

Cisco UCS Mini Branch Office Solution for EMC VSPEX

With EMC VNXe3200 and VMware vSphere 5.5 for up to 100 Virtual Machines Last Updated: September 10, 2014



Building Architectures to Solve Business Problems

· I | I · I | I · CISCO ..



About the Authors

Vijay Durairaj, Technical Marketing Engineer, Cisco Systems

Vijay Durairaj is a Technical Marketing Engineer with Cisco UCS Solutions and Performance group has over 10+ years of experience in UCS, network, storage and server virtualization design. Vijay has worked on performance and benchmarking on Cisco UCS servers and has delivered benchmark results on SPEC CPU2006 and SPECj ENT 2010. Vijay holds certification in VMware Certified Professional and Cisco Unified Computing systems Design specialist.





Mehul Bhatt, Virtualization Architect, Cisco Systems

Mehul Bhatt is a Virtualization Architect with Server Access virtualization Business Unit (SAV) with over 13 years of Experience in virtually all layers of computer networking. His focus area includes Unified Compute Systems, network and server virtualization design. Prior to joining Cisco Technical Marketing team, Mehul was Technical Lead at Cisco, Nuova systems and Bluecoat systems. Mehul holds a Master's degree in computer systems engineering and holds various Cisco career certifications.

Acknowledgment

For their support and contribution to the design, validation, and creation of the Cisco Validated Design, we would like to thank:

1

- Shiva Shastri (Cisco)
- Bathu Krishnan (Cisco)
- Kevin Phillips (EMC)

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 (COLLEC-TIVELY, "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 SUP-PLIERS 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.

© 2014 Cisco Systems, Inc. All rights reserved.



cisco.

Cisco UCS Mini Branch Office Solution for EMC VSPEX

Executive Summary

Cisco solution on EMC VSPEX is a pre-validated and modular architecture built with proven best of-breed technologies. Because EMC VSPEX solutions are rigorously tested, they drastically reduce 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) focuses on a VSPEX solution consisting of new components from Cisco such as the UCS Mini compute chassis and EMC VNXe3200 storage array with VMware vSphere 5.5 catered to the small to medium business (SMB) segment with an initial need of about 100 Virtual Machines. A typical use case would be a branch office/remote office 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 VMware platform 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.



Target Audience

The reader of this document is expected to have the necessary training and background to install and configure VMware vSphere, 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 with VMware 5.5 as the hypervisor. Centralized management of this branch office solution through UCS Central located in the data center is also highlighted. The level of details covered allows for confirmation of the correct functioning of the basic components in the solution. The solution documented is expected to cover a VMware architecture for small-to medium-sized businesses with a need for about 100 VMs. This document show cases the solution with EMC VNXe 3200 series storage array using NFS for data storage and Fiber Channel (FC) for OS booting 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:

- Provide an end-to-end virtualization solution to take full advantage of unified infrastructure components.
- Show implementation progression of VMware vCenter 5.5 design and results.
- · Provide a reliable, flexible and scalable reference design
- It is beyond the scope of this document to consider performance related details pertaining to the solution.

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 due to converged stacks such as the VSPEX are further enhanced when integrated with centralized provisioning and management.

Solution Overview

Cisco UCS Mini Branch solution for EMC VSPEX VMware architecture

This solution provides an end-to-end architecture with Cisco, EMC, VMware, 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 Implementation)
- EMC VNXe3200
- VMware vCenter 5.5
- Microsoft SQL database
- VMware DRS
- VMware HA

The solution is designed to host scalable, mixed application workloads of up to 100 reference virtual machines.

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 (NFS 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.

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 Figure 1. The 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) 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 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[1] 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 the fabric 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.



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.

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.



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.

- 1. 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.
- 2. 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 or rack server deployment.
- **3.** 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 extending easily while keeping the existing external connectivity to LAN, SAN and management networks.
- 4. 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 show cases the policy based resource classification of UCSM.

- 5. 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.
- 6. 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 VMware vCloud director, Microsoft system center, and Citrix Cloud Platform.
- 7. 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.
- 8. Loose referential integrity: In UCSM, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each-other. This provides great flexibilities where different experts from different domains, such as network, storage, security, server and virtualization work together to accomplish a complex task.
- **9.** 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 specific name is found in the hierarchy till root organization, then special policy named "default" is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibilities to owners of different organizations.
- **10.** 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.
- 11. Built-in multi-tenancy support: Combination of policies, pools and templates, loose referential integrity, policy resolution in organization hierarchy and service profile based approach to compute resources makes UCSM inherently friendly to multi-tenant environment typically observed in private and public clouds.
- 12. 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.
- **13.** 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.

VMware vSphere 5.5

VMware vSphere 5.5 is a next-generation virtualization solution from VMware which builds upon ESXi 5.1 and provides greater levels of scalability, security, and availability to virtualized environments. vSphere 5.5 offers improvements in performance and utilization of CPU, memory, and I/O. It also offers

users the option to assign up to thirty two virtual CPU to a virtual machine—giving system administrators more flexibility in their virtual server farms as processor-intensive workloads continue to increase.

The vSphere 5.5 provides the VMware vCenter Server that allows system administrators to manage their ESXi hosts and virtual machines on a centralized management platform. With the Cisco Fabric Interconnects Switch integrated into the vCenter Server, deploying and administering virtual machines is similar to deploying and administering physical servers. Network administrators can continue to own the responsibility for configuring and monitoring network resources for virtualized servers as they did with physical servers. System administrators can continue to "plug-in" their virtual machines into network ports that have Layer 2 configurations, port access and security policies, monitoring features, etc., that have been pre-defined by the network administrators; in the same way they would plug in their physical servers to a previously-configured access switch. In this virtualized environment, the system administrator has the added benefit of the network port configuration/policies moving with the virtual machine if it is ever migrated to different server hardware.

VMware vSphere 5.5 includes an expansive list of new and improved features that enhance performance, reliability, availability, and recovery of virtualized environments. Of those features, several have significant impacts upon VSPEX Private Cloud deployments, including:

- Expanded maximum memory and CPU limits for ESX hosts. Logical and virtual CPU counts have doubled in this version, as have non-uniform memory access (NUMA) node counts and maximum memory. This means host servers can support larger workloads.
- 62TB Virtual Machine Disk (VMDK) file support including Raw Device Mapping (RDM). Datastores can hold more data from more virtual machines, which simplifies storage management and leverages larger capacity NL-SAS drives.
- Enhanced Single-Root Input/Output (I/O) Virtualization (SR-IOV) support that simplifies configuration via workflows, and surfaces more properties into the virtual functions.
- 16 Gb end-to-end support for FC environments.
- Enhanced Link Aggregation Control Protocal (LACP) functions offering additional hash algorithms and up to 64 Link Aggregation Groups (LAGs).
- vSphere Data Protection (VDP), which can now replicate backup data directly to EMC avamar.
- Virtual Machine File System (VMFS) heap improvements, which reduce memory requirements while allowing access to the full 64TB VMFS address space.

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.

I

Table 1 shows the customer benefits that are provided by the VNXe series.

Table 1 VNXe Customer Benefits

Features	Benefits
Next-generation unified storage, optimized for virtualization applications	Tight integration with VMWare 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 and SAN 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 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 domains, where Cisco UCS Manager puts the policies into effect. Cisco UCS Central software manages multiple, globally distributed Cisco UCS domains with thousands of servers 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.



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 why that is inconsistent with standards, and 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 similar 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).

I



UCS-Mini Management with UCS Central Policy Based Management



Architectural overview

ſ

This CVD focuses on the architecture for EMC VSPEX for VMware private cloud, targeted for mid-market segment, using EMC VNXe storage arrays. This architecture uses UCS 3.0(1c) with combined Cisco UCS B200M3 servers with VNXe3200 directly attached to UCS 6324 fabric interconnect. VMware vSphere 5.5 is used as server virtualization architecture



Illustrates the Architectural Overview of VSPEX Remote Office and Branch Office Solution

Table 2 lists the various hardware and software components which occupies different tiers of the Cisco Branch office solution for EMC VSPEX VMware architectures under test.

1

Vendor	Name	Version	Description
Cisco	Cisco UCS Manager	3.0(1c)	UCS Manager
Cisco	Cisco UCS Fabric Interconnect 6324UP	5.0(3)N2(3.01c)	UCS Fabric Interconnects
Cisco	Cisco UCS 5108 AC2 Chassis	N/A	UCS Blade server chassis
Cisco	Cisco UCS B200 M3 Server	2.2.1a	Cisco B200 M3 Blade Servers
Cisco	Cisco UCS VIC 1240	3.0(1c)	Cisco VIC 1240 adapters
EMC	EMC VNXe 3200		VNXe Storage
VMware	VMware ESXi 5.5	5.5 build XXXXX	Hypervisor
VMware	VMware vCenter Server	5.5 build XXXXX	VMware Management
Microsoft	Microsoft Windows Server 2012 R2	2012 R2 SP1 data center	Operating System to host vCenter server & Operating System for VSPEX Virtual Machine
Microsoft	Microsoft SQL Server 2008 R2	2008 R2 Enterprise	SQL Database Server Enterprise Edition for vCenter Server

Table 2 Hardware and Software Components of the VMware Architecture

Table 3 outlines the Cisco UCS B200 M3 Server configuration of this architecture. Table 3 shows the configuration per server basis.

Table 3	Cisco UCS B200 M3 Server Configuration L	<i>etails</i>
---------	--	---------------

I

Components	Capacity
Memory (RAM)	256 GB (16X16 GB DIMM)
Processor	2XIntel® Xeon® E5-2640 v2 CPUs, 2GHz, 8cores, 16 thread
Local Storage	Cisco UCS RAID SAS 2008M-8i Mezzanine Card

This SMB architecture contains the infrastructure server on the same chassis in a vSphere Environment manages the virtual machine hosting vCenter server and Windows Active Directory / DNS server are present.

• This design does not dictate or require any specific layout of infrastructure network. The vCenter server, Microsoft AD server and Microsoft SQL server are hosted on infrastructure Blade Server. However, the design does require that certain VLANs are accessible from both the infrastructure blade server and the VSPEX servers.

• ESXi 5.5 is used as hypervisor operating system on each server and is installed on SAN LUNs in both architectures. All the VSPEX Virtual Machines storage is accessed thru NFS protocols. Typical load is 32 reference virtual machines per server.

Memory Configuration Guidelines

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

ESXi/ESXi Memory Management Concepts

vSphere virtualizes guest physical memory by adding an extra level of address translation. Shadow page tables make it possible to provide this additional translation with little or no overhead. Managing memory in the hypervisor enables the following:

- Memory sharing across virtual machines that have similar data (that is, same guest operating systems).
- Memory overcommitment, which means allocating more memory to virtual machines than is
 physically available on the ESX/ESXi host.
- A memory balloon technique whereby virtual machines that do not need all the memory they were
 allocated will give memory to virtual machines that require additional allocated memory.

For more information about vSphere memory management concepts, see the VMware vSphere Resource Management Guide at:

http://www.vmware.com/files/pdf/perf-vsphere-memory_management.pdf

Virtual Machine Memory Concepts

Figure 8 illustrates the use of memory settings parameters in the virtual machine.

Figure 8

```
8 Virtual Machine Memory Settings
```



The vSphere memory settings for a virtual machine include the following parameters:

- Configured memory Memory size of virtual machine assigned at creation.
- Touched memory Memory actually used by the virtual machine. vSphere allocates only guest operating system memory on demand.
- Swappable Virtual machine memory that can be reclaimed by the balloon driver or by vSphere swapping. Ballooning occurs before vSphere swapping. If this memory is in use by the virtual machine (that is, touched and in use), the balloon driver causes the guest operating system to swap. Also, this value is the size of the per-virtual machine swap file that is created on the VMware Virtual

Machine File System (VMFS) file system (VSWP file). If the balloon driver is unable to reclaim memory quickly enough, or is disabled or not installed, vSphere forcibly reclaims memory from the virtual machine using the VMkernel swap file.

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:

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

Table 4Virtual Memory Details

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 virtual machine devices, depending on applications and internal data structures. The amount of overhead required depends on the number of vCPUs, configured memory, and whether the guest operating system is 32-bit or 64-bit. As an example, a running virtual machine with one virtual CPU and two gigabytes of memory may consume about 100 megabytes of memory overhead, where a virtual machine with two virtual CPUs and 32 gigabytes of memory may consume approximately 500 megabytes of memory overhead. This memory overhead is in addition to the memory allocated to the virtual machine and must be available on the ESXi 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. In most cases, hot-adding of memory is supported and can provide instant access to the additional memory if needed.
- Intelligently overcommit Memory management features in vSphere allow for overcommitment of physical resources without severely impacting performance. Many workloads can participate in this type of resource sharing while continuing to provide the responsiveness users require of the application. When looking to scale beyond the underlying physical resources, consider the following:
- Establish a baseline before overcommitting Note the performance characteristics of the
 application before and after. Some applications are consistent in how they utilize resources and may
 not perform as expected when vSphere memory management techniques take control. Others, such
 as Web servers, have periods where resources can be reclaimed and are perfect candidates for higher
 levels of consolidation.

- Use the default balloon driver settings The balloon driver is installed as part of the VMware Tools suite and is used by ESXi/ESXi if physical memory comes under contention. Performance tests show that the balloon driver allows ESXi/ESXi to reclaim memory, if required, with little to no impact to performance. Disabling the balloon driver forces ESXi/ESXi to use host-swapping to make up for the lack of available physical memory which adversely affects performance.
- Set a memory reservation for virtual machines that require dedicated resources Virtual machines running Search or SQL services consume more memory resources than other application and Web front-end virtual machines. In these cases, memory reservations can guarantee that those services have the resources they require while still allowing high consolidation of other virtual machines.

Storage Guidelines

VSPEX architecture for VMware virtual machines for mid-market segment uses FC for boot or NFS to store Virtual machine data in a VNXe Storage Array. vSphere provides many features that take advantage of EMC storage technologies such as auto discovery of storage resources and ESXi hosts in vCenter and VNXe respectively. Features such as VMware vMotion, VMware HA, and VMware Distributed Resource Scheduler (DRS) use these storage technologies to provide high availability, resource balancing, and uninterrupted workload migration.

Storage Protocol Capabilities

VMware vSphere provides vSphere and storage administrators with the flexibility to use the storage protocol that meets the requirements of the business. This can be a single protocol datacenter wide, such as NFS, or multiple protocols for tiered scenarios such as using Fibre Channel for high-throughput storage pools and NFS for high-capacity storage pools. For more information, see the VMware whitepaper Comparison of Storage Protocol Performance in VMware vSphere 5 at:

http://www.vmware.com/files/pdf/perf_vsphere_storage_protocols.pdf

Storage Best Practices

The following are vSphere storage best practices:

- Host multi-pathing Having a redundant set of paths to the storage area network is critical to protecting the availability of your environment. This redundancy is in the form of dual adapters connected to separate fabric switches.
- Partition alignment Partition misalignment can lead to severe performance degradation due to I/O operations having to cross track boundaries. Partition alignment is important both at the VMFS level as well as within the guest operating system. Use the vSphere Client when creating VMFS datastores to be sure they are created aligned. When formatting volumes within the guest, Windows 2008 aligns NTFS partitions on a 1024KB offset by default.
- Use shared storage In a vSphere environment, many of the features that provide the flexibility in
 management and operational agility come from the use of shared storage. Features such as VMware
 HA, DRS, and vMotion take advantage of the ability to migrate workloads from one host to another
 host while reducing or eliminating the downtime required to do so.
- Calculate your total virtual machine size requirements Each virtual machine requires more space than that used by its virtual disks. Consider a virtual machine with a 20GB OS virtual disk and 16GB of memory allocated. This virtual machine will require 20GB for the virtual disk, 16GB for the virtual machine swap file (size of allocated memory), and 100MB for log files (total virtual disk size + configured memory + 100MB) or 36.1GB total.

Understand I/O Requirements – Under-provisioned storage can significantly slow responsiveness and performance for applications. In a multitier 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 VMFS volume. Over-subscription of the I/O resources can go unnoticed at first and slowly begin to degrade performance if not monitored proactively.

Virtual Networking

Each B200 M3 blade server has one physical Cisco VIC adapter carved out with six 10 GE vNIC interfaces evenly distributed to fabric A and fabric B for high availability and also presents two virtual Host Bus Adapters (vHBAs) for the booting ESXi from SAN, one vHBA per fabric path. The MAC addresses to these vNICs are assigned using MAC address pool defined on the UCSM. The vNICs are used in active-active configuration for load-balancing and high-availability. Following are vSphere networking best practices implemented in this architecture:

- "Separate virtual machine and infrastructure traffic Keep virtual machine and VMkernel or service console traffic separate." This is achieved by having two vSwitches per hypervisor:
 - vSwitch (default) used for management and vMotion traffic
 - vSwitch1 used for Virtual Machine data traffic
- "Use NIC Teaming Use two physical NICs per vSwitch, and if possible, uplink the physical NICs to separate physical switches." This is achieved by using two vNICs per vSwitch, each going to different Fabric Interconnects. Teaming provides redundancy against NIC failure and FI fabric failures.
- "Jumbo MTU for vMotion and Storage traffic" this best practice is implemented in the architecture by configuring jumbo MTU end-to-end.

VSPEX VMware Storage Virtualization

Storage Layout

The architecture diagram in this section shows the physical disk layout. Disk provisioning on the VNXe series 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 illustrates storage architecture for 100 virtual machines on VNXe3200 for NFS based storage architecture:



Figure 9 Storage layout for up to 100 Reference VMs on VNXe3200

The VNX family 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.

Storage Virtualization

VMFS is a cluster file system that provides storage virtualization optimized for virtual machines. Each virtual machine is encapsulated in a small set of files and VMFS is the default storage system for these files on physical SCSI disks and partitions.

It is preferable to deploy virtual machine files on shared storage to take advantage of VMware VMotion, VMware High AvailabilityTM (HA), and VMware Distributed Resource SchedulerTM (DRS). This is considered a best practice for mission-critical deployments, which are often installed on third-party, shared storage management solutions.

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 ESXi host uses following identities in this architecture:
 - Host UUID
 - Mac Addresses: one per 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 procured within minutes:

- Put the faulty server in maintenance mode using vCenter. 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 ESXi 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 ESXi server in vCenter.

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. We would demonstrate that blade servers can be added in the same server pool.

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
- VNICs on fabric A and fabric B are used for NFS based access high-availability



NFS would require external LAN switch connectivity from Fabric A & Fabric B in case of link failure from FI to storage server.

Storage is made highly available by deploying following practices:

- FC access is for booting each of the ESXi hypervisor images.
- VSPEX VMs are deployed on the NFS Datastore.
- VNXe storage arrays provide two Storage Processors (SPs): SP-A and SP-B for both FC(Block) & NFS (File).



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

Architecture Design Layout for Optional Topology:

As described in Technology overview section, the UCS Mini chassis and EMC VNXe3200 supports Unified fabric design and provides support for both NAS (NFS, CIFS Protocols) and SAN (FC, iSCSI protocols) based Storage Architecture.

In this solution, we have shown only the NFS variant Architecture, which show cases FC for ESXi Hypervisor boot and NFS for Virtual Machine Datastore.

Due to UCS Mini chassis port limitations and EMC VNXe3200 storage limitations, we cannot showcase all the NAS and SAN protocols in a single architecture design.

In following sections, there are two other possible topologies using the same components:



Figure 11 Architecture Design Logical Layout for FC Topology

Note

Γ

FC only topology option will only support VMFS but free a FI port for possible C-Series expansion.



Figure 12 Architecture Design Logical Layout for iSCSI (Ethernet only) Topology



Ethernet only iSCSI topology option will also support VMFS but free a FI port for possible C-series expansion. Also, the failover is not dependent on the upstream LAN switch above but the multi-pathing capabilities of the host OS.

Jumbo MTU:

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

- NFS Storage access
- vMotion 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:

- 1. Ethernet ports on VNX Storage Processors
- 2. System QoS classes in UCS Manager
- 3. vNICS in service profiles
- 4. VM-Kernel ports used for vMotion and storage access on the ESXi hosts

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

Sizing Guideline

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, we have defined a representative customer reference workload. By comparing your actual customer usage to this reference workload, you 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 5 Virtual Machine Characteristics

Characteristics	Value
Virtual machine OS	Microsoft Windows Server 2012
Virtual processor per virtual machine (vCPU)	1
RAM per virtual machine	2GB
Available storage capacity per virtual machine	100GB
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.

VSPEX Configuration Guidelines

The configuration for Cisco solution for EMC VSPEX VMware architectures is divided in to following steps:

- 1. Pre-deployment tasks
- 2. Connect network cables
- 3. Prepare UCS FIs and configure UCSM
- 4. Configure data stores for ESXi images
- 5. Install ESXi servers and vCenter infrastructure
- 6. Install and configure vCenter server
- 7. Configure storage for VM data stores, install and instantiate VMware VMs from vCenter
- 8. Test the installation

Next pages go into details of each section mentioned above.

Pre-deployment tasks

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 hostnames, 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 related documents listed in the Preface. 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 6 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.

I

Requirements	Description	Reference
Hardware	Cisco UCS Mini chassis with 6324 Fabric Interconnect for network and compute infrastructure	See the corresponding product documentation
	Cisco UCS B200 M3 servers to host virtual machines	
	VMware vSphere [™] 5.5 server to host virtual infrastructure servers	
	Note This requirement may be covered in the existing infrastructure	
	EMC VNXe storage: Multiprotocol storage array with the required disk layout as per architecture requirements	
Software	VMware ESXi [™] 5.5 installation media	See the corresponding product documentation
	VMware vCenter Server 5.5 installation media	
	Microsoft Windows Server 2102 installation media (suggested OS for VMware vCenter)	
License	Microsoft SQL Server 2008 R2 SP1	Consult your corresponding vendor for the license
	Note This requirement may be covered in the existing infrastructure	
	VMware vCenter 5.5 license key	-
	VMware ESXi 5.5 license keys	-
	Microsoft SQL Server 2008 R2 license key	
	Note This requirement may be covered in the existing infrastructure	

Table 6 Hardware and Software Requirements

Customer Configuration Data

ſ

To reduce the onsite time, information such as IP addresses and hostnames should be assembled as part of the planning process. "Customer Configuration Data Sheet" section on page 174 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, complete the "Customer Configuration Data Sheet" section on page 174, 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 VMware architecture covered in this document.



1

Figure 13 Cabling Diagram for UCS Mini and VNXe Array System - Port Description



Figure 14 Cabling Diagram for UCS Mini and VNXe Array Systems - Port Number Details

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

Follow the step-by-step guide to configure UCSM tasks mentioned above.

Initial Configuration of UCS FIs

I

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 strips. 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 as shown in the below image. Save the configuration, which would eventually lead to UCSM CLI login prompt.

```
- 0 -X
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 MgmtO 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 MgmtO IP Address= 10.29.180.201
    Physical Switch MgmtO 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):
```

2. Now disconnect the RJ-45 serial console from the FI that you just configured and attach it to the other FI. Other FI would detect that its peer has been configured, and would prompt you to just join the cluster. The only information you need to provide is the FI specific management IP address, subnet mask and default gateway, as shown in the image below. Save the configuration.



3. Once initial configurations on both FIs are completed, you can disconnect the serial console cable. Now, UCSM would 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 see both FI A and FI B in "Up" state as shown in the figure below.



Chassis and Server Discovery on UCS Manager

1. After the FI management IP configuration, launch the UCS Manager via web browser using the Virtual IP. You will see the Chassis discovered Automatically under Equipment tab and it is showing as "operable".

Figure 15 Chassis Dis	covery Policy
0 4 7 2	>> 🚆 Equipment + 🥡 Chassis + 🗊 Chassis 1 (primary)
Equipment Servers LAN SAN VM Admin Filter: All	Installed Firmware SEL Logs Power Control Monitor Connectivity Policy Events FSM Faults Statistics General Servers Service Profiles FI-IO Modules Fans PSUs Hybrid
Equipment Chassis Chassis	Fault Summary Status Overall Status: Operable Status Overall Status: Operable Status Actions Action
	Summerssion Task Promerties

1

Also You will see 4 blades discovered automatically under **Equipment** tab with over-all status as **Unassociated** and availability state as **Available**, and discovery state as **Complete** as shown below:

On equipment tab, under **Equipment** > **Chassis** > **Chassis** < **id** > > **Servers** as shown below:


Upstream / global network configuration

I

This subsection includes a few upstream/ global network configuration listed below:

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

Follow these steps for network configuration:

1. From the **Equipment** tab, select and right-click on **Fabric Interconnect A**, and click **Set FC Switching Mode**.



Figure 17 Setting Cisco UCS FI to FC Switching Mode

- 2. You would see a warning message that Fabric Interconnects would be restarted as a result of this action. Click **Yes**. Both the FIs would reboot (first the secondary FI and then the primary FI). This action is traffic disruptive, so make sure that you perform this operation during maintenance window, if you are working on a production environment.
- 3. From the LAN tab, expand LAN > LAN Cloud, and right-click on VLANs, and click Create VLANs.

