



# FlashStack Data Center using Cisco UCS B-Series, VMware Horizon 8 and VMware vSphere 7 for up to 2300 Seats

Deployment Guide for Virtual Desktop Infrastructure built on Cisco UCS B200 M6 Series with 3rd Generation Intel Xeon Scalable Processors, Cisco Intersight, Pure Storage FlashArray//X70 R3, VMware Horizon 8 2212, and VMware vSphere 7.0 U3d Hypervisor

---

Published: April 2023



In partnership with:



---

## About the Cisco Validated Design Program

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

---

## Executive Summary

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

This document details the design of the FlashStack Virtual Desktop Infrastructure for VMware Horizon 8 VMware vSphere 7.0 U3 Design Guide, which describes a validated Converged Infrastructure (CI) jointly developed by Cisco and Pure Storage.

The solution covers the deployment of a predesigned, best-practice data center architecture with:

- VMware Horizon and VMware vSphere.
- Cisco Unified Computing System (Cisco UCS) incorporating the Cisco B-Series modular platform.
- Cisco Nexus 9000 family of switches.
- Cisco MDS 9000 family of Fibre Channel switches.
- Pure Storage FlashArray//X R3 all flash array supporting Fibre Channel storage access.

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

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

Customers interested in understanding the FlashStack design and deployment details, including the configuration of various elements of design and associated best practices, should refer to Cisco Validated Designs for FlashStack, here: [Data Center Design Guides - FlashStack Platforms](#)



---

## Solution Overview

This chapter contains the following:

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

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, Pure Storage and VMware have partnered to deliver this Cisco Validated Design, which uses best of breed storage, server, and network components to serve as the foundation for desktop virtualization workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

### Audience

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

### Purpose of this Document

This document provides a step-by-step design, configuration, and implementation guide for the Cisco Validated Design for:

- Large-scale VMware Horizon 8 VDI.
- Pure Storage FlashArray//X array.
- Cisco UCS B200 M6 Blade Servers running VMware vSphere 7.0 U3d.
- Cisco Nexus 9000 Series Ethernet Switches.
- Cisco MDS 9100 Series Multilayer Fibre Channel Switches.

### What's New in this Release?

Highlights for this design include:

- Support for Cisco UCS 5108 blade server chassis with Cisco UCS B200 M6 compute nodes.
- Support for Pure Storage FlashArray//X70 R3 with Purity version 6.3.3.
- VMware Horizon 8 2212 (Horizon 8 version-2212).
- Support for VMware vSphere 7.0 U3d.
- Support for the Cisco UCS Manager 4.2.
- Support for VMware vCenter 7.0 U3 to set up and manage the virtual infrastructure as well as integration of the virtual environment with Cisco Intersight software.
- Support for Cisco Intersight platform to deploy, maintain, and support the FlashStack components.
- Support for Cisco Intersight Assist virtual appliance to help connect the Pure Storage FlashArray and VMware vCenter with the Cisco Intersight platform.
- Fully automated solution deployment describing the FlashStack infrastructure and VMware vSphere virtualization and VMware vSphere virtualization.

---

These factors have led to the need for a 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 Data Center
- Service Provider Data Center
- Large Commercial Data Center

## Technology Overview

This chapter contains the following:

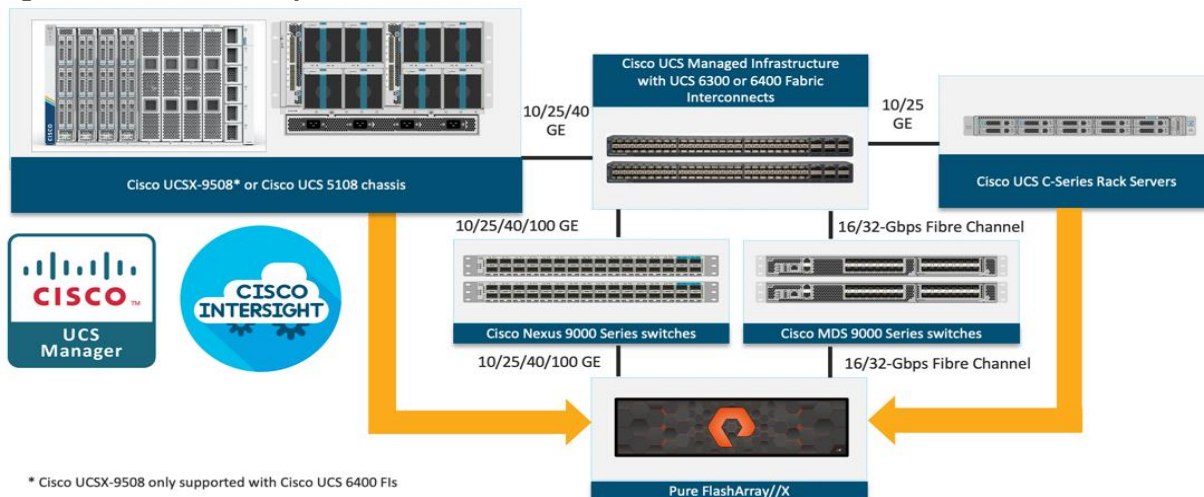
- [FlashStack](#)
- [Cisco Unified Computing System](#)
- [Cisco UCS Fabric Interconnect](#)
- [Cisco Unified Computing System B-Series](#)
- [Cisco UCS Virtual Interface Cards \(VICs\)](#)
- [Cisco Switching](#)
- [VMware Horizon](#)
- [VMware vSphere 7.0 U3](#)
- [Cisco Intersight Assist Device Connector for VMware vCenter and Pure Storage FlashArray](#)
- [Pure Storage for VDI](#)
- [Purity for FlashArray](#)
- [Pure1](#)

Cisco and Pure Storage have partnered to deliver several Cisco Validated Designs, which use best-in-class storage, server, and network components to serve as the foundation for virtualized workloads such as Virtual Desktop Infrastructure (VDI), enabling efficient architectural designs that you can deploy quickly and confidently.

### FlashStack

The FlashStack architecture was jointly developed by Cisco and Pure Storage. All FlashStack components are integrated, allowing customers to deploy the solution quickly and economically while eliminating many of the risks associated with re-searching, designing, building, and deploying similar solutions from the foundation. One of the main benefits of FlashStack is its ability to maintain consistency at scale. Each of the component families shown in [Figure 1](#) (Cisco UCS, Cisco Nexus, Cisco MDS, and Pure Storage FlashArray systems) offers platform and resource options to scale up or scale out the infrastructure while supporting the same features and functions.

Figure 1. FlashStack components



---

## Cisco Unified Computing System

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

Cisco Unified Computing System consists of the following subsystems:

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

## Cisco UCS Differentiators

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

- **Embedded Management:** In Cisco UCS, the servers are managed by the embedded firmware in the Fabric Interconnects, eliminating the need for any external physical or virtual devices to manage the servers.
- **Unified Fabric:** In Cisco UCS, from blade server chassis or rack servers to FI, there is a single Ethernet cable used for LAN, SAN, and management traffic. This converged I/O results in reduced cables, SFPs and adapters – reducing capital and operational expenses of the overall solution.
- **Auto Discovery:** By simply inserting the blade server in the chassis or connecting the rack server to the fabric interconnect, discovery and inventory of compute resources occurs automatically without any management intervention. The combination of unified fabric and auto-discovery enables the wire-once architecture of Cisco UCS, where compute capability of Cisco UCS can be extended easily while keeping the existing external connectivity to LAN, SAN, and management networks.
- **Policy Based Resource Classification:** Once Cisco UCS Manager discovers a compute resource, it can be automatically classified to a given resource pool based on policies defined. This capability is useful in multi-tenant cloud computing. This CVD showcases the policy-based resource classification of Cisco UCS Manager.

- **Combined Rack and Blade Server Management:** Cisco UCS Manager can manage Cisco UCS B-series blade servers and Cisco UCS C-series rack servers under the same Cisco UCS domain. This feature, along with stateless computing makes compute resources truly hardware form factor agnostic.
- **Model based Management Architecture:** The Cisco UCS Manager architecture and management database is model based, and data driven. An open XML API is provided to operate on the management model. This enables easy and scalable integration of Cisco UCS Manager with other management systems.
- **Policies, Pools, Templates:** The management approach in Cisco UCS Manager is based on defining policies, pools, and templates, instead of cluttered configuration, which enables a simple, loosely coupled, data driven approach in managing compute, network, and storage resources.
- **Loose Referential Integrity:** In Cisco UCS Manager, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each other. This provides great flexibility where different experts from different domains, such as network, storage, security, server, and virtualization work together to accomplish a complex task.
- **Policy Resolution:** In Cisco UCS Manager, a tree structure of organizational unit hierarchy can be created that mimics the re-al-life tenants and/or organization relationships. Various policies, pools and templates can be defined at different levels of organization hierarchy. A policy referring to another policy by name is resolved in the organizational hierarchy with closest policy match. If no policy with specific name is found in the hierarchy of the root organization, then the special policy named “default” is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibility to owners of different organizations.
- **Service Profiles and Stateless Computing:** A service profile is a logical representation of a server, carrying its various identities and policies. This logical server can be assigned to any physical compute resource as far as it meets the resource requirements. Stateless computing enables procurement of a server within minutes, which used to take days in legacy server management systems.
- **Built-in Multi-Tenancy Support:** The combination of policies, pools and templates, loose referential integrity, policy resolution in the organizational hierarchy and a service profiles-based approach to compute resources makes Cisco UCS Manager inherently friendly to multi-tenant environments typically observed in private and public clouds.
- **Extended Memory:** The enterprise-class Cisco UCS Blade server extends the capabilities of the Cisco Unified Computing System portfolio in a half-width blade form factor. It harnesses the power of the latest Intel Xeon Scalable Series processor family CPUs and Intel Optane DC Persistent Memory (DCPMM) with up to 18TB of RAM (using 256GB DDR4 DIMMs and 512GB DCPMM).
- **Simplified QoS:** Even though Fibre Channel and Ethernet are converged in the Cisco UCS fabric, built-in support for QoS and lossless Ethernet makes it seamless. Network Quality of Service (QoS) is simplified in Cisco UCS Manager by representing all system classes in one GUI panel.

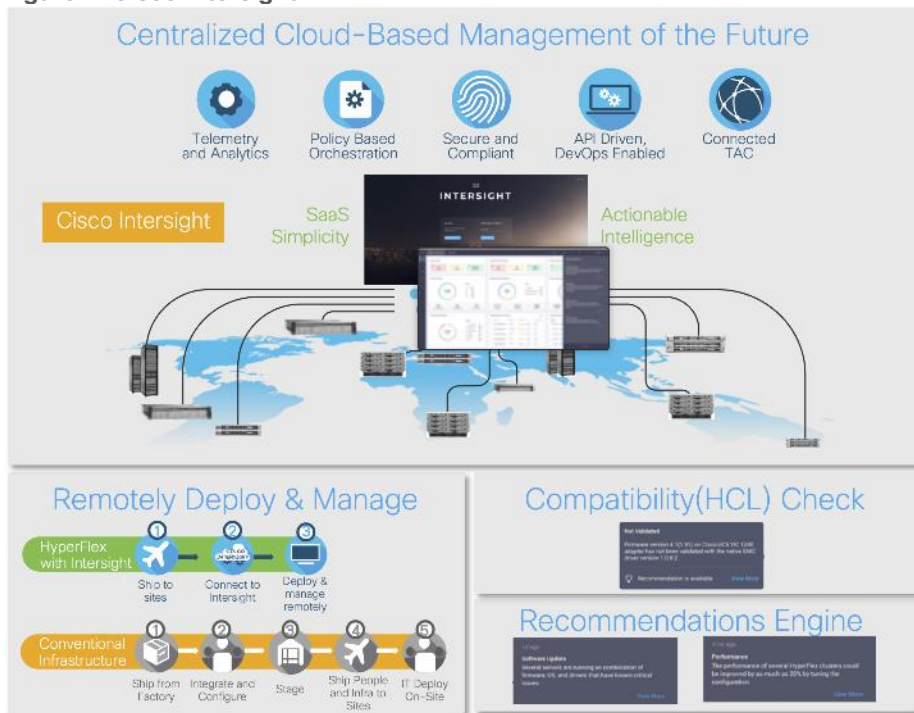
## Cisco Intersight

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

Cisco Intersight software delivers a new level of cloud-powered intelligence that supports lifecycle management with continuous improvement. It is tightly integrated with the Cisco Technical Assistance Center (TAC). Expertise and information flow seamlessly between Cisco Intersight and IT teams, providing global management

of Cisco infrastructure, anywhere. Remediation and problem resolution are supported with automated upload of error logs for rapid root-cause analysis.

**Figure 2. Cisco Intersight**



- Automate your infrastructure.
 

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

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

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

Simplify the user experience by managing your infrastructure regardless of where it is installed.
- Actionable intelligence.



- Use best practices to enable faster, proactive IT operations.
- Gain actionable insight for ongoing improvement and problem avoidance.
- Manage anywhere.
- Deploy in the data center and at the edge with massive scale.
- Get visibility into the health and inventory detail for your Intersight Managed environment on-the-go with the Cisco Inter-sight Mobile App.

For more information about Cisco Intersight and the different deployment options, go to: [Cisco Intersight - Manage your systems anywhere.](#)

## Cisco UCS Fabric Interconnect

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

For networking performance, the Cisco UCS 6454 Series uses a cut-through architecture, supporting deterministic, low latency, line rate 10/25/40/100 Gigabit Ethernet ports, 3.82 Tbps of switching capacity, and 320 Gbps bandwidth per Cisco 5108 blade chassis when connected through the IOM 2208/2408 model. The product family supports Cisco low-latency, lossless 10/25/40/100 Gigabit Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over the Ethernet fabric from the servers to the uplinks. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

### Cisco UCS 6454 Fabric Interconnect

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

Figure 3. Cisco UCS 6454 Fabric Interconnect



## Cisco UCS B200 M6 Blade Server

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

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

Figure 4. Cisco UCS B200M6



## Cisco UCS VIC 1440 mLOM Interface Card

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

Figure 5. Cisco UCS VIC 1440 mLOM Card





---

## Cisco Switching

### Cisco Nexus 93180YC-FX Switches

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

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

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

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

- Hot swappable 3+1 redundant fan trays.

**Figure 6. Cisco Nexus 93180YC-EX Switch**



### Cisco MDS 9132T 32-Gb Fiber Channel Switch

The next-generation Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switch ([Figure 7](#)) provides high-speed Fibre Channel connectivity from the server rack to the SAN core. It empowers small, midsize, and large enterprises that are rapidly deploying cloud-scale applications using extremely dense virtualized servers, providing the dual benefits of greater bandwidth and consolidation.

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

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

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

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

**Figure 7. Cisco MDS 9132T 32-Gb Fibre Channel Switch**



**Figure 8. Cisco MDS 9132T 32-Gb 16-Port Fibre Channel Port Expansion Module**



- Features

- High performance: Cisco MDS 9132T architecture, with chip-integrated nonblocking arbitration, provides consistent 32-Gb low-latency performance across all traffic conditions for every Fibre Channel port on the switch.
- Capital Expenditure (CapEx) savings: The 32-Gb ports allow users to deploy them on existing 16- or 8-Gb transceivers, reducing initial CapEx with an option to upgrade to 32-Gb transceivers and adapters in the future.
- High availability: Cisco MDS 9132T switches continue to provide the same outstanding availability and reliability as the previous-generation Cisco MDS 9000 Family switches by providing optional redundancy on all major components such as the power supply and fan. Dual power supplies also facilitate redundant power grids.
- Pay-as-you-grow: The Cisco MDS 9132T Fibre Channel switch provides an option to deploy as few as eight 32-Gb Fibre Channel ports in the entry-level variant, which can grow by 8 ports to 16 ports, and thereafter with a port expansion module with sixteen 32-Gb ports, to up to 32 ports. This approach results in lower initial investment and power consumption for entry-level configurations of up to 16 ports compared to a fully loaded switch. Upgrading through an expansion module also reduces the overhead of managing multiple instances of port activation licenses on the switch. This unique combination of port upgrade options allow four possible configurations of 8 ports, 16 ports, 24 ports and 32 ports.
- Next-generation Application-Specific Integrated Circuit (ASIC): The Cisco MDS 9132T Fibre Channel switch is powered by the same high-performance 32-Gb Cisco ASIC with an integrated network processor that powers the Cisco MDS 9700 48-Port 32-Gb Fibre Channel Switching Module. Among all the advanced features that this ASIC enables, one of the most notable is inspection of Fibre Channel and Small Computer System Interface (SCSI) headers at wire speed on every flow in the smallest form-factor Fibre Channel switch without the need for any external taps or appliances. The recorded flows can be analyzed on the switch and also exported using a dedicated 10/100/1000BASE-T port for telemetry and analytics purposes.
- Intelligent network services: Slow-drain detection and isolation, VSAN technology, Access Control Lists (ACLs) for hardware-based intelligent frame processing, smartzoning and fabric wide Quality of Service (QoS) enable migration from SAN islands to enterprise-wide storage networks. Traffic encryption is optionally available to meet stringent security requirements.
- Sophisticated diagnostics: The Cisco MDS 9132T provides intelligent diagnostics tools such as Inter-Switch Link (ISL) diagnostics, read diagnostic parameters, protocol decoding, network analysis tools, and integrated Cisco Call Home capability for greater reliability, faster problem resolution, and reduced service costs.
- Virtual machine awareness: The Cisco MDS 9132T provides visibility into all virtual machines logged into the fabric. This feature is available through HBAs capable of priority tagging the Virtual Machine Identifier (VMID) on every FC frame. Virtual machine awareness can be extended to intelligent fabric services such as analytics[1] to visualize performance of every flow originating from each virtual machine in the fabric.
- Programmable fabric: The Cisco MDS 9132T provides powerful Representational State Transfer (REST) and Cisco NX-API capabilities to enable flexible and rapid programming of utilities for the SAN as well as polling point-in-time telemetry data from any external tool.
- Single-pane management: The Cisco MDS 9132T can be provisioned, managed, monitored, and troubleshoot using Cisco Data Center Network Manager (DCNM), which currently manages the entire suite of Cisco data center products.
- Self-contained advanced anticounterfeiting technology: The Cisco MDS 9132T uses on-board hardware that protects the entire system from malicious attacks by securing access to critical components such as the bootloader, system image loader and Joint Test Action Group (JTAG) interface.

---

## VMware Horizon

VMware Horizon is a modern platform for running and delivering virtual desktops and apps across the hybrid cloud. For administrators, this means simple, automated, and secure desktop and app management. For users, it provides a consistent experience across devices and locations.

For more information, go to: [VMware Horizon](#).

## VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions and Windows 10 Desktops

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

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

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

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

For more information, go to:

<https://docs.vmware.com/en/VMware-Horizon/8-2212/rn/vmware-horizon-8-2212-release-notes/index.html>

[https://customerconnect.vmware.com/en/downloads/info/slug/desktop\\_end\\_user\\_computing/vmware\\_horizon/2212](https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_horizon/2212)

## VMware Horizon 8 2212

VMware Horizon 8 version 2212 includes the following new features and enhancements. This information is grouped by installable component.

- Horizon Agent for Linux.
  - This release adds support for the following Linux distributions:
    - Ubuntu 22.04/22.04.
    - Red Hat Enterprise Linux (RHEL) Workstation 8.8/9.0/9.1.
    - Red Hat Enterprise Linux (RHEL) Server 8.8/9.0/9.1.
  - Beginning with this release, the following Linux distributions are no longer supported:
    - RHEL Server 8.7/9.0/9.1.
  - Horizon Agent for Linux now supports Real-Time Audio-Video redirection, which includes both audio-in and webcam redirection of locally connected devices from the client system to the remote session.
  - VMware Integrated Printing now supports printer redirection from Linux remote desktops to client devices running Horizon Client for Chrome or HTML Access.
  - Session Collaboration is now supported on the MATE desktop environment.

- A vGPU desktop can support a maximum resolution of 3840x2160 on one, two, three, or four monitors configured in any arrangement.
- A non-vGPU desktop can support a maximum resolution of 3840x2160 on a single monitor only.
- Agent and Agent RDS levels are now supported for Horizon Agent for Linux.
- Virtual Desktops.
  - Option to create multiple custom compute profiles (CPU, RAM, Cores per Socket) for a single golden image snapshot during desktop pool creation.
  - VMware Blast now detects the presence of a vGPU system and applies higher quality default settings.
  - VMware vSphere Distributed Resource Scheduler (DRS) in vSphere 7.0 U3f and later can now be configured to automatically migrate vGPU desktops when entering ESXi host maintenance mode. For more information, see <https://kb.vmware.com/s/article/87277>.
  - Forensic quarantine feature that archives the virtual disks of selected dedicated or floating Instant Clone desktops for forensic purposes.
  - The VMware Blast CPU controller feature is now enabled by default in scale environments.
  - Removed pop-up for suggesting best practices during creation of an instant clone. The information now appears on the first tab/screen of the creation wizard.
  - Help Desk administrator roles are now applicable to all access groups, not just to the root access group as with previous releases.
  - Administrators can encrypt a session recording file into a .bin format so that it cannot be played from the file system.
  - If using an older Web browser, a message appears when launching the Horizon Console indicating that using a modern browser will provide a better user experience.
  - Added Support for HW encoding on Intel GPU for Windows.
    - Supports Intel 11th Generation Integrated Graphics and above (Tigerlake+) with a minimum required driver version of: 30.0.101.1660  
(<https://www.intel.com/content/www/us/en/download/19344/727284/intel-graphics-windows-dch-drivers.html>).
  - VVC-based USB-R is enabled by default for non-desktop (Chrome/HTML Access/Android) Blast clients.
  - Physical PC (as Unmanaged Pool) now supports Windows 10 Education and Pro (20H2 and later) and Windows 11 Education and Pro (21H2) with the VMware Blast protocol.
  - Storage Drive Redirection (SDR) is now available as an alternative option to USB or CDR redirection for better I/O performance.
- Horizon Connection Server.
  - Horizon Connection Server now enables you to configure a customized timeout warning and set the timer for the warning to appear before a user is forcibly disconnected from a remote desktop or published application session. This warning is supported with Horizon Client for Windows 2212 and Horizon Client for Mac 2212 or later.
  - Windows Hello for Business with certificate authentication is now supported when you Log In as Current User on the Horizon Client for Windows.
  - Added limited support for Hybrid Azure AD.
- Horizon Agent.
  - The Horizon Agent Installer now includes a pre-check to confirm that .NET 4.6.2 is installed if Horizon Performance Tracker is selected.
- Horizon Client.

- For information about new features in a Horizon client, including HTML Access, review the release notes for that Horizon client.
- General.
  - The View Agent Direct-Connection Plug-In product name was changed to Horizon Agent Direct-Connection Plug-In in the documentation set.
  - Customers are automatically enrolled in the VMware Customer Experience Improvement Program (CEIP) during installation.

## VMware vSphere 7.0 U3

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 U3 has several improvements and simplifications including, but not limited to:

- vSphere Memory Monitoring and Remediation, and support for snapshots of PMem VMs: vSphere Memory Monitoring and Remediation collects data and provides visibility of performance statistics to help you determine if your application workload is regressed due to Memory Mode. vSphere 7.0 Update 3 also adds support for snapshots of PMem VMs.
- Improved interoperability between vCenter Server and ESXi versions: Starting with vSphere 7.0 Update 3, vCenter Server can manage ESXi hosts from the previous two major releases and any ESXi host from version 7.0 and 7.0 updates. For example, vCenter Server 7.0 Update 3 can manage ESXi hosts of versions 6.5, 6.7 and 7.0, all 7.0 update releases, including later than Update 3, and a mixture of hosts between major and update versions.
- New VMNIC tag for NVMe-over-RDMA (NVMe/RoCEv2) storage traffic: ESXi 7.0 Update 3 adds a new VMNIC tag for NVMe-over-RDMA (NVMe/RoCEv2) storage traffic. This VMkernel port setting enables NVMe-over-RDMA traffic to be routed over the tagged interface. You can also use the ESXCLI command `esxcli network ip interface tag add -i <interface name> -t NVMeRDMA` to enable the NVMeRDMA VMNIC tag.
- NVMe over TCP support: vSphere 7.0 Update 3 extends the NVMe-oF suite with the NVMe over TCP storage protocol to enable high performance and parallelism of NVMe devices over a wide deployment of TCP/IP networks.
- Micro-second level time accuracy for workloads: ESXi 7.0 Update 3 adds the hardware timestamp Precision Time Protocol (PTP) to enable micro-second level time accuracy. For more information, see [Use PTP for Time and Date Synchronization of a Host](#).

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.



## Red Hat Ansible

Ansible is simple and powerful, allowing users to easily manage various physical devices within FlashStack including the provisioning of Cisco UCS servers, Cisco Nexus switches, Pure Storage FlashArray storage and VMware vSphere. Using Ansible's Playbook-based automation is easy and integrates into your current provisioning infrastructure.

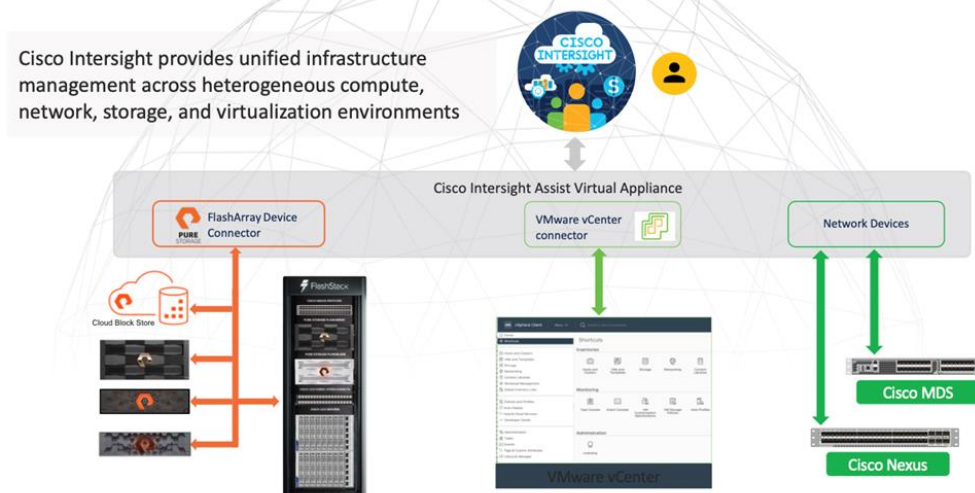
## Cisco Intersight Assist Device Connector for VMware vCenter and Pure Storage FlashArray

Cisco Intersight integrates with VMware vCenter and Pure Storage FlashArray 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 all Pure Storage FlashArray models. The newest version 1.1 of Pure Storage integration to Cisco Intersight introduces support for REST API 2.x for FlashArray products (running Purity//FA 6.0.3 or later), along with User Agent support (for telemetry). Intersight Cloud Orchestrator now has new storage tasks for adding/removing a Pure Storage snapshot and copy a Pure Storage volume from snapshot.

Figure 9. Cisco Intersight and vCenter and Pure Storage Integration

### Storage, VMware and Network Integration



The device connector provides a safe 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 FlashArray storage environments. The integration architecture enables FlashStack customers to use new management capabilities with no compromise in their existing VMware or Pure Storage FlashArray 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 the Pure Storage dashboard for comprehensive analysis, diagnostics, and reporting of virtual and storage environments. The next section addresses the functions that this integration provides.

## Pure Storage for VDI

Pure Storage helps organizations—of all sizes and across multiple industries—overcome the most common reasons for disappointing results from a VDI. All-flash storage delivers:

- Always-on, always fast and always secure VDI, ensuring a consistently superior end-user experience.
- Efficiency with up to 2x better data-reduction rates, lowering capital and operating costs.
- Effortless storage management, sharply reducing the demands on IT staff.
- Evergreen growth and scalability, incorporating non-disruptive upgrades and clearly defined costs known well in advance.

Whether you're planning a VDI rollout or have already implemented VDI that's delivering sub-par results, this white paper will provide valuable guidance—citing actual end-user deployments—that clearly illustrates how deploying flash storage can optimize your end user productivity and experience with VDI.

## Purity for FlashArray

The essential element of every FlashArray is the Purity Operating Environment software. Purity implements advanced data reduction, storage management, and flash management features, enabling organizations to enjoy Tier 1 data services for all workloads, proven 99.9999% availability over multiple years (inclusive of maintenance and generational upgrades), completely non-disruptive operations, 2X better data reduction versus alternative all-flash solutions, and – with FlashArray//X – the power and efficiency of DirectFlash.



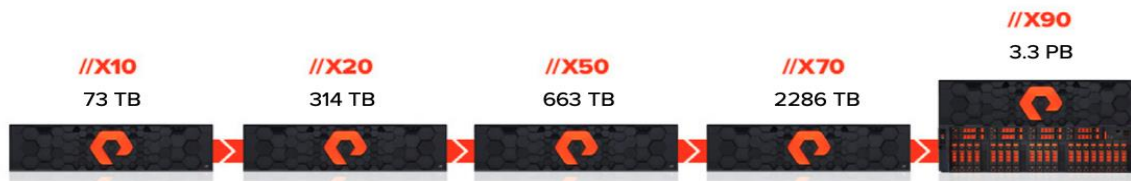
Moreover, Purity includes enterprise-grade data security, modern data protection options, and complete business continuity and global disaster recovery through ActiveCluster multi-site stretch cluster and ActiveDR\* for continuous replication with near zero RPO. All these features are included with every array.

## FlashArray File Services

Pure Storage acquired Compuverde last year, and they've been busy at work integrating this technology into the Purity//FA operating environment. They emphasize the “integrating,” because they didn't just take the existing product, drop it onto a FlashArray system, and run it on top of Purity. Instead, they incorporated key parts of it into Purity to give you the advantages of native files alongside blocks.

The SMB and NFS protocols bring consolidated storage to the Purity//FA operating system, complementing its block capabilities, while the file system offers features like directory snapshots and directory-level performance and space monitoring. For the purposes of this reference architecture, we will be focusing on using File Services for User Profile management.

Figure 10. FlashArray//X Specifications





	CAPACITY	PHYSICAL
<b>//X10</b>	Up to 73TB / 66.2TiB effective capacity** Up to 22TB / 19.2TiB raw capacity	3U; 640 – 845 Watts (nominal – peak) 95 lbs (43.1 kg) fully loaded; 5.12" x 18.94" x 29.72"
<b>//X20</b>	Up to 314TB / 285.4TiB effective capacity** Up to 94TB / 88TiB raw capacity†	3U; 741 – 973 Watts (nominal – peak) 95 lbs (43.1 kg) fully loaded; 5.12" x 18.94" x 29.72"
<b>//X50</b>	Up to 663TB / 602.9TiB effective capacity** Up to 185TB / 171TiB raw capacity†	3U; 868 – 1114 Watts (nominal – peak) 95 lbs (43.1 kg) fully loaded; 5.12" x 18.94" x 29.72"
<b>//X70</b>	Up to 2286TB / 2078.9TiB effective capacity** Up to 622TB / 544.2TiB raw capacity†	3U; 1084 – 1344 Watts (nominal – peak) 97 lbs (44.0 kg) fully loaded; 5.12" x 18.94" x 29.72"
<b>//X90</b>	Up to 3.3PB / 3003.1TiB effective capacity** Up to 878TB / 768.3TiB raw capacity†	3U – 6U; 1160 – 1446 Watts (nominal – peak) 97 lbs (44 kg) fully loaded; 5.12" x 18.94" x 29.72"
<b>DirectFlash Shelf</b>	Up to 1.9PB effective capacity** Up to 512TB / 448.2TiB raw capacity	3U; 460 – 500 Watts (nominal – peak) 87.7 lbs (39.8kg) fully loaded; 5.12" x 18.94" x 29.72"

## //X Connectivity

ONBOARD PARTS (PER CONTROLLER)	HOST I/O CARDS (3 SLOTS/CONTROLLER)	
<ul style="list-style-type: none"> <li>• 2 x 1/10/25Gb Ethernet</li> <li>• 2 x 1/10/25Gb Ethernet Replication</li> <li>• 2 x 1Gb Management Ports</li> </ul>	<ul style="list-style-type: none"> <li>• 2-port 10GBase-T Ethernet</li> <li>• 2-port 1/10/25Gb Ethernet</li> <li>• 2-port 40Gb Ethernet</li> </ul>	<ul style="list-style-type: none"> <li>• 2-port 25/50Gb NVMe/RoCE</li> <li>• 2-port 16/32Gb Fibre Channel (NVMe-oF Ready)</li> <li>• 4-port 16/32Gb Fibre Channel (NVMe-oF Ready)</li> </ul>

\*\* Effective capacity assumes HA, RAID, and metadata overhead, GB-to-GiB conversion, and includes the benefit of data reduction with always-on inline deduplication, compression, and pattern removal. Average data reduction is calculated at 5-to-1 and does not include thin provisioning or snapshots.

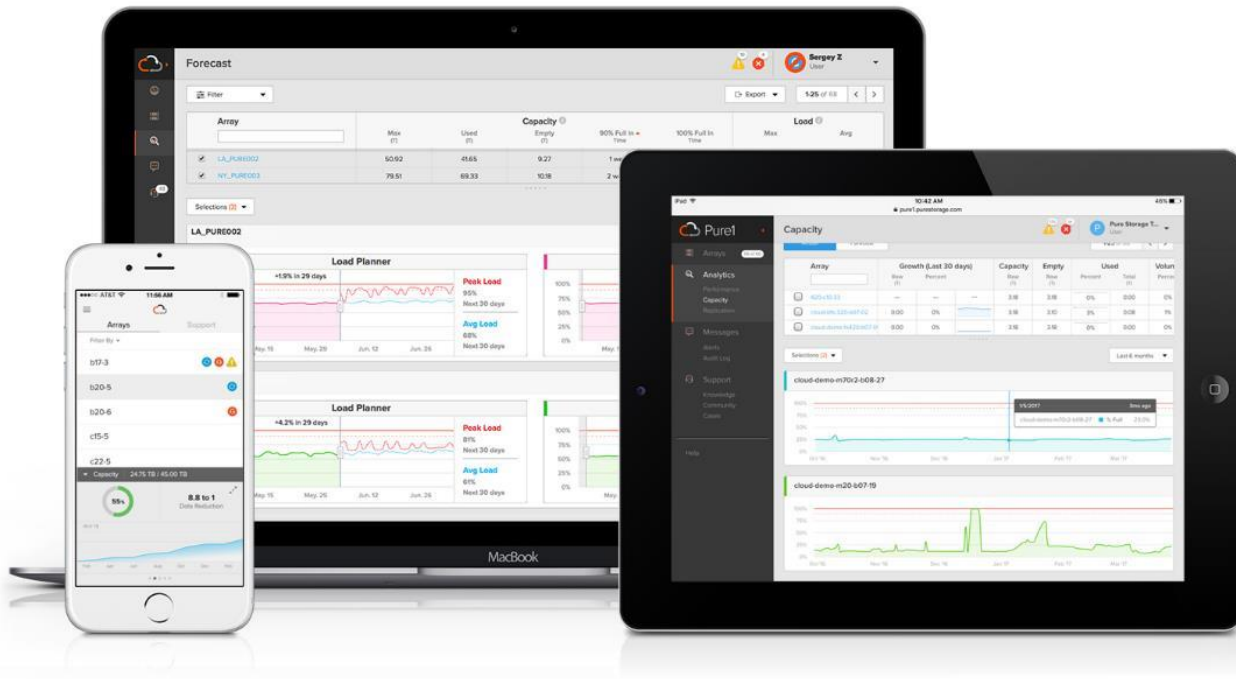
† Array accepts Pure Storage DirectFlash Shelf and/or Pure Storage SAS-based expansion shelf.

## Evergreen Storage

Customers can deploy storage once and enjoy a subscription to continuous innovation through Pure's Evergreen Storage ownership model: expand and improve performance, capacity, density, and/or features for 10 years or more – all without downtime, performance impact, or data migrations. Pure Storage has disrupted the industry's 3-5-year rip-and-replace cycle by engineering compatibility for future technologies right into its products, notably nondisruptive capability to upgrade from //M to //X with NVMe, DirectMemory, and NVMe-oF capability.

## Pure1

Pure1, our cloud-based management, analytics, and support platform, expands the self-managing, plug-n-play design of Pure Storage all-flash arrays with the machine learning predictive analytics and continuous scanning of Pure1 Meta to enable an effortless, worry-free data platform.



### Pure1 Manage

In the Cloud IT operating model, installing, and deploying management software is an oxymoron: you simply login. Pure1 Manage is SaaS-based, allowing you to manage your array from any browser or from the Pure1 Mobile App – with nothing extra to purchase, deploy, or maintain. From a single dashboard you can manage all your arrays, with full visibility on the health and performance of your storage.

### Pure1 Analyze

Pure1 Analyze delivers true performance forecasting – giving customers complete visibility into the performance and capacity needs of their arrays – now and in the future. Performance forecasting enables intelligent consolidation and unprecedented workload optimization.

### Pure1 Support

Pure Storage combines an ultra-proactive support team with the predictive intelligence of Pure1 Meta to deliver unrivaled support that's a key component in our proven FlashArray 99.9999% availability. Customers are often surprised and delighted when we fix issues they did not even know existed.

### Pure1 META

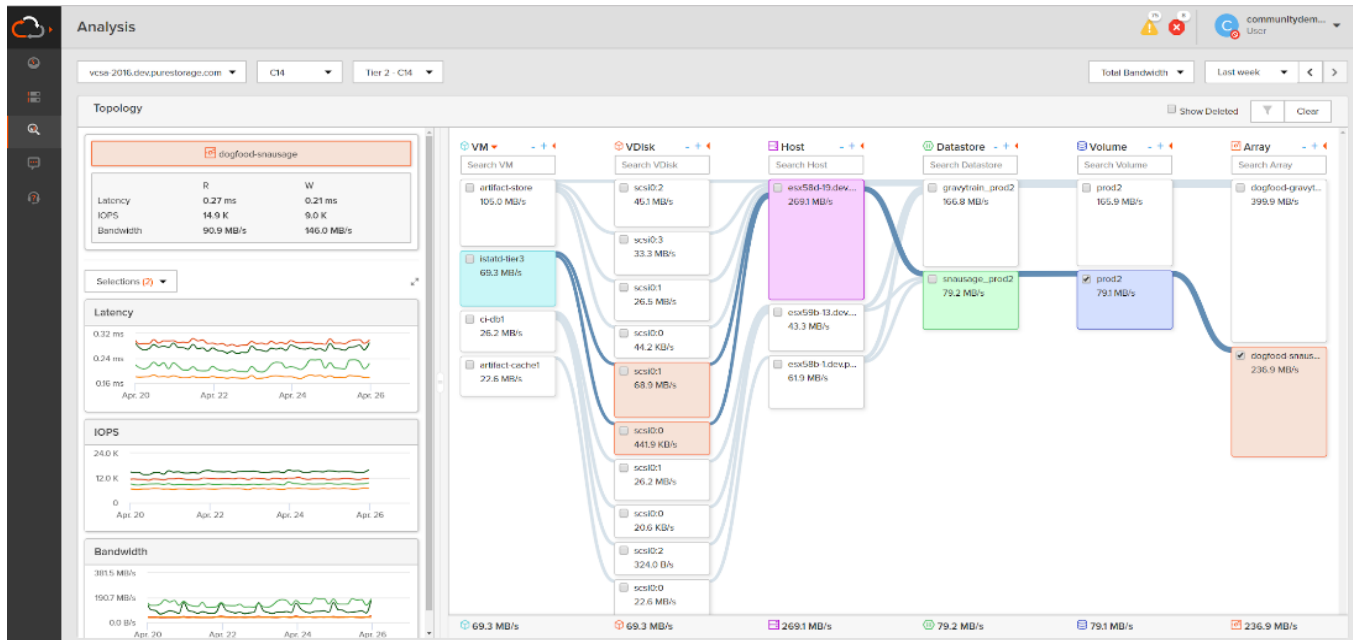
The foundation of Pure1 services, Pure1 Meta is global intelligence built from a massive collection of storage array health and performance data. By continuously scanning call-home telemetry from Pure's installed base, Pure1 Meta uses machine learning predictive analytics to help resolve potential issues and optimize workloads. The result is both a white glove customer support experience and breakthrough capabilities like accurate performance forecasting.

Meta is always expanding and refining what it knows about array performance and health, moving the Data Platform toward a future of self-driving storage.

## Pure1 VM Analytics

Pure1 helps you narrow down the troubleshooting steps in your virtualized environment. VM Analytics provides you with a visual representation of the IO path from the VM all the way through to the FlashArray. Other tools and features guide you through identifying where an issue might be occurring in order to help eliminate potential candidates for a problem.

VM Analytics doesn't only help when there's a problem. The visualization allows you to identify which volumes and arrays particular applications are running on. This brings the whole environment into a more manageable domain.



## CloudSnap

Pure portable snapshots provide simple, built-in, local and cloud protection for Pure Storage FlashArrays. Purity Snapshots enable free movement of space-efficient copies between FlashArrays, to FlashBlade, to 3rd party NFS servers, and to the cloud. Pure's portable snapshot technology encapsulates metadata along with data into the snapshot, making the snapshot portable, so it can be offloaded from a FlashArray to the cloud in a format that is recoverable to any FlashArray.

## Benefits

CloudSnap is a self-backup technology built into FlashArray. It does not require the purchase of additional backup software or hardware, nor is there a need to learn and use an additional management interface. CloudSnap is natively managed via Pure Storage FlashArray's GUI, CLI, and REST interfaces and is integrated with the Pure1 Snapshot Catalog. Since FlashArray connects to AWS via https, data is encrypted in transit and stored in an encrypted format in the S3 bucket using server-side encryption. Since CloudSnap was built from scratch for FlashArray, it is deeply integrated with the Purity Operating Environment, resulting in highly efficient operation. A few examples of the efficiency of CloudSnap:

- CloudSnap preserves data compression on the wire, and in the S3 bucket, saving network bandwidth and increasing storage space efficiency.
- CloudSnap preserves data reduction across snapshots of a volume. After offloading the initial baseline snapshot of a volume, it only sends delta changes for subsequent snaps of the same volume. The snapshot differencing engine runs within the Purity Operating Environment in FlashArray and uses a local copy of the previous snapshot to compute the delta changes. Therefore, there is no back and forth

---

network traffic between FlashArray and the cloud to compute deltas between snapshots, further reducing network congestion and data access costs in the cloud.

- CloudSnap knows which data blocks already exist on FlashArray, so during restores it only pulls back missing data blocks to rebuild the complete snapshot on FlashArray. In addition, CloudSnap uses dedupe preserving restores, so when data is restored from the offload target to FlashArray, it is deduped to save space on FlashArray.

The highly efficient operation of CloudSnap provides the following benefits:

- Less space is consumed in the S3 bucket
- Network utilization is minimized
- Backup windows are much smaller
- Data retrieval costs from the S3 bucket are lower

---

## Solution Design

This chapter contains the following:

- [Design Considerations for Desktop Virtualization](#)
- [Understanding Applications and Data](#)
- [Project Planning and Solution Sizing Sample Questions](#)
- [Hypervisor Selection](#)
- [Storage Considerations](#)
- [Desktop Virtualization Design Fundamentals](#)
- [VMware Horizon Design Fundamentals](#)

### Design Considerations for Desktop Virtualization

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 as the needs of the organization change, tops the list.

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

- Traditional PC: A traditional PC is what typically constitutes a desktop environment: physical device with a locally installed operating system.
- Remoted Desktop Server Hosted Sessions: 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 2019, 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 VMware 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 be 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.

**Note:** For the purposes of the validation represented in this document, both Single-session OS and Multi-session OS VDAs were validated.

## 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 of 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

The following key project and solution sizing questions should be considered:

- 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 Single-session OS version?
- 32-bit or 64-bit desktop OS?
- How many virtual desktops will be deployed in the pilot? In production?
- 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 Multi-session OS version?
- What is a method be used for virtual desktop deployment?
- 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 there a 3rd party graphics component?
- Is anti-virus a part of the image?
- What is the SQL server version for database?
- 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 7.0 U3d has been selected as the hypervisor for this VMware Horizon Virtual Desktops and Remote Desktop Server Hosted (RDSH) Sessions deployment.

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 web site](#).

## Storage Considerations

### Boot from SAN

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

### Pure Storage FlashArray Considerations

Make sure Each FlashArray Controller is connected to BOTH storage fabrics (A/B).

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

How big should a Volume be? With the Purity Operating Environment, we remove the complexities of aggregates, RAID groups, and so on. When managing storage, you just create a volume based on the size required, availability and performance are taken care of through RAID-HD and DirectFlash Software. As an administrator you can create 1 10TB volume or 10 1TB Volumes and their performance/availability will be the same, so instead of creating volumes for availability or performance you can think about recoverability, manageability, and administrative considerations. For example, what data do I want to present to this application or what data do I want to store together so I can replicate it to another site/system/cloud, and so on.



---

## Port Connectivity

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

16/32Gb Fiber Channel support (N-2 support) – Pure Storage offers up to 32Gb FC support on the latest FlashArray//X arrays. Always make sure the correct number of HBAs and the speed of SFPs are included in the original FlashArray BOM.

## Oversubscription

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

## Topology

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

## VMware Virtual Volumes Considerations

**Note:** VMware Horizon 8 only supports VVols with full-clone virtual machines. Virtual Volumes datastores are not supported for instant clone desktop pools.

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

Ensure that the Config vVol is either part of an existing FlashArray Protection Group, Storage Policy that includes snapshots, or manual snapshots of the Config vVol are taken. This will help with the VM recovery process if the VM is deleted.

There are some FlashArray limits on Volume Connections per Host, Volume Count, and Snapshot Count. For more information about FlashArray limits, review the following:

[https://support.purestorage.com/FlashArray/PurityFA/General\\_Troubleshooting/Pure\\_Storage\\_FlashArray\\_Limits](https://support.purestorage.com/FlashArray/PurityFA/General_Troubleshooting/Pure_Storage_FlashArray_Limits)

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

## Pure Storage FlashArray Best Practices for VMware vSphere 7.0

The following Pure Storage best practices for VMware vSphere should be followed as part of a design:

- FlashArray Volumes are automatically presented to VMware vSphere using the Round Robin Path Selection Policy (PSP) and appropriate vendor Storage Array Type Plugin (SATP) for vSphere 7.0.



- vSphere 7.0 also uses the Latency SATP that was introduced in vSphere 6.7U1 (This replaces the I/O Operations Limit of 1 SATP, which was the default from vSphere 6.5U1).
- When using iSCSI connected FlashArray volumes, it is recommended to set DelayedAck to false (disabled) and LoginTimeout to 30 seconds. Jumbo Frames are optional when using iSCSI.
- For VMFS-6, keep automatic UNMAP enabled.
- `DataMover.HardwareAcceleratedMove`, `DataMover.HardwareAcceleratedInit`, and `VMFS3.HardwareAcceleratedLocking` should all be enabled.
- Ensure all ESXi hosts are connected to both FlashArray controllers. A minimum of two paths to each in order to achieve total redundancy.
- Install VMware tools or Open VM tools whenever possible.
- Queue depths should be left at the default. Changing queue depths on the ESXi host is a tweak and should only be examined if a performance problem (high latency) is observed.
- When mounting snapshots, use the ESXi resignature option and avoid force-mounting.
- Configure Host Groups on the FlashArray identically to clusters in vSphere. For example, if a cluster has four hosts in it, create a corresponding Host Group on the relevant FlashArray with exactly those four hosts—no more, no less.
- When possible, use Paravirtual SCSI adapters for virtual machines.
- Atomic Test and Set (ATS) is required on all Pure Storage volumes. This is a default configuration, and no changes should normally be needed.

For more information about the VMware vSphere Pure Storage FlashArray Best Practices, go to: [https://support.purestorage.com/Solutions/VMware\\_Platform\\_Guide/001VMwareBestPractices/hhhWeb\\_Guide%3A\\_FlashArray\\_VMware\\_Best\\_Practices](https://support.purestorage.com/Solutions/VMware_Platform_Guide/001VMwareBestPractices/hhhWeb_Guide%3A_FlashArray_VMware_Best_Practices)

## Pure Storage FlashArray Best Practices for VMware Virtual Volumes (vVols)

**Note:** VMware Horizon 8 only supports VVols with full-clone virtual machines. Virtual Volumes datastores are not supported for instant clone desktop pools.

Along with the Pure Storage Best Practices for VMware vSphere, the following should be considered as part of a design that includes the implementation of vVols as part of the solution:

- Create a Local FlashArray Array Admin user to register the storage provider with vs using the local pureuser account, v vols-admin for example.
- Use the Round Robin pathing policy (default) for the Protocol Endpoint.
- Use the Pure Storage Plugin for the vSphere Client to register the FlashArray storage provider and mount the vVols Datastore if possible.
- If manually registering the storage providers, Register both controllers' storage providers with CT0.ETH0 and CT1.ETH0. It is supported to use Eth1 if a customer certificate is used.
- If manually mounting the vVol datastore, you will need to connect the protocol endpoint.
- A single PE should be enough for the design utilizing the default device queue depth for the PE.
- Keep VM Templates on vVols when deploying new vVol VMs from a template.
- When resizing a VM's VMDK that resides on a vVol, complete the task from vSphere Client and not the FlashArray GUI.
- vCenter Server should not reside on a vVol

- All ESXi Hosts, vCenter Server and FlashArray should have the same NTP Server synchronization configuration and be configured to send their logs to a syslog target.
- TCP port 8084 must be open and accessible from vCenter Servers and ESXi hosts to the FlashArray that will be used for vVol.
- The FlashArray Protocol Endpoint object 'pure-protocol-endpoint' must exist. The FlashArray admin must not rename, delete, or otherwise edit the default FlashArray Protocol Endpoint.

For more information about vVols best practices, go to:

[https://support.purestorage.com/Solutions/VMware\\_Platform\\_Guide/Quick\\_Reference\\_by\\_VMware\\_Product\\_and\\_Integration/Virtual\\_Volumes\\_Quick\\_Reference](https://support.purestorage.com/Solutions/VMware_Platform_Guide/Quick_Reference_by_VMware_Product_and_Integration/Virtual_Volumes_Quick_Reference)

## Desktop Virtualization Design Fundamentals

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

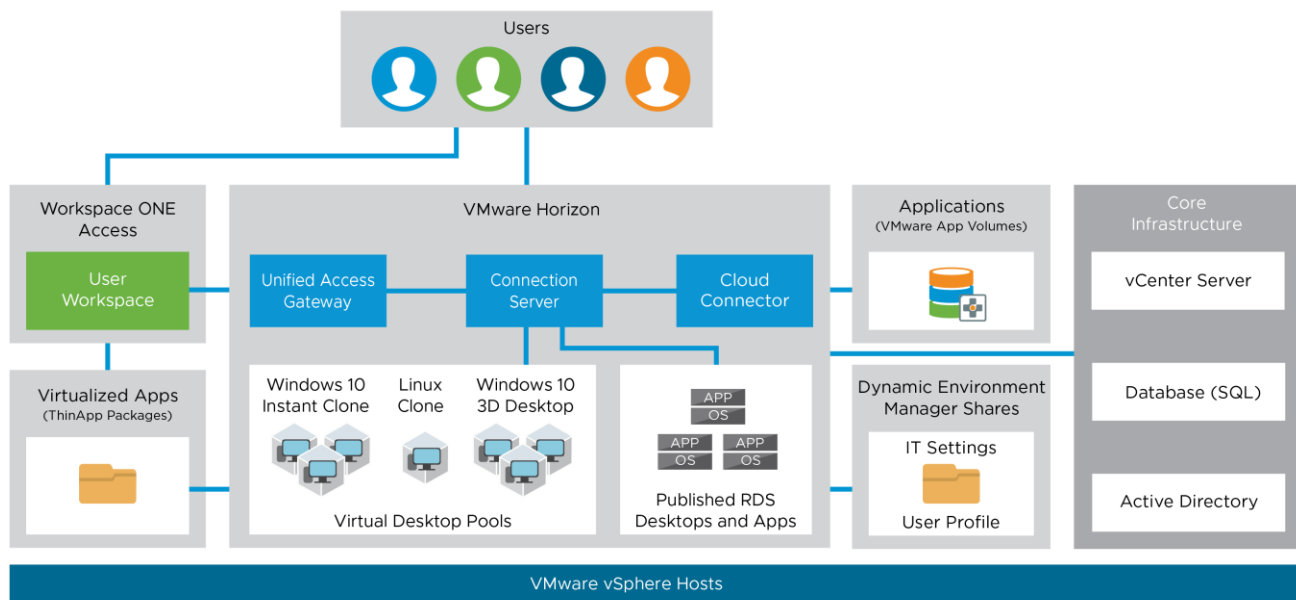
## VMware Horizon Design Fundamentals

VMware Horizon 8 integrates Remote Desktop Server Hosted sessions users and VDI desktop virtualization technologies into a unified architecture that enables a scalable, simple, efficient, mixed users and manageable solution for delivering Windows applications and desktops as a service.

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

Several components must be deployed to create a functioning Horizon environment to deliver the VDI. These components refer to as common services and encompass: Domain Controllers, DNS, DHCP, User Profile managers, SQL, vCenters, VMware Horizon View Connection Servers.

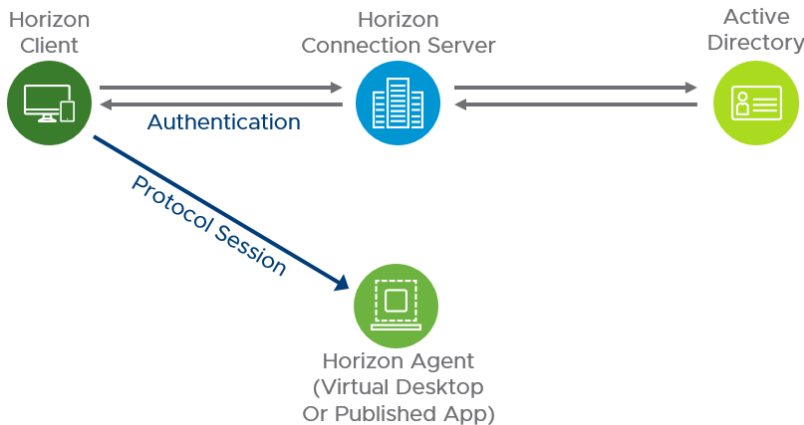
**Figure 11. VMware Horizon Design Overview**



## Horizon VDI Pool and RDSH Servers Pool

Collections of identical Virtual Machines (VMs) or physical computers are managed as a single entity called a Desktop Pool. The VM provisioning relies on VMware Horizon Connection Server, vCenter Server and AD components. The Horizon Client then forms a session using PCoIP, Blast, or RDP protocols to a Horizon Agent running in a virtual desktop, RDSH server, or physical computer. In this CVD, virtual machines in the Pools are configured to run either a Windows Server 2019 OS (for RDS Hosted shared sessions using RDP protocol) and a Windows 10 Desktop OS (for pooled VDI desktops using Blast protocol).

**Figure 12. Horizon VDI and RDSH Desktop Delivery Based on Display Protocol (PcoIP/Blast/RDP)**

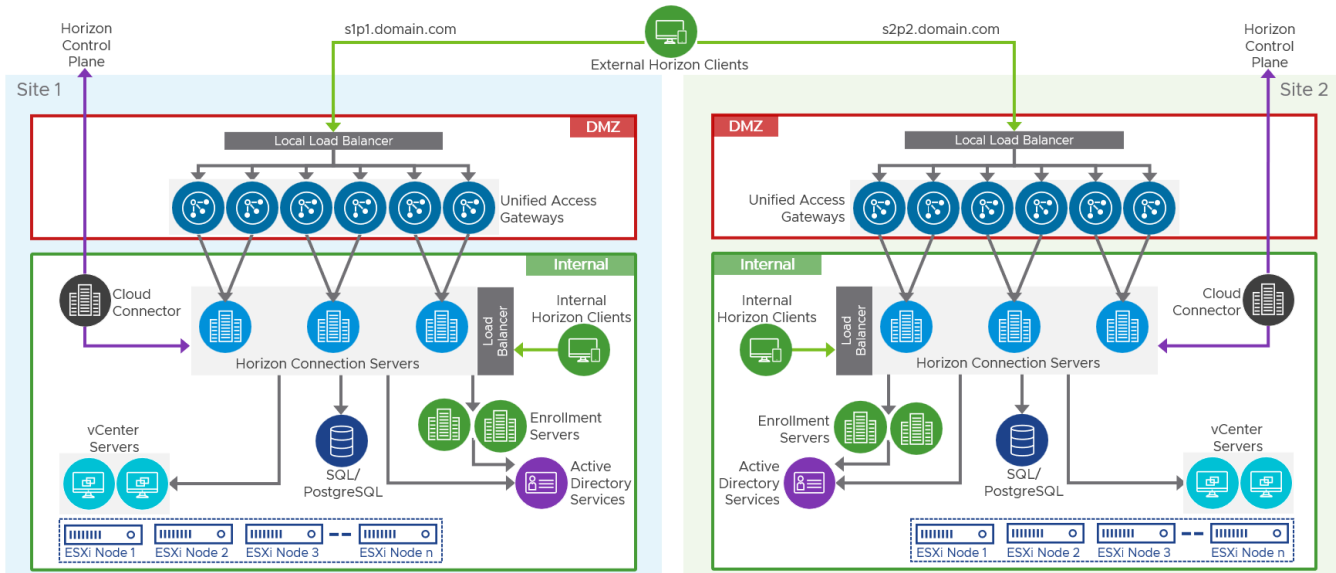


## Multiple-Site Configuration

If you have multiple regional sites, you can use any of the Load Balances Tools to direct the user connections to the most appropriate site to deliver the desktops and application to users.

Figure 13 illustrates the logical architecture of the Horizon multisite deployment. Such architecture eliminates any single point of failure that can cause an outage for desktop users.

**Figure 13. Multisite Configuration Overview**



Based on the requirement and the number of data centers or remote locations, you can choose any of the available load balancing software to increase security and optimize the user experience.

**Note:** Multisite configuration is shown as the example and was not used as part of this CVD testing.

## Designing a Virtual Desktop Environment for Different Workloads

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

**Table 1.** Desktop type and user experience

Desktop Type	User 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 data center.</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 Remote Desktop Server Hosted sessions (RDSH) using RDS based Server OS and VMware Horizon pooled Instant and Full Clone Virtual Machine Desktops using VDI based desktop OS machines were configured and tested.

---

## Deployment Hardware and Software

This chapter contains the following:

- [Architecture](#)
- [Products Deployed](#)
- [Physical Topology](#)
- [Logical Architecture](#)
- [Configuration Guidelines](#)

### Architecture

This FlashStack architecture delivers a Virtual Desktop Infrastructure that is redundant and uses the best practices of Cisco and Pure Storage.

It includes:

- VMware vSphere 7.0 U3d hypervisor installed on the Cisco UCS B200 M6 compute nodes configured for stateless compute design using boot from SAN.
- Pure Storage FlashArray//X70 R3 provides the storage infrastructure required for VMware vSphere hypervisors and the VDI workload delivered by VMware Horizon 8 2212.
- Cisco Intersight provides UCS infrastructure management with lifecycle management capabilities.

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

### Products Deployed

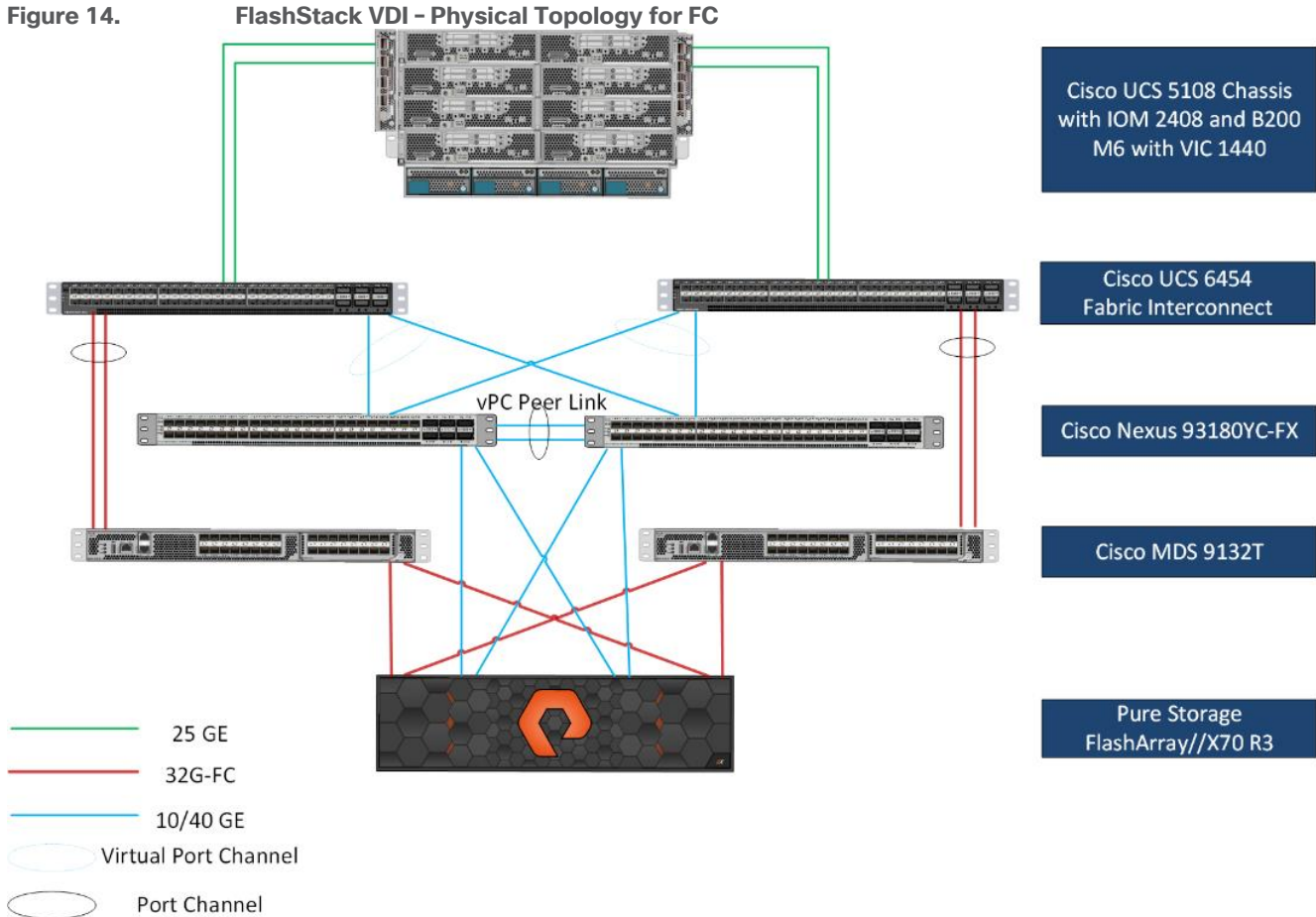
This CVD details the deployment of up to 2300 multi-session OS, 1700 Single-session OS VDI users featuring the following software:

- VMware vSphere ESXi 7.0 U3d hypervisor.
- VMware vCenter 7.0 U3 to set up and manage the virtual infrastructure as well as integration of the virtual environment with Cisco Intersight software.
- Microsoft SQL Server 2019.
- Microsoft Windows Server 2019 and Windows 10 64-bit virtual machine Operating Systems.
- VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) Sessions provisioned as Instant Clone RDS Servers and stored on the Pure Storage FlashArray//X70 R3.
- VMware Horizon 8 2212 Non-Persistent Win 10 Virtual Desktops (VDI) provisioned as Instant Clones virtual machines and stored on Pure Storage FlashArray//X70 R3.
- VMware Horizon 8 2212 Persistent Win 10 Virtual Desktops (VDI) provisioned as Full Clones virtual machines and stored on Pure Storage FlashArray//X70 R3.
- Microsoft Office 2016 for Login VSI End User Measurement Knowledge worker workload test.
- FSLogix for User Profile Management.
- Cisco Intersight platform to deploy, maintain, and support the FlashStack components.

- Cisco Intersight Assist virtual appliance to help connect the Pure Storage FlashArray and VMware vCenter with the Cisco Intersight platform.

## Physical Topology

FlashStack VDI with Cisco UCS B200 M6 Modular System is a Fibre Channel (FC) based storage access design. Pure Storage FlashArray and Cisco UCS are connected through Cisco MDS 9132T switches and storage access utilizes the FC network. For VDI IP based file share storage access Pure Storage FlashArray and Cisco UCS are connected through Cisco Nexus C93180YC-FX switches. The physical connectivity details are explained below.



**Figure 14** details the physical hardware and cabling deployed to enable this solution:

- Two Cisco Nexus 93180YC-FX Switches in NX-OS Mode.
- Two Cisco MDS 9132T 32-Gb Fibre Channel Switches.
- One Cisco UCS 5108 Chassis with two Cisco UCS-IOM-2408 25GB IOM Modules.
- Eight Cisco UCS B200 M6 Blade Servers with Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM, and one Cisco VIC1440 mezzanine card, providing N+1 server fault tolerance.
- Pure Storage FlashArray//X70 R3 with dual redundant controllers, with Twenty 1.92TB DirectFlash NVMe drives.

**Note:** The management components and LoginVSI Test infrastructure are hosted on a separate vSphere cluster and are not a part of the physical topology of this solution.

[Table 2](#) lists the software versions of the primary products installed in the environment.

**Table 2.** Software and Firmware Versions

Vendor	Product/Component	Version/Build/Code
Cisco	UCS Component Firmware	4.2(2d)
Cisco	UCS B200 M6 Compute Node	4.2(2d)
Cisco	VIC 1440 (Virtual Interface Card)	4.2(2d)
Cisco	Cisco Nexus 93180YC-FX Switches	9.3(7a)
Cisco	Cisco MDS 9132T	8.5(1a)
Pure Storage	FlashArray//X70 R3	Purity//FA 6.3.3
VMware	vCenter Server Appliance	7.0.3 Build:20395099
VMware	vSphere 7. 0. 3d	7.0.3, 19482537
VMware	VMware Horizon 8 2212 Connection server	8.8.0-20099816
VMware	VMware Horizon 8 2212 Agent	8.8.0.20088748
Cisco	Intersight Assist	1.0.11-759
Microsoft	FSLogix 2105 HF_01 (User Profile Mgmt.)	2.9.7979.62170
VMware	Tools	11.3.5.18557794

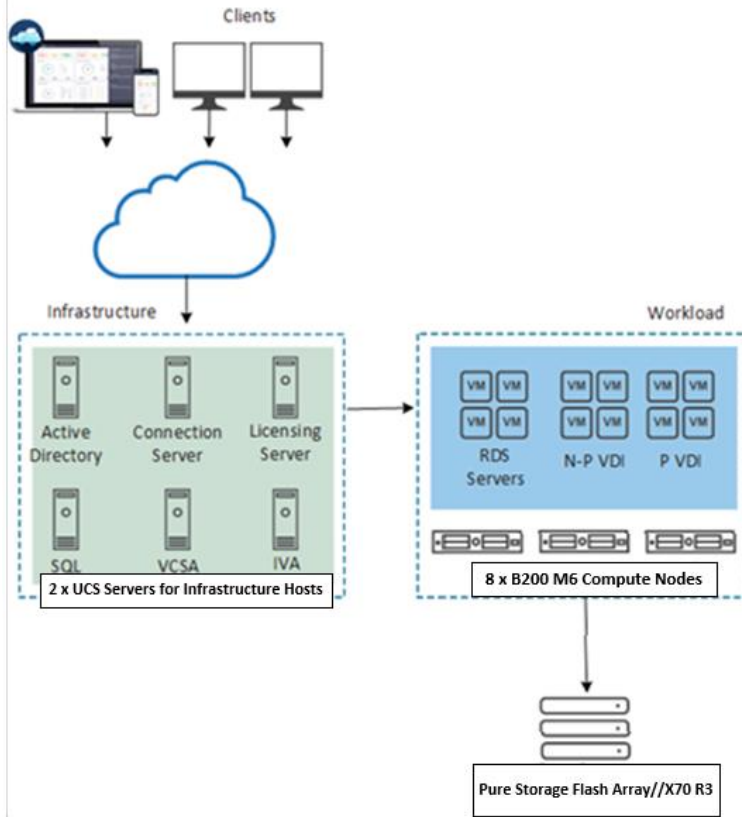
## Logical Architecture

The logical architecture of the validated solution which is designed to run desktop and RDSH server VMs supporting up to 2300 users on a single chassis containing 8 blades, with physical redundancy for the blade servers for each workload type and have a separate vSphere cluster to host management services, is illustrated in [Figure 15](#).

**Note:** Separating management components and desktops is a best practice for the large environments.



Figure 15. Logical Architecture Overview



## VMware Clusters

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

- VDI Cluster Flashstack Datacenter with Cisco UCS.
  - Infrastructure: Infra VMs (vCenter, Active Directory, DNS, DHCP, SQL Server, VMware Horizon Connection Servers, VMware Horizon Replica Servers, VMware vSphere, VSMs, and required VMs or plug in VMS so on).
  - VDI Workload VMs (Windows Server 2019 streamed RDS Server VMs with VMware Horizon for Remote Desktop Server Hosted (RDSH) Sessions, Windows 10 Streamed with VMware Horizon Instant Cloned (non-persistent) and Full Cloned (persistent) desktops).
- VSI Launchers and Launcher Cluster.

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

## Configuration Guidelines

The VMware Horizon 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, Cisco Nexus A and Cisco 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 the reader to configure the VMware Horizon customer environment as a stand-alone solution.

## VLANs

The VLAN configuration recommended for the environment includes a total of six VLANs as outlined in [Table 3](#).

**Table 3.** VLANs Configured in this study

VLAN Name	VLAN ID	VLAN Purpose
Default	1	Native VLAN
FS-InBand-Mgmt_70	70	In-Band management interfaces
FS-Infra-Mgmt_71	71	Infrastructure Virtual Machines
FS-VDI_72	72	RDSH, VDI Persistent and Non-Persistent
FS-vMotion_73	73	VMware vMotion
OOB-Mgmt_164	164	Out of Band management interfaces

## VSANs

[Table 4](#) lists the two virtual SANs that were configured for communications and fault tolerance in this design.

**Table 4.** VSANs Configured in this study

VSAN Name	VSAN ID	VSAN Purpose
VSAN 100	100	VSAN for Primary SAN communication
VSAN 101	101	VSAN for Secondary SAN communication

---

## Solution Configuration

This chapter contains the following:

- [Solution Cabling](#)

### Solution Cabling

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

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

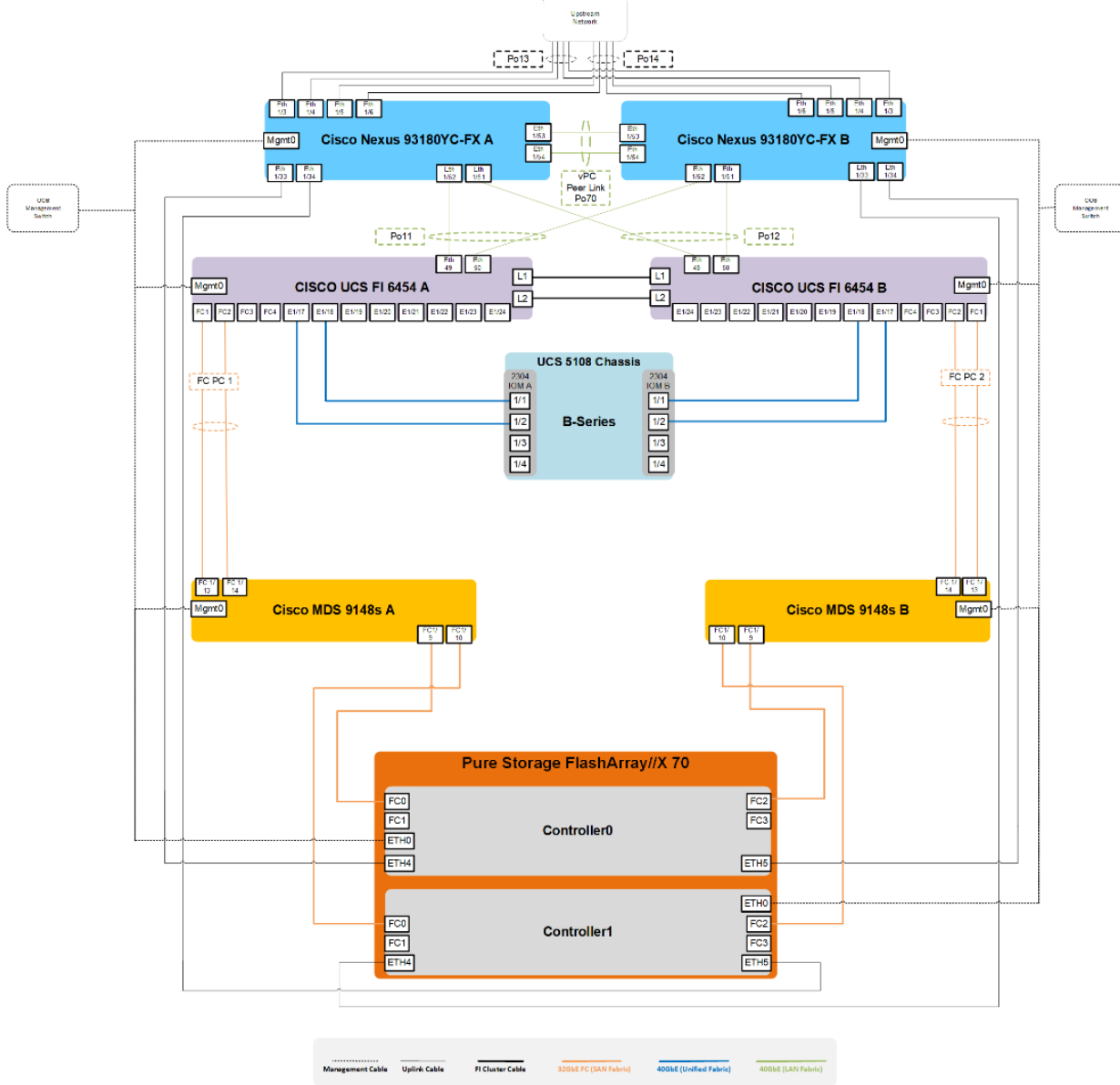
The tables in this section list the details for the prescribed and supported configuration of the Pure Storage FlashArray//X70 R3 storage array to the Cisco 6454 Fabric Interconnects through Cisco MDS 9132T 32-Gb FC switches.

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

**Note:** Be sure to follow the cabling directions in this section. Failure to do so will result in problems with your deployment.

[Figure 16](#) details the cable connections used in the validation lab for FlashStack topology based on the Cisco UCS 6454 fabric interconnect. Four 32Gb uplinks connect as port-channels to each Cisco UCS Fabric Interconnect from the MDS switches, and a total of eight 32Gb links connect the MDS switches to the Pure Storage FlashArray//X R3 controllers, four of these have been used for scsi-fc and the other four to support nvme-fc. Also, the 25Gb links connect the Cisco UCS Fabric Interconnects to the Cisco Nexus Switches and the Pure Storage FlashArray//X R3 controllers to the Cisco Nexus Switches. Additional 1Gb management connections will be needed for an out-of-band network switch that sits apart from the FlashStack infrastructure. Each Cisco UCS fabric interconnect and Cisco Nexus switch is connected to the out-of-band network switch, and each FlashArray controller has a connection to the out-of-band network switch. Layer 3 network connectivity is required between the Out-of-Band (OOB) and In-Band (IB) Management Subnets.

**Figure 16. FlashStack solution cabling diagram**



## Configuration and Installation

This chapter contains the following:

- [FlashStack Automated Deployment with Ansible](#)
- [FlashStack Manual Deployment](#)
- [Cisco UCS B200 M6 Configuration – Intersight Managed Mode \(IMM\)](#)
- [Cisco MDS 9132T 32-Gb FC Switch Configuration](#)
- [Pure Storage FlashArray//X70 R3 to MDS SAN Fabric Connectivity](#)
- [Configure Pure Storage FlashArray//X70 R3](#)
- [Install and Configure VMware ESXi 7.0](#)
- [Cisco Intersight Orchestration](#)
- [Pure Storage CloudSnap](#)

### FlashStack Automated Deployment with Ansible

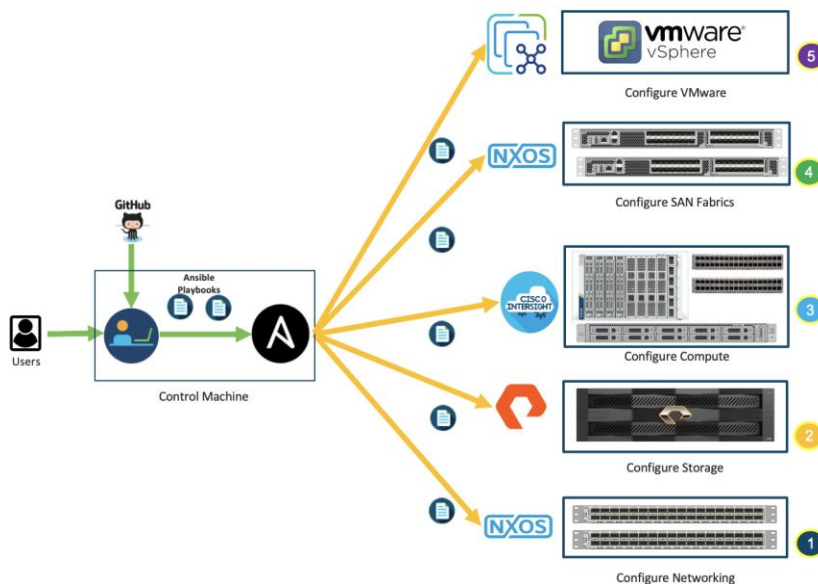
This solution offers Ansible Playbooks that are made available from a GitHub repository that customers can access to automate the FlashStack deployment.

GitHub repository is available here: [https://github.com/ucs-compute-solutions/FlashStack\\_IMM\\_Ansible](https://github.com/ucs-compute-solutions/FlashStack_IMM_Ansible).

This repository contains Ansible playbooks to configure all the components of FlashStack including:

- Cisco UCS in Intersight Managed Mode (IMM)
- Cisco Nexus and MDS Switches
- Pure Storage FlashArray
- VMware ESXi and VMware vCenter

Figure 17. High-Level FlashStack Automation



## FlashStack Manual Deployment

Cisco Intersight Managed Mode standardizes policy and operation management for Cisco UCS B200 M6. The compute nodes in Cisco UCS B200 M6 are configured using server profiles defined in Cisco Intersight. These server profiles derive all the server characteristics from various policies and templates. At a high level, configuring Cisco UCS using Cisco Intersight Managed Mode consists of the steps shown in [Figure 18](#). Figure 18.

**Figure 18. Configuration Steps for Cisco Intersight Managed Mode**



## Cisco UCS B200 M6 Configuration - Intersight Managed Mode (IMM)

### Procedure 1. Configure Cisco UCS Fabric Interconnects for IMM

**Step 1.** Verify the following physical connections on the fabric interconnect:

- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router.
- The L1 ports on both fabric interconnects are directly connected to each other.
- The L2 ports on both fabric interconnects are directly connected to each other.

**Step 2.** Connect to the console port on the first Fabric Interconnect.

**Step 3.** 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

#### Procedure 1. Configure the Cisco UCS for use in Intersight Managed Mode

**Step 1.** 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 2.** 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 3.** 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 B
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. Claim a Cisco UCS Fabric Interconnect in the Cisco Intersight Platform

If you do not already have a Cisco Intersight account, you need to set up a new account in which to claim your Cisco UCS deployment. Start by connecting to <https://intersight.com>.

All information about Cisco Intersight features, configurations can be accessed in the [Cisco Intersight Help Center](#).

**Step 1.** Click Create an account.

**Step 2.** Sign in with your Cisco ID.

**Step 3.** Read, scroll through, and accept the end-user license agreement. Click Next.

**Step 4.** Enter an account name and click Create.

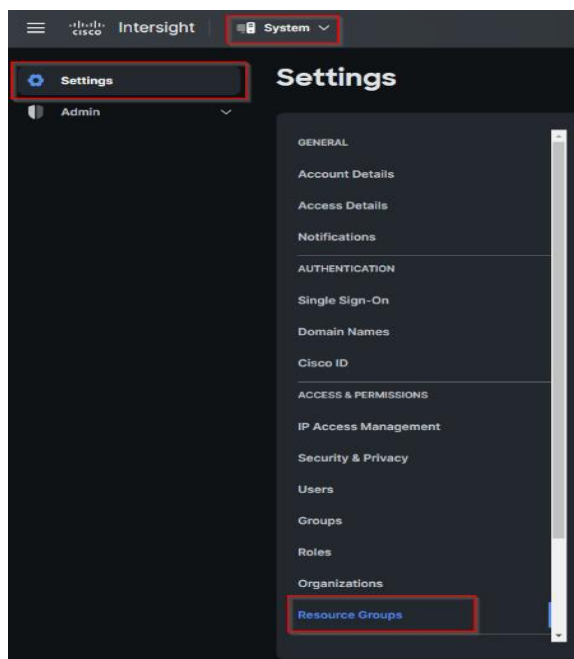
If you have an existing Cisco Intersight account, connect to <https://intersight.com> and sign in with your Cisco ID, select the appropriate account.

**Note:** In this step, a Cisco Intersight organization is created where all Cisco Intersight managed mode configurations including policies are defined.

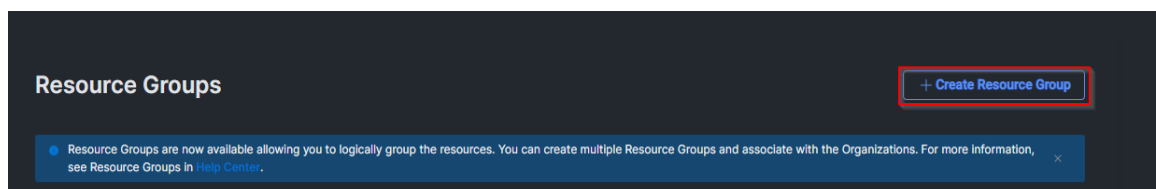
**Step 5.** Log into the Cisco Intersight portal as a user with account administrator role.

**Step 6.** From the Service Selector drop-down list, select System.

**Step 7.** Navigate to Settings > General > Resource Groups.



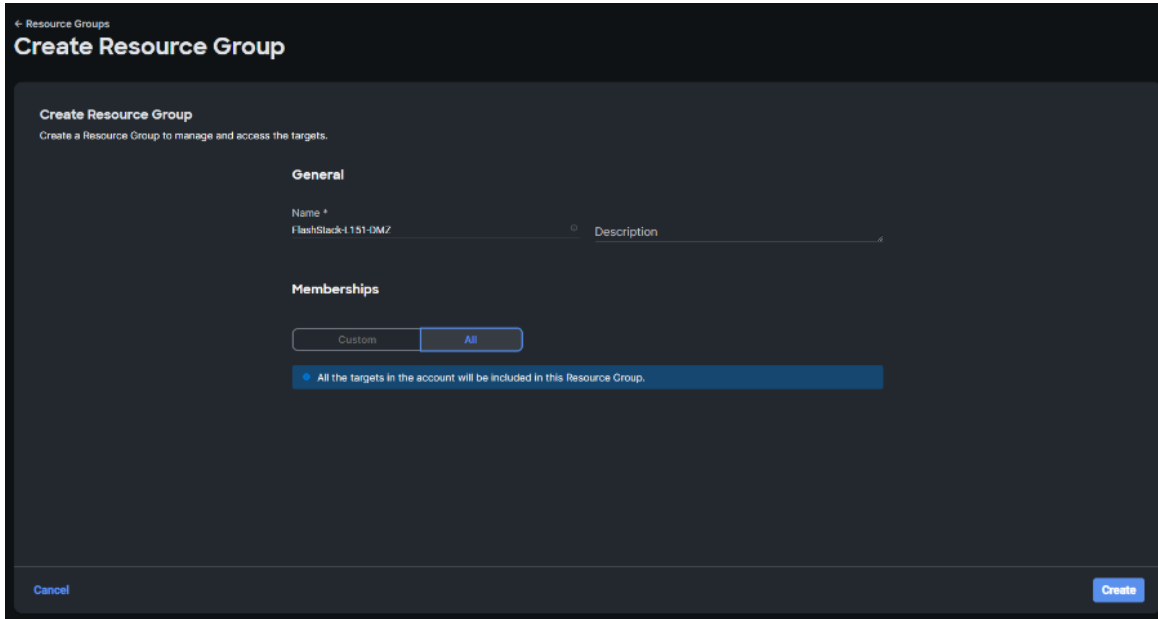
**Step 8.** On Resource Groups panel click + Create Resource Group in the top-right corner.



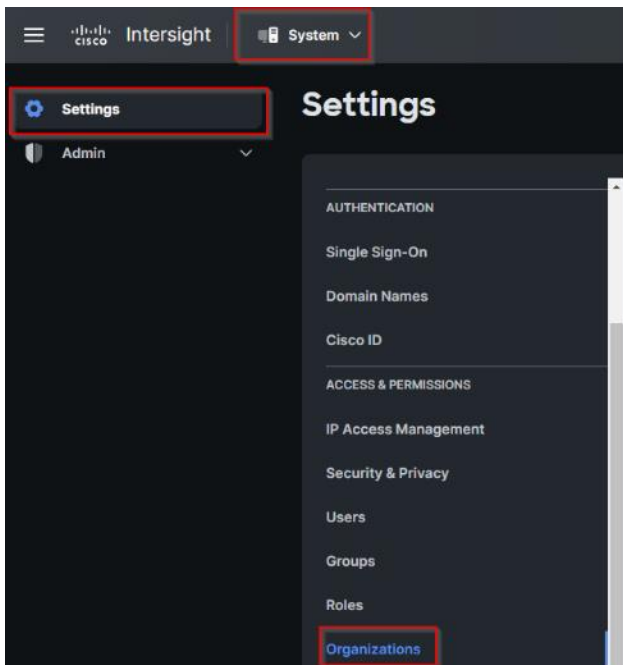
**Step 9.** Provide a name for the Resource Group (for example, FlashStack-L151-DMZ).

**Step 10.** Click Create.

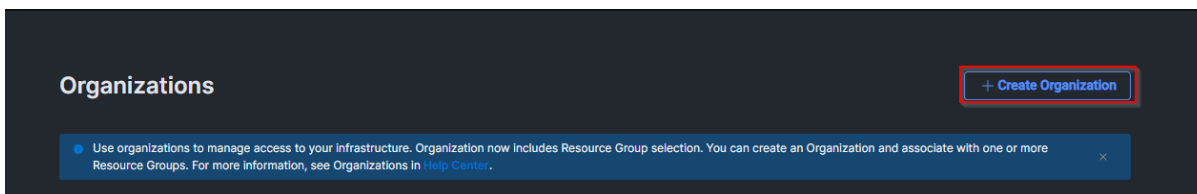




**Step 11.** Navigate to Settings > General > Organizations.



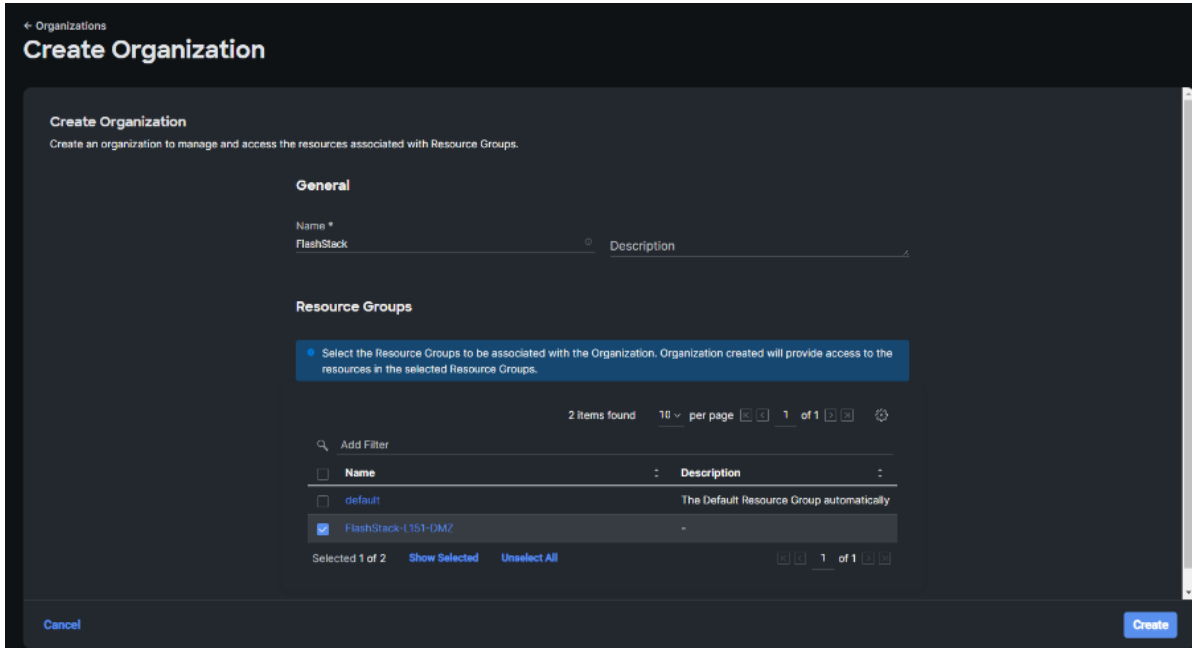
**Step 12.** On Organizations panel click + Create Organization in the top-right corner.



**Step 13.** Provide a name for the organization (FlashStack).

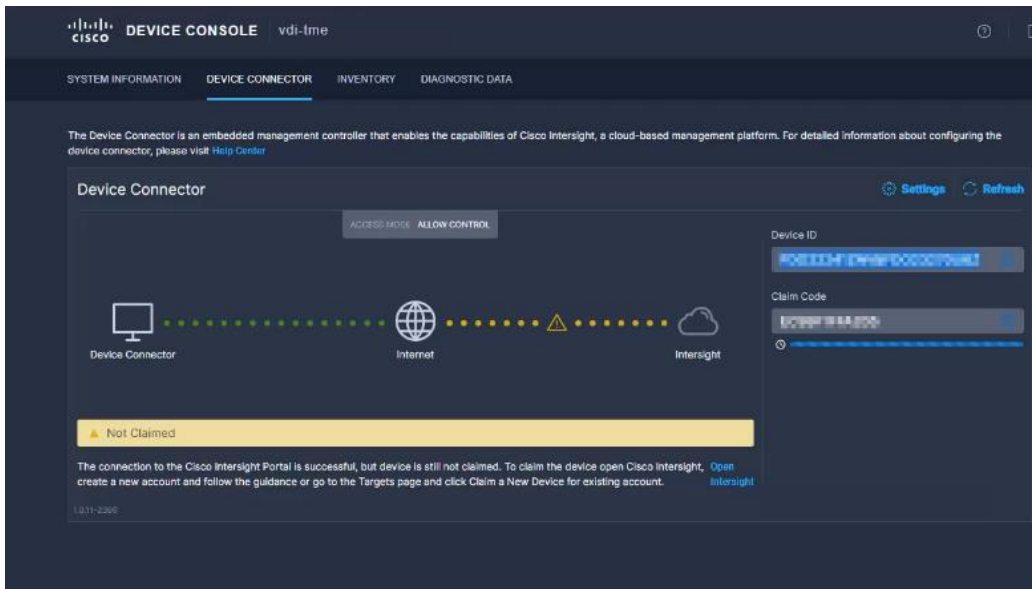
**Step 14.** Select the Resource Group created in the last step (for example, FlashStack-L151-DMZ).

**Step 15.** Click Create.

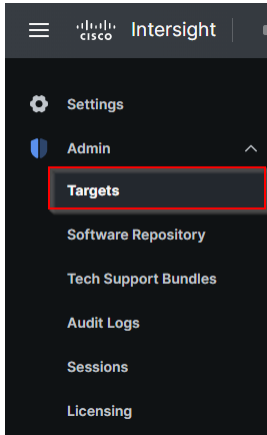


**Step 16.** Use the management IP address of Fabric Interconnect A to access the device from a web browser and the previously configured admin password to log into the device.

**Step 17.** 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.



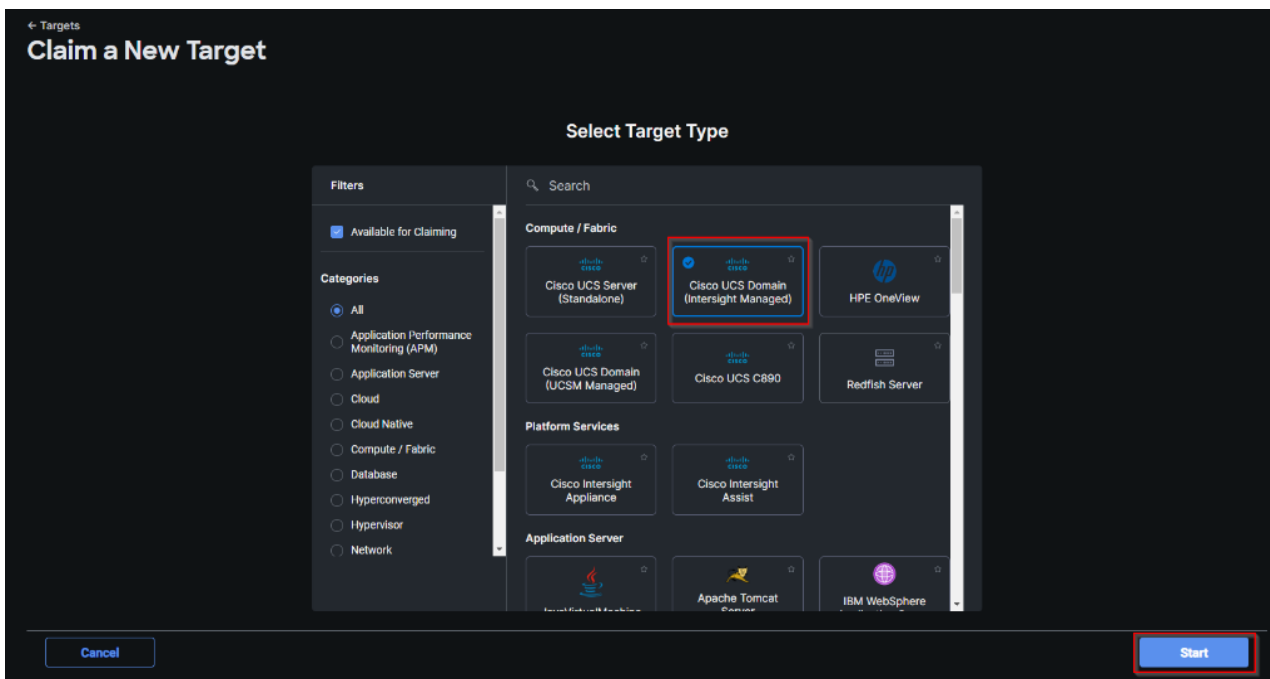
**Step 18.** Navigate to Admin > General > Targets.



**Step 19.** On Targets panel click Claim a New Target in the top-right corner.

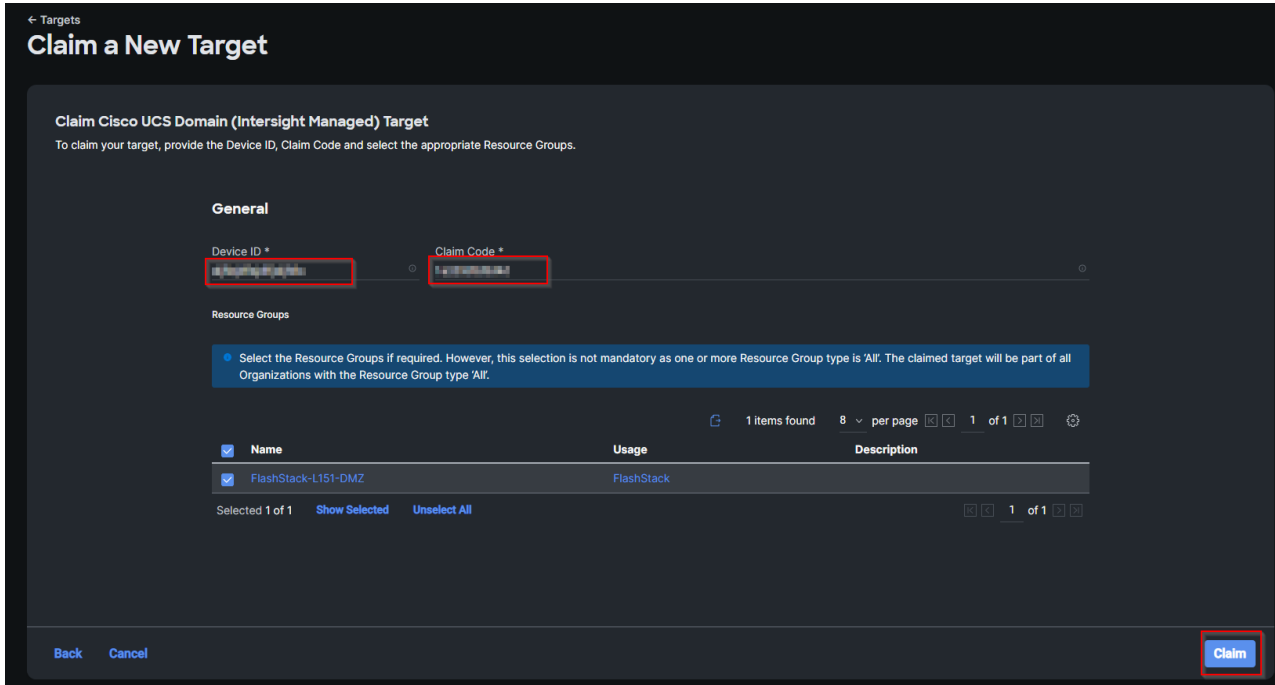


**Step 20.** Select Cisco UCS Domain (Intersight Managed) and click Start.

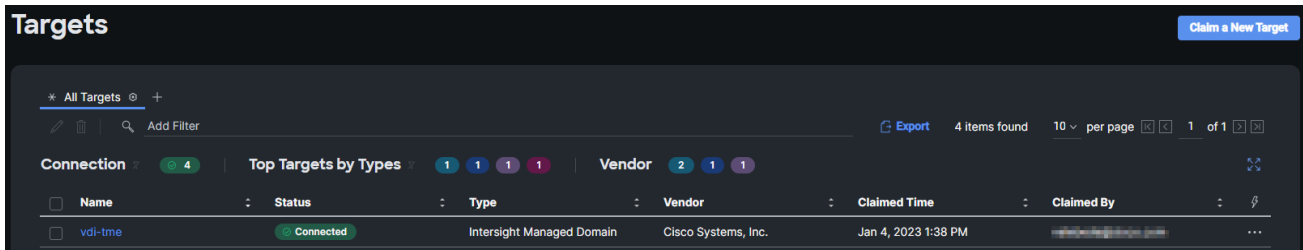


**Step 21.** Enter the Device ID and Claim Code captured from the Cisco UCS FI.

**Step 22.** Select the previously created Resource Group and click Claim.



**Step 23.** On successfully device claim, Cisco UCS FI should appear as a target in Cisco Intersight.



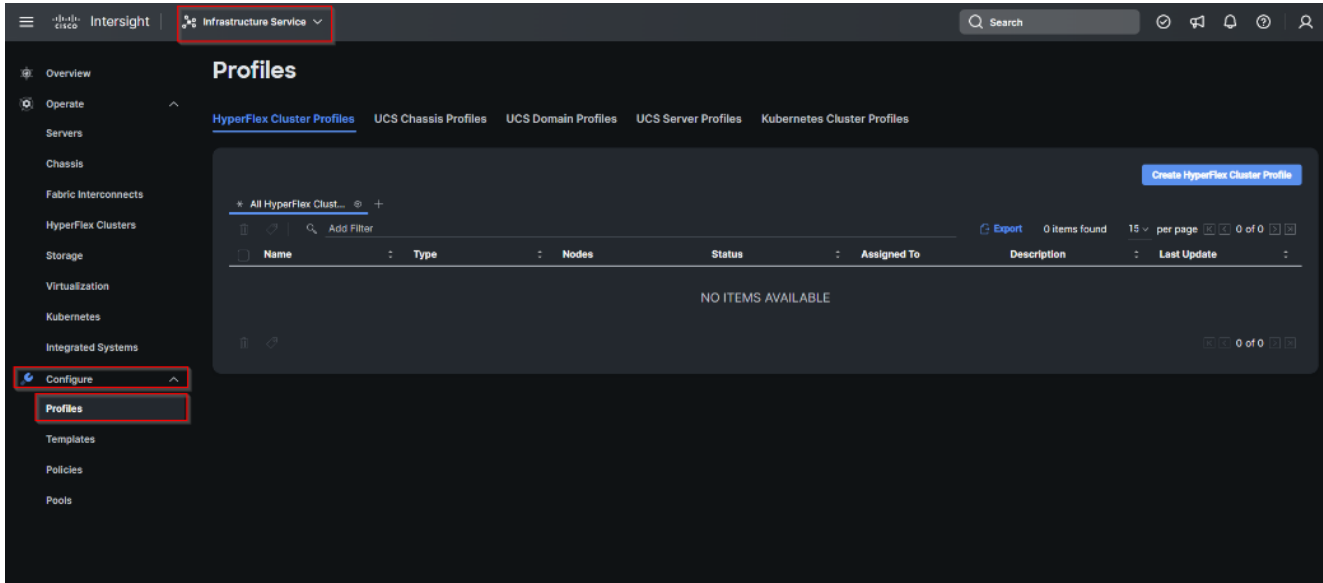
## Configure a Cisco UCS Domain Profile

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.

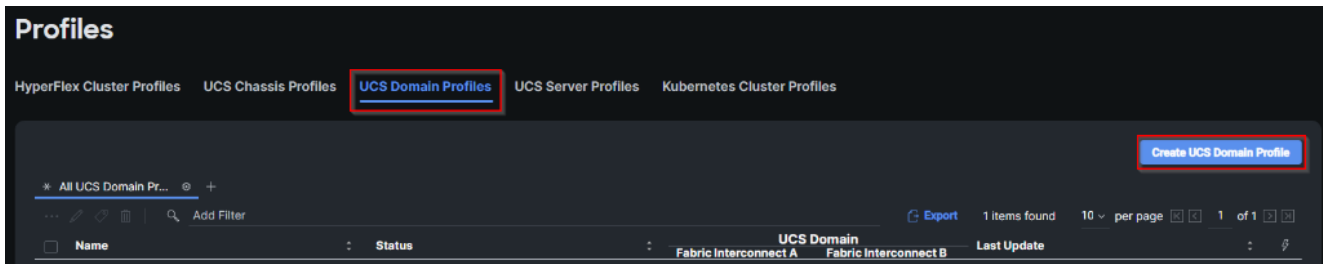
After the Cisco UCS domain profile has been successfully created and deployed, the policies including the port policies are pushed to Cisco UCS Fabric Interconnects. Cisco UCS domain profile can easily be cloned to install additional Cisco UCS systems. When cloning the UCS domain profile, the new UCS domains utilize the existing policies for consistent deployment of additional Cisco UCS systems at scale.

