



# FlexPod Datacenter with Citrix VDI and VMware vSphere 7 for up to 2500 Seats

Deployment Guide for a 2500 Seat Virtual Desktop Infrastructure Built on X-Series Compute Nodes M6 with NetApp AFF A-Series using Citrix Virtual Apps & Desktops and VMware vSphere ESXi 7 Hypervisor Platform

---

Published: April 2022



In partnership with:



---

## Document Organization

This document is organized into the following chapters:

- [Executive Summary](#)
- [Solution Overview](#)
- [Solution Summary](#)
- [Solution Components](#)
- [Citrix Virtual Apps & Desktops 7 LTSR](#)
- [NetApp A-Series All Flash FAS](#)
- [Architecture and Design Considerations for Desktop Virtualization](#)
- [Deployment Hardware and Software](#)
- [Solution Configuration](#)
- [Storage Configuration](#)
- [Cisco Intersight Managed Mode Configuration](#)
- [Storage Configuration – Boot LUNs](#)
- [Test Setup and Configurations](#)
- [Test Results](#)
- [Appendix–Cisco Switch Configuration](#)
- [References](#)
- [About the Authors](#)





























---

## 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>.



## Icons Used in this Document

	Layer 3 Switch (Multilayer switch)		Layer 3 Switch Stack		Layer 3 Routed Link		Internet (untrusted)
	Layer 2 Switch		Layer 2 Switch Stack		Layer 2 Switched Link		Private Network or the remainder of campus network (trusted)
	Router		SD-Access Embedded Wireless		Layer 3 EtherChannel Routed Link		Private WAN Circuit (trusted)
	Router		Layer 3 Switch (Multilayer switch)		Layer 2 EtherChannel Switched Link		Wired Endpoint (802.1X)
	StackWise Virtual (SVL) or Virtual Switching System (VSS)		Firewall		Redundancy Port (WLC)		Wireless Endpoint (802.1X)
	WLC (Wireless LAN Controller)		Cisco DNA Center		Multi-box, single logical unit such as HA Pair, VSS, SVL		Wired Endpoint
	AP (Access Point)		Identity Service Engine		Services (DHCP, DNS, AD, NTP, etc)		Wireless Endpoint

---

## Executive Summary

Cisco® Validated Designs include 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 customers. Cisco and NetApp have partnered to deliver this document, which serves as a specific step by step guide for implementing this solution. This Cisco Validated Design provides an efficient architectural design that is based on customer requirements. The solution that follows is a validated approach to deploying Cisco, NetApp, Citrix and VMware technologies as a shared, high performance, resilient, virtual desktop infrastructure.

This document provides a Reference Architecture for a virtual desktop and application design using Citrix RDS/Citrix Virtual Apps & Desktops 7 LTSR built on Cisco UCS with a NetApp® All Flash FAS (AFF) A400 storage and the VMware vSphere ESXi 7.02 hypervisor platform.

This document explains deployment details of incorporating the Cisco X-Series modular platform into the FlexPod Datacenter and the ability to manage and orchestrate FlexPod components from the cloud using Cisco Intersight. Some of the key advantages of integrating Cisco UCS X-Series into the FlexPod infrastructure are:

- **Simpler and programmable infrastructure:** infrastructure as a code delivered through a single partner integrable open API
- **Power and cooling innovations:** higher power headroom and lower energy loss due to a 54V DC power delivery to the chassis
- **Better airflow:** midplane-free design with fewer barriers, therefore lower impedance
- **Fabric innovations:** PCIe/Compute Express Link (CXL) topology for heterogeneous compute and memory composability
- **Innovative cloud operations:** continuous feature delivery and no need for maintaining on-premise virtual machines supporting management functions
- **Built for investment protections:** design ready for future technologies such as liquid cooling and high-Wattage CPUs; CXL-ready

In addition to the compute-specific hardware and software innovations, the integration of the Cisco Intersight cloud platform with VMware vCenter and NetApp Active IQ Unified Manager delivers monitoring, orchestration, and workload optimization capabilities for different layers (virtualization and storage) of the FlexPod infrastructure. The modular nature of the Cisco Intersight platform also provides an easy upgrade path to additional services, such as workload optimization and Kubernetes.

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 new Cisco UCS X-Series M6 high-performance Cisco UCS Compute Nodes 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 compute end user. The solution virtualized on fifth generation Cisco UCS X-Series Compute Nodes, booting VMware vSphere 7.02 Update 2 through FC SAN from the AFF A400 storage array. The virtual desktops are powered using Citrix Virtual Apps & Desktops, with a mix of RDS hosted shared desktops (2500), pooled/non-persistent hosted virtual Windows 10 desktops (2500) and persistent hosted 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 is organized into the following subjects:

- [Introduction](#)
- [Audience](#)
- [Purpose of this Document](#)
- [What's New in this Release](#)

### Introduction

Cisco Unified Computing System (Cisco UCS) X-Series is a brand-new modular compute system, configured and managed from the cloud. It is designed to meet the needs of modern applications and to improve operational efficiency, agility, and scale through an adaptable, future-ready, modular design. The Cisco Intersight platform is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support.

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.

### Audience

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

### Purpose of this Document

This document provides a step-by-step design, configuration, and implementation guide for the Cisco Validated Design for a large-scale Citrix VDI mixed workload solution with NetApp AFF A400, NS224 NVMe Disk Shelf, Cisco UCS X210c M6 compute nodes, Cisco Nexus 9000 series Ethernet switches and Cisco MDS 9000 series fibre channel switches.

### What's New in this Release?

This is the first Citrix Virtual Apps & Desktops desktop virtualization Cisco Validated Design with Cisco UCS 6<sup>th</sup> generation servers and a NetApp AFF A-Series system.

It incorporates the following features:

- Integration of Cisco UCS X-Series into FlexPod Datacenter
- Deploying and managing Cisco UCS X9508 chassis equipped with Cisco UCS X210c M6 compute nodes from the cloud using Cisco Intersight

- 
- Integration of Cisco Intersight with NetApp Active IQ Unified Manager for storage monitoring and orchestration
  - Integration of Cisco Intersight with VMware vCenter for interacting with, monitoring, and orchestrating the virtual environment
  - Cisco UCS Cisco UCS X210c M6 compute nodes with Intel Xeon Scalable Family processors and 3200 MHz memory
  - Validation of Cisco Nexus 9000 with NetApp AFF A400 system
  - Validation of Cisco MDS 9000 with NetApp AFF A400 system
  - Support for the Cisco UCS 5.0(1b) release and Cisco X-Series Compute nodes
  - Support for the latest release of NetApp AFF A400 hardware and NetApp ONTAP® 9.9
  - VMware vSphere 7 U2 Hypervisor
  - Citrix Virtual Apps & Desktops for Server 2019 RDS hosted shared virtual desktops
  - Citrix Virtual Apps & Desktops non-persistent hosted virtual Windows 10 desktops
  - Citrix Virtual Apps & Desktops persistent full clones hosted virtual Windows 10 desktops

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 of management and scalability.

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

The use cases include:

- Enterprise Datacenter
- Service Provider Datacenter
- Large Commercial Datacenter

---

## Solution Summary

This chapter is organized into the following subjects:

- [Cisco Desktop Virtualization Solutions: Data Center](#)
- [Cisco Desktop Virtualization Focus](#)
- [Physical Topology](#)
- [Configuration Guidelines](#)
- [What is FlexPod?](#)
- [Why FlexPod?](#)

This Cisco Validated Design prescribes a defined set of hardware and software that serves as an integrated foundation for both Citrix Virtual Apps & Desktops Microsoft Windows 10 virtual desktops and Citrix Virtual Apps & Desktops RDS server desktop sessions based on Microsoft Server 2019.

The mixed workload solution includes NetApp AFF A400 storage, Cisco Nexus® and MDS networking, the Cisco UCS X210c M6 Compute Nodes, Citrix Virtual Apps & Desktops and VMware vSphere software in a single package. The design is space optimized such that the network, compute, and storage required can be housed in one data center rack. Switch port density enables the networking components to accommodate multiple compute and storage configurations of this kind.

The infrastructure is deployed to provide Fibre Channel-booted hosts with access to shared storage using NFS mounts. The reference architecture reinforces the "wire-once" strategy because as additional storage is added to the architecture, no re-cabling is required from the hosts to the Cisco UCS fabric interconnect.

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

- **More power.** Cisco UCS X210c M6 compute nodes with dual 28-core 2.6 GHz Intel® Xeon® Gold (6348) processors and 1 TB of memory supports more virtual desktop workloads than the previously released generation processors on the same hardware. The Intel 28-core 2.6 GHz Intel® Xeon® Gold (6348) processors used in this study provided a balance between increased per-blade capacity and cost.
- **Fault-tolerance with high availability built into the design.** The various designs are based on using one Unified Computing System chassis with multiple Cisco UCS X210c M6 compute nodes for virtualized desktop and infrastructure workloads. The design provides N+1 server fault tolerance for hosted virtual desktops, hosted shared desktops and infrastructure services.
- **Stress-tested to the limits during simulated login storms.** All 2500 simulated users logged in and started running workloads up to steady state in 48-minutes without overwhelming the processors, exhausting memory, or exhausting the storage subsystems, providing customers with a desktop virtualization system that can easily handle the most demanding login and startup storms.

- **Ultra-condensed computing for the datacenter.** The rack space required to support the system is a single 42U rack, conserving valuable data center floor space.
- **All Virtualized:** This CVD presents a validated design that is 100 percent virtualized on VMware ESXi 7.02. All of the virtual desktops, user data, profiles, and supporting infrastructure components, including Active Directory, SQL Servers, Citrix Virtual Apps & Desktops components, Citrix Virtual Apps & Desktops VDI desktops and RDS servers were hosted as virtual machines. This provides customers with complete flexibility for maintenance and capacity additions because the entire system runs on the FlexPod converged infrastructure with stateless Cisco UCS X210c M6 compute nodes and NetApp FC storage.
- **Cisco maintains industry leadership** with the new Cisco Intersight that simplifies scaling, guarantees consistency, and eases maintenance. Cisco's ongoing development efforts with Cisco Intersight, ensure that customer environments are consistent locally, across Cisco UCS Domains and across the globe, our software suite offers increasingly simplified operational and deployment management, and it continues to widen the span of control for customer organizations' subject matter experts in compute, storage, and network.
- **Our 25G unified fabric story** gets additional validation on Cisco UCS 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 & Desktops and RDS Advantage.** RDS and Citrix Virtual Apps & Desktops are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

RDS and Citrix Virtual Apps & Desktops allow:

- End users to run applications and desktops independently of the device's operating system and interface.
- Administrators to manage the network and control access from selected devices or from all devices.
- Administrators to manage an entire network from a single data center.
- RDS and Citrix Virtual Apps & Desktops share a unified architecture called FlexCast Management Architecture (FMA). FMA's key features are the ability to run multiple versions of RDS or Citrix Virtual Apps & Desktops from a single Site and integrated provisioning.
- Optimized to achieve the best possible performance and scale. For hosted shared desktop sessions, the best performance was achieved when the number of vCPUs assigned to the 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 provides two core provisioning methods for Citrix Virtual Apps & Desktops and RDS virtual machines: Citrix Provisioning Services for pooled virtual desktops and RDS virtual servers and Citrix Machine Creation Services for pooled or persistent virtual desktops. This paper provides guidance on how to use each method and documents the performance of each technology.

## Cisco Desktop Virtualization Solutions: Data Center

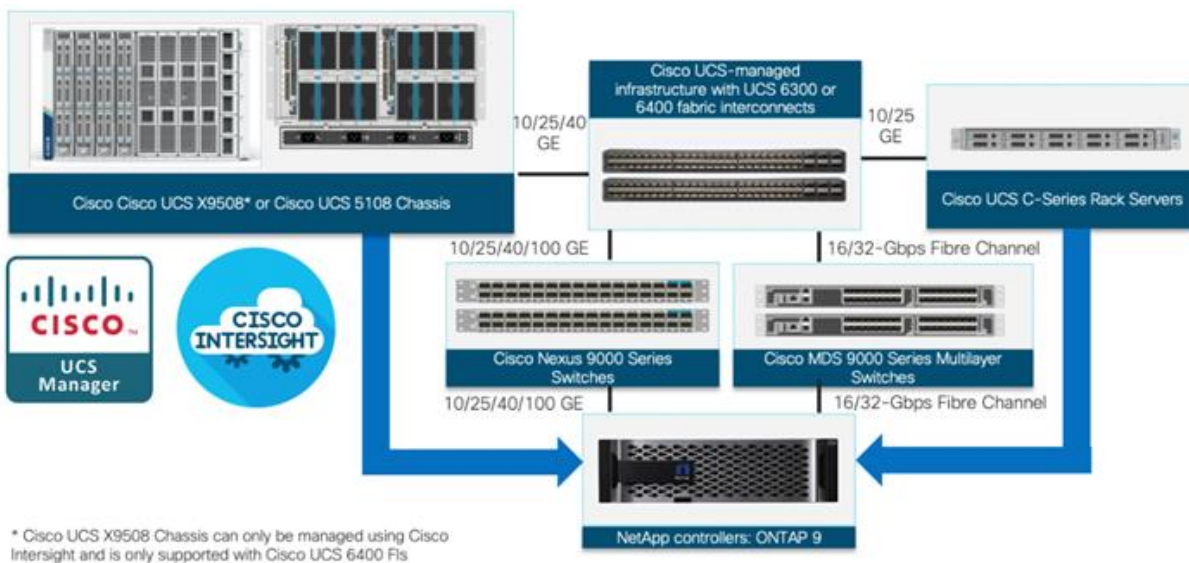
### The Evolving Workplace

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 the protection of corporate data and prevent data leakage or loss through any combination of user, endpoint device, and desktop access scenarios ([Figure 1](#)).

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

**Figure 1. Cisco Data Center Partner Collaboration**



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



---

## Cisco Desktop Virtualization Focus

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

### Simplified

Cisco UCS provides a radical new approach to industry-standard computing and provides the core of the data center infrastructure for desktop virtualization. Among the many features and benefits of Cisco UCS are the drastic reduction in the number of servers needed and in the number of cables used per server, and the capability to rapidly deploy or reprovision 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 server 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 X-Series modular servers, B-Series Blade Servers and C-Series Rack Servers with large memory footprints enable high desktop density that helps reduce server infrastructure requirements.

Simplification also leads to more successful desktop virtualization implementation. Cisco and its technology partners like VMware Technologies and NetApp have developed integrated, validated architectures, including predefined converged architecture infrastructure packages such as FlexPod. Cisco Desktop Virtualization Solutions have been tested with VMware vSphere, VMware Horizon, Citrix Virtual Apps and Desktops.

### 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 the 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 server 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 30 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.

## **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.

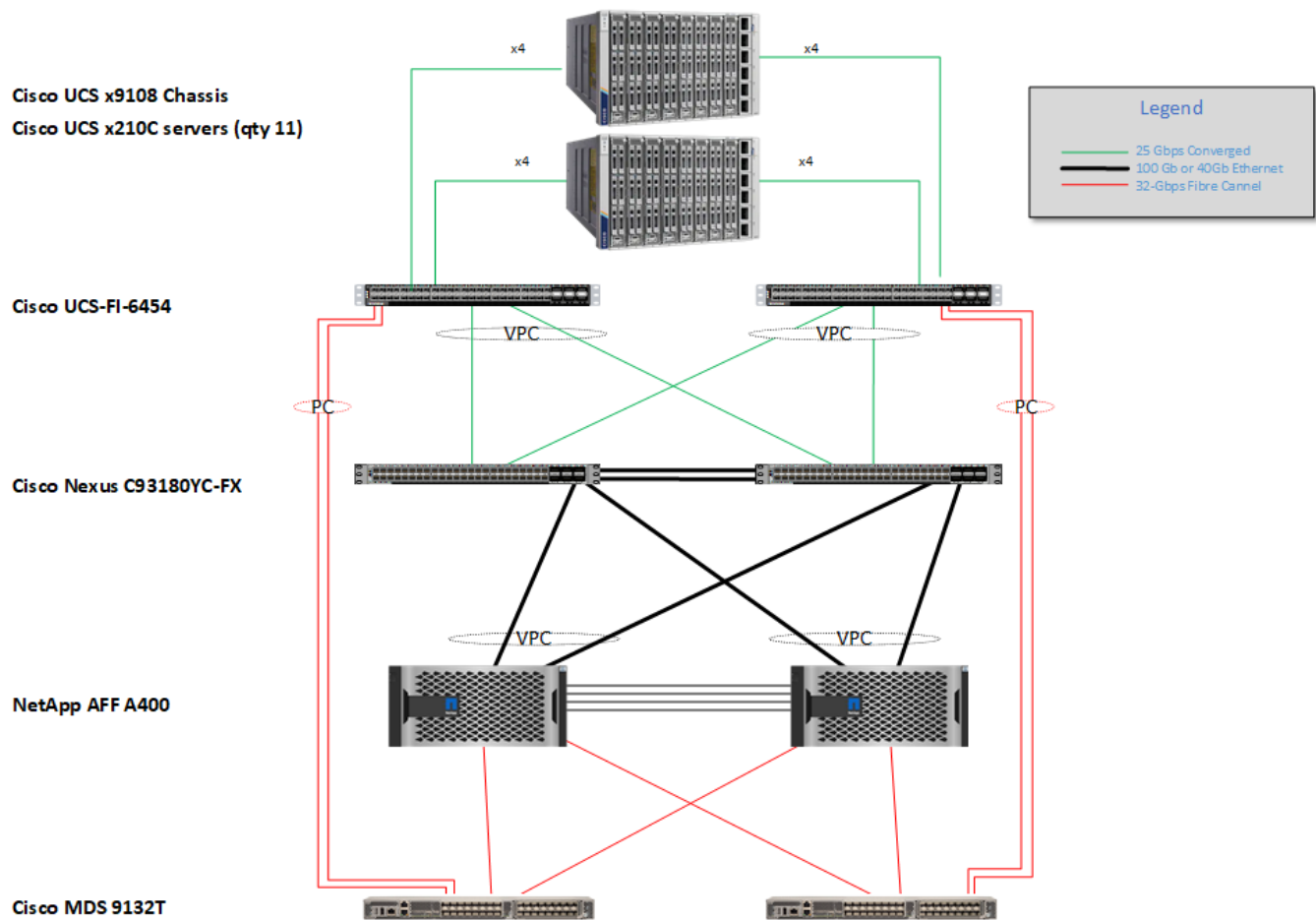
The simplified deployment of Cisco UCS for desktop virtualization accelerates the time to productivity and enhances business agility. IT staff and end users are more productive more quickly, and the business can respond to new opportunities quickly by deploying virtual desktops whenever and wherever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

The ultimate measure of desktop virtualization for any organization is its efficiency and effectiveness in both the near term and the long term. The Cisco Desktop Virtualization Solutions are very efficient, allowing rapid deployment, requiring fewer devices and cables, and reducing costs. The solutions are also very 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 storage, 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 for the platform for desktop virtualization.

## **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
- Two Cisco UCS X-Series Chassis
- Eleven X-Series Compute Nodes (for VDI workload)
- One NetApp AFF A400 Storage System
- Two NetApp NS224 Disk Shelves

For desktop virtualization, the deployment includes Citrix Virtual Apps & Desktops 7 LTSR running on VMware vSphere 7.02.

The design is intended to provide a large-scale building block for Citrix Virtual Apps & Desktops workloads consisting of RDS Windows Server 2019 hosted shared desktop sessions and Windows 10 non-persistent and persistent hosted desktops in the following:

- 2500 Random Hosted Shared Windows 2019 user sessions with office 2016 (PVS)
- 2500 Random Pooled Windows 10 Desktops with office 2016 (PVS)
- 2500 Static Full Copy Windows 10 Desktops with office 2016 (MCS)

The data provided in this document will allow our customers to adjust the mix of HSD and HSD 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 covers 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 mixed workload virtual 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.

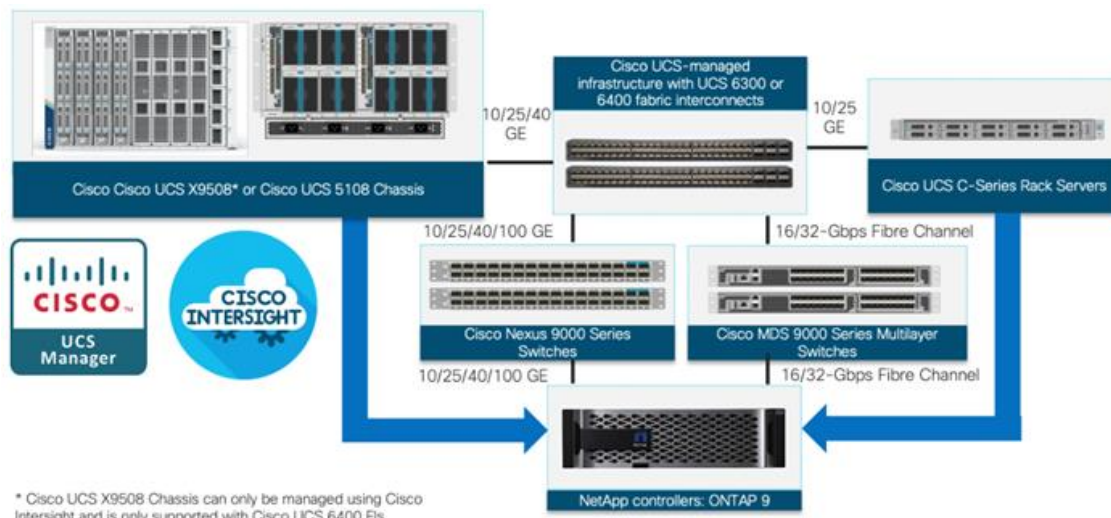
The Cisco UCS 6454 Fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-RDSH-01, VM-Host-VDI-01 and so on. Finally, to indicate that you 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**



These components are connected and configured according to the best practices of both Cisco and NetApp to provide an ideal platform for running a variety of enterprise workloads with confidence. FlexPod can scale up for greater performance and capacity (adding compute, network, or storage resources individually as needed), or it can scale out for environments that require multiple consistent deployments (such as rolling out of additional FlexPod stacks). The reference architecture covered in this document leverages Cisco Nexus 9000 for the network switching element and pulls in the Cisco MDS 9000 for the SAN switching component.

One of the key benefits of FlexPod is its ability to maintain consistency during scale. Each of the component families shown (Cisco UCS, Cisco Nexus, and NetApp AFF) offers platform and resource options to scale the infrastructure up or down, while supporting the same features and functionality that are required under the configuration and connectivity best practices of FlexPod.

## Why FlexPod?

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

## Solution Components

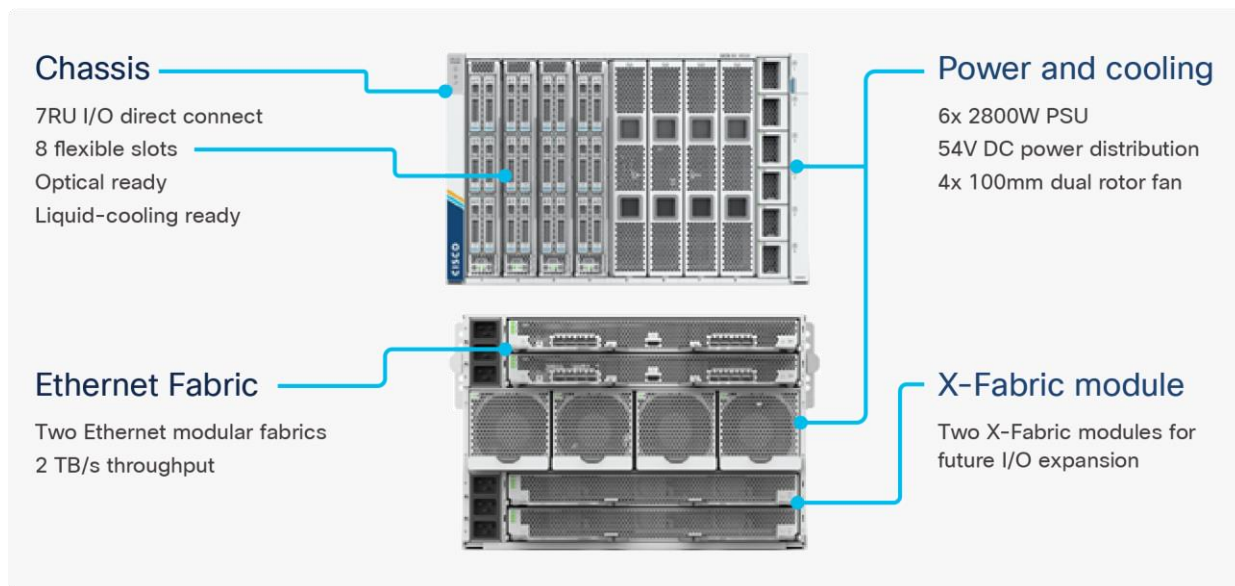
This chapter is organized into the following subjects:

- [Cisco Unified Compute System X-Series](#)
- [Cisco Intersight](#)
- [Cisco Nexus Switching Fabric](#)
- [Cisco MDS 9132T 32G Multilayer Fabric Switch](#)
- [Cisco DCNM-SAN](#)
- [NetApp AFF A-Series Storage](#)
- [VMware vSphere 7.0](#)
- [Cisco Intersight Assist Device Connector for VMware vCenter and NetApp ONTAP](#)

### Cisco Unified Compute System X-Series

The Cisco UCS X-Series Modular System is designed to take the current generation of the Cisco UCS platform to the next level with its future-ready design and cloud-based management. Decoupling and moving the platform management to the cloud allows Cisco UCS to respond to customer feature and scalability requirements in a much faster and efficient manner. Cisco UCS X-Series state of the art hardware simplifies the data-center design by providing flexible server options. A single server type, supporting a broader range of workloads, results in fewer different data-center products to manage and maintain. The Cisco Intersight cloud-management platform manages Cisco UCS X-Series as well as integrating with third-party devices, including VMware vCenter and NetApp storage, to provide visibility, optimization, and orchestration from a single platform, thereby driving agility and deployment consistency.

Figure 4. Cisco UCS X9508 Chassis





The various components of the Cisco UCS X-Series are described in the following sections.

## Cisco UCS X9508 Chassis

The Cisco UCS X-Series chassis is engineered to be adaptable and flexible. As seen in [Figure 5](#), Cisco UCS X9508 chassis has only a power-distribution midplane. This midplane-free design provides fewer obstructions for better airflow. For I/O connectivity, vertically oriented compute nodes intersect with horizontally oriented fabric modules, allowing the chassis to support future fabric innovations. Cisco UCS X9508 Chassis' superior packaging enables larger compute nodes, thereby providing more space for actual compute components, such as memory, GPU, drives, and accelerators. Improved airflow through the chassis enables support for higher power components, and more space allows for future thermal solutions (such as liquid cooling) without limitations.

**Figure 5. Cisco UCS X9508 Chassis - Midplane Free Design**



The Cisco UCS X9508 7-Rack-Unit (7RU) chassis has eight flexible slots. These slots can house a combination of compute nodes and a pool of future I/O resources that may include GPU accelerators, disk storage, and non-volatile memory. At the top rear of the chassis are two Intelligent Fabric Modules (IFMs) that connect the chassis to upstream Cisco UCS 6400 Series Fabric Interconnects. At the bottom rear of the chassis are slots ready to house future X-Fabric modules that can flexibly connect the compute nodes with I/O devices. Six 2800W Power Supply Units (PSUs) provide 54V power to the chassis with N, N+1, and N+N redundancy. A higher voltage allows efficient power delivery with less copper and reduced power loss. Efficient, 100mm, dual counter-rotating fans deliver industry-leading airflow and power efficiency, and optimized thermal algorithms enable different cooling modes to best support the customer's environment.

## Cisco UCSX 9108-25G Intelligent Fabric Modules

For the Cisco UCS X9508 Chassis, the network connectivity is provided by a pair of Cisco UCSX 9108-25G Intelligent Fabric Modules (IFMs). Like the fabric extenders used in the Cisco UCS 5108 Blade Server Chassis, these modules carry all network traffic to a pair of Cisco UCS 6400 Series Fabric Interconnects (FIs). IFMs also host the Chassis Management Controller (CMC) for chassis management. In contrast to systems with fixed networking components, Cisco UCS X9508's midplane-free design enables easy upgrades to new networking technologies as they emerge making it straightforward to accommodate new network speeds or technologies in the future.

**Figure 6. Cisco UCSX 9108-25G Intelligent Fabric Module**



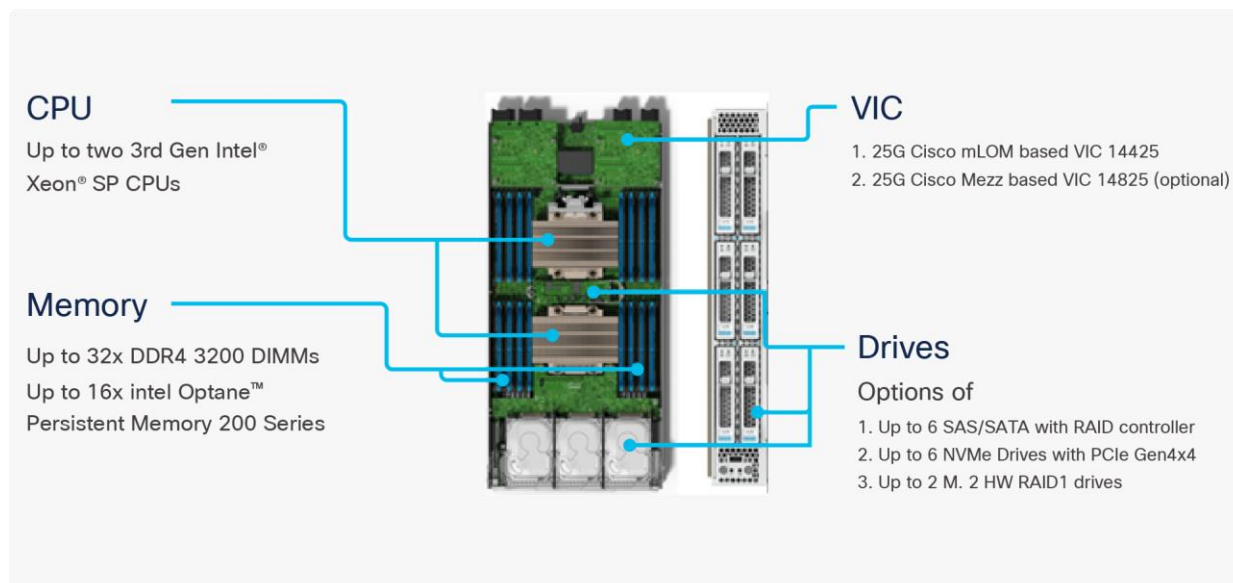


Each IFM supports eight 25Gb uplink ports for connecting the Cisco UCS X9508 Chassis to the FIs and 32 25Gb server ports for the eight compute nodes. IFM server ports can provide up to 200 Gbps of unified fabric connectivity per compute node across the two IFMs. The uplink ports connect the chassis to the UCS FIs, providing up to 400Gbps connectivity across the two IFMs. The unified fabric carries management, VM, and Fibre Channel over Ethernet (FCoE) traffic to the FIs, where management traffic is routed to the Cisco Intersight cloud operations platform, FCoE traffic is forwarded to the native Fibre Channel interfaces through unified ports on the FI (to Cisco MDS switches), and data Ethernet traffic is forwarded upstream to the data center network (via Cisco Nexus switches).

## Cisco UCS X210c M6 Compute Node

The Cisco UCS X9508 Chassis is designed to host up to 8 Cisco UCS X210c M6 Compute Nodes. The hardware details of the Cisco UCS X210c M6 Compute Nodes are shown in [Figure 7](#):

**Figure 7. Cisco UCS X210c M6 Compute Node**



The Cisco UCS X210c M6 features:

- **CPU:** Up to 2x 3rd Gen Intel Xeon Scalable Processors with up to 40 cores per processor and 1.5 MB Level 3 cache per core
- **Memory:** Up to 32 x 256 GB DDR4-3200 DIMMs for a maximum of 8 TB of main memory. The Compute Node can also be configured for up to 16 x 512-GB Intel Optane persistent memory DIMMs for a maximum of 12 TB of memory
- **Disk storage:** Up to 6 SAS or SATA drives can be configured with an internal RAID controller, or customers can configure up to 6 NVMe drives. 2 M.2 memory cards can be added to the Compute Node with RAID 1 mirroring.
- **Virtual Interface Card (VIC):** Up to 2 VICs including an mLOM Cisco VIC 14425 and a mezzanine Cisco VIC card 14825 can be installed in a Compute Node.

- **Security:** The server supports an optional Trusted Platform Module (TPM). Additional security features include a secure boot FPGA and ACT2 anticounterfeit provisions.

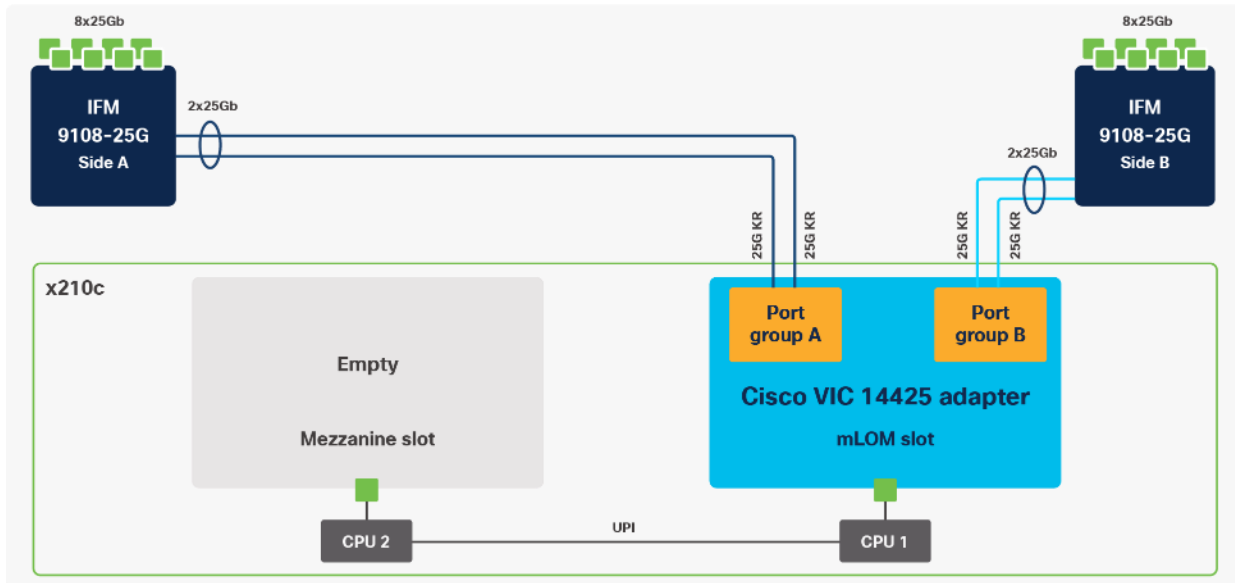
## Cisco UCS Virtual Interface Cards (VICs)

Cisco UCS X210c M6 Compute Nodes support the following two Cisco fourth-generation VIC cards:

### Cisco VIC 14425

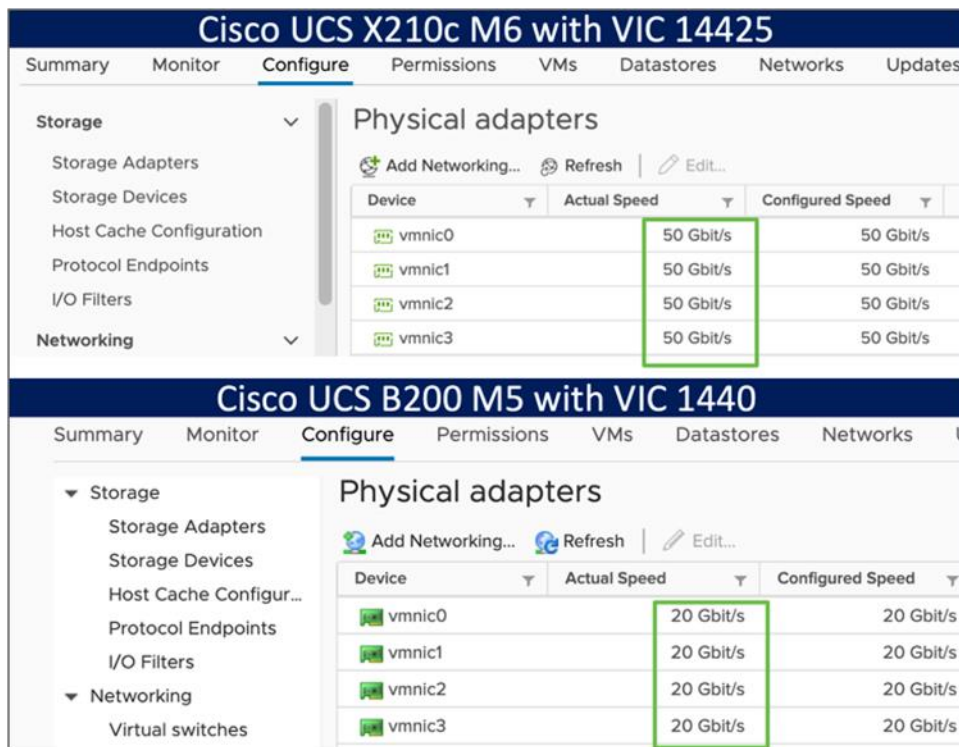
Cisco VIC 14425 fits the mLOM slot in the Cisco X210c Compute Node and enables up to 50 Gbps of unified fabric connectivity to each of the chassis IFMs for a total of 100 Gbps of connectivity per server. Cisco VIC 14425 connectivity to the IFM and up to the fabric interconnects is delivered through 4x 25-Gbps connections, which are configured automatically as 2x 50-Gbps port channels. Cisco VIC 14425 supports 256 virtual interfaces (both Fibre Channel and Ethernet) along with the latest networking innovations such as NVMeoF over RDMA (ROCEv2), VxLAN/NVGRE offload, and so on.

**Figure 8. Single Cisco VIC 14425 in Cisco UCS X210c M6**



The connections between the 4<sup>th</sup> generation Cisco VIC (Cisco UCS VIC 1440) in the Cisco UCS B200 blades and the I/O modules in the Cisco UCS 5108 chassis comprise of multiple 10Gbps KR lanes. The same connections between Cisco VIC 14425 and IFMs in Cisco UCS X-Series comprise of multiple 25Gbps KR lanes resulting in 2.5x better connectivity in Cisco UCS X210c M6 Compute Nodes. The network interface speed comparison between VMware ESXi installed on Cisco UCS X210C M6 with VIC 1440 and Cisco UCS X210c M6 with VIC 14425 is shown in [Figure 7](#).

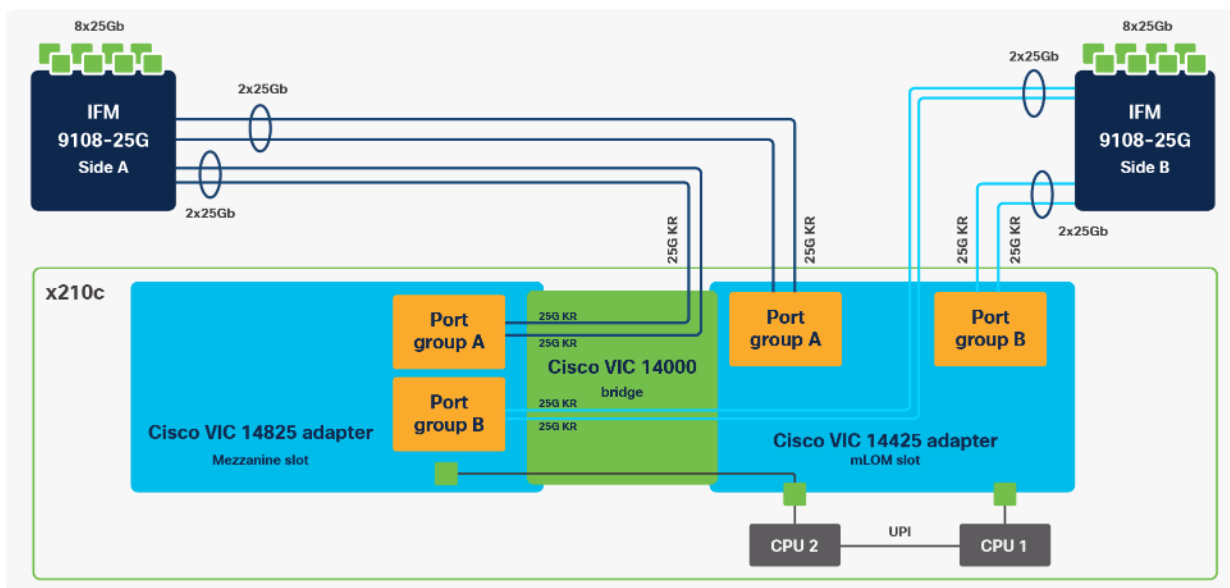
Figure 9. Network Interface Speed Comparison



### Cisco VIC 14825

The optional Cisco VIC 14825 fits the mezzanine slot on the server. A bridge card (UCSX-V4-BRIDGE) extends this VIC's 2x 50 Gbps of network connections up to the mLOM slot and out through the mLOM's IFM connectors, bringing the total bandwidth to 100 Gbps per fabric for a total bandwidth of 200 Gbps per server.

Figure 10. Cisco VIC 14425 and 14825 in Cisco UCS X210c M6



## Cisco UCS 6400 Series Fabric Interconnects

The Cisco UCS Fabric Interconnects (FIs) provide a single point for connectivity and management for the entire Cisco UCS system. Typically deployed as an active/active pair, the system's FIs integrate all components into a single, highly available management domain controlled by Cisco Intersight. Cisco UCS FIs provide a single unified fabric for the system, with low-latency, lossless, cut-through switching that supports LAN, SAN, and management traffic using a single set of cables.

Figure 11. Cisco UCS 6454 Fabric Interconnect



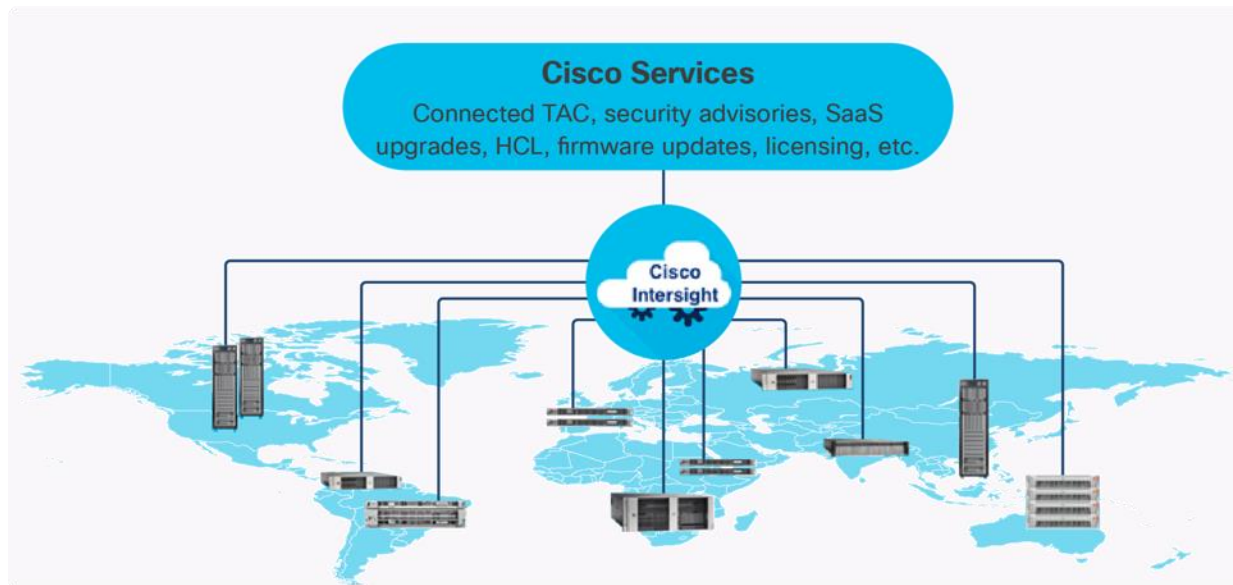
Cisco UCS 6454 utilized in the current design is a 54-port Fabric Interconnect. This single RU device includes 28 10/25 Gbps Ethernet ports, 4 1/10/25-Gbps Ethernet ports, 6 40/100-Gbps Ethernet uplink ports, and 16 unified ports that can support 10/25 Gigabit Ethernet or 8/16/32-Gbps Fibre Channel, depending on the SFP.

**Note:** For supporting the Cisco UCS X-Series, the fabric interconnects must be configured in Intersight Managed Mode (IMM). This option replaces the local management with Cisco Intersight cloud- or appliance-based management.

## 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 12. Cisco Intersight Overview



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, see [https://intersight.com/help/getting\\_started#licensing\\_requirements](https://intersight.com/help/getting_started#licensing_requirements).

View current [Cisco Intersight Infrastructure Service licensing](#).

## Cisco Nexus Switching Fabric

The Cisco Nexus 9000 Series Switches offer both modular and fixed 1/10/25/40/100 Gigabit Ethernet switch configurations with scalability up to 60 Tbps of nonblocking performance with less than five-microsecond latency, wire speed VXLAN gateway, bridging, and routing support.

**Figure 13. Cisco Nexus 93180YC-FX3 Switch**



The Cisco Nexus 9000 series switch featured in this design is the Cisco Nexus 93180YC-FX3 configured in NX-OS standalone mode. NX-OS is a purpose-built data-center operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. It provides a robust and comprehensive feature set that meets the demanding requirements of virtualization and automation.

The Cisco Nexus 93180YC-FX3 Switch is a 1RU switch that supports 3.6 Tbps of bandwidth and 1.2 bpps. The 48 downlink ports on the 93180YC-FX3 can support 1-, 10-, or 25-Gbps Ethernet, offering deployment flexibility and investment protection. The six uplink ports can be configured as 40- or 100-Gbps Ethernet, offering flexible migration options.

## Cisco MDS 9132T 32G Multilayer Fabric Switch

The Cisco MDS 9132T 32G Multilayer Fabric Switch is the next generation of the highly reliable, flexible, and low-cost Cisco MDS 9100 Series switches. It combines high performance with exceptional flexibility and cost effectiveness. This powerful, compact one Rack-Unit (1RU) switch scales from 8 to 32 line-rate 32 Gbps Fibre Channel ports.

**Figure 14. Cisco MDS 9132T 32G Multilayer Fabric Switch**



The Cisco MDS 9132T delivers advanced storage networking features and functions with ease of management and compatibility with the entire Cisco MDS 9000 family portfolio for reliable end-to-end connectivity. 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 in-



---

cludes a dedicated 10/100/1000BASE-T telemetry port to maximize data delivery to any telemetry receiver, including Cisco Data Center Network Manager.

## 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.

## NetApp AFF A-Series Storage

NetApp AFF A-Series controller lineup provides industry leading performance while continuing to provide a full suite of enterprise-grade data management and data protection features. AFF A-Series systems support end-to-end NVMe technologies, from NVMe-attached SSDs to frontend NVMe over Fibre Channel (NVMe/FC) host connectivity. These systems deliver enterprise class performance, making them a superior choice for driving the most demanding workloads and applications. With a simple software upgrade to the modern NVMe/FC SAN infrastructure, you can drive more workloads with faster response times, without disruption or data migration. Additionally, more and more organizations are adopting a “cloud first” strategy, driving the need for enterprise-grade data services for a shared environment across on-premises data centers and the cloud. As a result, modern all-flash arrays must provide robust data services, integrated data protection, seamless scalability, and new levels of performance – plus deep application and cloud integration. These new workloads demand performance that first-generation flash systems cannot deliver.

For more information about the NetApp AFF A-series controllers, see the AFF product page:

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

You can view or download more technical specifications of the AFF A-series controllers here:

<https://www.netapp.com/us/media/ds-3582.pdf>

## 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.

**Note:** Cisco UCS X-Series is supported with all NetApp AFF systems running NetApp ONTAP 9 release.

**Figure 15. NetApp AFF A400 Front View**



**Figure 16. NetApp AFF A400 Rear View**



## 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 FAS or AFF 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>.



---

## NetApp Active IQ Unified Manager

NetApp Active IQ 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. The Unified Manager can be deployed 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 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 virtual machines running on it. When an issue occurs on the storage infrastructure, Unified Manager can notify you about the details of the issue to help with identifying the root cause. The virtual machine 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 configure custom alerts for events so that when issues occur, you are notified through email and SNMP Traps. Active IQ Unified Manager enables planning for the storage requirements of your users by forecasting capacity and usage trends to proactively act before issues arise, preventing reactive short-term decisions that can lead to additional problems in the long term.

## 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

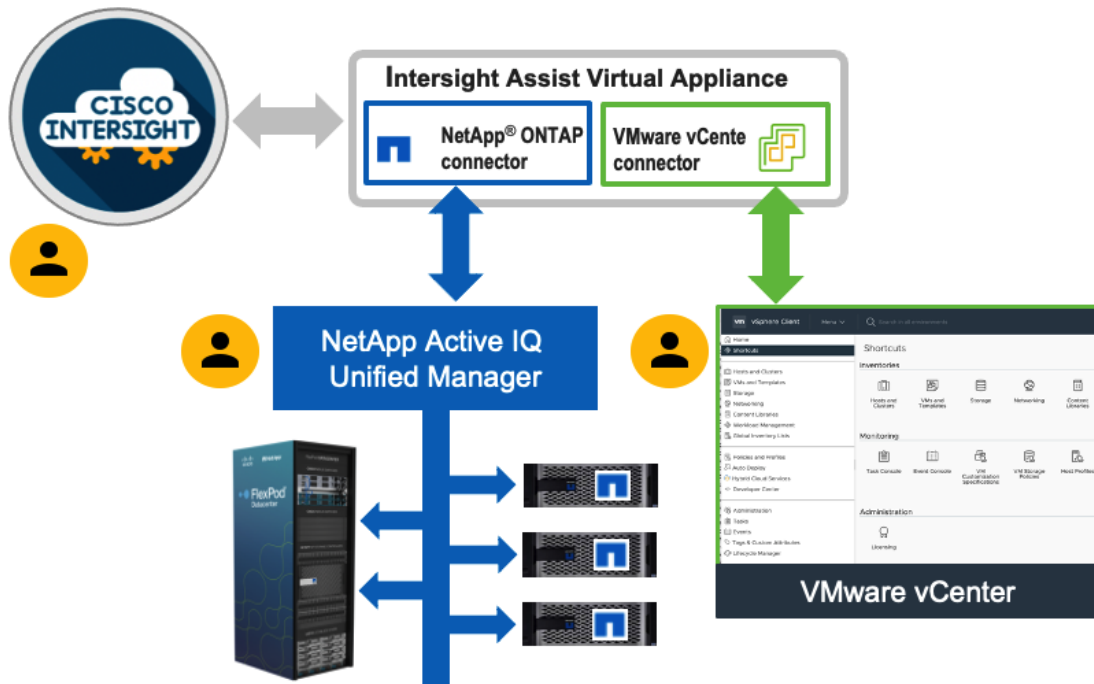
VMware vCenter Server provides unified management of all hosts and VMs from a single console and aggregates performance monitoring of clusters, hosts, and VMs. VMware vCenter Server gives administrators a deep insight into the status and configuration of compute clusters, hosts, VMs, storage, the guest 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 17. 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.

---

## Citrix Virtual Apps & Desktops 7 LTSR

This chapter is organized into the following subjects:

- [Key Benefits](#)
- [Citrix Provisioning Services 7 LTSR](#)

Enterprise IT organizations are tasked with the challenge of provisioning Microsoft Windows apps and desktops while managing cost, centralizing control, and enforcing corporate security policy. Deploying Windows apps to users in any location, regardless of the device type and available network bandwidth, enables a mobile workforce that can improve productivity. With Citrix Virtual Apps & Desktops 7 LTSR, IT can effectively control app and desktop provisioning while securing data assets and lowering capital and operating expenses.

The Citrix Virtual Apps & Desktops 7 LTSR release offers these benefits:

- **Comprehensive virtual desktop delivery for any use case.** The Citrix Virtual Apps & Desktops 7 LTSR release incorporates the full power of RDS, delivering full desktops or just applications to users. Administrators can deploy both RDS published applications and desktops (to maximize IT control at low cost) or personalized VDI desktops (with simplified image management) from the same management console. Citrix Virtual Apps & Desktops 7 LTSR leverages common policies and cohesive tools to govern both infrastructure resources and user access.
- **Simplified support and choice of BYO (Bring Your Own) devices.** Citrix Virtual Apps & Desktops 7 LTSR brings thousands of corporate Microsoft Windows-based applications to mobile devices with a native-touch experience and optimized performance. HDX technologies create a “high definition” user experience, even for graphics intensive design and engineering applications.
- **Lower cost and complexity of application and desktop management.** Citrix Virtual Apps & Desktops 7 LTSR helps IT organizations take advantage of agile and cost-effective cloud offerings, allowing the virtualized infrastructure to flex and meet seasonal demands or the need for sudden capacity changes. IT organizations can deploy Citrix Virtual Apps & Desktops application and desktop workloads to private or public clouds.
- **Protection of sensitive information through centralization.** Citrix Virtual Apps & Desktops decreases the risk of corporate data loss, enabling access while securing intellectual property and centralizing applications since assets reside in the datacenter.
- **Virtual Delivery Agent improvements.** Universal print server and driver enhancements and support for the HDX 3D Pro graphics acceleration for Windows 10 are key additions in Citrix Virtual Apps & Desktops 7 LTSR
- **Improved high-definition user experience.** Citrix Virtual Apps & Desktops 7 LTSR continues the evolutionary display protocol leadership with enhanced Thinwire display remoting protocol and Framehawk support for HDX 3D Pro.

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

---

## Citrix RDS delivers:

- RDS published apps, also known as server-based hosted applications: These are applications hosted from Microsoft Windows servers to any type of device, including Windows PCs, Macs, smartphones, and tablets. Some RDS editions include technologies that further optimize the experience of using Windows applications on a mobile device by automatically translating native mobile-device display, navigation, and controls to Windows applications; enhancing performance over mobile networks; and enabling developers to optimize any custom Windows application for any mobile environment.
- RDS published desktops, also known as server-hosted desktops: These are inexpensive, locked-down Windows virtual desktops hosted from Windows server operating systems. They are well suited for users, such as call center employees, who perform a standard set of tasks.
- Virtual machine-hosted apps: These are applications hosted from machines running Windows desktop operating systems for applications that can't be hosted in a server environment.
- Windows applications delivered with Microsoft App-V: These applications use the same management tools that you use for the rest of your RDS deployment.
- Citrix Virtual Apps & Desktops: Includes significant enhancements to help customers deliver Windows apps and desktops as mobile services while addressing management complexity and associated costs. Enhancements in this release include:
  - Unified product architecture for RDS and Citrix Virtual Apps & Desktops: The FlexCast Management Architecture (FMA). This release supplies a single set of administrative interfaces to deliver both hosted-shared applications (RDS) and complete virtual desktops (VDI). Unlike earlier releases that separately provisioned Citrix RDS and Citrix Virtual Apps & Desktops farms, the Citrix Virtual Apps & Desktops 7 LTSR release allows administrators to deploy a single infrastructure and use a consistent set of tools to manage mixed application and desktop workloads.
  - Support for extending deployments to the cloud. This release provides the ability for hybrid cloud provisioning from Microsoft Azure, Amazon Web Services (AWS) or any Cloud Platform-powered public or private cloud. Cloud deployments are configured, managed, and monitored through the same administrative consoles as deployments on traditional on-premises infrastructure.

## Citrix Virtual Apps & Desktops delivers:

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

---

This product release includes the following new and enhanced features:

**Note:** Some Citrix Virtual Apps & Desktops editions include the features available in RDS.

## Key Benefits

The following are some of the key benefits of Citrix Virtual Apps & Desktops:

### Zones

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

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

For more information, see the [Zones](#) article.

### Improved Database Flow and Configuration

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

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

For more information, see the [Databases](#) and [Controllers](#) articles.

### Application Limits

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

For more information, see the [Manage applications](#) article.

### Multiple Notifications before Machine Updates or Scheduled Restarts

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

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

---

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

For more information, see the [Manage Machine Catalogs](#) and [Manage machines in Delivery Groups](#) articles.

### **API Support for Managing Session Roaming**

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

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

For more information, see the [Sessions](#) article.

### **API Support for Provisioning VMs from Hypervisor Templates**

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

### **Support for New and Additional Platforms**

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

When installing a Controller, Microsoft SQL Server Express LocalDB 2017 with Cumulative Update 16 is installed for use with the Local Host Cache feature. This installation is separate from the default SQL Server Express installation for the site database. (When upgrading a Controller, the existing Microsoft SQL Server Express LocalDB version is not upgraded. If you want to upgrade the LocalDB version, follow the guidance in [Database actions](#)).

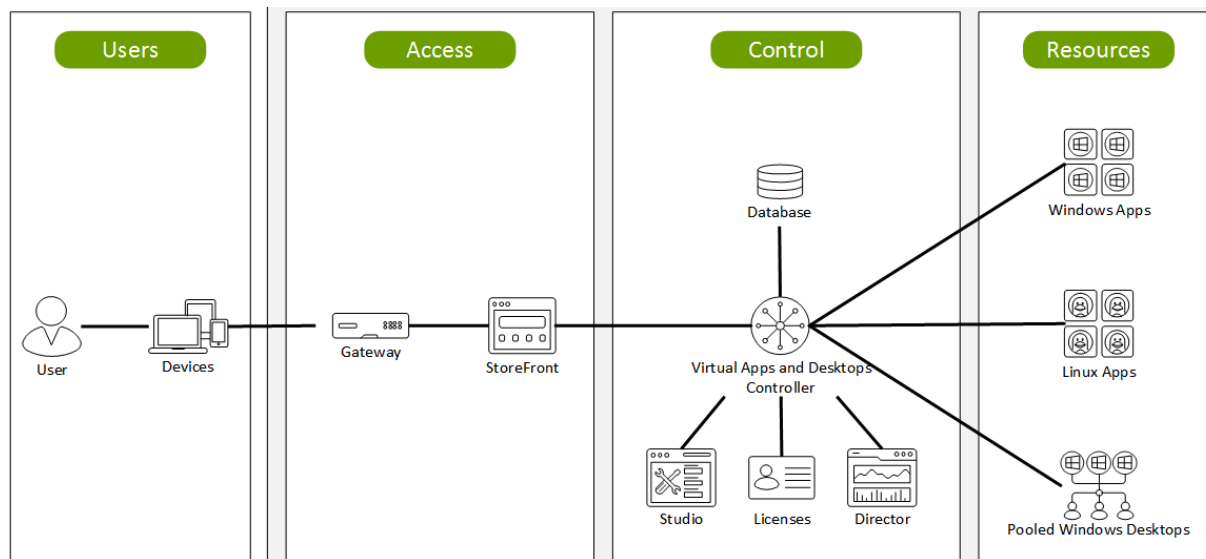
Installing the Microsoft Visual C++ 2017 Runtime on a machine that has the Microsoft Visual C++ 2015 Runtime installed can result in automatic removal of the Visual C++ 2015 Runtime. This is as designed.

If you've already installed Citrix components that automatically install the Visual C++ 2015 Runtime, those components will continue to operate correctly with the Visual C++ 2017 version.

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

You can create connections to Microsoft Azure virtualization resources.

**Figure 18. Logical Architecture of Citrix Virtual Apps & Desktops**



## Citrix Provisioning Services 7 LTSR

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

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

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

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

## Benefits for Citrix RDS and Other Server Farm Administrators

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



---

pens, getting the server resynchronized with the rest of the farm can be challenging, and sometimes a full reimaging of the machine is required.

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

### **Benefits for Desktop Administrators**

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

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

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

### **Citrix Provisioning Services Solution**

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

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

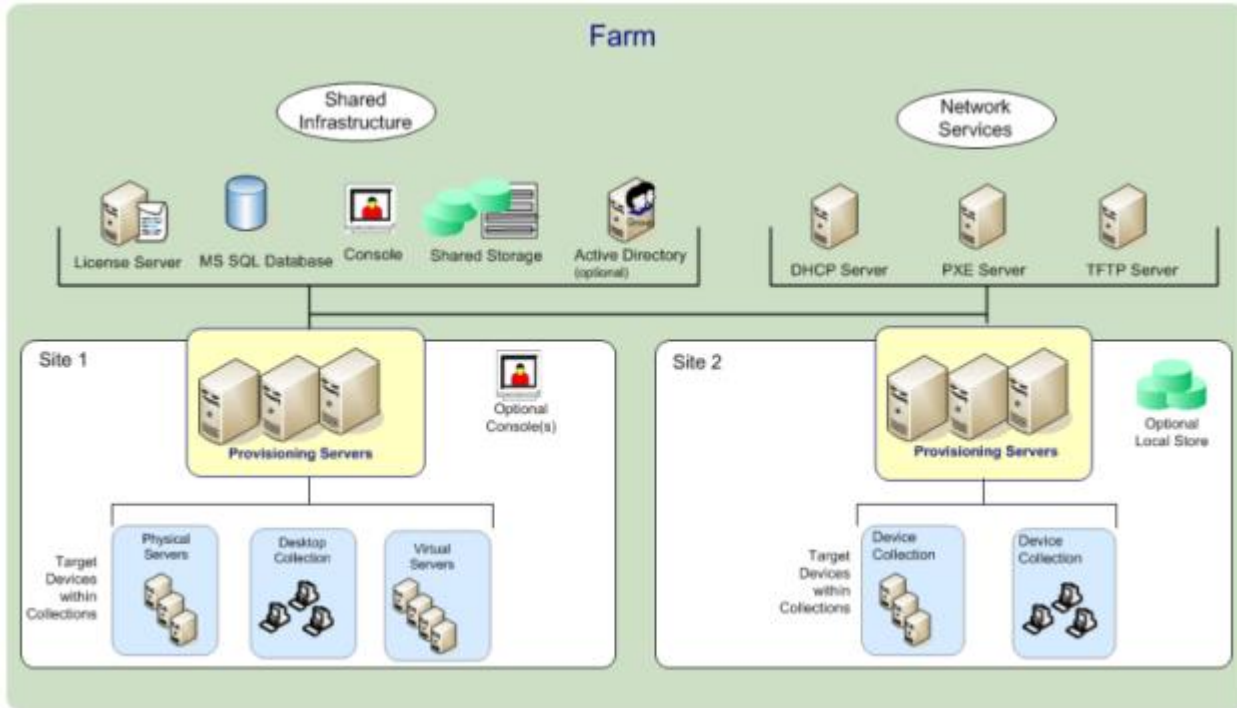


## Citrix Provisioning Services Infrastructure

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

A PVS farm contains several components. [Figure 19](#) provides a high-level view of a basic PVS infrastructure and shows how PVS components might appear within that implementation.

**Figure 19. Logical Architecture of Citrix Provisioning Services**



The following new features are available with Provisioning Services 7 LTSR:

- Linux streaming
- Citrix Hypervisor proxy using PVS-Accelerator

## NetApp A-Series All Flash FAS

This chapter is organized into the following subjects:

- [NetApp A-Series All Flash FAS](#)
- [NetApp ONTAP 9.9](#)
- [Space Savings](#)
- [ONTAP Tools for VMware vSphere](#)
- [NetApp NFS Plug-in for VMware VAAI](#)
- [NetApp SnapCenter Plug-In for VMware vSphere 4.4](#)
- [NetApp Active IQ Unified Manager 9.8](#)
- [NetApp XCP File Analytics](#)

NetApp® All Flash FAS (AFF) 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.

The NetApp AFF A400 offers full end-to-end NVMe support at the midrange. The front-end NVMe/FC connectivity makes it possible to achieve optimal performance from an all-flash array for workloads that include Virtual Desktop Environments. The AFF A-Series lineup includes the A200, A400, A700, and A800. These controllers and their specifications 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://www.netapp.com/pdf.html?item=/media/7828-ds-3582.pdf>

<https://hwu.netapp.com/Controller/Index?platformTypeld=13684325>

**Table 1. NetApp A-Series Controller Specifications**

Specifications	AFF A250	AFF A400	AFF A700
Max Raw capacity (HA)	1101.6 TB	14688 TB	14688 TB
Max Storage Devices (HA)	48 (drives)	480 (drives)	480 (drives)
Processor Speed	2.10 Ghz	2.20 Ghz	2.30 Ghz
Total Processor Cores (Per Node)	12	20	35
Total Processor Cores (Per HA)	24	40	72

Specifications	AFF A250	AFF A400	AFF A700
Pair)			
Memory	128 GB	256 GB	1024 GB
NVRAM	N/A	32 GB	64 GB
Ethernet Ports	4 x RJ45 (10Gb)	4 x QSFP28 (40Gb) 8 x SFP28 (25Gb)	24x IO Module
Rack Units	2	4	8
Maximum number of storage virtual machines (SVMs) - SAN	HA Pair - 250 Cluster - 1000	HA Pair - 250 Cluster - 1000	HA Pair - 250 Cluster - 1000
Maximum number of flexible volumes - SAN	HA Pair - 400 Cluster - 1600	HA Pair - 400 Cluster - 1600	HA Pair - 400 Cluster - 1600

This solution utilizes the NetApp AFF A400, seen in [Figure 20](#) and [Figure 21](#). The NetApp AFF A400 offers greater port availability, network connectivity, and expandability. When buying a storage system, most customers plan to use it for 3 to 5 years, but it's difficult to predict how requirements may change during that time frame. The NetApp AFF A400 has 10 PCIe Gen3 slots per HA pair. Many customers have a strong preference for additional I/O capabilities, and now with the NetApp AFF A400, the increased number of PCIe Gen3 slots makes additional I/O possible.

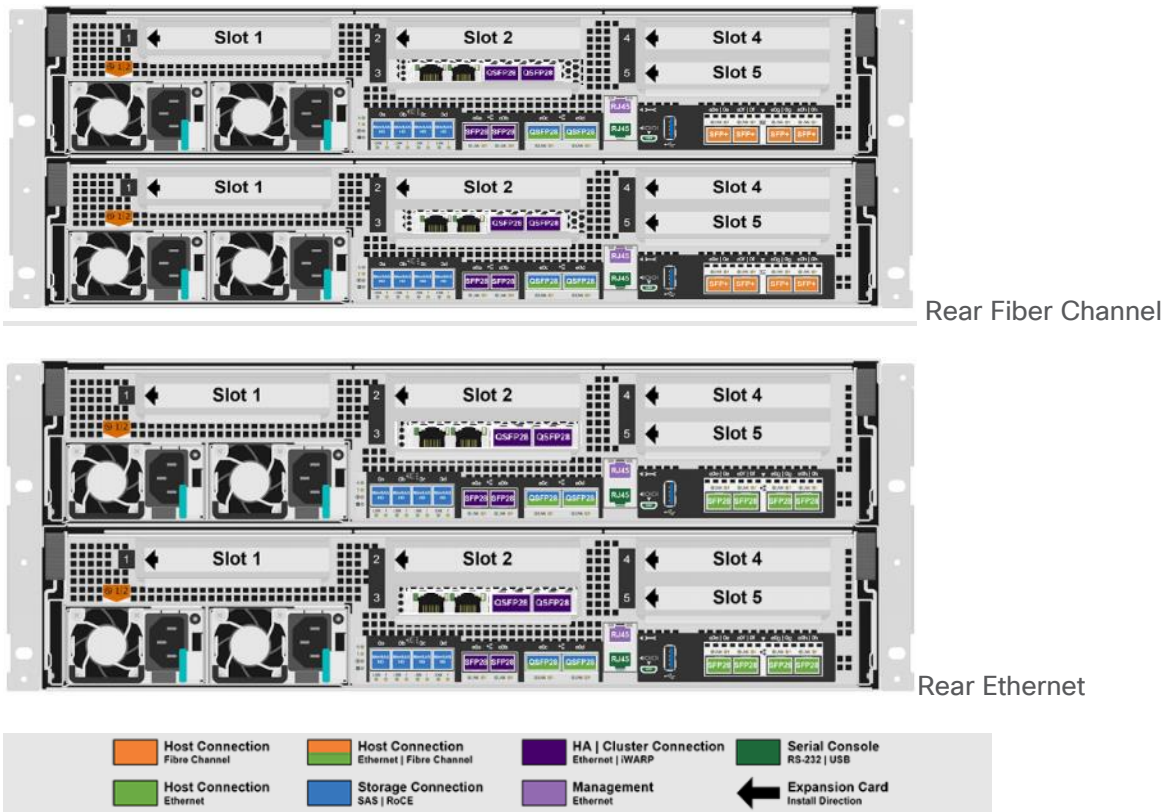
The NetApp AFF A400 offers 25GbE or 100GbE, as well as 32Gb/FC and NVMe/FC network connectivity, which is at the leading edge of a midrange system. This model was created to keep up with changing business needs and performance and workload requirements by merging the latest technology for data acceleration and ultra-low latency in an end-to-end NVMe storage system, along with additional slots for expansion.

For more information about the AFF A-Series product family, see: <http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx>

**Figure 20. NetApp AFF A400 Front View**



Figure 21. 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 9.9

### 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 & 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 **Error!**  
**Reference source not found.**

## 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 22](#)).

Figure 22. Storage Efficiency Features

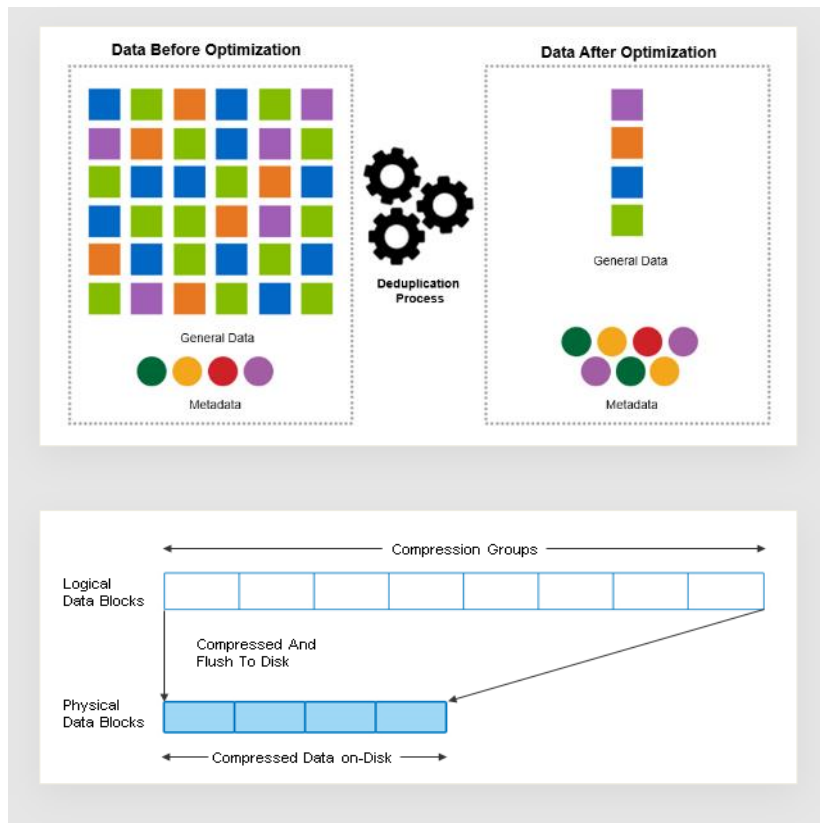
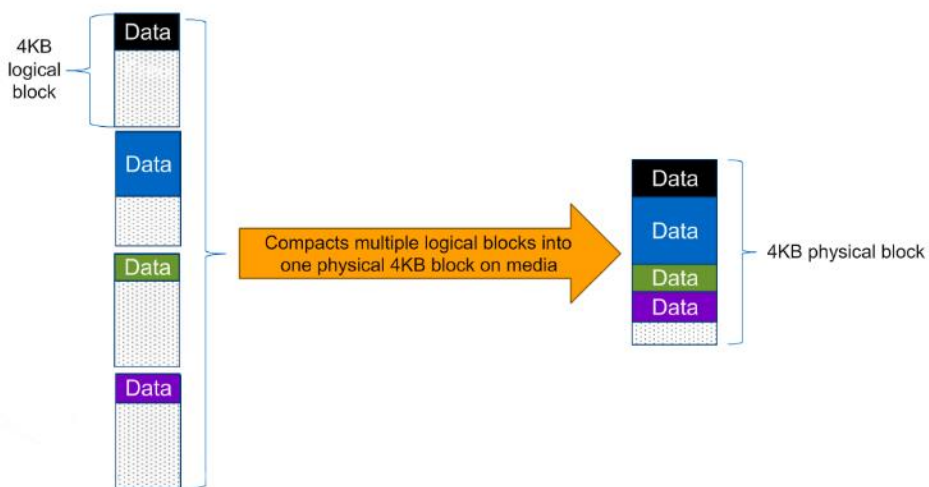


Figure 23. Storage Efficiency



**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 compres-



---

sion 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)	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Inline zero-block deduplication</li> <li>• Inline deduplication (Data ONTAP 8.3.2 and above)</li> </ul>	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Inline zero-block deduplication</li> <li>• Inline deduplication (Data ONTAP 8.3.2 and above)</li> </ul>	<p>For primary workloads, use:</p> <ul style="list-style-type: none"> <li>• Inline zero-block deduplication</li> </ul> <p>For secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Adaptive background compression</li> <li>• Inline zero-block deduplication</li> </ul>
VDI and SVI	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> <li>• Inline deduplication (Data ONTAP 8.3.2 and above)</li> </ul>	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> <li>• Inline deduplication (Data ONTAP 8.3.2 and above)</li> </ul>	<p>For primary workloads, use:</p> <ul style="list-style-type: none"> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul> <p>For secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Adaptive background compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>
Exchange	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Set schedule to off peak hours</li> <li>• Inline zero-block</li> </ul>	<p>For primary and secondary workloads, use:</p> <ul style="list-style-type: none"> <li>• Inline secondary compression</li> <li>• Background secondary compression</li> <li>• Deduplication</li> </ul>

Workload	Storage Efficiency Guidelines		
		deduplication	<ul style="list-style-type: none"> <li>• Inline zero-block deduplication</li> </ul>
<b>File Services</b>	For primary and secondary workloads, use: <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>	For primary and secondary workloads, use: <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>	For primary and secondary workloads, use: <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Adaptive background compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>
<b>Mixed Workload</b>	For primary and secondary workloads, use: <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>	For primary and secondary workloads, use: <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>	For primary workloads, use: <ul style="list-style-type: none"> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul> For secondary workloads, use: <ul style="list-style-type: none"> <li>• Adaptive inline compression</li> <li>• Adaptive background compression</li> <li>• Deduplication</li> <li>• Inline zero-block deduplication</li> </ul>

## 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

## Typical Savings Ratios with ONTAP 9

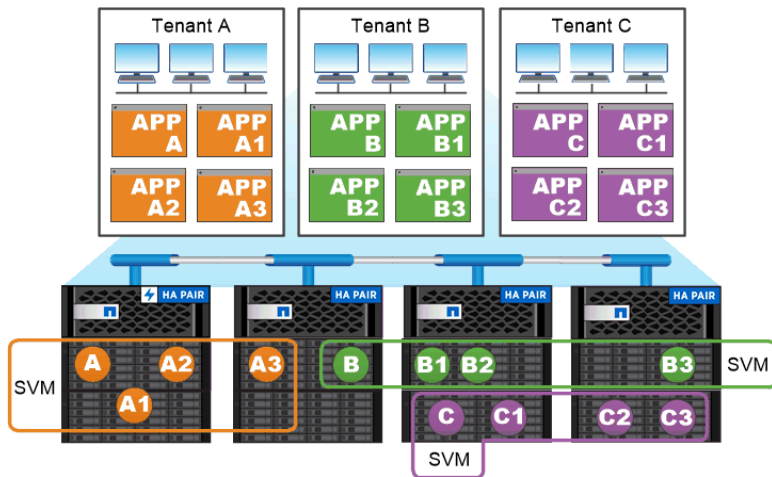
Software development	2:1 - 10:1
VDI VMware Horizon full clone desktops (persistent) - NetApp Clones	6:1 - 10:1
VDI VMware Horizon linked clone desktops (nonpersistent)	5:1 - 7:1
VDI Citrix Virtual Apps & Desktops full clone desktops (persistent) - NetApp Clones	6:1 - 10:1
VDI Citrix Virtual Apps & Desktops MCS desktops (nonpersistent)	5:1 - 7:1
VDI Citrix Provisioning services desktops (nonpersistent)	3.3:1 - 5:1
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
Precompressed data (such as video and image files, audio files, pdfs, etc.)	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 24. NetApp Storage Virtual Machine**



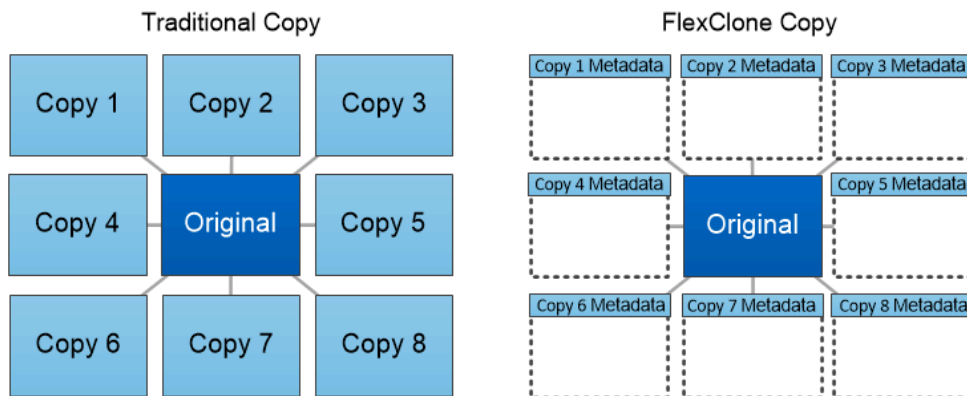
*Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.*

## 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.



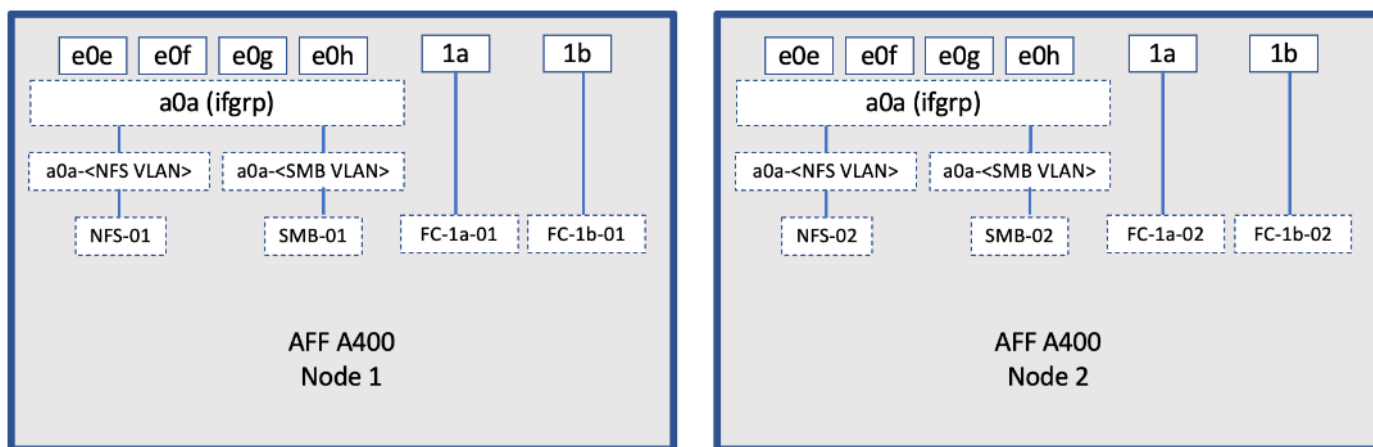
*FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.*

## 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 16G 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 25](#) shows the port and LIF layout

Figure 25. FC - SVM ports and LIF layout

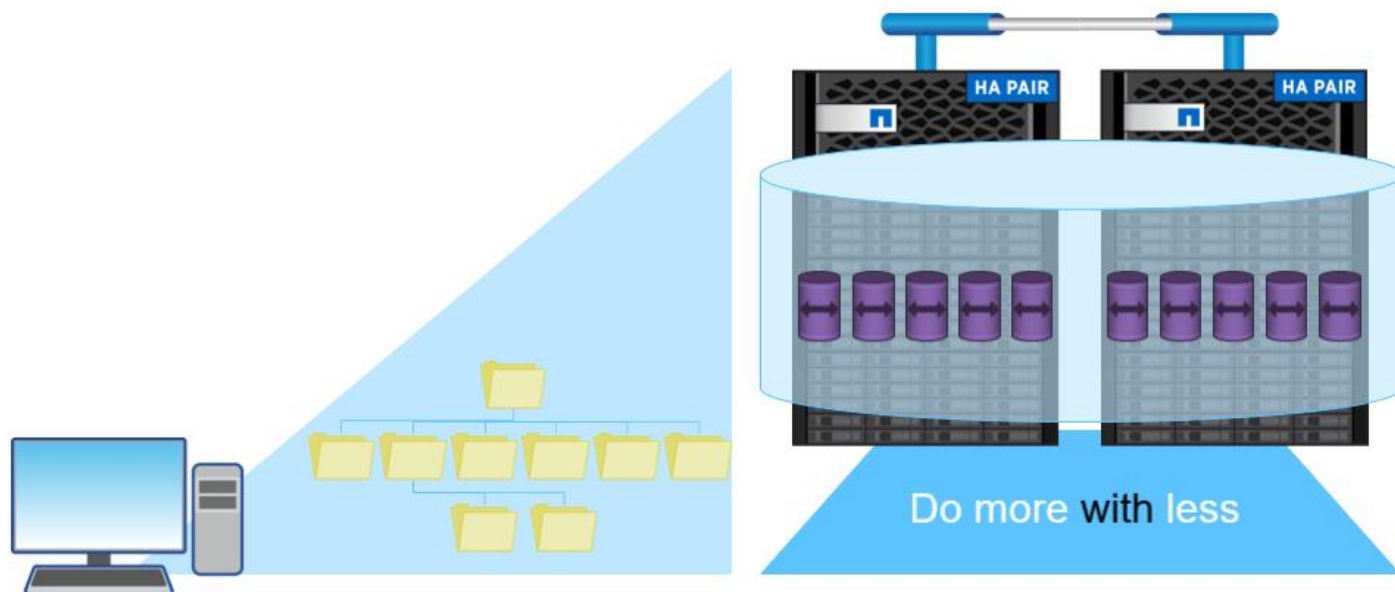


Unlike NAS network interfaces, the SAN network interfaces are not configured to fail over during a failure. Instead if a network interface becomes unavailable, the ESXI host chooses a new optimized path to an available network interface. ALUA is a standard supported by NetApp used to provide information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



## 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:

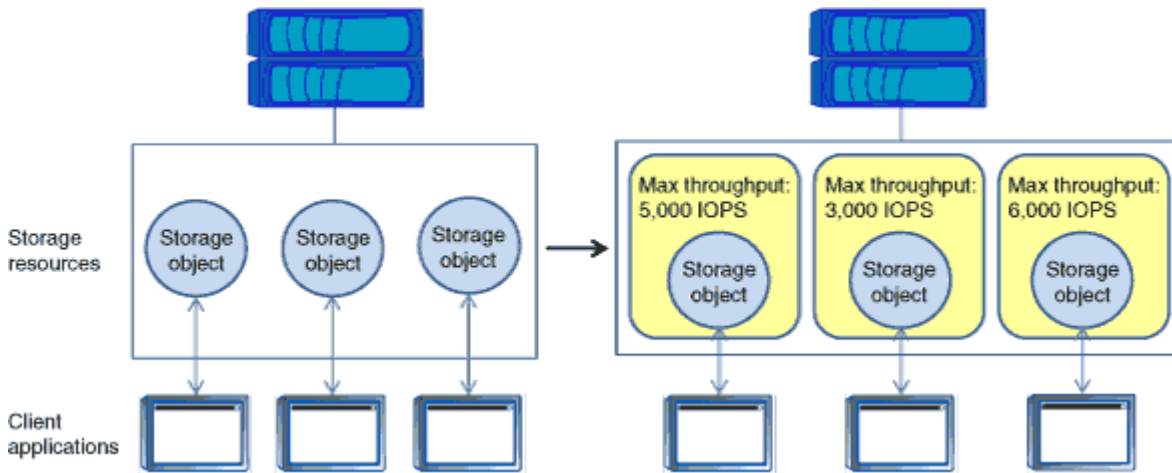
- FlexVol volumes
- LUNs

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

[Figure 26](#) shows 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 26. 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

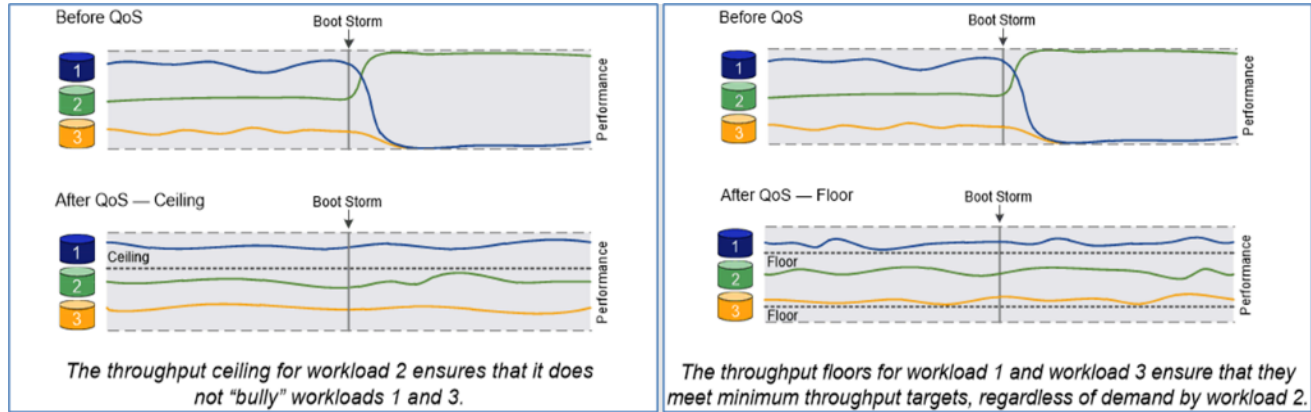
Adaptive QoS automatically scales the policy group (A *policy group* defines the throughput ceiling for one or more workloads) value to workload (A *workload* represents the I/O operations for a storage object: a volume, file, qtree or LUN, or all the volumes, files, qtrees, or LUNs in an SVM) size, 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 shown 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	Peck IOPS/TB	Absolute Min IOPS
Extreme	6,144	12,288	1000
Performance	2,048	4,096	500

Default Policy Group	Expected IOPS/TB	Peck IOPS/TB	Absolute Min IOPS
Value	128	512	75



## Security and Data Protection

### Vscan

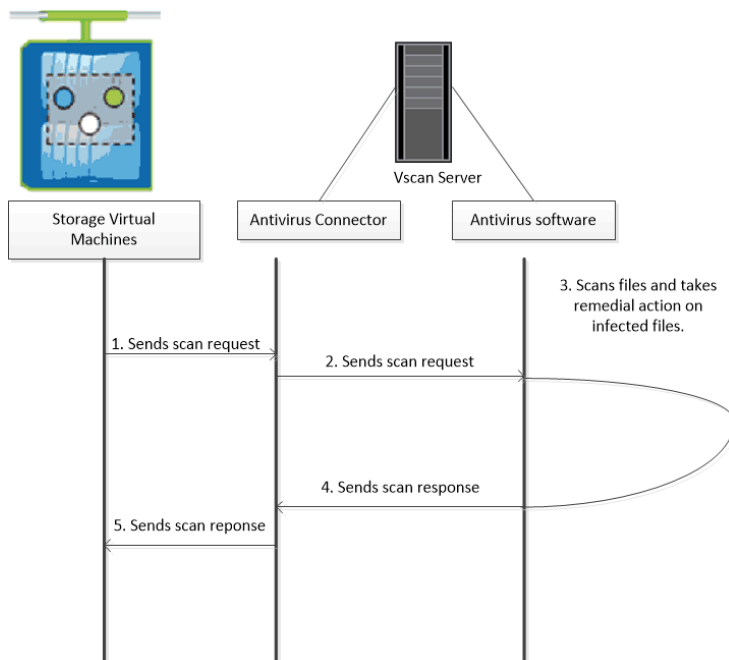
With Vscan you can use integrated antivirus functionality on NetApp storage systems to protect data from being compromised by viruses or other malicious code. NetApp virus scanning, called Vscan, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you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

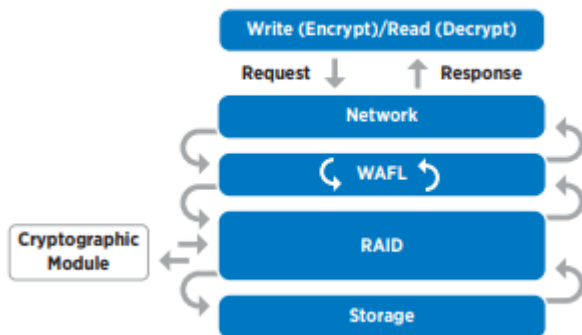


### NetApp Volume Encryption(NVE) and NetApp Aggregate Encryption (NAE)

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 Crypto-Mod, and is then sent up the rest of the stack. This process is outlined in [Figure 27](#).

Figure 27. 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.

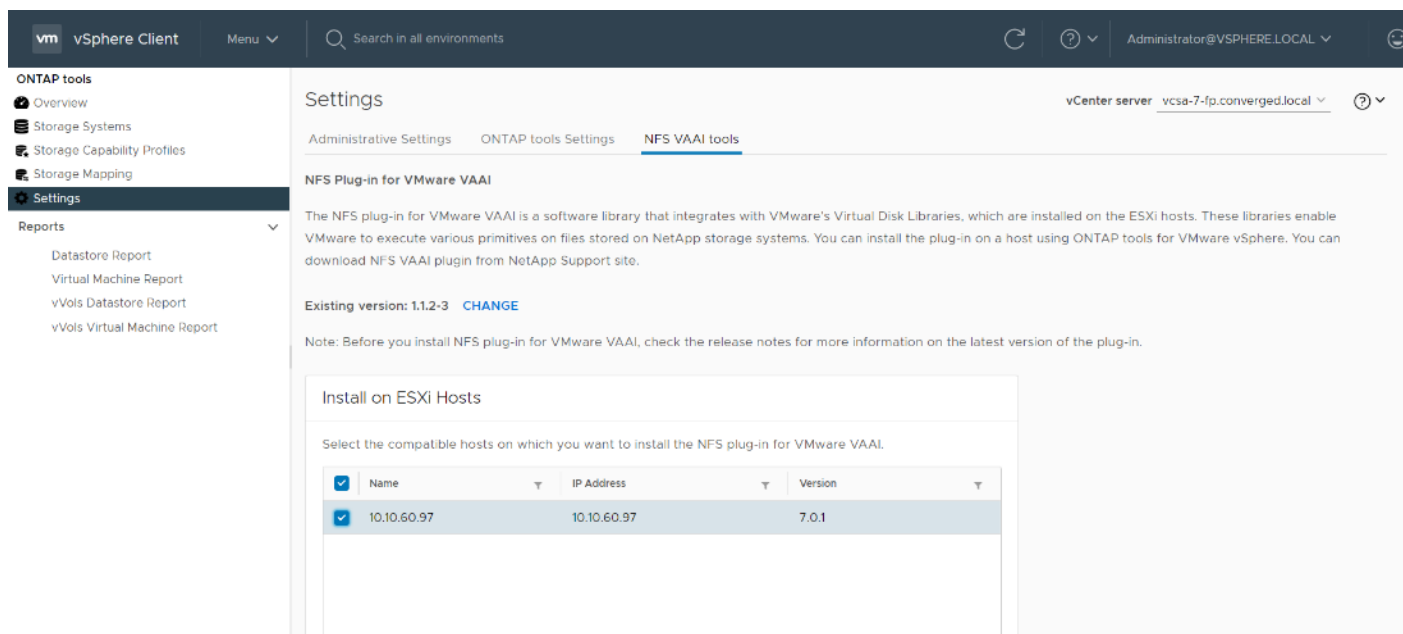
## ONTAP Tools for VMware vSphere

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 & 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.

## 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.

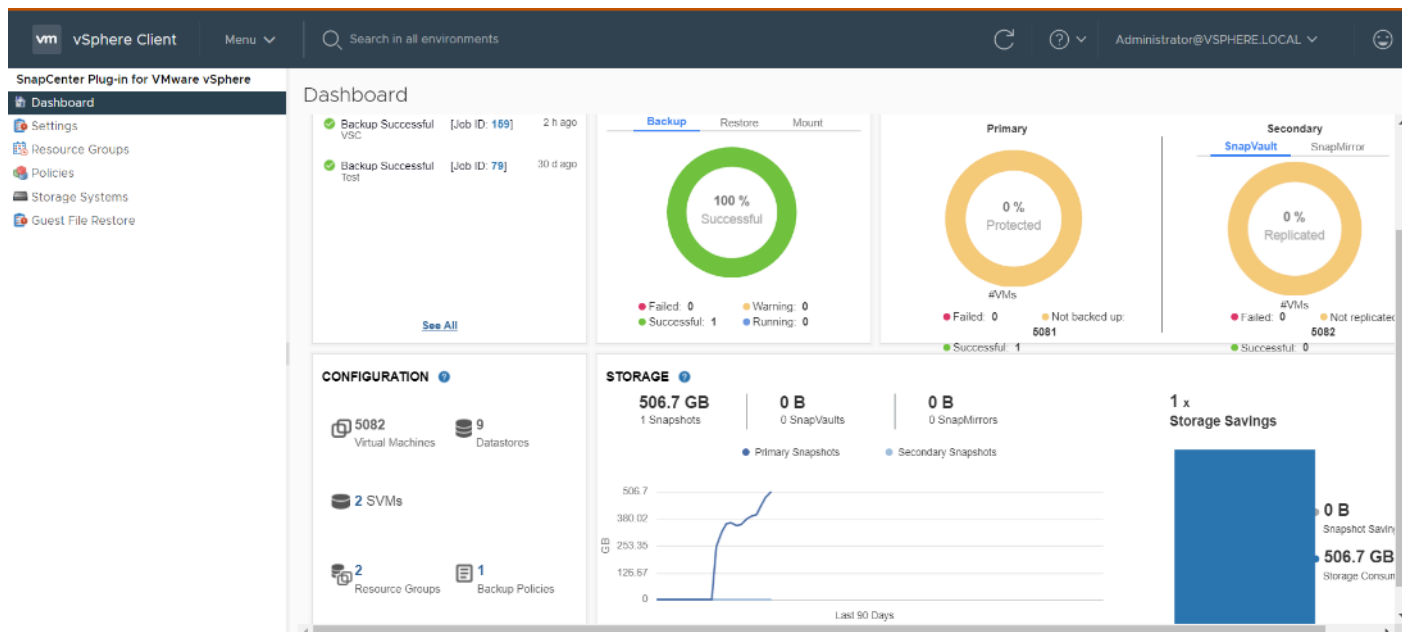


The copy offload feature and space reservation feature improve the performance of VSC operations. The NetApp NFS Plug-in for VAAI is not shipped with VSC, but you can install it by using VSC. You can download the plug-in installation package and obtain the instructions for installing the plug-in from 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 4.4

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.



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.

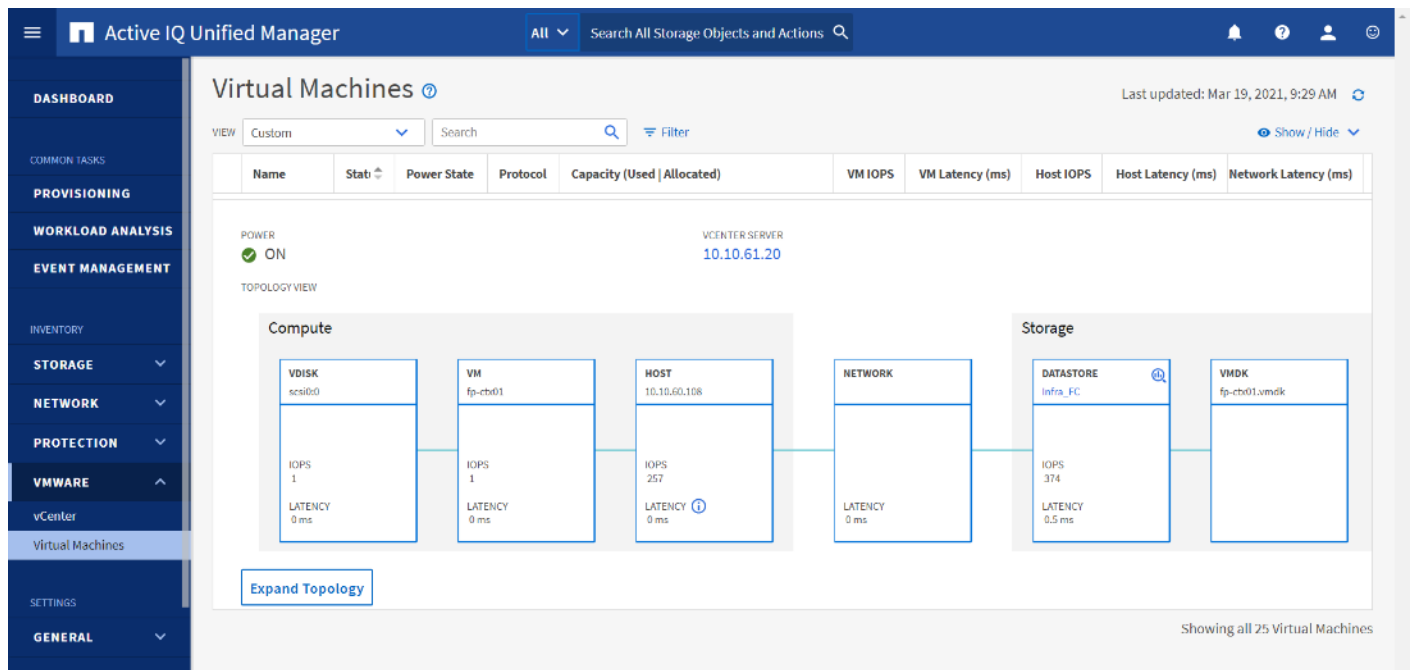
**Note:** For additional information, requirements, licensing, and limitations of the NetApp SnapCenter Plug-In for VMware vSphere, see the NetApp Product Documentation.

## NetApp Active IQ Unified Manager 9.8

NetApp Active IQ 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.

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.



## 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. 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 is organized into the following subjects:

- [Understanding Applications and Data](#)
- [Project Planning and Solution Sizing Sample Questions](#)
- [Hypervisor Selection](#)
- [Citrix Virtual Apps & Desktops Design Fundamentals](#)
- [Example Citrix Virtual Apps & Desktops Deployments](#)

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 2016, 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 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 type 1 hypervisor and is synced with the data center when the device is connected to the network.

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

## Understanding Applications and Data

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

The process of analyzing the variety of application and data pairs for an organization will likely be complicated by the inclusion cloud applications, 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 HSD Sessions and HVD based 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 7.02 Update 1.

Server OS and Desktop OS Machines configured in this CVD to support Remote Desktop Server Hosted (RDSH) shared sessions and Hosted Virtual Desktops (both non-persistent and persistent).

## Citrix Virtual Apps & 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 & Desktops 7 LTSR integrates Hosted Shared and VDI desktop virtualization technologies into a unified architecture that enables a scalable, simple, efficient, and manageable solution for delivering Windows applications and desktops as a service.

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

## Machine Catalogs

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

## Delivery Groups

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

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

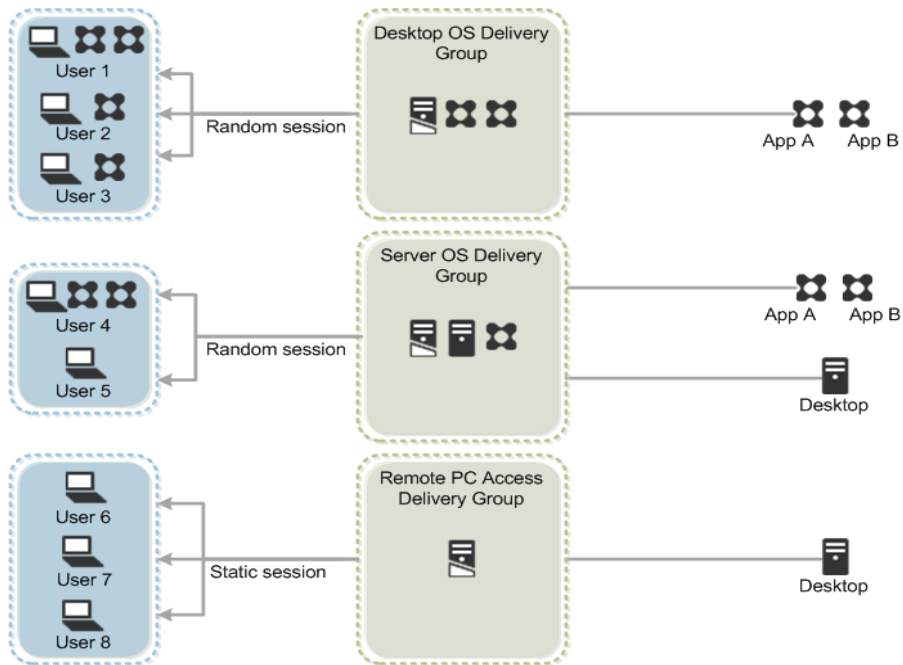
As part of the creation process, you specify the following Delivery Group properties:

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

[Figure 28](#) illustrates how users access desktops and applications through machine catalogs and delivery groups.

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

Figure 28. Access Desktops and Applications through Machine Catalogs and Delivery Groups



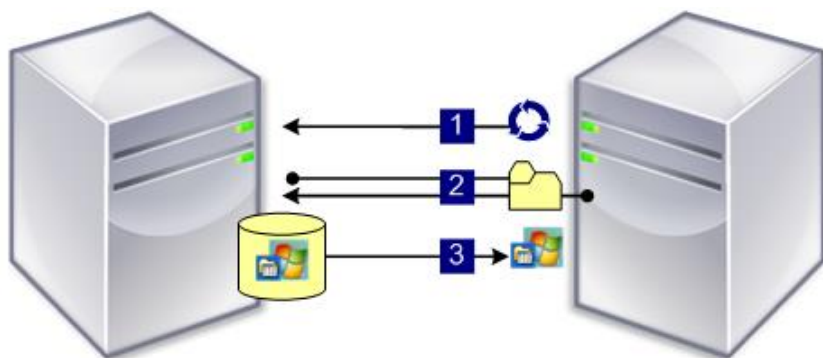
### Citrix Provisioning Services

Citrix Virtual Apps & Desktops 7 LTSR 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 for 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 29. 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 Citrix Virtual Apps & 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 7 LTSR was used to manage Pooled/Non-Persistent VDI Machines and RDS Machines with “Cache in device RAM with Overflow on Hard Disk” for each virtual machine. This design enables good scalability to many thousands of desktops. Provisioning Server 7 LTSR 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 & Desktops Deployments

Two examples of typical Citrix Virtual Apps & Desktops deployments are the following:

- A distributed components configuration
- A multiple site configuration

Since RDS and Citrix Virtual Apps & Desktops 7 LTSR are based on a unified architecture, combined they can deliver a combination of Hosted Shared Desktops (HSDs, using a Server OS machine) and Hosted Virtual Desktops (HVDs, using a Desktop OS).

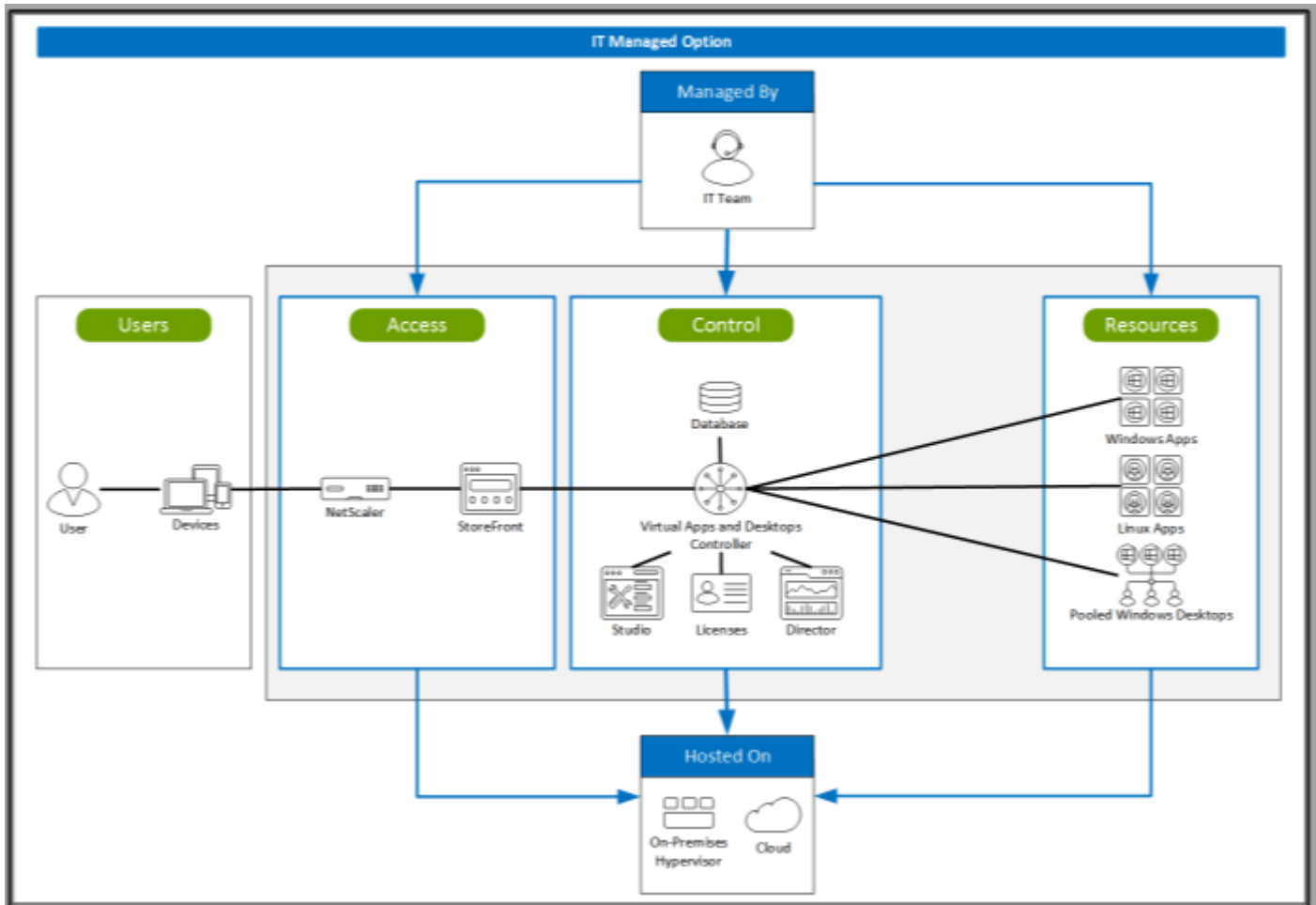
### Distributed Components Configuration

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

[Figure 30](#) 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 & Desktops in a configuration that resembles this distributed components configuration shown. Eight HX220 M5 servers host the required infrastructure services (AD, DNS, DHCP, License Server, SQL, Citrix Virtual Apps & Desktops management, and StoreFront servers).



Figure 30. Example of a Distributed Components Configuration

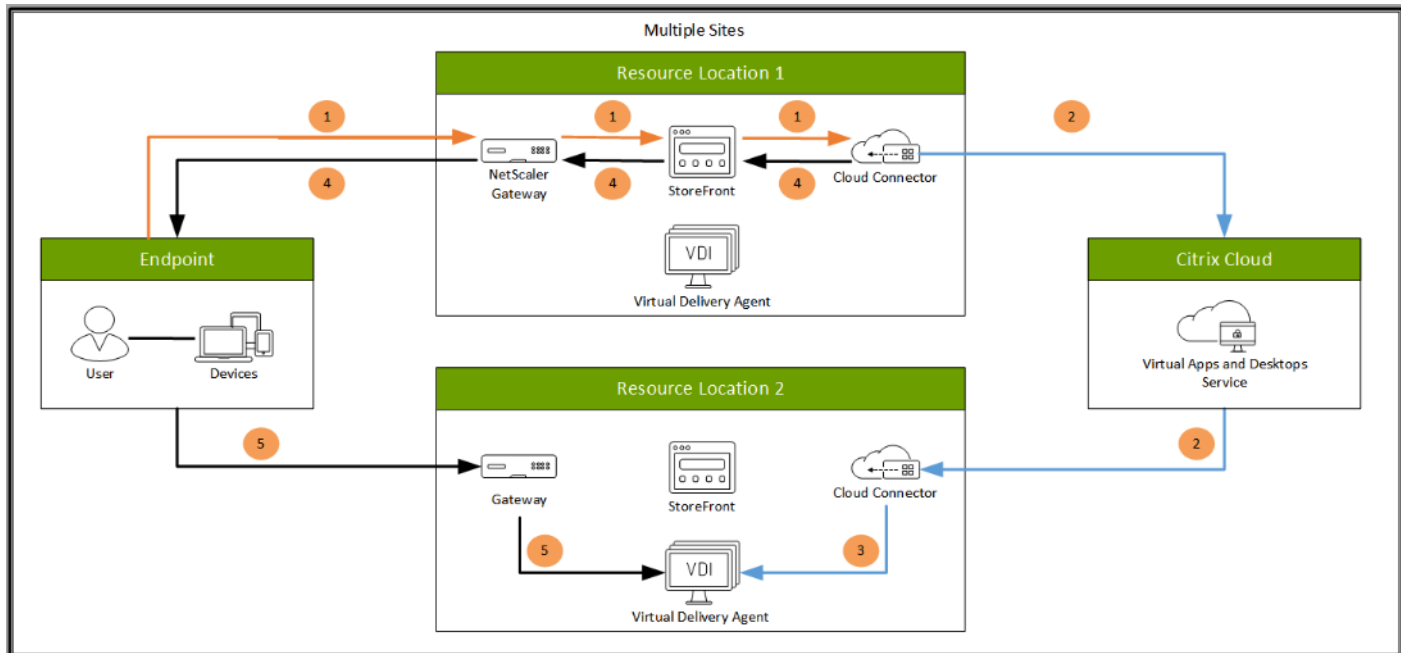


### Multiple Site Configuration

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 31](#) depicts multiple sites with a site created in two data centers. Having two sites globally, rather than just one, minimizes the amount of unnecessary WAN traffic.

**Figure 31. Multiple Sites**



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

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

### Citrix Cloud Services

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

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

### Designing a Citrix Virtual Apps & Desktops Environment for a Mixed Workload

With Citrix Virtual Apps & Desktops 7 LTSR, 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 for the types of users and user experience you want to provide.

Method	Experience
Server OS machines	<p>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.</p> <p>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.</p> <p>Application types: Any application.</p>
Desktop OS machines	<p>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.</p> <p>Your users: Are internal, external contractors, third-party collaborators, and other provisional team members. Users do not require off-line access to hosted applications.</p> <p>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.</p> <p>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.</p>
Remote PC Access	<p>You want: Employees with secure remote access to a physical computer without using a VPN. For example, the user may be accessing their physical desktop PC from home or through a public WIFI hotspot. Depending upon the location, you may want to restrict the ability to print or copy and paste outside of the desktop. This method enables BYO device support without migrating desktop images into the datacenter.</p> <p>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.</p> <p>Host: The same as Desktop OS machines.</p> <p>Application types: Applications that are delivered from an office computer and display seamlessly in high definition on the remote user's device.</p>

For the Cisco Validated Design described in this document, a mix of Windows Server 2019 based Hosted Shared Desktops sessions (RDS), and Windows 10 Hosted Virtual desktops (Statically assigned Persistent and Random Pooled) were configured and tested.

---

## Deployment Hardware and Software

This chapter is organized into the following subjects:

- [Products Deployed](#)
- [Logical Architecture](#)
- [Software Revisions](#)
- [Configuration Guidelines](#)

### Products Deployed

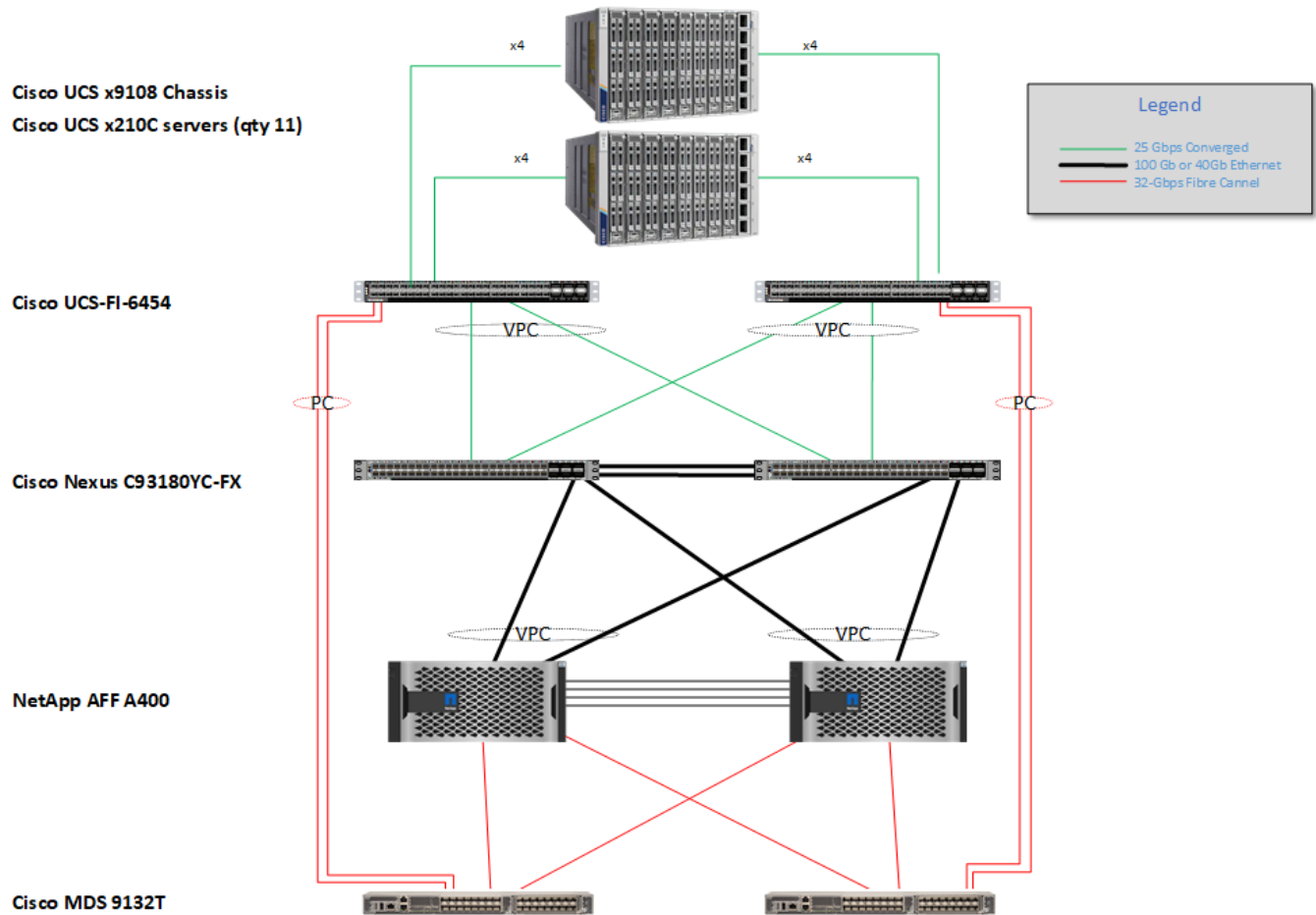
The architecture deployed is highly modular. While each customer's environment might vary in its exact configuration, once the reference architecture contained in this document is built, it can easily be scaled as requirements and demands change. This includes scaling both up (adding additional resources within a Cisco UCS Domain) and out (adding additional Cisco UCS Domains and NetApp AFF Storage platform).

The Citrix solution includes Cisco networking, Cisco UCS, and NetApp AFF storage, which efficiently fits into a single data center rack, including the access layer network switches.