Figure 18	Creating	g VLANs					
V	V		<u> </u>	Ŀ.	I	1	1
0	3	7	2		>> 📃 LAN 🕴 🙆 Appliances 🛀	VLANs	
Equipment S	ervers LAN	SAN VM	Admin	lh	VLANs		
Filter:	All		-		🔍 Filter 🖨 Export 😸 Print		
m o L				Ш	Name		ID
				Ш	VLAN default (1)	1	
	N Cloud opliances Fabric A Fabric B VLAN					-	
	- V	Show Navio	jator				
⊡ ⊒ Inl	ternal I Intern	Create VLA	Ns				
	Internal Fat Threshold P	oric B olicies					

4. Give name to the VLAN and assign ID. Keep the default option **Common/Global** radio button selected.

Figure 19 Creating VLANs for Manag

Γ

🚔 Create ¥LANs
Create VLANs
VLAN Name/Prefix: vSphereMgmt
Multicast Policy Name: <not set=""> Create Multicast Policy</not>
Common/Global C Fabric A C Fabric B C Both Fabrics Configured Differently
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")
VLAN IDs: 11
Sharing Type: 💿 None 🔘 Primary 🔿 Isolated

- **5.** Click **OK** and deploy vSphereMgmt VLAN. Repeat these steps to create VLANs for Storage VLAN20, VM-Data VLAN30 and vMotion VLAN40.
- 6. Click the LAN tab, expand LAN > Appliance Cloud, and right-click on VLANs, and click Create VLANs.

1

Figure 20	Creatir	ıg VLANs				
0	3	7	2		>> 🗐 LAN + 🙆 Appliances + 🗄	VLANs
Equipment S Filter:	iervers LAN All	DSAN VM	Admin		VLANs	
• • I				ш	Name	IC
	N Cloud pliances Fabric A Fabric B VI ANC ter Sho Crea	w Navigator ate VLANs olicies			VLAN default (1)	1

7. Give name to the VLAN and assign ID. Keep the default option **Common/Global** radio button selected.

Figure 21	Creating VLANs for Storage	
📥 Create VLA	ANs	×
Create '	VLANs	Ø
VLAN Name/P	Prefix: Storage Common/Global O Fabric A O Fabric B O Both Fabrics Configured Differently	
You are creat	ating global VLANs that map to the same VLAN IDs in all available fabrics.	
VLAN IDs:	ange of VLANIDs (e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")	
	Check Overlap OK	Cancel

I

Γ

8. Click the SAN tab, and expand Storage Cloud, and right-click on VSANs. Click Create Storage VSAN.



9. Give a name to the VSAN, enable FC zoning and provide VSAN ID and its corresponding FCoE VLAN ID. FCoE VLAN ID should not have conflict with any of the VLANs configured earlier.

1

Figure 23 Creating Storage VSAN			
A Create Storage VSAN			×
Create Storage VSAN			0
Name: Storage			
FC Zoning Settings			
FC Zoning: O Disabled O Enabled			
Do NOT enable zoning for this VSAN if the fa upstream switch that has zoning enabled on	abric interconnect is connected to an the same VSAN.		
Ocommon/Global ○ Fabric A ○ Fabric B	 Both Fabrics Configured Differently 	Y	
You are creating a global VSAN that maps to the same VSAN ID in all available fabrics.	A VLAN can be used mapped to this VSAN	to carry FCoE traffic ar I.	nd can be
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID th	at maps to this VSAN.	
VSAN ID: 10	FCoE VLAN: 10		
		0	K Cancel

10. The new Cisco UCS 6324UP Fabric Interconnects have 4 Universal Ports. By default, 4 of the physical ports on the FI are unconfigured, but can be converted to Fibre-Channel ports, Ethernet ports or Appliance Ports. For this design we chose Port 4 as the Network Uplink Port (for LAN connection), Port 2 and Port 3 as Appliance Ports for Direct connect Storage to VNXe Array, and configured Port 1 as an FC storage port for SAN Booting the ESXi5.5 from VNXe array.



I

- **Note** On the 6324 Fabric Interconnect Converting the Unified Port into FC ports is supported only starting from Port 1, not from Port 4.(Configuring the FC storage port on Fabric Interconnect is shown in step15).
- 11. As shown below, Click Fabric Interconnect B > Port 4 and Click Configure as Uplink Port and then click Yes to confirm. Repeat the same step on Fabric Interconnect A.



12. Click Fabric Interconnect B > Port 2 and click Configure as Appliance Port and then click Yes.



Select Priority as Platinum for Jumbo MTU 9000 and Speed as 1 Gbps. Click Access and then select VLAN as Storage. (In this solution, we use 1 Gbps Ethernet for NFS Storage connectivity) and click OK to confirm the selection.

Figure 26Appliance Port Configuration Window	
📥 Configure as Appliance Port	×
Configure as Appliance Port	0
j	
Priority: Platinum	
Pin Group: <not set=""></not>	Create LAN Pin Group
Elow Control Policy: default	
Advis Speed(abox 1 Gbrs C 10 Gbrs C 20 Gbrs C 40 Gbrs	
VLANs	
Port Mode: O Trunl O Access	
Select VLAN: Storage	
Create VLAN	
Ethernet Target Endpoint	
Name:	
MAC Address:	
	OK Cancel

- 14. Repeat step 12 and 13 to configure Fabric Interconnect A Ethernet Port 2 and Port3 as Appliance Ports.
- 15. We need FC connectivity to EMC VNXe storage array at least for SAN boot. For configuring FC connectivity, click Equipment tab, expand Fabric Interconnects and click Fabric Interconnect A > Configure Unified Ports. Click Yes in the warning message window.

ſ



- **16.** Click **Configure Unified Ports** to open the wizard. This will pop-up a warning message about Fabric Interconnect reboot on port changes. Click **Yes** to continue.
- 17. Move the slider bar at the top to select Port1. Make sure that Port 1 is showing FC Uplink. Then, right-click Port 1 and click **Configure as FC Storage Port** and then click **Finish**. Click **OK** to reboot the FI.



- **18.** Once the Fabric Interconnect A is rebooted, repeat steps 15, 16 and 17 for Fabric Interconnect B as well.
- 19. After the successful reboot of both FIs, physical FC ports further need to be classified as FC storage ports for directly attached storage array. Click Fabric Interconnect A > Expand Fixed Module > Expand FC ports > FC port 1. On the right pane, choose the VSAN we created earlier and click Save Changes.

I

Figure 29 Choosing VSAN	N Storage for FC Ports	
0 3 7	>> 🛱 Equipment 🕨 🚥 Fabric Interconnects 🕨	🎫 Fabric Interconnect A (primary) 🕨 🎫 Fixed Module 🛌
Equipment Servers LAN SAN M	General Faults Events FSM Statistics	
Filter: All	Fault Summary	
• •		Properties
Equipment		ID: 1
🕀 🗐 Chassis	Status	User Label:
🗄 🐟 🔿 Rack-Mounts	Status	WWPN: 20:01:50:87:89:AC:73:C0
Er est Fabric Interconnects	Overall Status: 👚 Up	Port Type: Physical Negot
📋 🔤 Fabric Interconnect A (prin	Additional Info:	
Er III Fixed Module	Admin State: Enabled	VSAN: Fabric dual/vsan default (1) 🔻
🖃 🚽 Ethernet Ports		Fabric dual/vsan Storage (10)
	Actions	License Del Fabric dual/vsan default (1)
		Licence States Licence Ok
	Enable Port	License State: License Ok
🛨 🚽 Scalability Port		License Grace Period: U
E T FC Ports		
FC Port 1	Configure as Uplink Port	

1

Repeat the Step18, for Fabric Interconnect B FC ports.

20. After the above changes, EMC VNXe storage array would do Fibre Channel flogi into the Fabric Interconnect's. Using the WWPN of the VNXe storage array, we can carve out the SAN boot policy on the UCS Manager. Use SSH connection to the UCSM Virtual IP address, and issue "connect nxos a" command. In the read-only NXOS shell, issue "show flogi database" command and note down the WWPN of the storage array.

VSPEX-FI-1# 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)# show 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								
Total number of flogi = 1.								
VSPEX-FI-A(nxos)#								

21. On UCSM GUI, click **Servers**, **Expand Policies** > **root**, and right-click Boot Policies and click **Create Boot Policy**.

Figure 30	Creating Boot	Policy			
0	3	7	>	>> 🔊 Policies 🕴 👬 root 🕨 🔊 Boot Poli	cies
Equipment Serv	ers LAN SAN	VM Admin		Boot Policies Events	
	Filter: Policies	•		🛨 😑 🛃 Filter 🖨 Export 📚 Print	
ΞΞ				Name	Order
			- 11	⊡…∑ Boot Policy LocalBoot	
				🗄 🖓 🗐 Boot Policy SAN-Boot	
⊢ 👷 root				E Soot Policy default	
	dapter Policies			E S Boot Policy diag	
. <u>.</u>	lOS Defaults				
. Ē.∽ ≦ Bi	IOS Policies			主 🖅 🔊 Boot Policy utility	
	oot Policies ,				
	ost Firmwar	Boot Policies			
[] IF	MI Access				
	ocal Disk Co	Create Boot Policy			
Щ. П. С. М	aintenance Dolici	or .			

22. Specify Boot Policy Name, check the **Reboot on Boot Order Change** check box. Then click **Add Local CD/DVD** as first Boot order, click **Add SAN Boot** and specify the vHBA name for Fabric A as **Primary** and similarly specify the vHBA name for Fabric B as **Secondary**.

Figure 31	Creating Boot Policy Window
1 15 11 0 0 1	creating boor I oney withdow

Γ

🚖 Create Boot Policy						×
Create Boot Policy						0
,						
Name: SAN-Boot			_			
Description:			_			
Reboot on Boot Order Change						
Enforce vNIC/vHBA/iSCSI Name						
Boot Mode: 💿 Legacy 🔘 Uefi						
WADNINGS						
The type (primary/secondary) does not indicate a boot order	presence.					
The effective order of boot devices within the same device of If Enforce vNIC/vHBA/iSCSI Name is selected and the v	lass (LAN/Storage/iSCSI) i: NIC/vHBA/iSCSI does not	s determined by PC exist, a config erro	Ie bus scan order. r will be reported.			
If it is not selected, the vNICs/vHBAs/iSCSI are selected if th	ey exist, otherwise the vf	VIC/VHBA/iSCSI wit	h the lowest PCIe bus scan ord	ler is used.		
Boot Order						
👰 Add CD/DVD 📃 🗨 🖃 🔍	Filter 📥 Export 📚 Print	t				
Add Local CD/DVD	Name	Order	VNIC/VHBA/ISCSI VNIC	Туре	Lun ID	WWN 📭
Add Remote CD/DVD	CD/DVD	1				
🔒 Add Floppy	Neximate	2		Drimoviu		
Add Local Floppy	N secondary		/HBA-B	Secondary		
Add Remote Floppy	Add SAN Boot			X		
Add Remote Virtual Drive		4		0		
	Add SAN BO	000				
vNICs 🛛						
	VHBA: VHBA-B		-			
vHBAs 🕆	Type: O Primary	Secondary				
Add SAN Boot	1,100					
Add SAN Boot Target						
						•
iSCSI vNICs 🛛 🖉				2		
			OK Can		OK	Cancel

23. Once both the vHBAs are added, click Add SAN Boot Target under the vHBAs area, and click Add SAN Boot Target to SAN primary.

₽

٠

•

Cancel

I

Figure 32 Add External USB Boot Order Add CD/DVD 🚯 🖃 🔍 Filter 🛋 Export 📚 Print Add Local CD/DVD Name Order VNIC/VHBA/iSCSI VNIC Lun ID WWN Туре Add Remote CD/DVD 😽 Local CD/DVD 🗄 🛒 San 🔚 Add Floppy VHRA-A 🗐 SAN primary Primary 🔚 Add Local Floppy 🛒 SAN secondary vHBA-B Secondary 릚 Add Remote Floppy Add Remote Virtual Drive vNICs vHBAs 8 Add SAN Boot Add San Boot Target To SAN primary Add San Boot Target To SAN secondary iSCSI vNICs 8 🔺 Move Up 🛛 🗢 Move Down 👘 Delete OK

Adding SAN Boot Target to SAN Primary

24. Provide target WWPN of the VNXe storage device (which can be obtained using "show flogi database" on UCSM CLI command executed under "connect nxos {a|b}" shell as described in the previous subsection). Keep the target as **Primary**.

Figure 33	Adding SAN Boot Target as Primary	
📥 Add SAN	Boot Target	×
Add S/	AN Boot Target	Ø
Boot Tar Boot Targe	rget LUN: 0 t WWPN: 50:06:01:64:08:E0:03:68 Type: • Primary • Secondary	
	ОК	Cancel

25. Repeat step 24 to add secondary VHBA SAN boot target for the Target WWPN for the fabric B too.

Figure 34	Setting SAN Book	t Target					
Boot Order							
🛨 🖃 🔍 Filter	🖨 Export 📚 Pr	int					
Na	me	Order	VNIC/VHBA/iSCSI VNIC	Туре	Lun ID	WWN	₽
Local CD/D ^v	/D	1					
🗅 式 San		2					
🖨 🚍 SAN pri	mary		VHBA-A	Primary			
SAN	I Target primary			Primary	0	50:06:01:64:08:E0:03:68	
🗄 🛒 SAN se	condary		VHBA-B	Secondary			
🔤 🛒 SAN Target primary				Primary	0	50:06:01:65:08:E0:03:68	
1							-

I

Γ

26. Next global configuration task is QoS configuration. Click the LAN tab, expand LAN > LAN Cloud > QoS System Class. Enable Platinum priority, and set MTU to 9216. Keep other configuration as default and save the configuration.

Figure 35 QoS Configure	ation									
🛕 Cisco Unified Computing System Manager - VSPEX-FI		-			The second s		822			
Fault Summary	3 🕘 🖿 New -	Option	s 🕜 🕚	Pending Ad	tivities 🛛 🚺 Exit				ahaha cisco	
0 8 0 4	>> 🗐 LAN + 🙆 I	AN Cloud 🕨	🙀 QoS S	ystem Class				🙀 QoS System Class		
Equipment Servers LAN 5AN VM Admin	General Events	FSM								
Filter: All	Priority	Enabled	Co5	Packet Drop	Weight	Weight (%)	мти	Multicast Optimize	ed	
•	Platinum	V	5		10	• 50	9216	- 🔳		
	Gold		4	V	9	▼ N/A	normal	▼ □		
E-C LAN Cloud	Silver		2		8	▼ N/A	normal	-		
Fabric B	Bronze		1	V	7	▼ N/A	normal	-		
QoS System Class Appliances	Best Effort		Any		5	• 25	normal	-		
Internal LAN	Fibre Channel		3		5	• 25	fc	▼ N/A		

27. From the LAN tab, expand LAN > Policies > root, and right-click on Create QoS Policy.



28. Create a QoS policy with name jumboMTU and select the Priority **Platinum**. Click **OK** to save the configuration.

Figure 37 Creating QoS Policy Window	
A Create QoS Policy	
Create QoS Policy	0
Name: jumboMTU G Egress	
Priority: Platinum Burst(Bytes): 10240 Rate(Kbps): line-rate	
Host Control: None: Full	
	OK Cancel

Configure identifier pools

ſ

In this section, we would configure following identifier pools used by service profile:

- 1. Server UUID pool
- 2. MAC address pool
- 3. WWN pool
- 4. Management IP address pool

Follow the following steps to configure pools mentioned above.

1. From the Servers tab, expand Servers > Pools > root, and right-click on UUID Suffix pools and click Create UUID Suffix Pool.



2. Provide name and description to the UUID suffix pool. Keep other configuration as default.

Figure 39 Create UUID Suj	ffix Pool
📥 Create UUID Suffix Pool	×
Unified C	omputing System Manager
Create UUID Suffix Pool	Define Name and Description 🥹
Description	
2. Add UUID Blocks	Name: BO-VSPEX-UUIDs
	Description: UUID Pool for Branch Office VSPEX Servers
	Prefix: O Derived O other
	Assignment Order: 💿 Default 🔘 Sequential
	< Prev Next > Finish Cancel

3. Click Add to add the UUID block.

I

Γ

🚖 Create UUID Suffix Pool					
Unified Co	omputing	l System	Mana	geı	
Create UUID Suffix Pool	Add UUID Bloc	ks		Ø	
Description 2. √ <u>Add UUID Blocks</u>	Name	From	То	F	
		🛨 Add 🍵 Delete		+	
		<pre>< Prev Next ></pre>	Finish Ca	ancel	

4. Specify the beginning of the UUIDs, and have a large size of UUID block to accommodate future expansion.

Figure 41	Range for UUID Block		
📥 Create a E	Block of UUID Suffixes	2	K
Create	a Block of UUID Suffix	xes 🤫	
From: 6000	0-00000000001 Size: 8 🛨		
		OK Cancel	

- 5. Click **OK** and then **Finish** to deploy UUID pool.
- 6. From the LAN tab, expand LAN > Pools > root, right-click on MAC Pools and then click Create MAC Pool.

Figure 42 Creating MAC Pool



I

7. Provide name and description of the MAC pool and click Next.

Figure 43Creating MAC Po	pol Window
📥 Create MAC Pool	×
Unified Co	omputing System Manager
Create MAC Pool	Define Name and Description 🤨
 ✓ <u>Define Name and</u> <u>Description</u> 2. △ <u>Add MAC Addresses</u> 	Name: BO-VSPEX-MACs
	Assignment Order: O Default O Sequential
	< Prev Next > Finish Cancel

8. Click Add to add MAC pool block.

ſ

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

🛕 Create MAC Pool					
Unified Co	omputing	<mark>j Syste</mark> m	Mana	geı	
Create MAC Pool 1. V <u>Set MAC Pool Name</u>	Add MAC Addr	esses		0	
2. √ <u>Add MAC Addresses</u>	Name	From	То	E	
		+ Add Delete		-	
		<pre>Prev Next ></pre>	Finish	ancel	

9. Provide the initial MAC address and size of the block. As always, provide large number of MAC addresses to accommodate future expansion. We require 6 MAC addresses per server.

Figure 45	Range for MAC Address Block	
📥 Create a I	Block of MAC Addresses	×
Create	a Block of MAC Addresses	0
First MAC Ac To ensure ur encouraged 00:25:85:x :	ddress: 00:25:B5:66:DD:00 niqueness of MACs in the LAN fabric, you are strongly to use the following MAC prefix: x:xx:xx	Size: 40 🛨
		OK Cancel

- 10. Click OK and Finish to complete configuration.
- From the SAN tab, expand SAN > Pools > root, right-click on WWxN Pools, and click Create WWxN Pool.



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

1

Figure 47 Create WWxN	Pool - Defining Pool	l				
📥 Create WWxN Pool						×
Unified C	omputir	ng Syste	em N	lanag	jer	
Create WWxN Pool	Define Name	and Descript	tion			0
1. √ <u>Define Name and</u> <u>Description</u>						
2. ✓ <u>Add WWN Blocks</u>	Name: B	O-VSPEX-WWNs				
	Description:	ombined WWNN and W	/WPN Pool for	VSPEX Servers		
	Max Ports per Node: 3	Ports Per Node	•			
	Assignment Order:	🖲 Default 🔿 Sequential	I			
<u> </u>						
			< Prev	Next >	Finish	Cancel

13. Click Add to add a block of WWxN IDs.

I

Γ

Figure 48	Create WWxN Pool - Adding	a Block of WWrN
rigure +0	Create 11 11 x 11 1 001 - Adding	a Dioch of 11 11 All

A Create WWxN Pool				X
Unified C	omput	ing System	n Manage	r
Create WWXN Pool	Add WWN	Blocks		0
Description 2. ✓ <u>Add WWN Blocks</u>	Name	From	То	
				Ŧ
		E Add De	elete	
		< Pre	w Next > Finis	h Cancel

14. Provide beginning of the WWN IDs and sufficiently large number of block size. Click **OK** and **Finish**.

Figure 49	Range for WWxN Block		
🌲 Create WW	'N Block		×
Create \	WWN Block		0
From: 20:00 To ensure unio encouraged to 20:00:00:25:	:00:25:85:06:0D:00 queness of WWNs in the SAN fabric, you are strongly o use the following WWN prefix: b5:xx:xx:xx	Size:	48 🚖
		ОК	Cancel

15. Next step is creation of the management IP address block for KVM access of the servers. The default pool for server CIMC management IP addresses are created with the name ext-mgmt. From the LAN tab, expand LAN > Pools > root > IP Pools and select IP Pool ext-mgmt, and click the Create Block of IP addresses link on right hand side.





16. Provide initial IP address, size of the pool, default gateway and subnet mask. Click **OK** to deploy the configuration. IP addresses would be assigned to various blade server KVM or CIMC management access from this block.

Figure 51	Size of IPv4 Addresses		
📥 Create Blo	ock of IPv4 Addresses		×
Create	a Block of IPv4 Addresse	S	0
From	10.29.180.225	Size:	8
Subnet Mask	255.255.255.0	Default Gateway: 10.29.180.1	
Primary DNS	. 0.0.0.0	Secondary DNS: 0.0.0.0	
			OK Cancel

That concludes configuration of all identifier pools and blocks.

Configure server pool and qualifying policy

I

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

- **1.** Creation of server pool
- 2. Creation of server pool policy qualification
- 3. Creation of server pool policy

Follow these steps the accomplish the above mentioned tasks:

1. From the Servers tab, expand Servers > Pools > root, right-click on Server Pools and click Create Server Pool.



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

Figure 53 Creating Server Pool - Defining Server Pool

🗼 Create Server Pool	×
Unified C	omputing System Manager
Create Server Pool	Set Name and Description 0
 √<u>Set Name and</u> <u>Description</u> 2. <u>Add Servers</u> 	Name: BO-VSPEX-Server-Pool Description: Server Pool for Branch Office VSPEX Servers
	< Prev Next > Finish Cancel

1

3. Click **Finish** to create the empty server pool. We can add the compute resources to this pool dynamically, based on policy.

Create Server Pool Outified Computing System Manager Add Servers Add Servers Servers	Figure 54 C	reating Server Pool - Adding Servers		
Unified Computing System Manager Create Server Pol • \set Servers • \set Servers Servers Codelis for blade=1 UCSB-B200-M3 UCS UCS UCSB-B200-M3 UCS UCS UCSB-B200-M3 UCS UCSB-B200-M3 UCS UCSB-B200-M3 UCS UCSB-B200-M3 UCS UCSB-B200-M3 UCS UCSB-B200-M3 	🜲 Create Server Pool			X
Create Server Pool Add Servers 1. √ Set Name and Description Servers 2. √ Add Servers Servers 1 1 UCSB-B200-MI3 UCS 1 2 UCSB-B200-MI3 UCS 1 2 UCSB-B200-MI3 UCS 1 2 UCSB-B200-MI3 UCS 1 2 UCSB-B200-MI3 UCS 1 3 UCSB-B200-MI3 UCS Vendor: Cfcli6337DYX Vendor: Clisco Systems Inc	Unified	Computing System Mana	ager	
1. $\sqrt{\text{Set Name and Description}}$ 2. $\sqrt{\text{Add Servers}}$ Chassis ID Slot ID PID R In Ada A A III 1 1 UCSB-B200-M3 UCS III2 Details for blade-1 Model: UCSB-B200-M3 Serial Number: FCH16337DVX Vendor: Cisco Systems Inc	Create Server Pool	Add Servers		0
Servers Pooled Servers Chassis ID Slot ID PID R Rda Rda Rda Rda Ada Ada Rda Rda Ada Ada Ada Rda Rda Rda Ada Ada Rda	 √<u>Set Name and Description</u> √Add Servers 	n		
		Servers Chassis ID Slot ID PID R Ada A A II II III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	*	Pooled Servers Ch Slo Ra Us PID Ad Ad Ad Serial Cor R Model: Serial Number: Vendor:
A Design of the second se				

I

Γ

4. From the Servers tab, expand Servers > Policies > root, right-click on Server Pool Policy Qualifications and click Create Server Pool Policy Qualification.