### Procedure 1. Create a Domain Profile

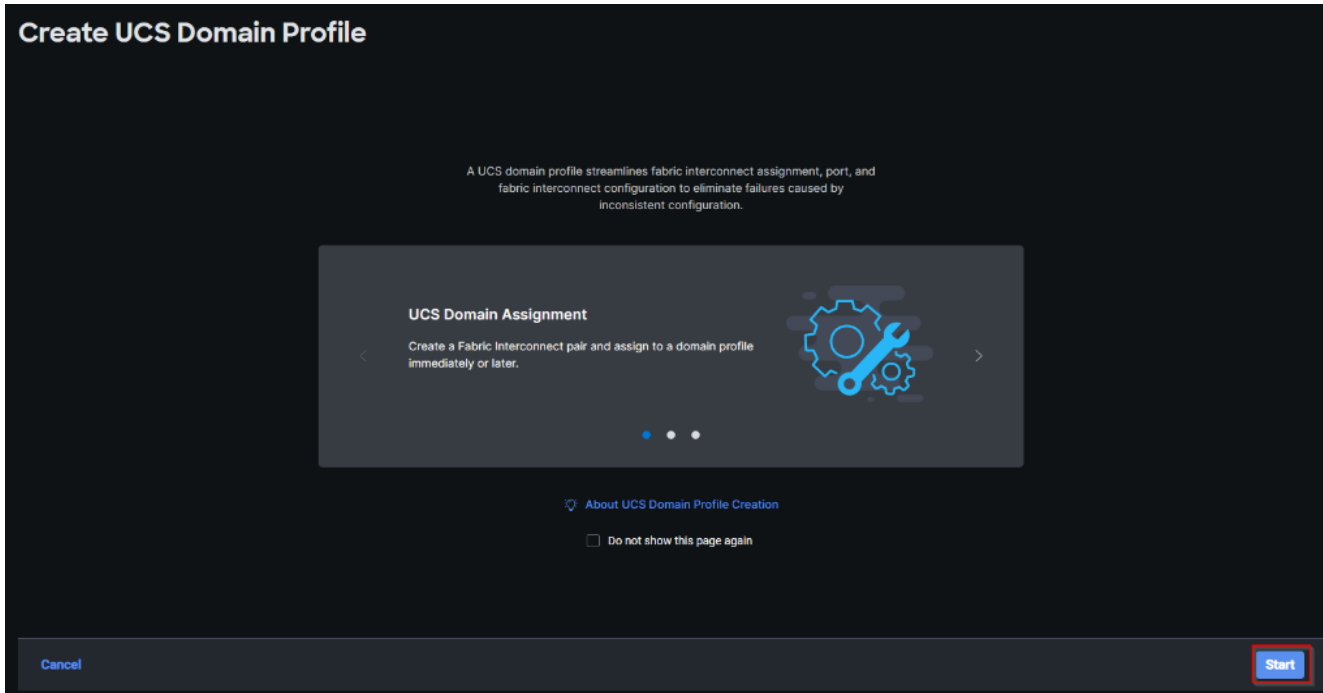
**Step 1.** From the Service Selector drop-down list, select Infrastructure Service. Navigate to Configure > Profiles, to launch the Profiles Table view.



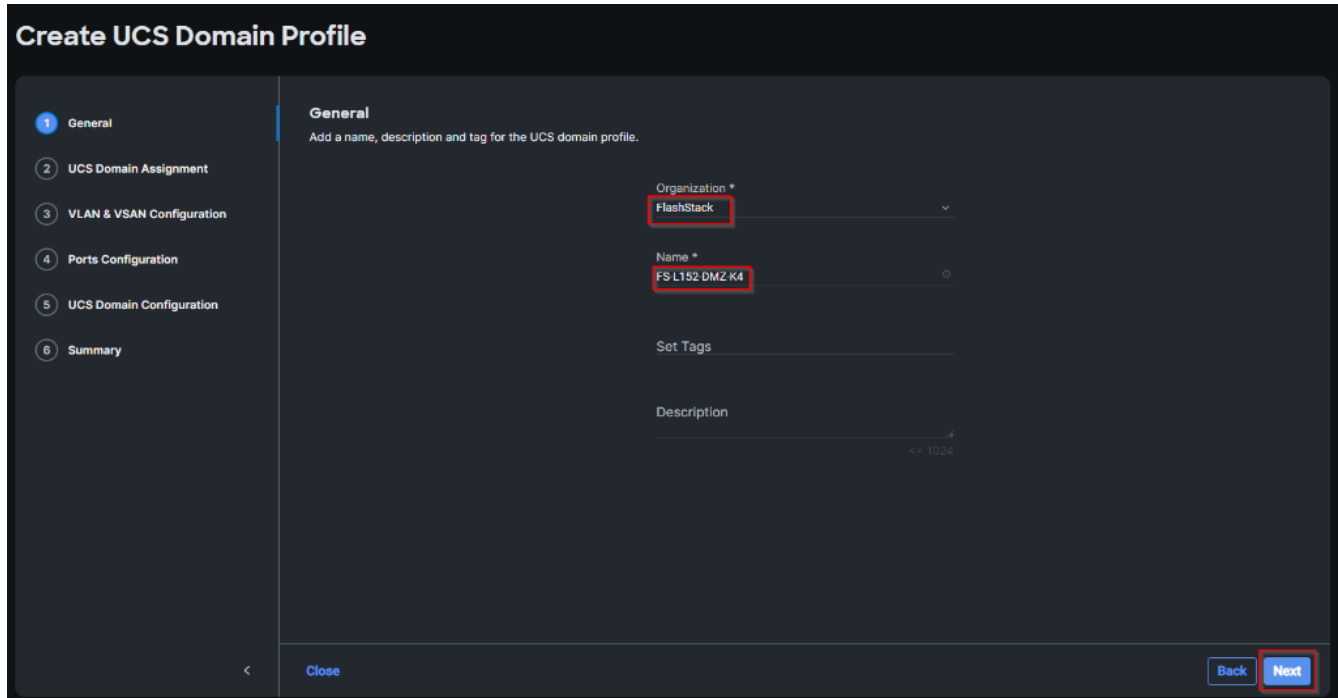
**Step 2.** Navigate UCS Domain Profiles tab and click Create UCS Domain Profile.



**Step 3.** On the Create UCS Domain Profile screen, click Start.

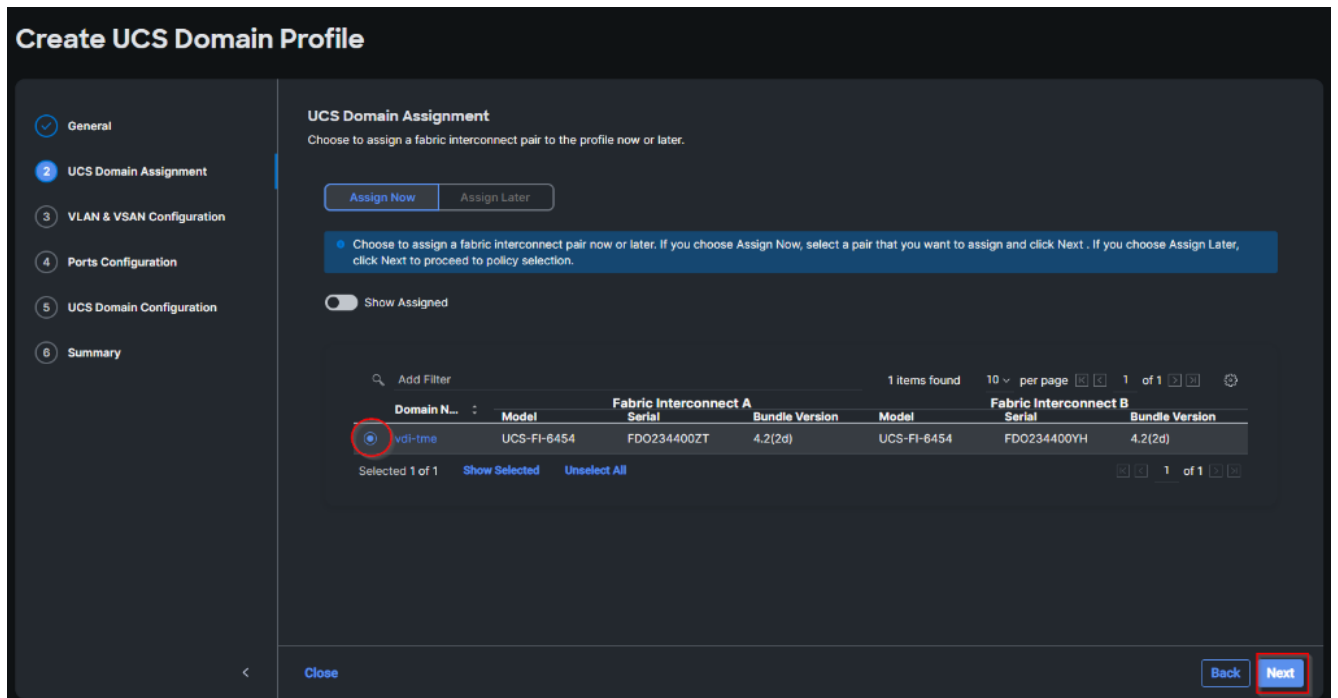


**Step 4.** On the General page, select the organization created before and enter a name for your profile (for example, FS-L152-DMZ-K4). Optionally, include a short description and tag information to help identify the profile. Tags must be in the key:value format. For example, Org: IT or Site: APJ. Click Next.



**Step 5.** On the Domain Assignment page, assign a switch pair to the Domain profile. Click Next.

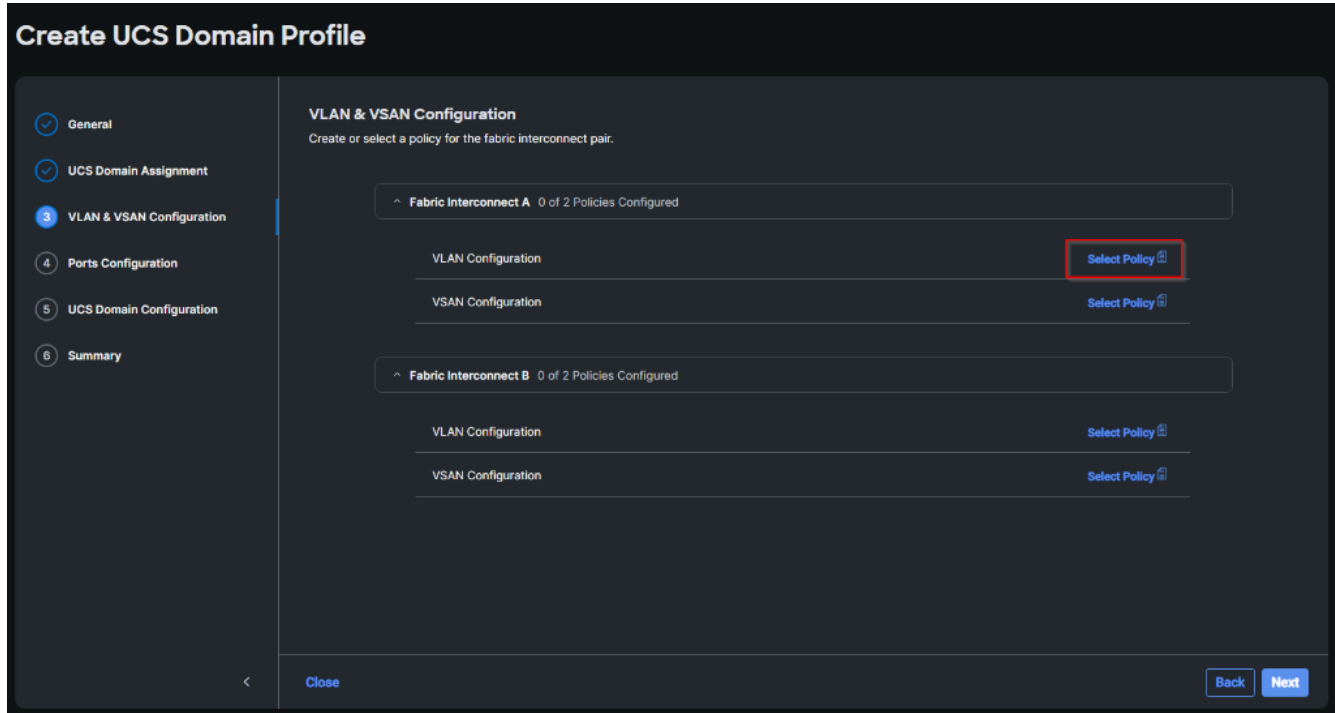
**Note:** You can also click Assign Later and assign a switch pair to the Domain profile at a later time.



**Step 6.** On the VLAN & VSAN Configuration page, attach VLAN and VSAN policies for each switch to the UCS Domain Profile.

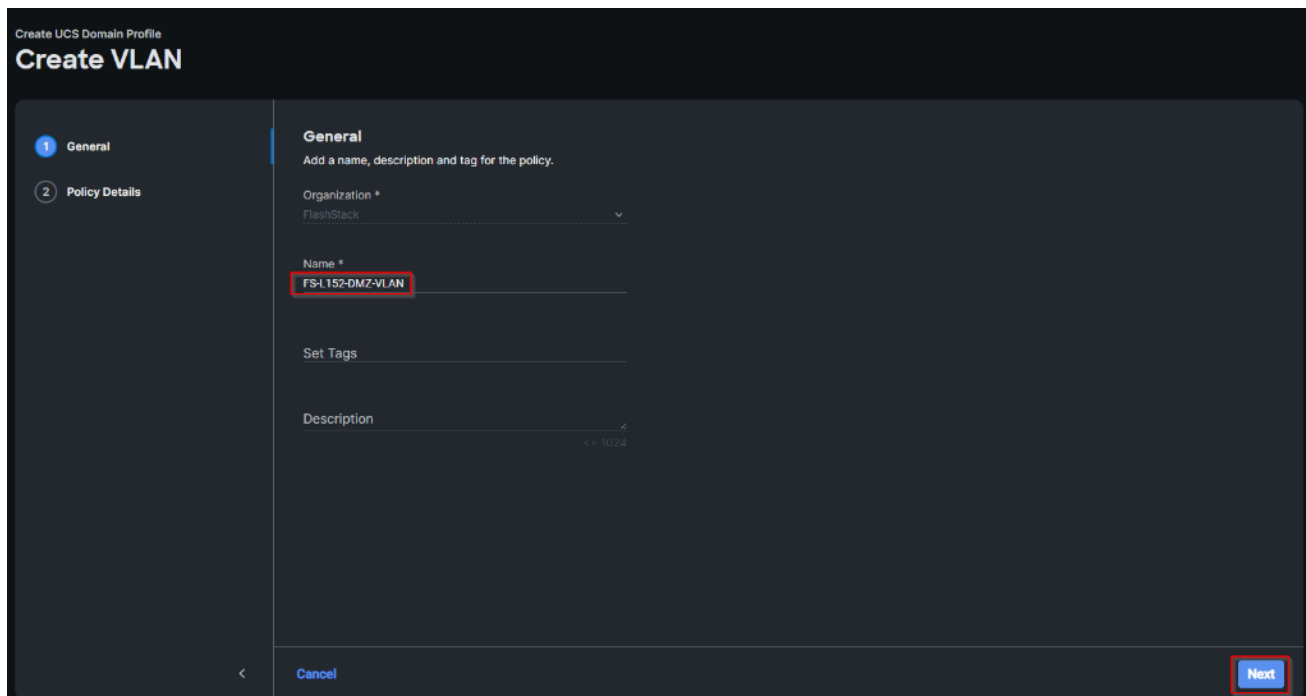
**Note:** In this step, a single VLAN policy is created for both fabric interconnects and two individual VSAN policies are created because the VSAN IDs are unique for each fabric interconnect.

**Step 7.** Click Select Policy next to VLAN Configuration under Fabric Interconnect A.



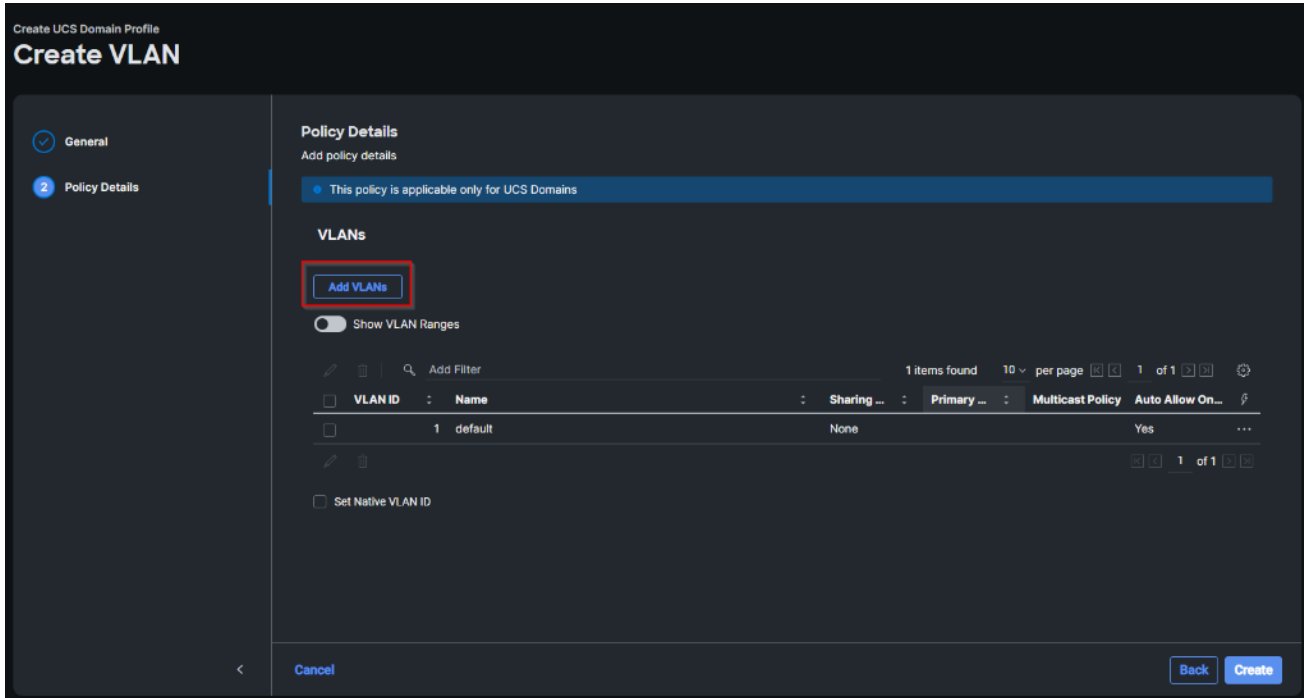
**Step 8.** In the pane on the right, click Create New.

**Step 9.** Verify correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L152-DMZ-VLAN). Click Next.

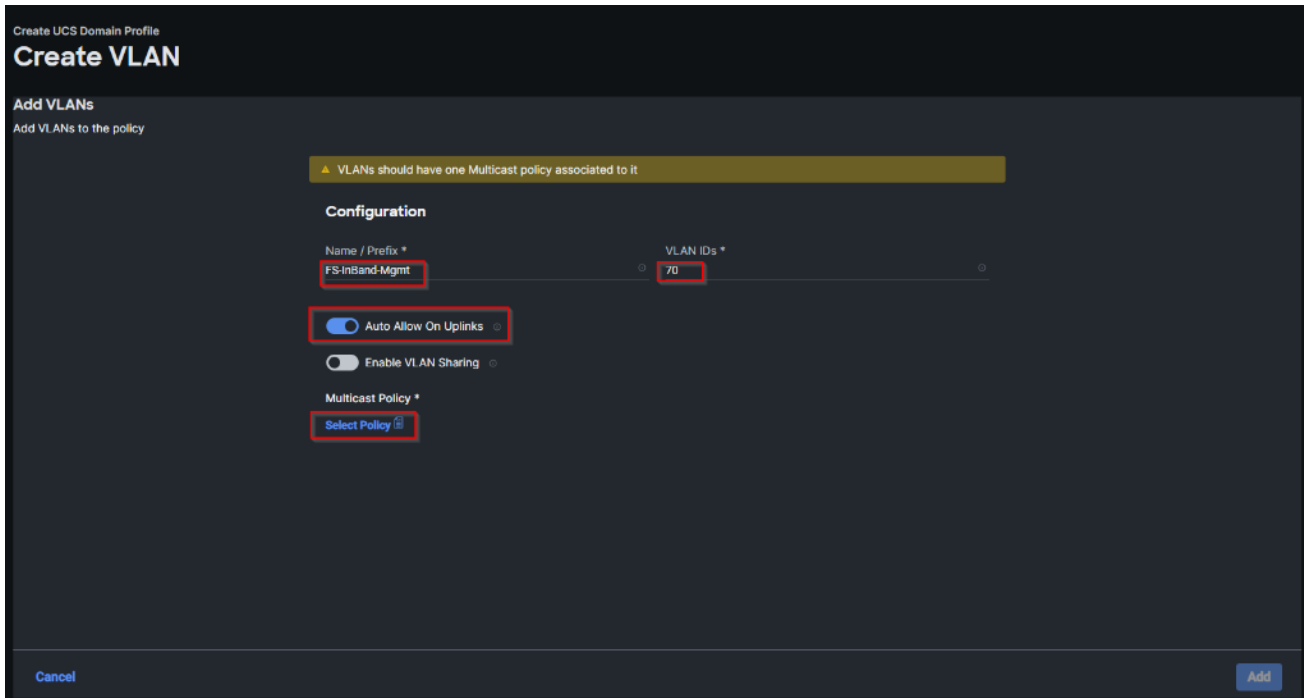


**Step 10.** Click Add VLANs.



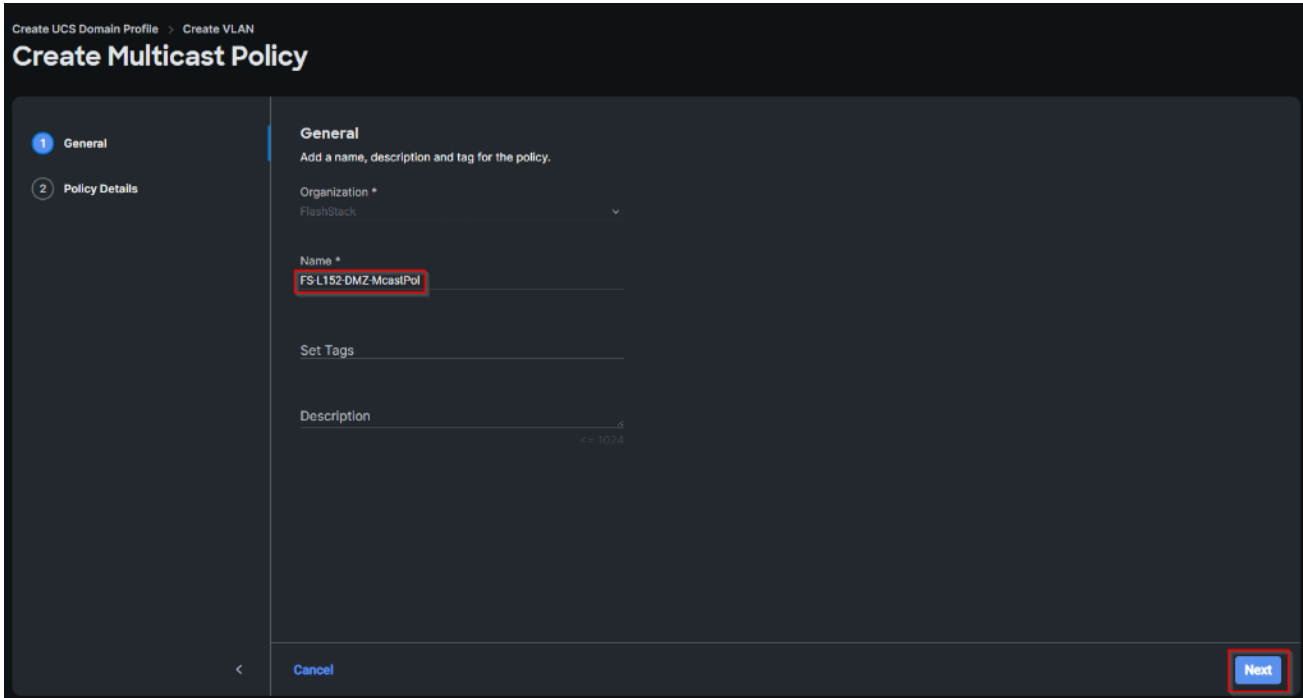


**Step 11.** Provide a name and VLAN ID for the VLAN from you list (for example, 70, 71, 72,73). Enable Auto Allow On Uplinks. To create the required Multicast policy, click Select Policy under Multicast\*.

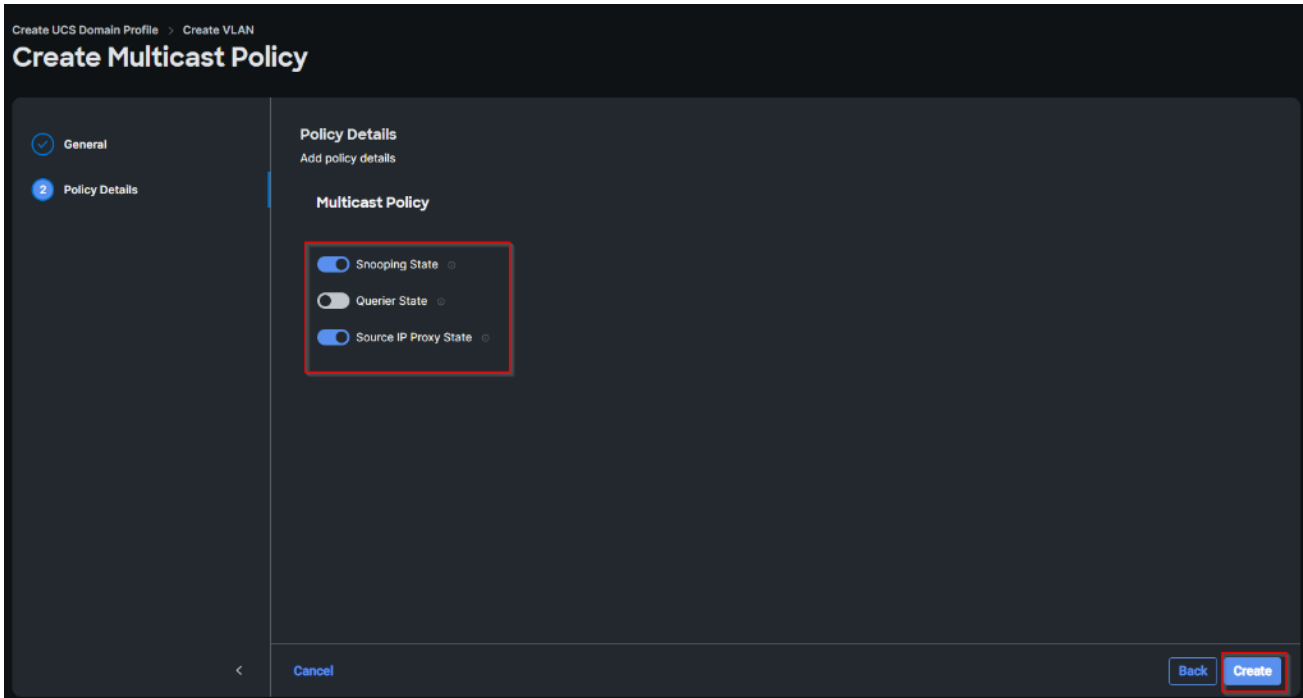


**Step 12.** In the window on the right, click Create New to create a new Multicast Policy.

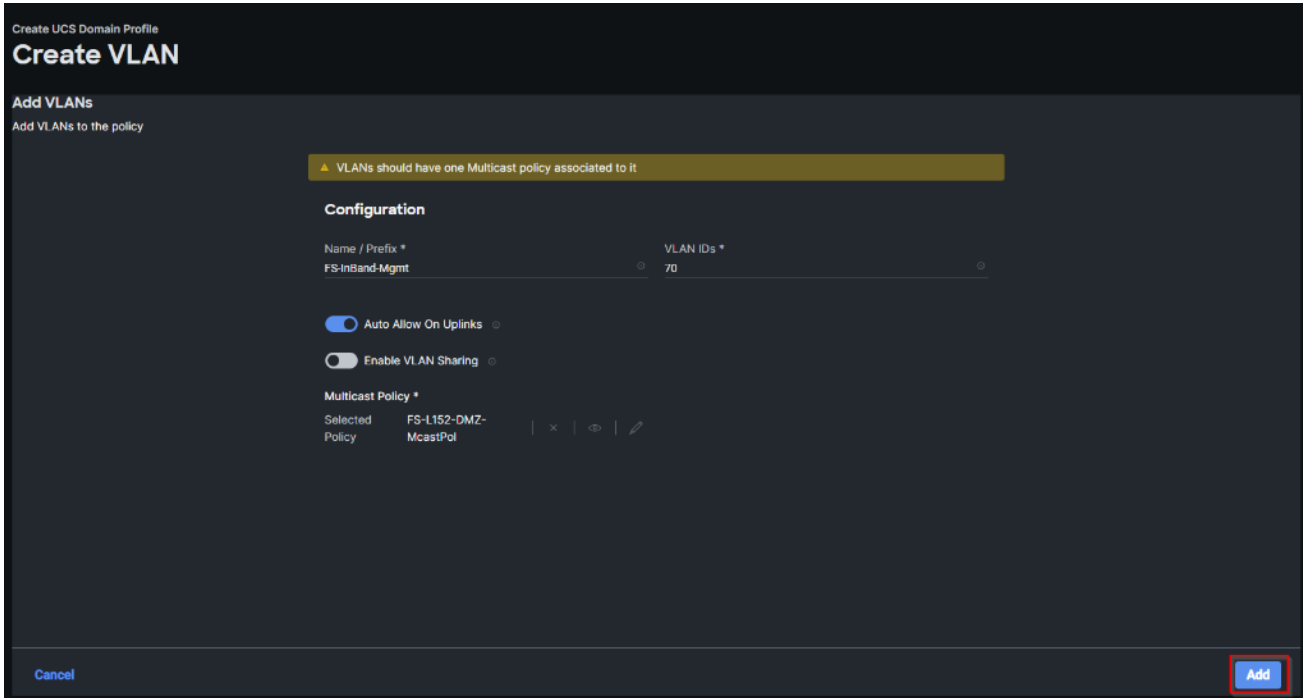
**Step 13.** Provide a Name for the Multicast Policy (for example, FS-L152-DMZ-McastPol). Provide optional Description and click Next.



**Step 14.** Leave defaults selected and click Create.

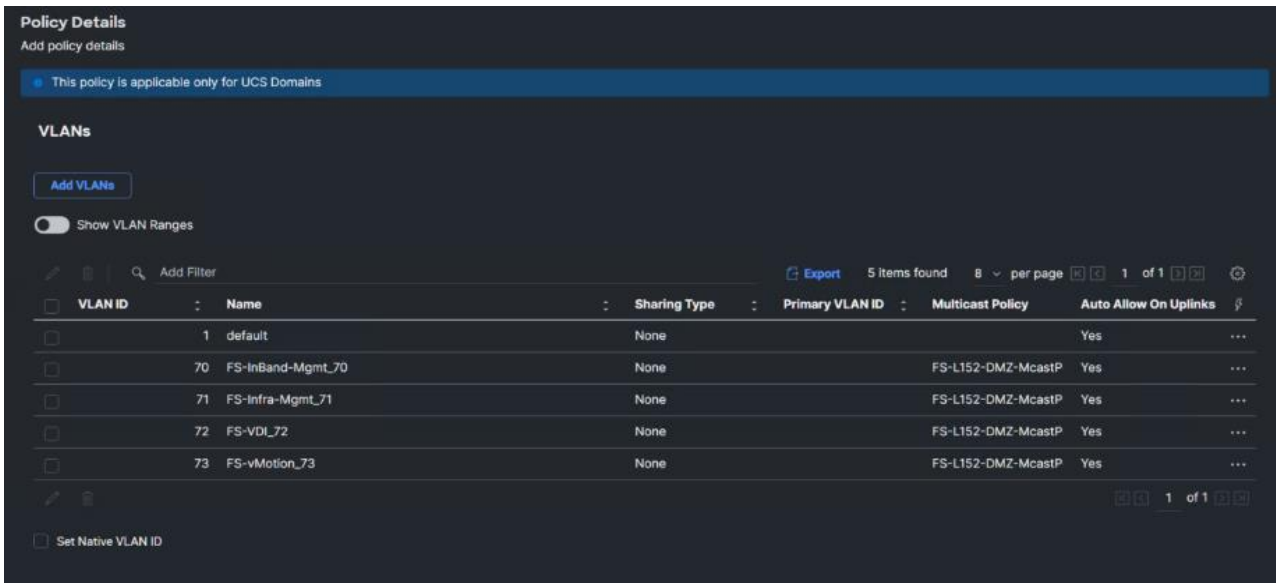


**Step 15.** Click Add to add the VLAN.



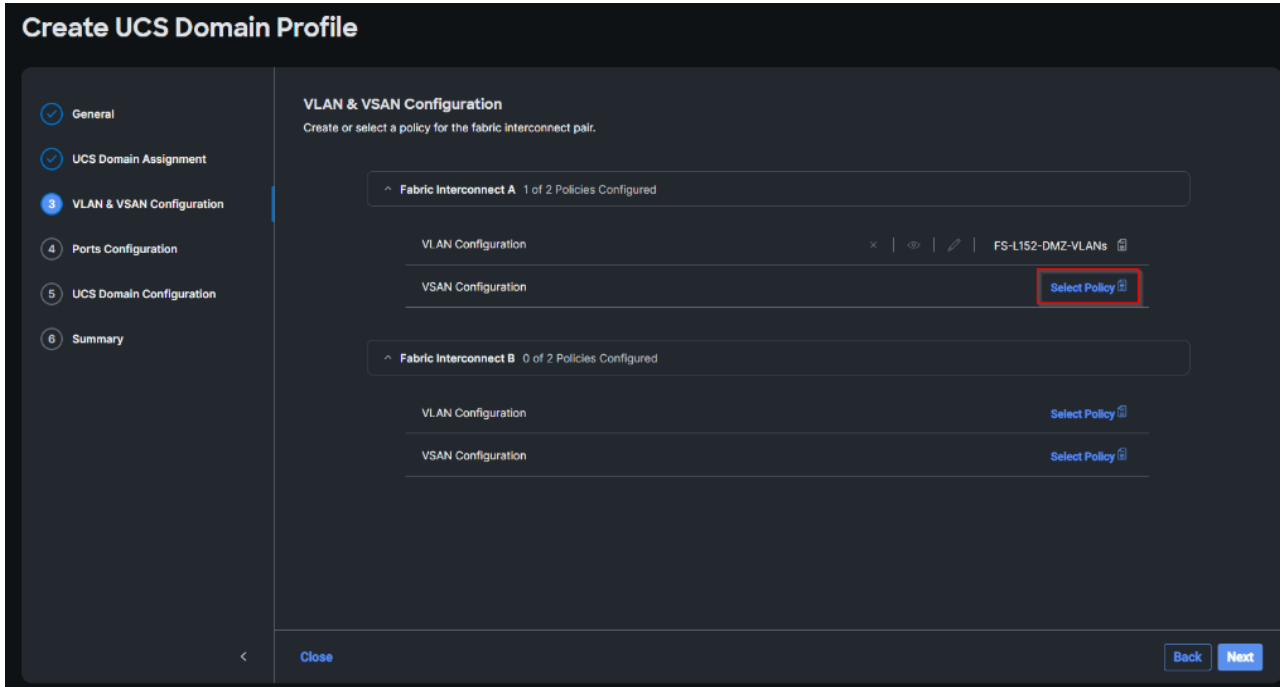
**Step 16.** Add the remaining VLANs from you list by clicking Add VLANs and entering the VLANs one by one. Reuse the previously created multicast policy for all the VLANs.

The VLANs created during this validation are shown below:

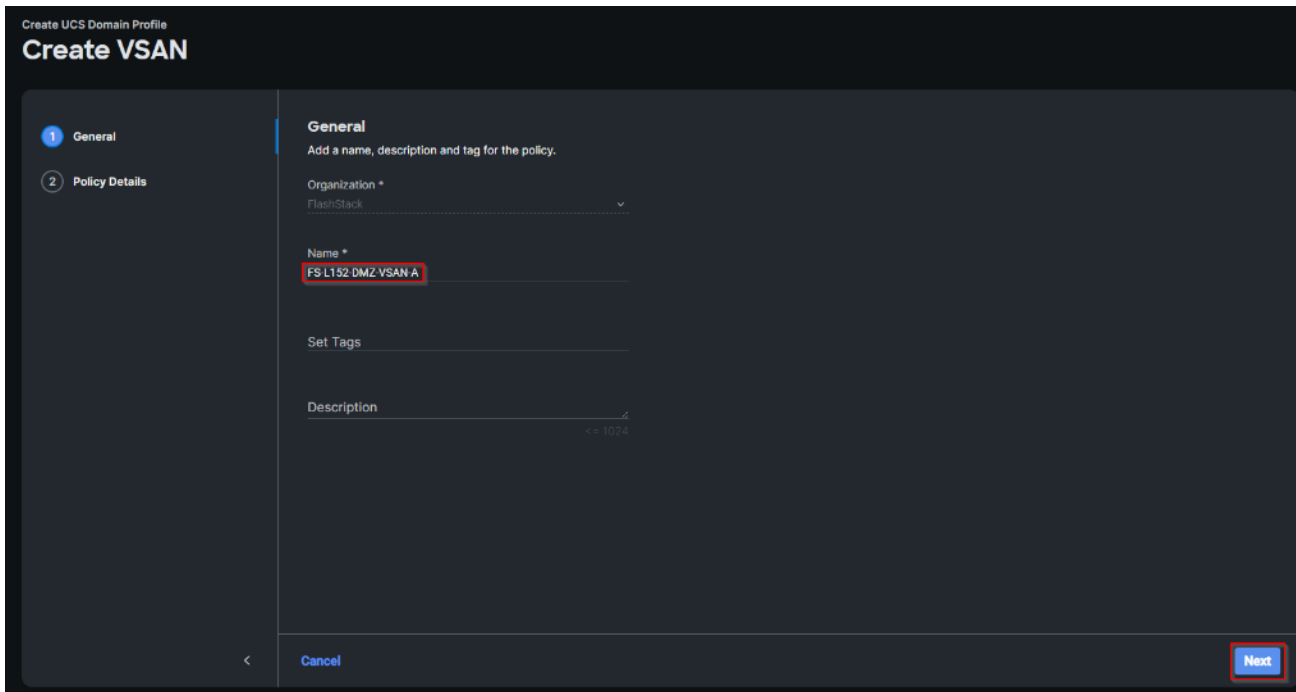


**Note:** A VSAN policy is only needed when configuring Fibre Channel and can be skipped when configuring IP-only storage access.

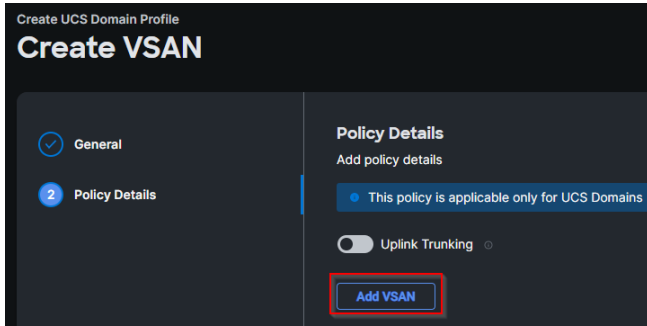
**Step 17.** Click Select Policy next to VSAN Configuration under Fabric Interconnect A. Click Create New.



**Step 18.** Verify correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L152-DMZ-VSAN-A). Click Next.



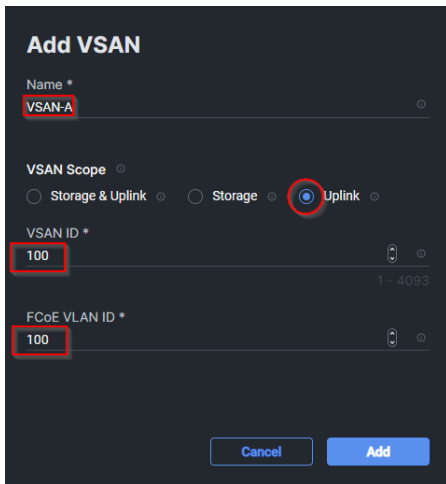
**Step 19.** Click Add VSAN.



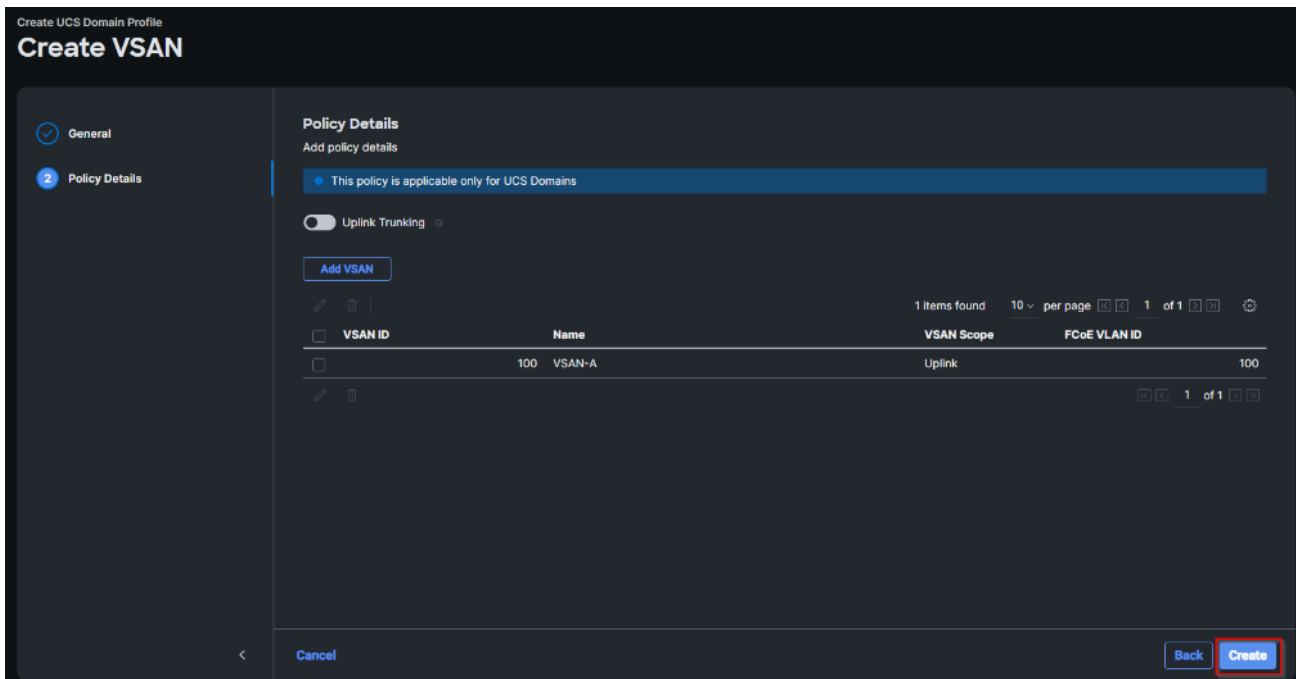
**Step 20.** Provide a name (for example, VSAN-A), VSAN ID (for example, 100), and associated Fibre Channel over Ethernet (FCoE) VLAN ID (for example, 100) for VSAN A.

**Step 21.** Set VLAN Scope as Uplink.

**Step 22.** Click Add.

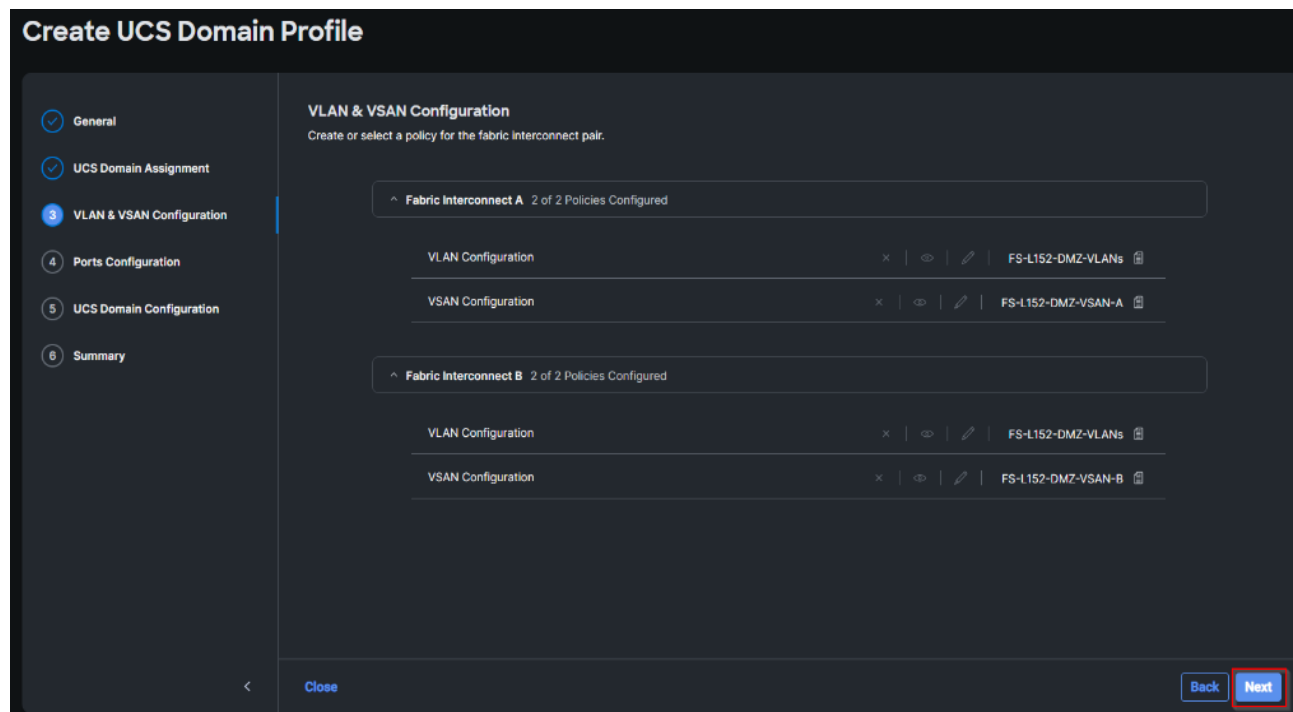


**Step 23.** Click Create to finish creating VSAN policy for fabric A.



**Step 24.** Repeat steps 7 - 23 for fabric interconnect B assigning the VLAN policy created previously and creating a new VSAN policy for VSAN-B. Name the policy to identify the SAN-B configuration (for example, FS-L152-DMZ-VSAN-B) and use appropriate VSAN and FCoE VLAN (for example, 101).

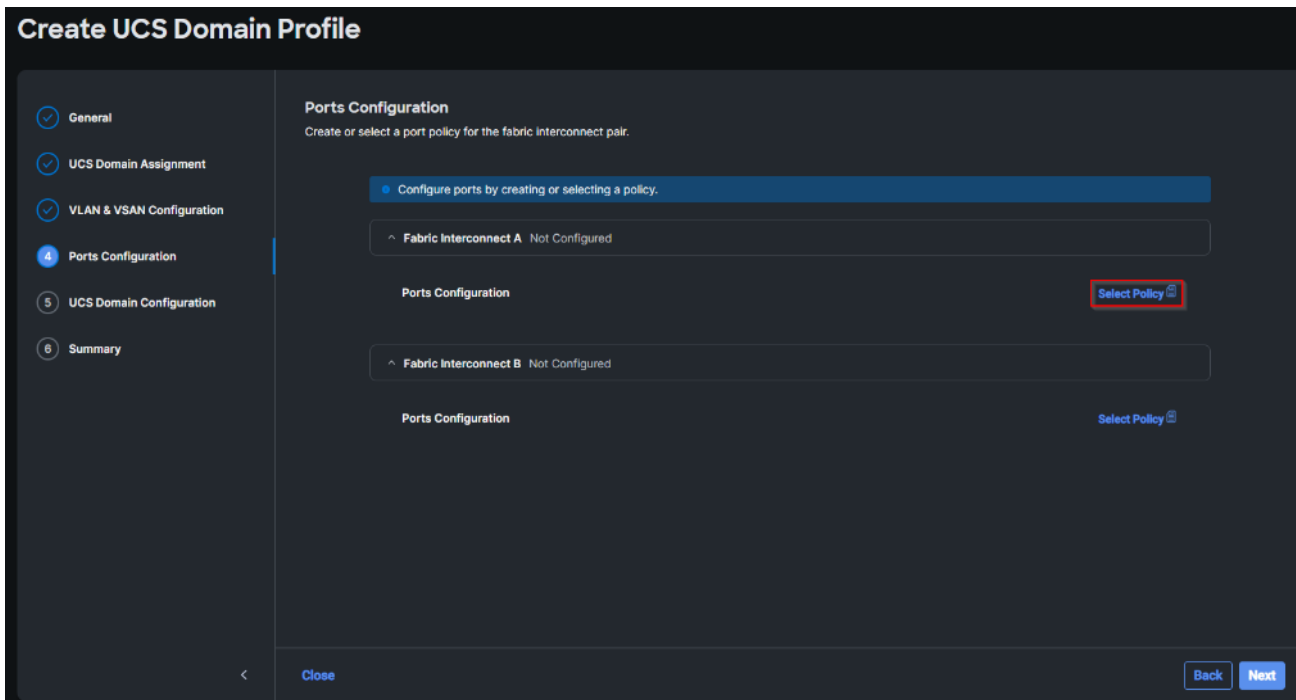
**Step 25.** Verify that a common VLAN policy and two unique VSAN policies are associated with the two fabric interconnects. Click Next.



**Step 26.** On the Ports Configuration page, attach port policies for each switch to the UCS Domain Profile.

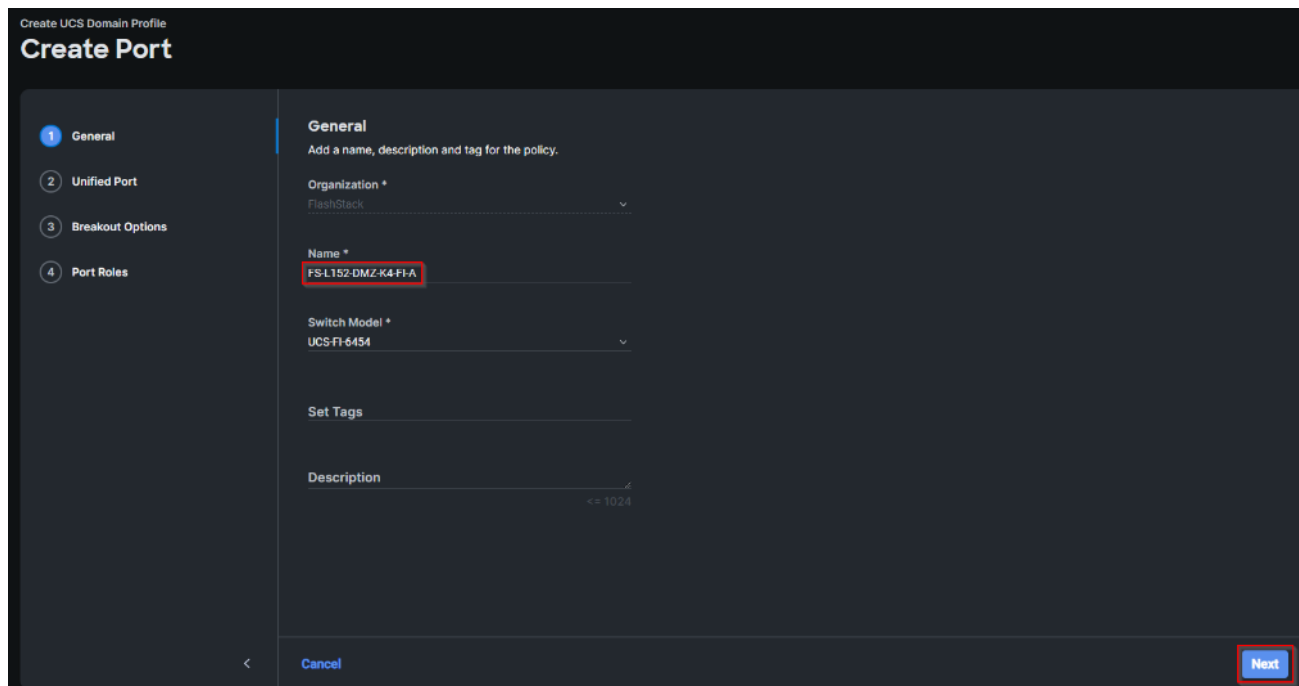
**Note:** Use two separate port policies for the fabric interconnects. Using separate policies provide flexibility when port configuration (port numbers or speed) differs between the two FIs. When configuring Fibre Channel, two port policies are required because each fabric interconnect uses unique Fibre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

**Step 27.** Click Select Policy for Fabric Interconnect A.



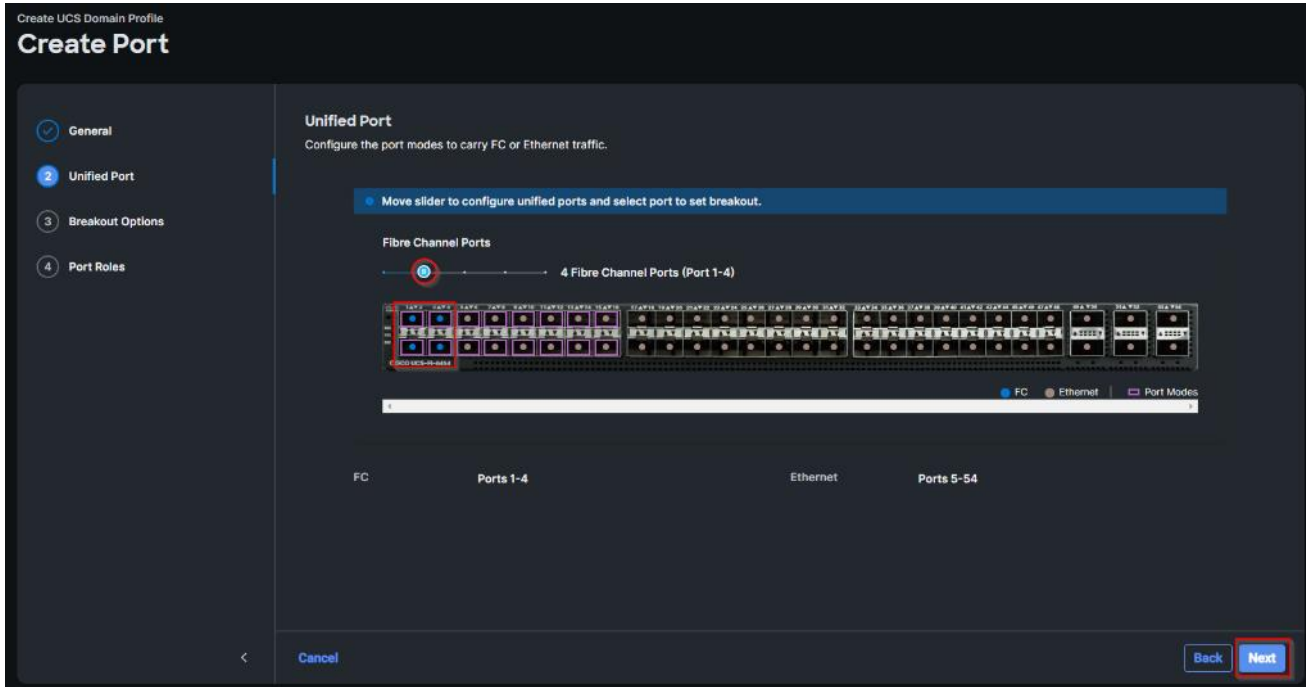
**Step 28.** Click Create New.

**Step 29.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L152-DMZ-K4-FI-A). Click Next.



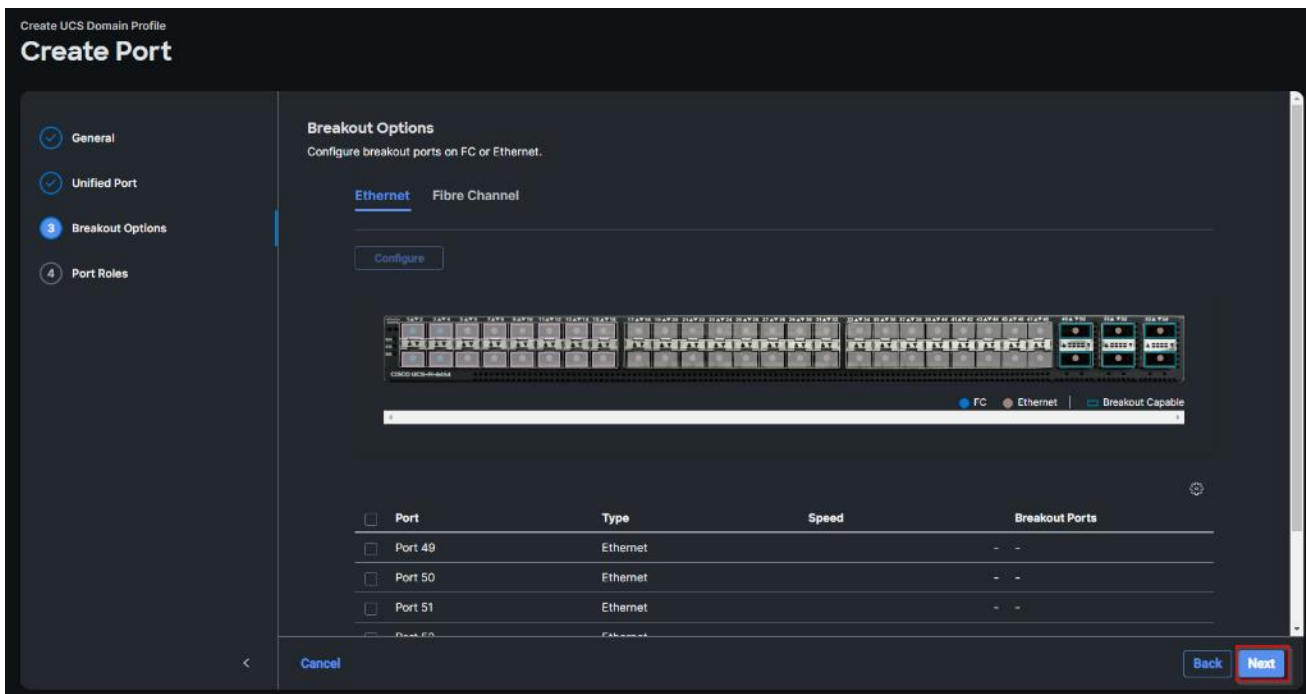
**Step 30.** Move the slider to set up unified ports. In this deployment, the first four ports were selected as Fibre Channel ports. Click Next.



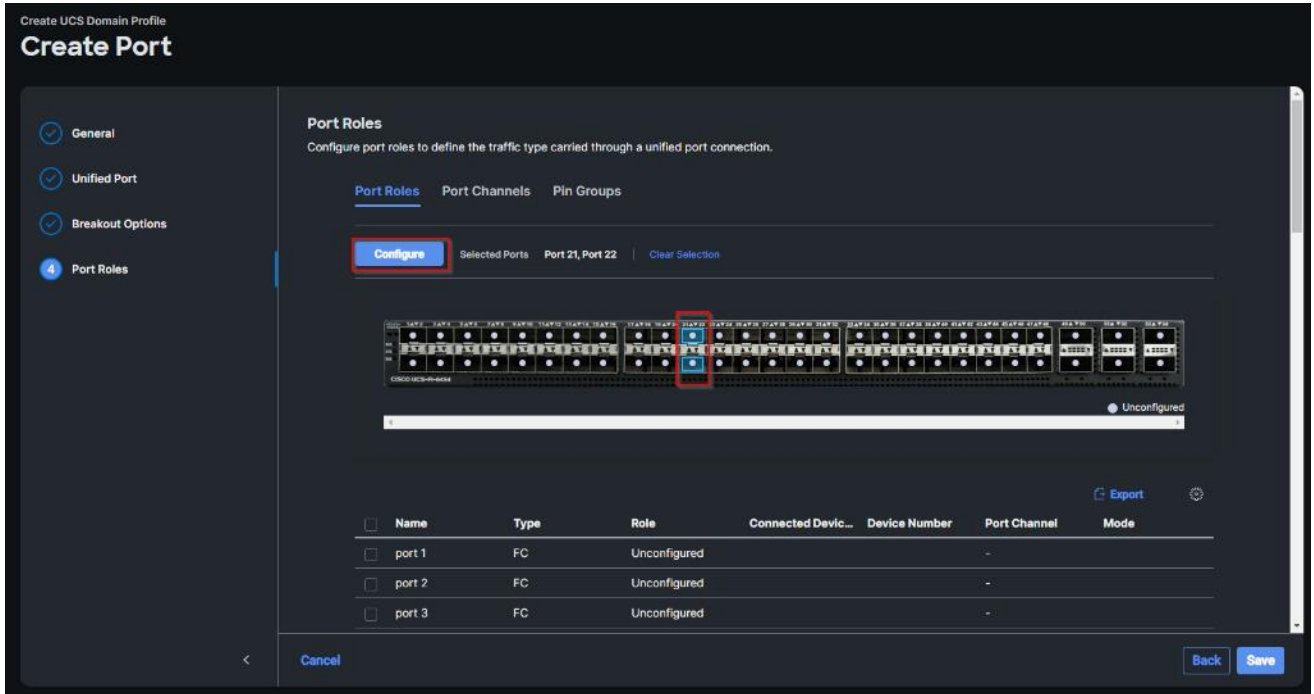


**Step 31.** On the breakout Options page click Next.

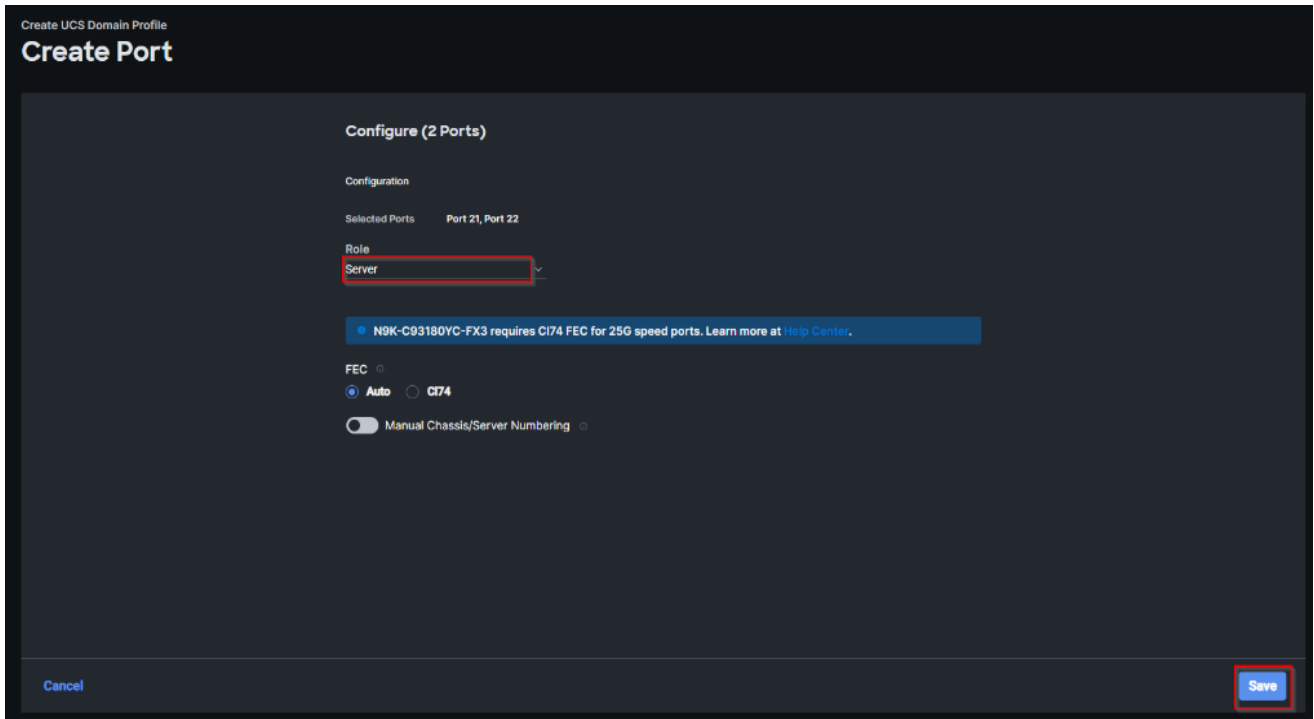
**Note:** No Ethernet/Fibre Channel breakouts were used in this validation.



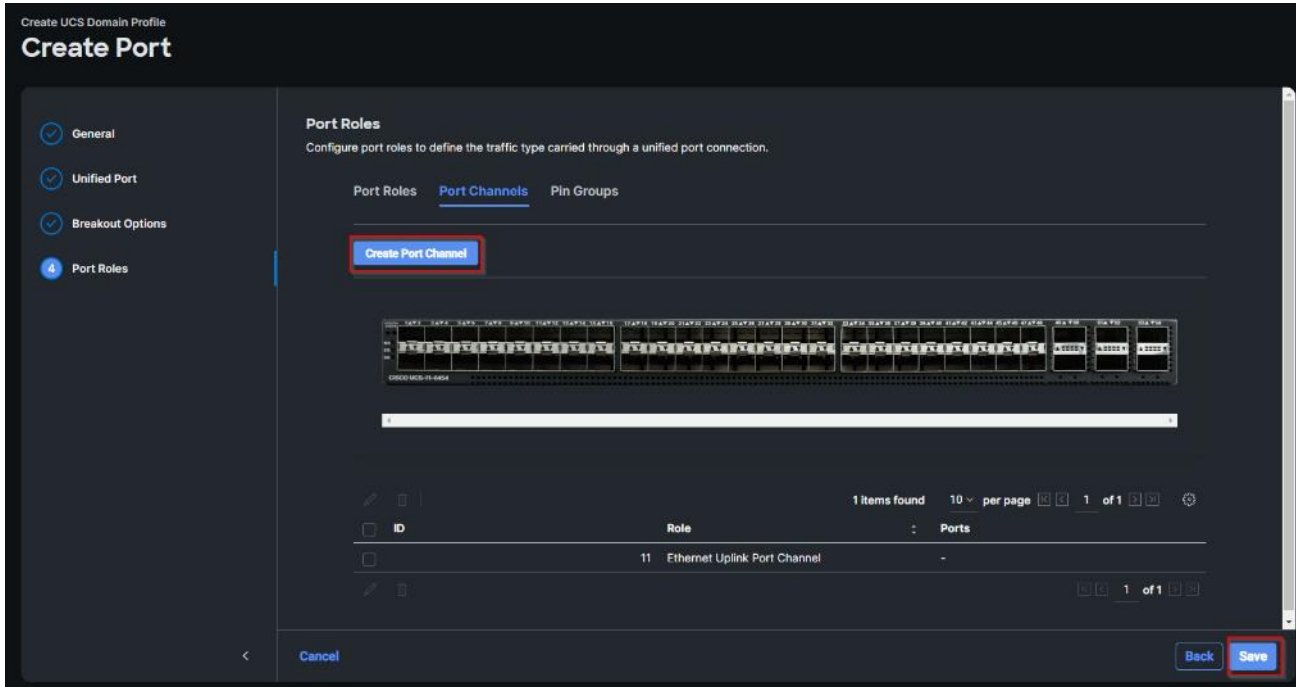
**Step 32.** Select the ports that need to be configured as server ports by clicking the ports in the graphics (or select from the list below the graphic). When all ports are selected, click Configure.



**Step 33.** From the drop-down list, select Server as the role. Click Save.



**Step 34.** Configure the Ethernet uplink port channel by selecting the Port Channel in the main pane and then clicking Create Port Channel.

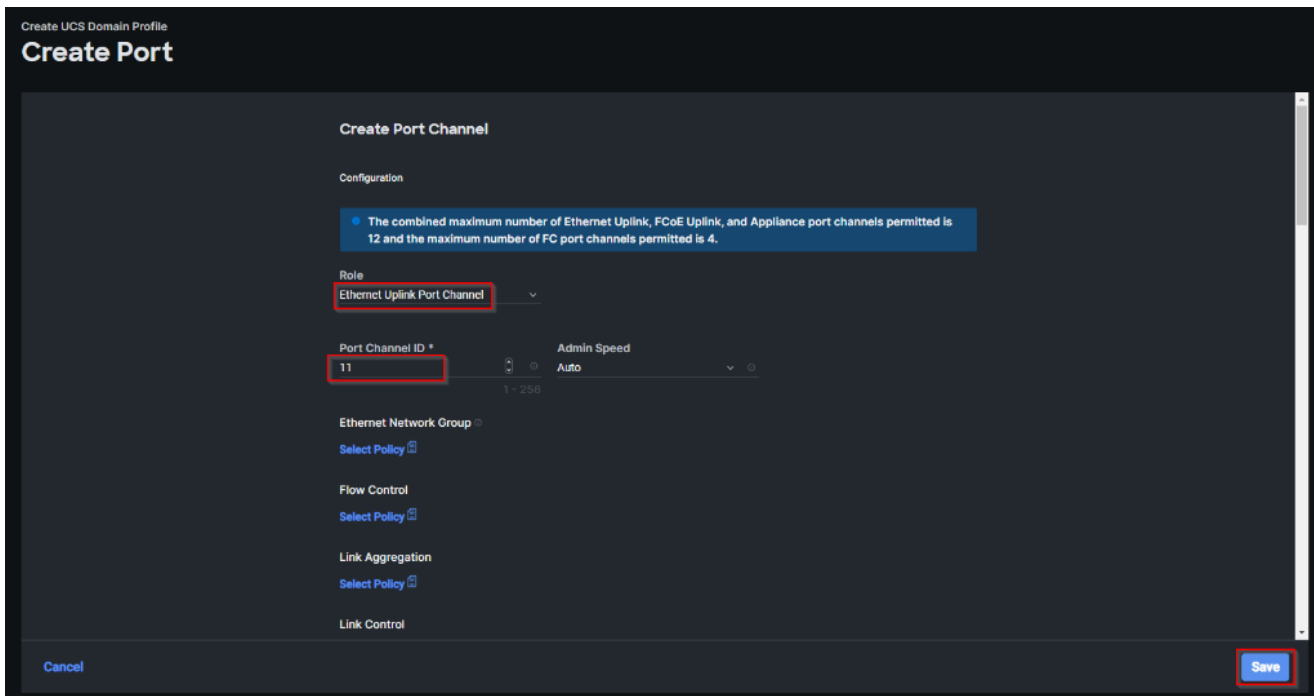


**Step 35.** Select Ethernet Uplink Port Channel as the role, provide a port-channel ID (for example, 11).

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

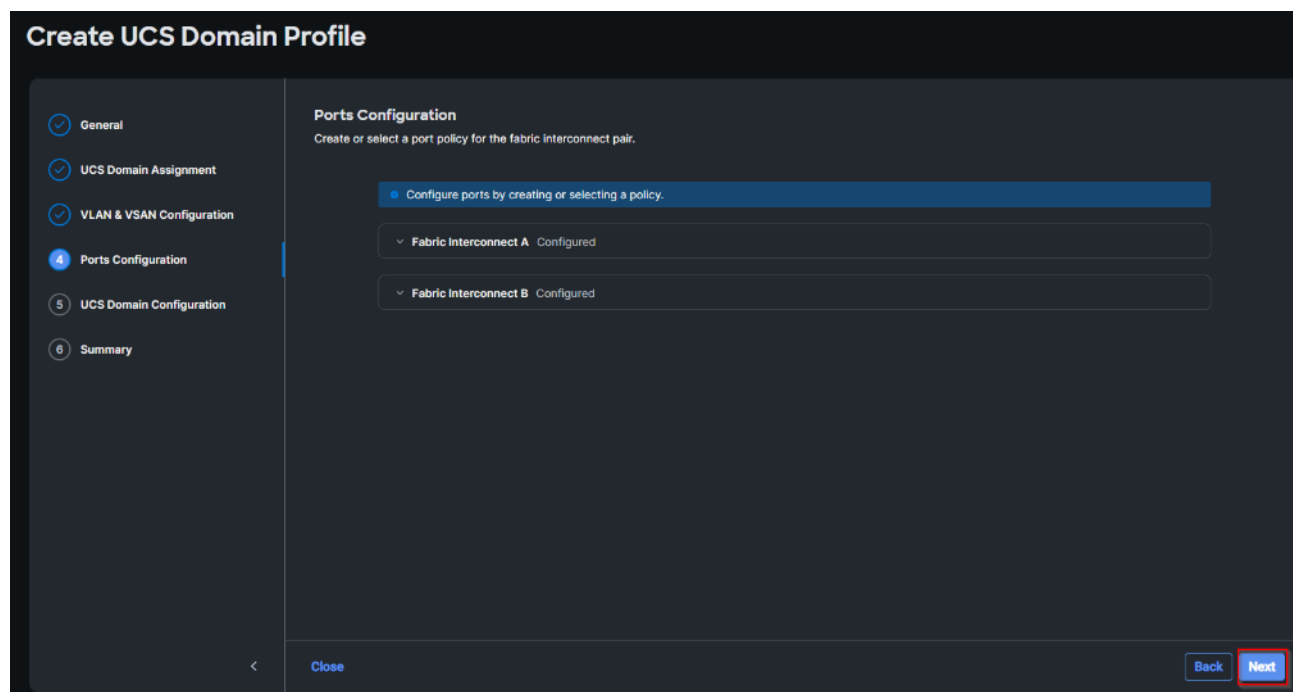
**Step 37.** Click Save.



**Step 38.** Repeat steps 27 - 37 to create the port policy for Fabric Interconnect B. Use the following values for various parameters:

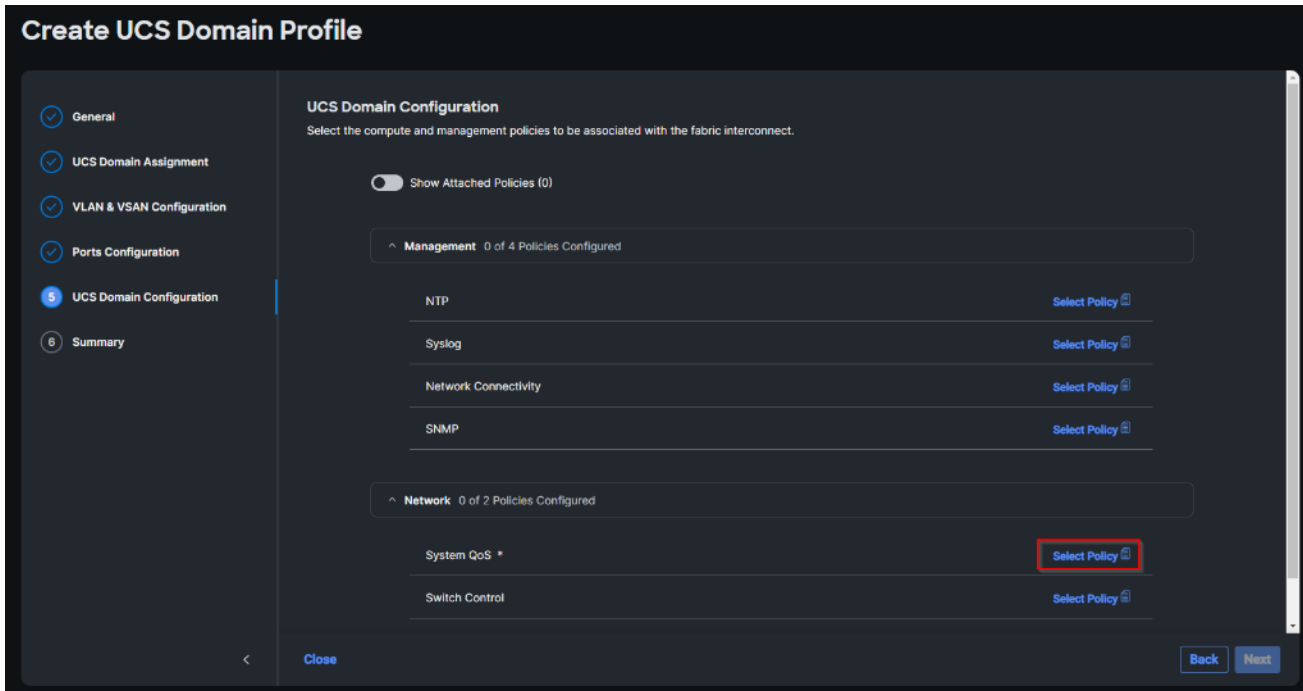
- Name of the port policy: FS-L152-DMZ-K4-FI-B
- Ethernet port-Channel ID: 12

**Step 39.** When the port configuration for both fabric interconnects is complete and looks good, click Next.

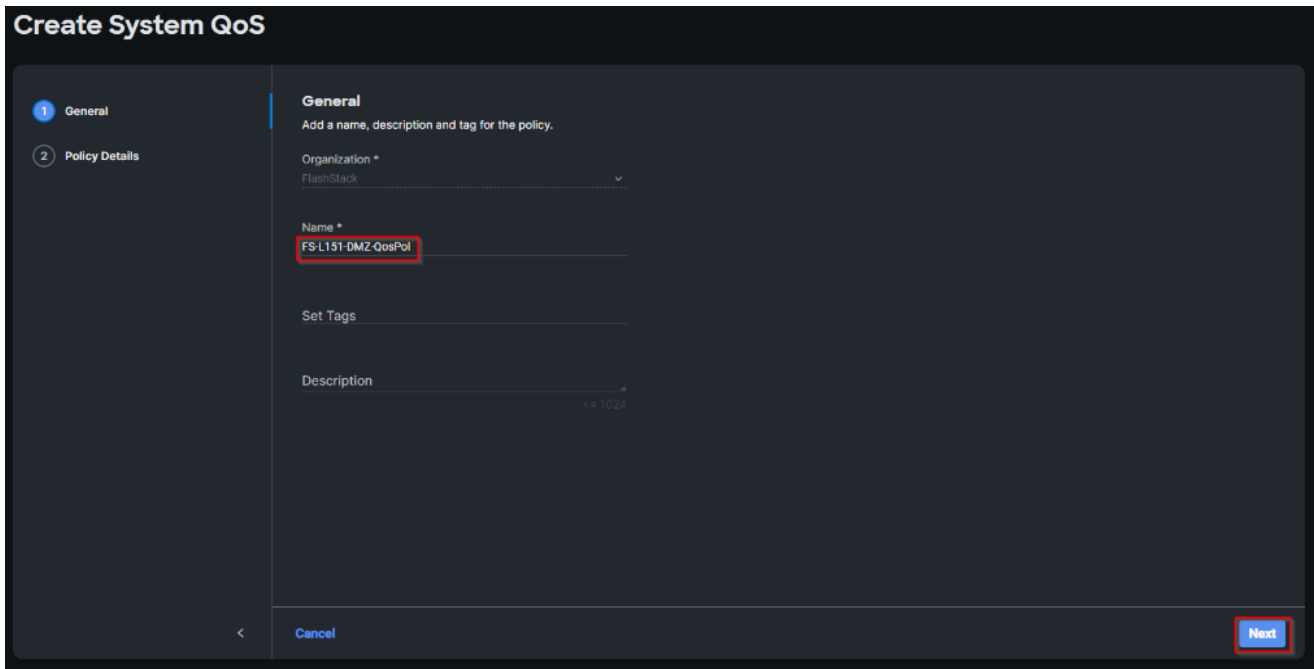


**Step 40.** Under UCS domain configuration, additional policies can be configured to setup NTP, Syslog, DNS settings, SNMP, QoS and UCS operating mode (end host or switch mode). For this deployment, System QoS will be configured.

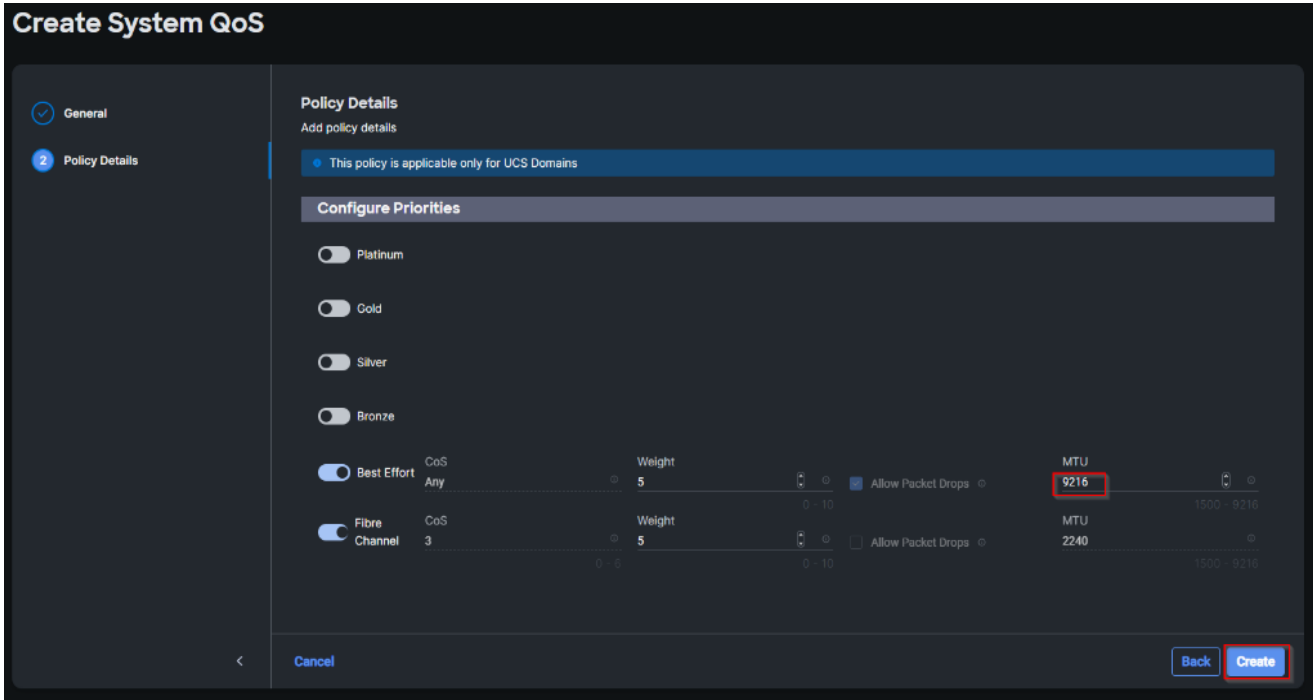
**Step 41.** Click Select Policy next to System QoS\* and click Create New to define the System QOS policy.



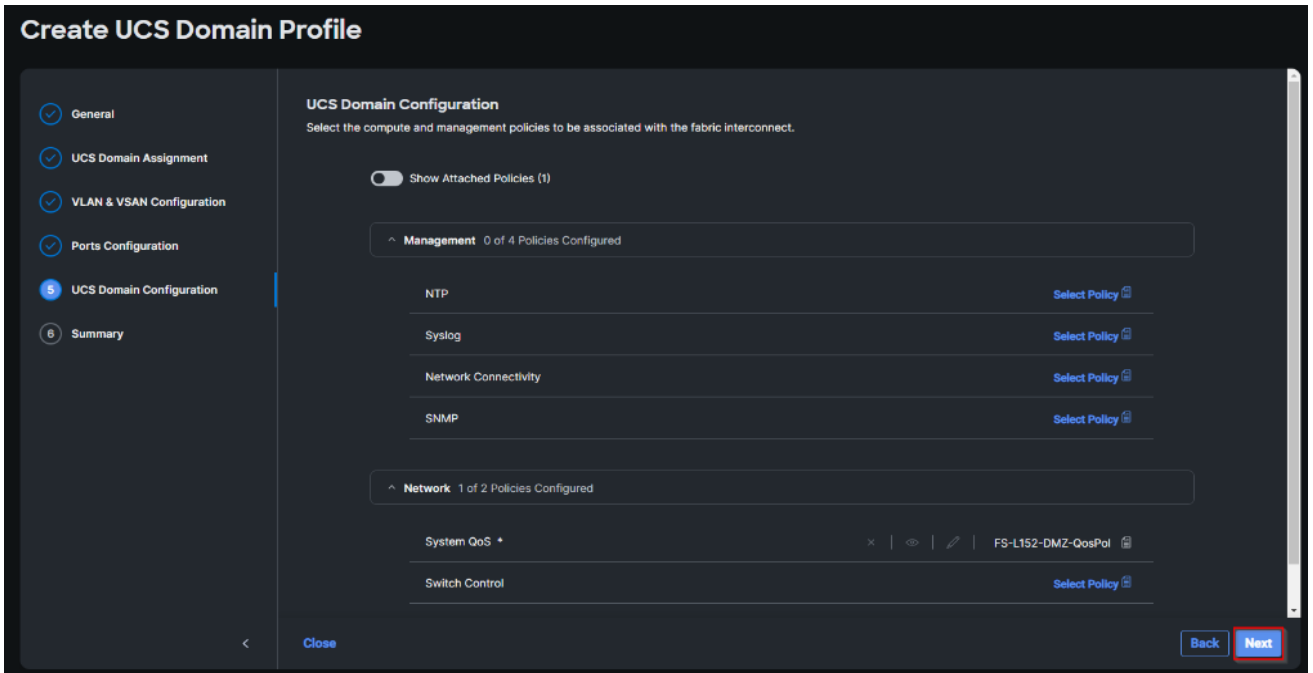
**Step 42.** Verify correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L152-DMZ-QoSPol). Click Next.



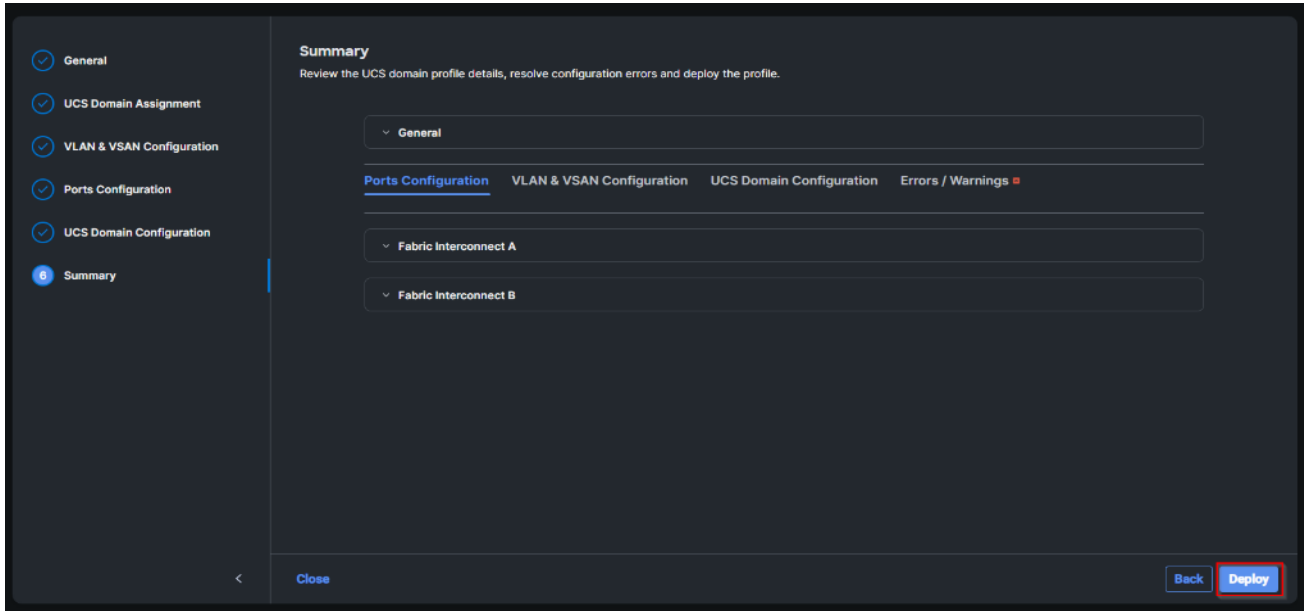
**Step 43.** Change the MTU for Best Effort class to 9216. Keep the rest default selections. Click Create.



Step 44. Click Next.



Step 45. From the UCS domain profile Summary view, Verify all the settings including the fabric interconnect settings, by expanding the settings and make sure that the configuration is correct. Click Deploy.



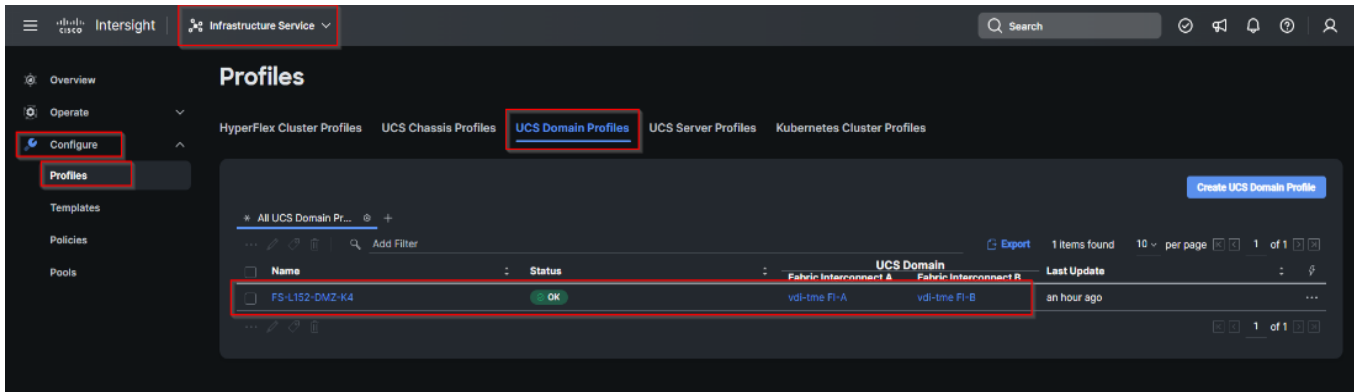
The system will take some time to validate and configure the settings on the fabric interconnects. Log into the console servers to see when the Cisco UCS fabric interconnects have finished configuration and are successfully rebooted.

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

It takes a while to discover the blades for the first time. Cisco Intersight provides an ability to view the progress in the Requests page:

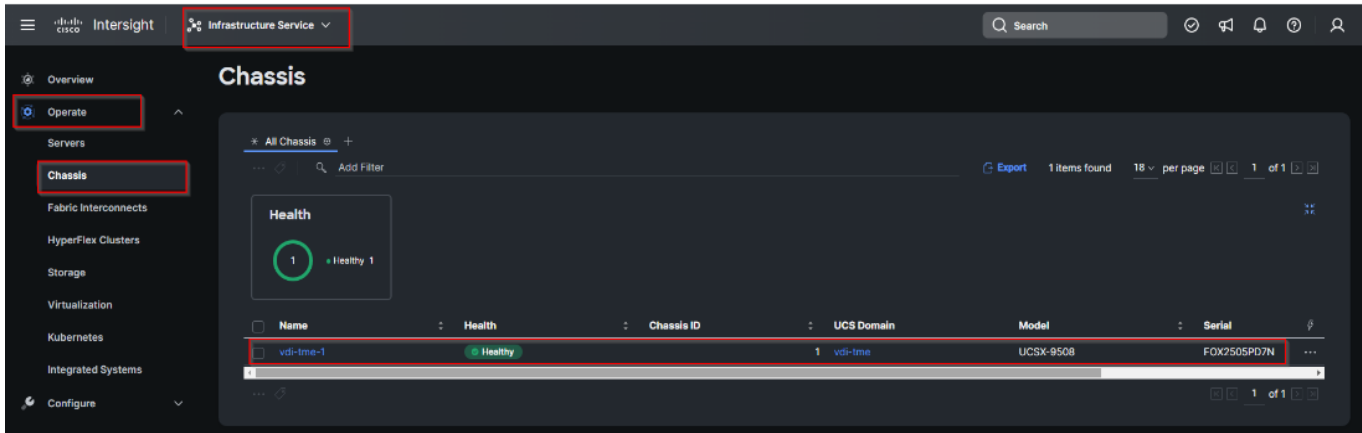


**Step 46.** From the Service Selector drop-down list, select Infrastructure Service. Navigate to Configure > Profiles, select UCS Domain Profiles, verify that the domain profile has been successfully deployed.

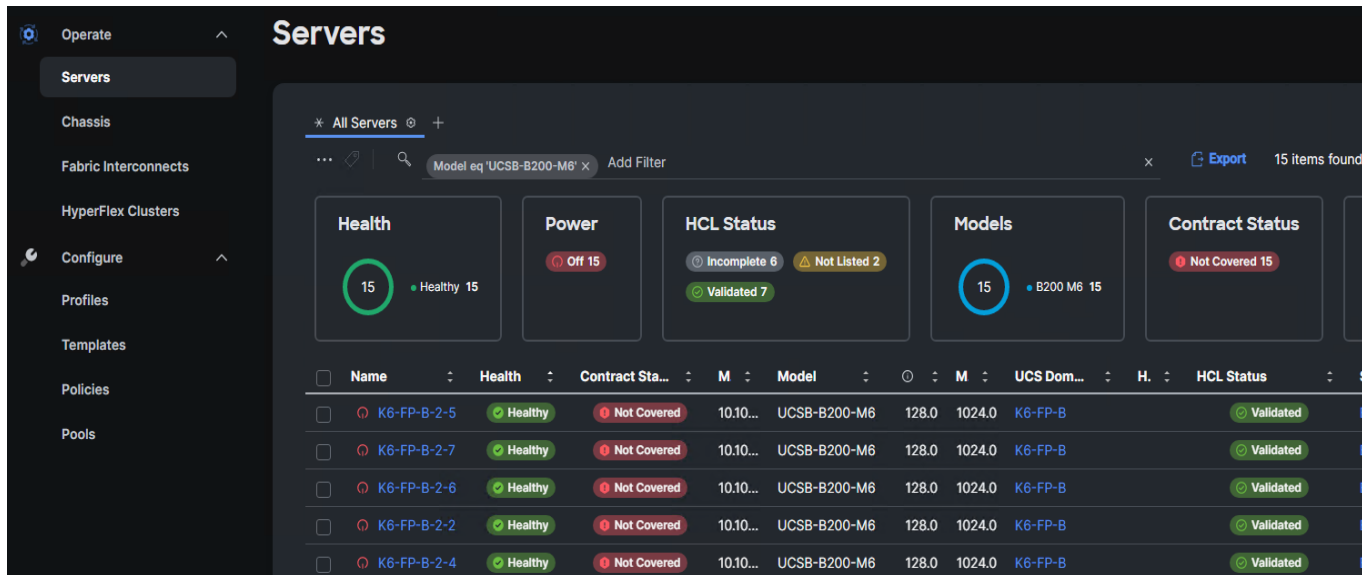


**Step 47.** From the Service Selector drop-down list, select Infrastructure Service. Navigate to Operate > Chassis, verify that the chassis has been discovered.





**Step 48.** From the Service Selector drop-down list, select Infrastructure Service. Navigate to Operate > Servers, verify that the servers have been successfully discovered.

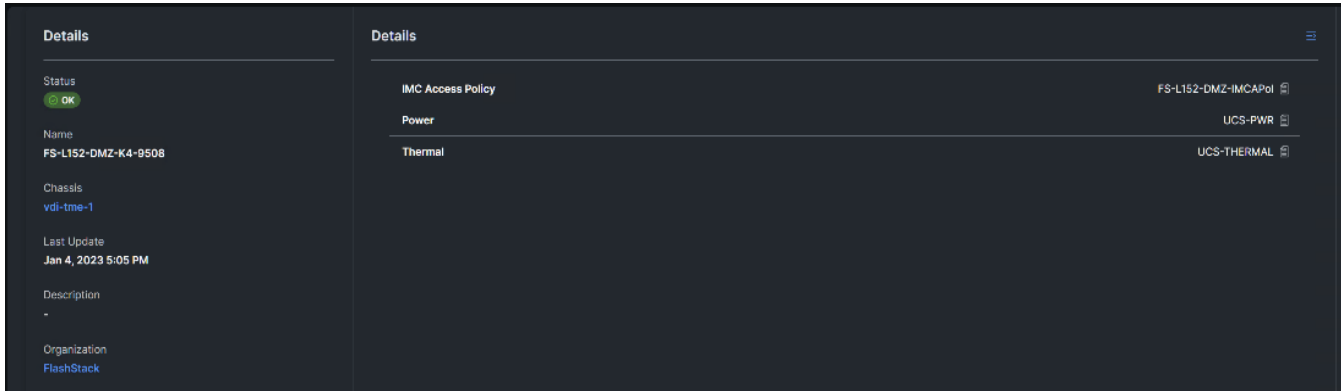


### Configure Cisco UCS Chassis Profile

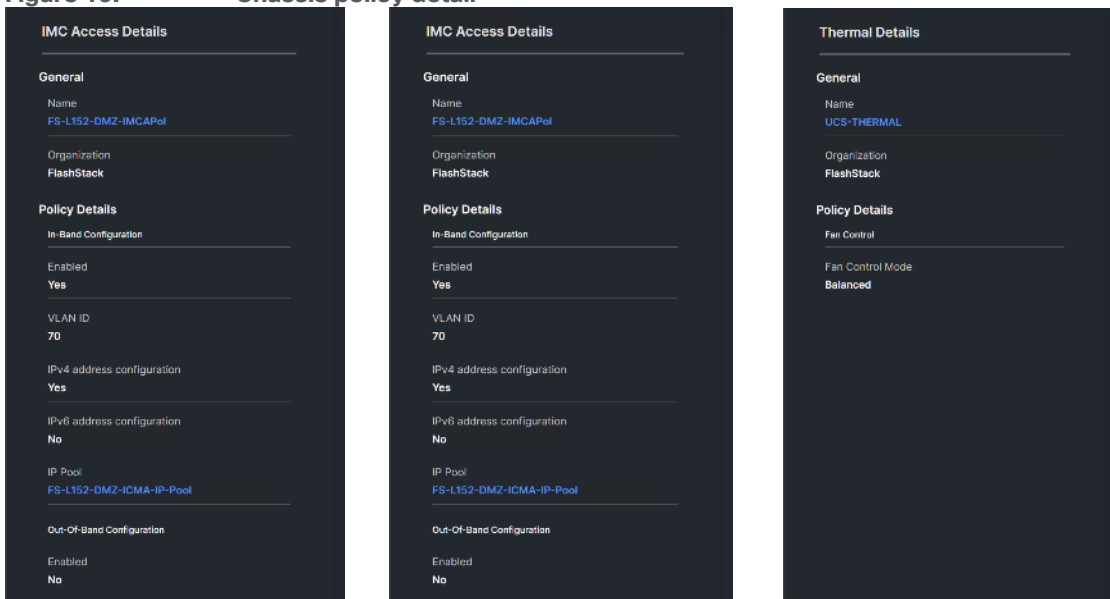
Cisco UCS Chassis profile in Cisco Intersight allows you to configure various parameters for the chassis, including:

- 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, chassis profile was created and attached to the chassis with the settings shown in [Figure 19](#).



**Figure 19.** Chassis policy detail



## Configure Server Profiles

### Configure Server Profile Template

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 blade servers and Cisco UCS B200 M6 compute nodes.

### Procedure 1. Create vNIC and vHBA Placement for the Server Profile Template

In this deployment, four vNICs and two vHBAs are configured. These devices are manually placed as listed in [Table 5](#).

**Table 5.** vHBA and vNIC placement for FC connected storage

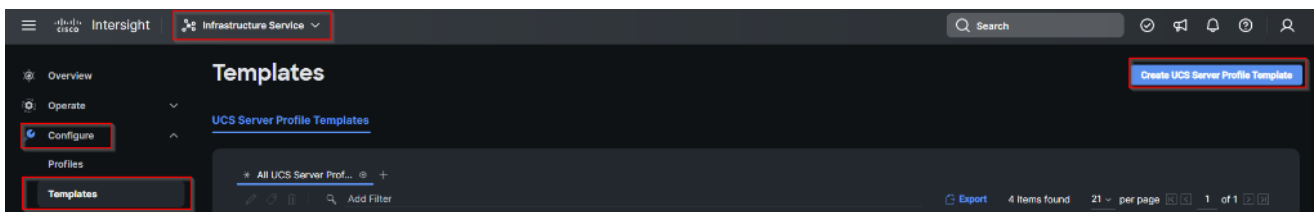
vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-A	MLOM	A	0

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

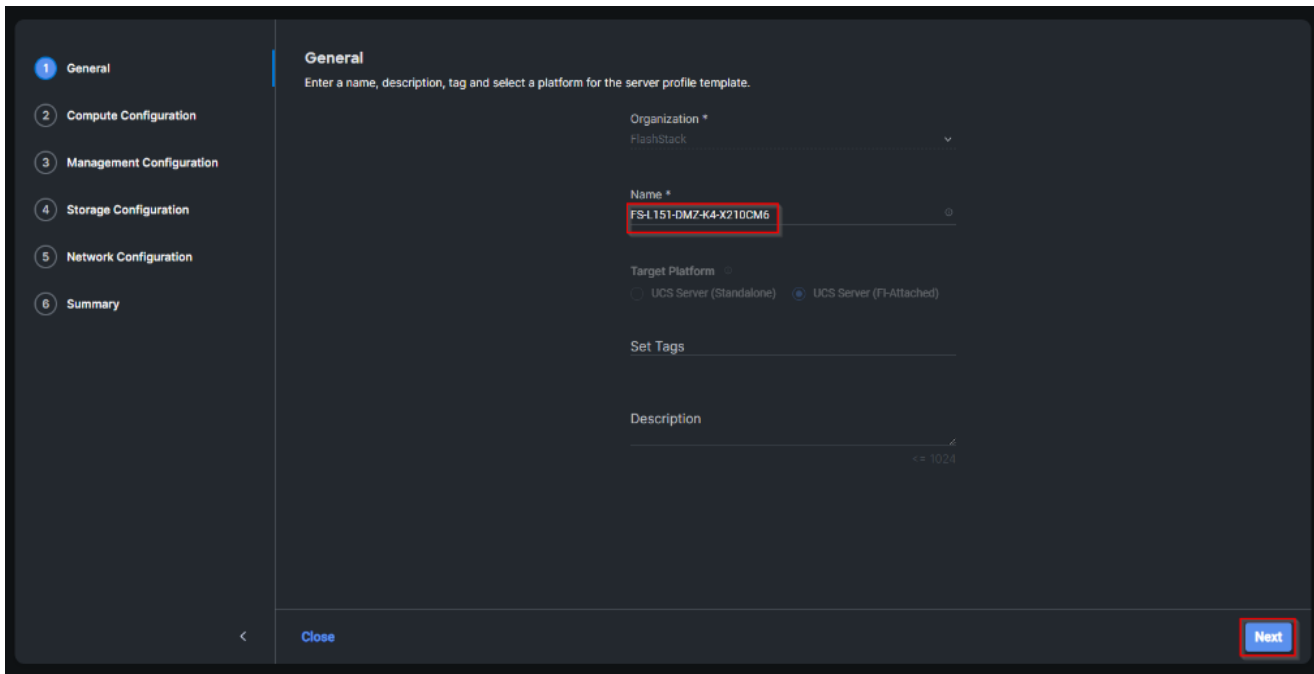
**Note:** Two vHBAs (vHBA-A and vHBA-B) are configured to support FC boot from SAN.

