

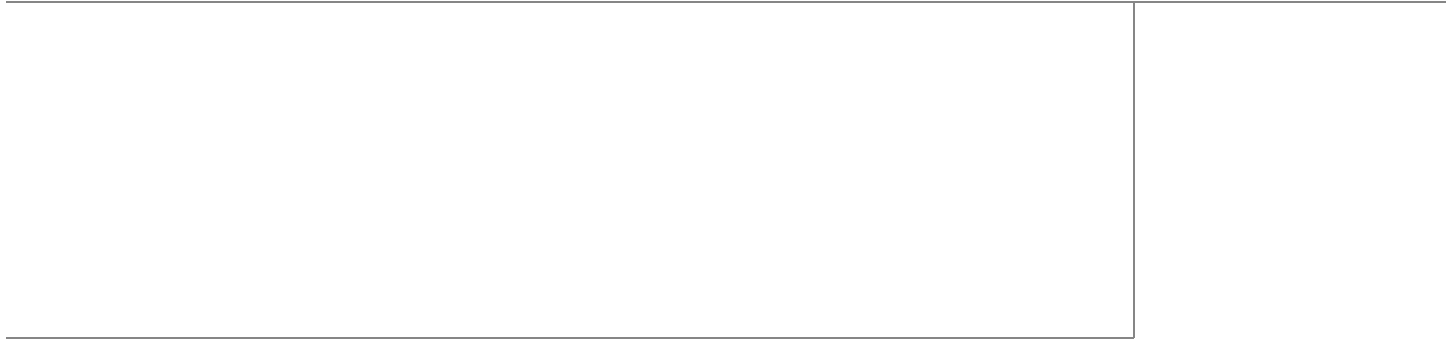
## Cisco UCS Mini Branch Office Solution for EMC VSPEX

With EMC VNXe3200 and Microsoft Windows Server 2012 R2 Hyper-V for up to 100 Virtual Machines

Last Updated: December 19, 2014



Building Architectures to Solve Business Problems



## About the Authors



Sanjeev Naldurgkar

### **Sanjeev Naldurgkar, Technical Marketing Engineer, UCS Data Center Solutions Engineering, Cisco Systems**

Sanjeev has over 12 years of experience in information technology, his focus areas include UCS, Microsoft product technologies, server virtualization, and storage technologies. Prior to joining Cisco, Sanjeev was Support Engineer at Microsoft Global Technical Support Center. Sanjeev holds a Bachelor's Degree in Electronics and Communication Engineering and Industry certifications from Microsoft, and VMware.

## About Cisco Validated Design (CVD) Program

---

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

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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: <http://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).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco UCS Mini Branch Office Solution for EMC VSPEX

© 2014 Cisco Systems, Inc. All rights reserved.



# Acknowledgment

For their contributions in developing this document the authors acknowledges the contributions of:

- Vijay Durairaj (Cisco Systems)
- Tim Cerling (Cisco Systems)
- Bathu Krishnan (Cisco Systems)
- Vadi Bhatt (Cisco Systems)
- Sindhu Sudhir (Cisco Systems)
- David Hartman (EMC Corporation)
- Richard Preston (EMC Corporation)



# Cisco UCS Mini Branch Office Solution for EMC VSPEX

---

## Executive Summary

Cisco UCS Mini Branch Office Solution for EMC VSPEX is a pre-validated and modular architecture built with proven best-of-breed technologies. Because EMC VSPEX solutions are rigorously tested, the solution drastically reduces server virtualization planning and configuration overhead while contributing to IT transformation through faster deployments, greater choice of components and flexibility at reduced risk.

This Cisco Validated Design (CVD) leverages the EMC VSPEX Private Cloud Proven Infrastructure with Microsoft Windows Server 2012 R2 Hyper-V reference architecture for up to 100 virtual machines. This solution uses Cisco components such as UCS Mini compute chassis, UCS Central and EMC's VNXe3200 storage array. A typical use case would be the Remote Office/Branch Office (ROBO) location with centralized management to ensure consistent standards-based deployment. The platform has sufficient scalability in compute and storage areas, if necessary.

This Cisco Validated Design document defines the architectural design and deployment procedure of the previously-defined VSPEX Private Cloud Proven Infrastructure with Microsoft Windows Server Hyper-V with a focus on features and options that underscore functionality, scalability and standardized management as well as simplicity, efficiency, and flexibility for a platform which can be an extension of a data center solution or serve as a standalone platform with similar benefits.

## Introduction

Virtualization is a critical deployment strategy for reducing the Total Cost of Ownership (TCO). It allows for consolidation for better utilization of underlying compute, network and storage components. However, selecting the appropriate platform for virtualization can be confusing given the myriad of choices at every level. Platforms should be flexible for scaling while also being reliable and cost effective to facilitate virtualization. In the VSPEX converged infrastructure, compatible components come together for a scalable reference architecture with provisions for scale within each individual component. Cisco solutions implemented as part of EMC VSPEX reference architectures leverage available flexibility and functionality for effective resource utilization while also preserving existing support structure.



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2014 Cisco Systems, Inc. All rights reserved.

## Audience

The reader of this document is expected to have the necessary training and background to install and configure Microsoft Windows Server 2012 R2 Hyper-V, EMC VNXe series storage arrays, and Cisco UCS Mini chassis (mini), Unified Computing Systems Manager (UCSM) and UCS Central Management. External references are provided where applicable and it is recommended that the reader be familiar with these documents.

Readers are also expected to be familiar with the infrastructure and database security policies of the customer installation.

## Purpose of this Document

This document illustrates the design and deployment steps required for implementing the Cisco branch office solution on EMC VSPEX Private Cloud with Microsoft Windows Server 2012 R2 Hyper-V Centralized management of this branch office solution through UCS Central located in the data center is also highlighted. The detail provided in this document allows the configuration and functionality of specific aspects of the solution to be verified, and ensure the configuration meets core availability requirements. The solution that is documented covers Microsoft Hyper-V architecture for small-to medium-sized businesses with a need for up to 100 VMs. This document show cases the solution with EMC VNXe 3200 series storage array using Fiber Channel (FC) for OS booting and data storage through the pair of Cisco UCS 6324 Fabric Interconnects. While readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are important to the deployment of this solution s are specifically mentioned.

Following are elements within scope of this Cisco solution:

- Providing an end-to-end virtualization solution to take full advantage of unified infrastructure components.
- Showing implementation progression of Microsoft Windows Server 2012 R2 Hyper-V design and results.
- Providing a reliable, flexible and scalable reference design

## Business Needs

Businesses have always had a need for consistent provisioning and management of remote office IT resources. The new Cisco UCS Mini presents appropriate levels of compute and connectivity options to cater to the needs of a branch office while leveraging inherent strengths of UCS Manager resident within the chassis. Complimenting this setup is integration with UCS Central in the data center for a hierarchical management structure ensuring consistent standards based deployment and management of all branch office sites from a central office. Efficiencies from converged stacks such as the VSPEX Private Cloud Solution are further enhanced when integrated with centralized provisioning and management.

## Solution Overview

The Cisco solution for EMC VSPEX with Microsoft Windows Server 2012 R2 provides an end-to-end architecture with Cisco, EMC, and Microsoft technologies that demonstrate support for up to 100 generic virtual machines and provide high availability and server redundancy.

The following are the components used for the design and deployment:

- Cisco Unified Computing System
- Cisco UCS Manager 3.0(1c)
- Cisco UCS B200M3 server
- Cisco UCS VIC adapters
- Cisco UCS Central ROBO (Remote Office/Branch Office Implementation)
- EMC VNXe3200
- Microsoft Windows Server 2012 R2 Hyper-V
- Microsoft Active Directory (provided by customer)

The solution is designed to host scalable and mixed application workloads. The scope of this Cisco Validated Design document is limited to the Cisco solution for EMC VSPEX Microsoft Windows Server 2012 R2 Hyper-V solutions for up to 100 virtual machines only. When the base configuration is in place, it is a simple matter of adding more servers or storage to handle the larger workloads.

## Technology Overview

### Cisco Unified Computing System

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

The main components of the Cisco UCS are:

- **Compute**—The system is based on an entirely new class of computing system that incorporates rack mount and blade servers based on Intel Xeon 2600 v2 Series Processors.
- **Network**—The system is integrated onto a low-latency, lossless, 10-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- **Virtualization**—The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access**—The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying the storage access the Cisco Unified Computing System can access storage over Ethernet (SMB 3.0 or iSCSI), Fibre Channel, and Fibre

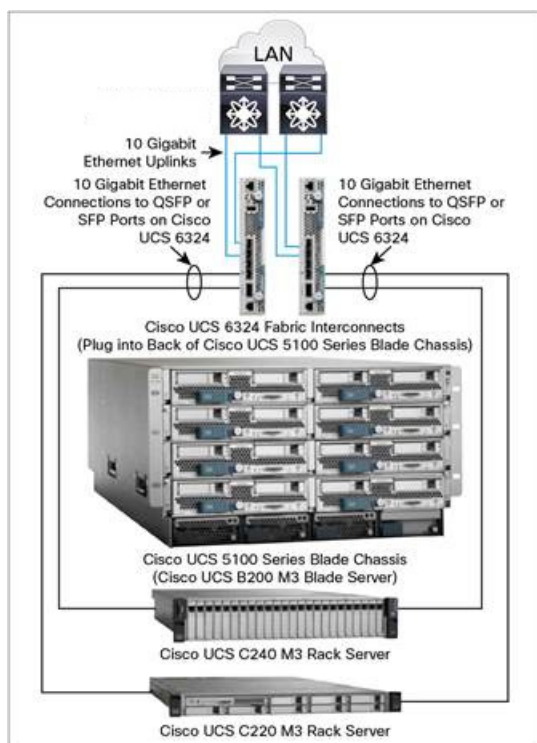
Channel over Ethernet (FCoE). This provides customers with storage choices and investment protection. In addition, the server administrators can pre-assign storage-access policies to storage resources, for simplified storage connectivity and management leading to increased productivity.

- **Management**—the system uniquely integrates all system components to enable the entire solution to be managed as a single entity by the Cisco UCS Manager. The Cisco UCS Manager has an intuitive graphical user interface (GUI), a command-line interface (CLI), and a powerful scripting library module for Microsoft PowerShell built on a robust application programming interface (API) to manage all system configuration and operations.

Cisco Unified Computing System (Cisco UCS) fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

The Cisco UCS 6324 Fabric Interconnect extends the Cisco UCS architecture into environments with lesser resource requirements. Providing the same unified server and networking capabilities as the full-scale Cisco UCS solution, the Cisco UCS 6324 Fabric Interconnect embeds the connectivity within the Cisco UCS 5108 Blade Server Chassis to provide a smaller domain of up to 15 servers (8 blade servers and up to 7 direct-connect rack servers).

**Figure 1** *Cisco UCS Mini Architecture*



## Cisco UCS Manager 3.0

Cisco Unified Computing System (UCS) Manager provides unified, embedded management of all software and hardware components of the Cisco UCS through choice of an intuitive GUI, a Command Line Interface (CLI), a Microsoft PowerShell module, or an XML API. The Cisco UCS Manager provides unified management domain with centralized management capabilities and controls multiple chassis and thousands of virtual machines.

The Cisco UCS 6324 Fabric Interconnect hosts and runs Cisco UCS Manager in a highly available configuration, enabling the fabric interconnects to fully manage all Cisco UCS elements. The Cisco UCS 6324 Fabric Interconnects support out-of-band management through dedicated 10/100/1000-Mbps Ethernet management ports. Cisco UCS Manager typically is deployed in a clustered active-passive configuration with two UCS 6324 Fabric Interconnects connected through the cluster interconnect built into the chassis.

Cisco UCS Manager 3.0 supports the 6324 Fabric Interconnect that integrates the FI into the UCS Chassis and provides an integrated solution for a smaller deployment environment. Cisco UCS Mini simplifies the system management and saves cost for smaller scale deployments. The hardware and software components support Cisco unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

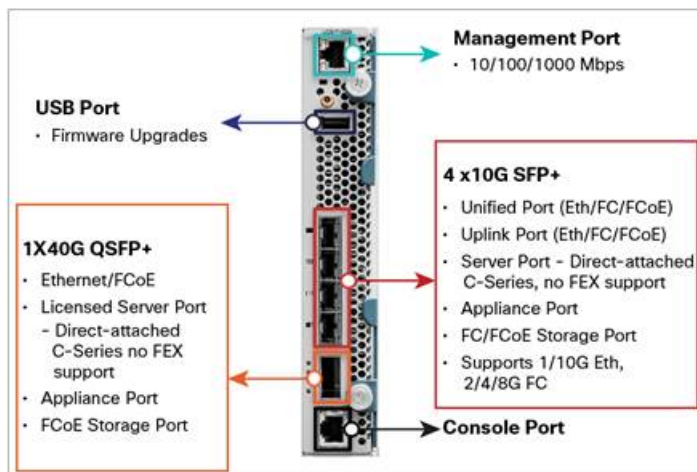
## Cisco UCS 6324UP Fabric Interconnect

The Cisco UCS 6324 Fabric Interconnect provides the management, LAN and storage connectivity for the Cisco UCS 5108 Blade Server Chassis and direct-connect rack-mount servers. It provides the same full-featured Cisco UCS management capabilities and XML API as the full-scale Cisco UCS solution in addition to integrating with Cisco UCS Central Software and Cisco UCS Director (Figure 2).

From a networking perspective, the Cisco UCS 6324 Fabric Interconnect uses a cut-through architecture supporting deterministic, low-latency, line-rate 10 Gigabit Ethernet on all ports with switching capacity of up to 500Gbps, independent of packet size and enabled services. Sixteen 10Gbps links connect to the servers, providing a 20Gbps link from each Cisco UCS 6324 Fabric Interconnect to each server. The product family supports Cisco low-latency, lossless 10 Gigabit Ethernet unified network fabric capabilities that increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over a lossless Ethernet fabric from the blade through an interconnect. Significant TCO savings come from Fibre Channel over Ethernet (FCoE)-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

The Cisco UCS 6324 Fabric Interconnect (Figure 2) is a 10 Gigabit Ethernet, FCoE and Fibre Channel switch offering up to 500Gbps throughput and up to four unified ports and one scalability port.

**Figure 2** Cisco UCS 6324 Fabric Interconnect



## Cisco UCS B200 M3 Blade Server

Building on the success of the Cisco UCS B200 M2 Blade Servers, the enterprise-class Cisco UCS B200 M3 further extends the capabilities of the Cisco Unified Computing System portfolio in a half-blade form factor. The Cisco UCS B200 M3 Server harnesses the power of the Intel® Xeon® E5-2600 v2 processor product family, up to 786 GB of RAM, two hard drives, and up to 8 x 10GE to deliver exceptional levels of performance, memory expandability, and I/O throughput for nearly all applications. In addition, the Cisco UCS B200 M3 blade server offers a modern design that removes the need for redundant switching components in every chassis in favor of a simplified top of rack design, allowing more space for server resources, providing a density, power, and performance advantage over previous generation servers. The Cisco UCS B200 M3 Server is shown in figure 3.

**Figure 3** *Cisco UCS B200 M3 Blade Server*



## Cisco I/O Adapters

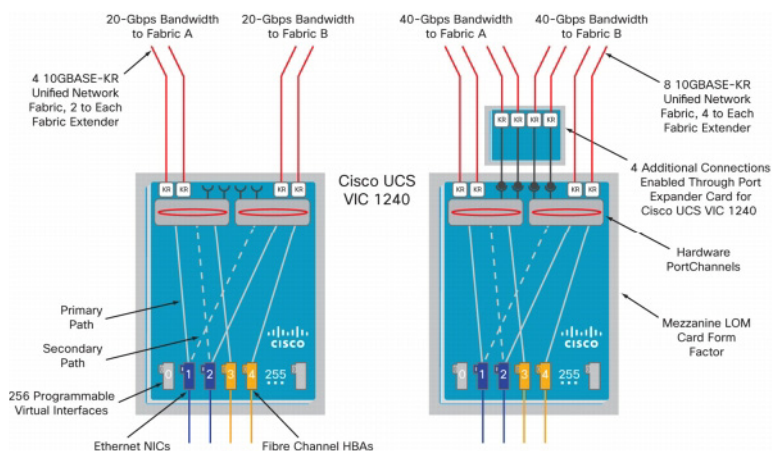
The Cisco UCS blade server has various Converged Network Adapters (CNA) options. The UCS VIC 1240 Virtual Interface Card (VIC) option is used in this Cisco Validated Design.

Cisco UCS VIC 1240 is a 4-port 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed exclusively for the M3 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional Port Expander, the Cisco UCS VIC 1240 capabilities can be expanded to eight ports of 10 Gigabit Ethernet.

The Cisco UCS VIC 1240 enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1240 supports Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.



**Figure 4** *Cisco UCS VIC 1240*



## Cisco UCS Differentiators

Cisco Unified Compute System is revolutionizing the way servers are managed in data center. Following are the unique differentiators of UCS and UCS-Manager.

- **Embedded management:** In UCS, the servers are managed by the embedded firmware in the Fabric Interconnects, eliminating need for any external physical or virtual devices to manage the servers.
- **Unified fabric**—The new UCS Fabric Interconnect 6324 supports unified fabric ports, which operates LAN, SAN and management traffic on the same chassis for both blade server and rack server deployment. This converged I/O results in reduced cables, SFPs, and adapters - reducing capital and operational expenses of overall solution.
- **Auto Discovery**—By simply inserting the blade server in the chassis, the discovery and inventory of compute resource occurs automatically without any management intervention. Combination of unified fabric and auto-discovery enables wire-once architecture of UCS, where compute capability of UCS can extend easily while keeping the existing external connectivity to LAN, SAN and management networks.
- **Policy based resource classification**—Once a compute resource is discovered by UCSM, 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 shows the policy based resource classification of UCSM.
- **Combined Rack and Blade server management**—UCSM can manage B-series blade servers and C-series rack server under the same UCS domain—This feature, along with stateless computing makes compute resources truly hardware form factor agnostic. In this CVD, we are showcasing only B series servers to demonstrate stateless and form factor independent computing work load.
- **Model based management architecture**—UCSM architecture and management database is model based and data driven. Open, standard based XML API is provided to operate on the management model. This enables easy and scalable integration of UCSM with other management system, such as Microsoft System Center, VMware vCloud director, and Citrix Cloud Platform.
- **Policies, Pools, Templates**—Management approach in UCSM is based on defining policies, pools and templates, instead of cluttered configuration, which enables simple, loosely coupled, data driven approach in managing compute, network and storage resources.

- —In UCSM, a service profile, port profile or policies can refer to other policies or logical resources with . A referred policy need not 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 flexibilities where different experts from different domains, such as network, storage, security, server and virtualization work together to accomplish a complex task.
- Policy resolution—In UCSM, a tree structure of organizational unit hierarchy can be created that mimics the real life tenants and/or organization relationships. Various policies, pools and templates can be defined at different levels of organization hierarchy. A policy referring to other policy by name is resolved in the organization hierarchy with closest policy match. If no policy with the specified name is found in the hierarchy, then a special policy name ‘default’ is used from the root organization’. This policy resolution practice enables automation friendly management APIs and provides great flexibilities to owners of different organizations.
- Service profiles and stateless computing—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—Combination of policies, pools and templates, , policy resolution in organization hierarchy and service profile based approach to compute resources make UCSM inherently friendly to multi-tenant environment typically observed in private and public clouds.
- Virtualization aware network—VM-FEX technology makes access layer of network aware about host virtualization. This prevents domain pollution of compute and network domains with virtualization when virtual network is managed by port-profiles defined by the network administrator’s team. VM-FEX also offloads hypervisor CPU by performing switching in the hardware, thus allowing hypervisor CPU to do more virtualization related tasks. VM-FEX technology is well integrated with VMware vCenter, Linux KVM and Hyper-V SR-IOV to simplify cloud management.
- Simplified QoS—Even though fibre-channel and Ethernet are converged in UCS fabric, built-in support for QoS and lossless Ethernet makes it seamless. Network Quality of Service (QoS) is simplified in UCSM by representing all system classes in one GUI panel.

## Microsoft Windows Server 2012 R2 Hyper-V

Microsoft Hyper-V is a hypervisor-based virtualization technology that is available as a server role in Microsoft Windows Server, and as a standalone product - Microsoft Hyper-V Server. Hyper-V 2012 R2 is Microsoft’s latest version of its next-generation virtualization technology which builds upon previous releases and provides greater levels of scalability, security, and available in virtual environments. Hyper-V Server 2012 R2 offers improvements in performance and utilization of CPU, memory, and I/O. It also offers users the option to assign up to 64 virtual CPUs to a virtual machine—giving system administrators more flexibility in their virtual server farms as processor-intensive workloads continue to increase.

**Table 1** *Illustrates the Increase in Scale From Previous Major Release*

System	Resource	Maximum Number	
		Windows Server 2008 R2	Windows Server 2012 R2
Host	Logical Processor on hardware	64	320
	Physical Memory	1 TB	4 TB
	Virtual Processor on host	512	2048
Virtual Machine	Virtual Processor per VM	4	64
	Memory per VM	64 GB	1 TB
	Actual Virtual Machines	384	1024
	Virtual Disk Size	2 TB	64 TB
Cluster	Nodes	16	64
	Virtual Machines	1000	8000

Hyper-V provides significant management capabilities and included in the base capabilities of Hyper-V are:

- High availability—up to 64 Hyper-V hosts can be formed into a single cluster hosting up to 8,000 virtual machines.
- Disaster recovery—virtual machine replicas can be created and kept up to date in other locations for rapid recovery and restart in case of a disaster.
- Live migration—virtual machines can be live migrated (moved from one host to another with no service downtime) between any two Hyper-V hosts, whether they are clustered or not, without the need for any shared storage.
- Live storage migration—as with live machine migration, storage for a virtual machine can be migrated without any service downtime.
- Dynamic memory—virtual machines defined with dynamic memory can release unused memory for use by other virtual machines that require it.
- Cluster Shared Volumes—storage volumes in a failover cluster environment allow any virtual machine executing on any cluster host full read/write access to its virtual hard drives from any node in the cluster. This also provides additional high availability by ensuring access to the volume and uninterrupted virtual machine execution even if the Hyper-V host loses physical connection to the volume.
- Clustering of virtual machines—virtual machine clusters can use storage from many locations: iSCSI Targets, Virtual HBA to directly access FC and FCoE storage, SMB 3.0 file shares, or virtual hard drives residing on Cluster Shared Volumes.
- PowerShell—a complete PowerShell module enables management of virtual machines and their resources via scripting so repetitive tasks can be easily executed.
- NIC teaming—teaming at the host level enables up to 32 physical NICs to form a single team. Within a virtual machine, two virtual NICs can form a team.
- Data deduplication—automatically deduplicate common data on disk, including operating system files on virtual hard drives.

# EMC Storage Technologies and Benefits

The Storage layer is also a key component of any cloud infrastructure solution that serves data generated by applications and operating system in the data center storage processing systems. In this VSPEX solution, EMC VNXe series arrays provide features and performance to enable and enhance any virtualization environment. This increases storage efficiency, management flexibility, and reduces total cost of ownership.

The EMC VNXe series is optimized for virtual applications and delivers industry-leading innovation and enterprise capabilities for file and block storage in a scalable, easy-to-use solution. This next-generation storage platform combines powerful and flexible hardware with advanced efficiency, management, and protection software to meet the demanding needs of today's enterprises.

Intel Xeon Processors power the VNXe series for intelligent storage that automatically and efficiently scales in performance, while ensuring data integrity and security. The VNXe series is designed to meet the high performance, high-scalability requirements of small and midsize enterprises

**Table 2** *Customer Benefits Provided by VNXe Series*

Feature	Benefit
Next-generation unified storage, optimized for virtualization applications	Tight integration with Microsoft Windows and System Center allows for advanced array features and centralized management
Capacity optimization features including compression, deduplication, thin provisioning and application-consistent copies	Reduced storage costs, more efficient use of resources and easier recovery of applications
High-availability, designed to deliver five 9s availability	Higher levels of uptime and reduced outage risk
Automated tiering with FAST VP and FAST Cache that can be optimized for the highest system performance and lowest storage cost simultaneously	More efficient use of storage resources without complicated planning and configuration
Simplified management with EMC Unisphere with a single management interface for all NAS, SAN and replication needs	Reduced management overhead and toolsets required to manage environment

Various software suites and packs are available for the VNXe series. These provide multiple features for enhanced protections and performance. They include the following:

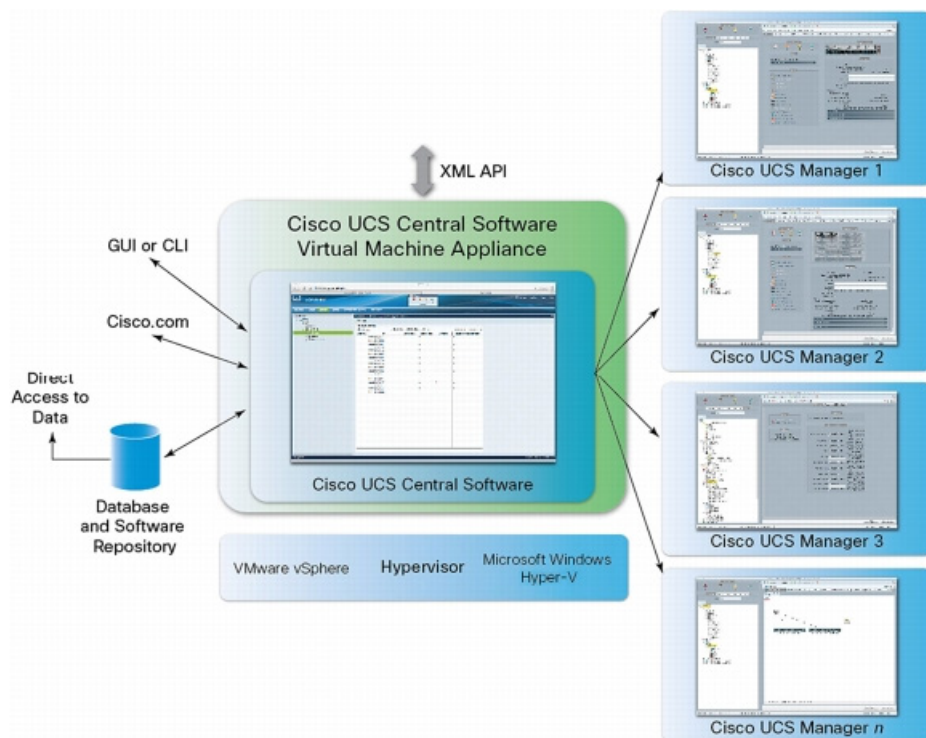
- FAST Suite—Automatically optimizes for the highest system performance and the lowest storage cost simultaneously.
- Security and Compliance Suite—Keeps data safe from changes, deletions, and malicious activity.

## Cisco UCS Central

For Cisco UCS customers managing growth within a single data center, growth across multiple sites, or both, Cisco UCS Central Software centrally manages multiple Cisco UCS domains using the same concepts that Cisco UCS Manager uses to support a single UCS domain (Figure 5). Cisco UCS Central Software manages global resources (including identifiers and policies) that can be consumed within

individual Cisco UCS Manager instances. It can delegate the application of policies (embodied in global service profiles) to individual UCS domains, where Cisco UCS Manager puts the policies into effect. Cisco UCS Central software manages multiple, globally distributed Cisco UCS domains from a single pane. Every instance of Cisco UCS Manager and all of the components managed by it form a domain. Cisco UCS Central integrates with Cisco UCS Manager, and utilizes it to provide global configuration capabilities for pools, policies, and firmware.

**Figure 5** *Cisco UCS Central Software Architecture*



Cisco UCS Central Software makes global policy and compliance easier. When Cisco UCS domains are registered with Cisco UCS Central Software, they can be configured to automatically inherit global identifiers and policies that are centrally defined and managed. Making identifiers such as universal user IDs (UUIDs), MAC addresses, and worldwide names (WWNs) global resources allows every server worldwide to be configured uniquely so that identifier conflicts are automatically avoided. Globally defined policies take this concept significantly further: by defining and enforcing server identity, configuration, and connectivity policies centrally, standards compliance is essentially ensured. The system simply will not configure a server in a way that is inconsistent with standards, so configuration drift and an entire class of errors that can cause downtime are avoided.

## UCS Manager (Mini) Management with UCS Central

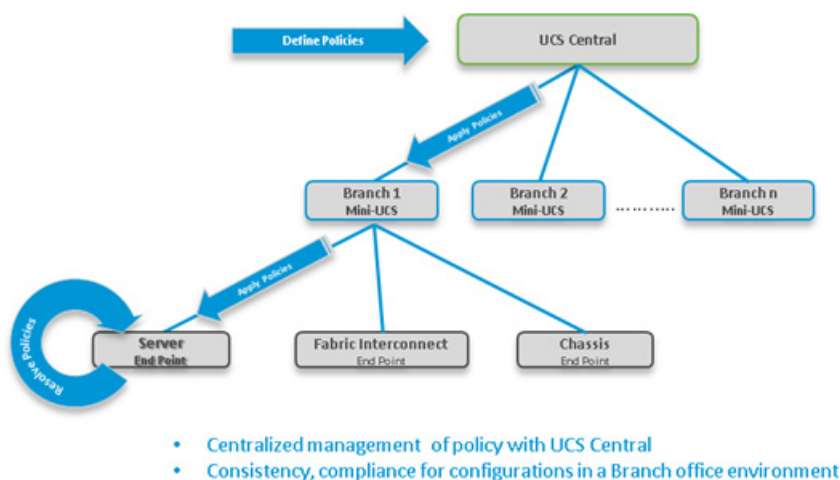
Cisco UCS Central Software is designed and operates comparable to Cisco UCS Manager in that policies and configuration definitions, which make up a Cisco UCS service profile, can be created at a central location and then applied to the endpoint recipient, where they are resolved. With Cisco UCS Manager, the endpoint recipients are the Cisco UCS infrastructure (servers, network, etc.).

For Cisco UCS Central Software, the recipients are individual Cisco UCS Manager instances that have been registered with Cisco UCS Central Software. With Cisco UCS Central Software, global Cisco UCS service profiles are defined centrally and are passed to Cisco UCS Manager instances according to the way they are registered with Cisco UCS Central Software (Figure 6).

**Figure 6** Cisco UCS Manager (Mini) Management with UCS Central

## UCS-Mini Management with UCS Central

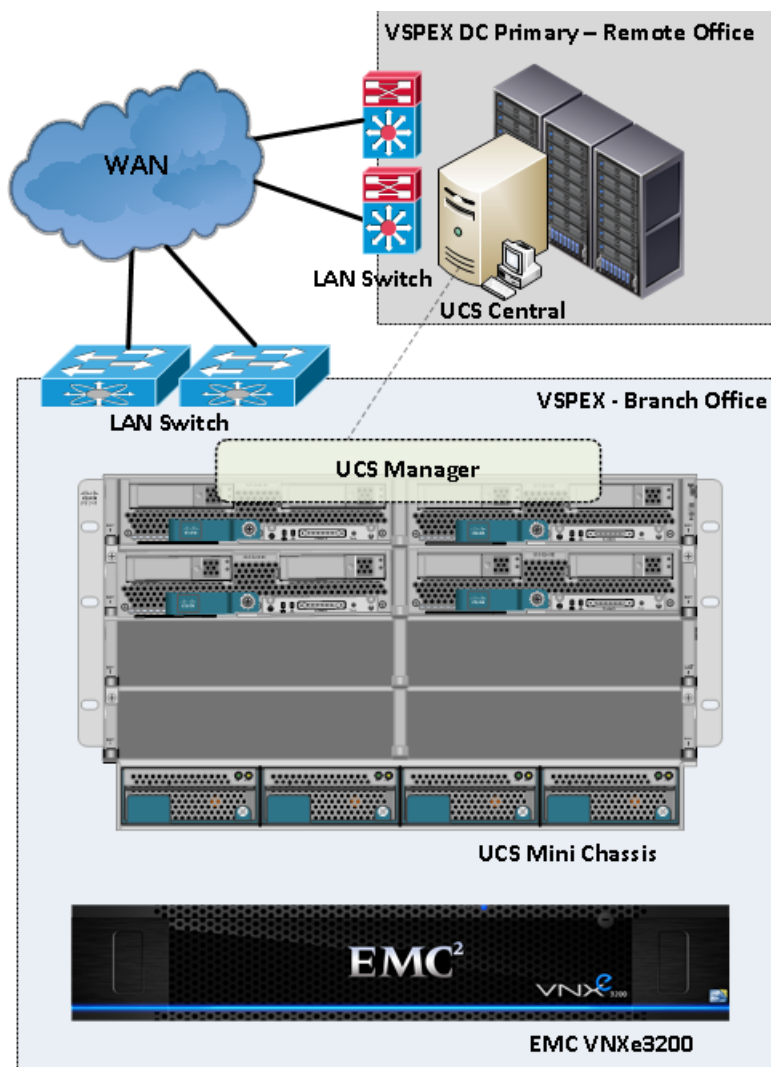
### Policy Based Management



## Architecture

This CVD discusses the deployment model of EMC VSPEX Private Cloud with Microsoft Hyper-V reference architecture for up to 100 virtual machines using EMC VNXe storage array in a Remote Office/Branch Office (ROBO) environments. This architecture uses the UCS direct-attach SAN feature where the EMC VNXe3200 storage array is directly connected to UCS 6324 fabric interconnect ports. Microsoft Windows Server 2012 R2 Hyper-V is used as server virtualization architecture.

**Figure 7** Architectural Overview of VSPEX Remote Office and Branch Office Solution



**Table 3** Hardware and Software Components of Cisco Branch office Solution for EMC VSPEX Microsoft Hyper-V architectures.

Vendor	Name	Version	Description
Cisco	UCSM	3.0(1c)	Cisco UCS Manager software
Cisco	UCS 6324UP FI	5.0(3)N2(3.01c)	Cisco UCS Fabric Interconnect firmware
Cisco	UCS 5108 AC2 Chassis	N/A	Cisco UCS Blade server chassis
Cisco	UCS B200 M3 servers	2.2.1a	Cisco B200 M3 blade server BIOS
Cisco	UCS VIC 1240	3.0(1c)	Cisco Virtual Interface card firmware



**Table 3** *Hardware and Software Components of Cisco Branch office Solution for EMC VSPEX Microsoft Hyper-V architectures.*

Vendor	Name	Version	Description
EMC	VNXe3200	3.0.0.2960754	EMC VNXe storage array
Microsoft	Windows Server 2012 R2	2012 R2 Datacenter Edition	Operating System with Hyper-V role for physical servers and Operating System for Virtual Machines

**Table 4** *Hardware and Software Components of Microsoft Hyper-V Architecture*

Component	Capacity
Memory (RAM)	256 GB (16 x 16 GB DIMM)
Processor	2 x Intel® Xenon® E5-2640 v2 CPUs, 2 GHz, 8 cores, 16 threads
Local Storage	Cisco UCS RAID SAS 2008M-8i Mezzanine Card

This SMB architecture assumes there is an existing infrastructure / management network available in which a virtual machine hosting Windows Active Directory/DNS/DHCP servers are present.

This design does not recommend or require any specific layout of infrastructure network. The AD/DNS/DHCP virtual machines are hosted on the infrastructure network. However, design does require accessibility of certain VLANs from the infrastructure network to reach the servers.

Hyper-V 2012 R2 is used as the hypervisor on each server and is installed on fiber channel SAN. The defined load is 32 virtual machines per Cisco UCS B200 M3 blade server.

## Memory Configuration Guidelines

This section provides guidelines for allocating memory to the virtual machines. The guidelines outlined here take into account Hyper-V memory overhead and the virtual machine memory settings.

## Hyper-V Memory Management Concepts

Microsoft Hyper-V has a number of advanced features to maximize performance, and overall resource utilization. The most important features relate to memory management. This section describes some of these features, and the items to consider when using these features in the VSPEX Private Cloud environment.

## Dynamic Memory

Dynamic Memory was introduced in Windows Server 2008 R2 SP1 to increase physical memory efficiency by treating memory as a shared resource, and dynamically allocating it to virtual machines. The amount of memory used by each virtual machine is adjustable at any time. Dynamic Memory

reclaims unused memory from idle virtual machines, which allows more virtual machines to run at any given time. In Windows Server 2012, Dynamic Memory enables administrators to dynamically increase the maximum memory available to virtual machines.

Dynamic memory pools all the physical memory available on a physical host and dynamically distributes it to virtual machines running on that host as the virtual machines need it. As workloads change, virtual machines will be able to dynamically ask for memory if it is needed or dynamically release memory if it is no longer needed without service interruptions.

Dynamic Memory requires that a virtual machine have a minimum and maximum size of virtual memory assigned. The virtual machine will never have less memory assigned to it than what is specified by the minimum and never ask for more than what is specified as the maximum. When a virtual machine is initialized, it is given the minimum amount specified. As processes are loaded, they create a demand for a specific amount of memory. If the virtual machine does not yet have enough physical memory assigned to it based on its demand, the hypervisor and SLAT (Secondary Level Address Translation). SLAT is a feature in the CPU which allocates more physical memory. to ensure optimal performance. If the virtual machine is no longer using memory, it uses a ballooning technique to free up unused physical memory to return to Hyper-V to be allocated to other virtual machines that need the memory.

One of the things that often happens is that when a machine, physical or virtual, is first starting, it may require more physical memory than it would require while it is running its normal tasks. This happens due to the many startup processes that are run to get the system running but then stop once they have performed their function. Therefore, Hyper-V also has a startup RAM setting that can be set larger than the minimum, thereby ensuring more memory at startup for a faster startup time. After the virtual machine has started and has its normal processes running, the ballooning technology will free any excess memory for use by other virtual machines.

In addition to the startup, minimum, and maximum settings offered by Hyper-V, it also allows two other settings to optimize memory usage. One setting is to specify the percentage of memory that Hyper-V should try to reserve as a buffer for the virtual machine. Then when the virtual machine has a demand for more physical memory, it can draw from this buffer instead going through the more intensive route of asking for new physical memory. This ensures a quicker response to memory demands within the virtual machine. The second setting is a memory weight that specifies how to prioritize memory demands for one virtual machine in relationship to the demands of other virtual machines. This allows for high-priority virtual machines to have their memory demands satisfied before lower priority virtual machines.

## Smart Paging

Even with Dynamic Memory, Hyper-V allows more virtual machines than the available physical memory can support. In most cases, there is a memory gap between minimum memory and startup memory. Smart Paging is a memory management technique that uses disk resources as temporary memory replacement. It swaps out less-used memory to disk storage, and swaps in when needed. Performance degradation is a potential drawback of Smart Paging. Hyper-V continues to use the guest paging when the host memory is oversubscribed because it is more efficient than Smart Paging.

## Non-Uniform Memory Access

Non-Uniform Memory Access (NUMA) is a multi-node computer technology that enables a CPU to access remote-node memory. This type of memory access degrades performance, so Windows Server 2012 employs a process known as processor affinity, which pins threads to a single CPU to avoid remote-node memory access. In previous versions of Windows, this feature is only available to the host. Windows Server 2012 extends this functionality to the virtual machines, which provides improved performance in symmetrical multiprocessor (SMP) environments.

## Allocating Memory to Virtual Machines

The proper sizing of memory for a virtual machine in VSPEX architectures is based on many factors. With the number of application services and use cases available determining a suitable configuration for an environment requires creating a baseline configuration, testing, and making adjustments, as discussed later in this paper. Table 4 outlines the resources used by a single virtual machine:

**Table 5** *Virtual Memory Details*

Characteristic	Value
Virtual processor per virtual machine (vCPU)	1
RAM per virtual machine	2 GB
Available storage capacity per virtual machine	100 GB
I/O operations per second (IOPS) per VM25	25
I/O pattern	Random
I/O read/write ratio	2:1

The following are descriptions of recommended best practices:

- **Account for memory overhead**—Virtual machines require memory beyond the amount allocated, and this memory overhead is per virtual machine. Memory overhead includes space reserved for integration
- **Services and other virtualization-related processes**—The amount of overhead is somewhat trivial, but it still needs to be factored in. VMs with 1 GB or less of RAM only use about 32 MB of memory for virtualization-related overhead. You should add 8 MB for every gigabyte of additional RAM. For example, a VM with 2 GB of RAM would use 40 MB (32 MB plus 8 MB) of memory for virtualization-related overhead. Likewise, a VM with 4 GB of memory would have 56 MB of memory overhead. Each running virtual machine also has an associated virtual machine worker process to coordinate management tasks for the virtual machine. This process uses a little less than 7 MB of memory. This memory and process overhead is in addition to the memory allocated to the virtual machine and must be available on the Hyper-V host.
- **Right-size memory allocations**—Over-allocating memory to virtual machines can waste memory unnecessarily, but it can also increase the amount of memory overhead required to run the virtual machine, thus reducing the overall memory available for other virtual machines. Fine-tuning the memory for a virtual machine is done easily and quickly by adjusting the virtual machine properties. Using Dynamic Memory helps ease the administration of this right-sizing.
- **Do not overcommit**—as the term 'overcommit' implies, this is trying to use more than is available. Just as you cannot pump 10 gigabits of data through a 1 Gbps network in one second, you cannot use more memory than what is physically available. Again, Dynamic Memory helps ease the administration of memory on a physical system that is running close to its memory capacity.
- **Monitor usage**—Hyper-V provides performance monitoring statistics for resources used by virtual machines. These statistics can be monitored from the host environment without the need to go into every virtual machine individually. Perform, a performance monitoring utility that is part of the operating system, provides these statistics in counters prefixed with the string 'Hyper-V'. For more information about monitoring performance on Hyper-V see [http://technet.microsoft.com/en-US/library/cc768535\(v=BTS.10\).aspx](http://technet.microsoft.com/en-US/library/cc768535(v=BTS.10).aspx)

In addition to accounting for the memory used by the virtual machines, you should also allow the host to have at least 2 GB for the parent partition. This partition includes processes for monitoring and managing the environment and features such as the built-in failover clustering capability. Additionally control information for the running of the virtual machines is also stored in this memory.

## Storage Guidelines

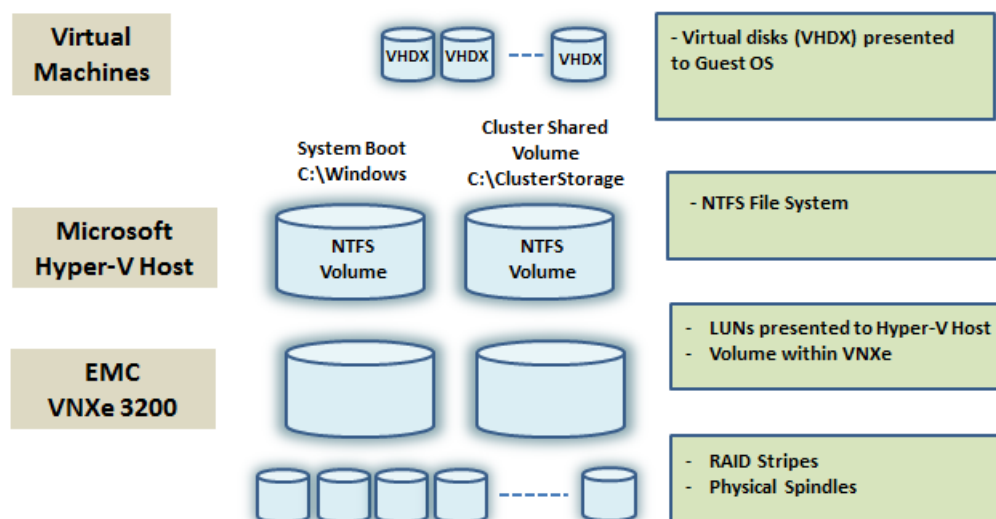
The VSPEX architecture used for this solution utilizes Fibre Channel to access the VNXe3200 storage array. The Hyper-V hosts boot from the SAN storage, ensuring stateless configuration for the individual Hyper-V hosts. If one of the Cisco UCS B200 M3 servers becomes unavailable for any reason, the service profile defining that server's configuration can be associated to another Cisco UCS B200 M3 server and boot from the same operating system image on the SAN without any reconfiguration to bring it into service. The shared storage for storing VMs and their data uses the same storage array and protocol, minimizing the management overhead associated with managing VM storage. VMs can access Fibre Channel LUNs directly (optional) using virtual HBAs in the VMs. Highly available failover clusters built with VMs can use either the virtual HBAs or simply shared virtual hard disks (VHDX) stored on the array.

## Virtual Server Configuration

Storage for Hyper-V can be categorized into three layers of storage technology:

- The storage array is the bottom layer consisting of physical disk spindles. These spindles are aggregated into RAID sets and then LUNs are defined on the RAID sets to present to the Hyper-V hosts.
- Storage array LUNs presented to the Hyper-V hosts. These are used for:
  - Boot volumes—operating system image used for booting the Hyper-V host
  - Cluster Shared Volumes—shared storage that is read/write accessible by all Hyper-V hosts configured in a Microsoft Failover Cluster
- Virtual disk files (VHDX) are created on the Cluster Shared Volumes and are used for multiple purposes:
  - Boot Volumes—guest operating system image used for booting a virtual machine
  - Data Volumes—data volumes required by applications
  - Share storage—shared volumes used by virtual machine guest clusters

**Figure 8** *Hyper-V Storage Virtualization Stack*



## Storage Protocol Capabilities

The EMC VNXe3200 provides Hyper-V and storage administrators with the flexibility to use the storage protocol that meets the requirements or standards of the business. This can be a single protocol data center-wide or multiple protocols for tiered scenarios. The EMC VNXe3200 can support Fibre Channel, iSCSI, and NFS protocols.

The Cisco solution for EMC VSPEX with Microsoft Hyper-V recommends a single protocol, Fibre Channel, throughout in order to simplify the design.

## Storage Best Practices

It is recommended that storage administrators become familiar with Microsoft's suggestions for performance tuning. They have published a document that can be found at:

<http://msdn.microsoft.com/en-us/library/windows/hardware/jj248719.aspx>

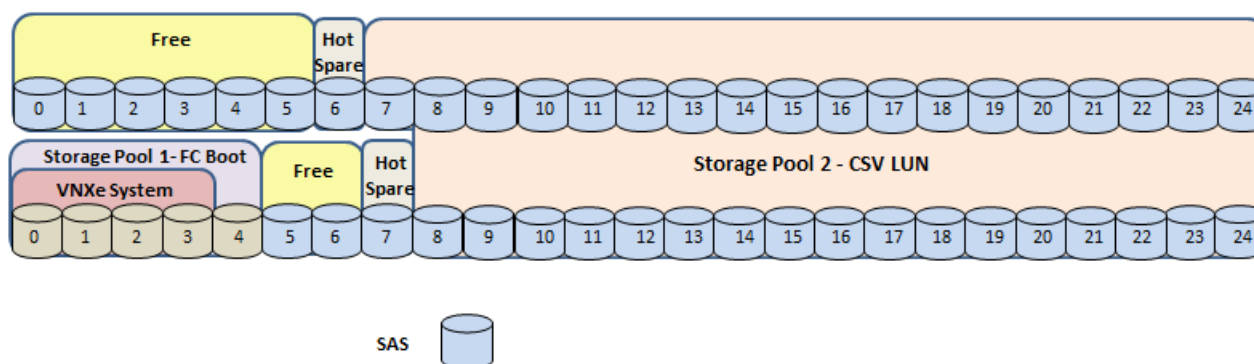
- **Multi-path**—having a redundant set of paths to the EMC VNXe3200 is critical to protecting the availability of the environment as well as ensuring the best performance. Microsoft provides built-in multi-path IO support as part of its operating system. EMC builds on top of this built-in capability to provide added functions with its PowerPath software.
- **Partition alignment**—in the past, it was often recommended to manually align partitions on disk volumes to ensure optimal performance. Since Windows Server 2008, Microsoft has taken the guess-work out of partition alignment. Microsoft Windows Server 2012 and later natively supports the 4K sector disks that are commonly available today and automatically aligns the partitions for optimal performance.
- **Shared storage**—Cluster Shared Volumes provide a high level of availability to the virtual machine environment. VHDX files (virtual hard disks) can be accessed from any node of the cluster (up to 64 nodes) with full read/write capability. If a node loses its physical connection to a CSV, it can still access the VHDX files via the network, ensuring uninterrupted service from that VM owning those VHDX files.

- Calculate total VM storage requirements—each virtual machine may require more space than the total of its VHDX files. One of the settings for a virtual machine is to take an automatic stop action; that is action to be performed if the host machine is gracefully shut down. One of the automatic stop actions often used is to save the virtual machine state. Ensure that enough space is available on disk when an automatic stop action is initiated, Hyper-V will create file on disk with enough space to save the memory contents of the virtual machine. For example, assume that you have a virtual machine with 8 GB of RAM allocated and a 40 GB VHDX system volume and a 50 GB VHDX data volume. If the automatic stop action for a virtual machine is to save the virtual machine state (the default setting), you will need to ensure that you have at least 98 GB of disk space available for this VM.
- Understand I/O requirements—Under-provisioned storage can significantly slow responsiveness and performance for applications. In a multi-tier application, you can expect each tier of application to have different I/O requirements. As a general recommendation, pay close attention to the amount of virtual machine disk files hosted on a single CSV. Over-subscription of the I/O resources can go unnoticed at first and slowly begin to degrade performance if not monitored proactively.

## Storage Layout

The architecture diagram in this section shows the physical disk layout. Disk provisioning on the VNXe3200 storage array is simplified through the use of wizards, so that administrators do not choose which disks belong to a given storage pool. The wizard may choose any available disk of the proper type, regardless of where the disk physically resides in the array.

**Figure 9** Storage Layout for Upto 100 Reference VMs on VNXe3200



The reference architecture uses the following configuration:

- Thirty five 600 GB SAS disks are allocated to a block based storage pool.
- Two 600 GB SAS disks are automatically reserved as hot spares by the array operating system.
- For block storage, allocate at least two LUNs to the Hyper-V Failover Cluster from a single storage pool to server as CSV.



**Note**

- Allocate at least one hot spare for every 30 disks of a given type and size.



**Note**

- System drives are specifically excluded from the pools and are not used for additional storage.

The VNXe series is designed for “five 9s” availability by using redundant components throughout the array. All of the array components are capable of continued operation in case of hardware failure. The RAID disk configuration on the array provides protection against data loss due to individual disk failures, and the available hot spare drives can be dynamically allocated to replace a failing disk.

## Networking Guidelines

The following are some recommended best practices for networking with Hyper-V:

- Fabric failover—always use the fabric failover feature of Cisco UCS VIC adapters for high-availability of network access.
- Separate virtual machine and host traffic—keep virtual machine and host traffic separate. This can be accomplished physically using separate virtual switches for VM networks that are defined on separate physical NICs or virtually using VLAN segmentation.

## Recommended NICs

The recommended and suggested networking for a Microsoft Hyper-V solution has the following NICs:

- Host (or infrastructure) management—used by the Hyper-V host for management functions.
- Live Migration—used by Hyper-V host for live migrating virtual machines. This is not a required network, but it is highly recommended to separate this traffic.
- Cluster Shared Volume—used by the Hyper-V host for managing the cluster shared volumes. This is not a required network, but it is highly recommended.
  - Normal operations—this network sees very little traffic. Each node in the cluster is directly accessing the CSV to read/write to the VHDX files in use by the virtual machines running on that node. The only traffic that passes over this network is what is known as 'metadata updates'. Metadata updates comprise file and directory creation/deletion/extension at the Hyper-V level. Most I/O is directly to the contents of the VHDX files in use by the VMs, and none of that is considered a metadata update. Metadata updates are handled by the node in the cluster that owns the LUN presented as a CSV.
  - Redirected mode—should a node of the cluster lose physical connectivity to a CSV, the CSV is set in redirected mode for that host. This means that read/write operations that would normally go directly to the CSV from the VM are redirected over the network designated as the CSV network to the node in the cluster that owns the LUN. This mode also may be initiated by backup programs.
- Virtual machine access—this network should be a separate network for accessing the resources of the virtual machines running on Hyper-V host. It is recommended that this network be defined as not available for use by the host. There should be a minimum of one virtual machine access network. Depending on your needs, you may require more.

## Quality of Service

It is recommended to define a quality of service for the Live Migration network to ensure optimal performance. If iSCSI and/or SMB networks are defined, it is recommended to define a quality of service for their use. In general, the QoS defined for storage will be different from the QoS defined for live migration.



## Service Profile Design

This architecture implements following design steps to truly achieve stateless computing on the servers:

- Service profiles are derived from service profile template for consistency.
- The Microsoft Hyper-V host uses the following identities:
  - Host UUID
  - MAC Addresses assigned to each vNIC on the server
  - One WWNN and two WWPN for FC boot
- All of these identifiers are defined in their respective identifier pools and the pool names are referred in the service profile template.
- Local disks are NOT used for booting. Boot policy in service profile template suggests host to boot from the storage devices using FC protocol.
- Server pool is defined with automatic qualification policy and criteria. Blade servers are automatically put in the pool as and when they are fully discovered by UCSM. This eliminates the need to manually assign servers to server pool.
- Service profile template is associated to the server pool. This eliminates the need to individually associating service profiles to physical servers.

