administrators
-Based Datastore Browser
your web browser to find and download files (for
nple, virtual machine and virtual disk files).
rowse datastores in the vSphere inventory
Developers
here Web Services SDK
n about our latest SDKs, Toolkits, and APIs for
Windows Server 2012 R2

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted People

Browse...

Next | Cancel

Step 9. Click Next and then click Finish.

Step 10. Repeat steps 1-9 on all Delivery Controllers and Provisioning Servers.

Install Citrix Virtual Apps and Desktops Delivery Controller, Citrix Licensing, and StoreFront

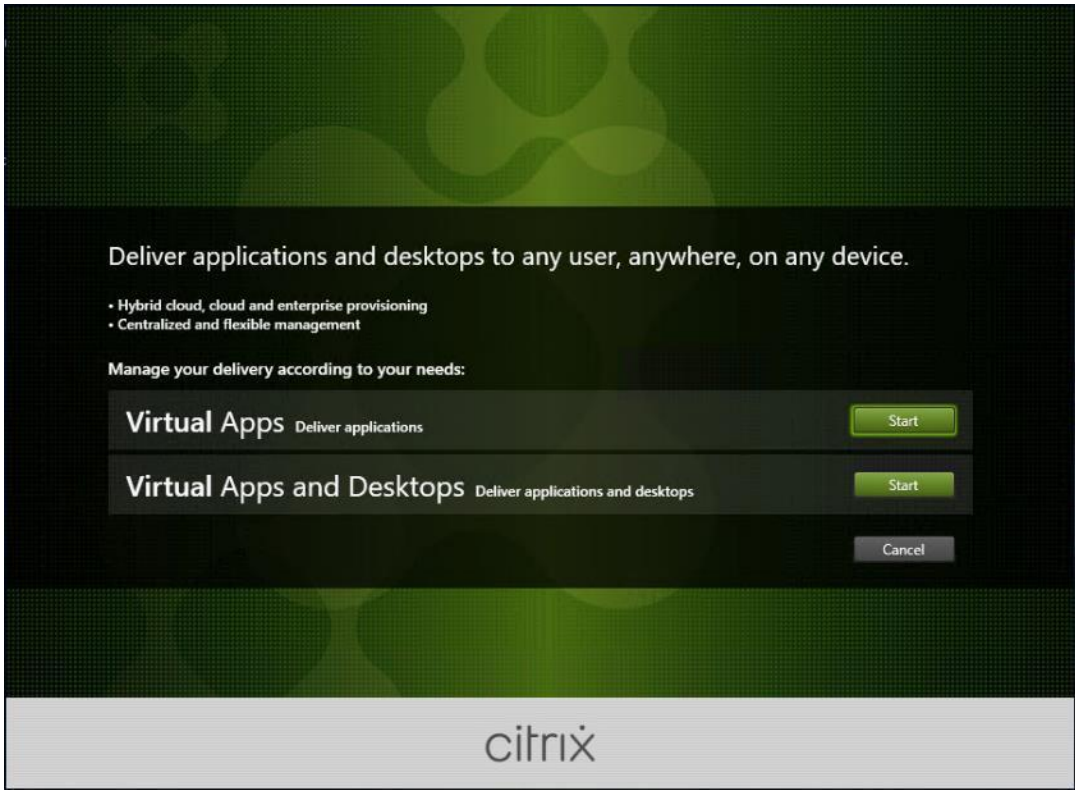
The process of installing the Citrix Virtual Apps and Desktops Delivery Controller also installs other key Citrix Virtual Apps and Desktops software components, including Studio, which is used to create and manage infrastructure components, and Director, which is used to monitor performance and troubleshoot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

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

Procedure 1. Install Citrix License Server

Step 1. To begin the installation, connect to the first Citrix License server and launch the installer from the Citrix_Virtual_Apps_and_Desktops_7_2203 ISO.

Step 2. Click Start.



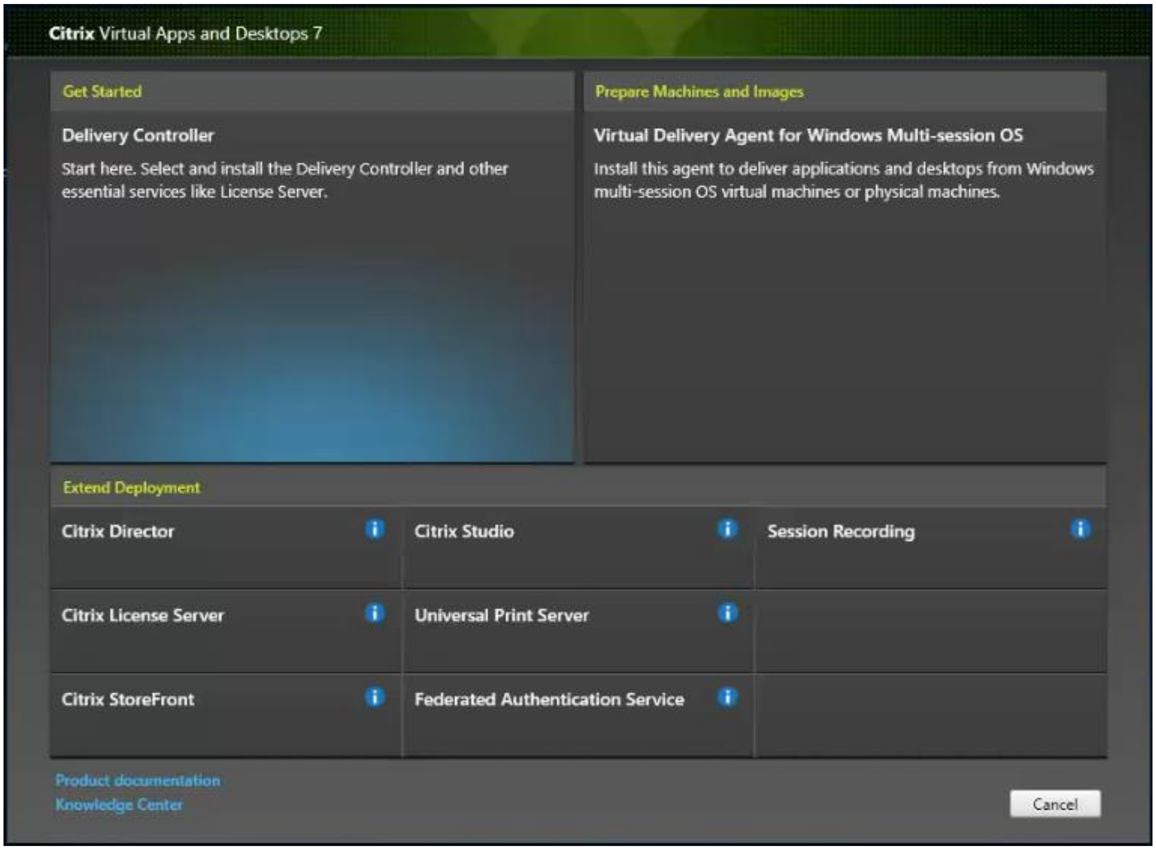
Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

Virtual Apps Deliver applications
Start
Virtual Apps and Desktops Deliver applications and desktops
Start
Cancel
citrix

Step 3. Click Extend Deployment – Citrix License Server.



Delivery Controller

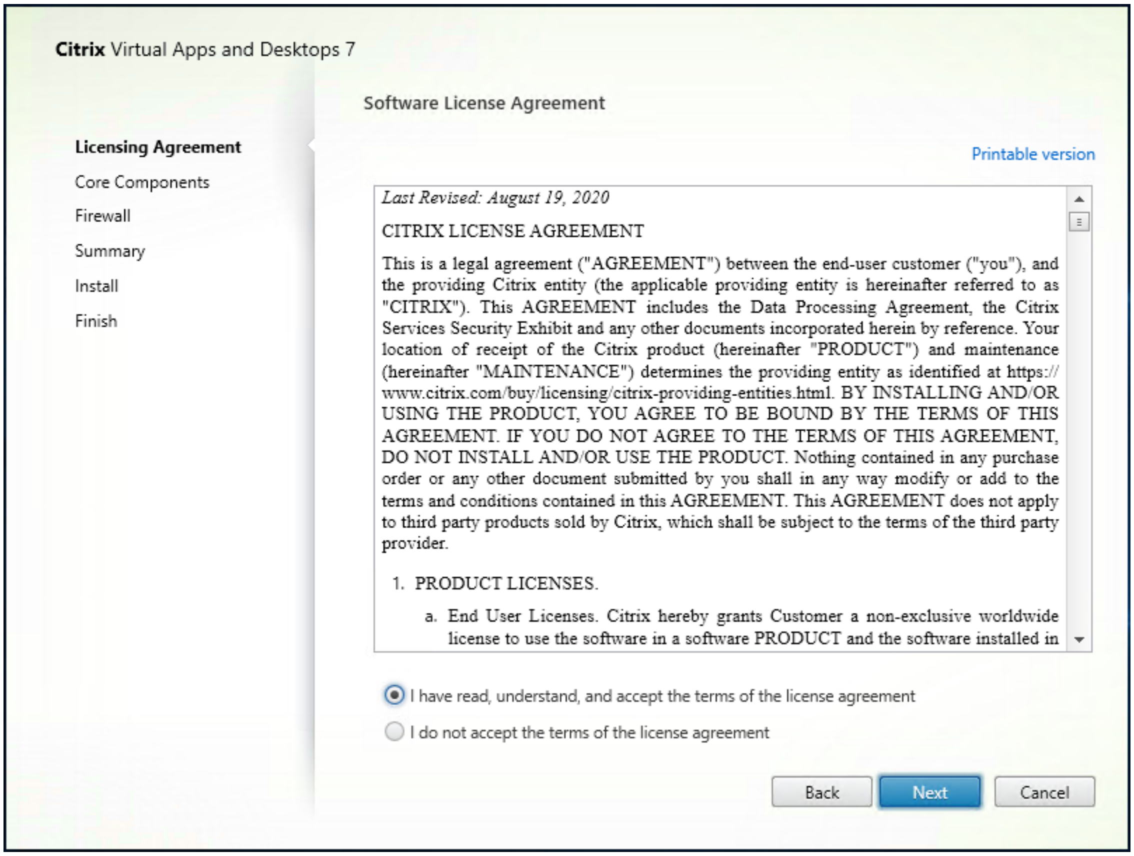
Start here. Select and install the Delivery Controller and other essential services like License Server.

Virtual Delivery Agent for Windows Multi-session OS

Install this agent to deliver applications and desktops from Windows multi-session OS virtual machines or physical machines.

Step 4. Read the Citrix License Agreement. 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.

Step 5. Click Next.



Software License Agreement

Last Revised: August 19, 2020

CITRIX LICENSE AGREEMENT

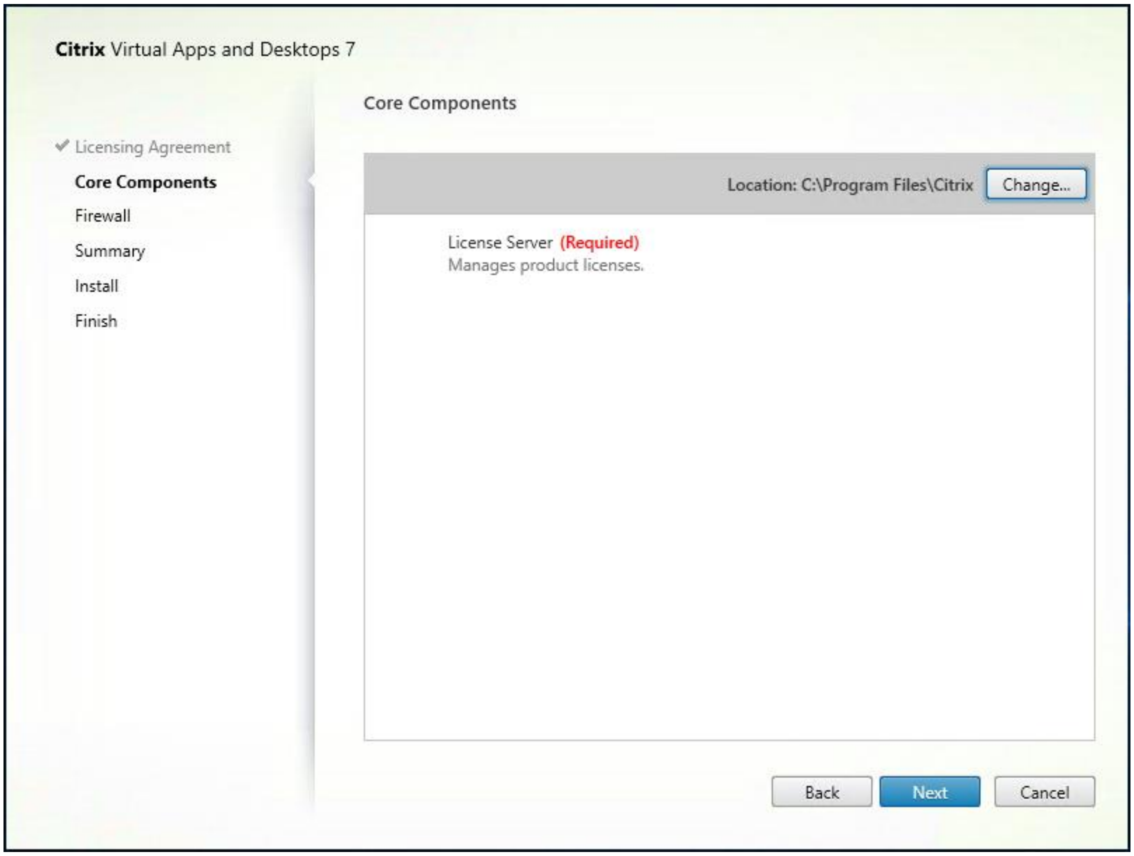
This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix-providing-entities.html. BY INSTALLING AND/OR USING THE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT. This AGREEMENT does not apply to third party products sold by Citrix, which shall be subject to the terms of the third party provider.

1. PRODUCT LICENSES.
   a. End User Licenses. Citrix hereby grants Customer a non-exclusive worldwide license to use the software in a software PRODUCT and the software installed in

● I have read, understand, and accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Step 6. Click Next.



Citrix Virtual Apps and Desktops 7

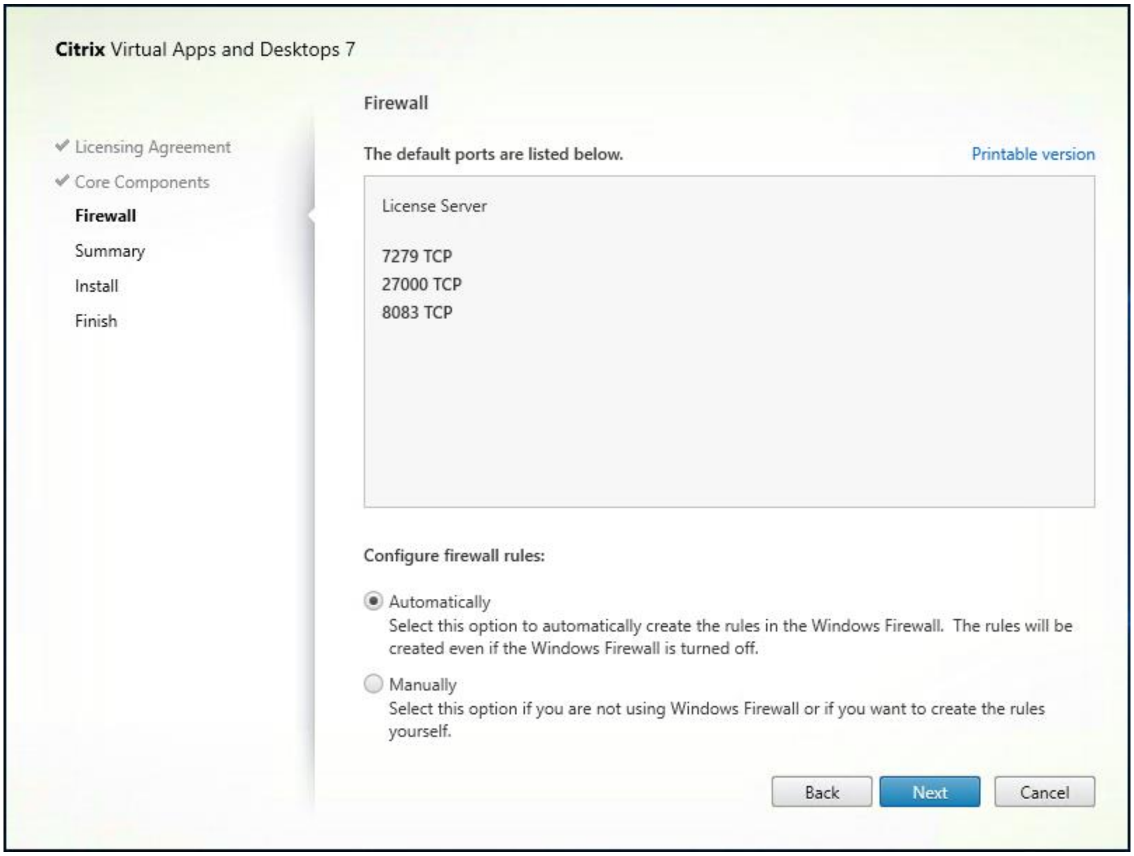
Core Components

Location: C:\Program Files\Citrix

License Server (Required)
Manages product licenses.

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

Step 8. Click Next.



Firewall

The default ports are listed below.

License Server

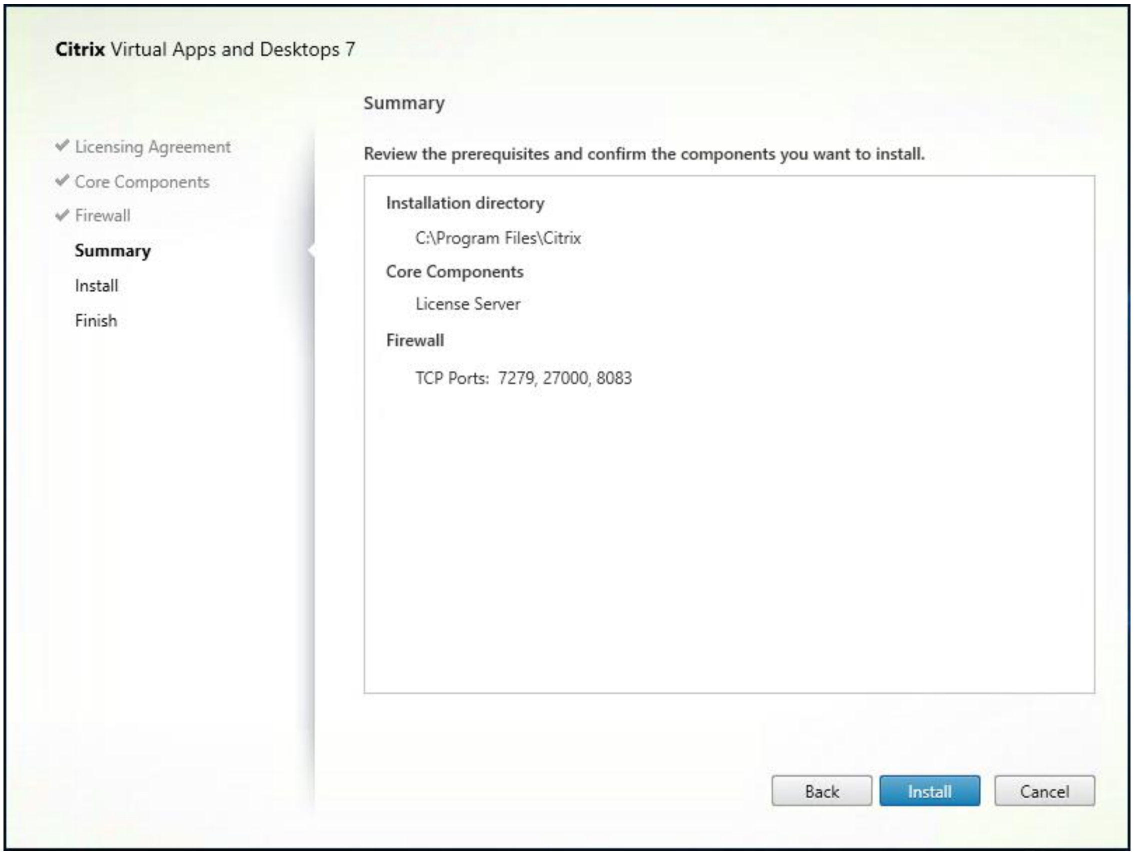
7279 TCP
27000 TCP
8083 TCP

Configure firewall rules:

● Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

○ Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

Step 9. Click Install.



Summary

Review the prerequisites and confirm the components you want to install.

Installation directory

C:\Program Files\Citrix

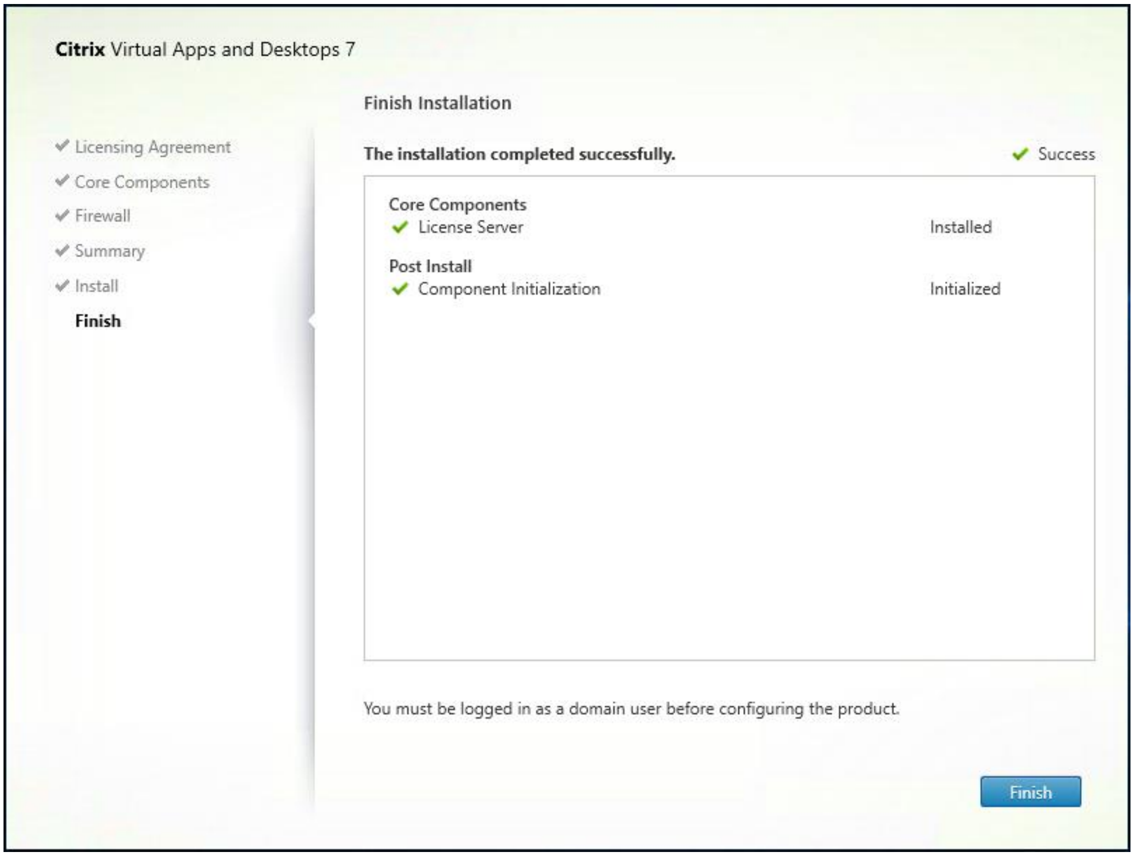
Core Components

License Server

Firewall

TCP Ports: 7279, 27000, 8083

Step 10. Click Finish to complete the installation.



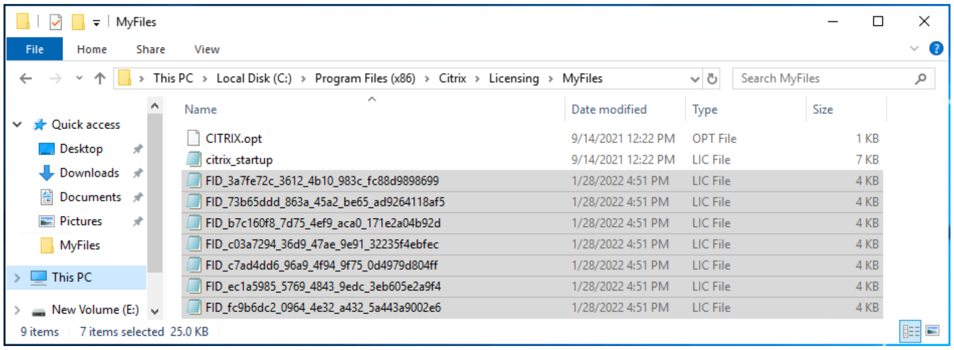
The installation completed successfully. ✓ Success

Core Components	
✓ License Server	Installed
Post Install	
✓ Component Initialization	Initialized

You must be logged in as a domain user before configuring the product.

Procedure 2. Install Citrix Licenses

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

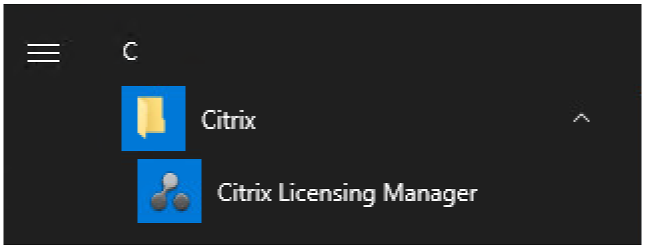


Name	Date modified	Type	Size
CITRIX.opt	9/14/2021 12:22 PM	OPT File	1 KB
citrix_startup	9/14/2021 12:22 PM	LIC File	7 KB
FID_3a7fe72c_3612_4b10_983c_fc88d9898699	1/28/2022 4:51 PM	LIC File	4 KB
FID_73b65ddd_863a_45a2_be65_ad9264118af5	1/28/2022 4:51 PM	LIC File	4 KB
FID_b7c160f8_7d75_4ef9_aca0_171e2a04b92d	1/28/2022 4:51 PM	LIC File	4 KB
FID_c03a7294_36d9_47ae_9e91_32235f4ebfec	1/28/2022 4:51 PM	LIC File	4 KB
FID_c7ad4dd6_96a9_4f94_9f75_0d4979d804ff	1/28/2022 4:51 PM	LIC File	4 KB
FID_ec1a5985_5769_4843_9edc_3eb605e2a9f4	1/28/2022 4:51 PM	LIC File	4 KB
FID_fc9b6dc2_0964_4e32_a432_5a443a9002e6	1/28/2022 4:51 PM	LIC File	4 KB

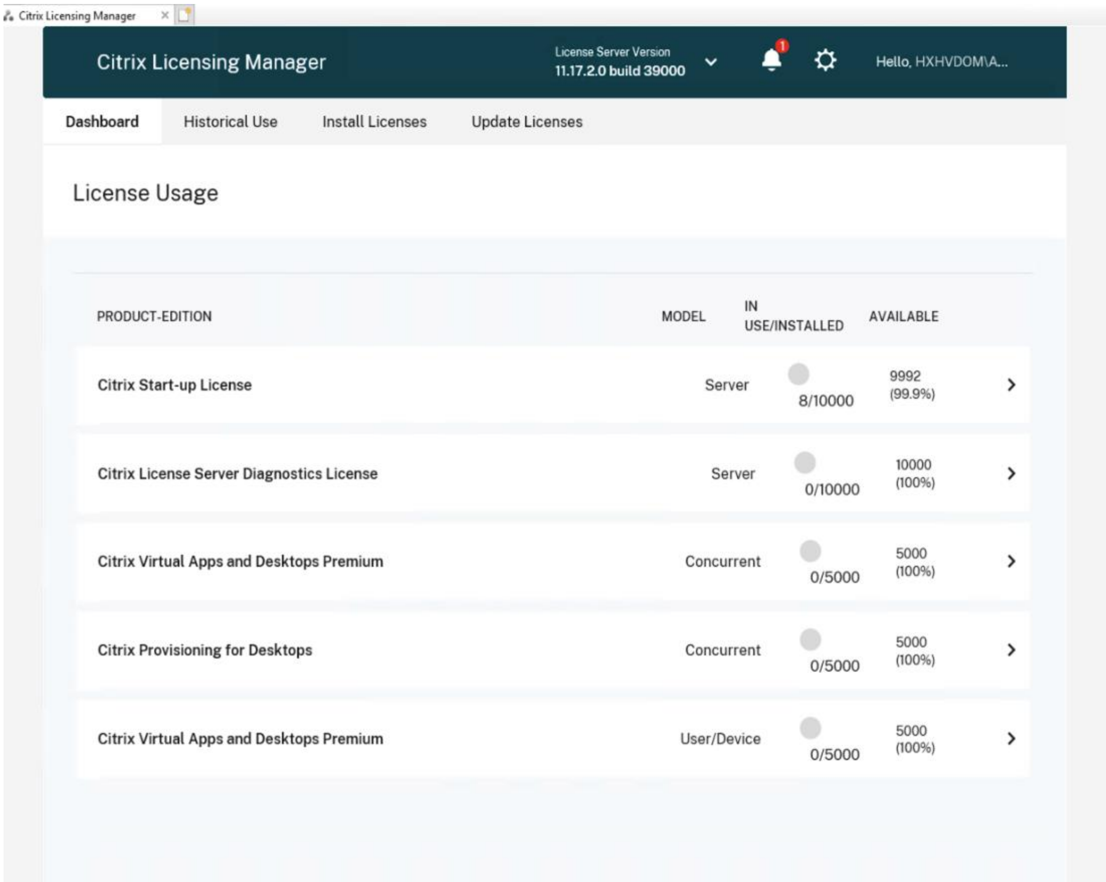
9 items 7 items selected 25.0 KB

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

Step 3. Run the application Citrix License Administration Console.



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



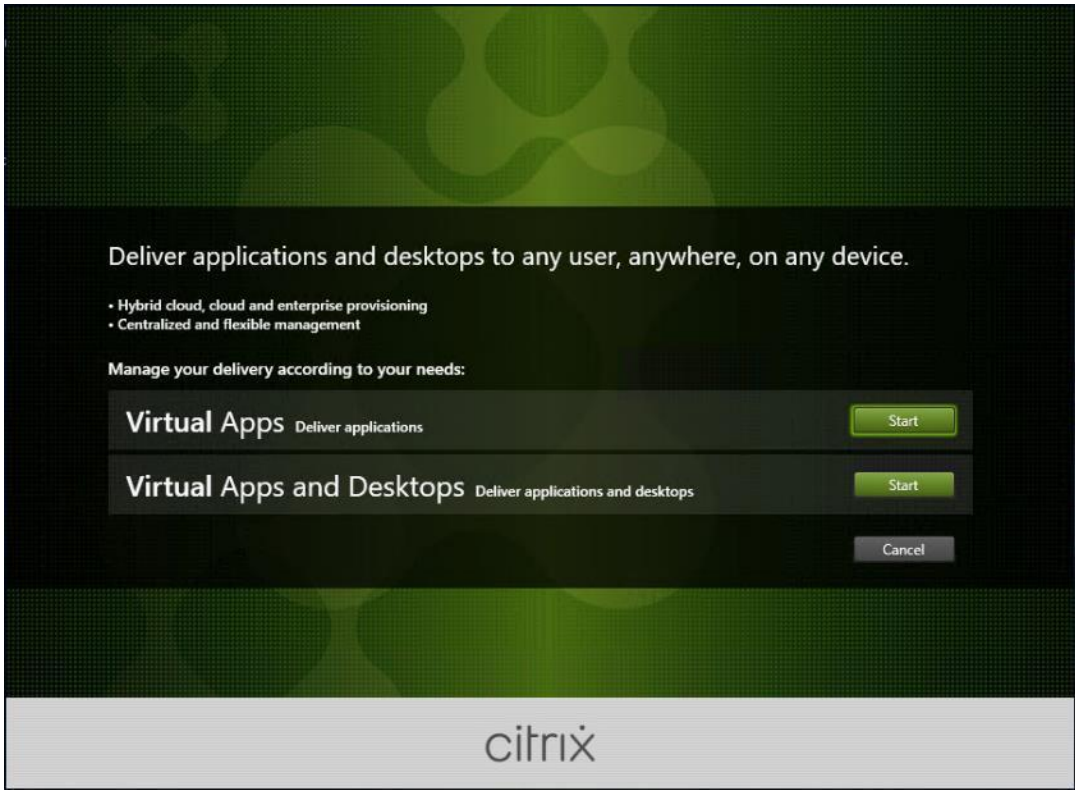
License Usage

PRODUCT-EDITION	MODEL	IN USE/INSTALLED	AVAILABLE
Citrix Start-up License	Server	8/10000	9992 (99.9%)
Citrix License Server Diagnostics License	Server	0/10000	10000 (100%)
Citrix Virtual Apps and Desktops Premium	Concurrent	0/5000	5000 (100%)
Citrix Provisioning for Desktops	Concurrent	0/5000	5000 (100%)
Citrix Virtual Apps and Desktops Premium	User/Device	0/5000	5000 (100%)

Procedure 3. Install the Citrix Virtual Apps and Desktops

Step 1. To begin the installation, connect to the first Delivery Controller server and launch the installer from the Citrix_Virtual_Apps_and_Desktops_7_2203 ISO.

Step 2. Click Start.



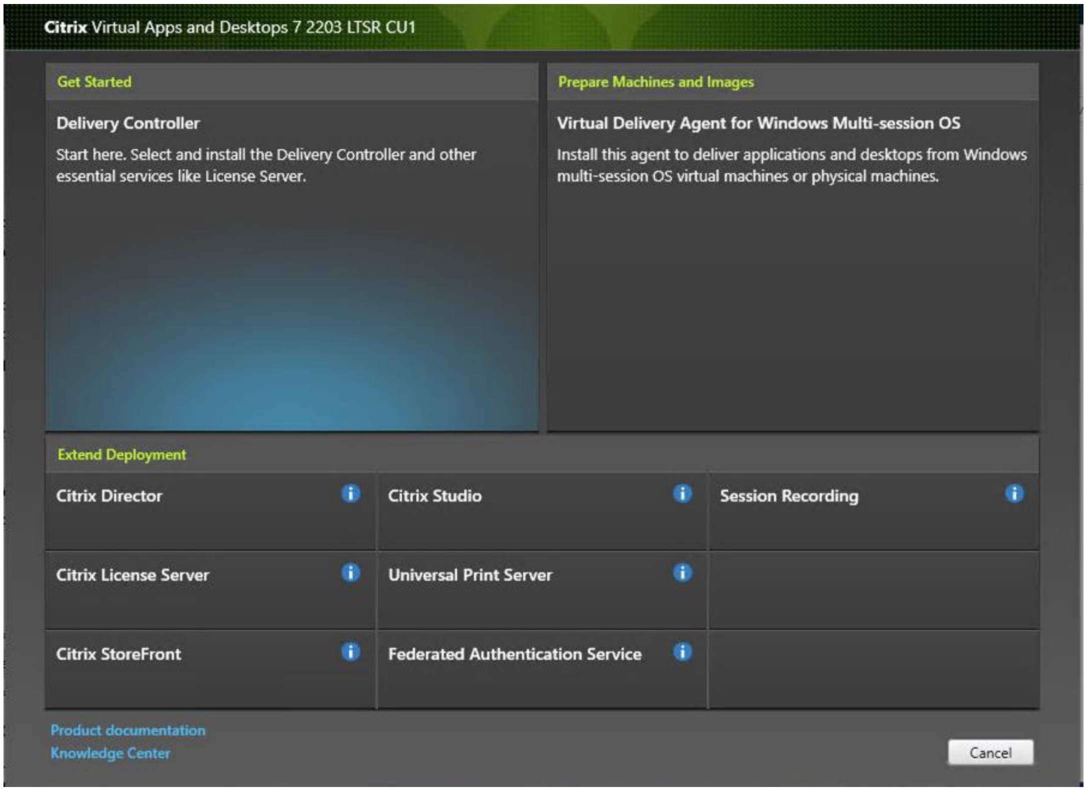
Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

Virtual Apps Deliver applications
Start
Virtual Apps and Desktops Deliver applications and desktops
Start
Cancel
citrix

Step 3. The installation wizard presents a menu with three subsections. Click Get Started - Delivery Controller.



Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

Get Started

Delivery Controller

Start here. Select and install the Delivery Controller and other essential services like License Server.

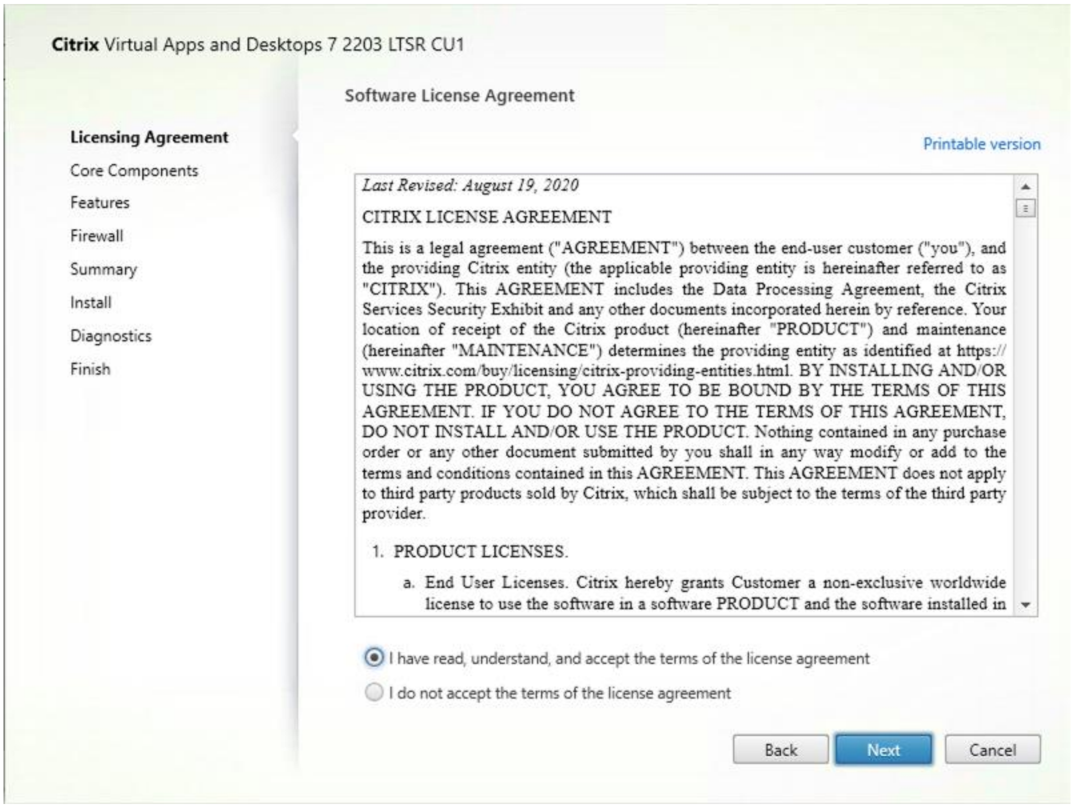
Prepare Machines and Images

Virtual Delivery Agent for Windows Multi-session OS

Install this agent to deliver applications and desktops from Windows multi-session OS virtual machines or physical machines.

Step 4. Read the Citrix License Agreement. 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.

Step 5. Click Next.



Software License Agreement

Last Revised: August 19, 2020

CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix-providing-entities.html. BY INSTALLING AND/OR USING THE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT. This AGREEMENT does not apply to third party products sold by Citrix, which shall be subject to the terms of the third party provider.

1. PRODUCT LICENSES.
   a. End User Licenses. Citrix hereby grants Customer a non-exclusive worldwide license to use the software in a software PRODUCT and the software installed in

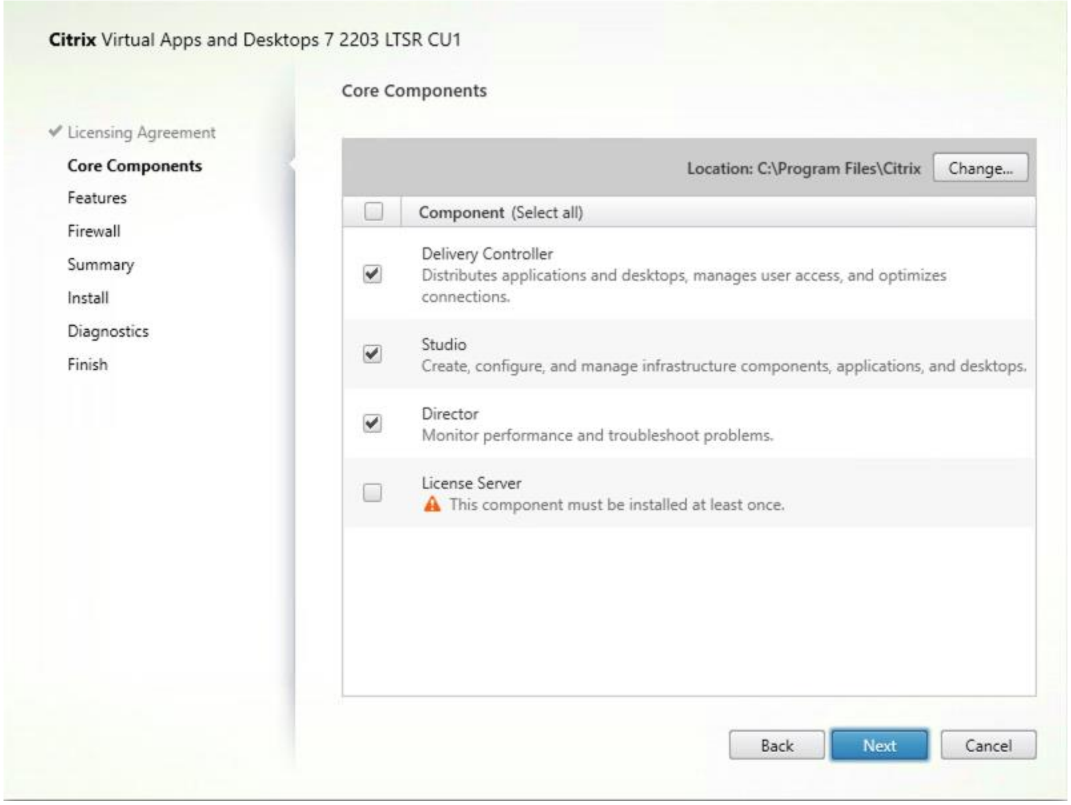
● I have read, understand, and accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Step 6. Select the components to be installed on the first Delivery Controller Server:

- Delivery Controller
- Studio
- Director

Step 7. Click Next.



Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

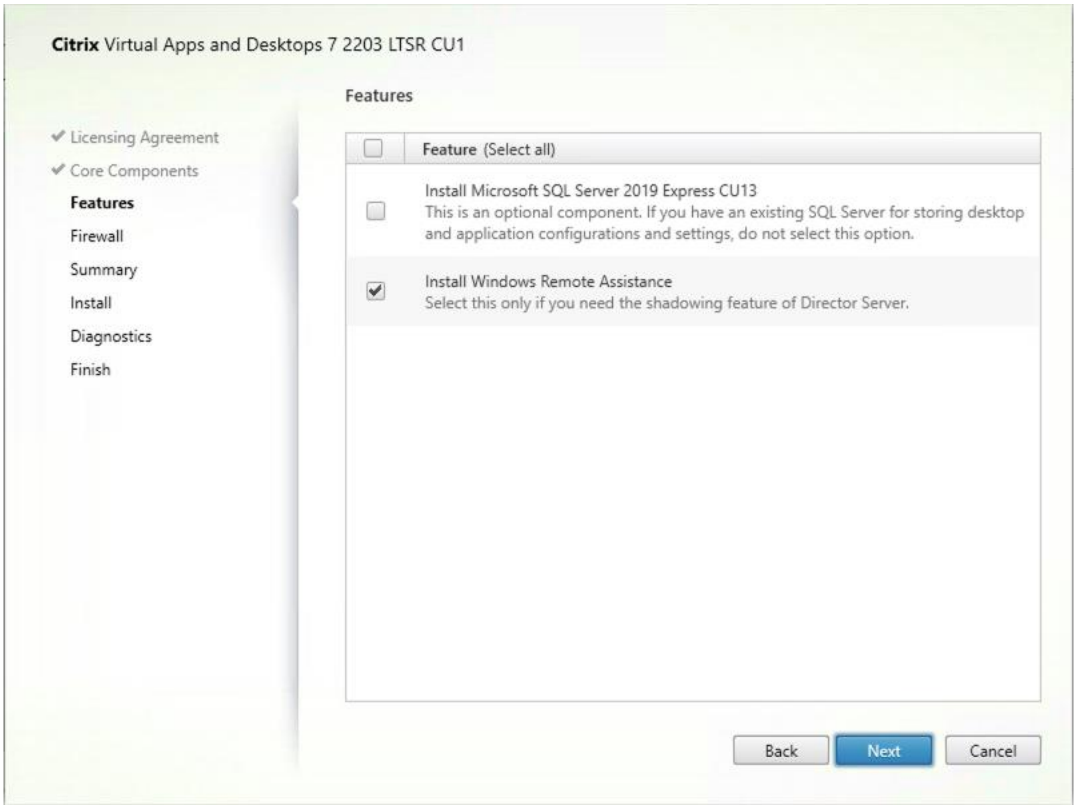
Core Components

Location: C:\Program Files\Citrix

	Component (Select all)
☑	Delivery Controller Distributes applications and desktops, manages user access, and optimizes connections.
☑	Studio Create, configure, and manage infrastructure components, applications, and desktops.
☑	Director Monitor performance and troubleshoot problems.
□	License Server ⚠ This component must be installed at least once.

Step 8. Since a dedicated SQL Server will be used to Store the Database, leave "Install Microsoft SQL Server 2014 SP2 Express" unchecked.

Step 9. Click Next.



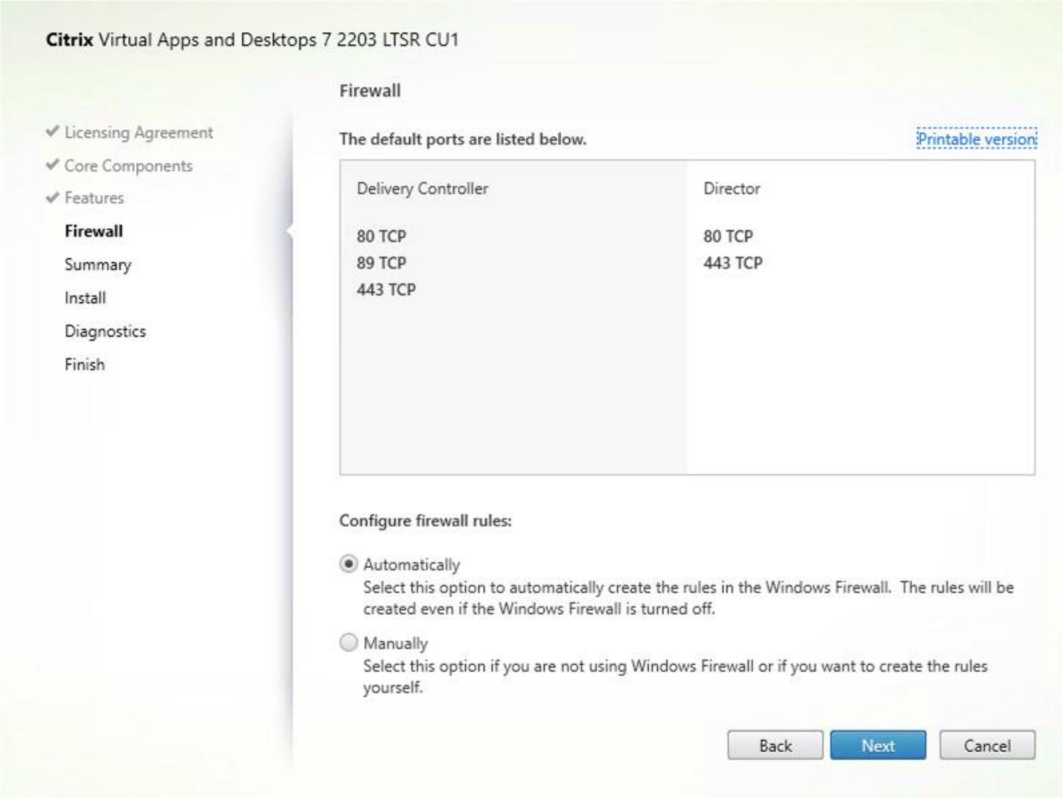
Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

Features

	Feature (Select all)
□	Install Microsoft SQL Server 2019 Express CU13 This is an optional component. If you have an existing SQL Server for storing desktop and application configurations and settings, do not select this option.
☑	Install Windows Remote Assistance Select this only if you need the shadowing feature of Director Server.

Step 10. Select the default ports and automatically configured firewall rules.

Step 11. Click Next.



Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

Firewall

The default ports are listed below.

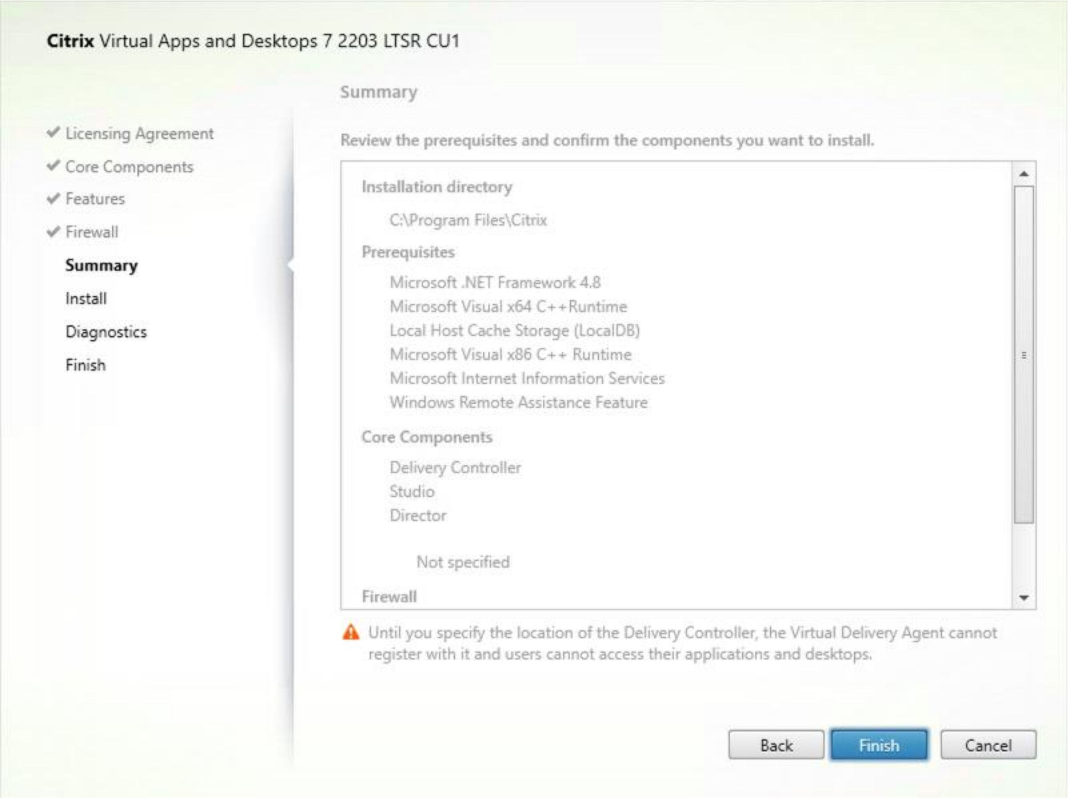
Delivery Controller	Director
80 TCP	80 TCP
89 TCP	443 TCP
443 TCP	

Configure firewall rules:

● Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

○ Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

Step 12. Click Finish to begin the installation.



Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

Summary

Review the prerequisites and confirm the components you want to install.

Installation directory

C:\Program Files\Citrix

Prerequisites

Microsoft .NET Framework 4.8
Microsoft Visual x64 C++Runtime
Local Host Cache Storage (LocalDB)
Microsoft Visual x86 C++ Runtime
Microsoft Internet Information Services
Windows Remote Assistance Feature

Core Components

Delivery Controller
Studio
Director

Not specified

Firewall

⚠ Until you specify the location of the Delivery Controller, the Virtual Delivery Agent cannot register with it and users cannot access their applications and desktops.

Note: Multiple reboots may be required to finish installation.

Step 13. (Optional) Collect diagnostic information/Call Home participation.

Step 14. Click Next.

Step 15. Click Finish to complete the installation.

Step 16. (Optional) Check Launch Studio to launch Citrix Studio Console.

Procedure 4. Additional Delivery Controller Configuration

Note: 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 Delivery Controllers, repeat the steps in section Install the Citrix Virtual Apps and Desktops.

Step 1. To begin the installation of the second Delivery Controller, connect to the second Delivery Controller server and launch the installer from the Citrix_Virtual_Apps_and_Desktops_7_2203 ISO.

Step 2. Click Start.

Step 3. Click Delivery Controller.

Step 4. Repeat the same steps used to install the first Delivery Controller; Install the Citrix Virtual Apps and Desktops, including the step of importing an SSL certificate for HTTPS between the controller and vSphere.

Step 5. Review the Summary configuration. Click Finish.

Step 6. (Optional) Configure Collect diagnostic information /Call Home participation. Click Next.

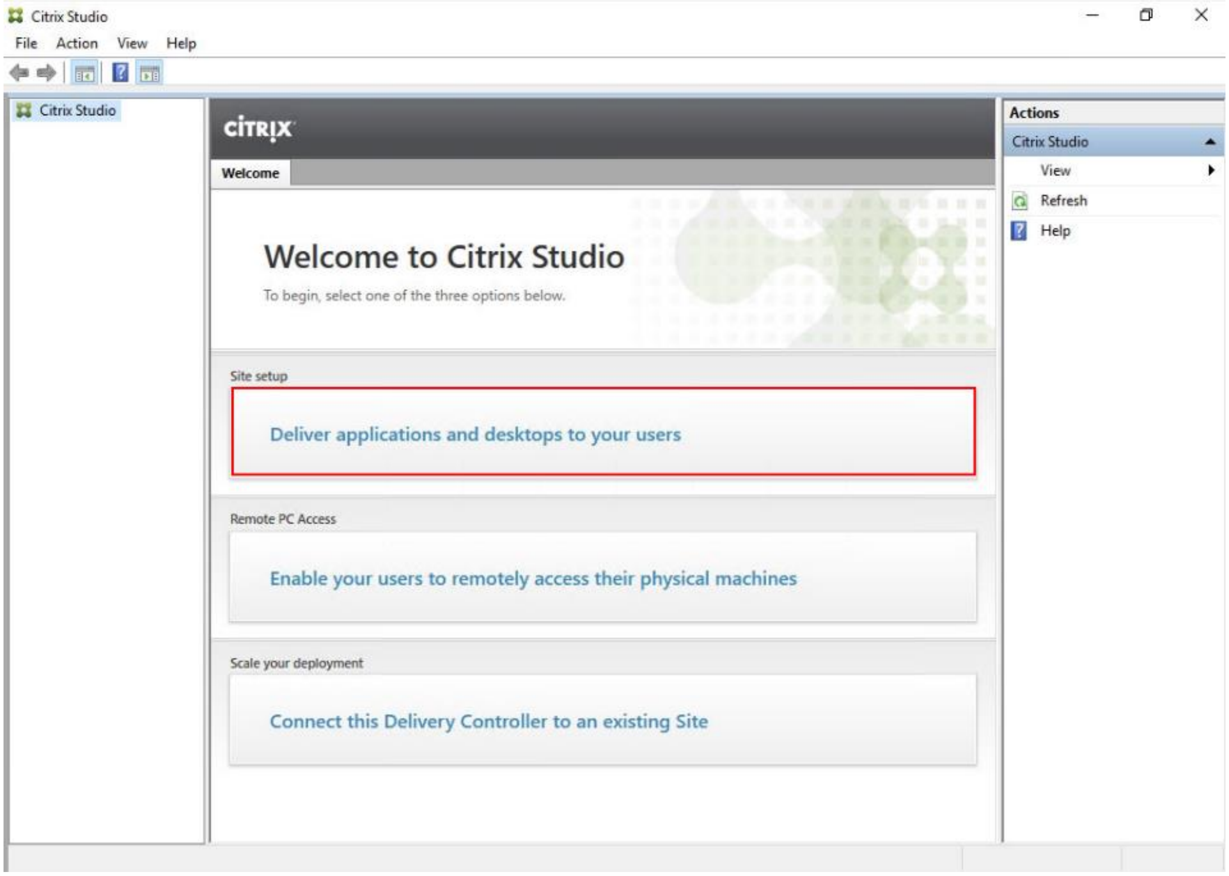
Step 7. Verify the components installed successfully. Click Finish.

Procedure 5. Create 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 Delivery Controller installation, or if necessary, it can be launched manually. Studio is used to create a Site, which is the core of the Citrix Virtual Apps and Desktops environment consisting of the Delivery Controller and the Database.

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



Welcome to Citrix Studio

To begin, select one of the three options below.

Site setup

Deliver applications and desktops to your users

Remote PC Access

Enable your users to remotely access their physical machines

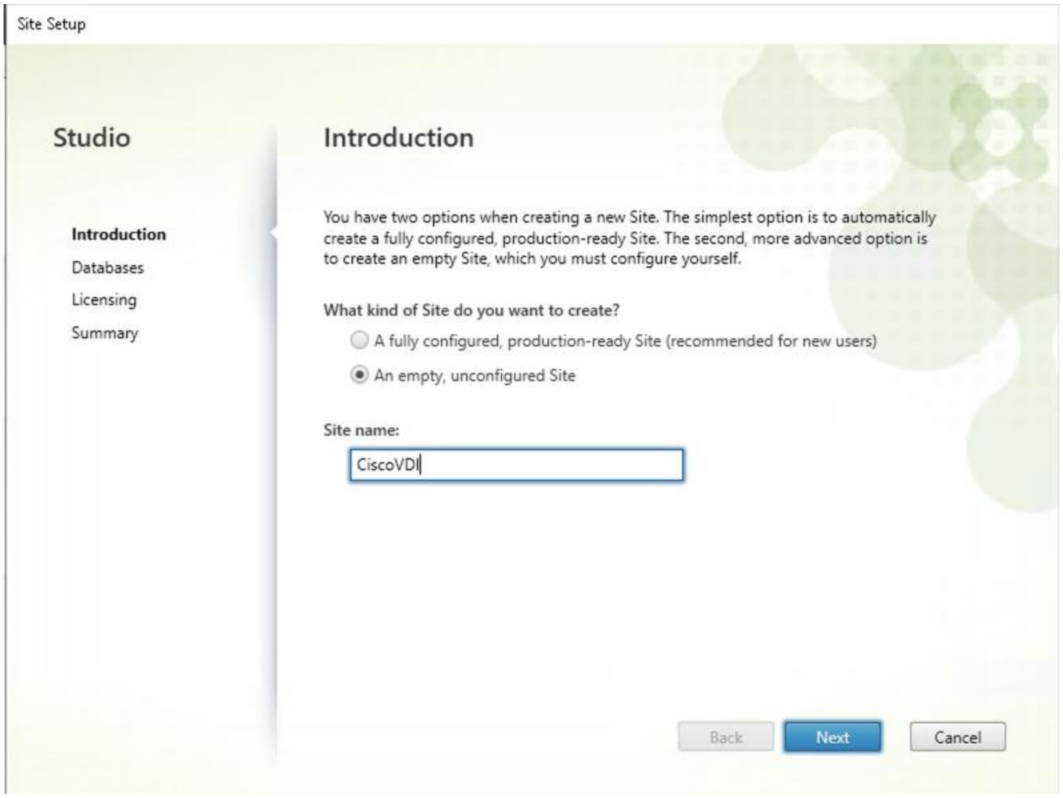
Scale your deployment

Connect this Delivery Controller to an existing Site

Step 2. Select the “An empty, unconfigured Site” radio button.

Step 3. Enter a site name.

Step 4. Click Next.



Introduction

You have two options when creating a new Site. The simplest option is to automatically create a fully configured, production-ready Site. The second, more advanced option is to create an empty Site, which you must configure yourself.

What kind of Site do you want to create?

○ A fully configured, production-ready Site (recommended for new users)

● An empty, unconfigured Site

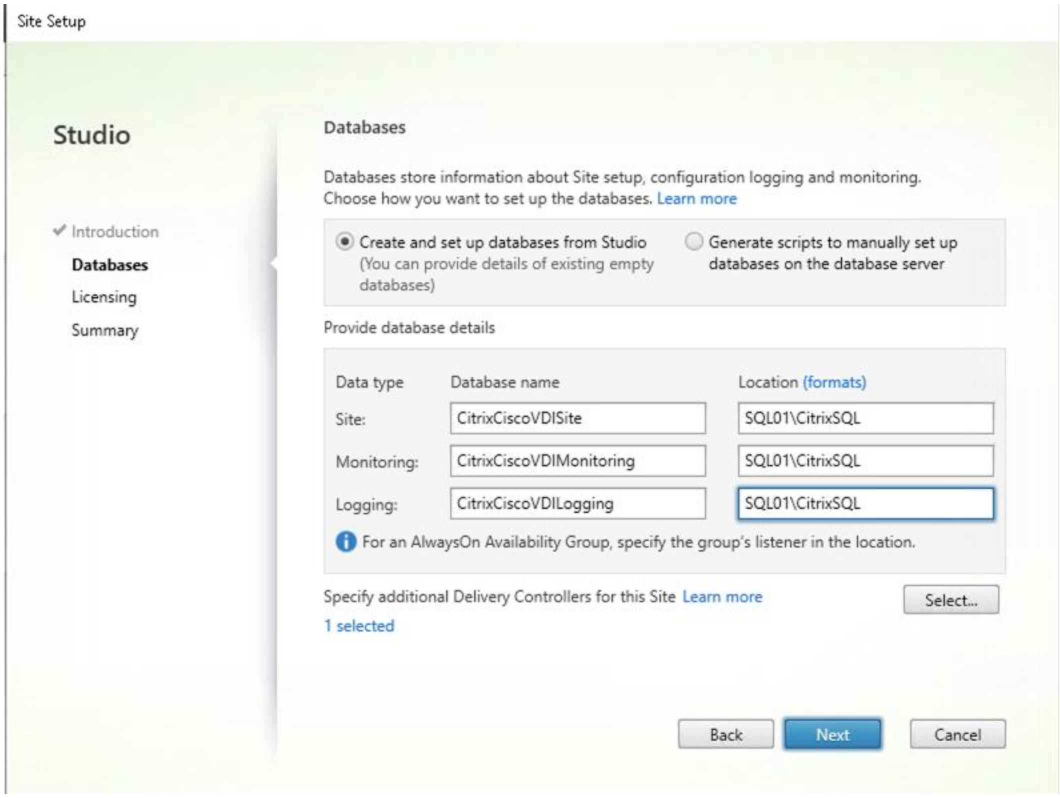
Site name: CiscoVDI

Step 5. Provide the Database Server Locations for each data type.

Note: For an SQL AlwaysOn Availability Group, use the group's listener DNS name.

Step 6. Click Select to specify additional controllers (Optional at this time. Additional controllers can be added later).

Step 7. Click Next.



Databases

Databases store information about Site setup, configuration logging and monitoring. Choose how you want to set up the databases. Learn more

● Create and set up databases from Studio (You can provide details of existing empty databases)

○ Generate scripts to manually set up databases on the database server

Provide database details

Data type	Database name	Location (formats)
Site:	CitrixCiscoVDISite	SQL01\CitrixSQL
Monitoring:	CitrixCiscoVDIMonitoring	SQL01\CitrixSQL
Logging:	CitrixCiscoVDILogging	SQL01\CitrixSQL

For an AlwaysOn Availability Group, specify the group's listener in the location.

Specify additional Delivery Controllers for this Site Learn more

1 selected

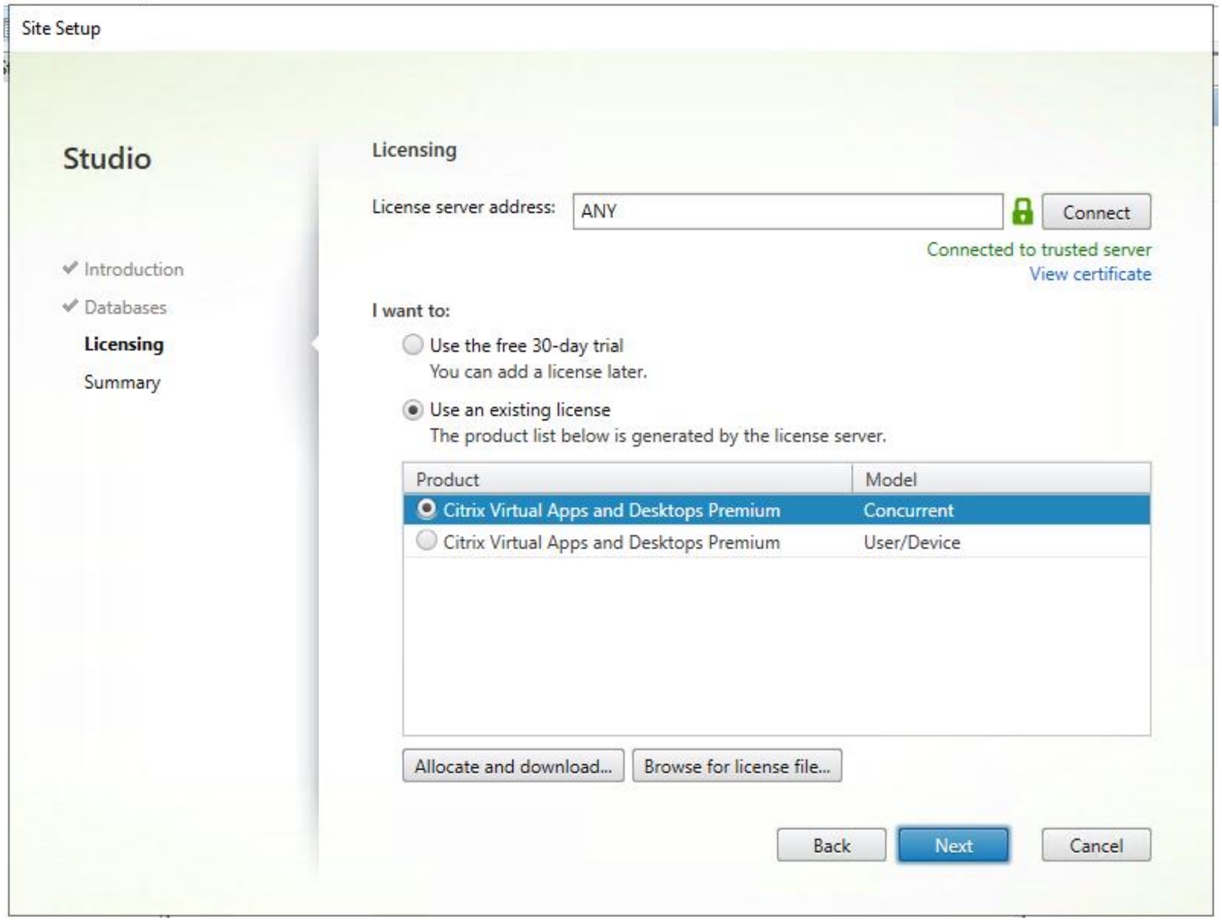
Step 8. Provide the FQDN of the license server.

Step 9. Click Connect to validate and retrieve any licenses from the server.

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

Step 10. Select the appropriate product edition using the license radio button.

Step 11. Click Next.



Site Setup

Studio

Licensing

License server address: ANY

Connected to trusted server

I want to:

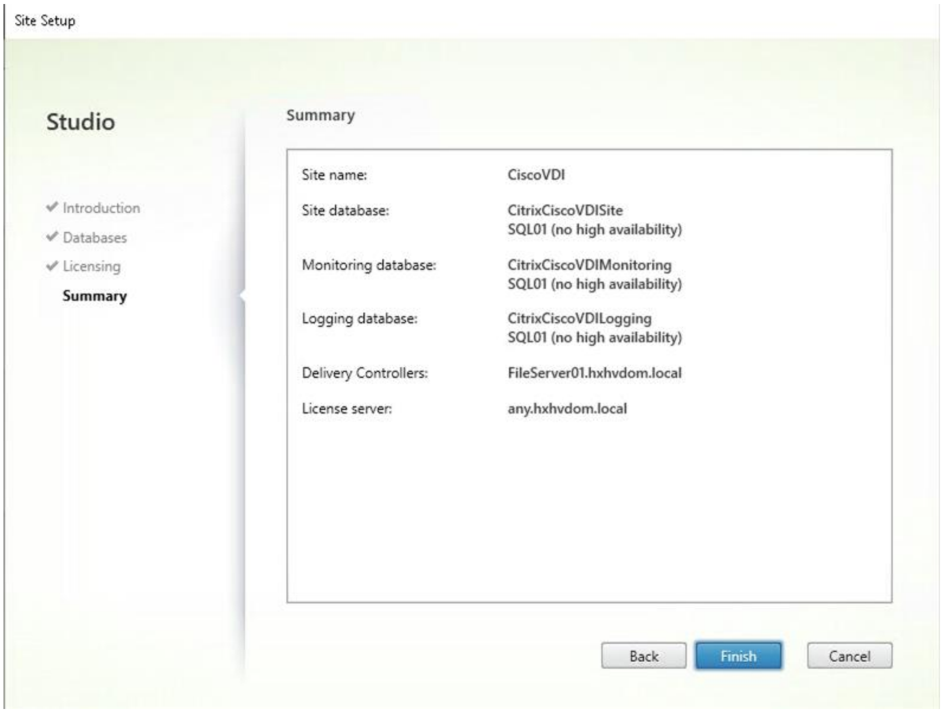
○ Use the free 30-day trial
You can add a license later.

● Use an existing license
The product list below is generated by the license server.

Product	Model
● Citrix Virtual Apps and Desktops Premium	Concurrent
○ Citrix Virtual Apps and Desktops Premium	User/Device

Step 12. Verify information on the Summary page.

Step 13. Click Finish.



Site Setup

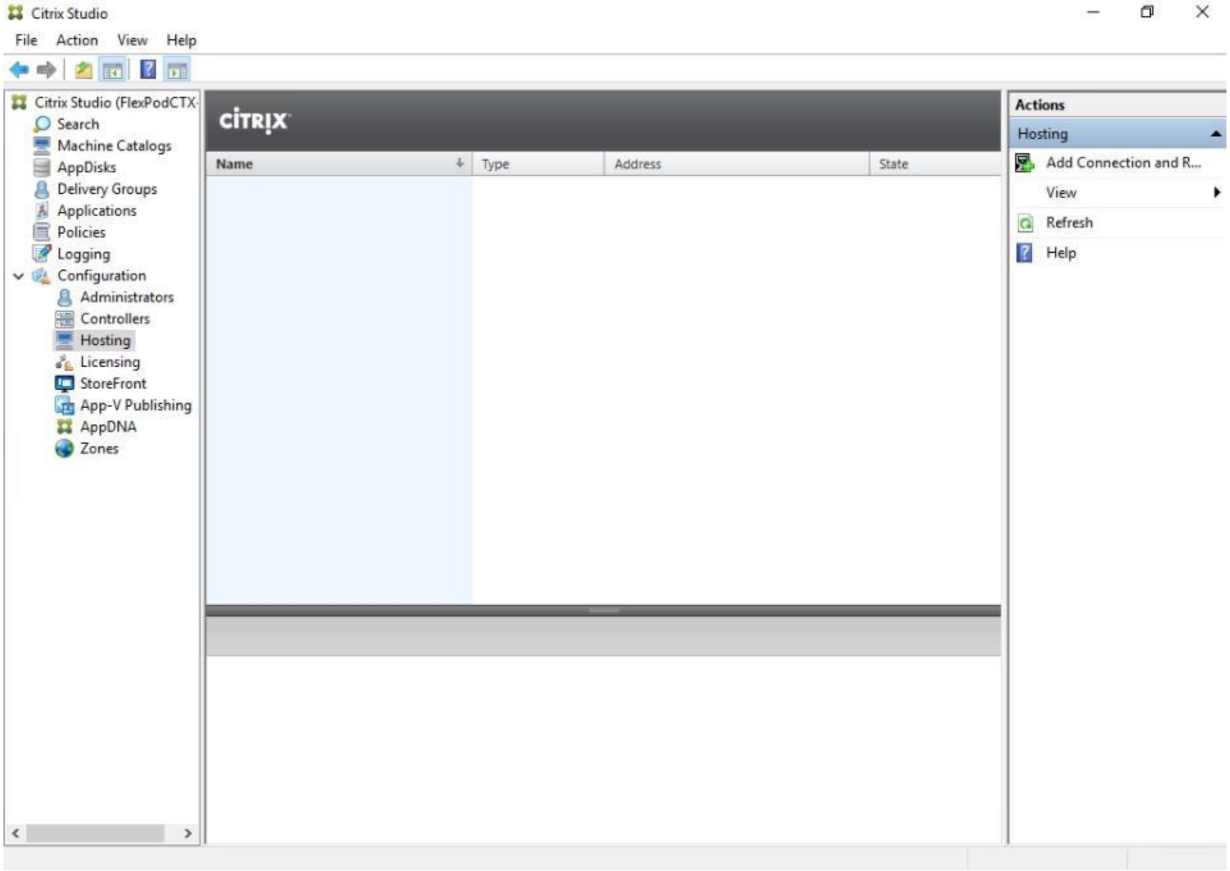
Studio

Summary

Site name:	CiscoVDI
Site database:	CitrixCiscoVDISite SQL01 (no high availability)
Monitoring database:	CitrixCiscoVDIMonitoring SQL01 (no high availability)
Logging database:	CitrixCiscoVDILogging SQL01 (no high availability)
Delivery Controllers:	FileServer01.hxhvdom.local
License server:	any.hxhvdom.local

Procedure 6. Configure the Citrix Virtual Apps and Desktops Site Hosting Connection

Step 1. From Configuration > Hosting in Studio, click Add Connection and Resources in the right pane.



Step 2. On the Connection page:

a. Select the Connection type of VMware vSphere.

b. Enter the FQDN of the vCenter server (in Server_FQDN/sdk format).

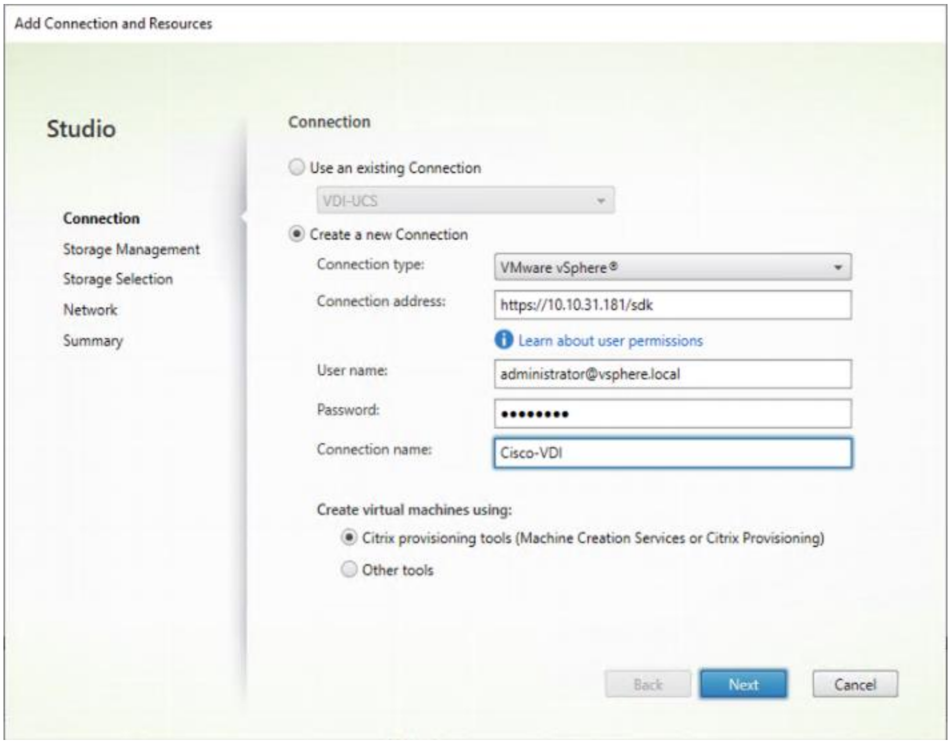
c. Enter the username (in domain\username format) for the vSphere account.

d. Provide the password for the vSphere account.

e. Provide a connection name.

f. Choose the tool to create virtual machines: Machine Creation Services or Citrix Provisioning

Step 3. Click Next.



Add Connection and Resources

Studio

Connection

○ Use an existing Connection

VDI-UCS

● Create a new Connection

Connection type: VMware vSphere®

Connection address: https://10.10.31.181/sdk

Learn about user permissions

User name: administrator@vsphere.local

Password: ••••••••

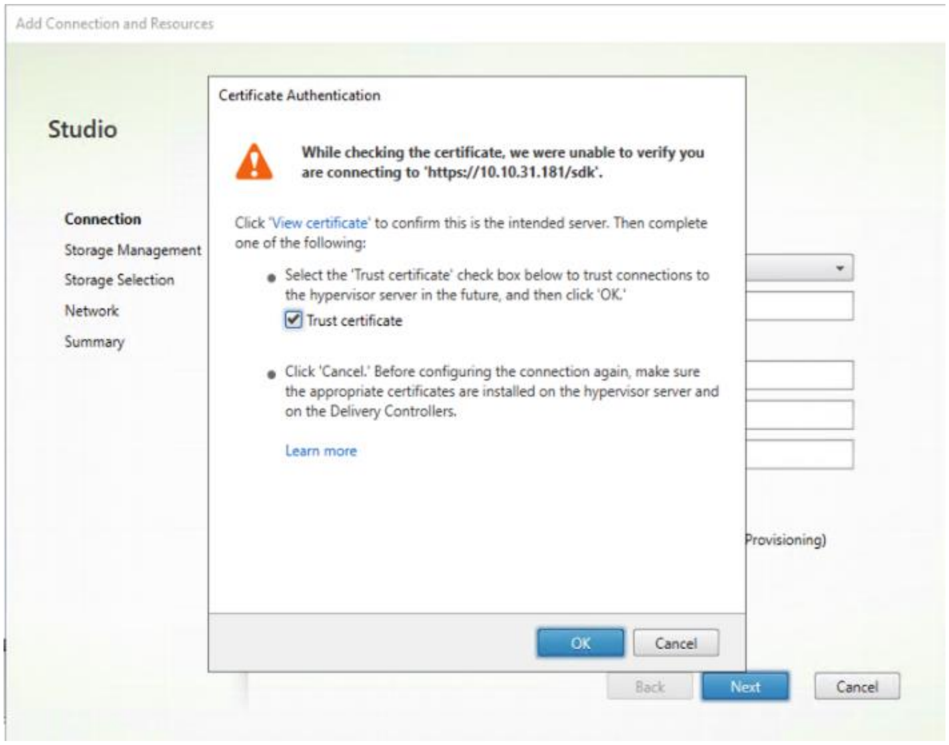
Connection name: Cisco-VDI

Create virtual machines using:

● Citrix provisioning tools (Machine Creation Services or Citrix Provisioning)

○ Other tools

Step 4. Accept the certificate and click OK to trust the hypervisor connection.



Add Connection and Resources

Studio

Certificate Authentication

While checking the certificate, we were unable to verify you are connecting to 'https://10.10.31.181/sdk'.

Click 'View certificate' to confirm this is the intended server. Then complete one of the following:

- Select the 'Trust certificate' check box below to trust connections to the hypervisor server in the future, and then click 'OK.'

  ☑ Trust certificate

- Click 'Cancel.' Before configuring the connection again, make sure the appropriate certificates are installed on the hypervisor server and on the Delivery Controllers.

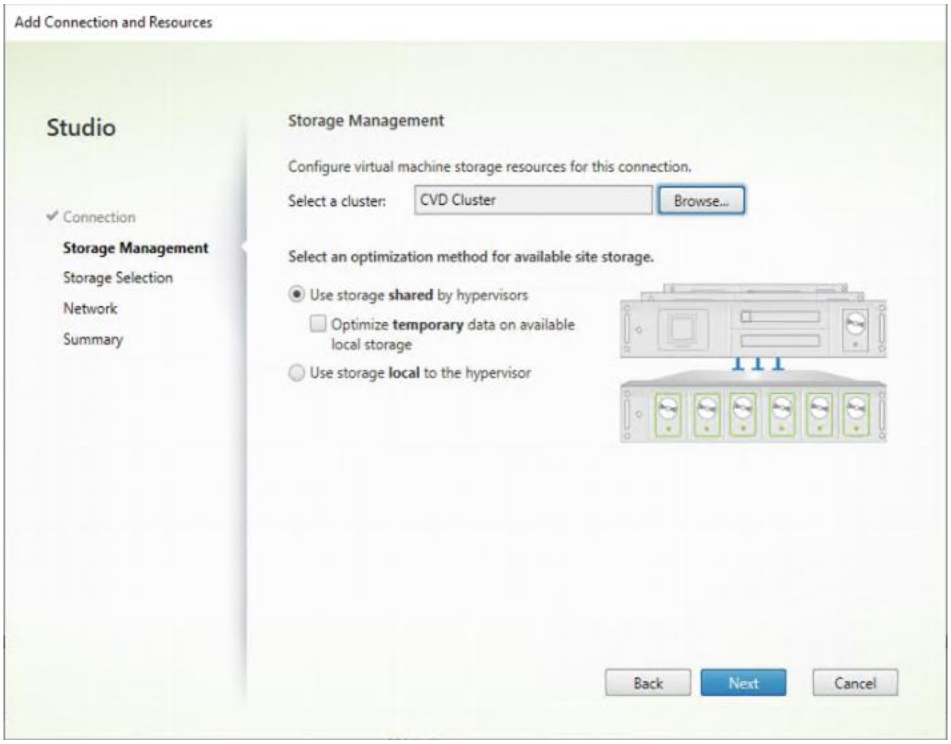
  Learn more

Step 5. Select a storage management method:

Step 6. Select Cluster that will be used by this connection.

Step 7. Check Use storage shared by hypervisors radio button.

Step 8. Click Next.



Storage Management

Configure virtual machine storage resources for this connection.

Select a cluster: CVD Cluster

Select an optimization method for available site storage.

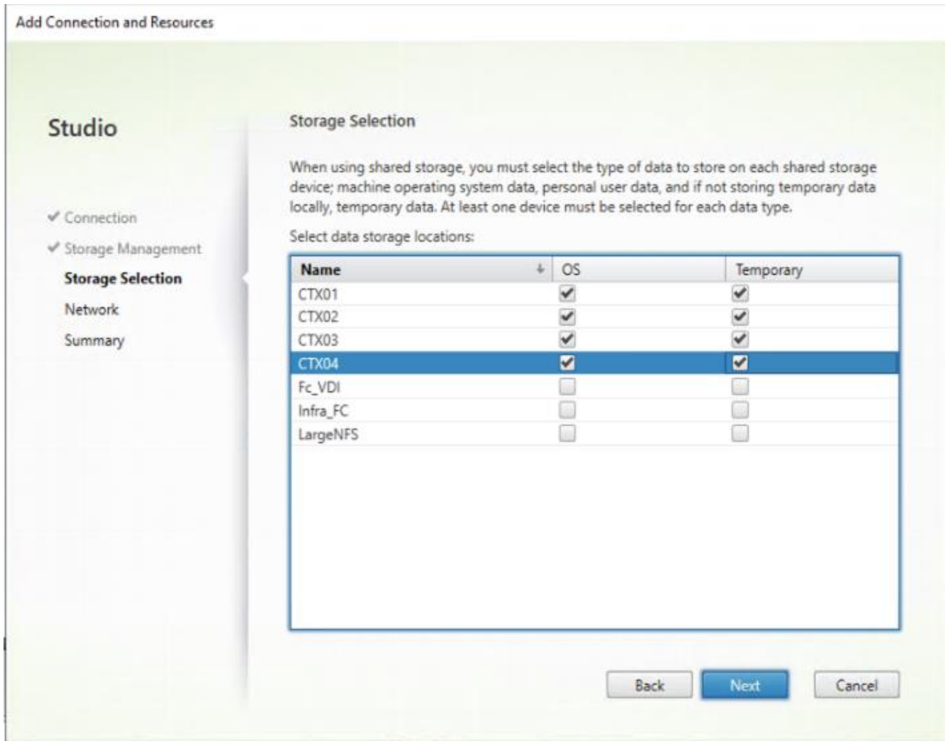
● Use storage **shared** by hypervisors

□ Optimize **temporary** data on available local storage

○ Use storage **local** to the hypervisor

Step 9. Select the Storage to be used by this connection, use all provisioned for desktops datastores.

Step 10. Click Next.



Storage Selection

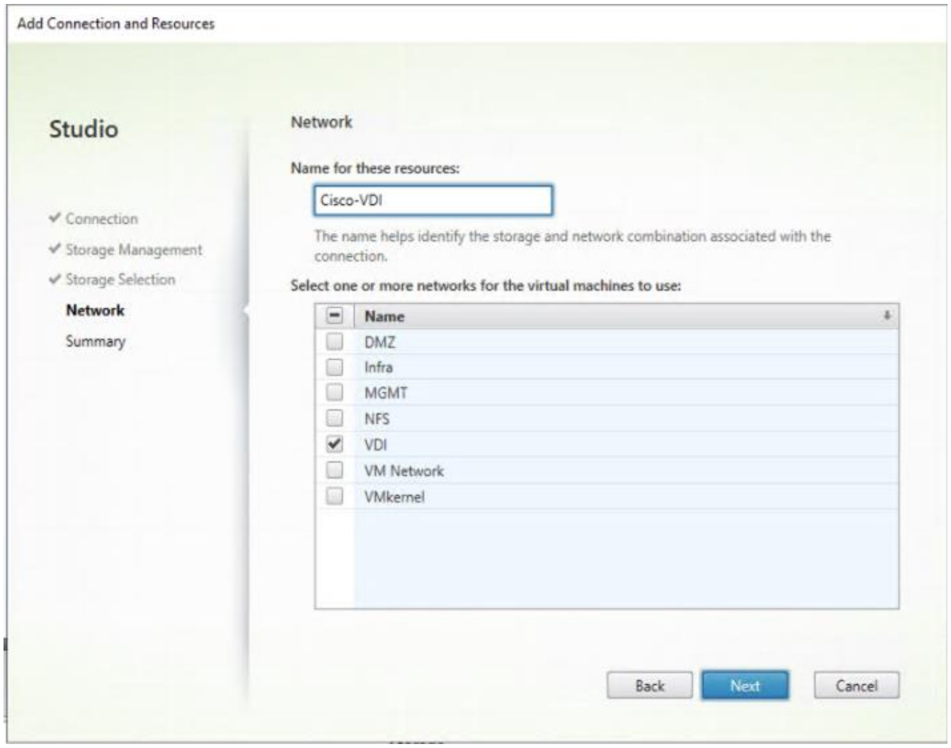
When using shared storage, you must select the type of data to store on each shared storage device; machine operating system data, personal user data, and if not storing temporary data locally, temporary data. At least one device must be selected for each data type.

Select data storage locations:

Name	OS	Temporary
CTX01	☑	☑
CTX02	☑	☑
CTX03	☑	☑
CTX04	☑	☑
Fc_VDI	□	□
Infra_FC	□	□
LargeNFS	□	□

Step 11. Select the Network to be used by this connection.

Step 12. Click Next.



Network

Name for these resources: Cisco-VDI

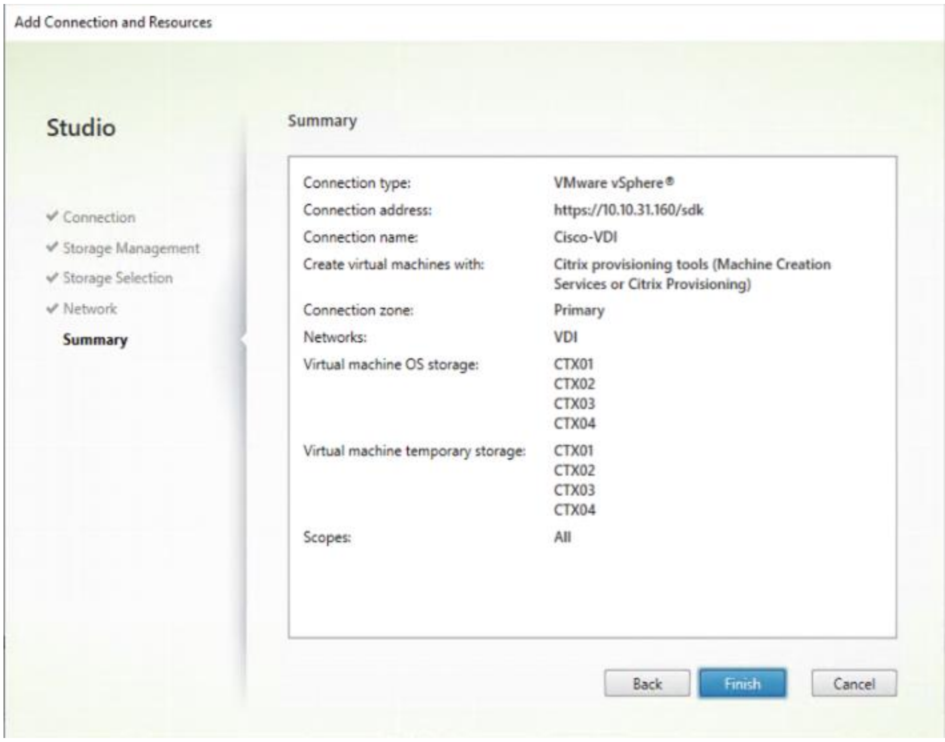
The name helps identify the storage and network combination associated with the connection.

Select one or more networks for the virtual machines to use:

☐	Name
☐	DMZ
☐	Infra
☐	MGMT
☐	NFS
☑	VDI
☐	VM Network
☐	VMkernel

Step 13. Review Add Connection and Recourses Summary.

Step 14. Click Finish.



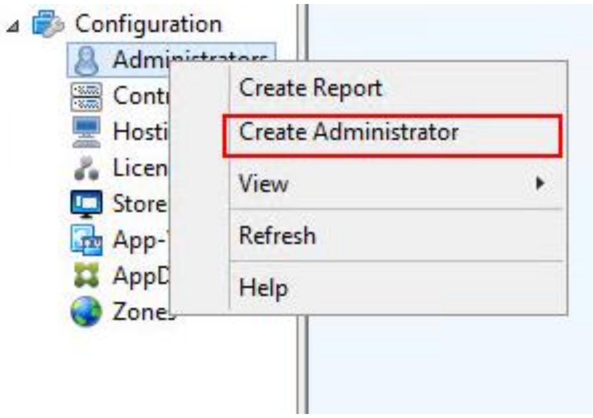
Summary

Connection type:	VMware vSphere®
Connection address:	https://10.10.31.160/sdk
Connection name:	Cisco-VDI
Create virtual machines with:	Citrix provisioning tools (Machine Creation Services or Citrix Provisioning)
Connection zone:	Primary
Networks:	VDI
Virtual machine OS storage:	CTX01 CTX02 CTX03 CTX04
Virtual machine temporary storage:	CTX01 CTX02 CTX03 CTX04
Scopes:	All

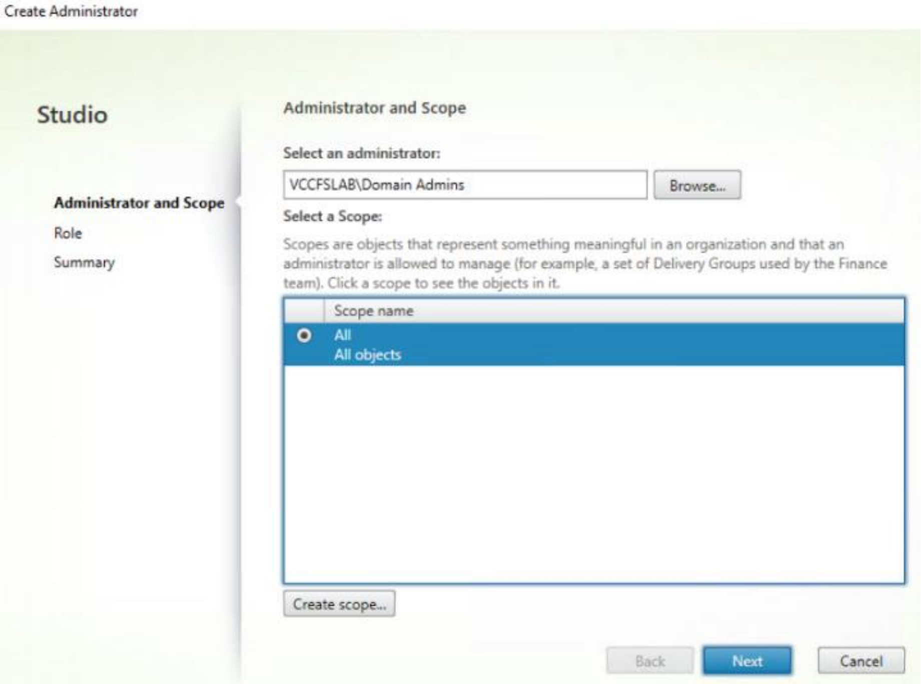
Procedure 7. Configure the Citrix Virtual Apps and Desktops Site Administrators

Step 1. Connect to the Citrix Virtual Apps and Desktops server and open Citrix Studio Management console.