**Step 1.** Log into the Cisco Intersight portal as a user with account administrator role.

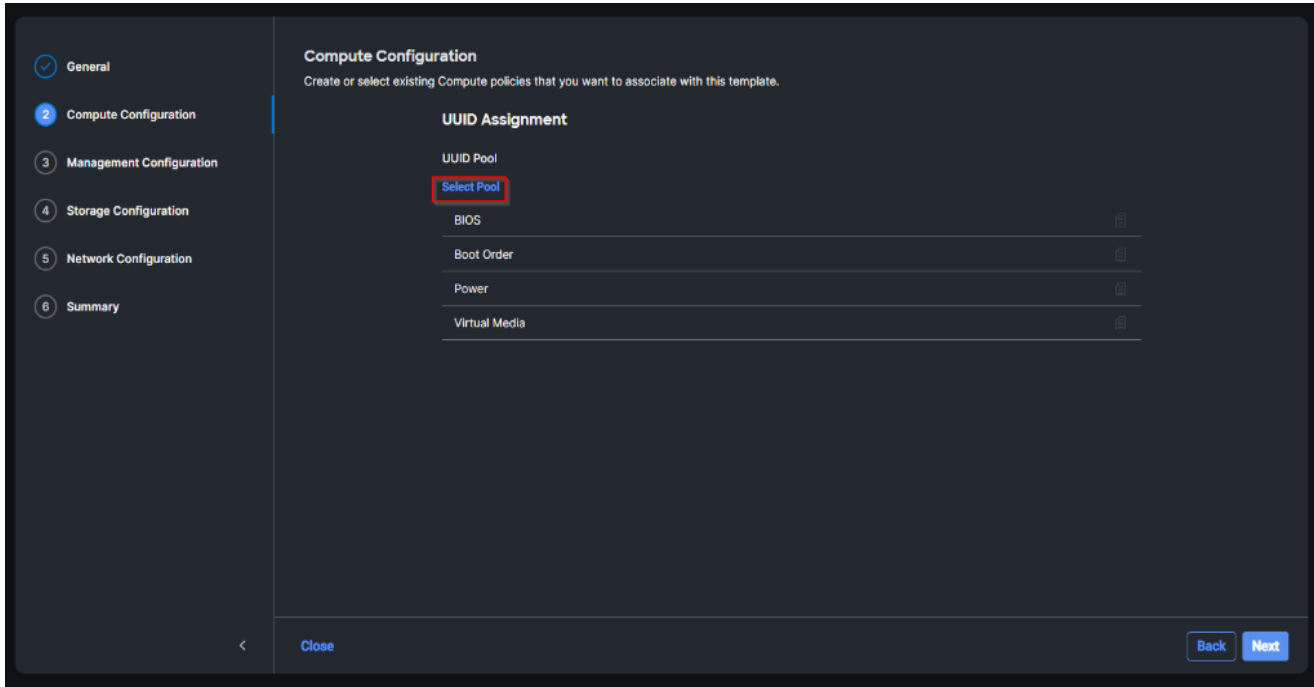
**Step 2.** Navigate to Configure > Templates and click Create UCS Server Profile Template.



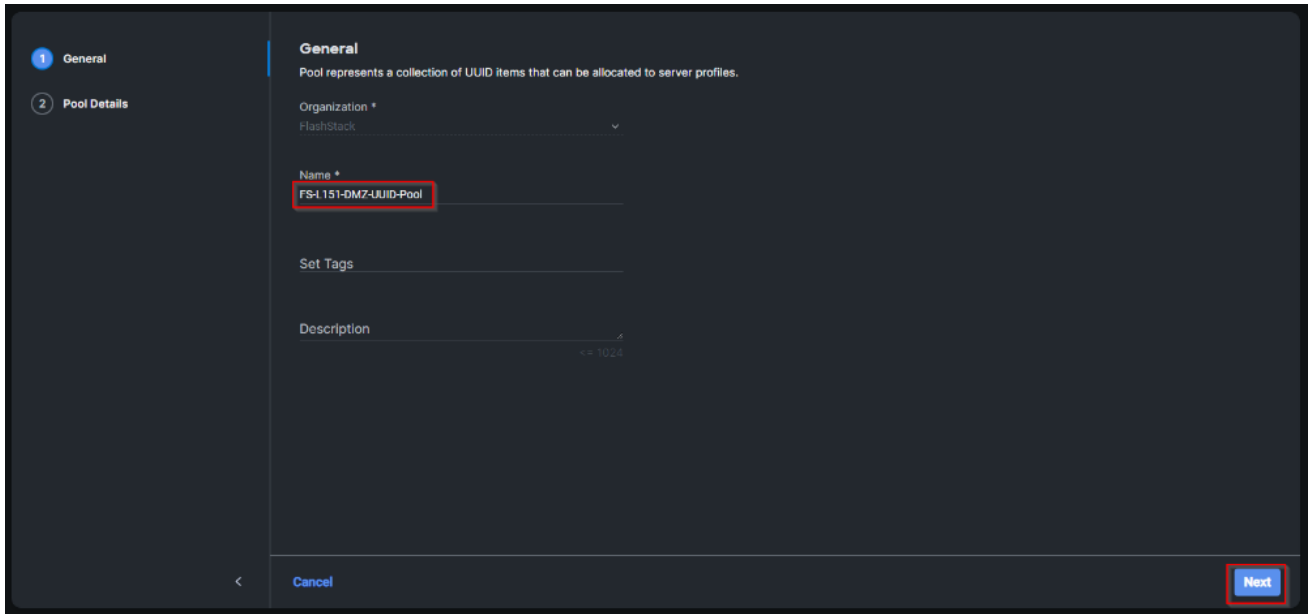
**Step 3.** Select the organization from the drop-down list. Provide a name for the server profile template (for example, FS-L151-DMZ-K4-B200 M6) for FI-Attached UCS Server. Click Next.



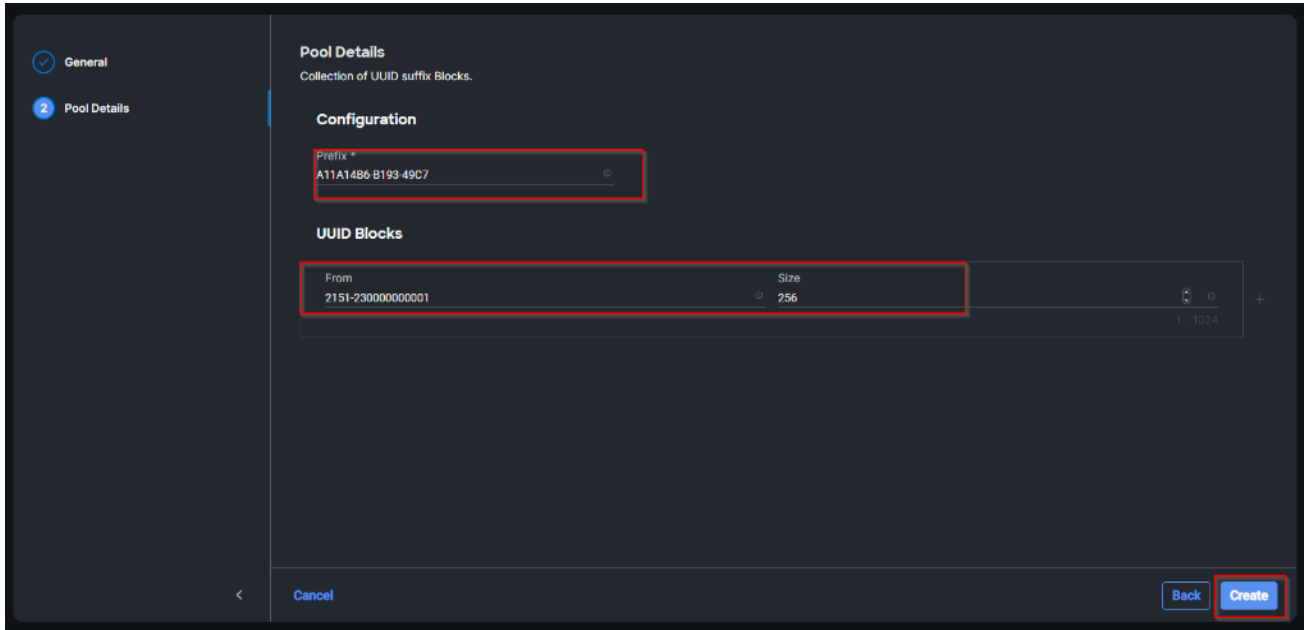
**Step 4.** Click Select Pool under UUID Pool and then click Create New.



**Step 5.** Verify correct organization is selected from the drop-down list and provide a name for the UUID Pool (for example, FS-L151-DMZ-UUID-Pool). Provide an optional Description and click Next.



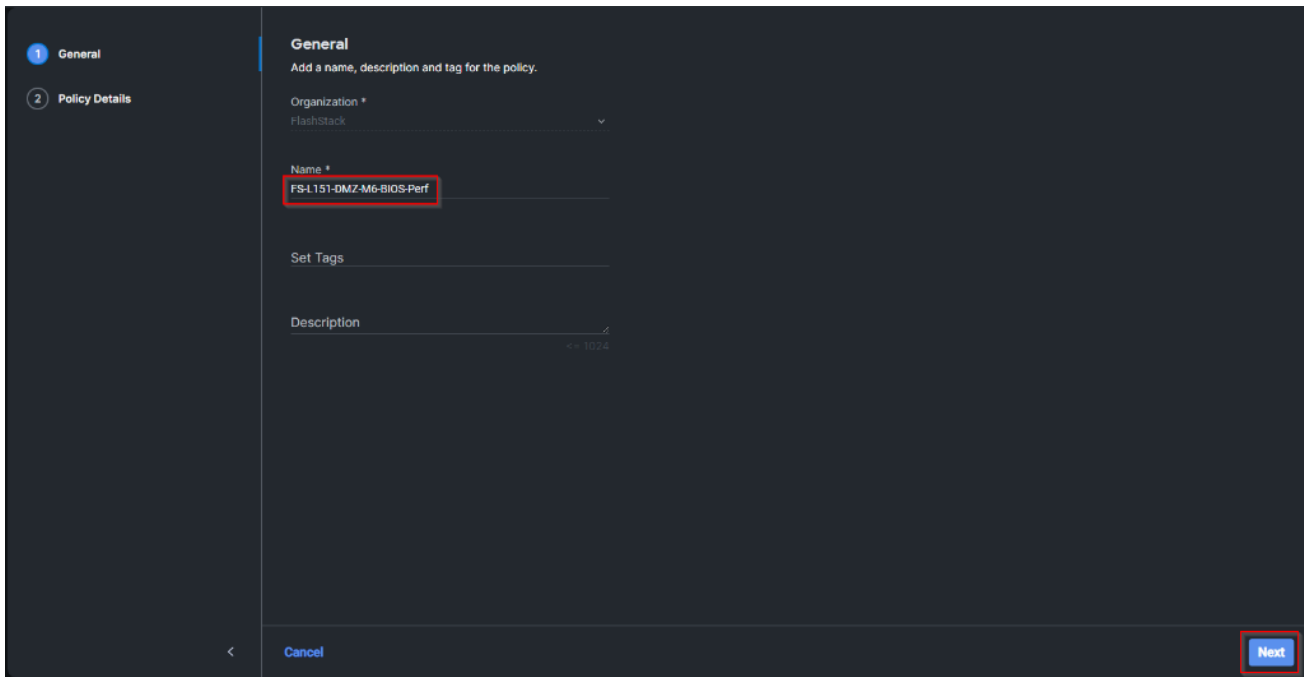
**Step 6.** Provide a UUID Prefix (for example, a random prefix of A11A14B6-B193-49C7 was used). Add a UUID block of appropriate size. Click Create.



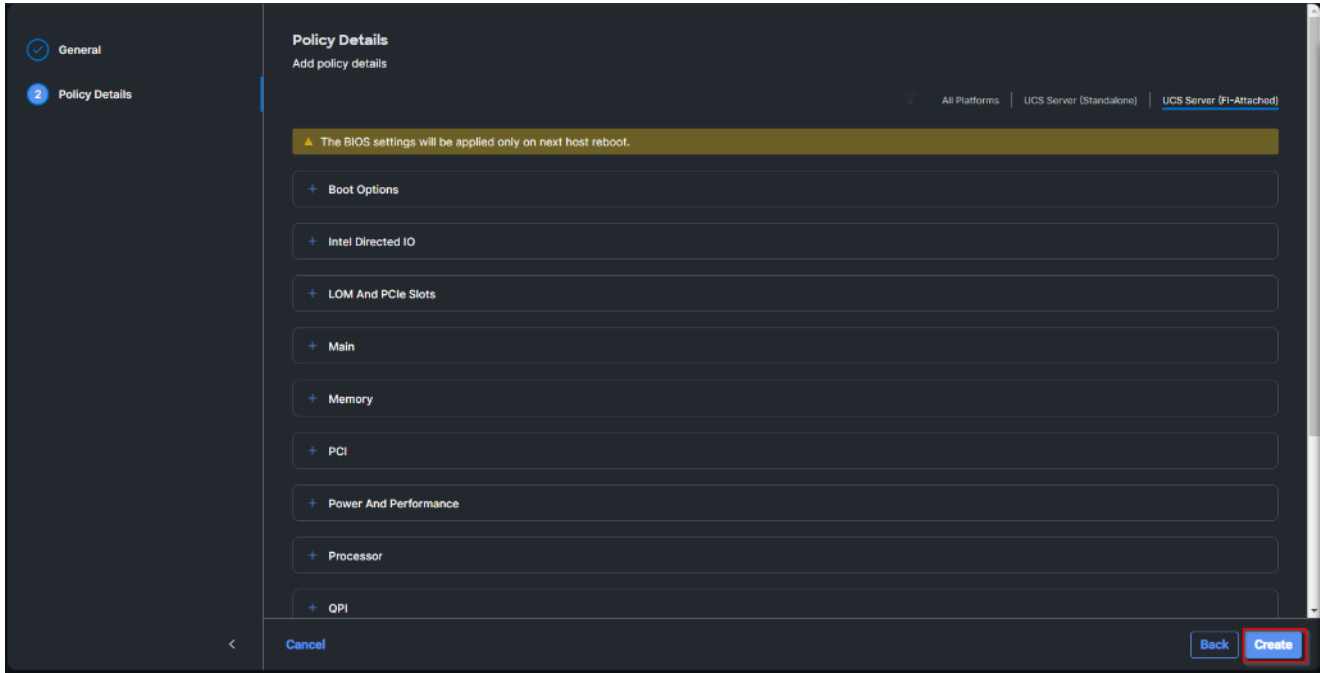
**Step 7.** Click Select Policy next to BIOS and in the pane on the right, click Create New.

**Step 8.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-M6-BIOS-Perf).

**Step 9.** Click Next.



**Step 10.** On the Policy Details screen, select appropriate values for the BIOS settings. Click Create.



**Note:** 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>.

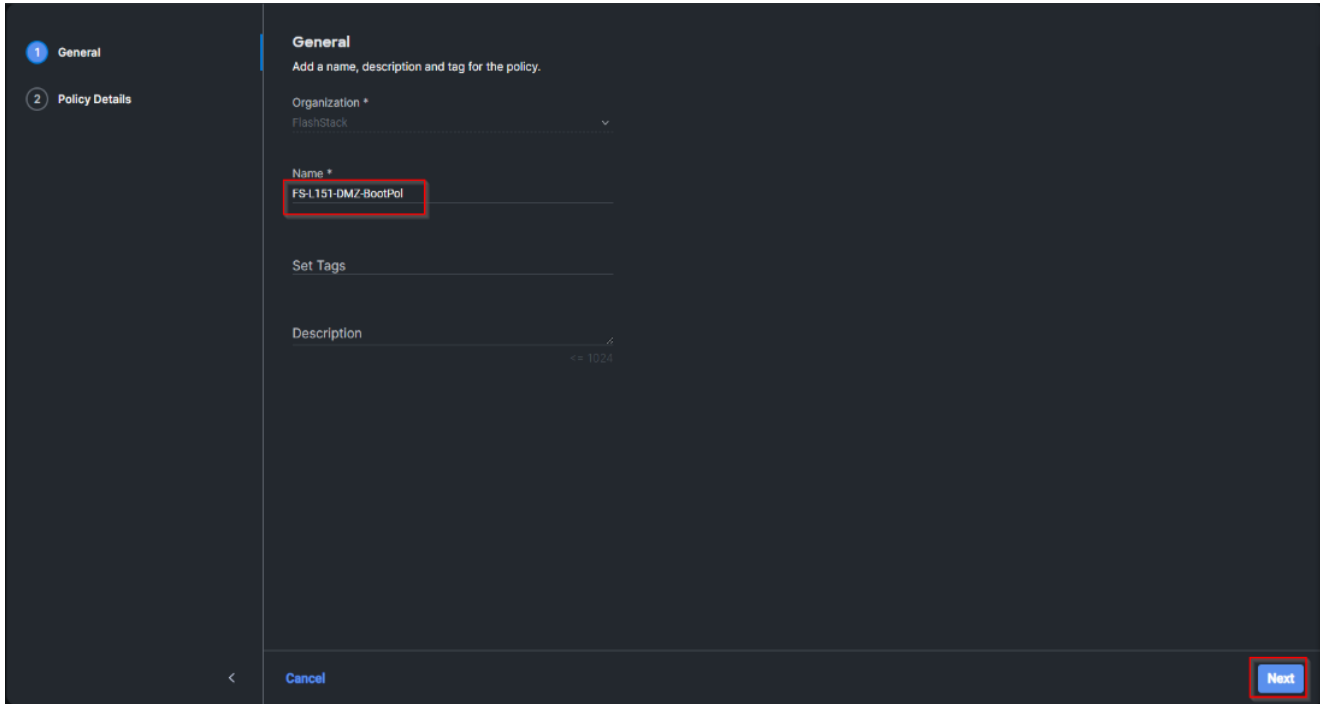
**Table 6.** FS-L151-DMZ-M6-BIOS-Perf token values

BIOS Token	Value
Intel Directed IO	
Intel VT for Directed IO	enabled
Memory	
Memory RAS Configuration	maximum-performance
Power And Performance	
Core Performance Boost	Auto
Enhanced CPU Performance	Auto
LLC Deadline	disabled
UPI Link Enablement	1
UPI Power Management	enabled
Processor	
Altitude	auto
Boot Performance Mode	Max Performance
Core Multiprocessing	all

BIOS Token	Value
CPU Performance	enterprise
Power Technology	performance
Direct Cache Access Support	enabled
DRAM Clock Throttling	Performance
Enhanced Intel Speedstep(R) Technology	enabled
Execute Disable Bit	enabled
IMC Interleaving	1-way Interleave
Intel HyperThreading Tech	Enabled
Intel Turbo Boost Tech	enabled
Intel(R) VT	enabled
DCU IP Prefetcher	enabled
Processor C1E	disabled
Processor C3 Report	disabled
Processor C6 Report	disabled
CPU C State	disabled
Sub Numa Clustering	enabled
DCU Streamer Prefetch	enabled

**Step 11.** Click Select Policy next to Boot Order and then click Create New.

**Step 12.** Verify correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-BootPol). Click Next.



**Step 13.** For Configured Boot Mode, select Unified Extensible Firmware Interface (UEFI).

**Step 14.** Turn on Enable Secure Boot.

**Step 15.** Click Add Boot Device drop-down list and select Virtual Media.

**Step 16.** Provide a device name (for example, vKVM-DVD) and then, for the subtype, select KVM Mapped DVD.

For Fibre Channel SAN boot, four connected FC ports on Pure Storage FlashArray//X70 R3 controllers will be added as boot options. The four FC ports are as follows:

- CT0.FC0, CT1.FC0 are connected to SAN-A
- CT1.FC2, CT0.FC2 are connected to SAN-B

**Figure 20.** Pure Storage FlashArray//X70 R3

FC Port	Name	Speed	Fallover	FC Port	Name	Speed	Fallover
CT0.FC0	524A93:71:56:84:09:00	32 Gb/s		CT1.FC0	524A93:71:56:84:09:10	32 Gb/s	
CT0.FC1	524A93:71:56:84:09:01	0		CT1.FC1	524A93:71:56:84:09:11	0	
CT0.FC2	524A93:71:56:84:09:02	32 Gb/s		CT1.FC2	524A93:71:56:84:09:12	32 Gb/s	
CT0.FC3	524A93:71:56:84:09:03	0		CT1.FC3	524A93:71:56:84:09:13	0	
CT0.FC8	524A93:71:56:84:09:08	0		CT1.FC8	524A93:71:56:84:09:18	0	
CT0.FC9	524A93:71:56:84:09:09	0		CT1.FC9	524A93:71:56:84:09:19	0	

**Step 17.** From the Add Boot Device drop-down list, select SAN Boot (Repeat steps for all 4 FC ports)

**Step 18.** Provide the Device Name: CT0FC0 and the Logical Unit Number (LUN) value (for example, 1).

**Step 19.** Provide an interface name vHBA-A. This value is important and should match the vHBA name.

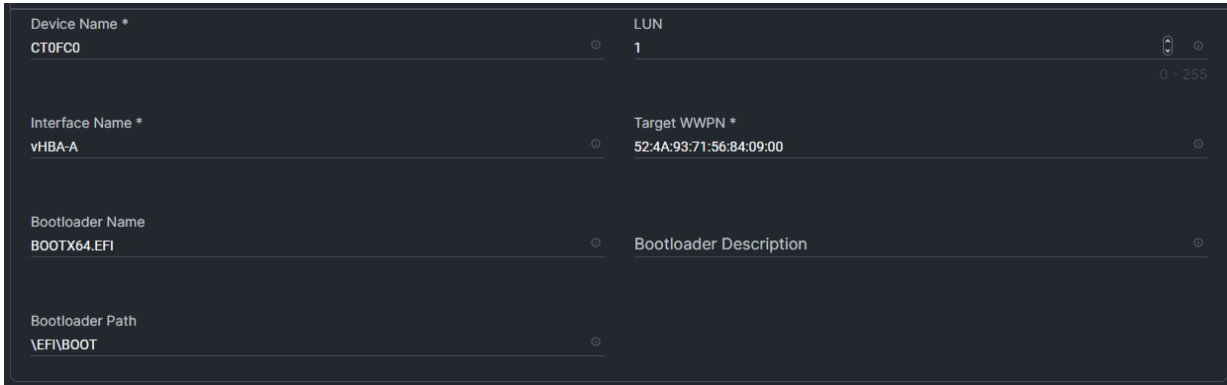
**Note:** vHBA-A is used to access CT0.FC0, CT1.FC0 and vHBA-B is used to access CT1.FC2, CT0.FC2.

**Step 20.** Add the appropriate World Wide Port Name (WWPN) as the Target WWPN (for example, 52:4A:93:71:56:84:09:00).

**Step 21.** Provide bootloader name as BOOTX64.EFI.



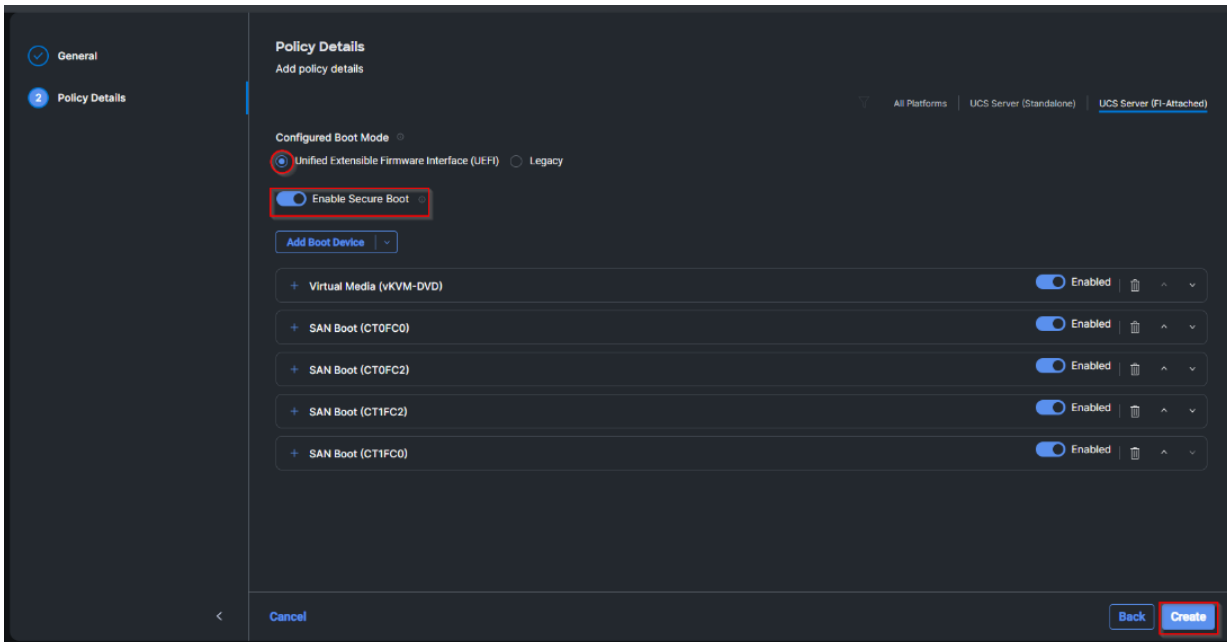
**Step 22.** Provide bootloader name as \EFI\BOOT.



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

Device Name *	CT0FC0	LUN	1
Interface Name *	vHBA-A	Target WWPN *	52:4A:93:71:56:84:09:00
Bootloader Name	BOOTX64.EFI	Bootloader Description	
Bootloader Path	\EFI\BOOT		

**Step 23.** Verify the order of the boot policies and adjust the boot order as necessary using the arrows next to delete icon. Click Create.



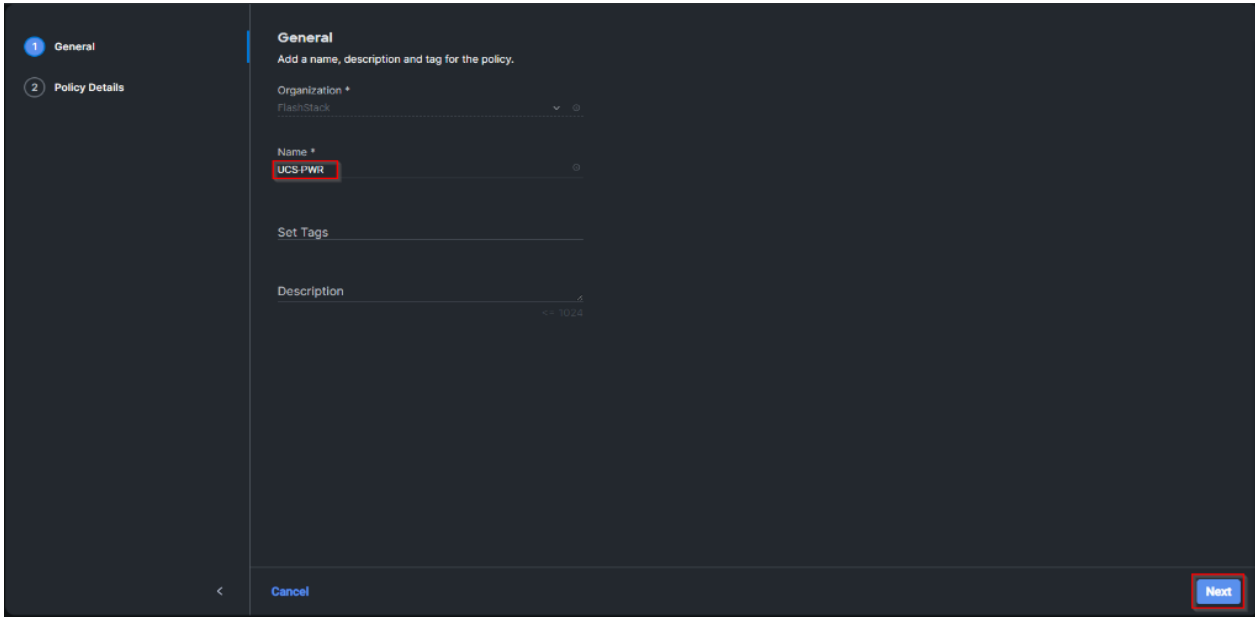
The screenshot shows the 'Policy Details' configuration page. The 'Configured Boot Mode' is set to 'Unified Extensible Firmware Interface (UEFI)'. The 'Enable Secure Boot' toggle is turned on. The boot devices list is as follows:

Device	Enabled	Delete	Move Up	Move Down
+ Virtual Media (vKVM-DVD)	Enabled	🗑️	⬆️	⬆️
+ SAN Boot (CT0FC0)	Enabled	🗑️	⬆️	⬆️
+ SAN Boot (CT0FC2)	Enabled	🗑️	⬆️	⬆️
+ SAN Boot (CT1FC2)	Enabled	🗑️	⬆️	⬆️
+ SAN Boot (CT1FC0)	Enabled	🗑️	⬆️	⬆️

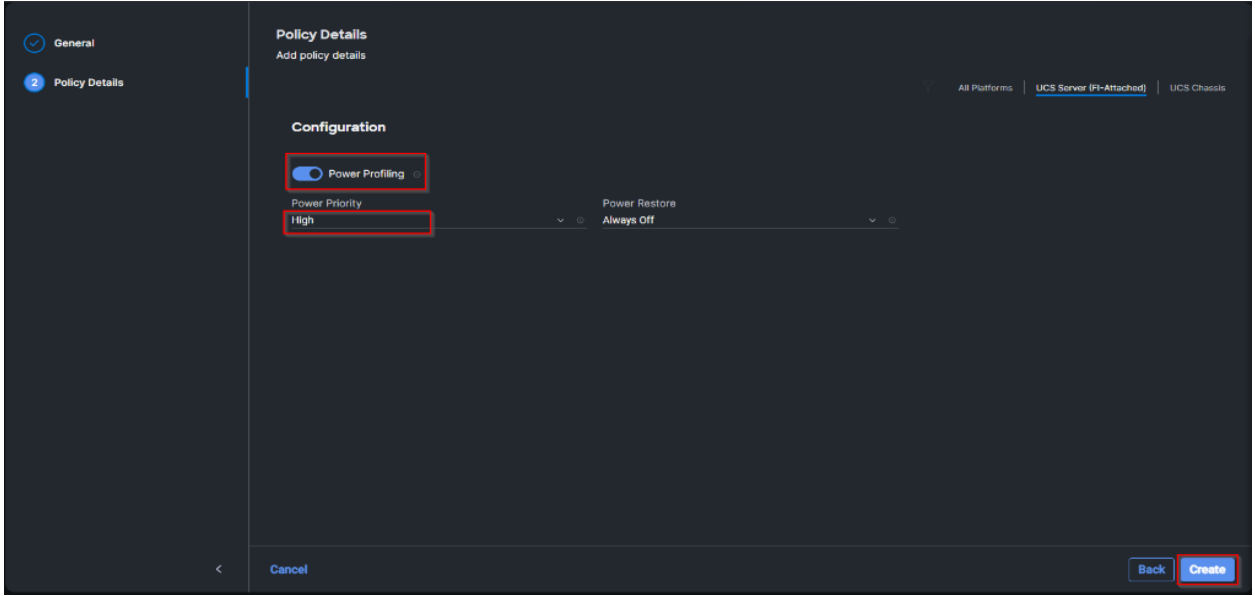
At the bottom, there are 'Cancel', 'Back', and 'Create' buttons. The 'Create' button is highlighted with a red box.

**Step 24.** Click Select Policy next to Power and in the pane on the right, click Create New.

**Step 25.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, UCS-PWR). Click Next.

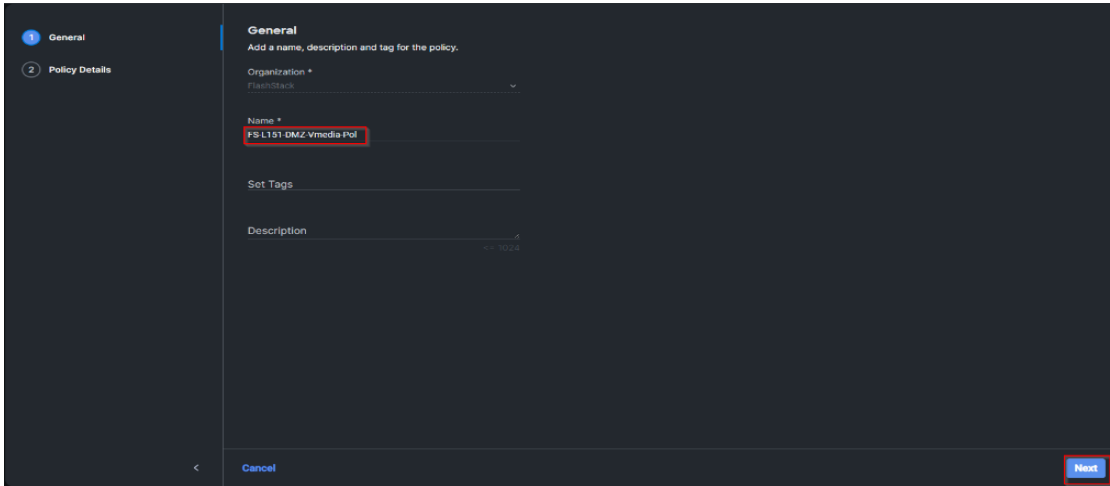


**Step 26.** Enable Power Profiling and select High from the Power Priority drop-down list. Click Create.

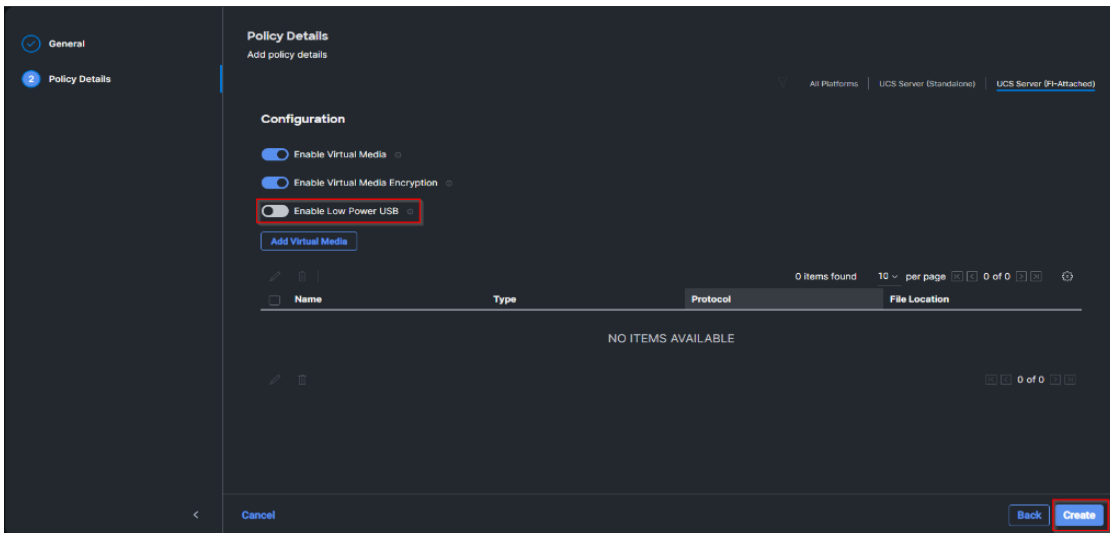


**Step 27.** Click Select Policy next to Virtual Media and in the pane on the right, click Create New (Optional)

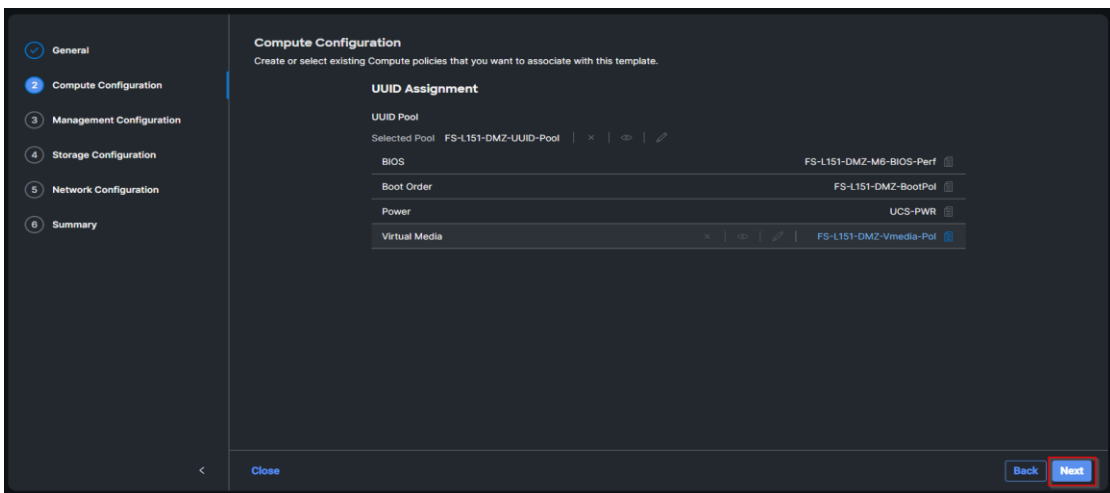
**Step 28.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-Vmedia-Pol). Click Next.



**Step 29.** Disable Lower Power USB and click Create.

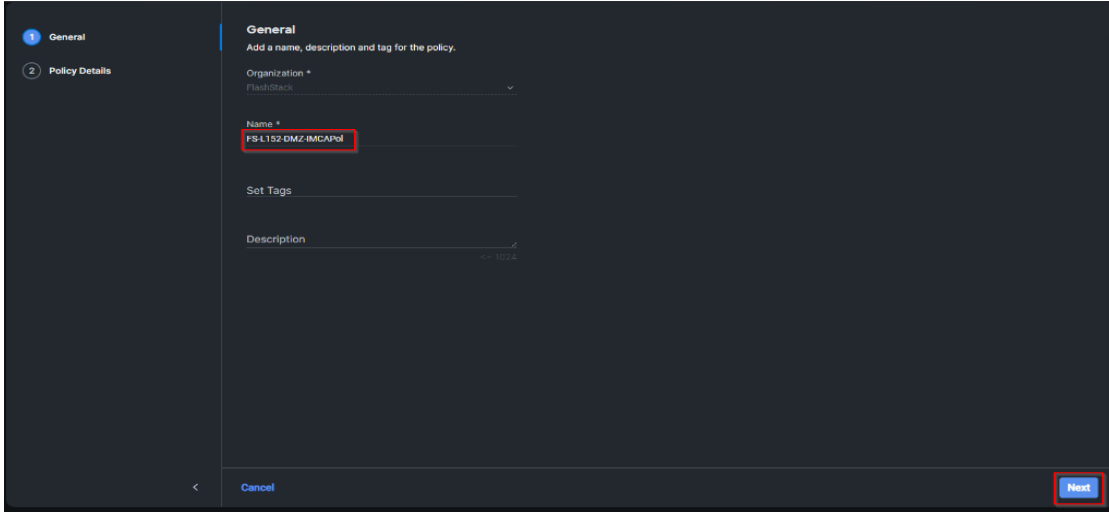


**Step 30.** Click Next to go to Management Configuration.



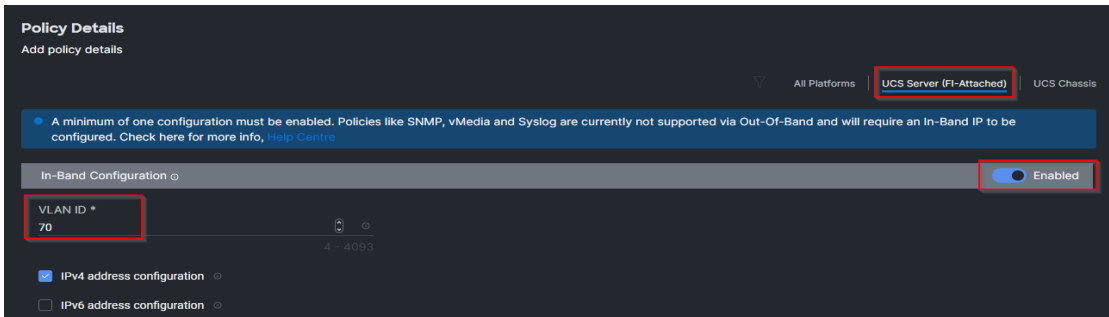
**Step 31.** Click Select Policy next to IMC Access and then click Create New.

**Step 32.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L152-DMZ-IMCAPol). Click Next.



**Note:** You can select in-band management access to the compute node using an in-band management VLAN (for example, VLAN 70) 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.

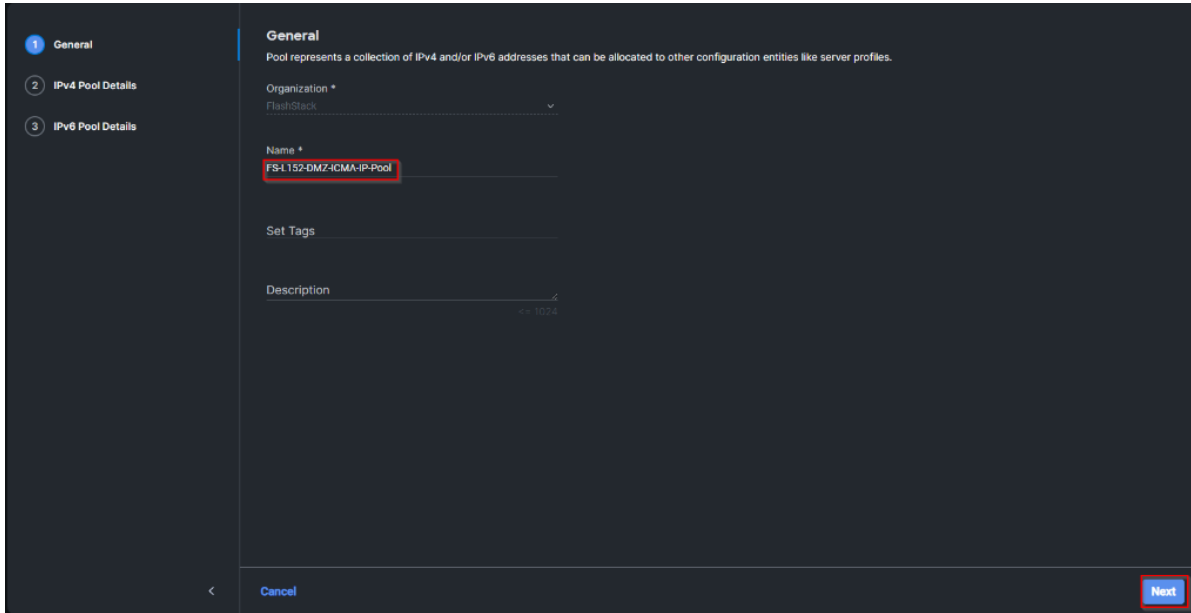
**Step 33.** Click UCS Server (FI-Attached). Enable In-Band Configuration and type VLAN Id designated for the In-Band management (for example, 70).



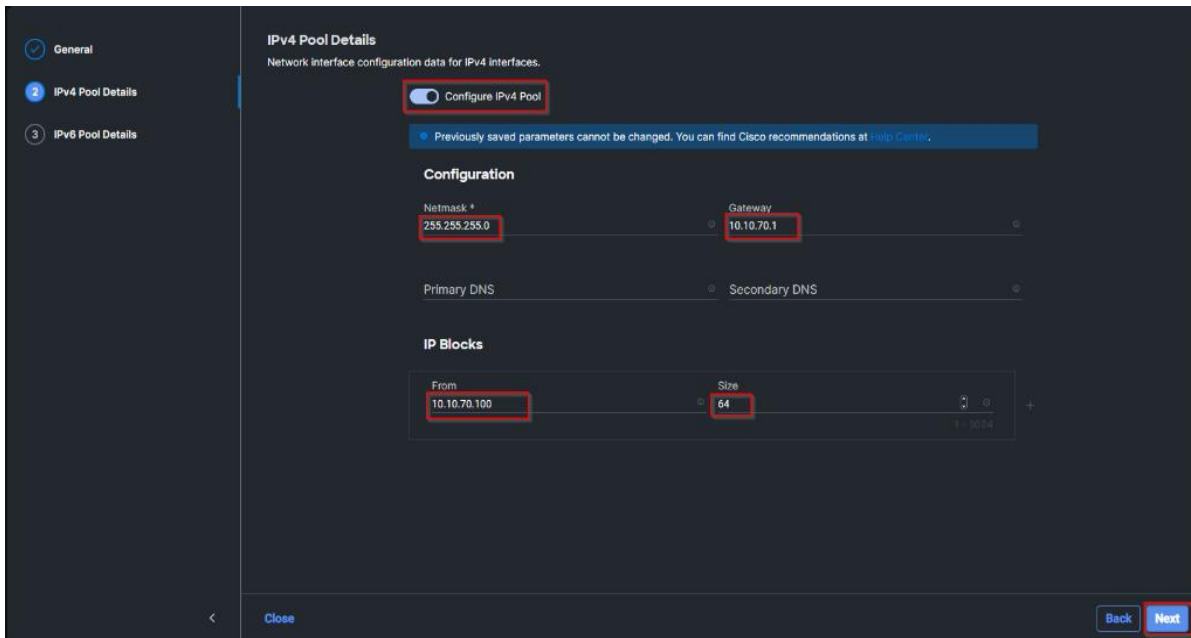
**Step 34.** Under IP Pool, click Select IP Pool and then click Create New.



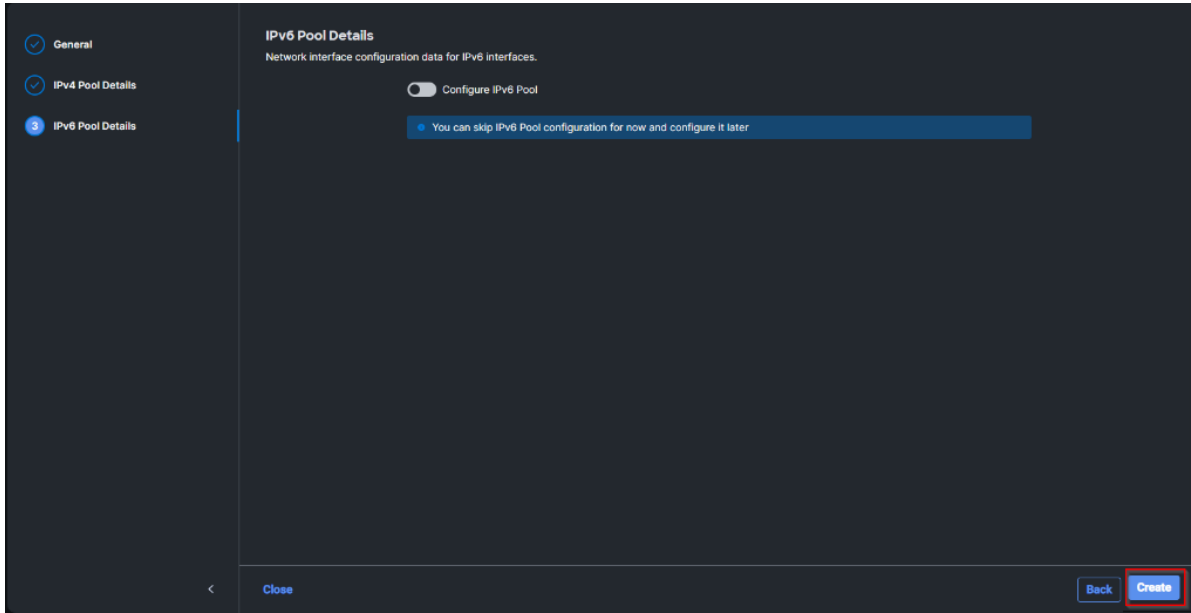
**Step 35.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L152-DMZ-ICMA-IP-Pool). Click Next.



**Step 36.** Select Configure IPv4 Pool and provide the information to define a pool for KVM IP address assignment including an IP Block.

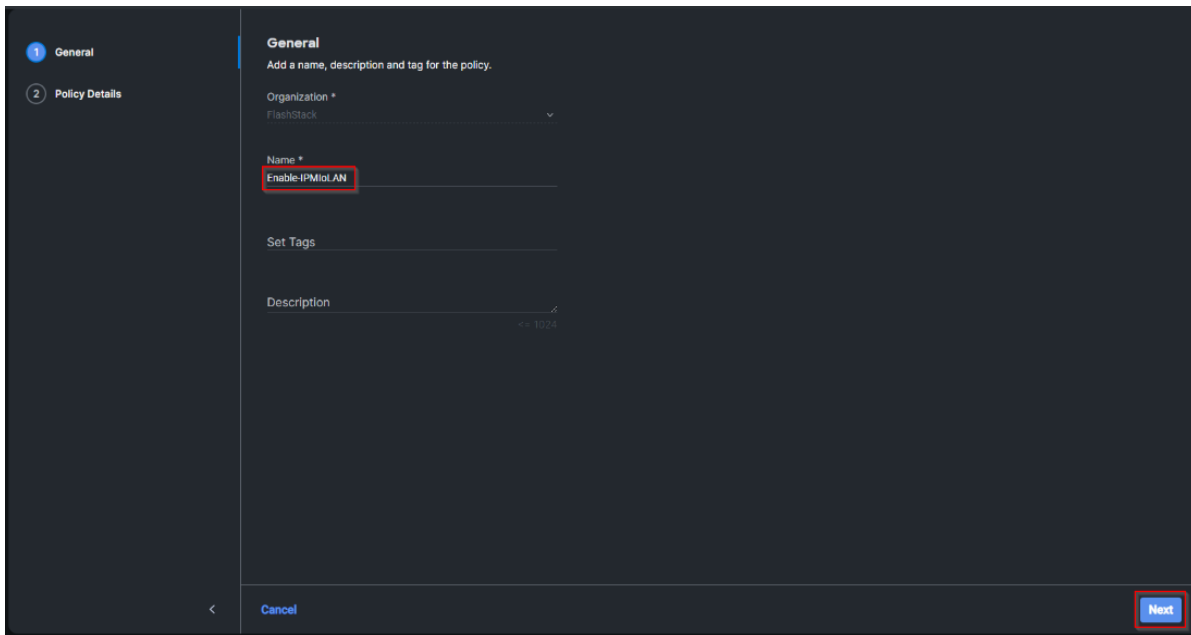


**Note:** The management IP pool subnet should be accessible from the host that is trying to open the KVM connection. In the example shown here, the hosts trying to open a KVM connection would need to be able to route to 10.10.70.0/24 subnet.



**Step 37.** Click Select Policy next to IPMI Over LAN and then click Create New.

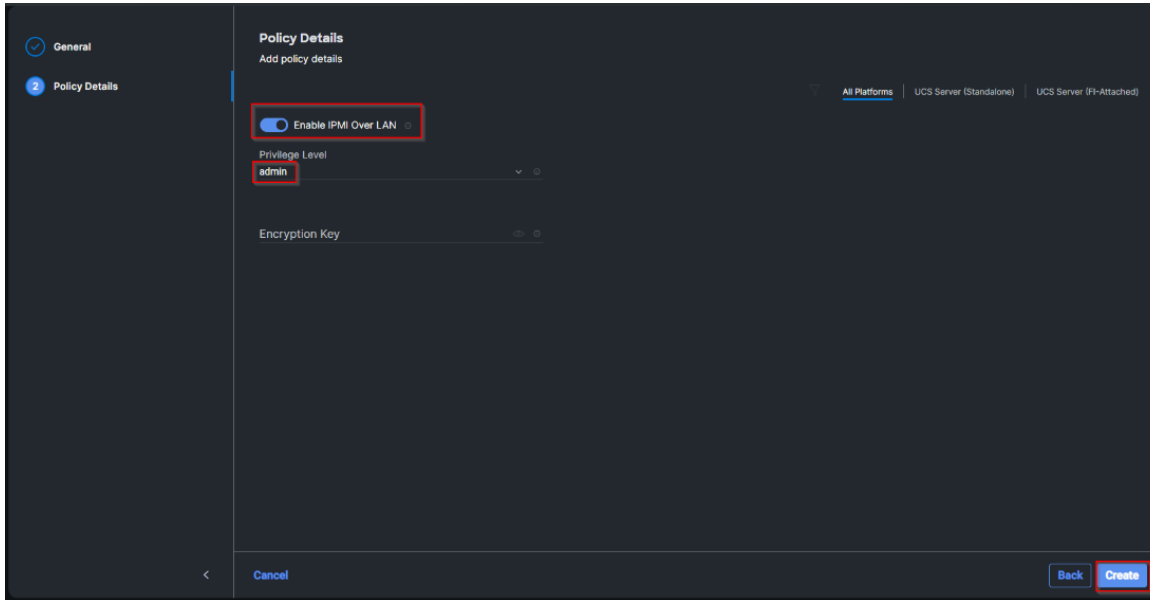
**Step 38.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, Enable-IPMIoLAN). Click Next.



**Step 39.** Turn on Enable IPMI Over LAN.

**Step 40.** From the Privilege Level drop-down list, select admin.

**Step 41.** Click Create.

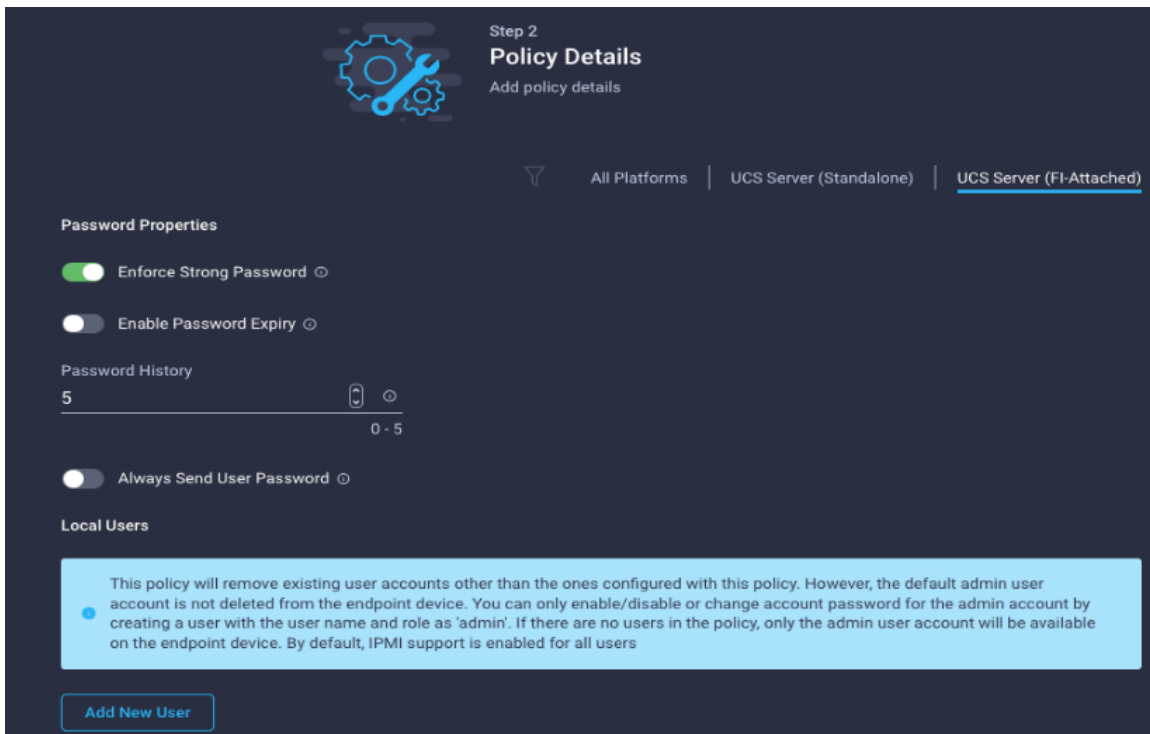


**Step 42.** Click Select Policy next to Local User and the, in the pane on the right, click Create New.

**Step 43.** Verify the correct organization is selected from the drop-down list and provide a name for the policy.

**Step 44.** Verify that UCS Server (FI-Attached) is selected.

**Step 45.** Verify that Enforce Strong Password is selected.



**Step 46.** Click Add New User and then click + next to the New User.

**Step 47.** Provide the username (for example, fpadmin), choose a role for example, admin), and provide a password.

**Add New User**

— fpadding (admin)  Enable

Username \*  Role

Password \*  Password Confirmation \*

**Note:** The username and password combination defined here will be used to log into KVMs. The typical Cisco UCS admin username and password combination cannot be used for KVM access.

**Step 48.** Click Create to finish configuring the user.

**Step 49.** Click Create to finish configuring local user policy.

**Step 50.** Click Next to move to Storage Configuration.

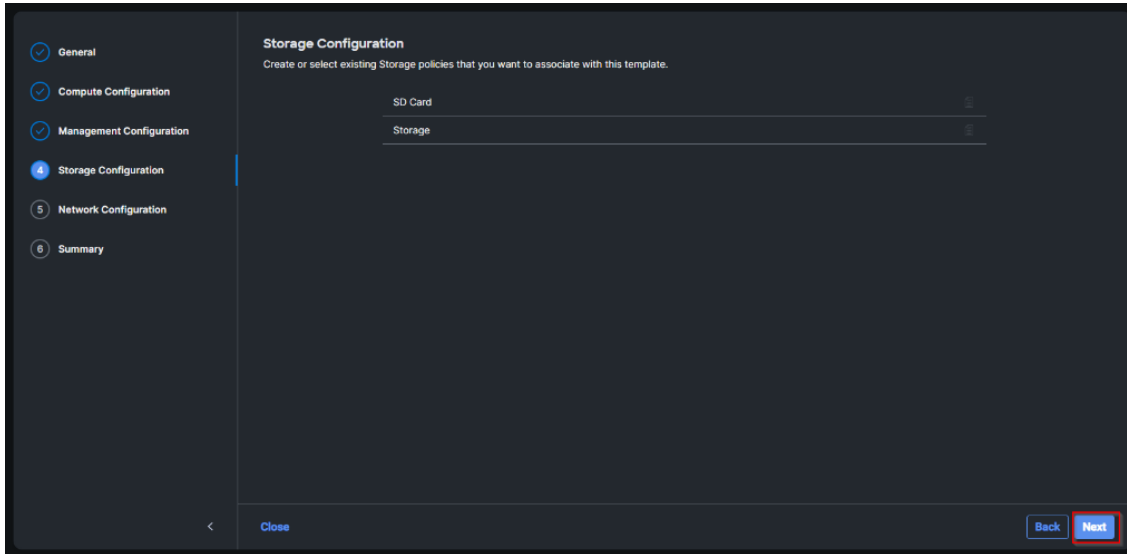
**Management Configuration**  
Create or select existing Management policies that you want to associate with this template.

Certificate Management	
IMC Access	FS-L152-DMZ-IMCAPol
IPMI Over LAN	Enable-IPMIoLAN
Local User	LocalUser-Pol
Serial Over LAN	
SNMP	
Syslog	
Virtual KVM	FS-L151-DMZ-vKVM

Close Back **Next**

**Step 51.** Click Next on the Storage Configuration screen. No configuration is needed in the local storage system.





**Step 52.** Click Select Policy next to LAN Connectivity and then click Create New.

**Note:** 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 consistent vNIC placement, manual vNIC placement is utilized.

The FC boot from SAN hosts uses 4 vNICs configured as listed in [Table 7](#).

**Table 7.** vNICs for LAN Connectivity

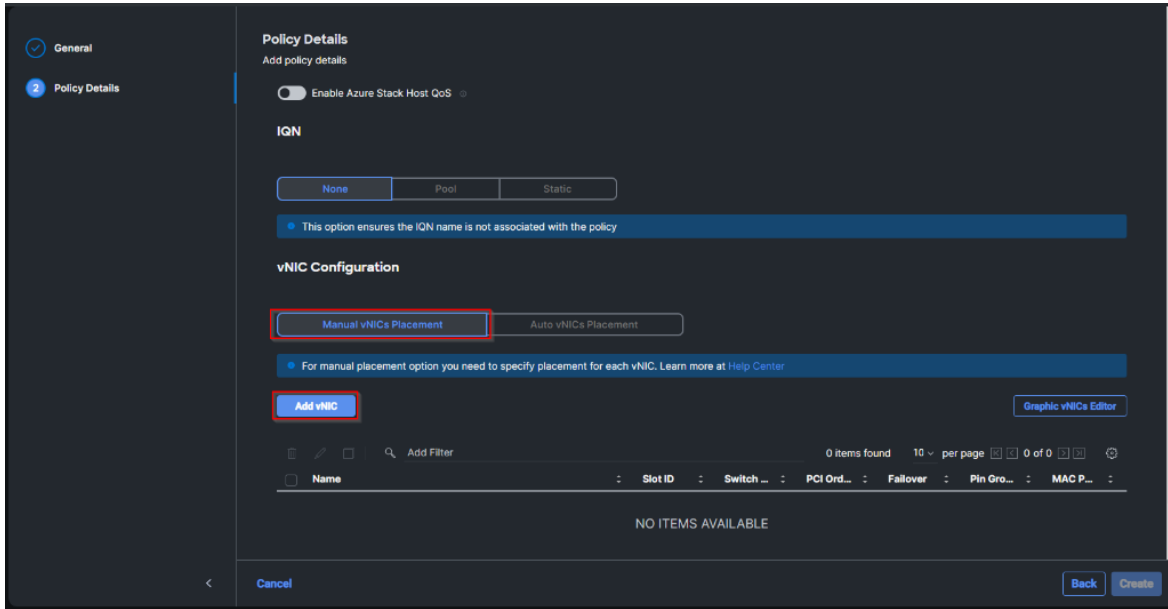
vNIC	Slot ID	Switch ID	PCI Order	VLANs
vSwitch0-A	MLOM	A	2	FS-InBand-Mgmt_70
vSwitch0-B	MLOM	B	3	FS-InBand-Mgmt_70
VDS0-A	MLOM	A	4	FS-VDI_72, FS-vMotion_73
VDS0-B	MLOM	B	5	FS-VDI_72, FS-vMotion_73

**Note:** The PCI order 0 and 1 will be used in the SAN Connectivity policy to create vHBA-A and vHBA-B.

**Step 53.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-LAN-Conn-Pol). Click Next.

**Step 54.** Under vNIC Configuration, select Manual vNICs Placement.

**Step 55.** Click Add vNIC.



**Step 56.** Click Select Pool under MAC Address Pool and then click Create New.

**Note:** 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 8.** MAC Address Pools

Pool Name	Starting MAC Address	Size	vNICs
FS-L151-DMZ-MAC-Pool-A	00:25:B5:04:0A:00	256*	vSwitch0-A, VDS0-A
FS-L151-DMZ-MAC-Pool-B	00:25:B5:04:0B:00	256*	vSwitch0-B, VDS0-B

**Step 57.** Verify the correct organization is selected from the drop-down list and provide a name for the pool from [Table 8](#) depending on the vNIC being created (for example, FS-L151-DMZ-MAC-Pool-A for Fabric A).

**Step 58.** Click Next.

**1 General**

**2 Pool Details**

**General**  
Pool represents a collection of MAC addresses that can be allocated to VNICs of a server profile.

Organization \*  
FlashStack

Name \*  
S-L151-DMZ-MAC-Pool-A

Set Tags

Description

< Cancel **Next**

**Step 59.** Provide the starting MAC address from [Table 8](#) (for example, 00:25:B5:04:0A:00) and the size of the MAC address pool (for example, 256). Click Create to finish creating the MAC address pool.

**General**

**2 Pool Details**

**Pool Details**  
Collection of MAC Blocks.

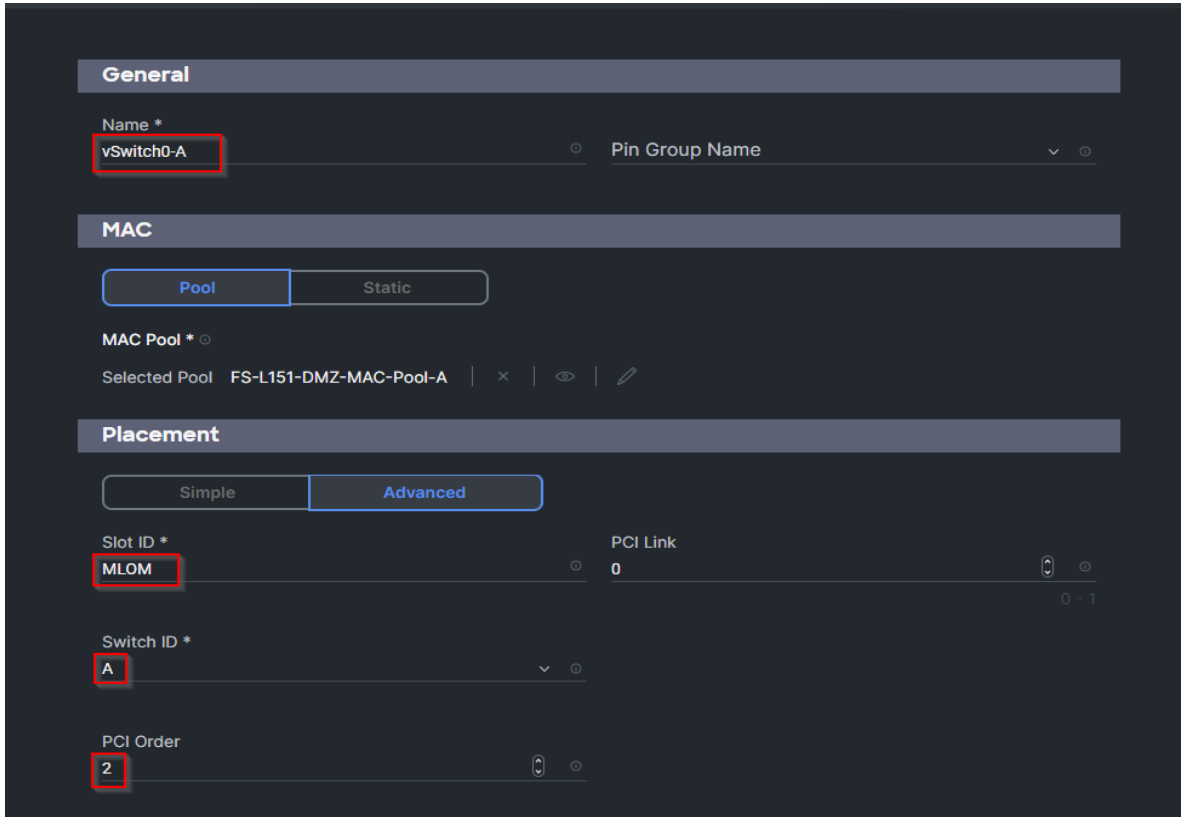
**MAC Blocks**

From: 00:25:B5:04:0A:00

Size: 256

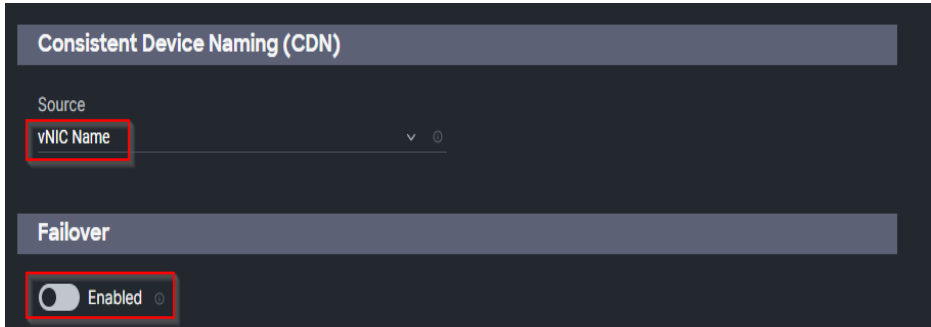
< Cancel **Back** **Create**

**Step 60.** From the Add vNIC window, provide vNIC Name, Slot ID, Switch ID, and PCI Order information from [Table 7](#).



**Step 61.** For Consistent Device Naming (CDN), from the drop-down list, select vNIC Name.

**Step 62.** Verify that Failover is disabled because the failover will be provided by attaching multiple NICs to the VMware vSwitch and VDS.



**Step 63.** Click Select Policy under Ethernet Network Group Policy and then click Create New.

**Note:** 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 listed in [Table 9](#).

**Table 9.** Ethernet Group Policy Values

Group Policy Name	Native VLAN	Apply to vNICs	VLANs
FS-L151-DMZ-vSwitch0-NetGrp-Pol	Native-VLAN (1)	vSwitch0-A, vSwitch0-B	FS-InBand-Mgmt_70
FS-L151-DMZ-vSwitch1-	Native-VLAN	VDS0-A, VDS0-B	FS-VDI_72, FS-

Group Policy Name	Native VLAN	Apply to vNICs	VLANs
NetGrp-Pol	(1)		vMotion_73

**Step 64.** Verify the correct organization is selected from the drop-down list and provide a name for the policy from [Table 9](#) (for example, FS-L151-DMZ-vSwitch0-NetGrp-Pol). Click Next.

The screenshot shows the 'General' tab of a configuration interface. The 'Name' field is highlighted with a red box and contains the text 'FS-L151-DMZ-vSwitch0-NetGrp-Pol'. Other fields include 'Organization' (FlashStack), 'Set Tags', and 'Description'. A 'Next' button is visible at the bottom right.

**Step 65.** Enter the allowed VLANs from [Table 7](#) (for example, 70) and the native VLAN ID from [Table 9](#) (for example, 1). Click Create.

The screenshot shows the 'Policy Details' tab of the configuration interface. Under the 'VLAN Settings' section, the 'Allowed VLANs' field is set to '70' and the 'Native VLAN' field is set to '1', both highlighted with red boxes. A 'Create' button is highlighted at the bottom right.

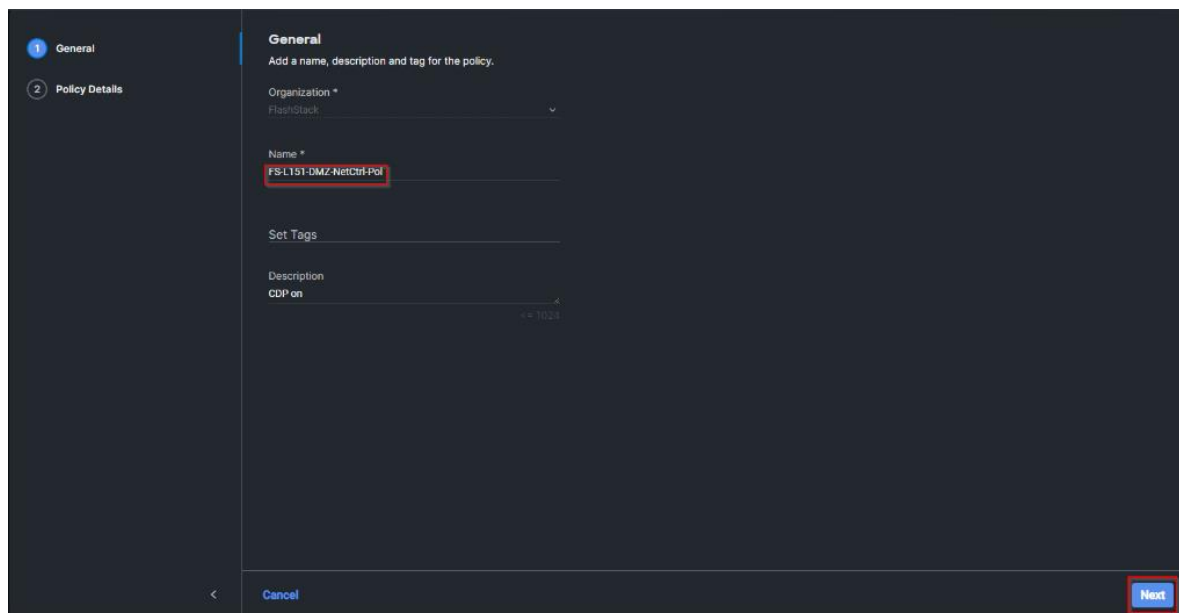
**Note:** When ethernet group policies are shared between two vNICs, the ethernet group policy only needs to be defined for the first vNIC. For subsequent vNIC policy mapping, just click Select Policy and pick the previously defined ethernet group policy from the list on the right.

**Step 66.** Click Select Policy under Ethernet Network Control Policy and then click Create New.

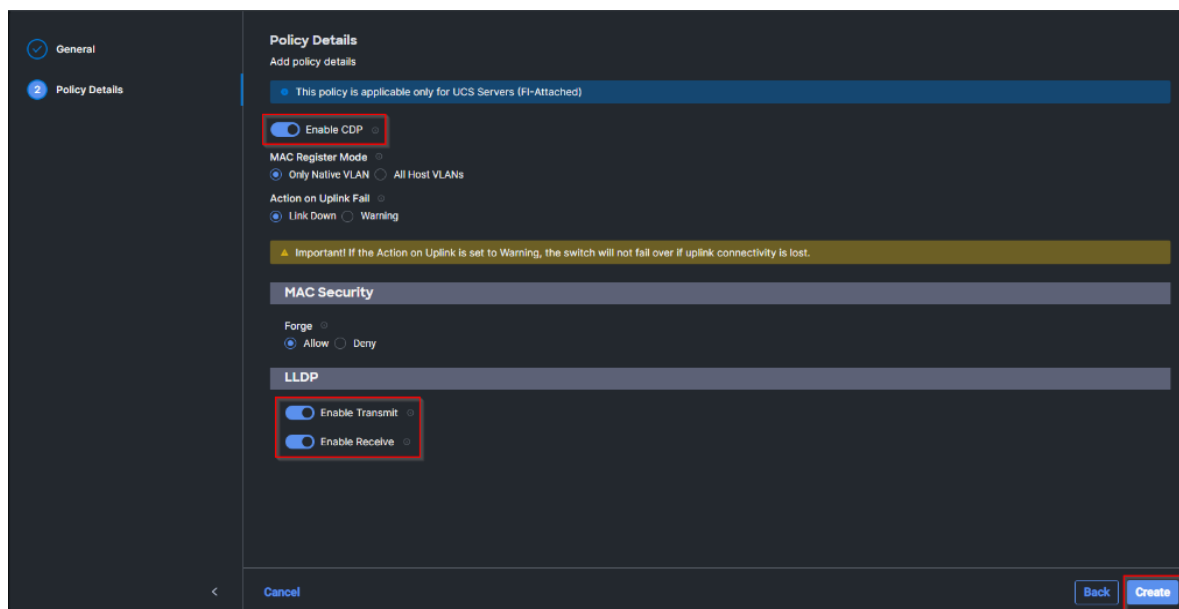
**Note:** The Ethernet Network Control Policy is used to enable Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) for the vNICs. A single policy will be created and reused for all the vNICs.

**Step 67.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-NetCtrl-Pol).

**Step 68.** Click Next.



**Step 69.** Enable Cisco Discovery Protocol and both Enable Transmit and Enable Receive under LLDP. Click Create.

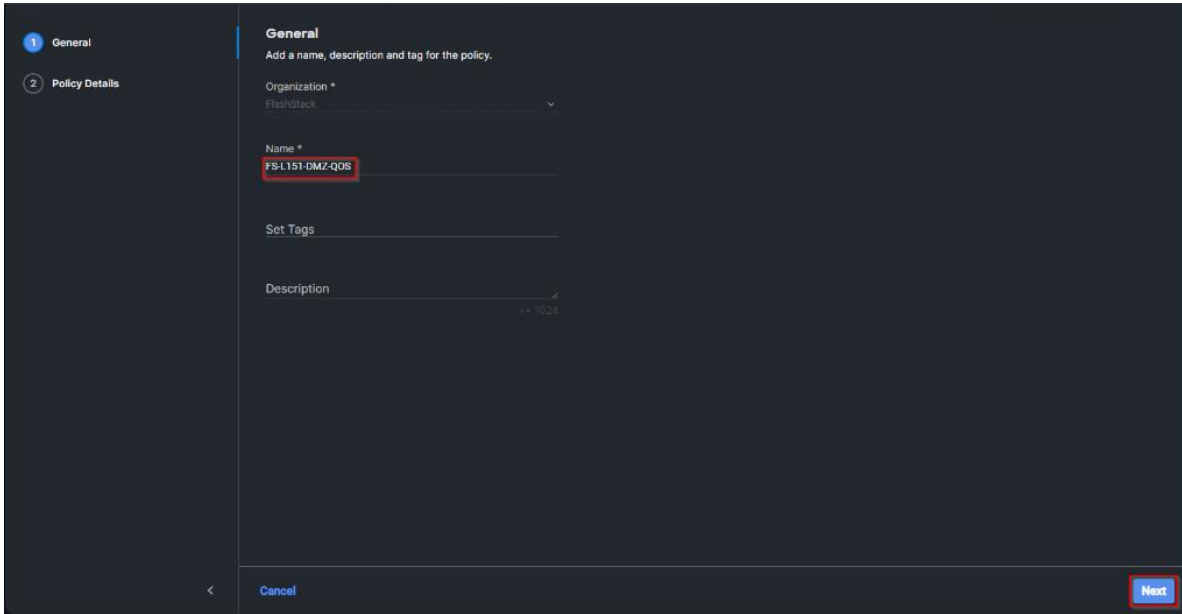


**Step 70.** Click Select Policy under Ethernet QoS and click Create New.

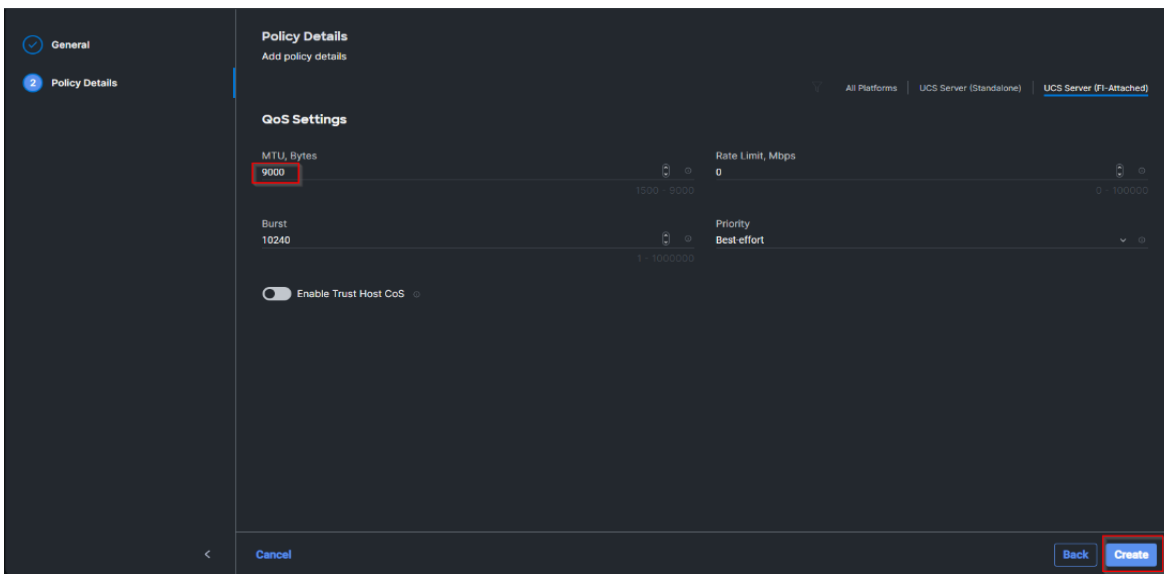
**Note:** The Ethernet QoS policy is used to enable jumbo maximum transmission units (MTUs) for all the vNICs. A single policy will be created and reused for all the vNICs.

**Step 71.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-QOS).

**Step 72.** Click Next.



**Step 73.** Change the MTU Bytes value to 9000. Click Create.



**Step 74.** Click Select Policy under Ethernet Adapter and then click Create New.

**Note:** The 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, FS-L151-DMZ-EthAdapt-VMware-HiTraffic, is created and attached to the VDS0-A and VDS0-B interfaces which handle vMotion.

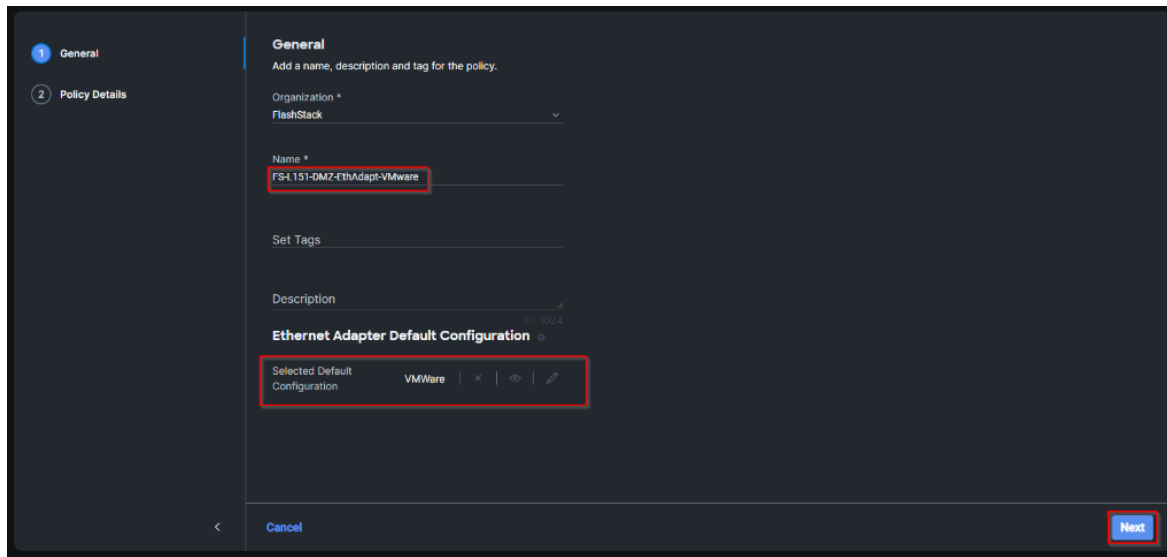
**Table 10.** Ethernet Adapter Policy association to vNICs

Policy Name	vNICs
FS-L151-DMZ-EthAdapt-VMware	vSwitch0-A, vSwitch0-B
FS-L151-DMZ-EthAdapt-VMware-HiTraffic	VDS0-A, VDS0-B,

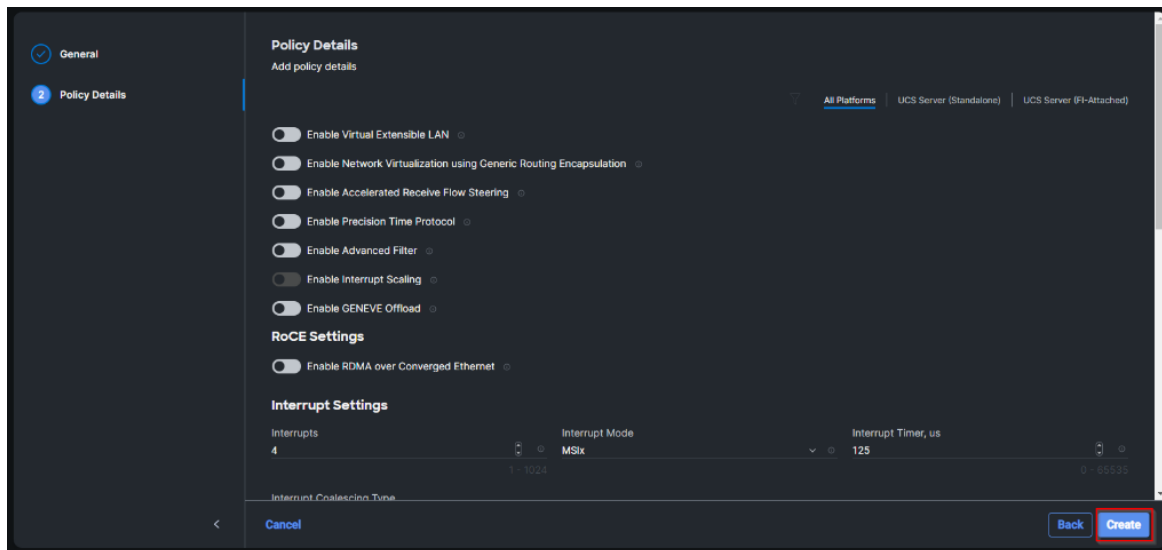
**Step 75.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-EthAdapt-VMware).

**Step 76.** Click Select Default Configuration under Ethernet Adapter Default Configuration.

**Step 77.** From the list, select VMware. Click Next.



**Step 78.** For the FS-L151-DMZ-EthAdapt-VMware policy, click Create and skip the rest of the steps in this section.



**Step 79.** For the optional FS-L151-DMZ-EthAdapt-VMware-HiTraffic policy used 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 - 16384)

**Transmit**

Transmit Queue Count: 1 (range 1 - 1000) | Transmit Ring Size: 256 (range 64 - 16384)

**Completion**

Completion Queue Count: 9 (range 1 - 2000) | Completion Ring Size: 1 (range 1 - 256)

Uplink Failback Timeout (seconds): 5 (range 0 - 600)

**Receive Side Scaling**

Enable Receive Side Scaling

Enable IPv4 Hash

**Step 80.** Click Create.

**Policy Details**

**Transmit**

Transmit Queue Count: 1 (range 1 - 1000) | Transmit Ring Size: 256 (range 64 - 16384)

**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**

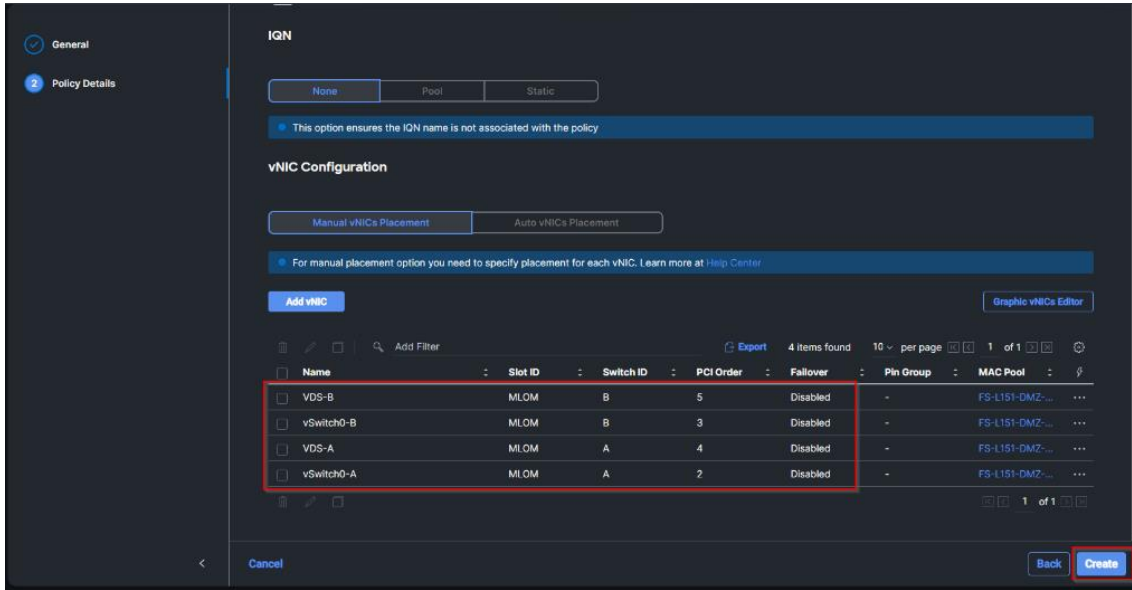
Enable Receive Side Scaling

Enable IPv4 Hash

Cancel | Back | **Create**

**Step 81.** Click Create to finish creating the vNIC.

**Step 82.** Repeat the vNIC creation steps for the rest of vNICs. Verify all four vNICs were successfully created. Click Create.



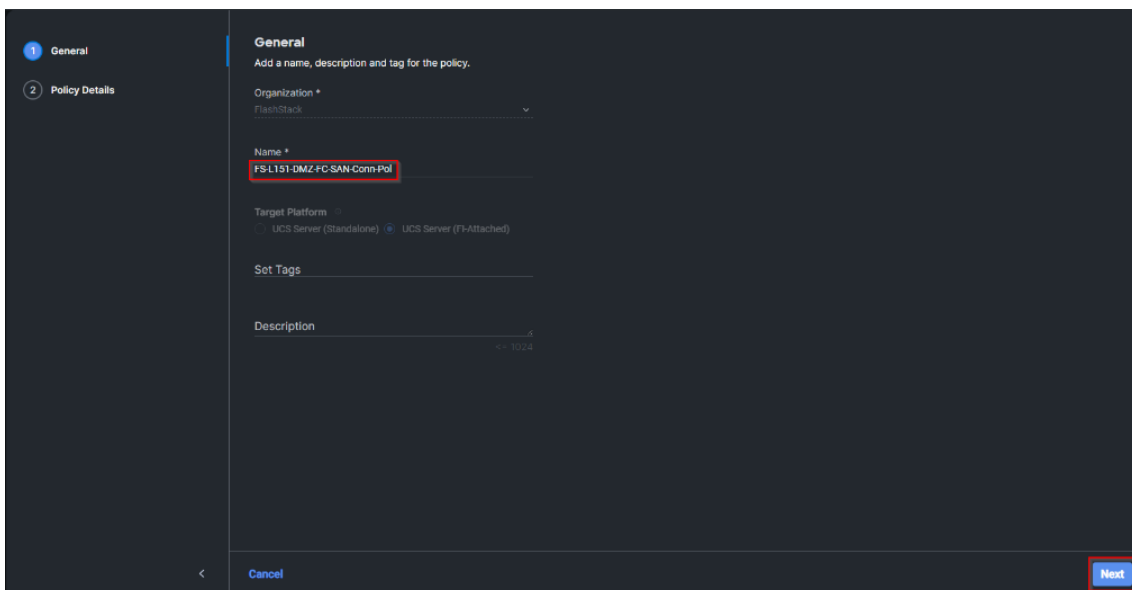
**Step 83.** Click Select Policy next to SAN Connectivity and then click Create New.

**Note:** 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.

**Table 11.** vHBA for boot from FC SAN

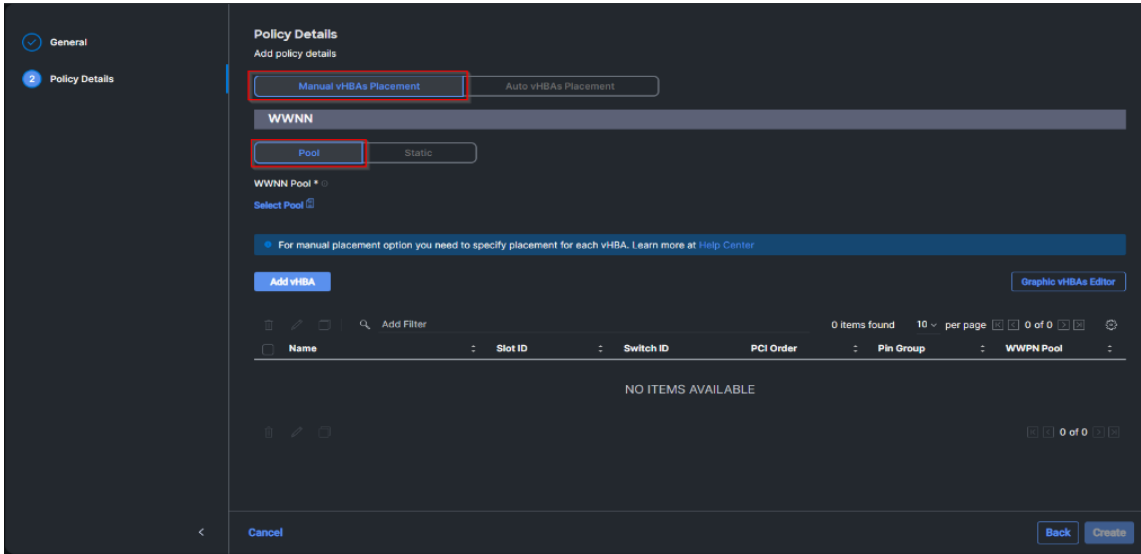
vNIC/vHBA Name	Slot	Switch ID	PCI Order
vHBA-A	MLOM	A	0
vHBA-B	MLOM	B	1

**Step 84.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-FC-SAN-Conn-Pol).



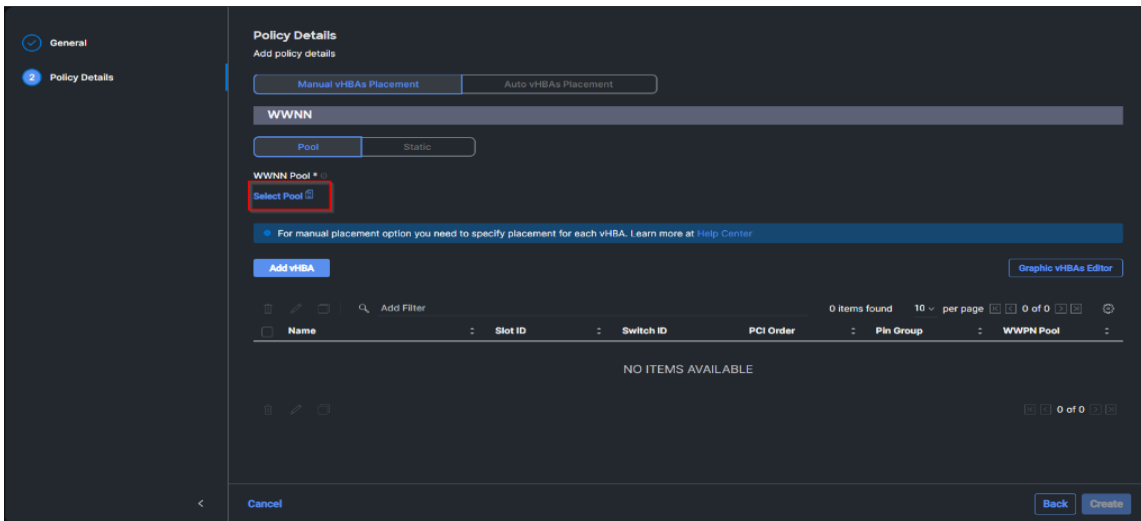
**Step 85.** Select Manual vHBAs Placement.

**Step 86.** Select Pool under WWNN.



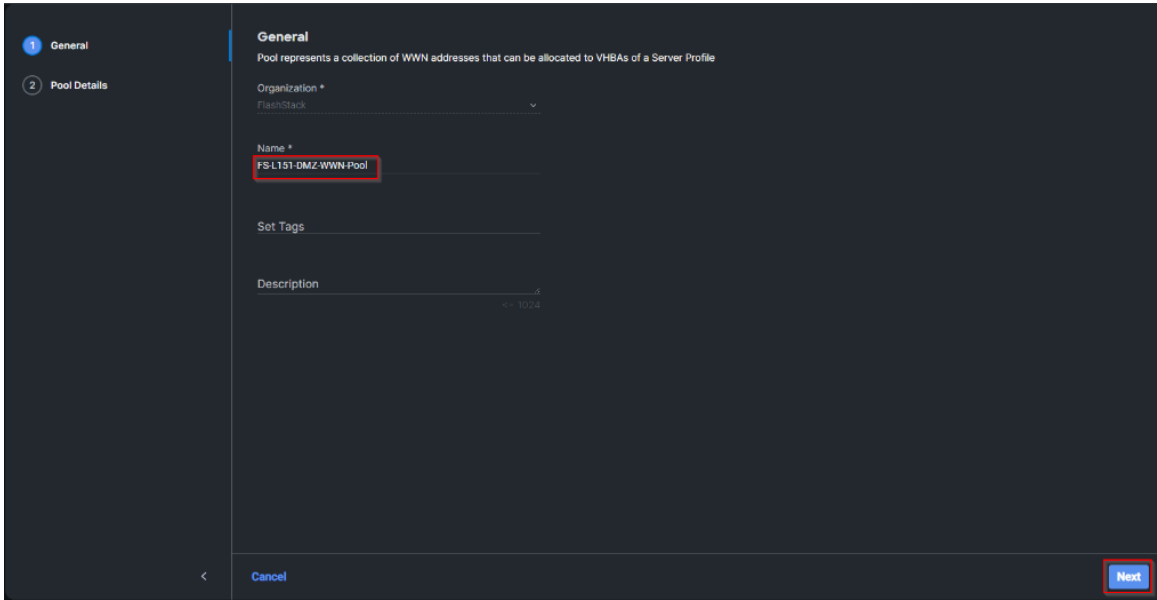
**Note:** The WWNN address pools have not been defined yet therefore a new WWNN address pool has to be defined.

**Step 87.** Click Select Pool under WWNN Pool and then click Create New.

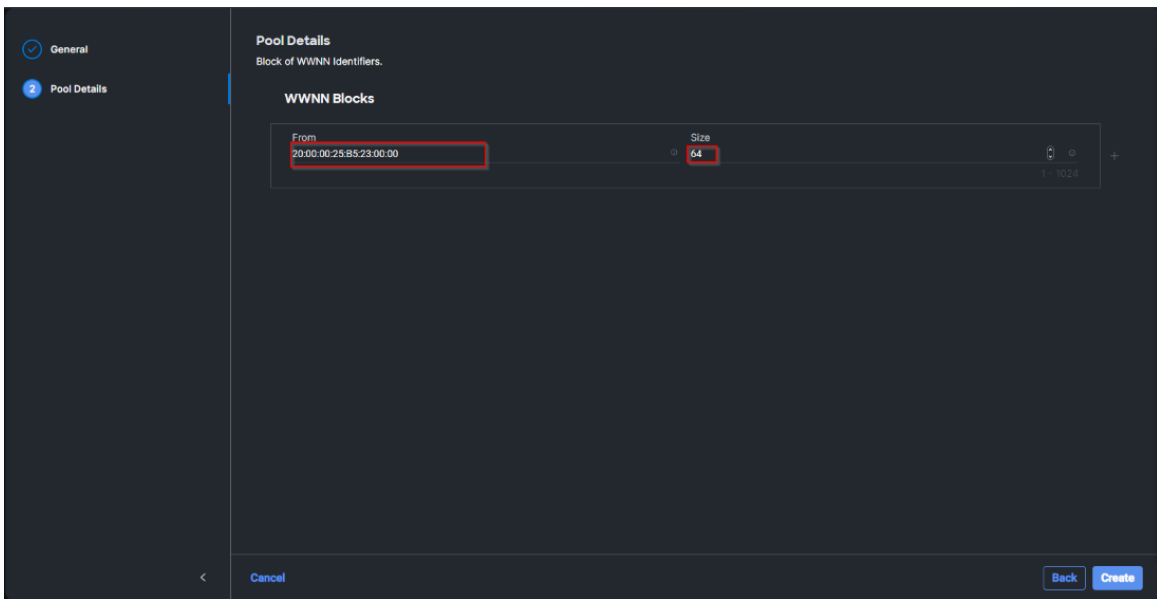


**Step 88.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-WWN-Pool).

**Step 89.** Click Next.

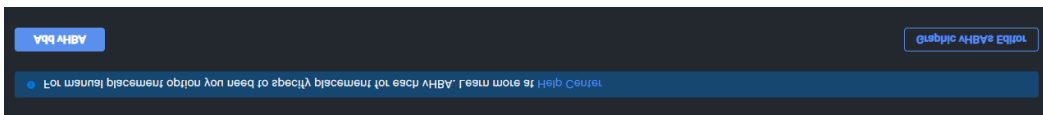


**Step 90.** Provide the starting WWNN block address and the size of the pool. Click Create.



**Note:** As a best practice, additional information should always be coded into the WWNN address pool for troubleshooting. For example, in the address 20:00:00:25:B5:23:00:00, 23 is the rack ID.

**Step 91.** Click Add vHBA.



**Step 92.** Enter vHBA-A for the Name and select fc-initiator from the drop-down list.

**General**

Name \*

vHBA Type

Pin Group Name

**Note:** The WWPN address pool has not been defined yet therefore a WWPN address pool for Fabric A will be defined.

**Step 93.** Click Select Pool under WWPN Address Pool and then click Create New.

**WWPN**

WWPN Pool \*

**Step 94.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-WWPN-Pool-A).

**General**

Pool represents a collection of WWN addresses that can be allocated to VHBA's of a Server Profile

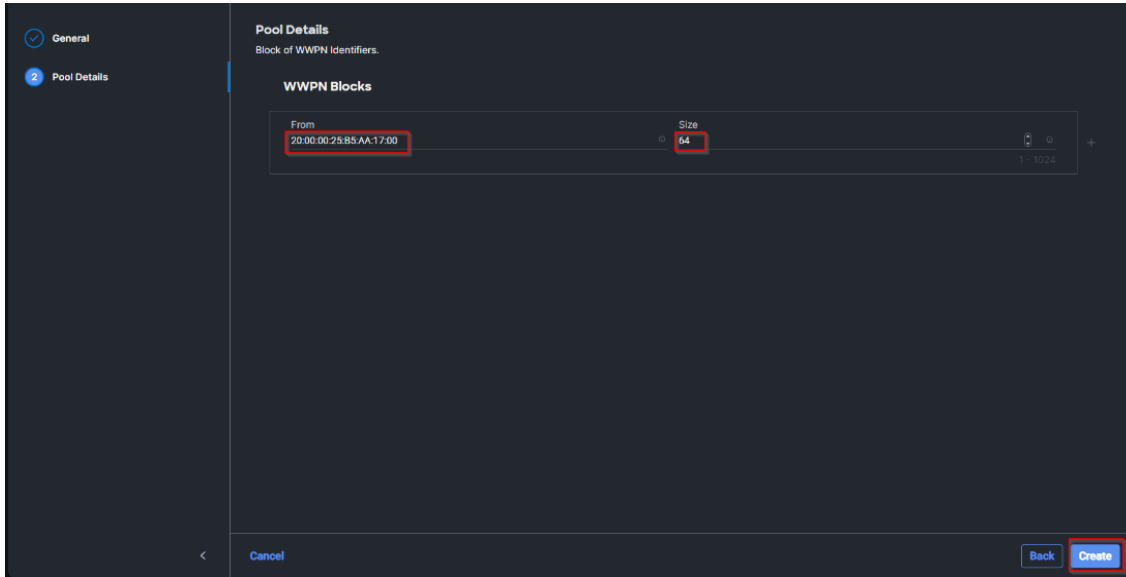
Organization \*

Name \*

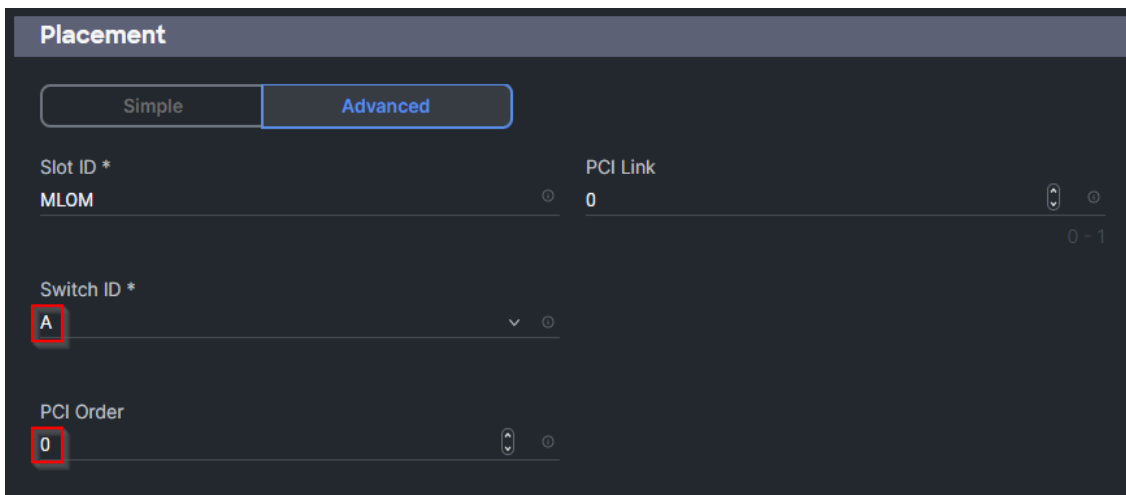
Set Tags

Description

**Step 95.** Provide the starting WWPN block address for SAN A and the size. Click Create.



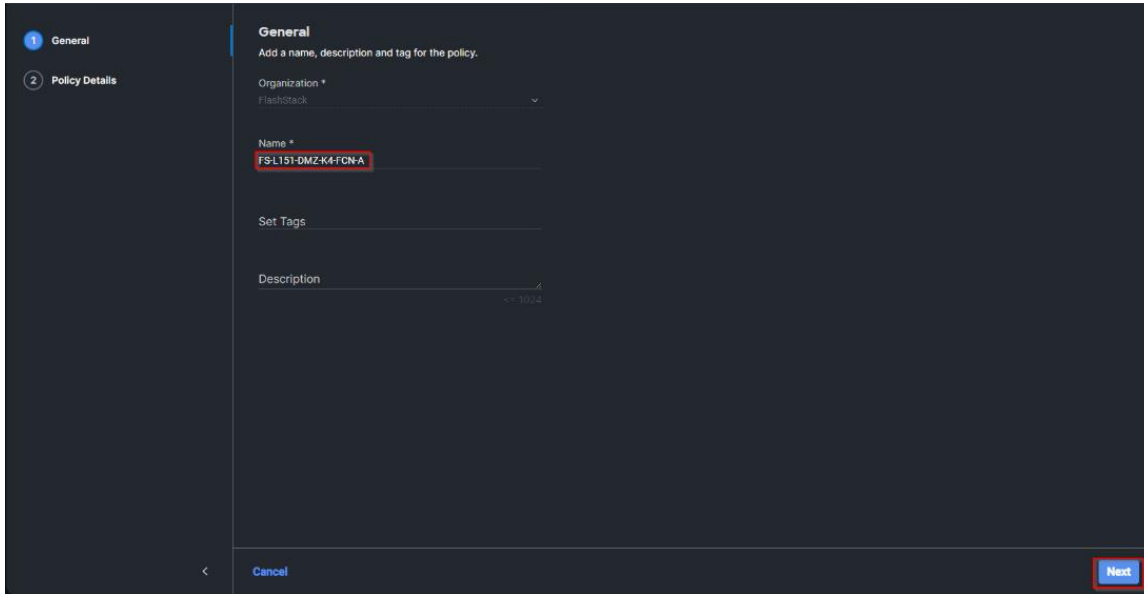
**Step 96.** Provide the Switch ID (for example, A) and PCI Order (for example, 0) from [Table 11](#).