Given this design and capabilities of UCS and UCSM, a new server can be procured within minutes if the scale needs to be increased or if a server needs to be replaced by different hardware. In case, if a server has physical fault (faulty memory, or PSU or fan, for example), using following steps, a new server can be provisioned within minutes:

- Put the faulty server in maintenance/drain mode. This would move VMs running on fault server to other healthy servers on the cluster.
- Disassociate the service profile from the faulty server and physically remove the server for replacement of faulty hardware (or to completely remove the faulty server).
- Physically install the new server on the chassis. Let the new server be discovered by UCSM.
- Associate the service profile to the newly deployed blade server. This would boot the same Microsoft Hyper-V server image from the storage array as what the faulty server was running.
- The new server would assume the role of the old server with all the identifiers intact. You can now end the maintenance mode of the Microsoft Hyper-V host.

Thus, the architecture achieves the true statelessness of the computing in the data center. If there are enough identifiers in all the id-pools, and if more servers are attached to UCS system in future, more service profiles can be derived from the service profile template and the private cloud infrastructure can be easily expanded.

## Network High Availability Design

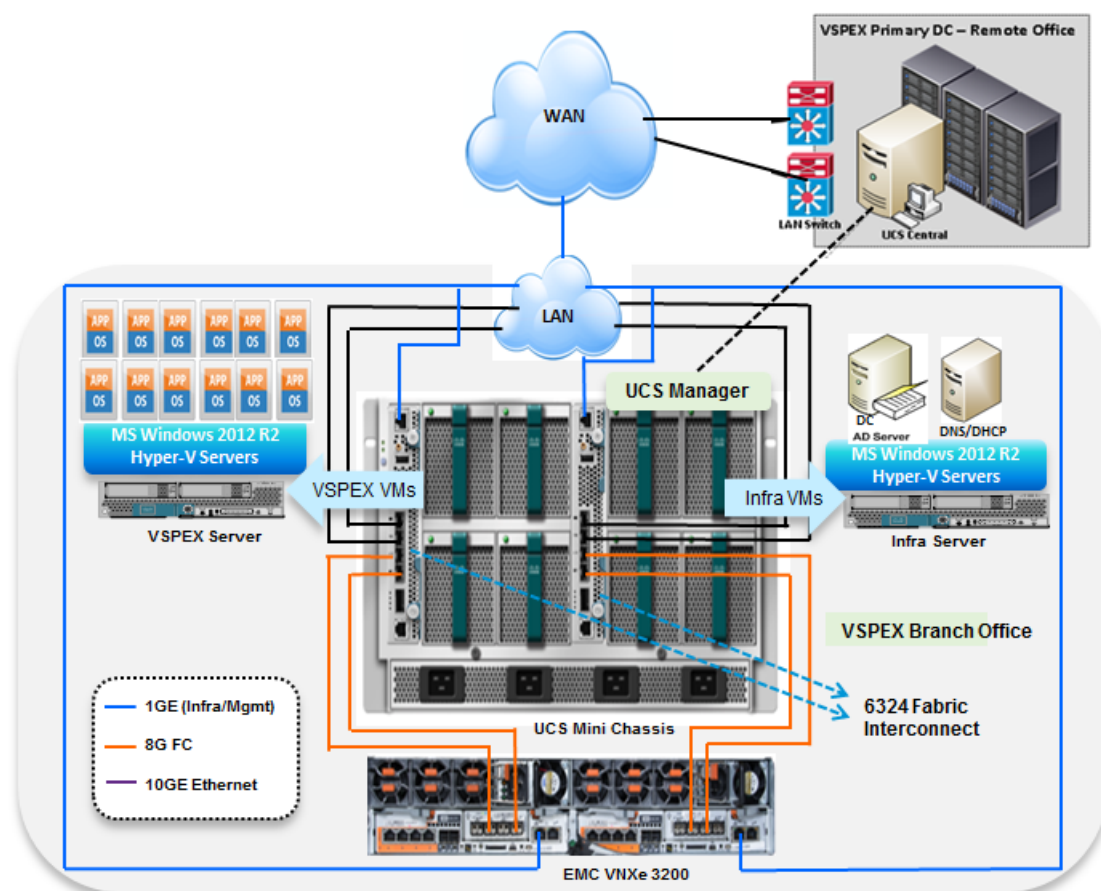
Following figure demonstrates logical layout of the architecture. Following are the key aspects of this solution:

- Cisco UCS B200 M3 servers are used, managed by UCS Manager/UCS Central.
- VNICs on fabric A and fabric B with failover are used for host management and Hyper-V cluster traffic.

Storage is made highly available by deploying following practices:

- FC access is for booting each of the Microsoft Hyper-V host and also for storing virtual machines in cluster shared volumes.
- VNXe storage arrays provide two Storage Processors (SPs): SP-A and SP-B for FC (Block)

**Figure 10** *Logical Layout of Branch Office Solution for NFS Based Architecture*



## Jumbo MTU

Jumbo MTU (size 9000) is used for following two types of traffic in this architecture:

- Live Migration traffic, and
- CSV traffic

Both of these traffic types are “bulk transfer” traffic, and larger MTU significantly improves the performance. Jumbo MTU must be configured end-to-end to ensure that IP packets are not fragmented by intermediate network nodes. Following is the checklist of end-points where jumbo MTU needs to be configured:

- System QoS classes in UCS Manager
- vNICs in service profiles
- Network adapters used for Live Migration and CSV traffic on the Hyper-V hosts.

Next sub section goes in to sizing guidelines of the Cisco Branch solution for EMC VSPEX Microsoft Hyper-V architectures outlined here.

## Sizing Guidelines

In any discussion about virtual infrastructures, it is important to first define a reference workload. Not all servers perform the same tasks, and it is impractical to build a reference that takes into account every possible combination of workload characteristics.

### Defining the Reference Workload

To simplify the discussion, a representative customer reference workload is defined as a virtual machine with specific characteristics. By comparing the actual customer usage to this reference workload, one can extrapolate which reference architecture to choose.

For the VSPEX solutions, the reference workload was defined as a single virtual machine. This virtual machine has the following characteristics.

**Table 6** *Reference Virtual Machine Workload*

Characteristic	Value
Virtual machine operating system	Microsoft Windows Server 2012 R2
Virtual processor per virtual machine (vCPU)	1
RAM per virtual machine	2 GB
Available storage capacity per virtual machine	100 GB
I/O operations per second (IOPS) per VM	25
I/O pattern	Random
I/O read/write ratio	2:1

This specification for a virtual machine is not intended to represent any specific application. Rather, it represents a single common point of reference to measure other virtual machines.

### Applying the Reference Workload

When considering an existing server which will move into a virtual infrastructure, you have the opportunity to gain efficiency by right-sizing the virtual hardware resources assigned to that system.

The reference architecture creates a pool of resources sufficient to host a target number of reference virtual machines as described above. It is entirely probable that customer virtual machines will not exactly match the specifications above. In that case, you can say that a single specific customer virtual machine is the equivalent of some number of reference virtual machines, and assume that number of virtual machines have been used in the pool.

You can continue to provision virtual machines from the pool of resources until it is exhausted. Consider these examples:

## Example 1 - Customer Built Application

A small custom-built application server will move into this virtual infrastructure. The physical hardware supporting the application is not being fully utilized at present. A careful analysis of the existing application reveals the application uses only one processor and needs 3 GB of memory to run efficiently. The IO workload ranges between 4 IOPS at idle time to 15 IOPS when busy. The entire application is only using about 30 GB on local hard drive storage.

The following resources are needed from the resource pool to virtualize this application:

- CPU resources for 1 VM
- Memory resources for 2 VMs
- Storage capacity for 1 VM
- IOPS for 1 VM

In this example a single virtual machine uses the resources of two reference virtual machines. When this VM is deployed, the solution's remaining capability would be 98 VMs.

## Example 2 - Point of Sale System

The database server for a customer's point-of-sale system will move into this virtual infrastructure. It is currently running on a physical system with four CPUs and 16 GB of memory. It uses 200 GB storage and generates 200 IOPS during an average busy cycle.

The following resources are needed from the resource pool to virtualize this application:

- CPUs of 4 reference VMs
- Memory of 8 reference VMs
- Storage of 2 reference VMs
- IOPS of 8 reference VMs

In this example, the one virtual machine uses the resources of eight reference virtual machines. Once this VM is deployed, the solution's remaining capability would be 92 VMs.

## Example 3 - Web Server

The customer's web server will move into this virtual infrastructure. It is currently running on a physical system with two CPUs and 8GB of memory. It uses 25 GB of storage and generates 50 IOPS during an average busy cycle.

The following resources are needed from the resource pool to virtualize this application:

- CPUs of 2 reference VMs
- Memory of 4 reference VMs
- Storage of 1 reference VMs
- IOPS of 2 reference VMs

In this example the virtual machine would use the resources of four reference virtual machines. Once this VM is deployed, the solution's remaining capability would be 96 VMs.

## Example 4 - Decision Support Database

The database server for a customer's decision support system will move into this virtual infrastructure. It is currently running on a physical system with 10 CPUs and 48 GB of memory. It uses 5 TB of storage and generates 700 IOPS during an average busy cycle.

The following resources are needed from the resource pool to virtualize this application:

- CPUs of ten reference VMs
- Memory of 24 reference VMs
- Storage of 50 reference VMs
- IOPS of 28 reference VMs

In this example the one virtual machine uses the resources of fifty reference virtual machines. When this VM is deployed, the solution's remaining capability would be 50 VMs.

## Summary of Examples

The four examples show the flexibility of the resource pool model. In all four cases the workloads simply reduce the number of available resources in the pool. If all four examples were implemented on the same virtual infrastructure, with an initial capacity of up to 100 virtual machines, they would leave a capacity for 236 reference virtual machines in the resource pool.

In more advanced cases, there may be trade-offs between memory and I/O or other relationships where increasing the amount of one resource, decreases the need for another. In these cases, the interactions between resource allocations become highly complex and are out of the scope of this document. However, when a change in the resource balance is observed, and the new level of requirements is known; these virtual machines can be added to the infrastructure using the method described in the above examples.

If the customer does not have a thorough understanding of the resource needs of their particular environment, Microsoft has a free tool, Microsoft Assessment and Planning Toolkit, which can be run against the customer environment to capture the actual characteristics. This tool is available at: [www.microsoft.com/map](http://www.microsoft.com/map).

## VSPEX Configuration Guidelines

Following are the deployment and configuration steps for the Cisco UCS Mini Branch Office for EMC VSPEX solution:

1. Pre-deployment tasks
2. Connect network cables
3. Prepare UCS FIs and configure UCSM
4. Prepare the EMC VNXe3200
5. Install Microsoft Windows Server 2012 R2 Datacenter Edition
6. Configure MPIO
7. Create Hyper-V Cluster

Next sub-sections detail each of these sections mentioned above.

## Pre-deployment Tasks

The pre-deployment tasks include procedures that do not directly relate to environment installation and configuration, but whose results will be needed at the time of installation. Examples of pre-deployment tasks are collection of host names, IP addresses, VLAN IDs, license keys, installation media, and so on. These tasks should be performed before the customer visit to decrease the time required onsite.

**Gather documents**—Gather the vendor product installation documents. These are used throughout the text of this document to provide detail on setup procedures and deployment best practices for the various components of the solution.

**Gather tools**—Gather the required and optional tools for the deployment. Use Table 7 to confirm that all equipment, software, and appropriate licenses are available before the deployment process.

**Gather data**—Collect the customer-specific configuration data for networking, naming, and required accounts. Enter this information into the Customer Configuration Data worksheet for reference during the deployment process.

**Table 7** *Hardware and Software Requirements*

Requirement	Description	Reference
Hardware	Cisco UCS Mini chassis with 6324 Fabric Interconnect for network and compute infrastructure	See corresponding product documentation
	Cisco UCS B200 M3 servers to host virtual machines	
	EMC VNXe3200 storage: Multiprotocol storage array with the required disk layout as per architecture requirements	
Software	Microsoft Windows Server 2012 R2 installation media	See corresponding product documentation
	EMC VNXe3200 array licenses	

## Customer Configuration Data

To reduce onsite time, information such as IP addresses and hostnames should be assembled as part of the planning process. The [Customer Configuration Data Sheet, page 170](#) provides a table to maintain a record of relevant information. This form can be expanded or contracted as required, and information may be added, modified, and recorded as deployment progresses.

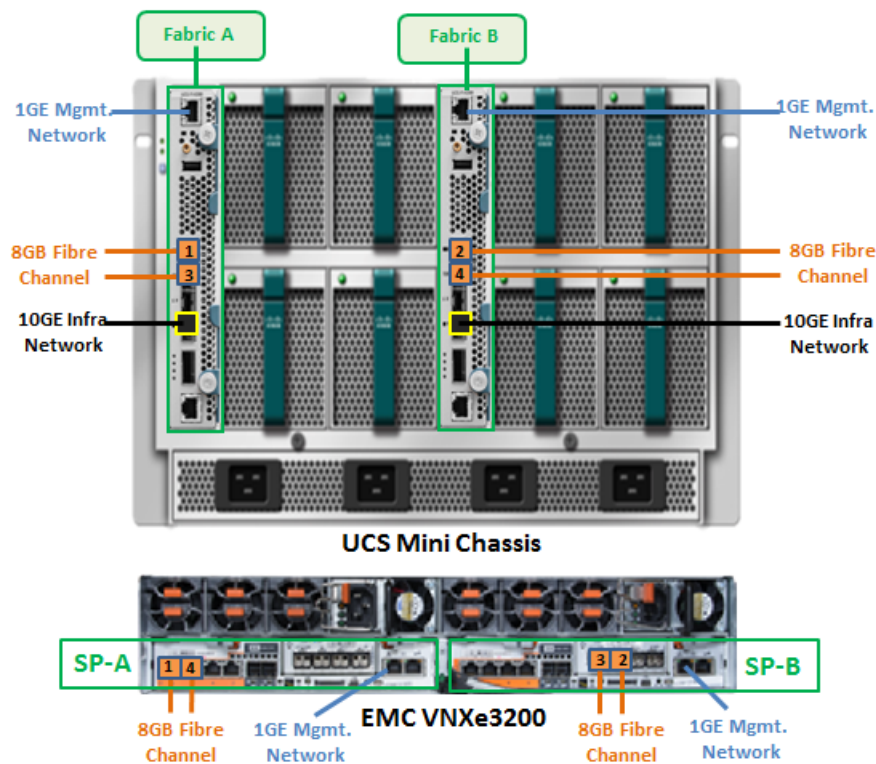
Additionally, a complete Customer Configuration Data Sheet is available on the EMC online support website, to provide the most comprehensive array-specific information.

## Connect Network Cables

See the Cisco UCS Mini Chassis, 6324 FI, B200M3 server and EMC VNXe3200 storage array configuration guide for detailed information about how to mount the hardware on the rack. Following diagrams show connectivity details for the VSPEX Microsoft Hyper-V architecture covered in this document.

- Connect FC port 1on UCS FAB-A to FC port 1 on EMC VNXe3200 SP-A
- Connect FC port 2on UCS FAB-B to FC port 2 on EMC VNXe3200 SP-B
- Connect FC port 3on UCS FAB-A to FC port 3 on EMC VNXe3200 SP-B
- Connect FC port 4on UCS FAB-B to FC port 4 on EMC VNXe3200 SP-A
- Connect the Infra and the management ports to the upstream Ethernet switch.

### Cabling Diagram for UCS Mini and VNXe Array System-Port Description



## Prepare UCS FIs and Configure UCS Manager

Next step is to configure UCS FIs and UCSM. This task can be subdivided in to following segments:

1. Initial configuration of UCS FIs.
2. Configuration for server discovery on UCS Manager.
3. Upstream/global network configuration.
4. Configure identifier pools.
5. Configure server pool and qualifying policy.
6. Configure service profile template.
7. Instantiate service profiles from the service profile template.
8. Follow the step-by-step guide to configure UCSM tasks mentioned above.



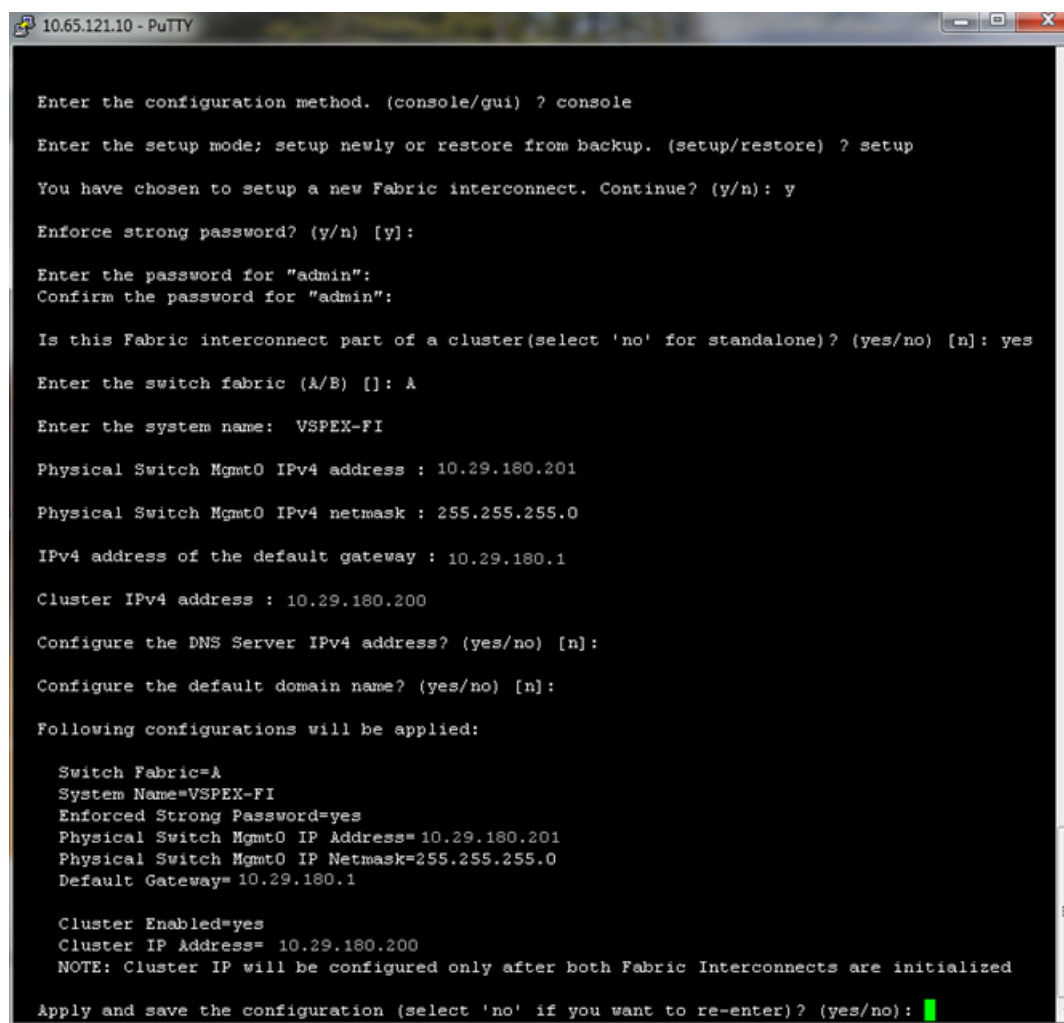
## Initial Configuration of Cisco Unified Computing System

At this point of time, mount the UCS 6324 FIs and the UCS chassis with B200 M3 Blade Servers on the rack and make sure that the cable connections are appropriate as suggested in this section. Two 100 Mbps Ethernet cables must be connected between two FIs for management pairing. Two redundant power supplies are provided per FI, it is highly recommended that both are plugged in, ideally drawing power from two different power sources. Connect mgmt0 interfaces of each FI to the infrastructure network, and put the switch port connected to FI in access mode with access VLAN as management VLAN. Now follow these steps to perform initial configuration of FIs:

1. Attach RJ-45 serial console cable to the first FI, and connect the other end to the serial port of laptop. Configure password for the “admin” account, fabric ID “A”, UCS system name, management IP address, subnet mask and default gateway and cluster IP address (or UCSM Virtual IP address), as the initial configuration script walks you through the configuration (see Figure 12).

Save the configuration and this would eventually lead to UCSM CLI login prompt.

**Figure 12** UCS Manager Initial Configuration



```

10.65.121.10 - PuTTY

Enter the configuration method. (console/gui) ? console
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]:
Enter the password for "admin":
Confirm the password for "admin":
Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes
Enter the switch fabric (A/B) []: A
Enter the system name: VSPEX-FI
Physical Switch Mgmt0 IPv4 address : 10.29.180.201
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.29.180.1
Cluster IPv4 address : 10.29.180.200
Configure the DNS Server IPv4 address? (yes/no) [n]:
Configure the default domain name? (yes/no) [n]:
Following configurations will be applied:
Switch Fabric=A
System Name=VSPEX-FI
Enforced Strong Password=yes
Physical Switch Mgmt0 IP Address=10.29.180.201
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=10.29.180.1
Cluster Enabled=yes
Cluster IP Address= 10.29.180.200
NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):
  
```

- Now, disconnect the RJ-45 serial console from Fabric Interconnect (FI) that you configured and attach it to the other FI. The Other FI would detect its peer that has been configured, and prompts you to join the cluster. The requirement information that you need to provide are FI specific management IP address, subnet mask and default gateway (see Figure 13).

**Figure 13** *Specify Management IP, Subnet Mask and Default Gateway*

```

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:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IP Address: 10.29.180.202
Peer Fabric interconnect Mgmt0 IP Netmask: 255.255.255.0
Cluster IP address      : 10.29.180.200

Physical Switch Mgmt0 IPv4 address : 10.29.180.201

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): █

```

- Once the initial configuration on both FIs are completed, you can disconnect the serial console cable. The UCSM will now be accessible through web interface (<https://<ucsm-virtual-ip>>) or SSH. Connect to UCSM using SSH, and check the HA status. As there is a common device connected between two FIs, the status would say “HA NOT READY”, but you must check if both FI A and FI B are in “Up” state (see Figure 14).

**Figure 14** *Checking HA Status*

```

VSPEX-FI-A# show cluster state
Cluster Id: 0xec91409a491011e2-0xb7a4547feeaa1564

A: UP, PRIMARY
B: UP, SUBORDINATE

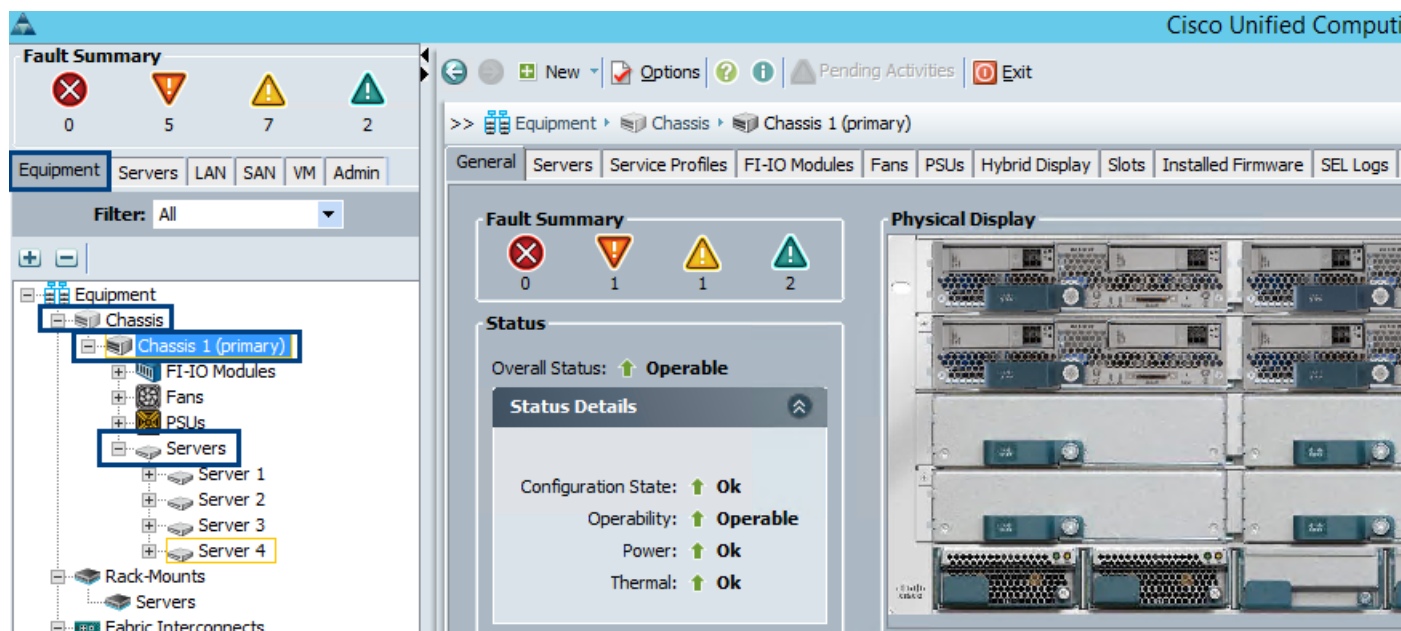
HA NOT READY
No device connected to this Fabric Interconnect
VSPEX-FI-A# █

```

## Chassis and Server Discovery on UCS Manager

After configuring the FI management IP, use the Virtual IP address to launch the UCS Manager via web browser. You will see the chassis discovered automatically under **Equipment** tab and the status will be shown as “operable” in the Status area in the right pane.

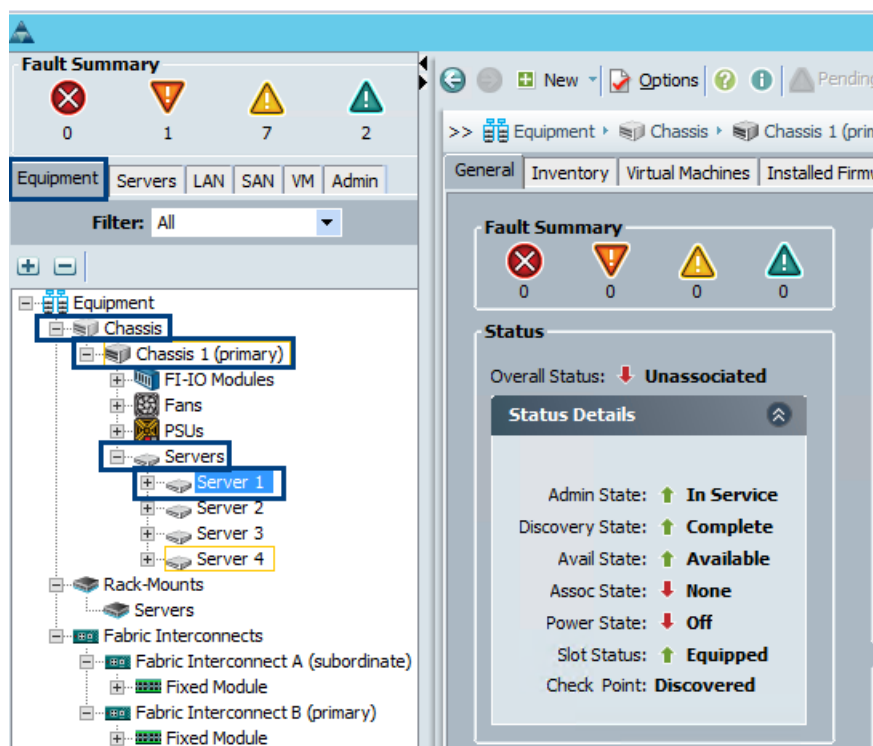
Figure 15 Chassis Discovery Policy



Also, you will see four blades discovered automatically under **Equipment** tab. The overall status is shown as **Unassociated** while the availability status displays as **Available**, and the discovery status displays as **Complete** (see Figure 16):

1. In **Equipment** tab, choose **Equipment** > **Chassis** > **Chassis <id>** **Servers** (see Figure 16).

Figure 16 Server Association State



## Creating VSPEX Private Cloud Environment with Cisco UCS Manager

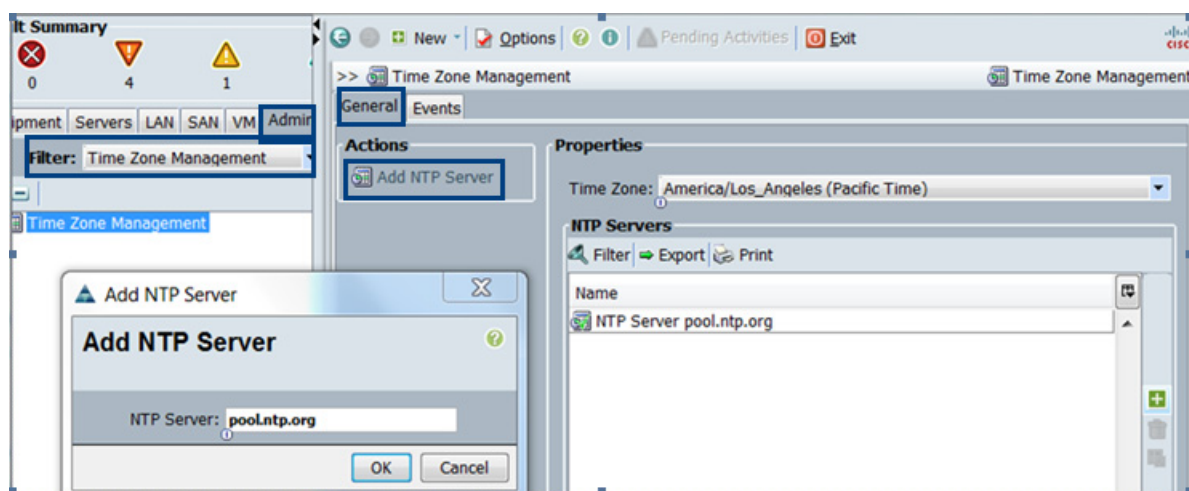
The following steps explain configuration details for the VSPEX Private Cloud environment.

### Synchronizing Cisco UCS to NTP

Follow the steps given below to synchronize Cisco UCS environment to the NTP server:

1. Select **Admin** tab and choose **All > Time Zone Management**.
2. From the right pane, Choose a timezone from the **Time Zone** drop-down list.
3. Click **Add NTP Server** and click **OK** to save the changes.

Figure 17 Adding NTP Server

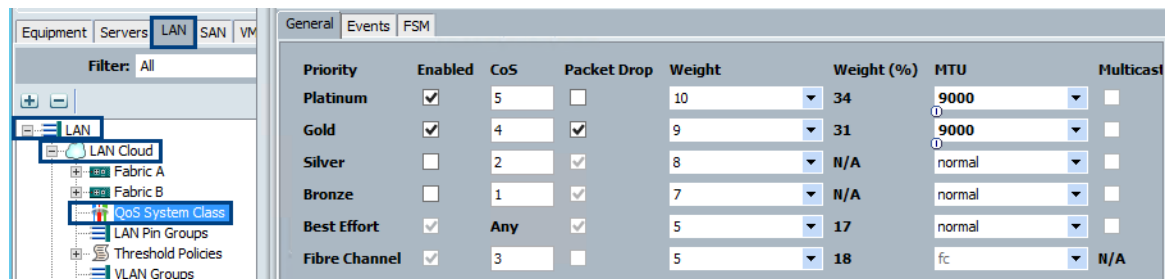


### Enable Quality of Service in Cisco UCS Fabric

Follow the steps given below to enhance the service quality in the Cisco UCS Fabric and set Jumbo frames that are applied later to Live Migration and CSV traffic.

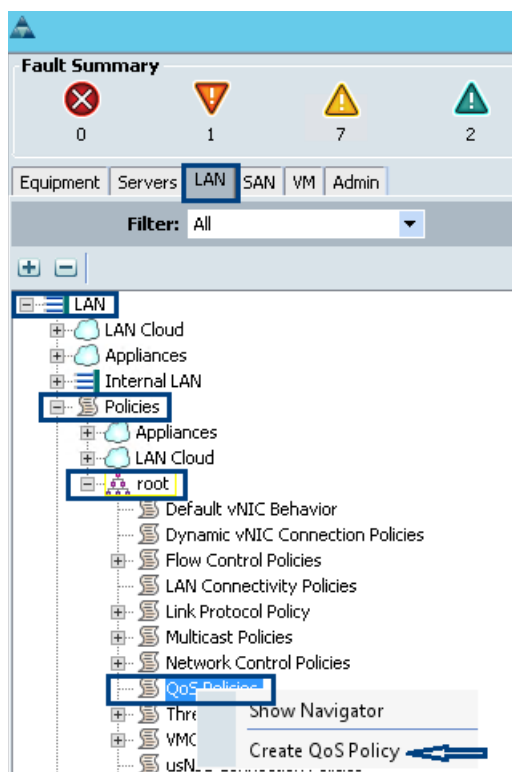
1. Select **LAN** tab and choose **LAN Cloud > QoS System Class**.
2. From the right pane, choose **General** tab.
3. In the **Platinum**, **Gold**, and **Best Effort** fields, type 9000 in the MTU boxes.
4. Click **Save Changes** and click **OK** to continue.

Figure 18 Defining QoS System Class



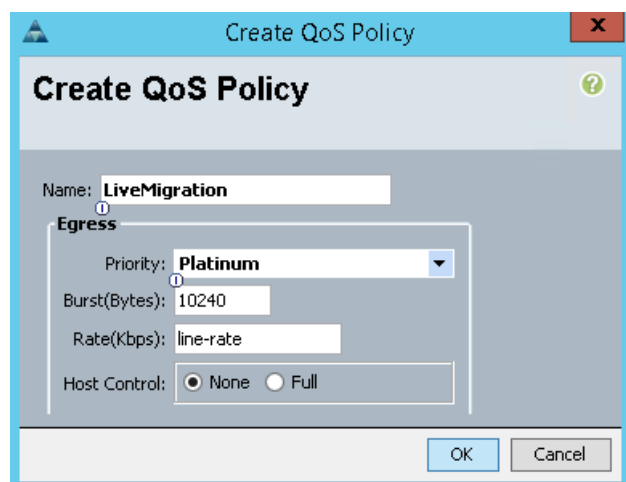
5. Choose **LAN** tab from the left pane and choose **LAN > Policies > Root**.
6. Right-click the **QoS Policies** option and choose **Create QoS Policy**.

**Figure 19** *Creating QoS Policy*



7. Enter **<LiveMigration>** as the QoS Policy name.
8. Change the Priority to **Platinum**. Leave Burst (Bytes) set to 10240. Leave Rate (Kbps) set to line-rate.
9. Keep the Host Control radio button to **None** and click **OK**.

**Figure 20** *Creating QoS Policy for LiveMigration*



10. Follow the above steps to create another QoS policy with 'CSV' and 'Gold' as priority.

## Upstream/Global Network Configuration

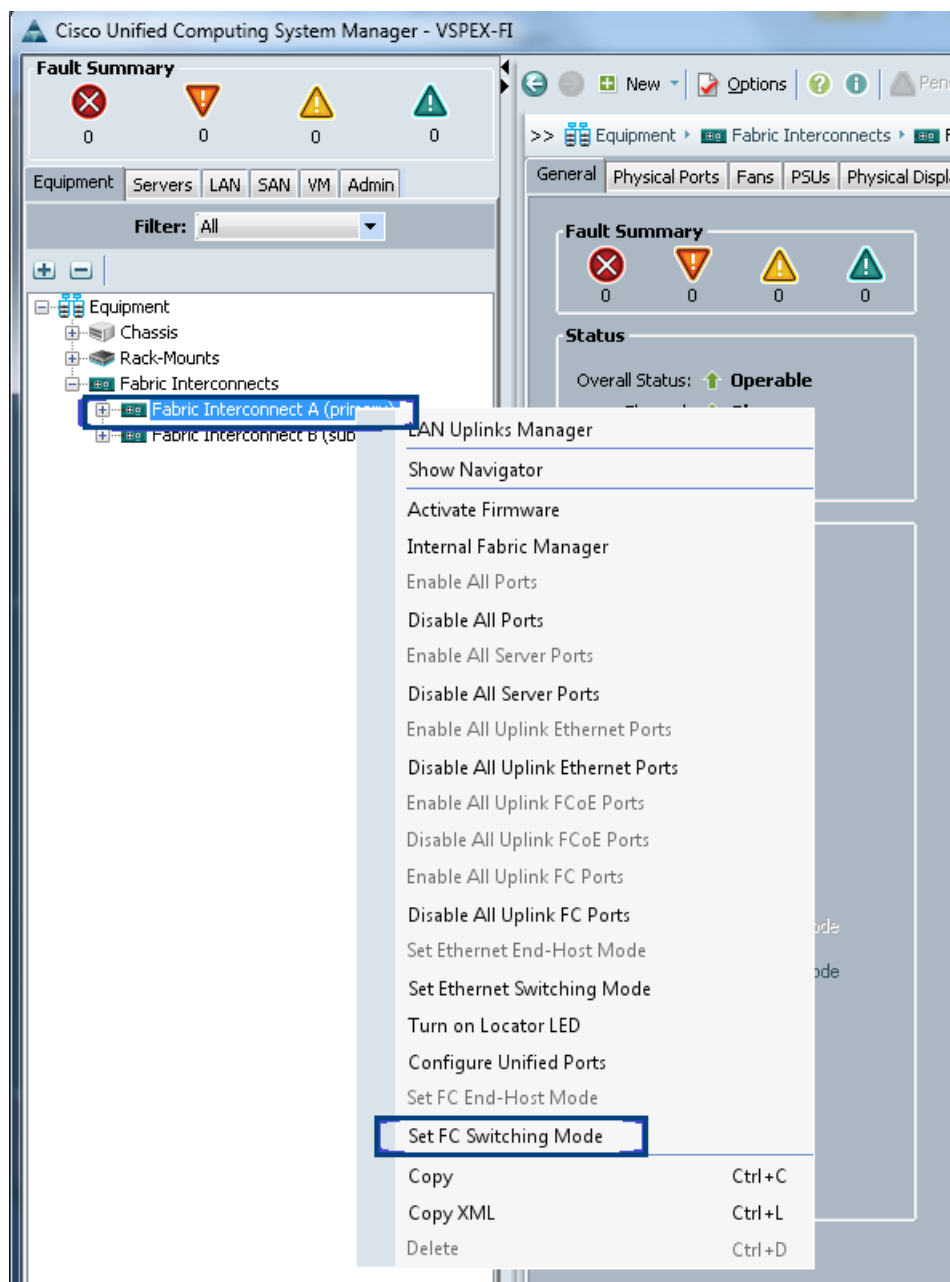
The following steps explain the upstream/global network configuration:

1. Move to FC switching mode
2. Uplink VLAN configuration
3. Configure universal ports as FC ports
4. Configure uplink ports
5. Configure FC appliance ports
6. Configure FC Zoning policies
7. Configure QoS classes and QoS policy for jumbo MTU

Follow these steps for network configuration:

1. From the **Equipment** tab, select and right-click **Fabric Interconnect A**, and choose **Set FC Switching Mode** (see Figure 21).

**Figure 21**      *Setting Cisco UCS FI to FC Switching Mode*



2. You will see a warning message that Fabric Interconnects (FI) will reboot as a result of this action. Click **Yes**. The FIs would reboot (first the secondary FI and then the primary FI).



**Note**

This reboot action is traffic disruptive, so make sure that you perform this operation during maintenance window, if you are working on a production environment.

## Create VLANs

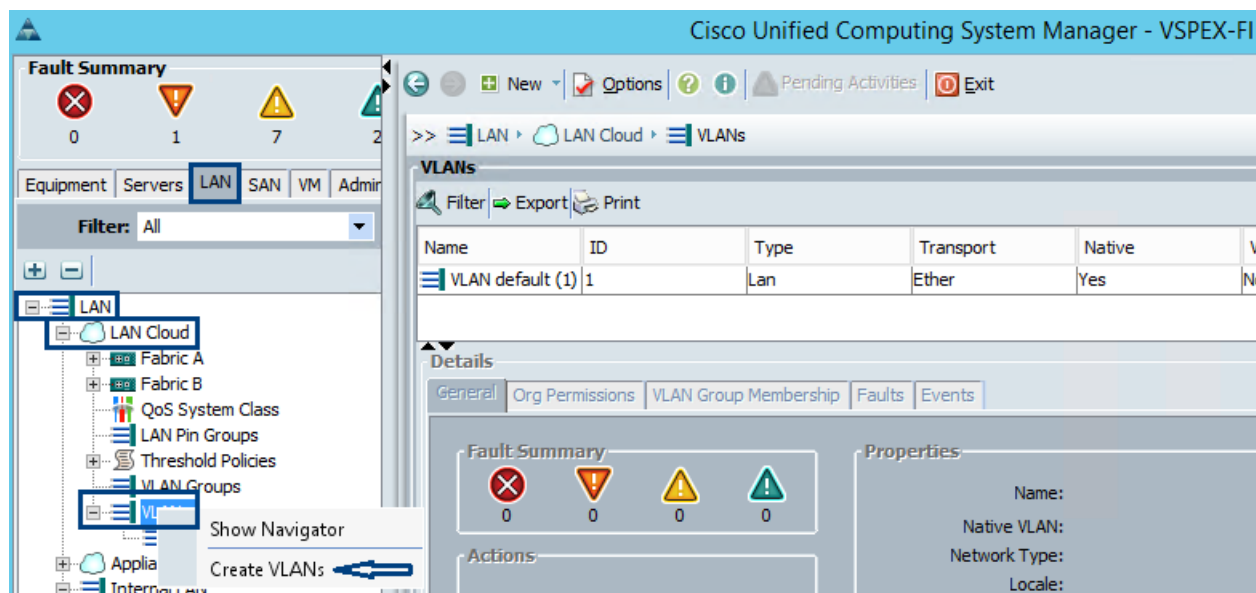
The following steps provide the necessary configuration details for VLANs in the Cisco UCS environment.

**Table 8** *VLAN Names and IDs Used in this Document*

VLAN Name	VLAN Purpose	VLAN ID
Default	VLANs to which untagged frames are assigned	1
VMaccess	VM access	20
LM	Hyper-V Live Migration	30
CSV	Cluster Shared Volume	40
Mgmt	Host management interface	50

1. Choose **LAN** tab,
2. Expand LAN and choose **LAN Cloud**
3. Right-click the **VLANs**, and choose **Create VLANs**

**Figure 22** *Creating VLANs*



4. Provide a name to the VLAN and assign an identification number. Keep the default option **Common/Global** radio button selected and Sharing Type value as None.



**Figure 23**      *Creating VLANs for VMaccess*

5. Click **OK**.
6. Repeat these steps to create VLANs for Live Migration, CSV and Management traffic as listed in Table 8.

## Create VSANs

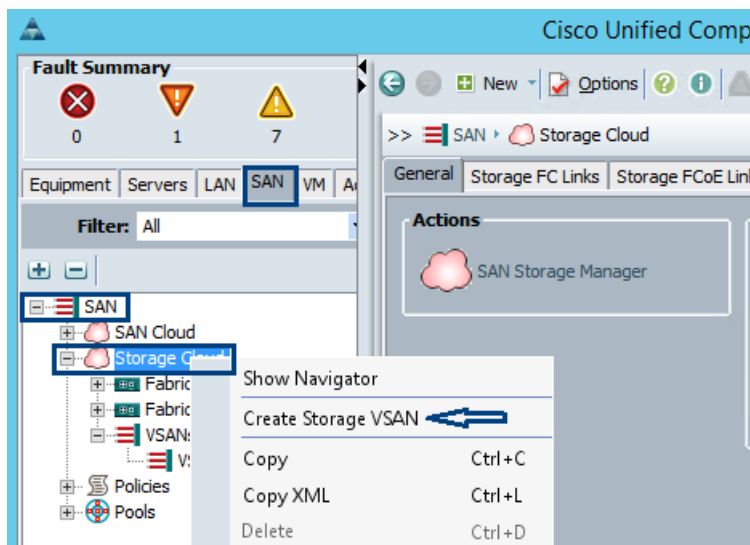
The following steps provide the necessary configuration details for VSANs in the Cisco UCS environment.

**Table 9**      *Create VSANs*

VSAN Name	VSAN Purpose	VSAN ID	FCoE VLAN ID
Storage	FC Storage Access	10	10

1. Choose **SAN** tab,
2. Expand **Storage Cloud** folder and choose **VSANs**.
3. Right-click VSANs, and choose **Create Storage VSAN**

Figure 24 Create VSAN



4. Provide a name for VSAN, enable FC zoning, provide VSAN ID and corresponding FCoE VLAN ID.

**Note**

The FCoE VLAN ID should not conflict with the VLANs configured earlier.

Figure 25 Creating Storage VSAN

**Create Storage VSAN**

Name:

**FC Zoning Settings**

FC Zoning: ☐ Disabled ☒ Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

You are creating a global VSAN that maps to the same VSAN ID in all available fabrics.

Enter the VSAN ID that maps to this VSAN.

VSAN ID:

A VLAN can be used to carry FCoE traffic to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN:

## Configuring Ports on UCS Fabric Interconnects

The Cisco UCS 6324UP Fabric Interconnects (FI) has four Universal Ports. By default, four physical ports on the FI are unconfigured, but can be converted to Fibre-Channel ports, Ethernet ports, Appliance Ports and FC/FCoE Storage ports. For this design, port 4 is configured as the Network Uplink Port (for LAN connection), ports 1 and 2 as FC Storage ports for direct connect of VNXe array for SAN boot and shared LUNs for CSV.



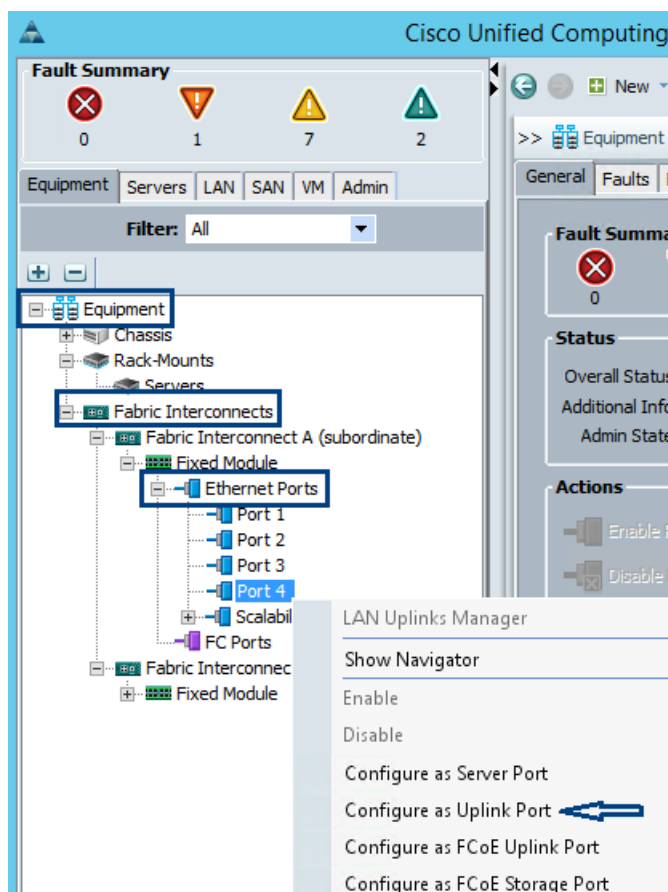
### Note

On the 6324 Fabric Interconnect, converting the Unified Port into FC ports is supported only starting from port 1, not from port 4. For information about Configuring the FC storage port on Fabric Interconnect, see [Configure Unified Ports for Fibre Channel, page 44](#).

## Configure Uplink Ports

1. Choose **Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module**.
2. Expand the **Unconfigured Ethernet Ports** section.
3. Choose the ports that are connected to the Cisco UCS chassis.
4. Click **Reconfigure**, and then choose that configuration as **Uplink Port** from the drop-down list.

Figure 26 Configuring Uplink Ports



5. A prompt displays. Click **Yes**, then **OK** to continue.
6. Repeat for Fabric Interconnect B.

## Configure Unified Ports for Fibre Channel

These steps provide details for modifying an unconfigured Ethernet port into FC uplink ports in the Cisco UCS environment and followed by configuring these FC ports to FC Storage ports for direct connect of FC-based storage array to the Fabric Interconnects.

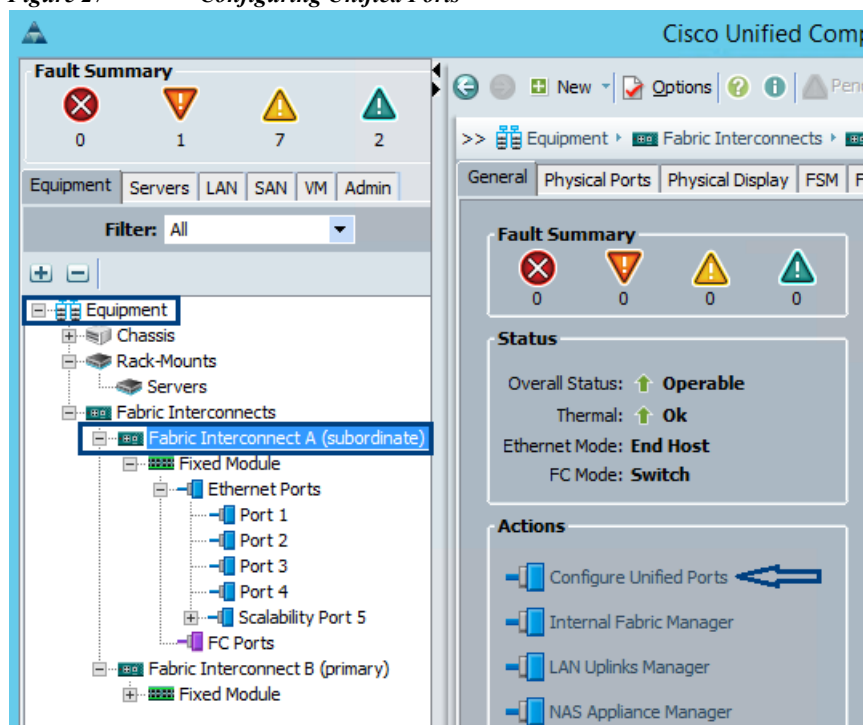


### Note

Modification of the unified ports on the built-in ports leads to a reboot of the Fabric Interconnect being modified.

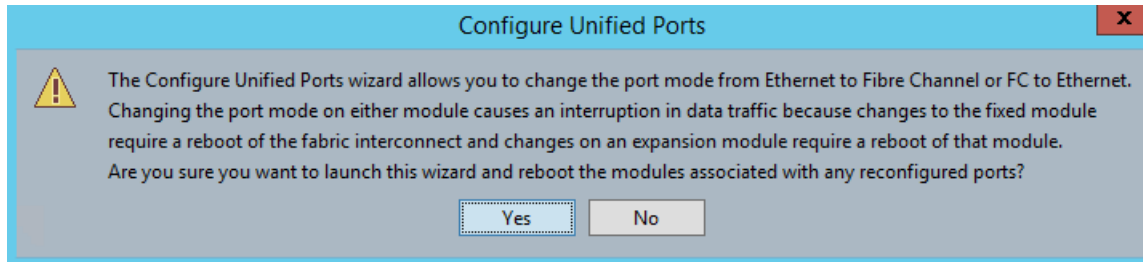
1. Navigate to the **Equipment** tab in the left pane and choose **Fabric Interconnect A**.
2. In the right pane, choose the **General** tab.
3. Choose **Configure Unified Ports**.

Figure 27 Configuring Unified Ports



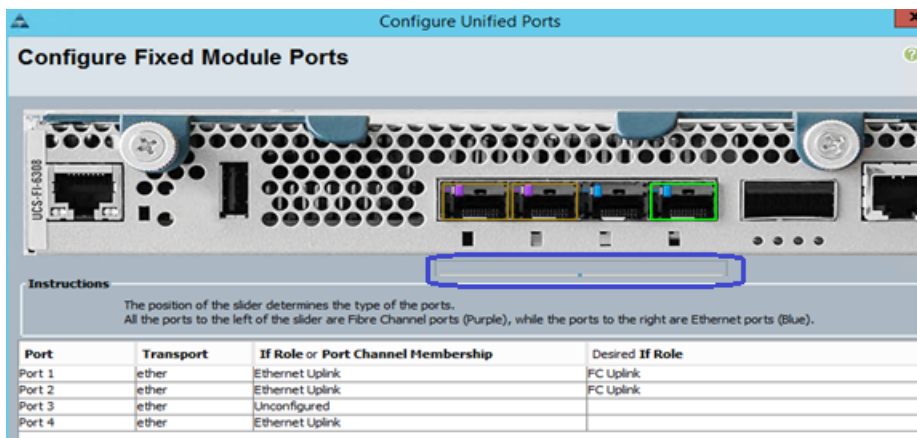
4. Choose **Yes** to launch the wizard.