Figure 55 Creating Server Pool Policy Qualification

5. Give a name to server policy qualification criterion. We are choosing memory qualification criterion as an example.

Figure 56 Creating Server Pool Policy Qualification W

reate Server Pool Policy Qualificati	011									
eate Server Pool Pol	icy Qua	lificatio	on							
ming										
Name: Min-Memory										
Name: Minimum momory	is to add com		EX control of	nal						
is server pool policy qualification will ap	la to add serv	discovered a	EX server po	D OI ind cerverc a	re not qual	ified until they are re	discovered			
as server to out the vitilation according to the	JIV LU HEW UF FE	-uiscovereu s	servers, Exisu	ing servers a	re noc quai	ineu unui uney are re	-uiscovereu			
	.,									
actions	Qualificatio	ins								
ctions	Qualificatio	ns Filter 🖨 E	ixport 🗞 Pr	int	-	_	-	-	_	
ctions Create Adapter Qualifications Create Chassis/Server Qualifications	Qualificatio	ns Filter 👄 E Max	xport 🔀 Pr	int From	То	Architecture	Speed	Stepping	Power Group	E.
ctions Create Adapter Qualifications Create Chassis/Server Qualifications Create Memory Qualifications	Qualificatio	ns Filter 👄 E Max	xport 🔀 Pr Model	int From	То	Architecture	Speed	Stepping	Power Group	Ţ
ctions Create Adapter Qualifications Create Chassis/Server Qualifications Create Memory Qualifications Create CPU/Cores Qualifications	Qualificatio	ns Filter 👄 E Max	xport 😺 Pr Model	int From	То	Architecture	Speed	Stepping	Power Group	Ţ
ctions Create Adapter Qualifications Create Chassis/Server Qualifications Create Memory Qualifications Create CPU/Cores Qualifications Create Storage Qualifications	Qualificatio	ins Filter 👄 E Max	Export 😺 Pr Model	int From	То	Architecture	Speed	Stepping	Power Group	Ţ
Actions Create Adapter Qualifications Create Chassis/Server Qualifications Create Memory Qualifications Create CPU/Cores Qualifications Create Storage Qualifications Create Server PID Qualifications	Qualificatio	ns Filter 👄 E Max	xport 😺 Pr Model	int	То	Architecture	Speed	Stepping	Power Group	Ę
Actions Create Adapter Qualifications Create Chassis/Server Qualifications Create Memory Qualifications Create CPU/Cores Qualifications Create Storage Qualifications Create Server PID Qualifications Create Power Group Qualifications	Qualificatio	ns Filter 👄 E Max	Export 😺 Pr Model	int From	То	Architecture	Speed	Stepping	Power Group	P

6. Set minimum 128 GB RAM for the pool qualification criterion. Note that this is an example criterion, you may choose a criterion that suites your requirement. Click **OK** twice to create the qualification.

ſ

🌲 Create Mem	ory Qualifications					×
Create N	lemory Qualifi	cations				0
Clock (MHz):	• Unspecified • select	Latency (ns):	 Unspecified 	C select		
Min Cap (MB):	C Unspecified 💿 select	Max Cap (MB):	 Unspecified 	C select		
	131072					
Width:	🖲 Unspecified 🔿 select	Units:	 Unspecified 	O select		
						(
					OK	Cancel

7. Finally, from the Servers > Policies > root, right-click on Server Pool Policies and click Create Server Pool Policy.

Figure 57 Creating Memory Qualification



Figure 58 Creating Server Pool Policy

8. Give 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	
📥 Create Se	rver Pool Policy	×
Create	Server Pool Policy	0
_		
Name	BO-VSPEX-Servers	
Description	Policy for VSPEX server Pool Classfication	
Target Poo	Server Pool BO-VSPEX-Server-P 💌	
Qualification	: Min-Memory	
		OK Cancel

9. Click the **Servers** tab on right hand side, you will see that all the compute resources that meet the memory qualification criteria are dynamically added to the server pool.



Configure service profile template

I

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. From the Servers tab. Expand Servers, right-click on Service Profile Templates and click Create Service Profile Template.



Figure 61 **Creating Service Profile Template**

2. Provide service profile template name, keep the type as Initial Template, and choose UUID pool for UUID assignment.

I



3. On next step, select configure LAN connectivity as Expert. Click Add to create a vNIC.

Figure 63	Creating	Service	Profile	Template -	- Networking
igure os	Creating	Service	110jue	rempune .	- Inciworking

🚠 Create Service Profile Template	2				×	
Unified C	Computing	System Mar	nager			
Create Service Profile Template	Networking				0	
1. √ <u>Identify Service Profile</u>	Optionally specify LAN c	onfiguration information.				
<u>Template</u>					-	
3. Storage	Dynamic vMIC Connection Policy:	Select a Policy to use (no Dynamic yNIC R	Policy by defa 💌 🛄 Graats	Dupartic UNIC Copposition Policy		
4. Dzoning	by namic wive connection rolley.	Delect of oney to use (no bynamic water	Creati	B Dynamic VNIC Connection Policy	í l	
5. D <u>vNIC/vHBA Placement</u>						
6. 🗋 <u>Server Boot Order</u>						
7. Maintenance Policy	How would you	like to configure LAN connectivity?	Simple • Expert O No vNICs	C Use Connectivity Policy		
9. Operational Policies	Ignment Click Add to specify one or more vNICs that the server should use to connect to the LAN.					
	Name	MAC Address	Fabric ID	Native VLAN		
					-	
		ma Delete	+ Add Modify		1	
					-	
	iSCSI vNICs 📎					
					_	
	•				•	
			< Prev	Next > Finish	Cancel	

4. Create a system VNIC for fabric A. Enter system A as the VNIC name, choose the created MAC pool, click the radio button Fabric A for Fabric ID, check the vMotion and vSphereMgmt check boxes for VLANs and vSphereMgmt as native VLAN. Choose MTU as 9000, VMware adapter policy and jumboMTU QoS policy.

Name: system-A Jse vNIC Template: MAC Address MAC Address Assignment BO-VSPEX-MACs(40/40) Create vNIC Template Create MAC Pool The MAC address will be automatically assigned from the selected pool. Extere TDI Eabric B Extere TDI Eabric B	
VLANS	
Select Name Native VLAN Image Image Image Image <tr< td=""><td></td></tr<>	
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.	
Pin Group: <not set=""> Create LAN Pin Group Operational Parameters</not>	
Adapter Performance Profile Adapter Policy: VMWare Cos Policy: UMWboMTU Cos Policy: UMboMTU Cos Policy	

- 5. Similarly, create one more VNIC with exact same properties on fabric B.
- 6. Create two more VNICs for NFS server access. Specify the name as Storage A and Storage B for VNICs on Fabric A and B respectively. Check the Storage VLAN check box and mark it as native VLAN. Choose VMware and JumboMTU for adapter policy and QoS policy respectively.

U Create vi	NIC .	22 C
U		
Name: Stora	ae-A	MAC Address
		MAC Address Assignment: BO-VSPEX-MACs(40/40)
I Use vNIC Templ	ate:	
		E Create MAC Pool
		The MAC address will be automatically assigned from the selected pool.
+ Create vNIC	. Template	,
Fabric ID:	Fabric A C Fabric B 🔽 Enable F	Failover
VLANs	Furnauk 🔂 Duink	
	efault	
St 🔽	orage	<u>ه</u>
	1-Data	<u> </u>
	iotion johereMamt	
🛨 Create VL	AN	
Warning		
Make sure th	at the MTU has the same value in t	the QoS System Class
correspondin	g to the Egress priority of the selec	acted QoS Policy.
Pin Group: <r< td=""><td>iot set > 💌 🛨 Create</td><th>a LAN Pin Group</th></r<>	iot set > 💌 🛨 Create	a LAN Pin Group
Operationa	Parameters	8
Adapter Perfe	ormance Profile	
Adapte	r Policy: VMWare 🔹	Create Ethernet Adapter Policy
Qc	S Policy: jumboMTU	Create QoS Policy
	A set of the set of th	- Create Network Control Policy
Network Contro	ol Policy: <not set=""></not>	Create Network Control Policy
Network Contr	ol Policy: <not set=""></not>	

Figure 65 Networking - Create vNIC Window for Storage Traffic

I

Γ

7. Create a VNIC for VM data traffic. Enter data-A for the VNIC name, choose the created MAC address pool, **Fabric A** for Fabric ID. Mark VM-Data as native VLAN, and choose VMware adapter policy.

Figure 66	Networking - Creat	e vNIC for VM Data Traffic		
Create vNIC				0
Name: data-A Use vNIC Template:	plate M	AC Address	40)	
Fabric ID	: A 🔿 Fabric B 🔽 Enable Fai	over	-	
Select default Storage VM-Dat vMotion	Name e a n eMgmt	Native VLAN		
Create VLAN MTU: 1500 Pin Group: <not operational="" para<="" se="" td=""><td>t> 🔹 🛨 Create LA ameters</td><td>IN Pin Group</td><td>8</td><td></td></not>	t> 🔹 🛨 Create LA ameters	IN Pin Group	8	
Adapter Performa Adapter Pol QoS Poli Network Control Poli	rce Profile v: VMWare cy: <not set=""> cy: <not set=""> cy: <not set=""></not></not></not>	Create Ethernet Adapter Policy Create QoS Policy Create Network Control Policy		
				OK Cancel

1

8. Similarly, create another VNIC for Fabric B for VM data traffic. Table 7 summarizes all the VNICs created on the service profile:

vNIC Name	MAC Address Assignment	VLANs	Native VLANs	Fabric	MTU	Adapter Policy	QoS Policy
System- A	MAC pool	vSphereMgmt, vMotion	vSphereMgmt	А	9000	VMware	JumboMT U
System- B	MAC pool	vSphereMgmt, vMotion	vSphereMgmt	В	9000	VMware	JumboMT U
Storage- A*	MAC pool	Storage	Storage	А	9000	VMware	JumboMT U

Table 7Summary of all the vNICs Created
vNIC Name	MAC Address Assignment	VLANs	Native VLANs	Fabric	MTU	Adapter Policy	QoS Policy
Storage- B*	MAC pool	Storage	Storage	В	9000	VMware	JumboMT U
Data-A	MAC pool	VM-Data	VM-Data	А	1500	VMware	-
Data-B	MAC pool	VM-Data	VM-Data	В	1500	VMware	-

 Table 7
 Summary of all the vNICs Created

* Storage vNICs are created for NFS-variant only

 In the Storage window of the Create Service Profile Template wizard, click the Expert radio button for SAN connectivity and choose VSPEX-WWNs for WWNN pool from the drop-down menu. Click Add to add vHBA.

right of Creating Service Projue Template - Stora	Figure 67	Creating S	Service Profile	Template -	Storage
---	-----------	------------	-----------------	------------	---------

Γ

Create Service Profile Templa	ite		×
Unified	Computing System	Manager	
iervice Profile Template • √Identify Service Profile	Storage Optionally specify disk policies and SAN configur	ation information.	0
Template Template Template Vetworking Storage Joning Order Order	Select a local disk configuration policy. Local Storage: Select Local Storage Policy to use	If nothing is selected, the default Local Storage configuration policy will be assigned to this service profile.	<u>*</u>
Operational Policies	How would you like to configure SAN com A server is identified on a SAN by its World Wide Node Name (W profile. World Wide Node Name WWNN Assignment: 20-VSPEX-WWNIs(48/48) The WWNN will be assigned from the selected pool	nectivity? © Simple © Expert © No vHBAs © Use Conne WNN). Specify how the system should assign a WWNN to the serv	ctivity Policy rer associated with this
	The vHBAs's WWPN will also be derived from this pool as lon The available/total WWNNs are displayed after the pool nam	g as you select derived for their address. .e.	
	Name	WWPN	9
		Delete Add Modify	
		< Prev Next :	> Finish Cancel

Create a vHBA with the name vHBA-A, keep the WWPN assignment as Derived, select A as the Fabric ID, select Storage VSAN from drop-down menu for VSAN, and select Adapter policy as VMWare. Click OK to deploy the vHBA.

Figure 68	Storage - Creating vHBA		
🛕 Create vHBA		And and an and an and an and an	×
Create vH	BA		0
Name	VHRA-A	Yorld Wide Port Name	
Use vHBA Templata		WWPN Assignment: Derived	
🛨 Create vHBA T	emplate	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 manifacturer assigned WWPN is used, the WWPN will not be migrated if the service profile is moved to a new server.	
Fabric Select VS/ Pin Grov Persistent Bindir Max Data Field Si	D: • A • B N: Storage • + Create p: <not set=""> • + Create g: • Disabled • Enabled e: 2048</not>	VSAN SAN Pin Group	
Operational Pa	rameters	8	
Adapter Perform	ance Profile		
Adapter Policy:	MWare	annel Adapter Policy	
QoS Policy:	not set> 🔹 🛨 Create QoS Poli		
		ОК	Cancel

- 11. Repeat step 10 for vHBA-B on Fabric B, with the same configuration. Click Next.
- 12. Keep the default configuration for Zoning and vNIC/vHBA Placement policy. Click Next.
- **13.** In the Server Boot Order window, choose **SAN-Boot** for the Boot policy from the drop-down menu. Click **Next**.

Figure 69 Cro	eating Service Profile Templa	ate - Serv	ver Boot Order					
🌲 Create Service Profile Templa	ate							×
Unified	Computing Sy	yste	m Mana	ger				
Create Service Profile Template	Server Boot Order Optionally specify the boot poli	icy for this s	ervice profile template.					0
Template 2. √Networking 3. √Storage 4. √Zoning 5. √vNIC/vH8A Placement 6. √Server Boot Order 7. √Maintenance Policy 8. Server Assignment 9. Operational Policies	Select a boot policy. Boot Policy: SAN-Boot Name: SAN-B Description: Reboot on Boot Order Change: Yes Enforce vNIC/vHBA/ISCSI Name: Yes Boot Mode: Legacy WARNINGS: The type (primary/secondary) does not in The effective order of boot devices within If Enforce vNIC/vHBA/ISCSI Name is If it is not selected, the vNICs/vHBAS/ISCSI Boot Order	Cre oot Y A A A A A A A A A A A A	ate Boot Policy order presence. vice class (LAN/Storage/ISC the vNIC/vHBA/ISCSI does d if they exist, otherwise th	:SI) is determin not exist, a co he vNIC/vHBA/	ed by PCIe bu nfig error will SCSI with the	s scan order. e reported. lowest PCIe bus scan order is	used.	<u> </u>
	🛨 🖃 🔍 Filter 👄 Export 😸 Print	t						
	Name	Order	VNIC/VHBA/ISCSI VNIC	Туре	Lun ID	WWN		
	Local CD/DVD	1						
	SAN primary	2	HBA-A	Primary				
	SAN Target primary			Primary	0	50:06:01:64:08:E0:03:68		
	SAN secondary	\ \	НВА-В	Secondary				
	SAN Target primary			Primary	0	50:06:01:6C:08:E0:03:68		
							1	
							-	-
					< P	rev Next > Fi	nish	Cancel

I

ſ

14. Click Next to go to the Maintenance Policy window. Keep all other fields at default and click Next. In the Server Assignment window, assign the server to Pool Assignment, and choose the created Server Pool and also select the Server Pool Qualification from drop-down. Click Next.

Figure 70 Creati	ng Service Profile Template - Server Assignment	
🍌 Create Service Profile Template		×
Unified C	Computing System Manager	
Create Service Profile Template 1. √ <u>Identify Service Profile</u>	Server Assignment Optionally specify a server pool for this service profile template.	0
Template. 2. √ <u>Networking</u> 3. √ <u>Storage</u> 4. √ <u>Zoning</u> 5. √ <u>VNIC/VHBA Placement</u> 6. √ <u>Server Boot Order</u> 7. √ <u>Maintenance Policy</u> 8. √ <u>Server Assignment</u> 9. √ <u>Operational Policies</u>	You can select a server pool you want to associate with this service profile template. Pool Assignment BO-VSPEX-Server-Pool Select the power state to be applied when this profile is associated with the server. Up C Down The service profile template will be associated with one of the servers in the selected pool. The service profile template will be associated with one of the servers in the selected pool.	*
	To do so, select the qualification from the list. Server Pool Qualification: Restrict Migration:	

1

1

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

Figure 71	Creating	Service I	Profile Tem	plate - O	perational Policies

Create Service Profile Template	the game of a line	×
Unified C	computing System Manager	_
Create Service Profile Template	Operational Policies Optionally specify information that affects how the system operates.	0
2. √ <u>Networking</u>	BIOS Configuration	8
3. √ <u>Storage</u> 4. √Zonina	External IPMI Management Configuration	۲
5. √ <u>vyIIC/vHBA Placement</u> 6. √ <u>Server Boot Order</u> 7. √ <u>Maintenance Policy</u> 8. √ <u>Server Assignment</u> 9. √ <u>Operational Policies</u>	Management IP Address	۲
	Monitoring Configuration (Thresholds)	8
	Power Control Policy Configuration	8
	Scrub Policy	8
	<pre>Prev Next > Finish</pre>	Cancel

That concludes the service profile template creation.

Instantiate service profiles from the service profile template

As a final step to configure UCSM, we will instantiate service profiles from the service profile template. Follow these steps to instantiate Service Profiles:

 From the Servers tab, expand Servers > Service Profiles > root, and click Create Service Profile from Template on the right pane.



17. Provide naming prefix, number of service profile Instances to be instantiated and choose the service profile template from the drop-down menu. Refer to the sizing guidelines for the number of servers needed for your deployment.

Figure 72Creating Service Profile from Template

Figure 73	Creating Service Profiles from Template Window	
📥 Create S	ervice Profiles From Template	×
Create	e Service Profiles From Template	0
	Naming Prefix: BO-VSPEX-Server-	
Name Suffi Nu	x Starting Number: 1 mber of Instances: 2	
Servic	e Profile Template: Service Template BO-VSPEX-Servers-SP-Template	•
	OK Cano	:el

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

Figure 74Service Profiles Created from Service Profile Template

Equipment Servers LAN SAN VM Admin	General Sub-Organizations Service Profiles Pools Policies FC Zones Faults Events
Filter: Service Profiles 🔹	Service Profiles Associated Blades Associated Racks Pooled Servers Service Profile Tem
•	🕒 🖃 🖨 Export 😸 Print
E Service Profiles	Name
⊟- <mark>, 🏩 root</mark>	E
⊕	🕀 🚭 BO-VSPEX-Server-1
	🕀 🖶 🐺 BO-VSPEX-Server-2
	🗄 🖶 🖶 BranchOffice-InfraSrv
666 9	

1

1

19. As 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 select a service profile and see its association state, and with which server it is associated.

Figure 75

Equipment Servers LAN SAN VM Admin	General Storage Network SCSI vNICs Boot Order Virtual Machines FC	Zones
Filter: Service Profiles 🔹	Fault Summary	- Pr
	S V 🛆 🔺	
Service Profiles Service Profiles BO-VSPEX-Server-1 BO-VSPEX-Server-2	0 19 0 0 Status Overall Status:	
BranchOffice-InfraSrv	Status Details	
	Desired Power State: † Up Assoc State: † Associated Assigned State: † Assigned	
	Note: The "Desired Power State" is the Power State of the server set via UCSM. It may be therefore different from the actual value. For the actual server power state click the "Server Details" Tab	Se

20. Eventually, all four servers would be associated – you can also see the summary by clicking on the **Servers** under the **Equipment** tab.

Figure 76 Created Servers Showing Overall Status

2 3 7	>> 📋 Equipment '	剩 Chassis 🕨 🌒	Chassis 1 (primary) 🕨 🧠	> Se	rvers				
quipment Servers LAN SAN VM A	Servers								
Filter: All	🛨 🖃 💐 Filter	👄 Export 📚 Prir	nt						
	Name	Overall Status	Model		Profile	Us	Cores	Cores Enabled	Thre
	Server 1	🕇 Ok	Cisco UCS B200 M3	[org-root/ls-BO-VSPEX-Server-1	1	16	16	32
Equipment	Server 2	🕇 Ok	Cisco UCS B200 M3		org-root/ls-BO-VSPEX-Server-2		16	16	32
E S Chassis	Server 3	Unassociated	Cisco UCS B200 M3			1.1	12	12	24
Chassis 1 (primary)	Server 4	🕇 Ok	Cisco UCS B200 M3		org-root/ls-BranchOffice-InfraSrv		16	16	32
E Server 1									



We have not yet carved out specific data store to install ESXi hypervisor OS image on the VNXe storage array. We need specific WWPN and WWNN addresses to allow access to the data store, and hence we needed to configure the Service Profile before we can carve out the space for each ESXi server on the storage pool.

Configure Data Stores for ESXi Images

I

This section walks you through the steps to create FC accessible data stores for the ESXi boot image per server basis. This includes four steps:

- 1. Host Initiator discovery on VNXe Array
- 2. Create Host
- 3. Configure Storage Pool
- 4. Create Boot LUNs and Configure Host Access.

Host Initiator Discovery on VNXe Array

Once the UCS service profile is associated on the UCS Blades. Make sure you power on all the blades in order to discover the Host initiators (vHBA-A & vHBA-B) on the VNXe Array.

Click **Servers** > **Service Profiles** > **root**. Select the Service Profile and on the right pane click **Storage** > **vHBAs**.

Figure 77 Host Initiator (vHBAs) from VSPEX Server1



Figure 78 Host Initiator (vHBAs) from VSPEX Server2

Equipment Servers LAN SAN VM Admin	
Filter: All	
• -	
Eng Servers	
🖨 🚚 Service Profiles	
🖻 💑 root	
🕀 🖏 BO-VSPEX-Server-1	
😥 🖏 BO-VSPEX-Server-2	
🖻 🦈 BranchOffice-InfraSrv	

General Storage Net	work 🛛 iSCSI vNICs 🗍 Boot Orde	er Virtual Machines FC Z
VHBAs VHBA Initiator	Groups	
vHBAs		
🔍 Filter 🖨 Export 🕻	😸 Print	
Name	WWPN	Desired Order
- VHBA VHBA-A	20:00:00:25:85:06:0D:0E	7
- VHBA VHBA-B	20:00:00:25:85:06:0D:0D	8

I

Create Host

To see VSPEX Servers Host Initiator Discovery on VNXe Array, Launch Unisphere and click **Hosts** and then click **Initiators**.



Figure 79 EMC Unisphere Showing Host Initiators

Configure Storage Pool

ſ

Follow these steps to create storage pool and carve boot LUNs from that on per server basis.

1. Connect to EMC VNXe Unisphere GUI, click the Storage tab. Select Storage Configuration and Storage Pools and then click Create.

Figure 80	Creating Storage Pools				
Dashboard	System Storage	Hosts 🐝 Settings	📀 Support		
VNXe > Storage > S	Storage Configuration > Storage Pools				
List View Grap	ph View				
! Name	▲ Total Space	Used Space	Percent Used	Available Space	Subscription
Used Space:	Available Space: 📕 🛛 Alert Threshold	:			
Create Expand	Details Delete Refresh				

2. Click the Custom Storage Pools radio button. Specify the Pool name for the Storage Pool and skip the FAST VP and click Next.

Figure 81	Storage Pool - Configuration Mode
Storage I	Pool Wizard
	Select Configuration Mode
Select her	Step 1 of 8
Select hov	v you want to configure the system's disks:
Quick	start
Con	figure unused disks into multiple storage pools, where each disk type is in its own pool.
0	This option is only available when no storage pools exist.
💿 Custo	m storage pools
Crea	ate storage pools with custom storage characteristics. If licensed, you can create tiered pools og FAST VP and configure pools to use the FAST Cache.

1

3. Check the Performance Tier check box for using SAS drives for SAN boot LUNs. And keep the default RAID Type: RAID 5 (4+1).

 Figure 82
 Storage Pool - Select Storage

Step 4 of 8			0
he storage tiers you want to u	se for the new poo	1.2	
Storage Tier	Disk Type	Unused Disks	Unused Raw Capacity
Extreme Performance Tier	Flash	5	917.2 GB
Performance Tier	SAS	45	23.5 TB
Capacity Tier	NL SAS	0	0 GB (None Available)
	mance. These disk	s do not provide the s	ame read/write performan
AS disks to provide high perforr e Performance (Flash) disks, b ance Tier	out offer much low	er cost per GB of stora	ige.
AS disks to provide high perforr e Performance (Flash) disks, b ance Tier D Type: RAID 5 (4+1) (Usab	le capacity: 16.4	rer cost per GB of stora	ige.

4. From Performance Tier, Choose 5 of 45 disks (2.0TB) for 600GB SAS disks from the drop-down list and click **Next**. Click **Finish** to confirm the Storage Pool creation.

🕋 Select Amo	unt of Storage			
Step 5 of 7				>
used to satisfy the hot spare polic	/.		nsure that eno	
nused to satisfy the hot spare polic ore information Performance Tier 600 GB (10K RPM) SAS Disks:	Use 35 of 45 disks (14.6 TB)	~	nsure that eno	
nused to satisfy the hot spare polic ore information Performance Tier 600 GB (10K RPM) SAS Disks:	Use 35 of 45 disks (14.6 TB) Use none of the 45 disks	~	nsure that eno	
nused to satisfy the hot spare polic ore information Performance Tier 600 GB (10K RPM) SAS Disks:	Use 35 of 45 disks (14.6 TB) Use none of the 45 disks Use 5 of 45 disks (2.0 TB)	×	nsure that eno	
nused to satisfy the hot spare polic ore information Performance Tier 600 GB (10K RPM) SAS Disks: Total Disks to Configure: 35	Use 35 of 45 disks (14.6 TB) Use none of the 45 disks Use 5 of 45 disks (2.0 TB) Use 10 of 45 disks (4.1 TB)		nsure that eno	
nused to satisfy the hot spare polic ore information Performance Tier 600 GB (10K RPM) SAS Disks: Total Disks to Configure: 35 Total Usable Capacity: 14	Use 35 of 45 disks (14.6 TB) Use none of the 45 disks Use 5 of 45 disks (2.0 TB) Use 10 of 45 disks (4.1 TB) . ⁴ Use 15 of 45 disks (6.2 TB)		nsure that eno	

5. After the successful Storage Pool creation, you will see the Storage Pool for ESXi Boot.

Figure 84 Created Storage Pool for ESXi Boot

💆 Dashboard 🛛 🗮 System	Storage	Hosts 🐝 Settings	Support	
Xe > Storage > Storage Configuratio	n > Storage Pools			
rage Pools				
List View Graph View				
List View Graph View	▲ Total Space	Used Space	Percent Used	Available Space

Create Boot LUNs and Configure Host Access

ſ

Follow these steps to create storage pool and carve boot LUNs from that on per server basis.