**Step 97.** Click Select Policy under Fibre Channel Network and then click Create New.

**Note:** A Fibre Channel network policy governs the VSAN configuration for the virtual interfaces. In this deployment, VSAN 100 will be used for vHBA-A and VSAN 101 will be used for vHBA-B.

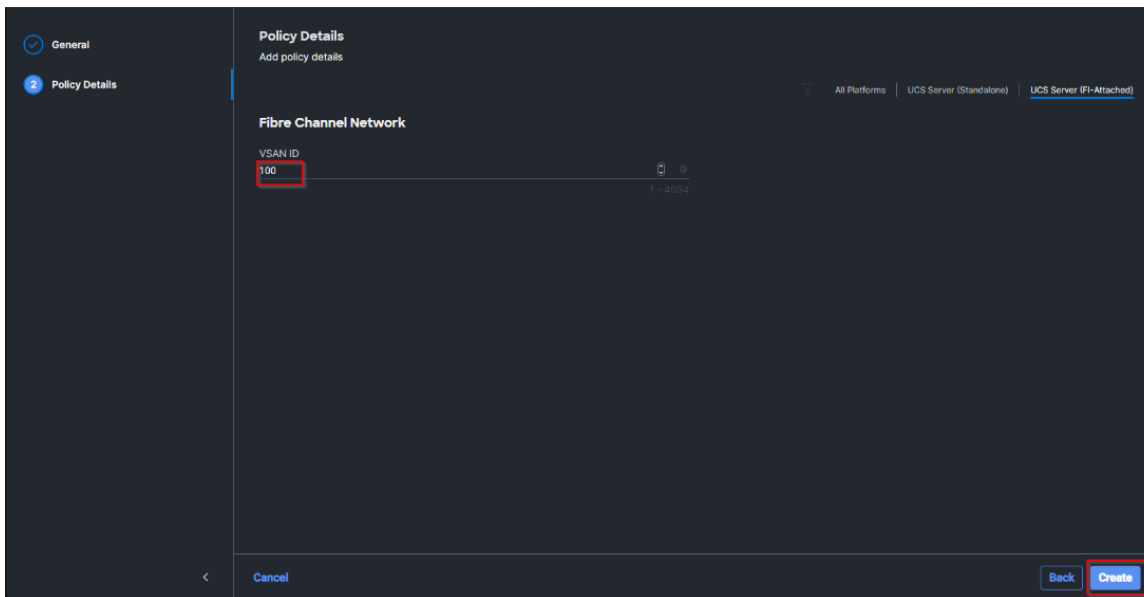
**Step 98.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-K4-FCN-A). Click Next.



**Step 99.** For the scope, select UCS Server (FI-Attached).

**Step 100.** Under VSAN ID, provide the VSAN information (for example, 100).

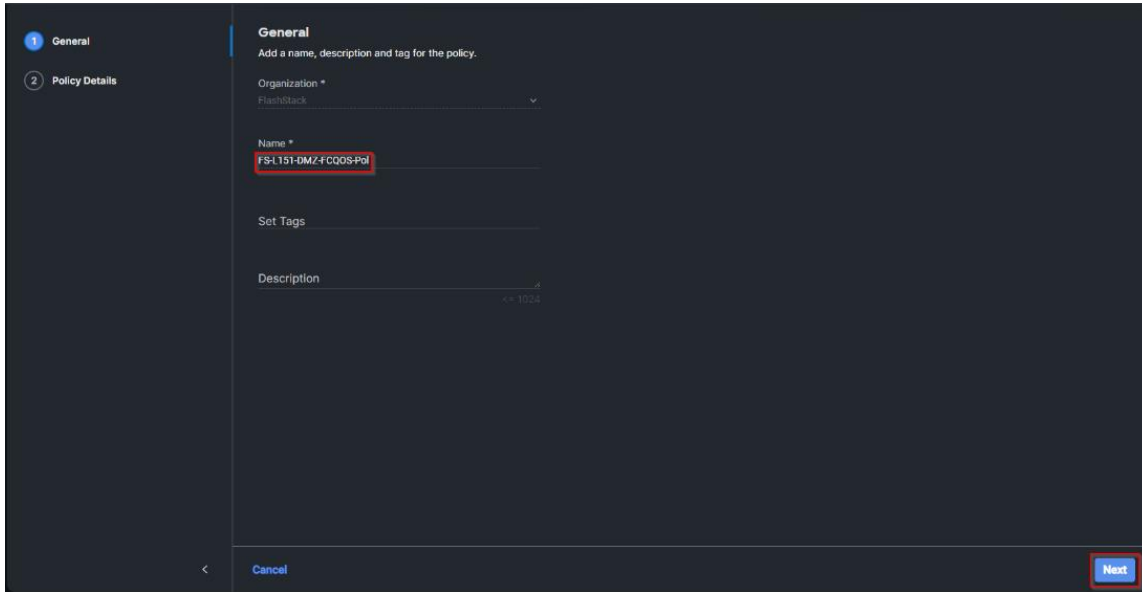
**Step 101.** Click Create.



**Step 102.** Click Select Policy under Fibre Channel QoS and then click Create New.

**Note:** 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.

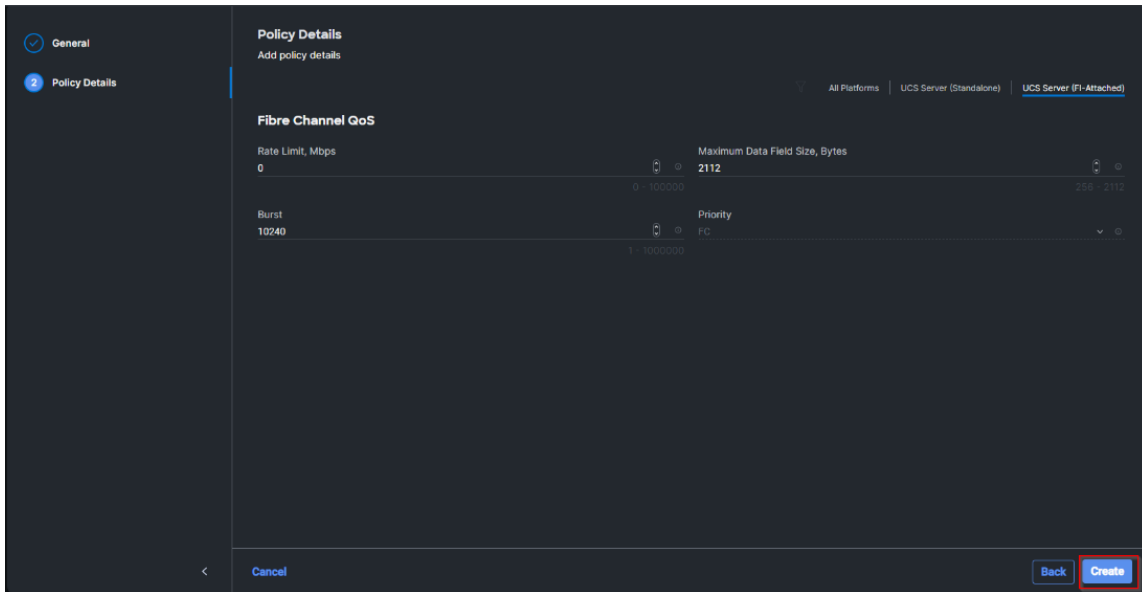
**Step 103.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-FCQOS-Pol). Click Next.



**Step 104.** For the scope, select UCS Server (FI-Attached).

**Note:** Do not change the default values on the Policy Details screen.

**Step 105.** Click Create.

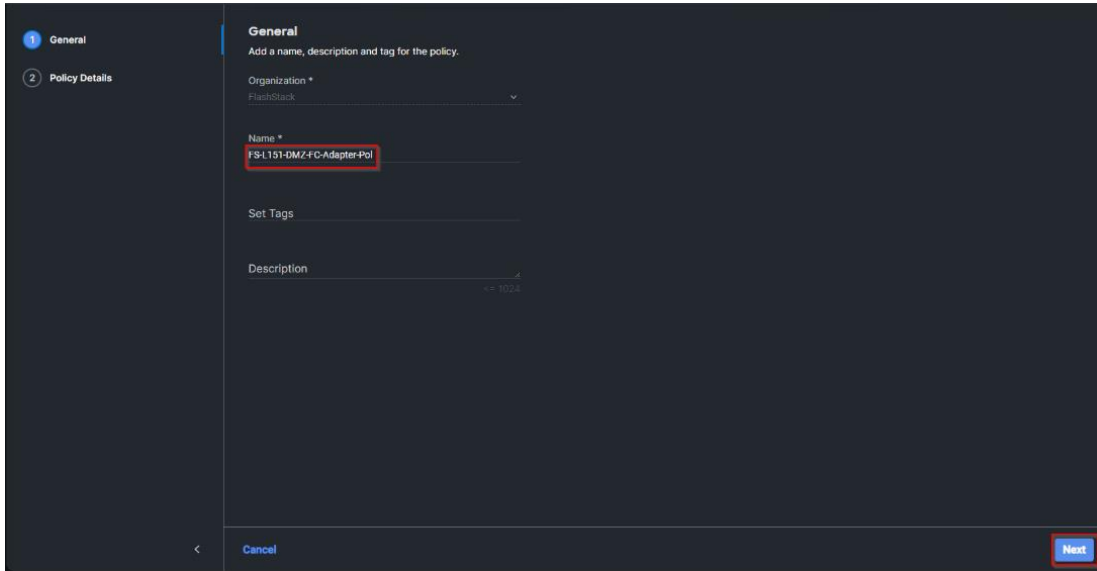


**Step 106.** Click Select Policy under Fibre Channel Adapter and then click Create New.

**Note:** 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 107.** Verify the correct organization is selected from the drop-down list and provide a name for the policy (for example, FS-L151-DMZ-FC-Adapter-Pol).

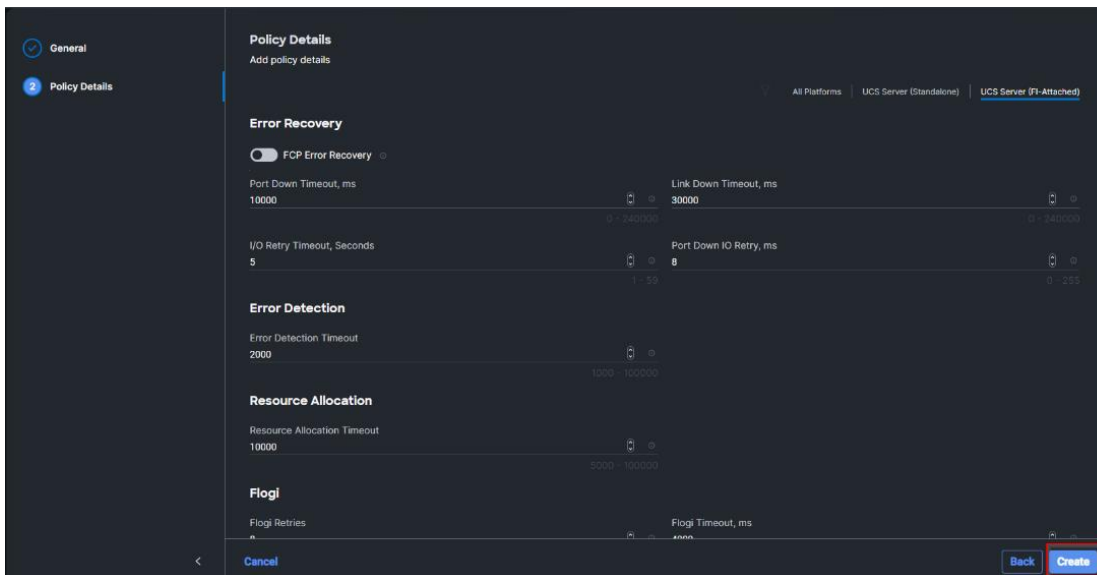




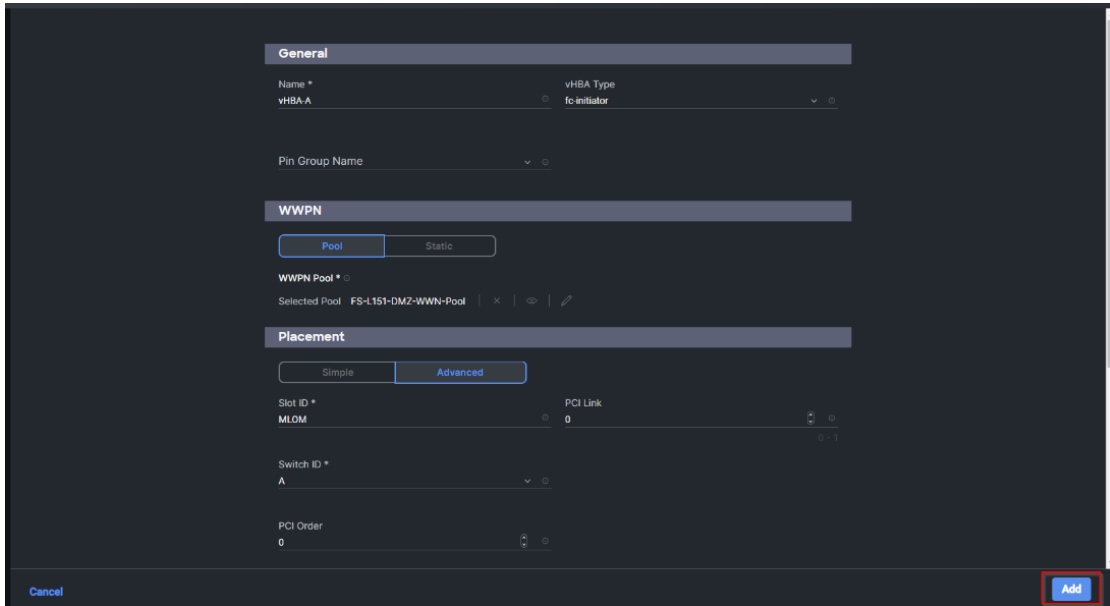
**Step 108.** For the scope, select UCS Server (FI-Attached).

**Note:** Do not change the default values on the Policy Details screen.

**Step 109.** Click Create.

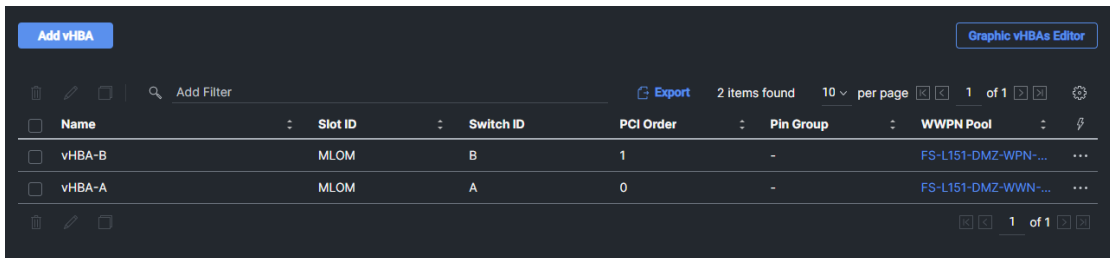


**Step 110.** Click Add to create vHBA-A.

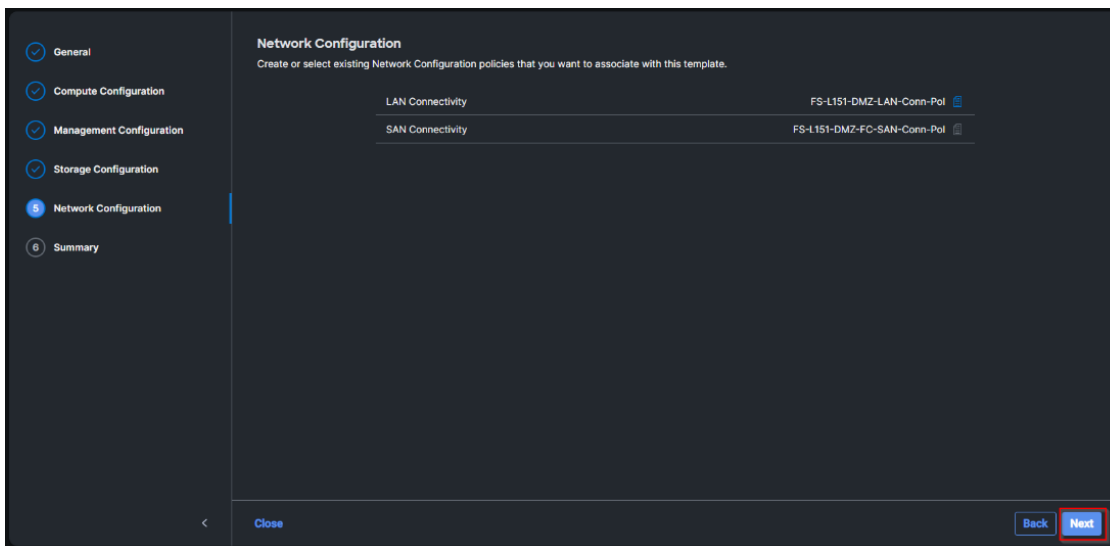


**Step 111.** Create the vHBA-B using the same steps from above using pools and Fibre Channel Network policy for SAN-B.

**Step 112.** Verify both vHBAs are added to the SAN connectivity policy.

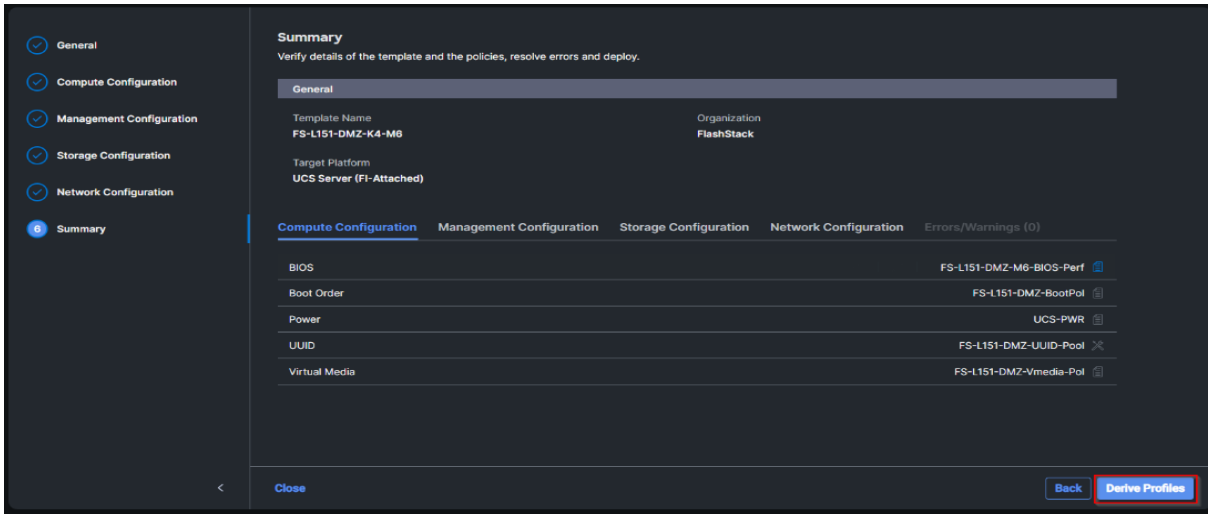


**Step 113.** When the LAN connectivity policy and SAN connectivity policy are created and assigned, click Next to move to the Summary screen.

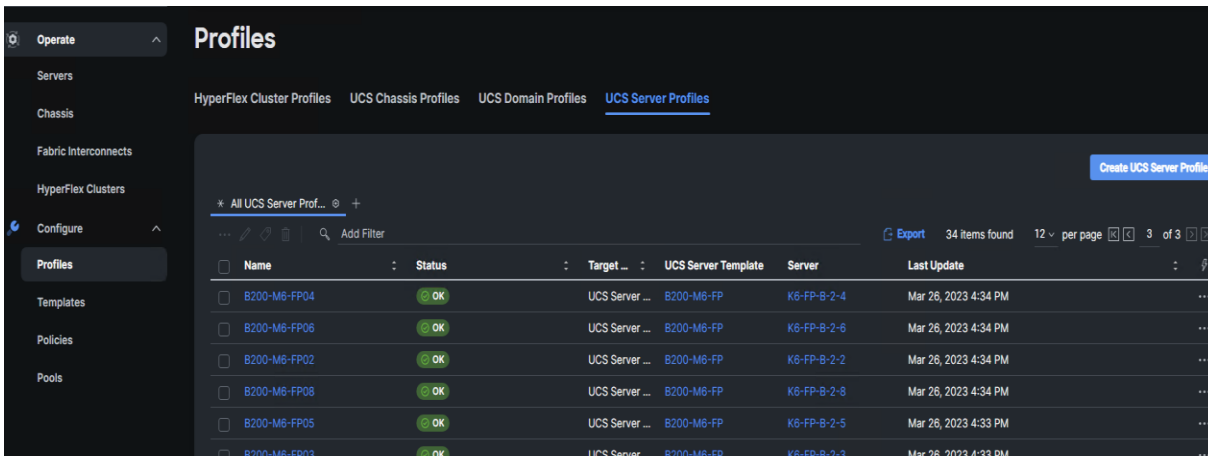


**Step 114.** From the Server profile template Summary screen, click Derive Profiles.

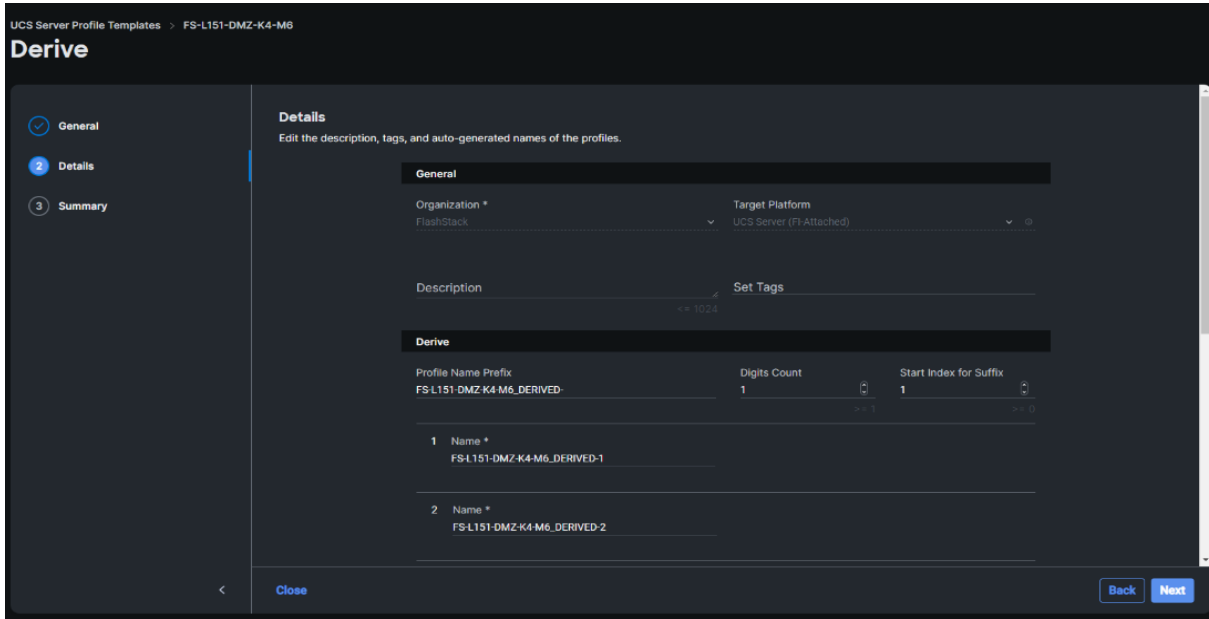
**Note:** This action can also be performed later by navigating to Templates, clicking “...” next to the template name and selecting Derive Profiles.



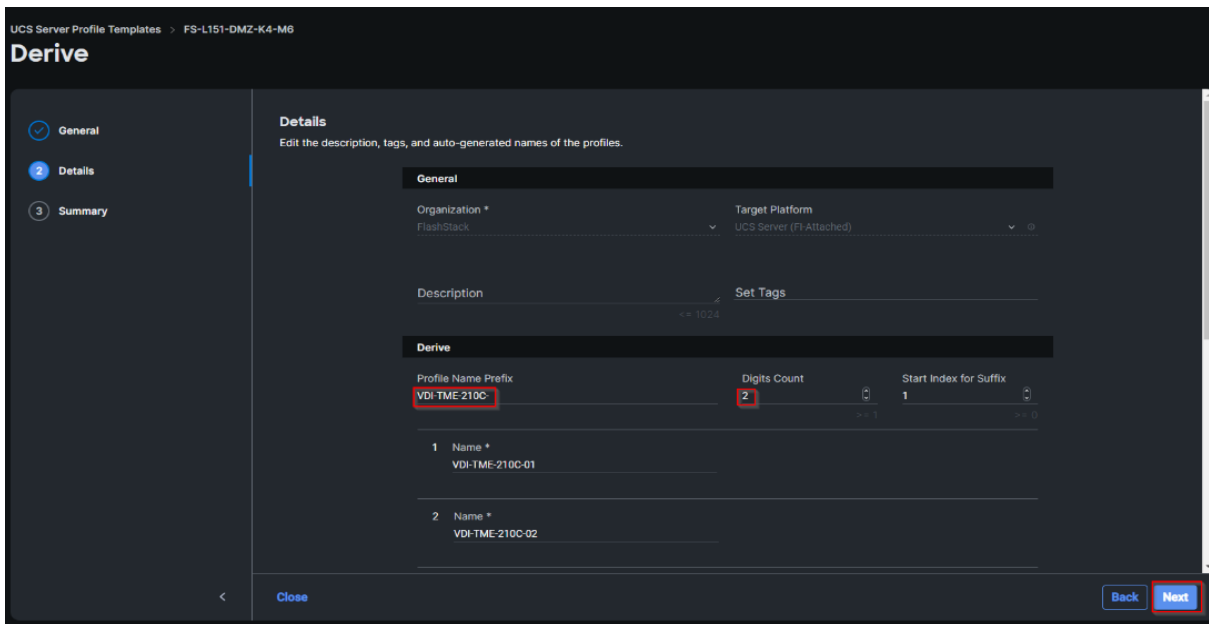
**Step 115.** Under the Server Assignment, select Assign Now and select Cisco UCS B200 M6 Nodes. You can select one or more servers depending on the number of profiles to be deployed. Click Next.



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



**Step 116.** Adjust the Prefix and number as needed. Click Next.



**Step 117.** Verify the information and click Derive to create the Server Profiles.

## Configure Cisco Nexus 93180YC-FX Switches

This section details the steps for the Cisco Nexus 93180YC-FX switch configuration.

### Procedure 1. Configure Global Settings for Cisco Nexus A and Cisco Nexus B

**Step 1.** Log in as admin user into the Cisco Nexus Switch A and run the following commands to set global configurations and jumbo frames in QoS:

```
conf terminal
policy-map type network-qos jumbo
class type network-qos class-default
mtu 9216
exit
```

```

class type network-qos class-fcoe
pause no-drop
mtu 2158
exit
exit
system qos
service-policy type network-qos jumbo
exit
copy running-config startup-config

```

**Step 2.** Log in as admin user into the Cisco Nexus Switch B and run the same commands (above) to set global configurations and jumbo frames in QoS.

## Procedure 2. Configure VLANs for Cisco Nexus A and Cisco Nexus B Switches

**Note:** For this solution, we created VLAN 70, 71, 72, 73 and 76.

**Step 1.** Log in as admin user into the Cisco Nexus Switch A.

**Step 2.** Create VLAN 70:

```

config terminal
VLAN 70
name InBand-Mgmt
no shutdown
exit
copy running-config startup-config

```

**Step 3.** Log in as admin user into the Nexus Switch B and create VLANs.

## Virtual Port Channel (vPC) Summary for Data and Storage Network

In the Cisco Nexus 93180YC-FX switch topology, a single vPC feature is enabled to provide HA, faster convergence in the event of a failure, and greater throughput. Cisco Nexus 93180YC-FX vPC configurations with the vPC domains and corresponding vPC names and IDs for Oracle Database Servers is listed in [Table 12](#).

**Table 12.** vPC Summary

vPC Domain	vPC Name	vPC ID
50	Peer-Link	1
50	vPC Port-Channel to FI-A	11
50	vPC Port-Channel to FI-B	12

As listed in [Table 12](#), a single vPC domain with Domain ID 50 is created across two Cisco Nexus 93180YC-FX member switches to define vPC members to carry specific VLAN network traffic. In this topology, a total number of 3 vPCs were defined:

- vPC ID 1 is defined as Peer link communication between two Nexus switches in Fabric A and B.
- vPC IDs 11 and 12 are defined for traffic from Cisco UCS fabric interconnects.

## Cisco Nexus 93180YC-FX Switch Cabling Details

The following tables list the cabling information.

**Table 13.** Cisco Nexus 93180YC-FX-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93180YC-	Eth1/51	40Gbe	Cisco UCS fabric interconnect	Eth1/49

Local Device	Local Port	Connection	Remote Device	Remote Port
FX Switch A			B	
	Eth1/52	40Gbe	Cisco UCS fabric interconnect A	Eth1/49
	Eth1/1	10Gbe	Cisco Nexus 93180YC-FX B	Eth1/1
	Eth1/2	10Gbe	Cisco Nexus 93180YC-FX B	Eth1/2
	Eth1/3	10Gbe	Cisco Nexus 93180YC-FX B	Eth1/3
	Eth1/4	10Gbe	Cisco Nexus 93180YC-FX B	Eth1/4
	MGMT0	1Gbe	Gbe management switch	Any

**Table 14.** Cisco Nexus 93180YC-FX-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 93180YC-FX Switch B	Eth1/51	40Gbe	Cisco UCS fabric interconnect B	Eth1/50
	Eth1/52	40Gbe	Cisco UCS fabric interconnect A	Eth1/50
	Eth1/1	10Gbe	Cisco Nexus 93180YC-FX A	Eth1/1
	Eth1/2	10Gbe	Cisco Nexus 93180YC-FX A	Eth1/2
	Eth1/3	10Gbe	Cisco Nexus 93180YC-FX A	Eth1/3
	Eth1/4	10Gbe	Cisco Nexus 93180YC-FX A	Eth1/4
	MGMT0	1Gbe	Gbe management switch	Any

## Cisco UCS Fabric Interconnect 6454 Cabling

The following tables list the FI 6454 cabling information.

**Table 15.** Cisco UCS Fabric Interconnect (FI) A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS FI-6454-A	FC 1/1	32G FC	Cisco MDS 9132T 32-Gb-A	FC 1/13
	FC 1/2	32G FC	Cisco MDS 9132T 32-Gb-A	FC 1/14
	Eth1/17-18	25Gbe	UCS 5108 Chassis IFM-A Chassis 1	Intelligent Fabric Module 1 Port1-2
	Eth1/49	40Gbe	Cisco Nexus 93180YC-FX Switch A	Eth1/52

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/50	40Gbe	Cisco Nexus 93180YC-FX Switch B	Eth1/52
	Mgmt 0	1Gbe	Management Switch	Any
	L1	1Gbe	Cisco UCS FI - A	L1
	L2	1Gbe	Cisco UCS FI - B	L2

**Table 16.** Cisco UCS Fabric Interconnect (FI) B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS FI-6454-B	FC 1/1	32Gb FC	Cisco MDS 9132T 32-Gb-B	FC 1/13
	FC 1/2	32Gb FC	Cisco MDS 9132T 32-Gb-B	FC 1/14
	Eth1/17-18	25Gbe	UCS 5108 Chassis IFM-B Chassis 1	Intelligent Fabric Module 1 Port1-2
	Eth1/49	40Gbe	Cisco Nexus 93180YC-FX Switch A	Eth1/51
	Eth1/50	40Gbe	Cisco Nexus 93180YC-FX Switch B	Eth1/51
	Mgmt 0	1Gbe	Management Switch	Any
	L1	1Gbe	Cisco UCS FI - A	L1
	L2	1Gbe	Cisco UCS FI - B	L2

### Procedure 1. Create vPC Peer-Link Between the Two Cisco Nexus Switches

**Step 1.** Log in as “admin” user into the Cisco Nexus Switch A.

**Note:** For vPC 1 as Peer-link, we used interfaces 53-54 for Peer-Link. You may choose the appropriate number of ports for your needs.

**Step 2.** Create the necessary port channels between devices by running these commands on both Cisco Nexus switches:

```

config terminal
feature vpc
feature lacp
vpc domain 50
peer-keepalive destination 173.37.52.104 source 173.37.52.103
exit
interface port-channel 10
description VPC peer-link
switchport mode trunk
switchport trunk allowed VLAN 1,70-76
spanning-tree port type network
vpc peer-link
interface Ethernet1/1
description VPC to K23-N9K-A

```

```
switchport mode trunk
switchport trunk allowed vlan 1,70-76,132
channel-group 10 mode active
no shutdown
exit
```

```
interface Ethernet1/2
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,70-76,132
channel-group 10 mode active
no shutdown
exit
```

```
interface Ethernet1/3
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,70-76,132
channel-group 10 mode active
no shutdown
exit
```

```
interface Ethernet1/4
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,70-76,132
channel-group 10 mode active
no shutdown
exit
copy running-config startup-config
```

**Step 3.** Log in as admin user into the Nexus Switch B and repeat the above steps to configure second Cisco Nexus switch.

**Step 4.** Make sure to change the peer-keepalive destination and source IP address appropriately for Cisco Nexus Switch B.

## Procedure 2. Create vPC Configuration Between Cisco Nexus 93180YC-FX and Cisco Fabric Interconnects

Create and configure vPC 11 and 12 for the data network between the Cisco Nexus switches and fabric interconnects.

**Note:** Create the necessary port channels between devices, by running the following commands on both Cisco Nexus switches.

**Step 1.** Log in as admin user into Cisco Nexus Switch A and enter the following:

```
config terminal
interface port-channel11
description FI-A-Uplink
switchport mode trunk
switchport trunk allowed VLAN 1,70-76
spanning-tree port type edge trunk
vpc 11
no shutdown
exit
interface port-channel12
description FI-B-Uplink
switchport mode trunk
switchport trunk allowed VLAN 1,70-76
spanning-tree port type edge trunk
vpc 12
no shutdown
exit
interface Ethernet1/51
description FI-A-Uplink
switch mode trunk
switchport trunk allowed vlan 1,70-76
spanning-tree port type edge trunk
```



```
mtu 9216
channel-group 11 mode active
no shutdown
exit
interface Ethernet1/52
description FI-B-Uplink
switch mode trunk
switchport trunk allowed vlan 1,70-76
spanning-tree port type edge trunk
mtu 9216
channel-group 12 mode active
no shutdown
exit
copy running-config startup-config
```

**Step 2.** Log in as admin user into the Nexus Switch B and complete the following for the second switch configuration:

```
config Terminal
interface port-channel11
description FI-A-Uplink
switchport mode trunk
switchport trunk allowed VLAN 1,70-76
spanning-tree port type edge trunk
vpc 11
no shutdown
exit
interface port-channel12
description FI-B-Uplink
switchport mode trunk
switchport trunk allowed VLAN 1,70-76
spanning-tree port type edge trunk
vpc 12
no shutdown
exit
interface Ethernet1/51
description FI-A-Uplink
switch mode trunk
switchport trunk allowed vlan 1,70-76
spanning-tree port type edge trunk
mtu 9216
channel-group 11 mode active
no shutdown
exit
interface Ethernet1/52
description FI-B-Uplink
switch mode trunk
switchport trunk allowed vlan 1,70-76
spanning-tree port type edge trunk
mtu 9216
channel-group 12 mode active
no shutdown
exit
copy running-config startup-config
```

**Verify all vPC Status is up on both Cisco Nexus Switches**

[Figure 21](#) shows the verification of the vPC status on both Cisco Nexus Switches.

**Figure 21. vPC Description for Cisco Nexus Switch A and B**

```

M23-N9K-A# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 50
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role               : secondary
Number of vPCs configured : 4
Peer Gateway           : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Enabled, timer is off.(timeout = 240s)
Delay-restore status   : Timer is off.(timeout = 150s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode  : Disabled

vPC Peer-link status
-----
id  Port  Status Active vlans
--  --  ---  -
1   Po10  up    1,50-56,70-76

vPC status
-----
id  Port  Status Consistency Reason      Active vlans
--  --  ---  -
11  Po11  up    success success                1,50-56,70-76
12  Po12  up    success success                1,50-56,70-76

M23-N9K-B# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 50
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role               : primary
Number of vPCs configured : 4
Peer Gateway           : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status   : Enabled, timer is off.(timeout = 240s)
Delay-restore status   : Timer is off.(timeout = 150s)
Delay-restore SVI status : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router : Disabled
Virtual-peerlink mode  : Disabled

vPC Peer-link status
-----
id  Port  Status Active vlans
--  --  ---  -
1   Po10  up    1,50-56,70-76

vPC status
-----
id  Port  Status Consistency Reason      Active vlans
--  --  ---  -
11  Po11  up    success success                1,50-56,70-76
12  Po12  up    success success                1,50-56,70-76
    
```

## Cisco MDS 9132T 32-Gb FC Switch Configuration

Figure 20 illustrates the cable connectivity between the Cisco MDS 9132T 32-Gb switch and the Cisco 6454 Fabric Interconnects and Pure Storage FlashArray//X70 R3 storage.

**Note:** We used two 32Gb FC connections from each fabric interconnect to each MDS switch and two 32Gb FC connections from each Pure Storage FlashArray//X70 R3 array controller to each MDS switch.

**Table 17.** Cisco MDS 9132T-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9132T-A	FC1/9	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 0	CT0.FC0
	FC1/10	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 1	CT1.FC0
	FC1/13	32Gb FC	Cisco 6454 Fabric Interconnect-A	FC1/1
	FC1/14	32Gb FC	Cisco 6454 Fabric Interconnect-A	FC1/2

**Table 18.** Cisco MDS 9132T-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9132T-B	FC1/9	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 0	CT0.FC2
	FC1/10	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 1	CT1.FC2
	FC1/13	32Gb FC	Cisco 6454 Fabric Interconnect-B	FC1/1
	FC1/14	32Gb FC	Cisco 6454 Fabric Interconnect-B	FC1/2

## Pure Storage FlashArray//X70 R3 to MDS SAN Fabric Connectivity

### Pure Storage FlashArray//X70 R3 to MDS A and B Switches using VSAN 100 for Fabric A and VSAN 101 Configured for Fabric B

In this solution, two ports (ports FC1/9 and FC1/10) of MDS Switch A and two ports (ports FC1/9 and FC1/10) of MDS Switch B are connected to Pure Storage System as listed in [Table 19](#). All ports connected to the Pure Storage Array carry 32 Gb/s FC Traffic.

**Table 19.** MDS 9132T 32-Gb switch Port Connection to Pure Storage System

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9132T-A	FC1/9	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 0	CT0.FC0
	FC1/10	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 1	CT1.FC0
Cisco MDS 9132T-B	FC1/9	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 0	CT0.FC2
	FC1/10	32Gb FC	Pure Storage FlashArray//X70 R3 Controller 1	CT1.FC2

#### Procedure 1. Configure Features and name for MDS Switch A and MDS Switch B

Follow these steps on both MDS switches.

**Step 1.** Log in as admin user into MDS Switch A:

```
config terminal
feature npiv
feature telnet
switchname FlashStack-MDS-A
copy running-config startup-config
```

**Step 2.** Log in as admin user into MDS Switch B. Repeat step 1 on MDS Switch B.

#### Procedure 2. Configure VSANs for MDS Switch A and MDS Switch B

**Step 1.** Log in as admin user into MDS Switch A. Create VSAN 100 for Storage Traffic:

```
config terminal
VSAN database
vsan 100
exit
zone smart-zoning enable vsan 100
vsan database
vsan 100 interface fc 1/9-16
exit
interface fc 1/9-16
switchport trunk allowed vsan 100
switchport trunk mode off
port-license acquire
no shutdown
exit
copy running-config startup-config
```

**Step 2.** Log in as admin user into MDS Switch B. Create VSAN 101 for Storage Traffic:

```
config terminal
VSAN database
vsan 101
```

```

exit
zone smart-zoning enable vsan 101
vsan database
vsan 101 interface fc 1/9-16
exit
interface fc 1/9-16
switchport trunk allowed vsan 101
switchport trunk mode off
port-license acquire
no shutdown
exit
copy running-config startup-config

```

### Procedure 3. Create and Configure Fiber Channel Zoning

This procedure sets up the Fibre Channel connections between the Cisco MDS 9132T 32-Gb switches, the Cisco UCS Fabric Interconnects, and the Pure Storage FlashArray systems.

**Note:** Before you configure the zoning details, decide how many paths are needed for each LUN and extract the WWPN numbers for each of the HBAs from each server. We used 2 HBAs for each Server. One of the HBAs (HBA-A) is connected to MDS Switch-A and other HBAs (HBA-B) is connected to MDS Switch-B.

**Step 1.** Log into the Cisco Intersight portal as a user with account administrator role.

**Step 2.** From the Service Selector drop-down list, choose Infrastructure Service.

**Step 3.** Navigate to Configure > Pools. Filter WWPN type pools.

The screenshot shows the Cisco Intersight 'Pools' configuration page. The left-hand navigation menu has 'Configure' and 'Pools' highlighted. The main area features a search bar labeled 'Search WWPN' and a table of pool configurations. The table has columns for Name, Type, Size, Used, Available, Reserved, Description, and Last Update. Two WWPN pools are listed:

Name	Type	Size	Used	Available	Reserved	Description	Last Update
FS-151-DM2-WWPN-Pool-B	WWPN	64	8	56	0		7 minutes ago
FS-151-DM2-WWPN-Pool-A	WWPN	64	8	56	0		7 minutes ago

**Step 4.** Select Usage tab and collect the WWPNs and profiles to which they are assigned.

**FS-L151-DMZ-WWPN-Pool-A** Actions

**Details**

Name  
FS-L151-DMZ-WWPN-Pool-A

Type  
WWPN

Size  
8

Used  
8

Reserved  
0

Available  
0

Last Update  
Feb 14, 2023 2:08 PM

Description  
-

Organization  
FlashStack

**Configuration & Usage**

Export 8 Items found 21 per page 1 of 1

**Status**

8 Used 8

Identifier	Status	Server Profile
20:00:00:25:B5:AA:17:00	Used	FS-L151-DMZ-K4-M6_DERIVED-1
20:00:00:25:B5:AA:17:01	Used	FS-L151-DMZ-K4-M6_DERIVED-2
20:00:00:25:B5:AA:17:02	Used	FS-L151-DMZ-K4-M6_DERIVED-3
20:00:00:25:B5:AA:17:03	Used	FS-L151-DMZ-K4-M6_DERIVED-4
20:00:00:25:B5:AA:17:04	Used	FS-L151-DMZ-K4-M6_DERIVED-5
20:00:00:25:B5:AA:17:05	Used	FS-L151-DMZ-K4-M6_DERIVED-6
20:00:00:25:B5:AA:17:06	Used	FS-L151-DMZ-K4-M6_DERIVED-7
20:00:00:25:B5:AA:17:07	Used	FS-L151-DMZ-K4-M6_DERIVED-8

**Step 5.** Connect to the Pure Storage System Health and go to the Connections tab and extract the WWPN of FC Ports connected to the Cisco MDS Switches from Array Ports section.

**Note:** We connected 4 FC ports from Pure Storage System to Cisco MDS Switches. FC ports CT0.FC0, CT1.FC0 are connected to MDS Switch-A and similarly FC ports CT1.FC2, CT0.FC2 are connected to MDS Switch-B.

FC Port	Name	Speed	Fallover	FC Port	Name	Speed	Fallover
CT0.FC0	52:4A:93:71:56:84:09:00	32 Gb/s		CT1.FC0	52:4A:93:71:56:84:09:10	32 Gb/s	
CT0.FC1	52:4A:93:71:56:84:09:01	0		CT1.FC1	52:4A:93:71:56:84:09:11	0	
CT0.FC2	52:4A:93:71:56:84:09:02	32 Gb/s		CT1.FC2	52:4A:93:71:56:84:09:12	32 Gb/s	
CT0.FC3	52:4A:93:71:56:84:09:03	0		CT1.FC3	52:4A:93:71:56:84:09:13	0	
CT0.FC8	52:4A:93:71:56:84:09:08	0		CT1.FC8	52:4A:93:71:56:84:09:18	0	
CT0.FC9	52:4A:93:71:56:84:09:09	0		CT1.FC9	52:4A:93:71:56:84:09:19	0	

**Procedure 4.** Create Device Aliases for Fiber Channel Zoning for SAN Boot Paths and Datapaths on Cisco MDS Switch A

**Step 1.** Log in as admin user and run the following commands from the global configuration mode:

```

configure terminal
device-alias mode enhanced
device-alias database
device-alias name Host-FCP-1-HBA0 pwwn 20:00:00:25:B5:AA:17:00
device-alias name X70R3-CT0-FC0 pwwn 52:4A:93:71:56:84:09:00
device-alias name X70R3-CT1-FC0 pwwn 52:4A:93:71:56:84:09:10
exit
device-alias commit

```

**Procedure 5.** Create Device Aliases for Fiber Channel Zoning for SAN Boot Paths and Datapaths on Cisco MDS Switch B

**Step 1.** Log in as admin user and run the following commands from the global configuration mode:

```

configure terminal

```

```
device-alias mode enhanced
device-alias database
device-alias name Host-FCP-1-HBA1 pwnn 20:00:00:25:b5:bb:17:00
device-alias name X70R3-CT0-FC2 pwnn 52:4A:93:71:56:84:09:02
device-alias name X70R3-CT1-FC2 pwnn 52:4A:93:71:56:84:09:12
exit
device-alias commit
```

## Procedure 6. Create Fiber Channel Zoning for Cisco MDS Switch A for each Service Profile

**Step 1.** Log in as admin user and create the zone:

```
configure terminal
zone name FlashStack-Fabric-A vsan 100
  member device-alias X70R3-CT0-FC0 target
  member device-alias X70R3-CT1-FC0 target
  member device-alias Host-FCP-1-HBA0 init
```

**Step 2.** After the zone for the Cisco UCS service profile has been created, create the zone set and add the created zones as members:

```
configure terminal
zoneset name VDI-Fabric-A vsan 100
  member FlashStack-Fabric-A
```

**Step 3.** Activate the zone set by running following commands:

```
zoneset activate name VDI-Fabric-A vsan 100
exit
copy running-config startup-config
```

## Procedure 7. Create Fiber Channel Zoning for Cisco MDS Switch B for each Service Profile

**Step 1.** Log in as admin user and create the zone as shown below:

```
configure terminal zone name FlashStack-Fabric-B vsan 101
  member device-alias X70R3-CT0-FC2 target
  member device-alias X70R3-CT1-FC2 target
  member device-alias Host-FCP-1-HBA1 init
```

**Step 2.** After the zone for the Cisco UCS service profile has been created, create the zone set and add the necessary members:

```
zoneset name VDI-Fabric-B vsan 101
  member FlashStack-Fabric-B
```

**Step 3.** Activate the zone set by running following commands:

```
zoneset activate name VDI-Fabric-B vsan 101
exit
copy running-config startup-config
```

## Configure Pure Storage FlashArray//X70 R3

The design goal of the reference architecture is to best represent a real-world environment as closely as possible. The approach included the features of Cisco UCS to rapidly deploy stateless servers and use Pure Storage FlashArray's boot LUNs to provision the ESXi on top of Cisco UCS. Zoning was performed on the Cisco MDS 9132T 32-Gb switches to enable the initiators to discover the targets during the boot process.

A Service Profile was created within Cisco UCS Manager to deploy the thirty-two servers quickly with a standard configuration. SAN boot volumes for these servers were hosted on the same Pure Storage FlashArray//X70 R3. Once the stateless servers were provisioned, the following process was performed to enable rapid deployment of thirty-two blade servers.

---

Each Blade Server has dedicated single LUN to install operating system and all the thirty-two Blade Servers configured to boot from SAN. For this solution, we installed VMware vSphere ESXi 7.0 Update 3d Cisco Custom ISO on these LUNs.

Using logical servers that are disassociated from the physical hardware removes many limiting constraints around how servers are provisioned. Cisco UCS Service Profiles contain values for a server's property settings, including virtual network interface cards (vNICs), MAC addresses, boot policies, firmware policies, fabric connectivity, external management, and HA information. The service profiles represent all the attributes of a logical server in Cisco UCS model. By abstracting these settings from the physical server into a Cisco Service Profile, the Service Profile can then be deployed to any physical compute hardware within the Cisco UCS domain. Furthermore, Service Profiles can, at any time, be migrated from one physical server to another. Cisco is the only hardware provider to offer a truly unified management platform, with Cisco UCS Service Profiles and hardware abstraction capabilities extending to both blade and rack servers.

In addition to the service profiles, using Pure Storage FlashArray with SAN boot policy provides the following benefits:

- Scalability - Rapid deployment of new servers to the environment in a very few steps.
- Manageability - Enables seamless hardware maintenance and upgrades without any restrictions. This is a huge benefit in comparison to another appliance model like Exadata.
- Flexibility - Easy to repurpose physical servers for different applications and services as needed.
- Availability - Hardware failures are not impactful and critical. In the rare case of a server failure, it is easier to associate the logical service profile to another healthy physical server to reduce the impact.

## Configure Host, WWNs, and Volume Connectivity with FlashArray Management Tools

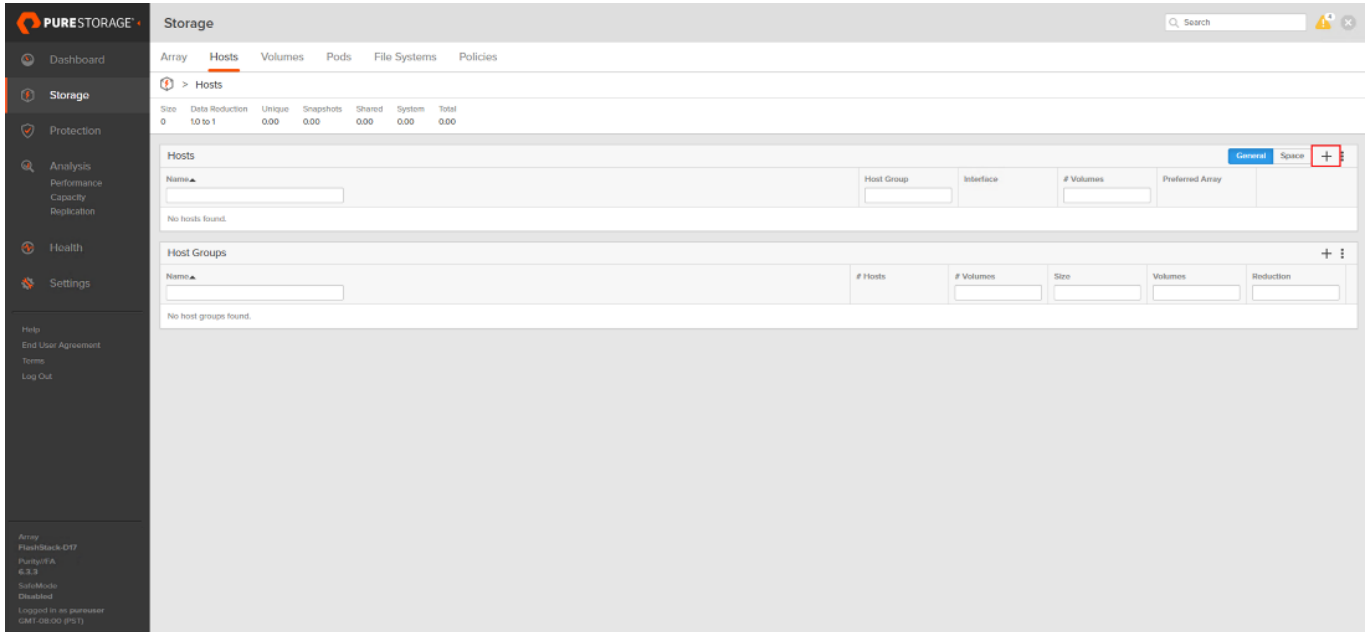
### Procedure 1. Configure Host

**Note:** Before using a boot volume (LUN) by a Cisco UCS Blade Server, a host representing this blade server must be defined on Pure Storage FlashArray.

**Step 1.** Log into Pure Storage FlashArray Management interface.

**Step 2.** Click the Storage tab.

**Step 3.** Click the + sign in the Hosts section and select Create Host.



**Step 4.** Click Create Multiple to create a Host entries under the Hosts category.

### Create Host

**Name**

**Step 5.** Enter the required information and click Create.

### Create Multiple Hosts

**Name**

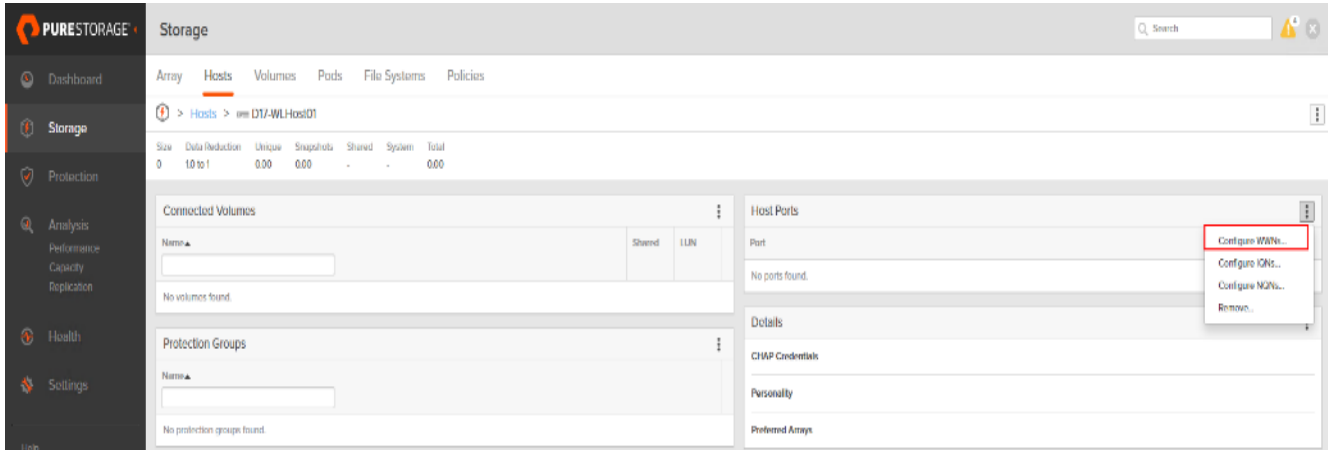
**Start Number**

**Count**

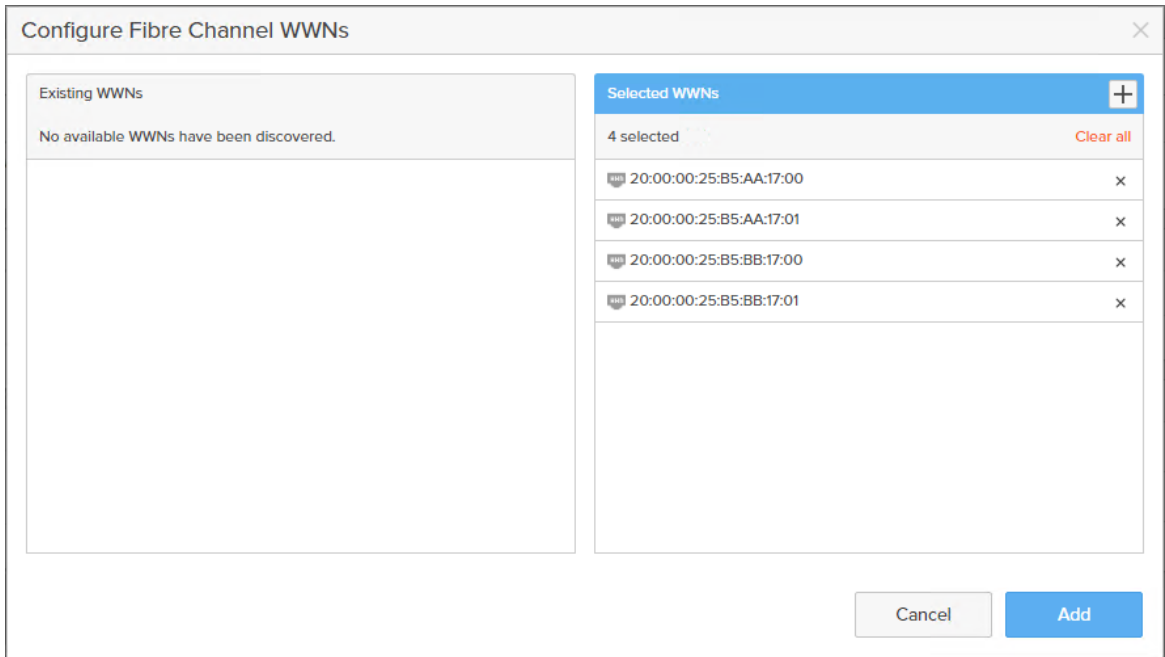
**Number of Digits**

**Step 6.** Select one of the newly created hosts, in the Host Ports section from the drop-down list select Configure WWNs.





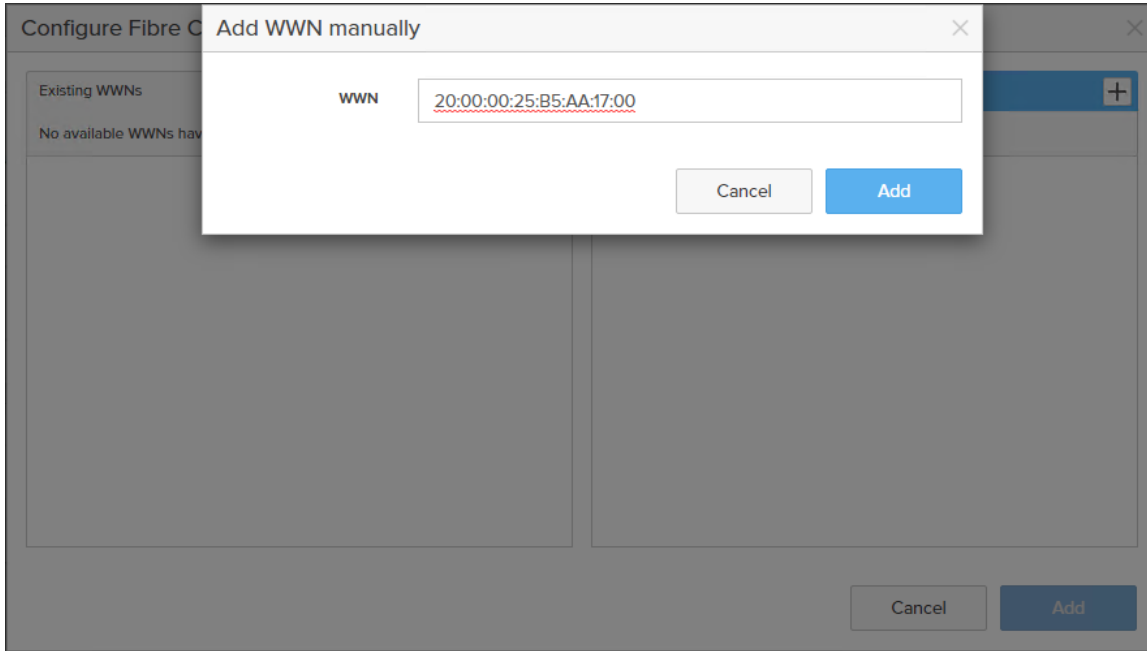
**Step 7.** Select the list of WWNs that belong to the host in the next window and click Add.



**Note:** Make sure the zoning has been setup to include the WWNs details of the initiators along with the target, without which the SAN boot will not work.

**Note:** WWNs will appear only if the appropriate FC connections were made, and the zones were setup on the underlying FC switch.

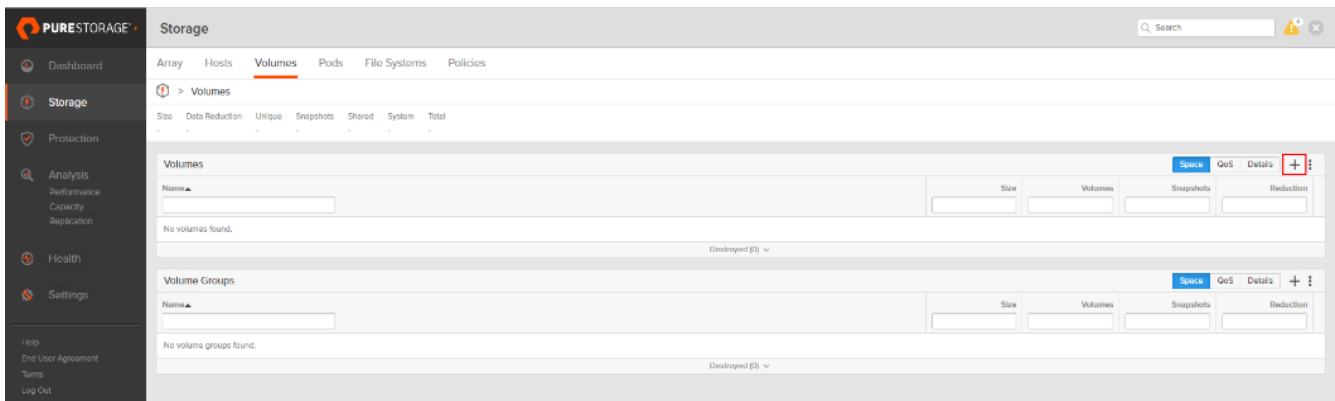
**Note:** Alternatively, the WWN can be added manually by clicking the + in the Selected WWNs section and manually inputting the blade's WWNs.



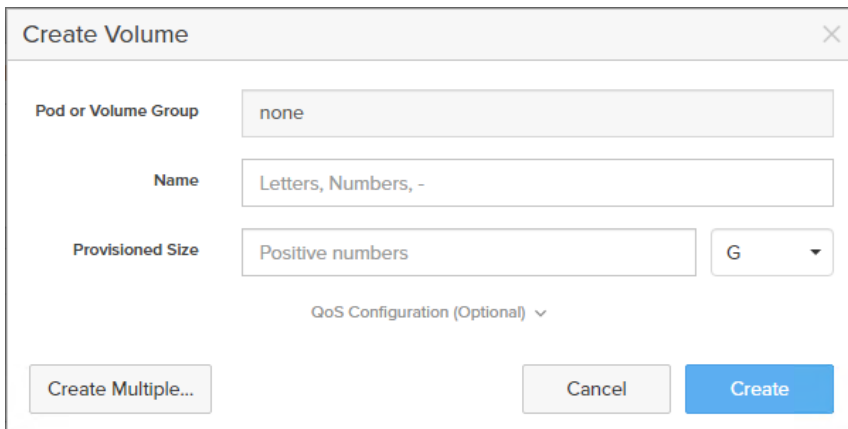
## Procedure 2. Configure Volume Connectivity

**Step 1.** Click the Storage tab.

**Step 2.** Click the + sign in the Volumes section and click Create Volume.



**Step 3.** Click Create Multiple to open Create Multiple Volumes wizard.



**Step 4.** Provide the common name of the volume, size, choose the size type (KB, MB, GB, TB, PB) and click Create to create volumes.

Create Multiple Volumes
✕

**Pod or Volume Group**

**Name**

**Provisioned Size**  G

**Start Number**

**Count**

**Number of Digits**

QoS Configuration (Optional) ▾

Create Single...
Cancel
Create

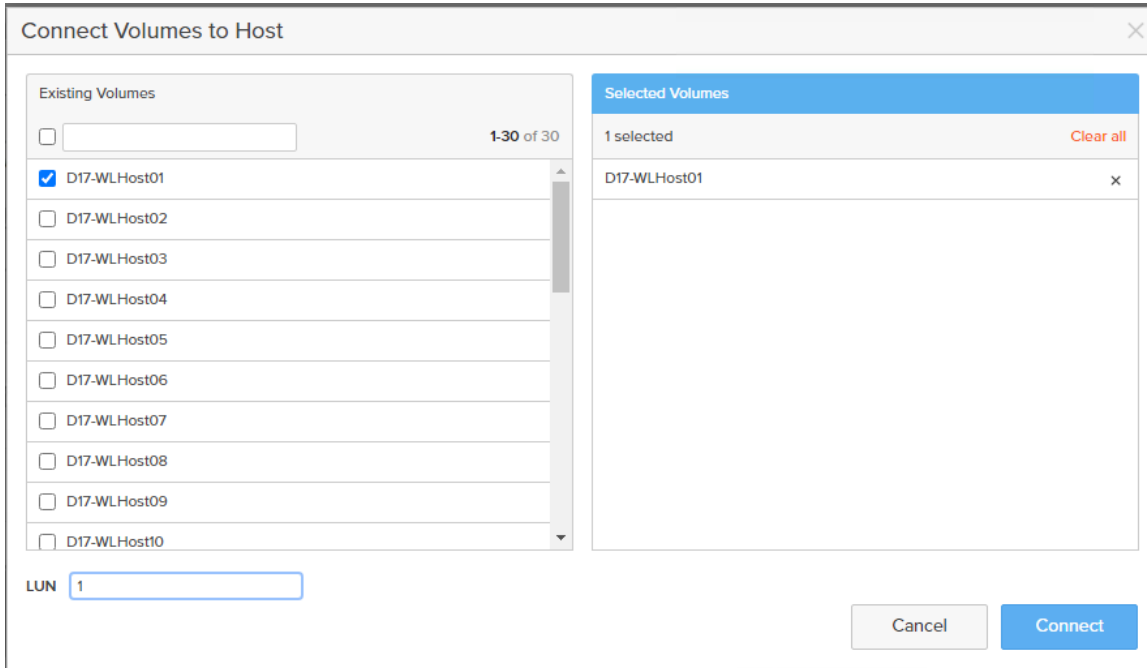
**Step 5.** Select one of the hosts and in the Connected Volumes section, from the drop-down list, select Connect.

The screenshot shows the Pure Storage console interface. The main content area is titled 'Hosts' and shows details for 'D17-WLHost01'. A table at the top shows storage metrics. Below this, there are sections for 'Connected Volumes', 'Protection Groups', and 'Host Ports'. The 'Connected Volumes' section has a dropdown menu open with 'Connect...' selected. The 'Host Ports' section shows a table with four entries, each with a port name, IP address, and MAC address.

Size	Data Reduction	Unique	Snapshots	Shared	System	Total
0	10 to 1	0.00	0.00	-	-	0.00

Port	IP	MAC	Actions
20:00:00:25:B5:AA:07:00	20:00:00:25:B5:AA:07:01	20:00:00:25:B5:BB:07:00	🔗 ✕
20:00:00:25:B5:AA:07:01	20:00:00:25:B5:BB:07:00	20:00:00:25:B5:BB:07:01	🔗 ✕

**Step 6.** In the Connect Volumes to Host wizard select the volume configured for ESXi installation, click Connect.



**Note:** Make sure the SAN Boot Volumes has the LUN ID “1” since this is important while configuring Boot from SAN. You will also configure the LUN ID as “1” when configuring Boot from SAN policy in Cisco UCS Manager.

**Note:** More LUNs can be connected by adding a connection to existing or new volume(s) to an existing node.

### Configure File Services

Pure Storage Technical Services (Support) can activate FA File services. Please refer to [FA File Services Support Matrix](#) to verify that your hardware offers support for running File Services.

Currently all FA File services activations require Pure Storage Product Management approval. Customers can work with their local account representatives to obtain approval to activate File Services.

For additional information on FA File Services setup and configuration see:

- [FA File Services Quick Start Guide](#)
- [FA File Services Best Practices](#)

### Procedure 1. Create Virtual Interface(s)

The VIF provides high-availability network access across 2 physical Ethernet ports per array controller. Each VIF requires 2 physical ports per controller. Any physical ethernet port can be used with the restriction that any port that is in use by management services, a bond, or subnet configuration cannot be part of a VIF. For the maximum number of VIFs supported, please see the FA File Services Limits KB.

**Note:** VIFs are created by CLI over SSH, configured and enabled using the Management Console. An account with administrator privileges is required.

**Step 1.** Connect to the array via SSH.

**Step 2.** Run the following syntax to create the VIF on the array:

```
purenetwork create vif --subinterfacelist ct0.ethX,ct1.ethX,ct0.ethY,ct1.ethY <name of interface>
```

## Procedure 2. Configure and Enable the Virtual Interface for File Services

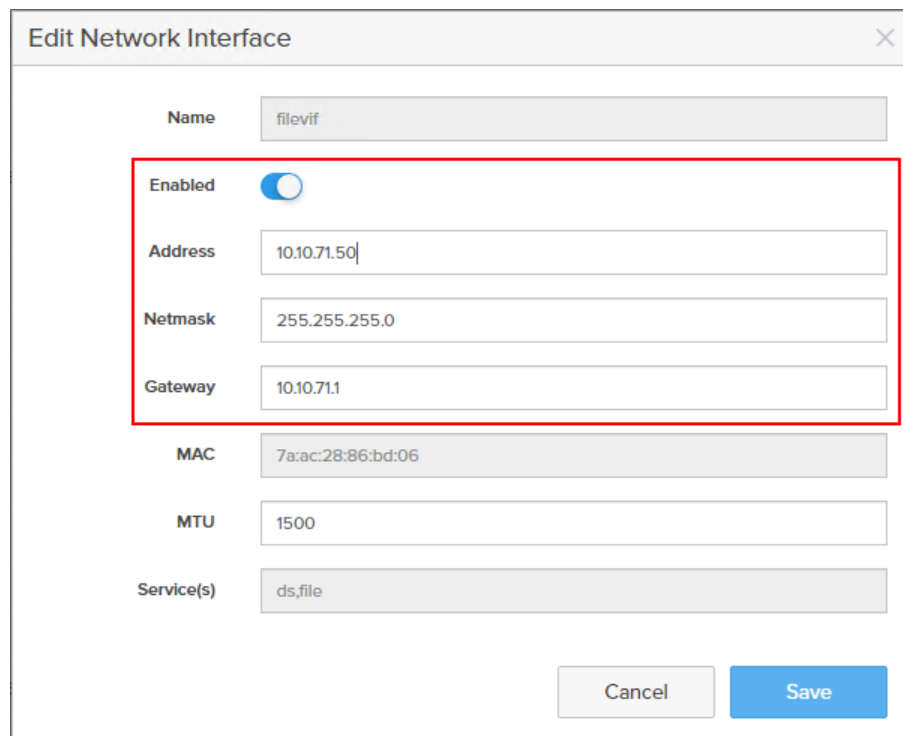
**Step 1.** Connect to the array GUI.

**Step 2.** Navigate to Settings > Network.

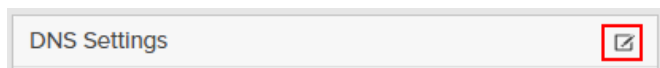
**Step 3.** Locate the File VIF in the interface list and click the edit icon.



**Step 4.** In the Edit Interface dialog turn on the Enabled option, provide the IP Address, Netmask, and Gateway used by the interface. Click Save.

A screenshot of the 'Edit Network Interface' dialog box. The dialog has a title bar with a close button. It contains several fields: 'Name' (filevif), 'Enabled' (a toggle switch that is turned on), 'Address' (10.10.71.50), 'Netmask' (255.255.255.0), 'Gateway' (10.10.71.1), 'MAC' (7a:ac:28:86:bd:06), 'MTU' (1500), and 'Service(s)' (ds,file). A red rectangle highlights the 'Enabled' toggle, the 'Address', 'Netmask', and 'Gateway' fields. At the bottom, there are 'Cancel' and 'Save' buttons.

**Step 5.** Scroll to the bottom of the Network tab and click the edit icon for DNS Settings.



**Step 6.** In the Edit DNS Settings dialog, enter desired values for Domain and DNS server IPs. Click Save.

**Edit DNS**

Domain: vccslab.local

DNS 1: 10.10.71.11

DNS 2:

DNS 3:

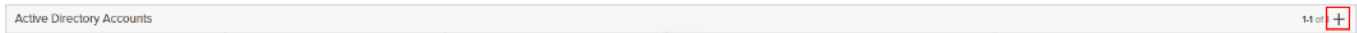
Cancel Save

**Note:** More than one DNS server can be configured with the caveat that all DNS servers must have a record for Directory Service servers such as LDAP or Microsoft Active Directory.

### Procedure 3. Create Active Directory Account for the Array

**Step 1.** Navigate to Settings > Access > Active Directory Accounts.

**Step 2.** To open the Create Dialog, click the + icon.



Enter the following information:

- Name = Array management name for this AD account
- Domain = AD domain name
- Computer Name = Computer Object name within AD
- User = Domain user that can create computer objects and join to the domain.
- Password = Users password for the above domain user

**Step 3.** Click Create to finalize AD account creation.

**Create Active Directory Account**

Name: purefile

Domain: vccslab.local

Computer Name: purefile

Kerberos Server:

Directory Server:

User: administrator@vccslab.local

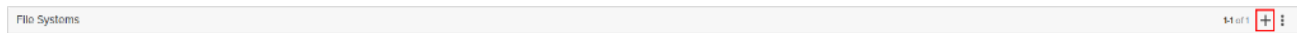
Password: .....

Cancel Create

### Procedure 4. Create a File System and Shared Directory

**Step 1.** Navigate to Storage > File Systems.

**Step 2.** Click the + icon.

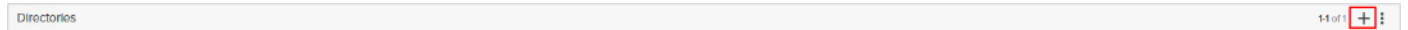


**Step 3.** In Create File System enter a file system name and click Create.

A dialog box titled 'Create File System' with a close button (X) in the top right corner. It contains a single text input field labeled 'Name' with the text 'vdi' entered. Below the field are two buttons: 'Cancel' and 'Create'.

**Step 4.** Navigate to Storage > File Systems > Directories.

**Step 5.** Click the + icon.



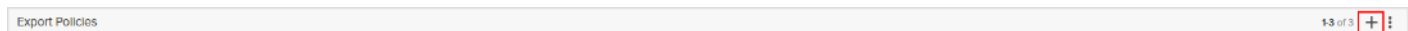
**Step 6.** In Create Directory, enter Select a file system from the drop-down list, enter the desired management name of the directory, and enter the directory path in the file system. (for example, dir or /dir, for sub-level directories /dir/subdir or /dir/subdir/subdir1 can be used). Click Create.

A dialog box titled 'Create Directory' with a close button (X) in the top right corner. It contains three text input fields: 'File System' with 'vdi', 'Name' with 'root', and 'Path' with '/'. Below the fields are two buttons: 'Cancel' and 'Create'.

**Note:** Policies for exports/shares/snapshots can only be attached to managed directories at the file system root or 1 level deep (/ and /dir in the example above). Space and performance metrics can be seen at all levels of managed directories.

**Step 7.** Navigate to Storage > Policies.

**Step 8.** Click the + icon.



**Step 9.** In the Create Export Policy pop-up choose SMB from the Type drop-down list and enter a name for the policy. Click Create.

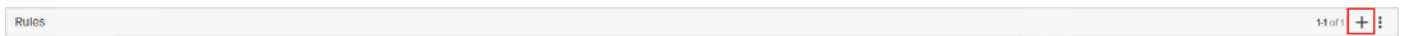
**Create Export Policy**

Type:

Name:

Enabled:

**Step 10.** Click Created Policy and click the + icon.



**Step 11.** Complete the Client filter for read-write access and click Add to complete the rule creation.

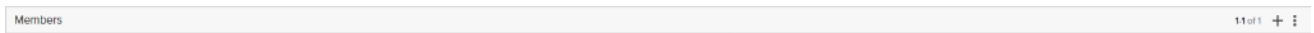
**Add Rule for Policy 'smb'**

Client:   
Hostname, IPv4 or IPv4 mask. e.g., \*, \*.cs.foo.edu, 192.168.255.255, or 192.168.10.0/24

Access:  no-anonymous-access  anonymous-access

Encryption:  optional-smb-encryption  smb-encryption

**Step 12.** Attach the export policy(s) to a managed directory. Click the + icon.



**Step 13.** Select a managed directory from the drop-down list, enter a share/export name, and click Create.

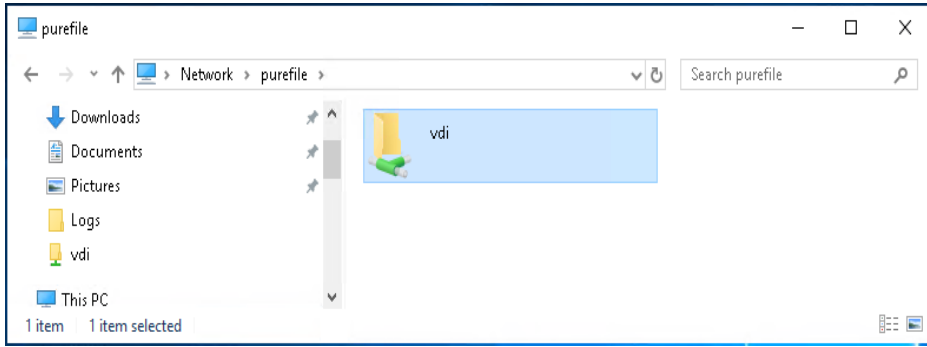
**Add Member to Policy 'smb'**

Directory:

Export Name:   
Name used to mount this path for clients to access

**Step 14.** Verify access to the created share from the Windows client.





## Install and Configure VMware ESXi 7.0

This section explains how to install VMware ESXi 7.0 Update 3d in an environment.

There are several methods to install 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 install ESXi on boot logical unit number (LUN). Upon completion of steps outlined here, ESXi hosts will be booted from their corresponding SAN Boot LUNs.

### Download Cisco Custom Image for VMware vSphere ESXi 7.0 U3d

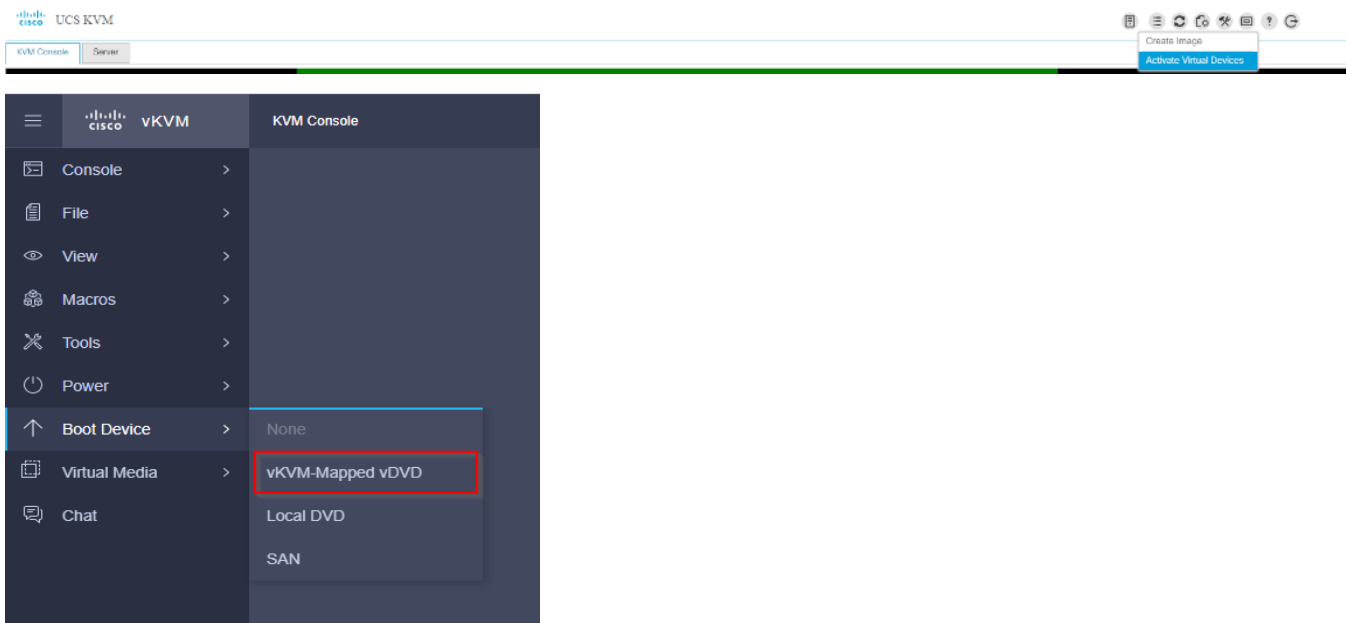
To download the Cisco Custom Image for VMware ESXi 7.0 Update 3d, from the [VMware vSphere Hypervisor 7.0 U3d](#) page click the Custom ISOs tab.

#### Procedure 1. Install VMware vSphere ESXi 7.0 U3d

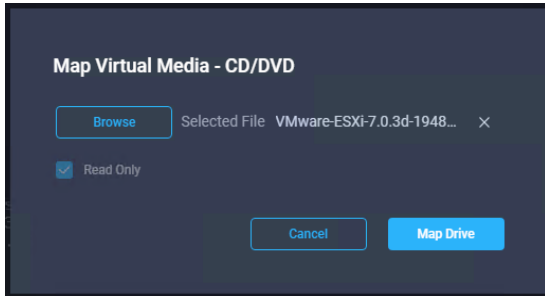
**Step 1.** From the Service Selector drop-down list, select Infrastructure Service. Navigate to Operate > Servers.

**Step 2.** Right-click on the ... icon for the server being access and select Launch vKVM.

**Step 3.** Click Boot Device and then select vKVM Mapped vDVD.

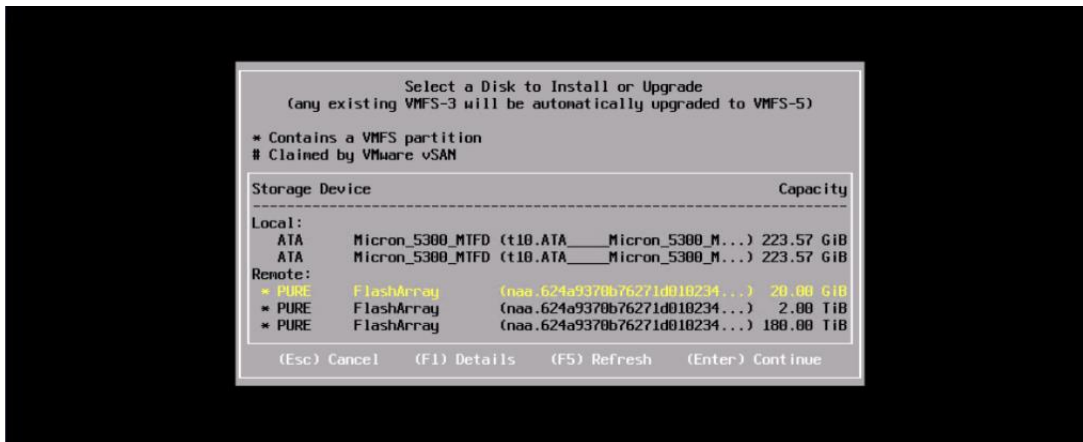


**Step 4.** Browse to the ESXi iso image file. Click Map Drive to mount the ESXi ISO image.



**Step 5.** Boot into ESXi installer and follow the prompts to complete installing VMware vSphere ESXi hypervisor.

**Step 6.** When selecting a storage device to install ESXi, select Remote LUN provisioned through Pure Storage Administrative console and access through FC connection.



## Procedure 2. Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host and connection to vCenter Server. Select the IP address that can communicate with existing or new vCenter Server.

**Step 1.** After the server has finished rebooting, press F2 to enter into configuration wizard for ESXi Hypervisor.

**Step 2.** Log in as root and enter the corresponding password.

**Step 3.** Select the Configure the Management Network option and press Enter.

**Step 4.** Select the VLAN (Optional) option and press Enter. Enter the VLAN In-Band management ID and press Enter.

**Step 5.** From the Configure Management Network menu, select IP Configuration and press Enter.

**Step 6.** Select the Set Static IP Address and Network Configuration option by using the space bar. Enter the IP address to manage the first ESXi host. Enter the subnet mask for the first ESXi host. Enter the default gateway for the first ESXi host. Press Enter to accept the changes to the IP configuration.

**Note:** IPv6 Configuration is set to automatic.

**Step 7.** Select the DNS Configuration option and press Enter.

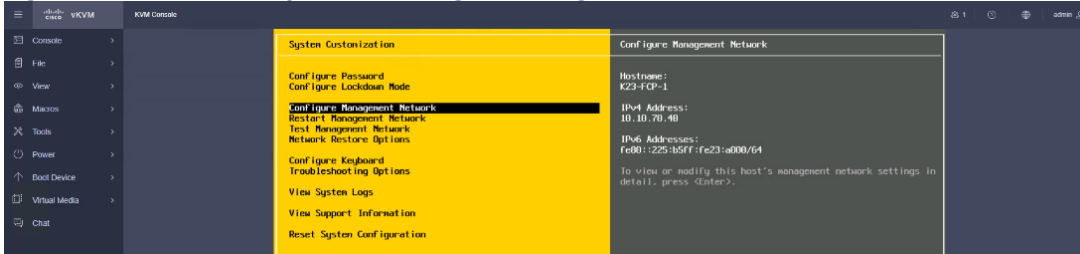
**Step 8.** Enter the IP address of the primary and secondary DNS server. Enter Hostname

**Step 9.** Enter DNS Suffixes.

**Note:** Since the IP address is assigned manually, the DNS information must also be entered manually.

**Note:** The steps provided vary based on the configuration. Please make the necessary changes according to your configuration.

**Figure 22.** Sample ESXi Configure Management Network

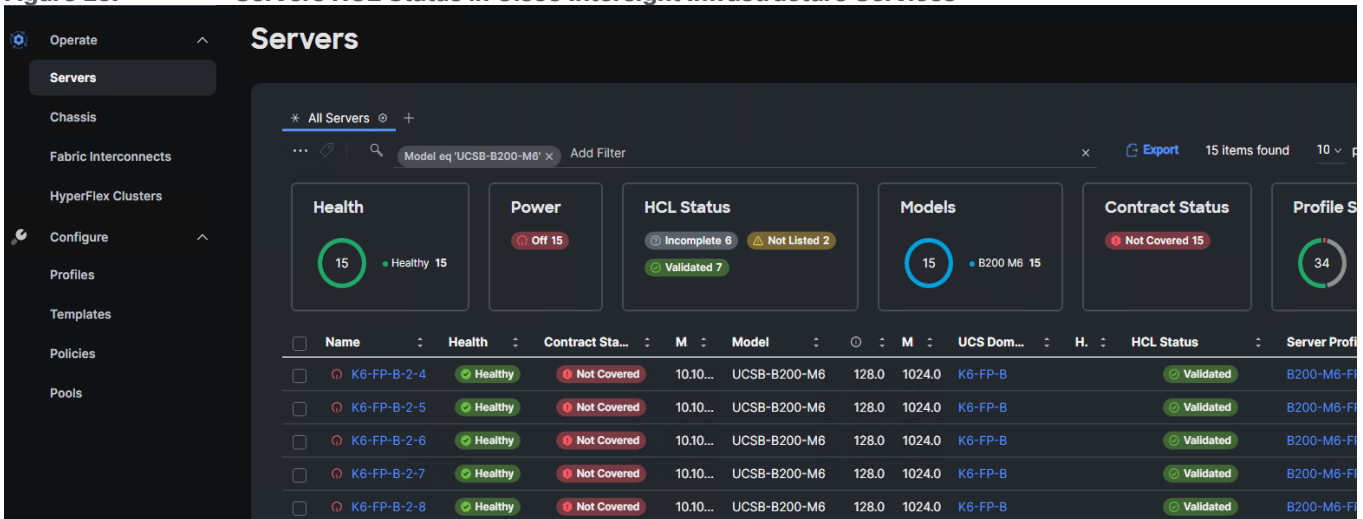


### Update Cisco VIC Drivers for ESXi

When ESXi is installed from Cisco Custom ISO, you might have to update the Cisco VIC drivers for VMware ESXi Hypervisor to match the current [Cisco Hardware and Software Interoperability Matrix](#).

Additionally, Cisco Intersight incorporates an HCL check.

**Figure 23.** Servers HCL Status in Cisco Intersight Infrastructure Services



In this Validated Design, the following drivers were used (VMware-ESXi-7.0.3d-19482537-Custom-Cisco-4.2.2-a):

- Cisco-nenic- 1.0.35.0
- Cisco-nfnic- 5.0.0.15

**Note:** For additional information on how to update Cisco VIC drivers on ESXi refer to the [Cisco UCS Virtual Interface Card Drivers for ESX Installation Guide](#).

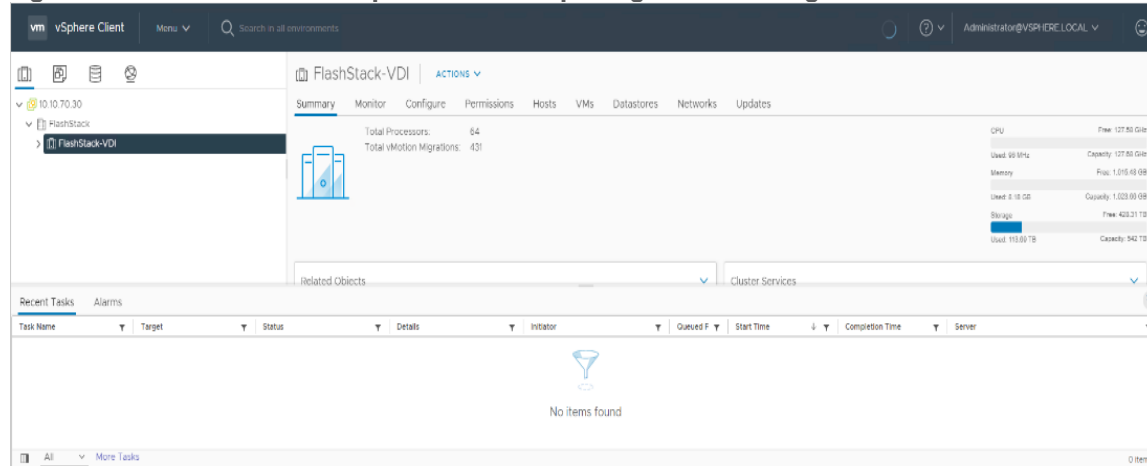
### VMware Clusters

The VMware vSphere Client was configured to support the solution and testing environment as follows:

- Datacenter: FlashStack - Pure Storage FlashArray//X70 R3 with Cisco UCS.
- Cluster: FlashStack-VDI - Single-session/Multi-session OS VDA workload.
- Infrastructure: Infrastructure virtual machines (vCenter, Active Directory, DNS, DHCP, SQL Server,) VMware Horizon Connection Server and Horizon Replica Servers, Login VSI launcher infrastructure and

work web servers were connected using the same set of switches but hosted on separate VMware cluster.

**Figure 24. VMware vSphere WebUI Reporting Cluster Configuration for this Validated Design**



## Cisco Intersight Orchestration

Cisco Intersight Assist helps you add endpoint devices to Cisco Intersight. FlashStack environment includes 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, and helps you add devices into Cisco Intersight.

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. You can install the appliance on an ESXi server. For more information, see the [Cisco Intersight Virtual Appliance Getting Started Guide](#).

After claiming Cisco Intersight Assist into Cisco Intersight, you can claim endpoint devices using the Claim Through Intersight Assist option.

### Procedure 1. Configure Cisco Intersight Assist Virtual Appliance

**Step 1.** To install Cisco Intersight Assist from an Open Virtual Appliance (OVA) in your VMware FlashStack-Management Cluster, first download the latest release of the OVA from: <https://software.cisco.com/download/home/286319499/type/286323047/release/1.0.9-342>.

**Step 2.** To set up the DNS entries for the Cisco Intersight Assist hostname as specified under Before you Begin, go to: [https://www.cisco.com/c/en/us/td/docs/unified\\_computing/Intersight/cisco-intersight-assist-getting-started-guide/m-installing-cisco-intersight-assist.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/cisco-intersight-assist-getting-started-guide/m-installing-cisco-intersight-assist.html).

**Step 3.** From Hosts and Clusters in the VMware vCenter HTML5 client, right-click the FlashStack-Management cluster and click Deploy OVF Template.

**Step 4.** Specify a URL or browse to the intersight-appliance-installer-vsphere-1.0.9-342.ova file. Click NEXT.

## Deploy OVF Template

### 1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

### Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

intersight-virtual-appliance-1.0.9-148.ova

**Step 5.** Name the Cisco Intersight Assist VM and choose the location. Click NEXT.

**Step 6.** Select the FlashStack-Management cluster and click NEXT.

**Step 7.** Review details and click NEXT.

**Step 8.** Select a deployment configuration (Tiny recommended) and click NEXT.

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Configuration**
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

### Configuration

Select a deployment configuration

	Description
<input type="radio"/> Small(16 vCPU, 32 Gi RAM)	Deployment size supports Intersight Assist only.
<input type="radio"/> Medium(24 vCPU, 64 Gi RAM)	
<input checked="" type="radio"/> Tiny(8 vCPU, 16 Gi RAM)	

3 Items

**Step 9.** Select the appropriate datastore for storage and select the Thin Provision virtual disk format. Click NEXT.

**Step 10.** Select IB-MGMT Network for the VM Network. Click NEXT.

**Step 11.** Fill in all values to customize the template. Click NEXT.

**Step 12.** Review the deployment information and click FINISH to deploy the appliance.

**Step 13.** Once the OVA deployment is complete, right-click the Cisco Intersight Assist VM and click Edit Settings.

**Step 14.** Expand CPU and adjust the Cores per Socket so that 2 Sockets are shown. Click OK.

Virtual Hardware VM Options

ADD NEW DEVICE

▼ CPU	8	▼	ⓘ
Cores per Socket	4	▼ Sockets: 2	
CPU Hot Plug	<input checked="" type="checkbox"/>	Enable CPU Hot Add	
Reservation	0	▼ MHz ▼	
Limit	Unlimited	▼ MHz ▼	
Shares	Normal	▼ 8000	
CPUID Mask	Expose the NX/XD flag to guest ▼ Advanced...		
Hardware virtualization	<input type="checkbox"/>	Expose hardware assisted virtualization to the guest OS	
Performance Counters	<input type="checkbox"/>	Enable virtualized CPU performance counters	
CPU/MMU Virtualization	Automatic ▼		ⓘ
> Memory	16	▼ GB ▼	
> Hard disks	8 total   500 GB		
> SCSI controller 0	LSI Logic SAS		

CANCEL OK

**Step 15.** Right-click the Cisco Intersight Assist VM and choose Open Remote Console.

**Step 16.** Power on the VM.

**Step 17.** When you see the login prompt, close the Remote Console, and connect to <https://intersight-assist-fqdn>.

**Note:** It may take a few minutes for <https://intersight-assist-fqdn> to respond.

**Step 18.** Navigate the security prompts and select Intersight Assist. Click Proceed.

What would you like to Install ?

Intersight Connected Virtual Appliance

Intersight Private Virtual Appliance

Intersight Assist

 Recover from backup

Proceed

**Step 19.** From Cisco Intersight, click ADMIN > Devices. Click Claim a New Device. Copy and paste the Device ID and Claim Code shown in the Cisco Intersight Assist web interface to the Cisco Intersight Device Claim Direct Claim window. In Cisco Intersight, click Claim.

**Step 20.** In the Cisco Intersight Assist web interface, click Continue.

**Note:** The Cisco Intersight Assist software will now be downloaded and installed into the Cisco Intersight Assist VM. This can take up to an hour to complete.

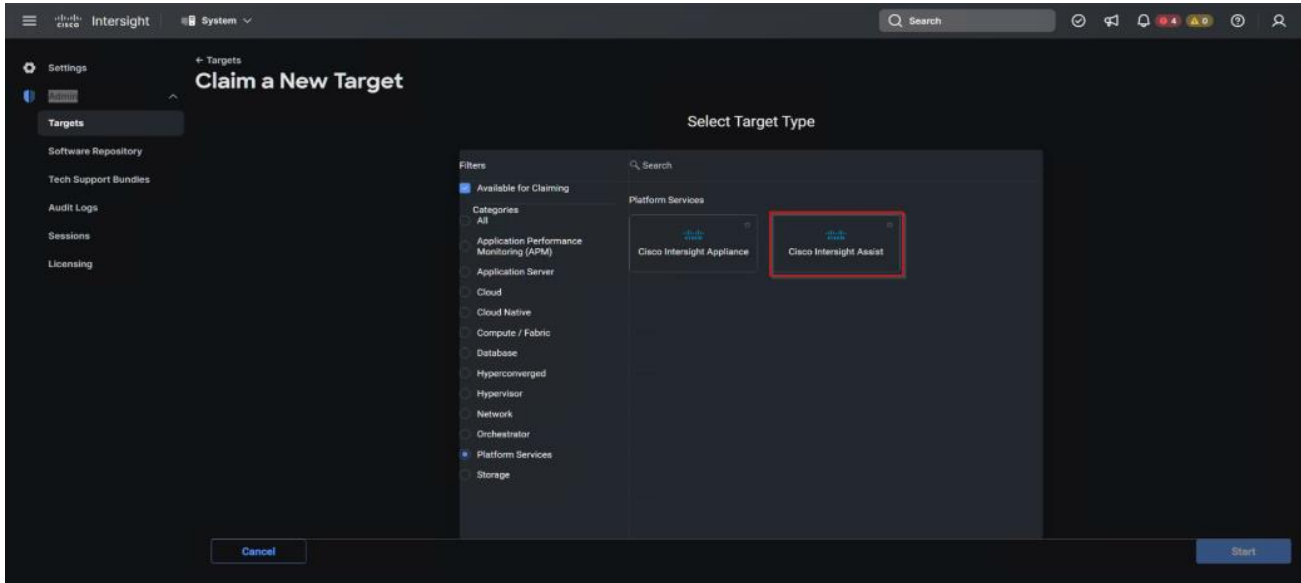
**Note:** The Cisco Intersight Assist VM will reboot during the software download process. It will be necessary to refresh the Web Browser after the reboot is complete to follow the status of the download process.

**Step 21.** When the software download is complete, navigate the security prompts and a Cisco Intersight Assist login screen will appear. Log into Cisco Intersight Assist with the admin user and the password supplied in the OVA installation. Check the Cisco Intersight Assist status and log out of Intersight Assist.

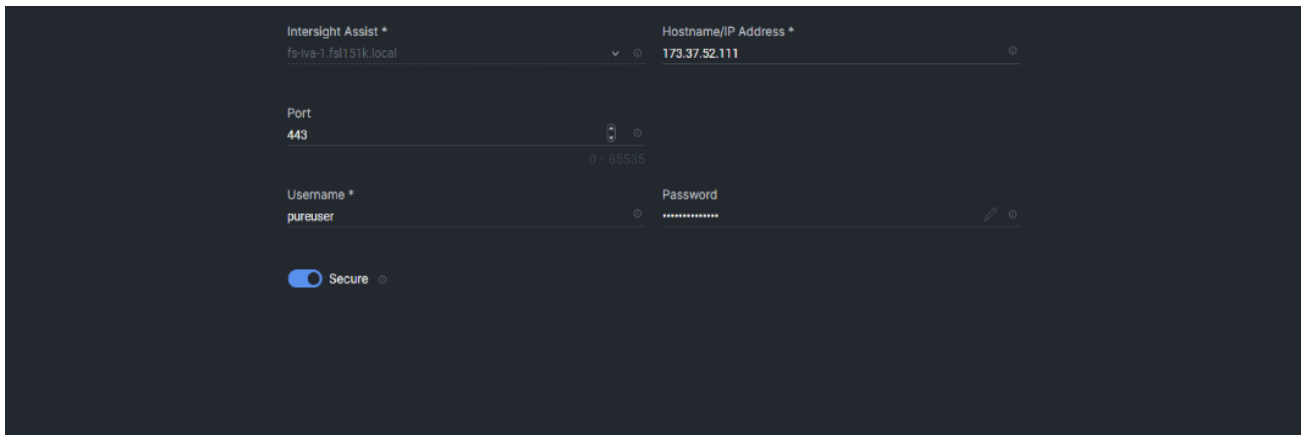
## Procedure 2. Claim Intersight Assist into Cisco Intersight

**Step 1.** To claim the Intersight assist appliance, from the Service Selector drop-down list, select System.

**Step 2.** From Cisco Intersight, click ADMIN > Targets. Click Claim a New Target. In the Select Target Type window, select Cisco Intersight Assist under Platform Services and click Start.