**Figure 28** Confirmation to Launch Wizard



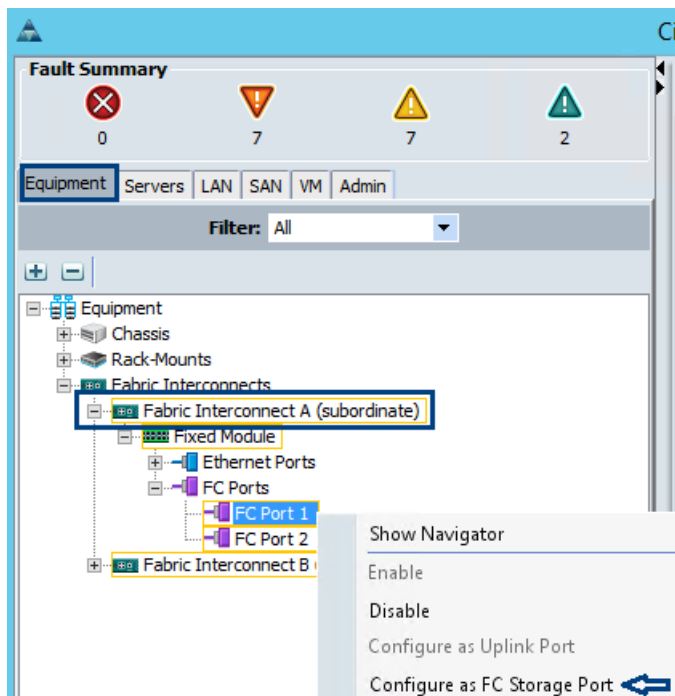
5. Use the slider tool and move two positions to the right to configure the first two ports (1 and 2) as FC uplink ports. Ports 1 and 2 now indicate their reconfiguration as FC uplink ports under the “Desired If Role” section.

**Figure 29** Configuring Unconfigured Ports as FC Port



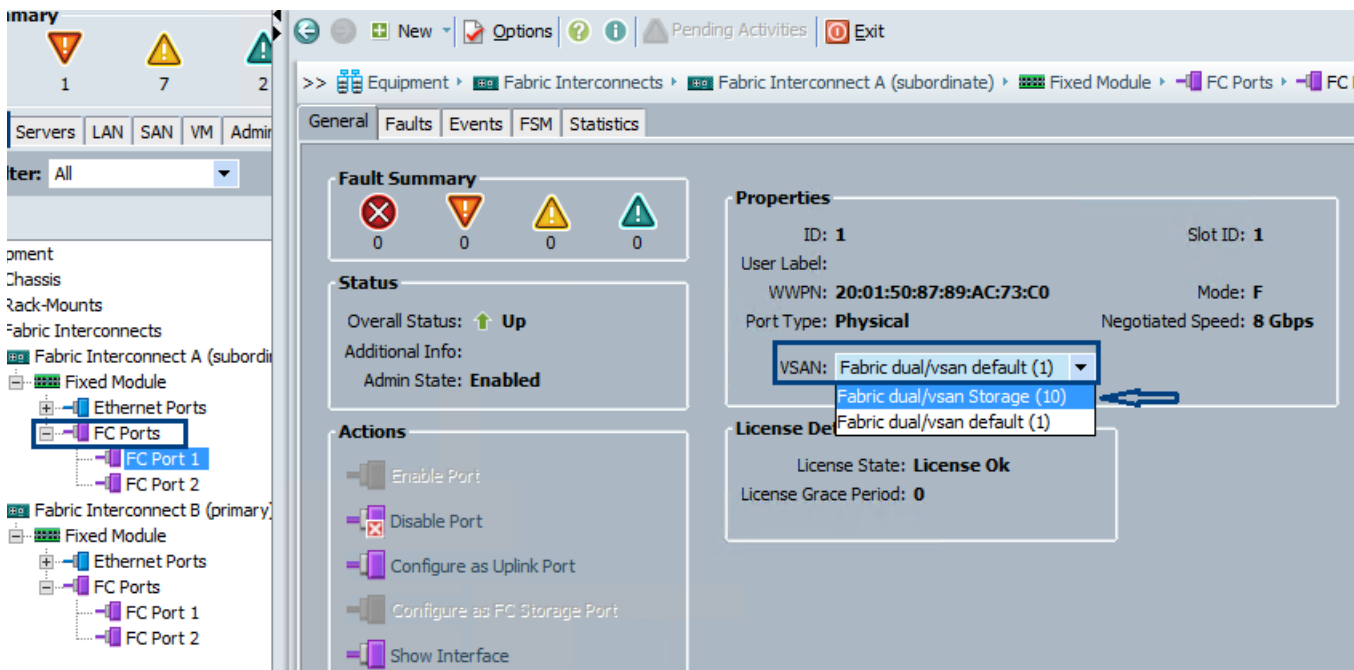
6. Click **Finish**, and then click **OK**.
7. As the primary Fabric Interconnect reboots, the Cisco UCSM GUI will close. Upon successful reboot, repeat the above steps for Fabric B and reboot it.
8. After the FI reboot, the FC ports further needs to be classified as FC Storage ports for directly attached array. Choose **Fabric Interconnect A > Expand Fixed Module > Expand FC ports > FC port 1**.

**Figure 30** *Configuring FC port as FC Storage Port*



9. In the right pane, choose **VSAN** (that you created before) and click **Save Changes**.

**Figure 31** *Choosing VSAN Storage for FC Storage Ports*



10. Repeat the steps from 7 to 9 to configure FC port 2 on the same FI and as well as for the corresponding ports on Fabric B.

After the above changes, EMC VNXe storage array would do Fibre Channel flogi into the Fabric Interconnects. Using the WWPN of the VNXe storage array, we can create a SAN boot policy on the UCS Manager. Use SSH connection to log into Cisco UCSM using the cluster IP address, and provide “connect nxos a” command to connect to NXOS. In the read-only NXOS shell, provide “show flogi database” command and note down the WWPN of the storage array. Similarly note down the WWPNs flogi entries on the fabric B by issuing “connect nxos b”.

**Figure 32** *WWPN Details of the Storage Array*

```

10.29.180.160 - PuTTY
VSPEX-FI-B# connect nxos a
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
VSPEX-FI-A(nxos)# sh flogi database
-----
--
INTERFACE          VSAN    FCID          PORT NAME          NODE NAME
-----
--
fc1/1               10      0x1b00ef      50:06:01:64:08:e0:03:68 50:06:01:60:88:e0:03:68
fc1/2               10      0x1b01ef      50:06:01:6c:08:e0:03:68 50:06:01:60:88:e0:03:68

Total number of flogi = 2.
VSPEX-FI-A(nxos)#

```

## Create Boot Policy

The following steps provide details for creating boot policies for the Cisco UCS environment. The WWPN of the EMC VNXe3200 array is required for creating boot policy. Alternatively, the WWPN information can be collected by logging into **EMC Unisphere > VNXe > Settings > More Configuration > Port Settings**.

The below table provides the storage connectivity details from **vHBA-to-FI-to-VNXe**.

**Table 10** *Storage Connectivity Details From vHBA-to-FI-to-VNXe*

vHBA	Fabric Path	Fabric Port#	VNXe Storage Processor	VNXe Port#	Target Port WWPN
vHBA-A	Fabric-A	Port 1	SP-A	Port 0	50:06:01:64:08:E0:03:68
vHBA-A	Fabric-A	Port 2	SP-B	Port 0	50:06:01:6C:08:E0:03:68

**Table 10** *Storage Connectivity Details From vHBA-to-FI-to-VNXe*

vHBA	Fabric Path	Fabric Port#	VNXe Storage Processor	VNXe Port#	Target Port WWPN
vHBA-B	Fabric-B	Port 1	SP-B	Port 1	50:06:01:6D:08:E0:03:68
vHBA-B	Fabric-B	Port 2	SP-A	Port 1	50:06:01:65:08:E0:03:68

The below UCS SAN boot policy table with all the available paths is used in this solution to create the boot policy.

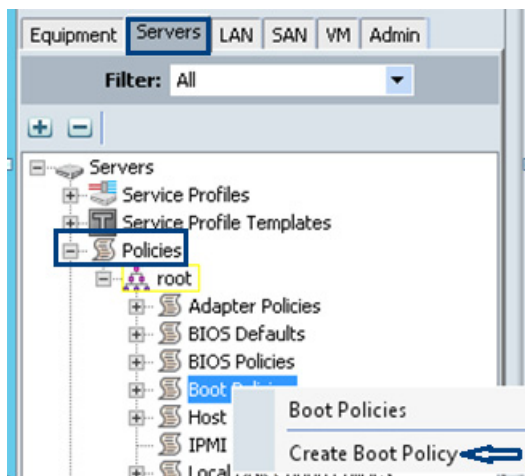
**Table 11** *UCS SAN Boot Policy Details*

SAN Type	vHBA	LUN ID	Target Port WWPN	SAN Target Type
Primary	vHBA-A	0	50:06:01:64:08:E0:03:68 (VNXe-SPA-Port0)	Primary
		0	50:06:01:6C:08:E0:03:68 (VNXe-SPB-Port0)	Secondary
Secondary	vHBA-A	0	50:06:01:65:08:E0:03:68 (VNXe-SPA-Port1)	Secondary
			50:06:01:6D:08:E0:03:68 (VNXe-SPB-Port1)	Primary

The initial boot policy provides a single path to the SAN. If more than one path is defined to the boot volume, and there is no multipath software available, as is the case for an initial installation of Windows Server 2012 R2, data corruption can occur on the disk. After installing the operating system and enabling the MPIO feature, you can define the secondary boot path.

Follow the steps given below to create a boot policy with single path:

1. Click the **Servers** tab and choose **Policies > root**.
2. Right-click the **Boot Policies** and choose **Boot Policy**.

**Figure 33** *Creating Boot Policy*



3. Name the boot policy.
4. (Optional) Provide a short description about the Boot Policy
5. Check **Reboot** checkbox on Boot Order Change and Enforce vNIC/vHBA Name.
6. Expand **Local Devices** drop-down list and choose **Add Local CD/DVD**

**Figure 34** *Creating Boot Policy Window*

**Create Boot Policy**

Name: **SAN-Boot**

Description: **Boot from SAN Policy for VSPEX Branch office Servers**

Reboot on Boot Order Change: ☒

Enforce vNIC/vHBA/iSCSI Name: ☒

Boot Mode: ☒ Legacy ☐ Uefi

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

**vNICs**

**vHBAs**

**iSCSI**

**Boot Order**

Name	Order	vNIC/vHBA/iSCSI ...	Type	Lun ID	WWN
Local CD/DVD	1				

Move Up Move Down Delete

OK Cancel

7. Expand the **vHBAs** drop-down list and choose **Add SAN Boot**.
8. Specify the vHBA name in the vHBA field in the **Add SAN Boot** window that displays.
9. Click **Primary** radio button as boot type.

**Figure 35** *Adding SAN Boot Target to SAN Primary*

**Add SAN Boot**

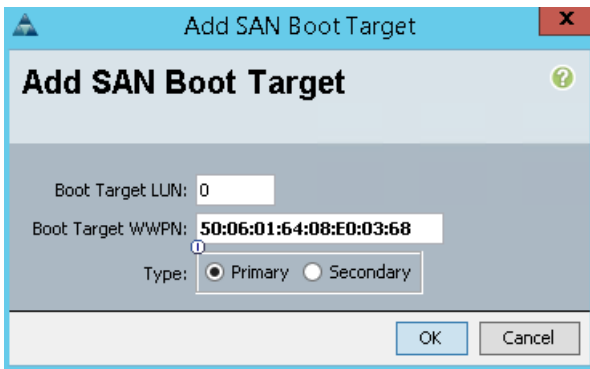
vHBA: **vHBA-A**

Type: ☒ Primary ☐ Secondary

OK Cancel

10. Click **OK** to add the SAN boot initiator
11. Under the **vHBA** drop-down menu, Choose **Add SAN Boot Target** and keep the value for Boot Target LUN as 0.
12. Enter the WWPN of the VNXe array connected to the Fabric-A.
13. Click **Primary** radio button as boot type.

*Figure 36 Adding SAN Boot Target as Primary*



14. Click **OK** to add the SAN boot target.

Figure 37 Setting SAN Boot Target

**Create Boot Policy**

Name: **SAN-Boot**

Description: **Boot from SAN Policy for VSPEX Branch office Servers**

Reboot on Boot Order Change: ☒

Enforce vNIC/vHBA/iSCSI Name: ☒

Boot Mode: ☒ Legacy ☐ Uefi

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

Name	Order	vNIC/vHBA/i...	Type	Lun ID	WWN
Local CD/DVD	1				
San	2				
SAN primary		vHBA-A	Primary		
SAN Target primary			Primary	0	50:06:01:64:08:E0:03:68

Move Up Move Down Delete

OK Cancel

## Configure Identifier Pools

In this section, configure the following identifier pools for the Cisco UCS environment. These pools will be used later in the creation of service profile template.

- Create UUID Suffix Pool
- Create MAC Address Pool
- Create WWxN Pool
- Create Management IP Pool for KVM Access

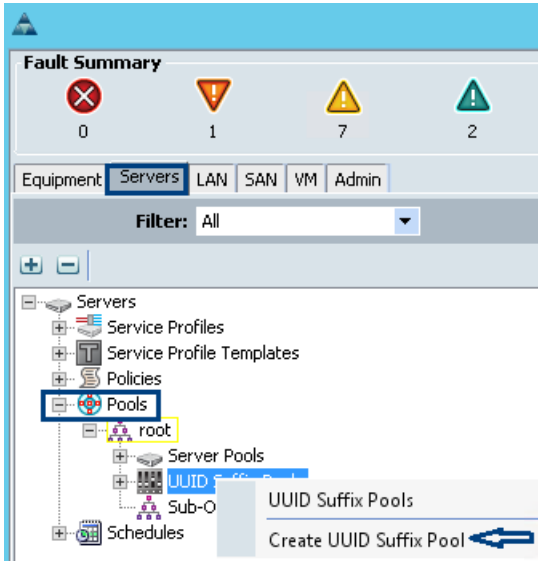
Follow the steps below to configure pools as mentioned above.

## Create UUID Suffix Pools

These steps provide details for creating UUID suffix pool in the Cisco UCS environment:

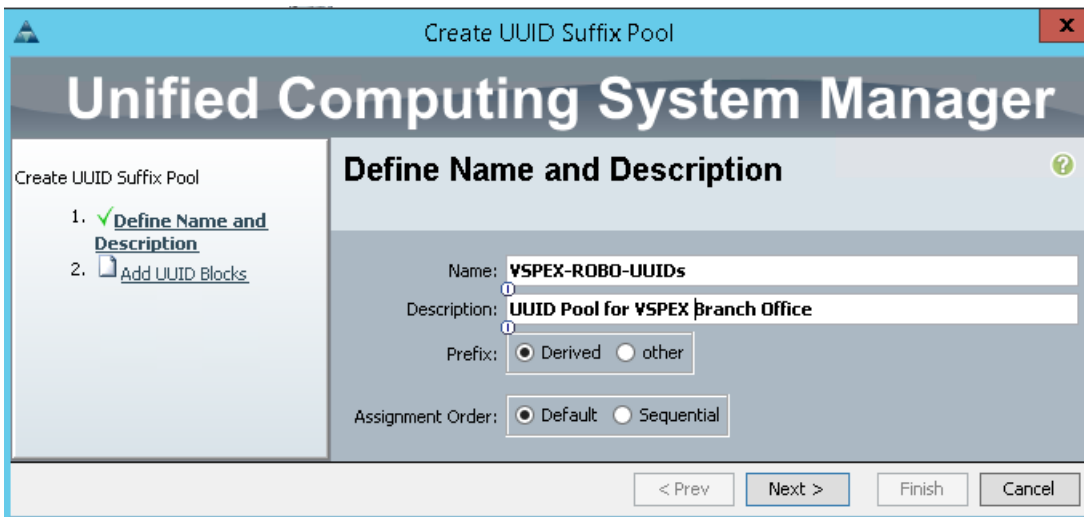
1. Click the **Servers** tab and choose **Pools > root**.
2. Right-click the UUID Suffix Pools
3. Choose **Create UUID Suffix Pool**.

**Figure 38** *Creating UUID Suffix Pool*



4. Enter a name and description to the UUID suffix pool. Leave the Prefix and Assignment Order to derived and default value respectively.

**Figure 39** *Create UUID Suffix Pool*



5. Click **Next** to continue

**Figure 40**      *Adding a Block of UUID Suffixes*

6. Click **Add** to add a block of UUID's
7. The From field is fine at the default setting, or you can create a hexadecimal string that is unique for your environment.
8. Specify the beginning of the UUIDs, and have a large size of UUID block to accommodate future expansion.

**Figure 41**      *Range for UUID Block*

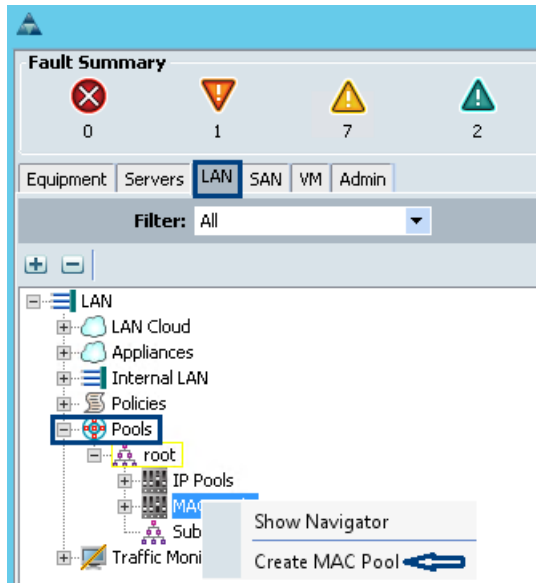
9. Click **OK**, and then click **Finish** to proceed.

## Create MAC Pool

These steps provide details for creating MAC address pool in the Cisco UCS environment:

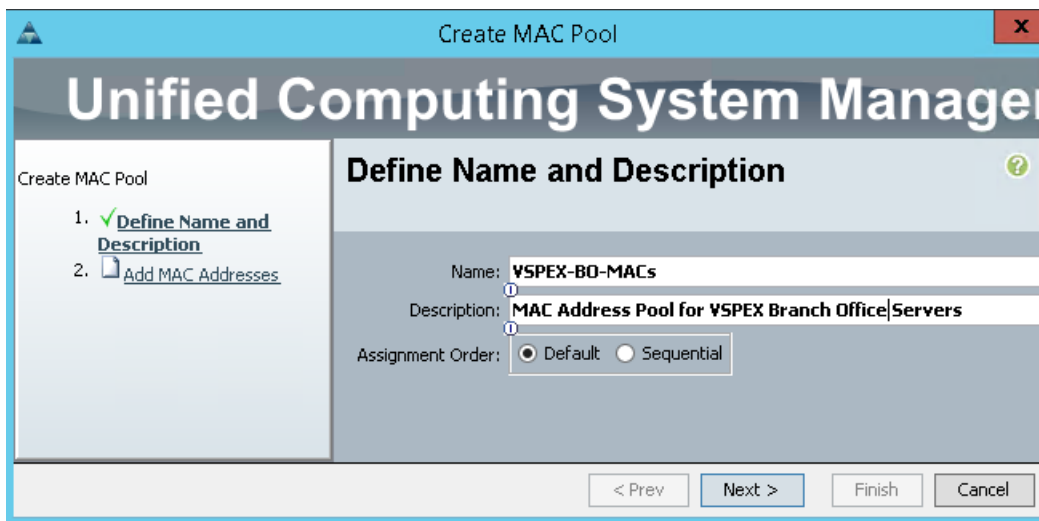
1. Choose the **LAN** tab and choose **Pools > root**.
2. Right-click the MAC Pools.
3. Choose **Create MAC Pool** to create the MAC address pool.

**Figure 42** *Create MAC Pool*

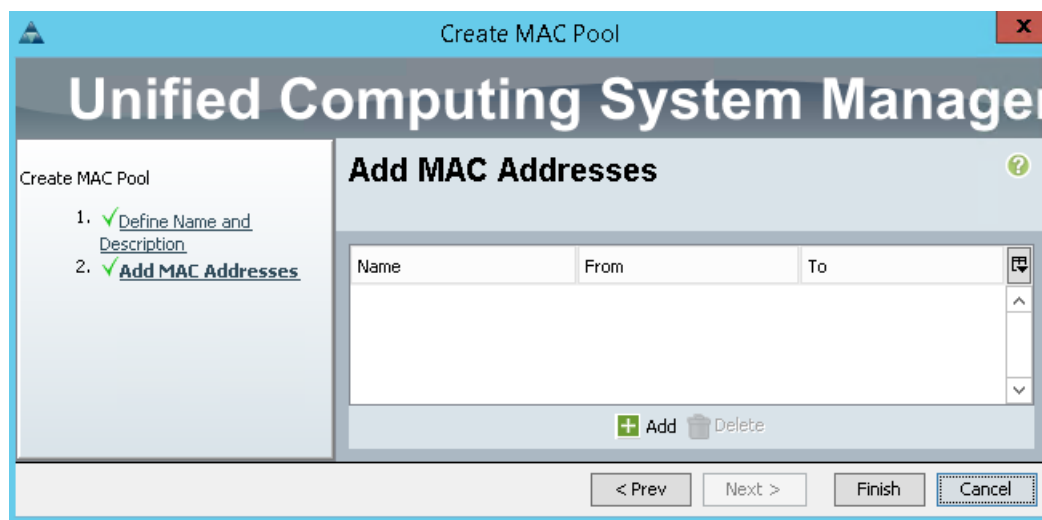


4. Provide name and description for the selected MAC pool and click **Next**.

**Figure 43** *Creating MAC Pool Window*

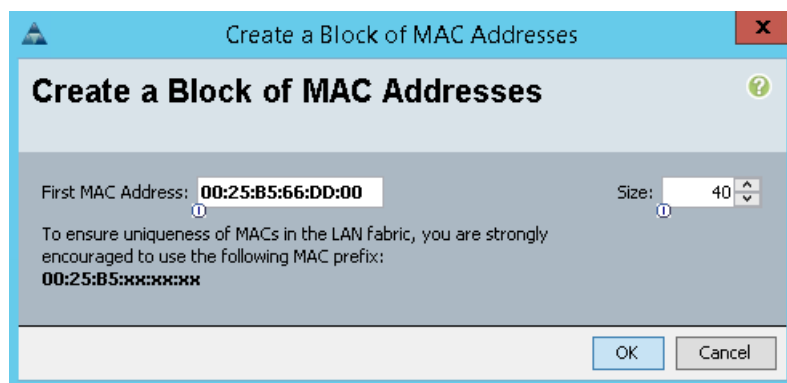


**Figure 44** Adding a Block of MAC Addresses



5. Click **Add** to add MAC pool block.
6. Specify a starting MAC address.
7. Specify a size of the MAC address pool sufficient to support current and future requirement also.
8. Click **OK**, and then click **Finish**.
9. In the message box that displays, click **OK**

**Figure 45** Range for MAC Address Block

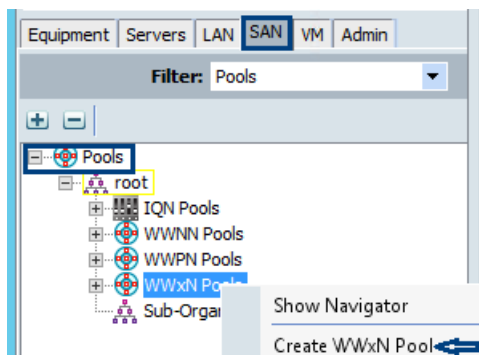


## Create WWxN Pool

These steps provide details for creating WWxN pool in the Cisco UCS environment:

1. Click the **SAN** tab at the top left of the window and choose **Pools > root**.
2. Right-click the **WWxN Pools**
3. Choose **Create WWxN Pool**.

Figure 46 Creating WWxN Pool



4. Provide name, description and choose **3 Ports per Node** from the drop-down menu

Figure 47 Create WWxN Pool - Defining Pool

**Unified Computing System Manage**

Create WWxN Pool

1. ✓ Define Name and Description
2. Add WWN Blocks

**Define Name and Description**

Name: VSPEX-BO-WWxN

Description: Combined WWNN & WWPN for VSPEX Branch Office Serve

Max Ports per Node: 3 Ports Per Node

Assignment Order: ☒ Default ☐ Sequential

< Prev Next > Finish Cancel

5. Click **Add** to add a block of WWxN IDs

Figure 48 Create WWxN Pool - Adding a Block of WWxN

**Unified Computing System Mar**

Create WWxN Pool

1. ✓ Define Name and Description
2. ✓ Add WWN Blocks

**Add WWN Blocks**

Name	From	To

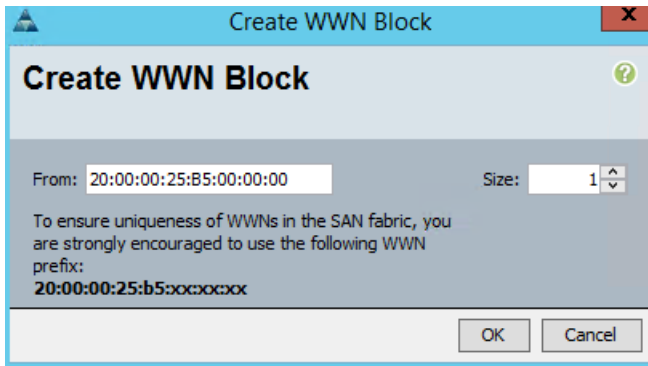
+ Add - Delete

< Prev Next > Finish Cancel

6. Provide beginning of the WWN IDs and specify a size of the WWNN block sufficient to support current and future requirement also.



Figure 49 Range for WWxN Block



**Create WWN Block**

From: 20:00:00:25:B5:00:00:00      Size: 1

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:  
20:00:00:25:b5:xx:xx:xx

OK Cancel

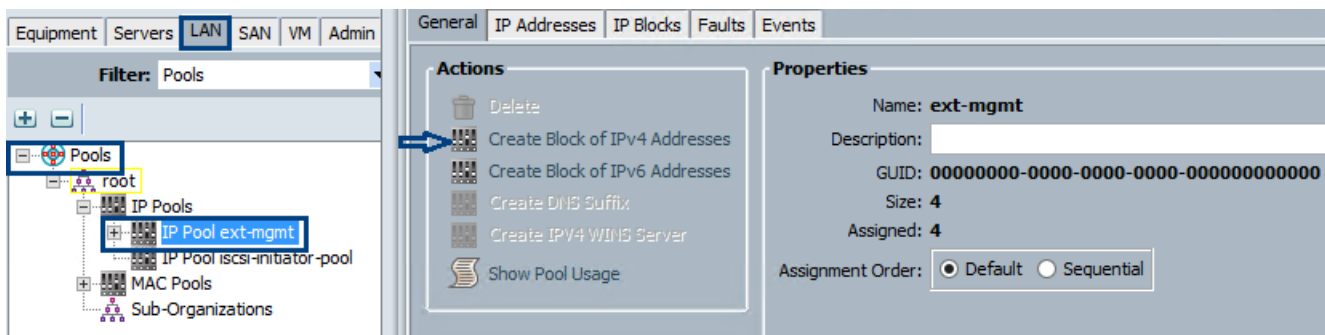
7. Click **OK**, then click **Finish** to proceed.
8. Click **OK** to **Finish**.

## Create Management IP Pool

These steps provide details for creating a block of KVM IP addresses for server access in the Cisco UCS environment:

1. Click the **LAN** tab and choose **Pools > root > IP Pools > IP Pool ext-mgmt**

Figure 50 Creating a Block of IP



2. Click the appropriate radio button for the preferred assignment order.
3. Choose **Create Block of IP Addresses**.
4. Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.
5. Click **OK** to create the IP block.
6. Click **OK** in the message box

**Figure 51** *Size of IPv4 Addresses Address*

The ext-mgmt pool is the default management pool. By default, IP addresses are assigned to the physical servers as they are recognized. That concludes configuration of all identifier pools and blocks.

## Configure Server Pool and Qualifying Policy

Creation and policy based auto-population of server pool can be divided in to the following 3 tasks:

1. Creating server pool
2. Creating of server pool policy qualification
3. Creating of server pool policy

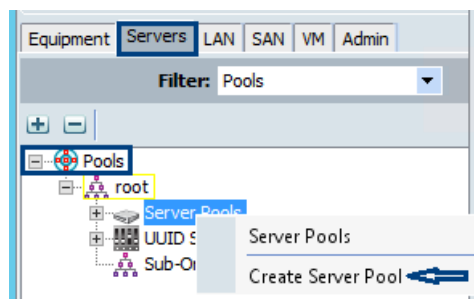
Follow these steps to accomplish the above mentioned tasks:

### Creating Server Pool

The following steps provide configuration details for server pools in the Cisco UCS environment.

1. Click the **Servers** tab and choose **Pools > root**.
2. Right-click the **Server Pools**.
3. Choose **Create Server Pool**.

**Figure 52** *Creating Server Pools*



4. Enter the name and description for the server pool, and click **Next**.

Figure 53 Creating Server Pool - Defining Server Pool

The screenshot shows the 'Create Server Pool' wizard in the Unified Computing System Manager. The title bar says 'Create Server Pool'. The main header is 'Unified Computing System Manager'. The left sidebar shows the progress: 1. Set Name and Description (checked) and 2. Add Servers. The main area is titled 'Set Name and Description'. It has two input fields: 'Name' with the value 'VSPEX-B0-Server-Pool' and 'Description' with the value 'Server Pool for VSPEX Branch Office Servers'. At the bottom are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'.

5. Click **Finish** to create the empty server pool

Figure 54 Creating Server Pool - Adding Servers

The screenshot shows the 'Create Server Pool' wizard in the Unified Computing System Manager, Step 2: Add Servers. The left sidebar shows the progress: 1. Set Name and Description (checked) and 2. Add Servers (checked). The main area is titled 'Add Servers'. It contains a table of servers, a 'Details for blade-1' section, and a 'Pooled Servers' section. The 'Servers' table has columns: Chassis ID, Slot ID, PID, R..., Ada..., A..., A..., ..., and a dropdown. The 'Details for blade-1' section has fields for Model (UCSB-B200-M3), Serial Number (FCH16337DYX), and Vendor (Cisco Systems Inc). The 'Pooled Servers' section has fields for Model, Serial Number, and Vendor. At the bottom are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'.

Servers	Chassis ID	Slot ID	PID	R...	Ada...	A...	A...	...	...
1	1	UCSB-B200-M3			UCS...			...	16
1	2	UCSB-B200-M3			UCS...			...	20
1	3	UCSB-B200-M3			UCS...			...	12

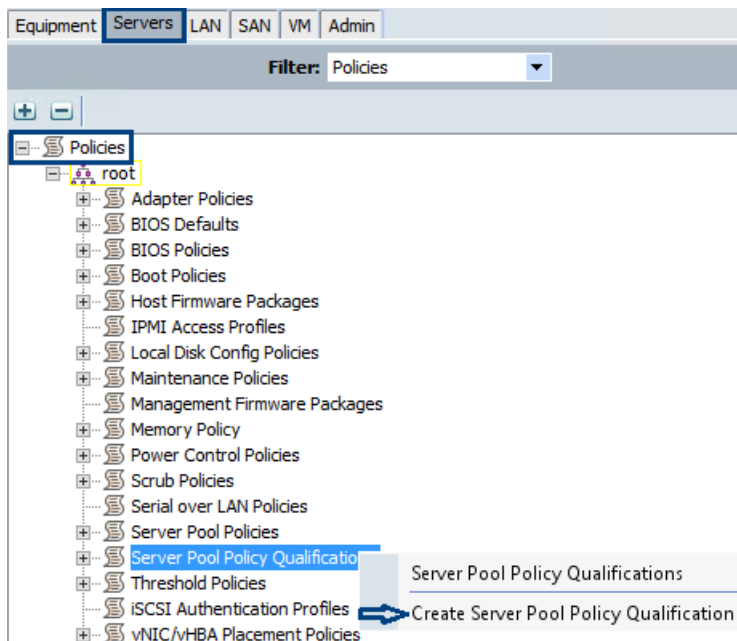
We can add the compute resources to this pool dynamically, based on a qualification policy created in the following section.

## Creating Server Pool Policy Qualification

These steps provide details for configuring the necessary server pool policy qualification for the Cisco UCS environment.

1. Click the **Servers** tab and choose **Policies > root**.
2. Right-click the **Server Pool Policy Qualifications**.
3. Choose **Create Server Pool Policy Qualification**.

**Figure 55** *Creating Server Pool Policy Qualification*



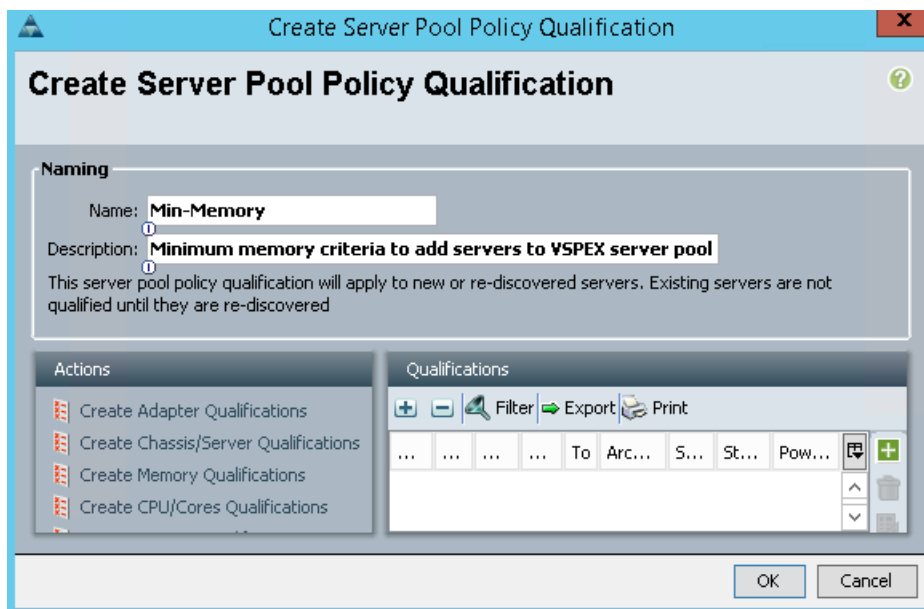
4. Give a name to server policy qualification criterion.
5. Choose **Create Memory Qualifications** criterion.
6. Click **OK** twice to create the qualification.



**Note**

Memory Qualifications is an example criterion, you may choose a criterion that suits your requirement.

**Figure 56** *Creating Server Pool Policy Qualification Window*



- Set minimum 128 GB RAM for the pool qualification criterion.

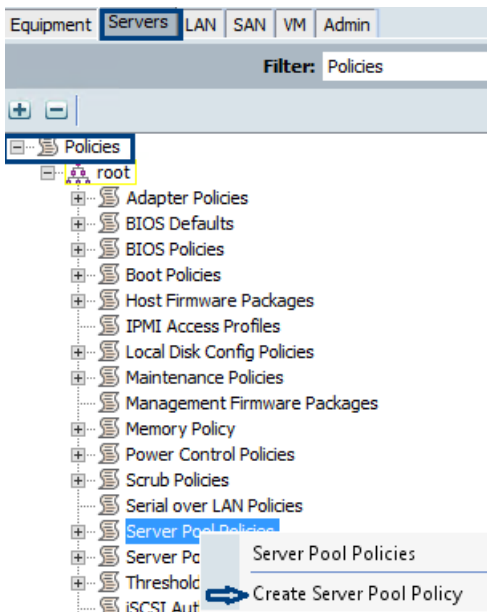
**Figure 57** *Creating Memory Qualification*

## Creating Server Pool Policy

These steps provide details for configuring the necessary server pool policy for the Cisco UCS environment.

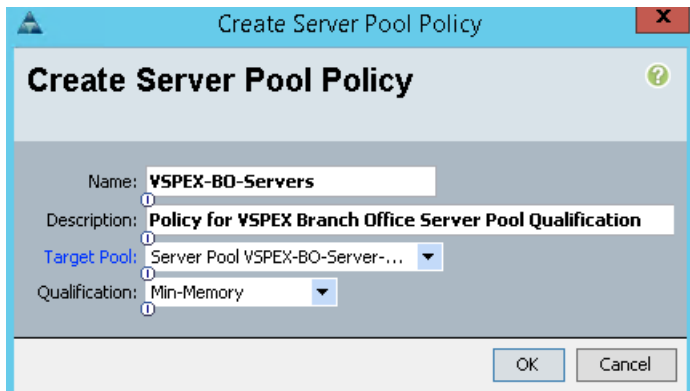
- Click the **Servers** tab and choose **Policies > root**.
- Right-click the **Server Pool Policy**.
- Choose **Create Server Pool Policy**.

**Figure 58** *Creating Server Pool Policy*



- Provide a name and description to the server pool policy. Choose recently created Target Pool and Qualification.
- Click **OK** to deploy the configuration.

**Figure 59** *Creating Server Pool Policy Window*



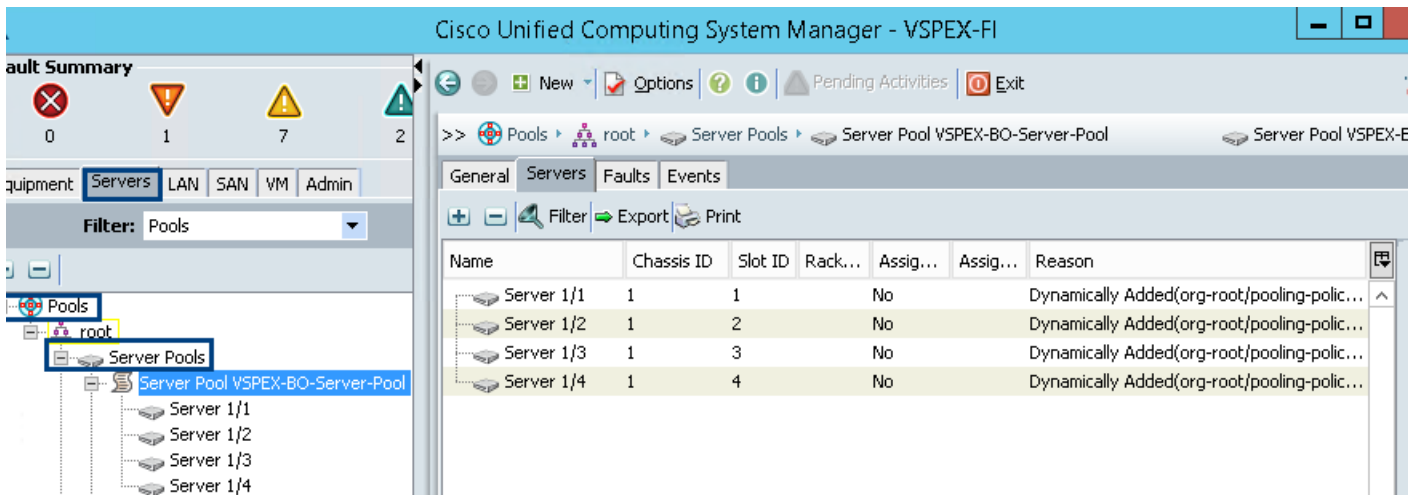
The 'Create Server Pool Policy' window is shown. It has a title bar with a close button. The main area contains the following fields:

- Name:** VSPEX-BO-Servers
- Description:** Policy for VSPEX Branch Office Server Pool Qualification
- Target Pool:** Server Pool VSPEX-BO-Server-...
- Qualification:** Min-Memory

At the bottom are 'OK' and 'Cancel' buttons.

Figure 60 shows all the compute resources that meet the memory qualification criteria are dynamically added to the server pool.

**Figure 60** *Dynamically Added Servers Based on Memory Qualification*



The screenshot shows the Cisco Unified Computing System Manager - VSPEX-FI interface. The left pane shows a tree view with 'Pools' selected, and 'Server Pool VSPEX-BO-Server-Pool' highlighted. The right pane shows the 'Servers' tab for this pool, displaying a table of dynamically added servers.

Name	Chassis ID	Slot ID	Rack...	Assig...	Assig...	Reason
Server 1/1	1	1		No		Dynamically Added(org-root/pooling-polic...
Server 1/2	1	2		No		Dynamically Added(org-root/pooling-polic...
Server 1/3	1	3		No		Dynamically Added(org-root/pooling-polic...
Server 1/4	1	4		No		Dynamically Added(org-root/pooling-polic...

## Create vNIC Templates

This section provides details for creating vNIC templates for the Cisco UCS environment. It is recommended to isolate the different network traffic types from each other and based on this four vNIC templates are created in this section. The below table summarizes the same and helps in creating the vNIC templates.

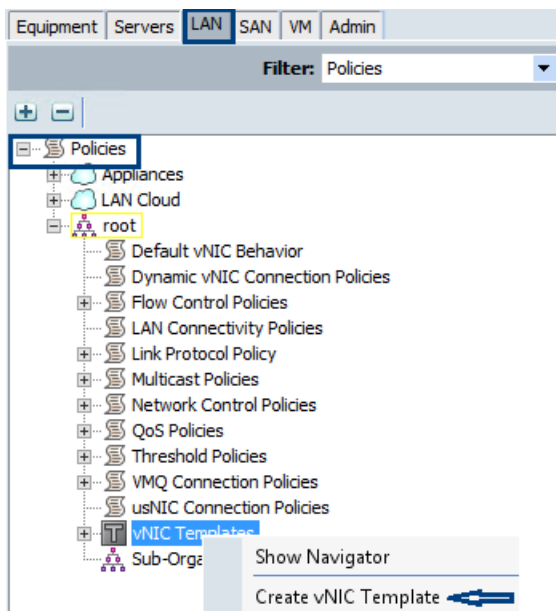
**Table 12**      *Summarizing vNIC Template Details*

<b>vNIC Template Name</b>	<b>Purpose</b>	<b>Native VLAN</b>	<b>Fabric ID</b>	<b>Fabric Failover</b>	<b>Target</b>	<b>Template Type</b>	<b>MTU Size</b>	<b>QoS Policy</b>	<b>MAC Pool</b>	<b>Connection Policy</b>
Mgmt	Host management traffic	Mgmt	A	Yes	Adapter only	Updating	Default	Default	VSPEX-BO-MAC	Default
CSV	Cluster Shared Volume traffic	CSV	B	Yes	Adapter only	Updating	9000	CSV	VSPEX-BO-MAC	Default
LiveM-igrati-on	Live Migration traffic	LiveM-igrati-on	A	Yes	Adapter only	Updating	9000	Live Migration	VSPEX-BO-MAC	Default
VMac-cess	Virtual Machine traffic	VMac-cess	B	Yes	Adapter only	Updating	Default	Default	VSPEX-BO-MAC	Default

The following steps provide details to create a vNIC template for the cluster shared volume network traffic.

1. Click the **LANs** tab and choose **Policies > root**.
2. Right-click the vNIC Templates.
3. Choose **Create vNIC Template**.

**Figure 61** *Creating vNIC Template*



4. Enter a name and description for the vNIC template.
5. Check **Fabric A** checkbox.
6. Check the **Enable Failover** checkbox.
7. Under target, choose **Adapter** and uncheck the **VM** checkbox.
8. Choose **Updating Template** as the template type.
9. Under VLANs, choose the **VLAN (CSV)** created for CSV traffic in the “Create VLANs” section. Set Native VLAN.
10. Under MTU, set to 9000.
11. Under MAC Pool, choose the **MAC Pool (VSPEX-BO-MACs)** created in the “Create MAC-Pool” section.
12. For QoS Policy, choose the QoS Policy named CSV in the “Create QoS Policy” section.



Figure 62 Create vNIC Template Window

**Create vNIC Template**

Name: **CSV**

Description: **Dedicated NIC for Cluster Shared Volume Traffic**

Fabric ID: ☐ Fabric A ☒ Fabric B ☒ Enable Failover

**Target**

☒ Adapter  
☐ VM

**Warning**  
If **VM** is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type: ☐ Initial Template ☒ Updating Template

**VLANs**

Filter Export Print

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input checked="" type="checkbox"/>	CSV	<input checked="" type="radio"/>
<input type="checkbox"/>	LiveMigration	<input type="radio"/>
<input type="checkbox"/>	Mgmt	<input type="radio"/>
<input type="checkbox"/>	VMaccess	<input type="radio"/>

+ Create VLAN

MTU: **9000**

**Warning**  
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool: **VSPEX-BO-MACs(40/...**

QoS Policy: **CSV**

Network Control Policy: **<not set>**

Pin Group: **<not set>**

Stats Threshold Policy: **default**

**Connection Policies**

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy: **<not set>**

OK Cancel

13. Click **OK** to complete creating the vNIC template

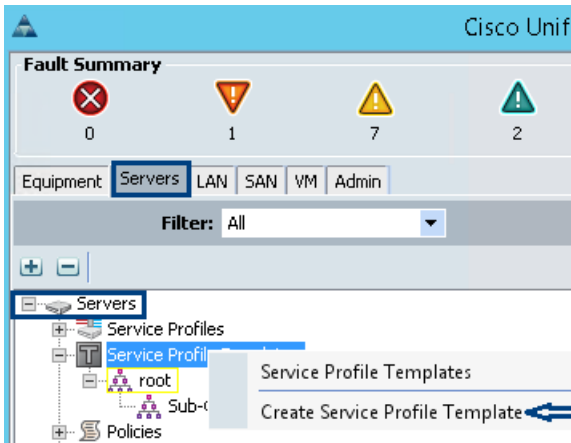
Similarly create the remaining vNIC templates by referring to the table and the steps mentioned above in this section.

## Create Service Profile Template

At this point, we are ready to create service profile template, from which we can instantiate individual service profiles later. Follow the following steps to create the service profile template:

1. Click the **Servers** tab and choose **Service Profile Templates > root**.
2. Right-click the root and choose **Create Service Profile Template**

**Figure 63** *Creating Service Profile Template*



3. In the **identify Service Profile Template** section provide a service profile template name,
4. Choose the type as **Updating Template**
5. Choose **UUID** pool from the drop-down by selecting the one (VSPEX-ROBO-UUID) created in the “Create UUID Suffix Pool” section.

**Figure 64** *Creating Service Profile Template – Identification*

**Create Service Profile Template**

# Unified Computing System Manager

Create Service Profile Template

1. **Identify Service Profile Template**
2. Networking
3. Storage
4. Zoning
5. vNIC/vHBA Placement
6. Server Boot Order
7. Maintenance Policy
8. Server Assignment
9. Operational Policies

## Identify Service Profile Template

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name: **VSPEX-B0-Server-SP-Template**

The template will be created in the following organization. Its name must be unique within this organization.

Where: **org-root**

The template will be created in the following organization. Its name must be unique within this organization.

Type: ☐ Initial Template ☒ Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.

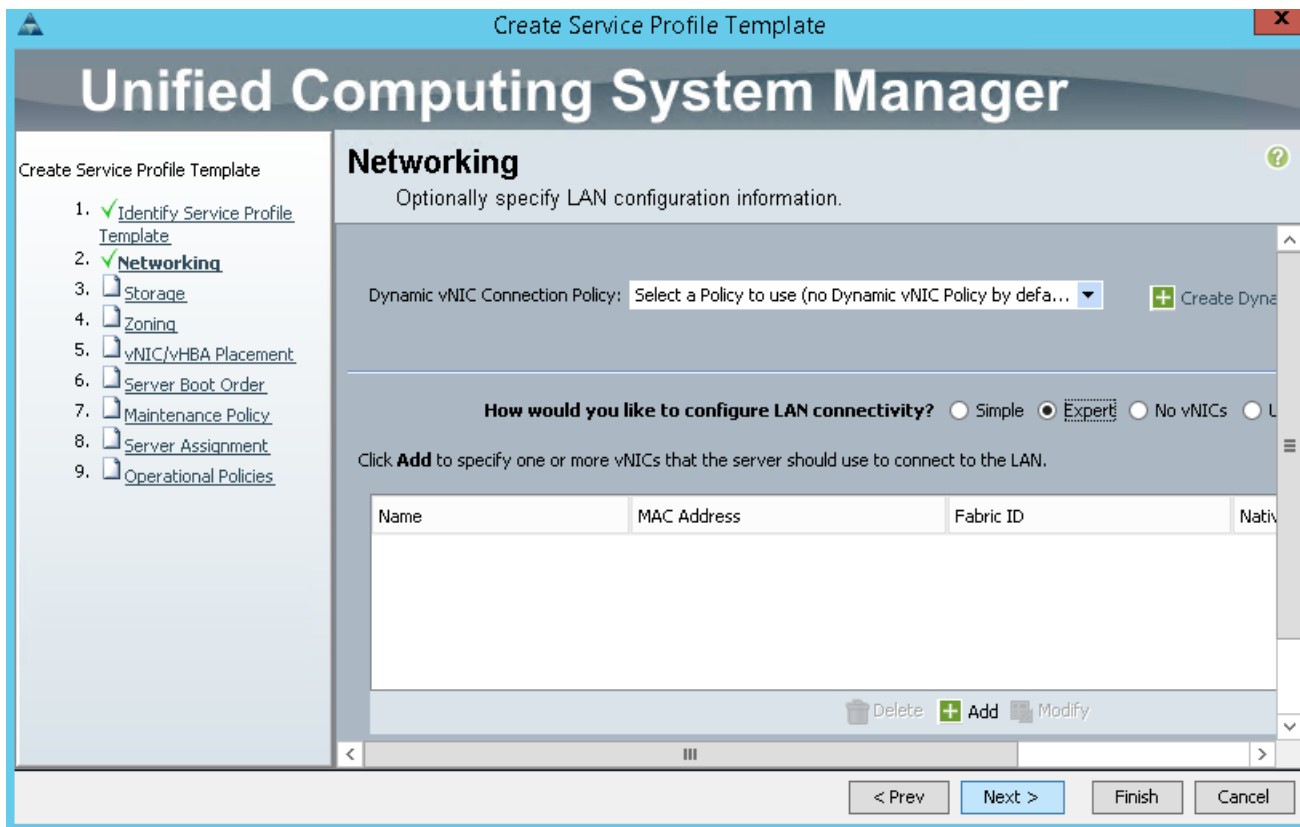
**UUID**

UUID Assignment: VSPEX-ROBO-UUIDs(8/8)

< Prev Next > Finish Cancel

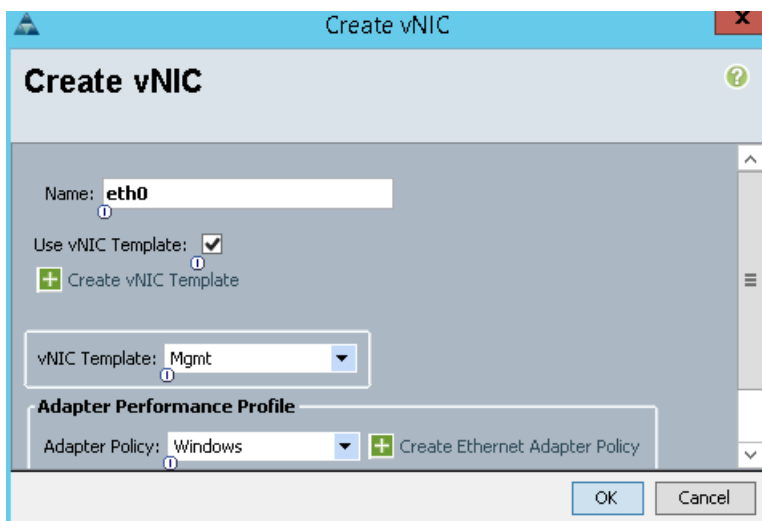
6. In the **Networking** Section, leave the **Dynamic vNIC Connection Policy** field at the default.
7. Choose **Expert** for the How would you like to configure LAN connectivity? option.
8. Click **Add** to add a vNIC to the service profile template.

**Figure 65** *Creating Service Profile Template – Networking*



9. The **Create vNIC** window displays. Name the vNIC.
10. Check the **Use LAN Connectivity Template** checkbox.
11. Choose **Mgmt** from the drop-down menu for the **vNIC Template** field.
12. Choose **Windows** in the **Adapter Policy** field.