This validated design document details the deployment of the multiple configurations extending to 2500 users for a mixed Citrix Virtual Apps & Desktops workload featuring the following software:

- Citrix RDS 7 LTSR Hosted Shared Virtual Desktops (HSD) with PVS write cache on NFS storage
- Citrix Virtual Apps & Desktops 7 LTSR Non-Persistent Hosted Virtual Desktops (HVD) with PVS write cache on NFS storage
- Citrix Virtual Apps & Desktops 7 LTSR Persistent Hosted Virtual Desktops (VDI) provisioned with MCS and stored on NFS storage
- Citrix Provisioning Server 7 LTSR
- FSlogix for Profile Management
- Citrix StoreFront 7 LTSR
- VMware vSphere ESXi 7.02 Hypervisor
- Microsoft Windows Server 2019 and Windows 10 (build 2004) 64-bit virtual machine Operating Systems
- Microsoft SQL Server 2017

Figure 32. Virtual Desktop and Application Workload Architecture



The workload contains the following hardware as shown in [Figure 32](#):

- Two Cisco Nexus 93180YC-FX Layer 2 Access Switches
- Two Cisco UCS X9508 chassis with two built-in UCS 9108-25G IO Modules
- Cisco UCS HX220c rack servers with Intel Xeon Scalable 6320 2.20-GHz 20-core processors, 768GB 2666MHz RAM, and one Cisco VIC1440 mezzanine card for the hosted infrastructure, providing N+1 server fault tolerance
- 11 Cisco UCS X-Series Compute Nodes M6 Blade Servers with Intel Xeon Gold 6348 2.60-GHz 28-core processors, 1TBGB 3200MHz RAM, and one Cisco VIC 14425 mezzanine card for the desktop workload, providing N+1 server fault tolerance at the workload cluster level
- 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.

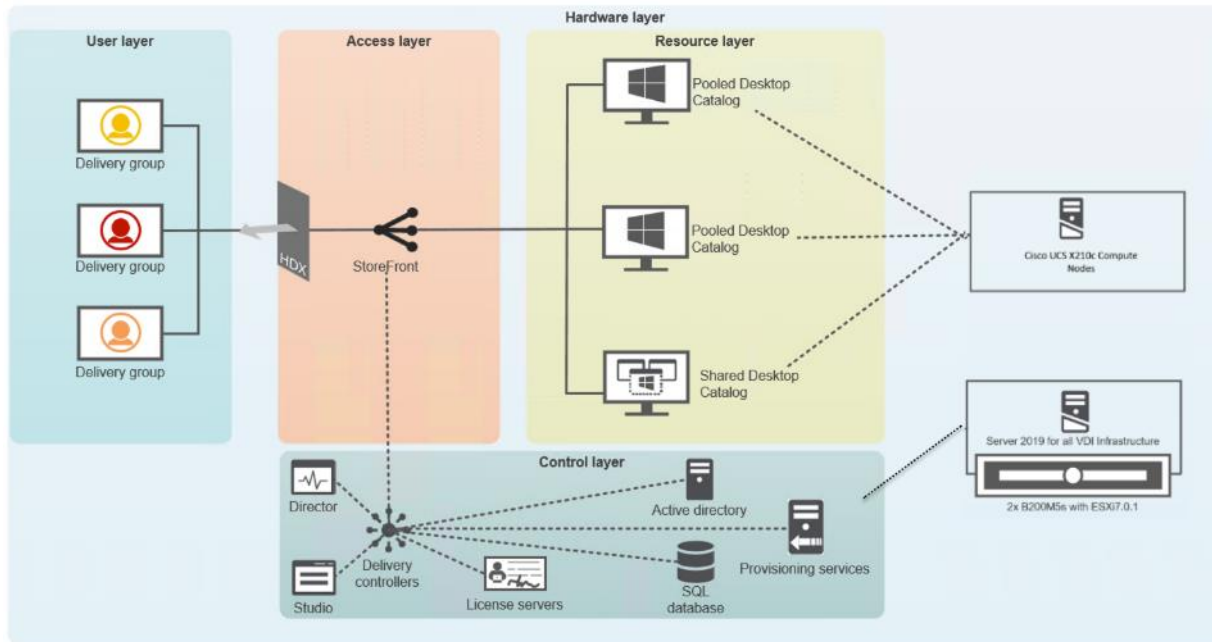
**Note:** (LoginVSI Test infrastructure is not a part of the solution) Sixteen X-Series Compute NodesM4 Blade servers with Intel E5-2680 v4 processors, 256GB RAM, and VIC1240 mezzanine cards plus a NetApp FAS2240 for the Login VSI launcher and logging infrastructure

The NetApp AFF400 configuration is detailed later in this document.

## Logical Architecture

The logical architecture of the validated solution which is designed to support up to 2500 users within a single 42u rack containing 32 blades in 4 chassis, with physical redundancy for the blade servers for each workload type is outlined in [Figure 33](#).

**Figure 33. Logical Architecture Overview**



## Software Revisions

This section includes the software versions of the primary products installed in the environment.

**Table 5. Software Revisions**

Vendor	Product	Version
Cisco	UCS Component Firmware	5.0(1b) bundle release
Cisco	UCS Manager	5.0(1b) bundle release
Cisco	Cisco X210c Compute nodes	5.0(1b) bundle release
Cisco	VIC 14425	5.0(1b)
Cisco	UCS X210C M6 Blades for Infrastructure	5.0(1b) bundle release

Vendor	Product	Version
Citrix	RDS VDA	7 LTSR
Citrix	Citrix Virtual Apps & Desktops VDA	7 LTSR
Citrix	Citrix Virtual Apps & Desktops Controller	7 LTSR
Citrix	Provisioning Services	7 LTSR
Citrix	StoreFront Services	7 LTSR
VMware	vCenter Server Appliance	7.02
VMware	vSphere ESXi 7.02	7.02.16850804
NetApp	Clustered Data ONTAP	9.9 P10
NetApp	ONTAP tools for VMware vSphere	9.9
NetApp	ActiveIQ Unified Manager	9.9
NetApp	SnapCenter Plug-in for VMware vSphere	4.4
NetApp	XCP File Analytics	1.6.3

## Configuration Guidelines

The Citrix Virtual Apps & 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.

**Note:** This document is intended to allow you to configure the Citrix Virtual Apps & Desktops 7 LTSR customer environment as stand-alone solution.

## VLANs

The VLAN configuration recommended for the environment includes a total of seven VLANs as listed in [Table 6](#).

**Table 6. VLAN Configuration**

VLAN Name	VLAN ID	VLAN Purpose	VLAN Name
Default	1	Native VLAN	Default

VLAN Name	VLAN ID	VLAN Purpose	VLAN Name
In-Band-Mgmt	30	VLAN for in-band management interfaces	In-Band-Mgmt
Infra-Mgmt	31	VLAN for Virtual Infrastructure	Infra-Mgmt
CIFS	32	VLAN for CIFS traffic	CIFS
NFS	33	VLAN for Infrastructure NFS traffic	NFS
vMotion	36	VLAN for VMware vMotion	vMotion

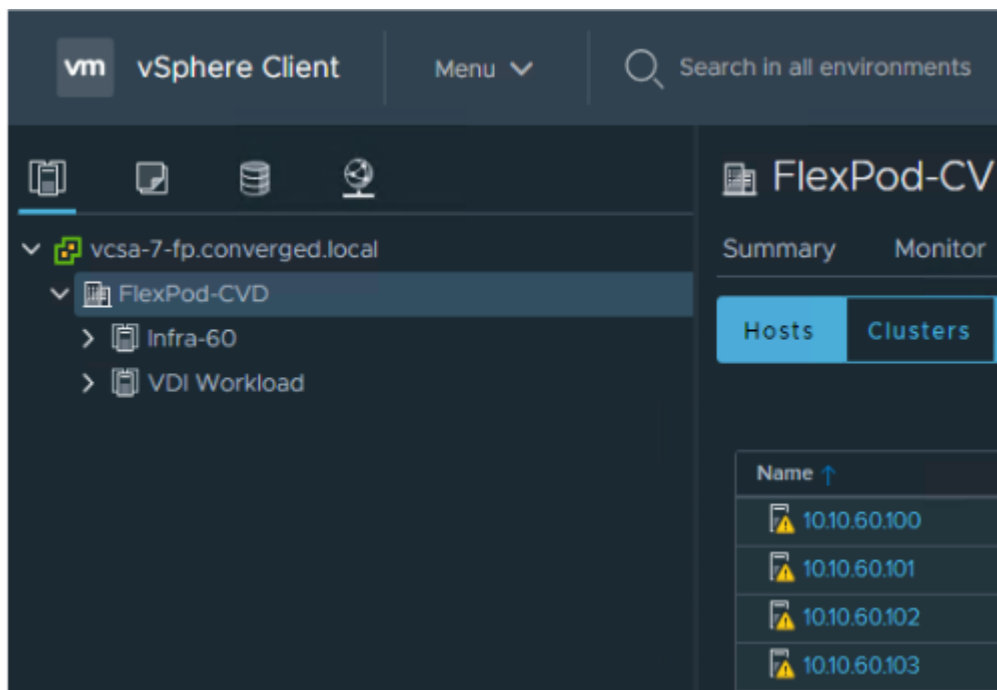
## VMware Clusters

We utilized Two VMware Clusters in one vCenter data center 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, Citrix Virtual Apps & Desktops Controllers, Provisioning Servers, and NetApp VSC, ActiveIQ Unified Manager, VSMs, and so on)
  - VDI Workload VMs (Windows Server 2019 streamed with PVS, Windows 10 Streamed with PVS and persistent desktops with Machine Creation Services)
- VSI Launchers and Launcher Cluster
  - LVS-Launcher-CLSTR: Login VSI Cluster (The Login VSI launcher infrastructure was connected using the same set of switches and vCenter instance but was hosted on separate storage and servers)



Figure 34. vCenter Data Center and Clusters Deployed



---

## Solution Configuration

This chapter is organized into the following subjects:

- [Configuration Topology for a Scalable RDS/Citrix Virtual Apps & Desktops 7 LTSR Workload Desktop Virtualization Solution](#)
- [Network Switch Configuration](#)
- [FlexPod Cisco Nexus Switch Configuration](#)

### **Configuration Topology for a Scalable RDS/Citrix Virtual Apps & Desktops 7 LTSR Workload Desktop Virtualization Solution**

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 35](#) details the physical connectivity configuration of the Citrix Virtual Apps & Desktops 7 LTSR environment.

Figure 35. Cabling Diagram of the FlexPod Data Center with Cisco UCS

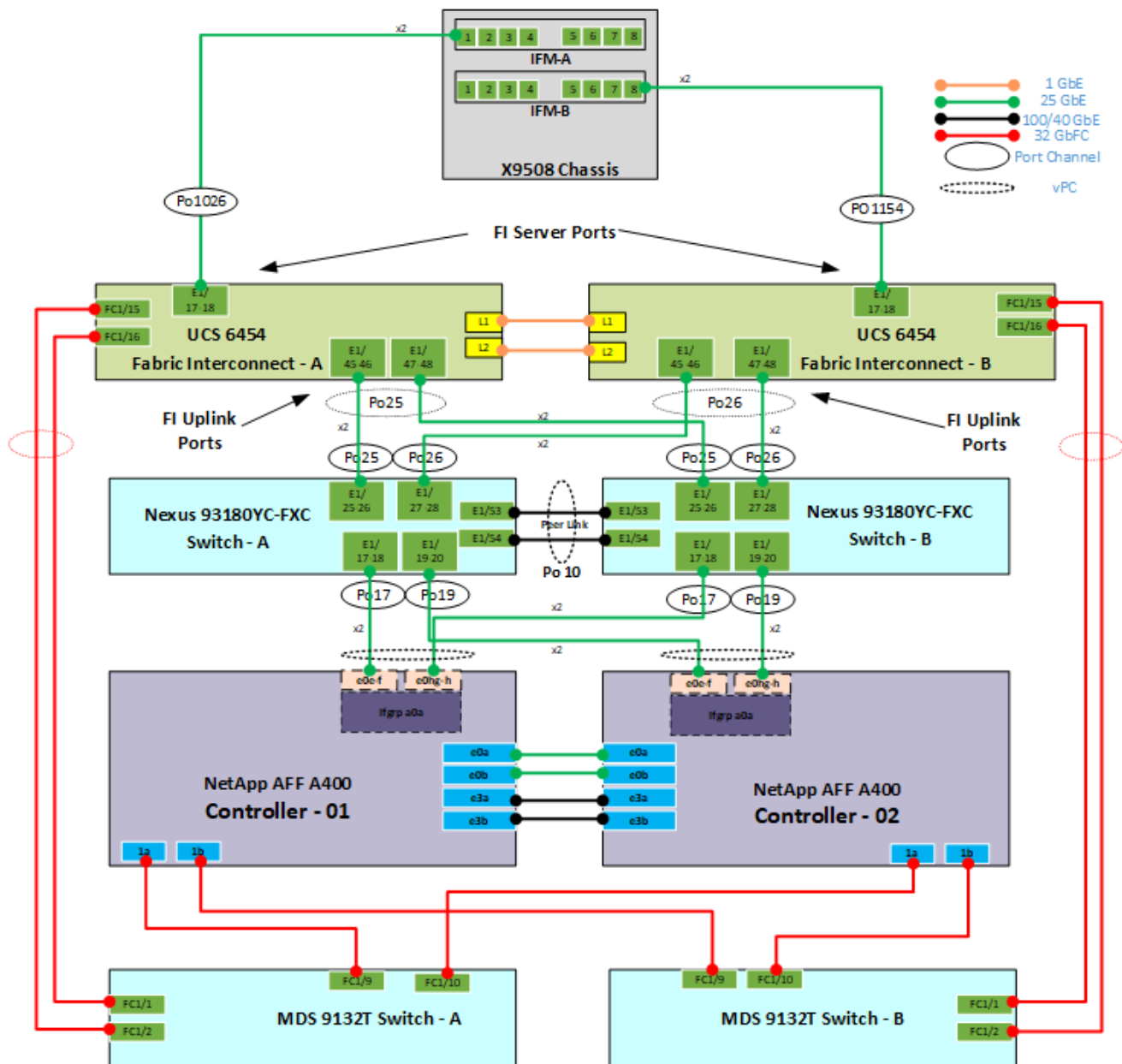


Table 7, Table 8, Table 9, Table 10, Table 11, and Table 12 list the details of all the connections in use.

Table 7. Cisco Nexus 93108-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93108 A	Eth1/15	25GbE	NetApp Controller 2	e0e

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/14	25GbE	NetApp Controller 2	e1a
	Eth1/15	25GbE	NetApp Controller 1	e0e
	Eth1/16	25GbE	NetApp Controller 1	e4a
	Eth1/17	25GbE	NetApp Controller 1	e0h
	Eth1/18	25GbE	NetApp Controller 1	e0g
	Eth1/19	25GbE	NetApp Controller 2	e0e
	Eth1/20	25GbE	NetApp Controller 2	e0h
	Eth1/21	25GbE	Cisco UCS fabric interconnect A	Eth2/1
	Eth1/22	25GbE	Cisco UCS fabric interconnect A	Eth2/2
	Eth1/23	25GbE	Cisco UCS fabric interconnect B	Eth2/3
	Eth1/24	25GbE	Cisco UCS fabric interconnect B	Eth2/4
	Eth1/49	40GbE	Cisco Nexus 93108 B	Eth1/49
	Eth1/50	40GbE	Cisco Nexus 93108 B	Eth1/50
	MGMT0	GbE	GbE management switch	Any

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

**Table 8. Cisco Nexus 93108-B Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93108 B	Eth1/14	25GbE	NetApp Controller 2	e0g
	Eth1/15	25GbE	NetApp Controller 2	e1b

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/16	25GbE	NetApp Controller 1	e0g
	Eth1/17	25GbE	NetApp Controller 1	e0e
	Eth1/18	25GbE	NetApp Controller 1	e0f
	Eth1/19	25GbE	NetApp Controller 2	e0f
	Eth1/20	25GbE	NetApp Controller 2	e0g
	Eth1/21	25GbE	NetApp Controller 1	e1b
	Eth1/22	25GbE	Cisco UCS fabric interconnect A	Eth2/1
	Eth1/23	25GbE	Cisco UCS fabric interconnect A	Eth2/2
	Eth1/24	25GbE	Cisco UCS fabric interconnect B	Eth2/3
	Eth1/14	25GbE	Cisco UCS fabric interconnect B	Eth2/4
	Eth1/49	40GbE	Cisco Nexus 93108 B	Eth1/49
	Eth1/50	40GbE	Cisco Nexus 93108 B	Eth1/50
	MGMT0	GbE	GbE management switch	Any

**Table 9. 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

Local Device	Local Port	Connection	Remote Device	Remote Port
	e0c	100GbE	NS224-1	e0a
	e0d	100GbE	NS224-2	e0b
	e0e	25GbE	Cisco Nexus 93108 B	Eth1/17
	e0f	25GbE	Cisco Nexus 93108 B	Eth1/18
	e0g	25GbE	Cisco Nexus 93108 A	Eth1/18
	e0h	25GbE	Cisco Nexus 93108 A	Eth1/17
	e3a	100GbE	NetApp Controller 2	e3a
	e3b	100GbE	NetApp Controller 2	e3b
	e5a	100GbE	NS224-2	e0a
	e5b	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 10. 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 2	e0a
	e0b	25GbE	NetApp Controller 2	e0b
	e0c	100GbE	NS224-1	e0a
	e0d	100GbE	NS224-2	e0b
	e0e	25GbE	Cisco Nexus 93108 A	Eth1/19

Local Device	Local Port	Connection	Remote Device	Remote Port
	e0f	25GbE	Cisco Nexus 93108 B	Eth1/19
	e0g	25GbE	Cisco Nexus 93108 B	Eth1/20
	e0h	25GbE	Cisco Nexus 93108 A	Eth1/20
	e3a	100GbE	NetApp Controller 2	e3a
	e3b	100GbE	NetApp Controller 2	e3b
	e5a	100GbE	NS224-2	e0a
	e5b	100GbE	NS224-1	e0b

**Table 11. Cisco UCS Fabric Interconnect A Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth2/1	25GbE	Cisco Nexus 93108 A	Eth1/17
	Eth2/2	25GbE	Cisco Nexus 93108 A	Eth1/18
	Eth2/3	25GbE	Cisco Nexus 93108 B	Eth1/19
	Eth2/4	25GbE	Cisco Nexus 93108 B	Eth1/20
	Eth1/1	25GbE	Cisco UCS Chassis1 FEX A	IOM 1/1
	Eth1/2	25GbE	Cisco UCS Chassis1 FEX A	IOM 1/2
	Eth1/3	25GbE	Cisco UCS Chassis1 FEX A	IOM 1/3
	Eth1/4	25GbE	Cisco UCS Chassis1 FEX A	IOM 1/4
	Eth1/5	25GbE	Cisco UCS Chassis2 FEX A	IOM 1/1
	Eth1/6	25GbE	Cisco UCS Chassis2 FEX A	IOM 1/2
Eth1/7	25GbE	Cisco UCS Chassis2 FEX A	IOM 1/3	

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/8	25GbE	Cisco UCS Chassis2 FEX A	IOM 1/4
	Eth1/9	25GbE	Cisco UCS Chassis3 FEX A	IOM 1/1
	Eth1/10	25GbE	Cisco UCS Chassis3 FEX A	IOM 1/2
	Eth1/11	25GbE	Cisco UCS Chassis3 FEX A	IOM 1/3
	Eth1/12	25GbE	Cisco UCS Chassis3 FEX A	IOM 1/4
	Eth1/13	25GbE	Cisco UCS Chassis4 FEX A	IOM 1/1
	Eth1/14	25GbE	Cisco UCS Chassis4 FEX A	IOM 1/2
	Eth1/15	25GbE	Cisco UCS Chassis4 FEX A	IOM 1/3
	Eth1/16	25GbE	Cisco UCS Chassis4 FEX A	IOM 1/4
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2

**Table 12. Cisco UCS Fabric Interconnect B Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect B	Eth2/1	25GbE	Cisco Nexus 93108 A	Eth1/17
	Eth2/2	25GbE	Cisco Nexus 93108 A	Eth1/18
	Eth2/3	25GbE	Cisco Nexus 93108 B	Eth1/19
	Eth2/4	25GbE	Cisco Nexus 93108 B	Eth1/20
	Eth1/1	25GbE	Cisco UCS Chassis1 FEX B	IOM 2/1



Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/2	25GbE	Cisco UCS Chassis1 FEX B	IOM 2/2
	Eth1/3	25GbE	Cisco UCS Chassis1 FEX B	IOM 2/3
	Eth1/4	25GbE	Cisco UCS Chassis1 FEX B	IOM 2/4
	Eth1/5	25GbE	Cisco UCS Chassis2 FEX B	IOM 2/1
	Eth1/6	25GbE	Cisco UCS Chassis2 FEX B	IOM 2/2
	Eth1/7	25GbE	Cisco UCS Chassis2 FEX B	IOM 2/3
	Eth1/8	25GbE	Cisco UCS Chassis2 FEX B	IOM 2/4
	Eth1/9	25GbE	Cisco UCS Chassis3 FEX B	IOM 2/1
	Eth1/10	25GbE	Cisco UCS Chassis3 FEX B	IOM 2/2
	Eth1/11	25GbE	Cisco UCS Chassis3 FEX B	IOM 2/3
	Eth1/12	25GbE	Cisco UCS Chassis3 FEX B	IOM 2/4
	Eth1/13	25GbE	Cisco UCS Chassis4 FEX B	IOM 2/1
	Eth1/14	25GbE	Cisco UCS Chassis4 FEX B	IOM 2/2
	Eth1/15	25GbE	Cisco UCS Chassis4 FEX B	IOM 2/3
	Eth1/16	25GbE	Cisco UCS Chassis4 FEX B	IOM 2/4
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	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.

**Note:** 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 [FlexPod 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(4), the Cisco suggested Nexus switch release at the time of this validation.

If using the Cisco Nexus 93180YC-FX switches for both LAN and SAN switching, please refer to section [FlexPod with Cisco Nexus 93180YC-FX SAN Switching Configuration - Part 1](#) in the Appendix.

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

**Step 1.** Configure the switch.

**Step 2.** 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]: n
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

**Step 3.** 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

**Step 1.** Configure the switch.

**Step 2.** 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]: Enter
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

**Step 3.** 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 for Cisco Nexus A and Cisco Nexus B](#)
- [Add NTP Distribution Interface on Cisco Nexus A](#)
- [Add NTP Distribution Interface on Cisco Nexus B](#)
- [Add Port Profiles on Cisco A and Cisco 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](#)
- [Switch Testing Commands](#)

### Procedure 1. Enable features on Cisco Nexus A and Cisco Nexus B

**Note:** 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 udd
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 for Cisco Nexus A and Cisco Nexus B

**Note:** To create the necessary virtual local area networks (VLANs), follow this step on both switches:

**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
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 A and Cisco B

**Note:** 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 2.** 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>
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>, <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>, <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 Eth1/21
description <ucs-clustername>-a:1/45
udld enable
interface Eth1/22
description <ucs-clustername>-a:1/46
udld enable
interface Eth1/23
description <ucs-clustername>-b:1/45
udld enable
interface Eth1/24
description <ucs-clustername>-b:1/46
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 Eth1/49
description <nexus-b-hostname>:1/49
interface Eth1/50
description <nexus-b-hostname>:1/50
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 Eth1/21
description <ucs-clustername>-a:1/47
udld enable
interface Eth1/22
description <ucs-clustername>-a:1/48
udld enable
interface Eth1/23
description <ucs-clustername>-b:1/47
udld enable
interface Eth1/24
description <ucs-clustername>-b:1/48
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 Eth1/49
description <nexus-a-hostname>:1/49
interface Eth1/50
description <nexus-a-hostname>:1/50
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 Eth1/49-50
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 Po121
description <ucs-clustername>-a
interface Eth1/21-22
channel-group 121 mode active
no shutdown
interface Po123
description <ucs-clustername>-b
interface Eth1/23-24
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 Po121
inherit port-profile FP-UCS
interface Po123
```

```
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 Po121
vpc 121
interface Po123
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 Po121
vpc 121
interface Po123
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.

### Procedure 13. Switch Testing Commands

**Note:** The following commands can be used to check for correct switch configuration. 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 is organized into the following subjects:

- [NetApp AFF A400 Controllers](#)
- [NetApp ONTAP 9.9.1P2](#)

### NetApp AFF A400 Controllers

See the following section ([NetApp Hardware Universe](#)) for planning the physical location of the storage systems:

- Site Preparation
- System Connectivity Requirements
- Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements
- AFF Series Systems

### 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 9.9.1P2

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 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](#)
- [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 a NetApp FlexVol volume](#)
- [Modify Volume Efficiency](#)
- [Create NFS LIFs](#)
- [Create FC LIFs \(required only for FC configuration\)](#)
- [Create iSCSI LIFs \(required only for iSCSI configuration\)](#)
- [Configure FC-NVMe Datastore for vSphere 7U2 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 13](#) lists the information needed to configure two ONTAP nodes. Customize the cluster-detail values with the information applicable to your deployment.

**Table 13. 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 9.9 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 9.9.1P2 is not the version of software being booted, continue with the following steps to install new software. If ONTAP 9.9.1P2 is the version being booted, choose option 8 and `y` to reboot the node. Then 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:** The initialization and creation of the root aggregate can take 90 minutes or more to complete, depending on the number and type of disks attached. When initialization is complete, the storage system reboots. Note that SSDs take considerably less time to initialize. You can continue with the configuration of node 02 while the disks for node 01 are zeroing.

## 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 9.9.1P2 is not the version of software being booted, continue with the following steps to install new software. If ONTAP 9.9.1 is the version being booted, choose 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:** The initialization and creation of the root aggregate can take 90 minutes or more to complete, depending on the number and type of disks attached. When initialization is complete, the storage system reboots. Note that SSDs take considerably less time to initialize.

### 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 9.9.1P2 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 accessing <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 14. 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 Detail	Cluster Detail Value
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:

Health

✔ 2 healthy nodes were found.

AFF-A400

### Initialize Storage System

STORAGE SYSTEM NAME

ADMINISTRATIVE PASSWORD




---

### Networking

<small>CLUSTER MANAGEMENT IP ADDRESS</small>	<small>SUBNET MASK</small>	<small>GATEWAY</small>
<input type="text" value="IP Address"/>	<input type="text" value="Length"/>	<input type="text" value="IP Address"/>
<small>NODE SERIAL NUMBERS</small>	<small>NODE MANAGEMENT IP ADDRESSES</small>	
72:	<input type="text" value="IP Address"/>	
72:	<input type="text" value="IP Address"/>	

Use Domain Name Service (DNS)

- Step 13.** From the Cluster screen, enter the cluster name and administrator password.
- Step 14.** Complete the Networking information for the cluster and each node.
- Step 15.** Check the box for Use time services (NTP) and enter the IP addresses of the time servers in a comma separated list.

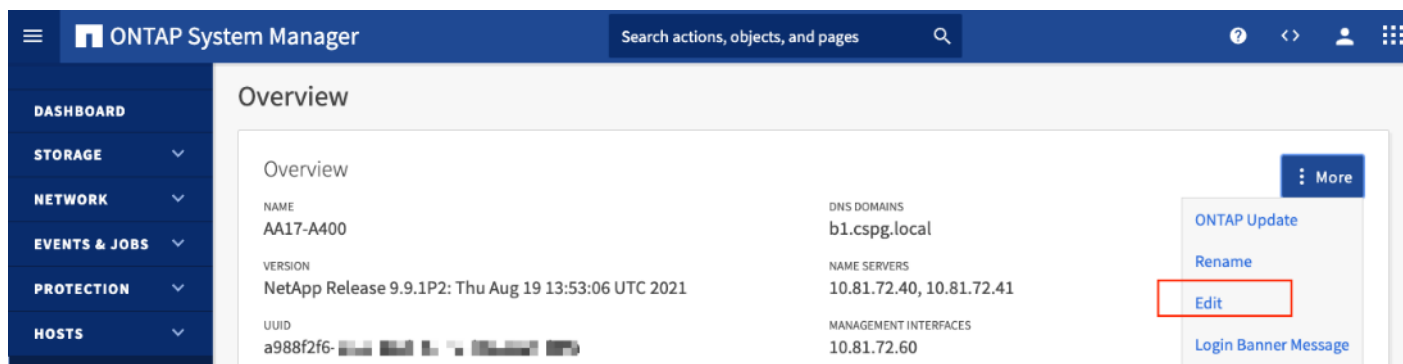
**Tech tip**

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 16.** Click **Submit**.
- Step 17.** A few minutes will pass while the cluster is configured. When prompted, login to ONTAP System Manager to continue the cluster configuration.
- Step 18.** From the Dashboard click the **Cluster** menu on the left and select **Overview**.
- Step 19.** Click the **More** ellipsis button in the Overview pane at the top right of the screen and select **Edit**.

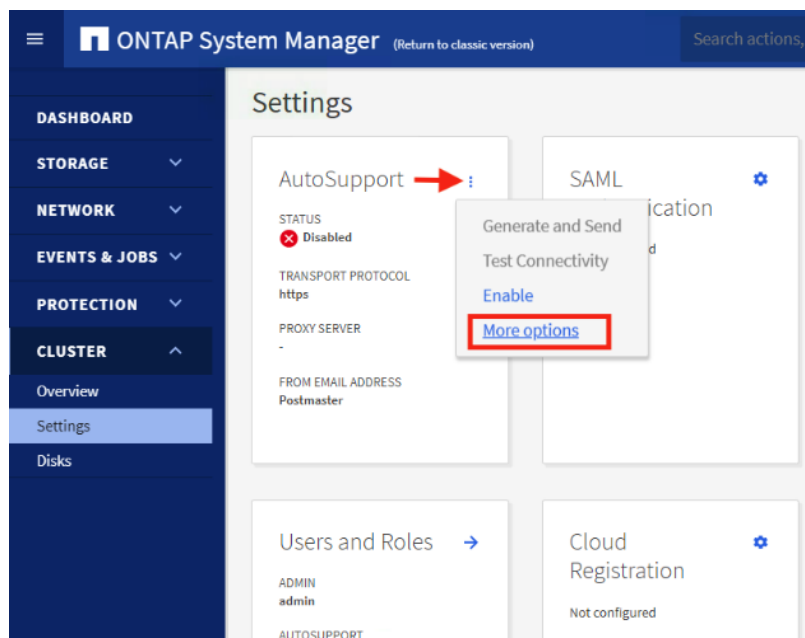


**Step 20.** Add additional cluster configuration details and click **Save** to make the changes persistent:

- 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 21.** Click **Save** to make the changes persistent.

**Step 22.** Select the **Settings** menu under the **Cluster** menu.



**Step 23.** If AutoSupport was not configured during the initial setup, click the ellipsis in the AutoSupport tile and select **More options**.

**Step 24.** To enable AutoSupport click the slider.

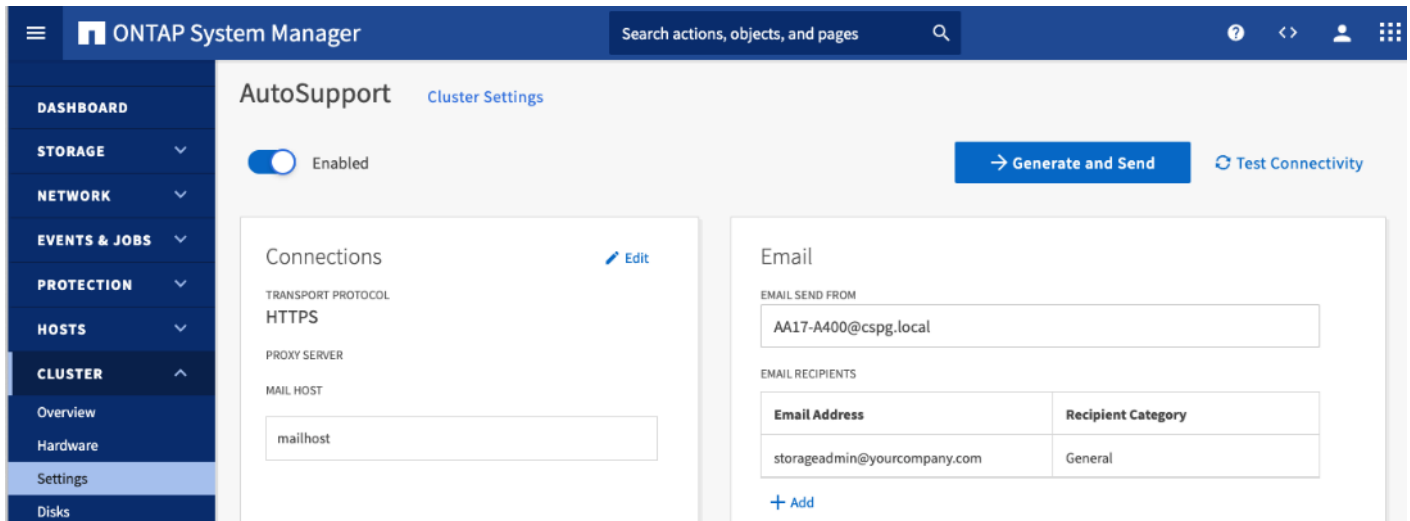
**Step 25.** Click **Edit** to change the transport protocol, add a proxy server address and a mail host as needed.

**Step 26.** Click **Save** to enable the changes.

**Step 27.** In the Email tile to the right, click **Edit** and enter the desired email information:

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

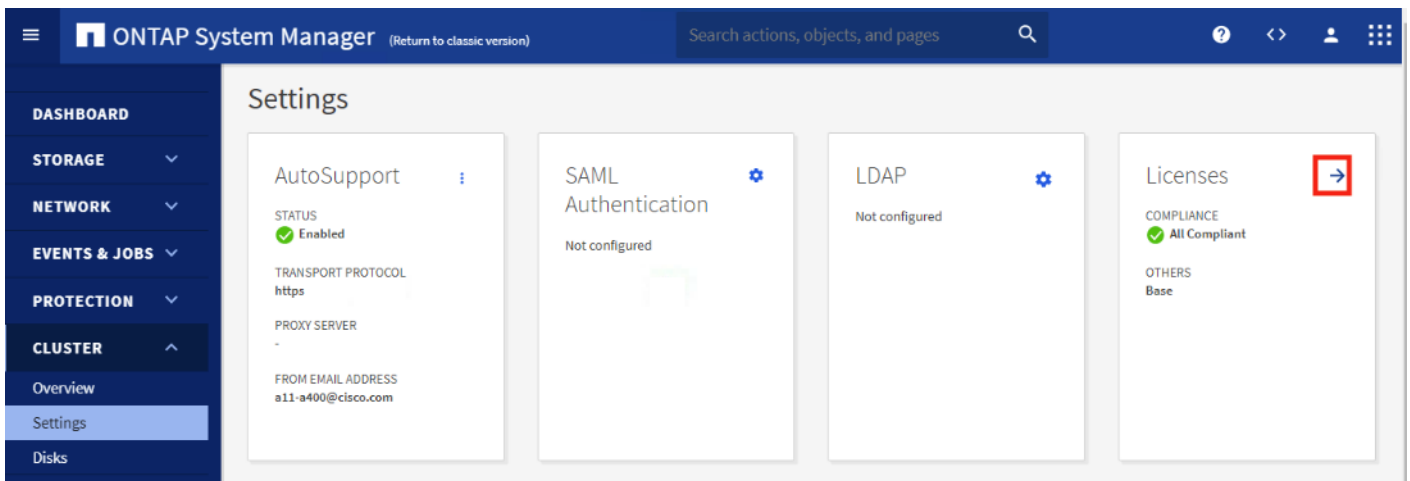
**Step 28.** Click **Save** when complete.

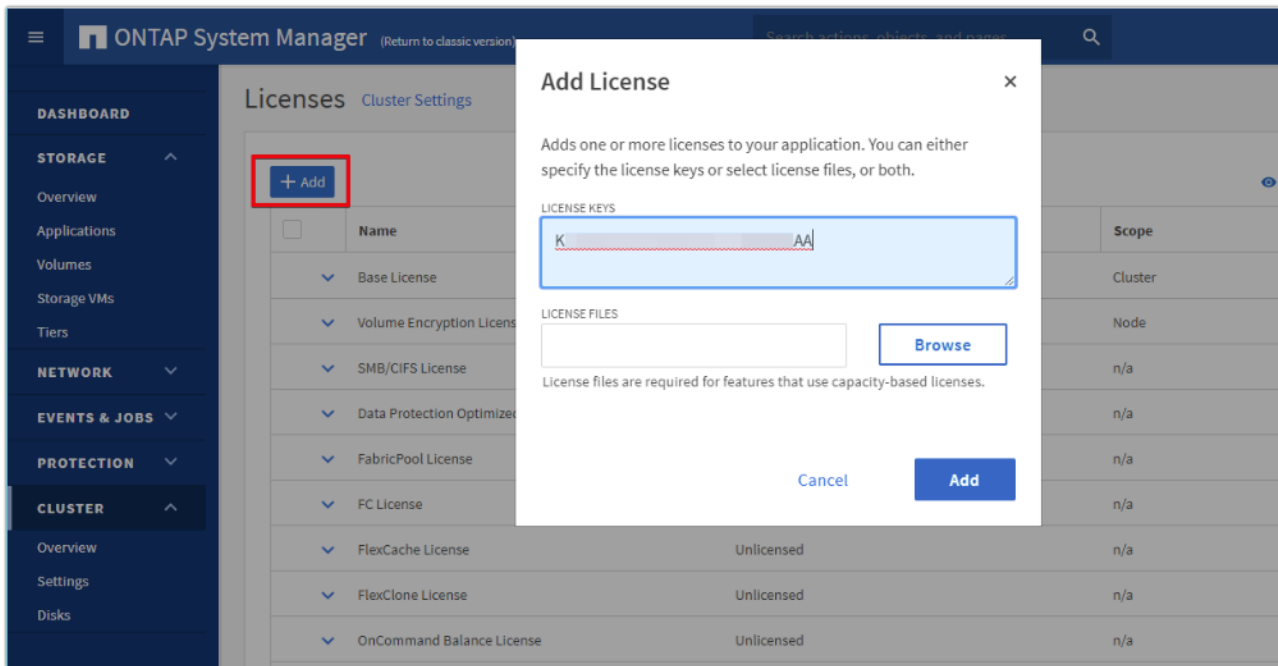


**Step 29.** Select **CLUSTER > Settings** at the top left of the page to return to the cluster settings page.

**Step 30.** Locate the **Licenses** tile on the right and click the detail arrow.

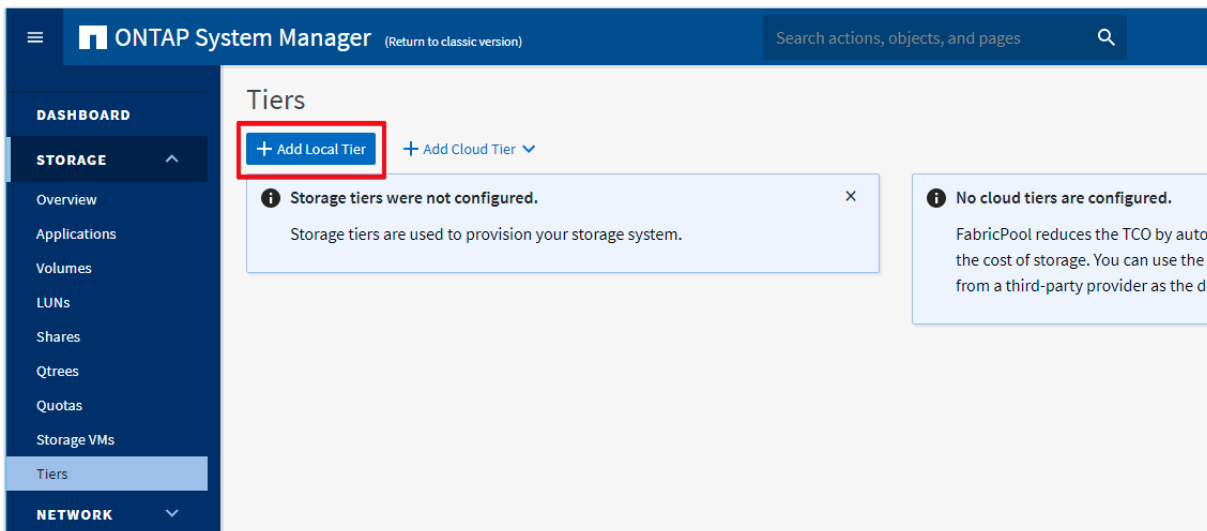
**Step 31.** Add the desired licenses to the cluster by clicking **Add** and entering the license keys in a comma separated list.





**Step 32.** Configure storage aggregates by selecting the **Storage** menu on the left and selecting **Tiers**.

**Step 33.** Click **Add Local Tier** and allow ONTAP System Manager to recommend a storage aggregate configuration.



**Step 34.** ONTAP will use best practices to recommend an aggregate layout. Click the **Recommended details** link to view the aggregate information.

**Step 35.** Optionally, enable NetApp Aggregate Encryption (NAE) by checking the box for Configure Onboard Key Manager for encryption.

**Step 36.** Enter and confirm the passphrase and save it in a secure location for future use.

**Step 37.** 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

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

Cancel

Save

**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:

```
AA17-A400::> storage failover show
```





```
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
```

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

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.

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.

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> -ip-space 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
```

```
AA17-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
```

```
-----
AA17-A400-01 e0e auto auto none
```

```

AA17-A400-01 e0f auto auto none
AA17-A400-01 e0g auto auto none
AA17-A400-01 e0h auto auto none
AA17-A400-02 e0e auto auto none
AA17-A400-02 e0f auto auto none
AA17-A400-02 e0g auto auto none
AA17-A400-02 e0h auto auto none

```

8 entries were displayed.

```

AA17-A400::> net port show -node * -port e3a,e3 -fields speed-admin,duplex-admin,flowcontrol-
admin (network port show)

```

```

node port duplex-admin speed-admin flowcontrol-admin
-----
AA17-A400-01 e3a auto auto none
AA17-A400-01 e3b auto auto none
AA17-A400-02 e3a auto auto none
AA17-A400-02 e3b auto auto none

```

4 entries were displayed.

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

In accordance with the best practices for FC host ports, to disable auto-negotiate on each FCP adapter in each controller node, follow these steps:

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

```

fcg adapter modify -node <st-node01> -adapter 5a -status-admin down
fcg adapter modify -node <st-node01> -adapter 5b -status-admin down
fcg adapter modify -node <st-node02> -adapter 5a -status-admin down
fcg adapter modify -node <st-node02> -adapter 5b -status-admin down

```

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

```

fcg adapter modify -node <st-node01> -adapter 5a -speed 32 -status-admin up
fcg adapter modify -node <st-node01> -adapter 5b -speed 32 -status-admin up
fcg adapter modify -node <st-node02> -adapter 5a -speed 32 -status-admin up
fcg adapter modify -node <st-node02> -adapter 5b -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 iSCSI Broadcast Domains (Required only for iSCSI configuration)

**Step 2.** 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 18. 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:

```
AA17-A400::> network port ifgrp show
```

	Port	Distribution		Active	
Node	IfGrp	Function	MAC Address	Ports	Ports
AA17-A400-01	a0a	port	d2:39:ea:29:d4:4a	full	e0e, e0f, e0g, e0h
AA17-A400-02	a0a	port	d2:39:ea:29:ce:d5	full	e0e, e0f, e0g, e0h

```
2 entries were displayed.
```

## Procedure 19. 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 20. 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:

```
AA17-A400::> network port vlan show

                Network Network
Node   VLAN Name Port   VLAN ID  MAC Address
-----
AA17-A400-01
      a0a-17   a0a     17      d2:39:ea:29:d4:4a
      a0a-3017
                a0a     3017    d2:39:ea:29:d4:4a
      a0a-3117
                a0a     3117    d2:39:ea:29:d4:4a
      a0a-3217
                a0a     3217    d2:39:ea:29:d4:4a
AA17-A400-02
      a0a-17   a0a     17      d2:39:ea:29:ce:d5
      a0a-3017
                a0a     3017    d2:39:ea:29:ce:d5
      a0a-3117
                a0a     3117    d2:39:ea:29:ce:d5
      a0a-3217
                a0a     3217    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.** 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 21. 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 22. 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 23. 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-prot>>
```

```
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 [SNMP Configuration Express Guide](#) for additional information when configuring SNMPv3 security users.

## Procedure 24. 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
```

### Step 2. Remove the unused data protocols from the SVM:

```
vserver remove-protocols -vserver Infra-SVM -protocols cifs
```

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

### Step 3. 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 4. 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 5. Verify the NFS `vstorage` parameter for the NetApp NFS VAAI plug-in was enabled:

```
AA17-A400::> vserver nfs show -fields vstorage
vserver    vstorage
-----
Infra-SVM enabled
```

## Procedure 25. 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:

```
AA17-A400::> snapmirror show -type ls
```

Source Path	Destination Type Path	Mirror State	Relationship Status	Total Progress	Healthy	Progress Last Updated
-----						
AA17-A400://Infra-SVM/Infra_SVM_root						
	LS	AA17-A400://Infra-SVM/infra_svm_root_m01	Snapmirrored	Idle	-	true -
		AA17-A400://Infra-SVM/infra_svm_root_m02	Snapmirrored	Idle	-	true -

2 entries were displayed.

**Procedure 26.** 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:

```
AA17-A400::> vserver fcp show
```

Vserver	Target Name	Status 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 27. 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:

```
AA17-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 28. Vserver Protocol Verification

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

```
AA17-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 29. 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 certifi-

cates 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 30. 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 31. 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 32. 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 33. Create NFS LIFs

**Step 1.** To create NFS LIFs, run the following commands:

```
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.** To verify, run the following:

```
AA17-A400::> network interface show -vserver Infra-SVM -data-protocol nfs
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Infra-SVM	nfs-lif-01	up/up	192.168.30.1/24	AA17-A400-01	a0a-3017	true
	nfs-lif-02	up/up	192.168.30.2/24	AA17-A400-02	a0a-3017	true

2 entries were displayed.

### Procedure 34. 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 5a -status-admin up
```

```
network interface create -vserver Infra-SVM -lif fcp-lif-01b -role data -data-protocol fcp -
home-node <st-node01> -home-port 5b -status-admin up
```

```
network interface create -vserver Infra-SVM -lif fcp-lif-02a -role data -data-protocol fcp -
home-node <st-node02> -home-port 5a -status-admin up
```

```
network interface create -vserver Infra-SVM -lif fcp-lif-02b -role data -data-protocol fcp -
home-node <st-node02> -home-port 5b -status-admin up
```

#### Step 2. To verify, run the following:

```
AA17-A400::> network interface show -vserver Infra-SVM -data-protocol fcp
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Infra-SVM	fcp-lif-01a	up/up	20:01:d0:39:ea:29:ce:d4	AA17-A400-01	5a	true
	fcp-lif-01b	up/up	20:02:d0:39:ea:29:ce:d4	AA17-A400-01	5b	true
	fcp-lif-02a	up/up	20:03:d0:39:ea:29:ce:d4	AA17-A400-02	5a	true
	fcp-lif-02b	up/up	20:04:d0:39:ea:29:ce:d4			

AA17-A400-02 5b true

4 entries were displayed.

### Procedure 35. 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
```

**Step 2.** To verify, run the following:

```
AA17-A400::> network interface show -vserver Infra-SVM -data-protocol iscsi
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Infra-SVM	iscsi-lif-01a	up/up	192.168.31.1/24	AA17-A400-01	a0a-3117	true
	iscsi-lif-01b	up/up	192.168.32.1/24	AA17-A400-01	a0a-3217	true
	iscsi-lif-02a	up/up	192.168.31.2/24	AA17-A400-02	a0a-3117	true
	iscsi-lif-02b	up/up	192.168.32.2/24	AA17-A400-02	a0a-3217	true

4 entries were displayed.

## Procedure 36. Configure FC-NVMe Datastore for vSphere 7U2 on existing SVM (Infra-SVM) for FC-NVMe configuration only

**Note:** To Configure FC-NVMe Datastores for vSphere 7U2, 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:

```
AA17-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:

```
AA17-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 5a -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 5b -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 5a -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 5b -status-admin up
```

**Step 7.** To verify, run the following:

```
AA17-A400::> network interface show -vserver Infra-SVM -data-protocol fc-nvme
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----						
Infra-SVM	fc-nvme-lif-01a	up/up	20:06:d0:39:ea:29:ce:d4	AA17-A400-01	5b	true
	fc-nvme-lif-01b	up/up	20:08:d0:39:ea:29:ce:d4	AA17-A400-01	5a	true
	fc-nvme-lif-02a	up/up	20:07:d0:39:ea:29:ce:d4	AA17-A400-02	5b	true
	fc-nvme-lif-02b	up/up	20:09:d0:39:ea:29:ce:d4	AA17-A400-02	5a	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 AA17_A400_01_NVME_SSD_1 -
size 500G -state online -space-guarantee none -percent-snapshot-space 0
```

**Procedure 37.** 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:

```
AA17-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 38. 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"
```

The following 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 FlexGroups 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
PVS	8	2TB (2% used)	performance	4096	163.84
Data	8	10TB (25% used)	performance	20480	10240

For NFS, the DNS Load balancing feature was used and is available on ONTAP. DNS load balancing helps in selecting an appropriately loaded data LIF and balancing user network traffic across all available ports (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.

The screenshot shows the DNS Manager console with the 'NFSserver' zone selected. An 'Edit Name Server Record' dialog box is open, showing the configuration for the NS record 'A400-nfs.converged.local'. The dialog includes a 'Server fully qualified domain name (FQDN)' field with the value 'A400-nfs.converged.local', a 'Resolve' button, and a table of IP addresses for this NS record.

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

Buttons for 'Delete', 'Up', and 'Down' are visible on the right side of the IP address table. At the bottom of the dialog are 'OK' and 'Cancel' buttons. Below the dialog, the main window's 'OK', 'Cancel', and 'Apply' buttons are partially visible.

## Cisco Intersight Managed Mode Configuration

This chapter is organized into the following subjects:

- [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](#)
- [SAN Switch 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 X210c 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](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 Managed 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
```

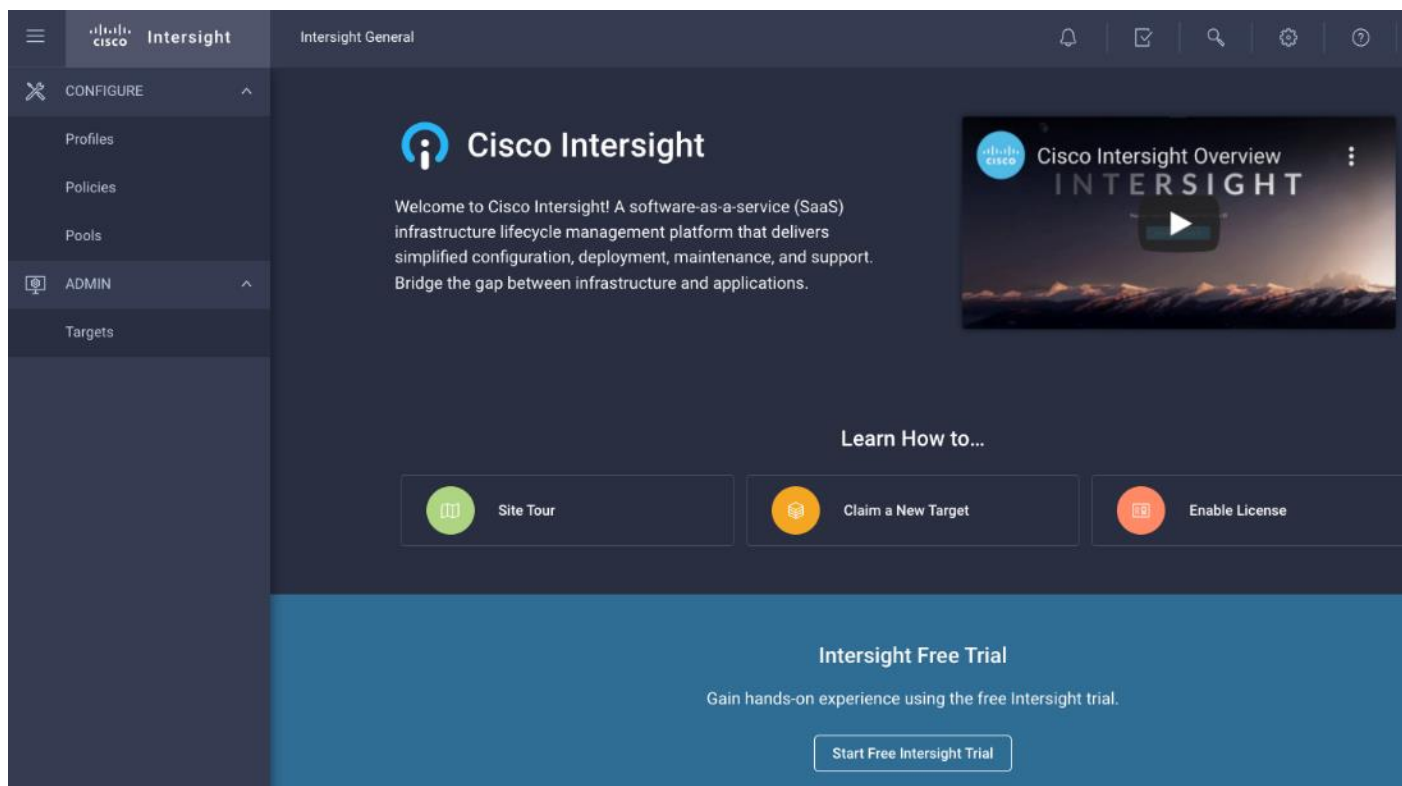
**Procedure 2. Set up a new Cisco Intersight account**

**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:



**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/cs/ws/platform/home?locale=en\\_US#module/SmartLicensing](https://software.cisco.com/software/cs/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: Cisco - Intersight

Description : RTP IMM

\* 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

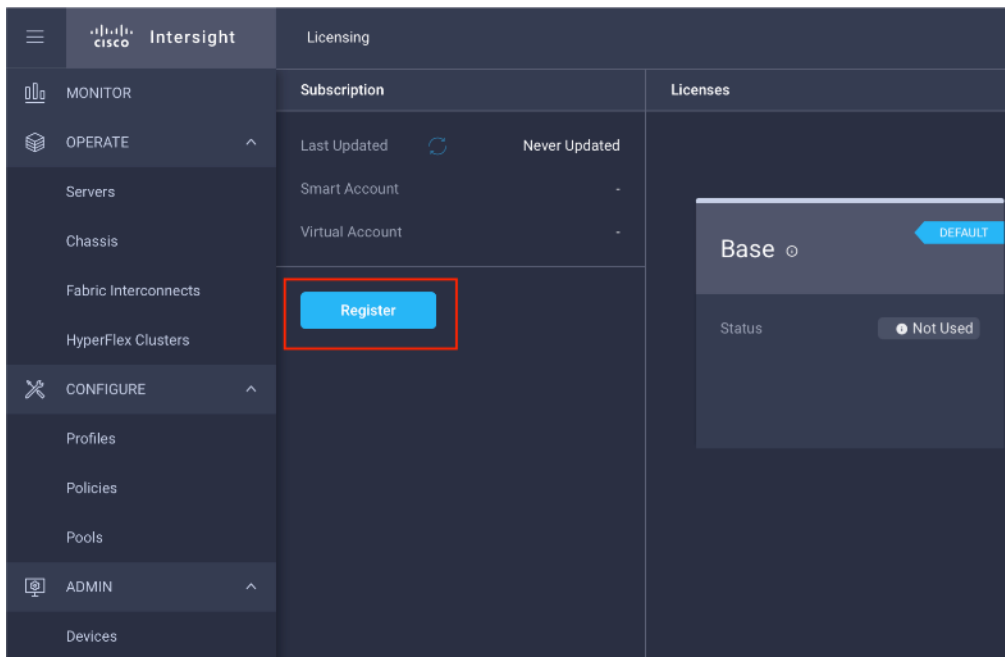
Create Token

Cancel

**Step 5.** Log into the Cisco Intersight portal and click **Settings** (the gear icon) in the top-right corner. Click **Licensing**.



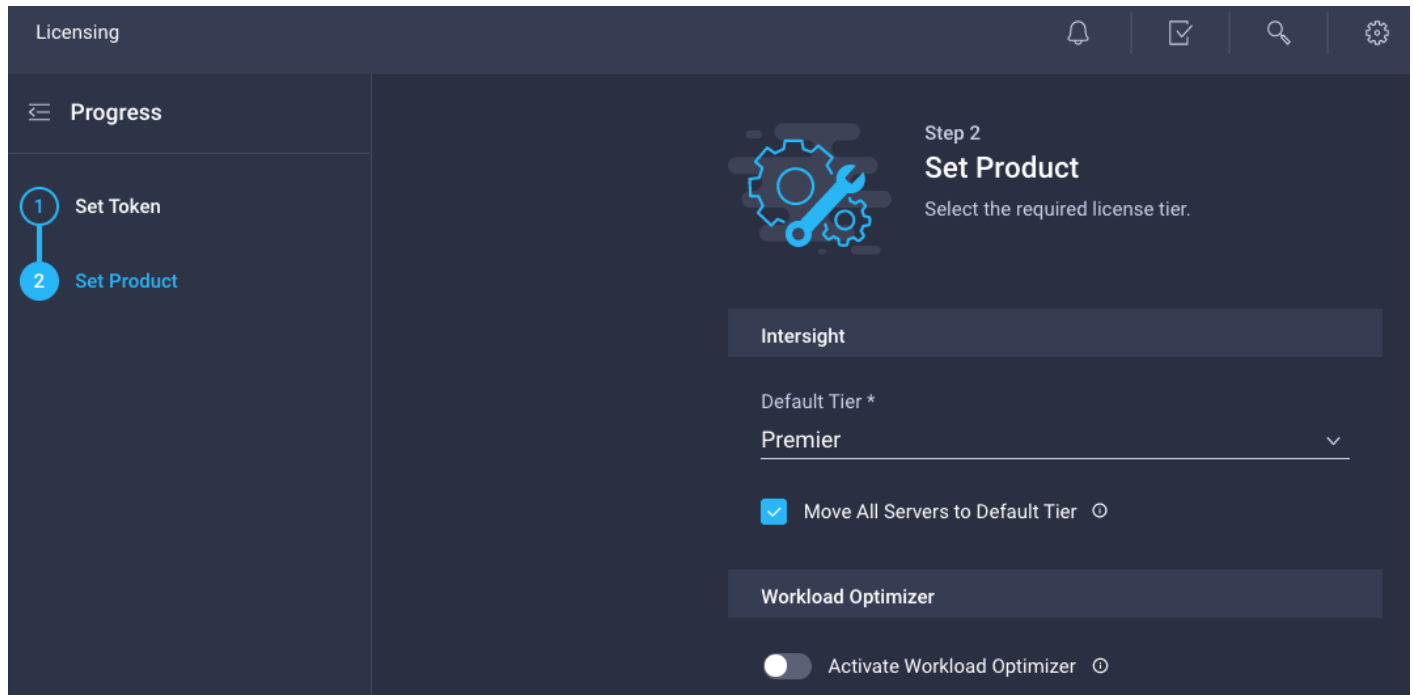
**Step 6.** Under **Cisco Intersight > Licensing**, click **Register**.



**Step 7.** Enter the copied token from the Cisco Smart Licensing portal. Click **Next**.

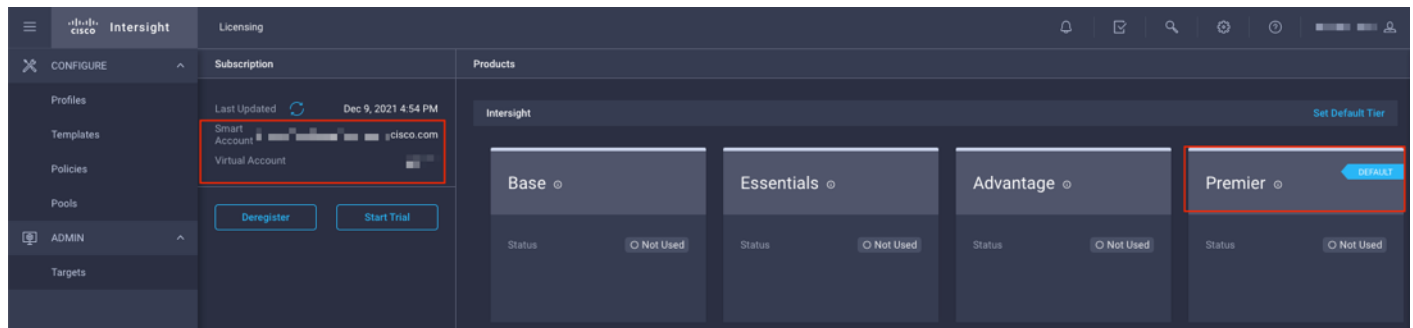
**Step 8.** From the drop-down list, select the pre-selected Default Tier \* and select the license type (for example, Premier).

**Step 9.** Select **Move All Servers to Default Tier**.



**Step 10.** Click **Register**.

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.



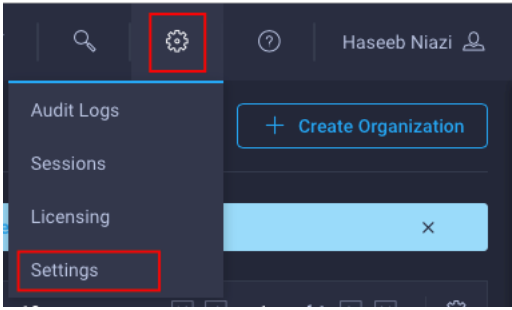
#### Procedure 4. Set up Cisco Intersight Resource Group

**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**.

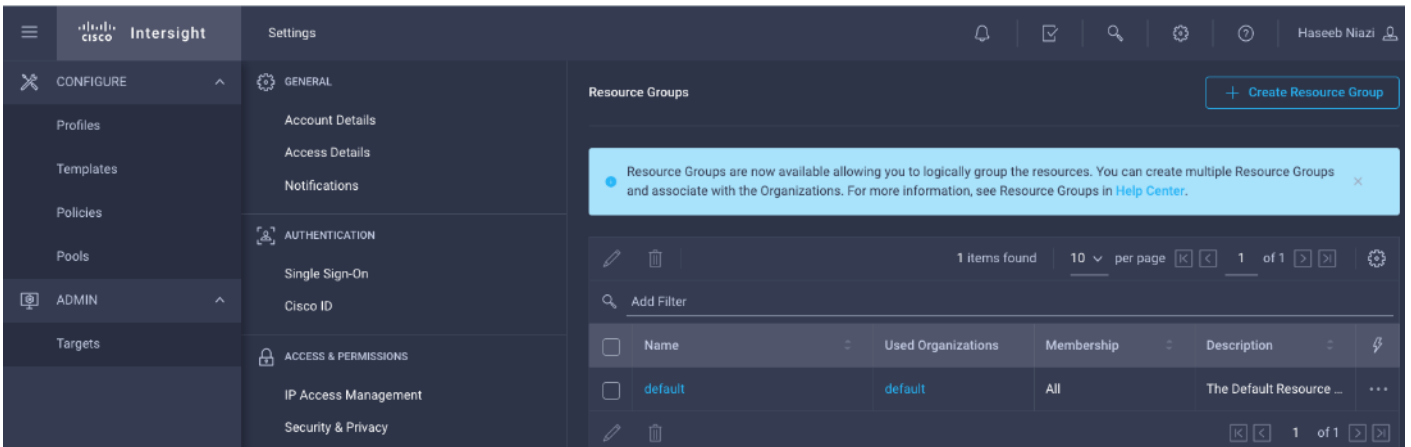
**Step 2.** Click **Settings** (the gear icon) and click **Settings**.



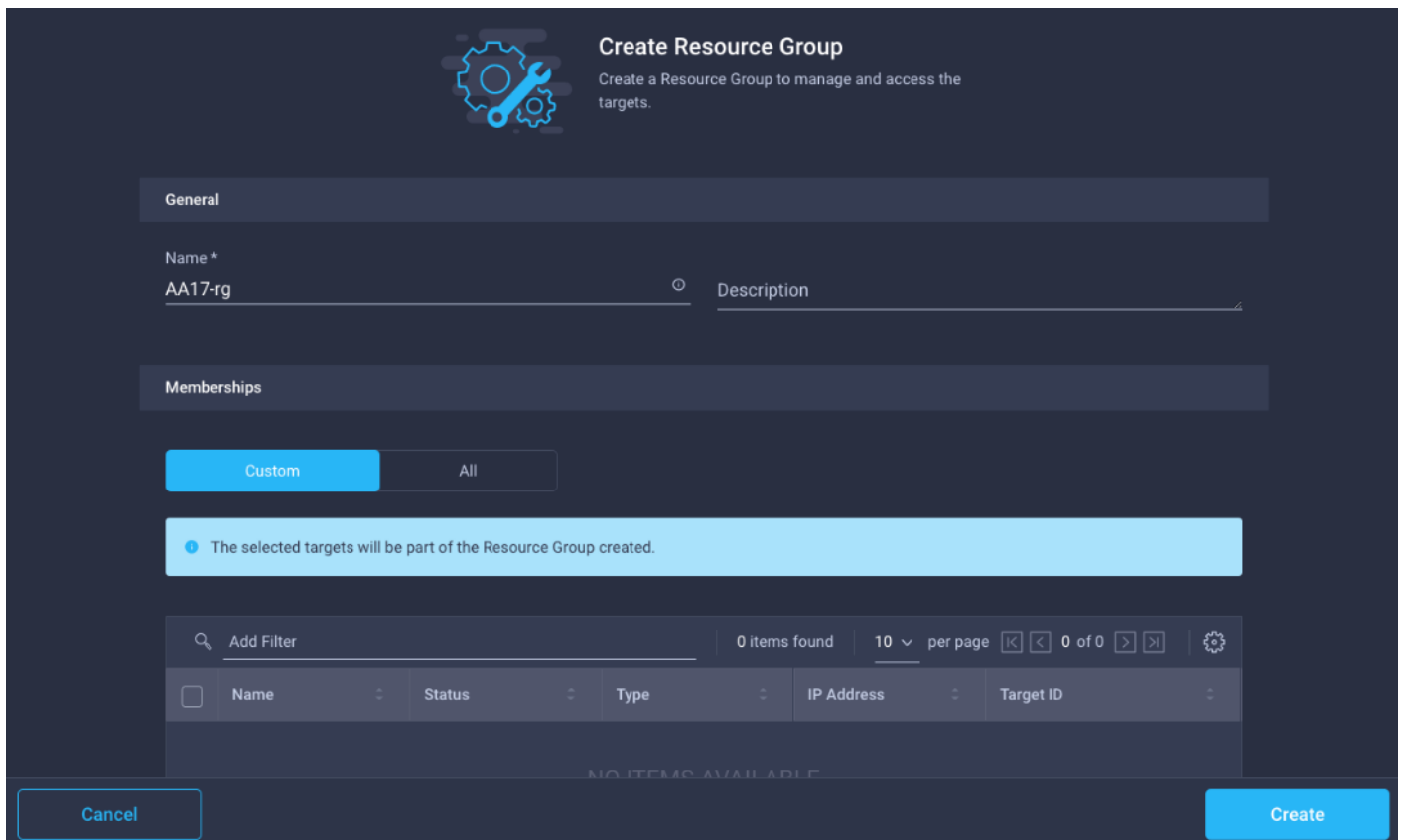


**Step 3.** Click **Resource Groups** in the middle panel.

**Step 4.** Click **+ Create Resource Group** in the top-right corner.



**Step 5.** Provide a name for the Resource Group (for example, AA17-rg).



**Step 6.** Under Memberships, click **Custom**.

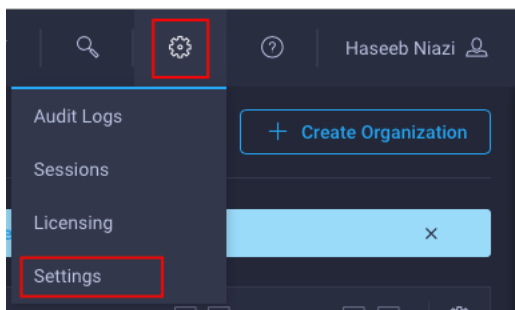
**Step 7.** Click **Create**.

### 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.

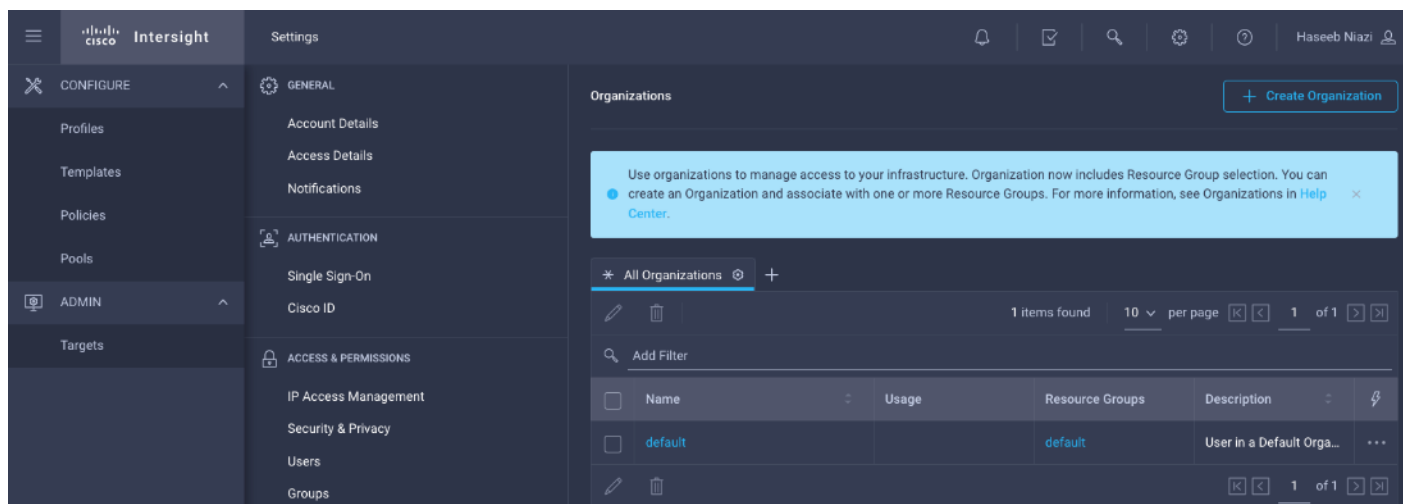
**Step 1.** Log into the Cisco Intersight portal.

**Step 2.** Click **Settings** (the gear icon) and choose **Settings**.



**Step 3.** Click **Organizations** in the middle panel.

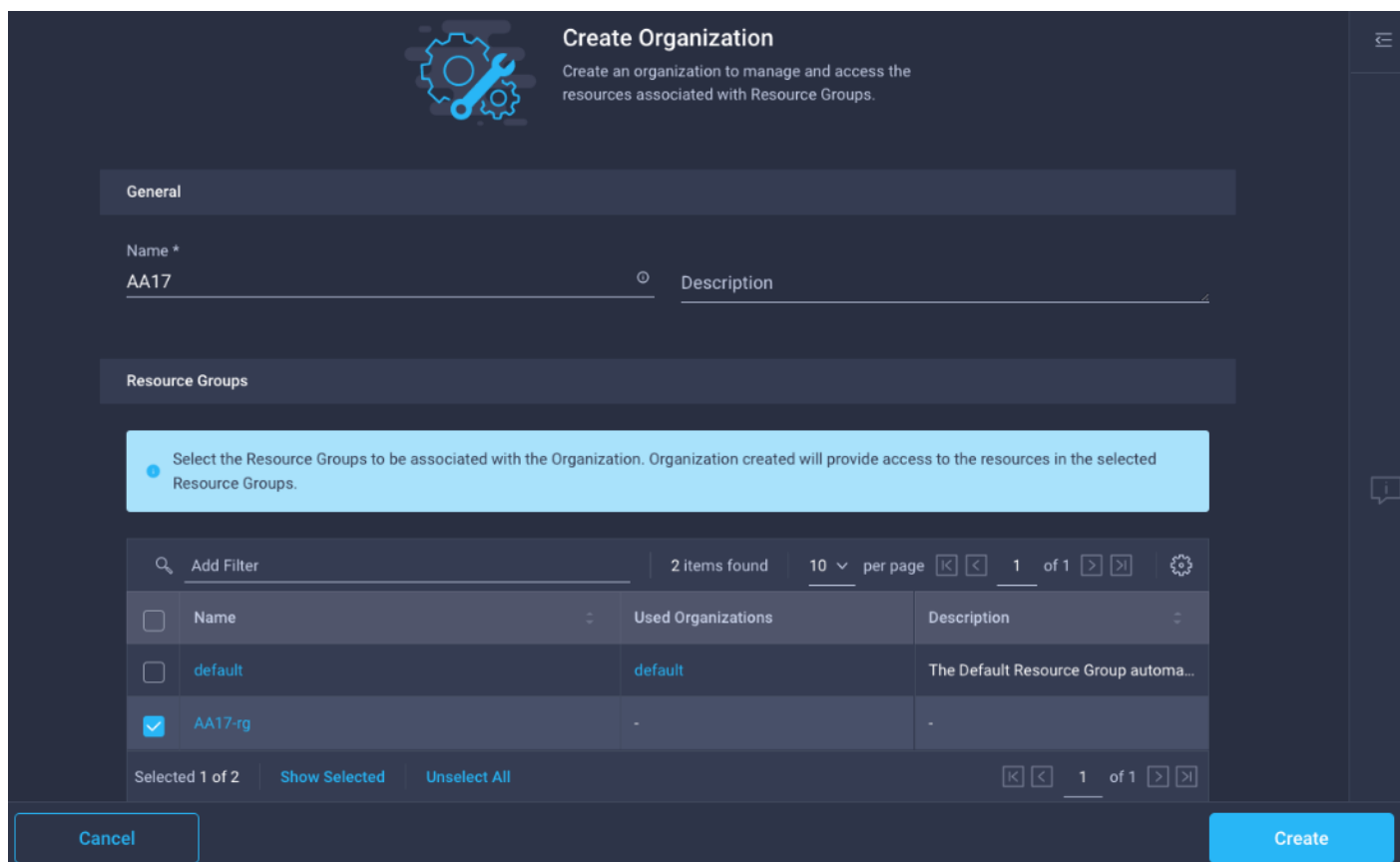
**Step 4.** Click **+ Create Organization** in the top-right corner.



**Step 5.** Provide a name for the organization (for example, AA17).

**Step 6.** Select the Resource Group created in the last step (for example, AA17-rg).

**Step 7.** Click **Create**.

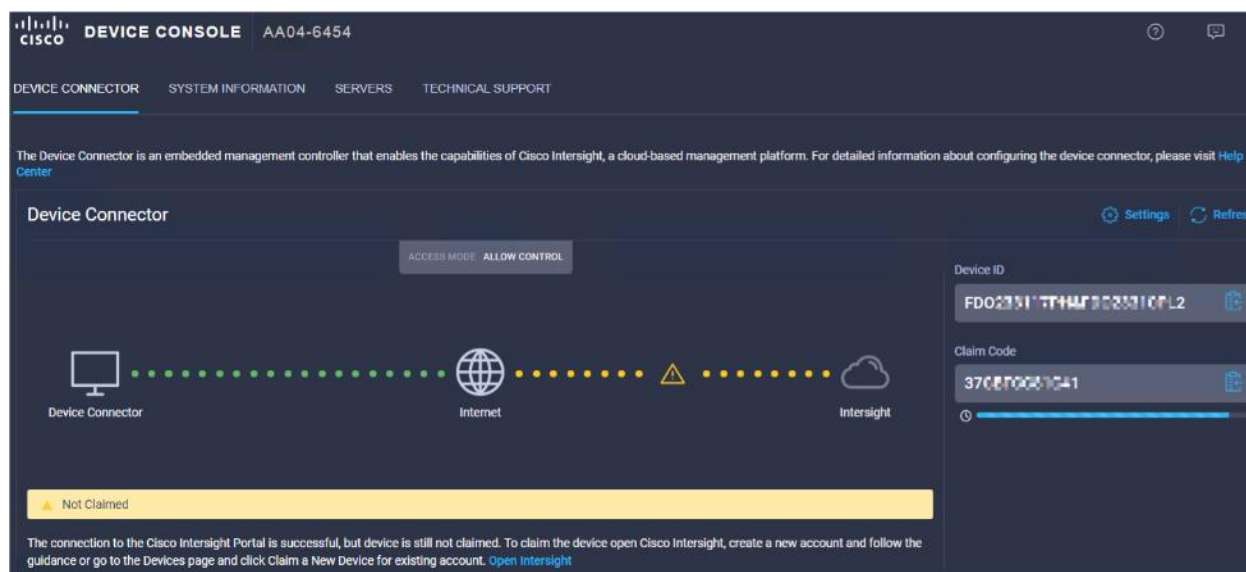


**Procedure 6.** Claim Cisco UCS Fabric Interconnects in Cisco Intersight

**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.

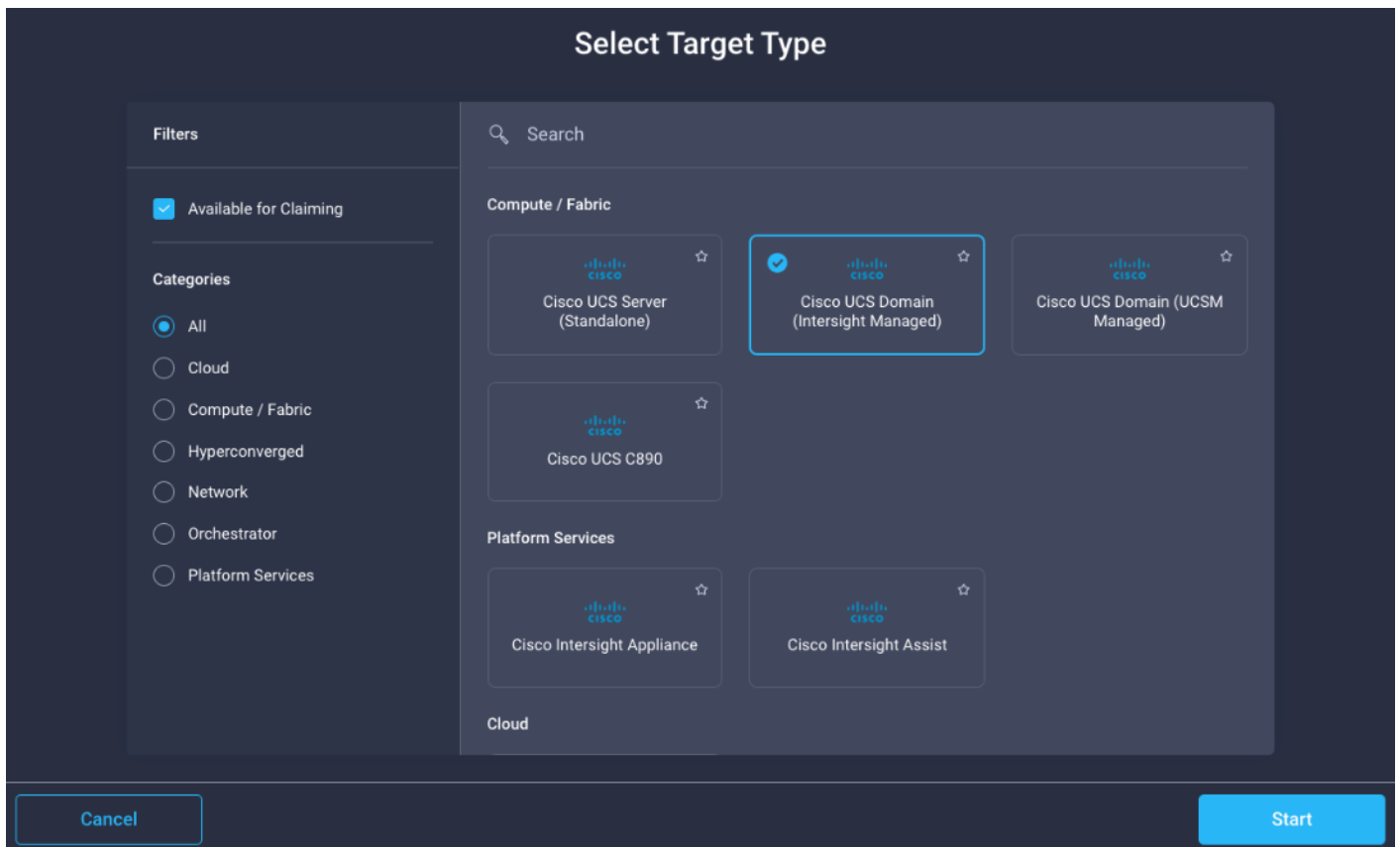


**Step 3.** Log into **Cisco Intersight**.

**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**.

**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'.

Name	Usage	Description
AA17-rg	AA17	

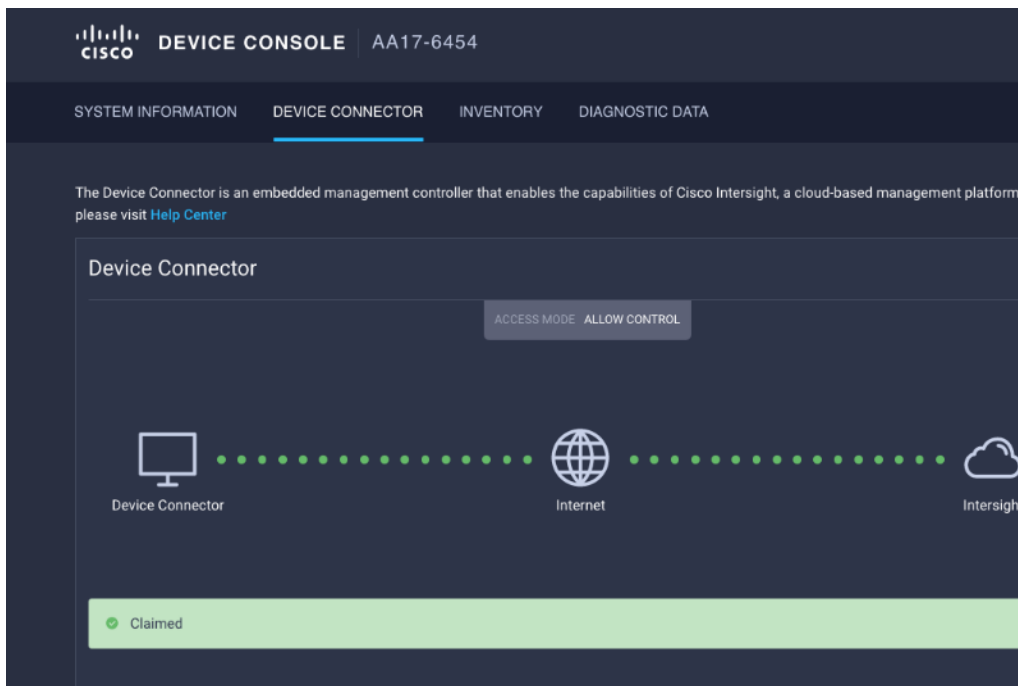
On successfully device claim, Cisco UCS FI should appear as a target in Cisco Intersight.

Name	Status	Name	Email	Resource Groups
AA17-6454	Connected	Intersight Mana...	hniazi@cisco.com	default, AA17-rg ... (2), default, AA17 ... (2)

**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

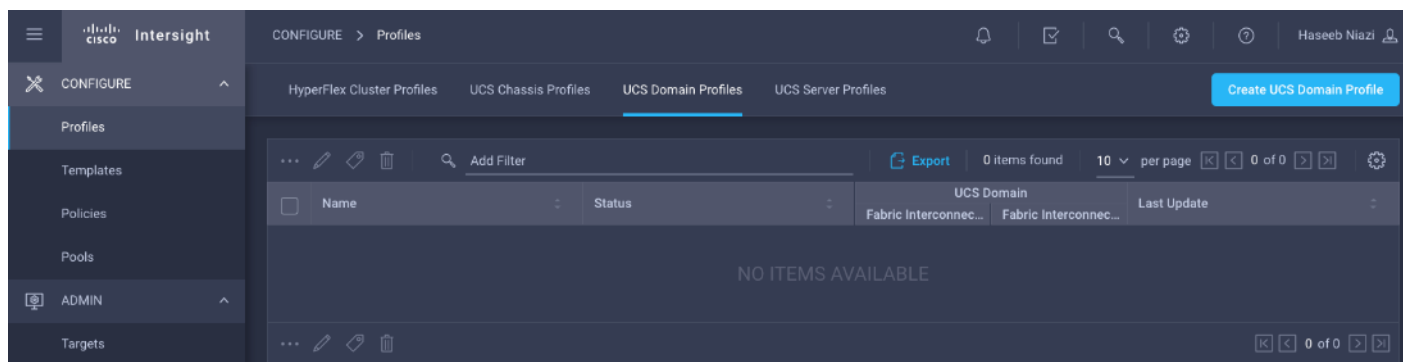
This subject contains the following procedures:

- [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](#)

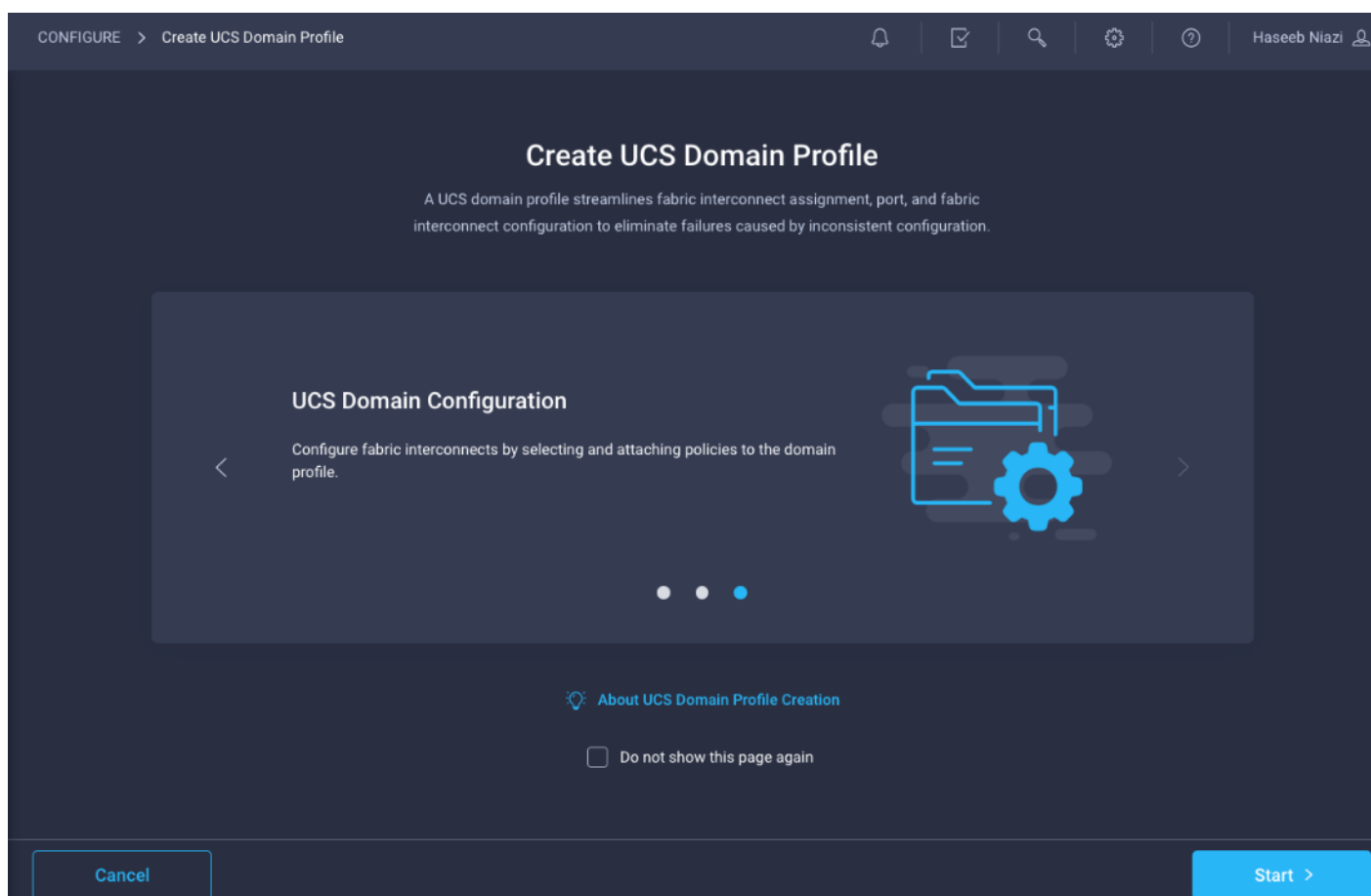
A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, allows configuration of the ports and port channels, and configures the VLANs and VSANs in the network. It defines the characteristics of and configured ports on fabric interconnects. The domain-related policies 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.** Click to expand **CONFIGURE** in the left pane and click **Profiles**.
- Step 3.** In the main window, click **UCS Domain Profiles** and click **Create UCS Domain Profile**.



**Step 4.** On the Create UCS Domain Profile screen, click **Start**.



## Procedure 2. General Configuration

- Step 1.** Select the organization from the drop-down list (for example, AA17).
- Step 2.** Provide a name for the domain profile (for example, AA17-Domain-Profile).
- Step 3.** Provide an optional Description.



Step 1  
**General**  
Add a name, description and tag for the UCS domain profile.

Organization \*  
AA17

Name \*  
AA17-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, AA17-6454).

**Progress**

- 1 General
- 2 UCS Domain Assignment**
- 3 VLAN & VSAN Configuration
- 4 Ports Configuration
- 5 UCS Domain Configuration
- 6 Summary

Step 2  
**UCS Domain Assignment**

Choose to assign a fabric interconnect pair to the profile now or later.

Assign Now
Assign 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

Domain Name	Fabric Interconnect A			Fabric Interconnect B		
	Model	Serial	Firmware Ver...	Model	Serial	Firmware Ver...
<input checked="" type="radio"/> AA17-6454	UCS-FI-6454	FD024350M...	9.3(5) 42(1f)	UCS-FI-6454	FDO24350G32	9.3(5) 42(1f)

< Back
Close
Next >

**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.



**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, AA17) and provide a name for the policy (for example, AA17-VLAN).

Step 1  
**General**  
Add a name, description and tag for the policy.

Organization \*  
AA17

Name \*  
AA17-VLAN

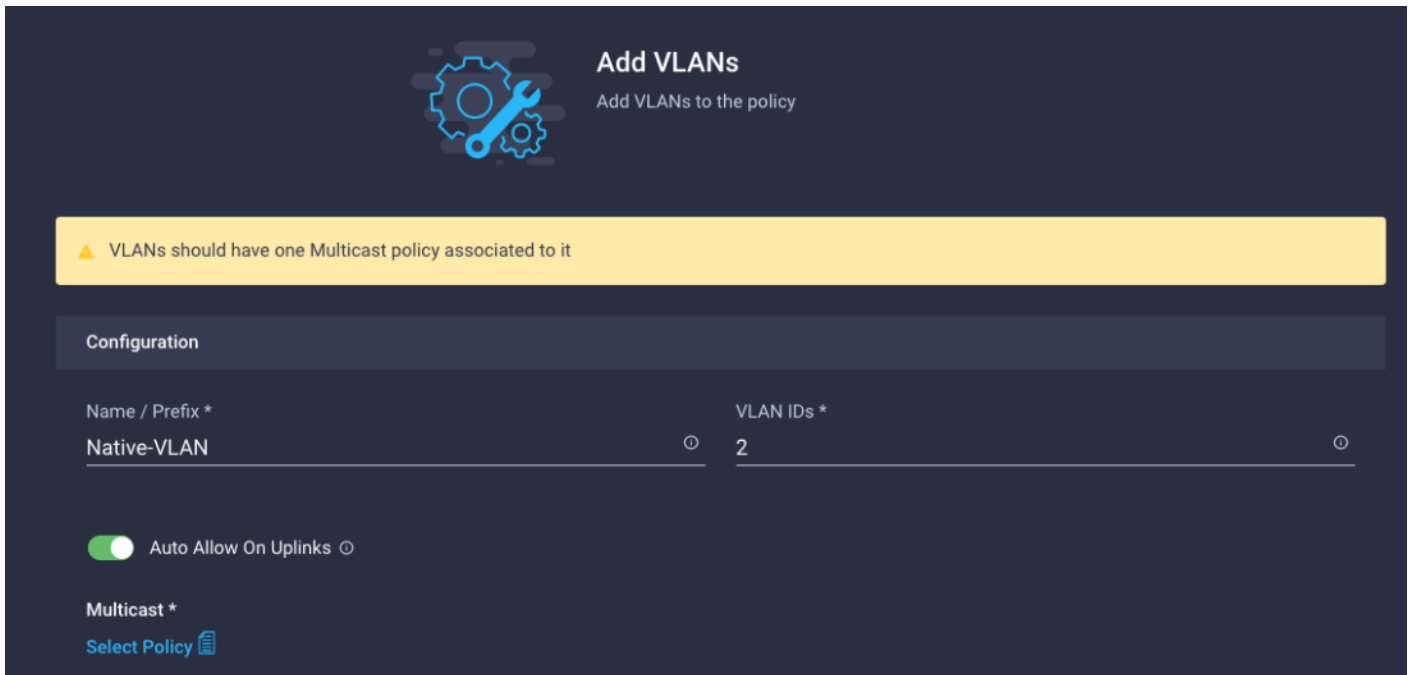
Set Tags

Description  
VLAN Policy for both FIs  
<= 1024

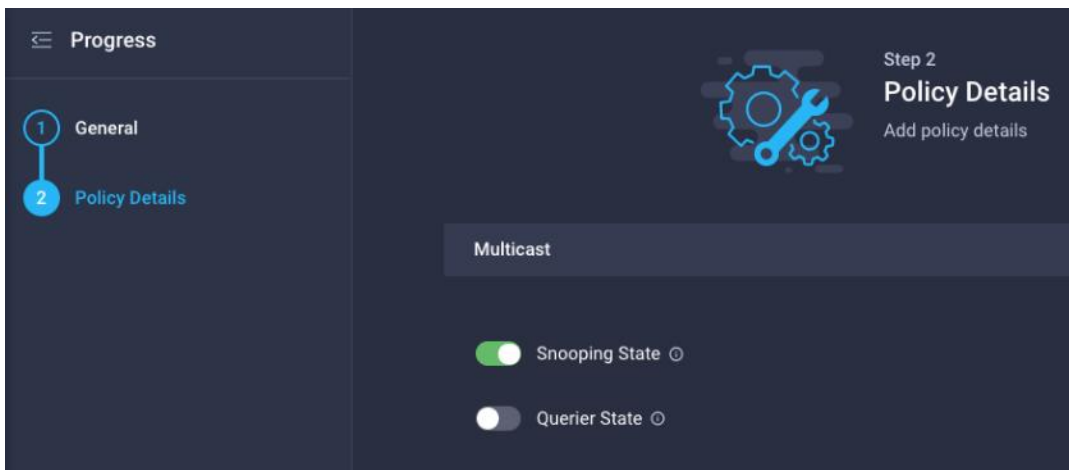
**Step 4.** Click **Next**.

**Step 5.** Click **Add VLANs**.

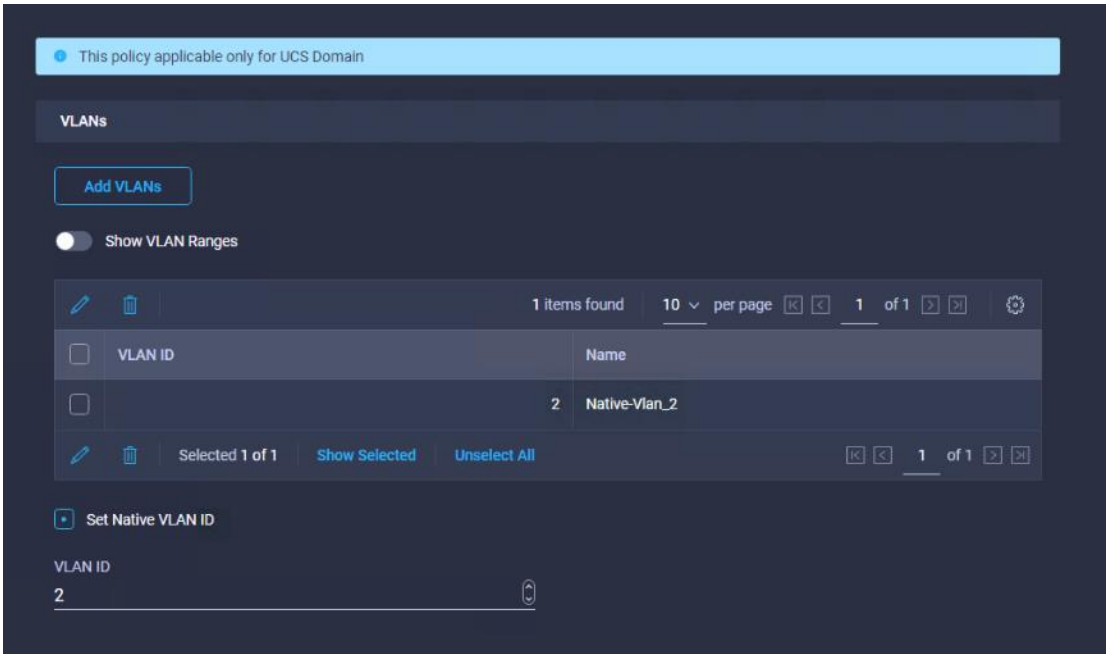
**Step 6.** Provide a name and VLAN ID for the native VLAN.



- 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, AA17-MCAST-Pol).
- Step 11.** Provide optional Description and click **Next**.
- Step 12.** Leave the Snooping State selected and click **Create**.



- 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.



**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	Multicast	Auto Allow On Uplinks
2	Native_2	AA17-MCAST-Pol	Yes
17	AA17-IB-Mgmt_17	AA17-MCAST-Pol	Yes
172	vm-traffic_172	AA17-MCAST-Pol	Yes
3017	nfs_3017	AA17-MCAST-Pol	Yes
3072	OOB-Mgmt_3072	AA17-MCAST-Pol	Yes
3117	iscsi-a_3117	AA17-MCAST-Pol	Yes
3217	iscsi-b_3217	AA17-MCAST-Pol	Yes
3317	vmotion_3317	AA17-MCAST-Pol	Yes

Set Native VLAN ID

VLAN ID  
2

**Note:** The iSCSI VLANs shown in the screen image above are only needed when iSCSI is configured in the environment.

**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)

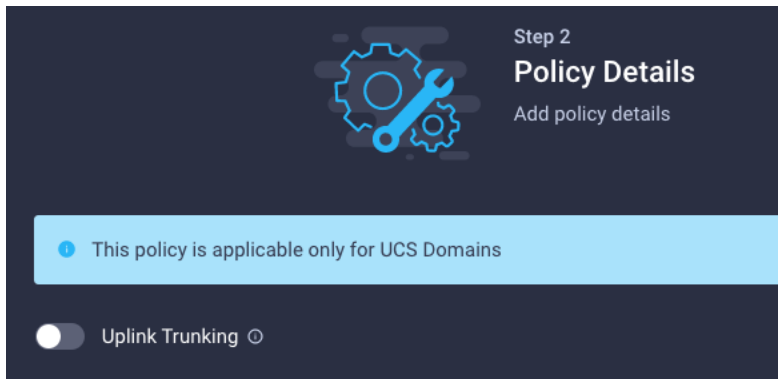
**Note:** A VSAN policy is only needed when configuring Fibre Channel and can be skipped when configuring IP-only storage access.

**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, AA17) and provide a name for the policy (for example, AA17-VSAN-Pol-A).

**Step 3.** Click **Next**.

**Step 4.** Enable **Uplink Trunking**.



**Step 5.** Click **Add VSAN** and provide a name (for example, VSAN-A), VSAN ID (for example, 101), and associated Fibre Channel over Ethernet (FCoE) VLAN ID (for example, 101) for SAN A.

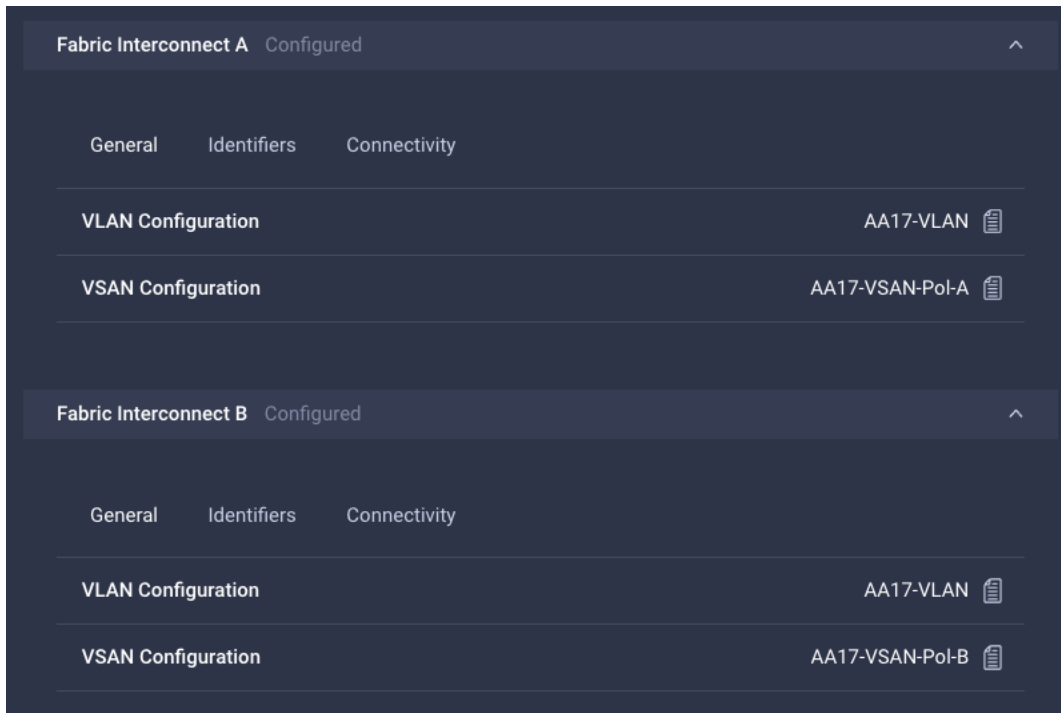
**Step 6.** Set VLAN Scope as **Uplink**.

**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, AA17-VSAN-Pol-B) and use appropriate VSAN and FCoE VLAN (for example, 102).

**Step 10.** Verify that a common VLAN policy and two unique VSAN policies are associated with the two fabric interconnects.



**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.

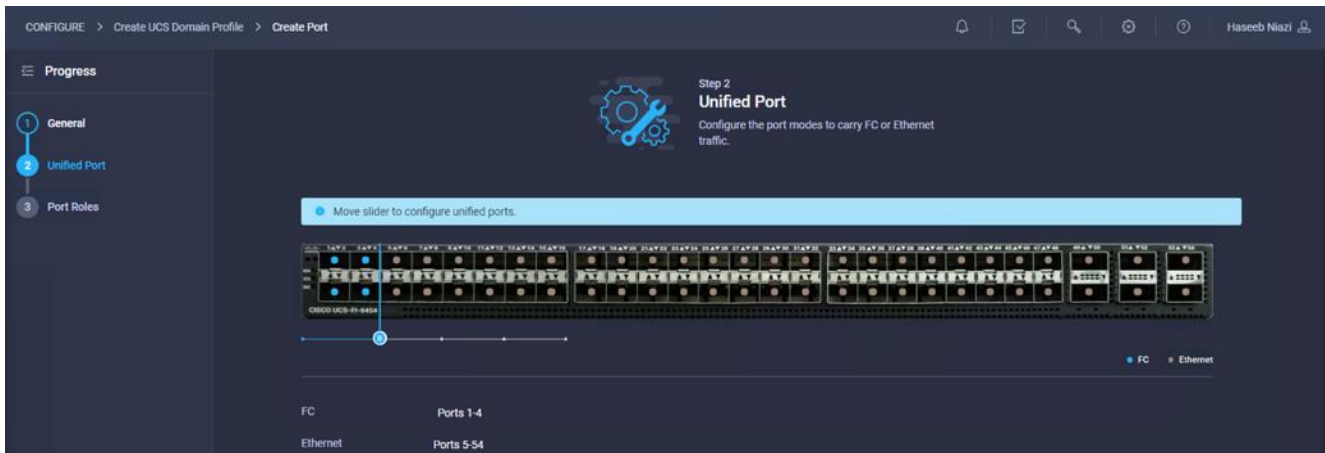
**Note:** Use two separate port policies for the fabric interconnects. Using separate policies provide flexibility when port configuration (port numbers or speed) differs between the two FIs. When configuring Fibre Channel, two port policies are required because each fabric interconnect uses unique Fibre Channel VSAN ID.

**Step 3.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the policy (for example, AA17-PortPol-A).

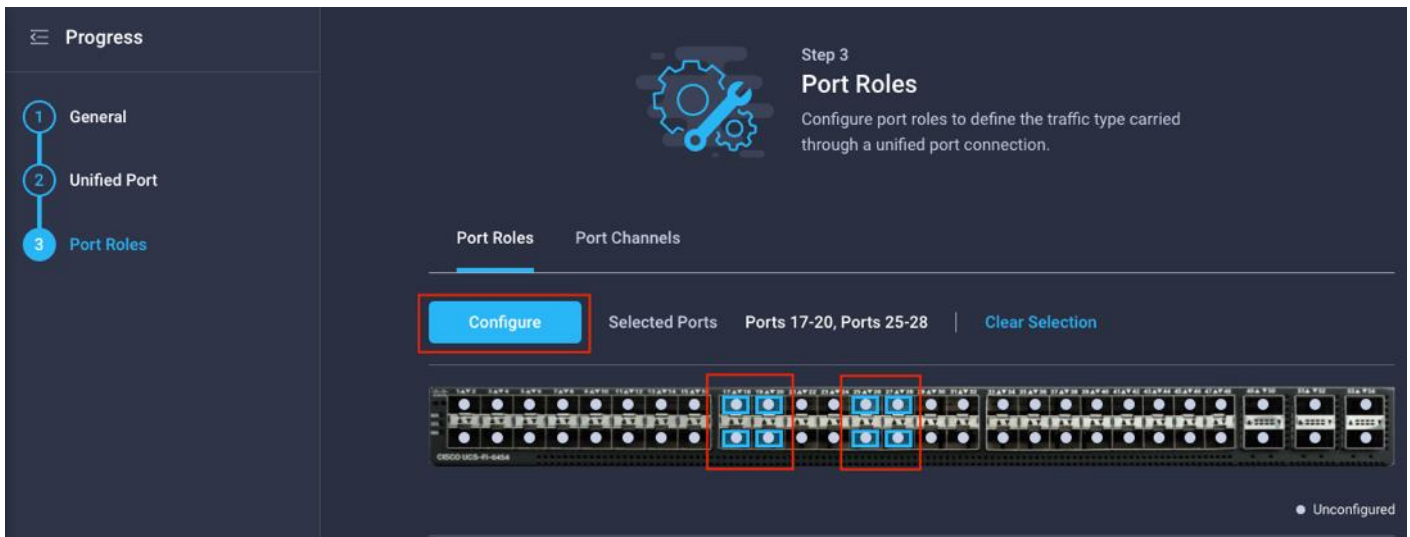
**Step 4.** Click **Next**.

**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**.

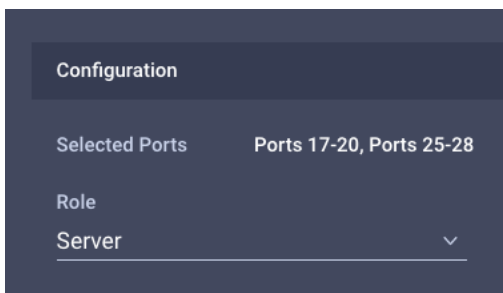




**Step 6.** Select the ports that need to be configured as server ports by clicking the ports in the graphics (or select from the list below the graphic). When all ports are selected, click **Configure**.

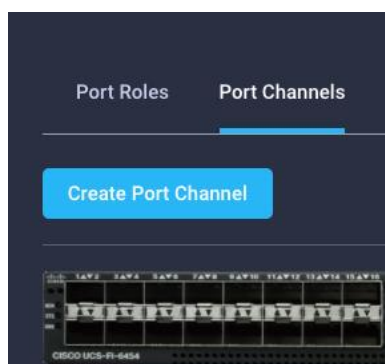


**Step 7.** From the drop-down list, select **Server** as the role.



**Step 8.** Click **Save**.

**Step 9.** Configure the Ethernet uplink port channel by selecting the Port Channel in the main pane and then clicking **Create Port Channel**.



**Step 10.** 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, Link 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 11.** Scroll down and select uplink ports from the list of available ports (for example, port 49 and 50)

**Step 12.** 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, 101).



## Create Port Channel

### Configuration

Role

FC Uplink Port Channel

Port Channel ID \*

1

1 - 256

Admin Speed

32Gbps

VSAN ID \*

101

1 - 4093

### Select 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.

**Step 3**  
**Port Roles**  
 Configure port roles to define the traffic type carried through a unified port connection.

Port Roles    Port Channels

Create Port Channel

ID	Role	Ports
11	Ethernet Uplink Port Channel	Port 49, Port 50
1	FC Uplink Port Channel	Port 3, Port 4

Legend: ● Ethernet Uplink Port Channel Member    ● FC Uplink Port Channel Member

**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: AA17-PortPol-B
- Ethernet port-Channel ID: 12
- FC port-channel ID: 2
- FC VSAN ID: 102

**Step 2.** When the port configuration for both fabric interconnects is complete and looks good, click **Next**.

## 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, AA17) and provide a name for the policy (for example, AA17-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.

The screenshot shows the 'Step 2 Policy Details' configuration interface. It features a gear icon and the text 'Add policy details'. A breadcrumb trail at the top right shows 'All Platforms' | 'UCS Server (Standalone)' | 'UCS Domain'. A toggle switch for 'Enable NTP' is turned on. Below this is a text input field labeled 'NTP Servers \*' containing the IP address '10.81.72.17' and a plus sign to the right. At the bottom, a dropdown menu for 'Timezone' is set to 'America/New\_York'.

**Step 6.** Click **Create**.

### Procedure 2. Configure Network Connectivity Policy

**Note:** To define the Domain 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, AA17) and provide a name for the policy (for example, AA17-NetConn-Pol).

**Step 3.** Provide DNS server IP addresses for Cisco UCS (for example, 10.81.72.40 and 10.81.72.41).

Step 2  
**Policy Details**  
Add policy details

All Platforms | UCS Server (Standalone) | UCS Domain

Common Properties

Enable Dynamic DNS

IPv4 Properties

Obtain IPv4 DNS Server Addresses from DHCP

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, AA17) and provide a name for the policy (for example, AA17-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.



## Step 2 Policy Details

Add policy details

This policy is applicable only for UCS Domains

### Configure Priorities

Platinum

Gold

Silver

Bronze

<input checked="" type="checkbox"/> Best Effort	CoS 255 ----- 0 - 6	Weight 5 ----- 0 - 10	<input checked="" type="checkbox"/> Allow Packet Drops	MTU 9216 ----- 1500 - 9216
<input checked="" type="checkbox"/> Fibre Channel	CoS 3 ----- 0 - 6	Weight 5 ----- 0 - 10	<input type="checkbox"/> Allow Packet Drops	MTU 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.

**Progress**

- General
- UCS Domain Assignment
- VLAN & VSAN Configuration
- Ports Configuration
- UCS Domain Configuration
- Summary**

**Step 6 Summary**  
Review the UCS domain profile details, resolve configuration errors and deploy the profile.

**General**

Name	AA17-Domain-Profile	Status
Organization	AA17	

Fabric Interconnect	Model	Serial	Requires Reboot
AA17-6454 FI-A	UCS-FI-6454	FD ■■■■	No
AA17-6454 FI-B	UCS-FI-6454	FD ■■■■	No

Ports Configuration | VLAN & VSAN Configuration | UCS Domain Configuration | Errors / Warnings

Fabric Interconnect A

Fabric Interconnect B

### 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

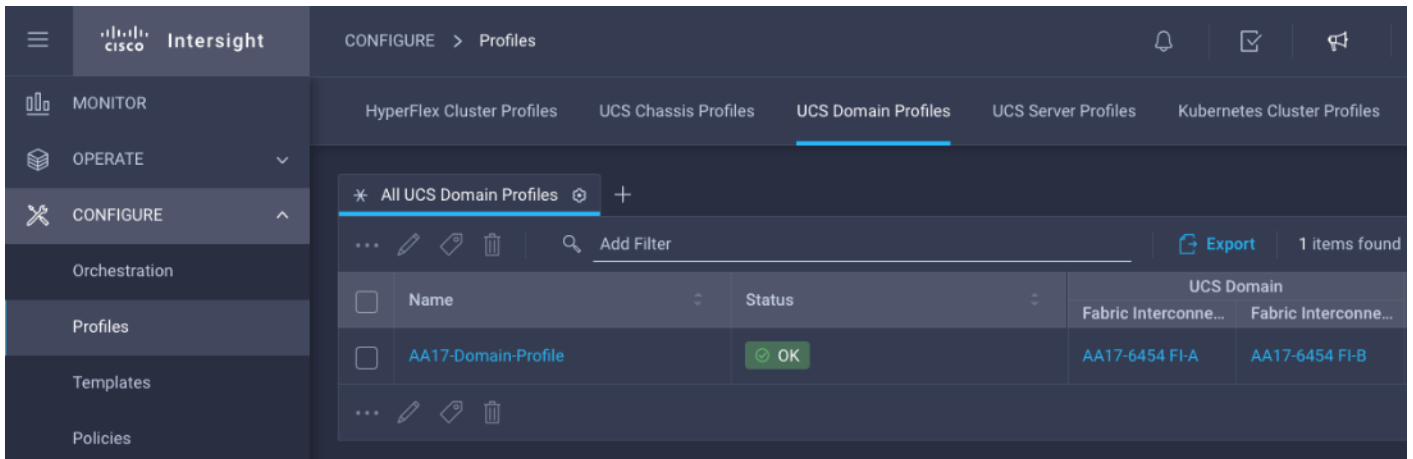
When the Cisco UCS domain profile has been successfully deployed, the Cisco UCS chassis and the blades should be successfully discovered.

**Note:** It takes a while to discover the blades for the first time. Watch the number of outstanding tasks in Cisco Intersight:

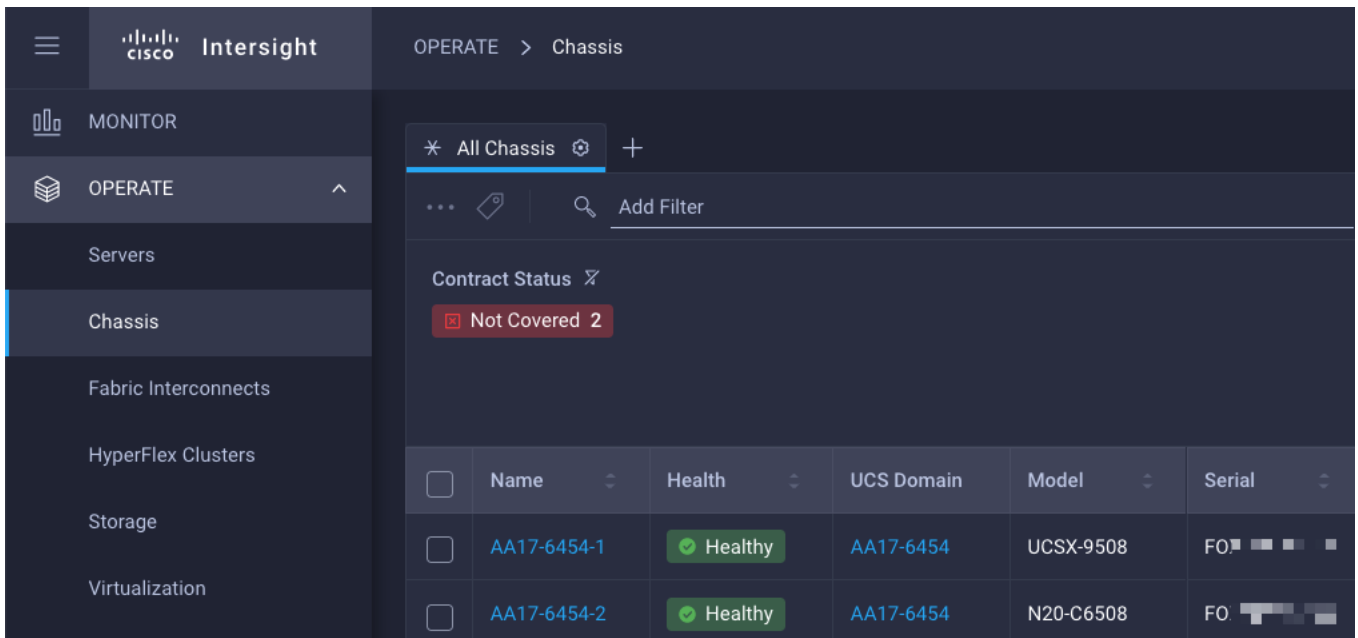


**Step 1.** Log into **Cisco Intersight**. Under **CONFIGURE > Profiles > UCS Domain Profiles**, verify that the domain profile has been successfully deployed.