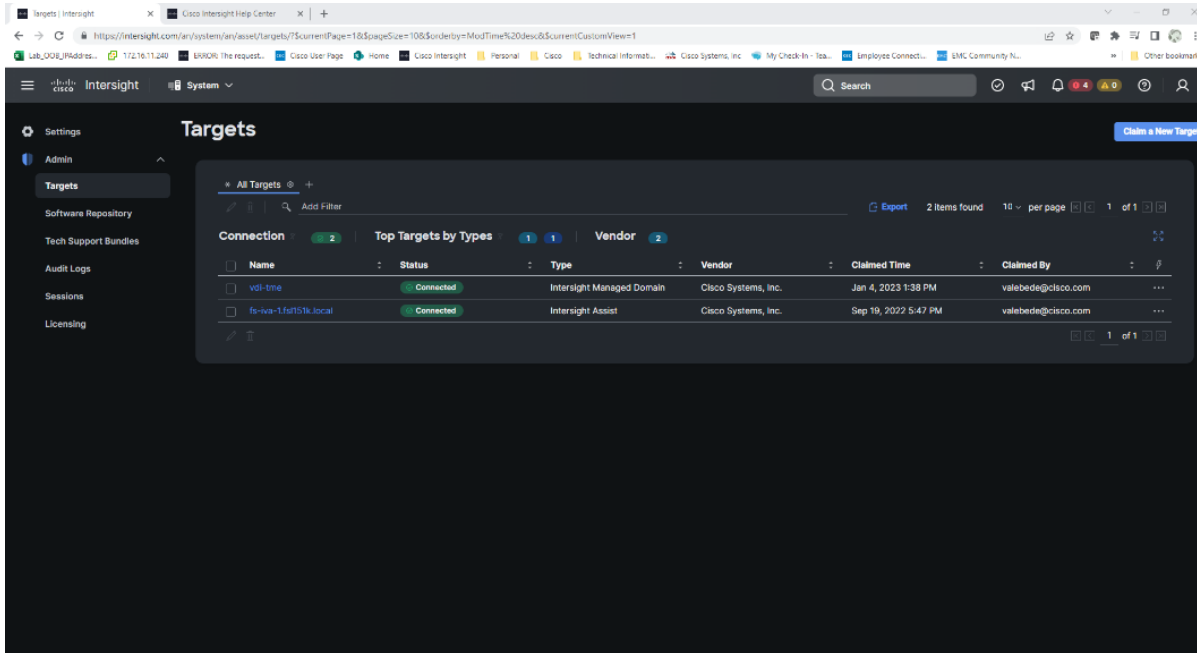


**Step 3.** Fill in the Intersight Assist information and click Claim.



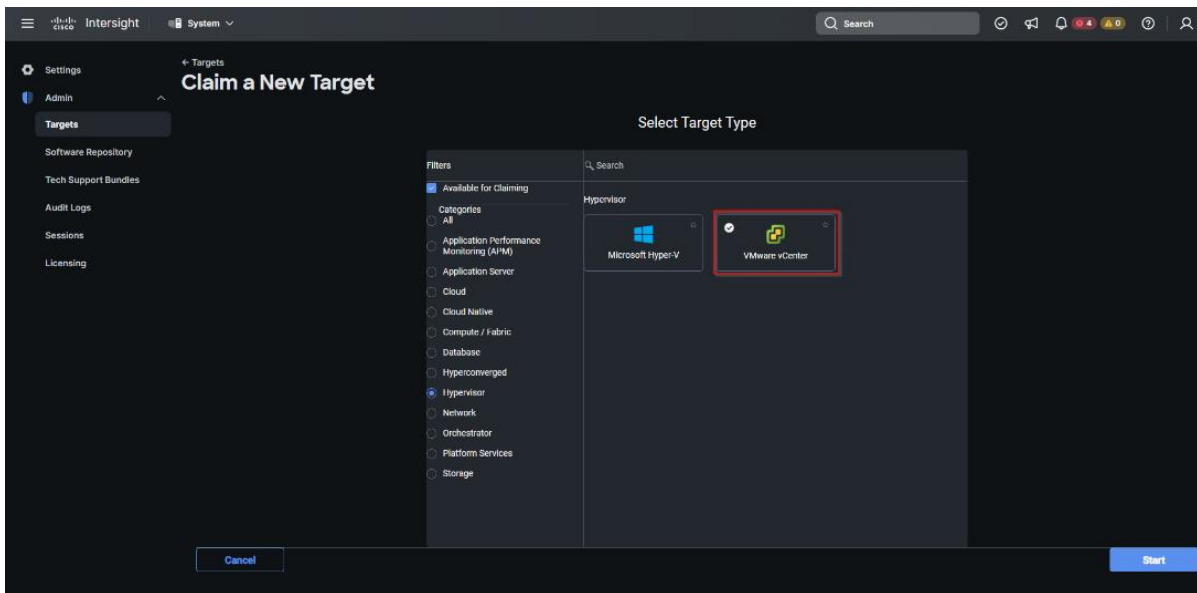
After a few minutes, Cisco Intersight Assist will appear in the Targets list.



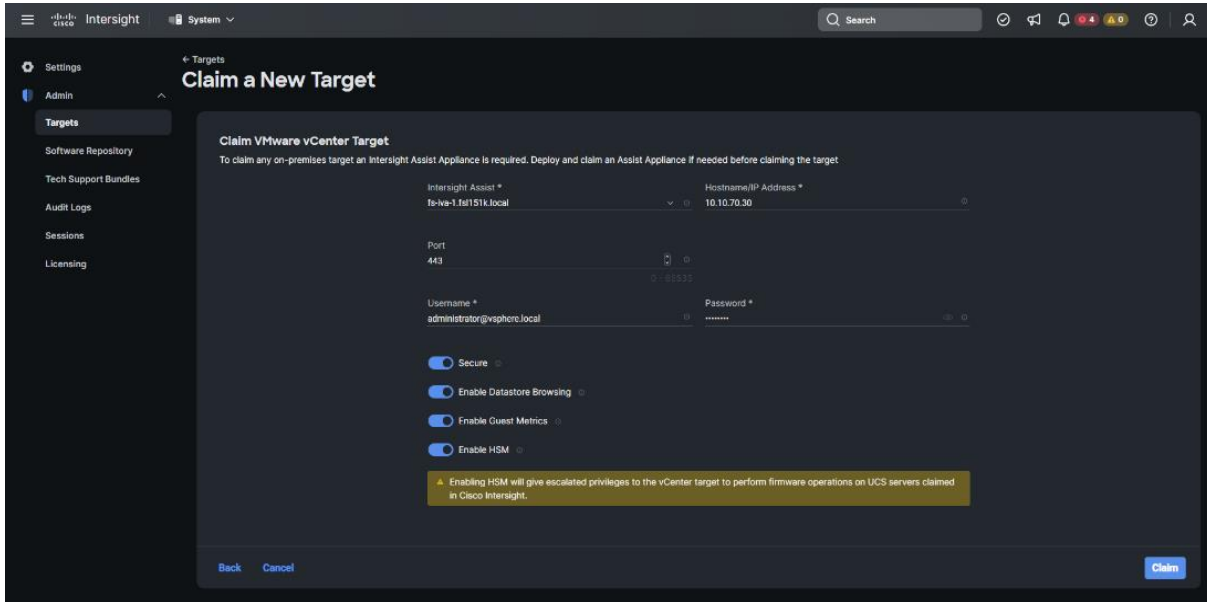


### Procedure 3. Claim vCenter in Cisco Intersight

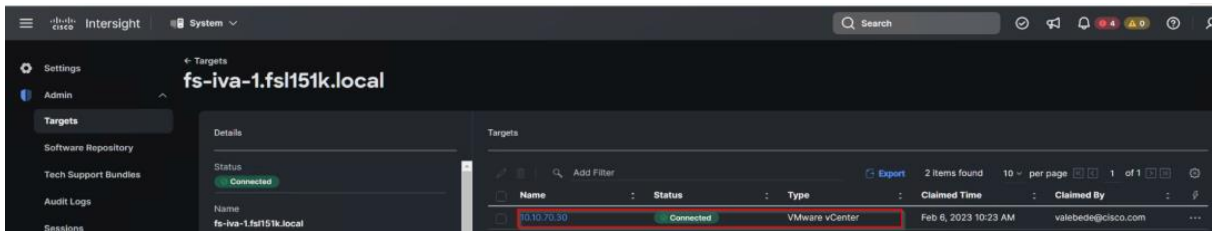
**Step 1.** To claim the vCenter, from Cisco Intersight, click ADMIN > Targets. Click Claim a New Target. In the Select Target Type window, select VMware vCenter under Hypervisor and click Start.



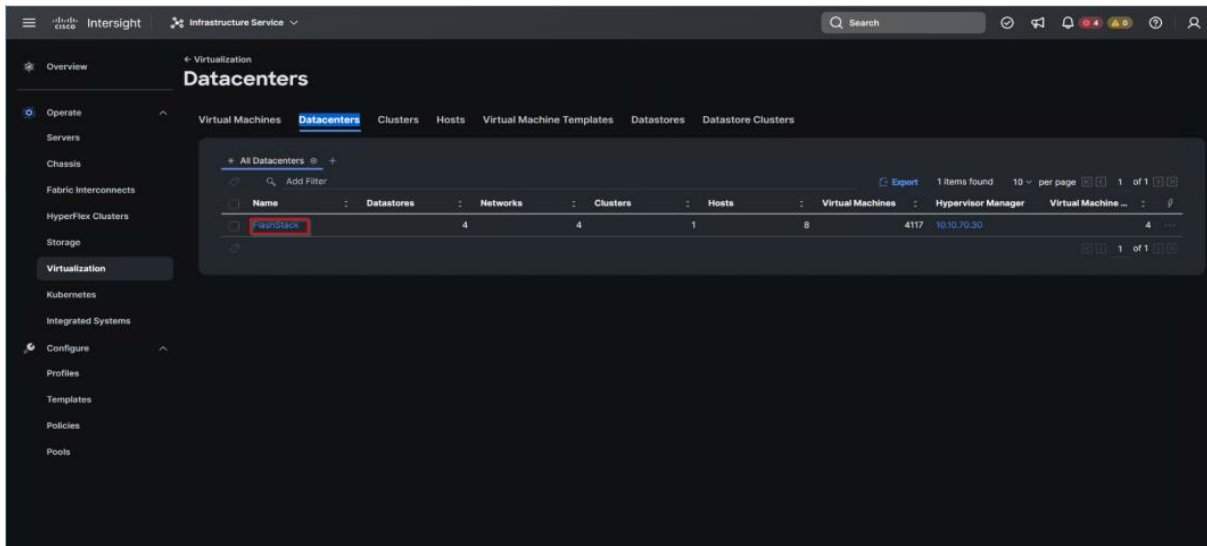
**Step 2.** In the VMware vCenter window, make sure the Intersight Assist is correctly selected, fill in the vCenter information, and click Claim.



**Step 3.** After a few minutes, the VMware vCenter will appear in the Devices list. It also can be viewed by clicking Intersight Assist in the Devices list.



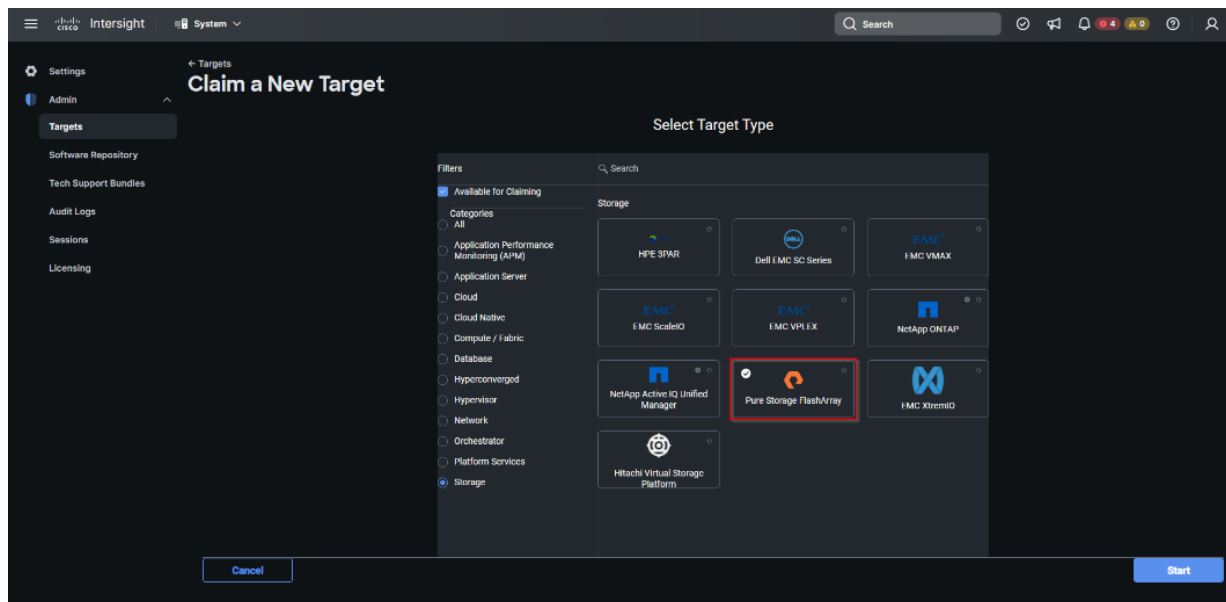
**Step 4.** Detailed information obtained from the vCenter can now be viewed by clicking Virtualization from the Infrastructure service > Operate menu.



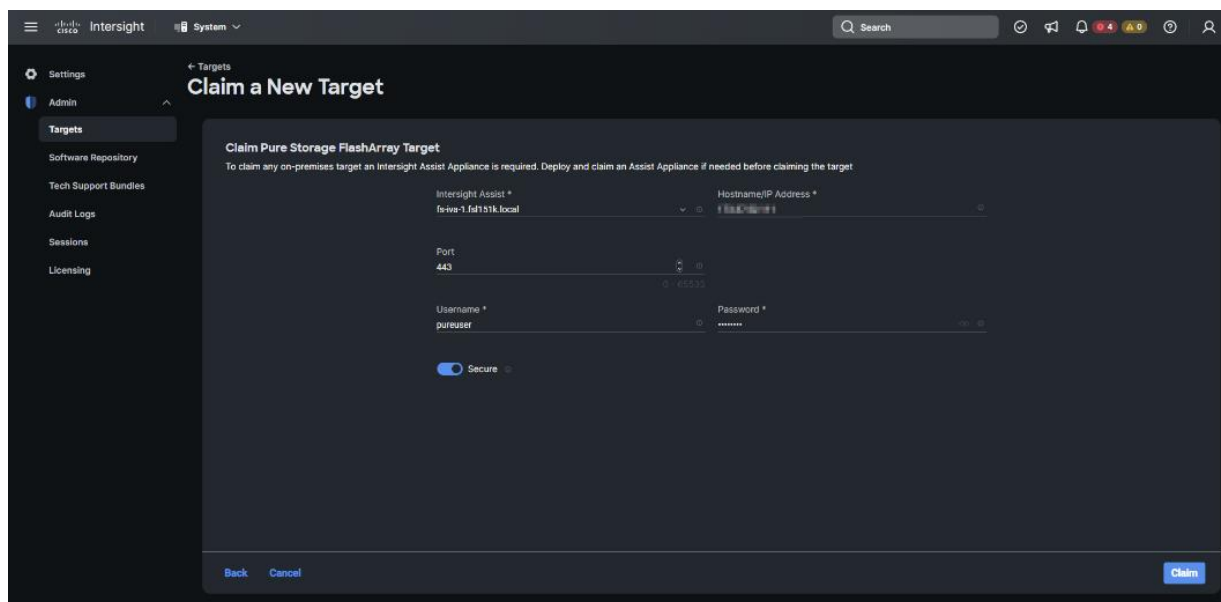
#### Procedure 4. Claim Pure Storage FlashArray//X in Cisco Intersight

**Note:** Claiming a Pure Storage FlashArray also requires the use of an Intersight Assist virtual machine.

**Step 1.** To claim the vCenter, from Cisco Intersight, click ADMIN > Targets. Click Claim a New Target. In the Select Target Type window, select Pure Storage FlashArray under Storage and click Start.



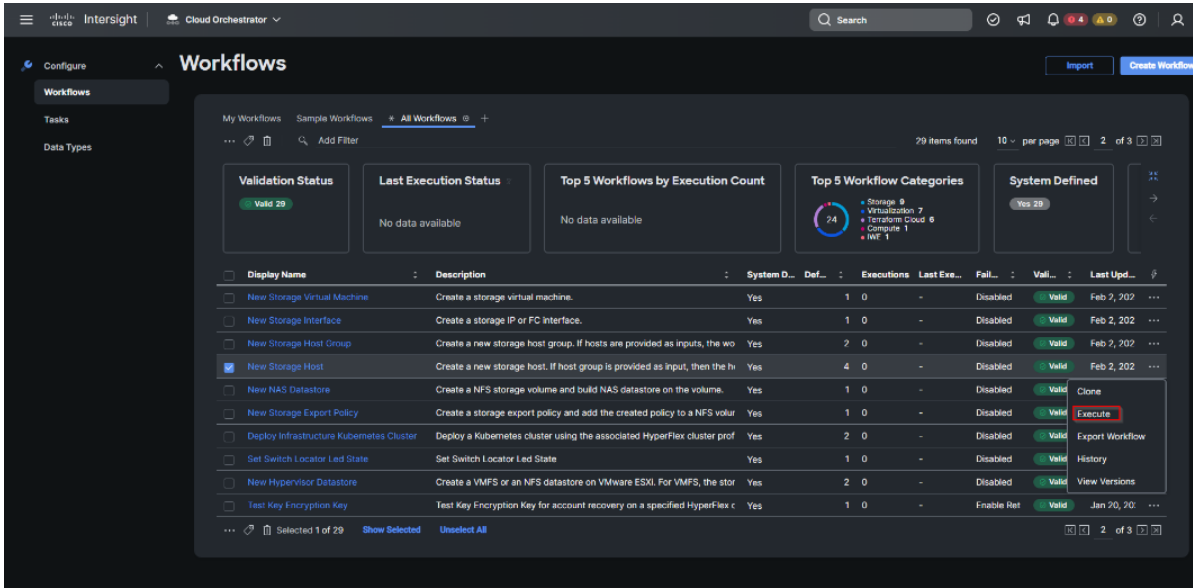
**Step 2.** Enter FlashArray Hostname/ IP address and credentials and click Claim.



## Procedure 5. FC Host Registration using Cisco Intersight

**Step 1.** From Cloud Orchestration service, select Configure > Workflows.

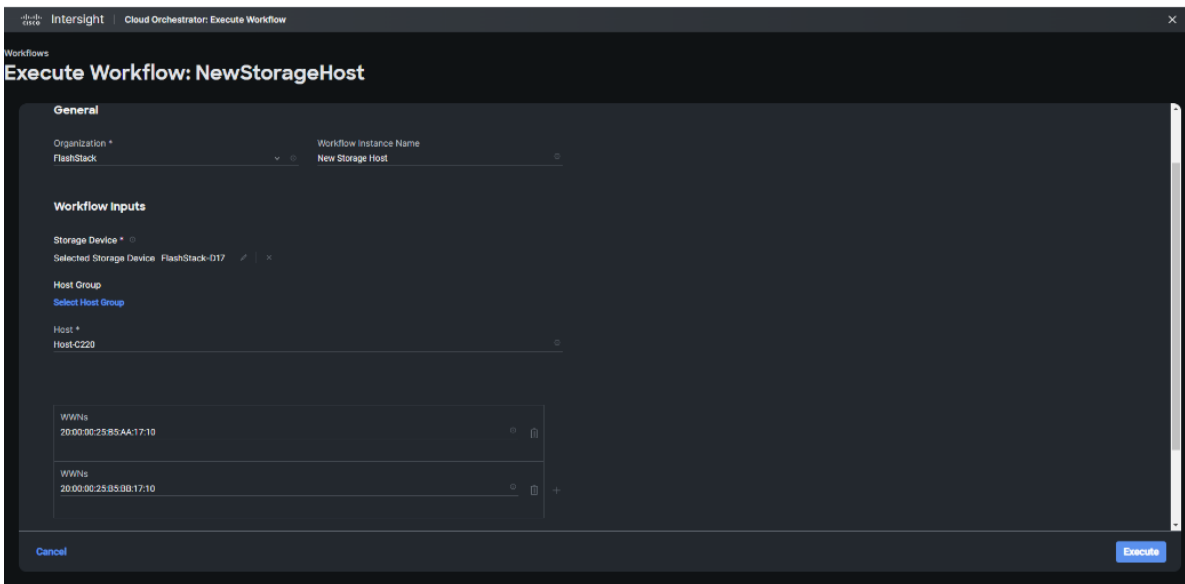
**Step 2.** Select New Storage Host. Click Execute.



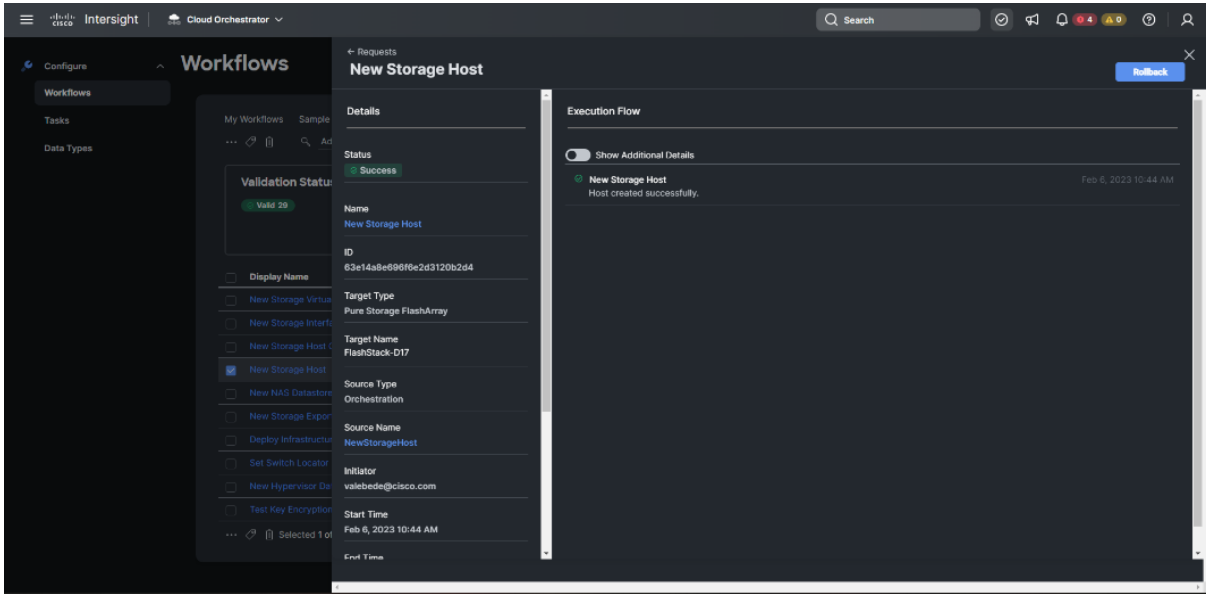
**Step 3.** Select the appropriate Organization (default by default).

**Step 4.** Select the appropriate Pure Storage device.

**Step 5.** Enter the name of the Host name and WWNs for ESX host. Click Execute.

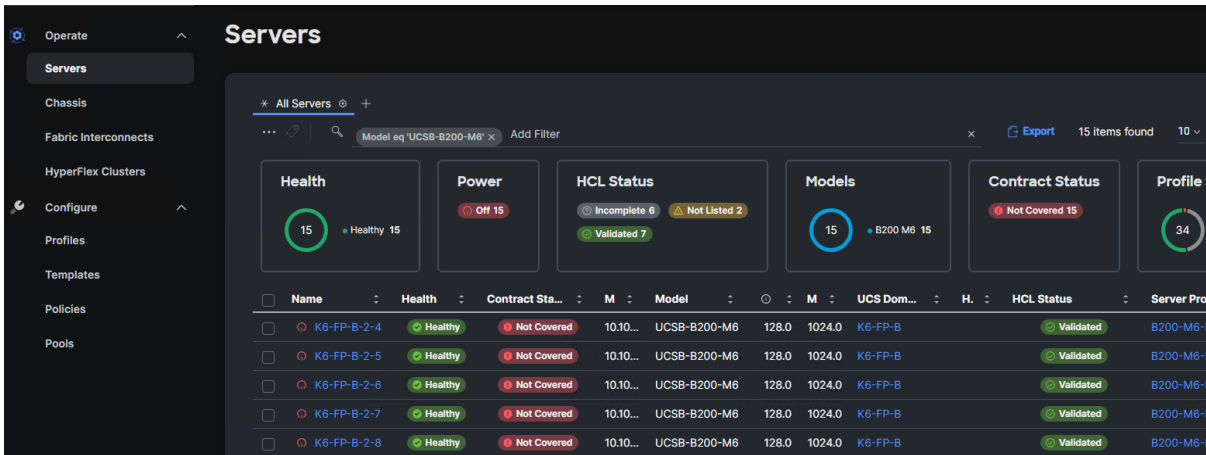


The workflow can be monitored and rolled back.

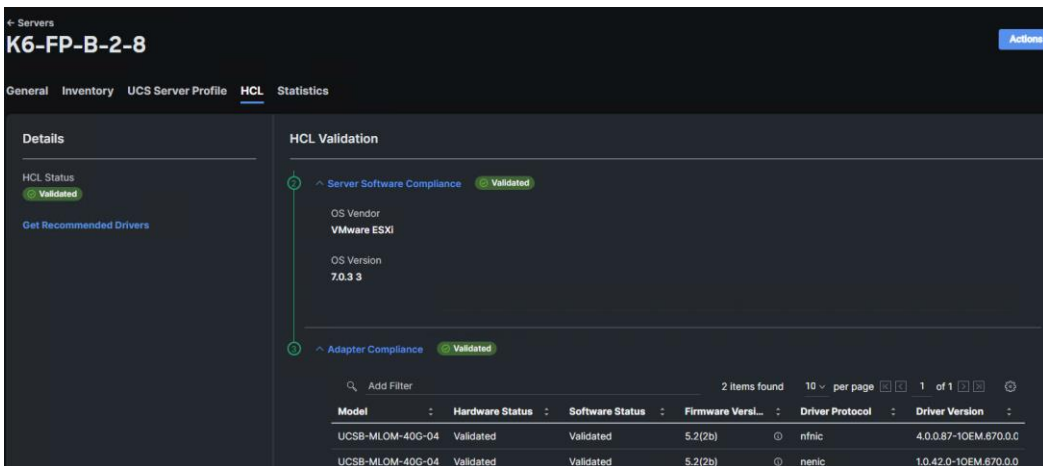


**Procedure 6. Verify Cisco UCS Server HCL Status using Cisco Intersight**

**Step 1.** From the Infrastructure Service click Operate >Servers, HCL Status field will provide the status overview.



**Step 2.** Select a server and click the HCL tab to view validation details.



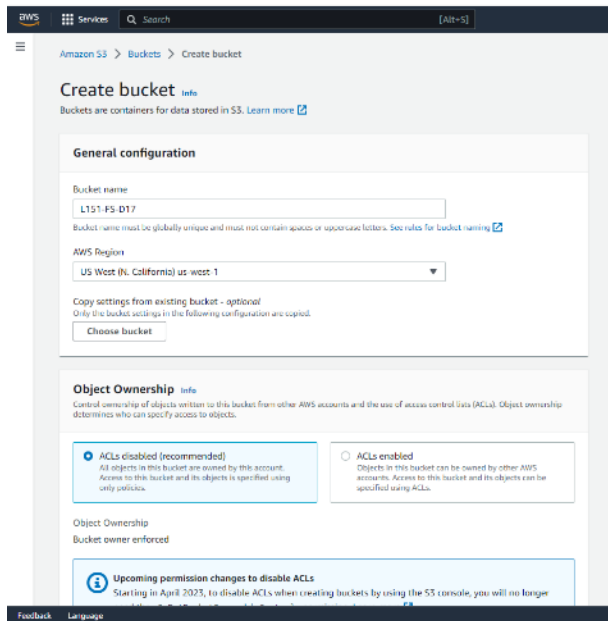
## Pure Storage CloudSnap

Pure Storage introduced its portable snapshot technology for the first time with the Snap-to-NFS feature in Purity//FA 5.1. This feature enables the FlashArray to transfer snapshots to Pure FlashBlade and other NFS servers, allowing for rapid restoration on-premises and the consolidation of siloed workloads. The technology has now been extended to include data protection in the cloud, with the AWS S3 object-based cloud storage service being the first replication target to be added. This new feature, called CloudSnap, allows FlashArray to directly transfer snapshots to an S3 bucket without the need for extra backup software or a cloud gateway. Essentially, CloudSnap acts as a built-in "self-backup to cloud" feature for FlashArray.

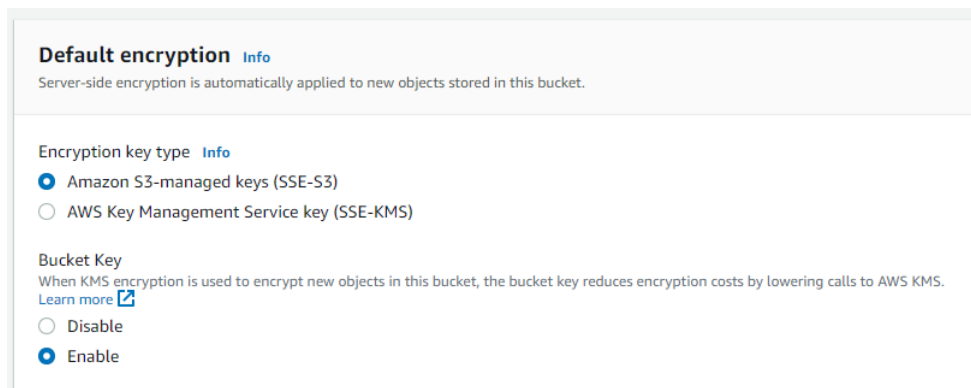
## Configure Pure Storage CloudSnap

### Procedure 1. Create an S3 Bucket in the Customer's AWS Account

**Step 1.** Log in to the AWS management console and go to S3. From the AWS S3 console dashboard, select Create Bucket.

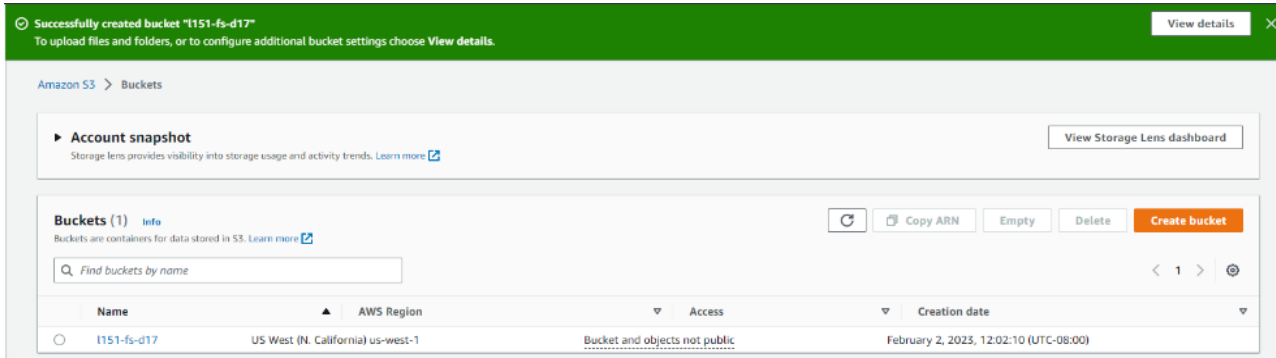


**Step 2.** Select Default encryption.

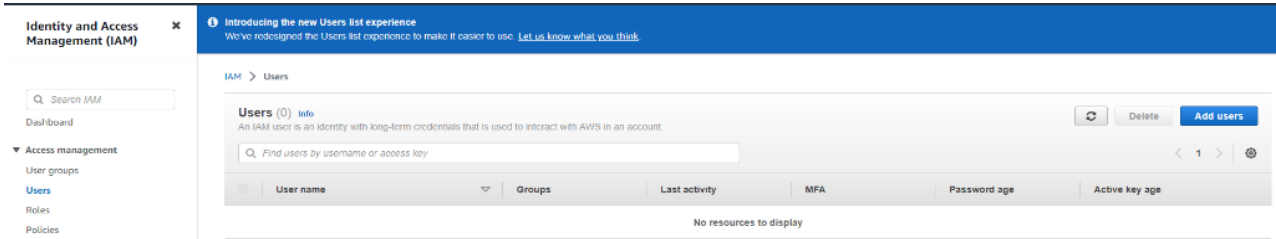


**Step 3.** Click Create bucket.

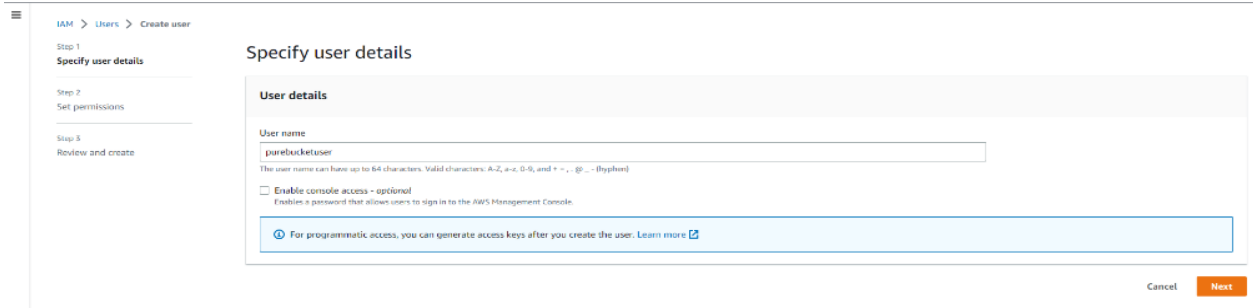




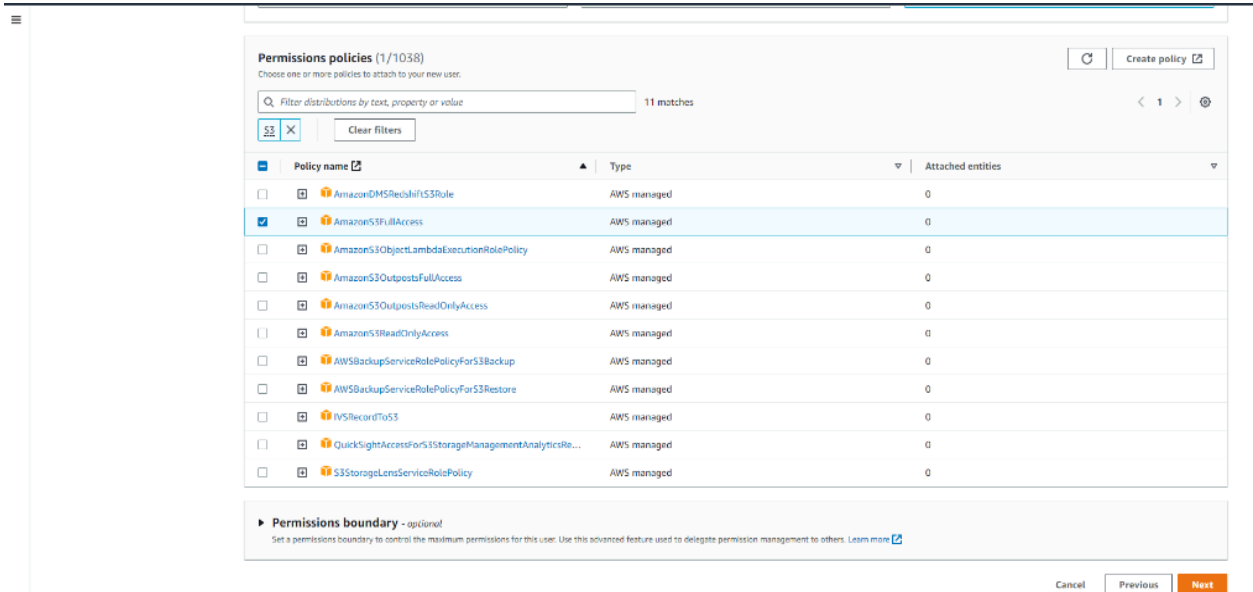
**Step 4.** From the AWS IAM console click Add users.



**Step 5.** Provide a user name and click Install.



**Step 6.** Attach the appropriate access policy and click Next.



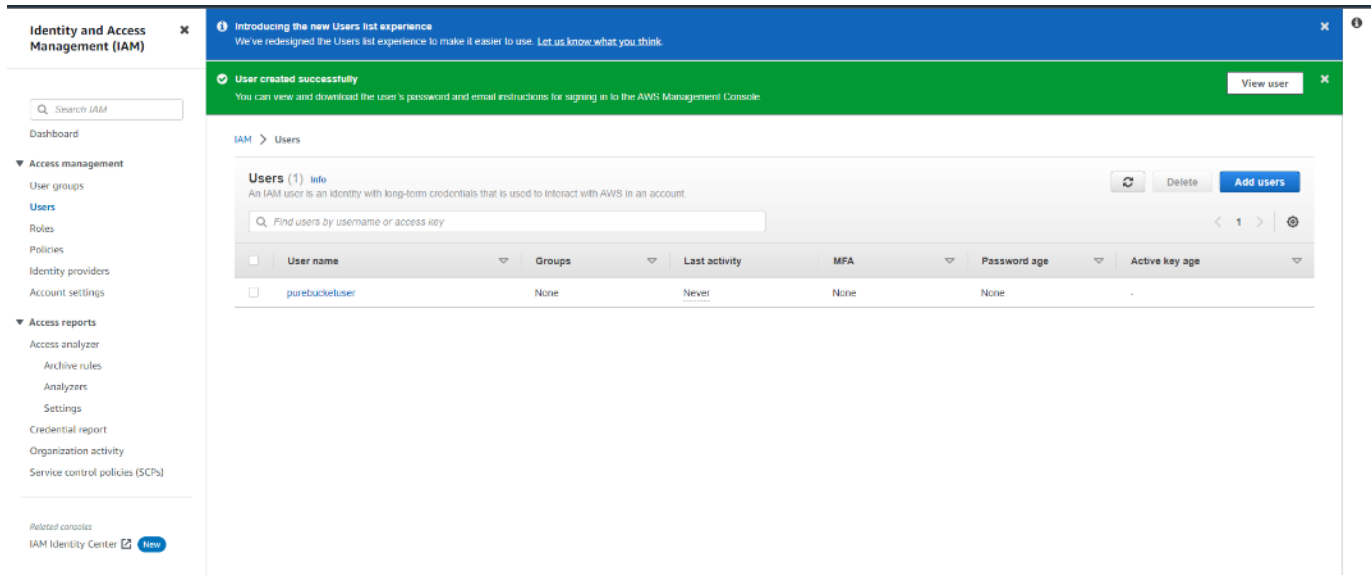
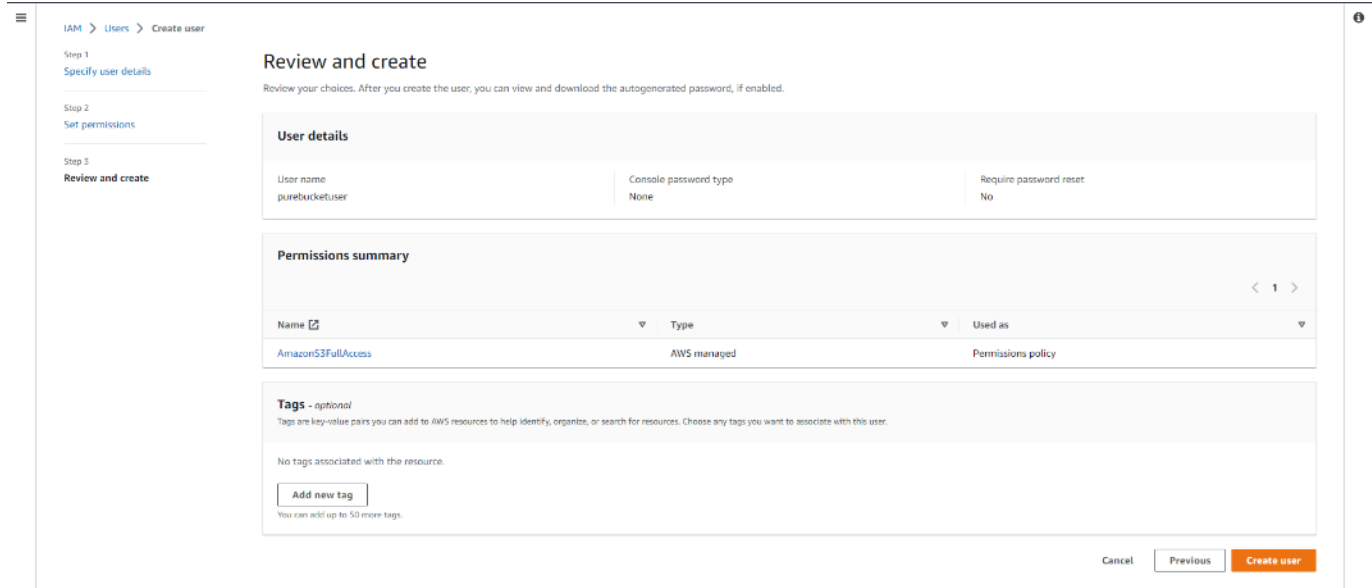
- **OPTION 1, THE SIMPLE METHOD - USING AN EXISTING AWS MANAGED POLICY.**

The easier option is to use AWS’s pre-configured policy called AmazonS3FullAccess. This AWS policy grants the IAM user (Pure FlashArray) full access to all S3 buckets in the customer’s AWS account.

- **OPTION 2, THE MORE RESTRICTIVE METHOD - CREATING A CUSTOMER MANAGED POLICY.**

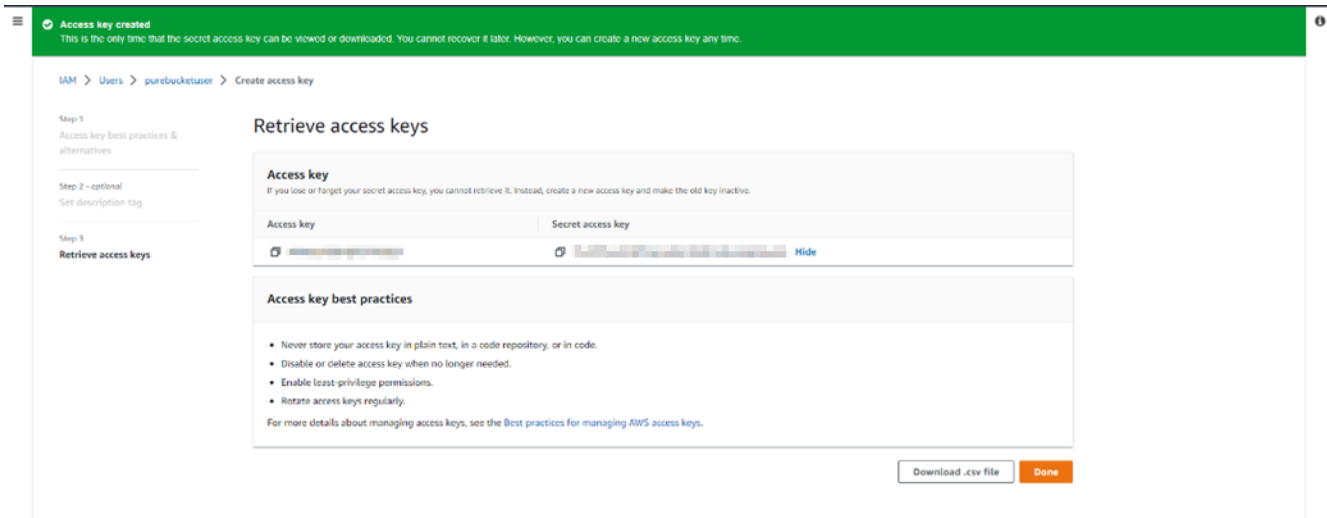
This option is for users who want to create a customer managed policy which would allow the IAM user (Pure FlashArray) full access to only the specific S3 bucket that will be used by CloudSnap to store offloaded data from FlashArray.

**Step 7.** Review the information and click Create user.



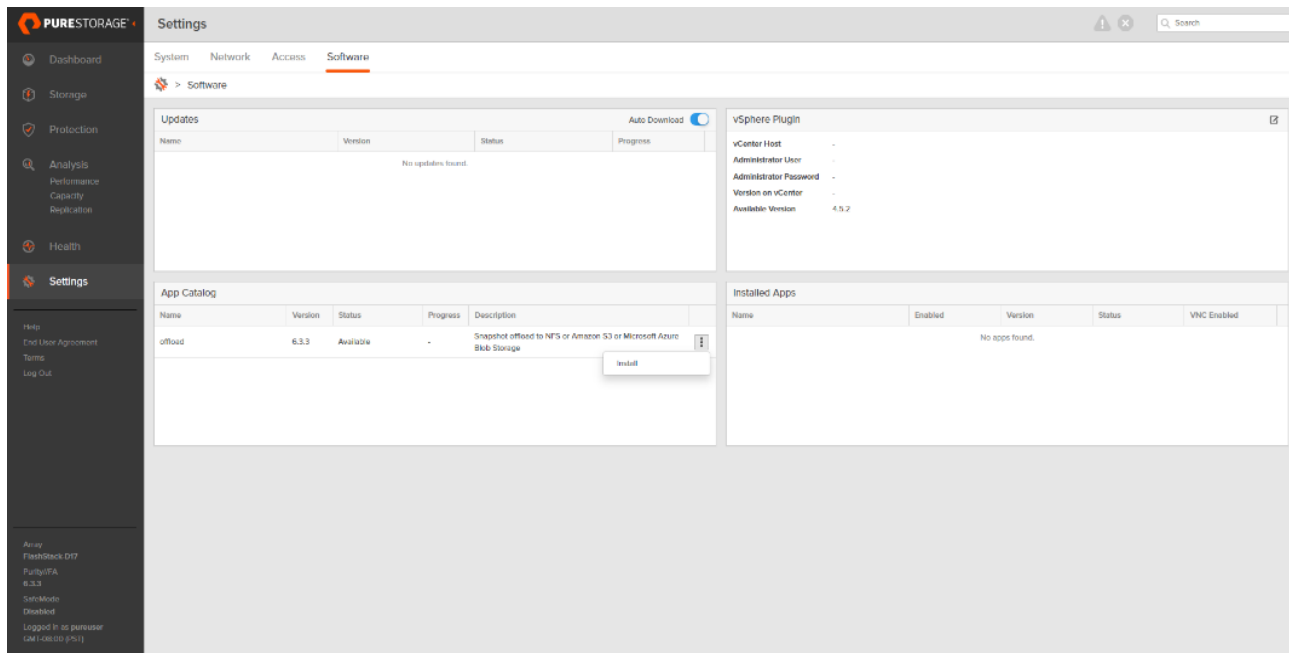
**Step 8.** Create a key for the array access.





## Procedure 2. Configure Offload on the FlashArray//x R3

**Step 1.** From the Pure Storage FlashArray Management interface, go to Settings > Software > App Catalog. Select Offload and click Install.



**Step 2.** Wait for the application to finish installation.

Installed Apps				
Name	Enabled	Version	Status	VNC Enabled
offload	false	6.3.3	unhealthy	false

**Step 3.** In the ssh array session, create the virtual offload interface.

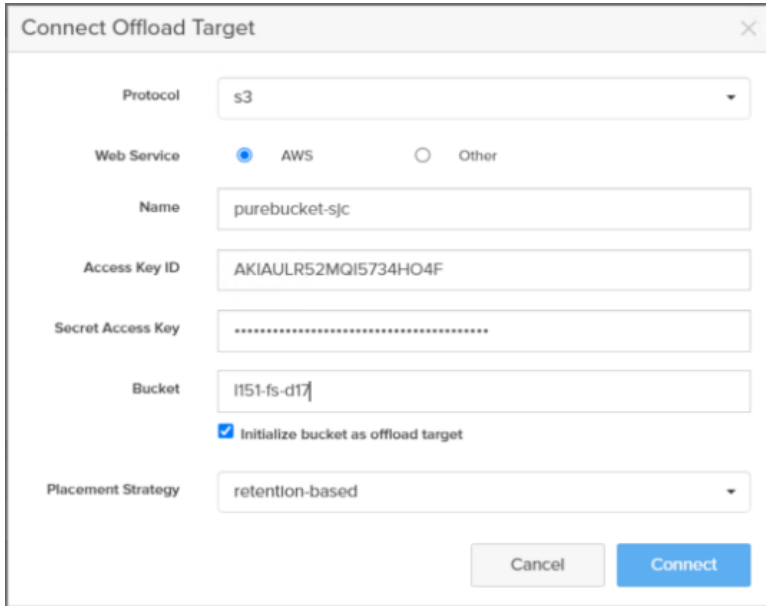
```
pureuser@FlashStack-D17> purenetwork eth create vif @offload.data0 --subinterfacelist ct0.eth2,ct1.eth2
Name           Enabled Type Subnet Address Mask Gateway MTU MAC           Speed  Services Subinterfaces
@offload.data0 False  vif  -      -      -      1500 52:54:30:3b:84:36 25.00 Gb/s  app      ct0.eth2
                                                       ct1.eth2
```

**Step 4.** Configure the offload interface with the appropriate customer environment IP information.

**Step 5.** From the Pure Storage FlashArray Management interface, go to Settings > Software > Installed Apps. Select Offload and click Enable App.

**Step 6.** From the Pure Storage FlashArray Management interface, go to Storage > Array. Next to Offload Targets, click +.

**Step 7.** Provide the Connection details and click Connect.



**Connect Offload Target**

Protocol: s3

Web Service:  AWS  Other

Name: purebucket-sjc

Access Key ID: AKIAULR52MQI5734HO4F

Secret Access Key: .....

Bucket: i151-fs-d17

Initialize bucket as offload target

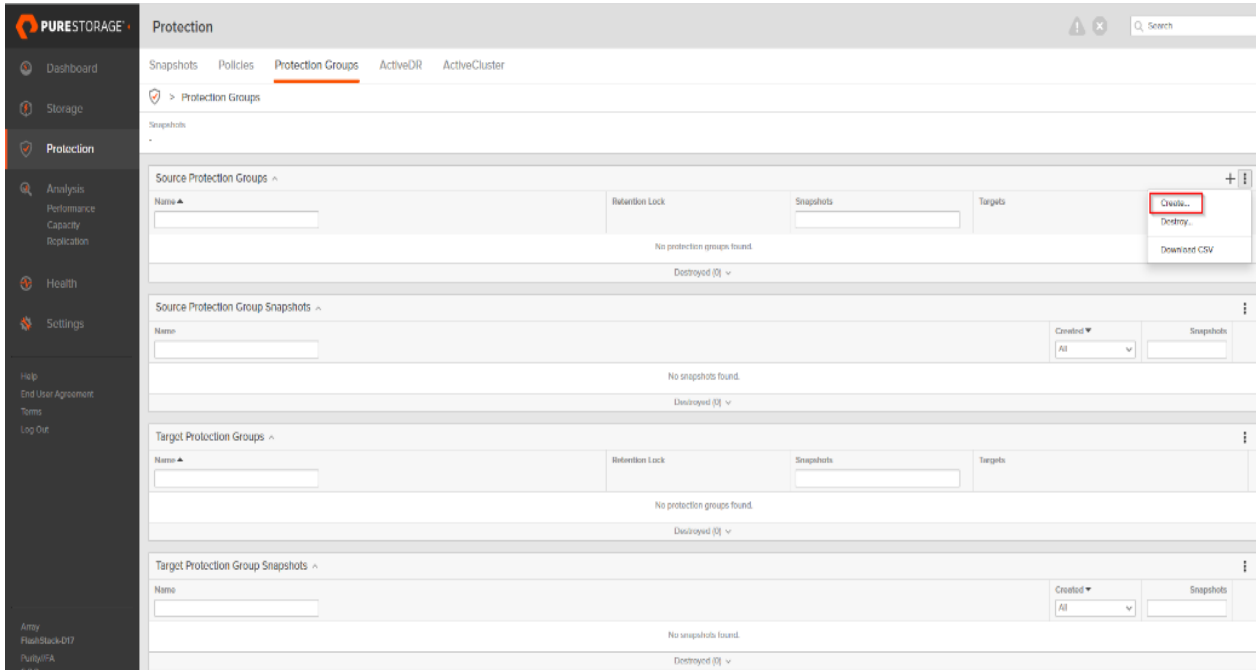
Placement Strategy: retention-based

Buttons: Cancel, Connect

**Step 8.** Select the newly added target.

Name	Status	Protocol	Details
purebucket-sjc	connected	s3	Bucket: i151-fs-d17 Access Key ID: AKIAULR52MQI5734HO4F Secret Access Key: **** Placement Strategy: retention-based

**Step 9.** From the Pure Storage FlashArray Management interface, go to Protection > Protection Groups. Select Source Protection Groups and click Create.



**PURE STORAGE** Protection

Snapshots Policies **Protection Groups** ActiveDR ActiveCluster

> Protection Groups

Source Protection Groups

Name	Retention Lock	Snapshots	Targets
<input type="text"/>		<input type="text"/>	

No protection groups found.

Destroyed (0)

Buttons: Create..., Destroy, Download CSV

Source Protection Group Snapshots

Name	Created	Snapshots
<input type="text"/>	All	<input type="text"/>

No snapshots found.

Destroyed (0)

Target Protection Groups

Name	Retention Lock	Snapshots	Targets
<input type="text"/>		<input type="text"/>	

No protection groups found.

Destroyed (0)

Target Protection Group Snapshots

Name	Created	Snapshots
<input type="text"/>	All	<input type="text"/>

No snapshots found.

Destroyed (0)

**Step 10.** Enter a Name and click Create.

**Create Protection Group** ✕

Pod

Name

**Step 11.** From the Pure Storage FlashArray Management interface, go to Protection > Protection Groups. Select Target and click Add.

The screenshot shows the 'Protection Groups' configuration page in the Pure Storage interface. The breadcrumb navigation is 'Protection > Protection Groups > aws-s3-cloudsnap'. The 'Targets' section is currently empty, and a red box highlights the 'Add...' button. Other sections include 'Members', 'Snapshot Schedule', 'Replication Schedule', and 'SafeMode'.

**Step 12.** Add the offload target.

**Add Targets** ✕

**Available Targets**

- 
- purebucket-sjc

1-1 of 1

**Selected Targets**

1 selected Clear all

- purebucket-sjc ✕

**Step 13.** Start protecting your volumes (such as Full Clones Desktops) to AWS.

Protection

Snapshots Policies **Protection Groups** ActiveDR ActiveCluster

> Protection Groups > aws-s3-cloudsnap

Snapshots  
0:00

**Members** ^ 1 of 1

Name ▲

X70VDH-2 ✕

**Targets** ^ 1 of 1

Name ▲	Allowed
purebucket-6jc	True

**Snapshot Schedule**

Enabled: True  
Create a snapshot on source every 1 weeks  
Retain all snapshots on source for 1 weeks  
then retain 4 snapshots per day for 30 more days

**Replication Schedule**

Enabled: True  
Replicate a snapshot to targets every 1 weeks  
Retain all snapshots on targets for 1 weeks  
then retain 1 snapshots per day for 7 more days

**SafeMode**

Retention Lock: unlocked

## Build the Virtual Machines and Environment for Workload Testing

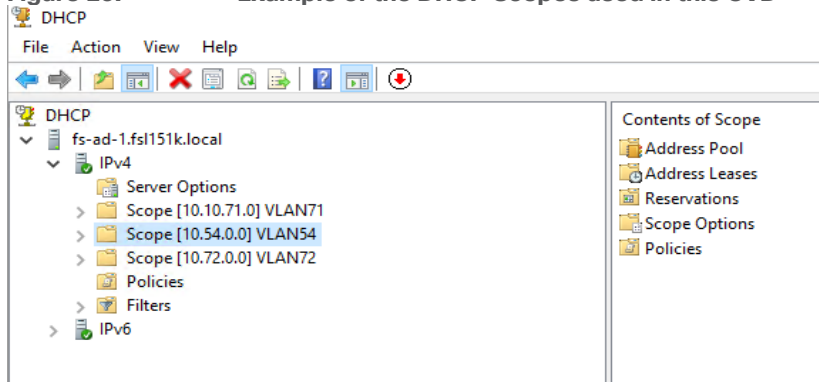
This chapter contains the following:

- [Prerequisites](#)
- [Software Infrastructure Configuration](#)
- [Prepare the Master Targets](#)
- [Install and Configure VMware Horizon](#)

### Prerequisites

Create the necessary DHCP scopes for the environment and set the scope options.

**Figure 25.** Example of the DHCP Scopes used in this CVD



### Software Infrastructure Configuration

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

Install and configure the infrastructure virtual machines by following the process listed in [Table 20](#).

**Table 20.** Test Infrastructure Virtual Machine Configuration

Configuration	Microsoft Active Directory DCs Virtual Machine	vCenter Server Appliance Virtual Machine
Operating system	Microsoft Windows Server 2019	VCSA - SUSE Linux
Virtual CPU amount	4	16
Memory amount	8 GB	32 GB
Network	VMXNET3 k23-Infra-Mgmt-71	VMXNET3 k23-Infra-Mgmt-71
Disk-1 (OS) size	40 GB	698.84 GB (across 13 VMDKs)
Disk-2 size		

Configuration	Microsoft SQL Server Virtual Machine	VMware Horizon Connection Server Virtual Machine
Operating system	Microsoft Windows Server 2019	Microsoft Windows Server 2019

Configuration	Microsoft SQL Server Virtual Machine	VMware Horizon Connection Server Virtual Machine
Virtual CPU amount	6	4
Memory amount	24GB	8 GB
Network	VMXNET3 FS-Infra-Mgmt_71	VMXNET3 FS-Infra-Mgmt_71
Disk-1 (OS) size	40 GB	40
Disk-2 size	100 GB SQL Databases\Logs	

## Prepare the Master Targets

This section provides guidance regarding creating the golden (or master) images for the environment. Virtual machines for the master targets must first be installed with the software components needed to build the golden images. Additionally, all available security patches as of October 2022 for the Microsoft operating systems and Microsoft Office 2016 were installed.

The single-session OS and multi-session OS master target virtual machines were configured as detailed in [Table 21](#).

**Table 21.** Single-session OS and Multi-session OS Virtual Machines Configurations

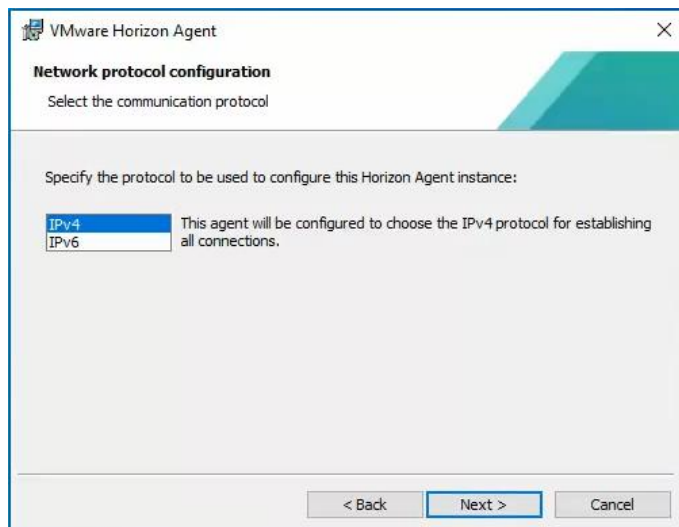
Configuration	Single-session OS Virtual Machine	Mutli-session OS Virtual Machine
Operating system	Microsoft Windows 10 64-bit 21H2 (19044.2006)	Microsoft Windows Server 2019 Standard 1809 (17763.3469)
Virtual CPU amount	2	8
Memory amount	3 GB reserve for all guest memory	32 GB reserve for all guest memory
Network	VMXNET3 FS-VDI_64	VMXNET3 FS-VDI_64
vDisk size	48 GB	60 GB
Additional software used for testing	Microsoft Office 2016 Office Update applied Login VSI 4.1.39.6 Target Software (Knowledge Worker Workload)	Microsoft Office 2016 Office Update applied Login VSI 4.1.39.6 Target Software (Knowledge Worker Workload)
Additional Configuration	Configure DHCP Add to domain Install VMWare tools Install .Net 3.5 Activate Office Install Horizon Agent Install FSLogix 2105 HF_01	Configure DHCP Add to domain Install VMWare tools Install .Net 3.5 Activate Office Install Horizon Agent Install FSLogix 2105 HF_01

## Procedure 1. Prepare the Master Virtual Machines

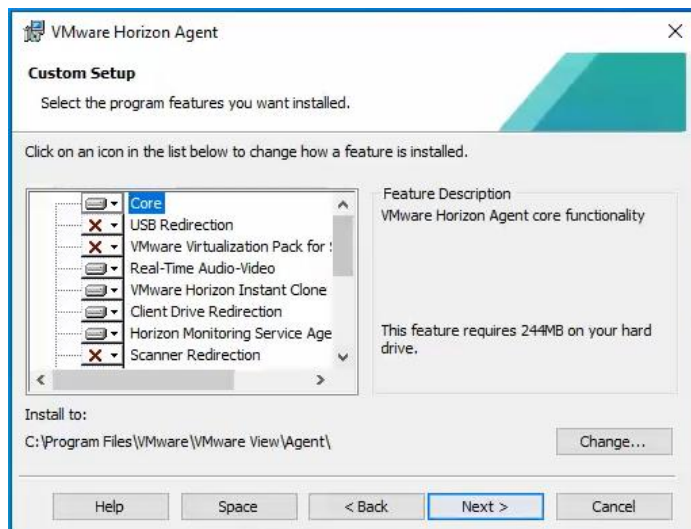
To prepare the master virtual machines, there are three major steps: installing the operating system and VMware tools, installing the application software, and installing the VMware Horizon Agent.

**Note:** For this CVD, the images contain the basics needed to run the Login VSI workload.

**Step 1.** During the VMware Horizon Agent installation, select IPv4 for the network protocol.

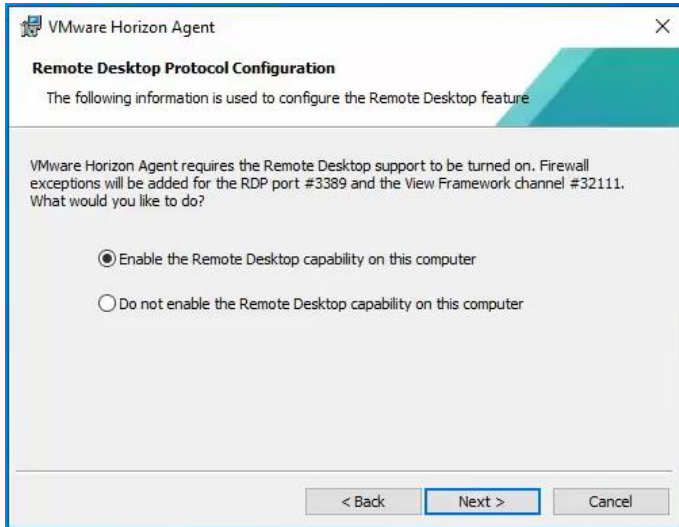


**Step 2.** On the Custom Setup screen, leave the defaults preparing the Instant clone master image. Deselect the VMware Horizon Instant Clone option for the Full clone master image.

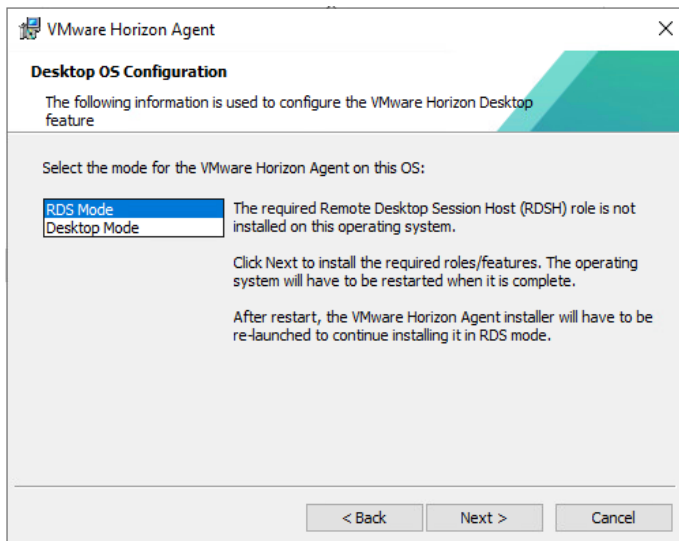


**Step 3.** Enable the remote Desktop Protocol.





**Step 4.** During the VMware Horizon Agent installation on the Windows server select RDS Mode.



The final step is to optimize the Windows OS. VMware OSOT, the optimization tool, includes customizable templates to enable or disable Windows system services and features using VMware recommendations and best practices across multiple systems. Since most Windows system services are enabled by default, the optimization tool can be used to easily disable unnecessary services and features to improve performance.

**Note:** In this CVD, the Windows OS Optimization Tool for VMware Horizon. Version 1.0 (2203) was used.

Home / Windows OS Optimization Tool for VMware Horizon

## Download Product

Select Version

Documentation [Release Notes](#)

Release Date 2022-04-05

OSOT Template: Default optimization template for Windows 10 (1809-21H2) and Windows 11 (21H2) or Server 2019 and Server 2022.

To successfully run the Login VSI knowledge worker workload the 'Disable animation in web pages - Machine Policy' option in Default Template under Programs -> Internet Explorer was disabled.

▼	Programs (75 items)			
>	.Net (5 items)			
▼	Internet Explorer (20 items)			
<input checked="" type="checkbox"/>	Turn off suggestions for all user-installed providers - Machine Policy	0	NA	Turn off suggestions for all user-installed providers
<input checked="" type="checkbox"/>	Disable Internet Explorer Enhanced Security - HKLM Registry	0	1	Disable Internet Explorer Enhanced Security.
<input checked="" type="checkbox"/>	Disable IE Customization Wizard - Machine Policy	1	NA	Removes the customization wizard upon first launch of Internet Explor
<input checked="" type="checkbox"/>	Disable Background Synchronization - Machine Policy	0	NA	Turn off background synchronization for feeds and Web Slices
<input checked="" type="checkbox"/>	Turn off the next pre-loaded page of a website - Machine Policy	0	NA	Turn off the flip ahead with page prediction feature
<input type="checkbox"/>	Disable animations in web pages - Machine Policy	no	NA	Only animated GIF files are affected by this setting

## Install and Configure FSLogix

FSLogix, a Microsoft tool, was used to manage user profiles in this validated design.

A Windows user profile is a collection of folders, files, registry settings, and configuration settings that define the environment for a user who logs on with a particular user account. These settings may be customizable by the user, depending on the administrative configuration. Profile management in VDI environments is an integral part of the user experience.

FSLogix allows you to:

- Roam user data between remote computing session hosts.
- Minimize sign in times for virtual desktop environments.
- Optimize file IO between host/client and remote profile store.
- Provide a local profile experience, eliminating the need for roaming profiles.
- Simplify the management of applications and 'Gold Images'.

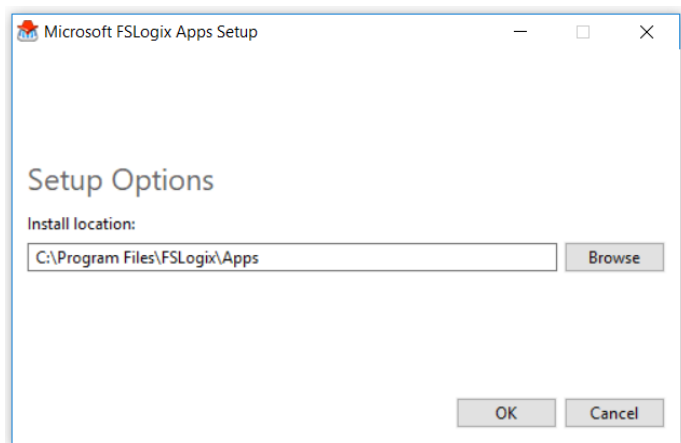
Additional documentation about the tool can be found [here](#).

### Procedure 1. FSLogix Apps Installation

**Step 1.** Download the FSLogix file [here](#).

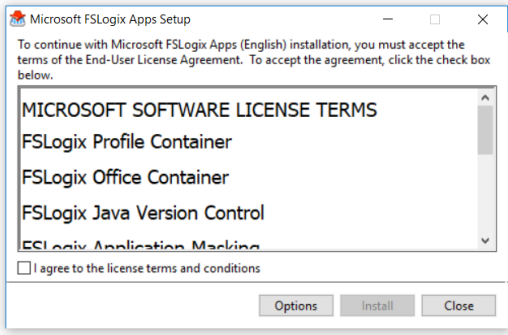
**Step 2.** Run FSLogixAppSetup.exe on VDI master image (32 bit or 64 bit depending on your environment).

**Step 3.** Click OK to proceed with default installation folder.



**Step 4.** Review and accept the license agreement.

**Step 5.** Click Install.



**Step 6.** Reboot.

## Procedure 2. Configure Profile Container Group Policy

**Step 1.** Copy "fslogix.admx" to C:\Windows\PolicyDefinitions, and "fslogix.adml" to C:\Windows\PolicyDefinitions\en-US on Active Directory Domain Controllers.

**Step 2.** Create FSLogix GPO and apply to the desktops OU:

- Navigate to Computer Configuration > Administrative Templates > FSLogix > Profile Containers.
- Configure the following settings:
- Enabled – Enabled
- VHD location – Enabled, with the path set to \\<FileServer>\<Profiles Directory>

**Note:** Consider enabling and configuring FSLogix logging as well as limiting the size of the profiles and excluding additional directories.

**Figure 26.** Example of FSLogix Policy

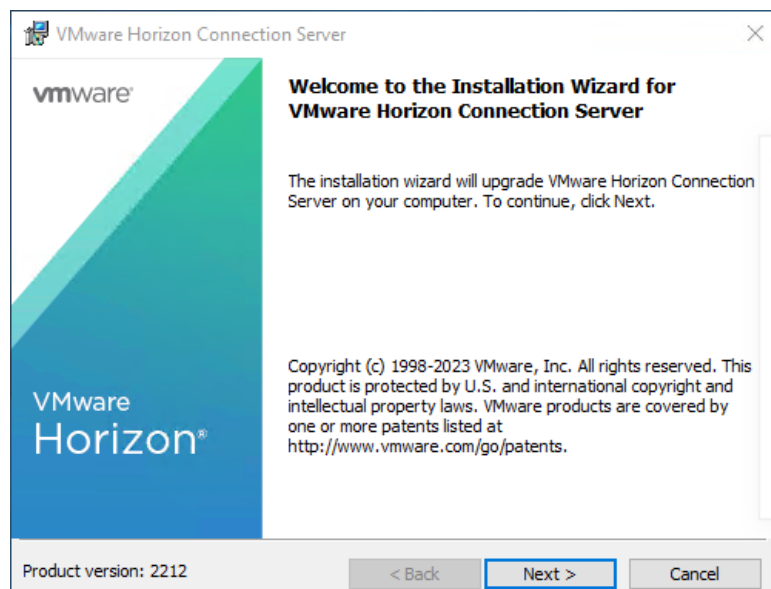
FSLogix		
Policy	Setting	Comment
<b>FSLogix/Profile Containers</b>		
Delete local profile when FSLogix Profile should apply	Enabled	
Delete local profile when FSLogix Profile should apply		
Dynamic VHD(X) allocation	Enabled	
Dynamic VHD(X) allocation		
Enabled	Enabled	
Enabled		
Profile type	Enabled	
Try for read-write profile and fallback to read-only		
Size in MBs	Enabled	
Size in MBs		
2048		
VHD location	Enabled	
VHD location		
\\purefile\wd\RDS		
<b>FSLogix/Profile Containers/Advanced</b>		
<b>FSLogix/Profile Containers/Container and Directory Naming</b>		
Virtual disk type	Enabled	
VHDX		

## Install and Configure VMware Horizon

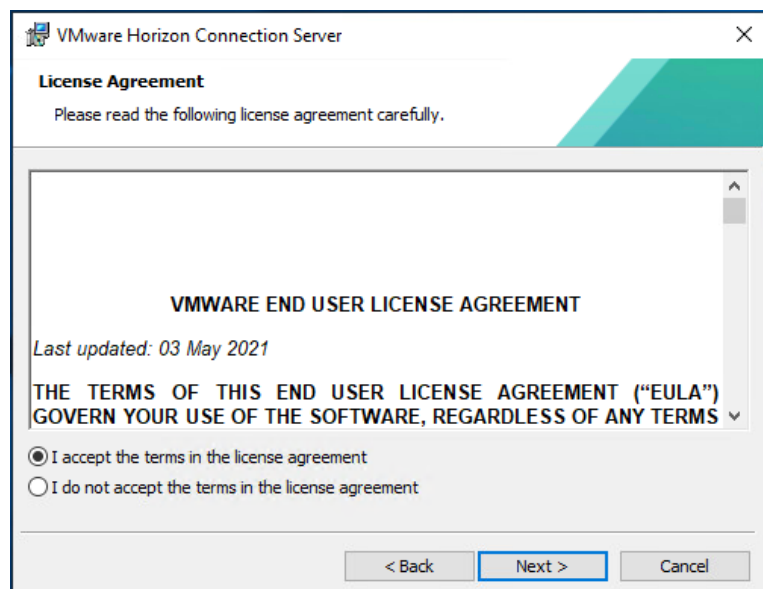
### Procedure 1. Configure VMware Horizon Connection Server

**Step 1.** Download the Horizon Connection server installer from VMware and click Install on the Connection Server Windows Server Image. In this study, we used version Connection Server Horizon 8 2212 build 8.8.0-21073894.exe.

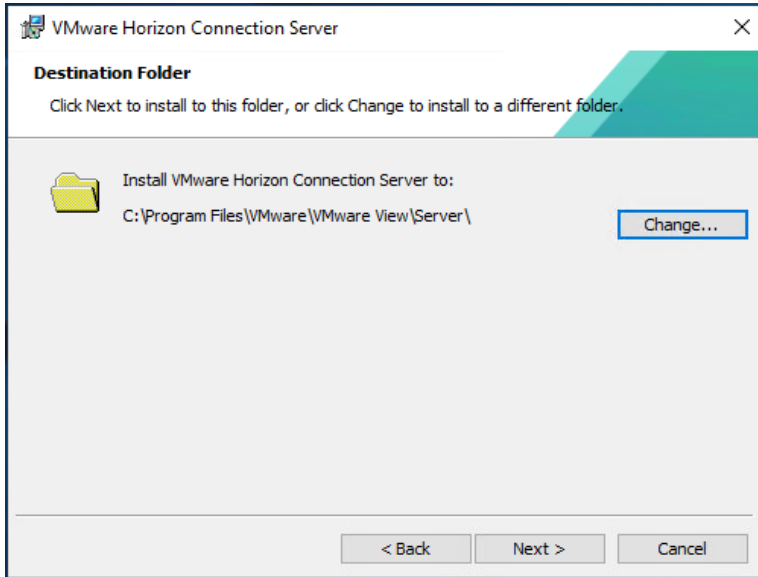
**Step 2.** Click Next.



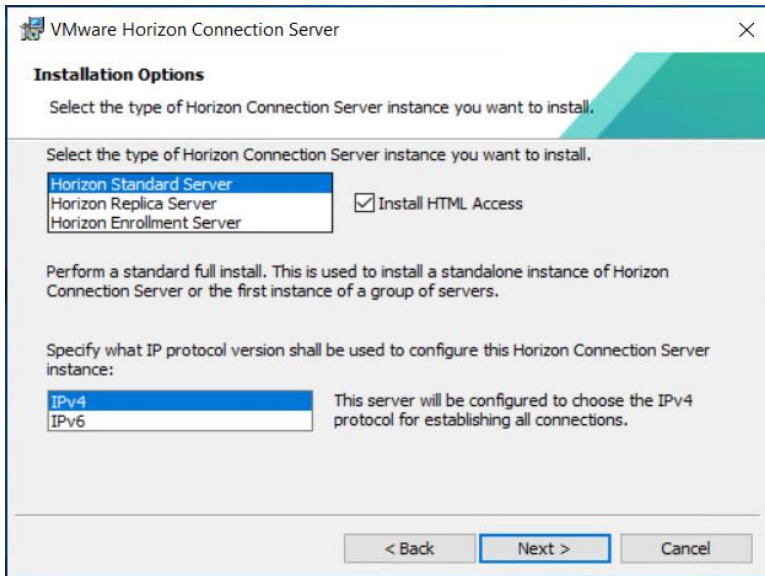
**Step 3.** Read and accept the End User License Agreement and click Next.



**Step 4.** Select the destination folder where you want to install the application and click Next.



**Step 5.** Select the Standard Server and IPv4 for the IP protocol version.



**Step 6.** Provide the data recovery details.

VMware Horizon Connection Server

### Data Recovery

Enter data recovery password details.

This password protects data backups of your Horizon Connection Server. Recovering a backup will require entry of this password.

Enter data recovery password:

Re-enter password:

Enter password reminder (optional):

< Back   Next >   Cancel

**Step 7.** Select Configure Windows Firewall automatically. Click Next.

VMware Horizon Connection Server

### Firewall Configuration

Automatically configure the Windows Firewall to allow incoming TCP protocol connections.

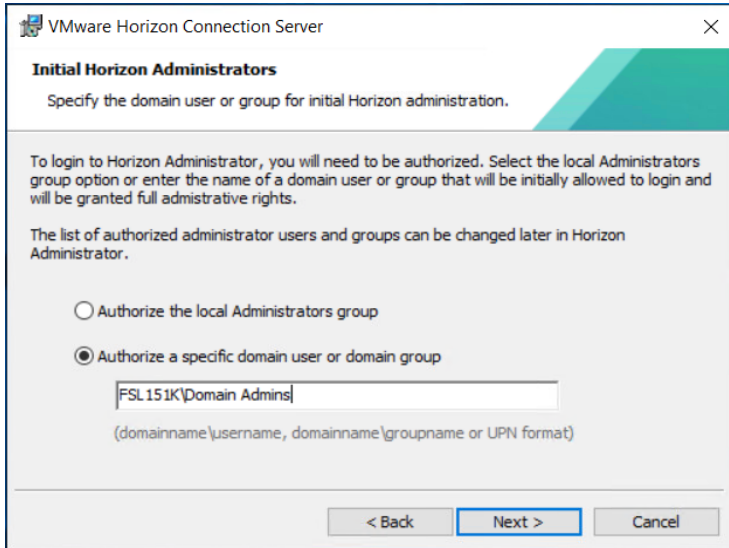
In order for Horizon Connection Server to operate on a network, specific incoming TCP ports must be allowed through the local Windows Firewall service. The incoming TCP ports for the Replica Server are 8009 (AJP13), 80 (HTTP), 443 (HTTPS), 4001 (JMS), 4002 (JMS-SSL), 4100 (JMSIR), 4101 (JMSIR-SSL), 4172 (PCoIP), 8472 (Inter-pod API), and 8443 (HTML Access). UDP packets on port 4172 (PCoIP) are allowed through as well.

Configure Windows Firewall automatically

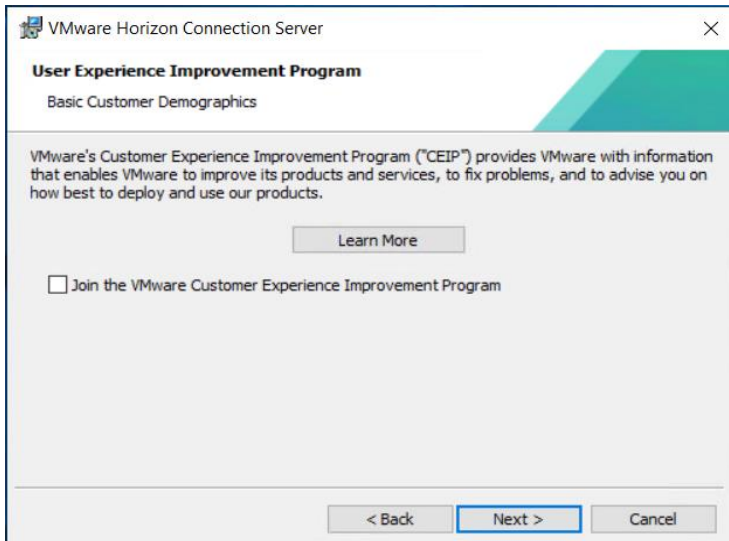
Do not configure Windows Firewall

< Back   Next >   Cancel

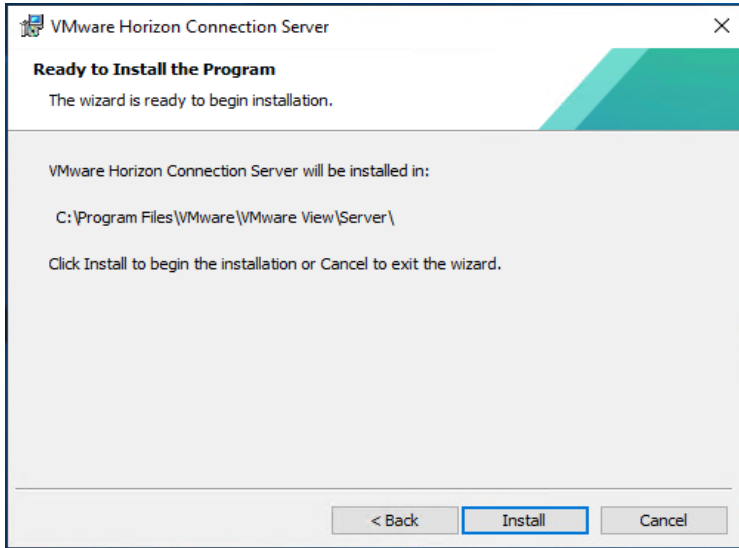
**Step 8.** Authorize Domain Admins to be VMware Horizon administrators.



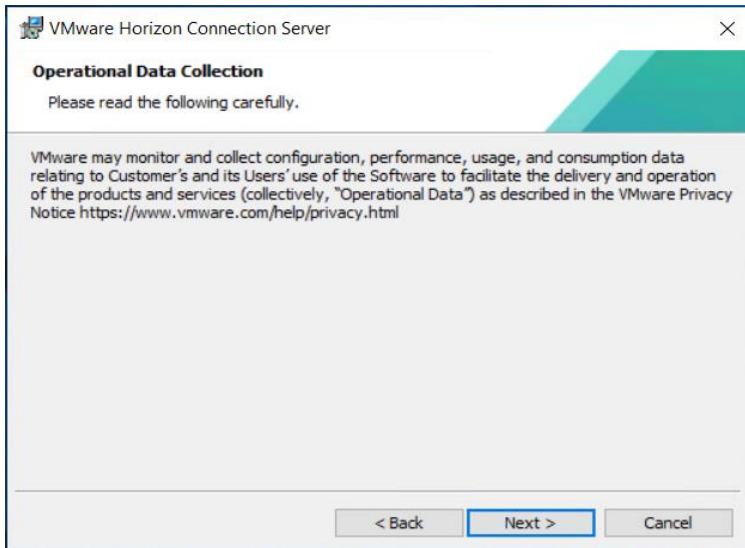
**Step 9.** (Optional) Join Customer Experience Program.



**Step 10.** Click Install to begin installation.

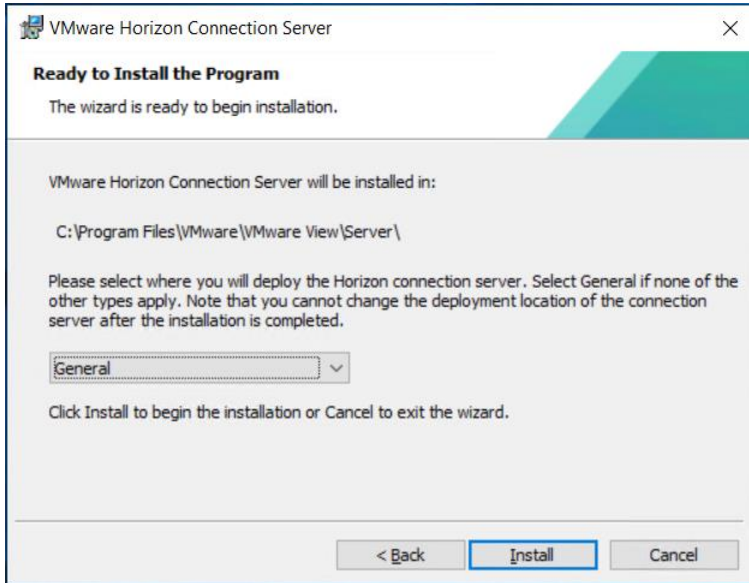


**Step 11.** Click Next.

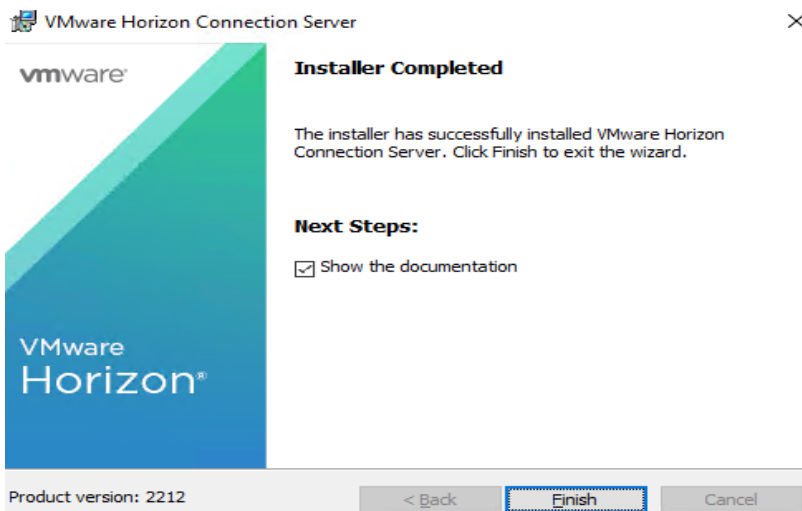


**Step 12.** Select General for the type of the type of installation. Click Install.





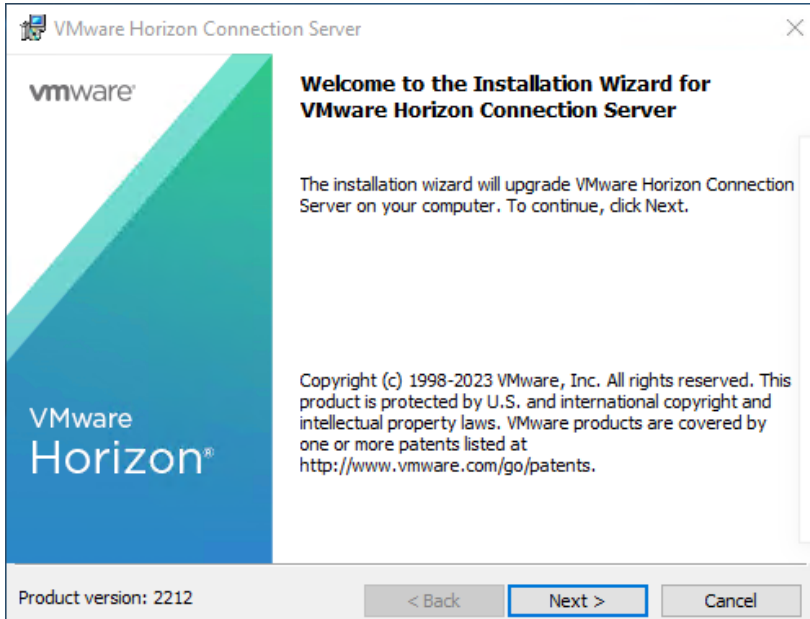
**Step 13.** After Horizon Connection Server installation is complete, click Finish.



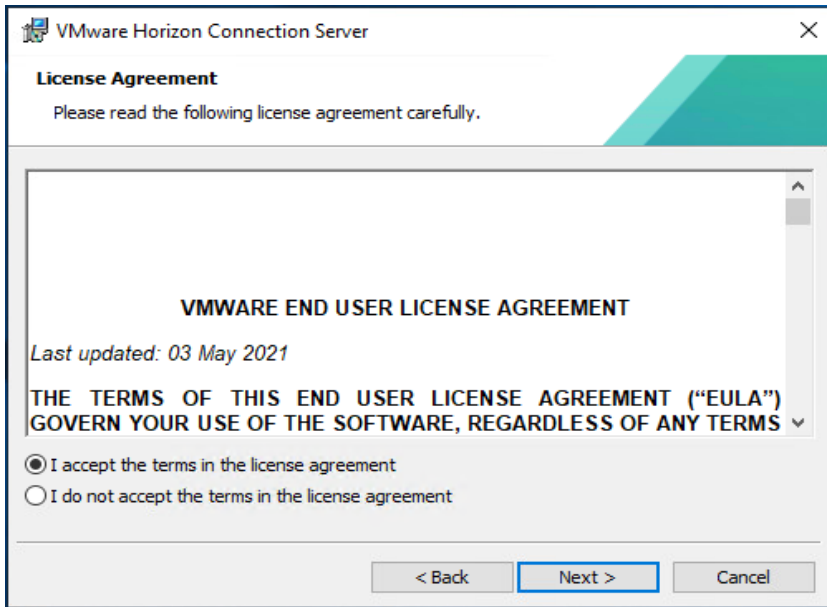
## Procedure 2. Install VMware Horizon Replica Server

**Step 1.** Click the Connection Server installer based on your Operating System.

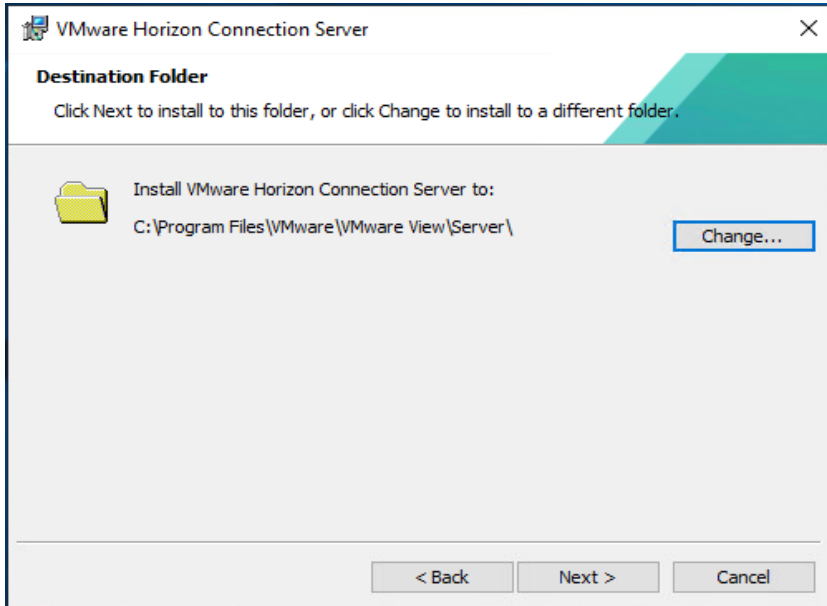
**Step 2.** Click Next.



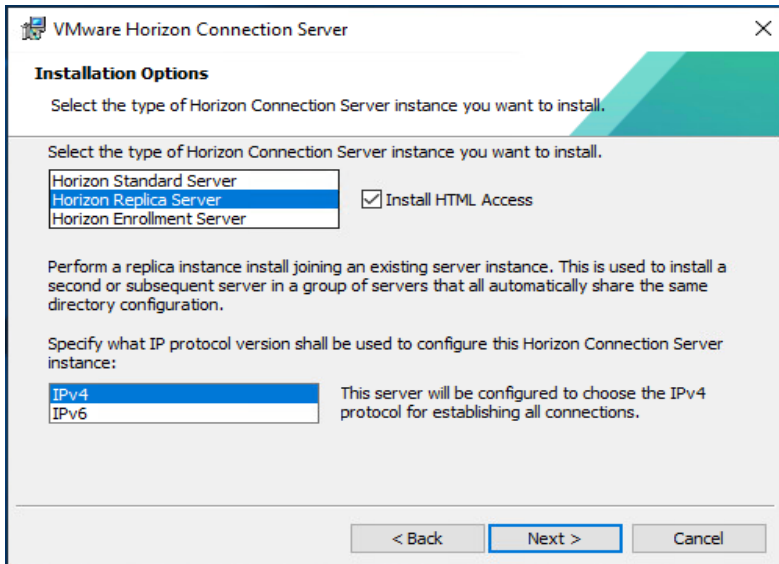
**Step 3.** Read and accept the End User License Agreement and click Next.



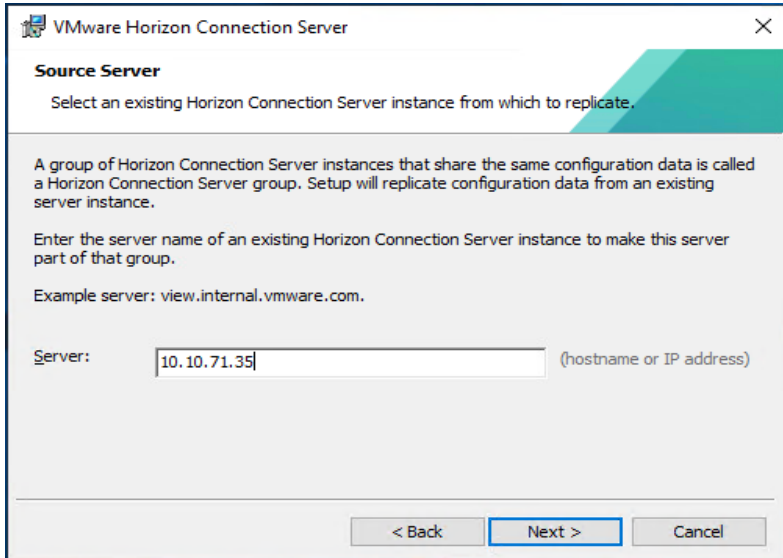
**Step 4.** Select the destination folder where you want to install the application and click Next.



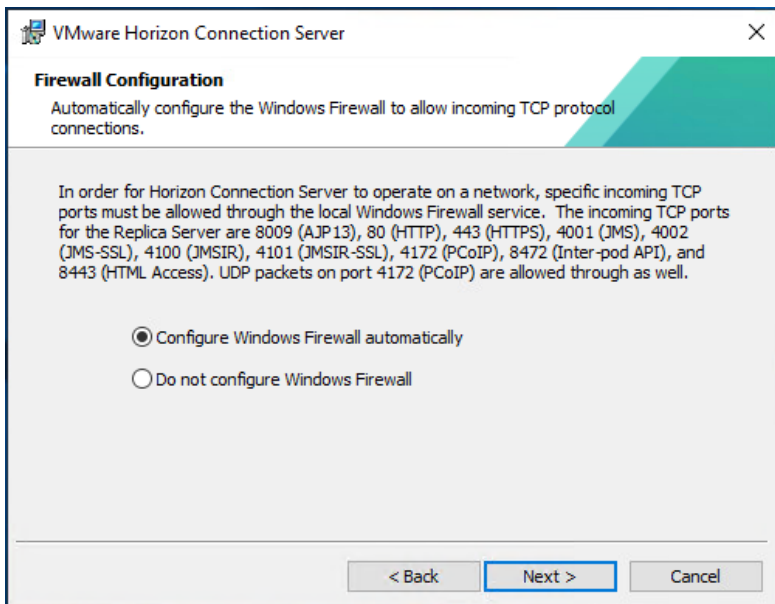
**Step 5.** Select the Replica Server and IPv4 for the IP protocol version.



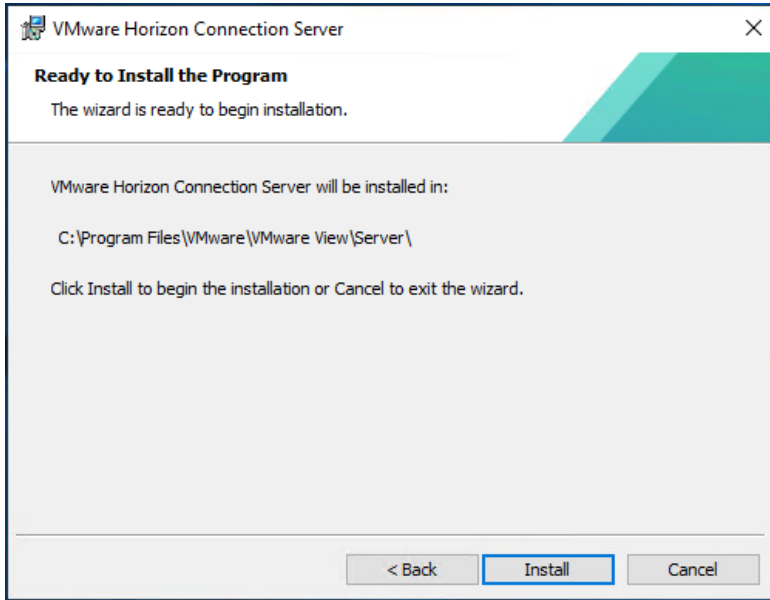
**Step 6.** Provide the existing Standard View Connection Server's FQDN or IP address and click Next.



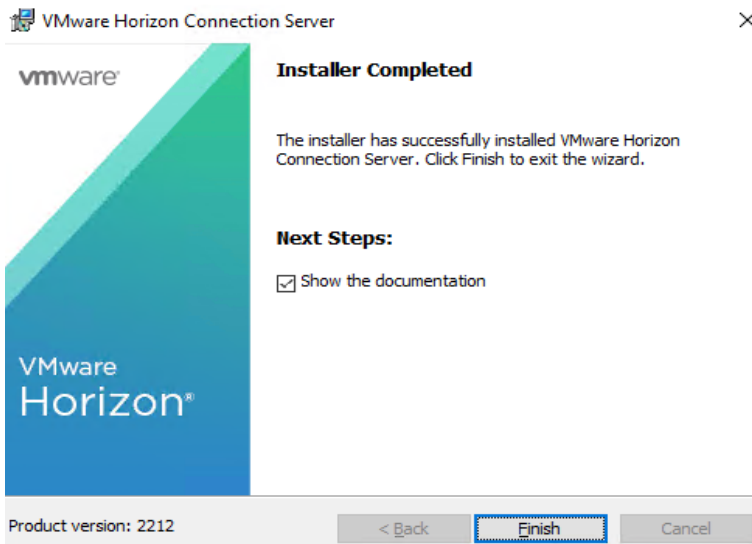
**Step 7.** Select Configure the Windows Firewall automatically.



**Step 8.** Click Install to begin the installation process.



**Step 9.** After installation is complete, click Finish.



## VMware Horizon Desktop Configuration

Management of the desktops, application pools and farms is accomplished in VMware Horizon Console (HTML5) or Horizon Administrator (Flex). We used Horizon Console to administer VMware Horizon environment in this validated design.

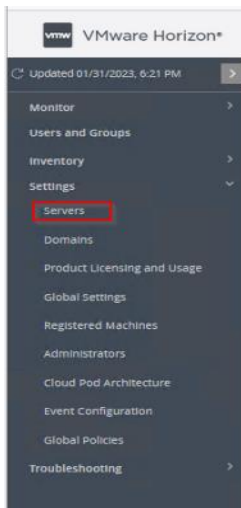
**Note:** VMware recommends using Horizon Console, an HTML5 based interface with enhanced security, capabilities, and performance.

### Procedure 1. Configure VMware Horizon Desktop

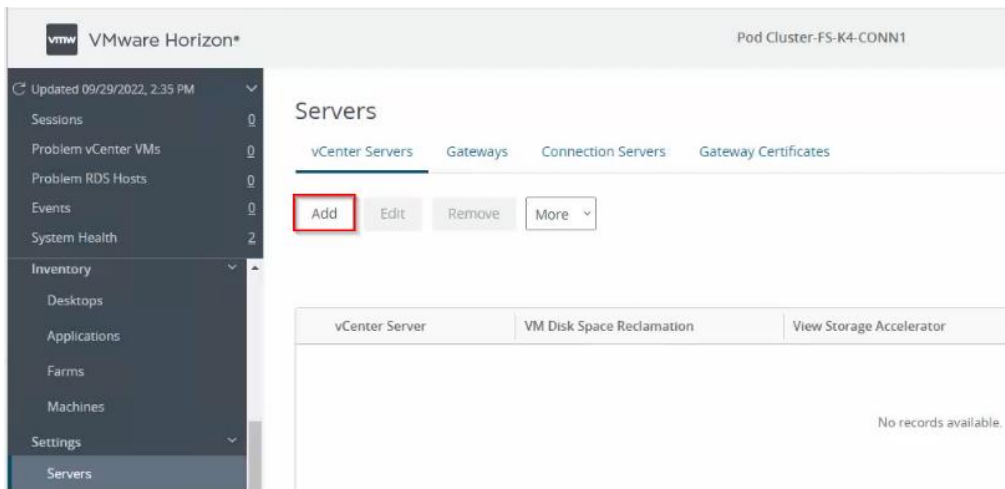
**Step 1.** Log into Horizon Console 2212 via a web browser using Address or FQDN>/admin/#/login.



**Step 2.** In Horizon Console, expand Settings and click Servers.



**Step 3.** Select the vCenter Settings tab and click Add.



**Step 4.** Provide the Server Address (IP or FQDN) and the credentials that Horizon will use to login to vCenter, then click Next.

### Add vCenter Server

1 vCenter Information

2 Storage

3 Ready to Complete

Asterisk (\*) denotes required field

\* Server address

\* User Name

\* Password

Description

**Step 5.** If you receive a message stating an invalid certificate, click View Certificate.

#### Invalid Certificate Detected ✕

09/29/2022, 2:39 PM

The identity of the specified vCenter Server cannot be verified for the following reasons:

- ⚠ Server's certificate subject name does not match the server's External URL.
- ⚠ Server's certificate is not trusted.
- ⚠ Server's certificate cannot be checked.

VMware recommends the use of certificates signed by a trusted Certificate Authority.

**Step 6.** Click Accept.

#### Certificate Information ✕

Issued to	vcsa-h8-2111.fsl151k.local
Issued by	CA
Valid from	04/08/2022, 3:17 PM to 04/07/2024, 3:17 PM
Subject	C=US CN=vcsa-h8-2111.fsl151k.local
Issuer	OU=VMware Engineering O=vcsa-h8-2111.fsl151k.local ST=California C=US DC=local DC=vsphere CN=CA
Serial Number	00 f7 a3 d6 b4 2f d0 f4 11
Version	3
Signature Algorithm	SHA256withRSA
Public Key Algorithm	RSA
Public Key	30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 a3 3c 88 9a 20 c6 53 40 aa 78 10 36 bc 86 40 3c 8d 31 2c 3d ed ae 4c fa 0f 0f de ad 6c 69 8b cb 15 7f c1 7f cf f9 ed 50 42 ea 66

**Step 7.** Keep the defaults, select Reclaim VM disk space and Enable Horizon Storage Accelerator with cache size of 1024MB. Click Next.

### Add vCenter Server

- ✔ vCenter Information
- 2** Storage
- 3 Ready to Complete

#### Storage Settings ⓘ

- Reclaim VM disk space
- Enable View Storage Accelerator

Default Host Cache Size  MB

Cache must be between 100 MB and 32,768 MB.