**Figure 66** *Create vNIC Window for the Management Traffic*

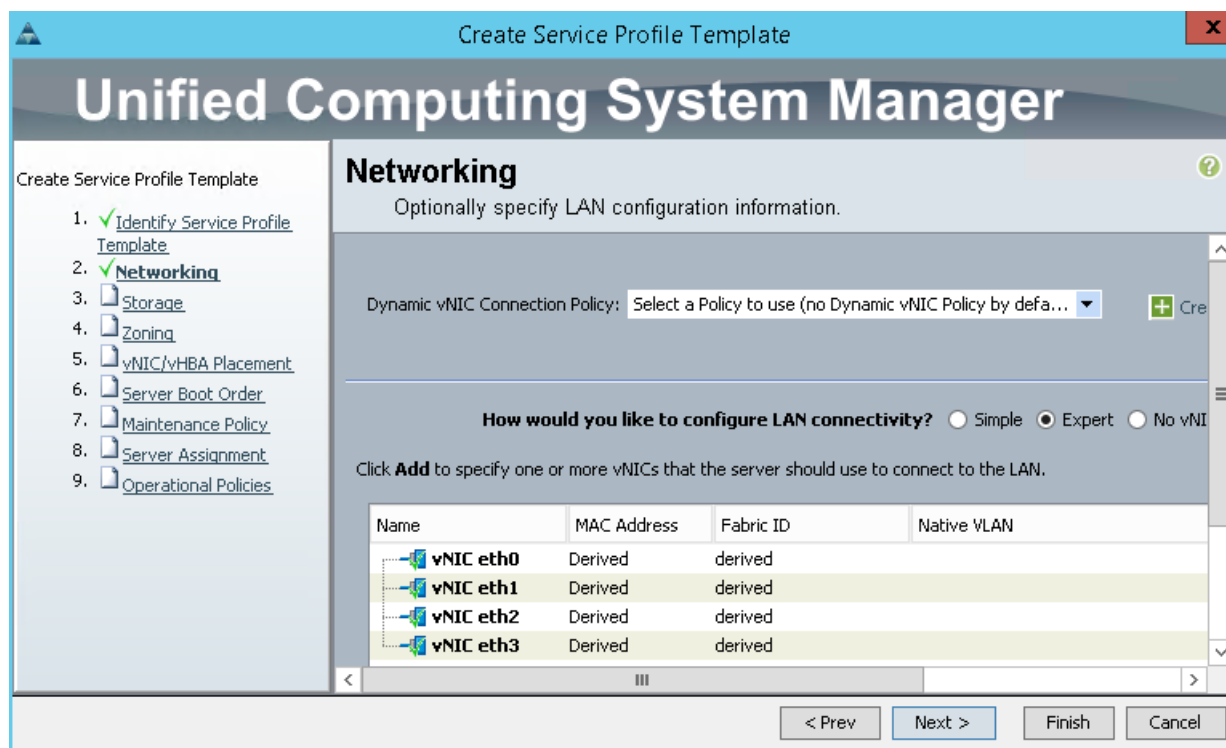


13. Click **OK** to add the vNIC to the template. This returns you to the Networking window.
14. Repeat the above steps to add all the desired vNICs by referring to table 13 and verify the same to see if all of the vNICs were created as shown the below figure.

**Table 13** *vNICs Created Summary*

vNIC Name	vNIC Template Name	Adaptor Policy
eth0	Mgmt	Windows
eth1	CSV	Windows
eth2	LiveMigration	Windows
eth3	VMaccess	Windows

**Figure 67** *Creating Service Profile Template*



15. Click **Next** to continue.
16. In the **Storage** section, choose the **Local Storage** policy defined earlier.
17. Choose **Expert** for the How would you like to configure SAN connectivity? question.
18. Choose the pool (VSPEX-BO-WWxNs) created in the “Create WWxN Pool” section for WWNN Assignment.
19. In the **WWPN** section, click **Add** to add the WWPNs to be used.

**Figure 68** *Creating Service Profile Template – Storage*

20. Enter a value in the **Name** field.
21. For the **WWPN Assignment** under World Wide Port Name, choose **Derived** from the drop-down list.
22. Choose A as the Fabric ID and choose Storage (created in the “Create VSANs” section) as the VSAN
23. Choose **Windows** from the **Adapter Policy** drop down list and leave the rest at defaults.
24. Click **OK** to deploy the vHBA

Figure 69 Storage - Creating vHBA

**Create vHBA**

Name:

Use vHBA Template: ☐

**World Wide Port Name**

WWPN Assignment:

**Create vHBA Template**

**Create WWPN Pool**  
 If you select a WWxN Pool for the World Wide Node Name, the WWPN will be derived from that pool.  
 If you did not select a WWxN Pool for the World Wide Node Name, the WWPN assigned by the manufacturer will be used.  
 Note: When a manufacturer assigned WWPN is used, the WWPN will not be migrated if the service profile is moved to a new server.

Fabric ID: ☒ A ☐ B

Select VSAN:  **Create VSAN**

Pin Group:  **Create SAN Pin Group**

Persistent Binding: ☒ Disabled ☐ Enabled

Max Data Field Size:

**Operational Parameters**

**Adapter Performance Profile**

Adapter Policy:  **Create Fibre Channel Adapter Policy**

QoS Policy:  **Create QoS Policy**

OK Cancel

25. Repeat steps 20-24 for vHBA-B on Fabric B, with the same configuration. Click **Next**.
26. Keep the default configuration for Zoning and vNIC/vHBA Placement policy. Click **Next**.
27. In the **Server Boot Order** window, choose SAN-Boot (created in the "" section) for the **Boot policy** from the drop-down menu and Click **Next**.

**Figure 70** *Creating Service Profile Template - Server Boot Order*

**Create Service Profile Template**

**Server Boot Order**

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: **SAN-Boot** + Create Boot Policy

Name: **SAN-Boot**  
 Description: **Boot from SAN Policy for VSPEX Branch office Servers**  
 Reboot on Boot Order Change: **Yes**  
 Enforce vNIC/vHBA/iSCSI Name: **Yes**  
 Boot Mode: **Legacy**

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus

**Boot Order**

+ - Filter Export Print

Name	Order	vNIC/vHBA/iSCSI v...	Type	Lun ID	WWN
Local CD/DVD	1				
San	2				
SAN primary		vHBA-A	Primary		
SAN Target primary			Primary	0	50:06:01:64:08:E0:03:68

< Prev Next > Finish Cancel

28. In the **Maintenance Policy** window leave all the fields at default and click **Next**.
29. In the **Server Assignment** window, choose the **VSPEX-BO-Server-Pool** (created in the “Create Server Pool” section) from the drop-down list to the **Pool Assignment**.
30. For the **Server Pool Qualification** choose the **Min-Memory** (created in the “Create Server Pool Policy Qualification”) from drop-down.
31. Leave the other settings to defaults and Click **Next**.



**Figure 71** *Creating Service Profile Template - Server Assignment*

**Create Service Profile Template**

# Unified Computing System Manager

Create Service Profile Template

1. ✓ Identify Service Profile Template
2. ✓ Networking
3. ✓ Storage
4. ✓ Zoning
5. ✓ vNIC/vHBA Placement
6. ✓ Server Boot Order
7. ✓ Maintenance Policy
8. ✓ **Server Assignment**
9. ☐ Operational Policies

## Server Assignment

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: VSPEX-BO-Server-Pool + Create Server Pool

Select the power state to be applied when this profile is associated with the server.

☒ Up ☐ Down

The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification: Min-Memory

Restrict Migration: ☐

< Prev Next > Finish Cancel

32. In the **Operation Policies** window, keep all the fields at default, and click **Finish** to deploy the Service Profile Template.

**Figure 72** *Creating Service Profile Template - Operational Policies*

**Create Service Profile Template**

# Unified Computing System Manager

Create Service Profile Template

1. ✓ Identify Service Profile Template
2. ✓ Networking
3. ✓ Storage
4. ✓ Zoning
5. ✓ vNIC/vHBA Placement
6. ✓ Server Boot Order
7. ✓ Maintenance Policy
8. ✓ Server Assignment
9. ✓ **Operational Policies**

## Operational Policies

Optionally specify information that affects how the system operates.

- BIOS Configuration
- External IPMI Management Configuration
- Management IP Address
- Monitoring Configuration (Thresholds)
- Power Control Policy Configuration
- Scrub Policy

< Prev Next > Finish Cancel

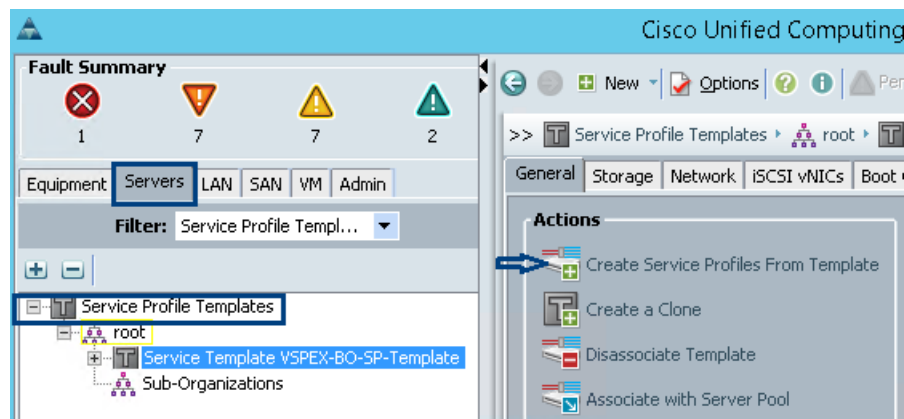
That concludes the service profile template creation.

## Instantiate Service Profiles from the Service Profile Template

This section deals with the instantiation of service profiles from the service profile template. This is the last step in the configuration of Cisco UCSM. Follow these steps to instantiate Service Profiles:

1. Click the **Servers** tab and choose **Service Profile Templates** that was created in the previous section.
2. Choose **Create Service Profiles From Template** (see Figure 73).

**Figure 73** *Creating Service Profile from Template*



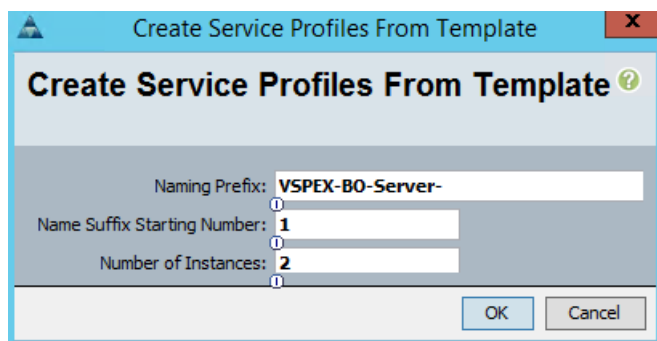
3. Enter a name for the Naming Prefix.
4. Enter 1 for the Name Suffix Starting Number.
5. Enter a number for the Number of Instances to be created.
6. Click **OK** to create the service profile and again click **OK**



**Note**

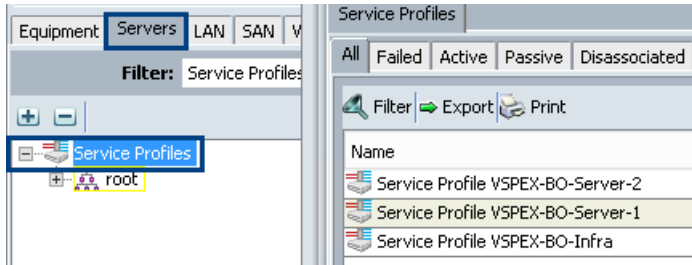
Refer to the sizing guidelines for the number of servers needed for your deployment.

**Figure 74** *Creating Service Profiles from Template Window*



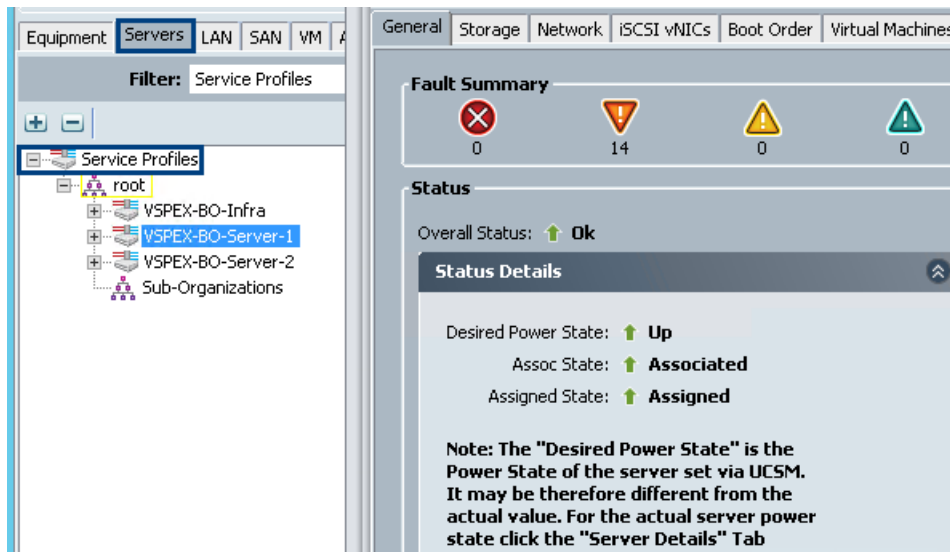
According to the Service profile instances you will see the Service profiles created from the template.

**Figure 75** *Service Profiles Created from Service Profile Template*



As the Service Profile Template is assigned to a server pool, the service profiles instantiated from the template would be assigned to individual server resource from the server pool as far as they are available. You can choose a service profile and see its association state, and with which server it is associated.

**Figure 76** *Service Profile Status*



Once the service profile association is complete as show in the above figure, the blade servers are now automatically assigned with the identifiers (UUIDs, MAC Addresses and WWxNs) from the pools. You can see the zones are also created automatically as shown in the below figure. Note down the WWPN information from this window because it will be required in the next section while configuring the EMC VNXe3200 storage array.

**Figure 77** *WWxN and Zoning information in Service Profile after the association*

The figure consists of two screenshots of the Cisco UCS Central web interface. Both screenshots show the 'FC Zones' tab under the 'Service Profiles' section. The left screenshot shows a tree view on the left with 'Service Profiles' expanded, and a table on the right showing the FC Zones configuration. The right screenshot is a similar view, showing the same configuration details.

Name	Initiator WWPN	Target WWPN	Initi...	Admi...	Op...
ucs_VSPEX-FI_A_1_VSPEX-BO-Server-1_vHBA-A	20:00:00:25:B5:06:0D:2E		vHBA-A	Applied	Active
FC Target 50:06:01:64:08:E0:03:68		50:06:01:64:08:E0:03:68			

Name	Initiator WWPN	Target WWPN	Initi...	Ad...	Op...	F
ucs_VSPEX-FI_A_2_VSPEX-BO-Server-2_vHBA-A	20:00:00:25:B5:06:0D:0E		vHBA-A	Applied	Active	A
FC Target 50:06:01:64:08:E0:03:68		50:06:01:64:08:E0:03:68				

## Prepare EMC VNXe3200

Preparing the EMC VNXe3200 array for this solution can be broadly classified into the below tasks:

- Initial setup of VNXe Array
- Create Hosts
- Create Storage Pool for SAN Boot
- Create Boot LUNs and access to the Hosts

## Initial Setup of VNXe Array

### Rack and Install

Initial configuration and implementation of an EMC VNXe3200 is covered in detail from the EMC documentation library which can be downloaded from the below URL. Installation documentation covers all areas from unpacking VNXe storage components, installing in rack, provisioning power requirements, and physical cabling.

[https://support.emc.com/docu52658\\_VNXe3200-Installation-Guide.pdf?language=en\\_US](https://support.emc.com/docu52658_VNXe3200-Installation-Guide.pdf?language=en_US)

### Assign an IP to Management Interface

After you finish installing, cabling, and powering up the system, the system must acquire an IP address for its management interface before you can register, license, or configure it. The VNXe3200 supports both IPv4 and IPv6. You can assign an IP address to a VNXe system in the following ways:

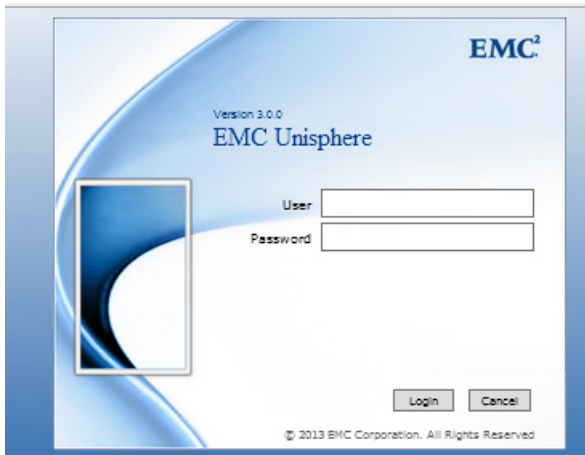
- Dynamically assigned from a DHCP server in the network.
- Manually assign a static IP address from a VNXe connection utility as explained in the above URL.

The VNXe connection utility can be downloaded from the below EMC web site:

[https://download.emc.com/downloads/DL31479\\_VNXe-Connection-Utility-\(Windows-32-bit\).exe](https://download.emc.com/downloads/DL31479_VNXe-Connection-Utility-(Windows-32-bit).exe)

Connect to the VNXe system from a web browser using the management IP address.

**Figure 78** *EMC Unisphere Login Page*

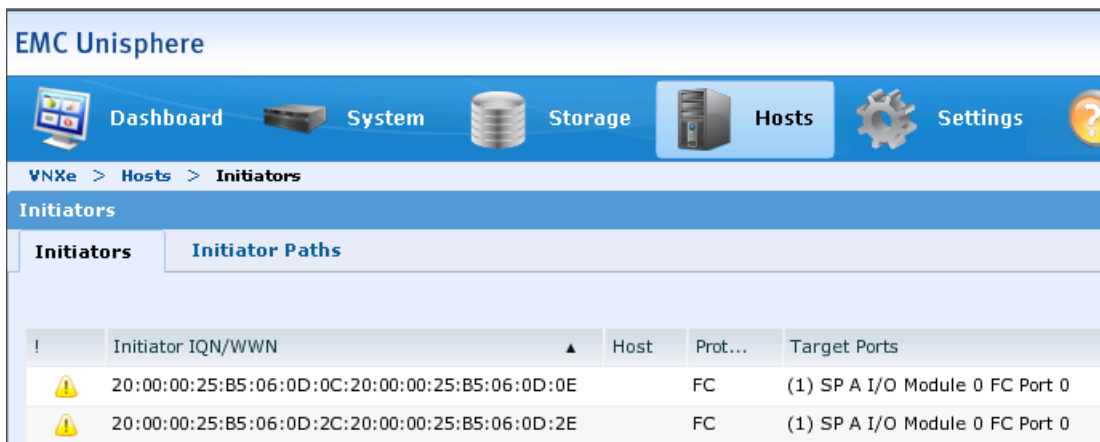


## Create Hosts

This section provides details on the discovery of host initiators on the VNXe array and creating host list.

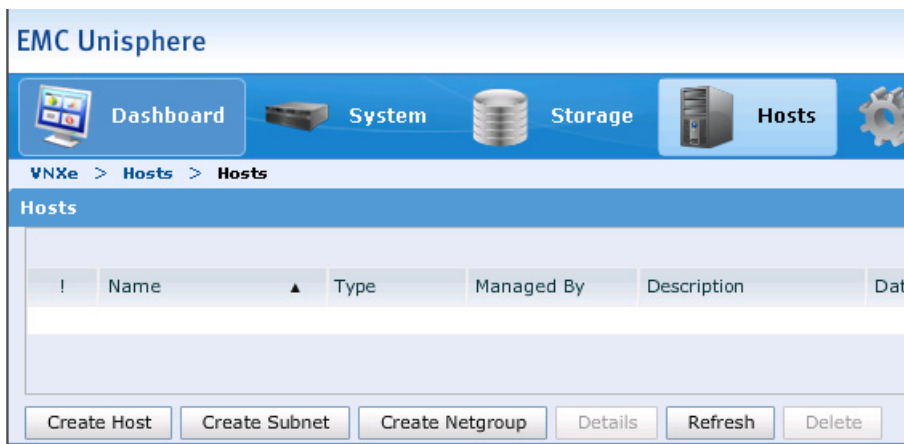
1. Connect to the VNXe system from a web browser using the management IP address and launch the Unisphere.
2. Click **Hosts** tab and then click Initiators to see if the array has discovered the host initiators.

**Figure 79** *EMC Unisphere Showing Host Initiators*



3. Choose the **Hosts** tab, and then click **Create Host**


**Figure 80** *VNXe Create Host Wizard*



4. The **Create Host** window appears. In the Name and Description fields, type the name and description of the new host. Click **Next**.

**Figure 81** *Specify Name in the VNXe Host Wizard*

**Host Wizard**

 **Specify Name**

**Step 1 of 7**

Enter a name and optional description for the host configuration:


Name: \* VSPEX-BO-Server-1

Description: Host Group for VSPEX Branch Office Hyper-V Server 1

5. In the **Operating System** page, choose the host OS from the **Operating System** list box. Click **Next**.

**Figure 82** *Operating System Page in VNXe Host Wizard*

**Host Wizard**

 **Operating System**

**Step 2 of 7**

Specify the host operating system.


While this information is not required, providing this information is recommended.

Operating System: Microsoft Hyper-V

6. The **Network Address** page appears. choose Network Name or IP Address to enter the details of the host.

**Figure 83**      *Network Address Page in VNXe Host Wizard*

**Host Wizard**

 **Network Address**

**Step 3 of 7**

Specify the host network address.

You can specify the network address of the host as either a network name or IP Address.


Network Address: ☒ Network Name:

☐ IP Address:

- In the **Fiber Channel Access** page, choose the WWPN of VSPEX-BO-Server-1 UCS service profile for this HyperV1 host.


**Figure 84**      *Fibre Channel Access Page in VNXe Host Wizard*

**Host Wizard**

 **Fibre Channel Access**

**Step 5 of 7**

Register discovered FC connections with host VSPEX-BO-Server-1:


 Filter for:


	Initiator WWN	Connected To
<input type="checkbox"/>	20:00:00:25:B5:06:0D:0C:20:00:00:25:B5:06:0D:0E	(1) SP A I/O Module 0 FC Port 0
<input checked="" type="checkbox"/>	20:00:00:25:B5:06:0D:2C:20:00:00:25:B5:06:0D:2E	(1) SP A I/O Module 0 FC Port 0

- In the **Summary** page, confirm the host configuration and click **Finish**.

Figure 85 Summary Page in VNXe Host Wizard

**Host Wizard**

 **Summary**

**Step 6 of 7**  >>

Confirm the following Host configuration:

Name: VSPEX-BO-Server-1  
 Description: Host Group for VSPEX Branch Office Hyper-V Server 1  
 Operating System: Microsoft Hyper-V  
 Network Name: HyperV1

Initiators to be registered with this host: ▼ 1

Protocol ▲	Initiator IQN/WWN
FC	20:00:00:25:B5:06:0D:2C:20:00:00:25:B5:06:0D:2E

1 items

< Back   Next >   Finish   Cancel   Help

9. And finally in the **Results** page click **Finish**.

10. Repeat the above steps to create Host list for all Hyper-V hosts used for this solution.

## Create Storage Pool

This section provides the steps for creating storage pools. For this solution we will be creating two storage pools - one for SAN-Boot LUNs and the second one for the Hyper-V CSV LUNs

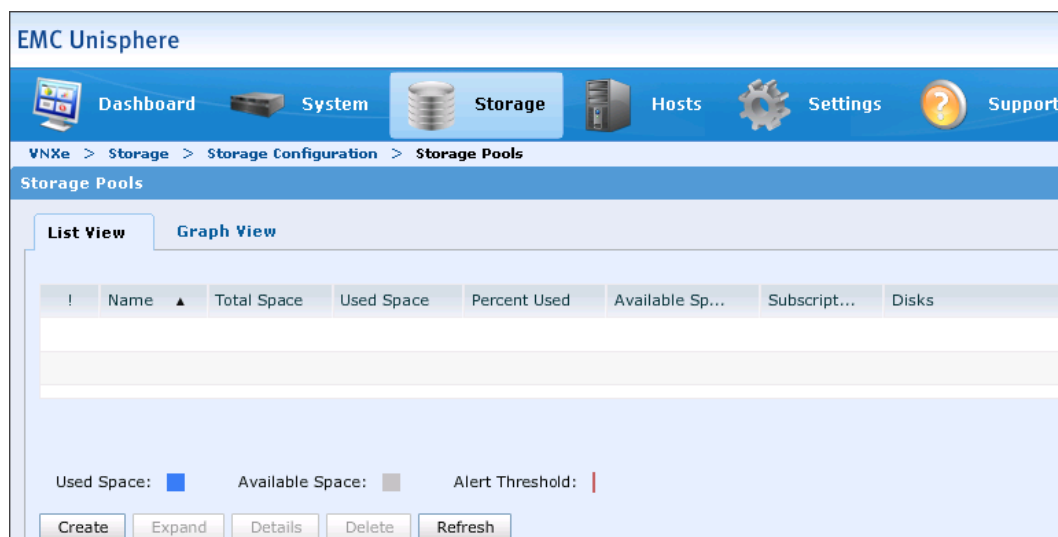
Table 14 Storage Pool Summary

Storage Pool Name	RAID Type	Storage Tier Type	Number of Disks
VSPEX-SAN-Boot	RAID 5	Performance	5
VSPEX-HyperV-CSV	RAID 5	Performance	35

1. Launch the EMC VNXe Unisphere.
2. Choose **VNXe > Storage > Storage Configuration > Storage Pools** and click **Create**, (see Figure 86).

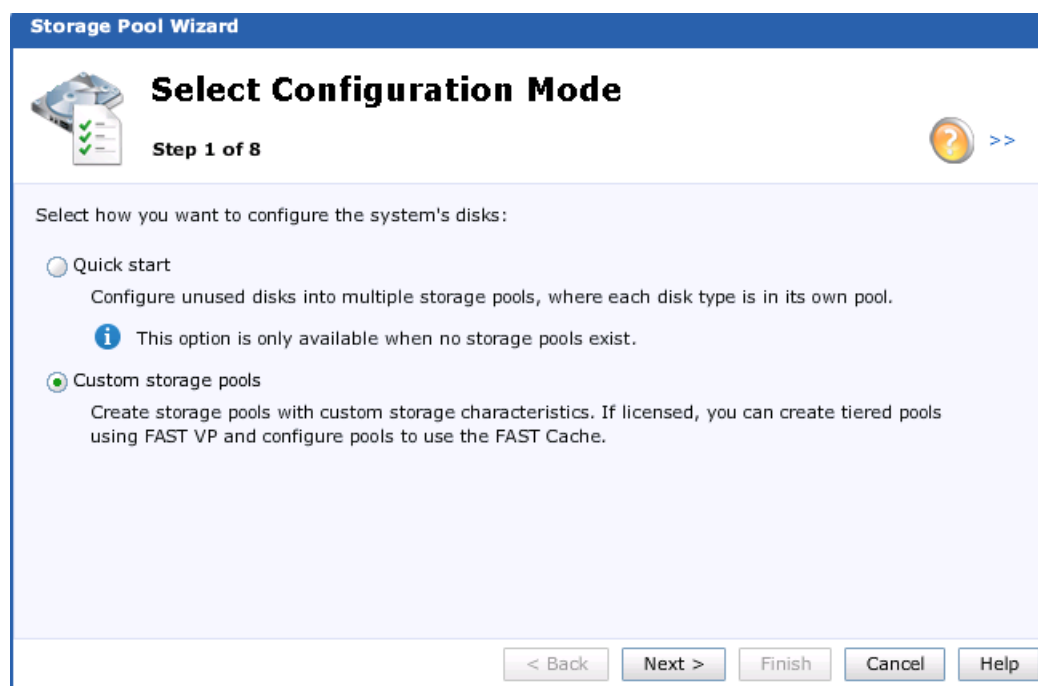


**Figure 86** *Creating Storage Pools in EMC Unisphere*



3. In the **Select Configuration Mode** window, choose **Custom Storage Pools**.


**Figure 87** *Storage Pool – Configuration Mode*



4. In the **Specify Pool Name** window provide a name and description and click **Next**.

Figure 88 Storage Pool – Name and Description

**Storage Pool Wizard**

 **Specify Pool Name**

**Step 2 of 8**

Specify a name and optional description.


Name: \*

Description:

5. Skip the **Fast VP Not Licensed** page by clicking **Next**.
6. In the **Select Storage** window select **Performance Tier** and have the **Performance Tier RAID Type** as default - RAID 5 (4+1) as shown in the below figure.

Figure 89 Storage Pool – Storage Tier

**Storage Pool Wizard**

 **Select Storage**

**Step 4 of 8**

Select the storage tiers you want to use for the new pool.

	Storage Tier	Disk Type	Unused Disks	Unused Raw Capacity
<input type="checkbox"/>	Extreme Performance Tier	Flash	3	550.3 GB
<input checked="" type="checkbox"/>	Performance Tier	SAS	45	23.5 TB
<input type="checkbox"/>	Capacity Tier	NL SAS	0	0 GB (None Available)

Uses SAS disks to provide high performance. These disks do not provide the same read/write performance as Extreme Performance (Flash) disks, but offer much lower cost per GB of storage.

Performance Tier

RAID Type: RAID 5 (4+1) (Usable capacity: 16.4 TB) [Change](#)

< Back Next > Finish Cancel Help

7. In the **Select Amount of Storage** window, choose Use 5 of 45 disks from the drop-down list under the **Performance Tier** section.

**Figure 90** *Storage Pool – Amount of Storage*

**Storage Pool Wizard**

**Select Amount of Storage**

Step 5 of 8

Select the amount of storage for each selected tier. The number of disks you can choose is based on the RAID configuration selected. The maximum number of disks you can configure will ensure that enough disks are kept unused to satisfy the hot spare policy.  
[More information](#)

Performance Tier

600 GB (10K RPM) SAS Disks: Use 5 of 45 disks (2.0 TB)

Total Disks to Configure: 5

Total Usable Capacity: 2.0

Use none of the 45 disks

Use 5 of 45 disks (2.0 TB)

Use 10 of 45 disks (4.1 TB)

Use 15 of 45 disks (6.2 TB)

Use 20 of 45 disks (8.3 TB)

< Back Next > Finish Cancel Help

- Click **Next** and Choose No to “do you want this storage pool to use the Fast Cache?” question and click **Next**.

**Figure 91** *Storage Pool – Fast Cache*

**Storage Pool Wizard**

**FAST Cache**

Step 6 of 8

The FAST Cache exists on the system. Each storage pool can be configured to use the FAST Cache. The FAST Cache is shared by all storage pools configured to use it.

Do you want this storage pool to use the FAST Cache?

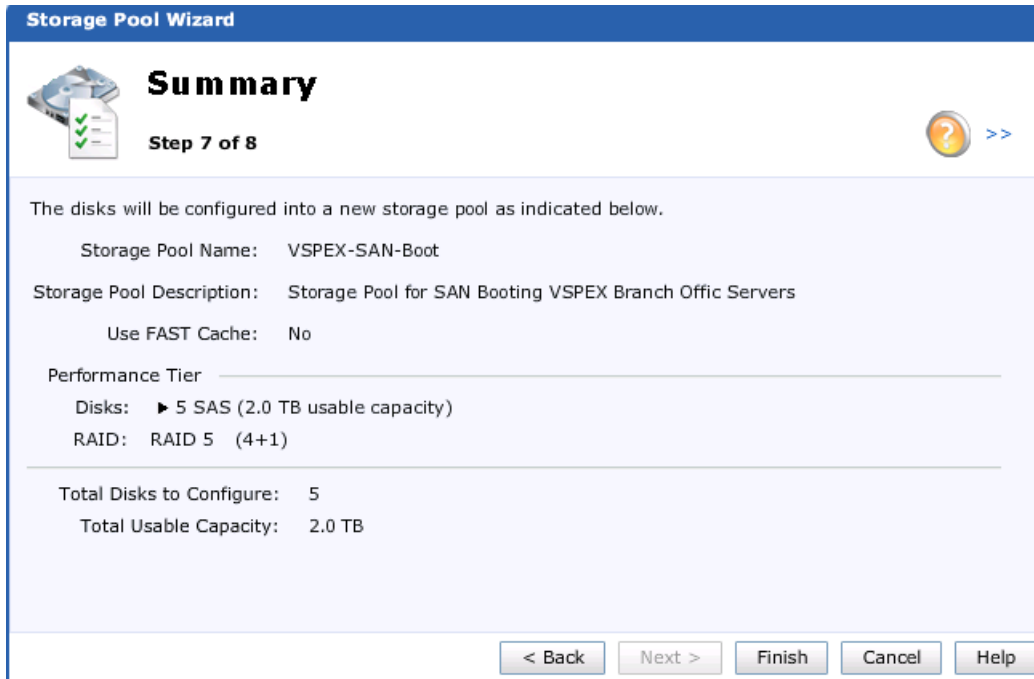
☐ Yes

☒ No

< Back Next > Finish Cancel Help

- Review the disk configuration for this storage pool in the **Summary** page and click **Finish**.

**Figure 92** *Storage Pool – Summary*



**Storage Pool Wizard**

**Summary**

Step 7 of 8

The disks will be configured into a new storage pool as indicated below.

Storage Pool Name: VSPEX-SAN-Boot

Storage Pool Description: Storage Pool for SAN Booting VSPEX Branch Office Servers

Use FAST Cache: No

Performance Tier

Disks: 5 SAS (2.0 TB usable capacity)

RAID: RAID 5 (4+1)

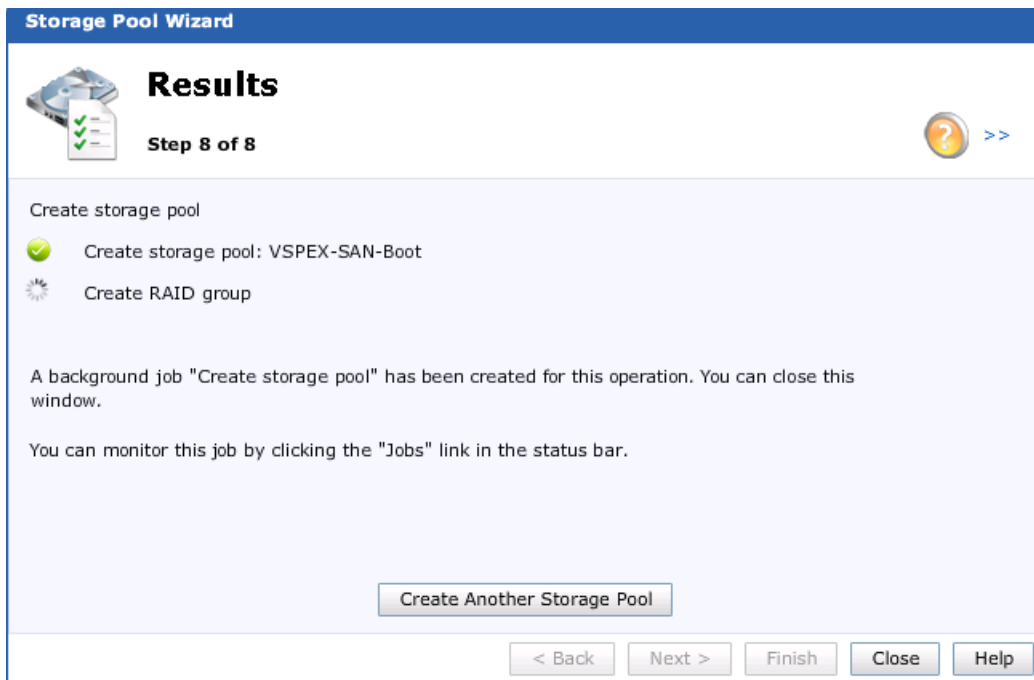
Total Disks to Configure: 5

Total Usable Capacity: 2.0 TB

< Back Next > Finish Cancel Help

10. In **Results** page, click **Create Another Storage Pool**.

**Figure 93** *Storage Pool – Results*



**Storage Pool Wizard**

**Results**

Step 8 of 8

Create storage pool

✓ Create storage pool: VSPEX-SAN-Boot

⌚ Create RAID group

A background job "Create storage pool" has been created for this operation. You can close this window.

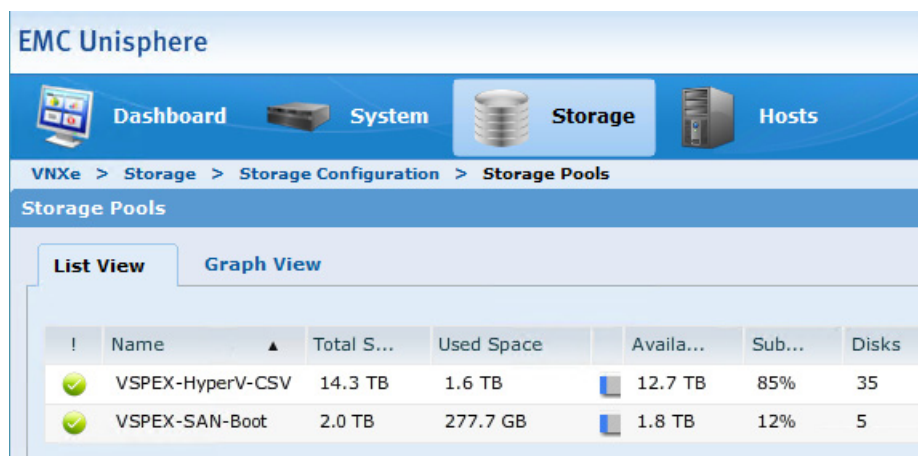
You can monitor this job by clicking the "Jobs" link in the status bar.

Create Another Storage Pool

< Back Next > Finish Close Help

11. Repeat the above steps to create the second storage pool for Hyper-V CSV with the same settings except for in the **Select Amount of Storage** window, Use 35 of 45 disks for this storage pool.

**Figure 94** Created Storage Pools in List View



The screenshot shows the EMC Unisphere interface with the 'Storage' tab selected. The breadcrumb trail is 'VNXe > Storage > Storage Configuration > Storage Pools'. Below the breadcrumb, there are tabs for 'List View' (selected) and 'Graph View'. A table lists two storage pools:

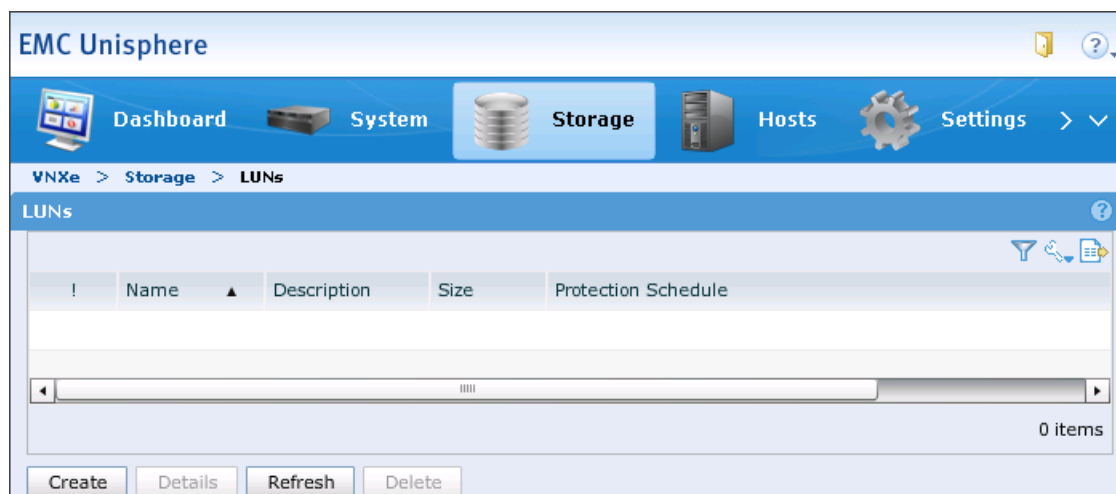
!	Name	Total S...	Used Space	Availa...	Sub...	Disks
✓	VSPEX-HyperV-CSV	14.3 TB	1.6 TB	12.7 TB	85%	35
✓	VSPEX-SAN-Boot	2.0 TB	277.7 GB	1.8 TB	12%	5

## 5. Create Boot LUNs and Configure Host Access

In this section we will be creating boot LUNs from the “VSPEX-SAN-Boot” storage pool and providing access to the hosts. LUNS for Hyper-V cluster shared volumes will be created and presented later after the installation and basic configuration of Operating System.

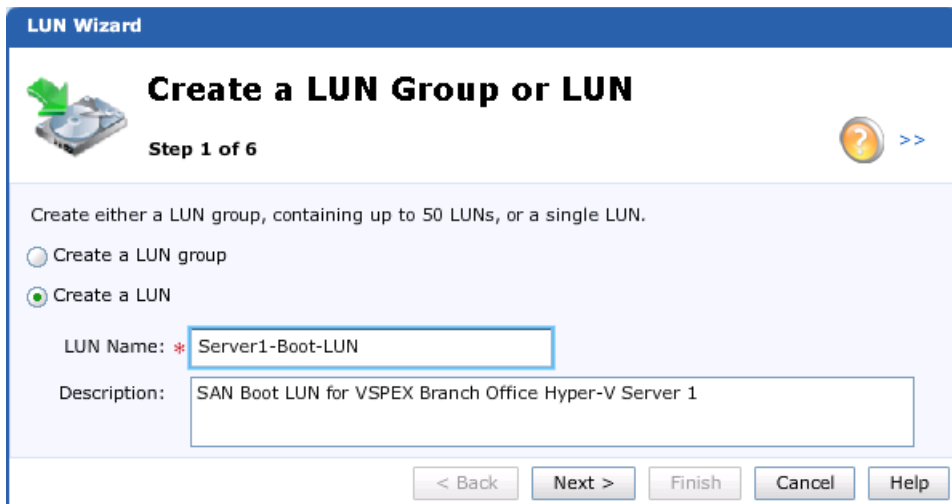
1. Launch the EMC VNXe Unisphere GUI.
2. Choose **Storage > LUNs** and click **Create**.

**Figure 95** Create LUNs



3. Click the **Create a LUN** radio button in the **Create a LUN Group** or **LUN** window.
4. Specify a name and description for the LUN. Click **Next**.

Figure 96 Creating LUN - Define LUN



**LUN Wizard**

**Create a LUN Group or LUN**

Step 1 of 6

Create either a LUN group, containing up to 50 LUNs, or a single LUN.

☐ Create a LUN group

☒ Create a LUN

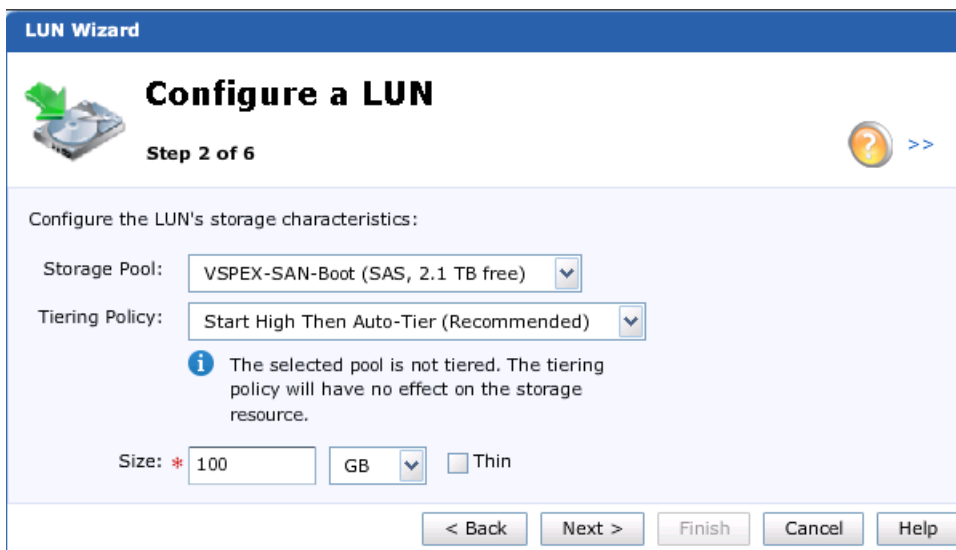
LUN Name: \* Server1-Boot-LUN

Description: SAN Boot LUN for VSPEX Branch Office Hyper-V Server 1

< Back Next > Finish Cancel Help

5. In the **Configure a LUN** window Choose the created “VSPEX-SAN-Boot” Storage Pool for the Hyper-V Boot LUN. Specify the LUN size and uncheck the Thin check box and click **Next**.

Figure 97 Creating LUN - Configure a LUN



**LUN Wizard**

**Configure a LUN**

Step 2 of 6

Configure the LUN's storage characteristics:

Storage Pool: VSPEX-SAN-Boot (SAS, 2.1 TB free)

Tiering Policy: Start High Then Auto-Tier (Recommended)

*The selected pool is not tiered. The tiering policy will have no effect on the storage resource.*

Size: \* 100 GB ☐ Thin

< Back Next > Finish Cancel Help

6. In the **Configure Snapshot Schedule** window choose Do not configure a snapshot schedule and click **Next**. (It is not recommended to configure snapshot for Boot LUNs)
7. In the **Configure Host Access** window of the LUN wizard, choose **LUN** from the drop-down list only for the VSPEX-BO-Server-1 and click **Next**.



**Note** Do not share boot LUN with multiple hosts. It is specific to a single host.

**Figure 98** *Creating LUN - Configure Host Access*

**LUN Wizard**

**Configure Host Access**

Step 4 of 6

Configure which hosts will access this storage:

Filter for:  Protocols: FC or iSCSI

!	Name	Network Address	Operating System	Protocol	Access
✓	VSPEX-BO-Server-1	hyperv1	Microsoft Hyper-V	FC, File	LUN
✓	VSPEX-BO-Server-2	hyperv2	Microsoft Hyper-V	FC, File	No Access

Filtered: 2 of 2

< Back Next > Finish Cancel Help

8. In the **Summary** page, confirm the LUN configuration and click **Finish** to complete the LUN creation and host access.
9. Repeat the above steps 1 to 5 to create boot LUNs for other hosts.
10. In the **Results** page, verify the configuration completion and click **Close**.

**Figure 99** *Creating LUN - Summary*

**LUN Wizard**

**Summary**

Step 5 of 6

Confirm the following LUN configuration:

Name: Server1-Boot-LUN

Description: SAN Boot LUN for VSPEX Branch Office Hyper-V Server 1

Storage Pool: VSPEX-SAN-Boot

Size: 100.0 GB

Thin: No

Tiering Policy: Start High Then Auto-Tier (Recommended)

Protection Schedule: None configured

LUN Access: ▼ 1 hosts configured  
VSPEX-BO-Server-1

Snapshot Access: No hosts configured

< Back Next > Finish Cancel Help

**Figure 100** Created Boot LUNs for Server 1 and Server 2



At this point, we have end-to-end FC storage access from servers in UCS to the specific boot LUN on the VNXe storage devices. The physical servers are now ready for the Microsoft Windows Server 2012 R2 OS installation.

## Installation of Windows Server 2012 R2 Datacenter

The following steps provide the details necessary to prepare the host for the installation of Windows Server 2012 R2 Datacenter Edition. It is assumed that the SAN has been zoned and the VNXe3200 has masked the LUN so that only a single path to server is available at this stage. All the steps given below need to be carried out on all the physical servers used for this solution.

1. Install Windows Server 2012 R2 on all the physical servers with the boot volume on the EMC VNXe3200.
2. Perform some initial configuration tasks that are common for all servers used for this solution.
  - Install the latest hardware drivers.
  - Configure the network.
  - Rename computer and join it to Active Directory Domain.
  - Install Windows roles and features.
  - Configure other common criteria.
  - Configure Networks and Virtual Switches.
  - Configure MPIO.
  - Create Cluster.

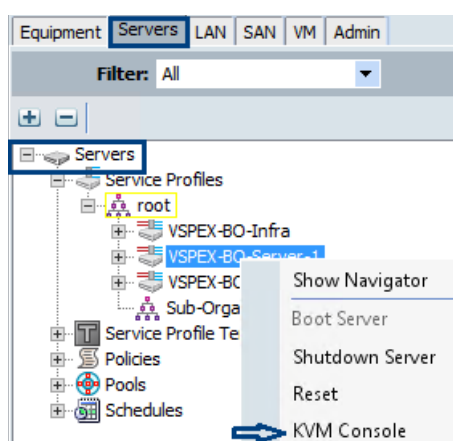


**Note**

In order for the Windows Installer to recognize the Fibre Channel SAN boot disk for the initial server, the Cisco UCS fnic (storage) driver must be loaded into the Windows installer during installation. Download the latest Unified Computing System (UCS) drivers from [www.cisco.com](http://www.cisco.com) under Cisco UCS B-Series Blade Server Software and place the ISO on the same machine with the Windows Server 2012 R2 installation media.

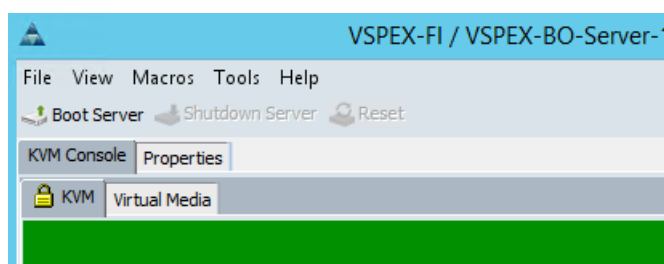
1. Launch the **Cisco UCS Manager** in a browser.
2. Expand the node as **Servers > Service Profiles > root > VSPEX-BO-Server-1**
3. Right-click the **Service Profile** and choose **KVM Console** from the menu.

**Figure 101** *KVM Console for Service Profile*



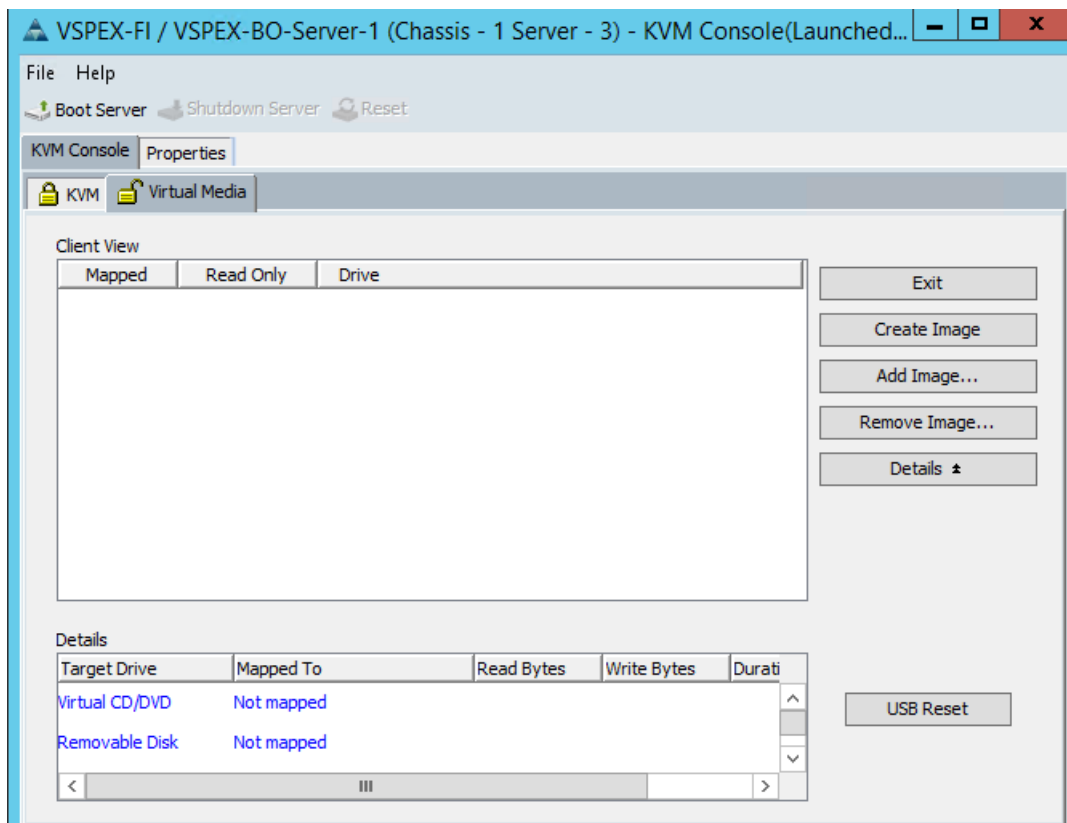
4. Click the **Virtual Media** tab. In the **Unencrypted Virtual Media Session** window accept the session and click **Apply**.

**Figure 102** *KVM Console – Virtual Media*



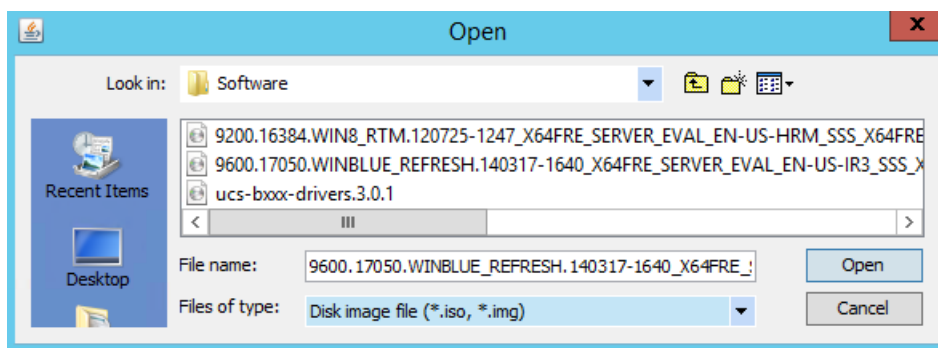
5. Click **Add Image** on the right (see Figure 103).