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



Step 3. Select or Create appropriate scope and click Next.



Administrator and Scope

Select an administrator:

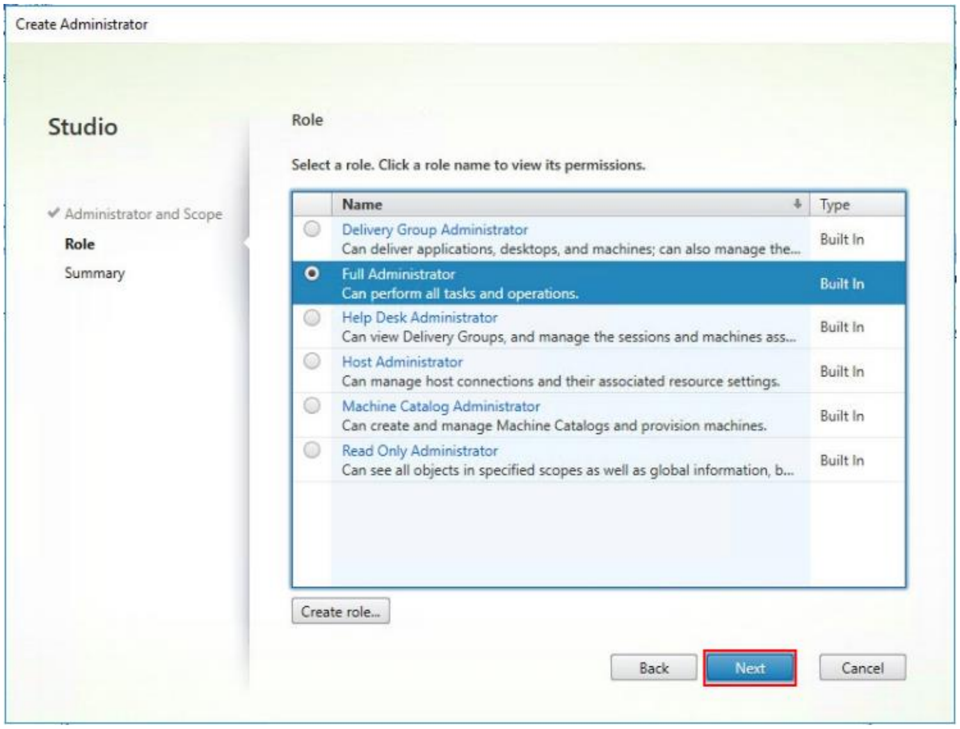
VCCFSLAB\Domain Admins

Select a Scope:

Scopes are objects that represent something meaningful in an organization and that an administrator is allowed to manage (for example, a set of Delivery Groups used by the Finance team). Click a scope to see the objects in it.

	Scope name
●	All All objects

Step 4. Select an appropriate Role.


Create Administrator

Studio

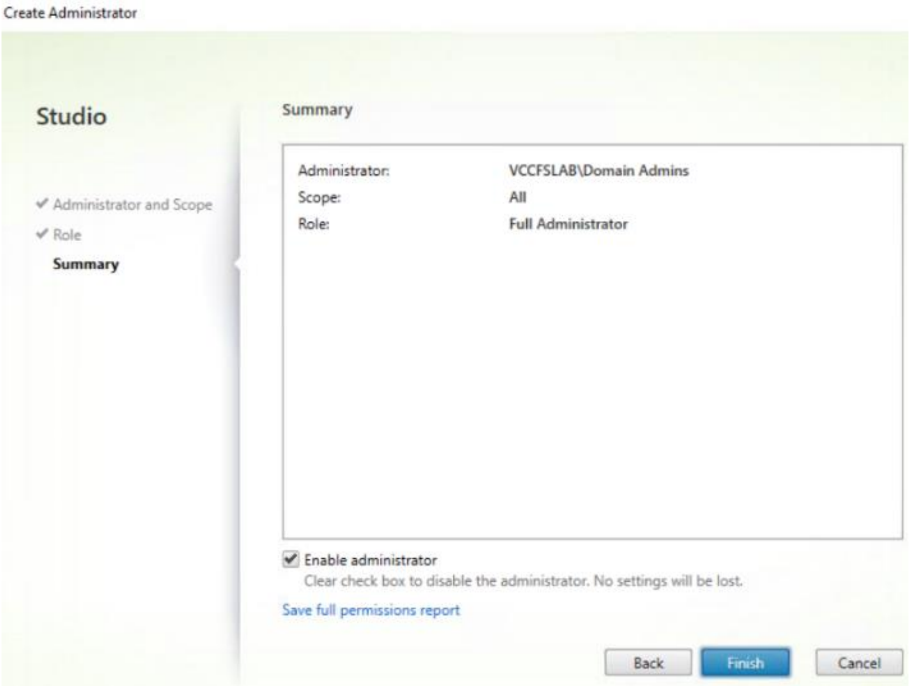
✓ Administrator and Scope
Role
Summary

Role

Select a role. Click a role name to view its permissions.

	Name	Type
○	Delivery Group Administrator Can deliver applications, desktops, and machines; can also manage the...	Built In
●	Full Administrator Can perform all tasks and operations.	Built In
○	Help Desk Administrator Can view Delivery Groups, and manage the sessions and machines ass...	Built In
○	Host Administrator Can manage host connections and their associated resource settings.	Built In
○	Machine Catalog Administrator Can create and manage Machine Catalogs and provision machines.	Built In
○	Read Only Administrator Can see all objects in specified scopes as well as global information, b...	Built In

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


Create Administrator

Studio

✓ Administrator and Scope
✓ Role
Summary

Summary

Administrator: VCCFSLAB\Domain Admins
Scope: All
Role: Full Administrator

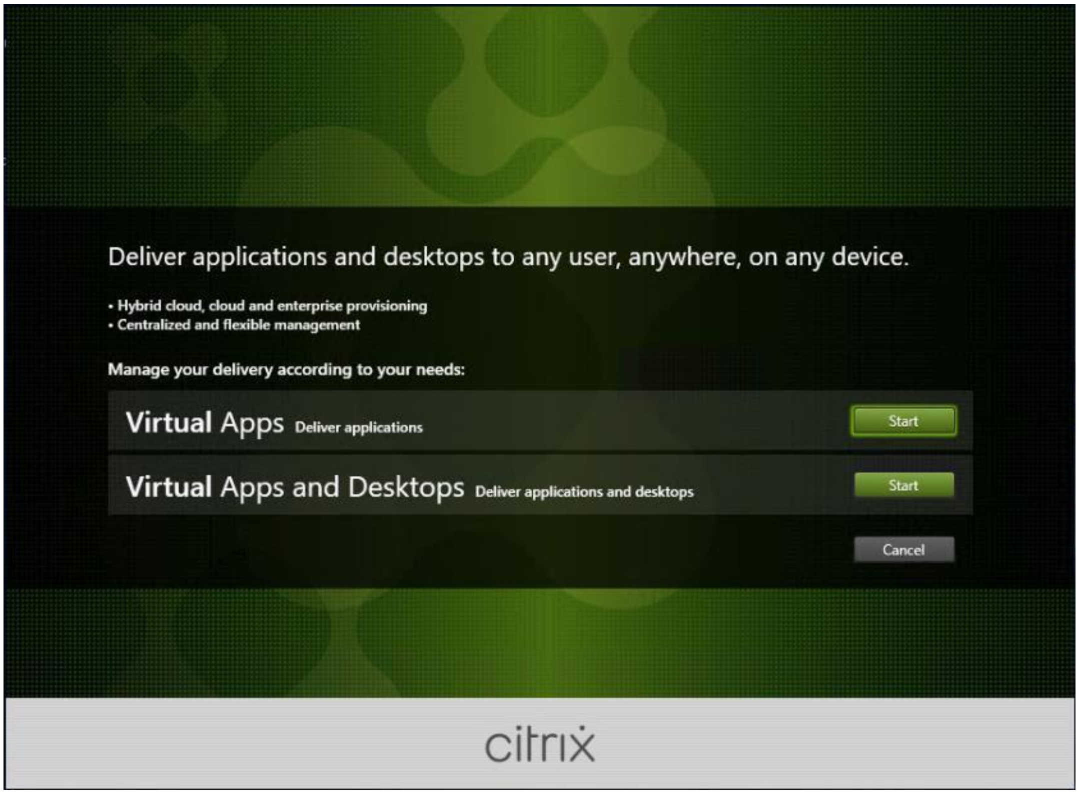
☑ Enable administrator
Clear check box to disable the administrator. No settings will be lost.

Procedure 8. Install and Configure StoreFront

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

Step 1. To begin the installation of the StoreFront, connect to the first StoreFront server and launch the installer from the Citrix_Virtual_Apps_and_Desktops_7_2203 ISO.

Step 2. Click Start.



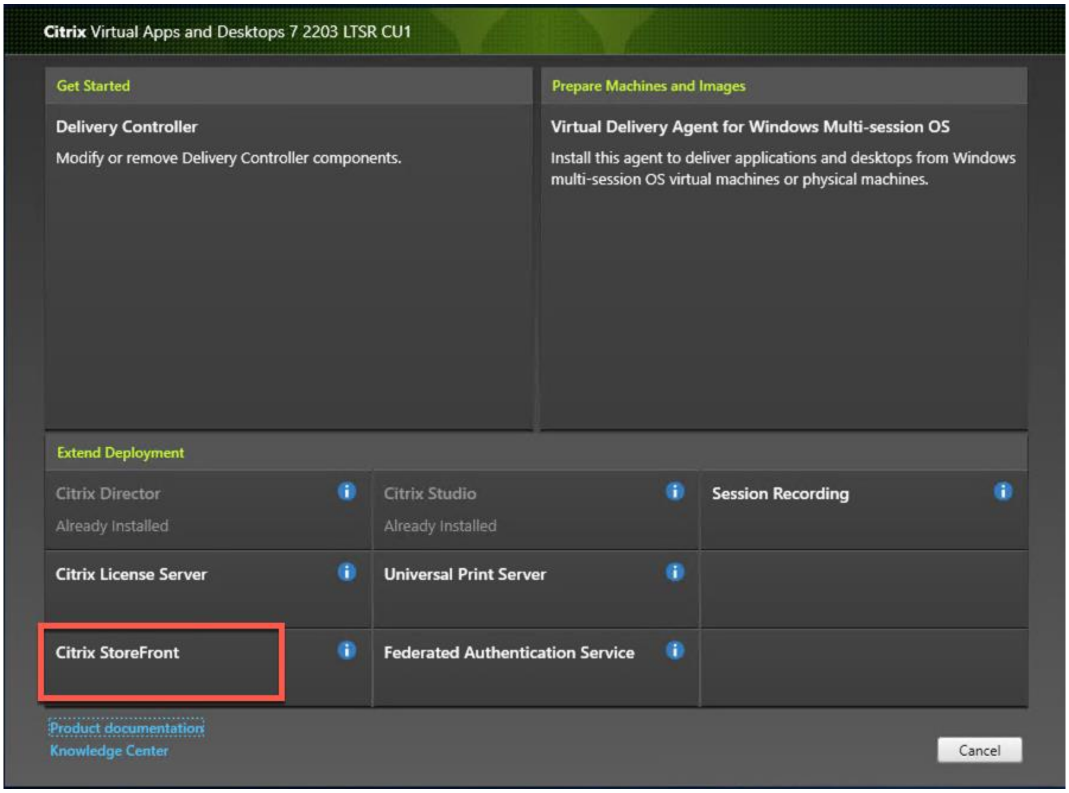
Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

Virtual Apps Deliver applications
Start
Virtual Apps and Desktops Deliver applications and desktops
Start
Cancel
citrix

Step 3. Click Extend Deployment Citrix StoreFront.



Citrix Virtual Apps and Desktops 7 2203 LTSR CU1

Get Started

Delivery Controller

Modify or remove Delivery Controller components.

Prepare Machines and Images

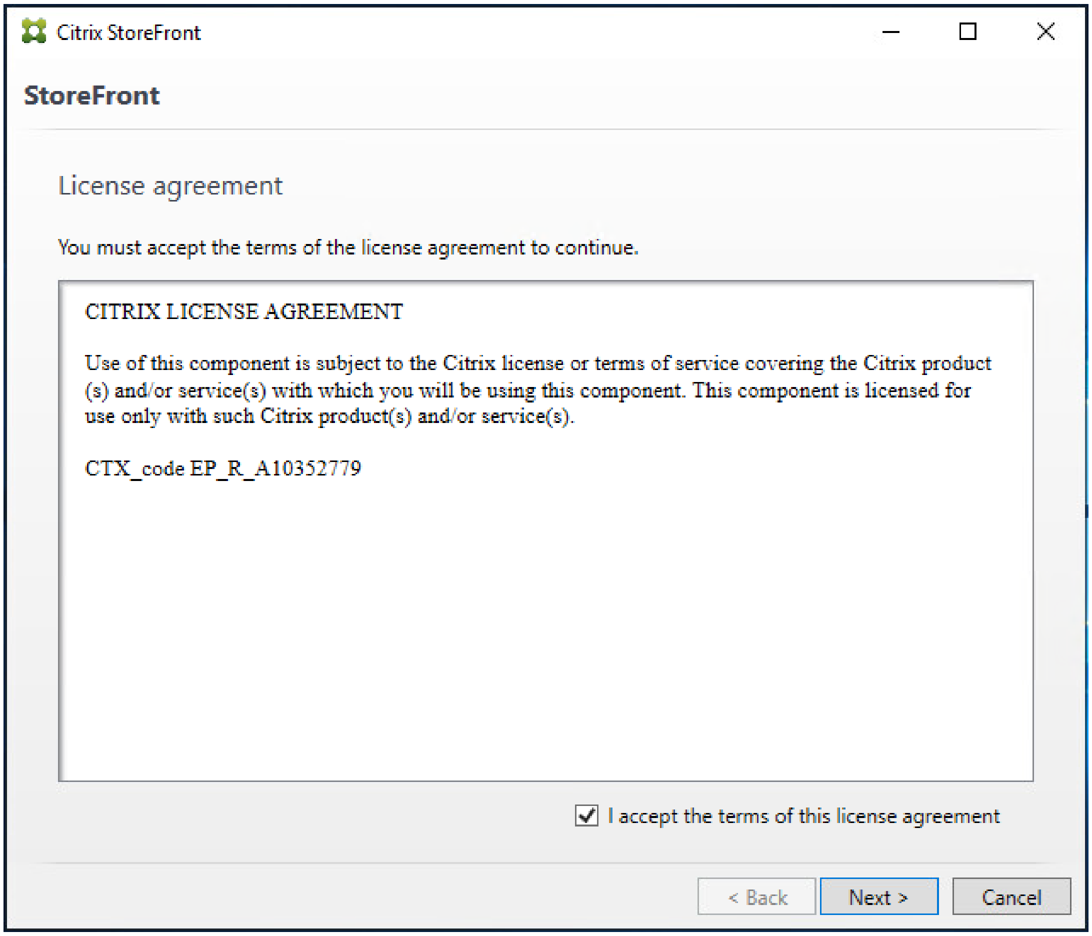
Virtual Delivery Agent for Windows Multi-session OS

Install this agent to deliver applications and desktops from Windows multi-session OS virtual machines or physical machines.

Extend Deployment

Step 4. Indicate your acceptance of the license by selecting the “I have read, understand, and accept the terms of the license agreement.”

Step 5. Click Next.



License agreement

You must accept the terms of the license agreement to continue.

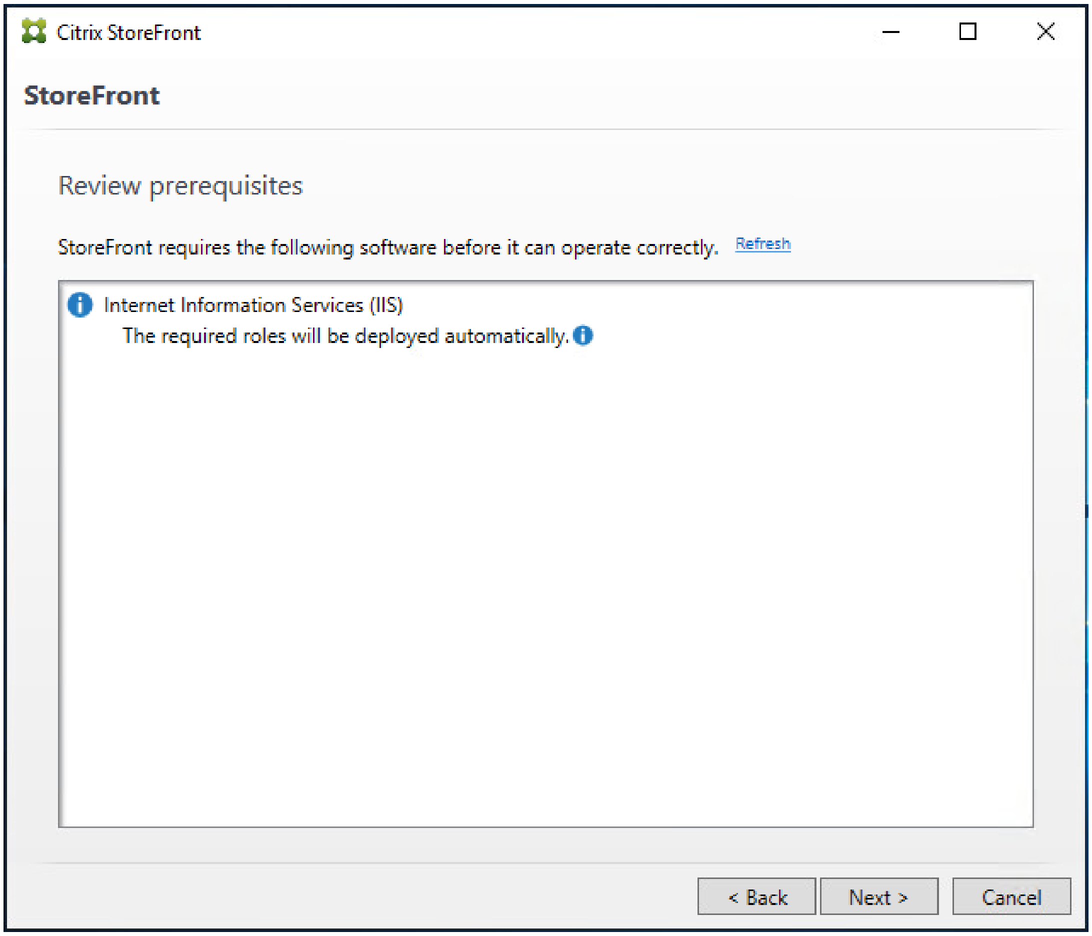
CITRIX LICENSE AGREEMENT

Use of this component is subject to the Citrix license or terms of service covering the Citrix product (s) and/or service(s) with which you will be using this component. This component is licensed for use only with such Citrix product(s) and/or service(s).

CTX_code EP_R_A10352779

☑ I accept the terms of this license agreement

Step 6. Review the prerequisites and click Next.



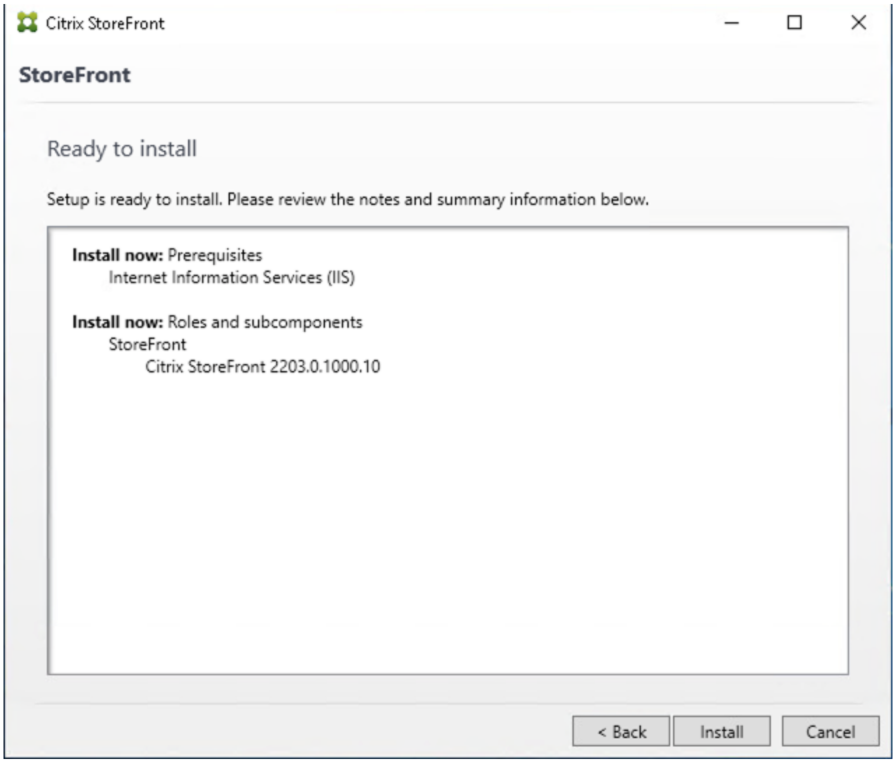
StoreFront

Review prerequisites

StoreFront requires the following software before it can operate correctly. Refresh

Internet Information Services (IIS)
The required roles will be deployed automatically.

Step 7. Click Install.



StoreFront

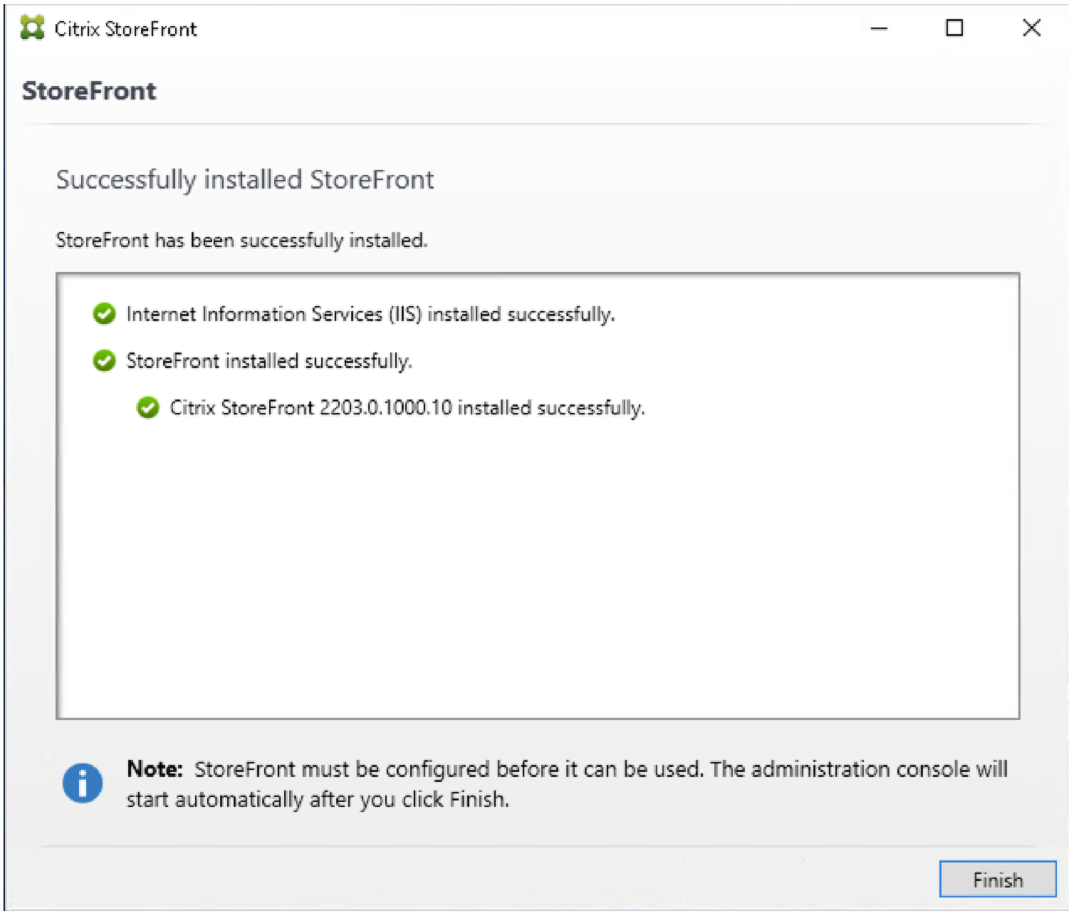
Ready to install

Setup is ready to install. Please review the notes and summary information below.

Install now: Prerequisites
Internet Information Services (IIS)

Install now: Roles and subcomponents
StoreFront
Citrix StoreFront 2203.0.1000.10

Step 8. Click Finish.



StoreFront

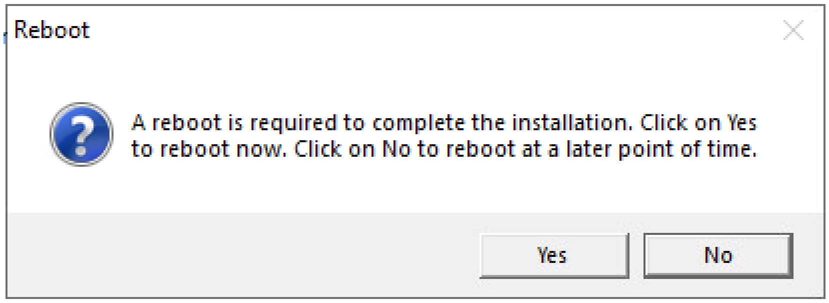
Successfully installed StoreFront

StoreFront has been successfully installed.

- ✓ Internet Information Services (IIS) installed successfully.
- ✓ StoreFront installed successfully.
  - ✓ Citrix StoreFront 2203.0.1000.10 installed successfully.

Note: StoreFront must be configured before it can be used. The administration console will start automatically after you click Finish.

Step 9. Click Yes to reboot the server.

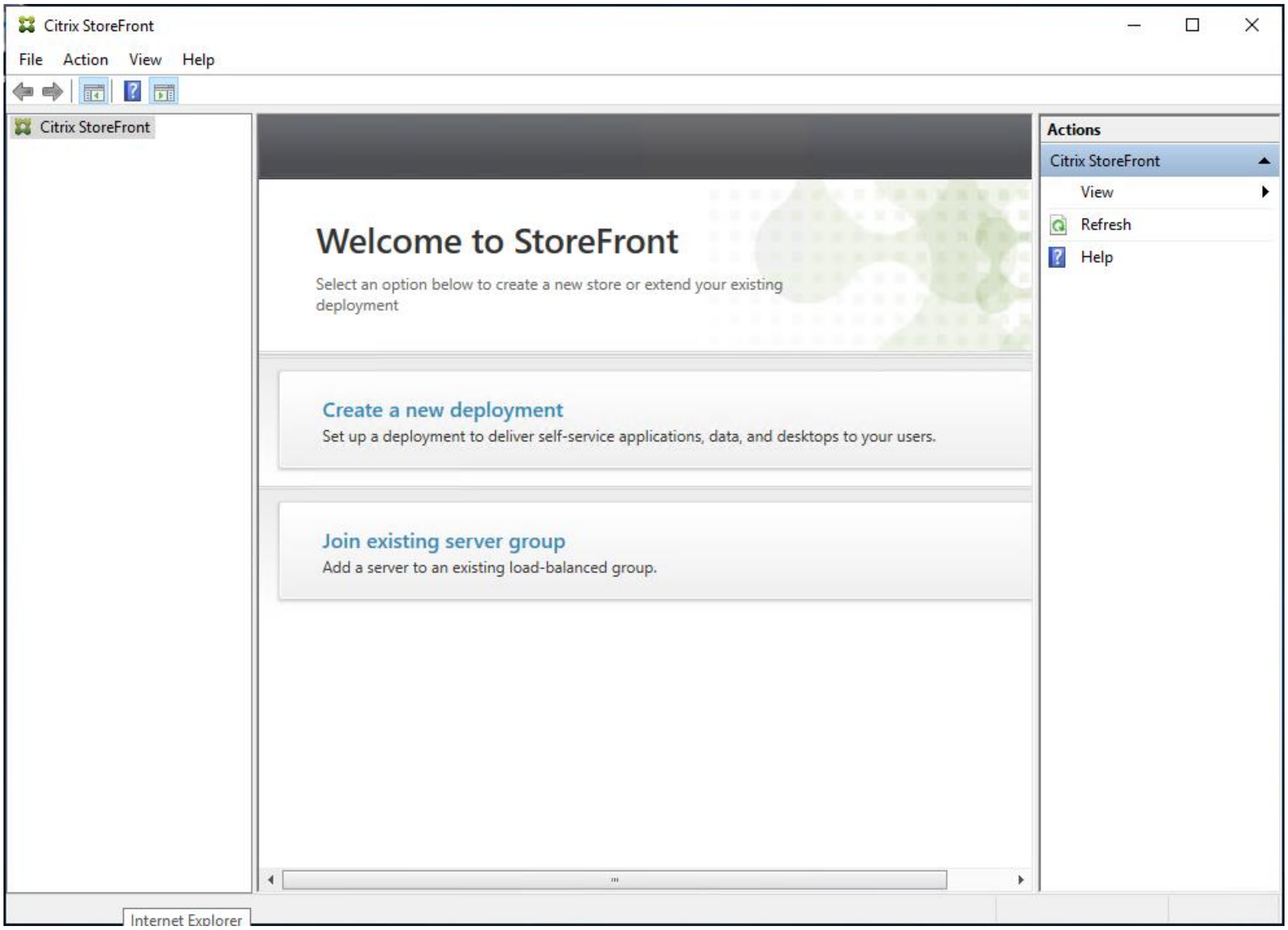


Reboot

A reboot is required to complete the installation. Click on Yes to reboot now. Click on No to reboot at a later point of time.

Step 10. Open the StoreFront Management Console.

Step 11. Click Create a new deployment.



Welcome to StoreFront

Select an option below to create a new store or extend your existing deployment

Create a new deployment

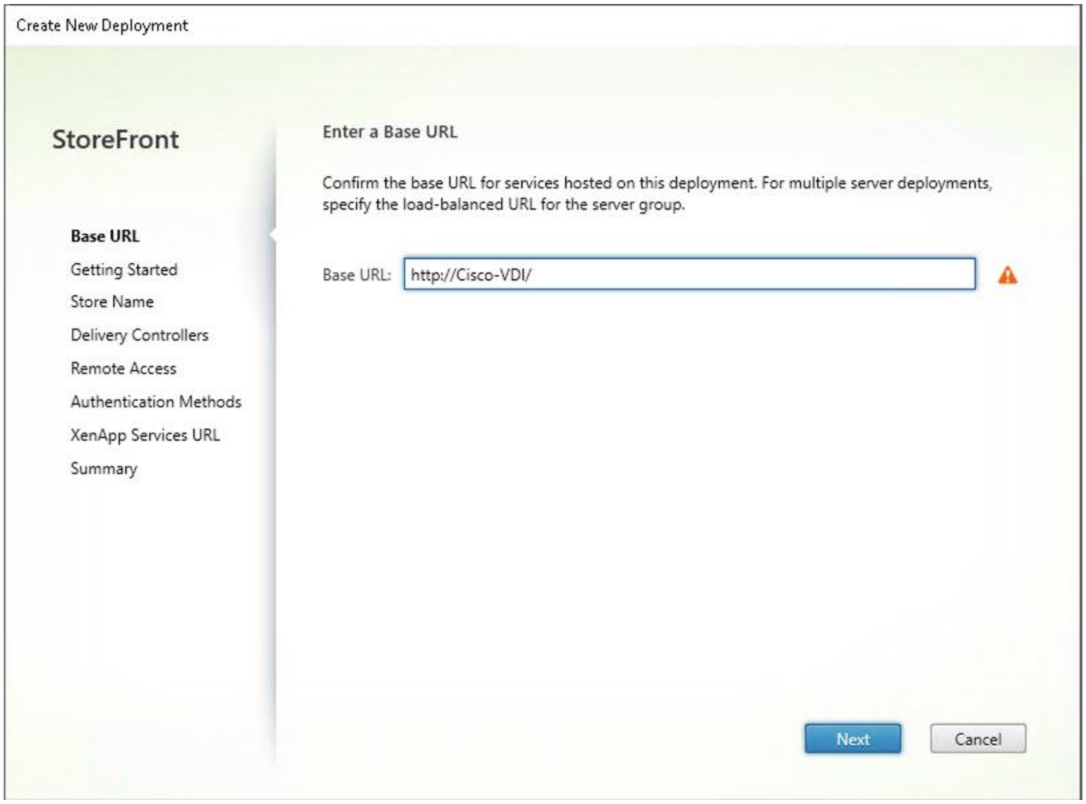
Set up a deployment to deliver self-service applications, data, and desktops to your users.

Join existing server group

Add a server to an existing load-balanced group.

Step 12. Specify name for your Base URL.

Step 13. Click Next.



Create New Deployment

StoreFront

Base URL

Getting Started

Store Name

Delivery Controllers

Remote Access

Authentication Methods

XenApp Services URL

Summary

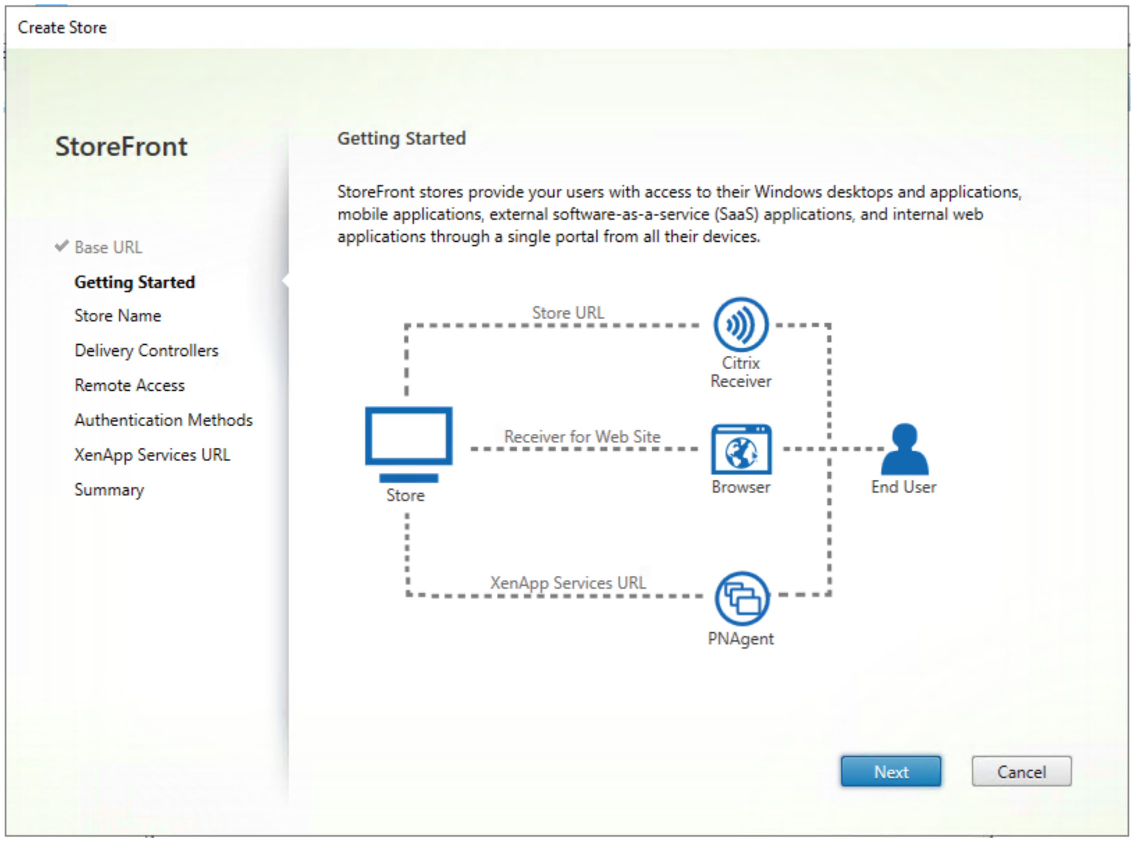
Enter a Base URL

Confirm the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.

Base URL: http://Cisco-VDI/

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

Step 14. Click Next.



Create Store

StoreFront

✓ Base URL

Getting Started

Store Name

Delivery Controllers

Remote Access

Authentication Methods

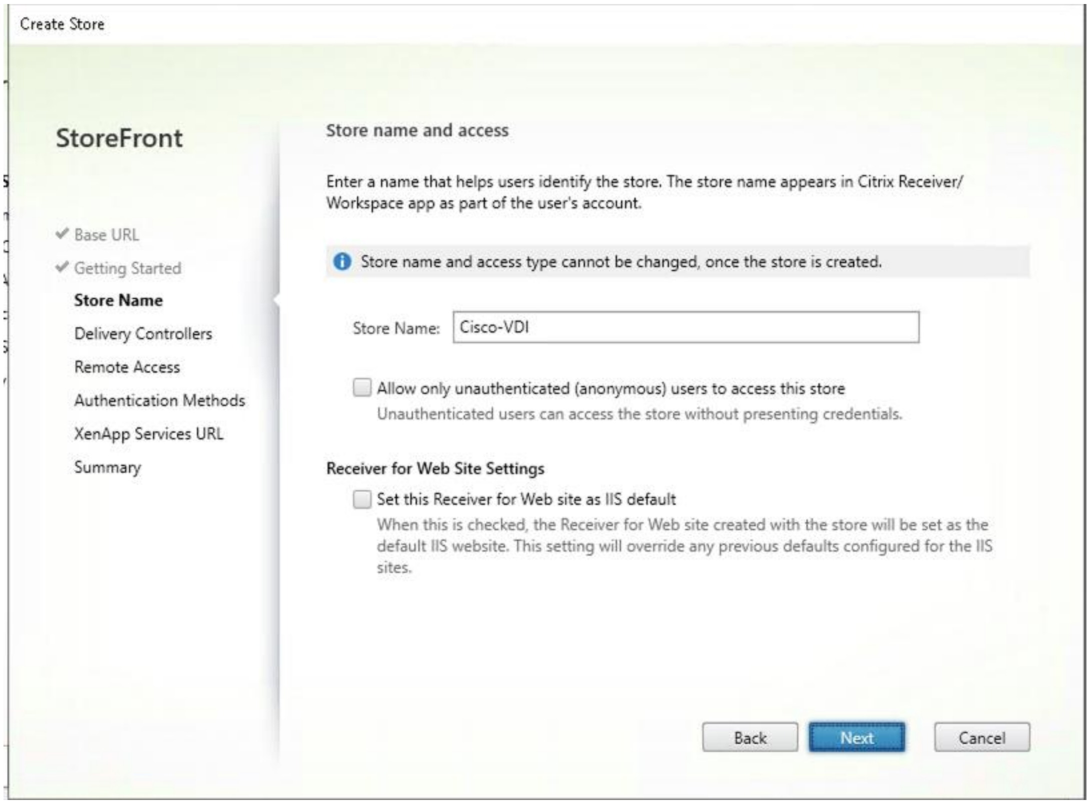
XenApp Services URL

Summary

Getting Started

StoreFront stores provide your users with access to their Windows desktops and applications, mobile applications, external software-as-a-service (SaaS) applications, and internal web applications through a single portal from all their devices.

Step 15. Specify a name for your store.



Create Store

StoreFront

✔ Base URL
✔ Getting Started
Store Name
Delivery Controllers
Remote Access
Authentication Methods
XenApp Services URL
Summary

Store name and access

Enter a name that helps users identify the store. The store name appears in Citrix Receiver/ Workspace app as part of the user's account.

Store name and access type cannot be changed, once the store is created.

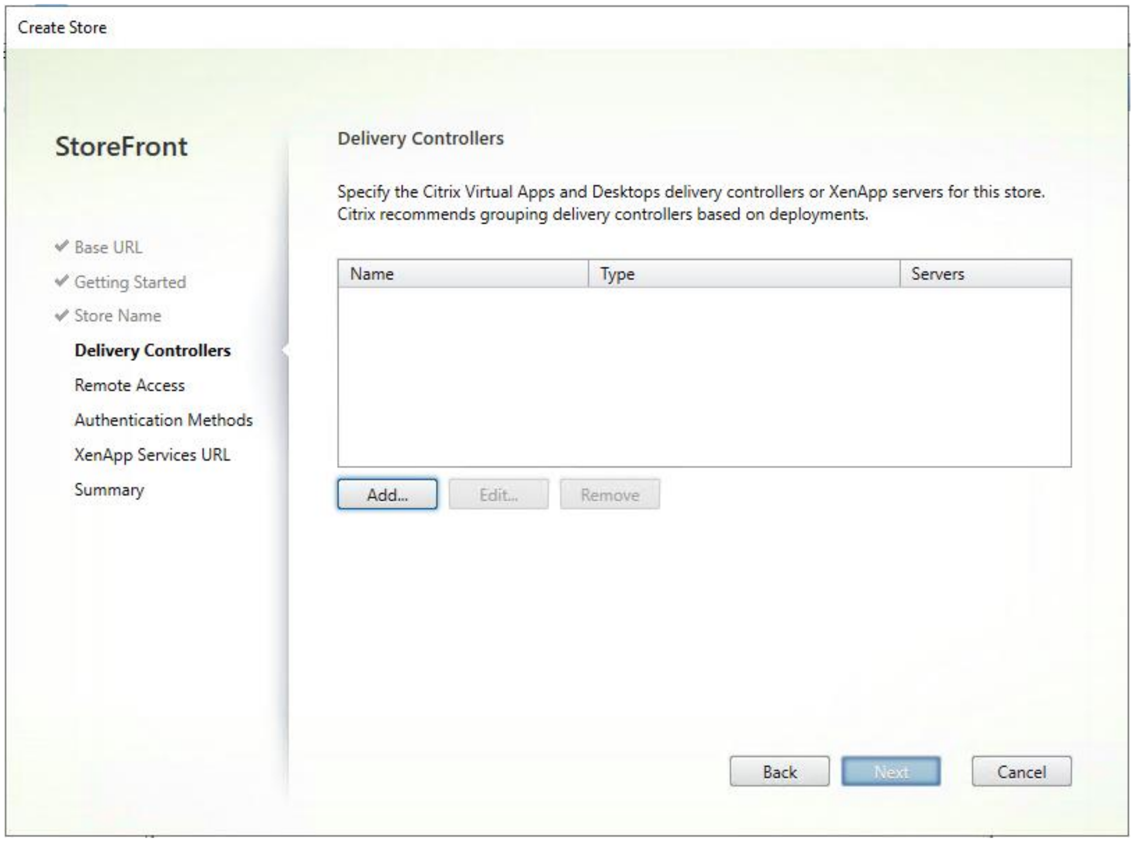
Store Name: Cisco-VDI

☐ Allow only unauthenticated (anonymous) users to access this store
Unauthenticated users can access the store without presenting credentials.

Receiver for Web Site Settings

☐ Set this Receiver for Web site as IIS default
When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.

Step 16. Click Add to specify Delivery controllers for your new Store.



Create Store

StoreFront

✔ Base URL
✔ Getting Started
✔ Store Name
Delivery Controllers
Remote Access
Authentication Methods
XenApp Services URL
Summary

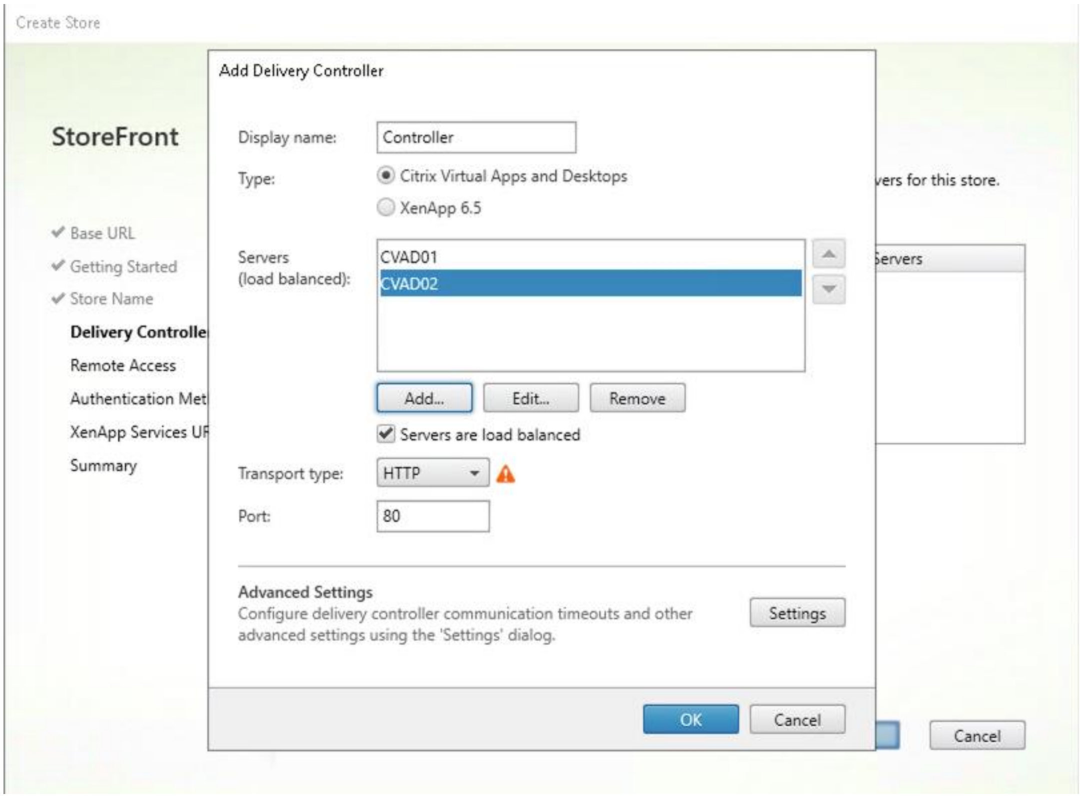
Delivery Controllers

Specify the Citrix Virtual Apps and Desktops delivery controllers or XenApp servers for this store. Citrix recommends grouping delivery controllers based on deployments.

Name	Type	Servers

Step 17. Add the required Delivery Controllers to the store.

Step 18. Click OK.



Add Delivery Controller

Display name: Controller

Type: ● Citrix Virtual Apps and Desktops ○ XenApp 6.5

Servers (load balanced): CVAD01, CVAD02

☑ Servers are load balanced

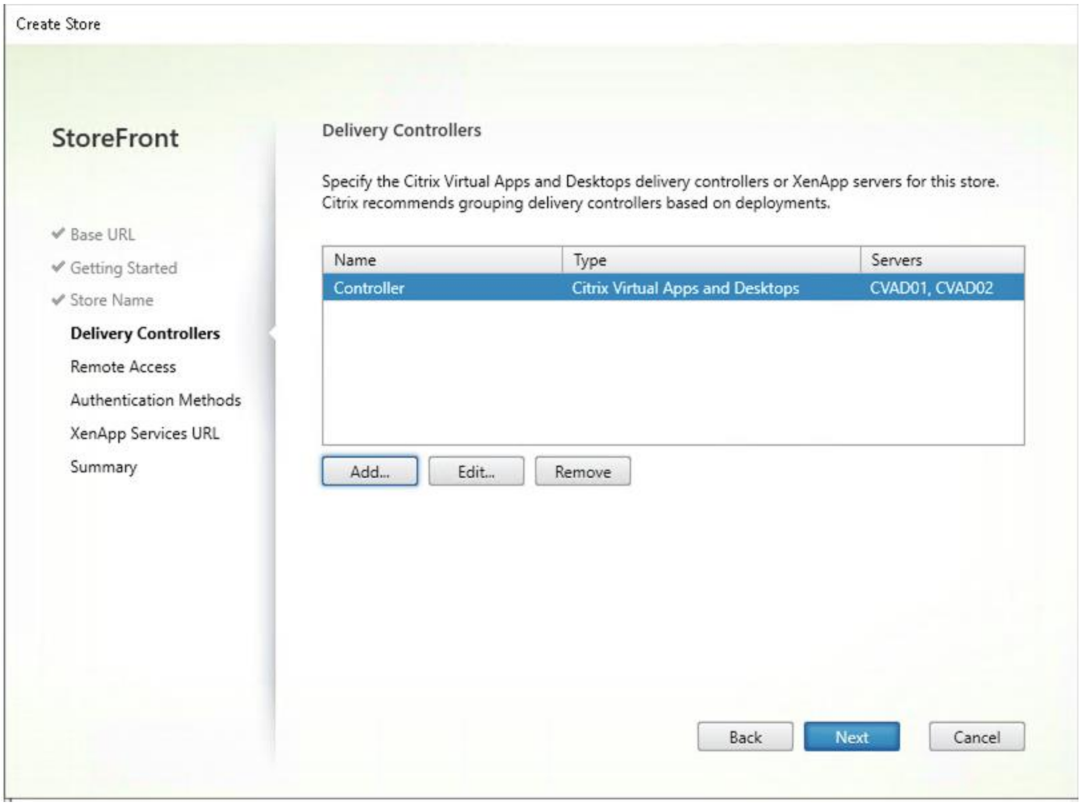
Transport type: HTTP

Port: 80

Advanced Settings

Configure delivery controller communication timeouts and other advanced settings using the 'Settings' dialog.

Step 19. Click Next.



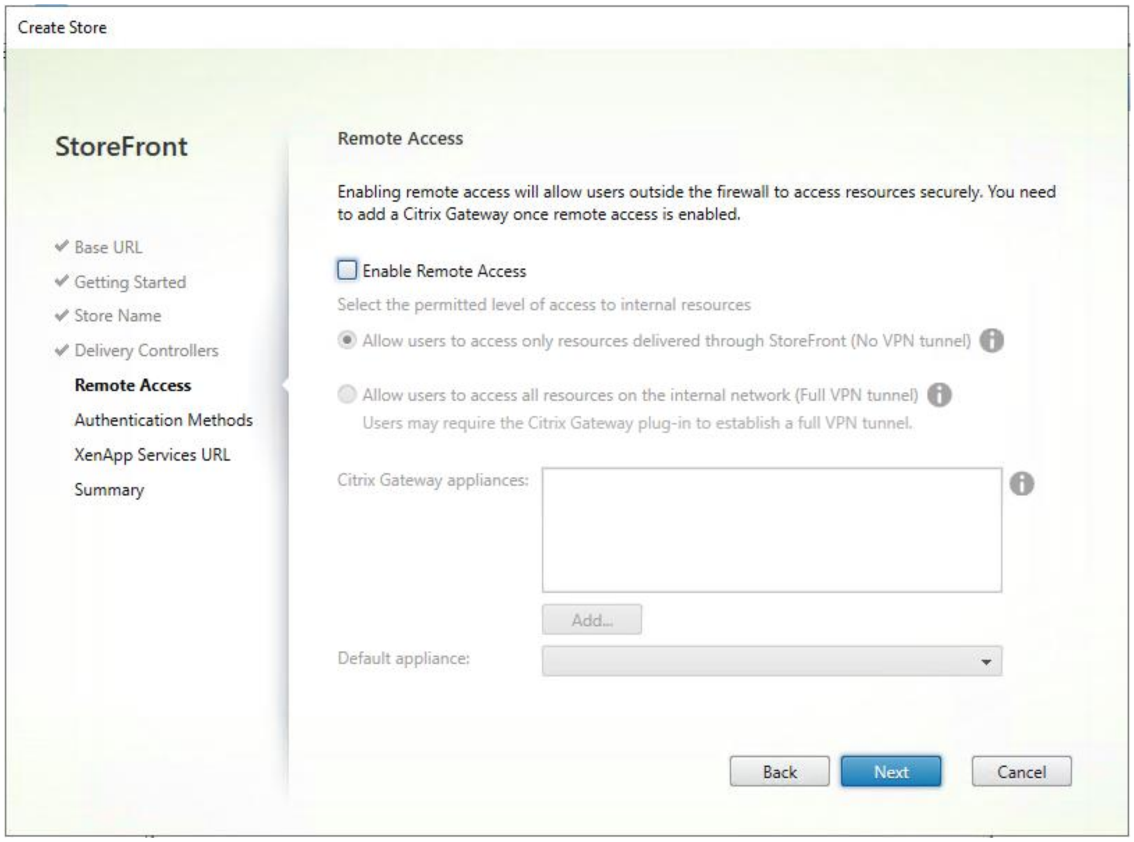
Delivery Controllers

Specify the Citrix Virtual Apps and Desktops delivery controllers or XenApp servers for this store. Citrix recommends grouping delivery controllers based on deployments.

Name	Type	Servers
Controller	Citrix Virtual Apps and Desktops	CVAD01, CVAD02

Step 20. Specify how connecting users can access the resources, in this environment only local users on the internal network are able to access the store.

Step 21. Click Next.



Create Store

StoreFront

✓ Base URL
✓ Getting Started
✓ Store Name
✓ Delivery Controllers
Remote Access
Authentication Methods
XenApp Services URL
Summary

Remote Access

Enabling remote access will allow users outside the firewall to access resources securely. You need to add a Citrix Gateway once remote access is enabled.

□ Enable Remote Access

Select the permitted level of access to internal resources

● Allow users to access only resources delivered through StoreFront (No VPN tunnel)

○ Allow users to access all resources on the internal network (Full VPN tunnel)
Users may require the Citrix Gateway plug-in to establish a full VPN tunnel.

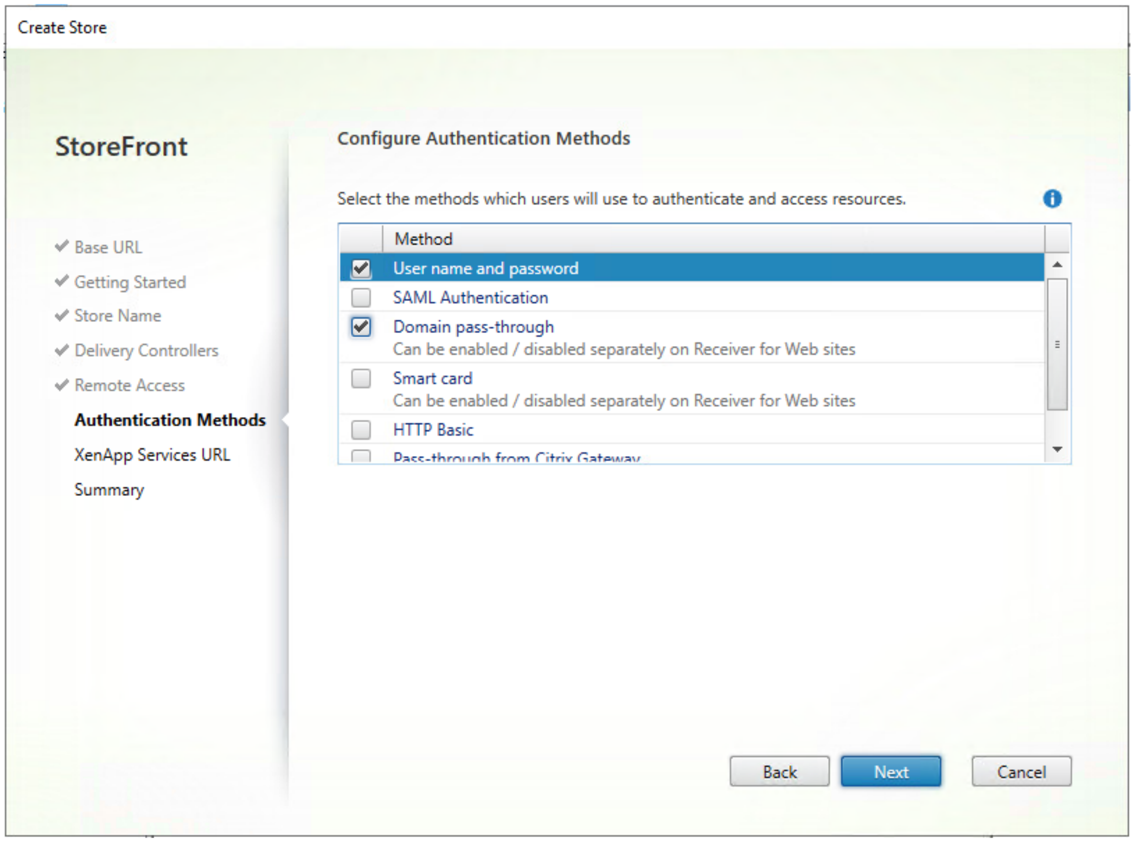
Citrix Gateway appliances:

Default appliance:

Step 22. On the "Authentication Methods" page, select the methods your users will use to authenticate to the store. The following methods were configured in this deployment:

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

Step 23. Click Next.



Create Store

StoreFront

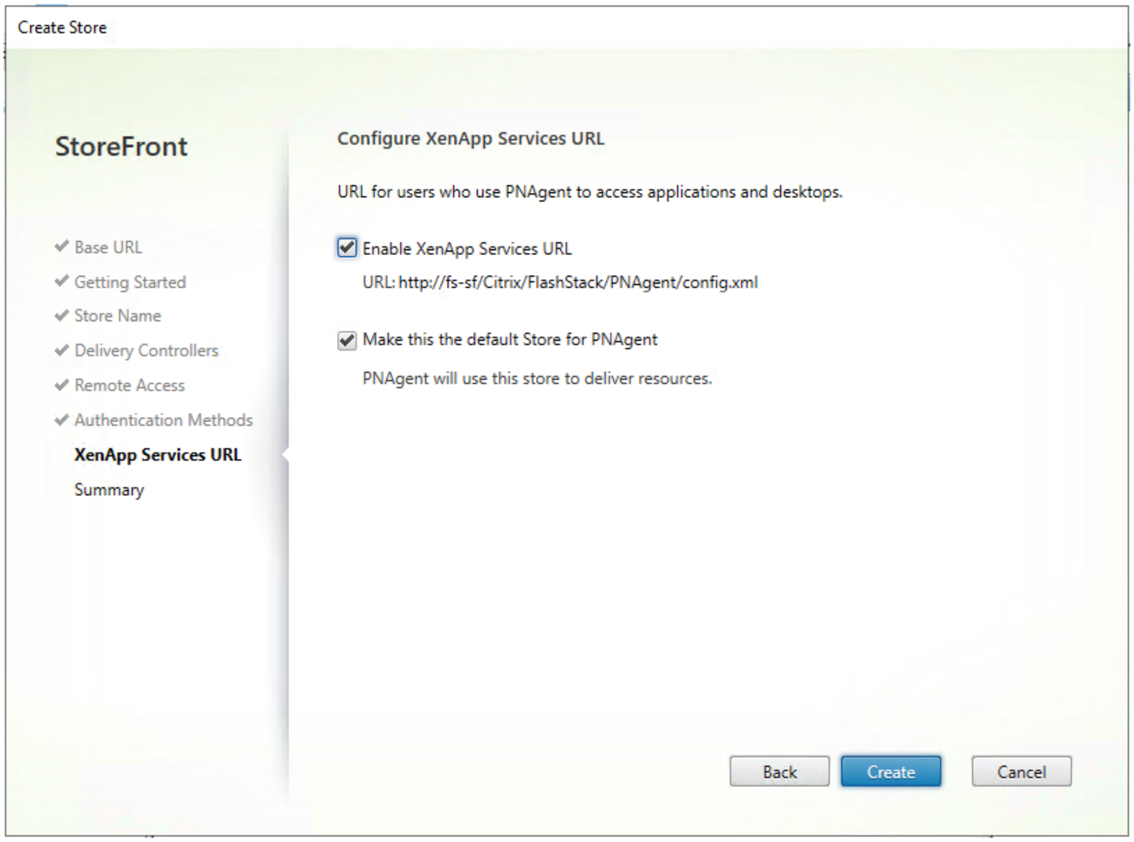
Configure Authentication Methods

Select the methods which users will use to authenticate and access resources.

	Method
☑	User name and password
□	SAML Authentication
☑	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites
□	Smart card Can be enabled / disabled separately on Receiver for Web sites
□	HTTP Basic
□	Pass-through from Citrix Gateway

Step 24. Configure the XenApp Service URL for users who use PNAgent to access the applications and desktops.

Step 25. Click Create.



Create Store

StoreFront

Configure XenApp Services URL

URL for users who use PNAgent to access applications and desktops.

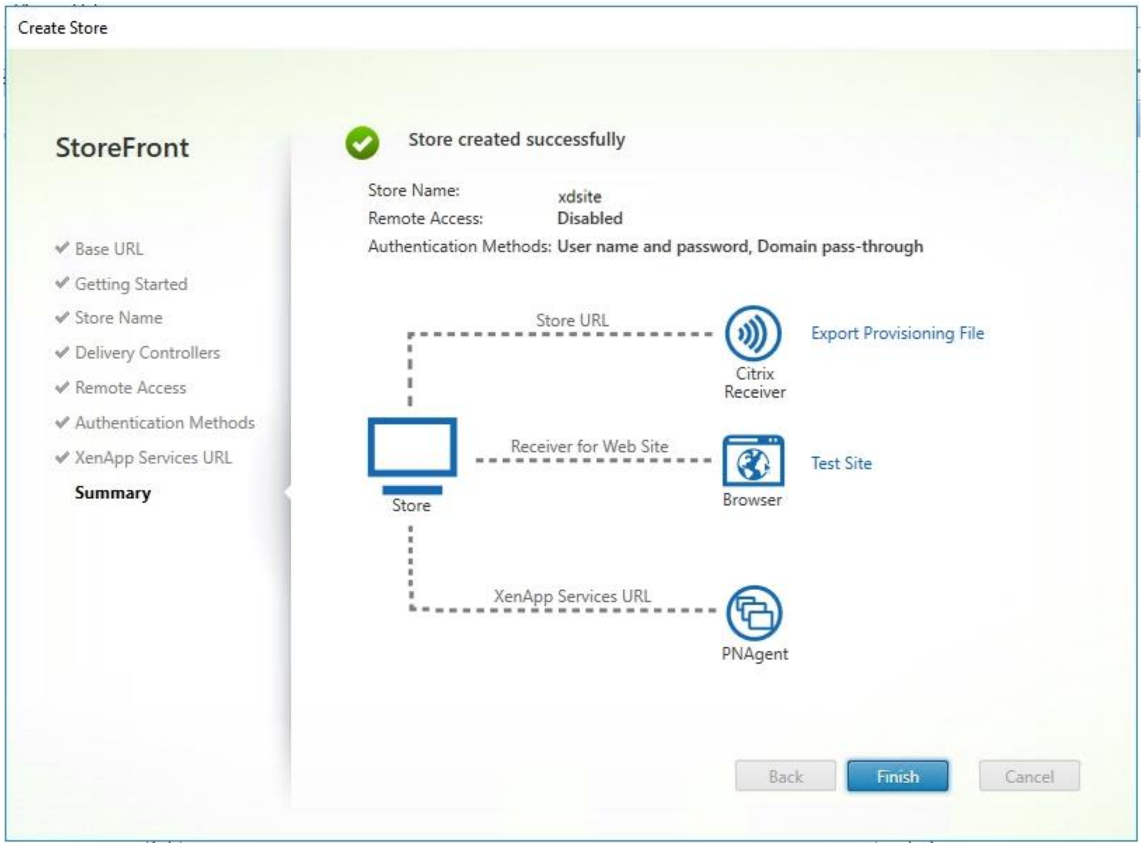
☑ Enable XenApp Services URL

URL: http://fs-sf/Citrix/FlashStack/PNAgent/config.xml

☑ Make this the default Store for PNAgent

PNAgent will use this store to deliver resources.

Step 26. After creating the store click Finish.



Create Store

StoreFront

Store created successfully

Store Name: xdsite

Remote Access: Disabled

Authentication Methods: User name and password, Domain pass-through

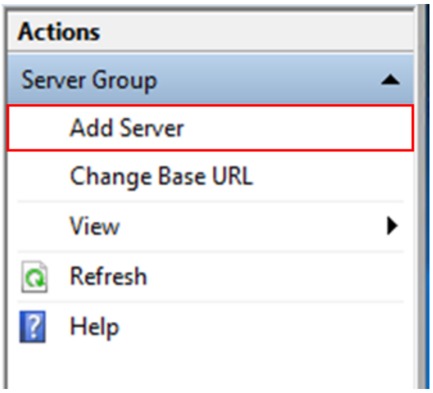
Procedure 9. Additional StoreFront Configuration

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

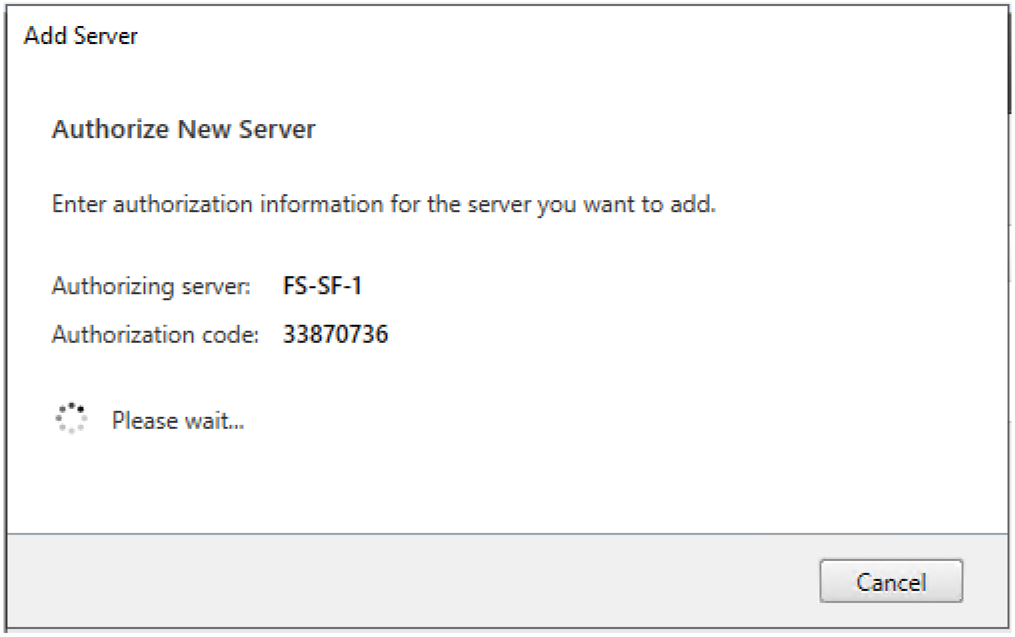
Step 1. Install the second StoreFront using the same installation steps outlined above.

Step 2. Connect to the first StoreFront server

Step 3. To add the second server and generate the authorization information that allows the additional StoreFront server to join the server group, select Add Server from Actions pane in the Server Group.



Step 4. Copy the authorization code.



Authorize New Server

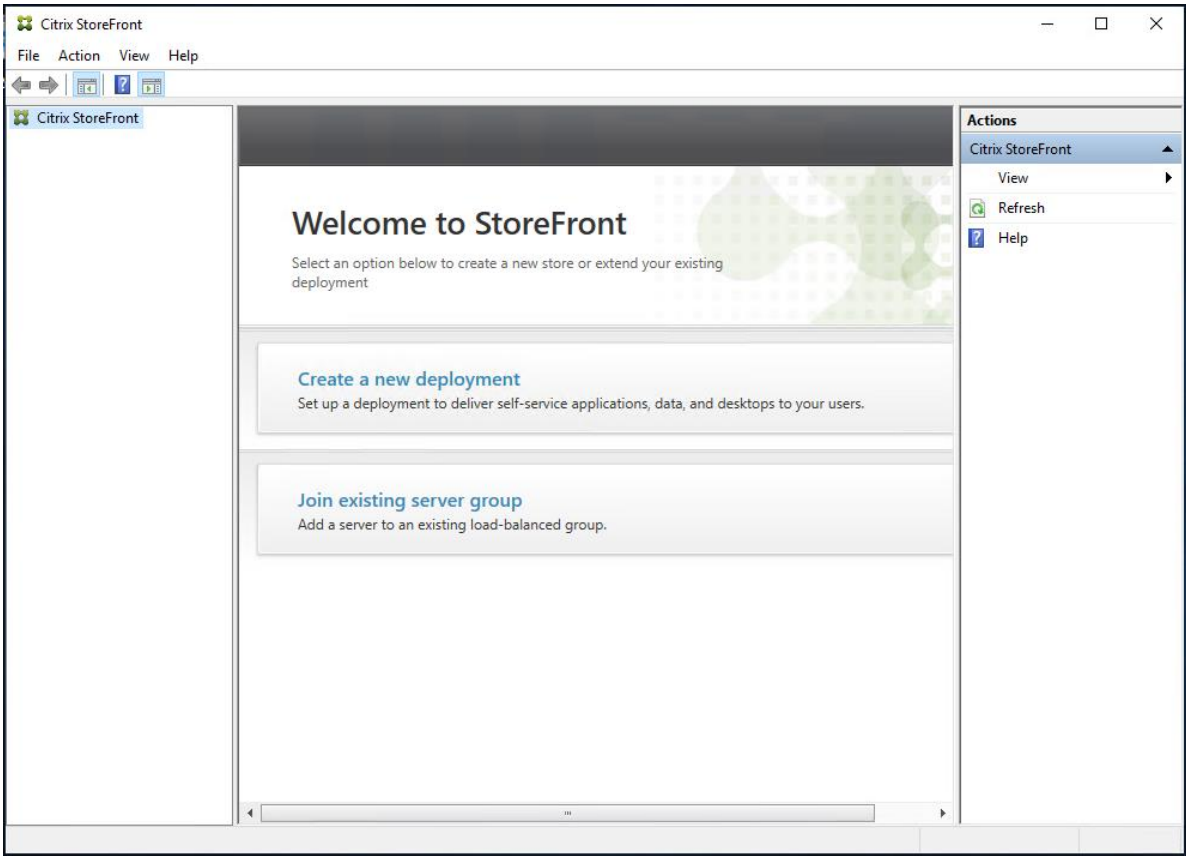
Enter authorization information for the server you want to add.

Authorizing server: FS-SF-1

Authorization code: 33870736

Please wait...

Step 5. From the StoreFront Console on the second server select “Join existing server group.”



Welcome to StoreFront

Select an option below to create a new store or extend your existing deployment

Create a new deployment

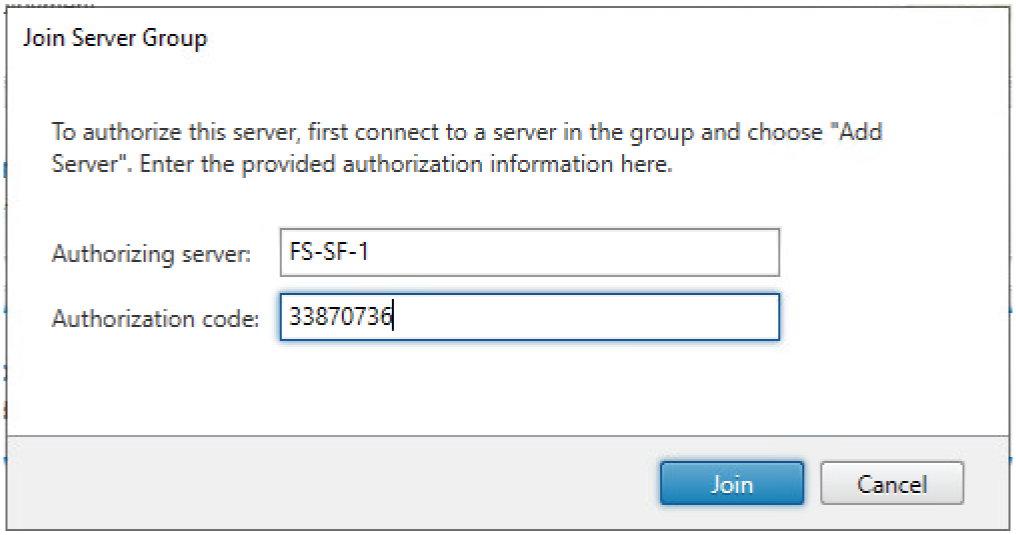
Set up a deployment to deliver self-service applications, data, and desktops to your users.

Join existing server group

Add a server to an existing load-balanced group.

Step 6. In the Join Server Group dialog, enter the name of the first Storefront server and paste the Authorization code into the Join Server Group dialog.

Step 7. Click Join.



Join Server Group

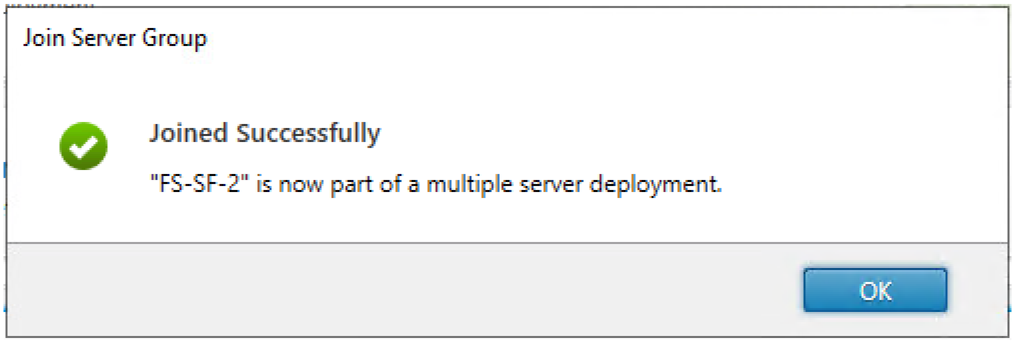
To authorize this server, first connect to a server in the group and choose "Add Server". Enter the provided authorization information here.

Authorizing server: FS-SF-1

Authorization code: 33870736

Step 8. A message appears when the second server has joined successfully.

Step 9. Click OK.

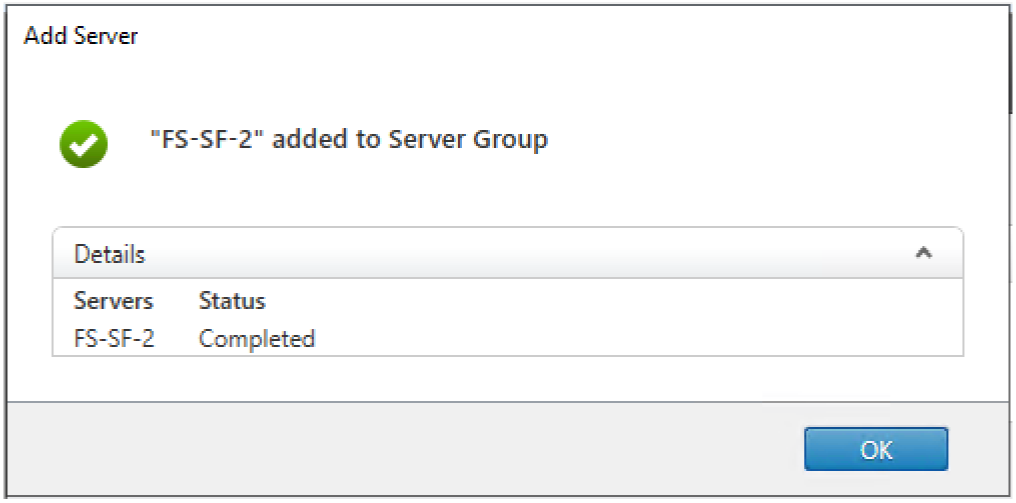


Join Server Group

Joined Successfully

"FS-SF-2" is now part of a multiple server deployment.

The second StoreFront is now in the Server Group.



Add Server

"FS-SF-2" added to Server Group

Details

Servers	Status
FS-SF-2	Completed

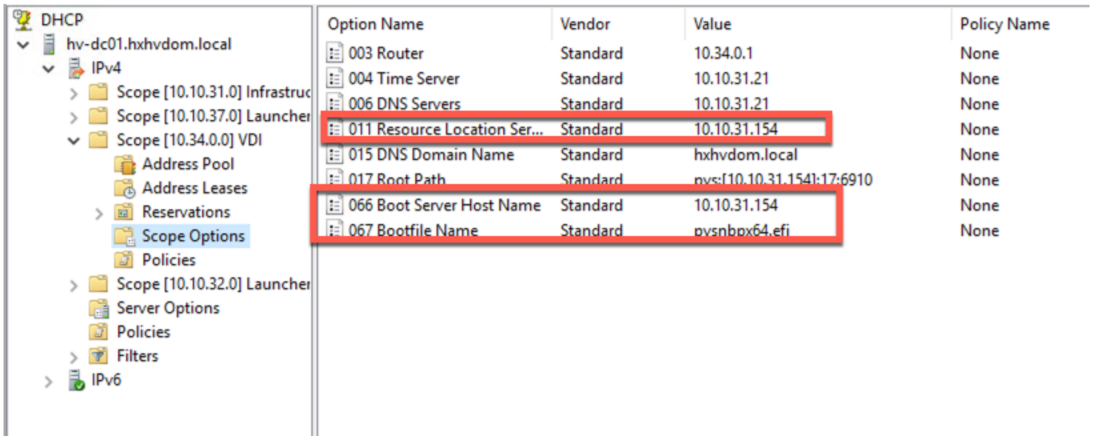
Install and Configure Citrix Provisioning Server 2203

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 in the Provisioning Services 2203 document.

Procedure 1. Configure Prerequisites

Step 1. Set the following Scope Options on the DHCP server hosting the PVS target machines:



DHCP
- hv-dc01.hxhvdom.local
  - IPv4
    - Scope [10.10.31.0] Infrastruc
    - Scope [10.10.37.0] Launcher
    - Scope [10.34.0.0] VDI
      - Address Pool
      - Address Leases
      - Reservations
      - Scope Options
      - Policies
    - Scope [10.10.32.0] Launcher
    - Server Options
    - Policies
    - Filters
  - IPv6

Option Name	Vendor	Value	Policy Name
003 Router	Standard	10.34.0.1	None
004 Time Server	Standard	10.10.31.21	None
006 DNS Servers	Standard	10.10.31.21	None
011 Resource Location Ser...	Standard	10.10.31.154	None
015 DNS Domain Name	Standard	hxhvdom.local	None
017 Root Path	Standard	pvs:[10.10.31.154]:17:6910	None
066 Boot Server Host Name	Standard	10.10.31.154	None
067 Bootfile Name	Standard	pvsnbpx64.efi	None

Step 2. Create a DNS host records with multiple PVS Servers IP for TFTP Load Balancing:

Step 3. 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"
```

Note: 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.

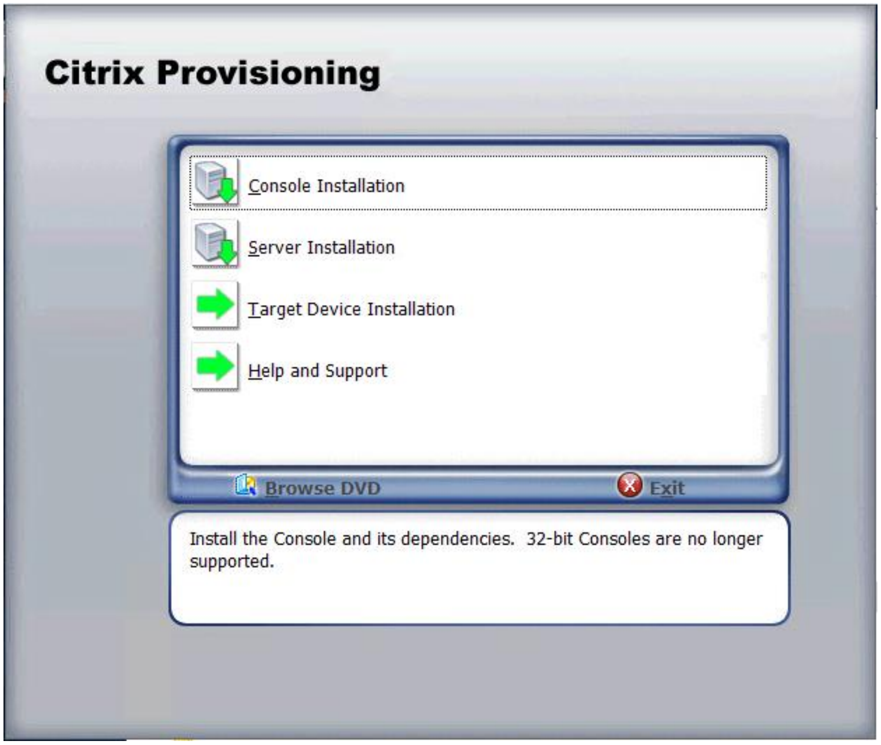
The following databases are supported: Microsoft SQL Server 2008 SP3 through 2016 (x86, x64, and Express editions). Please check Citrix documentation for further reference.

Note: Microsoft SQL 2019 was installed separately for this CVD.

Procedure 2. Install and Configure Citrix Provisioning Service 2203

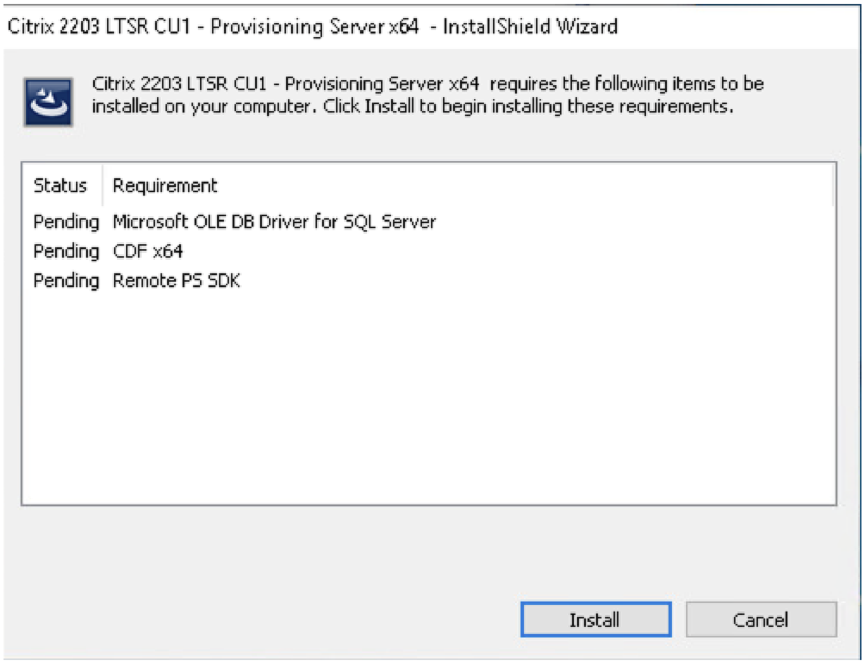
Step 1. Connect to Citrix Provisioning server and launch Citrix Provisioning Services 2203 ISO and let AutoRun launch the installer.

Step 2. Click Console Installation.



Install the Console and its dependencies. 32-bit Consoles are no longer supported.

Step 3. Click Install to start the console installation.

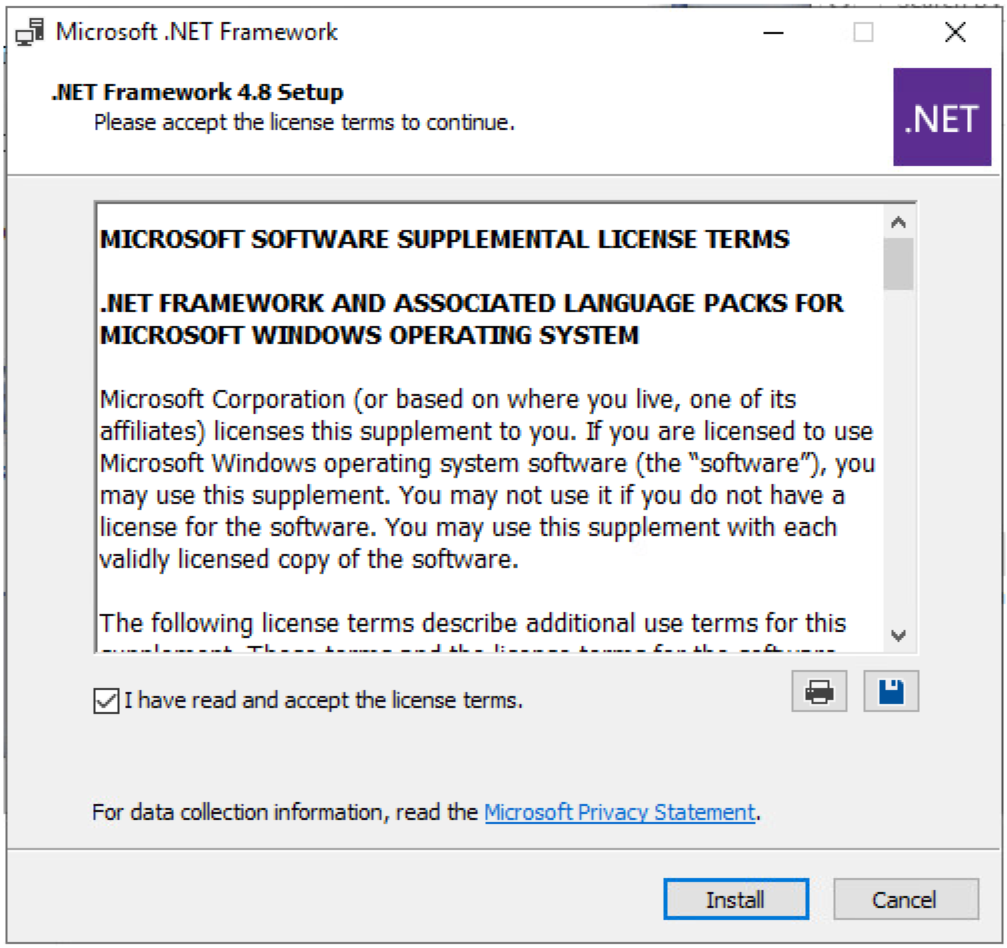

Citrix 2203 LTSR CU1 - Provisioning Server x64 - InstallShield Wizard
Install
Cancel

Citrix 2203 LTSR CU1 - Provisioning Server x64 requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	Microsoft OLE DB Driver for SQL Server
Pending	CDF x64
Pending	Remote PS SDK

Step 4. Read the .NET License Agreement. If acceptable, check “I have read and accept the license terms.”

Step 5. Click Next.



.NET Framework 4.8 Setup

Please accept the license terms to continue.

MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

.NET FRAMEWORK AND ASSOCIATED LANGUAGE PACKS FOR MICROSOFT WINDOWS OPERATING SYSTEM

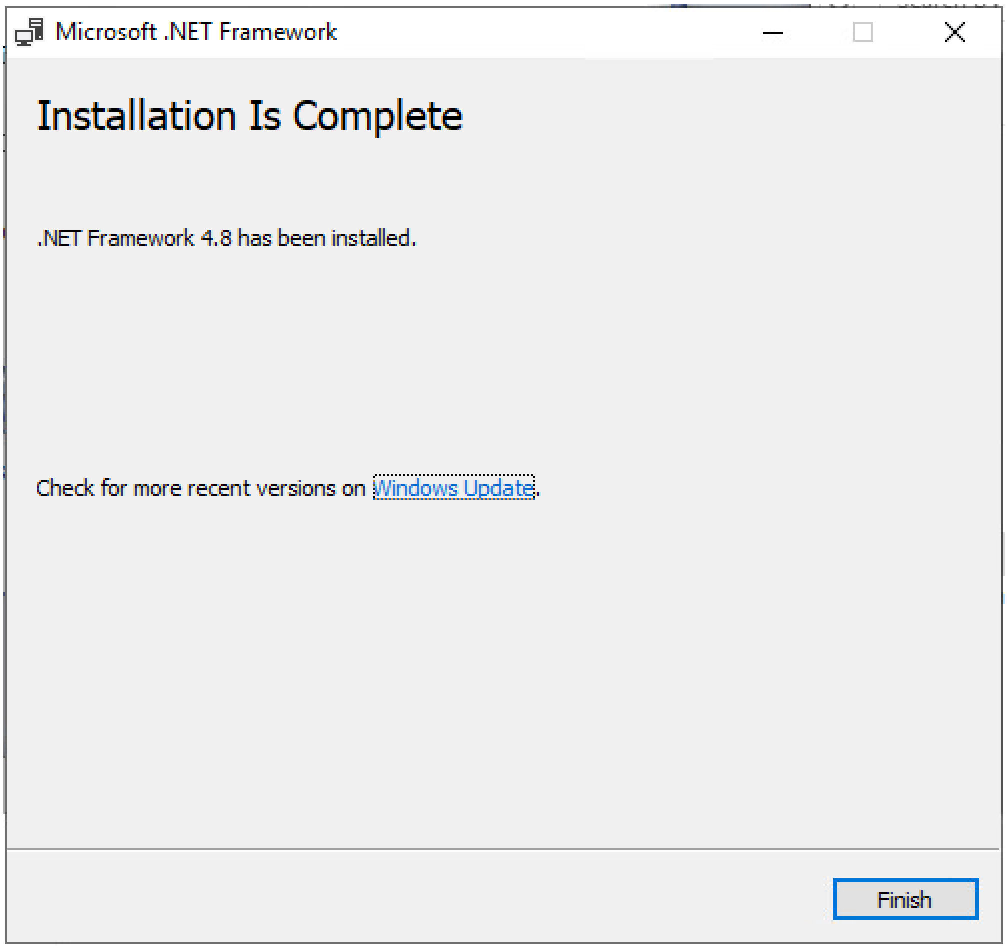
Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows operating system software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use this supplement with each validly licensed copy of the software.

The following license terms describe additional use terms for this

☑ I have read and accept the license terms.

For data collection information, read the Microsoft Privacy Statement.

Step 6. Click Finish.



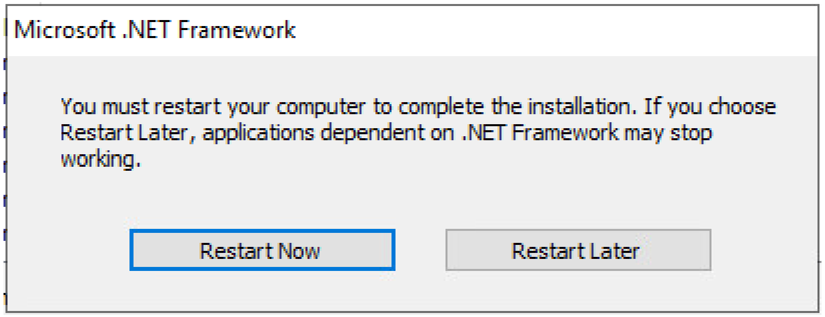
Microsoft .NET Framework

Installation Is Complete

.NET Framework 4.8 has been installed.

Check for more recent versions on Windows Update.

Step 7. Restart the Virtual Machine.

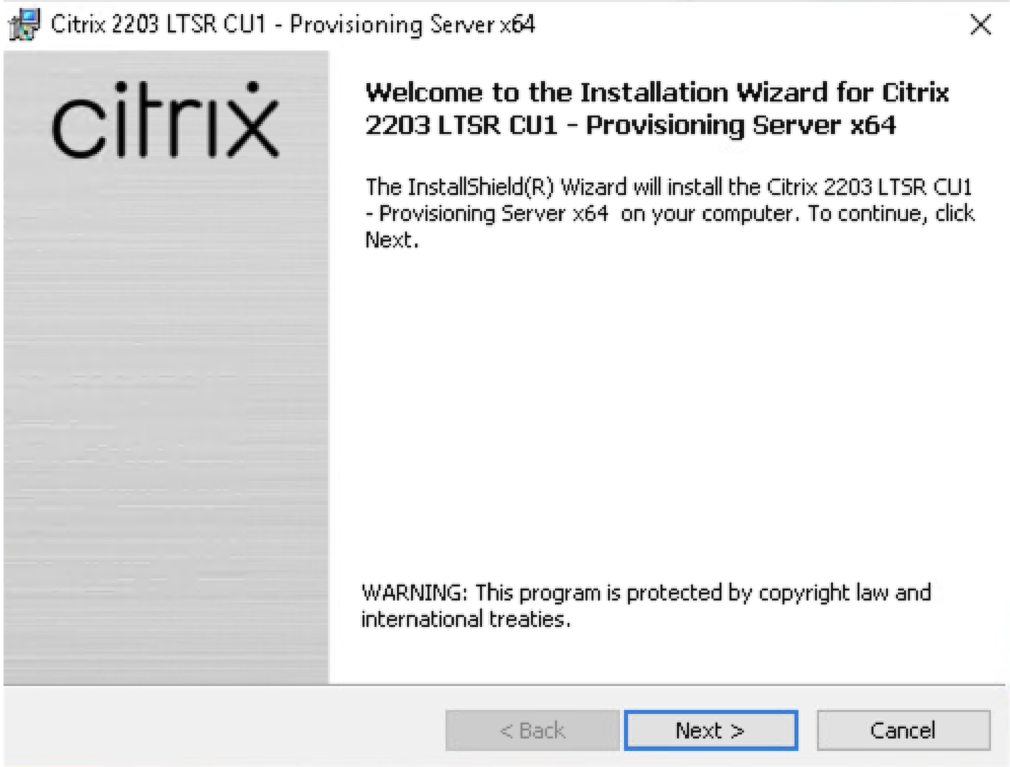


Microsoft .NET Framework

You must restart your computer to complete the installation. If you choose Restart Later, applications dependent on .NET Framework may stop working.

Step 8. Logging into the Operating system automatically launches the installation wizard.

Step 9. Click Next.



Citrix 2203 LTSR CU1 - Provisioning Server x64

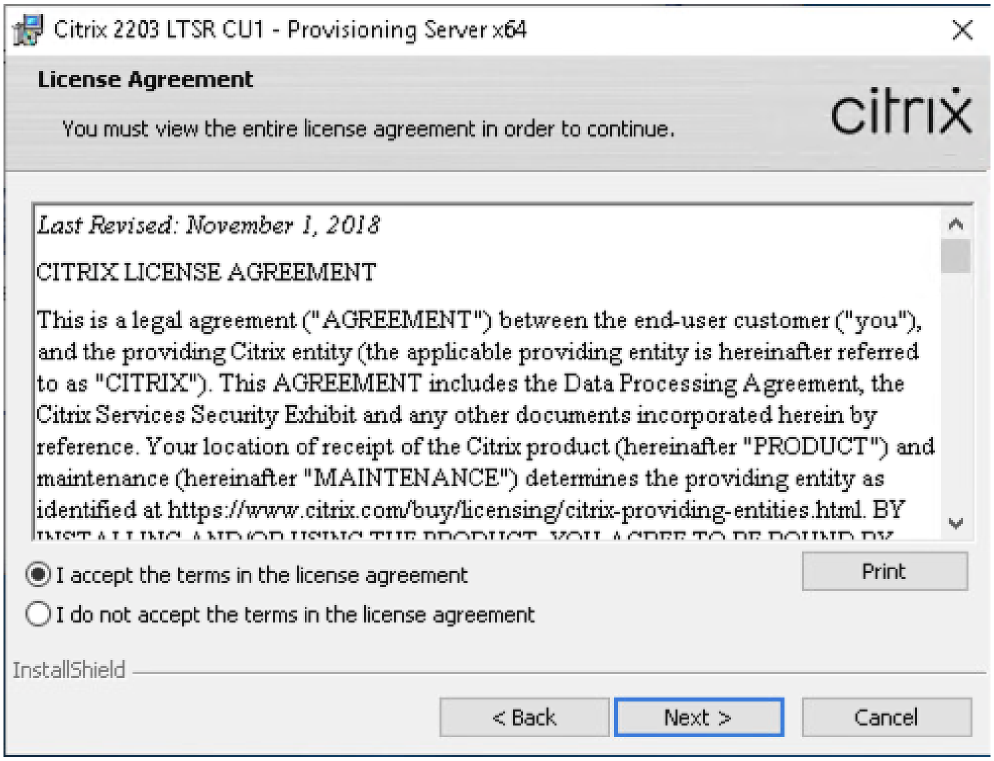
Welcome to the Installation Wizard for Citrix 2203 LTSR CU1 - Provisioning Server x64

The InstallShield(R) Wizard will install the Citrix 2203 LTSR CU1 - Provisioning Server x64 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 10. Read the Citrix License Agreement. If acceptable, select the radio button labeled "I accept the terms in the license agreement."

Step 11. Click Next.



Citrix 2203 LTSR CU1 - Provisioning Server x64

License Agreement

You must view the entire license agreement in order to continue.

Last Revised: November 1, 2018

CITRIX LICENSE AGREEMENT

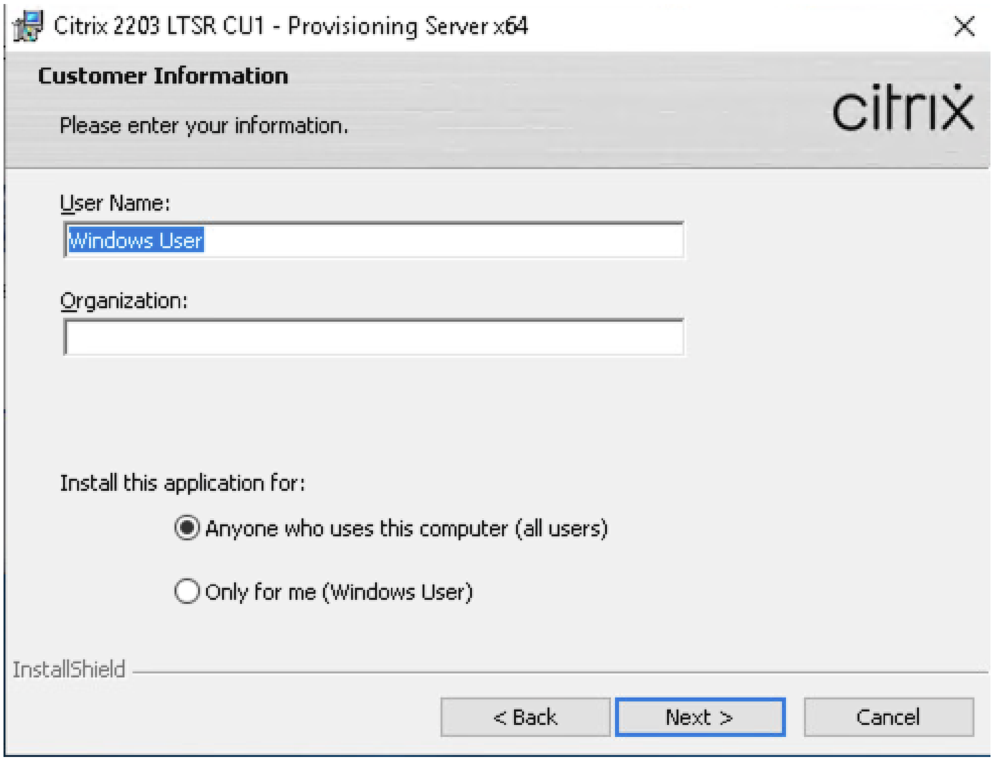
This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix-providing-entities.html. BY

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 12. Optionally, provide User Name and Organization.

Step 13. Click Next.



Citrix 2203 LTSR CU1 - Provisioning Server x64

Customer Information

Please enter your information.

User Name: Windows User

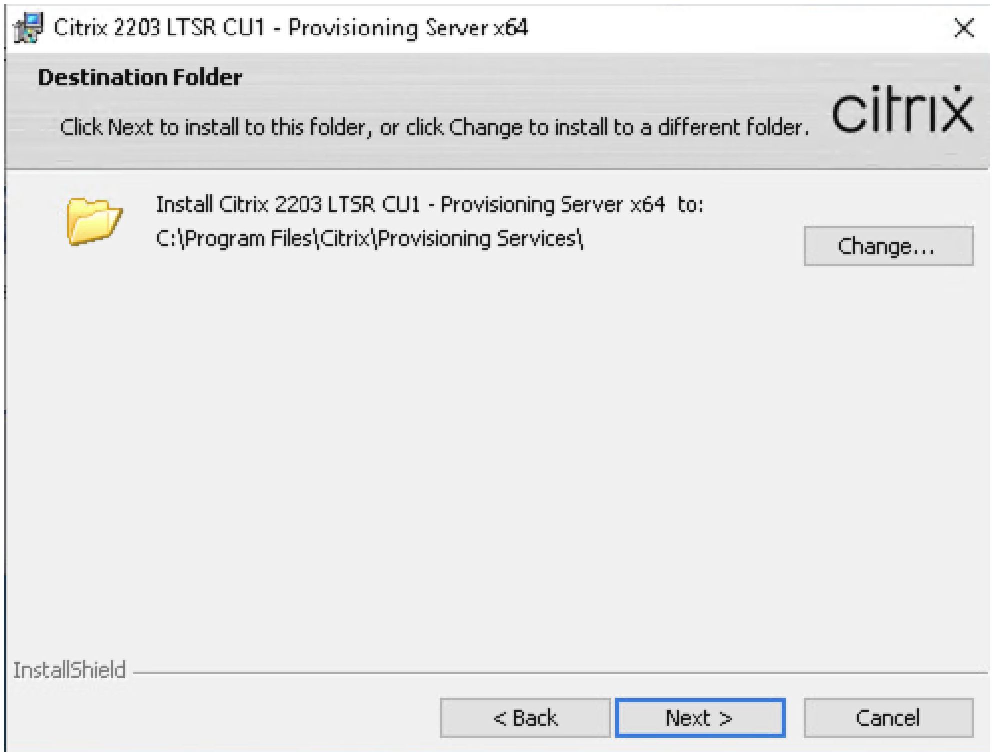
Organization:

Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Windows User)

Step 14. Accept the default path.



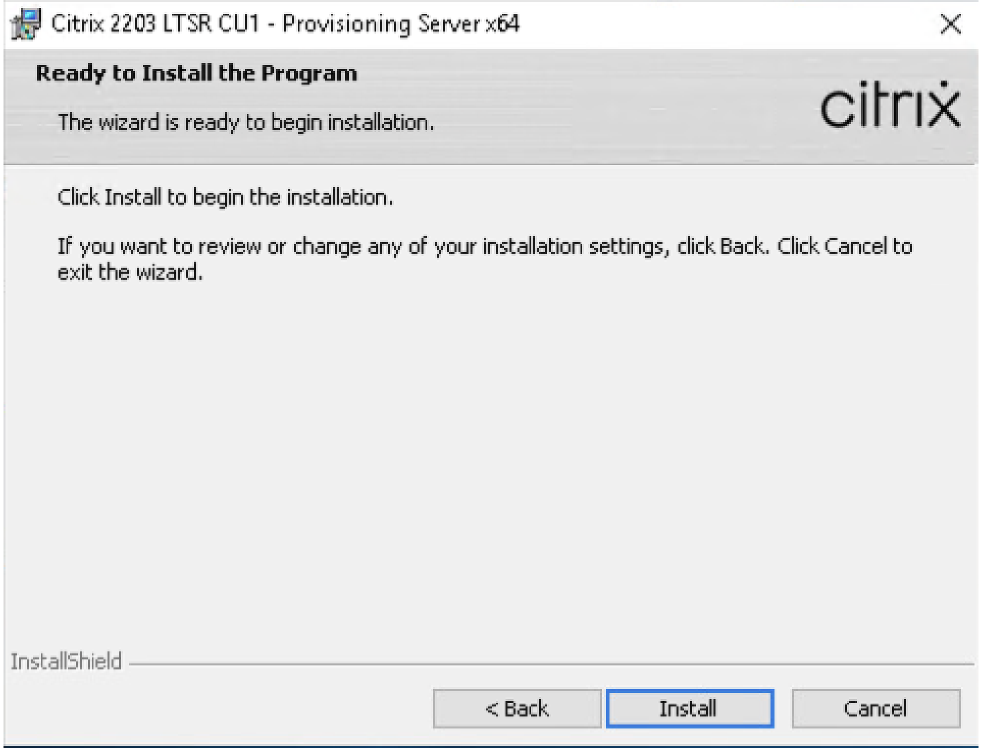
Citrix 2203 LTSR CU1 - Provisioning Server x64

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Citrix 2203 LTSR CU1 - Provisioning Server x64 to:
C:\Program Files\Citrix\Provisioning Services\

Step 15. Click Install.



Citrix 2203 LTSR CU1 - Provisioning Server x64

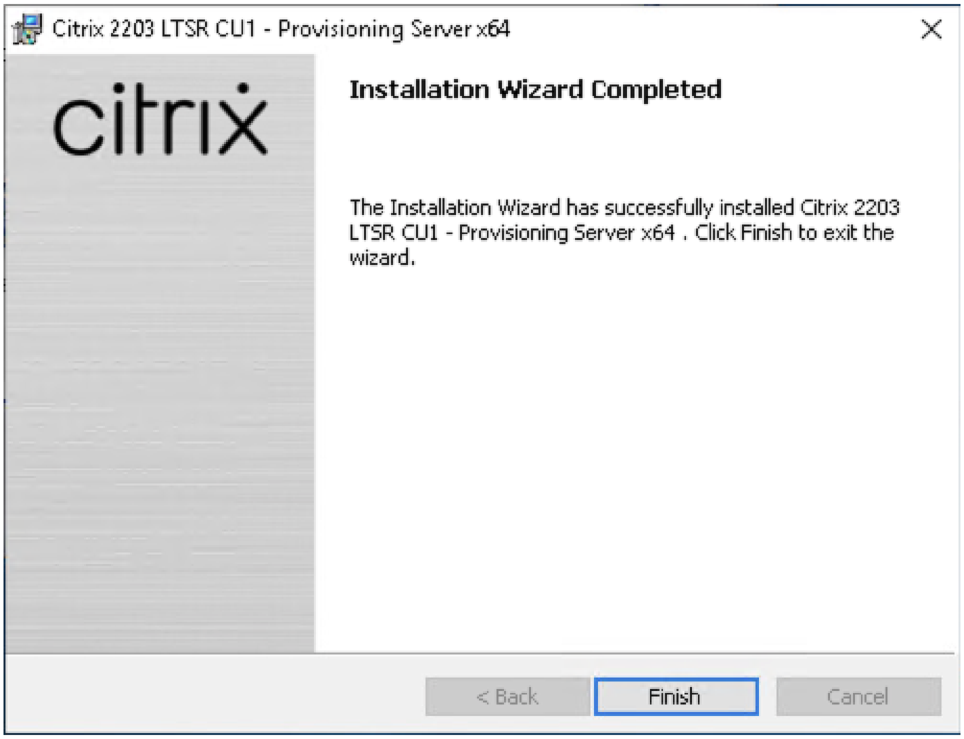
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 16. Click Finish after successful installation.

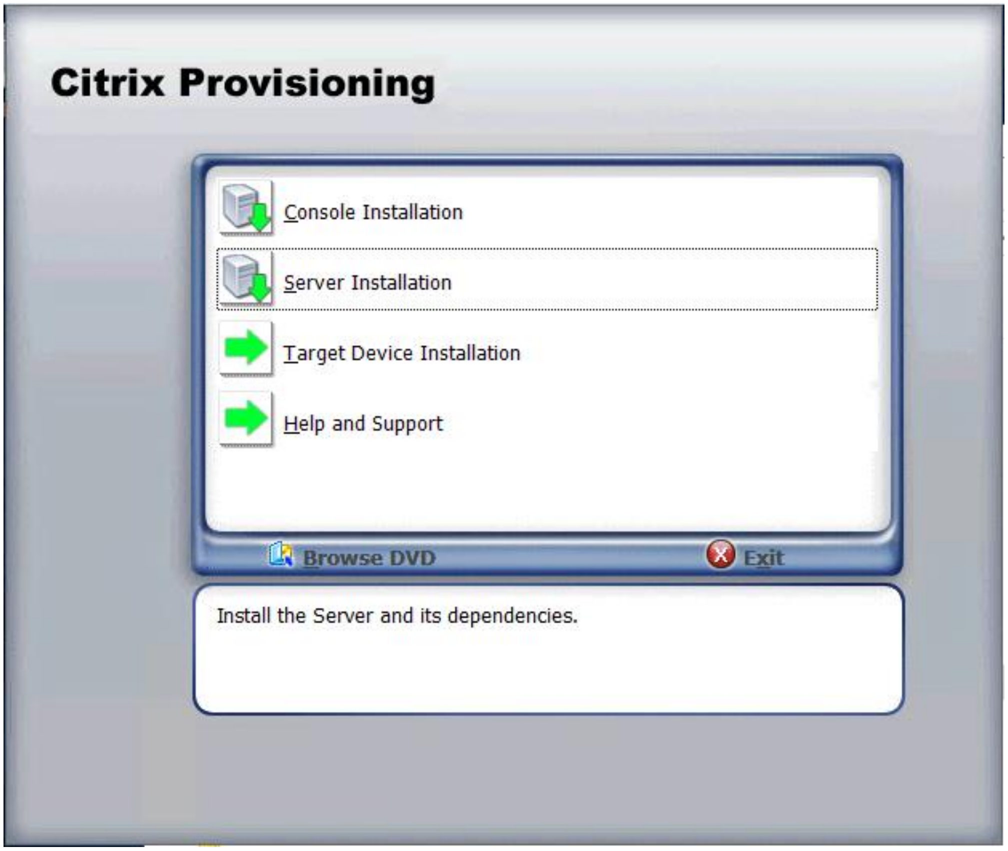


Citrix 2203 LTSR CU1 - Provisioning Server x64

Installation Wizard Completed

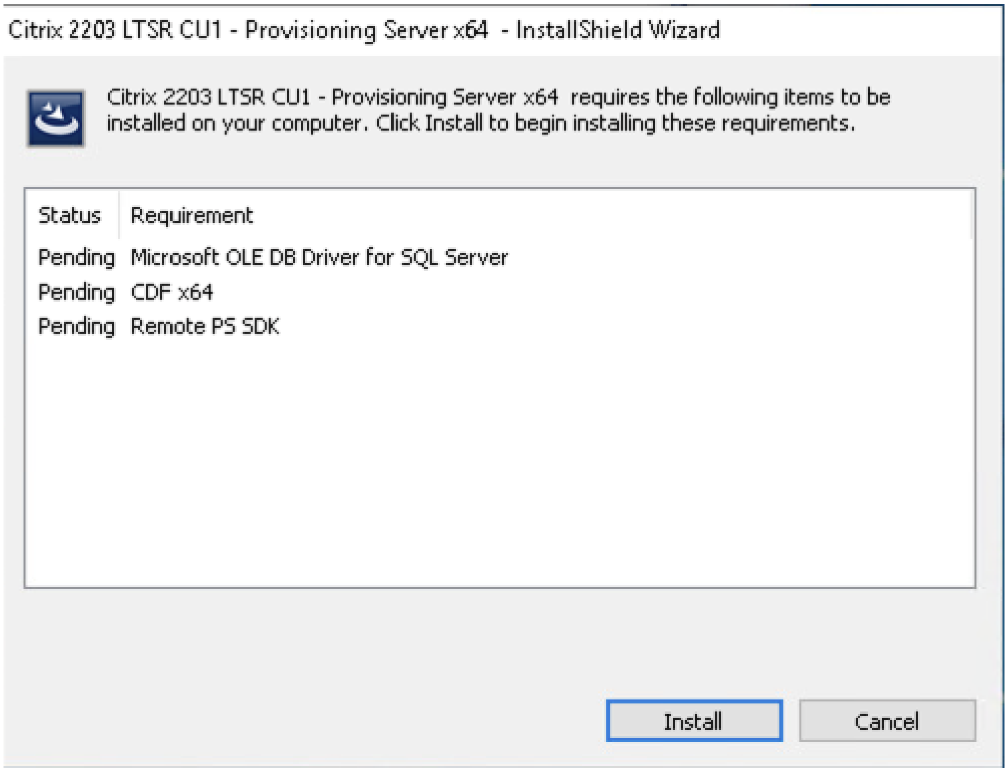
The Installation Wizard has successfully installed Citrix 2203 LTSR CU1 - Provisioning Server x64 . Click Finish to exit the wizard.

Step 17. From the main installation screen, select Server Installation.



Install the Server and its dependencies.

Step 18. Click Install on the prerequisites dialog.

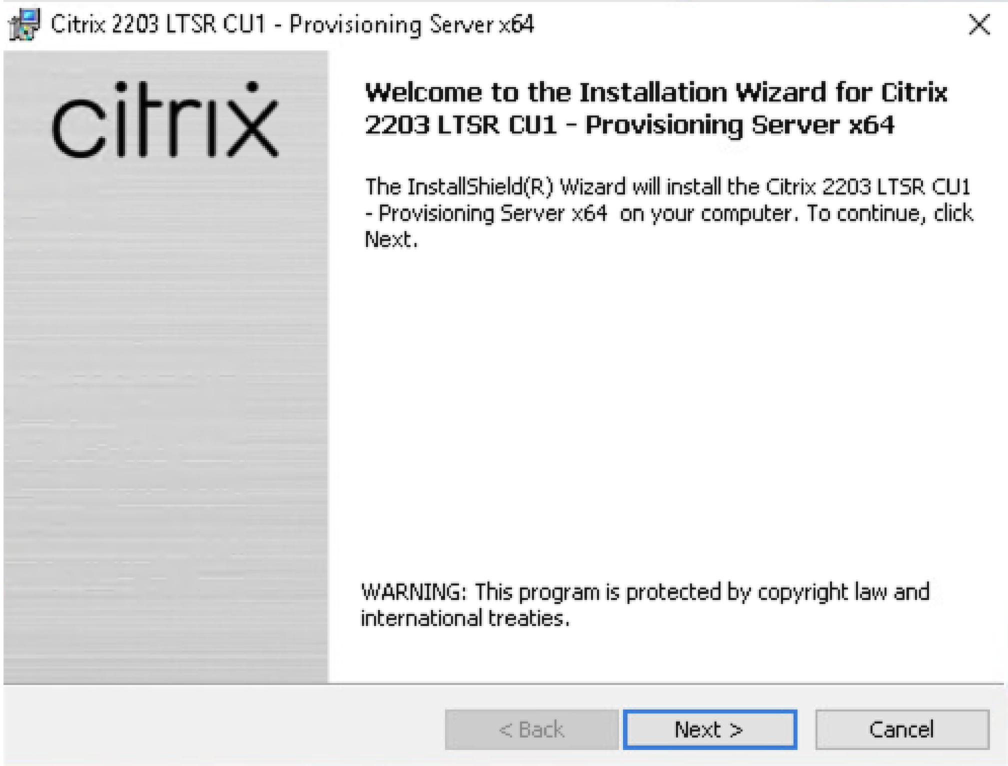


Citrix 2203 LTSR CU1 - Provisioning Server x64 - InstallShield Wizard

Citrix 2203 LTSR CU1 - Provisioning Server x64 requires the following items to be installed on your computer. Click Install to begin installing these requirements.

Status	Requirement
Pending	Microsoft OLE DB Driver for SQL Server
Pending	CDF x64
Pending	Remote PS SDK

Step 19. Click Next when the Installation wizard starts.


Citrix 2203 LTSR CU1 - Provisioning Server x64

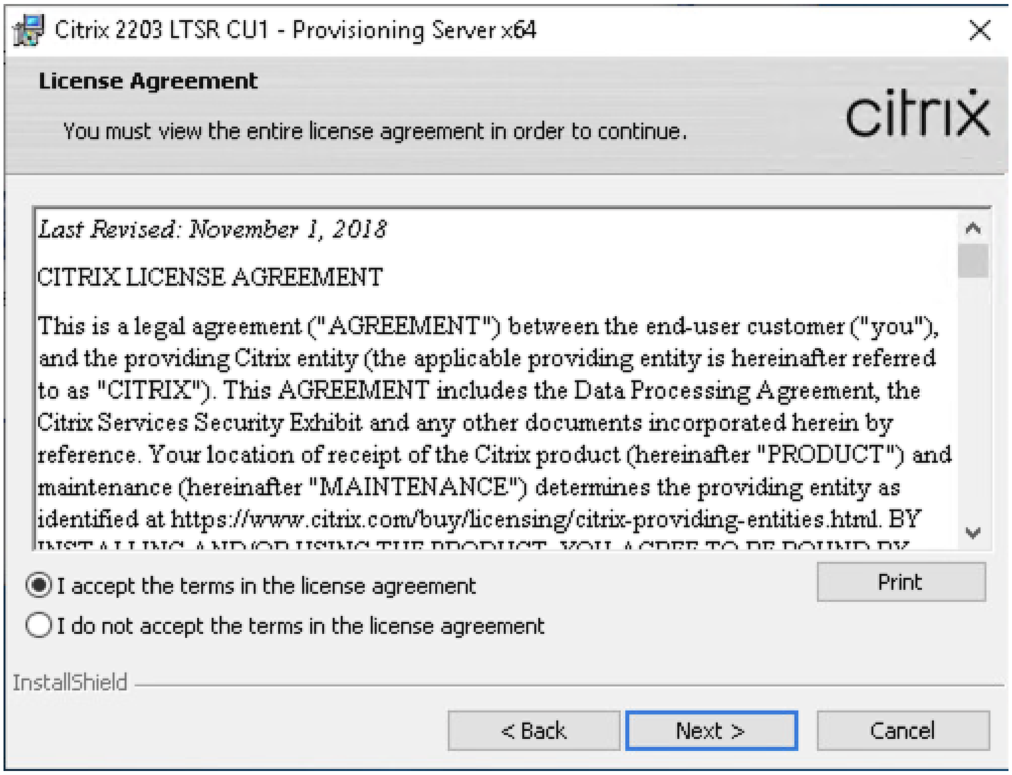
Welcome to the Installation Wizard for Citrix 2203 LTSR CU1 - Provisioning Server x64

The InstallShield(R) Wizard will install the Citrix 2203 LTSR CU1 - Provisioning Server x64 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 20. Review the license agreement terms. If acceptable, select the radio button labeled "I accept the terms in the license agreement."

Step 21. Click Next.


Citrix 2203 LTSR CU1 - Provisioning Server x64

License Agreement

You must view the entire license agreement in order to continue.

Last Revised: November 1, 2018

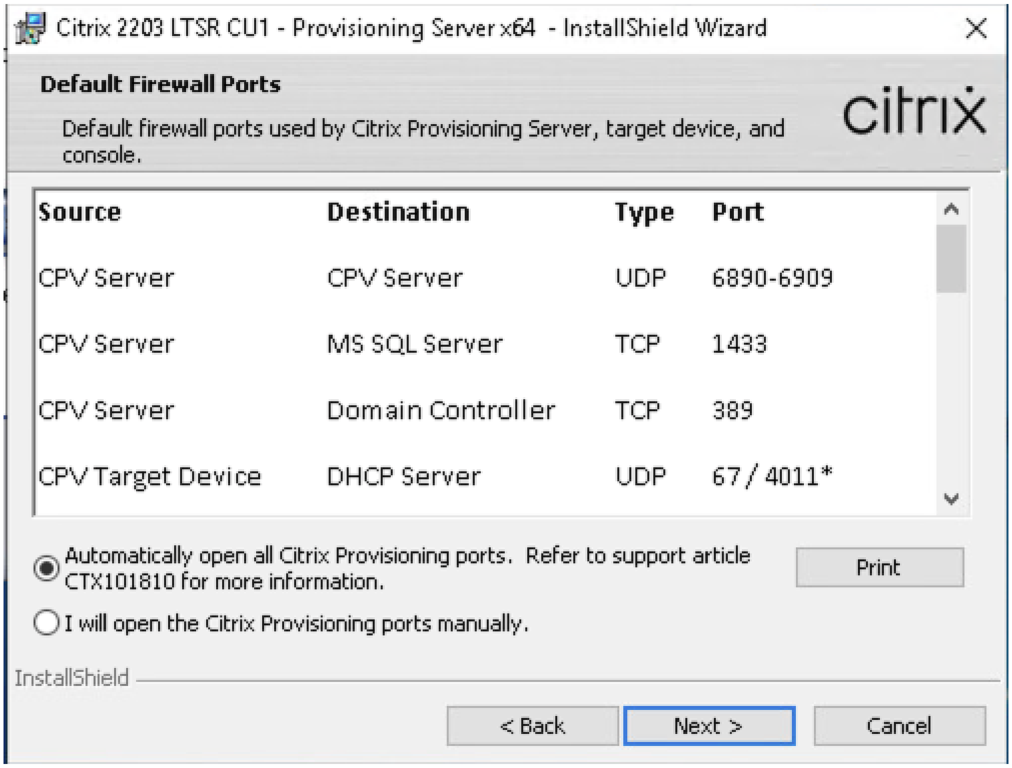
CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix-providing-entities.html. BY

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 22. Select Automatically open Citrix PVS Firewall Ports.



Citrix 2203 LTSR CU1 - Provisioning Server x64 - InstallShield Wizard

Default Firewall Ports

Default firewall ports used by Citrix Provisioning Server, target device, and console.

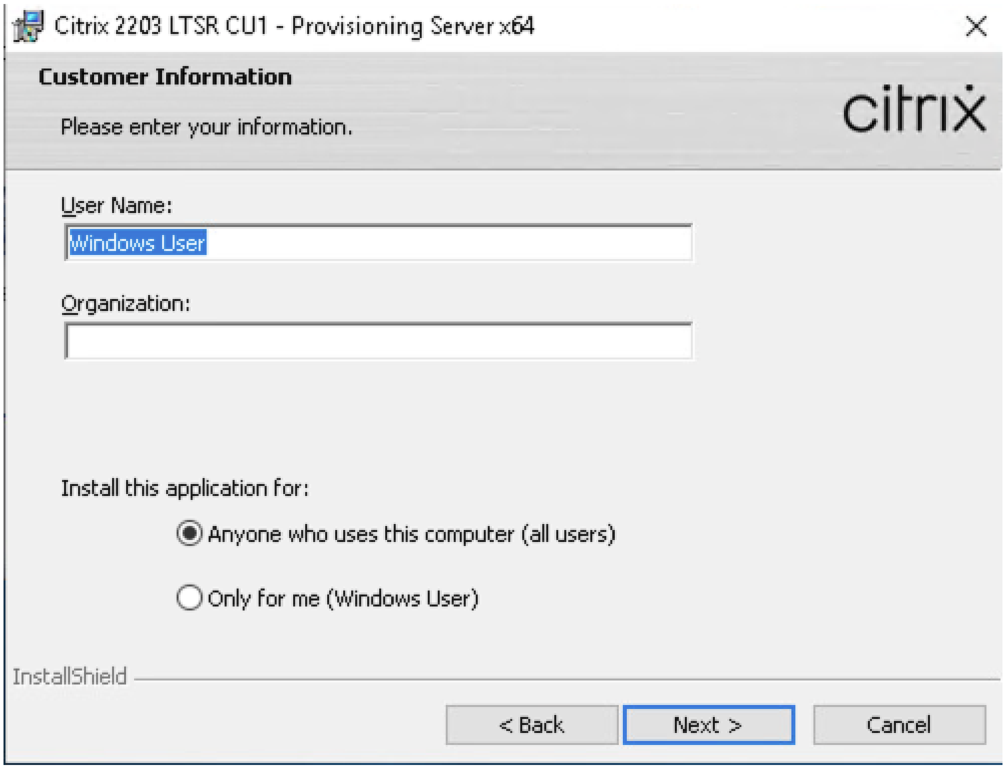
Source	Destination	Type	Port
CPV Server	CPV Server	UDP	6890-6909
CPV Server	MS SQL Server	TCP	1433
CPV Server	Domain Controller	TCP	389
CPV Target Device	DHCP Server	UDP	67 / 4011*

● Automatically open all Citrix Provisioning ports. Refer to support article CTX101810 for more information.

○ I will open the Citrix Provisioning ports manually.

Step 23. Provide User Name and Organization information. Select who will see the application.

Step 24. Click Next.



Citrix 2203 LTSR CU1 - Provisioning Server x64

Customer Information

Please enter your information.

User Name: Windows User

Organization:

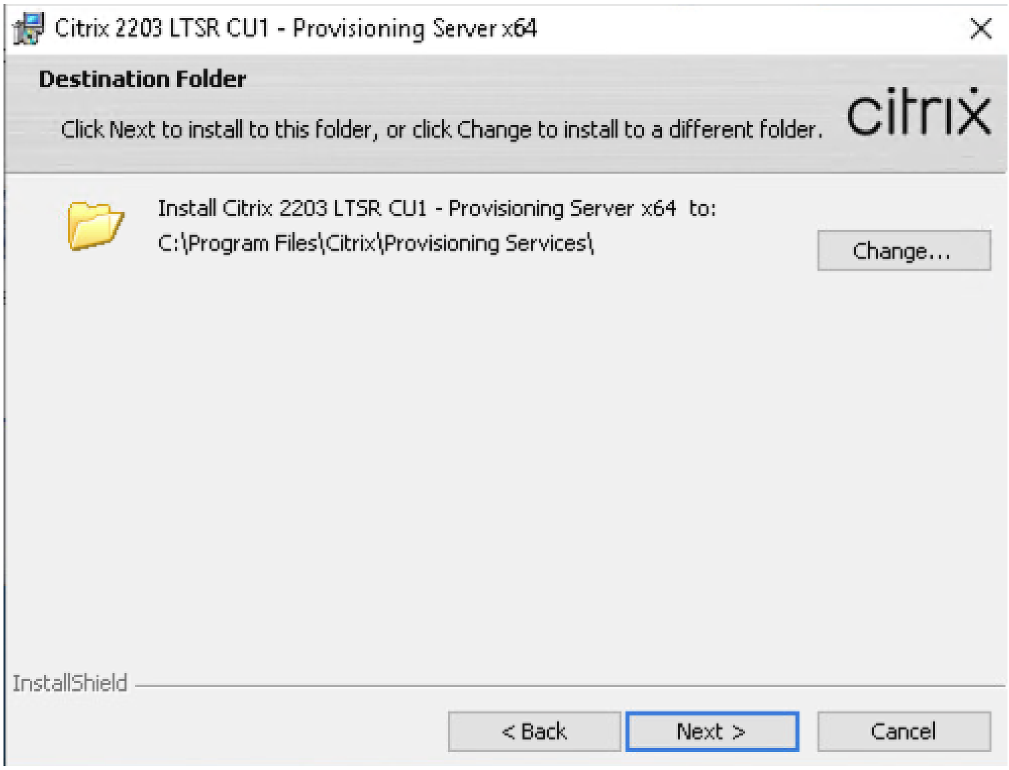
Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Windows User)

Step 25. Accept the default installation location.

Step 26. Click Next.

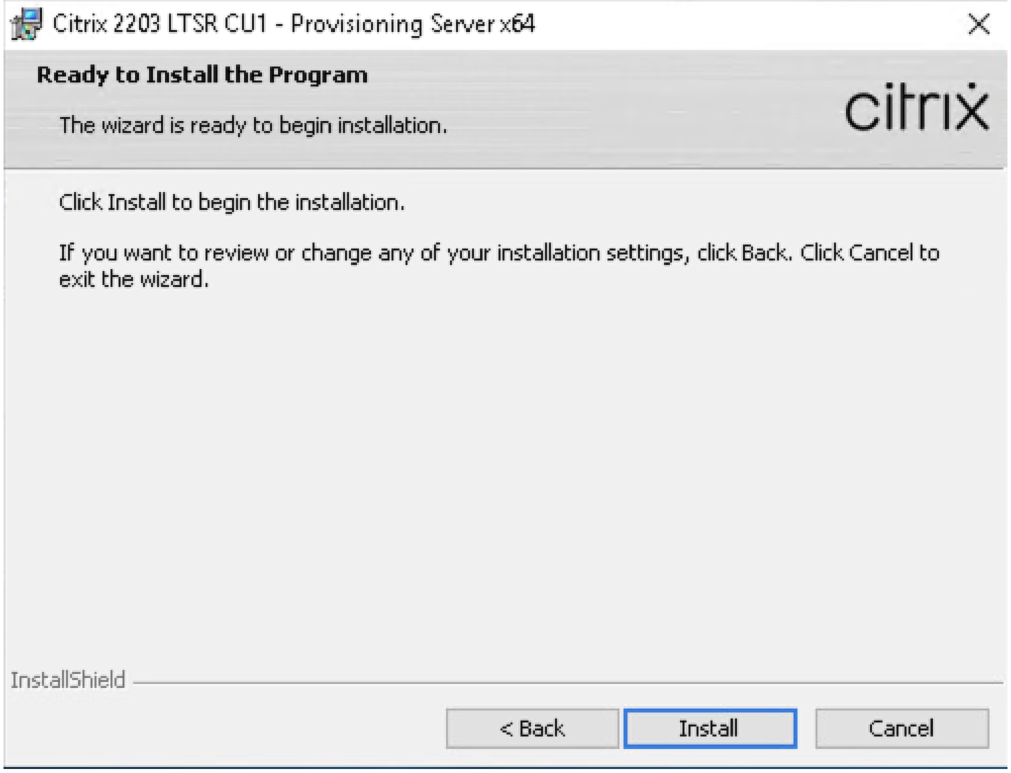

Citrix 2203 LTSR CU1 - Provisioning Server x64

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Citrix 2203 LTSR CU1 - Provisioning Server x64 to:
C:\Program Files\Citrix\Provisioning Services\

Step 27. Click Install to begin the installation.


Citrix 2203 LTSR CU1 - Provisioning Server x64

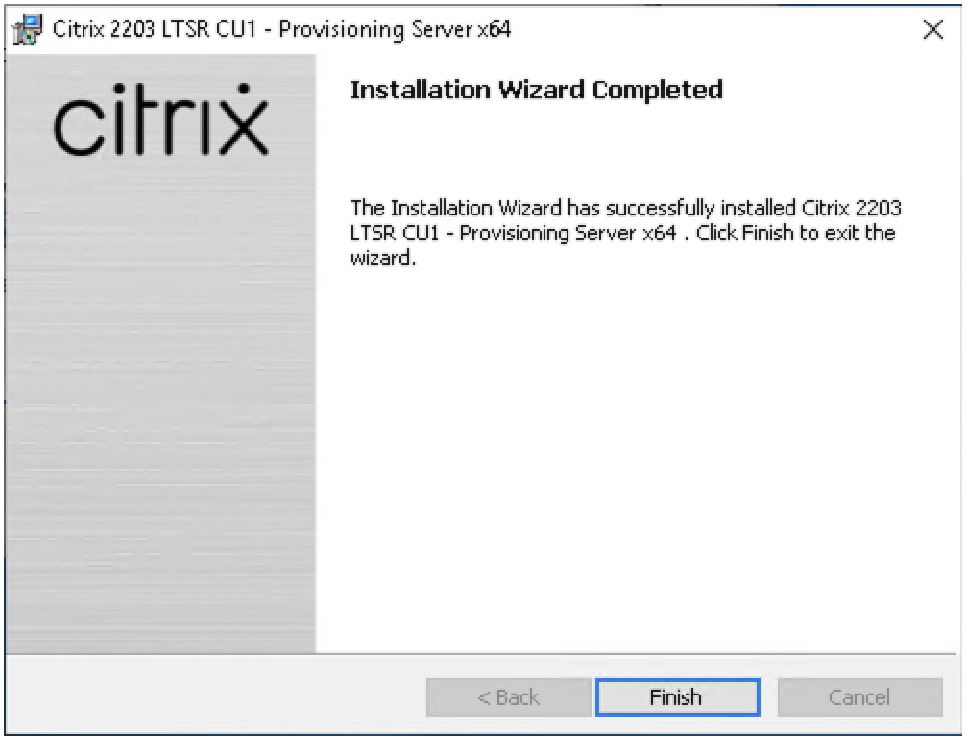
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 28. Click Finish when the install is complete.



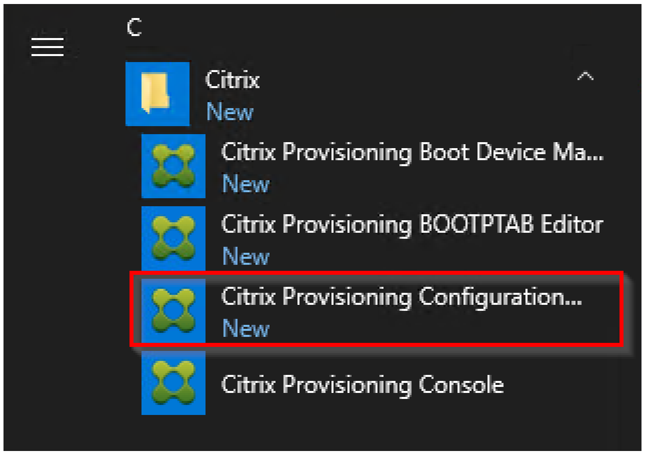
Citrix 2203 LTSR CU1 - Provisioning Server x64

Installation Wizard Completed

The Installation Wizard has successfully installed Citrix 2203 LTSR CU1 - Provisioning Server x64 . Click Finish to exit the wizard.

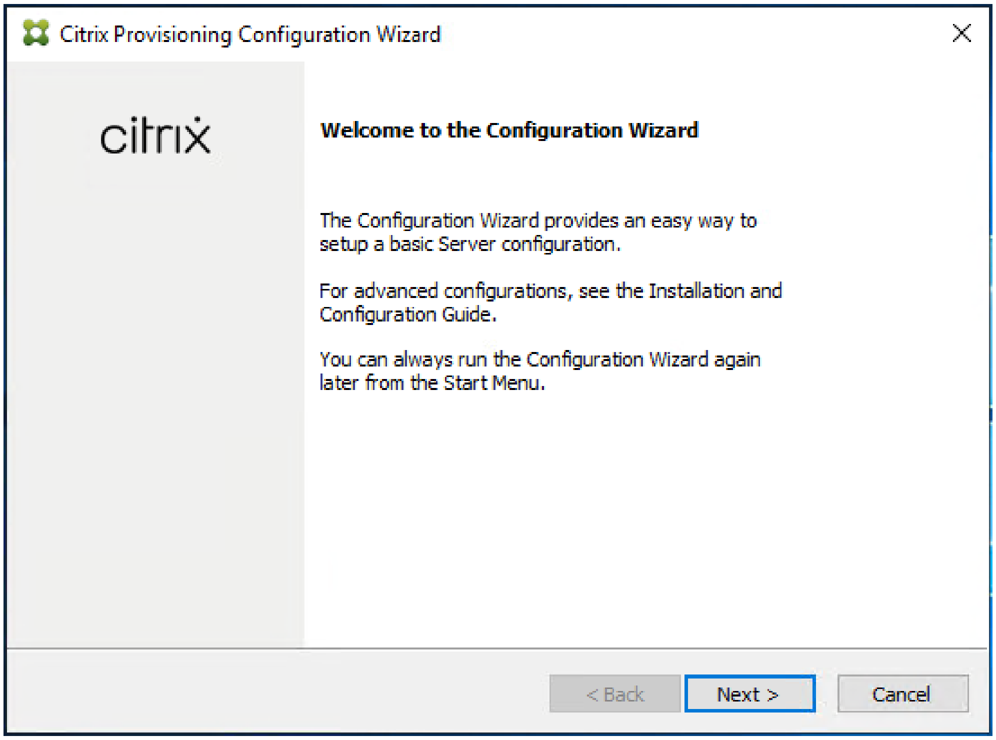
Procedure 3. Configure Citrix Provisioning Services

Step 1. Start PVS Configuration Wizard.



C
Citrix
New
Citrix Provisioning Boot Device Ma...
New
Citrix Provisioning BOOTPTAB Editor
New
Citrix Provisioning Configuration...
New
Citrix Provisioning Console

Step 2. Click Next.



Citrix Provisioning Configuration Wizard

Welcome to the Configuration Wizard

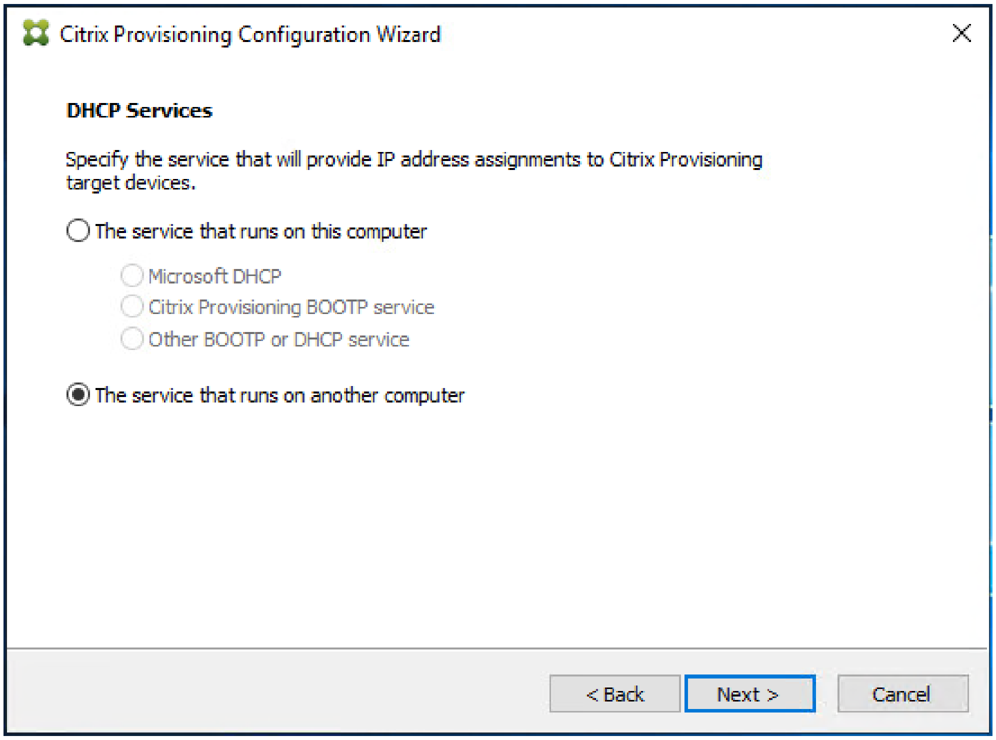
The Configuration Wizard provides an easy way to setup a basic Server configuration.

For advanced configurations, see the Installation and Configuration Guide.

You can always run the Configuration Wizard again later from the Start Menu.

Step 3. Since the PVS server is not the DHCP server for the environment, select the radio button labeled, "The service that runs on another computer."

Step 4. Click Next.



Citrix Provisioning Configuration Wizard

DHCP Services

Specify the service that will provide IP address assignments to Citrix Provisioning target devices.

○ The service that runs on this computer

○ Microsoft DHCP

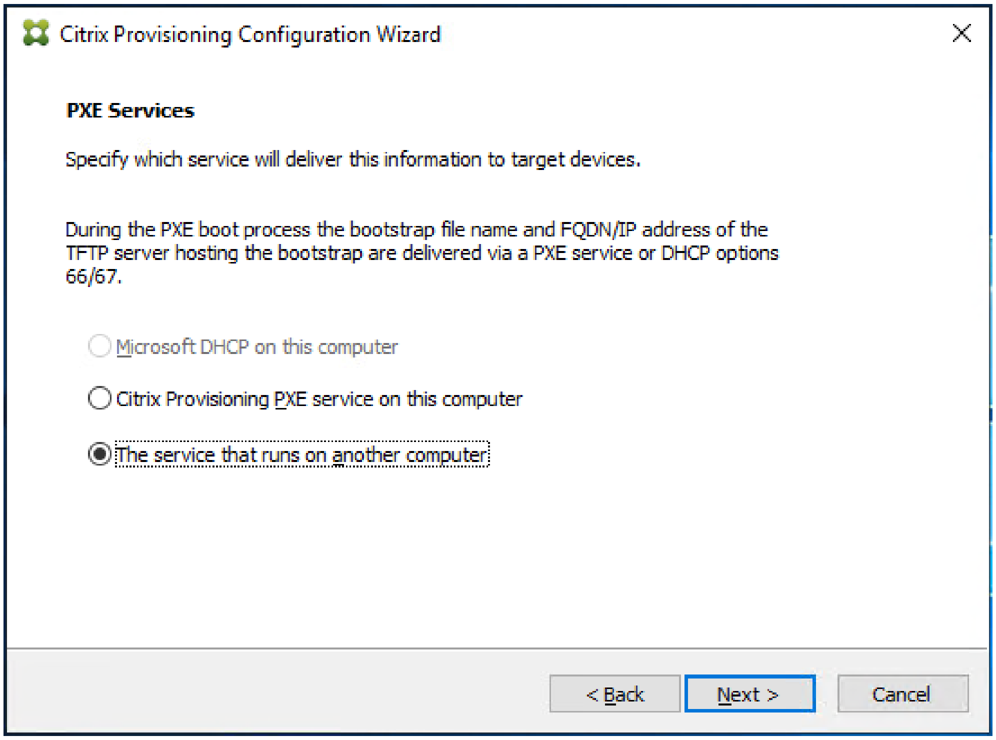
○ Citrix Provisioning BOOTP service

○ Other BOOTP or DHCP service

● The service that runs on another computer

Step 5. Since DHCP boot options are used for TFTP services, select the radio button labeled, "The service that runs on another computer."

Step 6. Click Next.



PXE Services

Specify which service will deliver this information to target devices.

During the PXE boot process the bootstrap file name and FQDN/IP address of the TFTP server hosting the bootstrap are delivered via a PXE service or DHCP options 66/67.

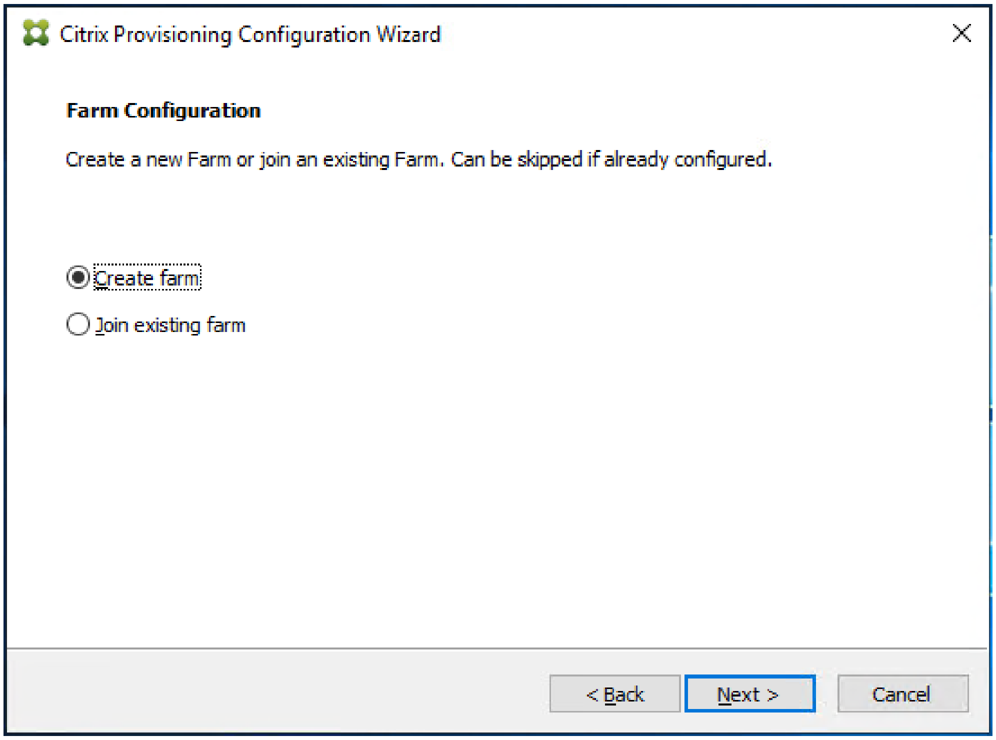
○ Microsoft DHCP on this computer

○ Citrix Provisioning PXE service on this computer

● The service that runs on another computer

Step 7. Since this is the first server in the farm, select the radio button labeled, "Create farm."

Step 8. Click Next.



Farm Configuration

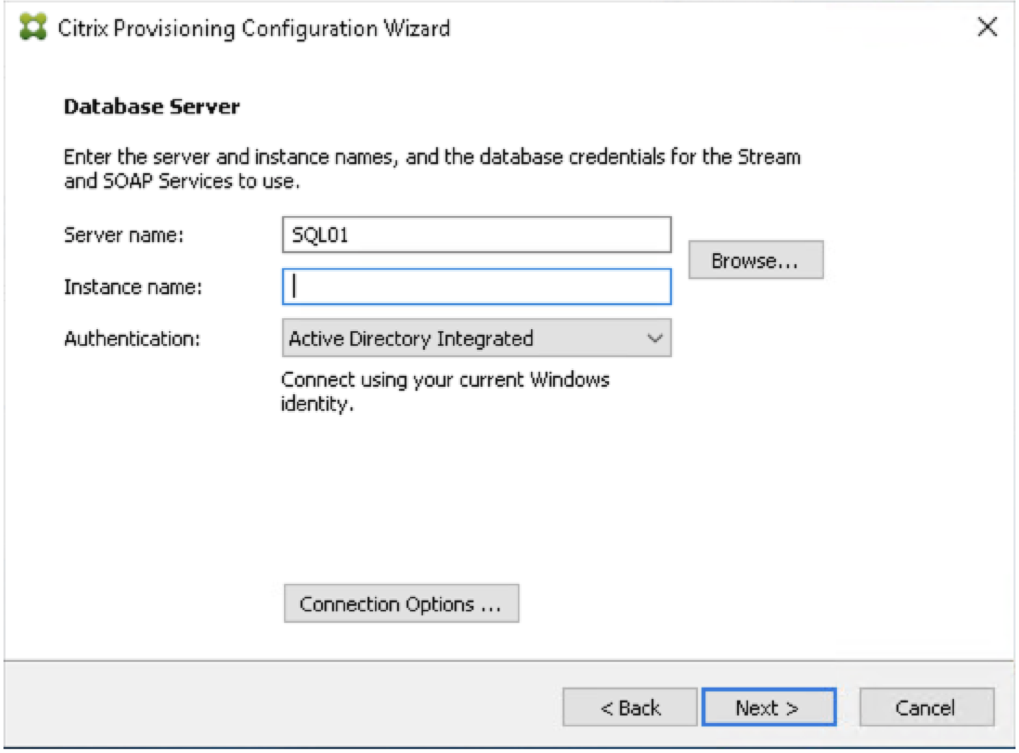
Create a new Farm or join an existing Farm. Can be skipped if already configured.

● Create farm

○ Join existing farm

Step 9. Enter the FQDN of the SQL server.

Step 10. Click Next.



Database Server

Enter the server and instance names, and the database credentials for the Stream and SOAP Services to use.

Server name: SQL01

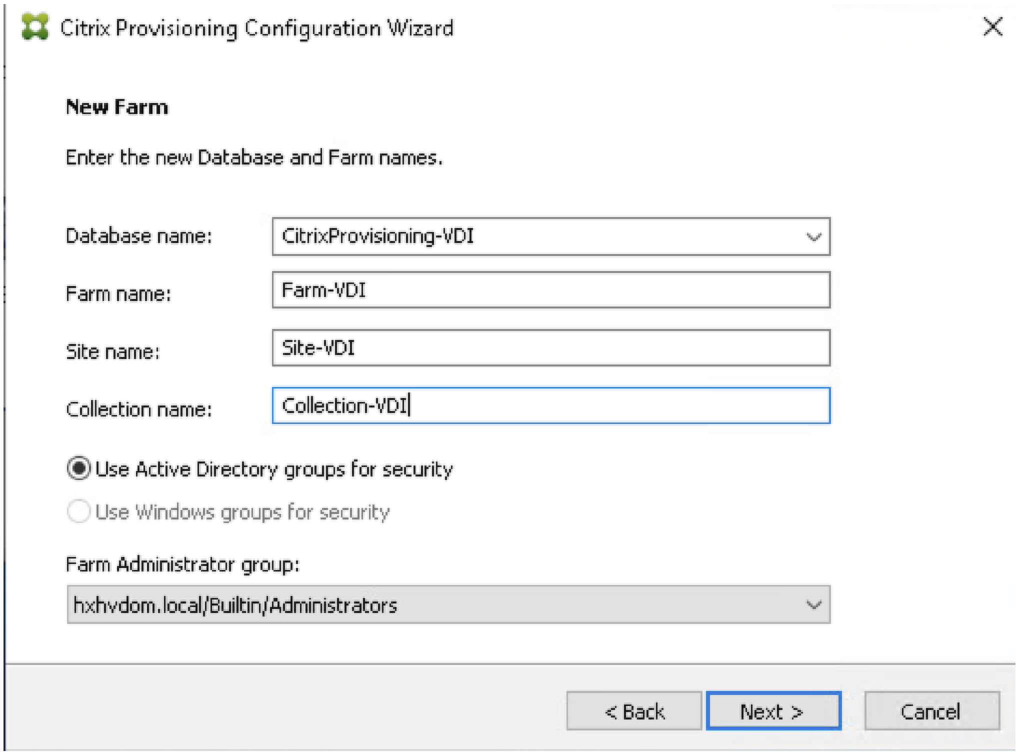
Instance name:

Authentication: Active Directory Integrated

Connect using your current Windows identity.

Step 11. Provide the Database, Farm, Site, and Collection name.

Step 12. Click Next.



New Farm

Enter the new Database and Farm names.

Database name: CitrixProvisioning-VDI

Farm name: Farm-VDI

Site name: Site-VDI

Collection name: Collection-VDI

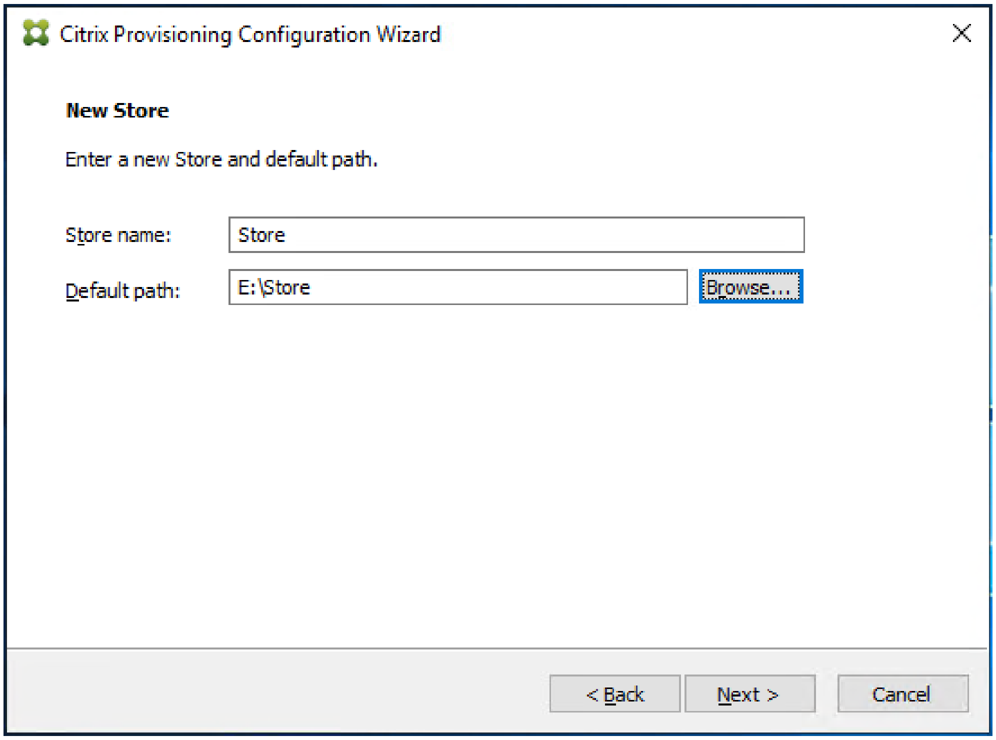
● Use Active Directory groups for security

○ Use Windows groups for security

Farm Administrator group: hxhvdom.local/Builtin/Administrators

Step 13. Provide the vDisk Store details.

Step 14. Click Next.



Citrix Provisioning Configuration Wizard

New Store

Enter a new Store and default path.

Store name: Store

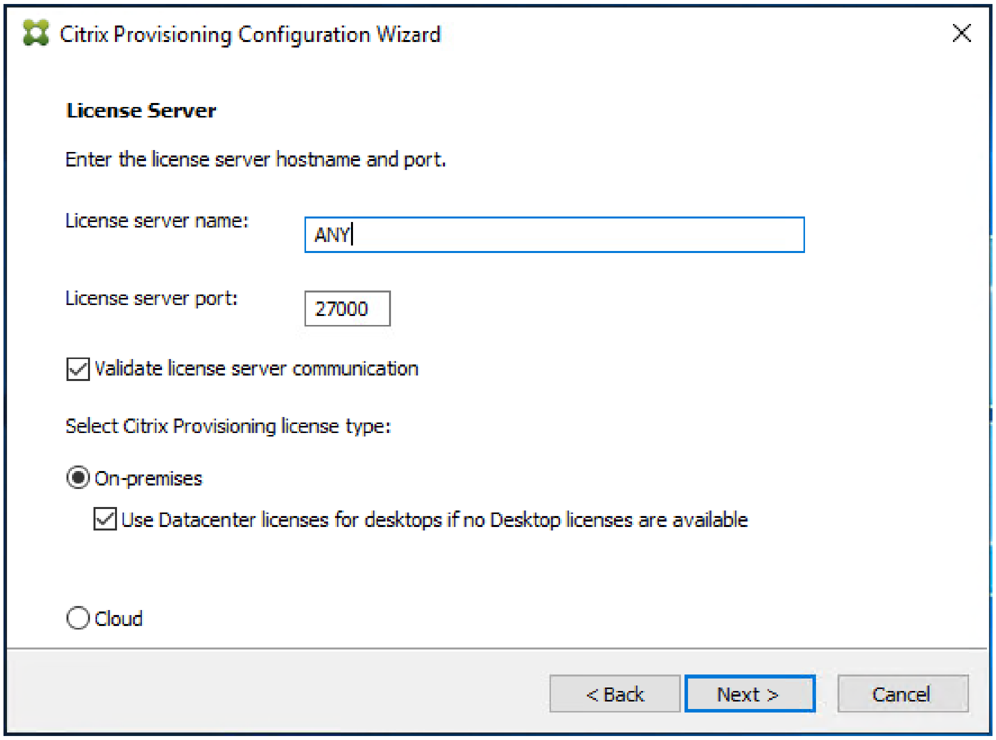
Default path: E:\Store

Step 15. For large scale PVS environment, it is recommended to create the share using support for CIFS/SMB3 on an enterprise ready File Server.

Step 16. Provide the FQDN of the license server.

Step 17. Optionally, provide a port number if changed on the license server.

Step 18. Click Next.



Citrix Provisioning Configuration Wizard

License Server

Enter the license server hostname and port.

License server name: ANY

License server port: 27000

☑ Validate license server communication

Select Citrix Provisioning license type:

● On-premises

☑ Use Datacenter licenses for desktops if no Desktop licenses are available

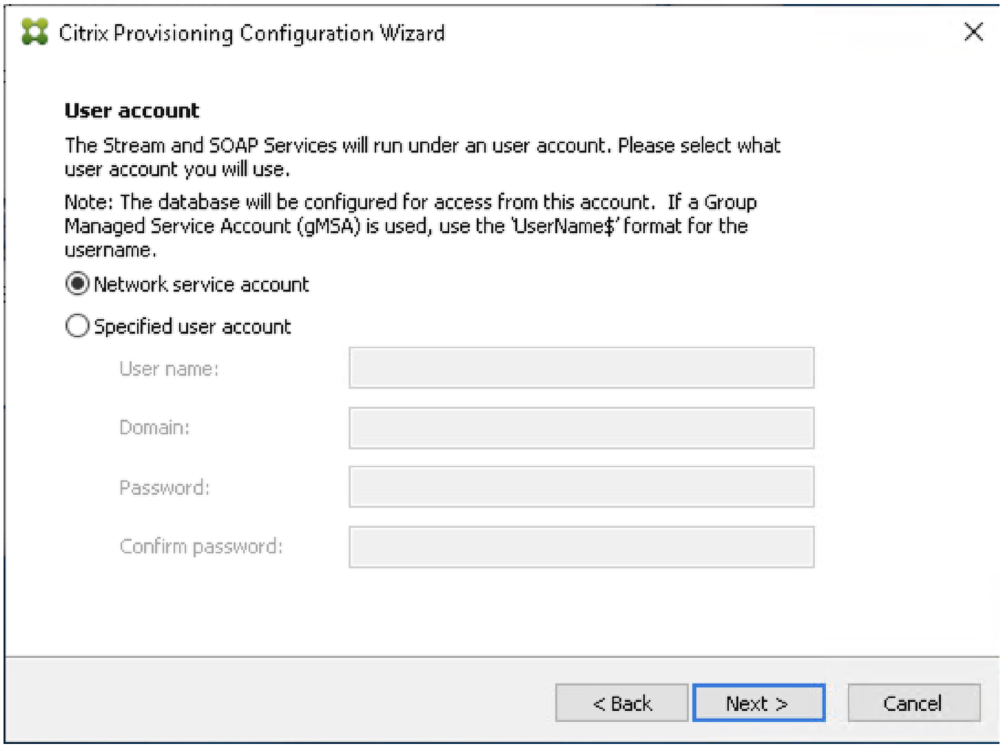
○ Cloud

Step 19. If an Active Directory service account is not already setup for the PVS servers, create that account prior to clicking Next on this dialog.

Step 20. Select the Specified user account radio button.

Step 21. Complete the User name, Domain, Password, and Confirm password fields, using the PVS account information created earlier.

Step 22. Click Next.



Citrix Provisioning Configuration Wizard

User account

The Stream and SOAP Services will run under an user account. Please select what user account you will use.

Note: The database will be configured for access from this account. If a Group Managed Service Account (gMSA) is used, use the 'UserName$' format for the username.

● Network service account

○ Specified user account

User name:

Domain:

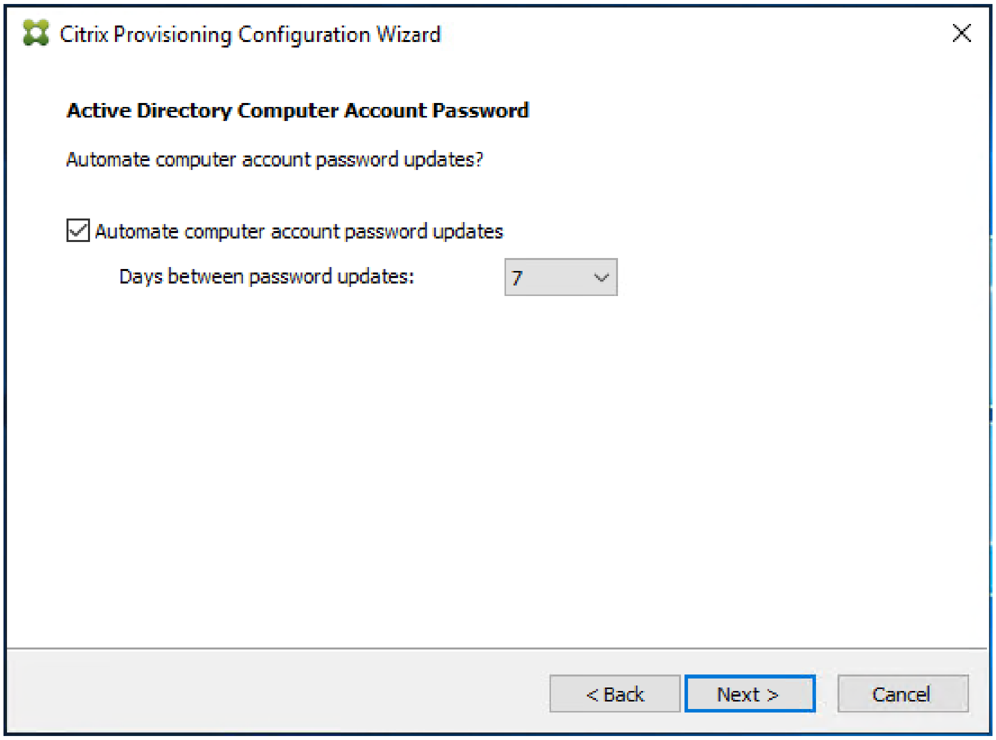
Password:

Confirm password:

Step 23. Set the Days between password updates to 7.

Note: This will vary per environment. "7 days" for the configuration was appropriate for testing purposes.

Step 24. Click Next.



Citrix Provisioning Configuration Wizard

Active Directory Computer Account Password

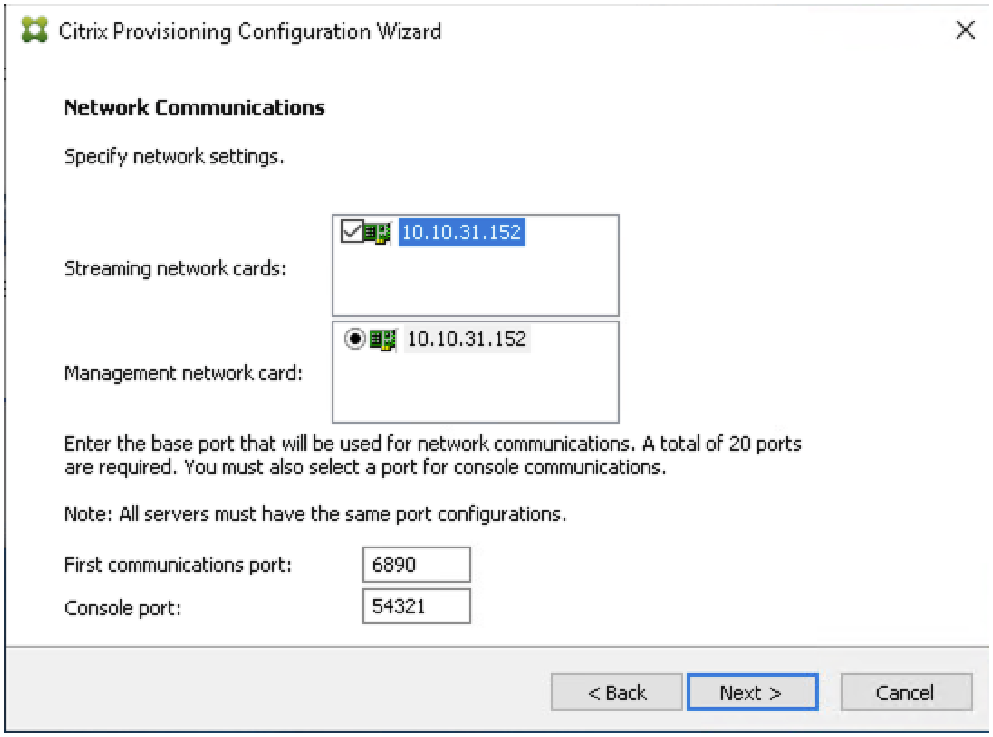
Automate computer account password updates?

☑ Automate computer account password updates

Days between password updates: 7

Step 25. Keep the defaults for the network cards.

Step 26. Click Next.



Citrix Provisioning Configuration Wizard

Network Communications

Specify network settings.

Streaming network cards: ☑ 10.10.31.152

Management network card: ● 10.10.31.152

Enter the base port that will be used for network communications. A total of 20 ports are required. You must also select a port for console communications.

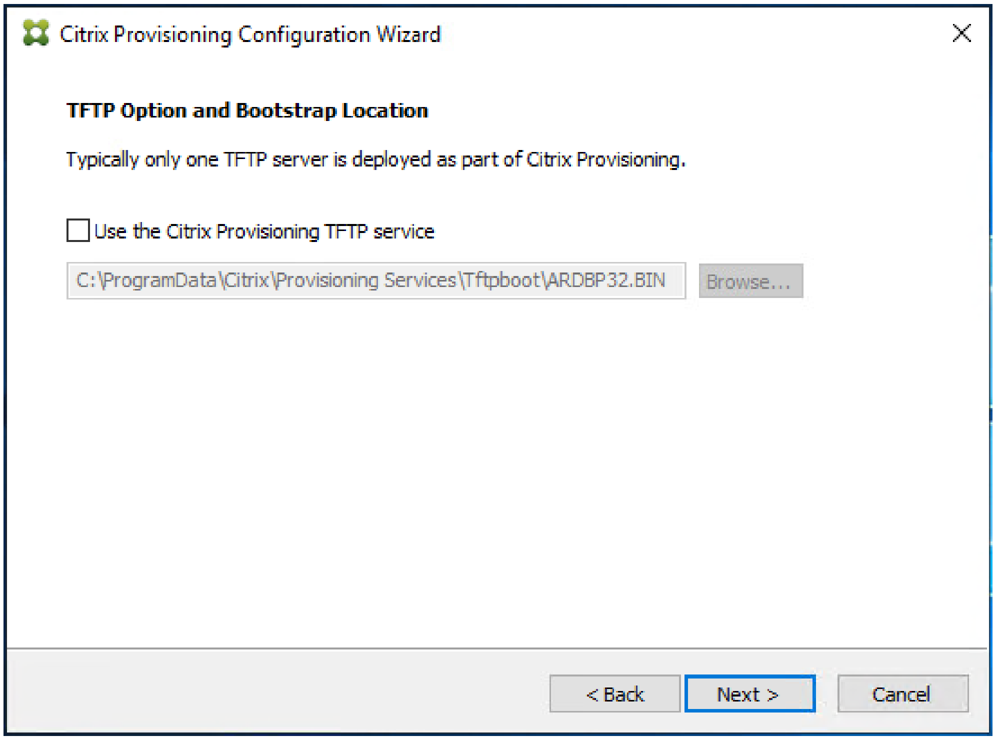
Note: All servers must have the same port configurations.

First communications port: 6890

Console port: 54321

Step 27. Select Use the Provisioning Services TFTP service checkbox.

Step 28. Click Next.



Citrix Provisioning Configuration Wizard

TFTP Option and Bootstrap Location

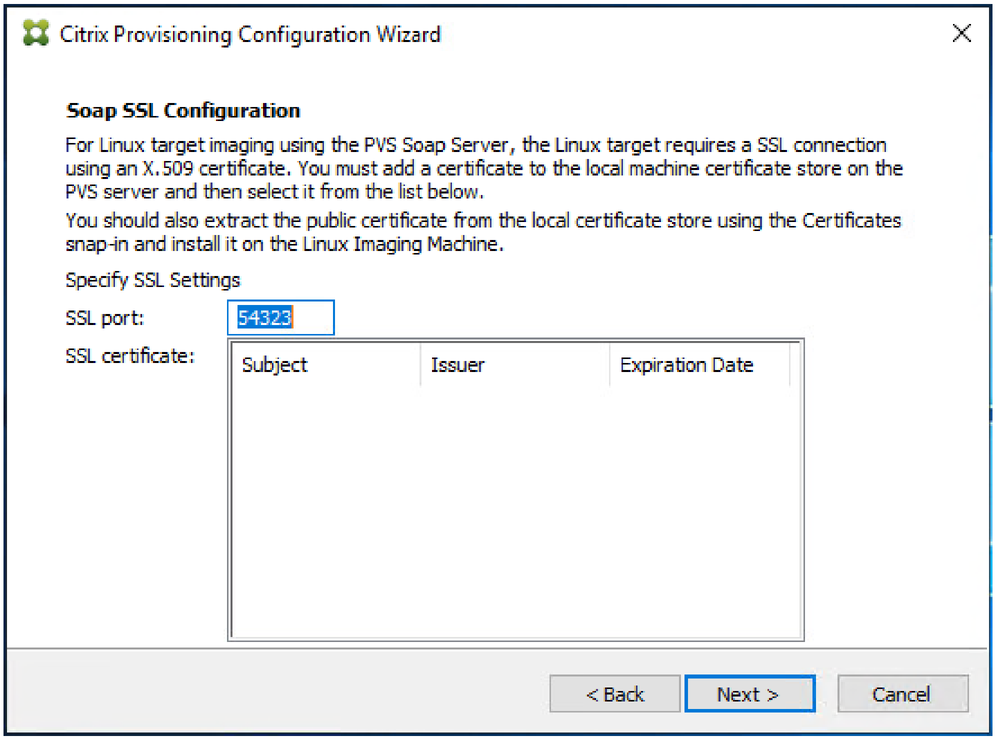
Typically only one TFTP server is deployed as part of Citrix Provisioning.

☐ Use the Citrix Provisioning TFTP service

C:\ProgramData\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN

Step 29. If Soap Server is used, provide details.

Step 30. Click Next.



Citrix Provisioning Configuration Wizard

Soap SSL Configuration

For Linux target imaging using the PVS Soap Server, the Linux target requires a SSL connection using an X.509 certificate. You must add a certificate to the local machine certificate store on the PVS server and then select it from the list below.

You should also extract the public certificate from the local certificate store using the Certificates snap-in and install it on the Linux Imaging Machine.

Specify SSL Settings

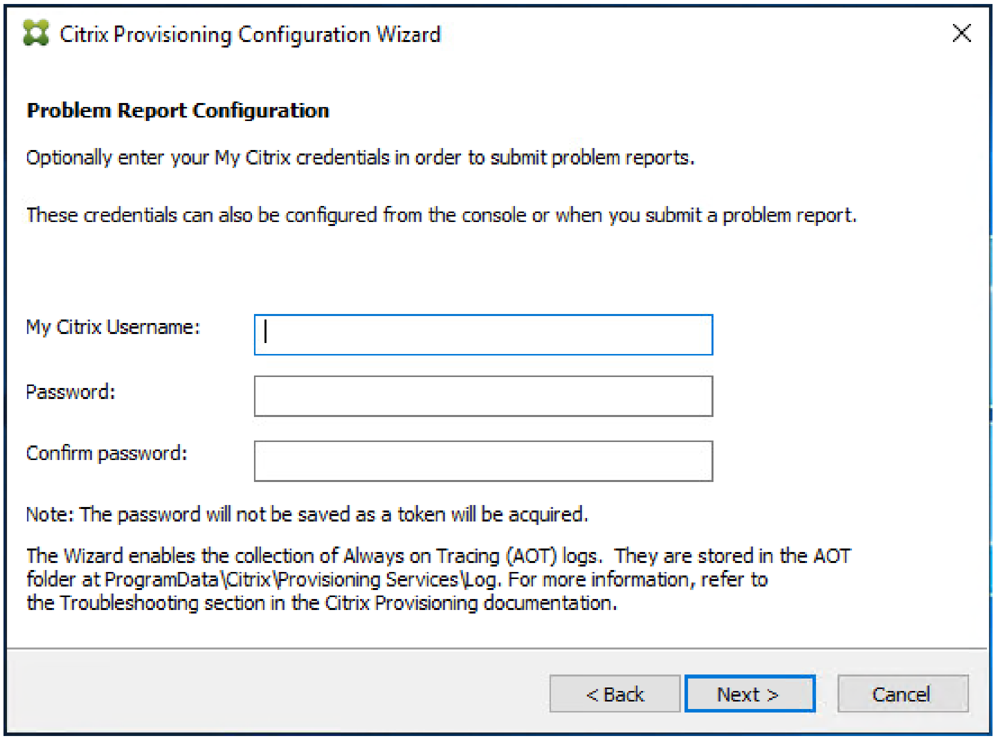
SSL port: 54323

SSL certificate:

Subject	Issuer	Expiration Date

Step 31. If desired fill in Problem Report Configuration.

Step 32. Click Next.



Problem Report Configuration

Optionally enter your My Citrix credentials in order to submit problem reports.

These credentials can also be configured from the console or when you submit a problem report.

My Citrix Username:

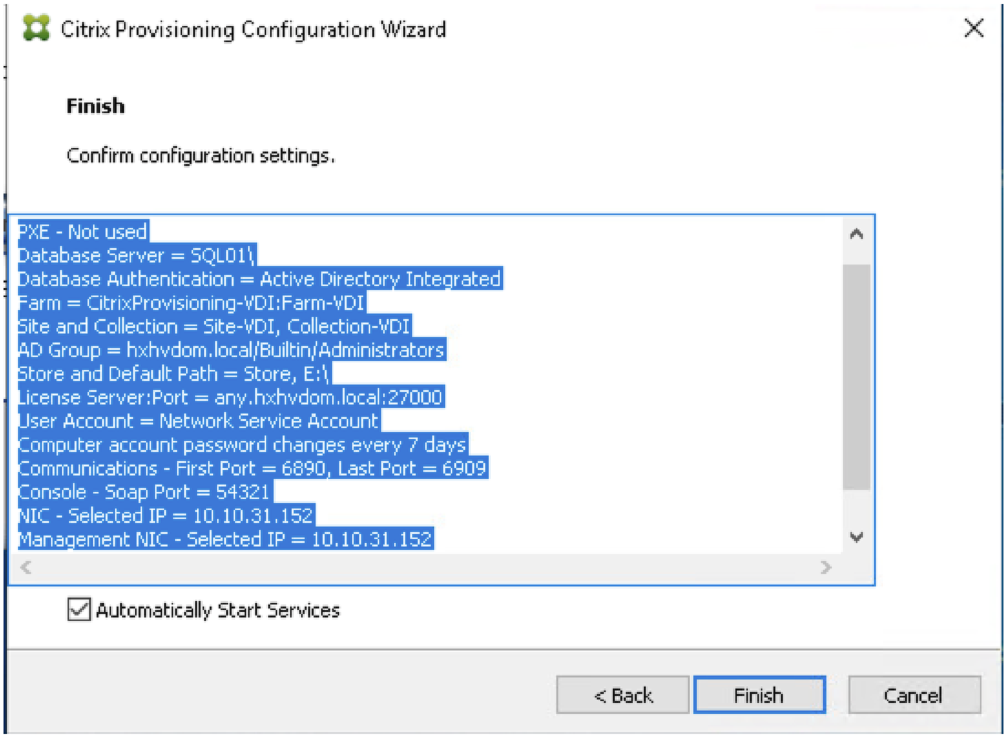
Password:

Confirm password:

Note: The password will not be saved as a token will be acquired.

The Wizard enables the collection of Always on Tracing (AOT) logs. They are stored in the AOT folder at ProgramData\Citrix\Provisioning Services\Log. For more information, refer to the Troubleshooting section in the Citrix Provisioning documentation.

Step 33. Click Finish to start the installation.



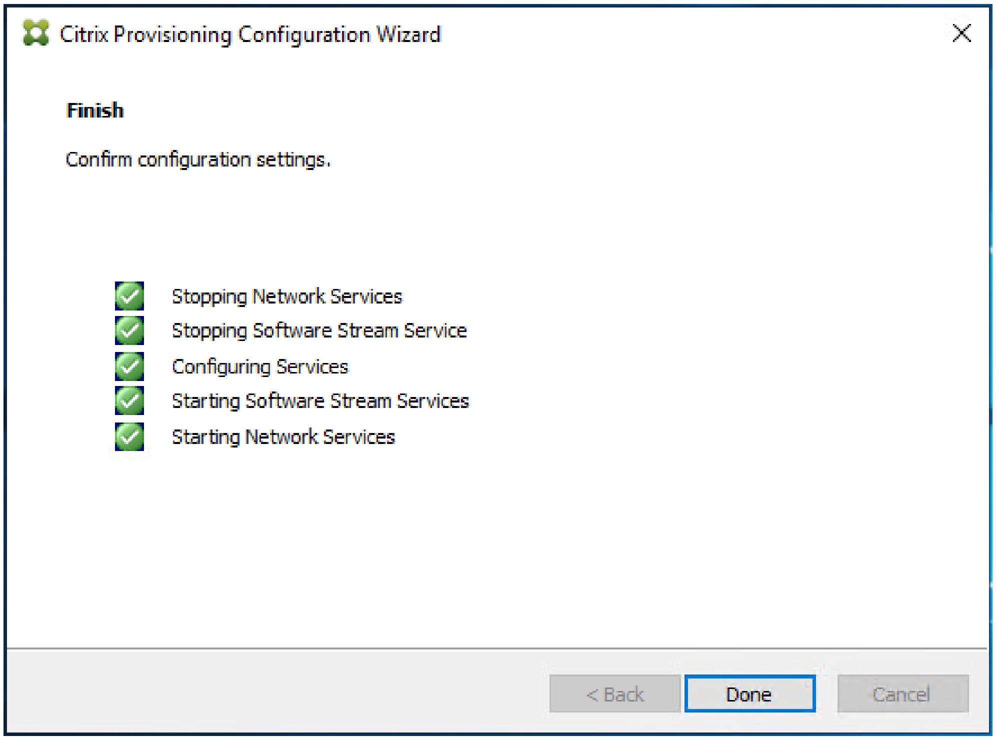
Finish

Confirm configuration settings.