1. launch EMC VNXe Unisphere GUI, click the Storage tab. Click LUNs and Create.

Figure 85	Creating LUNs	5					
EMC Unisphere] ?,
Dashboard	System	Storage	Hosts	🐝 Settings	🗿 Support		
VNXe > Storage > L	UNs						
LUNs							0
							🍸 🔍 🗈
! Name		▲ Description		Size		Protection Schedule	
							0.11.000
							0 items
Create Details	Refresh Delete						
🥝 Name: VNXe320	01 Alerts: 🖄	104 Jobs: 🚸	0	User:	admin	System Time: 18:10 (UT)	C-07:00)

1

2. Click the Create a LUN radio button. And specify the LUN name for the VSPEX ESXi host1 Boot LUN and click Next.

Figure 86	Creating LUN - Define LUN
LUN Wizard	
Step	eate a LUN Group or LUN Plof6
Create either a LU Create a LUN g Create a LUN	UN group, containing up to 50 LUNs, or a single LUN. group
LUN Name: *	VSPEX-Server1-Boot-LUN-1
Description:	SAN Boot LUN for VSPEX ESXI5.5 host1
	< Back Next > Finish Cancel Help

3. Choose the created Storage Pool for ESXi Boot LUN. Specify the LUN size and uncheck the check box **Thin** and click **Next**.

Figure 87	Creating LUN - Configure a LUN	
LUN Wizard		
Ste	onfigure a LUN P 2 of 6 ?>>	
Configure the LL	JN's storage characteristics:	
Storage Pool: Tiering Policy:	StoragePool-ESXi-Boot (SAS, 2.1 TB free)	
	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	

- 4. Select **Do not configure a snapshot schedule** and click **Next**. (It is not recommended to configure snapshot for Boot LUNs)
- 5. In the LUN wizard, In the Configure Host Access window, choose LUN from the drop-down list only for the VSPEX ESXi host1 and click **Next**.



Note

I

Boot LUN is specific to single ESXi host, so we don't provide access to VSPEX ESXi host2 for the same Boot LUN.

Figure 88	Creati	ing LUN - Conf	gure Host Access	1			
LUN Wiza	ırd						
	Config Step 4 of 6	jure Hos	t Access				?>
Configure	which hosts wil	ll access this sto	age:				
¶. F	ilter for:		Protocols	FC or iSCSI	Y		
!	Name	▲ Network Ad	dress Op	erating System	Protocol	Access	
	BO-VSPEX-Se	rv 10.29.180.	211 VM	ware ESX	FC, File	LUN	~
e	BO-VSPEX-Se	rv 10.29.180.	212 VM	ware ESX	FC, File	No Access	*
						Fil	tered: 2 of 2
				< Bac	ck Next >	Finish Car	icel Help

1

6. Confirm the summary of the LUN configuration and click **Finish** to complete the LUN creation and host access. Repeat steps 1 to 5 to create Boot LUN for VSPEX ESXi host2.

Figure 89 Creat	ing LUN - Summary	
LUN Wizard		
Sumn Step 5 of	ar y 6	() >>
Confirm the following LU	N configuration:	<u>•</u>
Name:	VSPEX-Server1-Boot-LUN-1	
Description:	SAN Boot LUN for VSPEX ESXi5.5 host1	
Storage Pool:	StoragePool-ESXi-Boot	
Size:	100.0 GB	=
Thin:	No	-
Tiering Policy:	Start High Then Auto-Tier (Recommended)	
Protection Schedule:	None configured	
LUN Access:	 ▼ 1 hosts configured BO-VSPEX-Server-1 	
Snapshot Access:	No hosts configured	•
	< Back Next > Finish Cancel	Help

7. Repeat the steps 1 to 6 to create Boot LUN for VSPEX ESXi host2.

EMC U	nisphere] 3
	Dashboard 🔤	System	Stor	age	losts 🐇	Settings	📀 Support		
VNXe 3	> Storage > LUNs								
LUNS									(
									🍸 🔍 🖬
1	Name		▲ Descript	ion		Size		Protection Schedu	le
e	VSPEX-Server1-Bo	ot-LUN-1	SAN Boo	t LUN for VSPEX ES	SXi5.5 host1	L00.0 GB		Not configured	
e	VSPEX-Server2-Bo	ot-LUN-2	SAN Boo	t LUN for VSPEX ES	Xi5.5 Host2	L00.0 GB		Not configured	
									2 items
Creat	e Details Refre	sh Delete							
📀 Nar	me: VNXe32001	Alerts: 🔼	104 Jo	bs: 🚸 O		U	ser: admin	System Time:	18:20 (UTC-07:00)

Figure 90 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. We are ready to install ESXi images on the UCS server.

Install ESXi servers and vCenter Infrastructure

Follow these steps to install ESXi5.5 image on the UCS servers:

 From UCSM GUI, click the Servers tab, expand Servers > Service Profiles > root, and select a service profile. Click KVM Console on right pane.



2. Once the Java applet of KVM is launched, click the Virtual Media tab and click Add Image. That would open a dialog box to select an ISO image. Traverse the local directory structure and select ISO image of the ESXi 5.5 hypervisor installer media. Once the ISO image shows up in the list, check the Mapped check box and reset the server and click Reset.

Figu	re 92	Aa	lding ESXi	5.5 ISO I	mage				
File	PEX-FI / BO- Help ot Server	VSPEX-Server	1 (Chassis - 1 Se	'ver - 3) - KVM	l Console(Laur	iched By: admin)			
KVM C	ionsole Prope VM 💣 Virtu ent View	al Media							
	Mapped	Read Only	Drive						Exit
		\checkmark	F: - Removable	Disk					Create Image
		\checkmark	🖃 E: - Removable	Disk					Add Image
	<u> </u>		D: - Removable	Disk			_		
			🛃 D:\ISO\ESXi-AL	-Versions-Toget	:her-092513\E5>	ii5.5\ESXi5.5-VMware]		Remove Image
	<u> </u>								Details ±
Del	tails								
Ta	arget Drive	Mapped 1	0	Read Bytes	Write Bytes	Duration			
Vir	tual CD/DVD	🙆 D:\IS	D\ESXi-ALL-Versio	20480	0	00:00:02			USB Reset

1

3. Click OK in the Reset Server warning message pop-up window.

Figure 93 Warning Message to Reset Server

Reset S	erver X
	You have selected the Reset action for one or more servers. If you are trying to boot a server from a power-down state, you should not use this method. If you continue the power-up with this process, the desired power state of the servers will become out of sync with the actual power state and the servers may unexpectedly shut down at a later time. To safely reboot the selected servers from a power-down state, click Cancel then select the Boot Server action. If you are certain that you want to continue with the Reset operation, click OK .

4. Click the **Power Cycle** radio button and click **OK**.

Figure 94	Selecting the Reset Type	
Reset Se	rver Service Profile VSPEX-Server-1	×
	You are attempting to reset a server. The server can be reset by gracefully restarting the OS or via a brute force power cycle. How would you like to reset? Power Cycle Gracefully restart OS If Graceful OS Restart is not supported by the OS or it	
	does not happen within a reasonable amount of time, the system will perform a power cycle.	
	The UCS system might be in the process of performing some tasks on this server. Would you like this operation to wait until the completion of outstanding activities?	
	Wait for completion of outstanding UCS tasks on this server.	
	OK Cancel	

5. Click the KVM tab to view the boot process. During the Boot process, Press F6 for the Boot Selection window to appear and verify that the Cisco Virtual KVM-mapped vDVD is the 1st boot device and Storage LUNs as 2nd Boot device.



I

6. At this point of time, ESXi5.5 installation media would boot from the virtual disk mounted on the KVM. Follow these steps to install ESXi 5.5 hypervisor on the boot LUN. Make sure that you select the Storage boot LUN we created and not the local disk to install the hypervisor image. You can select all the default parameters or as per your requirements.

gure 96	Sele	ecting a Disk to	o Install or Upgrade		
		:	Select a Disk t	o Install or Upg	rade
	* Contair # Claimed	ns a VMFS 1 by vSAN	partition		
	Storage [)evice			Capacity
	Local: (none: Remote: DCC) VRA ID	(naa	.6006016022d0360	08da4d) 100.00 GiB
	(Esc)	Cancel	(F1) Details	(F5) Refresh	(Enter) Continue

1

7. Once the ESXi is installed, login the system by pressing F2 on the KVM window. You need to configure basic management network for the ESXi host. Make sure that you have selected two system vNICs.

Figure 97 Selecting	Network Adapters
---------------------	------------------

Network Adapters Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.					
Device Name [X] vmnic0 [X] vmnic1 [] vmnic2 [] vmnic3 [] vmnic4 [] vmnic5	Hardware Label (MAC Address) N/A (00:25:b5:66:dd:1e) N/A (00:25:b5:66:dd:0e) N/A (00:25:b5:66:dd:1d) N/A (00:25:b5:66:dd:0d) N/A (00:25:b5:66:dd:1f) N/A (00:25:b5:66:dd:0f)	Status Connected () Connected () Connected () Connected () Connected () Connected ()			
<d></d> View Details	<pre>Space> Toggle Selected</pre>	<pre></pre>			

Easiest way to figure out which vmnic adapter should be used for the vSphere managemet purpose, you can identify the vmnic by MAC address. The MAC addresses of the VNICs (vmnics) are summarized on the following UCSM GUI window. Click the **Servers** tab, expand **Servers** > **Service Profiles** > **root**, and select a particular service profile and click the **VNICs**. The VNIC names and MAC addresses are listed on the right pane of the window.

i iguite s o o o o o o o o o o o o o o o o o o	stem 12 and System	2			
Fault Summary	G	Options 🤤 🔞 💧 🗥	Pending Activities 🛛 🧿	<u>E</u> xit	
2 2 7	>> 🥪 Servers 🕨 👼 Serv	vice Profiles 🕨 🍰 root 🕨 🍮	Service Profile BO-VSPEX-	Server-1	
Equipment Servers LAN SAN VM Admin	Virtual Machines	FC Zones Policies	Server Details	CIMC Sessions	s FSM
Filter: All	General	Storage			.51 (14105
* -	VNICs	Print			
E					
🖹 🖶 🤩 Service Profiles	Name	MAC Address	Desired Order 🛆	Actual Order	Fabric ID
	- vNIC system-A	00:25:85:66:DD:1E	1 1	. Α	ΑB
EO-VSPEX-Server-1	VNIC system-B	00:25:85:66:DD:0E	J 2 2	2 8	3 A
H	- VNIC data-A	00:25:85:66:DD:1D	3 3	3 A	¥В
. Sub-Organizations	📕 📲 vNIC data-B	00:25:85:66:DD:0D	4 4	F B	3 A
E- Service Profile Templates	-I vNIC Storage-A	00:25:85:66:DD:1F	5 5	; A	¥В
📄 🧙 root	-I vNIC Storage-B	00:25:85:66:DD:0F	6 6	; B	3 A
🕀 📊 Service Template BO-VSPEX-Ser					

Figure 98 Created vNICs for System-A and System-B

Repeat the ESXi installation steps for the remaining VSPEX server2 similarly.

VMware vCenter Server Deployment

This section describes the installation of VMware vCenter for VMware environment and to get the following configuration:

- A running VMware vCenter virtual machine
- VMware DRS and HA functionality enabled.

For detailed information on installing a vCenter Server, see the link:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalI d=2032885

Following steps provides high level configuration steps to configure vCenter server:

1. Create the vCenter host VM

If the VMware vCenter Server is to be deployed as a virtual machine on an ESXi server installed as part of this solution, connect directly to an Infrastructure ESXi server using the vSphere Client. Create a virtual machine on the ESXi server with the customer's guest OS configuration, using the Infrastructure server datastore presented from the storage array. The memory and processor requirements for the vCenter Server are dependent on the number of ESXi hosts and virtual machines being managed. The requirements are outlined in the vSphere Installation and Setup Guide.

2. Install vCenter guest OS

Install the guest OS on the vCenter host virtual machine. VMware recommends using Windows Server 2012 R2 SP1. To ensure that adequate space is available on the vCenter installation drive, see vSphere Installation and Setup Guide.

3. Install vCenter server

Install vCenter by using the VMware VIM Setup installation media. Easiest method is to install vCenter single sign on, vCenter inventory service, and vCenter server using Simple Install. Use the customer-provided username, organization, and vCenter license key when installing vCenter.

4. Apply vSphere license keys

To perform license maintenance, log into the vCenter Server and select the Administration -Licensing menu from the vSphere client. Use the vCenter License console to enter the license keys for the ESXi hosts. After this, they can be applied to the ESXi hosts as they are imported into vCenter.

Configuring cluster, HA and DRS on the vCenter

Perform the following steps to add all the VMware on virtual machine vCenter:

- 1. Log into VMware ESXi Host using VMware vSphere Client.
- 2. Create a vCenter Datacenter.
- 3. Create a new management cluster with DRS and HA enabled.
 - a. Right-click on the cluster and, in the corresponding context menu, click Edit Settings.
 - **b.** Select the checkboxes Turn On vSphere HA and Turn On vSphere DRS, as shown in the Figure 99.

c. Click OK, to save changes.

2	New Cluster Wizard	
Cluster Features What features do you want	to enable for this duster?	
Cluster Features vSphere DRS Power Management vSphere HA Virtual Machine Options VM Monitoring VMware EVC VM Swapfile Location Ready to Complete	Name BO-VSPEX-Cluster Cluster Features Select the features you would like to use with this duster. ✓ Turn On vSphere HA vSphere HA detects failures and provides rapid recovery for the virtual machines running within a duster. Core functionality includes host and virtual machine monitoring to minimize downtime when heartbeats cannot be detected. vSphere HA must be turned on to use Fault Tolerance. ✓ Turn On vSphere DRS vSphere DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources can be divided into smaller resource pools for users, gr and virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines. vSphere DRS and VMware EVC should be enabled in the cluster in order to permit pla and migrating VMs with Fault Tolerance turned on, during load balancing.	pups, ines , and cing
Help	< Back Next > Ca	ncel

d. Add all ESXi hosts to the cluster by providing servers management IP addresses and login credentials one by one.

Figure 100	Adding E	SXi Hosts to the Clu	ster				
Ø			VCenter55.DC.lo	ocal - vSphere Client			
File Edit Viev	w Inventory Admini	stration Plug-ins Help					
	🖸 🔝 🏠 Home 🕨 🖓 Inventory 🕨 🗊 Hosts and Clusters						
6 6 8	t o						
□ 🗗 VCenter5 □ 🌆 VSPE □ 📂 B □ 👔	55.DC.local EX-BO 30-Infra bo-infra-host AD-DNS SQLDB	bo-vspex-host1 VM ware ESXi, 5.5.0, 1331820 Getting Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permissions Maps Configuration Issues The number of vSphere HA heartbeat datastores for this host is 0, which is less than required: 2					
	VCSS-W2K12 30-VSPEX-Cluster bo-vspex-host1	General Manufacturer: Model: CPU Cores: Processor Type:	Cisco Systems Inc UCSB-8200-M3 16 CPUs x 1.999 GHz Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz	Resources CPU usage: 40 MHz Memory usage: 3177.00 MB	Capacity 16 x 1.999 GHz Capacity 262085.60 MB		

a 00 Configuring HA and DPS on Ch

I

Γ

Virtual Networking Configuration

In UCSM service profile, we created six vNICs per server for NFS-Variant. This shows up as six network adaptors or vmnics in ESXi server. You can see these adapters in the vCenter by selecting **Home** > **Inventory** > **Hosts and Clusters** view, select a server, click the **Configuration** tab on the right pane and click **Network Adapters**.

Figure 101 Network Adapters Created Through UCS Manager

Ø	VCenter55.DC.local - vSphere Client								
File Edit View Inventory Admir	File Edit View Inventory Administration Plug-ins Help								
🕞 💽 🚺 Home 🕨 🛃 In	🖸 🔯 Home 🕨 🛃 Inventory 🕨 🛅 Hosts and Clusters								
a e 38									
 □ I VCenter55.DC.local □ I VSPEX-BO □ I BO-Infra 	bo-vspex-host1 VMware ESXi, 5.5.0, 1 Getting Started Summary Virtual Ma	L331820 Ichines Performance Configura	tion Tasks & Events	Alarms	nissions Maps	Storage Views Hard	dware Status		
Do-infra-host	Hardware	Network Adapters							
SQLDB VCS5-W2K12 DO-VSPEX-Cluster R bo-vspex-host1 bo-vspex-host2	Processors Memory Storage Networking Storage Adapters Network Adapters Advanced Settings Power Management Software	Verice Cisco Systems Inc Cisco V wmic5 wmic4 wmic3 wmic3 wmic2 wmic1 wmic1	7 /C Ethernet NIC 10000 F 10000 F 10000 F 10000 F 10000 F	10000 Full 10000 Full 10000 Full 10000 Full 10000 Full 10000 Full	None None None None vSwitch0 vSwitch0	MAC Address 00:25:b5:66:dd:0f 00:25:b5:66:dd:0 00:25:b5:66:dd:0 00:25:b5:66:dd:0e 00:25:b5:66:dd:0e 00:25:b5:66:dd:1e	None None None None 0.0.0.1-255.255.255.254 0.0.0.1-255.255.255.254		

Using Figure 101 and Figure 98 from UCSM, it would be a good idea to make a table like following on per ESXi host basis.

For Example, below we have shown the ESXi host1 identity such as UCS Blade vNIC, vSphere vmnic & corresponding VLAN ID.

Table 8 Service Profile vNIC and vSphere vmnic Relations

UCS Manager vNICs	vSphere NIC	MAC Address	VLAN IDs
System-A	vmnic0		11 for vSphereMgmt and 40 for vMotion
System-B	vmnic1		11 for vSphereMgmt and 40 for vMotion
Storage-A	vmnic2		20 for Storage
Storage-B	vmnic3		20 for Storage
Data-A	vmnic4		30 for VMData
Data-B	vmnic5		30 for VMData



You can use the virtual switching strategy with any variant of architecture.

We would create 3 native Standard default virtual switches for virtual network configuration as follows:

- 1. vSwitch0 For management traffic and vMotion traffic
- 2. vSwitch1 For VM data traffic
- 3. vSwitch 2 For NFS Storage traffic

Each vSwitch listed above would have two vmnics, one on each fabric for load balancing and high-availability. Also, for vMotion traffic, jumbo MTU needs to be configured in virtual network too. Follow these steps to configure the two vSwitches to achieve that goal.

 Choose Home > Inventory > Hosts and Clusters panel on vCenter, expand the VSPEX cluster and select an ESXi host. Click the Configuration tab > Networking > Properties to view the properties of vSwitch0.

Figure 102 Properti	ies of vSwitch	
🖸 🔝 🏠 Home 🕨 🚮 Int	ventory 👂 🗊 Hosts and Clusters	
ø ∉ #		
 □ I VCenter55.DC.local □ □ VSPEX-BO □ I P BO-Infra 	bo-vspex-host1 VMware ESXi, 5.5.0, 13 Getting Started Summary Virtual Mac	3 1820 hines Performance Configuration Tasks & Events Alarms Permissions Maps St
□ □ bo-infra-host	Hardware Processors	View: vSphere Standard Switch vSphere Distributed Switch
□ ① BO-VSPEX-Cluster □ 0 No-vspex-host1 ↓ bo-vspex-host1 ↓	Storage Networking Storage Adapters	Standard Switch: vSwitch0 Remove Properties Virtual Machine Port Group Physical Adapters
	Network Adapters Advanced Settings Power Management	VM Network Image: Second sec
	Software	

2. Select the vSwitch and then click Edit.

ſ

Ø			vSwitch0 Properties		_ □	x
F	orts Network Adapters					
	Configuration	Summary	vSphere Standard Switch Properties -			^
Ir	vSwitch	120 Ports	Number of Ports:	120		
	VM Network	Virtual Machine				
	Management Net	vMotion and IP	Advanced Properties			
			MTU:	1500		
			Default Policies			
			Security			
			Promiscuous Mode:	Reject		
			MAC Address Changes:	Accept		=
			Forged Transmits:	Accept		
			Traffic Shaping			
			Average Bandwidth:	-		
			Peak Bandwidth:			
			Burst Size:			
			Failover and Load Balancing			
			Load Balancing:	Port ID		
			Network Failure Detection:	Link status only		
			Notify Switches:	Yes		
			Failback:	Yes		
	Add	Edit Remove	Active Adapters:	vmnic0		~
				Close	Hel	p

1

Figure 103 Changing the vSwitch Properties

3. Change the MTU to 9000 in the General tab.

4. Click the NIC Teaming tab. Move up the Standby Adapter to the Active Adapters list, and then click OK.

Γ

			X
		vSwitch0 Properties	
General Security	Traffic Shaping	NIC Teaming	
	د · · -		
Load Balancing:	5	Poute based on the origination	irtual port ID
Network Esilove	r Detection:		
Network Fallove	Detection.	Link status only	
Notify Switches:		Yes	<u> </u>
Failback:		Yes	_
Failover Order:			
adapters activa	te in the order sp	pecified below.	, cando y
Name	Speed	Networks	Move Up
Active Adapte	10000 Full	0.0.0.1-255.255.255.254	Move Down
Standby Adap	oters		
vmnic1	10000 Full	0.0.0.1-255.255.255.254	
Adapter Detail Cisco Systems	s Inc Cisco VIC Ett	hernet NIC	
Name:		vmnic1	
Location:		PCI 07:00.0	
Driver:		enic	
		OK Canc	el Help

1

Figure 105 Specifying the vmnic Order for the Port Group

5. That would bring you back to vSwitch0 configuration window. Click the **Ports** tab, and then click **Add**.

Ø		vSwitch0 Properties		_ □	x
Ports Network Adapters					
Configuration	Summary	vSphere Standard Switch Properties -			
T vSwitch	120 Ports	Number of Ports:	120		
VM Network	Virtual Machine				
Management Net	vMotion and IP	Advanced Properties			
		MTU:	9000		
		Default Policies			
		Security			
		Promiscuous Mode:	Reject		
		MAC Address Changes:	Accept		=
		Forged Transmits:	Accept		
		Traffic Shaping			
		Average Bandwidth:			
		Peak Bandwidth:			
		Burst Size:			
		Failover and Load Balancing			
		Load Balancing:	Port ID		
		Network Failure Detection:	Link status only		
		Notify Switches:	Yes		
		Failback:	Yes		
Add	Edit Remove	Active Adapters:	vmnic0, vmnic1		~
			Close	Н	elp

Figure 106 Adding Ports in the vSwitch Property Window

Γ

6. Click the VMKernel radio button and then click Next in the Add Network wizard window.

Figure	e 107 Adding N	Network - Connection Type			
6		Add Network Wizard	-		x
C	Connection Type Networking hardware can	be partitioned to accommodate each service that requires connectivity.			
Cc Cc Su	onnection Type onnection Settings ummary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, and host management.	NFS,]
	Help	< Back Next >]_	Canc	el

1

7. Specify a name as vMotion in the Network Label field. Choose the VLAN ID, as standard vSwitch0 carries both management and vMotion VLANs. Management traffic leaves vSwitch0 untagged, using the native VLAN of the vNIC, but the vMotion traffic must be tagged with appropriate VLAN ID. Check the Use this port group for vMotion check box.

2	Add Network Wizard
VMkernel - Connection Use network labels to i	Settings dentify VMkernel connections while managing your hosts and datacenters.
Connection Type Connection Settings IP Settings Summary	Port Group Properties Network Label: VLAN ID (Optional): Use this port group for vMotion Use this port group for Fault Tolerance logging Use this port group for management traffic
	Preview: VMkernel Port VMotion VLAN ID: 40 Vrtual Machine Port Group VM Network VMkernel Port Wanagement Network vmk0 : 10.29.180.211
Help	< Back Next > Cancel

8. Configure IP address and subnet mask for the vmkernel interface in the next step.

L

Γ

Figure 109 Adding	g Network - IP Settings
Ø	Add Network Wizard
VMkernel - IP Connectio Specify VMkernel IP set	n Settings ttings
Connection Type Connection Settings IP Settings Summary	C Obtain IP settings automatically Use the following IP settings: IP Address: Subnet Mask: VMkernel Default Gateway: 10 . 29 . 180 . 1 Edit Preview: VMkernel Port VMkernel Port VMkernel Port Group VM Network WMkernel Port Management Network Vmk0 : 10.29.180.211
Help	< Back Next > Cancel

1

9. Click **Next** and in the next window click **Finish** to deploy the vMotion vmkernel. Back in the vSwitch0 properties window, select the newly created vMotion port group and click **Edit**.