**Step 2.** Verify that the chassis has been discovered and is visible under **OPERATE > Chassis**.



**Step 3.** Verify that the servers have been successfully discovered and are visible under **OPERATE > Servers**.

<input type="checkbox"/>	AA17-6454-1-1	UCSX-210C-M6	140.8	5.0(1b)
<input type="checkbox"/>	AA17-6454-1-2	UCSX-210C-M6	140.8	5.0(1b)
<input type="checkbox"/>	AA17-6454-1-3	UCSX-210C-M6	140.8	5.0(1b)
<input type="checkbox"/>	AA17-6454-1-5	UCSX-210C-M6	166.4	5.0(1b)
<input type="checkbox"/>	AA17-6454-1-6	UCSX-210C-M6	166.4	5.0(1b)
<input type="checkbox"/>	AA17-6454-1-7	UCSX-210C-M6	166.4	5.0(1b)

## 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.

**Note:** The server profile captured in this deployment guide supports both Cisco UCS B200 M6 blade servers and Cisco UCS X210c M6 compute nodes.

## 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 15. vHBA and vNIC placement for FC connected storage**

vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-A	MLOM	A	0

vNIC/vHBA Name	Slot	Switch ID	PCI Order
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 16. 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	
vHBA-NVMe-A	MLOM	A	6	Used for NVMe-o-FC
vHBA-NVMe-B	MLOM	B	7	Used for NVMe-o-FC

### 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, AA17).
- Step 4.** Provide a name for the server profile template. The names used in this deployment are:
  - FC-Boot-Template (FC boot from SAN)
  - FC-Boot-NVME-Template (FC boot from SAN with support for NVMe-o-FC).

**Step 5.** Click **UCS Server (FI-Attached)**.

**Step 6.** Provide an optional description.

**Step 1**  
**General**

Enter a name, description, tag and select a platform for the server profile.

Organization \*  
X-Series

Name \*  
FC-Boot-vdi

Target Platform  UCS Server (Standalone)  UCS Server (FI-Attached)

Set Tags

Description  
Supports FC

<= 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, AA17) and provide a name for the UUID Pool (for example, AA17-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.

The screenshot shows a configuration interface with a dark theme. At the top, there is a section titled "Configuration". Below this, there is a field for "Prefix \*" containing the value "33FB3F9C-BF35-4BDE". Below the prefix field is a section titled "UUID Blocks". Underneath, there is a table with two columns: "From \*" and "Size \*". The first row in the table has the value "0000-0000A1700001" in the "From \*" column and "64" in the "Size \*" column. To the right of the "Size \*" column, there are two small circular icons with arrows, and a plus sign. At the bottom right of the table, there is a range indicator "1 - 1000".

**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, AA17) and provide a name for the policy (for example, AA17-NTPPol).

**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>.



## Step 2 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

- 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 including hosts that support NVMe-o-FC storage access.

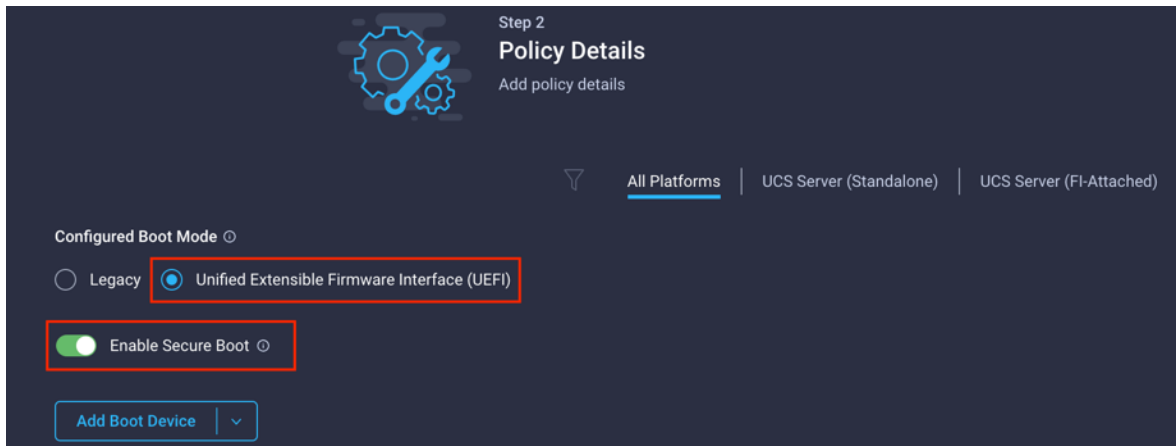
**Step 1.** Click **Select Policy** next to BIOS Configuration and then click **Create New**.

**Step 2.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the policy (for example, AA17-FC-BootOrder-Pol).

**Step 3.** Click **Next**.

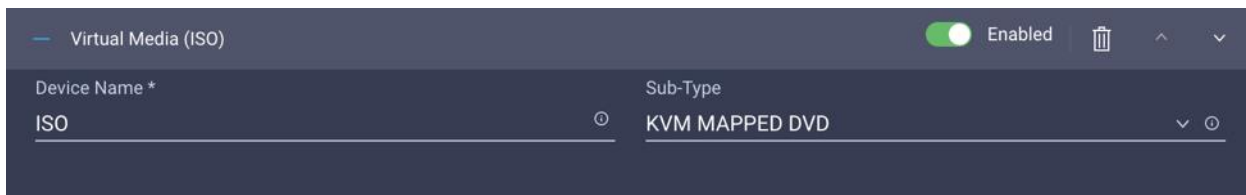
**Step 4.** For Configured Boot Mode, select **Unified Extensible Firmware Interface (UEFI)**.

**Step 5.** Turn on **Enable Secure Boot**.



**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**.



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 \*  


LUN      
0 - 255

Slot  

Interface Name \*  

Target WWPN \*  




Bootloader Name  


Bootloader Description  

**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**.

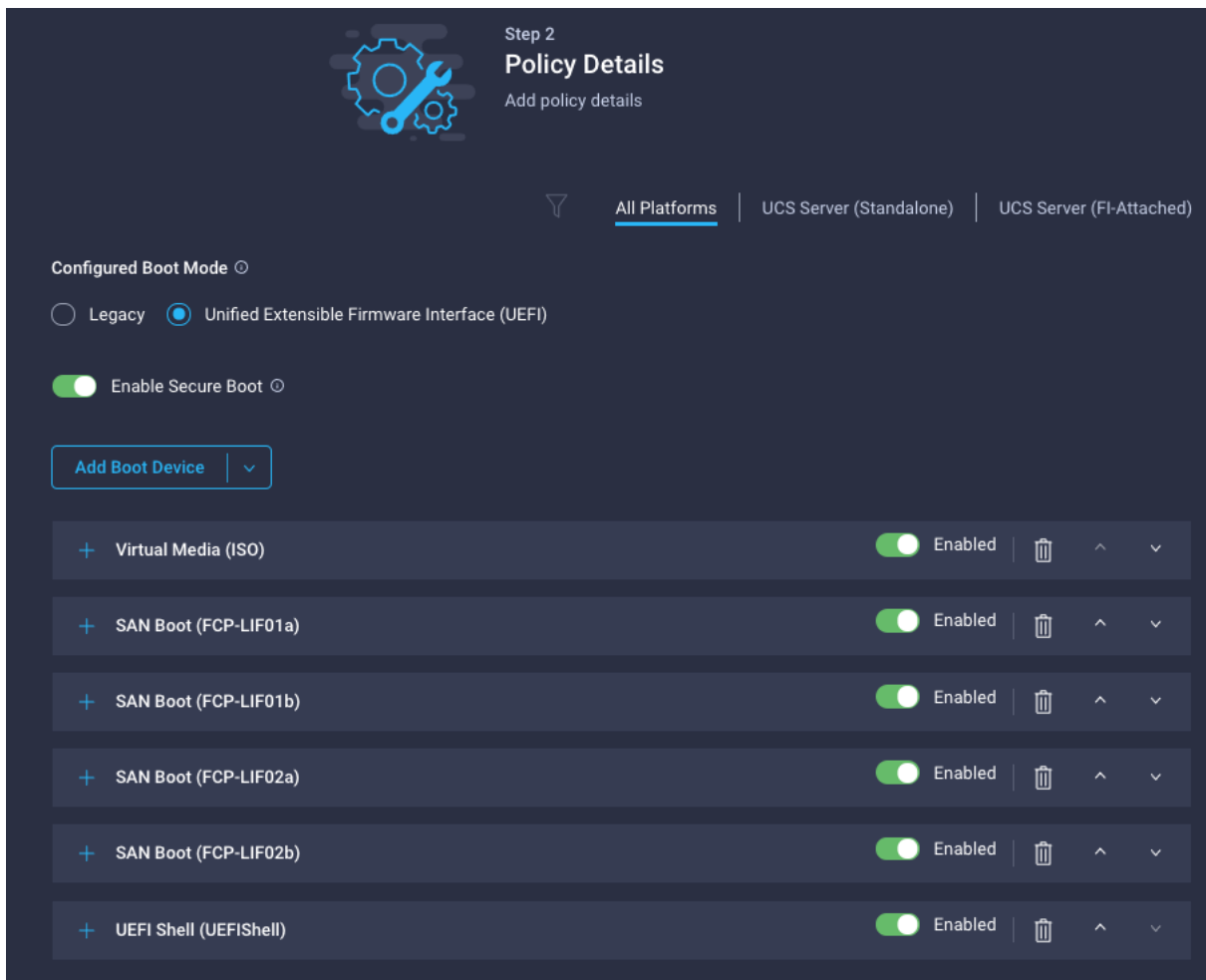
**Step 14.** Add Device Name **UEFIShell**.

UEFI Shell (UEFIShell) Enabled   

Device Name \*  

**Step 15.** Verify the order of the boot policies and adjust the boot order as necessary using arrows next to delete button.





**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 1. Configure Cisco IMC Access Policy

**Step 1.** Click **Select Policy** next to IMC Access and then click **Create New**.

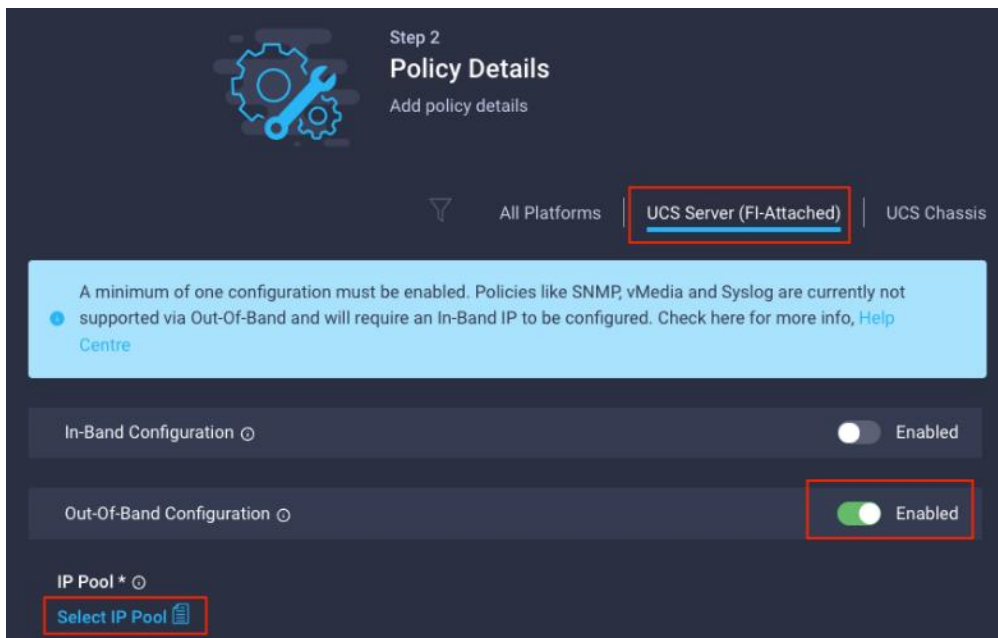
**Step 2.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the policy (for example, AA17-IMC-Access).

**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 17) 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)**.

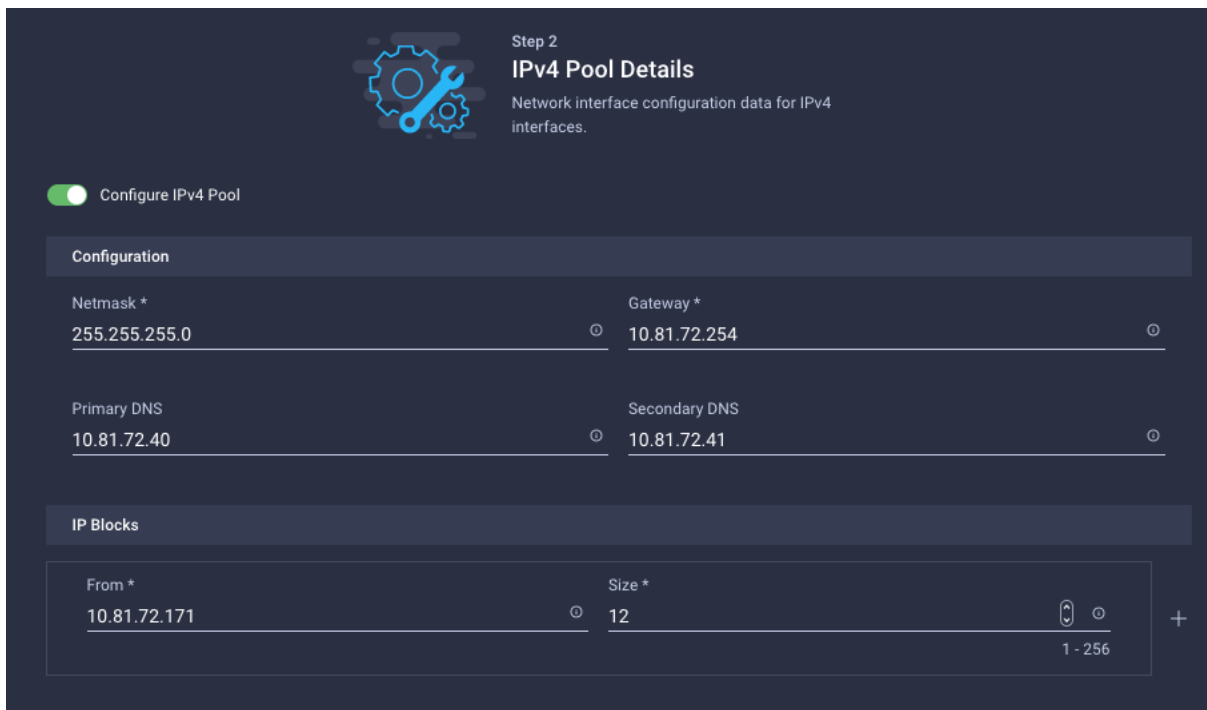
**Step 5. Enable Out-Of-Band Configuration.**



**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, AA17) and provide a name for the policy (for example, AA17-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.



**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 2. Configure IPMI Over LAN Policy

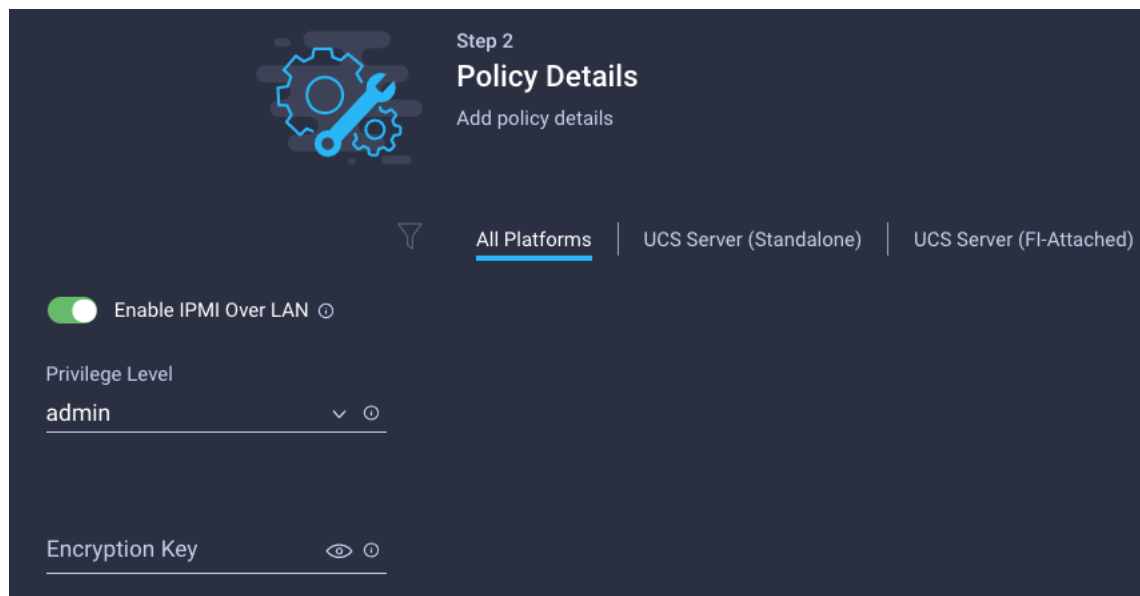
**Step 1.** Click **Select Policy** next to IPMI Over LAN and then click **Create New**.

**Step 2.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the policy (for example, Enable-IPMIoLAN).

**Step 3.** Turn on **Enable IPMI Over LAN**.

**Step 4.** From the **Privilege Level** drop-down list, select **admin**.

**Step 5.** Click **Create**.



The screenshot shows the 'Policy Details' configuration page. At the top, there is a gear icon and the text 'Step 2 Policy Details Add policy details'. Below this is a filter menu with three options: 'All Platforms', 'UCS Server (Standalone)', and 'UCS Server (FI-Attached)'. The 'Enable IPMI Over LAN' toggle is turned on. The 'Privilege Level' dropdown is set to 'admin'. The 'Encryption Key' field is visible at the bottom.

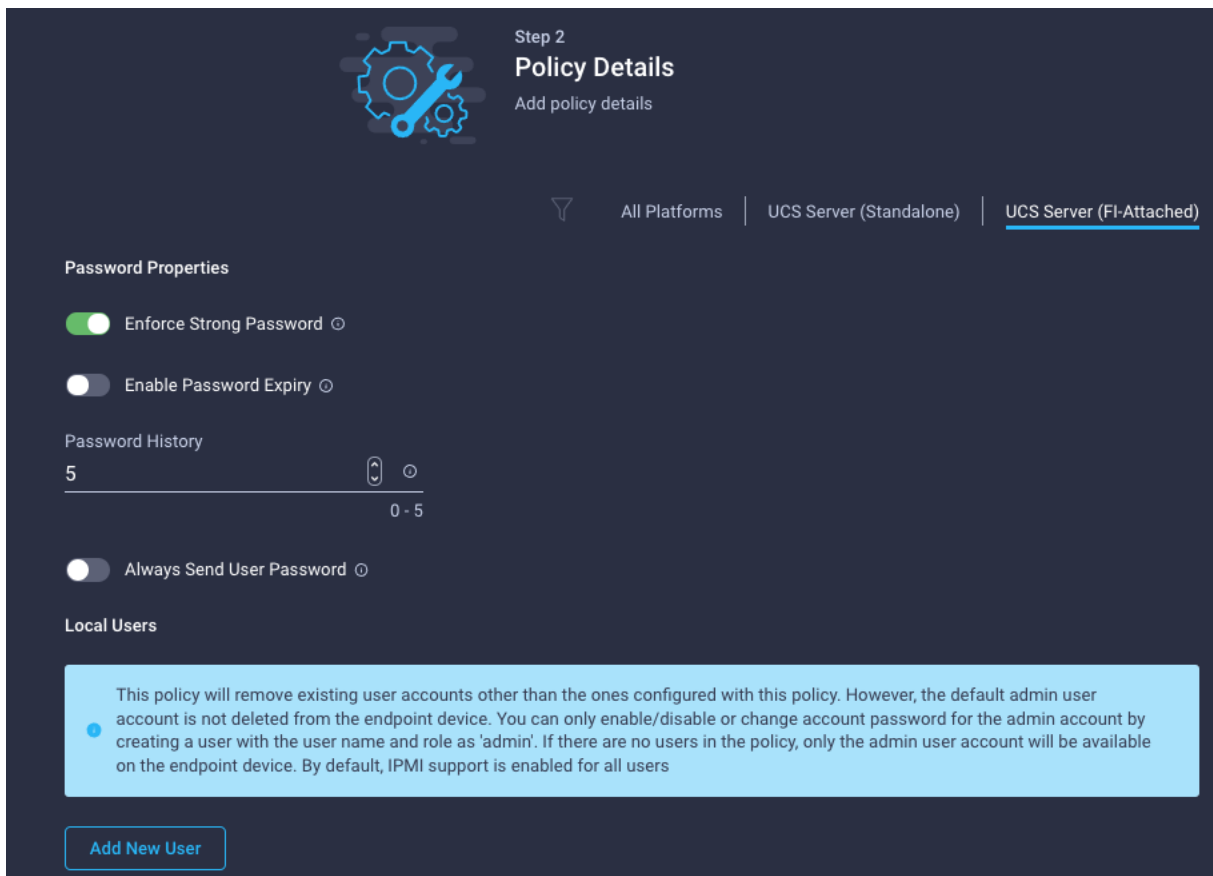
## Procedure 3. Configure Local User Policy

**Step 1.** Click **Select Policy** next to Local User and then, in the pane on the right, click **Create New**.

**Step 2.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the policy (for example, AA17-LocalUser-Pol).

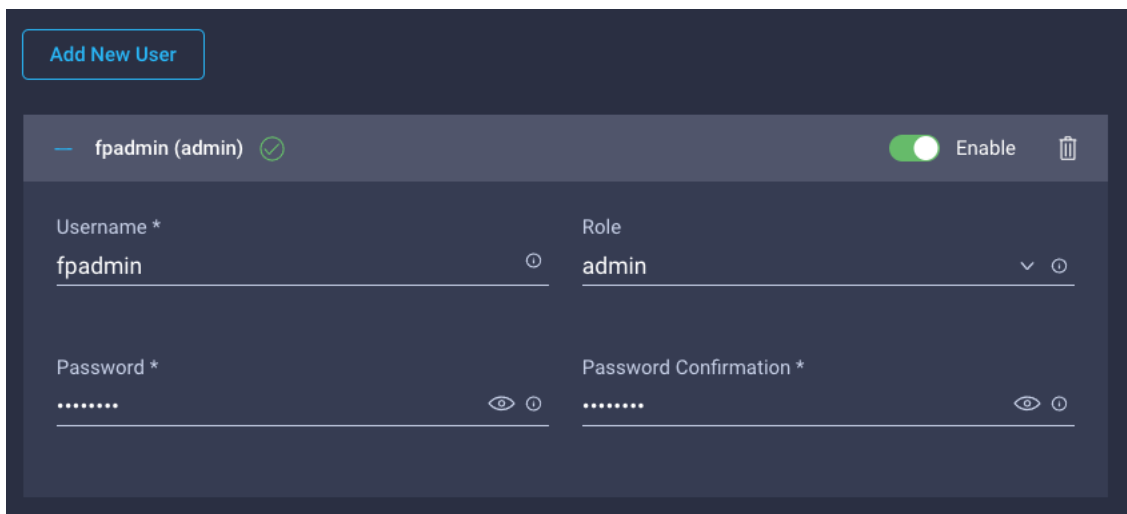
**Step 3.** Verify that **UCS Server (FI-Attached)** is selected.

**Step 4.** Verify that **Enforce Strong Password** is selected.



**Step 5.** Click **Add New User** and then click **+** next to the New User

**Step 6.** Provide the username (for example, fpadding), choose a role for example, admin), and provide a password.



**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 4. 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 5. Create LAN Connectivity Policy for FC Hosts**

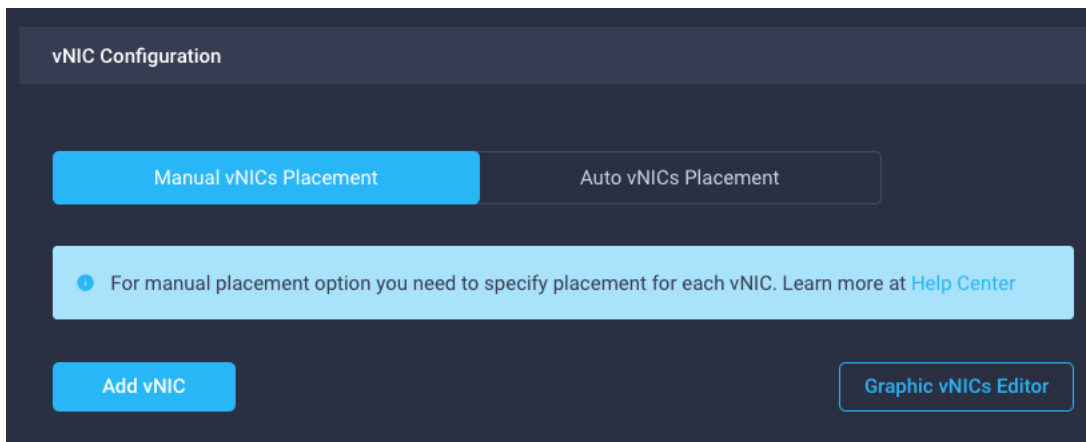
The FC boot from SAN hosts uses 4 vNICs configured as follows:

**Table 17. 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, AA17) and provide a name for the policy (for example, AA17-FC-ESXi-LanConn). Click **Next**.
- Step 3.** Under vNIC Configuration, select **Manual vNICs Placement**.
- Step 4.** Click **Add vNIC**.



### Procedure 6. 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 18. 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**.

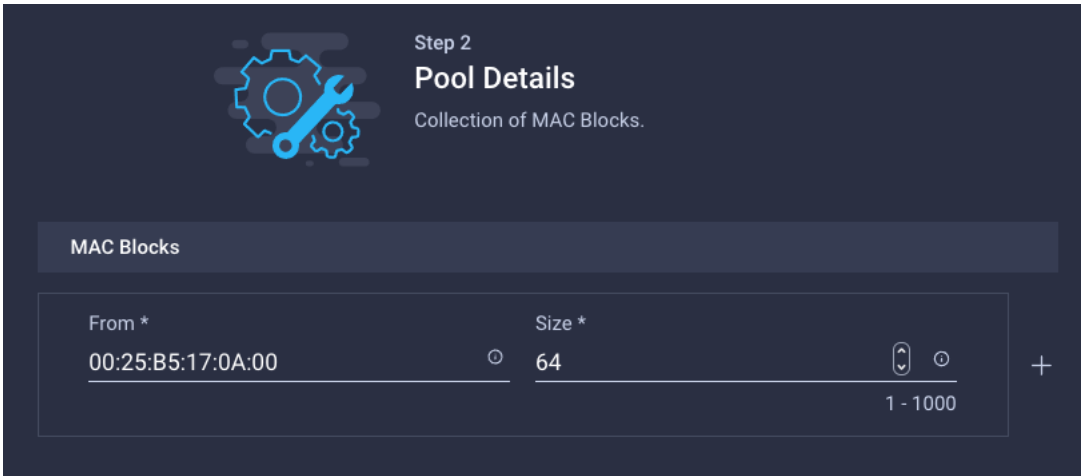
**Step 2.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the pool from Table 18 depending on the vNIC being created (for example, MAC-Pool-A for Fabric A).

**Step 3.** Click **Next**.

**Step 4.** Provide the starting MAC address from [Table 18](#) (for example, 00:25:B5:17:0A:00)

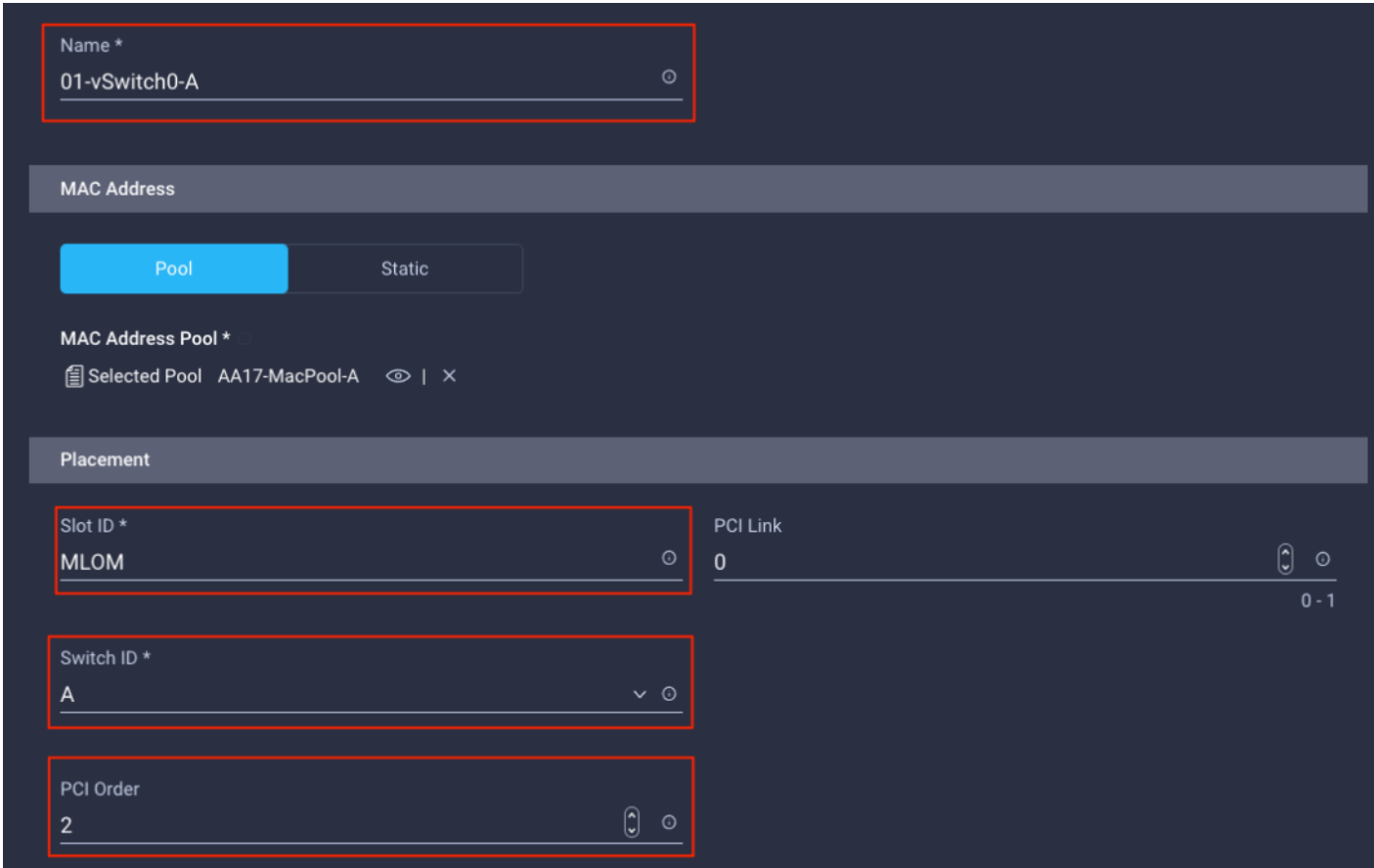
**Note:** For troubleshooting FlexPod, some additional information is always coded into the MAC address pool. For example, in the starting address 00:25:B5:17:0A:00, 17 is the rack ID and 0A indicates Fabric A.

**Step 5.** Provide the size of the MAC address pool from [Table 18](#) (for example, 64).



**Step 6.** Click **Create** to finish creating the MAC address pool.

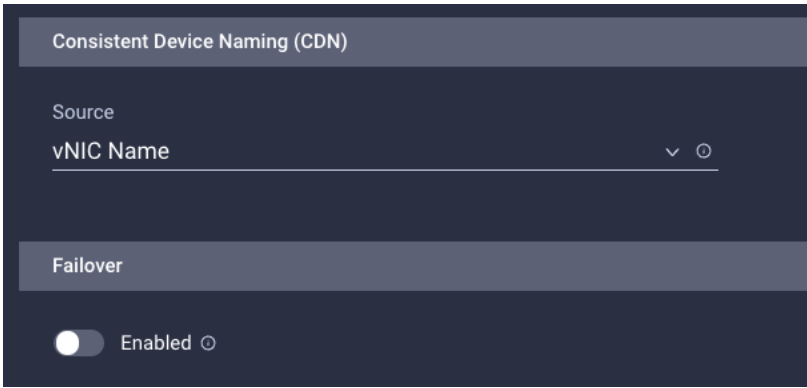
**Step 7.** From the Add vNIC window, provide vNIC Name, Slot ID, Switch ID and PCI Order information from [Table 17](#).



**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.





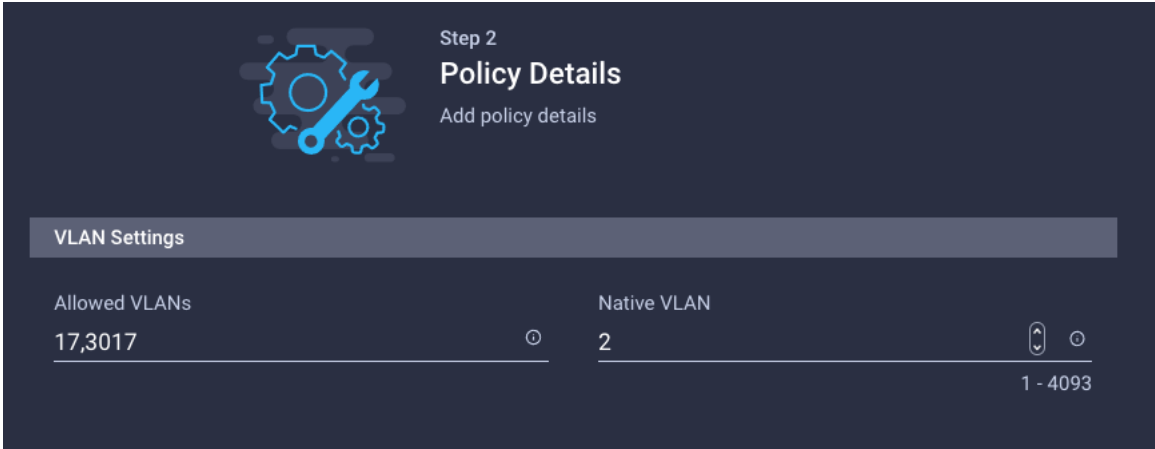
**Procedure 7. Create Ethernet Network Group Policy for a vNIC**

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 19. Ethernet Group Policy Values**

Group Policy Name	Native VLAN	Apply to vNICs	VLANs
AA17-vSwitch0-NetGrp	Native-VLAN (2)	01-vSwitch0-A, 02-vSwitch0-B	1B-MGMT, NFS
AA17-VDS0-NetGrp	Native-VLAN (2)	03-VDS0-A, 04-VDS0-B	VM Traffic, vMotion

- Step 1.** Click **Select Policy** under Ethernet Network Group Policy and then click **Create New**.
- Step 2.** Verify correct organization is selected from the drop-down list (for example, AA17) and provide a name for the policy from [Table 19](#) (for example, AA17-vSwitch0-NetGrp).
- Step 3.** Click **Next**.
- Step 4.** Enter the allowed VLANs from [Table 19](#) (for example, 17,3017) and the native VLAN ID from [Table 19](#) (for example, 2).



- Step 5.** 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 8. 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, AA17) and provide a name for the policy (for example, AA17-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

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

Enable Receive

**Step 5.** Click **Create** to finish creating Ethernet network control policy.

### Procedure 9. 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, AA17) and provide a name for the policy (for example, AA17-EthQos-Pol).

**Step 3.** Click **Next**.

**Step 4.** Change the MTU, Bytes value to **9000**.

The screenshot shows the 'Policy Details' configuration page for a UCS Server (FI-Attached). The page is titled 'Step 2 Policy Details' with the subtitle 'Add policy details'. There are three tabs: 'All Platforms', 'UCS Server (Standalone)', and 'UCS Server (FI-Attached)'. The 'UCS Server (FI-Attached)' tab is selected. Under 'QoS Settings', there are four input fields: 'MTU, Bytes' (9000), 'Rate Limit, Mbps' (0), 'Burst' (10240), and 'Priority' (Best-effort). Each field has a range indicator below it: '1500 - 9000' for MTU, '0 - 100000' for Rate Limit, '1 - 1000000' for Burst, and a dropdown arrow for Priority. At the bottom, there is a toggle switch for 'Enable Trust Host CoS' which is currently turned off.

**Step 5.** Click **Create** to finish setting up the Ethernet QoS policy.

## Procedure 10. 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, AA17-VMware-High-Traffic, is created and attached to the 03-VDS0-A and 04-VDS0-B interfaces which handle vMotion.

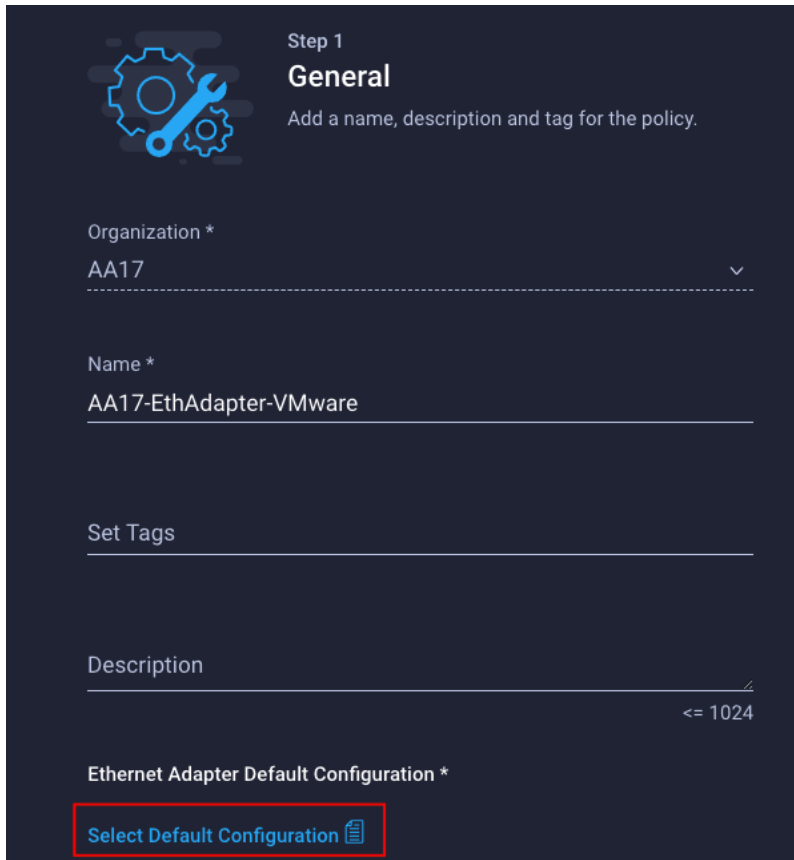
**Table 20. Ethernet Adapter Policy association to vNICs**

Policy Name	vNICs
AA17-EthAdapter-VMware	01-vSwitch0-A, 02-vSwitch0-B
AA17-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, AA17) and provide a name for the policy (for example, AA17-EthAdapter-VMware).

**Step 3.** Click **Select Default Configuration** under Ethernet Adapter Default Configuration.



Step 1  
**General**  
Add a name, description and tag for the policy.

Organization \*  
AA17

Name \*  
AA17-EthAdapter-VMware

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 AA17-EthAdapter-VMware policy, click **Create** and skip the rest of the steps in this section.

**Step 7.** For the optional AA17-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 (range 1 - 1024)

Interrupt Mode: MSIx

Interrupt Timer, us: 125 (range 0 - 65535)

Interrupt Coalescing Type: Min

**Receive**

Receive Queue Count: 8 (range 1 - 1000)

Receive Ring Size: 512 (range 64 - 4096)

**Transmit**

Transmit Queue Count: 1 (range 1 - 1000)

Transmit Ring Size: 256 (range 64 - 4096)

**Completion**

Completion Queue Count: 9 (range 1 - 2000)

Completion Ring Size: 1 (range 1 - 256)

Uplink Failback Timeout (seconds): 5 (range 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

- 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.

<input type="checkbox"/>	Name	Slot ID	Switch ID	PCI Link	PCI Order	Failover	⚡
<input type="checkbox"/>	01-vSwitch0-A	MLOM	A	0	2	Disabled	...
<input type="checkbox"/>	03-VDS0-A	MLOM	A	0	4	Disabled	...
<input type="checkbox"/>	02-vSwitch0-B	MLOM	B	0	3	Disabled	...
<input type="checkbox"/>	04-VDS0-B	MLOM	B	0	5	Disabled	...

**Step 12.** Click **Create** to finish creating the LAN Connectivity policy for FC hosts.

### Procedure 11. 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 21](#) lists the details of two vHBAs that are used to provide FC connectivity and boot from SAN functionality.

**Table 21. vHBA for boot from FC SAN**

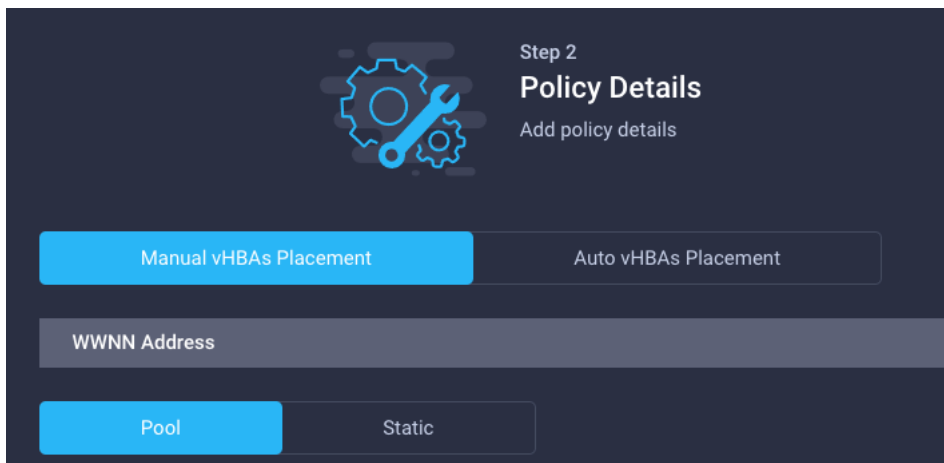
vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-A	MLOM	A	0
vHBA-B	MLOM	B	1

**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, AA17) and provide a name for the policy (for example, AA17-SanConn-Pol).

**Step 3.** Select **Manual vHBAs Placement**.

**Step 4.** Select **Pool** under WWNN Address.



### Procedure 12. Create the WWNN Address Pool

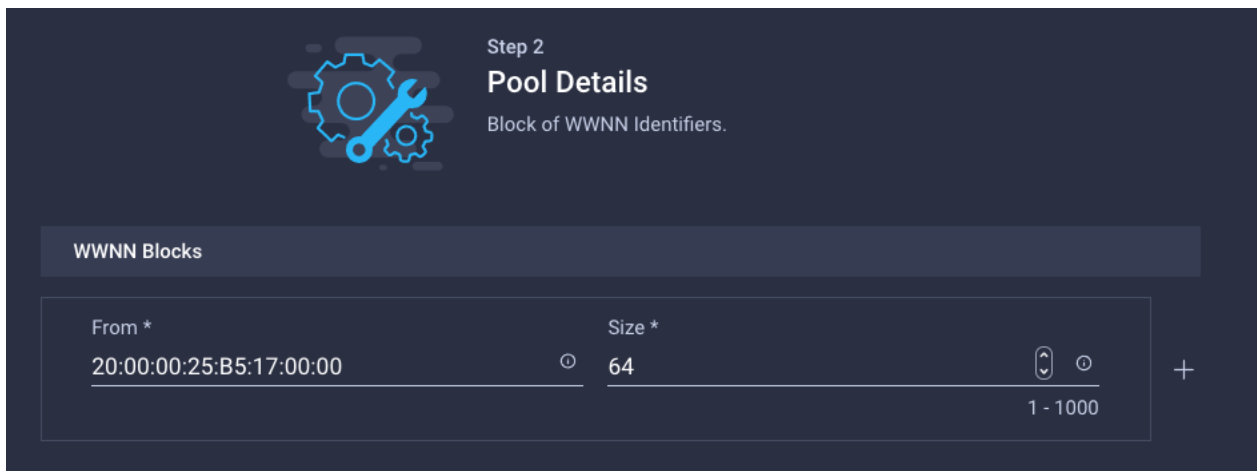
The WWNN address pools have not been defined yet therefore a new WWNN address pool has to be defined.

**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, AA17) and provide a name for the policy (for example, AA17-WWNN-Pool).

**Step 3.** Click **Next**.

**Step 4.** Provide the starting WWNN block address and the size of the pool.



**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 13. 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 14. Create the WWPN Pool for SAN A

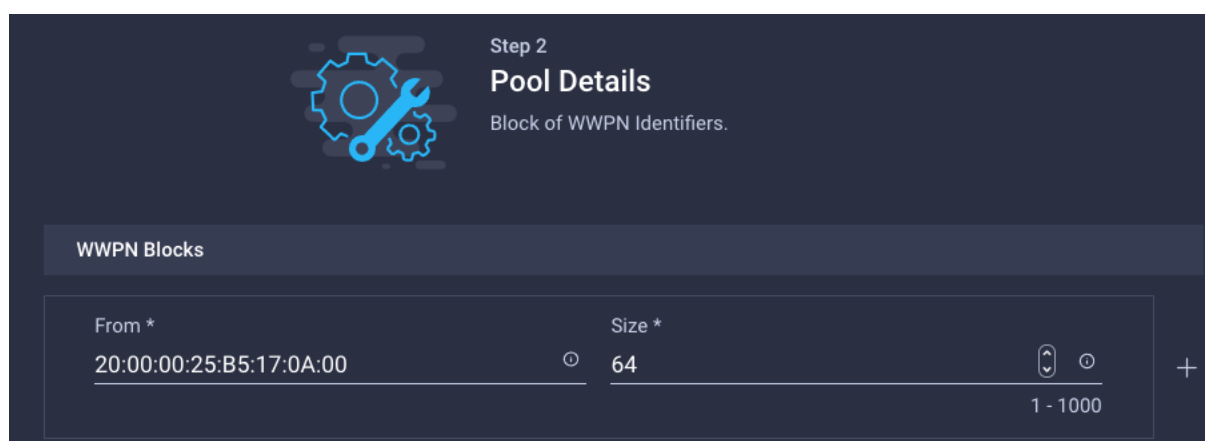
The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric A will be defined. This pool will also be used for the NVMe-o-FC vHBAs if the vHBAs are defined.

**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, AA17) and provide a name for the policy (for example, AA17-WWPN-Pool-A).

**Step 3.** Provide the starting WWPN block address for SAN A and the size.

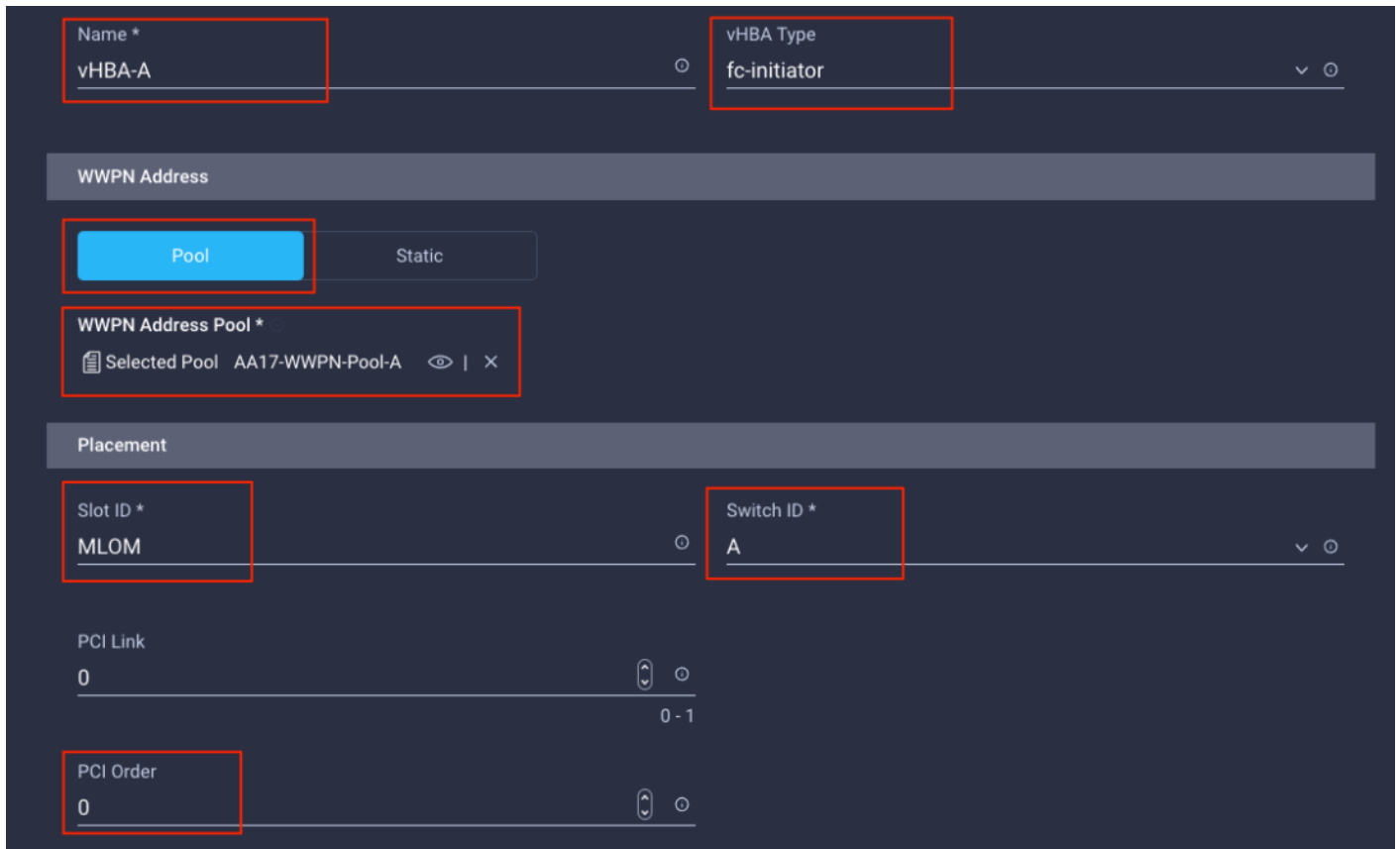
**Note:** As a best practice, in FlexPod some additional information is always coded into the WWPN address pool for troubleshooting. For example, in the address 20:00:00:25:B5:17:0A:00, 17 is the rack ID and 0A signifies SAN A.



**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](#).





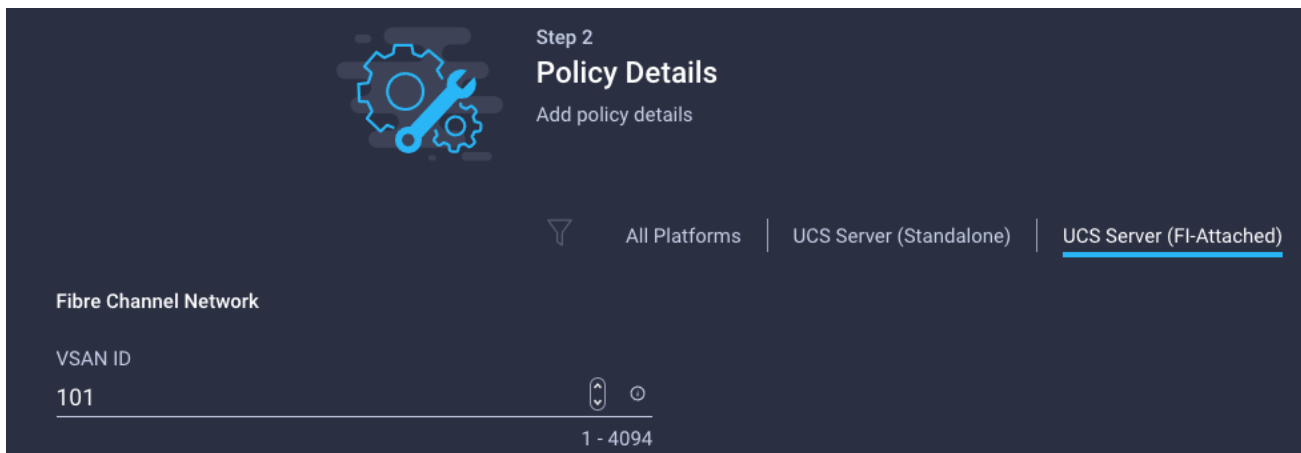
The screenshot shows a configuration form for a vHBA. The fields are as follows:

- Name \***: vHBA-A
- vHBA Type**: fc-initiator
- WWPN Address**: Pool (selected), Static
- WWPN Address Pool \***: Selected Pool AA17-WWPN-Pool-A
- Placement**:
  - Slot ID \***: MLOM
  - Switch ID \***: A
  - PCI Link**: 0 (range 0-1)
  - PCI Order**: 0

### Procedure 15. 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, AA17) and provide a name for the policy (for example, AA17-SAN-A-Network).
- Step 3.** For the scope, select **UCS Server (FI-Attached)**.
- Step 4.** Under VSAN ID, provide the VSAN information (for example, 101).



**Step 5.** Click **Create** to finish creating the Fibre Channel network policy.

### Procedure 16. Create Fibre Channel QoS Policy

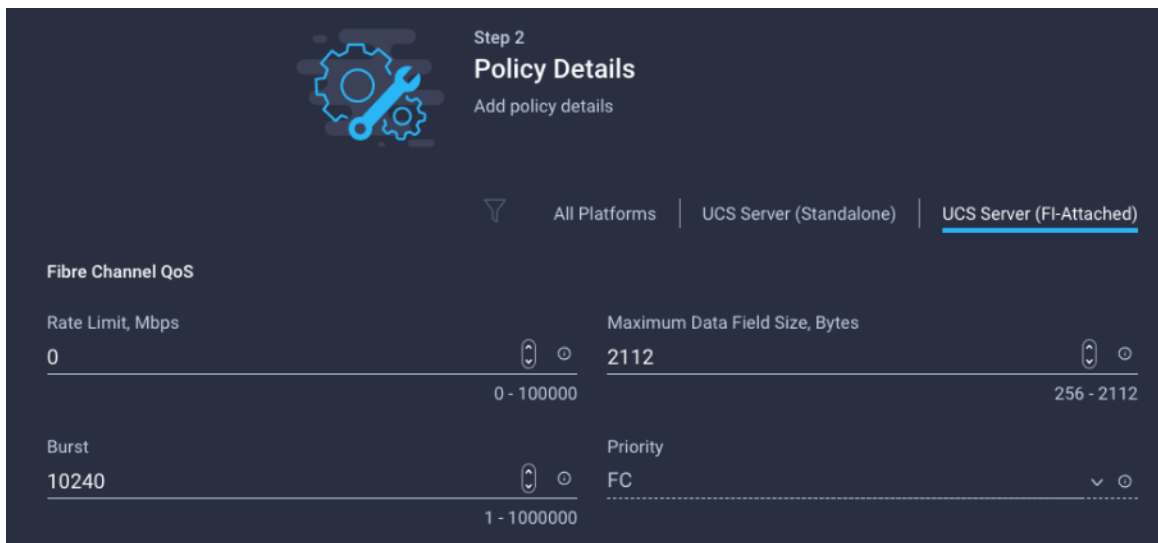
The Fibre Channel QoS policy assigns a system class to the outgoing traffic for a vHBA. This system class determines the quality of service for the outgoing traffic. The Fibre Channel QoS policy used in this deployment uses default values and will be shared by all vHBAs.

**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, AA17) and provide a name for the policy (for example, AA17-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.



**Step 5.** Click **Create** to finish creating the Fibre Channel QoS policy.

### Procedure 17. 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, AA17) and provide a name for the policy (for example, AA17-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.

The screenshot displays the 'Policy Details' configuration page for a Fibre Channel adapter policy. The page is titled 'Step 2 Policy Details' and includes a sub-header 'Add policy details'. A navigation bar at the top shows three tabs: 'All Platforms', 'UCS Server (Standalone)', and 'UCS Server (FI-Attached)', with the latter being the active tab. The configuration is organized into sections: 'Error Recovery' and 'Error Detection'. Under 'Error Recovery', there is a toggle for 'FCP Error Recovery' which is currently turned off. Below this are four adjustable settings: 'Port Down Timeout, ms' (set to 10000, range 0-240000), 'Link Down Timeout, ms' (set to 30000, range 0-240000), 'I/O Retry Timeout, Seconds' (set to 5, range 1-59), and 'Port Down IO Retry, ms' (set to 30, range 0-255). Under 'Error Detection', there is one adjustable setting: 'Error Detection Timeout' (set to 2000, range 1000-100000). Each setting is represented by a horizontal slider with up and down arrow icons and a reset icon.

**Step 5.** Click **Create** to finish creating the Fibre Channel adapter policy.

**Step 6.** Click **Add** to create vHBA-A.

#### Procedure 18. 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 19. Create the WWPN Pool for SAN B

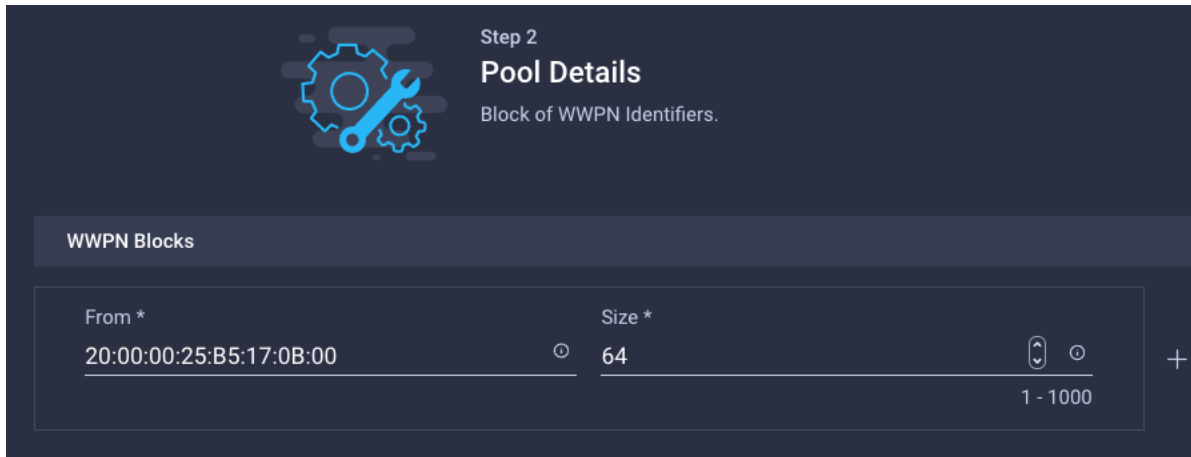
The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric B will be defined. This pool will also be used for the NVMe-o-FC vHBAs if the vHBAs are defined.

**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, AA17) and provide a name for the policy (for example, AA17-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.



The screenshot shows a dark-themed interface for configuring WWPN blocks. At the top left is a gear and wrench icon. The title is 'Step 2 Pool Details' with the subtitle 'Block of WWPN Identifiers.' Below this is a section titled 'WWPN Blocks'. It contains a table with two columns: 'From \*' and 'Size \*'. The 'From \*' column has the value '20:00:00:25:B5:17:0B:00' and a small circular icon to its right. The 'Size \*' column has the value '64' and a small circular icon to its right. To the right of the 'Size \*' column is a vertical slider control with a plus sign to its right. Below the slider, the range '1 - 1000' is displayed.

**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](#).

The screenshot shows a configuration form for a vHBA. The fields are as follows:

- Name \***: vHBA-B
- vHBA Type**: fc-initiator
- WWPN Address**: Pool (selected), Static
- WWPN Address Pool \***: Selected Pool AA17-WWPN-Pool-B
- Placement**:
  - Slot ID \***: MLOM
  - Switch ID \***: B
  - PCI Link**: 0 (range 0-1)
  - PCI Order**: 1

## Procedure 20. Create Fibre Channel Network Policy for SAN B

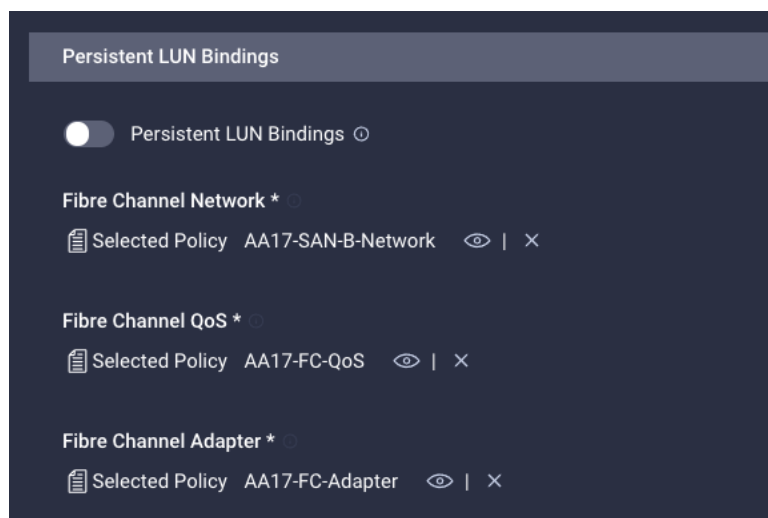
**Note:** In this deployment, VSAN 102 will be used for vHBA-B.

- 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, AA17) and provide a name for the policy (for example, AA17-SAN-B-Network).
- Step 3.** For the scope, select UCS Server (FI-Attached).
- Step 4.** Under VSAN ID, provide the VSAN information (for example, 102).

The screenshot shows the 'Policy Details' configuration page. The details are as follows:

- Step 2**: Policy Details
- Add policy details**
- Filters**: All Platforms | UCS Server (Standalone) | UCS Server (FI-Attached)
- Fibre Channel Network**
- VSAN ID**: 102 (range 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 AA17-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 AA17-FC-Adapter.
- Step 10.** Verify all the vHBA policies are mapped.



- 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 Link	PCI Order	
<input type="checkbox"/>	vHBA-A	MLOM	A	0	0	...
<input type="checkbox"/>	vHBA-B	MLOM	B	0	1	...

**Note:** If the customers don't need the NVMe-o-FC connectivity, skip the following sections for creating NVMe vHBAs.

**Procedure 21.** Configure vHBA-NVMe-A and vHBA-NVMe-B

To configure (optional) NVMe-o-FC, two vHBAs, one for each fabric, needs to be added to the server profile template. These vHBAs are in addition to the FC boot from SAN vHBAs, vHBA-A and vHBA-b.

**Table 22. vHBA placement for NVMe-o-FC**

vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-NVMe-A	MLOM	A	6
vHBA-NVMe-B	MLOM	B	7

**Procedure 22. Configure vHBA-NVMe-A**

- Step 1.** Click **Add vHBA**.
- Step 2.** For vHBA Type, select **fc-nvme-initiator** from the drop-down list.
- Step 3.** Click **Select Pool** under WWPN Address Pool and then select the previously created pool AA17-WWPN-Pool-A.
- Step 4.** Provide the Name (for example, vHBA-NVMe-A), Switch ID (for example, A) and PCI Order from [Table 22](#).

The screenshot shows a configuration form for a vHBA. The fields are as follows:

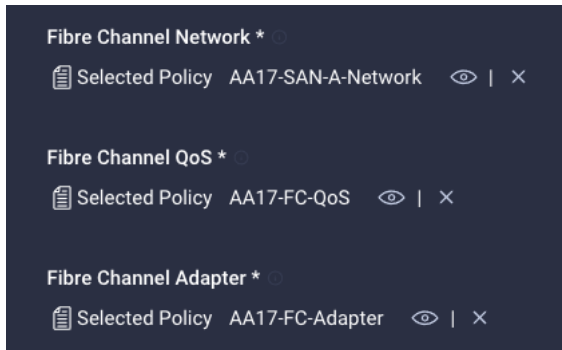
- Name \***: vHBA-NVMe-A
- vHBA Type**: fc-nvme-initiator
- WWPN Address**: Pool (selected), Static
- WWPN Address Pool \***: Selected Pool AA17-WWPN-Pool-A
- Placement**:
  - Slot ID \***: MLOM
  - Switch ID \***: A
- PCI Link**: 0 (range 0-1)
- PCI Order**: 6

- Step 5.** Click **Select Policy** under Fibre Channel Network and then select the previously created policy for SAN A, AA17-SAN-A-Network.

**Step 6.** Click **Select Policy** under Fibre Channel QoS and then select the previously created QoS policy AA17-FC-QoS.

**Step 7.** Click **Select Policy** under Fibre Channel Adapter and then select the previously created Adapter policy AA17-FC-Adapter.

**Step 8.** Verify all the vHBA policies are mapped.



### Procedure 23. Configure vHBA-NVMe-B

**Step 1.** Click **Add vHBA**.

**Step 2.** For vHBA Type, select **fc-nvme-initiator** from the drop-down list.

**Step 3.** Click **Select Pool** under WWPN Address Pool and then select the previously created pool AA17-WWPN-Pool-B.

**Step 4.** Provide the Name (for example, vHBA-NVMe-B), Switch ID (for example, B) and PCI Order from [Table 22](#).



The screenshot shows a configuration form for a vHBA. The following fields are highlighted with red boxes:

- Name \***: vHBA-NVMe-B
- vHBA Type**: fc-nvme-initiator
- WWPN Address**: Pool (selected), Static
- WWPN Address Pool \***: Selected Pool AA17-WWPN-Pool-B
- Slot ID \***: MLOM
- Switch ID \***: B
- PCI Link**: 0
- PCI Order**: 7

**Step 5.** Click **Select Policy** under Fibre Channel Network and then select the previously created policy for SAN B, AA17-SAN-B-Network.

**Step 6.** Click **Select Policy** under Fibre Channel QoS and then select the previously created QoS policy AA17-FC-QoS.

**Step 7.** Click **Select Policy** under Fibre Channel Adapter and then select the previously created Adapter policy AA17-FC-Adapter.

**Step 8.** Verify all the vHBA policies are mapped correctly.

The screenshot shows three sections of policy selection:

- Fibre Channel Network \***: Selected Policy AA17-SAN-B-Network
- Fibre Channel QoS \***: Selected Policy AA17-FC-QoS
- Fibre Channel Adapter \***: Selected Policy AA17-FC-Adapter

**Step 9.** Verify all four vHBAs are added to the SAN connectivity policy.

<input type="checkbox"/>	Name	Slot ID	Switch ID	PCI Link	PCI Order	⚙️
<input type="checkbox"/>	vHBA-NVMe-A	MLOM	A	0	6	⋮
<input type="checkbox"/>	vHBA-B	MLOM	B	0	1	⋮
<input type="checkbox"/>	vHBA-A	MLOM	A	0	0	⋮
<input type="checkbox"/>	vHBA-NVMe-B	MLOM	B	0	7	⋮

**Step 10.** Click **Create** to create the SAN connectivity policy with NVMe-o-FC support.

#### Procedure 24. 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.



Step 6

## Summary

Verify details of the template and the policies, resolve errors and deploy.

### General

Template Name	FC-Boot-Template	Organization	AA17
Target Platform	UCS Server (FI-Attached)		

Description  
FC Boot


Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors/Warnings (0)
-----------------------	--------------------------	-----------------------	-----------------------	---------------------

BIOS	AA17-BIOS-Pol	
Boot Order	AA17-FC-BootOrder-Pol	
UUID	AA17-UUID-Pool	

Description  
FC Boot

Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors/Warnings (0)
-----------------------	--------------------------	-----------------------	-----------------------	---------------------

IMC Access	AA17-IMC-Access	
IPMI Over LAN	Enable-IPMIoLAN	
Local User	AA17-LocalUserPol	

Description				
FC Boot				
Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors/Warnings (0)
LAN Connectivity			AA17-FC-ESXi-LANConn-Manual	
SAN Connectivity			AA17-SanConn-Pol	
Adapter #MLOM (vNICs)	4	Adapter #MLOM (vHBAs)	2	

### Procedure 25. 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 X210c M6**. You can select one or more servers depending on the number of profiles to be deployed.

**Server Assignment**

Assign Now    Assign Server from a Resource Pool    Assign Later

🔍 Add Filter    🔄    14 items found    10 ▾

<input checked="" type="checkbox"/>	Name	User Label	Health	Model
<input checked="" type="checkbox"/>	vdi-tme-2-7		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-3		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-4		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-8		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-1-5		<span>Healthy</span>	UCSBX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-1		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-1-8		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-2		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-6		<span>Healthy</span>	UCSX-210C-M6
<input checked="" type="checkbox"/>	vdi-tme-2-5		<span>Healthy</span>	UCSX-210C-M6

**Note:** The server profile template and policies in this document apply to both Cisco UCS X210x M6 and Cisco UCS B200 M6 servers.

**Step 3.**            Click **Next**.

**Note:** Cisco Intersight will fill the default information for the number of servers selected.

**Step 2**  
**Details**  
Edit the description, tags, and auto-generated names of the profiles.

**General**

Organization \*  
X-Series

Target Platform  
UCS Server (FI-Attached)

Description  
VDI\_FC\_Boot

Set Tags

<= 1024

**Derive**

Profile Name Prefix  
vdi-FC-Boot\_DERIVED-

Start Index for Suffix  
1

> 0

1 Name \*  
vdi-FC-Boot\_DERIVED-1

**Step 4.** Adjust the Prefix and number if needed.

**Step 2**  
**Details**  
Edit the description, tags, and auto-generated names of the profiles.

**General**

Organization \*  
X-Series

Target Platform  
UCS Server (FI-Attached)

Description  
VDI\_FC\_Boot

Set Tags

<= 1024

**Derive**

Profile Name Prefix  
vdi-tme|

Start Index for Suffix  
1

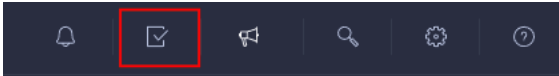
> 0

1 Name \*  
vdi-tme-1

**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.

The screenshot shows the 'CONFIGURE > Profiles' page. The 'UCS Server Profiles' tab is selected and highlighted with a red box. Below the tabs, there is a filter bar for 'All UCS Server Profiles' and a table of profiles.

	Name	Status	Target Platform	UCS Server Template
<input type="checkbox"/>	vdi-09	OK	UCS Server (FI-Attached)	vdi-SvcPrfl
<input type="checkbox"/>	vdi-08	OK	UCS Server (FI-Attached)	vdi-SvcPrfl
<input type="checkbox"/>	vdi-07	OK	UCS Server (FI-Attached)	vdi-SvcPrfl
<input type="checkbox"/>	vdi-06	OK	UCS Server (FI-Attached)	vdi-SvcPrfl
<input type="checkbox"/>	vdi-05	OK	UCS Server (FI-Attached)	vdi-SvcPrfl
<input type="checkbox"/>	vdi-04	OK	UCS Server (FI-Attached)	vdi-SvcPrfl
<input type="checkbox"/>	vdi-03	OK	UCS Server (FI-Attached)	vdi-SvcPrfl

## SAN Switch Configuration

This subject explains how to configure the Cisco MDS 9000s for use in a FlexPod environment.

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

**Note:** If you're directly connecting storage to the Cisco UCS fabric interconnects, skip this section.

### Physical Connectivity

Follow the physical connectivity guidelines for FlexPod as explained here: [FlexPod Cabling](#).

### FlexPod Cisco MDS Base

This section has the following procedures:

- [Configure Cisco MDS 9132T A Switch](#)
- [Configure Cisco MDS 9132T B Switch](#)

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod environment. This procedure assumes you are using the Cisco MDS 9132T with NX-OS 8.4(1a).

### 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. 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. Review the configuration:**

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

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

## FlexPod Cisco MDS Switch Configuration

This subject has the following procedures:

- [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. 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 2. 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, please see the [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 3. Configure Individual Ports for Cisco MDS 9132T A

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

```

interface fc1/9
switchport description <st-clustername>-1:2a
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/10
switchport description <st-clustername>-2:2a
switchport speed 3 2000
switchport trunk mode off
no shutdown
exit

interface fc1/5
switchport description <ucs-clustername>-a:1/1
channel-group 15
no shutdown
exit

interface fc1/6
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 4. Configure Individual Ports for Cisco MDS 9132T B

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

```
interface fc1/9
```

```
switchport description <st-clustername>-1:2b
switchport speed 32000
switchport trunk mode off
no shutdown
exit
```

```
interface fc1/10
switchport description <st-clustername>-2:2b
switchport speed 32000
switchport trunk mode off
no shutdown
exit
```

```
interface fc1/5
switchport description <ucs-clustername>-b:1/1
channel-group 15
no shutdown
exit
```

```
interface fc1/6
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 5.** 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 6. 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 UCS Manager and disable and then enable the FC port-channel interfaces to get the port-channels to come up.

## Procedure 7. 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 pwnn <fcp-lif-01a-wwpn>
device-alias name Infra-SVM-fcp-lif-02a pwnn <fcp-lif-02a-wwpn>
device-alias name VM-Host-Infra-01-A pwnn <vm-host-infra-01-wwpna>
device-alias name VM-Host-Infra-02-A pwnn <vm-host-infra-02-wwpna>
device-alias name VM-Host-Infra-03-A pwnn <vm-host-infra-03-wwpna>
device-alias commit
```

## Procedure 8. 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 pwnn <fcp-lif-01b-wwpn>
device-alias name Infra-SVM-fcp-lif-02b pwnn <fcp-lif-02b-wwpn>
device-alias name VM-Host-Infra-01-B pwnn <vm-host-infra-01-wwpnb>
device-alias name VM-Host-Infra-02-B pwnn <vm-host-infra-02-wwpnb>
device-alias name VM-Host-Infra-03-B pwnn <vm-host-infra-03-wwpnb>
device-alias commit
```

## Procedure 9. 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 10. 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 is organized into the following subjects:

- [ONTAP Boot Storage Setup](#)
- [Install VMware ESXi 7.0](#)
- [VMware vCenter 7.0](#)
- [Build the Virtual Machines and Environment](#)
- [Prepare the Master Targets](#)
- [Install and Configure Citrix Virtual Apps & Desktops and RDS](#)
- [Install and Configure Citrix Desktop Delivery Controller, Citrix Licensing, and StoreFront](#)
- [FSLogix for Citrix Virtual Apps & Desktops Profile Management](#)

### ONTAP Boot Storage Setup

This subject contains the following procedures:

- [Create igroups](#)
- [Map Boot LUNs to igroups](#)

#### Procedure 1. 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.** Use the values listed in [Table 6](#) and [Table 7](#) for the WWPN information.

**Step 3.** To view the three igroups just created, use the command `lun igroup show`:

```
lun igroup show -protocol fcp
```