```
PXE - Not used
Database Server = SQL01\
Database Authentication = Active Directory Integrated
Farm = CitrixProvisioning-VDI:Farm-VDI
Site and Collection = Site-VDI, Collection-VDI
AD Group = hxhvdom.local/Builtin/Administrators
Store and Default Path = Store, E:\
License Server:Port = any.hxhvdom.local:27000
User Account = Network Service Account
Computer account password changes every 7 days
Communications - First Port = 6890, Last Port = 6909
Console - Soap Port = 54321
NIC - Selected IP = 10.10.31.152
Management NIC - Selected IP = 10.10.31.152
```

☑ Automatically Start Services

Step 34. When the installation is completed, click Done.


Citrix Provisioning Configuration Wizard

Finish

Confirm configuration settings.

- ✓ Stopping Network Services
- ✓ Stopping Software Stream Service
- ✓ Configuring Services
- ✓ Starting Software Stream Services
- ✓ Starting Network Services

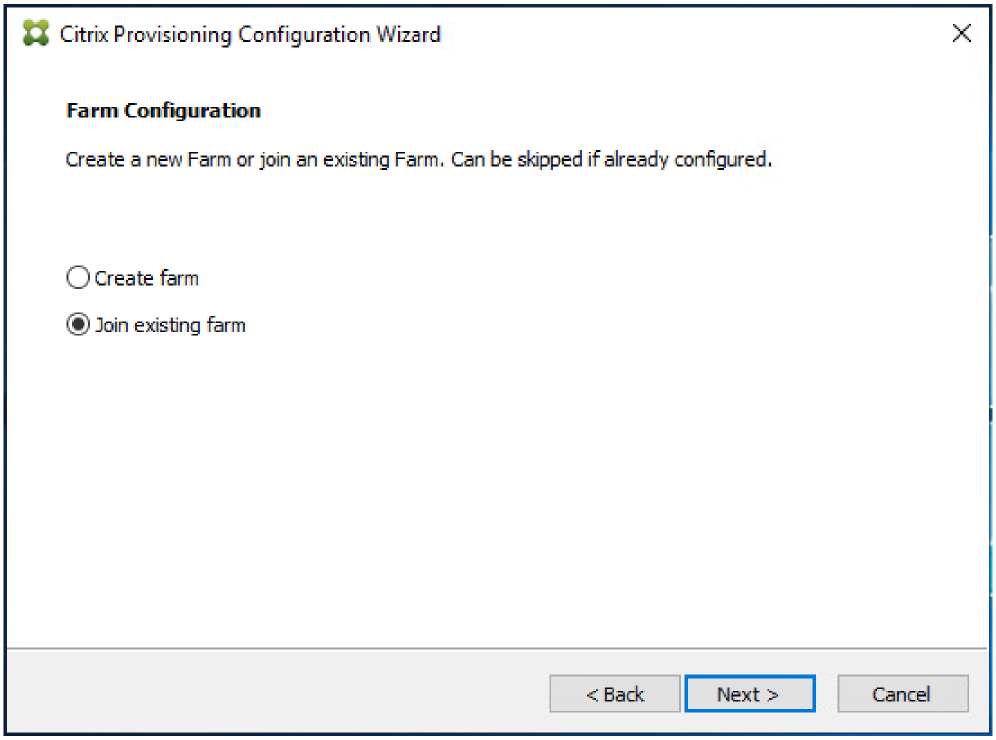
Procedure 4. Install Additional PVS Servers

Note: 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 three PVS servers.

This procedure details how to join additional Provisioning servers to the farm already configured in the previous steps.

Step 1. On the Farm Configuration dialog, select "Join existing farm."

Step 2. Click Next.



Farm Configuration

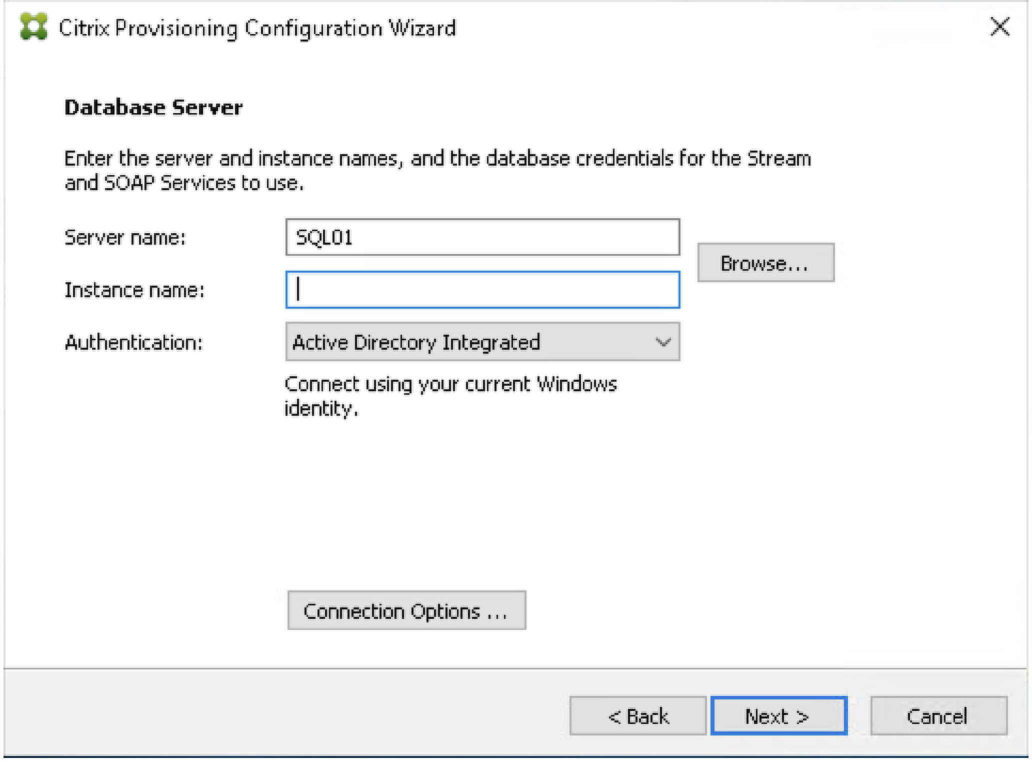
Create a new Farm or join an existing Farm. Can be skipped if already configured.

○ Create farm

● Join existing farm

Step 3. Provide the FQDN of the SQL Server.

Step 4. Click Next.



Database Server

Enter the server and instance names, and the database credentials for the Stream and SOAP Services to use.

Server name: SQL01

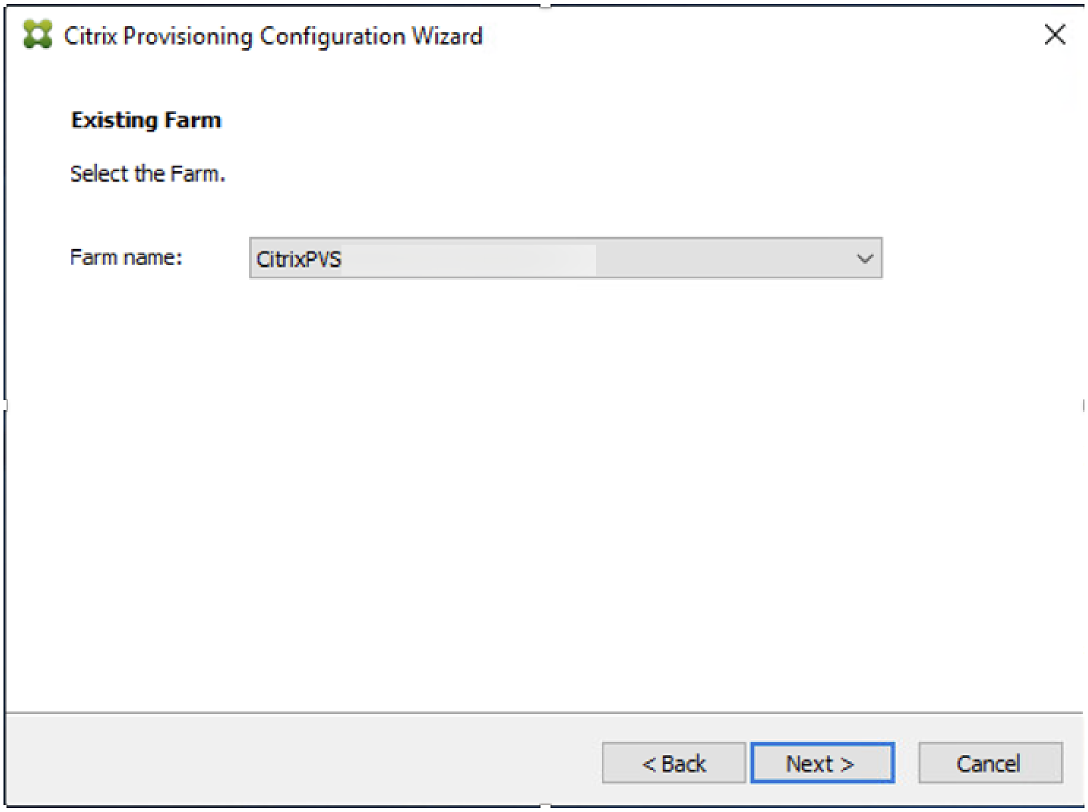
Instance name:

Authentication: Active Directory Integrated

Connect using your current Windows identity.

Step 5. Accept the Farm Name.

Step 6. Click Next.



Citrix Provisioning Configuration Wizard

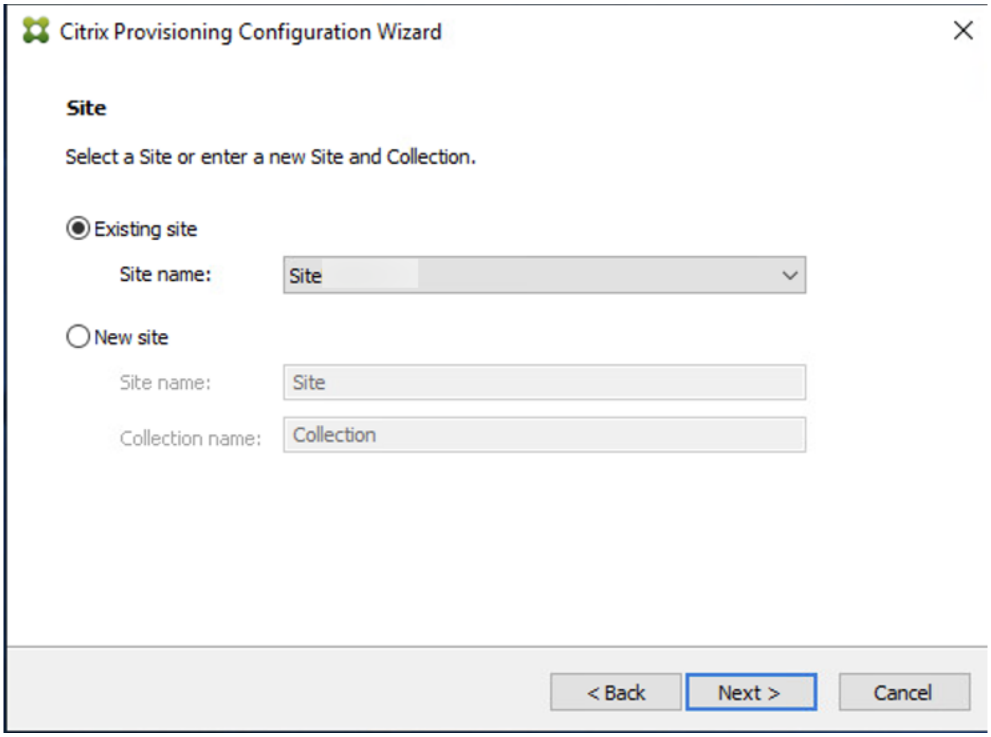
Existing Farm

Select the Farm.

Farm name: CitrixPVS

Step 7. Accept the Existing Site.

Step 8. Click Next.



Citrix Provisioning Configuration Wizard

Site

Select a Site or enter a new Site and Collection.

● Existing site

Site name: Site

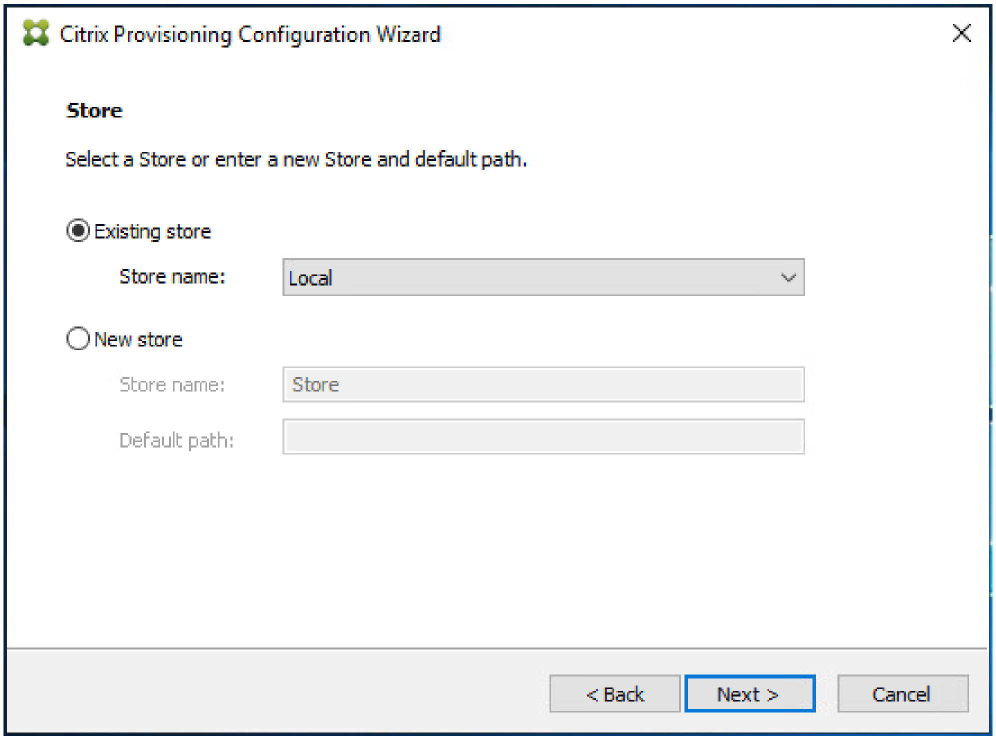
○ New site

Site name: Site

Collection name: Collection

Step 9. Accept the existing vDisk store.

Step 10. Click Next.



Citrix Provisioning Configuration Wizard

Store

Select a Store or enter a new Store and default path.

● Existing store

Store name: Local

○ New store

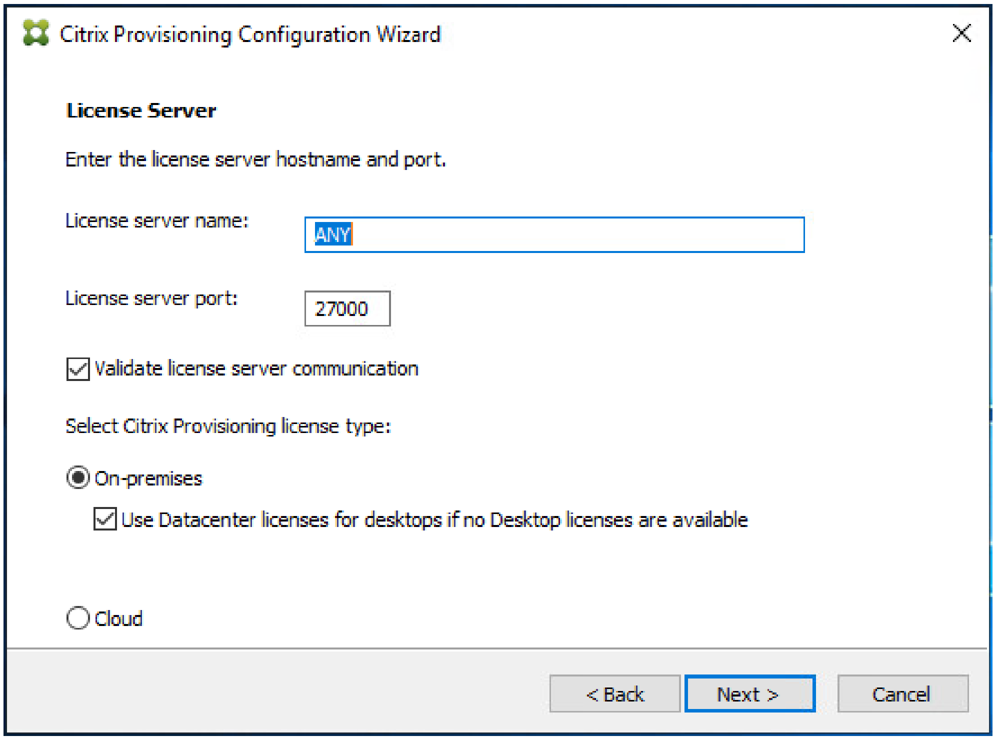
Store name: Store

Default path:

Step 11. Provide the FQDN of the license server.

Step 12. Optionally, provide a port number if changed on the license server.

Step 13. Click Next.



Citrix Provisioning Configuration Wizard

License Server

Enter the license server hostname and port.

License server name: ANY

License server port: 27000

☑ Validate license server communication

Select Citrix Provisioning license type:

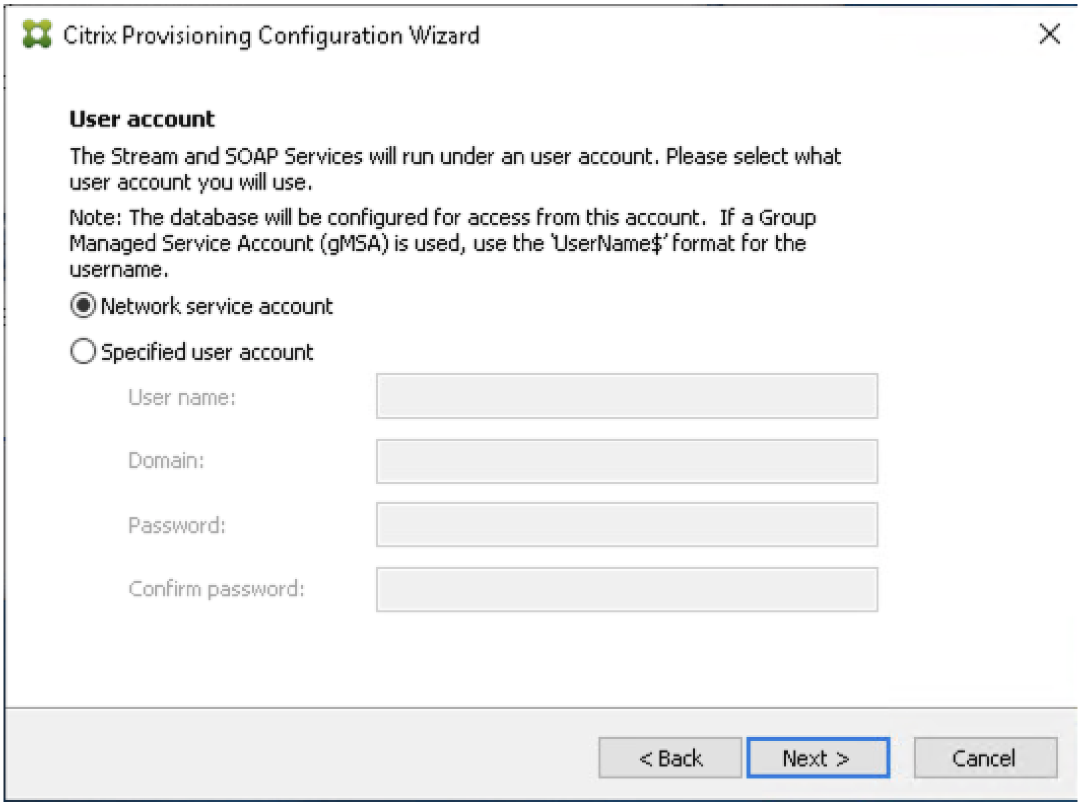
● On-premises

☑ Use Datacenter licenses for desktops if no Desktop licenses are available

○ Cloud

Step 14. Provide the PVS service account information.

Step 15. Click Next.



Citrix Provisioning Configuration Wizard

User account

The Stream and SOAP Services will run under an user account. Please select what user account you will use.

Note: The database will be configured for access from this account. If a Group Managed Service Account (gMSA) is used, use the 'UserName$' format for the username.

● Network service account

○ Specified user account

User name:

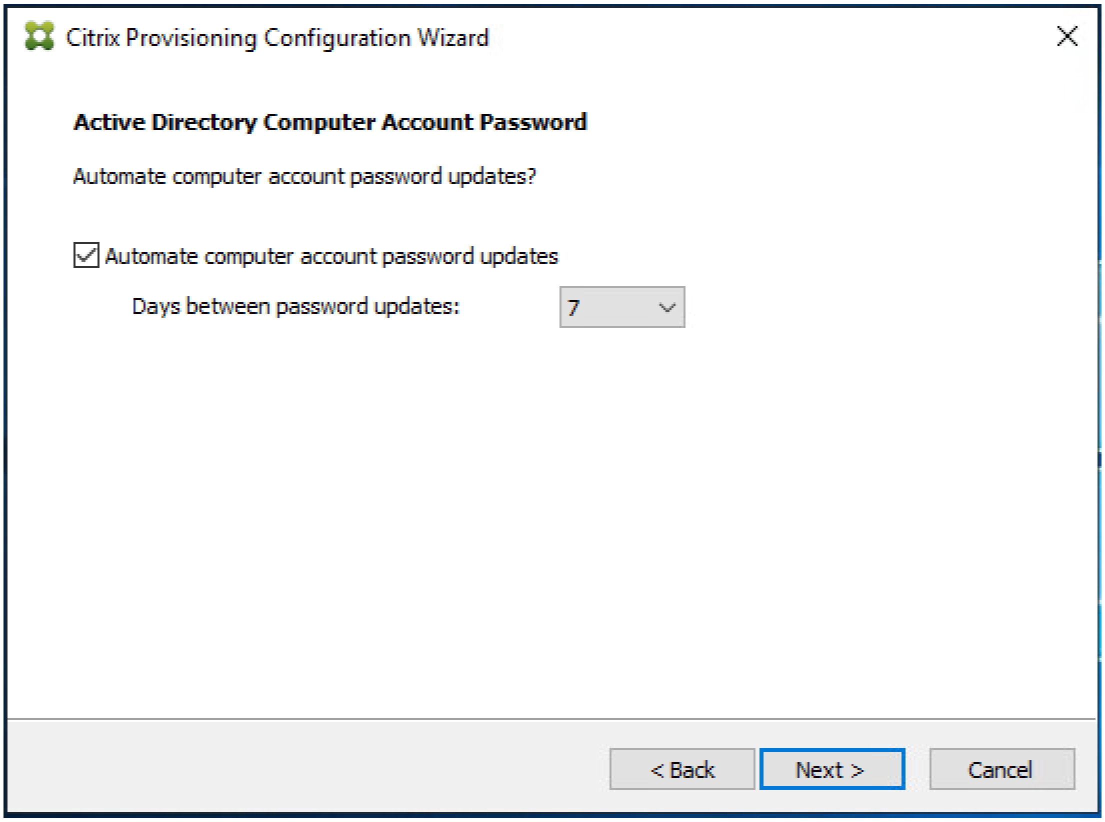
Domain:

Password:

Confirm password:

Step 16. Set the Days between password updates to 7.

Step 17. Click Next.



Citrix Provisioning Configuration Wizard

Active Directory Computer Account Password

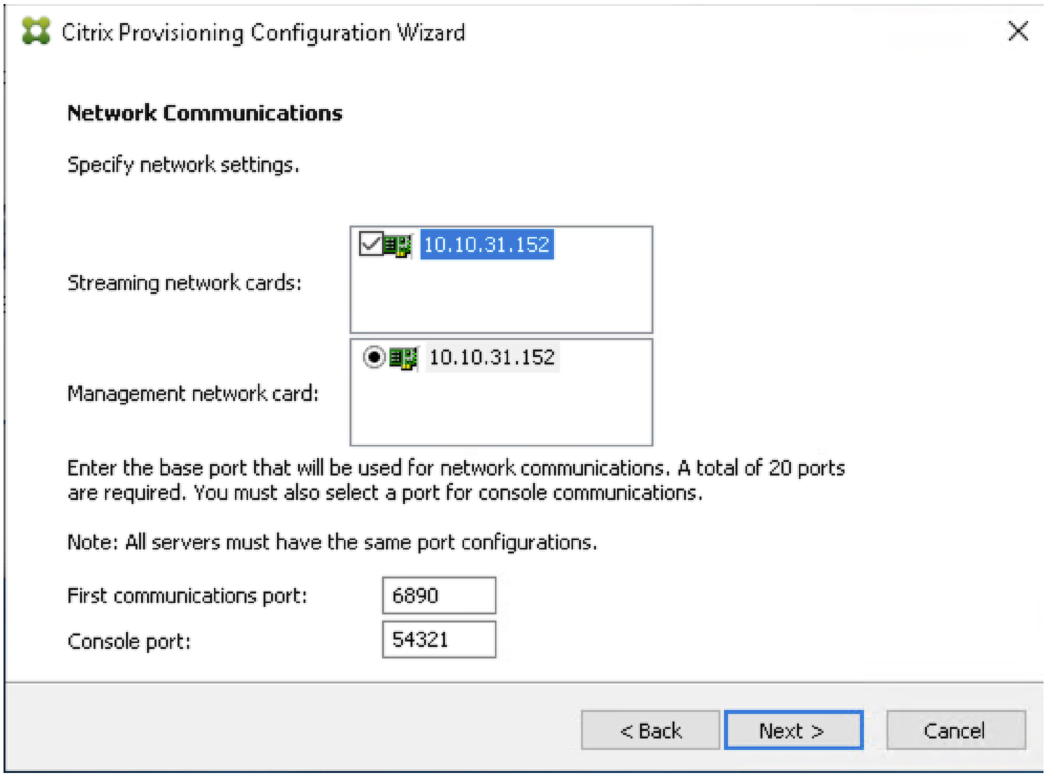
Automate computer account password updates?

☑ Automate computer account password updates

Days between password updates: 7

Step 18. Accept the network card settings.

Step 19. Click Next.



Citrix Provisioning Configuration Wizard

Network Communications

Specify network settings.

Streaming network cards: ☑ 10.10.31.152

Management network card: ● 10.10.31.152

Enter the base port that will be used for network communications. A total of 20 ports are required. You must also select a port for console communications.

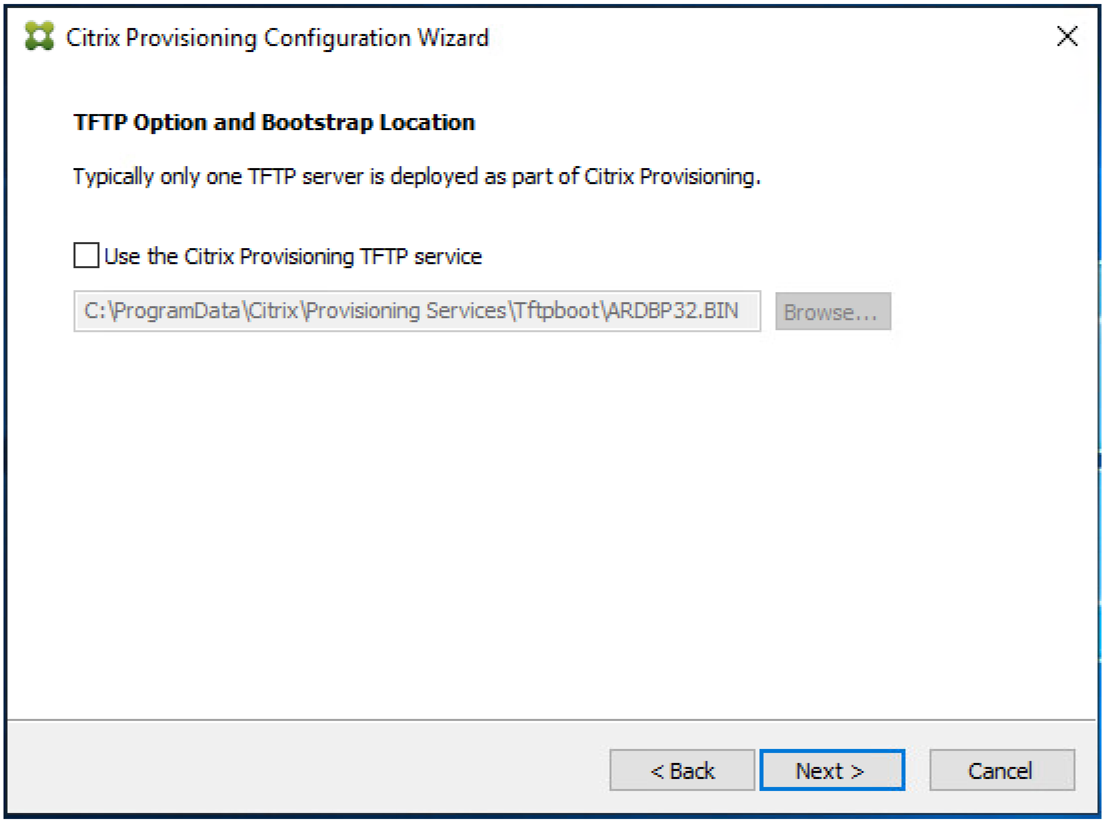
Note: All servers must have the same port configurations.

First communications port: 6890

Console port: 54321

Step 20. Select Use the Provisioning Services TFTP service checkbox.

Step 21. Click Next.



Citrix Provisioning Configuration Wizard

TFTP Option and Bootstrap Location

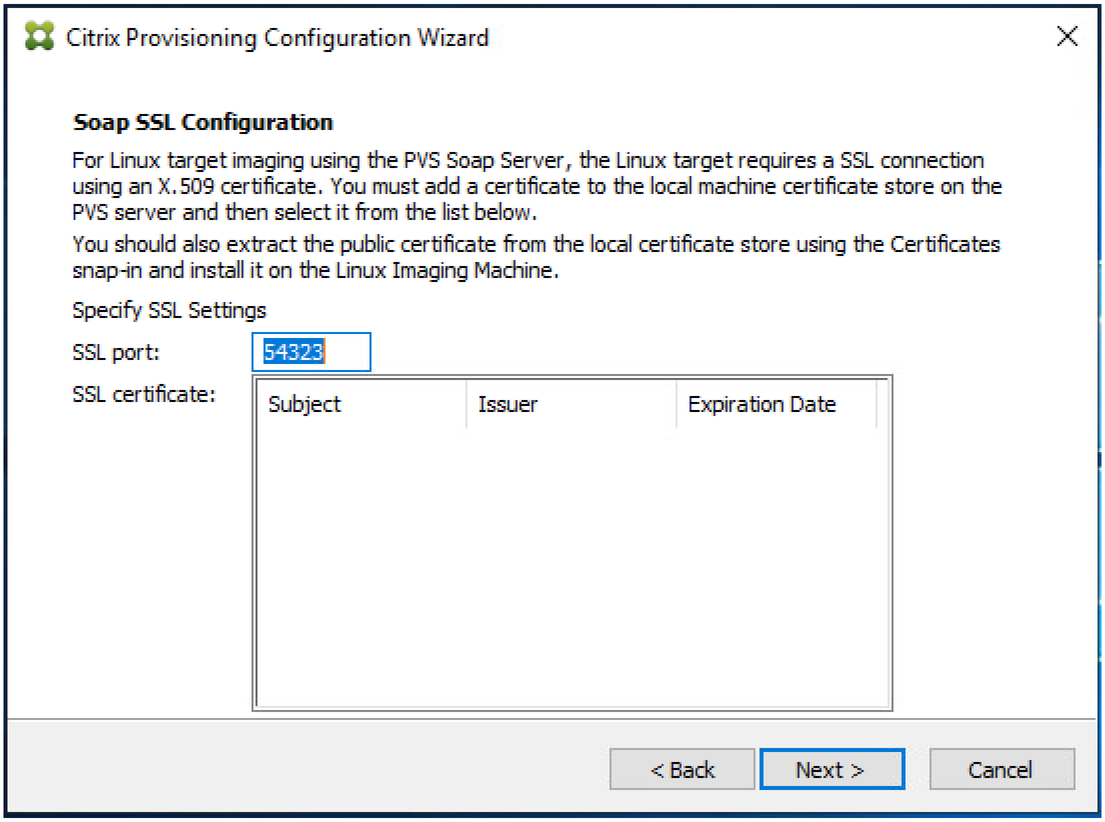
Typically only one TFTP server is deployed as part of Citrix Provisioning.

☐ Use the Citrix Provisioning TFTP service

C:\ProgramData\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN

Step 22. If Soap Server is used, provide details.

Step 23. Click Next.



Soap SSL Configuration

For Linux target imaging using the PVS Soap Server, the Linux target requires a SSL connection using an X.509 certificate. You must add a certificate to the local machine certificate store on the PVS server and then select it from the list below.

You should also extract the public certificate from the local certificate store using the Certificates snap-in and install it on the Linux Imaging Machine.

Specify SSL Settings

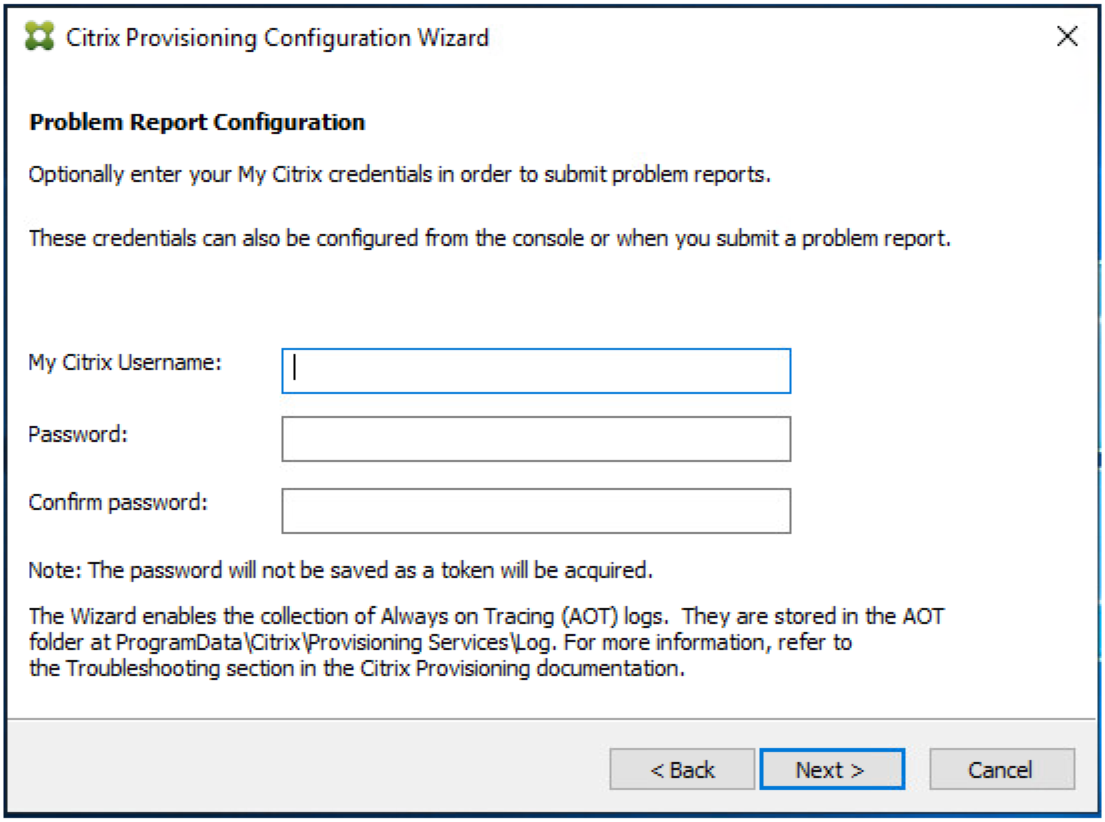
SSL port: 54323

SSL certificate:

Subject	Issuer	Expiration Date

Step 24. If desired, fill in Problem Report Configuration.

Step 25. Click Next.



Citrix Provisioning Configuration Wizard

Problem Report Configuration

Optionally enter your My Citrix credentials in order to submit problem reports.

These credentials can also be configured from the console or when you submit a problem report.

My Citrix Username:

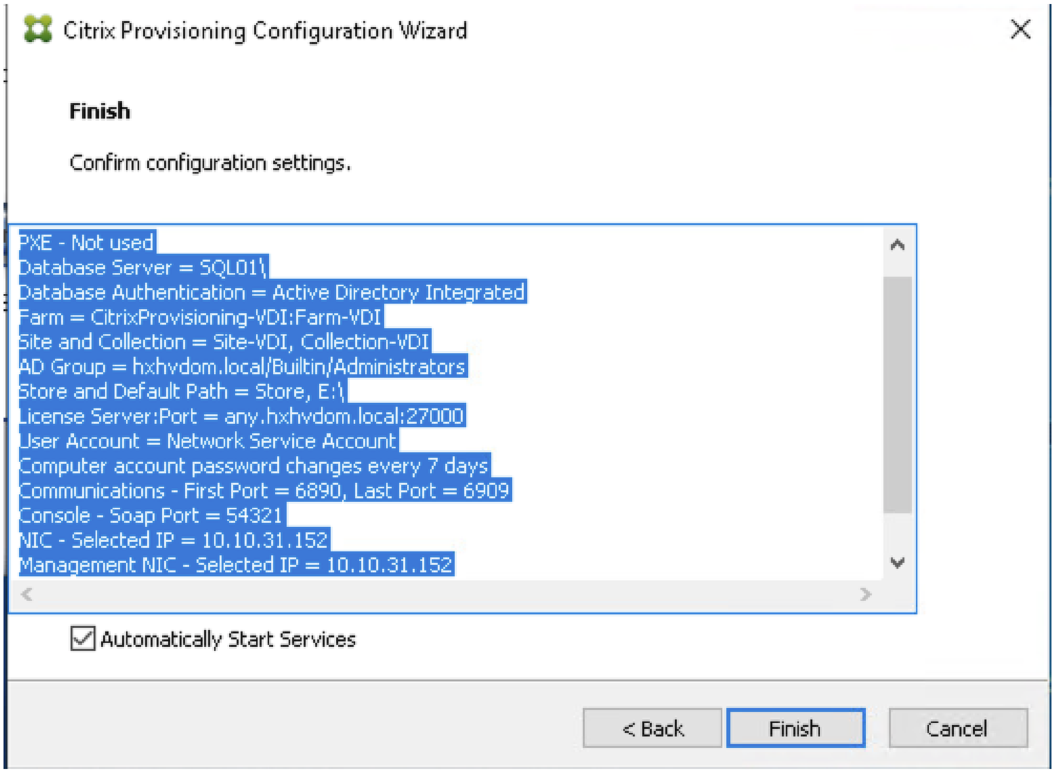
Password:

Confirm password:

Note: The password will not be saved as a token will be acquired.

The Wizard enables the collection of Always on Tracing (AOT) logs. They are stored in the AOT folder at ProgramData\Citrix\Provisioning Services\Log. For more information, refer to the Troubleshooting section in the Citrix Provisioning documentation.

Step 26. Click Finish to start the installation process.



Citrix Provisioning Configuration Wizard

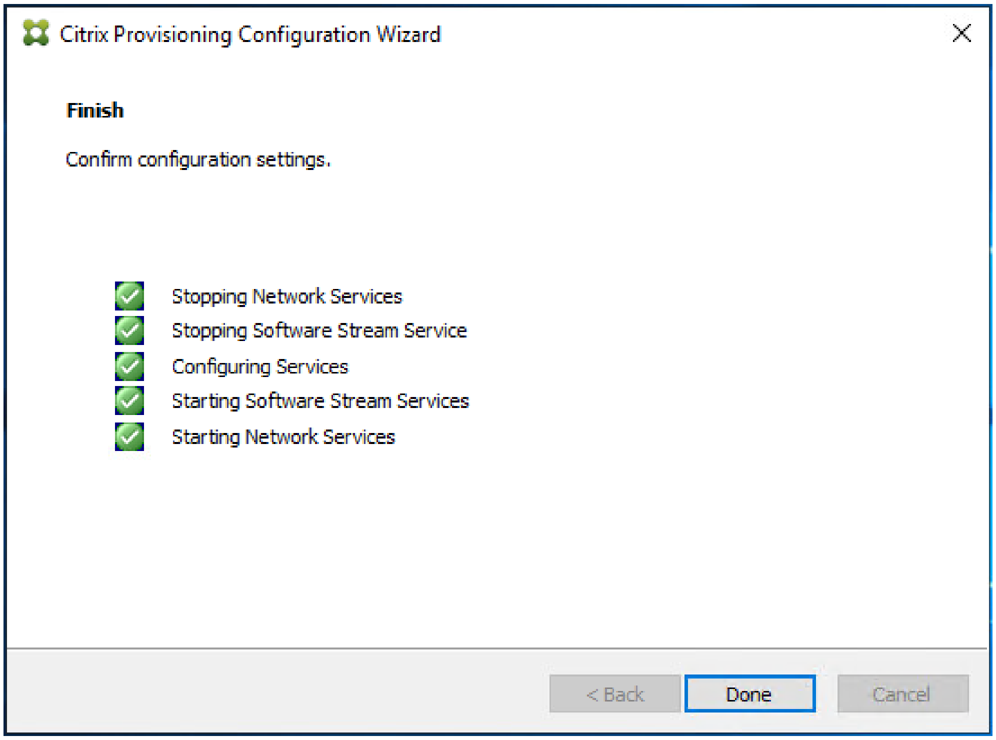
Finish

Confirm configuration settings.

```
PXE - Not used
Database Server = SQL01\
Database Authentication = Active Directory Integrated
Farm = CitrixProvisioning-VDI:Farm-VDI
Site and Collection = Site-VDI, Collection-VDI
AD Group = hxhvdom.local/Builtin/Administrators
Store and Default Path = Store, E:\
License Server:Port = any.hxhvdom.local:27000
User Account = Network Service Account
Computer account password changes every 7 days
Communications - First Port = 6890, Last Port = 6909
Console - Soap Port = 54321
NIC - Selected IP = 10.10.31.152
Management NIC - Selected IP = 10.10.31.152
```

☑ Automatically Start Services

Step 27. Click Done when the installation finishes.


Citrix Provisioning Configuration Wizard

Finish

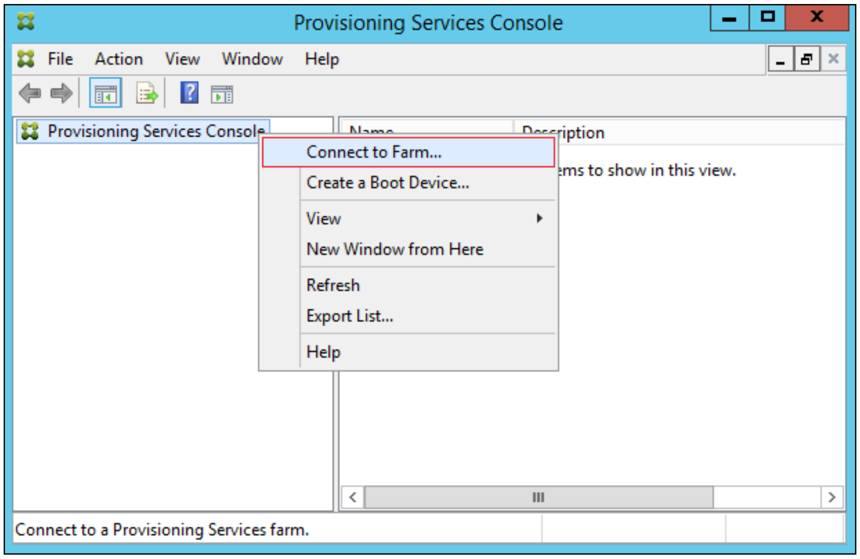
Confirm configuration settings.

- ✓ Stopping Network Services
- ✓ Stopping Software Stream Service
- ✓ Configuring Services
- ✓ Starting Software Stream Services
- ✓ Starting Network Services

Note: You can optionally install the Provisioning Services console on the second PVS server following the procedure in the section Install the Citrix Provisioning Server Target Device Software.

Step 28. After completing the steps to install the three additional PVS servers, launch the Provisioning Services Console to verify that the PVS Servers and Stores are configured and that DHCP boot options are defined.

Step 29. Launch Provisioning Services Console and select Connect to Farm.

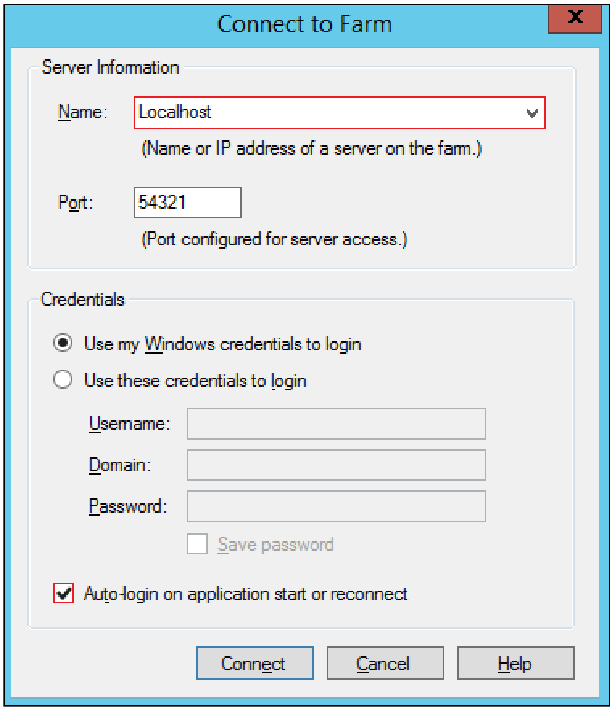


...ems to show in this view.

Connect to a Provisioning Services farm.

Step 30. Enter localhost for the PVS1 server.

Step 31. Click Connect.



Connect to Farm

Server Information

Name: Localhost

(Name or IP address of a server on the farm.)

Port: 54321

(Port configured for server access.)

Credentials

● Use my Windows credentials to login

○ Use these credentials to login

Username:

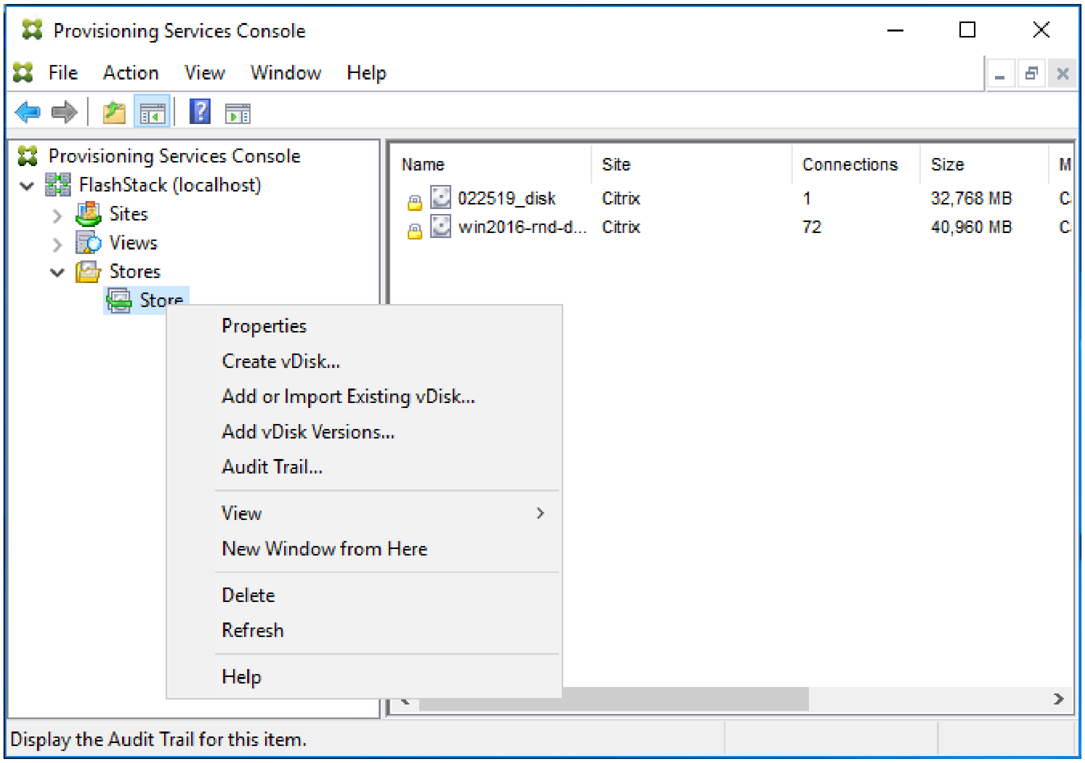
Domain:

Password:

□ Save password

☑ Auto-login on application start or reconnect

Step 32. Select Store Properties from the drop-down list.

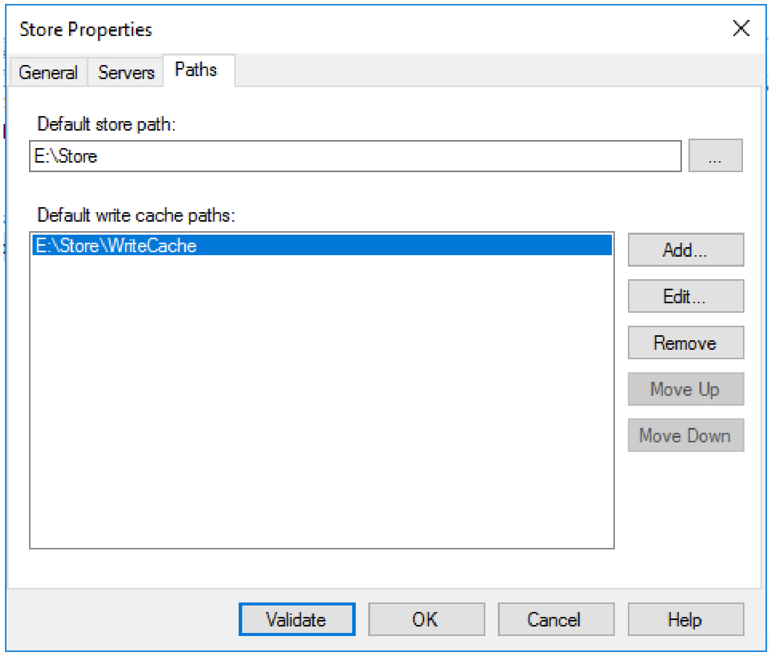


Provisioning Services Console

Name	Site	Connections	Size	M
022519_disk	Citrix	1	32,768 MB	C
win2016-rnd-d...	Citrix	72	40,960 MB	C

Display the Audit Trail for this item.

Step 33. In the Store Properties dialog, add the Default store path to the list of Default write cache paths.

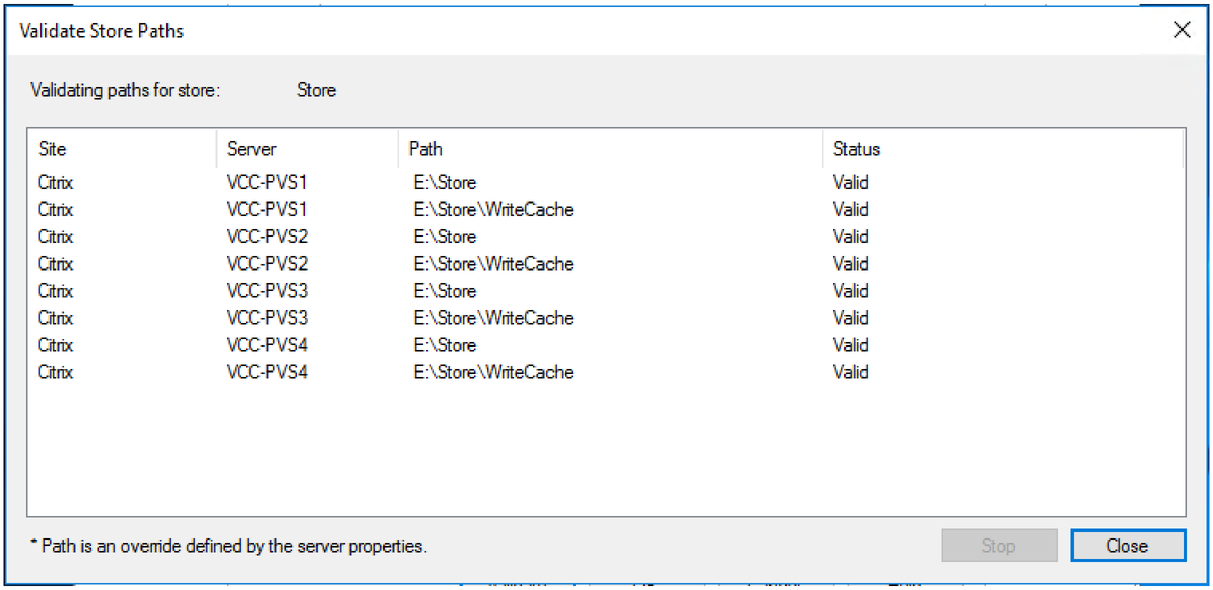


Store Properties

Default store path: E:\Store

Default write cache paths: E:\Store\WriteCache

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



Validate Store Paths

Validating paths for store: Store

Site	Server	Path	Status
Citrix	VCC-PVS1	E:\Store	Valid
Citrix	VCC-PVS1	E:\Store\WriteCache	Valid
Citrix	VCC-PVS2	E:\Store	Valid
Citrix	VCC-PVS2	E:\Store\WriteCache	Valid
Citrix	VCC-PVS3	E:\Store	Valid
Citrix	VCC-PVS3	E:\Store\WriteCache	Valid
Citrix	VCC-PVS4	E:\Store	Valid
Citrix	VCC-PVS4	E:\Store\WriteCache	Valid

* Path is an override defined by the server properties.

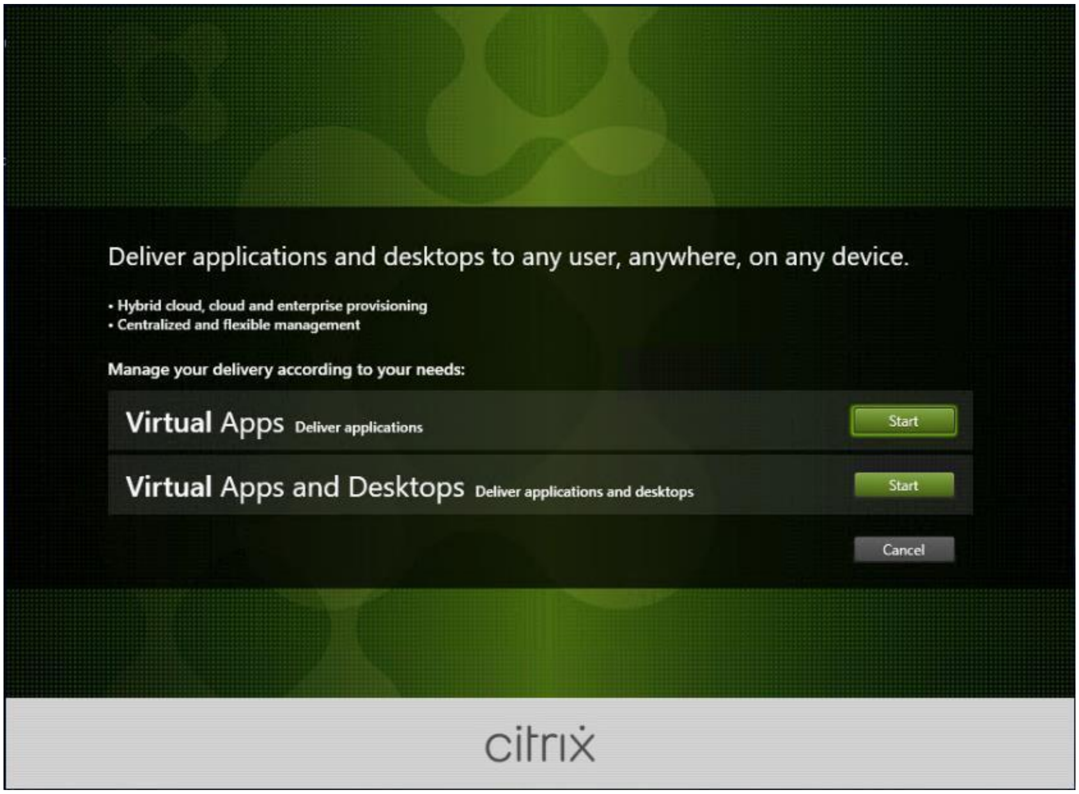
Procedure 5. Install Citrix Virtual Apps and Desktops Virtual Desktop Agents

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 Single-session OS and Multi-session OS.

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 FSLogix was used for this CVD and is described in a later section.)

Step 1. Launch the Citrix Virtual Apps and Desktops installer from the Citrix_Virtual_Apps_and_Desktops_7_2203 ISO.

Step 2. Click Start on the Welcome Screen.



Deliver applications and desktops to any user, anywhere, on any device.

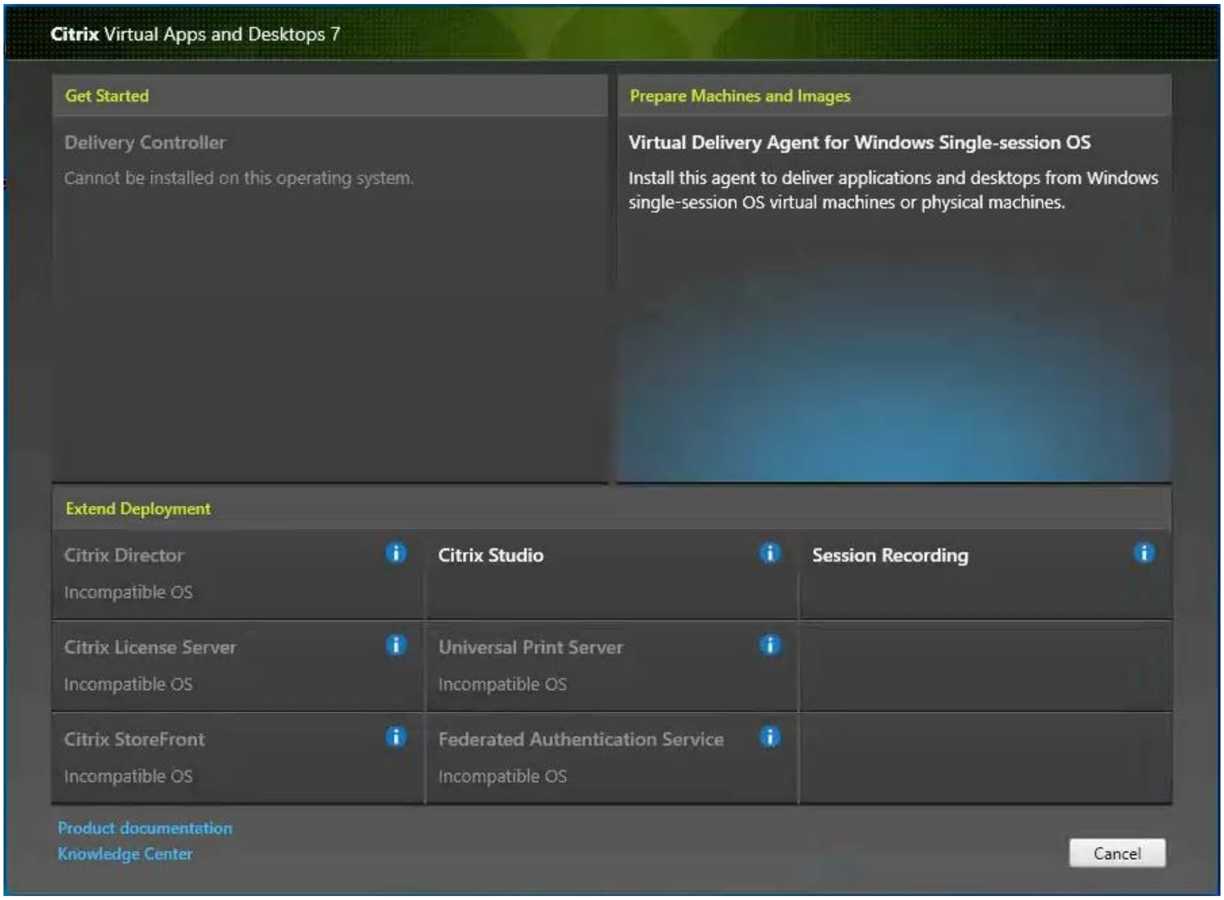
- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

Virtual Apps Deliver applications

Virtual Apps and Desktops Deliver applications and desktops

Step 3. To install the VDA for the Hosted Virtual Desktops (VDI), select Virtual Delivery Agent for Windows Single-session OS.



Citrix Virtual Apps and Desktops 7

Get Started

Delivery Controller

Cannot be installed on this operating system.

Prepare Machines and Images

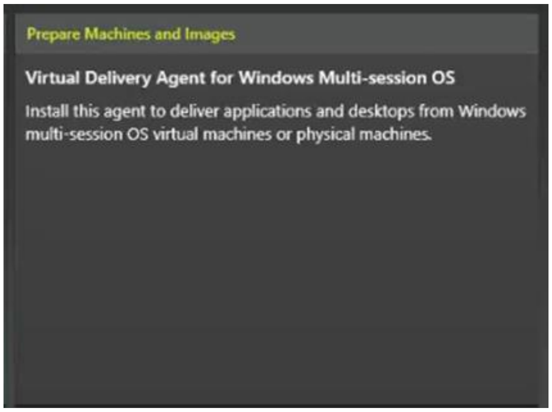
Virtual Delivery Agent for Windows Single-session OS

Install this agent to deliver applications and desktops from Windows single-session OS virtual machines or physical machines.

Extend Deployment

Citrix Director Incompatible OS	Citrix Studio	Session Recording
Citrix License Server Incompatible OS	Universal Print Server Incompatible OS	
Citrix StoreFront Incompatible OS	Federated Authentication Service Incompatible OS	

Step 4. Complete the steps found in the Virtual Delivery Agent installation.



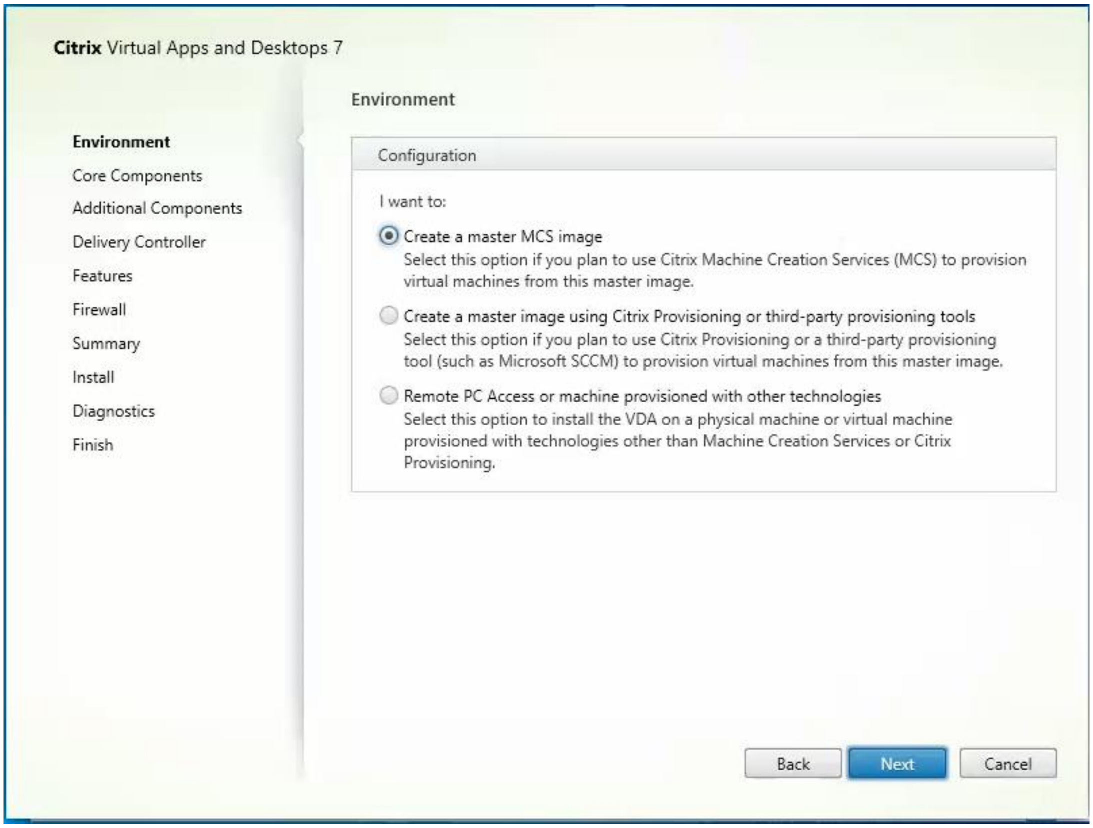
Prepare Machines and Images

Virtual Delivery Agent for Windows Multi-session OS

Install this agent to deliver applications and desktops from Windows multi-session OS virtual machines or physical machines.

Step 5. Select Create a master MCS image.

Step 6. Click Next.



Citrix Virtual Apps and Desktops 7

Environment

Configuration

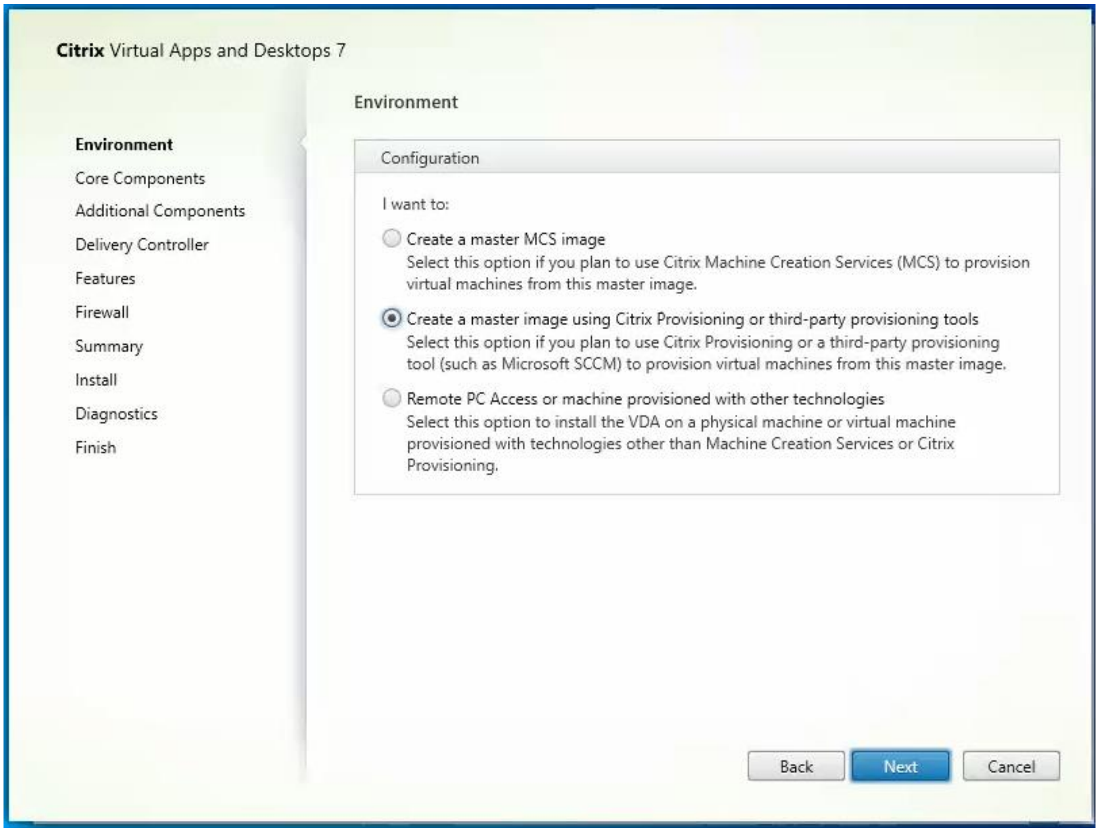
I want to:

● Create a master MCS image
Select this option if you plan to use Citrix Machine Creation Services (MCS) to provision virtual machines from this master image.

○ Create a master image using Citrix Provisioning or third-party provisioning tools
Select this option if you plan to use Citrix Provisioning or a third-party provisioning tool (such as Microsoft SCCM) to provision virtual machines from this master image.

○ Remote PC Access or machine provisioned with other technologies
Select this option to install the VDA on a physical machine or virtual machine provisioned with technologies other than Machine Creation Services or Citrix Provisioning.

Step 7. Select "Create a master image using Citrix Provisioning or third-party provisioning tools" when building image to be delivered with Citrix Provisioning tools.



Environment

Configuration

I want to:

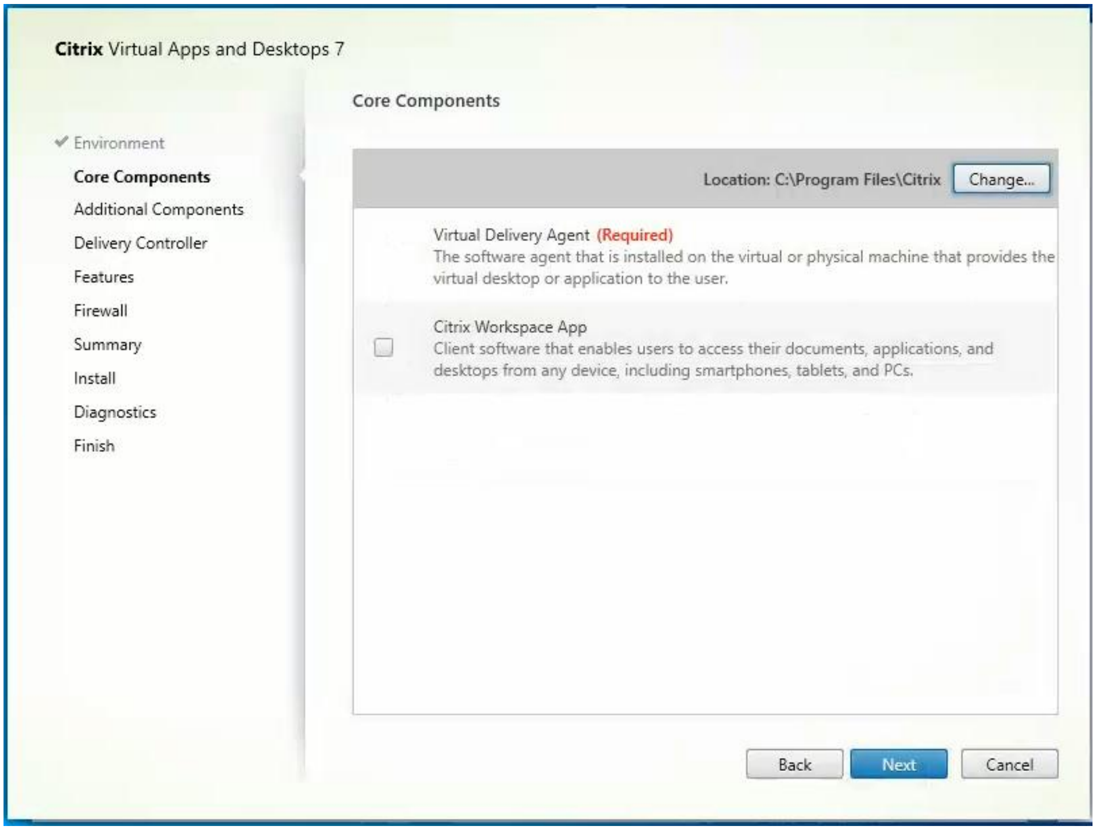
○ Create a master MCS image
Select this option if you plan to use Citrix Machine Creation Services (MCS) to provision virtual machines from this master image.

● Create a master image using Citrix Provisioning or third-party provisioning tools
Select this option if you plan to use Citrix Provisioning or a third-party provisioning tool (such as Microsoft SCCM) to provision virtual machines from this master image.

○ Remote PC Access or machine provisioned with other technologies
Select this option to install the VDA on a physical machine or virtual machine provisioned with technologies other than Machine Creation Services or Citrix Provisioning.

Step 8. Optional; do not select Citrix Workspace App**.**

Step 9. Click Next.



Citrix Virtual Apps and Desktops 7

Core Components

Location: C:\Program Files\Citrix

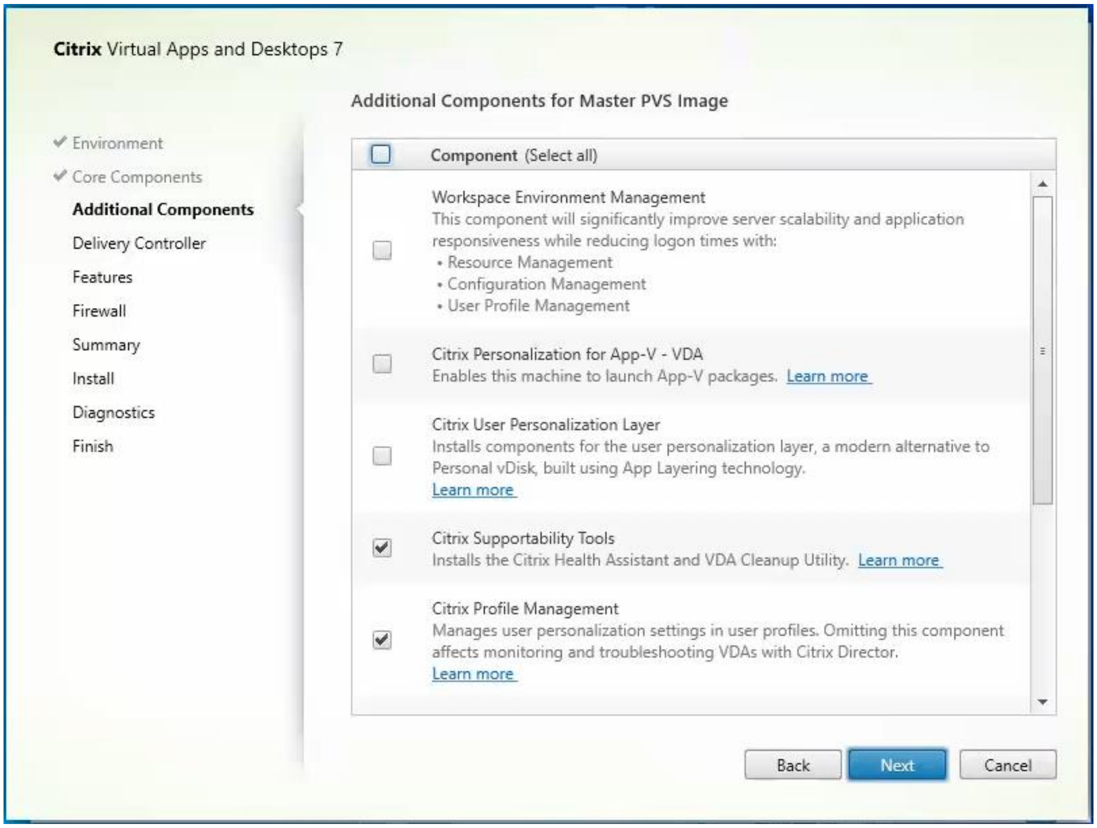
Virtual Delivery Agent (Required)
The software agent that is installed on the virtual or physical machine that provides the virtual desktop or application to the user.

□ Citrix Workspace App
Client software that enables users to access their documents, applications, and desktops from any device, including smartphones, tablets, and PCs.

Step 10. Select the additional components required for your image.

Note: In this design, only the default components were installed on the image.

Step 11. Click Next.



Citrix Virtual Apps and Desktops 7

Additional Components for Master PVS Image

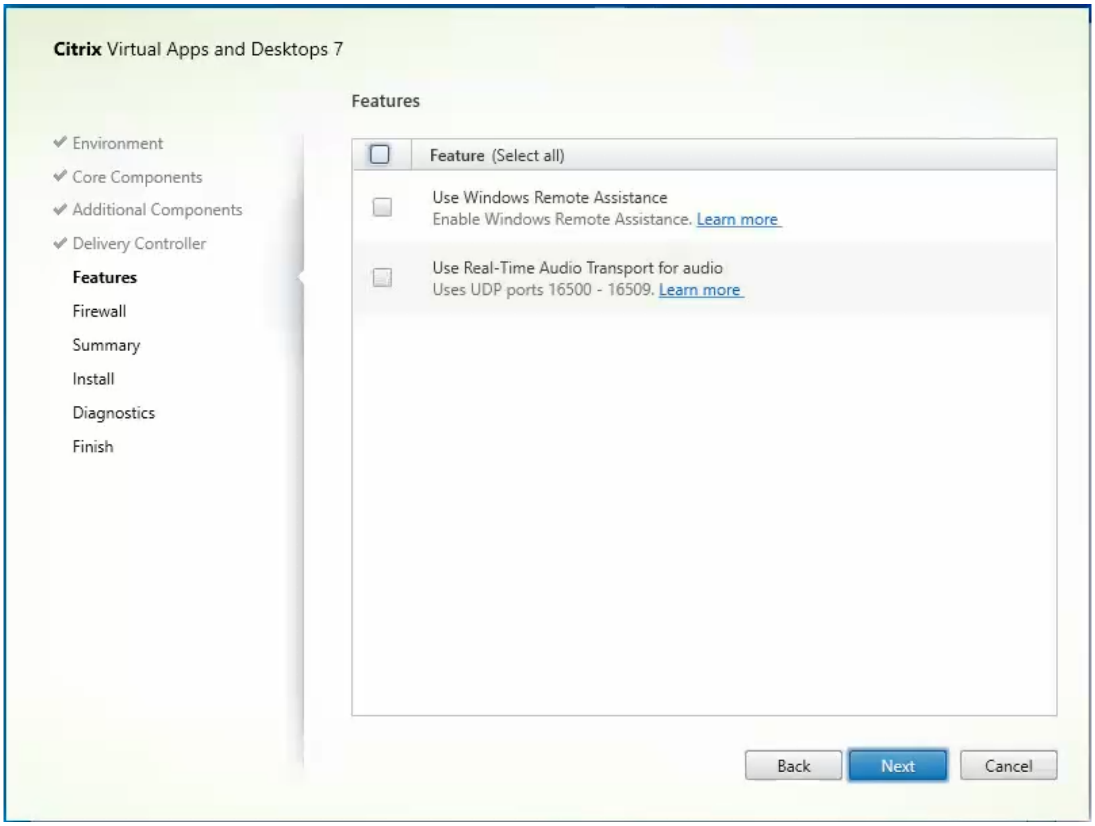
	Component (Select all)
□	Workspace Environment Management This component will significantly improve server scalability and application responsiveness while reducing logon times with: • Resource Management • Configuration Management • User Profile Management
□	Citrix Personalization for App-V - VDA Enables this machine to launch App-V packages. Learn more
□	Citrix User Personalization Layer Installs components for the user personalization layer, a modern alternative to Personal vDisk, built using App Layering technology. Learn more
☑	Citrix Supportability Tools Installs the Citrix Health Assistant and VDA Cleanup Utility. Learn more
☑	Citrix Profile Management Manages user personalization settings in user profiles. Omitting this component affects monitoring and troubleshooting VDAs with Citrix Director. Learn more

Step 12. Configure Delivery Controllers at this time.

Step 13. Click Next.

Step 14. Optional, select additional features**.**

Step 15. Click Next.



Citrix Virtual Apps and Desktops 7

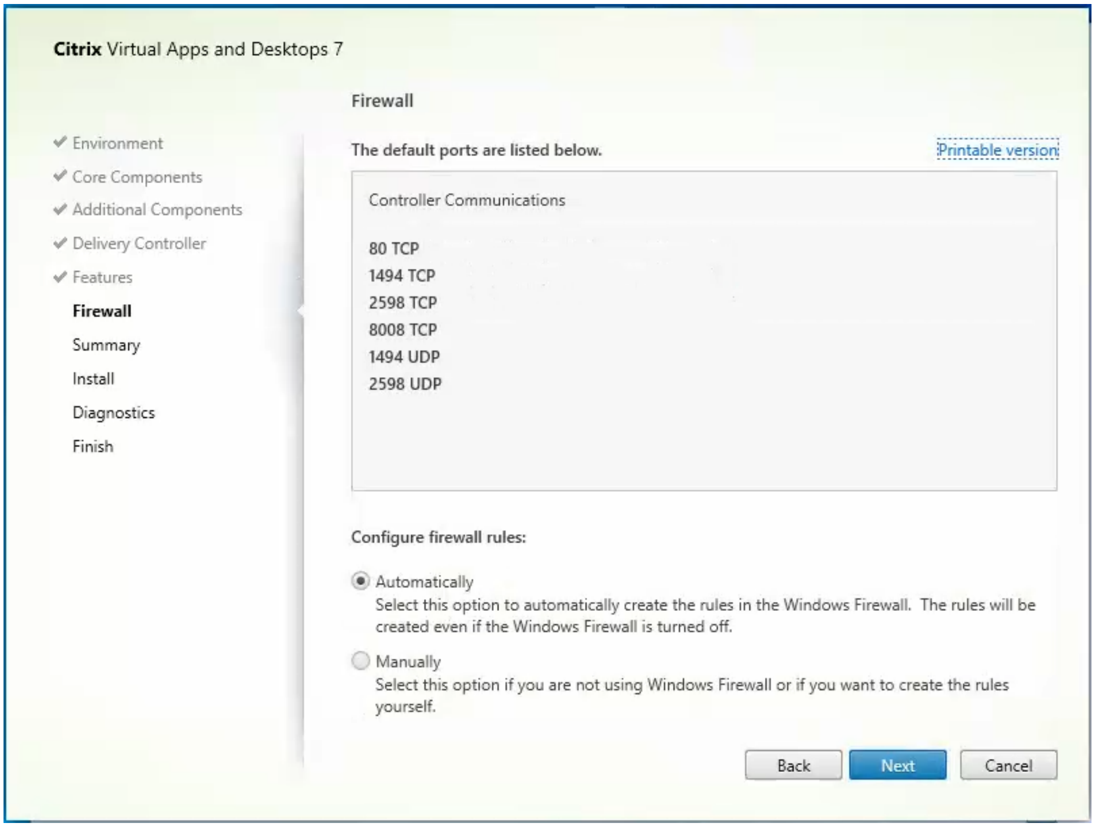
Features

✔ Environment
✔ Core Components
✔ Additional Components
✔ Delivery Controller
Features
Firewall
Summary
Install
Diagnostics
Finish

□	**Feature** (Select all)
□	Use Windows Remote Assistance Enable Windows Remote Assistance. Learn more
□	Use Real-Time Audio Transport for audio Uses UDP ports 16500 - 16509. Learn more

Step 16. Allow the firewall rules to configure Automatically.

Step 17. Click Next.



Citrix Virtual Apps and Desktops 7

Firewall

✔ Environment
✔ Core Components
✔ Additional Components
✔ Delivery Controller
✔ Features
Firewall
Summary
Install
Diagnostics
Finish

The default ports are listed below. Printable version

Controller Communications

80 TCP
1494 TCP
2598 TCP
8008 TCP
1494 UDP
2598 UDP

Configure firewall rules:

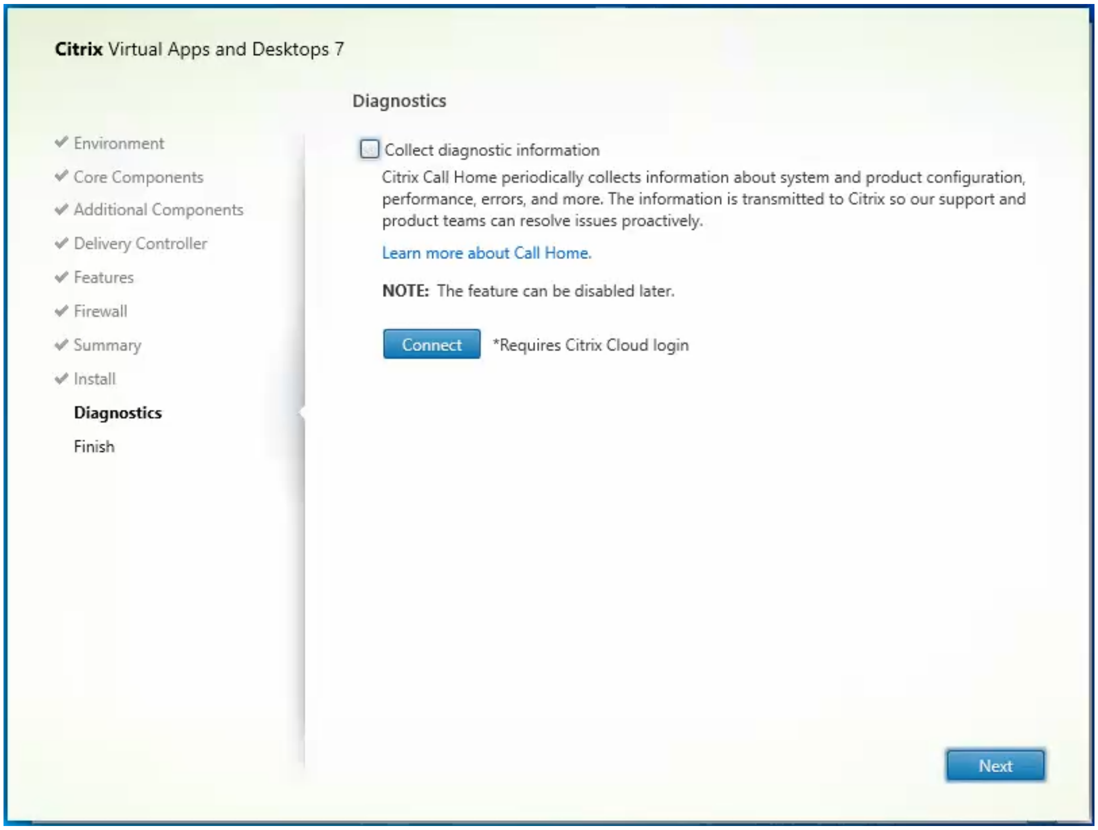
● Automatically
Select this option to automatically create the rules in the Windows Firewall. The rules will be created even if the Windows Firewall is turned off.

○ Manually
Select this option if you are not using Windows Firewall or if you want to create the rules yourself.

Step 18. Verify the Summary and click Install**.**

Step 19. Optional, configure Citrix Call Home participation.

Step 20. Click Next.



Citrix Virtual Apps and Desktops 7

Diagnostics

☐ Collect diagnostic information

Citrix Call Home periodically collects information about system and product configuration, performance, errors, and more. The information is transmitted to Citrix so our support and product teams can resolve issues proactively.

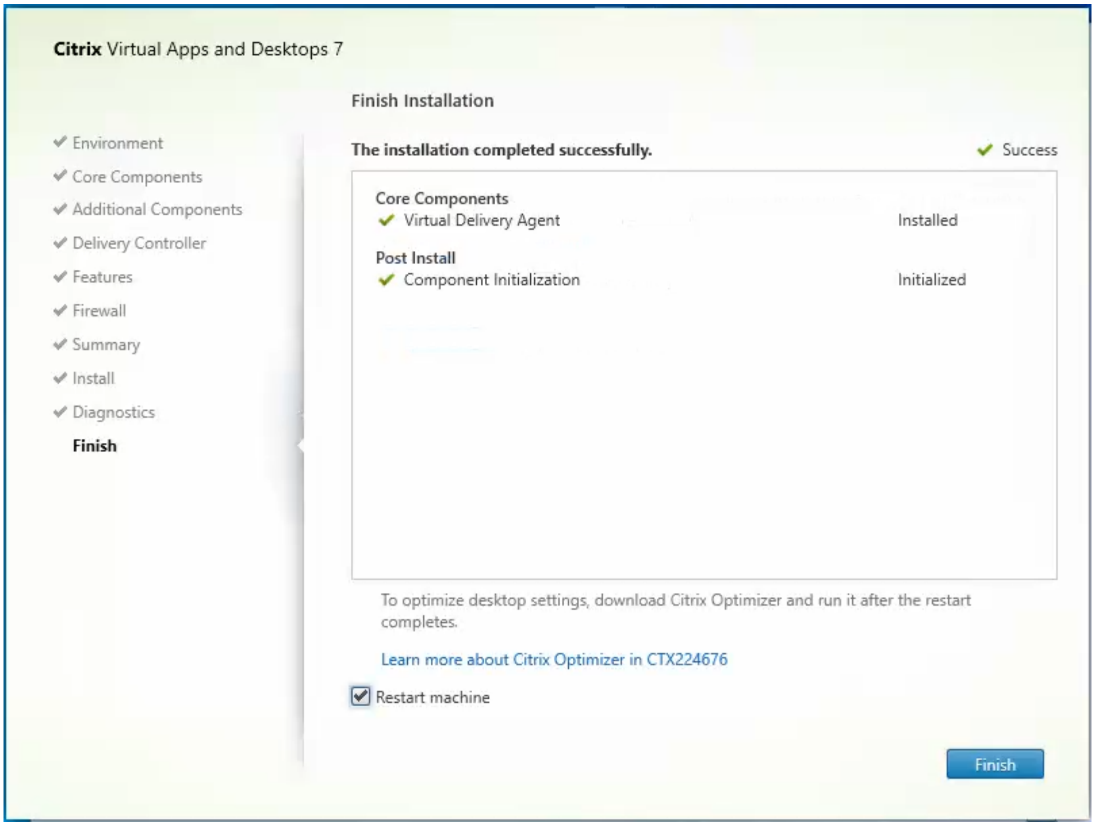
Learn more about Call Home.

NOTE: The feature can be disabled later.

*Requires Citrix Cloud login

Step 21. Check Restart Machine.

Step 22. Click Finish and the machine will reboot automatically.



Finish Installation

The installation completed successfully. ✓ Success

Core Components
✓ Virtual Delivery Agent Installed

Post Install
✓ Component Initialization Initialized

To optimize desktop settings, download Citrix Optimizer and run it after the restart completes.

Learn more about Citrix Optimizer in CTX224676

☑ Restart machine

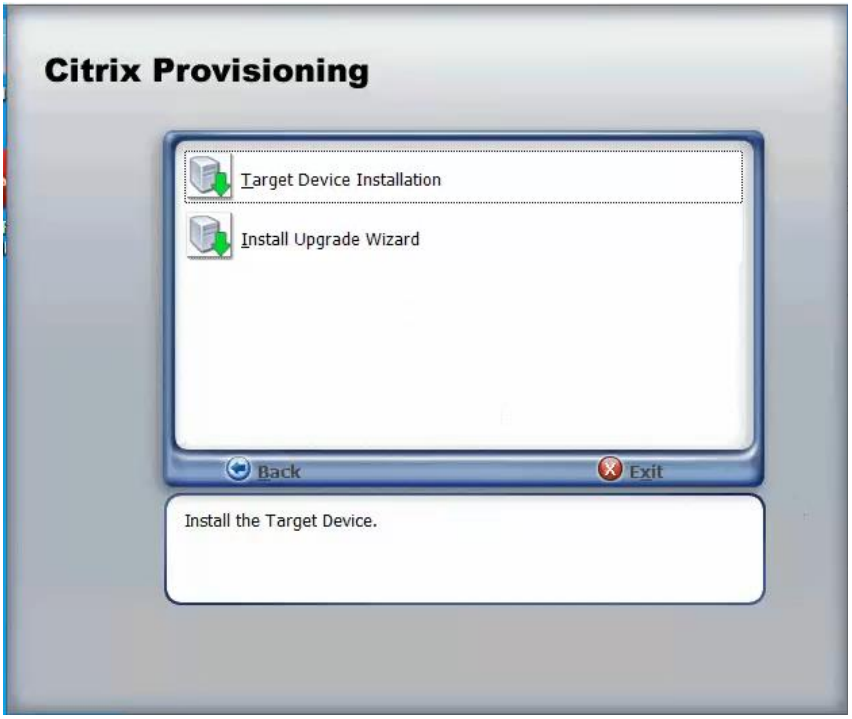
Install the Citrix Provisioning Server Target Device Software

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.

Procedure 1. Install the Citrix Provisioning Server Target Device software

Step 1. Launch the PVS installer from the Citrix_Provisioning_2203 ISO.

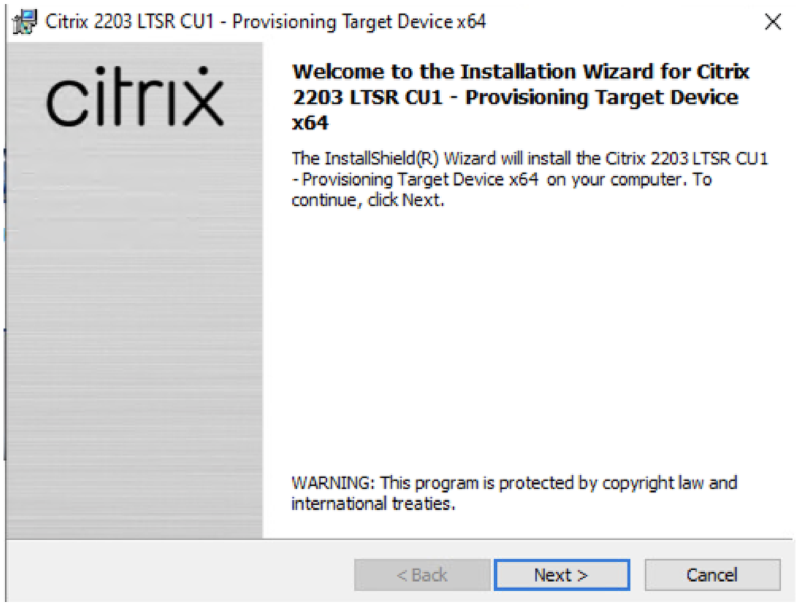
Step 2. Click Target Device Installation.



Install the Target Device.

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

Step 3. Click Next.



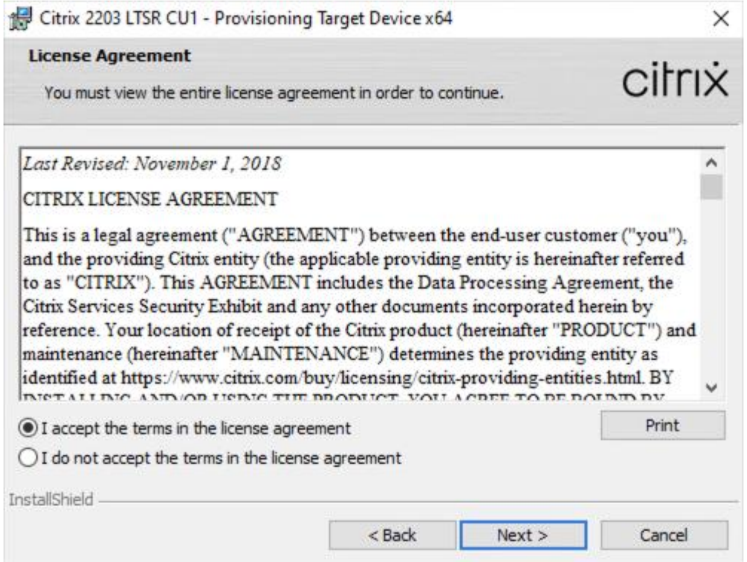
Welcome to the Installation Wizard for Citrix 2203 LTSR CU1 - Provisioning Target Device x64

The InstallShield(R) Wizard will install the Citrix 2203 LTSR CU1 - Provisioning Target Device x64 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Step 4. Indicate your acceptance of the license by selecting the "I have read, understand, and accept the terms of the license agreement" radio button.

Step 5. Click Next.



License Agreement

You must view the entire license agreement in order to continue.

Last Revised: November 1, 2018

CITRIX LICENSE AGREEMENT

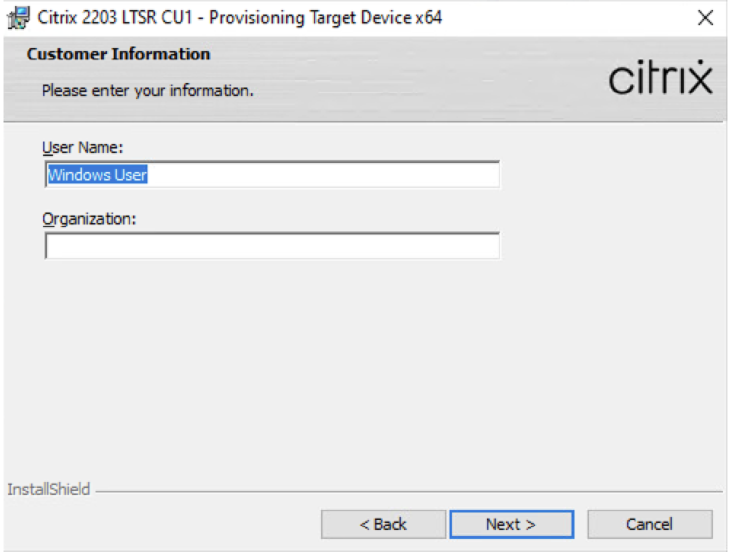
This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix-providing-entities.html. BY

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Step 6. Optionally, provide the Customer information.

Step 7. Click Next.



Customer Information

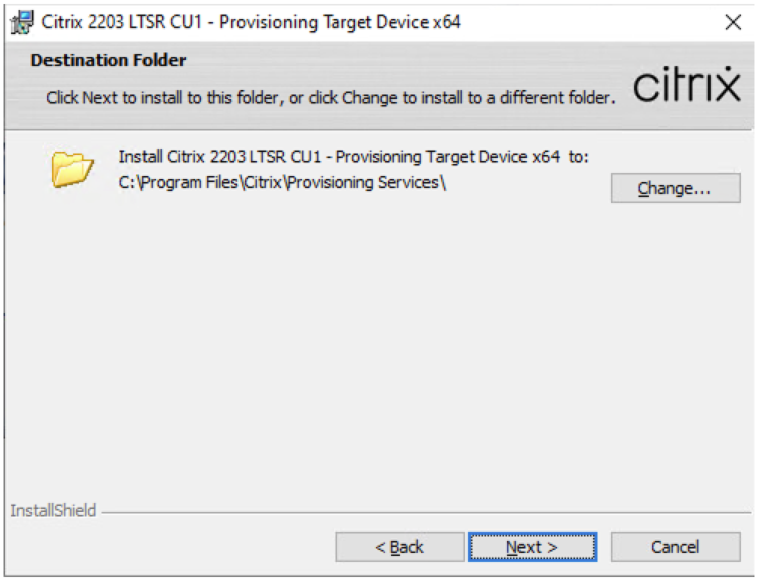
Please enter your information.

User Name: Windows User

Organization:

Step 8. Accept the default installation path.

Step 9. Click Next.



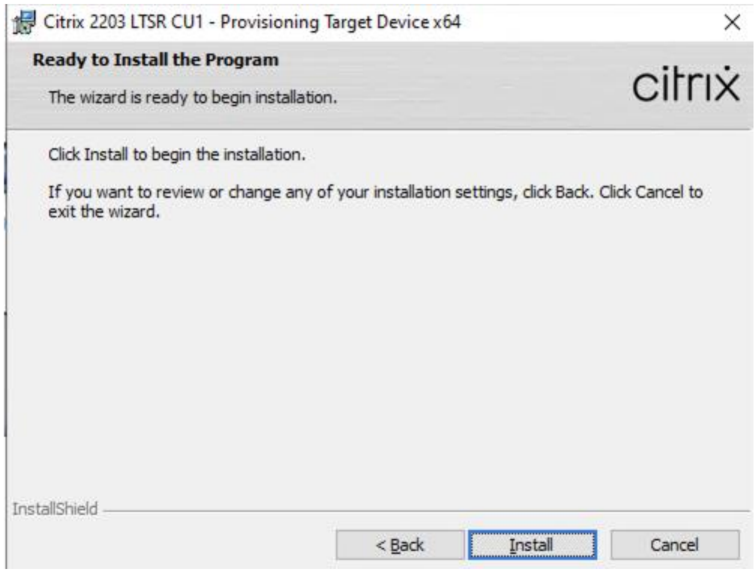
Citrix 2203 LTSR CU1 - Provisioning Target Device x64

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Citrix 2203 LTSR CU1 - Provisioning Target Device x64 to:
C:\Program Files\Citrix\Provisioning Services\

Step 10. Click Install.



Citrix 2203 LTSR CU1 - Provisioning Target Device x64

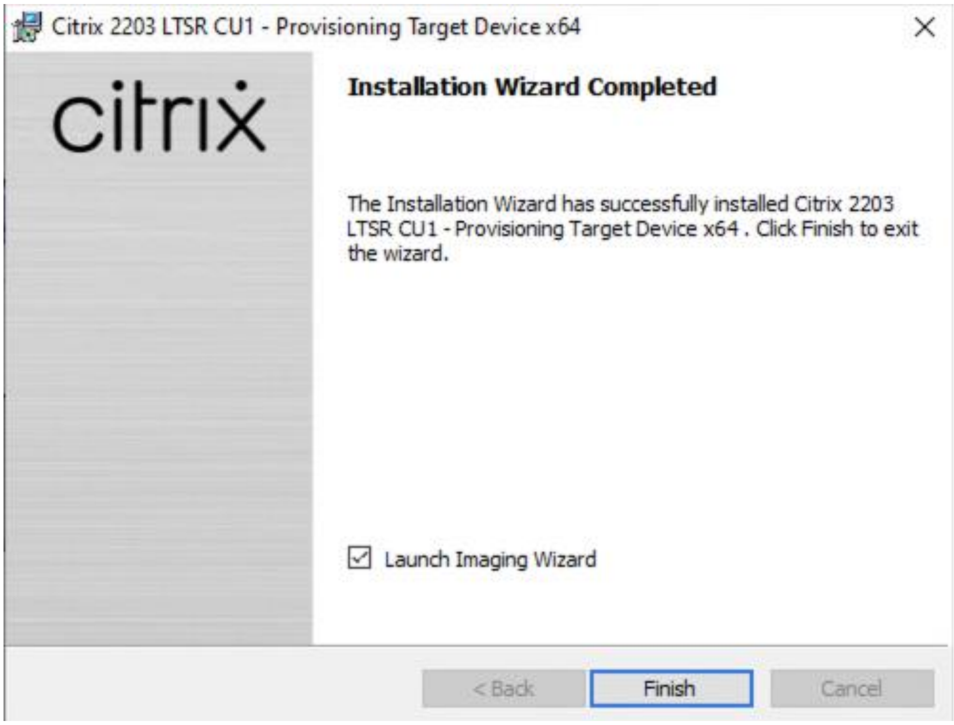
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Step 11. Deselect the checkbox to launch the Imaging Wizard and click Finish.


Citrix 2203 LTSR CU1 - Provisioning Target Device x64

Installation Wizard Completed

The Installation Wizard has successfully installed Citrix 2203 LTSR CU1 - Provisioning Target Device x64 . Click Finish to exit the wizard.

☑ Launch Imaging Wizard

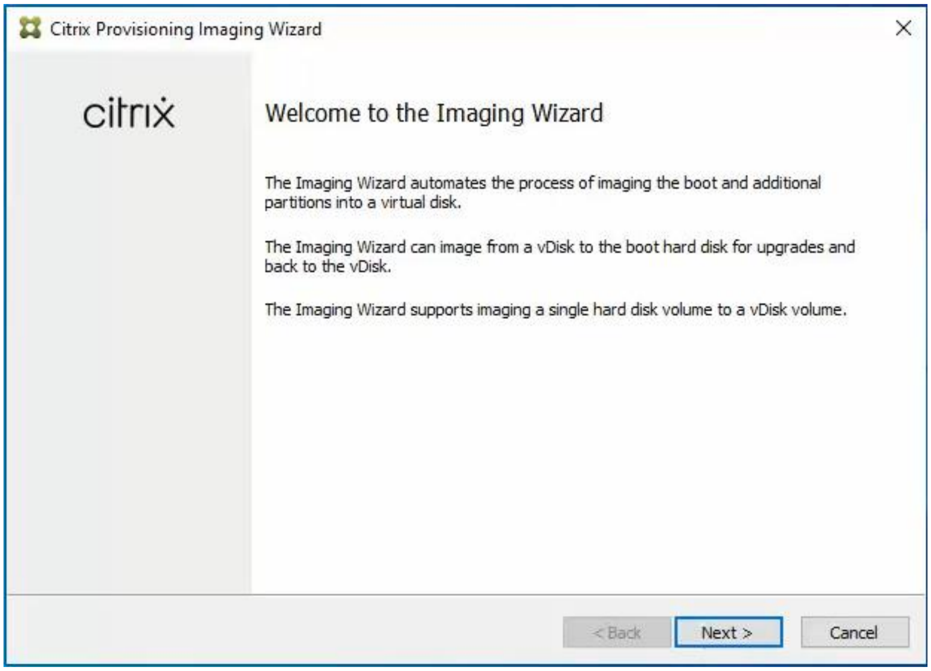
Step 12. Click Yes to reboot the machine.

Procedure 2. Create Citrix Provisioning Server vDisks

The PVS Imaging Wizard automatically creates a base vDisk image from the master target device.

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

Step 2. Click Next.


Citrix Provisioning Imaging Wizard

Welcome to the Imaging Wizard

The Imaging Wizard automates the process of imaging the boot and additional partitions into a virtual disk.

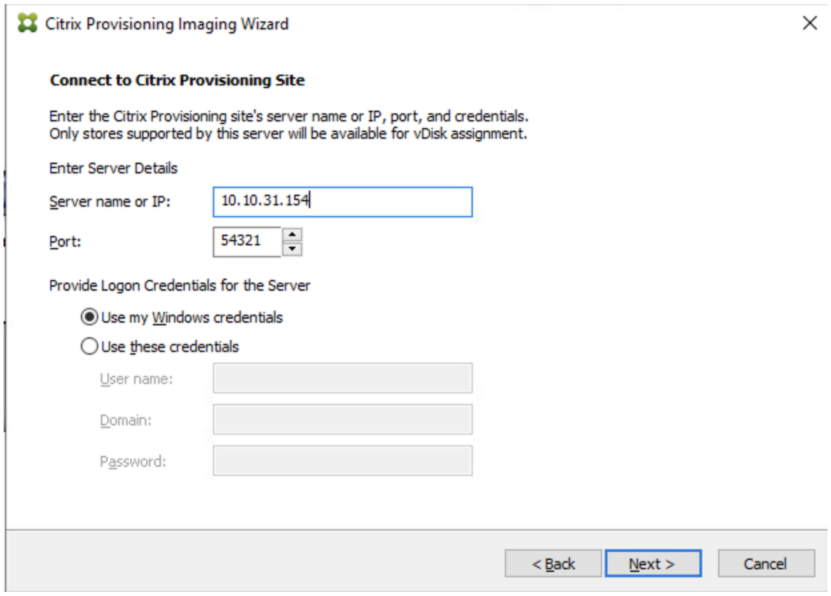
The Imaging Wizard can image from a vDisk to the boot hard disk for upgrades and back to the vDisk.

The Imaging Wizard supports imaging a single hard disk volume to a vDisk volume.

Step 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.

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

Step 5. Click Next.



Citrix Provisioning Imaging Wizard

Connect to Citrix Provisioning Site

Enter the Citrix Provisioning site's server name or IP, port, and credentials.
Only stores supported by this server will be available for vDisk assignment.

Enter Server Details

Server name or IP: 10.10.31.154

Port: 54321

Provide Logon Credentials for the Server

● Use my Windows credentials

○ Use these credentials

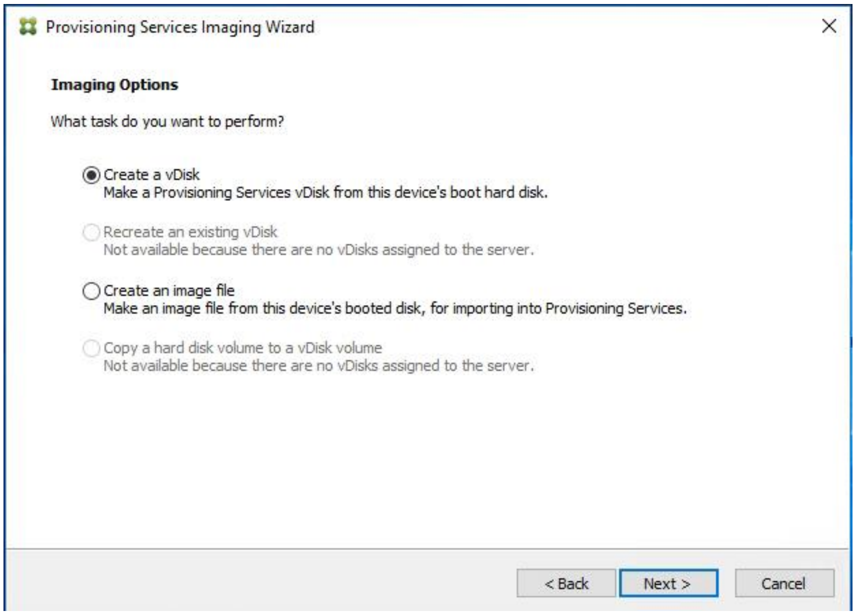
User name:

Domain:

Password:

Step 6. Select Create a vDisk.

Step 7. Click Next.



Provisioning Services Imaging Wizard

Imaging Options

What task do you want to perform?

● Create a vDisk
Make a Provisioning Services vDisk from this device's boot hard disk.

○ Recreate an existing vDisk
Not available because there are no vDisks assigned to the server.

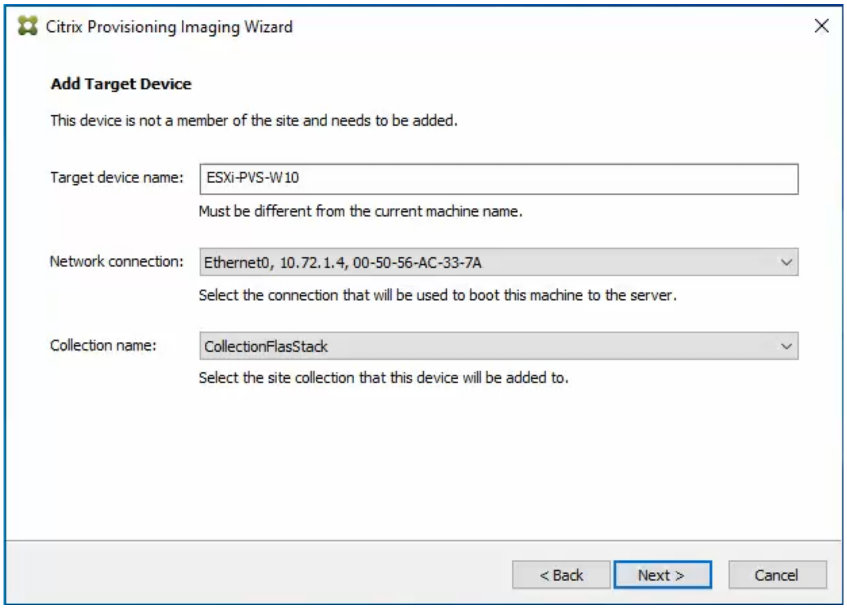
○ Create an image file
Make an image file from this device's booted disk, for importing into Provisioning Services.

○ Copy a hard disk volume to a vDisk volume
Not available because there are no vDisks assigned to the server.

The Add Target Device page appears.

Step 8. 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.

Step 9. Click Next.



Citrix Provisioning Imaging Wizard

Add Target Device

This device is not a member of the site and needs to be added.

Target device name: ESXi-PVS-W10

Must be different from the current machine name.

Network connection: Ethernet0, 10.72.1.4, 00-50-56-AC-33-7A

Select the connection that will be used to boot this machine to the server.

Collection name: CollectionFlasStack

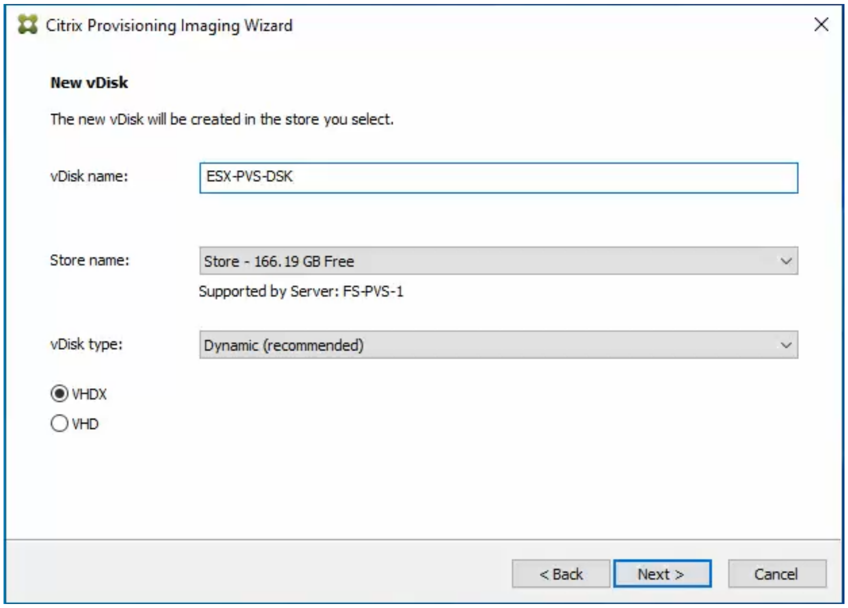
Select the site collection that this device will be added to.

Step 10. The New vDisk dialog displays. Enter the name of the vDisk.

Step 11. Select the Store where the vDisk will reside. Select the vDisk type, either Fixed or Dynamic, from the drop-down list.

Note: This CVD used Dynamic rather than Fixed vDisks.

Step 12. Click Next.



Citrix Provisioning Imaging Wizard

New vDisk

The new vDisk will be created in the store you select.

vDisk name: ESX-PVS-DSK

Store name: Store - 166.19 GB Free

Supported by Server: FS-PVS-1

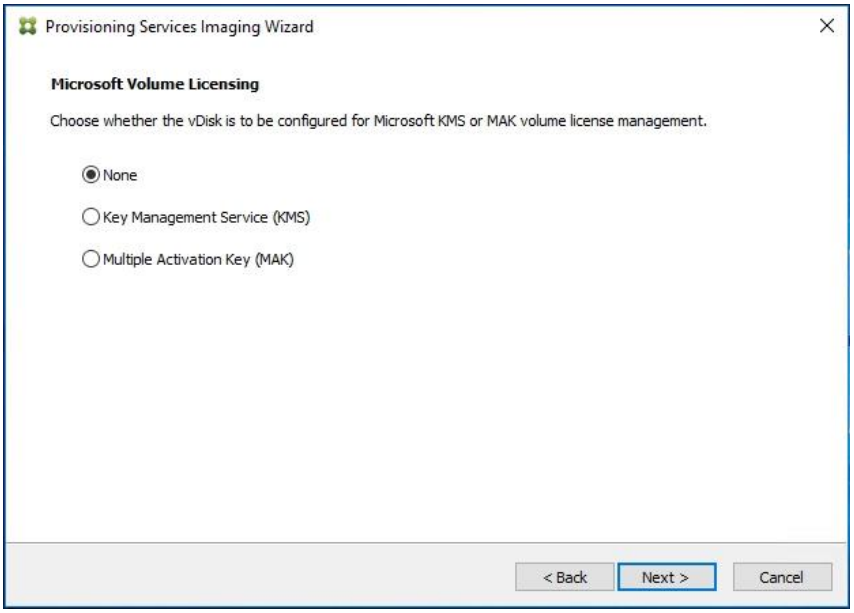
vDisk type: Dynamic (recommended)

● VHDX

○ VHD

Step 13. 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.

Step 14. Click Next.


Provisioning Services Imaging Wizard

Microsoft Volume Licensing

Choose whether the vDisk is to be configured for Microsoft KMS or MAK volume license management.

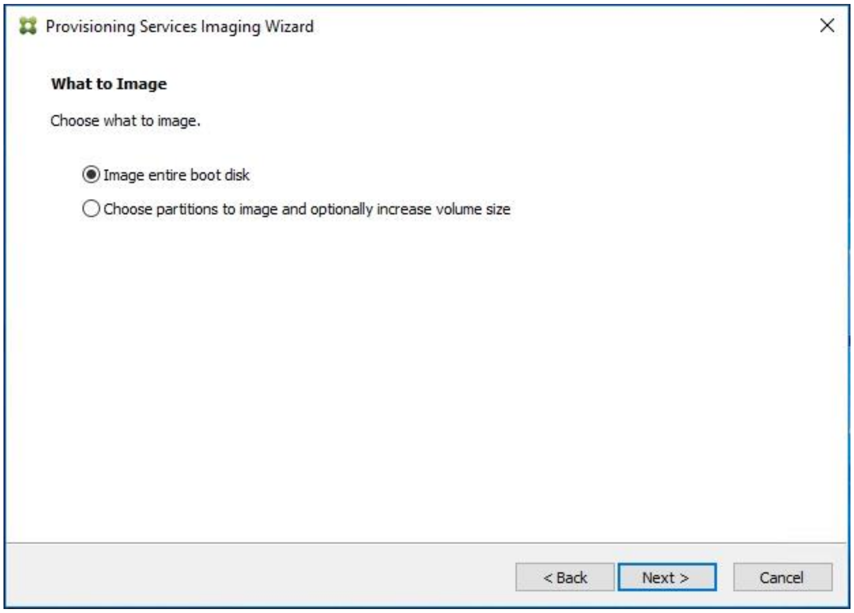
● None

○ Key Management Service (KMS)

○ Multiple Activation Key (MAK)

Step 15. Select Image entire boot disk on the Configure Image Volumes page.

Step 16. Click Next.


Provisioning Services Imaging Wizard

What to Image

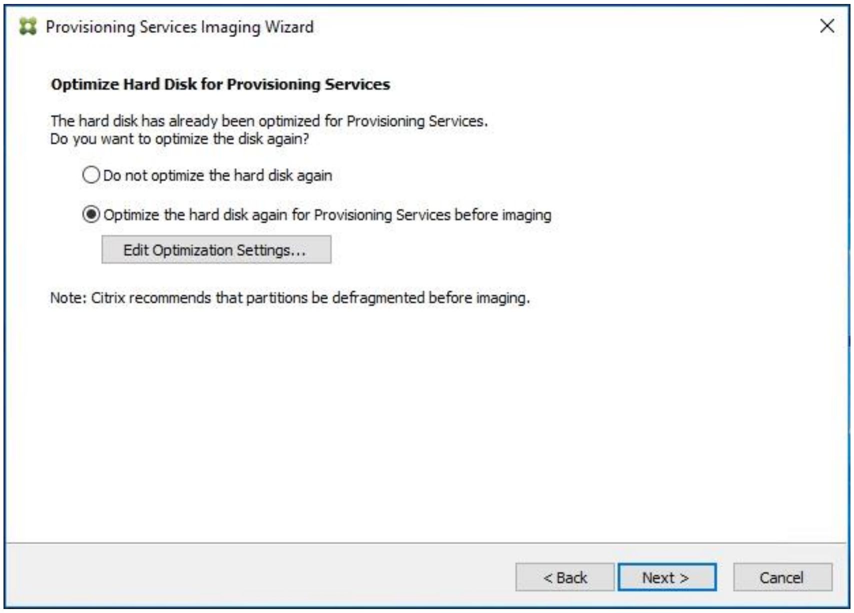
Choose what to image.

● Image entire boot disk

○ Choose partitions to image and optionally increase volume size

Step 17. Select Optimize for hard disk again for Provisioning Services before imaging on the Optimize Hard Disk for Provisioning Services.

Step 18. Click Next.



Provisioning Services Imaging Wizard

Optimize Hard Disk for Provisioning Services

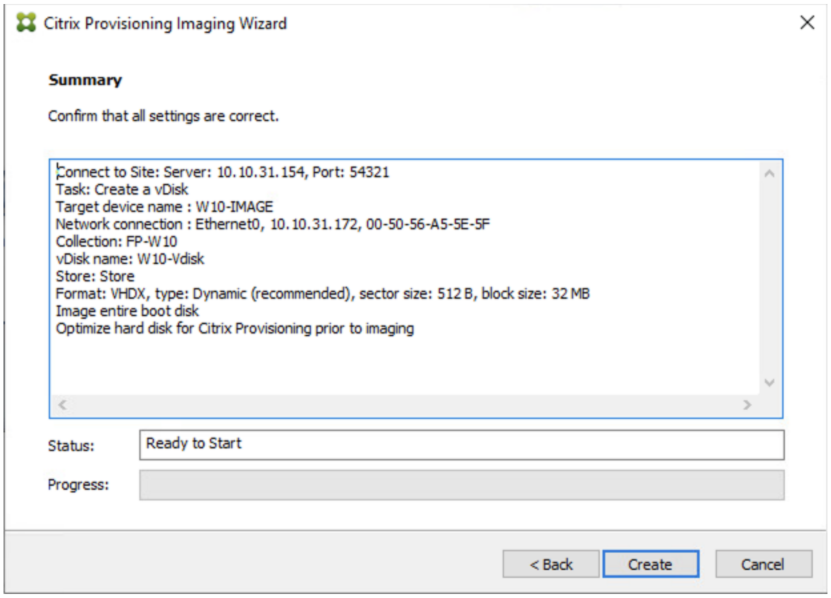
The hard disk has already been optimized for Provisioning Services.
Do you want to optimize the disk again?

○ Do not optimize the hard disk again

● Optimize the hard disk again for Provisioning Services before imaging

Note: Citrix recommends that partitions be defragmented before imaging.

Step 19. Click Create on the Summary page.



Citrix Provisioning Imaging Wizard

Summary

Confirm that all settings are correct.

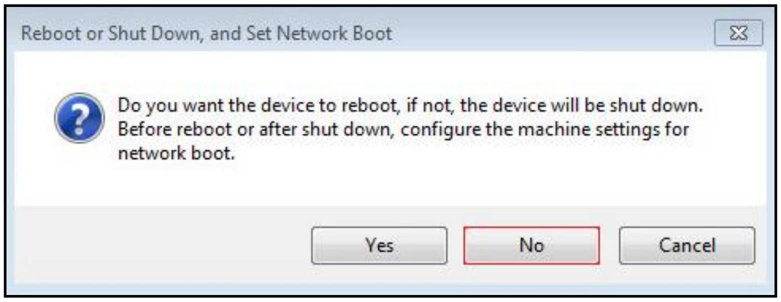
```
Connect to Site: Server: 10.10.31.154, Port: 54321
Task: Create a vDisk
Target device name : W10-IMAGE
Network connection : Ethernet0, 10.10.31.172, 00-50-56-A5-5E-5F
Collection: FP-W10
vDisk name: W10-Vdisk
Store: Store
Format: VHDX, type: Dynamic (recommended), sector size: 512 B, block size: 32 MB
Image entire boot disk
Optimize hard disk for Citrix Provisioning prior to imaging
```

Status: Ready to Start

Progress:

Step 20. Review the configuration and click Continue.

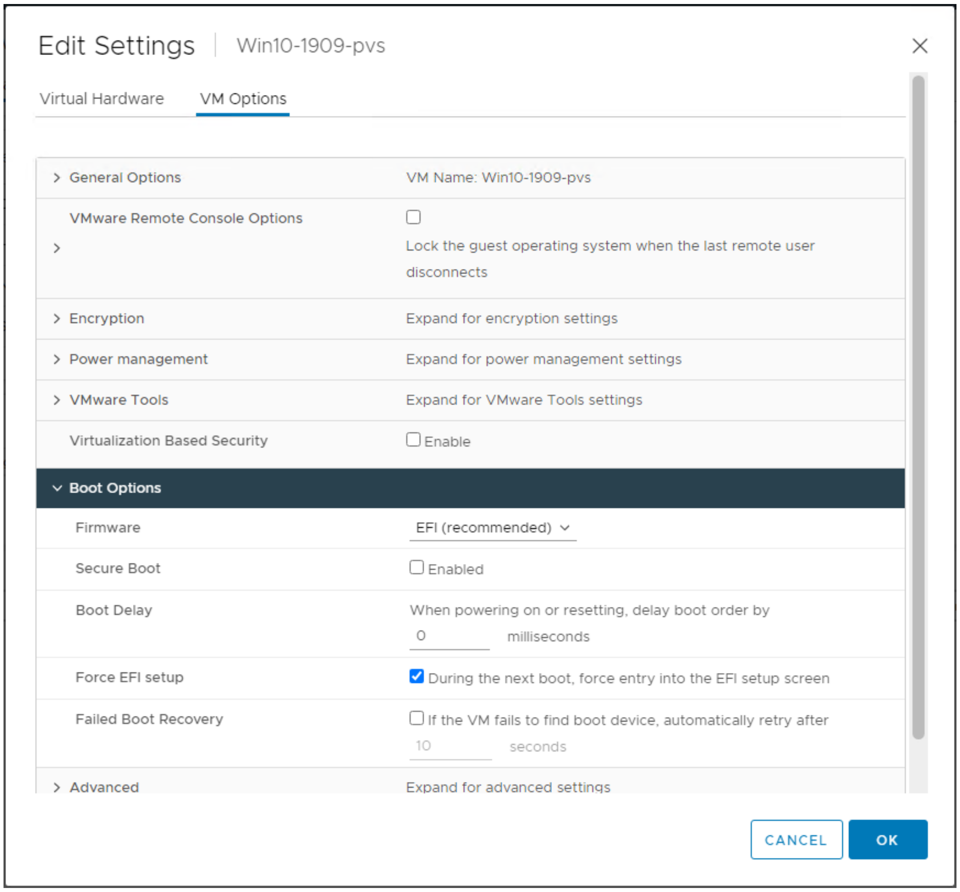
Step 21. When prompted, click No to shut down the machine.



Reboot or Shut Down, and Set Network Boot

Do you want the device to reboot, if not, the device will be shut down. Before reboot or after shut down, configure the machine settings for network boot.

Step 22. Edit the VM settings and select Force EFI Setup under Boot Options.

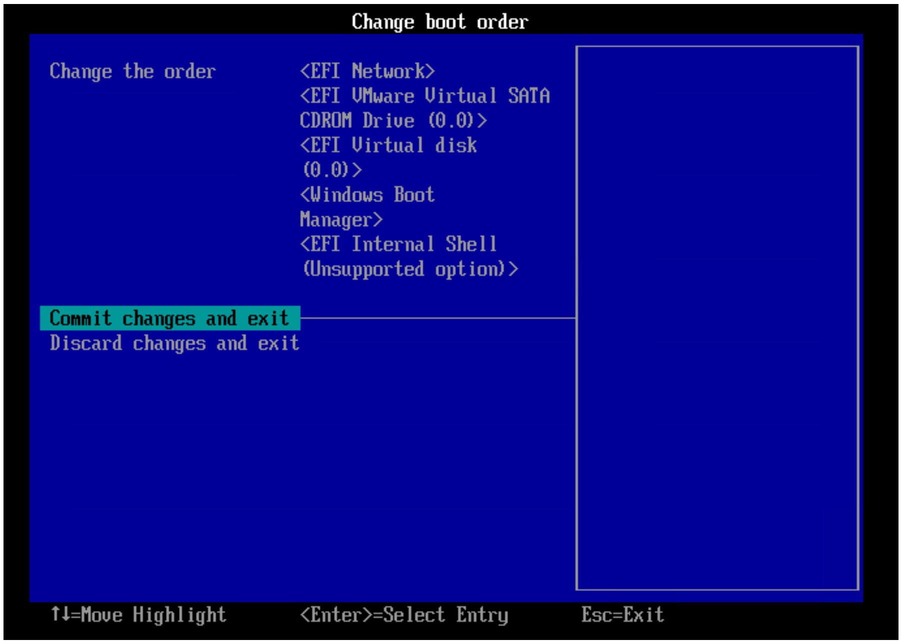


Edit Settings | Win10-1909-pvs

› General Options	VM Name: Win10-1909-pvs
› VMware Remote Console Options	□ Lock the guest operating system when the last remote user disconnects
› Encryption	Expand for encryption settings
› Power management	Expand for power management settings
› VMware Tools	Expand for VMware Tools settings
Virtualization Based Security	□ Enable
⌄ Boot Options	
Firmware	EFI (recommended) ⌄
Secure Boot	□ Enabled
Boot Delay	When powering on or resetting, delay boot order by 0 milliseconds
Force EFI setup	☑ During the next boot, force entry into the EFI setup screen
Failed Boot Recovery	□ If the VM fails to find boot device, automatically retry after 10 seconds
› Advanced	Expand for advanced settings

Step 23. Configure the VM settings for EFI network boot.

Step 24. Click Commit changes and exit.



Change boot order

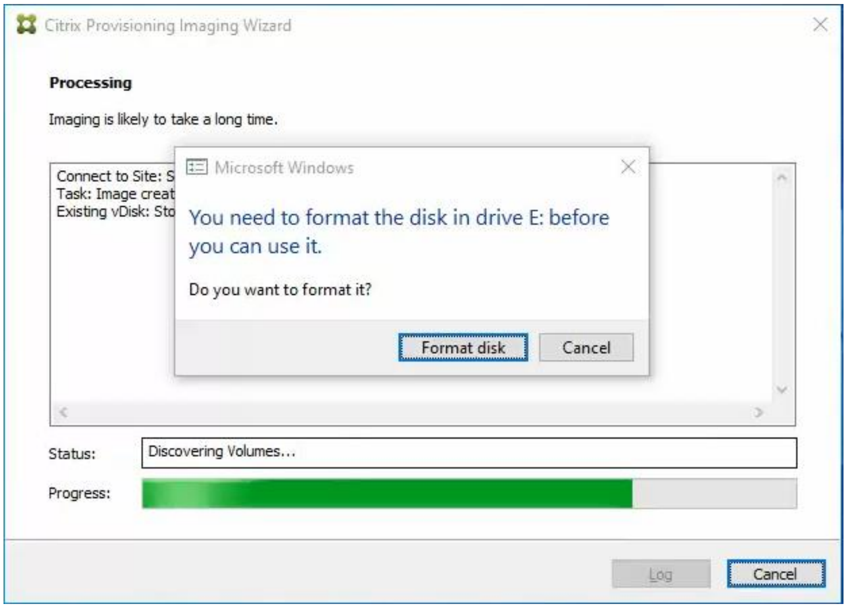
Change the order <EFI Network> <EFI VMware Virtual SATA CDROM Drive (0.0)> <EFI Virtual disk (0.0)> <Windows Boot Manager> <EFI Internal Shell (Unsupported option)>

Commit changes and exit
Discard changes and exit

↑↓=Move Highlight <Enter>=Select Entry Esc=Exit

Step 25. After restarting the virtual machine, log into the master target. The PVS imaging process begins, copying the contents of the C: drive to the PVS vDisk located on the server.

Note: If prompted to Format disk, disregard the message, and allow Provisioning Imaging Wizard to finish.


Citrix Provisioning Imaging Wizard

Processing

Imaging is likely to take a long time.

Connect to Site: S
Task: Image creat
Existing vDisk: Sto

Microsoft Windows

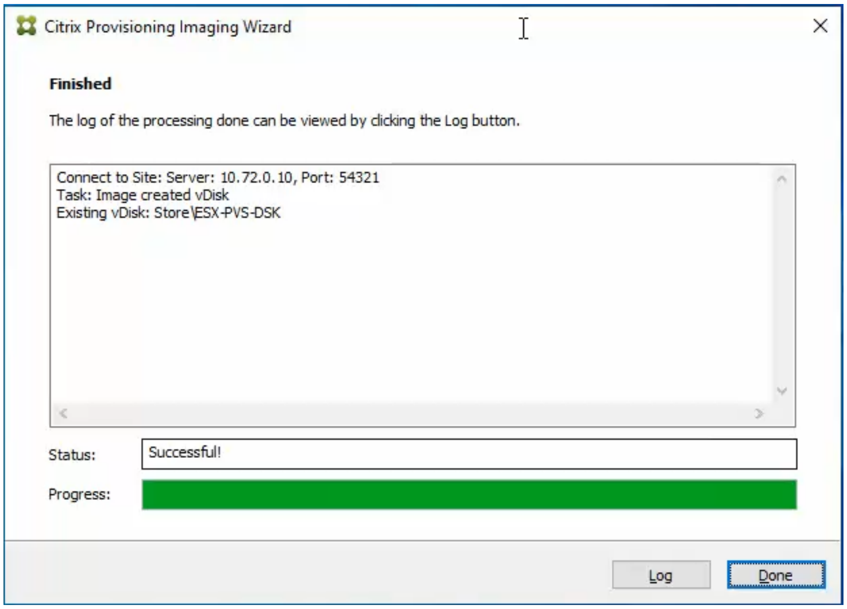
You need to format the disk in drive E: before you can use it.

Do you want to format it?

Status: Discovering Volumes...

Progress:

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


Citrix Provisioning Imaging Wizard

Finished

The log of the processing done can be viewed by clicking the Log button.