**Step 8.** Review the information you provided and click Submit.

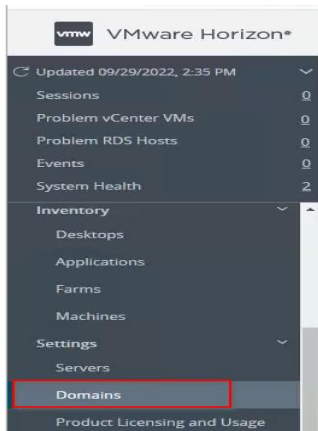
### Add vCenter Server

- ✔ vCenter Information
- ✔ Storage
- 3** Ready to Complete

vCenter Server	10.10.70.32
User Name	administrator@vsphere.local
Password	*****
Description	-
Server Port	443
Max Provision	20
Max Power	50
Max concurrent maintenance operations	12
Max Instant Clone Engine Provision	20
Enable View Storage Accelerator	Yes
Default host cache size (MB)	1,024
VM Disk Space Reclamation	Yes
Deployment Type	General

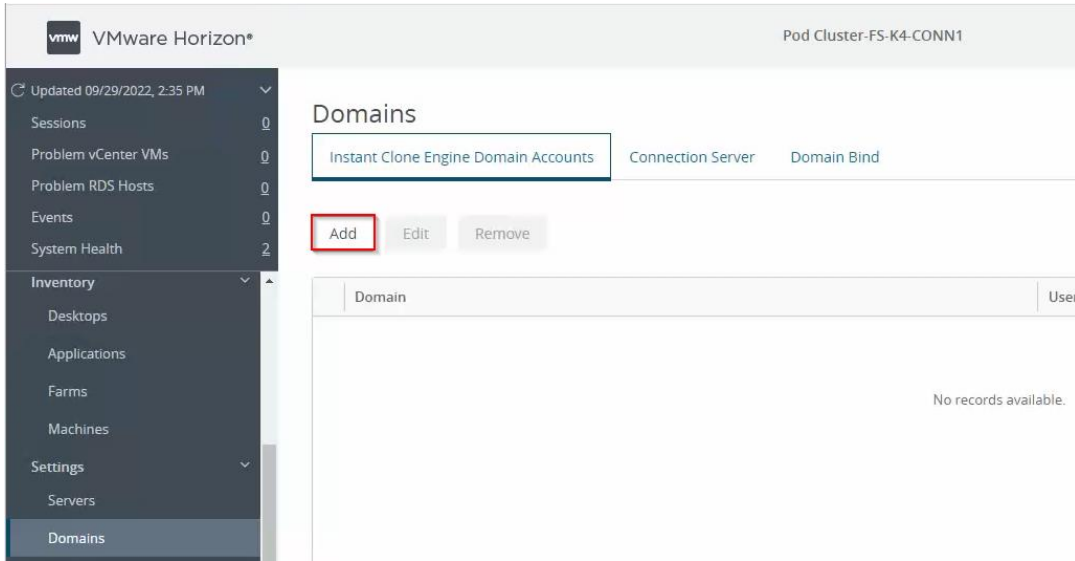
Cancel Previous Submit

**Step 9.** In Horizon Console, expand Settings and click Domains.

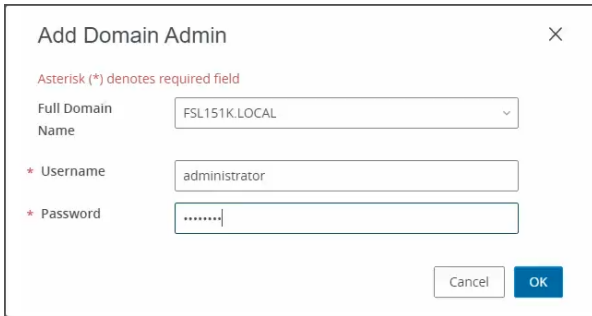




**Step 10.** Select the Instant Clone Engine Domain Accounts tab and click Add.

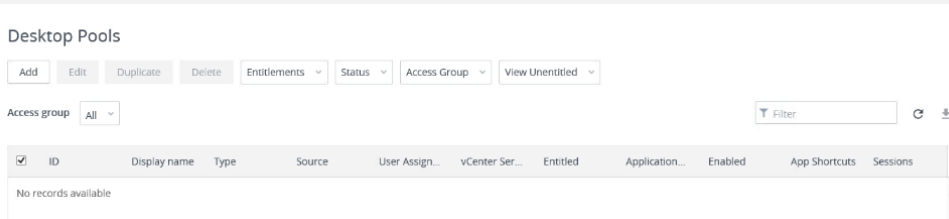


**Step 11.** Provide a domain name and credentials that Horizon will use to login to AD during Instant Clone management tasks, then click OK.

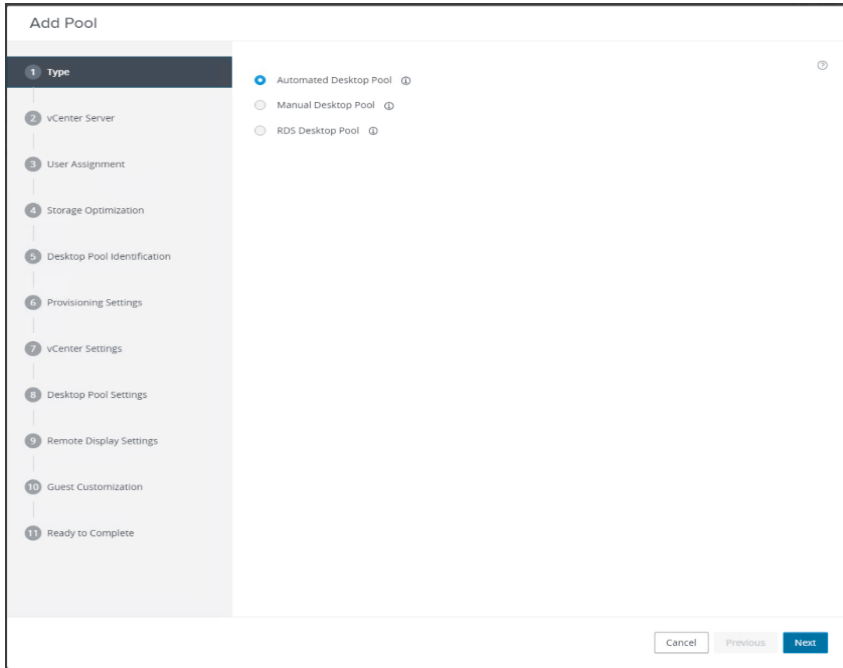


## Procedure 2. Create VDI Instant Clone Desktop Pool

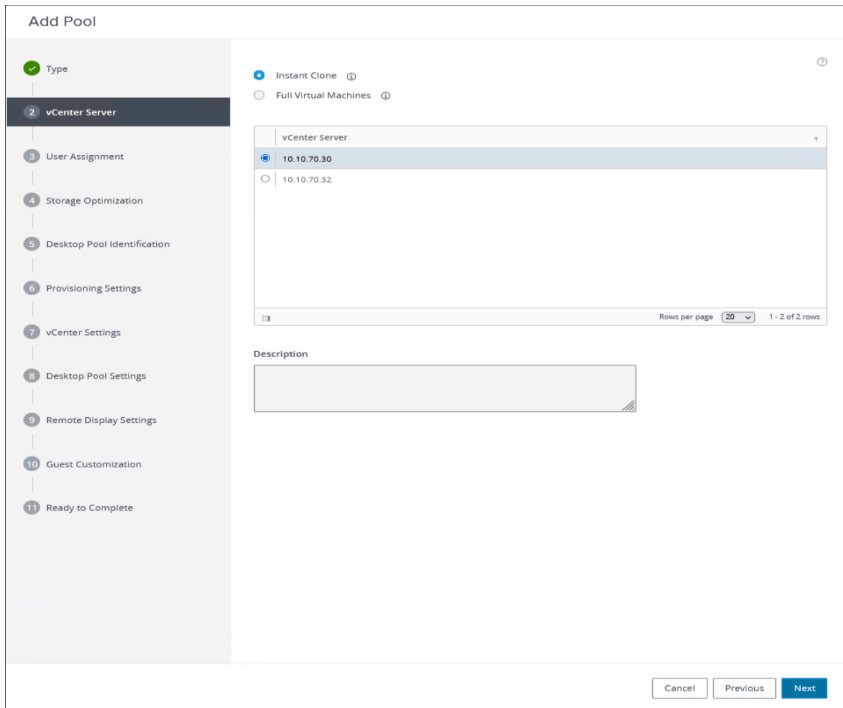
**Step 1.** In Horizon Console on the left plane, expand Inventory, select Desktops. Click Add.



**Step 2.** Select Type of Desktop pool to be created. Click Next.

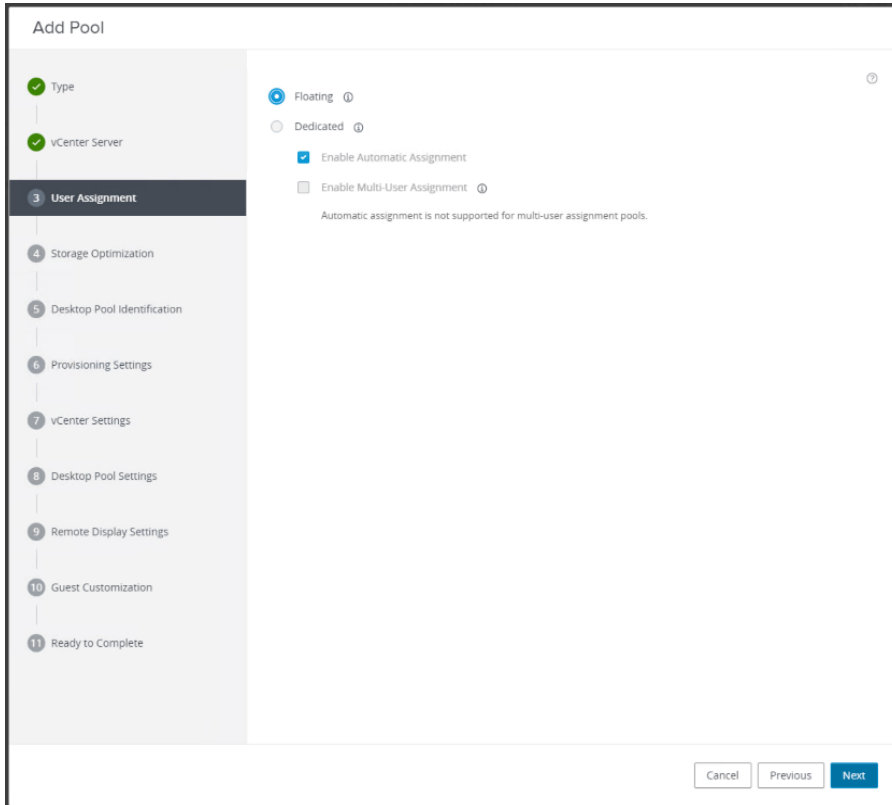


**Step 3.** Select the provisioning type for the desktops in the pool (we created Instant Clones and Full Virtual Machines pools in this design). Click Next.

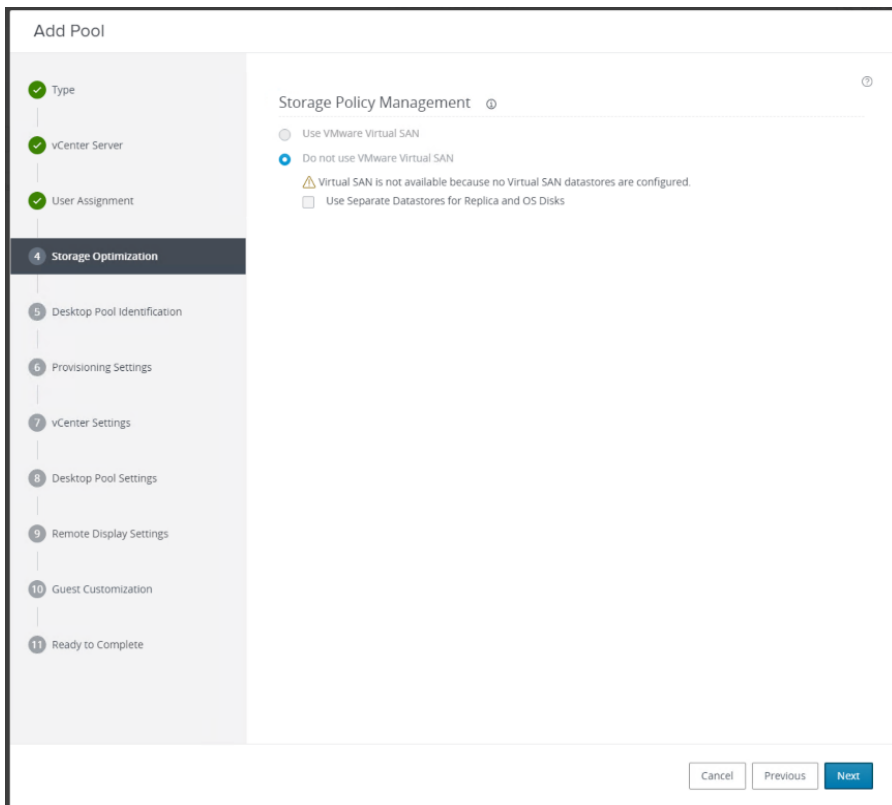


**Step 4.** Select the User assignment to be used by the desktop pool. Click Next.

**Note:** We used the Floating assignment for the Instance clone pool.



**Step 5.** Select the required option for Storage Policy Management. Click Next.



**Step 6.** Provide Desktop Pool ID and virtual display name. Click Next.

Add Pool - VDI-IC

Asterisk (\*) denotes required field

- Type
- vCenter Server
- User Assignment
- Storage Optimization
- 5 Desktop Pool Identification**
- 6 Provisioning Settings
- 7 vCenter Settings
- 8 Desktop Pool Settings
- 9 Remote Display Settings
- 10 Guest Customization
- 11 Ready to Complete

\* ID

Display Name

Access Group

Description

Cancel Previous Next

**Step 7.** Provide the naming pattern and the number of desktops to be provisioned. Click Next.

**Note:** In this Cisco Validate Design, we used:

Single Server pool - 240

Cluster pool - 1700

Add Pool - VDI-IC

Asterisk (\*) denotes required field

- Type
- vCenter Server
- User Assignment
- Storage Optimization
- Desktop Pool Identification
- 6 Provisioning Settings**
- 7 vCenter Settings
- 8 Desktop Pool Settings
- 9 Remote Display Settings
- 10 Guest Customization
- 11 Ready to Complete

Basic

Enable Provisioning

Stop Provisioning on Error

Virtual Machine Naming

Specify Names Manually

0 names entered  Enter Names

Use a Naming Pattern

\* Naming Pattern

Provision Machines

Machines on Demand

Min Number of Machines

All Machines Up-Front

Desktop Pool Sizing

\* Maximum Machines

\* Spare (Powered On) Machines

Virtual Device

Add vTPM Device to VMs

Cancel Previous Next

**Step 8.** Provide the parent VM, snapshot and host/cluster info, and data store information for the virtual machines to create. Click Next.

**Add Pool - VDI-IC**

Progress: 1 Type, 2 vCenter Server, 3 User Assignment, 4 Storage Optimization, 5 Desktop Pool Identification, 6 Provisioning Settings, **7 vCenter Settings**, 8 Desktop Pool Settings, 9 Remote Display Settings, 10 Guest Customization, 11 Ready to Complete

**Default Image**  
Asterisk (\*) denotes required field

- \* Golden Image in vCenter: /FlashStack/vm/W10-101322 [Browse]
- \* Snapshot: /gold-101622-1438/gold-101722-1215/gold-110822-1340 [Browse]

**Virtual Machine Location**

- \* VM Folder Location: /FlashStack/vm [Browse]

**Resource Settings**

- \* Cluster: /FlashStack/host/VDI [Browse]
- \* Resource Pool: /FlashStack/host/VDI/Resources [Browse]
- \* Datastores: 1 selected [Browse]

**Network**  
Golden Image network selected [Browse]

**VM Compute Profile Settings**  
Review the default VM Compute Profile settings and modify if needed.

- \* CPU: 2

Buttons: Cancel, Previous, Next

**Step 9.** Configure the State and Session Type for Desktop Pool Settings. Click Next.

**Add Pool - VDI-IC**

Progress: 1 Type, 2 vCenter Server, 3 User Assignment, 4 Storage Optimization, 5 Desktop Pool Identification, 6 Provisioning Settings, 7 vCenter Settings, **8 Desktop Pool Settings**, 9 Remote Display Settings, 10 Guest Customization, 11 Ready to Complete

**State**: Enabled

**Connection Server Restrictions**  
None [Browse]

**Category Folder**  
None [Browse]

**Client Restrictions**  Enabled

**Session Types**: Desktop

**Log Off After Disconnect**: Never

**Allow Users to Restart Machines**: No

**Allow Separate Desktop Sessions from Different Client Devices**: No

Buttons: Cancel, Previous, Next

**Step 10.** Configure the Remote Display Protocol. Click Next.

### Add Pool - VDI-IC

- ✓ Type
- ✓ vCenter Server
- ✓ User Assignment
- ✓ Storage Optimization
- ✓ Desktop Pool Identification
- ✓ Provisioning Settings
- ✓ vCenter Settings
- ✓ Desktop Pool Settings
- 9 Remote Display Settings**
- 10 Guest Customization
- 11 Ready to Complete

#### Remote Display Protocol

Default Display Protocol  
 VMware Blast

Allow Users to Choose Protocol  
 No

3D Renderer  
 Manage using vSphere Client

Allow Session Collaboration  Enabled

Requires VMware Blast Protocol.

**Step 11.** Select the AD Container for desktops to place in a Domain Controller computer location.

### Add Pool - VDI-IC

- ✓ Type
- ✓ vCenter Server
- ✓ User Assignment
- ✓ Storage Optimization
- ✓ Desktop Pool Identification
- ✓ Provisioning Settings
- ✓ vCenter Settings
- ✓ Desktop Pool Settings
- ✓ Remote Display Settings
- 10 Guest Customization**
- 11 Ready to Complete

Asterisk (\*) denotes required field

Domain  
 FSL151K.LOCAL(administrator)

\* AD Container  
 OU=VDI,OU=Target,OU=Computers,OU=LoginVSI

Allow Reuse of Existing Computer Accounts

Image Publish Computer Account

Use ClonePrep

Power-Off Script Name

Power-Off Script Parameters  
Example: p1 p2 p3

Post-Synchronization Script Name

Post-Synchronization Script Parameters  
Example: p1 p2 p3

Use a customization specification (SysPrep)

Name	Guest OS	Description
Win10 Spec	Windows	

**Step 12.** Review the deployment specifications and click Submit to complete the deployment.

The screenshot shows the 'Add Pool - VDI-IC' configuration wizard. On the left, a vertical progress bar lists steps from 'Type' to 'Guest Customization', with '11 Ready to Complete' highlighted at the bottom. The main area displays a list of configuration items and their values:

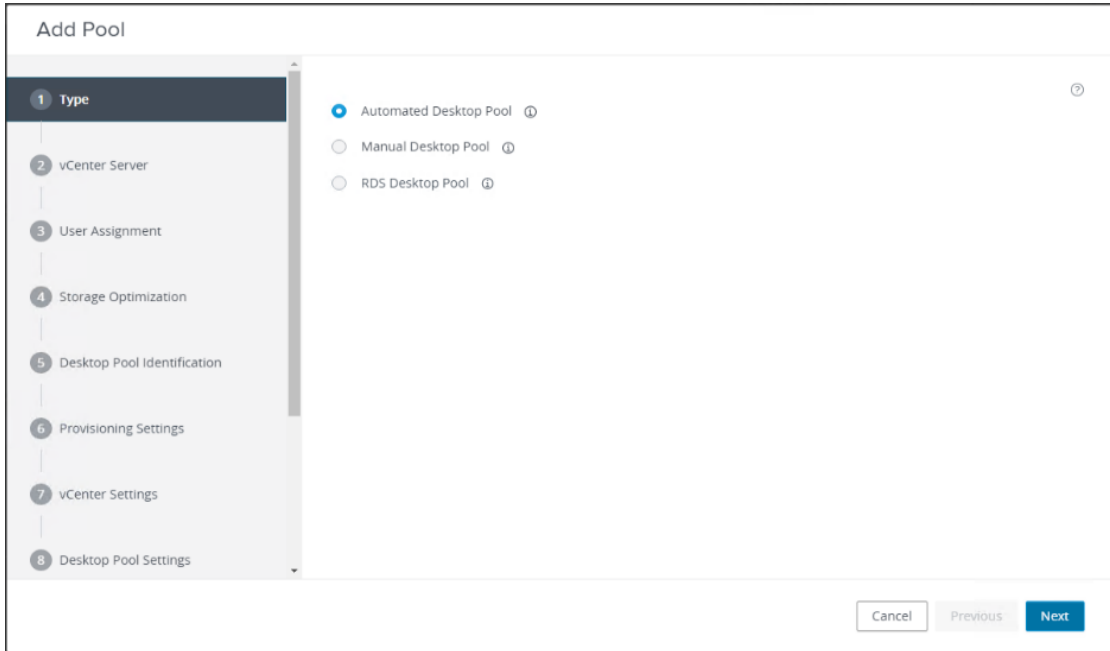
<input type="checkbox"/> Entitle Users After Adding Pool	
Type	Automated Desktop Pool
User Assignment	Floating Assignment
vCenter Server	10.10.70.32
Unique ID	VDI-IC
Description	-
Display Name	VDI-IC
Access Group	/
Desktop Pool State	Enabled
Session Types	Desktop
Client Restrictions	Disabled
Log Off After Disconnect	Never
Connection Server Restrictions	None
Category Folder	None
Allow Users to Restart Machines	No
Allow Separate Desktop Sessions from Different Client Devices	No
Default Display Protocol	VMware Blast

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Submit'.

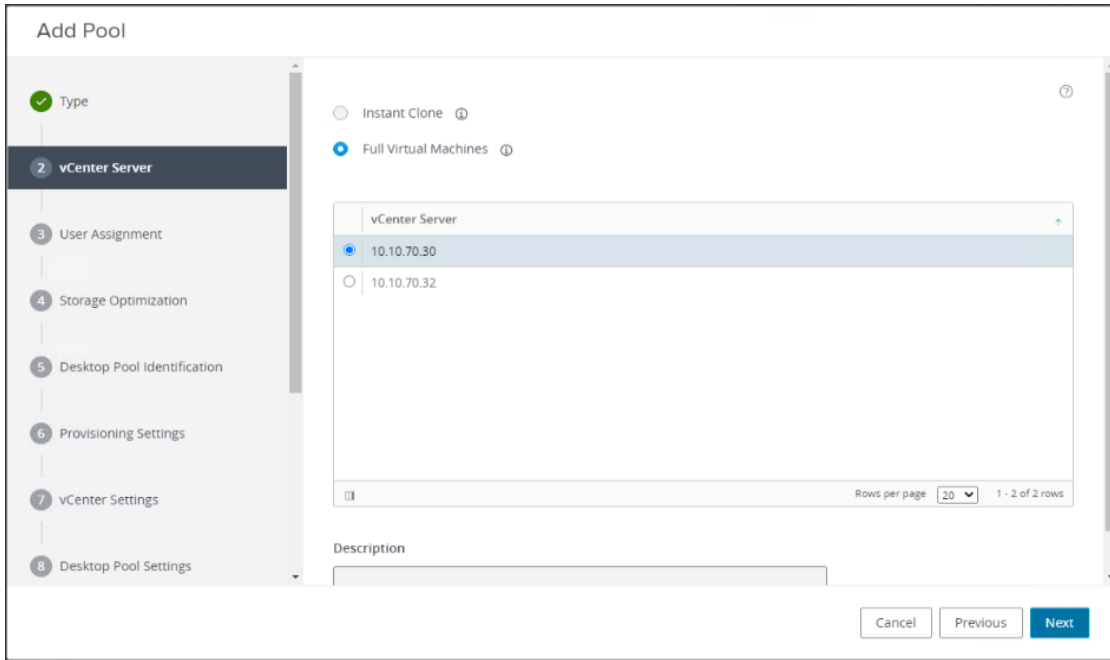
**Step 13.** Select Entitle users after this wizard finishes, to enable desktop user group/users to access this pool.

### Procedure 3. Create VDI Full Clone Desktop Pool

**Step 1.** Select Type of Desktop pool to be created. Click Next.

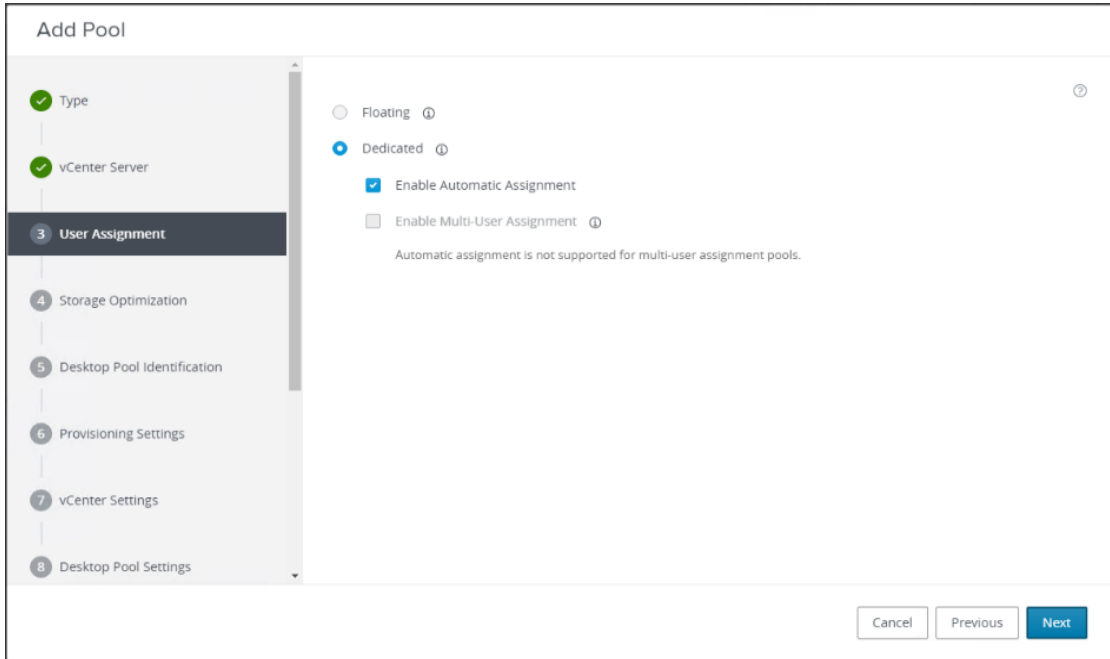


**Step 2.** Select the provisioning type for the desktops in the pool (we created Instant Clones and Full Virtual Machines pools in this design). Click Next.

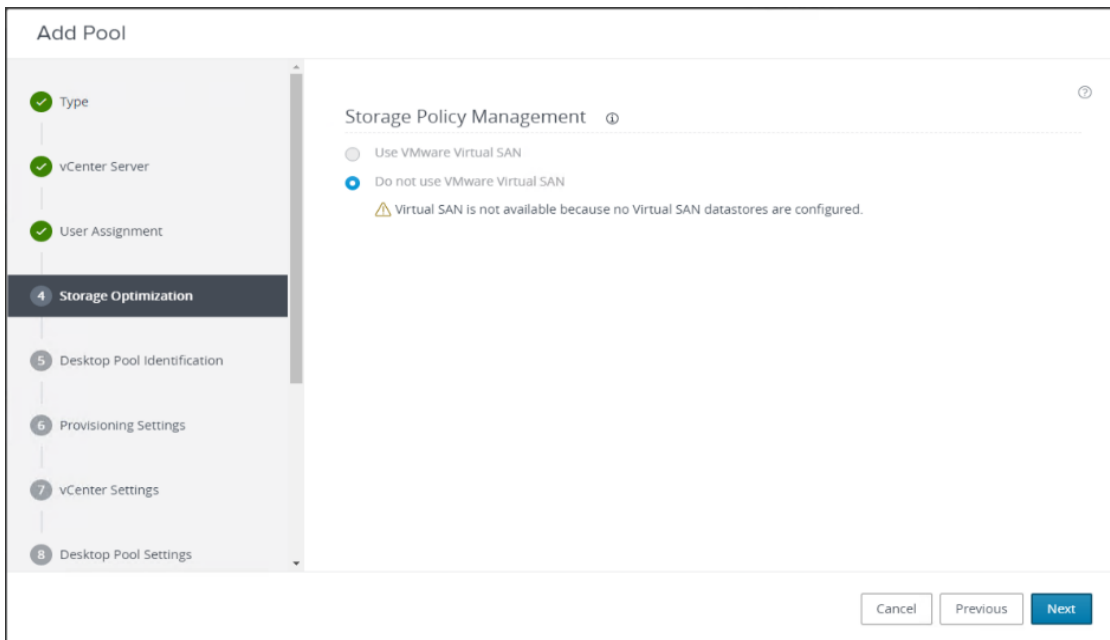


**Step 3.** Select the User assignment to be used by the desktop pool, we used Dedicated assignment for Full Cone pool. Click Next.





**Step 4.** On Storage Optimization screen click Next.



**Step 5.** Provide the Desktop Pool ID and Display Name. Click Next.

**Add Pool - VDI-FC**

Asterisk (\*) denotes required field

- Type
- vCenter Server
- User Assignment
- Storage Optimization
- 5 Desktop Pool Identification**
- 6 Provisioning Settings
- 7 vCenter Settings
- 8 Desktop Pool Settings

\* ID ⓘ  
VDI-FC

Display Name ⓘ  
VDI-FC

Access Group ⓘ  
/

Description

Cancel Previous Next

**Step 6.** Provide the naming pattern and the number of desktops to be provisioned. Click Next.

**Note:** In this validated design for VDI pools we used:

Single Server pool – 240

Cluster pool – 1700

**Add Pool - VDI-FC**

Asterisk (\*) denotes required field

- Type
- vCenter Server
- User Assignment
- Storage Optimization
- Desktop Pool Identification
- 6 Provisioning Settings**
- 7 vCenter Settings
- 8 Desktop Pool Settings

Basic

- Enable Provisioning ⓘ
- Stop Provisioning on Error

Virtual Machine Naming

- Specify Names Manually
- 0 names entered Enter Names
- Start machines in maintenance mode
- # Unassigned Machines Kept Powered On  
1
- Use a Naming Pattern ⓘ
- \* Naming Pattern  
VDI-W10-FC-

Provision Machines

- Machines on Demand

Cancel Previous Next

**Step 7.** Provide the parent VM, snapshot and host/cluster info, data store information for the virtual machines to create.

### Add Pool - VDI-FC

- Desktop Pool Identification
- Provisioning Settings
- vCenter Settings
- 8 Desktop Pool Settings
- 9 Remote Display Settings
- 10 Advanced Storage Options
- 11 Guest Customization
- 12 Ready to Complete

#### Virtual Machine Template

Asterisk (\*) denotes required field

\* **Template**

#### Virtual Machine Location

\* **VM Folder Location**

#### Resource Settings

\* **Host or Cluster**

\* **Resource Pool**

\* **Datastores**

1 selected

**Note:** A single datastore was used per 8 host pools.

#### Select Datastores

Select the Datastore Type

Select the datastores to use for this desktop pool. Only datastores that can be used by the selected host or cluster can be selected.

<input type="checkbox"/>	Datastore	Datastore Cluster	Capacity (GB)	Free Space (GB)	FS Type	Drive Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> ESXTOP		2,047.75	1,059.38	VMFS6	SSD
<input type="checkbox"/>	<input checked="" type="checkbox"/> X70RDS-1		184,319.75	184,087.07	VMFS6	SSD
<input type="checkbox"/>	<input checked="" type="checkbox"/> X70VDI-1		184,319.75	183,702.05	VMFS6	SSD
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> X70VDI-2		184,319.75	184,001.65	VMFS6	SSD

Free Space Selected 184,001.65 (A minimum of 14,420 GB is recommended for new virtual machines)

**Step 8.** Configure Desktop Pool settings.

**Add Pool - VDI-FC**

- Desktop Pool Identification
- Provisioning Settings
- vCenter Settings
- 8 Desktop Pool Settings**
- 9 Remote Display Settings
- 10 Advanced Storage Options
- 11 Guest Customization
- 12 Ready to Complete

State: Enabled

Connection Server Restrictions: None

Category Folder: None

Client Restrictions:  Enabled

Session Types: Desktop ⓘ

Remote Machine Power Policy: Take no power action ⓘ

Log Off After Disconnect: Never

Allow Users to Restart Machines:

**Step 9.** Provide the customizations to remote display protocol to be used by the desktops in the pool.

**Note:** We used the defaults in this deployment.

**Add Pool - VDI-FC**

- Desktop Pool Identification
- Provisioning Settings
- vCenter Settings
- Desktop Pool Settings
- 9 Remote Display Settings**
- 10 Advanced Storage Options
- 11 Guest Customization
- 12 Ready to Complete

Remote Display Protocol

Default Display Protocol: VMware Blast

Allow Users to Choose Protocol: No

3D Renderer: Disabled ⓘ

VRAM Size: 96 MB  
More VRAM can improve 3D performance.

Maximum number of monitors: 2 ⓘ  
Might require power cycle of related virtual machines. ⓘ

Maximum Resolution of Any One Monitor: 1920x1200 ⓘ

**Note:** For Advanced Storage Options, we used defaults in this deployment.

**Step 10.** Click Next.

**Add Pool - VDI-FC**

- Desktop Pool Identification
- Provisioning Settings
- vCenter Settings
- Desktop Pool Settings
- Remote Display Settings
- 10 Advanced Storage Options**
- 11 Guest Customization
- 12 Ready to Complete

### Advanced Storage Options

The following features are recommended based on your resource selection. Options that are not supported by the selected hardware are disabled.

**Asterisk (\*) denotes required field**

- Use View Storage Accelerator
  - Regenerate Storage Accelerator After:  Days

#### Blackout Times

Storage accelerator regeneration and VM disk space reclamation do not occur during blackout times. The same blackout policy applies to both operations.

Day	Time

**Step 11.** Select the VM Customization Specification to be used during deployment. Click Next.

**Add Pool - VDI-FC**

- Desktop Pool Identification
- Provisioning Settings
- vCenter Settings
- Desktop Pool Settings
- Remote Display Settings
- Advanced Storage Options
- 11 Guest Customization**
- 12 Ready to Complete

None - Customization will be done manually  
 Do not Power on Virtual Machines After Creation  
 Use this customization specification  
 Allow Reuse of Existing Computer Accounts

Name	Guest OS	Description
<input checked="" type="radio"/> Win10 Spec	Windows	

Rows per page: 20 1 - 1 of 1 row(s)

**Note:** The following VM Customization Specifications were used:

Name	Win10 Spec
Description	
OS type	Windows
OS options	Generate new security ID
Registration info	Owner name: cisco Organization: cisco
Computer name	Use Virtual Machine name
> Windows license	No product key specified
> Log in	Do not log in automatically as Administrator
Time zone	(UTC-08:00) Pacific Time (US & Canada)
Network type	Standard
Workgroup/Domain	Windows Server domain: FSL151K.LOCAL

**Step 12.** Review all the deployment specifications and click Submit to complete the deployment.

Setting	Value
Entitle Users After Adding Pool	<input type="checkbox"/>
Type	Automated Desktop Pool
User Assignment	Dedicated Assignment
Assign on First Login	Yes
Enable Multi-User Assignment	No
vCenter Server	10.10.70.29
Unique ID	W10_FULL
Description	-
Display Name	W10-FULL
Access Group	/
Desktop Pool State	Enabled
Session Types	Desktop
Display Assigned Machine Name	No
Remote Machine Power Policy	Take no power action
Automatically Logoff After Disconnect	Never
Connection Server Restrictions	None
Category Folder	None

**Note:** The automated pool creation will add AD computer accounts to Computers OU. Move this account according to your policies, in our case the machine accounts were moved to Login VSI OU.

#### Procedure 4. Create RDSH Farm and Pool

**Step 1.** Select the FARM when creating the RDS Pool.

**Note:** You can entitle the user access at the RDS Pool level for RDS users/groups who can access the RDS VMs.

**Step 2.** Select Type of the Farm. We used Automated Farm the RDS desktops in this design. Click Next.

**Add Farm**

✓ Type

2 vCenter Server

3 Storage Optimization

4 Identification and Settings

5 Load Balancing Settings

6 Provisioning Settings

7 vCenter Settings

8 Guest Customization

9 Ready to Complete

Automated Farm ⓘ

Manual Farm ⓘ

Cancel Previous Next

**Step 3.** Select the provisioning type and vCenter Server for the desktops in the pool. Click Next.

**Add Farm**

✓ Type

2 vCenter Server

3 Storage Optimization

4 Identification and Settings

5 Load Balancing Settings

6 Provisioning Settings

7 vCenter Settings

8 Guest Customization

9 Ready to Complete

Instant Clone ⓘ

vCenter Server
<input checked="" type="radio"/> 10.10.70.30
<input type="radio"/> 10.10.70.32

Rows per page 20 1 - 2 of 2 rows

Description

Cancel Previous Next

**Step 4.** On Storage Optimization screen, click Next.

### Add Farm

- ✔ Type
- ✔ vCenter Server
- 3 Storage Optimization
- 4 Identification and Settings
- 5 Load Balancing Settings
- 6 Provisioning Settings
- 7 vCenter Settings
- 8 Guest Customization
- 9 Ready to Complete

#### Storage Policy Management ⓘ

Use VMware Virtual SAN  
 Do not use VMware Virtual SAN

⚠ Virtual SAN is not available because no Virtual SAN datastores are configured.

Use Separate Datastores for Replica and OS Disks

Cancel Previous Next

**Step 5.** Provide the ID and Description for RDS FARM. Select the Display Protocol which is required for users to connect to the RDS Sessions. Click Next.

### Add Farm - WS2019

- ✔ Type
- ✔ vCenter Server
- ✔ Storage Optimization
- 4 Identification and Settings
- 5 Load Balancing Settings
- 6 Provisioning Settings
- 7 vCenter Settings
- 8 Guest Customization
- 9 Ready to Complete

Asterisk (\*) denotes required field

**\* ID**

**Description**

**Access Group**

**Farm Settings**

**Default Display Protocol** ⓘ

**Allow Users to Choose Protocol**

**3D Renderer** ⓘ

vSphere doesn't support 3D option other than NVIDIA Grid vGPU for Windows Server OS

**Pre-launch Session Timeout (Applications Only)** ⓘ

  minutes

Cancel Previous Next

**Step 6.** Select Load Balancing Settings. Click Next.



Add Farm - WS2019

- Type
- vCenter Server
- Storage Optimization
- Identification and Settings
- 5 Load Balancing Settings**
- 6 Provisioning Settings
- 7 vCenter Settings
- 8 Guest Customization
- 9 Ready to Complete

Use Custom Script  Enabled ⓘ

Include Session Count  Enabled ⓘ

Asterisk (\*) denotes required field

\* CPU Usage Threshold  
0 ⓘ

\* Memory Usage Threshold  
0 ⓘ

\* Disk Queue Length Threshold  
0 ⓘ

\* Disk Read Latency Threshold  
0 ⓘ

\* Disk Write Latency Threshold  
0 ⓘ

\* Connecting Session Threshold  
0 ⓘ

\* Load Index Threshold  
0 ⓘ

Cancel Previous Next

**Step 7.** Provide naming pattern and a number of virtual machines to create. Click Next.

Add Farm - RDS

- Type
- vCenter Server
- Storage Optimization
- Identification and Settings
- Load Balancing Settings
- 6 Provisioning Settings**
- 7 vCenter Settings

Asterisk (\*) denotes required field

Basic

Enable Provisioning ⓘ

Stop Provisioning on Error

Virtual Machine Naming ⓘ

\* Naming Pattern  
RDS

Farm Sizing

\* Maximum Machines  
80

\* Minimum Number of Ready (Provisioned) Machines during Instant Clone Maintenance Operations  
0

Cancel Previous Next

**Step 8.** Select the previously created golden image to be used as RDS host. Select datastore where RDS hosts will be deployed. Click Next.

Add Farm - WS2019

- Type
- vCenter Server
- Storage Optimization
- Identification and Settings
- Load Balancing Settings
- Provisioning Settings
- 7 vCenter Settings**
- 8 Guest Customization
- 9 Ready to Complete

**Default Image**

Asterisk (\*) denotes required field

\* Golden Image in vCenter

\* Snapshot

**Virtual Machine Location**

\* VM Folder Location

**Resource Settings**

\* Cluster

\* Resource Pool

\* Datastores  
 1 selected

**Network**  
 Golden Image network selected

**Step 9.** Select the AD Container for desktops to place in a Domain Controller computer location.

Add Farm - WS2019

- Type
- vCenter Server
- Storage Optimization
- Identification and Settings
- Load Balancing Settings
- Provisioning Settings
- vCenter Settings
- 8 Guest Customization**
- 9 Ready to Complete

Asterisk (\*) denotes required field

**Domain**

\* AD Container

Allow Reuse of Existing Computer Accounts

**Image Publish Computer Account**  
 ⓘ

Use ClonePrep

**Power-Off Script Name**  
 ⓘ

**Power-Off Script Parameters**  
  
 Example: p1 p2 p3

**Post-Synchronization Script Name**  
 ⓘ

**Post-Synchronization Script Parameters**  
  
 Example: p1 p2 p3

**Step 10.** Review the Farm information and click Submit to complete the RDS Farm creation.

**Add Farm - WS2019**

- ✓ Type
- ✓ vCenter Server
- ✓ Storage Optimization
- ✓ Identification and Settings
- ✓ Load Balancing Settings
- ✓ Provisioning Settings
- ✓ vCenter Settings
- ✓ Guest Customization
- 9 Ready to Complete**

ID	WS2019
Description	-
Access Group	/
<b>Farm Settings</b>	
Default Display Protocol	Microsoft RDP
Allow Users to Choose Protocol	No
3D Renderer	Manage using vSphere Client
Pre-launch Session Timeout (Applications Only)	10 minutes
Empty Session Timeout (Applications Only)	1 minute
When Timeout Occurs	Disconnect
Logoff Disconnected Sessions	Never
Bypass Session Timeout	Disabled
Allow Session Collaboration	Disabled
CPU	4

Cancel Previous **Submit**

**Procedure 5. Create RDS Pool**

When the RDS FARM is created, you need to create an RDS pool to absorb the RDS VMS FARM into the Pool for further managing the RDS pool.

**Step 1.** Select type as RDS Desktop Pool.

**Add Pool**

- 1 Type**
- 2 Desktop Pool ID
- 3 Desktop Pool Settings
- 4 Select RDS Farms
- 5 Ready to Complete

Automated Desktop Pool ⓘ  
 Manual Desktop Pool ⓘ  
 **RDS Desktop Pool** ⓘ

Cancel Previous **Next**

**Step 2.** Provide an ID and Display Name for the Pool. Click Next.

Add Pool - RDSPool

1 Type

2 Desktop Pool ID

3 Desktop Pool Settings

4 Select RDS Farms

5 Ready to Complete

ID

Display Name

Description

Cancel Previous Next

**Step 3.** Leave the default settings for the Desktop Pool Settings. Click Next.

Add Pool - RDSPool

1 Type

2 Desktop Pool ID

3 Desktop Pool Settings

4 Select RDS Farms

5 Ready to Complete

State

Connection Server Restrictions  
None

Category Folder  
None

Client Restrictions  Enabled

Allow Users to initiate separate Desktop sessions from different client devices (desktops only)

Cancel Previous Next

**Step 4.** Select the RDS Farm. Select the farm which was already created for this desktop pool. Click Next.

Add Pool - RDSPool

Type  
 Desktop Pool ID  
 Desktop Pool Settings  
 **Select RDS Farms**  
 Ready to Complete

Create a new RDS farm  
 Select an RDS farm for this desktop pool

Filter

Farm ID	Description	RDS Hosts	Max Number of Co...	Status
RDS2019		2	2	Farm disabled

**Step 5.** Review the RDS Pool deployment specifications and click Next to complete the RDS pool deployment.

Add Pool - RDSPool

Type  
 Desktop Pool ID  
 Desktop Pool Settings  
 Select RDS Farms  
 **Ready to Complete**

Entitle Users After Adding Pool

Entitle Users After Adding Pool

Type: RDS Desktop Pool  
 Unique ID: RDSPool  
 Description: -  
 Display Name: RDSPool  
 Desktop Pool State: Enabled  
 Client Restrictions: No  
 Connection Server Restrictions: None  
 Category Folder: None  
 Allow Users to Initiate separate Desktop sessions from different client devices (desktops only): No  
 RDS Farm: RDS2019  
 Number of RDS Hosts in the Farm: 2

**Step 6.** Select Entitle users after this wizard finishes, to enable desktop user group/users to access this pool.

## Test Setup, Configuration, and Load Recommendation

This chapter contains the following:

- [Cisco UCS Test Configuration for Single Blade Scalability](#)
- [Cisco UCS Test Configuration for Full Scale Testing](#)
- [Test Methodology and Success Criteria](#)

We tested a single Cisco UCS B200 M6 Compute Node to validate against the performance of one server and eight Cisco UCS B200 M6 Compute Nodes as a cluster on a single chassis to illustrate linear scalability for each workload use case tested.

### Cisco UCS Test Configuration for Single Blade Scalability

This test case validates Recommended Maximum Workload per host server using VMware Horizon 8 2212 with 300 Multi Server VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions.

Figure 27. Test Configuration for Single Server Scalability VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) multi-session

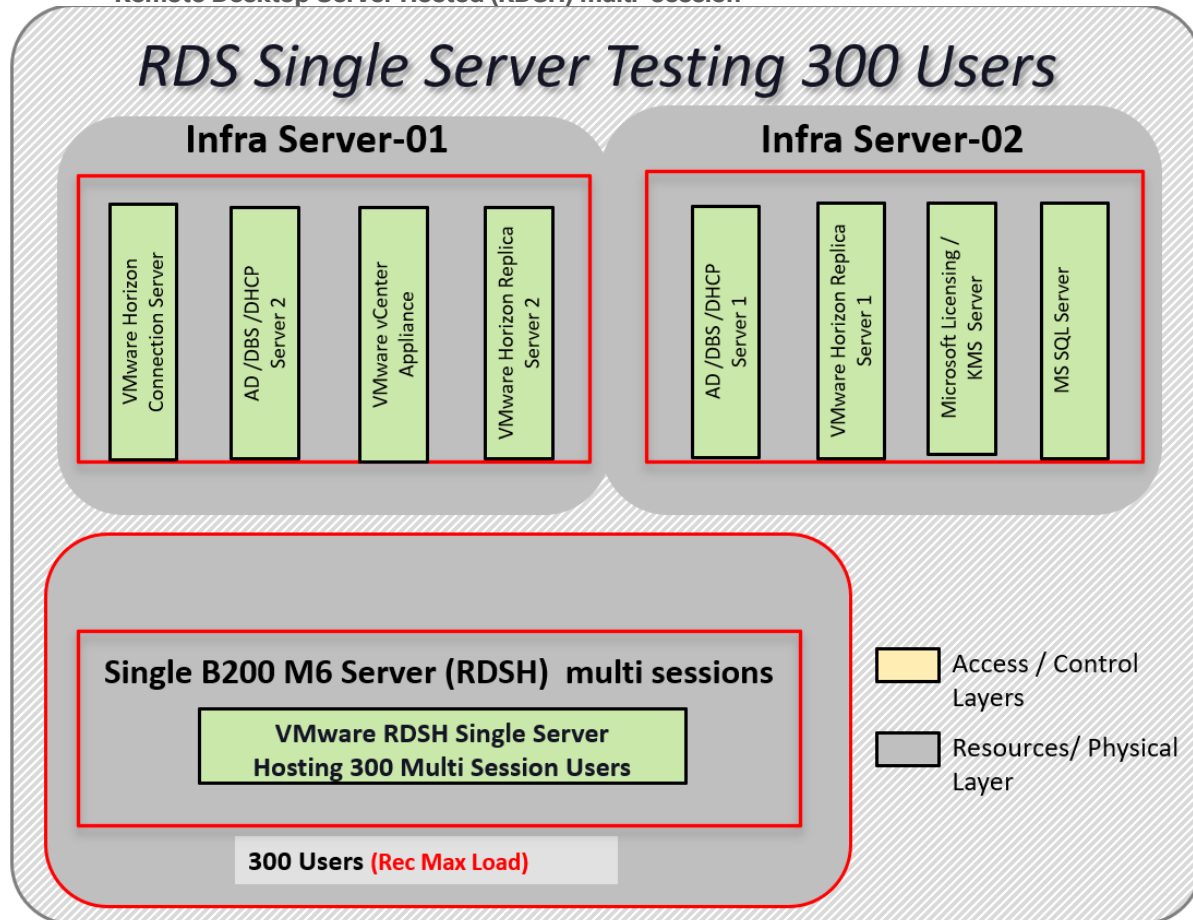
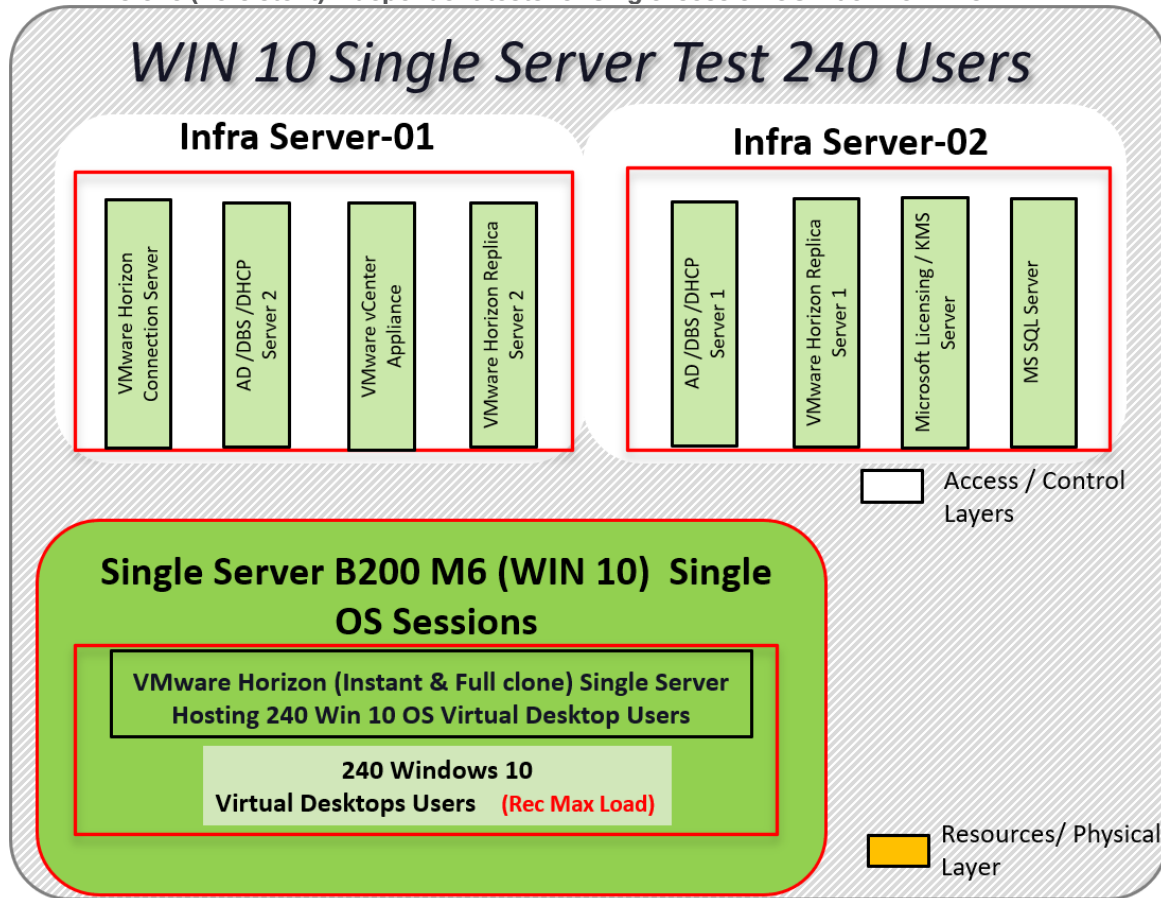


Figure 28. Test configuration for Single Server Scalability VMware Horizon 8 2212 Instant Clone and Full Clone (Persistent) independent tests for Single-session OS machine VDAs



Hardware components:

- Cisco UCS 5108 Chassis.
- 2 Cisco UCS 6454 4th Gen Fabric Interconnects.
- 1 Cisco UCS B200 M6 Compute Node Servers with Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM for all host blades.
- 2 Cisco Nexus 93180YC-FX Access Switches.
- 2 Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switches.
- Pure Storage FlashArray//X70 R3 with dual redundant controllers, with 20 1.92TB DirectFlash NVMe drives.

Software components:

- Cisco UCS firmware 4.2(2d).
- Pure Storage Purity//FA 6.3.3.
- ESXi 7.0 Update 3d for host blades.
- VMware Horizon 8 2212.
- Microsoft SQL Server 2019.
- Microsoft Windows 10 64 bit (1909), 2vCPU, 3 GB RAM, 40 GB HDD (master).

- Microsoft Windows Server 2019 (1809), 4vCPU, 24GB RAM, 100 GB vDisk (master).
- Microsoft Office 2019 32-bit.
- FSLogix 2105 HF\_01.
- Login VSI 4.1.39 Knowledge Worker Workload (Benchmark Mode).

### Cisco UCS Test Configuration for Full Scale Testing

These test cases validate eight blades in a cluster hosting three distinct workloads using VMware Horizon 8.8 or VMware 2212 with:

- 2300 VMware Horizon Remote Desktop Server Hosted (RDSH) sessions Instant-clone RDS VMs
- 1700 VMware Horizon VDI-Non persistent Instant clone Single-session OS sessions
- 1700 VMware Horizon VDI-Persistent Full Clone Single-session OS sessions

**Note:** Server N+1 fault tolerance is factored into this solution for each cluster/workload.

**Figure 29.** Test Configuration for Full Scale / Cluster Test VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) multi-session OS machines

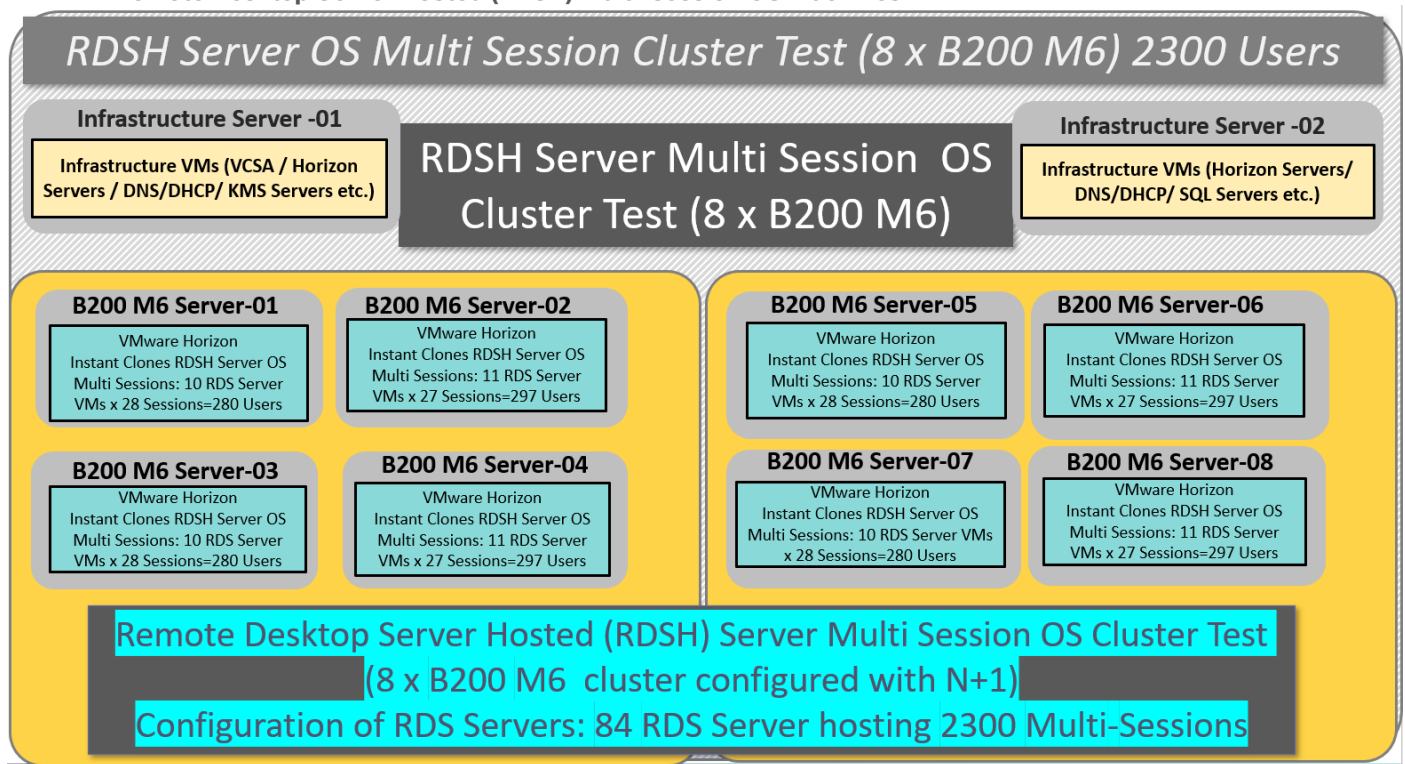




Figure 30. Test Configuration for Full Scale VMware Horizon 8 2212 Instant Clone (non-persistent) single-session Win 10 OS machines

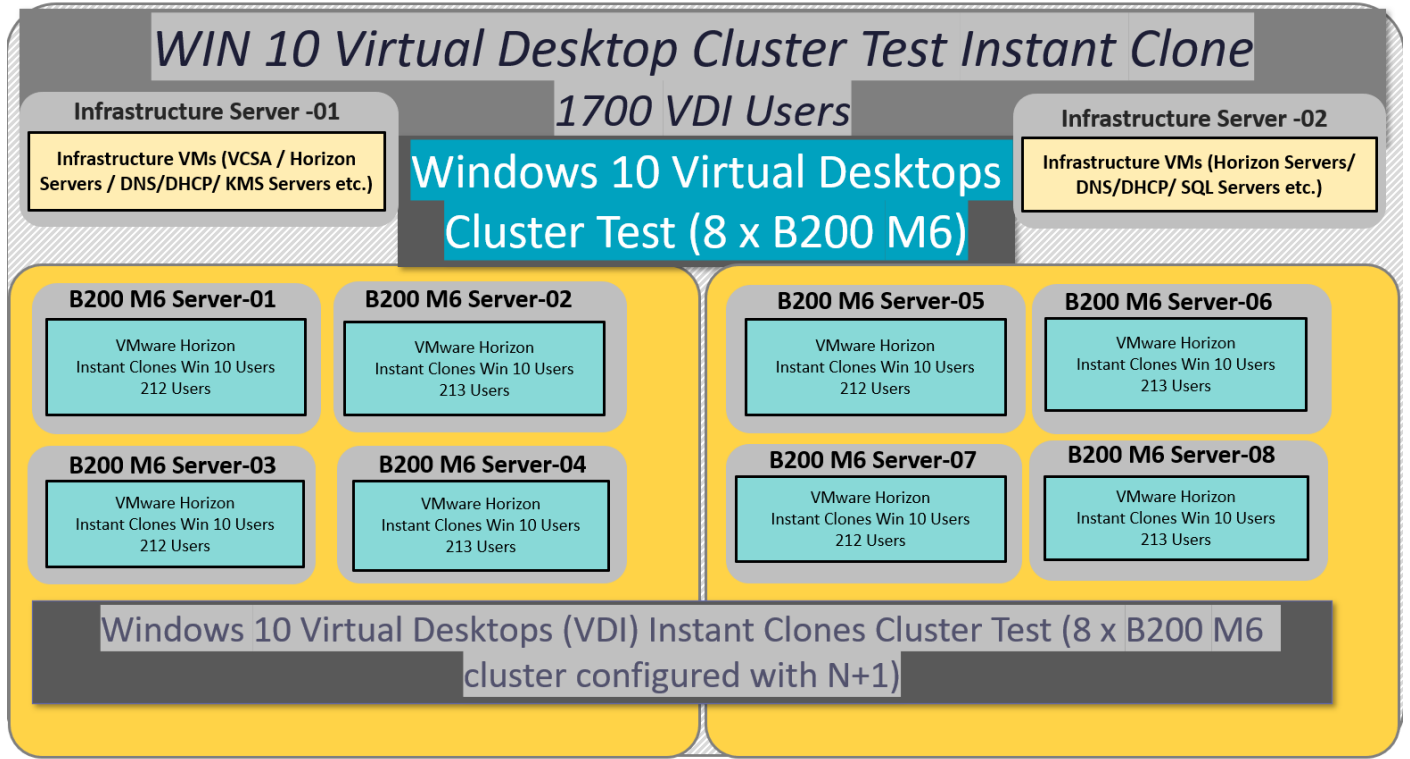
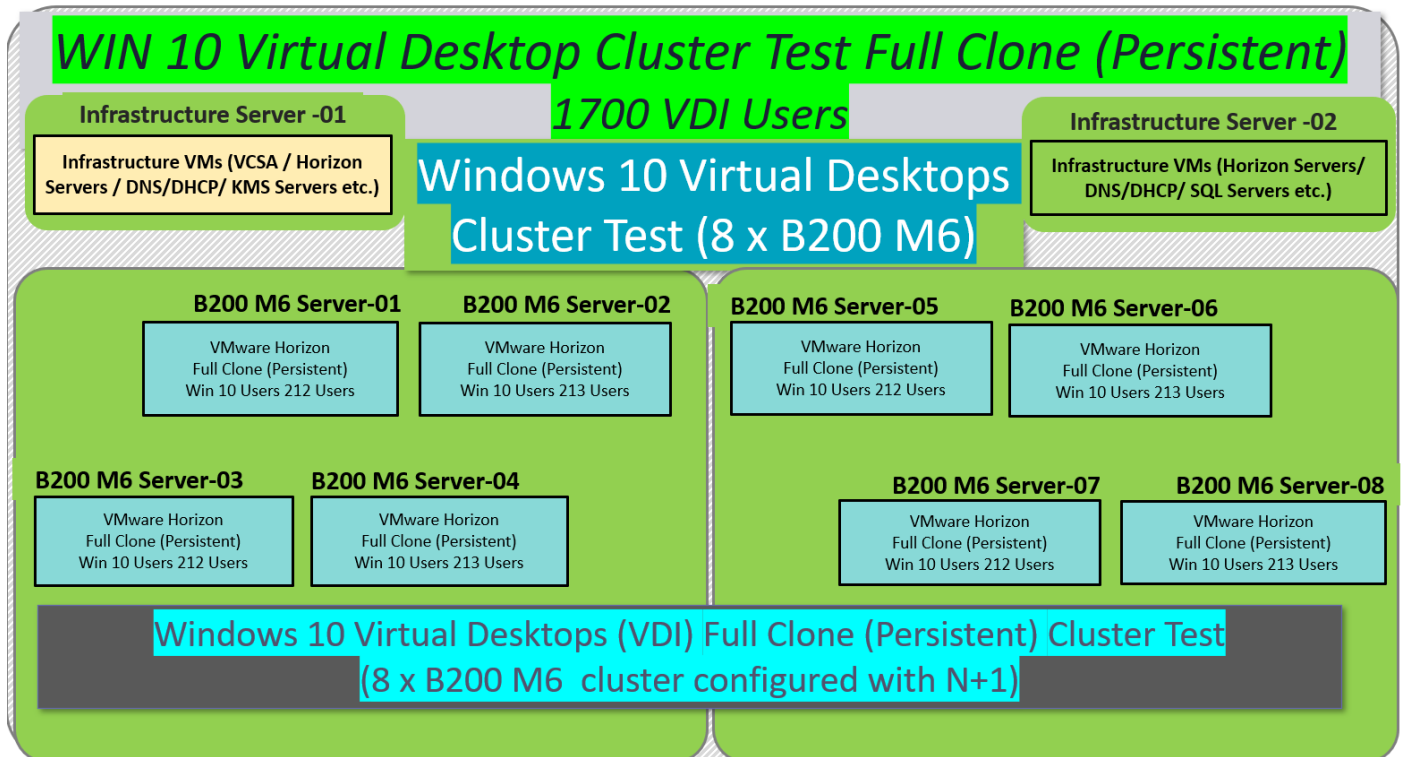


Figure 31. Test Configuration for Full Scale VMware Horizon 8 2212 Full Clone (Persistent) single-session Win 10 OS machines



Hardware components:

- 
- Cisco UCS 5108 Chassis.
  - 2 Cisco UCS 6454 4th Gen Fabric Interconnects.
  - 8 Cisco UCS B200 M6 Compute Node Servers with Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM for all host blades.
  - Cisco VIC 1440 CNA (1 per blade).
  - 2 Cisco Nexus 93180YC-FX Access Switches.
  - 2 Cisco MDS 9132T 32-Gb 32-Port Fibre Channel Switches.
  - Pure Storage FlashArray//X70 R3 with dual redundant controllers, with 20 1.92TB DirectFlash NVMe drives.

Software components:

- Cisco UCS firmware 4.2(2d).
- Pure Storage Purity//FA 6.3.3.
- ESXi 7.0 Update 3d for host blades.
- VMware Horizon 8 2212.
- Microsoft SQL Server 2019.
- Microsoft Windows 10 64 bit (1909), 2vCPU, 3 GB RAM, 40/100 GB (full clone) HDD (master).
- Microsoft Windows Server 2019 (1809), 8vCPU, 32GB RAM, 100 GB vDisk (master).
- Microsoft Office 2019 32-bit.
- FSLogix 2015 HF\_01.
- Login VSI 4.1.39 Knowledge Worker Workload (Benchmark Mode).

## Test Methodology and Success Criteria

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

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

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

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

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

---

## Test Procedure

This chapter contains the following:

- [Pre-Test Setup for Single and Multi-Blade Testing](#)
- [Test Run Protocol](#)
- [Success Criteria](#)
- [VSImax 4.1.x Description](#)

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 VMware Horizon Console 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. For testing where the user session count exceeds 1000 users, we will now deem the test run successful with up to 1% session failure rate.

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

1. Time 0:00:00 Start PerfMon/Esxtop Logging on the following system:
  - Infrastructure and VDI Host Blades used in the test run
2. vCenter used in the test run.
3. All Infrastructure virtual machines used in test run (AD, SQL, brokers, image mgmt., and so on)
4. Time 0:00:10 Start Storage Partner Performance Logging on Storage System.
5. Time 0:05: Boot Virtual Desktops/RDS Virtual Machines using View Connection server.
6. The boot rate should be around 10-12 virtual machines per minute per server.
7. Time 0:06 First machines boot.
8. Time 0:30 Single Server or Scale target number of desktop virtual machines booted on 1 or more blades.
9. No more than 30 minutes for boot up of all virtual desktops is allowed.
10. Time 0:35 Single Server or Scale target number of desktop virtual machines desktops available on View Connection Server.
11. Virtual machine settling time.
12. No more than 60 Minutes of rest time is allowed after the last desktop is registered on the XD Studio or available in View Connection Server dashboard. Typically, a 30-45-minute rest period is sufficient.
13. Time 1:35 Start Login VSI 4.1.x Office Worker Benchmark Mode Test, setting auto-logoff time at 15 minutes, with Single Server or Scale target number of desktop virtual machines utilizing sufficient number of Launchers (at 20-25 sessions/Launcher).

- 
14. Time 2:23 Single Server or Scale target number of desktop virtual machines desktops launched (48-minute benchmark launch rate).
  15. Time 2:25 All launched sessions must become active. id test run within this window.
  16. Time 2:40 Login VSI Test Ends (based on Auto Logoff 15 minutes period designated above).
  17. Time 2:55 All active sessions logged off.
  18. Time 2:57 All logging terminated; Test complete.
  19. Time 3:15 Copy all log files off to archive; Set virtual desktops to maintenance mode through broker; Shutdown all Windows machines.
  20. Time 3:30 Reboot all hypervisor hosts.
  21. Time 3:45 Ready for the new test sequence.

## Success Criteria

Our pass criteria for this testing is as 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.x 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 VMware Horizon Console 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. FlashStack Data Center with Cisco UCS and VMware Horizon 8 2212 on VMware ESXi 7.0 Update 3d Test Results.

The purpose of this testing is to provide the data needed to validate VMware Horizon Remote Desktop Sessions (RDS) and VMware Horizon Virtual Desktop (VDI) instant-clones and VMware Horizon Virtual Desktop (VDI) full-clones models using ESXi and vCenter to virtualize Microsoft Windows 10 desktops and Microsoft Windows Server 2019 sessions on Cisco UCS B200 M6 Compute Node Servers using the Pure Storage FlashArray//X70 R3 storage system.

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

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

---

## VSImax 4.1.x Description

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

After a test is performed, the response times can be analyzed to calculate the maximum active session/desktop capacity. Within Login VSI this is calculated as VSImax. When the system is coming closer to its saturation point, response times will rise. When reviewing the average response time, it will be clear the response times escalate at saturation point.

This VSImax is the “Virtual Session Index (VSI).” With Virtual Desktop Infrastructure (VDI) and Terminal Services (RDS) workloads this is valid and useful information. This index simplifies comparisons and makes it possible to understand the true impact of configuration changes on hypervisor host or guest level.

### Server-Side Response Time Measurements

It is important to understand why specific Login VSI design choices have been made. An important design choice is to execute the workload directly on the target system within the session instead of using remote sessions. The scripts simulating the workloads are performed by an engine that executes workload scripts on every target system and are initiated at logon within the simulated user’s desktop session context.

An alternative to the Login VSI method would be to generate user actions client side through the remoting protocol. These methods are always specific to a product and vendor dependent. More importantly, some protocols simply do not have a method to script user actions client side.

For Login VSI, the choice has been made to execute the scripts completely server side. This is the only practical and platform independent solution, for a benchmark like Login VSI.

### Calculating VSImax v4.1.x

The simulated desktop workload is scripted in a 48 minute loop when a simulated Login VSI user is logged on, performing generic Office worker activities. After the loop is finished it will restart automatically. Within each loop, the response times of sixteen specific operations are measured in a regular interval: sixteen times in within each loop. The response times of these five operations are used to determine VSImax.

The five operations from which the response times are measured are:

- Notepad File Open (NFO)

Loading and initiating VSINotepad.exe and opening the openfile dialog. This operation is handled by the OS and by the VSINotepad.exe itself through execution. This operation seems almost instant from an end-user’s point of view.

- Notepad Start Load (NSLD)

Loading and initiating VSINotepad.exe and opening a file. This operation is also handled by the OS and by the VSINotepad.exe itself through execution. This operation seems almost instant from an end-user’s point of view.

- Zip High Compression (ZHC)

This action copy's a random file and compresses it (with 7zip) with high compression enabled. The compression will very briefly spike CPU and disk IO.

- Zip Low Compression (ZLC)

This action copy's a random file and compresses it (with 7zip) with low compression enabled. The compression will very briefly spike disk IO and creates some load on the CPU.

- CPU

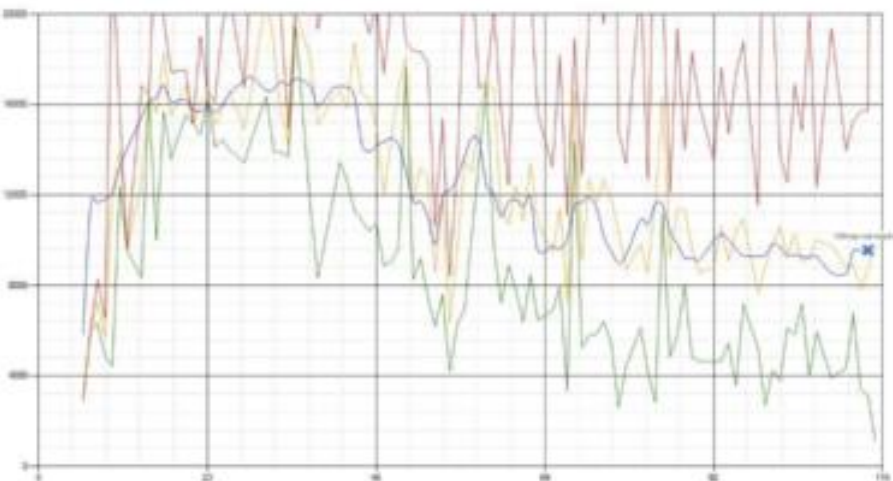
Calculates a large array of random data and spikes the CPU for a short period of time.

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, and so on. 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 32. Sample of a VSI Max Response Time Graph, Representing a Normal Test**



**Figure 33. Sample of a VSI Test Response Time Graph with a Performance Issue**





---

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

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

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

The following actions are part of the VSImax v4.1.x 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.x, 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 the 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.

To summarize:

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

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

Always a 5 Login VSI response time samples are averaged + 40 percent of the number of “active” sessions. For example, if the active sessions are 60, then latest 5 + 24 (=40 percent of 60) = 31 response time measurement is 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 the lowest 2 results are removed (5 percent of 31 = 1.55, rounded to 2). At 60 users the average is then calculated over the 27 remaining results.

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

In VSImax v4.1.x this latency threshold is fixed to 1000ms, this allows better and fairer comparisons between two different systems, especially when they have different baseline results. Ultimately, in VSImax v4.1.x, the

performance of the system is not decided by the total average response time, but by the latency 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 3000 the maximum average response time may not be greater than 4000ms (3000+1000).

When the threshold is not exceeded by the average VSI response time during the test, VSI<sub>max</sub> is not hit, and the number 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.x 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 VSI<sub>max</sub> method is introduced: VSI<sub>max</sub> v4.1.x. This methodology gives much better insight into system performance and scales to extremely large systems.

### Single-Server Recommended Maximum Workload

For both the VMware Horizon 8 2212 Virtual Desktop and VMware Horizon 8 2212 Remote Desktop Service Hosts (RDSH) 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 ensure that end user experience is outstanding. Additionally, during steady state, the processor utilization should average no more than 90-95 percent.

**Note:** Memory should never be oversubscribed for Desktop Virtualization workloads.

**Table 22.** 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 30-45 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



---

Test Phase	Description
Steady state	The steady state phase is where all users are logged in and performing various workload tasks such as using Microsoft Office, Web browsing, PDF printing, playing videos, and compressing files (typically for the 15-minute duration)
Logoff	Sessions finish executing the Login VSI workload and logoff

## Test Results

This chapter contains the following:

- [Single-Server Recommended Maximum Workload Testing](#)
- [Full Scale Workload Testing](#)

### 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 following three tests:

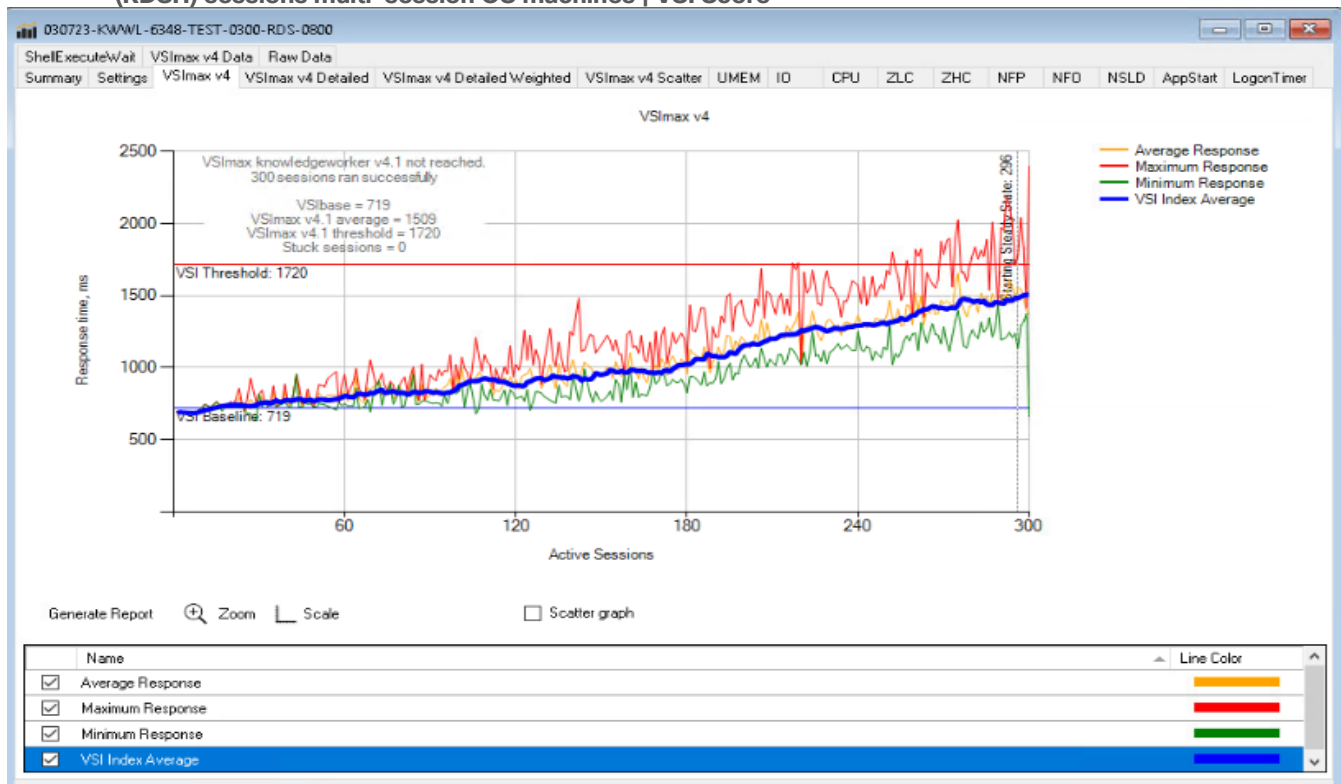
- 300 VMware Horizon Remote Desktop Server Hosted (RDSH) Instant clone multi session OS RDS sessions (Random)
- 240 VMware Horizon VDI non-persistent Instant clone single OS sessions (Random)
- 240 VMware Horizon VDI persistent full clone single OS sessions (Static)

#### Single-Server Recommended Maximum Workload for non-persistent single-session OS Random Sessions with 300 Users

The recommended maximum workload for a Cisco UCS B200 M6 blade server with dual Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM is 300 VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions with 8 vCPU and 32 GB RAM.

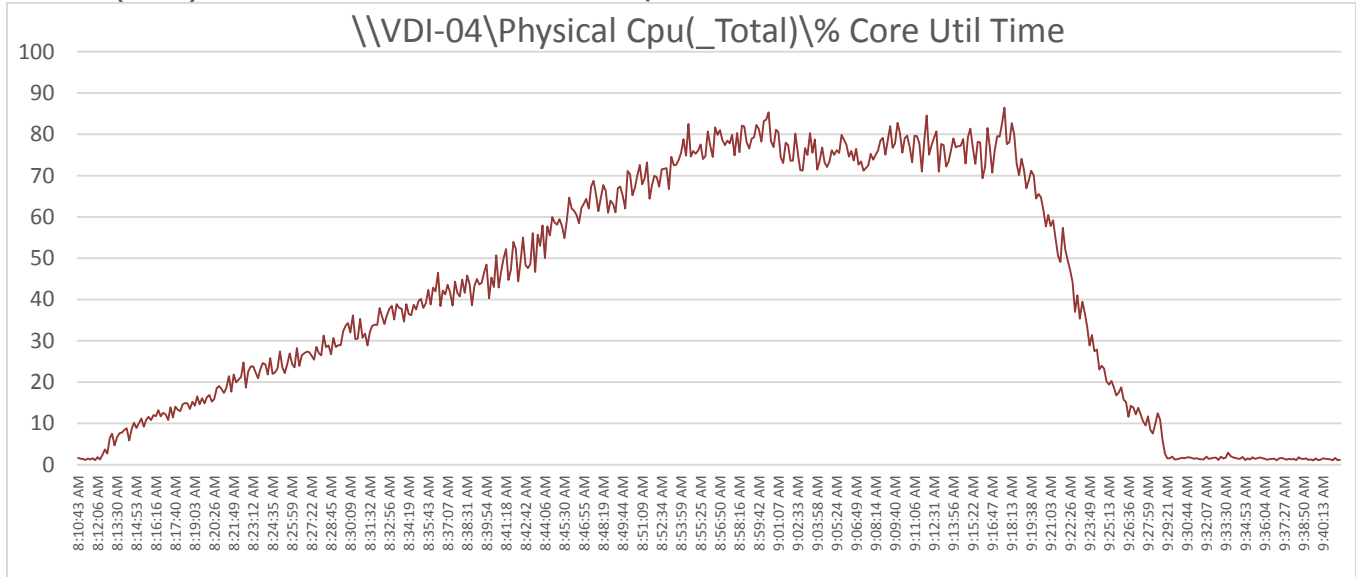
Login VSI performance data is shown below:

**Figure 34. Single Server | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) sessions multi-session OS machines | VSI Score**

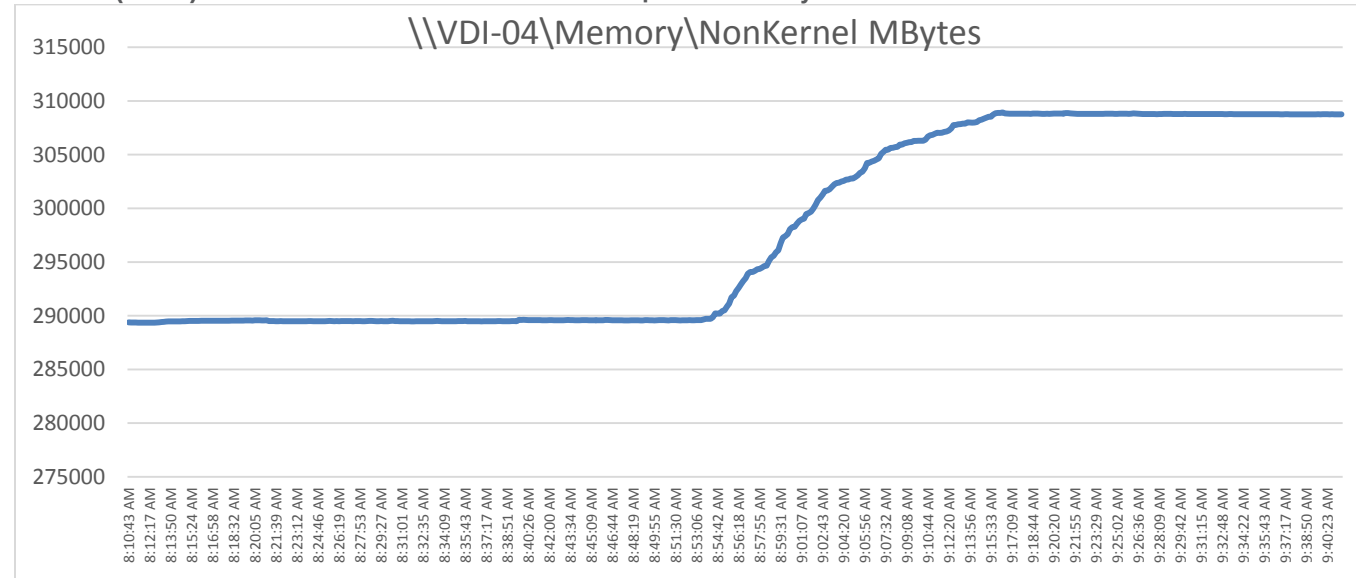


Performance data for the server running the workload is shown below:

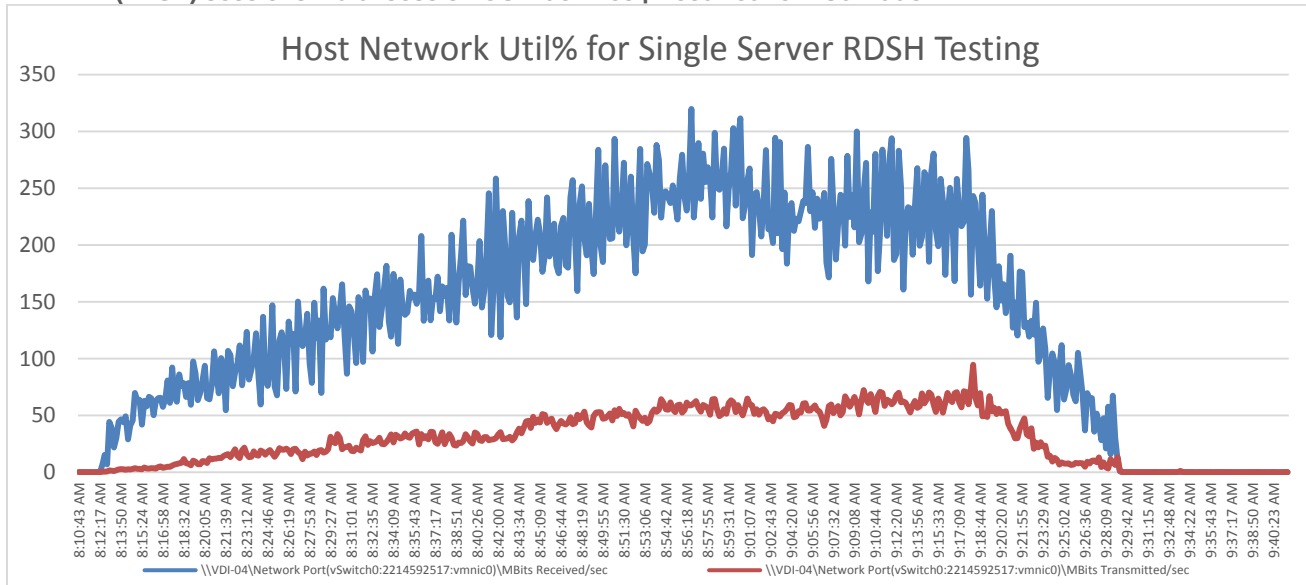
**Figure 35. Single Server | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions Multi-session OS machines | Host CPU Utilization**



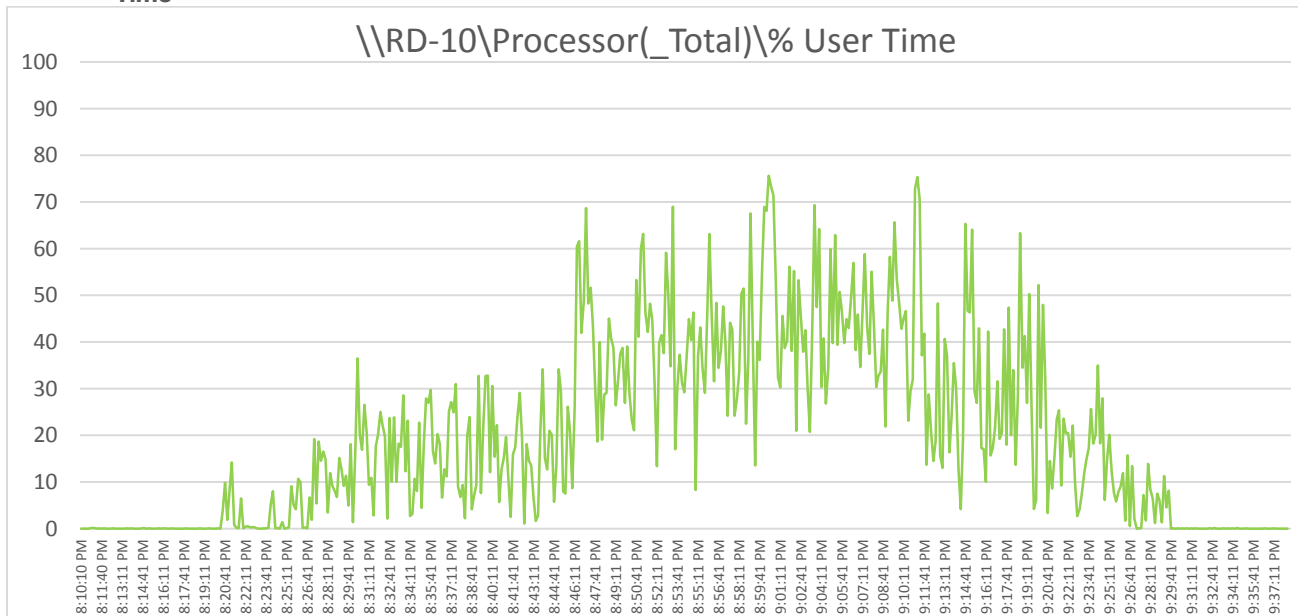
**Figure 36. Single Server | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) sessions multi-session OS machines | Host Memory Utilization**



**Figure 37. Single Server | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) sessions multi-session OS machines | Host Network Utilization**



**Figure 38. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) sessions multi-session OS machines | RDS Server Total % User Time**

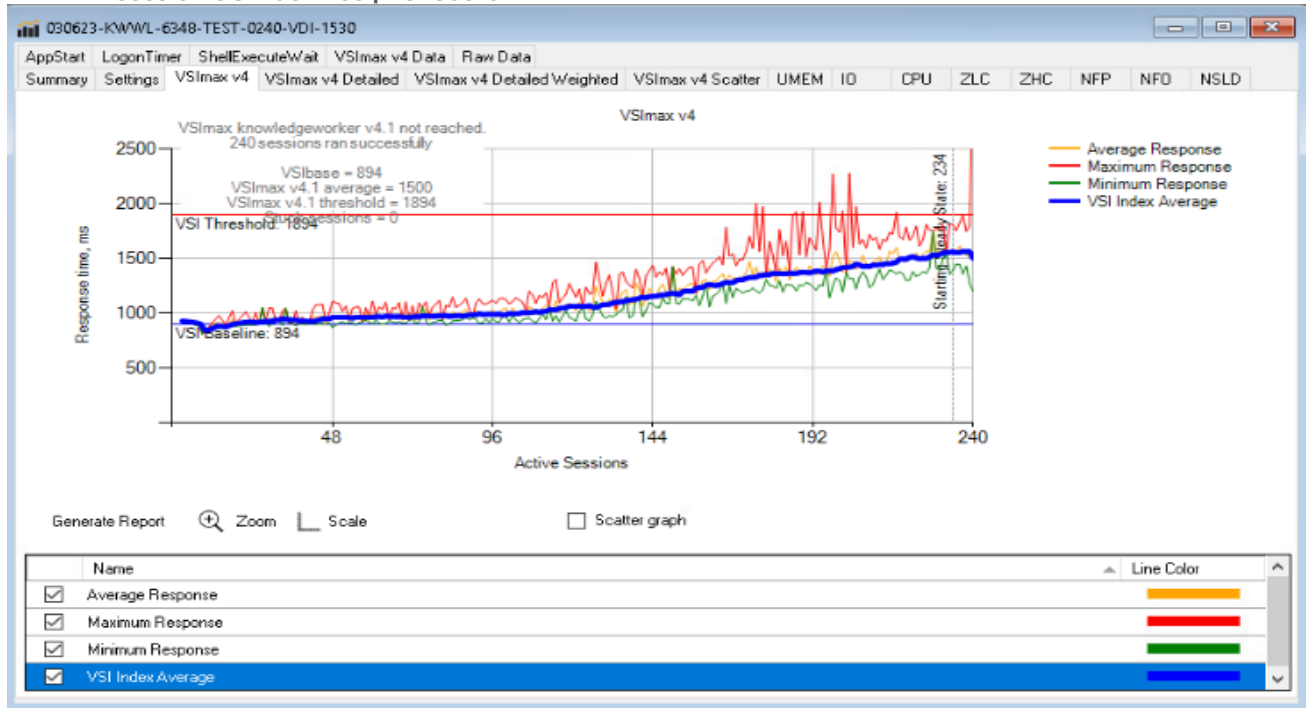


**Single-Server Recommended Maximum Workload for VMware Horizon non-persistent Instant Clone Win10 virtual machines single-session with 240 Users**

The recommended maximum workload for a Cisco UCS B200 M6 blade server with dual Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM is 240 Windows 10 64-bit VDI non-persistent VMware Instant Clone virtual machines with 2 vCPU and 3GB RAM.

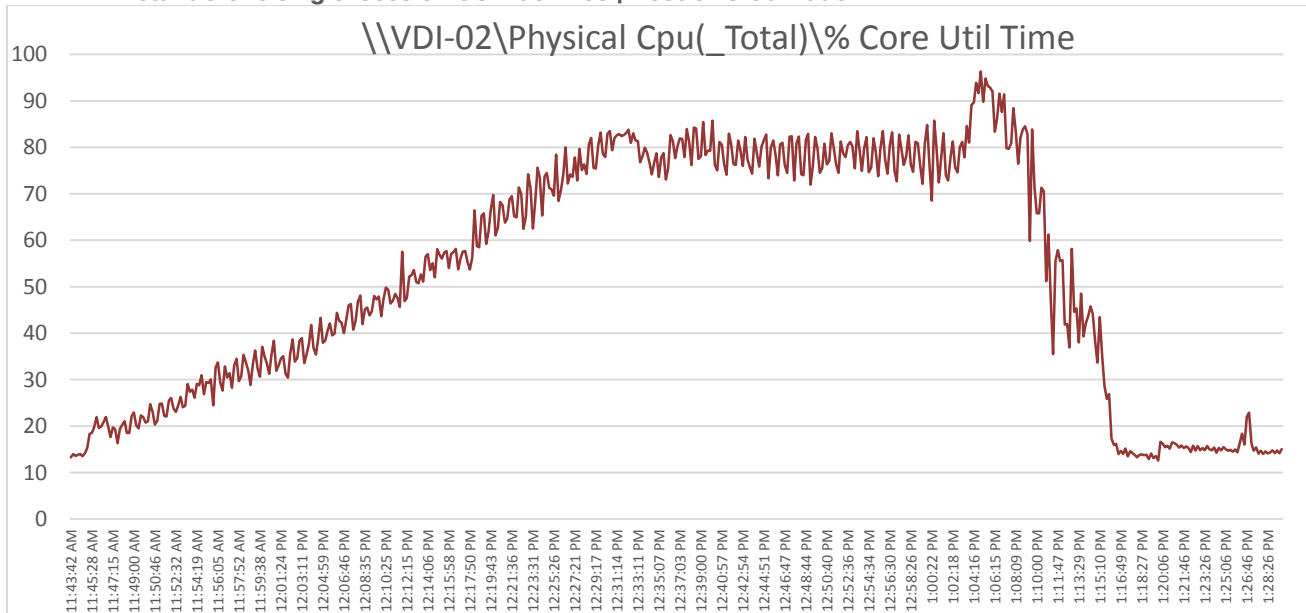
Login VSI performance data is as shown below:

**Figure 39. Single Server | VMware Horizon 8 2212 VMware Horizon Non-Persistent Instant Clone Single-session OS machines | VSI Score**

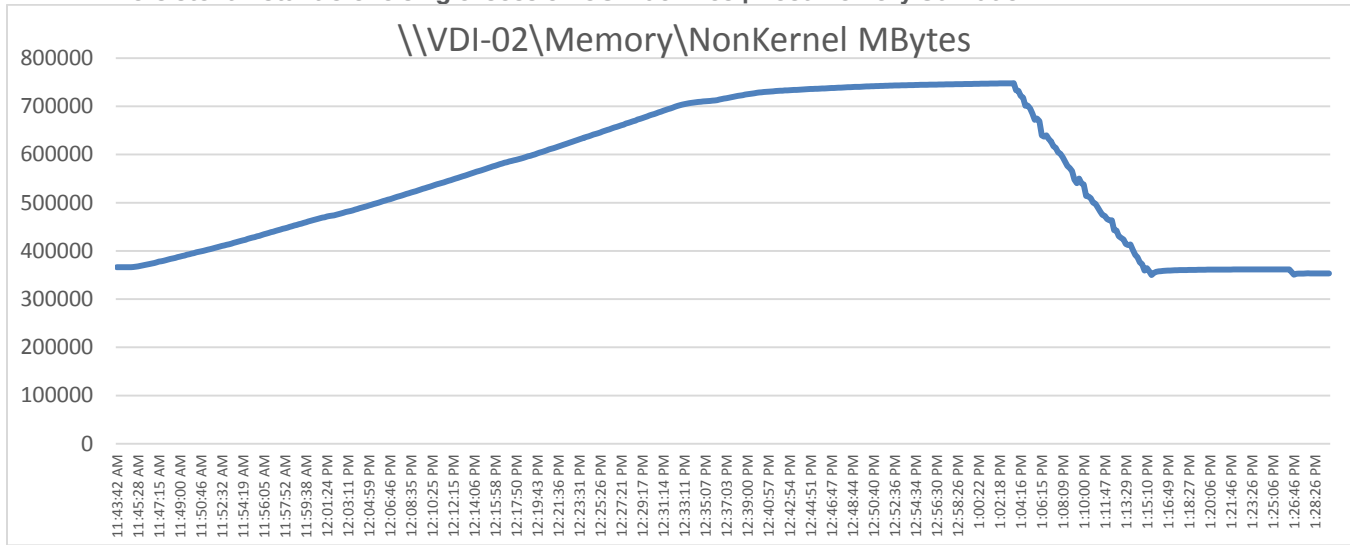


Performance data for the server running the workload is shown below:

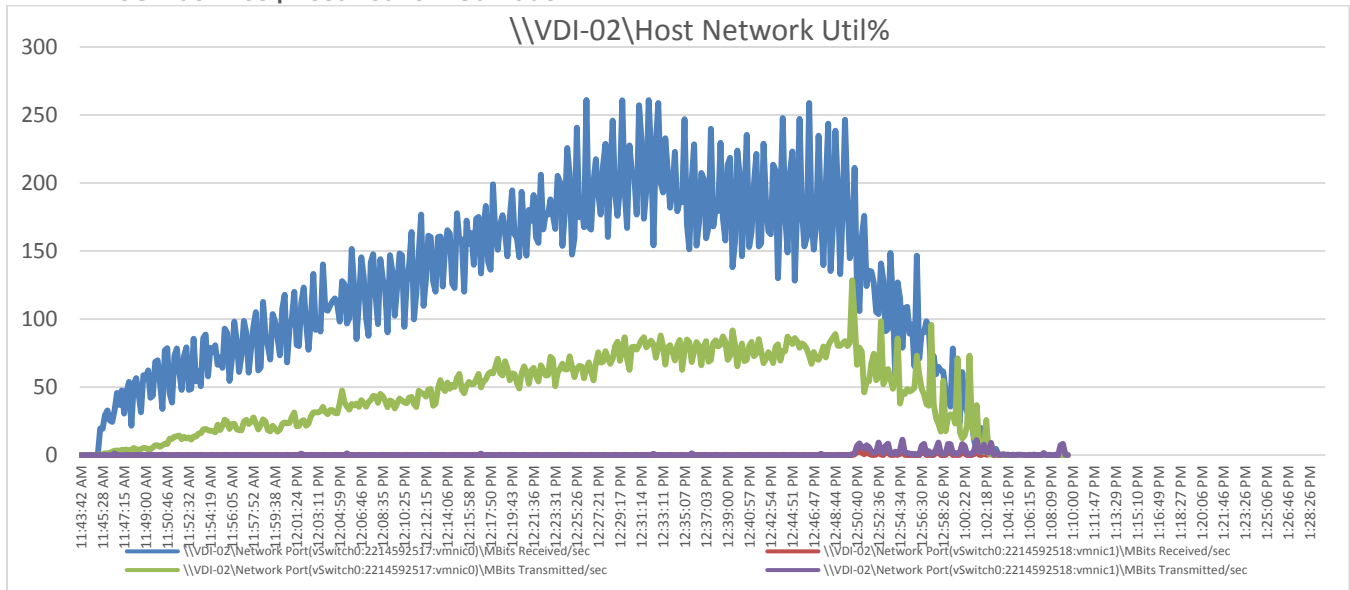
**Figure 40. Single Server Recommended Maximum Workload | VMware Horizon 8 Horizon Non-Persistent Instant Clone single-session OS machines | Host CPU Utilization**



**Figure 41. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 Horizon Non-Persistent Instant Clone single-session OS machines | Host Memory Utilization**



**Figure 42. Single Server | VMware Horizon 8 2212 Horizon Non-Persistent Instant Clone single-session OS machines | Host Network Utilization**

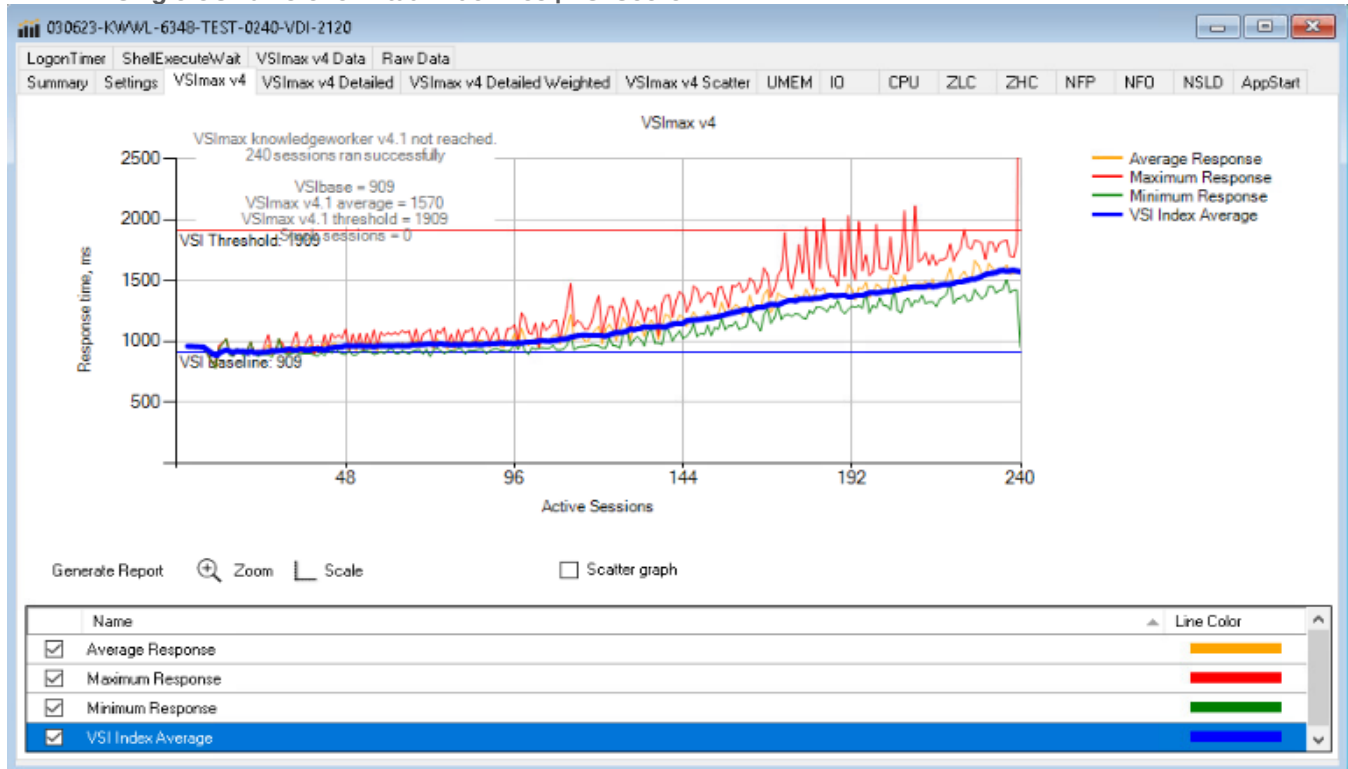


**Single-Server Recommended Maximum Workload for VMware Horizon Full Clone Persistent Win 10 virtual machine single-session OS dedicated with 240 Users.**

The recommended maximum workload for a Cisco UCS B200 M6 blade server with dual Intel(R) Xeon(R) Gold 6338 CPU 2.00GHz 32-core processors, 1TB 3200MHz RAM is 240 Windows 10 64-bit VDI persistent VMware Horizon Full Clone virtual machines with 2 vCPU and 3GB RAM.