#### Procedure 2. 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
```

## 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 UCS Manager](#)
- [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 UCS Manager 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 4.1.2a](#). You will need a user id and password on vmware.com to download this software.

**Note:** The Cisco Custom ISO for UCS 4.1.2a 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 UCS Manager

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 UCS Manager application.
- Step 2.** Click the **Launch UCS Manager** link to launch the HTML 5 UCS Manager 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 UCS Manager, 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.** Choose **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.

**Note:** 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 3.** After the installer is finished loading, press **Enter** to continue with the installation.

**Step 4.** Read and accept the end-user license agreement (EULA). Press **F11** to accept and continue.

**Note:** It may be necessary to map function keys as User Defined Macros under the Macros menu in the Cisco UCS KVM console.

**Step 5.** Select the LUN that was previously set up for the installation disk for ESXi and press **Enter** to continue with the installation.

**Step 6.** Select the appropriate keyboard layout and press **Enter**.

**Step 7.** Enter and confirm the root password and press **Enter**.

**Step 8.** The installer issues a warning that the selected disk will be repartitioned. Press **F11** to continue with the installation.

**Step 9.** After the installation is complete, press **Enter** to reboot the server.

**Note:** The ESXi installation image will be automatically unmapped in the KVM when Enter is pressed.

**Step 10.** In Cisco UCS Manager, 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**.

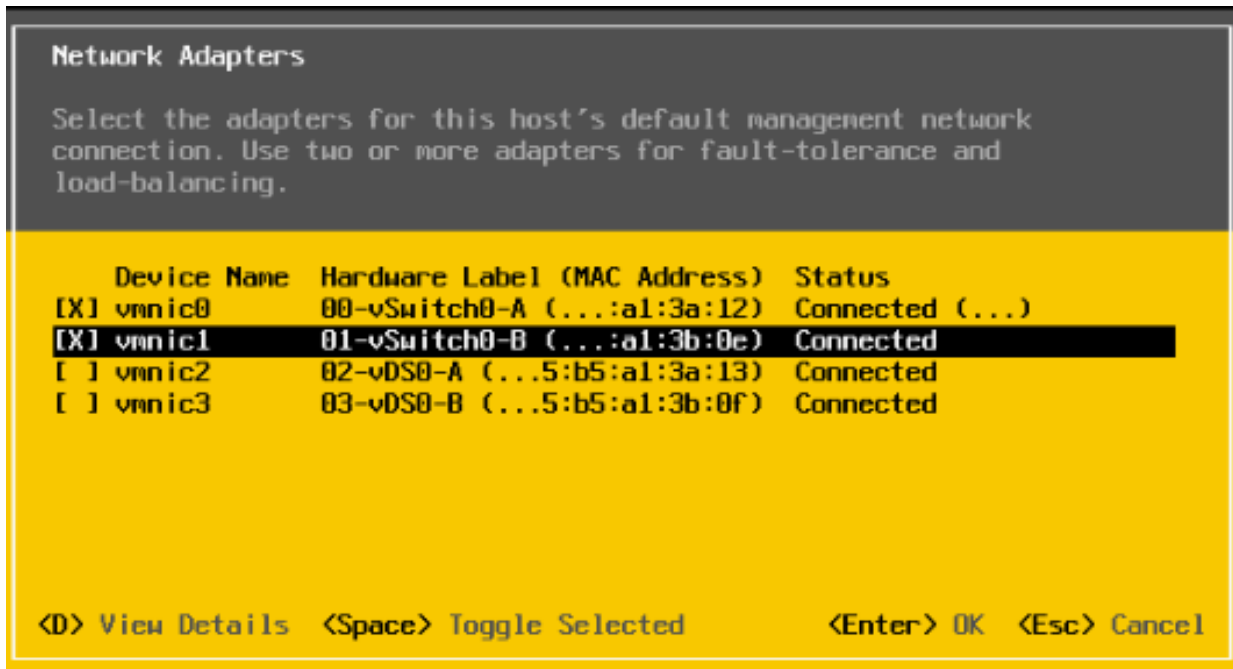
**Step 6.** Press **Esc** to exit the Troubleshooting Options menu.

**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**.



**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 KVM window, 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 re-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 re-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.
- 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.
  - To remove vmk1, type **esxcfg-vmknic -d "iScsiBootPG-A"**.
  - To re-add vmk1 with a random MAC address, type **esxcfg-vmknic -a -i <vmk1-ip> -n <vmk1-netmask> -m 9000 "iScsiBootPG-A"**.
  - Verify vmk1 has been re-added with a random MAC address by typing **esxcfg-vmknic -l**.
- Step 10.** Type **exit** to log out of the command line interface.
- Step 11.** 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)

## [NetApp NFS Plug-in 1.1.2-3 for VMware VAAI](#) (ucs-tool-esxi\_1.1.2-1OEM.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 7.0.0, Cisco UCS version 4.1(2a), and the latest patch NetApp ONTAP 9.7. 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.** Select **Edit** settings.
- Step 5.** Change the MTU to **9000**.
- Step 6.** Expand **NIC teaming**.
- Step 7.** In the Failover order section, select **vmnic1** and click **Mark active**.
- Step 8.** Verify that vmnic1 now has a status of Active.
- Step 9.** Click **Save**.
- Step 10.** Select **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.** 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, select **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, select **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.** Select 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:
- Click **Add VMkernel NIC**.
  - For New port group, enter **VMkernel-vMotion1**.
  - For Virtual switch, select **vSwitch0**.
  - 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. Select 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, select **vSwitch0**.
- m. Enter **<vmotion-vlan-id>** for the VLAN ID.
- n. Change the MTU to **9000**.
- o. Select **Static IPv4 settings** and expand IPv4 settings.
- p. Enter the ESXi host's third vMotion IP address and netmask.
- q. Select the **vMotion stack for TCP/IP stack**.
- r. Click **Create**.

**Step 34.** Select the **Virtual Switches** tab, then **vSwitch0**. The properties for vSwitch0 VMkernel NICs should be similar to the following example:



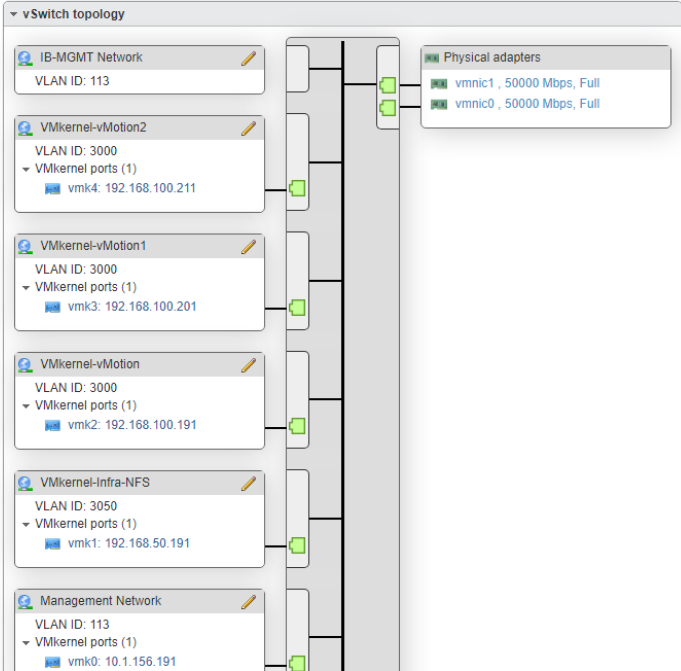
**vSwitch0**  
 Type: Standard vSwitch  
 Port groups: 6  
 Uplinks: 2

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



The diagram shows the vSwitch topology for vSwitch0. It includes several port groups: IB-MGMT Network (VLAN ID: 113), VMkernel-vMotion2 (VLAN ID: 3000), VMkernel-vMotion1 (VLAN ID: 3000), VMkernel-vMotion (VLAN ID: 3000), VMkernel-Infra-NFS (VLAN ID: 3050), and Management Network (VLAN ID: 113). Each port group has one or more VMkernel ports with their respective IP addresses. On the right, physical adapters vmnic1 and vmnic0 are shown, both configured for 50000 Mbps Full duplex.

**Step 35.** Select **Networking** and the **VMkernel NICs** tab to confirm configured virtual adapters. The adapters listed should be similar to the following example:

VMkernel NICs						
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	

## 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**.

**New datastore**

- 1 Select creation type
- 2 Provide NFS mount details
- 3 Ready to complete

### 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

vmware

Back Next Finish Cancel

- 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**.

New datastore - infra\_datastore

✓ 1 Select creation type  
**2 Provide NFS mount details**  
 3 Ready to complete

### 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	<input checked="" type="radio"/> NFS 3 <input type="radio"/> NFS 4

Back Next Finish Cancel

**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.

Datstores Adapters Devices Persistent Memory

New datastore Increase capacity Register a VM Datastore browser Refresh Actions

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, go to **System > Time & date**.

**Step 3.** Click **Edit NTP settings**.

- Step 4.** Click **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 select **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, go to **System > Swap**.
- Step 3.** Click **Edit settings**.
- Step 4.** Use the drop-down list to select **infra\_swap**. Leave all other settings unchanged.

Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Datastore	infra_swap
Local swap enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Host cache enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No

Save Cancel

**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**.

**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.

OK Cancel

---

## VMware vCenter 7.0

This subject contains the following procedures:

- [Build the VMware vCenter Server Appliance](#)
- [Adjust vCenter CPU Settings](#)
- [Set up VMware vCenter Server](#)

**Note:** These procedures provide detailed instructions for installing the VMware vCenter 7.0D Server Appliance in a FlexPod environment. After the procedures are completed, a VMware vCenter Server will be configured.

### Procedure 1. Build the VMware vCenter Server Appliance

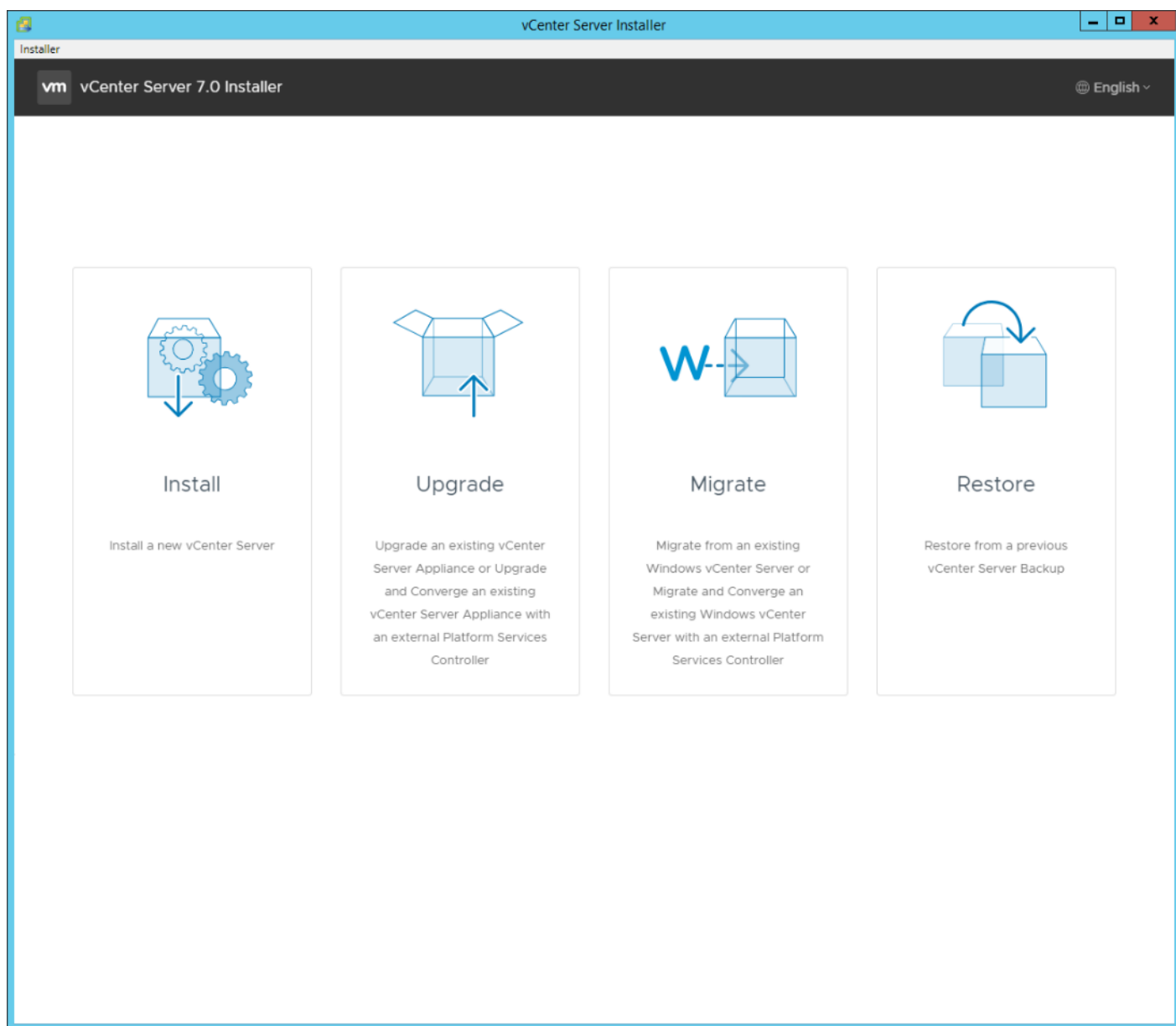
**Note:** The VCSA deployment consists of 2 stages: install and configure.

**Step 1.** Locate and copy the VMware-VCSA-all-7.0.0-16749653.iso file to the desktop of the management workstation. This ISO is for the VMware vSphere 7.0 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.



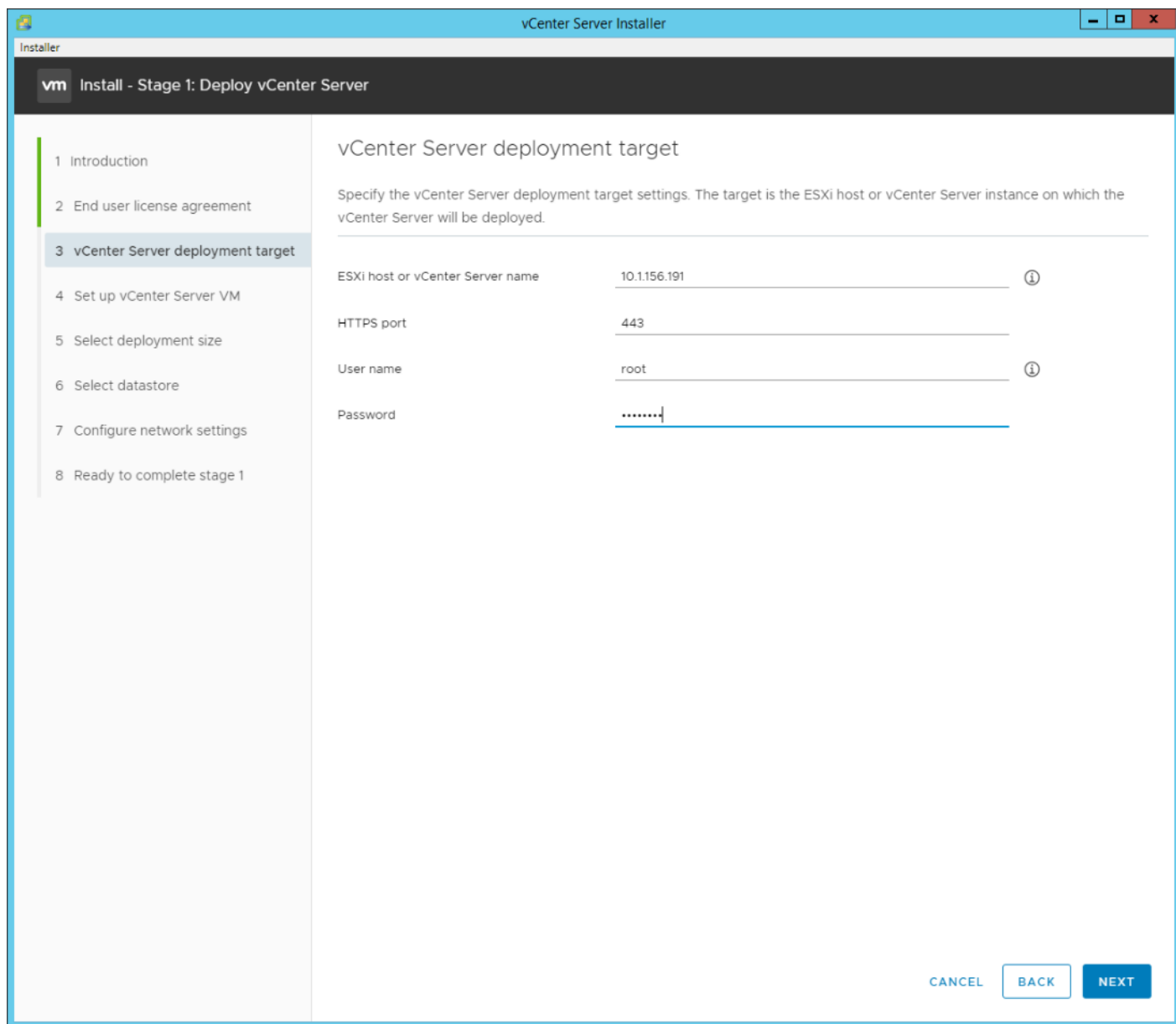
**Step 4.** Click **Install** to start the vCenter Server Appliance deployment wizard.

**Step 5.** Click **NEXT** in the Introduction section.

**Step 6.** Read and accept the license agreement and click **NEXT**.

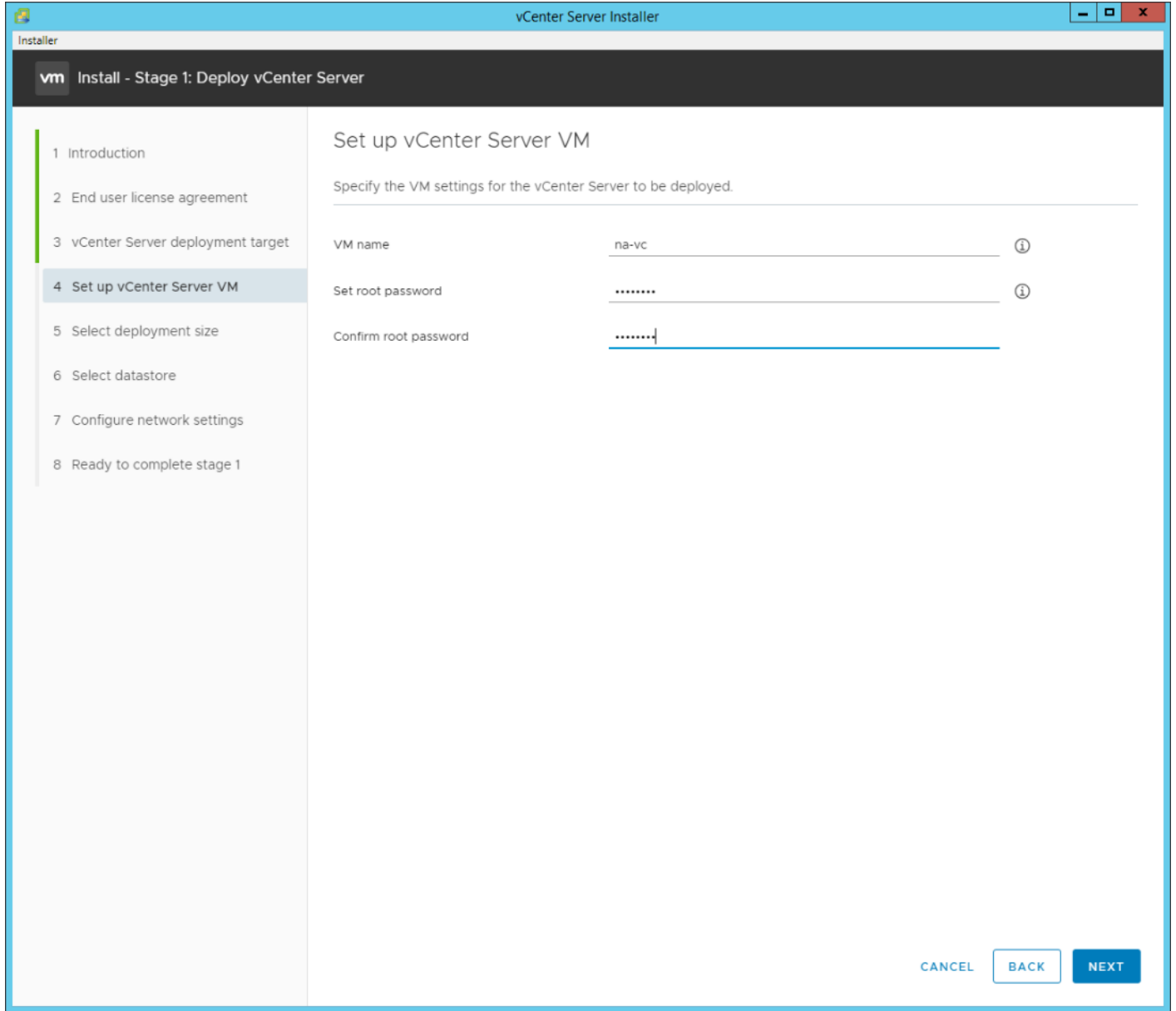
**Step 7.** In the “vCenter Server deployment target” window, enter the host name or IP address of the first ESXi host, User name (root) and Password. Click **NEXT**.



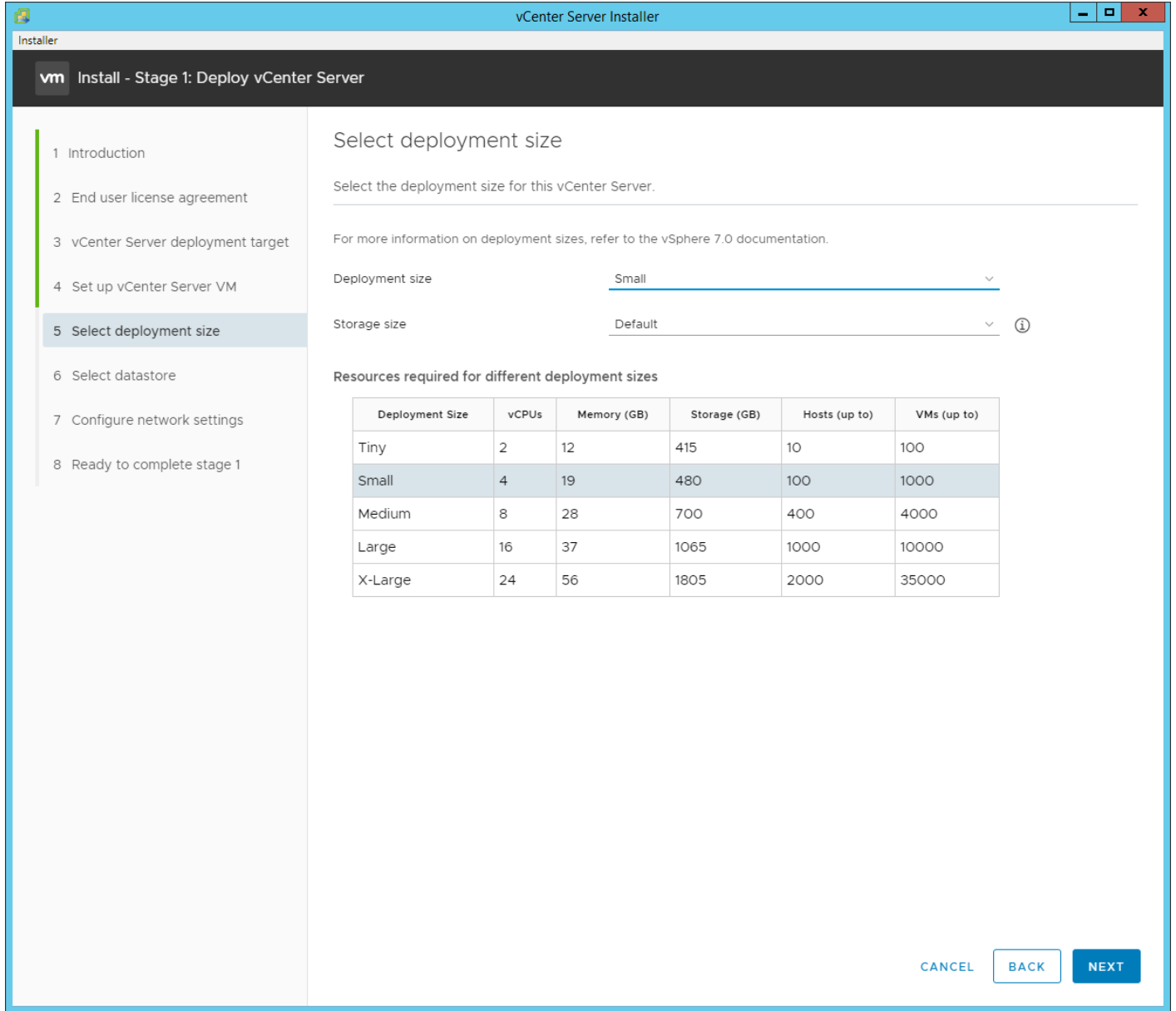


**Step 8.** Click **YES** to accept the certificate.

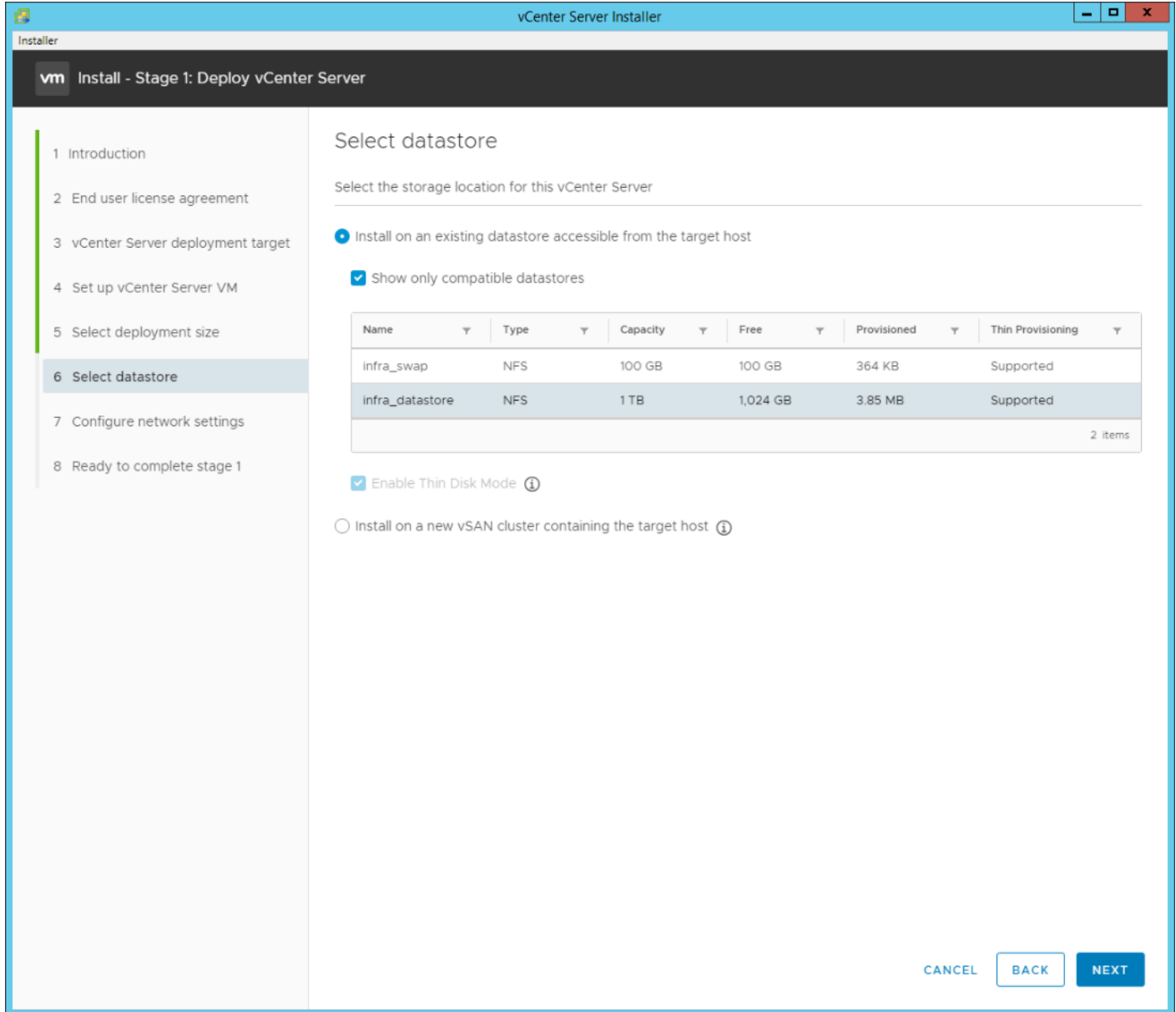
**Step 9.** Enter the Appliance VM name and password details in the “Set up vCenter Server VM” section. Click **NEXT**.



**Step 10.** In the “Select deployment size” section, select the Deployment size and Storage size. For example, choose “Small” and “Default”. Click **NEXT**.



**Step 11.** Select **infra\_datastore** for storage. Click **NEXT**.

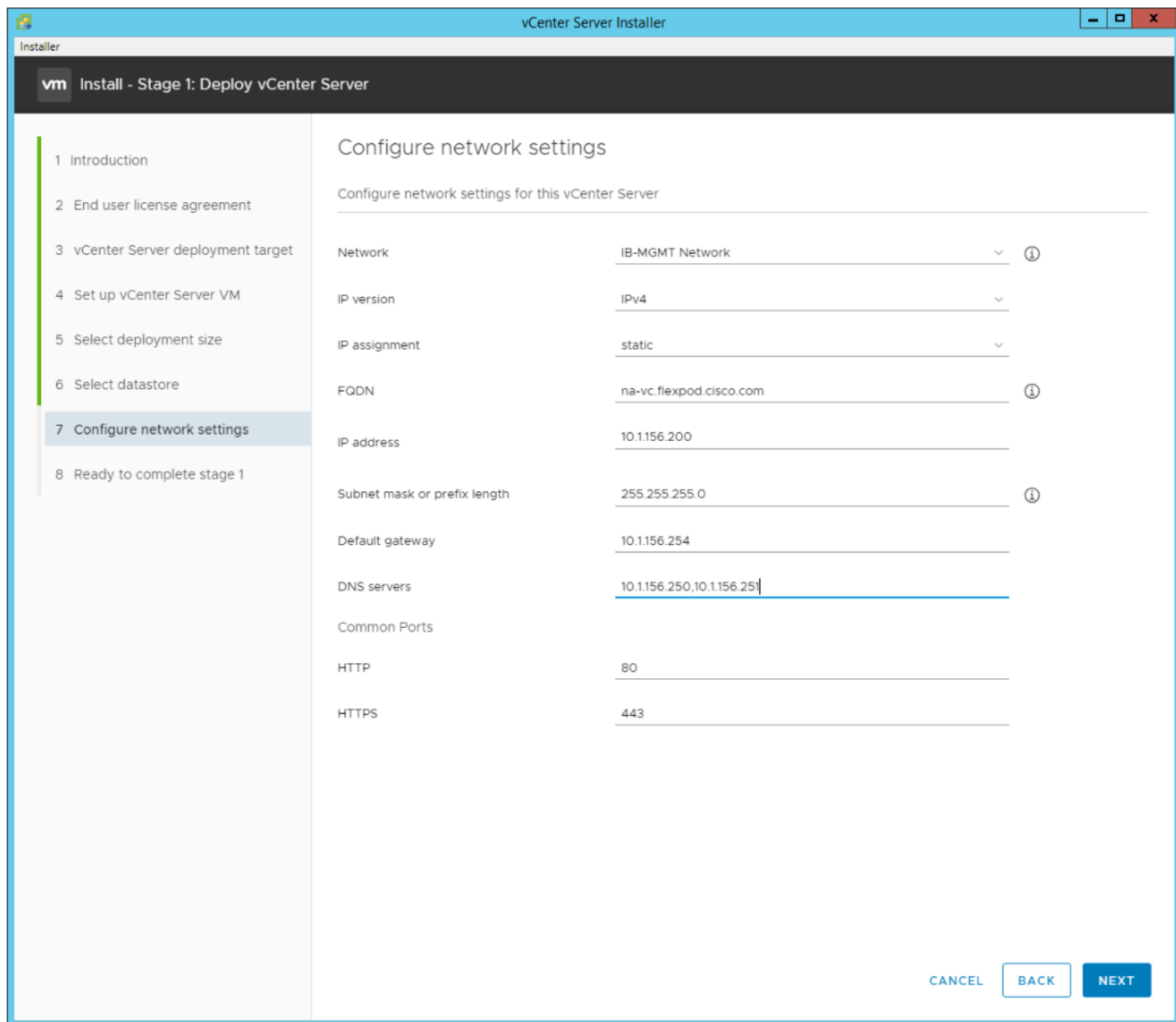


**Step 12.** In the “Network Settings” section, configure the below settings:

- a. Select 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.

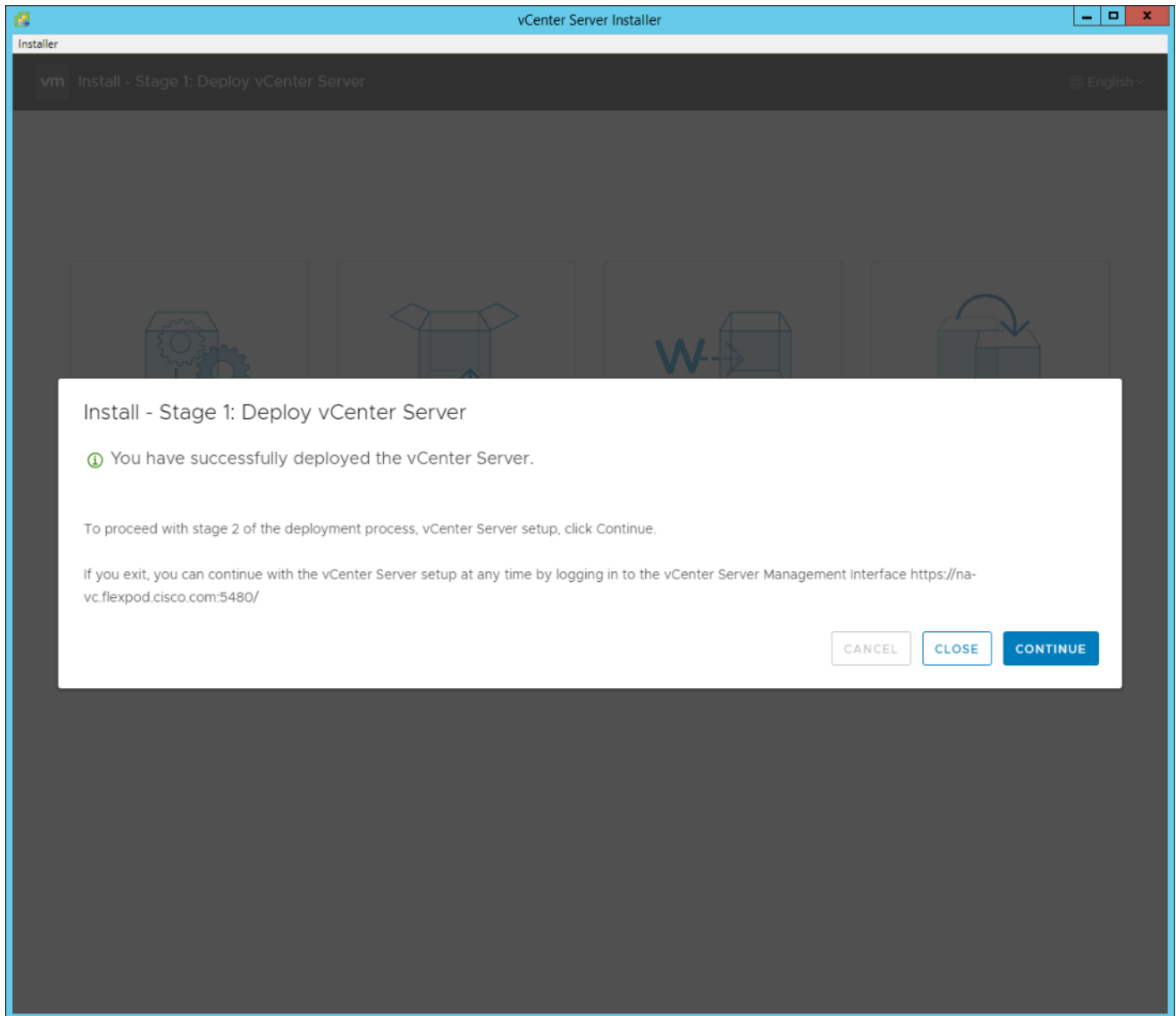
- b. IP version: IPV4
- c. IP assignment: static
- d. FQDN: <vcenter-fqdn>
- e. IP address: <vcenter-ip>
- f. Subnet mask or prefix length: <vcenter-subnet-mask>
- g. Default gateway: <vcenter-gateway>
- h. DNS Servers: <dns-server1>,<dns-server2>



**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.

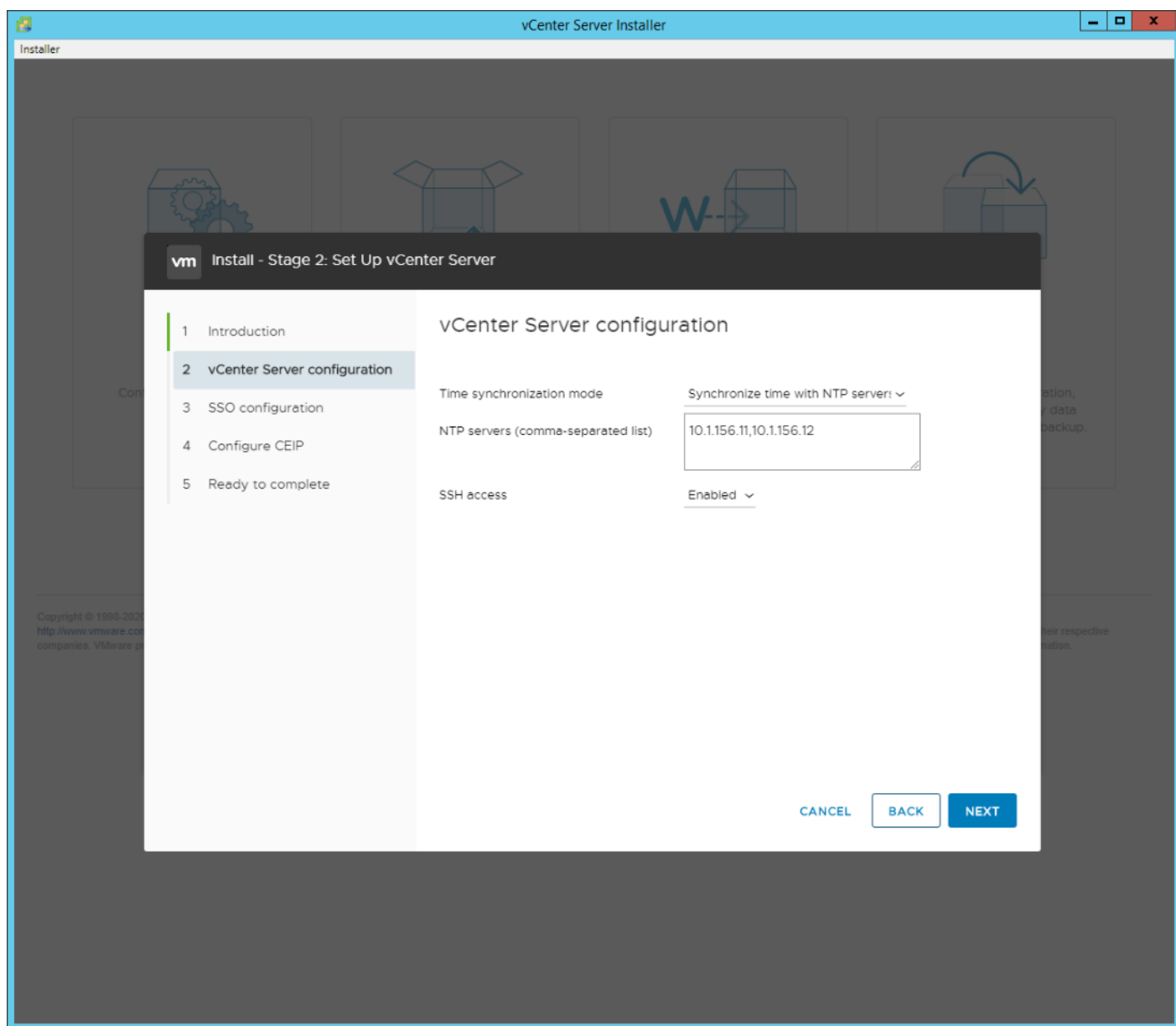


**Step 15.** Click **CONTINUE** to proceed with stage 2 configuration.

**Step 16.** Click **NEXT**.

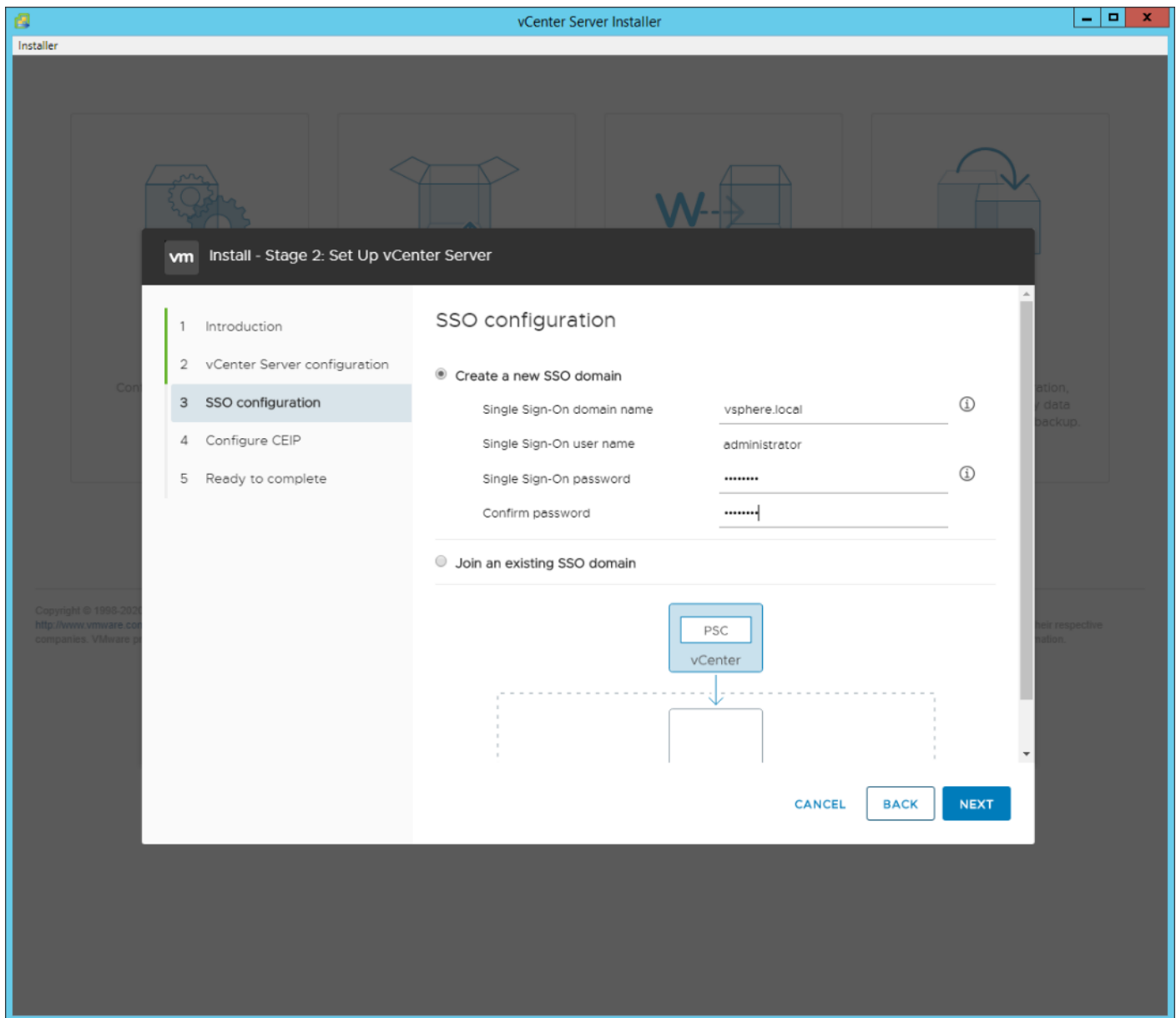
**Step 17.** In the vCenter Server configuration window, configure these settings:

- a. Time Synchronization Mode: Synchronize time with NTP servers.
- b. NTP Servers: <nexus-a-ntp-ip>,<nexus-b-ntp-ip>
- c. SSH access: Enabled.



**Step 18.** Click **NEXT**.

**Step 19.** Complete the SSO configuration as shown below or according to your organization's security policies:



**Step 20.** Click **NEXT**.

**Step 21.** Decide whether to join VMware's Customer Experience Improvement Program (CEIP).

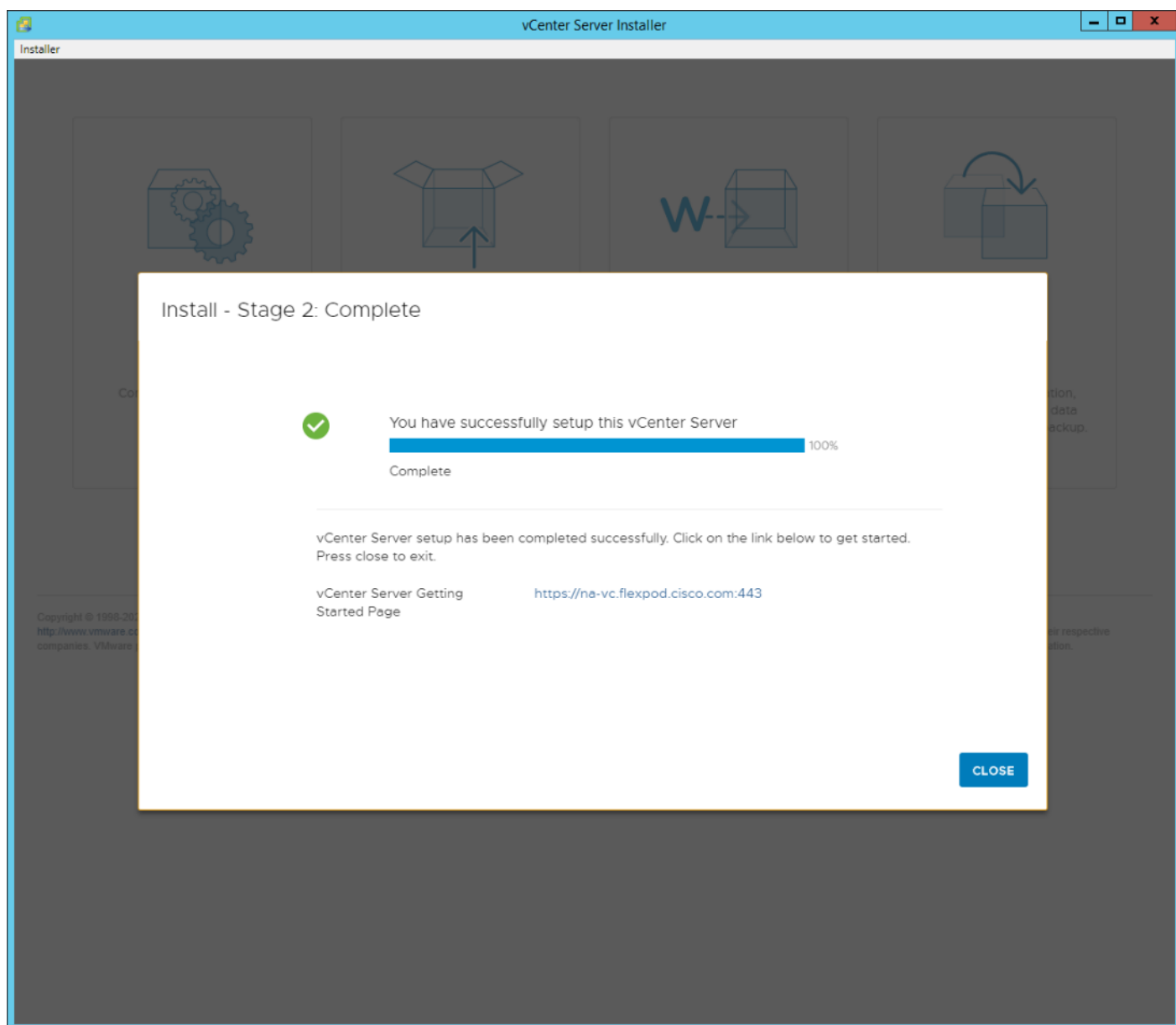
**Step 22.** Click **NEXT**.

**Step 23.** Review the configuration and click **FINISH**.

**Step 24.** Click **OK**.

**Note:** vCenter Server setup will take a few minutes to complete.





**Step 25.** Click **CLOSE**. Eject or unmount the VCSA installer ISO.

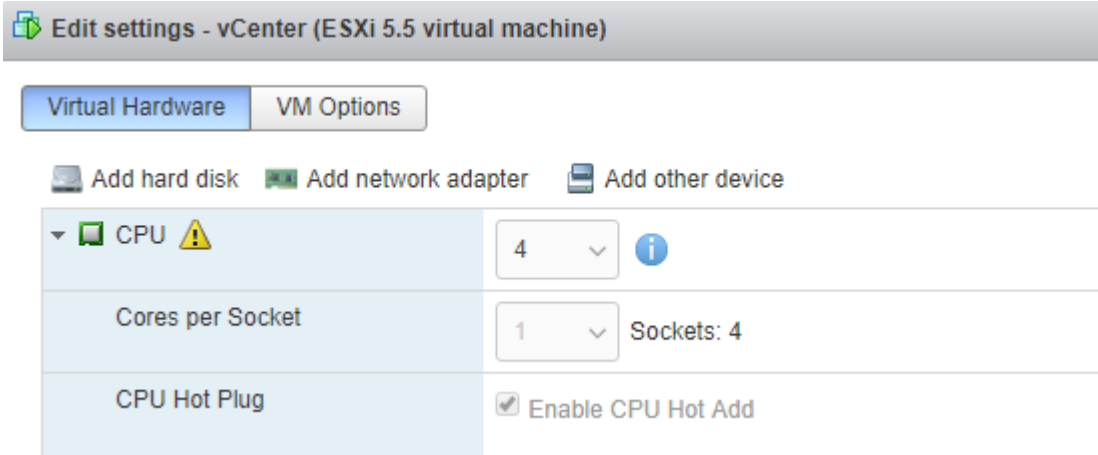
### **Procedure 2.** Adjust vCenter CPU Settings

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**.

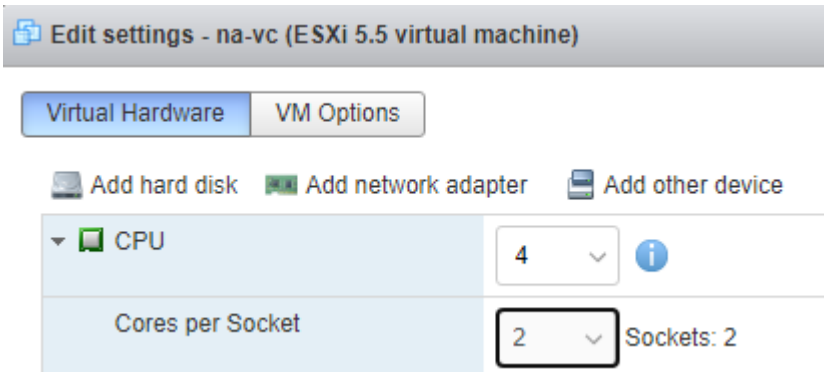
**Step 2.** Enter **root** for the user name.

- Step 3.** Enter the **root** password.
- Step 4.** Click **Login** to connect.
- Step 5.** Click **Virtual Machines**.
- Step 6.** Right-click the **vCenter VM** and click **Edit settings**.
- Step 7.** In the Edit settings window, expand CPU and check the value of Sockets.



**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 choose Guest OS > Shut down. Click Yes on the confirmation.
  - b. Once vCenter is shut down, right-click the vCenter VM and choose 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 go to **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.** Click **Time**.

**Step 4.** Click **EDIT** to the right of Time zone.

**Step 5.** Select the appropriate Time zone and click **SAVE**.

**Step 6.** 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 7.0.0.10700 was installed.

**Step 10.** Go to **root > Logout** to logout of the Appliance Management interface.

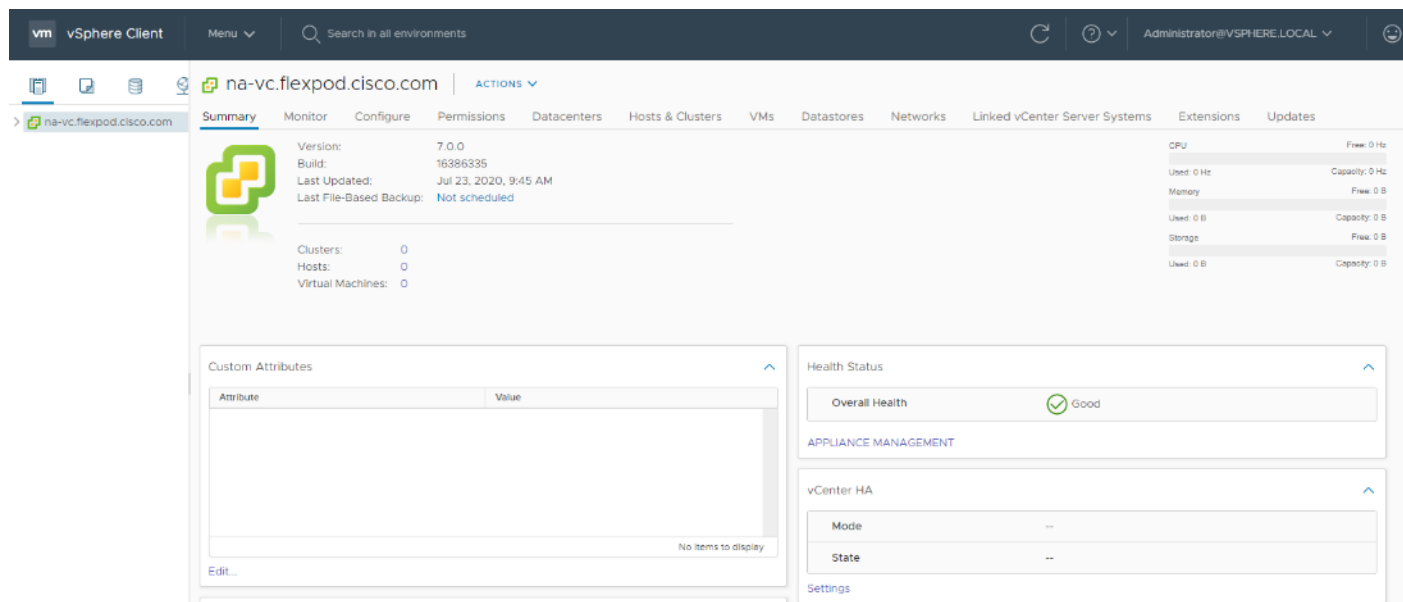
**Step 11.** Using a web browser, navigate to **https://<vcenter-fqdn>** You will need to navigate security screens.

**Note:** With VMware vCenter 7.0, 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](mailto:administrator@vsphere.local)) and password created during the vCenter installation. Dismiss the Licensing warning at this time.



**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

CANCEL

OK

- Step 16.** Click **OK**.
- Step 17.** Expand the **vCenter**.
- Step 18.** Right-click the datacenter **FlexPod-DC**. 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	
vSphere HA	
vSAN	

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

CANCEL

OK

- Step 21.** Click **OK** to create the new cluster.
- Step 22.** Right-click **FlexPod-Management** and click **Settings**.
- Step 23.** Go to **Configuration > General** and click **EDIT**.
- Step 24.** Select **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.

CANCEL

OK

**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, select 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.

**Note:** The added ESXi host will have Warnings that the ESXi Shell and SSH have been enabled. These warnings can be suppressed.

**Step 30.** Right-click the added **ESXi host** and click **Settings**.

**Step 31.** In the center pane under Virtual Machines, click **Swap File location**.

**Step 32.** Click **EDIT**.

**Step 33.** Select 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

CANCEL

OK

**Step 34.** In the list under System, click **Time Configuration**.

**Step 35.** Click **EDIT**. Set the time and date to the correct local time and click **OK**.

**Step 36.** Click **EDIT**.

**Step 37.** 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	<input type="text" value="10.1.156.11,10.1.156.12"/>
Separate servers with commas, e.g. 10.31.21.2, fe00::2800	
NTP Service Status:	Stopped
	<input checked="" type="checkbox"/> Start NTP Service
NTP Service Startup Policy:	<input type="text" value="Start and stop with host"/>

**Step 38.** 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, choose EDIT POWER POLICY. Choose High performance and click OK.

**Step 39.** 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 40.** Click the **Paths** tab.

**Step 41.** Ensure that 4 paths appear, two of which should have the status Active (I/O).

Storage Devices

Refresh Attach Detach Rename... Turn On LED Turn Off LED Erase Partitions... Mark as HDD Disk Mark as Local Mark as Perennially Reserved

Name	LUN	Type	Capacity	Datastore	Operational St...	Hardware Accelerat...	Drive Ty...	Transport
Local ATA Disk (t10.ATA____Micron_5100_MTF...	0	disk	223.57 GB	Not Consu...	Attached	Not supported	Flash	Block Adapter
NETAPP Fibre Channel Disk (naa.600a09803831...	0	disk	32.00 GB	Not Consu...	Attached	Supported	Flash	Fibre Channel
Local ATA Disk (t10.ATA____Micron_5100_MTF...	0	disk	223.57 GB	Not Consu...	Attached	Not supported	Flash	Block Adapter

Copy All | 3 items

Properties **Paths** Partition Details

Enable Disable

Runtime Name	Status	Target	Name	Preferred
vmhba0:C0:T1:L0	Active (I/O)	20:00:d0:39:ea:16:6b:8b 20:01:d0:39:ea:16:6b:8b	vmhba0:C0:T1:L0	
vmhba1:C0:T2:L0	Active	20:00:d0:39:ea:16:6b:8b 20:04:d0:39:ea:16:6b:...	vmhba1:C0:T2:L0	
vmhba1:C0:T1:L0	Active (I/O)	20:00:d0:39:ea:16:6b:8b 20:02:d0:39:ea:16:6b:...	vmhba1:C0:T1:L0	
vmhba0:C0:T2:L0	Active	20:00:d0:39:ea:16:6b:8b 20:03:d0:39:ea:16:6b:...	vmhba0:C0:T2:L0	



## Build the Virtual Machines and Environment

### Software Infrastructure Configuration

This section details how to configure the software infrastructure components that comprise this solution. Install and configure the infrastructure virtual machines by following the process provided in [Table 23](#).

**Table 23. Test Infrastructure Virtual Machine Configuration**

Configuration	Citrix Virtual Apps & Desktops Controllers Virtual Machines	Citrix Provisioning Servers Virtual Machines
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2019
Virtual CPU amount	6	8
Memory amount	8 GB	16 GB
Network	VMXNET3 Infra-Mgmt	VMXNET3 VDI
Disk-1 (OS) size	40 GB	40 GB

Configuration	Microsoft Active Directory DCs	Configuration
Operating system	Microsoft Windows Server 2019	VCSA - SUSE Linux
Virtual CPU amount	2	16
Memory amount	4 GB	32 GB
Network	VMXNET3 Infra-Mgmt	VMXNET3 In-Band-Mgmt
Disk size	40 GB	

Configuration	Microsoft SQL Server Virtual Machine	Citrix StoreFront Controller Virtual Machine
Operating system	Microsoft Windows Server 2019 Microsoft SQL Server 2012 SP1	Microsoft Windows Server 2019

Configuration	Microsoft SQL Server Virtual Machine	Citrix StoreFront Controller Virtual Machine
Virtual CPU amount	6	4
Memory amount	24GB	8 GB
Network	VMXNET3 Infra-Mgmt	VMXNET3 Infra-Mgmt
Disk-1 (OS) size	40 GB	40 GB
Disk-2 size	100 GB SQL Databases\Logs	

## Prepare the Master Targets

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

To prepare the master VMs for the Hosted Virtual Desktops (HVDs) and Hosted Shared Desktops (HSDs), there are three major steps:

1. Installing the PVS Target Device x64 software
2. Installing the Virtual Delivery Agents (VDAs)
3. Installing application software.

The master target Hosted Virtual Desktop (HVD) and Hosted Shared Desktop (HSD) VMs were configured as listed in [Table 24](#).

**Table 24. VDI and RDS Configurations**

Configuration	HVD Virtual Machines	HSD Virtual Machines
Operating system	Microsoft Windows 10 64-bit	Microsoft Windows Server 2019
Virtual CPU amount	2	8
Memory amount	4 GB memory	32 GB memory
Network	VMXNET3 DV-VDI	VMXNET3 DV-VDI

Configuration	HVD Virtual Machines	HSD Virtual Machines
Citrix PVS vDisk size	24 GB (dynamic)	40 GB (dynamic)
Full Clone Disk Size	45 GB	
Citrix PVS write cache	6 GB	30 GB
Disk size		
Citrix PVS write cache	256 MB	1024 MB
RAM cache size		
Additional software used for testing	Microsoft Office 2016 Login VSI 4.1.40 (Knowledge Worker Workload)	Microsoft Office 2016 Login VSI 4.1.40 (Knowledge Worker Workload)

## Install and Configure Citrix Virtual Apps & Desktops and RDS

This subject contains the following procedure:

- [Install vCenter Server Self-Signed Certificate](#)

This section details the installation of the core components of the Citrix Virtual Apps & Desktops and RDS 7 LTSR system. This CVD installs two Citrix Virtual Apps & Desktops Delivery Controllers to support both hosted shared desktops (HSD), non-persistent hosted virtual desktops (HVD), and persistent hosted virtual desktops (HVD).

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

### 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 for the URL).

**Step 3.** Accept the security warnings.

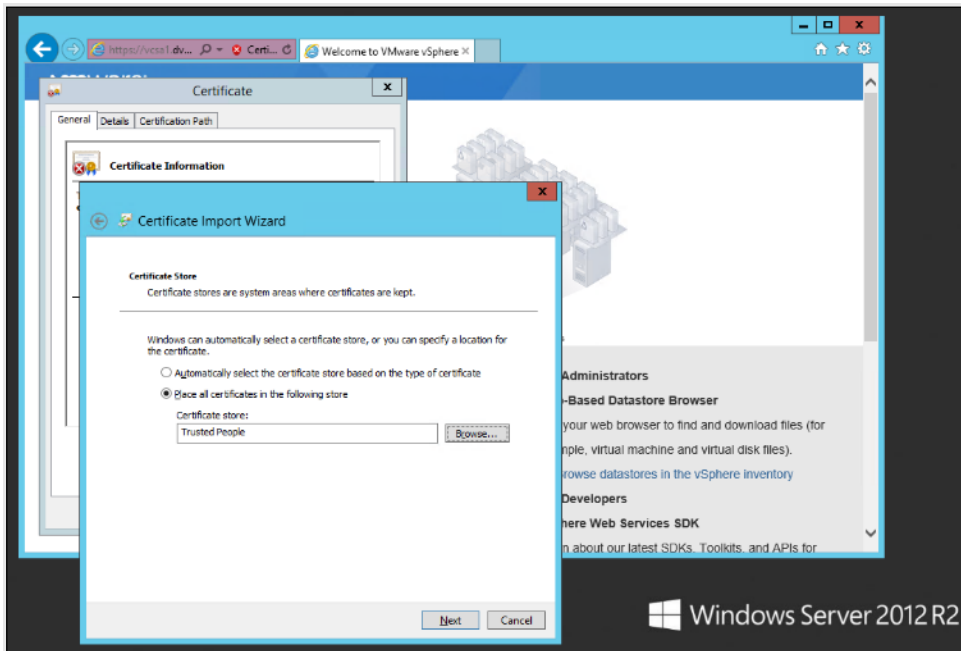
**Step 4.** Click the **Certificate Error** in the Security Status bar and select **View certificates**.

**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.** Select **Show physical stores**.

## Step 8. Select Trusted People.



**Step 9.** Click **Next** and then click **Finish**.

**Step 10.** Repeat steps 1 – 9 on all Delivery Controllers and Provisioning Servers.

## Install and Configure Citrix Desktop Delivery Controller, Citrix Licensing, and Store-Front

This subject contains the following procedures:

- [Install Citrix License Server](#)
- [Install Citrix Licenses](#)
- [Install Citrix Desktop Broker/Studio](#)
- [Configure the Citrix VDI Site](#)
- [Configure the Citrix VDI Site Administrators](#)
- [Configure Additional Citrix Desktop Controller](#)
- [Add the Second Delivery Controller to the Citrix Desktop Site](#)
- [Install and Configure StoreFront](#)
- [Additional StoreFront Configuration](#)
- [Install the Citrix Provisioning Services Target Device Software](#)
- [Create Citrix Provisioning Services vDisks](#)
- [Install Citrix Virtual Apps and Desktop Virtual Desktop Agents](#)
- [Provision Virtual Desktop Machines](#)

- [Provision Desktop Machines from Citrix Provisioning Services Console](#)
- [Citrix Machine Creation Services](#)
- [Create Delivery Groups](#)

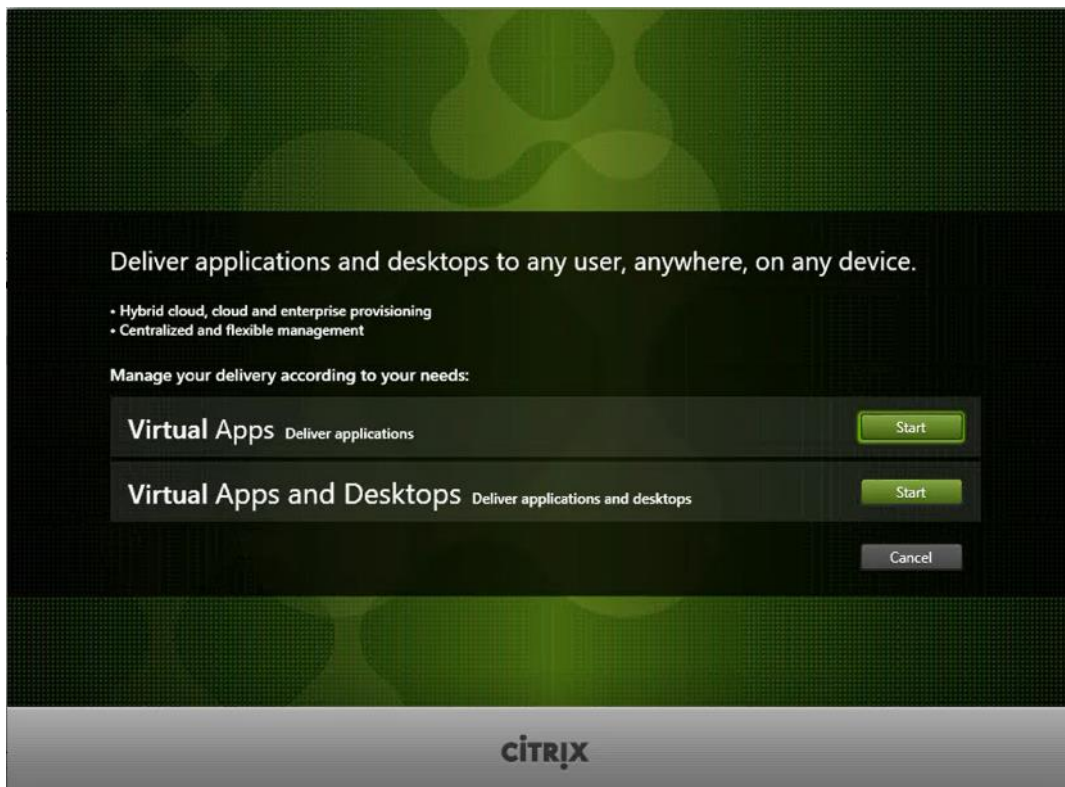
This section details the installation of the core components of the Citrix Virtual Apps and Desktops 7 LTSR system. This CVD provides the process to install two Desktop Delivery Controllers to support hosted shared desktops (HSD), non-persistent virtual desktops (VDI), and persistent virtual desktops (VDI).

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

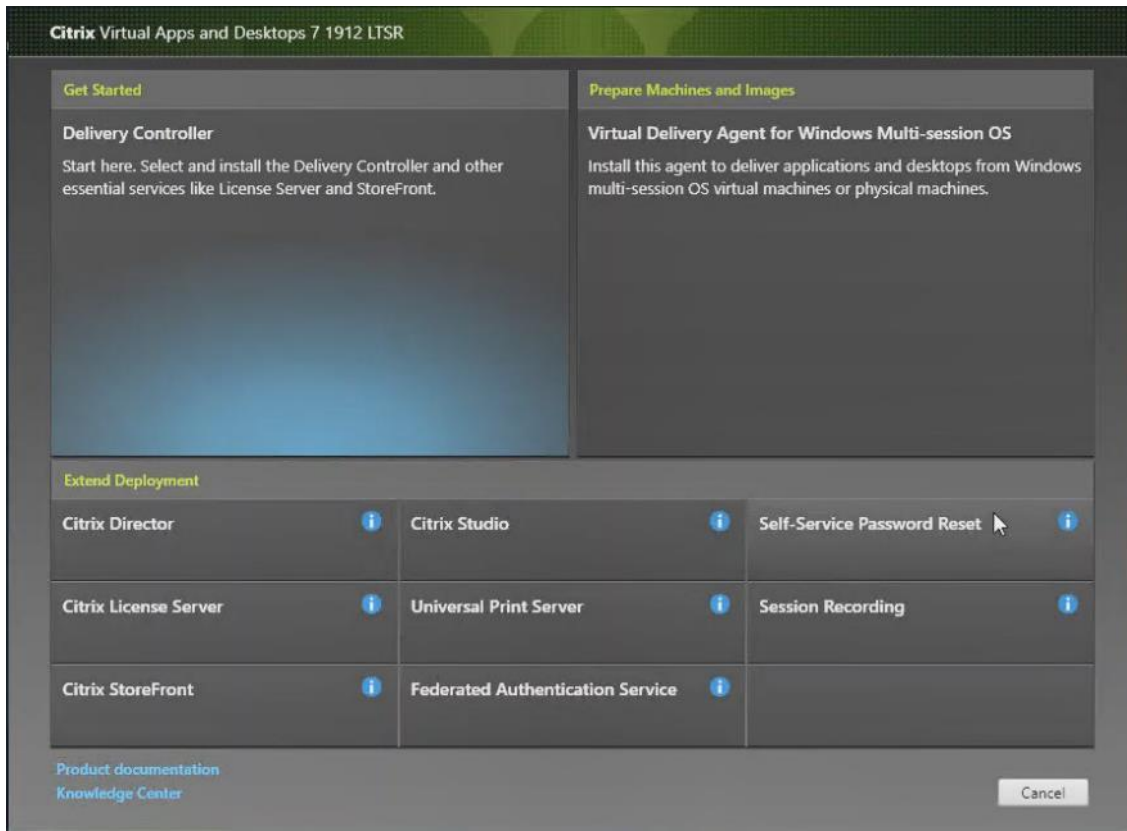
### Procedure 1. Install Citrix License Server

**Step 1.** Connect to the first Citrix License server and launch the installer from the Citrix Virtual Apps and Desktops 7 LTSR ISO.

**Step 2.** Click **Start**.

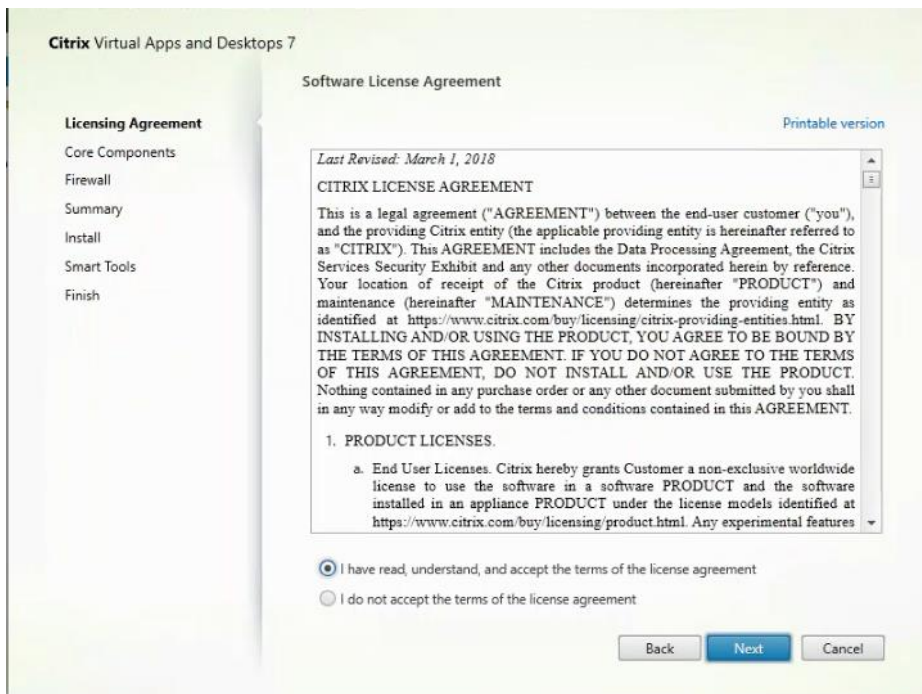


**Step 3.** Click **Extend Deployment - Citrix License Server**.

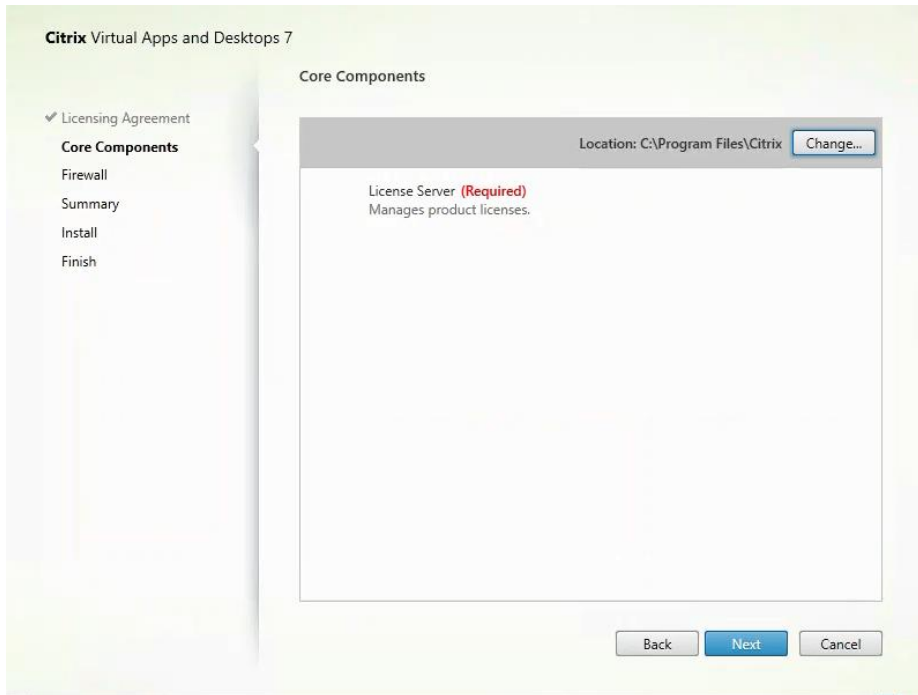


**Step 4.** Read the Citrix License Agreement. If acceptable, indicate your acceptance of the license by selecting the **I have read, understand, and accept the terms of the license agreement** radio button.

**Step 5.** Click **Next**.

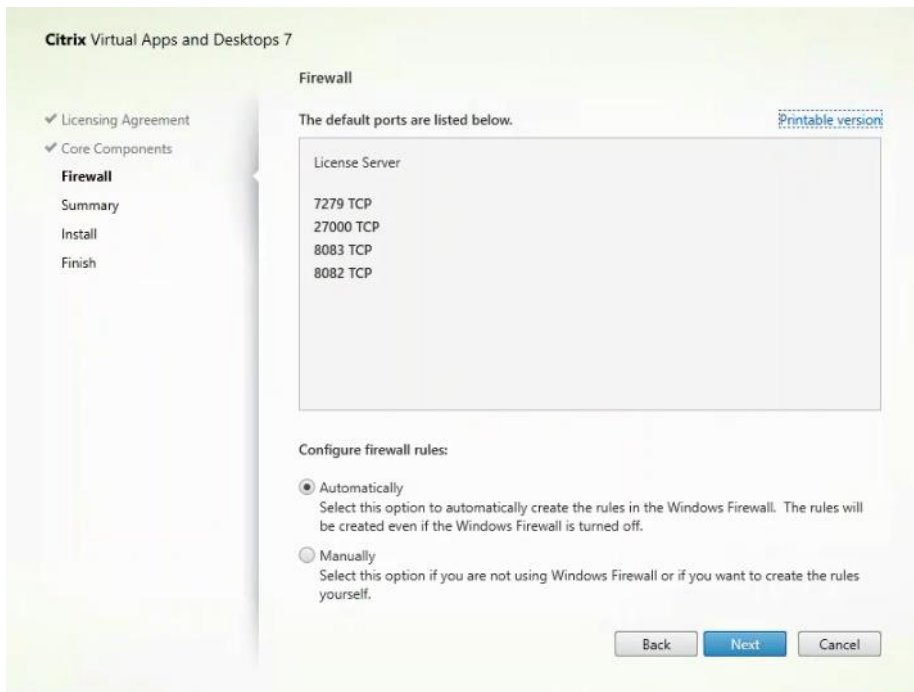


**Step 6.** Click **Next**.

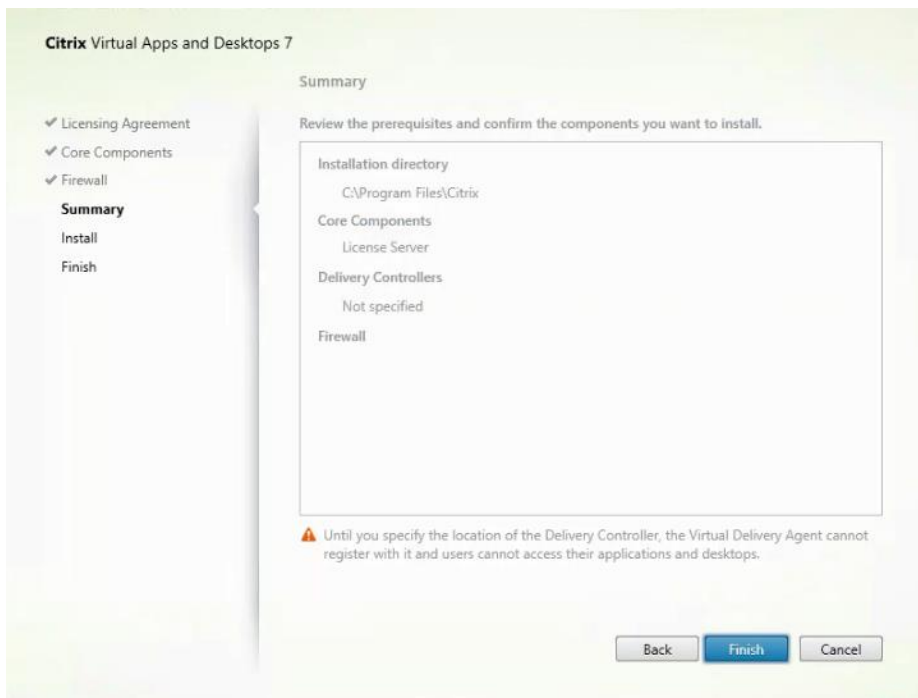


**Step 7.** Select the default ports and automatically configured firewall rules.

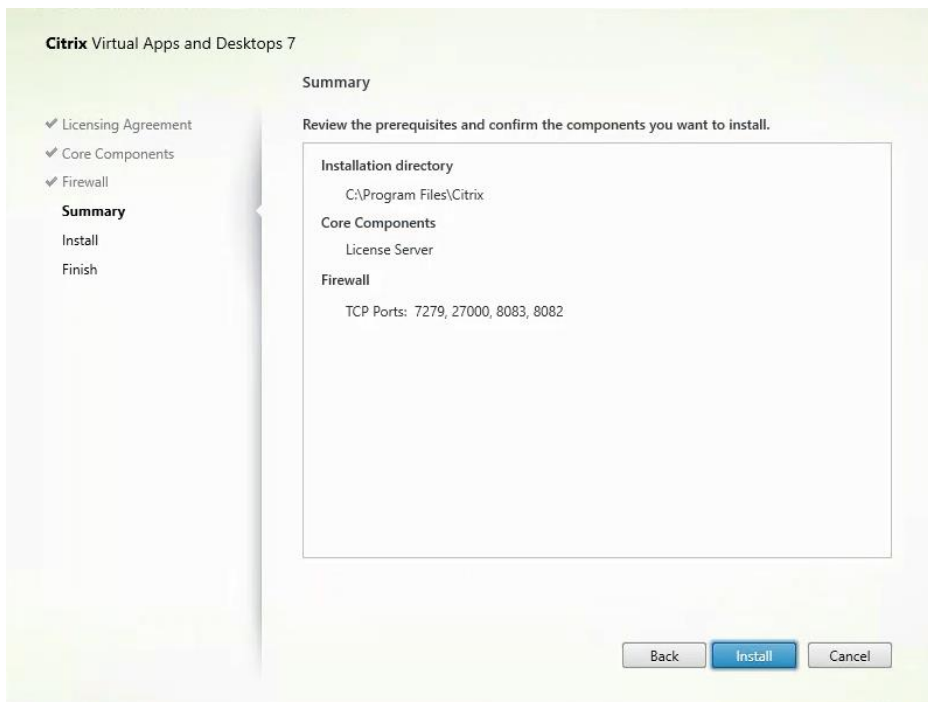
**Step 8.** Click **Next**.



**Step 9.** Click **Install**.



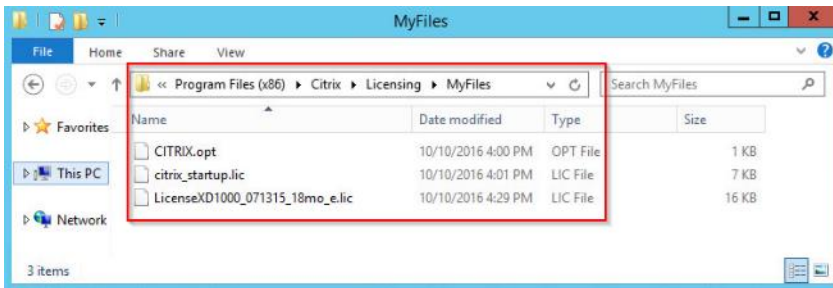
**Step 10.** Click **Finish** to complete the installation.



## 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.



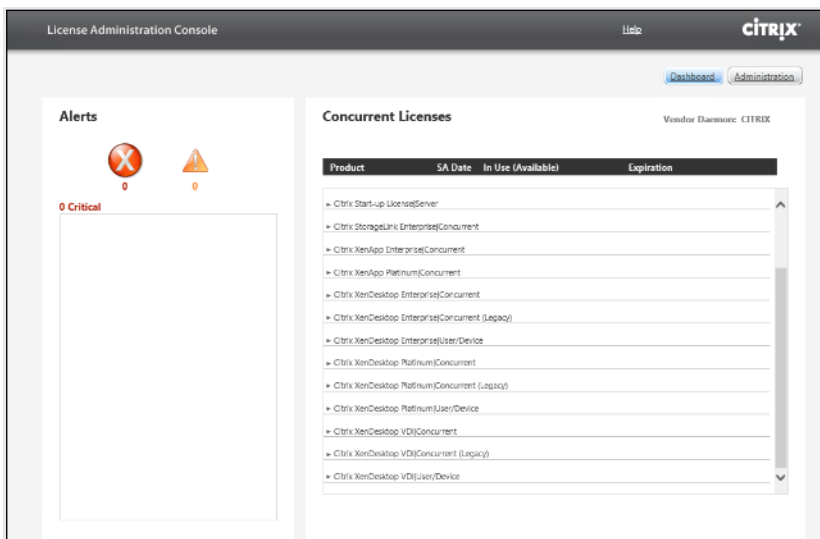


**Step 2.** Restart the server or Citrix licensing services so that the licenses are activated.

**Step 3.** Run the application Citrix License Administration Console.

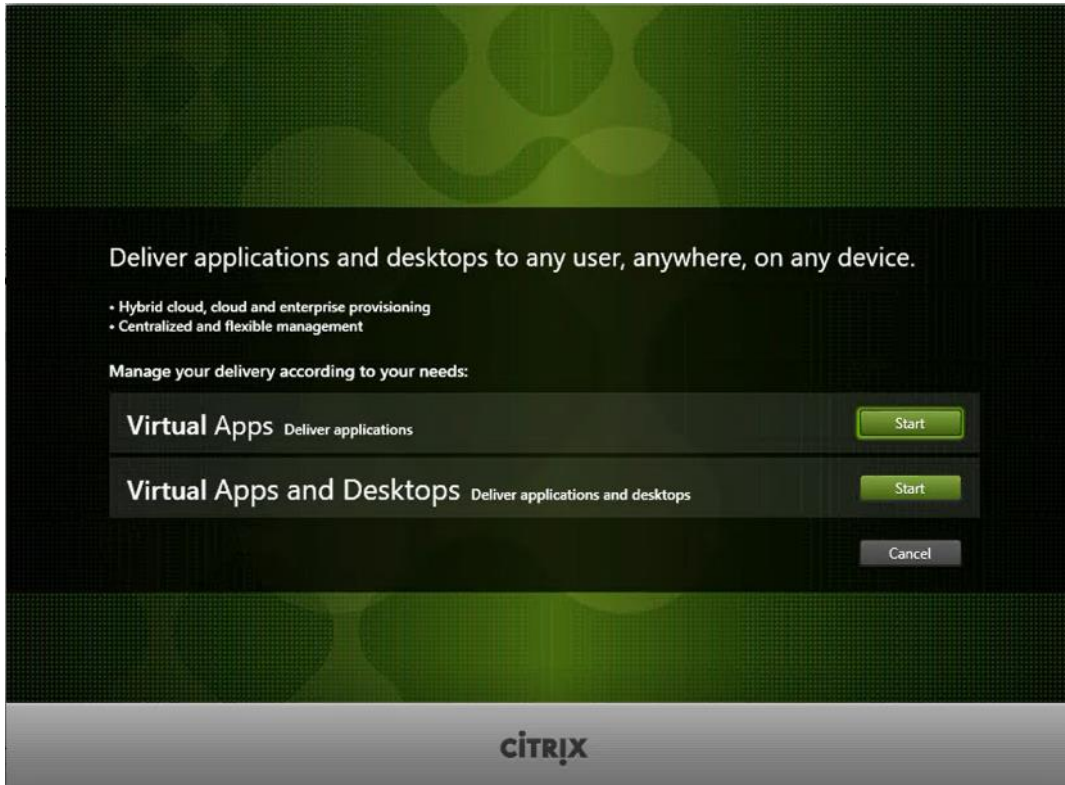


**Step 4.** Confirm that the license files have been read and enabled correctly.



**Procedure 3.** Install Citrix Desktop Broker/Studio

- 
- Step 1.** Connect to the first Citrix VDI server and launch the installer from the Citrix Desktop 7 LTSR ISO.
- Step 2.** Click **Start**.



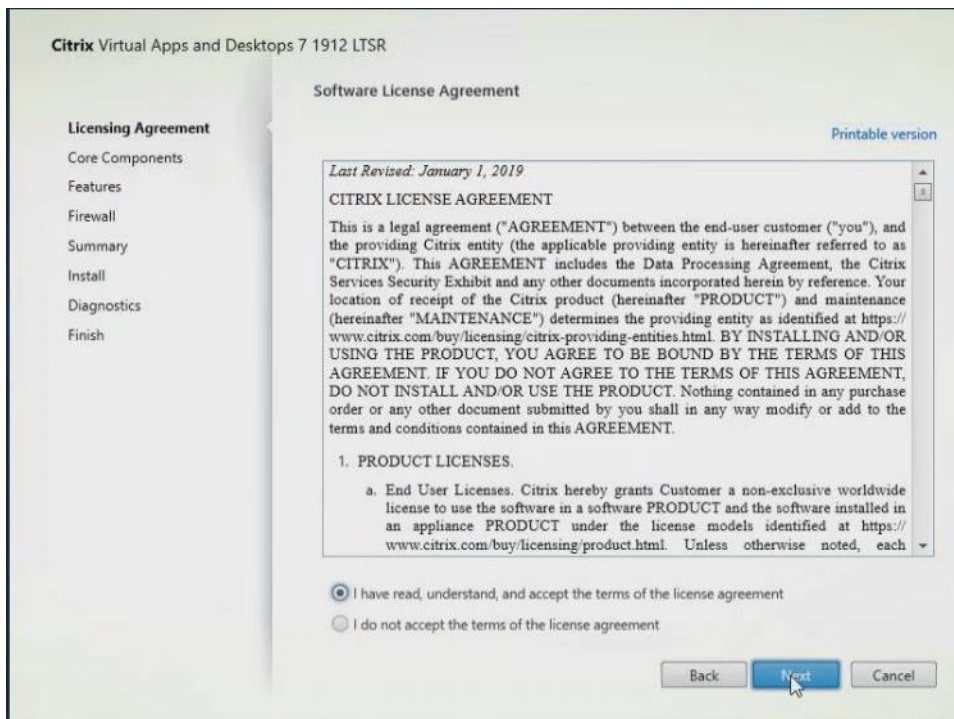
The installation wizard presents a menu with three subsections.

- Step 3.** Click **Get Started - Delivery Controller**.



**Step 4.** Read the Citrix License Agreement and if acceptable, indicate your acceptance of the license by selecting the **I have read, understand, and accept the terms of the license agreement** radio button.

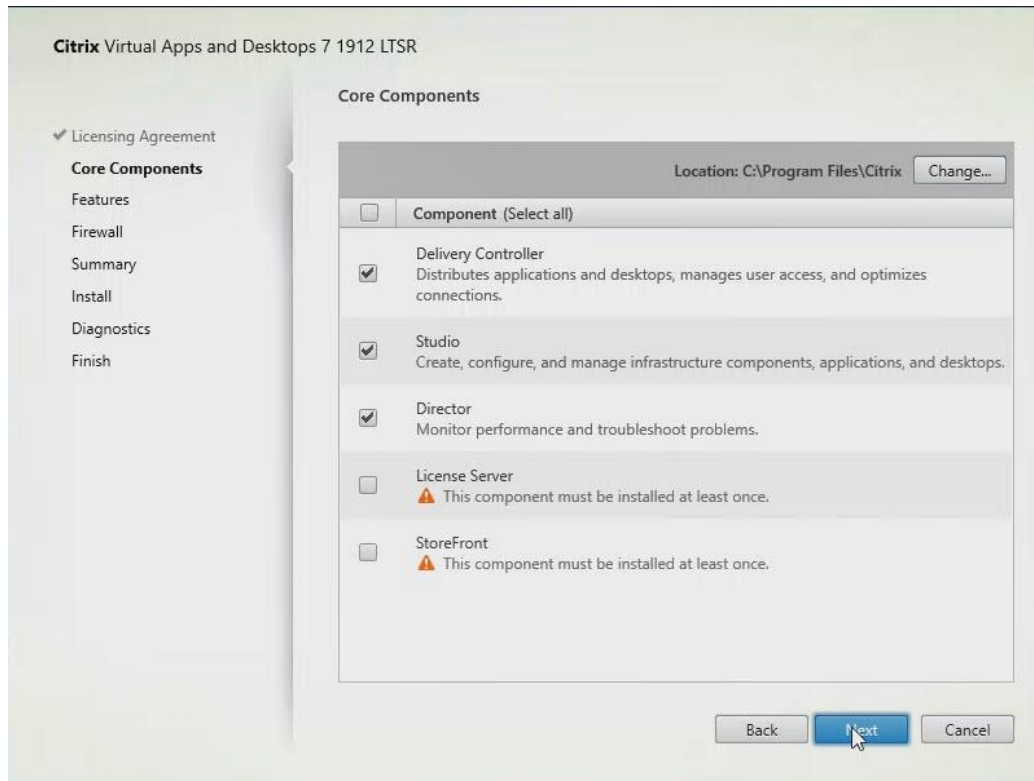
**Step 5.** Click **Next**.



**Step 6.** Select the components to be installed on the first Delivery Controller Server:

- a. Delivery Controller
- b. Studio
- c. Director

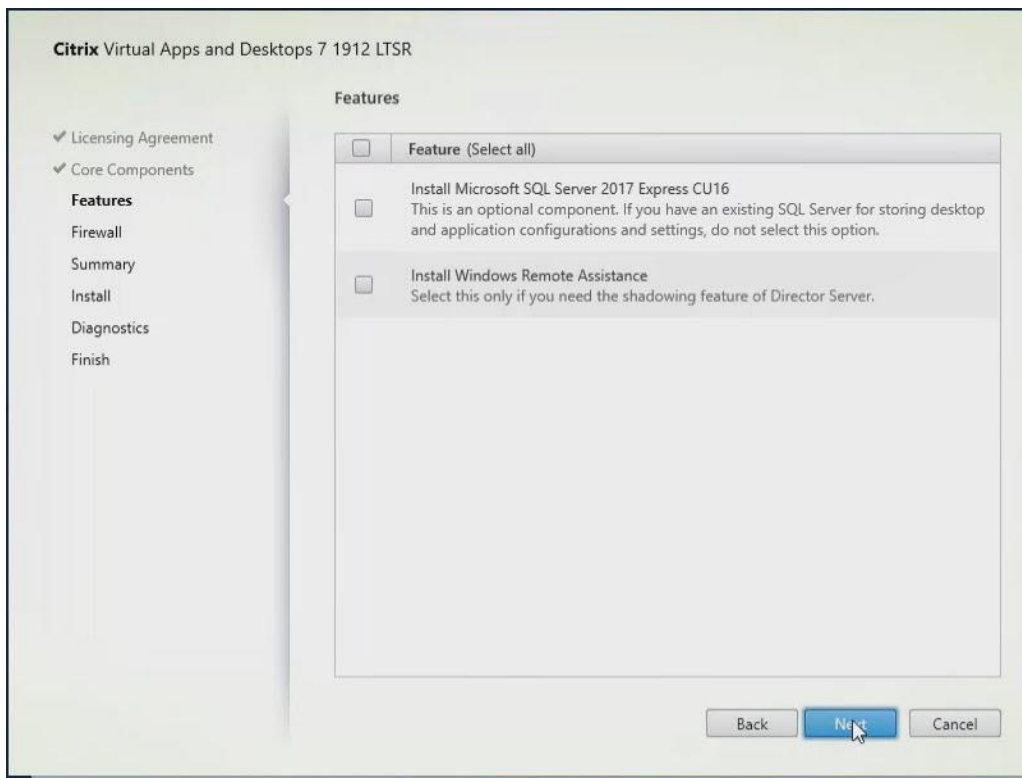
**Step 7.** Click **Next**.



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

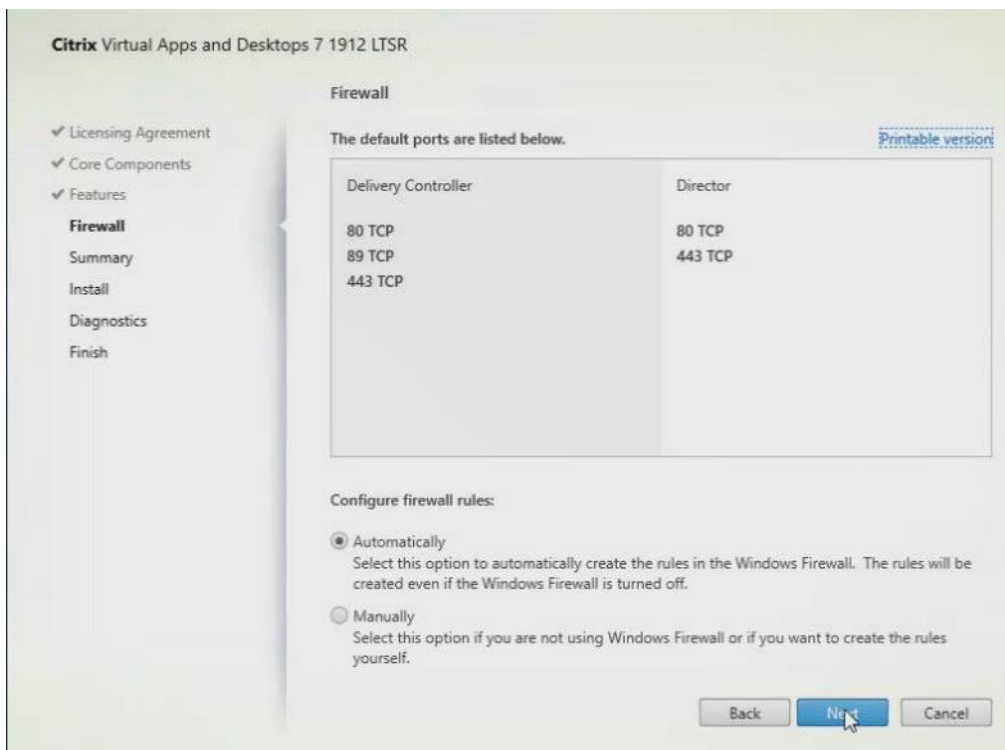
**Step 8.** Since a SQL Server will be used to Store the Database, leave "Install Microsoft SQL Server 2017 CU16 Express" unchecked.

**Step 9.** Click **Next**.

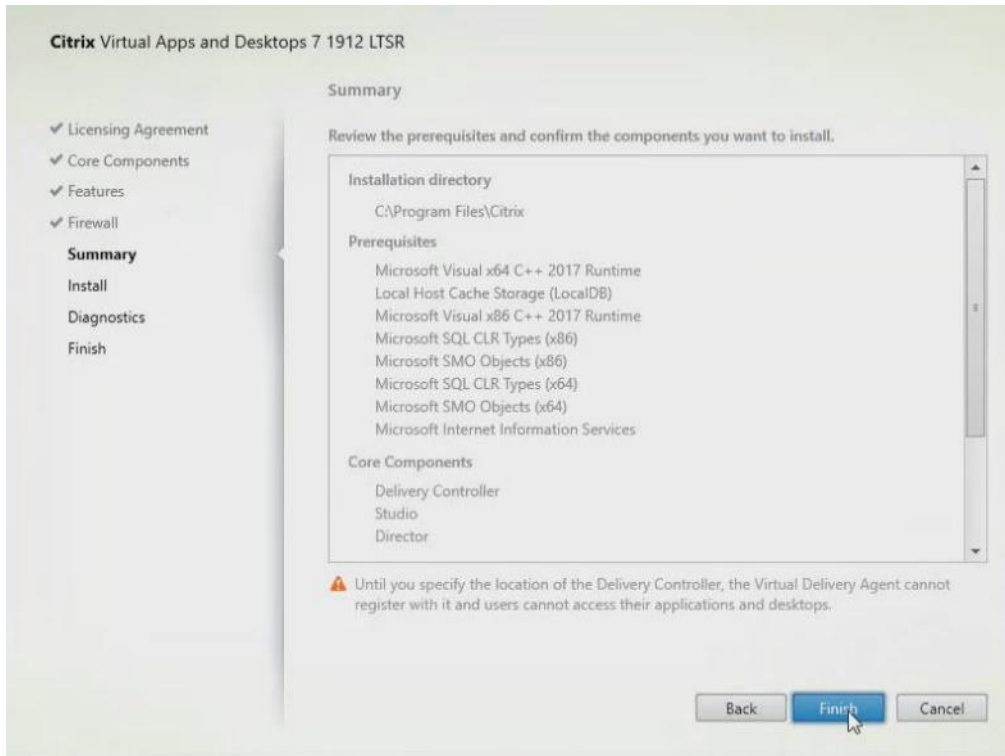


**Step 10.** Select the default ports and automatically configured firewall rules.

**Step 11.** Click **Next**.

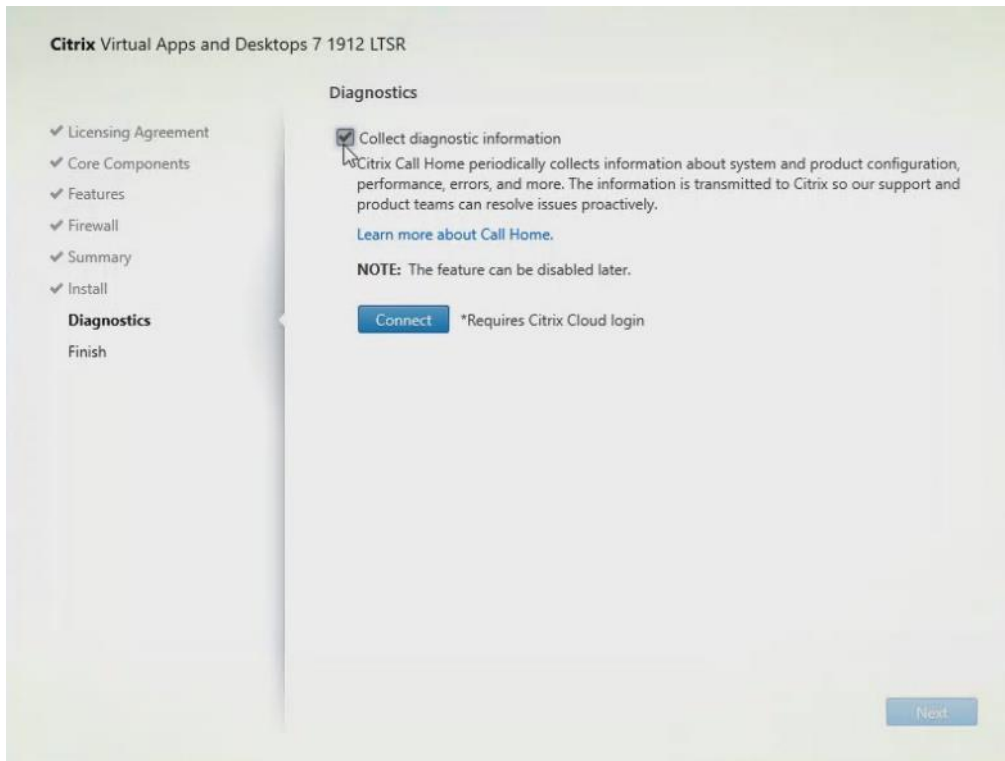


**Step 12.** Click **Install**.



**Step 13.** (Optional) Click the **Call Home** participation.

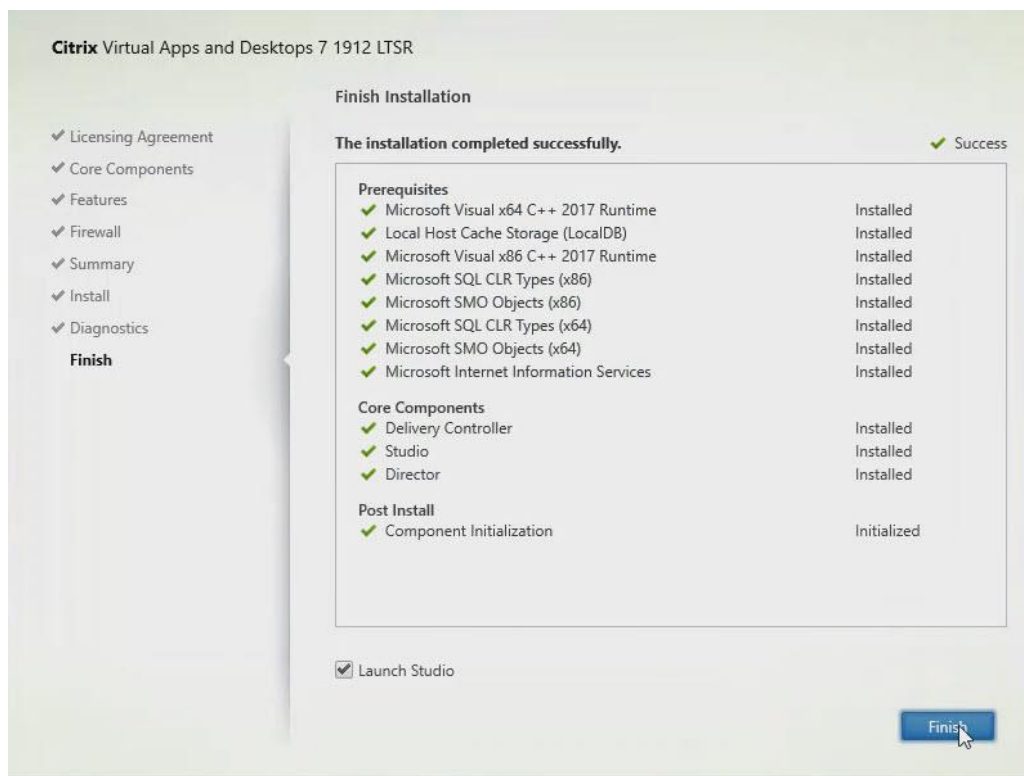
**Step 14.** Click **Next**.



**Step 15.** Click **Finish** to complete the installation.

**Step 16.** (Optional) **Check Launch Studio** to launch Citrix Studio Console.

**Step 17.** Click **Finish**.



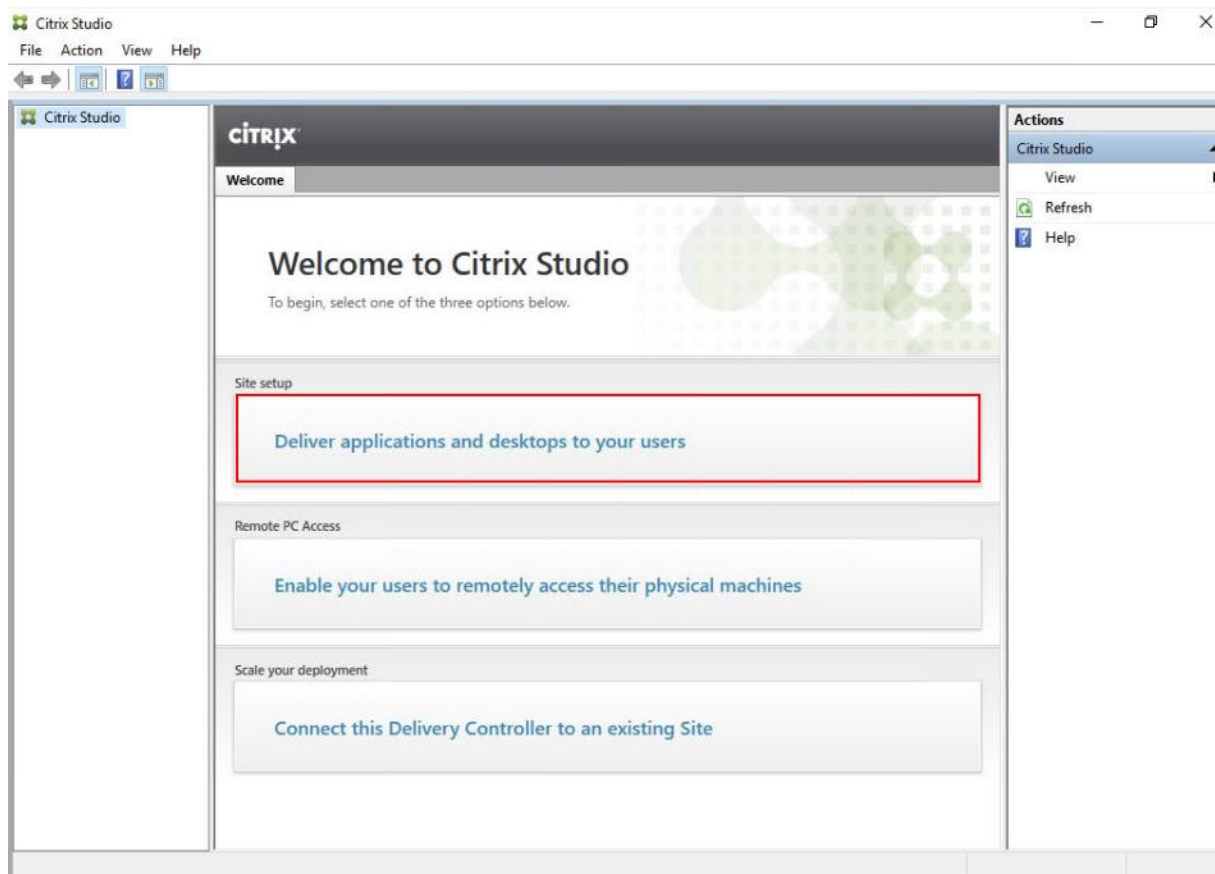
#### Procedure 4. Configure the Citrix VDI Site

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

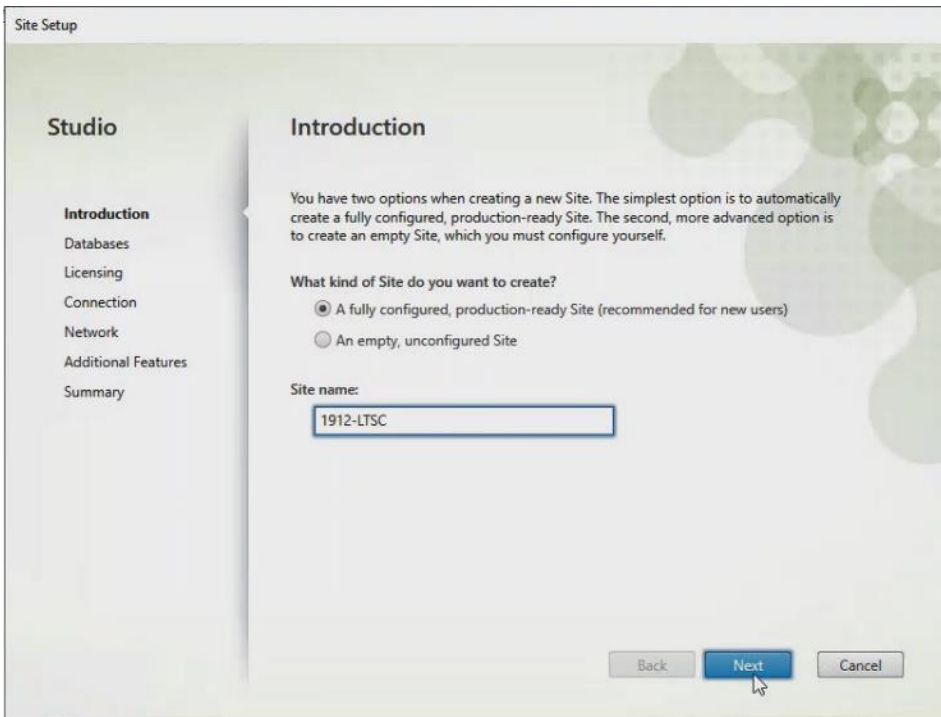
Citrix Studio launches automatically after the Citrix VDI Delivery Controller installation, or if necessary, it can be launched manually. Citrix Studio is used to create a Site, which is the core Citrix VDI environment consisting of the Delivery Controller and the Database.

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

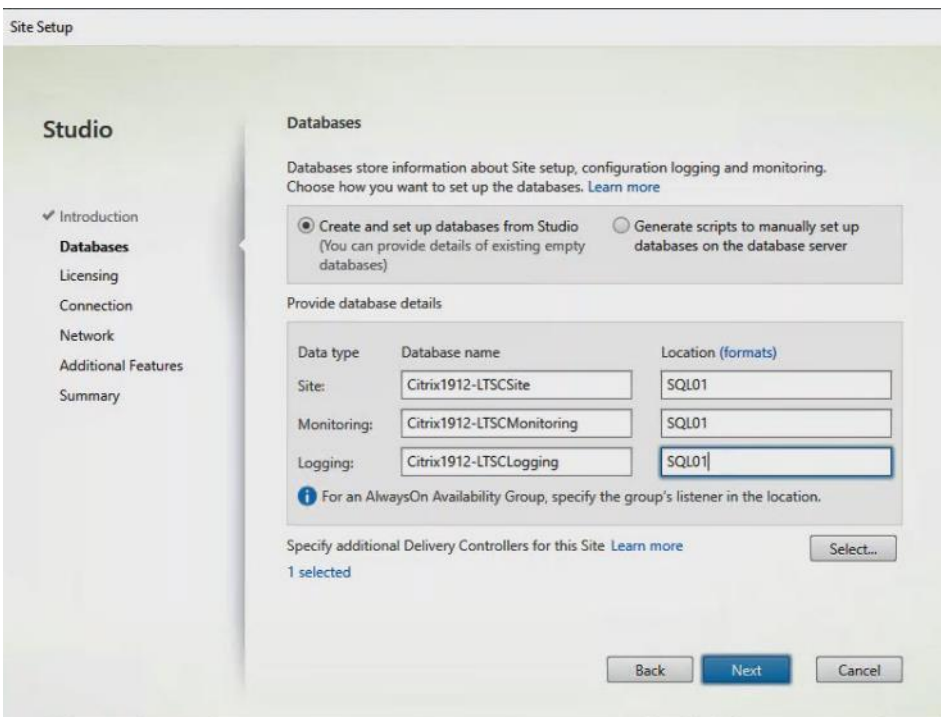




- Step 2.** Select the **A fully configured, production-ready Site** radio button.
- Step 3.** Enter a site name.
- Step 4.** Click **Next**.



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



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

**Step 7.** Provide the FQDN of the license server.

**Step 8.** 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 9.** Select the appropriate product edition using the license radio button.

**Step 10.** Click **Next**.

Site Setup

**Studio**

- Introduction
- Databases
- Licensing**
- Connection
- Network
- Additional Features
- Summary

**Licensing**

License server address:   Connected to trusted server  
View certificate

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
<input checked="" type="radio"/> Citrix XenDesktop Platinum	User/Device
<input type="radio"/> Citrix XenApp Platinum	Concurrent

**Step 11.** Select the Connection type **Microsoft System Center Virtual Machine Manager**.

**Step 12.** Enter the Connection Address to the VCenter Server Appliance.

**Step 13.** Enter the username (in username@domain format) for the vCenter account.

**Step 14.** Provide the password for the VCenter Admin account.

**Step 15.** Provide a connection name.

**Step 16.** Select the **Studio tools** radio button.

Add Connection and Resources

**Studio**

- Connection
- Storage Management
- Storage Selection
- Network
- Summary

**Connection**

Use an existing Connection

8x16

Create a new Connection

Connection type: VMware vSphere®

Connection address: *Example: https://vmware.example.com/sdk*

[Learn about user permissions](#)

User name: *Example: domain\username*

Password:

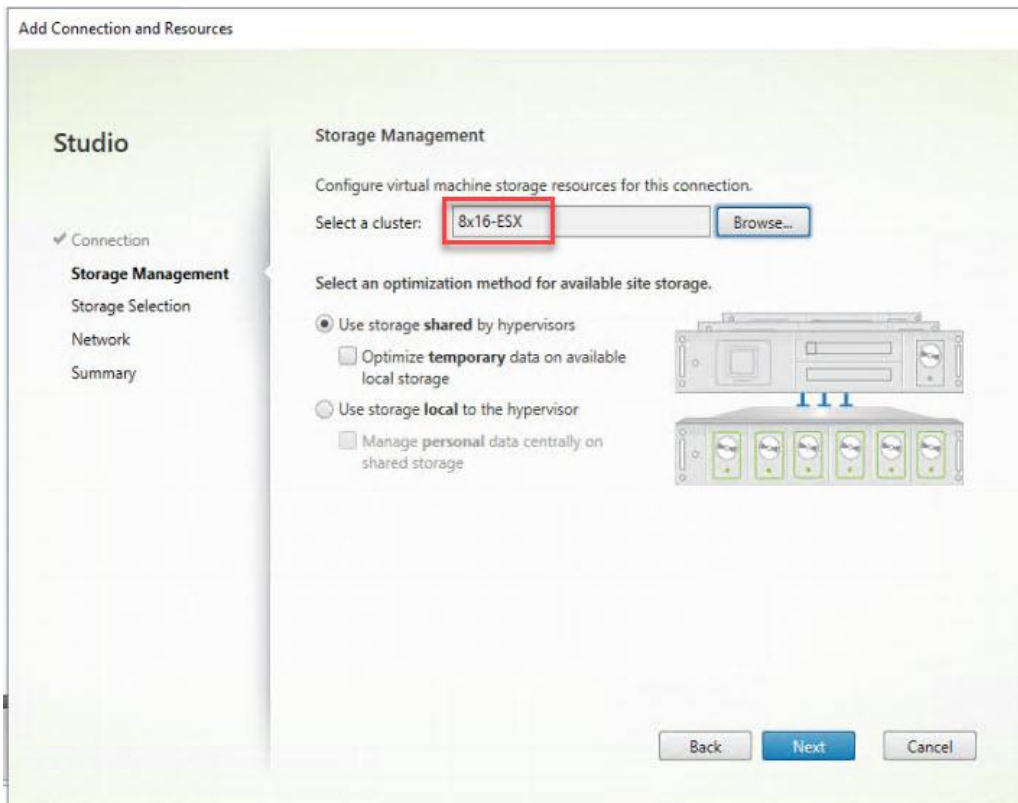
Connection name: *Example: MyConnection*

Create virtual machines using:

Studio tools (Machine Creation Services)  
Select this option when using AppDisks, even if you are using Citrix Provisioning.

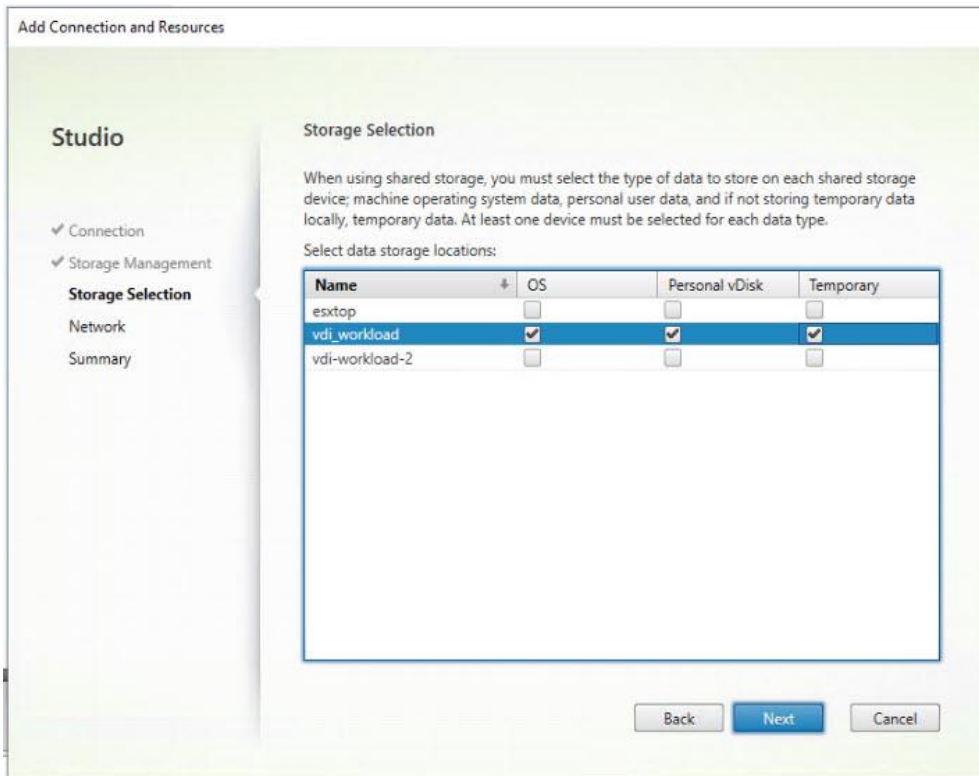
Other tools

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



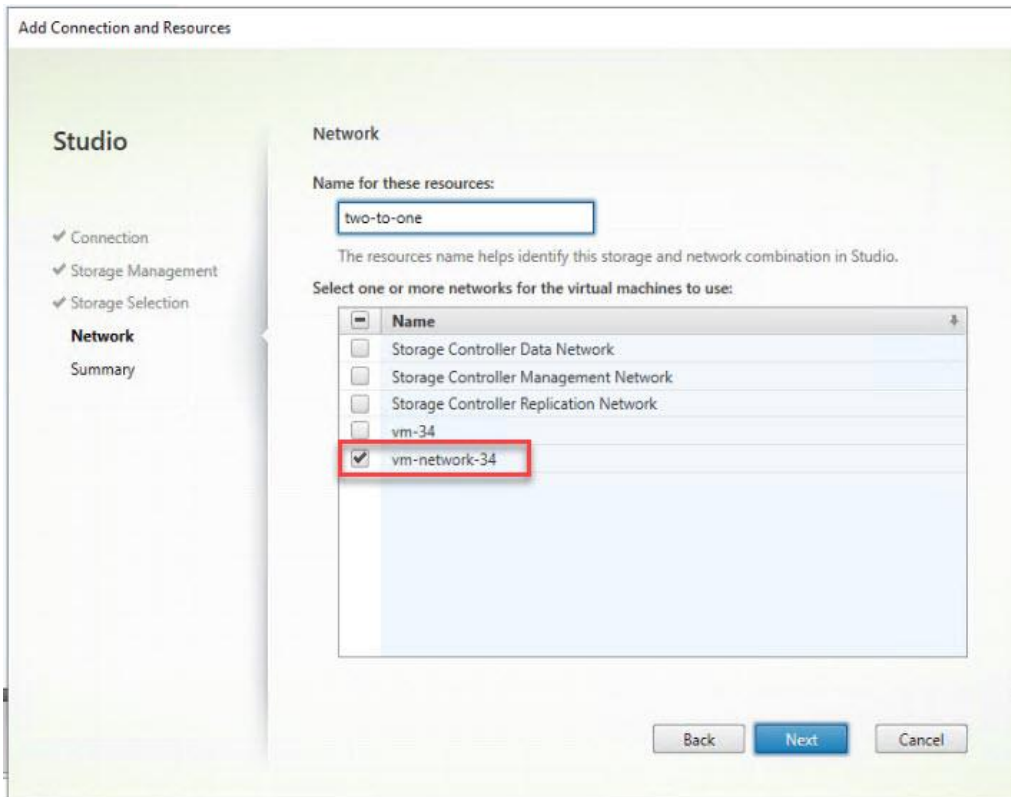
**Step 21.** Make the Storage selection to be used by this connection.

**Step 22.** Click **Next**.



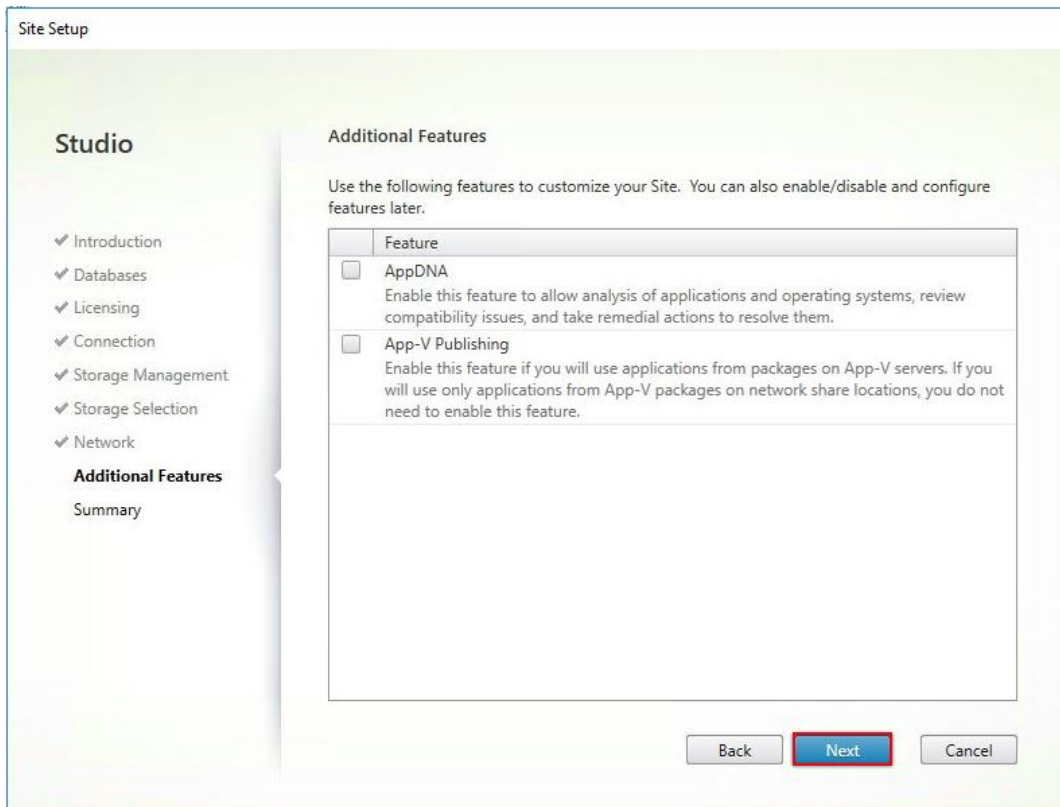
**Step 23.** Select the Network to be used by this connection.

**Step 24.** Click **Next**.



**Step 25.** Select **Additional features**.

**Step 26.** Click **Next**.

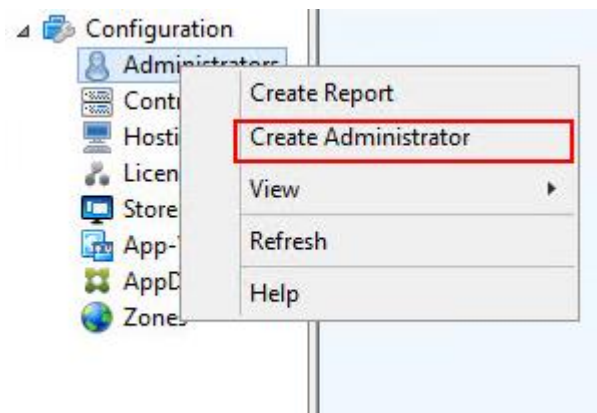


**Step 27.** Review Site configuration Summary and click **Finish**.

**Procedure 5.** Configure the Citrix VDI Site Administrators

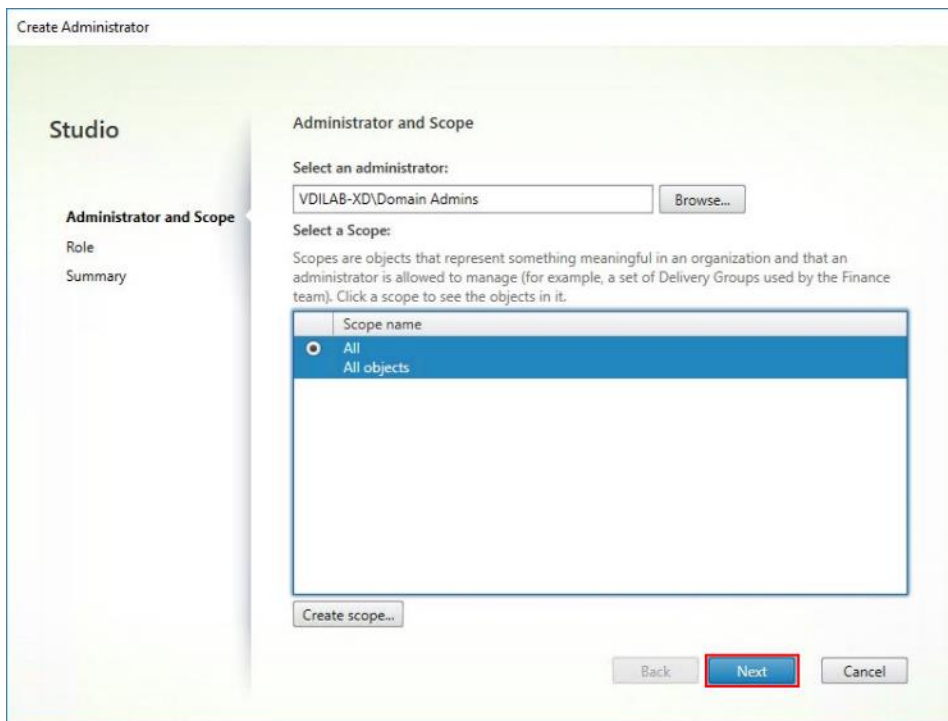
**Step 1.** Connect to the **Citrix VDI server** and open **Citrix Studio Management** console.

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

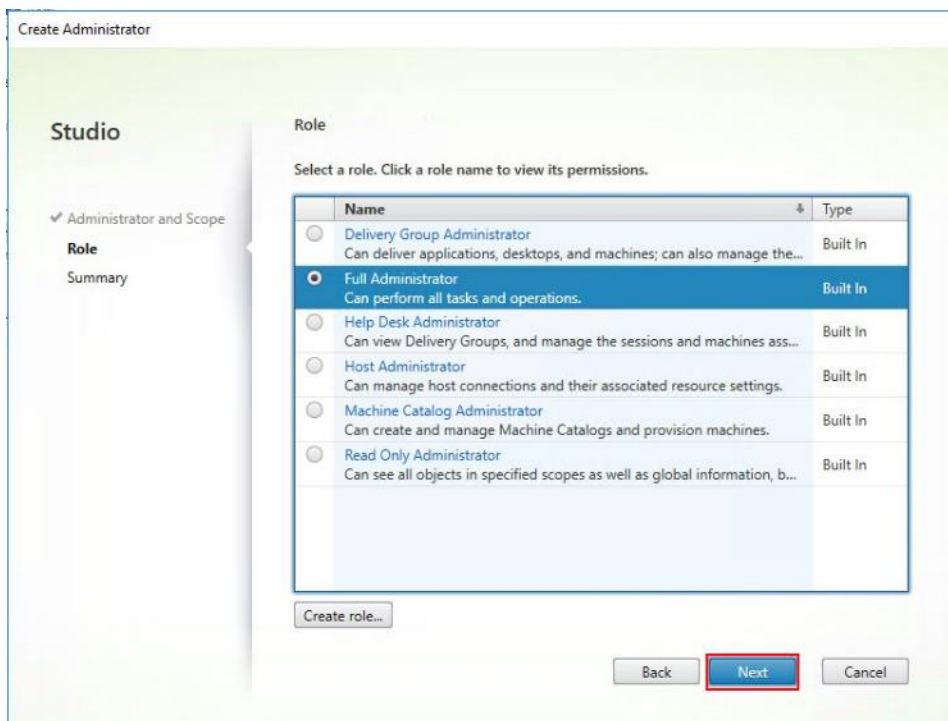


**Step 3.** Select/Create appropriate scope and click **Next**.

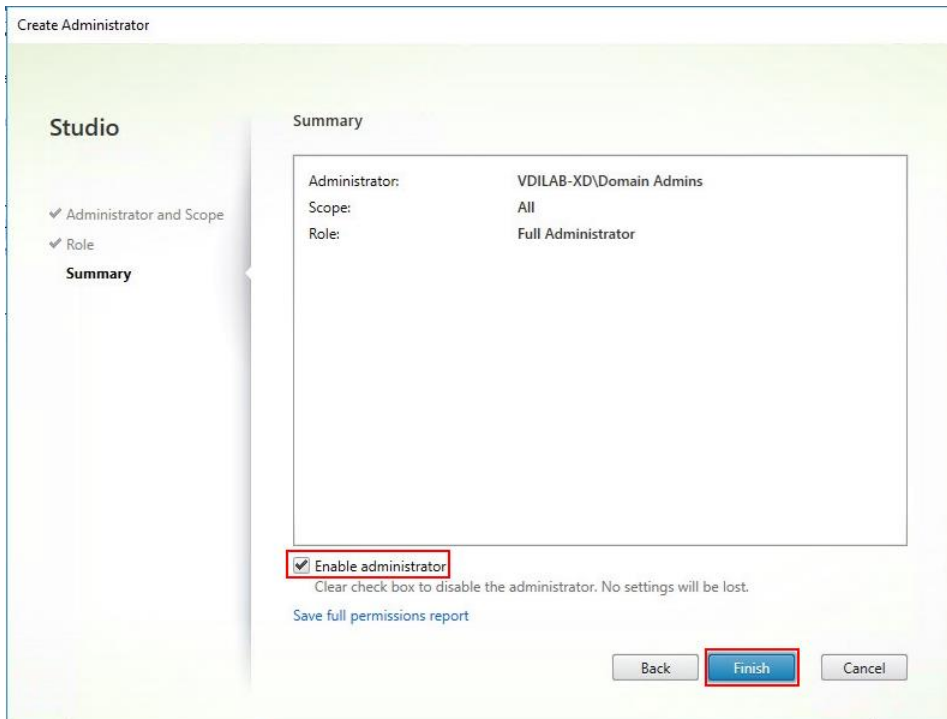




**Step 4.** Select an appropriate Role.



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



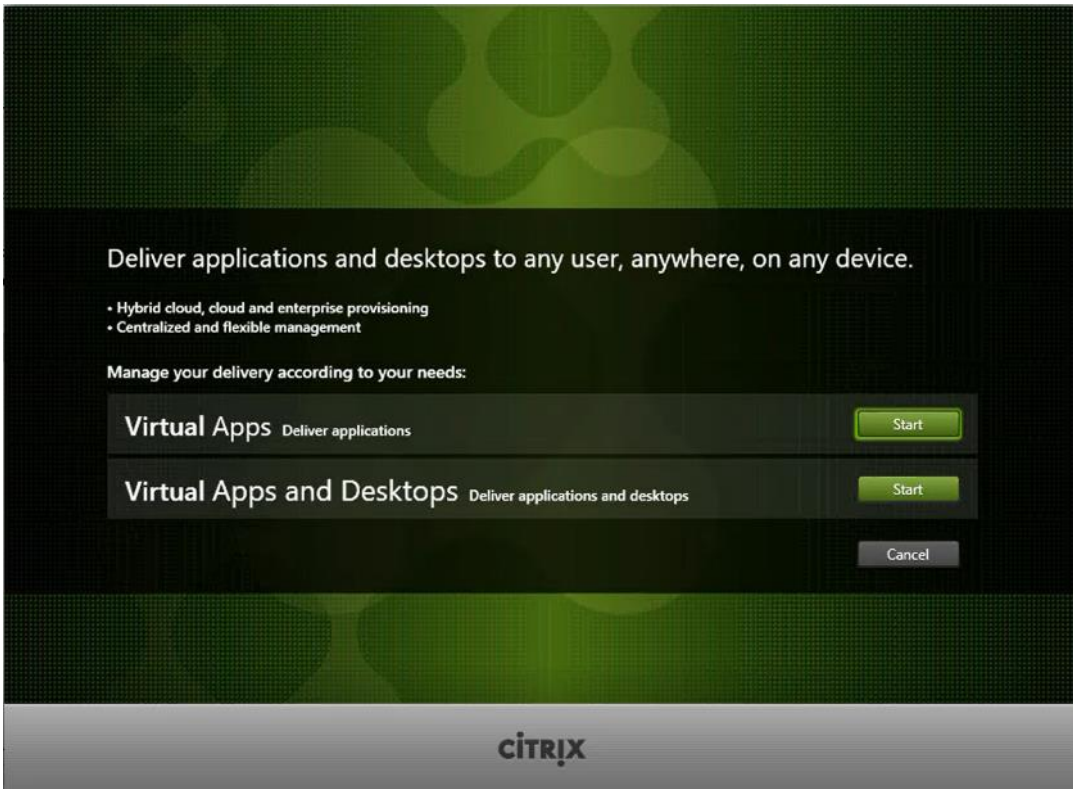
## Procedure 6. Configure Additional Citrix Desktop Controller

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

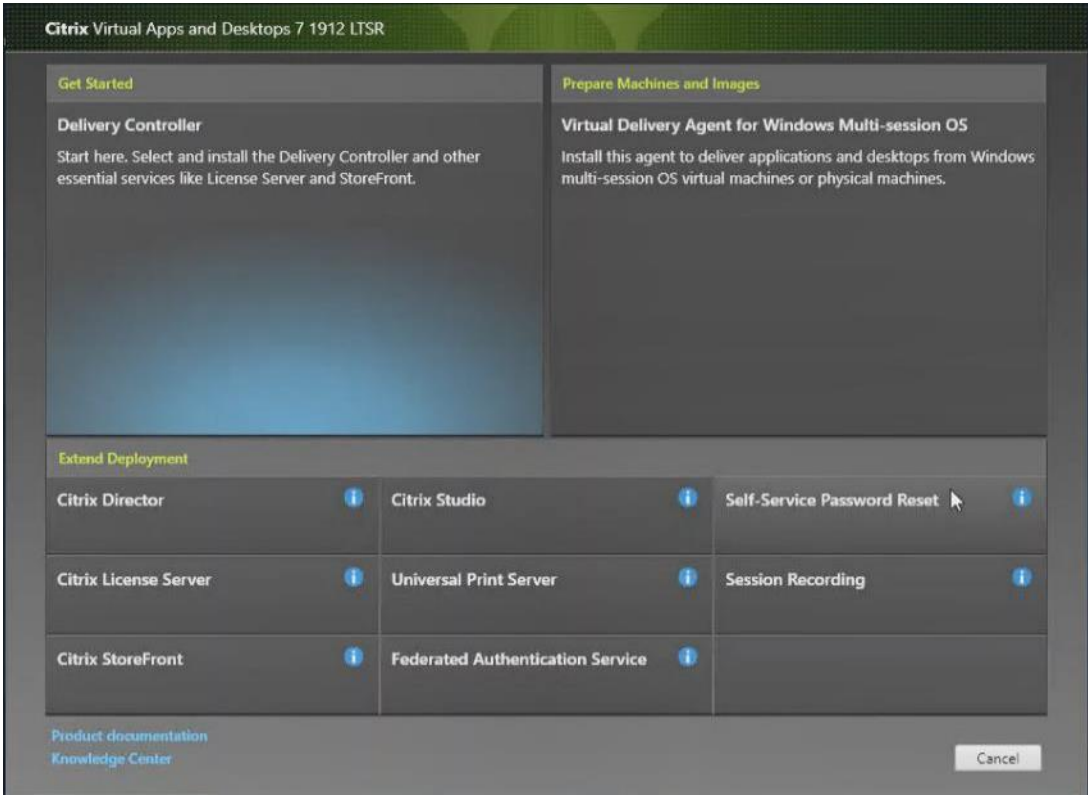
**Note:** In this CVD, we created 4 Delivery Controllers. Citrix recommends 1 Delivery Controller per 1000 users

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

**Step 2.** Click **Start**.



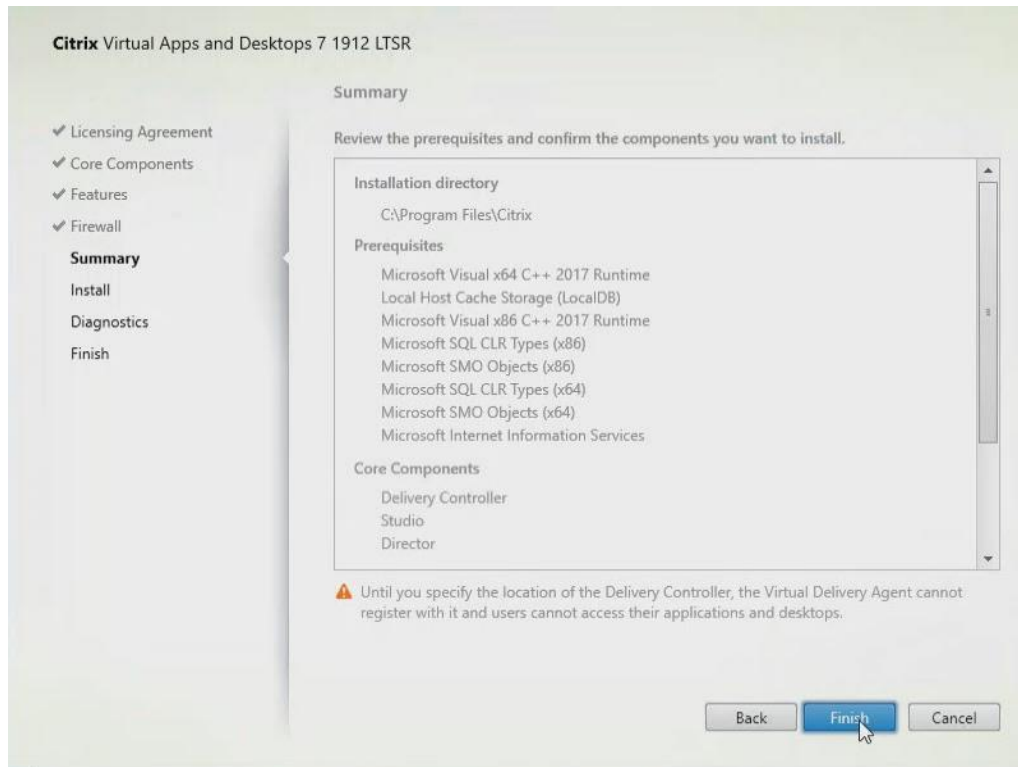
**Step 3.** Click **Delivery Controller**.



**Step 4.** Repeat the steps used to install the first Delivery Controller, including the step of importing an SSL certificate for HTTPS between the controller and Hyper-V.

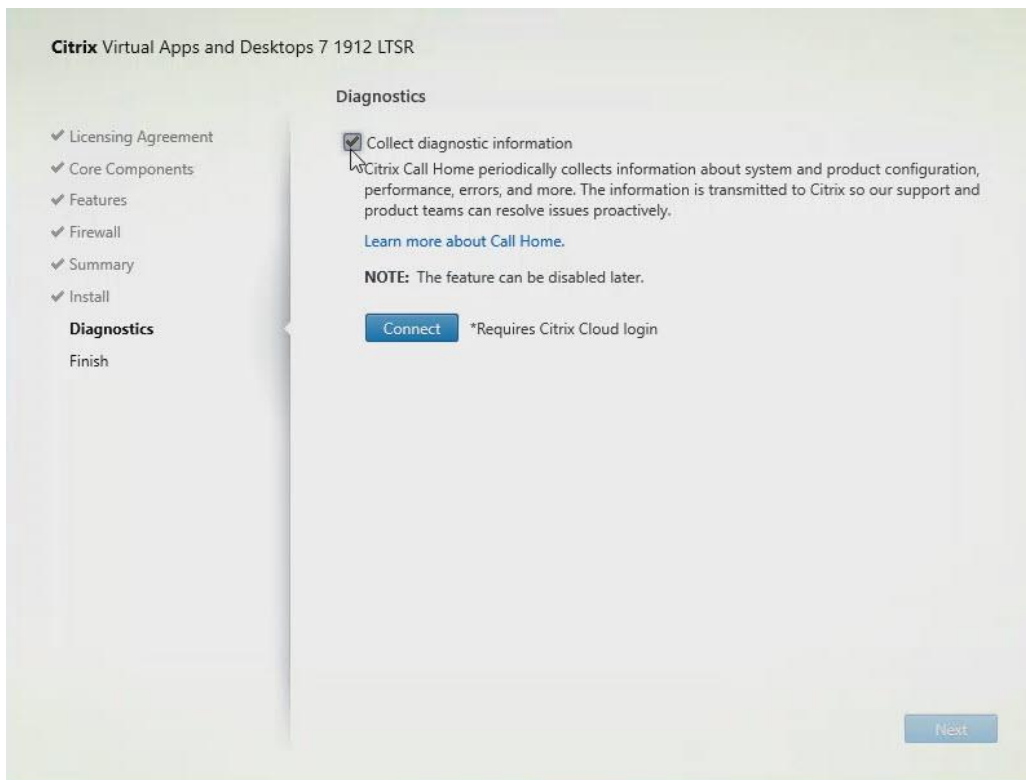
**Step 5.** Review the Summary configuration.

**Step 6.** Click **Install**.



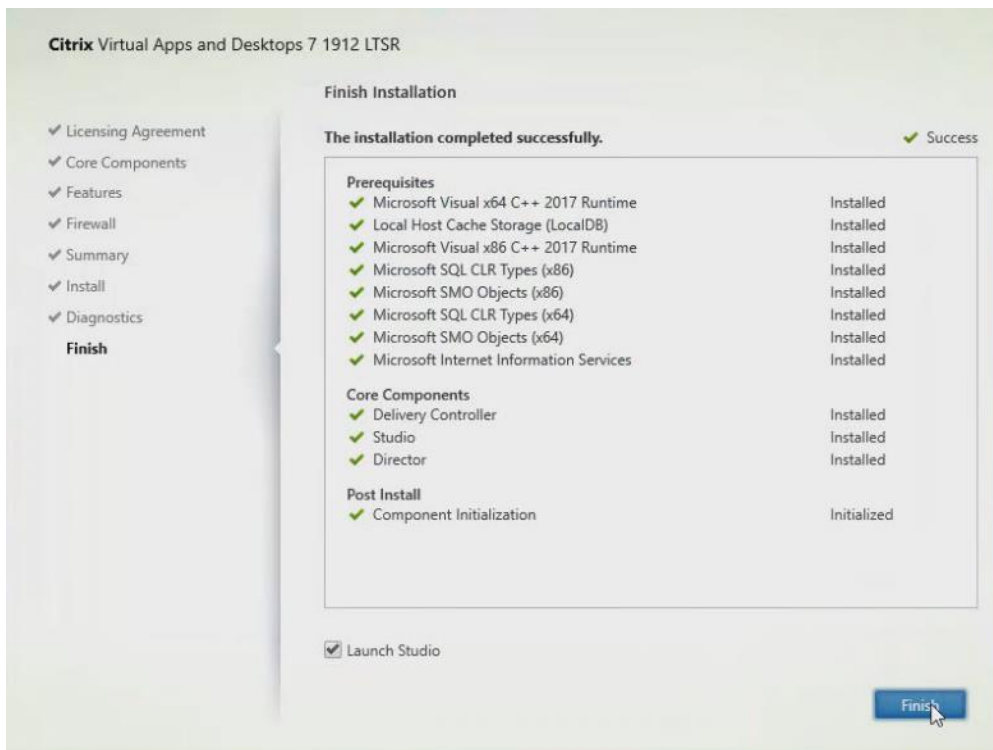
**Step 7.** (Optional) Click **Collect diagnostic information**.

**Step 8.** Click **Next**.



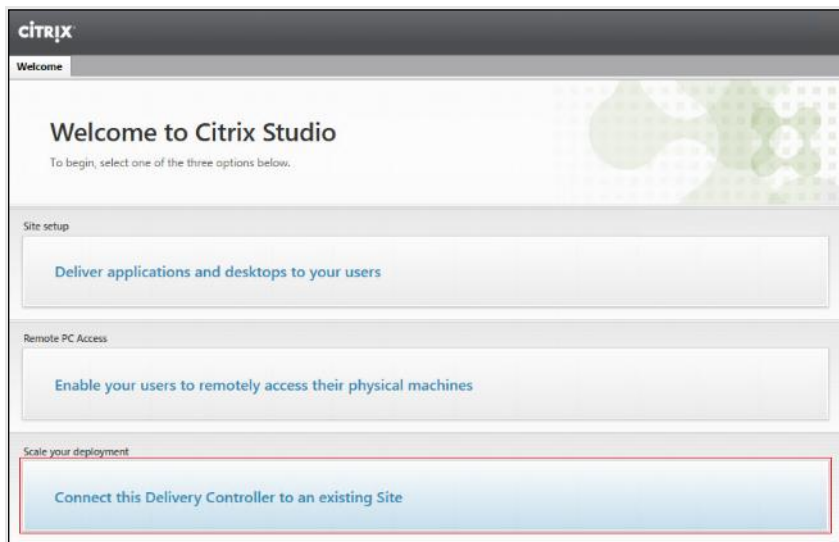