```
Connect to Site: Server: 10.72.0.10, Port: 54321
Task: Image created vDisk
Existing vDisk: Store\ESX-PVS-DSK
```

Status: Successful!

Progress:

Step 27. Shutdown the virtual machine used as the VDI or RDS master target.

Step 28. Connect to the PVS server and validate that the vDisk image is available in the Store.

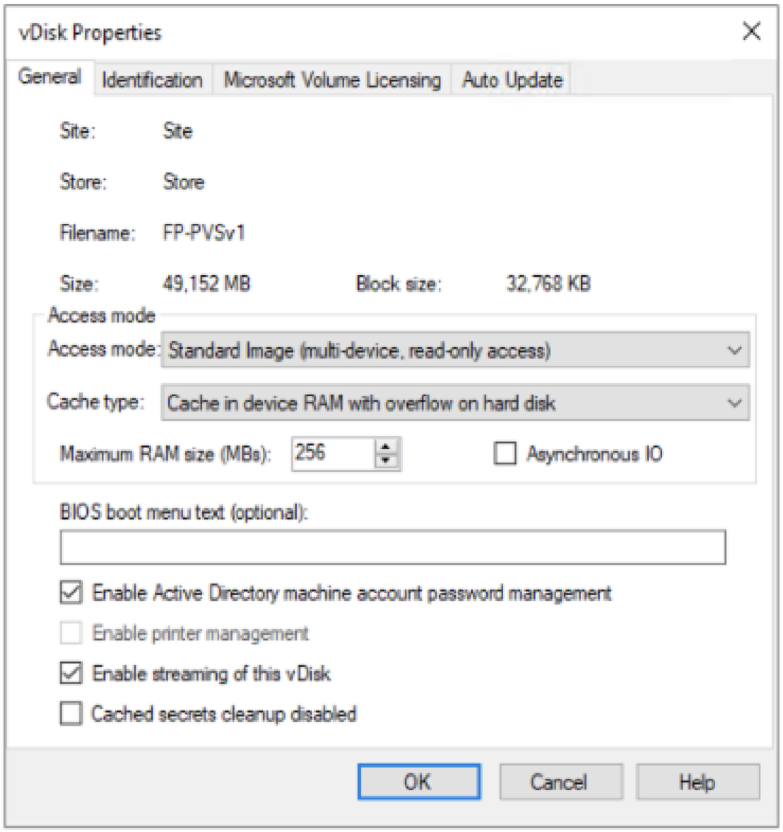
Step 29. Right-click the newly created vDisk and select Properties.

Step 30. On the vDisk Properties dialog, change Access mode to “Standard Image (multi-device, read-only access).”

Step 31. Set the Cache Type to “Cache in device RAM with overflow on hard disk.”

Step 32. Set Maximum RAM size (MBs): 256.

Step 33. Click OK.



vDisk Properties

Site: Site

Store: Store

Filename: FP-PVSv1

Size: 49,152 MB Block size: 32,768 KB

Access mode

Access mode: Standard Image (multi-device, read-only access)

Cache type: Cache in device RAM with overflow on hard disk

Maximum RAM size (MBs): 256 □ Asynchronous IO

BIOS boot menu text (optional):

☑ Enable Active Directory machine account password management

□ Enable printer management

☑ Enable streaming of this vDisk

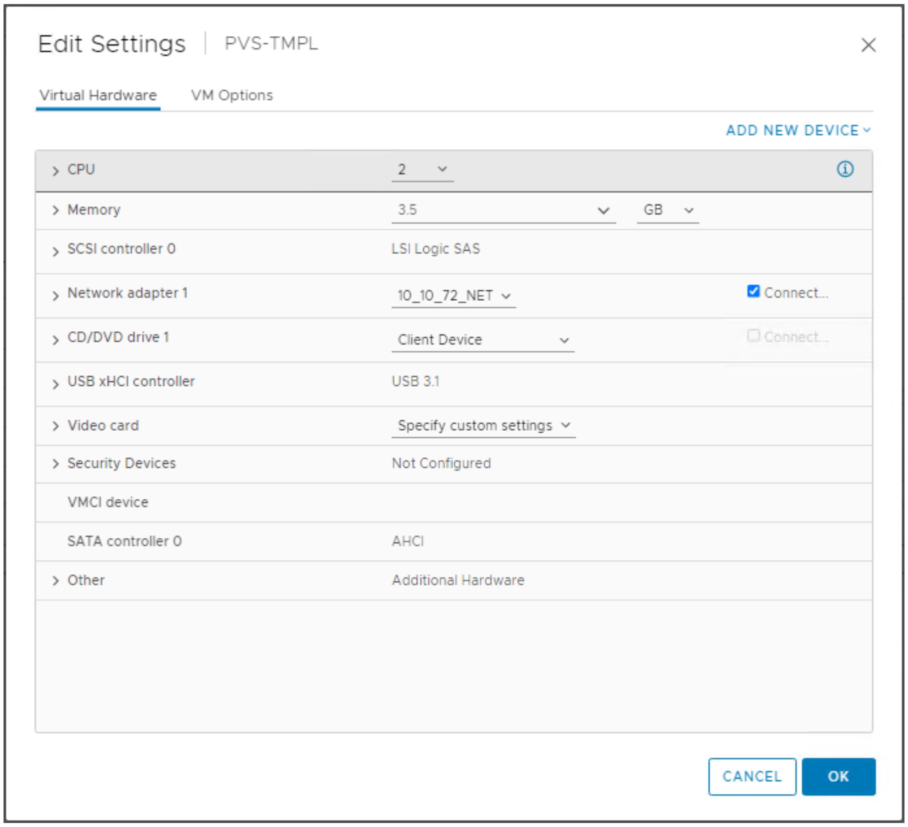
□ Cached secrets cleanup disabled

Provision Virtual Desktop Machines

Citrix Provisioning Services Citrix Virtual Desktop Setup Wizard

Procedure 1. Create PVS Streamed Virtual Desktop Machines

Step 1. Create a Master Target Virtual Machine:



Edit Settings | PVS-TMPL

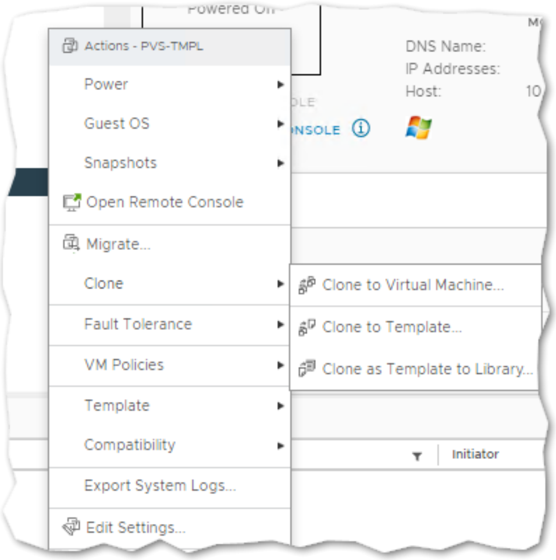
Virtual Hardware   VM Options

ADD NEW DEVICE

CPU	2	
Memory	3.5 GB	
SCSI controller 0	LSI Logic SAS	
Network adapter 1	10_10_72_NET	☑ Connect...
CD/DVD drive 1	Client Device	□ Connect...
USB xHCI controller	USB 3.1	
Video card	Specify custom settings	
Security Devices	Not Configured	
VMCI device		
SATA controller 0	AHCI	
Other	Additional Hardware	

CANCEL   OK

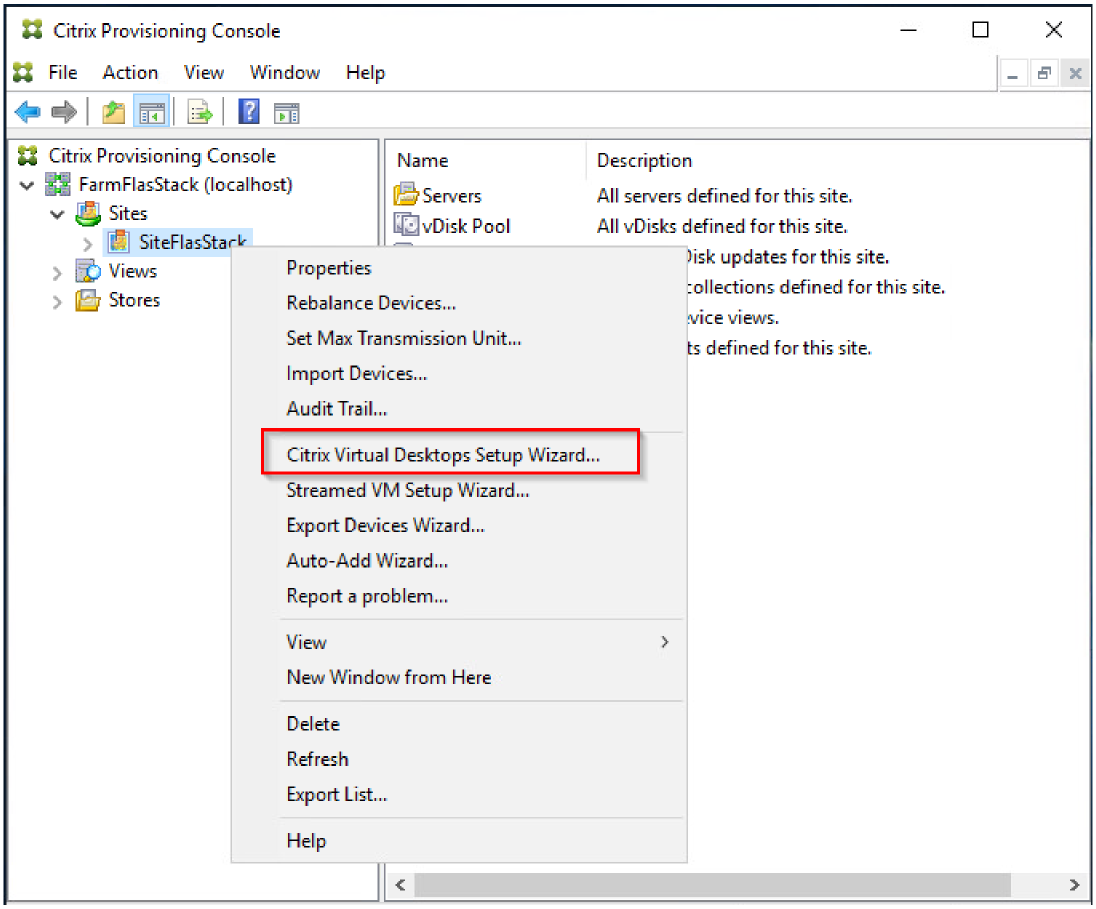
Step 2. Right-click and clone the Master Target VM to the Template.



Step 3. Start the Citrix Virtual Apps and Desktops Setup Wizard from the Provisioning Services Console.

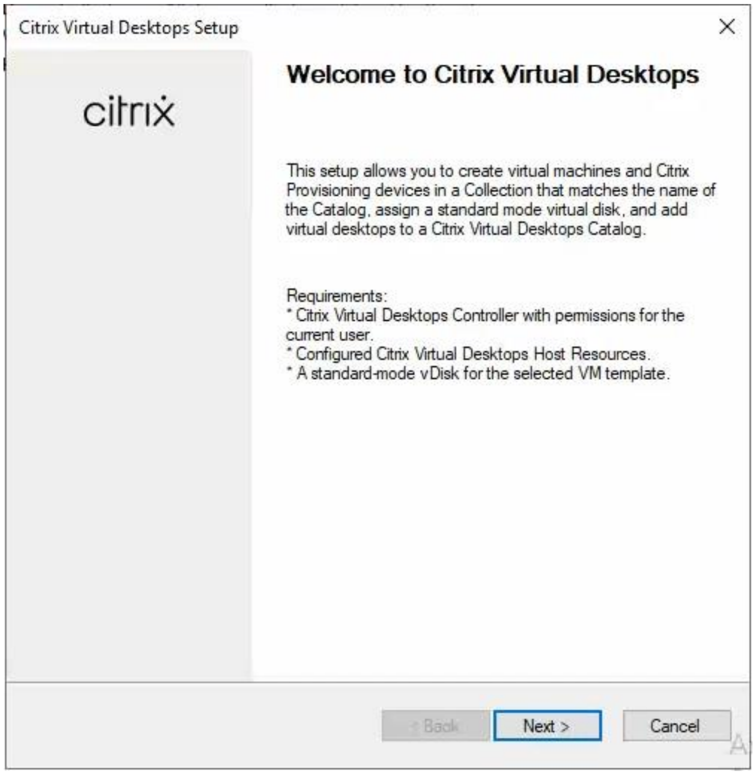
Step 4. Right-click the Site.

Step 5. Select Citrix Virtual Desktop Setup Wizard... from the context menu.



Name	Description
Servers	All servers defined for this site.
vDisk Pool	All vDisks defined for this site.
	)isk updates for this site.
	:ollections defined for this site.
	vice views.
	ts defined for this site.

Step 6. Click Next.



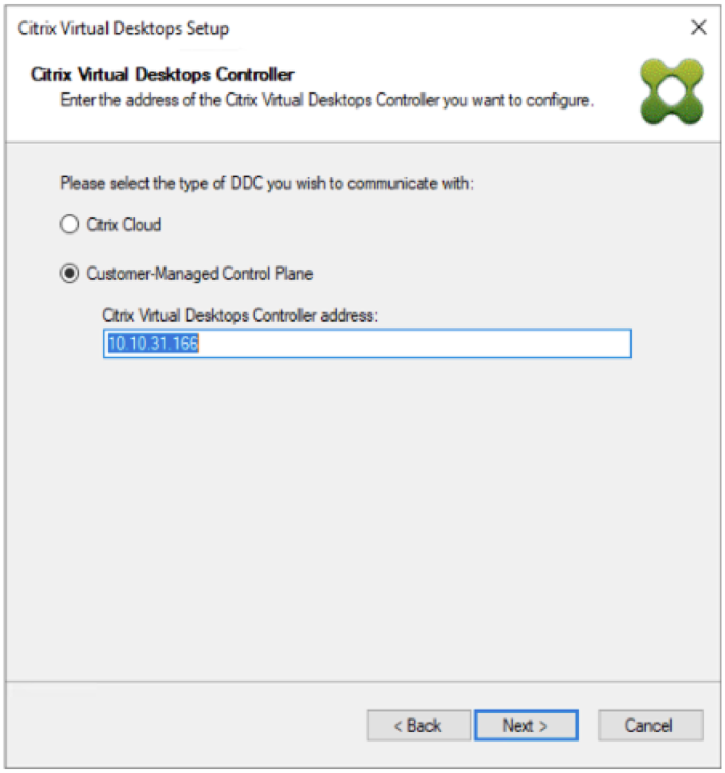
Welcome to Citrix Virtual Desktops

This setup allows you to create virtual machines and Citrix Provisioning devices in a Collection that matches the name of the Catalog, assign a standard mode virtual disk, and add virtual desktops to a Citrix Virtual Desktops Catalog.

Requirements:
* Citrix Virtual Desktops Controller with permissions for the current user.
* Configured Citrix Virtual Desktops Host Resources.
* A standard-mode vDisk for the selected VM template.

Step 7. Enter the address of the Citrix Virtual Desktop Controller that will be used for the wizard operations.

Step 8. Click Next.



Citrix Virtual Desktops Setup

Citrix Virtual Desktops Controller

Enter the address of the Citrix Virtual Desktops Controller you want to configure.

Please select the type of DDC you wish to communicate with:

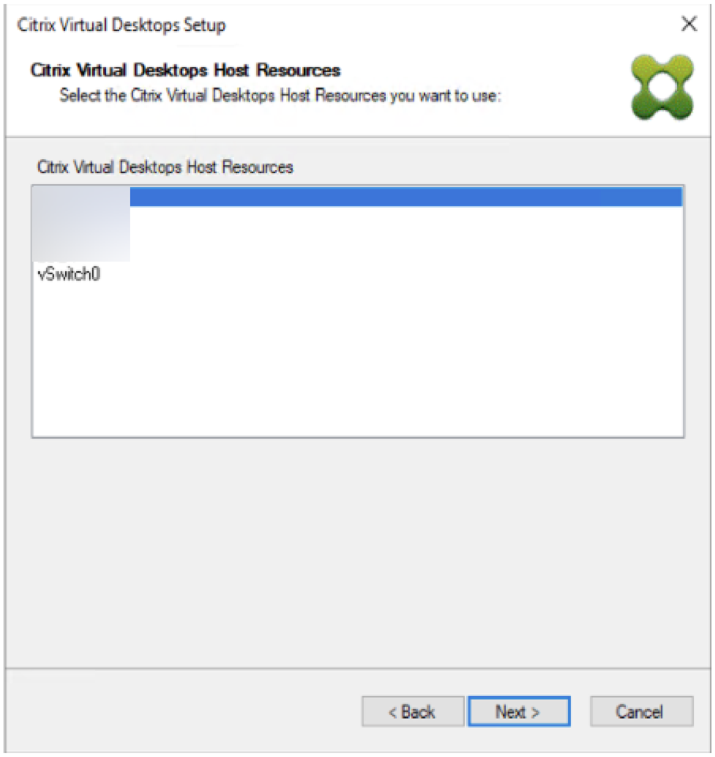
○ Citrix Cloud

● Customer-Managed Control Plane

Citrix Virtual Desktops Controller address: 10.10.31.166

Step 9. Select Host Resources that will be used for the wizard operations

Step 10. Click Next.



Citrix Virtual Desktops Setup

Citrix Virtual Desktops Host Resources

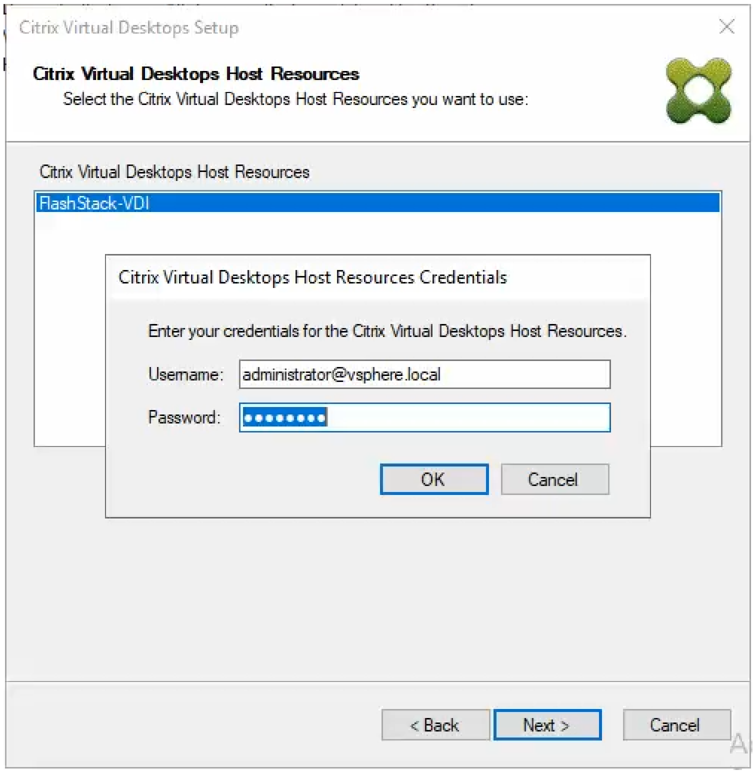
Select the Citrix Virtual Desktops Host Resources you want to use:

Citrix Virtual Desktops Host Resources

vSwitch0

Step 11. Provide Citrix Virtual Desktop Controller credentials.

Step 12. Click OK.



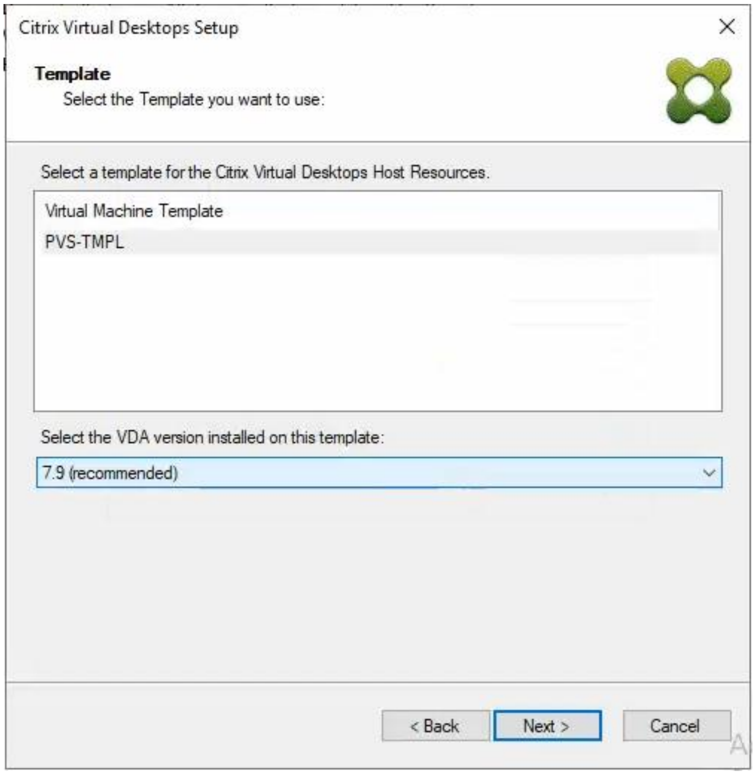
Citrix Virtual Desktops Setup
Citrix Virtual Desktops Host Resources
Select the Citrix Virtual Desktops Host Resources you want to use:
Citrix Virtual Desktops Host Resources
FlashStack-VDI
Citrix Virtual Desktops Host Resources Credentials
Enter your credentials for the Citrix Virtual Desktops Host Resources.
OK
Cancel
< Back
Next >
Cancel

Username: administrator@vsphere.local

Password: ••••••••

Step 13. Select the Template created earlier.

Step 14. Click Next.

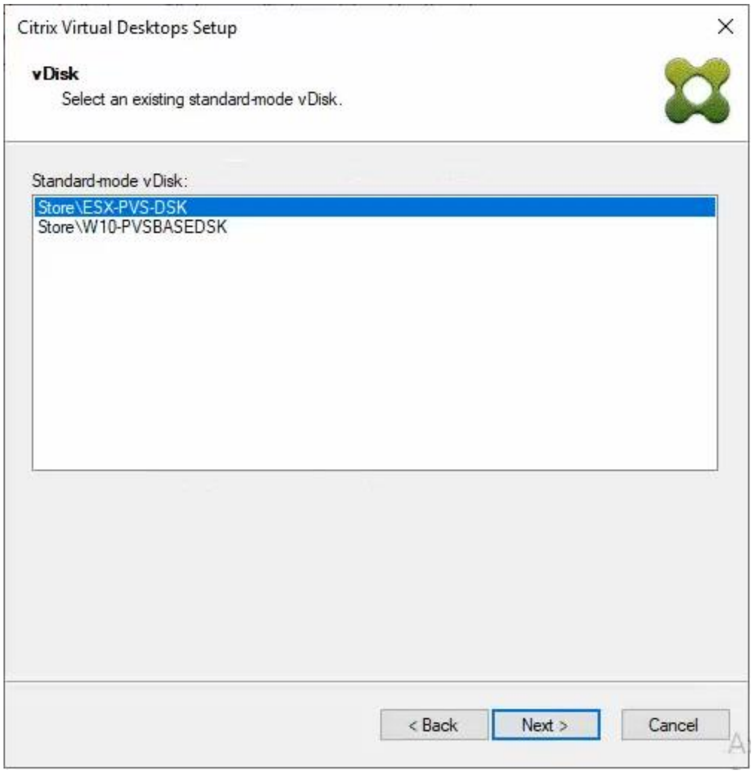


Citrix Virtual Desktops Setup
Template
Select the Template you want to use:
Select a template for the Citrix Virtual Desktops Host Resources.
Virtual Machine Template
PVS-TMPL
< Back
Next >
Cancel

Select the VDA version installed on this template: 7.9 (recommended)

Step 15. Select the virtual disk (vDisk) that will be used to stream the provisioned virtual machines.

Step 16. Click Next.


Citrix Virtual Desktops Setup

vDisk

Select an existing standard-mode vDisk.

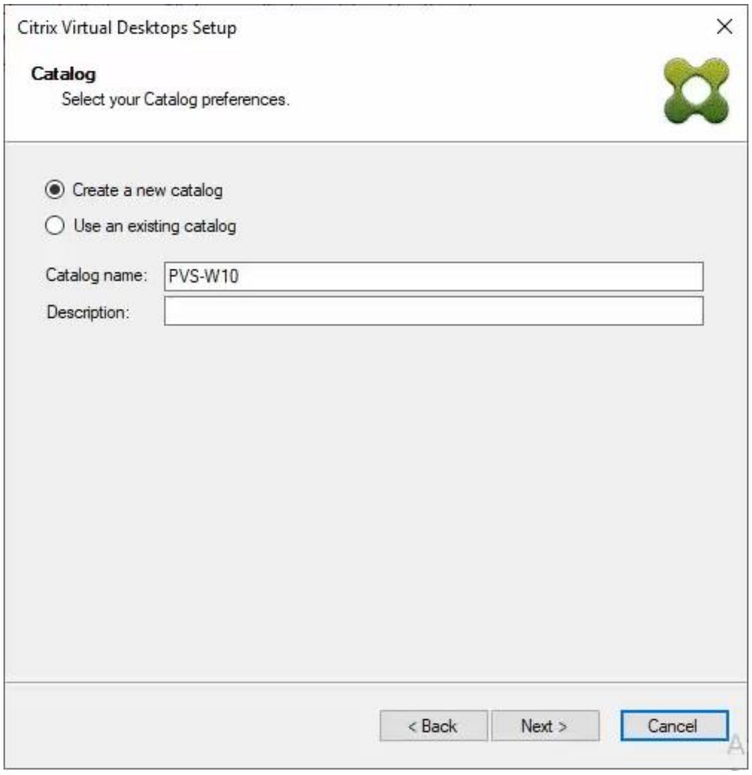
Standard-mode vDisk:

Store\ESX-PVS-DSK
Store\W10-PVSBASEDSK

Step 17. Select Create new catalog.

Step 18. Provide a catalog name.

Step 19. Click Next.


Citrix Virtual Desktops Setup

Catalog

Select your Catalog preferences.

● Create a new catalog

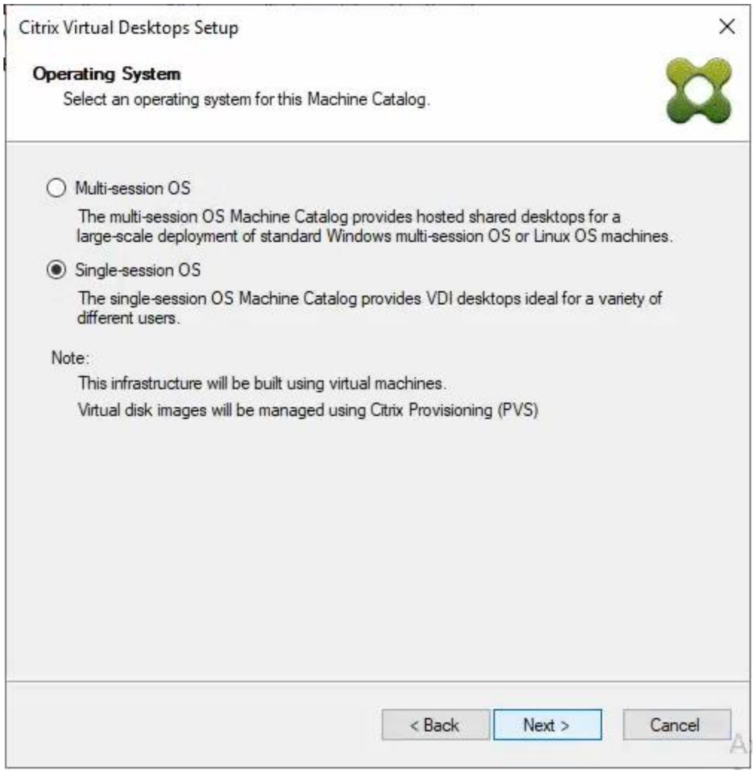
○ Use an existing catalog

Catalog name: PVS-W10

Description:

Step 20. Select Single-session OS for Machine catalog Operating System.

Step 21. Click Next.



Citrix Virtual Desktops Setup

Operating System

Select an operating system for this Machine Catalog.

○ Multi-session OS

The multi-session OS Machine Catalog provides hosted shared desktops for a large-scale deployment of standard Windows multi-session OS or Linux OS machines.

● Single-session OS

The single-session OS Machine Catalog provides VDI desktops ideal for a variety of different users.

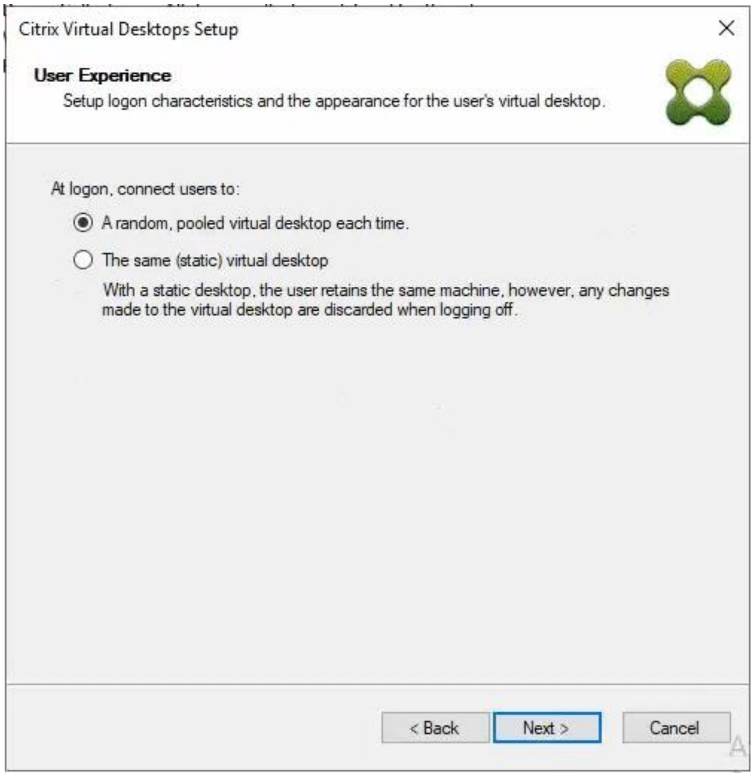
Note:

This infrastructure will be built using virtual machines.

Virtual disk images will be managed using Citrix Provisioning (PVS)

Step 22. Select random for the User Experience.

Step 23. Click Next.



Citrix Virtual Desktops Setup

User Experience

Setup logon characteristics and the appearance for the user's virtual desktop.

At logon, connect users to:

● A random, pooled virtual desktop each time.

○ The same (static) virtual desktop

With a static desktop, the user retains the same machine, however, any changes made to the virtual desktop are discarded when logging off.

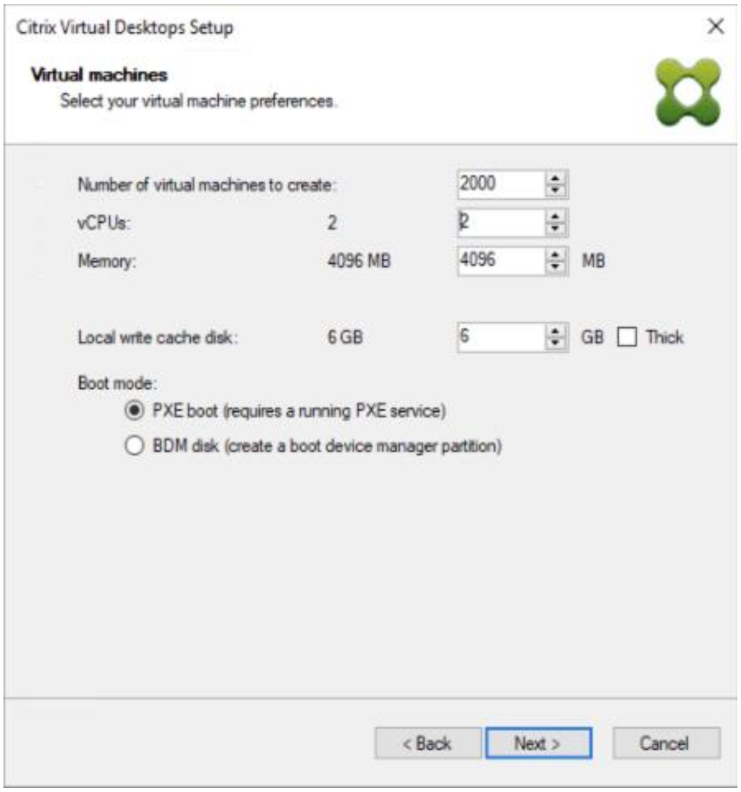
Step 24. On the Virtual machines dialog, specify the following:

- The number of virtual machines to create.

Note: It is recommended to create 200 or less per provisioning run. Create a single virtual machine at first to verify the procedure.

- 2 for Number of vCPUs for the virtual machine
- 3584 MB for the amount of memory for the virtual machine
- 6GB for the Local write cache disk.

Step 25. Click Next.



Citrix Virtual Desktops Setup

Virtual machines

Select your virtual machine preferences.

Number of virtual machines to create: 2000

vCPUs: 2 2

Memory: 4096 MB 4096 MB

Local write cache disk: 6 GB 6 GB □ Thick

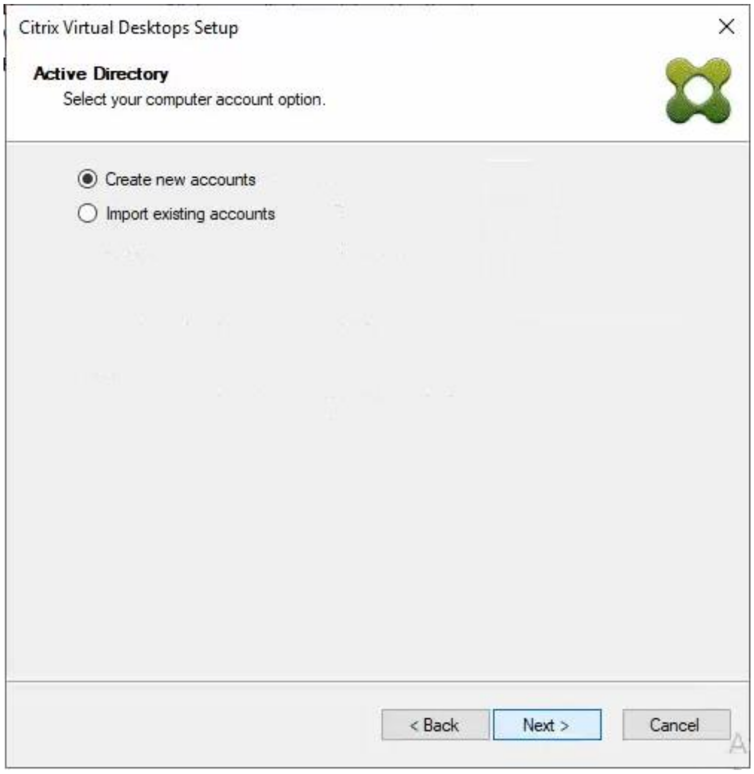
Boot mode:

● PXE boot (requires a running PXE service)

○ BDM disk (create a boot device manager partition)

Step 26. Select the Create new accounts.

Step 27. Click Next.



Citrix Virtual Desktops Setup

Active Directory

Select your computer account option.

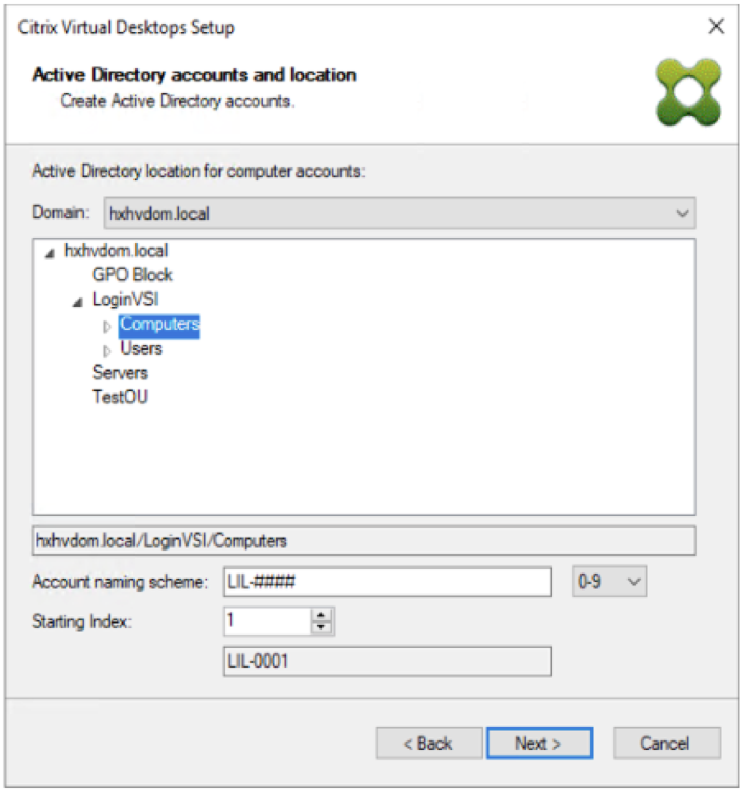
● Create new accounts

○ Import existing accounts

Step 28. Specify the Active Directory Accounts and Location. This is where the wizard should create computer accounts.

Step 29. Provide the Account naming scheme. An example name is shown in the text box below the naming scheme selection location.

Step 30. Click Next.



Citrix Virtual Desktops Setup

Active Directory accounts and location

Create Active Directory accounts.

Active Directory location for computer accounts:

Domain: hxhvdom.local

hxhvdom.local/LoginVSI/Computers

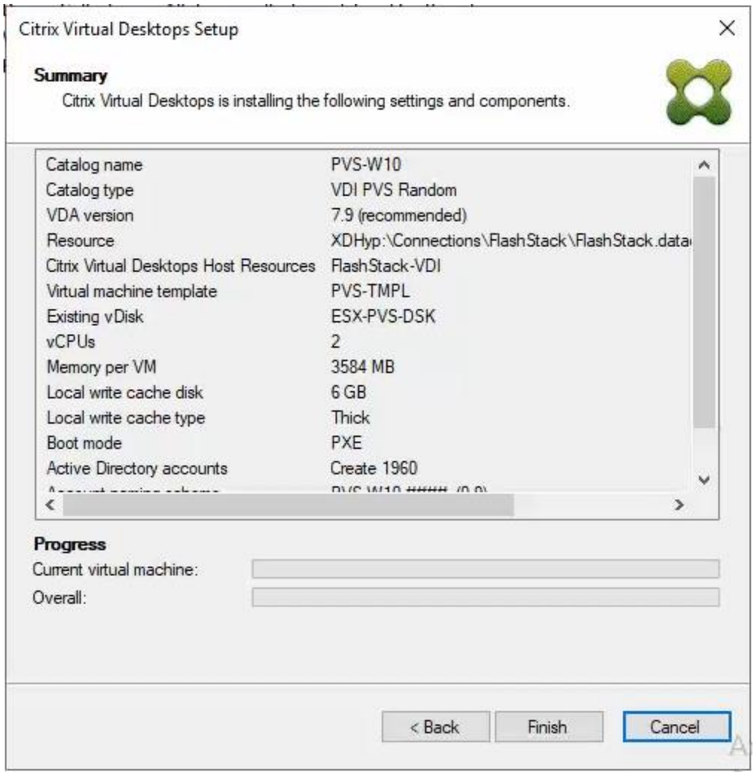
Account naming scheme: LIL-#### 0-9

Starting Index: 1

LIL-0001

Step 31. Verify the information on the Summary screen.

Step 32. Click Finish to begin the virtual machine creation.



Citrix Virtual Desktops Setup

Summary

Citrix Virtual Desktops is installing the following settings and components.

Catalog name	PVS-W10
Catalog type	VDI PVS Random
VDA version	7.9 (recommended)
Resource	XDHyp:\Connections\FlashStack\FlashStack.data
Citrix Virtual Desktops Host Resources	FlashStack-VDI
Virtual machine template	PVS-TMPL
Existing vDisk	ESX-PVS-DSK
vCPUs	2
Memory per VM	3584 MB
Local write cache disk	6 GB
Local write cache type	Thick
Boot mode	PXE
Active Directory accounts	Create 1960
Account naming scheme	PVS-W10-#### (0-9)

Progress

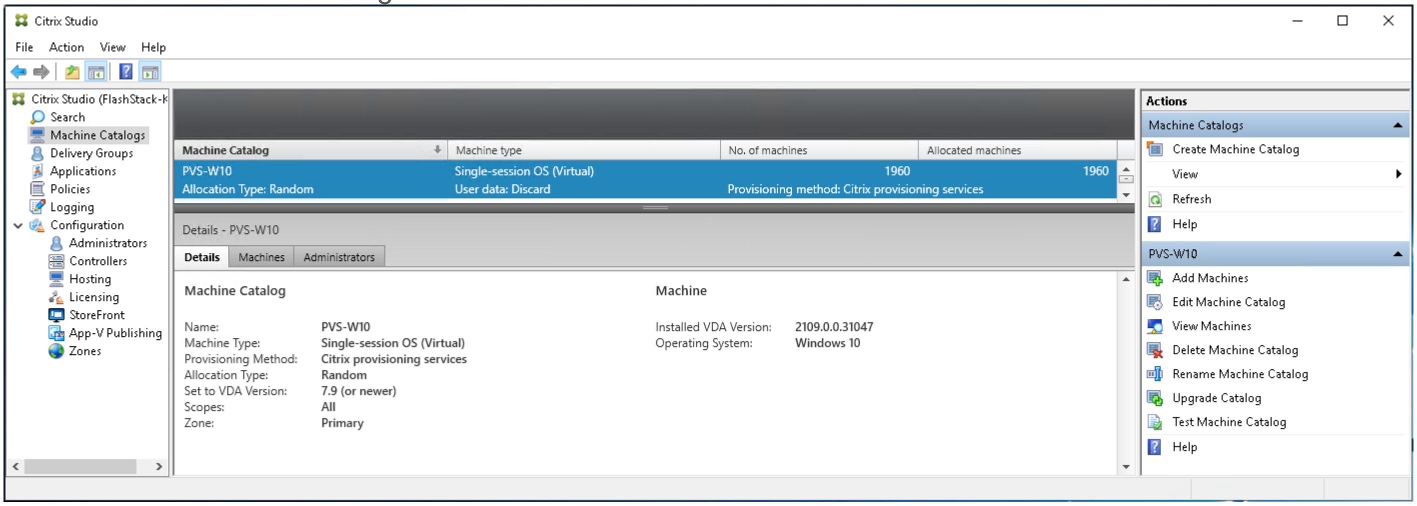
Current virtual machine:

Overall:

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

3. When the wizard is done provisioning the virtual machines, verify the Machine Catalog on the Citrix Virtual Apps and Desktops Controller:

    - Connect to a Citrix Virtual Apps and Desktops server and launch Citrix Studio.
    - Select Machine Catalogs in the Studio navigation pane.
    - Select a machine catalog.



Machine Catalog	Machine type	No. of machines	Allocated machines
PVS-W10 Allocation Type: Random	Single-session OS (Virtual) User data: Discard	1960 Provisioning method: Citrix provisioning services	1960

Details - PVS-W10

Details | Machines | Administrators

Machine Catalog

Name:	PVS-W10
Machine Type:	Single-session OS (Virtual)
Provisioning Method:	Citrix provisioning services
Allocation Type:	Random
Set to VDA Version:	7.9 (or newer)
Scopes:	All
Zone:	Primary

Machine

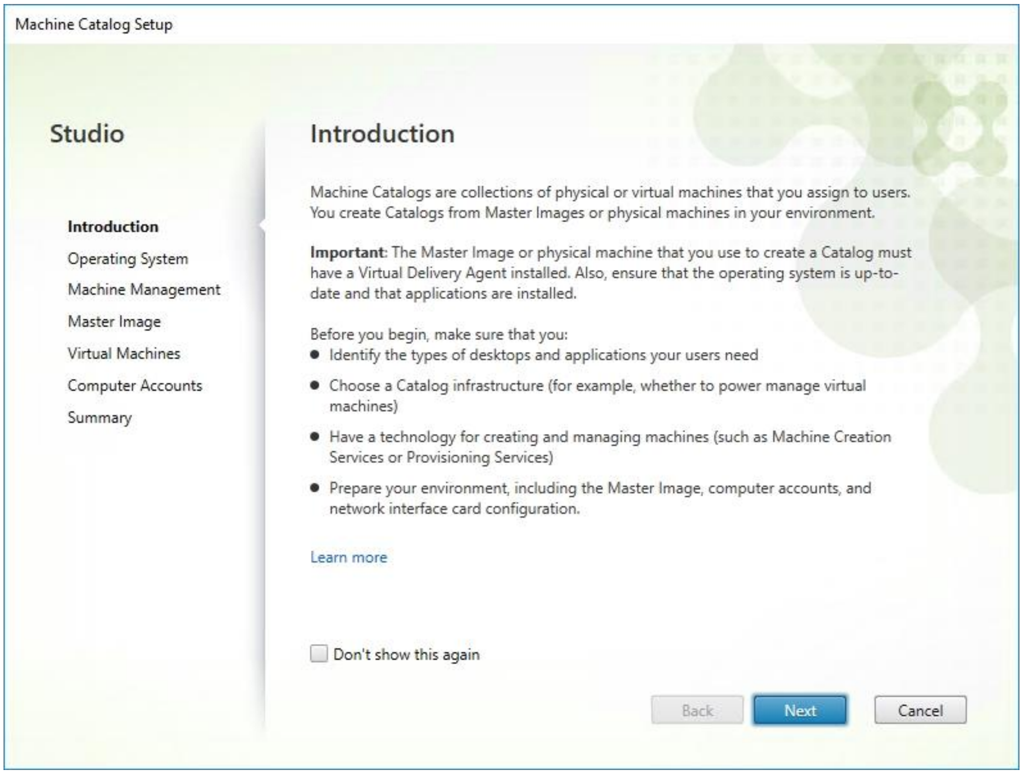
Installed VDA Version:	2109.0.0.31047
Operating System:	Windows 10

Procedure 2. Citrix Machine Creation Services

Step 1. Connect to a Citrix Virtual Apps and Desktops server and launch Citrix Studio.

Step 2. Choose Create Machine Catalog from the Actions pane.

Step 3. Click Next.



Machine Catalog Setup

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.

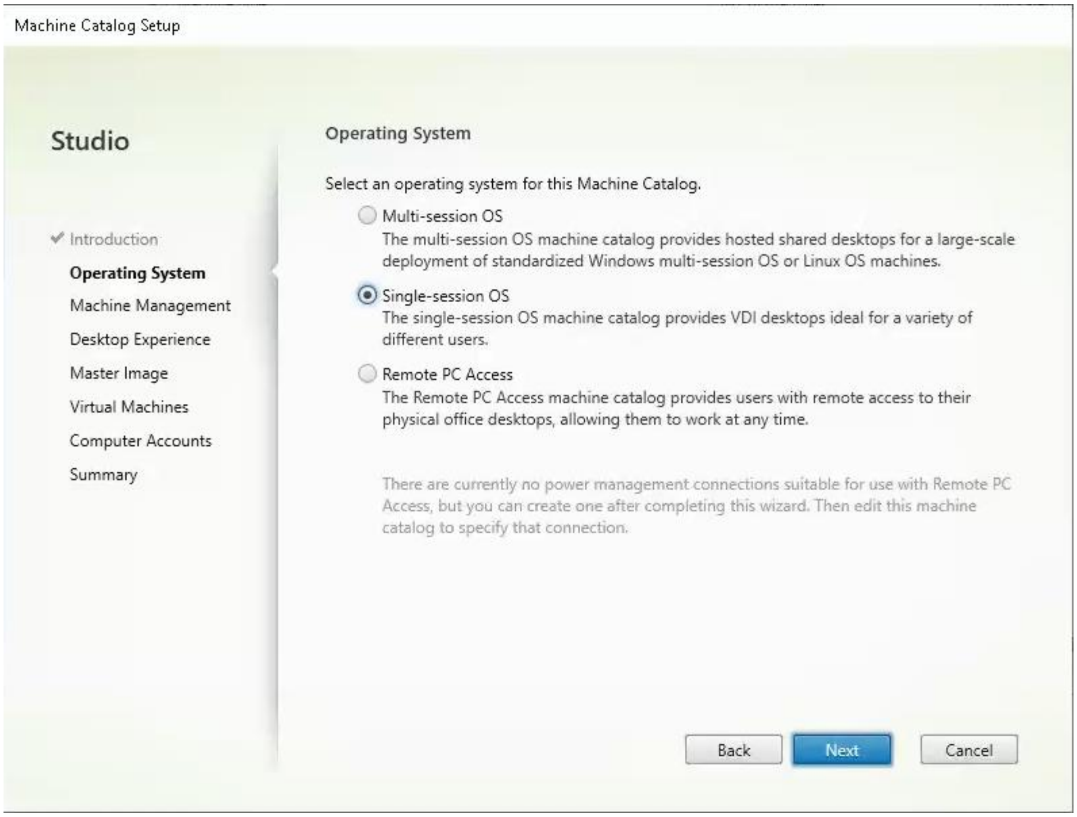
Important: The Master Image or physical machine that you use to create a Catalog must have a Virtual Delivery Agent installed. Also, ensure that the operating system is up-to-date and that applications are installed.

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.

Step 4. Select Single-session OS.

Step 5. Click Next.



Machine Catalog Setup

Studio

Operating System

Select an operating system for this Machine Catalog.

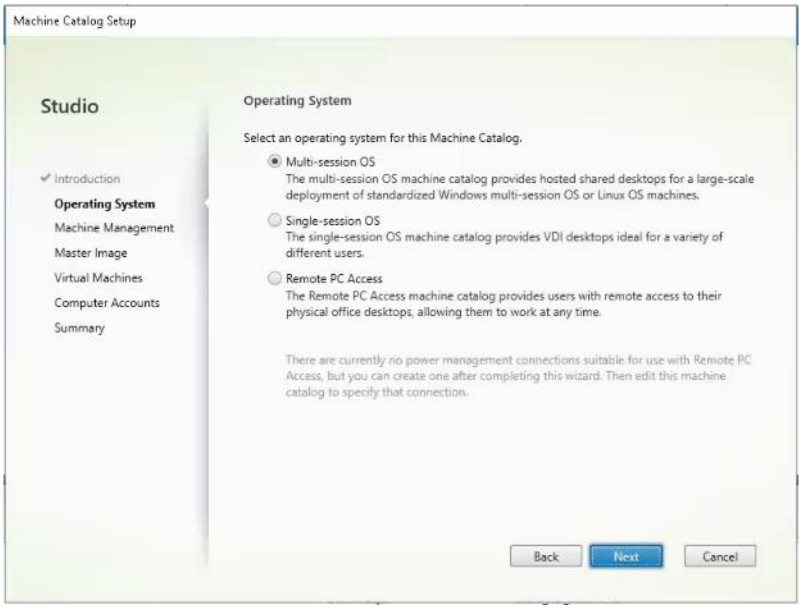
○ Multi-session OS
The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session OS or Linux OS machines.

● Single-session OS
The single-session OS machine catalog provides VDI desktops ideal for a variety of different users.

○ Remote PC Access
The Remote PC Access machine catalog provides users with remote access to their physical office desktops, allowing them to work at any time.

There are currently no power management connections suitable for use with Remote PC Access, but you can create one after completing this wizard. Then edit this machine catalog to specify that connection.

Step 6. Select Multi-session OS when using Windows Server 2019 desktops.



Machine Catalog Setup

Studio

Operating System

Select an operating system for this Machine Catalog.

● Multi-session OS
The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session OS or Linux OS machines.

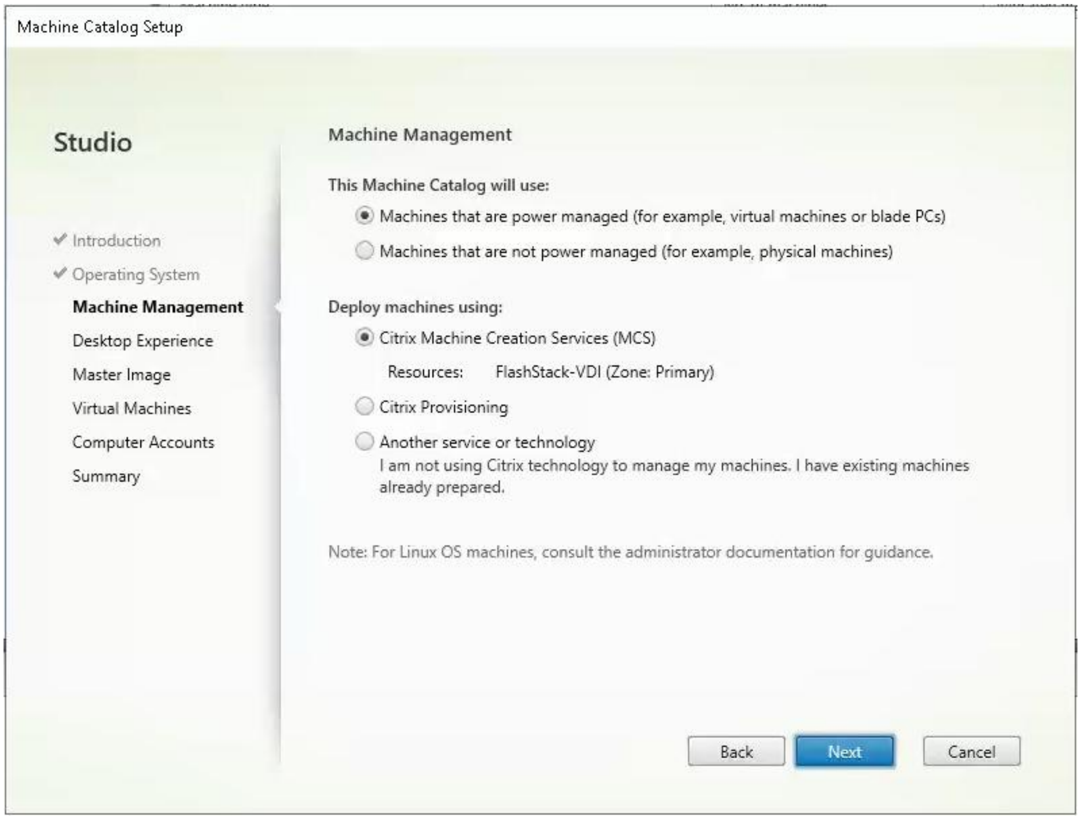
○ Single-session OS
The single-session OS machine catalog provides VDI desktops ideal for a variety of different users.

○ Remote PC Access
The Remote PC Access machine catalog provides users with remote access to their physical office desktops, allowing them to work at any time.

There are currently no power management connections suitable for use with Remote PC Access, but you can create one after completing this wizard. Then edit this machine catalog to specify that connection.

Step 7. Select the appropriate machine management.

Step 8. Click Next.



Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- **Machine Management**
- Desktop Experience
- Master Image
- Virtual Machines
- Computer Accounts
- Summary

Machine Management

This Machine Catalog will use:

● Machines that are power managed (for example, virtual machines or blade PCs)

○ Machines that are not power managed (for example, physical machines)

Deploy machines using:

● Citrix Machine Creation Services (MCS)

Resources: FlashStack-VDI (Zone: Primary)

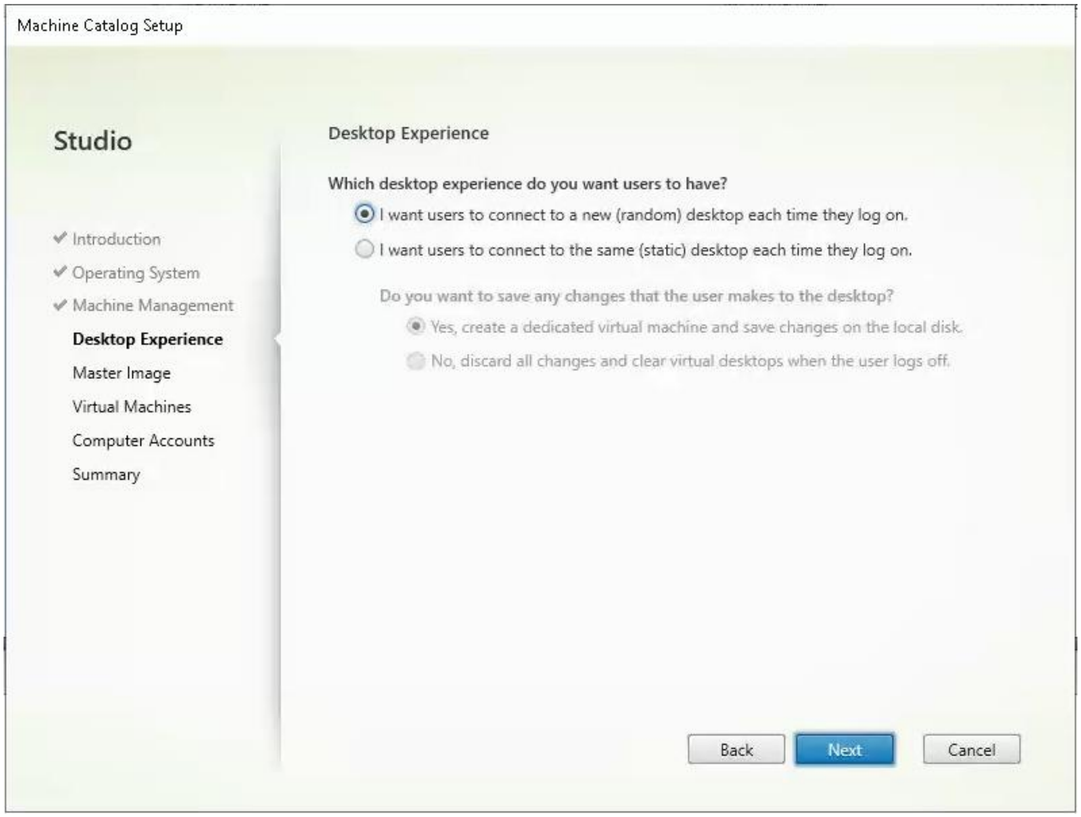
○ Citrix Provisioning

○ Another service or technology
I am not using Citrix technology to manage my machines. I have existing machines already prepared.

Note: For Linux OS machines, consult the administrator documentation for guidance.

Step 9. Select (random) for Desktop Experience.

Step 10. Click Next.



Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- **Desktop Experience**
- Master Image
- Virtual Machines
- Computer Accounts
- Summary

Desktop Experience

Which desktop experience do you want users to have?

● I want users to connect to a new (random) desktop each time they log on.

○ I want users to connect to the same (static) desktop each time they log on.

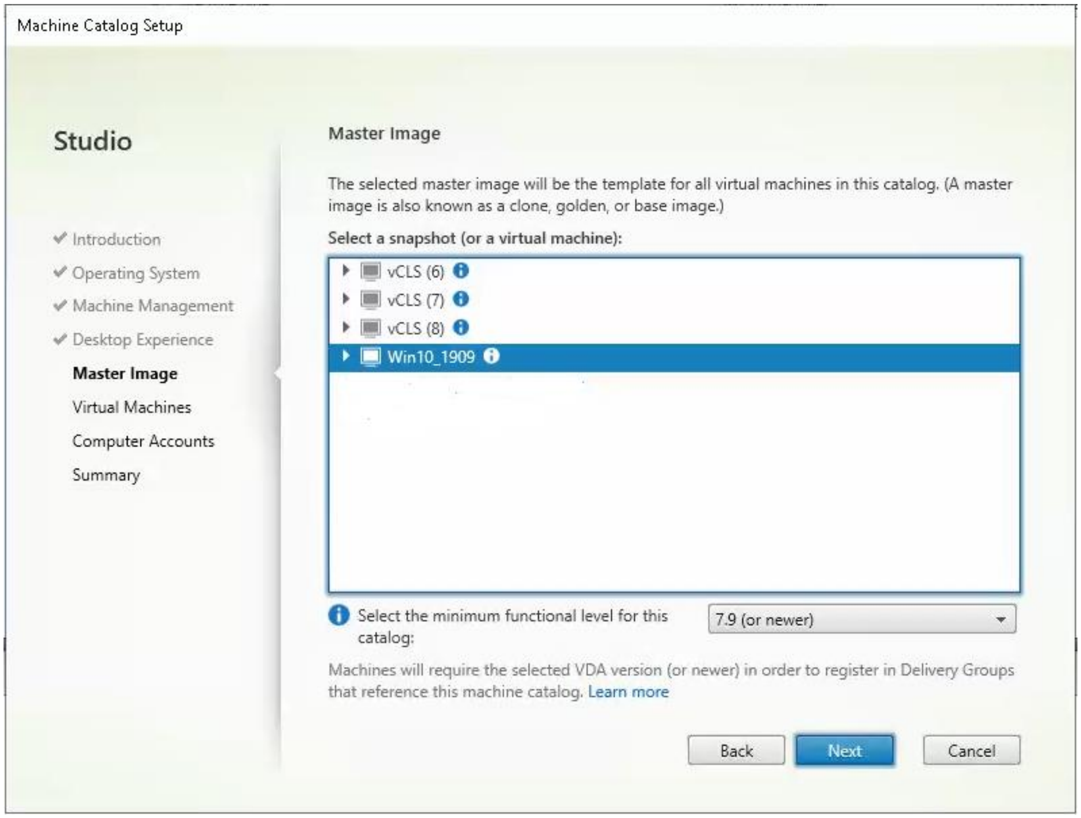
Do you want to save any changes that the user makes to the desktop?

● Yes, create a dedicated virtual machine and save changes on the local disk.

○ No, discard all changes and clear virtual desktops when the user logs off.

Step 11. Select a Virtual Machine to be used for Catalog Master Image.

Step 12. Click Next.



Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- **Master Image**
- Virtual Machines
- Computer Accounts
- Summary

Master Image

The selected master image will be the template for all virtual machines in this catalog. (A master image is also known as a clone, golden, or base image.)

Select a snapshot (or a virtual machine):

- vCLS (6)
- vCLS (7)
- vCLS (8)
- Win10_1909

Select the minimum functional level for this catalog: 7.9 (or newer)

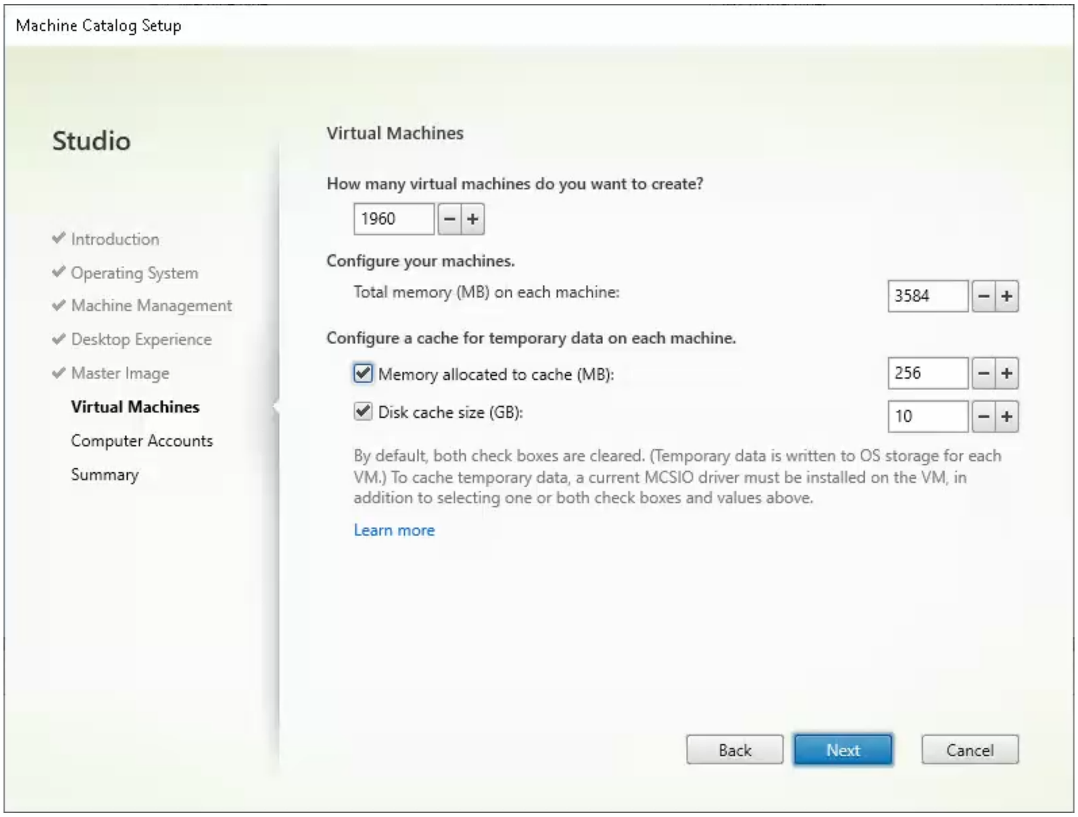
Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. Learn more

Step 13. Specify the number of desktops to create and machine configuration.

Step 14. Set amount of memory (MB) to be used by virtual desktops.

Step 15. Select Full Copy for machine copy mode.

Step 16. Click Next.



Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- **Virtual Machines**
- Computer Accounts
- Summary

Virtual Machines

How many virtual machines do you want to create?

1960

Configure your machines.

Total memory (MB) on each machine: 3584

Configure a cache for temporary data on each machine.

☑ Memory allocated to cache (MB): 256

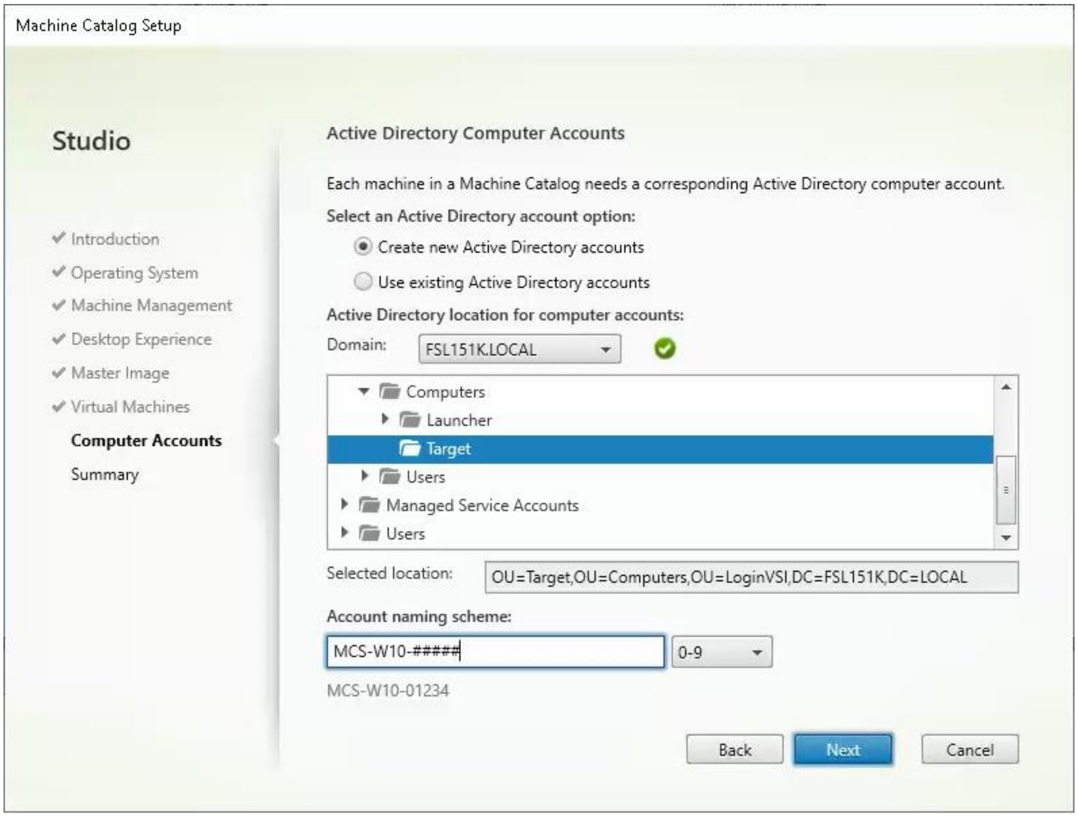
☑ Disk cache size (GB): 10

By default, both check boxes are cleared. (Temporary data is written to OS storage for each VM.) To cache temporary data, a current MCSIO driver must be installed on the VM, in addition to selecting one or both check boxes and values above.

Learn more

Step 17. Specify the AD account naming scheme and OU where accounts will be created.

Step 18. Click Next.



Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- ✓ Virtual Machines
- **Computer Accounts**
- Summary

Active Directory Computer Accounts

Each machine in a Machine Catalog needs a corresponding Active Directory computer account.

Select an Active Directory account option:

● Create new Active Directory accounts

○ Use existing Active Directory accounts

Active Directory location for computer accounts:

Domain: FSL151K.LOCAL ✓

- Computers
  - Launcher
  - Target
  - Users
- Managed Service Accounts
- Users

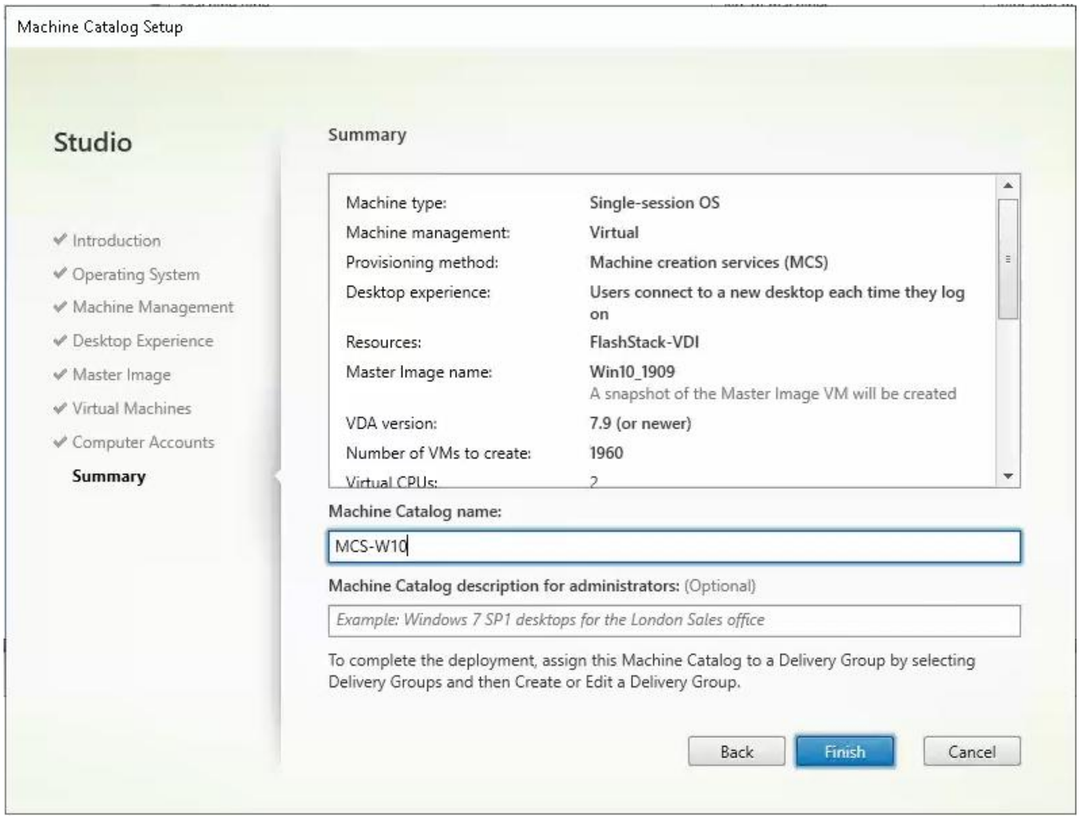
Selected location: OU=Target,OU=Computers,OU=LoginVSI,DC=FSL151K,DC=LOCAL

Account naming scheme:

MCS-W10-##### 0-9

MCS-W10-01234

Step 19. On the Summary page specify Catalog name and click Finish to start the deployment.



Machine Catalog Setup

Studio

Summary

Machine type:	Single-session OS
Machine management:	Virtual
Provisioning method:	Machine creation services (MCS)
Desktop experience:	Users connect to a new desktop each time they log on
Resources:	FlashStack-VDI
Master Image name:	Win10_1909 A snapshot of the Master Image VM will be created
VDA version:	7.9 (or newer)
Number of VMs to create:	1960
Virtual CPUs:	2

Machine Catalog name: MCS-W10

Machine Catalog description for administrators: (Optional)

Example: Windows 7 SP1 desktops for the London Sales office

To complete the deployment, assign this Machine Catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

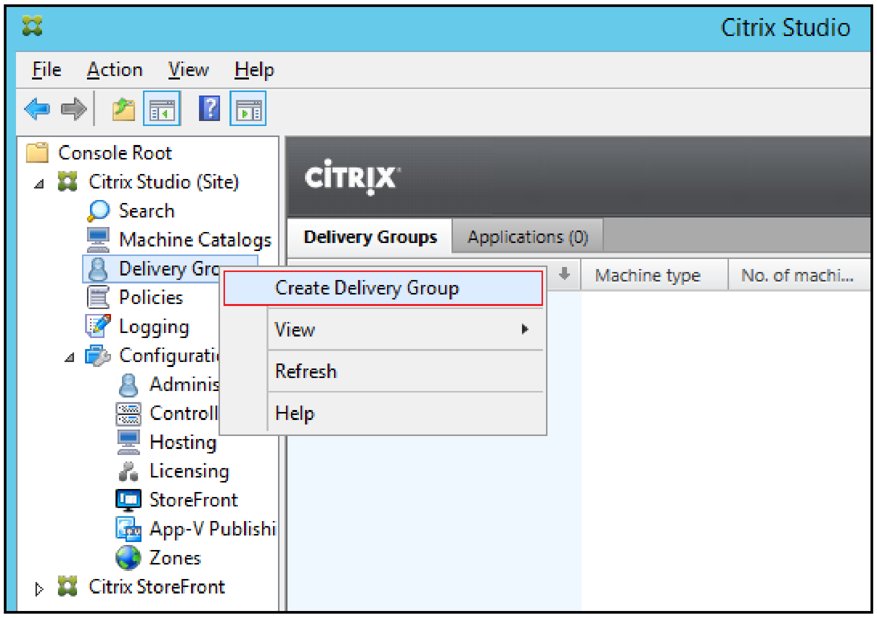
Procedure 3. Create Delivery Groups

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.

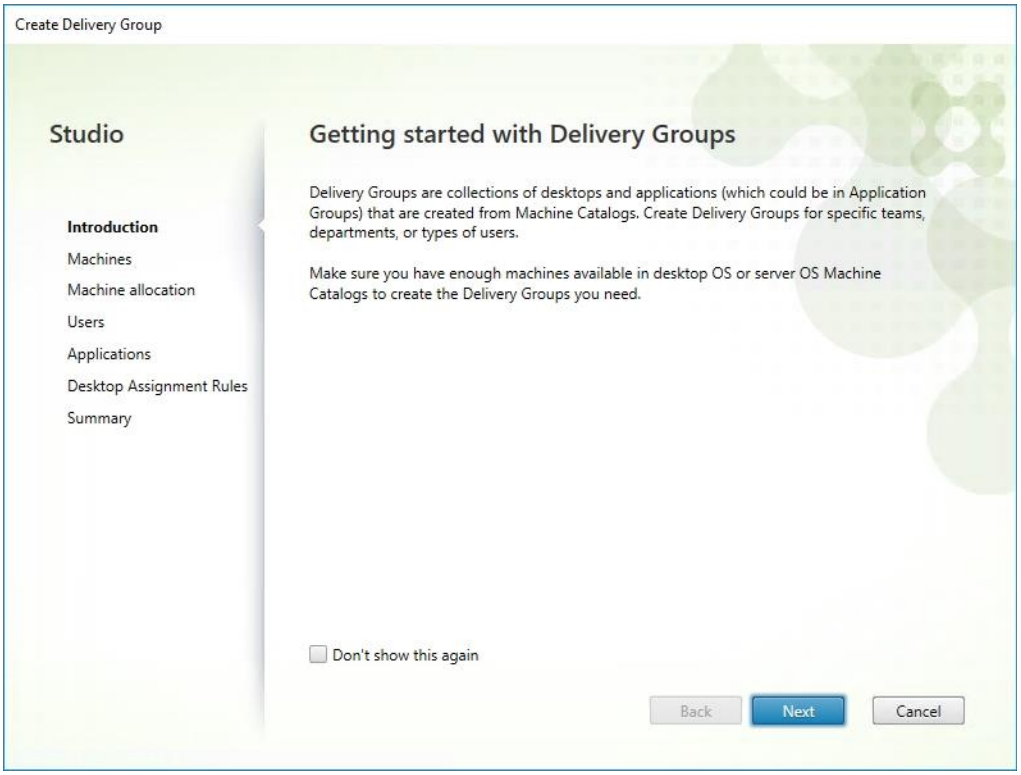
Note: The instructions below outline the procedure to create a Delivery Group for persistent VDI desktops. When you have completed these steps, repeat the procedure to a Delivery Group for RDS desktops.

Step 1. Connect to a Citrix Virtual Apps and Desktops server and launch Citrix Studio.

Step 2. Choose Create Delivery Group from the drop-down list.



Step 3. Click Next.



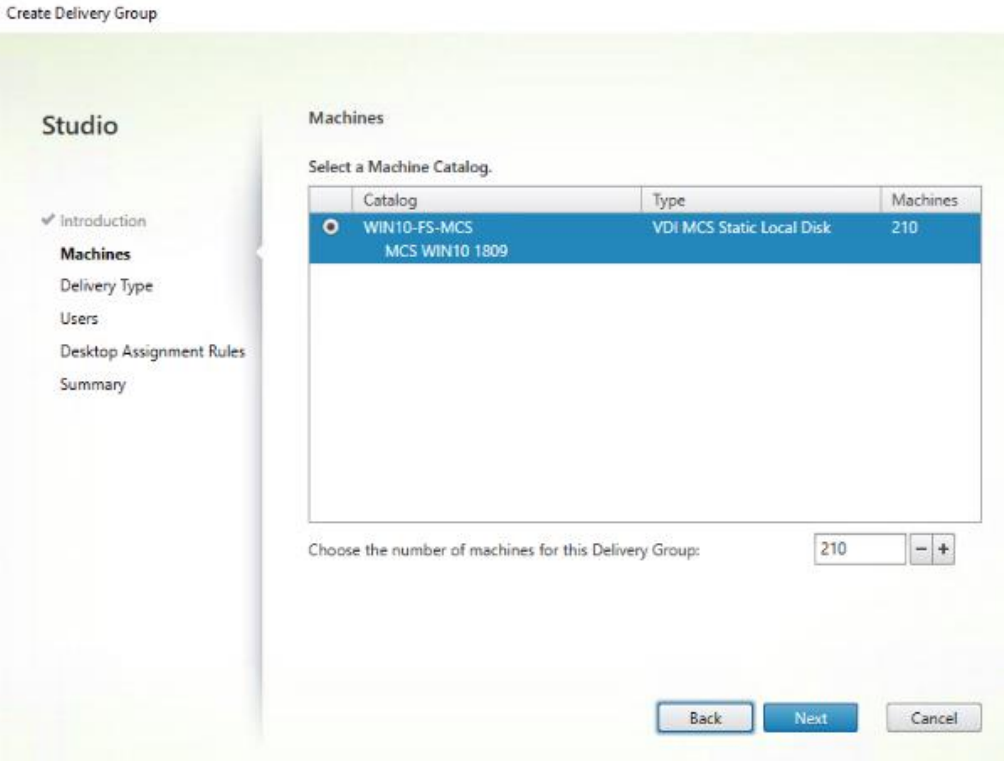
Getting started with Delivery Groups

Delivery Groups are collections of desktops and applications (which could be in Application Groups) that are created from Machine Catalogs. Create Delivery Groups for specific teams, departments, or types of users.

Make sure you have enough machines available in desktop OS or server OS Machine Catalogs to create the Delivery Groups you need.

Step 4. Specify the Machine Catalog and increment the number of machines to add.

Step 5. Click Next.


Create Delivery Group

Machines

Select a Machine Catalog.

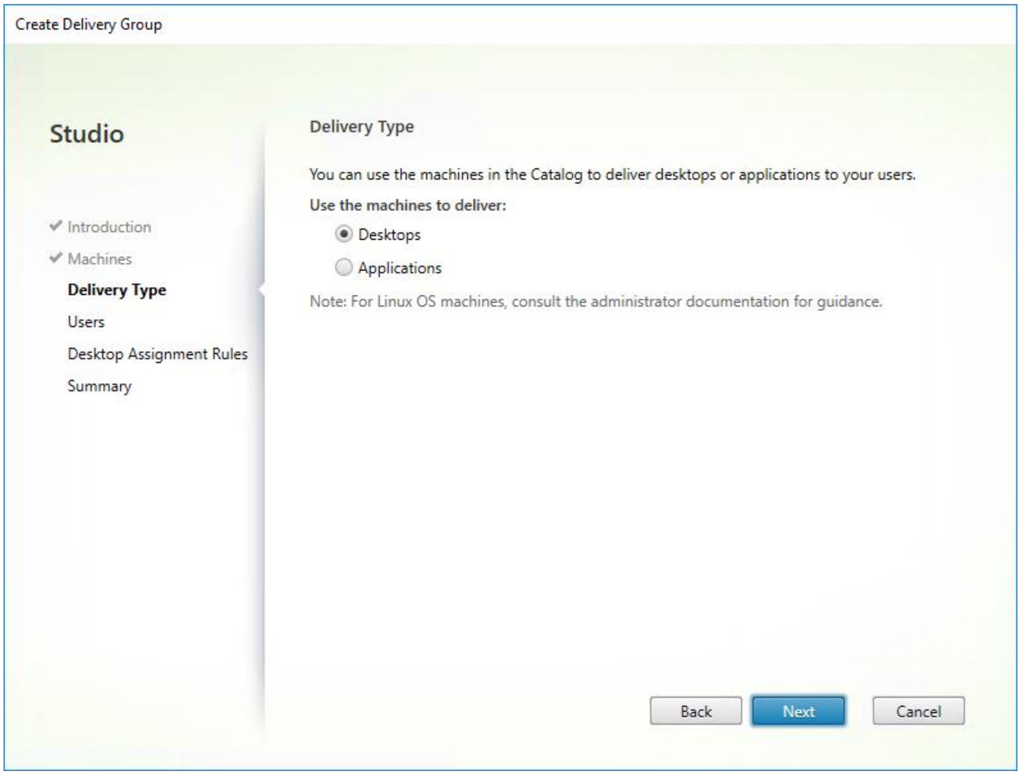
	Catalog	Type	Machines
●	WIN10-FS-MCS MCS WIN10 1809	VDI MCS Static Local Disk	210

Choose the number of machines for this Delivery Group: 210

Step 6. Specify what the machines in the catalog will deliver: Desktops, Desktops and Applications, or Applications.

Step 7. Select Desktops.

Step 8. Click Next.


Create Delivery Group

Delivery Type

You can use the machines in the Catalog to deliver desktops or applications to your users.

Use the machines to deliver:

● Desktops

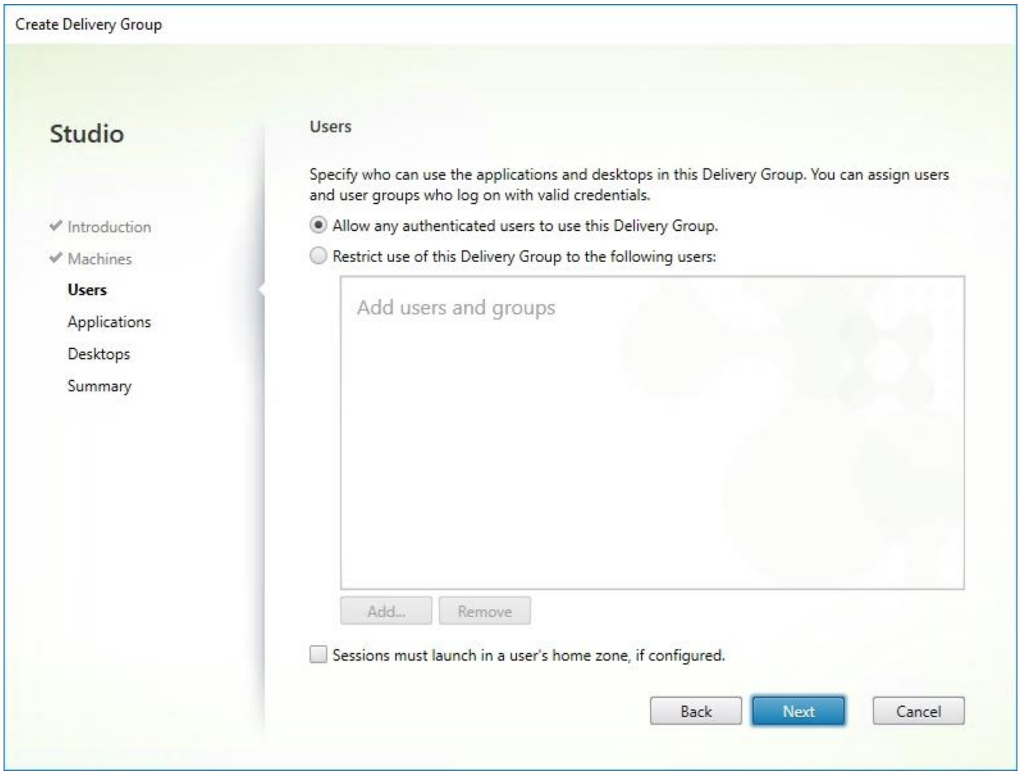
○ Applications

Note: For Linux OS machines, consult the administrator documentation for guidance.

Step 9. To make the Delivery Group accessible, you must add users. Select Allow any authenticated users to use this Delivery Group.

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

Step 10. Click Next.



Create Delivery Group

Studio

Users

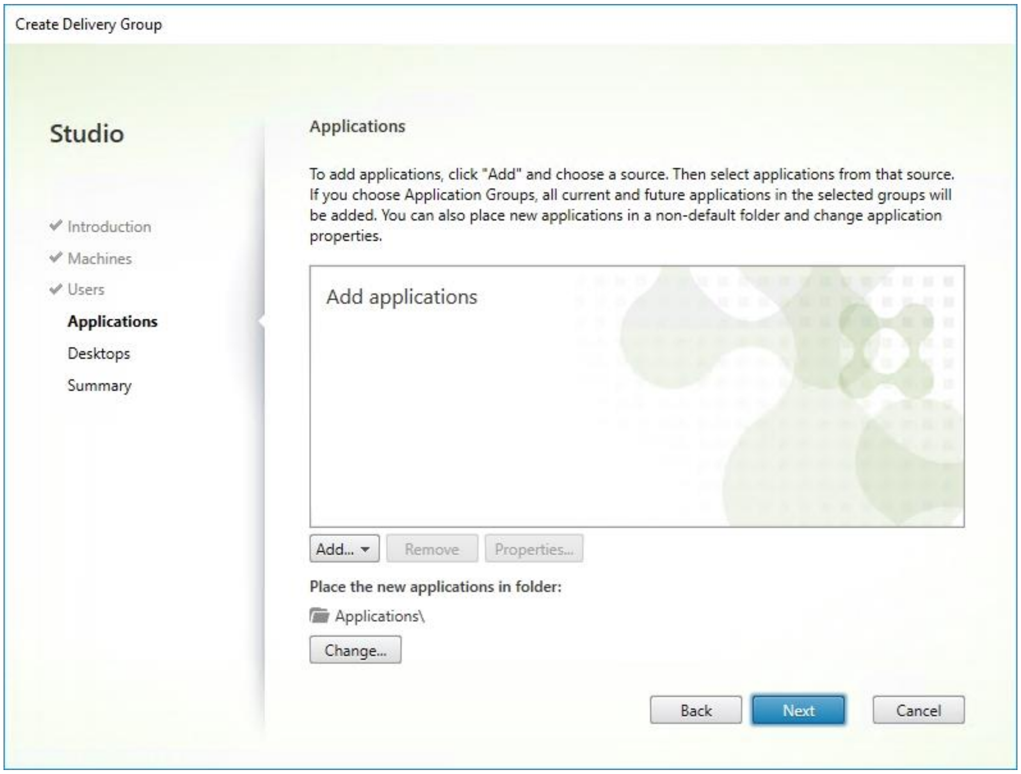
Specify who can use the applications and desktops in this Delivery Group. You can assign users and user groups who log on with valid credentials.

● Allow any authenticated users to use this Delivery Group.

○ Restrict use of this Delivery Group to the following users:

□ Sessions must launch in a user's home zone, if configured.

Step 11. Click Next (no applications are used in this design).



Create Delivery Group

Studio

✓ Introduction
✓ Machines
✓ Users
Applications
Desktops
Summary

Applications

To add applications, click "Add" and choose a source. Then select applications from that source. If you choose Application Groups, all current and future applications in the selected groups will be added. You can also place new applications in a non-default folder and change application properties.

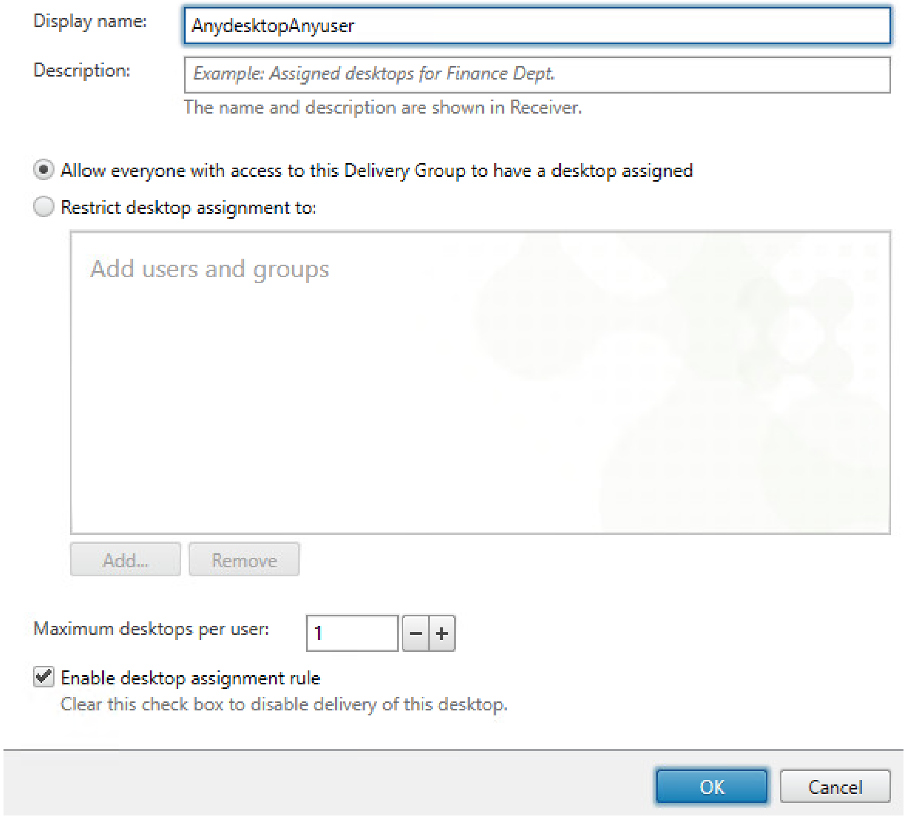
Add applications

Place the new applications in folder:

Applications\

Step 12. Enable Users to access the desktops.

Step 13. Click Next.



Display name: AnydesktopAnyuser

Description: *Example: Assigned desktops for Finance Dept.*

The name and description are shown in Receiver.

● Allow everyone with access to this Delivery Group to have a desktop assigned

○ Restrict desktop assignment to:

Add users and groups

Maximum desktops per user: 1

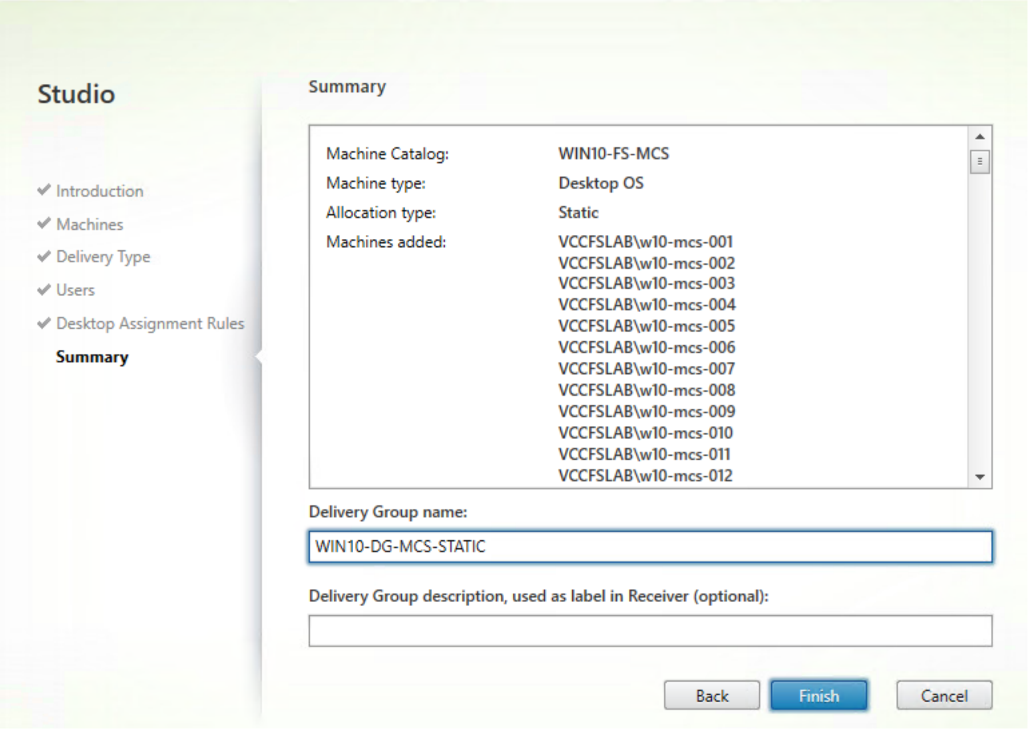
☑ Enable desktop assignment rule

Clear this check box to disable delivery of this desktop.

Step 14. On the Summary dialog, review the configuration. Enter a Delivery Group name and a Description (Optional).

Step 15. Click Finish.

Create Delivery Group



Summary

Machine Catalog: WIN10-FS-MCS
Machine type: Desktop OS
Allocation type: Static
Machines added: VCCFSLAB\w10-mcs-001
VCCFSLAB\w10-mcs-002
VCCFSLAB\w10-mcs-003
VCCFSLAB\w10-mcs-004
VCCFSLAB\w10-mcs-005
VCCFSLAB\w10-mcs-006
VCCFSLAB\w10-mcs-007
VCCFSLAB\w10-mcs-008
VCCFSLAB\w10-mcs-009
VCCFSLAB\w10-mcs-010
VCCFSLAB\w10-mcs-011
VCCFSLAB\w10-mcs-012

Delivery Group name: WIN10-DG-MCS-STATIC

Delivery Group description, used as label in Receiver (optional):

Citrix Studio lists the created Delivery Groups as well as the type, number of machines created, sessions, and applications for each group in the Delivery Groups tab.

Step 16. From the drop-down list, select “Turn on Maintenance Mode.”

Citrix Virtual Apps and Desktops Policies and Profile Management

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

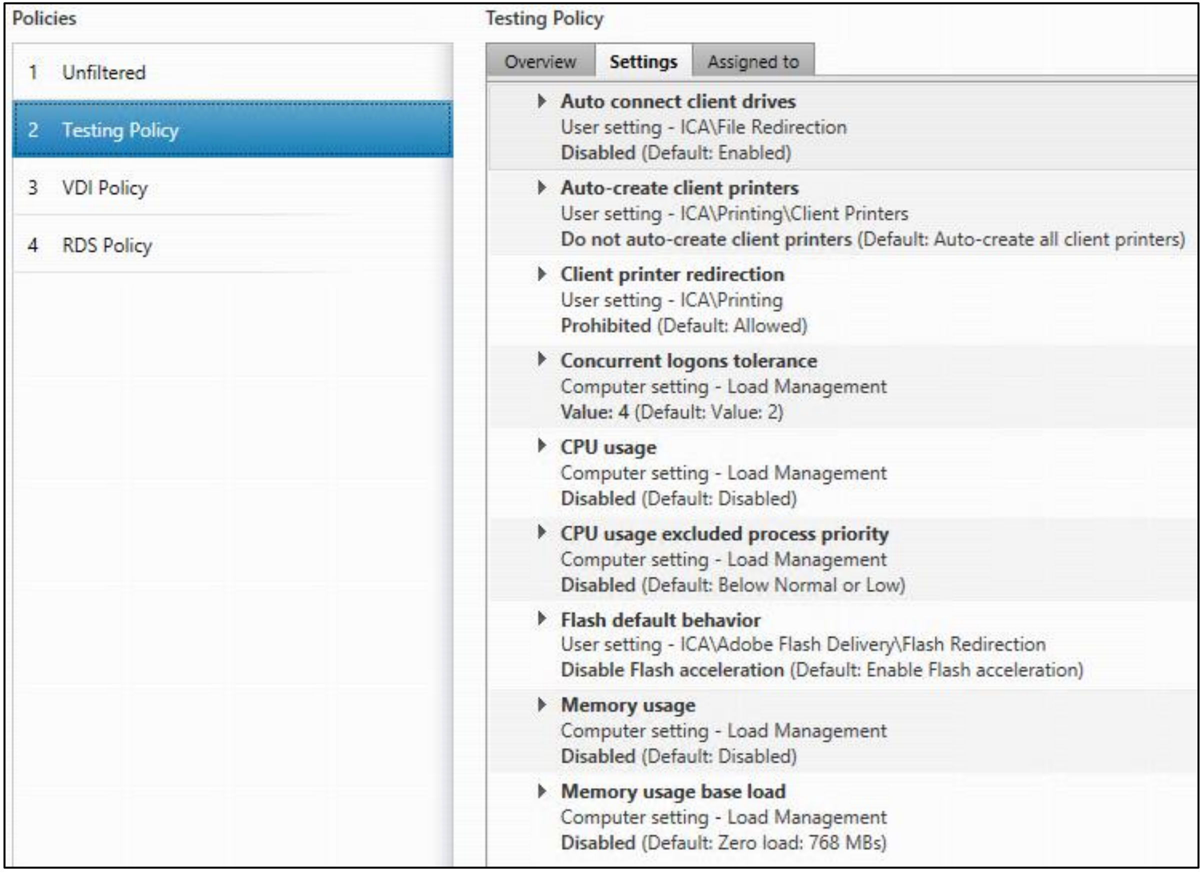
Configure Citrix Virtual Apps and Desktops Policies

Citrix Virtual Apps and Desktops policies control user access and session environments, and are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types with each policy. Policies can contain multiple settings and are typically defined through Citrix Studio.

Note: The Windows Group Policy Management Console can also be used if the network environment includes Microsoft Active Directory and permissions are set for managing Group Policy Objects).

Figure 37 shows the policies for Login VSI testing in this CVD.

Figure 37. Citrix Virtual Apps and Desktops Policy



Auto connect client drives
User setting - ICA\File Redirection
Disabled (Default: Enabled)

Auto-create client printers
User setting - ICA\Printing\Client Printers
Do not auto-create client printers (Default: Auto-create all client printers)

Client printer redirection
User setting - ICA\Printing
Prohibited (Default: Allowed)

Concurrent logons tolerance
Computer setting - Load Management
Value: 4 (Default: Value: 2)

CPU usage
Computer setting - Load Management
Disabled (Default: Disabled)

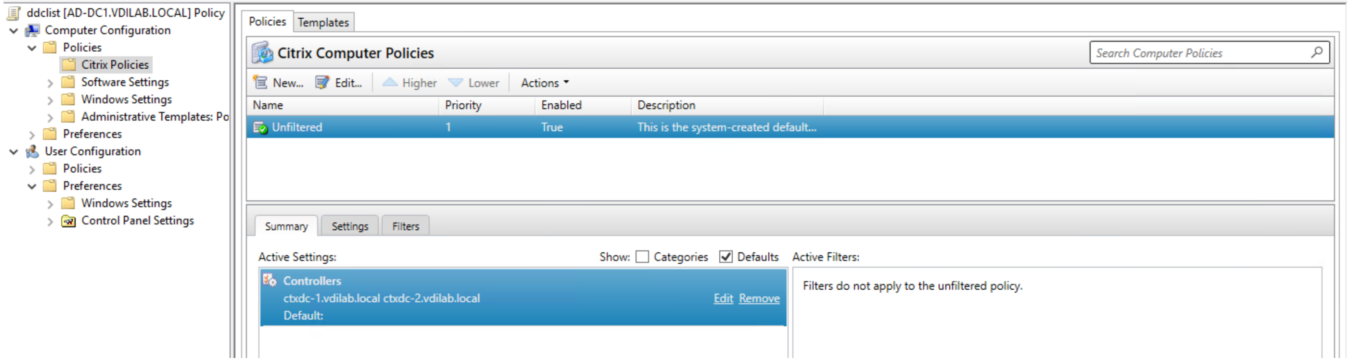
CPU usage excluded process priority
Computer setting - Load Management
Disabled (Default: Below Normal or Low)

Flash default behavior
User setting - ICA\Adobe Flash Delivery\Flash Redirection
Disable Flash acceleration (Default: Enable Flash acceleration)

Memory usage
Computer setting - Load Management
Disabled (Default: Disabled)

Memory usage base load
Computer setting - Load Management
Disabled (Default: Zero load: 768 MBs)

Figure 38. Delivery Controllers Policy



Name	Priority	Enabled	Description
Unfiltered	1	True	This is the system-created default...

Active Settings: Show: □ Categories ☑ Defaults

Controllers
ctxdc-1.vdilab.local ctxdc-2.vdilab.local
Default:

Active Filters:
Filters do not apply to the unfiltered policy.

FSLogix for Citrix Virtual Apps and Desktops Profile Management

This subject contains the following procedures:

- Configure FSLogix for Citrix Virtual Apps and Desktops Profiles Profile Container
- Configure FSLogix Profile Management

FSLogix for user profiles allows the Citrix Virtual Apps and Desktops environment to be easily and efficiently customized.

Procedure 1. Configure FSLogix for Citrix Virtual Apps and Desktops Profiles Profile Container

Profile Container is a full remote profile solution for non-persistent environments. Profile Container redirects the entire user profile to a remote location. Profile Container configuration defines how and where the profile is redirected.

Note: Profile Container is inclusive of the benefits found in Office Container.

When using Profile Container, both applications and users see the profile as if it's located on the local drive.

Step 1. Verify that you meet all entitlement and configuration requirements.

Step 2. Download and install FSLogix Software

Step 3. Consider the storage and network requirements for your users' profiles (in this CVD, we used the Netapp A400 to store the FSLogix Profile disks).

Step 4. Verify that your users have appropriate storage permissions where profiles will be placed.

Step 5. Profile Container is installed and configured after stopping use of other solutions used to manage remote profiles.

Step 6. Exclude the VHD(X) files for Profile Containers from Anti-Virus (AV) scanning.

Procedure 2. Configure FSLogix Profile Management

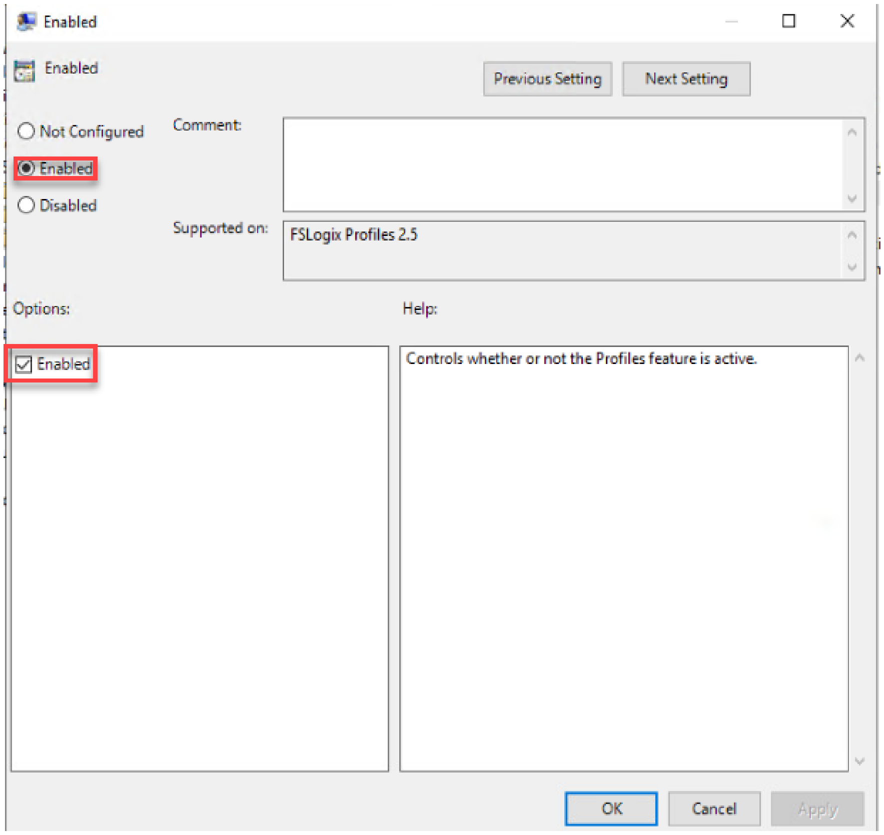
Step 1. When the FSLogix software is downloaded, copy the ‘fslogix.admx and fslogix.adml’ to the ‘PolicyDefinitions’ folder in your domain to manage the settings with Group Policy.

Step 2. On your VDI master image, install the FSLogix agent ‘FSLogixAppsSetup’ and accept all the defaults.

Step 3. Create a Group Policy object and link it to the Organizational Unit the VDI computer accounts.

Step 4. Right-click the **FSLogix GPO** policy.

Step 5. Enable FSLogix Profile Management.



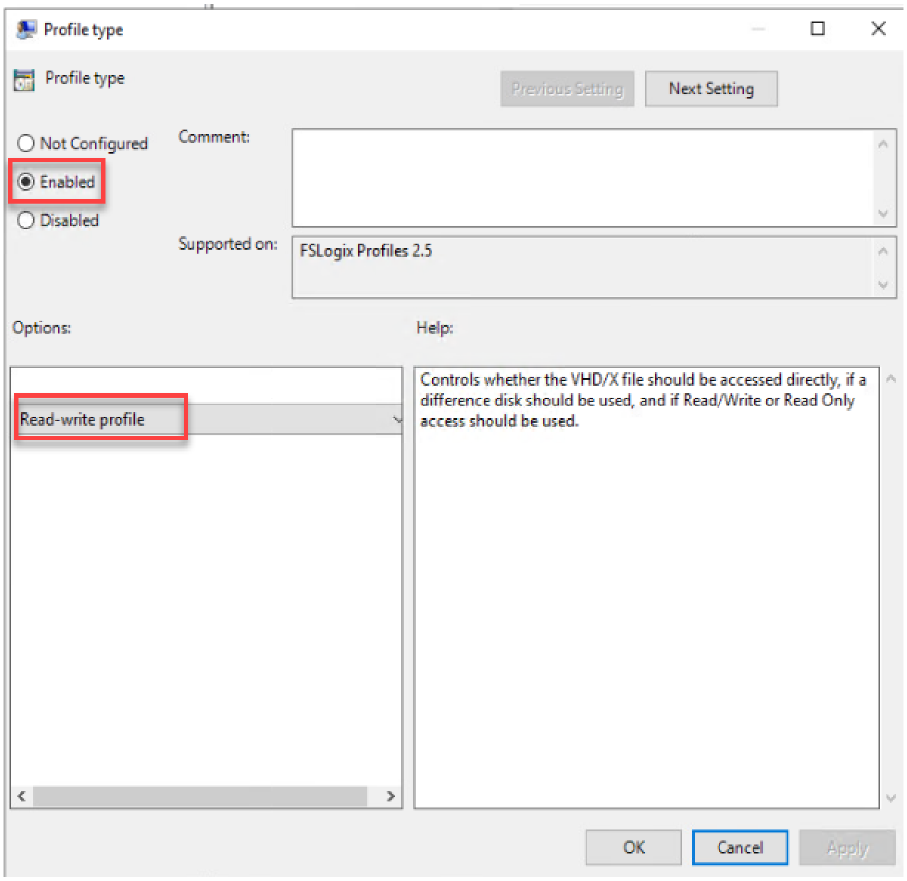
○ Not Configured
● Enabled
○ Disabled

Supported on: FSLogix Profiles 2.5

☑ Enabled

Controls whether or not the Profiles feature is active.

Step 6. Select Profile Type (in this solution, we used Read-Write profiles).



Profile type

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: FSLogix Profiles 2.5

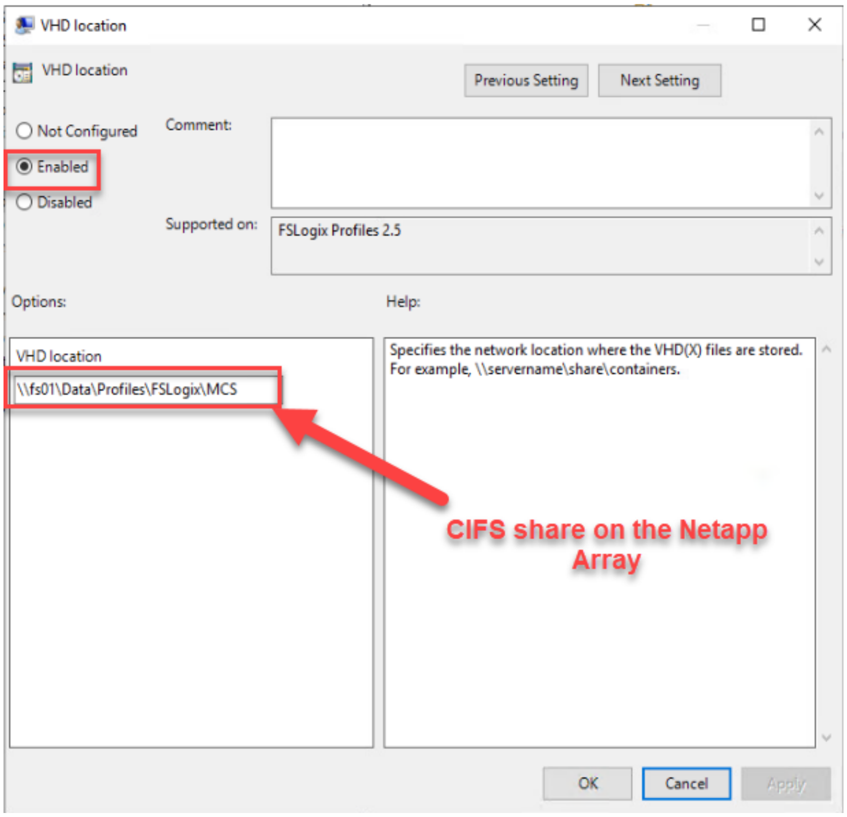
Options:

Read-write profile

Help:

Controls whether the VHD/X file should be accessed directly, if a difference disk should be used, and if Read/Write or Read Only access should be used.

Step 7. Enter the location of the Profile location (our solution used a CIFS share on the NetApp Array).



VHD location

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: FSLogix Profiles 2.5

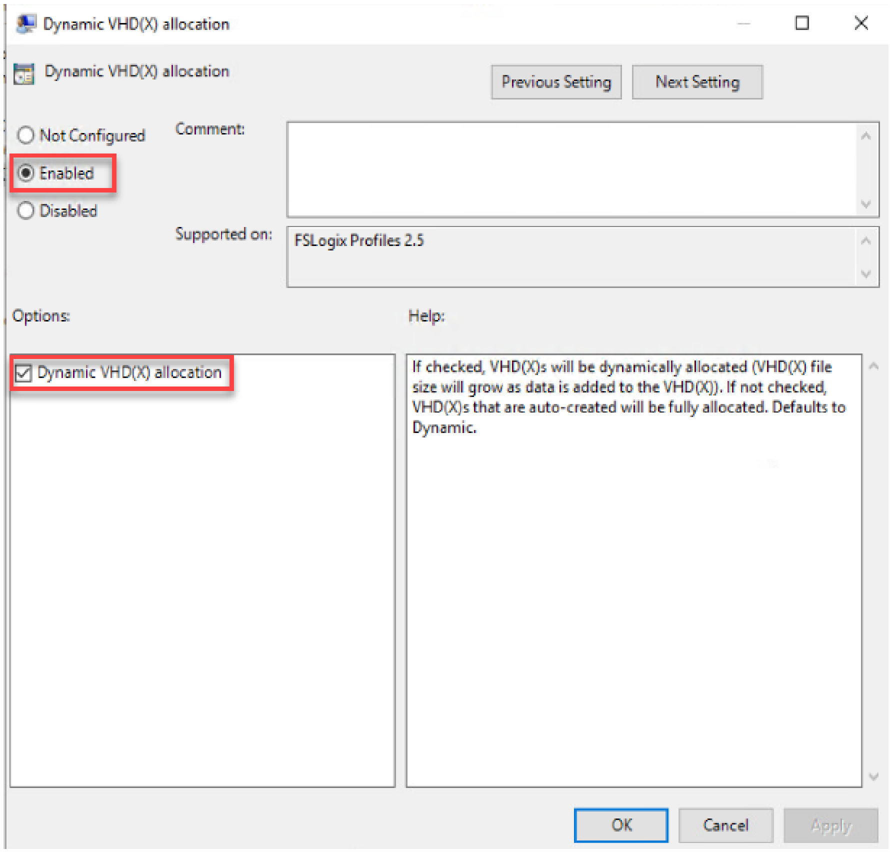
Options:

VHD location
\\fs01\Data\Profiles\FSLogix\MCS

Help:

Specifies the network location where the VHD(X) files are stored. For example, \\servername\share\containers.

Note: We recommend using the Dynamic VHDX setting.



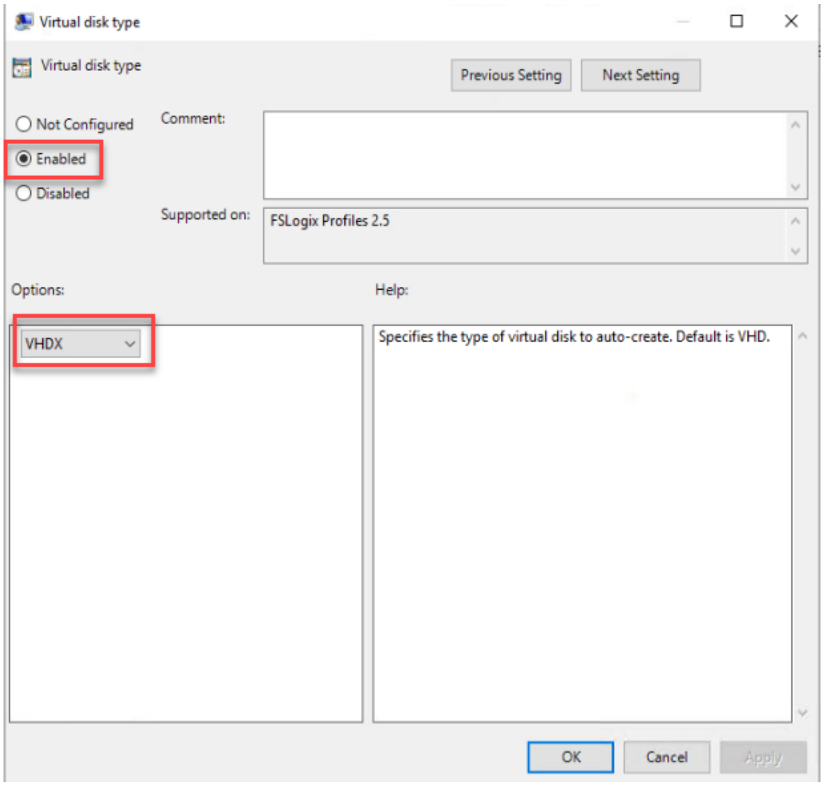
○ Not Configured
● Enabled
○ Disabled

Supported on: FSLogix Profiles 2.5

☑ Dynamic VHD(X) allocation

If checked, VHD(X)s will be dynamically allocated (VHD(X) file size will grow as data is added to the VHD(X)). If not checked, VHD(X)s that are auto-created will be fully allocated. Defaults to Dynamic.

Note: VHDX is recommended over VHD.



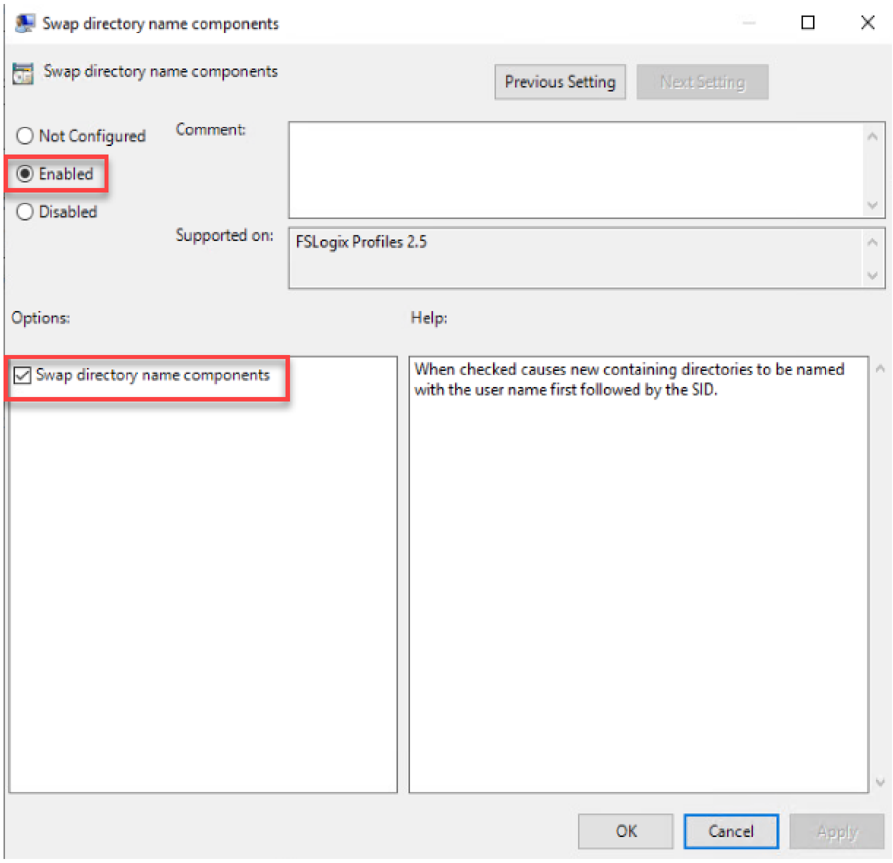
○ Not Configured
● Enabled
○ Disabled

Supported on: FSLogix Profiles 2.5

VHDX

Specifies the type of virtual disk to auto-create. Default is VHD.

Note: We enabled the ‘Swap directory name components’ setting for an easier administration but is not necessary for improved performance.



Swap directory name components

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: FSLogix Profiles 2.5

Options:

☑ Swap directory name components

Help:

When checked causes new containing directories to be named with the user name first followed by the SID.

Tech tip
FSLogix is an outstanding method of controlling the user experience and profile data in a VDI environment. There are many helpful settings and configurations for VDI with FSLogix that were not used in this solution.

Hybrid Cloud for Disaster Recovery Deployment

Disasters can come in many forms for a business and protecting data with disaster recovery (DR) is a critical goal for businesses continuity. DR allows organizations to failover their business operations to a secondary location and later recover and failback to the primary site efficiently and reliably.

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

Procedure 1. Access NetApp BlueXP

Step 1. To access NetApp BlueXP and other cloud services, you need to sign up on NetApp Cloud Central.

Procedure 2. Deploy Connector

Step 1. To deploy Connector in Microsoft Azure Cloud, go to: https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-creating-connectors-azure.html#overview.

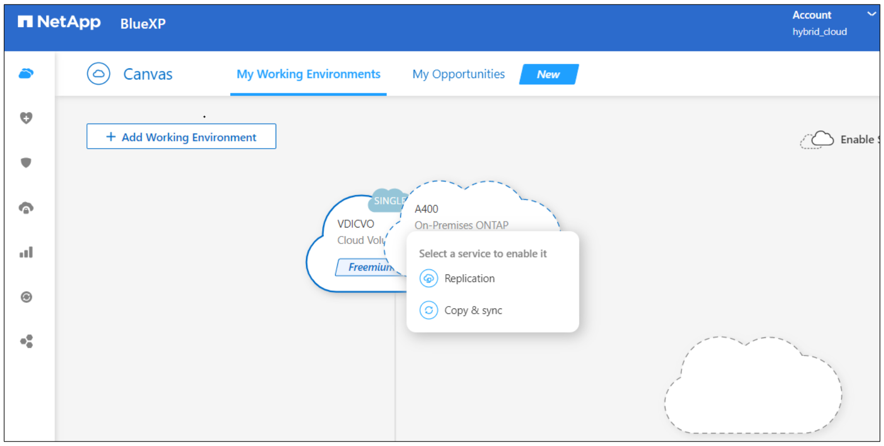
Procedure 3. Deploy CVO in Azure

Step 1. To deploy CVO in Microsoft Azure Cloud, go to: https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-azure.html.

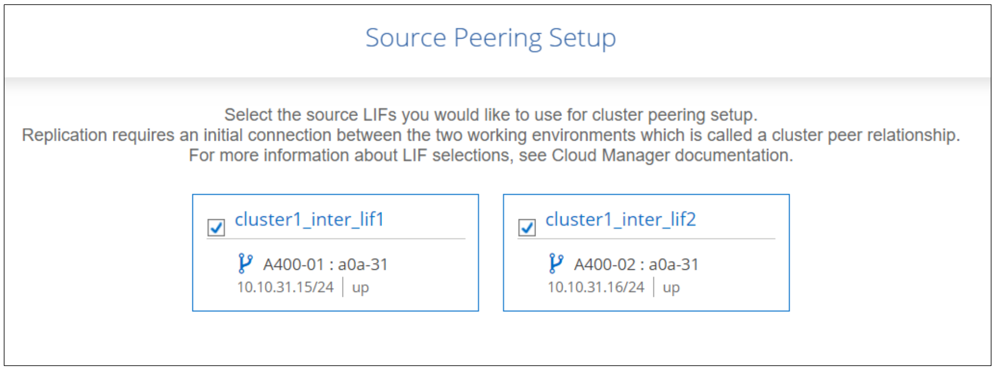
Procedure 4. Set up SnapMirror relationship

Step 1. In the BlueXP window, select your workspace and connector.

Step 2. Drag and drop the source “on-prem ontap” to the “Azure Cloud Volumes ONTAP” instance which will be your destination.



Step 3. In the “Source Peering Setup” select the intercluster LIF.



Source Peering Setup

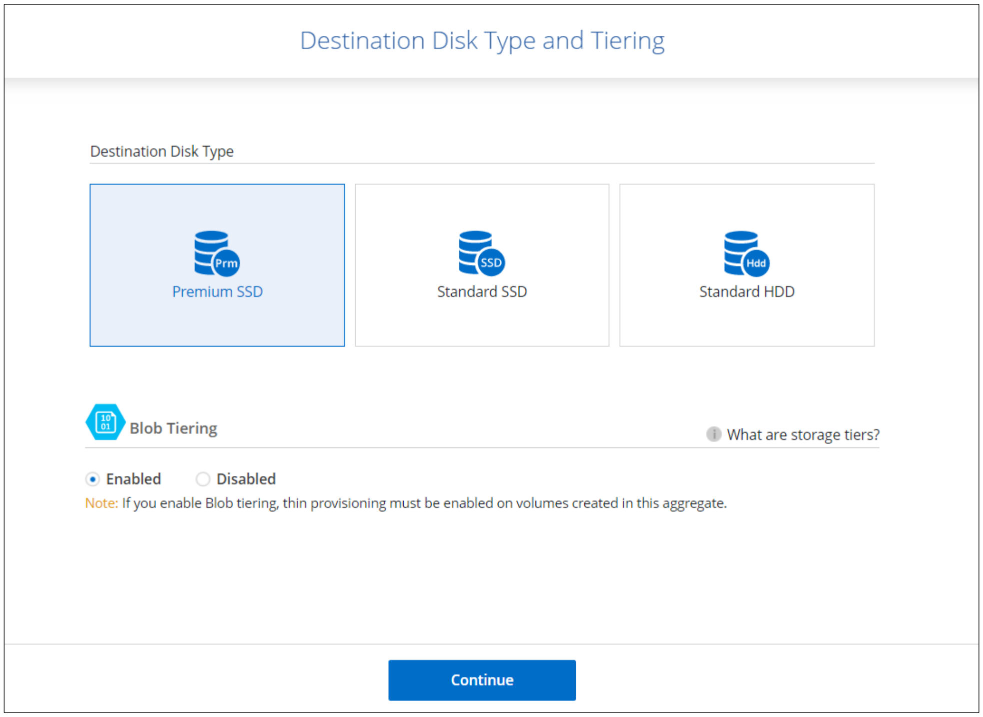
Select the source LIFs you would like to use for cluster peering setup.
Replication requires an initial connection between the two working environments which is called a cluster peer relationship.
For more information about LIF selections, see Cloud Manager documentation.

☑ cluster1_inter_lif1
A400-01 : a0a-31
10.10.31.15/24 | up

☑ cluster1_inter_lif2
A400-02 : a0a-31
10.10.31.16/24 | up

Step 4. In the "Source Volume Selection" select the volume to replicate.

Step 5. On the "Destination Disk Type and Tiering" select the default Destination disk type.



Destination Disk Type and Tiering

Destination Disk Type

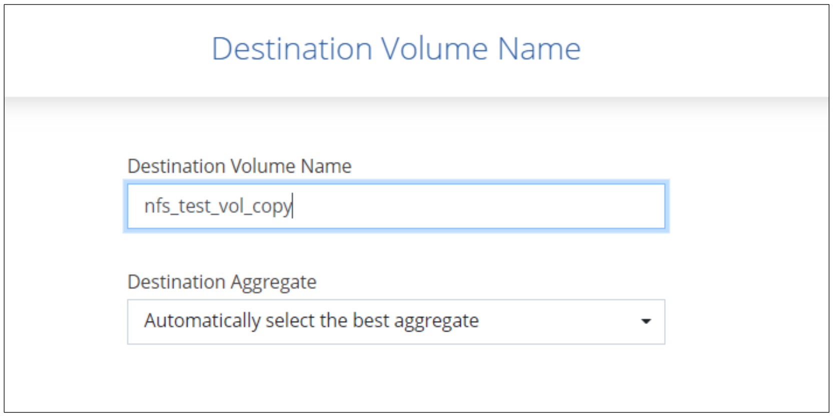
Blob Tiering

What are storage tiers?

● Enabled ○ Disabled

Note: If you enable Blob tiering, thin provisioning must be enabled on volumes created in this aggregate.

Step 6. On the "Destination Volume Name" accept all the defaults.



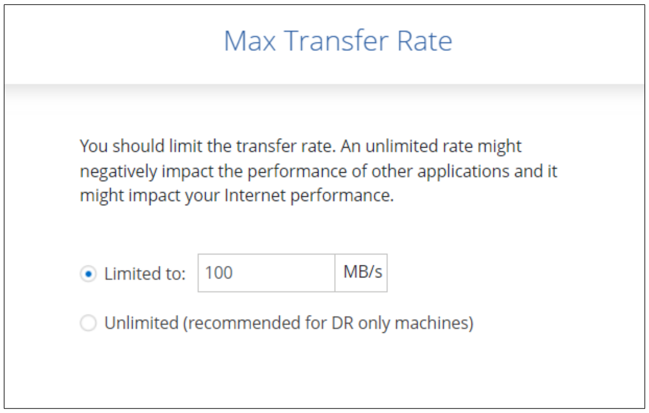
Destination Volume Name

Destination Volume Name: nfs_test_vol_copy

Destination Aggregate: Automatically select the best aggregate

Step 7. Click Continue.

Step 8. Accept the default for the "Max Transfer Rate."



Max Transfer Rate

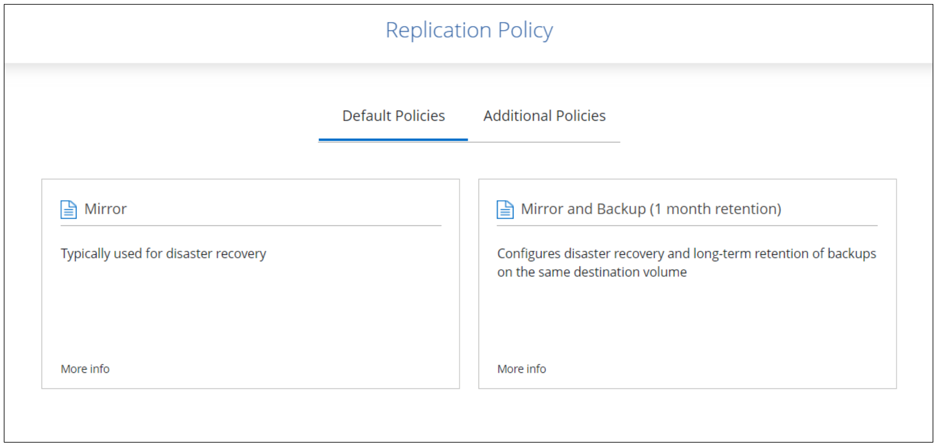
You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

● Limited to: 100 MB/s

○ Unlimited (recommended for DR only machines)

Step 9. Click Continue.

Step 10. Click Mirror to select a "Replication Policy."



Replication Policy

Default Policies | Additional Policies

Mirror

Typically used for disaster recovery

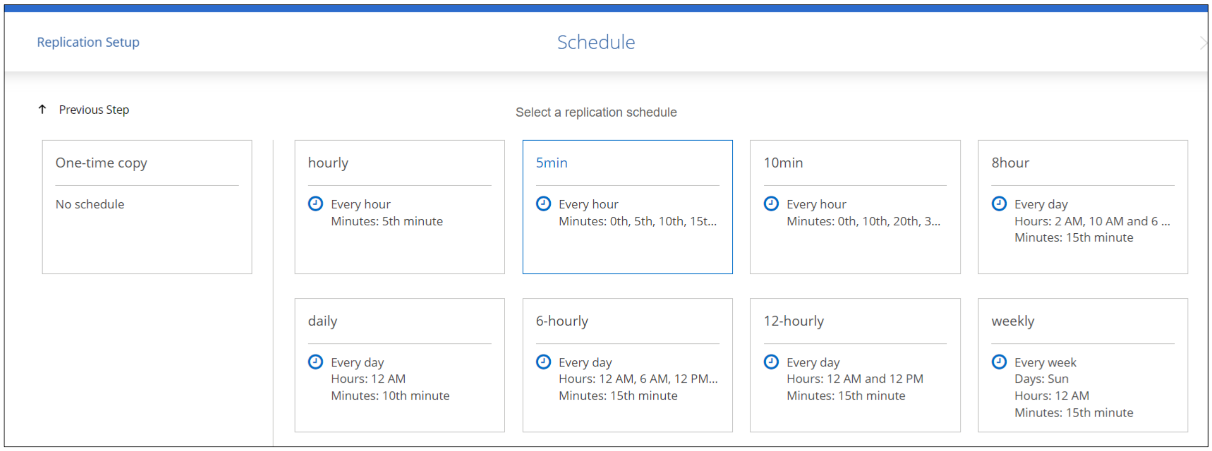
More info

Mirror and Backup (1 month retention)

Configures disaster recovery and long-term retention of backups on the same destination volume

More info

Note: To control the frequency of the replication updates, you can select a replication schedule. If you scroll down the window, you will see there are many from which to choose.



Replication Setup

Schedule

↑ Previous Step

Select a replication schedule

One-time copy
No schedule

hourly
Every hour
Minutes: 5th minute

5min
Every hour
Minutes: 0th, 5th, 10th, 15t...

10min
Every hour
Minutes: 0th, 10th, 20th, 3...

8hour
Every day
Hours: 2 AM, 10 AM and 6 ...
Minutes: 15th minute

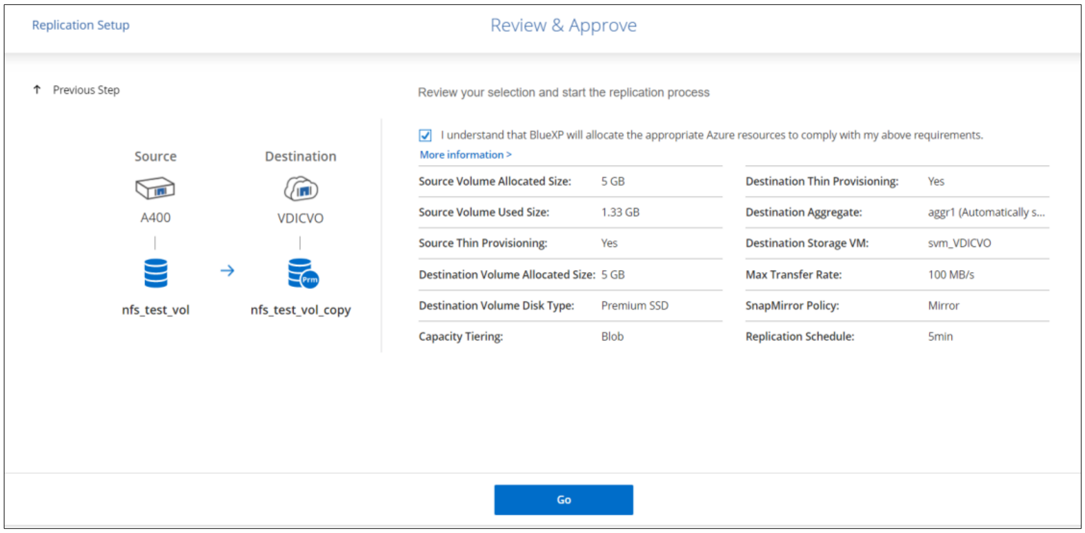
daily
Every day
Hours: 12 AM
Minutes: 10th minute

6-hourly
Every day
Hours: 12 AM, 6 AM, 12 PM...
Minutes: 15th minute

12-hourly
Every day
Hours: 12 AM and 12 PM
Minutes: 15th minute

weekly
Every week
Days: Sun
Hours: 12 AM
Minutes: 15th minute

Step 11. Review and accept the choices by clicking the checkbox next to I understand ....



Review your selection and start the replication process

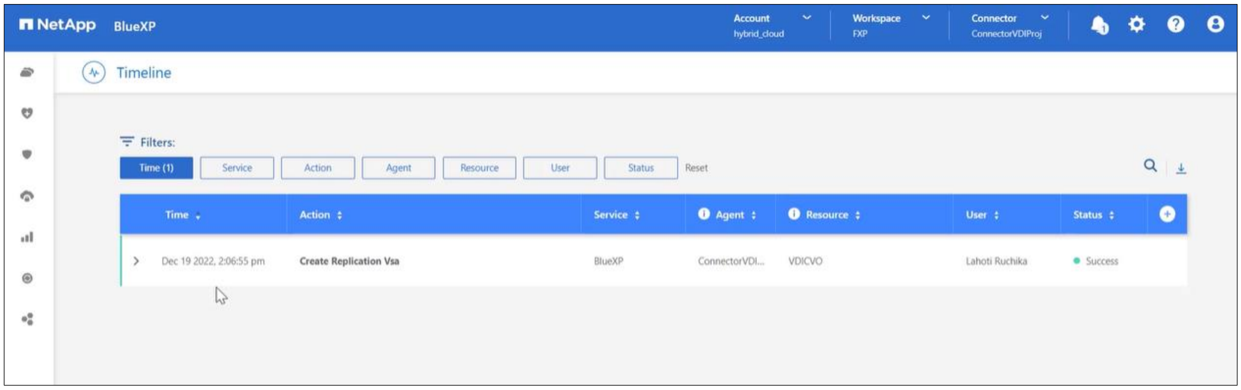
☑ I understand that BlueXP will allocate the appropriate Azure resources to comply with my above requirements.

More information >

Source Volume Allocated Size:	5 GB	Destination Thin Provisioning:	Yes
Source Volume Used Size:	1.33 GB	Destination Aggregate:	aggr1 (Automatically s...
Source Thin Provisioning:	Yes	Destination Storage VM:	svm_VDICVO
Destination Volume Allocated Size:	5 GB	Max Transfer Rate:	100 MB/s
Destination Volume Disk Type:	Premium SSD	SnapMirror Policy:	Mirror
Capacity Tiering:	Blob	Replication Schedule:	5min

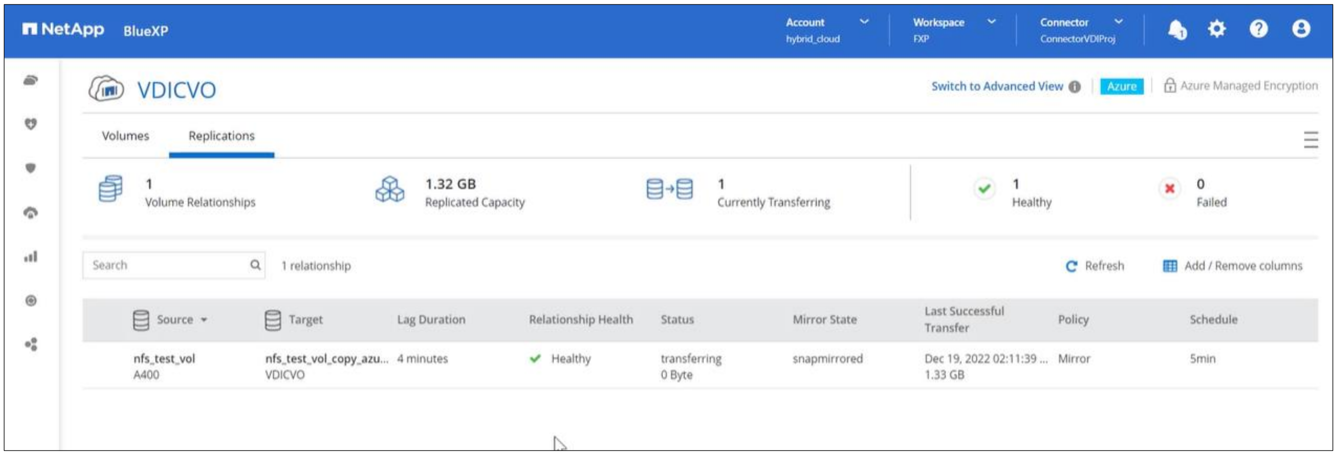
Step 12. Click Go.

Step 13. Click Timeline to monitor when the creation of the protection relationship is complete.



	Time	Action	Service	Agent	Resource	User	Status
>	Dec 19 2022, 2:06:55 pm	Create Replication Vsa	BlueXP	ConnectorVDI...	VDICVO	Lahoti Ruchika	Success

Step 14. Click on the CVO instance and go to replication tab. Wait for the “Mirror State” to change to “snapmirrored.”



Source	Target	Lag Duration	Relationship Health	Status	Mirror State	Last Successful Transfer	Policy	Schedule
nfs_test_vol A400	nfs_test_vol_copy_azu... VDICVO	4 minutes	✓ Healthy	transferring 0 Byte	snapmirrored	Dec 19, 2022 02:11:39 ... 1.33 GB	Mirror	5min

Test Setup and Configuration

This chapter contains the following:

- Cisco UCS Test Configuration for Single Blade Scalability
- Testing Methodology and Success Criteria
- Single-Server Recommended Maximum Workload

Note: In this solution, we tested a single Cisco UCS B200 M6 blade server to validate against the performance of one blade and eleven Cisco UCS B200 M6 blade servers across two chassis to illustrate linear scalability for each workload use case studied.

Cisco UCS Test Configuration for Single Blade Scalability

This test case validates Recommended Maximum Workload per host server using Citrix Virtual Apps and Desktops 7 LTSR with 370 RDS sessions, 250 VDI Non-Persistent sessions, and 250 VDI Persistent sessions.

Figure 39. Test configuration for Single Server Scalability Citrix Virtual Apps and Desktops 7 LTSR VDI (Persistent) Using MCS

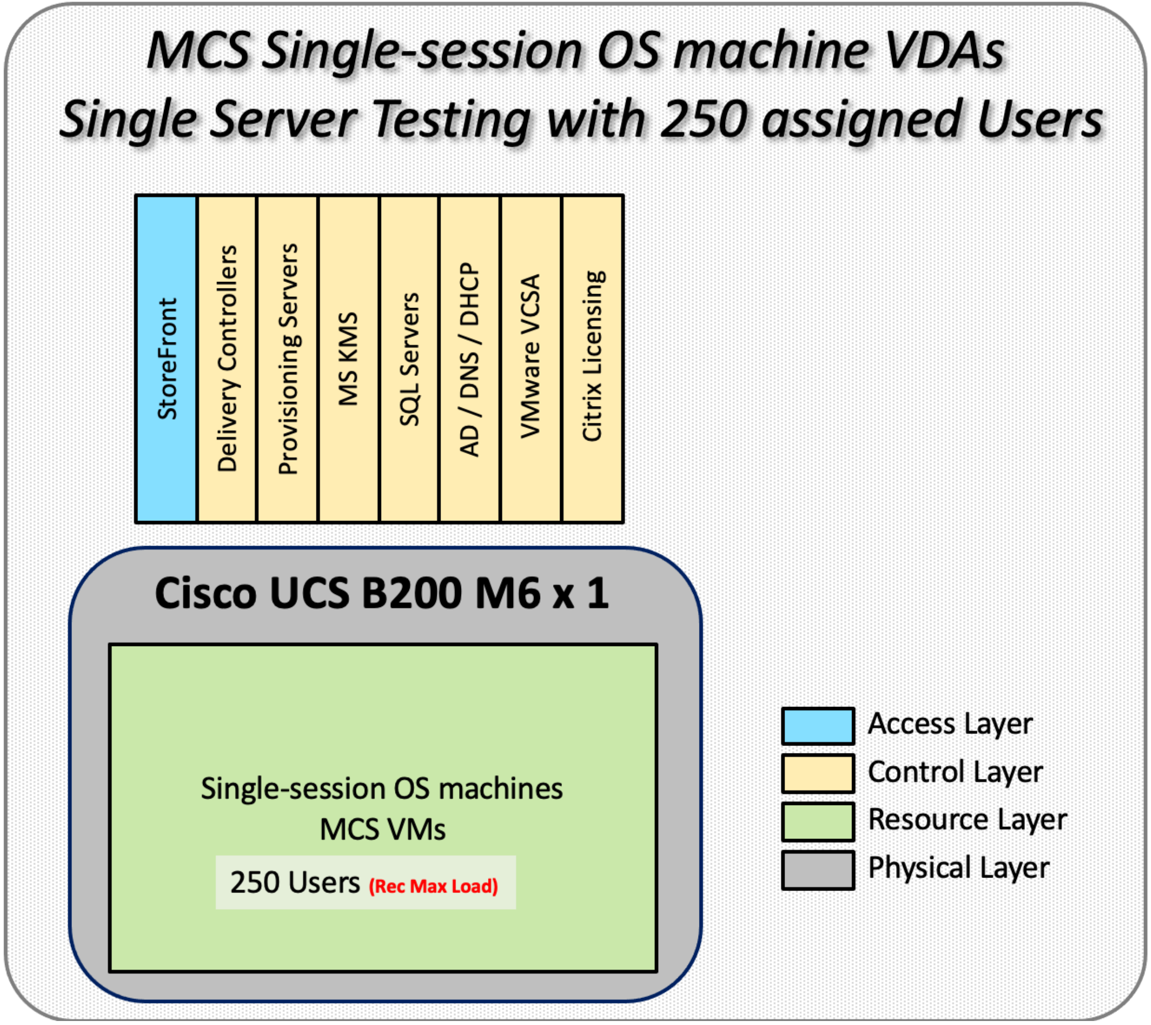


Figure 40. Test configuration for Single Server Scalability Citrix Virtual Apps and Desktops 7 LTSR VDI (Non-Persistent) using PVS

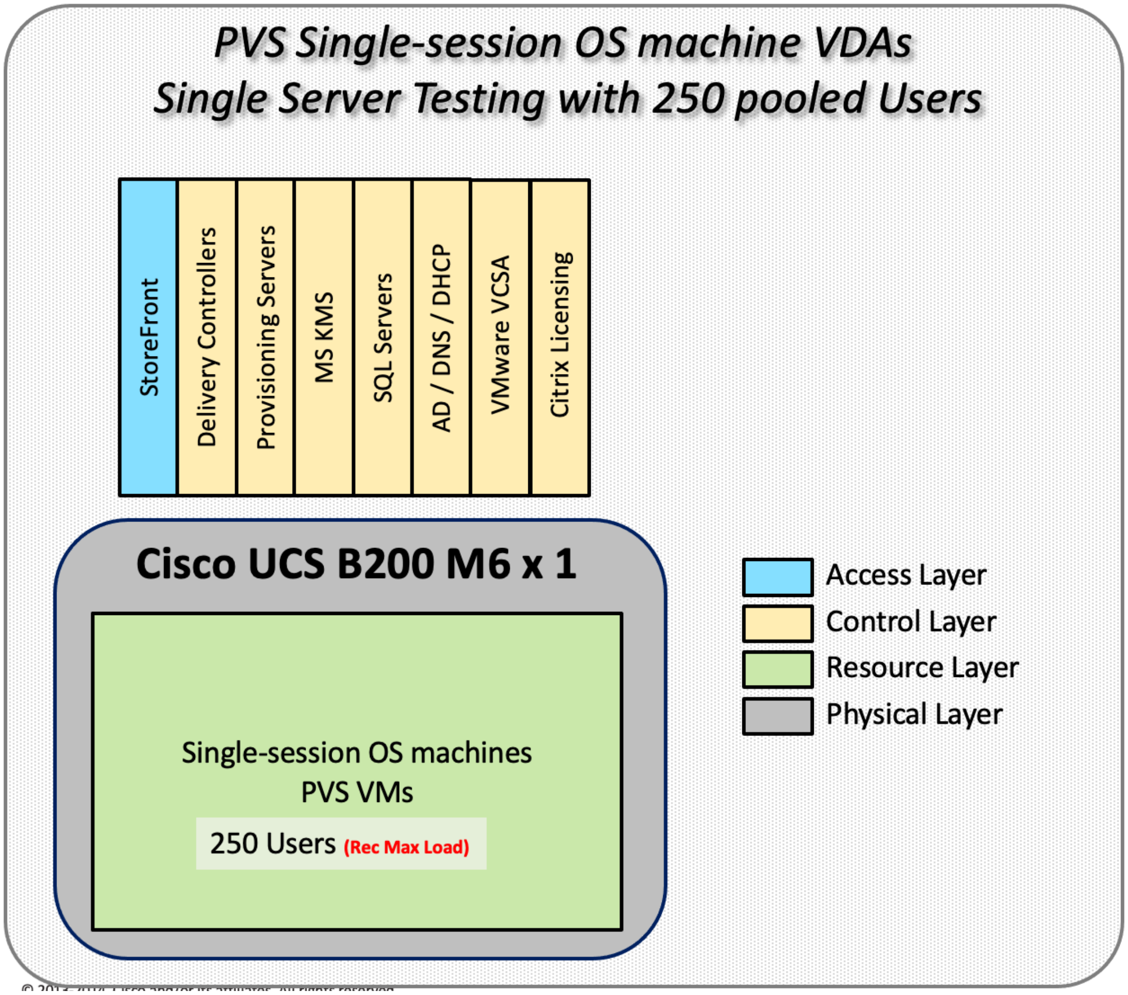
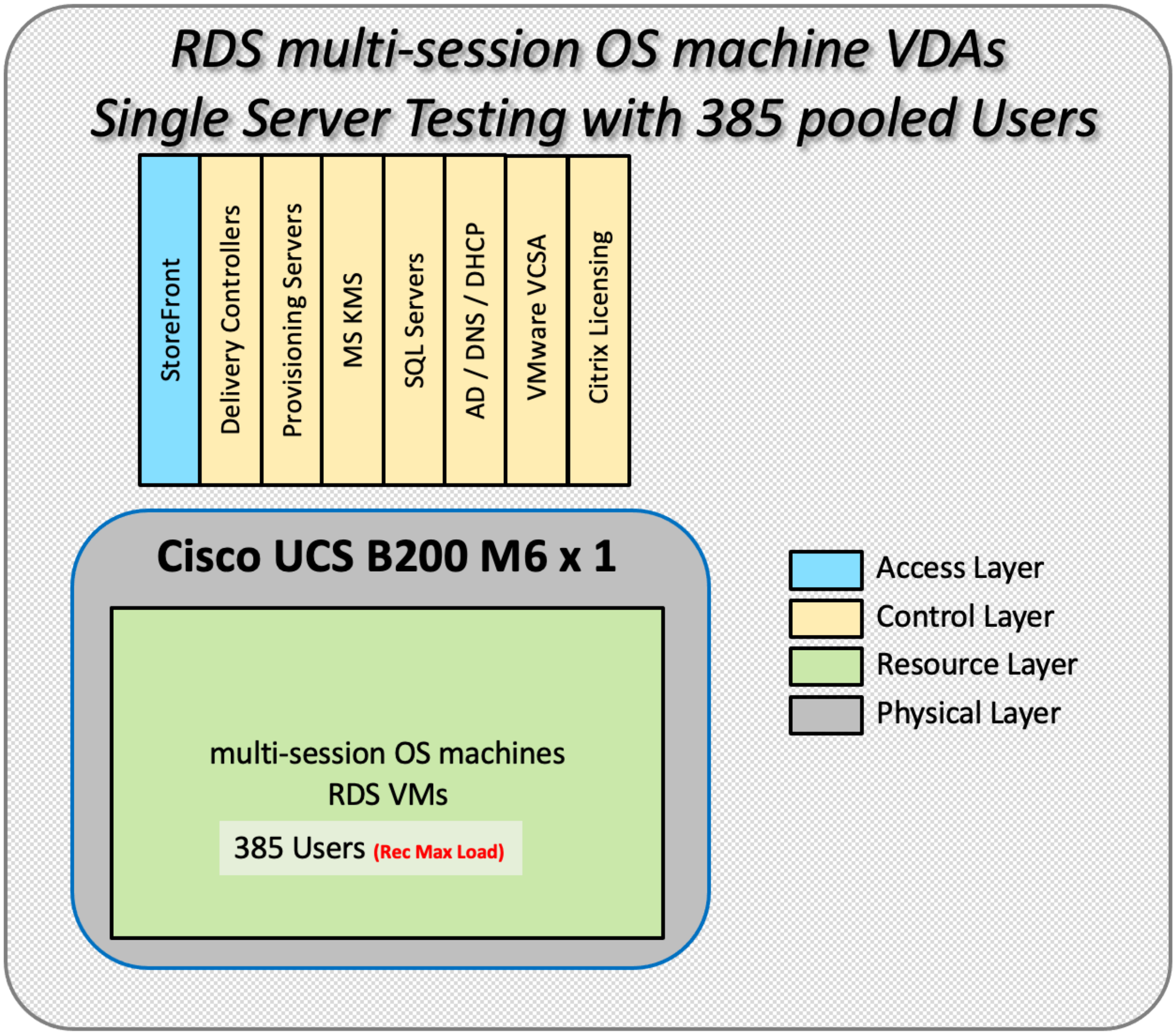


Figure 41. Test configuration for Single Server Scalability Citrix Virtual Apps and Desktops 7 LTSR RDS



Hardware components:

- Cisco UCSX 9508 Blade Server Chassis
- 2 Cisco UCS 6454 4th Gen Fabric Interconnects
- 4 (Infrastructure Hosts) HX220 M5 rack servers with Intel Xeon Gold 6230 2.20-GHz processors, 768GB 2933MHz RAM for all host blades
- 1 (RDS/VDI Host) Cisco UCS B200-M6 Compute Nodes with Intel Xeon Gold 6338 2.0-GHz 32-core processors, 1TB 3200MHz RAM for all host blades
- Cisco VIC 1440 CNA (1 per blade)
- 2 Cisco Nexus 93180YC-FX Access Switches
- 2 Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switches
- NetApp A400

Software components:

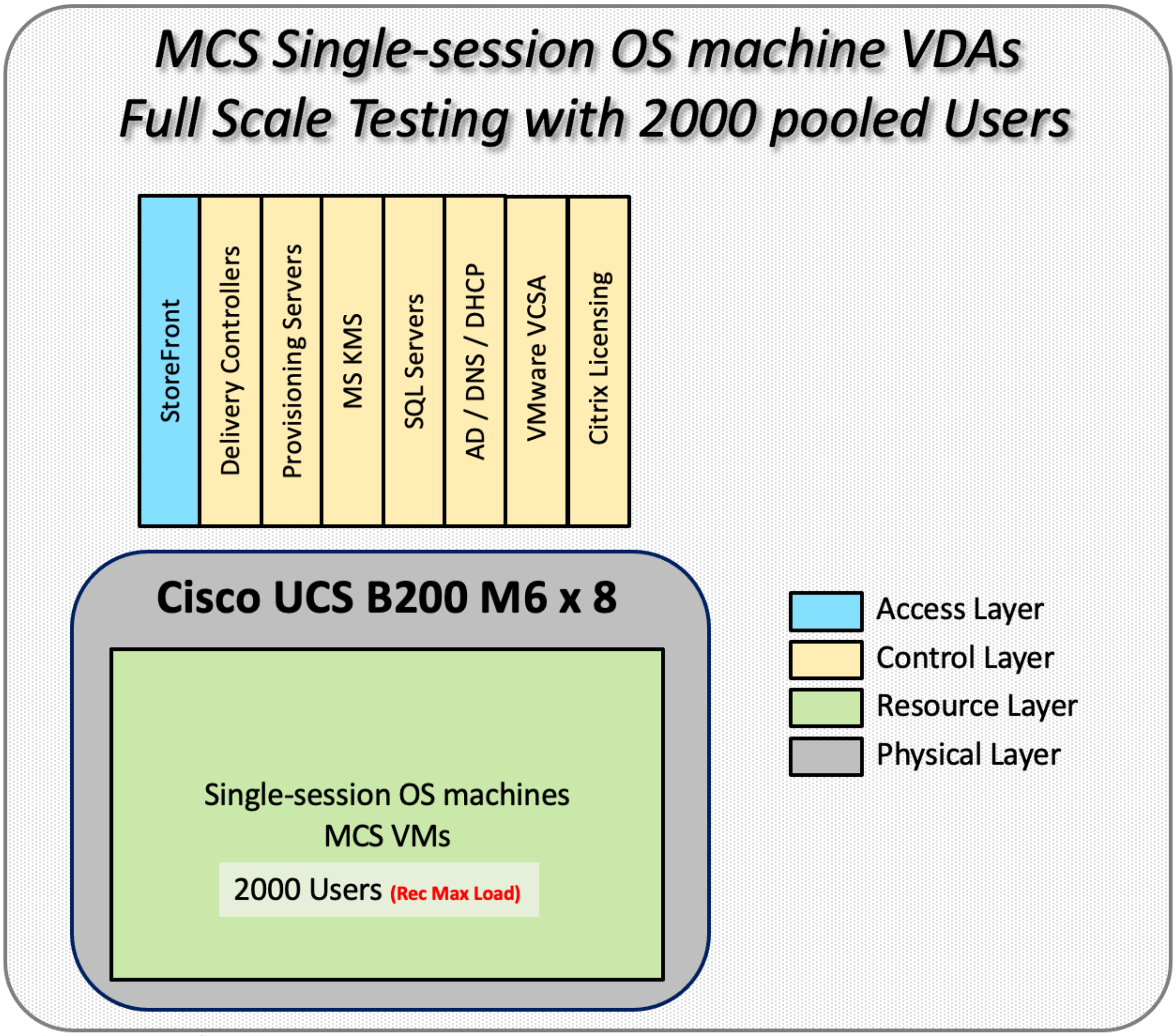
- Cisco UCS firmware 4.2(2a)
- Netapp ONTAP 9.10

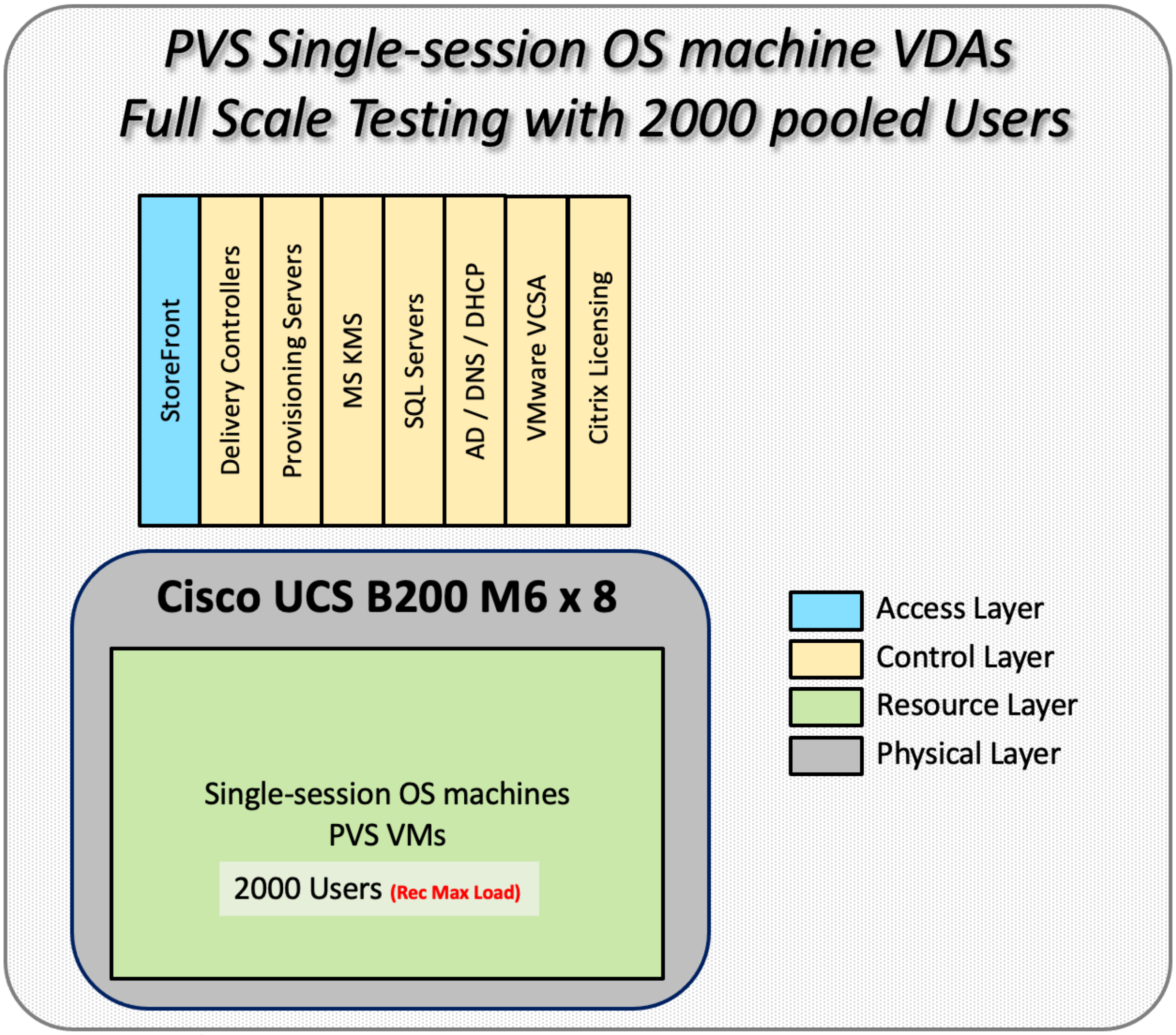
- VMware ESXi 7.0 3 for host blades
- Citrix Virtual Apps and Desktops 7 LTSR VDI Desktops and RDS Desktops
- FSLogix
- Microsoft SQL Server 2019
- Microsoft Windows 10 64 bit, 2vCPU, 4 GB RAM, 40 GB HDD (master)
- Microsoft Windows Server 2019, 8vCPU, 32GB RAM, 60 GB vDisk (master)
- Microsoft Office 2016
- Login VSI 4.1.40 Knowledge Worker Workload (Benchmark Mode)
- NetApp Harvest, Graphite and Grafana

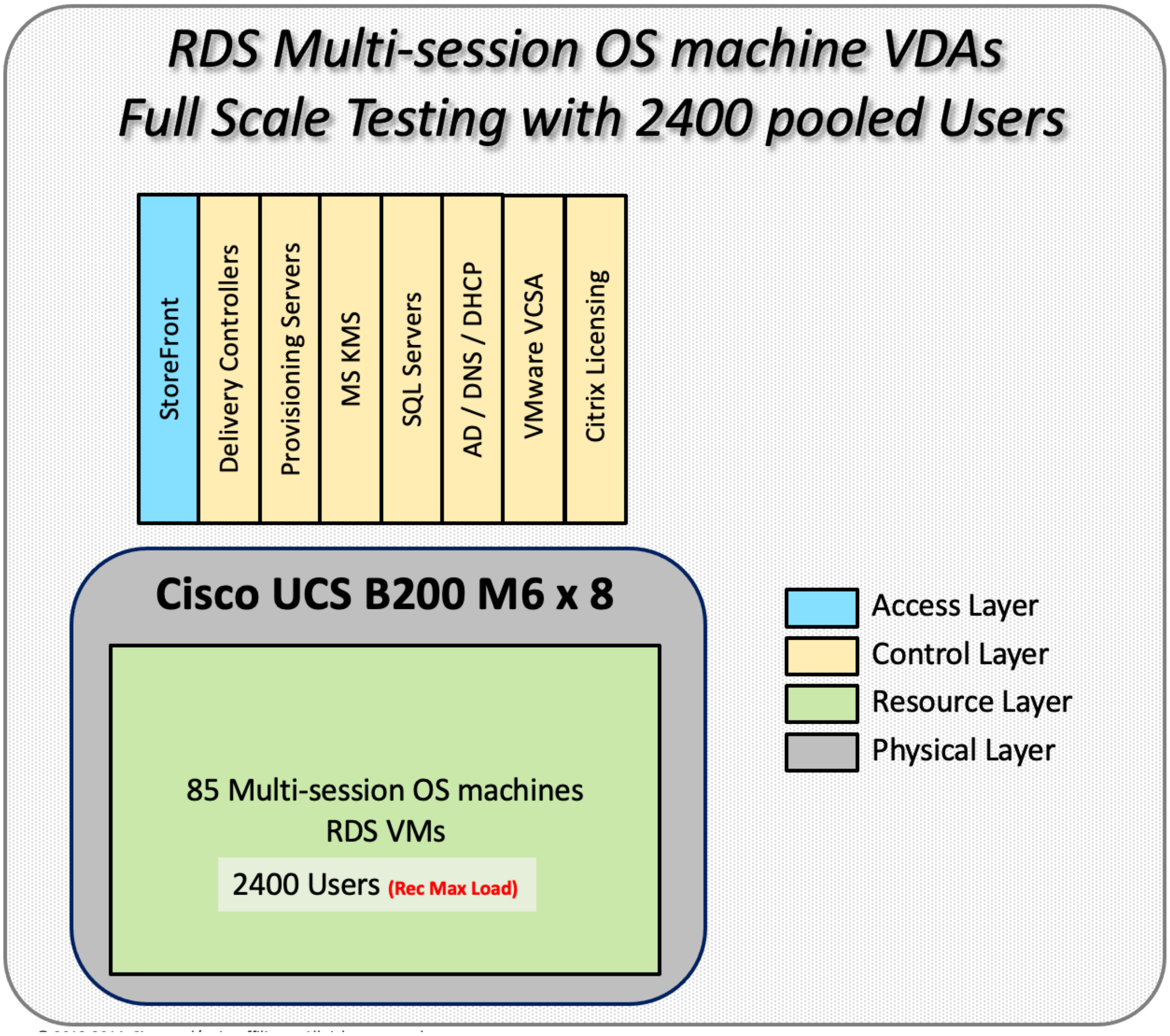
Cisco UCS Configuration for Full Scale Testing

This test case validates thirty blade workloads using RDS/Citrix Virtual Apps and Desktops 7 LTSR with 2500 RDS sessions, 2000 VDI Non-Persistent sessions, and 2000 VDI Persistent sessions. Server N+1 fault tolerance is factored into this solution for each workload and infrastructure cluster.

Figure 42. Full Scale Test Configuration with 11 Blades




PVS Single-session OS machine VDAs
Full Scale Testing with 2000 pooled Users
StoreFront
Delivery Controllers
Provisioning Servers
MS KMS
SQL Servers
AD / DNS / DHCP
VMware VCSA
Citrix Licensing
Cisco UCS B200 M6 x 8
Single-session OS machines
PVS VMs
2000 Users (Rec Max Load)
Access Layer
Control Layer
Resource Layer
Physical Layer



Hardware components:

- Cisco UCS 9508 Blade Server Chassis
- 2 Cisco UCS 6454 4th Gen Fabric Interconnects
- 4 (Infrastructure Hosts) HX220 M5 rack servers with Intel Xeon Gold 6230 2.20-GHz processors, 768GB 2933MHz RAM for all host blades
- 8 (RDS/VDI Host) Cisco UCS B200-M6 Compute Nodes with Intel Xeon Gold 6338 2.0-GHz 32-core processors, 1TB 3200MHz RAM for all host blades
- Cisco UCS VIC 1440 CNA (1 per blade)
- 2 Cisco Nexus 93180YC-FX Access Switches
- 2 Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switches
- 1 NetApp AFF A400 storage system (2x storage controllers- Active/Active High Availability pair) with 2x DS224C disk shelves, 24x 3.8TB SSD- 65TB usable / 130TB effective (2:1 efficiency)

Software components:

- Cisco UCS firmware 4.2(2a)
- VMware ESXi 7.03 Update 1 for host blades

- Citrix RDS/Citrix Virtual Apps and Desktops 7 LTSR VDI Hosted Virtual Desktops and RDS Hosted Shared Desktops
- Citrix Provisioning Server 7 LTSR
- FSLogix for Profile Management
- Microsoft SQL Server 2019
- Microsoft Windows 10 64 bit, 2vCPU, 4 GB RAM, 32 GB vDisk (master)
- Microsoft Windows Server 2019, 8vCPU, 32GB RAM, 40 GB vDisk (master)
- Microsoft Office 2016
- Login VSI 4.1.40 Knowledge Worker Workload (Benchmark Mode)

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 Citrix RDS and Citrix Virtual Apps and Desktops Hosted Virtual Desktop and RDS Hosted Shared models under test.

Test metrics were gathered from the hypervisor, 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

This section contains the following procedure:

- Test Run Protocol

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

Pre-Test Setup for Single and Multi-Blade Testing

All virtual machines were shut down utilizing the Citrix Virtual Apps and Desktops Administrator and vCenter.

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.

All VMware ESXi VDI host blades to be tested were restarted prior to each test cycle.

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, it’s required to start all sessions, whether single server users or 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 be 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.

1. Time 0:00:00 Start Esxtop Logging on the following systems:
    a. Infrastructure and VDI Host Blades used in the test run
    b. vCenter used in the test run
    c. All Infrastructure VMs used in test run (AD, SQL, brokers, image mgmt., and so on)
2. Time 0:00:10 Start Storage Partner Performance Logging on Storage System
3. Time 0:05: Boot Virtual Desktops/RDS Virtual Machines using Citrix Virtual Apps and Desktops Studio

Note: The boot rate should be around 10-12 VMs per minute per server.

4. Time 0:06 First machines boot
5. Time 0:30 Single Server or Scale target number of desktop VMs booted on 1 or more blades

Note: No more than 30 minutes for boot up of all virtual desktops is allowed.

6. Time 0:35 Single Server or Scale target number of desktop VMs desktops registered on Citrix Virtual Apps and Desktops Studio
7. Virtual machine settling time.

Note: No more than 60 Minutes of rest time is allowed after the last desktop is registered on the Citrix Virtual Apps and Desktops Studio . Typically, a 30-40 minute rest period is sufficient.

8. Time 1:35 Start Login VSI 4.1.40 Office Worker Benchmark Mode Test, setting auto-logoff time at 900 seconds, with Single Server or Scale target number of desktop VMs utilizing sufficient number of Launchers (at 20-25 sessions/Launcher)
9. Time 2:23 Single Server or Scale target number of desktop VMs desktops launched (48 minute benchmark launch rate)
10. Time 2:25 All launched sessions must become active

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

11. Time 2:40 Login VSI Test Ends (based on Auto Logoff 900 Second period designated above.)
12. Time 2:55 All active sessions logged off
13. Time 2:57 All logging terminated; Test complete
14. Time 3:15 Copy all log files off to archive; Set virtual desktops to maintenance mode through broker; Shutdown all Windows machines
15. Time 3:30 Reboot all hypervisor hosts.
16. Time 3:45 Ready for the new test sequence.

Success Criteria

Our pass criteria for this testing follows:

Cisco will run tests at a session count level that effectively utilizes the blade capacity measured by CPU utilization, memory utilization, storage utilization, and network utilization. We will use Login VSI to launch version 4.1 Office Worker workloads. The number of launched sessions must equal active sessions within two minutes of the last session launched in a test as observed on the VSI Management console.

The Citrix Virtual Apps and Desktops Studio should be monitored throughout the steady state to make sure of the following:

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

Within 20 minutes of the end of the test, all sessions on all launchers must have logged out automatically and the Login VSI Agent must have shut down. Stuck sessions define a test failure condition.

Cisco requires three consecutive runs with results within +/-1% variability to pass the Cisco Validated Design performance criteria. For white papers written by partners, two consecutive runs within +/-1% variability are accepted. (All test data from partner run testing must be supplied along with the 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. FlexPod Data Center with Cisco UCS and Citrix RDS/Citrix Virtual Apps and Desktops 7 LTSR on VMware ESXi 7.02 Update 1 Test Results

The purpose of this testing is to provide the data needed to validate Citrix RDS Hosted Shared Desktop (RDS) and Citrix Virtual Apps and Desktops Hosted Virtual Desktop (VDI) randomly assigned, non-persistent with Citrix Provisioning Services 7 LTSR and Citrix Virtual Apps and Desktops Hosted Virtual Desktop (VDI) statically assigned, persistent full-clones models using ESXi and vCenter to virtualize Microsoft Windows 10 desktops and Microsoft Windows Server 2019 sessions on X-Series Compute Nodes M6 Blade Servers using a NetApp AFF400 storage system.

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 products with VMware vSphere.

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

VSImax 4.1.x Description

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

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

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

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

Server-Side Response Time Measurements

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

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

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

Calculate 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 43. Sample of a VSI max response time graph, representing a normal test

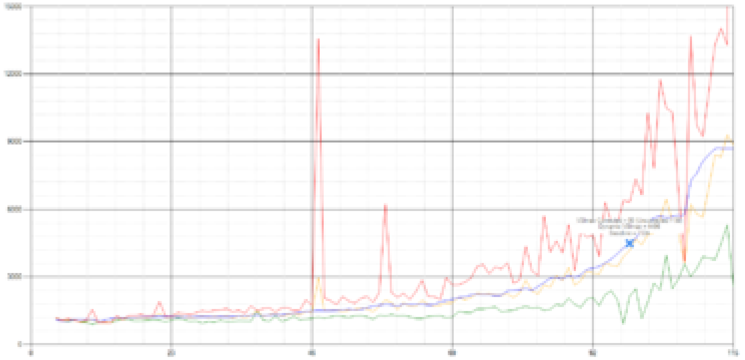
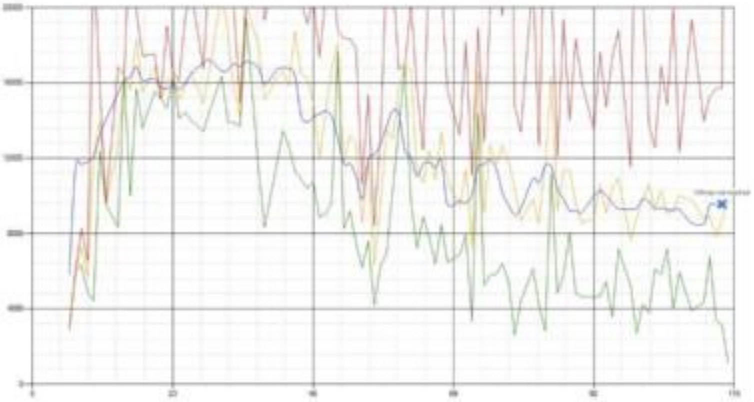


Figure 44. Sample of a VSI test response time graph where there was a clear performance issue



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. These response time of these actions are weighted before they are added to the total. This ensures that each activity has an equal impact on the total response time.

In comparison to previous VSImax models, this weighting much better represents system performance. All actions have very similar weight in the VSImax total. The following weighting of the response times is 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 basephase of an environment. With the new workloads (Taskworker, Powerworker, and so on) enabling 'basephase' 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.

Calculate the Basephase

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

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

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

To remove noise (accidental spikes) from the calculation, the top 5 percent, and bottom 5 percent of the VSI response time samples are removed from the average calculation, with a minimum of 1 top and 1 bottom sample. As a result, with 60 active users, the last 31 VSI response time sample are taken. From those 31 samples the top 2 samples are removed and lowest 2 results are removed (5 percent of 31 = 1.55, rounded to 2). At 60 users the average is then calculated over the 27 remaining results.

VSImax v4.1.x is reached when the VSIbase + a 1000 ms latency threshold is not reached by the average VSI response time result. Depending on the tested system, VSImax response time can grow 2 - 3x the baseline average. In end-user computing, a 3x increase in response time in comparison to the baseline is typically regarded for 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 4000 the maximum average response time may not be greater than 4000ms (4000+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 into system performance and scales to extremely large systems.

Single-Server Recommended Maximum Workload

For both the Citrix Virtual Apps and Desktops 7 LTSR Hosted Virtual Desktop and Citrix RDS 7 LTSR RDS Hosted Shared Desktop use cases, a recommended maximum workload was determined by the Login VSI Knowledge Worker Workload in VSI Benchmark Mode end user experience measurements and blade 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%.

Note: Memory should never be oversubscribed for Desktop Virtualization workloads.

Table 25. Phases of test runs

Test Phase	Description
Boot	Start all RDS and VDI virtual machines at the same time
Idle	The rest time after the last desktop is registered on the XD Studio. (typically, a 30-40 minute, <60 min)
Logon	The Login VSI phase of the test is where sessions are launched and start executing the workload over a 48 minutes duration
Steady state	The steady state phase is where all users are logged in and performing various workload tasks such as using Microsoft Office, Web browsing, PDF printing, playing videos, and compressing files (typically for 15-minute duration)
Logoff	Sessions finish executing the Login VSI workload and logoff

Test Results

This chapter contains the following:

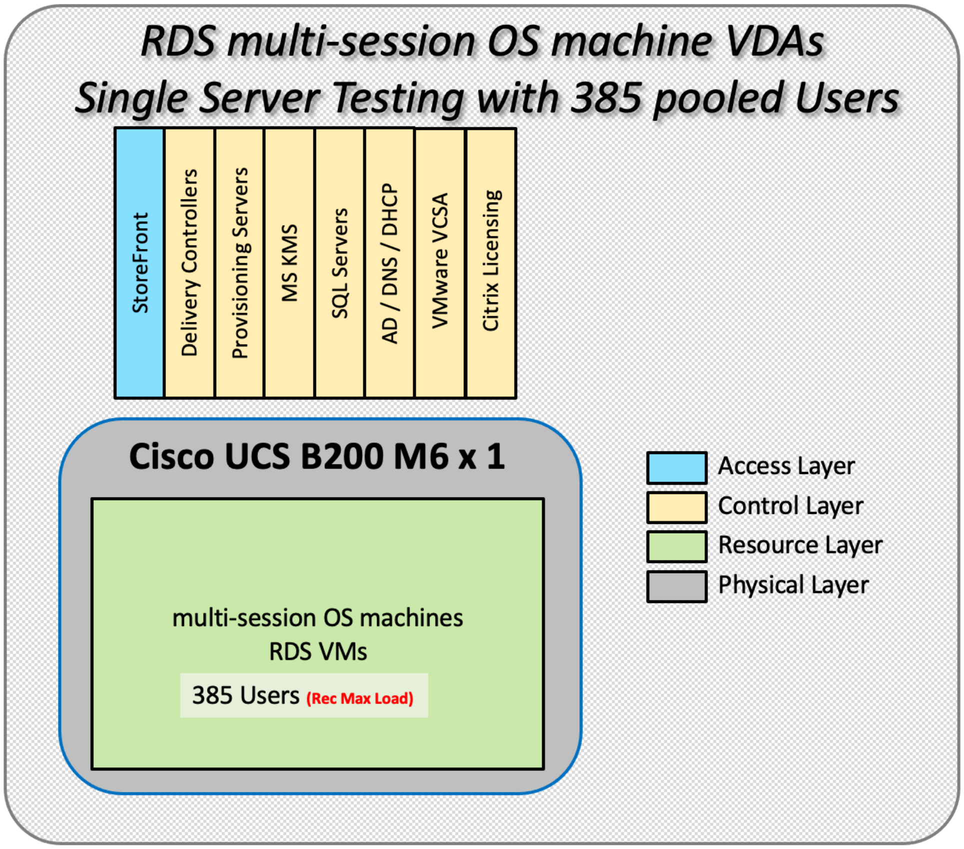
Single-Server Recommended Maximum Workload Testing

This section shows the key performance metrics that were captured on the Cisco UCS host blades during the single server testing to determine the Recommended Maximum Workload per host server. The single server testing comprised of three tests: 385 RDS sessions, 250 VDI Non-Persistent sessions, and 250 VDI Persistent sessions.

Single-Server Recommended Maximum Workload for RDS with 385 Users

The Figure 45 illustrates the single-server recommended maximum workload for RDS with 385 users.

Figure 45. Single Server Recommended Maximum Workload for RDS with 385 Users



The recommended maximum workload for a Cisco UCS B200 M6 Compute Node with dual Intel Xeon Gold 6338 processors, 1TB 3200MHz RAM is 385 Server 2019 Hosted Shared Desktop sessions. Each dedicated blade server ran 10 Server 2019 Virtual Machines. Each virtual server was configured with 8 vCPUs and 32GB RAM.

Figure 46. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | VSI Score

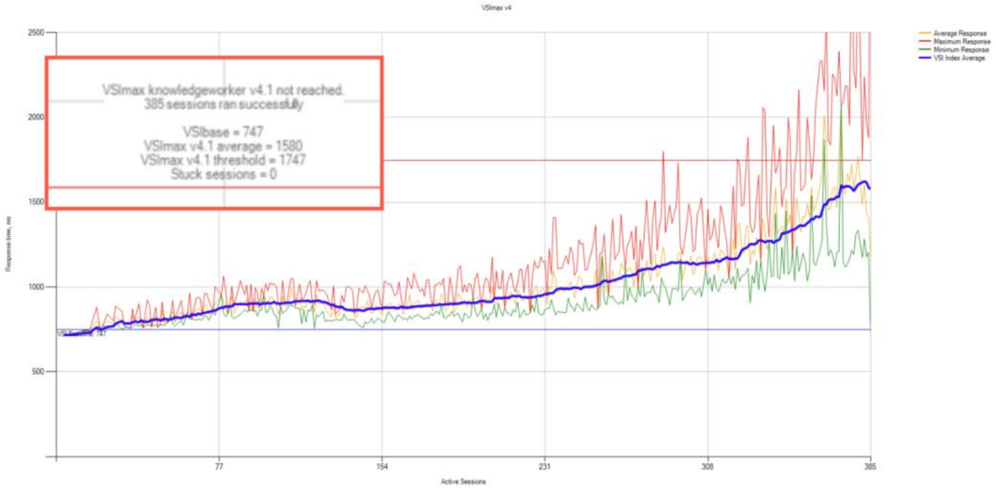
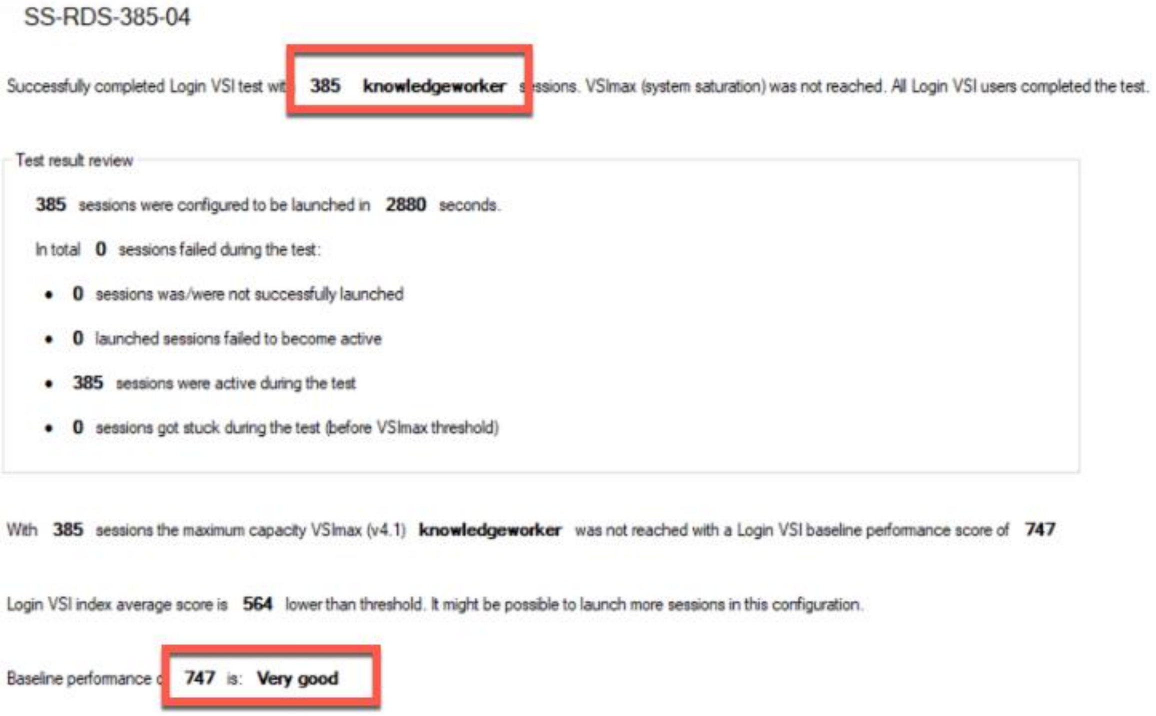


Figure 47. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | VSI Repeatability



SS-RDS-385-04

Successfully completed Login VSI test with 385 knowledgeworker sessions. VSImax (system saturation) was not reached. All Login VSI users completed the test.

Test result review

385 sessions were configured to be launched in **2880** seconds.

In total **0** sessions failed during the test:

- **0** sessions was/were not successfully launched
- **0** launched sessions failed to become active
- **385** sessions were active during the test
- **0** sessions got stuck during the test (before VSImax threshold)

With **385** sessions the maximum capacity VSImax (v4.1) **knowledgeworker** was not reached with a Login VSI baseline perfomance score of **747**

Login VSI index average score is **564** lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance of **747** is: **Very good**

Performance data for the server running the workload as follows:

Figure 48. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | Host CPU Utilization

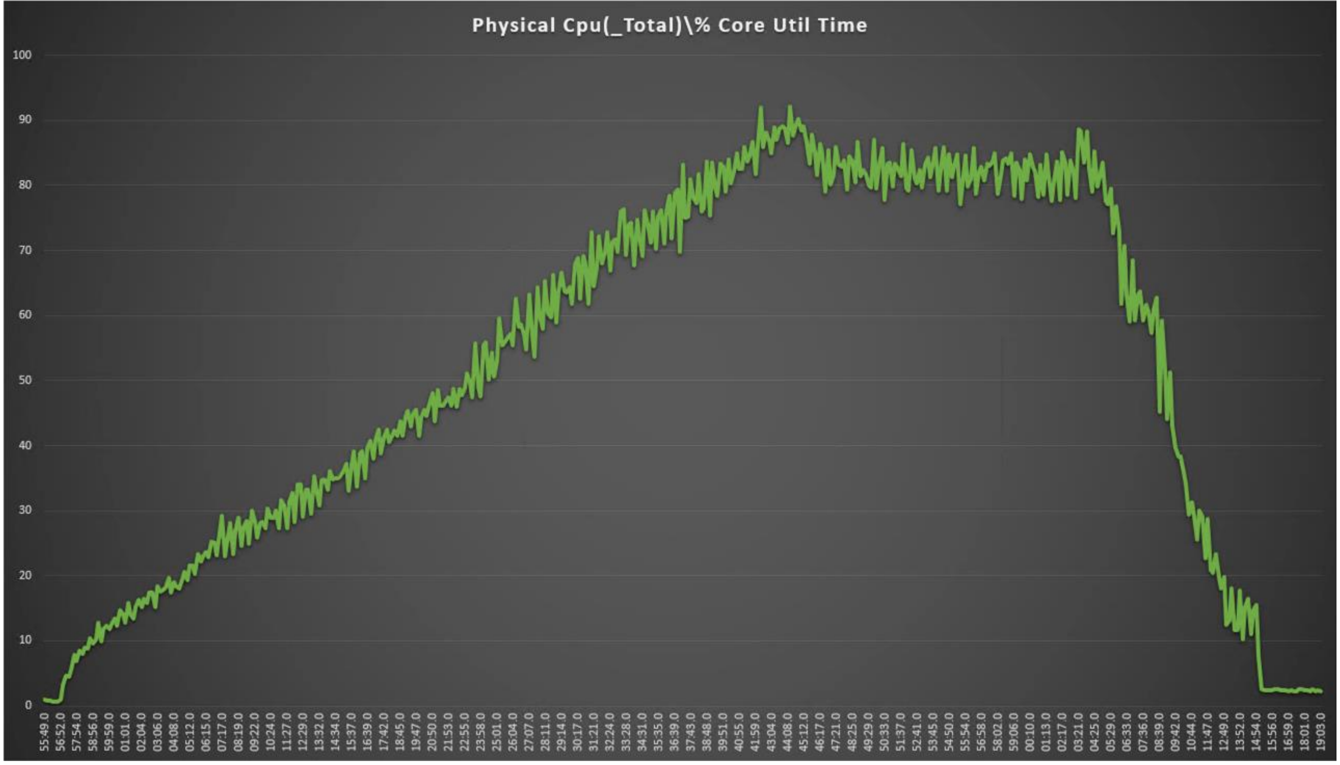


Figure 49. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | Host Memory Utilization

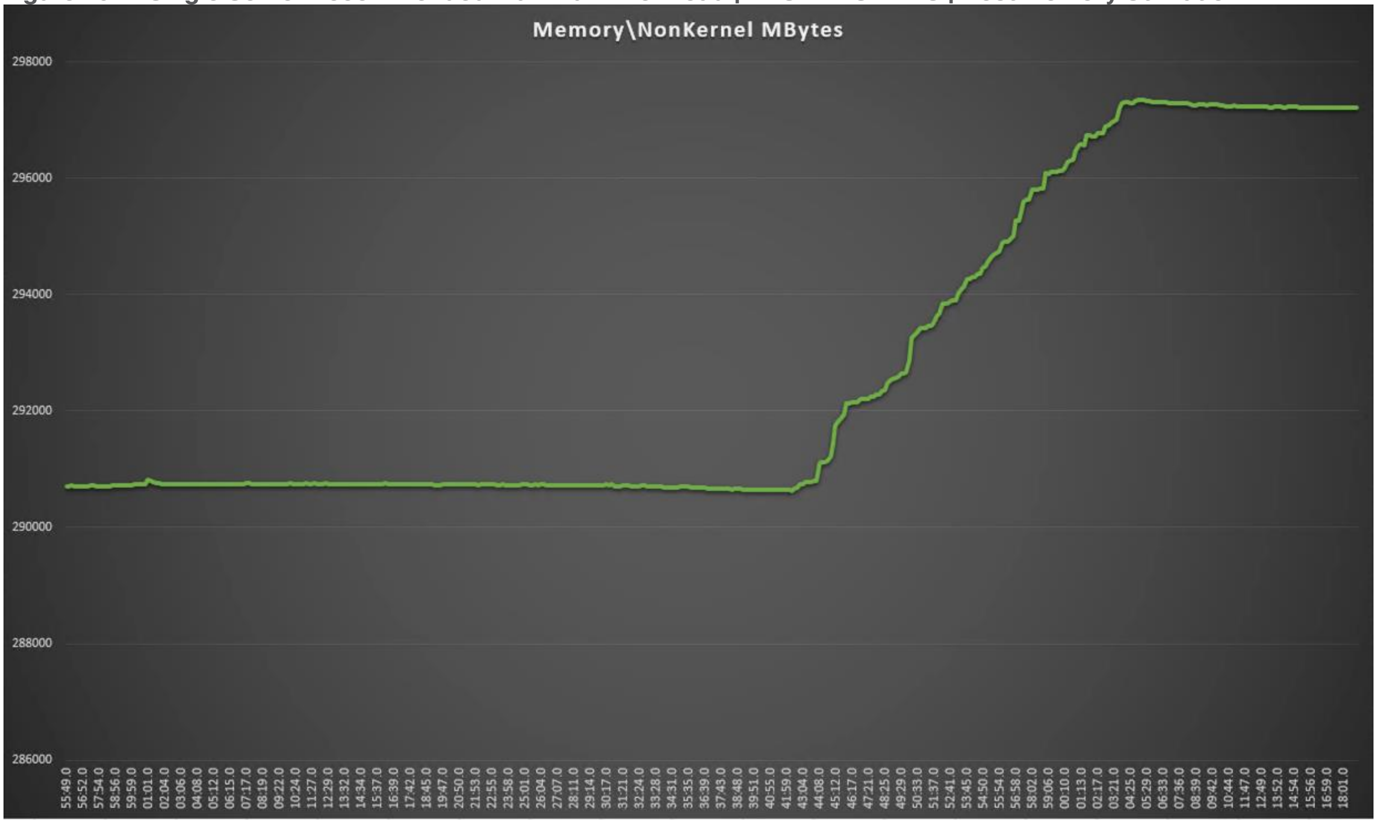
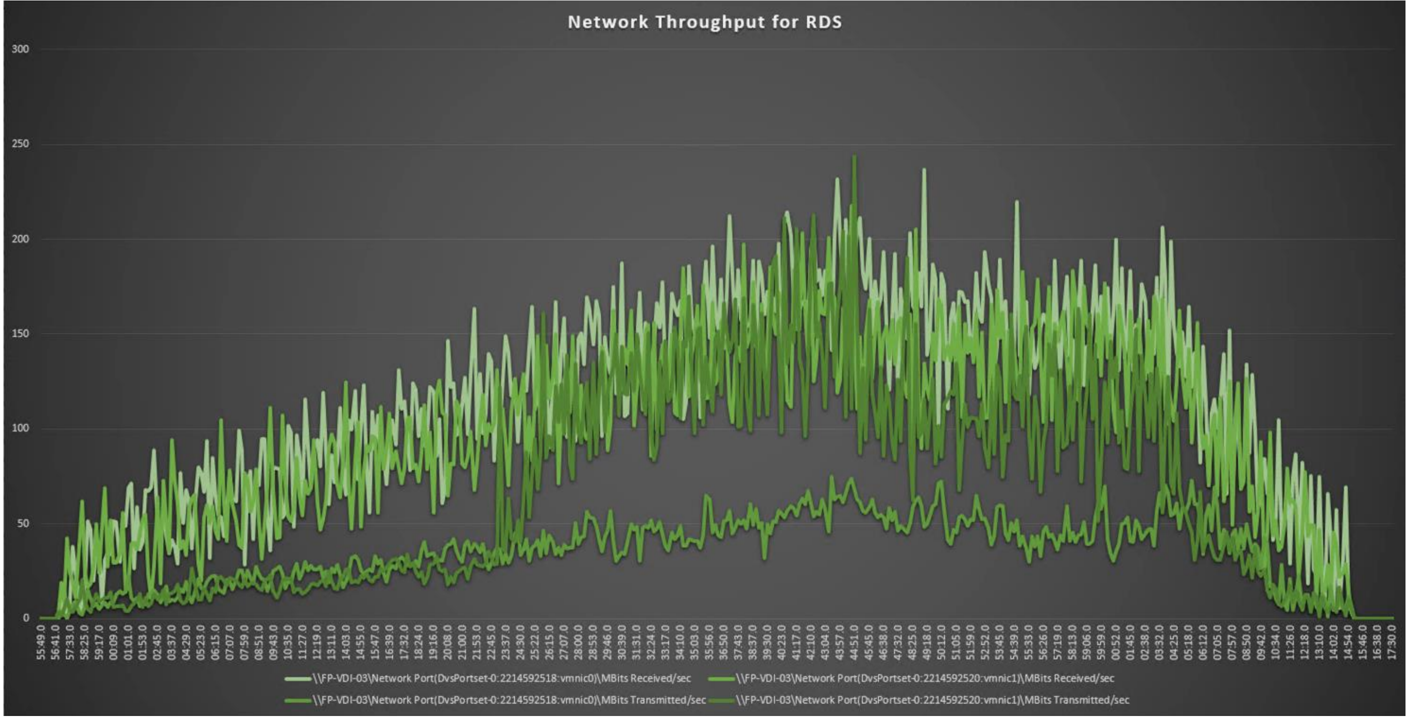


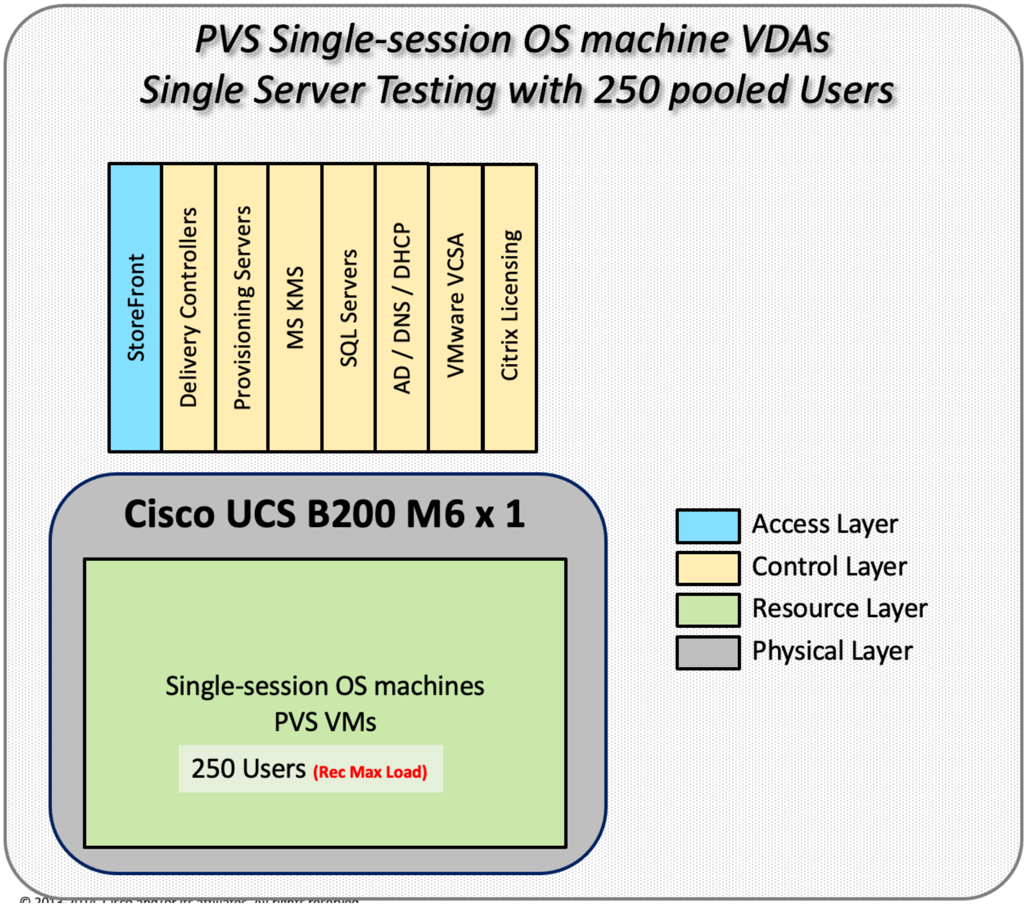
Figure 50. Single Server | RDS 7 LTSRRDS | Host Network Utilization



Single-Server Recommended Maximum Workload for VDI Non-Persistent with 250 Users

The Figure 51 illustrates single-server recommended maximum workload for VDI non-persistent with 250 users.

Figure 51. Single Server Recommended Maximum Workload for VDI Non-Persistent with 270 Users



The recommended maximum workload for a Cisco UCS B200 M6 Compute Node with dual Intel Xeon Gold 6338 processors, 1TB 3200MHz RAM is 270 Windows 10 64-bit virtual machines with 2 vCPU and 4GB RAM. Login VSI and node performance data as follows:

Figure 52. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-NP | VSI Score

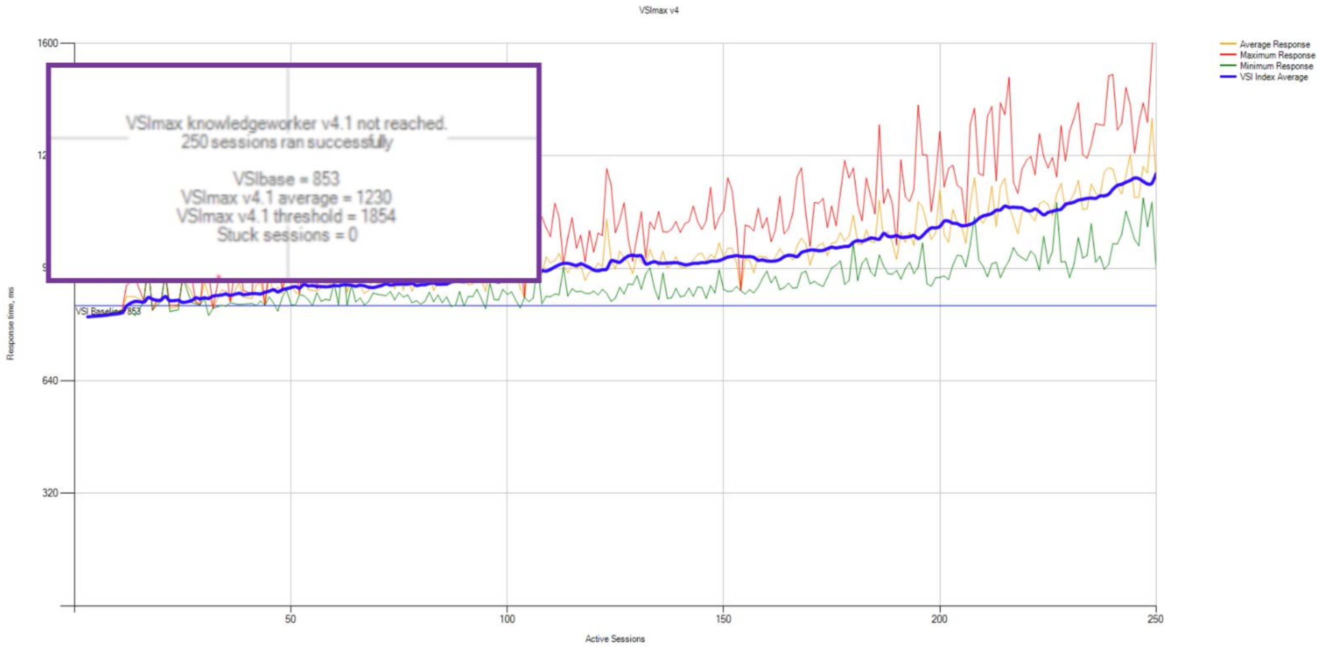
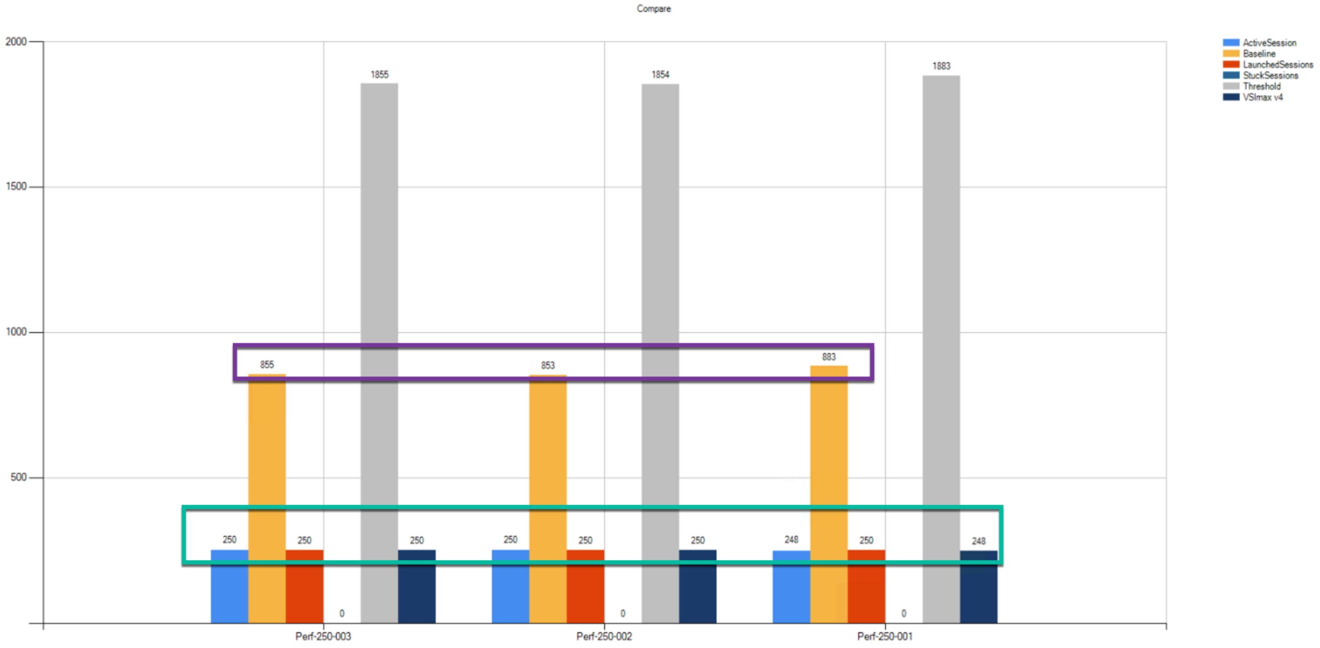


Figure 53. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-NP | VSI Repeatability



Performance data for the server running the workload as follows:

Figure 54. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-NP | Host CPU Utilization

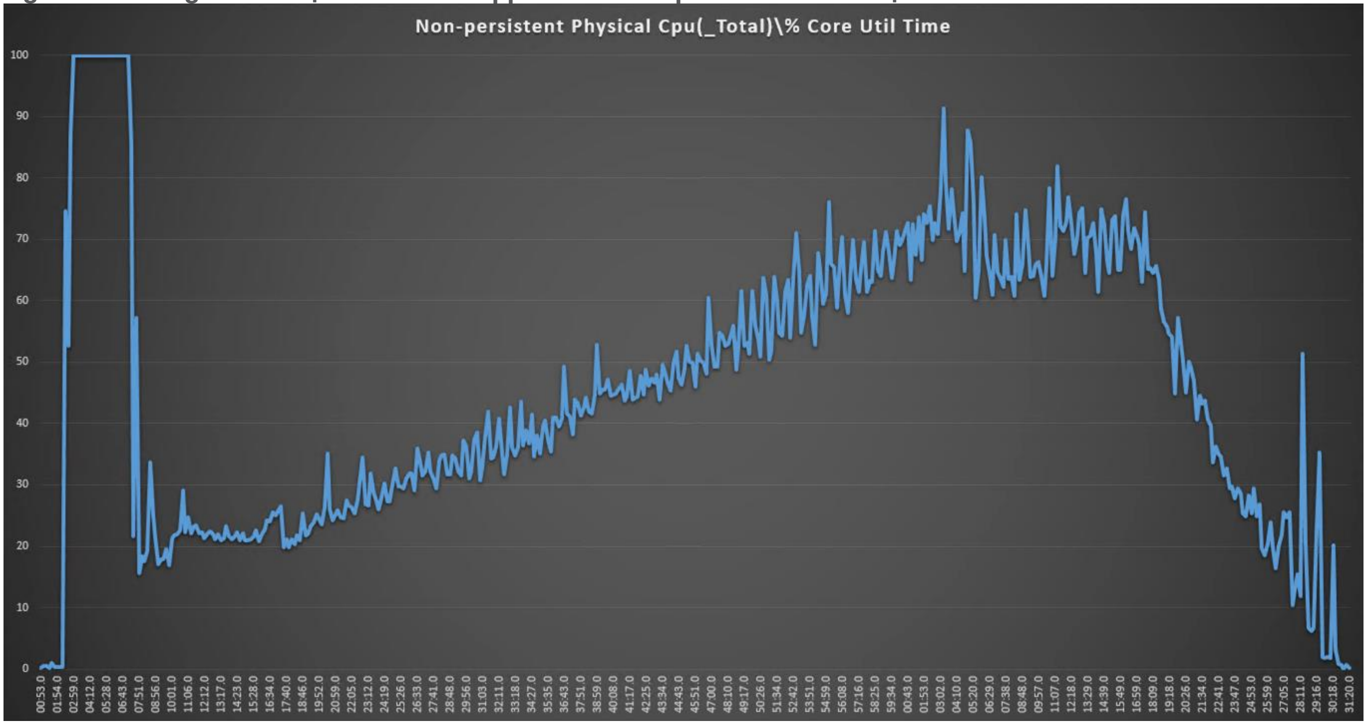


Figure 55. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-NP | Host Memory Utilization

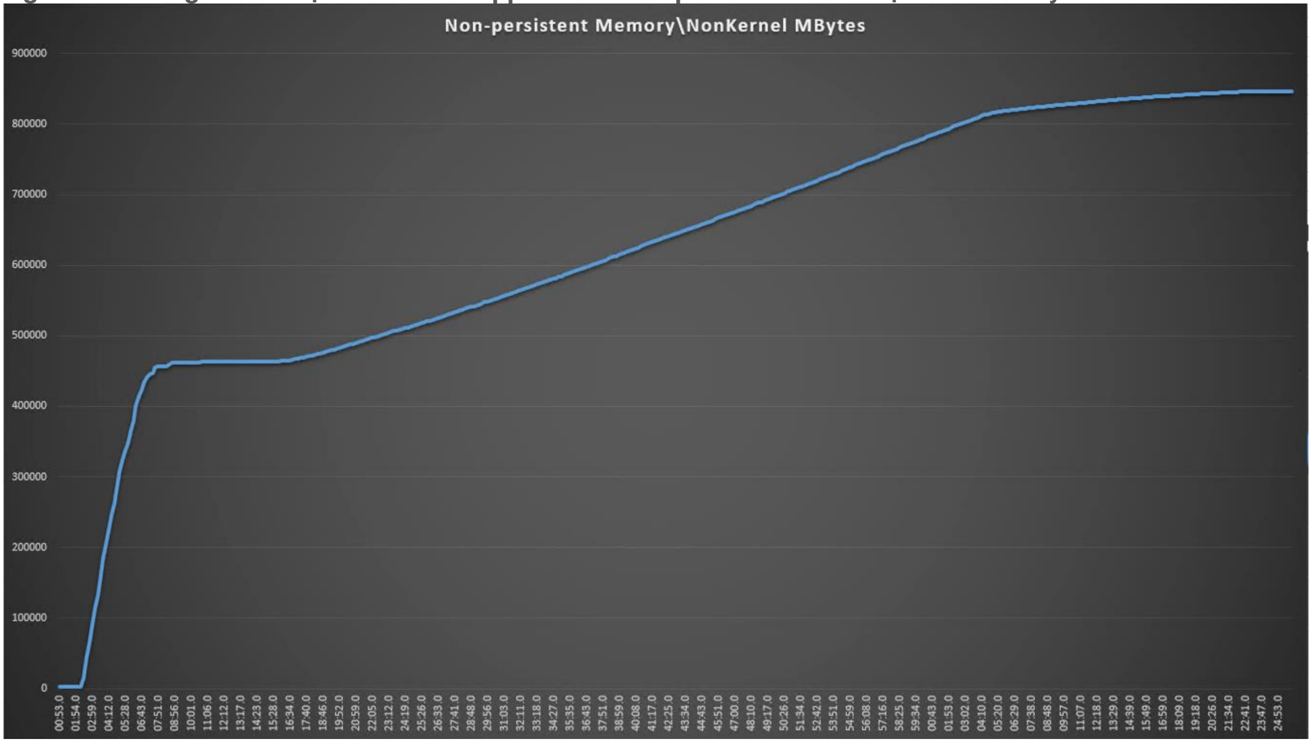
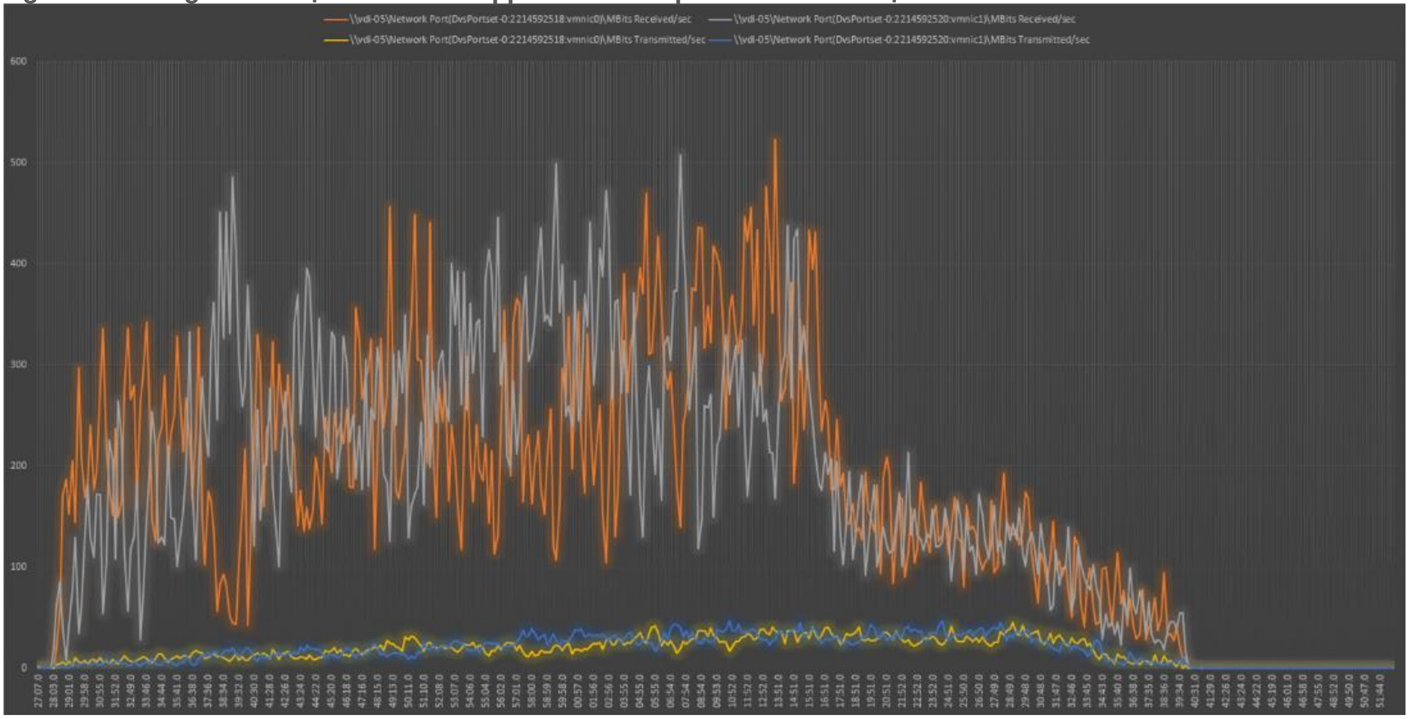


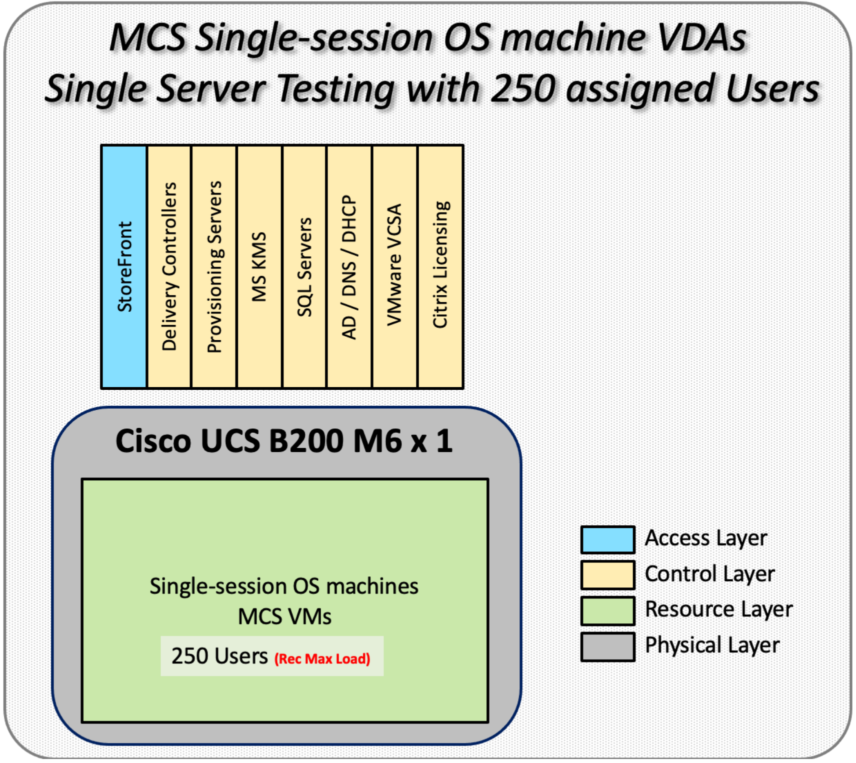
Figure 56. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-NP | Host Network Utilization



Single-Server Recommended Maximum Workload for VDI Persistent with 270 Users

The Figure 57 illustrates the single-server recommended maximum workload for VDI persistent with 250 users.

Figure 57. Single Server Recommended Maximum Workload for VDI Persistent with 270 Users



The recommended maximum workload for a Cisco UCS B200 M6 Compute Node with dual Intel Xeon Gold 6338 processors, 1TB 3200MHz RAM is 270 Windows 10 64-bit virtual machines with 2 vCPU and 4GB RAM. Login VSI and blade performance data as follows:

Figure 58. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-P | VSI Score

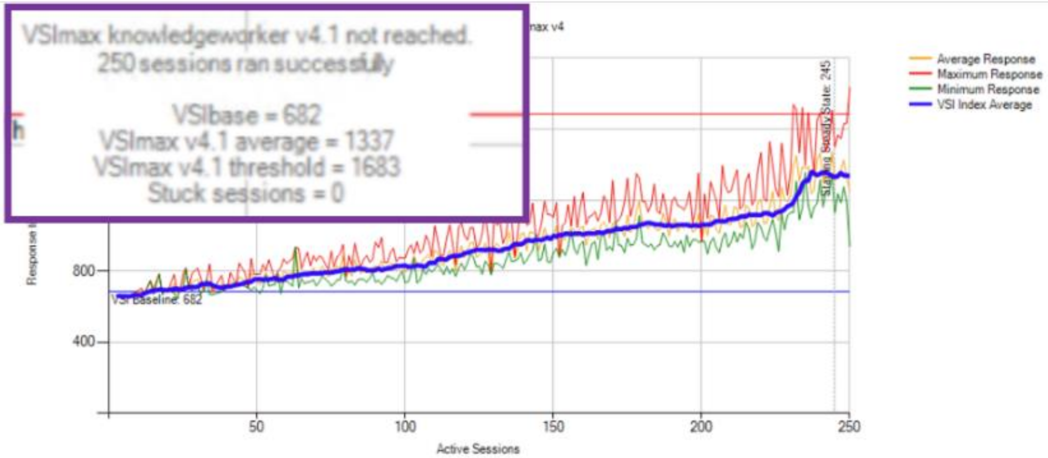
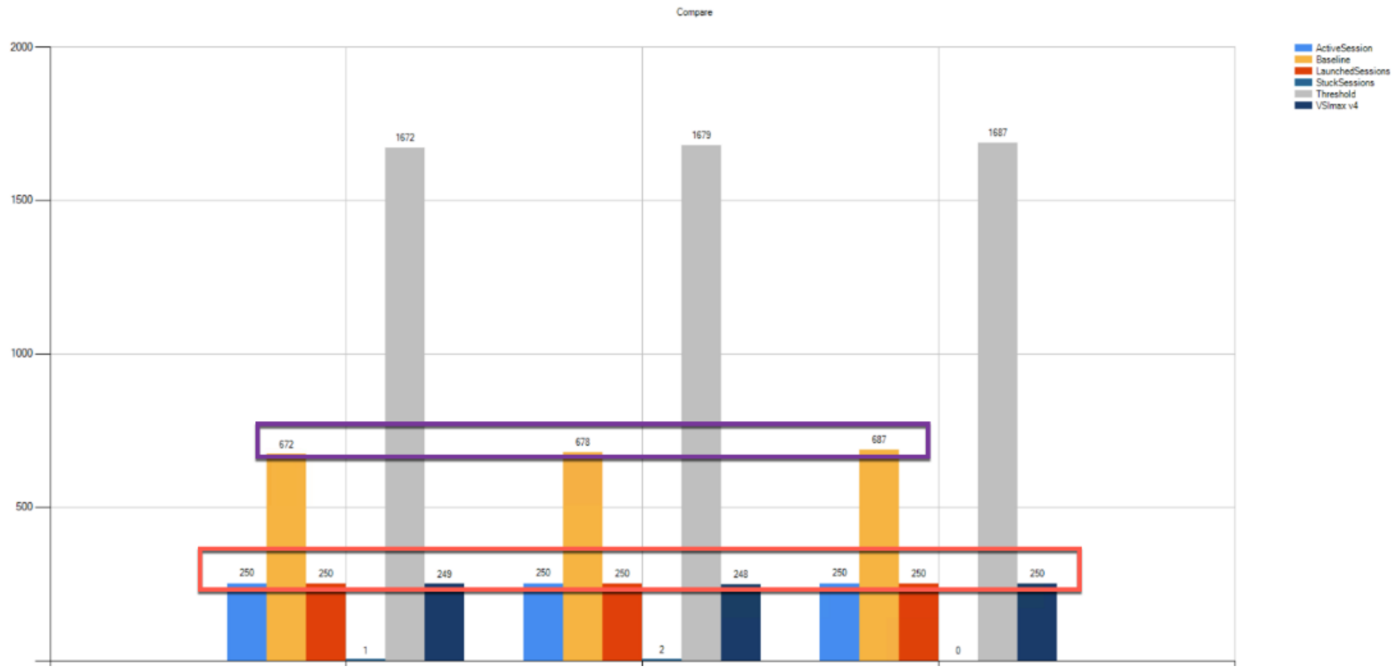


Figure 59. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-P | VSI Repeatability



Performance data for the server running the workload as follows:

Figure 60. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-P | Host CPU Utilization

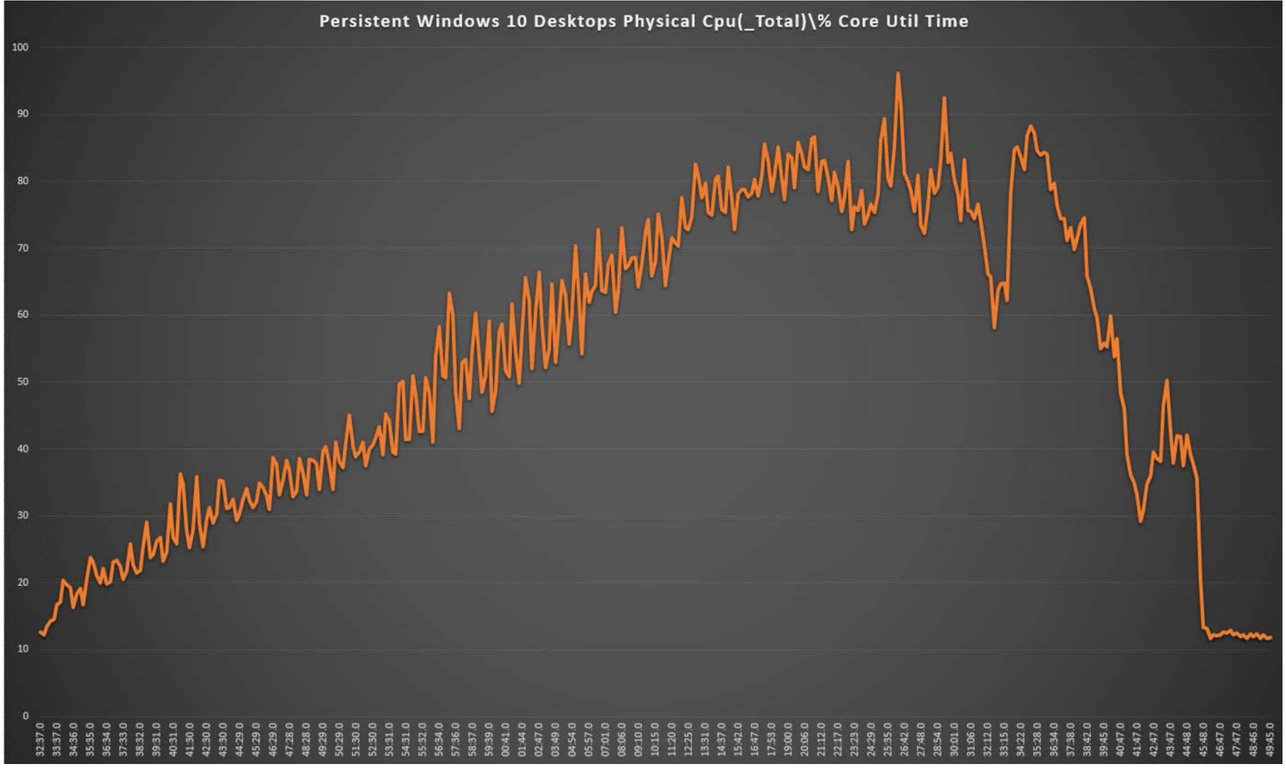
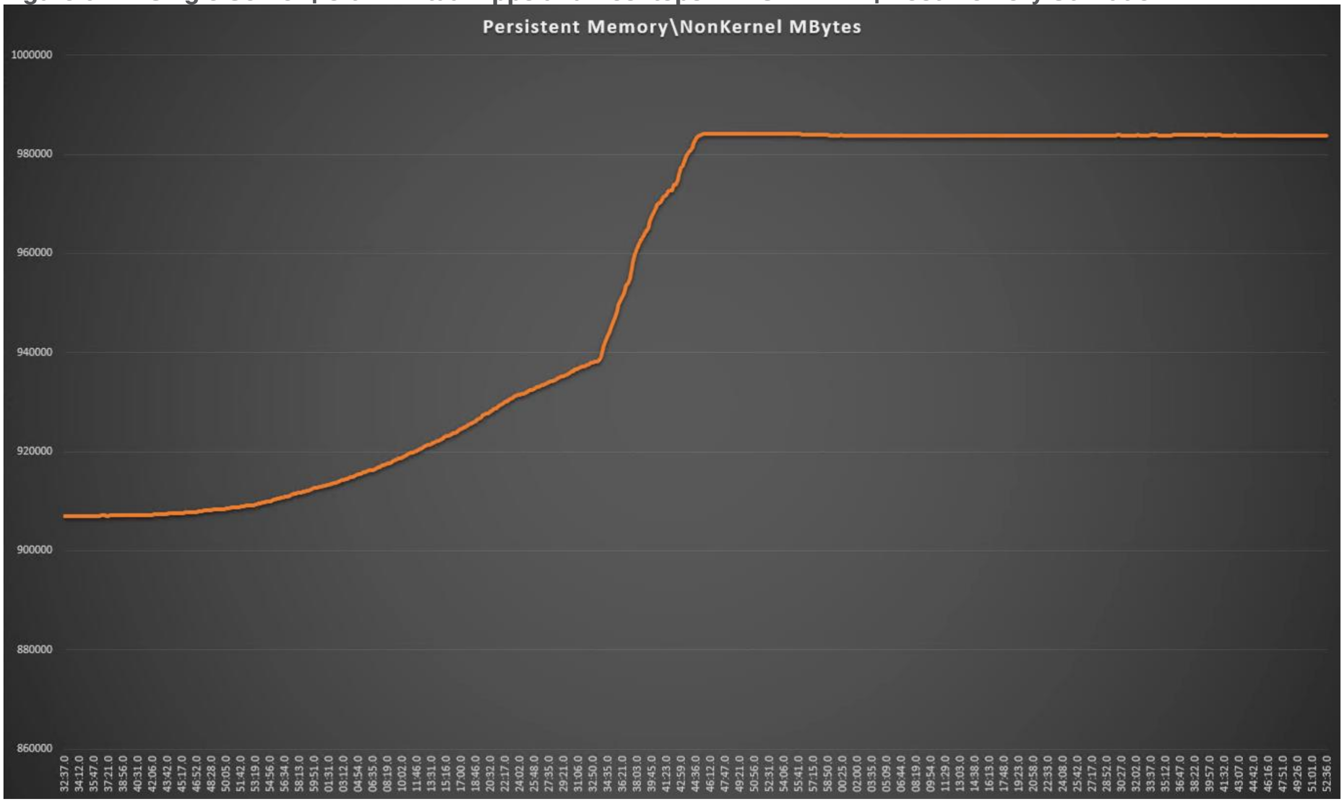


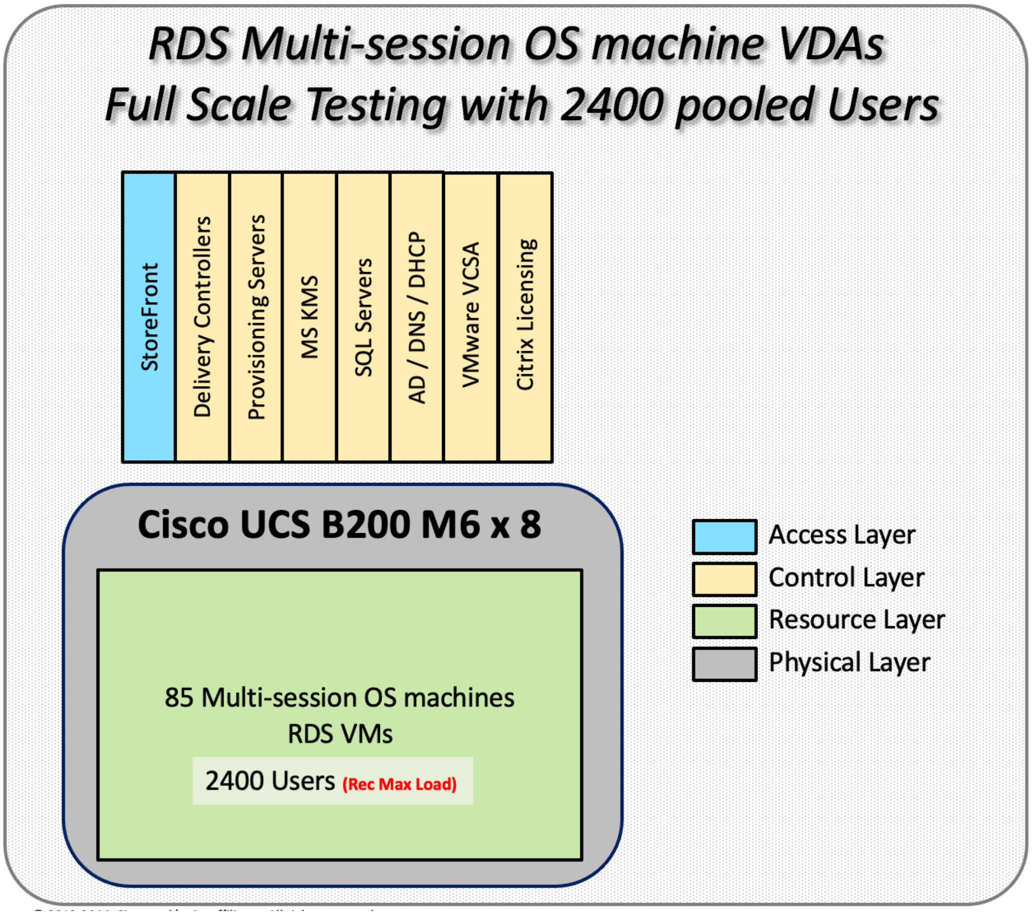
Figure 61. Single Server | Citrix Virtual Apps and Desktops 7 LTSR VDI-P | Host Memory Utilization



Full-Scale RDS Workload Testing with 2400 Users

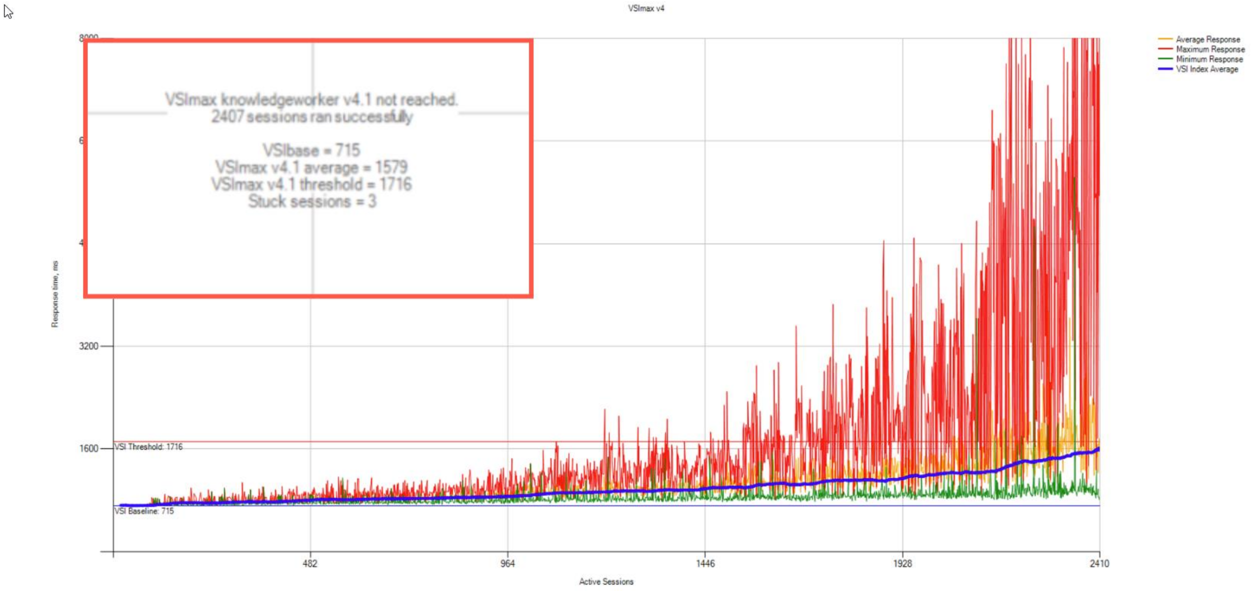
This section shows the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. The full-scale testing with 2400 users comprised of: 2400 Hosted Shared Desktop Sessions using 8 compute nodes.

To achieve the target, sessions were launched against all workload clusters concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.



The configured system efficiently and effectively delivered the following results.

Figure 62. **Full Scale | 2400 RDS Users | VSI Score**



VSImax knowledgeworker v4.1 not reached.
2407 sessions ran successfully

VSIbase = 715
VSImax v4.1 average = 1579
VSImax v4.1 threshold = 1716
Stuck sessions = 3

Figure 63. Full Scale | 2400 RDS Users | VSI Repeatability

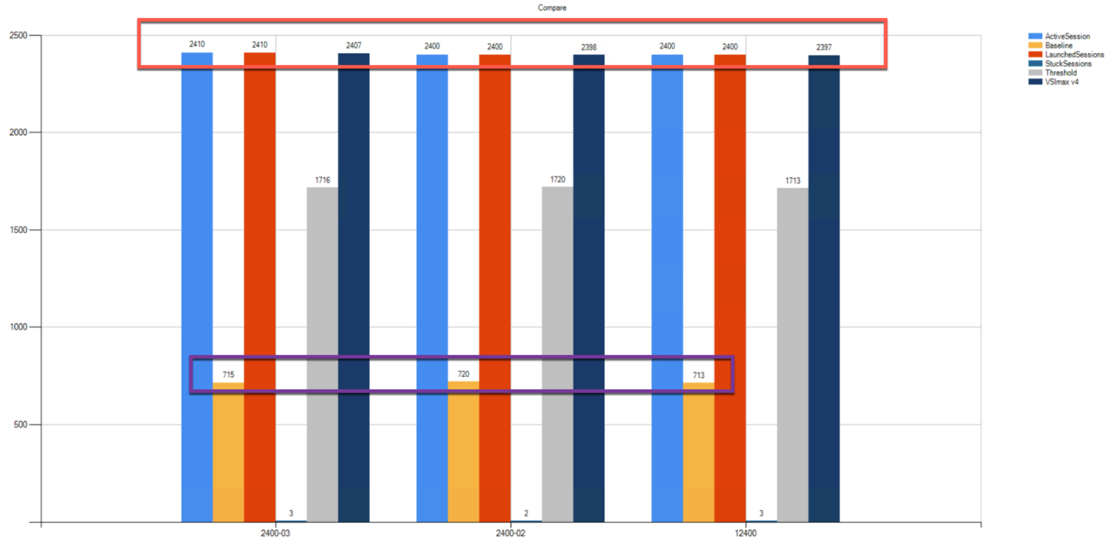


Figure 64. **Full Scale | 2400 RDS Users | RDS Hosts | Host CPU Utilization**

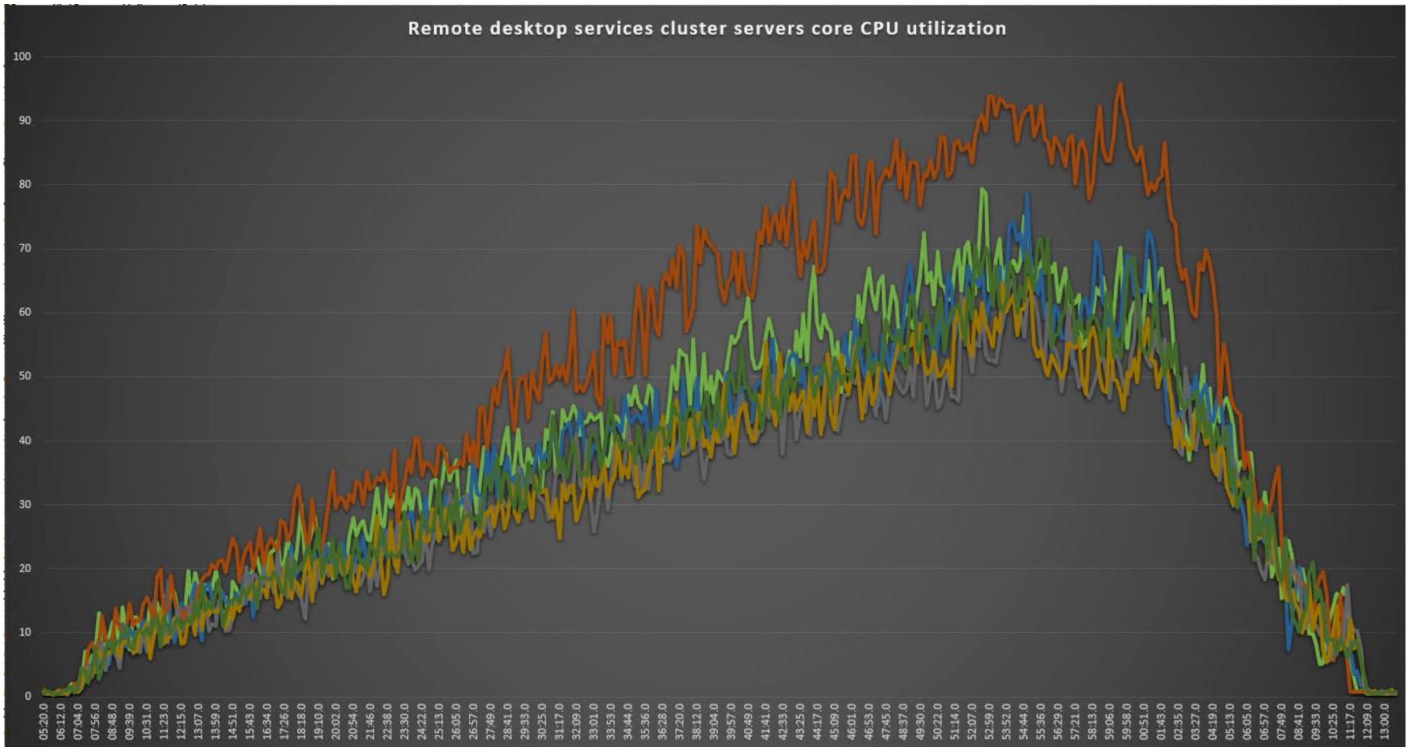
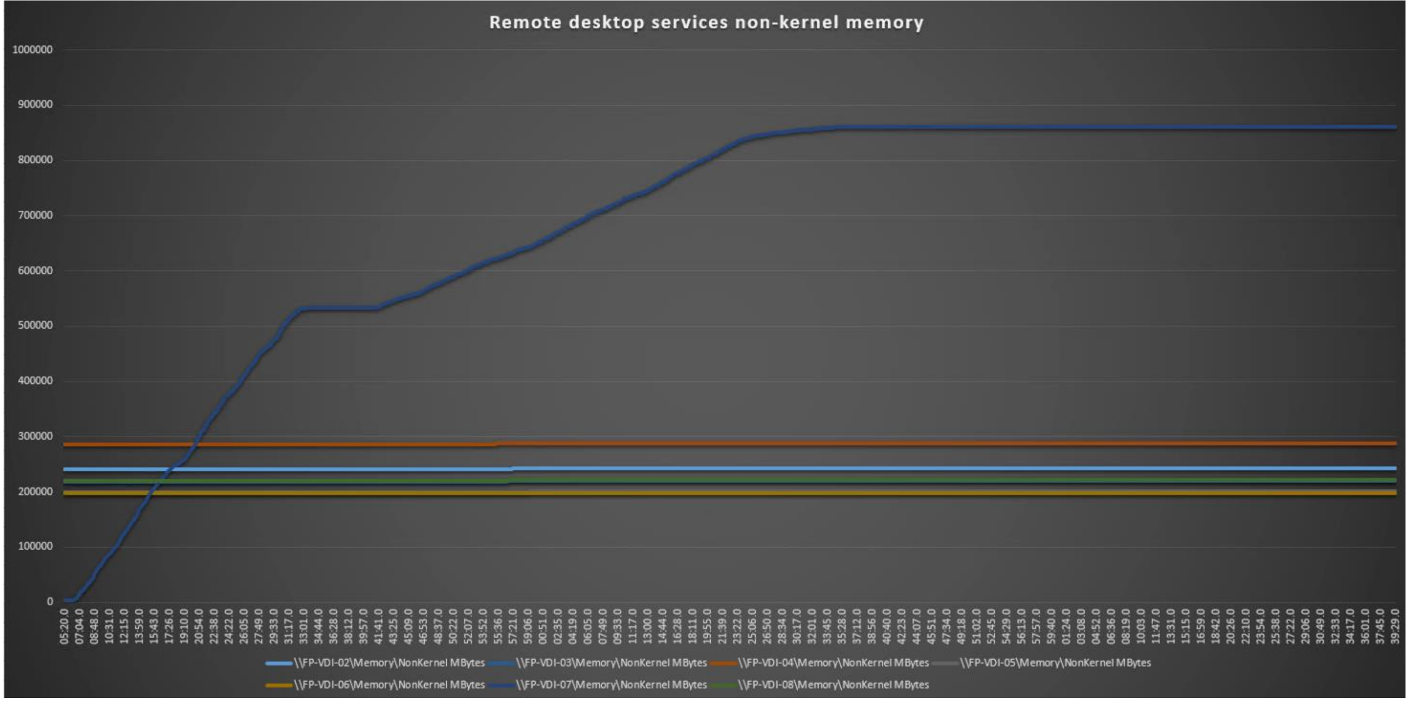


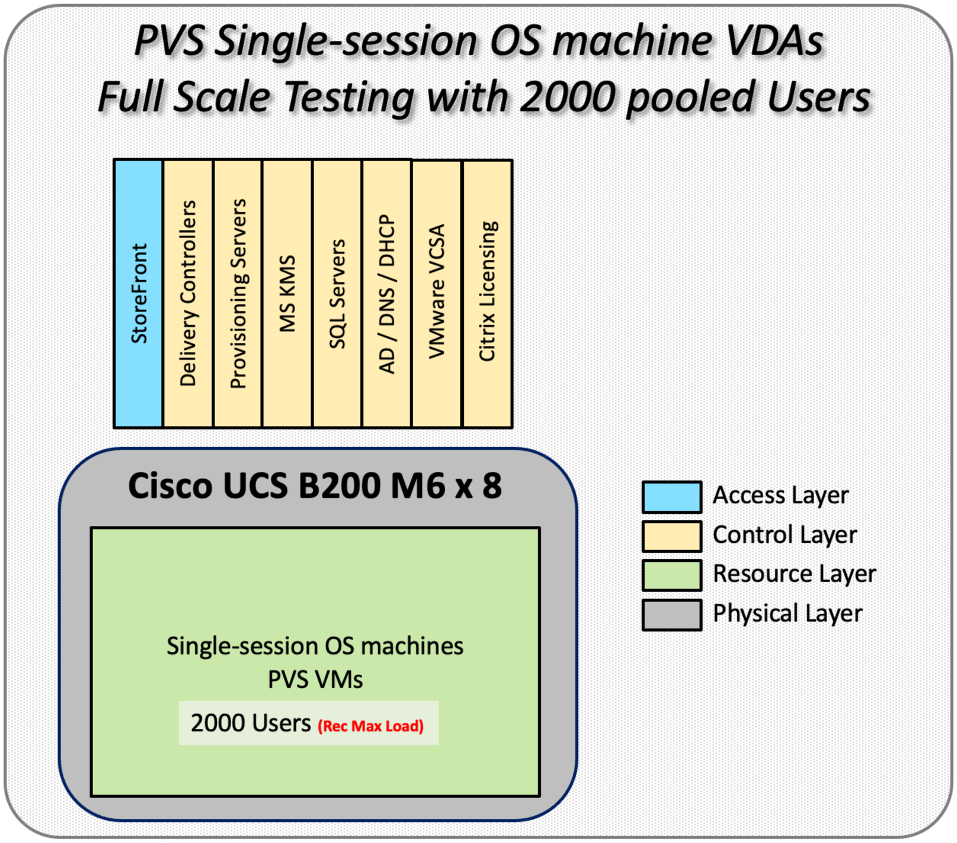
Figure 65. **Full Scale | 2400 RDS Users | RDS Hosts | Host Memory Utilization**



Full-Scale Non-Persistent Workload Testing with 2000 Users

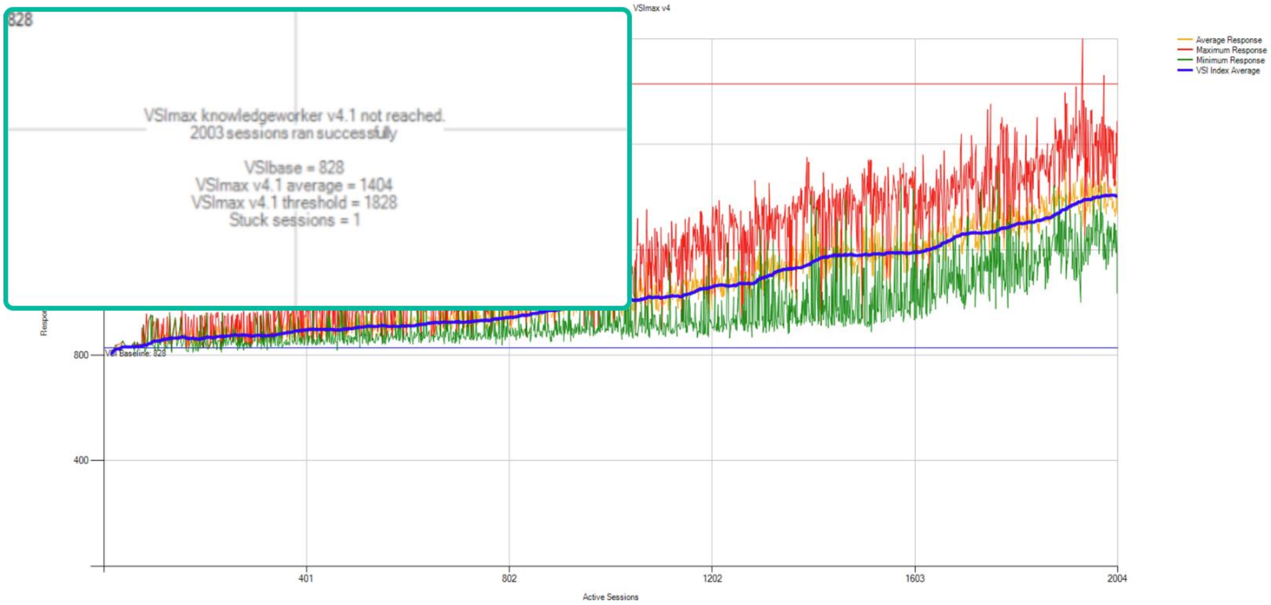
This section shows the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. The full-scale testing with 2000 users comprised of: 2000 Hosted Virtual Desktops using 8 compute nodes.

The combined mixed workload for the solution is 2000 users. To achieve the target, sessions were launched against all workload clusters concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.



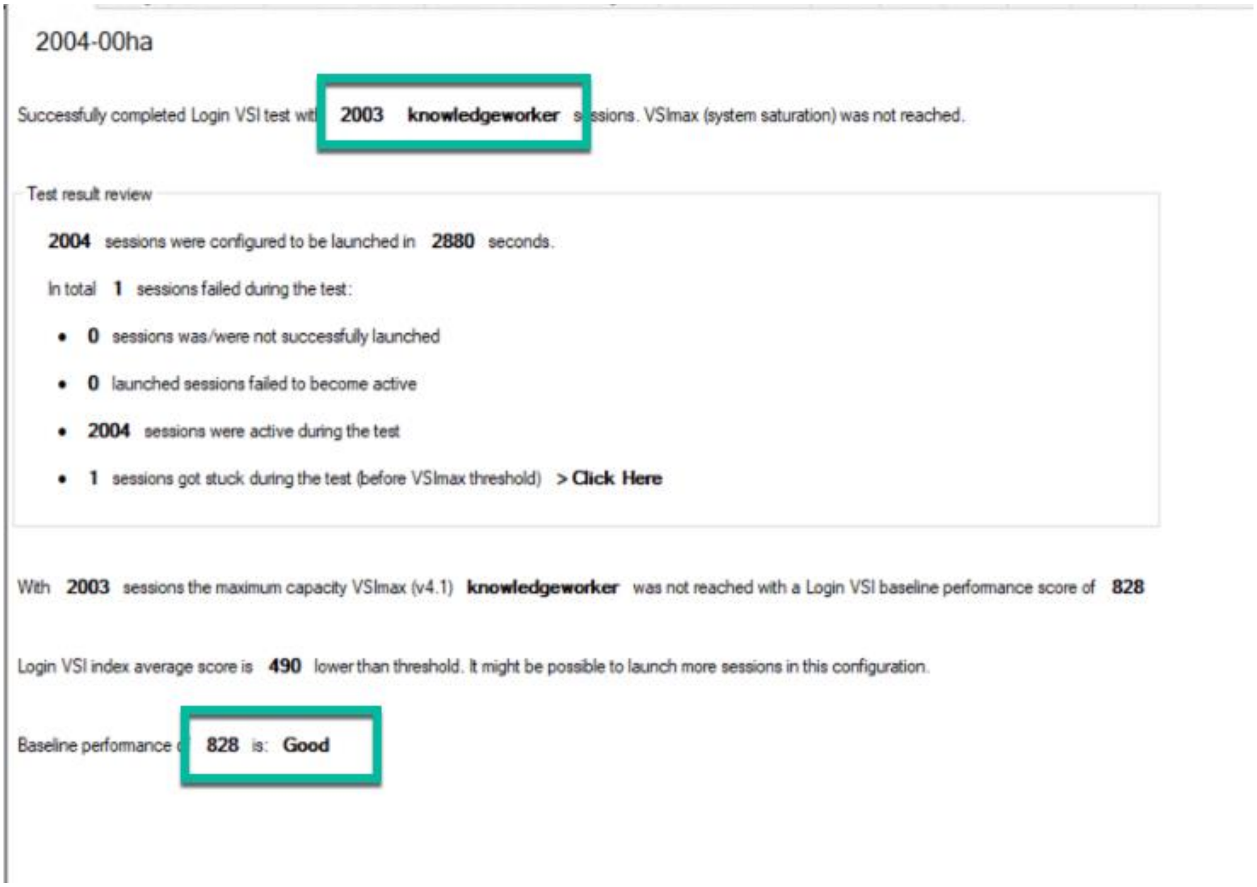
The configured system efficiently and effectively delivered the following results.

Figure 66. Full-Scale | 2000 non-persistent Users | VSI Score



VSImax knowledgeworker v4.1 not reached.
2003 sessions ran successfully

VSIbase = 828
VSImax v4.1 average = 1404
VSImax v4.1 threshold = 1828
Stuck sessions = 1



2004-00ha

Successfully completed Login VSI test wit **2003 knowledgeworker** s ssions. VSImax (system saturation) was not reached.

Test result review

2004 sessions were configured to be launched in **2880** seconds.

In total **1** sessions failed during the test:

- **0** sessions was/were not successfully launched
- **0** launched sessions failed to become active
- **2004** sessions were active during the test
- **1** sessions got stuck during the test (before VSImax threshold) **> Click Here**

With **2003** sessions the maximum capacity VSImax (v4.1) **knowledgeworker** was not reached with a Login VSI baseline performance score of **828**

Login VSI index average score is **490** lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance c **828** is: **Good**

Figure 67. Full-Scale | 2000 Non-persistentUsers | VSI Repeatability

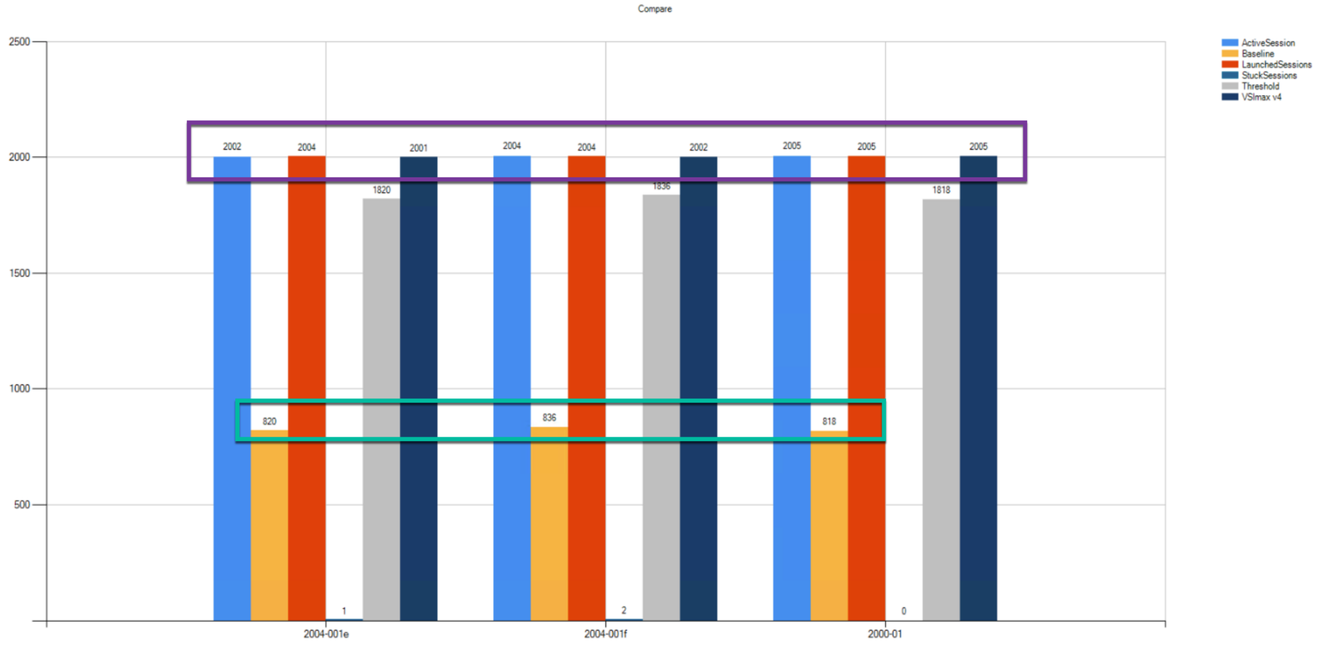


Figure 68. Full-Scale | 2000 non-persistent users | NP-VDI Hosts | Host CPU Utilization

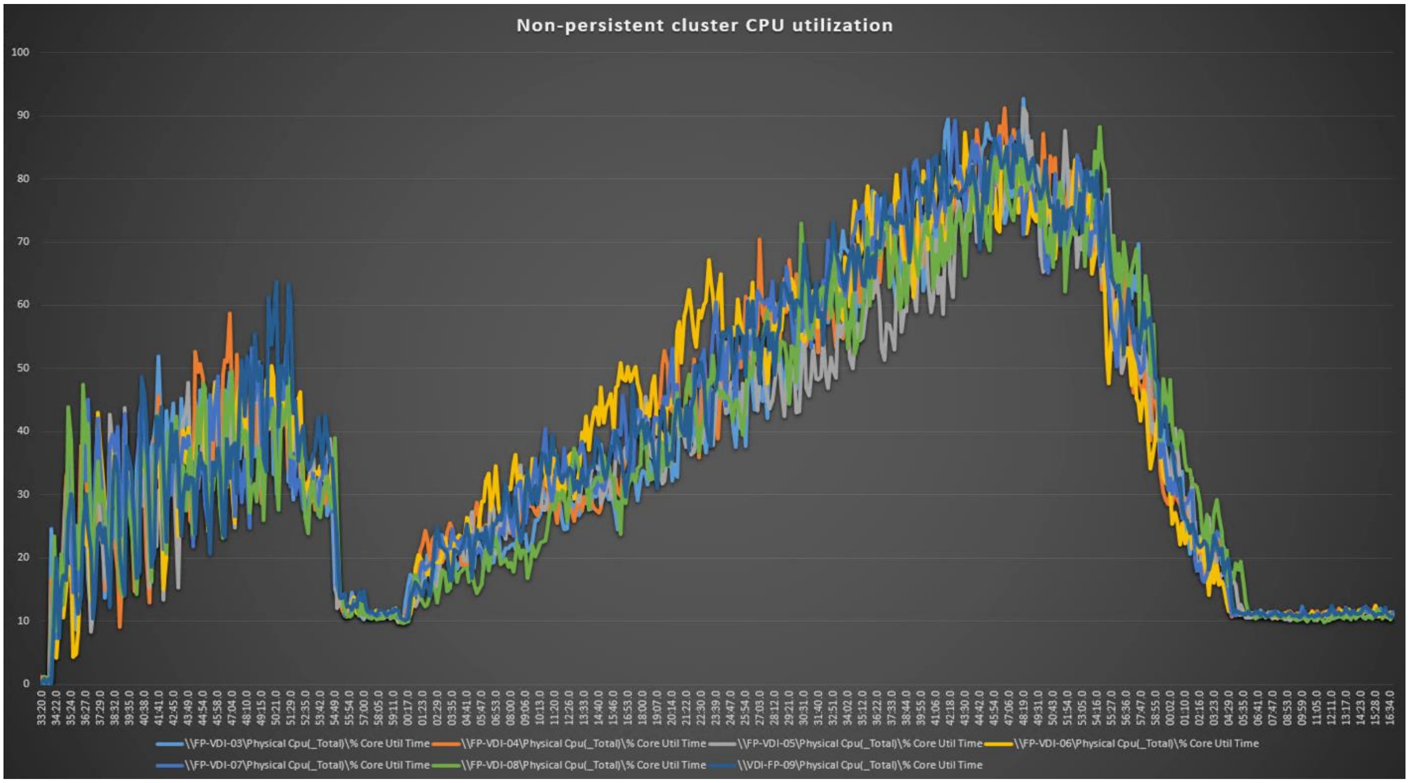
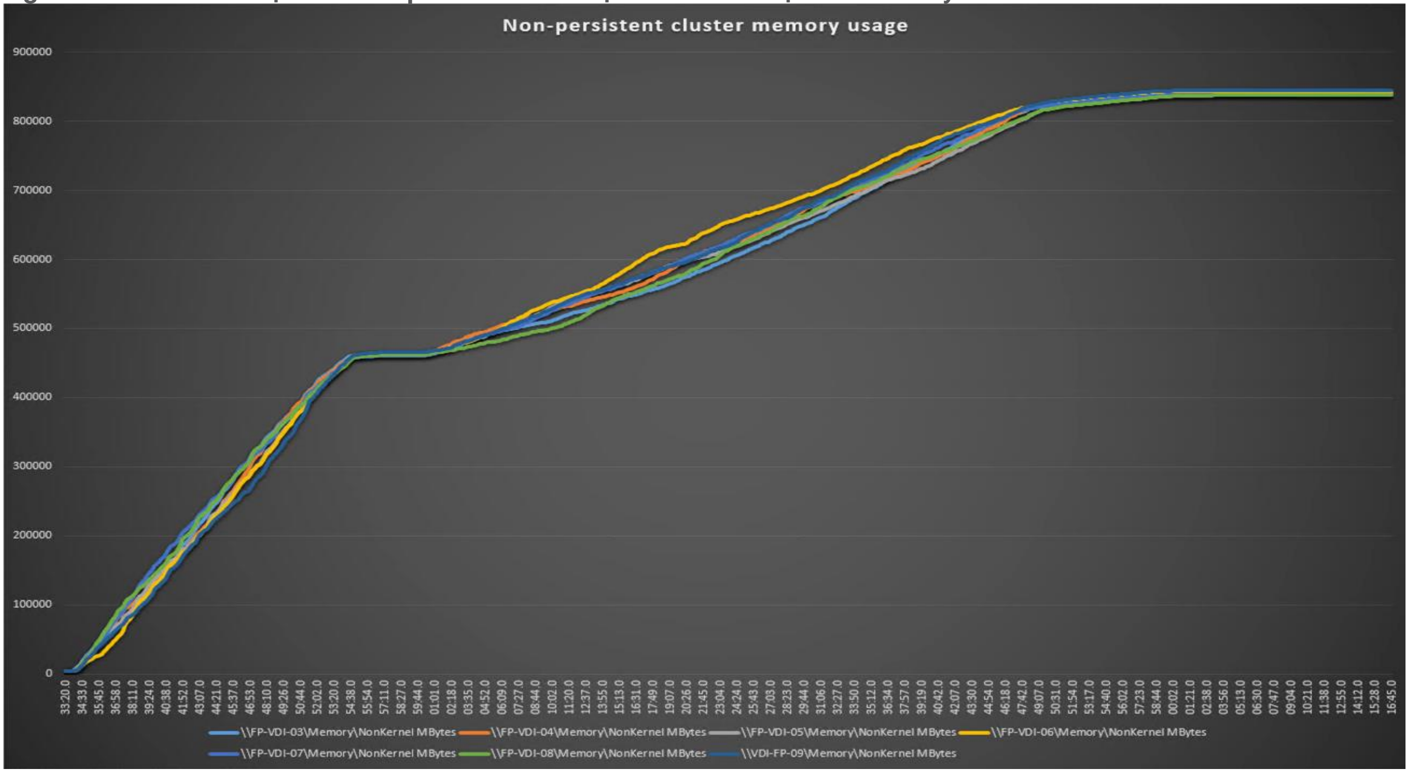


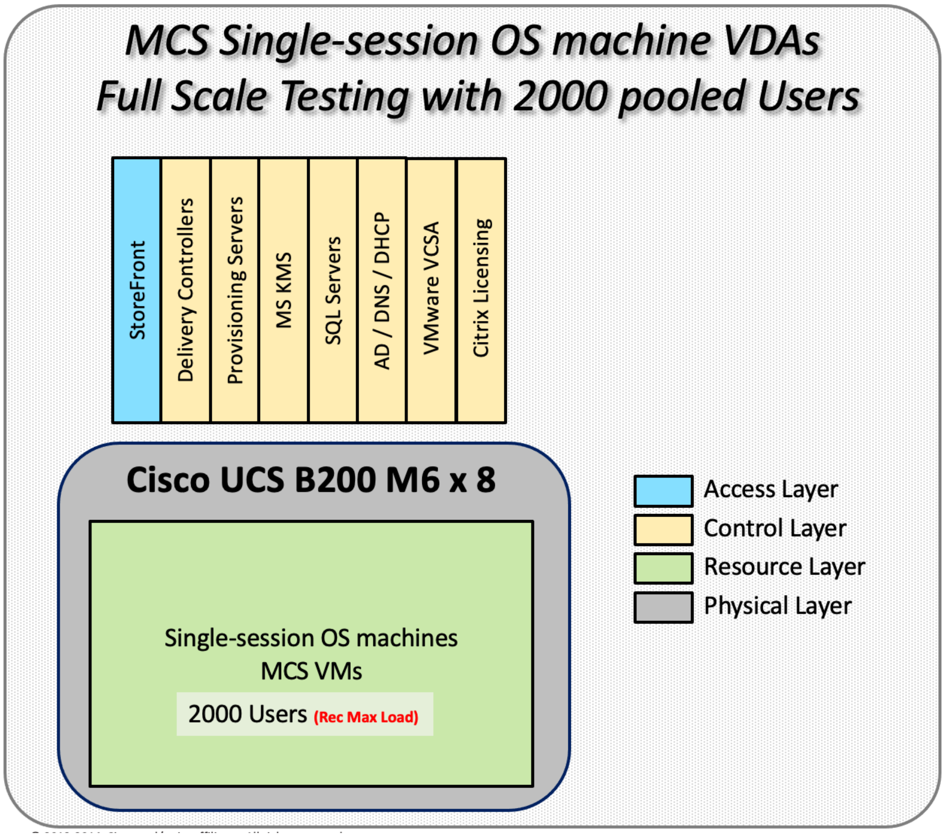
Figure 69. Full-Scale | 2000 non-persistent users | NP-VDI Hosts | Host Memory Utilization



Full-Scale Persistent Workload Testing with 2000 Users

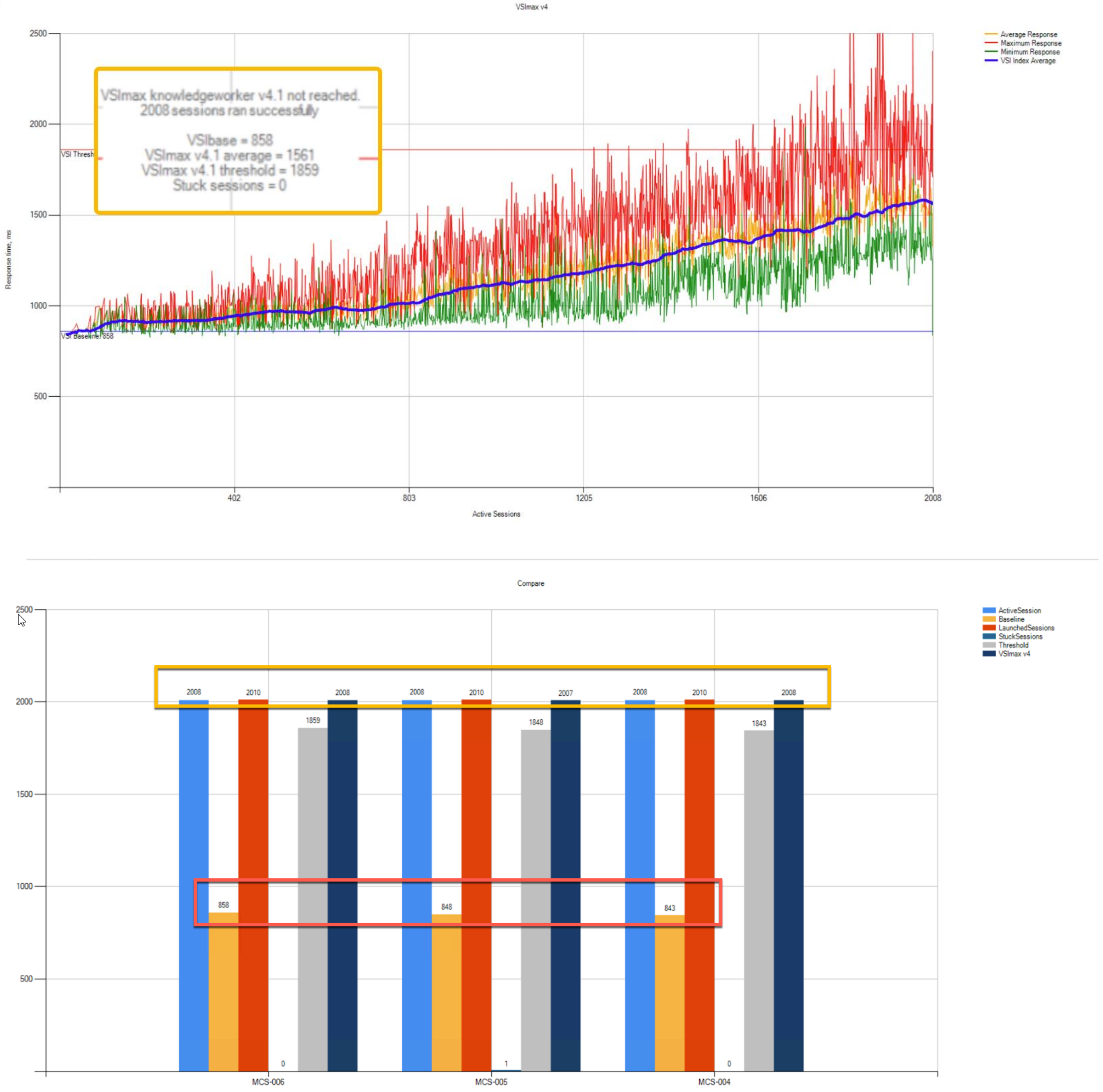
This section shows the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. The full-scale testing with 2000 users comprised of: 2000 Persistent Hosted Virtual Desktop using 8 compute nodes.

The combined mixed workload for the solution is 2000 users. To achieve the target, sessions were launched against all workload clusters concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.



The configured system efficiently and effectively delivered the following results.

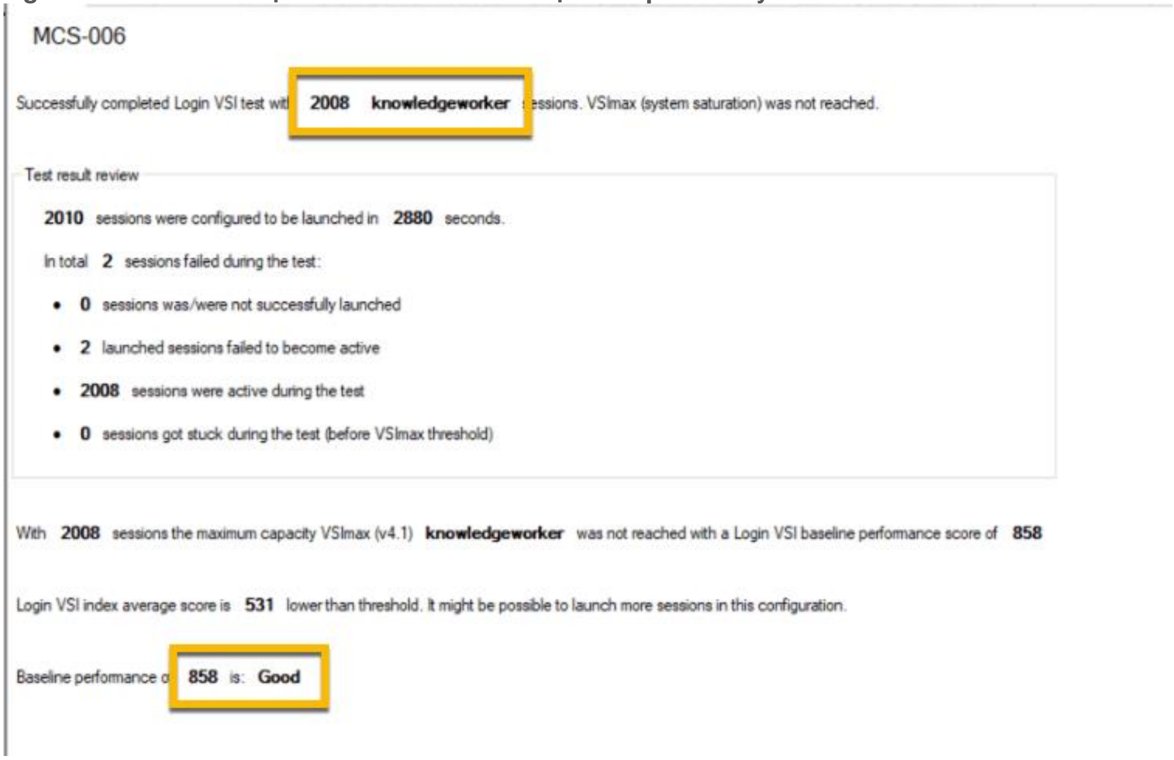
Figure 70. **Full-Scale | 2000 Persistent Users | VSI Score**



VSImax knowledgeworker v4.1 not reached.
2008 sessions ran successfully

VSIbase = 858
VSImax v4.1 average = 1561
VSImax v4.1 threshold = 1859
Stuck sessions = 0

Figure 71. Full-Scale | 2000 Persistent Users | VSI Repeatability



MCS-006

Successfully completed Login VSI test wit **2008 knowledgeworker** essions. VSImax (system saturation) was not reached.

Test result review

2010 sessions were configured to be launched in **2880** seconds.

In total **2** sessions failed during the test:

- **0** sessions was/were not successfully launched
- **2** launched sessions failed to become active
- **2008** sessions were active during the test
- **0** sessions got stuck during the test (before VSImax threshold)

With **2008** sessions the maximum capacity VSImax (v4.1) **knowledgeworker** was not reached with a Login VSI baseline performance score of **858**

Login VSI index average score is **531** lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance o **858** is: **Good**

Figure 72. Full-Scale | 2000 persistent users | P-VDI Hosts | Host CPU Utilization

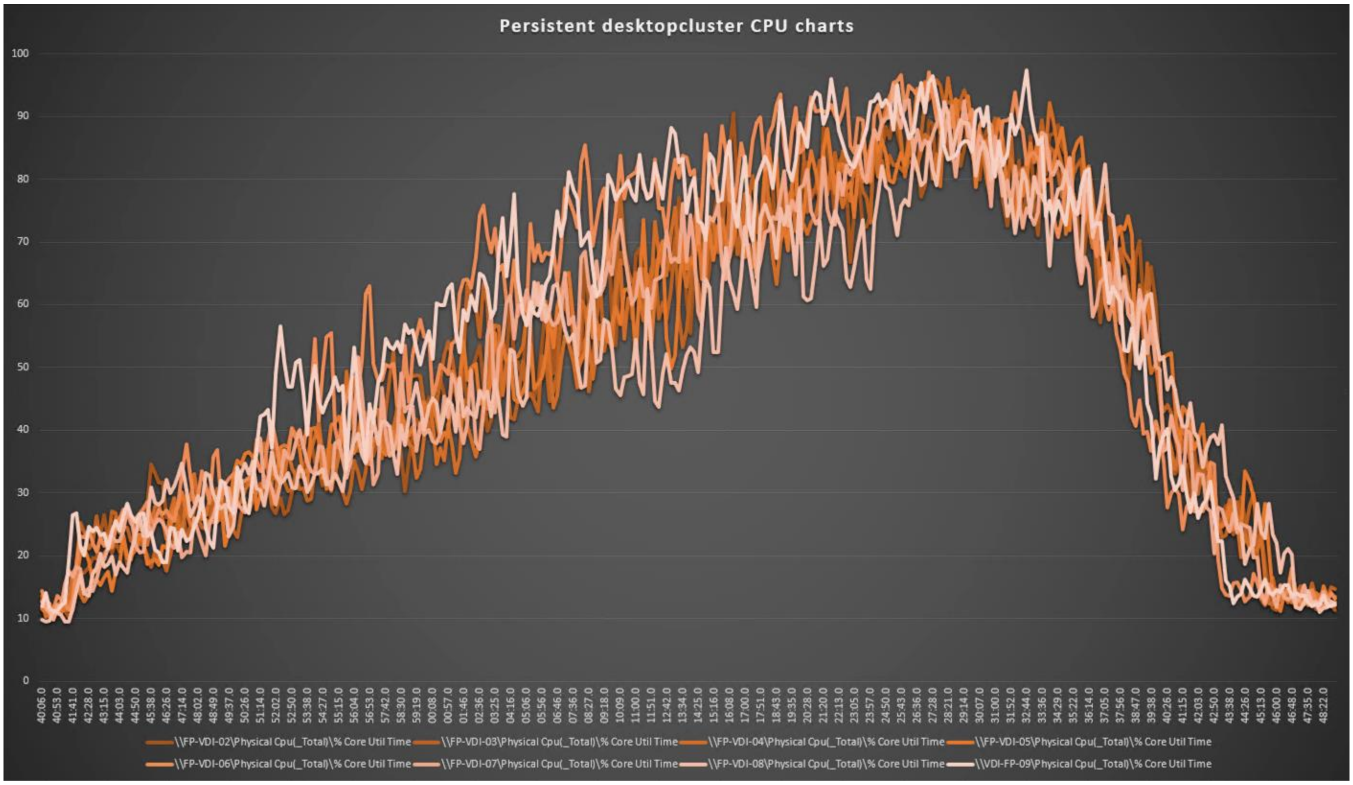
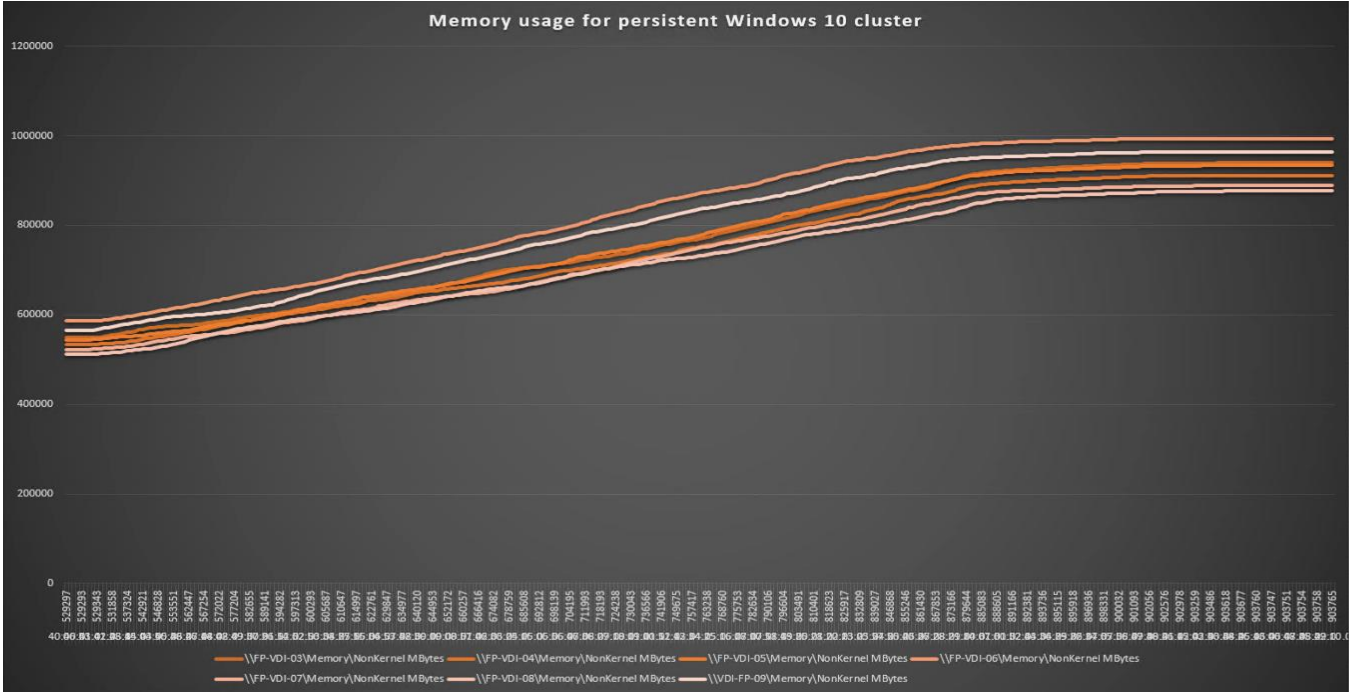


Figure 73. Full-Scale | 2000 persistent users | P-VDI Hosts | Host Memory Utilization



AFF A400 Storage Detailed Test Results for Cluster Scalability Test

This section provides analysis of the NetApp AFF A400 storage system performance results for each of the Citrix software module testing (HSD, PVS, Persistent), which we call cluster testing, and they are identified previously in this document. Specifically, it depicts and discusses the results for the following test case scenarios:

- 2400 Windows Server 2019 Citrix Hosted Shared desktops (RDS)
- 2000 Windows 10 x64 Citrix PVS Non-Persistent desktops
- 2000 Windows 10 x64 Citrix Persistent Full-Clone desktops

From a storage perspective, it is critical to maintain a latency of less than a millisecond for an optimal end-user experience no matter the IOPS and bandwidth being driven. The test results indicate that the AFF A400 storage delivers that essential minimum level of latency despite thousands of desktops hosted on the AFF A400 system.

The sections that follow show screenshots of the AFF A400 storage test data for all three use case scenarios with information about IOPS, bandwidth, and latency at the peak of each use case test. In all three use cases (cluster level testing with HSD PVS VDI, full clone persistent desktops and full-scale mixed workload sessions, the criteria followed prior to launching Login VSI workload test are the same.

2400 Users Citrix HSD (RDS) Windows 2019 Sessions

This test uses Login VSI for the workload generator in Benchmark mode with the Knowledge Worker user type and with Citrix Remote Desktop Service Hosted (RDSH) sessions for the VDI delivery mechanism. For this test, we used 4 volumes. This test uses Citrix Cache on RAM feature which takes a lot of stress off of the storage, so you can see low IOPS for all the volumes in the following figures.

Figure 74. **Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 1 for 2400 RDS**

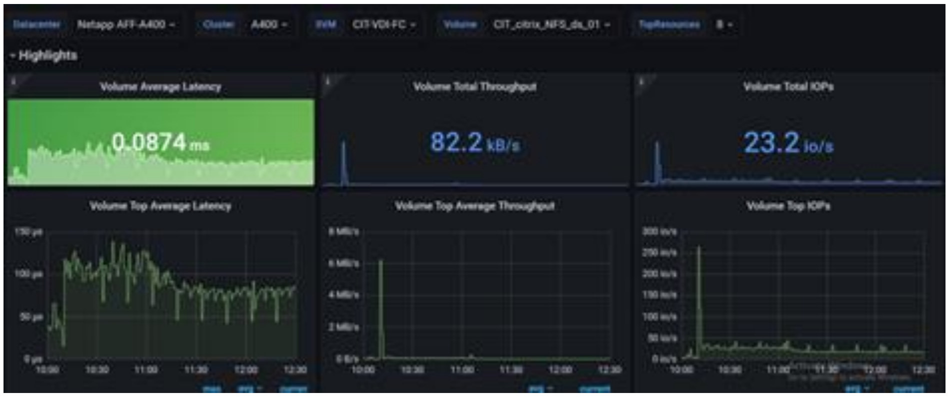


Figure 75. **Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 2 for 2400 RDS**

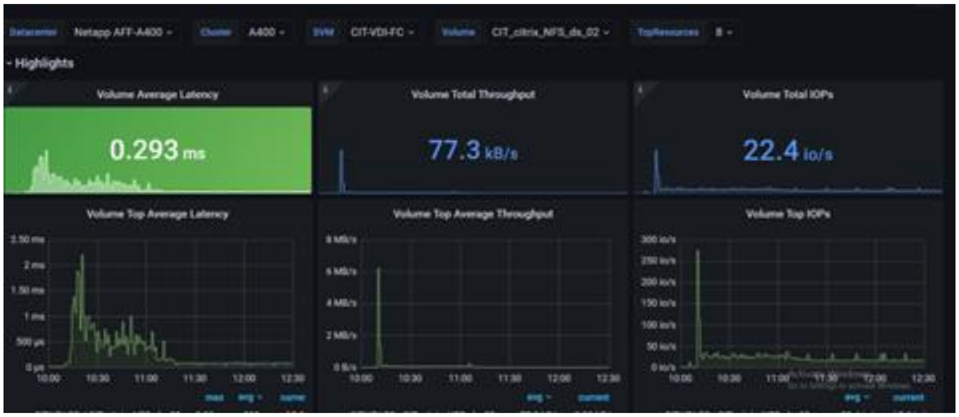
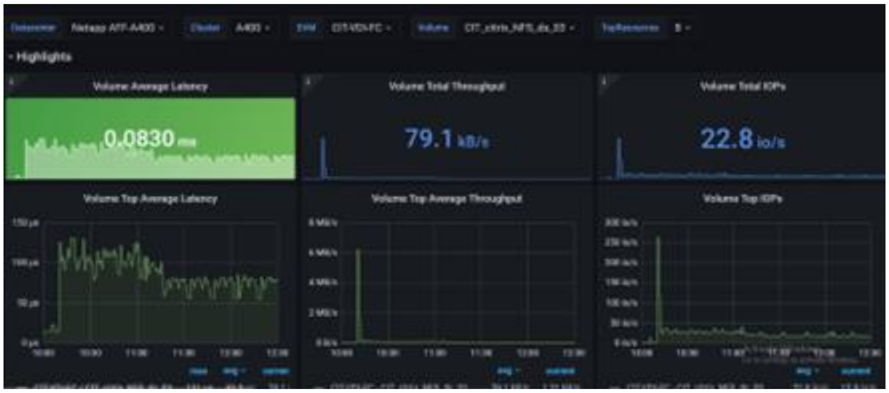
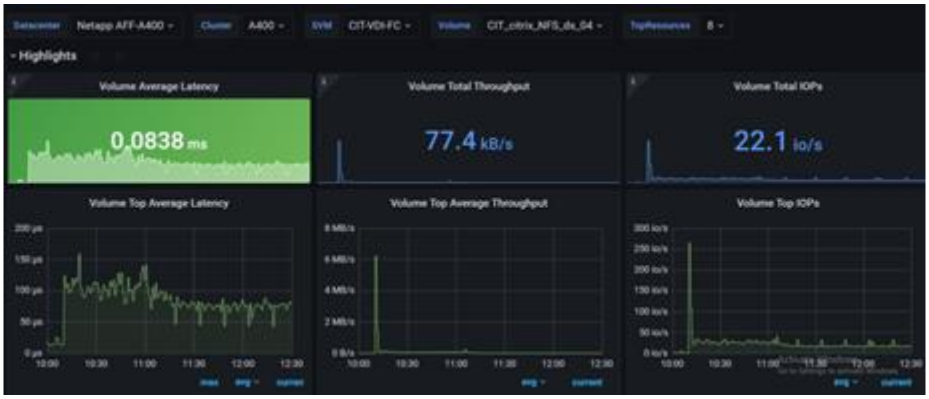


Figure 76. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 3 for 2400 RDS



Datacenter Netapp AFF-A400 Cluster A400 SVM CIT-VDI-FC Volume CIT_citrix_NFS_ds_03 TopResources 8

Figure 77. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 4 for 2400 RDS



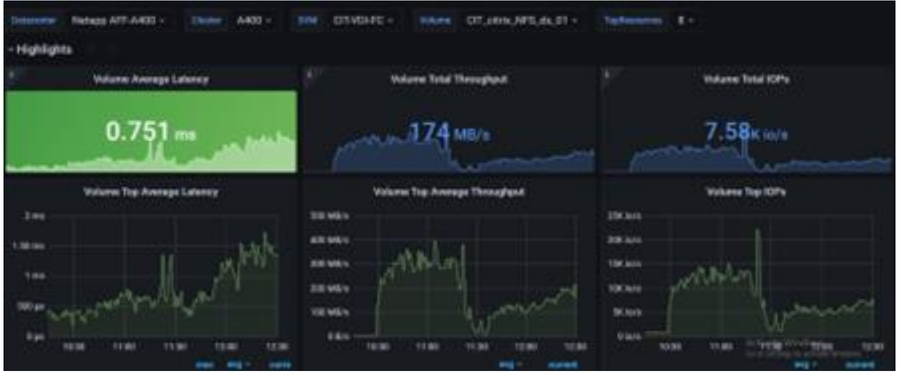
Datacenter Netapp AFF-A400 Cluster A400 SVM CIT-VDI-FC Volume CIT_citrix_NFS_ds_04 TopResources 8

2000 Users Persistent Desktops Cluster Test

NetApp AFF A400 Test Results for 2000 Persistent Windows 10 x64 Citrix MCS Desktops

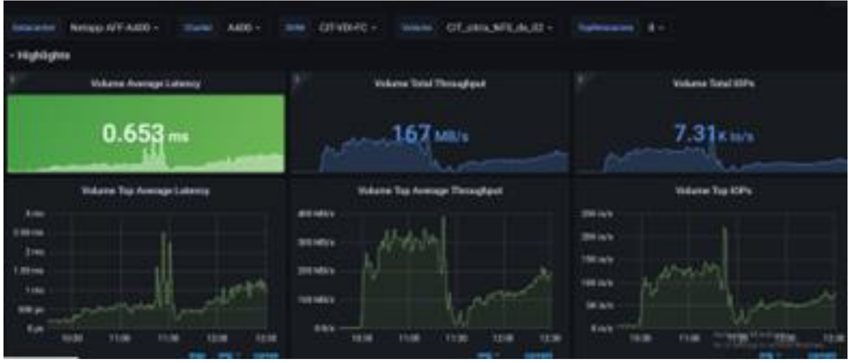
This section describes the key performance metrics that were captured on the NetApp Storage AFF A400 array during the testing with 2000 persistent desktops. For this test 4 volumes were used, and the average latency is below 1ms for all the volumes.

Figure 78. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 1 for 2000 persistent desktops



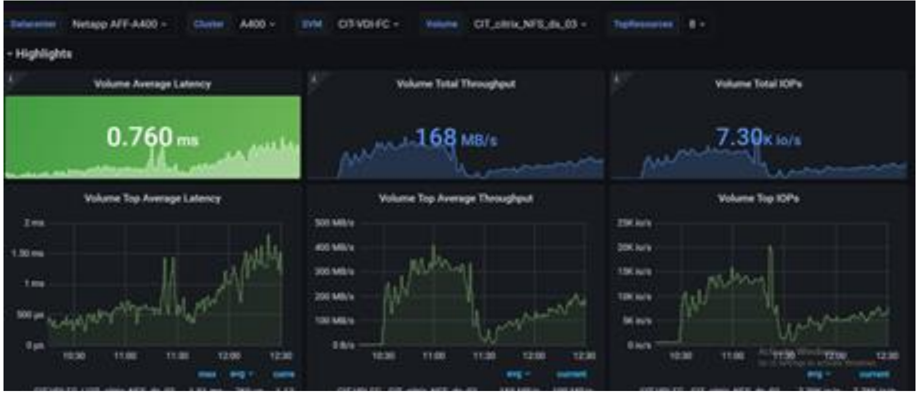
Datacenter Netapp AFF-A400 Cluster A400 SVM CIT-VDI-FC Volume CIT_citrix_NFS_ds_01 TopResources 8

Figure 79. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 2 for 2000 persistent desktops



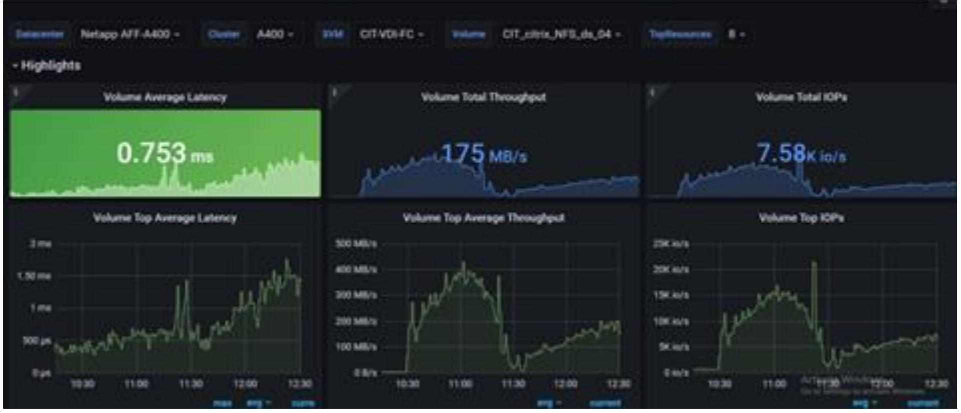
Datacenter Netapp AFF-A400 · Cluster A400 · SVM CIT-VDI-FC · Volume CIT_citrix_NFS_ds_02 · TopResources 8

Figure 80. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 3 for 2000 persistent desktops



Datacenter Netapp AFF-A400 · Cluster A400 · SVM CIT-VDI-FC · Volume CIT_citrix_NFS_ds_03 · TopResources 8

Figure 81. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 4 for 2000 persistent desktops



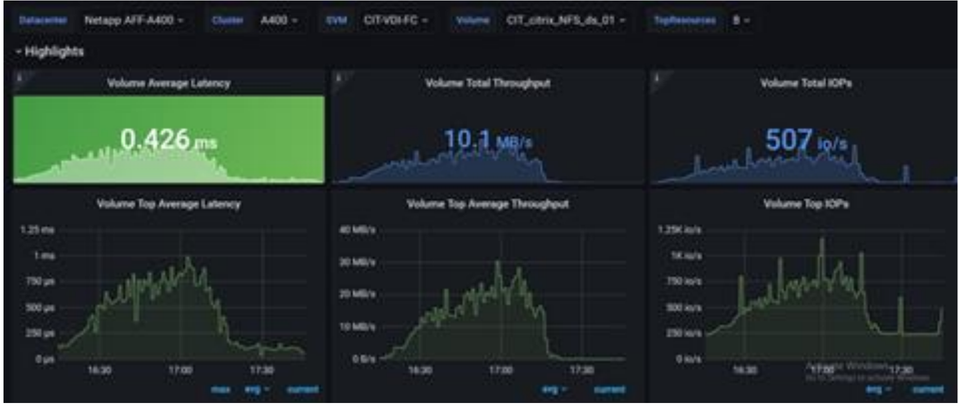
Datacenter Netapp AFF-A400 · Cluster A400 · SVM CIT-VDI-FC · Volume CIT_citrix_NFS_ds_04 · TopResources 8

2000 Users PVS Non-Persistent Desktops Cluster Test

NetApp AFF A400 Test Results for 2000 Non-Persistent Windows 10 x64 Citrix MCS Desktops

For this test, 4 volumes were used, and the average latency is way below 1ms for all the volumes and the latency was not higher than 1ms at any time.

Figure 82. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 1 for 2000 non persistent desktops



W

Figure 83. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 2 for 2000 non persistent desktops

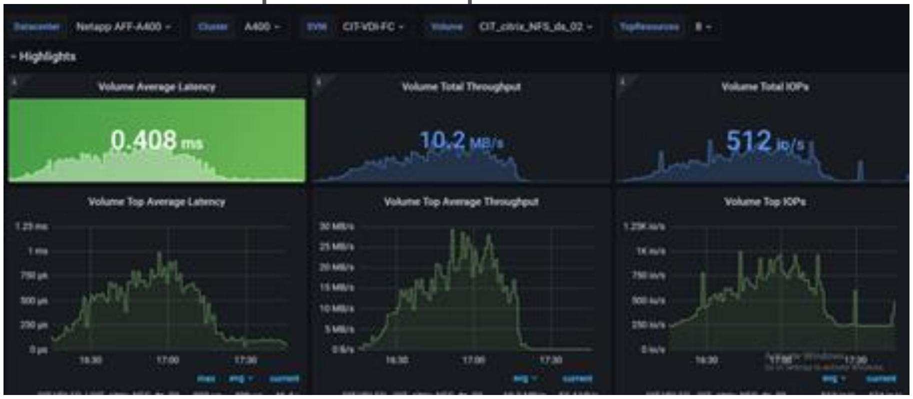


Figure 84. Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 3 for 2000 non persistent desktops

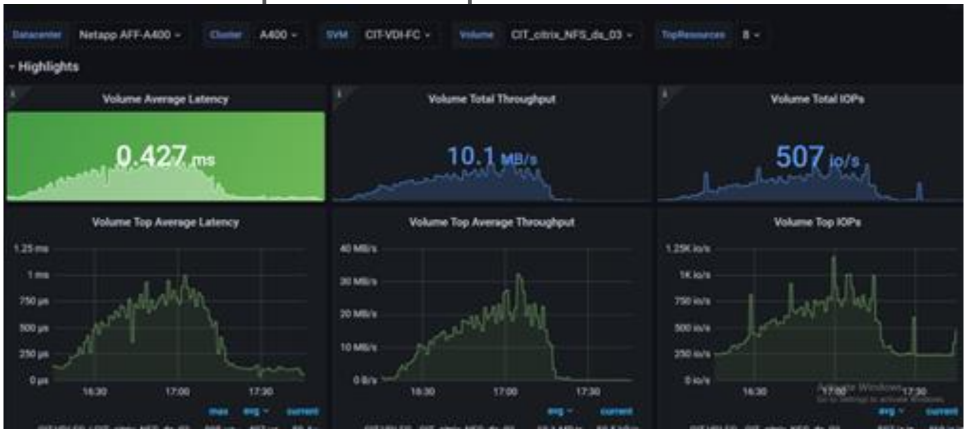
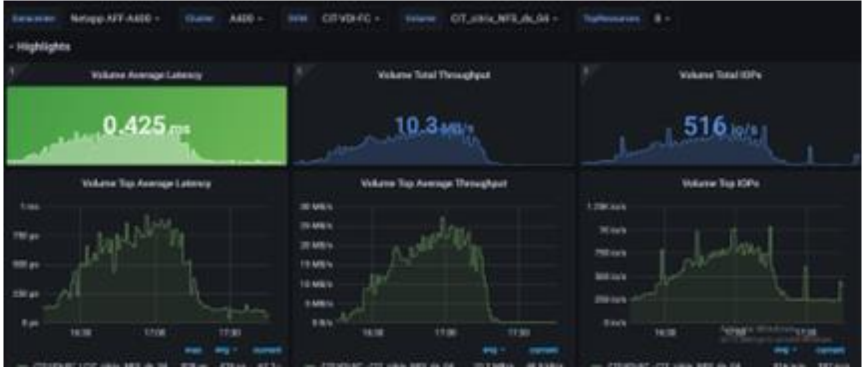


Figure 85. **Volume Average Latency, Volume Total Throughput and Volume Total IOPS AFF A400 volume 4 for 2000 non persistent desktops**



Scalability Considerations and Guidelines

There are many factors to consider when you begin to scale beyond 2500 Users, which this reference architecture has successfully tested. This 2500-seat solution provides a large-scale building block that can be replicated to confidently scale-out to tens of thousands of users.

Cisco UCS System Scalability

As our results indicate, we have proven linear scalability in the Cisco UCS Reference Architecture as tested:

- Cisco UCS domains consist of a pair of Fabric Interconnects and a pair of chassis that can easily be scaled out with VDI growth.
- With Intersight, you get all of the benefits of SaaS delivery and full lifecycle management of distributed Intersight-connected servers and third-party storage across data centers, remote sites, branch offices, and edge environments. This empowers you to analyze, update, fix, and automate your environment in ways that were not possible with prior generations' tools. As a result, your organization can achieve significant TCO savings and deliver applications faster in support of new business initiatives.
- As scale grows, the value of the combined Cisco UCS fabric and Cisco Nexus physical switches increases dramatically to define the Quality of Services required to deliver excellent end user experience 100 percent of the time.
- To accommodate the Cisco Nexus 9000 upstream connectivity in the way we describe in the network configuration section, two Ethernet uplinks are needed to be configured on the Cisco UCS 6454 Fabric Interconnect.

The backend storage has to be scaled accordingly, based on the IOP considerations as described in the NetApp scaling section. Please refer the NetApp section that follows this one for scalability guidelines.

NetApp FAS Storage Guidelines for Scale Desktop Virtualization Workloads

Storage sizing has three steps:

1. Gathering solution requirements
2. Estimating storage capacity and performance
3. Obtaining recommendations for the storage configuration

Solution Assessment

Assessment is an important first step. Liquidware Labs Stratusphere FIT, and Lakeside VDI Assessment are recommended to collect network, server, and storage requirements. NetApp has contracted with Liquidware Labs to provide free licenses to NetApp employees and channel partners. For information on how to obtain software and licenses, refer to this FAQ. Liquidware Labs also provides a storage template that fits the NetApp system performance modeler. For guidelines on how to use Stratusphere FIT and the NetApp custom report template, refer to TR-3902: Guidelines for Virtual Desktop Storage Profiling.

Virtual desktop sizing depends on the following:

- The number of the seats
- The VM workload (applications, VM size, and VM OS)
- The connection broker (Citrix Virtual Apps and Desktops)
- The hypervisor type (vSphere, Citrix Hypervisor, or Hyper-V)
- The provisioning method (NetApp clone, Linked clone, PVS, and MCS)
- Future storage growth
- Disaster recovery requirements
- User home directories

NetApp has developed a sizing tool called the System Performance Modeler (SPM) that simplifies the process of performance sizing for NetApp systems. It has a step-by-step wizard to support varied workload requirements and provides recommendations for meeting your performance needs.

Storage sizing has two factors: capacity and performance. NetApp recommends using the NetApp SPM tool to size the virtual desktop solution. To use this tool, contact NetApp partners and NetApp sales engineers who have the access to SPM. When using the NetApp SPM to size a solution, NetApp recommends separately sizing the VDI workload (including the write cache and personal vDisk if used), and the CIFS profile and home directory workload. When sizing CIFS, NetApp recommends sizing with a heavy user workload. Eighty percent concurrency was assumed in this solution.

Capacity Considerations

Deploying Citrix Virtual Apps and Desktops with PVS imposes the following capacity considerations:

- vDisk. The size of the vDisk depends on the OS and the number of applications installed. It is a best practice to create vDisks larger than necessary in order to leave room for any additional application installations or patches. Each organization should determine the space requirements for its vDisk images.
- As an example, a 20GB vDisk with a Windows 7 image is used. NetApp deduplication can be used for space savings.
- Write cache file. NetApp recommends a size range of 4 to 18GB for each user. Write cache size is based on what type of workload and how often the VM is rebooted. In this example, 4GB is used for the write-back cache. Since NFS is thin provisioned by default, only the space currently used by the VM will be consumed on the NetApp storage. If iSCSI or FCP is used, N x 4GB would be consumed as soon as a new virtual machine is created.
- PvDisk. Normally, 5 to 10GB is allocated, depending on the application and the size of the profile. Use 20 percent of the master image as a starting point. NetApp recommends running deduplication.

- CIFS home directory. Various factors must be considered for each home directory deployment. The key considerations for architecting and sizing a CIFS home directory solution include the number of users, the number of concurrent users, the space requirement for each user, and the network load. Run deduplication to obtain space savings.
- Infrastructure. Host Citrix Virtual Apps and Desktops, PVS, SQL Server, DNS, and DHCP.

The space calculation formula for a 2000-seat deployment is as follows: Number of vDisk x 20GB + 2000 x 4GB write cache + 2000 x 10GB PvDisk + 2000 x 5GB user home directory x 70% + 2000 x 1GB vSwap + 500GB infrastructure.

Performance Considerations

The collection of performance requirements is a critical step. After using Liquidware Labs Stratusphere FIT and Lakeside VDI Assessment to gather I/O requirements, contact the NetApp account team to obtain recommended software and hardware configurations.

Size, the read/write ratio, and random or sequential reads comprise the I/O considerations. We use 90 percent write and 10 percent read for PVS workload. Storage CPU utilization must also be considered. Table 26 can be used as guidance for your sizing calculations for a PVS workload when using a LoginVSI heavy workload.

Table 26. Typical IOPS without RamCache plus Overflow Feature

	Boot IOPS	Login IOPS	Steady IOPS
Write Cache (NFS)	8-10	9	7.5
vDisk (CIFS SMB 3)	0.5	0	0
Infrastructure (NFS)	2	1.5	0

Scalability of Citrix Virtual Apps and Desktops 7 LTSR Configuration

Citrix Virtual Apps and Desktops environments can scale to large numbers. When implementing Citrix Virtual Apps and Desktops, consider the following in scaling the number of hosted shared and hosted virtual desktops:

- Types of storage in your environment
- Types of desktops that will be deployed
- Data protection requirements
- For Citrix Provisioning Server pooled desktops, the write cache sizing and placement

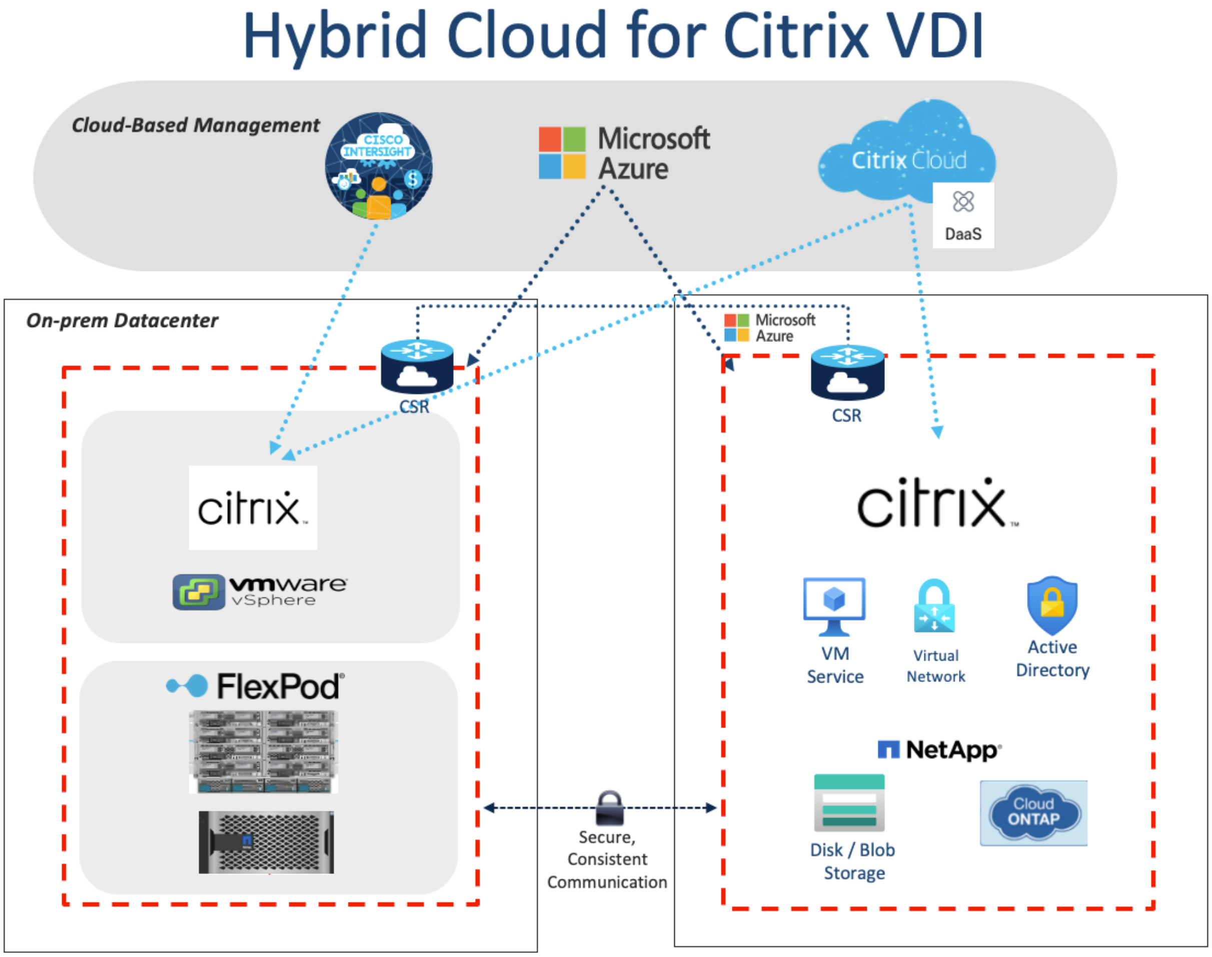
When designing and deploying this CVD environment Cisco and Citrix recommends using N+1 schema for virtualization host servers to accommodate resiliency. In all Reference Architectures (such as this CVD), this recommendation is applied to all host servers.

Hybrid Cloud Disaster Recovery Testing and Results

Cloud computing has clearly been one of the most disruptive IT trends of recent times. With the undeniable benefits of cloud computing, many enterprises are now moving aggressively towards a cloud first strategy. While the benefits of public cloud have been proven for certain workloads and use cases, there is growing acknowledgement of its trade-offs in areas such as availability, performance, customization, and security. To overcome these public cloud challenges, organizations are adopting hybrid cloud models that offer enterprises a more cohesive approach to adopt cloud computing. A hybrid cloud model gives organizations the flexibility to leverage the right blend of public and private cloud services, while addressing the availability, performance, and security challenges

FlexPod Datacenter for Hybrid Cloud delivers a validated FlexPod infrastructure design that allows customers to utilize resources in the public cloud based on the organization workload deployment policies or when the workload demand exceeds the available resources in the Datacenter. The VDI FlexPod Datacenter for Hybrid Cloud showcases:

- Citrix Virtual Apps and Desktops in the Citrix Cloud
- Data Replication and backup with NetApp Cloud Ontap
- VDI redundancy using virtual machines in Microsoft Azure

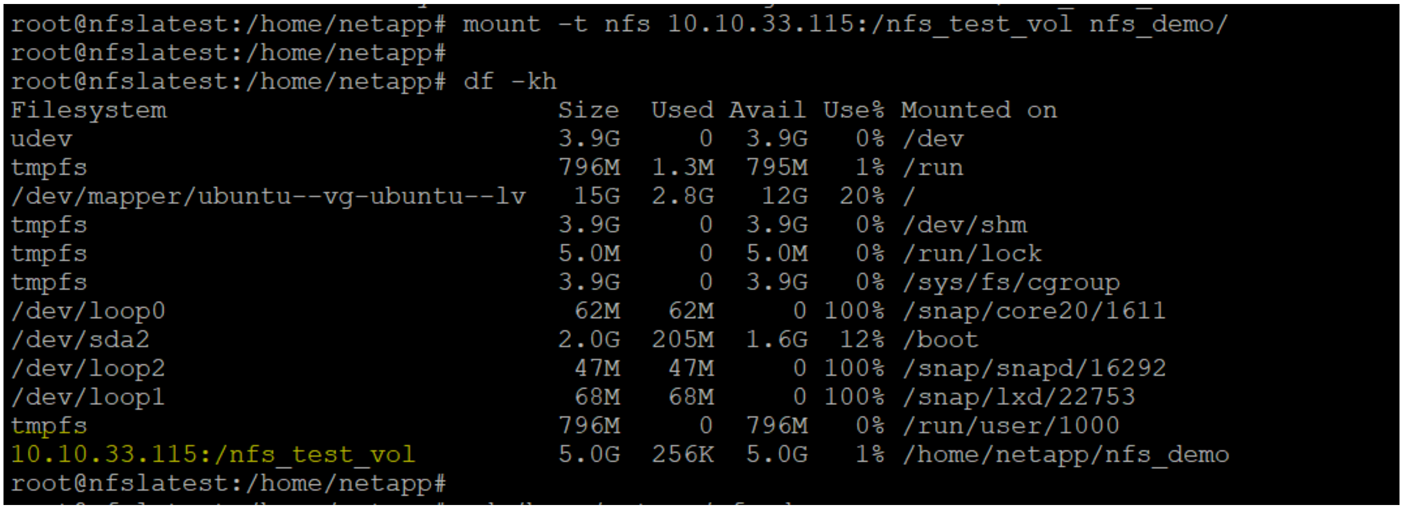


In this disaster recovery solution, Citrix Cloud was used for the VDI components. NetApp Cloud Manager and Volumes were used to protect the on-premise data and virtual machines. Finally, Microsoft Azure was used to ensure the infrastructure capabilities in the cloud, such as Active Directory, SQL, DNS, and Virtual Machines. For detailed steps to configure the FlexPod for Hybrid Cloud, follow the steps in this CVD: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_hybridcloud_design.html

Note: In this solution, disaster recovery was implemented and tested. To perform the validation of a successful DR scenario, first move data from a volume in ONTAP that is part of FlexPod to Cloud Volumes ONTAP using SnapMirror. Then you can access the data from the Microsoft Azure cloud compute instance followed by a data integrity check.

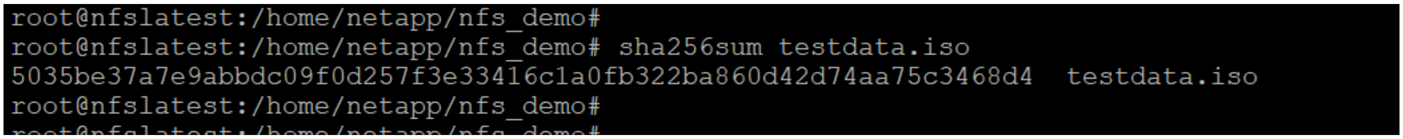
Procedure 1. Verify the success criteria of this solution

Step 1. Create a NFS mount on On-prem linux machine and add a sample dataset in the mount directory.