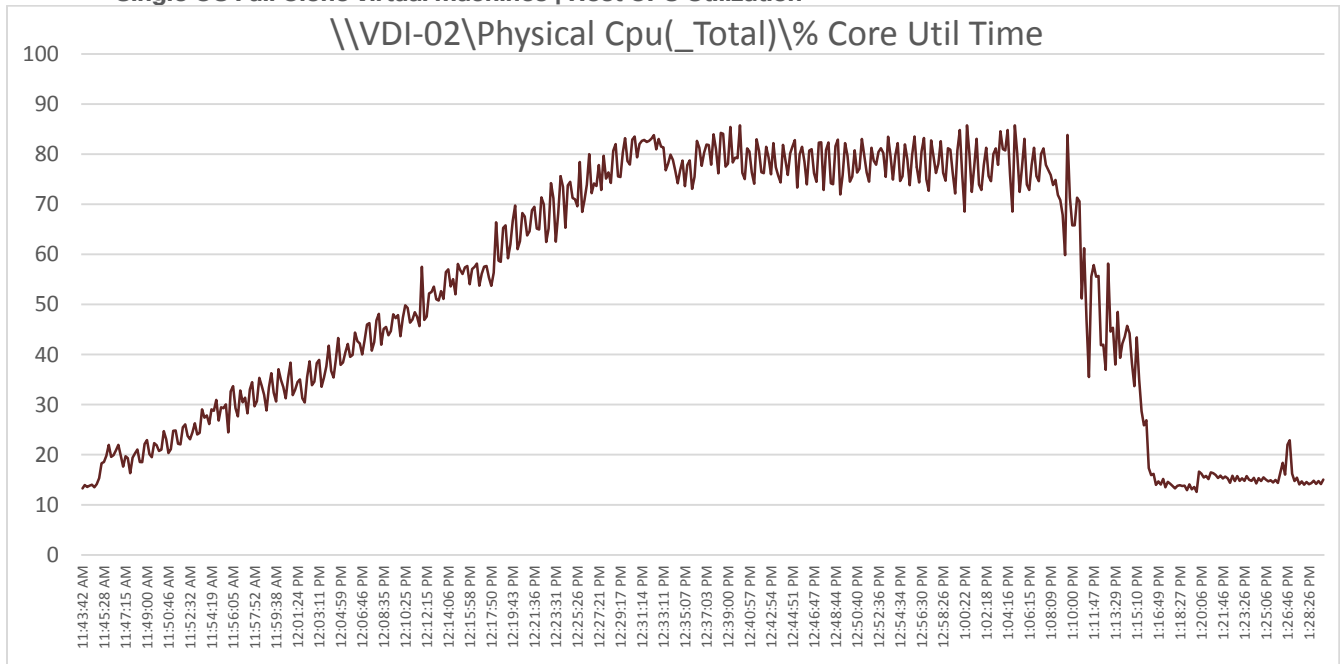
LoginVSI data is shown below:

**Figure 43. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 Persistent Win 10 Single OS Full Clone virtual machines | VSI Score**

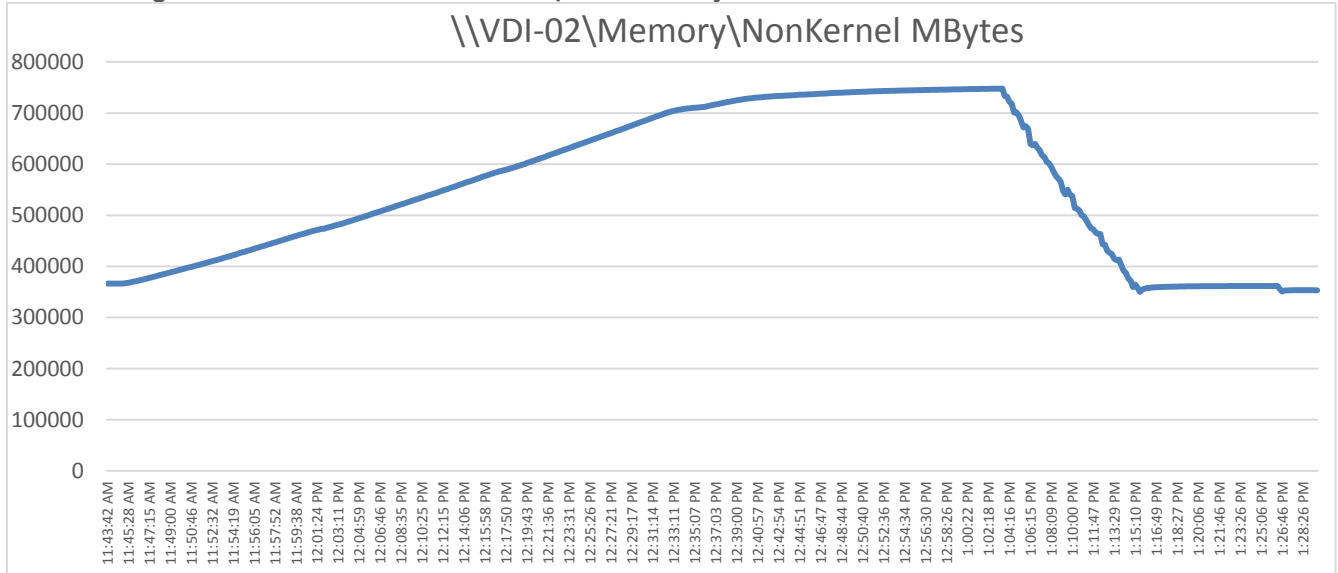


Performance data for the server running the workload is shown below:

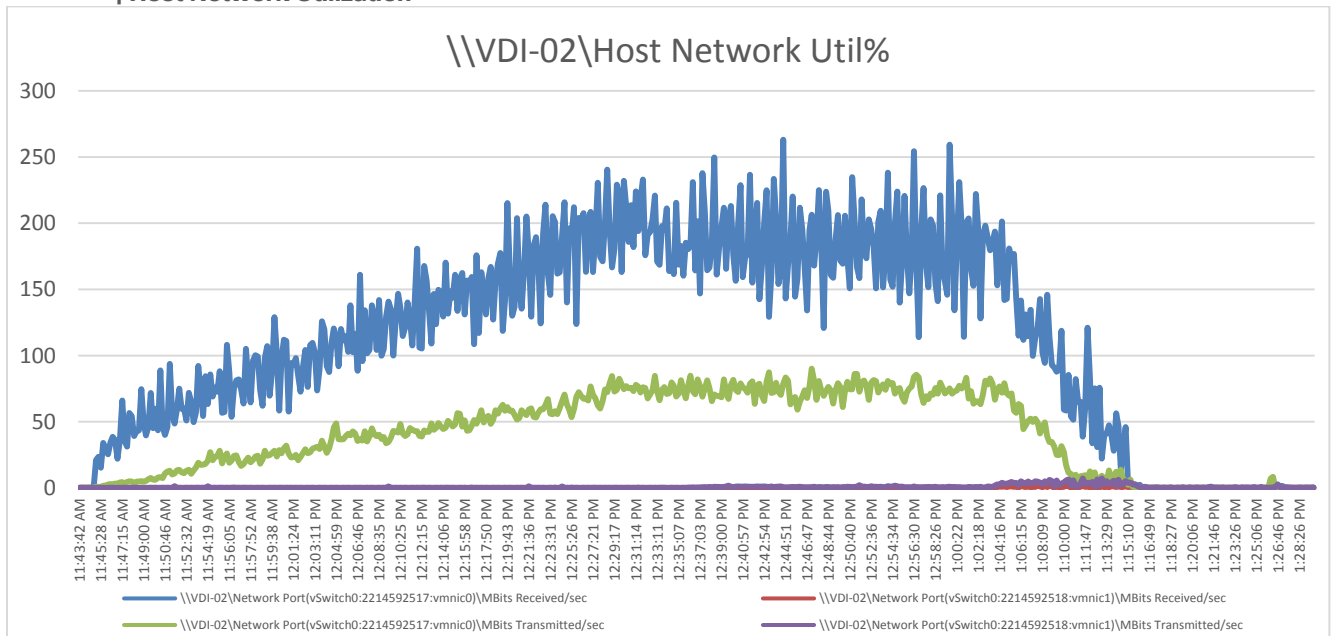
**Figure 44. Single Server Recommended Maximum Workload VMware Horizon 8 2212 Persistent Win 10 Single OS Full Clone virtual machines | Host CPU Utilization**



**Figure 45. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 Persistent Win 10 Single OS Full Clone virtual machines | Host Memory Utilization**



**Figure 46. Single Server | VMware Horizon 8 2212 Persistent Win 10 Single OS Full Clone virtual machines | Host Network Utilization**



## Full Scale Workload Testing

This section describes the key performance metrics that were captured on the Cisco UCS, during the full-scale testing. Full Scale testing was done with following Workloads using eight Cisco UCS B200 M6 Compute Node Servers, configured in a single ESXi Host Pool, and designed to support single Host failure (N+1 Fault tolerance):

- 2300 VMware Remote Desktop Server Hosted (RDSH) Multi OS Server sessions
- 1700 VMware Horizon Instant Clone (Non-persistent) Single-session OS Win 10 sessions
- 1700 VMware Horizon Full Clone (Persistent) Single-session OS Win 10 sessions



To achieve the target, sessions were launched against each workload set at a time. 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.

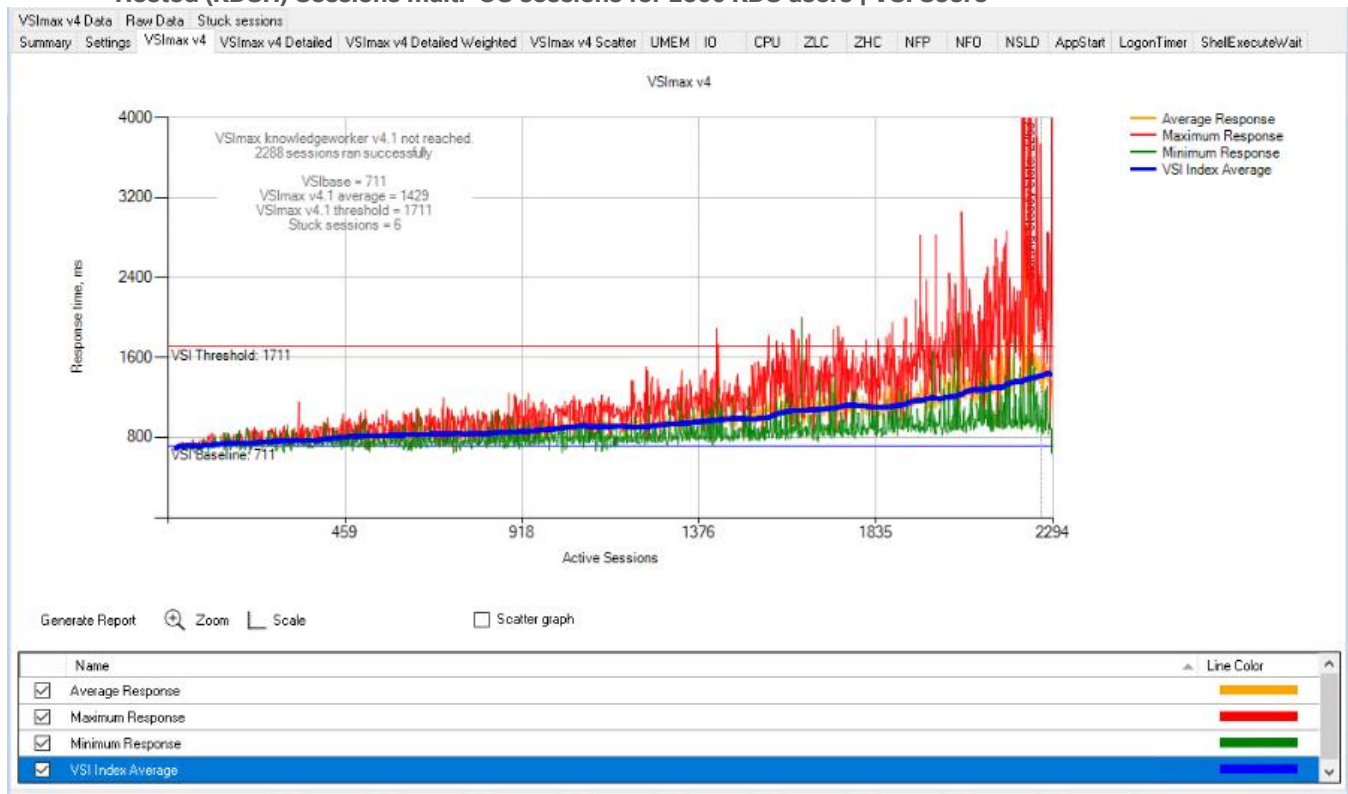
### Full Scale Recommended Maximum Workload Testing for VMware Horizon Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users.

This section describes the key performance metrics that were captured on the Cisco UCS and Pure Storage FlashArray//X70 R3 array during the full-scale testing with 2300 VMware Horizon Remote Desktop Server Hosted (RDSH) multi-OS sessions using 8 blades in a single pool.

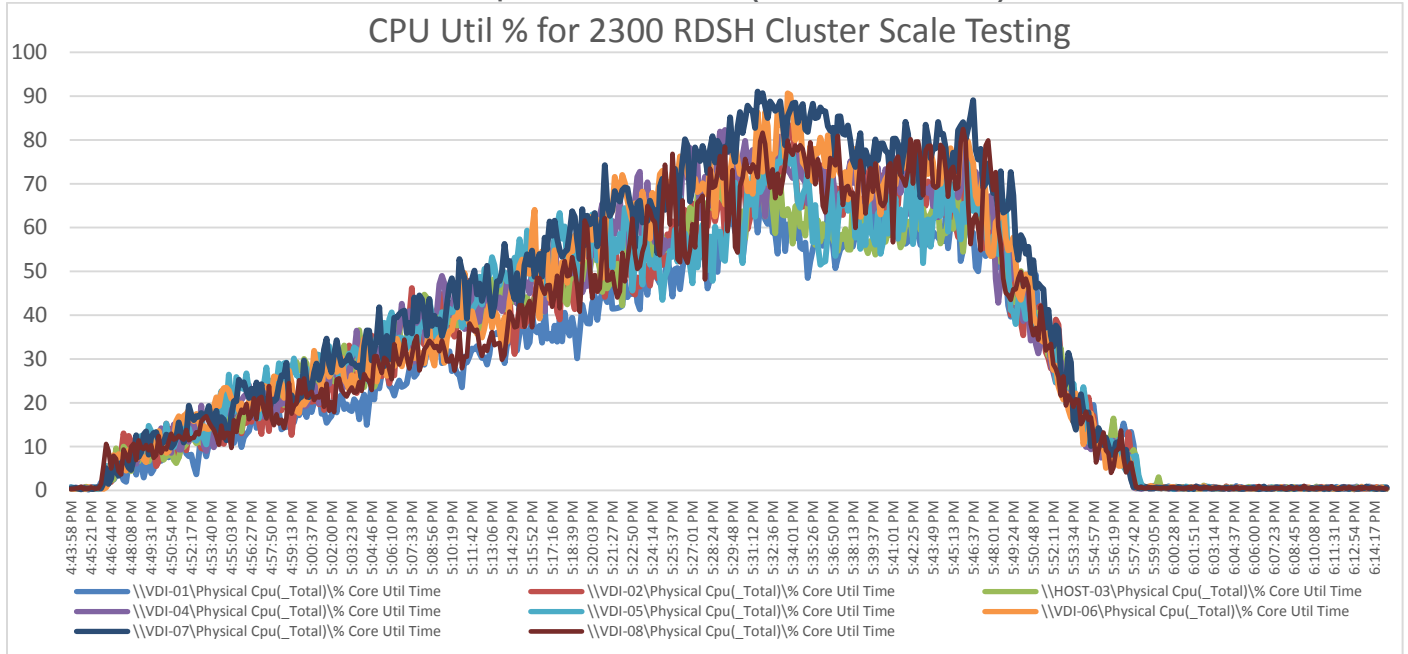
The workload for the test is 2300 RDSH Multi OS Server Session users. To achieve the target, sessions were launched against all workload hosts concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.

The configured system efficiently and effectively delivered the following results:

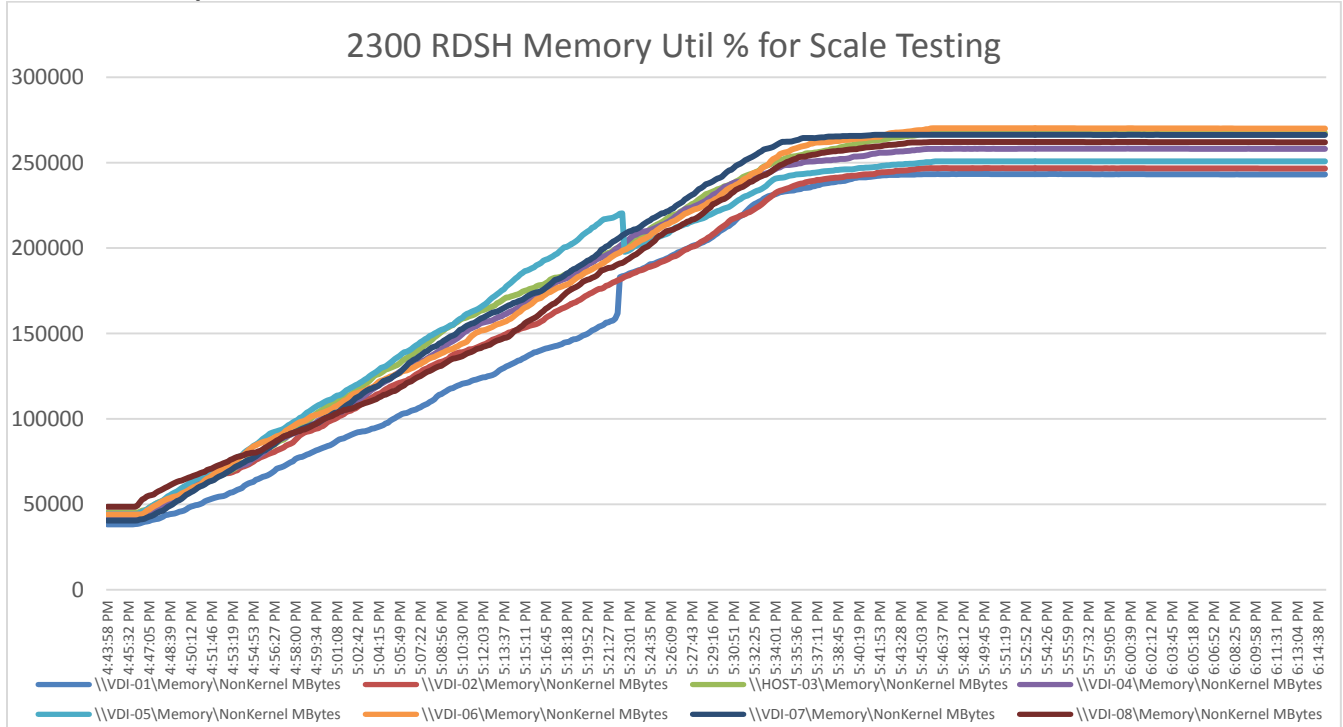
**Figure 47. Full Scale | 2300 Users | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions multi-OS sessions for 2300 RDS users | VSI Score**



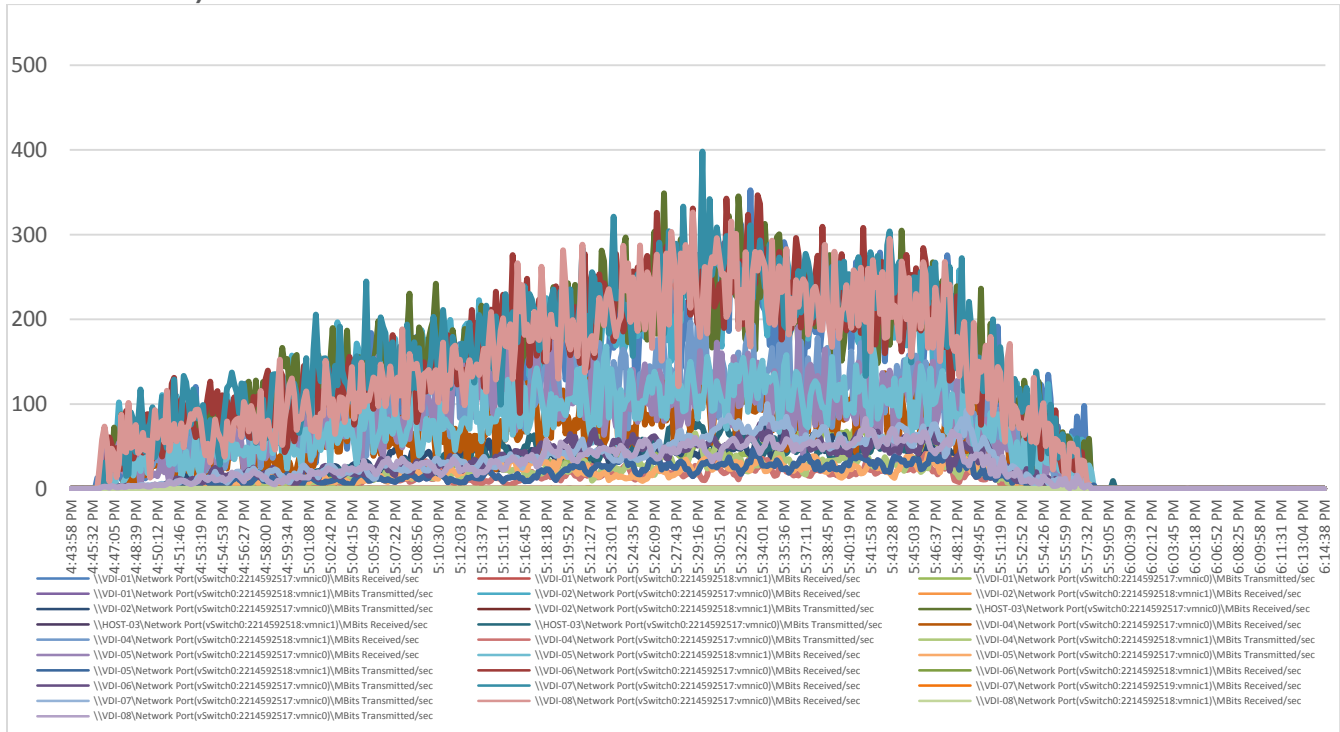
**Figure 48. Full Scale | 2300 Users | VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users | Host CPU Utilization (for 8 hosts in cluster)**



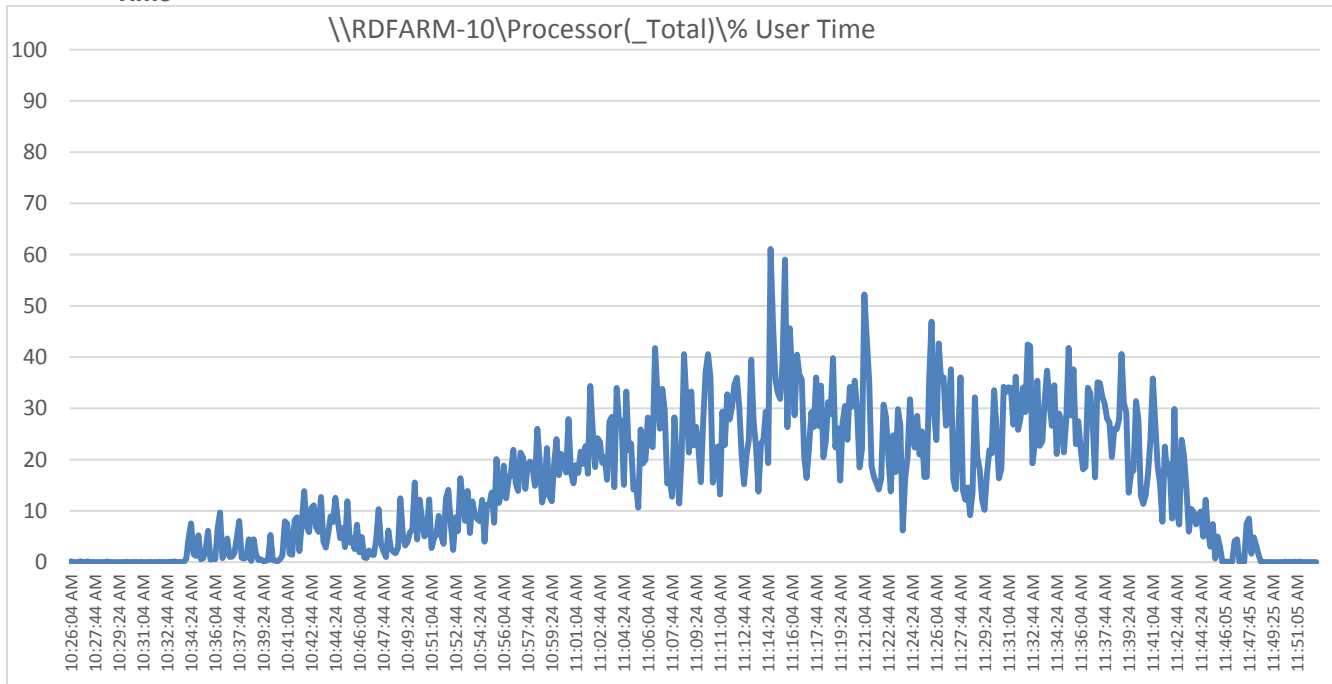
**Figure 49. Full Scale | 2300 Users | VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users multi-session OS machine | Host Memory Utilization (for 8 hosts in cluster)**



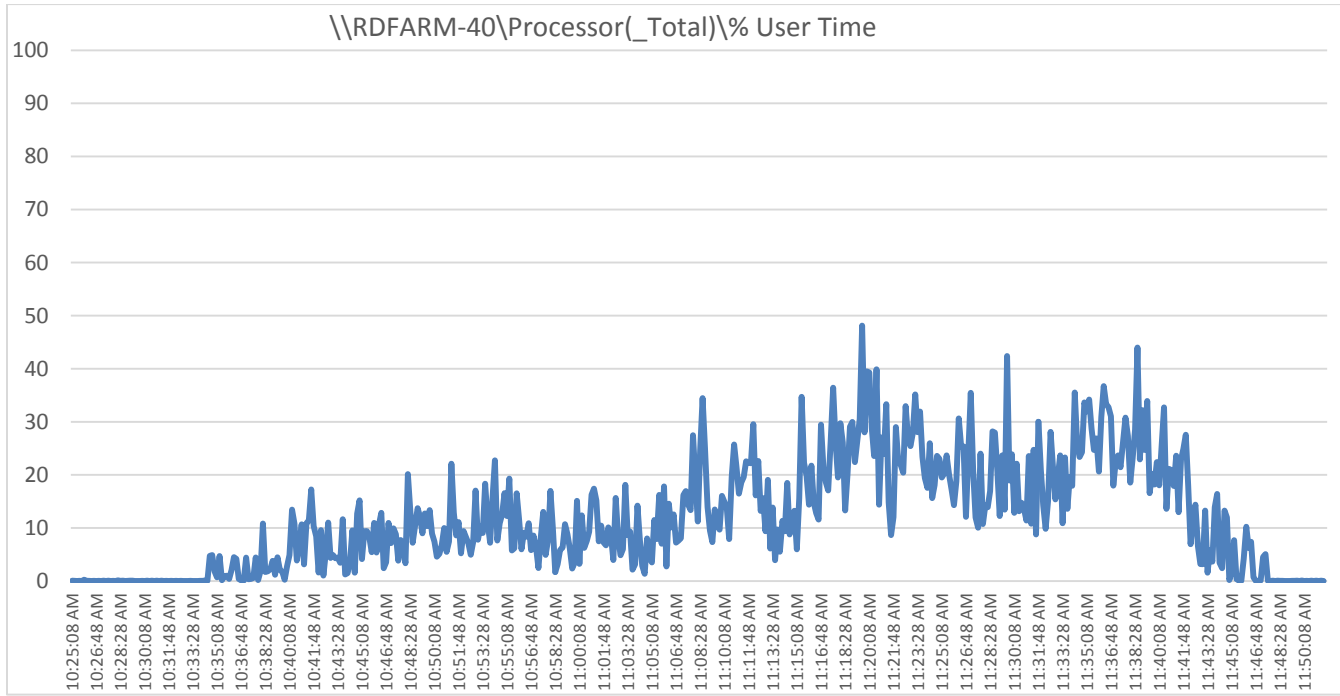
**Figure 50. Full Scale | 2300 Users | VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users multi-session OS sessions | Host Network Utilization (for 8 hosts in cluster)**



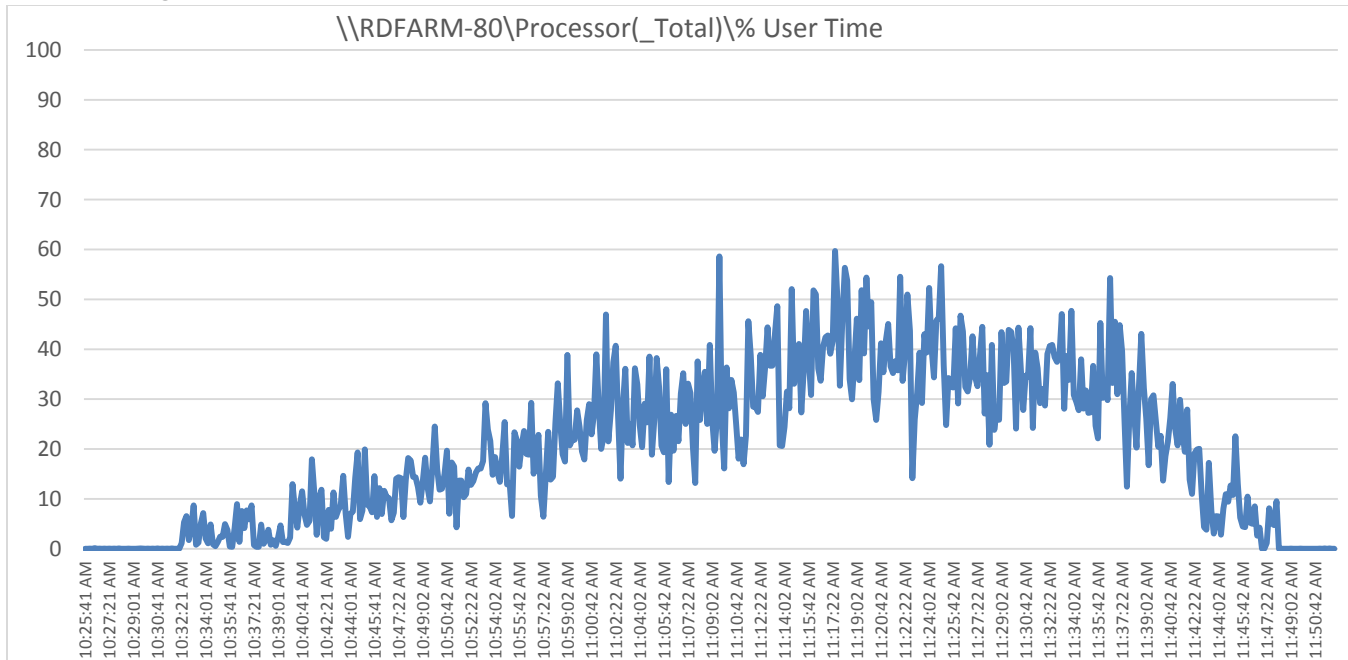
**Figure 51. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) sessions multi-session OS machines | RDS Server Total % User Time**



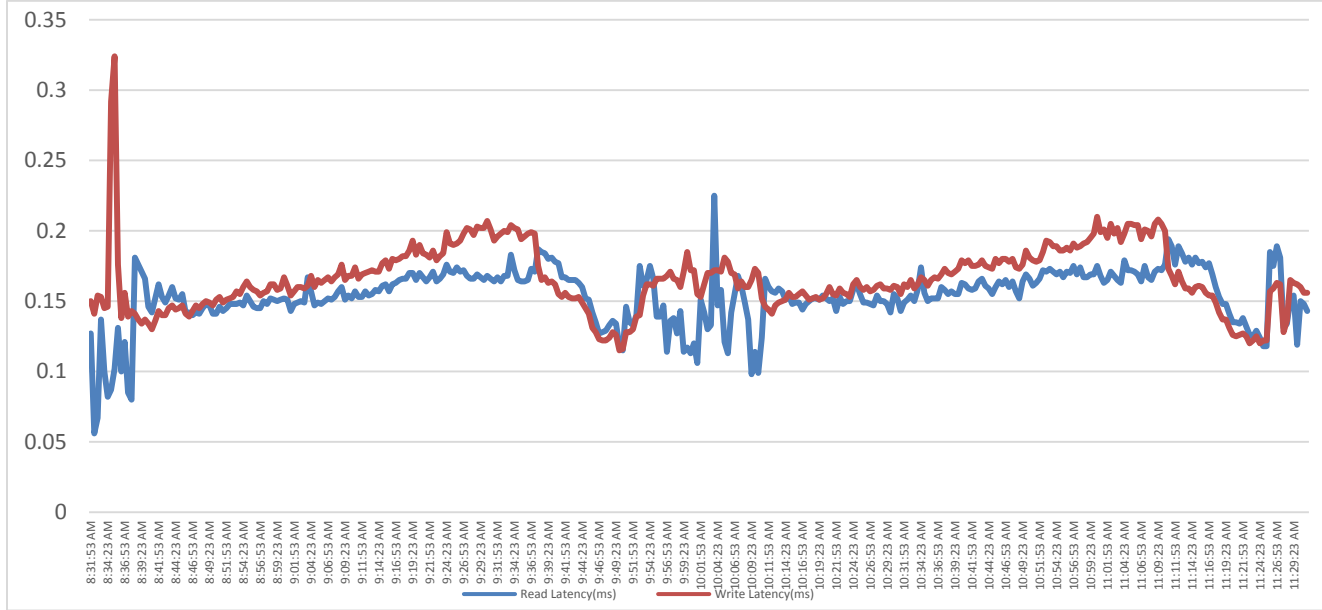
**Figure 52. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions Multi-session OS machines | RDS Server Total % User Time**



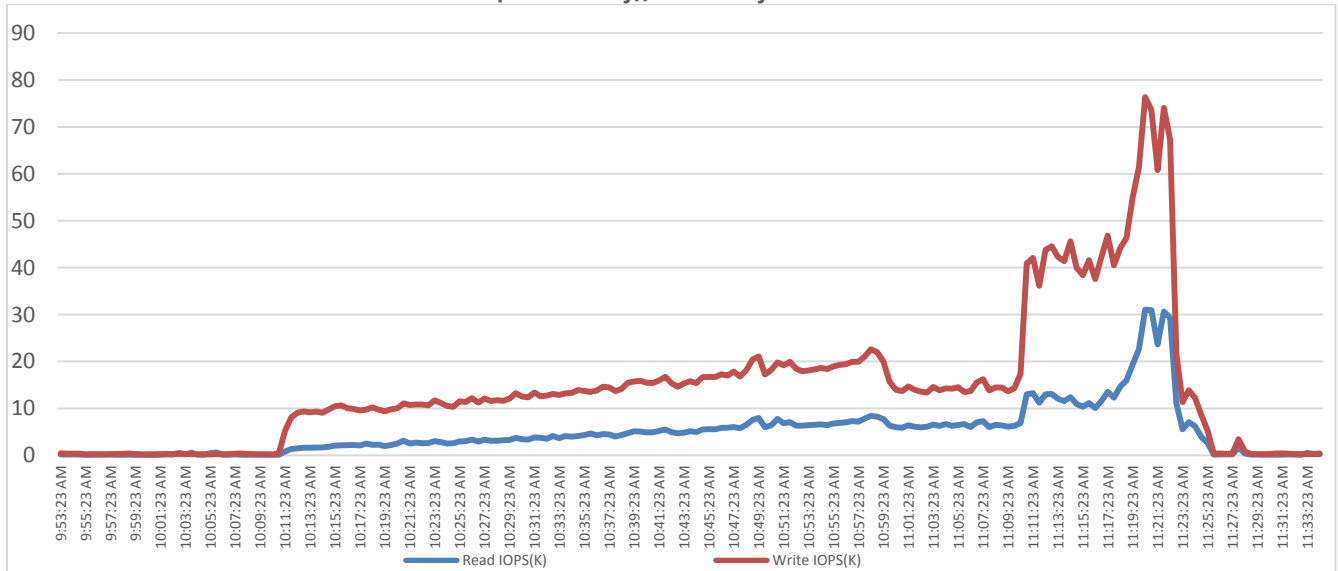
**Figure 53. Single Server Recommended Maximum Workload | VMware Horizon 8 2212 VMware Horizon Remote Desktop Server Hosted (RDSH) Sessions Multi-session OS machines | RDS Server Total % User Time**



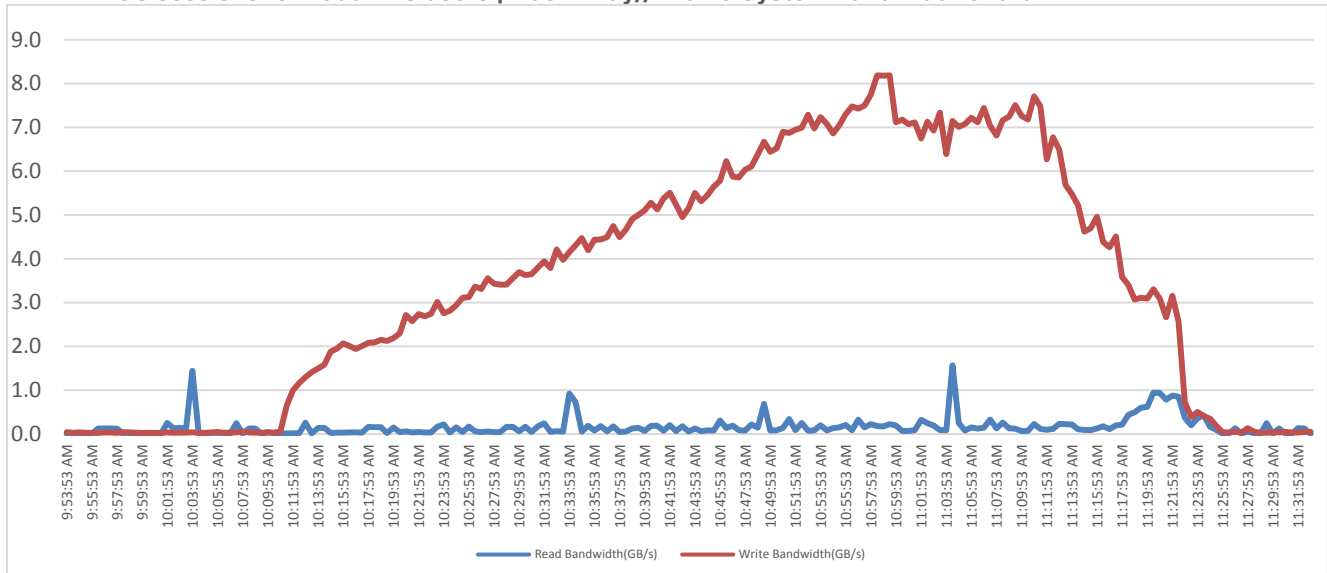
**Figure 54. Full Scale | 2300 Users | VMware Horizon 8 2212 Horizon Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users | Pure Storage FlashArray//X70 R3 System Latency Chart**



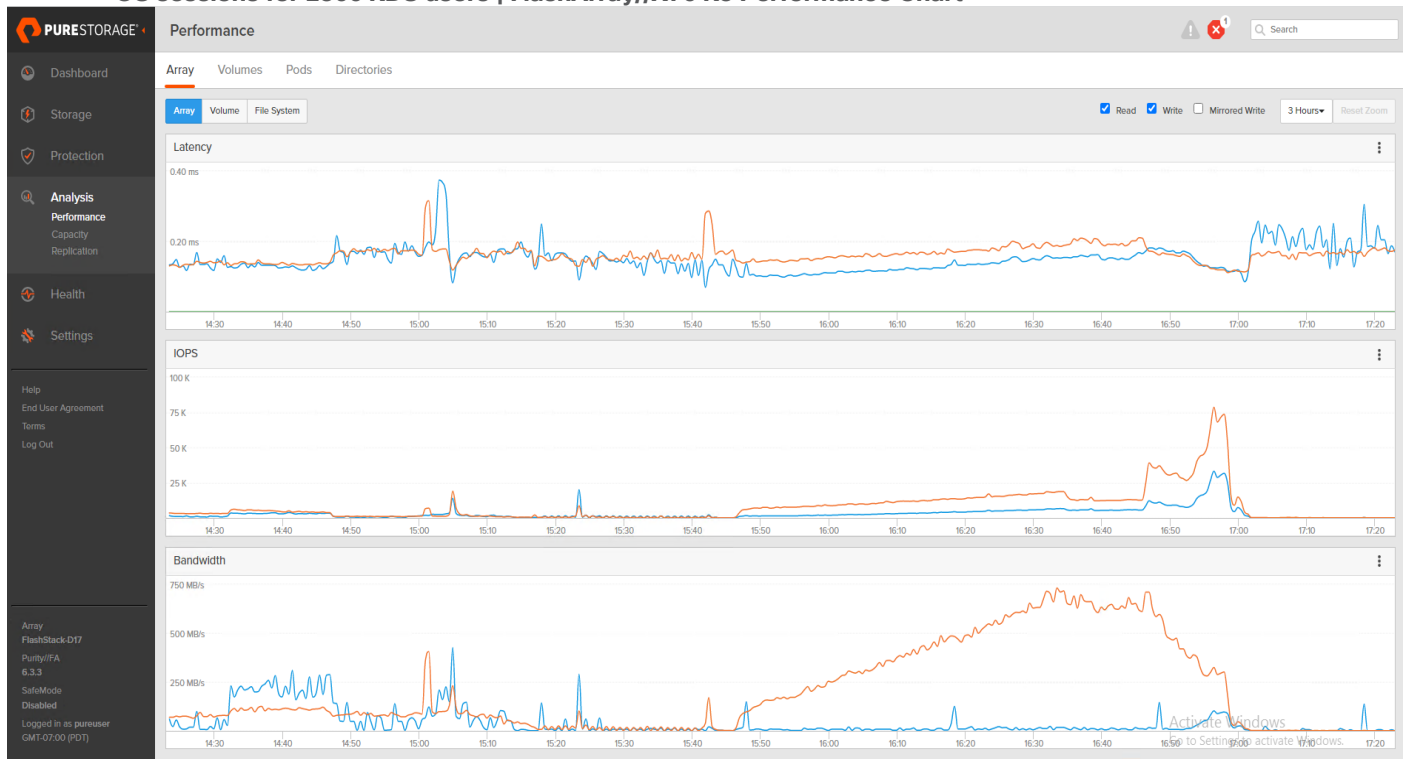
**Figure 55. Full Scale | 2300 Users | VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users | FlashArray//X70 R3 System IOPS Chart**



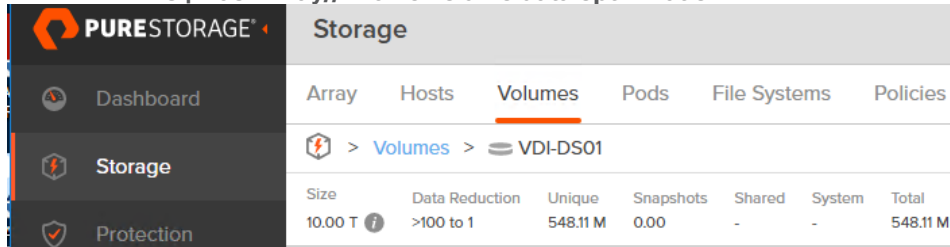
**Figure 56. Full Scale | 2300 Users | VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users | FlashArray//X70 R3 System Bandwidth Chart**



**Figure 57. Full Scale | 2300 Users | VMware Horizon 8 2212 Remote Desktop Server Hosted (RDSH) multi-OS sessions for 2300 RDS users | FlashArray//X70 R3 Performance Chart**



**Figure 58. Full Scale | 2300 Users | VMware Horizon 8 2212 Non-persistent Single-session OS machine VDAs | FlashArray//X70 R3 volume data optimization**



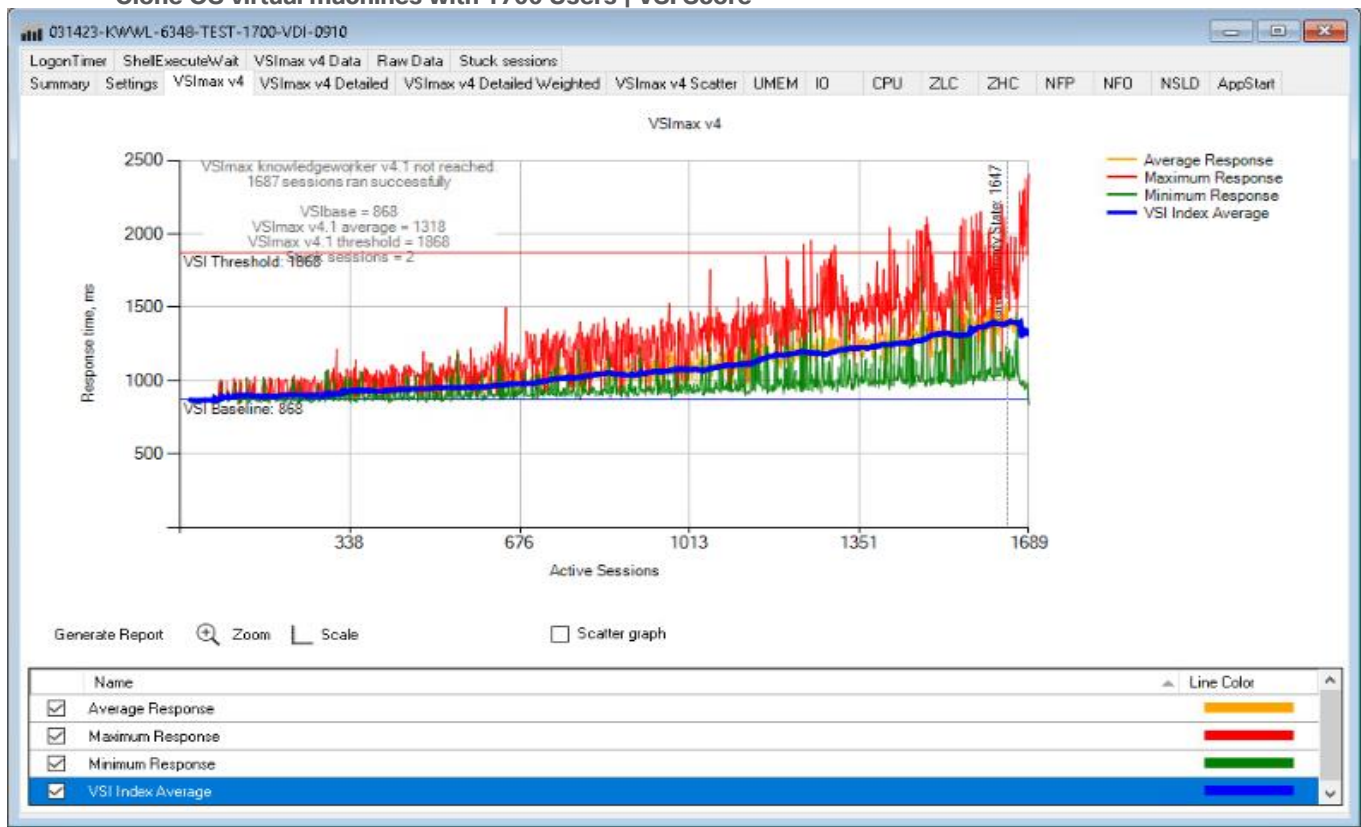
**Full Scale Recommended Maximum Workload Testing for non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users.**

This section describes the key performance metrics that were captured on the Cisco UCS and Pure Storage FlashArray during the persistent desktop full-scale testing with 1700 non-persistent, single-session Win 10 OS machines using 8 blades in a single pool.

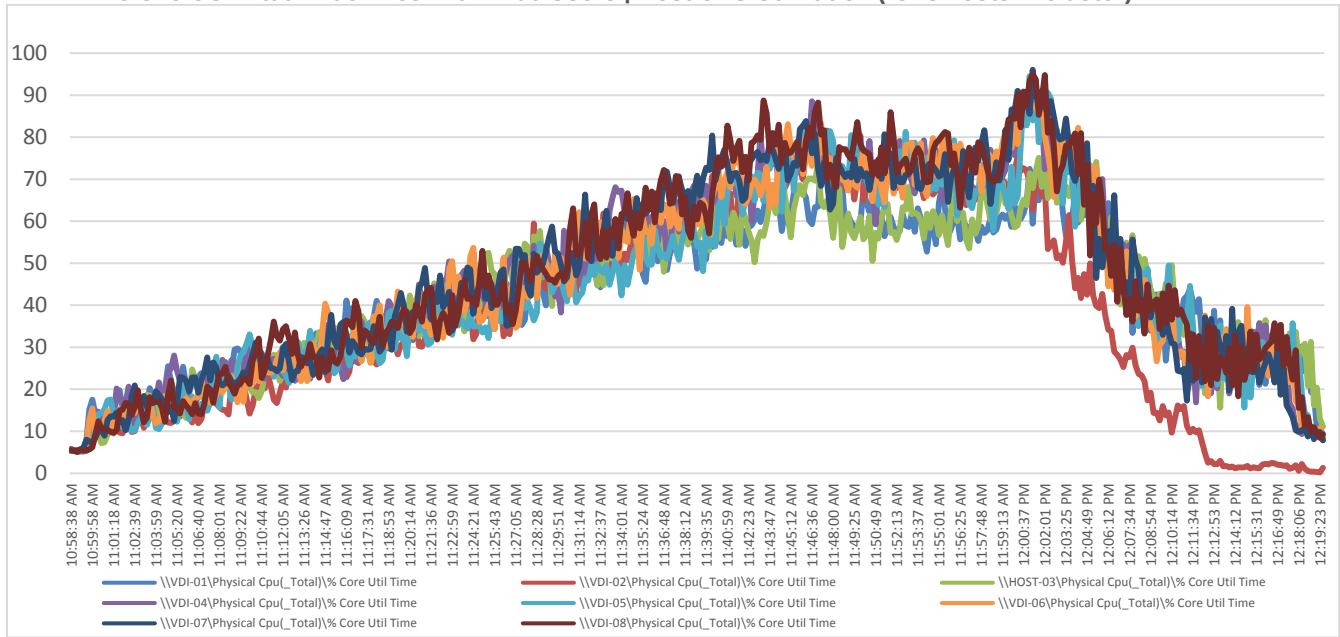
The workload for the test is 1700 Non-Persistent VDI users. To achieve the target, sessions were launched against all workload clusters concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.

The configured system efficiently and effectively delivered the following results:

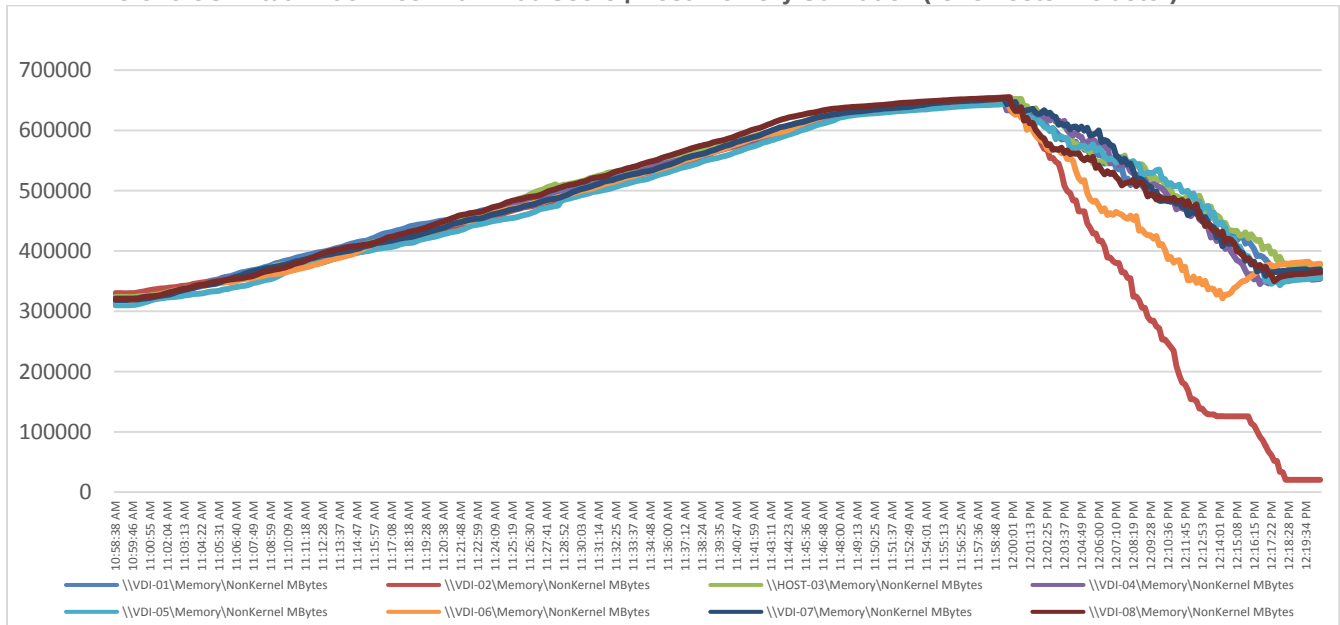
**Figure 59. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | VSI Score**



**Figure 60. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | Host CPU Utilization (for 8 hosts in cluster)**

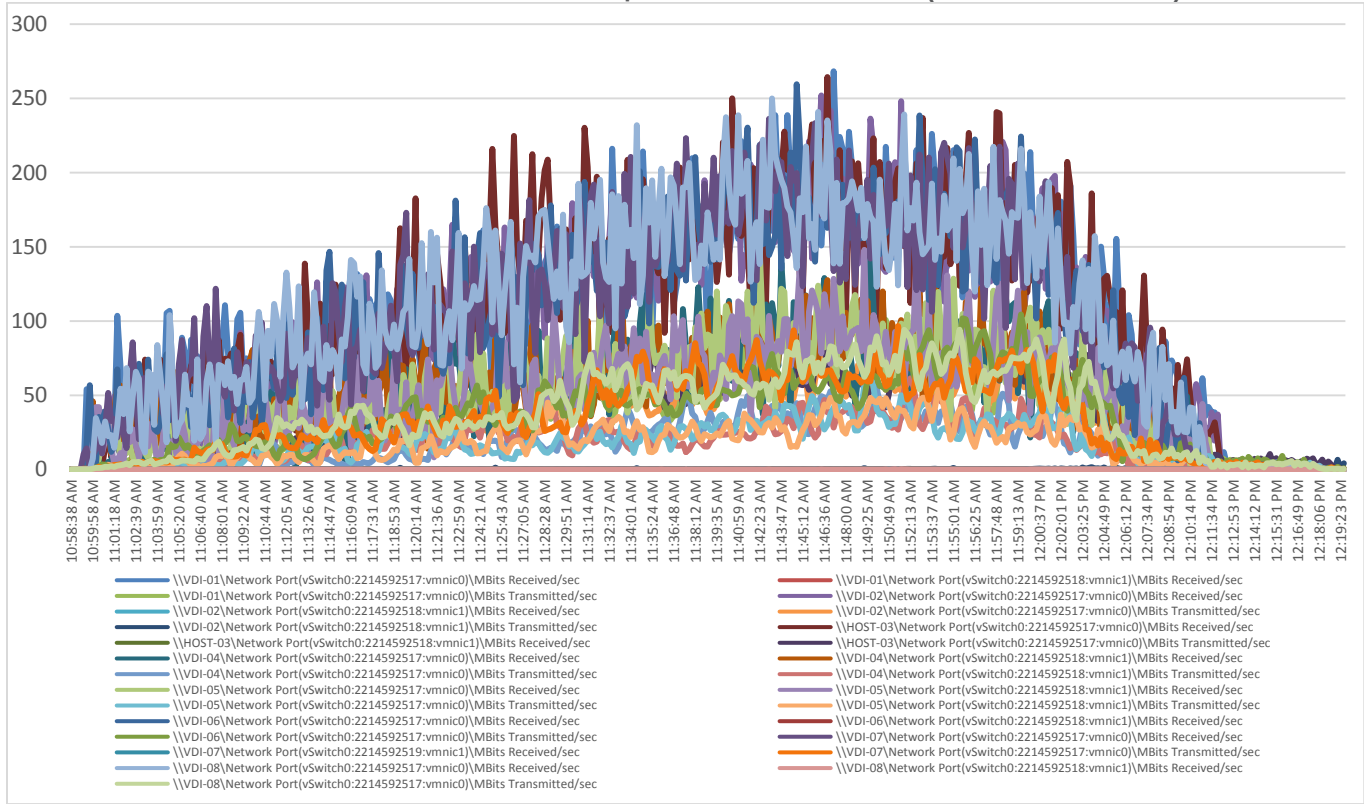


**Figure 61. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | Host Memory Utilization (for 8 hosts in cluster)**

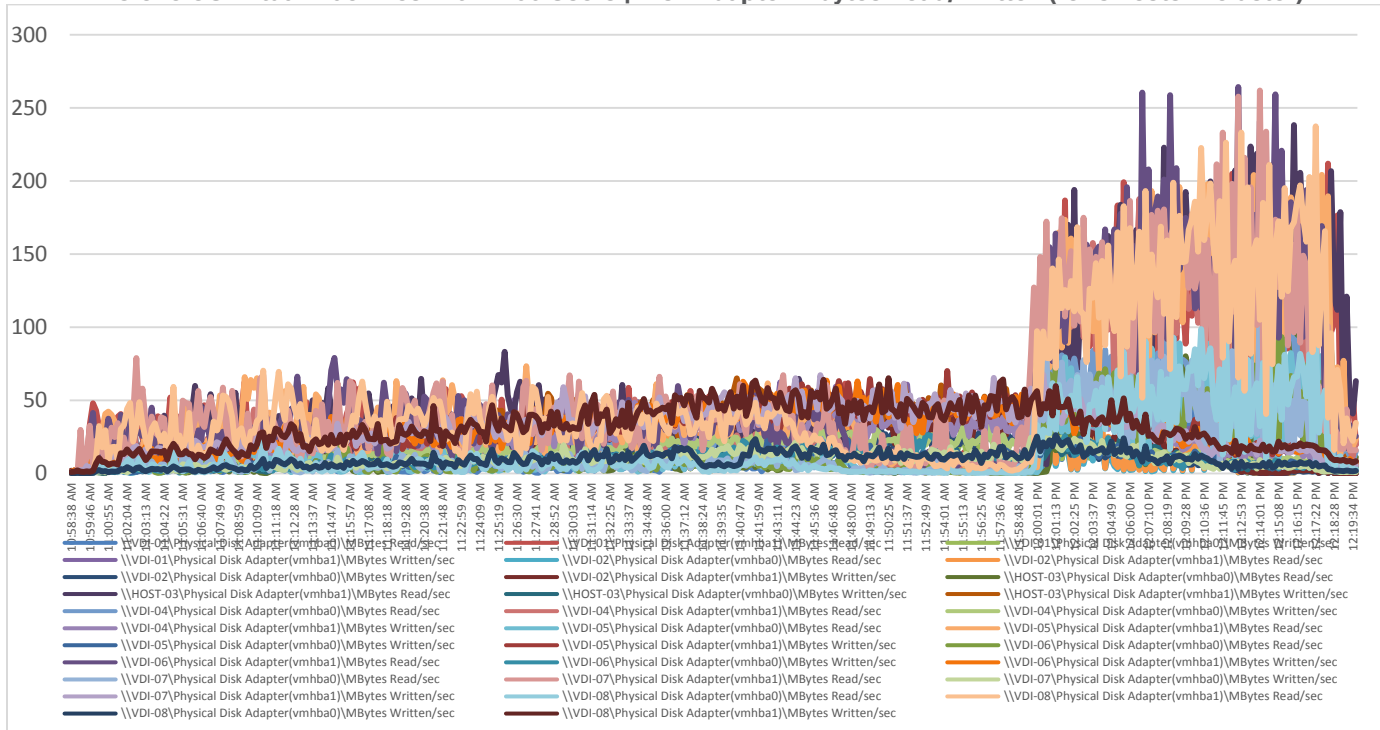




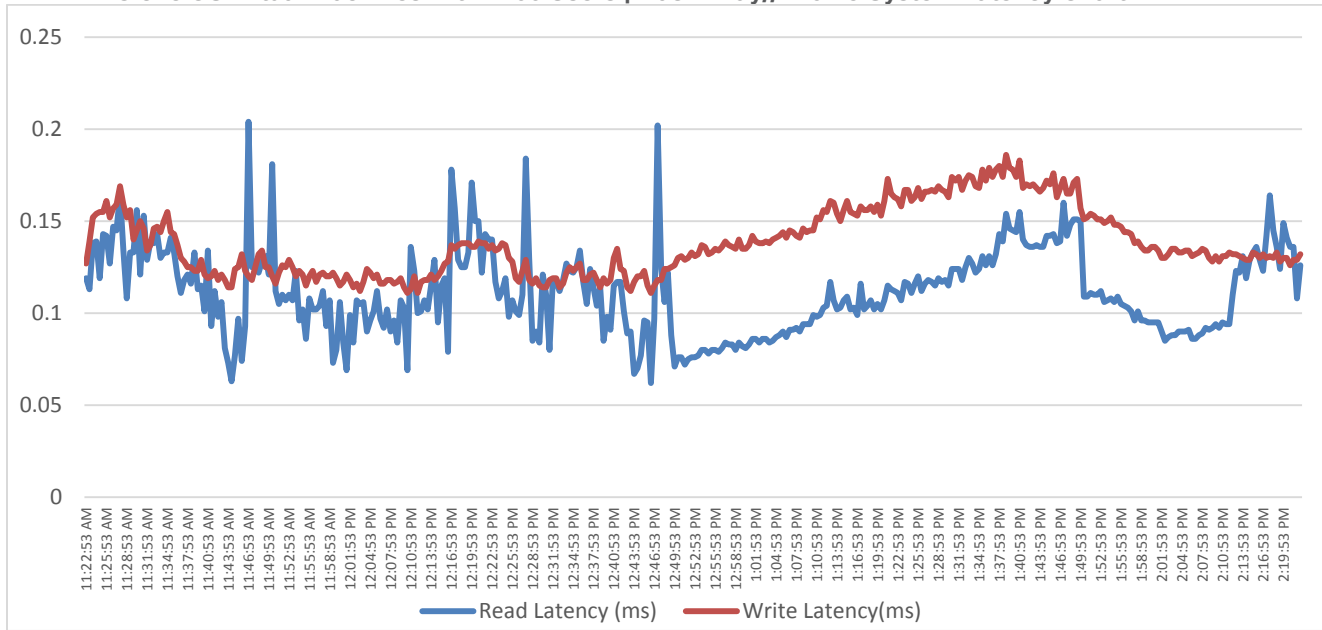
**Figure 62. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | Host Network Utilization (for 8 hosts in cluster)**



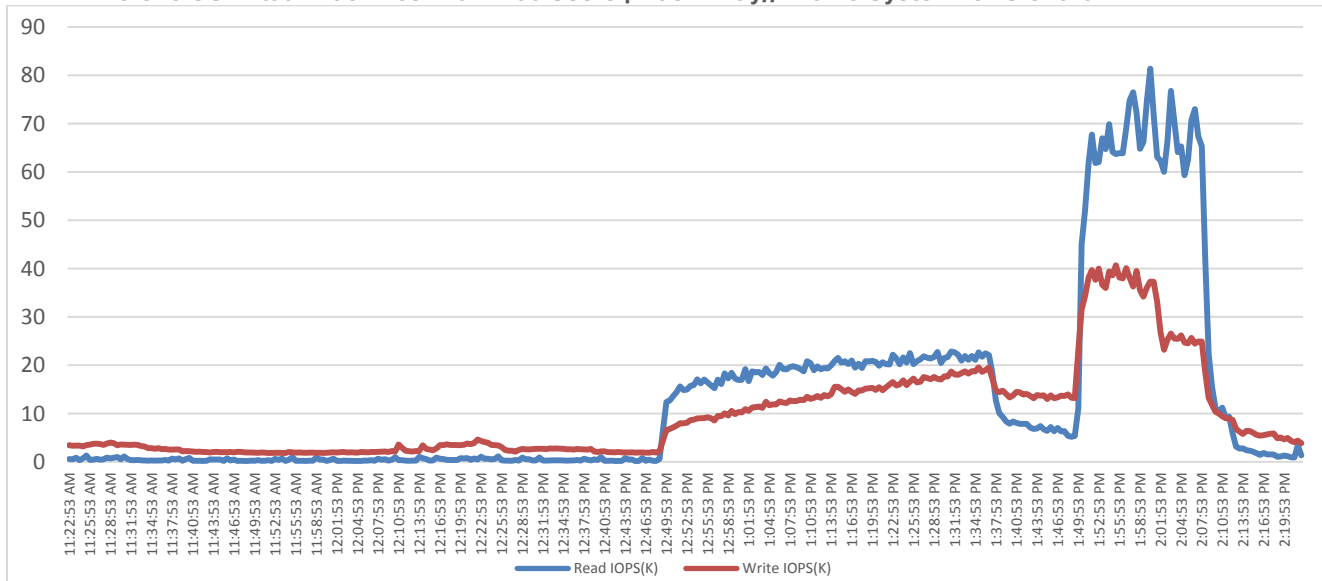
**Figure 63. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | Disk Adapter Mbytes Read/Written (for 8 hosts in cluster)**



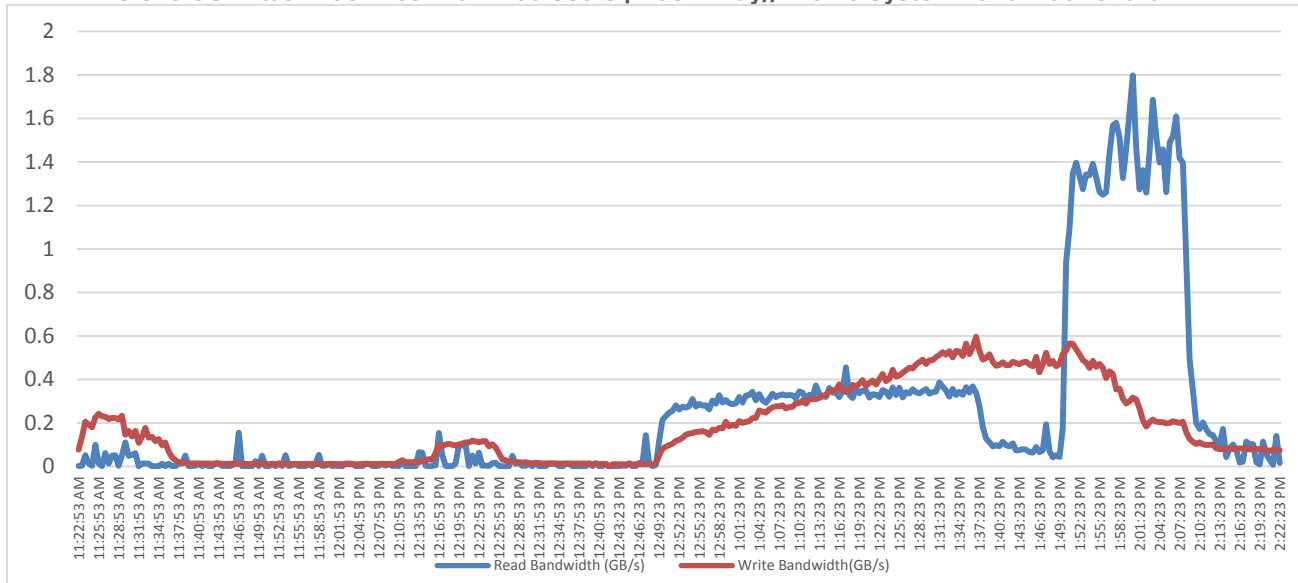
**Figure 64. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | FlashArray//X70 R3 System Latency Chart**



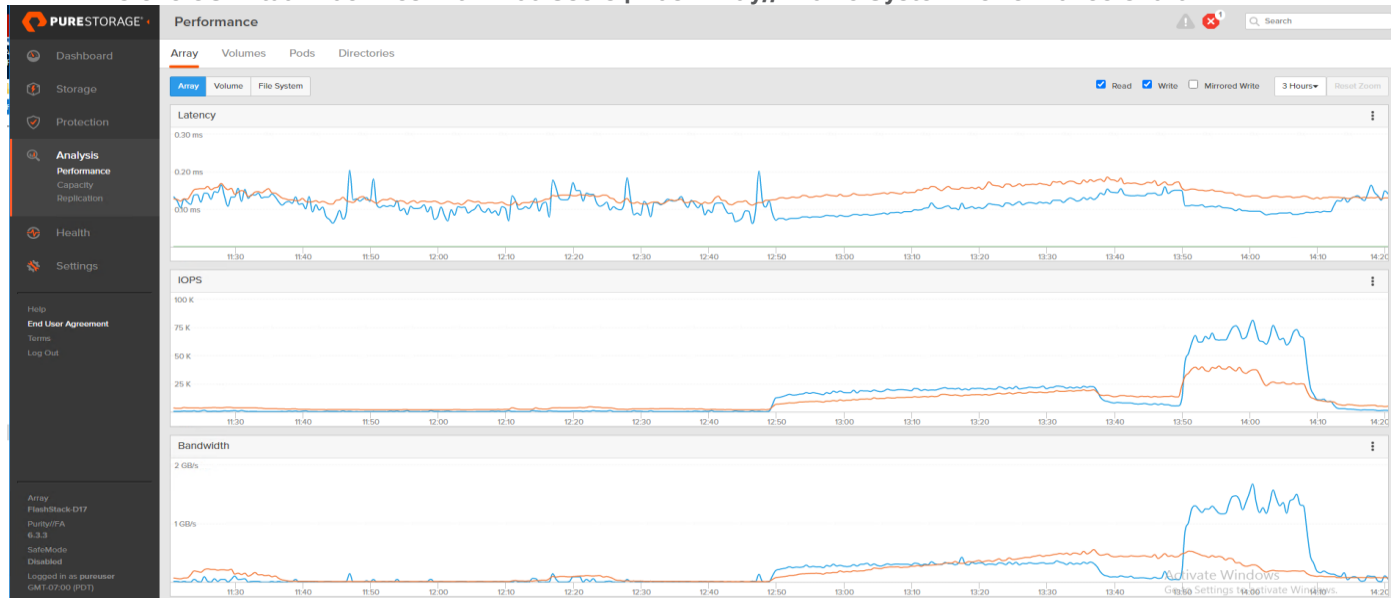
**Figure 65. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | FlashArray//X70 R3 System IOPS Chart**



**Figure 66. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | FlashArray//X70 R3 System Bandwidth Chart**



**Figure 67. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | FlashArray//X70 R3 System Performance Chart**



**Figure 68. Full Scale | 1700 Users | VMware Horizon 8 2212 non-persistent Win 10 single-session Instant Clone OS virtual machines with 1700 Users | FlashArray//X70 R3 volume data optimization**

⚡ > Volumes > X70VDI-2

Size	Data Reduction	Unique	Snapshots	Shared	System	Total
180.00 T <i>i</i>	>100 to 1	388.65 G	0.00	-	-	388.65 G

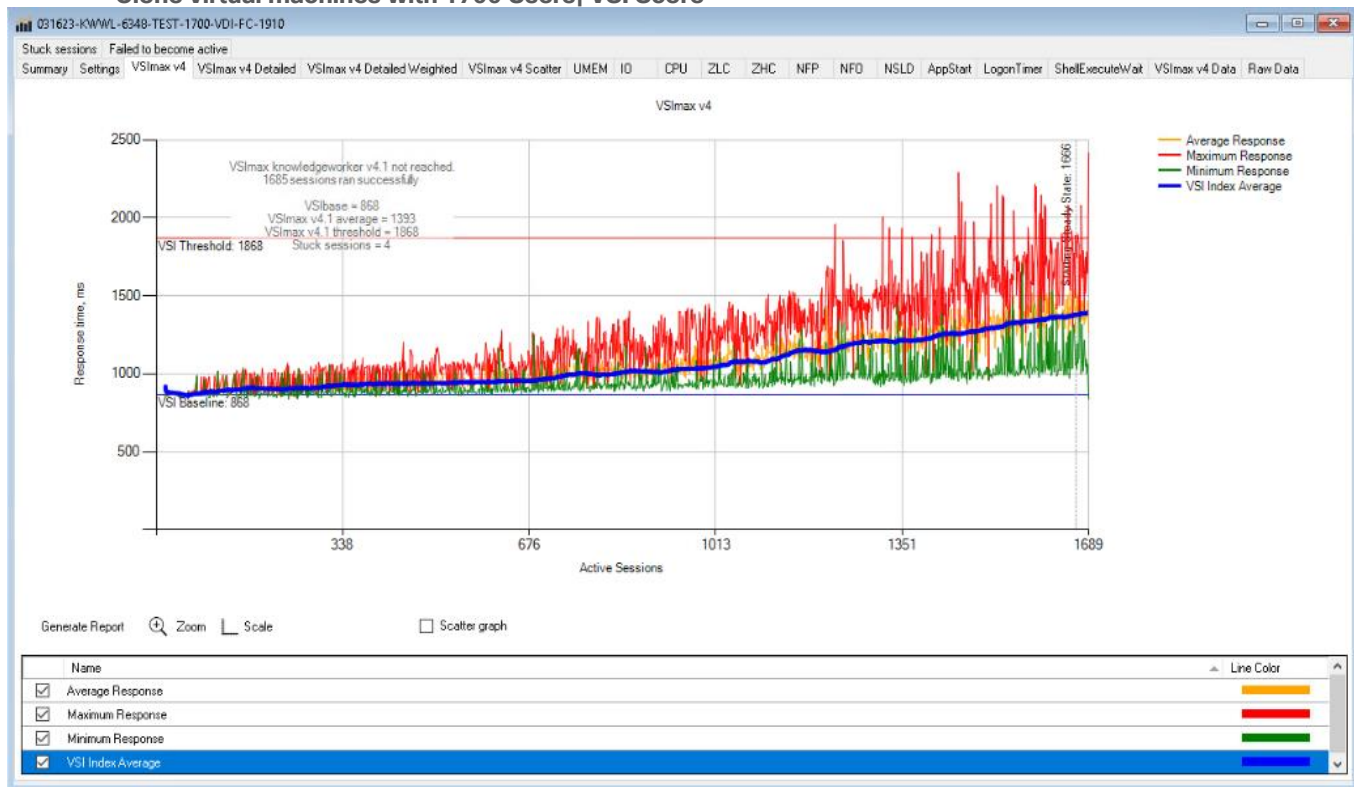
## Full Scale Recommended Maximum Workload for VMware Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users.

This section describes the key performance metrics that were captured on the Cisco UCS and Pure Storage FlashArray//X70 R3 array, during the persistent single-session Win 10 OS full-scale testing with 1700 Desktop Sessions using 8 blades configured in single Host Pool.

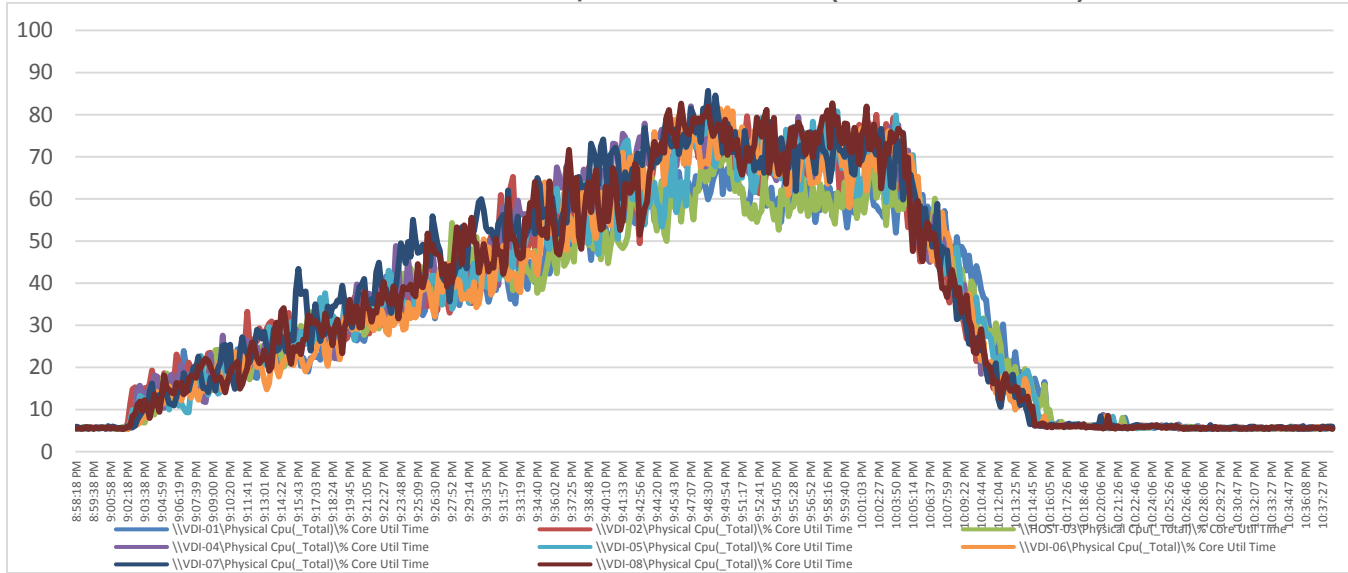
The single-session OS workload for the solution is 1700 users. To achieve the target, sessions were launched against all workload clusters concurrently. As per the Cisco Test Protocol for VDI solutions, all sessions were launched within 48 minutes (using the official Knowledge Worker Workload in VSI Benchmark Mode) and all launched sessions became active within two minutes subsequent to the last logged in session.

The configured system efficiently and effectively delivered the following results:

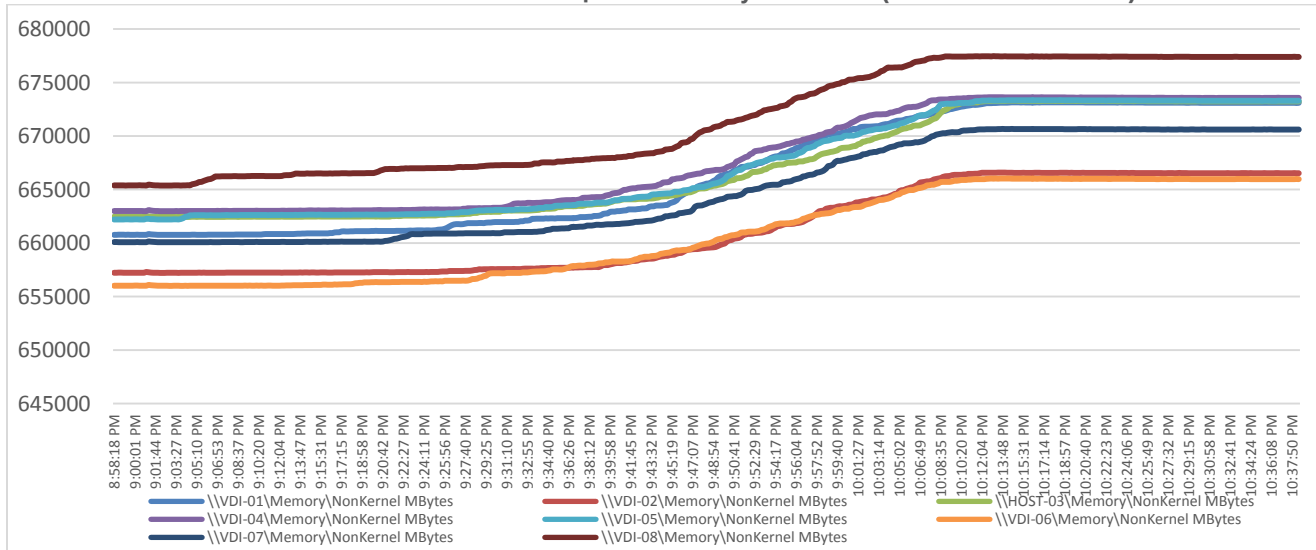
**Figure 69. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users| VSI Score**



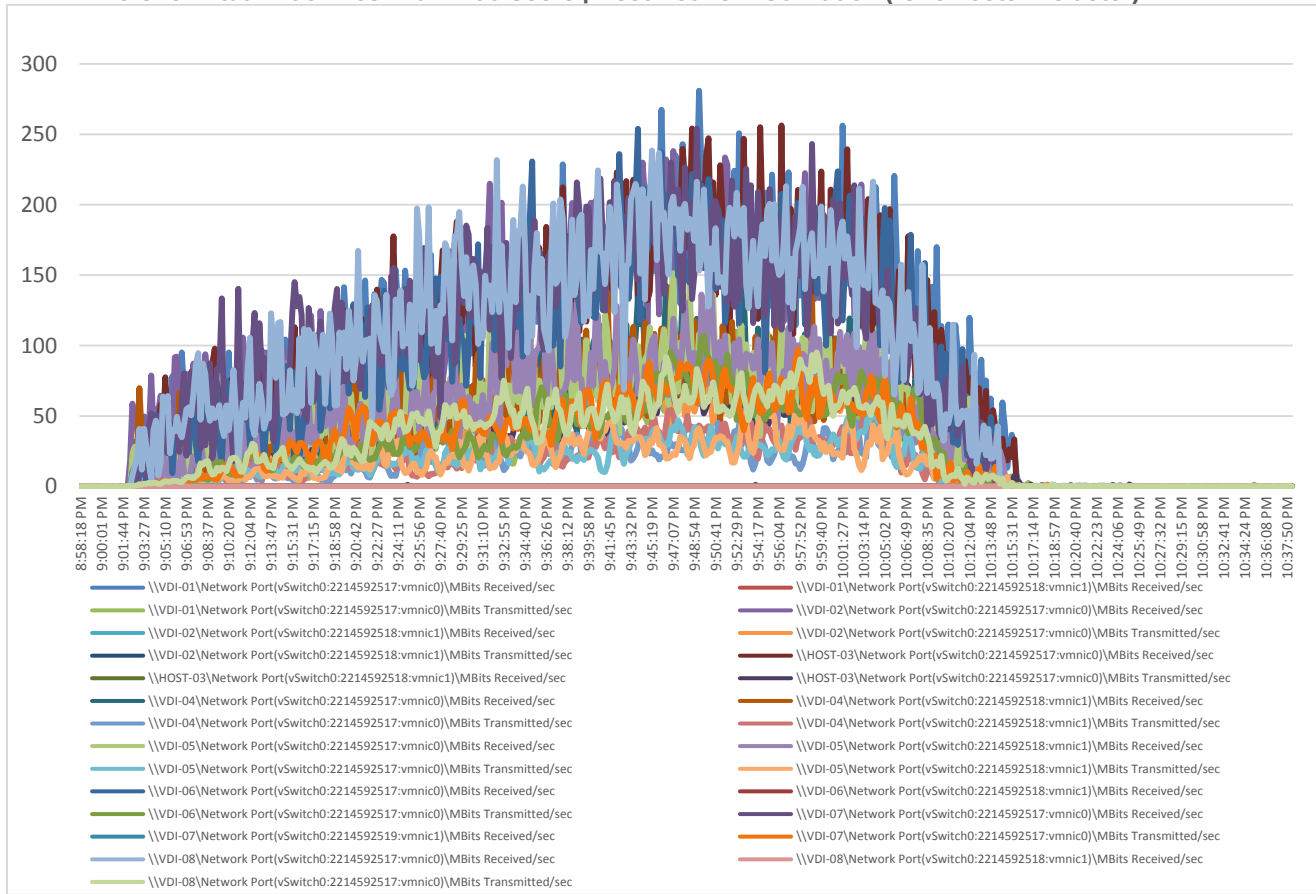
**Figure 70. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users| Host CPU Utilization (for 8 hosts in cluster)**



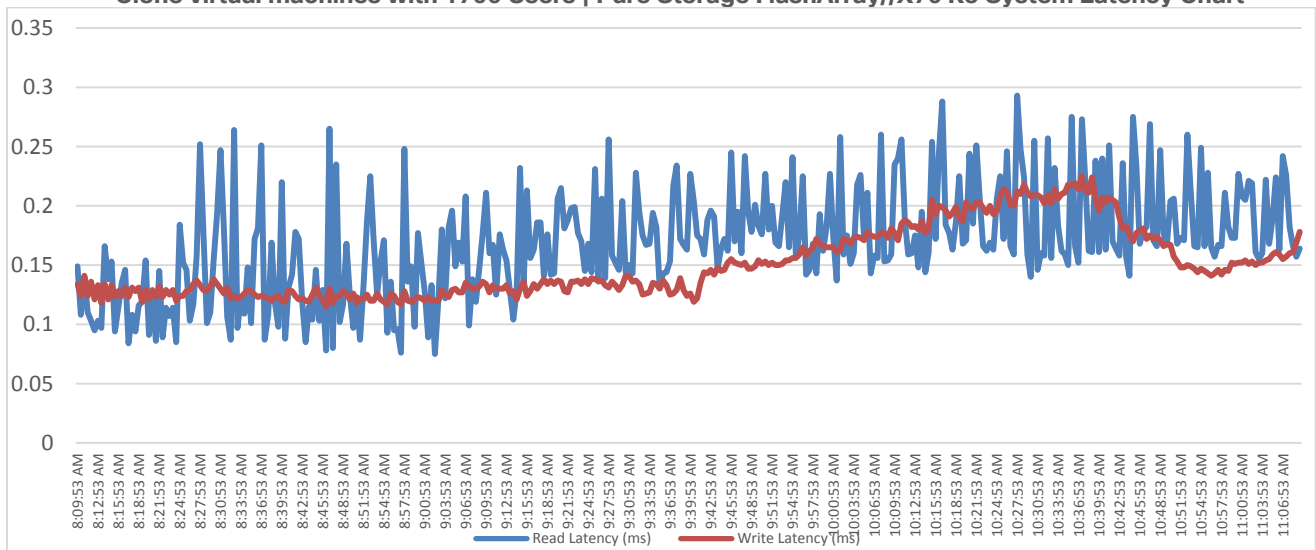
**Figure 71. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | Host Memory Utilization (for 8 hosts in cluster)**



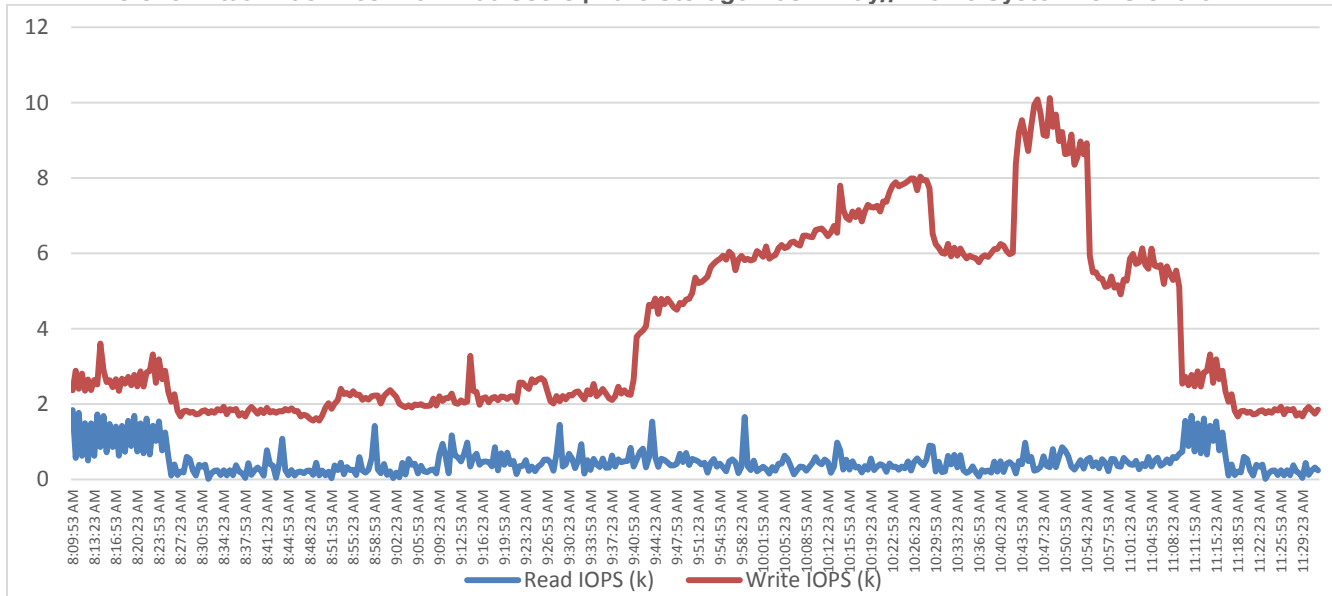
**Figure 72. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | Host Network Utilization (for 8 hosts in cluster)**



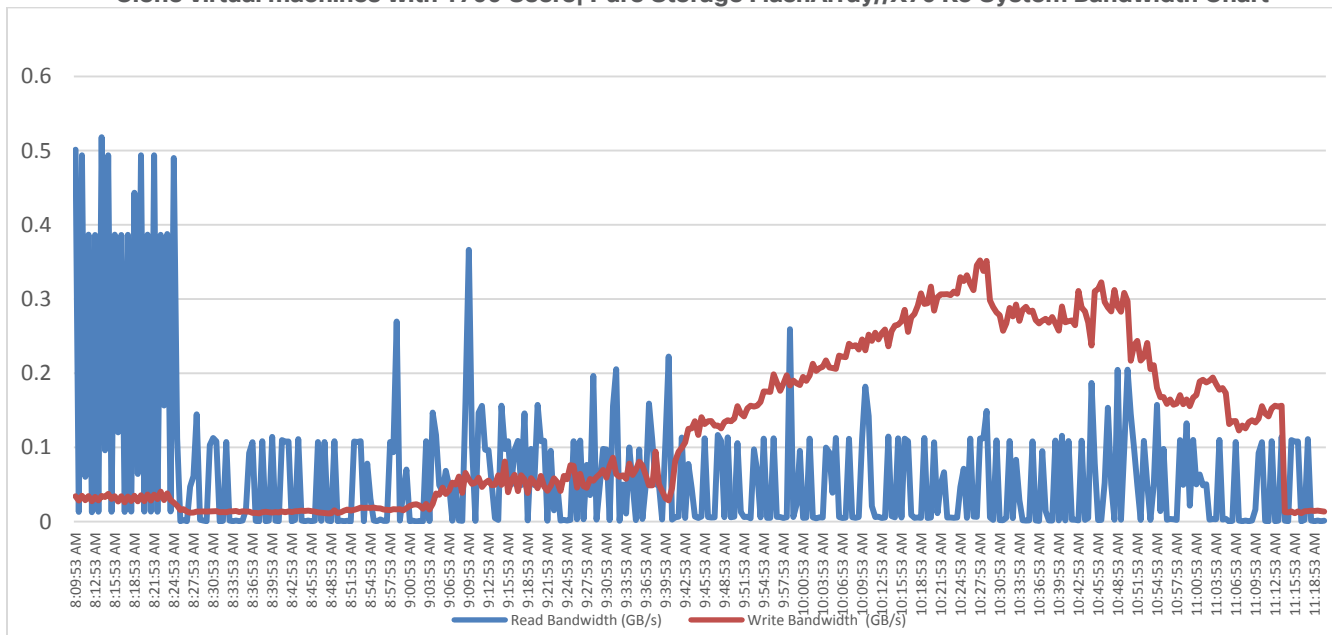
**Figure 73. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | Pure Storage FlashArray//X70 R3 System Latency Chart**



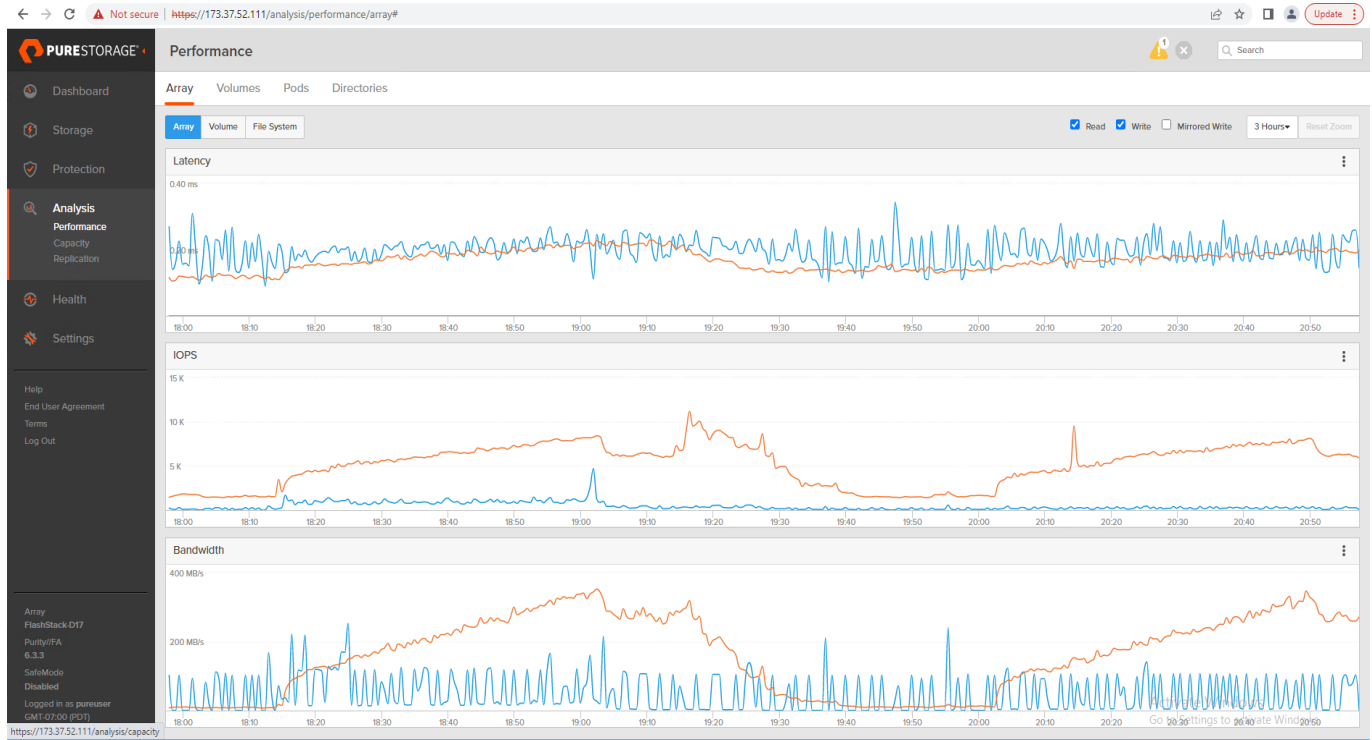
**Figure 74. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | Pure Storage FlashArray//X70 R3 System IOPS Chart**



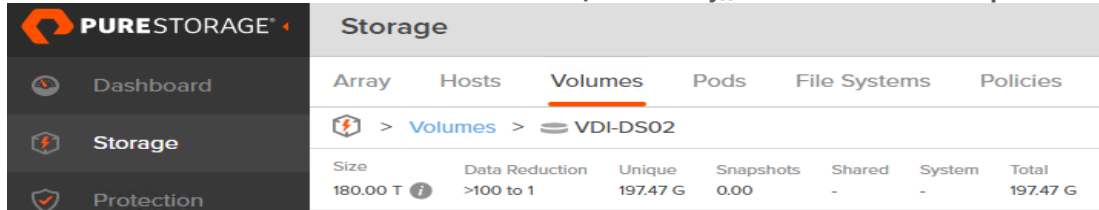
**Figure 75. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | Pure Storage FlashArray//X70 R3 System Bandwidth Chart**



**Figure 76. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | FlashArray//X70 R3 System Performance Chart**



**Figure 77. Full Scale | 1700 Users | VMware Horizon 8 2212 Horizon persistent Win 10 single-session Full Clone virtual machines with 1700 Users | FlashArray//X70 R3 volume data optimization**





---

## Summary

FlashStack is a powerful and reliable platform that has been specifically developed for enterprise end-user computing deployments and cloud data centers. It utilizes a range of innovative technologies, including Cisco UCS Blade and Rack Servers, Cisco Fabric Interconnects, Cisco Nexus 9000 switches, Cisco MDS 9100 Fibre Channel switches, and Pure Storage FlashArray//X70 R3 Storage Array, to provide customers with a comprehensive solution that is designed and validated using best practices for compute, network, and storage.

With the introduction of Cisco UCS B200 M6 Series modular platform and Cisco Intersight, FlashStack now offers even more benefits to its users. These technologies enhance the ability to provide complete visibility and orchestration across all elements of the FlashStack datacenter, enabling users to modernize their infrastructure and operations. This means that users can achieve higher levels of efficiency, scalability, and flexibility while also reducing deployment time, project risk, and IT costs.

FlashStack has been validated using industry-standard benchmarks to ensure that it meets the highest standards of performance, management, scalability, and resilience. This makes it the ideal choice for customers who are looking to deploy enterprise-class VDI and other IT initiatives. With its powerful combination of hardware and software, FlashStack is capable of meeting the demands of the most complex and demanding IT environments, ensuring that users can focus on their core business objectives without having to worry about the underlying infrastructure.

## Get More Business Value with Services

Whether you are planning your next-generation environment, need specialized know-how for a major deployment, or want to get the most from your current storage, Cisco Advanced Services, Pure Storage FlashArray//X70 R3 storage and our certified partners can help. We collaborate with you to enhance your IT capabilities through a full portfolio of services for your IT lifecycle with:

- Strategy services to align IT with your business goals.
- Design services to architect your best storage environment.
- Deploy and transition services to implement validated architectures and prepare your storage environment.
- Operations services to deliver continuous operations while driving operational excellence and efficiency.

Additionally, Cisco Advanced Services and Pure Storage Support provide in-depth knowledge transfer and education services that give you access to our global technical resources and intellectual property.

---

## About the Author

Ramesh Guduru, Technical Marketing Engineer, Desktop Virtualization and Graphics Solutions, Cisco Systems, Inc.

Ramesh Guduru is a member of the Cisco's Computing Systems Product Group team focusing on design, testing, and solutions validation, technical content creation, performance testing/benchmarking and end user computing. He has years of experience in VMware products, Microsoft Server and Desktop Virtualization, Virtual Desktop Infrastructure (VDI) in converged and hyper converged environments.

Ramesh is a subject matter expert on Desktop and Server virtualization, Cisco HyperFlex, Cisco Unified Computing System, Cisco Nexus Switching, and NVIDIA/AMD Graphics.

## Acknowledgements

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

- Tristan Todd, Staff Field Solutions Architect, Pure Storage, Inc.
- Jason Langer, Sr. Cloud Solutions Marketing Manager, Pure Storage, Inc.
- Joe Houghes, Senior Solutions Architect, Pure Storage, Inc.
- Craig Waters, Technical Director, Pure Storage, Inc.