**Step 9.** Verify the components installed successfully.

**Step 10.** Click **Finish**.



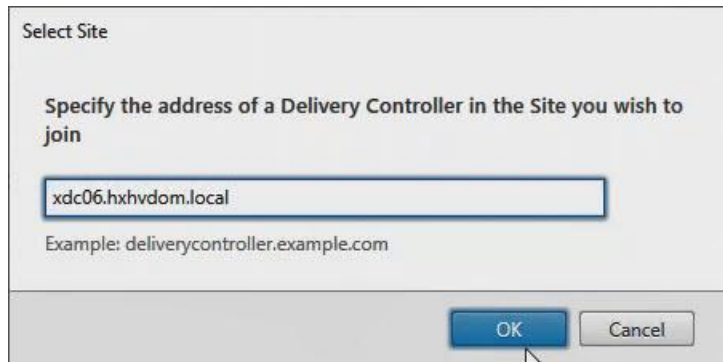
## Procedure 7. Add the Second Delivery Controller to the Citrix Desktop Site

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



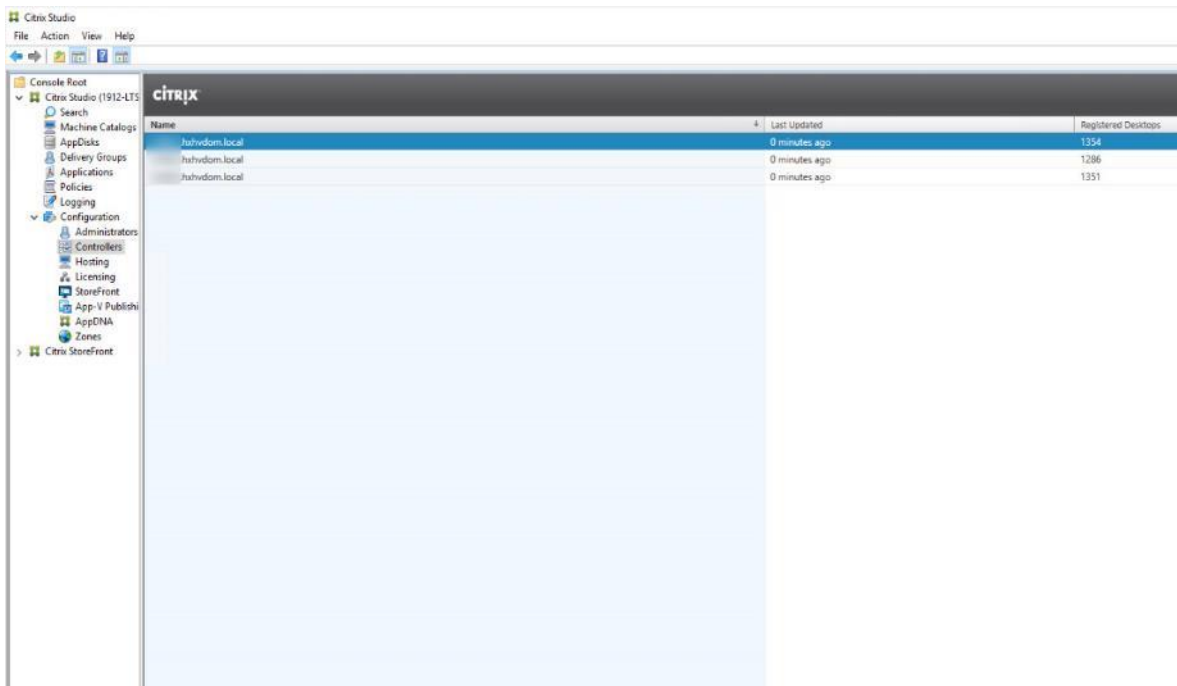
**Step 2.** Enter the FQDN of the first delivery controller.

**Step 3.** Click **OK**.



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

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



## Procedure 8. Install and Configure StoreFront

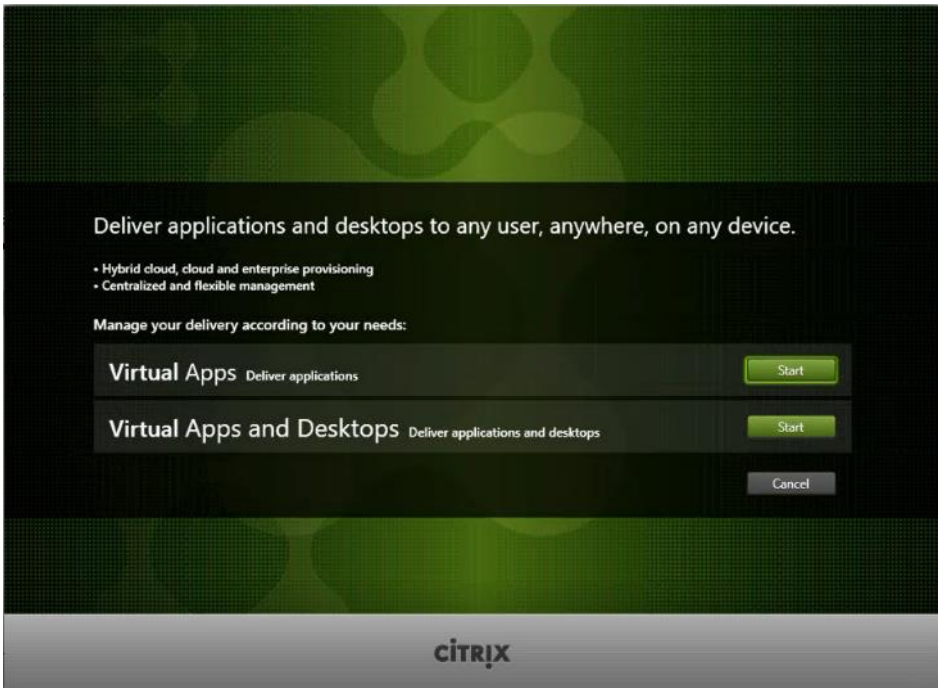
Citrix StoreFront stores aggregate desktops and applications from Citrix VDI sites, making resources readily available to users.

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

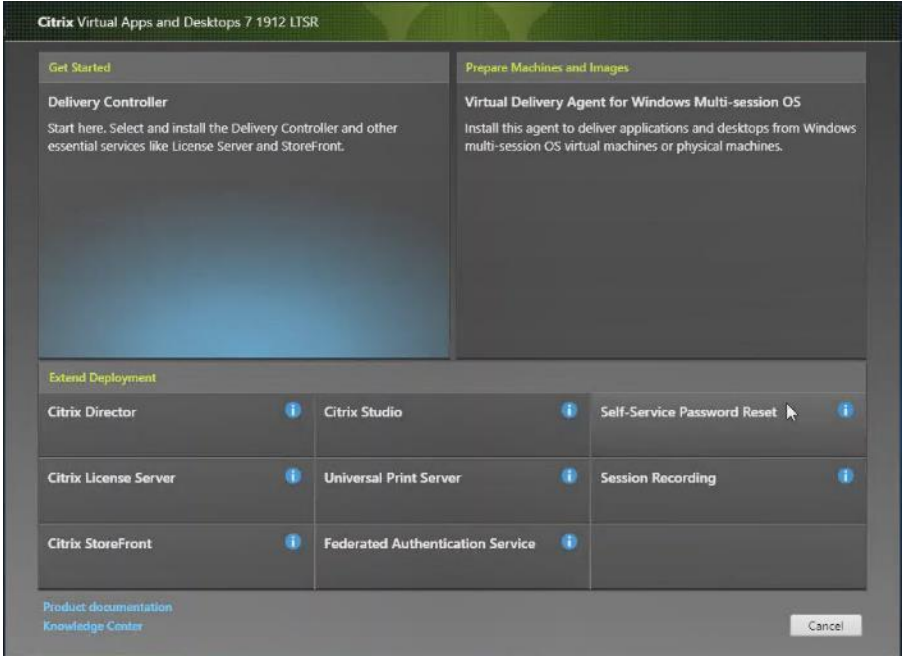
**Step 1.** To begin the installation of the StoreFront, connect to the first StoreFront server and launch the installer from the Citrix Desktop 7 LTSR ISO.

**Step 2.** Click **Start**.





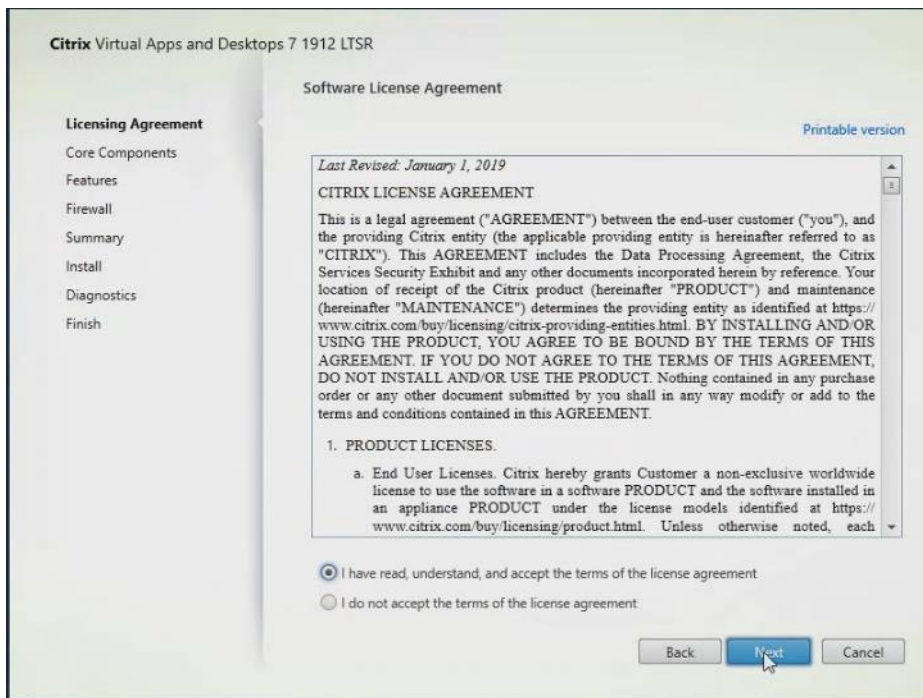
**Step 3.** Click **Extend Deployment Citrix StoreFront**.



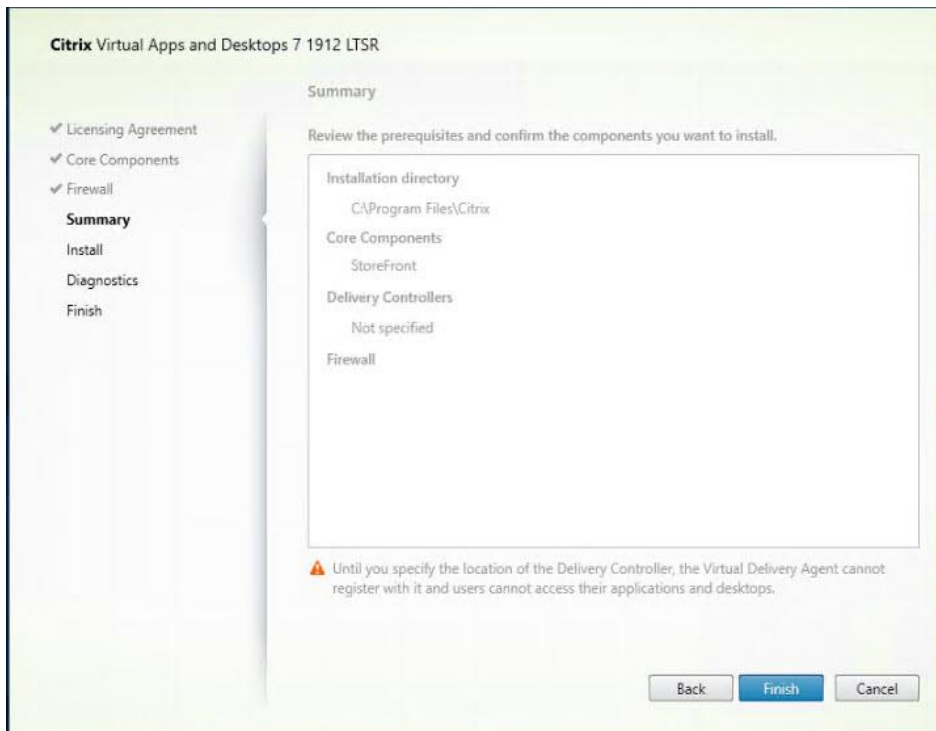
**Step 4.** If acceptable, indicate your acceptance of the license by selecting the **I have read, understand, and accept the terms of the license agreement** radio button.

**Step 5.** Click **Next**.





**Step 6.** Select **Storefront** and click **Next**.



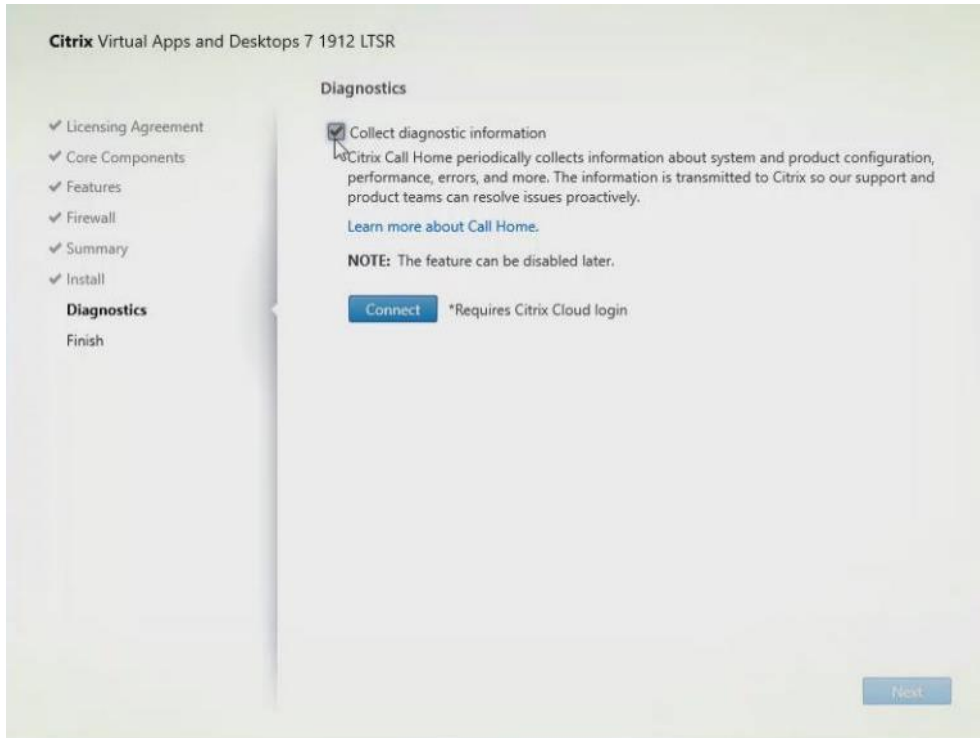
**Step 7.** Select the default ports and automatically configured firewall rules.

**Step 8.** Click **Next**.

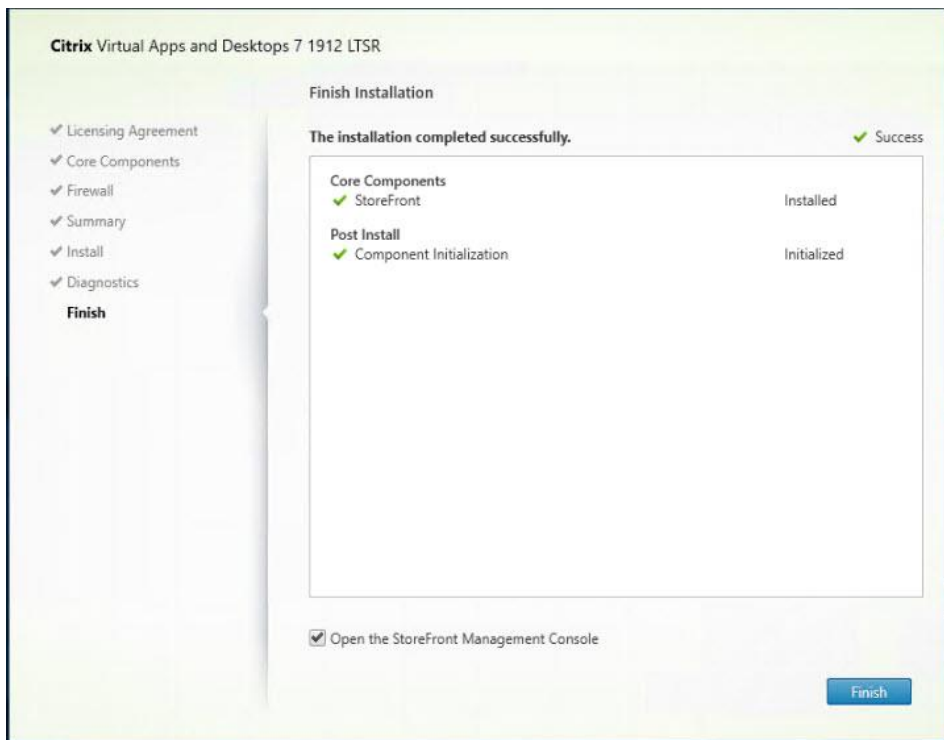
**Step 9.** Click **Install**.

**Step 10.** (Optional) Click **Collect diagnostic information**.

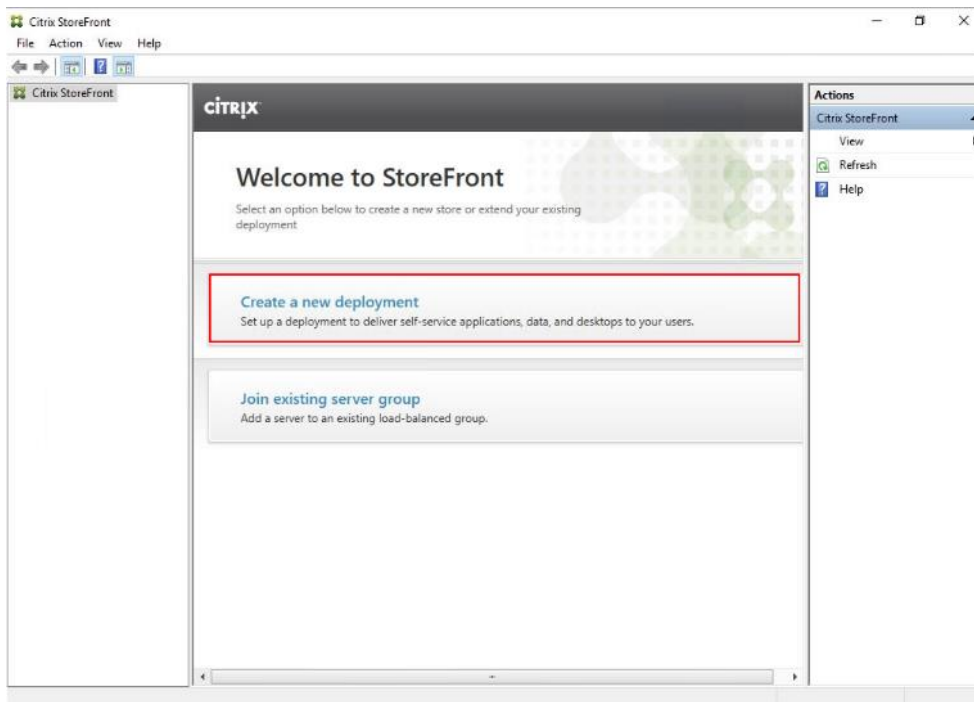
**Step 11.** Click **Next**.



**Step 12.** Click **Finish**.

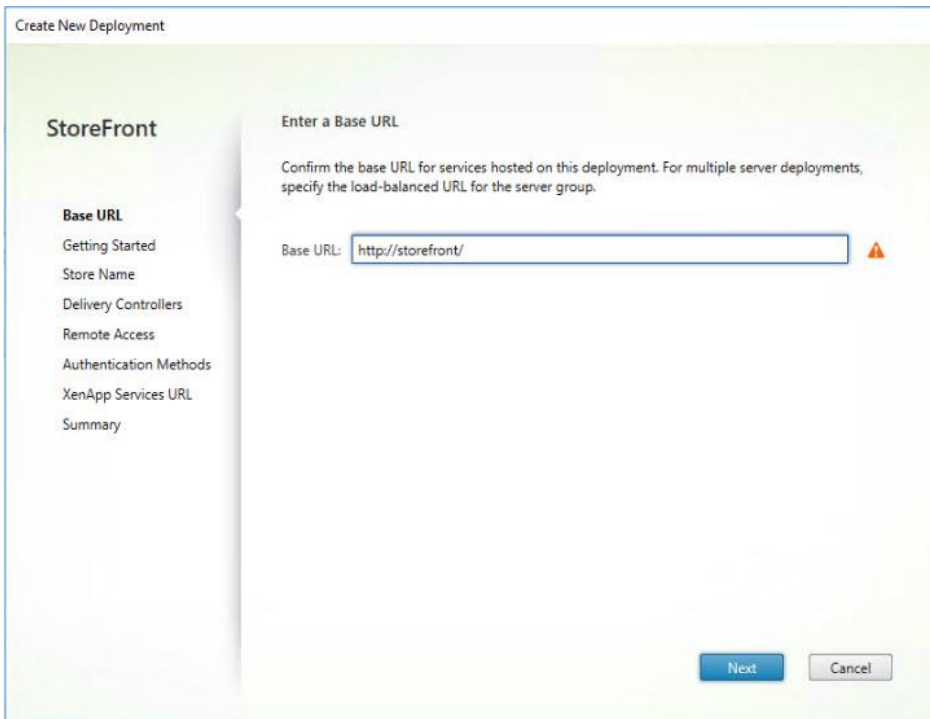


**Step 13.** Click **Create a new deployment.**

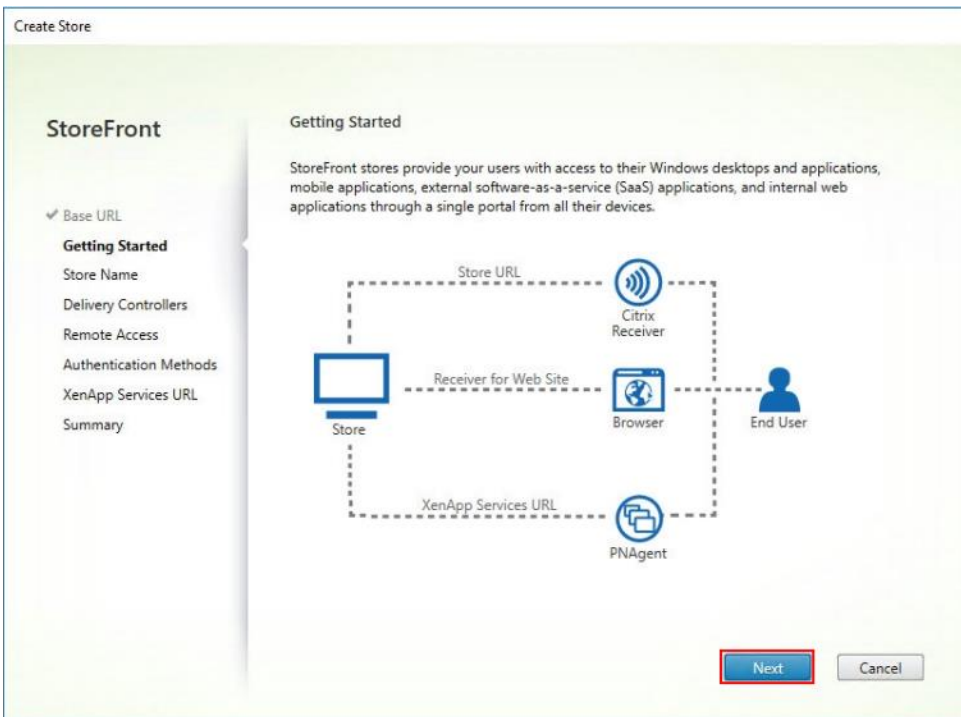


**Step 14.** Specify the URL of the StoreFront server and click **Next.**

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



**Step 15.** Click **Next**.



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

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 as part of the user's account.

**i** Store name and access type cannot be changed, once the store is created.

Store Name:

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.

Back Next Cancel

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

Create Store

### StoreFront

- ✓ Getting Started
- ✓ Store Name
- Delivery Controllers**
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

#### Delivery Controllers

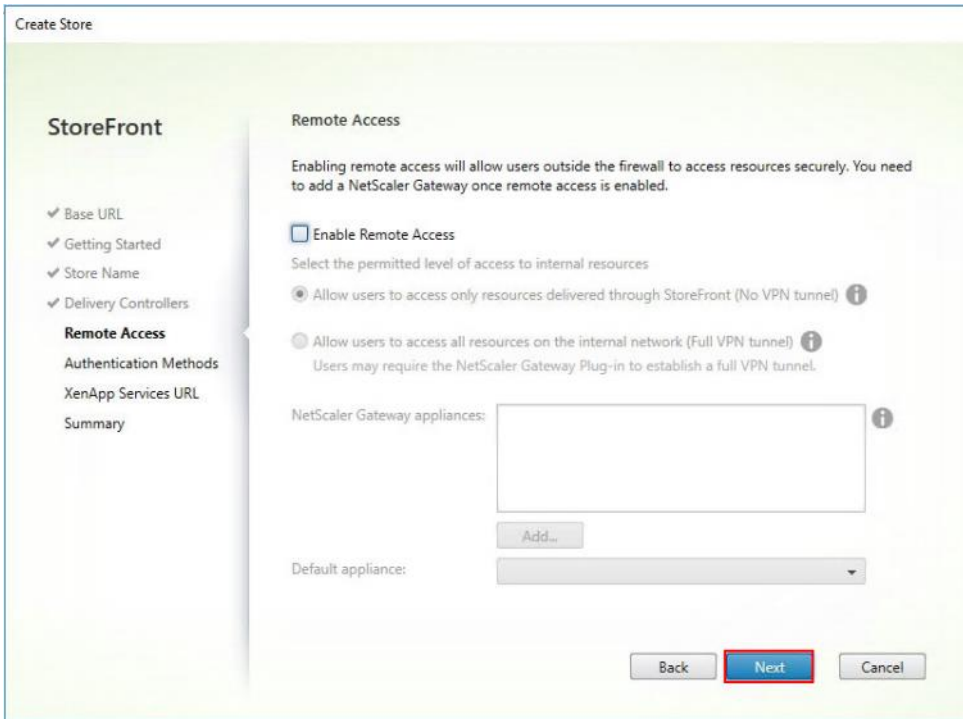
Specify the Citrix Virtual Apps and Desktops delivery controllers or XenApp servers for this store. Citrix recommends grouping delivery controllers based on deployments.

Name	Type	Servers
Controller	Citrix Virtual Apps and Desktops	10.10.30.230

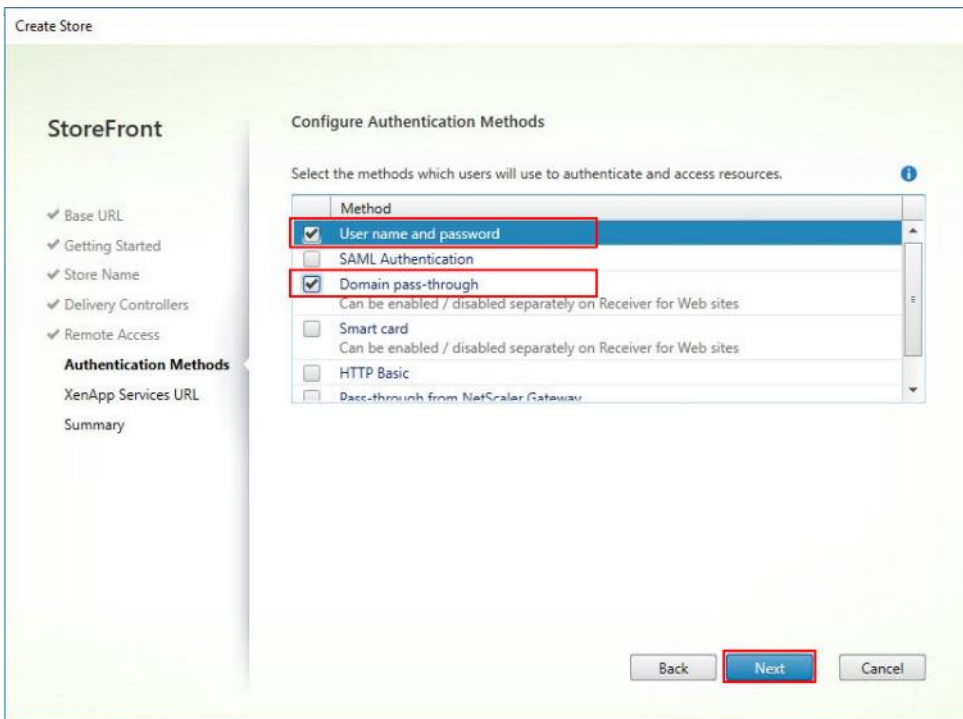
Add... Edit... Remove

Back Next Cancel

**Step 18.** Specify how connecting users can access the resources, in this environment only local users on the internal network are able to access the store and click **Next**.



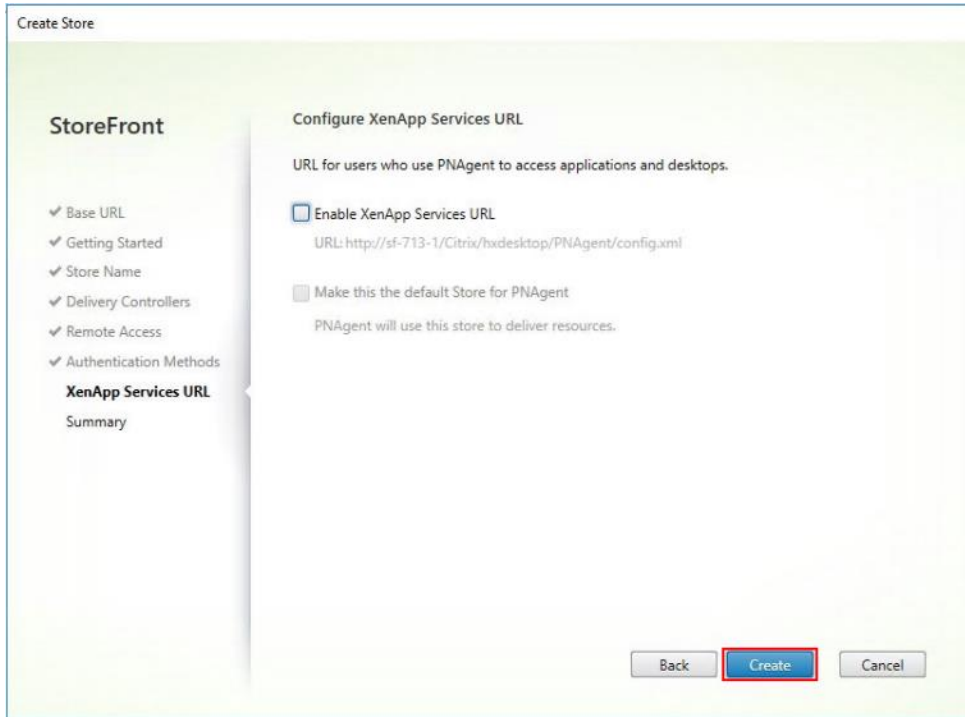
**Step 19.** On the “Authentication Methods” page, select the methods you’ll use to authenticate to the store and click **Next**. You can select from the following methods as shown below:



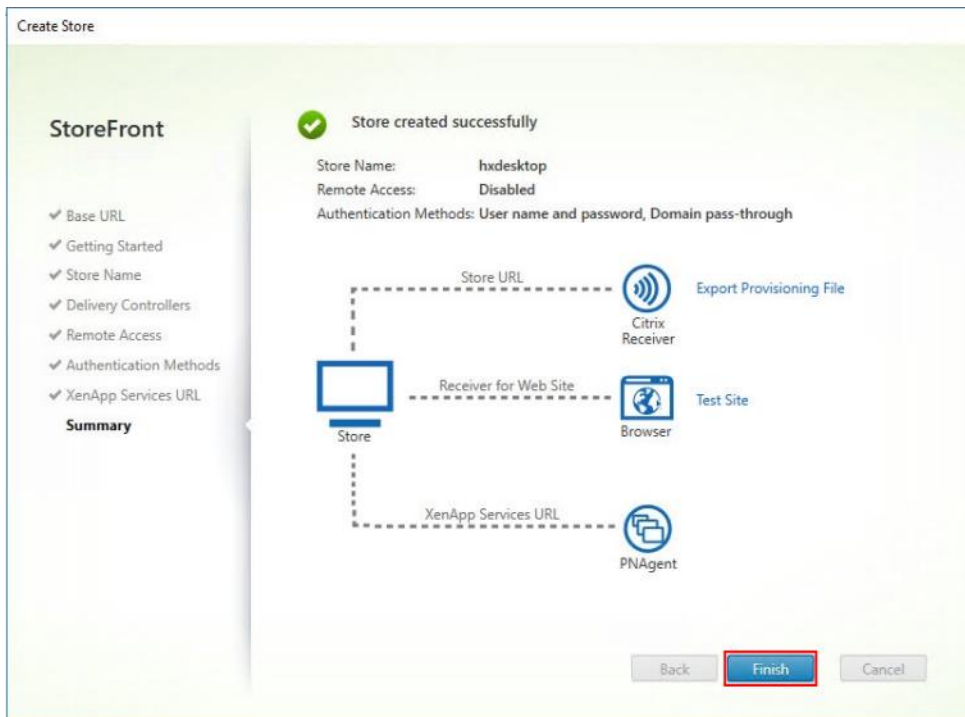
**Step 20.** Username and password: Users enter their credentials and are authenticated when they access their stores.

**Step 21.** Domain pass-through: Users authenticate to their domain-joined Windows computers and their credentials are used to log them on automatically when they access their stores.

**Step 22.** Configure the XenApp Service URL for users who use PNAgent to access the applications and desktops and click **Create**.



**Step 23.** After creating the store click **Finish**.



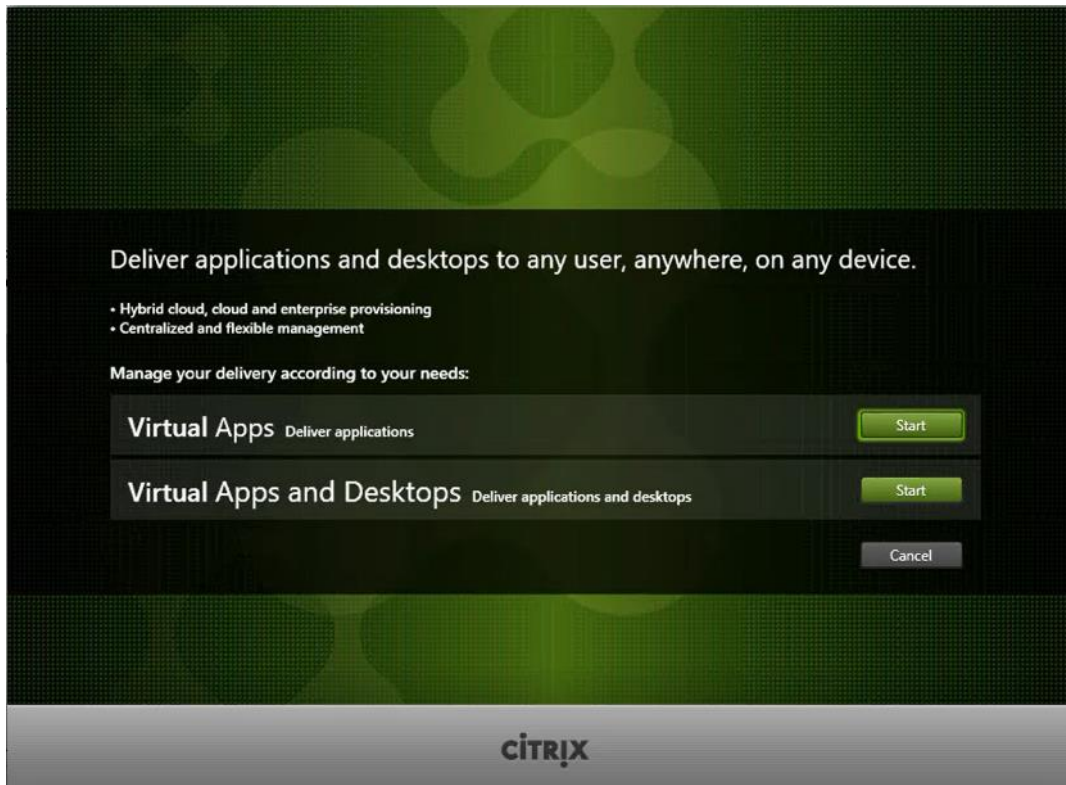


## Procedure 9. Additional StoreFront Configuration

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

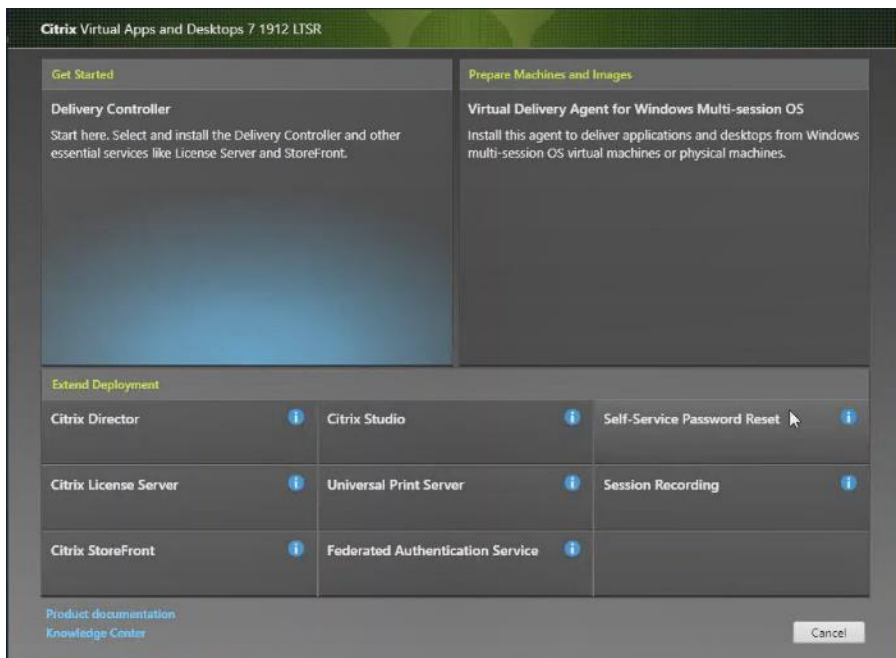
**Step 1.** To begin the installation of the second StoreFront, connect to the second StoreFront server and launch the installer from the Citrix VDI ISO.

**Step 2.** Click **Start**.



**Step 3.** Click **Extended Deployment Citrix StoreFront**.

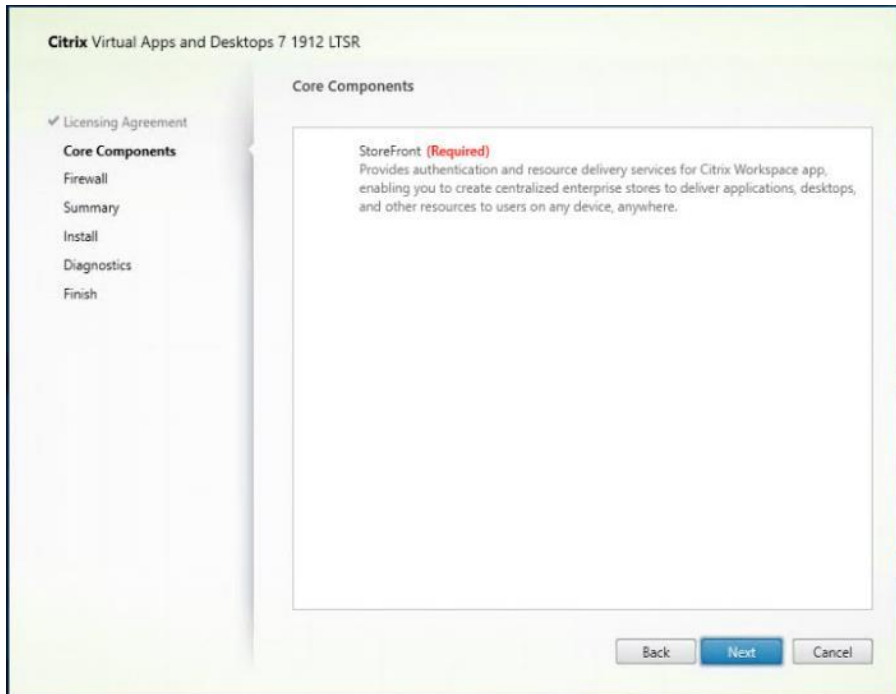




**Step 4.** Repeat steps 1-3 used to install the first StoreFront.

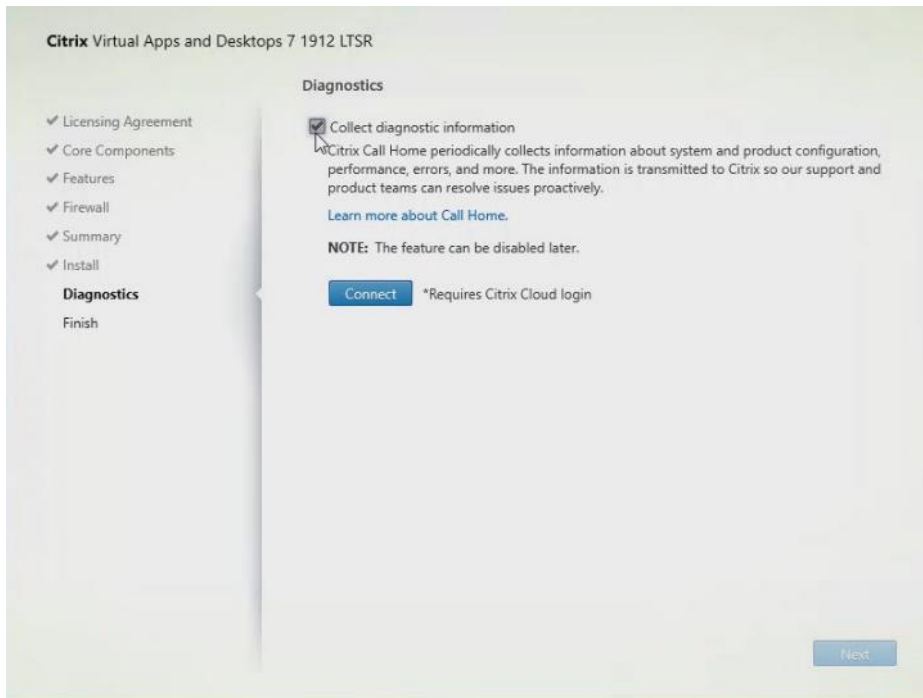
**Step 5.** Review the Summary configuration.

**Step 6.** Click **Install**.



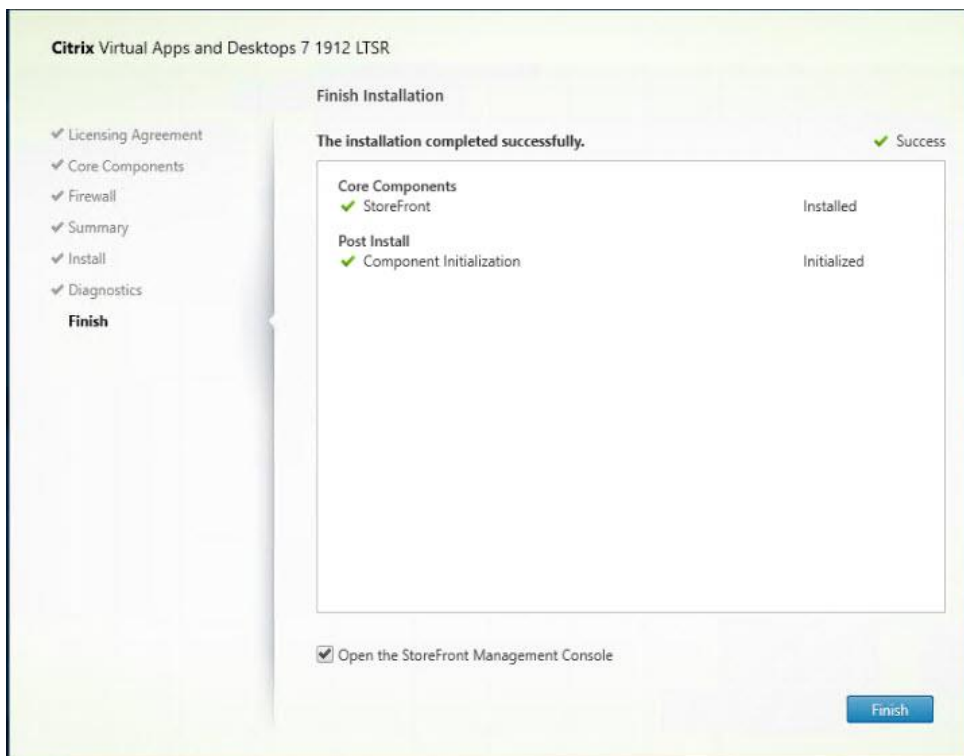
**Step 7.** (Optional) Click **Collect diagnostic information**.

**Step 8.** Click **Next**.



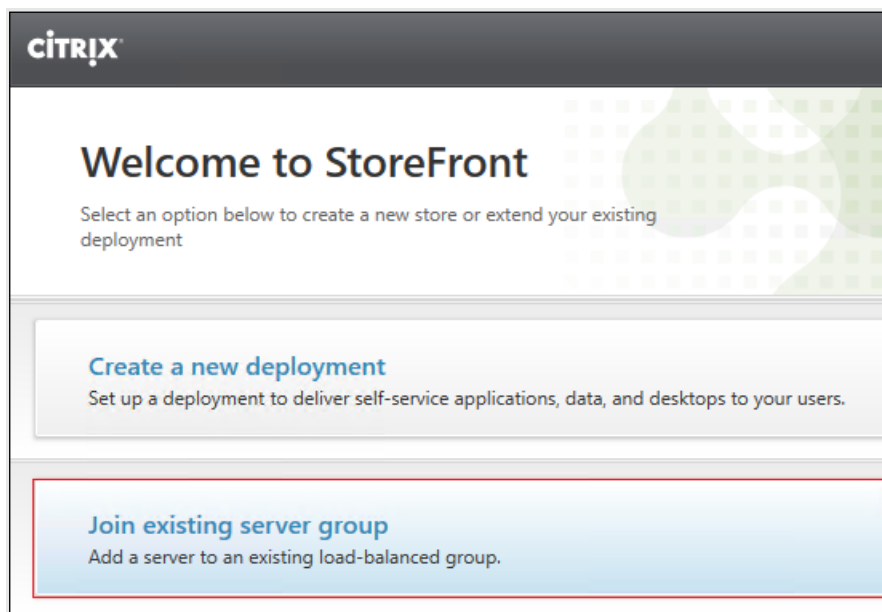
**Step 9.** Check **Open the StoreFront Management Console.**

**Step 10.** Click **Finish.**

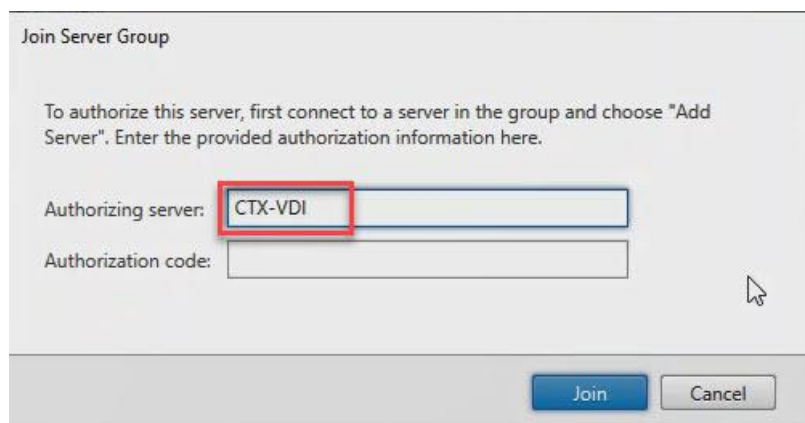


To configure the second StoreFront if used, follow these steps:

**Step 1.** From the StoreFront Console on the second server, select **Join existing server group**.



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

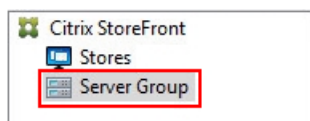


**Step 3.** Before the additional StoreFront server can join the server group, you must connect to the first Storefront server, add the second server, and obtain the required authorization information.

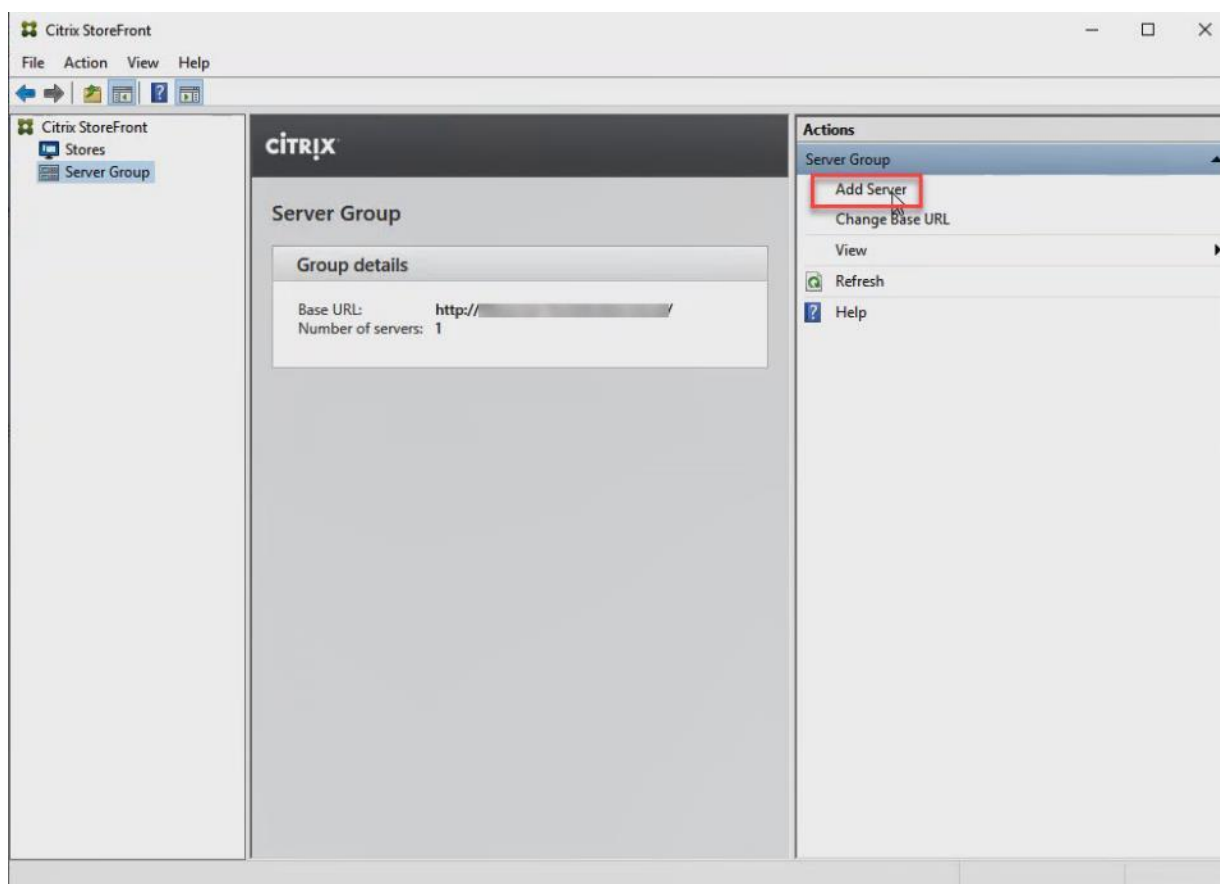
**Step 4.** Connect to the first StoreFront server.

**Step 5.** Using the StoreFront menu, you can scroll through the StoreFront management options.

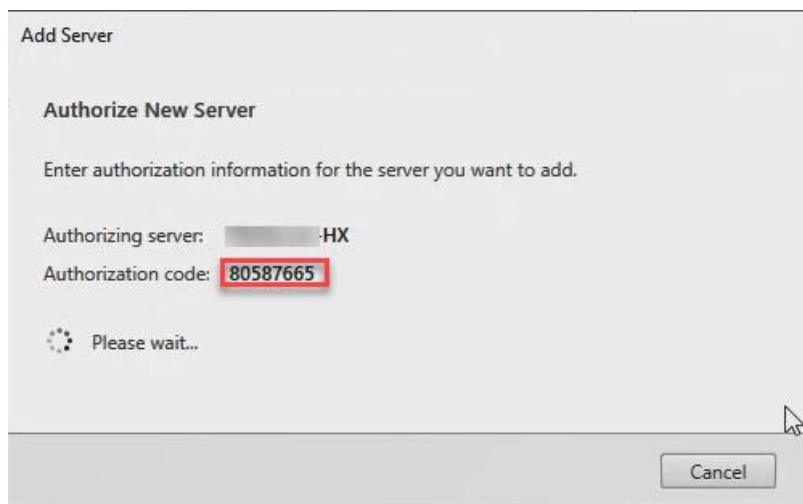
**Step 6.** Select **Server Group** from the menu.



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

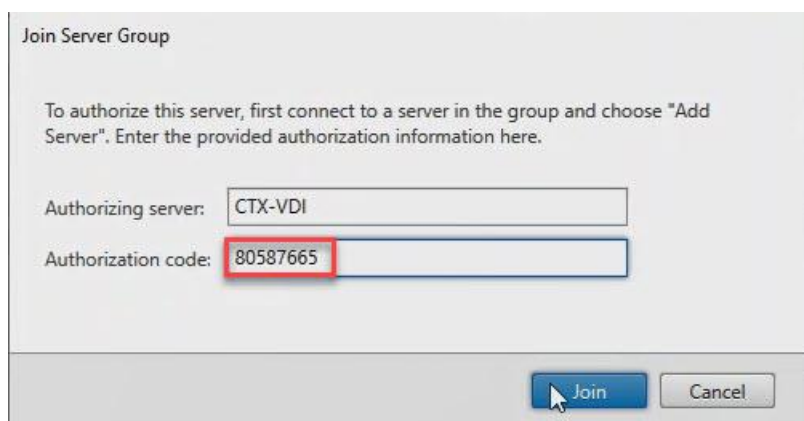


**Step 8.** Copy the Authorization code from the Add Server dialog.



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

**Step 10.** Click **Join**.



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

**Step 12.** Click **OK**.



The second StoreFront is now in the Server Group.

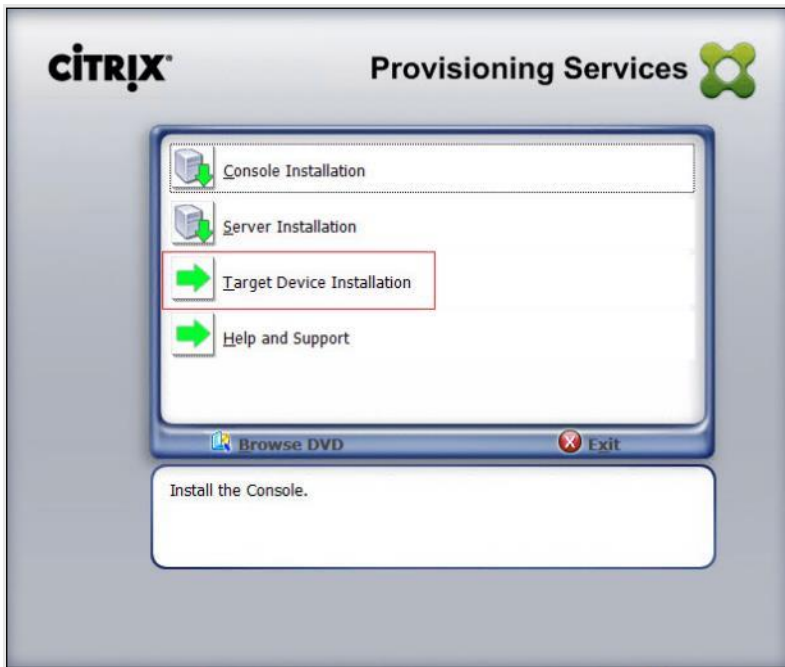
### **Procedure 10. Install the Citrix Provisioning Services Target Device Software**

For non-persistent Windows 10 virtual desktops and Server 2019 RDS virtual machines, Citrix Provisioning Services (PVS) is used for deployment. The Master Target Device refers to the target device from which a hard disk image is built and stored on a vDisk. Provisioning Services then streams the contents of the vDisk created to other target devices. This procedure installs the PVS Target Device software that is used to build the RDS and VDI golden images.

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

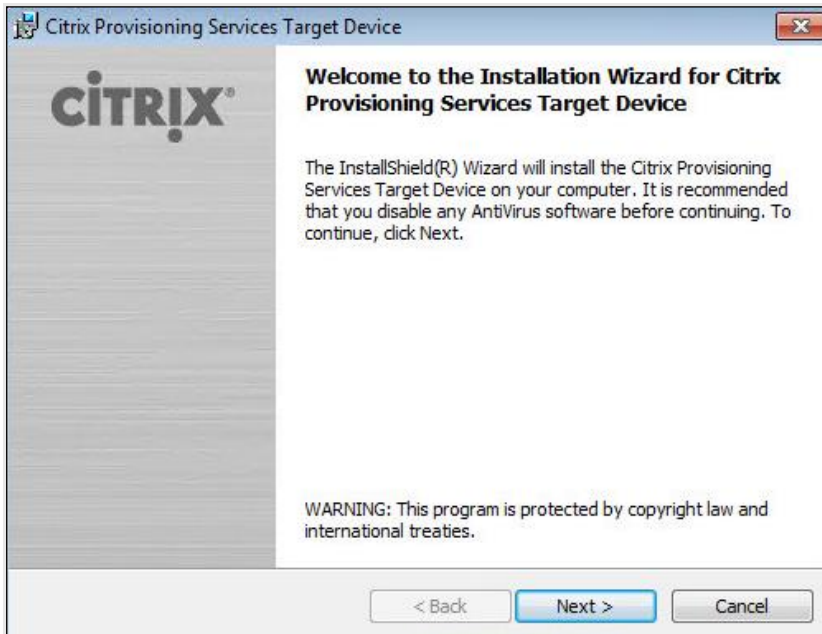
**Step 1.** On the Windows 10 Master Target Device, launch the **PVS installer** from the Provisioning Services ISO.

**Step 2.** Click **Target Device Installation**.



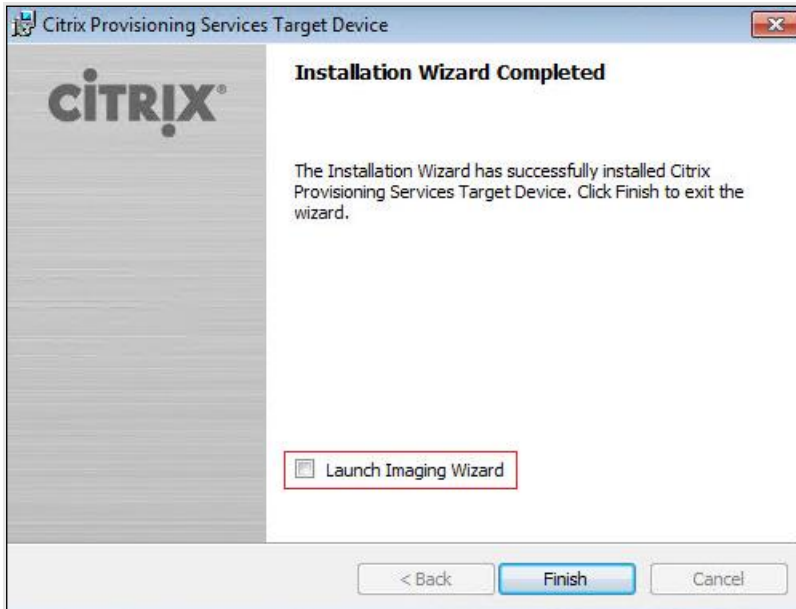
**Note:** The installation wizard will check to resolve dependencies and then begin the PVS target device installation process.

**Step 3.** Click **Next**.



**Step 4.** Confirm the installation settings and click **Install**.

**Step 5.** Deselect the checkbox to launch the Imaging Wizard and click **Finish**.



**Step 6.** Reboot the machine.

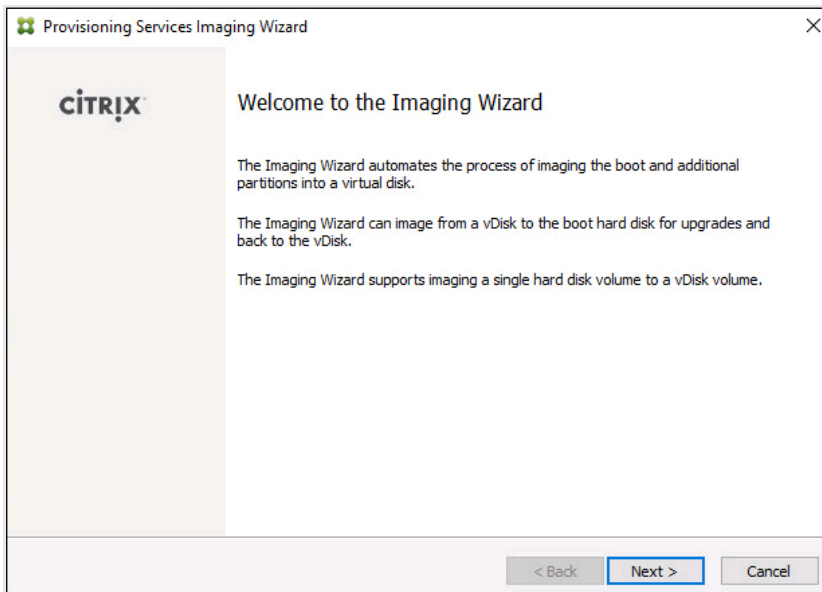
### Procedure 11. Create Citrix Provisioning Services vDisks

The PVS Imaging Wizard automatically creates a base vDisk image from the master target device.

**Note:** The following procedure explains how to create a vDisk for VDI desktops. When you have completed these steps, repeat the procedure to build a vDisk for RDS.

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

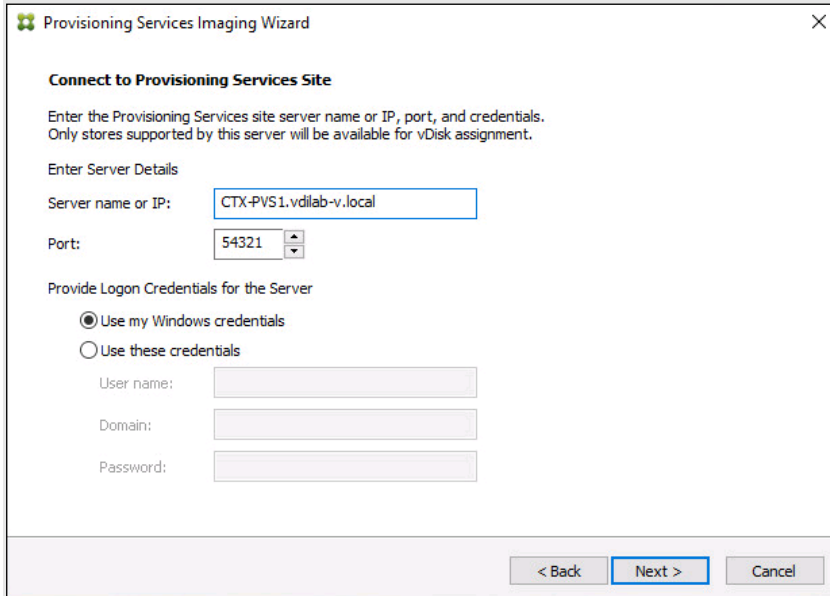
**Step 2.** Click **Next**.



**Step 3.** The Connect to Farm page appears. Enter the name or IP address of a Provisioning Services 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.

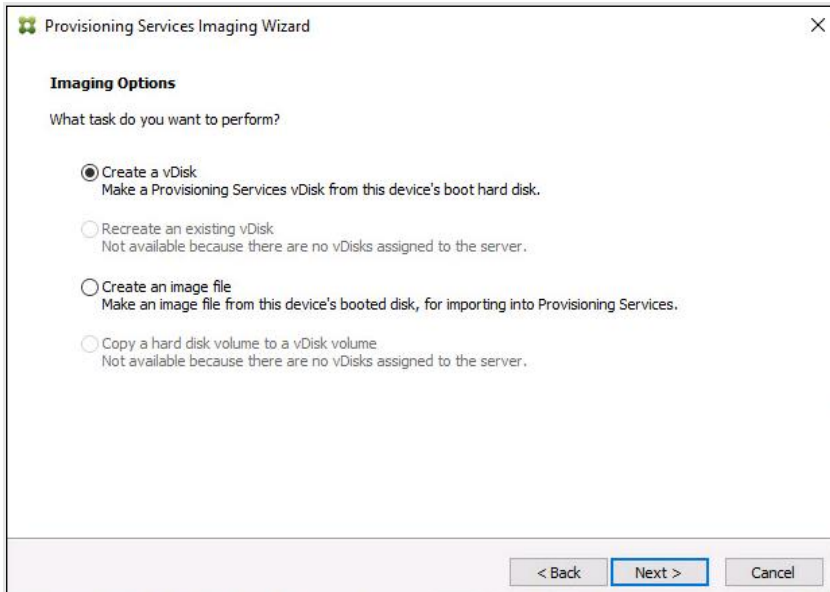
**Step 5.** Click **Next**.



The screenshot shows the 'Provisioning Services Imaging Wizard' window. The title bar includes a close button (X). The main heading is 'Connect to Provisioning Services Site'. Below this, there is a sub-heading: 'Enter the Provisioning Services site server name or IP, port, and credentials. Only stores supported by this server will be available for vDisk assignment.' The 'Enter Server Details' section contains three input fields: 'Server name or IP:' with the text 'CTX-PVS1.vdlib-v.local', 'Port:' with a dropdown menu showing '54321', and 'Provide Logon Credentials for the Server' with two radio buttons. The first radio button, 'Use my Windows credentials', is selected. Below these are three empty text boxes for 'User name:', 'Domain:', and 'Password:'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

**Step 6.** Click **Create new vDisk**.

**Step 7.** Click **Next**.



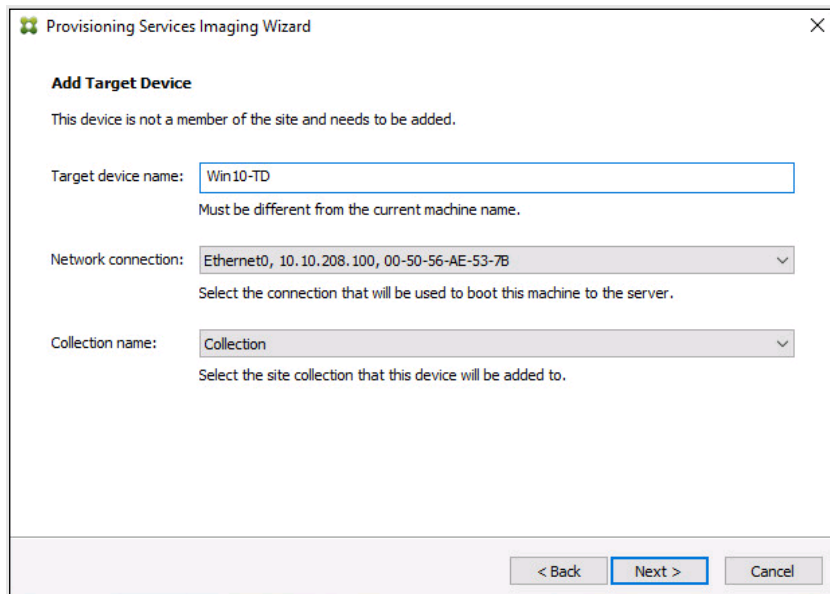
The screenshot shows the 'Provisioning Services Imaging Wizard' window. The title bar includes a close button (X). The main heading is 'Imaging Options'. Below this is the question 'What task do you want to perform?'. There are four radio button options: 1) 'Create a vDisk' (selected) with the sub-text 'Make a Provisioning Services vDisk from this device's boot hard disk.' 2) 'Recreate an existing vDisk' with the sub-text 'Not available because there are no vDisks assigned to the server.' 3) 'Create an image file' with the sub-text 'Make an image file from this device's booted disk, for importing into Provisioning Services.' 4) 'Copy a hard disk volume to a vDisk volume' with the sub-text 'Not available because there are no vDisks assigned to the server.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

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**.

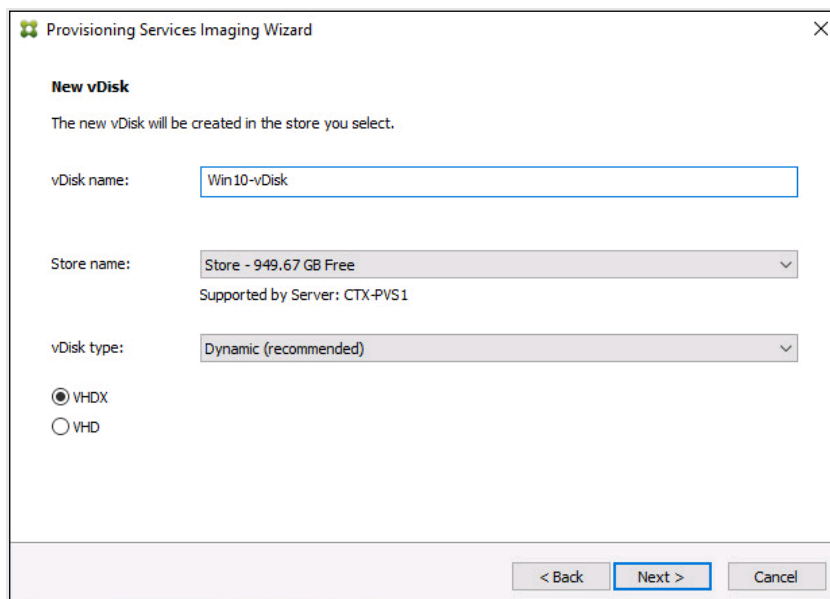


The screenshot shows the 'Add Target Device' step of the Provisioning Services Imaging Wizard. The dialog box has a title bar with a close button (X) and a green icon. The main content area is titled 'Add Target Device' and contains the following text: 'This device is not a member of the site and needs to be added.' Below this, there are three input fields: 'Target device name:' with the value 'Win10-TD' and a note 'Must be different from the current machine name.'; 'Network connection:' with a dropdown menu showing 'Ethernet0, 10.10.208.100, 00-50-56-AE-53-7B' and a note 'Select the connection that will be used to boot this machine to the server.'; and 'Collection name:' with a dropdown menu showing 'Collection' and a note 'Select the site collection that this device will be added to.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

**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. (This CVD used Dynamic rather than Fixed vDisks.)

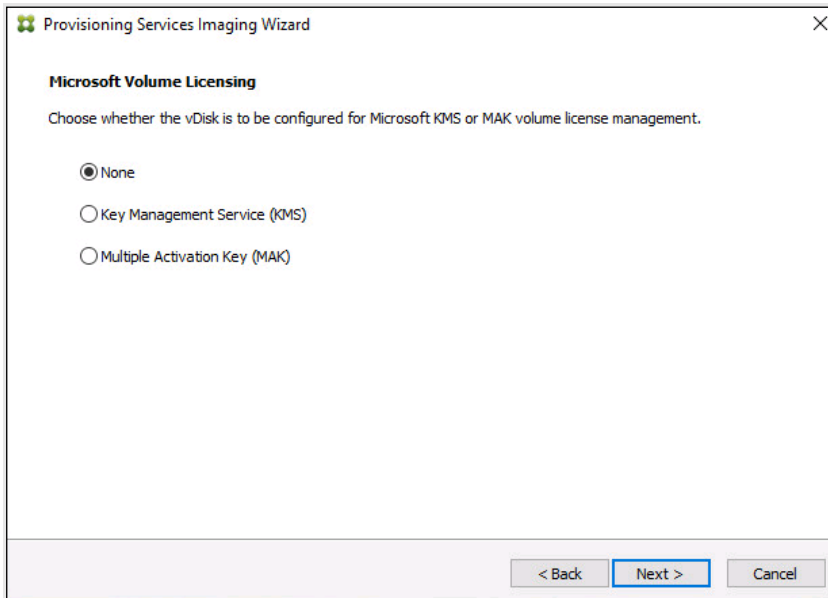
**Step 12.** Click **Next**.



The screenshot shows the 'New vDisk' step of the Provisioning Services Imaging Wizard. The dialog box has a title bar with a close button (X) and a green icon. The main content area is titled 'New vDisk' and contains the following text: 'The new vDisk will be created in the store you select.' Below this, there are three input fields: 'vDisk name:' with the value 'Win10-vDisk'; 'Store name:' with a dropdown menu showing 'Store - 949.67 GB Free' and a note 'Supported by Server: CTX-PVS1'; and 'vDisk type:' with a dropdown menu showing 'Dynamic (recommended)'. Below the dropdowns, there are two radio buttons: 'VHDX' (selected) and 'VHD'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

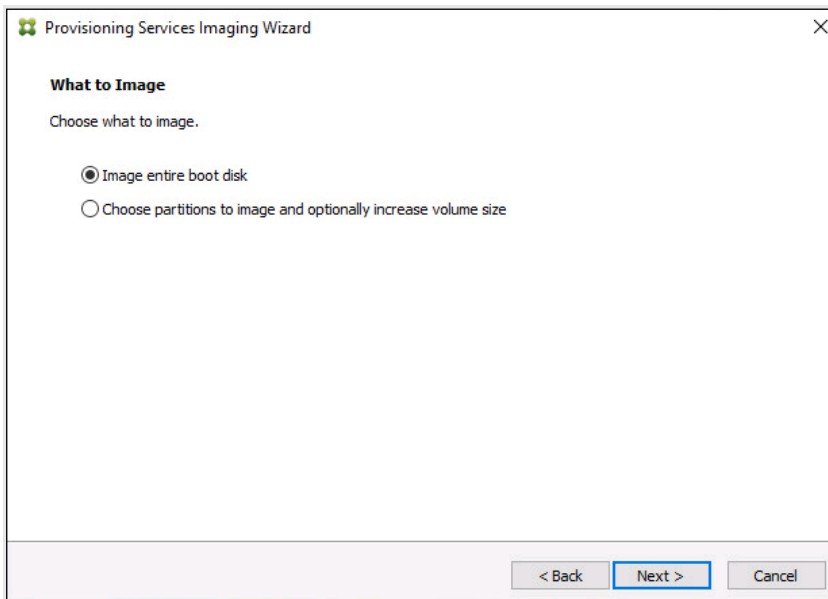
**Step 13.** On the Microsoft Volume Licensing page, select the volume license option to use for target devices. For this CVD, volume licensing is not used, so the None is selected.

**Step 14.** Click **Next**.



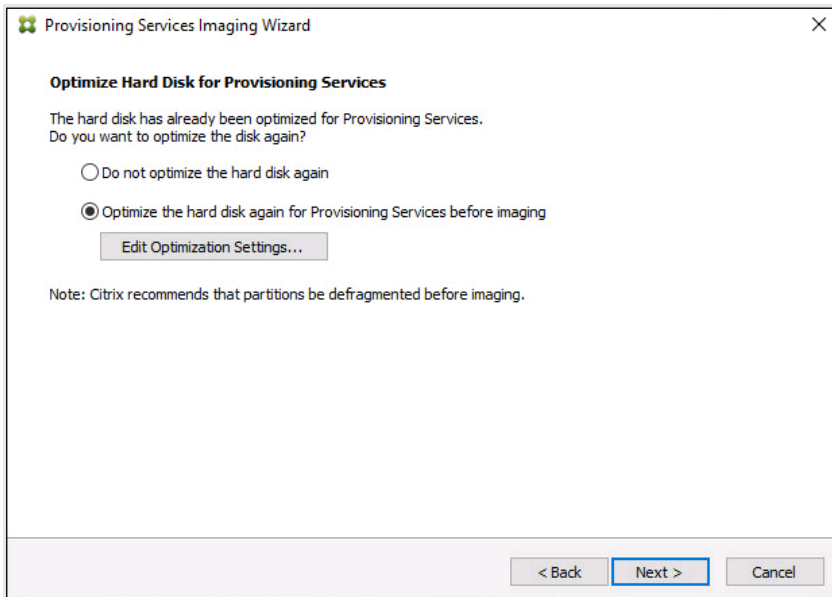
**Step 15.** Select **Image entire boot disk** on the Configure Image Volumes page.

**Step 16.** Click **Next**.

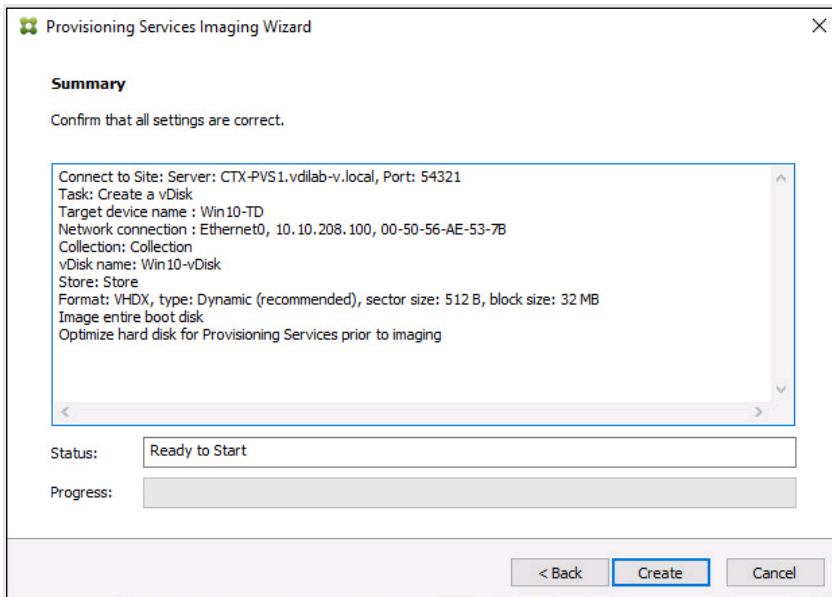


**Step 17.** Select **Optimize for hard disk again for Provisioning Services before imaging** on the Optimize Hard Disk for Provisioning Services.

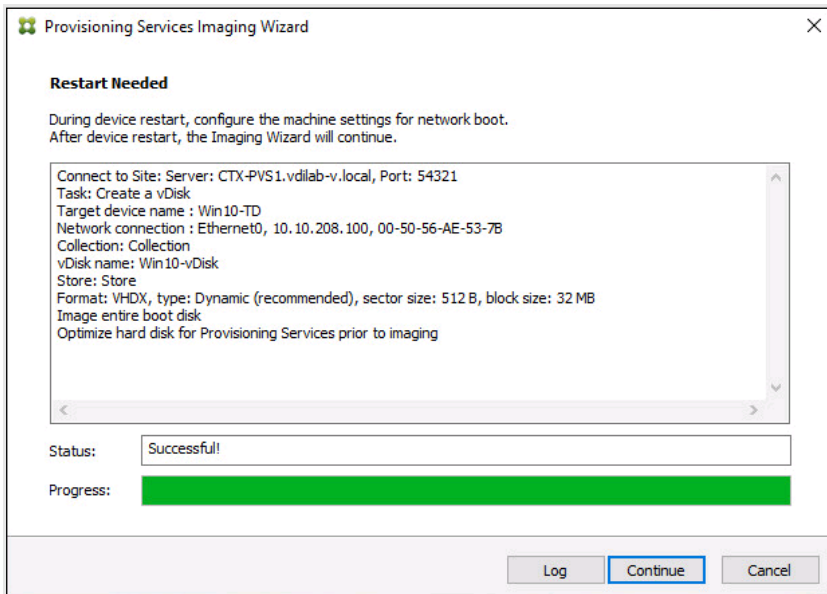
**Step 18.** Click **Next**.



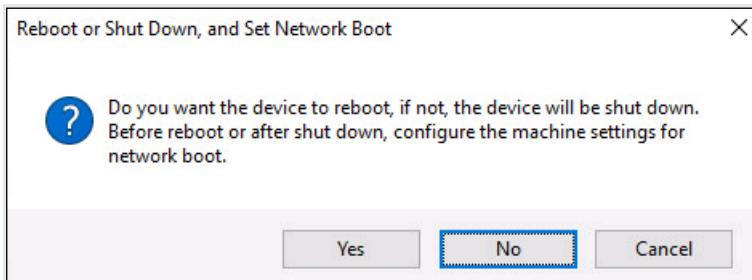
**Step 19.** Click **Create** on the Summary page.



**Step 20.** Review the configuration and click **Continue**.

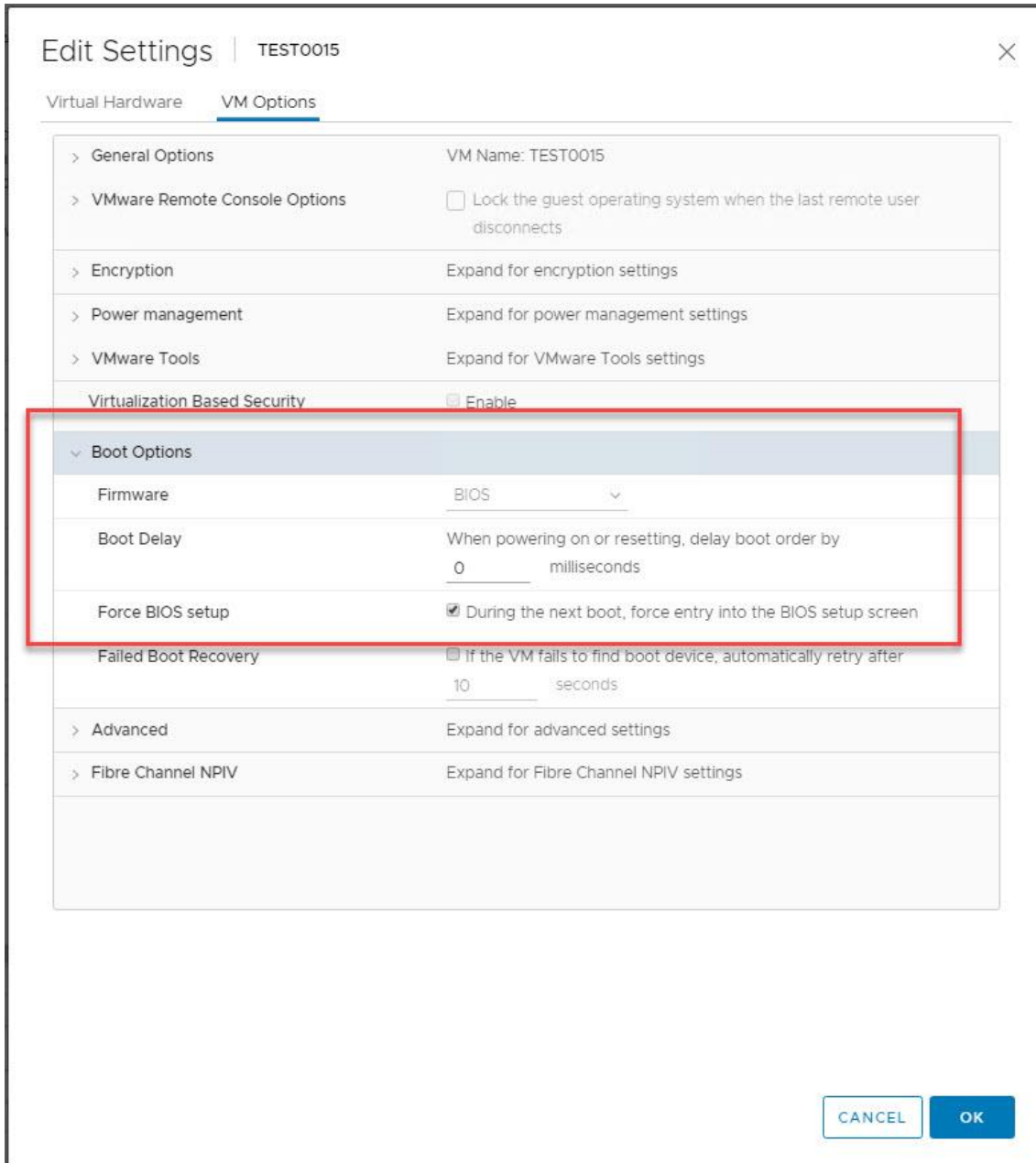


**Step 21.** When prompted, click **No** to shut down the machine.



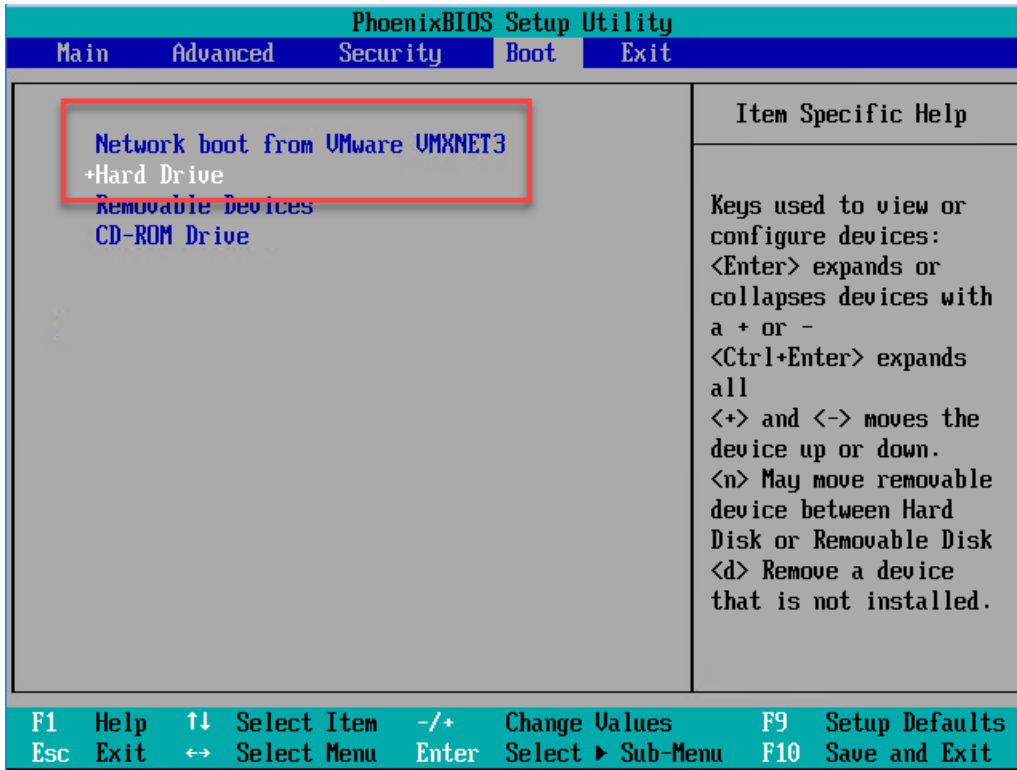
**Step 22.** Edit the virtual machine settings and select **Boot Options** under VM Options.

**Step 23.** Click **Force BIOS setup** and click **OK**.



**Step 24.** Restart the Virtual Machine.

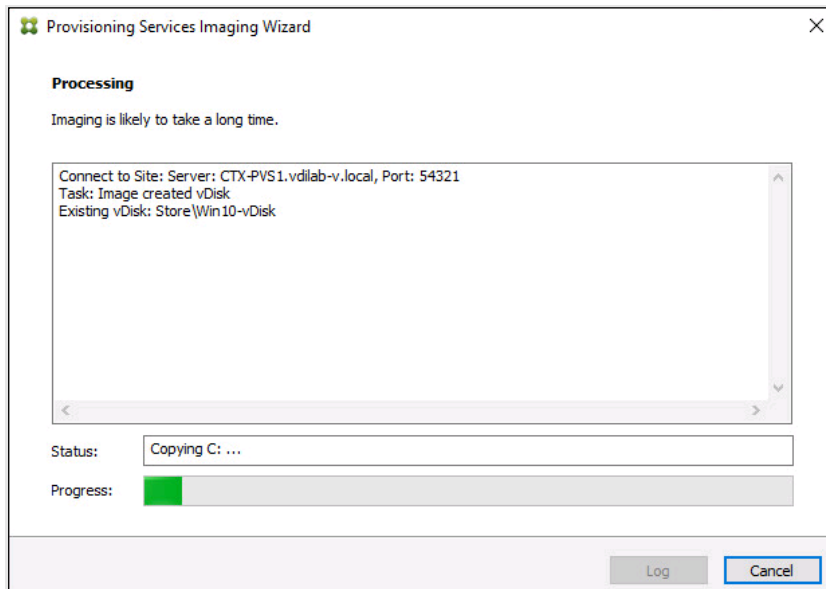
**Step 25.** When the VM boots into the BIOS, go to the Boot menu to move the Network boot from VMware VMXNET3 to the top of the list.



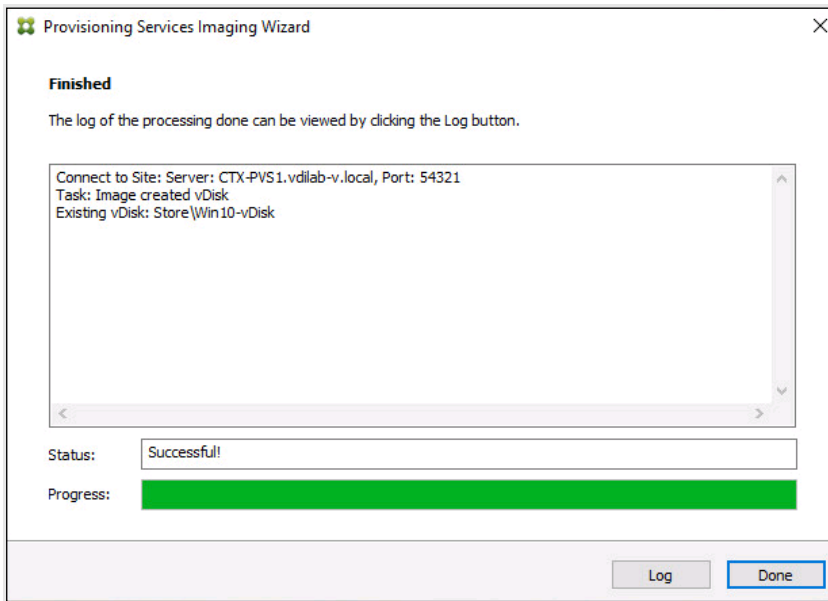
**Step 26.** Restart the Virtual Machine.

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

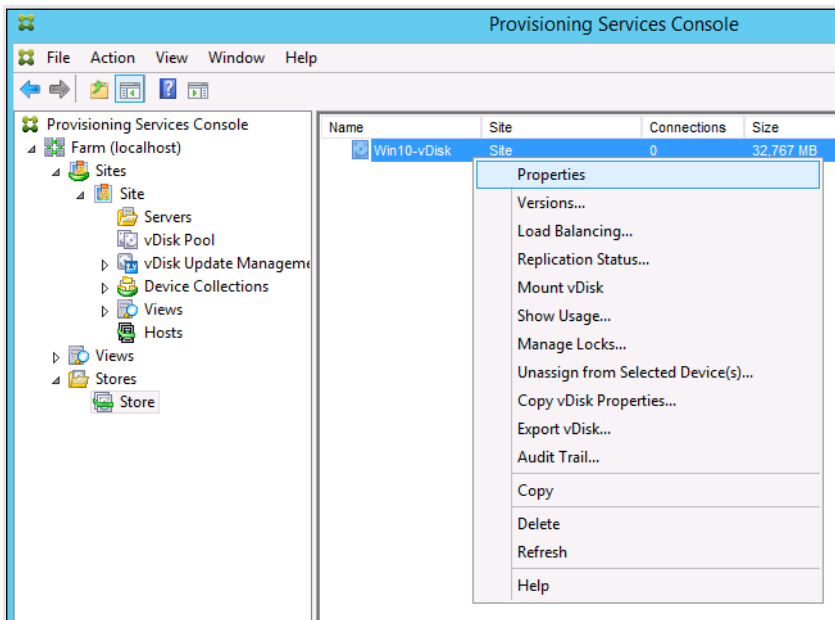
**Step 27.** If prompted to Restart select **Restart Later**.



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



- Step 29.** Shutdown the virtual machine used for the VDI or RDS master target.
- Step 30.** Connect to the PVS server and validate that the vDisk image is available in the Store.
- Step 31.** Right-click the newly created vDisk and select **Properties**.



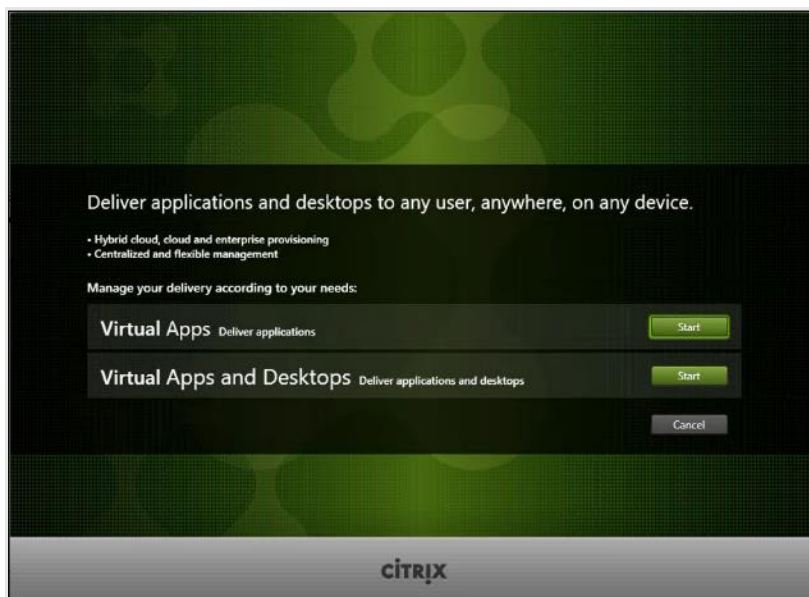
- Step 32.** On the vDisk Properties dialog, change Access mode to **Private mode** so the Citrix Virtual Desktop Agent can be installed.

**Procedure 12.** Install Citrix Virtual Apps and Desktop Virtual Desktop Agents

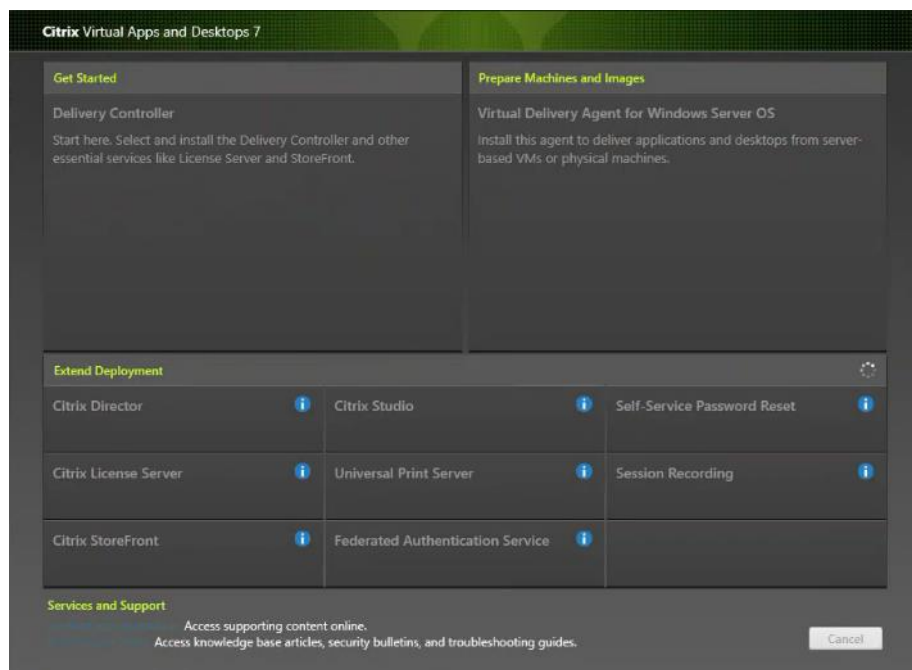
Virtual Delivery Agents (VDAs) are installed on the server and workstation operating systems and enable connections for desktops and apps. The following procedure was used to install VDAs for both HVD and HSD environments.

**Step 1.** Launch the **Citrix Desktop installer** from the CVA Desktop 7 LTSR ISO.

**Step 2.** Click **Start** on the Welcome Screen.



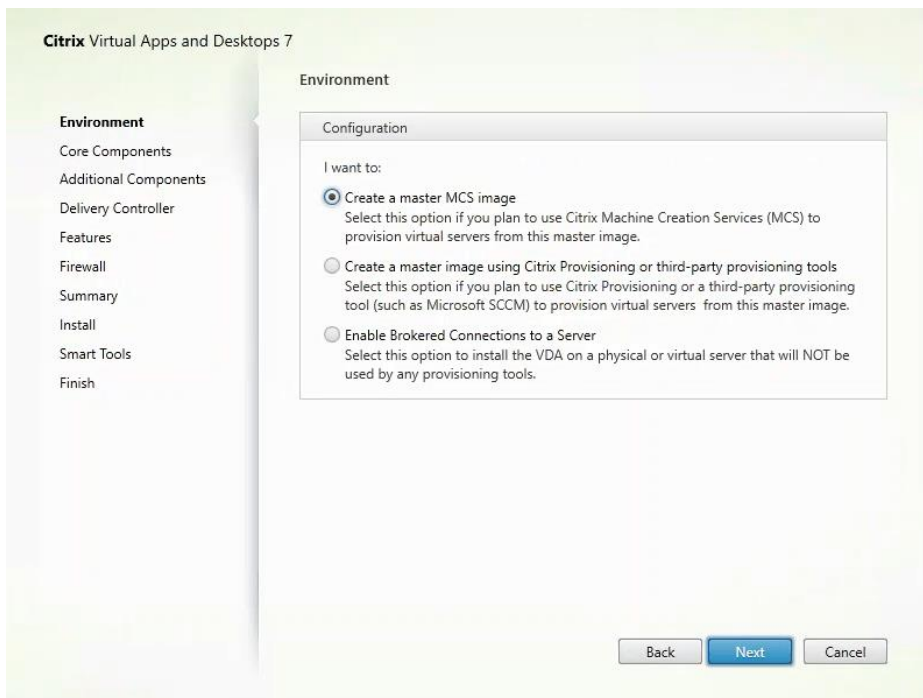
**Step 3.** To install the VDA for the Hosted Virtual Desktops (VDI), select **Virtual Delivery Agent for Windows Desktop OS**. After the VDA is installed for Hosted Virtual Desktops, repeat the procedure to install the VDA for Hosted Shared Desktops (RDS). In this case, select Virtual Delivery Agent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



**Step 4.** Select **Create a Master Image**. Be sure to select the proper provisioning technology.

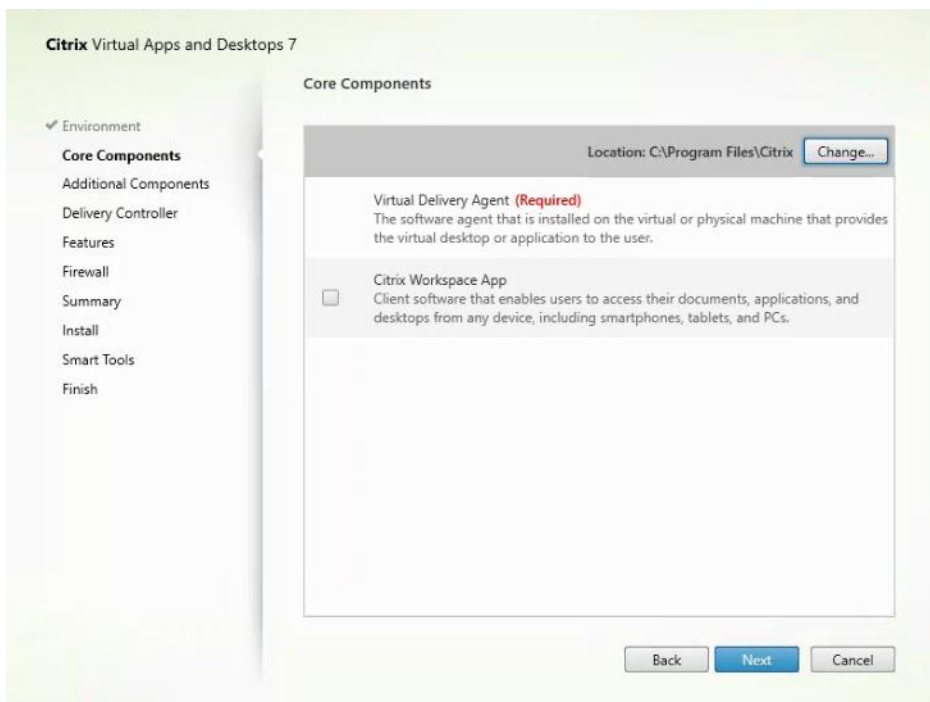
**Step 5.** Click **Next**.



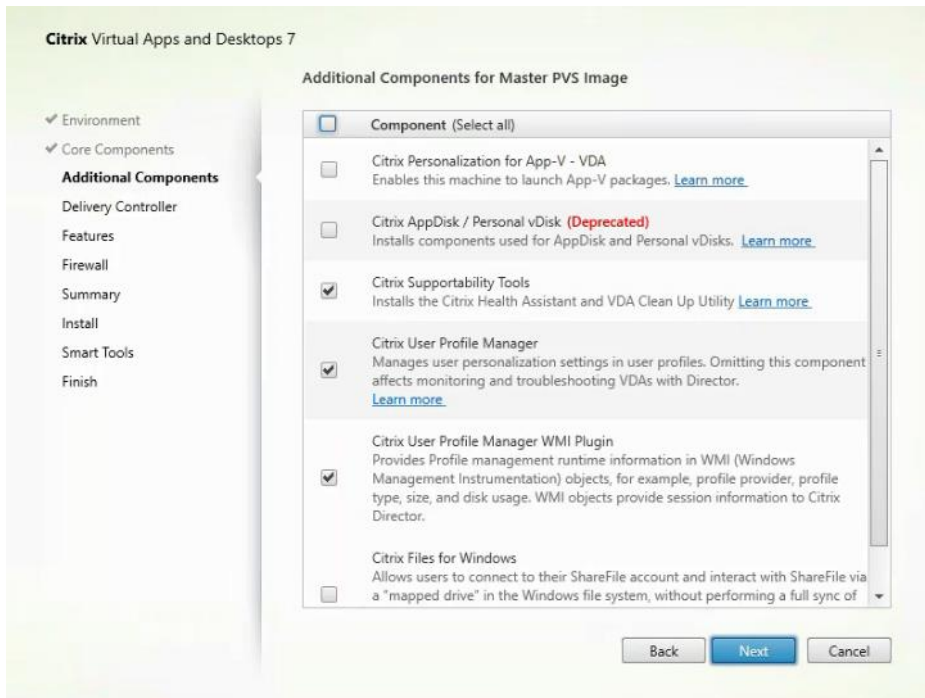


**Step 6.** Optional: Select **Citrix Workspace App**.

**Step 7.** Click **Next**.

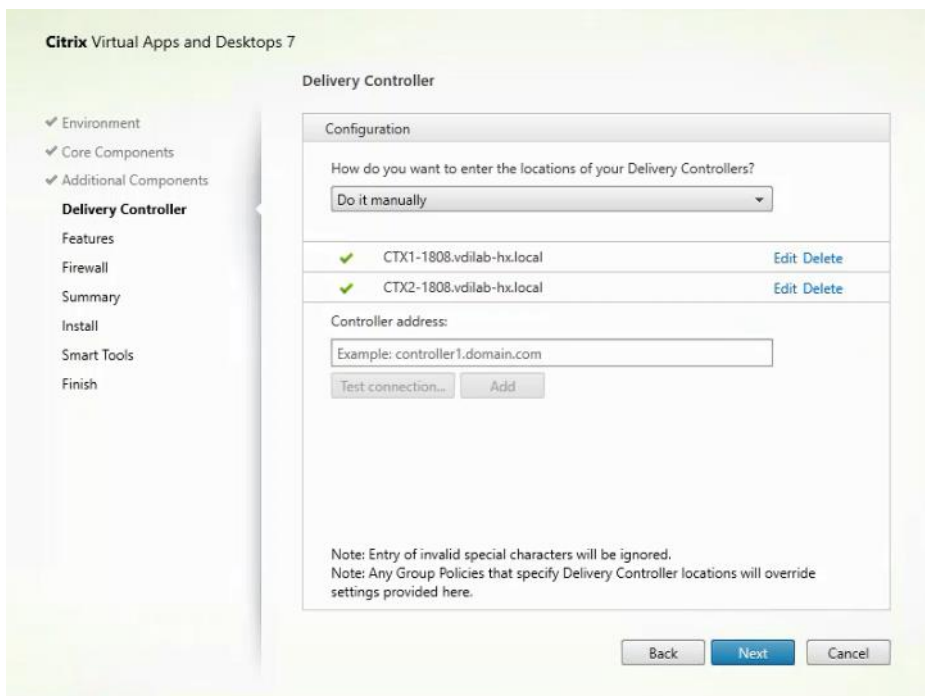


**Step 8.** Click **Next**.



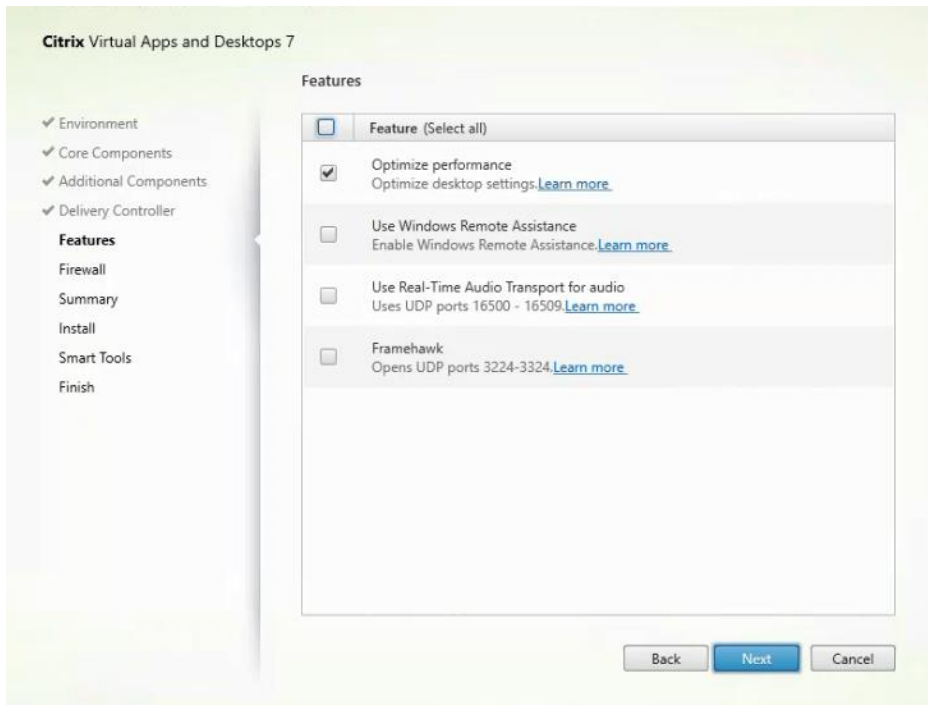
**Step 9.** Select **Do it manually** and specify the FQDN of the Delivery Controllers.

**Step 10.** Click **Next**.



**Step 11.** Accept the default features.

**Step 12.** Click **Next**.

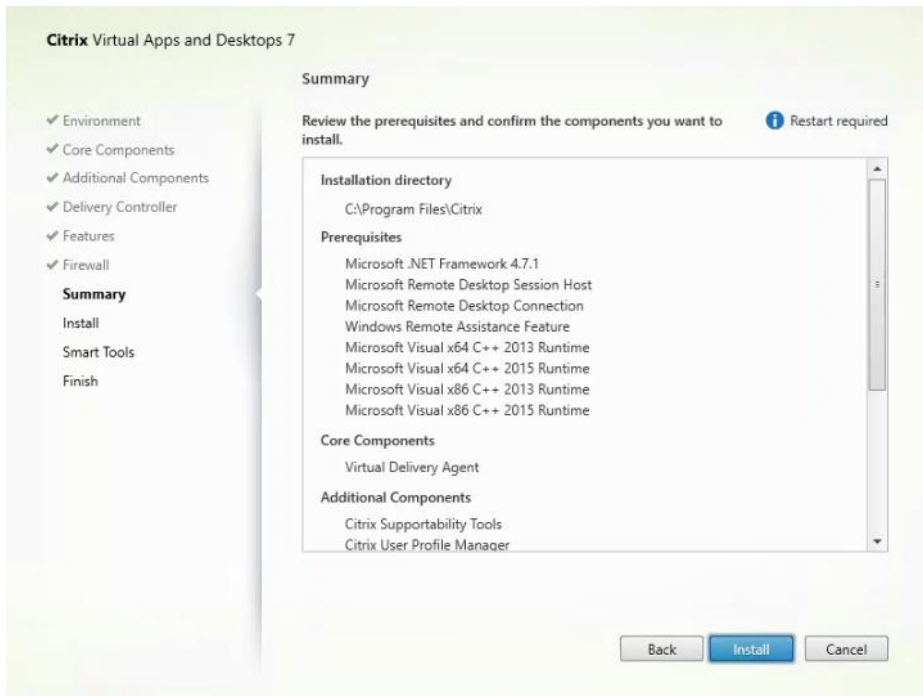


**Step 13.** Allow the firewall rules to be configured automatically.

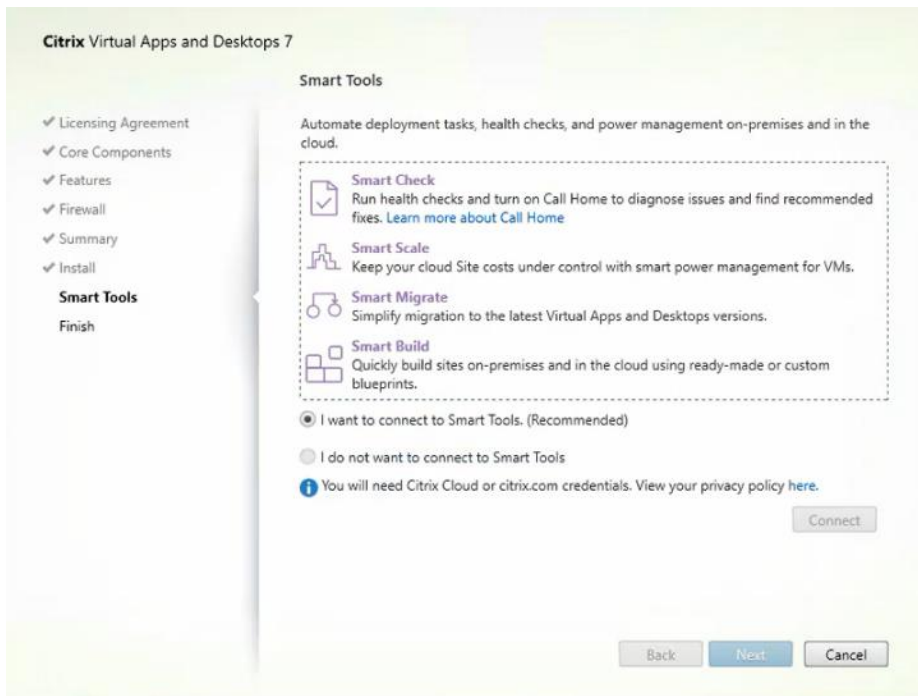
**Step 14.** Click **Next**.



**Step 15.** Verify the Summary and click **Install**.



**Step 16.** (Optional) Select **Call Home participation**.

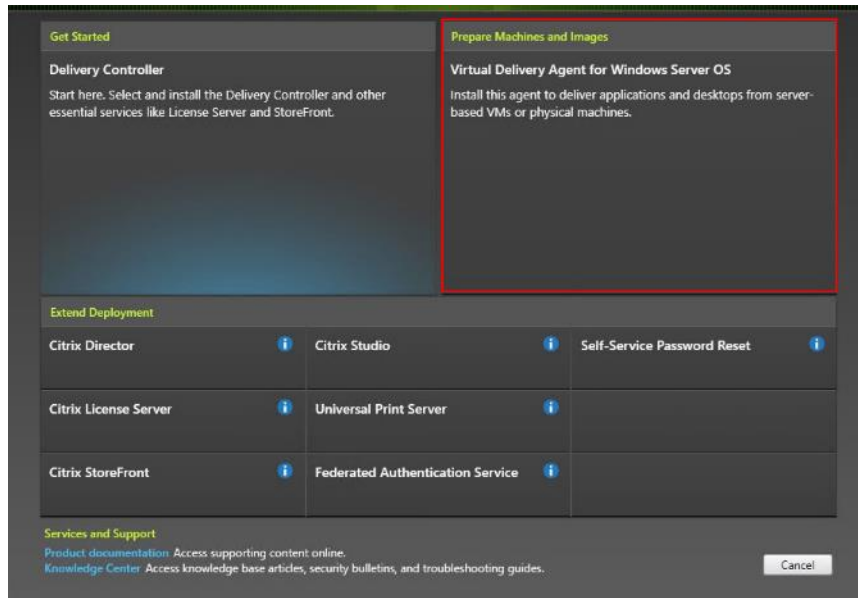


**Step 17.** (Optional) Click **Restart Machine**.

**Step 18.** Click **Finish**.

**Step 19.** Repeat steps 1-18 so that VDAs are installed for both HVD (using the Windows 10 OS image) and the HSD desktops (using the Windows Server 2019 image).

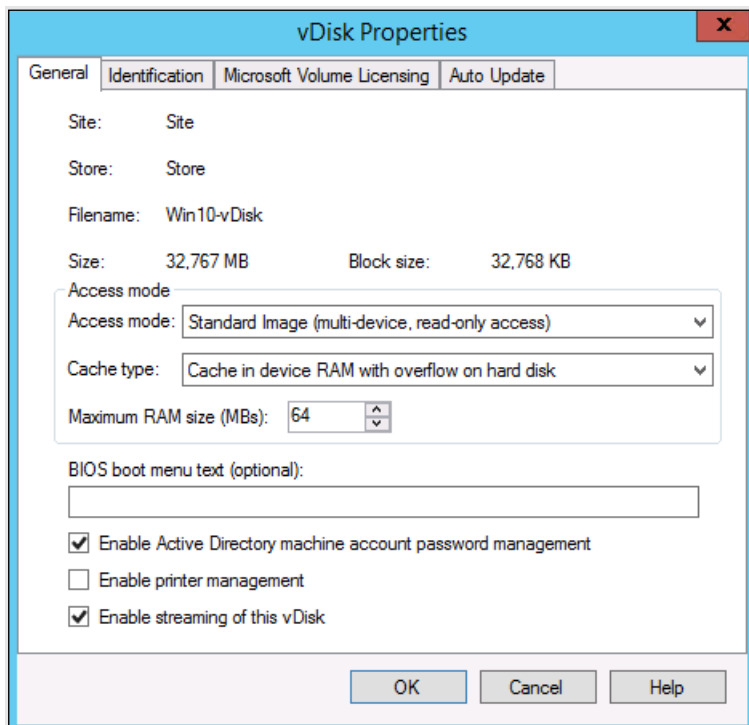
**Step 20.** Select an appropriate workflow for the HSD desktop.



**Step 21.** When the Citrix VDA is installed, on the vDisk Properties dialog, change Access mode to Standard Image (multi-device, read-only access).

**Step 22.** Set the Cache Type to **Cache in device RAM with overflow on hard disk**.

**Step 23.** Set Maximum RAM size (MBs): 256 for VDI and set 1024 MB for RDS vDisk.

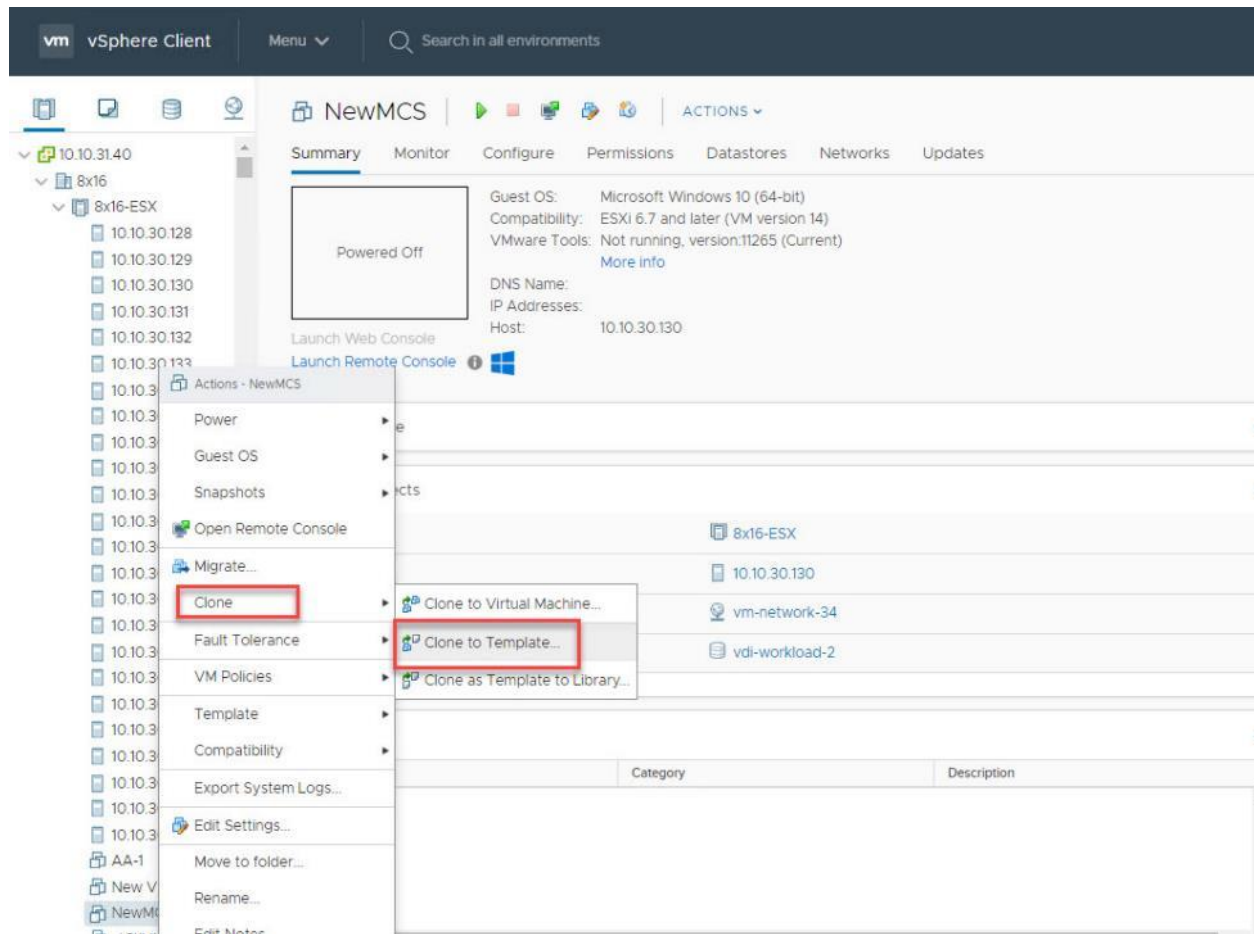


**Step 24.** Click **OK**.

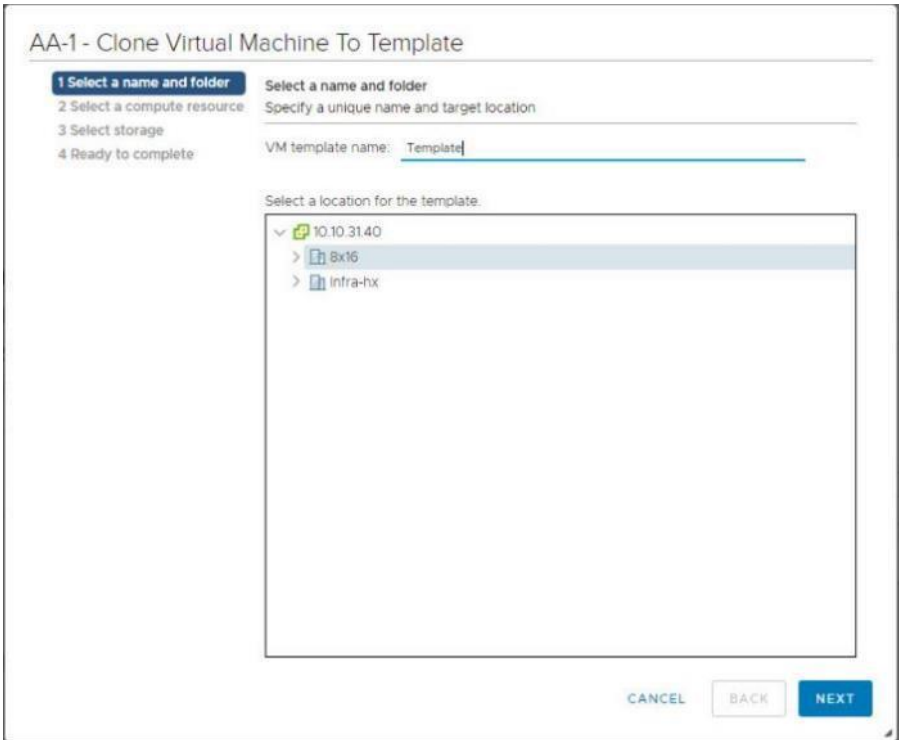
**Note:** Repeat steps 1-23 to create vDisks for both the Hosted VDI Desktops (using the Windows 10 OS image) and the Hosted Shared Desktops (using the Windows Server 2019 image).

### Procedure 13. Provision Virtual Desktop Machines

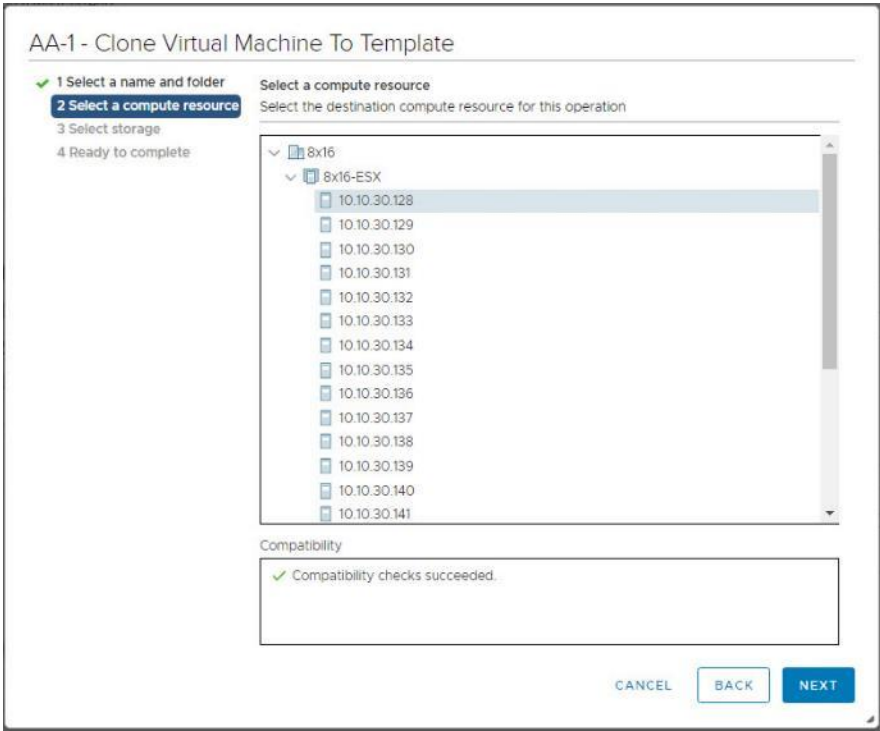
- Step 1.** Select the Master Target Device virtual machine from the VCenter Client.
- Step 2.** Right-click the virtual machine and go to **Clone -> Clone to Template**.
- Step 3.** Name the clone template.
- Step 4.** Select the cluster and datastore where the first phase of provisioning will occur.



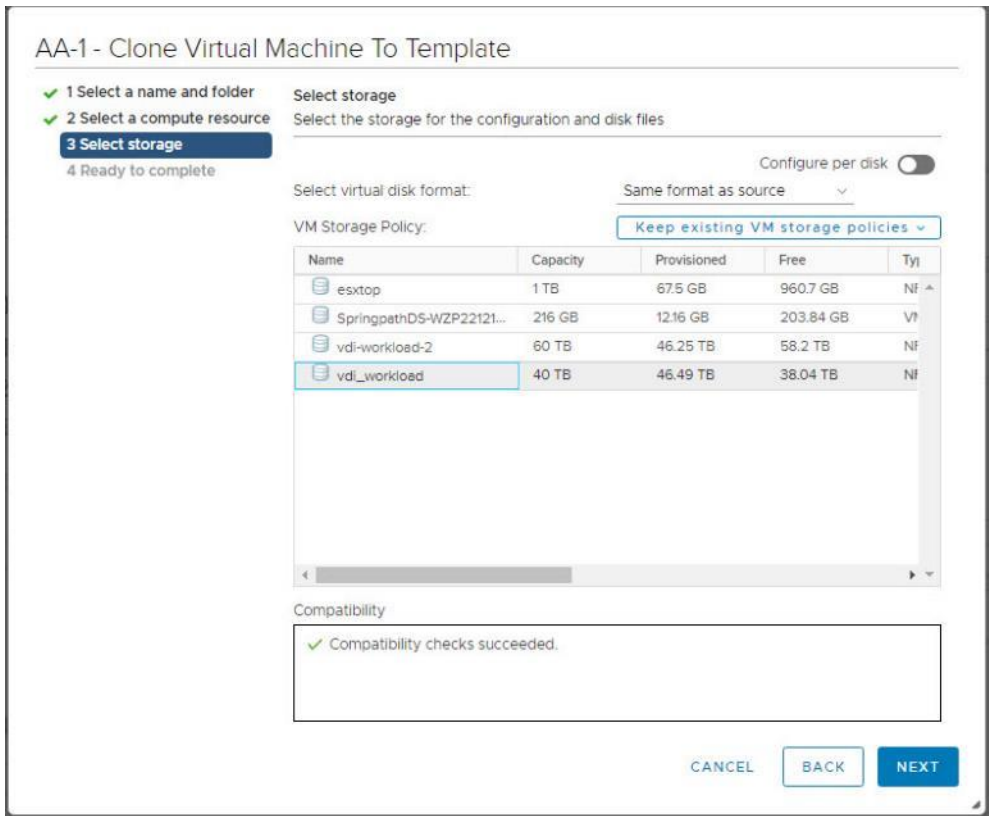
- Step 5.** Name the template and click **Next**.



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

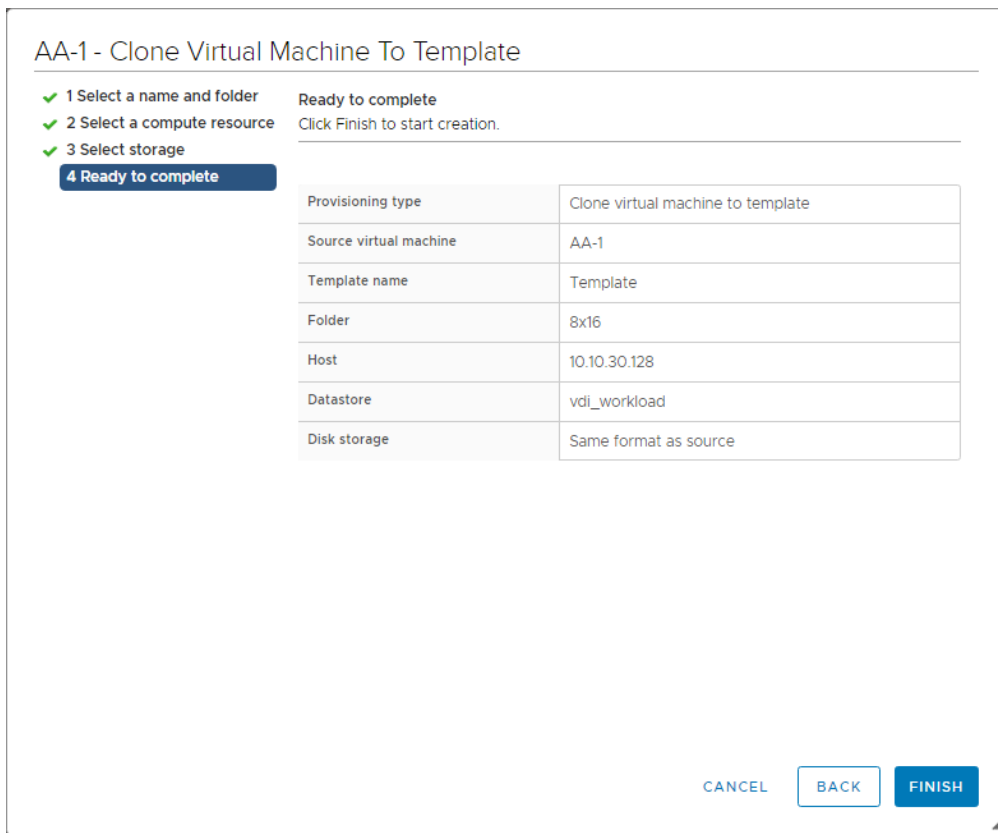


**Step 7.** Click **Next** after selecting a datastore.



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

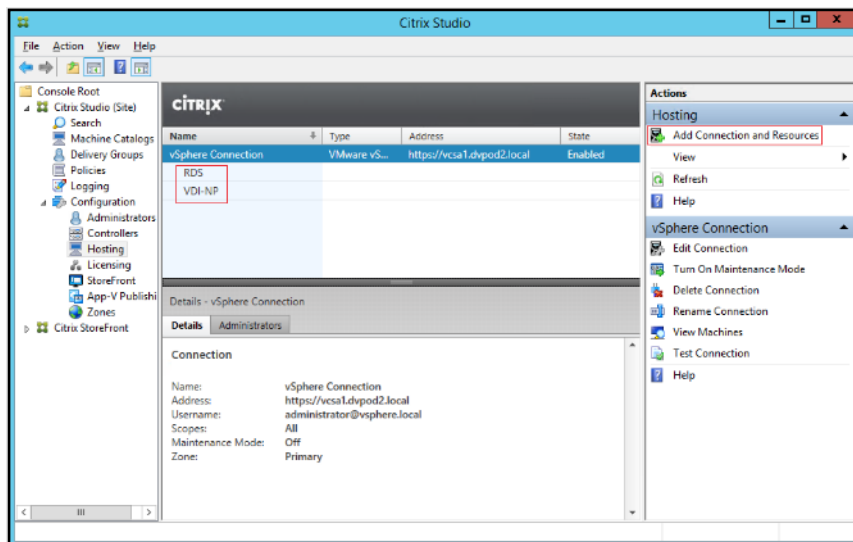




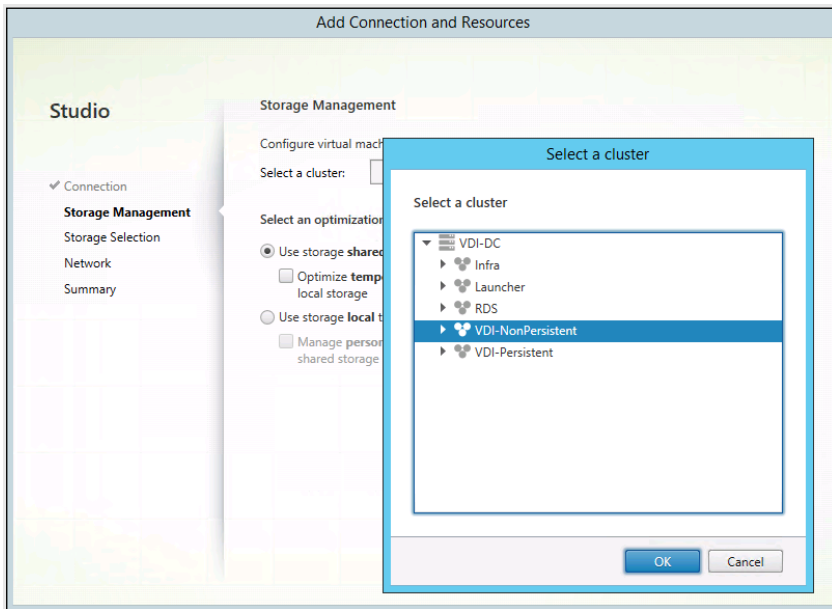
**Step 11.** From Citrix Studio on the Desktop Controller, select **Hosting** and **Add Connection and Resources**.

**Step 12.** Select **Use an existing Connection** and click **Next**.

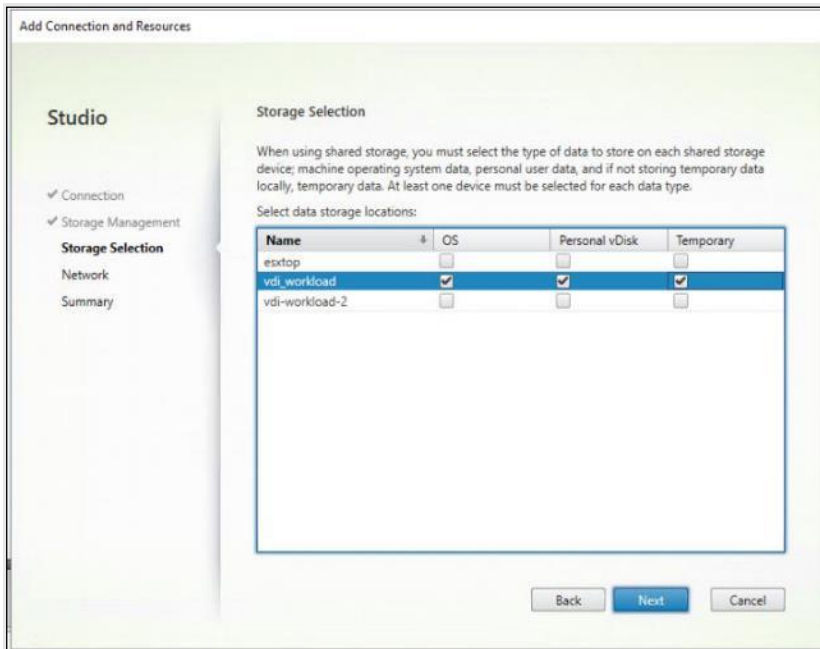
**Step 13.** Correspond the name of the resource with desktop machine clusters.



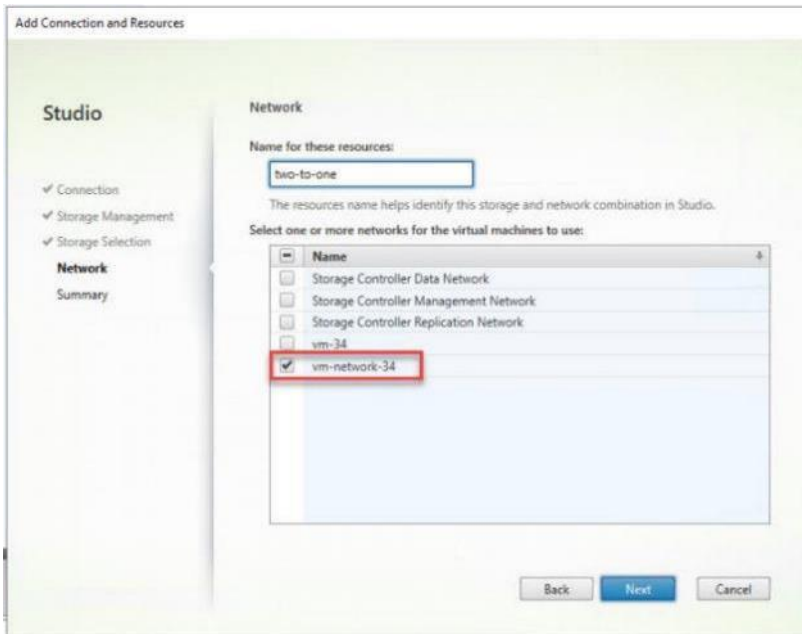
**Step 14.** Browse and select the VCenter cluster for desktop provisioning and use the default storage method Use storage shared by hypervisors.



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



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

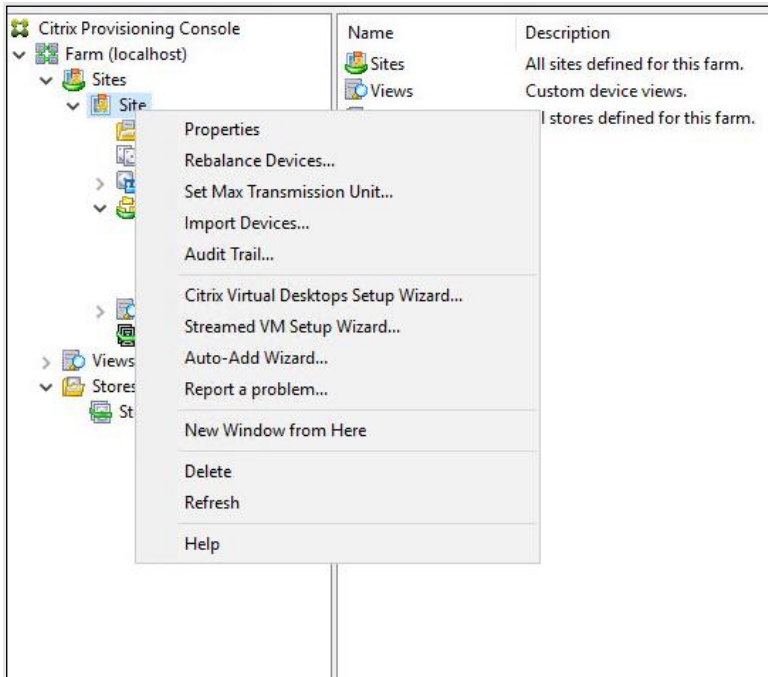


**Step 17.** Click **Finish**.

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

#### **Procedure 14.** Provision Desktop Machines from Citrix Provisioning Services Console

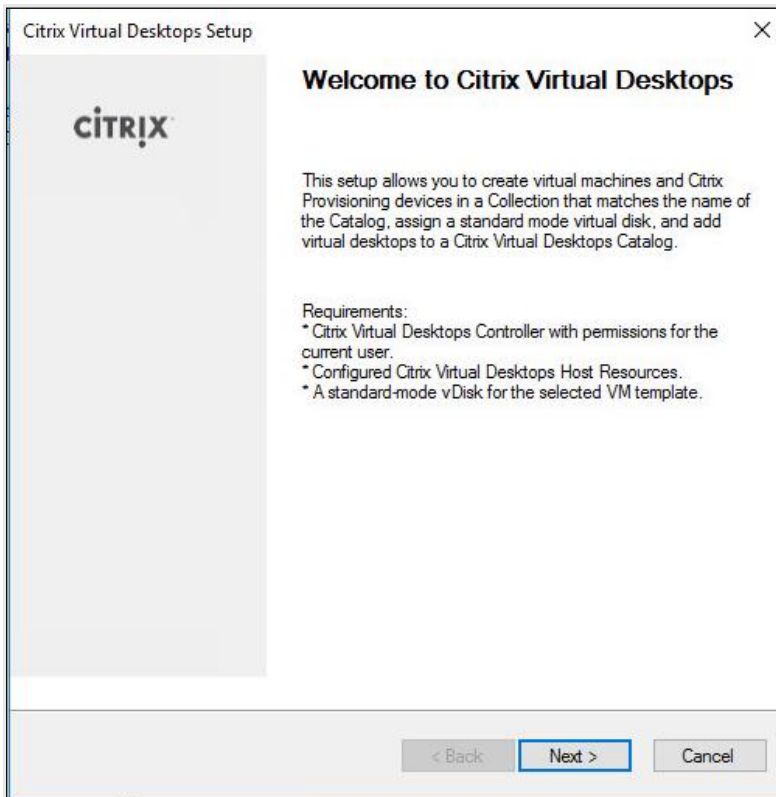
- Step 1.** Start the **Virtual Desktops Setup Wizard** from the Provisioning Services Console.
- Step 2.** Right-click **Site**.
- Step 3.** Select **Citrix Virtual Desktops Setup Wizard...** from the context menu.



**Step 4.** Click **Next**.

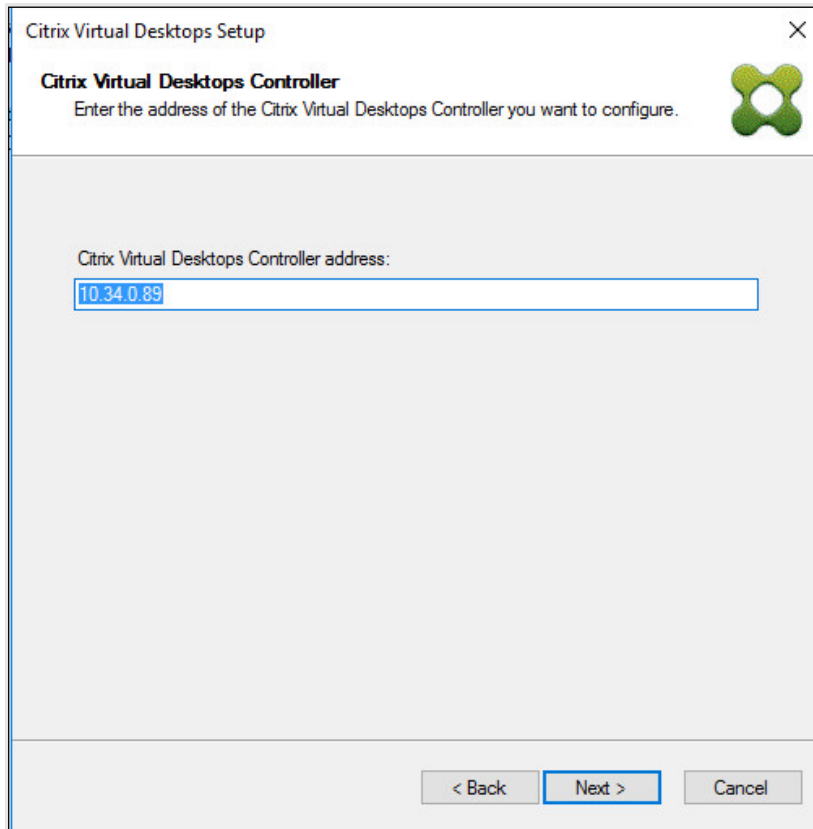
**Step 5.** Enter the Virtual Desktops Controller address that will be used for the wizard operations.

**Step 6.** Click **Next**.



**Step 7.** Select the Host Resources on which the virtual machines will be created.

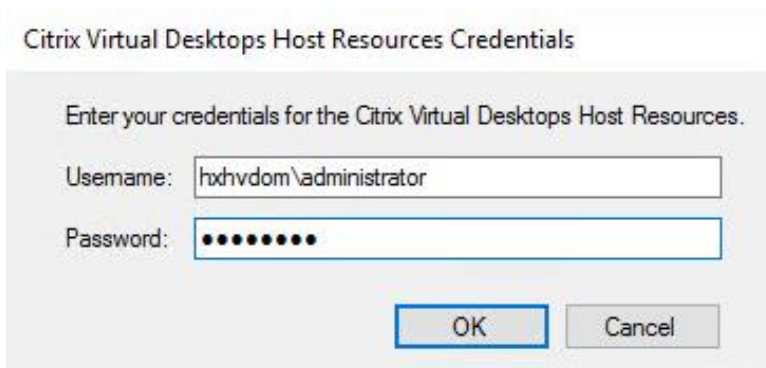
**Step 8.** Click **Next**.



The image shows a Windows dialog box titled "Citrix Virtual Desktops Setup". The main heading is "Citrix Virtual Desktops Controller" with a sub-instruction: "Enter the address of the Citrix Virtual Desktops Controller you want to configure." Below this, there is a text input field labeled "Citrix Virtual Desktops Controller address:" containing the IP address "10.34.0.89". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel". A Citrix logo is visible in the top right corner of the dialog.

**Step 9.** Provide the Host Resources Credentials (Username and Password) to the Virtual Desktops controller when prompted.

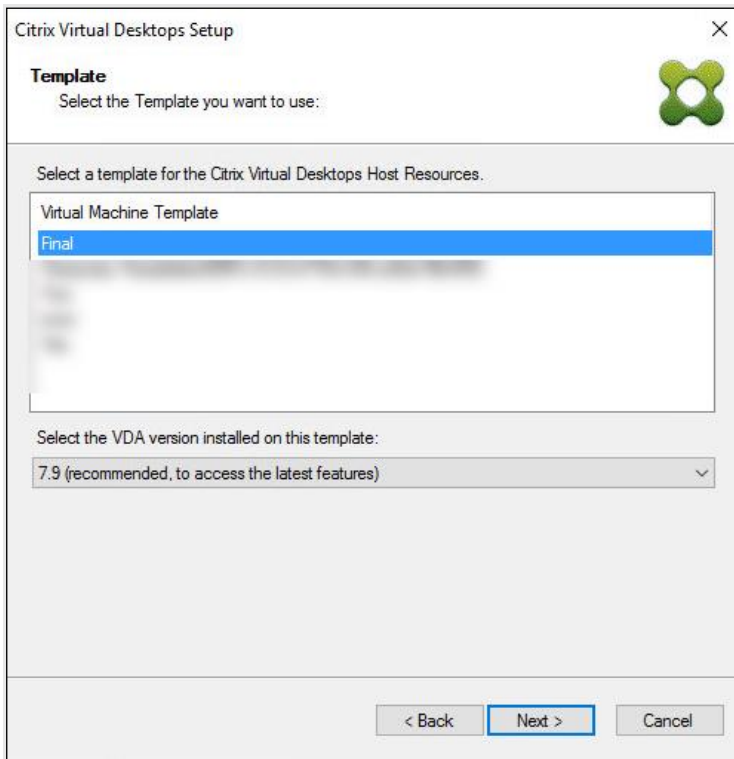
**Step 10.** Click **OK**.



The image shows a Windows dialog box titled "Citrix Virtual Desktops Host Resources Credentials". The main heading is "Citrix Virtual Desktops Host Resources Credentials" with a sub-instruction: "Enter your credentials for the Citrix Virtual Desktops Host Resources." Below this, there are two text input fields: "Username:" containing "hxhvdcm\administrator" and "Password:" containing a series of black dots. At the bottom of the dialog, there are two buttons: "OK" (highlighted with a blue border) and "Cancel".

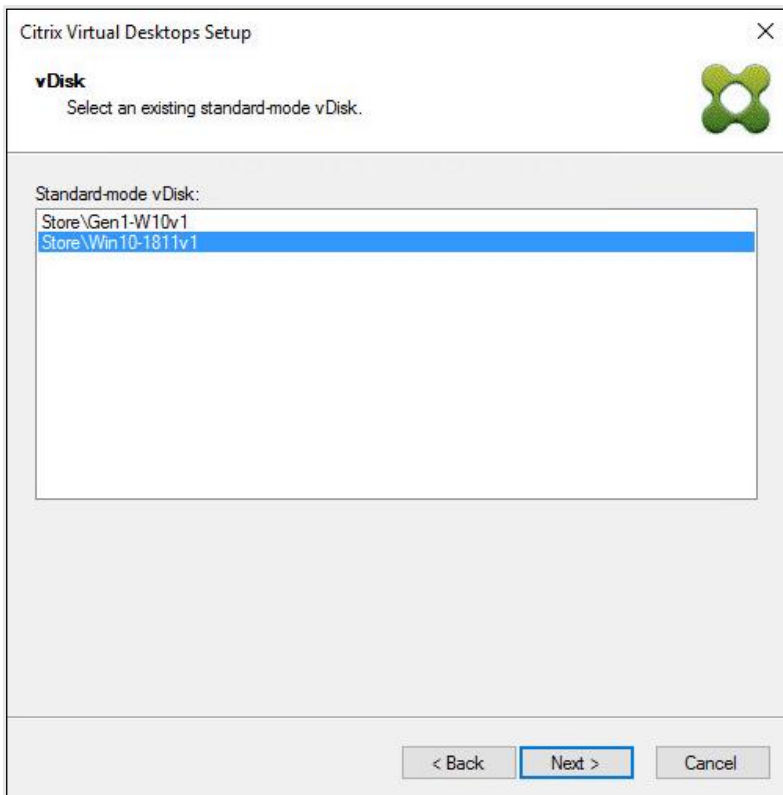
**Step 11.** Select the template previously created.

**Step 12.** Click **Next**.



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

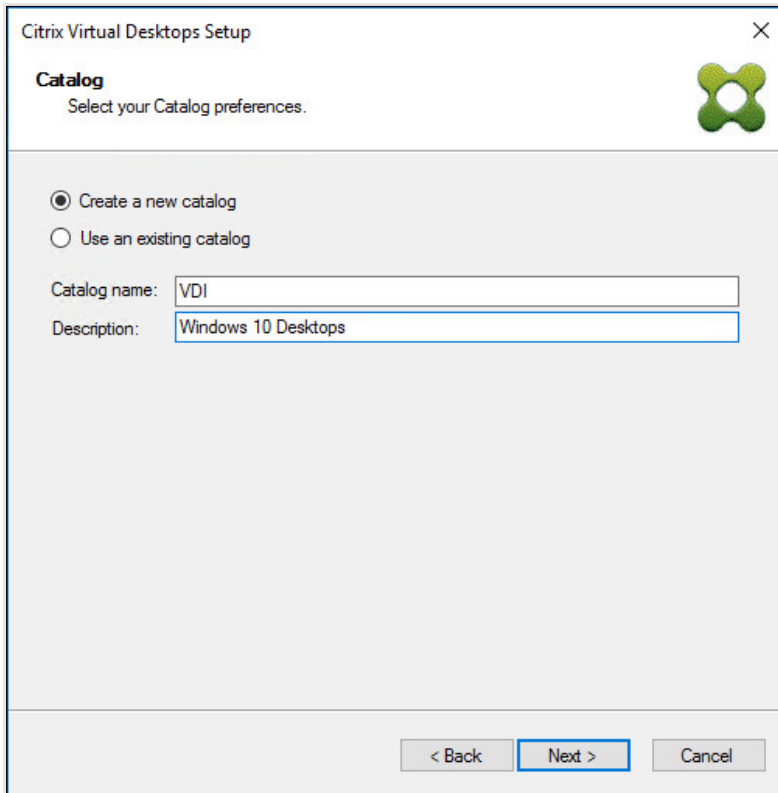
**Step 14.** Click **Next**.



**Step 15.** Select **Create a new catalog**.

**Note:** The catalog name is also used for the collection name in the PVS site.

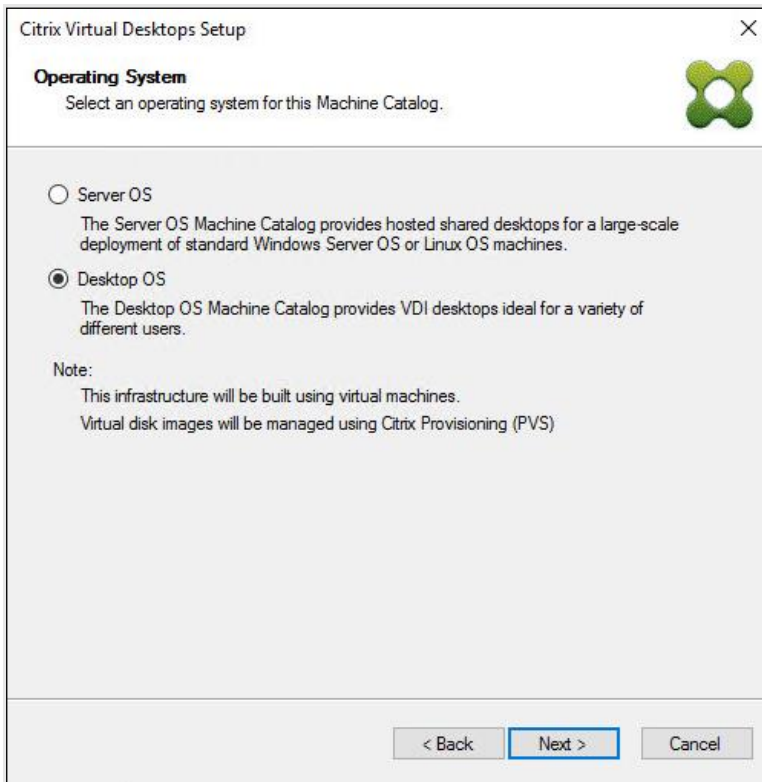
**Step 16.** Click **Next**.



The screenshot shows a dialog box titled "Citrix Virtual Desktops Setup" with a close button (X) in the top right corner. Below the title bar, the word "Catalog" is displayed in bold, followed by the instruction "Select your Catalog preferences." and a green Citrix logo. There are two radio button options: "Create a new catalog" (which is selected) and "Use an existing catalog". Below these options are two text input fields: "Catalog name:" with the value "VDI" and "Description:" with the value "Windows 10 Desktops". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

**Step 17.** On the Operating System dialog, specify the operating system for the catalog. Specify Windows Desktop Operating System for VDI and Windows Server Operating System for RDS.

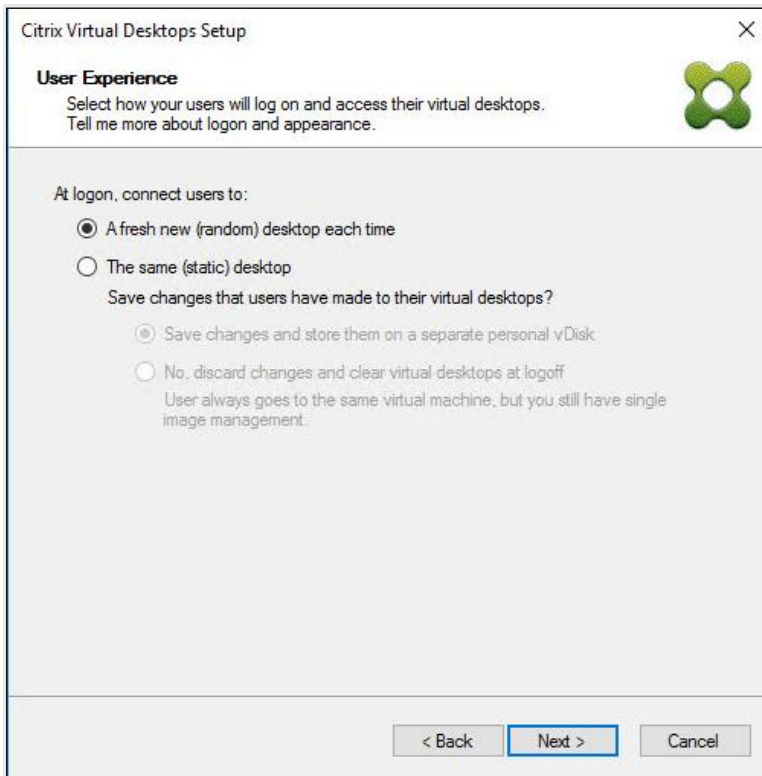
**Step 18.** Click **Next**.



**Step 19.** If you specified a Windows Desktop OS for VDIs, a User Experience dialog appears. Specify that the user will connect to **A fresh new (random) desktop each time.**

**Step 20.** Click **Next.**





**Step 21.** On the Virtual machines dialog, specify:

- a. The number of virtual machines to create.
- b. Number of vCPUs for the virtual machine (2 for VDI, 8 for RDS).
- c. The amount of memory for the virtual machine (4GB for VDI, 24GB for RDS).
- d. The write-cache disk size (10GB for VDI, 30GB for RDS).
- e. PXE boot for the Boot Mode.

**Step 22.** Click **Next**.

Citrix Virtual Desktops Setup

**Virtual machines**  
Select your virtual machine preferences.

Number of virtual machines to create: 800

vCPUs: 2

Memory: 4096 MB

Local write cache disk: 6 GB

Boot mode:

- PXE boot (requires a running PXE service)
- BDM disk (create a boot device manager partition)

< Back   Next >   Cancel

**Step 23.**      Select **Create new accounts**.

**Step 24.**      Click **Next**.

Citrix Virtual Desktops Setup

**Active Directory**  
Select your computer account option.

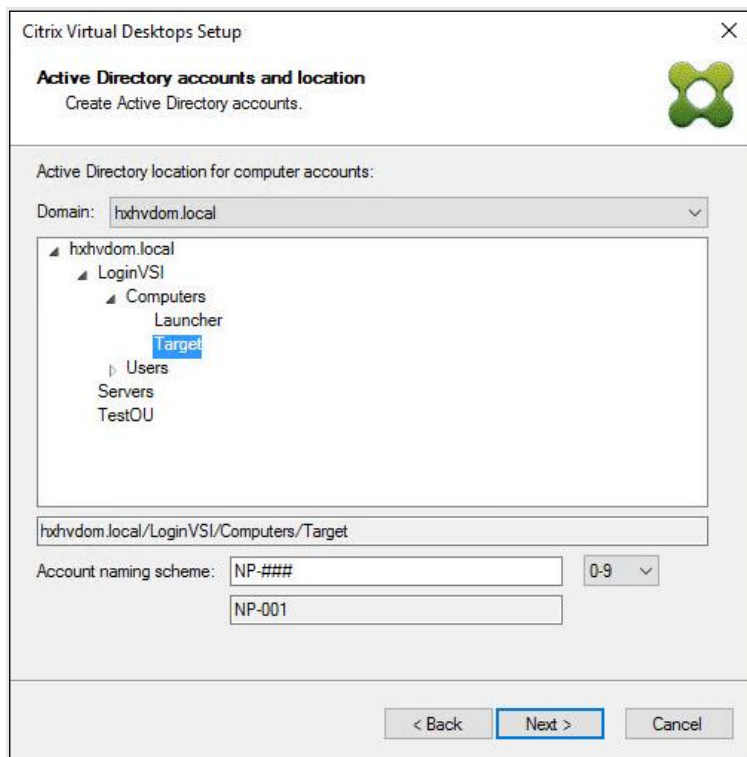
- Create new accounts
- Import existing accounts

< Back   Next >   Cancel

**Step 25.** Specify the Active Directory Accounts and Location. This is where the wizard should create the computer accounts.

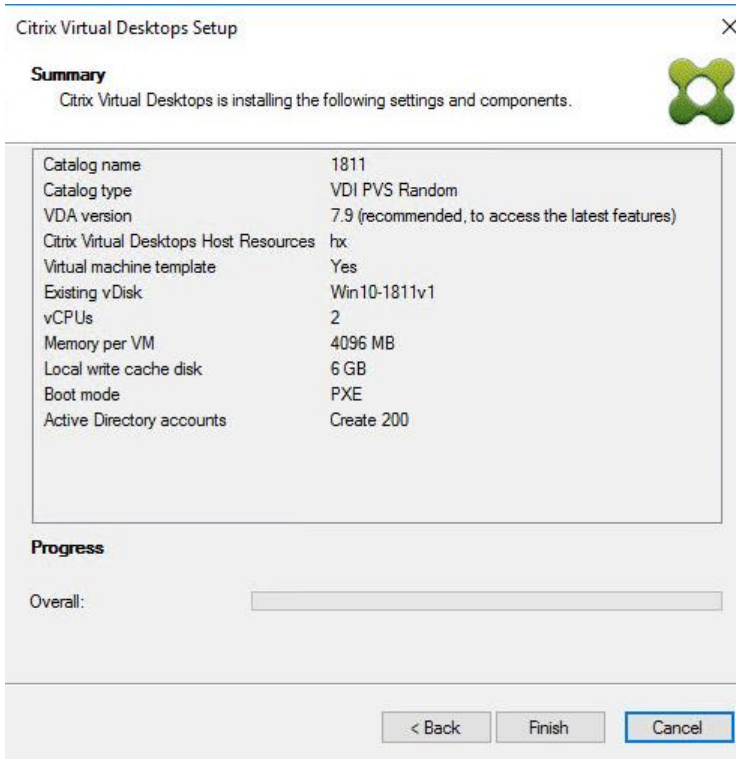
**Step 26.** Provide the Account naming scheme. An example name is shown in the text box below the name scheme selection location.

**Step 27.** Click **Next**.



The screenshot shows the 'Citrix Virtual Desktops Setup' wizard window. The title bar reads 'Citrix Virtual Desktops Setup' with a close button. The main heading is 'Active Directory accounts and location' with a sub-heading 'Create Active Directory accounts.' and a Citrix logo. Below this, the text 'Active Directory location for computer accounts:' is followed by a 'Domain:' dropdown menu set to 'hxhvd.com.local'. A tree view shows the directory structure: 'hxhvd.com.local' expanded to show 'LoginVSI', which is expanded to show 'Computers', which is expanded to show 'Launcher' and 'Target'. The 'Target' folder is selected. Below the tree view, a text box contains the path 'hxhvd.com.local/LoginVSI/Computers/Target'. Underneath, the 'Account naming scheme:' is set to 'NP-###' with a dropdown menu showing '0-9'. A text box below shows the example name 'NP-001'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

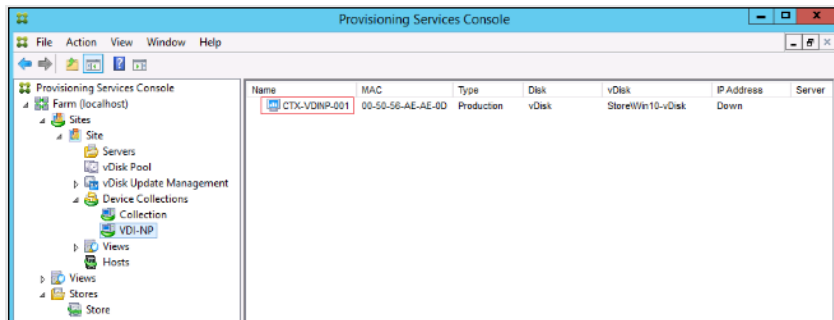
**Step 28.** Click **Finish** to begin the virtual machine creation.



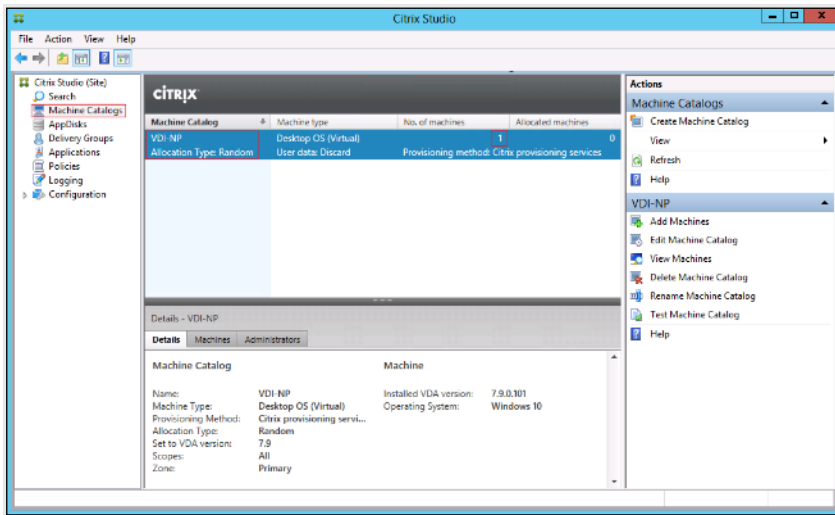
**Step 29.** When the wizard is done provisioning the virtual machines, click **Done**.

**Step 30.** Verify the desktop machines were successfully created in the following locations:

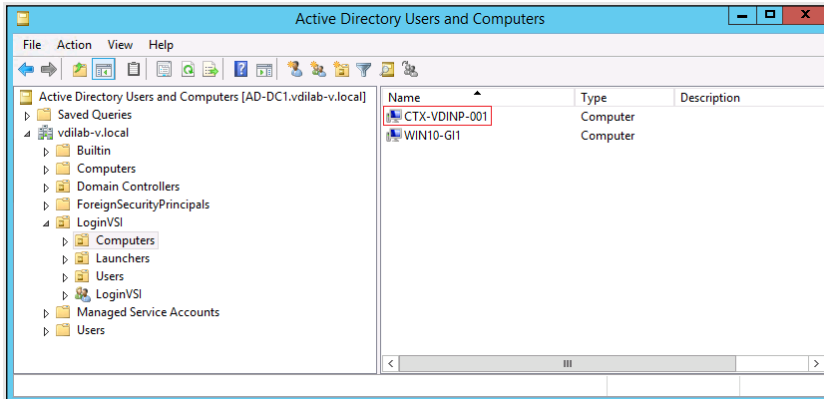
- a. PVS1 > Provisioning Services Console > Farm > Site > Device Collections > VDI-NP > CTX-VDI-001



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



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



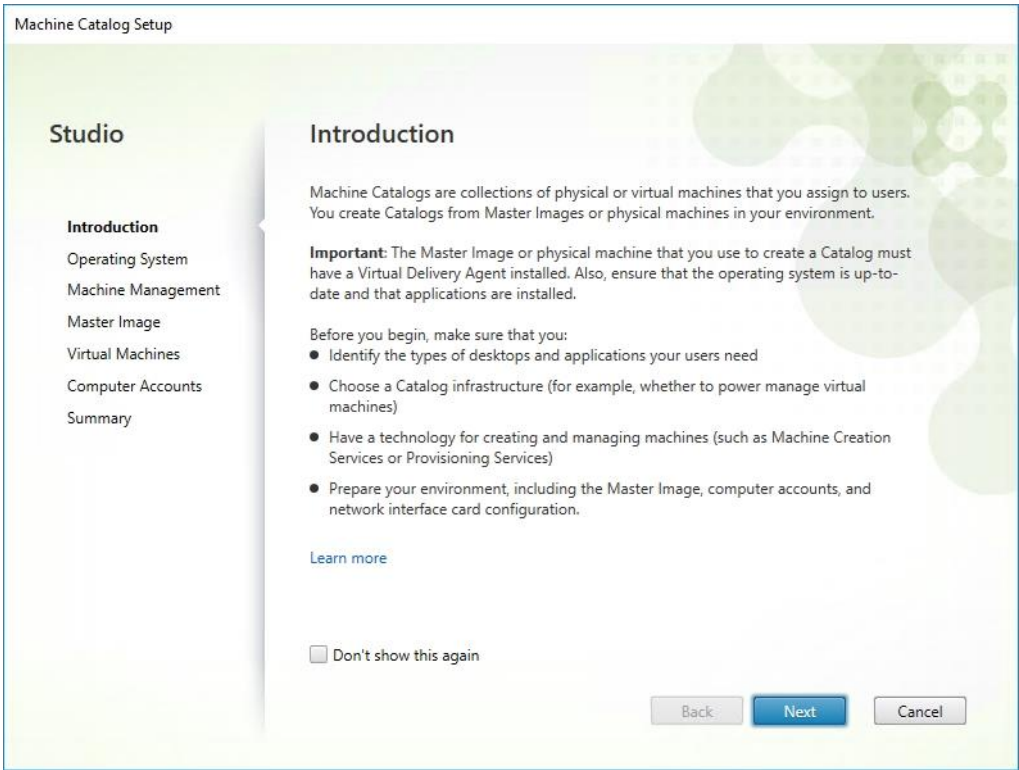
**Step 31.** Log into the newly provisioned desktop machine, using the Virtual Disk Status verify the image mode is set to Ready Only and the cache type as Device Ram with overflow on local hard drive.

## Procedure 15. Citrix Machine Creation Services

**Step 1.** Connect to a Citrix Virtual Apps & Desktops server and launch Citrix Studio.

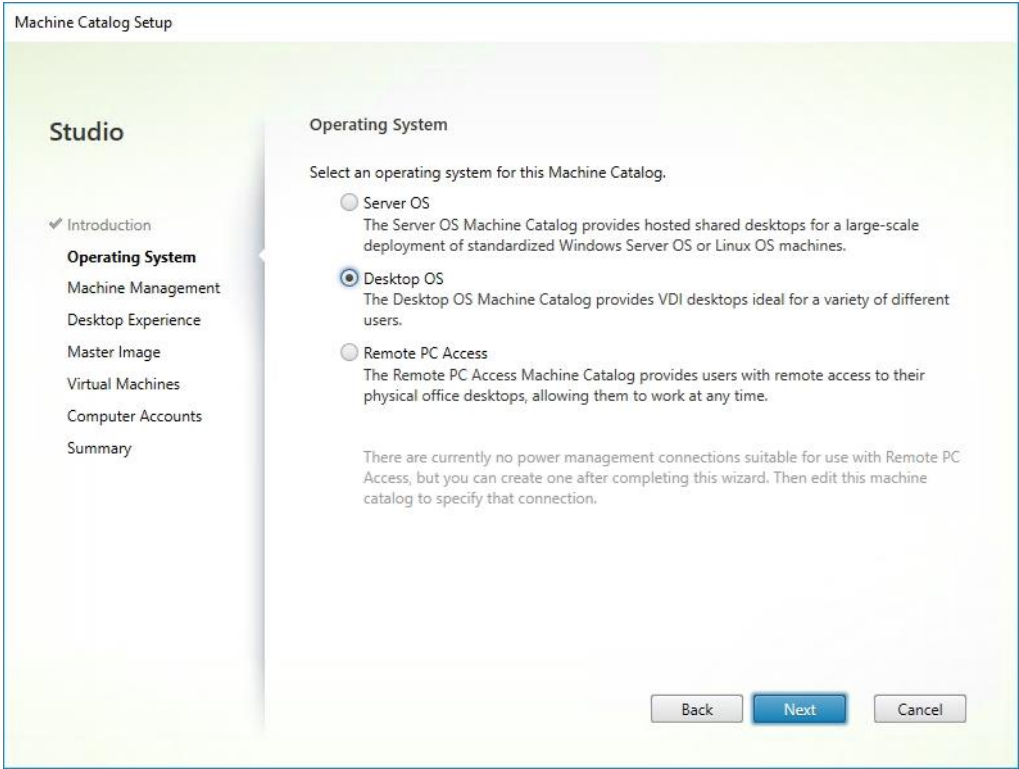
**Step 2.** Select **Create Machine Catalog** from the Actions pane.

**Step 3.** Click **Next**.



**Step 4.** Select **Desktop OS**.

**Step 5.** Click **Next**.



**Step 6.** Select the appropriate machine management.

**Step 7.** Click **Next**.

The screenshot shows the 'Machine Catalog Setup' wizard. On the left is a 'Studio' sidebar with a list of steps: Introduction, Operating System, Machine Management (highlighted), Desktop Experience, Master Image, Virtual Machines, Computer Accounts, and Summary. The main area is titled 'Machine Management' and contains the following options:

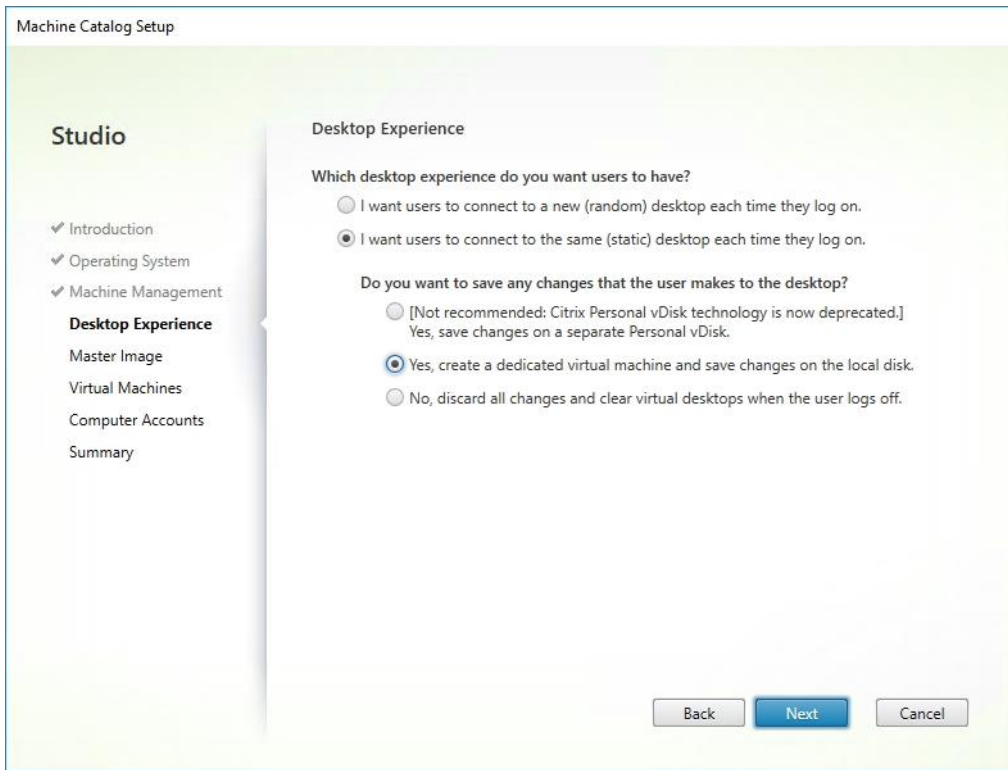
- This Machine Catalog will use:**
  - Machines that are power managed (for example, virtual machines or blade PCs)
  - Machines that are not power managed (for example, physical machines)
- Deploy machines using:**
  - Citrix Machine Creation Services (MCS)
    - Resources:** MCS-FC-STATIC (Zone: Primary) (dropdown menu)
  - Citrix Provisioning Services (PVS)
  - 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.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

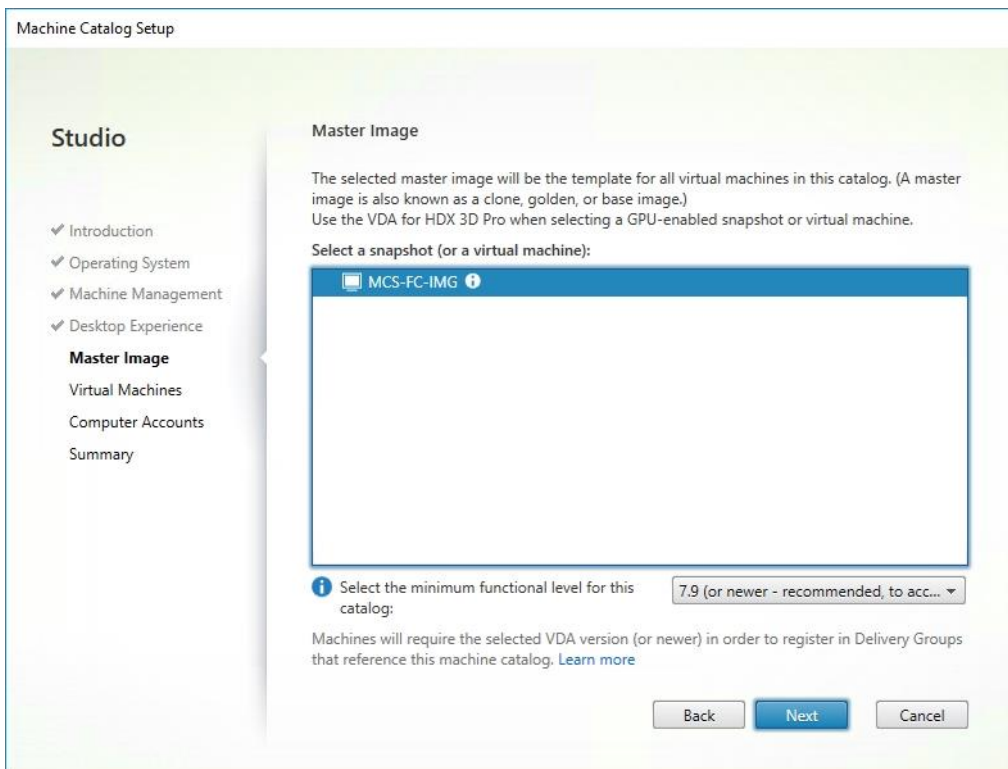
**Step 8.** Select **Static, Dedicated Virtual Machine** for Desktop Experience.

**Step 9.** Click **Next**.



**Step 10.** Select a Virtual Machine to be used for Catalog Master Image.

**Step 11.** Click **Next**.





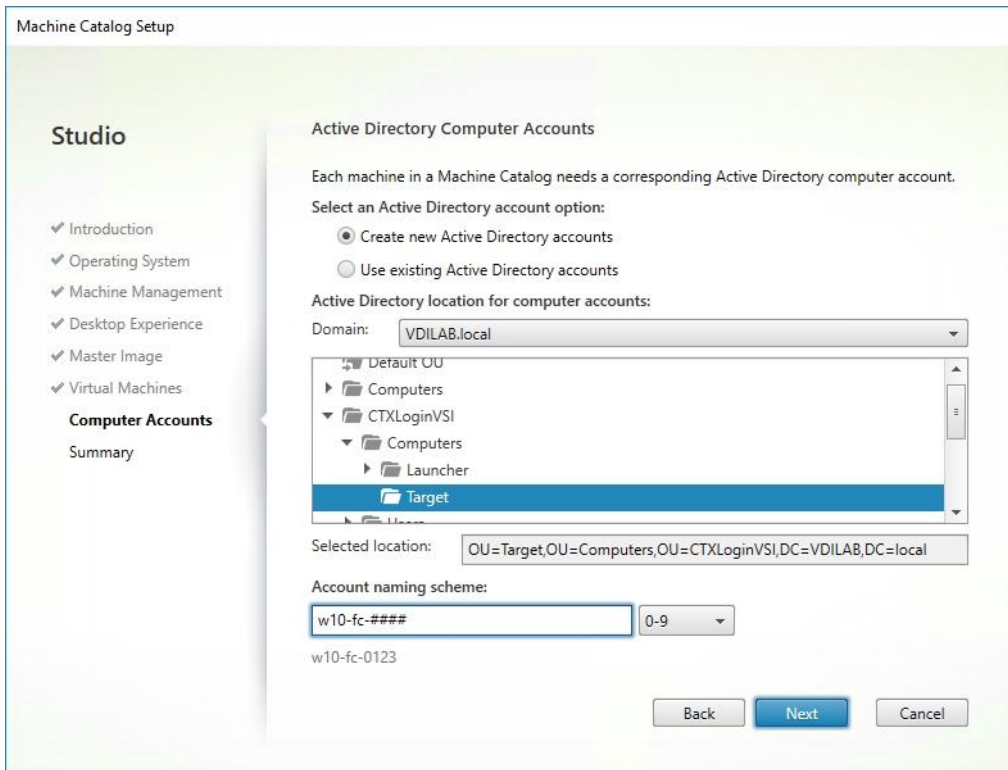
- Step 12.** Specify the number of desktop to create and machine configuration.
- Step 13.** Set amount of memory (MB) to be used by virtual desktops.
- Step 14.** Select **Full Copy** for machine copy mode.
- Step 15.** Click **Next**.

The screenshot shows the 'Machine Catalog Setup' wizard at the 'Virtual Machines' step. On the left is a 'Studio' sidebar with a list of steps: Introduction, Operating System, Machine Management, Desktop Experience, Master Image, **Virtual Machines** (highlighted), Computer Accounts, and Summary. The main area contains the following configuration options:

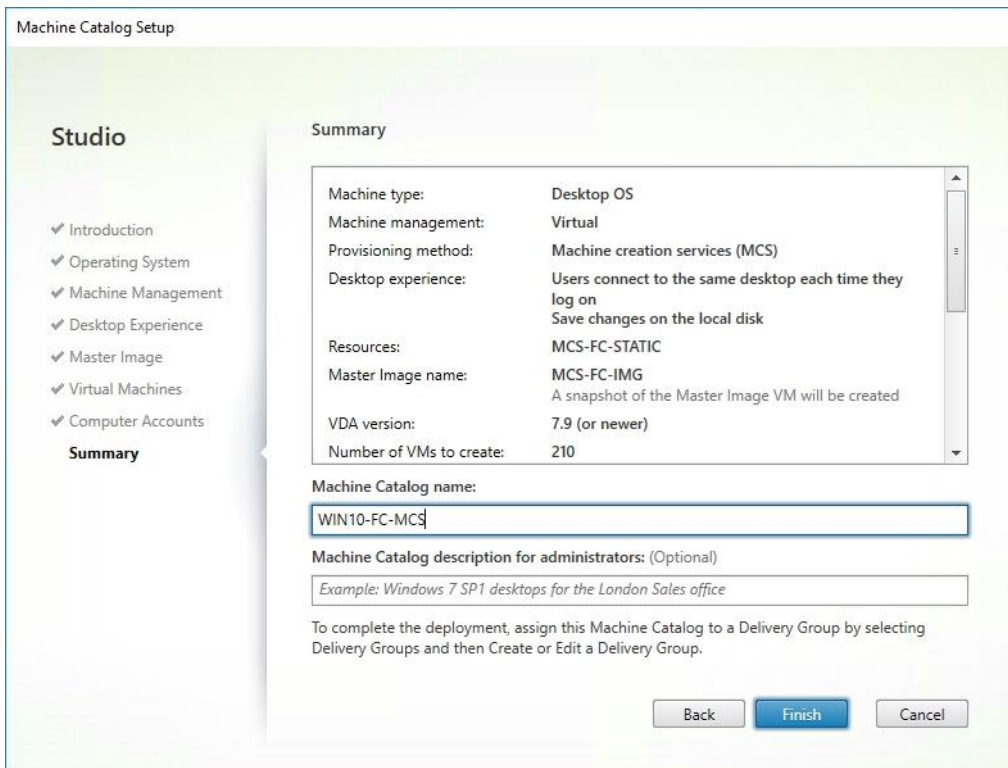
- Virtual Machines**
- How many virtual machines do you want to create? (Input: 210)
- Configure your machines.  
Total memory (MB) on each machine: (Input: 4096)
- Select a virtual machine copy mode.
  - Use fast clone for more efficient storage use and faster machine creation.
  - Use full copy for better data recovery and migration support, with potentially reduced IOPS after the machines are created.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