```
root@nfslatest:/home/netapp# mount -t nfs 10.10.33.115:/nfs_test_vol nfs_demo/
root@nfslatest:/home/netapp#
root@nfslatest:/home/netapp# df -kh
Filesystem                          Size  Used Avail Use% Mounted on
udev                                3.9G     0  3.9G   0% /dev
tmpfs                               796M  1.3M  795M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv    15G  2.8G   12G  20% /
tmpfs                               3.9G     0  3.9G   0% /dev/shm
tmpfs                               5.0M     0  5.0M   0% /run/lock
tmpfs                               3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/loop0                           62M   62M     0 100% /snap/core20/1611
/dev/sda2                           2.0G  205M  1.6G  12% /boot
/dev/loop2                           47M   47M     0 100% /snap/snapd/16292
/dev/loop1                           68M   68M     0 100% /snap/lxd/22753
tmpfs                               796M     0  796M   0% /run/user/1000
10.10.33.115:/nfs_test_vol          5.0G  256K  5.0G   1% /home/netapp/nfs_demo
root@nfslatest:/home/netapp#
```

Step 2. Generate an SHA256 checksum on the sample dataset that is present in an ONTAP volume in FlexPod.

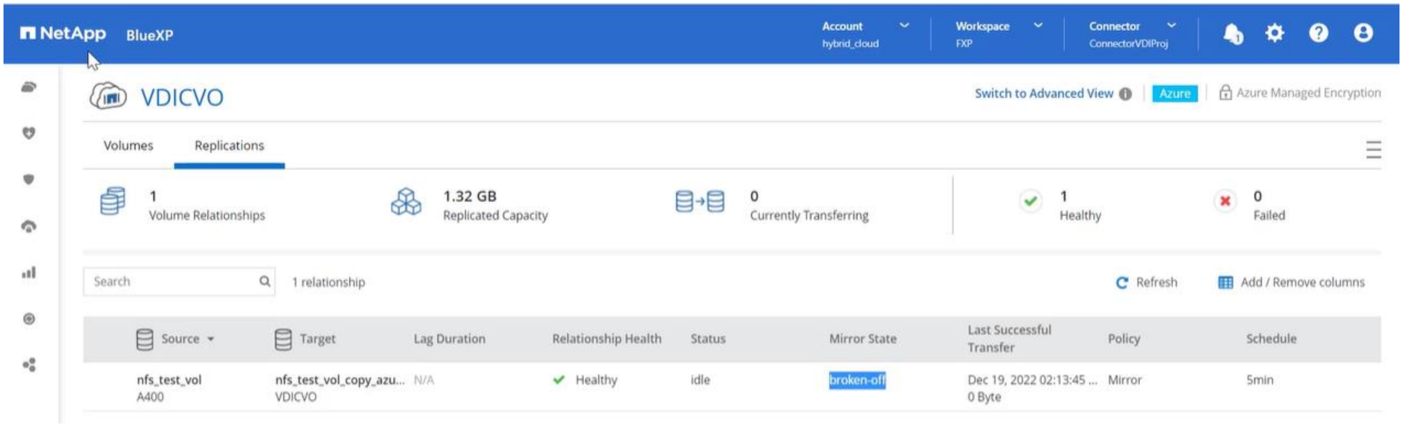