**Figure 103**      *Adding OS Image*



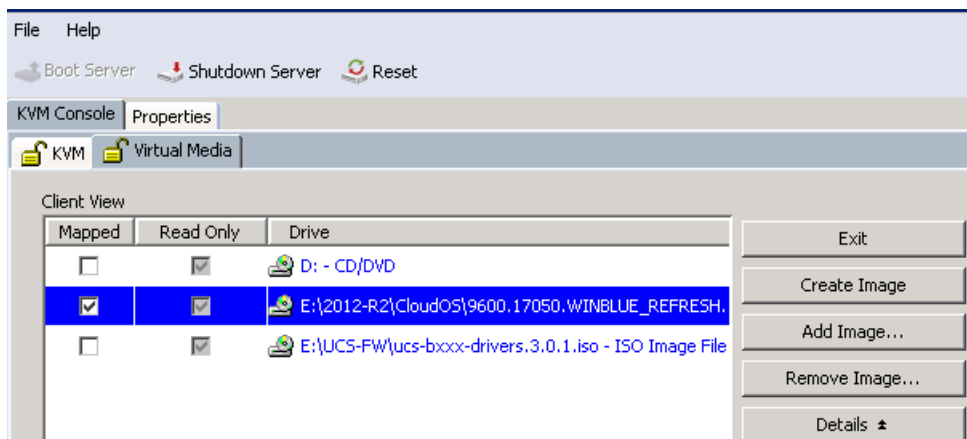
6. Browse to the location where you have stored the Windows Server 2012 R2 installation media, select it and click **Open**.
7. Repeat the process to add an image of the Cisco device driver installation media.

**Figure 104**      *Select Windows Server 2012 R2 Image*



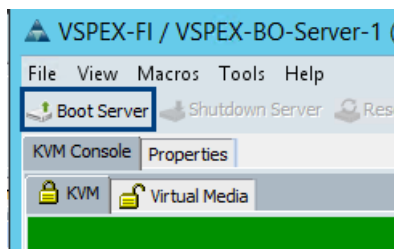
8. Click the check box by the Windows Server 2012 R2 installation media. Then click the **KVM** tab to return to the KVM window.

**Figure 105**      *Map ISO Image File*



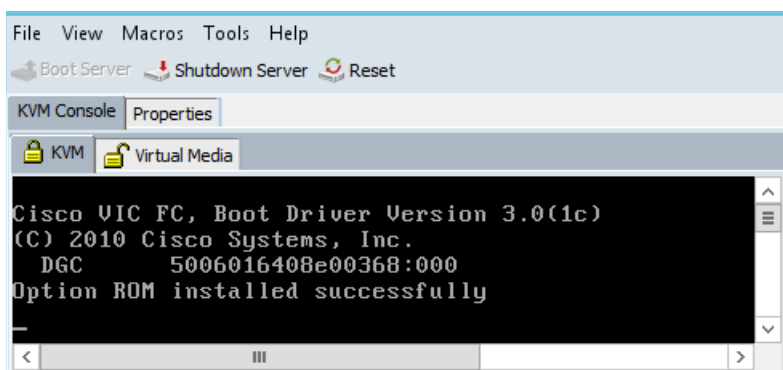
9. Click **Boot Server** to boot the server.
10. Click **OK** twice on the pop-up window to proceed with the booting of the server

**Figure 106**      *Reboot Server*



If the Cisco UCS and EMC VNXe are configured correctly in the previous sections then you will see the SAN boot LUN during the server boot (see Figure 107).

**Figure 107**      *Verify SAN Boot LUN on Reboot*



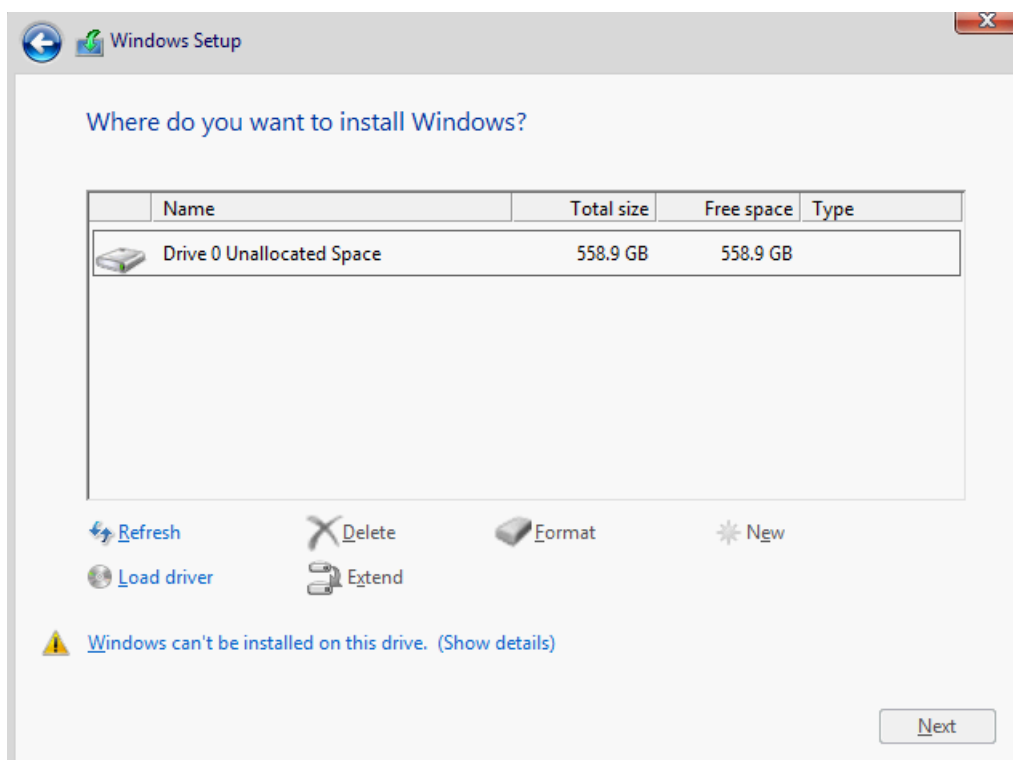
11. The installation of Windows Server 2012 R2 starts. Select the appropriate localization features and click **Next**. On the following screen click **Install Now**.

**Figure 108**      *Windows Server 2012 Setup*



12. Select the Windows Server 2012 R2 Datacenter (Server with a GUI) option. Click **Next**.
13. Click the check box to accept the license terms and click **Next**.
14. Click Custom: Install Windows only (advanced).
15. You will not see any SAN disks because the Cisco VIC 1240 drivers are not included as part of the Windows Server 2012 R2 installation media. You will have to manually load them. So click **Load Driver**.

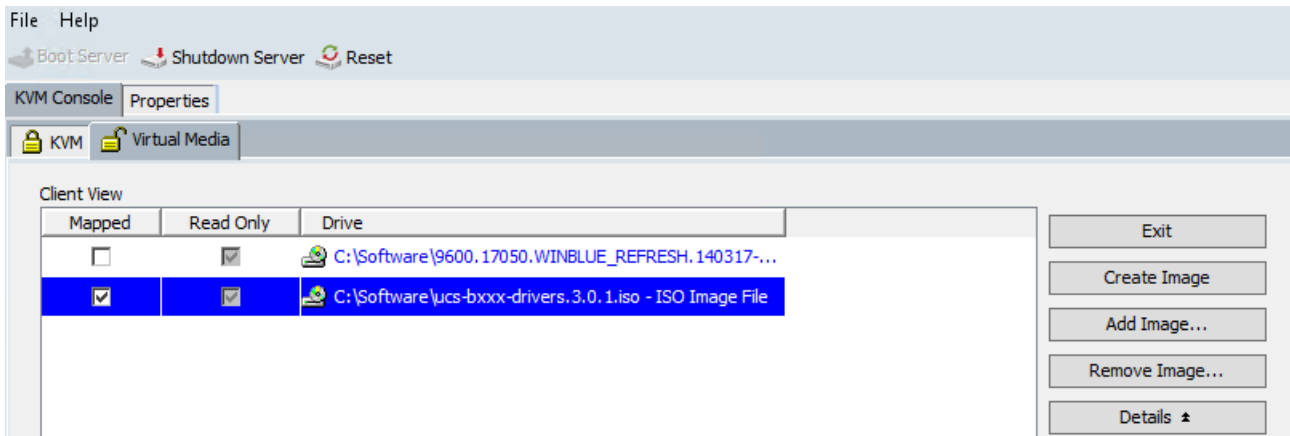
**Figure 109**      *Load Driver for Windows Server 2012 R2 Installation*



16. The **Load driver** window appears. Before continuing, mount the Cisco driver image.
17. On the KVM console, select the **Virtual Media** tab.

18. Uncheck the checkbox by the Windows installation media. On the warning message click **OK** to continue.
19. Now, check the file checkbox by the Cisco driver media and click the **KVM** tab.

**Figure 110**      *Map Cisco Driver Media*



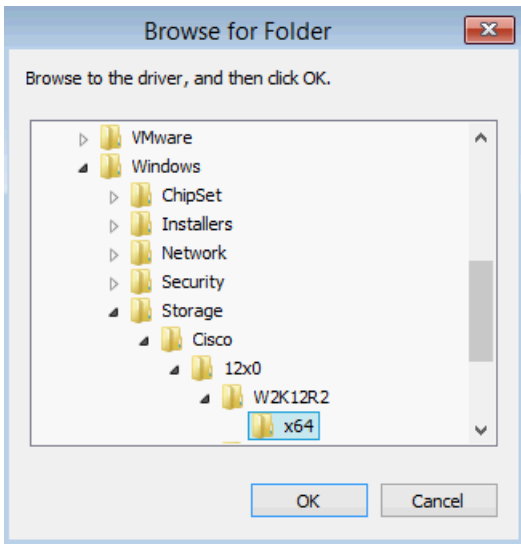
20. Back on the **Load driver** page, click **Browse**.

**Figure 111**      *Specify Installation Media*



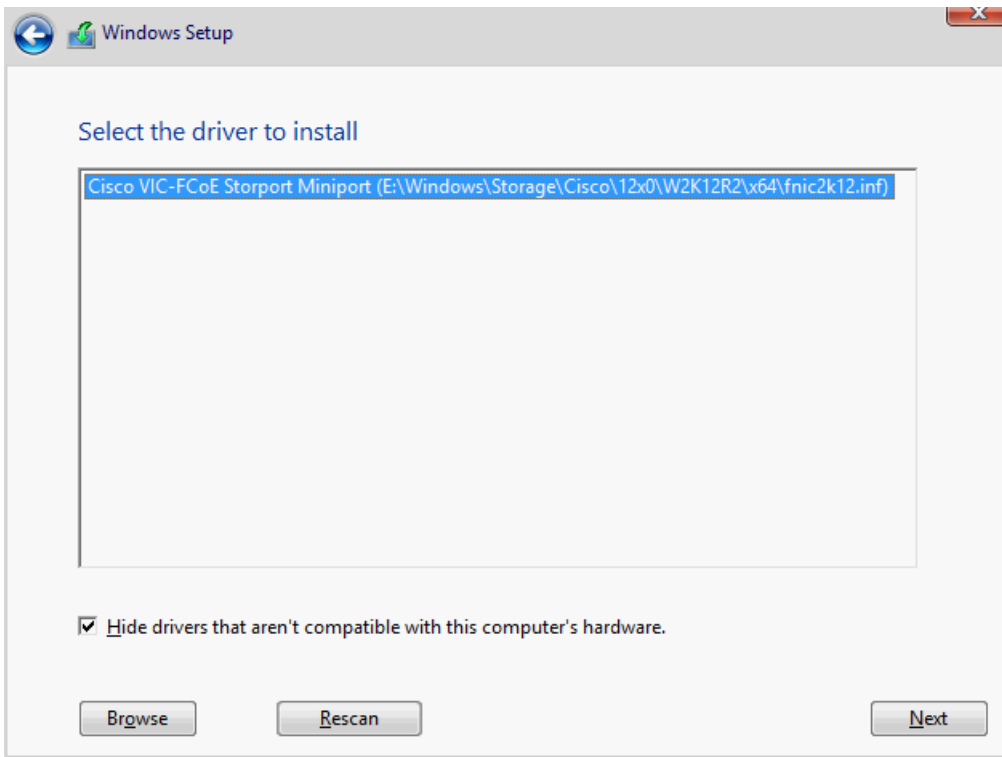
21. Expand the CDROM containing the Cisco driver media. Browse to **Windows > Storage > Cisco > 12x0 > W2K12R2 > x64**.
22. Click **OK** to continue.

**Figure 112**      *Navigate to the folder*



23. On the **Select the driver to install** page, validate you have selected the proper driver and click **Next** to continue.

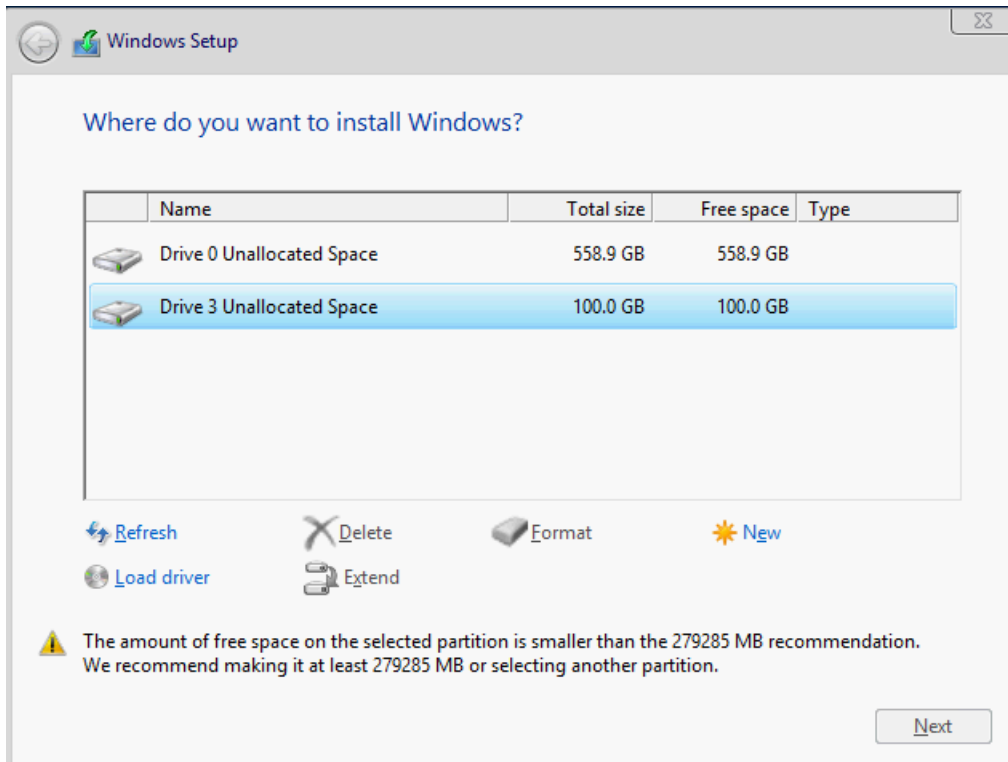
**Figure 113**      *Select Driver to Install*



24. Repeat this process to install the NIC drivers now or it can be installed after the OS installation is completed.
25. After the driver installation, the boot SAN disk is now visible. Return to the **Virtual Media** tab and re-select the Windows installation media.

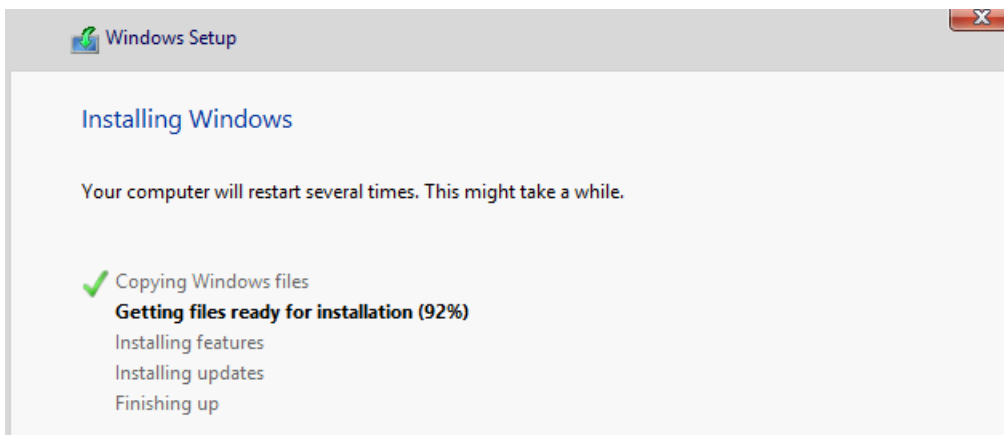
26. Back on the **KVM** tab, click Refresh and click **Next** to continue.

*Figure 114 Select Drive to Install Windows*



27. Windows will now proceed with installation and after the completion of this process it will reboot.

*Figure 115 Install Windows*



28. Enter a password for the local administrator account. Re-enter to validate. Click **Finish** to complete the installation

**Figure 116**      *Authentication for Completing Installation*

The image shows a Windows Settings window with a dark blue background. At the top, the word "Settings" is displayed in large white font. Below it, a message reads: "Type a password for the built-in administrator account that you can use to sign in to this computer." There are three input fields: "User name" with the text "Administrator" entered, "Password" which is empty, and "Reenter password" which is also empty.

## Install Device Drivers

1. Select Macros on the KVM console. From the drop down menu, select Static Macros and Ctrl-Alt-Del to bring up the Windows sign in screen.
2. Log into the new machine using the password entered in the previous step. Enter a carriage return after entering the password.
3. If you did not load the NIC drivers earlier, open a PowerShell window and issue the command as shown in the below figure assuming the Cisco driver media is mounted on drive F:

**Figure 117**      *Load NIC Drivers Using PowerShell*

```
PS C:\Users\Administrator> PnPutil.exe -i -a F:\Windows\Network\Cisco\12x0\W2K12R2\x64\enic6x64.inf
Microsoft PnP Utility

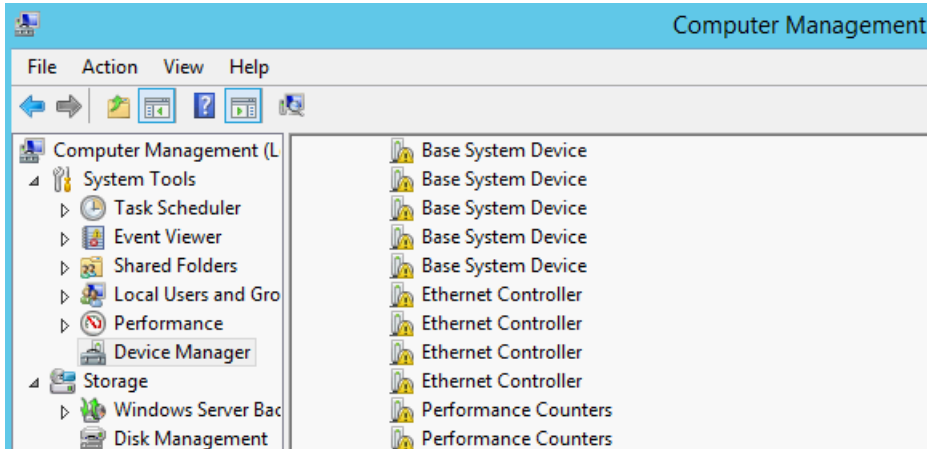
Processing inf :          enic6x64.inf
Successfully installed the driver on a device on the system.
Driver package added successfully.
Published name :          oem3.inf

Total attempted:          1
Number successfully imported: 1
```

4. Also install the Intel Chipset Driver software from the Cisco driver media to get rid of other uninstalled drivers (see Figure 118).

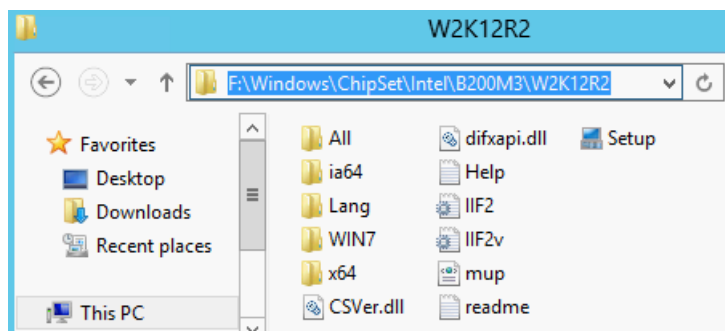


**Figure 118**      *Install Intel Chipset Driver Software*



5. Browse to the chipset driver location and double-click setup.exe to start the installation.

**Figure 119**      *Browse Chipset Driver Location and Install Software*



6. Click **Next** and after the installation is complete.
7. click **Finish**.

Figure 120 Intel Chipset Device Software

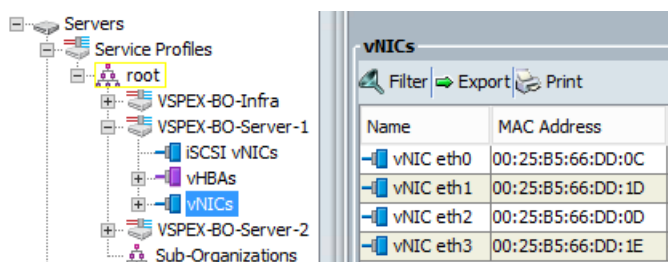


## Configure the Network

This section provides details on configuring the network adapters like renaming and assigning IP addresses to them as per their intended roles/functions.

1. In the **Cisco UCS Manager** GUI, expand the **Service Profile** for the machine, and select the vNICs to display the MAC addresses assigned by UCS and also determine their respective VLAN Name/ID.

Figure 121 MAC Addresses Assigned by UCS for vNICs



2. In the **Windows PowerShell** prompt, enter the Get-NetAdapter cmdlet. This will list the MAC addresses of the networks assigned within the operating system (see Figure 122).

Figure 122 Verify MAC Addresses Using PowerShell Command

```
PS C:\Users\Administrator> Get-NetAdapter | Format-Table -AutoSize
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet 4	Cisco VIC Ethernet Interface #4	30	Up	00-25-B5-66-DD-1E	10 Gbps
Ethernet 3	Cisco VIC Ethernet Interface #3	26	Up	00-25-B5-66-DD-1D	10 Gbps
Ethernet 2	Cisco VIC Ethernet Interface #2	22	Up	00-25-B5-66-DD-0D	10 Gbps
Ethernet	Cisco VIC Ethernet Interface	18	Up	00-25-B5-66-DD-0C	10 Gbps

- From the above information gathered compare the MAC addresses and their respective VLAN to rename the adapters using the Rename-NetAdapter cmdlet as per their intended role for easy identification and troubleshooting.

**Figure 123** *Rename the Network Adapters*

```
PS C:\Users\Administrator> Rename-NetAdapter -Name "Ethernet" -NewName "Mgmt"
PS C:\Users\Administrator> Rename-NetAdapter -Name "Ethernet 3" -NewName "CSV"
PS C:\Users\Administrator> Rename-NetAdapter -Name "Ethernet 2" -NewName "Livemigration"
PS C:\Users\Administrator> Rename-NetAdapter -Name "Ethernet 4" -NewName "VMaccess"
PS C:\Users\Administrator> Get-NetAdapter | Format-Table -AutoSize
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
VMaccess	Cisco VIC Ethernet Interface #4	15	Up	00-25-B5-66-DD-1E	10 Gbps
CSV	Cisco VIC Ethernet Interface #3	14	Up	00-25-B5-66-DD-1D	10 Gbps
Livemigration	Cisco VIC Ethernet Interface #2	13	Up	00-25-B5-66-DD-0D	10 Gbps
Mgmt	Cisco VIC Ethernet Interface	12	Up	00-25-B5-66-DD-0C	10 Gbps

- From within PowerShell assign IP addresses to the Management, LiveMigration and CSV network Adapters using the syntax as shown in the below figure. Also configure DNS server address for the management network.

**Figure 124** *Assign IP Addresses Using PowerShell Command*

```
PS C:\Users\Administrator> New-NetIPAddress -ifIndex 12 -IPAddress 10.29.180.169 -PrefixLength 24 -DefaultGateway 10.29.180.1
```

## Rename Computer and Join it to Active Directory Domain

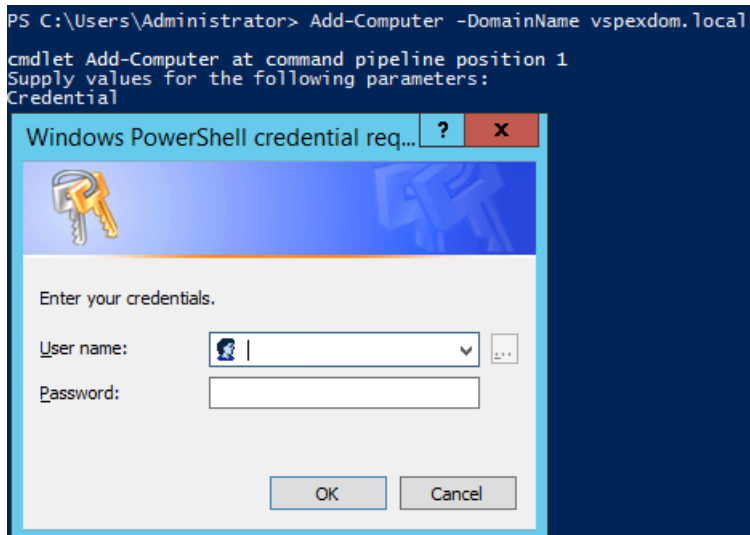
- Rename the computer using the below PowerShell command syntax and restart.

**Figure 125** *Rename Computer Using PowerShell Command*

```
PS C:\Users\Administrator> Rename-Computer -NewName Hyperv1
WARNING: The changes will take effect after you restart the computer WIN-A5CEQ33T01C.
PS C:\Users\Administrator> Restart-Computer_
```

- Join the computer to the Active Directory domain as shown in the below figure and restart the server. A domain account credentials with appropriate permissions is required to join a computer to the domain.

**Figure 126** *Join Computer to Active Directory Domain*



## Install Windows Roles and Features

This section shows the installation of Windows roles and features that will be required for this solution from the PowerShell command line.

1. Install the MPIO Windows feature using the below PowerShell command

**Install-WindowsFeature -Name Multipath-IO -IncludeManagementTools**

2. Install the Failover-Clustering Windows feature using the below PowerShell command

**Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools**

3. Install the Hyper-V Windows role using the below PowerShell command

**Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart**

You can also manually add the roles and features through **Server Manager > Manage > Add Roles and Features**.

## Configure Other Common Criteria

1. At this stage install any management agent or configure other system settings like firewall, remote desktop, etc. as per your organization requirements and policies.
2. Run **Windows Update** to fully patch the server.

## Configuring Virtual Switches

This section provides the steps to configure the Hyper-V virtual using the Hyper-V manager switch. The virtual machine network adapters attach to this virtual switch to communicate with the outside world. A dedicated NIC named VMaccess is used for creating the Hyper-V virtual switch.

1. Determine the network adapter name on the Hyper-V host by executing the following PowerShell cmdlet:

```
Get-NetAdapter | ft -AutoSize
```

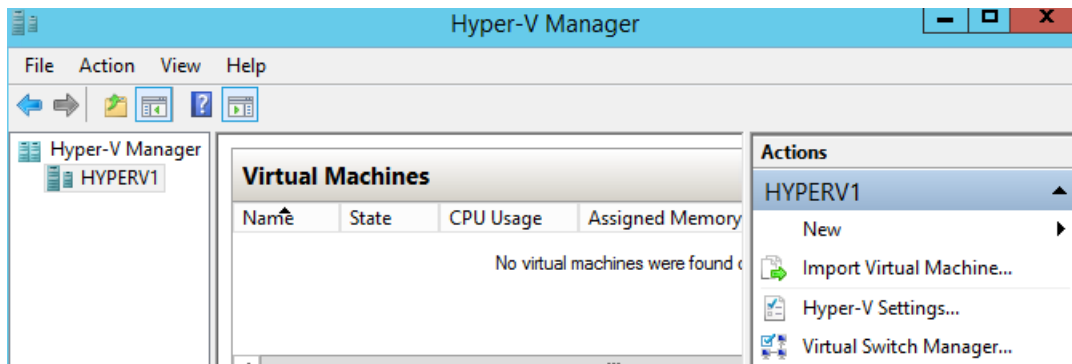
**Figure 127**      *Identifying Network Adapter Name*

```
PS C:\Users\administrator.VSPEXDOM> Get-NetAdapter | ft -AutoSize
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
VMaccess	Cisco VIC Ethernet Interface #4	15	Up	00-25-B5-66-DD-1E	10 Gbps
CSV	Cisco VIC Ethernet Interface #3	14	Up	00-25-B5-66-DD-1D	10 Gbps
LiveMigration	Cisco VIC Ethernet Interface #2	13	Up	00-25-B5-66-DD-0D	10 Gbps
Mgmt	Cisco VIC Ethernet Interface	12	Up	00-25-B5-66-DD-0C	10 Gbps

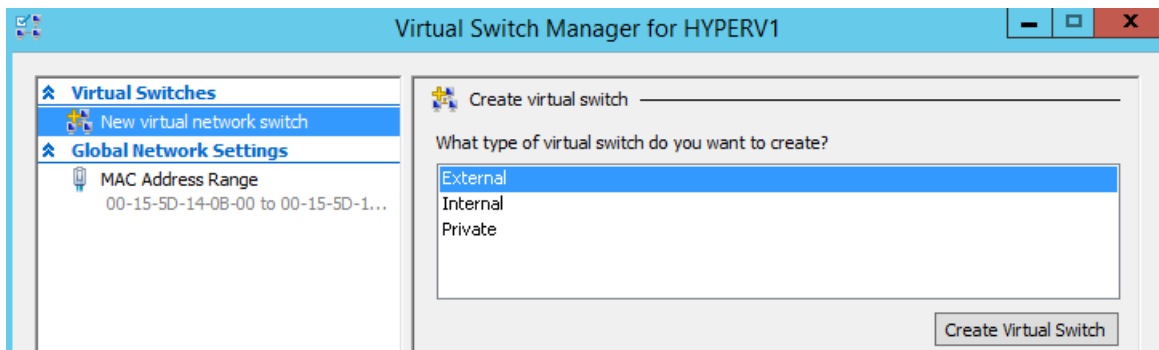
2. Launch the **Hyper-V Manager** console and choose **Virtual Switch Manager** under Actions.

**Figure 128**      *Select vSwitch in Hyper-V Manager*



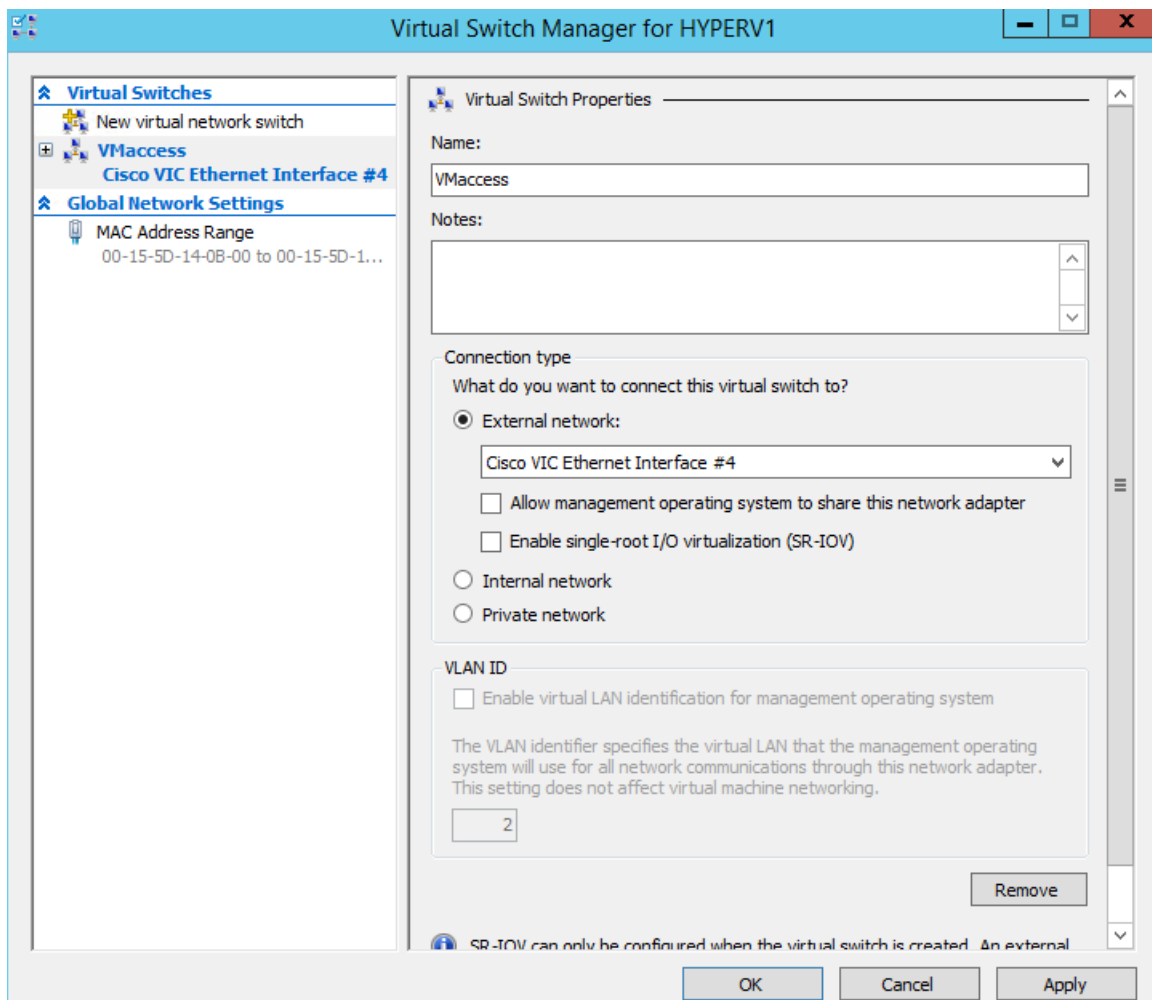
3. In the **Virtual Switch Manager** page, choose **New virtual network switch** under Virtual Switches and **External** under **Create Virtual Switch** and click **Create Virtual Switch**.

**Figure 129**      *Select vSwitch Type*



4. On the Properties of the virtual switch, enter a Name. Make sure the radio button for External network is selected. From the drop down list, select the description of the vNIC on which you are creating this virtual switch.
5. Uncheck the **Allow management operating system to share this network adapter** checkbox and click **OK**.

**Figure 130**      *Virtual Switch Manager*



6. Repeat the above steps in this section to create virtual switches on all the Hyper-V hosts.

## Configure MPIO

Now that Windows MPIO feature is enabled, we can add the additional paths to the boot LUN and configure MPIO. This segment can be subdivided into the following segments:

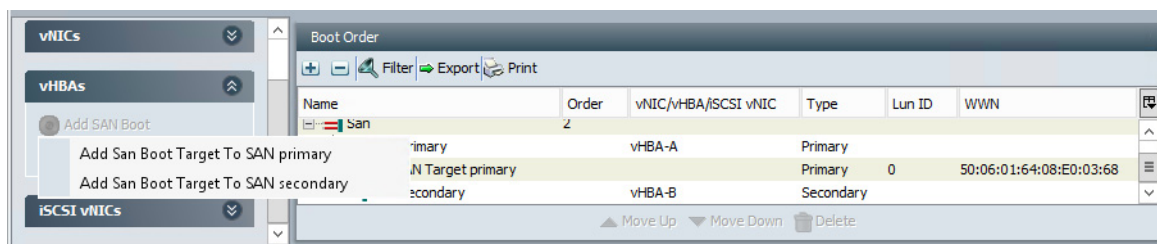
1. Add additional Paths in UCS boot Policy
2. Add additional paths to the boot LUN in EMC VNXe
3. Create shared storage in EMC VNXe
4. Configure MPIO in Hyper-V hosts.

## Add additional Paths in UCS boot Policy

In the previous section we have created a UCS boot policy named SAN-Boot-Policy with single path. The below steps provides details to modify the UCS boot policy to add additional paths to the boot LUN. Refer the tables in the “” section above.

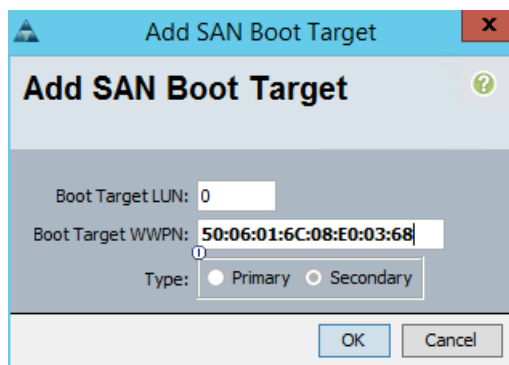
1. Launch **Cisco UCS Manager** and choose the **Servers** tab.
2. Go to **Policies > root > Boot Policies**
3. Under Boot Policies, select the SAN-boot Policy that was created earlier in the “” section.
4. On the right side of the window under **vHBAs**, click **Add SAN Boot Target** and choose **Add San Boot Target to SAN Primary** (see Figure 131).

**Figure 131** Add SAN Boot Target



5. In the **Add SAN Boot Target** window, enter 0 in the Boot Target LUN field.
6. In the **Boot Target WWPN** field, add the WWPN of the VNxe-SPB-Port0
7. The Type is automatically selected as Secondary since the primary boot target already exists.
8. Click **Yes** to confirm the changes. This will reboot the servers that use this policy for the changes to be applied.

**Figure 132** Add SAN Boot Target for Secondary



9. Similarly add SAN Secondary for vHBA-B and add SAN Boot Targets to SAN Secondary (both Primary and Secondary targets) to it to add the remaining paths to the boot LUN.
10. Verify the UCS service profiles boot order and FC zones to see if they are updated with all the additional paths (see Figure 133 and 134).

Figure 133 Verify UCS Service Profile Boot Order

Name	Initiator WWPN	Initi...	Target WWPN
ucs_VSPEX-FI_A_1_VSPEX-BO-Server-1_vHBA-A	20:00:00:25:B5:06:0D:2E	vHBA-A	
FC Target 50:06:01:64:08:E0:03:68			50:06:01:64:08:E0:03:68
ucs_VSPEX-FI_A_4_VSPEX-BO-Server-1_vHBA-A	20:00:00:25:B5:06:0D:2E	vHBA-A	
FC Target 50:06:01:6C:08:E0:03:68			50:06:01:6C:08:E0:03:68
ucs_VSPEX-FI_B_7_VSPEX-BO-Server-1_vHBA-B	20:00:00:25:B5:06:0D:2D	vHBA-B	
FC Target 50:06:01:6D:08:E0:03:68			50:06:01:6D:08:E0:03:68
ucs_VSPEX-FI_B_8_VSPEX-BO-Server-1_vHBA-B	20:00:00:25:B5:06:0D:2D	vHBA-B	
FC Target 50:06:01:65:08:E0:03:68			50:06:01:65:08:E0:03:68

Figure 134 Verify FC Zones

Name	Initiator WWPN	Initi...	Target WWPN
ucs_VSPEX-FI_A_1_VSPEX-BO-Server-1_vHBA-A	20:00:00:25:B5:06:0D:2E	vHBA-A	
FC Target 50:06:01:64:08:E0:03:68			50:06:01:64:08:E0:03:68
ucs_VSPEX-FI_A_4_VSPEX-BO-Server-1_vHBA-A	20:00:00:25:B5:06:0D:2E	vHBA-A	
FC Target 50:06:01:6C:08:E0:03:68			50:06:01:6C:08:E0:03:68
ucs_VSPEX-FI_B_7_VSPEX-BO-Server-1_vHBA-B	20:00:00:25:B5:06:0D:2D	vHBA-B	
FC Target 50:06:01:6D:08:E0:03:68			50:06:01:6D:08:E0:03:68
ucs_VSPEX-FI_B_8_VSPEX-BO-Server-1_vHBA-B	20:00:00:25:B5:06:0D:2D	vHBA-B	
FC Target 50:06:01:65:08:E0:03:68			50:06:01:65:08:E0:03:68

This concludes the UCS boot policy configuration part for additional paths.

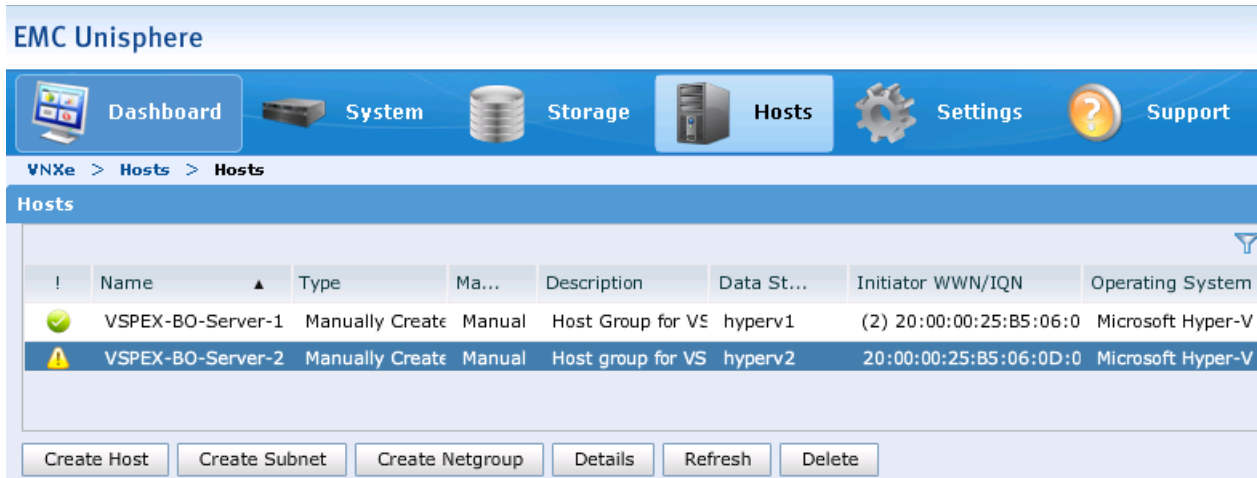
## Add Additional Paths to Boot LUN in EMC VNXe

After adding additional paths to the UCS boot policy the zones and zonesets will be updated to reflect the multiple paths to the LUN, it is necessary to configure the EMC VNXe 3200 array to also present the boot LUN to the additional paths.

1. In the Unisphere, choose to **Hosts > Hosts**.
2. Select a Host and click **Details**.

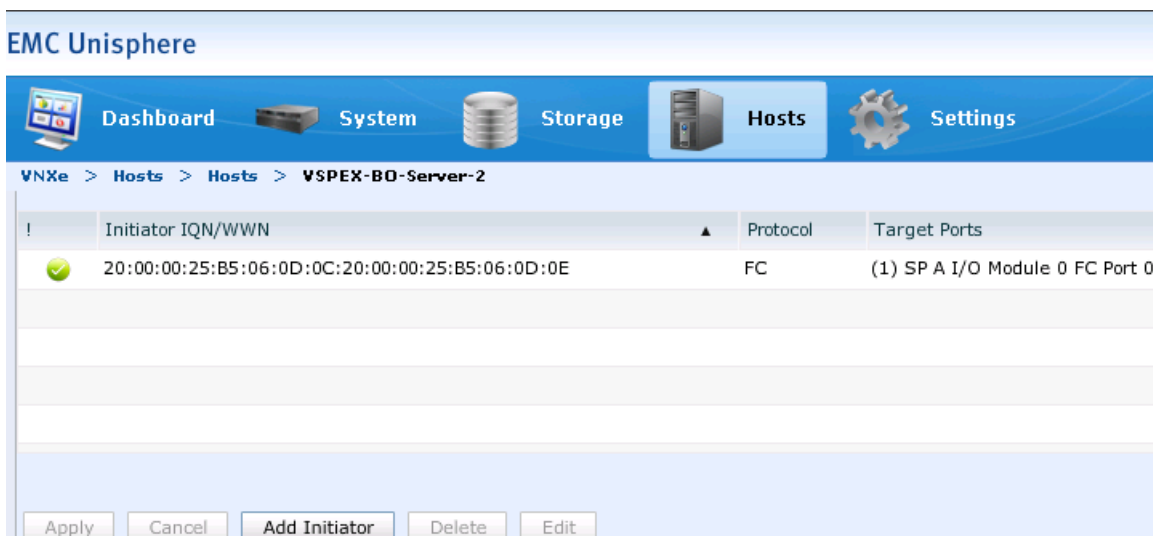


**Figure 135**      *Select Host in EMC Unisphere*



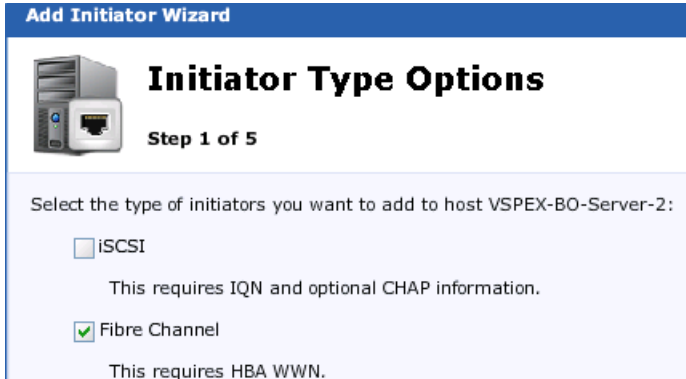
- Next click **Initiator** tab and click **Add Initiator**.

**Figure 136**      *Add Initiator for Host*



- In the **Initiator wizard** window, choose **Fibre Channel** for the **Initiator Type** options and click **Next**.

Figure 137 Add Initiator: Select Initiator Type



**Add Initiator Wizard**

**Initiator Type Options**

Step 1 of 5

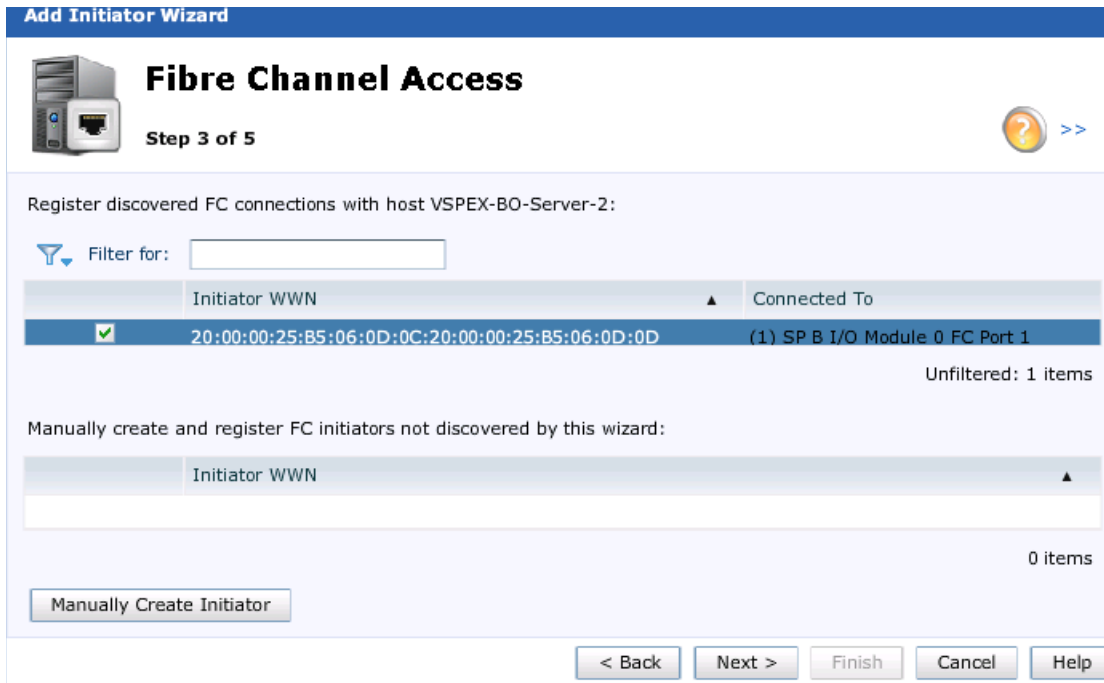
Select the type of initiators you want to add to host VSPEX-BO-Server-2:

☐ iSCSI  
This requires IQN and optional CHAP information.

☒ Fibre Channel  
This requires HBA WWN.

- In the **Fibre channel Access** page select the appropriate Initiator WWN from the list for the host. In this case it is the vHBA-B WWN for server 2 (see Figure 138).

Figure 138 Add Initiator: FC Access



**Add Initiator Wizard**

**Fibre Channel Access**

Step 3 of 5

Register discovered FC connections with host VSPEX-BO-Server-2:

Filter for:

	Initiator WWN	Connected To
<input checked="" type="checkbox"/>	20:00:00:25:B5:06:0D:0C:20:00:00:25:B5:06:0D:0D	(1) SP B I/O Module 0 FC Port 1

Unfiltered: 1 items

Manually create and register FC initiators not discovered by this wizard:

Initiator WWN
<input type="text"/>

0 items

- In the **Summary** page verify the initiator configuration and click **Finish**.
- Finally click **Close** in the **Results** window and verify the same as shown in the below figure.
- Repeat the above steps for the other hosts to add the additional paths and verify the same (see Figure 139).

Figure 139 Verify the Added Initiator

VNXe > Hosts > Initiators					
Initiators					
Initiators		Initiator Paths			
!	Initiator IQN/WWN	Host	P..	Target Ports	
✓	20:00:00:25:B5:06:0D:0C:20:00:00:25:B5:06:0D:0D	VSPEX-BO-Server-2	FC	(1) SP B I/O Module 0 FC Port 1	
✓	20:00:00:25:B5:06:0D:0C:20:00:00:25:B5:06:0D:0E	VSPEX-BO-Server-2	FC	(1) SP A I/O Module 0 FC Port 0	
✓	20:00:00:25:B5:06:0D:2C:20:00:00:25:B5:06:0D:2D	VSPEX-BO-Server-1	FC	(1) SP B I/O Module 0 FC Port 1	
✓	20:00:00:25:B5:06:0D:2C:20:00:00:25:B5:06:0D:2E	VSPEX-BO-Server-1	FC	(1) SP A I/O Module 0 FC Port 0	

This concludes the EMC VNXe configuration part for additional paths

## Create Shared Storage in EMC VNXe

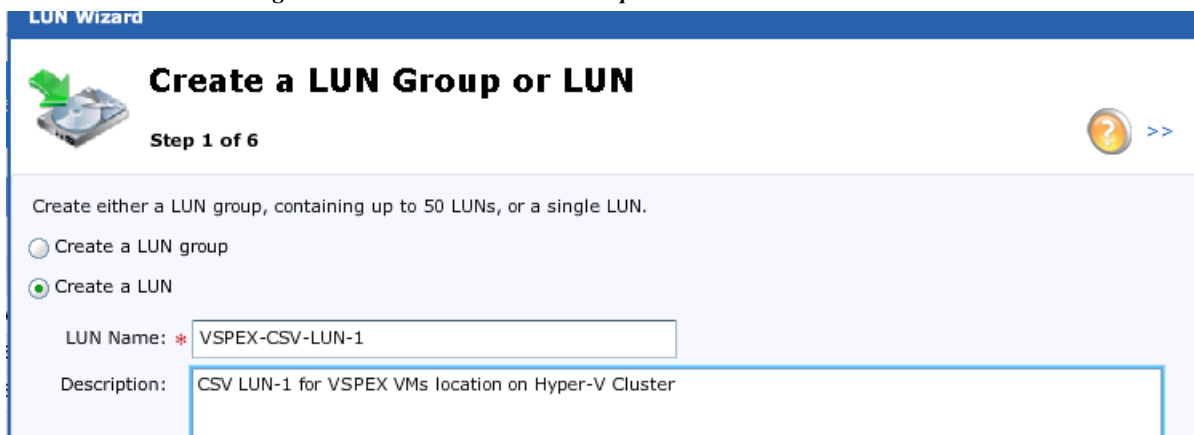
Microsoft Failover Clusters use shared storage for storing the VMs. For this solution we are creating three shared LUNs. The witness disk is used exclusively by the cluster and the cluster shared volumes will be used to store VM disks (vhdx). Table 15 summarizes the shared LUN details which will be used in this section to create them in the EMC VNXe array. The SP ownerships for the LUNs are spread across both the VNXe storage processors, A and B for better load balancing.

Table 15 LUN Details

LUN Name	LUN Site	Storage Pod	SP Owner	LUN Access	Purpose
Witness Disk	2 GB	VSPEX-HyperV-CSV	SP-B	Shared	Cluster quorum
CSV-LUN-1	6 TB	VSPEX-HyperV-CSV	SP-A	Shared	VM store location
CSV-LUN-2	6 TB	VSPEX-HyperV-CSV	SP-B	Shared	VM store location

1. Launch the **EMC VNXe Unisphere** GUI.
2. Select **Storage > LUNs** and click **Create**.
3. Click **Create a LUN** radio button in the **Create a LUN Group or LUN** window.
4. Specify a name and description for the LUN. click **Next**.

Figure 140 Create LUN Group



**LUN Wizard**

**Create a LUN Group or LUN**

Step 1 of 6

Create either a LUN group, containing up to 50 LUNs, or a single LUN.

☐ Create a LUN group

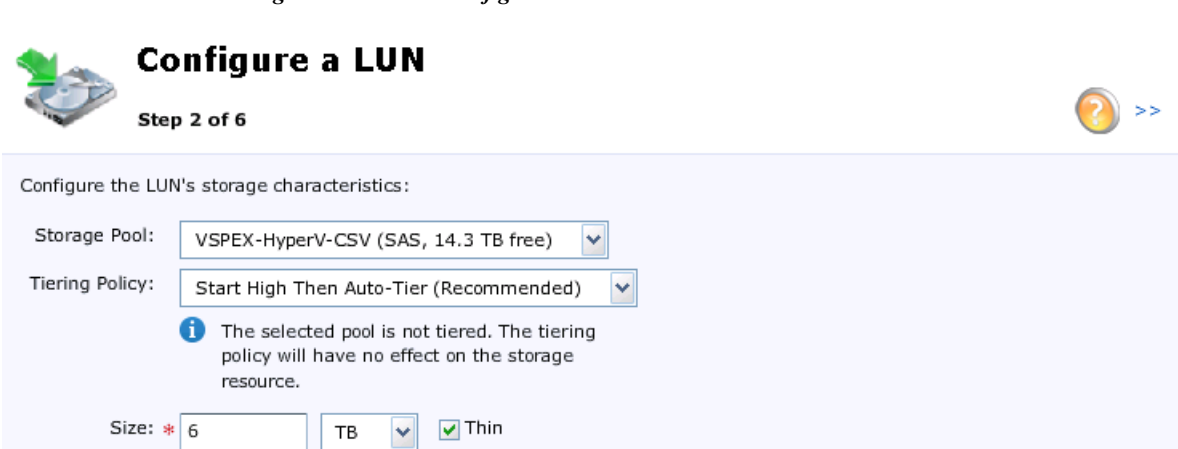
☒ Create a LUN

LUN Name: \* VSPEX-CSV-LUN-1

Description: CSV LUN-1 for VSPEX VMs location on Hyper-V Cluster

5. In the **Configure a LUN** window select the created “VSPEX-SAN-Boot” Storage Pool for the Hyper-V Boot LUN. Specify the LUN size and uncheck **Thin** check box and click **Next**.

Figure 141 Configure LUN



**Configure a LUN**

Step 2 of 6

Configure the LUN's storage characteristics:

Storage Pool: VSPEX-HyperV-CSV (SAS, 14.3 TB free)

Tiering Policy: Start High Then Auto-Tier (Recommended)

*The selected pool is not tiered. The tiering policy will have no effect on the storage resource.*

Size: \* 6 TB ☒ Thin

6. In the **Configure Snapshot Schedule** window select Do not configure a snapshot schedule and click **Next**.
7. In the **Configure Host Access** window of the LUN wizard, choose LUN for all the servers participating in the Hyper-V cluster from the drop-down list and click **Next**.

Figure 142 Configure Host Access

**LUN Wizard**

## Configure Host Access

**Step 4 of 6**

Configure which hosts will access this storage:

Filter for:  Protocols: FC or iSCSI

!	Name	Network Address	Operating System	Protocol	Access
✓	VSPEX-BO-Server-1	hyperv1	Microsoft Hyper-V	FC, File	LUN
✓	VSPEX-BO-Server-2	hyperv2	Microsoft Hyper-V	FC, File	LUN

8. In the **Summary** page confirm the LUN configuration and click **Finish** to complete the LUN creation and host access.

Figure 143 Summary of LUN Configuration

**Summary**

**Step 5 of 6**

Confirm the following LUN configuration:

Name: VSPEX-CSV-LUN-1

Description: CSV LUN-1 for VSPEX VMs location on Hyper-V Cluster

Storage Pool: VSPEX-HyperV-CSV

Size: 6.0 TB

Thin: Yes

Tiering Policy: Start High Then Auto-Tier (Recommended)

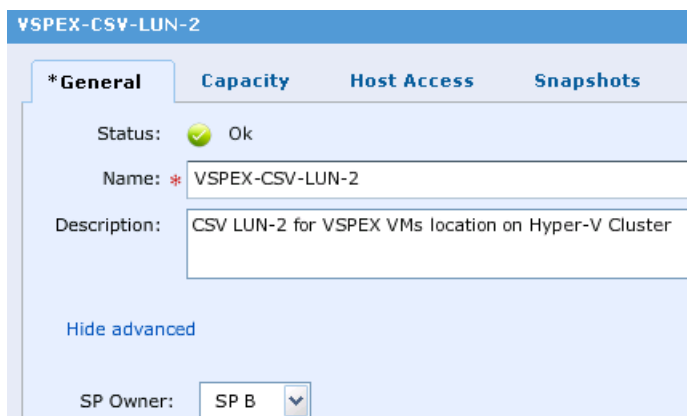
Protection Schedule: None configured

LUN Access: ▼ 2 hosts configured  
VSPEX-BO-Server-1  
VSPEX-BO-Server-2

Snapshot Access: No hosts configured

9. In the **Results** page click **Close**.
10. By default when a LUN is created in the VNXe the SP A is the owner, hence to change the ownership navigate to **Storage > LUNs** and select the LUN and click **Details**.
11. In the **General** tab click **Show advanced** and from the drop-down list next to SP Owner, select the storage processor.

Figure 144 Select Storage Processor



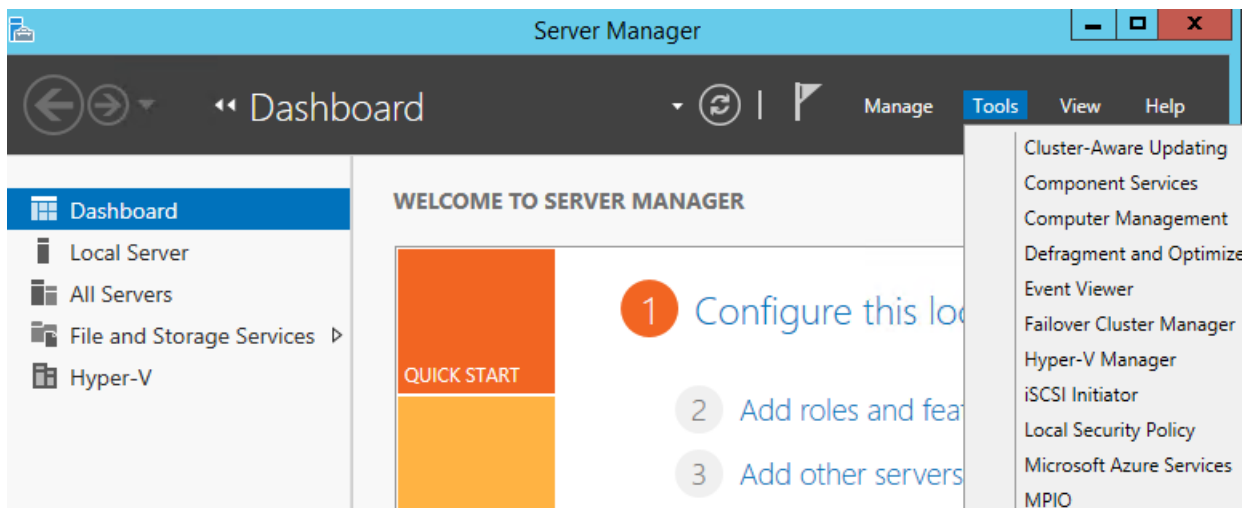
12. Repeat the above steps in this section to create the remaining shared LUNs.

## Configure MPIO in Hyper-V hosts

Follow these steps to configure the Microsoft MPIO:

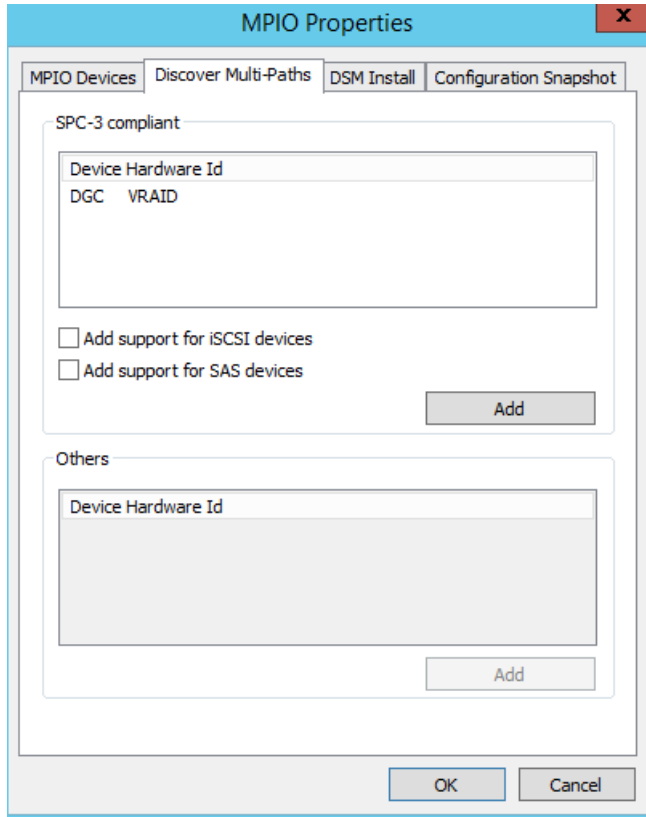
1. Connect and login to the Windows Hyper-V host. And open Server Manager.
2. Navigate to **Server Manager > Tools** and click **MPIO**

Figure 145 Server Manager: MPIO



3. Select **Discover Multi-Paths** tab in the **MPIO Properties** window.
4. Select “DGC VRAID” that the Microsoft MPIO has discovered and click **Add**.
5. Click **Yes** to reboot the host.

**Figure 146**      *Configuring MPIIO Properties*



6. After reboot, verify the MPIIO configuration information as shown in the below figure.

**Figure 147**      *Verify MPIIO Configuration*