Ø			vSwitch0 Properties		_ □	x
Ports	Network Adapters					
Con	figuration	Summary	Port Properties			
1	vSwitch	120 Ports	VLAN ID:	vMotion		
T 👸	vMotion	virtual Machine vMotion and IP	vMotion:	40 Epobled		
l Yê	Management Net	VMOLION and IP	Fault Tolerance Logging:	Disabled		
			Management Traffic:	Disabled		
			iSCSI Port Binding:	Disabled		=
			NIC Settings	00.50.56.62.31.66		
			MTU:	1500		
			IP Settings			1
			IP Address:	10.10.40.11		
			Subnet Mask:	255.255.255.0	Mary Davidson Table	
					view Routing Table	
			Effective Policies			
			Security			
			Promiscuous Mode:	Reject		
			MAC Address Changes:	Accept		
A		Edit Remove	Forged Transmits:	Accept		~
					Close He	
					close He	Ψ

Figure 110 Adding Network - Editing Configuration

I

Γ

10. Set the MTU to 9000 and click OK. Click Close in the parent window.

<u> </u>		vMotion Properties
Ge	neral IP Settings Security 1	Traffic Shaping NIC Teaming
Г	Port Properties	
	Network Label:	vMotion
	VLAN ID (Optional):	40
	vMotion:	
	Fault Tolerance Logging:	
	Management Traffic:	Enabled
	iSCSI Port Binding:	Enabled
	NIC Settings	
	MTU:	9000

I

1

---- --Figu

11. Repeat steps 1 to 10 for the remaining ESXi hosts in the cluster. Once all the ESXi hosts are configured, you must be able to ping from one host to another on the vMotion vmkernel port with jumbo MTU. Validate this by pinging the respective IPs with using the option do not fragment.

```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.
VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
- # vmkping -d -s 8972 10.10.40.12
PING 10.10.40.12 (10.10.40.12): 8972 data bytes
8980 bytes from 10.10.40.12: icmp_seq=0 ttl=64 time=0.499 ms
8980 bytes from 10.10.40.12: icmp seq=1 ttl=64 time=0.310 ms
8980 bytes from 10.10.40.12: icmp seq=2 ttl=64 time=0.349 ms
 -- 10.10.40.12 ping statistics ---
                                                                                 Ξ
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.310/0.386/0.499 ms
 #
```

 Back in the vCenter view, select ESXi host1 from the Hosts and Clusters, click the Configuration tab > Networking. Make sure vSwitch0 has both management traffic and vMotion traffic for vmnic0 and vmnic1.





13. To Create vSwitch1 for VM-Data traffic, click Networking and then click Add Networking.

	a		
🖸 🔝 🏠 Home 🕨 🚮 Inv	entory 🕨 🗊 Hosts and Clusters		Search Inventory
s e H			
 □ I Center55.DC.local □ I VSPEX-BO □ I OSPEX-BO □ I OSPEX-BO □ I OSPEX-BO 	bo-vspex-host1 VMware ESXi, 5.5.0, 13 Getting Started Summary Virtual Mac	331820 hines Performance Configuration Tasks & Events Alarms Permissions Maps	Storage Views Hardware Status
Do-Infra-host	Hardware	View: vSphere Standard Switch vSphere Distributed Switch	
GOLDB VC55-W2K12 BO-VSPEX-Cluster Go-vspex-host1 bo-vspex-host2	Processors Memory Storage Networking Storage Adapters Network Adapters Advanced Settings Power Management Licensed Features Time Configuration DNS and Routing Authentication Services Power Management Virtual Machine Starbup/Shutdown Virtual Machine Swapfile Location	Standard Switch: vSwitch0 Remove Properties VInual Machine Port Group Wilcall Adapters wincil 10000 Full VM Havork Image: vmnic0 10000 Full Image: vmnic0 10000 Full VMikemal Port Wilkemal Port Image: vmnic0 10000 Full VMikemal Port Image: vmnic0 10000 Full Image: vmnic0 10000 Full VMikemal Port Image: vmnic0 10000 Full Image: vmnic0 10000 Full VMikemal Port Image: vmnic0 10000 Full Image: vmnic0 10000 Full	Refresh Add Networking Properties.

1

Figure 113 Add Networking to Create vSwitch for VM-Data

- 14. Click the radio button Virtual Machine in the Add Networking Wizard, click Next.
- Figure 114 Adding Network Connection Type

9	Add Network Wizard			x
Connection Type Networking hardware c	an be partitioned to accommodate each service that requires connectivity.			
Connection Type Network Access Connection Settings Summary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VHkernel The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iS and host management.	CSI, NFS,		
Help	< Back Next >		Cano	el

15. Select the two vmnics corresponding to the VM-Data VNICs and click Next.



16. Specify the name for Network Label as VM-Data, and keep VLAN ID as 0 to signify the absence of VLAN tag. Click Next.

I

Figure 116 Adding Network - Connection Settings				
Ø	Add Network Wizard	-		x
Virtual Machines - Connection Settings Use network labels to identify migration compatible connections common to two or more hosts.				
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VM-Data VLAN ID (Optional): None (O) Preview: VM-Data VM-Data VM-Data VM-Data VM-Data			
Help	< Back Next >]	Cance	

1

- **17.** In the next window click **Finish** to deploy the vSwitch1 creation for VM-Data traffic. Repeat steps 13 to 16 for the remaining ESXi host in the cluster.
- 18. To create vSwitch2 and VMkernel for Storage traffic, click Networking > Add Networking.
| | - | | | |
|--|---|--|-------------------------------|-----------------------------|
| File Edit View Inventory Administration | on Plug-ins Help | | | |
| 🕞 💽 🏠 Home 🕨 🚮 Inventory | y 🕨 🗊 Hosts and Clusters | | | Search Inventory |
| 5 6 35 | | | | |
| □ ☐ VCenter55.DC.local bo- □ ↓ VSPEX-BO Get □ ↓ Bo-infra Get | vspex-host1 VMware ESXi, 5.5.0, 1331820
tting Started Summary Virtual Machines | Performance Configuration Tasks & Even | ts Alarms Permissions Maps St | orage Views Hardware Status |
| AD-DNS | Vie | w: vSphere Standard Switch vSphere Dis | tributed Switch | |
| 🚡 SQLDB | Processors Ne | tworking | | Refresh Add Networking |
| 👘 VC55-W2K12 | Memory | - | | |
| BO-VSPEX-Cluster | Storage | | | |
| bo-vspex-host1 | Networking Sta | ndard Switch: vSwitch0 | Remove Properties | |
| bo-vspex-host2 | Storage Adapters | -Virtual Machine Port Group | ysical Adapters | |
| | Notwork Adoptors | VM Network | 🛯 🌃 vmnic1 10000 Full | |
| | Network Adapters | -VMkernel Port | 💵 vmnic0 10000 Full 🖓 | |
| | Advanced Settings | vMotion 👤 🔶 | | |
| | Power Management | vmk1:10.10.40.11 VLAN ID:40 | | |
| 50 | ftware | VMkernel Port | | |
| | Licensed Features | vmk0 : 10 29 180 211 | | |
| | Time Configuration | | | |
| | DNS and Routing | | | |
| | Authentication Services Sta | ndard Switch: vSwitch1 | Remove Properties | |
| | Rever Management | -Virtual Machine Port Group | sical Adapters | |
| | Fower Management | 🛛 VM-Data 🛛 👲 🔶 🛶 🖕 | 📟 vmnic2 10000 Full 🖵 | |
| | virtual Machine Startup/Shutdown | | 📟 vmnic3 10000 Full 🖵 | |
| | Virtual Machine Swapfile Location | | | |
| | Security Profile | | | |

Figure 117 Add Networking to Create vSwitch and vmKernel for Storage Traffic

19. Click the VMKernel radio button and then click Next in the Add Network Wizard window.

2	Add Network Wizard
Connection Type Networking hardware car	n be partitioned to accommodate each service that requires connectivity.
Connection Type Connection Settings Summary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXI services: vSphere vMotion, iSCSI, NFS, and host management.
Help	< Back Next > Cancel

Figure 118 Adding Network - Connection Type

I

Γ

20. Select the two vmnics (vmnic4 and vmnic5) corresponding to the NFS Storage VNICs and click Next.

1

1

Ø	Add Network Wizard						
VMkernel - Network Acce The VMkernel reaches n	ess etworks through uplink adapters attached to vSphe	re standard swit	tches.				
Connection Type Network Access Connection Settings Summary	Select which vSphere standard switch will handle vSphere standard switch using the undaimed ne Cisco Systems Inc Cisco VIC Ethern Cisco Systems Inc Cisco VIC Ethern Use vSwitch0 Cisco Systems Inc Cisco VIC Ethern Winco Use vSwitch1 Preview: VMkernel Port VMkernel	e the network tra twork adapters Speed et NIC 10000 Full 10000 Full 10000 Full 10000 Full Speed Physical Adapters • • • vmnic4 • • vmnic5	affic for this connection. You may als listed below. Networks None Networks 0.0.0.1-255.255.255.254 0.0.0.1-255.255.255.254	o create a n	ew	× III ×	
Help	1		< Back Next >		Cance		

Figure 119 Adding Network - Network Access

21. Configure IP address and subnet mask for the vmkernel interface in the next step.

Ø	Add Network Wizard
VMkernel - IP Connection Specify VMkernel IP se	on Settings Ittings
Connection Type Network Access Connection Settings IP Settings Summary	C Obtain IP settings automatically Use the following IP settings: IP Address: Subnet Mask: VMkernel Default Gateway: 10 . 10 . 20 . 11 255 . 255 . 255 . 0 10 . 29 . 180 . 1 Edit
	VMkernel Port Physical Adapters Storage Image: Storage 10.10.20.11 Image: Storage
Help	< Back Next > Cancel

Figure 120 Adding Network - IP Configuration Settings

22. Click Next and in the next window click **Finish** to deploy the vSwitch2 and VMkernel for Storage traffic. Repeat the steps 18 to 21 to create Storage VMkernel for the remaining ESXi host.

This concludes the Virtual Networking configuration on the vCenter.

Configure storage for VM data stores, install and instantiate VSPEX VMs from vCenter

This section describes the steps to configure VNXe Storage for VM Data stores to install and instantiate VSPEX VMs from vCenter. This includes five steps:

- 1. Configure Link Aggregation
- 2. Create NAS Server
- 3. Configure Storage Pool for NFS-Data
- 4. Create VMware Datastores
- 5. Mount NFS share on ESXi hosts

Configure Link Aggregation

1. Connect to the EMC VNXe Unisphere GUI, click the Settings tab > Port Settings.



Figure 121Port Configuration in EMC Unisphere

2. We connected 1GbE ports Ethernet Port 2 and Port 3 for NFS Storage Access from UCS Blades.

MC Unisphere			
평 Dashboard 👅	System	1	torage 👔 Hosts <u> Settings</u> 📀 Support
VNXe > Settings > More c	onfiguration >	Port Setti	ngs
ort Settings — IO Modules ————			Port Details
Port	SP A	SP B	Select a port from the IO Modules list to the left.
▼ Base Ports			
Ethernet Port 2	0	e	
Ethernet Port 3	0	0	
Ethernet Port 4	e	0	
Ethernet Port 5	e	0	
▼ IO Module 0			
FC port 0	e	0	
FC port 1	e	0	
FC port 2	0	0	
FC port 3	e	0	

Figure 122 Verify the Ports for NFS Storage Access

- **3.** To Create Aggregation, click **Ethernet Port 2** and choose Ethernet Port 3 from the drop-down list and click **Create Aggregation**.
- 4. A pop-up window to confirm the Link Aggregation Creation appears. Click Yes to confirm.

Figure 123	Creating Link Aggrega	tion		
— Port Detai	ls			
		Port Name:	Ethernet Port 2	
		Type:	Ethernet	
		Link State:	SP A (Link Up), SP B (Link Up)	
	Agg	regate With:	Ethernet Port 3 🗸 Create Aggregation	
Selected Maximum Transmission Unit (MTU) Size:			1500 🖌 Bytes	
		Actual MTU:	SP A (1500 Bytes), SP B (1500 Bytes)	
	Sele	acted Speed:	Auto Mbps	
	A	Create Link	Aggregation	
Network A	ddresses:	Are you sur port?	re you want to create aggregation with this	
Storage	. Network Ad	dress	Yes No VLAN ID	Used For

5. After confirmation, you will see the created Link Aggregation between Ethernet Port 2 and Ethernet Port 3.

Figure 124 Verify the Created Link Aggregation

MC Unisphere			
Dashboard	System	Sto	torage 👔 Hosts 🐝 Settings 📀 Support
VNXe > Settings > More of	onfiguration	> Port Setting	ngs
ort Settings			
- IU Modules			Port Details
Port	SP A	SP B	Part Names - Ethomat Part 2
▼ Base Ports			Port Name: Ethernet Port 3
Ethernet Port 4		e	Type: Ethernet
Ethernet Port 5	0	0	Link State: SP A (Link Up), SP B (Link Up)
Link Aggregation 3			Aggregate With: Link Aggregation 3 Remove from Aggregation
Ethernet Port 3		2	Selected Maximum Transmission Unit (MTU) Size: 1500 V Bytes
Ethernet Port 2	0	a	Actual MTU: SP A (9000 Bytes), SP B (9000 Bytes)
▼ IO Module 0			Folgsted Speed:
FC port 0	0	0	Auto Mups
FC port 1	0	0	Actual Speed: SP A (1000 Mbps), SP B (1000 Mbps)
FC port 2	0	0	
FC port 3	0	0	Network Addresses:
	100 To 100	1 m 1	

Create NAS Server

ſ

1. Connect to the EMC VNXe Unisphere GUI, click the Settings tab > NAS Servers.



Figure 125 NAS Servers in EMC Unisphere

2. To create NAS Server for NFS Storage, click Create.

Figure 126 Creating NAS Server for NFS Storage

EM	C Unisphere						
Ę	Dashboard	System	Storage	Hosts	Setting	s 📀 Support	
VN	Xe > Settings >	NAS Servers					
NA	5 Servers						
	Name	 IP Address 	Domain,	/Workgroup	Storage Processor	Port	
	Create Detail	s Delete					

3. To configure NAS Server Address, specify the NAS Server name, and then choose the storage pool that we created for NFS-Data from the drop-down list. Specify the IP address and the Subnet Mask for NAS server and choose Link Aggregation 3 from the Ethernet port drop-down list. Click **Next** to proceed.

I

Figure 127 Creating NAS Server - Configure NAS Server Address	
NAS Server Wizard	
Configure NAS Server Address	 >>
Server Name: * NASServer01	·
Storage Pool: StoragePool-NFS-Data	
IP Address: 🐐 10.10.20.10	
Subnet Mask/Prefix Length: * 255.255.255.0	
Gateway:	
Hide advanced	≣
Storage Processor: SP A 🗸	
Ethernet Port: Link Aggregation 3 (Link Up)	
VLAN ID: 0 <click edit="" to=""></click>	
	•
< Back Next > Finish	Cancel Help

4. To configure Share Types, check the Linux/Unix shares (NFS) check box and click Next.



5. Skip the Configure NAS Server DNS and NIS settings and click **Next**. Then, verify the NAS Server settings summary and click **Finish**.

I

Figure 129 Creating NAS Server -	Summary
NAS Server Wizard	
Step 4 of 5	Server Summary 📀 >>
Verify the following NAS server setting	gs:
Server Name:	NASServer01
Storage Processor	SP A
IP Address:	10.10.20.10
Subnet Mask:	255.255.255.0
Gateway:	Not Specified
Advanced Attributes:	► Custom
Storage Pool:	StoragePool-NFS-Data
Support Linux/Unix Shares (NFS):	Configured
Support Windows Shares (CIFS)	Not configured
NIS Domain Name:	
	< Back Next > Finish Cancel Help

I

1

6. After the successful creation of NAS Server, you will see the newly created NAS Server.

Figure 130 Created NAS Server with Created Link Aggregation

EMC Unisphere					
Dashboard 🗮	System	Storage	Hosts Settings	Support	
VNXe > Settings > NAS Se	ervers				
NAS Servers					
! Name	▲ IP Address	Domain/Workgroup	Storage Processor	Port	
Server01	10.10.20.10	Not configured	SP A	Link Aggregation 3	Normal
Create Details D	Delete				

Configure Storage Pool for NFS-Data

Connect to the EMC VNXe Unisphere GUI, Click the Storage tab > Storage Configuration > Storage pools.



2. Specify the pool name in the Name field and Click Next.

Figure 132 Creating Storage Pool - Define Pool

ſ

Storage Pool Wizard	
Specify Pool Name Step 1 of 6	e (2) >>
Specify a name and optional description.	
Name: * StoragePool-NFS-Data Description: Storage pools for NFS Data	
	< Back Next > Finish Cancel Help

3. Check the Performance Tier to use 600GB SAS disks check box and Click Next.

Figure 133 Creating Storage Pool - S	Selecting Storage		
Storage Pool Wizard			
Select Storag	je		<< (9)
Select the storage tiers you want to us	e for the new pool.		
Storage Tier	Disk Type	Unused Disks	Unused Raw Capacity
Extreme Performance Tier	Flash	5	917.2 GB
Performance Tier	SAS	40	20.9 TB
Capacity Tier	NL SAS	0	0 GB (None Available)
Uses SAS disks to provide high perform Extreme Performance (Flash) disks, bu Performance Tier RAID Type: RAID 5 (4+1) (Usable	ance. These disks d ut offer much lower o e capacity: 14.3 TB)	o not provide the san cost per GB of storage <u>Change</u>	ne read/write performance as
	< Bi	ack Next >	Finish Cancel Help

1

4. For SAS Disks, choose Use 35 of 40 disks (14.3TB) from the drop-down list to use 35 SAS disks for creating storage pool for NFS-Datastore and Click on Next.

Figure 134 Creating Storage Pool - Storage Size	
Storage Pool Wizard	
Select Amount of Sto Step 3 of 5	rage 📀 >>
Select the amount of storage for each selected tier. The configuration selected. The maximum number of disks y unused to satisfy the hot spare policy. <u>More information</u> <u>Performance Tier</u>	number of disks you can choose is based on the RAID you can configure will ensure that enough disks are kept
600 GB (10K RPM) SAS Disks: Use 35 of 40 dis	ks (14.3 TB) 🗸
This option uses the system disks. The portion reduced capacity and storage resources in the	of the storage pool that uses these disks will have pool may experience reduced performance.
Total Disks to Configure: 35	
Total Usable Capacity: 14.3 TB	
	< Back Next > Finish Cancel Help

5. Verify the Storage pool creation and click **Finish**.

Γ

Figure 135 Creating Storage Pool - Summary	
Storage Pool Wizard	
Summary Step 4 of 5	< (
The disks will be configured into a new storage pool as indicated below.	
Storage Pool Name: StoragePool-NFS-Data	
Storage Pool Description: Storage pools for NFS Data	
Performance Tier Disks: ► 35 SAS (14.3 TB usable capacity)	
RAID: RAID 5 (4+1)	
Total Disks to Configure: 35	
Total Usable Capacity: 14.3 TB	
< Back Next > Finish Can	cel Help

1

6. Now you will see the Storage pool created for NFS Data.

Figure 136 Verify the Created Storage Pool for NFS Data

a Da	shboard 📷 Sys	tem 🕃 Sto	rage Hosts	Settings	Support		L.
E te⊃st	torage > Storage Configu	ation > Storage Por		100			
age Po	ols	addit > [Storage Por					
	Craph View						
ist viev	di apit view						7 (
1 N	lame 🔺	Total Space	Used Space	Percent Used	Available Space	Subscription	Disks
0	StoragePool-ESXi-Boot	2.0 TB	213.7 GB		9% 1.8 TB	9%	5
0	StoragePool-NFS-Data	14.3 TB	22.5 GB		0% 14.3 TB	0%	35
	2						
Used Spa	ace: 📕 🛛 Available Sp	ace: 📕 🛛 Alert T	hreshold:				2
	_		•				

Create VMware Data Stores

1. Connect to the EMC VNXe Unisphere GUI, then click the **Storage** > **VMware Datastores** > **Create** to create VMware datastore.

Figure 1	37 Ci	reating VI	Mware Da	itastores					
EMC U	nisphere								
	Dashboard		System		Storage	Hosts	Settings	0	Support
VNXe 0	> Storage >	VMware Dat	tastores						
VMware	Datastores								
1	Name		NAS Serve	er	Туре	Descriptio	n	Size	Protection Sch
	_								
Create	e Details	Refresh	Delete						

2. Click the NFS radio button for the Datastore Type and choose the NAS server as NASServer01 from the drop-down list.

Figure 138 Creating VMware Storage - Specifying Datastore Type

VMware Storage Wizard	
Specify Datastore Type Step 1 of 7	?>
Configure the type of datastore to create:	
Datastore Type: O NES	
VMware NFS datastores can be accessed using the NFS protocol.	
NAS Server: NASServer01 🗸	
VMFS	=
VMware VMFS datastores can be accessed using the block protocols.	
Show advanced	
< Back Next > Finish Can	cel Help

3. Specify the name for the VMware datastore and Click Next.

I

Figure 139	Creating VMware Sto	rage - Specify Name					
VMware Sto	rage Wizard						
vm	Specify Name					6	>>
Enter a name	o for the VMware datastore.						
Name	e: * NFS-DataStore1						
Descriptior	N: VMFS Datastore for VSF	EX Server					
			< Back	Next >	Finish	Cancel	Help

1

4. From the Storage Pool drop down list choose the created **StoragePool-NFS-Data**. And specify the datastore size as **6TB** and check the check box **Thin** and click **Next**.

Figure 140 Cr	reating VMware	Storage - Confi	igure Storage
---------------	----------------	-----------------	---------------

VMware Storage	e Wizard
Co Step	onfigure Storage 9 3 of 7 O
Configure the stor	rage for this datastore:
Storage Pool:	StoragePool-NFS-Data (SAS, 14.3 TB free)
Tiering Policy:	Start High Then Auto-Tier (Recommended)
Size: *	 The selected pool is not tiered. The tiering policy will have no effect on the storage resource. TB V Thin
	< Back Next > Finish Cancel Help

5. Skip Configure Snapshot Schedule by clicking the **Do not configure a snapshot schedule** radio button and click **Next**.

Figure 141 Creating VMware Storage - Configure Snapshot Schedule	
VMware Storage Wizard	
Configure Snapshot Schedule Step 4 of 7	?>
Configure a recurring snapshot schedule for automatic data protection:	
O not configure a snapshot schedule.	
A snapshot schedule can be selected at a later time.	
Select a snapshot schedule:	Default Protection
This schedule will create snapshots and synchronize data	
Every day at 01:00, keep for 2 days	
Note: Times are displayed in Local Time (UTC-07:00) in 24-hour format	
< Back Next >	Finish Cancel Help

6. Configure the hosts access by choosing **Read/Write**, allow **Root** from the drop-down list for Default Access setting for both the VSPEX servers.

Figure 142 Creating VMware Storage - Configure Host Access

VMware Storage Wizard		
Configure Host Access Step 5 of 7		?>
Configure which hosts will access this storage:		
Default Access: Read/Write, allow Root The Default Access setting applies to hosts configured in Unisph configured outside Unisphere that can reach the share.	ere with Access set to "	'Use Default Access" and hosts
Y→ Filter for: Protocols File	×	
! Name 🔺 Network Address	Protocol	Access
O-VSPEX-Serve 10.29.180.211	FC, File	Use Default Access
or BO-VSPEX-Serve 10.29.180.212	FC, File	Use Default Access
		Filtered: 2 of 2
	< Back Next >	Finish Cancel Help

7. Verify the VMware Datastore Configuration summary and click **Finish** to confirm.

ſ

Figure 143 Crea	uting VMware Storage - Summary
VMware Storage Wiz	ard
Sum Sum Step 6 of	mary 7 (2) >>
Confirm the following V	'Mware datastore configuration:
Name Description NAS Server Datastore Type Storage Pool Size	 NFS-DataStore1 VMFS Datastore for VSPEX Server NASServer01 (10.10.20.10) NFS StoragePool-NFS-Data 6.0 TB
Thin	: Yes
Tiering Policy	: Start High Then Auto-Tier (Recommended)
Advanced Attributes	: Vse Defaults
Drotection Schedule	None configured
	< Back Next > Finish Cancel Help

I

1

- 8. Repeat the Steps 1 to 7 and create NFS-DataStore2 with 6.0TB size.
- 9. After successful creation, you will see both the VMware Datastores created with 6TB NFS volume.

Figure 144 Verify the Created VMware Datastores

0	Dashboard 📷	System	storage	Hosts	Settings	👩 Support	
Xe	> Storage > VMware [atastores					
-	a Datastanas						
vare	e Datastores						
varo !	e Datastores Name 🔻	NAS Server	Туре	Descr	iption	Size	F
l S	Name VRS-Datastore2	NAS Server NASServer01 (10.10.20	Туре).10) NFS	Descr	iption ire NFS Datastore for V	Size SPE 6.0 TB	F

Mount NFS share on ESXi hosts

1. Select the Home > Inventory > Hosts and Clusters tab in vCenter, expand the VSPEX cluster and select an ESXi host. Click the Configuration tab> Storage > Add Storage.