```
root@nfslatest:/home/netapp/nfs_demo#
root@nfslatest:/home/netapp/nfs_demo# sha256sum testdata.iso
5035be37a7e9abbdc09f0d257f3e33416c1a0fb322ba860d42d74aa75c3468d4  testdata.iso
root@nfslatest:/home/netapp/nfs_demo#
```

Step 3. Set up a volume SnapMirror relationship between ONTAP in FlexPod and Cloud Volumes ONTAP.

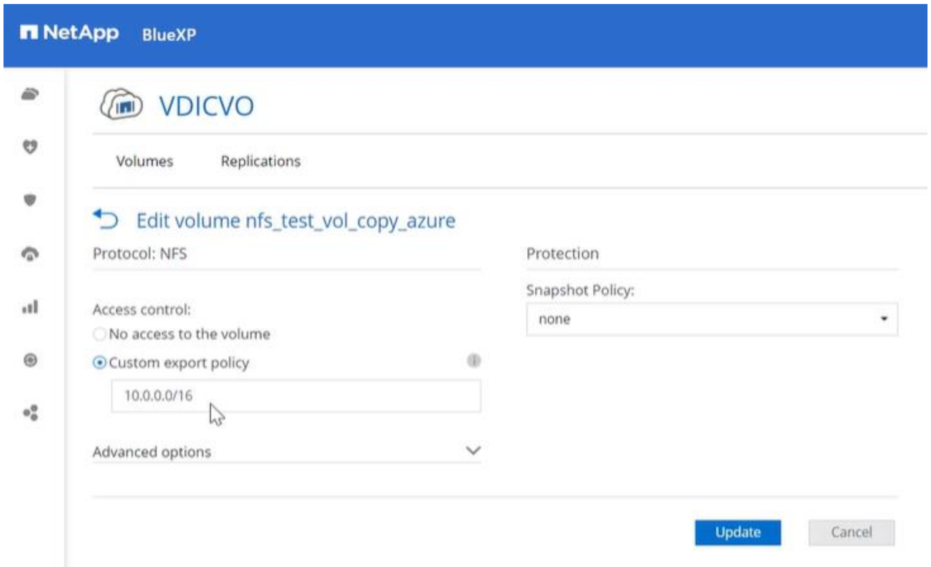
Step 4. Replicate the sample dataset from FlexPod to Cloud Volumes ONTAP.

Step 5. Break the SnapMirror relationship and promote the volume in Cloud Volumes ONTAP to production.



Source	Target	Lag Duration	Relationship Health	Status	Mirror State	Last Successful Transfer	Policy	Schedule
nfs_test_vol A400	nfs_test_vol_copy_azu... VDICVO	N/A	✓ Healthy	idle	broken-off	Dec 19, 2022 02:13:45 ... 0 Byte	Mirror	5min

Step 6. Edit the Cloud volume ONTAP volume and modify the custom export policy.



Edit volume nfs_test_vol_copy_azure

Protocol: NFS

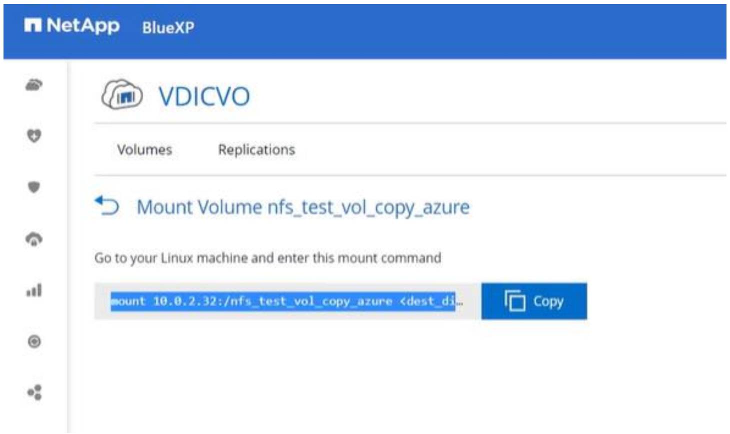
Access control:
○ No access to the volume
● Custom export policy
10.0.0.0/16

Advanced options

Protection

Snapshot Policy: none

Step 7. Copy the mount command.

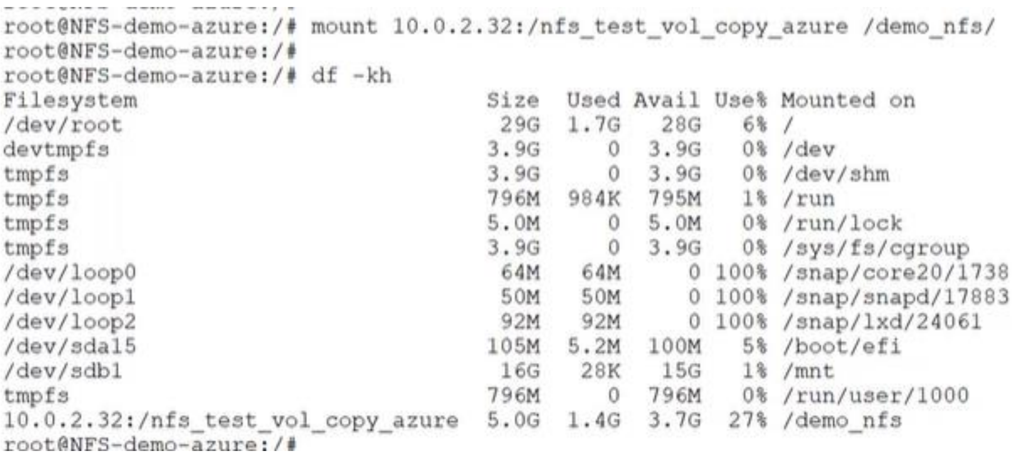


Mount Volume nfs_test_vol_copy_azure

Go to your Linux machine and enter this mount command

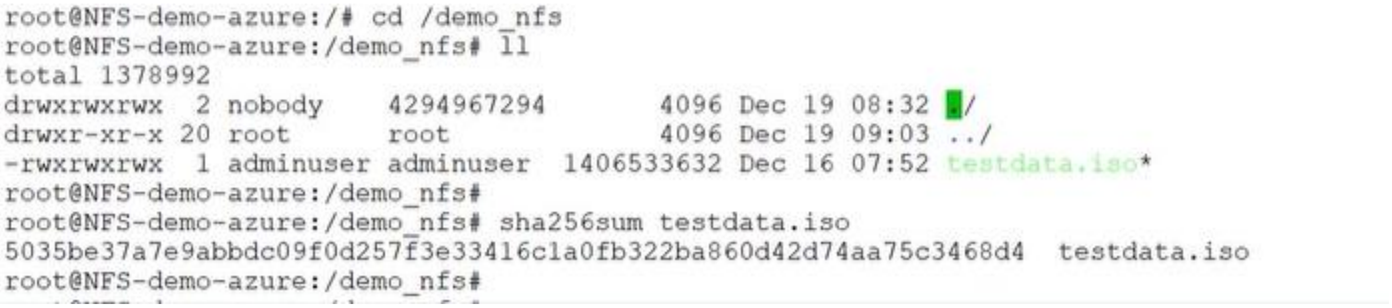
```
mount 10.0.2.32:/nfs_test_vol_copy_azure <dest_di…
```

Step 8. Map the Cloud Volumes ONTAP volume with the dataset to a compute instance in Microsoft Azure.