```
PS C:\Users\administrator.VSPEXDOM> mpclaim -s -d
For more information about a particular disk, use 'mpclaim -s -d #' where # is the MPIIO disk number.
MPIIO Disk    System Disk  LB Policy    DSM Name
-----
MPIIO Disk3   Disk 4       RRWS         Microsoft DSM
MPIIO Disk2   Disk 3       RRWS         Microsoft DSM
MPIIO Disk1   Disk 2       RRWS         Microsoft DSM
MPIIO Disk0   Disk 1       RRWS         Microsoft DSM
PS C:\Users\administrator.VSPEXDOM> mpclaim -s -d 3
MPIIO Disk3: 02 Paths, Round Robin with Subset, Implicit and Explicit
Controlling DSM: Microsoft DSM
SN: 6006016022D0360022BD4554512B5903
Supported Load Balance Policies: F00 RRWS LQD WP LB

Path ID          State          SCSI Address  Weight
-----
0000000077020000 Active/Optimized 002|000|000|003 0
* TPG_State : Active/Optimized , TPG_Id: 2, : 19
0000000077010000 Active/Unoptimized 001|000|000|003 0
TPG_State : Active/Unoptimized, TPG_Id: 1, : 5
```

## Create Hyper-V Cluster

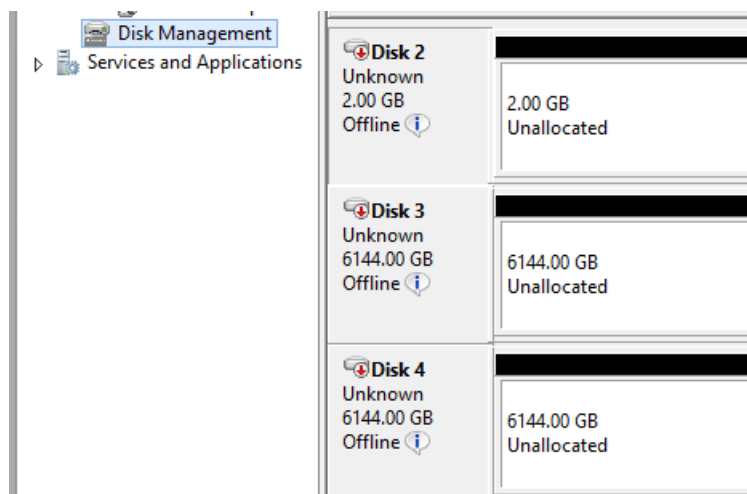
After building and configuring all Hyper-V servers, including SAN boot, MPIO, and joining the Active Directory domain, create the Windows Failover Cluster on which 100 highly available virtual machines will be deployed. This task is subdivided into the following segments:

- Prepare Shared Storage
- Run Cluster Validation
- Create Cluster
- Configure Cluster Disks
- Configure Cluster Networks
- Create HA Virtual Machines

### Prepare Shared Storage

Before you can test and form the cluster, it is necessary to format the shared LUNs as NTFS volumes. Perform the following steps on only one node of the cluster to format the drives. Navigate to **Server Manager > Tools > Computer Management > Disk Management** to see the shared storages presented to the host in the previous section.

*Figure 148 Disk Management*



1. Login to the Hyper-V server and from the **Server Manager** window, navigate to **File and Storage Services > Volumes > Disks**.



**Figure 149** Managing Disk space in Host

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only	Cluster...	Subsyst...	Bus Type	Name
HyperV2 (4)										
0		Online	100 GB	0.00 B	MBR				Fibre Cha...	DGC VRAID Multi-Path Disk Device
1		Offline	2.00 GB	2.00 GB	Unknown	✓			Fibre Cha...	DGC VRAID Multi-Path Disk Device
2		Offline	6.00 TB	6.00 TB	Unknown	✓			Fibre Cha...	DGC VRAID Multi-Path Disk Device
3		Offline	6.00 TB	6.00 TB	Unknown	✓			Fibre Cha...	DGC VRAID Multi-Path Disk Device

2. Right-click each disk that is listed as Offline and choose **Bring Online**.
3. Click **Yes** to acknowledge the warning and bring the disk online.

**Figure 150** Bringing Disk Online

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only
HyperV2 (4)						
0		Online	100 GB	0.00 B	MBR	
1		Offline	2.00 GB	2.00 GB	Unknown	✓
2		Offline	6.00 TB	6.00 TB		
3		Offline	6.00 TB	6.00 TB		

4. Right-click the first Unknown disk and choose **Initialize**

**Figure 151** Initializing Unknown Disk

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only
HyperV2 (4)						
0		Online	100 GB	0.00 B	MBR	
1		Offline	2.00 GB	2.00 GB		
2		Offline	6.00 TB	6.00 TB		
3		Offline	6.00 TB	6.00 TB		

5. Click **Yes** to acknowledge the warning and start the initialization.
6. Repeat for all the disks labeled Unknown. When complete, all disks should show a Partition of GPT.
7. Right-click the first disk and select **New Volume**.

Figure 152 Selecting New Volume

Number	Virtual Disk	Status	Capacity	Unallocated	Partition	Read Only
HyperV2 (4)						
0		Online	100 GB	0.00 B	MBR	
1		Online	2.00 GB	1.97 GB	GPT	
2		Online	6.00 TB	6.00 TB	GPT	
3		Online	6.00 TB	6.00 TB	GPT	

8. Click Next on the **New Volume Wizard splash** screen.
9. On the Select the server and disk page, select a disk and click **Next** to continue.

Figure 153 New Volume: Server and Disk

**New Volume Wizard**

Select the server and disk

Before You Begin

**Server and Disk**

Size

Drive Letter or Folder

File System Settings

Confirmation

Results

Server:

Provision to	Status	Cluster Role	Destination
HyperV2	Online	Not Clustered	Local

Refresh Rescan

Disk:

Disk	Virtual Disk	Capacity	Free Space	Subsystem
Disk 1		2.00 GB	1.97 GB	
Disk 2		6.00 TB	6.00 TB	
Disk 3		6.00 TB	6.00 TB	

< Previous Next > Create Cancel

10. On the Specify the size of the volume, accept the default (maximum) and click **Next** to continue.

Figure 154 New Volume: Size

**New Volume Wizard**

### Specify the size of the volume

Before You Begin | Server and Disk | **Size** | Drive Letter or Folder

Available Capacity: 1.97 GB

Minimum size: 8.00 MB

Volume size:  GB

11. On the **Assign to a drive letter** or folder page, select Don't assign to a drive letter or folder radio button. Click **Next** to continue

Figure 155 New Volume: Drive Letter or Folder

**New Volume Wizard**

### Assign to a drive letter or folder

Before You Begin | Server and Disk | Size | **Drive Letter or Folder** | File System Settings | Confirmation | Results

Select whether to assign the volume to a drive folder, the volume appears as a folder within

Assign to:

☐ Drive letter:

☐ The following folder:

☒ Don't assign to a drive letter or folder.

12. On the **Select file system settings** page, leave File system as NTFS. Leave the Allocation unit size to Default. Enter a Volume label and click **Next** to continue.

Figure 156 New Volume: File System Settings

**New Volume Wizard**

### Select file system settings

Before You Begin | Server and Disk | Size | Drive Letter or Folder | **File System Settings** | Confirmation | Results

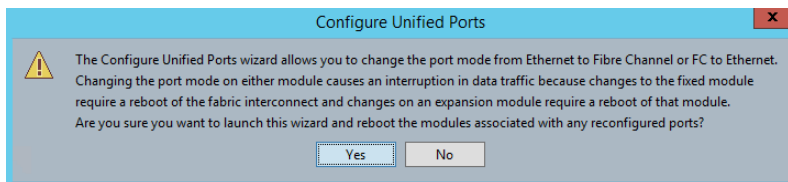
File system:

Allocation unit size:

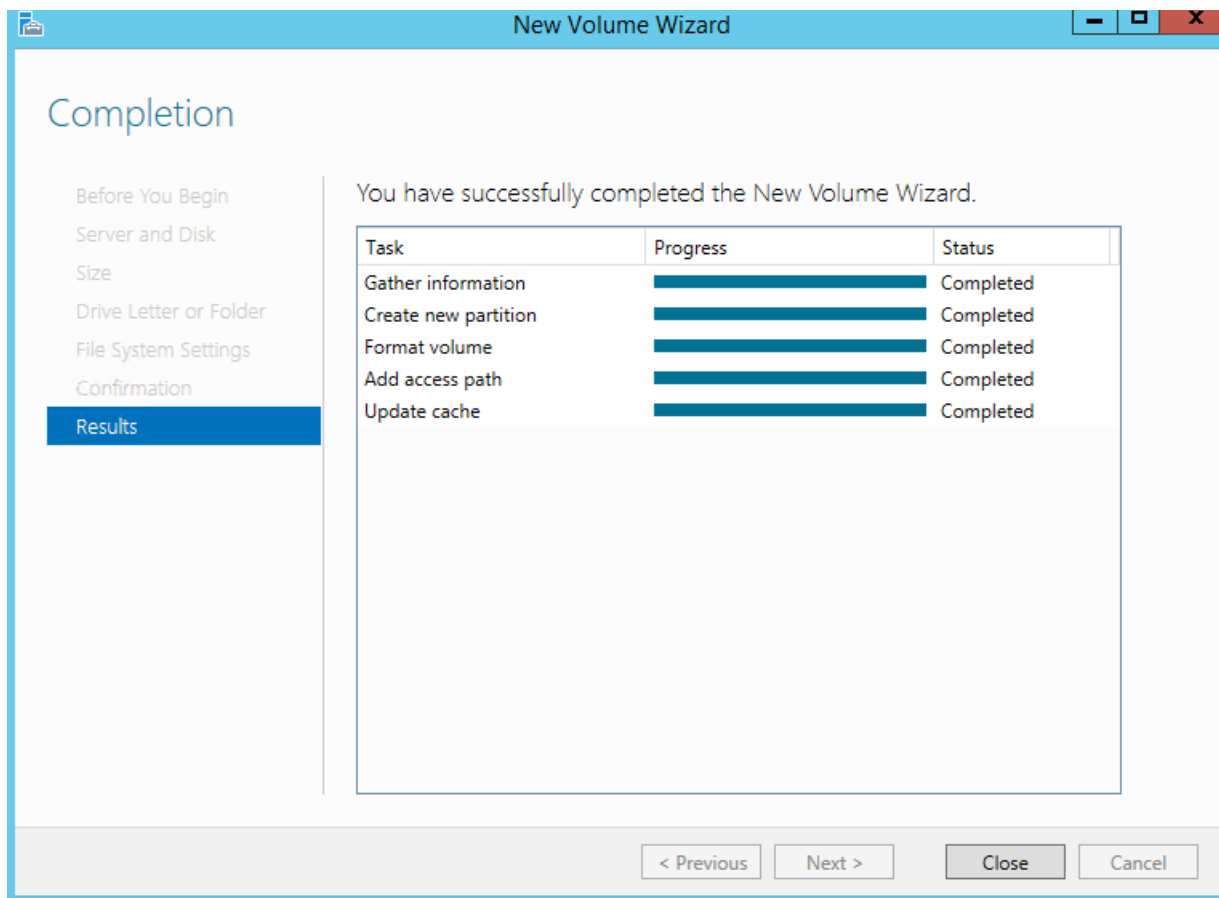
Volume label:

☐ Generate short file names (not recommended)

13. On the **Confirm selections** page, review the settings and click **Create** to create the volume.

**Figure 157** *New Volume: Confirmation Page*

14. On the **Completion** page, click **Close** when the creation is complete.
15. Repeat the volume creation steps for all disks.

**Figure 158** *New Volume: Results*

16. When volumes have been created on all the disks, right-click each data disks and select Take Offline. When the disks have been initialized and formatted, it is a good practice to go through each server that will be part of the cluster to make sure the disks can be brought online on each node.

## Run Cluster Validation

Run the Cluster Validation Wizard by issuing the following PowerShell cmdlet:

```
Test-Cluster hyperv1, hyperv2
```

**Figure 159**      *Run Cluster Validation*

```
PS C:\Users\administrator.VSPEXDOM> Test-Cluster hyperv1, hyperv2

Test-Cluster
Arbitrating for Test Disk 0 from node HyperV2.VSPEXDOM.LOCAL.
[ooooooooooooooooooooo]
```

Check the validation report for any errors or warning and fix it.

**Figure 160**      *Check Validation Report*

```
PS C:\Users\administrator.VSPEXDOM> Test-Cluster hyperv1, hyperv2

Mode                LastWriteTime         Length Name
----                -
-a---          11/1/2014   1:50 PM          511166 Validation Report 2014.11.01 At 13.46.05.xml.mht

PS C:\Users\administrator.VSPEXDOM>
```

C:\Windows\Cluster\Reports\Validation Report 2014.11.01 At 13.46.05.xml. Failover Cluster Validation ...

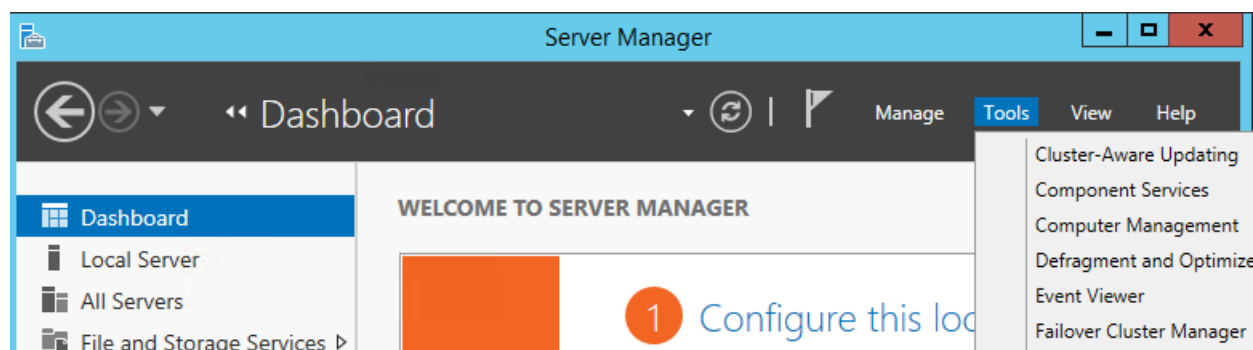
Testing has completed successfully and the configuration is suitable for clustering.

If the report output says testing completed successfully and the configuration is suitable for clustering then proceed with the creation of cluster.

## Create Cluster

1. Login to the Hyper-V server and navigate to **Server Manager > Tools** and click **Failover Cluster Manager**.

**Figure 161**      *Failover Cluster Manager*



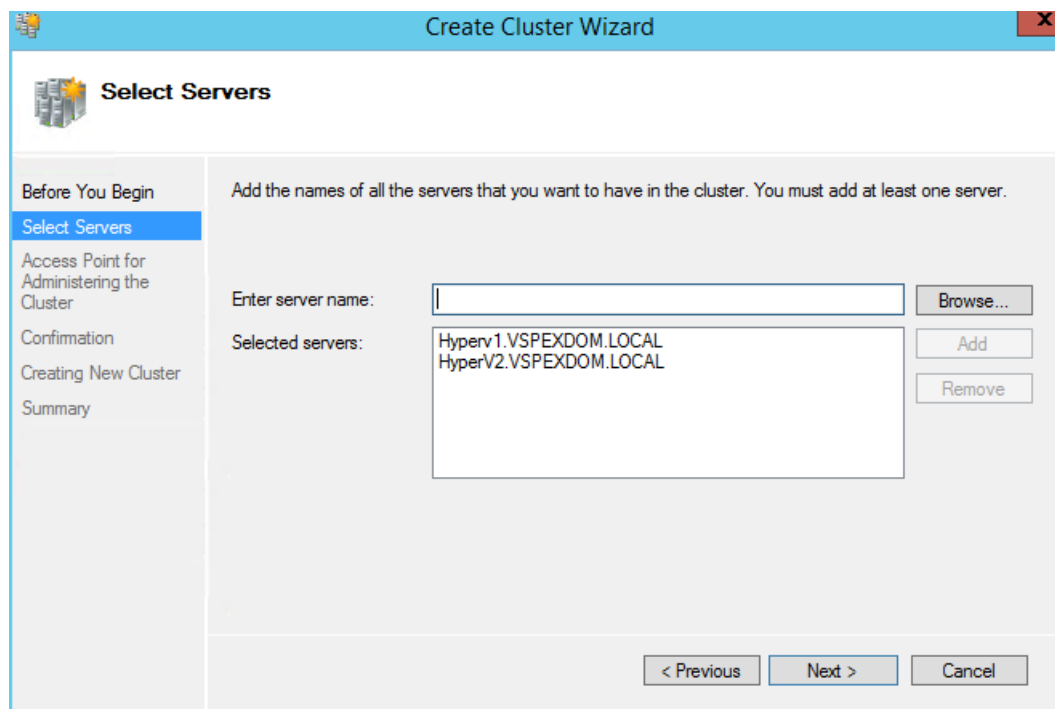
2. In the **Management** section of the **Failover Cluster Manager**, select **Create Cluster**
3. This launches the **Create Cluster** wizard. On the **Before You Begin** window, click **Next** to continue.

**Figure 162**      *Create Failover Cluster Manager*



4. On the **Select Servers** page, enter either the FQDN or NetBIOS names of the servers to form the cluster. Click **Next** to continue.

**Figure 163**      *Create Cluster: Select Servers*



5. On the **Access Point for Administering the Cluster** page, enter a name in the **Cluster Name** field and an **IP address** under the Address field. The cluster name and IP address will be registered in DNS and the cluster name will be registered in Active Directory

**Figure 164**      *Create Cluster: Access Point for Administering the Cluster*

The screenshot shows the 'Create Cluster Wizard' window with the 'Access Point for Administering the Cluster' step selected in the left sidebar. The main area contains a text box for 'Cluster Name' with the value 'VSPEXCLUS'. Below it, a message states: 'The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.' A table below this message shows a selected network and its IP address.

	Networks	Address
<input checked="" type="checkbox"/>	10.29.180.0/24	10 . 29 . 180 . 171

At the bottom, there are buttons for '< Previous', 'Next >', and 'Cancel'.

- Review your settings on the **Confirmation** page and click **Next** to create the cluster.

**Figure 165**      *Create Cluster: Confirmation*

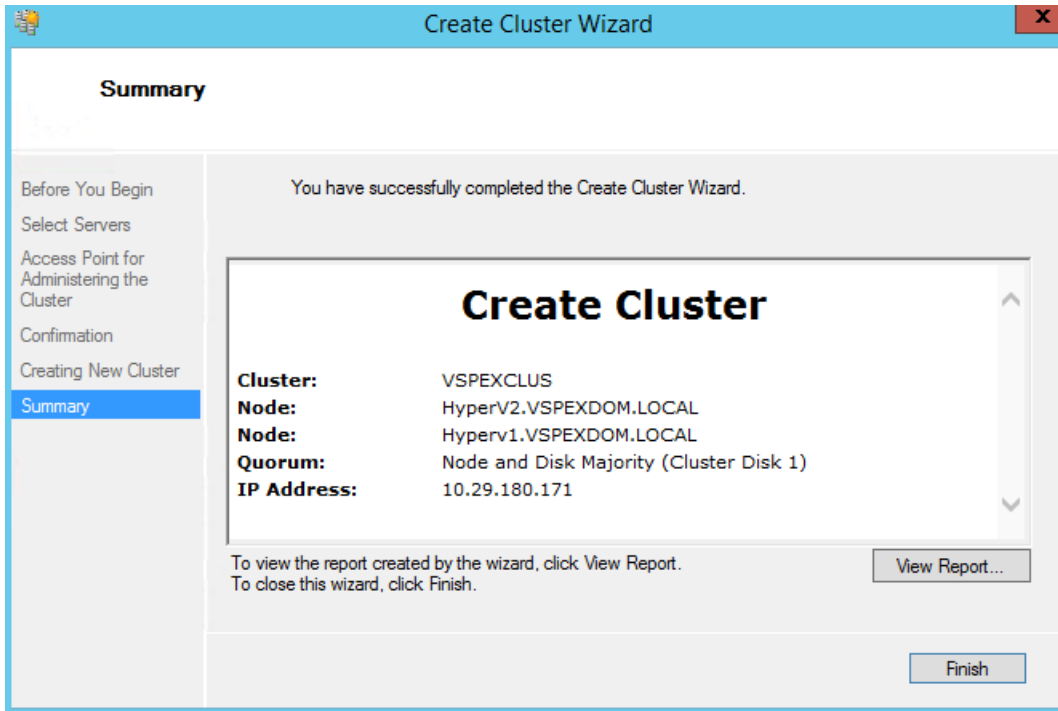
The screenshot shows the 'Create Cluster Wizard' window with the 'Confirmation' step selected in the left sidebar. The main area displays the following settings:

- Cluster:** VSPEXCLUS
- Node:** Hyperv2.VSPEXDOM.LOCAL
- Node:** Hyperv1.VSPEXDOM.LOCAL
- IP Address:** 10.29.180.171

Below the settings, there is a checkbox labeled 'Add all eligible storage to the cluster.' which is checked. A message below the checkbox says: 'To continue, click Next.' At the bottom, there are buttons for '< Previous', 'Next >', and 'Cancel'.

- Click **Finish** on the **Summary** window

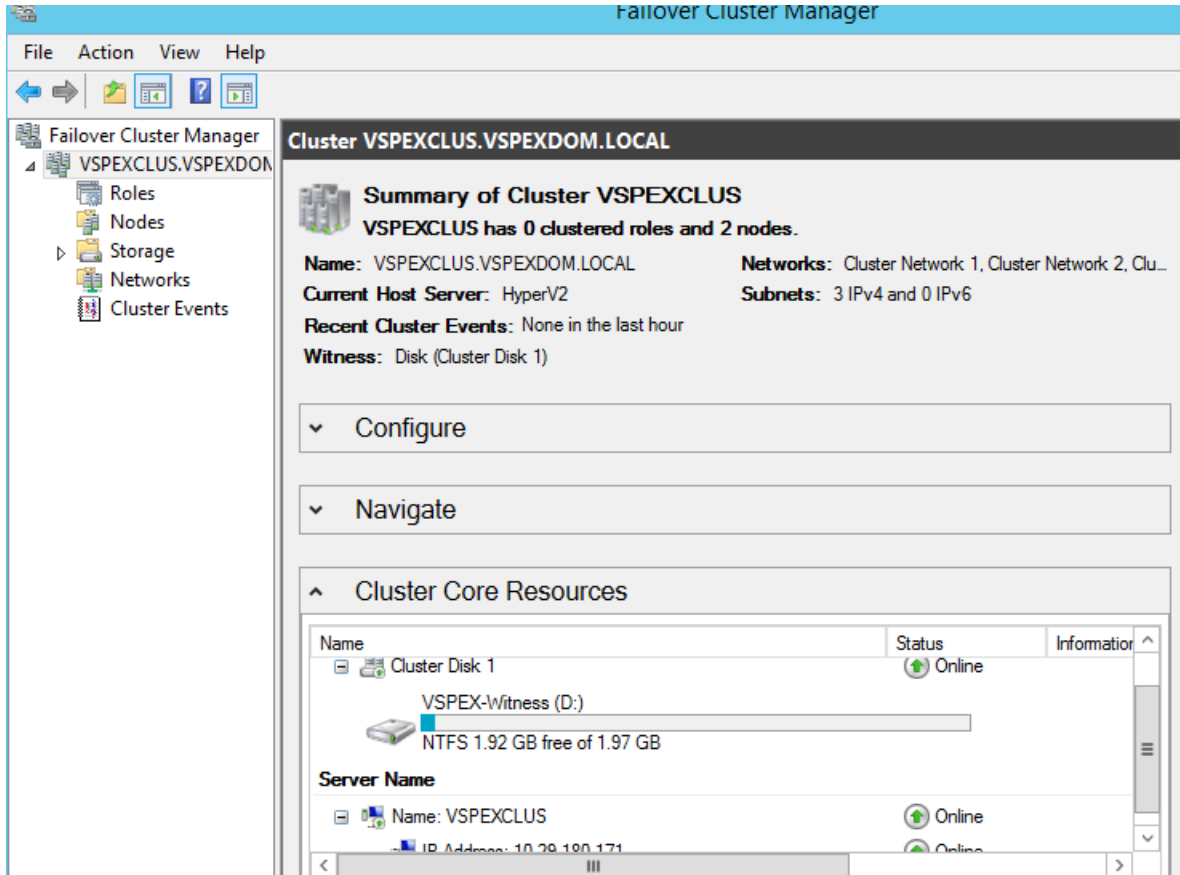
**Figure 166**      *Create Cluster: Summary*



The below figure shows **Failover Cluster Manager** window after the successful creation of cluster.



Figure 167 Failover Cluster Manager



## Configure Cluster Disks

The disks are added into the cluster as Available Storage, meaning they have not been assigned to any specific role or resource group within the cluster. Additionally, the disks have generic names of Disk 1, Disk 2, etc. Using the Failover Cluster Manager console, the disk names can be changed to something meaningful and the data disks can be assigned as Cluster Shared Volumes for use by the virtual machines

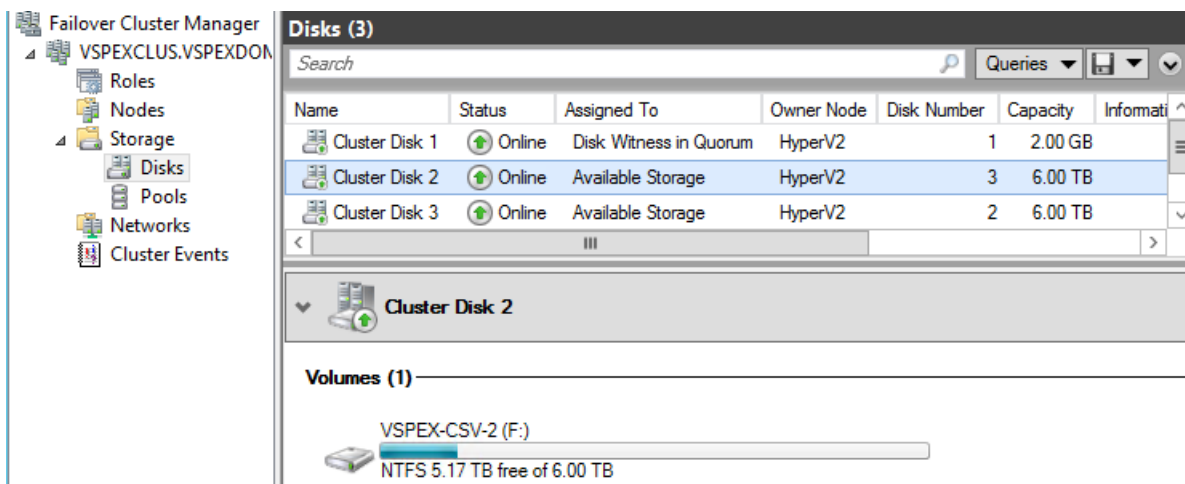
1. From the Failover Cluster Manager console, expand the cluster, expand the **Storage**, and click **Disks**.



**Note**

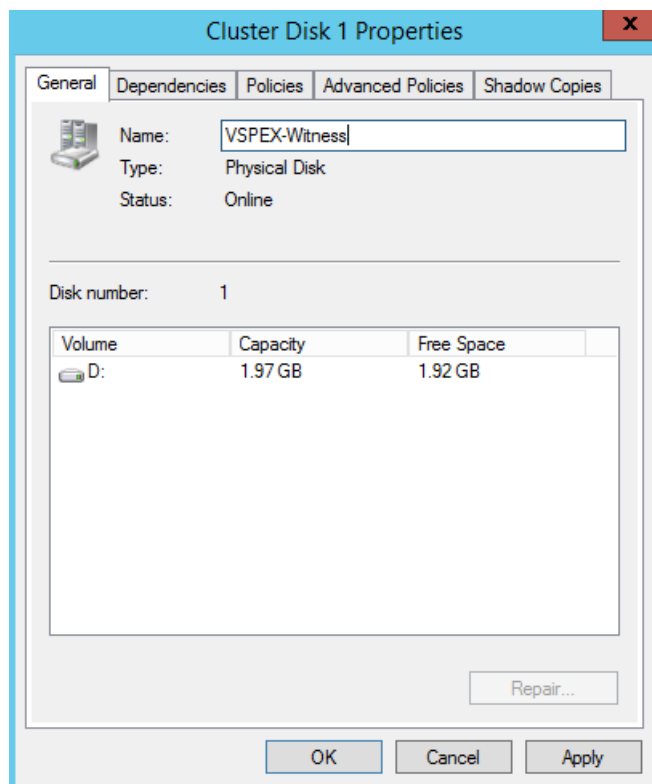
The cluster will automatically add the smallest NTFS formatted disk as the witness disk.

**Figure 168** *Failover Cluster Manager: Disks*



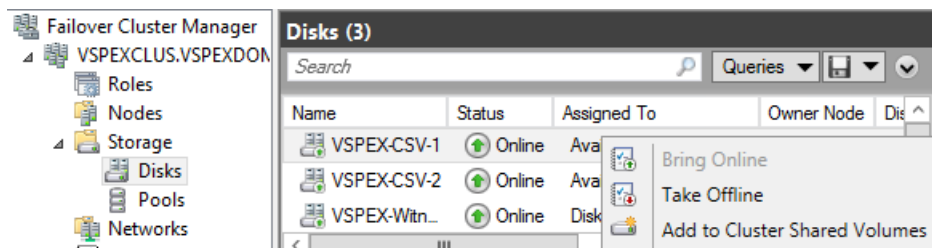
2. Right-click the disk and select Properties. Change the name to reflect the name you assigned when you formatted the disk. Click **OK** to continue.
3. Repeat on all other disks to rename them.

**Figure 169** *Rename Disk Properties for All Disks*



4. Right-click the first **Available Storage** volume and select **Add to Cluster Shared Volumes**.
5. Repeat for the other Available Storage volumes.

**Figure 170** Add Available Storage to Cluster Shared Volumes



## Configure Cluster Networks

Multiple networks have been defined for specific usage within the cluster – Mgmt, CSV, and Live Migration. The cluster has different capabilities that can be assigned to each network, and during the creation of the cluster, the cluster attempts to assign the appropriate capabilities. But those do not always match. We need to make sure the capabilities are properly assigned.

The cluster build process assigns default names to the NICs. For documentation and debugging purposes it is recommended to assign meaningful names to the NICs.

All networks are available for Live Migration in a default configuration, and we want to make sure the network we defined for Live Migration is the only one configured.

The Cluster Shared Volume network has a special requirement. By default, the cluster could assign CSV traffic to the wrong NIC, so we need to make sure the cluster uses the NIC we defined for CSV.

Though the first three changes can be handled through the Failover Cluster Manager console, setting the CSV network is done through PowerShell. The following sample script shows how to take care of all the above steps using a few PowerShell cmdlets.

```
# Rename cluster NICs based upon IP address
(Get-ClusterNetwork -Cluster VSPEXclus | ? {$_.Address -like "10.29.180.*"}).Name = "Mgmt"
(Get-ClusterNetwork -Cluster VSPEXclus | ? {$_.Address -like "192.168.30.*"}).Name =
"LiveMigration"
(Get-ClusterNetwork -Cluster VSPEXclus | ? {$_.Address -like "192.168.40.*"}).Name = "CSV"

# Set cluster network roles based on cluster NIC names set in previous step
(Get-ClusterNetwork -Cluster VSPEXclus -Name "Mgmt").Role = 3
(Get-ClusterNetwork -Cluster VSPEXclus -Name "LiveMigration").Role = 0
(Get-ClusterNetwork -Cluster VSPEXclus -Name "CSV").Role = 1

# Set the Live Migration network by excluding all other networks
Get-ClusterResourceType -Name "Virtual Machine" | Set-ClusterParameter -Name
MigrationExcludeNetworks -Value ([String]::Join(";", (Get-ClusterNetwork | Where-Object
{$_.Name -ne "LiveMigration"}).ID))