Figure 145 Add	ding Storage							
File Edit View Inventory Admini	istration Plug-ins Help							
🖸 🔝 🏠 Home 🕨 🛃 Inv	entory 🕨 🗊 Hosts and Clusters					💦 🗣 Search I	Inventory	
5 \$ \$								
Center55.DC.local VSPEX-BO Second by BO-Infra bo-infra-host bo-infra-host Solubs Solubs	bo-vspex-host1 VMware ESKi, 5.5.0, 1331 Getting Started Summary Virtual Machin Hardware Processors	1820 Performance Configu View: Datastores Devi Datastores	ration Tasks & I	Events Alarms Per	missions Maps	Storage Views I	Hardware Status	Rescan All
VC55-W2K12	Memory Storage Networking Storage Adapters Network Adapters	Identification A	Status Normal	Device DGC Fibre Channel.	Drive Type Non-SSD	Capacity 92.50 GB	Free Type 91.55 GB VMFS5	Last Update 3/22/2011
	Advanced Settings Power Management							

2. Click the Network File System radio button for the Storage Type and click Next.

Figure 146 Adding Storage - Select Storage Type

Γ

Ø	Add Storage
Select Storage Type Specify if you want to forr	nat a new volume or use a shared folder over the network.
■ NAS Network File System Ready to Complete	Storage Type Disk/LUN Create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS volume. Network File System Choose this option if you want to create a Network File System.
Help	< Back Next > Cancel

3. Specify the NAS Server IP in the Server field and the VMware Datastore name in Folder field as we created in the EMC Unisphere wizard. Then, specify the Datastore name and click **Next**.

Ø	Add Storage
Locate Network File System Which shared folder will be u	ised as a vSphere datastore?
NAS Network File System Ready to Complete	Properties Server: 10.10.20.10 Examples: nas, nas.it.com, 192.168.0.1 or FE80:01:01:2AA:FF:FE9A:4CA2 Folder: [MFS-Datastore 1] Example: /vols/vol0/datastore-001 Mount NFS read only If a datastore already exists in the datacenter for this NFS share and you intend to configure the same datastore on new hosts, make sure that you enter the same input data (Server and Folder) that you used for the original datastore. Different input data would mean different datastores even if the underlying NFS storage is the same. Datastore Name NFS-DS1
Help	< Back Next > Cancel

1

Figure 147 Adding Storage - Locate NFS

4. After the successful creation, now you will see the new Storage for NFS-Data created.

Figure 148 Verify the Created Storage for NFS-Data

) 🔁 VCenter55.DC.local	bo-vspex-host1 VMware ESXi, 5.5.0, 133 Getting Started Summary Virtual Machi Hardware	1820 nes Performance Configuration Tasks & View: Datastores Devices	Events Alarms Permissions Maps	Storage Views H	Hardware Status
SQLDB	Processors	Datastores		Refresh Delete	Add Storage R
VC55-W2K12	Memory	Identification 🛆 Status	Device Drive Type	Capacity	Free Type
bo-vspex-host1	Storage	👔 datastore1 (1) 🥏 Normal	DGC Fibre Channel Non-SSD	92.50 GB	91.55 GB VMFS5
bo-vspex-host2	Networking	👔 NFS-DS1 📀 Normal	10.10.20.10:/NFS Unknown	5.99 TB	5.99 TB NFS
<u> </u>	Storage Adapters				

5. Repeat the steps from 1 to 3 to create NFS datastore for the remaining VMware Datastore.

i igui e i i>	sigy life el calca 111 s	Educitor e jor un ine i	111000002	ulusione			
 □ I VCenter55.DC.local □ I VSPEX-BO □ I P I BO-Infra 	bo-vspex-host2 VMware ESXi, 5. Getting Started Summary Virt	.5.0, 1331820 ual Machines Performance Configu	ration Tasks &	Events Alarms Permissio	ons Maps Storage Views	Hardware Status	
 BO-VSPEX-Cluster bo-vspex-host1 bo-vspex-host2 	Hardware Processors	View: Datastores Dev Datastores	ces				
VSPEX-VM	Memory	Identification 🗠	Status	Device Drive	e Type Capacity	Free Type	Las
WSPEX-WZKIZ	Storage	datastore1 (2)	🥏 Normal	DGC Fibre Channel Non-	SSD 92.50 GB	91.55 GB VMFS5	3/2
	Networking	NFS-DS1	🦁 Normal	10.10.20.10:/NFS Unkr	iown 5.99 TB] 5.99 TB NFS	3/2
	Storage Adapters	NFS-DS2	📀 Normal	10.10.20.10:/NFS Unkr	iown 5.99 TB	5.99 TB NFS	3/2
	Network Adapters						
	Advanced Settings						
	Power Management						

Figure 149 Verify the Created NFS Datastore for all the VMware Datastore

This concludes the NFS storage for VM datastores.

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 therefor is ideal for managing a branch office VSPEX based solution, where it can provide the management console to drive consistency and compliance across all of the UCS domains.

UCS Central is supplied a 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 deployed as a standalone solution.

Install and Configure UCS Central

In this architecture, we deployed UCS Central.ova appliance on the VMWare Hypervisor and configured in a standalone mode.

Following are the major steps to deploy Cisco UCS central on Remote VSPEX Primary data center.

- 1. Install UCS Central
- 2. Configure UCS Central
- 3. Adding Cisco UCS Managers to Cisco UCS Central

Install UCS Central

As mentioned before, the UCS Central installation media is available as VMware virtual machine OVF template. The UCS central must be deployed on the infrastructure network of the Remote VSPEX datacenter, and *not* on one of the VSPEX ESXi servers. Follow these steps to install VSM VM:

1. From the **Hosts and Cluster** tab in vCenter, select the infrastructure ESX/ESXi host and click **File** Deploy new Virtual Machine through OVF template. Select UCS central OVF, and click **Next**.



Deploy OVF Template		
Source Select the source location.		
Source OVF Template Details Name and Location Disk Format Ready to Complete	Deploy from a file or URL Image: Control UCS-Centrol Ucs-Centrol I.1.2.1 a.ova Image: Device Ima	
Help	< Back Next >	Cancel

2. In the OVF template window, click **Next**. Then on the next window, Select the data center where you want to install the UCS central.

Deploy OVF Template		
Name and Location		
Specify a name and loca	ation for the deployed template	
Source		
OVF Template Details	Name:	
Name and Location		
Disk Format	The name can contain up to 80 characters and it must be unique within the inventory folder.	
Network Mapping		
Ready to Complete	Inventory Location:	
	E IAAS-DC	
	Discovered virtual machine	
Help		el

Figure 151 Deploying OVF Template - Specify Name and Location

1. In the next window, let us restore the default values and click **Next**. In the next window, choose the Destination Network from the drop-down list.

ſ

Deploy OVF Template		_ 🗆 ×
Network Mapping What networks should th	the deployed template use?	
Source OVF Template Details Name and Location	Map the networks used in this OVF template to networks in your inventory	
Disk Format	Source Networks Destination Networks	
Network Mapping	VM Network LabNetwork	
	Description: This network provides connectivity to this virtual machine.	A
		Y
Help	< Back Next > Ca	ancel

1

Figure 152Deploying OVF Template - Network Mapping

2. Verify the deployment settings and check the **Power on after deployment** check box and click **Finish**.

Source DVF Template Details Name and Location Disk Format Network Mapping	When you click Finish, the deployme Deployment settings:	ent task will be started.
teady to Complete	OVF file: Download size: Size on disk: Name: Folder: Host/Cluster: Specific Host: Datastore: Disk provisioning: Network Mapping:	Z:\UCS-Central\ucs-central.1.2.1a.ova 1.2 GB 80.0 GB UCSCentral-DC IAAS-DC Infra.IAAS infrasrv1.iaas.local datastore1 (7) Thick Provision Lazy Zeroed "VM Network" to "LabNetwork"

Figure 153 Deploying OVF Template - Verify in the Ready to Complete Summary

Configure UCS Central

Open up a console window to the Cisco UCS Central VM. Once, the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the VM console window:

- 1. Setup new configuration or restore full-state configuration from backup [setup/restore] prompt, type **setup** and press **Enter**.
- 2. At the "Enter the UCS Central VM eth0 IPv4 Address:" Enter IP address **10.29.150.252** as assigned to Cisco UCS Central and press **Enter**.



- 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).
- 3. At the "Enter the UCS Central VM eth0 IPv4 Netmask:" prompt, enter the netmask 255.255.255.0 as assigned to Cisco UCS Central and press Enter.

- 4. At the "Enter the Default Gateway:" prompt, enter the default gateway **10.29.150.1** as used by Cisco UCS Central and press **Enter**.
- 5. At the "Is this VM part of a cluster(select 'no' for standalone) (yes/no):" prompt, select **no** and press **Enter**.
- 6. At the "Enter the UCS Central VM host name:" prompt, enter the host name as UCSCentral-DC for the Cisco UCS Central VM and press Enter.
- 7. (Optional) At the "Enter the DNS Server IPv4 Address:" prompt, enter the IP address for the DNS server you want to use for Cisco UCS Central and press **Enter**.

If you do not plan to use a DNS server for Cisco UCS Central, leave this blank and press Enter.

8. (Optional) At the "Enter the Default Domain Name:" prompt, enter the domain in which you want to include Cisco UCS Central and press Enter.

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 localdomain.

- 9. 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**.
- **10.** At the "Enforce Strong Password(Yes/No):" prompt, if you want to set up strong password alert, select **yes** and press **Enter**.
- **11.** At the "Enter the admin Password:" prompt, enter the password you want to use for the admin account and press **Enter**.
- **12.** At the "Confirm admin Password:" prompt, re-enter the password you want to use for the admin account and press **Enter**.
- **13.** 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**.
- 14. At the "Confirm Shared Secret:" prompt, re-enter the shared secret and press Enter.
- **15.** 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.

16. For the "Proceed with this configuration, please confirm[yes/no]: prompt, enter yes and press Enter.

After you confirm that you want to proceed with the configuration, the network interface reinitializes with your settings and Cisco UCS Central becomes accessible via the IP address.

2	UCSCen	tral-DC on infrasrv1.iaas.local	_ 🗆 🗵
Fil	e View	VM	
		🕑 🧐 🖾 🕼 🕼 🤣 🤣 🤛	
:		Average disk read speed measured: 212 Disk speed validation - Succeeded	
		Setup new configuration or restore full-state configuration from backup[setup/re store] – setup	
1		Enter the UCS Central VM eth0 IPv4 Address : 10.29.150.252	
1		Enter the UCS Central VM eth0 IPv4 Netmask : 255.255.255.0 Enter the VM IPv4 Default Gateway : 10.29.150.1	
:		Is this VM part of a cluster(select 'no' for standalone) (yes/no) ? no	
		Enter the UCS Central VM Hostname : UCSC-DC	
		Enter the Default Domain Name :	
		Use a Shared Storage Device for Database (yes/no) ? no	
:		Enforce Strong Password (yes/no) ? yes Enter the admin Password :	
		Confirm admin Password : Enter the Shared Secret :	
		Confirm Shared Secret :	
		Statistics Manager – configuration	
		Do you want Statistics collection [yes / no] ? no_	
Tor	elease cu	ursor, press CTRL + ALT	

Adding Cisco UCS Managers to UCS central

I

Γ

1. Launch UCS manager GUI using the UCS mini Virtual IP.



2. Specify the IP address of the UCS Central and Specify the Shared Secret password we created on the previous section.

1

ostname/IP Address [10.29.150.2	52		
Shared Secret:			
All Global			
Infrastructure & Catalog Firmware:	C Local	 Global 	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Time Zone Management:	C Local	 Global 	Determines whether the time zone and NTP server settings are defined locally or comes from Cisco UCS Central.
Communication Services:	C Local	 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:	C Local	 Global 	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management:	C Local	⊙ Global	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined local or in Cisco UCS Central.
DNS Management:	C Local	 Global 	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies:	🔿 Local	⊙ Global	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring:	C Local	⊙ Global	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy:	C Local	 Global 	Determines whether the SEL Policy is defined locally or in Cisco UCS Central.
Power Allocation Policy:	C Local	💿 Global	Determines whether the Global Power Allocation Policy is defined locally or in Cisco UCS Central.
Power Policy:	🔿 Local	💿 Global	Determines whether the Power Policy is defined locally or in Cisco UCS Central.

L

Γ

3. You will see a pop-up confirmation window confirming the registration with UCS central. Click **Accept**.



Figure 156 Confirmation Window for Registering UCS Central

- 4. Now you will see the UCS Central is registered successfully on the UCS Manager.

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 157 Verify the UCS Central Registration

2 3 7 4	>> 🧧 Cor	mmunication Management 🕨 冒 UCS Central 👘	
Equipment Servers LAN SAN VM Admin	UCS Centra	al Providers FSM Faults	
Filter: Communication Managem 💌			Properties
± =	Action	15	Hostname/IP Address: 10.29.150.252
	1 R	egister With UCS Central nregister From UCS Central	Policy Resolution Control
	Status	5	Infrastructure & Catalog Firmware: 💿
	Regist	Repair State:	Time Zone Management: 📀
	Ackno	wledge State:	Communication Services:

5. You can also login to UCS Central web GUI and view the connected UCS Manager for UCS mini and traditional UCS manager in Remote DC.

Figure 158 UCS Domain in UCS Central GUI

allalla				UCS	Domains	Fault Summary						Profemances	Lon Out	About
cisco UCS Central				0	V	A A						Alexandra and a second	a second a second a	
				0	37	8 9								
and the second se				_										
Domaina Servers Network Storag	e Operations Manage	ement Statit	stics L	ogs and Fa	sults Ac	dministration	Import							
Equipment UCS Fault Summary														
Filter: All														
UCS Domains	UCS Domains													
	Summary													
	Guinnary	In Use 7 (70%) of 10		Available	10									
	Servers:	r (res) or re		a facility of	10									
	JUIVUIS.			r										
	UCS Domains Fabric I	Interconnects S	ervers Ch	assis Fex	Status									
	Systems Firmware U	Jsage												
	A Filter (off)	1										Reco	rds: 2 Si	howing: 2
	UCS Name	Platform 0	D. S. D.	Tota 1 .	Free Se	Management	IP UCS VI.	Suspend	Last Re	Invento	Licens	Grace P	Connect	tion State
	VSPEX-FI	ucs-mini		4	3	10.29.180.200) visible	t off	2014-08	ok	license	5	connected	1
	sjc02-151-d20-	ucs-classic		6	0	10.29.150.151	visible	t off	2014-08	ok	license	5	connected	1
							-							

Configure UCS Central for Branch Office Deployment

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

- 1. Configure UCS Central Domain Group
- 2. Configure Pools and Policies
- 3. Configure Global Service Profile Template
- 4. Configure Global Service Profile Instance

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.

Follow these steps for 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 159 Creating a Domain Group

ahah.			UC	S Domains Fau	ult Summary	
cisco UCS Ce	entral		8 0	36	▲ ▲ 8 8	
Domains Servers	Network Storage O	perations Management St	atistics Logs and I	Faults Admi	inistration Im	port
Equipment UCS Fault Sum	mary					
Filter: All		🛗 UCS Domains 🕨 🎒 Dom	ain Groups 🕨			
VCS Domains		Domain Group root				
v 📸 Domain Groups		General Grouped Membersh	ips Faults Events			
ү 🏥 Domain Group	p root	Properties				
Policies	Properties	Name: root				
w- st Ungrouped Doma	Create Domain Group	Description:				
UCS Domain	🖞 Delete					
	Copy XML to Clipboard	Domain Group Members	hip			
		🛋 Filter (off) 🛛 🕂 Assi	gn/Unassign Member			
		UCS Name		Owner		Site

2. Specify the Domain group name and description and Click OK.

ure 160	Creating a Domain Group - Define Domain Group	
Create		•
Create I	Domain Group	Ø
Properties		
Name:	BranchOffice-1	
Description:	Domain group for Branch office in Site 1	
<u> </u>)	
		OK Close

I

1

3. Click Ungrouped Domains and click the discovered Branch office UCS Domain **VSPEX-FI** and in the right pane click **Change Group Assignment**.

Figure 161	Changing Group Assignments
	C

alath	UCS Domains Fault Summary
cisco UCS Central	
	0 36 8 8
Domains Servers Network Storage C	perations Management Statistics Logs and Faults Administration Import
Equipment UCS Fault Summary	
Filter: All	🟥 UCS Domains 🕨 🏥 Ungrouped Domains 🕨
v He UCS Domains	UCS Domain VSPEX-FI
Domain Groups	General Status Faults Events Audits Tech Support Files
Domain Group root	
Domain Group BranchOffice-1	EE Launch UCS Manager In Use Available
Policies	Change Group Assignment
Ungrouped Domains	Re-evaluate Membership Servers: Servers:
UCS Domain sjc02-151-d20-ucs	Full Summany
UCS Domain VSPEX-FI	FW Status: ready Site:
	Domain Group: Owner:
	0 Z 8 3 Last Modified: 2014-08-06T13:16:06 Inventory Status: ok
	Estade Internenments Servers Chossis Eav IO Modules
	Status Hardware Firmware
	S Filter (off)
	ID Status Operability Power Performance Thermal
	Fabric Interconnect A operable
	Fabric Interconnect B operable

4. Choose the Domain Group as **Branch Office-1** and click **OK**.

Figure 162	Changing Group Assignments - Select the Domain Group	
🔺 Change Gr	oup Assignment	□ ×
Change	e Group Assignment for UCS VSPEX-FI	0
O Unass ▼ ∰O Doma	igned in Group root omain Group BranchOffice-1	
	0	K Close

5. Repeat the same steps 1, 2, 3, and 4 to add the discovered VSPEX primary UCS Domain to the domain group created for Primary DC. After the successful creation, you can see both VSPEX Primary DC domain and Branch office Domain added to their respective groups.

Figure 163 Summary Showing Added Domain Groups

quipment UCS Fault Summary								
Filter: All V St UCS Domains V St Domain Groups V St Domain Groups V St Domain Group BranchOffice-1 V St Domain Group BranchOffice-1 V St Domain Group VSPEX-FI St Domain Group VSPEX-Primary-DC V St Domain St Domain Group VSPEX-Primary-DC V St Domain Group VSPEX-Primary-DC V St Domain St	UCS Domains >> 47 C UCS Domain VSPE General Status Fouts 0 Change Group V Re-evaluate M Fault Summary 0 2 Fabric Interconnects S Status Hardware Firm	Acmain Groups ► X-FI Events Audits Te Anager 2 Assignment tembership 8 3 ervers Chassis f ware	Domain Group of Servern Fw Version Fw Version Fw Statur Domain Group Last Modified Fox IO Modules	oot ▶ ∰ Domi 1(25%) of 4 1: • • • • • • • • • • • • • • • • • • •	in Group Branch p-root/domaingr f13:16:06	Available 3 (75%) of 4 oup-BranchOffice-1	Management IP: Description: Site: Owner: Inventory Status:	10.29.180.200 ok
	ID		Status	Operability	Power	Performance	Thermal	
	Fabric Interconne	ect A	1	operable				

Cisco UCS Central Image Management

ſ

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.

altala	and the second se		UCS Domains Fault Summary		Dustances	an Ord Alband Ma
cisco UCS Central			♥ ▲ ▲ 2 32 0 5		Preterences	Log Uur Abour He
Domains Servers Network Stora	age l <mark>Oper</mark> a	ntions Management	I Statistics I Logs and Faults I Adr	ninistration	l Import	
Filter: All ▼ ● Images ● Library ● Sornfigure Downloads From Cisco ● Backup and Import ● Sormain Groups ● License Management	Cibrary of Library of General Fa -Fault Sun O Packages	i Images utts wmary V A 0 0 Downloads	▲ 0			C Refresh
	Drotocol	Uli) 🔂 Downioa	Filmare	Heer	Record	IS: 3 Showing: 3
	Incal	Incalhost	urs-k9-hundle-h-series 3.0.1r B hin	nía	nía	downloaded
	local	Incalhost	ucs-k9-bundle-infra 3 0 1 c A bin	n/a	n/a	downloaded
	local	localhost	ucs-mini-k9-bundle-infra.3.0.1c.A.bin	n/a	n/a	downloaded

Figure 164 Downloading Software Bundles to UCS Central

Cisco UCS Central Fault Management

Cisco UCS Central globally manages Fault and Error management for all registered UCS domains in single pane. Figure 165 shows the UCS faults for VSPEX primary DC site and VSPEX Branch office site managed by UCS central in single pane.

Figure 165	UCS Cen	tral GUI	Showing	Fault	Summary
					~

le alte						UCS Dor	mains Fault Summary					Abo
UCS Central					1			-				~
Domains Servers Network Storage Opera	tions Manager	ment	Stat	istics	Logs a	nd Faults	Administration	Import				
quipment UCS Fault Summary												
UCS Faults												
Fault Summary by Type/Severity					👩 Fau	Its for V	SPEX-FI. Note: Clicking	g on "Affected	Object" launches UCS Manager for that doma	ain		
✓ Re-evaluate Membership	mowledge		Records	: 12	A, FI	iter (off)				Refresh	P	Recor
Туре	0				ID	Sever	Affected Object	Cause	Description	Last Transition	A	1
▼ All Types	1	38	8	8	7992	8	sys/chassis-1/blade	health-led-a	Health LED of server 1/2 shows error. Reaso.	2014-08-06T15:		equ
ij sjc02-151-d20-ucs	0	34	0	5								
VSPEX-FI	1	4	8	3								
▶ sysdebug	0	0	0	0								
▶ operational	0	0	0	0								
► environmental	0	4	0	4								
▶ network	0	24	0	0								
▶ security	0	1	0	0								
► configuration	0	0	0	0								
▶ fsm	0	0	0	0								
				A COLUMN TO A COLUMN								

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.

I

All of the pool types (UUID, MAC, 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 that 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 166 Detecting presence of Overlapping IDs or Duplicate ID

Cisco UCS Central Service Profile Management

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 167

cisco UCS Central	UCS DO	Image: mains Fault Summary Image: main of the second s	Preferences
Domains Servers Network St Fitter: All Image: Compare the service profiles Image: Compare the service profiles Image: Compare the service profiles	orage Operations Management Statistic <u>Servers</u> Local Service Profiles Local Service Profiles	s I Logs and Faults I Administration	i Import
 Global Service Profile Templates Uccal Service Profiles 	Kamo -	Org	@ R
	IAAS-BLADE-TEST-SRV1 IAAS-BLADE-TEST-SRV2 IAAS-BLADE-TEST-SRV3 IAAS-BLADE-TEST-SRV4 IAAS-BLADE-TEST-SRV4 IAAS-RACK-TEST-SRV1 IAAS-RACK-TEST-SRV2	root root root root root	ok ok ok ok ok ok ok ok ok ok

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

Figure 168 Global Service Profiles Shown in UCS Manager

Locally Defined Service Profiles

											_
-Fault Sun	imary V	Δ		3 🔘	🗄 New 🔻	Options		0	🛆 Pendi	ng Activities	<u>E</u> xi
1	4	8	90	>> 🥪 S	5ervers 🕨 🚱	Pools 🕨 🎎 r	oot 🕨 🧠	> Serv	er Pools		
Equipment	Servers LAN SAN	VM Admin		Server	Pools						
	Filter: All	· · ·		Ð	🔍 Filter 🗖	🗢 Export 📚	Print				
a a l			_				Name	;			
	0.0			§	Server Pool de	efault					0
- -	Service Profiles		<u> </u>								
<u> </u>	🎪 root										
	🗄 💽 BO-Site1-VS	PEX-Server-1									
	🗄 💽 BO-Site1-VS	PEX-Server-2									
	🕀 💽 BO-Site1-VS	PEX-Server-3									
	🕀 📑 BO-VSPEX-INF	FRA									
	ትር መስከር መስከር መስከር መስከር መስከር መስከር መስከር መስከ	tions									
	Service Profile Templa	tes									

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

- Existing local Services profiles templates cannot be imported into Cisco UCS Central.
- Existing local service profiles cannot be assigned to Cisco UCS Central.
- Existing local policies (for example local disk policies) can be made Global and therefore be used by global service profile templates.

- Globally defined policies can be used by local service profiles.
- Global Service Profiles can be made local but once localized, these service profiles cannot be assigned back to Cisco UCS Central.



For this solution, 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 taps are also in line with the Cisco UCS Manager's tabs for Server, Network, and Storage. Following the steps to configure Cisco UCS Manager, the 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 both Primary DC Cisco UCS Domain and Branch office Cisco UCS domains from Cisco UCS Central.

Configuring VLANs and VSANs

This section covers the creation of VLAN, VSAN, Pools, Policies, Service profile template and Service profile for Branch office VSPEX servers using UCS Central Management web GUI.