- Step 16.** Specify AD account naming scheme and OU where accounts will be created.
- Step 17.** Click **Next**.



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



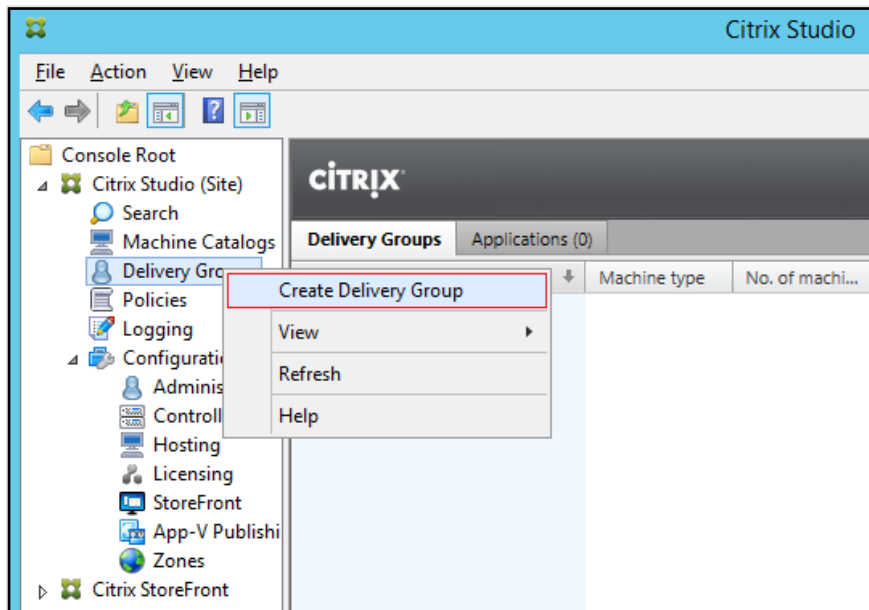
**Procedure 16.** Create Delivery Groups

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.

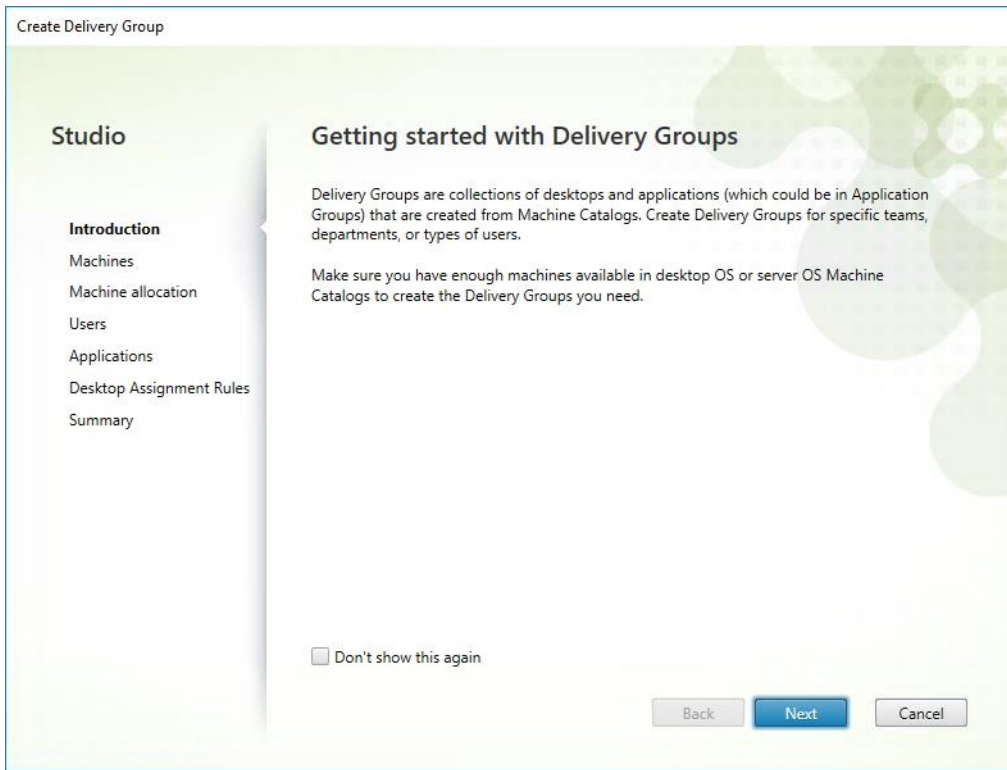
**Note:** The instructions below outline the procedure to create a Delivery Group for VDI desktops. When you have completed these steps, repeat the procedure to a Delivery Group for RDS desktops.

**Step 1.** Connect to a **Citrix Virtual Apps & Desktops server** and launch **Citrix Studio**.

**Step 2.** Select **Create Delivery Group** from the drop-down list.

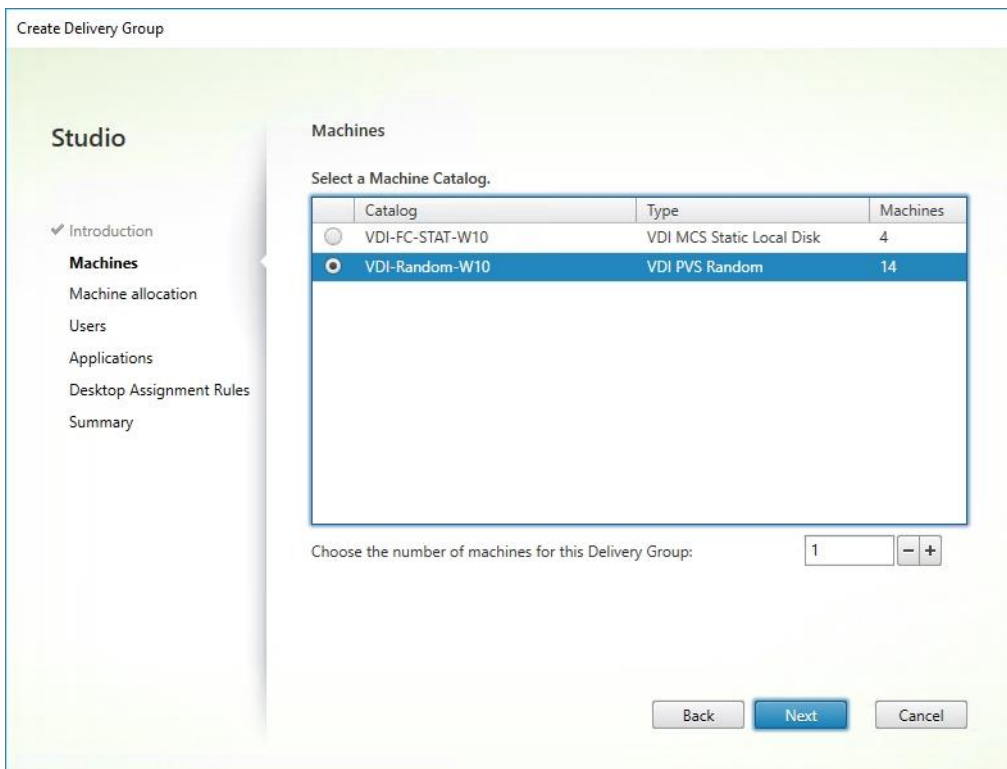


**Step 3.** Click **Next**.



**Step 4.** Specify the Machine Catalog and increment the number of machines to add.

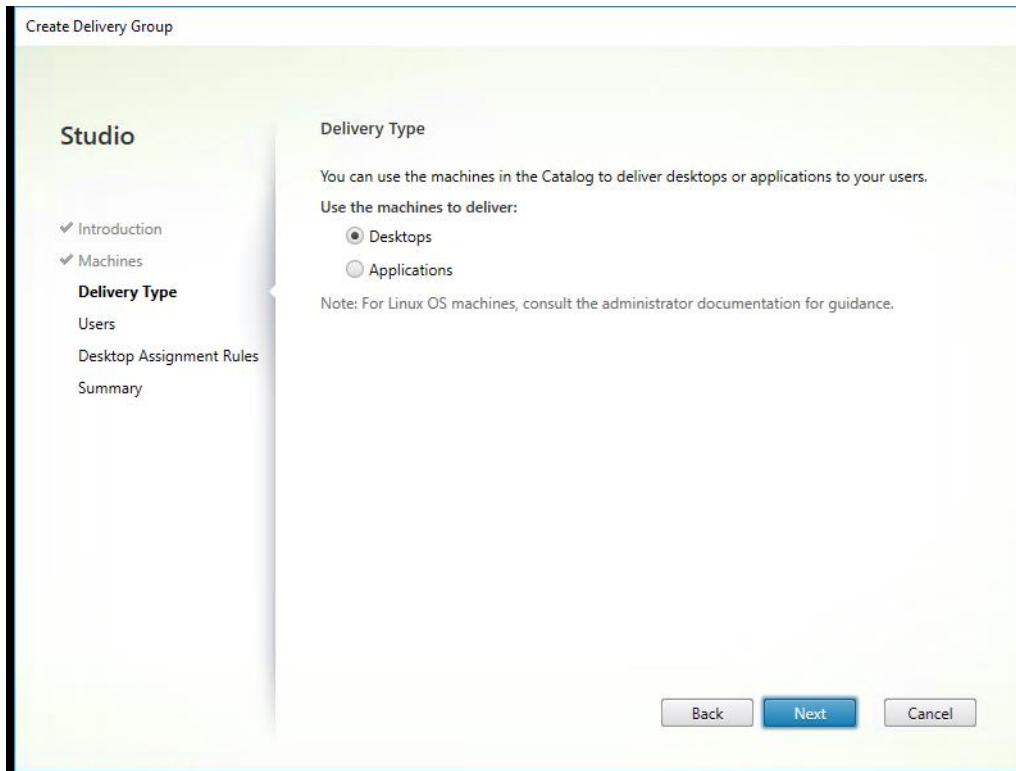
**Step 5.** Click **Next**.



**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**.

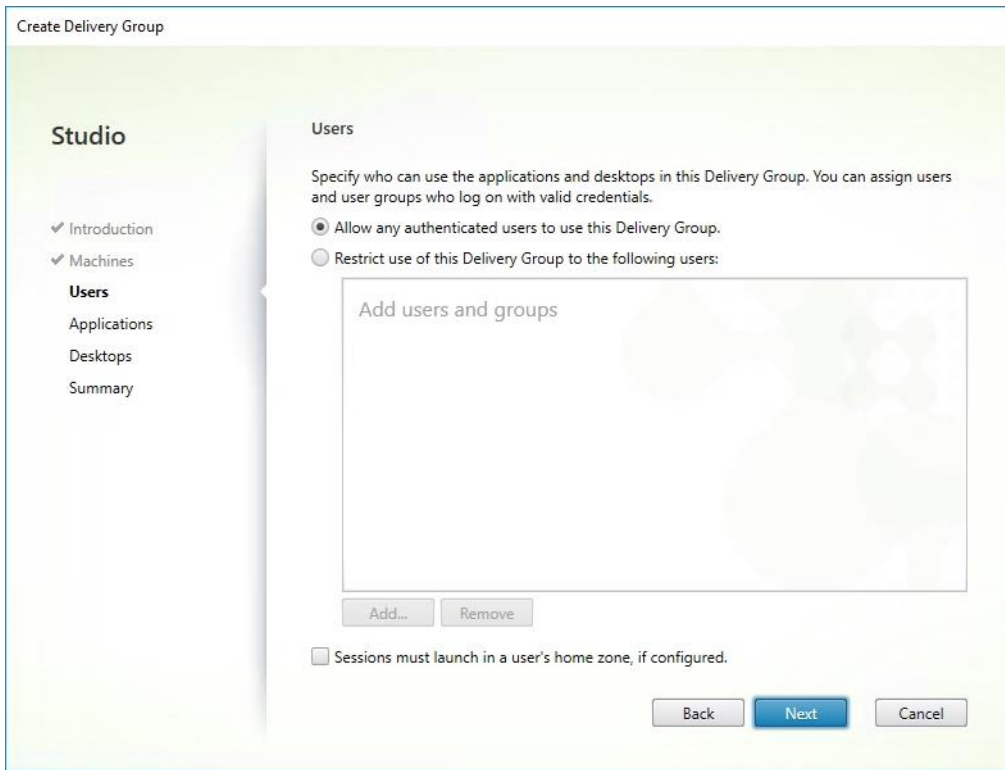


The screenshot shows the 'Create Delivery Group' wizard in Desktop Studio. The left sidebar, titled 'Studio', contains a navigation pane with the following items: 'Introduction', 'Machines', 'Delivery Type' (which is highlighted), 'Users', 'Desktop Assignment Rules', and 'Summary'. The main content area is titled 'Delivery Type' and contains the following text: 'You can use the machines in the Catalog to deliver desktops or applications to your users.' Below this, it says 'Use the machines to deliver:' followed by two radio button options: 'Desktops' (which is selected) and 'Applications'. A note at the bottom of the main area reads: 'Note: For Linux OS machines, consult the administrator documentation for guidance.' At the bottom right of the wizard, there are three buttons: 'Back', 'Next' (which is highlighted in blue), and 'Cancel'.

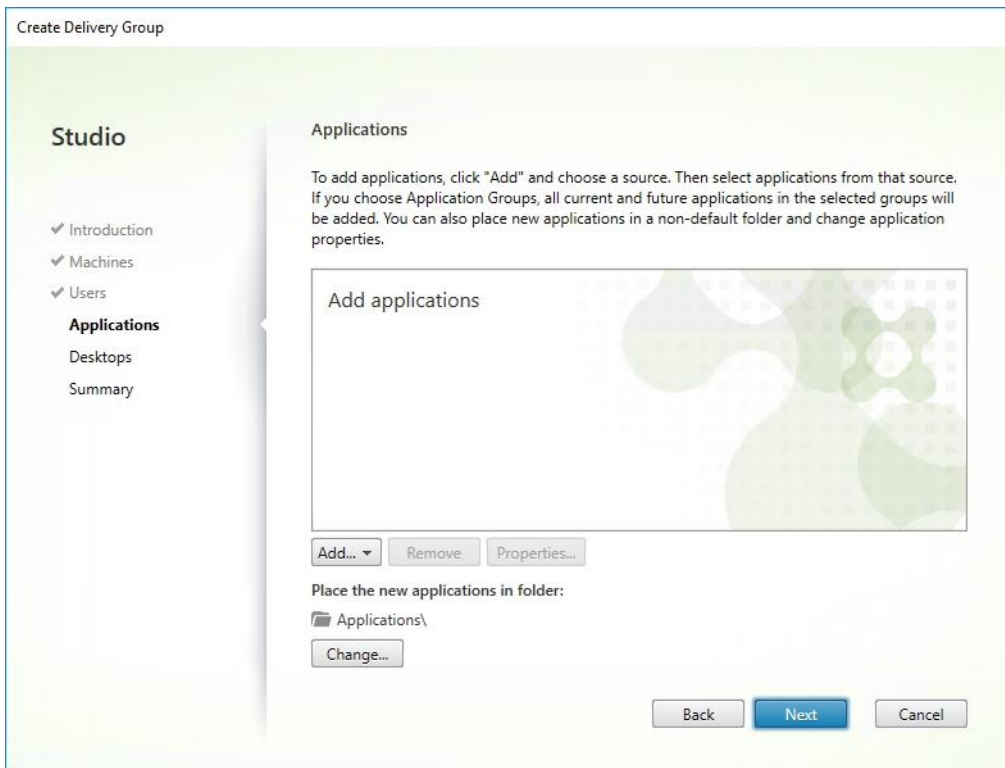
**Step 9.** To make the Delivery Group accessible, you must add users, select **Allow any authenticated users to use this Delivery Group**.

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

**Step 10.** Click **Next**.

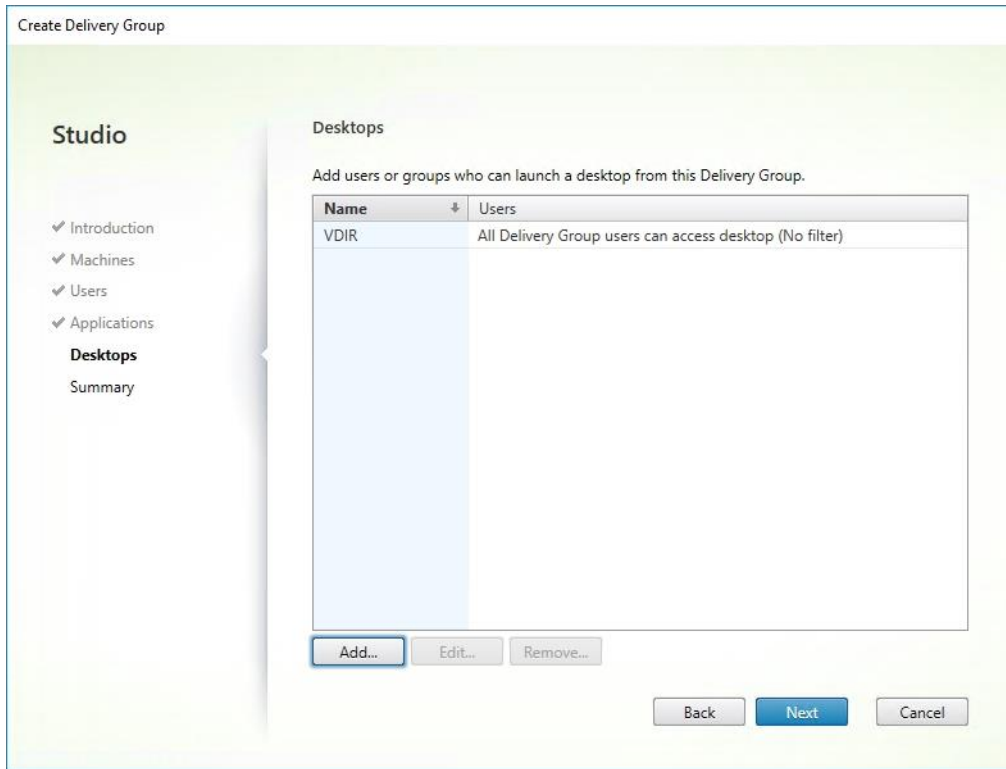


**Step 11.** Click **Next** (no applications used in this design).



**Step 12.** Enable Users to access the desktops.

**Step 13.** Click **Next**.



**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

**Studio**

- ✓ Introduction
- ✓ Machines
- ✓ Users
- ✓ Applications
- ✓ Desktops
- Summary**

**Summary**

Machine Catalog:	VDI-Random-W10
Machine type:	Desktop OS
Allocation type:	Random
Machines added:	VDILAB\w10-rnd-2586 1 unassigned
Users:	Allow authenticated users
Desktops:	VDIR
Launch in user's home zone:	No

Delivery Group name:

Delivery Group description, used as label in Receiver (optional):

Back Finish Cancel

Citrix Studio lists the created Delivery Groups as well for 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**.

## FSLogix for Citrix Virtual Apps & Desktops Profile Management

This subject contains the following procedures:

- [Configure FSLogix for Citrix Virtual Apps & Desktops Profiles Profile Container](#)
- [Configure FSLogix Profile Management](#)

FSLogix for user profiles allows the Citrix Virtual Apps & Desktops environment to be easily and efficiently customized.

### Procedure 1. Configure FSLogix for Citrix Virtual Apps & 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

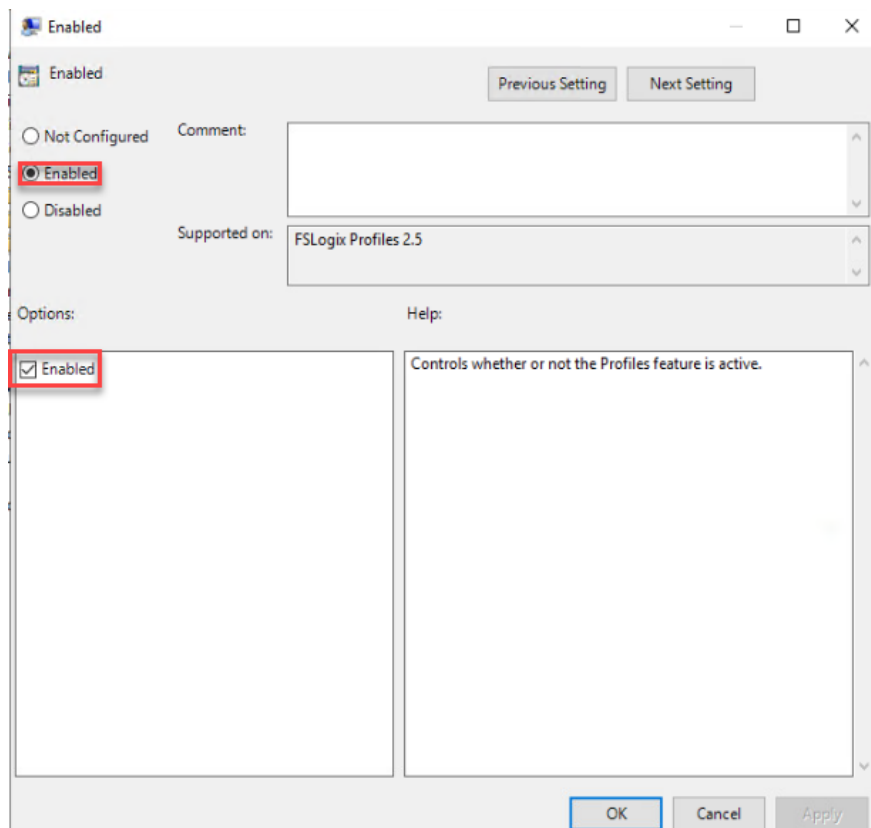
**Step 1.** When the FSLogix software is downloaded, copy the 'fslogix.admx and fslogix.adml' to the 'PolicyDefinitions' folder in your domain to manage the settings with Group Policy.

**Step 2.** On your VDI master image, install the FSLogix agent 'FSLogixAppsSetup' and accept all the defaults.

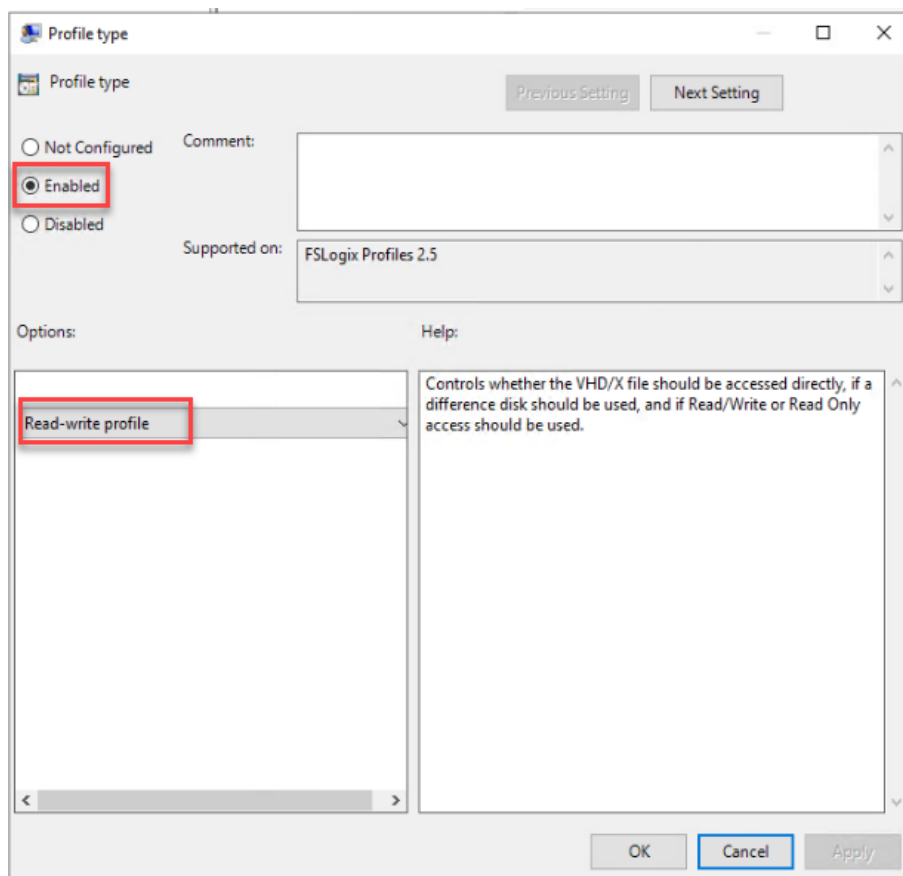
**Step 3.** Create a Group Policy object and link it to the Organizational Unit the VDI computer accounts.

**Step 4.** Right-click the **FSLogix GPO** policy.

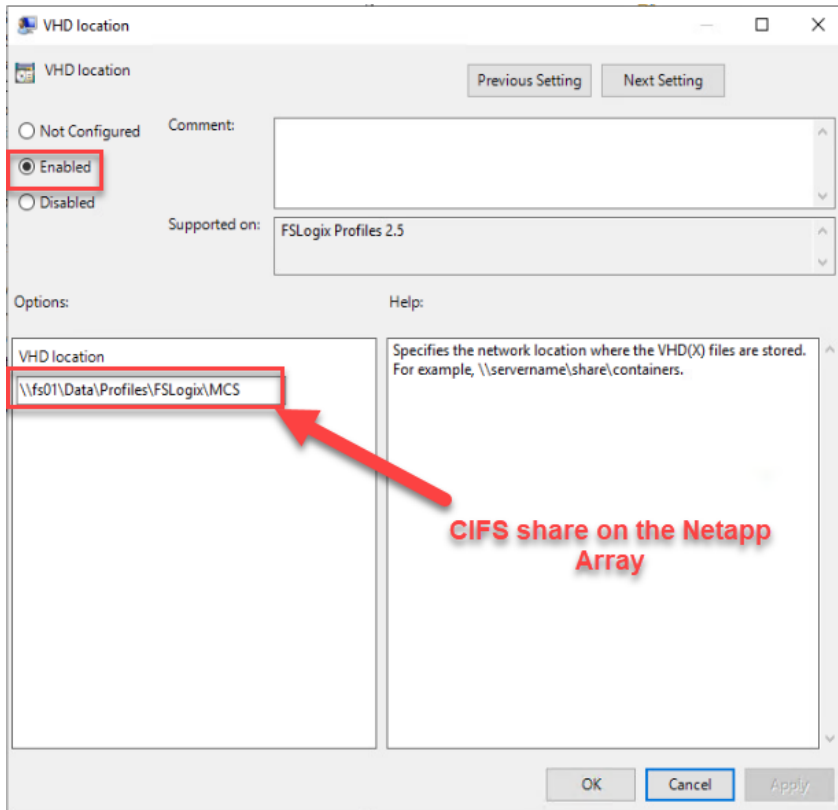
**Step 5.** Enable FSLogix Profile Management.



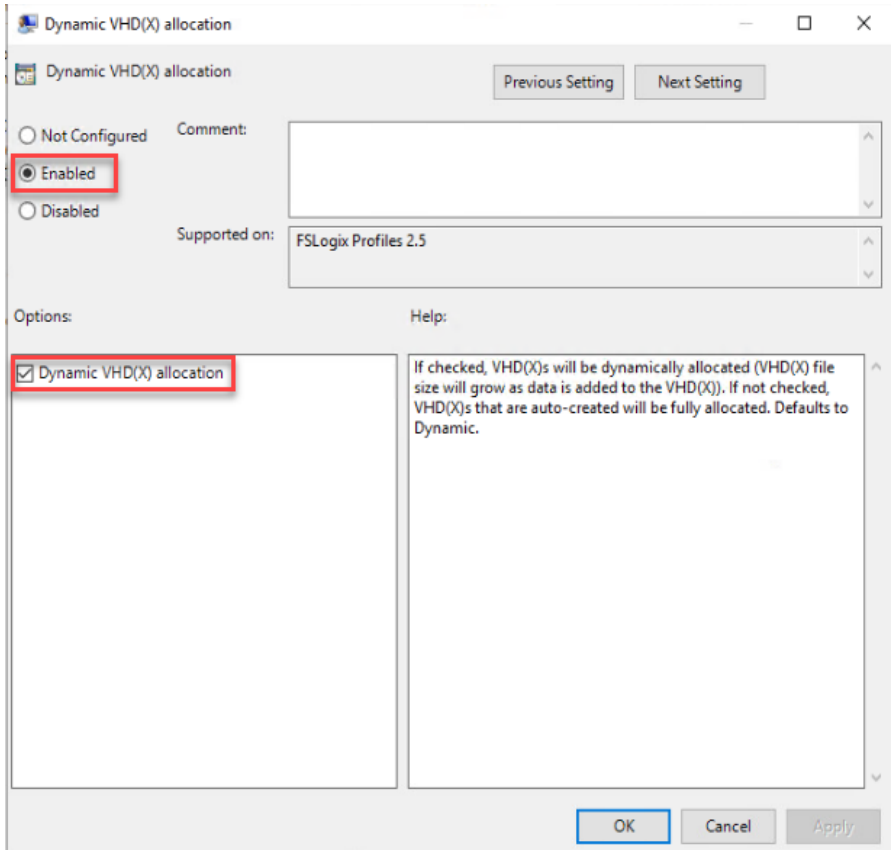
**Step 6.** Select Profile Type (in this solution, we used Read-Write profiles).



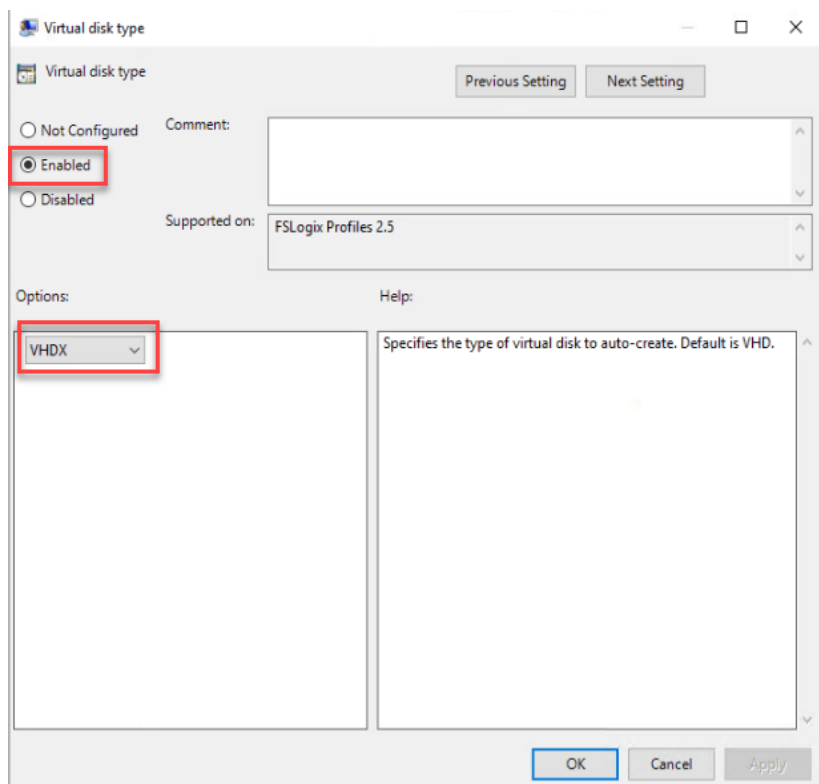
**Step 7.** Enter the location of the Profile location (our solution used a CIFS share on the Netapp Array).



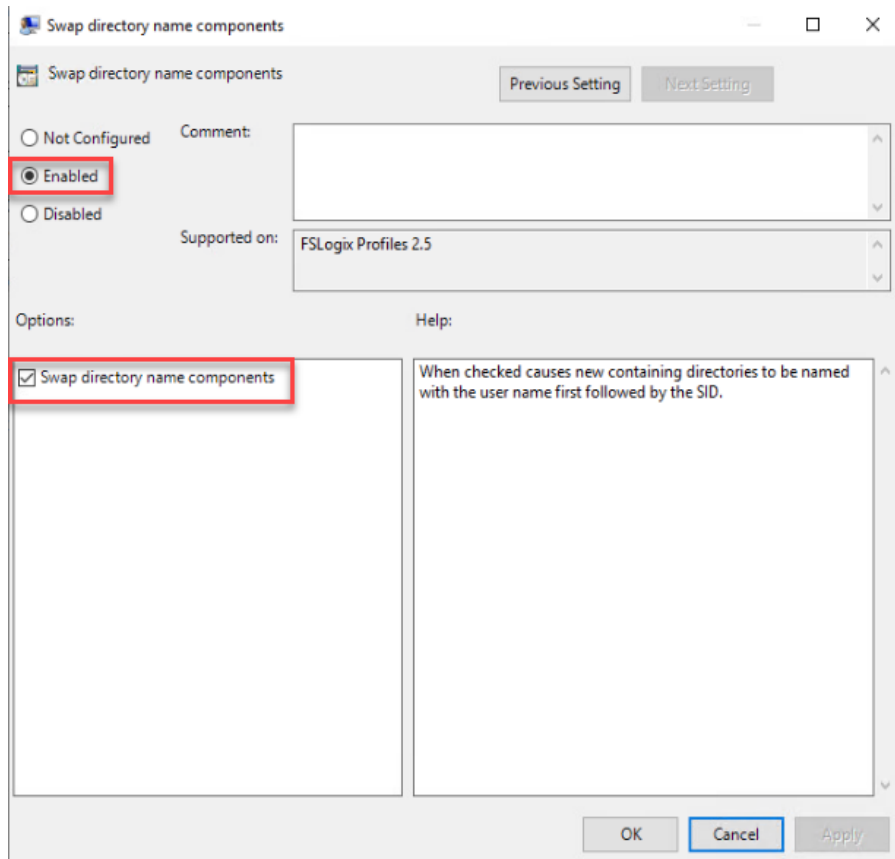
**Note:** We recommend using the Dynamic VHDX setting.



**Note:** VHDX is recommended over VHD.



**Note:** We enabled the 'Swap directory name components' setting for an easier administration but is not necessary for improved performance.



### 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.

---

## Test Setup and Configurations

This chapter is organized into the following subjects:

- [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 X210C M6 blade server to validate against the performance of one blade and eleven Cisco UCS X210C 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 & Desktops 7 LTSR with 260 RDS sessions, 250 VDI Non-Persistent sessions, and 250 VDI Persistent sessions.

Figure 36. Test configuration for Single Server Scalability Citrix Virtual Apps & Desktops 7 LTSR VDI (Persistent) Using MCS

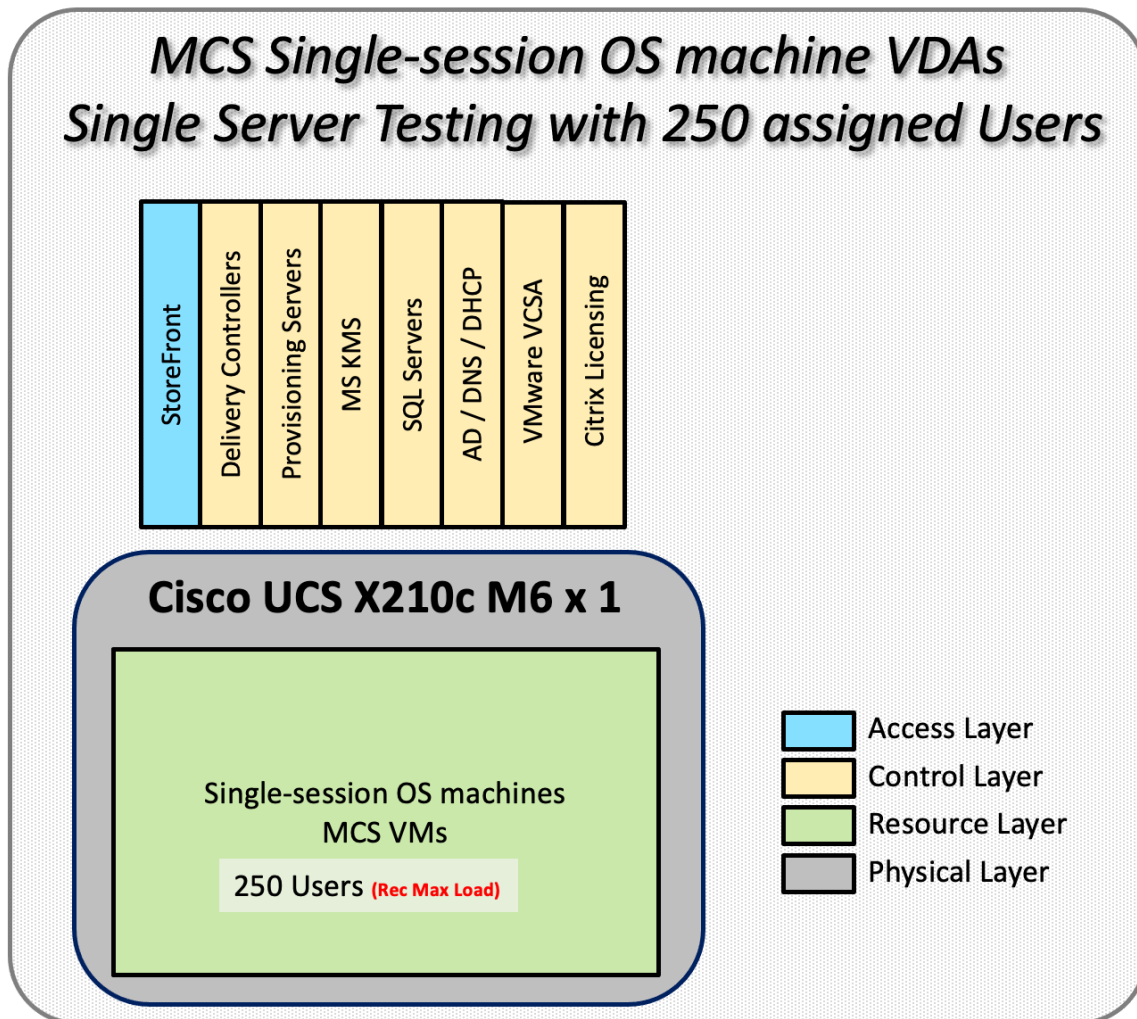




Figure 37. Test configuration for Single Server Scalability Citrix Virtual Apps & Desktops 7 LTSR VDI (Non-Persistent) using PVS

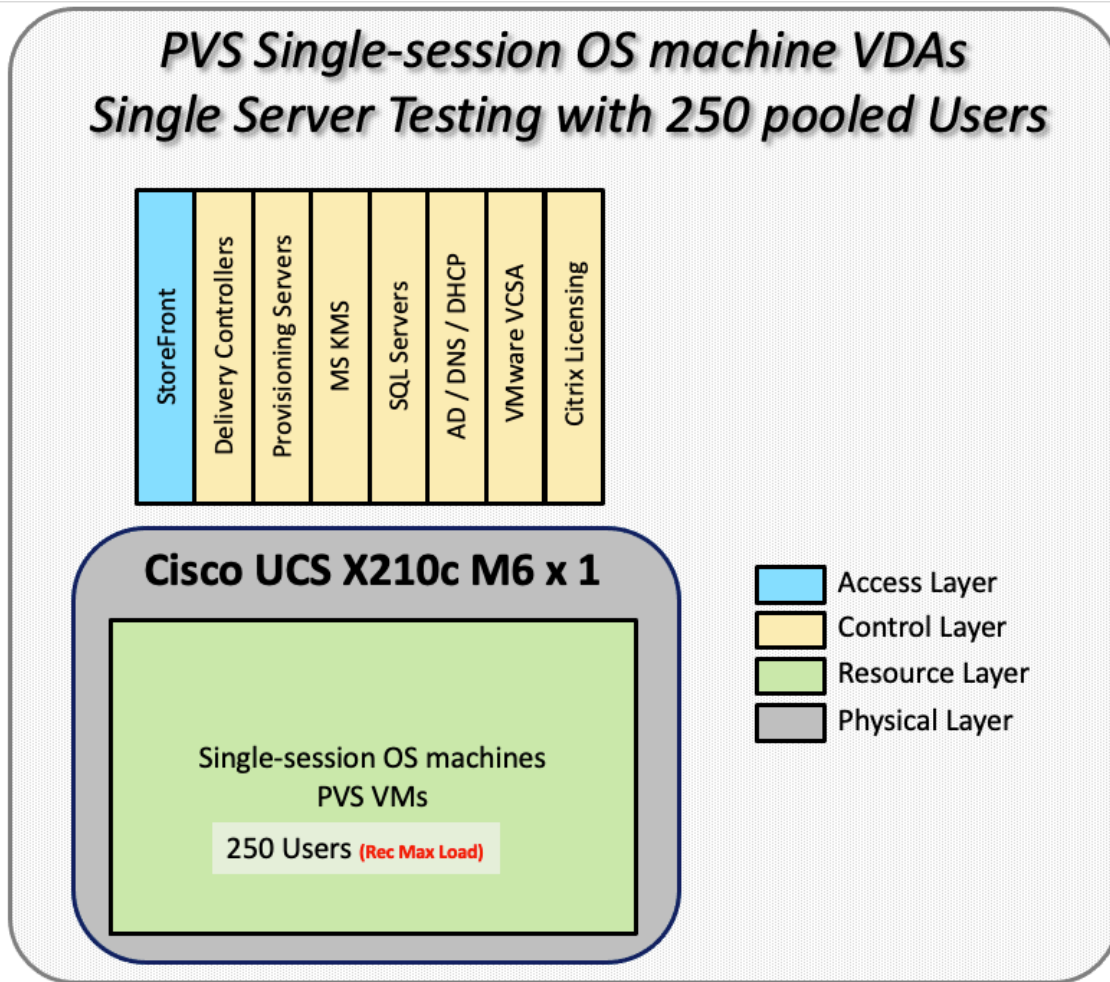
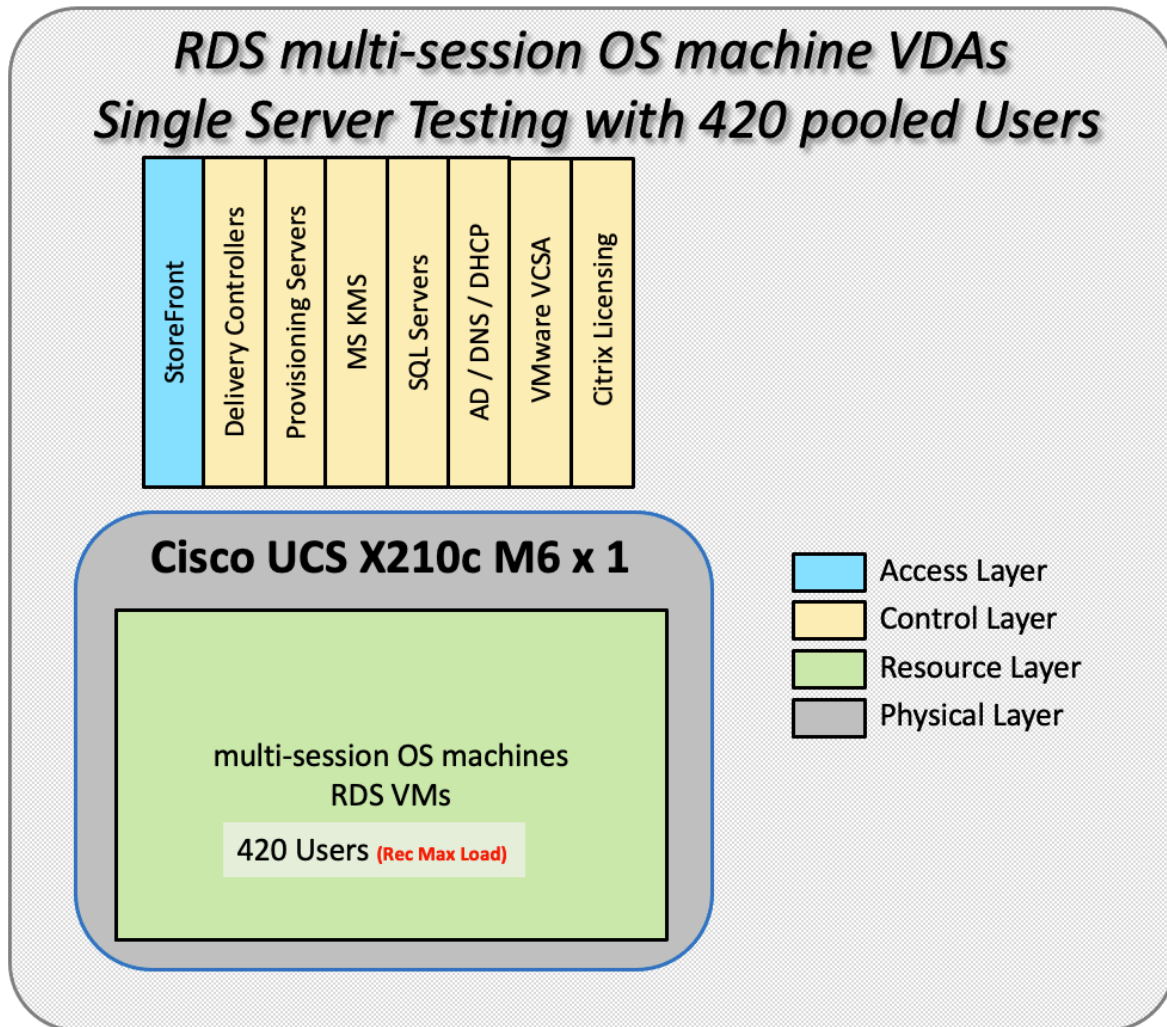


Figure 38. Test configuration for Single Server Scalability Citrix Virtual Apps & Desktops 7 LTSR RDS



Hardware components:

- Cisco UCSX 9508 Blade Server Chassis
- 2 Cisco UCS 6454 4<sup>th</sup> 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) UCSX-210c Compute Nodes with Intel Xeon Gold 6348 2.6-GHz 32-core processors, 1TB 3200MHz RAM for all host blades
- Cisco VIC 14425 CNA (1 per blade)
- 2 Cisco Nexus 93180YC-FX Access Switches
- 2 Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switches
- NetApp A400

---

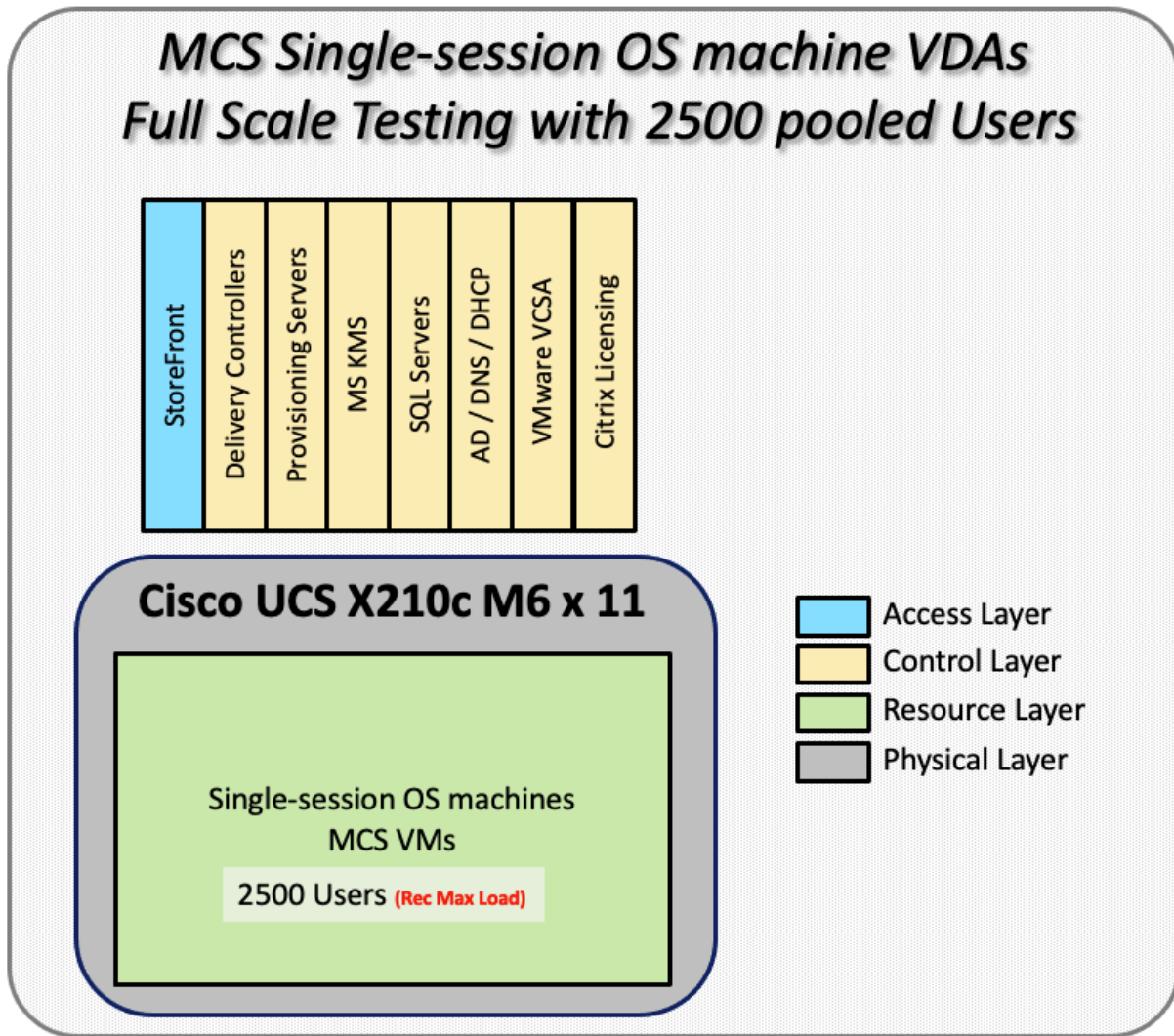
Software components:

- Cisco UCS firmware 5.0(1b)
- Netapp ONTAP 9.9
- VMware ESXi 7.0 2 for host blades
- Citrix Virtual Apps & 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**

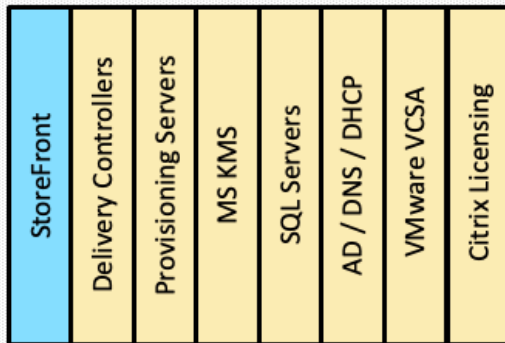
This test case validates thirty blade workloads using RDS/Citrix Virtual Apps & Desktops 7 LTSR with 2500 RDS sessions, 2500 VDI Non-Persistent sessions, and 2500 VDI Persistent sessions. Server N+1 fault tolerance is factored into this solution for each workload and infrastructure cluster.

Figure 39. Full Scale Test Configuration with 11 Blades

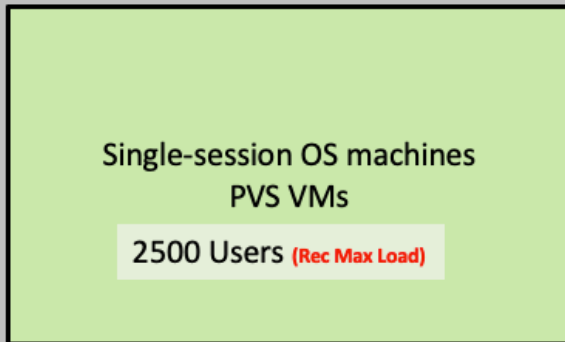






© 2013-2014 Cisco and/or its affiliates. All rights reserved.

## *PVS Single-session OS machine VDAs Full Scale Testing with 2500 pooled Users*

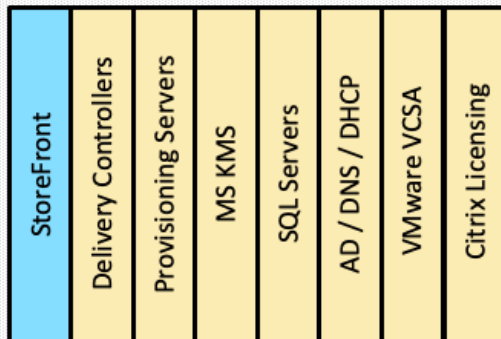


### **Cisco UCS X210c M6 x 11**



-  Access Layer
-  Control Layer
-  Resource Layer
-  Physical Layer

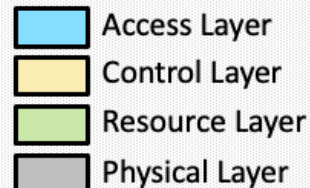
## *RDS Multi-session OS machine VDAs* *Full Scale Testing with 2600 pooled Users*



### **Cisco UCS X210c M6 x 11**

130 Multi-session OS machines  
RDS VMs

2600 Users **(Rec Max Load)**



Hardware components:

- Cisco UCSX 9508 Blade Server Chassis
- 2 Cisco UCS 6454 4<sup>th</sup> 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
- 11(RDS/VDI Host) UCSX-210c Compute Nodes with Intel Xeon Gold 6348 2.6-GHz 32-core processors, 1TB 3200MHz RAM for all host blades
- Cisco VIC 14425 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 5.0(1b)
- VMware ESXi 7.02 Update 1 for host blades
- Citrix RDS/Citrix Virtual Apps & 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 & 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 & 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 is used for all single server and scale testing. This assures that our tests represent real-world scenarios. For each of the three consecutive runs on single server tests, the same process was followed.

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 & 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 & 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 & 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; Shut-down 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 & 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 VSI<sub>max</sub> dynamic in our testing. FlexPod Data Center with Cisco UCS and Citrix RDS/Citrix Virtual Apps & 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 & Desktops Hosted Virtual Desktop (VDI) randomly assigned, non-persistent with Citrix Provisioning Services 7 LTSR and Citrix Virtual Apps & 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 environ-

---

ment 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

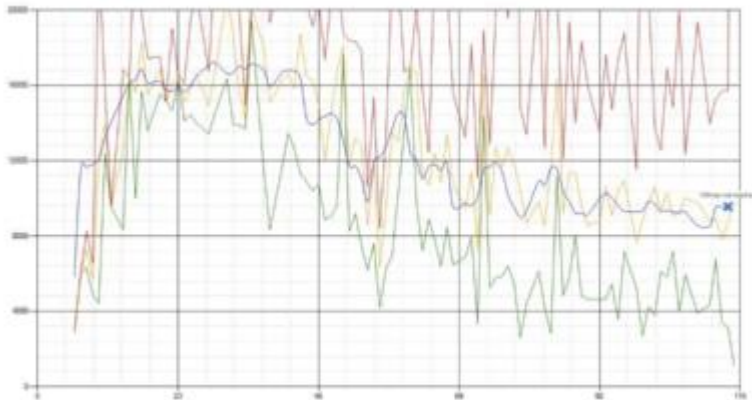
Calculates a large array of random data and spikes the CPU for a short period of time.

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 40. Sample of a VSI max response time graph, representing a normal test**



**Figure 41. Sample of a VSI test response time graph where there was a clear performance issue**



When the test is finished, VSI<sub>max</sub> can be calculated. When the system is not saturated, and it could complete the full test without exceeding the average response time latency threshold, VSI<sub>max</sub> 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 VSI<sub>max</sub> models, this weighting much better represents system performance. All actions have very similar weight in the VSI<sub>max</sub> total. The following weighting of the response times is applied.

The following actions are part of the VSI<sub>max</sub> 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 VSI<sub>max</sub> 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.

VSI<sub>max</sub> v4.1.x is reached when the VSI<sub>base</sub> + a 1000 ms latency threshold is not reached by the average VSI response time result. Depending on the tested system, VSI<sub>max</sub> 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 VSI<sub>max</sub> 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 VSI<sub>max</sub> v4.1.x, the performance of the system is not decided by the total average response time, but by the latency it 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, VSI<sub>max</sub> is not hit and the amount of sessions ran successfully. This approach is fundamentally different in comparison to previous VSI<sub>max</sub> methods, as it was always required to saturate the system beyond VSI<sub>max</sub> threshold.

Lastly, VSI<sub>max</sub> v4.1.x is now always reported with the average baseline VSI response time result. For example: “The VSI<sub>max</sub> 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. VSI<sub>max</sub> 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 an 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 VSI<sub>max</sub> v4.1.x, and the higher VSI<sub>max</sub> 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 & 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%. (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 is organized into the following subjects:

- [Single-Server Recommended Maximum Workload Testing](#)
- [Single-Server Recommended Maximum Workload for RDS with 420 Users](#)
- [Single-Server Recommended Maximum Workload for VDI Non-Persistent with 250 Users](#)
- [Single-Server Recommended Maximum Workload for VDI Persistent with 250 Users](#)
- [Single-Server Recommended Maximum Workload for VDI Non-Persistent with 250 Users with Intel Optane Persistent Memory](#)
- [Full-Scale RDS Workload Testing with 2500 Users](#)
- [Full-Scale Non-Persistent Workload Testing with 2500 Users](#)
- [Full-Scale Persistent Workload Testing with 2500 Users](#)
- [AFF A400 Storage Detailed Test Results for Cluster Scalability Test](#)
- [2500 Users Citrix HSD \(RDS\) Windows 2019 Sessions](#)
- [2500 Users Persistent Desktops Cluster Test](#)
- [2500 Users PVS Non-Persistent Desktops Cluster Test](#)
- [Scalability Considerations and Guidelines](#)
- [Scalability of Citrix Virtual Apps & Desktops 7 LTSR Configuration](#)

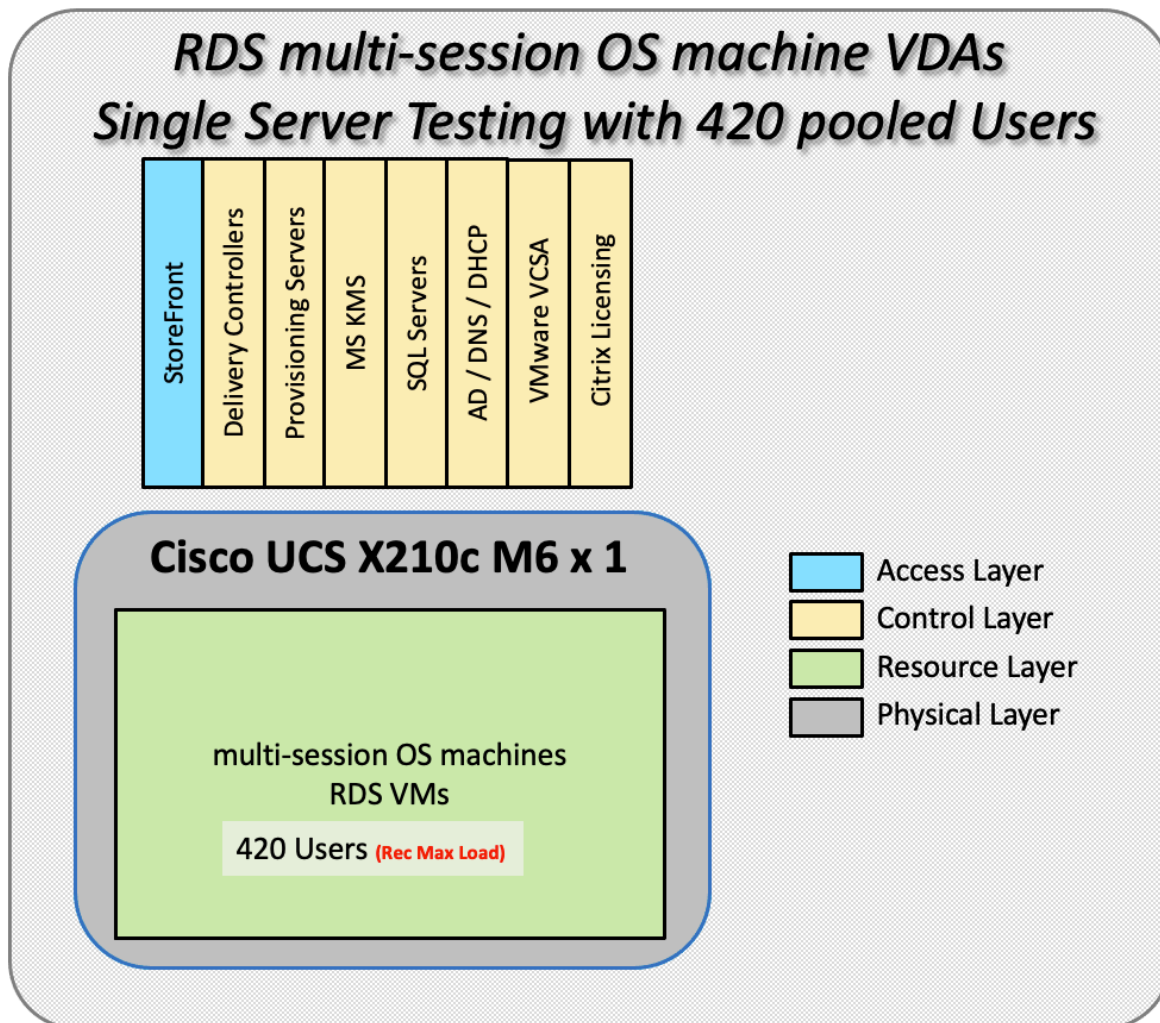
### Single-Server Recommended Maximum Workload Testing

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: 420 RDS sessions, 250 VDI Non-Persistent sessions, and 250 VDI Persistent sessions.

### Single-Server Recommended Maximum Workload for RDS with 420 Users

The following figure illustrates the single-server recommended maximum workload for RDS with 420 users.

Figure 42. Single Server Recommended Maximum Workload for RDS with 420 Users



The recommended maximum workload for a Cisco UCS x210c-M6 Compute Node with dual Intel Xeon Gold 6348 processors, 1TB 3200MHz RAM is 420 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 43. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | VSI Score

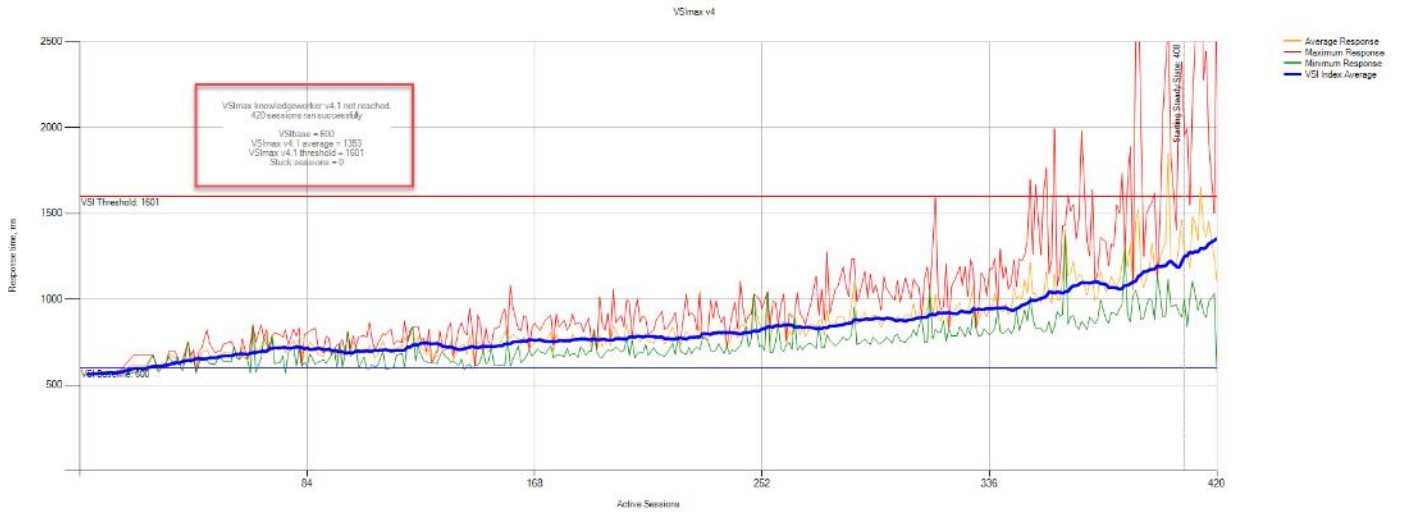


Figure 44. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | VSI Repeatability

Summary Settings VSImax v4 VSImax v4 Detailed VSImax v4 Detailed Weighted VSImax v4 Scatter UMEM IO CPU ZLC ZHC NFP NFO NSLD AppStart Log

RDS-420-03

Successfully completed Login VSI test with **420 knowledgeworker** sessions. VSImax (system saturation) was not reached. All Login VSI users completed the test.

Test result review

**420** 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
- **420** sessions were active during the test
- **0** sessions got stuck during the test (before VSImax threshold)

With **420** sessions the maximum capacity VSImax (v4.1) **knowledgeworker** was not reached with a Login VSI baseline performance score of **600**

Login VSI index average score is **500** lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance of **600** is: **Very good**

Performance data for the server running the workload as follows:

Figure 45. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | Host CPU Utilization

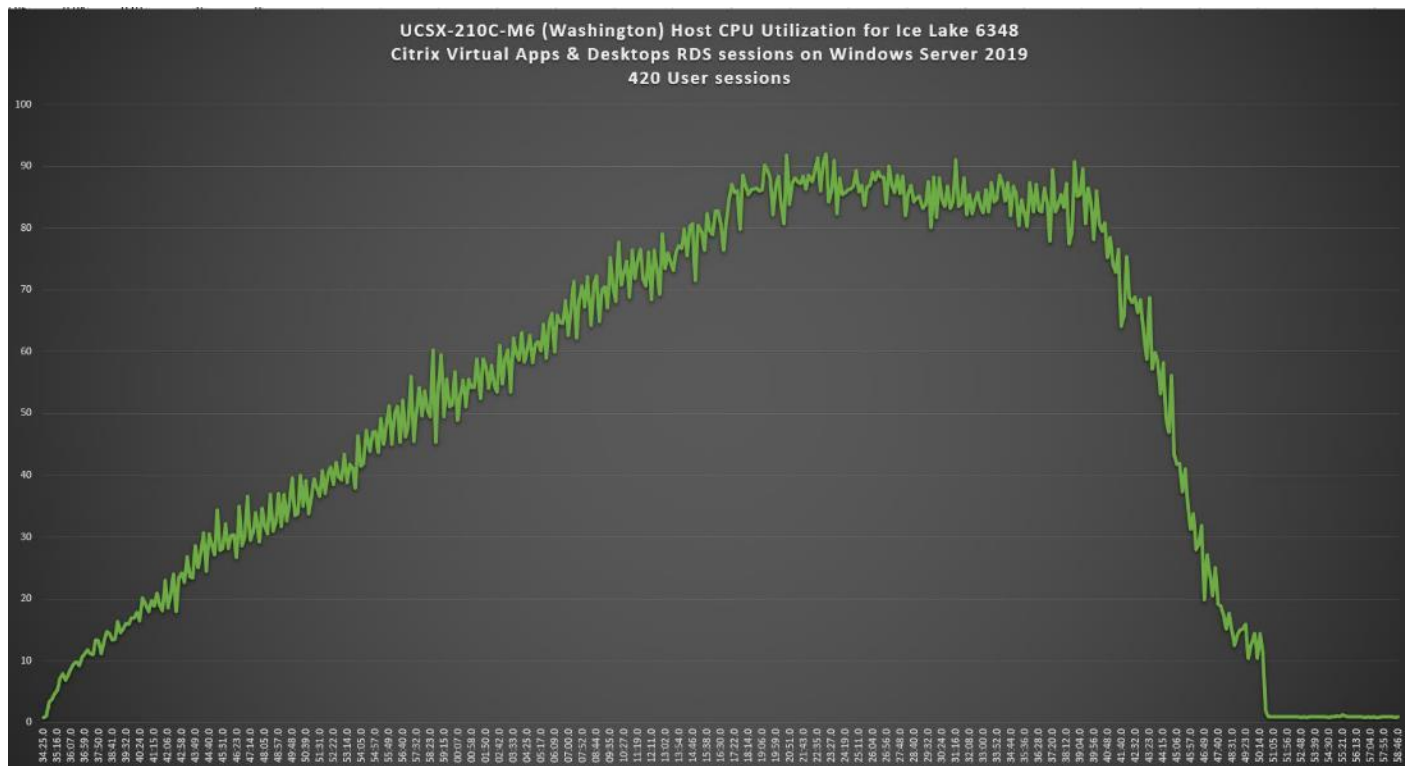


Figure 46. Single Server Recommended Maximum Workload | RDS 7 LTSR RDS | Host Memory Utilization

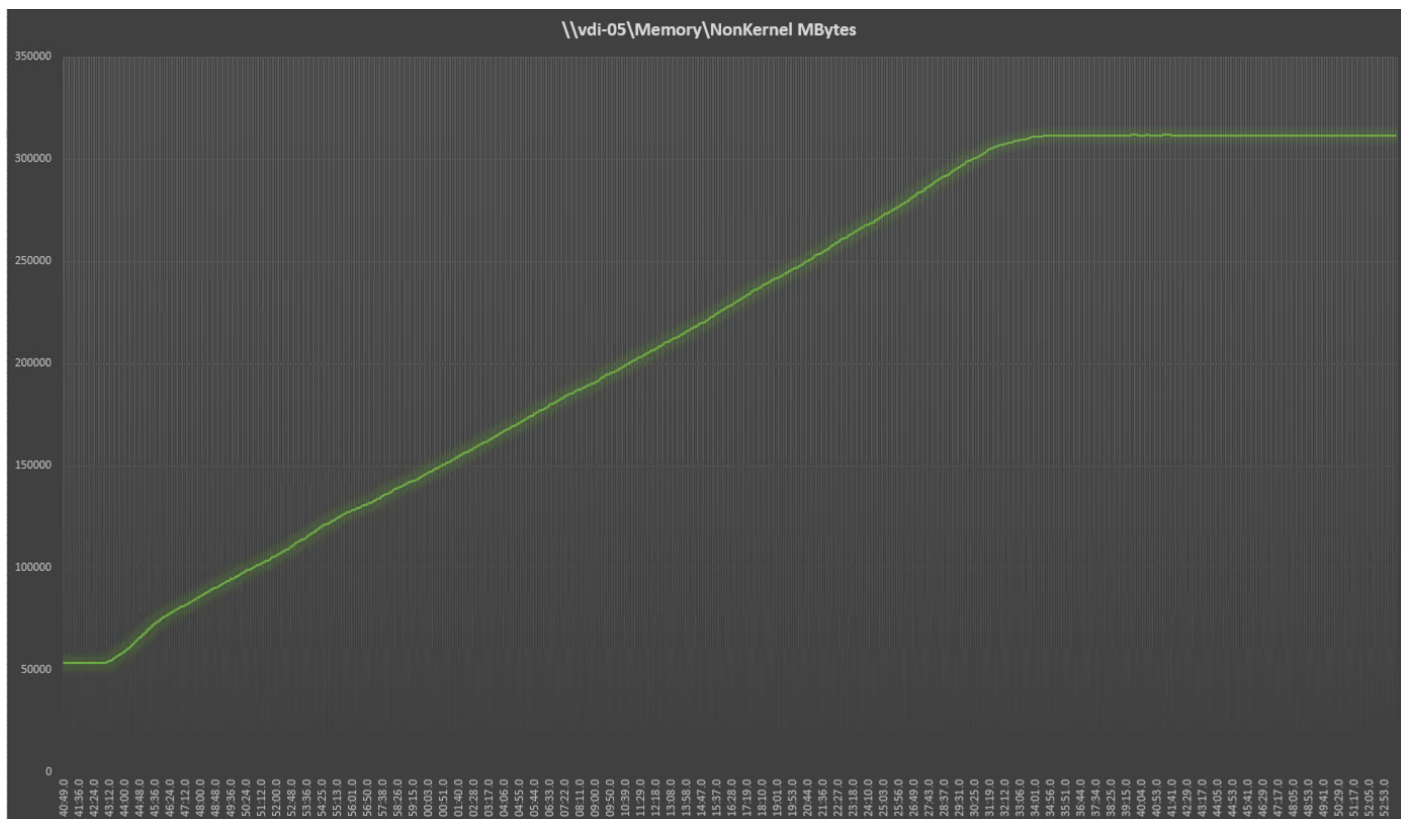
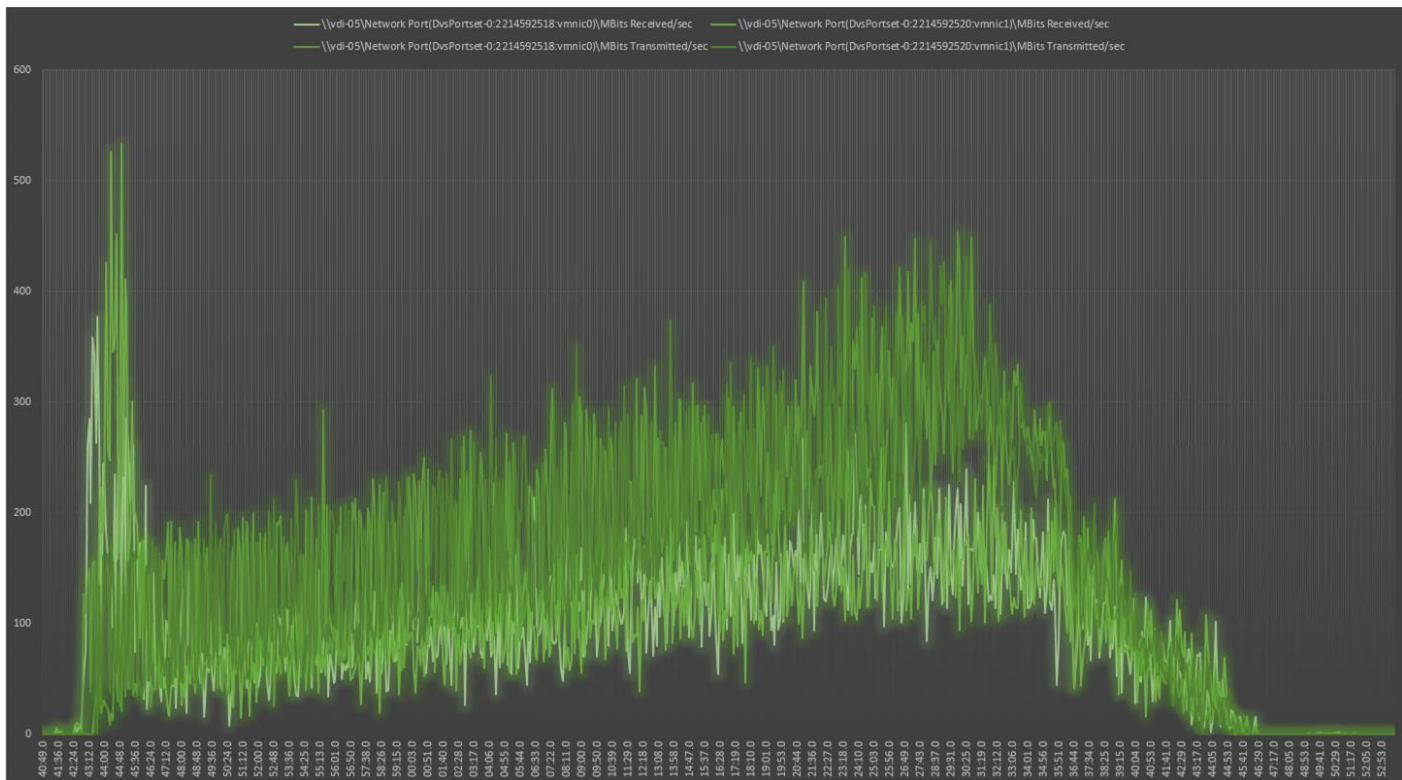


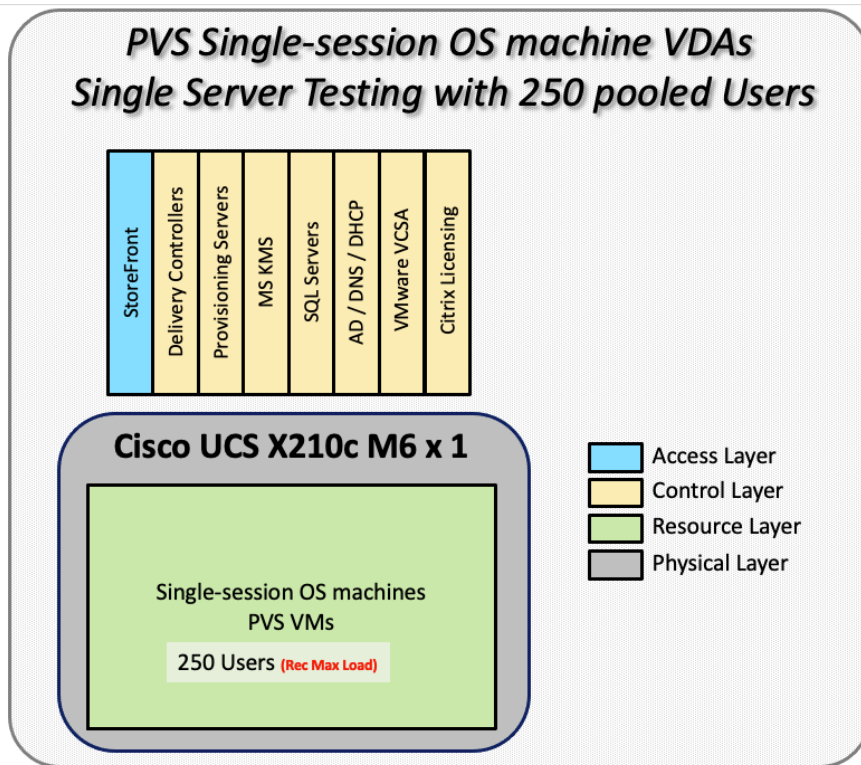
Figure 47. Single Server | RDS 7 LTSRRDS | Host Network Utilization



### Single-Server Recommended Maximum Workload for VDI Non-Persistent with 250 Users

The following figure illustrates single-server recommended maximum workload for VDI non-persistent with 250 users.

Figure 48. Single Server Recommended Maximum Workload for VDI Non-Persistent with 250 Users



The recommended maximum workload for a Cisco UCS x210c-M6 Compute Node with dual Intel Xeon Gold 6348 processors, 1TB 3200MHz RAM is 250 Windows 10 64-bit virtual machines with 2 vCPU and 4GB RAM. Login VSI and node performance data as follows:

Figure 49. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | VSI Score

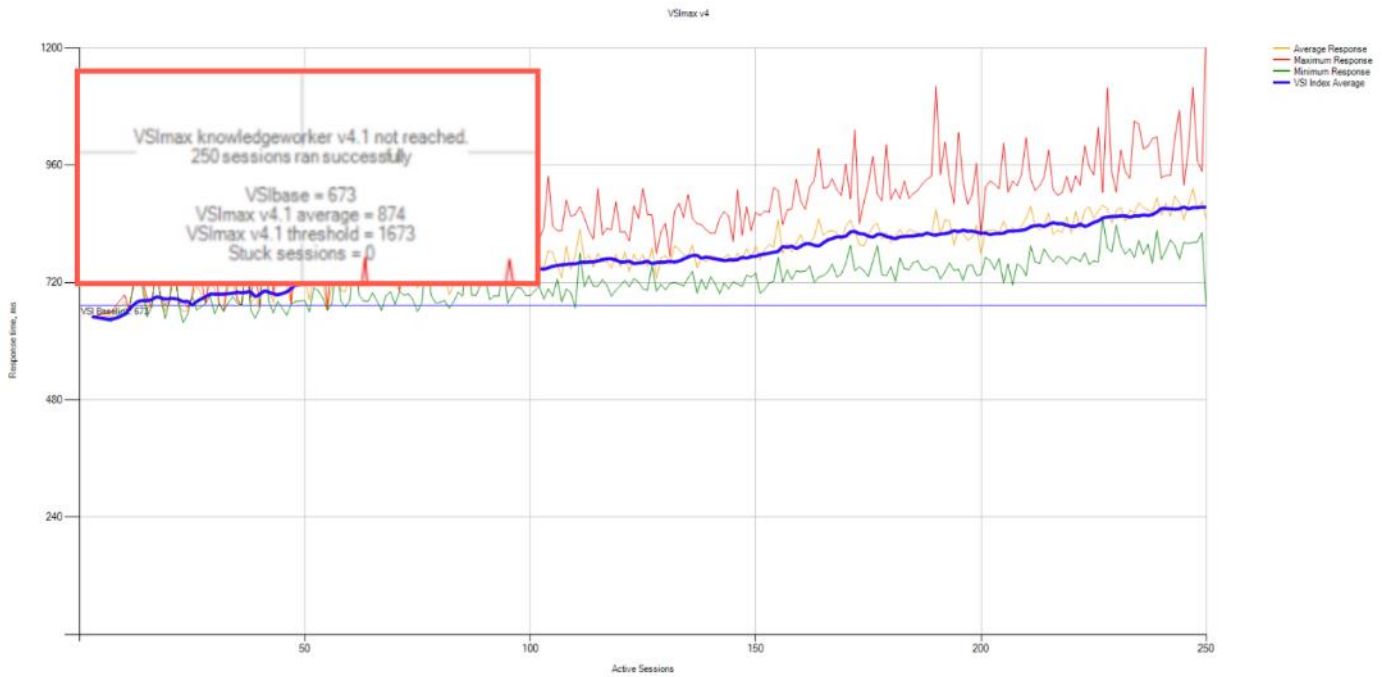
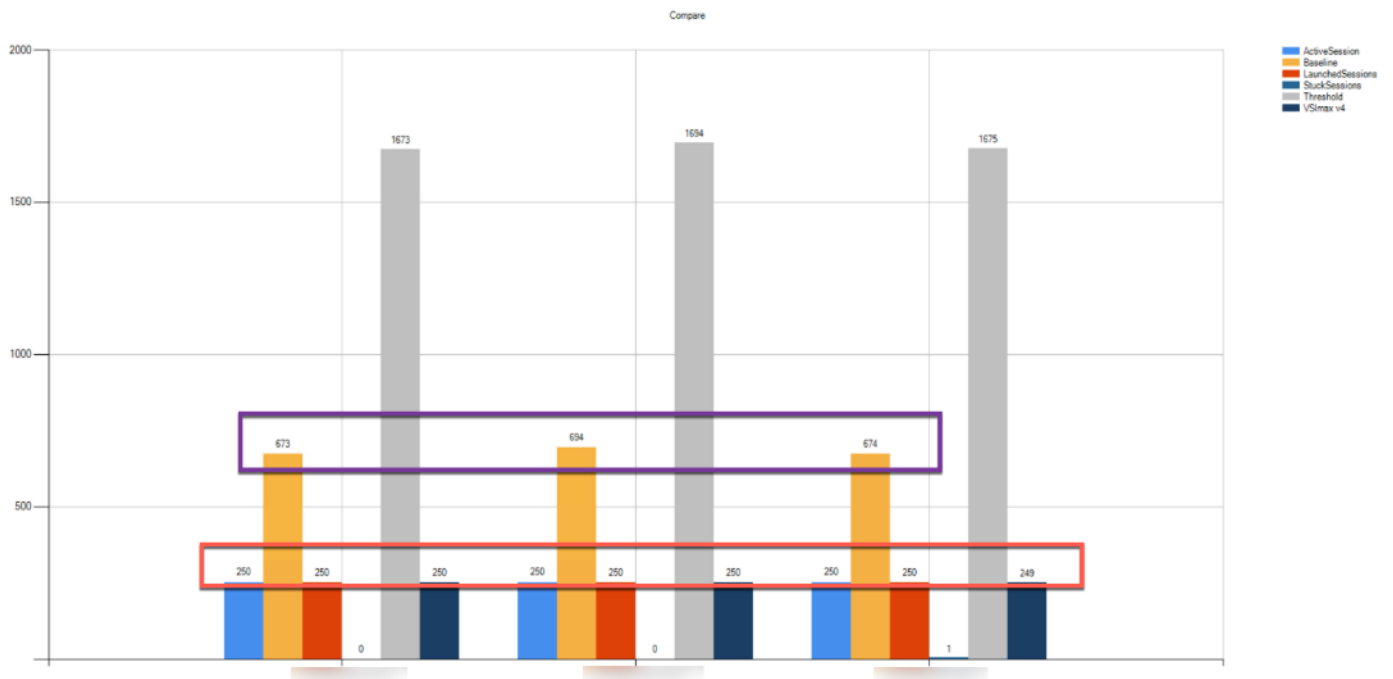


Figure 50. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | VSI Repeatability



Performance data for the server running the workload as follows:

Figure 51. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | Host CPU Utilization

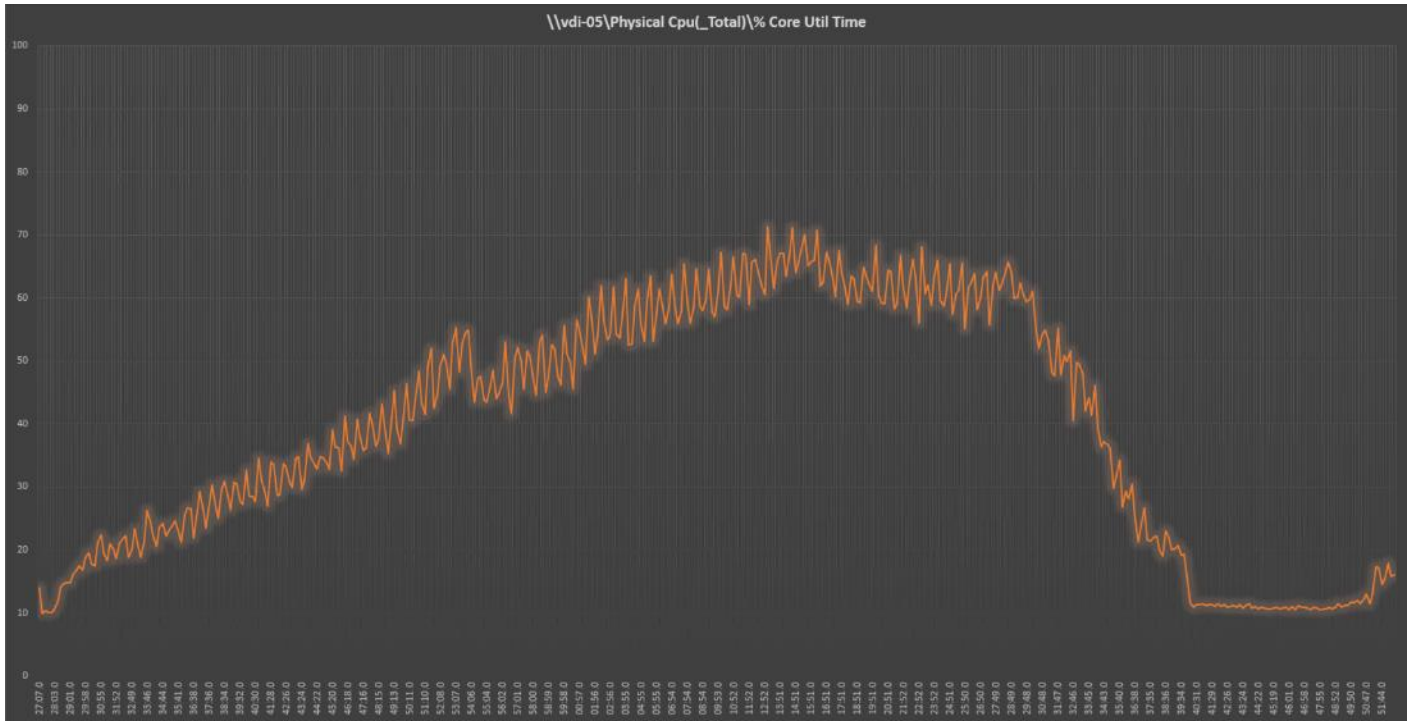


Figure 52. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | Host Memory Utilization

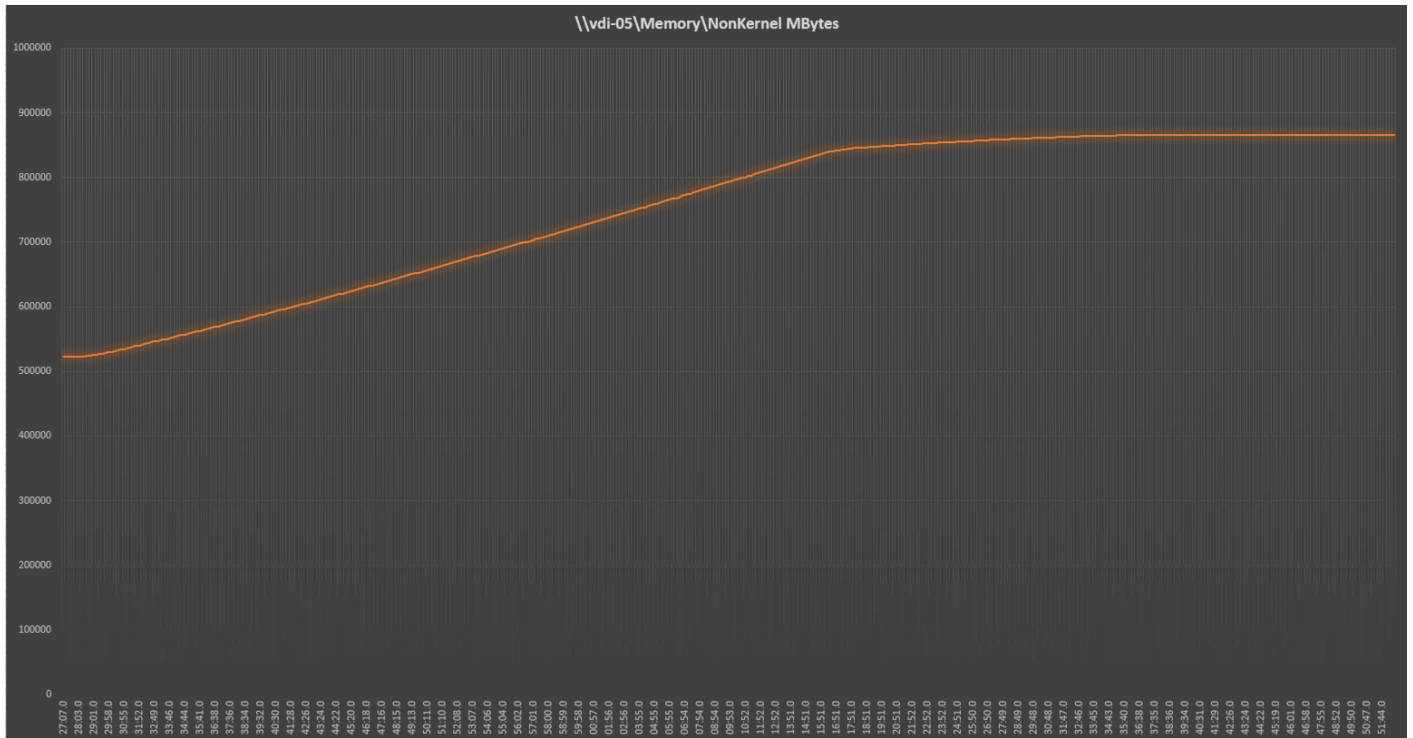
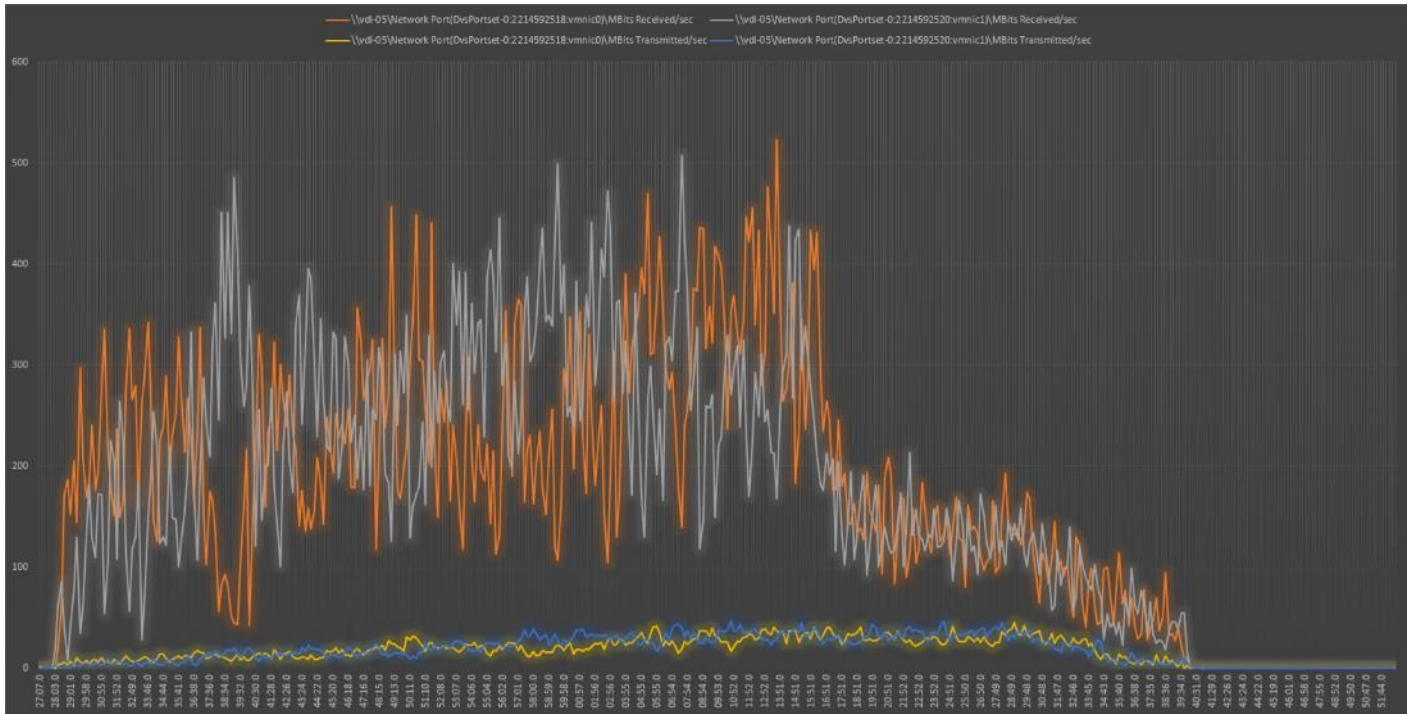


Figure 53. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | Host Network Utilization

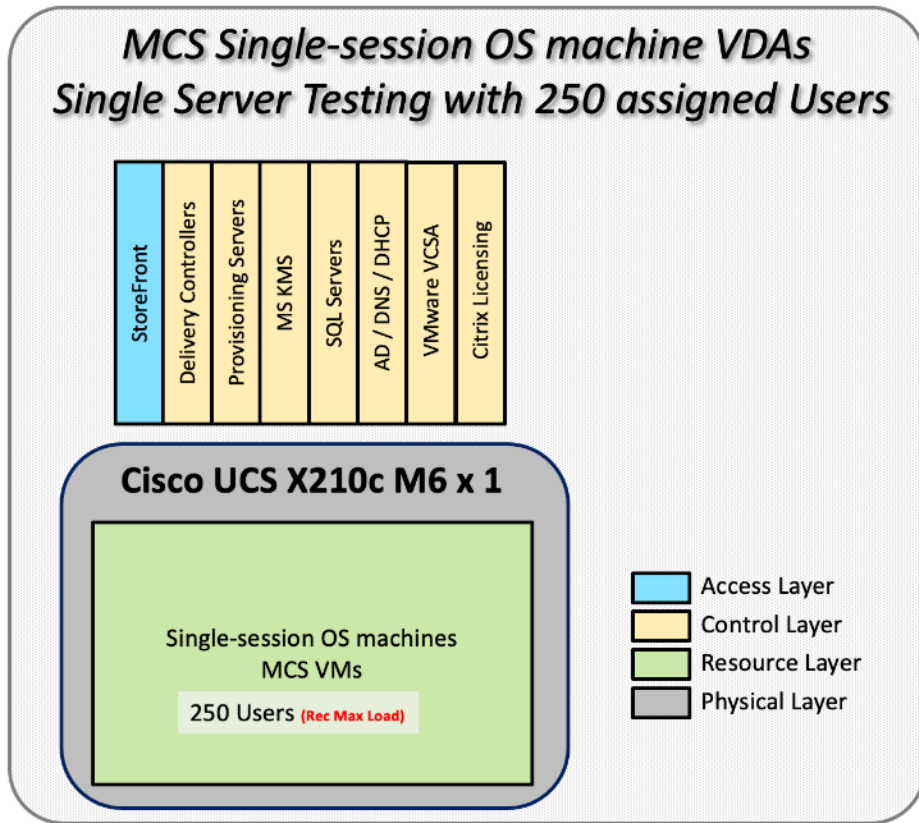


### Single-Server Recommended Maximum Workload for VDI Persistent with 250 Users

The following figure illustrates the single-server recommended maximum workload for VDI persistent with 250 users.



Figure 54. Single Server Recommended Maximum Workload for VDI Persistent with 250 Users



The recommended maximum workload for a Cisco UCS x210c-M6 Compute Node with dual Intel Xeon Gold 6348 processors, 1TB 3200MHz RAM is 250 Windows 10 64-bit virtual machines with 2 vCPU and 4GB RAM. Login VSI and blade performance data as follows:

Figure 55. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-P | VSI Score

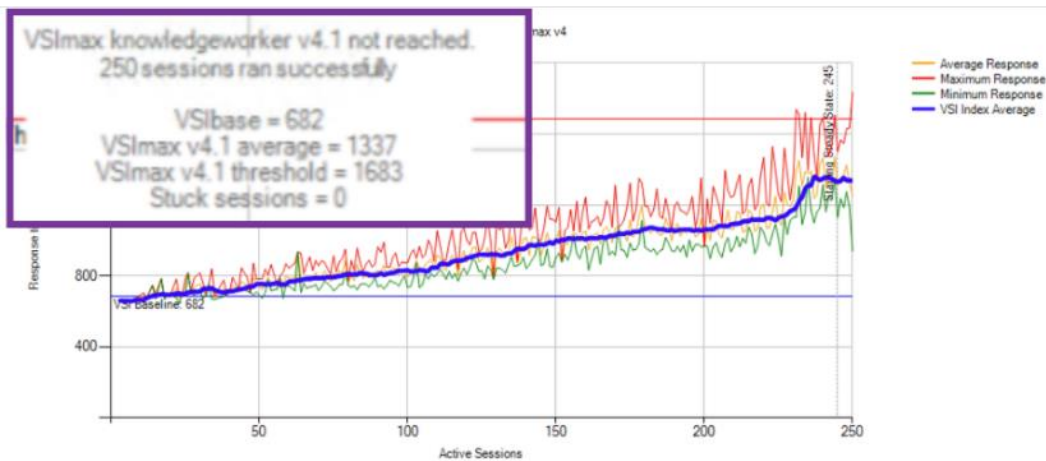
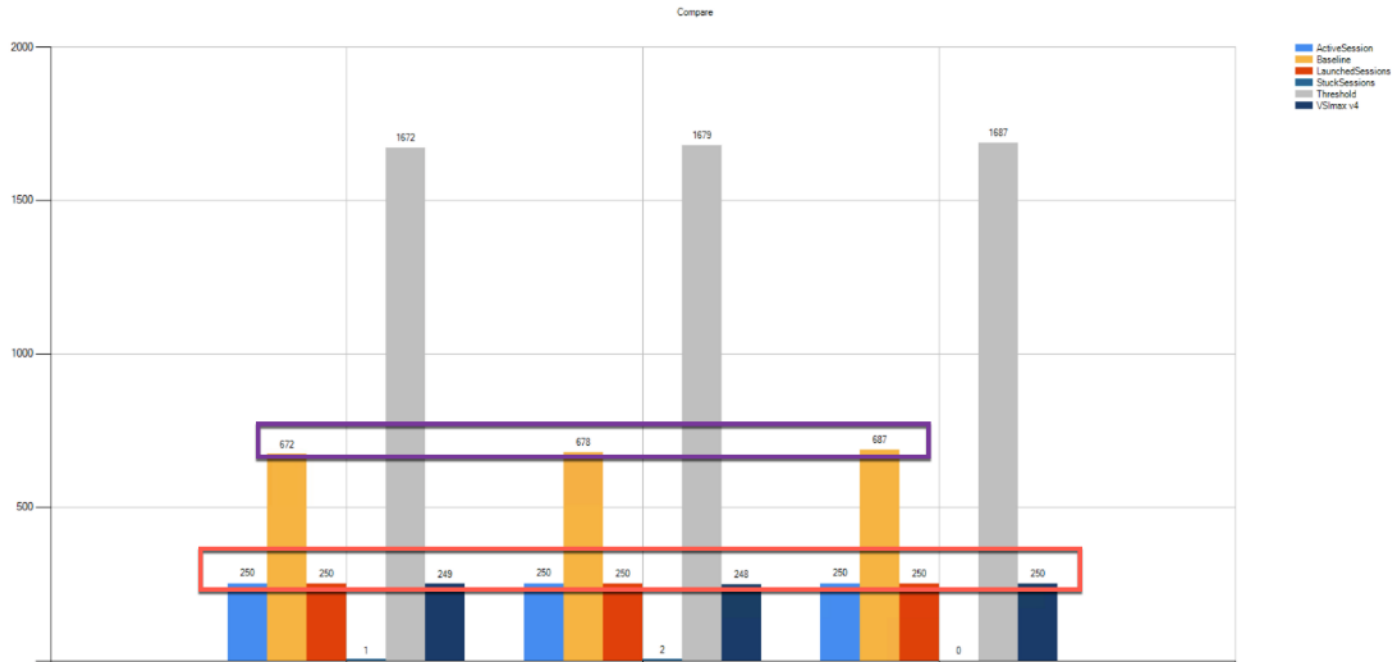


Figure 56. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-P | VSI Repeatability



Performance data for the server running the workload as follows:

Figure 57. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-P | Host CPU Utilization

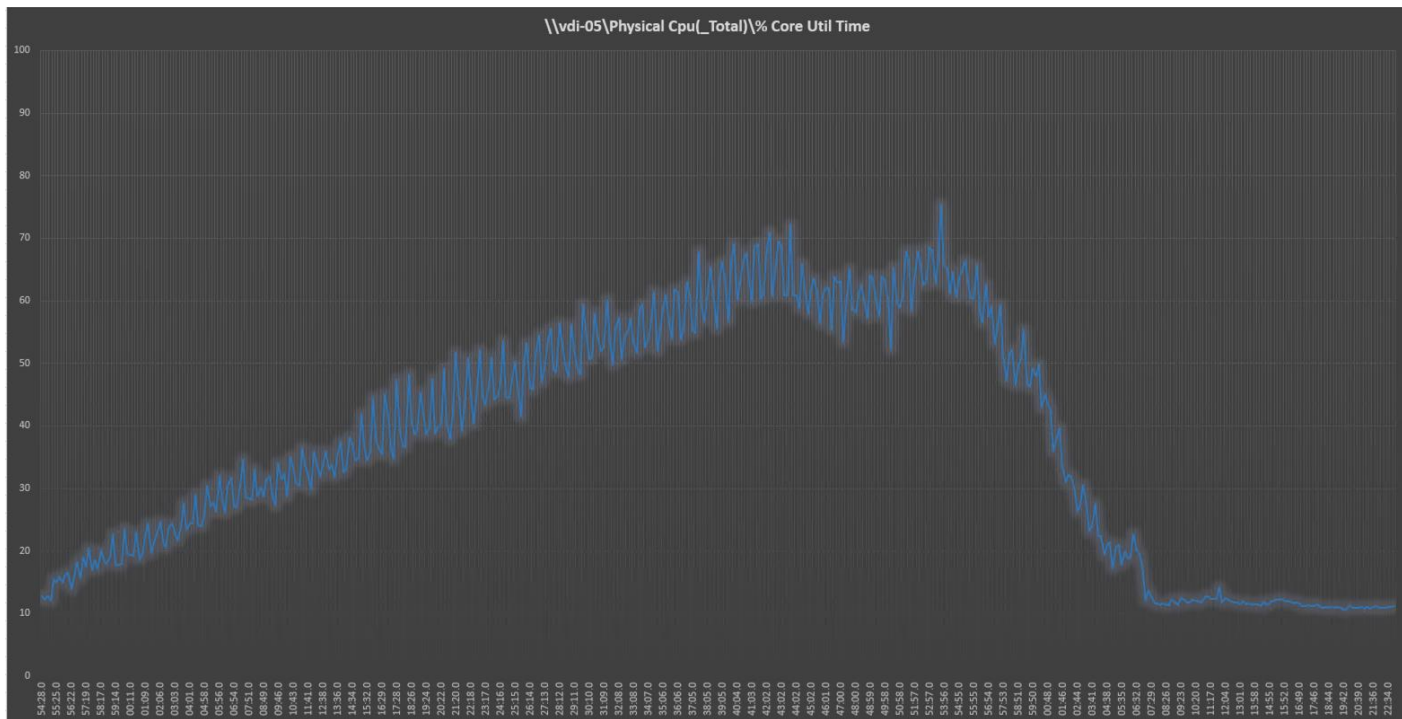


Figure 58. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-P | Host Memory Utilization

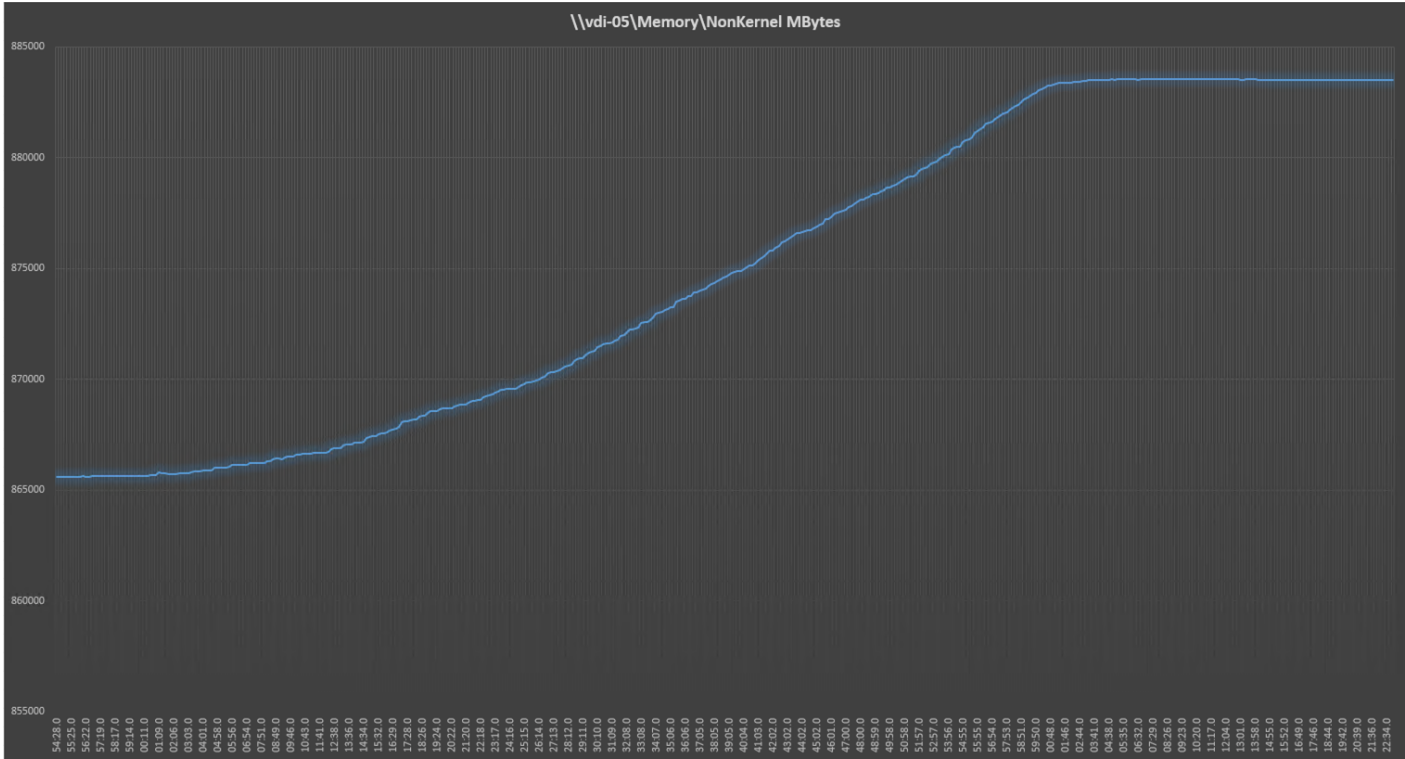
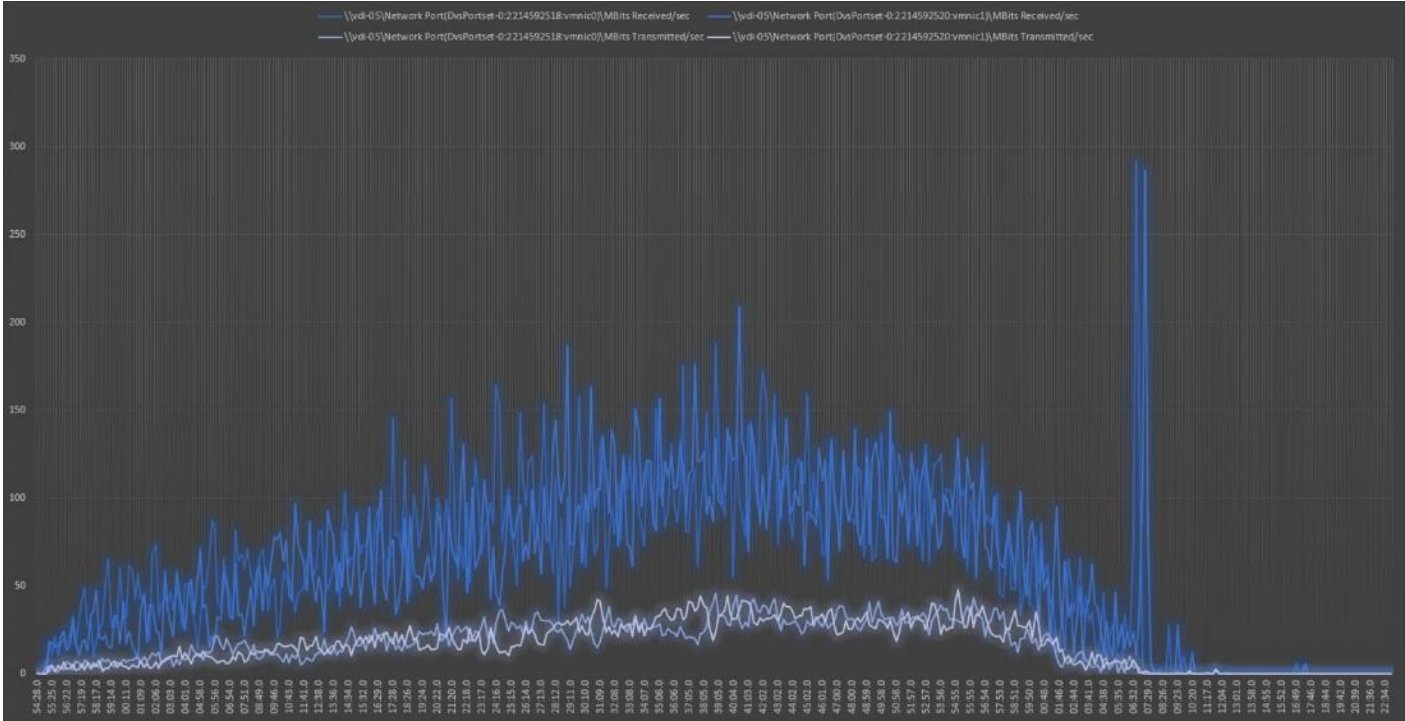


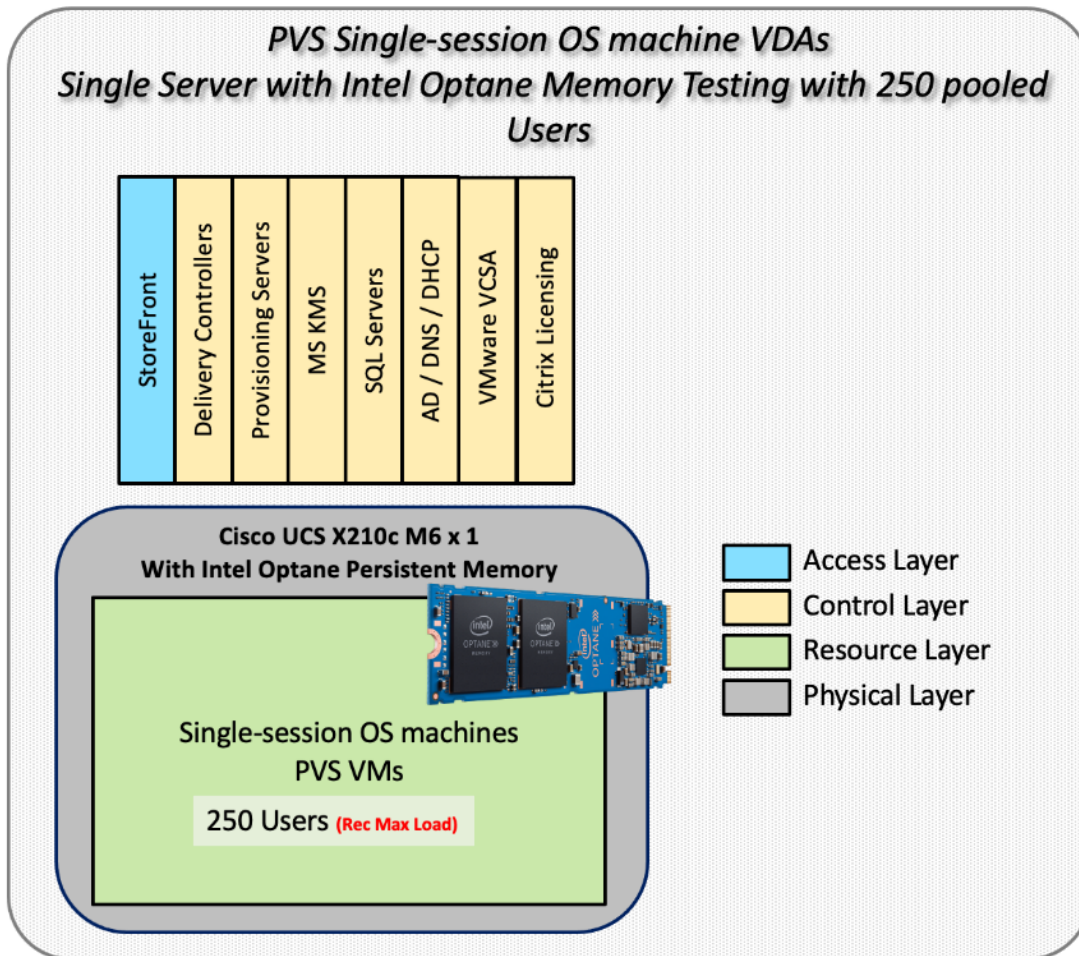
Figure 59. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-P | Host Network Utilization



## Single-Server Recommended Maximum Workload for VDI Non-Persistent with 250 Users with Intel Optane Persistent Memory

The following figure illustrates the single-server recommended maximum workload for VDI non-persistent with 250 users.

Figure 60. Single Server Recommended Maximum Workload for VDI non-persistent with 250 Users



The recommended maximum workload for a Cisco UCS x210c-M6 Compute Node with dual Intel Xeon Gold 6348 processors, 1TB of Intel Optane Memory is 250 Windows 10 64-bit virtual machines with 2 vCPU and 4GB RAM. Login VSI and node performance data as follows:

Figure 61. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | VSI Score

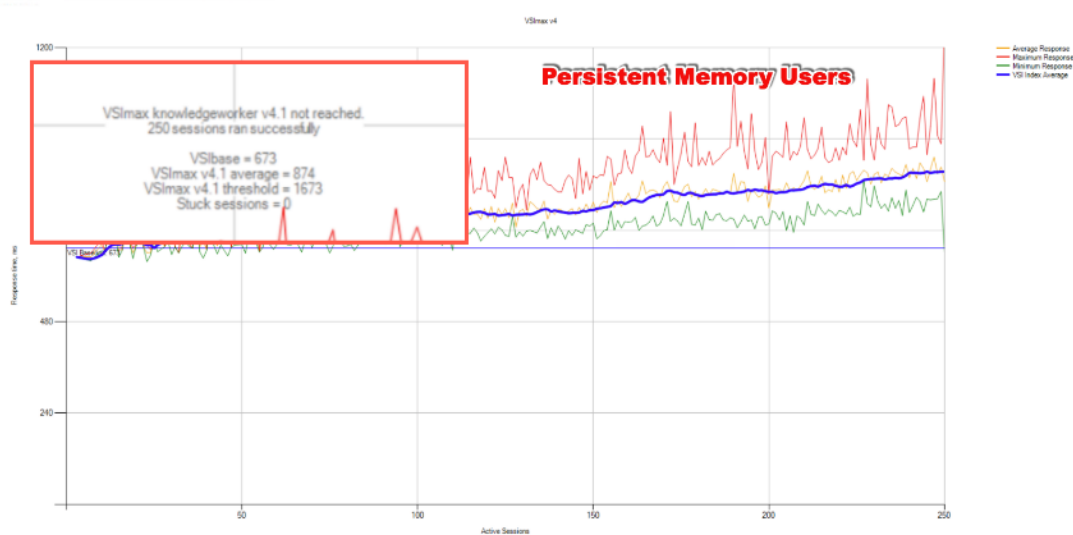


Figure 62.

Figure 63. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | VSI Summary

Summary Settings VSImax v4 VSImax v4 Detailed VSImax v4 Detailed Weighted VSImax v4 Scatter UMEM IO CPU ZLC ZHC NFP NFO NSLD AppStart

SS-PMEM-03-Fixed

Successfully completed Login VSI test with **250 knowledgeworker** sessions. VSImax (system saturation) was not reached. All Login VSI users completed the test.

Test result review

250 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
- 250 sessions were active during the test
- 0 sessions got stuck during the test (before VSImax threshold)

Persistent Memory Users

With 250 sessions the maximum capacity VSImax (v4.1) **knowledgeworker** was not reached with a Login VSI baseline performance score of 673

Login VSI index average score is 825 lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance of **673** is: **Very good**

Performance data for the server running the workload as follows:



Figure 64. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | Host CPU Utilization

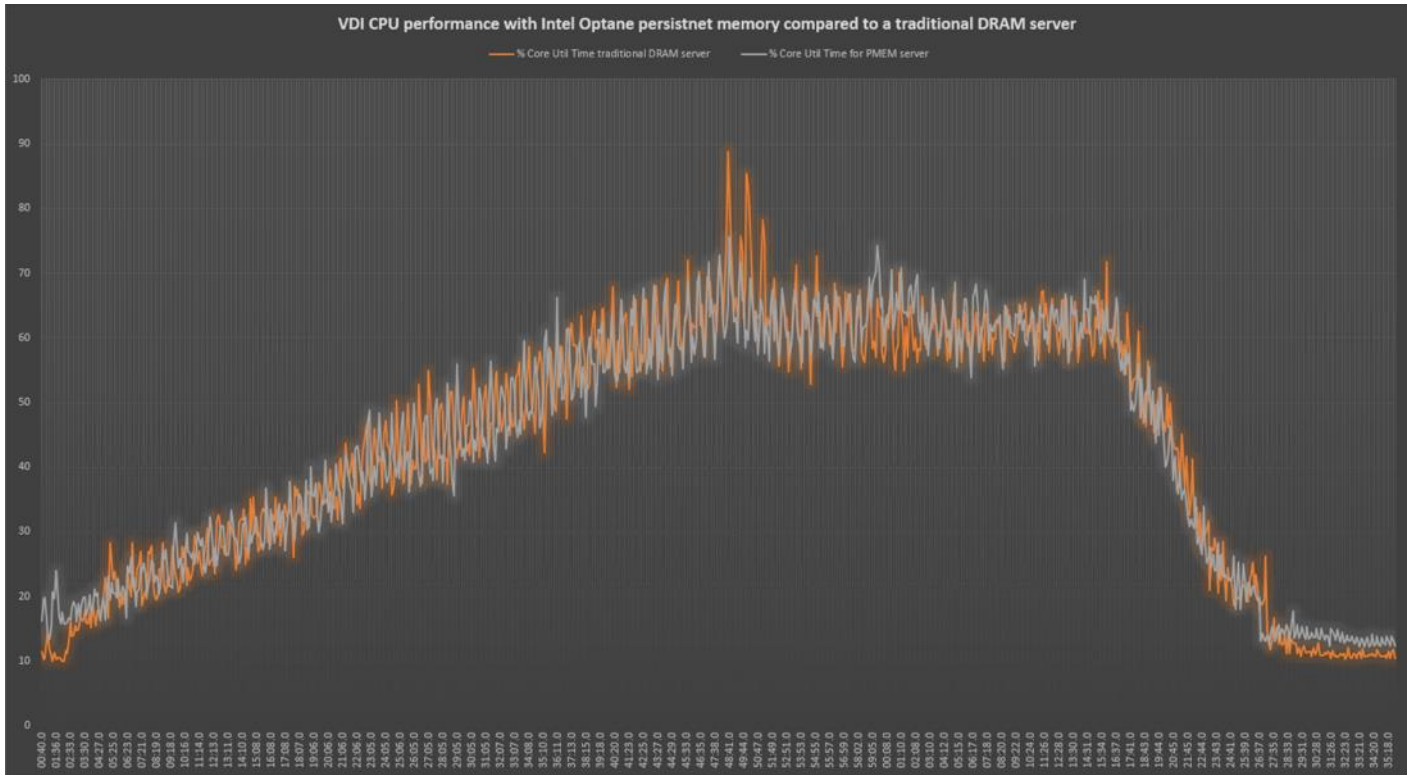
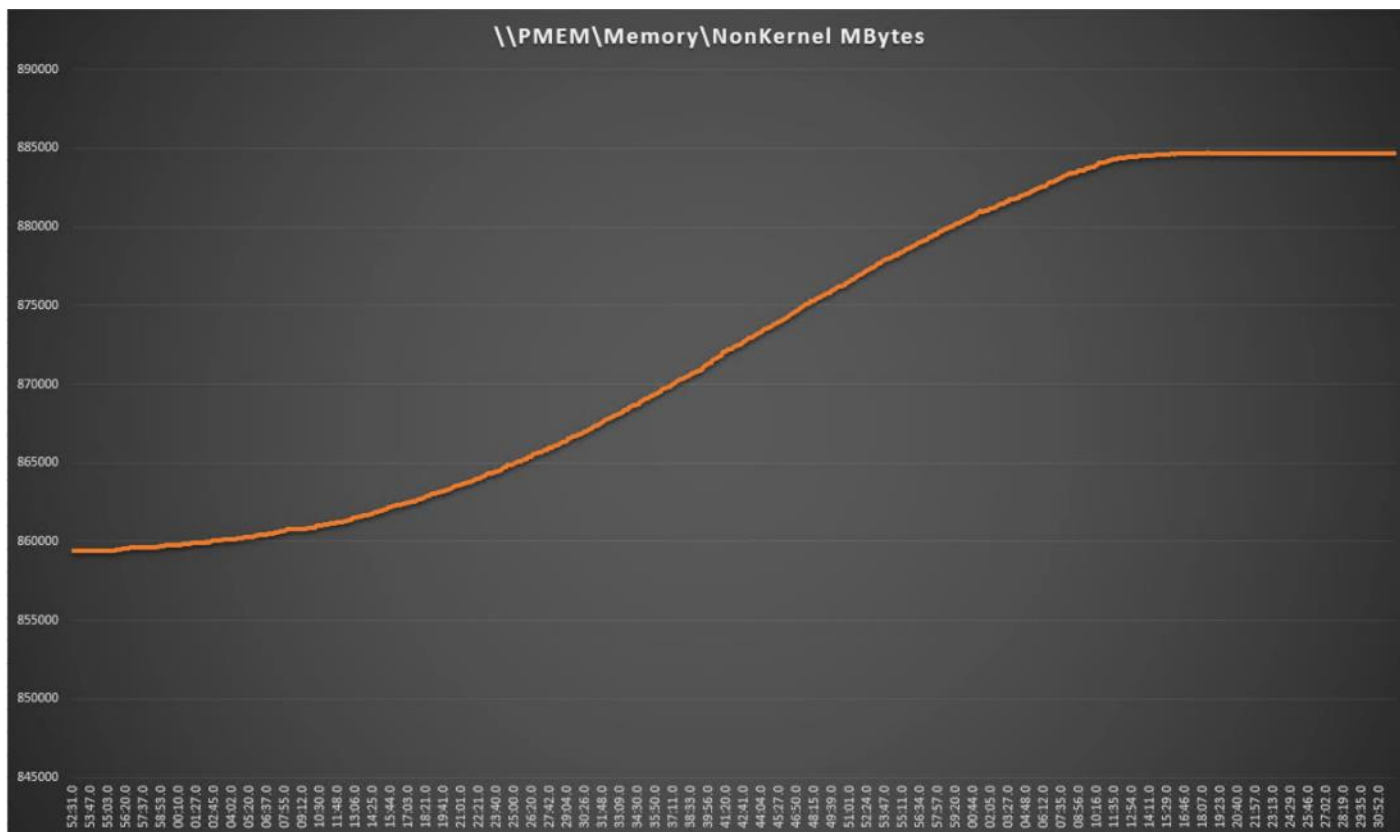


Figure 65. Single Server | Citrix Virtual Apps & Desktops 7 LTSR VDI-NP | Host Memory Utilization

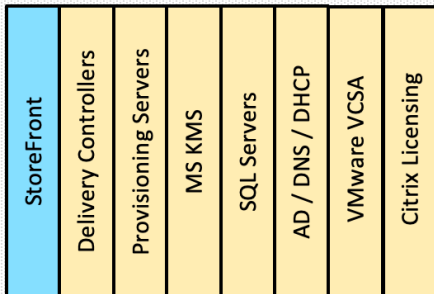


## Full-Scale RDS Workload Testing with 2500 Users

This section shows the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. The full-scale testing with 2500 users comprised of: 2500 Hosted Shared Desktop Sessions using 11 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.

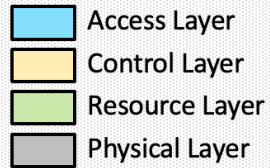
## RDS Multi-session OS machine VDAs Full Scale Testing with 2500 pooled Users



### Cisco UCS X210c M6 x 11

130 Multi-session OS machines  
RDS VMs

2500 Users (Rec Max Load)



The configured system efficiently and effectively delivered the following results.



Figure 66. Full Scale | 2500 RDS Users | VSI Score

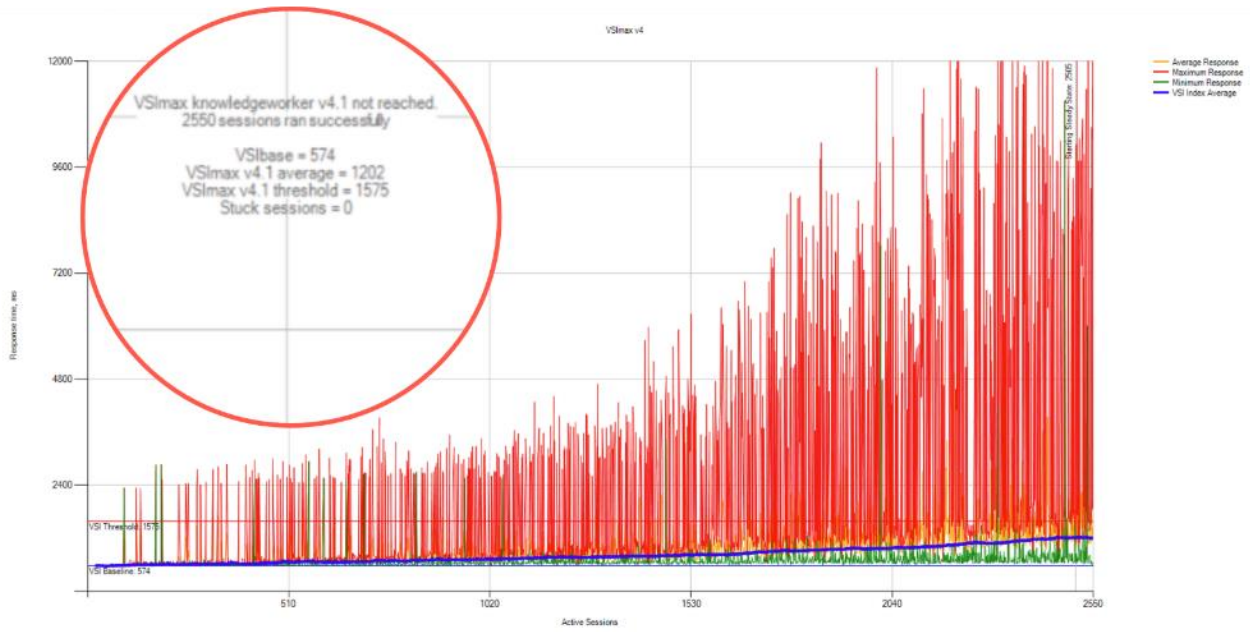


Figure 67. Full Scale | 2500 RDS Users | VSI Repeatability

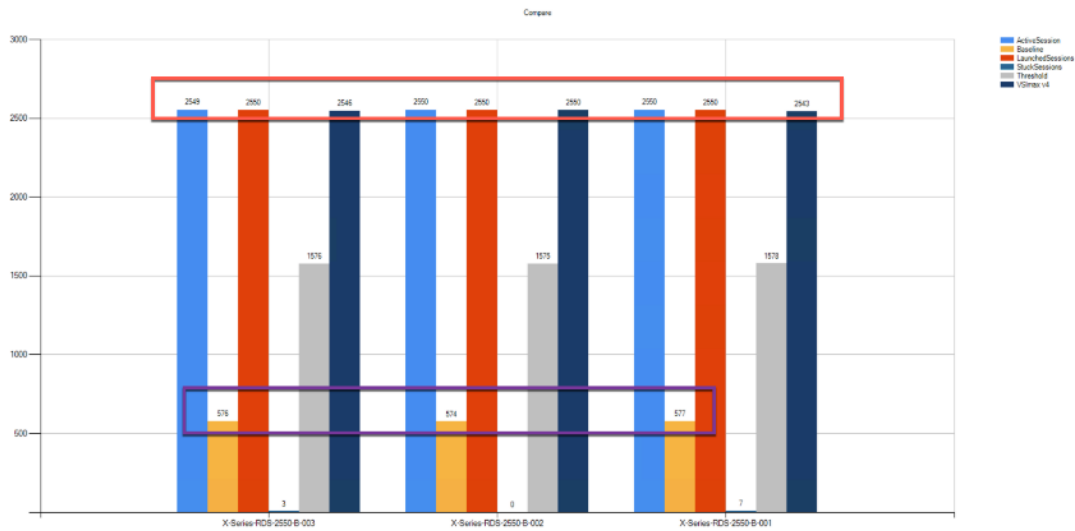


Figure 68. Full Scale | 2500 RDS Users | RDS Hosts | Host CPU Utilization

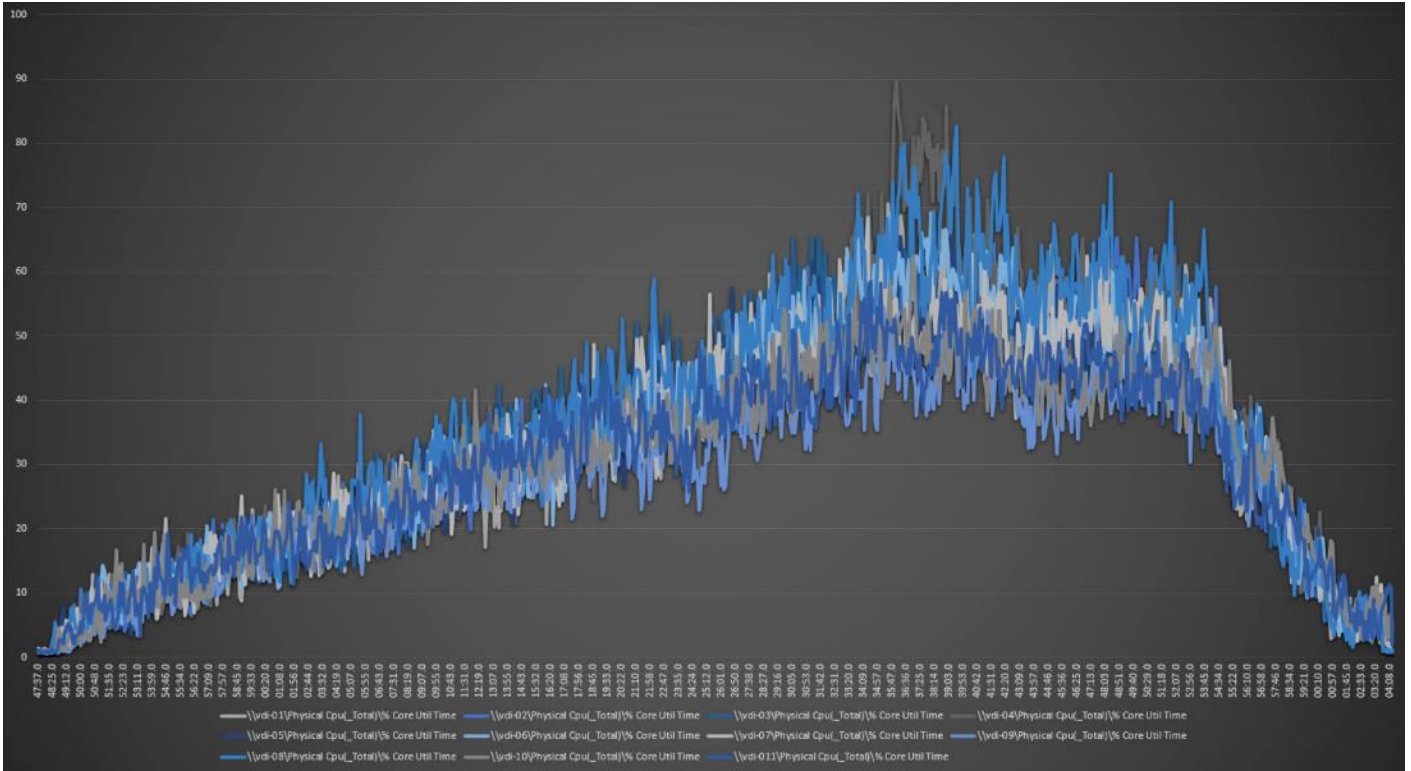
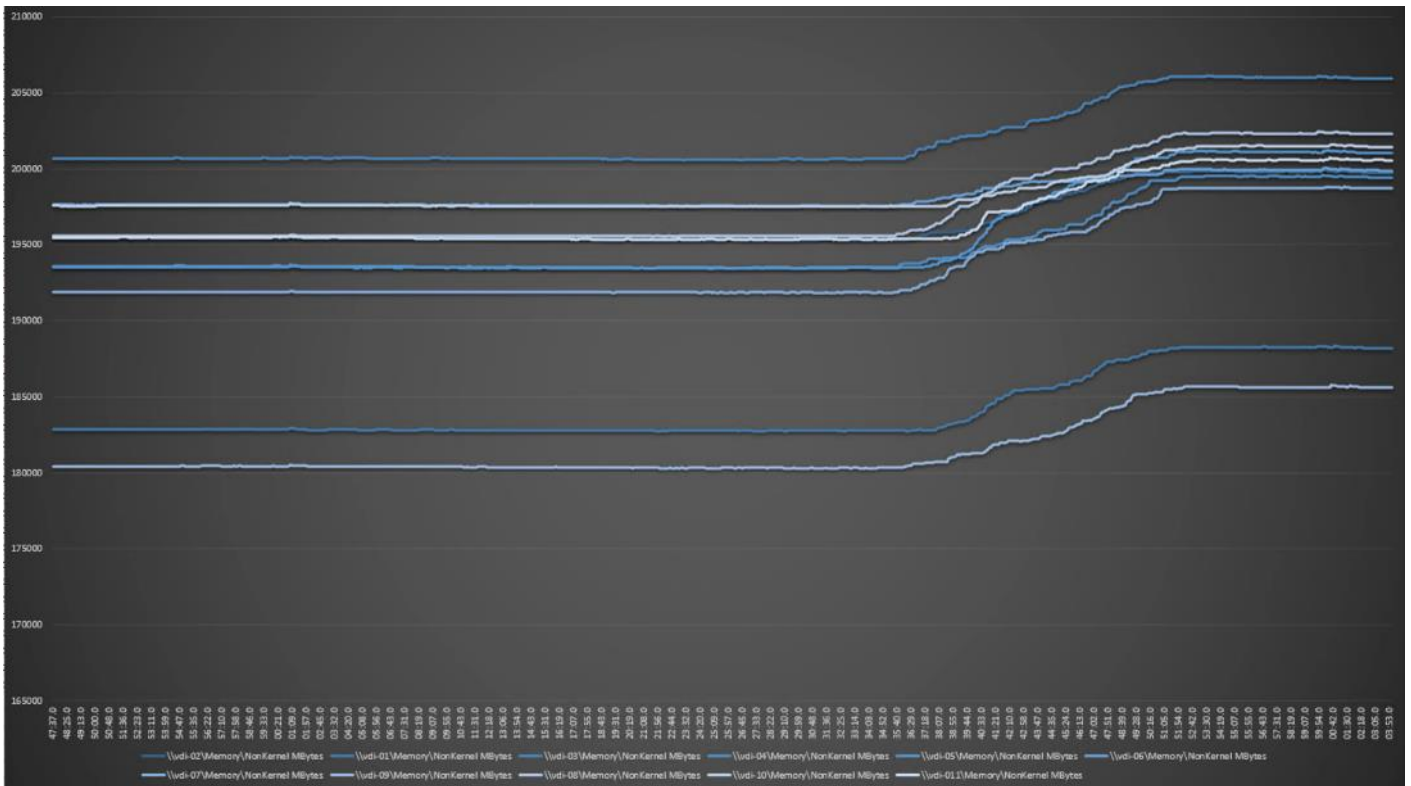


Figure 69. Full Scale | 2500 RDS Users | RDS Hosts | Host Memory Utilization

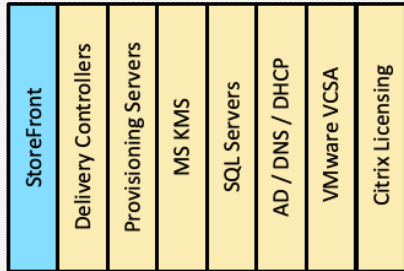


## Full-Scale Non-Persistent Workload Testing with 2500 Users

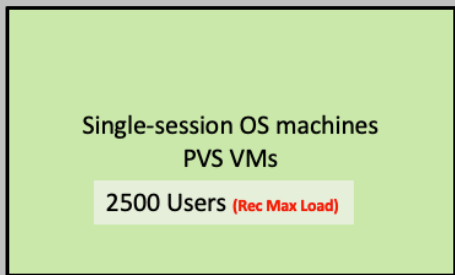
This section shows the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. The full-scale testing with 2500 users comprised of: 2500 Hosted Virtual Desktops using 11 compute nodes.

The combined mixed workload for the solution is 2500 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.

## PVS Single-session OS machine VDAs Full Scale Testing with 2500 pooled Users



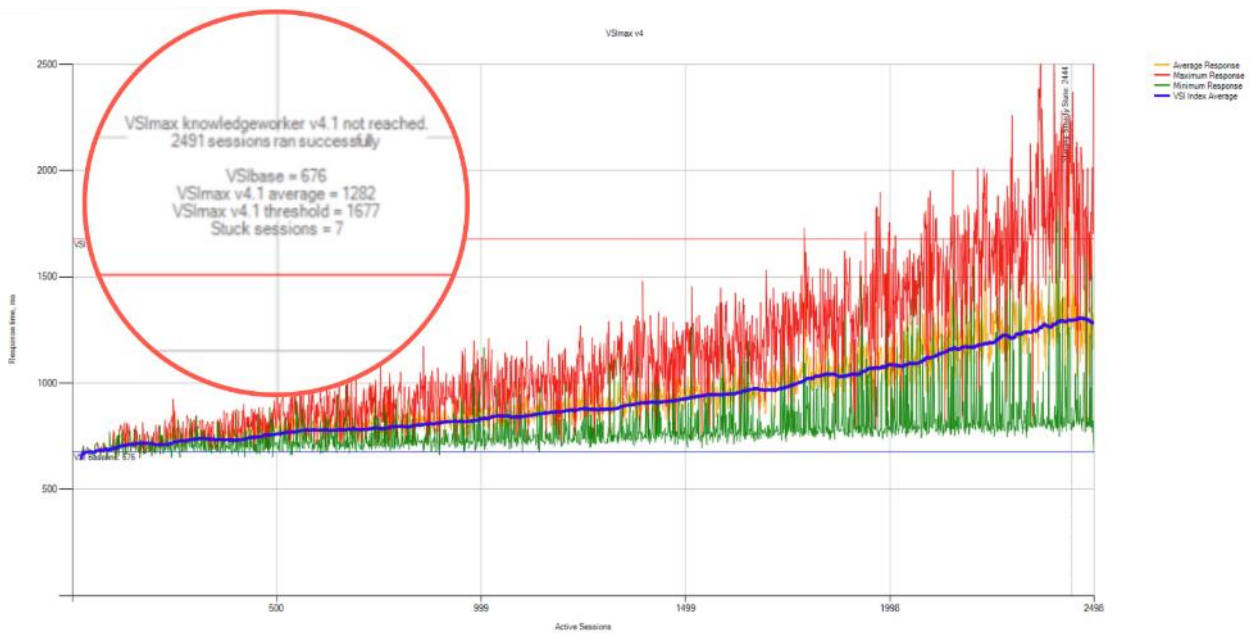
### Cisco UCS X210c M6 x 11



- Access Layer
- Control Layer
- Resource Layer
- Physical Layer

The configured system efficiently and effectively delivered the following results.

Figure 70. Full-Scale | 2500 non-persistent Users | VSI Score



## X-VDI-NP-002

Successfully completed Login VSI test with **2491 knowledgeworker** sessions. VSImax (system saturation) was not reached.

### Test result review

**2500** sessions were configured to be launched in **2880** seconds.

In total **9** sessions failed during the test:

- **0** sessions was/were not successfully launched
- **2** launched sessions failed to become active
- **2498** sessions were active during the test
- **7** sessions got stuck during the test (before VSImax threshold) > [Click Here](#)

With **2491** sessions the maximum capacity VSImax (v4.1) **knowledgeworker** was not reached with a Login VSI baseline performance score of **676**

Login VSI index average score is **515** lower than threshold. It might be possible to launch more sessions in this configuration.

Baseline performance of **676** is: **Very good**

Figure 71. Full-Scale | 2500 Non-persistentUsers | VSI Repeatability

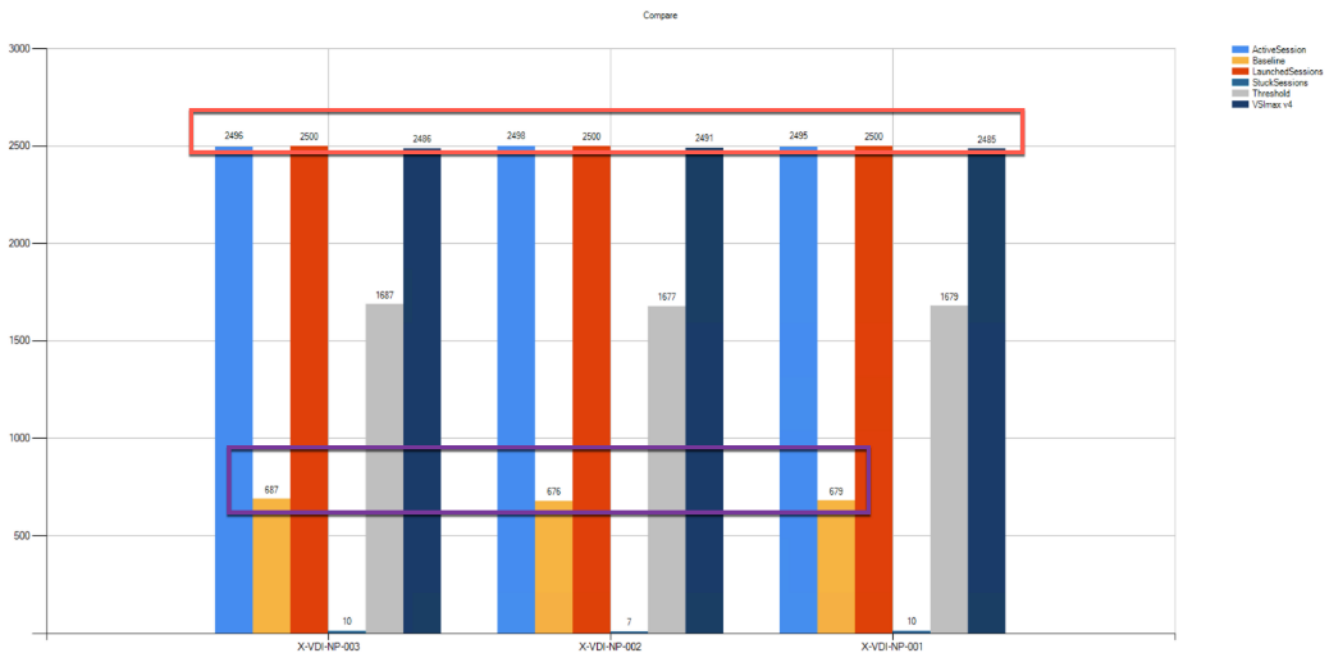
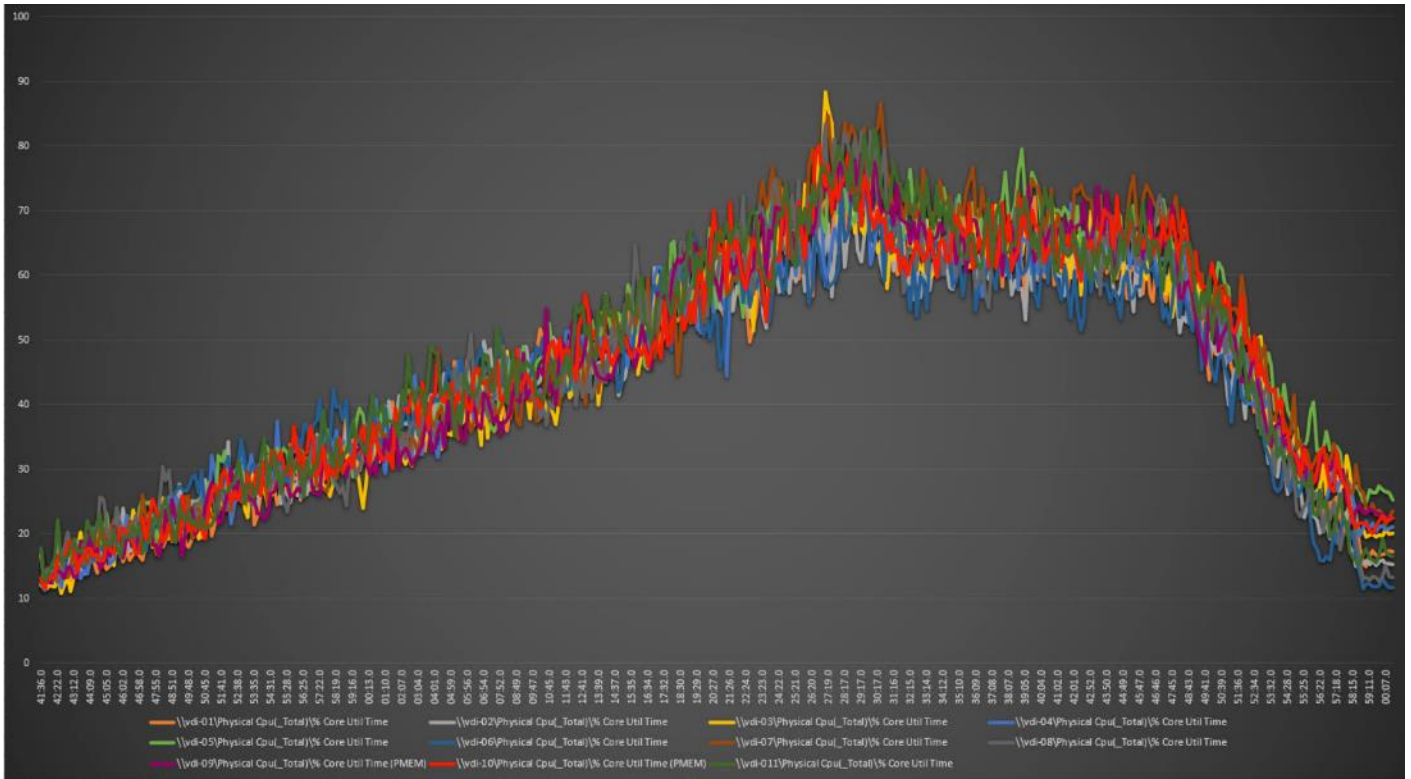
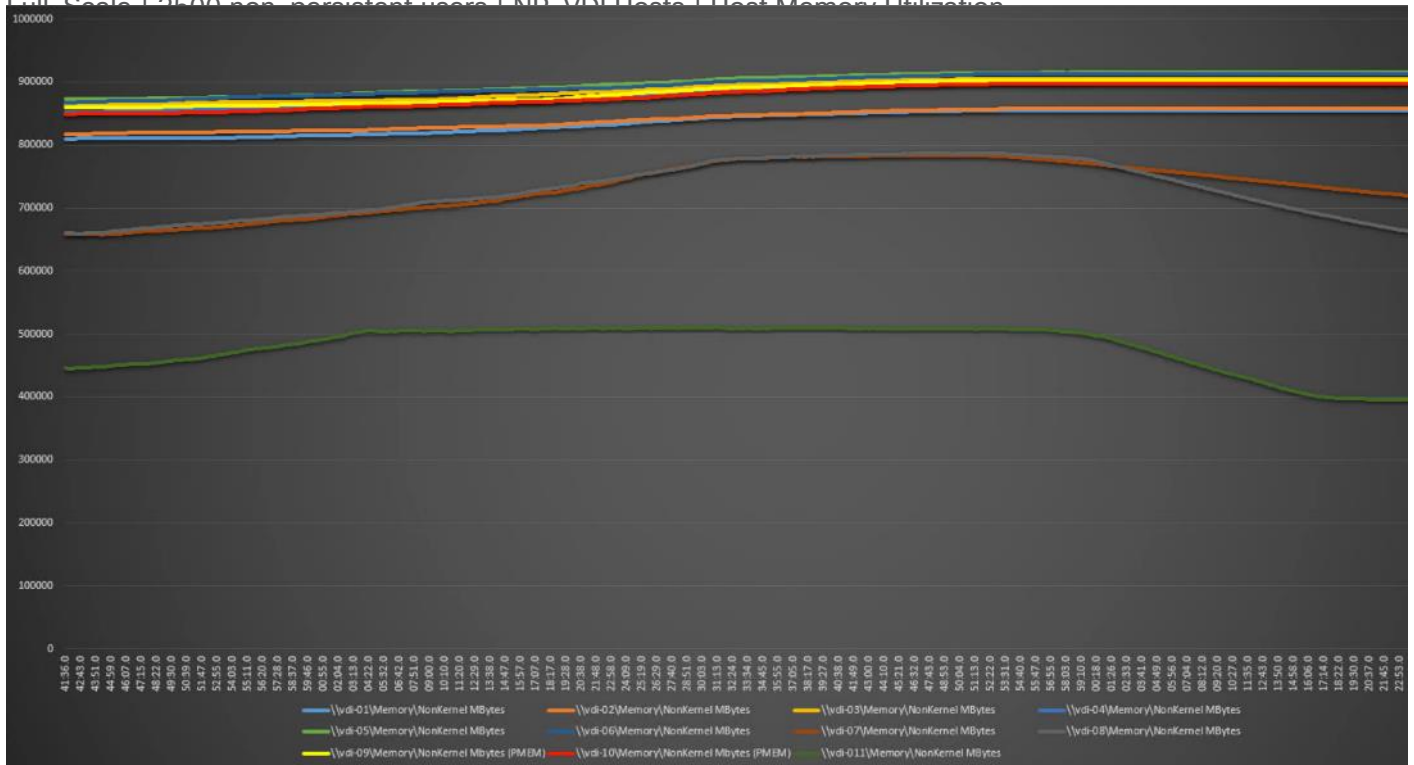


Figure 72. Full-Scale | 2500 non-persistent users | NP-VDI Hosts | Host CPU Utilization



Full Scale | 2500 non-persistent users | ND VDI Hosts | Host Memory Utilization



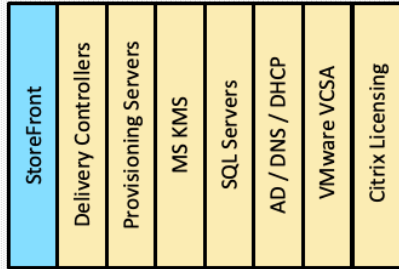
## Full-Scale Persistent Workload Testing with 2500 Users

This section shows the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. The full-scale testing with 2500 users comprised of: 2500 Persistent Hosted Virtual Desktop using 11 compute nodes.

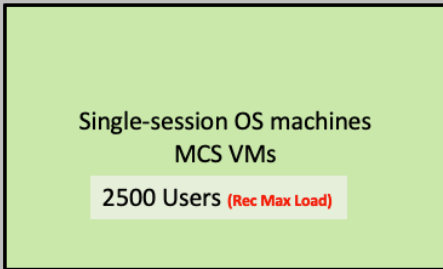
The combined mixed workload for the solution is 2500 users. To achieve the target, sessions were launched against all workload clusters concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.



## MCS Single-session OS machine VDAs Full Scale Testing with 2500 pooled Users



### Cisco UCS X210c M6 x 11



- Access Layer
- Control Layer
- Resource Layer
- Physical Layer

The configured system efficiently and effectively delivered the following results.



Figure 73. Full-Scale | 2500 Persistent Users | VSI Score

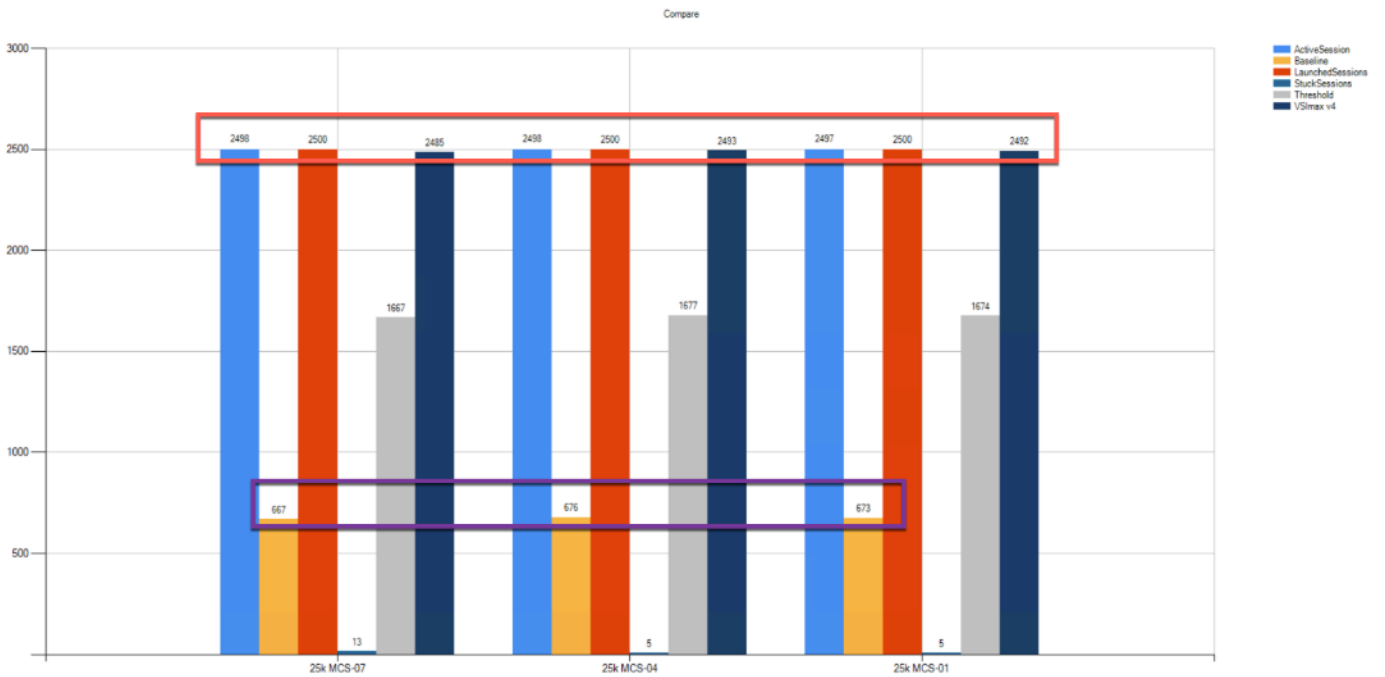
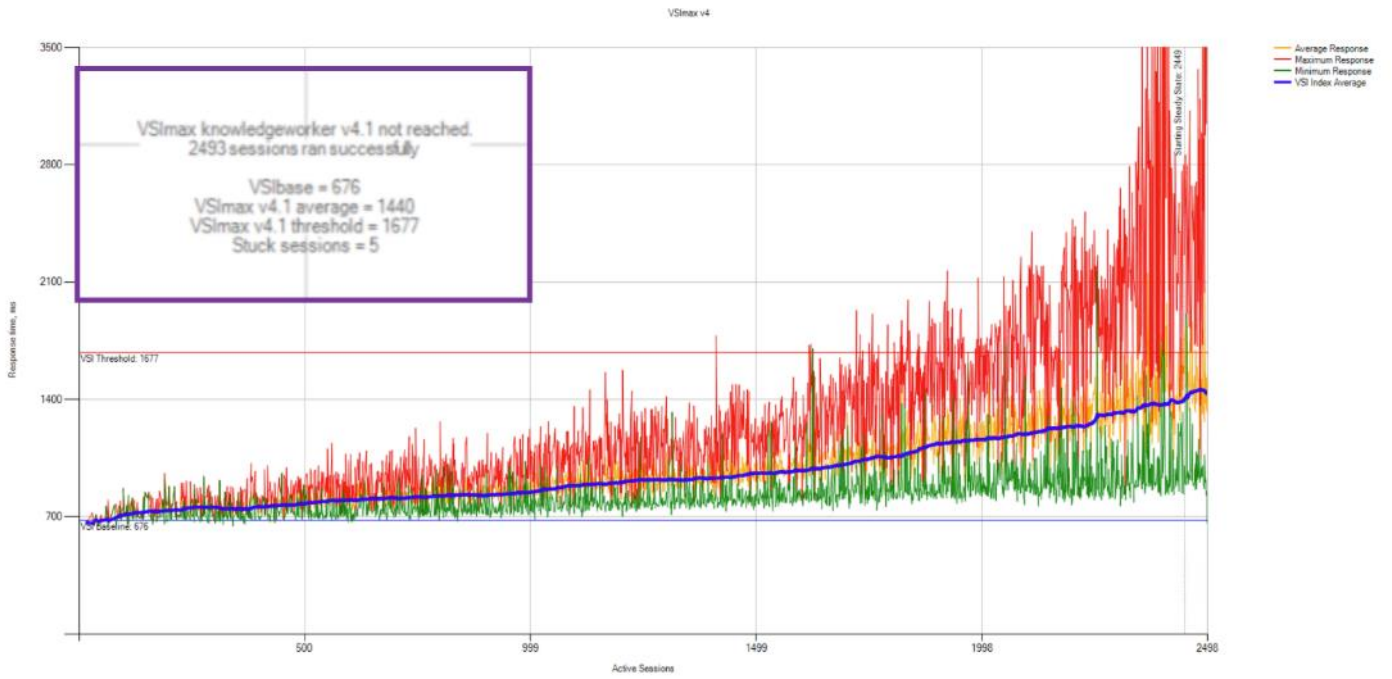


Figure 74. Full-Scale | 2500 Persistent Users | VSI Repeatability

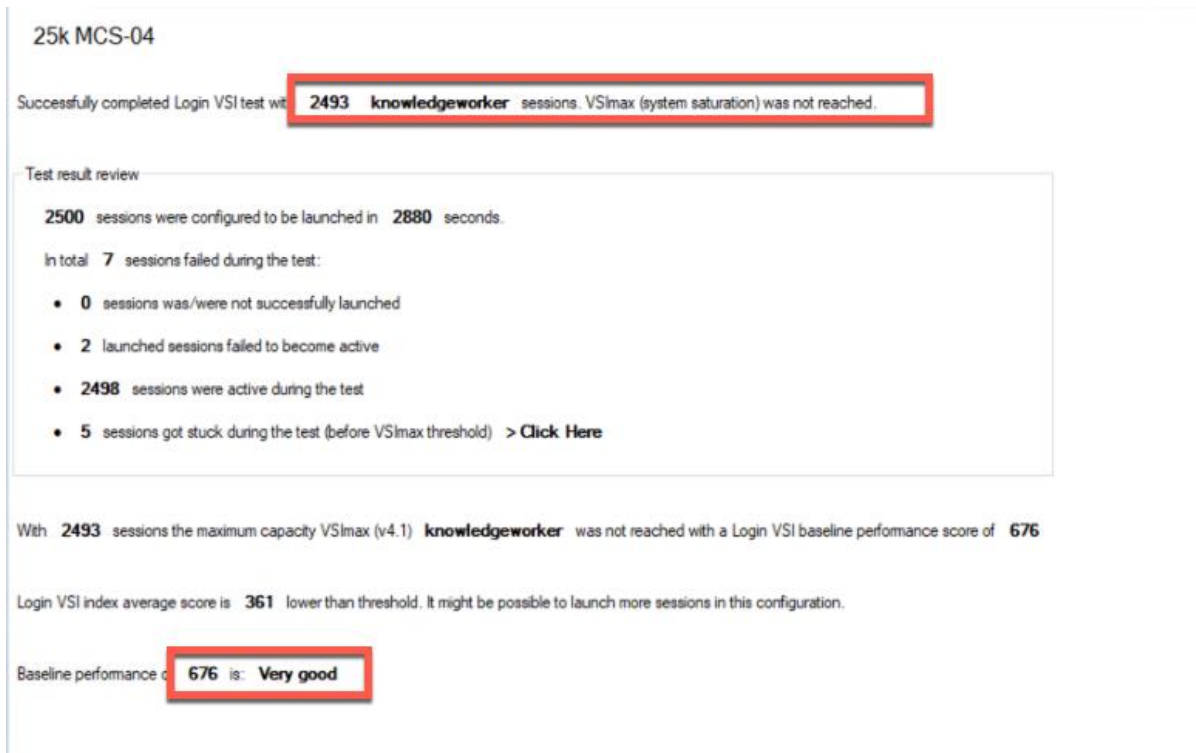


Figure 75. Full-Scale | 2500 persistent users | P-VDI Hosts | Host CPU Utilization

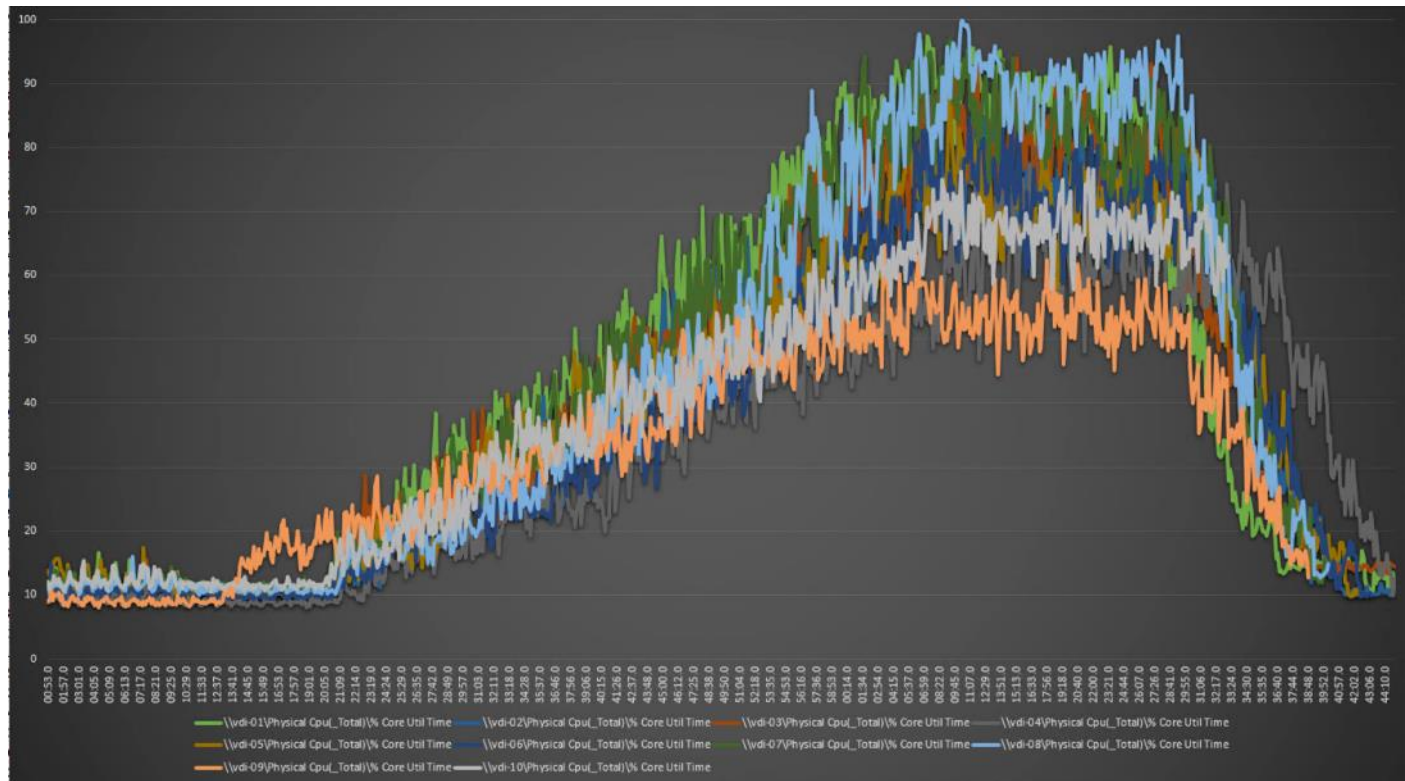
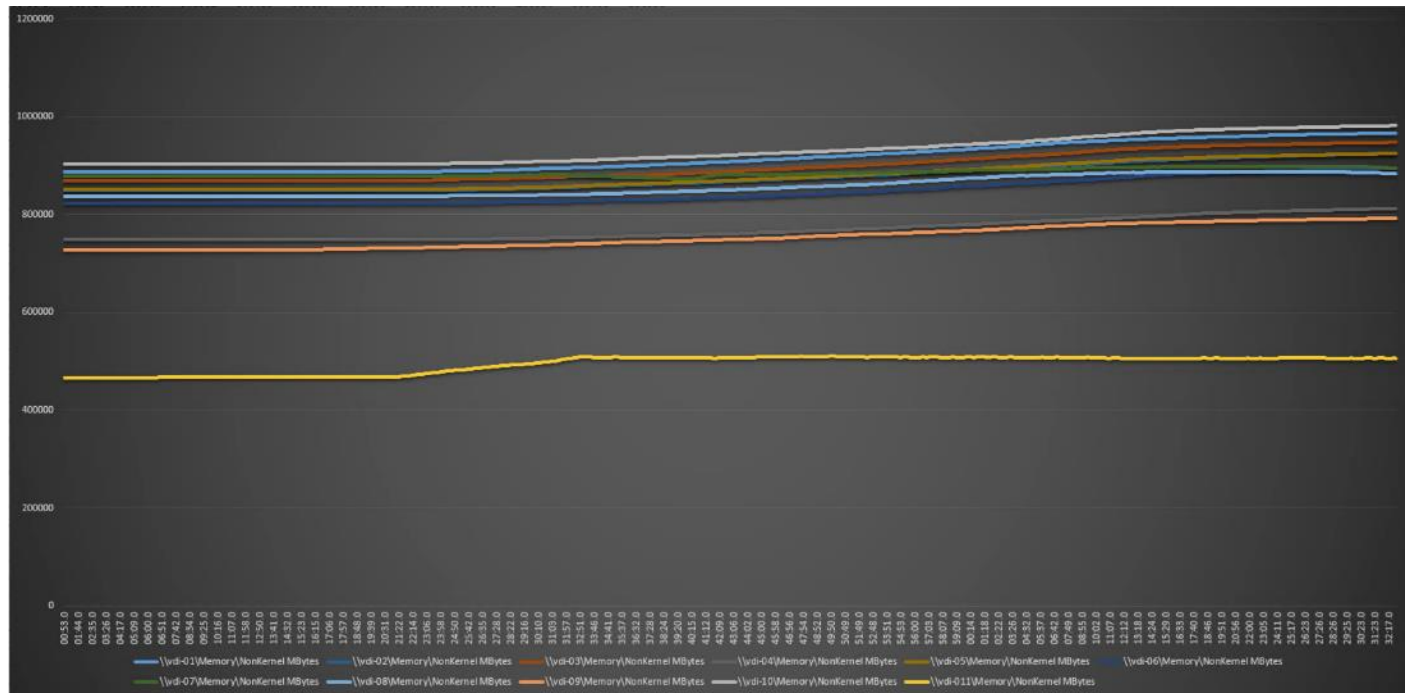


Figure 76. Full-Scale | 2500 persistent users | P-VDI Hosts | Host Memory Utilization



## 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:

- 2500 Windows Server 2016 Citrix Hosted Shared desktops (RDS)
- 2500 Windows 10 x64 Citrix PVS Non-Persistent desktops
- 2500 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 driving a substantial amount of IOPs and bandwidth for the 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.

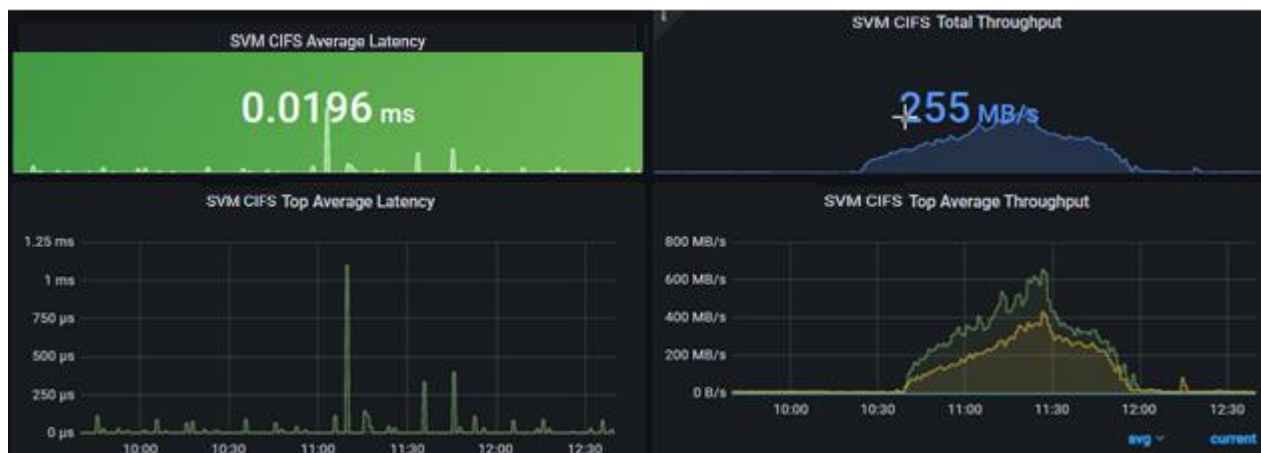
### 2500 Users Citrix HSD (RDS) Windows 2019 Sessions

This test uses Login VSI for the workload generator in Benchmark mode with the Knowledge Worker user type and with Citrix Hosted Shared Desktops (RDSH) Sessions for the VDI delivery mechanism. This first highlighted cluster test shows that the AFF A400 can easily handle this workload with exceptional end-user experience as confirmed from Login VSI.

### 2500 Citrix HSD (RDS) Cluster Test: Storage Charts

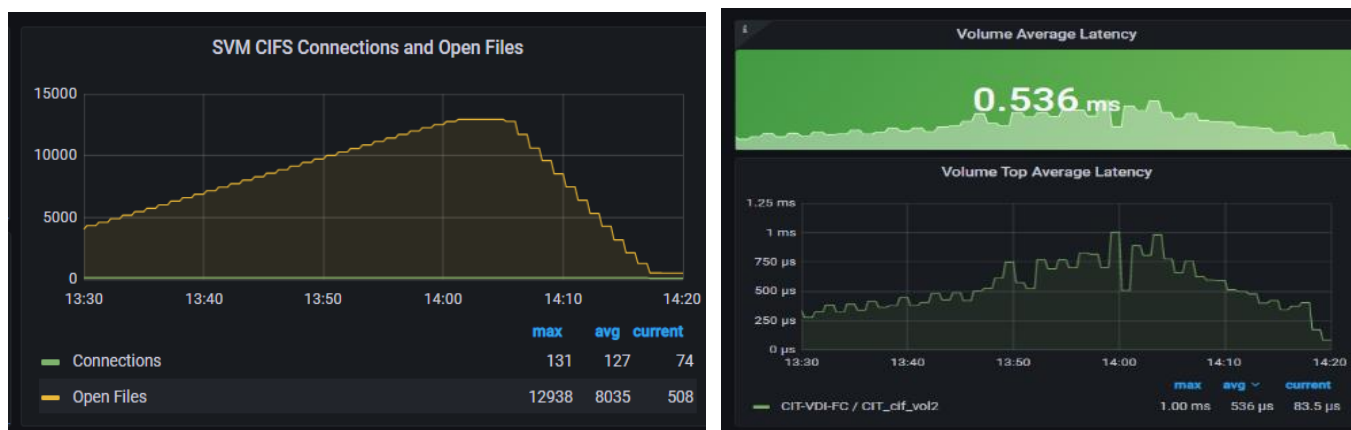
#### SVM Performance

From the charts below, during the bootup of the virtual machines, consistent sub-millisecond latency was observed which produces quicker build time for the administrators of the infrastructure and produces better response time for the users

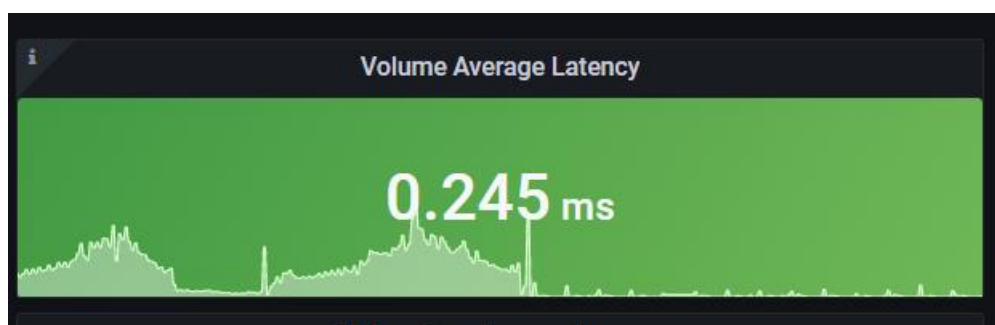
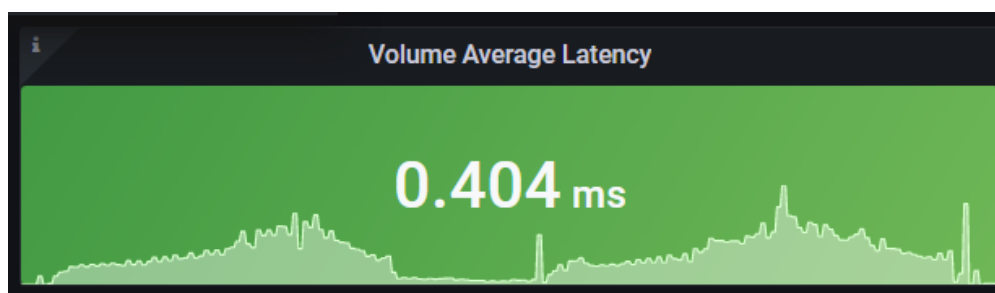


## SMB/CIFS

The file share is used for storing user profile containers with FSLogix. The first image shows one volume of 8 presenting a max of over 1200 files/profiles on 131 connections and an average of over 8000 files are presenting profiles on 127 connections to the virtual machines during boot up. During this time, the Cifs volume Max latency never goes above 1ms with an average of 0.5ms latency per volume. After bootup the storage systems smooths out the average latency under a millisecond consistently.



The first image shows the average volume latency during the build and boot up of the virtual machines. The second image shows the latency consistency smooths out as the most intensive part of the boot up is over.

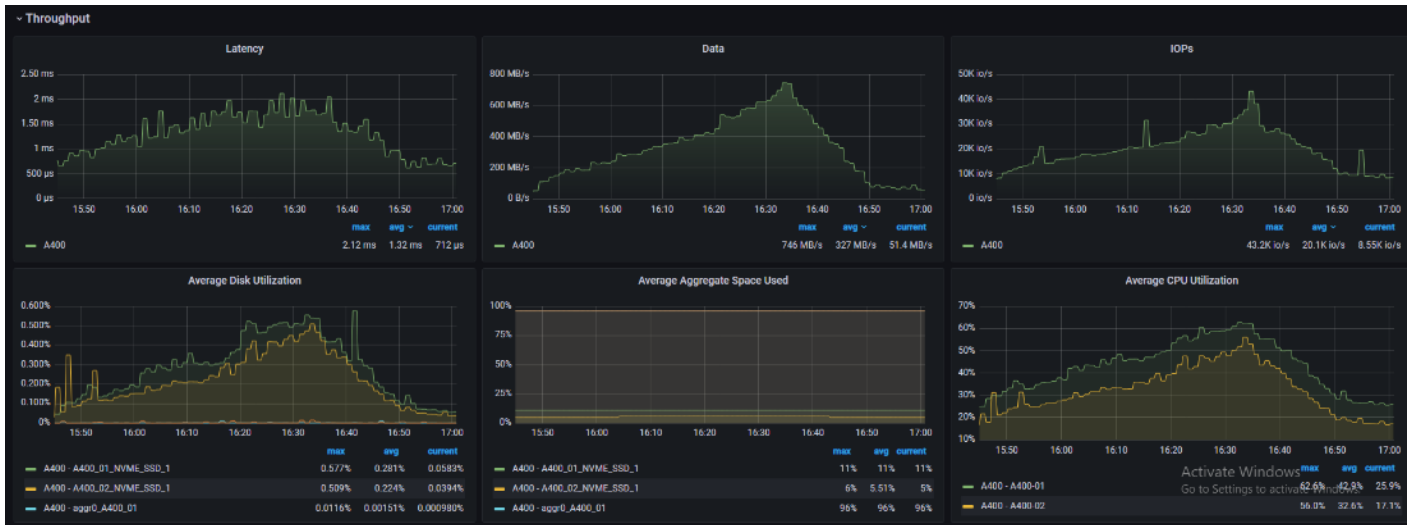


## 2500 Users Persistent Desktops Cluster Test

### NetApp AFF A400 Test Results for 2500 Persistent Windows 10 x64 Citrix MCS Desktops

#### SVM Performance

For this test, SVM noticed IOPS of around 40000 while Read/Write latency below is way below 1ms. Read/Write ratio is around 1:6.



#### NFSv3

We noticed that all NFS volumes peaked above 1ms but never higher than 1.59ms. The average latency did stay below 1ms.

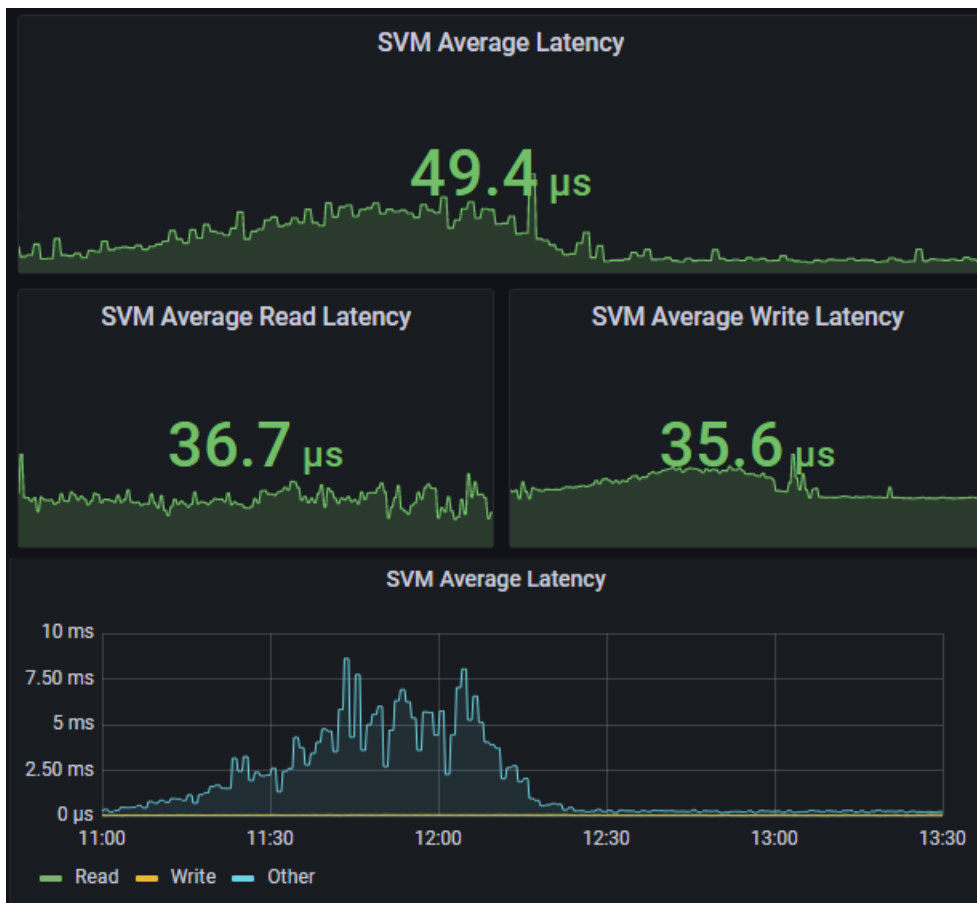


## 2500 Users PVS Non-Persistent Desktops Cluster Test

### NetApp

#### SVM

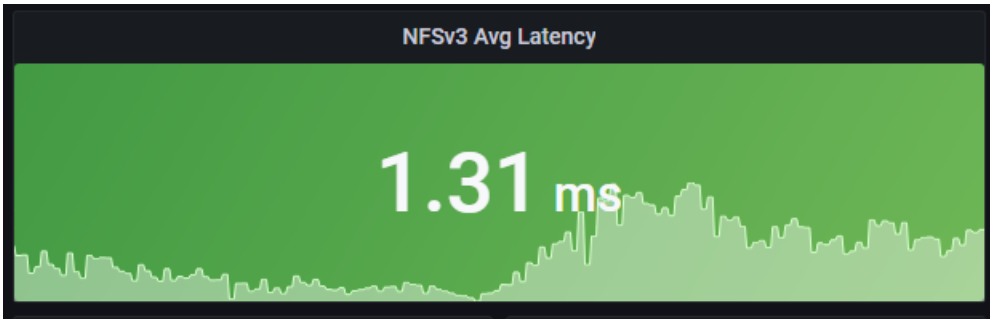
In this use case, we noticed the read/write ratio is about 1:7. Read/write latency stayed below 0.5ms



#### NFSv3

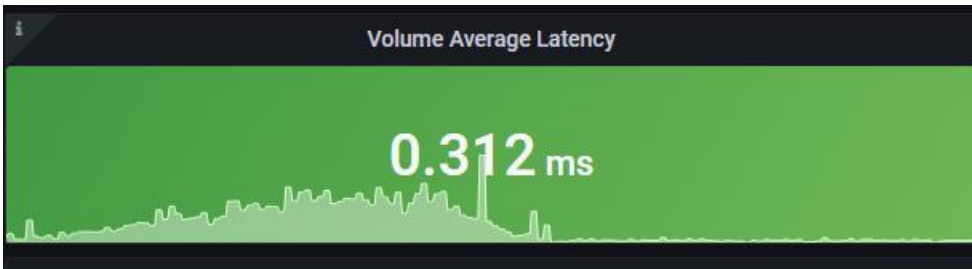
With PVS, the desktop image is retrieved from SMB share, then uses compute resources & SMB share for user profiles. The reason we are seeing activity with NFS is, we distributed infrastructure VMs across FC datastore and NFS datastore. Even though the NFS datastore is different, it used the logical network interfaces since we had single SVM. To avoid this scenario, need to have separate SVM for Infrastructure and workloads like how the compute resources are separated out.





### NFS Volume(s)

For this use case, The 8 NFS volumes shows an average latency of .3 ms, during vm build and bootup. You also notice after startup how the system evens out with minimum latency to the volumes.



## 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 & 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 & 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 & 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 & Desktops 7 LTSR Configuration

Citrix Virtual Apps & Desktops environments can scale to large numbers. When implementing Citrix Virtual Apps & 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.

---

## Appendix—Cisco Switch Configuration

This chapter contains the following subjects:

- [Network Configuration](#)
- [Fibre Channel Configuration](#)

### Network Configuration

#### N93180YC-FX -A Configuration