```
root@NFS-demo-azure:/# mount 10.0.2.32:/nfs_test_vol_copy_azure /demo_nfs/
root@NFS-demo-azure:/#
root@NFS-demo-azure:/# df -kh
Filesystem                          Size  Used Avail Use% Mounted on
/dev/root                            29G  1.7G   28G   6% /
devtmpfs                            3.9G     0  3.9G   0% /dev
tmpfs                               3.9G     0  3.9G   0% /dev/shm
tmpfs                               796M  984K  795M   1% /run
tmpfs                               5.0M     0  5.0M   0% /run/lock
tmpfs                               3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/loop0                           64M   64M     0 100% /snap/core20/1738
/dev/loop1                           50M   50M     0 100% /snap/snapd/17883
/dev/loop2                           92M   92M     0 100% /snap/lxd/24061
/dev/sda15                          105M  5.2M  100M   5% /boot/efi
/dev/sdb1                            16G   28K   15G   1% /mnt
tmpfs                               796M     0  796M   0% /run/user/1000
10.0.2.32:/nfs_test_vol_copy_azure  5.0G  1.4G  3.7G  27% /demo_nfs
root@NFS-demo-azure:/#
```

Step 9. Generate an SHA256 checksum on the sample dataset in Cloud Volumes ONTAP.



```
root@NFS-demo-azure:/# cd /demo_nfs
root@NFS-demo-azure:/demo_nfs# ll
total 1378992
drwxrwxrwx  2 nobody    4294967294       4096 Dec 19 08:32 ./
drwxr-xr-x 20 root      root             4096 Dec 19 09:03 ../
-rwxrwxrwx  1 adminuser adminuser  1406533632 Dec 16 07:52 testdata.iso*
root@NFS-demo-azure:/demo_nfs#
root@NFS-demo-azure:/demo_nfs# sha256sum testdata.iso
5035be37a7e9abbdc09f0d257f3e33416c1a0fb322ba860d42d74aa75c3468d4  testdata.iso
root@NFS-demo-azure:/demo_nfs#
```

Step 10. Compare the checksum on the source and destination; presumably, the checksums on both sides match.

Cisco Intersight

The entire Cisco solution for VDI on FlexPod was deployed and managed on Cisco Intersight. All policies and profiles were deployed using tried and true best practices for VDI on Cisco UCS systems.

Citrix Cloud

Citrix Cloud is a platform that hosts and administers Citrix cloud services. It connects to your resources through connectors on any cloud or infrastructure you choose (on-premises, public cloud, private cloud, or hybrid cloud). It allows you to create, manage, and deploy workspaces with apps and data to your end-users from a single console.

To learn more about key service components in Citrix Cloud, see the following resources:

- Citrix Workspace conceptual diagram: Provides an overview of key areas such as identity, workspace intelligence, and single sign-on.
- Reference Architectures: Provides comprehensive guides for planning your Citrix Workspace implementation, including use cases, recommendations, and related resources.
- Citrix DaaS reference architectures: Provides in-depth guidance for deploying Citrix DaaS (formerly Virtual Apps and Desktops service) with related services.

With this test, the Citrix Cloud was configured to run on-premise virtual desktops for user access. For more information, see https://docs.citrix.com/en-us/tech-zone/learn/poc-guides/cvads.html

For the users to have desktops available in the event of an on-premise failure, the Citrix desktops were configured in the Microsoft Azure tenant, to copy the user data and virtual machines using Ontap. For more information, see https://docs.citrix.com/en-us/citrix-daas-azure.html

Microsoft Azure and Citrix Cloud

Procedure 1. Solution Steps

Step 1. Configure Azure Active Directory to enable directory services are consistent.

Step 2. Create Public IP for the CSR/VPN gateway.

Step 3. Configure on-prem subnets in the Azure Local Network Gateway.

Step 4. Configure subnets for Azure resource use to create the Virtual Network Gateway and creating Azure based subnets.

Step 5. Create a site to site VPN with Cisco CSR to connect the on-premise resources with Azure resources.

Step 6. Test two way connectivity between on-prem subnets and Azure subnets.

Step 7. Build virtual machines in Azure with software and Citrix image.

Step 8. In Citrix Cloud create hosting connection and catalog to Microsoft Azure.

Step 9. Add on-prem and cloud VMs to a single desktop delivery group

For more information, see https://docs.citrix.com/en-us/citrix-daas-azure/catalogs-create.html#creating-catalogs-of-azure-ad-domain-joined-machines

When the on-premise desktops are no longer available, the Microsoft Azure-based desktops will power on and register with the delivery group. You will be able to access their corporate desktops while their data and files are being replicated using NetApp's Cloud technology previously described.

Summary

FlexPod delivers a platform for enterprise end user computing deployments and cloud data centers using Cisco UCS blade and rack servers, Cisco fabric interconnects, Cisco Nexus 9000 switches, Cisco MDS 9100 fibre channel switches and NetApp Storage AFF A400 Storage Array. FlexPod is designed and validated using compute, network and storage best practices and high availability to reduce deployment time, project risk and IT costs while maintaining scalability and flexibility for addressing a multitude of IT initiatives. This CVD validates the design, performance, management, scalability, and resilience that FlexPod provides to customers wanting to deploy enterprise-class VDI.

About the Authors

Jeff Nichols—Leader, Technical Marketing, CSPG UCS Solutions - US, Cisco Systems, Inc.

Jeff Nichols is a member of the Cisco Computing Systems Product Group team focusing on design, testing, solutions validation, technical content creation, and performance testing/benchmarking. He has years of experience in Virtual Desktop Infrastructure (VDI), Server and Desktop Virtualization using Microsoft and VMware products.

Jeff is a subject matter expert on desktop and server virtualization, Cisco HyperFlex, Cisco Unified Computing System, Cisco Nexus Switching, and NVIDIA/AMD Graphics.

Ruchika Lahoti—Technical Marketing Engineer, NetApp
Ruchika has more than five years of experience in the IT industry. She focuses on FlexPod hybrid cloud infrastructure solution design, implementation, validation, automation. Ruchika earned a bachelor's degree in Computer Science.

Acknowledgements

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

- Bobby Oommen–Manager, Technical Marketing, NetApp

References

This section provides links to additional information for each partner's solution component of this document.

Cisco UCS B200 M6 Servers

- https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200m6-specsheet.pdf
- https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/blade-servers/B200M6/B200M5_preface_0100.html
- https://www.intel.com/content/dam/www/central-libraries/us/en/documents/c45-2372313-00-cisco-ucs-b200-m6-blade-server-aag-v1c.pdf

Cisco Intersight Configuration Guides

- https://www.cisco.com/c/en/us/support/servers-unified-computing/intersight/products-installation-guides-list.html
- https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide.html
- https://intersight.com/help/saas/supported_systems#supported_hardware_for_intersight_managed_mode

Cisco Nexus Switching References

- http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
- http://www.cisco.com/c/en/us/products/switches/nexus-93180YC-FX -switch/index.html

Cisco MDS 9000 Service Switch References

- http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html
- http://www.cisco.com/c/en/us/products/storage-networking/product-listing.html
- http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/datasheet-listing.html

Citrix References

- https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/7-ltsr.html
- https://docs.citrix.com/en-us/provisioning/7-ltsr.html
- https://support.citrix.com/article/CTX216252?recommended
- https://support.citrix.com/article/CTX224676
- https://support.citrix.com/article/CTX117374
- https://support.citrix.com/article/CTX202400
- https://support.citrix.com/article/CTX210488

FlexPod

- https://www.flexpod.com

- https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html

VMware References

- https://docs.vmware.com/en/VMware-vSphere/index.html
- https://labs.vmware.com/flings/vmware-os-optimization-tool
- https://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-6CAFE558-A0AB-4894-A0F4-97CF556784A9.html

Microsoft References

- https://technet.microsoft.com/en-us/library/hh831620(v=ws.11).aspx
- https://technet.microsoft.com/en-us/library/dn281793(v=ws.11).aspx
- https://support.microsoft.com/en-us/kb/2833839
- https://technet.microsoft.com/en-us/library/hh831447(v=ws.11).aspx

Login VSI Documentation

- https://www.loginvsi.com/documentation/Main_Page
- https://www.loginvsi.com/documentation/Start_your_first_test

NetApp Reference Documents

- http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx
- http://www.netapp.com/us/products/data-management-software/ontap.aspx
- https://mysupport.netapp.com/documentation/docweb/index.html?productID=62379&language=en-US
- http://www.netapp.com/us/products/management-software/
- http://www.netapp.com/us/products/management-software/vsc/

Appendices

The appendices are as follows:

Appendix A Glossary of Acronyms

Appendix B Glossary of Terms

Appendix A—Glossary of Acronyms

AAA–Authentication, Authorization, and Accounting

ACP–Access-Control Policy

ACI–Cisco Application Centric Infrastructure

ACK–Acknowledge or Acknowledgement

ACL–Access-Control List

AD–Microsoft Active Directory

AFI–Address Family Identifier

AMP–Cisco Advanced Malware Protection

AP–Access Point

API–Application Programming Interface

APIC– Cisco Application Policy Infrastructure Controller (ACI)

ASA–Cisco Adaptative Security Appliance

ASM–Any-Source Multicast (PIM)

ASR–Aggregation Services Router

Auto-RP–Cisco Automatic Rendezvous Point protocol (multicast)

AVC–Application Visibility and Control

BFD–Bidirectional Forwarding Detection

BGP–Border Gateway Protocol

BMS–Building Management System

BSR–Bootstrap Router (multicast)

BYOD–Bring Your Own Device

CAPWAP–Control and Provisioning of Wireless Access Points Protocol

CDP–Cisco Discovery Protocol

CEF–Cisco Express Forwarding

CMD–Cisco Meta Data

CPU–Central Processing Unit

CSR–Cloud Services Routers

CTA–Cognitive Threat Analytics

CUWN–Cisco Unified Wireless Network

CVD–Cisco Validated Design

CYOD–Choose Your Own Device

DC–Data Center

DHCP–Dynamic Host Configuration Protocol

DM–Dense-Mode (multicast)

DMVPN–Dynamic Multipoint Virtual Private Network

DMZ–Demilitarized Zone (firewall/networking construct)

DNA–Cisco Digital Network Architecture

DNS–Domain Name System

DORA–Discover, Offer, Request, ACK (DHCP Process)

DWDM–Dense Wavelength Division Multiplexing

ECMP–Equal Cost Multi Path

EID–Endpoint Identifier

EIGRP–Enhanced Interior Gateway Routing Protocol

EMI–Electromagnetic Interference

ETR–Egress Tunnel Router (LISP)

EVPN–Ethernet Virtual Private Network (BGP EVPN with VXLAN data plane)

FHR–First-Hop Router (multicast)

FHRP–First-Hop Redundancy Protocol

FMC–Cisco Firepower Management Center

FTD–Cisco Firepower Threat Defense

GBAC–Group-Based Access Control

GbE–Gigabit Ethernet

Gbit/s–Gigabits Per Second (interface/port speed reference)

GRE–Generic Routing Encapsulation

GRT–Global Routing Table

HA–High-Availability

HQ–Headquarters

HSRP–Cisco Hot-Standby Routing Protocol

HTDB–Host-tracking Database (SD-Access control plane node construct)

IBNS–Identity-Based Networking Services (IBNS 2.0 is the current version)

ICMP– Internet Control Message Protocol

IDF–Intermediate Distribution Frame; essentially a wiring closet.

IEEE–Institute of Electrical and Electronics Engineers

IETF–Internet Engineering Task Force

IGP–Interior Gateway Protocol

IID–Instance-ID (LISP)

IOE–Internet of Everything

IoT–Internet of Things

IP–Internet Protocol

IPAM–IP Address Management

IPS–Intrusion Prevention System

IPSec–Internet Protocol Security

ISE–Cisco Identity Services Engine

ISR–Integrated Services Router

IS-IS–Intermediate System to Intermediate System routing protocol

ITR–Ingress Tunnel Router (LISP)

LACP–Link Aggregation Control Protocol

LAG–Link Aggregation Group

LAN–Local Area Network

L2 VNI–Layer 2 Virtual Network Identifier; as used in SD-Access Fabric, a VLAN.

L3 VNI– Layer 3 Virtual Network Identifier; as used in SD-Access Fabric, a VRF.

LHR–Last-Hop Router (multicast)

LISP–Location Identifier Separation Protocol

MAC–Media Access Control Address (OSI Layer 2 Address)

MAN–Metro Area Network

MEC–Multichassis EtherChannel, sometimes referenced as ***MCEC***

MDF–Main Distribution Frame; essentially the central wiring point of the network.

MnT–Monitoring and Troubleshooting Node (Cisco ISE persona)

MOH–Music on Hold

MPLS–Multiprotocol Label Switching

MR–Map-resolver (LISP)

MS–Map-server (LISP)

MSDP–Multicast Source Discovery Protocol (multicast)

MTU–Maximum Transmission Unit

NAC–Network Access Control

NAD–Network Access Device

NAT–Network Address Translation

NBAR–Cisco Network-Based Application Recognition (NBAR2 is the current version).

NFV–Network Functions Virtualization

NSF–Non-Stop Forwarding

OSI–Open Systems Interconnection model

OSPF–Open Shortest Path First routing protocol

OT–Operational Technology

PAgP–Port Aggregation Protocol

PAN–Primary Administration Node (Cisco ISE persona)

PCI DSS–Payment Card Industry Data Security Standard

PD–Powered Devices (PoE)

PETR–Proxy-Egress Tunnel Router (LISP)

PIM–Protocol-Independent Multicast

PITR–Proxy-Ingress Tunnel Router (LISP)

PnP–Plug-n-Play

PoE–Power over Ethernet (Generic term, may also refer to IEEE 802.3af, 15.4W at PSE)

PoE+–Power over Ethernet Plus (IEEE 802.3at, 30W at PSE)

PSE–Power Sourcing Equipment (PoE)

PSN–Policy Service Node (Cisco ISE persona)

pxGrid–Platform Exchange Grid (Cisco ISE persona and publisher/subscriber service)

PxTR–Proxy-Tunnel Router (LISP - device operating as both a PETR and PITR)

QoS–Quality of Service

RADIUS–Remote Authentication Dial-In User Service

REST–Representational State Transfer

RFC–Request for Comments Document (IETF)

RIB–Routing Information Base

RLOC–Routing Locator (LISP)

RP–Rendezvous Point (multicast)

RP–Redundancy Port (WLC)

RP–Route Processer

RPF–Reverse Path Forwarding

RR–Route Reflector (BGP)

RTT–Round-Trip Time

SA–Source Active (multicast)

SAFI–Subsequent Address Family Identifiers (BGP)

SD–Software-Defined

SDA–Cisco Software Defined-Access

SDN–Software-Defined Networking

SFP–Small Form-Factor Pluggable (1 GbE transceiver)

SFP+– Small Form-Factor Pluggable (10 GbE transceiver)

SGACL–Security-Group ACL

SGT–Scalable Group Tag, sometimes reference as Security Group Tag

SM–Spare-mode (multicast)

SNMP–Simple Network Management Protocol

SSID–Service Set Identifier (wireless)

SSM–Source-Specific Multicast (PIM)

SSO–Stateful Switchover

STP–Spanning-tree protocol

SVI–Switched Virtual Interface

SVL–Cisco StackWise Virtual

SWIM–Software Image Management

SXP–Scalable Group Tag Exchange Protocol

Syslog–System Logging Protocol

TACACS+–Terminal Access Controller Access-Control System Plus

TCP–Transmission Control Protocol (OSI Layer 4)

UCS– Cisco Unified Computing System

UDP–User Datagram Protocol (OSI Layer 4)

UPoE–Cisco Universal Power Over Ethernet (60W at PSE)

UPoE+– Cisco Universal Power Over Ethernet Plus (90W at PSE)

URL–Uniform Resource Locator

VLAN–Virtual Local Area Network

VM—Virtual Machine

VN–Virtual Network, analogous to a VRF in SD-Access

VNI–Virtual Network Identifier (VXLAN)

vPC–virtual Port Channel (Cisco Nexus)

VPLS–Virtual Private LAN Service

VPN–Virtual Private Network

VPNv4–BGP address family that consists of a Route-Distinguisher (RD) prepended to an IPv4 prefix

VPWS–Virtual Private Wire Service

VRF–Virtual Routing and Forwarding

VSL–Virtual Switch Link (Cisco VSS component)

VSS–Cisco Virtual Switching System

VXLAN–Virtual Extensible LAN

WAN–Wide-Area Network

WLAN–Wireless Local Area Network (generally synonymous with IEEE 802.11-based networks)

WoL–Wake-on-LAN

xTR–Tunnel Router (LISP - device operating as both an ETR and ITR)

Appendix B—Glossary of Terms

This glossary addresses some terms used in this document, for the purposes of aiding understanding. This is not a complete list of all multicloud terminology. Some Cisco product links are supplied here also, where considered useful for the purposes of clarity, but this is by no means intended to be a complete list of all applicable Cisco products.

aaS/XaaS **(IT capability provided as a Service)**	Some IT capability, X, provided as a service (XaaS). Some benefits are: • The provider manages the design, implementation, deployment, upgrades, resiliency, scalability, and overall delivery of the service and the infrastructure that supports it. • There are low barriers to entry, so that services can be quickly adopted and dropped in response to business demand, without the penalty of inefficiently utilized CapEx. • The service charge is an IT OpEx cost (pay-as-you-go), whereas the CapEx and the service infrastructure is the responsibility of the provider. • Costs are commensurate to usage and hence more easily controlled with respect to business demand and outcomes. Such services are typically implemented as “microservices,” which are accessed via REST APIs. This architectural style supports composition of service components into systems. Access to and management of aaS assets is via a web GUI and/or APIs, such that Infrastructure-as-code (IaC) techniques can be used for automation, for example, Ansible and Terraform.

	The provider can be any entity capable of implementing an aaS “cloud-native” architecture. The cloud-native architecture concept is well-documented and supported by open-source software and a rich ecosystem of services such as training and consultancy. The provider can be an internal IT department or any of many third-party companies using and supporting the same open-source platforms. Service access control, integrated with corporate IAM, can be mapped to specific users and business activities, enabling consistent policy controls across services, wherever they are delivered from.
Ansible	An infrastructure automation tool, used to implement processes for instantiating and configuring IT service components, such as VMs on an IaaS platform. Supports the consistent execution of processes defined in YAML “playbooks” at scale, across multiple targets. Because the Ansible artefacts (playbooks) are text-based, they can be stored in a Source Code Management (SCM) system, such as GitHub. This allows for software development like processes to be applied to infrastructure automation, such as, Infrastructure-as-code (see IaC below). https://www.ansible.com
AWS **(Amazon Web Services)**	Provider of IaaS and PaaS. https://aws.amazon.com
Azure	Microsoft IaaS and PaaS. https://azure.microsoft.com/en-gb/
Co-located data center	“A colocation center (CoLo)...is a type of data center where equipment, space, and bandwidth are available for rental to retail customers. Colocation facilities provide space, power, cooling, and physical security for the server, storage, and networking equipment of other firms and also connect them to a variety of telecommunications and network service providers with a minimum of cost and complexity.” https://en.wikipedia.org/wiki/Colocation_centre

Containers **(Docker)**	A (Docker) container is a means to create a package of code for an application and its dependencies, such that the application can run on different platforms which support the Docker environment. In the context of aaS, microservices are typically packaged within Linux containers orchestrated by Kubernetes (K8s). https://www.docker.com https://www.cisco.com/c/en/us/products/cloud-systems-management/containerplatform/index.html
DevOps	The underlying principle of DevOps is that the application development and operations teams should work closely together, ideally within the context of a toolchain that automates the stages of development, test, deployment, monitoring, and issue handling. DevOps is closely aligned with IaC, continuous integration and deployment (CI/CD), and Agile software development practices. https://en.wikipedia.org/wiki/DevOps https://en.wikipedia.org/wiki/CI/CD
Edge compute	Edge compute is the idea that it can be more efficient to process data at the edge of a network, close to the endpoints that originate that data, or to provide virtualized access services, such as at the network edge. This could be for reasons related to low latency response, reduction of the amount of unprocessed data being transported, efficiency of resource utilization, and so on. The generic label for this is Multi-access Edge Computing (MEC), or Mobile Edge Computing for mobile networks specifically. From an application experience perspective, it is important to be able to utilize, at the edge, the same operations model, processes, and tools used for any other compute node in the system. https://en.wikipedia.org/wiki/Mobile_edge_computing
IaaS **(Infrastructure as-a-Service)**	Infrastructure components provided aaS, located in data centers operated by a provider, typically accessed over the public Internet. IaaS provides a base platform for the deployment of workloads, typically with containers and Kubernetes (K8s).
IaC **(Infrastructure as-Code)**	Given the ability to automate aaS via APIs, the implementation of the automation is typically via Python code, Ansible playbooks, and similar. These automation artefacts are programming code that define how the services are consumed. As such, they can be subject to the same code management and software development regimes as any other body of code. This means that infrastructure automation can be subject to all of the quality and consistency benefits, CI/CD, traceability, automated testing, compliance checking, and so on, that could be applied to any coding project. https://en.wikipedia.org/wiki/Infrastructure_as_code
IAM **(Identity and Access Management)**	IAM is the means to control access to IT resources so that only those explicitly authorized to access given resources can do so. IAM is an essential foundation to a secure multicloud environment. https://en.wikipedia.org/wiki/Identity_management
IBM **(Cloud)**	IBM IaaS and PaaS. https://www.ibm.com/cloud
Intersight	Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. https://www.cisco.com/c/en/us/products/servers-unified-computing/intersight/index.html

GCP **(Google Cloud Platform)**	Google IaaS and PaaS. https://cloud.google.com/gcp
Kubernetes **(K8s)**	Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications. https://kubernetes.io
Microservices	A microservices architecture is characterized by processes implementing fine-grained services, typically exposed via REST APIs and which can be composed into systems. The processes are often container-based, and the instantiation of the services often managed with Kubernetes. Microservices managed in this way are intrinsically well suited for deployment into IaaS environments, and as such, are the basis of a cloud native architecture. https://en.wikipedia.org/wiki/Microservices
PaaS **(Platform-as-a-Service)**	PaaS is a layer of value-add services, typically for application development, deployment, monitoring, and general lifecycle management. The use of IaC with IaaS and PaaS is very closely associated with DevOps practices.
Private on-premises data center	A data center infrastructure housed within an environment owned by a given enterprise is distinguished from other forms of data center, with the implication that the private data center is more secure, given that access is restricted to those authorized by the enterprise. Thus, circumstances can arise where very sensitive IT assets are only deployed in a private data center, in contrast to using public IaaS. For many intents and purposes, the underlying technology can be identical, allowing for hybrid deployments where some IT assets are privately deployed but also accessible to other assets in public IaaS. IAM, VPNs, firewalls, and similar are key technologies needed to underpin the security of such an arrangement.
REST API	Representational State Transfer (REST) APIs is a generic term for APIs accessed over HTTP(S), typically transporting data encoded in JSON or XML. REST APIs have the advantage that they support distributed systems, communicating over HTTP, which is a well-understood protocol from a security management perspective. REST APIs are another element of a cloud-native applications architecture, alongside microservices. https://en.wikipedia.org/wiki/Representational_state_transfer
SaaS **(Software-as-a-Service)**	End-user applications provided "aaS" over the public Internet, with the underlying software systems and infrastructure owned and managed by the provider.
SAML **(Security Assertion Markup Language)**	Used in the context of Single-Sign-On (SSO) for exchanging authentication and authorization data between an identity provider, typically an IAM system, and a service provider (some form of SaaS). The SAML protocol exchanges XML documents that contain security assertions used by the aaS for access control decisions. https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
Terraform	An open-source IaC software tool for cloud services, based on declarative configuration files. https://www.terraform.io

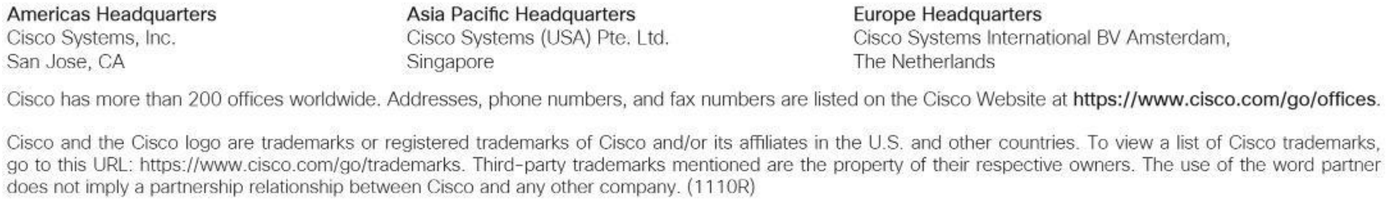
Feedback

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

CVD Program

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

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



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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