 Launch UCS Central web GUI and click the Domain Group BranchOffice-1. Click LAN Cloud > Create VLANs.

halls.	UCSI	Domains Fault Summary	
Isco UCS Central	⊗ 0	▼ ▲ ▲ 36 8 8	
Domains Servers Network Storage Ope	rations Management Statistics Logs and Fat	ults Administration Impo	rt
Filter: All	Network > 👬 Domain Groups > 👬 Domain Grou	up root 👂 🏄 Domain Group Bra	nchOffice-1 🕨 🧮 LAN 🕨
Domain Groups Domain Group root Domain Group BranchOffice-1	You are creating VLANs common to all available fabric	es of this domain group	
LAN Cloud	Name	VLAN ID	VLAN Sharing
► ➡ LAN ► ⑤ Policies			
► 💮 Pools = VLAN Org Permissions			

I

1

Figure 169 Creating VLANs in UCS Central

- 2. Specify the VLAN Name and VLAN ID. Click OK.
- Figure 170 Creating VLANs Window

🚖 Create	⊐ ×
Create VLANs	0
You are creating VLANs common to all available fabrics of this domain group	
Create: Single VLAN Multiple VLANs 	
Name Overlap Check: Strictly Enforced Optional 	
VLAN Name: vSphereMgmt	
ID Overlap Check: Strictly Enforced Optional 	
Multicast Policy Name:	
Multicast Policy Instance: Multicast policy name is resolved from UCS domain, on deployment	
ОК	Close

- **3.** Repeat these steps to create VLANs for Storage VLAN20, VM-Data VLAN30 and vMotion -VLAN40.
- 4. After the successful VLAN creation, you can see all the created VLANs.
| dealer- | | JCS Domain | s Fault Summ | ary | |
|---|--------------------------------|----------------|------------------|--------------------|--------------------------|
| UCS Central | 5 | 56 | 8 | ▲
9 | |
| Domains Servers Network Storage Op | perations Management Stati | stics Log | s and Faults | Administration | Import |
| Filter: All | 🗮 <u>Network</u> 🕨 🏥 Domain Gr | oups 🕨 🏄 I | Domain Group r | root 🕨 🎁 Dom | ain Group BranchOffice-1 |
| V I Network | LAN Cloud | | | | |
| Bomain Groups | You are creating VLANs com | non to all ava | ilable fabrics o | of this domain gro | up |
| Domain Group root Domain Group BranchOffice-1 | 🕰 Filter (off) 🛛 🛨 Crea | e VLANs | | | |
| ↓ ∃ LAN | Nai | ne | | VLAN ID | VLAN Sharin |
| LAN Cloud | Storage | | | 20 | none |
| 🕨 🍰 Domain Group VSPEX-Primary-DC | VM-Data | | | 30 | none |
| LAN | vMotion | | | 40 | none |
| ▶ ∰ Policies
▶ ∯ Pools | vSphereMgmt | | | 11 | none |

Figure 171 Created VLANs are Shown in UCS Central

5. Click the VLAN properties, we have access permissions for **Org-root**.

Figure 172 Setting Org Permissions

Γ

Domains Servers Network Storage Operat	tions Management Statistics Logs and Faults Administration Import
Filter: All	Network Demain Groups Demain Group root Demain Group BranchOffed LAN Cloud You are creating VLANs common to all available fabrics of this domain group Filter (off) Create VLANs Properties Delete Froperties Properties Properties Properties Org Permissions Faults Events Modifying org permissions will provide access to all vlans with name 'S Org Levels Permitted Access To VLANs with Name 'Storage' Context: Modify VLAN Org Permissions > Selected: org-root @

6. To create VSAN, Click the **Domain Group BranchOffice-1** and Click **SAN Cloud** > **Create VSAN**.

Figure 173 Crea	ing VSAN in	UCS Central
-----------------	-------------	-------------

alualu		UCS D	omains	Fault Sum	mary		
cisco UCS Central		8	36	<u>A</u>	A		
Domains Servers Network Storage	Operations Management Statistics I	ogs and Faul	ls A	dministratio	on Import		-
Filter: All	🗐 Storage 🕨 🎒 Domain Groups 🕨 🏥	Domain Group	root 🕨	Doma	in Group BranchOffice-	1 🕨 🗮 <u>SAN</u> 🕨	
▼	SAN Cloud						
Domain Groups	Fabric A Fabric B						
Domain Group BranchOffice-1	🕰 Filter (off) 🛛 🔠 Create VSAN						
SAN	Name		-	ID	if Type	if Role	_
SAN Cloud							
Fabric F							
Pomain Group Vs 🖉 Sort Descendin	9						
	ipboard						
SAN Cloud							
Poiles							

1

7. Specify the VSAN name and for FC zoning settings, click **Enabled** radio button and Specify the VSAN ID and FCoE ID.

Figure 174 Creating VSAN Window

📥 Create	□ ×
Create VSAN	0
Name Storage]
FC Zoning: O Disabled Enabled Do NOT enable zoning for this VSAN, if the fabric interconnect is connected to an on the same VSAN.	upstream switch that has zoning enabled
Enter the VSAN ID that maps to this VSAN.	
Enter the VLAN ID that maps to this VSAN.	
	OK Close

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

UCS D 1111111 **UCS** Central cisco 8 5 56 8 9 Servers | Network | Storage | Operations Management | Statistics | Logs and Faults | Administration Import Domains SAN Storage 🕨 🏄 Do ain Groups 🕨 🏄 Domain Group root 🕨 👬 Do ain Group BranchOffice-1 Filter: All -SAN Cloud ∃ Storage pomain Groups bric A Fabric B Bomain Group root A Filter (off) Create VSAN Properties 🕆 Delete Bomain Group BranchOffice-1 Transport SAN Name ID if Type if Role Bomain Group VSPEX-Primary-D E SAN

Figure 175 Verify the Created VSAN for Storage

Configuring Pools and Polices

I

- 1. Launch UCS Central web GUI and Click Network > Pools > IP Pools > global-ext-mgmt and click Create a Block of IPv4 Addresses.
- Figure 176 Creating a Block of IPv4 Addresses

allalla		UCS Domain	ns Fault Sum	mary
cisco UCS Central		S 90	△ 9	8
Domains Servers Network Storage O	perations Management Statistics Log	s and Faults A	dministration	Import
Pilter: All Image: Second state st	General IP Blocks IP Addresses Faults Actions Create a Block of IPv6 Addresses Create a Block of IPv6 Addresses Delete	Events Properties Name: Description: Usage:	global-ext-n	ngmt

2. Specify the IP range for the IP Pool for managing the UCS blades KVM console. And click OK.

Figure 177 Creating a Block of IPv4 Addresses Window	
🚖 Create	— ×
Create a Block of IPv4 Addresses	0
From: 9 10 . 29 . 180 . 225 Size: 8	
Subnet: 255.255.0	
Default Gateway: 0 . 180 . 1	
Primary Dns: 0.0.0.0	
Secondary Dns: 0.0.0.0	
Scope: public 💌	
ID Range Qualification Policy Create ID Range Qualification Policy	
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.	
ID Range Qualification Policy:	
ОК	Close

1

3. To create UUID pools, click Servers > Pools > UUID Suffix Pools and then click Create UUID Suffix Pool.

Figure 178 Creating UUID Suffix Pool

alada		UCS	Domains	Fault Sum	mary
cisco UCS Central		8	V	Δ	
		5	56	8	9
Domains Servers Network Stora	ge Operations Management	Statistics	i Logs	and Faults	Administr
Filter: Pools	🤝 <u>Servers</u> 🕨 🍄 <u>Pools</u> 🕨 🛕	root 🕨			
▼ _≪ Servers	Kilter (on) [Create L	UID Suffix	Pool		
Pools	Name				Siz
v					
Server Pools					
UUID Suffix Pools					
Sub-Organizations					

4. In the General tab, specify the UUID Pool name and description. Click OK.

Figure 179	Creating UUID Suffix Pool Window	
🔺 Create		□ ×
Create	UUID Suffix Pool	0
General UUID B Properties Name Description	Iocks : VSPEX-UUID-Pool-BO-Site1 : UUID pools for VSPEX servers in Branch ofice Site1	
Prefix	• Derived () Other	
		OK Close

5. In UUID Blocks, click Create a Block of UUID Suffixes.

Figure 180 Creating a Block of UUID Suffixes

🗼 Create			□ >	ĸ
Create	UUID Suffix	Pool	0	
General UUID B	locks			
Kilter (off)	E Create a Block of U	UID Suffixes	Records: 0 Showing: 0	
	Name	From	То	
			OK Close	J

6. Specify the UUID range as shown below and click **OK**.

Γ

Figure 181 Creating a Block of UUID Suffixes Window	
A Create	×
Create a Block of UUID Suffixes	0
From: 700D-00000000001 Size: A ID Range Qualification Policy Image: Create ID Range Qualification Policy 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. ID Range Qualification Policy:	
ОК	lose

1

7. To create UUID pools, click Network > Pools > MAC Pools and click Create MAC Pool.

Figure 182 Creating MAC Pools						
		UCS	Domains	Fault Sum	mary	
cisco UCS Central		8	V	Δ		
		0	36	8	8	
		_				
Domains Servers Network Storag	e Operations Management Statistics	Logs and F	aults A	dministratio	on Import	
Filter: All						
▼	MAC Pools					
🕨 🍰 Domain Groups	A Filter (off)					
Policies						-
Pools	Name			Size		-
to the root	global-default		0			0
Lig ID Usage						
▶ global-default						
Sub-Organizations						
VLAN Org Permissions						

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

Figure 183	Creating MAC Pools Window	
📥 Create		□ ×
Create I	MAC Pool	0
General MAC Blo	cks	
Name:	VSPEX-MAC-Pools-BO-Site1	
Description:	MAC Pools for VSPEX servers in Branch office Site1	
		OK Close

9. In the MAC Blocks tab, click Create a Block of MAC Addresses and then click OK.

Figure 184	Creating a Block of M	AC Addresses		
🛕 Create				□ ×
Create	MAC Pool			0
General MAC B	locks			
A Filter (off)	E Create a Block of N	AC Addresses	Records: 0	Showing: 0
	Name	From	То	
2				
			ОК	Close

10. Specify the MAC range and size. Click OK.

Γ

Figure 185 Creating a Block of MAC Addresses Window	
A Create	□ ×
Create a Block of MAC Addresses	0
From: 00:25:B5:07:0D:00 Size: 40	
Warning:Pools containing an ID block referencing ID range qualification policy can only be used by local service pro Global service profiles cannot use pools referencing this policy.	files.
ID Range Qualification Policy:	
	OK Close

1

11. To create WWxN Pools for WorldWideNodeName and WorldWidePortName. Click Storage > Pools > WWN Pools > WWxN and click Create WWxN Pool.

Figure 186 Creating WWxN Pool

allalla		UCS	Domains	Fault Sum	mary
cisco UCS Central		8	V	Δ	
		5	56	8	9
Domains Servers Network Storag	Operations Management	Statistics	Logs	and Faults	Adminis
Filter: Pools	📕 Storage 🕨 🌵 <u>Pools</u> 🕨 🛕	root 🕨 🍕	WWN Po	ols 🕨	
	WWxN				
			_		
V Pools	🛋 Filter (on) 📑 Create V	WxN Pool			
V····· dia root		Name			
IQN Pools					
WWN Pools					
ID Usage					
🕨 💮 WWNN					
WWPN					
🖌 💮 WWxN					
Sub-Organizations					

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

🚖 Create	□ ×
Create WWxN Pool	•
General WWN Initiator Blocks	
Properties	
Name: VSPEX-WWxN-Pool-BO-Site1	
Description:	
Purpose: Node and Port WWN Assignment	
Max Ports per Node: 3 Ports Per Node	
ОК	Close

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

Figure 188	Creating WWxN Initia	tor Blocks			
📥 Create					□ ×
Create	WWxN Pool				0
General WWN I	nitiator Blocks				
A Filter (off)	E Create Block		Records:	0 Showing	j: 0
	Name	From	То		
			ОК	Clo	se

14. Specify the range for the Block and click **OK**.

Γ

Figure 189 Creating WWxN Block Window	
🗻 Create	.□ ×
Create Block	0
From: 20:00:00:25:B5:06:0D:00 Size: 48 ID Range Qualification Policy Image: Create ID Range Qualification Policy 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. ID Range Qualification Policy: ID Range Qualification Policy: Image:	
OK	Close

1

15. After the successful creation, the WWN block will be created.

Figure 190	Verify the Created W	WWxN Initiator Block
0		

📥 Create					×
Create V	WXN Pool			(3
General WWN Initi	iator Blocks				
A Filter (off)	+ Create Block		Records: 1	Showing:	1
N	lame	From	То		
[20:00:00:25:B5:06	6:0D:00-20:00:00:25:B5	20:00:00:25:B5:06:0D:00	20:00:00:25:B5:06:0D:2F]	
			ОК	Close	

16. To create Server Pool, click Servers > Pools > Server Pools and click Create Server Pool.

Figure 191 **Creating Server Pool** UCS Domains Fault Summary 11 111 11 **UCS** Central 8 CISCO 0 36 8 8 Servers Network | Storage | Operations Management | Statistics | Logs and Faults Administration | Import Domains 🥪 Servers 🕨 🚸 Pools 🕨 🛕 root 👂 Filter: All -Server Pools 🛛 🥪 Servers 5 Global Service Profiles A Filter (off) E Create Server Pool Global Service Profile Templates Name Size 5 Local Service Profiles Create Server Pool Local Service Profile Templates S Policies Pools 🔻 🛕 root Server Pools UUID Suffix Pools Sub-Organizations Schedules

17. In the **General** tab, specify the Server pool name and description and click **Finish** to create a new server pool. We will add the compute resources in this pool dynamically based on the Server Pool Policy.

Figure 192 Creating Server Pool - Main

I

🚖 Create Se	erver Pool	×□
Create	e Server Pool	0
Main	You must enter the name for the server pool to continue.	
Add Server	Name VSPEX-ServerPool-BO-Site1 Description: Server pool for Branch office Site1	
	< Prev Next > Finish (Close

 To create Server Pool Policy Qualification. Click Servers > Policies > Server Pool Policy Qualifications and click Create Policy Qualification.

ulu.		JCS Domains Fault Summa	ry
co UCS Central			
	•		•
mains Servers Network Storage Op	erations Management Statistics Logs an	d Faults Administration	Import
Filter: Policies	Servers > S Policies > A root >		
Servers	Server Pool Policy Qualifications		
V SPolicies	Kilter (off)		
∳å root	Name	Max	Model
Adapter Policies	▶ 🗐 all-domain		
BIOS Policies			
Boot Policies			
Host Firmware Packages			
IPMI Access Profiles			
SCSI Authentication Profile			
Local Disk Config Policies			
Maintenance Policies			
Sover Control Policies			
Scrub Policies			
Serial over LAN Policies			
Server Pool Policies			
Server Pool Policy Qualifications			
🗐 🗐 all-domain			
Figure Streshold Policies			
VNIC/vHBA Placement Policies			
Sub-Organizations			

1

Figure 193 Creating Server Pool Policy Qualification

19. Specify Policy name and description and click Create Memory Qualification.

Figure 194 Creating Policy Qualification Window

🔶 Create			
Create Policy Qualifica	tion		
Name: Min-Memory			
Description: Min Memory Qualification for	VSPEX Servers in Branch office Site1		
Actions	ualifications		
🕂 Create Domain Qualification	Filter (off)		
Create Adapter Qualification	Name	Max	Model
Create Memory Qualification			
Create Processor Qualification			
E Create Storage Qualification			
E Create Server PID Qualification			

20. Uncheck the check box Min Cap(MB) and specify the minimum memory value in MB for 128GB. Click OK.

0	· · ~ ·			
📥 Create				⊐ ×
Create M	emory Qualification	on		0
Clock (MHz):	Unspecified	Latency (ns):	Unspecified	
Min Cap (MB):	Unspecified	Max Cap (MB):	Unspecified	
Width:	Unspecified	Units:	Unspecified	
Speed:	✓ Unspecified			
			ОК	Close

Figure 195 Creating Memory Qualification Window

21. After the successful creation, you can see the created Memory Qualification.

Figure 196	Verify the Created Memory	Qualification
------------	---------------------------	---------------

ſ

	1								
Name:	Min-Memory								
escription:	Min Memory Qualificai	ton for VSPEX Servers in Branch office Site1							
tions		Qualifications							
Create Dorr	nain Qualification	A Filter (off)							Records
Create Adap	pter Qualification	Name	Max	Model	From	То	Architecture	Speed	Steppin
Croste Mar	non Qualification	S Memory Qualification						unspecified	
Create Men	nory Quannoauon								
Create Proc	essor Qualification								
Create Stor	age Qualification								
Create Sen	er PID Qualification								
Cieate Serv	er Pib Quanication								

22. To create Server Pool policy, click Servers > Policies > Server Pool Policies and click Create Server Pool Policy.

<i>Creating Server Pool Pol Creating Server Pool Pol</i>	icy		
UCS Central	0 0	S Domains Fault Summary Image: Sum	
Domains Servers Network Storage Op Filter: Policies	erations Management Statistics Logs and F ■ Servers ▶ S Policies ▶ A root ▶ Servers Pack Policies	aults Administration Impo	rt
v ⇔ Servers v S Policies v k root	Generation Policies Generation Policies Generation Policy Name	Tarret Pool Da	Qualificati
Adapter Policies BIOS Policies Boot Policies Boot Policies Si Host Firmware Packages Difference Policies	Raine	larger PON DI	quanneau
 SiscSI Authentication Profile Local Disk Config Policies Maintenance Policies Power Control Policies 			
Scrub Policies Serial over LAN Policies Server Pool Policies Server Pool Policy Qualifications Sall-domain			

1

23. Specify the Server pool policy name and description. Then choose the respective Target Pool and Qualification that we have created earlier and click **OK**.

Figure 108	Creating	Sorvor	Pool	Policy	Window
rigure 170	Creating	Server	1 001	1 out y	muuow

🚖 Create	□ ×
Create Server Pool Policy	0
Name: SP-Policy-VSPEX	
Target Pool: VSPEX-ServerPool-BO-Site1 (3/3)	
Target Pool Instance: org-root/compute-pool-VSPEX-ServerPool-BO-Site1	
Qualification: Min-Memory Create Policy Qualification	
Qualification Instance: org-root/blade-qualifier-Min-Memory	
Description: or VSPEX Srv in Branch office Site	
Estimate Impact OK	Close

24. After the successful Server Pool Policy creation, you will see the created VSPEX Servers are added dynamically to the Branch Office Site.



Figure 199 Verify the Dynamically Added Servers to the Branch Office Site

Configuring Global Service Profile Template

I

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.

 To create Global Server Profile Templates for Branch office VSPEX servers, launch the UCS Central Web GUI. Click Servers > Global Service Profile Templates > root and then click Create Service Profile Template.



alate			UCS D	omains Fault S	Summary	
cisco UCS Central			⊗ 0	▼ ▲ 36 8	▲ 9	
Domains Servers Network Storage O	Operations Manageme	nt Statistics Lo	gs and Fault	s Administ	ration Impo	ort
Filter: Global Service Profile Templates	🗢 Servers 🕨 🎹 🤇	Global Service Profile Tem	plates 🕨			
V 🥪 Servers	root					_
V- Global Service Profile Templates	General Sub-Organ	nizations Global Servic	e Profile Te	mplates Statu	s Faults Even	ts
Sub-Organizations	A Filter (off)	E Create Service Prof	ile Template			
P- The Out-Organizations						Name

2. Specify the Service Profile Template name and description and click the **Updating Template** radio button for Type. Then, choose the UUID Pool that we have earlier and Click **Next**.

General	You must enter the name for the Service Profile Template and specify the template type. You can also specify how a UUID will be assigned to this template a	nd enter a description.
Networking Storage vNIC/VHBA Placement Boot Order Maintenance Policy Server Assigment Policies	Name: VSPEX-SP-Template-BO-Site1 Description: Service Profile Template for VSPEX Servers in Branch office Site1 Type: Initial-template • updating-template • UUID Assignment • Create UUID Suffix Pool Indicate the method to use to assign UUIDs to the server. • Hardware Default • UUID Pool global-default (0/0) • VSPEX-UUID-Pool-BO-Site1 (6/8)	

1

Figure 201 Creating Service Profile Template - General

3. Choose the Configuration Type as vNICs – Expert Mode from the drop-down list and click Create vNIC. Click Next.

sale Serv	nce Prome remplate		
al	Optionally specify dynamic vNic Connection policy and LAN cont	figuration information.	
rking	Dynamic vNIC Connections Greate Dynamic vNIC Connection Policy		
e HBA Placement	Indicate the whether dynamic vNICs should be used and if so the poli Dynamic vNIC Connection Usage: Do not u	Icy to be used.	
roer nance Policy Assigment S	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 Filter (off) Create vNIC	e to connect to the LAN.	Records:
	Name	MAC Address	Fabric ID
	- ISCSI vNICs		

Figure 202 Creating Service Profile Template - Networking

4. To create a system vNIC for Fabric A, enter System-A as the vNIC name, choose the created MAC Pool, then choose the Fabric ID as Fabric A and specify MTU size as 9000. Then, Select vMotion and vSphereMgmt vLANs with vSphereMgmt as native VLAN. Then choose, VMware for the adapter policy.

operties					
N	System-A				_
Name:	Cycloin / C				_
MAC Address Assignment:	O Hardware De	fault			
	• Using Pool	VSPEX-MAC-Poo	ols-BO-Site1 (40/40) 🔻 Create MA	C Pool 🔛 Reset Pool	
	Instance:				
	Address:	derived			
Use vNIC Template:					_
)etails					
Details Fabric ID:	ОВ				
Fabric ID: A) B				
Details Fabric ID: O A Failover: I Ena) B ble				
Details Fabric ID: ⊙ A Failover: ☑ Ena MTU: 9000	О В ble				
Details Fabric ID: • A Failover: Failover: Ena MTU: 9000 Permitted VLANs	O B ble		Selected VLANs		
Details Fabric ID: • A Failover: Fina MTU: 9000 Permitted VLANs Filter (off) •	O B ble → Refresh Records:	4	Selected VLANs	≫ Refresh Records: 0	0
Details Fabric ID: A Failover: Filover: Ena MTU: 9000 9000 9000 9000 9000 9000 9000 90	B ble Refresh Records:	4	Selected VLANs	≫ Refresh Records: 0 Set Native	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage	B ble Refresh Records: ne	4	Selected VLANs Name VMotion	Refresh Records: 0 Set Native	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage VM-Data	B B B Refresh Records: ne	4	Selected VLANs Name VMotion vSphereMgmt	Refresh Records: 0 Set Native O O O	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage VM-Data Motion	O B ble Refresh Records: ne	4 Select >	Selected VLANs Name VMotion vSphereMgmt	Refresh Records: 0 Set Native	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage VM-Data Motion /SphereMgmt	O B ble Refresh Records: ne	4 Select >	Selected VLANs Name VMotion vSphereMgmt	Refresh Records: 0 Set Native	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage VM-Data Motion /SphereMgmt	O B ble Refresh Records: ne	4 Select >	Selected VLANs Name VMotion vSphereMgmt	Refresh Records: 0 Set Native	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage VM-Data Motion /SphereMgmt	O B ble Refresh Records: me	4 Select >	Selected VLANs Name VMotion vSphereMgmt	Refresh Records: 0 Set Native	0
Details Fabric ID: ● A Failover: ✓ Ena MTU: 9000 Permitted VLANs ✓ Filter (off) Nan Storage VM-Data Motion /SphereMgmt	O B ble Refresh Records: me	4 Select >	Selected VLANs Name VMotion vSphereMgmt	Refresh Records: 0 Set Native	0

Figure 203	Networking - Properties	s for System-A
115416 205	nerworking - I roperite.	s joi bysiem-1