```
!Command: show running-config
!

version 7.0(3)I1(3b)
switchname DV-Pod-2-N9K-A
class-map type network-qos class-platinum
match qos-group 2
class-map type network-qos class-all-flood
match qos-group 2
class-map type network-qos system_nq_policy
match qos-group 2
class-map type network-qos class-ip-multicast
match qos-group 2
policy-map type network-qos jumbo
  class type network-qos class-platinum
    mtu 9216
  class type network-qos class-default
    mtu 9216
vdc DV-Pod-2-N9K-A id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature telnet
cfs ipv4 distribute
cfs eth distribute
```

```
feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc
feature lldp
clock protocol none vdc 1

no password strength-check
username admin password 5 $1$tYYajkfc$7P7nLjWYvfTWA1vFDnwJZ. role network-admin
ip domain-lookup
ip access-list NFS_VLAN63
  10 permit ip 10.10.63.0 255.255.255.0 any
  20 deny ip any any
ip access-list iSCSI-A_64
  10 permit ip 10.10.64.0 255.255.255.0 any
  20 deny ip any any
ip access-list iSCSI-B_65
  10 permit ip 10.10.65.0 255.255.255.0 any
  20 deny ip any any
class-map type qos match-any class-platinum
  match cos 5
policy-map type qos jumbo
  class class-platinum
    set qos-group 2
  class class-default
    set qos-group 0
system qos
  service-policy type network-qos jumbo
copp profile strict
snmp-server user admin network-admin auth md5 0xf747567d6cfecf362a9641ac6f3cefc9 priv
0xf747567d6cfecf362a9641ac6f3cefc9 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 10.81.254.202

vlan 1-2,60-70,102,164
```

```
vlan 60
  name In-Band-Mgmt
vlan 61
  name Infra-Mgmt
vlan 62
  name CIFS
vlan 63
  name NFS
vlan 64
  name iSCSI-A
vlan 65
  name iSCSI-B
vlan 66
  name vMotion
vlan 67
  name N1KV
vlan 68
  name LauncherPXE
vlan 69
  name Launcher81
vlan 70
  name other-3
vlan 102
  name VDI
vlan 164
  name Out-Of-Band-Mgmt

spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
service dhcp
ip dhcp relay
ipv6 dhcp relay
vrf context management
  ip route 0.0.0.0/0 10.29.164.1
port-channel load-balance src-dst l4port
vpc domain 10
  peer-switch
  role priority 10
```

---