# Set cluster metric on CSV network to Make sure it is used exclusively for CSV traffic
(Get-ClusterNetwork -Cluster VSPEXclus -Name "CSV").Metric = 900
```

## Cisco UCS Mini Branch Office Management with UCS Central

Cisco UCS Central Software extends the simplicity and agility of managing a single Cisco UCS domain to multiple Cisco UCS domains that can extend across globally distributed data centers. UCS Central provides a single point of management for thousands of UCS servers and provides centralized inventory,

fault management, global ID pooling and centralized policy based firmware upgrades. UCS central therefore is ideal for managing a VSPEX based branch office solution, where it can provide the management console to drive consistency and compliance across all of the UCS domains.

UCS Central is supplied as a virtual appliance that runs on VMware and Microsoft hypervisors and is pre-packaged as a VMware ova or an ISO image for ease of installation. Redundancy can be provided with an active standby configuration (not supported across WAN links) and to ensure separation of the management plane it should be installed on separate servers that are not part of UCS Domain.

Profiles and policies defined in Cisco UCS Central (UCSC) can co-exist with the local Cisco UCS Manager defined information. Both Cisco UCS Manager and Cisco UCS Central manage the information defined in the respective tool and show the information defined in other as read-only.

For the Cisco Remote Office Branch office solutions, some of the key advantages of the Cisco UCS Central are:

- All the UCS resources, errors and warnings from two or more domains are presented in a single common interface
- Various Pools, Service Profiles and Settings are configured once, centrally
- Service Profiles can be managed and deployed from a single management pane
- Branch office setup can be managed from a series of templates ensuring that each branch has a consistent setup

In this design UCS Central will be deployed as a standalone solution.

## Install and Configure UCS Central

As mentioned above you can install Cisco UCS Central using either one of the following:

- OVA file
- ISO Image

In this architecture, we have deployed UCS Central using the ISO image on the Hyper-V server configured in a standalone mode. You can download the ISO image from the below URL:

<http://www.cisco.com/cisco/web/support/index.html>

Following are the major steps to deploy Cisco UCS central in the remote Primary data center.

1. Install **UCS Central**
2. Logging into **Cisco UCS Central GUI**
3. Adding Cisco UCS Managers to Cisco UCS Central

## Installing UCS Central

As mentioned before, the UCS Central installation media is available as an ISO image. The UCS central must be deployed on the infrastructure network of the remote datacenter, and not on any of the Hyper-V servers in the VSPEX Branch Office.

The step-by-step procedure for installing Cisco UCS Central ISO File in Microsoft Hyper-V is given below:

1. Create a VM with the following settings:

**Table 16**      *VM Recommendations*

Setting	Recommended Value
Name	A descriptive name that includes information about the Cisco UCS Central deployment
RAM	No less than 12GB
Network adapter	Default
Number of vCPU	4
Virtual disk	No less than 40GB. To be mapped using a new SCSI controller.  You also need to create a second 40GB virtual disk under IDE Controller in Step 3.
Setting Physical hard disk (Optional for standalone mode)	No less than 40GB. To be mapped using a new SCSI controller.

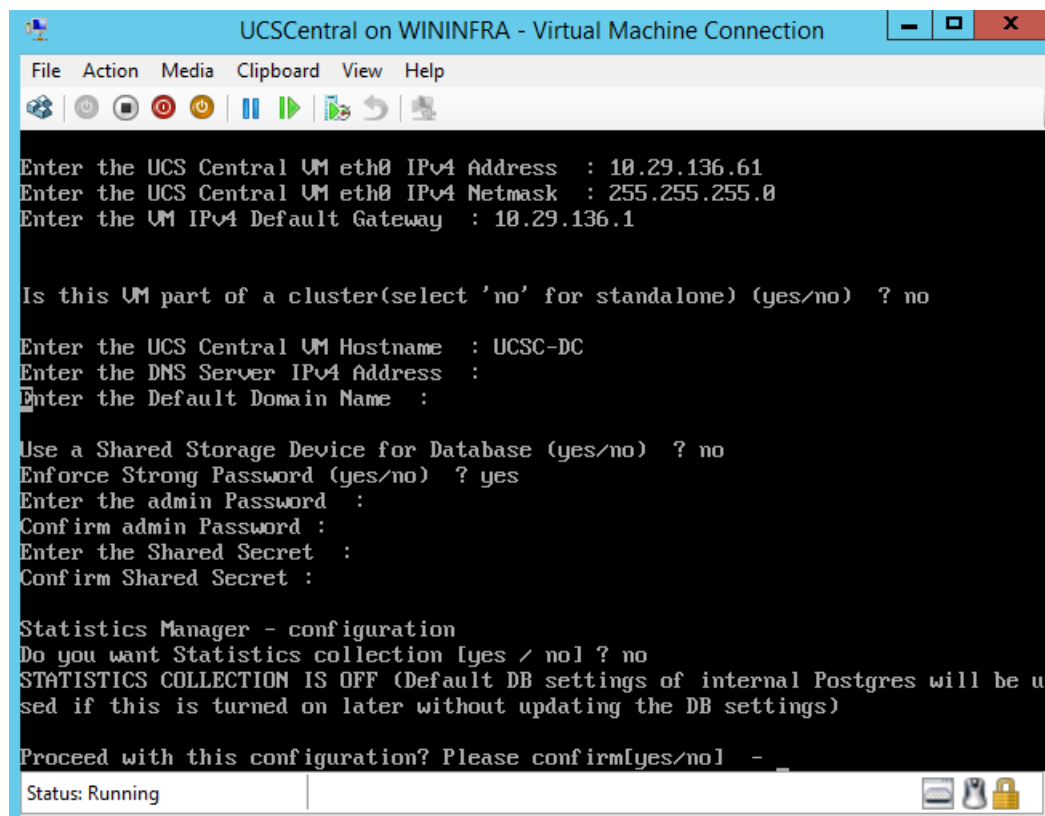
2. In the settings for the VM, do the following:
  - a. Delete the default network adapter.
  - b. Create a new legacy network adapter.
  - c. Apply.
3. Under the same IDE controller as the first virtual drive, create a second virtual drive for the VM with no less than 40GB of available disk space.
4. In the VM settings > Management > Integration Services, uncheck Time synchronization to disable it.
5. Mount the Cisco UCS Central ISO image to the CD/DVD drive.
6. Start the VM and connect to the console.
7. From the Cisco UCS Central Installation menu on the ISO image, choose Install Cisco UCS Central.
8. The Cisco UCS Central installer checks that the VM has the required RAM and disk space (two disks, both with 40GBs). If the VM meets the requirements, the installer formats the disks, transfers the files, and installs Cisco UCS Central.
9. When the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the **VM console** window:
  - a. Setup new configuration or restore full-state configuration from backup [setup/restore] prompt, enter setup and press Enter.
  - b. At the Enter the UCS Central VM eth0 IPv4 Address : prompt, enter the IP address assigned to Cisco UCS Central and press **Enter**.
10. You must enter a static IP address that is reserved for this Cisco UCS Central VM. Cisco UCS Central does not support Dynamic Host Configuration Protocol (DHCP).
  - a. At the Enter the UCS Central VM eth0 IPv4 Netmask—prompt, enter the netmask assigned to Cisco UCS Central and press **Enter**.
  - b. At the Enter the Default Gateway—prompt, enter the default gateway used by Cisco UCS Central and press **Enter**.

- c. At the Is this VM part of a cluster (select 'no' for standalone) (yes/no) prompt, select no and press **Enter**.
- d. Selecting yes will setup Cisco UCS Central in cluster mode. For more information about setting up Cisco UCS Central in cluster mode, see *Installing Cisco UCS Central in Cluster Mode*.
- e. At the Enter the UCS Central VM host name—prompt, enter the host name you want to use for the Cisco UCS Central VM and press **Enter**.
- f. At the Enter the DNS Server IPv4 Address (optional)—prompt, enter the IP address for the DNS server you want to use for Cisco UCS Central and press **Enter**.
- g. If you do not plan to use a DNS server for Cisco UCS Central, leave this blank and press Enter.
- h. At the Use Shared Storage Device for Database (yes/no) prompt, if you want to setup shared storage, enter yes, if not enter no and press **Enter**. See *Setting up a Shared Storage on Microsoft Hyper-V*.
- i. Optional—At the Enter the Default Domain Name—prompt, enter the domain in which you want to include Cisco UCS Central and press **Enter**.
- j. If you do not plan to include Cisco UCS Central in a domain, leave this blank and press Enter. Cisco UCS Central will use the default domain named local domain.
- k. At the Enforce Strong Password (Yes/No) prompt, if you want to set up strong password alert, select yes and press **Enter**.
- l. At the Enter the admin Password—prompt, enter the password you want to use for the admin account and press **Enter**.
- m. At the Confirm admin Password—prompt, re-enter the password you want to use for the admin account and press **Enter**.
- n. At the Enter the Shared Secret—prompt, enter the shared secret (or password) that you want to use to register one or more Cisco UCS domains with Cisco UCS Central and press **Enter**.
- o. At the Confirm Shared Secret—prompt, re-enter the shared secret and press **Enter**.
- p. At the Do you want Statistics Collection (yes/no) prompt, if you want to enable statistics collection, enter yes and press **Enter**.

If you do not want to enable statistics collection now, you can enter no and proceed with the installation. You can enable the statistics collection using Cisco UCS Central CLI at any time. If you have entered yes, you will be prompted to provide the database server information. See *Database Server Information*

- At the Proceed with this configuration. Please confirm [yes/no] prompt, enter yes and press Enter. If you think you made an error when completing any of these steps, enter no and press Enter. You will then be prompted to answer the questions again.

Figure 171 Cisco UCS Central CLI



11. Unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.
12. Reboot the Cisco UCS Central VM.

## Logging into Cisco UCS Central GUI

To access Cisco UCS Central GUI, follow the below steps:

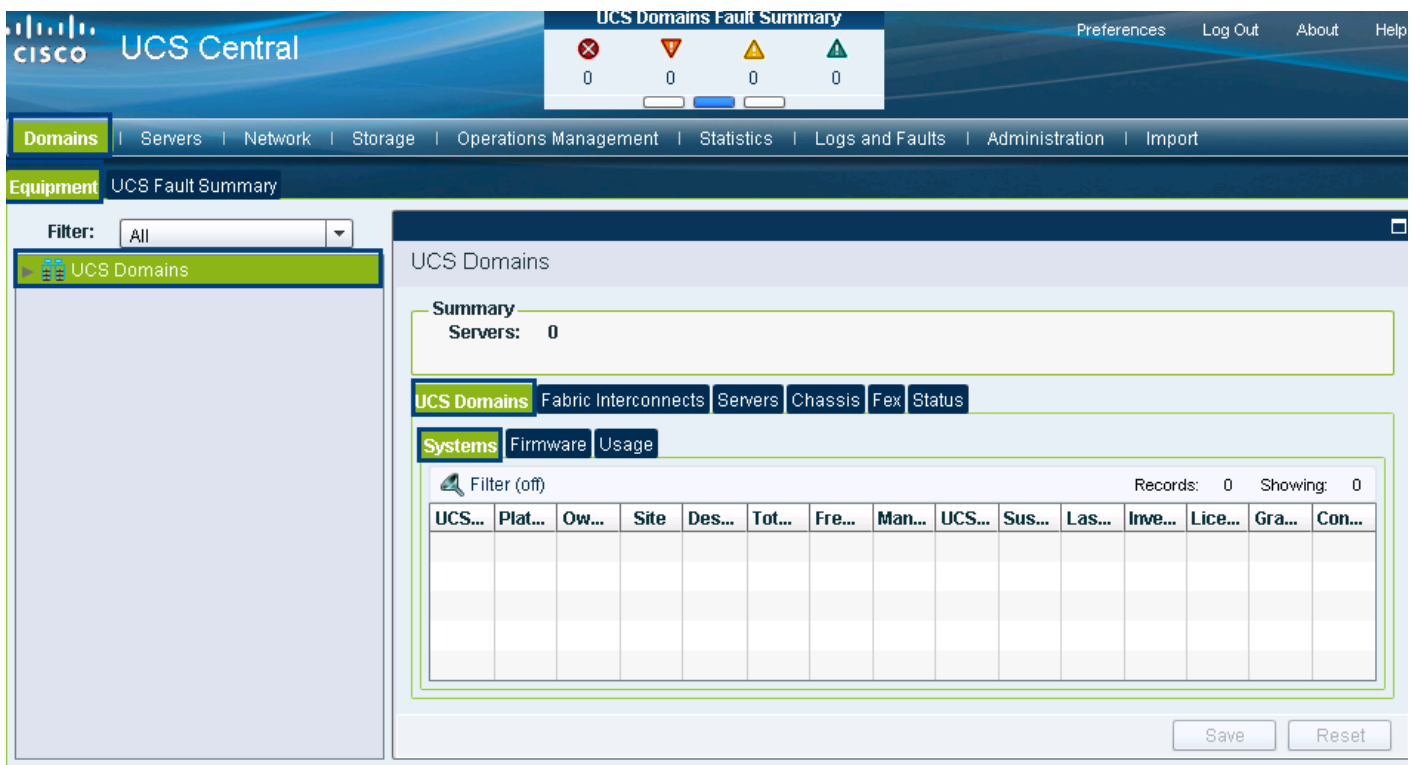
1. In your web browser, type the IP address assigned to the Cisco UCS Central during the installation.  
[http://UCSCentral\\_IP](http://UCSCentral_IP)
2. On the launch page, Enter your user name and password and click **Log In**.

**Figure 172** *Cisco UCS Central Login Page*



The login page features the Cisco logo and 'UCS Central Version 1.2(1a)' on the left. On the right, there are input fields for 'Username:', 'Password:', and 'Domain:' (set to '(Native)'). Below these are 'Log In' and 'Launch KVM' buttons. At the bottom, there is a copyright notice for 2014 Cisco Systems, Inc.

**Figure 173** *Cisco UCS Central: UCS Domains*



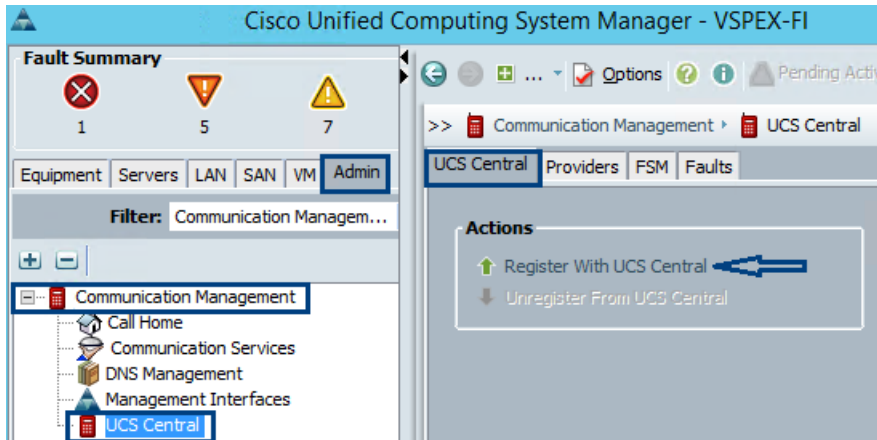
The interface shows the 'UCS Domains' section. At the top, there's a 'UCS Domains Fault Summary' bar with four icons (red X, orange triangle, yellow triangle, green triangle) and a count of 0 for each. Below this is a navigation bar with 'Domains' selected. The main content area has a 'Filter: All' dropdown and a 'UCS Domains' link. The 'Summary' section shows 'Servers: 0'. Below this are tabs for 'UCS Domains', 'Fabric Interconnects', 'Servers', 'Chassis', 'Flex', and 'Status'. The 'Systems' tab is active, showing a table with columns: UCS..., Plat..., Ow..., Site, Des..., Tot..., Fre..., Man..., UCS..., Sus..., Las..., Inve..., Lice..., Gra..., and Con... The table is currently empty. At the bottom right, there are 'Save' and 'Reset' buttons.

## Adding Cisco UCS Managers to UCS central

1. Launch **UCS Manager** GUI using the UCS mini Virtual IP.



**Figure 174**      *Register with UCS Central*



2. Enter the IP address and the Shared Secret password of the UCS Central and click **OK**.

**Figure 175** *Register with UCS Central Window*

**Register With UCS Central**

Hostname/IP Address: **10.29.136.61**

Shared Secret: **.....**

**Policy Resolution Control**

**All Global**

Infrastructure & Catalog Firmware:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Time Zone Management:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the time zone and NTP server settings are defined locally or comes from Cisco UCS Central.
Communication Services:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Global Fault Policy:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
DNS Management:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the SEL Policy is defined locally or in Cisco UCS Central.
Power Allocation Policy:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the Global Power Allocation Policy is defined locally or in Cisco UCS Central.
Power Policy:	<input type="radio"/> Local <input checked="" type="radio"/> Global	Determines whether the Power Policy is defined locally or in Cisco UCS Central.

OK Cancel

- Click **Accept** on the pop-window to continue registration with the UCS Central.

**Figure 176** *Confirm Registration for UCS Central*

**UCS Manager - Register With UCS Central**

Registering this domain with UCS Central will terminate all open GUI sessions.

**Do you want to continue registration with UCS Central?**

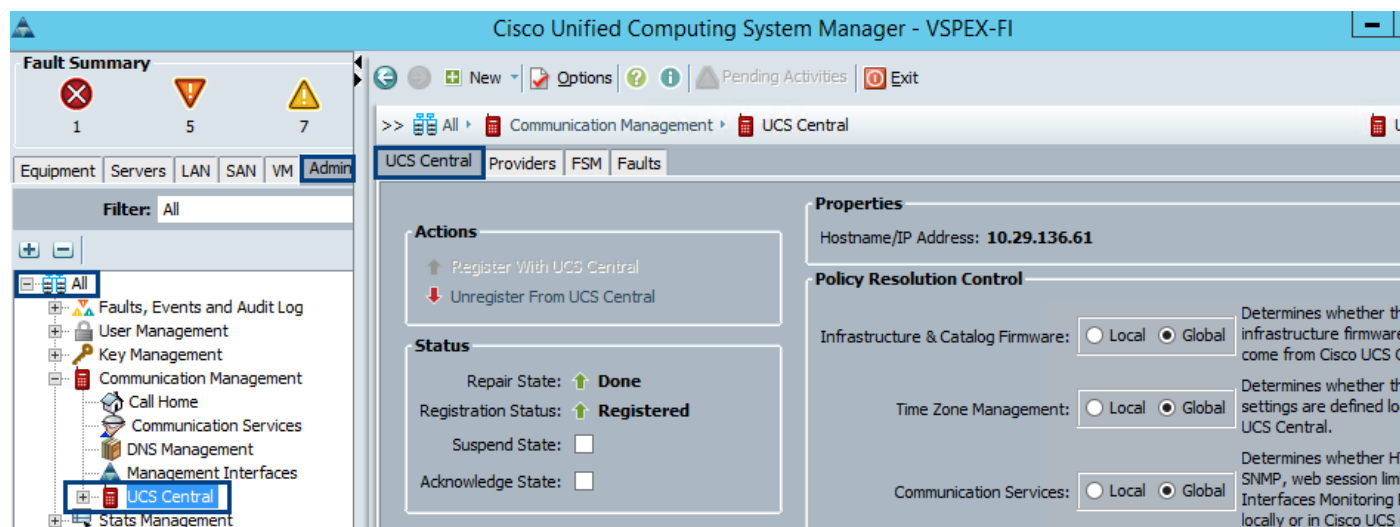
Accept Reject

- Click **OK** on the registration of UCS Central successfully initiated pop-window.

**Note**

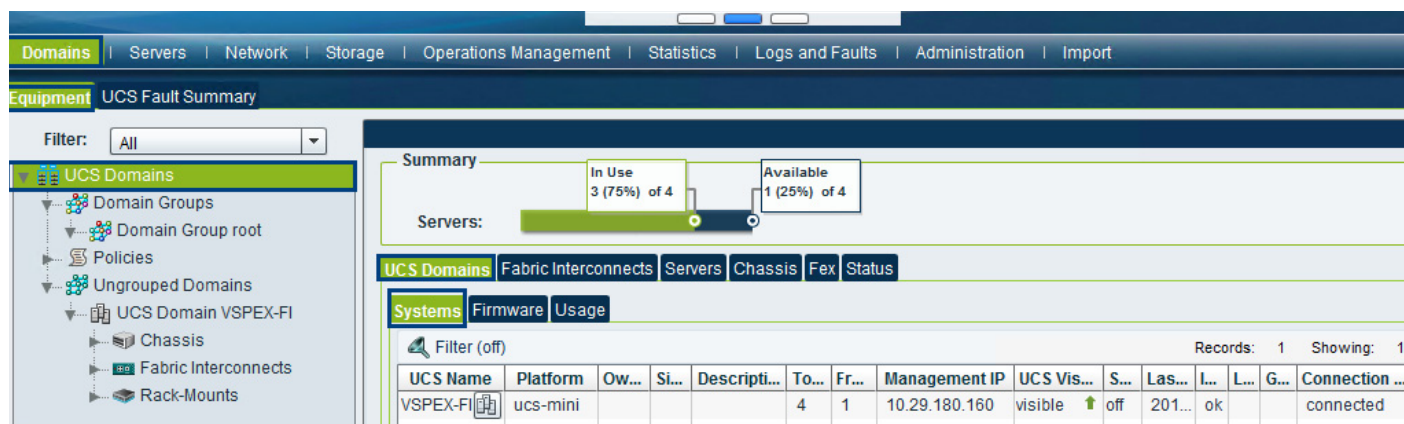
Make sure that the UCS central and UCS manager date & time is in sync. If not in sync, the UCS central registration will not be successful. (It is recommended to use NTP server for time sync).

**Figure 177** *Verify UCS Central Registration*



- Launch the UCS Central GUI to verify the newly registered UCS domain as shown in the below figure

**Figure 178** *UCS Domain in UCS Central GUI*



## Configure UCS Central for Branch Office Deployment

Following are the major steps to configure UCS Mini from UCS Central.

- Configure UCS Central Domain group
- Configure Pools and Policies
- Configure Global Service Profile template

#### 4. Configure Global Service Profile instance

### Configure UCS Central Domain Group

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains. You will have the following categories of domain groups in Cisco UCS Central:

**Domain Group**— A group that contains multiple Cisco UCS domains. You can group similar Cisco UCS domains under one domain group for simpler management.

**Ungrouped Domains**—When a new Cisco UCS domain is registered in Cisco UCS Central, it is added to the ungrouped domains. You can assign the ungrouped domain to any domain group.

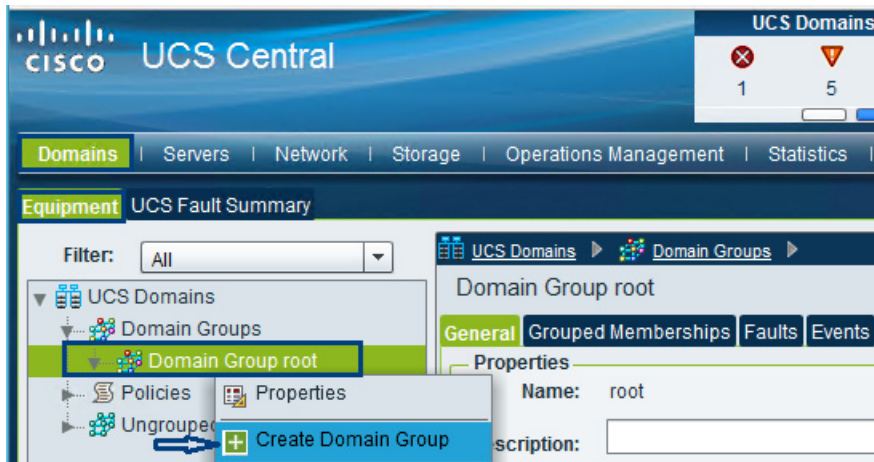
If you have created a domain group policy, a new registered Cisco UCS domain meets the qualifiers defined in the policy; it will automatically be placed under the domain group specified in the policy. If not, it will be placed in the ungrouped domains category. You can assign this ungrouped domain to a domain group.

Each Cisco UCS domain can only be assigned to one domain group. You can assign or reassign membership of the Cisco UCS domains at any time. When you assign a Cisco UCS domain to a domain group, the Cisco UCS domain will automatically inherit all management policies specified for the domain group.

Below we have shown the UCS central Domain group creation.

1. Launch **UCS Central** web GUI, then click **Domains > Domain Groups > Domain Group root** and the click **Create Domain Group**

*Figure 179 Create Domain Group*



2. Provide a Domain group name and description and Click **OK**.

**Figure 180** *Create Domain Group Window*

**Create**

## Create Domain Group

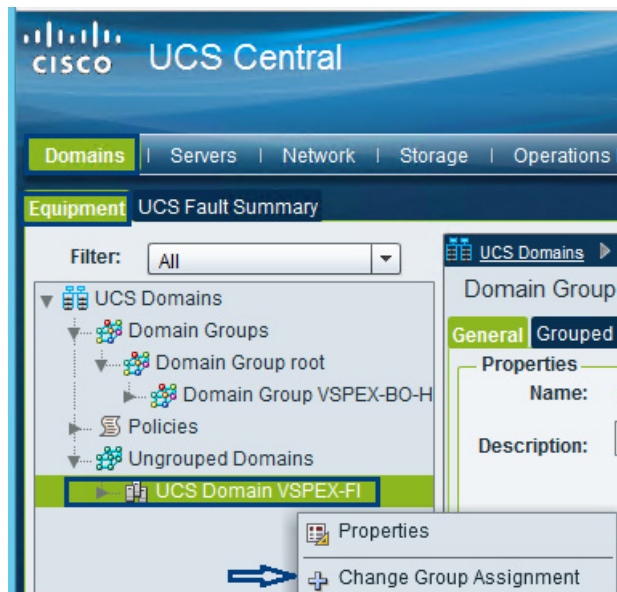
**Properties**

**Name:** VSPEX-BO-HyperV

**Description:** Domain Group for Hyper-V Branch Office in Site 1

3. Click **Ungrouped Domains** and right-click on discovered Branch office UCS Domain “VSPEX-FI” and click **Change Group Assignment**.

**Figure 181** *Change Group Assignment*



4. Choose the Domain group “Branch Office-1” and click **OK**.

**Figure 182** *Select Domain Group*

**Change Group Assignment**

## Change Group Assignment for UCS VSPEX-FI

☐ Unassigned

☐ Domain Group root

☒ Domain Group VSPEX-BO-HyperV

5. Next click **Yes** to confirm. You can now see the VSPEX Branch Office domain (VSPEX-BO-Hyper-V) added to the group.

Figure 183 Domain Group: Properties

The screenshot shows the Cisco UCS Central interface with the 'Domains' tab selected. The left sidebar shows a tree view with 'UCS Domains' expanded, showing 'Domain Groups' and 'Domain Group root'. The 'Domain Group VSPEX-BO-H' is selected. The main area displays the 'Domain Group VSPEX-BO-HyperV' properties. The 'General' tab is active, showing the 'Name' as 'VSPEX-BO-HyperV' and the 'Description' as 'Domain Group for Hyper-V Branch Office in Site 1'. Below this, the 'Domain Group Membership' section shows a table with one member: 'VSPEX-FI'.

UCS Name	Owner	Site	Management IP	UCS Visibility
VSPEX-FI			10.29.180.160	visible ↑

## Cisco UCS Central Image Management

Cisco UCS software bundles should be downloaded to Cisco UCS Central for later use in host firmware management or Cisco UCS system upgrades. The server and infrastructure images can be uploaded by navigating to Operations Management.

Figure 184 Upload UCS Central Bundle

The screenshot shows the Cisco UCS Central interface with the 'Operations Management' tab selected. The left sidebar shows a tree view with 'Images' expanded, showing 'Library'. The main area displays the 'Library of Images' section. The 'General' tab is active, showing a 'Fault Summary' with 0 errors, 0 warnings, 0 info, and 0 debug. Below this, the 'Packages' section shows a table with 5 records. The 'UCS Central bundle' is highlighted.

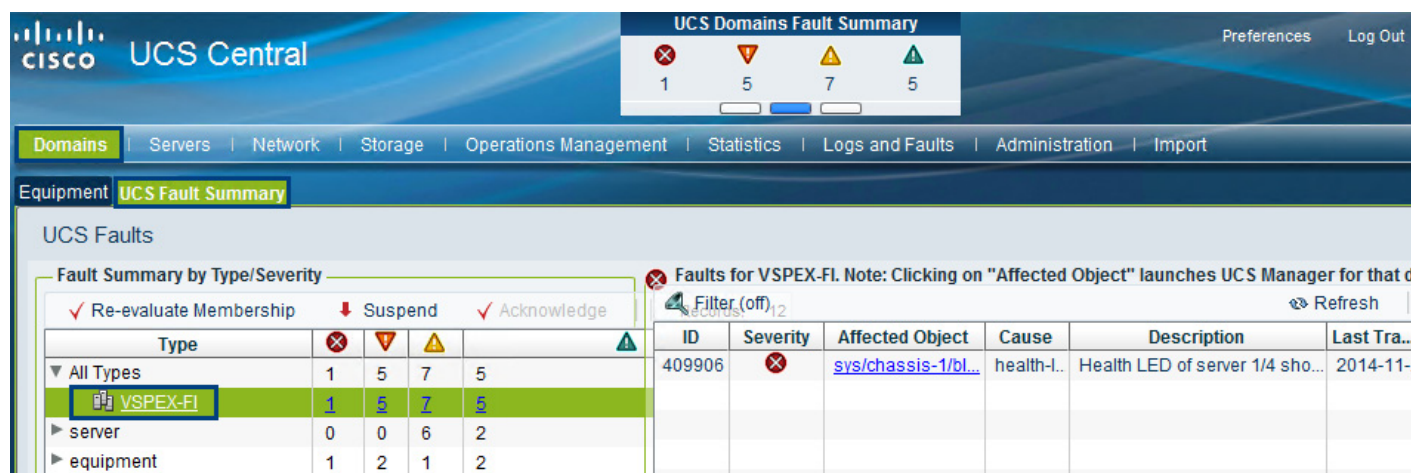
Name	Version	Source	State	Type	Hide
b-series-bundle					
c-series-bundle					
catalog					
infrastructure bundle					
UCS Central bundle					
ucs-central-bundle.1.2.1a.bin	1.2(1a)	local	downloaded	provider-bundle	<input type="checkbox"/>



## Cisco UCS Central Fault Management

The Cisco UCS Central globally manages Fault and Error management for all registered UCS domains in single pane. Figure 185 shows the UCS faults for the VSPEX Branch Office site managed by UCS Central on a single pane.

Figure 185 UCS Faults Summary for VSPEX Branch Office



## Global Identifier Management

Global identifier management addresses one of the biggest challenges around multi-domain management: unique address management for system identifiers (MAC's, WWxN's, UUID's, etc.). Previously, UCS Manager best practices recommend embedding a "domain ID" within the high-order bytes of the ID pool ranges. However, this still involved manual intervention and could be error prone.

With UCS Central, all the ID pools can be defined and accessed globally across all UCS domains. Service Profile assignment can be guaranteed unique and non-overlapping with respect to ID's across all UCS domains. Global ID Pools belong to the organization structure. Global pools do not terminate on DGs, as the UCS Central "Operational Policies" do. Instead, the range of Global ID Pools extends across all UCS domains in the scope of the organization structure within UCS Central; regardless of any DG partitioning UCS Central provides visibility in to possible duplicate ID usage.

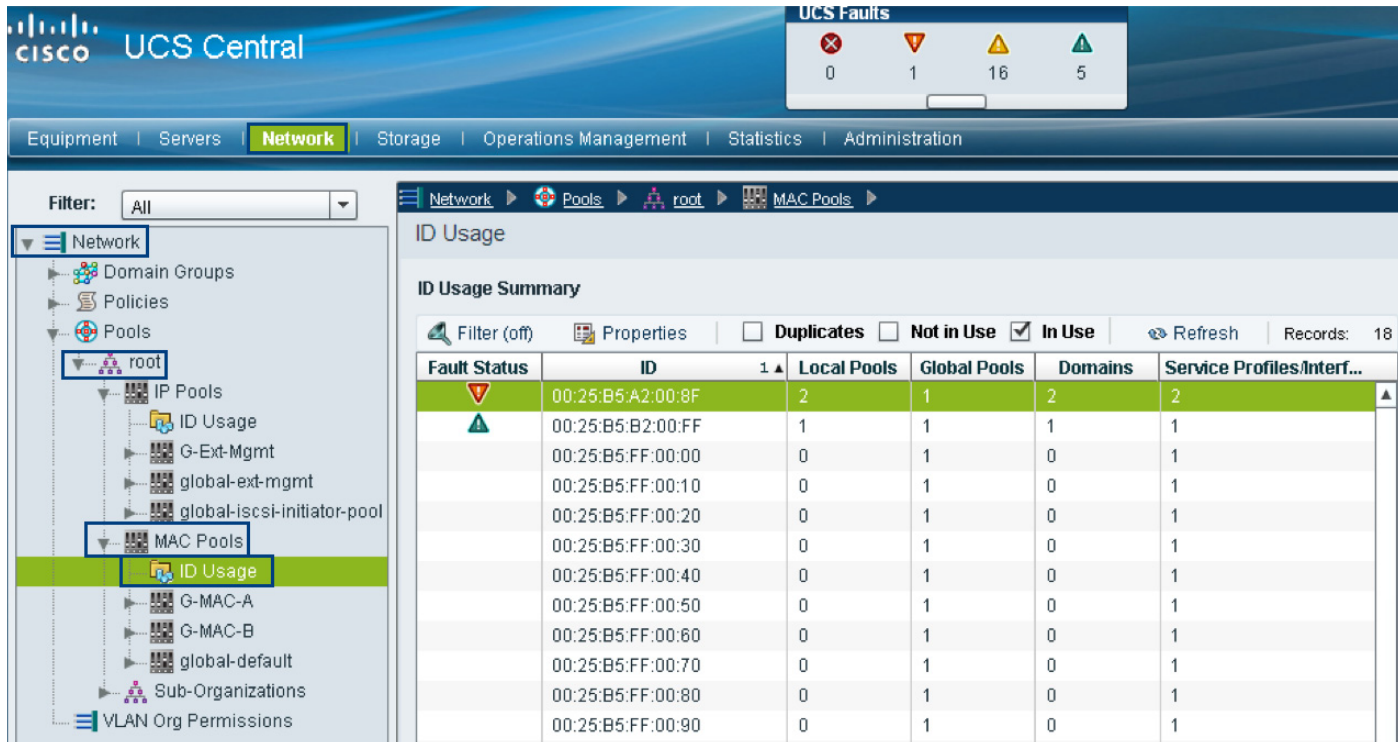
All of the pool types (UUID, MAC, and WWxN) offer the ability to display duplicate IDs that may exist across UCS domains, through the "ID Usage Summary". Duplicate ID severity will be flagged as either "Major", for IDs that appear in multiple Service Profiles, or flagged as "Warning" for IDs that appear in multiple local pools.



### Note

The only way to view Local ID Pool consumption is to select an individual ID, and view the corresponding drill-down details to the right (Local Pool and Local Service Profile) conflicting pool assignments are reported as faults. Unallocated IDs that belong to overlapping pools are reported as warnings.

Figure 186 Pool ID Usage

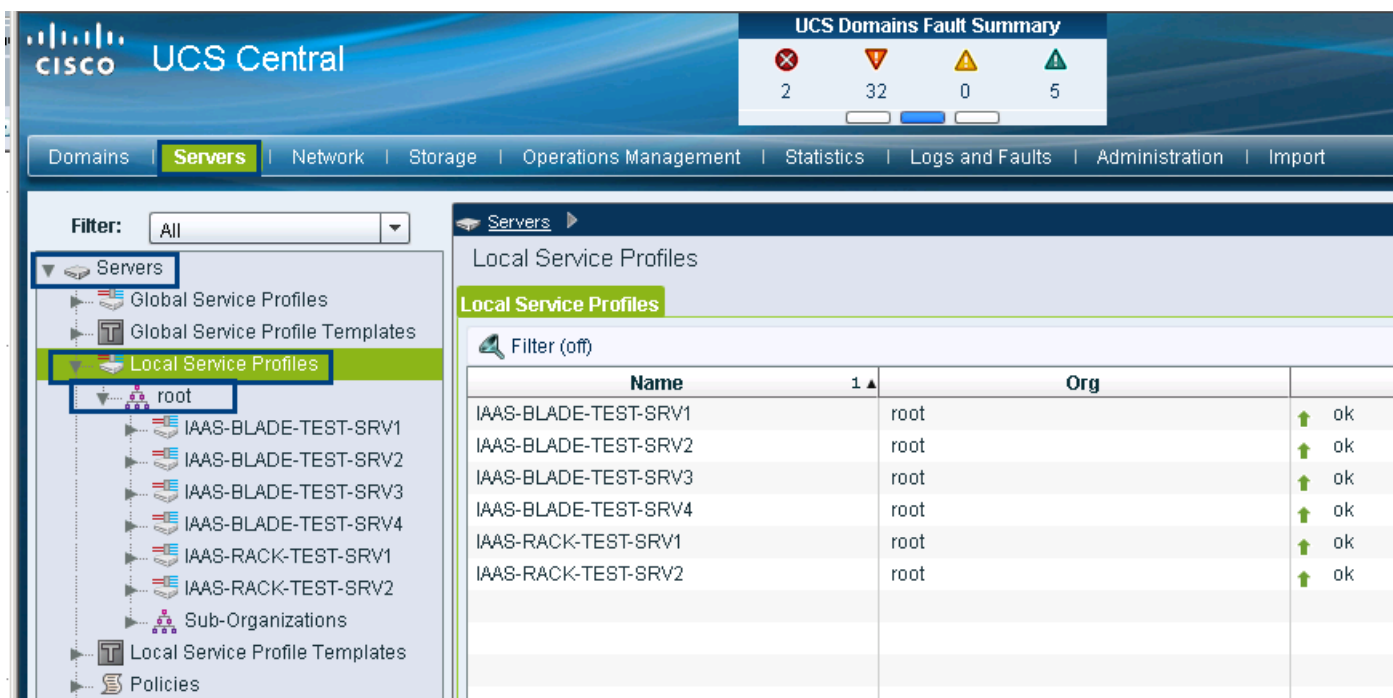


## Cisco UCS Central Service Profile Management

The Cisco UCS Central manages both local Service profile and global service profile in a single pane. Since Local service profiles are completely managed by UCS Manager, the UCS central has limited options to manage these local service profiles. The Cisco UCS Central shows limited options and different icon for a locally defined Service Profile.

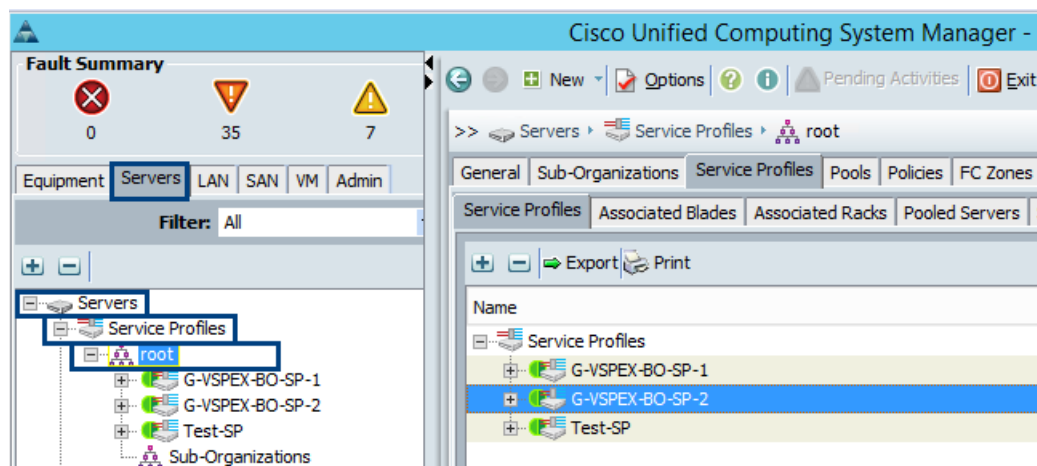


**Figure 187**      *List of Local Service Profiles*



Below you can see the Cisco UCS Manager displays a green circle next to the Global Service Profile icon and most of the configuration options are grayed out for a globally defined Service Profile.

**Figure 188**      *Configuring Global Service Profile*



The global and locally defined information conforms to the following key principles at this time:

1. Existing local service profile templates can be imported into Cisco UCS Central.
2. Existing local service profiles cannot be assigned to Cisco UCS Central
3. Existing local policies (for example local disk policies) can be made "global" and therefore be used by global service profile templates
4. Globally defined policies can be used by local service profiles.

5. Global Service Profiles can be made local but once localized, these service profiles cannot be assigned back to Cisco UCS Central

**Note**

For this solution design, unique policies, templates and pools were defined in Cisco UCS Central. If possible, a suffix should be added to the names of globally defined profiles, pools and policies to uniquely signify the value definition in Cisco UCS Central.

## Configuring Cisco UCS Central

Cisco UCS Central configuration is very similar to the Cisco UCS Manager configuration. Cisco UCS Central tabs are also in line with the Cisco UCS Manager's tabs for Server, Network and Storage. Using the steps used to configure Cisco UCS Manager, following parameters need to be configured in Cisco UCS Central:

- IP Pools for Management (Network | IP Pools | global-ext-mgmt)
- Server Pools (Servers | Pools | Server Pools)
- UUID Suffix Pools (Servers | Pools | UUID Suffix Pools)
- MAC Address Pools (Network | Pools | MAC Pools)
- WWNN Pools (Storage | Pools | WWN Pools | WWNN)
- WWPN Pools (Storage | Pools | WWN Pools | WWNN)
- Boot Policies (Servers | Policies | Boot Policies)
- BIOS Policy (Servers | Policies | BIOS Policies)
- Host Firmware Policy (Servers | Policies | Host Firmware Packages)
- Power Control Policy (Servers | Policies | Power Control Policies)
- vNIC/vHBA Placement Policy (Servers | Policies | vNIC/vHBA Placement Policies)
- vNIC Template (Network | Policies | vNIC Templates)
- vHBA Template (Storage | Policies | vHBA Templates)
- Service Profile Templates (Servers | Global Service Profile Templates)

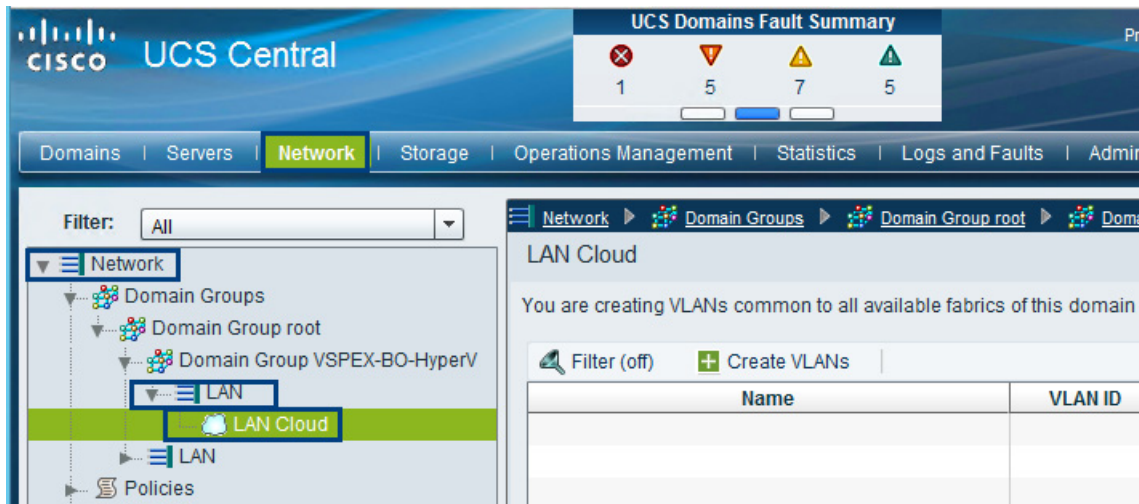
With all the configurations in place, Service Profiles can be deployed on the Cisco UCS domains from Cisco UCS Central.

Next Section covers the creation of VLAN, VSAN, Pools, Policies, Service Profile Template and Service Profile for the VSPEX Branch Office servers using UCS Central Management GUI. Creating all new pools, policies, templates and service profiles for the exiting UCS domain is disruptive and hence requires downtime. The other option is to import the local service profile templates along with policy and resource dependencies and instantiate new global service profiles and apply it. UCS Central allows you to run estimate impact on actions (like import) to ensure that potential impacts are understood.

## Configuring VLANs, VSANs and vNIC Templates

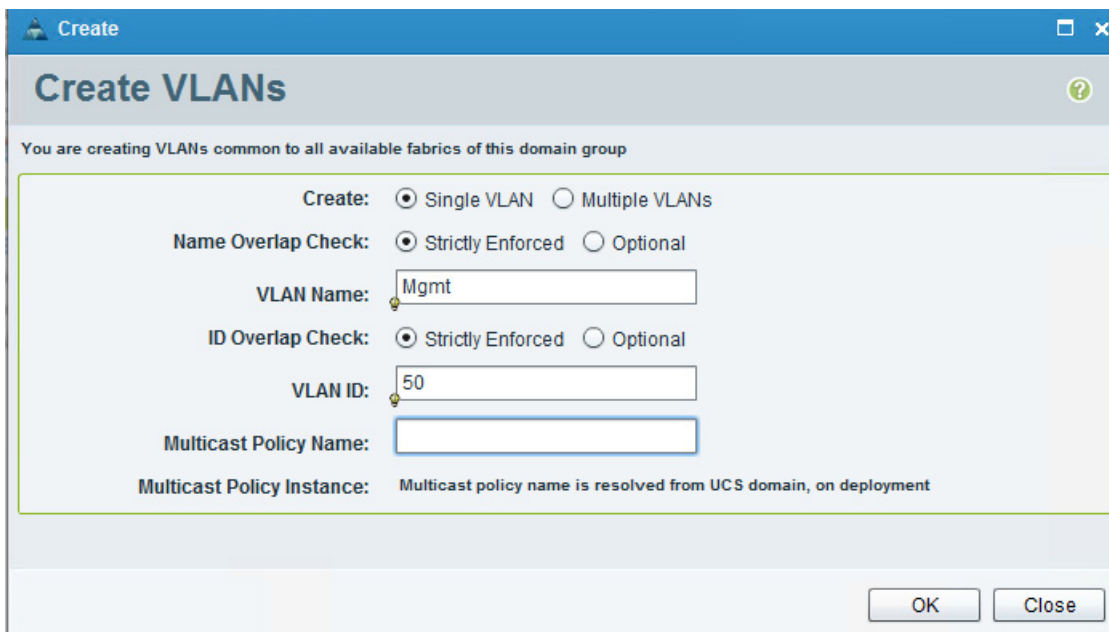
1. Launch **Cisco UCS Central** web user interface and click the domain group as **BranchOffice-1**. Click **LAN Cloud** and then click **Create VLANs**.

**Figure 189**      **Create VLANs**



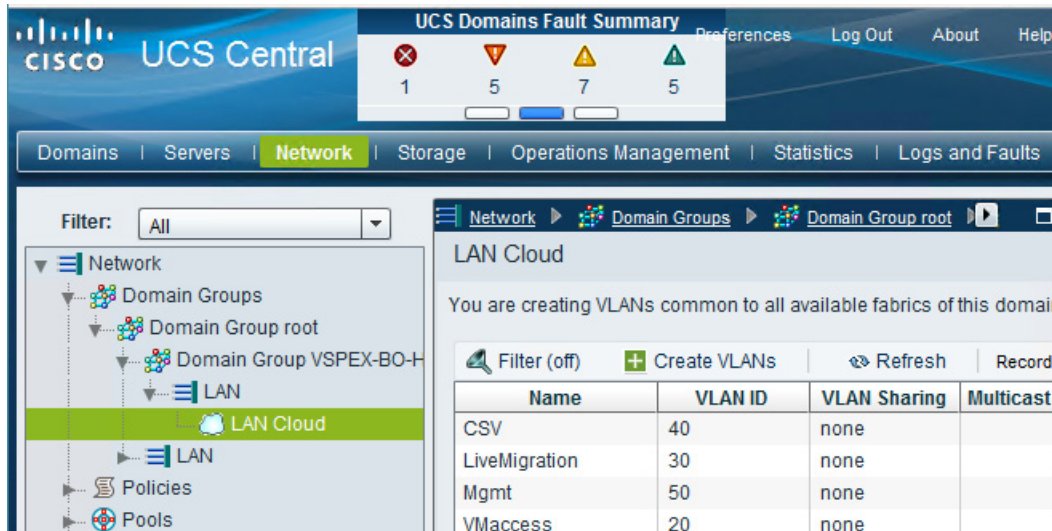
2. Specify the VLAN Name and VLAN ID. Click **OK**.

**Figure 190**      **Create VLAN Window**



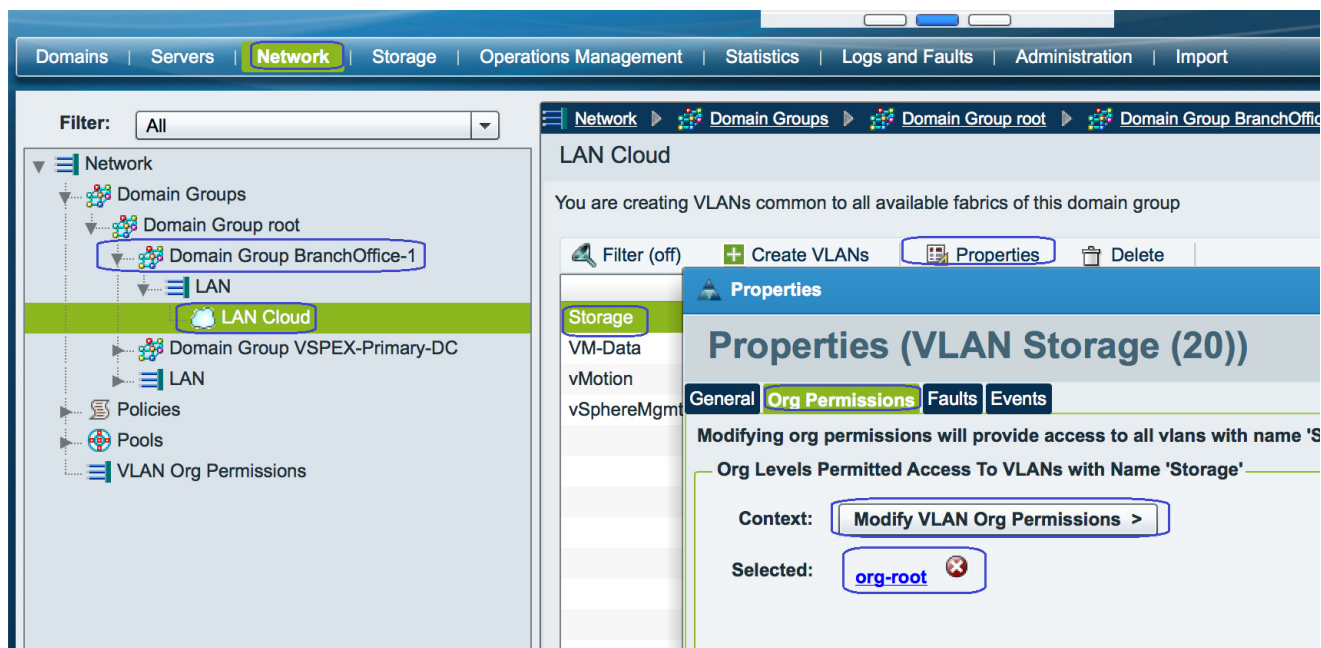
3. Repeat these steps to create VLANs for “VMaccess - VLAN20”, “LiveMigration - VLAN30” and “CSV -VLAN40”.
4. After successful creation of VLANs, you can see all the VLANs as shown below:

Figure 191 Created VLANs



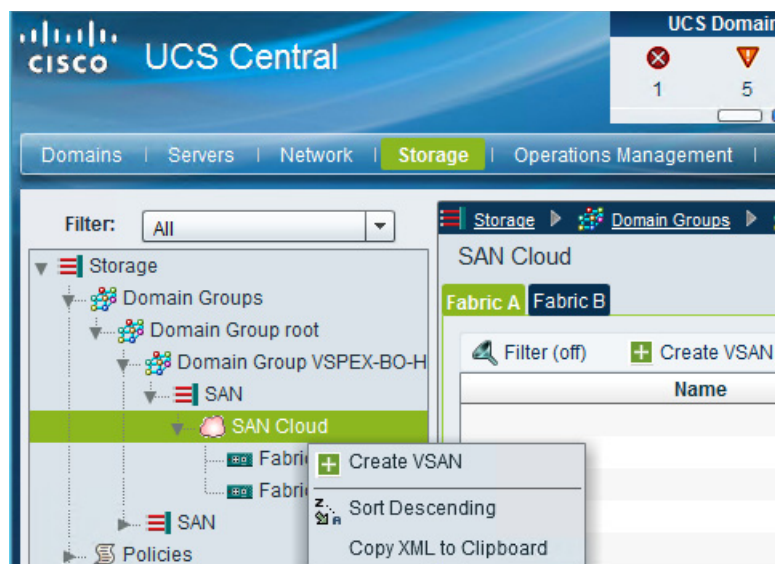
5. Select a VLAN and click Properties and then on Org Permissions. Click **Modify VLAN Org Permissions** to select the appropriate organization as shown in the below figure.

Figure 192 Select Organization



6. To create VSAN, navigate to Domain Group **VSPEX-BO-HyperV** > **SAN Cloud** and click **Create VSAN**

Figure 193 Create VSAN



7. In the **Create VSAN** window, specify a Name and select Fabric A and Fabric B. Select Enabled for FC Zoning and specify a VSAN ID and a corresponding VLAN ID for FCoE VLAN (see Figure 194).

Figure 194 Create VSAN Windows

**Create VSAN**

Name:

☐ Fabric A ☐ Fabric B ☒ Fabric A & Fabric B

**FC Zoning Settings**

FC Zoning: ☐ Disabled ☒ Enabled

Do NOT enable zoning for this VSAN, if the fabric interconnect is connected to an upstream switch that has zoning enabled on the same VSAN.

**Fabric A**  
Enter the VSAN ID that maps to this VSAN.  
VSAN ID:

**Fabric B**  
Enter the VSAN ID that maps to this VSAN.  
VSAN ID:

**Fabric A**  
Enter the VLAN ID that maps to this VSAN.  
FCoE VLAN:

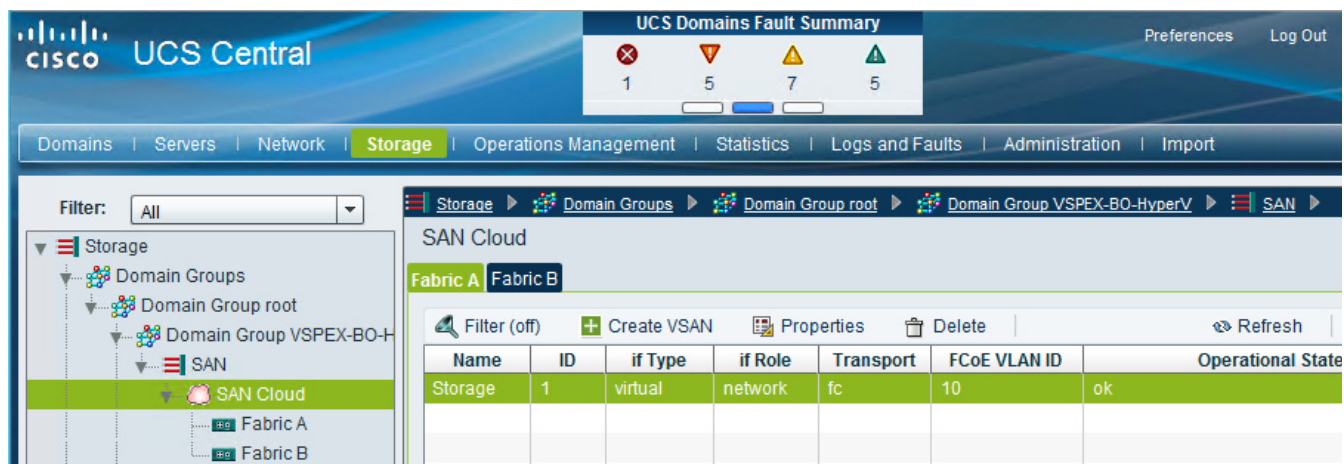
**Fabric B**  
Enter the VLAN ID that maps to this VSAN.  
FCoE VLAN:

OK Close

8. After successful creation, you can see the VSAN “Storage” under SAN cloud.



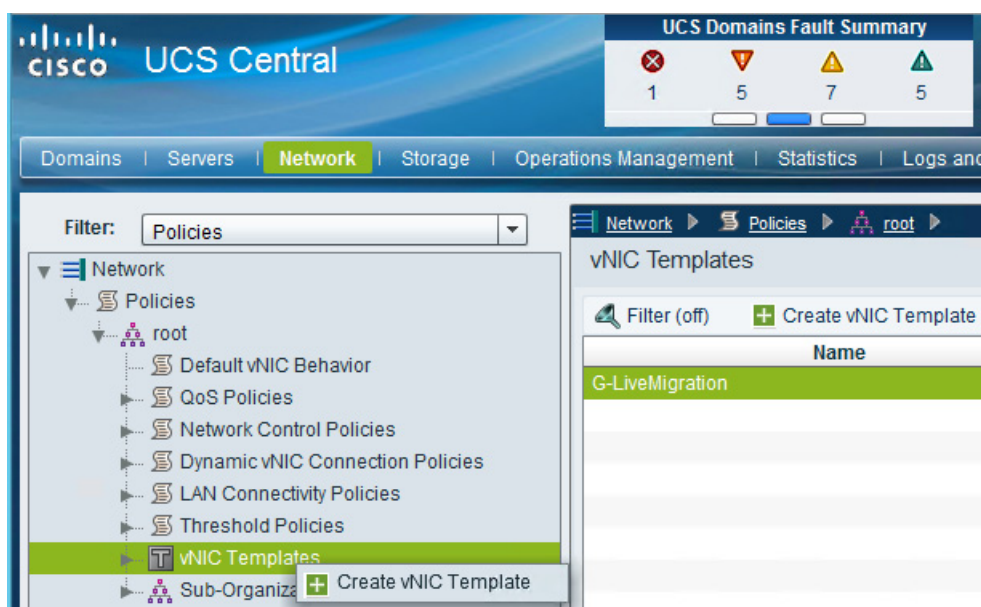
Figure 195 Create VSAN Storage

**Note**

With UCS Central 1.2(1a), physical device configuration of the Fabric Interconnect ports can now be configured through UCS Central. However, the configuration types are currently limited to “Server” and “Uplink” ports. Managed objects that depend on physical ports cannot be managed through UCS Central, including Pin Groups and Port-Channels for both Ethernet and FC.

9. Launch the **UCS Manager**, to create VSAN under Storage Cloud and configure the FI ports as “FC Storage Port” by following the steps listed in Prepare UCS FIs and Configure **UCS Manager** > **Upstream/Global Network Configuration** > **Create VSANs and Configuring Ports on UCS Fabric Interconnects** > **Configure Unified Ports for Fibre Channel** sections.
10. In the UCS Central GUI, to create vNIC Templates navigate to **Network** > **Domain Groups** > **Policies** > **root** > **vNIC Templates** and right-click the **Create vNIC Templates**.

Figure 196 Create vNIC Template



- On the **Create vNIC Template** window, select and provide details with the information given in [Table 12](#).

Figure 197 Create vNIC Template Window

**Create vNIC Template**

**Properties**

Name:

Description:

Template Type: ☐ initial-template ☒ updating-template

**Details**

Fabric ID: ☐ A ☒ B

Failover: ☒ Enable

MTU:

Type: ☒ adaptor ☐ vm

**Permitted VLANs**

Filter (off) Refresh Records: 4

Name
CSV
LiveMigration
Mgmt
VMaccess

Select >

**Selected VLANs**

Properties Delete Refresh Records: 0

Name	Set Native
CSV	<input checked="" type="radio"/>

**Policies**

MAC Pool:  [+ Create MAC Pool](#)

QoS Policy:  [+ Create QoS Policy](#)

Network Control Policy:  [+ Create Network Control Policy](#)

Stats Threshold Policy:  [+ Create Threshold Policy](#)

Pin Group Name:

Pin Group Instance: Pin Group policy name is resolved from UCS domain, on deployment

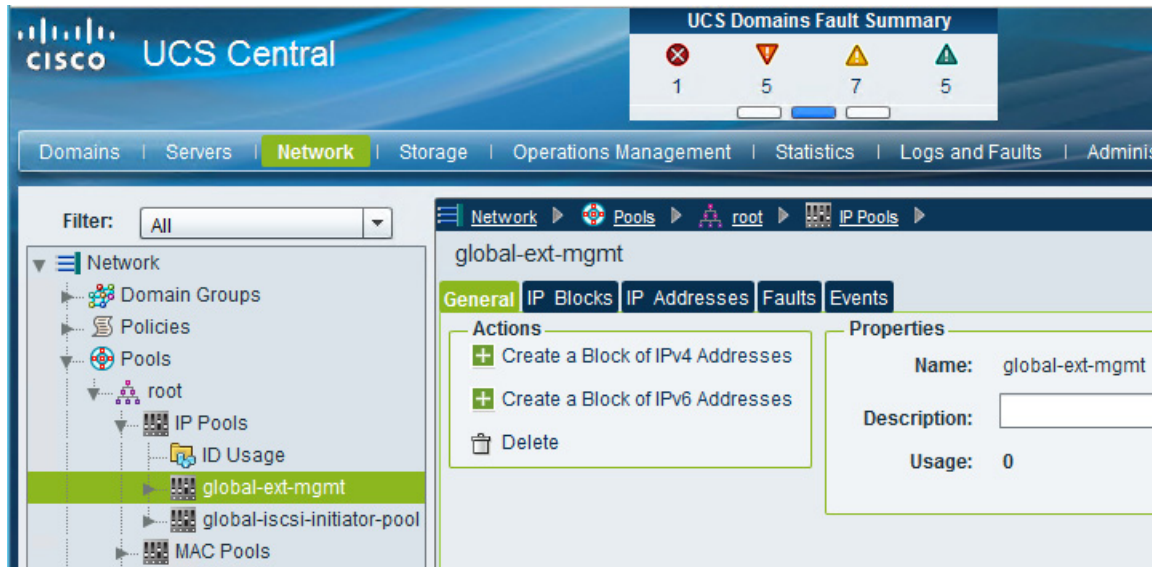
OK Close

Repeat steps 9 and 10 to create vNIC templates for management, live migration and VMaccess using the details as provided in the Table 13

## Configuring Pools and Polices

- Launch UCS Central GUI and choose **Network > Pools > IP Pools > global-ext-mgmt** and then click **Create a Block of IPv4 Addresses**.

**Figure 198** *Create IPv4 Address Block*



2. Specify the IP range for the IP Pool for managing the UCS blades KVM console.
3. Click OK.

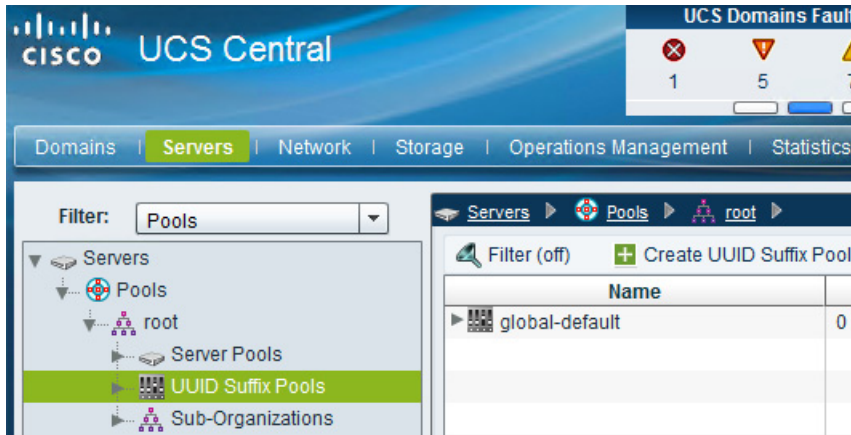
**Figure 199** *Create IPv4 Address Block Window*

The screenshot shows a 'Create a Block of IPv4 Addresses' dialog window. It has a title bar with a question mark icon. The main area contains several input fields: 'From:' (10 . 29 . 180 . 225), 'Size:' (8), 'Subnet:' (255 . 255 . 255 . 0), 'Default Gateway:' (10 . 29 . 180 . 1), 'Primary Dns:' (0 . 0 . 0 . 0), 'Secondary Dns:' (0 . 0 . 0 . 0), and 'Scope:' (public). Below these fields is a section titled 'ID Range Qualification Policy' with a '+ Create ID Range Qualification Policy' button. A warning message states: 'Warning: Pools containing an ID block referencing ID range qualification policy can only be used by local service profiles. Global service profiles cannot use pools referencing this policy.' Below the warning is a dropdown menu for 'ID Range Qualification Policy:'. At the bottom right are 'OK' and 'Close' buttons.



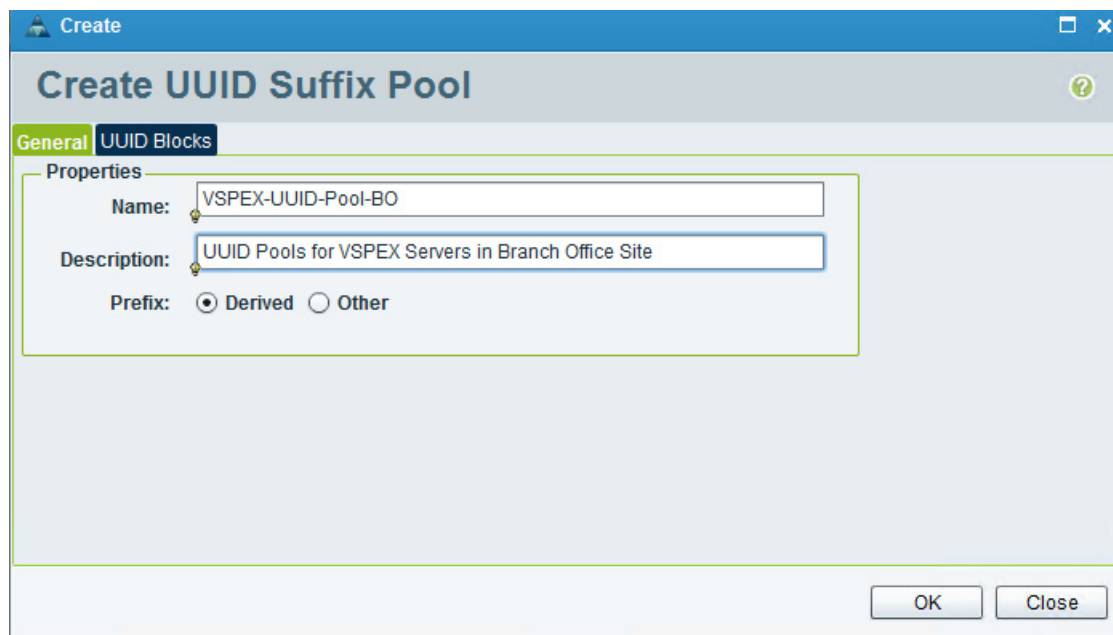
- To create UUID pools, choose **Servers > Pools > root > UUID Suffix Pools** and then click **Create UUID Suffix Pool** as shown below.

*Figure 200 Create UUID Pools*



- In the **General** tab page, specify the UUID Pool name and description and click **OK**.

*Figure 201 Create UUID Suffix Pool: UUID Blocks*



- In the **Create UUID Suffix Pool** window, choose **UUID Blocks** and then click **Create a Block of UUID Suffixes**.

**Figure 202** *Create UUID Suffix Pool*

Name	From

- Specify an UUID range (See figure 203) and click **OK**

**Figure 203** *Create UUID Suffixes Block*

To create MAC pools, navigate to **Network > Pools > root > MAC Pools** and click **Create MAC Pool**

**Figure 204** *Create MAC Pool*

Name
global-default

- In the **General** tab, specify the MAC Pool name and description and click **OK**.

**Figure 205** *Create MAC Pool: General*

**Create**

## Create MAC Pool

**General** | **MAC Blocks**

**Properties**

**Name:** VSPEX-BO-MAC-Pool

**Description:** MAC Pools for VSPEX Servers in Branch Office Site 1

- In the **Create MAC Pool** window, click **Create a Block of MAC Addresses**.

**Figure 206** *Create MAC Pool: MAC Block*

**Create**

## Create MAC Pool

**General** | **MAC Blocks**

Filter (off) | **+ Create a Block of MAC Addresses**

Name	From

- Specify a MAC range and size. Click **OK**

**Figure 207** *Create MAC Address Block*

**Create**

## Create a Block of MAC Addresses

**From:** 00:25:B5:07:0D:00 **Size:** 40

**ID Range Qualification Policy**

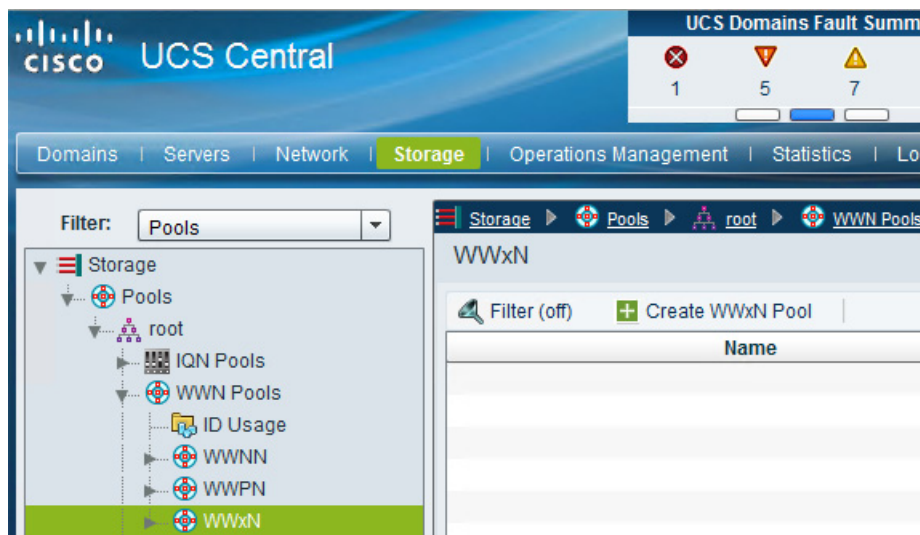
**+ Create ID Range Qualification Policy**

Warning: Pools containing an ID block referencing ID range qualification policy can only be used in Global service profiles cannot use pools referencing this policy.

**ID Range Qualification Policy:** ▼

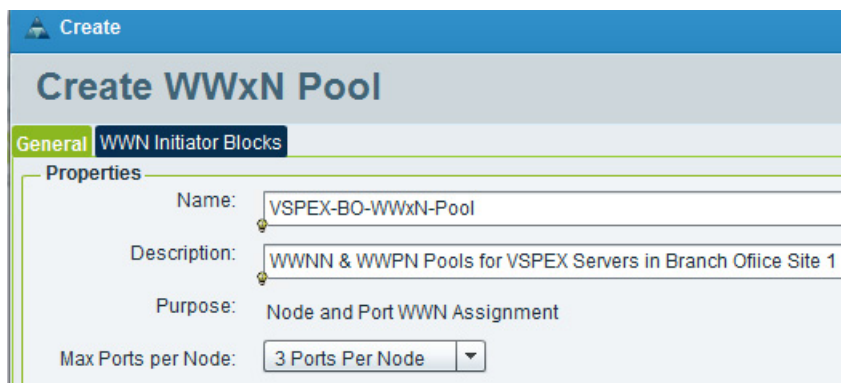
- To create WWN Pools, navigate to **Storage > root > Pools > WWN Pools > WWxN** and click **Create WWxN Pool**.

Figure 208 Create WWxN Pool



12. On the **Create WWxN Pool > General** tab, specify WWxN pool name and description and choose 3 Ports per Node from the drop-down list.

Figure 209 Create WWxN Pool Windows



13. From the **WWN Initiator Blocks** tab, click Create Block and then click **OK**.

Figure 210 Create Initiator Block

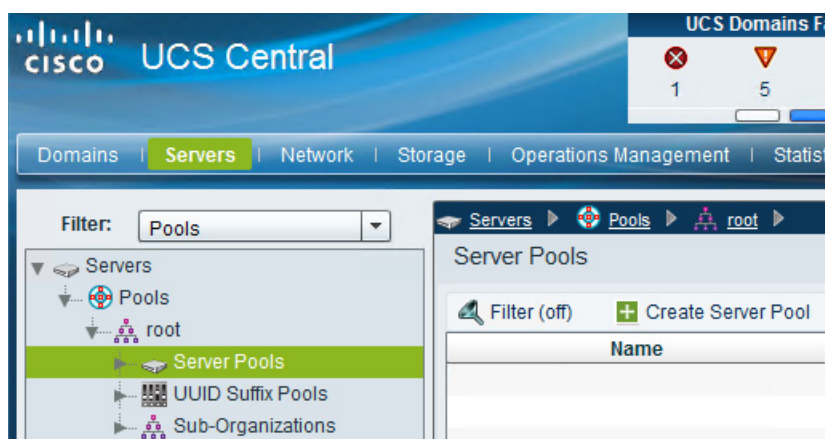


14. Specify the range for the Block and click **OK**

**Figure 211**      **Create Initiator Block**

15. To create Server Pool, navigate to **Servers > Pools > root > Server Pools** and click **Create Server Pool**

**Figure 212**      **Create Server Pool**



16. In the Main page of **Create Server Pool** window, provide a name and description and click **Finish** to create a server pool.

The compute resources in this pool will be added dynamically based on a server pool policy created in the next few steps

Figure 213 Create Server Pool Window

**Create Server Pool**

**Main**

You must enter the name for the server pool to continue.

Name: VSPEX-BO-Server-Pool

Description: Server Pool for VSPEX Branch Off

< Prev   Next >   Finish   Close

- To create a Server Pool Policy Qualification, navigate to **Servers > Policies > root > Server Pool Policy Qualifications** and choose **Create Policy Qualification**.

Figure 214 Create Server Pool Policy Qualification

**UCS Central**

UCS Domains Fault Summary

1	5	7	5
---	---	---	---

Domains | **Servers** | Network | Storage | Operations Management | Statistics | Logs

Filter: Policies

Servers > Policies > root > Server Pool Policy Qualifications

Filter (off) + Create Policy Qualification

Name
all-domain

- Specify a name and description and click **Create Memory Qualification**.

**Figure 215**      *Creating Policy Qualification Window*

**Create**

## Create Policy Qualification

Name:

Description:

**Actions**

- + Create Domain Qualification
- + Create Adapter Qualification
- + Create Memory Qualification
- + Create Processor Qualification

**Qualifications**

Filter (off)

Name	Max

19. Deselect the check box Min Cap (MB) and specify the minimum memory value in MB for 128GB. Click **OK**.

**Figure 216**      *Create Memory Qualification*

**Create**

## Create Memory Qualification

Clock (MHz): ☒ Unspecified

Min Cap (MB): ☐ Unspecified

Width: ☒ Unspecified

Speed: ☒ Unspecified

Latency (ns): ☒ Unspecified

Max Cap (MB): ☒ Unspecified

Units: ☒ Unspecified

**OK** **Close**

20. Click **OK/Close** on the **Create Policy Qualification** window



**Figure 217**      *Verify the Created Memory Qualification*

**Properties (Min-Memory)**

**General** | **Events**

**Name:** Min-Memory

**Description:** Minimum Memory Qualification for VSPEX Servers in BO Site 1

**Actions**

- + Create Domain Qualification
- + Create Adapter Qualification
- + Create Memory Qualification

**Qualifications**

Filter (off) Records: 1

Name	Max	Model	From	To	Archite...	Speed	Stepping
Memory Qualification						unspecified	

To create Server Pool policy, navigate to **Servers > Policies > root > Server Pool Policies** and choose **Create Server Pool Policy**.

**Figure 218**      *Create Server Pool Policy*

**UCS Central**

UCS Domains Fault Summary

1 5 7 5

Domains | **Servers** | Network | Storage | Operations Management | Statistics | Logs

Filter: Policies

Servers

- Policies
  - root
    - Adapter Policies
    - BIOS Policies
    - Boot Policies
    - Host Firmware Packages
    - IPMI Access Profiles
    - iSCSI Authentication Profile
    - Local Disk Config Policies
    - Maintenance Policies
    - Power Control Policies
    - Scrub Policies
    - Serial over LAN Policies
    - Server Pool Policies**
    - Server Pool Policy Qualifications

Servers > Policies > root > Server Pool Policies

Server Pool Policies

Filter (off) + Create Server Pool Policy

Name

Provide a name and description. Then choose the respective Target Pool and Qualification that was created earlier and click **OK**.



**Figure 219** Create Server Pool Policy Window

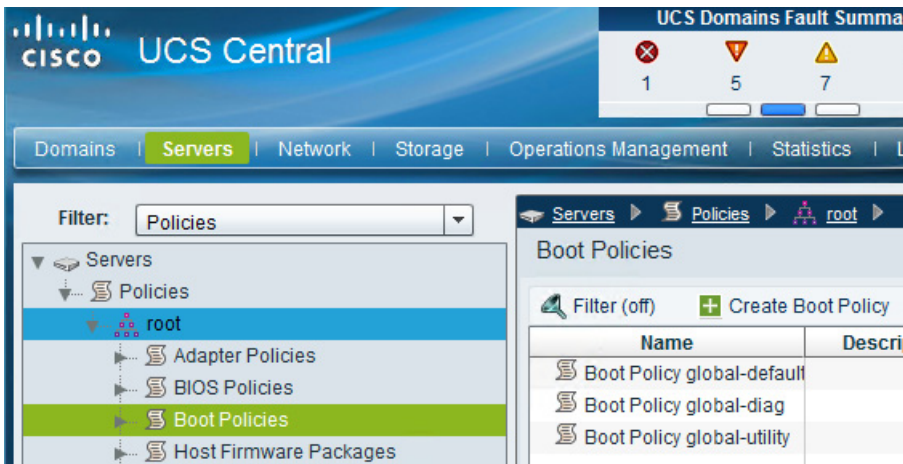
After successful Server Pool Policy creation, you will see the VSPEX Branch Office servers added dynamically as shown below:

**Figure 220** Verify the Dynamically Added Branch Office Servers

Name	UCS Domain	Chas...	Slot ID
Server 1/1	VSPEX-FI	1	1
Server 1/4	VSPEX-FI	1	4
Server 1/3	VSPEX-FI	1	3

To create SAN-Boot Policy, choose **Servers > Policies > root > Boot Policies** and click :

Figure 221 Boot Policies



Name the boot policy and give description. Check Reboot on Boot Order Change and Enforce vNIC/vHBA Name. Choose **Add Local CD/DVD** from under **Actions > Local Devices**.

### Create Boot Policy

[illegible]

Choose **Add SAN Boot** and specify a name and the SAN Type is automatically selected as Primary. Click **OK**.

**Figure 223**      *Add SAN Boot*

The screenshot shows the 'Create Boot Policy' window in Cisco UCS Central. At the top, there is a 'Create' button. Below it, the title 'Create Boot Policy' is displayed. A 'WARNINGS:' section contains the following text: 'The type (primary/secondary) does not indicate a boot order presence. The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order. If Enforce vNIC/vHBA/iSCSI Name is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.' Overlaid on this is the 'Add SAN Boot' dialog box. The dialog has a title bar 'Add SAN Boot' with a question mark icon. The main area is titled 'Add SAN Boot' and contains a 'Properties' section. In this section, the 'vHBA:' field is set to 'vHBA-A' and the 'Type:' is set to 'Primary' (selected with a radio button). Below these fields is a large empty text area. At the bottom right of the dialog are 'OK' and 'Close' buttons. In the background, the 'vHBAs' section of the 'Create Boot Policy' window is visible, showing a table with columns for Name, Type, and Status. The table has one row with 'vHBA-A' in the Name column and 'Primary' in the Type column. Below the table are three buttons: '+ Add LAN Boot', '+ Add SAN Boot', and '+ Add SAN Boot Target'.

Create

## Create Boot Policy

**WARNINGS:**  
The type (primary/secondary) does not indicate a boot order presence.  
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
If Enforce vNIC/vHBA/iSCSI Name is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.

**Add SAN Boot**

### Add SAN Boot

**Properties**

vHBA: vHBA-A

Type: ☒ Primary ☐ Secondary

OK Close

+ Add LAN Boot

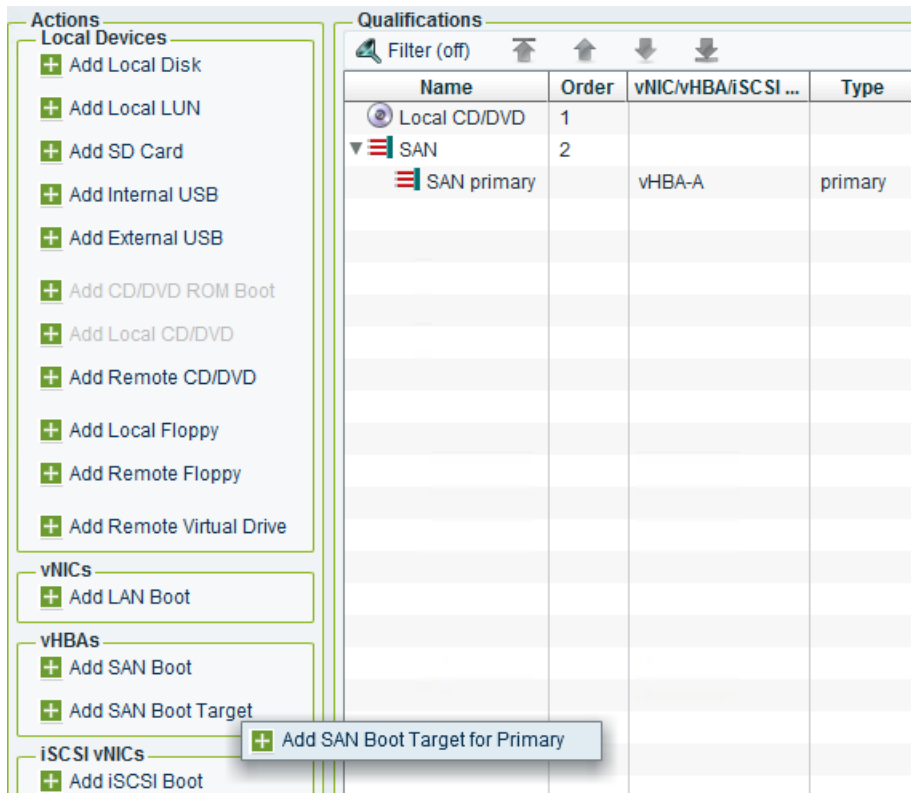
vHBAs

+ Add SAN Boot

+ Add SAN Boot Target

Choose **Actions > vHBAs > Add SAN Boot Target** and then click **Add SAN Boot Target** for Primary.

**Figure 224** Add SAN Boot Target for Primary



Keep the value for Boot Target LUN as 0 and enter the WWPN of the VNXe SP A Port 0.

21. Click **OK** to add the SAN boot target.

**Figure 225** Add SAN Boot Target for Primary: Properties

**Add SAN Boot Target for Primary**

**Add SAN Boot Target for Primary**

**Properties**

Boot Target LUN:

Boot Target WWPN:

Type: ☒ Primary ☐ Secondary

22. Repeat the above steps to add the additional paths using the SAN-Boot policy Table 11 provides in the create SAN Boot Policy section of UCS Manager.

23. After adding all the additional paths the boot policy should look like as shown in the below figure.

Figure 226 Create Boot Policy

## Create Boot Policy

Name:

Description:

Reboot on Boot Order Change: ☐

Enforce vNIC/vHBA/iSCSI Name: ☒

Boot Mode: ☒ Legacy ☐ Uefi

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If Enforce vNIC/vHBA/iSCSI Name is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

**Actions**  
**Local Devices**  
☒ Add Local Disk  
☒ Add Local LUN  
☒ Add SD Card  
☒ Add Internal USB  
☒ Add External USB  
☒ Add CD/DVD ROM Boot  
☒ Add Local CD/DVD

**Qualifications**  
☒ Filter (off) ☒ Properties ☒ Delete

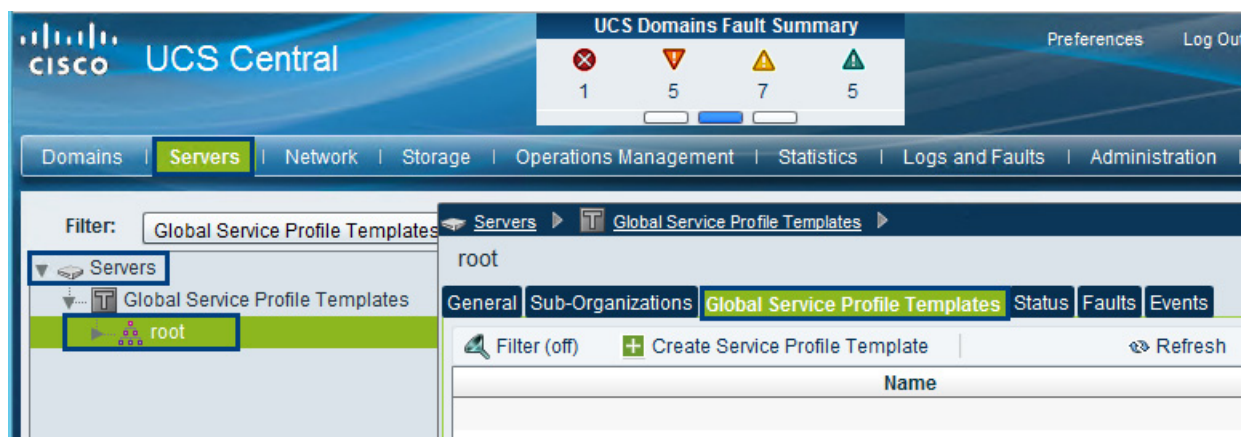
Name	Order	vNIC/vHBA/iSCSI vNIC	Type	LUN ID	
Local CD/DVD	1				
▼ SAN	2				
▼ SAN primary		vHBA-A	primary		
SAN Target primary			primary	0	50:06:01:64:0
SAN Target second			secondary	0	50:06:01:6C:0
▼ SAN secondary		vHBA-B	secondary		
SAN Target primary			primary	0	50:06:01:6D:0
SAN Target second			secondary	0	50:06:01:65:0

## Configuring Global Service Profile Template

Global service profile templates enable you to quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools. Service profile templates in Cisco UCS Central are similar to the service profile templates in Cisco UCS Manager.

1. To create Global Server Profile Templates for the VSPEX Branch Office servers, launch the **UCS Central** Web GUI. Navigate to **Servers > Global Service Profile Templates > root** and then choose **Create Service Profile Template**.

Figure 227 Create Global Service Profile Template



- Specify the Service Profile Template name and description. Select **Updating Template** radio button for Type and choose the UUID Pool that was created earlier. Click **Next**.

Figure 228 Create Service Profile Template: General

- In the **Networking** section, choose the **Configuration Type** as vNICs – Expert Mode from the drop-down list and choose **Create vNIC**. Click **Next**.



Figure 229 Create Service Profile Template: Networking

The screenshot shows the 'Create Service Profile Template' window with the 'Networking' tab selected. The left sidebar contains links for General, Networking, Storage, vNIC/MHBA Placement, Boot Order, Maintenance Policy, Server Assignment, and Policies. The main content area has a title bar 'Create' and a subtitle 'Create Service Profile Template'. Below the title bar, there is a section 'Optionally specify dynamic vNIC Connection policy and LAN configuration information.' with a '+ Create Dynamic vNIC Connection Policy' button. A text prompt says 'Indicate the whether dynamic vNICs should be used and if so the policy to be used.' followed by a dropdown menu 'Dynamic vNIC Connection Usage:' set to 'Do not use'. Below this is a section 'LAN Connectivity' with a '+ Create LAN Connectivity Policy' button. A text prompt says 'Indicate the method to use to configure LAN Connectivity.' followed by a dropdown menu 'Configuration Type:' set to 'vNICs - Expert mode'. Underneath is a section 'vNICs' with a text prompt 'Click Create to specify one or more vNICs that the server should use to connect to the LAN.' and a '+ Create vNIC' button. Below the button is a table with columns 'Name', 'MAC Address', and 'Fabric ID'. The table is currently empty. To the right of the table, it says 'Records: 0'.

- On the **Create vNIC** window, provide a name and choose **Use vNIC Template**. Choose the vNIC Template created earlier from the drop-down list and then choose **Windows** for Adapter Policy. Click **OK**.

Figure 230 Create vNIC

The screenshot shows the 'Create vNIC' window. The left sidebar contains links for Properties, Details, and Adapter Performance Profile. The main content area has a title bar 'Create vNIC' and a subtitle 'Create vNIC'. Below the title bar, there is a section 'Properties' with a 'Name:' field set to 'G-Mgmt' and a 'Use vNIC Template:' checkbox checked. Below this is a section 'Details' with a 'vNIC Template:' dropdown menu set to 'G-Mgmt', a '+ Create vNIC Template' button, a 'vNIC Template Instance:' field with a link 'org-root/lan-conn-templ-G-Mgmt', and an 'Adapter Performance Profile' section with an 'Adapter Policy:' dropdown menu set to 'global-Windows', a '+ Create Ethernet Adapter Policy' button, and an 'Adapter Policy Instance:' field with a link 'org-root/eth-profile-global-Windows'.

- Similarly add vNICs for CSV, LiveMigration and VMaccess using the vNIC templates created for them in the previous sections. After adding all the required vNICs, the table in the **Networking** page list is now populated as shown in the below figure.



**Figure 231**      *Create Service Profile Template: Networking*

**Create**

## Create Service Profile Template

[General](#)

**[Networking](#)**

[Storage](#)

[vNICvHBA Placement](#)

[Boot Order](#)

[Maintenance Policy](#)

[Server Assignment](#)

[Policies](#)

Optionally specify dynamic vNIC Connection policy and LAN configuration information.

**+ Create Dynamic vNIC Connection Policy**

Indicate the whether dynamic vNICs should be used and if so the policy to be used.

Dynamic vNIC Connection Usage: Do not use

**LAN Connectivity**

**+ Create LAN Connectivity Policy**

Indicate the method to use to configure LAN Connectivity.

Configuration Type: vNICs - Expert mode

**vNICs**

Click Create to specify one or more vNICs that the server should use to connect to the LAN.

Filter (off) **+ Create vNIC** Records: 4

Name	MAC Address	Fabric ID
G-CSV	derived	A
G-LiveMigration	derived	A
G-Mgmt	derived	A
G-VMaccess	derived	A

- Click **Next** to go to the Storage section to create vHBAs. Here choose Configuration Type as vHBAs – Simple Mode and choose the Global Pool we created before and specify the vHBA name for fabric A and Fabric B and then specify the VSAN as Storage for the vHBAs as shown below:

Figure 232 Create Service Profile Template: Storage

The screenshot shows the 'Create Service Profile Template' window with the 'Storage' tab selected in the left-hand navigation pane. The main content area is titled 'Create Service Profile Template' and contains several configuration sections:

- General** (selected in the left pane)
- Networking**
- Storage** (highlighted in green in the left pane)
- vNIC/vHBA Placement**
- Boot Order**
- Maintenance Policy**
- Server Assignment**
- Policies**

The main configuration area is titled 'Create Service Profile Template' and contains the following sections:

- Local Storage Policy**: A section titled 'Optionally specify the SAN configuration information.' containing a '+ Create Local Disk Configuration Policy' button. Below this, it says 'Indicate the method to use to manage the server's local storage.' with a dropdown menu for 'Local Storage Policy' set to 'global-default' and a label for 'Local Storage Policy Instance:'.
- SAN Connectivity**: A section titled 'Indicate the method to use to configure SAN Connectivity.' with a dropdown menu for 'Configuration Type' set to 'vHBAs - Simple Mode'.
- World Wide Node Name (WWNN)**: A section titled 'Indicate the method to use to configure WWNN.' with two radio buttons: 'Derived' (unselected) and 'Global Pool' (selected). The 'Global Pool' option has a dropdown menu set to 'VSPEX-BO-WWxN-Pool (41/48)' and buttons for '+ Create WWN Pool' and 'Reset Pool'.
- vHBAs**: A section containing two sub-sections:
  - vHBA 0 (Fabric A)**: A form with 'Name:' set to 'vHBA-A' and 'VSAN:' set to 'Storage'.
  - vHBA 1 (Fabric B)**: A form with 'Name:' set to 'vHBA-B' and 'VSAN:' set to 'Storage'.

- On the **vNIC/vHBA Placement** window, keep Assignment Method as Default and Click **Next**.

Figure 233 Create Service Profile Template: vNIC/vHBA Placement

**Create Service Profile Template**

Optionally specify how vNICs and vHBAs are placed on physical network adapters.

**Placement Method**  
 Create vNIC/vHBA Placement Policy

Indicate the method to use to assign vNICs and vHBAs to physical network adapters.

**Assignment Method:**

**PCI Order**  
 System will assign vNICs and vHBAs based on their PCI order. To change assignment change the order of the vNICs and vHBAs in the table below.

Filter (off) [Icons] Records: 6 Showing: 6

Name	Address	PCI Order
vNIC G-VMaccess	derived	unspecified
vNIC G-LiveMigration	derived	unspecified
vNIC G-Mgmt	derived	unspecified
vNIC G-CSV	derived	unspecified
vHBA vHBA-A	derived	unspecified
vHBA vHBA-B	derived	unspecified

- On the **Boot Order** window, choose **Boot Policy** for Configuration Type and SAN-Boot created earlier for Boot Policy from the drop-down list

Figure 234 Create Service Profile Template: Boot Order

**Create Service Profile Template**

Optionally specify the Boot Policy for this Service Profile.

**Boot Order Policy**  
 Create Boot Policy

Identify the boot order policy to be applied to the server.

**Configuration Type:**

**Boot Policy:**

**Boot Policy Instance:** [org-root/boot-policy-G-SAN-Boot](#)

**Properties**  
 Description:  
 Reboot on order change: ☒  
 Enforce device names: ☒  
 Boot Mode: legacy

**Boot Order**  
 Records: 2

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	LUN ID	WWN
Local CD/DVD	1				
▼ SAN	2				
▼ SAN primary		vHBA-A	primary		
SAN Target primary			primary	0	50:06:01:64:08:E0:03:68
SAN Target secondary			secondary	0	50:06:01:6C:08:E0:03:68
▼ SAN secondary		vHBA-B	secondary		
SAN Target primary			primary	0	50:06:01:6D:08:E0:03:68
SAN Target secondary			secondary	0	50:06:01:65:08:E0:03:68

9. On the **Maintenance Policy** window, click **Next** to leave the setting at Default.
10. On the **Server Assignment** page, choose the **Server Pool** and **Qualification** and click **Next**.

Figure 235 Define Values on Server Assignment Page

**Create Service Profile Template**

[General](#)  
[Networking](#)  
[Storage](#)  
[vNIC/MHBA Placement](#)  
[Boot Order](#)  
[Maintenance Policy](#)  
**[Server Assignment](#)**  
[Policies](#)

Optionally specify a Server or Server Pool for this Service Profile.

**Server Assignment Method**  
 Identify the method to use to server assignment method used to assign servers to the Service Profile.

Server Assignment Method: Select server from pool

Power state to apply on assignment: ☐ down ☒ up

**Server Pool**  
[+ Create Server Pool](#) [+ Create Policy Qualification](#)

Identify the Server Pool that the server will be assigned from.

Server Pool: VSPEX-BO-Server-Pool (0/3)

Server Pool Instance: [org-root/compute-pool-VSPEX-BO-Server-Pool](#)

Qualification: Min-Memory

Qualification Instance: [org-root/blade-qualifier-Min-Memory](#)

Restrict migration of server: ☐

11. On the **Policies** window, keep all the default values and Click **Finish**.

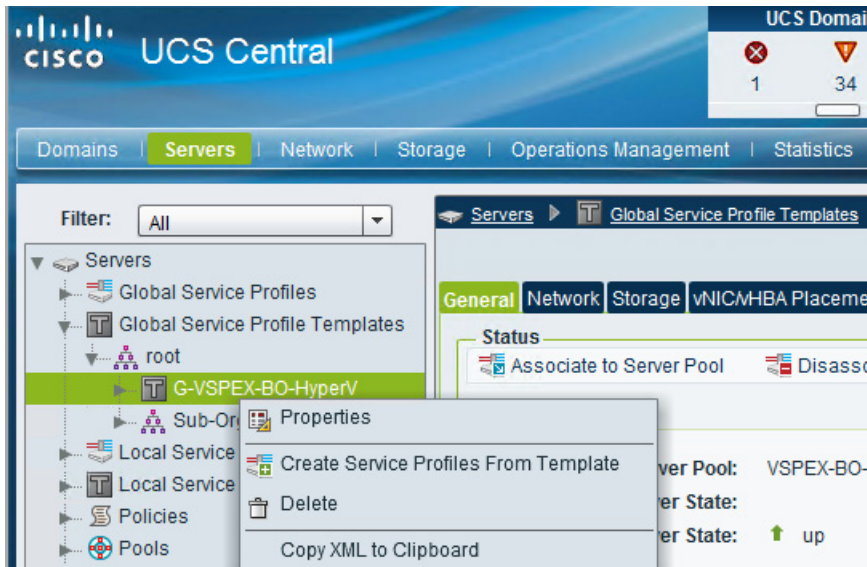
With the completion of global Service Profile Template creation, you can proceed to the next section to create service profiles

## Configuring Global Service Profile Instance

Global service profiles centralize the logical configuration deployed across the data center. This centralization enables the maintenance of all service profiles in the registered Cisco UCS domains from one central location, Cisco UCS Central.

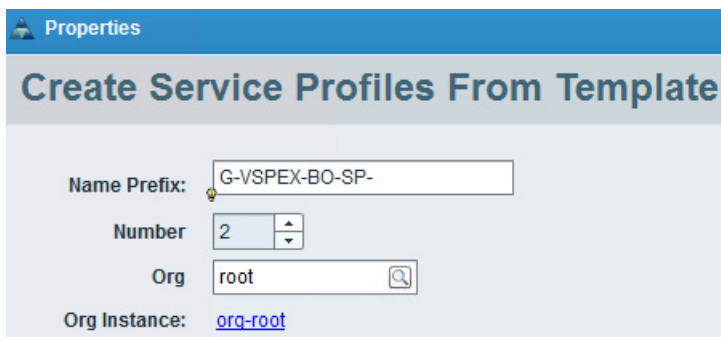
1. To create Global Service Profile for the VSPEX Branch Office servers, launch the **UCS Central** Web GUI. Click **Servers > Global Service Profile Templates > root** and choose **Create Service Profiles** from Template.

**Figure 236**      *Configuring Global Service Profile Instance*



2. Specify the naming prefix, number of service profile instances to be instantiated and click **Find** button next to Org and choose root. Click **OK**.

**Figure 237**      *Create Global Service Profile from Template*



3. After the successful creation of service profiles, navigate to **Servers > Global Service Profiles** to see them listed as shown in the below figure:

**Figure 238** *List of Created Global Service Profiles*

The screenshot shows the Cisco UCS Central web interface. At the top, there's a 'UCS Domains Fault Summary' bar with icons for errors (0), warnings (35), and critical alerts (7 and 3). Below this is a navigation menu with 'Servers' highlighted. The left sidebar shows a tree view under 'Servers' with 'Global Service Profiles' selected. The main content area, titled 'Global Service Profiles', contains a table with the following data:

Name	Org	Status	Associated Server	Domain
G-VSPEX-BO-SP-1	root	↑ ok	<a href="#">compute/sys-1008/chassis-1/blade-1</a>	VSPEX-FI
G-VSPEX-BO-SP-2	root	↑ ok	<a href="#">compute/sys-1008/chassis-1/blade-3</a>	VSPEX-FI

- Since the service profile template is assigned to a server pool, the service profiles instantiated from the template would be assigned to individual server resource from the server pool as far as they are available. You can choose a given service profile to see its overall status and association state (see Figure 239):

**Figure 239** *Overall Status of Created Service Profile*

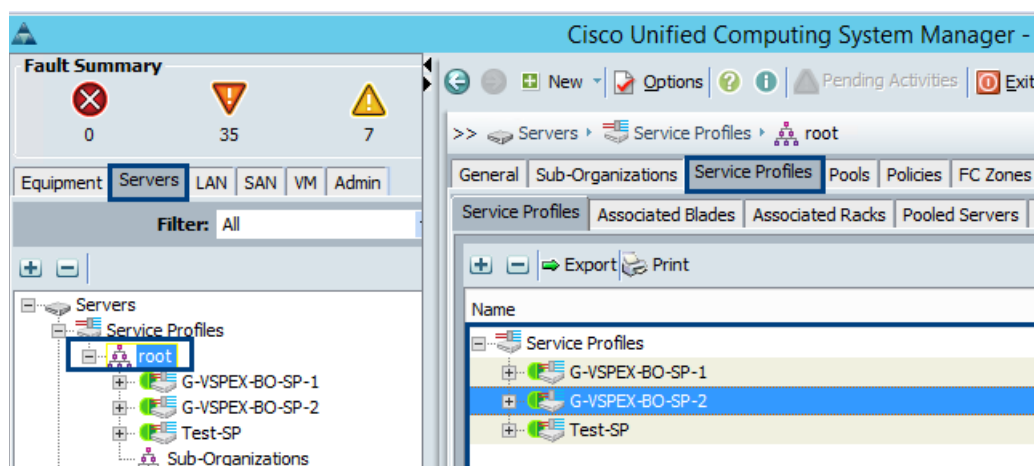
The screenshot shows the 'Properties' page for the service profile 'G-VSPEX-BO-SP-1'. The 'Status' tab is selected, showing the following information:

- Overall Status:** ↑ ok
- Association:**
  - Associate State: ↑ associated
  - Associated Server: [compute/sys-1008/chassis-1/blade-1](#)
  - UCS Domain: [VSPEX-FI](#)
- Assignment:**
  - Assigned State: ↑ assigned
  - Assigned Server: [compute/sys-1008/chassis-1/blade-1](#)
  - Server Pool:
  - Server Power State: ↑ on
  - Server Model: UCSB-B200-M3
  - Desired Power State: ↑ up
  - Restrict Migration: no
- Fault Summary:** 0 errors, 0 warnings, 0 critical alerts, 0 informational alerts.



5. Launch the **UCS Manager** GUI to see the global service profiles pushed to the UCS Manager.

**Figure 240** *Verify Global Service Profiles in UCS Manager GUI*



**Note**

Above procedure, presents a method for creating service profile for the VSPEX Branch Office servers using UCS Central management located in some primary DC Site.

In the event of deploying this solution with UCS Central Management, follow the steps 4 to 7 shown in the “VSPEX Configuration Guidelines” section:

- Prepare the EMC VNXe3200
- Installation of Windows Server 2012 R2 Datacenter
- Configure MPIO
- Create Hyper-V Cluster

## WAN Testing for UCS Central Management

The key benefit for using UCS Central Management is to provide centralized management for multiple UCS domains whether local or remote. Given UCS Central may reside in a data-center over distance, the test includes management of UCS Mini systems over the equivalent of an entry-level consumer grade DSL line – 1.5 Mbps, 500ms latency with better resiliency for temporary loss of connection between UCS Central and UCS Manager instances. While these enhancements are required for remote and branch offices, they are also useful for customers using UCS within a data center. We have used WAN emulator testing tool to simulate bandwidth, latency and packet loss measures defined above. During testing, we observed that UCS central management in primary data-center to be stable and responsive during configuration changes applied to the UCS Mini system in Branch Office site.

## Validating Cisco Branch Office Solution for EMC VSPEX Private Cloud with Microsoft Hyper-V Architectures

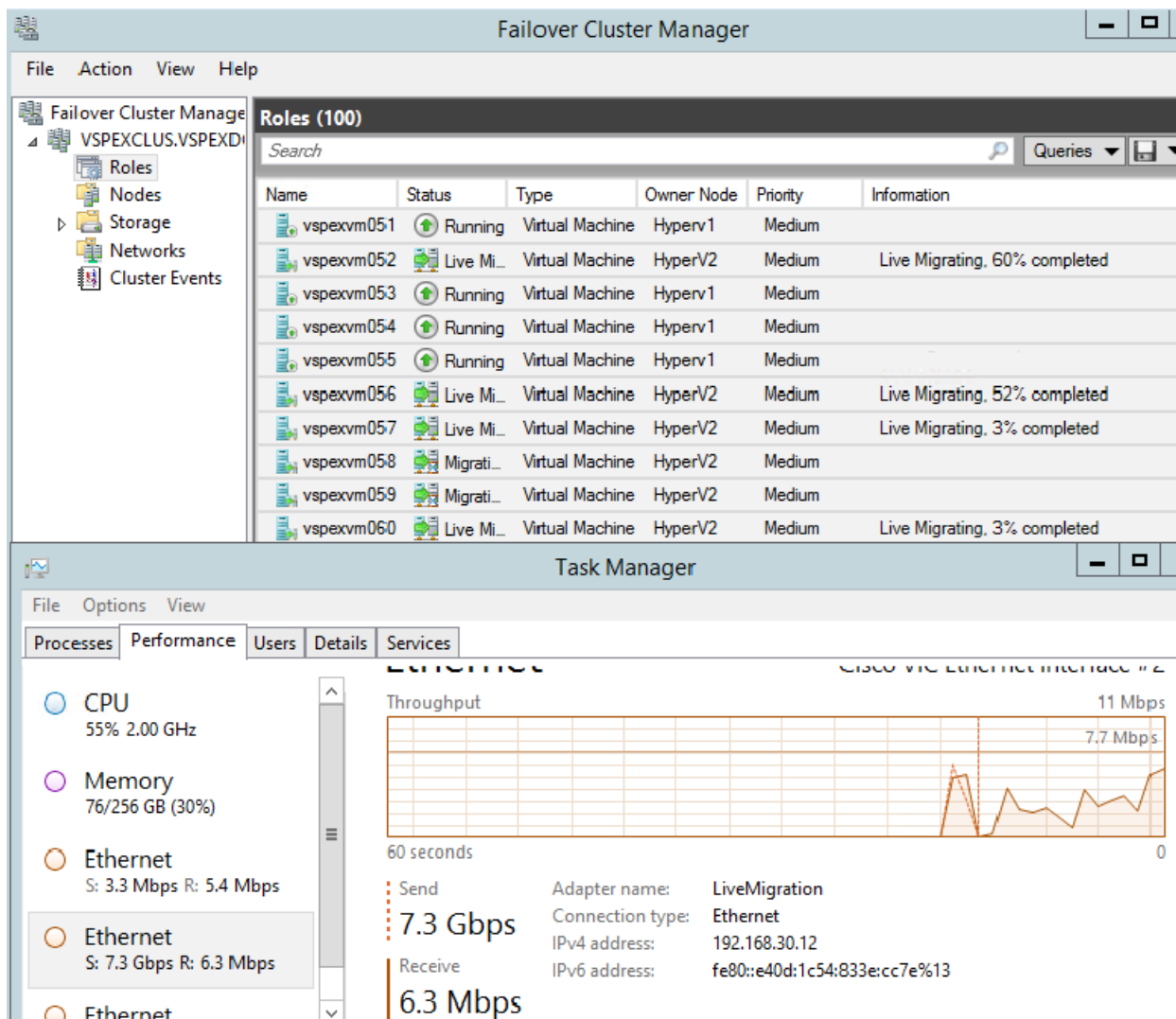
This section provides a list of items that should be reviewed once the solution has been configured. The goal of this section is to verify the configuration and functionality of specific aspects of the solution, and ensure that the configuration supports core availability requirements.

## Post Install Checklist

The following configuration items are critical to functionality of the solution, and should be verified prior to deployment into production.

1. Move cluster resources from one node to another node to check if they migrate successfully
2. Test Live Migration of VMs from one host to other using Failover Cluster Manager.

**Figure 241** Failover Cluster Manager Showing the VM Status



3. Restart hosts and check if VMs migrate to available hosts
4. Ping with 'do not fragment switch' to validate if jumbo frames are supported end-to-end on storage and live migration VLANs



**Figure 242**      *Validate Jumbo Frames*