L

Γ

5. Similarly, create one more vNIC for fabric B as System-B with exact same properties on Fabric B.

Figure 204

roperties (Syst	em-B)	
roperties		
Name:	System-B	
MAC Address Assignment:	O Hardware Default	
	Using Bool VSPEX-MAC. Pools BO-Site1 (40(40)	In MAC Bool III Popot Bool
		IS MAG FOOI DE RESELFOOI
	Instance:	
	Address: derived	
Line while Templeter		
Use vNIC Template:		
Use vNIC Template: Details Fabric ID: \(\cap A\)		
Use vNIC Template: Details Fabric ID: O A	D)B	
Use vNIC Template: Details Fabric ID: A G Failover: Failover:		
Use vNIC Template: Details Fabric ID: A Failover: Fanab MTU: 9000	B e	
Use vNIC Template: Details Fabric ID: A G Failover: Finab MTU: 9000 Permitted VLANS	B e Selected VLANs	
Use vNIC Template: Details Fabric ID: A G Failover: Finab MTU: 9000 Permitted VLANs Filter (off)	B B B Refresh Records: 4	֎ Refresh Records: 0
Use vNIC Template: Details Fabric ID: A G Failover: Finab MTU: 9000 Permitted VLANs Filter (off) Nam	B B Refresh Records: 4 e Name	
Use vNIC Template: Details Fabric ID: A G Failover: Finab MTU: 9000 Permitted VLANs Filter (off) Nam Storage	B B Refresh Records: 4 B Name VMotion	Refresh Records: 0 Set Native
Use vNIC Template: Details Fabric ID: A G Failover: Finab MTU: 9000 Permitted VLANs A Filter (off) Nam Storage VM-Data	B B Refresh Records: 4 e Name VMotion vSphereMgmt	
Use vNIC Template: Details Fabric ID: A C Failover: Filenab MTU: 9000 Permitted VLANs Filter (off) Nam Storage VM-Data VMotion	B B Refresh Records: 4 e Name VMotion vSphereMgmt Select >	
Use vNIC Template: Details Fabric ID: A C Failover: Finab MTU: 9000 Permitted VLANs Filter (off) Nam Storage VM-Data vMotion vSphereMgmt	B B Refresh Records: 4 e Name VMotion vSphereMgmt Select >	Refresh Records: 0 Set Native O O
Use vNIC Template: Details Fabric ID: A C Failover: Finab MTU: 9000 Permitted VLANS A Filter (off) Nam Storage VM-Data vMotion vSphereMgmt	B B Refresh Records: 4 B Select > Selected VLANs VMotion vSphereMgmt	Refresh Records: 0 Set Native O O
Use vNIC Template: Details Fabric ID: A C Failover: Finable MTU: 9000 Permitted VLANS Filter (off) Nam Storage VM-Data vMotion vSphereMgmt	Be Be Selected VLANs Select > Name VMotion vSphereMgmt	Refresh Records: 0 Set Native O O
Use vNIC Template: Details Fabric ID: A C Failover: Finable MTU: 9000 Permitted VLANS Filter (off) Nam Storage VM-Data vMotion vSphereMgmt	Be Be Selected VLANs Select > Name VMotion vSphereMgmt	Refresh Records: 0 Set Native O O

1

1

Networking - Properties for System-B

6. Repeat the above steps 4 to 6 to create vNICs for VM-Data and Storage o Fabric A and Fabric B. Following table summarizes all the VNICs created on the service profile:

vNIC Name	MAC Address Assignment	VLANs	Native VLANs	Fabric	MTU	Adapter Policy	QoS Policy
System- A	MAC pool	vSphereMgmt, vMotion	vSphereMgmt	А	9000	VMware	JumboMT U
System- B	MAC pool	vSphereMgmt, vMotion	vSphereMgmt	В	9000	VMware	JumboMT U
Storage- A*	MAC pool	Storage	Storage	А	9000	VMware	JumboMT U
Storage- B*	MAC pool	Storage	Storage	В	9000	VMware	JumboMT U

Table 9 Summary of all the vNICs Created

vNIC Name	MAC Address Assignment	VLANs	Native VLANs	Fabric	MTU	Adapter Policy	QoS Policy
Data-A	MAC pool	VM-Data	VM-Data	А	1500	VMware	-
Data-B	MAC pool	VM-Data	VM-Data	В	1500	VMware	-

 Table 9
 Summary of all the vNICs Created

7. Once after vNIC creation, click Next.

ſ

Figure 205 Creating Service Profile Template - Networking

🚖 Create				□ ×
Create Serv	vice Profile Template			0
General	Optionally specify dynamic vNic Connection policy and LAN	l configuration information.		
Networking Storage vNIC/vHBA Placement Boot Order Maintenance Policy Server Assigment Policies	Dynamic vNIC Connections Create Dynamic vNIC Connection Policy Indicate the whether dynamic vNIC should be used and if so th Dynamic vNIC Connection Usage: Do LAN Connectivity Do Create LAN Connectivity Policy Indicate the method to use to configure LAN Connectivity. Configuration Type: vNICs - Expert model VNICs Click Create to specify one or more vNICs that the server should be used to an experiment of the server should be used and if the server should be used to an experiment of the server should be server should be used to an experiment of th	not use		
	Name	MAC Address	Fabric I	D
	► - Storage-A ► - Storage-B	derived derived	A-B B-A	
	System-A	derived derived	B-A A-B	
	MData-B	derived	B-A	
	ISCSI vNICs			
			< Prev Next >	Finish Close

8. To create vHBAs, choose Configuration Type as vHBAs – Simple Mode and choose the Global Pool that we created earlier and specify the vHBA name for Fabric A and Fabric B. And then, specify the VSAN name for storage.

🏯 Create		□ ×
Create Serv	vice Profile Template	0
General	Optionally specify the SAN configuration information.	-
Networking	Note: If no selection is made, the default Storage configuration policy will be assigned.	
Storage vNIC/VHBA Placement Boot Order Maintenance: Policy Server: Assignment Policies	SAN Connectivity Create SAN Connectivity Policy Indicate the method to use to configure SAN Connectivity. Configuration Type: vHBAs - Simple Mode World Wide Node Name (WWNN) Indicate the method to use to configure WWNN. Derived O Global Pool VSPEX-WWXN-Pool-BO-Site1(Create WWN Pool Reset Pool VHBAs VHBA 0 (Fabric A) Name: vHBA-A VSAN: Storage SC	
	< Prev Next > Finish	Close

1

Figure 206 Creating Service Profile Template - Storage

9. In the next window, keep the Assignment Method as **Default** and Click Next.

Figure 207	Creating Service Profile Template - vNIC/vHBA Placement

Create					
Create Ser	vice Profile Template		(
General	Optionally specify how vNICs and vHBAs are placed	on physical network adapters.			
letworking	- Placement Method				
torage	Create vNIC/vHBA Placement Policy				
lorage	Indicate the method to use to assign vNICs and vHBAs	to physical network adapters.			
NIC/vHBA Placement	Assignment Method: Let System	Perform Placement			
pot Order	-				
alatananan Dallau	PCI Order				
annenarice Folicy	System will assign VNICs and VHBAs based on their P	CI order. To change assignment change the order of the VNIC:	s and VHBAs in the table below.		
erver Assigment	🍕 Filter (off) 🕋 🛊 🖶		Records: 8 Showing: 8		
olicies	Name	Address	PCI Order		
	vNIC System-B	derived	unspecified		
	vNIC System-A	derived	unspecified		
	vNIC Storage-A	derived	unspecified		
	vNIC VMData-B	derived	unspecified		
	vNIC VMData-A	derived	unspecified		
	vNIC Storage-B	derived	unspecified		
	vHBA vHBA-A derived unspecified				

10. Choose the Boot policy as SAN-boot as created earlier and click Next.

Create Serv	ice Frome remplate						
General	Optionally specify the Boot Policy for this S	ervice Profile.					
Networking	Boot Order Policy						
vNIC/vHBA Placement	Identify the boot order policy to be applied to the server. Configuration Type: Boot Policy -						
Boot Order	Boot Policy: SAN-boot						
Maintenance Policy Server Assigment Policies	Hoot Holiev Instance: org	not hoot policy SA					
Maintenance Policy Server Assigment Policies	Properties Description: ES Reboot on order change: Enforce device names: Boot Mode: leg Boot Order	Xi SAN boot policy acy	r for VSPEX Servers in Branch office	Site1		Records:	
Maintenance Policy Server Assigment Policies	Properties Description: ES Reboot on order change: Enforce device names: Boot Mode: leg Boot Order	Xi SAN boot policy acy Order	v for VSPEX Servers in Branch office	Site1	LUN ID	Records:	
Maintenance Policy Server Assigment Policies	Properties Description: ES Reboot on order change: Enforce device names: Boot Mode: leg Boot Order & Local CD/DVD	XI SAN boot policy acy 0rder 1	v for VSPEX Servers in Branch office	Site1	LUN ID	Records:	
Maintenance Policy Server Assigment Policies	Properties Description: ES Reboot on order change: ✓ Enforce device names: ✓ Boot Mode: leg Boot Order ● Local CD/DVD ▼ = SAN ▼ = SAN	XI SAN boot policy acy <u>Order</u> 1 2	r for VSPEX Servers in Branch office	Site1	LUN ID	Records:	
Maintenance Policy Server Assigment Policies	Boot Properties Description: ES Reboot on order change: ✓ Enforce device names: ✓ Boot Mode: leg Boot Order @ Local CD/DVD V = SAN V = SAN primary = SAN Target primary	Xi SAN boot policy acy 1 2	v for VSPEX Servers in Branch office	Site1	LUN ID	Records: WWN 50:06:01:64:08:E0:03:68	

Figure 208 Creating Service Profile Template - Boot Order

11. In the next window, keep the Maintenance Policy as **Default** and click **Next**.

Figure 209	Creating	Service	Profile	Template -	Maintenance	Policy
1 15410 207	creating	Surnee	I i OjiiC	remptuic	mannee	1 oncy

🚖 Create		⊐ ×
Create Serv	ice Profile Template	0
General Networking Storage vhtC/vHBA Placement Boot Order Maintenance Policy Server Assignent Policies	Optionally specify how disruptive changes (such as reboot, network interruptions, firmware upgrades) should be applied to the system. Maintenance Policy Identify the maintenance Identify the maintenan	
	< Prev Next > Finish	Close

12. Choose the created Server Pool and Qualification. Click Next.

ſ

🚊 Create		□ ×
Create Serv	vice Profile Template	0
General Networking Storage vNIC/vHBA Placement Boot Order Maintenance Policy Server Assigment 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 v Power state to apply on assignment: down <i>up Server Pool Create Policy Qualification Identify the Server Pool Create Policy Qualification Identify the Server Pool Instance: org-root/sompute-pool-Solie1 (2 v) Server Pool VSPEX-ServerPool-BO-Site1 (2 v) Gualification: Min-Memory v) Qualification: Min-Memory Restrict migration of server: </i>	
		Chart

1

Figure 210 Creating Service Profile Template - Server Assignment

13. Keep all the default values and click **Finish**.

Figure 211	Creating	Service	Profile	Template .	 Policies

🚖 Create		□ ×
Create Serv	vice Profile Template	0
General Networking Storage vNIC/vHBA Placement Boot Order Maintenance Policy Sanse Assistment	Optionally specify information that affects how the system operates. Host Firmware Management Create a Host FV Pack Host Firmware Package: global-default Host Firmware Package Instance: org-root/fw-host-pack-global-default BIOS Configuration Create BIOS Policy	
Policies	BIOS Policy:	
	Create IPMI Access Profile Create Serial over LAN Policy IPMI Access Policy: Serial over LAN Policy:	
	Management IP Address Outband IPv4 Inband Create IP Pool Management IP Address Policy: none	
	< Prev Next > Finite	sh Close

14. After the successful creation of Global Service profile Template, you can proceed with the Service Profile Creation.

Configuring Global Service Profile Instance

ſ

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.

 To create Global Service Profile for Branch office VSPEX servers, launch the UCS Central Web GUI. Click Servers > Global Service Profile Templates > root and click Create Service Profiles from Template.

abab	UCS Domains Fault Summary	
cisco UCS Central		
Domains Servers Network Storage C	ations Management Statistics Logs and Faults Administration Import	
Filter: Global Service Profile Templates	Servers 🕨 🌃 Global Service Profile Templates 👂 🚊 root 👂	
V Servers	Actions: Se	elect A
Image: Solution of the second seco	neral Network Storage vNIC/vHBA Placement Boot Order Policies Usage Faults Events	
VSPEX-SP-Template-BO-Site1	- Status	
Sub-C Properties		
Create Service Profiles From	iplate ment	
	Server Power State:	
Copy XML to Clipboard	Jesired Power State: 1 up	
	Properties	
	Kange UUID	
	Name: VSPEX-SP-Template-BO-Site1	
	User Label:	
	Description: Service Profile Template for VSPE	
	UUID: derived	
	Type: updating-template	

Figure 212 Creating Service Profile from Template

2. Specify the name for the service profile, number of service profile instances to be instantiated and choose the Org as **root**. Then, refer to the sizing guidelines for the number of servers needed for your deployment.

A Properties	⊐ ×
Create Service Profiles From Template	0
Name Prefix: BO-Site1-VSPEX-Server- Number 3 + Org root Org Instance: org-root	
ОК	Close

1

Figure 213 Creating Service Profile from Template - Properties

3. You will see that three service profiles are created.

Figure 214 Verify the Service Profiles Created from the Template

abab		UCS Domains	Fault Summary		Drafomocoo
cisco UCS Central		⊘ ∇			Preletences
		0 36	8 8		
Domains Servers Network Storage 0	Operations Management Statistic:	Logs and Faults A	Iministration Import		_
Filter:	🕳 Servers 👂 😽 Global Service Pr	ofiles 🕨			
- Samer	root				
V Clobal Samina Profiles					
Global Service Promes	General Sub-Organizations Globa	I Service Profiles Status P	auits Events		
	A Filter (off)	rice Profile			6
Global Service Profile Templates	Name	1 A Status	Associated Server	Domain	
Global Service Prolife templates	BO-Site1-VSPEX-Server-1	unassociated	compute/sys-1008/chassis-1/blade-1	VSPEX-FI	
- IN VSPEX SP. Template BO Site1	BO-Site1-VSPEX-Server-2	unassociated	compute/sys-1008/chassis-1/blade-2	VSPEX-FI	
VOPEX-OF-Template-bo-Site1	BO-Site1-VSPEX-Server-3	unassociated	compute/sys-1008/chassis-1/blade-3	VSPEX-FI	
A Sub-Omanizatione					
- M Sub-Organizations					
- A mot					
PAS-DLADE-TEST-SRV1					

4. As 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 select a given service profile and see it's overall status and the association state.

	Actions:	Select Action
eral Network Storage vNIC/vHBA Placement Boot Order UCS Domain View Policies Status Faults Event	s	
Pending Activities		
Reboot Now		
Pending Disruptions: up-time		
Pending Changes: boot-order, networking, operational-policies, server-identity, storage		
cknowledgement State: untriggered		
Acknowledge By:		
Acknowledge By: Change Performed By:		
Acknowledge By: Change Performed By: Schedule:		
Acknowledge By: Change Performed By: Schedule: Status		
Acknowledge By: Change Performed By: Schedule: Status The Change Association The Unassign Server Server Reset Server	Desired Power State	📑 KVM
Acknowledge By: Change Performed By: Schedule: Status Change Association Lucassign Boot Server Shutdown Server Reset Server Overall Status:	C Desired Power State	📑 KVM
Acknowledge By: Change Performed By: Schedule: Status Change Association Consistence Server Server Reset Server Overall Status: Config	C Desired Power State	📑 KVM
Acknowledge By: Change Performed By: Schedule: Status Change Association Consistence Server Server Server Overall Status: Config Association	C Desired Power State	🔀 КУМ
Acknowledge By: Change Performed By: Schedule: Status Change Association Config Association Associate State: Config Association	C Desired Power State	KVM
Acknowledge By: Change Performed By: Schedule: Status Change Association Config Association Associate State: Config Associated Server: compute/sys-1008/chassis-1/blade-3	Desired Power State	KVM
Acknowledge By: Change Performed By: Schedule: Status Change Association Config Association Associate State: Config Associated Server: compute/sys-1008/chassis-1/blade-3 UCS Domain: VSPEX-FI	Desired Power State	B KVM

Figure 215 Viewing Overall Status of the Server

5. Eventually, all the three VSPEX Servers would be associated. Click the Servers > Global Service **Profiles** > root to see the summary of all the servers.

Figure 216 Summary of the Created Global Service profiles

ſ

altaba		UCS	Domains	Fault Sum	nmary		and the second second	Dre
cisco UCS Central		8	V	4	▲			Fit
		1	93	8	8			
Domains Servers Network Storage Ope	rations Management Statistics	Logs and Fa	ults A	dministrati	ion Impor		_	
Filter: All	🔷 Servers 🕨 🐫 Global Service	Profiles >						
v Servers	▲ root							
Global Service Profiles	General Sub-Organizations	obal Service	Profiles	Status Fa	aults Events			
root	A Filter (off) 🕂 Create S	ervice Profile		Create a C	ione 📴 i	Rename Service Profile	Properties	🔂 Delet
Clubel Sector Berlin Templeter	Name	1 🔺	St	atus		Associated Server	Do	main
Global Service Profile Templates	BO-Site1-VSPEX-Server-1	1	ok		comput	e/sys-1008/chassis-1/blade-1	VSPEX-FI	
v-A root	BO-Site1-VSPEX-Server-2	1	ok		comput	e/sys-1008/chassis-1/blade-2	VSPEX-FI	
VSPEX-SP-Template-BO-Site1	BO-Site1-VSPEX-Server-3	+	ok		comput	e/sys-1008/chassis-1/blade-3	VSPEX-FI	
ISCSI vNICs								
v—− II vHBAs								
▶								

6. By launching the UCS Manager GUI, You can also see the Global Service Profiles created on the UCS Manager GUI for the Branch office VSPEX pod.



Figure 217 Verifying Global Service Profiles Through UCS Manager



The above procedure presents a method for creating service profile for Branch office VSPEX servers using UCS Central management located in VSPEX 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 on page 30:

- Configure data stores for ESXi images
- Install ESXi servers and vCenter infrastructure
- Install and configure VMware vCenter server
- Configure storage for VM data stores, install and instantiate VSPEX VMs from vCenter

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.

Figure 218 Rapid Provisioning

Template-Based Deployments for Rapid Provisioning

In an environment with established procedures, deploying new application servers can be streamlined, but can still take many hours or days to complete. Not only must you complete an OS installation, but downloading and installing service packs and security updates can add a significant amount of time. Many applications require features that are not installed with Windows by default and must be installed prior to installing the applications. Inevitably, those features require more security updates and patches. By the time all deployment aspects are considered, more time is spent waiting for downloads and installs than is spent configuring the application.

Virtual machine templates can help speed up this process by eliminating most of these monotonous tasks. By completing the core installation requirements, typically to the point where the application is ready to be installed, you can create a golden image which can be sealed and used as a template for all of your virtual machines. Depending on how granular you want to make a specific template, the time to deployment can be as little as the time it takes to install, configure, and validate the application. You can use PowerShell tools and VMware vSphere Power CLI to bring the time and manual effort down dramatically.

Make sure to spread VMs across different VM datastores to properly load-balance the storage usage. The final snapshot of VMs in a cluster would look similar to Figure 219.

Figure 219 Windo	ow Showing all VMs in	the Cluster		
🖸 🔝 🏠 Home 🕨 🚮 Inve	entory 🕨 🗊 Hosts and Clusters			
I 🗗 🤤 號				
VCenter55.DC.local	BO-VSPEX-Cluster			
BO-Infra	Getting Started Summary Virtu	al Machines Hosts DRS Resou	rce Allocation Performance Tasks & E	vents Alarms Permissions Maps Pr
E bo-infra-host		· · · · ·		
👘 AD-DNS	General		vSphere HA	
🝈 SQLDB	vSphere DRS:	On	Admission Control:	Enabled
➡ VC55-W2K1.	vSphere HA:	On	Current Failover Capacity:	1 host
BO-VSPEX-Cluster	VMware EVC Mode:	Disabled	Configured Failover Capacity:	1 host
bo-vspex-host1			Linet Manifesters	Cookied.
bo-vspex-host2 =	Total CPU Resources:	60 GHz	VM Monitoring:	Disabled
	Total Memory:	511.89 GB	Application Monitoring:	Disabled
VM100	Total Storage:	12.15 TB	Appleadon Honitoning.	Disubica
			Advanced Runtime Info	
× VM12	Number of Hosts:	2	Cluster Status	
N VM13	Total Processors:	28	Configuration Issues	
💑 VM14	Number of Datastara Chistory	0	vSphere DRS	
🝈 VM15 📃	Total Datastores:	4	Tophere bio	
👘 VM16	Total Datastores.	4	Migration Automation Level:	Fully Automated
👘 VM17	Virtual Machines and Templates:	102	Power Management Automation Level	Off
👘 VM18	Total Migrations using vMotion:	0	DRS Recommendations:	0
10 VM19			DRS Faults:	U Apply priority 1, priority 2, and
VM2			Migration Inreshold:	Apply priority 1, priority 2, and priority 3 recommendations
1 VM20	Alarm Actions:	Disabled	Target host load standard deviation:	N/A
VM21	Commende		Current host load standard deviation:	N/A
W122	Commands		View Resource Distribution Chart	
	New Virtual Machine	😭 New Datastore Cluster	View DRS Troubleshooting Guide	
× VM25	Et Add Host			
NM26	Add Host	Euro Setungs	Storage	
💑 VM27	S New Resource Pool		Champer many many	Duius Turan Consultu
💑 VM28			Storage resources A Status	Drive Type Capacity
🝈 VM29			datastorel (1)	mai Non-SSD 92.50 GE
👘 VM3			📋 datastore1 (2) 🥏 Nor	mal Non-SSD 92.50 GE
👘 VM30			NFS-DS1 📀 Nor	mal Unknown 5.99 TE
VM31			👔 NFS-DS2 📀 Nor	mal Unknown 5.99 TE
VM32			<	>
M VM33				

Validating Cisco Branch Office Solution for EMC VSPEX VMware 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.

- Create a test virtual machine that accesses the datastore and is able to do read/write operations. Perform the virtual machine migration (vMotion) to a different host on the cluster.
- Perform storage vMotion from one datastore to another datastore and ensure correctness of data.
- During the vMotion of the virtual machine, have a continuous ping to default gateway and make sure that network connectivity is maintained during and after the migration.

Verify the Redundancy of the Solution Components

Following redundancy checks were performed at the Cisco lab to verify solution robustness. A continuous ping from VM to VM, and vCenter to ESXi 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 FC port connected to Fabric Interconnect A. ESXi hosts should be able to use fabric interconnect B in this case.
- **3.** 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 ESXi 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.
- 4. Reboot one of the two 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.
- 5. Fully load all the virtual machines of the solution. Put one of the ESXi host in maintenance mode. 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 ESXi hosts to accommodate VMs from the host put in maintenance mode.
- 6. Reboot the host in maintenance mode, and put it out of the maintenance mode. This should rebalance the VM distribution across the cluster.

Cisco Validation Test Profile

"Vdbench" testing tool (ver.5.04) was used with Windows 2012 server to test scaling of the solution in Cisco labs. Following is the detail on the test profile used.

Profile Characteristics	Value
Number of virtual machines	100
Virtual machine OS	Windows Server 2012
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

Table 10Vdbench Test Profile

Bill of Material

The table 6. gives details of the components used in the CVD for 100 virtual machines configuration.

Table 11 Component Description	ion
--------------------------------	-----

Description	Part Number
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 at:

http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6300-series-fabric-int erconnects/datasheet-c78-732207.html

Customer Configuration Data Sheet

Before you start the configuration, gather some customer-specific network and host configuration information. Table 12, Table 13, Table 14, Table 15, Table 16, Table 17, and Table 18 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.

Server Name	Purpose	Primary IP
	Domain Controller	
	DNS Primary	
	DNS Secondary	
	DHCP	
	NTP	
	SMTP	
	SNMP	
	vCenter Console	
	SQL Server	

Table 12Common Server Information

Table 13ESXi Server Information

I

Γ

Server Name	Purpose	Management IP	Private Net (storage) addresses		vMotion IP
	ESXi Host 1				
	ESXi Host 5				

Table 14Storage Array Information

Array name	
Admin account	
Management IP	
Storage pool name	
Datastore name	
NFS server IP	

Table 15 Network Infrastructure Information

Purpose	IP	Subnet Mask	Default Gateway
Cisco UCS virtual IP address			
Cisco UCS FI A address			
Cisco UCS FI B address			

Table 16VLAN Information

Name	Network Purpose	VLAN ID	Allowed Subnets
vSphereMgmt	Virtual Machine Networking		
	VMware ESXi Management		
Storage	NFS VLAN		
vMotion	VMware vMotion traffic network		
VM-Data	Data VLAN of customer VMs as		
(multiple)	needed		

Table 17VSAN information

Name	Network Purpose	VSAN ID	FCoE VLAN ID
Storage	Storage Access		

Table 18 Service Accounts

Account	Purpose	Password (option, secure)
Admin	UCS Manager administrator	
Admin	UCS Central	
	Windows server administrator	
Root	ESXi root	
	EMC VNXe array administrator	
	vCenter administrator	
	SQL server administrator	

Conclusion

The Cisco branch office solution uses common components of EMC VSPEX Integrated Infrastructure with new introductions such as the Cisco UCS Mini and EMC VNXe 3200 for a version of traditional VSPEX solutions that is ideal for small and medium businesses. 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 the integrated computing stack, augmenting their original design with support for 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

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_Firm ware_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-su pport-series-home.html

VMware vSphere:

http://www.vmware.com/products/vsphere/overview.html

VMware vSphere 5.5 Documentation:

http://pubs.vmware.com/vsphere-55/index.jsp EMC VNXe32xx Series Resources: http://www.emc.com/storage/vnx/vnxe-series.htm#!resources EMC Support: (requires user registration) http://support.emc.com Microsoft SQL Server Installation Guide: http://msdn.microsoft.com/en-us/library/ms143219.aspx

ſ