```
peer-keepalive destination 10.29.164.66 source 10.29.164.65
delay restore 150
peer-gateway
auto-recovery
```

```
interface Vlan1
  no ip redirects
  no ipv6 redirects
```

```
interface Vlan2
  description Default native vlan 2
  no ip redirects
  no ipv6 redirects
```

```
interface Vlan60
  description Out of Band Management vlan 60
  no shutdown
  no ip redirects
  ip address 10.10.60.2/24
  no ipv6 redirects
  hsrp version 2
  hsrp 60
    preempt
    priority 110
    ip 10.10.60.1
```

```
interface Vlan61
  description Infrastructure vlan 61
  no shutdown
  no ip redirects
  ip address 10.10.61.2/24
  no ipv6 redirects
  hsrp version 2
  hsrp 61
    preempt
    ip 10.10.61.1
```

```
interface Vlan62
```

---

```
description CIFS vlan 62
no shutdown
no ip redirects
ip address 10.10.62.2/24
no ipv6 redirects
hsrp version 2
hsrp 62
  preempt
  priority 110
  ip 10.10.62.1
```

```
interface Vlan63
no shutdown
no ip redirects
ip address 10.10.63.2/24
no ipv6 redirects
hsrp version 2
hsrp 63
  preempt
  ip 10.10.63.1
```

```
interface Vlan64
description iSCSI Fabric A path vlan 64
no shutdown
no ip redirects
ip address 10.10.64.2/24
no ipv6 redirects
hsrp version 2
hsrp 64
  preempt
  priority 110
  ip 10.10.64.1
```

```
interface Vlan65
description iSCSI Fabric B path vlan 65
no shutdown
no ip redirects
ip address 10.10.65.2/24
no ipv6 redirects
```



```
hsrp version 2
hsrp 65
  preempt
  ip 10.10.65.1

interface Vlan66
  description vMotion network vlan 66
  no shutdown
  ip address 10.10.66.2/24
  hsrp version 2
  hsrp 66
    preempt
    ip 10.10.66.1

interface Vlan67
  description vlan 67
  no shutdown
  ip address 10.10.67.2/24
  hsrp version 2
  hsrp 67
    preempt
    ip 10.10.67.1

interface Vlan68
  description LoginVSI Launchers vlan 68
  no shutdown
  no ip redirects
  ip address 10.10.68.2/24
  no ipv6 redirects
  hsrp version 2
  hsrp 68
    preempt
    ip 10.10.68.1

interface Vlan69
  description LoginVSI Launchers 10.10.81-network vlan 69
  no shutdown
  no ip redirects
  ip address 10.10.81.2/24
```

```
no ipv6 redirects
hsrp version 2
hsrp 69
    preempt
    ip 10.10.81.1

interface Vlan102
    description VDI vlan 102
    no shutdown
    no ip redirects
    ip address 10.2.0.2/19
    no ipv6 redirects
    hsrp version 2
    hsrp 102
        preempt delay minimum 240
        priority 110
        timers 1 3
        ip 10.2.0.1
    ip dhcp relay address 10.10.61.30

interface port-channel10
    description VPC-PeerLink
    switchport mode trunk
    switchport trunk allowed vlan 1-2,60-70,102,164
    spanning-tree port type network
    vpc peer-link

interface port-channel11
    description FI-A_6k_UCS-Uplink
    switchport mode trunk
    switchport trunk allowed vlan 1-2,60-70,102,164
    spanning-tree port type edge trunk
    mtu 9216
    vpc 11

interface port-channel12
    description FI-B_6k_UCS-Uplink
    switchport mode trunk
    switchport trunk allowed vlan 1-2,60-70,102,164
```

---

```
spanning-tree port type edge trunk
mtu 9216
vpc 12
```

```
interface port-channel13
description NetApp_AFF400_Node_02_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
spanning-tree port type edge trunk
mtu 9216
vpc 13
```

```
interface port-channel14
description NetApp_AFF400_Node_02_NFS
switchport mode trunk
switchport trunk allowed vlan 63
spanning-tree port type edge trunk
mtu 9216
vpc 14
```

```
interface port-channel15
description FI-A_6k_Launchers-Uplink
switchport mode trunk
switchport trunk allowed vlan 1-2,60-70,102,164
spanning-tree port type edge trunk
mtu 9216
vpc 15
```

```
interface port-channel16
description FI-B_6k_Launchers-Uplink
switchport mode trunk
switchport trunk allowed vlan 1-2,60-70,102,164
spanning-tree port type edge trunk
mtu 9216
vpc 16
```

```
interface port-channel17
description NetApp_AFF400_Node_01_CIFS
switchport mode trunk
```

---

```
switchport trunk allowed vlan 62,64-65
spanning-tree port type edge trunk
mtu 9216
vpc 17
```

```
interface port-channel18
description NetApp_AFF400_Node_01_NFS
switchport mode trunk
switchport trunk allowed vlan 63
spanning-tree port type edge trunk
mtu 9216
vpc 18
```

```
interface Ethernet1/1
description NetApp_AFF400_Node-02_port_e0e_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
channel-group 14 mode active
```

```
interface Ethernet1/2
description NetApp_AFF400_Node-02_port_e1a_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
channel-group 14 mode active
```

```
interface Ethernet1/3
description NetApp_AFF400_Node-01_port_e0e_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
channel-group 18 mode active
```

```
interface Ethernet1/4
description NetApp_AFF400_Node-01_port_e4a_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
```

---

```
channel-group 18 mode active
```

```
interface Ethernet1/5
description NetApp_AFF400_Node-02_port_e0f_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 13 mode active
```

```
interface Ethernet1/6
description NetApp_AFF400_Node-02_port_e4a_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 13 mode active
```

```
interface Ethernet1/7
description NetApp_AFF400_Node-01_port_e0f_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 17 mode active
```

```
interface Ethernet1/8
description NetApp_AFF400_Node-01_port_e1a_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 17 mode active
```

```
interface Ethernet1/9
```

```
interface Ethernet1/10
```

```
interface Ethernet1/11
```

```
interface Ethernet1/12
```

```
interface Ethernet1/13
```

```
interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17
  description Uplink_from_FI-A_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/18
  description Uplink_from_FI-A_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/19
  description Uplink_from_FI-B_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/20
  description Uplink_from_FI-B_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/21

interface Ethernet1/22
```

---

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

```
interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45
  description Uplink_from_LoginVSI_Launchers_FI-A
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 15 mode active

interface Ethernet1/46
  description Uplink_from_LoginVSI_Launchers_FI-B
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 16 mode active

interface Ethernet1/47

interface Ethernet1/48
  description TOR
  switchport access vlan 164

interface Ethernet1/49
  description VPC Peer Link between 9ks
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  channel-group 10 mode active

interface Ethernet1/50
  description VPC Peer Link between 9ks
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  channel-group 10 mode active

interface Ethernet1/51
```



```
interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0
  vrf member management
  ip address 10.29.164.65/24
line console
line vty
boot nxos bootflash://sup-1/n9000-dk9.7.0.3.I1.3b.bin
```

### **N93180YC-FX -B Configuration**

```
!Command: show running-config
!Time: Fri Feb 26 16:47:01 2016

version 7.0(3)I1(3b)
switchname DV-Pod-2-N9K-B
class-map type network-qos class-platinum
match qos-group 2
class-map type network-qos class-all-flood
match qos-group 2
class-map type network-qos system_nq_policy
match qos-group 2
class-map type network-qos class-ip-multicast
match qos-group 2
policy-map type network-qos jumbo
  class type network-qos class-platinum
    mtu 9216
  class type network-qos class-default
    mtu 9216
vdc DV-Pod-2-N9K-B id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
```

```
feature telnet
cfs ipv4 distribute
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc
feature lldp
clock protocol none vdc 1

no password strength-check
username admin password 5 $1$fp3LrGLC$PF8eML85qkPBgdH/bZAKK/ role network-admin
ip domain-lookup
ip access-list NFS_VLAN63
  10 permit ip 10.10.63.0 255.255.255.0 any
  20 deny ip any any
ip access-list iSCSI-A_64
  10 permit ip 10.10.64.0 255.255.255.0 any
  20 deny ip any any
ip access-list iSCSI-B_65
  10 permit ip 10.10.65.0 255.255.255.0 any
  20 deny ip any any
class-map type qos match-any class-platinum
  match cos 5
policy-map type qos jumbo
  class class-platinum
    set qos-group 2
  class class-default
    set qos-group 0
system qos
  service-policy type network-qos jumbo
copp profile strict
snmp-server user admin network-admin auth md5 0x13ec164cc65d2b9854d70379681039c8 priv
0x13ec164cc65d2b9854d70379681039c8 localizedkey

ntp master 8

vlan 1-2,60-70,102,164
```

```
vlan 60
  name In-Band-Mgmt
vlan 61
  name Infra-Mgmt
vlan 62
  name CIFS
vlan 63
  name NFS
vlan 64
  name iSCSI-A
vlan 65
  name iSCSI-B
vlan 66
  name vMotion
vlan 67
  name N1KV
vlan 68
  name LauncherPXE
vlan 69
  name Launcher81
vlan 70
  name other-3
vlan 102
  name VDI
vlan 164
  name Out-Of-Band-Mgmt

spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
service dhcp
ip dhcp relay
ipv6 dhcp relay
vrf context management
  ip route 0.0.0.0/0 10.29.164.1
port-channel load-balance src-dst l4port
vpc domain 10
  peer-switch
  role priority 10
```

---

```
peer-keepalive destination 10.29.164.65 source 10.29.164.66
delay restore 150
peer-gateway
auto-recovery
```

```
interface Vlan1
  no ip redirects
  no ipv6 redirects
```

```
interface Vlan2
  description Default native vlan 2
  no ip redirects
  no ipv6 redirects
```

```
interface Vlan60
  description Out of Band Management vlan 60
  no shutdown
  no ip redirects
  ip address 10.10.60.3/24
  no ipv6 redirects
  hsrp version 2
  hsrp 60
    preempt
    priority 110
    ip 10.10.60.1
```

```
interface Vlan61
  description Infrastructure vlan 61
  no shutdown
  no ip redirects
  ip address 10.10.61.3/24
  no ipv6 redirects
  hsrp version 2
  hsrp 61
    preempt
    ip 10.10.61.1
```

```
interface Vlan62
```

---

```
description CIFS vlan 62
no shutdown
no ip redirects
ip address 10.10.62.3/24
no ipv6 redirects
hsrp version 2
hsrp 62
  preempt
  priority 110
  ip 10.10.62.1
```

```
interface Vlan63
description NFS vlan 63
no shutdown
no ip redirects
ip address 10.10.63.3/24
no ipv6 redirects
hsrp version 2
hsrp 63
  preempt
  ip 10.10.63.1
```

```
interface Vlan64
description iSCSI Fabric A path vlan 64
no shutdown
no ip redirects
ip address 10.10.64.3/24
no ipv6 redirects
hsrp version 2
hsrp 64
  preempt
  priority 110
  ip 10.10.64.1
```

```
interface Vlan65
description iSCSI Fabric B path vlan 65
no shutdown
no ip redirects
ip address 10.10.65.3/24
```

```
no ipv6 redirects
hsrp version 2
hsrp 65
    preempt
    ip 10.10.65.1

interface Vlan66
    description vMotion network vlan 66
    no shutdown
    ip address 10.10.66.3/24
    hsrp version 2
    hsrp 66
        preempt
        ip 10.10.66.1

interface Vlan67
    description vlan 67
    no shutdown
    ip address 10.10.67.3/24
    hsrp version 2
    hsrp 67
        preempt
        ip 10.10.67.1

interface Vlan68
    description LoginVSI Launchers vlan 68
    no shutdown
    no ip redirects
    ip address 10.10.68.3/24
    no ipv6 redirects
    hsrp version 2
    hsrp 68
        preempt
        ip 10.10.68.1

interface Vlan69
    description LoginVSI Launchers 10.10.81-network vlan 69
    no shutdown
    no ip redirects
```

```
ip address 10.10.81.3/24
no ipv6 redirects
hsrp version 2
hsrp 69
    preempt
    ip 10.10.81.1

interface Vlan102
    description VDI vlan 102
    no shutdown
    no ip redirects
    ip address 10.2.0.3/19
    no ipv6 redirects
    hsrp version 2
    hsrp 102
        preempt delay minimum 240
        priority 110
        timers 1 3
        ip 10.2.0.1
    ip dhcp relay address 10.10.61.30

interface port-channel10
    description VPC-PeerLink
    switchport mode trunk
    switchport trunk allowed vlan 1-2,60-70,102,164
    spanning-tree port type network
    vpc peer-link

interface port-channel11
    description FI-A_6k_UCS-Uplink
    switchport mode trunk
    switchport trunk allowed vlan 1-2,60-70,102,164
    spanning-tree port type edge trunk
    mtu 9216
    vpc 11

interface port-channel12
    description FI-B_6k_UCS-Uplink
    switchport mode trunk
```

---

```
switchport trunk allowed vlan 1-2,60-70,102,164
spanning-tree port type edge trunk
mtu 9216
vpc 12
```

```
interface port-channel13
description NetApp_AFF400_Node_02_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
spanning-tree port type edge trunk
mtu 9216
vpc 13
```

```
interface port-channel14
description NetApp_AFF400_Node_02_NFS
switchport mode trunk
switchport trunk allowed vlan 63
spanning-tree port type edge trunk
mtu 9216
vpc 14
```

```
interface port-channel15
description FI-A_6k_Launchers-Uplink
switchport mode trunk
switchport trunk allowed vlan 1-2,60-70,102,164
spanning-tree port type edge trunk
mtu 9216
vpc 15
```

```
interface port-channel16
description FI-B_6k_Launchers-Uplink
switchport mode trunk
switchport trunk allowed vlan 1-2,60-70,102,164
spanning-tree port type edge trunk
mtu 9216
vpc 16
```

```
interface port-channel17
description NetApp_AFF400_Node_01_CIFS
```



---

```
switchport mode trunk
switchport trunk allowed vlan 62,64-65
spanning-tree port type edge trunk
mtu 9216
vpc 17
```

```
interface port-channel18
description NetApp_AFF400_Node-01_port_NFS
switchport mode trunk
switchport trunk allowed vlan 63
spanning-tree port type edge trunk
mtu 9216
vpc 18
```

```
interface Ethernet1/1
description NetApp_AFF400_Node-02_port_e0g_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
channel-group 14 mode active
```

```
interface Ethernet1/2
description NetApp_AFF400_Node-02_port_e1b_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
channel-group 14 mode active
```

```
interface Ethernet1/3
description NetApp_AFF400_Node-01_port_e0g_NFS
switchport mode trunk
switchport trunk allowed vlan 63
mtu 9216
channel-group 18 mode active
```

```
interface Ethernet1/4
description NetApp_AFF400_Node-01_port_e4b_NFS
switchport mode trunk
switchport trunk allowed vlan 63
```

```
mtu 9216
channel-group 18 mode active

interface Ethernet1/5
description NetApp_AFF400_Node-02_port_e0h_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 13 mode active

interface Ethernet1/6
description NetApp_AFF400_Node-02_port_e4b_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 13 mode active

interface Ethernet1/7
description NetApp_AFF400_Node-01_port_e0h_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 17 mode active

interface Ethernet1/8
description NetApp_AFF400_Node-01_port_e1b_CIFS
switchport mode trunk
switchport trunk allowed vlan 62,64-65
mtu 9216
channel-group 17 mode active

interface Ethernet1/9
description Jumphost ToR
switchport access vlan 60
spanning-tree port type edge
speed 1000

interface Ethernet1/10
```

```
interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17
  description Uplink_from_FI-A_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/18
  description Uplink_from_FI-A_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/19
  description Uplink_from_FI-B_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 12 mode active

interface Ethernet1/20
  description Uplink_from_FI-B_6k
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 12 mode active
```

---

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

```
interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45
  description Uplink_from_LoginVSI_Launchers_FI-A
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 15 mode active

interface Ethernet1/46
  description Uplink_from_LoginVSI_Launchers_FI-B
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  mtu 9216
  channel-group 16 mode active

interface Ethernet1/47

interface Ethernet1/48
  description TOR
  switchport access vlan 164

interface Ethernet1/49
  description VPC Peer Link between 9ks
  switchport mode trunk
  switchport trunk allowed vlan 1-2,60-70,102,164
  channel-group 10 mode active

interface Ethernet1/50
  description VPC Peer Link between 9ks
  switchport mode trunk
```

```
switchport trunk allowed vlan 1-2,60-70,102,164
channel-group 10 mode active

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0
    vrf member management
    ip address 10.29.164.66/24
line console
line vty
boot nxos bootflash://sup-1/n9000-dk9.7.0.3.I1.3b.bin
```

## Fibre Channel Configuration

### Cisco MDS 9132T - A Configuration

```
!Command: show running-config
!Time: Wed Feb  7 00:49:39 2018

version 8.1(1)
power redundancy-mode redundant
feature npiv
feature fport-channel-trunk
role name default-role
    description This is a system defined role and applies to all users.
    rule 5 permit show feature environment
    rule 4 permit show feature hardware
    rule 3 permit show feature module
    rule 2 permit show feature snmp
    rule 1 permit show feature system
no password strength-check
username admin password 5 $1$DDq8vFlx$EwCSM003dlXZ4j1Py9ZoC.  role network-admin
ip domain-lookup
ip host MDS-A 10.29.164.238
aaa group server radius radius
```

```
snmp-server contact jnichols
snmp-server user admin network-admin auth md5 0x2efbf582e573df2038164f1422c231fe
  priv 0x2efbf582e573df2038164f1422c231fe localizedkey
snmp-server host 10.155.160.192 traps version 2c public udp-port 1163
snmp-server host 10.155.166.14 traps version 2c public udp-port 1163
snmp-server host 10.29.132.18 traps version 2c public udp-port 1163
snmp-server host 10.29.164.130 traps version 2c public udp-port 1163
snmp-server host 10.29.164.250 traps version 2c public udp-port 1164
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community public group network-operator
vsan database
  vsan 400 name "FlexPod-A"
device-alias database
  device-alias name X210c-SP pwwn 20:00:00:25:b5:03:9a:06
  device-alias name A400_N1P3 pwwn 50:01:73:80:59:16:01:12
  device-alias name A400_N2P1 pwwn 50:01:73:80:59:16:01:20
  device-alias name A400_N2P3 pwwn 50:01:73:80:59:16:01:22
  device-alias name A400_N3P1 pwwn 50:01:73:80:59:16:01:30
  device-alias name A400_N3P3 pwwn 50:01:73:80:59:16:01:32
  device-alias name VDI-1-hba1 pwwn 20:00:00:25:b5:3a:00:3f
  device-alias name VDI-2-hba1 pwwn 20:00:00:25:b5:3a:00:0f
  device-alias name VDI-3-hba1 pwwn 20:00:00:25:b5:3a:00:1f
  device-alias name VDI-4-hba1 pwwn 20:00:00:25:b5:3a:00:4e
  device-alias name VDI-5-hba1 pwwn 20:00:00:25:b5:3a:00:2e
  device-alias name VDI-6-hba1 pwwn 20:00:00:25:b5:3a:00:3e
  device-alias name VDI-7-hba1 pwwn 20:00:00:25:b5:3a:00:0e
  device-alias name VDI-9-hba1 pwwn 20:00:00:25:b5:3a:00:4d
  device-alias name A400-01-0g pwwn 20:01:00:a0:98:af:bd:e8
  device-alias name A400-02-0g pwwn 20:03:00:a0:98:af:bd:e8
  device-alias name srv01_HBA1 pwwn 20:00:00:25:b5:03:9a:12
  device-alias name srv02_HBA1 pwwn 20:00:00:25:b5:03:9a:14
  device-alias name srv03_HBA1 pwwn 20:00:00:25:b5:03:9a:0e
  device-alias name srv04_HBA1 pwwn 20:00:00:25:b5:03:9a:00
  device-alias name srv05_HBA1 pwwn 20:00:00:25:b5:03:9a:02
  device-alias name srv06_HBA1 pwwn 20:00:00:25:b5:03:9a:0c
```

```
device-alias name srv07_HBA1 pwwn 20:00:00:25:b5:03:9a:10
device-alias name srv09_HBA1 pwwn 20:00:00:25:b5:03:9a:16
device-alias name srv10_HBA1 pwwn 20:00:00:25:b5:03:9a:18
device-alias name srv11_HBA1 pwwn 20:00:00:25:b5:03:9a:1a
device-alias name srv12_HBA1 pwwn 20:00:00:25:b5:03:9a:1c
device-alias name srv13_HBA1 pwwn 20:00:00:25:b5:03:9a:1e
device-alias name srv14_HBA1 pwwn 20:00:00:25:b5:03:9a:20
device-alias name srv15_HBA1 pwwn 20:00:00:25:b5:03:9a:22
device-alias name srv17_HBA1 pwwn 20:00:00:25:b5:03:9a:24
device-alias name srv18_HBA1 pwwn 20:00:00:25:b5:03:9a:26
device-alias name srv19_HBA1 pwwn 20:00:00:25:b5:03:9a:30
device-alias name srv20_HBA1 pwwn 20:00:00:25:b5:03:9a:28
device-alias name srv21_HBA1 pwwn 20:00:00:25:b5:03:9a:2a
device-alias name srv22_HBA1 pwwn 20:00:00:25:b5:03:9a:2c
device-alias name srv23_HBA1 pwwn 20:00:00:25:b5:03:9a:2e
device-alias name srv24_HBA1 pwwn 20:00:00:25:b5:03:9a:32
device-alias name srv27_HBA1 pwwn 20:00:00:25:b5:03:9a:38
device-alias name VDI-10-hba1 pwwn 20:00:00:25:b5:3a:00:2d
device-alias name VDI-11-hba1 pwwn 20:00:00:25:b5:3a:00:3d
device-alias name VDI-12-hba1 pwwn 20:00:00:25:b5:3a:00:0d
device-alias name VDI-13-hba1 pwwn 20:00:00:25:b5:3a:00:1d
device-alias name VDI-14-hba1 pwwn 20:00:00:25:b5:3a:00:4c
device-alias name VDI-15-hba1 pwwn 20:00:00:25:b5:3a:00:2c
device-alias name VDI-17-hba1 pwwn 20:00:00:25:b5:3a:00:0c
device-alias name VDI-18-hba1 pwwn 20:00:00:25:b5:3a:00:1c
device-alias name VDI-19-hba1 pwwn 20:00:00:25:b5:3a:00:4b
device-alias name VDI-20-hba1 pwwn 20:00:00:25:b5:3a:00:2b
device-alias name VDI-21-hba1 pwwn 20:00:00:25:b5:3a:00:3b
device-alias name VDI-22-hba1 pwwn 20:00:00:25:b5:3a:00:0b
device-alias name VDI-23-hba1 pwwn 20:00:00:25:b5:3a:00:1b
device-alias name VDI-24-hba1 pwwn 20:00:00:25:b5:3a:00:4a
device-alias name VDI-25-hba1 pwwn 20:00:00:25:b5:3a:00:2a
device-alias name VDI-26-hba1 pwwn 20:00:00:25:b5:3a:00:3a
device-alias name VDI-27-hba1 pwwn 20:00:00:25:b5:3a:00:0a
device-alias name VDI-28-hba1 pwwn 20:00:00:25:b5:3a:00:1a
device-alias name VDI-29-hba1 pwwn 20:00:00:25:b5:3a:00:49
device-alias name VDI-30-hba1 pwwn 20:00:00:25:b5:3a:00:39
device-alias name VDI-31-hba1 pwwn 20:00:00:25:b5:3a:00:1e
device-alias name VDI-32-hba1 pwwn 20:00:00:25:b5:3a:00:3c
```



```
device-alias name SP-Infra1-fc0 pwwn 20:00:00:25:b5:00:00:2f
device-alias name SP-Infra2-fc0 pwwn 20:00:00:25:b5:00:00:0f
device-alias name SP-VDI-01-fc0 pwwn 20:00:00:25:b5:00:00:2c
device-alias name x210c-SP_HBA1 pwwn 20:00:00:25:b5:03:9a:04
device-alias name Infra01-8-hba1 pwwn 20:00:00:25:b5:3a:00:4f
device-alias name Infra02-16-hba1 pwwn 20:00:00:25:b5:3a:00:2f
```

```
device-alias commit
```

```
fcdomain fcid database
```

```
vsan 1 wwn 52:4a:93:72:0d:21:6b:11 fcid 0x290000 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:10 fcid 0x290100 dynamic
vsan 1 wwn 20:20:00:2a:6a:d3:df:80 fcid 0x290200 dynamic
vsan 1 wwn 24:01:00:2a:6a:d3:df:80 fcid 0x290400 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:00 fcid 0x290400 dynamic

vsan 1 wwn 50:01:73:80:59:16:01:10 fcid 0x290500 dynamic
vsan 1 wwn 50:01:73:80:59:16:01:20 fcid 0x290600 dynamic
!
[A400_N2P1]
vsan 1 wwn 50:01:73:80:59:16:01:30 fcid 0x290700 dynamic
!
[A400_N3P1]
vsan 1 wwn 50:01:73:80:59:16:01:12 fcid 0x290800 dynamic
!
[A400_N1P3]
vsan 1 wwn 50:01:73:80:59:16:01:22 fcid 0x290900 dynamic
!
[A400_N2P3]
vsan 1 wwn 50:01:73:80:59:16:01:32 fcid 0x290a00 dynamic
!
[A400_N3P3]
vsan 400 wwn 50:01:73:80:59:16:01:10 fcid 0xa30400 dynamic
vsan 400 wwn 50:01:73:80:59:16:01:20 fcid 0xa30400 dynamic
!
[A400_N2P1]
vsan 400 wwn 50:01:73:80:59:16:01:30 fcid 0xa30500 dynamic
!
[A400_N3P1]
vsan 400 wwn 50:01:73:80:59:16:01:12 fcid 0xa30600 dynamic
!
[A400_N1P3]
vsan 400 wwn 50:01:73:80:59:16:01:22 fcid 0xa30700 dynamic
!
[A400_N2P3]
vsan 400 wwn 50:01:73:80:59:16:01:32 fcid 0xa30800 dynamic
!
[A400_N3P3]
vsan 1 wwn 20:4d:54:7f:ee:83:42:00 fcid 0x290b00 dynamic
```

```
vsan 1 wwn 20:4e:54:7f:ee:83:42:00 fcid 0x290c00 dynamic
vsan 1 wwn 20:4f:54:7f:ee:83:42:00 fcid 0x290d00 dynamic
vsan 1 wwn 20:50:54:7f:ee:83:42:00 fcid 0x290e00 dynamic
vsan 400 wwn 50:0a:09:84:80:d3:67:d3 fcid 0x680000 dynamic
vsan 400 wwn 20:03:00:a0:98:af:bd:e8 fcid 0x680001 dynamic
!
[A400-02-0g]
vsan 400 wwn 50:0a:09:84:80:13:41:27 fcid 0x680100 dynamic
vsan 400 wwn 20:01:00:a0:98:af:bd:e8 fcid 0x680101 dynamic
!
[A400-01-0g]
vsan 400 wwn 20:02:00:de:fb:90:a0:80 fcid 0x680200 dynamic
vsan 400 wwn 20:03:00:de:fb:90:a0:80 fcid 0x680400 dynamic
vsan 400 wwn 20:04:00:de:fb:90:a0:80 fcid 0x680400 dynamic
vsan 400 wwn 20:01:00:de:fb:90:a0:80 fcid 0x680500 dynamic
vsan 400 wwn 20:00:00:25:b5:3a:00:49 fcid 0x680308 dynamic
!
[VDI-29-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:1a fcid 0x680415 dynamic
!
[VDI-28-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:4b fcid 0x680206 dynamic
!
[VDI-19-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:0a fcid 0x680508 dynamic
!
[VDI-27-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:0c fcid 0x680307 dynamic
!
[VDI-17-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:2c fcid 0x680402 dynamic
!
[VDI-15-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:3a fcid 0x680210 dynamic
!
[VDI-26-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:4a fcid 0x680505 dynamic
!
[VDI-24-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:2a fcid 0x680413 dynamic
!
[VDI-25-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:1c fcid 0x680207 dynamic
!
[VDI-18-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:3c fcid 0x680502 dynamic
!
[VDI-32-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:0b fcid 0x68020b dynamic
!
[VDI-22-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:4c fcid 0x680208 dynamic
!
[VDI-14-hba1]
```

```
vsan 400 wwn 20:00:00:25:b5:3a:00:39 fcid 0x680306 dynamic
!           [VDI-30-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:0d fcid 0x68040d dynamic
!           [VDI-12-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:1e fcid 0x680501 dynamic
!           [VDI-31-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:2b fcid 0x680202 dynamic
!           [VDI-20-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:0e fcid 0x680203 dynamic
!           [VDI-7-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:1b fcid 0x680509 dynamic
!           [VDI-23-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:2f fcid 0x680401 dynamic
!           [Infra02-16-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:4d fcid 0x680302 dynamic
!           [VDI-9-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:1d fcid 0x680507 dynamic
!           [VDI-13-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:3d fcid 0x68040e dynamic
!           [VDI-11-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:2d fcid 0x680305 dynamic
!           [VDI-10-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:3b fcid 0x680303 dynamic
!           [VDI-21-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:0f fcid 0x680201 dynamic
!           [VDI-2-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:3f fcid 0x680506 dynamic
!           [VDI-1-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:3e fcid 0x680304 dynamic
!           [VDI-6-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:4f fcid 0x680406 dynamic
!           [Infra01-8-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:1f fcid 0x680204 dynamic
!           [VDI-3-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:4e fcid 0x680504 dynamic
!           [VDI-4-hba1]
vsan 400 wwn 20:00:00:25:b5:3a:00:2e fcid 0x68050a dynamic
!           [VDI-5-hba1]
vsan 1 wwn 56:c9:ce:90:0d:e8:24:02 fcid 0x290f00 dynamic
```

---

!Active Zone Database Section for vsan 400

zone name A400\_VDI-1-hba1 vsan 400  
    member pwwn 20:00:00:25:b5:3a:00:3f  
!                    [VDI-1-hba1]  
    member pwwn 20:01:00:a0:98:af:bd:e8  
!                    [A400-01-0g]  
    member pwwn 20:03:00:a0:98:af:bd:e8  
!                    [A400-02-0g]

zone name A400\_VDI-2-hba1 vsan 400  
    member pwwn 20:01:00:a0:98:af:bd:e8  
!                    [A400-01-0g]  
    member pwwn 20:03:00:a0:98:af:bd:e8  
!                    [A400-02-0g]  
    member pwwn 20:00:00:25:b5:3a:00:0f  
!                    [VDI-2-hba1]

zone name A400\_VDI-3-hba1 vsan 400  
    member pwwn 20:01:00:a0:98:af:bd:e8  
!                    [A400-01-0g]  
    member pwwn 20:03:00:a0:98:af:bd:e8  
!                    [A400-02-0g]  
    member pwwn 20:00:00:25:b5:3a:00:1f  
!                    [VDI-3-hba1]

zone name A400\_VDI-4-hba1 vsan 400  
    member pwwn 20:01:00:a0:98:af:bd:e8  
!                    [A400-01-0g]  
    member pwwn 20:03:00:a0:98:af:bd:e8  
!                    [A400-02-0g]  
    member pwwn 20:00:00:25:b5:3a:00:4e  
!                    [VDI-4-hba1]

zone name A400\_VDI-5-hba1 vsan 400  
    member pwwn 20:01:00:a0:98:af:bd:e8  
!                    [A400-01-0g]  
    member pwwn 20:03:00:a0:98:af:bd:e8  
!                    [A400-02-0g]

---

```
    member pwnn 20:00:00:25:b5:3a:00:2e
!           [VDI-5-hba1]
```

```
zone name A400_VDI-6-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:3e
!           [VDI-6-hba1]
```

```
zone name A400_VDI-7-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:0e
!           [VDI-7-hba1]
```

```
zone name A400_Infra01-8-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:4f
!           [Infra01-8-hba1]
```

```
zone name A400_VDI-9-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:4d
!           [VDI-9-hba1]
```

```
zone name A400_VDI-10-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
```

```
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:2d
!           [VDI-10-hba1]

zone name A400_VDI-11-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:3d
!           [VDI-11-hba1]

zone name A400_VDI-12-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:0d
!           [VDI-12-hba1]

zone name A400_VDI-13-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:1d
!           [VDI-13-hba1]

zone name A400_VDI-14-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:4c
!           [VDI-14-hba1]

zone name A400_VDI-15-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
```

---

```
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:2c
!           [VDI-15-hba1]
```

```
zone name A400_Infra02-16-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:2f
!           [Infra02-16-hba1]
```

```
zone name A400_VDI-17-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:0c
!           [VDI-17-hba1]
```

```
zone name A400_VDI-18-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:1c
!           [VDI-18-hba1]
```

```
zone name A400_VDI-19-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:4b
!           [VDI-19-hba1]
```

```
zone name A400_VDI-20-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
```

```
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:2b
!           [VDI-20-hba1]
```

```
zone name A400_VDI-21-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:3b
!           [VDI-21-hba1]
```

```
zone name A400_VDI-22-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:0b
!           [VDI-22-hba1]
```

```
zone name A400_VDI-23-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:1b
!           [VDI-23-hba1]
```

```
zone name A400_VDI-24-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:4a
!           [VDI-24-hba1]
```

```
zone name A400_VDI-25-hba1 vsan 400
```



---

```
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:2a
!           [VDI-25-hba1]
```

```
zone name A400_VDI-26-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:3a
!           [VDI-26-hba1]
```

```
zone name A400_VDI-27-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:0a
!           [VDI-27-hba1]
```

```
zone name A400_VDI-28-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:1a
!           [VDI-28-hba1]
```

```
zone name A400_VDI-29-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:49
!           [VDI-29-hba1]
```

```
zone name A400_VDI-30-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:39
!           [VDI-30-hba1]
```

```
zone name A400_VDI-31-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:1e
!           [VDI-31-hba1]
```

```
zone name A400_VDI-32-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:3c
!           [VDI-32-hba1]
```

```
zoneset name FlexPod_FabricA vsan 400
  member A400_VDI-1-hba1
  member A400_VDI-2-hba1
  member A400_VDI-3-hba1
  member A400_VDI-4-hba1
  member A400_VDI-5-hba1
  member A400_VDI-6-hba1
  member A400_VDI-7-hba1
  member A400_Infra01-8-hba1
  member A400_VDI-9-hba1
  member A400_VDI-10-hba1
  member A400_VDI-11-hba1
  member A400_VDI-12-hba1
  member A400_VDI-13-hba1
  member A400_VDI-14-hba1
```

```
member A400_VDI-15-hba1
member A400_Infra02-16-hba1
member A400_VDI-17-hba1
member A400_VDI-18-hba1
member A400_VDI-19-hba1
member A400_VDI-20-hba1
member A400_VDI-21-hba1
member A400_VDI-22-hba1
member A400_VDI-23-hba1
member A400_VDI-24-hba1
member A400_VDI-25-hba1
member A400_VDI-26-hba1
member A400_VDI-27-hba1
member A400_VDI-28-hba1
member A400_VDI-29-hba1
member A400_VDI-30-hba1
member A400_VDI-31-hba1
member A400_VDI-32-hba1
```

```
zoneset activate name FlexPod_FabricA vsan 400
```

```
do clear zone database vsan 400
```

```
!Full Zone Database Section for vsan 400
```

```
zone name A400_VDI-1-hba1 vsan 400
```

```
member pwnn 20:00:00:25:b5:3a:00:3f
```

```
! [VDI-1-hba1]
```

```
member pwnn 20:01:00:a0:98:af:bd:e8
```

```
! [A400-01-0g]
```

```
member pwnn 20:03:00:a0:98:af:bd:e8
```

```
! [A400-02-0g]
```

```
zone name A400_VDI-2-hba1 vsan 400
```

```
member pwnn 20:01:00:a0:98:af:bd:e8
```

```
! [A400-01-0g]
```

```
member pwnn 20:03:00:a0:98:af:bd:e8
```

```
! [A400-02-0g]
```

```
member pwnn 20:00:00:25:b5:3a:00:0f
```

```
! [VDI-2-hba1]
```

```
zone name A400_VDI-3-hba1 vsan 400
```

---

```
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:1f
!           [VDI-3-hba1]
```

```
zone name A400_VDI-4-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:4e
!           [VDI-4-hba1]
```

```
zone name A400_VDI-5-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:2e
!           [VDI-5-hba1]
```

```
zone name A400_VDI-6-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:3e
!           [VDI-6-hba1]
```

```
zone name A400_VDI-7-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:0e
!           [VDI-7-hba1]
```

---

```
zone name A400_Infra01-8-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:1e
!           [VDI-31-hba1]
```

```
zone name A400_VDI-9-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:4d
!           [VDI-9-hba1]
```

```
zone name A400_VDI-10-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:2d
!           [VDI-10-hba1]
```

```
zone name A400_VDI-11-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:3d
!           [VDI-11-hba1]
```

```
zone name A400_VDI-12-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:0d
!           [VDI-12-hba1]
```

---

```
zone name A400_VDI-13-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:1d
!           [VDI-13-hba1]
```

```
zone name A400_VDI-14-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:4c
!           [VDI-14-hba1]
```

```
zone name A400_VDI-15-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:2c
!           [VDI-15-hba1]
```

```
zone name A400_Infra02-16-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:2f
!           [Infra02-16-hba1]
```

```
zone name A400_VDI-17-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:0c
```

```
! [VDI-17-hba1]

zone name A400_VDI-18-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
! [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
! [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:1c
! [VDI-18-hba1]
```

```
zone name A400_VDI-19-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
! [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
! [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:4b
! [VDI-19-hba1]
```

```
zone name A400_VDI-20-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
! [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
! [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:2b
! [VDI-20-hba1]
```

```
zone name A400_VDI-21-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
! [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
! [A400-02-0g]
  member pwwn 20:00:00:25:b5:3a:00:3b
! [VDI-21-hba1]
```

```
zone name A400_VDI-22-hba1 vsan 400
  member pwwn 20:01:00:a0:98:af:bd:e8
! [A400-01-0g]
  member pwwn 20:03:00:a0:98:af:bd:e8
! [A400-02-0g]
```

---

```
    member pwnn 20:00:00:25:b5:3a:00:0b
!           [VDI-22-hba1]
```

```
zone name A400_VDI-23-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:1b
!           [VDI-23-hba1]
```

```
zone name A400_VDI-24-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:4a
!           [VDI-24-hba1]
```

```
zone name A400_VDI-25-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:2a
!           [VDI-25-hba1]
```

```
zone name A400_VDI-26-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
    member pwnn 20:00:00:25:b5:3a:00:3a
!           [VDI-26-hba1]
```

```
zone name A400_VDI-27-hba1 vsan 400
    member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
    member pwnn 20:03:00:a0:98:af:bd:e8
```



---

```
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:0a
!           [VDI-27-hba1]
```

```
zone name A400_VDI-28-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:1a
!           [VDI-28-hba1]
```

```
zone name A400_VDI-29-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:49
!           [VDI-29-hba1]
```

```
zone name A400_VDI-30-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:39
!           [VDI-30-hba1]
```

```
zone name A400_VDI-31-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
  member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
  member pwnn 20:00:00:25:b5:3a:00:1e
!           [VDI-31-hba1]
```

```
zone name A400_VDI-32-hba1 vsan 400
  member pwnn 20:01:00:a0:98:af:bd:e8
!           [A400-01-0g]
```

```
member pwnn 20:03:00:a0:98:af:bd:e8
!           [A400-02-0g]
member pwnn 20:00:00:25:b5:3a:00:3c
!           [VDI-32-hba1]
```

```
zoneset name FlexPod_FabricA vsan 400
```

```
member A400_VDI-1-hba1
member A400_VDI-2-hba1
member A400_VDI-3-hba1
member A400_VDI-4-hba1
member A400_VDI-5-hba1
member A400_VDI-6-hba1
member A400_VDI-7-hba1
member A400_Infra01-8-hba1
member A400_VDI-9-hba1
member A400_VDI-10-hba1
member A400_VDI-11-hba1
member A400_VDI-12-hba1
member A400_VDI-13-hba1
member A400_VDI-14-hba1
member A400_VDI-15-hba1
member A400_Infra02-16-hba1
member A400_VDI-17-hba1
member A400_VDI-18-hba1
member A400_VDI-19-hba1
member A400_VDI-20-hba1
member A400_VDI-21-hba1
member A400_VDI-22-hba1
member A400_VDI-23-hba1
member A400_VDI-24-hba1
member A400_VDI-25-hba1
member A400_VDI-26-hba1
member A400_VDI-27-hba1
member A400_VDI-28-hba1
member A400_VDI-29-hba1
member A400_VDI-30-hba1
member A400_VDI-31-hba1
member A400_VDI-32-hba1
```

```
interface mgmt0
  ip address 10.29.164.238 255.255.255.0

interface port-channel1
  channel mode active
  switchport rate-mode dedicated

interface port-channel2
  channel mode active
  switchport rate-mode dedicated

interface port-channel30
  switchport rate-mode dedicated
vsan database
  vsan 400 interface fc1/37
  vsan 400 interface fc1/38
  vsan 400 interface fc1/43
  vsan 400 interface fc1/44
  vsan 400 interface fc1/45
  vsan 400 interface fc1/46
switchname MDS-A
no terminal log-all
line console
  terminal width 80
line vty
boot kickstart bootflash:/m9100-s5ek9-kickstart-mz.8.1.1.bin
boot system bootflash:/m9100-s5ek9-mz.8.1.1.bin
interface fc1/13
  switchport speed 8000
interface fc1/14
  switchport speed 8000
interface fc1/15
  switchport speed 8000
interface fc1/16
  switchport speed 8000
interface fc1/1
interface fc1/2
```

---

```
interface fc1/11
interface fc1/12
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/17
interface fc1/18
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
interface fc1/41
```

---

```
interface fc1/42
interface fc1/47
interface fc1/48
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/1
interface fc1/2
interface fc1/11
interface fc1/12
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
```

```
interface fc1/1
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/2
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/3
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/4
  switchport trunk mode off
```

---

```
port-license acquire
no shutdown
```

```
interface fc1/5
  port-license acquire
  no shutdown
```

```
interface fc1/6
  port-license acquire
  no shutdown
```

```
interface fc1/7
  port-license acquire
  no shutdown
```

```
interface fc1/8
  port-license acquire
  no shutdown
```

```
interface fc1/9
  port-license acquire
```

```
interface fc1/10
  port-license acquire
```

```
interface fc1/11
  port-license acquire
```

```
interface fc1/12
  port-license acquire
```

```
interface fc1/13
  port-license acquire
  no shutdown
```

```
interface fc1/14
  port-license acquire
  no shutdown
```

---

```
interface fc1/15
  port-license acquire
  no shutdown

interface fc1/16
  port-license acquire
  no shutdown

interface fc1/17
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/18
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/19
  switchport description CS700 CTRL-A:01
  port-license acquire
  no shutdown

interface fc1/20
  switchport description CS700 CTRL-A:05
  port-license acquire
  no shutdown

interface fc1/21
  switchport description Launcher-FIA
  port-license acquire
  no shutdown

interface fc1/22
  switchport description Launcher-FIA
  port-license acquire
  no shutdown

interface fc1/23
```

---

```
switchport description Launcher-FIA
port-license acquire
no shutdown
```

```
interface fc1/24
switchport description Launcher-FIA
port-license acquire
no shutdown
```

```
interface fc1/25
port-license acquire
no shutdown
```

```
interface fc1/26
port-license acquire
no shutdown
```

```
interface fc1/27
port-license acquire
no shutdown
```

```
interface fc1/28
port-license acquire
no shutdown
```

```
interface fc1/29
port-license acquire
```

```
interface fc1/30
port-license acquire
```

```
interface fc1/31
port-license acquire
```

```
interface fc1/32
port-license acquire
```

```
interface fc1/33
port-license acquire
```



---

```
interface fc1/34
  port-license acquire
```

```
interface fc1/35
  port-license acquire
```

```
interface fc1/36
  port-license acquire
```

```
interface fc1/37
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/38
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/39
  port-license acquire
  no shutdown
```

```
interface fc1/40
  port-license acquire
  no shutdown
```

```
interface fc1/41
  port-license acquire
  no shutdown
```

```
interface fc1/42
  port-license acquire
  no shutdown
```

```
interface fc1/43
  port-license acquire
  no shutdown
```

```
interface fc1/44
  port-license acquire
  no shutdown

interface fc1/45
  port-license acquire
  no shutdown

interface fc1/46
  port-license acquire
  no shutdown

interface fc1/47
  port-license acquire
  no shutdown

interface fc1/48
  port-license acquire
  no shutdown
ip default-gateway 10.29.164.1
```

MDS-A#

## Cisco MDS 9132T - B Configuration

```
login as: admin
User Access Verification
Using keyboard-interactive authentication.
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
MDS-B# show run
```

```
!Command: show running-config
```

```
!Time: Wed Feb 7 00:55:59 2018
```

```
version 8.1(1)
```

```
power redundancy-mode redundant
```

```
feature npiv
```

```
feature fport-channel-trunk
```

```
role name default-role
```

```
description This is a system defined role and applies to all users.
```

```
rule 5 permit show feature environment
```

```
rule 4 permit show feature hardware
```

```
rule 3 permit show feature module
```

```
rule 2 permit show feature snmp
```

```
rule 1 permit show feature system
```

```
no password strength-check
```

```
username admin password 5 $1$OPnyy3RN$s8SLqLN3W3JPvf4rEb2CD0 role network-admin
```

```
ip domain-lookup
```

```
ip host MDS-B 10.29.164.239
```

```
aaa group server radius radius
```

```
snmp-server user admin network-admin auth md5 0xc9e1af5dbb0bbac72253a1bef037bbbe  
priv 0xc9e1af5dbb0bbac72253a1bef037bbbe localizedkey
```

```
snmp-server host 10.155.160.192 traps version 2c public udp-port 1164
```

```
snmp-server host 10.29.164.250 traps version 2c public udp-port 1163
```

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

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

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

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

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

```
snmp-server community public group network-operator
```

```
vsan database
```

```
vsan 4 name "SP-FAB-B"
```

```
vsan 401
```

```
vsan 401 name "FlexPod-B"
```

```
fcdroplacency network 2000 vsan 1
```

```
device-alias database
```

```
device-alias name A400_N2P2 pwnn 50:01:73:80:59:16:01:21
```

```
device-alias name VDI-1-hba2 pwnn 20:00:00:25:d5:06:00:3f
```

```
device-alias name VDI-2-hba2 pwwn 20:00:00:25:d5:06:00:0f
device-alias name VDI-3-hba2 pwwn 20:00:00:25:d5:06:00:1f
device-alias name VDI-4-hba2 pwwn 20:00:00:25:d5:06:00:4e
device-alias name VDI-5-hba2 pwwn 20:00:00:25:d5:06:00:2e
device-alias name VDI-6-hba2 pwwn 20:00:00:25:d5:06:00:3e
device-alias name VDI-7-hba2 pwwn 20:00:00:25:d5:06:00:0e
device-alias name VDI-9-hba2 pwwn 20:00:00:25:d5:06:00:4d
device-alias name A400-01-0h pwwn 20:02:00:a0:98:af:bd:e8
device-alias name A400-02-0h pwwn 20:04:00:a0:98:af:bd:e8
device-alias name srv01_HBA2 pwwn 20:00:00:25:b5:03:9a:13
device-alias name srv02_HBA2 pwwn 20:00:00:25:b5:03:9a:15
device-alias name srv03_HBA2 pwwn 20:00:00:25:b5:03:9a:0f
device-alias name srv04_HBA2 pwwn 20:00:00:25:b5:03:9a:01
device-alias name srv05_HBA2 pwwn 20:00:00:25:b5:03:9a:03
device-alias name srv06_HBA2 pwwn 20:00:00:25:b5:03:9a:0d
device-alias name srv07_HBA2 pwwn 20:00:00:25:b5:03:9a:11
device-alias name srv09_HBA2 pwwn 20:00:00:25:b5:03:9a:17
device-alias name srv10_HBA2 pwwn 20:00:00:25:b5:03:9a:19
device-alias name srv11_HBA2 pwwn 20:00:00:25:b5:03:9a:1b
device-alias name srv12_HBA2 pwwn 20:00:00:25:b5:03:9a:1d
device-alias name srv13_HBA2 pwwn 20:00:00:25:b5:03:9a:1f
device-alias name srv14_HBA2 pwwn 20:00:00:25:b5:03:9a:21
device-alias name srv15_HBA2 pwwn 20:00:00:25:b5:03:9a:23
device-alias name srv17_HBA2 pwwn 20:00:00:25:b5:03:9a:25
device-alias name srv18_HBA2 pwwn 20:00:00:25:b5:03:9a:27
device-alias name srv19_HBA2 pwwn 20:00:00:25:b5:03:9a:31
device-alias name srv20_HBA2 pwwn 20:00:00:25:b5:03:9a:29
device-alias name srv21_HBA2 pwwn 20:00:00:25:b5:03:9a:2b
device-alias name srv22_HBA2 pwwn 20:00:00:25:b5:03:9a:2d
device-alias name srv23_HBA2 pwwn 20:00:00:25:b5:03:9a:2f
device-alias name srv24_HBA2 pwwn 20:00:00:25:b5:03:9a:33
device-alias name srv25_HBA2 pwwn 20:00:00:25:b5:03:9a:35
device-alias name srv26_HBA2 pwwn 20:00:00:25:b5:03:9a:37
device-alias name srv27_HBA2 pwwn 20:00:00:25:b5:03:9a:39
device-alias name srv28_HBA2 pwwn 20:00:00:25:b5:03:9a:3b
device-alias name srv29_HBA2 pwwn 20:00:00:25:b5:03:9a:3d
device-alias name VDI-10-hba2 pwwn 20:00:00:25:d5:06:00:2d
device-alias name VDI-11-hba2 pwwn 20:00:00:25:d5:06:00:3d
device-alias name VDI-12-hba2 pwwn 20:00:00:25:d5:06:00:0d
```

```
device-alias name VDI-13-hba2 pwwn 20:00:00:25:d5:06:00:1d
device-alias name VDI-14-hba2 pwwn 20:00:00:25:d5:06:00:4c
device-alias name VDI-15-hba2 pwwn 20:00:00:25:d5:06:00:2c
device-alias name VDI-17-hba2 pwwn 20:00:00:25:d5:06:00:0c
device-alias name VDI-18-hba2 pwwn 20:00:00:25:d5:06:00:1c
device-alias name VDI-19-hba2 pwwn 20:00:00:25:d5:06:00:4b
device-alias name VDI-20-hba2 pwwn 20:00:00:25:d5:06:00:2b
device-alias name VDI-21-hba2 pwwn 20:00:00:25:d5:06:00:3b
device-alias name VDI-22-hba2 pwwn 20:00:00:25:d5:06:00:6b
device-alias name VDI-23-hba2 pwwn 20:00:00:25:d5:06:00:1b
device-alias name VDI-24-hba2 pwwn 20:00:00:25:d5:06:00:4a
device-alias name VDI-25-hba2 pwwn 20:00:00:25:d5:06:00:2a
device-alias name VDI-26-hba2 pwwn 20:00:00:25:d5:06:00:3a
device-alias name VDI-27-hba2 pwwn 20:00:00:25:d5:06:00:0a
device-alias name VDI-28-hba2 pwwn 20:00:00:25:d5:06:00:1a
device-alias name VDI-29-hba2 pwwn 20:00:00:25:d5:06:00:49
device-alias name VDI-30-hba2 pwwn 20:00:00:25:d5:06:00:39
device-alias name VDI-31-hba2 pwwn 20:00:00:25:d5:06:00:1e
device-alias name VDI-32-hba2 pwwn 20:00:00:25:d5:06:00:3c
device-alias name SP-Infra2-fc1 pwwn 20:00:00:25:b5:00:00:1f
device-alias name X210c-SP_HBA2 pwwn 20:00:00:25:b5:03:9a:05
device-alias name Infra01-8-hba2 pwwn 20:00:00:25:d5:06:00:4f
device-alias name Infra02-16-hba2 pwwn 20:00:00:25:d5:06:00:2f
```

```
device-alias commit
```

```
fcdomain fcid database
```

```
vsan 1 wwn 20:20:00:2a:6a:d9:84:c0 fcid 0xb25000 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:05 fcid 0x5b1400 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:01 fcid 0xb60100 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:00 fcid 0xb60200 dynamic
vsan 401 wwn 20:20:00:2a:6a:d9:84:c0 fcid 0x6b0000 dynamic
vsan 401 wwn 20:1f:00:2a:6a:d9:84:c0 fcid 0x6b0100 dynamic
vsan 1 wwn 24:01:00:2a:6a:d9:84:c0 fcid 0xb60400 dynamic
vsan 401 wwn 24:01:00:2a:6a:d9:84:c0 fcid 0x6b0200 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:10 fcid 0xb60400 dynamic
vsan 4 wwn 24:01:00:2a:6a:d9:84:c0 fcid 0x5b0000 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:02 fcid 0x5b0100 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:06 fcid 0x5b0200 dynamic
```

```
vsan 4 wwn 20:00:00:25:b5:00:00:5a fcid 0x5b0004 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:1b fcid 0x5b0019 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:19 fcid 0x5b001f dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:1a fcid 0x5b0002 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:3a fcid 0x5b0012 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:1f fcid 0x5b001e dynamic
!      [SP-Infra2-fc1]
vsan 4 wwn 20:00:00:25:b5:00:00:58 fcid 0x5b001c dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:3c fcid 0x5b0008 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:3f fcid 0x5b0003 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:5b fcid 0x5b0006 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:3b fcid 0x5b0001 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:38 fcid 0x5b001b dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:1c fcid 0x5b0007 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:49 fcid 0x5b0021 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:08 fcid 0x5b0005 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:39 fcid 0x5b0009 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:02 fcid 0xb60500 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:12 fcid 0xb60600 dynamic
vsan 1 wwn 52:4a:93:72:0d:21:6b:13 fcid 0xb60700 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:37 fcid 0x5b0011 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:24 fcid 0x5b0014 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:05 fcid 0x5b001a dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:53 fcid 0x5b000b dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:42 fcid 0x5b0017 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:33 fcid 0x5b000f dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:62 fcid 0x5b0010 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:51 fcid 0x5b0015 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:44 fcid 0x5b000c dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:13 fcid 0x5b000e dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:02 fcid 0x5b0016 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:31 fcid 0x5b0018 dynamic
vsan 4 wwn 56:c9:ce:90:bc:34:85:02 fcid 0x5b0400 dynamic
vsan 4 wwn 56:c9:ce:90:bc:34:85:04 fcid 0x5b0400 dynamic
vsan 4 wwn 56:c9:ce:90:bc:34:85:06 fcid 0x5b0500 dynamic
vsan 4 wwn 56:c9:ce:90:bc:34:85:08 fcid 0x5b0600 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:0a fcid 0x5b0700 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:0c fcid 0x5b0800 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:0e fcid 0x5b0900 dynamic
```

```
vsan 4 wwn 56:c9:ce:90:0d:e8:24:10 fcid 0x5b0a00 dynamic
vsan 4 wwn 20:1e:00:2a:6a:d9:84:c0 fcid 0x5b0b00 dynamic
vsan 4 wwn 20:1d:00:2a:6a:d9:84:c0 fcid 0x5b0c00 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:25 fcid 0x5b000a dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:04 fcid 0x5b000d dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:22 fcid 0x5b0013 dynamic
vsan 1 wwn 50:01:73:80:59:16:01:11 fcid 0xb60800 dynamic
vsan 1 wwn 50:01:73:80:59:16:01:21 fcid 0xb60900 dynamic
!
[A400_N2P2]
vsan 1 wwn 50:01:73:80:59:16:01:31 fcid 0xb60a00 dynamic
vsan 1 wwn 50:01:73:80:59:16:01:13 fcid 0xb60b00 dynamic
vsan 1 wwn 50:01:73:80:59:16:01:23 fcid 0xb60c00 dynamic
vsan 1 wwn 50:01:73:80:59:16:01:33 fcid 0xb60d00 dynamic
vsan 401 wwn 50:01:73:80:59:16:01:11 fcid 0x6b0400 dynamic
vsan 401 wwn 50:01:73:80:59:16:01:21 fcid 0x6b0400 dynamic
!
[A400_N2P2]
vsan 401 wwn 50:01:73:80:59:16:01:31 fcid 0x6b0500 dynamic
vsan 401 wwn 50:01:73:80:59:16:01:13 fcid 0x6b0600 dynamic
vsan 401 wwn 50:01:73:80:59:16:01:23 fcid 0x6b0700 dynamic
vsan 401 wwn 50:01:73:80:59:16:01:33 fcid 0x6b0800 dynamic
vsan 1 wwn 20:4d:54:7f:ee:77:5b:c0 fcid 0xb60e00 dynamic
vsan 1 wwn 20:4e:54:7f:ee:77:5b:c0 fcid 0xb60f00 dynamic
vsan 1 wwn 20:4f:54:7f:ee:77:5b:c0 fcid 0xb61000 dynamic
vsan 1 wwn 20:50:54:7f:ee:77:5b:c0 fcid 0xb61100 dynamic
vsan 401 wwn 20:4d:54:7f:ee:77:5b:c0 fcid 0x6b0900 dynamic
vsan 401 wwn 20:4e:54:7f:ee:77:5b:c0 fcid 0x6b0a00 dynamic
vsan 401 wwn 20:4f:54:7f:ee:77:5b:c0 fcid 0x6b0b00 dynamic
vsan 401 wwn 20:50:54:7f:ee:77:5b:c0 fcid 0x6b0c00 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:0f fcid 0x6b1004 dynamic
!
[srv03_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:01 fcid 0x6b0f03 dynamic
!
[srv04_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:03 fcid 0x6b0e01 dynamic
!
[srv05_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:0d fcid 0x6b0e09 dynamic
!
[srv06_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:17 fcid 0x6b0d07 dynamic
!
[srv09_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:19 fcid 0x6b0e05 dynamic
```

```
! [srv10_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:1b fcid 0x6b0f09 dynamic
! [srv11_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:1d fcid 0x6b1001 dynamic
! [srv12_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:1f fcid 0x6b0d06 dynamic
! [srv13_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:21 fcid 0x6b0f07 dynamic
! [srv14_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:35 fcid 0x6b0d09 dynamic
! [srv25_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:37 fcid 0x6b0f02 dynamic
! [srv26_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:39 fcid 0x6b0f01 dynamic
! [srv27_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:3b fcid 0x6b0e0b dynamic
! [srv28_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:13 fcid 0x6b1003 dynamic
! [srv01_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:2b fcid 0x6b0e04 dynamic
! [srv21_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:27 fcid 0x6b0d01 dynamic
! [srv18_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:15 fcid 0x6b0f08 dynamic
! [srv02_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:29 fcid 0x6b0f04 dynamic
! [srv20_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:25 fcid 0x6b0d04 dynamic
! [srv17_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:0b fcid 0x6b0d03 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:31 fcid 0x6b0e03 dynamic
! [srv19_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:2d fcid 0x6b1002 dynamic
! [srv22_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:09 fcid 0x6b1006 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:33 fcid 0x6b1008 dynamic
! [srv24_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:3d fcid 0x6b0e0a dynamic
! [srv29_HBA2]
```



```
vsan 401 wwn 20:00:00:25:b5:03:9a:3f fcid 0x6b0d02 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:43 fcid 0x6b0c01 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:01 fcid 0x5b0020 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:14 fcid 0x5b0d00 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:18 fcid 0x5b0e00 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:12 fcid 0x5b0f00 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:16 fcid 0x5b1000 dynamic
vsan 4 wwn 20:00:00:25:b5:00:00:40 fcid 0x5b001d dynamic
vsan 4 wwn 20:1f:00:2a:6a:d9:84:c0 fcid 0x5b1100 dynamic
vsan 4 wwn 20:20:00:2a:6a:d9:84:c0 fcid 0x5b1200 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:45 fcid 0x6b0907 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:41 fcid 0x6b1007 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:11 fcid 0x6b0d05 dynamic
!
    [srv07_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:2f fcid 0x6b0e02 dynamic
!
    [srv23_HBA2]
vsan 401 wwn 20:00:00:25:b5:03:9a:23 fcid 0x6b0e08 dynamic
!
    [srv15_HBA2]
vsan 401 wwn 20:4d:00:de:fb:18:3c:00 fcid 0x6b0d00 dynamic
vsan 401 wwn 20:4e:00:de:fb:18:3c:00 fcid 0x6b0e00 dynamic
vsan 401 wwn 20:4f:00:de:fb:18:3c:00 fcid 0x6b0f00 dynamic
vsan 401 wwn 20:50:00:de:fb:18:3c:00 fcid 0x6b1000 dynamic
vsan 401 wwn 20:00:00:25:b5:03:9a:05 fcid 0x6b0e07 dynamic
!
    [X210c-SP_HBA2]
vsan 4 wwn 20:00:00:25:b5:00:00:10 fcid 0x5b0022 dynamic
vsan 4 wwn 20:00:00:25:b5:09:00:1f fcid 0x5b0023 dynamic
vsan 401 wwn 20:01:00:de:fb:92:0c:80 fcid 0x6b1100 dynamic
vsan 401 wwn 20:03:00:de:fb:92:0c:80 fcid 0x6b1200 dynamic
vsan 401 wwn 20:02:00:de:fb:92:0c:80 fcid 0x6b1400 dynamic
vsan 401 wwn 20:04:00:de:fb:92:0c:80 fcid 0x6b1400 dynamic
vsan 401 wwn 20:00:00:25:b5:30:00:4e fcid 0x6b1101 dynamic
vsan 401 wwn 20:00:00:25:d5:06:00:2f fcid 0x6b1201 dynamic
!
    [Infra02-16-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4f fcid 0x6b1408 dynamic
!
    [Infra01-8-hba2]
vsan 401 wwn 50:0a:09:83:80:d3:67:d3 fcid 0x6b1500 dynamic
vsan 401 wwn 20:04:00:a0:98:af:bd:e8 fcid 0x6b1501 dynamic
!
    [A400-02-0h]
vsan 401 wwn 50:0a:09:83:80:13:41:27 fcid 0x6b1600 dynamic
```

```
vsan 401 wwn 20:02:00:a0:98:af:bd:e8 fcid 0x6b1601 dynamic
!           [A400-01-0h]
vsan 401 wwn 20:00:00:25:d5:06:00:3f fcid 0x6b1402 dynamic
!           [VDI-1-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0f fcid 0x6b1412 dynamic
!           [VDI-2-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4e fcid 0x6b140a dynamic
!           [VDI-4-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1f fcid 0x6b1413 dynamic
!           [VDI-3-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2e fcid 0x6b1411 dynamic
!           [VDI-5-hba2]
vsan 401 wwn 24:1f:00:de:fb:92:0c:80 fcid 0x6b1700 dynamic
vsan 401 wwn 20:00:00:25:d5:06:00:3e fcid 0x6b1414 dynamic
!           [VDI-6-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0e fcid 0x6b1409 dynamic
!           [VDI-7-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4d fcid 0x6b1401 dynamic
!           [VDI-9-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2d fcid 0x6b140b dynamic
!           [VDI-10-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0d fcid 0x6b1403 dynamic
!           [VDI-12-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3d fcid 0x6b1415 dynamic
!           [VDI-11-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1d fcid 0x6b1416 dynamic
!           [VDI-13-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4c fcid 0x6b140c dynamic
!           [VDI-14-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2c fcid 0x6b1417 dynamic
!           [VDI-15-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2b fcid 0x6b1419 dynamic
!           [VDI-20-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0c fcid 0x6b140d dynamic
!           [VDI-17-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4a fcid 0x6b141b dynamic
!           [VDI-24-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2a fcid 0x6b140e dynamic
!           [VDI-25-hba2]
```

```
vsan 401 wwn 20:00:00:25:d5:06:00:49 fcid 0x6b1405 dynamic
!           [VDI-29-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3a fcid 0x6b141c dynamic
!           [VDI-26-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1a fcid 0x6b141d dynamic
!           [VDI-28-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:39 fcid 0x6b141e dynamic
!           [VDI-30-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1c fcid 0x6b1418 dynamic
!           [VDI-18-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3b fcid 0x6b1404 dynamic
!           [VDI-21-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4b fcid 0x6b1406 dynamic
!           [VDI-19-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0a fcid 0x6b140f dynamic
!           [VDI-27-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1b fcid 0x6b1407 dynamic
!           [VDI-23-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0b fcid 0x6b141a dynamic
vsan 401 wwn 20:00:00:25:d5:06:00:1e fcid 0x6b1410 dynamic
!           [VDI-31-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3c fcid 0x6b141f dynamic
!           [VDI-32-hba2]
vsan 401 wwn 50:0a:09:83:80:d3:67:d3 fcid 0x870000 dynamic
vsan 401 wwn 20:04:00:a0:98:af:bd:e8 fcid 0x870001 dynamic
!           [A400-02-0h]
vsan 401 wwn 50:0a:09:83:80:13:41:27 fcid 0x870100 dynamic
vsan 401 wwn 20:02:00:a0:98:af:bd:e8 fcid 0x870101 dynamic
!           [A400-01-0h]
vsan 401 wwn 20:01:00:de:fb:92:0c:80 fcid 0x870200 dynamic
vsan 401 wwn 20:02:00:de:fb:92:0c:80 fcid 0x870400 dynamic
vsan 401 wwn 20:03:00:de:fb:92:0c:80 fcid 0x870400 dynamic
vsan 401 wwn 20:04:00:de:fb:92:0c:80 fcid 0x870500 dynamic
vsan 401 wwn 20:00:00:25:d5:06:00:4f fcid 0x870203 dynamic
!           [Infra01-8-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:49 fcid 0x870214 dynamic
!           [VDI-29-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4b fcid 0x870207 dynamic
!           [VDI-19-hba2]
```

```
vsan 401 wwn 20:00:00:25:d5:06:00:1a fcid 0x870406 dynamic
!           [VDI-28-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0a fcid 0x870212 dynamic
!           [VDI-27-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2a fcid 0x870405 dynamic
!           [VDI-25-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3a fcid 0x870508 dynamic
!           [VDI-26-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0c fcid 0x870506 dynamic
!           [VDI-17-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1c fcid 0x87030a dynamic
!           [VDI-18-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4c fcid 0x870507 dynamic
!           [VDI-14-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2c fcid 0x870407 dynamic
!           [VDI-15-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1b fcid 0x870309 dynamic
!           [VDI-23-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3c fcid 0x870520 dynamic
!           [VDI-32-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1e fcid 0x870303 dynamic
!           [VDI-31-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0d fcid 0x870201 dynamic
!           [VDI-12-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2b fcid 0x870501 dynamic
!           [VDI-20-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4a fcid 0x870306 dynamic
!           [VDI-24-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2d fcid 0x870302 dynamic
!           [VDI-10-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4d fcid 0x870401 dynamic
!           [VDI-9-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3d fcid 0x870209 dynamic
!           [VDI-11-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2f fcid 0x870502 dynamic
!           [Infra02-16-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0e fcid 0x870504 dynamic
!           [VDI-7-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3e fcid 0x870305 dynamic
```

```
! [VDI-6-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1f fcid 0x870503 dynamic
! [VDI-3-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3b fcid 0x870505 dynamic
! [VDI-21-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:39 fcid 0x870307 dynamic
! [VDI-30-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:4e fcid 0x870402 dynamic
! [VDI-4-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:2e fcid 0x870403 dynamic
! [VDI-5-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:3f fcid 0x870404 dynamic
! [VDI-1-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0f fcid 0x870304 dynamic
! [VDI-2-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:1d fcid 0x870308 dynamic
! [VDI-13-hba2]
vsan 401 wwn 20:00:00:25:d5:06:00:0b fcid 0x870401 dynamic
vsan 4 wwn 56:c9:ce:90:0d:e8:24:01 fcid 0x5b1400 dynamic
vsan 1 wwn 56:c9:ce:90:0d:e8:24:01 fcid 0xb61200 dynamic
!Active Zone Database Section for vsan 4
zone name SP-VDI-01-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:3c
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-02-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:1c
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0a
```

---

```
zone name SP-VDI-03-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:5b
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-04-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:3b
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0a
```

```
zone name SP-VDI-05-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:1b
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-06-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:5a
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0a
```

```
zone name SP-VDI-07-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:3a
  member pwwn 56:c9:ce:90:0d:e8:24:02
```

---

```
member pwn 56:c9:ce:90:0d:e8:24:06
member pwn 56:c9:ce:90:0d:e8:24:10
member pwn 56:c9:ce:90:0d:e8:24:0c
member pwn 56:c9:ce:90:0d:e8:24:0a
member pwn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-08-fc1 vsan 4
```

```
member pwn 20:00:00:25:b5:00:00:1a
member pwn 56:c9:ce:90:0d:e8:24:02
member pwn 56:c9:ce:90:0d:e8:24:06
member pwn 56:c9:ce:90:0d:e8:24:10
member pwn 56:c9:ce:90:0d:e8:24:0c
member pwn 56:c9:ce:90:0d:e8:24:0e
member pwn 56:c9:ce:90:0d:e8:24:0a
```

```
zone name SP-VDI-09-fc1 vsan 4
```

```
member pwn 20:00:00:25:b5:00:00:49
member pwn 56:c9:ce:90:0d:e8:24:02
member pwn 56:c9:ce:90:0d:e8:24:06
member pwn 56:c9:ce:90:0d:e8:24:0c
member pwn 56:c9:ce:90:0d:e8:24:10
member pwn 56:c9:ce:90:0d:e8:24:0a
member pwn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-10-fc1 vsan 4
```

```
member pwn 20:00:00:25:b5:00:00:39
member pwn 56:c9:ce:90:0d:e8:24:02
member pwn 56:c9:ce:90:0d:e8:24:06
member pwn 56:c9:ce:90:0d:e8:24:10
member pwn 56:c9:ce:90:0d:e8:24:0c
member pwn 56:c9:ce:90:0d:e8:24:0a
member pwn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-11-fc1 vsan 4
```

```
member pwn 20:00:00:25:b5:00:00:19
member pwn 56:c9:ce:90:0d:e8:24:02
member pwn 56:c9:ce:90:0d:e8:24:06
member pwn 56:c9:ce:90:0d:e8:24:10
member pwn 56:c9:ce:90:0d:e8:24:0c
```

---

member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0a

zone name SP-VDI-12-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:58  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-13-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:38  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0a

zone name SP-VDI-14-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:08  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-Infrac1-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:3f  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:10



---

```
zone name SP-Infra2-fc1 vsan 4
  member pwnn 20:00:00:25:b5:00:00:1f
!
  [SP-Infra2-fc1]
  member pwnn 56:c9:ce:90:0d:e8:24:02
  member pwnn 56:c9:ce:90:0d:e8:24:06
  member pwnn 56:c9:ce:90:0d:e8:24:0e
  member pwnn 56:c9:ce:90:0d:e8:24:0a
  member pwnn 56:c9:ce:90:0d:e8:24:10
  member pwnn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-15-fc1 vsan 4
  member pwnn 20:00:00:25:b5:00:00:25
  member pwnn 56:c9:ce:90:0d:e8:24:0a
  member pwnn 56:c9:ce:90:0d:e8:24:0e
  member pwnn 56:c9:ce:90:0d:e8:24:0c
  member pwnn 56:c9:ce:90:0d:e8:24:10
```

```
zone name AFA-VDI-16-fc1 vsan 4
  member pwnn 20:00:00:25:b5:00:00:05
  member pwnn 56:c9:ce:90:0d:e8:24:0a
  member pwnn 56:c9:ce:90:0d:e8:24:0e
  member pwnn 56:c9:ce:90:0d:e8:24:0c
  member pwnn 56:c9:ce:90:0d:e8:24:10
```

```
zone name AFA-VDI-17-fc1 vsan 4
  member pwnn 20:00:00:25:b5:00:00:44
  member pwnn 56:c9:ce:90:0d:e8:24:0e
  member pwnn 56:c9:ce:90:0d:e8:24:0a
  member pwnn 56:c9:ce:90:0d:e8:24:10
  member pwnn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-18-fc1 vsan 4
  member pwnn 20:00:00:25:b5:00:00:24
  member pwnn 56:c9:ce:90:0d:e8:24:0a
  member pwnn 56:c9:ce:90:0d:e8:24:0e
  member pwnn 56:c9:ce:90:0d:e8:24:10
  member pwnn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-19-fc1 vsan 4
```

---

member pwn 20:00:00:25:b5:00:00:04  
member pwn 56:c9:ce:90:0d:e8:24:0a  
member pwn 56:c9:ce:90:0d:e8:24:0e  
member pwn 56:c9:ce:90:0d:e8:24:0c  
member pwn 56:c9:ce:90:0d:e8:24:10

zone name AFA-VDI-20-fc1 vsan 4

member pwn 20:00:00:25:b5:00:00:53  
member pwn 56:c9:ce:90:0d:e8:24:0e  
member pwn 56:c9:ce:90:0d:e8:24:0a  
member pwn 56:c9:ce:90:0d:e8:24:10  
member pwn 56:c9:ce:90:0d:e8:24:0c

zone name AFA-VDI-21-fc1 vsan 4

member pwn 20:00:00:25:b5:00:00:33  
member pwn 56:c9:ce:90:0d:e8:24:0a  
member pwn 56:c9:ce:90:0d:e8:24:0e  
member pwn 56:c9:ce:90:0d:e8:24:0c  
member pwn 56:c9:ce:90:0d:e8:24:10

zone name AFA-VDI-22-fc1 vsan 4

member pwn 20:00:00:25:b5:00:00:13  
member pwn 56:c9:ce:90:0d:e8:24:0a  
member pwn 56:c9:ce:90:0d:e8:24:0e  
member pwn 56:c9:ce:90:0d:e8:24:10  
member pwn 56:c9:ce:90:0d:e8:24:0c

zone name AFA-VDI-23-fc1 vsan 4

member pwn 20:00:00:25:b5:00:00:62  
member pwn 56:c9:ce:90:0d:e8:24:0e  
member pwn 56:c9:ce:90:0d:e8:24:0a  
member pwn 56:c9:ce:90:0d:e8:24:0c  
member pwn 56:c9:ce:90:0d:e8:24:10

zone name AFA-VDI-24-fc1 vsan 4

member pwn 20:00:00:25:b5:00:00:42  
member pwn 56:c9:ce:90:0d:e8:24:0a  
member pwn 56:c9:ce:90:0d:e8:24:0e  
member pwn 56:c9:ce:90:0d:e8:24:10

---

member pwnn 56:c9:ce:90:0d:e8:24:0c

zone name AFA-VDI-25-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:22

member pwnn 56:c9:ce:90:0d:e8:24:0a

member pwnn 56:c9:ce:90:0d:e8:24:0e

member pwnn 56:c9:ce:90:0d:e8:24:0c

member pwnn 56:c9:ce:90:0d:e8:24:10

member pwnn 56:c9:ce:90:0d:e8:24:02

member pwnn 56:c9:ce:90:0d:e8:24:06

zone name AFA-VDI-26-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:02

member pwnn 56:c9:ce:90:0d:e8:24:0a

member pwnn 56:c9:ce:90:0d:e8:24:0e

member pwnn 56:c9:ce:90:0d:e8:24:10

member pwnn 56:c9:ce:90:0d:e8:24:0c

member pwnn 56:c9:ce:90:0d:e8:24:06

member pwnn 56:c9:ce:90:0d:e8:24:02

zone name AFA-VDI-27-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:51

member pwnn 56:c9:ce:90:0d:e8:24:0a

member pwnn 56:c9:ce:90:0d:e8:24:0e

member pwnn 56:c9:ce:90:0d:e8:24:0c

member pwnn 56:c9:ce:90:0d:e8:24:10

member pwnn 56:c9:ce:90:0d:e8:24:02

member pwnn 56:c9:ce:90:0d:e8:24:06

zone name AFA-VDI-28-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:31

member pwnn 56:c9:ce:90:0d:e8:24:0a

member pwnn 56:c9:ce:90:0d:e8:24:0e

member pwnn 56:c9:ce:90:0d:e8:24:10

member pwnn 56:c9:ce:90:0d:e8:24:0c

member pwnn 56:c9:ce:90:0d:e8:24:02

member pwnn 56:c9:ce:90:0d:e8:24:06

zone name M6-a-fc1 vsan 4

---

```
member pwnn 20:00:00:25:b5:00:00:10
member pwnn 56:c9:ce:90:0d:e8:24:02
member pwnn 56:c9:ce:90:0d:e8:24:06
```

```
zoneset name SP-Infra-B vsan 4
```

```
member SP-VDI-01-fc1
member SP-VDI-02-fc1
member SP-VDI-03-fc1
member SP-VDI-04-fc1
member SP-VDI-05-fc1
member SP-VDI-06-fc1
member SP-VDI-07-fc1
member SP-VDI-08-fc1
member SP-VDI-09-fc1
member SP-VDI-10-fc1
member SP-VDI-11-fc1
member SP-VDI-12-fc1
member SP-VDI-13-fc1
member SP-VDI-14-fc1
member SP-Infra1-fc1
member SP-Infra2-fc1
member AFA-VDI-15-fc1
member AFA-VDI-16-fc1
member AFA-VDI-17-fc1
member AFA-VDI-18-fc1
member AFA-VDI-19-fc1
member AFA-VDI-20-fc1
member AFA-VDI-21-fc1
member AFA-VDI-22-fc1
member AFA-VDI-23-fc1
member AFA-VDI-24-fc1
member AFA-VDI-25-fc1
member AFA-VDI-26-fc1
member AFA-VDI-27-fc1
member AFA-VDI-28-fc1
member M6-a-fc1
```

```
zoneset activate name SP-Infra-B vsan 4
do clear zone database vsan 4
```

---

!Full Zone Database Section for vsan 4

zone name SP-VDI-01-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:3c  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-02-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:1c  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0a

zone name SP-VDI-03-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:5b  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-04-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:3b  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0a

zone name SP-VDI-05-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:1b

---

```
member pwnn 56:c9:ce:90:0d:e8:24:02
member pwnn 56:c9:ce:90:0d:e8:24:06
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-06-fc1 vsan 4
```

```
member pwnn 20:00:00:25:b5:00:00:5a
member pwnn 56:c9:ce:90:0d:e8:24:02
member pwnn 56:c9:ce:90:0d:e8:24:06
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0a
```

```
zone name SP-VDI-07-fc1 vsan 4
```

```
member pwnn 20:00:00:25:b5:00:00:3a
member pwnn 56:c9:ce:90:0d:e8:24:02
member pwnn 56:c9:ce:90:0d:e8:24:06
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-VDI-08-fc1 vsan 4
```

```
member pwnn 20:00:00:25:b5:00:00:1a
member pwnn 56:c9:ce:90:0d:e8:24:02
member pwnn 56:c9:ce:90:0d:e8:24:06
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0a
```

```
zone name SP-VDI-09-fc1 vsan 4
```

```
member pwnn 20:00:00:25:b5:00:00:49
member pwnn 56:c9:ce:90:0d:e8:24:02
member pwnn 56:c9:ce:90:0d:e8:24:06
member pwnn 56:c9:ce:90:0d:e8:24:0c
```

---

member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-10-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:39  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-11-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:19  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0a

zone name SP-VDI-12-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:58  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0a  
member pwnn 56:c9:ce:90:0d:e8:24:0e

zone name SP-VDI-13-fc1 vsan 4

member pwnn 20:00:00:25:b5:00:00:38  
member pwnn 56:c9:ce:90:0d:e8:24:02  
member pwnn 56:c9:ce:90:0d:e8:24:06  
member pwnn 56:c9:ce:90:0d:e8:24:10  
member pwnn 56:c9:ce:90:0d:e8:24:0c  
member pwnn 56:c9:ce:90:0d:e8:24:0e  
member pwnn 56:c9:ce:90:0d:e8:24:0a

---

```
zone name SP-VDI-14-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:08
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
```

```
zone name SP-Infra1-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:3f
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
```

```
zone name SP-Infra2-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:1f
!           [SP-Infra2-fc1]
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-15-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:25
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
```

```
zone name AFA-VDI-16-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:05
  member pwwn 56:c9:ce:90:0d:e8:24:0a
```



---

```
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:10
```

```
zone name AFA-VDI-17-fc1 vsan 4
member pwnn 20:00:00:25:b5:00:00:44
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-18-fc1 vsan 4
member pwnn 20:00:00:25:b5:00:00:24
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-19-fc1 vsan 4
member pwnn 20:00:00:25:b5:00:00:04
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:10
```

```
zone name AFA-VDI-20-fc1 vsan 4
member pwnn 20:00:00:25:b5:00:00:53
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:10
member pwnn 56:c9:ce:90:0d:e8:24:0c
```

```
zone name AFA-VDI-21-fc1 vsan 4
member pwnn 20:00:00:25:b5:00:00:33
member pwnn 56:c9:ce:90:0d:e8:24:0a
member pwnn 56:c9:ce:90:0d:e8:24:0e
member pwnn 56:c9:ce:90:0d:e8:24:0c
member pwnn 56:c9:ce:90:0d:e8:24:10
```

---

zone name AFA-VDI-22-fc1 vsan 4  
member pwwn 20:00:00:25:b5:00:00:13  
member pwwn 56:c9:ce:90:0d:e8:24:0a  
member pwwn 56:c9:ce:90:0d:e8:24:0e  
member pwwn 56:c9:ce:90:0d:e8:24:10  
member pwwn 56:c9:ce:90:0d:e8:24:0c

zone name AFA-VDI-23-fc1 vsan 4  
member pwwn 20:00:00:25:b5:00:00:62  
member pwwn 56:c9:ce:90:0d:e8:24:0e  
member pwwn 56:c9:ce:90:0d:e8:24:0a  
member pwwn 56:c9:ce:90:0d:e8:24:0c  
member pwwn 56:c9:ce:90:0d:e8:24:10

zone name AFA-VDI-24-fc1 vsan 4  
member pwwn 20:00:00:25:b5:00:00:42  
member pwwn 56:c9:ce:90:0d:e8:24:0a  
member pwwn 56:c9:ce:90:0d:e8:24:0e  
member pwwn 56:c9:ce:90:0d:e8:24:10  
member pwwn 56:c9:ce:90:0d:e8:24:0c

zone name AFA-VDI-25-fc1 vsan 4  
member pwwn 20:00:00:25:b5:00:00:22  
member pwwn 56:c9:ce:90:0d:e8:24:0a  
member pwwn 56:c9:ce:90:0d:e8:24:0e  
member pwwn 56:c9:ce:90:0d:e8:24:0c  
member pwwn 56:c9:ce:90:0d:e8:24:10  
member pwwn 56:c9:ce:90:0d:e8:24:02  
member pwwn 56:c9:ce:90:0d:e8:24:06

zone name AFA-VDI-26-fc1 vsan 4  
member pwwn 20:00:00:25:b5:00:00:02  
member pwwn 56:c9:ce:90:0d:e8:24:0a  
member pwwn 56:c9:ce:90:0d:e8:24:0e  
member pwwn 56:c9:ce:90:0d:e8:24:10  
member pwwn 56:c9:ce:90:0d:e8:24:0c  
member pwwn 56:c9:ce:90:0d:e8:24:06  
member pwwn 56:c9:ce:90:0d:e8:24:02

---

```
zone name AFA-VDI-27-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:51
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
```

```
zone name AFA-VDI-28-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:31
  member pwwn 56:c9:ce:90:0d:e8:24:0a
  member pwwn 56:c9:ce:90:0d:e8:24:0e
  member pwwn 56:c9:ce:90:0d:e8:24:10
  member pwwn 56:c9:ce:90:0d:e8:24:0c
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
```

```
zone name M6-a-fc1 vsan 4
  member pwwn 20:00:00:25:b5:00:00:10
  member pwwn 56:c9:ce:90:0d:e8:24:02
  member pwwn 56:c9:ce:90:0d:e8:24:06
```

```
zoneset name SP-Infra-B vsan 4
  member SP-VDI-01-fc1
  member SP-VDI-02-fc1
  member SP-VDI-03-fc1
  member SP-VDI-04-fc1
  member SP-VDI-05-fc1
  member SP-VDI-06-fc1
  member SP-VDI-07-fc1
  member SP-VDI-08-fc1
  member SP-VDI-09-fc1
  member SP-VDI-10-fc1
  member SP-VDI-11-fc1
  member SP-VDI-12-fc1
  member SP-VDI-13-fc1
  member SP-VDI-14-fc1
  member SP-Infra1-fc1
```

```
member SP-Infra2-fc1
member AFA-VDI-15-fc1
member AFA-VDI-16-fc1
member AFA-VDI-17-fc1
member AFA-VDI-18-fc1
member AFA-VDI-19-fc1
member AFA-VDI-20-fc1
member AFA-VDI-21-fc1
member AFA-VDI-22-fc1
member AFA-VDI-23-fc1
member AFA-VDI-24-fc1
member AFA-VDI-25-fc1
member AFA-VDI-26-fc1
member AFA-VDI-27-fc1
member AFA-VDI-28-fc1
member M6-a-fc1
```

```
!Active Zone Database Section for vsan 401
```

```
zone name AFF-A400-VDI-01-HBA2 vsan 401
```

```
member pwnn 20:00:00:25:d5:06:00:3f
!           [VDI-1-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name AFF-A400-VDI-02-HBA2 vsan 401
```

```
member pwnn 20:00:00:25:d5:06:00:0f
!           [VDI-2-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name AFF-A400-VDI01-HBA2 vsan 401
```

```
member pwnn 20:00:00:25:d5:06:00:3f
!           [VDI-1-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
```

```
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name AFF-A400-VDI02-HBA2 vsan 401
member pwnn 20:00:00:25:d5:06:00:0f
!           [VDI-2-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zoneset name AFF-A400_VDI vsan 401
member AFF-A400-VDI-01-HBA2
member AFF-A400-VDI-02-HBA2
member AFF-A400-VDI01-HBA2
member AFF-A400-VDI02-HBA2

zoneset activate name AFF-A400_VDI vsan 401
do clear zone database vsan 401
!Full Zone Database Section for vsan 401
zone name Infra01_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:09
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33

zone name Infra02_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:0b
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33

zone name srv01_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:13
!           [srv01_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!           [A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31
```

---

```
zone name srv02_HBA2__A400_1 vsan 401
  member pwwn 20:00:00:25:b5:03:9a:15
!
  [srv02_HBA2]
  member pwwn 50:01:73:80:59:16:01:13
  member pwwn 50:01:73:80:59:16:01:23
  member pwwn 50:01:73:80:59:16:01:33
```

```
zone name srv03_HBA2__A400_1 vsan 401
  member pwwn 20:00:00:25:b5:03:9a:0f
!
  [srv03_HBA2]
  member pwwn 50:01:73:80:59:16:01:11
  member pwwn 50:01:73:80:59:16:01:21
!
  [A400_N2P2]
  member pwwn 50:01:73:80:59:16:01:31
```

```
zone name srv04_HBA2__A400_1 vsan 401
  member pwwn 20:00:00:25:b5:03:9a:01
!
  [srv04_HBA2]
  member pwwn 50:01:73:80:59:16:01:13
  member pwwn 50:01:73:80:59:16:01:23
  member pwwn 50:01:73:80:59:16:01:33
```

```
zone name srv05_HBA2__A400_1 vsan 401
  member pwwn 20:00:00:25:b5:03:9a:03
!
  [srv05_HBA2]
  member pwwn 50:01:73:80:59:16:01:11
  member pwwn 50:01:73:80:59:16:01:21
!
  [A400_N2P2]
  member pwwn 50:01:73:80:59:16:01:31
```

```
zone name srv06_HBA2__A400_1 vsan 401
  member pwwn 20:00:00:25:b5:03:9a:0d
!
  [srv06_HBA2]
  member pwwn 50:01:73:80:59:16:01:13
  member pwwn 50:01:73:80:59:16:01:23
  member pwwn 50:01:73:80:59:16:01:33
```

```
zone name srv09_HBA2__A400_1 vsan 401
```

```
member pwnn 20:00:00:25:b5:03:9a:17
!
[srv09_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv10_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:19
!
[srv10_HBA2]
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv11_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:1b
!
[srv11_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv12_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:1d
!
[srv12_HBA2]
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv13_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:1f
!
[srv13_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv14_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:21
```

---

```
!           [srv14_HBA2]
  member pwnn 50:01:73:80:59:16:01:13
  member pwnn 50:01:73:80:59:16:01:23
  member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv17_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:25
```

```
!           [srv17_HBA2]
  member pwnn 50:01:73:80:59:16:01:11
  member pwnn 50:01:73:80:59:16:01:21
```

```
!           [A400_N2P2]
  member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv18_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:27
```

```
!           [srv18_HBA2]
  member pwnn 50:01:73:80:59:16:01:13
  member pwnn 50:01:73:80:59:16:01:23
  member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv19_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:31
```

```
!           [srv19_HBA2]
  member pwnn 50:01:73:80:59:16:01:11
  member pwnn 50:01:73:80:59:16:01:21
```

```
!           [A400_N2P2]
  member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv20_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:29
```

```
!           [srv20_HBA2]
  member pwnn 50:01:73:80:59:16:01:13
  member pwnn 50:01:73:80:59:16:01:23
  member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv21_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:2b
```

```
!           [srv21_HBA2]
  member pwnn 50:01:73:80:59:16:01:11
```



```
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv22_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:2d
!
[srv22_HBA2]
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv24_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:33
!
[srv24_HBA2]
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv25_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:35
!
[srv25_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31
```

```
zone name srv26_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:37
!
[srv26_HBA2]
member pwnn 50:01:73:80:59:16:01:13
member pwnn 50:01:73:80:59:16:01:23
member pwnn 50:01:73:80:59:16:01:33
```

```
zone name srv27_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:39
!
[srv27_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
```

```
member pwnn 50:01:73:80:59:16:01:31

zone name srv28_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:3b
!      [srv28_HBA2]
  member pwnn 50:01:73:80:59:16:01:13
  member pwnn 50:01:73:80:59:16:01:23
  member pwnn 50:01:73:80:59:16:01:33

zone name srv29_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:3d
!      [srv29_HBA2]
  member pwnn 50:01:73:80:59:16:01:11
  member pwnn 50:01:73:80:59:16:01:21
!      [A400_N2P2]
  member pwnn 50:01:73:80:59:16:01:31

zone name srv30_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:3f
  member pwnn 50:01:73:80:59:16:01:13
  member pwnn 50:01:73:80:59:16:01:23
  member pwnn 50:01:73:80:59:16:01:33

zone name srv32_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:43
  member pwnn 50:01:73:80:59:16:01:13
  member pwnn 50:01:73:80:59:16:01:23
  member pwnn 50:01:73:80:59:16:01:33

zone name srv31_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:41
  member pwnn 50:01:73:80:59:16:01:11
  member pwnn 50:01:73:80:59:16:01:21
!      [A400_N2P2]
  member pwnn 50:01:73:80:59:16:01:31

zone name srv23_HBA2__A400_1 vsan 401
  member pwnn 20:00:00:25:b5:03:9a:2f
!      [srv23_HBA2]
```

```
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31

zone name srv15_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:23
!
[srv15_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31

zone name srv07_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:11
!
[srv07_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31

zone name x210c-SP_HBA2__A400_1 vsan 401
member pwnn 20:00:00:25:b5:03:9a:05
!
[x210c-SP_HBA2]
member pwnn 50:01:73:80:59:16:01:11
member pwnn 50:01:73:80:59:16:01:21
!
[A400_N2P2]
member pwnn 50:01:73:80:59:16:01:31

zone name AFFA400_VDI vsan 401
member pwnn 20:01:00:a0:98:af:bd:e8
member pwnn 20:02:00:a0:98:af:bd:e8
!
[A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!
[A400-02-0h]

zone name Infra01_HBA2_AFF-A400 vsan 401
member pwnn 20:00:00:25:b5:3a:00:4f
member pwnn 20:02:00:a0:98:af:bd:e8
```

```
! [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]

zone name Infra02_HBA2_AFF-A400 vsan 401
  member pwnn 20:00:00:25:b5:3a:00:2f
  member pwnn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]

zone name AFF-A400-VDI-INFRA01-HBA2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:4f
! [Infra01-8-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]

zone name AFF-A400-VDI-INFRA02-HBA2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:2f
! [Infra02-16-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]

zone name AFF-A400-VDI-01-HBA2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3f
! [VDI-1-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]

zone name AFF-A400-VDI-02-HBA2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:0f
! [VDI-2-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
```

```
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name AFF-A400-VDI01-HBA2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3f
!           [VDI-1-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name AFF-A400-VDI02-HBA2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:0f
!           [VDI-2-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zoneset name AFF-A400_VDI vsan 401
  member AFF-A400-VDI-01-HBA2
  member AFF-A400-VDI-02-HBA2
  member AFF-A400-VDI01-HBA2
  member AFF-A400-VDI02-HBA2

!Active Zone Database Section for vsan 401
zone name A400_VDI-1-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3f
!           [VDI-1-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-2-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:0f
!           [VDI-2-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
```

---

```
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
```

```
!           [A400-02-0h]
```

```
zone name A400_VDI-3-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:1f
```

```
!           [VDI-3-hba2]
```

```
  member pwnn 20:02:00:a0:98:af:bd:e8
```

```
!           [A400-01-0h]
```

```
  member pwnn 20:04:00:a0:98:af:bd:e8
```

```
!           [A400-02-0h]
```

```
zone name A400_VDI-4-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:4e
```

```
!           [VDI-4-hba2]
```

```
  member pwnn 20:02:00:a0:98:af:bd:e8
```

```
!           [A400-01-0h]
```

```
  member pwnn 20:04:00:a0:98:af:bd:e8
```

```
!           [A400-02-0h]
```

```
zone name A400_VDI-5-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:2e
```

```
!           [VDI-5-hba2]
```

```
  member pwnn 20:02:00:a0:98:af:bd:e8
```

```
!           [A400-01-0h]
```

```
  member pwnn 20:04:00:a0:98:af:bd:e8
```

```
!           [A400-02-0h]
```

```
zone name A400_VDI-6-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3e
```

```
!           [VDI-6-hba2]
```

```
  member pwnn 20:02:00:a0:98:af:bd:e8
```

```
!           [A400-01-0h]
```

```
  member pwnn 20:04:00:a0:98:af:bd:e8
```

```
!           [A400-02-0h]
```

```
zone name A400_VDI-7-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:0e
```

```
!           [VDI-7-hba2]
```

---

```
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_Infra01-8-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:4f
!           [Infra01-8-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-9-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:4d
!           [VDI-9-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-10-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:2d
!           [VDI-10-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-11-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:3d
!           [VDI-11-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-12-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:0d
```

```
!           [VDI-12-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-13-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:1d
!           [VDI-13-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-14-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:4c
!           [VDI-14-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-15-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:2c
!           [VDI-15-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_Infra02-16-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:2f
!           [Infra02-16-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-17-hba2 vsan 401
```



```
member pwnn 20:00:00:25:d5:06:00:0c
!           [VDI-17-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-18-hba2 vsan 401
member pwnn 20:00:00:25:d5:06:00:1c
!           [VDI-18-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-19-hba2 vsan 401
member pwnn 20:00:00:25:d5:06:00:4b
!           [VDI-19-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-20-hba2 vsan 401
member pwnn 20:00:00:25:d5:06:00:2b
!           [VDI-20-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-21-hba2 vsan 401
member pwnn 20:00:00:25:d5:06:00:3b
!           [VDI-21-hba2]
member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

---

```
zone name A400_VDI-22-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:6b
!           [VDI-22-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-23-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:1b
!           [VDI-23-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-24-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:4a
!           [VDI-24-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-25-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:2a
!           [VDI-25-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-26-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:3a
!           [VDI-26-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-27-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:0a
!           [VDI-27-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-28-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:1a
!           [VDI-28-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-29-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:49
!           [VDI-29-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-30-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:39
!           [VDI-30-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-31-hba2 vsan 401
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
  member pwnn 20:00:00:25:d5:06:00:1e
```

```
!           [VDI-31-hba2]

zone name A400_VDI-32-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3c
!           [VDI-32-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zoneset name FlexPod_FabricB vsan 401
  member A400_VDI-1-hba2
  member A400_VDI-2-hba2
  member A400_VDI-3-hba2
  member A400_VDI-4-hba2
  member A400_VDI-5-hba2
  member A400_VDI-6-hba2
  member A400_VDI-7-hba2
  member A400_Infra01-8-hba2
  member A400_VDI-9-hba2
  member A400_VDI-10-hba2
  member A400_VDI-11-hba2
  member A400_VDI-12-hba2
  member A400_VDI-13-hba2
  member A400_VDI-14-hba2
  member A400_VDI-15-hba2
  member A400_Infra02-16-hba2
  member A400_VDI-17-hba2
  member A400_VDI-18-hba2
  member A400_VDI-19-hba2
  member A400_VDI-20-hba2
  member A400_VDI-21-hba2
  member A400_VDI-22-hba2
  member A400_VDI-23-hba2
  member A400_VDI-24-hba2
  member A400_VDI-25-hba2
  member A400_VDI-26-hba2
  member A400_VDI-27-hba2
  member A400_VDI-28-hba2
```

```
member A400_VDI-29-hba2
member A400_VDI-30-hba2
member A400_VDI-31-hba2
member A400_VDI-32-hba2

zoneset activate name FlexPod_FabricB vsan 401
do clear zone database vsan 401
!Full Zone Database Section for vsan 401
zone name A400_VDI-1-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:3f
!           [VDI-1-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-2-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:0f
!           [VDI-2-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-3-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:1f
!           [VDI-3-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-4-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:4e
!           [VDI-4-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-5-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:2e
!           [VDI-5-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-6-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3e
!           [VDI-6-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-7-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:0e
!           [VDI-7-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_Infra01-8-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:1e
!           [VDI-31-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-9-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:4d
!           [VDI-9-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
```

```
! [A400-02-0h]

zone name A400_VDI-10-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:2d
! [VDI-10-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]
```

```
zone name A400_VDI-11-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:3d
! [VDI-11-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]
```

```
zone name A400_VDI-12-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:0d
! [VDI-12-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]
```

```
zone name A400_VDI-13-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:1d
! [VDI-13-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
  member pwwn 20:04:00:a0:98:af:bd:e8
! [A400-02-0h]
```

```
zone name A400_VDI-14-hba2 vsan 401
  member pwwn 20:00:00:25:d5:06:00:4c
! [VDI-14-hba2]
  member pwwn 20:02:00:a0:98:af:bd:e8
! [A400-01-0h]
```

---

```
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-15-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:2c
!           [VDI-15-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_Infra02-16-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:2f
!           [Infra02-16-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-17-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:0c
!           [VDI-17-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-18-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:1c
!           [VDI-18-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-19-hba2 vsan 401
    member pwnn 20:00:00:25:d5:06:00:4b
!           [VDI-19-hba2]
    member pwnn 20:02:00:a0:98:af:bd:e8
```



```
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-20-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:2b
!           [VDI-20-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-21-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3b
!           [VDI-21-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-22-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:6b
!           [VDI-22-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-23-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:1b
!           [VDI-23-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]

zone name A400_VDI-24-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:4a
!           [VDI-24-hba2]
```

---

```
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-25-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:2a
!           [VDI-25-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-26-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:3a
!           [VDI-26-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-27-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:0a
!           [VDI-27-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-28-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:1a
!           [VDI-28-hba2]
    member pwwn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
    member pwwn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-29-hba2 vsan 401
    member pwwn 20:00:00:25:d5:06:00:49
```

```
!           [VDI-29-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-30-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:39
!           [VDI-30-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zone name A400_VDI-31-hba2 vsan 401
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
  member pwnn 20:00:00:25:d5:06:00:1e
!           [VDI-31-hba2]
```

```
zone name A400_VDI-32-hba2 vsan 401
  member pwnn 20:00:00:25:d5:06:00:3c
!           [VDI-32-hba2]
  member pwnn 20:02:00:a0:98:af:bd:e8
!           [A400-01-0h]
  member pwnn 20:04:00:a0:98:af:bd:e8
!           [A400-02-0h]
```

```
zoneset name FlexPod_FabricB vsan 401
  member A400_VDI-1-hba2
  member A400_VDI-2-hba2
  member A400_VDI-3-hba2
  member A400_VDI-4-hba2
  member A400_VDI-5-hba2
  member A400_VDI-6-hba2
  member A400_VDI-7-hba2
  member A400_Infra01-8-hba2
```

```
member A400_VDI-9-hba2
member A400_VDI-10-hba2
member A400_VDI-11-hba2
member A400_VDI-12-hba2
member A400_VDI-13-hba2
member A400_VDI-14-hba2
member A400_VDI-15-hba2
member A400_Infra02-16-hba2
member A400_VDI-17-hba2
member A400_VDI-18-hba2
member A400_VDI-19-hba2
member A400_VDI-20-hba2
member A400_VDI-21-hba2
member A400_VDI-22-hba2
member A400_VDI-23-hba2
member A400_VDI-24-hba2
member A400_VDI-25-hba2
member A400_VDI-26-hba2
member A400_VDI-27-hba2
member A400_VDI-28-hba2
member A400_VDI-29-hba2
member A400_VDI-30-hba2
member A400_VDI-31-hba2
member A400_VDI-32-hba2
```

```
interface mgmt0
  ip address 10.29.164.239 255.255.255.0
```

```
vsan database
```

```
vsan 401 interface fc1/37
vsan 401 interface fc1/38

vsan 401 interface fc1/43
vsan 401 interface fc1/44
vsan 401 interface fc1/45
vsan 401 interface fc1/46
```

```
switchname MDS-B
no terminal log-all
line console
    terminal width 80
line vty
boot kickstart bootflash:/m9100-s5ek9-kickstart-mz.8.1.1.bin
boot system bootflash:/m9100-s5ek9-mz.8.1.1.bin
interface fc1/13
    switchport speed 8000
interface fc1/14
    switchport speed 8000
interface fc1/15
    switchport speed 8000
interface fc1/16
    switchport speed 8000
interface fc1/1
interface fc1/2
interface fc1/11
interface fc1/12
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/17
interface fc1/18
```

---

```
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
interface fc1/41
interface fc1/42
interface fc1/47
interface fc1/48
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/1
interface fc1/2
interface fc1/11
interface fc1/12
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
```

---

```
interface fc1/1
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/2
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/3
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/4
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/5
  port-license acquire
  no shutdown
```

```
interface fc1/6
  port-license acquire
  no shutdown
```

```
interface fc1/7
  port-license acquire
  no shutdown
```

```
interface fc1/8
  port-license acquire
  no shutdown
```

```
interface fc1/9
  port-license acquire
  no shutdown
```

---

```
interface fc1/10
  port-license acquire
  no shutdown

interface fc1/11
  port-license acquire

interface fc1/12
  port-license acquire

interface fc1/13
  port-license acquire
  no shutdown

interface fc1/14
  port-license acquire
  no shutdown

interface fc1/15
  port-license acquire
  no shutdown

interface fc1/16
  port-license acquire
  no shutdown

interface fc1/17
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/18
  port-license acquire
  channel-group 1 force
  no shutdown

interface fc1/19
  switchport description CS700 CTRL-A:02
```



---

```
port-license acquire
no shutdown

interface fc1/20
switchport description CS700 CTRL-A:06
port-license acquire
no shutdown

interface fc1/21
switchport description Launcher-FIB
port-license acquire
no shutdown

interface fc1/22
switchport description Launcher-FIB
port-license acquire
no shutdown

interface fc1/23
switchport description Launcher-FIB
port-license acquire
no shutdown

interface fc1/24
switchport description Launcher-FIB
port-license acquire
no shutdown

interface fc1/25
port-license acquire
no shutdown

interface fc1/26
port-license acquire
no shutdown

interface fc1/27
port-license acquire
no shutdown
```

---

```
interface fc1/28
  port-license acquire
  no shutdown
```

```
interface fc1/29
  port-license acquire
```

```
interface fc1/30
  port-license acquire
```

```
interface fc1/31
  port-license acquire
```

```
interface fc1/32
  port-license acquire
```

```
interface fc1/33
  port-license acquire
```

```
interface fc1/34
  port-license acquire
```

```
interface fc1/35
  port-license acquire
```

```
interface fc1/36
  port-license acquire
```

```
interface fc1/37
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/38
  switchport trunk mode off
  port-license acquire
  no shutdown
```

---

```
interface fc1/39
  port-license acquire
  no shutdown
```

```
interface fc1/40
  port-license acquire
  no shutdown
```

```
interface fc1/41
  port-license acquire
  no shutdown
```

```
interface fc1/42
  port-license acquire
  no shutdown
```

```
interface fc1/43
  port-license acquire
  no shutdown
```

```
interface fc1/44
  port-license acquire
  no shutdown
```

```
interface fc1/45
  port-license acquire
  no shutdown
```

```
interface fc1/46
  port-license acquire
  no shutdown
```

```
interface fc1/47
  port-license acquire
  no shutdown
```

```
interface fc1/48
  port-license acquire
  no shutdown
```

---

```
ip default-gateway 10.29.164.1
```

```
MDS-B#
```

---

## References

This section provides links to additional information for each partner's solution component of this document.

### Cisco UCS X-Series Servers

- <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/ucs-x-series-modular-system-aag.html>
- <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/solution-overview-c22-2432175.html>
- <https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-x-series-modular-system/datasheet-c78-2472574.html>

### 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://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide.html)
- [https://intersight.com/help/saas/resources/cisco\\_x\\_series\\_management\\_guide](https://intersight.com/help/saas/resources/cisco_x_series_management_guide)

### 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](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/hh831620(v=ws.11).aspx)
- [https://technet.microsoft.com/en-us/library/dn281793\(v=ws.11\).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](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/Main_Page)
- [https://www.loginvsi.com/documentation/Start\\_your\\_first\\_test](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/>

---

## About the Authors

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

Jeff Nichols is a member of the Cisco's Computing Systems Product Group team focusing on design, testing, and solutions validation, technical content creation, and performance testing/benchmarking. He has years of experience in server and desktop virtualization. Jeff is a subject matter expert on Cisco HyperFlex, Cisco Unified Computing System, Cisco Nexus Switching, and Citrix Certified Expert - Virtualization.

### **Dre Jackson, Senior Technical Marketing Engineer, NetApp**

Dre Jackson is a Principal Architect and Technical Marketing Engineer at NetApp. As an EUC and VDI specialist, Dre works with NetApp's field team and partners to set VDI policy, research new VDI solutions, and share his latest insights into VDI with customers. He also works side by side with NetApp sales reps and partners to leverage his hands-on VDI experience when helping prospects determine their technical requirements and evaluate NetApp solutions.

---

## Feedback

For comments and suggestions about this guide and related guides, join the discussion on [Cisco Community](https://cs.co/en-cvds) 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 WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. (LDW\_P)

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



---

**Americas Headquarters**

Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**

Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**

Cisco Systems International BV Amsterdam,  
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)