```

PS C:\Users\administrator.VSPEXDOM> ping -f -l 8970 192.168.30.12

Pinging 192.168.30.12 with 8970 bytes of data:
Reply from 192.168.30.12: bytes=8970 time<1ms TTL=128
Reply from 192.168.30.12: bytes=8970 time<1ms TTL=128
Reply from 192.168.30.12: bytes=8970 time<1ms TTL=128
Reply from 192.168.30.12: bytes=8970 time<1ms TTL=128

Ping statistics for 192.168.30.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator.VSPEXDOM> ping -f -l 8970 192.168.40.12

Pinging 192.168.40.12 with 8970 bytes of data:
Reply from 192.168.40.12: bytes=8970 time<1ms TTL=128
Reply from 192.168.40.12: bytes=8970 time<1ms TTL=128
Reply from 192.168.40.12: bytes=8970 time<1ms TTL=128
Reply from 192.168.40.12: bytes=8970 time<1ms TTL=128

Ping statistics for 192.168.40.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator.VSPEXDOM>

```

## Verify Redundancy of Solution Components

Following redundancy checks were performed at the Cisco lab to verify solution robustness. A continuous ping from any host to VM and Hyper-V hosts should not show significant failures (one or two ping drops might be observed at times, such as FI reboot). Also, all the data-stores must be visible and accessible from all the hosts at all the time.

1. Administratively shutdown one of the Network uplink port from Fabric Interconnect A connected to upstream LAN (Lab Network). Make sure that connectivity is not affected. Upon administratively enabling the shutdown port, the traffic should be rebalanced. Repeat this step for the Network uplink port from Fabric Interconnect B and make sure the connectivity is not affected.
2. Administratively shutdown one of the two data links connected to the storage array from FI. Make sure that storage is still available from all the Hyper-V hosts. Upon administratively enabling the shutdown port, the traffic should be rebalanced. Repeat this step for each link connected to the Storage Processors one after another.
3. Reboot one of the Fabric Interconnects while storage and network access from the servers are going on. The switch reboot should not affect the operations of storage and network access from the VMs. Upon rebooting the FI, the network access load should be rebalanced across the two fabrics.
4. Reboot the active storage processor of the VNXe storage array and make sure that all the datastores are still accessible during and after the reboot of the storage processor.
5. Fully load all the virtual machines of the solution. Shutdown one of the Hyper-V nodes in the cluster. All the VMs running on that host should be migrated to other active hosts. No VM should lose any network or storage accessibility during or after the migration. This test assumes that enough RAM is available on active Hyper-V hosts to accommodate VMs from the host that was shutdown.

## Cisco Validation Test Profile

“Vdbench” testing tool (ver.5.0402) was used with Windows Server 2012 R2 to test scaling of the solution in Cisco labs. Following is the detail on the test profile used.

**Table 17** *VDbench Test Profile*

Profile Characteristic	Value
Number of virtual machines	100
Virtual machine OS	Windows Server 2012 R2
Processors per virtual machine	1
Number of virtual processors per physical CPU core	2
RAM per virtual machine	2 GB
Average storage available for each virtual machine	100 GB
Average IOPS per virtual machine	25 IOPS
Number of datastores to store VM disks	2 CVS
Disk and RAID type for datastores	RAID 5, 35 x 600 GB (10K RPM) SAS disks

## Bill of Materials

The following table provides the details of the components used in this solution:

**Table 18** *CVD Component Details*

Description	Part #
UCS Chassis 5108	UCS-5108-AC2
6324UP Fabric Interconnects	UCS-FI-M-6324
UCS B200 M3 Blade	UCSB-B200-M3
10 Gbps SFP+ multifiber mode	SFP-10G-SR
8 Gbps SFP+ fibre mode	DS-SFP-FC8G-SW
1000Base-T copper module	CIS-GLC-T-NP-OE

For more information about the part numbers and options available for customization, see Cisco UCS 6324 Fabric Interconnect datasheet:

<http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6300-series-fabric-interconnects/datasheet-c78-732207.html>

## Customer Configuration Data Sheet

Before you start the configuration, gather some customer-specific network and host configuration information. Tables 19 to 27 provide information on assembling the required network and host address, numbering, and naming information. This worksheet can also be used as a “leave behind” document for future reference.

The VNXe Series Configuration Worksheet should be cross-referenced to confirm customer information:

**Table 19**      *Common Server Information*

Server Name		Primary IP
	Domain Controller	
	DNS Primary	
	DNS Secondary	
	DHCP	
	NTP	
	SMTP	
	SNMP	

**Table 20**      *Hyper-V Server Information*

Server Name	Purpose	Mgmt IP	Live Migration IP	CSVIP	
	Hyper-V Host				
	Hyper-V Host				

**Table 21**      *Hyper-V Server WW/PN/WW/NN Information*

Device	Port	WWPN	WWNN
VSPEX01	Fabric A		
	Fabric B		
VSPEX02	Fabric A		
	Fabric B		
VSPEX03	Fabric A		
	Fabric B		

**Table 22**      *EMC Storage Array Information*

Array Name	
Admin account	
Management IP	

**Table 23** *EMC Storage Array WW/NN/WW/PN Information*

Port	WWNN	WWPN
SPA-Port 0		
SPA-Port 1		
SPA-Port 0		
SPA-Port 1		

**Table 24** *Network Infrastructure Information*

Name	Purpose	IP	Subnet Mask	Default Gateway
	Cisco UCS virtual IP address			
	Cisco UCS FI A address			
	Cisco UCS FI B address			
	Cisco UCS Central			

**Table 25** *VLAN Information*

Name	Purpose	VLAN ID	Allowed Solution
Mgmt	Infrastructure management		
LiveMigration	Live Migration		
CSV	Cluster Shared Volume		
VMAccess	Virtual Machine access		

**Table 26** *VSAN Information*

Name Network	VSAN ID	ECoe VLAN ID
Storage Access		

**Table 27**      *Service Accounts*

Account		Password (option, secure)
Admin	UCS Manager administrator	
Admin	UCS Central	
	Microsoft Windows Server administrator	
	Microsoft Windows Server AD domain administrator	
Admin	EMC VNXe array administrator	

## Conclusion

The Cisco Branch Office solution for EMC VSPEX Private Cloud uses new offerings such as the Cisco UCS Mini and EMC VNXe 3200 for solutions that are ideal for mid-size businesses and enterprises that require central management of IT infrastructure for remote and branch offices. Additional tools such as UCS Central provide the means to address business and infrastructure requirements from a central location. These functional requirements promote uniqueness and innovation in integrated computing stack, augmenting their original design to support essential services such as standards based centralized management of remote instances.

## References

Cisco UCS:

[http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns944/unified\\_computing.html](http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/ns944/unified_computing.html)

Cisco UCS Mini Firmware Management:

[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/sw/firmware-mgmt/gui/3-0/b\\_GUI\\_Firmware\\_Management\\_30/b\\_GUI\\_Firmware\\_Management\\_30\\_chapter\\_01.html](http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/firmware-mgmt/gui/3-0/b_GUI_Firmware_Management_30/b_GUI_Firmware_Management_30_chapter_01.html)

UCS Central Software and Installation Guide:

<http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-central-software/tsd-products-support-series-home.html>

UCS Central Best Practice Guide:

<https://communities.cisco.com/docs/DOC-35264>

Windows Server 2012 R2 and Windows Server 2012 Technical Library

<http://technet.microsoft.com/library/hh801901.aspx>

EMC VNXe32xx Series Resources:

<http://www.emc.com/storage/vnx/vnx-series.htm#!resources>

EMC Support: (requires user registration)

<http://support.emc.com>