---

## Appendix

This appendix contains the following:

- [Appendix A - Switch Configuration](#)
- [Appendix B - References Used in Guide](#)
- [Appendix C - Glossary](#)
- [Appendix D - Acronyms](#)

## Appendix A - Switch Configurations

### Cisco Nexus 93180YC-A Configuration

```
version 9.3(3) Bios:version 05.39
switchname K23-N9K-A
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
vdc K23-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
feature nxapi
feature bash-shell
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc
feature telemetry
no password strength-check
username admin password 5 $5$0BAB7aa4$v07pyr7xw1f5WpD2wZc3qmG3Flb04Wa62aNgxg82hUA role
network-admin
ip domain-lookup
system default switchport
ip access-list acl1
  10 permit ip 10.10.71.0/24 any
ip access-list acl_oob
  10 permit ip 10.10.71.0/24 any
system qos
  service-policy type network-qos jumbo
```

```
copp profile lenient
snmp-server user admin network-admin auth md5 0x83fa863523d7d94fe06388d7669f62f5 priv
0x83fa863523d7d94fe06388d7669f62f5 localizedkey
snmp-server host 173.37.52.102 traps version 2c public udp-port 1163
snmp-server host 192.168.24.30 traps version 2c public udp-port 1163
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO
ntp server 10.10.50.252 use-vrf default
ntp peer 10.10.50.253 use-vrf default
ntp server 171.68.38.65 use-vrf default
ntp logging
ntp master 8
vlan 1,50-56,70-76
vlan 50
    name Inband-Mgmt-C1
vlan 51
    name Infra-Mgmt-C1
vlan 52
    name StorageIP-C1
vlan 53
    name vMotion-C1
vlan 54
    name VM-Data-C1
vlan 55
    name Launcher-C1
vlan 56
    name Launcher-Mgmt-C1
vlan 70
    name InBand-Mgmt-SP
vlan 71
    name Infra-Mgmt-SP
vlan 72
    name VM-Network-SP
vlan 73
    name vMotion-SP
vlan 74
    name Storage_A-SP
vlan 75
    name Storage_B-SP
vlan 76
    name Launcher-SP
service dhcp
ip dhcp relay
ip dhcp relay information option
```

```
ipv6 dhcp relay
vrf context management
  ip route 0.0.0.0/0 173.37.52.1
hardware access-list tcam region ing-racl 1536
hardware access-list tcam region nat 256
vpc domain 50
  role priority 10
  peer-keepalive destination 173.37.52.104 source 173.37.52.103
  delay restore 150
  auto-recovery
interface Vlan1
  no shutdown
interface Vlan50
  no shutdown
  ip address 10.10.50.252/24
  hsrp version 2
  hsrp 50
    preempt
    priority 110
    ip 10.10.50.1
interface Vlan51
  no shutdown
  ip address 10.10.51.252/24
  hsrp version 2
  hsrp 51
    preempt
    priority 110
    ip 10.10.51.1
interface Vlan52
  no shutdown
  ip address 10.10.52.2/24
  hsrp version 2
  hsrp 52
    preempt
    priority 110
    ip 10.10.52.1
interface Vlan53
  no shutdown
  ip address 10.10.53.2/24
  hsrp version 2
  hsrp 53
    preempt
    priority 110
    ip 10.10.53.1
interface Vlan54
  no shutdown
  ip address 10.54.0.2/19
```

```
hsrp version 2
hsrp 54
  preempt
  priority 110
  ip 10.54.0.1
ip dhcp relay address 10.10.71.11
ip dhcp relay address 10.10.71.12
interface Vlan55
  no shutdown
  ip address 10.10.55.2/23
  hsrp version 2
  hsrp 55
    preempt
    priority 110
    ip 10.10.55.1
  ip dhcp relay address 10.10.51.11
  ip dhcp relay address 10.10.51.12
interface Vlan56
  no shutdown
  ip address 10.10.56.2/24
  hsrp version 2
  hsrp 56
    preempt
    ip 10.10.56.1
  ip dhcp relay address 10.10.51.11
  ip dhcp relay address 10.10.51.12
interface Vlan70
  no shutdown
  ip address 10.10.70.2/24
  hsrp version 2
  hsrp 70
    preempt
    priority 110
    ip 10.10.70.1
interface Vlan71
  no shutdown
  ip address 10.10.71.2/24
  hsrp version 2
  hsrp 71
    preempt
    priority 110
    ip 10.10.71.1
interface Vlan72
  no shutdown
  ip address 10.72.0.2/19
  hsrp version 2
  hsrp 72
```

```
preempt
priority 110
ip 10.72.0.1
ip dhcp relay address 10.10.71.11
ip dhcp relay address 10.10.71.12
interface Vlan73
no shutdown
ip address 10.10.73.2/24
hsrp version 2
hsrp 73
preempt
priority 110
ip 10.10.73.1
interface Vlan74
no shutdown
ip address 10.10.74.2/24
hsrp version 2
hsrp 74
preempt
priority 110
ip 10.10.74.1
interface Vlan75
no shutdown
ip address 10.10.75.2/24
hsrp version 2
hsrp 75
preempt
priority 110
ip 10.10.75.1
interface Vlan76
no shutdown
ip address 10.10.76.2/23
hsrp version 2
hsrp 76
preempt
priority 110
ip 10.10.76.1
ip dhcp relay address 10.10.71.11
ip dhcp relay address 10.10.71.12
interface port-channel10
description VPC-PeerLink
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
spanning-tree port type network
vpc peer-link
interface port-channel11
description FI-Uplink-K22-B
```

```
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
spanning-tree port type edge trunk
mtu 9216
vpc 11
interface port-channel12
description FI-Uplink-K22-B
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
spanning-tree port type edge trunk
mtu 9216
vpc 12
interface port-channel49
description FI-Uplink-K23
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
spanning-tree port type edge trunk
mtu 9216
vpc 49
interface port-channel50
description FI-Uplink-K23
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
spanning-tree port type edge trunk
mtu 9216
vpc 50
interface Ethernet1/1
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/2
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/3
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/4
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/5
```



```
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
interface Ethernet1/16
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
    switchport access vlan 71
    spanning-tree port type edge
interface Ethernet1/34
    switchport access vlan 71
    spanning-tree port type edge
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 VLAN 30 access JH
    switchport access vlan 30
    switchport trunk allowed vlan 1,30-36,60-68,132
```

```
speed 1000
interface Ethernet1/46
interface Ethernet1/47
    switchport access vlan 50
    spanning-tree port type edge
interface Ethernet1/48
interface Ethernet1/49
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    mtu 9216
    channel-group 49 mode active
interface Ethernet1/50
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    mtu 9216
    channel-group 50 mode active
interface Ethernet1/51
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    channel-group 11 mode active
interface Ethernet1/52
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    channel-group 12 mode active
interface Ethernet1/53
    switchport mode trunk
    switchport trunk allowed vlan 1,30-36,50-56,60-68,70-76,132
interface Ethernet1/54
interface mgmt0
    vrf member management
    ip address 173.37.52.103/23
line console
line vty
boot nxos bootflash:/nxos.9.3.3.bin
no system default switchport shutdown
telemetry
    certificate /bootflash/home/admin/telemetry-cert.pem localhost
    destination-profile
        use-nodeid timba-640142e96f72612d3459249f
    destination-group timba-640142e96f72612d3459249f-0
        ip address 10.10.71.20 port 443 protocol HTTP encoding JSON
    sensor-group timba-640142e96f72612d3459249f-0
        data-source NX-API
```

```

    path "show system resources all-modules" depth 0
sensor-group timba-640142e96f72612d3459249f-1
    data-source NX-API
    path "show module" depth 0
sensor-group timba-640142e96f72612d3459249f-2
    data-source NX-API
    path "show environment power" depth 0
sensor-group timba-640142e96f72612d3459249f-3
    data-source NX-API
    path "show interface fc regex *" depth 0
sensor-group timba-640142e96f72612d3459249f-4
    data-source DME
    path sys/ch depth 1 query-condition query-target=subtree&target-subtree-
class=eqptSensor
sensor-group timba-640142e96f72612d3459249f-5
    data-source DME
    path sys/ch query-condition query-target=subtree&target-subtree-class=eqptSupC
sensor-group timba-640142e96f72612d3459249f-6
    data-source DME
    path sys/ch query-condition query-target=subtree&target-subtree-class=eqptFt
sensor-group timba-640142e96f72612d3459249f-7
    data-source DME
    path sys/intf depth 0 query-condition query-target=subtree&target-subtree-
class=ethpmPhysIf filter-condition updated(ethpmPhysIf.operSt)
subscription 2643
    dst-grp timba-640142e96f72612d3459249f-0
    snsr-grp timba-640142e96f72612d3459249f-0 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-1 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-2 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-3 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-4 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-5 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-6 sample-interval 30000
    snsr-grp timba-640142e96f72612d3459249f-7 sample-interval 0

```

## Cisco Nexus 93180YC -B Configuration

```

version 9.3(3) Bios:version 05.39
switchname K23-N9K-B
policy-map type network-qos jumbo
    class type network-qos class-default
        mtu 9216
vdc K23-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
feature nxapi
feature bash-shell
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature dhcp
feature vpc
feature telemetry
no password strength-check
username admin password 5 $5$5TxyL6Rl$7U4nS.UfzkPgXl5mVqiuHoPLHyAZgnNAiKyz7aEVK05 role
network-admin
ip domain-lookup
system default switchport
system qos
  service-policy type network-qos jumbo
copp profile lenient
snmp-server user admin network-admin auth md5 0x57cdc0fb04a0dd922046cb694508c9b7 priv
0x57cdc0fb04a0dd922046cb694508c9b7 localizedkey
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO
ntp server 171.68.38.65 use-vrf default
vlan 1,50-56,70-76,132
vlan 50
  name Inband-Mgmt-C1
vlan 51
  name Infra-Mgmt-C1
vlan 52
  name StorageIP-C1
vlan 53
  name vMotion-C1
vlan 54
  name VM-Data-C1
vlan 55
  name Launcher-C1
vlan 56
  name Launcher-Mgmt-C1
vlan 70
  name InBand-Mgmt-SP
vlan 71
  name Infra-Mgmt-SP
```

```
vlan 72
  name VM-Network-SP
vlan 73
  name vMotion-SP
vlan 74
  name Storage_A-SP
vlan 75
  name Storage_B-SP
vlan 76
  name Launcher-SP
vlan 132
  name OOB-Mgmt
service dhcp
ip dhcp relay
ip dhcp relay information option
ipv6 dhcp relay
vrf context management
  ip route 0.0.0.0/0 173.37.52.1
vpc domain 50
  role priority 10
  peer-keepalive destination 173.37.52.103 source 173.37.52.104
  delay restore 150
  auto-recovery
interface Vlan1
  no shutdown
interface Vlan50
  no shutdown
  ip address 10.10.50.253/24
  hsrp version 2
  hsrp 50
    preempt
    priority 110
    ip 10.10.50.1
interface Vlan51
  no shutdown
  ip address 10.10.51.253/24
  hsrp version 2
  hsrp 51
    preempt
    priority 110
    ip 10.10.51.1
interface Vlan52
  no shutdown
  ip address 10.10.52.3/24
  hsrp version 2
  hsrp 52
    preempt
```

```
        priority 110
        ip 10.10.52.1
interface Vlan53
    no shutdown
    ip address 10.10.53.3/24
    hsrp version 2
    hsrp 53
        preempt
        priority 110
        ip 10.10.53.1
interface Vlan54
    no shutdown
    ip address 10.54.0.3/19
    hsrp version 2
    hsrp 54
        preempt
        priority 110
        ip 10.54.0.1
    ip dhcp relay address 10.10.71.11
    ip dhcp relay address 10.10.71.12
interface Vlan55
    no shutdown
    ip address 10.10.55.3/23
    hsrp version 2
    hsrp 55
        preempt
        priority 110
        ip 10.10.55.1
    ip dhcp relay address 10.10.51.11
    ip dhcp relay address 10.10.51.12
interface Vlan56
    no shutdown
    ip address 10.10.56.3/24
    hsrp version 2
    hsrp 56
        preempt
        ip 10.10.56.1
    ip dhcp relay address 10.10.51.11
    ip dhcp relay address 10.10.51.12
interface Vlan70
    no shutdown
    ip address 10.10.70.3/24
    hsrp version 2
    hsrp 70
        preempt
        priority 110
        ip 10.10.70.1
```

```
interface Vlan71
  no shutdown
  ip address 10.10.71.3/24
  hsrp version 2
  hsrp 71
    preempt
    priority 110
    ip 10.10.71.1
interface Vlan72
  no shutdown
  ip address 10.72.0.3/19
  hsrp version 2
  hsrp 72
    preempt
    priority 110
    ip 10.72.0.1
  ip dhcp relay address 10.10.71.11
  ip dhcp relay address 10.10.71.12
interface Vlan73
  no shutdown
  ip address 10.10.73.3/24
  hsrp version 2
  hsrp 73
    preempt
    priority 110
    ip 10.10.73.1
interface Vlan74
  no shutdown
  ip address 10.10.74.3/24
  hsrp version 2
  hsrp 74
    preempt
    priority 110
    ip 10.10.74.1
interface Vlan75
  no shutdown
  ip address 10.10.75.3/24
  hsrp version 2
  hsrp 75
    preempt
    priority 110
    ip 10.10.75.1
interface Vlan76
  no shutdown
  ip address 10.10.76.3/23
  hsrp version 2
  hsrp 76
```

```
    preempt
    priority 110
    ip 10.10.76.1
ip dhcp relay address 10.10.71.11
ip dhcp relay address 10.10.71.12
interface port-channel10
    description VPC-PeerLink
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type network
    vpc peer-link
interface port-channel11
    description FI-Uplink-K22-A
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    vpc 11
interface port-channel12
    description FI-Uplink-K22-B
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    vpc 12
interface port-channel49
    description FI-Uplink-K23-A
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    vpc 49
interface port-channel50
    description FI-Uplink-K23-B
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    vpc 50
interface Ethernet1/1
    description VPC to K23-N9K-A
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    channel-group 10 mode active
interface Ethernet1/2
    description VPC to K23-N9K-A
    switchport mode trunk
```



```
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/3
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/4
description VPC to K23-N9K-A
switchport mode trunk
switchport trunk allowed vlan 1,50-56,70-76,132
channel-group 10 mode active
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
interface Ethernet1/16
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
switchport access vlan 71
spanning-tree port type edge
interface Ethernet1/34
switchport access vlan 71
spanning-tree port type edge
interface Ethernet1/35
```

```
interface Ethernet1/36
interface Ethernet1/37
interface Ethernet1/38
interface Ethernet1/39
interface Ethernet1/40
interface Ethernet1/41
interface Ethernet1/42
interface Ethernet1/43
interface Ethernet1/44
interface Ethernet1/45
interface Ethernet1/46
    description K23-HXVDIJH
    switchport access vlan 70
    spanning-tree port type edge
interface Ethernet1/47
interface Ethernet1/48
interface Ethernet1/49
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    mtu 9216
    channel-group 49 mode active
interface Ethernet1/50
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    mtu 9216
    channel-group 50 mode active
interface Ethernet1/51
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    channel-group 11 mode active
interface Ethernet1/52
    switchport mode trunk
    switchport trunk allowed vlan 1,50-56,70-76,132
    spanning-tree port type edge trunk
    mtu 9216
    channel-group 12 mode active
interface Ethernet1/53
    switchport mode trunk
    switchport trunk allowed vlan 1,30-36,50-56,60-68,70-76,132
interface Ethernet1/54
interface mgmt0
    vrf member management
    ip address 173.37.52.104/23
line console
line vty
```

```

boot nxos bootflash:/nxos.9.3.3.bin
no system default switchport shutdown
telemetry
  certificate /bootflash/home/admin/telemetry-cert.pem localhost
  destination-profile
    use-nodeid timba-640143f86f72612d345931c3
  destination-group timba-640143f86f72612d345931c3-0
    ip address 10.10.71.20 port 443 protocol HTTP encoding JSON
  sensor-group timba-640143f86f72612d345931c3-0
    data-source NX-API
    path "show system resources all-modules" depth 0
  sensor-group timba-640143f86f72612d345931c3-1
    data-source NX-API
    path "show module" depth 0
  sensor-group timba-640143f86f72612d345931c3-2
    data-source NX-API
    path "show environment power" depth 0
  sensor-group timba-640143f86f72612d345931c3-3
    data-source NX-API
    path "show interface fc regex *" depth 0
  sensor-group timba-640143f86f72612d345931c3-4
    data-source DME
    path sys/ch depth 1 query-condition query-target=subtree&target-subtree-
class=eqptSensor
  sensor-group timba-640143f86f72612d345931c3-5
    data-source DME
    path sys/ch query-condition query-target=subtree&target-subtree-class=eqptSupC
  sensor-group timba-640143f86f72612d345931c3-6
    data-source DME
    path sys/ch query-condition query-target=subtree&target-subtree-class=eqptFt
  sensor-group timba-640143f86f72612d345931c3-7
    data-source DME
    path sys/intf depth 0 query-condition query-target=subtree&target-subtree-
class=ethpmPhysIf filter-condition updated(ethpmPhysIf.operSt)
subscription 1565
  dst-grp timba-640143f86f72612d345931c3-0
  snsr-grp timba-640143f86f72612d345931c3-0 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-1 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-2 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-3 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-4 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-5 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-6 sample-interval 30000
  snsr-grp timba-640143f86f72612d345931c3-7 sample-interval 0

```

## Cisco MDS 9132T-A Configuration

version 8.4(2d)

```
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 $5$Dcs72Ao/$8lHyVrotTm4skqb/84BC793tgdly/yWf9IoMx2OEg6C role
network-admin
ip domain-lookup
ip name-server 10.10.61.30
ip host ADD16-MDS-A 10.29.164.238
aaa group server radius radius
snmp-server user admin network-admin auth md5 0x616758aed4f07bab2d24f3d594ebd649 priv
0x616758aed4f07bab2d24f3d594ebd649 localizedkey
snmp-server host 10.24.30.91 traps version 2c public udp-port 1163
snmp-server host 10.24.46.67 traps version 2c public udp-port 1163
snmp-server host 10.24.66.169 traps version 2c public udp-port 1163
snmp-server host 10.24.72.119 traps version 2c public udp-port 1165
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 10.81.254.131
ntp server 10.81.254.202
vsan database
  vsan 100 name "FlashStack-VCC-CVD-Fabric-A"
device-alias database
  device-alias name X70R3-CT0-FC0 pwnn 52:4a:93:71:56:84:09:00
  device-alias name X70R3-CT1-FC0 pwnn 52:4a:93:71:56:84:09:10
  device-alias name VCC-Infra01-HBA0 pwnn 20:00:00:25:b5:aa:17:1e
  device-alias name VCC-Infra01-HBA2 pwnn 20:00:00:25:b5:aa:17:1f
  device-alias name VCC-Infra02-HBA0 pwnn 20:00:00:25:b5:aa:17:3e
  device-alias name VCC-Infra02-HBA2 pwnn 20:00:00:25:b5:aa:17:3f
  device-alias name VCC-WLHost01-HBA0 pwnn 20:00:00:25:b5:aa:17:00
  device-alias name VCC-WLHost01-HBA2 pwnn 20:00:00:25:b5:aa:17:01
  device-alias name VCC-WLHost02-HBA0 pwnn 20:00:00:25:b5:aa:17:02
  device-alias name VCC-WLHost02-HBA2 pwnn 20:00:00:25:b5:aa:17:03
  device-alias name VCC-WLHost03-HBA0 pwnn 20:00:00:25:b5:aa:17:04
  device-alias name VCC-WLHost03-HBA2 pwnn 20:00:00:25:b5:aa:17:05
  device-alias name VCC-WLHost04-HBA0 pwnn 20:00:00:25:b5:aa:17:06
  device-alias name VCC-WLHost04-HBA2 pwnn 20:00:00:25:b5:aa:17:07
```

```

device-alias name VCC-WLHost05-HBA0 pwn 20:00:00:25:b5:aa:17:08
device-alias name VCC-WLHost05-HBA2 pwn 20:00:00:25:b5:aa:17:09
device-alias name VCC-WLHost06-HBA0 pwn 20:00:00:25:b5:aa:17:0a
device-alias name VCC-WLHost06-HBA2 pwn 20:00:00:25:b5:aa:17:0b
device-alias name VCC-WLHost07-HBA0 pwn 20:00:00:25:b5:aa:17:0c
device-alias name VCC-WLHost07-HBA2 pwn 20:00:00:25:b5:aa:17:0d
device-alias name VCC-WLHost08-HBA0 pwn 20:00:00:25:b5:aa:17:0e
device-alias name VCC-WLHost08-HBA2 pwn 20:00:00:25:b5:aa:17:0f
device-alias name VCC-WLHost09-HBA0 pwn 20:00:00:25:b5:aa:17:10
device-alias name VCC-WLHost09-HBA2 pwn 20:00:00:25:b5:aa:17:11
device-alias name VCC-WLHost10-HBA0 pwn 20:00:00:25:b5:aa:17:12
device-alias name VCC-WLHost10-HBA2 pwn 20:00:00:25:b5:aa:17:13
device-alias name VCC-WLHost11-HBA0 pwn 20:00:00:25:b5:aa:17:14
device-alias name VCC-WLHost11-HBA2 pwn 20:00:00:25:b5:aa:17:15
device-alias name VCC-WLHost12-HBA0 pwn 20:00:00:25:b5:aa:17:16
device-alias commit
fcdomain fcid database
vsan 100 wwn 20:03:00:de:fb:92:8d:00 fcid 0x300000 dynamic
vsan 100 wwn 52:4a:93:75:dd:91:0a:02 fcid 0x300020 dynamic
! [X70-CT0-FC2]
vsan 100 wwn 52:4a:93:75:dd:91:0a:17 fcid 0x300040 dynamic
vsan 100 wwn 52:4a:93:75:dd:91:0a:06 fcid 0x300041 dynamic
! [X70-CT0-FC8]
vsan 100 wwn 52:4a:93:75:dd:91:0a:07 fcid 0x300042 dynamic
vsan 100 wwn 52:4a:93:75:dd:91:0a:16 fcid 0x300043 dynamic
! [X70-CT1-FC8]
vsan 100 wwn 20:00:00:25:b5:aa:17:3e fcid 0x300060 dynamic
! [VCC-Infra02-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:07 fcid 0x300061 dynamic
! [VCC-WLHost04-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:06 fcid 0x300062 dynamic
! [VCC-WLHost04-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:3a fcid 0x300063 dynamic
! [VCC-WLHost29-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:29 fcid 0x300064 dynamic
! [VCC-WLHost20-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:13 fcid 0x300065 dynamic
! [VCC-WLHost10-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:1c fcid 0x300066 dynamic
! [VCC-WLHost15-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:32 fcid 0x300067 dynamic
! [VCC-WLHost25-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:17 fcid 0x300068 dynamic
! [VCC-WLHost12-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:2e fcid 0x300069 dynamic
! [VCC-WLHost23-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:1f fcid 0x30006a dynamic

```

```
!           [VCC-Infra01-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:1b fcid 0x30006b dynamic
!           [VCC-WLHost14-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:1a fcid 0x30006c dynamic
!           [VCC-WLHost14-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:0a fcid 0x30006d dynamic
!           [VCC-WLHost06-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:34 fcid 0x30006e dynamic
!           [VCC-WLHost26-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:19 fcid 0x30006f dynamic
!           [VCC-WLHost13-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:36 fcid 0x300070 dynamic
!           [VCC-WLHost27-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:01 fcid 0x300071 dynamic
!           [VCC-WLHost01-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:12 fcid 0x300072 dynamic
!           [VCC-WLHost10-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:16 fcid 0x300073 dynamic
!           [VCC-WLHost12-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:2b fcid 0x300074 dynamic
!           [VCC-WLHost21-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:25 fcid 0x300075 dynamic
!           [VCC-WLHost18-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:27 fcid 0x300076 dynamic
!           [VCC-WLHost19-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:3d fcid 0x300077 dynamic
!           [VCC-WLHost30-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:15 fcid 0x300078 dynamic
!           [VCC-WLHost11-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:38 fcid 0x300079 dynamic
!           [VCC-WLHost28-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:23 fcid 0x30007a dynamic
!           [VCC-WLHost17-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:00 fcid 0x30007b dynamic
!           [VCC-WLHost01-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:04 fcid 0x30007c dynamic
!           [VCC-WLHost03-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:03 fcid 0x30007d dynamic
!           [VCC-WLHost02-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:0f fcid 0x30007e dynamic
!           [VCC-WLHost08-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:1d fcid 0x30007f dynamic
!           [VCC-WLHost15-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:31 fcid 0x300080 dynamic
!           [VCC-WLHost24-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:30 fcid 0x300081 dynamic
!           [VCC-WLHost24-HBA0]
```

```
vsan 100 wwn 20:00:00:25:b5:aa:17:02 fcid 0x300082 dynamic
!      [VCC-WLHost02-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:08 fcid 0x300083 dynamic
!      [VCC-WLHost05-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:26 fcid 0x300084 dynamic
!      [VCC-WLHost19-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:22 fcid 0x300085 dynamic
!      [VCC-WLHost17-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:2c fcid 0x300086 dynamic
!      [VCC-WLHost22-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:33 fcid 0x300087 dynamic
!      [VCC-WLHost25-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:21 fcid 0x300088 dynamic
!      [VCC-WLHost16-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:2d fcid 0x300089 dynamic
!      [VCC-WLHost22-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:24 fcid 0x30008a dynamic
!      [VCC-WLHost18-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:3f fcid 0x30008b dynamic
!      [VCC-Infra02-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:39 fcid 0x30008c dynamic
!      [VCC-WLHost28-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:3c fcid 0x30008d dynamic
!      [VCC-WLHost30-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:14 fcid 0x30008e dynamic
!      [VCC-WLHost11-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:11 fcid 0x30008f dynamic
!      [VCC-WLHost09-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:10 fcid 0x300090 dynamic
!      [VCC-WLHost09-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:05 fcid 0x300091 dynamic
!      [VCC-WLHost03-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:0e fcid 0x300092 dynamic
!      [VCC-WLHost08-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:0d fcid 0x300093 dynamic
!      [VCC-WLHost07-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:0c fcid 0x300094 dynamic
!      [VCC-WLHost07-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:1e fcid 0x300095 dynamic
!      [VCC-Infra01-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:0b fcid 0x300096 dynamic
!      [VCC-WLHost06-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:28 fcid 0x300097 dynamic
!      [VCC-WLHost20-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:37 fcid 0x300098 dynamic
!      [VCC-WLHost27-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:3b fcid 0x300099 dynamic
```

```
!           [VCC-WLHost29-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:09 fcid 0x30009a dynamic
!           [VCC-WLHost05-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:2a fcid 0x30009b dynamic
!           [VCC-WLHost21-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:2f fcid 0x30009c dynamic
!           [VCC-WLHost23-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:20 fcid 0x30009d dynamic
!           [VCC-WLHost16-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:35 fcid 0x30009e dynamic
!           [VCC-WLHost26-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:18 fcid 0x30009f dynamic
!           [VCC-WLHost13-HBA0]
vsan 100 wwn 20:02:00:de:fb:92:8d:00 fcid 0x3000a0 dynamic
vsan 100 wwn 20:04:00:de:fb:92:8d:00 fcid 0x3000c0 dynamic
vsan 100 wwn 20:01:00:de:fb:92:8d:00 fcid 0x3000e0 dynamic
vsan 100 wwn 52:4a:93:75:dd:91:0a:00 fcid 0x300044 dynamic
!           [X70-CT0-FC0]
vsan 100 wwn 20:01:00:3a:9c:0e:33:20 fcid 0x3000e1 dynamic
vsan 100 wwn 20:02:00:3a:9c:0e:33:20 fcid 0x3000a1 dynamic
vsan 100 wwn 20:04:00:3a:9c:0e:33:20 fcid 0x3000c1 dynamic
vsan 100 wwn 20:03:00:3a:9c:0e:33:20 fcid 0x300100 dynamic
vsan 100 wwn 52:4a:93:75:dd:91:0a:10 fcid 0x300021 dynamic
!           [X70-CT1-FC0]
vsan 100 wwn 52:4a:93:71:56:84:09:12 fcid 0x300022 dynamic
vsan 100 wwn 52:4a:93:71:56:84:09:10 fcid 0x300045 dynamic
!           [X70R3-CT1-FC0]
vsan 100 wwn 52:4a:93:71:56:84:09:02 fcid 0x300046 dynamic
vsan 100 wwn 52:4a:93:71:56:84:09:00 fcid 0x300023 dynamic
!           [X70R3-CT0-FC0]
vsan 100 wwn 20:00:00:25:b5:aa:17:40 fcid 0x3000e2 dynamic
!           [AMD-VMHost70-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:41 fcid 0x3000a2 dynamic
!           [AMD-VMHost70-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:44 fcid 0x3000e3 dynamic
!           [AMD-VMHost72-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:45 fcid 0x3000a3 dynamic
!           [AMD-VMHost72-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:4e fcid 0x3000e4 dynamic
!           [AMD-VMHost73-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:4f fcid 0x3000a4 dynamic
!           [AMD-VMHost73-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:42 fcid 0x3000e5 dynamic
!           [AMD-VMHost71-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:43 fcid 0x3000a5 dynamic
!           [AMD-VMHost71-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:46 fcid 0x3000e6 dynamic
```



```

!           [AMD-VMHost74-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:47 fcid 0x3000a6 dynamic
!           [AMD-VMHost74-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:48 fcid 0x3000e7 dynamic
!           [AMD-VMHost75-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:49 fcid 0x3000a7 dynamic
!           [AMD-VMHost75-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:4a fcid 0x3000e8 dynamic
!           [AMD-VMHost76-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:4b fcid 0x3000a8 dynamic
!           [AMD-VMHost76-HBA2]
vsan 100 wwn 20:00:00:25:b5:aa:17:4c fcid 0x3000e9 dynamic
!           [AMD-VMHost77-HBA0]
vsan 100 wwn 20:00:00:25:b5:aa:17:4d fcid 0x3000a9 dynamic
!           [AMD-VMHost77-HBA2]
!Active Zone Database Section for vsan 100
zone name FlaskStack-VCC-CVD-WLHost01 vsan 100
  member pwn 20:00:00:25:b5:aa:17:00
  !           [VCC-WLHost01-HBA0]
  member pwn 20:00:00:25:b5:aa:17:01
  !           [VCC-WLHost01-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost02 vsan 100
  member pwn 20:00:00:25:b5:aa:17:02
  !           [VCC-WLHost02-HBA0]
  member pwn 20:00:00:25:b5:aa:17:03
  !           [VCC-WLHost02-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost03 vsan 100
  member pwn 20:00:00:25:b5:aa:17:04
  !           [VCC-WLHost03-HBA0]
  member pwn 20:00:00:25:b5:aa:17:05
  !           [VCC-WLHost03-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost04 vsan 100
  member pwn 20:00:00:25:b5:aa:17:06
  !           [VCC-WLHost04-HBA0]
  member pwn 20:00:00:25:b5:aa:17:07

```

```
!           [VCC-WLHost04-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost05 vsan 100
member pwn 20:00:00:25:b5:aa:17:08
!           [VCC-WLHost05-HBA0]
member pwn 20:00:00:25:b5:aa:17:09
!           [VCC-WLHost05-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost06 vsan 100
member pwn 20:00:00:25:b5:aa:17:0a
!           [VCC-WLHost06-HBA0]
member pwn 20:00:00:25:b5:aa:17:0b
!           [VCC-WLHost06-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost07 vsan 100
member pwn 20:00:00:25:b5:aa:17:0c
!           [VCC-WLHost07-HBA0]
member pwn 20:00:00:25:b5:aa:17:0d
!           [VCC-WLHost07-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost08 vsan 100
member pwn 20:00:00:25:b5:aa:17:0e
!           [VCC-WLHost08-HBA0]
member pwn 20:00:00:25:b5:aa:17:0f
!           [VCC-WLHost08-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost09 vsan 100
member pwn 20:00:00:25:b5:aa:17:10
!           [VCC-WLHost09-HBA0]
member pwn 20:00:00:25:b5:aa:17:11
!           [VCC-WLHost09-HBA2]
member pwn 52:4a:93:71:56:84:09:00
```

```
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost10 vsan 100
member pwn 20:00:00:25:b5:aa:17:12
!           [VCC-WLHost10-HBA0]
member pwn 20:00:00:25:b5:aa:17:13
!           [VCC-WLHost10-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost11 vsan 100
member pwn 20:00:00:25:b5:aa:17:14
!           [VCC-WLHost11-HBA0]
member pwn 20:00:00:25:b5:aa:17:15
!           [VCC-WLHost11-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost12 vsan 100
member pwn 20:00:00:25:b5:aa:17:16
!           [VCC-WLHost12-HBA0]
member pwn 20:00:00:25:b5:aa:17:17
!           [VCC-WLHost12-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost13 vsan 100
member pwn 20:00:00:25:b5:aa:17:18
!           [VCC-WLHost13-HBA0]
member pwn 20:00:00:25:b5:aa:17:19
!           [VCC-WLHost13-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost14 vsan 100
member pwn 20:00:00:25:b5:aa:17:1a
!           [VCC-WLHost14-HBA0]
member pwn 20:00:00:25:b5:aa:17:1b
!           [VCC-WLHost14-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
```

```

!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost15 vsan 100
  member pwn 20:00:00:25:b5:aa:17:1c
!           [VCC-WLHost15-HBA0]
  member pwn 20:00:00:25:b5:aa:17:1d
!           [VCC-WLHost15-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-Infra01 vsan 100
  member pwn 20:00:00:25:b5:aa:17:1e
!           [VCC-Infra01-HBA0]
  member pwn 20:00:00:25:b5:aa:17:1f
!           [VCC-Infra01-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost16 vsan 100
  member pwn 20:00:00:25:b5:aa:17:20
!           [VCC-WLHost16-HBA0]
  member pwn 20:00:00:25:b5:aa:17:21
!           [VCC-WLHost16-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost17 vsan 100
  member pwn 20:00:00:25:b5:aa:17:22
!           [VCC-WLHost17-HBA0]
  member pwn 20:00:00:25:b5:aa:17:23
!           [VCC-WLHost17-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost18 vsan 100
  member pwn 20:00:00:25:b5:aa:17:24
!           [VCC-WLHost18-HBA0]
  member pwn 20:00:00:25:b5:aa:17:25
!           [VCC-WLHost18-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost19 vsan 100

```

```
member pwn 20:00:00:25:b5:aa:17:26
!          [VCC-WLHost19-HBA0]
member pwn 20:00:00:25:b5:aa:17:27
!          [VCC-WLHost19-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost20 vsan 100
member pwn 20:00:00:25:b5:aa:17:28
!          [VCC-WLHost20-HBA0]
member pwn 20:00:00:25:b5:aa:17:29
!          [VCC-WLHost20-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost21 vsan 100
member pwn 20:00:00:25:b5:aa:17:2a
!          [VCC-WLHost21-HBA0]
member pwn 20:00:00:25:b5:aa:17:2b
!          [VCC-WLHost21-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost22 vsan 100
member pwn 20:00:00:25:b5:aa:17:2c
!          [VCC-WLHost22-HBA0]
member pwn 20:00:00:25:b5:aa:17:2d
!          [VCC-WLHost22-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost23 vsan 100
member pwn 20:00:00:25:b5:aa:17:2e
!          [VCC-WLHost23-HBA0]
member pwn 20:00:00:25:b5:aa:17:2f
!          [VCC-WLHost23-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost24 vsan 100
member pwn 20:00:00:25:b5:aa:17:30
!          [VCC-WLHost24-HBA0]
```

```
member pwnn 20:00:00:25:b5:aa:17:31
!           [VCC-WLHost24-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost25 vsan 100
member pwnn 20:00:00:25:b5:aa:17:32
!           [VCC-WLHost25-HBA0]
member pwnn 20:00:00:25:b5:aa:17:33
!           [VCC-WLHost25-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost26 vsan 100
member pwnn 20:00:00:25:b5:aa:17:34
!           [VCC-WLHost26-HBA0]
member pwnn 20:00:00:25:b5:aa:17:35
!           [VCC-WLHost26-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost27 vsan 100
member pwnn 20:00:00:25:b5:aa:17:36
!           [VCC-WLHost27-HBA0]
member pwnn 20:00:00:25:b5:aa:17:37
!           [VCC-WLHost27-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost28 vsan 100
member pwnn 20:00:00:25:b5:aa:17:38
!           [VCC-WLHost28-HBA0]
member pwnn 20:00:00:25:b5:aa:17:39
!           [VCC-WLHost28-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost29 vsan 100
member pwnn 20:00:00:25:b5:aa:17:3a
!           [VCC-WLHost29-HBA0]
member pwnn 20:00:00:25:b5:aa:17:3b
!           [VCC-WLHost29-HBA2]
```

```
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost30 vsan 100
member pwnn 20:00:00:25:b5:aa:17:3c
!           [VCC-WLHost30-HBA0]
member pwnn 20:00:00:25:b5:aa:17:3d
!           [VCC-WLHost30-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-Infra02 vsan 100
member pwnn 20:00:00:25:b5:aa:17:3e
!           [VCC-Infra02-HBA0]
member pwnn 20:00:00:25:b5:aa:17:3f
!           [VCC-Infra02-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost70 vsan 100
member pwnn 20:00:00:25:b5:aa:17:40
!           [AMD-VMHost70-HBA0]
member pwnn 20:00:00:25:b5:aa:17:41
!           [AMD-VMHost70-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost71 vsan 100
member pwnn 20:00:00:25:b5:aa:17:42
!           [AMD-VMHost71-HBA0]
member pwnn 20:00:00:25:b5:aa:17:43
!           [AMD-VMHost71-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost72 vsan 100
member pwnn 20:00:00:25:b5:aa:17:44
!           [AMD-VMHost72-HBA0]
member pwnn 20:00:00:25:b5:aa:17:45
!           [AMD-VMHost72-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
```

```
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost73 vsan 100
member pwn 20:00:00:25:b5:aa:17:4e
!          [AMD-VMHost73-HBA0]
member pwn 20:00:00:25:b5:aa:17:4f
!          [AMD-VMHost73-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost74 vsan 100
member pwn 20:00:00:25:b5:aa:17:46
!          [AMD-VMHost74-HBA0]
member pwn 20:00:00:25:b5:aa:17:47
!          [AMD-VMHost74-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost75 vsan 100
member pwn 20:00:00:25:b5:aa:17:48
!          [AMD-VMHost75-HBA0]
member pwn 20:00:00:25:b5:aa:17:49
!          [AMD-VMHost75-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost76 vsan 100
member pwn 20:00:00:25:b5:aa:17:4a
!          [AMD-VMHost76-HBA0]
member pwn 20:00:00:25:b5:aa:17:4b
!          [AMD-VMHost76-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost77 vsan 100
member pwn 20:00:00:25:b5:aa:17:4c
!          [AMD-VMHost77-HBA0]
member pwn 20:00:00:25:b5:aa:17:4d
!          [AMD-VMHost77-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
```



```
zoneset name FlashStack-VCC-CVD vsan 100
  member FlaskStack-VCC-CVD-WLHost01
  member FlaskStack-VCC-CVD-WLHost02
  member FlaskStack-VCC-CVD-WLHost03
  member FlaskStack-VCC-CVD-WLHost04
  member FlaskStack-VCC-CVD-WLHost05
  member FlaskStack-VCC-CVD-WLHost06
  member FlaskStack-VCC-CVD-WLHost07
  member FlaskStack-VCC-CVD-WLHost08
  member FlaskStack-VCC-CVD-WLHost09
  member FlaskStack-VCC-CVD-WLHost10
  member FlaskStack-VCC-CVD-WLHost11
  member FlaskStack-VCC-CVD-WLHost12
  member FlaskStack-VCC-CVD-WLHost13
  member FlaskStack-VCC-CVD-WLHost14
  member FlaskStack-VCC-CVD-WLHost15
  member FlaskStack-VCC-CVD-Infra01
  member FlaskStack-VCC-CVD-Infra02
  zoneset activate name FlashStack-VCC-CVD vsan 100
do clear zone database vsan 100
!Full Zone Database Section for vsan 100
zone name FlaskStack-VCC-CVD-WLHost01 vsan 100
  member pwn 20:00:00:25:b5:aa:17:00
  !           [VCC-WLHost01-HBA0]
  member pwn 20:00:00:25:b5:aa:17:01
  !           [VCC-WLHost01-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost02 vsan 100
  member pwn 20:00:00:25:b5:aa:17:02
  !           [VCC-WLHost02-HBA0]
  member pwn 20:00:00:25:b5:aa:17:03
  !           [VCC-WLHost02-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost03 vsan 100
  member pwn 20:00:00:25:b5:aa:17:04
  !           [VCC-WLHost03-HBA0]
  member pwn 20:00:00:25:b5:aa:17:05
  !           [VCC-WLHost03-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
```

```

!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost04 vsan 100
  member pwn 20:00:00:25:b5:aa:17:06
!           [VCC-WLHost04-HBA0]
  member pwn 20:00:00:25:b5:aa:17:07
!           [VCC-WLHost04-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost05 vsan 100
  member pwn 20:00:00:25:b5:aa:17:08
!           [VCC-WLHost05-HBA0]
  member pwn 20:00:00:25:b5:aa:17:09
!           [VCC-WLHost05-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost06 vsan 100
  member pwn 20:00:00:25:b5:aa:17:0a
!           [VCC-WLHost06-HBA0]
  member pwn 20:00:00:25:b5:aa:17:0b
!           [VCC-WLHost06-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost07 vsan 100
  member pwn 20:00:00:25:b5:aa:17:0c
!           [VCC-WLHost07-HBA0]
  member pwn 20:00:00:25:b5:aa:17:0d
!           [VCC-WLHost07-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost08 vsan 100
  member pwn 20:00:00:25:b5:aa:17:0e
!           [VCC-WLHost08-HBA0]
  member pwn 20:00:00:25:b5:aa:17:0f
!           [VCC-WLHost08-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost09 vsan 100

```

```
member pwnn 20:00:00:25:b5:aa:17:10
!          [VCC-WLHost09-HBA0]
member pwnn 20:00:00:25:b5:aa:17:11
!          [VCC-WLHost09-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost10 vsan 100
member pwnn 20:00:00:25:b5:aa:17:12
!          [VCC-WLHost10-HBA0]
member pwnn 20:00:00:25:b5:aa:17:13
!          [VCC-WLHost10-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost11 vsan 100
member pwnn 20:00:00:25:b5:aa:17:14
!          [VCC-WLHost11-HBA0]
member pwnn 20:00:00:25:b5:aa:17:15
!          [VCC-WLHost11-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost12 vsan 100
member pwnn 20:00:00:25:b5:aa:17:16
!          [VCC-WLHost12-HBA0]
member pwnn 20:00:00:25:b5:aa:17:17
!          [VCC-WLHost12-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost13 vsan 100
member pwnn 20:00:00:25:b5:aa:17:18
!          [VCC-WLHost13-HBA0]
member pwnn 20:00:00:25:b5:aa:17:19
!          [VCC-WLHost13-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost14 vsan 100
member pwnn 20:00:00:25:b5:aa:17:1a
!          [VCC-WLHost14-HBA0]
```

```
member pwn 20:00:00:25:b5:aa:17:1b
!          [VCC-WLHost14-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost15 vsan 100
member pwn 20:00:00:25:b5:aa:17:1c
!          [VCC-WLHost15-HBA0]
member pwn 20:00:00:25:b5:aa:17:1d
!          [VCC-WLHost15-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-Infra01 vsan 100
member pwn 20:00:00:25:b5:aa:17:1e
!          [VCC-Infra01-HBA0]
member pwn 20:00:00:25:b5:aa:17:1f
!          [VCC-Infra01-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost16 vsan 100
member pwn 20:00:00:25:b5:aa:17:20
!          [VCC-WLHost16-HBA0]
member pwn 20:00:00:25:b5:aa:17:21
!          [VCC-WLHost16-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost17 vsan 100
member pwn 20:00:00:25:b5:aa:17:22
!          [VCC-WLHost17-HBA0]
member pwn 20:00:00:25:b5:aa:17:23
!          [VCC-WLHost17-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost18 vsan 100
member pwn 20:00:00:25:b5:aa:17:24
!          [VCC-WLHost18-HBA0]
member pwn 20:00:00:25:b5:aa:17:25
!          [VCC-WLHost18-HBA2]
```

```
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost19 vsan 100
member pwnn 20:00:00:25:b5:aa:17:26
!           [VCC-WLHost19-HBA0]
member pwnn 20:00:00:25:b5:aa:17:27
!           [VCC-WLHost19-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost20 vsan 100
member pwnn 20:00:00:25:b5:aa:17:28
!           [VCC-WLHost20-HBA0]
member pwnn 20:00:00:25:b5:aa:17:29
!           [VCC-WLHost20-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost21 vsan 100
member pwnn 20:00:00:25:b5:aa:17:2a
!           [VCC-WLHost21-HBA0]
member pwnn 20:00:00:25:b5:aa:17:2b
!           [VCC-WLHost21-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost22 vsan 100
member pwnn 20:00:00:25:b5:aa:17:2c
!           [VCC-WLHost22-HBA0]
member pwnn 20:00:00:25:b5:aa:17:2d
!           [VCC-WLHost22-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost23 vsan 100
member pwnn 20:00:00:25:b5:aa:17:2e
!           [VCC-WLHost23-HBA0]
member pwnn 20:00:00:25:b5:aa:17:2f
!           [VCC-WLHost23-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
```

```
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost24 vsan 100
member pwnn 20:00:00:25:b5:aa:17:30
!          [VCC-WLHost24-HBA0]
member pwnn 20:00:00:25:b5:aa:17:31
!          [VCC-WLHost24-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost25 vsan 100
member pwnn 20:00:00:25:b5:aa:17:32
!          [VCC-WLHost25-HBA0]
member pwnn 20:00:00:25:b5:aa:17:33
!          [VCC-WLHost25-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost26 vsan 100
member pwnn 20:00:00:25:b5:aa:17:34
!          [VCC-WLHost26-HBA0]
member pwnn 20:00:00:25:b5:aa:17:35
!          [VCC-WLHost26-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost27 vsan 100
member pwnn 20:00:00:25:b5:aa:17:36
!          [VCC-WLHost27-HBA0]
member pwnn 20:00:00:25:b5:aa:17:37
!          [VCC-WLHost27-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost28 vsan 100
member pwnn 20:00:00:25:b5:aa:17:38
!          [VCC-WLHost28-HBA0]
member pwnn 20:00:00:25:b5:aa:17:39
!          [VCC-WLHost28-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!          [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!          [X70R3-CT1-FC0]
```

```
zone name FlaskStack-VCC-CVD-WLHost29 vsan 100
  member pwn 20:00:00:25:b5:aa:17:3a
  !          [VCC-WLHost29-HBA0]
  member pwn 20:00:00:25:b5:aa:17:3b
  !          [VCC-WLHost29-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !          [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-WLHost30 vsan 100
  member pwn 20:00:00:25:b5:aa:17:3c
  !          [VCC-WLHost30-HBA0]
  member pwn 20:00:00:25:b5:aa:17:3d
  !          [VCC-WLHost30-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !          [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !          [X70R3-CT1-FC0]
zone name FlaskStack-VCC-CVD-Infra02 vsan 100
  member pwn 20:00:00:25:b5:aa:17:3e
  !          [VCC-Infra02-HBA0]
  member pwn 20:00:00:25:b5:aa:17:3f
  !          [VCC-Infra02-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !          [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost70 vsan 100
  member pwn 20:00:00:25:b5:aa:17:40
  !          [AMD-VMHost70-HBA0]
  member pwn 20:00:00:25:b5:aa:17:41
  !          [AMD-VMHost70-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !          [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost71 vsan 100
  member pwn 20:00:00:25:b5:aa:17:42
  !          [AMD-VMHost71-HBA0]
  member pwn 20:00:00:25:b5:aa:17:43
  !          [AMD-VMHost71-HBA2]
  member pwn 52:4a:93:71:56:84:09:00
  !          [X70R3-CT0-FC0]
  member pwn 52:4a:93:71:56:84:09:10
  !          [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost72 vsan 100
  member pwn 20:00:00:25:b5:aa:17:44
```

```
!           [AMD-VMHost72-HBA0]
member pwn 20:00:00:25:b5:aa:17:45
!           [AMD-VMHost72-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost73 vsan 100
member pwn 20:00:00:25:b5:aa:17:4e
!           [AMD-VMHost73-HBA0]
member pwn 20:00:00:25:b5:aa:17:4f
!           [AMD-VMHost73-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost74 vsan 100
member pwn 20:00:00:25:b5:aa:17:46
!           [AMD-VMHost74-HBA0]
member pwn 20:00:00:25:b5:aa:17:47
!           [AMD-VMHost74-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost75 vsan 100
member pwn 20:00:00:25:b5:aa:17:48
!           [AMD-VMHost75-HBA0]
member pwn 20:00:00:25:b5:aa:17:49
!           [AMD-VMHost75-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost76 vsan 100
member pwn 20:00:00:25:b5:aa:17:4a
!           [AMD-VMHost76-HBA0]
member pwn 20:00:00:25:b5:aa:17:4b
!           [AMD-VMHost76-HBA2]
member pwn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zone name FlaskStack-AMD-VMHost77 vsan 100
member pwn 20:00:00:25:b5:aa:17:4c
!           [AMD-VMHost77-HBA0]
member pwn 20:00:00:25:b5:aa:17:4d
```



```
!           [AMD-VMHost77-HBA2]
member pwnn 52:4a:93:71:56:84:09:00
!           [X70R3-CT0-FC0]
member pwnn 52:4a:93:71:56:84:09:10
!           [X70R3-CT1-FC0]
zoneset name FlashStack-VCC-CVD vsan 100
member FlaskStack-VCC-CVD-WLHost01
member FlaskStack-VCC-CVD-WLHost02
member FlaskStack-VCC-CVD-WLHost03
member FlaskStack-VCC-CVD-WLHost04
member FlaskStack-VCC-CVD-WLHost05
member FlaskStack-VCC-CVD-WLHost06
member FlaskStack-VCC-CVD-WLHost07
member FlaskStack-VCC-CVD-WLHost08
member FlaskStack-VCC-CVD-WLHost09
member FlaskStack-VCC-CVD-WLHost10
member FlaskStack-VCC-CVD-WLHost11
member FlaskStack-VCC-CVD-WLHost12
member FlaskStack-VCC-CVD-WLHost13
member FlaskStack-VCC-CVD-WLHost14
member FlaskStack-VCC-CVD-WLHost15
member FlaskStack-VCC-CVD-Infra01
member FlaskStack-VCC-CVD-Infra02
member FlaskStack-AMD-VMHost70
member FlaskStack-AMD-VMHost71
interface mgmt0
ip address 10.29.164.238 255.255.255.0
vsan database
vsan 400 interface fc1/1
vsan 400 interface fc1/2
vsan 400 interface fc1/3
vsan 400 interface fc1/4
vsan 400 interface fc1/5
vsan 400 interface fc1/6
vsan 400 interface fc1/7
vsan 400 interface fc1/8
vsan 100 interface fc1/9
vsan 100 interface fc1/10
vsan 100 interface fc1/11
vsan 100 interface fc1/12
vsan 100 interface fc1/13
vsan 100 interface fc1/14
vsan 100 interface fc1/15
vsan 100 interface fc1/16
clock timezone PST 0 0
clock summer-time PDT 2 Sun Mar 02:00 1 Sun Nov 02:00 60
switchname ADD16-MDS-A
```

```
cli alias name autozone source sys/autozone.py
line console
line vty
boot kickstart bootflash:/m9100-s6ek9-kickstart-mz.8.3.1.bin
boot system bootflash:/m9100-s6ek9-mz.8.3.1.bin
interface fc1/4
    switchport speed auto
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/4
interface fc1/1
    port-license acquire
    no shutdown
interface fc1/2
    port-license acquire
    no shutdown
interface fc1/3
    port-license acquire
    no shutdown
interface fc1/4
    port-license acquire
    no shutdown
interface fc1/5
    no port-license
interface fc1/6
    no port-license
interface fc1/7
    no port-license
interface fc1/8
    no port-license
interface fc1/9
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
```

```
no shutdown
interface fcl/10
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fcl/11
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fcl/12
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fcl/13
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fcl/14
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fcl/15
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fcl/16
    switchport trunk allowed vsan 100
    switchport trunk mode off
    port-license acquire
    no shutdown
ip default-gateway 10.29.164.1
```

## Cisco MDS 9132T-B Configuration

```
version 8.4(2d)
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 $5$1qs42bIH$hp2kMO3FA/4Zzg6EekVHWpA81A7Mc/kBsFZVU8q1uU7 role
network-admin
ip domain-lookup
ip host ADD16-MDS-B 10.29.164.239
aaa group server radius radius
snmp-server user admin network-admin auth md5 0x6fa97f514b0cdf3638e31dfd0bd19c71 priv
0x6fa97f514b0cdf3638e31dfd0bd19c71 localizedkey
snmp-server host 10.155.160.97 traps version 2c public udp-port 1164
snmp-server host 10.24.66.169 traps version 2c public udp-port 1164
snmp-server host 10.24.72.119 traps version 2c public udp-port 1166
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
ntp server 10.81.254.131
ntp server 10.81.254.202
vsan database
  vsan 101 name "FlashStack-VCC-CVD-Fabric-B"
device-alias database
  device-alias name X70R3-CT0-FC2 pwnn 52:4a:93:71:56:84:09:02
  device-alias name X70R3-CT1-FC2 pwnn 52:4a:93:71:56:84:09:12
  device-alias name VCC-Infra01-HBA1 pwnn 20:00:00:25:b5:bb:17:1e
  device-alias name VCC-Infra01-HBA3 pwnn 20:00:00:25:b5:bb:17:1f
  device-alias name VCC-Infra02-HBA1 pwnn 20:00:00:25:b5:bb:17:3e
  device-alias name VCC-Infra02-HBA3 pwnn 20:00:00:25:b5:bb:17:3f
  device-alias name VCC-WLHost01-HBA1 pwnn 20:00:00:25:b5:bb:17:00
  device-alias name VCC-WLHost01-HBA3 pwnn 20:00:00:25:b5:bb:17:01
  device-alias name VCC-WLHost02-HBA1 pwnn 20:00:00:25:b5:bb:17:02
  device-alias name VCC-WLHost02-HBA3 pwnn 20:00:00:25:b5:bb:17:03
  device-alias name VCC-WLHost03-HBA1 pwnn 20:00:00:25:b5:bb:17:04
  device-alias name VCC-WLHost03-HBA3 pwnn 20:00:00:25:b5:bb:17:05
  device-alias name VCC-WLHost04-HBA1 pwnn 20:00:00:25:b5:bb:17:06
  device-alias name VCC-WLHost04-HBA3 pwnn 20:00:00:25:b5:bb:17:07
  device-alias name VCC-WLHost05-HBA1 pwnn 20:00:00:25:b5:bb:17:08
  device-alias name VCC-WLHost05-HBA3 pwnn 20:00:00:25:b5:bb:17:09
  device-alias name VCC-WLHost06-HBA1 pwnn 20:00:00:25:b5:bb:17:0a
  device-alias name VCC-WLHost06-HBA3 pwnn 20:00:00:25:b5:bb:17:0b
  device-alias name VCC-WLHost07-HBA1 pwnn 20:00:00:25:b5:bb:17:0c
  device-alias name VCC-WLHost07-HBA3 pwnn 20:00:00:25:b5:bb:17:0d
  device-alias name VCC-WLHost08-HBA1 pwnn 20:00:00:25:b5:bb:17:0e
  device-alias name VCC-WLHost08-HBA3 pwnn 20:00:00:25:b5:bb:17:0f
```

```
device-alias name VCC-WLHost09-HBA1 pwn 20:00:00:25:b5:bb:17:10
device-alias name VCC-WLHost09-HBA3 pwn 20:00:00:25:b5:bb:17:11
device-alias name VCC-WLHost10-HBA1 pwn 20:00:00:25:b5:bb:17:12
device-alias name VCC-WLHost10-HBA3 pwn 20:00:00:25:b5:bb:17:13
device-alias name VCC-WLHost11-HBA1 pwn 20:00:00:25:b5:bb:17:14
device-alias name VCC-WLHost11-HBA3 pwn 20:00:00:25:b5:bb:17:15
device-alias name VCC-WLHost12-HBA1 pwn 20:00:00:25:b5:bb:17:16
device-alias name VCC-WLHost12-HBA3 pwn 20:00:00:25:b5:bb:17:17
device-alias name VCC-WLHost13-HBA1 pwn 20:00:00:25:b5:bb:17:18
device-alias name VCC-WLHost13-HBA3 pwn 20:00:00:25:b5:bb:17:19
device-alias name VCC-WLHost14-HBA1 pwn 20:00:00:25:b5:bb:17:1a
device-alias name VCC-WLHost14-HBA3 pwn 20:00:00:25:b5:bb:17:1b
device-alias name VCC-WLHost15-HBA1 pwn 20:00:00:25:b5:bb:17:1c
device-alias name VCC-WLHost15-HBA3 pwn 20:00:00:25:b5:bb:17:1d
device-alias name VCC-WLHost16-HBA1 pwn 20:00:00:25:b5:bb:17:20
device-alias commit
fcdomain fcid database
vsan 101 wwn 20:03:00:de:fb:90:a4:40 fcid 0xc40000 dynamic
vsan 101 wwn 52:4a:93:75:dd:91:0a:17 fcid 0xc40020 dynamic
! [X70-CT1-FC9]
vsan 101 wwn 52:4a:93:75:dd:91:0a:07 fcid 0xc40040 dynamic
! [X70-CT0-FC9]
vsan 101 wwn 52:4a:93:75:dd:91:0a:16 fcid 0xc40021 dynamic
vsan 101 wwn 52:4a:93:75:dd:91:0a:13 fcid 0xc40041 dynamic
! [X70-CT1-FC3]
vsan 101 wwn 20:00:00:25:b5:bb:17:3e fcid 0xc40060 dynamic
! [VCC-Infra02-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:07 fcid 0xc40061 dynamic
! [VCC-WLHost04-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:3c fcid 0xc40062 dynamic
! [VCC-WLHost30-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:11 fcid 0xc40063 dynamic
! [VCC-WLHost09-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:01 fcid 0xc40064 dynamic
! [VCC-WLHost01-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:00 fcid 0xc40065 dynamic
! [VCC-WLHost01-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:13 fcid 0xc40066 dynamic
! [VCC-WLHost10-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:04 fcid 0xc40067 dynamic
! [VCC-WLHost03-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:17 fcid 0xc40068 dynamic
! [VCC-WLHost12-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:16 fcid 0xc40069 dynamic
! [VCC-WLHost12-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:30 fcid 0xc4006a dynamic
! [VCC-WLHost24-HBA1]
```

```
vsan 101 wwn 20:00:00:25:b5:bb:17:21 fcid 0xc4006b dynamic
!          [VCC-WLHost16-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:1f fcid 0xc4006c dynamic
!          [VCC-Infra01-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:1a fcid 0xc4006d dynamic
!          [VCC-WLHost14-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:3f fcid 0xc4006e dynamic
!          [VCC-Infra02-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:0a fcid 0xc4006f dynamic
!          [VCC-WLHost06-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:38 fcid 0xc40070 dynamic
!          [VCC-WLHost28-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:19 fcid 0xc40071 dynamic
!          [VCC-WLHost13-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:22 fcid 0xc40072 dynamic
!          [VCC-WLHost17-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:2f fcid 0xc40073 dynamic
!          [VCC-WLHost23-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:1b fcid 0xc40074 dynamic
!          [VCC-WLHost14-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:3b fcid 0xc40075 dynamic
!          [VCC-WLHost29-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:2a fcid 0xc40076 dynamic
!          [VCC-WLHost21-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:29 fcid 0xc40077 dynamic
!          [VCC-WLHost20-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:1c fcid 0xc40078 dynamic
!          [VCC-WLHost15-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:0b fcid 0xc40079 dynamic
!          [VCC-WLHost06-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:0d fcid 0xc4007a dynamic
!          [VCC-WLHost07-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:37 fcid 0xc4007b dynamic
!          [VCC-WLHost27-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:31 fcid 0xc4007c dynamic
!          [VCC-WLHost24-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:08 fcid 0xc4007d dynamic
!          [VCC-WLHost05-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:10 fcid 0xc4007e dynamic
!          [VCC-WLHost09-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:34 fcid 0xc4007f dynamic
!          [VCC-WLHost26-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:25 fcid 0xc40080 dynamic
!          [VCC-WLHost18-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:3d fcid 0xc40081 dynamic
!          [VCC-WLHost30-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:15 fcid 0xc40082 dynamic
```

```
!           [VCC-WLHost11-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:23 fcid 0xc40083 dynamic
!           [VCC-WLHost17-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:3a fcid 0xc40084 dynamic
!           [VCC-WLHost29-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:28 fcid 0xc40085 dynamic
!           [VCC-WLHost20-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:32 fcid 0xc40086 dynamic
!           [VCC-WLHost25-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:0f fcid 0xc40087 dynamic
!           [VCC-WLHost08-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:0c fcid 0xc40088 dynamic
!           [VCC-WLHost07-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:2e fcid 0xc40089 dynamic
!           [VCC-WLHost23-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:03 fcid 0xc4008a dynamic
!           [VCC-WLHost02-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:02 fcid 0xc4008b dynamic
!           [VCC-WLHost02-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:2b fcid 0xc4008c dynamic
!           [VCC-WLHost21-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:35 fcid 0xc4008d dynamic
!           [VCC-WLHost26-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:2c fcid 0xc4008e dynamic
!           [VCC-WLHost22-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:27 fcid 0xc4008f dynamic
!           [VCC-WLHost19-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:18 fcid 0xc40090 dynamic
!           [VCC-WLHost13-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:14 fcid 0xc40091 dynamic
!           [VCC-WLHost11-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:0e fcid 0xc40092 dynamic
!           [VCC-WLHost08-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:1e fcid 0xc40093 dynamic
!           [VCC-Infra01-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:06 fcid 0xc40094 dynamic
!           [VCC-WLHost04-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:09 fcid 0xc40095 dynamic
!           [VCC-WLHost05-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:26 fcid 0xc40096 dynamic
!           [VCC-WLHost19-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:24 fcid 0xc40097 dynamic
!           [VCC-WLHost18-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:20 fcid 0xc40098 dynamic
!           [VCC-WLHost16-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:1d fcid 0xc40099 dynamic
!           [VCC-WLHost15-HBA3]
```

```
vsan 101 wwn 20:00:00:25:b5:bb:17:33 fcid 0xc4009a dynamic
! [VCC-WLHost25-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:36 fcid 0xc4009b dynamic
! [VCC-WLHost27-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:39 fcid 0xc4009c dynamic
! [VCC-WLHost28-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:2d fcid 0xc4009d dynamic
! [VCC-WLHost22-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:12 fcid 0xc4009e dynamic
! [VCC-WLHost10-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:05 fcid 0xc4009f dynamic
! [VCC-WLHost03-HBA3]
vsan 101 wwn 20:02:00:de:fb:90:a4:40 fcid 0xc400a0 dynamic
vsan 101 wwn 20:01:00:de:fb:90:a4:40 fcid 0xc400c0 dynamic
vsan 101 wwn 20:04:00:de:fb:90:a4:40 fcid 0xc400e0 dynamic
vsan 101 wwn 52:4a:93:75:dd:91:0a:00 fcid 0xc40022 dynamic
vsan 101 wwn 52:4a:93:75:dd:91:0a:12 fcid 0xc40042 dynamic
vsan 101 wwn 52:4a:93:75:dd:91:0a:11 fcid 0xc40023 dynamic
! [X70-CT1-FC1]
vsan 101 wwn 20:01:00:3a:9c:a4:fd:20 fcid 0xc400c1 dynamic
vsan 101 wwn 20:02:00:3a:9c:a4:fd:20 fcid 0xc400a1 dynamic
vsan 101 wwn 20:03:00:3a:9c:a4:fd:20 fcid 0xc40100 dynamic
vsan 101 wwn 20:04:00:3a:9c:a4:fd:20 fcid 0xc400e1 dynamic
vsan 101 wwn 52:4a:93:75:dd:91:0a:01 fcid 0xc40043 dynamic
! [X70-CT0-FC1]
vsan 101 wwn 52:4a:93:71:56:84:09:02 fcid 0xc40044 dynamic
! [X70R3-CT0-FC2]
vsan 101 wwn 52:4a:93:71:56:84:09:00 fcid 0xc40024 dynamic
vsan 101 wwn 52:4a:93:71:56:84:09:12 fcid 0xc40045 dynamic
! [X70R3-CT1-FC2]
vsan 101 wwn 20:00:00:25:b5:bb:17:40 fcid 0xc400c2 dynamic
! [AMD-VMHost70-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:41 fcid 0xc400a2 dynamic
! [AMD-VMHost70-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:44 fcid 0xc400c3 dynamic
! [AMD-VMHost72-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:45 fcid 0xc400a3 dynamic
! [AMD-VMHost72-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:4e fcid 0xc400c4 dynamic
! [AMD-VMHost73-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:4f fcid 0xc400a4 dynamic
! [AMD-VMHost73-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:42 fcid 0xc400c5 dynamic
! [AMD-VMHost71-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:43 fcid 0xc400a5 dynamic
! [AMD-VMHost71-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:46 fcid 0xc400c6 dynamic
```



```

!           [AMD-VMHost74-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:47 fcid 0xc400a6 dynamic
!           [AMD-VMHost74-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:48 fcid 0xc400c7 dynamic
!           [AMD-VMHost75-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:49 fcid 0xc400a7 dynamic
!           [AMD-VMHost75-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:4a fcid 0xc400c8 dynamic
!           [AMD-VMHost76-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:4b fcid 0xc400a8 dynamic
!           [AMD-VMHost76-HBA3]
vsan 101 wwn 20:00:00:25:b5:bb:17:4c fcid 0xc400c9 dynamic
!           [AMD-VMHost77-HBA1]
vsan 101 wwn 20:00:00:25:b5:bb:17:4d fcid 0xc400a9 dynamic
!           [AMD-VMHost77-HBA3]
!Active Zone Database Section for vsan 101
zone name FlaskStack-VCC-CVD-WLHost01 vsan 101
  member pwn 20:00:00:25:b5:bb:17:00
  !           [VCC-WLHost01-HBA1]
  member pwn 20:00:00:25:b5:bb:17:01
  !           [VCC-WLHost01-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
  !           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
  !           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost02 vsan 101
  member pwn 20:00:00:25:b5:bb:17:02
  !           [VCC-WLHost02-HBA1]
  member pwn 20:00:00:25:b5:bb:17:03
  !           [VCC-WLHost02-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
  !           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
  !           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost03 vsan 101
  member pwn 20:00:00:25:b5:bb:17:04
  !           [VCC-WLHost03-HBA1]
  member pwn 20:00:00:25:b5:bb:17:05
  !           [VCC-WLHost03-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
  !           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
  !           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost04 vsan 101
  member pwn 20:00:00:25:b5:bb:17:06
  !           [VCC-WLHost04-HBA1]
  member pwn 20:00:00:25:b5:bb:17:07

```

```
!           [VCC-WLHost04-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost05 vsan 101
member pwn 20:00:00:25:b5:bb:17:08
!           [VCC-WLHost05-HBA1]
member pwn 20:00:00:25:b5:bb:17:09
!           [VCC-WLHost05-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost06 vsan 101
member pwn 20:00:00:25:b5:bb:17:0a
!           [VCC-WLHost06-HBA1]
member pwn 20:00:00:25:b5:bb:17:0b
!           [VCC-WLHost06-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost07 vsan 101
member pwn 20:00:00:25:b5:bb:17:0c
!           [VCC-WLHost07-HBA1]
member pwn 20:00:00:25:b5:bb:17:0d
!           [VCC-WLHost07-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost08 vsan 101
member pwn 20:00:00:25:b5:bb:17:0e
!           [VCC-WLHost08-HBA1]
member pwn 20:00:00:25:b5:bb:17:0f
!           [VCC-WLHost08-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost09 vsan 101
member pwn 20:00:00:25:b5:bb:17:10
!           [VCC-WLHost09-HBA1]
member pwn 20:00:00:25:b5:bb:17:11
!           [VCC-WLHost09-HBA3]
member pwn 52:4a:93:71:56:84:09:02
```

```
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost10 vsan 101
member pwn 20:00:00:25:b5:bb:17:12
!           [VCC-WLHost10-HBA1]
member pwn 20:00:00:25:b5:bb:17:13
!           [VCC-WLHost10-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost11 vsan 101
member pwn 20:00:00:25:b5:bb:17:14
!           [VCC-WLHost11-HBA1]
member pwn 20:00:00:25:b5:bb:17:15
!           [VCC-WLHost11-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost12 vsan 101
member pwn 20:00:00:25:b5:bb:17:16
!           [VCC-WLHost12-HBA1]
member pwn 20:00:00:25:b5:bb:17:17
!           [VCC-WLHost12-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost13 vsan 101
member pwn 20:00:00:25:b5:bb:17:18
!           [VCC-WLHost13-HBA1]
member pwn 20:00:00:25:b5:bb:17:19
!           [VCC-WLHost13-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost14 vsan 101
member pwn 20:00:00:25:b5:bb:17:1a
!           [VCC-WLHost14-HBA1]
member pwn 20:00:00:25:b5:bb:17:1b
!           [VCC-WLHost14-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
```

```
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost15 vsan 101
  member pwn 20:00:00:25:b5:bb:17:1c
!           [VCC-WLHost15-HBA1]
  member pwn 20:00:00:25:b5:bb:17:1d
!           [VCC-WLHost15-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-Infra01 vsan 101
  member pwn 20:00:00:25:b5:bb:17:1e
!           [VCC-Infra01-HBA1]
  member pwn 20:00:00:25:b5:bb:17:1f
!           [VCC-Infra01-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost16 vsan 101
  member pwn 20:00:00:25:b5:bb:17:20
!           [VCC-WLHost16-HBA1]
  member pwn 20:00:00:25:b5:bb:17:21
!           [VCC-WLHost16-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost17 vsan 101
  member pwn 20:00:00:25:b5:bb:17:22
!           [VCC-WLHost17-HBA1]
  member pwn 20:00:00:25:b5:bb:17:23
!           [VCC-WLHost17-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost18 vsan 101
  member pwn 20:00:00:25:b5:bb:17:24
!           [VCC-WLHost18-HBA1]
  member pwn 20:00:00:25:b5:bb:17:25
!           [VCC-WLHost18-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost19 vsan 101
```

```
member pwn 20:00:00:25:b5:bb:17:26
!          [VCC-WLHost19-HBA1]
member pwn 20:00:00:25:b5:bb:17:27
!          [VCC-WLHost19-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost20 vsan 101
member pwn 20:00:00:25:b5:bb:17:28
!          [VCC-WLHost20-HBA1]
member pwn 20:00:00:25:b5:bb:17:29
!          [VCC-WLHost20-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost21 vsan 101
member pwn 20:00:00:25:b5:bb:17:2a
!          [VCC-WLHost21-HBA1]
member pwn 20:00:00:25:b5:bb:17:2b
!          [VCC-WLHost21-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost22 vsan 101
member pwn 20:00:00:25:b5:bb:17:2c
!          [VCC-WLHost22-HBA1]
member pwn 20:00:00:25:b5:bb:17:2d
!          [VCC-WLHost22-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost23 vsan 101
member pwn 20:00:00:25:b5:bb:17:2e
!          [VCC-WLHost23-HBA1]
member pwn 20:00:00:25:b5:bb:17:2f
!          [VCC-WLHost23-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost24 vsan 101
member pwn 20:00:00:25:b5:bb:17:30
!          [VCC-WLHost24-HBA1]
```

```
member pwn 20:00:00:25:b5:bb:17:31
!          [VCC-WLHost24-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost25 vsan 101
member pwn 20:00:00:25:b5:bb:17:32
!          [VCC-WLHost25-HBA1]
member pwn 20:00:00:25:b5:bb:17:33
!          [VCC-WLHost25-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost26 vsan 101
member pwn 20:00:00:25:b5:bb:17:34
!          [VCC-WLHost26-HBA1]
member pwn 20:00:00:25:b5:bb:17:35
!          [VCC-WLHost26-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost27 vsan 101
member pwn 20:00:00:25:b5:bb:17:36
!          [VCC-WLHost27-HBA1]
member pwn 20:00:00:25:b5:bb:17:37
!          [VCC-WLHost27-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost28 vsan 101
member pwn 20:00:00:25:b5:bb:17:38
!          [VCC-WLHost28-HBA1]
member pwn 20:00:00:25:b5:bb:17:39
!          [VCC-WLHost28-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost29 vsan 101
member pwn 20:00:00:25:b5:bb:17:3a
!          [VCC-WLHost29-HBA1]
member pwn 20:00:00:25:b5:bb:17:3b
!          [VCC-WLHost29-HBA3]
```

```
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost30 vsan 101
member pwnn 20:00:00:25:b5:bb:17:3c
!           [VCC-WLHost30-HBA1]
member pwnn 20:00:00:25:b5:bb:17:3d
!           [VCC-WLHost30-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-Infra02 vsan 101
member pwnn 20:00:00:25:b5:bb:17:3e
!           [VCC-Infra02-HBA1]
member pwnn 20:00:00:25:b5:bb:17:3f
!           [VCC-Infra02-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost70 vsan 101
member pwnn 20:00:00:25:b5:bb:17:40
!           [AMD-VMHost70-HBA1]
member pwnn 20:00:00:25:b5:bb:17:41
!           [AMD-VMHost70-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost71 vsan 101
member pwnn 20:00:00:25:b5:bb:17:42
!           [AMD-VMHost71-HBA1]
member pwnn 20:00:00:25:b5:bb:17:43
!           [AMD-VMHost71-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost72 vsan 101
member pwnn 20:00:00:25:b5:bb:17:44
!           [AMD-VMHost72-HBA1]
member pwnn 20:00:00:25:b5:bb:17:45
!           [AMD-VMHost72-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
```

```
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost73 vsan 101
member pwn 20:00:00:25:b5:bb:17:4e
!          [AMD-VMHost73-HBA1]
member pwn 20:00:00:25:b5:bb:17:4f
!          [AMD-VMHost73-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost74 vsan 101
member pwn 20:00:00:25:b5:bb:17:46
!          [AMD-VMHost74-HBA1]
member pwn 20:00:00:25:b5:bb:17:47
!          [AMD-VMHost74-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost75 vsan 101
member pwn 20:00:00:25:b5:bb:17:48
!          [AMD-VMHost75-HBA1]
member pwn 20:00:00:25:b5:bb:17:49
!          [AMD-VMHost75-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost76 vsan 101
member pwn 20:00:00:25:b5:bb:17:4a
!          [AMD-VMHost76-HBA1]
member pwn 20:00:00:25:b5:bb:17:4b
!          [AMD-VMHost76-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost77 vsan 101
member pwn 20:00:00:25:b5:bb:17:4c
!          [AMD-VMHost77-HBA1]
member pwn 20:00:00:25:b5:bb:17:4d
!          [AMD-VMHost77-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
```



```
zoneset name FlashStack-VCC-CVD vsan 101
  member FlaskStack-VCC-CVD-WLHost01
  member FlaskStack-VCC-CVD-WLHost02
  member FlaskStack-VCC-CVD-WLHost03
  member FlaskStack-VCC-CVD-WLHost04
  member FlaskStack-VCC-CVD-WLHost05
  member FlaskStack-VCC-CVD-WLHost06
  member FlaskStack-VCC-CVD-WLHost07
  member FlaskStack-VCC-CVD-WLHost08
  member FlaskStack-VCC-CVD-WLHost09
  member FlaskStack-VCC-CVD-WLHost10
  member FlaskStack-VCC-CVD-WLHost11
  member FlaskStack-VCC-CVD-WLHost12
  member FlaskStack-VCC-CVD-WLHost13
  member FlaskStack-VCC-CVD-WLHost14
  member FlaskStack-VCC-CVD-WLHost15
  member FlaskStack-VCC-CVD-Infra01
  member FlaskStack-VCC-CVD-Infra02
  member FlaskStack-AMD-VMHost70
  member FlaskStack-AMD-VMHost71
zoneset activate name FlashStack-VCC-CVD vsan 101
do clear zone database vsan 101
!Full Zone Database Section for vsan 101
zone name FlaskStack-VCC-CVD-WLHost01 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:00
  !          [VCC-WLHost01-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:01
  !          [VCC-WLHost01-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost02 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:02
  !          [VCC-WLHost02-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:03
  !          [VCC-WLHost02-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost03 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:04
  !          [VCC-WLHost03-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:05
  !          [VCC-WLHost03-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
```

```
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost04 vsan 101
member pwn 20:00:00:25:b5:bb:17:06
!           [VCC-WLHost04-HBA1]
member pwn 20:00:00:25:b5:bb:17:07
!           [VCC-WLHost04-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost05 vsan 101
member pwn 20:00:00:25:b5:bb:17:08
!           [VCC-WLHost05-HBA1]
member pwn 20:00:00:25:b5:bb:17:09
!           [VCC-WLHost05-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost06 vsan 101
member pwn 20:00:00:25:b5:bb:17:0a
!           [VCC-WLHost06-HBA1]
member pwn 20:00:00:25:b5:bb:17:0b
!           [VCC-WLHost06-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost07 vsan 101
member pwn 20:00:00:25:b5:bb:17:0c
!           [VCC-WLHost07-HBA1]
member pwn 20:00:00:25:b5:bb:17:0d
!           [VCC-WLHost07-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost08 vsan 101
member pwn 20:00:00:25:b5:bb:17:0e
!           [VCC-WLHost08-HBA1]
member pwn 20:00:00:25:b5:bb:17:0f
!           [VCC-WLHost08-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
```

```
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost09 vsan 101
  member pwn 20:00:00:25:b5:bb:17:10
!           [VCC-WLHost09-HBA1]
  member pwn 20:00:00:25:b5:bb:17:11
!           [VCC-WLHost09-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost10 vsan 101
  member pwn 20:00:00:25:b5:bb:17:12
!           [VCC-WLHost10-HBA1]
  member pwn 20:00:00:25:b5:bb:17:13
!           [VCC-WLHost10-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost11 vsan 101
  member pwn 20:00:00:25:b5:bb:17:14
!           [VCC-WLHost11-HBA1]
  member pwn 20:00:00:25:b5:bb:17:15
!           [VCC-WLHost11-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost12 vsan 101
  member pwn 20:00:00:25:b5:bb:17:16
!           [VCC-WLHost12-HBA1]
  member pwn 20:00:00:25:b5:bb:17:17
!           [VCC-WLHost12-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost13 vsan 101
  member pwn 20:00:00:25:b5:bb:17:18
!           [VCC-WLHost13-HBA1]
  member pwn 20:00:00:25:b5:bb:17:19
!           [VCC-WLHost13-HBA3]
  member pwn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
  member pwn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost14 vsan 101
```

```
member pwn 20:00:00:25:b5:bb:17:1a
!          [VCC-WLHost14-HBA1]
member pwn 20:00:00:25:b5:bb:17:1b
!          [VCC-WLHost14-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost15 vsan 101
member pwn 20:00:00:25:b5:bb:17:1c
!          [VCC-WLHost15-HBA1]
member pwn 20:00:00:25:b5:bb:17:1d
!          [VCC-WLHost15-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-Infra01 vsan 101
member pwn 20:00:00:25:b5:bb:17:1e
!          [VCC-Infra01-HBA1]
member pwn 20:00:00:25:b5:bb:17:1f
!          [VCC-Infra01-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost16 vsan 101
member pwn 20:00:00:25:b5:bb:17:20
!          [VCC-WLHost16-HBA1]
member pwn 20:00:00:25:b5:bb:17:21
!          [VCC-WLHost16-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost17 vsan 101
member pwn 20:00:00:25:b5:bb:17:22
!          [VCC-WLHost17-HBA1]
member pwn 20:00:00:25:b5:bb:17:23
!          [VCC-WLHost17-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost18 vsan 101
member pwn 20:00:00:25:b5:bb:17:24
!          [VCC-WLHost18-HBA1]
```

```
member pwn 20:00:00:25:b5:bb:17:25
!          [VCC-WLHost18-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost19 vsan 101
member pwn 20:00:00:25:b5:bb:17:26
!          [VCC-WLHost19-HBA1]
member pwn 20:00:00:25:b5:bb:17:27
!          [VCC-WLHost19-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost20 vsan 101
member pwn 20:00:00:25:b5:bb:17:28
!          [VCC-WLHost20-HBA1]
member pwn 20:00:00:25:b5:bb:17:29
!          [VCC-WLHost20-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost21 vsan 101
member pwn 20:00:00:25:b5:bb:17:2a
!          [VCC-WLHost21-HBA1]
member pwn 20:00:00:25:b5:bb:17:2b
!          [VCC-WLHost21-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost22 vsan 101
member pwn 20:00:00:25:b5:bb:17:2c
!          [VCC-WLHost22-HBA1]
member pwn 20:00:00:25:b5:bb:17:2d
!          [VCC-WLHost22-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost23 vsan 101
member pwn 20:00:00:25:b5:bb:17:2e
!          [VCC-WLHost23-HBA1]
member pwn 20:00:00:25:b5:bb:17:2f
!          [VCC-WLHost23-HBA3]
```

```
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost24 vsan 101
member pwnn 20:00:00:25:b5:bb:17:30
!           [VCC-WLHost24-HBA1]
member pwnn 20:00:00:25:b5:bb:17:31
!           [VCC-WLHost24-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost25 vsan 101
member pwnn 20:00:00:25:b5:bb:17:32
!           [VCC-WLHost25-HBA1]
member pwnn 20:00:00:25:b5:bb:17:33
!           [VCC-WLHost25-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost26 vsan 101
member pwnn 20:00:00:25:b5:bb:17:34
!           [VCC-WLHost26-HBA1]
member pwnn 20:00:00:25:b5:bb:17:35
!           [VCC-WLHost26-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost27 vsan 101
member pwnn 20:00:00:25:b5:bb:17:36
!           [VCC-WLHost27-HBA1]
member pwnn 20:00:00:25:b5:bb:17:37
!           [VCC-WLHost27-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost28 vsan 101
member pwnn 20:00:00:25:b5:bb:17:38
!           [VCC-WLHost28-HBA1]
member pwnn 20:00:00:25:b5:bb:17:39
!           [VCC-WLHost28-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
```

```
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost29 vsan 101
member pwn 20:00:00:25:b5:bb:17:3a
!          [VCC-WLHost29-HBA1]
member pwn 20:00:00:25:b5:bb:17:3b
!          [VCC-WLHost29-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-WLHost30 vsan 101
member pwn 20:00:00:25:b5:bb:17:3c
!          [VCC-WLHost30-HBA1]
member pwn 20:00:00:25:b5:bb:17:3d
!          [VCC-WLHost30-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-VCC-CVD-Infra02 vsan 101
member pwn 20:00:00:25:b5:bb:17:3e
!          [VCC-Infra02-HBA1]
member pwn 20:00:00:25:b5:bb:17:3f
!          [VCC-Infra02-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost70 vsan 101
member pwn 20:00:00:25:b5:bb:17:40
!          [AMD-VMHost70-HBA1]
member pwn 20:00:00:25:b5:bb:17:41
!          [AMD-VMHost70-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost71 vsan 101
member pwn 20:00:00:25:b5:bb:17:42
!          [AMD-VMHost71-HBA1]
member pwn 20:00:00:25:b5:bb:17:43
!          [AMD-VMHost71-HBA3]
member pwn 52:4a:93:71:56:84:09:02
!          [X70R3-CT0-FC2]
member pwn 52:4a:93:71:56:84:09:12
!          [X70R3-CT1-FC2]
```

```
zone name FlaskStack-AMD-VMHost72 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:44
  !          [AMD-VMHost72-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:45
  !          [AMD-VMHost72-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost73 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:4e
  !          [AMD-VMHost73-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:4f
  !          [AMD-VMHost73-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost74 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:46
  !          [AMD-VMHost74-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:47
  !          [AMD-VMHost74-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost75 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:48
  !          [AMD-VMHost75-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:49
  !          [AMD-VMHost75-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost76 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:4a
  !          [AMD-VMHost76-HBA1]
  member pwnn 20:00:00:25:b5:bb:17:4b
  !          [AMD-VMHost76-HBA3]
  member pwnn 52:4a:93:71:56:84:09:02
  !          [X70R3-CT0-FC2]
  member pwnn 52:4a:93:71:56:84:09:12
  !          [X70R3-CT1-FC2]
zone name FlaskStack-AMD-VMHost77 vsan 101
  member pwnn 20:00:00:25:b5:bb:17:4c
```



```

!           [AMD-VMHost77-HBA1]
member pwnn 20:00:00:25:b5:bb:17:4d
!           [AMD-VMHost77-HBA3]
member pwnn 52:4a:93:71:56:84:09:02
!           [X70R3-CT0-FC2]
member pwnn 52:4a:93:71:56:84:09:12
!           [X70R3-CT1-FC2]
zoneset name FlashStack-VCC-CVD vsan 101
  member FlaskStack-VCC-CVD-WLHost01
  member FlaskStack-VCC-CVD-WLHost02
  member FlaskStack-VCC-CVD-WLHost03
  member FlaskStack-VCC-CVD-WLHost04
  member FlaskStack-VCC-CVD-WLHost05
  member FlaskStack-VCC-CVD-WLHost06
  member FlaskStack-VCC-CVD-WLHost07
  member FlaskStack-VCC-CVD-WLHost08
  member FlaskStack-VCC-CVD-WLHost09
  member FlaskStack-VCC-CVD-WLHost10
  member FlaskStack-VCC-CVD-WLHost11
  member FlaskStack-VCC-CVD-WLHost12
  member FlaskStack-VCC-CVD-WLHost13
  member FlaskStack-VCC-CVD-WLHost14
  member FlaskStack-VCC-CVD-WLHost15
  member FlaskStack-VCC-CVD-Infra01
  member FlaskStack-VCC-CVD-Infra02
  member FlaskStack-AMD-VMHost70
  member FlaskStack-AMD-VMHost71
interface mgmt0
  ip address 10.29.164.239 255.255.255.0
vsan database
  vsan 101 interface fc1/9
  vsan 101 interface fc1/10
  vsan 101 interface fc1/11
  vsan 101 interface fc1/12
  vsan 101 interface fc1/13
  vsan 101 interface fc1/14
  vsan 101 interface fc1/15
  vsan 101 interface fc1/16
clock timezone PST 0 0
clock summer-time PDT 2 Sun Mar 02:00 1 Sun Nov 02:00 60
switchname ADD16-MDS-B
cli alias name autozone source sys/autozone.py
line console
line vty
boot kickstart bootflash:/m9100-s6ek9-kickstart-mz.8.3.1.bin
boot system bootflash:/m9100-s6ek9-mz.8.3.1.bin
interface fc1/1

```

```
interface fc1/2
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 fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/1
  no port-license
interface fc1/2
  no port-license
interface fc1/3
  no port-license
interface fc1/4
  no port-license
interface fc1/5
  no port-license
interface fc1/6
  no port-license
interface fc1/7
  no port-license
interface fc1/8
  no port-license
interface fc1/9
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/10
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/11
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/12
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/13
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/14
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/15
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/16
  switchport trunk allowed vsan 101
  switchport trunk mode off
  port-license acquire
  no shutdown
ip default-gateway 10.29.164.1
```

## Appendix B - References Used in Guide

This section provides links to additional information for each partner's solution component of this document.

- Cisco UCS B-Series Servers
- <http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/index.html>
- <https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200M6-specsheet.pdf>
- <https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/datasheet-listing.html>
- <https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b200-M6-blade-server/model.html>
- [https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/hw/blade-servers/B200M6.pdf](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/blade-servers/B200M6.pdf)
- Cisco UCS Manager Configuration Guides  
<http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-and-configuration-guides-list.html>  
<https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-release-notes-list.html>

- 
- Cisco UCS Virtual Interface Cards  
<https://www.cisco.com/c/en/us/products/interfaces-modules/unified-computing-system-adapters/index.html>
  - Cisco Nexus Switching References  
<http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html>  
<https://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>  
<https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html>
  - Cisco Intersight References  
<https://www.cisco.com/c/en/us/products/cloud-systems-management/intersight/index.html>  
<https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html>
  - FlashStack Cisco Design Guides  
<https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/data-center-design-guides-all.html#FlashStack>
  - Microsoft References  
<https://docs.microsoft.com/en-us/fslogix/>
  - VMware References  
<https://docs.vmware.com/en/VMware-vSphere/index.html>
  - Login VSI Documentation  
<https://www.loginvsi.com/resources/>
  - Pure Storage Reference Documents  
<https://www.flashstack.com/>  
[https://www.purestorage.com/content/dam/purestorage/pdf/datasheets/ps\\_ds\\_flasharray\\_03.pdf](https://www.purestorage.com/content/dam/purestorage/pdf/datasheets/ps_ds_flasharray_03.pdf)  
<https://www.purestorage.com>  
<https://www.purestorage.com/products/evergreen-subscriptions.html>  
<https://www.purestorage.com/solutions/infrastructure/vdi.html>  
<https://www.purestorage.com/solutions/infrastructure/vdi-calculator.html>  
[https://support.purestorage.com/FlashArray/PurityFA/FlashArray File Services/001 Getting Started/001\\_FA File Services Quick Start Guide](https://support.purestorage.com/FlashArray/PurityFA/FlashArray File Services/001 Getting Started/001_FA File Services Quick Start Guide)  
[https://support.purestorage.com/FlashArray/PurityFA/FlashArray File Services/001 Getting Started/002\\_FA File Services Requirements and Best Practices](https://support.purestorage.com/FlashArray/PurityFA/FlashArray File Services/001 Getting Started/002_FA File Services Requirements and Best Practices)

## Appendix C - Glossary

This glossary addresses some terms used in this document, for the purposes of aiding understanding. This is not a complete list of all multicloud terminology. Some Cisco product links are supplied here also, where considered useful for the purposes of clarity, but this is by no means intended to be a complete list of all applicable Cisco products.

<b>aaS/XaaS</b> <b>(IT capability provided as a Service)</b>	<p>Some IT capability, X, provided as a service (XaaS). Some benefits are:</p> <ul style="list-style-type: none"><li>• The provider manages the design, implementation, deployment, upgrades, resiliency, scalability, and overall delivery of the service and the infrastructure that supports it.</li><li>• There are very low barriers to entry, so that services can be quickly adopted and dropped in response to business demand, without the penalty of inefficiently utilized CapEx.</li><li>• The service charge is an IT OpEx cost (pay-as-you-go), whereas the CapEx and the service infrastructure is the responsibility of the provider.</li><li>• Costs are commensurate to usage and hence more easily controlled with respect to business demand and outcomes.</li></ul> <p>Such services are typically implemented as “microservices,” which are accessed via REST APIs. This architectural style supports composition of service components into systems. Access to and management of aaS assets is via a web GUI and/or APIs, such that Infrastructure-as-code (IaC) techniques can be used for automation, for example, Ansible and Terraform.</p> <p>The provider can be any entity capable of implementing an aaS “cloud-native” architecture. The cloud-native architecture concept is well-documented and supported by open-source software and a rich ecosystem of services such as training and consultancy. The provider can be an internal IT department or any of many third-party companies using and supporting the same open-source platforms.</p> <p>Service access control, integrated with corporate IAM, can be mapped to specific users and business activities, enabling consistent policy controls across services, wherever they are delivered from.</p>
<b>Ansible</b>	<p>An infrastructure automation tool, used to implement processes for instantiating and configuring IT service components, such as VMs on an IaaS platform. Supports the consistent execution of processes defined in YAML “playbooks” at scale, across multiple targets. Because the Ansible artefacts (playbooks) are text-based, they can be stored in a Source Code Management (SCM) system, such as GitHub. This allows for software development like processes to be applied to infrastructure automation, such as, Infrastructure-as-code (see IaC below).</p> <p><a href="https://www.ansible.com">https://www.ansible.com</a></p>
<b>AWS</b> <b>(Amazon Web Services)</b>	<p>Provider of IaaS and PaaS.</p> <p><a href="https://aws.amazon.com">https://aws.amazon.com</a></p>
<b>Azure</b>	<p>Microsoft IaaS and PaaS.</p> <p><a href="https://azure.microsoft.com/en-gb/">https://azure.microsoft.com/en-gb/</a></p>
<b>Co-located data center</b>	<p>“A colocation center (CoLo)...is a type of data center where equipment, space, and bandwidth are available for rental to retail customers. Colocation facilities provide space, power, cooling, and physical security for the server, storage, and networking equipment of other firms and also connect them to a variety of telecommunications and network service providers with a minimum of cost and complexity.”</p> <p><a href="https://en.wikipedia.org/wiki/Colocation_centre">https://en.wikipedia.org/wiki/Colocation_centre</a></p>

<b>Containers (Docker)</b>	<p>A (Docker) container is a means to create a package of code for an application and its dependencies, such that the application can run on different platforms which support the Docker environment. In the context of aaS, microservices are typically packaged within Linux containers orchestrated by Kubernetes (K8s).</p> <p><a href="https://www.docker.com">https://www.docker.com</a></p> <p><a href="https://www.cisco.com/c/en/us/products/cloud-systems-management/containerplatform/index.html">https://www.cisco.com/c/en/us/products/cloud-systems-management/containerplatform/index.html</a></p>
<b>DevOps</b>	<p>The underlying principle of DevOps is that the application development and operations teams should work closely together, ideally within the context of a toolchain that automates the stages of development, test, deployment, monitoring, and issue handling. DevOps is closely aligned with IaC, continuous integration and deployment (CI/CD), and Agile software development practices.</p> <p><a href="https://en.wikipedia.org/wiki/DevOps">https://en.wikipedia.org/wiki/DevOps</a></p> <p><a href="https://en.wikipedia.org/wiki/CI/CD">https://en.wikipedia.org/wiki/CI/CD</a></p>
<b>Edge compute</b>	<p>Edge compute is the idea that it can be more efficient to process data at the edge of a network, close to the endpoints that originate that data, or to provide virtualized access services, such as at the network edge. This could be for reasons related to low latency response, reduction of the amount of unprocessed data being transported, efficiency of resource utilization, and so on. The generic label for this is Multi-access Edge Computing (MEC), or Mobile Edge Computing for mobile networks specifically.</p> <p>From an application experience perspective, it is important to be able to utilize, at the edge, the same operations model, processes, and tools used for any other compute node in the system.</p> <p><a href="https://en.wikipedia.org/wiki/Mobile_edge_computing">https://en.wikipedia.org/wiki/Mobile_edge_computing</a></p>
<b>IaaS (Infrastructure as-a-Service)</b>	<p>Infrastructure components provided aaS, located in data centers operated by a provider, typically accessed over the public Internet. IaaS provides a base platform for the deployment of workloads, typically with containers and Kubernetes (K8s).</p>
<b>IaC (Infrastructure as-Code)</b>	<p>Given the ability to automate aaS via APIs, the implementation of the automation is typically via Python code, Ansible playbooks, and similar. These automation artefacts are programming code that define how the services are consumed. As such, they can be subject to the same code management and software development regimes as any other body of code. This means that infrastructure automation can be subject to all of the quality and consistency benefits, CI/CD, traceability, automated testing, compliance checking, and so on, that could be applied to any coding project.</p> <p><a href="https://en.wikipedia.org/wiki/Infrastructure_as_code">https://en.wikipedia.org/wiki/Infrastructure_as_code</a></p>
<b>IAM (Identity and Access Management)</b>	<p>IAM is the means to control access to IT resources so that only those explicitly authorized to access given resources can do so. IAM is an essential foundation to a secure multicloud environment.</p> <p><a href="https://en.wikipedia.org/wiki/Identity_management">https://en.wikipedia.org/wiki/Identity_management</a></p>
<b>IBM (Cloud)</b>	<p>IBM IaaS and PaaS.</p> <p><a href="https://www.ibm.com/cloud">https://www.ibm.com/cloud</a></p>
<b>Intersight</b>	<p>Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support.</p>

	<a href="https://www.cisco.com/c/en/us/products/servers-unified-computing/intersight/index.html">https://www.cisco.com/c/en/us/products/servers-unified-computing/intersight/index.html</a>
<b>GCP</b> (Google Cloud Platform)	Google IaaS and PaaS. <a href="https://cloud.google.com/gcp">https://cloud.google.com/gcp</a>
<b>Kubernetes</b> (K8s)	Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications. <a href="https://kubernetes.io">https://kubernetes.io</a>
<b>Microservices</b>	A microservices architecture is characterized by processes implementing fine-grained services, typically exposed via REST APIs and which can be composed into systems. The processes are often container-based, and the instantiation of the services often managed with Kubernetes. Microservices managed in this way are intrinsically well suited for deployment into IaaS environments, and as such, are the basis of a cloud native architecture. <a href="https://en.wikipedia.org/wiki/Microservices">https://en.wikipedia.org/wiki/Microservices</a>
<b>PaaS</b> (Platform-as-a-Service)	PaaS is a layer of value-add services, typically for application development, deployment, monitoring, and general lifecycle management. The use of IaC with IaaS and PaaS is very closely associated with DevOps practices.
<b>Private on-premises data center</b>	A data center infrastructure housed within an environment owned by a given enterprise is distinguished from other forms of data center, with the implication that the private data center is more secure, given that access is restricted to those authorized by the enterprise. Thus, circumstances can arise where very sensitive IT assets are only deployed in a private data center, in contrast to using public IaaS. For many intents and purposes, the underlying technology can be identical, allowing for hybrid deployments where some IT assets are privately deployed but also accessible to other assets in public IaaS. IAM, VPNs, firewalls, and similar are key technologies needed to underpin the security of such an arrangement.
<b>REST API</b>	Representational State Transfer (REST) APIs is a generic term for APIs accessed over HTTP(S), typically transporting data encoded in JSON or XML. REST APIs have the advantage that they support distributed systems, communicating over HTTP, which is a well-understood protocol from a security management perspective. REST APIs are another element of a cloud-native applications architecture, alongside microservices. <a href="https://en.wikipedia.org/wiki/Representational_state_transfer">https://en.wikipedia.org/wiki/Representational_state_transfer</a>
<b>SaaS</b> (Software-as-a-Service)	End-user applications provided “aaS” over the public Internet, with the underlying software systems and infrastructure owned and managed by the provider.
<b>SAML</b> (Security Assertion Markup Language)	Used in the context of Single-Sign-On (SSO) for exchanging authentication and authorization data between an identity provider, typically an IAM system, and a service provider (some form of SaaS). The SAML protocol exchanges XML documents that contain security assertions used by the aaS for access control decisions. <a href="https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language">https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language</a>
<b>Terraform</b>	An open-source IaC software tool for cloud services, based on declarative configuration files. <a href="https://www.terraform.io">https://www.terraform.io</a>

## Appendix D - Acronyms

**AAA**—Authentication, Authorization, and Accounting

**ACP**—Access-Control Policy

---

**ACI**—Cisco Application Centric Infrastructure

**ACK**—Acknowledge or Acknowledgement

**ACL**—Access-Control List

**AD**—Microsoft Active Directory

**AFI**—Address Family Identifier

**AMP**—Cisco Advanced Malware Protection

**AP**—Access Point

**API**—Application Programming Interface

**APIC**—Cisco Application Policy Infrastructure Controller (ACI)

**ASA**—Cisco Adaptive Security Appliance

**ASM**—Any-Source Multicast (PIM)

**ASR**—Aggregation Services Router

**Auto-RP**—Cisco Automatic Rendezvous Point protocol (multicast)

**AVC**—Application Visibility and Control

**BFD**—Bidirectional Forwarding Detection

**BGP**—Border Gateway Protocol

**BMS**—Building Management System

**BSR**—Bootstrap Router (multicast)

**BYOD**—Bring Your Own Device

**CAPWAP**—Control and Provisioning of Wireless Access Points Protocol

**CDP**—Cisco Discovery Protocol

**CEF**—Cisco Express Forwarding

**CMD**—Cisco Meta Data

**CPU**—Central Processing Unit

**CSR**—Cloud Services Routers

**CTA**—Cognitive Threat Analytics

**CUWN**—Cisco Unified Wireless Network

**CVD**—Cisco Validated Design

**CYOD**—Choose Your Own Device

**DC**—Data Center

**DHCP**—Dynamic Host Configuration Protocol

**DM**—Dense-Mode (multicast)

**DMVPN**—Dynamic Multipoint Virtual Private Network

**DMZ**—Demilitarized Zone (firewall/networking construct)



---

**DNA**—Cisco Digital Network Architecture

**DNS**—Domain Name System

**DORA**—Discover, Offer, Request, ACK (DHCP Process)

**DWDM**—Dense Wavelength Division Multiplexing

**ECMP**—Equal Cost Multi Path

**EID**—Endpoint Identifier

**EIGRP**—Enhanced Interior Gateway Routing Protocol

**EMI**—Electromagnetic Interference

**ETR**—Egress Tunnel Router (LISP)

**EVPN**—Ethernet Virtual Private Network (BGP EVPN with VXLAN data plane)

**FHR**—First-Hop Router (multicast)

**FHRP**—First-Hop Redundancy Protocol

**FMC**—Cisco Firepower Management Center

**FTD**—Cisco Firepower Threat Defense

**GBAC**—Group-Based Access Control

**GbE**—Gigabit Ethernet

**Gbit/s**—Gigabits Per Second (interface/port speed reference)

**GRE**—Generic Routing Encapsulation

**GRT**—Global Routing Table

**HA**—High-Availability

**HQ**—Headquarters

**HSRP**—Cisco Hot-Standby Routing Protocol

**HTDB**—Host-tracking Database (SD-Access control plane node construct)

**IBNS**—Identity-Based Networking Services (IBNS 2.0 is the current version)

**ICMP**—Internet Control Message Protocol

**IDF**—Intermediate Distribution Frame; essentially a wiring closet.

**IEEE**—Institute of Electrical and Electronics Engineers

**IETF**—Internet Engineering Task Force

**IGP**—Interior Gateway Protocol

**IID**—Instance-ID (LISP)

**IOE**—Internet of Everything

**IoT**—Internet of Things

**IP**—Internet Protocol

**IPAM**—IP Address Management

---

**IPS**—Intrusion Prevention System

**IPSec**—Internet Protocol Security

**ISE**—Cisco Identity Services Engine

**ISR**—Integrated Services Router

**IS-IS**—Intermediate System to Intermediate System routing protocol

**ITR**—Ingress Tunnel Router (LISP)

**LACP**—Link Aggregation Control Protocol

**LAG**—Link Aggregation Group

**LAN**—Local Area Network

**L2 VNI**—Layer 2 Virtual Network Identifier; as used in SD-Access Fabric, a VLAN.

**L3 VNI**—Layer 3 Virtual Network Identifier; as used in SD-Access Fabric, a VRF.

**LHR**—Last-Hop Router (multicast)

**LISP**—Location Identifier Separation Protocol

**MAC**—Media Access Control Address (OSI Layer 2 Address)

**MAN**—Metro Area Network

**MEC**—Multichassis EtherChannel, sometimes referenced as ***MCEC***

**MDF**—Main Distribution Frame; essentially the central wiring point of the network.

**MnT**—Monitoring and Troubleshooting Node (Cisco ISE persona)

**MOH**—Music on Hold

**MPLS**—Multiprotocol Label Switching

**MR**—Map-resolver (LISP)

**MS**—Map-server (LISP)

**MSDP**—Multicast Source Discovery Protocol (multicast)

**MTU**—Maximum Transmission Unit

**NAC**—Network Access Control

**NAD**—Network Access Device

**NAT**—Network Address Translation

**NBAR**—Cisco Network-Based Application Recognition (NBAR2 is the current version).

**NFV**—Network Functions Virtualization

**NSF**—Non-Stop Forwarding

**OSI**—Open Systems Interconnection model

**OSPF**—Open Shortest Path First routing protocol

**OT**—Operational Technology

**PAgP**—Port Aggregation Protocol

---

**PAN**—Primary Administration Node (Cisco ISE persona)

**PCI DSS**—Payment Card Industry Data Security Standard

**PD**—Powered Devices (PoE)

**PETR**—Proxy-Egress Tunnel Router (LISP)

**PIM**—Protocol-Independent Multicast

**PITR**—Proxy-Ingress Tunnel Router (LISP)

**PnP**—Plug-n-Play

**PoE**—Power over Ethernet (Generic term, may also refer to IEEE 802.3af, 15.4W at PSE)

**PoE+**—Power over Ethernet Plus (IEEE 802.3at, 30W at PSE)

**PSE**—Power Sourcing Equipment (PoE)

**PSN**—Policy Service Node (Cisco ISE persona)

**pxGrid**—Platform Exchange Grid (Cisco ISE persona and publisher/subscriber service)

**PxTR**—Proxy-Tunnel Router (LISP - device operating as both a PETR and PITR)

**QoS**—Quality of Service

**RADIUS**—Remote Authentication Dial-In User Service

**REST**—Representational State Transfer

**RFC**—Request for Comments Document (IETF)

**RIB**—Routing Information Base

**RLOC**—Routing Locator (LISP)

**RP**—Rendezvous Point (multicast)

**RP**—Redundancy Port (WLC)

**RP**—Route Processor

**RPF**—Reverse Path Forwarding

**RR**—Route Reflector (BGP)

**RTT**—Round-Trip Time

**SA**—Source Active (multicast)

**SAFI**—Subsequent Address Family Identifiers (BGP)

**SD**—Software-Defined

**SDA**—Cisco Software Defined-Access

**SDN**—Software-Defined Networking

**SFP**—Small Form-Factor Pluggable (1 GbE transceiver)

**SFP+**— Small Form-Factor Pluggable (10 GbE transceiver)

**SGACL**—Security-Group ACL

**SGT**—Scalable Group Tag, sometimes reference as Security Group Tag

---

**SM**—Spare-mode (multicast)  
**SNMP**—Simple Network Management Protocol  
**SSID**—Service Set Identifier (wireless)  
**SSM**—Source-Specific Multicast (PIM)  
**SSO**—Stateful Switchover  
**STP**—Spanning-tree protocol  
**SVI**—Switched Virtual Interface  
**SVL**—Cisco StackWise Virtual  
**SWIM**—Software Image Management  
**SXP**—Scalable Group Tag Exchange Protocol  
**Syslog**—System Logging Protocol  
**TACACS+**—Terminal Access Controller Access-Control System Plus  
**TCP**—Transmission Control Protocol (OSI Layer 4)  
**UCS**—Cisco Unified Computing System  
**UDP**—User Datagram Protocol (OSI Layer 4)  
**UPoE**—Cisco Universal Power Over Ethernet (60W at PSE)  
**UPoE+**—Cisco Universal Power Over Ethernet Plus (90W at PSE)  
**URL**—Uniform Resource Locator  
**VLAN**—Virtual Local Area Network  
**VM**—Virtual Machine  
**VN**—Virtual Network, analogous to a VRF in SD-Access  
**VNI**—Virtual Network Identifier (VXLAN)  
**vPC**—virtual Port Channel (Cisco Nexus)  
**VPLS**—Virtual Private LAN Service  
**VPN**—Virtual Private Network  
**VPNv4**—BGP address family that consists of a Route-Distinguisher (RD) prepended to an IPv4 prefix  
**VPWS**—Virtual Private Wire Service  
**VRF**—Virtual Routing and Forwarding  
**VSL**—Virtual Switch Link (Cisco VSS component)  
**VSS**—Cisco Virtual Switching System  
**VXLAN**—Virtual Extensible LAN  
**WAN**—Wide-Area Network  
**WLAN**—Wireless Local Area Network (generally synonymous with IEEE 802.11-based networks)  
**WoL**—Wake-on-LAN

---

**xTR**—Tunnel Router (LISP - device operating as both an ETR and ITR)

---

## 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\_P1)

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

**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)